



CHUPONEO Y CHUPONEOS TELEFÓNICOS (INTERCEPTACIÓN TELEFÓNICA)

Por: Ceferino Delgado Flores

ANTECEDENTES

OBJETIVO

El presente documento describe los puntos donde se realizan la interceptación telefónica (chuponeo), el alcance de responsabilidades y los actores que intervienen. No es la intención de decir como chuponear, sino, poner en tapete la problemática.

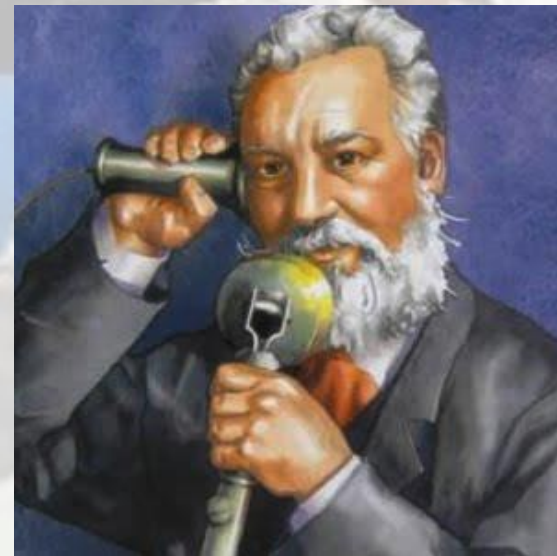
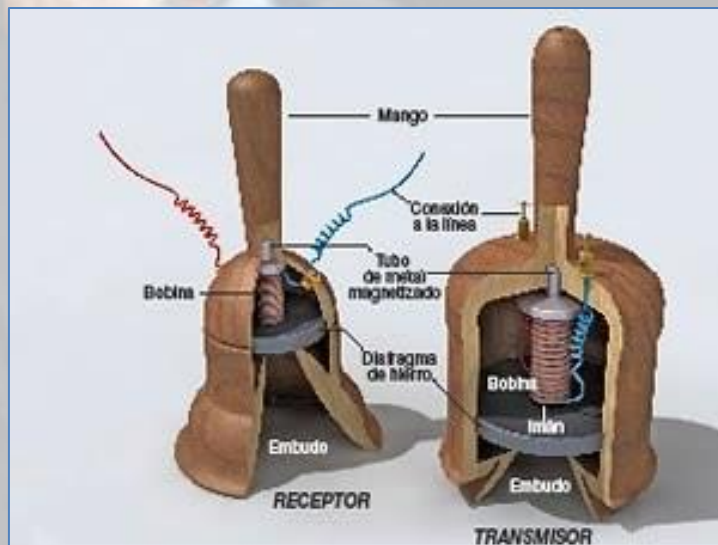
HISTORIA

En 1855, Antonio Meucci mientras trabajaba con enfermos reumáticos, a los que aplicaba pequeñas descargas eléctricas, un paciente recibió una corriente que le hizo gritar. Meucci, creyó haber oído el sonido del grito en otra habitación. Acto seguido comprobó que uno de los cables le llevaba de manera tenue la voz de su paciente, descubriendo que la transformación de las vibraciones sonoras en impulsos eléctricos permitía transmitir la voz a distancia, a través de un cable.



ANTECEDENTES

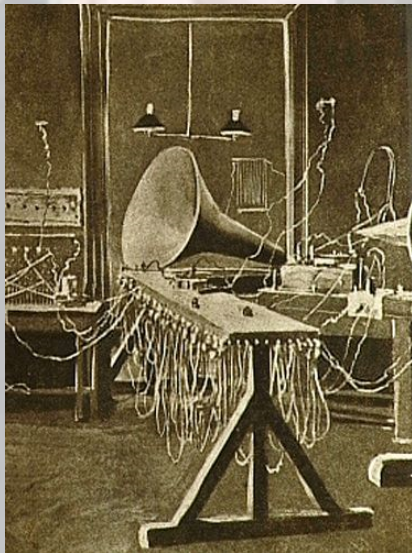
Meucci utiliza su invento (teletrófono) para crear una vía de comunicación desde su dormitorio (segundo piso) donde su esposa estaba postrada en la cama, hasta su taller, donde el trabajaba. Perfecciona su 'telégrafo parlante' y en **1857 construye el 'teléfono electromagnético'**, formado por una barra de acero imantada, una bobina de alambre y una lámina de hierro que hacía las veces de diafragma



