Gratis

entrevista con
Cap'n Crunch

DISCLAIMER:

Esta revista electrónica fue creada con el propósito de entretener y proporcionar material de investigación al pueblo mexicano y a nuestros hermanos hispano parlantes. Nosotros en la MHM no nos hacemos responsables del uso que se le dé a la información contenida en ella.

Los textos, gráficas y diagramas publicados aquí, se exponen con el fin de proporcionar datos y material técnico y de investigación mismos que deberán ser empleados siempre con fines educativos.

Los autores de cada texto son los únicos responsables de la veracidad de sus publicaciones y las ideas y opiniones dadas a conocer no necesariamente representan las del editor o el grupo.

Contenido

Información Nutrimental

Tamaño por Porción 1 zine
Porciones por Envase aprox. 46 páginas

Contenido Energético 2600 kcal
Contenido del E-Zine:

Tema	Autor	Página
Introducción	-=oSUKARu=-	4
Introducción a los PBX	-=oSUKARu=-	5
"Where Have All The Hackers Gone"?	Jump'n Jack	8
Emuladores T2G	o0ShellGhost0o	9
MegaCable	Angel Hack	15
Entrevista al Cap'n Crunch	-=oSUKARu=-	16
Derechos Humanos	-=oSUKARu=-	19
Phreaking el NEC 300	Jalisco	21
Caja de Neón	o0ShellGhost0o	23
Comix	-=oSUKARu=-	25
Estudio Venezolano de Telefonía Celular	*OoChip	26
·3N$AMBLADOR KON MANZANA$	(oPKo)	31
Nuevas Tecnologías	-=oSUKARu=-	35
KOMO HAM GRATI$ DE$DE LA UNITEC c. CUITLAHUAC	(oPKo)	38
Estudio sobre el Teléfono Modular	*OoChip	39
Despedida	-=oSUKARu=-	46

*Las cantidades de textos en esta revista electrónica están basados en la dosis recomendada para una dieta balanceada en phreaking, electrónica y tecnología underground.

Introducción

Notas del Editor

Llegamos a la edición 6 de este e-zine y nos complace anunciarles que esta vez si pudimos incluir la entrevista con el famoso Cap'n Crunch, además de ese artículo hemos incluido artículos que van desde creación de emuladores hasta una revisión a la tecnología de los monederos electrónicos pasando por trucos para llamar gratis e incluso una excelente guía de clonación de celulares.

El diseño de este número se basó un poco en el diseño usado en la página, nos gustaría mucho oír sus comentarios al respecto.

Y como hoy no tengo ganas de decir más, espero que disfruten los textos que preparamos!

-=oSUKARu=-
mhmphreak.com

Introducción a los PBX

"Guía básica para el Novato"

por -=oSUKARu=-

Introducción:

Muchos de ustedes han escuchado hablar o incluso han tenido la oportunidad de emplear un PBX para la realización de llamadas gratuitas de larga distancia, pero no tienen conocimiento de que son o como encontrarlos, en este texto intentaré explicar de forma clara el principio de funcionamiento de un PBX, y unas cuantas técnicas básicas para encontrarlos.

PBXs:

La primera duda que se viene a la cabeza al escuchar estas siglas es: ¿exactamente que significan?. PBX es la abreviatura de Private Branch eXchange (intercambiador de líneas privadas), y se puede definir como una pequeña centralita telefónica con la cual se administra el control de las líneas dentro de una empresa.

Los PBX's son comúnmente empleados en empresas privadas, instituciones de gobierno, universidades, etc. Y en cualquier lugar donde se requiera el manejo interno de varias líneas. Imagínate cuanto le costaría a una empresa tener una línea por cada ejecutivo o cada área dentro de esta misma. Hay es donde los PBX's entran en acción, multiplexando una sola línea en cientos de extensiones.

Aun y cuando este es el propósito general de tener un PBX, en realidad sirven para mucho más cosas, lo nuevos modelos tienen funciones bastante avanzadas, como forwarding, conferencias, correos de voz, y transferencia de líneas por nombrar algunos. Estos servicios son generalmente disponibles a todo el público pagando una cuota a TELMEX por cada uno de ellos, pero se encuentran ya entre las funciones que realizara un PBX. Un PBX también permite a las compañías controlar que tipo de números puede un empleado marcar.

Muchas empresas tienen contratados números 01-800, con los cuales sus ejecutivos pueden realizar llamadas de larga distancia sin necesidad de pagar por ellas. Este tipo de PBX son llamados Extenders y su única función es esa, permitir llamadas de larga distancia a través del 01-800. Estas llamadas se guardan en una base de datos y son cobradas a la compañía a la cual pertenece la persona que llamó.

Como encontrar Extenders:

Para encontrar un extender tendremos que hacer un scan de varios números 01-800 hasta encontrar una de estas señales:

- Tonos extraños
- Tonos con diferente cadencia (más rápido o más lento que un tono normal)
- Líneas que contestan pero sin tono ni grabaciones.

En caso de encontrar alguno de estos tipos de señales, apuntamos el numero en una libreta junto con el comentario de que fue lo que escuchamos.

Por ejemplo:

01-800-XXX-XXXX ← Tono agudo.

Una vez que encontramos ese número tenemos que encontrar como realizar la llamada. Por lo general se necesita una contraseña seguida de la lada y luego el número a marcar. Las contraseñas por lo general son de cuatro dígitos, pero pueden llegar a ser de muchos más.

También hay que tener en cuenta que algunos Extenders no funcionan de la misma forma, puede ser que te topes con un número que primero te pida la lada y el número seguidos por la clave o uno que te pida dos claves antes de permitirte ingresar el número a marcar.

¿Entonces, cómo jodidos voy a saber como hacerle? Prueba ingresando números hasta que el tono cambie, si presionaste cuatro números y en ese momento cambio el número significa que el extender te está pidiendo primero el código de acceso y después el numero a marcar, si en cambio te deja meter hasta 10 números antes de que cambie el tono significa que necesitas hacerlo de la otra forma.

Hay unos extenders que incluso te dirán: “El código de X dígitos es incorrecto, favor de introducirlo de nuevo”. Muchas veces esto ocurre también cuando dejas que pase el tiempo sin presionar nada.

Hay que recordar que debido a que el abuso de este tipo de sistemas no es cosa nueva, muchos de ellos necesitan de caracteres especiales para hacerle saber al extender que hemos terminado de digitar la clave. Por lo general se emplea el # aunque puede ser que también sea empleado el *.

Cómo encontrar PBX’s normales:

Por lo general al llamar a un PBX, la contestación que obtendremos será una grabación indicándonos que extensiones debemos marcar para llamar a cierta sección o área de la empresa.

La ventaja de buscar este tipo de PBX’s, es que por lo general se encuentran en números locales como llamando a una Universidad o a un Hospital y por lo general este tipo de instituciones no reciben tantos intentos de hacking a su sistema telefónico por lo que es seguro que no se molestarán en instalar medidas de identificación de llamadas o de rastreo.

El único problema es que puede llevar un poco más de tiempo encontrar como realizar una llamada desde el exterior e incluso puede ser que no tengan activado este servicio.

Para empezar a buscar haz lo siguiente:

1- Llama al número que sabes que tiene un PBX
2- Cuando escuches la grabación intenta presionando #, * o 9
3- Si estos dígitos no te dieron acceso a ningún lugar interesante prueba combinaciones distintas, tarde o temprano tendrá que ceder

Muchas veces a estar jugando con estos números caerás en algo interesante como puede ser escuchar los buzones de voz de ciertas personas, borrar sus mensajes, configurar que cuando llamen a ese número enlace a otro, etc...

Lo bueno de este tipo de PBX’s es que generalmente una grabación te asiste a lo largo de casi todo el camino.

Otra ventaja es el poder hacerte pasar por otra persona y emplear métodos de Ingeniería Social para obtener lo que queremos.

Notas Finales:

Como verán no es tan difícil encontrar números de extenders y PBX, y con un poco de paciencia y sentido común en poco tiempo se pueden encontrar las claves.

Que se necesita tiempo para encontrarlos y para crackearlos no hay duda, pero si escaneamos desde una caseta unos 20 números cada noche, y nos apoyamos en amigos para distribuirnos diferentes teléfonos el trabajo se hace mucho menos pesado.

Cuando encuentren un PBX o un Extender, traten de no abusar mucho para que la compañía no note que alguien esta abusando se sus sistemas. Además recuerda que aunque estas llamadas resultan gratis para ti, la compañía las tendrá que pagar de cualquier forma así que procura no cargarles mucho la mano.

-=oSUKARu=-
mhmphreak.com

"Where Have All The Hackers Gone"?

Original Poetry by: Jump'n Jack Flash -916-

On a cold night in the dead of winter a soul stumbles into #hack and asks:
'Where have all the Hackers Gone?'

Immediately the group recognizes him as one of the originals.

'Help us change our grades!' a voice calls out from the huddled masses.
'Help me hack root on a NYNEX system!' another voice asks.

The soul clutches his bowed head and covers his ears, trying to remember back to before he involuntarily left the scene a few years ago.

'The only thing that kept me sane while I was imprisioned was the thought of seeing my friends and fellow hackers, now I demand you tell me Where Have All The Hackers Gone?' the soul begs the crowd of jubulent newbies.

Silence is the only answer he receives,
For there are no real hackers here.

Then a voice speaks up and says,
'They're gone! You're the first we've seen!'
The soul asks,
'What do you mean?'

And Silence is the only answer he receives,
For there are no real hackers here.

And like a wall crumbling down it comes to him and he falls to his knees,
like hunting for human life after a Nuclear war he stumbles out of the room,
And he hurries to the place where only the Elite could go just a few years ago,

But when he arrives he is shocked and amazed,
There are no hackers here on this dark winter day.

And he stumbles into traffic,
feeling the snow crunch beneath his feet,
and he shouts into the night for the elite,

'Where Have All The Hackers Gone?'

And Silence is the only answer he receives,
For there are no real hackers here.

Poema extraído de Phrack 50

Emuladores T2G

"Guía acerca de los Emuladores T2G"

por o0ShellGhost0o

Introducción:

Veo que sigue habiendo gente que aun tiene bastantes dudas acerca de los emuladores y que cada que una persona entra a los foros o a la página, pregunta lo que muchas veces ya se ha escrito antes en otros lugares. Por eso mismo me dispongo a crear una guía que despeje las dudas más comunes que un novato pueda tener.

Teoría:

No voy a escribir toda la teoría relacionada con las tarjetas telefónicas, ya que sin duda alguna hay ya muy buenos textos que tratan de eso. Si tienes ganas de leerlos, baja los ezines del 1 al 4 y lee el texto escrito por mi amigo El Narco, o ve a nuestra página y entra a la sección de Telecards, ahí encontrarás un zip llamado "información de las tarjetas de 128 bits", bájalo y dale una buena leída.

A lo que me voy a enfocar en este texto es a la parte de crear todo lo necesario para realizar un emulador.

Antes que nada, **¿qué es un emulador?**

Un emulador es un dispositivo electrónico el cual te permite simular el funcionamiento de una tarjeta telefónica original. La idea de realizar un emulador nace en Europa y entre sus padres se reconoce al Francés Bausson, el mismo que escribiera el primer texto que se publicara acerca de esto para la revista Americana Phrack.

Para hacer un emulador es necesario tener conocimiento de cómo funcionan exactamente las tarjetas que queremos emular para después encontrar un algoritmo que nos permita por medio de microcontroladores o circuitos digítales crear el aparato.

¿Qué necesitamos para tener acceso a esa información?

Aparte de leer los dos textos que les sugerí al comienzo de este texto necesitarán lo siguiente:

- Lector de Tarjetas Telefónicas
- Logger de Datos
- Visualizador de datos
- Doblador de Logs (opcional)

Lector de Tarjetas Telefónicas

Un lector de tarjetas telefónicas como su nombre lo dice es la combinación de un hardware y software que te permiten leer el contenido de una tarjeta original. El contenido que te dará dicho lector es comúnmente conocido como **mapa de memoria**.

