LA MURPHYOLOGIA DE LA SEGURIDAD EN REDES MÓVILES

RESUMEN

En las últimas décadas las comunicaciones móviles han sorprendido a la humanidad con su evolución; las ventajas, privilegios y comodidades de poderse comunicar desde cualquier lugar del mundo sin depender de cables externos o cabinas telefónicas es sorprendente. Pero lo que verdaderamente se pretende destacar con este documento son los aspectos que enmarcan la gestión de seguridad en este tipo de redes móviles, pues la generación actual (3G) ofrece servicios de banca y comercio electrónico en donde se pueden realizar consultas, transacciones, movimientos de cuentas, pagos y demás utilidades, que ofrece una entidad bancaria desde su teléfono móvil con un modelo de seguridad no del todo fiable. Se presentarán los actuales modelos de seguridad para GSM, los que utilizará UMTS y de los que seguramente dependerán los de cuarta generación. De igual manera se presentará un análisis general de ellos y una invitación abierta a los futuros ingenieros para que incluyan en sus diseños de planificación y dimensionado la garantía del servicio.

PALABRAS CLAVES: GSM, UMTS, Redes Móviles, Gestión de Seguridad.

CARLOS A. GARCÍA TORRES
Master Comunicaciones Móviles
Universidad Politécnica de Cataluña
Dpto. Ingeniería de Red
Vodafone
Sevilla – España
ingcagt@rocketmail.com

ABSTRACT

In the last decades the mobile communications have surprised to the humanity with their evolution; the advantages, privileges and comfortablenesses of can communicate to him from any place of the world without depending of external cables or telephone box is surprising. But the most important about with this document is the aspects that frame the step of security in this type of mobile nets, because the current generation (3G) offers services of banking and e-commerce in which it can be sell out consultations, important transactions, movements, payments and other utilities that offers a bank entity from their mobile telephone with a model of security not wholly reliable. In this paper will appear the current models of security for GSM, those who it will use UMTS and of those who surely it will depend those of fourth generation (2010). Of equal way will be presented an analysis of the systems and an open invitation to the future engineers in order that include in his designs of planning and develop of the guarantee service.

KEYWORDS: GSM, UMTS, Network Mobile, Mobile Security.

1. INTRODUCCIÓN

Cuando Stuart Mc Clure, publicó su libro *Hackers, secretos y soluciones para la seguridad de redes* en el año 2000, no dudé en comprarlo, sobre todo porque me llamó la atención de manera particular, la letra cursiva color roja que traía el libro en la parte inferior izquierda de la portada "*-Es la una de la madrugada... ¿Sabe quien puede estar entrando en su red?-",* en este libro los autores explicaban el trabajo de los *tigre teams,* que llevaban a cabo pruebas de penetración contra las instalaciones informáticas corporativas y se preguntaban, *¿Con la rapidez con la que ha avanzado la tecnología, porque nadie ha inventado la seguridad perfecta?*, pero lo más acertado de esta pregunta, es su respuesta *"porque ningún diseño terrenal es perfecto"*.

Fecha de recepción: 31 Mayo de 2004
Fecha de aceptación: 23 Julio de 2004

Ahora bien, si el arma más efectiva de cualquier atacante bien intencionado o no, es la habilidad para encontrar defectos de un sistema, que a simple vista no resulten evidentes para los diseñadores o los mismos usuarios, se podría afirmar que la mejor forma de perfeccionar la seguridad de la misma es burlándola. Aparentemente los diseños de seguridad en redes móviles brindan la confianza suficiente para realizar aplicaciones comerciales, pero los modelos de seguridad en los que se basa GSM, aún presentan algunas limitantes.

Se prevee, según los expertos, que en el año 2010 saldrá al mercado la cuarta generación de comunicaciones móviles, en donde el usuario es quien elige el operador a gusto personal, desde cualquier punto del planeta con una

tarifa única de servicio. Estas ventajas resultan altamente sorprendentes y las comodidades serían aún innumerables. Conociendo los inconvenientes que todavía presentan los sistemas de comunicaciones móviles en una región en particular como cobertura, seguridad, colisión de llamadas, tiempo de respuesta entre otros. ¿Resulta confiable o mejor aún, "seguro", realizar transacciones bancarias y/o comerciales desde un lugar hipotético a otro en circunstancias similares?. Si la telefonía fija de banda ancha, posiblemente inalámbrica, la telemática ó teleinformática y las comunicaciones móviles, apuntan hacia lo que seguramente en pocos años llamaremos *mobile IP*, ¿Existirá una verdadera gestión de seguridad para estos tres tipos de sistemas, con protocolos, funcionamientos y servicios diferentes, soportados bajo una misma plataforma en una cobertura mundial?...