ANTECEDENTES

CENTRAL TELEFONICA

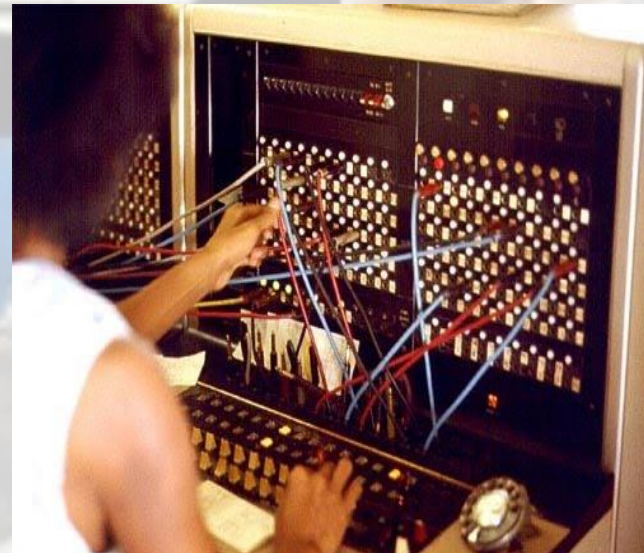
Las primeras centrales telefónicas eran switches eléctricos precarios, luego, el cuadro de conexiones, donde cada teléfono tenía su propia alimentación mediante una pila seca y una operadora que conectaba manualmente con un cable a dos interlocutores que necesitaban hablar.



Central telefónica, de switches eléctricos precarios



Central telefónica, manual, con operadora.



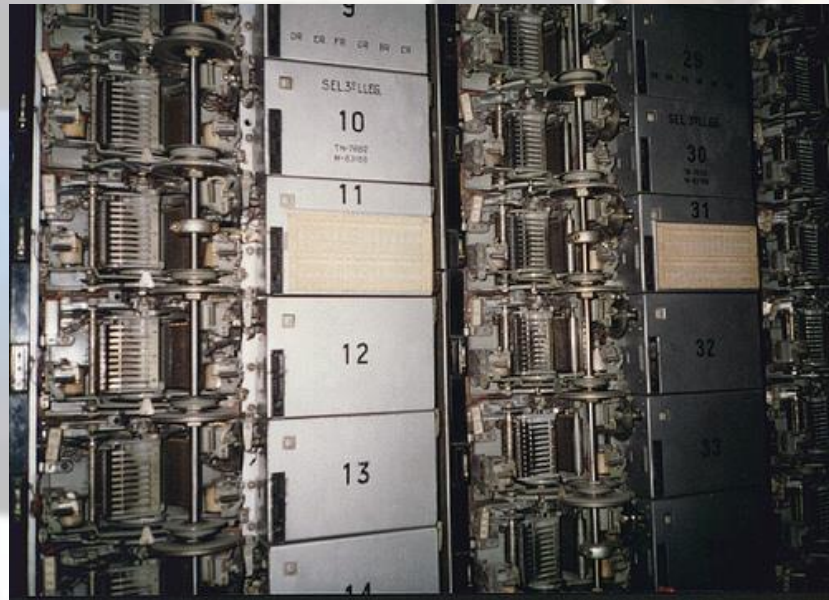
Primer cracking de la historia: la operadora de la central.

ANTECEDENTES

El primer cracking de la historia fue la operadora de la central telefónica que desviaba todas las llamadas que solicitaban el servicio de la funeraria de Almon Strowger a la del negocio de su esposo.

Este percance le da la idea a Strowger de eliminar el desvío de llamadas e eliminar a las operadoras que escuchaban las conversaciones y en 1889 patenta el Sistema Automático de Conmutación Telefónica

