Seguridad en UMTS: independencia entre conmutación de circuitos y conmutación de paquetes

Security in UMTS: independence between circuits switching and packages switching

Gustavo Adolfo Herazo Pérez*
Héctor Arturo Flórez Fernández**

Fecha de recepción: 16 de julio del 2009
Fecha de aceptación: 27 de agosto del 2009

Resumen

El presente artículo trata de visualizar los esquemas más relevantes y complejos que se presentan en la gestión de seguridad del esquema UMTS, su dimensionamiento y las incidencias que conllevan a los problemas de intrusión y confidencialidad.

Para conocer los puntos débiles, en cuanto a resolver qué representan las decisiones que a menudo deben tomar para fortalecer los perímetros de seguridad informática, por el momento, las grandes compañías de este país tienen como prioridad establecer modelos de ingeniería social y la gestión de la seguridad aplicadas al control de puertos y servicios de red, como solución a la detección y control de intrusos internos y

* Ingeniero de Sistemas de la Universidad Autónoma de Colombia, Especialista en Sistemas Gerenciales, Telecomunicaciones Móviles de la Universidad Distrital Francisco José de Caldas, Magíster en Ingeniería de Sistemas y Computación de la Universidad de los Andes. Docente investigador de la Fundación Universitaria Konrad Lorenz. Miembro del grupo de investigación Telemente de la Fundación Universitaria Konrad Lorenz. Correo electrónico: gustavoa.herazo@fukl.edu.

** Ingeniero Electrónico e ingeniero de Sistemas de la Universidad El Bosque, especialista en Alta Gerencia de la Universidad Militar Nueva Granada, magíster en Ciencias de Información y las Comunicaciones de la Universidad Distrital Francisco José de Caldas. Docente investigador de la Fundación Universitaria Konrad Lorenz, docente de la Universidad Distrital Francisco José de Caldas. Adscrito al grupo de investigación Promente de la Fundación Universitaria Konrad Lorenz. Correo electrónico: hectora.florezf@fukl.edu.

externos en una red de alerta. Sin embargo, los patrones de seguridad que implican a la estructura de los valores de control en los canales de ancho de banda para las redes emergentes están dando un giro vertiginoso en el que participan en particular diversas pruebas de penetración con el protocolo TCP, para tener una visión clara de los alcances y la protección en el que una red se considera vulnerable.

Palabras clave: GSM Sistema Global para las Comunicaciones Móviles, UMTS Sistema Universal de telecomunicaciones Móviles, IMSI Identidad permanente en UMTS. Identidad Internacional del Abonado a un Móvil, TMSI Identidad temporal de la estación móvil en UMTS, VLR Registro de localización del visitante, SGSN Nodo de soporte de servicios GPRS

Abstract

The present article tries to visualize the most excellent schemes and complex than they appear in the management of networks TCP/IP, their sizing in the transport protocol TCP and the incidences that the troyanos intrusion problems of and virus entail to.

To know the soft spots and as to solve they represent them decisions that often must take to fortify the perimeters of computer science security. At the moment the great companies of this country, must like priority establish models of social engineering and management of security applied to control of ports and services of network, like solution to the detection and control of internal and external intruders in an alert network. Nevertheless the security patrons who entail to structure values of control in the channels of bandwidth for the emergent networks are giving a vertiginous turn that specifically involves diverse tests of penetration with protocol TCP, to have a clear vision of the reaches and protection in which a network is considered vulnerable.

Key words: GSM Global System for Movil Comunications, UMTS Universal Movil Telecomunication System, IMSI International Mobile Subscriber Identity, TMSI "Temporary Mobile Subscriber Identity, VLR Visitor Location Register, SGSN Serving GPRS Support Node.

Introducción

La problemática de la seguridad siempre ha sido un factor crítico en la evolución del marco de las telecomunicaciones, en especial, del entorno celular. Sin embargo, las nuevas generaciones de telefonía móvil celular presentan un panorama de alto costo en las nuevas incidencias de ataques y amenazas para las entrantes tecnologías del servicio de 3G UMTS.