2. EVOLUCION

Antes de ahondar en el tema de la seguridad en redes móviles, es indispensable conocer la evolución de los sistemas, los servicios que se prestaban y las características que marcan la diferencia con los actuales.

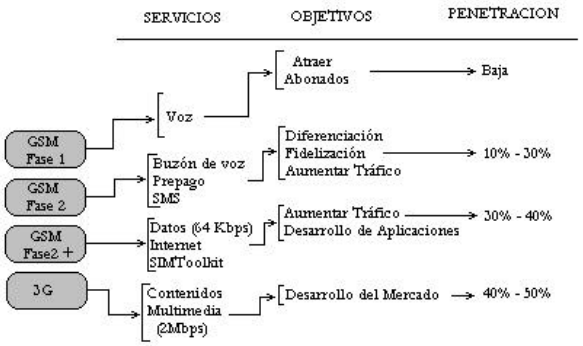

Figura 1 Evolución

A principios de los años 80's surgieron los servicios de primera generación, lo que se conocía como la generación analógica, que ofrecían servicios de voz y algunas aplicaciones de telefonía básica, en esta época, se destacaban sistemas como AMPS *(Advanced Mobile Pone Service)*, TACS *(Total Access Communication System)* y los servicios que ofrecían compañías como NTT *(Nipón Telegraph & Telephone)* y NMT *(Nordic Mobile Telephony)* entre otras. Una década mas tarde, a principios de los años 90's, la conversión analógica - digital invadía el mercado, era la generación de la transmisión digital en el interfaz radio, se mejoró la calidad de las comunicaciones por medio de técnicas de corrección de errores y se dotó de mayor capacidad a los sistemas, además de los servicios telefónicos se ofrecían el envío de SMS *(Small Message Service)* y portadores de datos a modo circuito. A esto se le denominó la segunda generación de las comunicaciones móviles (2G) y algunos sistemas que marcaron la pauta fueron D-AMPS *(Digital-AMPS)* CDMAone *(Code división múltiple Access One)*, también conocido por la norma ANSI como IS95 y GSM *(Global System for Mobile Communication)* en sus tres bandas de operación 900/1800/1900 Mhz.

Pero a pesar de las ventajas que se ofrecían, las limitaciones en lo referente al servicio de datos a modo circuito eran preocupantes, por ejemplo, GSM transmitía a 9600 bps, de manera que para suplir la necesidad de mayor velocidad a los sistemas, se logró una extensión al sistema 2G y se denominaron sistemas de generación 2'5 o como se conoce en el mercado 2+, entre dichas extensiones se encuentran HSCSD *(High- Speed Circuit-Switched Data)* cuya velocidad de transmisión máxima es de 115.2 kbps, EDGE *(Enhanced Data rates for GSM Evolution)* con un alcance de hasta 384 kbps, gracias a una técnica de modulación que permite sacar mayor partido a los canales radio GSM y GPRS *(General Packet Radio Service)* con un máximo permitido de 171,2 kbps, todos estos parámetros son en teoría realizables, pero en la práctica, debido a factores de distinta índole entre los que se destacan las limitaciones físicas de los terminales y la utilización de las estaciones base ya instaladas, sólo se pueden alcanzar velocidades máximas disponibles de 30 – 40 kbps[1]. Pero la demanda de mayor ancho de banda eran evidentes y previsibles para los servicios avanzados y en especial los que empleaban aplicaciones de multimedia (Audio, Vídeo y Datos), así que fue necesario un salto tecnológico importante, cuyo punto de partida fue el empleo de una interfaz radio de mayor capacidad. Esto es lo que en nuestros días se llama comercialmente sistemas de tercera generación (3G). En la normalización internacional estos sistemas se conocen como UMTS *(Universal Mobile Telecommunication System)* y CDMA2000 *(Code división múltiple Access 2000)*. La idea primordial de estos modelos era la de ofrecer itinerancia mundial a los usuarios, pero se han presentado algunos inconvenientes que han retrasado el proceso, ya que no se ha podido establecer un único estándar. UMTS en especial, se plantea como una solución para resolver los problemas existentes en GSM y las extensiones de las mismas, pero la tecnología de acceso empleada por estos sistemas, tanto en el interfaz radio basadas en una combinación de técnicas FDMA/TDMA *(Frequency División Múltiple Access / Time División Múltiple Access)* como la red de acceso donde se utiliza conmutación de circuitos y no de paquetes, han sido su mayor inconveniente[2].