Descripción de los mapas de memoria para tarjetas T2G mexicanas según Cartman:
//begin

Byte:	Función:
0	E8h, constante
1	3Dh, constante
2	59h, constante
3	num. serie (MSB)
4	num. serie
5	num. serie
6	num. serie
7	valor de la tarjeta: 23h=$30, 35h=$50 y 31h=$100
8	contador octal (MSB)
9	contador octal
10	contador octal
11	contador octal
12	contador octal (LSB)
13	FFh, constante
14	? presumiblemente checksum
15	? presumiblemente checksum
16-63	FFh, constante

//end

Aquí hay unas cuantas cosas que tomar en cuenta y que agradezco a SomeOne el haberlas mandado:

//begin
Escritura en el byte 0 produce lo mismo que solo pulsos de CLK, lectura.
En el Byte 1 ocurre un noWrite (no escribe y punto).
Bytes del 2-8 se produce un bloqueo se queda en el ultimo bit mandado, sea cero o uno.
9-13 Contador octal.
14 Bloqueo excepto en el bit 110 que activa el **challenge** (Sí, las tarjetas de telmex aceptan challenge)
15 -16 (16 bit data area) area de datos 1, escritura permitida pero WriteCarry no.
41-48 (bit 320-383) area de datos 2 de 64 bits, escritura permitida pero WriteCarry no.
//end

El contador octal es la parte donde se guarda toda la información del crédito en la tarjeta, es la única parte donde tu emulador debe permitir que se escriba.

El funcionamiento del contador octal es muy similar al funcionamiento de un ábaco, donde tenemos que cada bit en la parte inferior (en el LSB) vale 1, en el siguiente byte cada bit vale lo que vale el byte completo de abajo, es decir 8, y así se sigue hasta llegar al MSB.

Ejemplo:

Byte	Mapa	Valor
8	0000 0001	4096
9	0000 0001	512
10	0000 0001	64
11	0000 0001	8
12	0000 0001	1

Si tuviéramos este mapa de memoria, el saldo de la tarjeta sería: 4096+512+64+8+1 = 4681, en pesos sería $46 pesos con 81 centavos.

En caso de querer sacar el contador octal que tendría una tarjeta de $50, hacemos lo siguiente:

Tomamos la cantidad y le añadimos los centavos: 50,00 = 5000

Dividimos la cantidad entre el valor del primer byte para saber cuantos bits van en ese byte: 5000/4096 = 1.22

De ahí sabemos que un bit va a ir a 1 en ese byte, multiplicamos el numero de bits que salieron por el valor del byte y le restamos a el valor original el numero obtenido: 1*4096 = 4096; 5000 – 4096 = 904.

Este numero lo dividimos entre el valor del siguiente byte y realizamos los mismos cálculos que hicimos arriba. De estos cálculos tenemos que vamos a tener un bit a 1 en el byte 9, repitiendo el proceso tenemos 6 bits a 1 en el byte 10 y un bit a 1 en el 11, cero en el 12.

El resultado seria algo así:

Byte	Mapa	Valor
8	0000 0001	4096
9	0000 0001	512
10	0011 1111	64
11	0000 0001	8
12	0000 0000	1

1*4096 + 1*512 + 6*64 + 1*8 + 0*1 = 5000

Pero como se trata de un ábaco también podemos expresarlo como:

Byte	Mapa	Valor
8	0000 0001	4096
9	0000 0001	512
10	0011 1111	64
11	0000 0000	8
12	1111 1111	1

1*4096 + 1*512 + 6*64 + 0*8 + 8*1 = 5000

La caseta realiza esta operación de cambiar un bit de un nivel superior por un byte de un nivel inferior para descontar el saldo de las tarjetas. A esta operación se le llama **Writecarry**

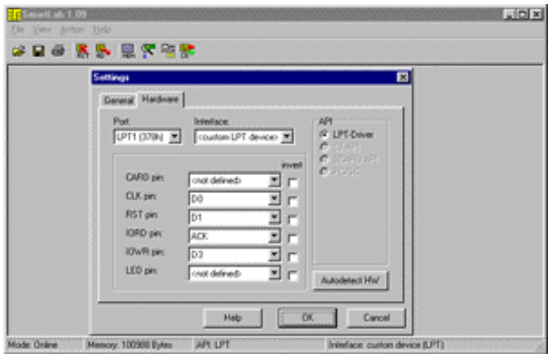
Comprendiendo bien esto del contador octal podemos tomar cualquier tarjeta, aun estando agotada y cambiar el ábaco para tener dinero al meter el mapa en el emulador.

Lectores recomendados:

- Elektron
- Smart Lab (solo con éste podrás probar el challenge/response)
- Chipy

Como hacer el Hardware para el Elektron y el SmartLab:

El Elektron no necesita de hardware especial, solo hay que conectarlo conforme dice el texto que viene dentro del zip. En caso de leer datos erróneos será necesario desconectar los pines que van a VCC Y GND, y conectar directamente una fuente externa a 5V CD.



El Smart Lab trae un archivo de Help bastante completo en el cual viene los tipos de hardware con los que funciona, sin embargo es posible emplear el mismo arreglo que se emplea para el elektron, haciendo unos pequeños ajustes en la configuración del programa como se ve en la figura 1.0

Figura 1.0 Settings del Smart Lab

Logger y Visualizador de LOGs

Aparte de saber que trae adentro una tarjeta telefónica, hay que saber como responde a los pulsos que envía una caseta. Esto es lo más importante porque no todas las casetas en México hacen las mismas comprobaciones, además de que estas comprobaciones no vienen descritas en ningún texto debido a que depende mucho de las técnicas que TELMEX use para comprobar que una tarjeta es valida o no.

Un logger es un programa que registra todos los datos generados por una caseta y los va guardando en un archivo para después analizarlo por medio del visualizador.

Loggers recomendados:

- Cartman
- ODT
- Sniffer

El de Cartman es el más recomendable debido a que fue hecho en C y es de todos conocido que este lenguaje tiene muchas ventajas al tratarse de acceso al hardware.

Las conexiones del logger vienen en el zip, e incluso Cartman puso una imagen de cómo conectarlo a la PC.

Al tener el log listo, solo es cuestión de abrir el visualizador y cargar el archivo como se ve en la figura 1.1.

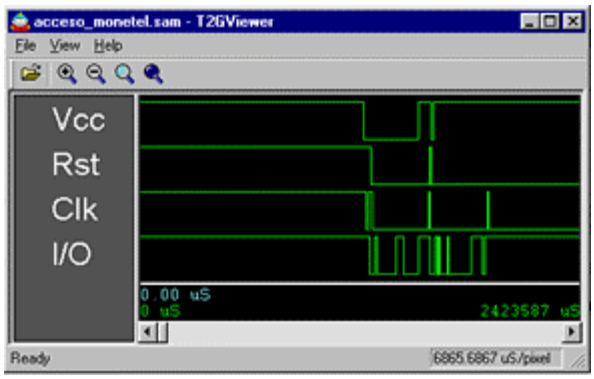


Figura 1.1 Visualizador de LOGs por Cartman

Cómo leer los LOGs:

Lo que te dan los logs son unos trenes de pulsos conocidos como **diagramas de tiempos**. Estos diagramas representan un 1 lógico cuando la línea está en alto y un 0 lógico cuando la línea está en bajo. Para comprender como funciona esto solo hay que ver que pasa en I/O cuando hay cambios en CLK y RST.

Si al ver esas gráficas no comprendes absolutamente nada, lee de nuevo los textos guías que recomendé en un principio, verás que poniéndole un poco de atención será fácil comprenderlos.

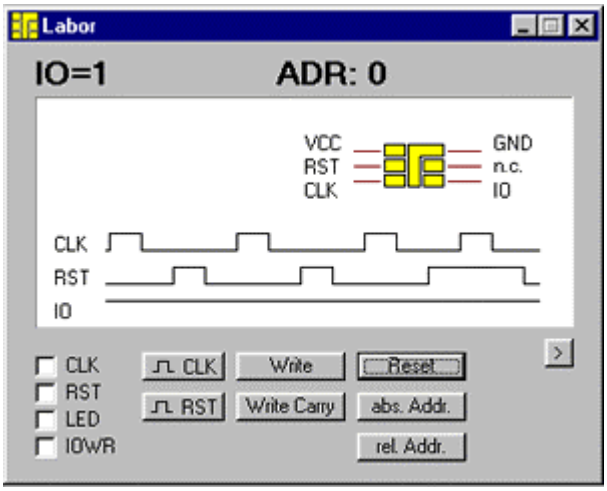


Figura 1.2

Doblador de LOGs

Un doblador de logs es un software que te permite tomar los datos obtenidos por medio de un logger de una tarjeta original para de ahí mandar impulsos al puerto paralelo y ver como responde tu emulador.

El único doblador de logs que conozco es para el Logger de ODT, sin embargo no es difícil crear uno si se tienen conocimientos básicos de programación.

Algo similar se puede hacer empleando el “Lab” del SmartLab, solo que mandando los datos uno a uno como se ve en la figura 1.2

Creando el Emulador

A estas alturas ya habrás conseguido suficiente información como para realizar tu emulador, ahora solo falta hacer el programa y el hardware.

Antes que nada necesitas escoger el microcontrolador que vas a emplear. El famoso PIC 16F84 parece ser la opción numero uno al momento de tratarse de emulación de tarjetas telefónicas. Sin embargo hay varios tipos de micros de cuales escoger, todo dependerá de tu experiencia en micros y tus preferencias.

Si aun evaluando diferentes opciones decides quedarte con el 16F84, quizás lo que más te convenga es emplear el hardware que todo el mundo esta empleando. El famoso hardware de T2G de Zacky se muestra en la figura 1.3

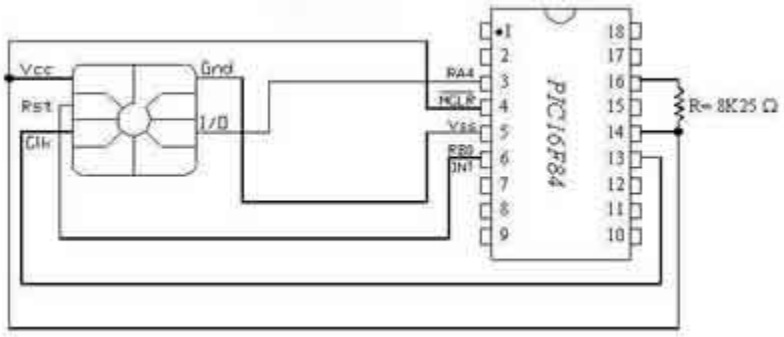


Figura 1.3 Esquema de un Emulador T2G

Este diseño puedes pasarlo a EAGLE para realizar el PCB o emplear alguno de los PCBs que se encuentran en nuestra página en la sección de telecards. Pero yo les recomendaría hacer el PCB de la tarjeta de prototipos que diseñe para el primer ezine para que puedan cambiar la configuración de pines, además de agregar y quitar dispositivos electrónicos según requieras durante la etapa de pruebas.

Haciendo el Software

Bueno ahora si ya tienes todo lo que necesitas, es hora de hacer el software. Si sabes bien programación de PICs no tendrás ningún problema realizando el software con toda la información obtenida, si no sabes programar, no te preocupes, el PIC16f84 consta de solo 35 instrucciones las cuales son relativamente fáciles de aprender, además de que en la página tenemos varios códigos en los cuales te puedes basar para realizar tu propio código.

Los PICs se programan en una especie de ensamblador especialmente creado por Microchip para este propósito. De la página principal de esta compañía puedes descargar el MPLAB, el software más usado para editar códigos para PICs.

No voy a entrar en más detalle de la programación, así que les recomiendo que se bajen el datasheet del PIC y uno que otro curso para PICs (tenemos un libro para descargar en la página).

Cuando hayas terminado con la programación al compilar tu código el MPLAB generará un archivo .HEX, este es el archivo que va dentro del PIC. Para meterselo a tu PIC solo necesitarás un programador de PICs como el JDM o el TE20 y un programa como el Icprog.

Si quieren saber más acerca del JDM o del Icprog lean la ezine 5, ahí oSUKARu hace un review de ambos.