Según investigaciones recientes, se encontró que más de la mitad de los proveedores de telefonía móvil celular manifestaron entidades malware, spam y spyware en muchos dispositivos móviles, asimismo, graves problemas en determinadas aplicaciones que afectaron las capacidades de la red. Esto conlleva a que la comunidad de desarrollo en el área móvil tendrá un costo elevado en la creación de rutinas, procedimientos y diversos parches que ayuden a enfrentar esta amenaza latente en la incursión de la era 3G UMTS. La comunidad 3G tiene grandes interrogantes con respecto a las aplicaciones de sus equipos, al Bluetooth y las conexiones a Internet.

Definitivamente, a pesar de los grandes esfuerzos de las empresas de telecomunicaciones, el impacto de la seguridad informática en la era móvil 3G está creciendo drásticamente en relación con el número de ataques y programas exploits que, de alguna manera, afectan considerablemente los procesos de comunicaciones y confidencial de los usuarios.

Actualmente, el sistema global de comunicaciones móviles (GSM), el sistema de seguridad tiene su principal foco en lo que corresponde al trayecto de radio, en otras palabras, esto equivale a las redes de acceso. Por el contrario, cuando se habla del sistema UMTS (sistema universal de telecomunicaciones móviles), el entorno de seguridad comprende de varias aéreas importantes y de sumo cuidado. Los actuales esquemas comerciales han llevado a situaciones en las que se puede enviar información privada y confidencial entre varias entidades de redes. El nuevo esquema de 3G o UMTS tiene la propiedad de integrar en un solo núcleo el esquema de todas las comunicaciones de voz y datos, apareciendo nuevas amenazas críticas que afectan este gran núcleo considerablemente.

Seguridad en el acceso a UMTS

La tecnología 3G estima que el método de acceso a radio adaptará y modificará el acceso múltiple por división de tiempo denominado TDMA y, en consecuencia, se implementará el WCDMA (acceso múltiple por división de código de banda ancha), cuando el núcleo de UMTS lidere la 3G y 3.5G. Pero, desafortunadamente, y a pesar del cambio, los estándares de seguridad seguirán siendo los mismos.

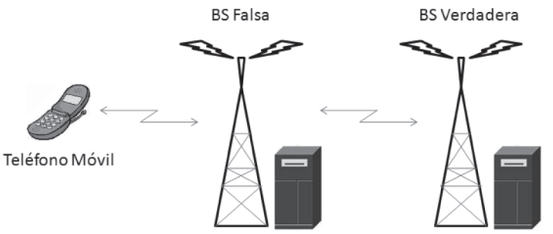
Los procesos de confidencialidad en UMTS en lo concerniente a las llamadas de voz se codifican y protegen en el tramo de la red de acceso aleatorio, denominado RAN. Se hace importante que la privacidad del paradero y ubicación del usuario, porque, por lo general, la mayor parte del tiempo si una persona está de pie no le molestaría que alguien supiera donde se encuentra en ese momento, pero si ese seguimiento fuera continuo y dinámico el usuario terminaría molestándose, y esto además se convertiría en un nuevo esquema de delincuencia y atracos para los ladrones, por tanto, la herramienta de seguridad más utilizada por los proveedores de servicios de telecomunicaciones móviles y los abonados es la criptografía.

Aunque cuando se trata de seguridad en entornos móviles, varios puntos se han heredado de la actual GSM y aunque el éxito de esta

tecnología ha arrojado luz sobre las carencias de sus controles de seguridad y entre ellos tenemos:

- En GSM, son evidentes los ataques activos contra la red, siempre y cuando se disponga del equipo necesario para suplantar o hacerse pasar por un NE (element network) que puede ser un terminal de usuario que sea legítimo o válido, como se encuentra a continuación.
- Los procesos de autentificación mutua entre el usuario y la red.
- El uso dinámico entre identidades temporales.
- El cifrado de la RAN.
- El proceso de protección de la integridad de la señalización en el interior de la red de acceso terrestre de UMTS, conocido como UTRAN.

Figura 1. Ataque activo



Autentificación mutua

En el proceso de autenticación de la red UMTS entran tres componentes que se relacionan a continuación:

- La red base.
- La red servidora (SN).
- El equipo terminal o también denominado módulo de identidad de abonado universal (USIM) compuesto en una tarjeta inteligente.