La especificación actual de UMTS corre a cargo del foro 3GPP[3] *(Third Generation Partnership Project)*, con la participación de varios organismos de normalización regionales entre los que se encuentra ETSI *(European Telecommunications Standards Institute)*. UMTS se basa en el empleo de una interfaz radio W-CDMA *(Wideband Code División Múltiple Access)* con dos modos de

operación FDD *(Frequency División Duplex)* y TDD *(Time División Duplex)* y una tasa de transmisión de 3.84 Mchip/s; dentro de la red, en una primera fase se considera la utilización de los actuales elementos disponibles en las redes GSM y GPRS, planteándose su operación para fases posteriores. En el sistema CDMA2000, la normalización corre por cuenta del foro 3GPP2[4] *(Third Generation Partnership Project 2)* promovidos por algunos organismos de normalización norteamericanos y asiáticos. Se trata de una solución incompatible con el sistema UMTS, ya que utiliza una evolución a los sistemas CDMAone, el cual maneja una interfaz radio diferente y una tasa de transmisión de 3.6864 Mchip/s.

3. PRINCIPIOS BÁSICOS

En la actualidad se identifican dos mecanismos de seguridad, los Específicos en los que se encuentran: Cifrado, firma digital, integridad de datos, mecanismos de control de acceso , intercambios de autenticación, control del rutado, funciones de relleno de tráfico *(Traffic Padding)* entre otros y los mecanismos pervasivos los cuales no son ligados a un servicio de forma específica como la detección de eventos, etiquetas de seguridad, auditorias de seguridad y la cobertura de la seguridad entre otros. Estos tipos de mecanismos hacen referencia a los dos modelos de seguridad existentes, el de Seguridad de red y el de Seguridad de Acceso. En el primer modelo, el de red, la información se protege en el emisor por medio de algoritmos de encriptación (claves) y se transmite por un canal en donde posiblemente un individuo no autorizado puede tener acceso a la confidencialidad, sin embargo, la información inicial solamente podrá ser recuperada por el destinatario ya que es quien dispone de los mecanismos (algoritmos y claves) necesarios para deshacer las modificaciones realizadas por el emisor, en la negociación de claves entre las partes implicadas puede intervenir una tercera entidad que se podría denominar de "confianza" *(Trusted Third Party)*. En el modelo de seguridad de acceso, existe un control de admisión a la información o recursos de un sistema ante la presencia de posibles individuos no autorizados, en la mayoría de los casos se utilizan técnicas criptográficas.

Cuando se habla de criptografía, se hace una simple referencia al estudio de mecanismos de cifrado de la información que cubre básicamente dos campos: Códigos: quienes reemplazan una palabra o conjunto de ellas por otras con distinto significado y Algoritmos de Cifrado (Ciphers): cuya funcionalidad es transformar un mensaje en claro en un mensaje ininteligible a menos que se disponga de una clave o conjunto de ellas. La criptografía también se considera como una técnica de protección de la información que engloba disciplinas tales como teoría de la información, teoría de los números y complejidad algorítmica. Pero todo esto apunta hacia lo que se denomina criptoanálisis, que no es más, que el estudio de las debilidades de un sistema criptográfico llamado comúnmente criptosistema. Todo criptosistema debe cumplir la condición: $D_K(E_K(m))=m$ en donde:
E: función de cifrado
D: función de descifrado
$_K$: clave usada en el cifrado/descifrado
m: texto sin cifrar (mensaje en claro)
$E_K(m)$: mensaje cifrado
Garantizando la no perdida de la información.
Los mecanismos criptográficos se pueden caracterizar por los siguientes aspectos:
Tipología de las operaciones de cifrado utilizadas: Substitución, Transposición, Producto (combinación de las dos anteriores)
Numero de clave: Clave única o privada
Mecanismo de proceso del texto en claro: Codificadores de bloque *(block ciphers)*, Codificadores de flujo *(stream ciphers)* [5]