Para Concluir:

Espero que esta guía haya sido de su agrado y que hayan aprendido algo nuevo leyéndola. Recuerden que hacer un emulador no es cosa de un solo día, lleva tiempo y requiere de paciencia. Si tu no tienes ganas de aprender el funcionamiento de una tarjeta telefónica y tan solo quieres realizar llamadas gratuitas, puedes ir a Tepito a comprar un emulador ya hecho.

El fin principal de hacer un emulador es aprender el funcionamiento de un sistema que en este caso son las tarjetas telefónicas y probarte a ti mismo que eres capaz de hacer una copia exacta con los conocimientos que has adquirido.

Cualquier duda que tengan al respecto súbanla al foro de telecards, ahí encontraran gente que se reúne con el mismo propósito y que estará gustosa de ayudar.

o0ShellGhost0o
Mexican Hackers Mafia 2003
http://www.mhmphreak.com
http://www.mhmphreak.da.ru

MegaCable

"Como abrir más canales"

por Ángel Hack

Un día estaba de huevon (raro en mi) estaba viendo la tv entonces le pasé a Warner Channel (Kanal 15), después volví a pasarle al kanal 15 y salió una imagen de otro kanal entonces agarre de inmediato el control y le agregue sintonía fina después de agregarle al fin apareció el kanal era el Sony (kanal 66). Que raro!!

Tenia 2 kanales 15 uno normal llamado 15 y el otro decía 15 CATV cheque con mas kanales y sucedió lo mismo kon los kanales 15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30 y aparecieron kanales como mtv(kanal 67) unikable (69) Telehit(68) animal planet (72) history (73) pero en el servicio Mini Basiko no tienes estos kanales solo del 2 al 40 esto podría servir pero después de checar en mi kaso yo pago MiniBasiko pero me dan el Básico.

Esto sucede porque en algunas partes no han agregado las kajas del MiniBasico pero en otros lados ya están así que no tienen todos los kanales y koneste pequeño truco logre abrir mas kanales espero les sirva de algo y respondan sobre los resultados ....

By Angel Hack
hugo_guapito@hotmail.com

- -

Provado con Tv:
LG Flatron RP-21FA37 21"

Entrevista al Cap'n Crunch

"Ideas y comentarios del inventor del Phreaking"

por -=oSUKARu=-

Introducción:

Su nombre es John Draper, y es sin duda alguna una de las personalidades más reconocidas en todo el mundo por sus descubrimientos acerca del funcionamiento del sistema telefónico a principios de los años 70's.

Obtuvo su apodo de la misma caja de la que obtuvo su famoso silbato capaz de reproducir un tono continuo de 2600Hz con el cual engañaba a las centralitas telefónicas para tener acceso a los sistemas de señalización, los cuales manipulaba a su gusto.

Es reconocido como el padre del phreaking y creador de caja más famosa de todas, la *"Blue Box".*

Se convirtió rápidamente en el héroe de miles de personas, entre ellos Steve Wozniak el inventor de las computadoras Apple y su colega Steve Jobs quienes recibieron importantes enseñanzas en materia de telecomunicaciones de este Icono de la cultura underground en su juventud.

Por más de 30 años John Draper ha sido una influencia notable en todo aquel que se inicia en el phreaking. No hay persona que en sus primeros años aprendiendo no haya leído acerca de él o de sus conocidas hazañas.

Por todas estas cosas me enorgullece realmente poder presentarles a todos ustedes una pequeña entrevista que nos da a conocer las ideas y comentarios que este hombre tiene que dar a la creciente comunidad phreak en México acerca de sus planes, proyectos y un poco de su vida personal.

Foto histórica. De izquierda a derecha
John Draper, Kevin Mitnik, Steve Wozniak

Entrevista (Versión Original):

-=oSUKARu=-: First of all, Mr. Draper thank you so much for accepting to do this interview, it means a lot to us.

-=oSUKARu=-: What's John Draper doing now and what plans does he have in mind for the near future?

Cap'n Crunch: I'm working on a means for people to have a spam free internet experience.

-=oSUKARu=-: How does it feel to be the creator of the whole phreaking scene?

Cap'n Crunch: It sucks... I'm constantly struggling to survive. I get it from both sides.

-=oSUKARu=-: Does it amazes you the huge impact that you've been causing on the youth for more than 30 years?

Cap'n Crunch: Huge impact? Me? Where have you heard that?

-=oSUKARu=-: Do you still phreak?

Cap'n Crunch: Come on, be serious... I think you know the answer to that.

-=oSUKARu=-: What do you think is the proportion of phreaks in the world?

Cap'n Crunch: Do you mean proportion? If so, probably not as high as one might think. After all, currently... global communication is free, there is no need to try and rip off the phone company anymore.

-=oSUKARu=-: What's the main diference you notice in the way that Telephone Companies handle security now, and the way they did on the 70's?

Cap'n Crunch: I wouldn't know. They are so diversified.

-=oSUKARu=-: It's known that you like to travel, have you had a chance to come to Mexico? If so, can you please tell us your impresions?

Cap'n Crunch: I've traveled to Mexico on MANY ocassions. I always look forward to visiting Mexico, and have lots of friends all over. Mexico City, Querétaro, Tijuana. I really like the people. They are more "real" and sincere.

-=oSUKARu=-: What advice would you give to the growing Mexican phreaking scene?

Cap'n Crunch: It's alive and wonderfully freakable...

-=oSUKARu=-: Thank you very much for taking some time of your schedule to let us know a bit more about you.

Cap'n Crunch: Sure...

Entrevista (Traducción):

-=oSUKARu=-: Antes que nada, Mr. Draper muchas gracias por acceder a esta entrevista, significa mucho para nosotros.

-=oSUKARu=-: ¿Qué está haciendo John Draper ahora y que planes tiene en mente para el futuro?

Cap'n Crunch: Estoy trabajando en los medios para ofrecer a las personas una experiencia de Internet sin e-mail no solicitado (spam).

-=oSUKARu=-: ¿Qué se siente ser el creador de toda la escena phreak?

Cap'n Crunch: Apesta... Me encuentro en constante lucha por sobrevivir. Me llega por ambos lados.

-=oSUKARu=-: ¿Le sorprende el impacto tan excepcional que ha causado en la juventud por más de 30 años?

Cap'n Crunch: ¿Impacto excepcional? ¿Yo? ¿Donde escuchaste eso?

-=oSUKARu=-: ¿Sigue phreakeando?

Cap'n Crunch: Vamos, en serio... Creo que ya sabes la respuesta a eso.

-=oSUKARu=-: ¿Cuan grande es la proporción de Phreaks en el Mundo?

Cap'n Crunch: ¿Proporción? Probablemente no tan alta como uno pudiera pensar. Después de todo, ahora... la comunicación global es gratuita, ya no hay necesidad de tratar de estafar a la compañía telefónica.

-=oSUKARu=-: ¿Cuál es la mayor diferencia en la forma en que las compañías telefónicas manejan la seguridad hoy en día a como lo hacían en los 70's?

Cap'n Crunch: No podría saberlo. Son muy diferentes unas de otras.

-=oSUKARu=-: Sabemos que le gusta viajar, ¿Ha tenido alguna chance de visitar México? De ser así, ¿podría comentarnos sus impresiones?

Cap'n Crunch: He viajado a México en MUCHAS ocasiones. Siempre estoy esperando ir de nuevo, porque tengo muchos amigos allá. En la ciudad de México, Querétaro y Tijuana. Realmente me gusta el pueblo mexicano. Son más "reales" y sinceros.

-=oSUKARu=-: ¿Qué consejo le daría a la nueva y creciente comunidad phreak Mexicana?

Cap'n Crunch: Estar viva y maravillosamente freakeable...

-=oSUKARu=-: Muchas gracias por tomar el tiempo para darnos a conocer un poco más de usted.

Cap'n Crunch: Claro...

Derechos Humanos

Tus derechos básicos ante la ley

por -=oSUKARu=-

Recibimos muy buenas críticas del artículo de Cult of the Dead Cow que publicamos sobre *hacktivismo* y muchos de ustedes nos pidieron algo acerca de leyes en México para saber como actuar en caso de ser victima de las autoridades, hice una pequeña investigación y esto es lo que encontré:

Con fundamento en los artículos 14 y 16 de la Constitución Política de los Estados Unidos Mexicanos; 61, 73 y 123 del Código Federal de Procedimientos Penales; 132, 262 y 266 del Código Penal para el Distrito Federal en materia del fuero común y para toda la República en materia de fuero federal y sus correlativos en los Estados de la República.

1. No puede usted ser detenido sin una orden de aprehensión expedida por un Juez; excepto en el momento de cometer el delito (flagrancia), o cuando no exista Juez en el lugar.
2. Nadie debe entrar en su casa sin su permiso si no lleva una orden de cateo, expedida por un Juez.
3. Una orden de presentación es la que gira el Ministerio Público para que, durante la investigación de un delito nos presentemos a declarar.

En caso de haber sido detenido:

Con fundamento en los artículos 16, 19 y 20 constitucionales; 123, 124 bis, 128, 134, 135, 206, 207, 217, 287, 298, 399, del Código de Procedimientos Penales para el Distrito Federal y demás relativos y aplicables.

Usted tiene derecho a :

1. No declarar nada ante agentes de la policía.
2. No ser incomunicado.
3. Comunicarse con su abogado, familia, amigo o cualquier persona de confianza.
4. No declarar si no quiere hacerlo ante el Ministerio Público.
5. Que se le explique de qué y quién lo acusa.
6. Firmar un amparo si quiere hacerlo.
7. Utilizar un teléfono o cualquier otro medio de comunicación.
8. Tener un traductor si no habla usted bien el castellano.
9. No ser maltratado física ni moralmente.
10. Que lo revise un médico cuando usted lo solicite.

11. Presentar testigos o pruebas de su inocencia.

12. Ser puesto en libertad si no hay elementos suficientes para ser consignado.

13. Que su detención no exceda de 24 horas sin que se justifique con su consignación o puesta a disposición de un Juez. A partir del momento en que sea puesto a disposición de un juzgado, no deben pasar más de 72 horas sin que la detención se justifique con auto de formal prisión.

14. Obtener su libertad bajo caución o arraigo si cumple con los requisitos para ello.

Está prohibida la tortura, jamás se le puede golpear, tener sin comer, amenazar, ni obligar por ningún medio a declarar en su contra.

Oficinas encargadas de proteger sus derechos a las que puede recurrir:

- Comisión Nacional de Derechos Humanos.
- Secretaría de la Contraloría General de la Federación.
- Sistema Nacional de Atención Ciudadana.

-=oSUKARu=-
mhmphreak.com

Phreaking el NEC 300

Como cambiar el ESN en este modelo

por Jalisco

1. Convertir en ESN a formato tacs habré el programa de **esn.exe** y te aparece un menú y seleccionas la opción 5 y te aparece un cuadro con tres opciones.

Ejemplo:

HEX: FFFFFFFF	aquí en este espacio ingresaras él numero de serie ó ESN para convetirlo para ingresarlo en la memoria del celular.
TACS: 63/63/63/65535	en este lugar te aparece el resultado el cual anotaras tal y como te aparezca para que puedas programar tu fon.
AMPS: 255/16777215	este espacio se utiliza cuando el ESN te lo dan en decimal y no en hexadecimal como lo ingresamos arriba.

2. Después de esto correrás el programa **p300.exe** el cual sirve para programar el teléfono al ejecutarlo te aparecerá lo siguiente:

ATTACH PHONE AND SWICH ON, THEN PRESS P FOR P300 OR N FOR 9a/11a:

Presiona “P” ya que esta opción es la del teléfono que tu tienes después aparace lo sig.

Enter new esn in the following format xx/xx/xx/xxxxx

Aquí pondrás el numero que anotaste de la conversión del numero de serie ó ESN y una vez ingresado prendes el teléfono y le conectas la interfase y presionas enter veras unos puntos que comienzan a correr en la pantalla de tu compu y si vez que se detiene en el punto 6 tienes problemas ya que el procesador que tienes es muy veloz y el programa no lo soporta.