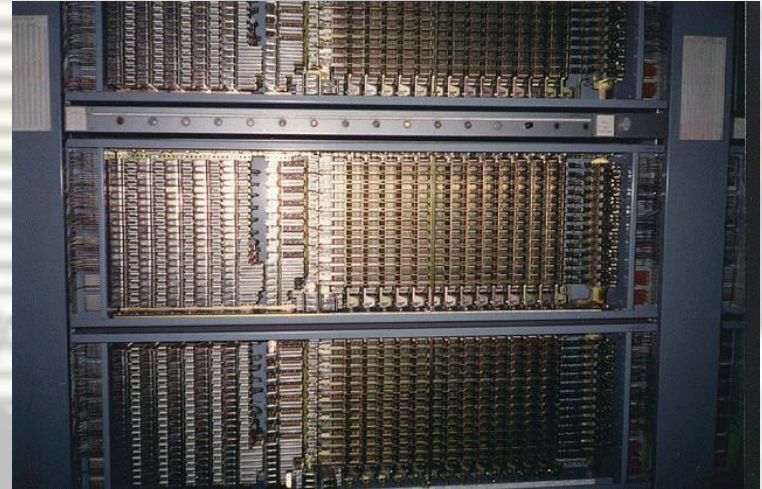
En el Perú, desde el 13 de abril de 1888 hasta diciembre de 1930, todas las centrales eran manuales con operadoras y, a partir de esa fecha se comenzaron a instalar las centrales automáticas. Entre ellas tenemos la central electromecánica secuencial tipo Rotary



Central Telefónica Rotary

ANTECEDENTES

Luego llegaron las centrales electromecánicas tipo Pentaconta 1000 o central de barras cruzadas que tenían mayor velocidad en establecer una llamada. Tanto la central Rotary como la central Pentaconta 1000 (P-1000), su red de conexión y la unidad de control eran electromecánicos.



La central Pentaconta 2000 (P-2000), su red de conexión era electromecánico pero su unidad de control era electrónico (con una pareja de dos miniordenadores de 16 bits trabajando en dúplex).



ANTECEDENTES

La primera central digital instalada en el Perú fue la Central Telefónica Neax de la NEC. La funcionalidad de esta central es que era modular y escalable. Por lo cual para que funcione otros aplicativos se tenía que comprar mas equipos a la NEC.



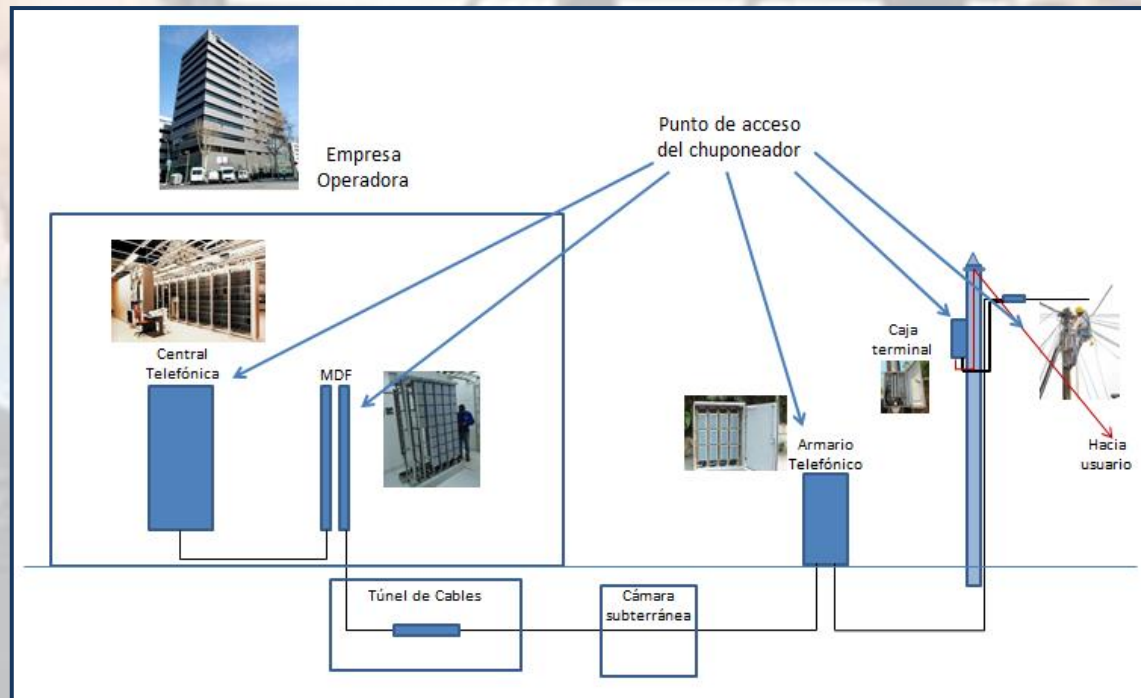
La ex INTINTEC, desarrolló la primera minicentral digital, pero por falta de componentes digitales su implementación fue del tipo electrónico. Esta minicentral debió producirse en masa para dar servicio a las localidades rurales. Los españoles abandonaron el proyecto.