El esquema consiste en que la SN comprueba la identidad del equipo transmisor –igualmente como en la red GSM–, mediante el procedimiento conocido como: desafío Y respuesta, mientras el equipo terminal valida si la SN tiene la autenticación de la red base para hacerlo. Este protocolo de autenticación mutua no evita la situación de la figura 1, pero gracias a otros mecanismos de seguridad sí garantiza que el asaltante activo no puede sacar beneficio real de la situación, por tanto, lo único que podría conseguir el asaltante es molestar la respectiva conexión.

El esquema del mecanismo de autenticación está basado en una clave maestra *k* que comparten el USIM del usuario y la base de datos de la red base, siendo esta clave de tipo permanente y secreta con una longitud de 128 bits. Esta clave nunca es visible entre dos ubicaciones y el usuario nunca la conoce; cuando se ejecuta el proceso de autenticación mutua se generan las claves para el cifrado y seguidamente se ejecuta la comprobación de la integridad y durante el proceso se derivan claves nuevas a raíz de la clave permanente *k*.

Proceso de autenticación y acuerdo de clave (AKA)

Este procedimiento arranca después de que el usuario está validado en la SN. La validación de identificación empieza cuando se transmite la identidad del usuario presentándose cuando la identidad permanente (IMSI) o la identidad temporal (TMSI) van al registro de posiciones de visitantes (VLR) o también al nodo de soporte de servicios GPRS (SGSN), Luego el VLR o SGSN transmite la solicitud de datos de autenticación al AuC (Centro de Autenticación) de la red base.

El equipo AuC guarda las claves maestras de los usuarios y gracias al conocimiento del

Figura 2. Centro de autenticación

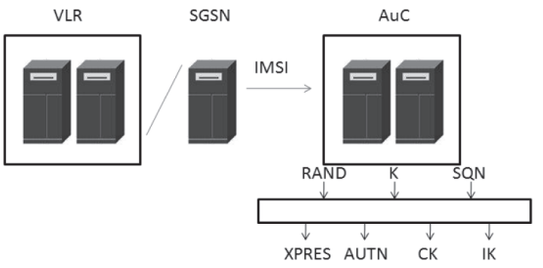
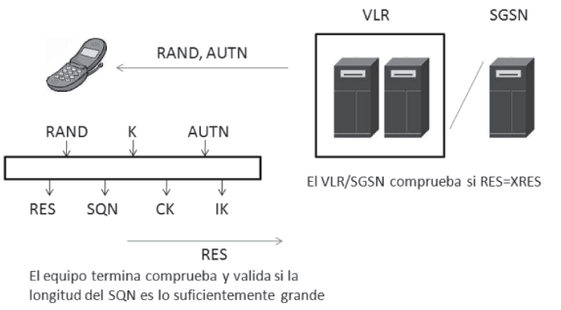


Figura 3. Proceso de autenticación



IMSI, el AuC tendrá en control para generar los vectores del usuario. Estos vectores se envían de vuelta a la base de datos del VLR/SGSN, como respuesta de autenticación. Mientras que la SN necesita un vector para cada evento de autenticación, de tal modo que la señalización no aplicaría en este caso, como por ejemplo para enlaces de larga distancia entre la SN y la base de datos del AuC.

La SN ya sea con el VLR o la SGSN, cuando transmiten la solicitud de autenticación del usuario al equipo terminal, se genera el mensaje conteniendo dos parámetros del vector previamente generado llamado RAND y AUTN, que son enviados a cualquier USIM que exista en una localidad o entorno resistente –ya sea una tarjeta de circuito integrado de la Red UMTS o UICC.

La USIM, teniendo la clave maestra y en compañía con los parámetros RAND y AUTN, procede a realizar el cálculo validando si el parámetro AUTN se generó en la AuC y si esto es verdadero, el parámetro RES se transmite de regreso al VLR/SGSN en respuesta como autenticación. Por tanto, el VLR/SGSN podría comparar la respuesta del usuario RES con la respuesta XRES esperada, que también forma parte del vector de autenticación.