Yo estoy usando un AMD k6 en DOS puro y funciona a la perfección; Bueno pero si los puntitos siguieron corriendo buenas esta madre si jalo y entonces al teléfono se el pondrá la pantalla en negro y parpadeará 3 veces y se detiene ahí te aparecerá en la pantalla el nuevo número de serie ósea el que quieres ingresar si esto es positivo ósea que si esta ahí el ESN seguirás con los siguientes pasos y si no vuelve a ingresarlo con p3.exe.

Una vez que esto sea exitoso desconecta el teléfono de la interfaz y presiona las teclas RCL # 71 y te aparece el numero telefónico ahí meterás el nuevo numero telefónico el cual lo ingresaras de la siguiente manera 52 y el numero telefónico ejemplo **525551223868** donde **52** es igual a lada del país **555** lada de México y **1223868** numero telefónico, después de que lo ingreses presiona # y después RCL # 02 y el teléfono se apaga y se prende solo y entonces ya lo pruebas.

A continuación anoto los parámetros que en su momento cambiaras dependiendo del número que sea.

Datos TELCEL
Home area 24580
IPCH 0334 ó 334
Datos IUSACEL
Home area 24587
IPCH 0333 ó 333

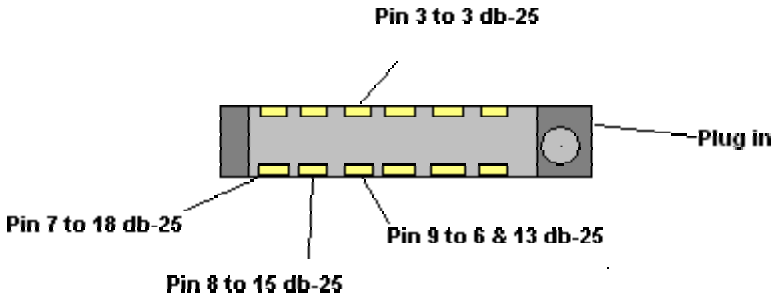


Figura 1.0 PinOut NEC 300

[Nota del editor] : Debido a que los archivos ocuparían demasiado espacio no fueron adjuntados al zip del eZine, pero podrán ser descargados de la página en la sección de telefonía celular.

Caja de Neón

Indicador visual de Repique

por o0ShellGhost0o

Introducción:

Todos hemos visto alguna vez en las películas como el típico nerd/hacker tiene en su casa un indicador visual de repique del teléfono. En muchas de ellas el indicador es un anuncio luminoso de neón con la imagen de un teléfono, en otras cuantas es un foco color rojo el cual prende y apaga con forme el timbre del teléfono suena.

Hoy he decidido hacer el diseño de un circuito que cumpla con ese propósito; la idea en mente, como siempre, es hacer un circuito muy sencillo y que requiera el mínimo de componentes y de espacio posible.

Materiales:

- Transistor 2N2222
- R1 (ver texto)
- R2 470 ohms
- LED Azul o Rojo
- Batería de 12 o 9 Volts

Diseño:

El objetivo de este circuito es prender y apagar un indicador luminoso para avisarnos que se nos está llamando, para sustituir o usar en conjunto con el timbre del teléfono.

He decidido emplear un transistor 2N2222, que es del tipo NPN de uso general por ser un componente de mucho uso y que se puede obtener en casi cualquier tienda de electrónica.

La teoría de operación es muy sencilla, el teléfono se encuentra en estado normal a un voltaje de 48V CD, cuando entra una llamada, la centralita quita esta señal y manda una corriente alterna de alrededor de 90V CA, esta señal es recibida por el teléfono y este activa una chicharra o timbre que es el que nosotros escuchamos y que nos hace saber que alguien nos esta llamando.

El circuito en si va a emplear el voltaje que es mandado a este timbre para, por medio de Q1 (transistor 2n2222) conmutar los estados del LED.

Habrán visto en la lista de materiales que a R1 no le hemos asignado un valor, esto es debido a que en diferentes teléfonos puede cambiar el voltaje que es mandado al timbre, he visto modelos que bajan el voltaje hasta valores cercanos a 9V CD y que emplean un buzzer en lugar de timbre.

Para calcular el valor de R1 ustedes tendrán que abrir el teléfono al cual le quieren agregar el indicador y medir el voltaje que emplea y usando la tan conocida ley de ohm calcular la resistencia que se usará.

Para todos aquellos que les de mucha flojera hacer esto prueben conectando una resistencia de 10K en serie con una de 4k7 de ½ Watt de potencia, pero les advierto que aun y cuando he tenido buenos resultados con este valor para mi teléfono, puede o no funcionarles a ustedes, así que no sean huevones y hagan sus cálculos.

Teoría de Operación:

Al recibir un pulso en la base el transistor permite la conducción de emisor a colector, prendiendo así el LED. En cuanto se deja de enviar el pulso el transistor dejará de permitir el flujo de electrones apagando el LED como consecuencia.

En caso de querer prender algo más potente que un simple LED, como sería en el caso de querer prender un foco de corriente alterna, el diseño únicamente tendría que emplear un relevador (con su debido diodo de protección) el cual se conectaría entre VCC y el transistor (quitando el LED y su resistencia) y en los contactos N.O. o N.C. (normalmente abierto o normalmente cerrado) conectar en serie un foco y su fuente de alimentación.

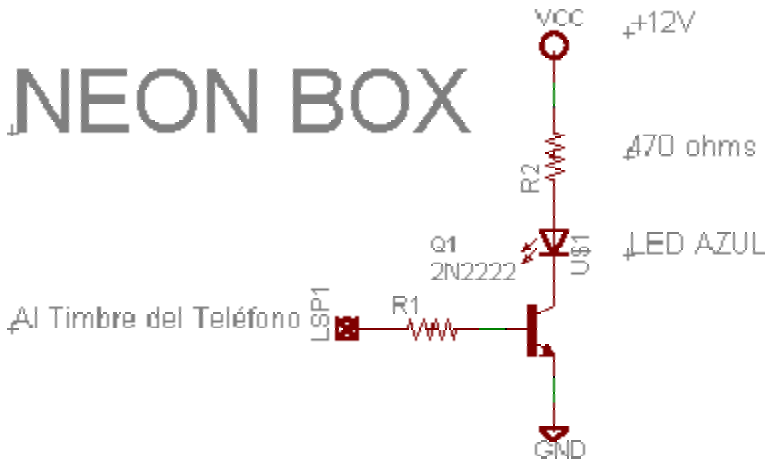


Figura 1.0 Esquema del Indicador Visual

Como conectarla:

La conexión es bastante simple, abre tu teléfono y encuentra los cables que van al timbre, desoldalos y conecta uno de ellos a la conexión marcada LSP1 en el diagrama y GND a la tierra de la Pila y al otro cable. En caso de querer usar tanto el timbre como el Indicador se pueden conectar en serie.

Comix

- Phreak & Freak -

¡Ya Basta!

Estudio Venezolano de Telefonía Celular

Por @gente*OoChip

Ya basta, hoy lo haré, escribiré el primer articulo de calidad, made in Venezuela, sobre phreaking *(si hay alguno escríbame y me retractare, pero como no he encontrado ¡uno solo! Pondré manos a la obra).*

Que me impulsa a escribir este articulo; Pues no encuentro algo de calidad ni mucho menos .ve, ósea venezolanito; en mis inicios *(haa, aquellos tiempos- pero que escribo si fue hace poquísimo mas de un año)* me jodi de lo lindo para encontrar algo de información útil entre la ingente cantidad de basura que existe en la red, y una vez mas, como no encontré nada venezolano, pos, *(se habrán dado cuenta que estoy orgulloso de mi país,- hablando de política-¿que te gusta mas?¡viva Chávez! o ¡muera Chávez!)*.

Adema ayer encontré el primer articulo *(en la Internet- bendita seas red de redes)* sobre los hackers y phreakers venezolano (fue en el nacional.com y estaba muy corto) que me llego al corazón, *(parecerá mentira pero la sensación fue comparable con la del orgasmo, saber que en mi país hay mas gente como yo, y como mis pocos "camaradas", gente que esta sedienta y cansada de que le den "papilla de bebe" cuando lo que quieren es un "jugoso trozo de carne" si es posible una vaca entera, pues bien para ustedes aquí tienen un pedacito de carne).*

En primer lugar, la respectiva aclaratoria;

La información es libre, y la constitución de la Republica Bolivariana de Venezuela, reza; que hay libertad de expresión, y nosotros los "adolescentes" tenemos derecho a la información oportuna (*yo me considero muy maduro, incluso mayor psicológica e intelectualmente que muchos del doble de mi edad; nota: tengo mucho menos de 20)*

Yo, no me hago responsable del uso que le des a esta información pues no incito a nadie a delinquir *(el poner en practica esta información es delito pero el divulgarla y el tenerla, estudiarla e investigarla no lo es).*

El que sigas leyendo implica que conoces lo anterior y que lo aceptas.

Si trabajas en la ChANTV o tienes algún vinculo con esta o con cualquier otra empresa de telecomunicaciones; no puedes leer este articulo, te esta terminantemente prohibido, si aun así quieres seguir bajo tu propio riesgo presiona ALT-F4-INTRO para continuar y para tener una mejor visualización.

Y para terminar, esta es la versión beta 0.1, así que puede tener muchos errores, si encuentras alguno escríbeme y los corregiré ¿o.k?

Bueno basta ya, entremos en materia.

Con este documento (*estoy trabajando en otros mas avanzados- primero lo básico)* aprenderás como funcionan las comunicaciones celulares en Venezuela *(y en todo el mundo – son estándares mundiales)*

Luego de eso aprenderás como emular un terminar móvil de la celula *(clonar **B)**)* y tal vez luego si me lo agradecen mucho, escriba y publique otros articulo*(uno muy fascinante seria como "hacer la tarjeta de teléfono publico con crédito ilimitado para Venezuela" o como engañar a la centralita de un "Centro de Comunicaciones ChANTV" para que no te tarifique -esto es llamar gratis desde un centro de comunicaciones)*

NOCIONES GENERALES, DEL FUNCIONAMIENTO ESTÁNDAR, DE LA TELEFONIA CELULAR.

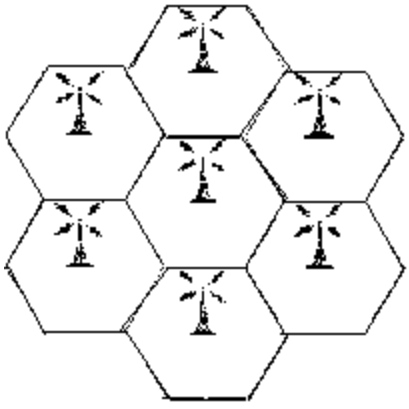
Uff, por donde empiezo.

Bien, la telefonía celular como todos sabemos en inalámbrica, pues usa ondas de radio de corto-medio alcance, estas ondas de radio se encuentran en la banda de radiofrecuencias de los 800-900 Mhz.

Las señales de radio se miden en Mhz. El corazón de este sistema es un aparato llamado MTSO *(o DMS-MTX, en nombre depende del fabricante)*, se encarga de conectar la telefonía alambrada con las torres de la celula y estas ultimas entres sí. Además de registrar las llamadas y los móviles que están activos en la celula. Entre otras cosa, pues tienen muchas mas funciones.

Tu celular al igual que tu Tv., usa canales *(estas son frecuencias predeterminadas)* para comunicarse con la MTSO, pero necesita dos frecuencias, pues a diferencia de la Tv., que solo recibe radiofrecuencias(Rx) el celular también debe transmitir(Tx) , si no por donde pensabas que se iba tu voz y como hacia el celular para registrase ante el MTSO. Estas dos frecuencias Tx y RX están separadas por 45 Mhz, osea que si mi celular esta usando el canal 1 *(hay 1000 canales)* y mi frecuencia de Rx *(recepción o lo que te sale por el auricular del celular y lo que te envía el MTSO)* es de 870.03 Mhz entonces mi frecuencia de Transmisión o Tx seria de 825.03 Mhz *(825.03 que es la frecuencia del móvil mas 45 Mhz de separación son igual a 870.03 Mhz que seria la frecuencia de la torre)*; entonces técnicamente hablando el canal se compone de dos frecuencias la frecuencia de transmisión del celular a la torre es llamada Reverse y la frecuencia de recepción o de la torre al celular se llama Forward

Imaginen un polígono de seis lados, mejor se los dibujo:



Este es un "cluster" de siete celular, cada celula tiene en su centro *(no es una mata de coco ok)* la torre o antena de la celula. Hay clusteres *(o racimos de celulas)* de 7, 9, 12 etc, etc pero la estándar es de 7, pero eso depende de las exigencias de cada ciudad.