Después, de la venta de las empresas peruanas, la empresa operadora trajo centrales AXE electrónicas, tiempo después recién llegaron a instalar centrales digitales. Hoy en día en el mercado, hay toda una variedad de centrales telefónicas, AXE, Huawei, Ericsson, Siemens, Alcatel, Nortel, Motorola, etc.

INTERCEPTACIÓN TELEFÓNICA

CONTENIDO

Según el tipo de medio de transmisión, varía la modalidad y los interventores en una interceptación telefónica.



La interceptación de llamadas telefónicas podían realizarse desde las centrales telefónicas con operadora hasta la central AXE y NEAX, y de todas maneras con conocimiento de la empresa operadora.

INTERCEPTACIÓN TELEFÓNICA

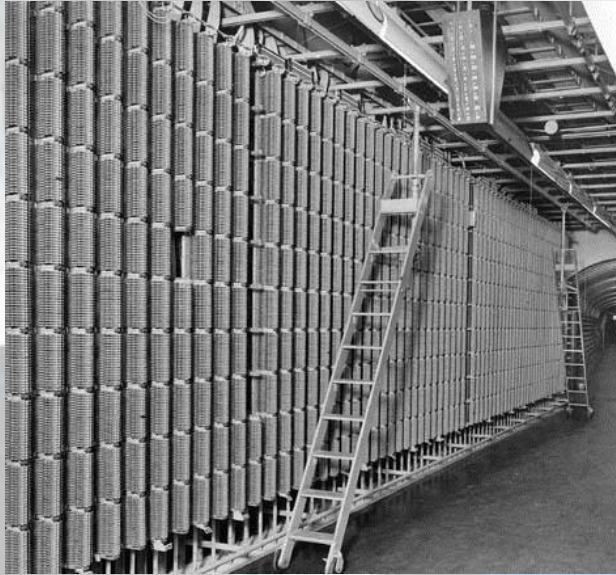
Tramo: Equipo – MDF (Main Distribution Frame)



En EEUU, en la lucha contra el crimen organizado, las centrales telefónicas con operadora, tenían doble cableado de la persona que se tenía que intervenir sus llamadas telefónicas.

En el Perú, dicen que en el MDF, de una central telefónica del centro de Lima, había varios blocks peinados a un cable que llegaba a las oficinas de un lugar cercano a la central telefónica.

INTERCEPTACIÓN TELEFÓNICA



Otros dicen que se utilizó un cable troncalero y la derivación de ese cable iba hacia una vivienda adquirida profesamente para interceptar las llamadas telefónicas, algo debe ser cierto pues estuvieron implicados cerca de 30 personas, entre técnicos y solo jefes de área y de sección. Cuando todos saben que las ordenes vienen de arriba, de la alta Gerencia..

En este tramo central y MDF, el alcance es: Gobierno, Empresa Operadora, Gerente de Desarrollo, Jefe de Área y Técnico, porque está dentro de la central telefónica. Si el beneficio es solo para la Empresa entonces, el alcance es: Empresa Operadora, Gerente de Desarrollo, Jefe de Área y Técnico. Dicen que hubo un caso donde el alcance era: Gerente de Desarrollo, Jefe de área y Técnico.

INTERCEPTACIÓN TELEFÓNICA



En las centrales telefónicas, en la actualidad, las empresas operadoras tienen instalado un elemento denominado SBC (Session Border Controllers) por razones de seguridad, calidad de servicio, señalización, contabilidad del tráfico y llamadas a los servicios de emergencia.

En el encaminamiento de la información dentro de estas redes IP se emplean estos elementos en la interconexión que están ubicados en la frontera o punto de interconexión de las redes. Pero adicionalmente, estos elementos pueden realizar funciones de control de admisión, privacidad, encriptación, adaptación de formatos (transcodificación), conversión de protocolos, interceptación legal, etc.

