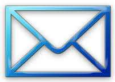

CIBERDEFENSA
PROGRAMA DE VINCULACIÓN Y DIFUSIÓN
CIBERDEFENSA
JORNADA REGIONAL EN ROSARIO
11 DE AGOSTO DE 2014
UTN Rosario - Zeballos 1341 - Salón de usos múltiples
inscripción e informes www.mindef.gob.ar
ORGANIZAN:
Facultad Regional Rosario
Universidad Tecnológica Nacional
AGASSI
CUANDO UN PAÍS SE JUNTA.
HAY FUERZA.
Ministerio de
Defensa
Presidencia de la Nación

Ministerio de Defensa
Presidencia de la Nación

Fernando A. Corvalán

Coordinador Técnico del Comité de Ciberdefensa

Jefatura de Gabinete de asesores



fernando.corvalan@mindef.gov.ar

@fercorvalan

Dispositivos Móviles y Cifrado

Estado del arte de la seguridad en comunicaciones móviles GSM / GPRS / 3G

Funcionalidad vs. Seguridad

- La mayoría de los productos, servicios, protocolos de red fueron pensados para ***usarse*** y que ***funcionen rápidamente.***
- No fueron diseñados como ***seguros.***
- La seguridad casi siempre fue una ***modificación posterior*** que afecta la performance y suele ser una complicación de diseño e implementación.

Funcionalidad vs. Seguridad

- ***Protocolos no seguros:***

HTTP – NFS – SMB – FTP

DNS – Telnet – POP3 – SNMP

- ***Protocolos seguros:***

HTTPS – SFTP - DNSsec – SSH – SSL - IPsec

Telefonía Móvil GSM: Conceptos

- La arquitectura esta basada en celdas
- Medio fisico compartido
  (TDMA - Time Division Multiple Access)
- Frecuency Hopping (saltos de frecuencia - ciclicos o basados en un algoritmo complejo)
- Seleccion automatica de celda sin intervención del usuario

Telefonía Móvil GSM:
Selección inicial de celdas

- Debe ser una celda de la PLNM seleccionada (Public Land Mobile Network)
- No debe ser una celda restringida por el operador
- No debe ser una celda de una LA (Location Area) de la lista prohibida para roaming
- El parametro C1 (Radio Path Loss) debe ser mayor al limite establecido por el operador (basado en una formula de nivel de señal, potencia necesaria de la base y del movil, SNR, etc)

Telefonía Móvil GSM:
Reselección de celdas

- Parametros C1/C2 indican que hay una mejor opción de nivel de señal
- Fallo en el downlink
- La celda pasó a ser restingida por el operador

Seguridad de la red GSM

- Confidencialidad del suscriptor
  Su IMSI (International Mobile Subscriber Identity) se considera ***confidencial***.
  Puede usarse para geolocalizarlo. El sistema lo transmite cifrado para evitar que quien pueda escuchar el canal podria descubrir la ubicacion de un telefono.
  Suele utilizarse en la practica un *alias* TMSI (Temporary Mobile Suscriber Number) y existe una tabla TMSI-IMSI por celda

- Autenticación del suscriptor (evitar fraudes)
  El proceso de autenticacion se produce una vez que la celda vincula IMSI con TMSI. Utiliza un esquema *chalenge-response* basado en una clave precompartida entre el operador y el suscriptor (SIM) denominada Ki (individual suscriber Authentication Key) y tambien se genera la clave de sesion (Kc) o tambien llamada clave de cifrado (Cipher Key de 64Bits)

- No autenticación de la radio base (vulnerabilidad)

- Se utilizan las familias de Algoritmos A de cifrado.
  En este caso los algoritmos A8 y A5

Algoritmos de criptograficos GSM

- ***A3:*** Autenticacion de la identidad del usuario
  Ki (128bits) / RAND (128bits) -> SRES 32bits
- ***A8:*** Se utiliza para computar la clave de cifrado a partir de un *challenge-response* con datos en la SIM.
  Los algoritmos A3 y A8 no estan especificados en la norma GSM, y son de uso interno del operador (PLMN), aunque de facto son usados por casi todos los operadores.