Esa torre esta conectada a el MSTO (*regularmente la torres tienen en su base un cuartito, en el cuartito esta o bien el MTSO o bien un cable especial que va al MTSO- a propósito el cable es un "enlace T1" y es el mismo que se usa para comunicar dos MTSO entre si, ya sea de la misma operadora (compañía celular-ya sabes telcel/telcel , movilnet/movilnet) o de diferentes operadoras (telcel/movilnet)y un MTSO y una centralita de ChANTV).*

Pero que mas, bien, como ya escribí esa torre funciona entre los 800 y los 900 Mhz *(aunque también esta la segunda banda para GSM que esta en los 1800-1900 Mhz).*

Pero si solo son 100 Mhz como hacen para darle servicio a tanta gente. Como ya te dije los celulares son de corto alcance máximo unos 50 Km. En áreas rurales y 10 Km. en áreas urbanas desde la torre *(y esos 50Km. seria con mucha interferencia usando un amplificador de señal y aun así la comunicación seria muy mala).* Esos 100 Mhz estas divididos en dos bandas Banda A y B *(recuerdas cuando CONATEL estaba asignando unas bandas A y B para telefonía celular, pues son las mismas*) la banda "A" esta entre los 800 a 850 Mhz y la "B" *¡si!* entre los 850 y los 900 Mhz.

Cada banda *(a y b)* tiene entonces 50 Mhz . De esos 50 Mhz, se dividen en dos llamémosle sub. Bandas, una de 40 Mhz y otra de 10 Mhz.

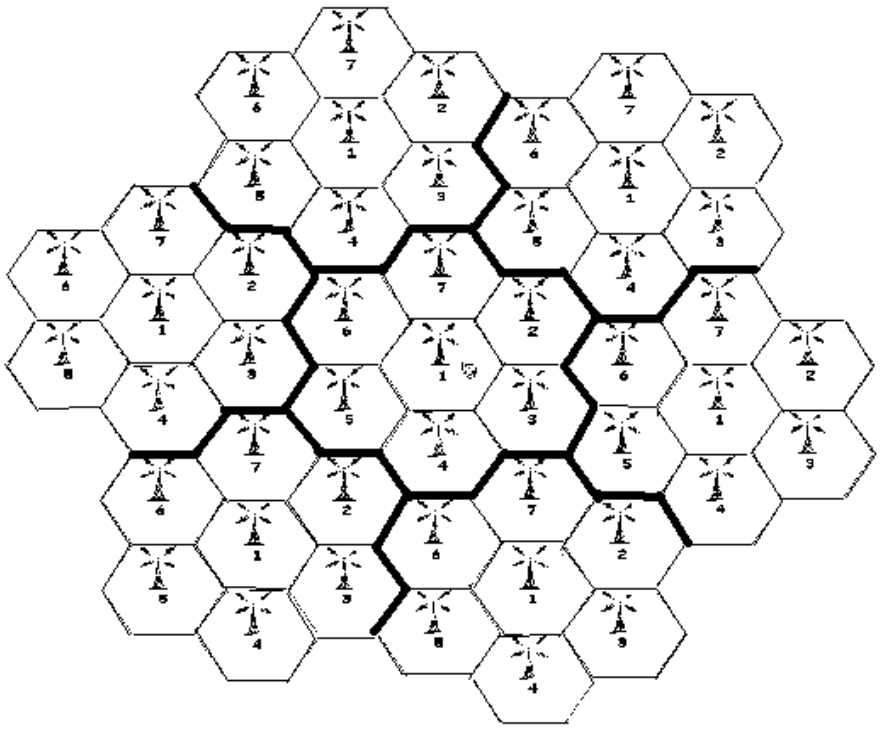
Los 40 Mhz de cada sudbanda son para los canales de voz y se conocen como sudbanda de espectro no expandido y los 10 Mhz como espectro expandido y son para los canales de control, por donde el móvil y el MTSO se comunican, intercambian datos, ordenes, etc.

Cada frecuencia sin importar sea Forward o Reverse del canal esta separada por 0.03 Mhz, que es bastante separación dada la precisión de los transreceptores de los celulares.

Entonces las primeras frecuencias serian (teóricamente) 800.00; 800.03; 800.06... pertenecientes a la banda "A" y las ultimas de dicha banda "A" serian 849.97; 850.00; ok.

Entonces tenemos unos 1000 canales compuestos por 2000 frecuencias, dos frecuencias para cada canal, (si eres observador y estudias la pagina anterio, esta y la siguiente, descubrirás algo, me escribirás, me lo contaras y serás un buen "camarada") .

Entonces, se dividen esos 1000 canales entre dos bandas; serian 500 canales por banda, esos 500 canales se dividen entre el numero de celulas que tiene un racimo, *(7 es el estándar)* serian, según el estándar, unos 71 canales por celula mas cuatro que serian dados a la celula que los necesite, eso implica algo llamado reutilización de frecuencias, volvamos al dibujito.



La celula uno usa el grupo de canales uno, la celula dos usa el grupo de canales dos y así hasta siete.

Entonces si hay que usar mas celulas rehúsan las frecuencias, pues como el celular es una transmisor de bajo alcance, la señal se atenúa o debilita con la distancia, y eso hace posible el reutilización de las frecuencias, a cierta distancia, y esa cierta distancia es menor que el tamaño de una celula, y en el diseño anterior se puede apreciar que entre las celulas numero 1, por ejemplo hay una distancia mayor que una celula. Al final si se agrupan las celulas en racimos, esos racimos se pueden agrupar hasta el infinito.

Pero que es lo que transmiten tanto celular como torre, pues señales estándares que comprenden todos los celulares sin importar en que plataforma trabajen*(hay las antiguas plataformas o tecnologías G1 o primera generación –analógicas- AMPS y Etacs- los G2 o segunda generación como TDMA -la usa movilnet actualmente- y CDMA-telcel- y GSM-digitel, digicel e infonet; pero eso ya es otro cuento, cuento que conseguí con sudor y sangre, tuve que tomarlo prestado a algunas compañías , en horario de reposo de su personal, si me entiendes),* si quieres saber mas detalladamente como funciona la telefonía celular tengo un librote *(muy técnico)* o si quieres el resumen hecho por mi y adaptado a Venezuela por los mejores de la @gencia, ,y en un lenguaje mas coloquial *(osea un lenguaje mas simple) (incluye el nuevo sistema GPRS de digiter)* , escríbeme).

Que pasa cuando tu prendes tu celular, pues el Tel. empieza por indicarle *(mediante señales)* al MTSO a través de la torre de la celula, que esta disponible y listo para hacer y recibir llamadas*(entre otras cosa **;))***
Este proceso se llama registro, si quieres hacer una llamada el teléfono se re-registra al MTOS y le dice que quiere hacer una llamada el MTSO le pregunta algunas cosa y el numero; procesa el numero y le dice al teléfono que la llamada esta en proceso *(solo después de cumplir con unos requisitos).*

¿Pero que requisitos son esos?; cuando prendes tu celular , para este registrase, busca el aire *(en canales predeterminados)* el SID *(mas adelante sabrás que es el SID)* de tu operador, una vez encontrado dicho SID, le envía al MTSO que tenga ese SID a través de la frecuencia "reverse" *(celular a torre)(desde ahora lo llamaremos reverse link)* sus datos ,que los más esenciales son ESN, SID y NAM *(mas adelante sabrás que son),* el MTSO compara esos datos con los de su base de datos *(la base de datos donde la operadora te inscribe cuando le pones línea a tu celular)* si todos los datos concuerdan tendrás acceso a llamar y podrás recibir llamadas. *(Si no tu celular te dirá que hay servicio pero no recibirás jamás y si intentas llamar recibirás un típico mensaje en la que las operadoras te ofrecen sus servicios o te dicen que tu serial electrónico (ESN) esta malo o x*).

Cuando te llaman, el MTSO de la celula empieza a buscar tu móvil, esto se llama voceo y, luego que encuentra tu móvil le dice que se sintonice a un canal x (*ese canal x lo escoge él, dependiendo de en cual canal, de los que están disponibles, tu señal es mas fuerte)* , una vez tu te sintonizas a ese canal. Si respondes entonces hablas (*al que te llama se le envía el tono de que respondiste para que comience la acción especifica-tarificacion entre otras*), si no respondes, contestadora o mensaje.

Cuando tu llamas *(presta atención que esto es vital para la emulación)* tu móvil se re-registra (*recuerda que ya se registro cuando lo encendiste para decirle al MTSO que estaba disponible)* reenviando por el reverse link su SID, ESN y NAM, si el MTSO al compararlos los valida; procesa tu llamada, una vez que verifica la ruta o numero al que marcar, le indica a tu móvil el canal asignado para la comunicación (*esto lo hace por el forward o frecuencia de la torre al móvil, de ahora en adelante será forward link)* el móvil se sintoniza y a hablar .(*cuando te responden te es enviado el tono de tarificacion, y gasto pa' rriba).*

Ahora que pasa si durante una llamada te mueves de una celula a otra *(hay celulas tan pequeñas como 3 Km.- que si así de pequeñas yo las he visto en Maturín, San Félix, Pto. Ordaz y Caracas, seguro que hay en otras ciudades grandes pero no he viajado tanto)* pues sucede el milagro del hand-off; el MTSO permanentemente esta vigilando tu móvil, midiendo desde su torre la intensidad de tu señal *(mejor dicho la de tu móvil)* y pidiendo a los MTSO vecinos que hagan lo mismo, esto se llama SAT, si en algún momento la señal de tu móvil es mas fuerte en otro MTSO tu actual MTSO le ordena a tú móvil que use como MTSO el que tiene una mejor señal de tu móvil, esto ocurre en milésimas de segundos *(podríamos decir que el MTSO lo hace unas*

30 veces cada minuto y con cada móvil- esto no necesitaría mas de 56 Kbps en velocidad de conexión entre MTSO's pero se usan 1 y 10 Mbps) si en un momento dado de tu conversación tu señal es mas fuerte en otro MTSO (*en otra celula, torre, etc)* entonces ocurre este cambio de MTSO que se llama hand-off y tu ni lo notas, *(una vez mas te digo esto es un resumen, lo mas básico, si quieres saber mas –que te servirá para cosas mucho muy avanzadas- te servirá es mi resumen. Escríbeme).*

Tengo que decirte que cuando el MTSO hace un SAT (mide la intensidad de la señal de tu móvil) tu móvil entre otras señales envía el NAM y el ESN, por lo que estos datos estas siempre en el aire

Como nota curiosa y para cerrar este capitulo; imagina que estas en un sitio cualquiera de una celula y que durante el SAT tu MTOS mide tu señal *(cosa que como sabes hace muy frecuentemente)* y pide a los MTOS vecinos que hagan lo mismo, pues imagina que tres MTOS miden tu señal, pues con esos tres resultado y aplicando una intrincada formula matemática *(o usando un programita muy bueno escrito by me)* puedes calcular la distancia a la que esta el móvil de cada antena y sabiendo la localización geográfica de al menos dos de las tres antenas puedes calcular con un margen de error de unos 15 metros donde esta ese móvil, y por ende la persona que lo usa.

También, como el móvil esta siempre transmitiendo a la torre señales, se puede enviar a un móvil un programita *(tienes que estar a menos de 50 Mts del móvil victima y con un equipo especial, en el momento de bajarle el programa- pero puedes estar en cualquier parte de la celula para escuchar)* y ponerlo en modo micrófono de ambiente, al ordenarle al móvil *(como si fueras su MTOS)* que sintonice un canal *(de otra celula para evitar interferencia)* y transmita por el audio, esto conservando su pantalla como si estuviera en espera y así podrías escuchar todo lo que pasa alrededor de ese móvil *(he hecho pruebas y en máxima sensibilidad del micrófono un nokia 5120 con full señal tiene un alcance de unos 3 metros como micrófono de ambiente).*

Claro que para estos dos súper trucos necesitas ser un experto, tener una laptop potente*(a menos que vayas a cargar tu PC acuestas)*, y algunos jugeticos electrónicos que solos cuestan unos 7000 dolaritos americanos*(amenos que te los construyas tu mismo o compres uno tipo "caseros").*

@gente*OoChip

En el próximo número: Emulación de terminales móviles de una red de telefonía celular.