Por ejemplo un equipo Cisco XR 12000, es Router de enrutamiento inteligente con una plataforma de 2.5 Gbps y escalable a una próxima generación IP homologado al mercado y, desde una estación remota con una Lap Top se puede hacer interceptación legal.

INTERCEPTACIÓN TELEFÓNICA

Tramo: Salida del MDF – Línea de abonado

Este tramo es para la telefonía fija, ya que según el medio de transmisión varía la modalidad de interceptación telefónica. En este caso existe tres tipos de interceptación:

- Doble puente en el armario.
- Doble puente en caja terminal.
- Interceptación en el cable de acometida.
- Interceptación del teléfono inalámbrico.



Doble puente en el armario.

Como la seguridad y la manipulación del armario es de responsabilidad de un técnico, entonces el alcance es: jefe de grupo y técnico o solo técnico (de empresa operadora o empresa colaboradora). Aquí la interceptación es puntual, no es masivo.



INTERCEPTACIÓN TELEFÓNICA

Doble puente en caja terminal.

Este tipo de interceptación es similar al del anterior, pero aumenta los actores ya que es un elemento pasivo expuesto al aire libre: El alcance es: técnico, jefe de grupo o tercera persona ajena a la empresa operadora con conocimiento de planta externa y telefonía.



Intercepción en el cable de acometida.

En este tipo de interceptación telefónica es mayormente hecho por terceras personas ajenas a la empresa operadora. Una forma es picando el cable de acometida, algunas veces se puede confundir con el robo de línea. La responsabilidad es: del técnico, cuando existe dificultad en reconocer las facilidades técnicas y la de tercera persona cuando es fácil hacer seguimiento de línea.



INTERCEPTACIÓN TELEFÓNICA

Interceptación del teléfono inalámbrico

Con un radio scanner, solo se tiene que buscar dentro de la banda de los 900 MHz, 2.4 GHz (banda de los teléfonos inalámbricos) con el scanner se sintoniza la frecuencia, escuchar la conversación y realizar la grabación de la conversación telefónica.



La otra modalidad es mas sencilla, se utiliza un teléfono inalámbrico, se saca de la base, se enciende el teléfono (talk) para tener tono, desconectar la corriente de la base, dirigirse cerca de la vivienda, poner en modo "Mute", esperar hasta que se escuche la conversación. Para mayor comodidad se puede utilizar una antena para obtener mayor ganancia de señal y de lejos escuchar la conversación.



INTERCEPTACIÓN TELEFÓNICA

Para los teléfonos inalámbricos 1.9 MHz con tecnología DECT (GSM local). Como el descifrado mediante ingeniería inversa se han desarrollado en los teléfonos celulares, lo vamos a ver en esa parte, donde el conocer este algoritmo permite capturar el audio de una conversación e incluso suplantar a la estación base legítima. El alcance es tercera persona.



Como se ha podido ver en la telefonía fija no se requiere alta tecnología para interceptar una llamada telefónica. En la interceptación telefónica en central, ya existe el equipo, porque forma parte del área de control y mantenimiento. Además, las operadoras tienen el control total de los routers, donde se puede interceptar una llamada telefónica y data.

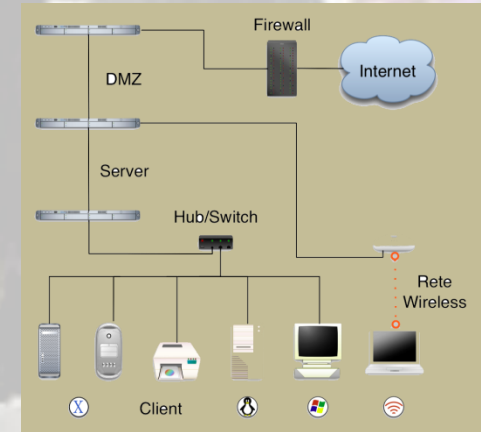
En el 2000, un marino del área de seguridad nos mostró un pequeño equipo de interceptación telefónica en cable de acometida, no sé porque hubo en ese tiempo tantos marinos trabajando en una empresa operadora.

INTERCEPTACIÓN TELEFÓNICA

Interceptación telefónica en la red LAN

Las empresas y las instituciones dan a algunos de sus trabajadores teléfonos celulares si, trabajan con RPM, la central PBX tiene las líneas troncales amarradas a un número RPM que sirve de canal para controlar las llamadas del trabajador.