Familia de algoritmos A/5

- El algoritmo es identico en todas las PLNM
- Algoritmo no publicado, solo compartido entre operadoras y organización GSM/MoU
- Longitud Kc 64bits / Count (22 bits) / bloques de 114 bits

Familia de algoritmos A/5

- A5/0 es equivalente a “no cifrado”
- A5/1 (1987) - Algoritmo base de GSM. Considerado roto en la actualidad tanto en sus versiones de 64 como 128 bits
- A5/2 (1989) - En desuso. Es un A5/1 debilitado para exportación
- A5/3 for GSM - Basado en KASUMI. Solo para celdas UTRAN
- A5/4 for GSM- de 128bits, de uso restringido

Debilidades de GSM

- IMSI en diversas etapas se transmite en claro. Puede solicitarse en ataques activos
- Debilidades criptográficas de A5
- No existe autenticación inversa (de la base) lo que facilita la suplantación de red
- La selección de celda se realiza sin autorización del usuario. Por nivel de señal
- El uso de A5/0 esta permitido, sin aviso

Algunas noticias sobre cifrado A5

martes, diciembre 29, 2009

Rompen cifrado GSM de 3,500 Millones de celulares en todo el mundo

eliax id: **7344** **josé elías** en dic 29, 2009 a las 10:15 AM (10:15 horas)

Esta noticia de hoy es bastante preocupante para toda persona cuyo celular utilice las redes GSM (es decir, prácticamente el 100% de todo celular que contenga un chip "SIM" reemplazable), lo que significa mas de 3,500 millones de celulares en todo el mundo.

Un alemán de nombre Karsten Nohl y experto en cifrados acaba de romper (a fuerza bruta) el algoritmo que protege todas nuestras comunicaciones celulares en redes GSM. Lo mas preocupante del caso, y algo que yo desconocía, es que el algoritmo de cifrado que nos protege de que cualquier persona escuche nuestras conversaciones es un dinosaurio de apenas 64 bits llamado el Algoritmo A5/1, creado en 1988.

Mas preocupante aun es que desde el 1997 ya existe el sucesor a ese algoritmo, llamado el A5/3 de 128 bits, pero según la Asociación GSM (encargada de estos estándares), las empresas de telefonía celular "han puesto poco interés en esta nueva versión" y la mayoría no la ha implementado, lo que les debe dar indicación a todos de cuántos aman estas empresas a sus clientes y se preocupan por su privacidad...

¿La solución a corto plazo? Pues según dicha Asociación GSM no tenemos que preocuparnos mucho, ya que existe un "Plan B" que permite que las empresas de telefonía cambien las claves de 64 bits encontradas, *pero por otras de 64 bits.*

Sin embargo, esa obviamente **no** es una solución, ya que el mismo método utilizado para encontrar la primera clave se puede utilizar perfectamente igual para averiguar la segunda clave. Lo que se necesita es que la industria se mueva de manera urgente al nuevo estándar de 128 bits lo antes posible, pues el código que demuestra el ataque ya está liberado y disponible para cualquier ciber-criminal en Internet, y es solo cuestión de tiempo (yo diría que de literalmente unos pocos días) para que sea trivial que cualquier persona escuche nuestras conversaciones desde cualquier celular.

Por otro lado, esta es una excelente oportunidad para el mercado de VoIP (Voz sobre IP, como son programas como Skype), para que anuncien estándares de cifrados de voz de alta potencia que son inmune a estos ataques. Recuerden que el problema con los sistemas tradicionales de telefonía es que están muy "amarrados" a hardware, pero el VoIP depende mas de software que otra cosa, lo que significa que se puede adaptar muchísimo mas rápidamente a este tipo de ataques.

Mientras tanto, mucho cuidado con lo que dicen por esos celulares...

Algunas noticias sobre cifrado A5

miércoles, enero 20, 2010

Seguridad de celulares GSM de 128 bits también violada...

eliax id: **7407** **josé elías** en ene 20, 2010 a las 12:39 AM (00:39 horas)

Si recuerdan hace apenas unas 3 semanas que publiqué un artículo en eliax sobre como un grupo de expertos había demostrado romper la seguridad básica que protege las comunicaciones de 3,500 millones de celulares tipo GSM (es decir, los que utilizan un chip SIM) en el mundo.

En ese entonces escribí que la solución propuesta por los expertos era dejar atrás el sistema obsoleto de 64 bits y del 1988, y adoptar un sucesor de 128 bits que fue aprobado en el 1997.