4. ASPECTOS DE SEGURIDAD EN GSM

El planteamiento inicial de los mecanismos de seguridad en GSM eran proporcionar a la red celular el mismo grado de seguridad que tiene la red telefónica convencional. A nivel del operador, facturar al usuario correcto, evitar fraudes y proteger el servicio y a nivel de clientes, la privacidad y el anonimato eran el objetivo primordial. En la situación actual, GSM sólo proporciona *access security*, es decir que las comunicaciones y la señalización en la red de transporte no están protegidas. La seguridad de la red GSM depende en gran medida de la seguridad de las redes a las que se conecta. La intercepción de llamadas se introdujo luego, la identidad del terminal no puede ser contrastada y existe una dificultad de actualización de los mecanismos criptográficos. De igual manera se presentan cinco tipos de ataques a las redes GSM:

1. Eavesdropping: Es la capacidad del intruso de capturar señalización o datos de los usuarios. El equipo requerido es un MS modificado
2. Suplantación de la identidad de un usuario: El equipo necesario es un terminal modificado.
3. Suplantación de red: El equipo requerido es una BTS modificada.
4. Man-in-the-middle: Se necesita una BTS y un terminal, ambos modificados
5. Robo de vectores de autenticación en la red: El intruso dispone de pares pregunta/respuesta y claves de cifrado que pudieron haberse obtenido mediante el acceso a nodos de la red o a enlaces fijos en la misma.

El orden en que se presentan los ataques está relacionado con la dificultad de realización o disponibilidad del equipo necesario, para GSM se pensó en combatir los dos primeros.

En GSM la gestión de claves es independiente del equipo, es decir que los usuarios pueden cambiar de

terminales sin comprometer la seguridad y la protección de la identidad del suscriptor es otra ventaja, pues se utilizan identificadores temporales que dificultan esta labor, por ejemplo los TMSI *(Temporary Mobile Subscriber Identity)*, que son los que proporcionan un anonimato. También el operador conoce quien está utilizando el sistema por medio de un mecanismo de autenticación de usuario, pero de igual manera existe una protección de la señalización y los datos del usuario, ya que ambos se transmiten encriptados por el canal radio[6].

En el mercado existen los GSM Mobile Station que consisten en dispositivos físicos con utilidades de identificación física y brindan un soporte a la seguridad en sistemas GSM a nivel global por medio de dispositivos de identidad internacional conocidos como IMEI *(International Mobile Equipment Identity)*. También existen módulos de identificación de suscriptores, el más común es la SIM *(Subscriber Identity Module)*, que consiste en una pequeña tarjeta que contiene llaves de acceso, identificadores y una serie de algoritmos. Dentro de los identificadores se pueden encontrar:
K_i *(Subscriber Auhtentication Key)* de 128 bits, IMSI *(International Mobile Subscriber Identity)*, TMSI *(Temporary Mobile Subscriber Identity)* MSISDN *(Mobile Station International Service Digital Network)*, PIN *(Personal identity Numbre Protecting a SIM)* y finalmente las denominadas LAI *(Location Area Identity)* que son las utilizadas por la mayoría de las redes locales.

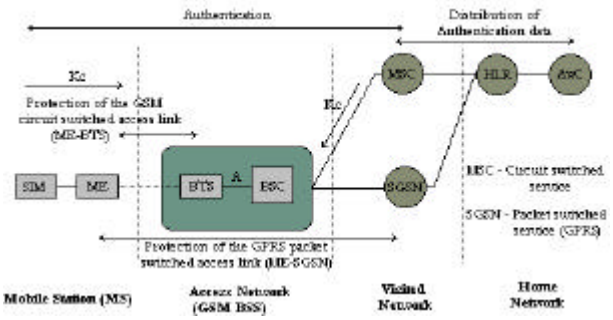

Figura 2 Autenticación y Encriptado

Obsérvese que la información en el canal radio está encriptada entre el *Mobile Equipment (ME)* y la *Base Transceiver Station (BTS)*, allí se utiliza la clave de encriptado Kc derivada durante la autenticación. La AuC *Authentication Center)* es la que proporciona los parámetros para la autenticación y encriptación (RAND, SRES, Kc), luego el HLR *(Home Location Register)* proporciona a la MSC *(Mobile Switching Center)* información con tripletas (RAND, SRES, Kc) y el VLR *(Visitor Location Register)* es quien guarda las tripletas recibidas provenientes desde el HLR cuando un usuario no se encuentra en su *Home Network*. [6]