En el trabajo de Pedro, su empresa tienen una central PAX Meridian Nortel, Norstar, con lo cual, el jefe puede escuchar a cualquier teléfono de línea directa o de los anexos (592 anexos) que en ese momento esté activado o grabar las conversaciones de todas las llamadas (tarjeta de grabación “sabueso”) y tener el reporte de las llamadas realizadas por cada línea o anexo (fecha, hora, número telefónico de entrada y salida. No sé si este es el caso del Callao.



INTERCEPTACIÓN TELEFÓNICA

Si el teléfono celular que da la empresa o institución es un teléfono libre, el administrador de red por encargo del Gerente General instala el software IPhone Monitor con el cual se intercepta las llamadas entrantes y salientes, graba las conversaciones, visualiza los MSM de entradas y salidas, avisa el cambio de chip, hace localización geográfica, etc. Este tipo de software los hay para todo tipo de tecnología.



Para interceptar el WhatsApp existe en versión gratuita (modo de prueba) y versión completa del SpyBubble. Tiene para la ubicación geográfica, rastreo a todas las llamadas celulares, acceso a la agenda, acceso al correo electrónico, acceso a las fotografías tomadas y acceso a todos los mensajes de texto. Este software solo hay para los Iphone y los teléfonos con Android. Alcance, administrador de red y gerente general o gerente de informática.



INTERCEPTACIÓN TELEFÓNICA

Interceptación telefónica en la red celular

Como ya se ha dicho, en la parte de la central telefónica, es fácil realizar una interceptación telefónica legal.

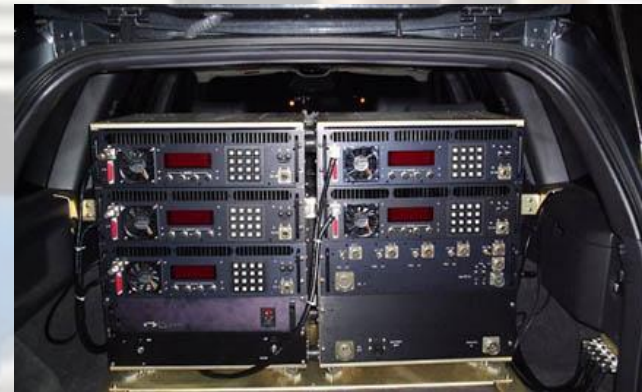
Modo Phishing - 1

Todas las llamadas y los mensajes de texto dentro de una cierta área (vivienda, refugio, antro, guarida, etc.) donde viven o se reúnen gente de mal vivir, se intercepta sus comunicaciones para eliminar el crimen organizado.

Por lo tanto, el alcance es: gobierno con las empresas operadoras, porque

el gobierno solicita a la empresa operadora los datos de las llamadas destino.

Este equipo multianalizador tiene tres tipos de funciones: Interceptar comunicaciones, bloquear e inhabilitar llamadas y garantizar la privacidad de equipos seleccionados.



NetHawk Call Blocker

INTERCEPTACIÓN TELEFÓNICA

Este equipo es de ultima generación, mas compacto y una amplia gama de sistemas.

Por lo tanto, el alcance es igual al anterior: gobierno con las empresas operadoras.



Utilizando el Modo Ingeniería del Motorola (solo sistema 2G)

Es una interceptación telefónica antigua utilizando el modo ingeniería del celular Motorola. Muchos teléfonos en este modo se puede visualizar; celda activa, nivel de potencia recibida, potencia máxima, parámetros del sistema, etc. Pero también, se utiliza para ingresar a un canal de transferencia celular y escuchar la conversación que se esta realizando.



INTERCEPTACIÓN TELEFÓNICA

Desde que el ingeniero informático alemán Karsten Nohl ha descifrado el algoritmo utilizado para cifrar las comunicaciones del estándar GSM, las comunicaciones son fáciles de interceptar. El algoritmo descifrado es técnicamente conocido como A5/1, se trata de un código binario, que se utiliza desde 1988 en mantener en la intimidad las conversaciones celulares.