·3N$AMBLADOR KON MANZANA$

2º parte

por (.oPKo.)

Continuamos con el ensamblador...

..::[Algunos saltos condicionales]::..

Sin Signo	Con signo	
JE	JE	Salta si es igual
JZ	JZ	Salta si es cero
JNE	JNE	Salta sino es igual
JNZ	JNZ	Salta sino es cero
JA	JG	Salta si es mayor
JNBE	JNLE	Salta sino es menor o igual
JAE	JGE	Salta si es mayor o igual
JNB	JNL	Salta sino es menor
JB	JL	Salta si es menor
JNAE	JNGE	Salta sino es mayor o igual
JBE	JLE	Salta si es menor o igual
JNA	JNG	Salta si no es mayor

..::[Algunos saltos especiales]::..
(revisan especialmente una bandera)

JS	Salta si el signo es negativo
JNS	Salta si el signo es positivo
JC	Salta si hay acarreo
JNC	Salta sino hay acarreo
JO	Salta si hay desbordamiento
JNO	Salta sino hay desbordamiento

..::[Rotacion]::..

ROR
```
    {reg/mem},{posicion a rolar}
```

ROL
```
    {reg/mem},{posicion a rolar}
```

Digamos que Bl es 157

```
ROR BL,1       BL 10011101
                        ^
               BL 11001110
```

BL se convirtio en 206

..::[Operaciones]::..

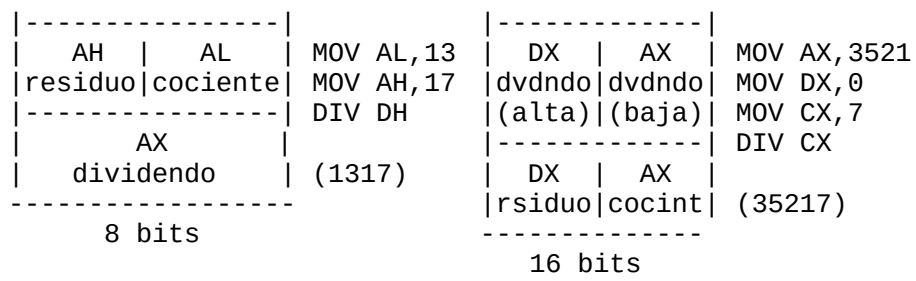
+ MULTIPLICACIÓN +

MUL {reg/mem}

```
|-----------|                |------------|
| DH |  AL  |   MOV AL,13    |  DX |  AX  |   MOV DX,1382
|    |multip|   MOV DH,17    |     |multip|   MOV AX,2
|-----------|   MUL DH       |------------|   MUL DX
|    AX     |                |  DX |  AX  |
|  producto |   (13x17)      |prod.|produc|   (1382x2)
-------------                |alta | baja |
   8 bits                    --------------  *El resultado de 32 bits
                                 16 bits       se guarda en DX y AX
```

+ DIVISION +

DIV {reg/mem}



..::[Pilas]::..
(recursividad)

Las pilas virtuales funcionan llamando un proceso desde el programa regresando al la funcionando un poco como un programa interno que ejecuta un proceso y linea siguiente del codigo de donde la llamamos sus funciones son

CALL	Llama una función o proceso (su uso no es exclusivo de pilas)
PUSH	Sirve para meter a la pila una variable
POP	Sirve para sacar de la pila la variable que metimos
RET	Te regresa a la línea posterior de donde llamaste el proceso de pila virtual

```
                                PAGE 60,132
                                TITLE FACTORIAL (RECURSIVO)
                                .MODEL SMALL
                                .STACK 1024
                                .DATA
                                NUM DW 3
                                FAC DW 0
                                .CODE
                                MAIN PROC FAR
                                MOV AX,@DATA
                                MOV DS,AX
                                PUSH NUM
                                PUSH FAC
aquí llamamos a nuestro  ->     CALL FACTOR
proceso de pila virtual         POP FAC
                                POP NUM
                                MOV AX,400CH
                                INT 21H
aquí termina el MAIN    ->      MAIN ENDP
empieza nuestro proceso ->      FACTOR PROC NEAR
de pila virtual apilando        PUSH AX
AX, DX, CX y BP con la          PUSH DX
función PUSH para               PUSH CX
modificar los valores que       PUSH BP
les asignamos                   MOV BP,SP
                                ADD BP,12
                                MOV AX,[BP]
                                CMP AX,1
                                JA RECUR
                                MOV AX,1
                                JMP FIN
este ciclo mete y saca  ->      RECUR:  MOV DX,AX
a DX y CX de la pila            DEC DX
para poder calcular un          PUSH DX
factorial                       PUSH CX
                                CALL FACTOR
                                POP CX
                                POP DX
                                MUL CX
                                FIN:  SUB BP,2
                                MOV [BP],AX
aqui salimos de la pila ->      POP BP
sacando las variables en        POP DX
el orden inverso que las        POP CX
metimos (desapilamos)           POP AX
este RET nos regresa a   ->     RET
la linea siguiente del          FACTOR ENDP
CALL                            END MAIN
```

Aqui terminamos con la 2 parte del cursillo, espero le entiendan, sino comentarios, dudas, preguntas e insultos a yoyosoy7256@yahoo.com yo yo soy oPko...

```
:
: :.:..:...:....:.....:......:.......:........:..........: : :
::::
:, ,....                      no hay que subir el monte
':._(.oPKo.)_.:''._.' para saber si este es alto...
```

Nuevas Tecnologías

Monederos Electrónicos en México

por -=oSUKARu=-

En esta sección que estoy comenzando en éste número voy a dar a conocer algunos aspectos tecnológicos de las nuevas tecnologías empleadas en México, en esta ocasión hablaré de las smartcards empleadas para control de dinero de forma “más segura”.

MONEDEROS ELECTRÓNICOS:

De momento hay dos grandes empresas que están dando a conocer esta tecnología en México, Banamex y la unión formada por Inbursa-Telmex.

La idea del monedero electrónico es remplazar en un futuro las tarjetas magnéticas bancarias debido a que estas tienen muy poca capacidad de almacenamiento y su seguridad deja mucho que desear.

El monedero electrónico consiste en emplear una tarjeta inteligente (smart card) con la capacidad de almacenar saldo, nombre de usuario, número de cuenta y prácticamente cualquier tipo de información que se requiera.

Banamex inició con un despegue algo tímido a mediados del año pasado, su tarjeta tiene la finalidad principal de guardar todas las claves y nombres de usuario de los sitios en Internet que visite una persona y en un futuro comenzar a utilizar la tecnología con el uso que se le da en Europa y Asia, es decir remplazando a las tarjetas de banda magnética en el manejo de dinero.

Telmex apoyado por Inbursa, por otro lado, tiene una estrategia más sólida bajo el amparo del conglomerado de empresas del magnate Carlos Slim. Cuenta con el respaldo de empresas como las tiendas Sanborns y Sears, y la red de panaderías El Globo del Grupo Carso.

Se planea que cada tarjeta tenga un saldo máximo de $1000 pesos y se manejaran tres status diferentes de acuerdo con la facturación de cada cliente: Platina, que contendrá un mínimo de 500 pesos mensuales, Oro, que incluirá 300 pesos y Azul con cien pesos de depósito mínimo.

La tarjeta permitirá hacer llamadas de larga distancia, pagar cuentas, realizar pagos en restaurantes, gasolineras y centros comerciales, además de obtener descuentos en tiendas y acumular puntos para conseguir beneficios con la compañía.

La tecnología detrás del monedero electrónico empleado por Telmex fue desarrollada por la compañía Proton World, creada en 1998 por la union de grandes transnacionales como: American Express, Banksys, ERG, Interpay Nederland y Visa International.

Proton World esta reconocida como la empresa líder mundial en seguridad tecnológica por medio del uso de tarjetas inteligentes gracias a que cuenta con el apoyo de uno de los principales Criptógrafos que fue punto clave en el diseño del algoritmo Rijnda el cual es empleado por el gobierno de los Estados Unidos de Norteamérica.

De entre una lista bastante amplia de empresas maquiladoras de esta tarjeta se destacan las compañías Anritsu, Ascom Monetel, Gemplus, Oberthur y Shlumberger, marcas conocidas por todos los que nos dedicamos a la investigación de tarjetas telefónicas. Con estas grandes compañías respaldando a la empresa Proton World no es raro que Telmex esté apostando en está tecnología.

¿Qué uso tendrá está tecnología?

Monedero electrónico: Es el uso que tiene pensado darle en estos momentos Telmex, es decir a manera de tarjeta bancaria con la cual se podrá pagar en tiendas, se podrá usar para realizar llamadas y para hacer consultas de saldo bancario, etc.

Control de Identidad: Se le podrá dar el uso de tarjeta de identificación personal debido a la capacidad que tiene de guardar información. Esto podría llegar a ser usado en tiendas para dar bonificaciones a clientes distinguidos, pero con su potencial podría llegar a ser usada como tarjeta de acceso en empresas (quizás hasta áreas restringidas dentro de Telmex).

Acceso a cuentas de banco de forma remota: Por medio de una computadora y un lector de smartcards se podría llegar a tener acceso más "seguro" a las cuentas de banco por medio de internet. Está característica me deja pensando en una cosa... si a través del tiempo se ha visto que la seguridad por hardware (como en el caso de los programas que usan "sentinelas") puede ser emulada o crackeada por medio de software y que por lo general la simple aplicación de un patch romperá toda la supuesta seguridad del dispositivo, ¿por qué las empresas siguen pensando que es una buena idea realizar este tipo de transacciones?

Algo que a muchos de ustedes debe de haberles llamado la atención es la característica de poder RECARGAR la tarjeta para poder usarla como telecard en cualquier caseta de tarjetas.

Ya veo a muchos de ustedes pensando en armarse un logger de datos para poder ver exactamente que secuencia le manda la caseta a la tarjeta para recargarla, pero por desgracia parece ser que no será tan fácil como creemos.

Guardar el saldo de la telecard dentro del mismo monedero electrónico significaría una terrible falla en la seguridad de la tarjeta, y dudo que a los ingenieros encargados de desarrollar el sistema se les haya pasado revisarla. ¿Y entonces como se almacenará el saldo?

La idea que me viene a la mente es: por medio de bases de datos dentro de las centralitas. Esa sería la forma más segura de guardar el saldo y funcionaría de la siguiente manera:

1- Metemos la tarjeta a la caseta, la caseta la valida y lee el numero de identificación de dicha tarjeta.
2- Si el saldo se agotó la caseta dará la opción de recarga.
3- En ese momento el usuario oprime la tecla correspondiente y a continuación su NIP bancario.
4- Se descuenta el monto deseado de la cuenta del usuario.
5- El saldo es guardado dentro de una base de datos la cual es revisada en cada validación para saber si la persona dispone de saldo.

Esa es la forma en que **yo** realizaría el algoritmo de recarga. En caso de que no sea así y el saldo sea guardado en la misma tarjeta telmex enfrentará una gran crisis económica causada por esta vulnerabilidad, pero las probabilidades de que eso suceda son mínimas.

Notas Finales:

Me hubiera gustado haber tenido acceso físico a cualquiera de los dos tipos de monederos electrónicos para realizar una investigación más detallada de su funcionamiento. Sin embargo espero que les sirva a manera de introducción a todos los que estén interesados en este tema.

Me gustaría saber que tanto interés hay sobre este tema para realizar un grupo de estudio de monederos electrónicos dentro de los foros de Tecnología Mexicana, así que si te gustaría participar plasma tu inquietud en el foro general.