Pues para sorpresa de muchos, en los pocos días desde que fue publicado el código de cómo atacar el sistema de 64 bits, un equipo del *Weizmann Institute of Science* logró romper también el sistema de 128 bits, y en tan solo dos horas de procesamiento.

Lo mas alarmante del caso es que esas 2 horas que tomó romper el esquema de seguridad, fue en una sola PC genérica utilizada para la investigación, y en un programa no optimizado. ¿Qué significa esto? Que con un programa optimizado, y creado para funcionar de manera en paralelo, que sería en principio romper la seguridad de 128 bits de GSM en tiempo real con un equipo relativamente barato.

En otras palabras, pueden estar casi 100% seguros que en estos precisos momentos varias agencias de inteligencia, así como hackers del mercado negro, ya poseen la capacidad de descifrar conversaciones de mas de 3,500 millones de celulares en todo el mundo.

Algunas noticias sobre cifrado A5

domingo, agosto 1, 2010

Con US$1500 dólares en equipos, se puede intervenir cualquier celular GSM 2G

eliax id: **7981** **josé elías** en ago 1, 2010 a las 12:52 PM (12:52 horas)

A finales del año pasado e inicios de este les hablé como hackers habían logrado romper los sistemas de cifrados de datos de celulares tipo GSM de todo el mundo, y ahora tenemos una noticia muchos mas preocupante.

Un hacker acaba de demostrar esta semana pasada en la conferencia DefCon 18 (en el mismo hotel en donde días ante en la BlackHat 2010 se demostró como romper la seguridad de millones de routers de Internet), que es posible ir al próximo paso, al menos con redes GSM 2G: Escuchar cualquier conversación cercana.

Lo que el hacker hizo, en resumen, fue comprar apenas US$1,500 dólares en equipos disponibles en cualquier lugar, y tomar ventaja de una gran debilidad de las redes GSm 2G: Los celulares se conectan siempre a la torre que tenga la mayor potencia de señal, *sin importar cual torre sea y sin autenticar que es una torre real.*

En otras palabras, lo que este hacker hizo fue bastante sencillo de entender conceptualmente: Creó un puente entre una torre real y celulares cercanos, y como su "torre" (es decir, su laptop con una antena mas o menos grande) ofrecía una señal mas clara a los celulares cercanos, estos se conectaban a su laptop en vez de a la torre real, lo que permitió que el investigador en seguridad escuchara sus conversaciones (cosa que demostró en vivo en la conferencia con celulares de los asistentes).

Aclaró que su software no está siquiera optimizado, pues por el momento alguien puede saber en el otro extremo que algo no está bien ya que saldría el *Caller ID* de su torre celular improvisada y no de la del celular que originó la llamada, pero asegura que eso es algo que ya lo hacen los sistemas profesionales y gubernamentales.

¿La solución a corto plazo? Cerrar acceso a todas las redes 2G del mundo y adoptar exclusivamente las redes 3G como mínimo. Para el que no sea muy técnico, por "2G" se refieren a servicios como conectividad EDGE que vemos en millones de celulares a diario.

Métodos de ataque a redes GSM

Equipamiento necesario para no profesionales:

- Radio de 900MHz (USRP + tarjeta RA900)
- Demodulador GSM (GNU Radio + Airprobe)
- Decodificador GSM (Airprobe + Wireshark)
- Tools de Criptoanalisis (A5 SecProject + Tablas de hash)
- Codec’s GSM (OpenBTS + asterisk)

Métodos de ataque a redes GSM

- Ataque al canal de señalización
  - Escucha de conversaciones
  - Captura de SMS

  Son de dificil ejecución, ya que requiere:
  - capturar trafico Downlink y Uplink
    lo que implica estar cerca de ambas locaciones
  - conocer algoritmos de *frecuency hopping*

Métodos de ataque a redes GSM

- Ataques SMS
  - Falsear origen del SMS -> inducir respuestas
  - OTA: ataques dirigidos al SIM
- Ataques WAP-Push / MMS
  - Permite insertar links que redireccionan al usuario a descarga de malware

Métodos de ataque a redes GSM

- Ataque de base falsa (fase inicial)
  - Requiere conocer el operador móvil
  - Estar en una ubicación física cercana al objetivo
  - Conocer el IMSI del objetivo u obtenerlo con ataques activos al móvil o al canal SS7 del operador móvil o por comparación de tablas en celdas donde estuvo registrado