A pesar que se actualizó el A5/1 con el A5/2, este nuevo código también ya ha sido descifrado

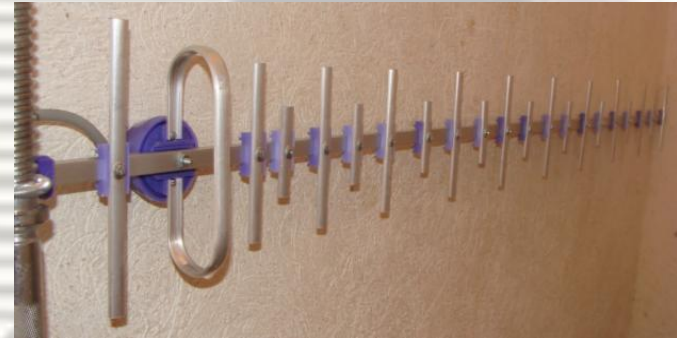
Interceptación telefónica Modo Phishing - 2

Esta técnica utiliza una antena “falsa” llamada INSI catchers, que engaña a todos los teléfonos celulares coberturados, haciéndoles creer que es la BTS (estación base) de la empresa operadora.

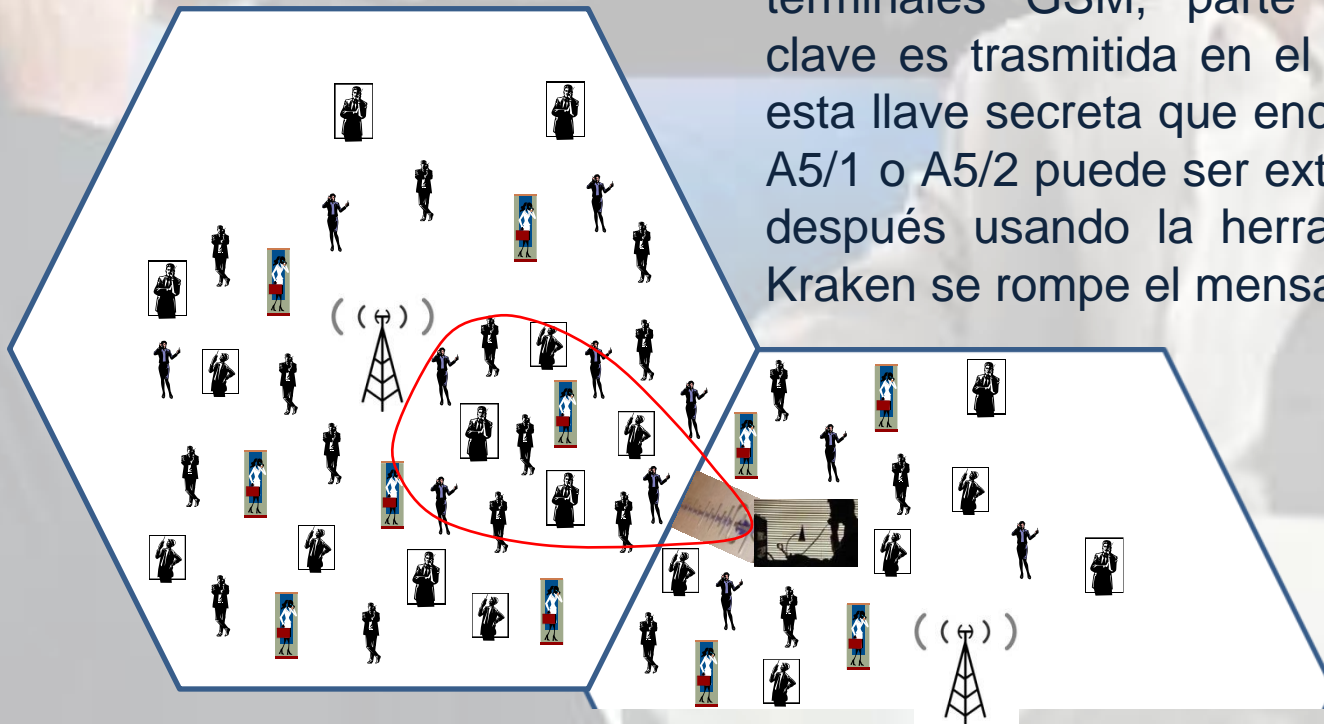
Cuando el usuario desea realizar una llamada, el teléfono celular envía un mensaje a la BTS solicitando una conexión a un numero de teléfono específico y es en ese momento que se inicia la interceptación telefónica.