La encriptación en GPRS presenta algunas diferencias con el encriptado de los servicios GSM en modo circuito. En GPRS la encriptación se extiende hasta el SGSN y se aplica en una capa superior de la torre de protocolos, exactamente en la capa de enlace lógico. También se presentó un nuevo algoritmo de cifrado denominado GEA *(GPRS Ecryption Algorithm)*, quien es el que genera la secuencia de cifrado en función de la clave de cifrado y del número de secuencia LLC Frame number *(Logical Link Layer)*. Vale la pena aclarar que el contador de tramas LLC es lo suficientemente largo como para evitar la repetición de la secuencia de cifrado. Los algoritmos actuales son los GEA1, GEA2 y GEA3, todos se encuentran estandarizados para que los terminales y las redes puedan operar globalmente, las especificaciones de los mismos, aún se mantienen como distribución restringida.

5. SEGURIDAD EN LA RED DE ACCESO PARA 3G

La seguridad en la red de acceso para 3G se basa en el modelo ya planteado de GSM, pero con cierta adición de servicios, como por ejemplo los mecanismos de autenticación de la red de acceso, que proporcionan una protección contra los ataques de suplantación de identidad de las estaciones base. Sin embargo los mecanismos empleados por GSM para asegurar la confidencialidad de la identidad de usuario, siguen siendo los mismos.

Confidencialidad de la identidad del usuario	**Definición**
User Indentity Confidentiality	El valor del IMSI no puede ser interceptado en el enlace radio
User Location Confidentiality	La presencia de un usuario en un área determinada no puede ser descubierta interceptado el canal radio
User Untraceability	Un intruso no puede determinar mediante la escucha del canal radio si un servicio o servicios se están ofreciendo al mismo usuario
Autenticación de las identidades	**Definición**
User Authentication	El usuario se autentica a la red
Network Authentication	La red se autentica al usuario de forma que el usuario sabe que la red de acceso está autorizada por su home operator para proporcionarle acceso a los servicios

Tabla 1 Seguridad en la red de acceso 3G

En la actualidad se han propuesto nuevos algoritmos para realizar la encriptación terminando su proceso en la RNC de la red, igualmente, la longitud de las claves se ha extendido a 128 bits y se han insertado mecanismos de integridad para autenticar el contenido de los mensajes.

* Confidencialidad:
  - Negociación del algoritmo de cifrado entre MS y la red SN *(service Network).*
  - Acuerdo mutuo en la clave de cifrado
  - Confidencialidad de los datos de usuario y de la señalización de usuario.

* Integridad:
  - Negociación del algoritmo de protección de integridad entre el MS y la red SN
  - Acuerdo mutuo en la clave del algoritmo de integridad
  - Integridad de datos y autenticación de origen en la señalización. Posibilidad de que el receptor (MS o SN) pueda confiar en que el mensaje no ha sido modificado desde su emisión y que la identidad emisora es quien realmente debe ser.

6. CONCLUSIONES

Existen importantes limitaciones en la seguridad de GSM debido al diseño propuesto inicialmente, del que ahora Colombia hace parte por empresas como Comcel y Ola Comunicaciones, Bellsouth, ahora Telefónica se comporta de manera similar, pero con especificaciones puntuales distintas, recordemos que mantienen el mismo principio de GSM:

El diseño actual sólo proporciona *access security*, las comunicaciones en la red no están protegidas por lo que se pueden presentar *Eavesdropping,* dejando parámetros de confiabilidad como la negociación del algoritmo de cifrado entre MS y la red SN (*Service Network)* al descubierto, por no establecer un acuerdo mutuo en las claves de cifrado.