Métodos de ataque a redes GSM

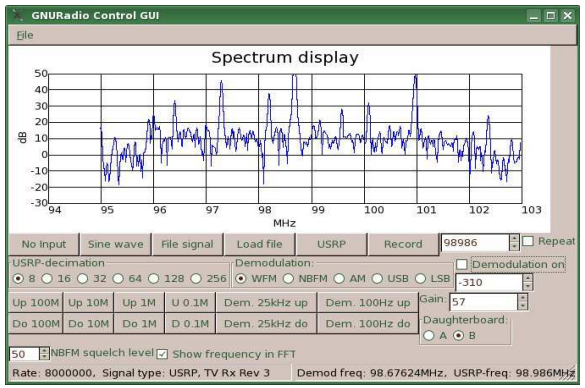
- Ataque de base falsa (fase 2)
  - Debe escuchar y emular parámetros de la celda y celdas vecinas (ID's, Frecuencias, PLNM, etc)
  - Capturar y emular el Beacom y niveles de señal
  - Inhibir (con un equipo transmisor) la frecuencia de la celda activa y a la par emitir en canal aledaño la señal BCCH para iniciar un proceso de ***Update Location*** automático en el móvil.
  - Emular los parámetros reales correspondientes al prestador MMC, NCC, ARFCN, PLNM, etc
  - Mediante vinculo VoIP se genera conexión saliente

Métodos de ataque a redes GSM

- Ataque de base falsa (fase 3)
  - La base falsa solicita el IMSI y el IMEI de la victima
  - En la fase de cifrado, acepta lo propuesto por el móvil, pero la base fuerza el uso de A5/0 (plano). Esto no es percibido por el usuario
  - El usuario no recibe llamadas entrantes ni SMS
  - Todo el trafico saliente (Voz y SMS) es interceptado mediante una variante de MitM en GSM

Algunas fuentes de información

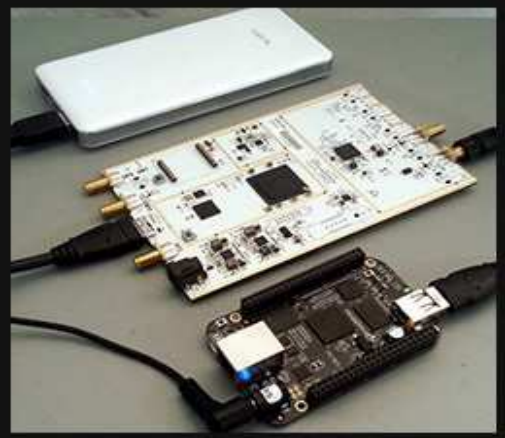
- OpenBTS.org
- GNURadio.org
- http://sdr.osmocom.org/trac/wiki/rtl-sdr
- http://www.ettus.com/ (USRP RF)



GSM Base station – u$s 750 (2014)

A GSM Base Station With Software Defined Radio

July 5, 2014 By Brian Benchoff • 34 Comments



If you're wondering how to get a better signal on your cellphone, or just want to set up your own private cell network, this one is for you. It's a GSM base station made with a BeagleBone Black and a not too expensive software defined radio board.

The key component of this build is obviously the software defined radio. [Julian] is using a USRP B200 radio for this project. It's not cheap, but it is a very nice piece of hardware capable of doing just about anything with GNU Radio. This board is controlled by a BeagleBone Black, a pretty cheap solution that puts the total cost of the hardware somewhere around $750.

The software side of the build is mostly handled by OpenBTS, the open source project for the software part of a cell station. This controls the transceiver, makes calls and SMS, and all the backend stuff every other cell station does. OpenBTS also includes support for Asterisk, the software of choice for PBX and VoIP setups. Running this allows you to make calls and send texts with your SDR-equipped, Internet-enabled BeagleBone Black anywhere on the planet.