-=oSUKARu=-
mhmphreak.com

KOMO HAM GRATI$ DE$DE LA UNITEC c. CUITLAHUAC

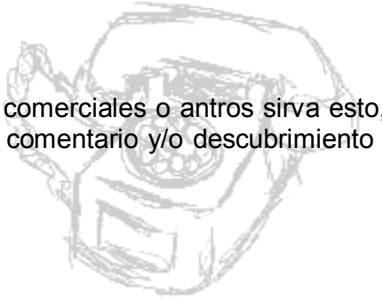
por (.oPKo.)

```
..::[Erase una vez]::..
```

Estaba con unas amigas en los teléfonos de tarjeta de la y estaba esperando a que una de ellas terminara de llamar a su mama mientras esperaba me percate de la existencia de un 'plug' que estaba del lado derecho del teléfono y no hice bulla en el momento pero pensé mañana me cargo un teléfono y lo pruebo.

Al día siguiente llegue con mi tel y lo conecte, y oh sorpresa!! me dio línea d inmediato llame un # al azar y me contestaron, entonces ya venia preparado con números de LD (larga distancia) y (ab)use un buen rato del descubrimiento.

Busque todos los teléfonos del campus y en los que esta abierto el 'plog' es en el del edificio B a un lado de la maquina de papas y gansitos, el teléfono derecho de las escaleras que conectan el edificio A con el C y el de la biblioteca (a veces). Estas líneas sirven hasta para llamadas internacionales y no se cortan, solo que a veces se abre un canal (como si descolgaran en otra extensión) nunca he tenido problema con eso, pero he preferido colgar cuando eso pasa...



No se si en todas las escuelas o tal vez hasta en algunas plazas o centros comerciales o antros sirva esto, la vdd no lo he comprobado, saludos y ojala les sirva y porfavorrrrr cualquier comentario y/o descubrimiento les será bien agradecido.

Les redigo mi 'meil'
yoyosoy7256@yahoo.com

```
: yo yo soy oPko 'bai'...
: :.:..:...:...:....:.....:.....:.....:.....:.....: : :
::::
:, ,....   mmmmm... no tengo frase para esta pero... recuerda que en
':._(.oPKo.)_.:''._.' la vida quedan muchas cosas por hacer
```

Hey tíos, espero que le sea de utilidad este resumen de un estudio que estoy desarrollando sobre los teléfonos públicos venezolanos para @gencia*OoChip , es algo corto pues lo resumí considerando que MHM tendría otros artículos que poner en este ezine (aprovecho la oportunidad para felicitarlos y alentarlos a que sigan desarrollando ideas sobre Prehacking y electrónica y a que compartan la información, pues considero que este es el pilar fundamentar para que personas interesadas en estos tópicos, y que vivimos en el llamado tercer mundo puedan evolucionar en su nivel) para no hacerlo mas largo entremos en materia.

*@gente*OoChip*

Phreaking
Telefonía Pública

Estudio sobre el Teléfono Modular Modelo E02

Disclaimer

@gencia*OoChip, el autor, ni ninguno de sus miembros se hace responsable ni solidario con el uso que le de el usuario a esta información, quedando bajo la absoluta y total responsabilidad del mismo cualquier uso inadecuado; esta información solo se proporciona con fines educativos; creemos por convicción en la libertad de expresiones, en una Internet sin censura y en el derecho a la información.

Introducción

Este Teléfono Modular (TM) esta protegido por una coraza externa de aleación de magnesio y acero inoxidable de 8 mm de espesor, construido de manera robusta para evitar las acciones vandálicas.

En este estudio nos centraremos más bien en la parte electrónica y la cerradura, lo explicare del modo más simple y atécnico posible para que todos (o al menos la mayoría) lo entiendan.

La parte electrónica, como su nombre lo indica esta construida de manera modular, de forma que si una pieza necesita ser cambiada, se pueda hacer en un mínimo de tiempo; el desarmado y rearme total del teléfono se puede hacer en aproximadamente 7 minutos.

En primer lugar esta el "Pci Conexión de Línea Tpas" que es donde se conecta la línea, el zumbador (rínger) y el microteléfono.

El microteléfono no tiene gran ciencia solo tres pares de cables; azules (seguridad) amarillos (auricular) y rojo (micrófono).

Los botones de recall y colgar son solo botones de ON OFF y un botón de dos entrada y una salida de estado, respectivamente.

Del "Pci Conexión Línea Tpas" sale un cable plano de 16 pelos que se conecta al corazón del TM (teléfono modular) llamado "Pci Principal ns Tpas" que seria como el mother boart del TM este; es la pieza que tendremos que tratar mas a fondo e incluso de ella se desprenden otros estudios (ejemplo: el programa de la EPROM para ver que se hace**;)**).

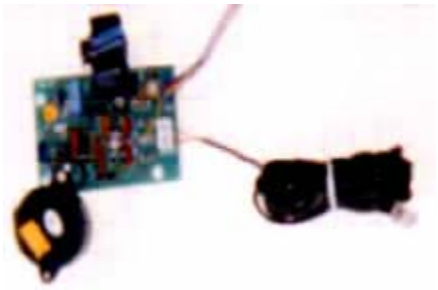
El "Pci Principal ns Tpas" tiene incrustado el "Pci Cont. Lect. Tarj. Cpld Tmi" o Pci Controlador Lector de Tarjetas; es el que se encarga de gestionar, para el PCI principal, los accesos al lector (bien sea para leer la tarjeta o para descontar crédito).

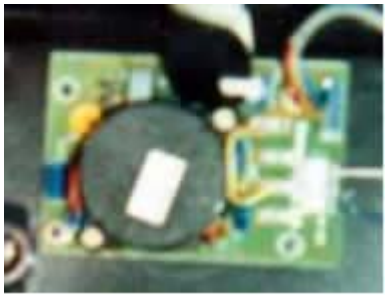
Luego esta en si el "Lector de Tarjetas" (¿para que servirá?)

Regresando otra vez al PCI principal esta la conexión para el teclado y el LCD que en este y otros modelos de TM son los mismos o al menos compatibles.

Están otras conexiones en el PCI principal que serán estudiadas mas adelante, que sirven para ampliación del TM como por ejemplo un "PCI de monitorización de línea TM"; para cuando la línea del TM sea pinchada, el TM lo sepa y envié un tono de interferencia haciendo imposible el uso de la caja marrón con dicha línea.

Capitulo I
PCI Conexión de Línea TPAS





En este modelo se usa un PBC de una sola cara, de 8.9 x 6 cm.

No es mas que una especie de protector de voltaje, así al PCI principal no llegan corrientes demasiado altas que lo podrían dañar, como un circuito independiente del TM, esta también en este Pci, el ringer que esta compuesto de un IC LS1240 conectado directamente a la línea, y a un ringer que al detectar la onda senoidal de timbre pós timbra.

Tiene un conector macho de 16 pines que va al PCI principal, estos 16 pines se distribuyen de la siguiente manera:

Nro. de pines	USO
2	Como salida hacia el PCI principal de la línea, ya filtrada de voltajes indeseados
1	Como línea de tierra para uso del PCI principal.
6	Que conectan directamente, sin intervención del PCI Conector de línea, el PCI Principal y el Microteléfono; de estos 6 pines , 2 son para el micrófono, 2 para la bocina y dos de seguridad.
2	No usados
5	Que conectan directamente, sin intervención del PCI Conector de línea, el PCI Principal a un conector de 5 pines que no se para que se usara; ademas en otros modelos mas antiguos de TM´s este conector no existe.

Capitulo II
El Microteléfono

De la cabina sale por su lado izquierdo un cable metálico semiflexible, de aproximadamente un metro, que en su interior contiene 6 cables, este cable metálico desemboca en la parte inferior del microteléfono, en el TM esta conectado al "PCI Conector de línea (en realidad hace escala en este porque como ya dije va directo al Pci principal).

De los 6 cables, 2 son rojos, 2 amarillos y 2 azules:

- Los rojos son para el micrófono.
- Los amarillos para el altavoz.
-.Los cables azules, mejor dicho, el cable azul no se conecta a ningún lado, puesto que es el mismo que va y vuelve, este cable es utilizado para detectar si el cordón metálico y el microteléfono siguen estando donde debería, ósea, bien agarradito al TM.

El método no puede ser más fácil, por el cable circular una carga a determinada frecuencia que cuando es interrumpida al cortar el cable es reportada la falla a la centralita que lo controla.

Capitulo III
El LCD , El Teclado y los Botones de Recall y Cuelgue

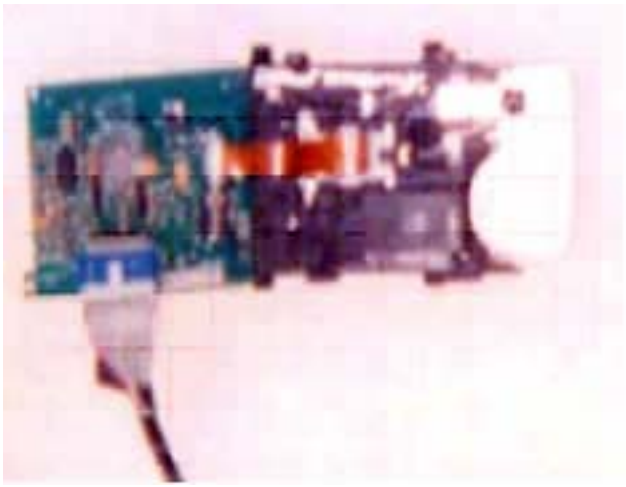
Todos estos componentes están conectados al Pci principal mediante un solo cable de 26 pelos (12 para el teclado y los botones R y C y 14 para el LCD) y vendrían a ser algo así como la interfaz de interacción entre el TM y el usuario; puesto que a través del teclado y los botones de R y C el usuario mete los datos y las ordenes al TM y a través del LCD el TM le indica al usuario los datos correspondientes.

El teclado se conecta al Pci principal mediante 12 pelo y esta protegido por una pieza de acero inoxidable que contiene los botones antidesgastes (con los caracteres formados por relieve) y la parte electrónica no es mas que un simple teclado matricial 4x5 pues toda la gestión de estado la hace el Pci principal; serian 20 posibles combinaciones, de las que solo se usan 16(17 si metemos al R), en el mismo PBC del teclado esta un conector de 5 pines al que se conectan los botones de R y C (R usa solo dos y es un simple botón de ON/OFF, los otros 3 son usado por un selector de dos entradas y una salida para el botón de C, y dependiendo de que entrada baya a la salida estará en ON o en OFF; es de destacar que este es el botón de encendido del TM y que en algunas variantes de este mismo modelo el botón de cuelgue externo en vez de ir conectado a el mismo conector que R va directo a un push button que esta en el PCI principal mediante un muelle.

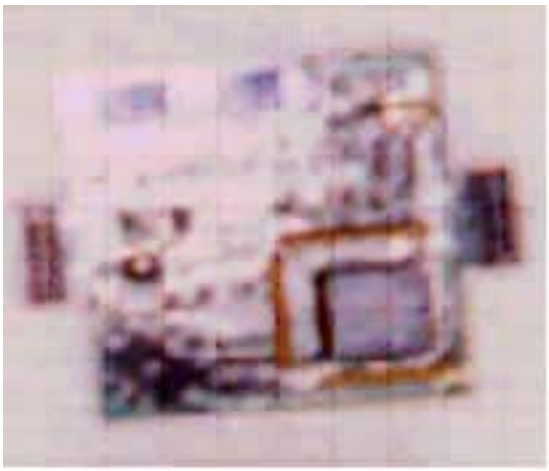
El LCD modelo 20265k (HT-12 compatible, basado en un controlador Hitachi HD44780) usa 14 pelos para conectarse al Pci principal(en vez de usar LCD´s retro iluminados); es un LCD de 2 líneas de 20 caracteres cada una. El LCD recibe ordenes (que caracteres poner en pantalla- porque el LCD tiene memoria RAM, un programa y un procesador independiente) del procesador principal que esta en el Pci Principal y del procesador principal del Pci controlador de tarjeta (de este ultimo cuando lo puede hacer).