INTERCEPTACIÓN TELEFÓNICA

Para esta interceptación se utiliza una antena GSM tipo yagui de 20 elementos que simulará a una estación base. Para tener mayor cobertura se puede colocar tres antenas, coberturando cada uno 160° .



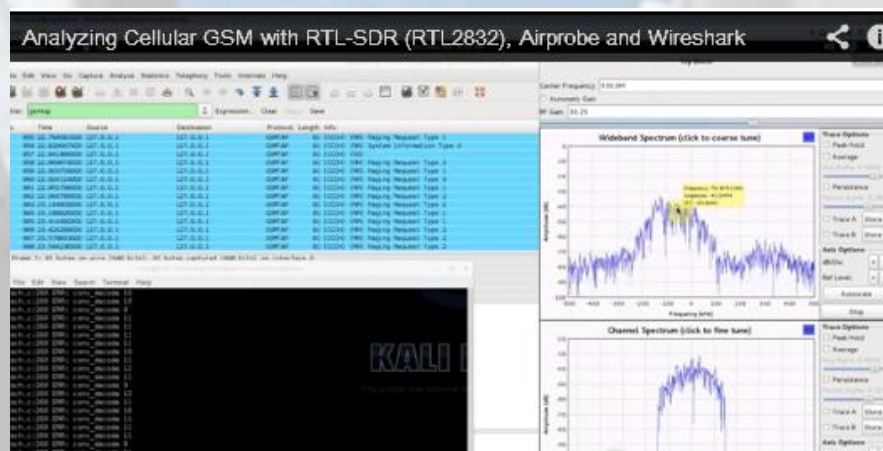
La conversación entre dos terminales GSM, parte de su clave es transmitida en el tráfico, esta llave secreta que encripta el A5/1 o A5/2 puede ser extraída y después usando la herramienta Kraken se rompe el mensaje.



INTERCEPTACIÓN TELEFÓNICA

Luego estas conversaciones telefónicas y los SMS pueden ser descifradas en segundos usando las tablas rainbow. Para esto realizan los siguientes pasos;

- Capturan y graban los datos de la llamada, utilizando como equipo USRP N210 y con software rainbowcrack-1.5 –win64 (Windows 8 de 64 bits).
- Procesan los datos (Utilizan el software Airprobe)
- Descifran las llaves A5/1, utilizando las tablas rainbow (Descargan las tablas rainbow en <http://project-rainbowcrack.com/table.htm>)
- Obtienen la voz con el Airprobe.



INTERCEPTACIÓN TELEFÓNICA

Conclusiones

Todos los medios de comunicación han mostrado como interceptación telefónica las realizadas por la persona que llama o el amigo que graba tu conversación o la de tu empresa que graba todo lo que haces, mas no lo que se ha presentado en este documento.

Los teléfonos con 2G son interceptables, los de 3G también, son interceptables, porque “obligan” al celular que automáticamente realice un downgrade de 3G a 2G y ahí interceptar la llamada.

Los políticos dicen que están siendo “chuponeados” por el gobierno, que se les esta haciendo reglaje, hasta ahora solo se ha podido encontrar que la DINI está enfrascado en la lucha contra el crimen organizado.

Cada nueva funcionalidad es una puerta abierta a la interceptación telefónica, por ejemplo hay un teléfono celular con la función de router, por lo tanto se puede ingresar a sus datos por su red WiFi.

INTERCEPTACIÓN TELEFÓNICA

Recomendaciones

Existe varios métodos para ver si tu teléfono tienen un software espía instalado, hay que chequear y eliminar el software.

Las conversaciones por teléfono celular deben de ser triviales y domesticas.

Cuando uno tiene una reunión privada, utilizar los bloqueadores de video y de audio.

Utilizar teléfonos prepago en las llamadas de importancia media, cambiar de chip con periodicidad regular.

Otros artículos:

<http://www.monografias.com/trabajos94/red-del-estado-caso-peruano/red-del-estado-caso-peruano.shtml>

<http://www.monografias.com/trabajos96/comunicaciones-inseguras/comunicaciones-inseguras.shtml>

<http://www.eumed.net/cursecon/ecolat/pe/2012/cdf.html>

INTERCEPTACIÓN TELEFÓNICA

GRACIAS