El objetivo del diseño fue el de proporcionar únicamente un nivel de seguridad equivalente o igual al que poseen las redes fijas a las cuales el sistema GSM se conecta. Vale la pena destacar que en red fija el control de acceso a abonados se hace por centro de conmutación, y desde allí se enruta por medio de prefijos a la llamada entrante y saliente de acuerdo a la zona a la que corresponda, por lo que el control del flujo de información es de un porcentaje casi nulo, de lo contrario no se presentarían desvíos de llamadas e intercepción de las mismas.

Si el terminal se encuentra en un entorno no seguro, no se puede confiar o presentar a la red la identidad del mismo, sobre todo en lugares público o de fronteras, hago referencia a ésta última en el caso de no respetarse los parámetros de cobertura o de utilización de frecuencias por operadores internacionales, o en su caso en áreas de solapamiento en donde no se tiene un estricto control de potencia tanto en *Uplink* como en *Downlink* debidamente establecido.

El estándar no cubre todos los aspectos, es decir, que los operadores deben introducir mecanismos de protección de las claves de autenticación de los usuarios en la red, esto se remite a recursos compartidos o a mecanismos *wireless* en un entorno de trabajo común. Se podría acceder a una base de datos de una entidad bancaria que posea en su edificio una conexión WLAN y violar las claves que el mismo operador asigna a sus funcionarios sin necesidad de entrar a en las instalaciones, es decir que se podría burlar la seguridad desde un punto cercano si poseo una equipo con tarjeta *wireless* y un software de acceso. Luego el diseño no tiene en cuenta los ataques de forma activa, por ello, los elementos de red pueden ser suplantados o simplemente ocultos ante un administrador de red, e incluso pueden ser agregados de forma virtual en un entorno temporal bajo máscaras codificadas.

7. LECCIONES PARA FUTUROS DISEÑADORES DE RED MOVIL

La seguridad debe ofrecerse sin la ayuda del usuario, pero éste debe saber todos los acontecimientos.

Se deben desarrollar estándares internacionales, independientes de las ventajas que ofrecen los operadores.

Contemplar la posibilidad de abordar la intercepción de llamadas por ley como base de diseño, especialmente cuando se consideran soluciones no seguras extremo a extremo, como medio de verificación de trama.

Basar la seguridad del usuario en tarjetas inteligentes con único usuario y para múltiples accesos en ráfagas controladas para la autenticación de la misma.

La posibilidad de que exista un ataque es un problema para toda la red y los elementos que la componen, auque sea poco probable o se manifieste con prioridad baja, se deben tener en cuenta elementos de red fija y de canal radio, esto incluye elementos de transmisión y recepción de señal.

8. ASPECTOS IMPORTANTES

Marzo 1991. Primera implementación de GSM
Abril 1998. La asociación Smartcard Developer (SDA) junto con investigadores de la universidad de Berkeley rompieron el algoritmo COMP128 almacenado en una

SIM y obtuvieron la clave de un usuario Ki en pocas horas y descubrieron que la clave de cifrado Kc únicamente utilizaba 54 bits.
Agosto 1999. El algoritmo A5/2 fue roto en un único PC en segundos
Diciembre 1999. Alex Biryukov, Adi Shamir y David Wagner publicaron el esquema para romper el algoritmo A5/1, con dos minutos de llamada interceptada y con un tiempo de ataque de sólo 1 segundo
Mayo 2002. Investigadores de IBM descubrieron un nuevo mecanismo para extraer las claves de COMP128 de forma rápida con mecanismos colaterales[9]

De esta manera se identifican tres tipos de ataques en GSM, ataques a la SIM, de intersección del canal radio y a la red del operador.

[1] HERNANDO, José María, Comunicaciones Móviles, 751 páginas, Fundación Airtel, Madrid, 2000
[2] RAMON, Calvo Miguel, Sistemas de Comunicaciones Móviles de Tercera Generación IMT-2000 (UMTS), 630 páginas, Fundación Airtel, Madrid, 2002.
[3] Especificaciones UMTS: http://www.3gpp.org, 2004
[4] Especificaciones CDMA2000:http://www.3gpp2.org, 2004
[5] STALLINGS, Williams. Criptography and Network Security. Third Edition. Prentice may,364 páginas.2003
[6] GRAFF, Jon C. Criptografy amd E-Commerce, Second Edition, John Wiley & Sons, 227 páginas 2001