Capitulo IV
PCI Controlador Lector de Tarjetas y el Lector de Tarjetas

El Lector de Tarjetas se conecta al Pci que lo controla a través de un cable plano de 20 pines y par de conectores en cada punta
El Lector de Tarjetas no es mas que un zócalo smart card conectado directamente al Pci controlador del lector de tarjetas que además de leer smart card (tarjetas de chip) también tiene un lector de tarjetas de banda magnética (para llamadas con cargo directo a tarjetas de debito o crédito y a tarjetas telefónicas prepagadas de banda magnética, aunque estas modalidades de cobro no esta implementadas en la actualidad) y además varios sistemas de seguridad y monitoreo (que si para saber cuando alimentar el lector dependiendo si hay o no tarjetas insertada, etc.) pero toda la información es gestionada por el Pci controlador.



El Pci controlador del Lector de tarjetas esta conectado al lector de tarjetas mediante un cable plano de 20 pines e incrustado en el Pci Principal mediante dos conectores de 14 pines (2 líneas de 7 pines).

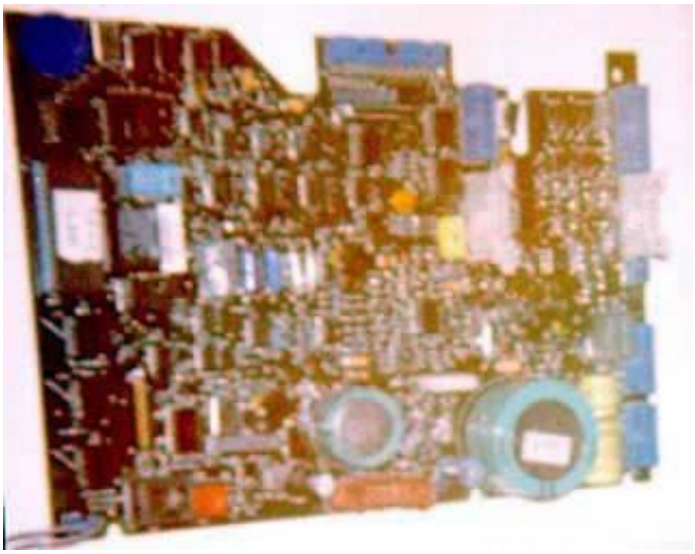


Se encarga de tramitar, para el Pci principal, el lector de tarjetas asumiendo las tareas de lectura, escritura y sistemas de seguridad del mismo; usa un CDP6823Q(este chip es muy usado en este y otro tipo de funciones de varios modelos diferentes del TM´s)

Hay una versión compatible (la mas avanzada que he visto) que usa un procesador (le pongo algo pa´ que averigüen) PZ5064|12BB1/BM93971 101 y dos memorias tipo 24LC256 para cuestiones de seguridad y que además tienen cinco zócalos smart card (del mismo tamaño que los zócalos de los móviles GSM) que según me he informado es para tener compatibilidad para cuando se implementen LAS TARGETAS DE TERCERA GENERACION.

Capitulo V
EL "Pci Principal"

Un PBC de 23x17cms, magníficamente diseñado que monta como procesador principal un 80c32 oscilando (por medio de un xtal) a 3.579545 Mhz (se usa este cristtar pa los tonos DTMF; este y el 80c31 son los únicos procesadores que he visto en TM´s) con una memoria eprom de acceso paralelo de 32 pines (2 hileras paralelas de 16 pines)del tipo 27C010A o 27C1001 (esta ultima es la que monta este modelo), una memoria RAM M48T59Y(con batería de litio dedicada) y como decodificador de direcciones un 74HC573, (se hace uso intensivo de este ultimo chip, en este modelo, para muchas tareas diferentes; desde monitorear el cable de seguridad del microteléfono hasta gestionar el teclado y el LCD y el controlador del lector de tarjetas).



Como sistema de respaldo de energía tiene dos condensadores electrolíticos, uno de 10 V y 0.47 F y otro de 5 V y 0.22 F, además de una batería de Ni-Cd de 8.4 V y 600 mAh, también tiene un conector para carga rápida; en este punto es importante aclarar que toda la energía la toma el TM de la tensión de la línea telefónica(son 48 Vlts en reposo), el único uso que se le da a la energía eléctrica C.A (120-240 V) es para las lámparas de la cabina pero esta no tiene nada que ver con el TM menos con el teléfono en si.

En el Pci principal también esta una resistencia variable de 10k que sirve para ajustar el contraste del LCD, un conector tipo RJ-45 (del mismo que se usa en los cables de redes) para bajada de data (que si para cambiar el software directamente) el botón T (un push button) y el censor de la puerta del TM; simplemente un push button, cuando esta pisado(por la puerta de la cabina) esta en OFF y si no en ON, al pasar al modo ON (al abril la puerta) el TM pide que saque tarjeta(si hay alguna metida) descuelgue y presione T para entrar al modo técnico de la cabina; pero esto lo trataremos en la sección del software.

Se me olvidada monta un MODEM CM3105 (el que me pregunte que es eso lo acribillo) a 1200/2400 Pbs.; de aquí sale un ¿DELIRIO?; como Uds. Saben algunos (ergunos k no todos) públicos aceptan llamadas entrantes (que reciben llamadas pues), con un análisis exhaustivo del ASM del TM´s y algunos conocimientos de programación (Visual Basic por ejemplo) y conociendo el método de Login que usa un TM (que lo sacas del ASM – como adelanto les digo que los TM´s ,aunque es posible y cuando menos los de aquí de Venezuela, no usan caller ID – esto de que no usan caller ID para aclarar que el TM no sabe que numero lo llama, que si la centralita) podes hacerte un programita que te permita "actualizar" el ASM del TM´s y este pensaría que el ASM lo actualiza la Chantv; esto serviría para por ejemplo poner la tarifa mas justa, en digamos 0.25 Bs. por impulso telefónico para cualquier destino.(nota; el Byte menos significativo del contador octal de una tarjeta telefónica venezolana representa 2 Bs., cada BIT 0.25, de allí esa tarifa)

Capitulo VI
La Cerradura

Todos los TM´s usan dos tipos de cerraduras ubicada en el lado contrario por donde sale el cable del microteléfono (al menos aquí en Venezuela):

1.) Cerradura de llave, tiene un cilindro de 5 pines, usa el mismo sistema que cualquier cerradura de casa pero según es una llave genérica que puede abrir cualquier cabina, aunque podría estar zonificada.

2.) Cerradura de combinación; este es el tipo de cerradura que usa este modelo, aunque podría también usar una de llave, pues el tamaño del agujero del TM donde va la cerradura así como el sistema de apertura es estándar.

Este tipo de cerradura como su nombre lo indica abre por combinación; externamente (fuera del TM) es un circulo de 3.9 cm. que dentro tiene otro mas pequeño de 2.5 cm. que puede girar a ambos lados.

Internamente el cilindro exterior pequeño tiene soldado un cilindro de unos 4.2 mm en su centro, que queda hacia el lado interno, y pasa por un agujero del circulo de 3.9 cm (circulo exterior grande); para mantenerlo allí se tiene una abrazadera a presión, del lado interno, que gira con el círculo pequeño, esta unión es cubierta por una tapa circular que cubre el circulo grande, esta tapa junto al circulo pequeño es lo que vemos externamente.

Entonces queda un espacio de 4 mm entre el cilindro del círculo pequeño y las paredes del círculo grande; hay es donde se meten las tres ruedas en su habitáculo, estas tres ruedas son aros de 2 mm y el agujero mide 5 mm (por lo que el ancho total serian 12 mm), mientras que el habitáculo, que separa las ruedas de combinación del cilindro soldado al circulo externo pequeño (el que gira) cubre en su base todo el espacio del circulo grande.

La figura 3 es una vista de la cerradura sin las ruedas de combinación, el habitáculo de las ruedas de combinación ni el muelle de estado desde la parte interna del TM.
El cilindro del circulo pequeño esta marcado como A verde.
El espacio como B y esta en azul.
La abrazadera a presión esta en rojo.
El circulo grande en amarillo
En gris la tapa circular externa
Donde esta la **W** esta impreso el modelo de la cerradura que seria **904481 STS 000**

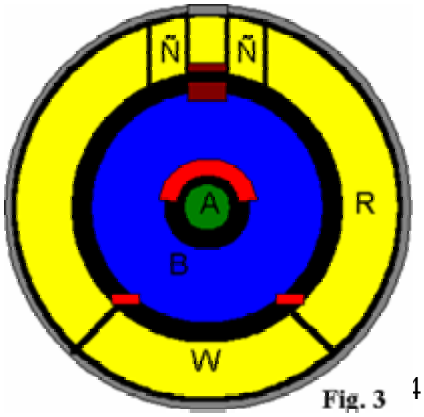


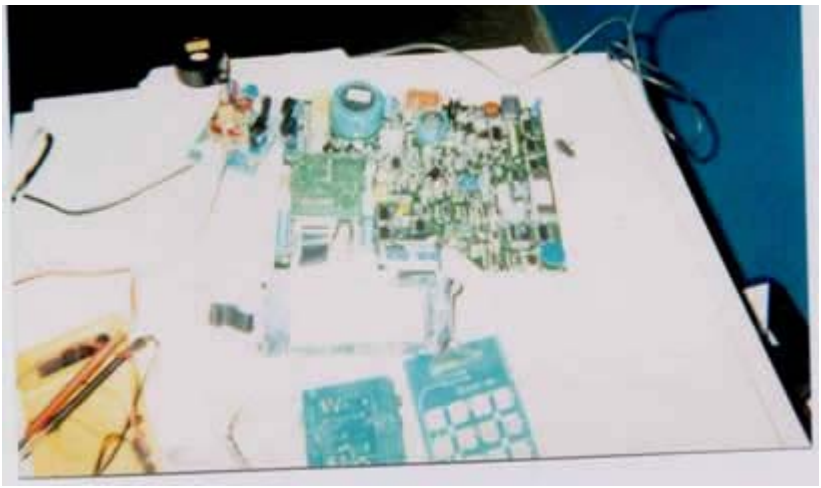
Fig. 3

En la **R** esta la combinación para abrir la cerradura con el aparatito ese que usan los técnicos de la compañía telefónica, dicha combinación es un número de tres cifras.
Donde están las **Ñ** por lo generar va el logo del fabricante de la cerradura o de la compañía telefónica.
La parte marrón es donde cae al final el muelle de estado
Los dos recuadros rojos son las muescas que anclan el habitáculo de las ruedas de combinación para que no gire con el círculo exterior pequeño.

Bueno hasta aquí esta primera parte, para la próxima les doy la llave de combinación y el estudio en detalle de todos los módulos a excepción de Pci Principal que será para la tercera parte; hubiese querido terminar este resumen antes y complementarlo mas, asi como póner mejores fotografias pero me enferme y coast.

A manera de despedida agradezco a MHM por publicarme y envio saludos a todos en la @gencia ; Gost, Guest, Boom, Allkimist@ y a SKripT(I LOVE YOU BABY).

A modo de despedida les dejo unas imágenes de la experimentación que estoy llevando a cabo con unos TM´s que tome prestado.



Les adelanto que ya logre averiguar como hace el TM para reportar fallas y demás, y como se hace para actualizar el ASM, es un poco más complicado de lo que creía.

Chau pichu

Despedida

Notas del Editor

Hemos llegado al final de un número más de nuestra revista de phreaking. Habrán notado unos pequeños cambios en el diseño y contenido de la revista, ejemplo de ello es la pequeña historieta ilustrada, que a manera de sátira nos da una visión de lo que sucede con la mayoría de las personas que se deciden a armar un emulador pero que no tienen la mínima idea de cómo hacerlo.

También habrán notado que la poesía de Jump'n Jack se publicó en su idioma original y no se incluyo una traducción a nuestro idioma, la razón es porque en la traducción se hubiera perdido parte de la esencia misma que hace a esa poesía notable.

Esta parte artística de la revista fue interesante haberla incluido para romper un poco con la monotonía que puede resultar de solo enfocarse al estudio. Sin embargo no estamos seguros de si se seguirán incluyendo este tipo de artículos en futuras ediciones, eso solo el tiempo lo dirá...

¡Nos vemos en el próximo número!

-=oSUKARu=-
mhmphreak.com

EOF