Similitudes / Diferencias GSM - GPRS

- Los protocolos de cifrado son de la familia GPRS A5. Soporta las especificaciones GEA1 – GEA2 – GEA3 y GEA0 (plano) que puede ser usado como vector de ataque de estacion base falsa (similar a GSM)
- No hay ataques pasivos publicados de GPRS, ya que el cifrado A5 es en la capa LLC

Vulnerabilidades GPRS

- Captura pasiva del trafico GPRS y obtengo RAND y SRES
- Fuerzo mediante estación falsa el inicio de cifrado A5/1. El móvil usa el mismo RAND.
- De esa forma puedo obtener Kc y aplicar análisis criptográfico al trafico capturado
- Es factible un ataque de base falsa forzando GEA0 sin cifrado y ataque de MitM IP

Telefonía SEGURA (consideraciones)

Seguridad por capas

- seguridad del hardware
- seguridad del S.O
- seguridad de las aplicaciones
- seguridad del vínculo

SMARTPHONES

- Potencia de procesamiento (1 o mas Cores)
- Internet 3G / WiFi
- Camara 5MP o mas
- GPS
- SO Android / IOS / Windows Mobile
- Acceso a millones de aplicaciones del playstore

SMARTPHONES: Riesgos

- Geoposicionamiento Tracking 3G/ WiFi / GPS
- SMS Premium (ejemplo Linterna)
- Robo de credenciales / Datos / Archivos / Contactos
- Grabacion de conversaciones e imagenes
- ubicacion de redes WiFi y sus claves de acceso
- Exceso de permisos
- Escribir en redes sociales / SMS en tu nombre
- Compras electronicas (billetera electronica)
- Clicking, trafico Web y spam -> consumo de ancho de banda, consumo del abono de datos y bateria

Aplicaciones y permisos / playstore

Ejemplo de abuso de permisos de una aplicación Android

"LINTERNA LED SUPER BRILLANTE" Surpax Technology Inc.

- recuperar aplicaciones en ejecución
- Fotos/archivos multimedia/archivos
- modificar o eliminar contenido del almacenamiento USB
- probar acceso a almacenamiento protegido
- Cámara/micrófono
- realizar fotografías y vídeos
- Información sobre la conexión Wi-Fi
- ver conexiones Wi-Fi
- ID de dispositivo y datos de llamada
- consultar la identidad y el estado del teléfono
- Envío y recepción de SMS
- Otros
  - recibir datos de Internet
  - controlar linterna ← **era lo unico que deberia tener como permisos**
  - modificar ajustes de visualización del sistema
  - modificar los ajustes del sistema
  - impedir que el dispositivo entre en modo de suspensión ← **2do permiso (teorico)**
  - ver conexiones de red
  - acceso completo a red

Telefonía SEGURA (requerimientos)

- Tráfico de Voz: destinos cifrados / no cifrados
- Mensajeria: SMS / email / Chat Cifrados
- Navegacion: Búsqueda y navegación seguras
- Compatibilidad: Redes GSM / 3G / LTE compatibles
- Gestión: Búsqueda y localización, Borrado y bloqueo remoto
- Almacenamiento: cifrado local y tránsito seguro

Smartphones en Defensa

- Hardware Seguro
  solo modelos testeados.
- Software Seguro
  - S.O Segurizado (no estándar)
- Aplicaciones Seguras
  - Solo APP autorizadas. Ecosistema cerrado
- Seguridad del vinculo
  - Cifrado de norma + sobrecifrado / VPN

Equipos disponibles en mercado

Blackphone

- Plataforma cerrada
- Basado en Android, segurizado (PrivatOS)
- SMS / Voz / Datos Cifrados / No Cifrados
- Infraestructura segura del fabricante
- Respaldo:
  Mike Janke. ex SEAL y especialista en seguridad.
  Phil Zimmermann, leyenda de la criptografía (creador de PGP y ZRTP)

Blackphone – Silent Circle app

CONNECTIVITY

- Single micro-SIM slot
- Bluetooth Class 4.0 LE
- Wi-Fi 802.11b/g/n
- Micro USB
- 3.5mm audio jack

SENSORS

- Gravity, light, proximity, magnetic
- GPS

HARDWARE

- Processor: Quad-core 2GHz System on Chip (SoC)
- 2000 mAh lithium polymer battery
- Up to 128GB microSDXC
- 1GB LPDDR3 RAM

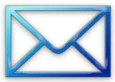
Otros fabricantes

Empresas de soluciones de cifrado militar y gobierno poseen equipos de cifrado para telefonia fija y movil con esquema similar:

- CryptoAG www.crypto.ch
- Omnisec www.omnisec.ch
- Motorola AME2000
- VMWare www.air-watch.com (BYOD)

Ministerio de Defensa
Presidencia de la Nación

Muchas gracias!


fernando.corvalan@mindef.gov.ar


@fercorvalan