Las claves respectivas para el cifrado de RAN y la protección de la integridad (CK e IK) se generan a partir de este proceso las claves temporales que están auto contenidas en el vector de autenticación y seguidamente se transmitirán al VLR/SGSN, donde se inicia y se transfiere al controlador de la red radioeléctrica llamado RNC de la RAN.

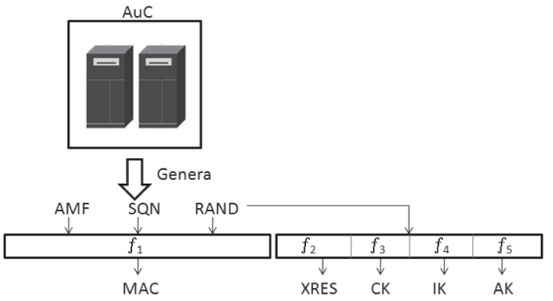
Por otro lado, la USIM empieza a calcular la clave de cifrado (CK) y su compañera IK (clave de integridad), después de generar el parámetro RAND y que AUTN lo haya validado y comprobado. Para finalizar se transmiten las claves temporales desde la USIM al celular donde se implementan el cifrado y los controles de integridad.

Perspectiva del modelo criptográfico

Este modelo visualiza la generación de los vectores de autenticación en el servidor AuC. Inicialmente, el modelo surge seleccionando un número de secuencia que sea válido y correcto, denominado SQN.

El proceso inicia con la generación del SQN; esta selección se hace en orden ascendente y su importancia radica en que dicha selección se realice de manera fresca, es decir, que no

Figura 3. Proceso de autenticación



hayan sido utilizados anteriormente; simultáneamente se dispara un proceso de generación de una cadena de bits aleatoria RAND de 128 bits.

El proceso de cálculo de estos vectores es una función matemática relativamente fácil de calcular, pero, prácticamente imposible de invertir; esto es, con los datos de entrada, que el algoritmo calcula rápidamente los datos de salida, pero si se tuviera los parámetros de salida no existe ningún programa de forma eficiente que pueda calcular los valores de entrada.

El total de funciones que se necesitan para calcular el vector de autenticación son cinco llamados f(1), f(2), f(3), f(4) y f(5). La diferencia entre las cinco funciones radica en que f(1) recibe cuatro parámetros de entrada que son los siguientes:

- La clave maestra K.
- El número aleatorio RAND.
- El número de secuencia SQN.
- El campo de gestión de autenticación AMF.

Mientras que las demás funciones solo trabajan con dos parámetros de entrada que son:
La clave maestra K.
El numero aleatorio RAND.

Todos los resultados de las funciones son excluyentes. Así el resultado de:

- F(1) = código de autenticación de mensaje (de 64 bits), llamado MAC.
- F(2) = XRES (de 32 a128 bits).
- F(3) = CK (de 128 bits).
- F(4) = IK (de 128 bits).
- F(5) = AK (de 64 bits).

El vector de autenticación está compuesto por los parámetros RAND, XRES, CK, IK y AUTN, Para la generación del parámetro AUTN se procede a concatenar tres parámetros: SQN agrega bit a bit a AK, AMF y MAC.

Proceso de autenticación del extremo USIM

Ya terminada la validación a nivel del AuC, se procede a validar el extremo USIM. Las funciones f(1) al f(5) también intervienen en este proceso, con la diferencia de que el orden varía. f(5) se debe calcular antes que f(1), ya que la función f(5) es la encargada de la no visualización y el ocultamiento del SQN.

EL resultado de f(1) se entiende como XMAC en el extremo de equipo terminal y se procede a compararlo con el MAC que recibe de la red móvil como parámetro del AUTN; si estos dos coinciden significa que RAND y AUTN han sido creados por alguna entidad que conoce la clave maestra K,

Puede existir la posibilidad de que algún hacker o cracker haya grabado una autenticación anterior y gracias a ello decida reproducir los parámetros RAND y AUTN. Para controlar esto, existe el SQN y el USIM, los cuales, sencillamente, harán la comprobación que no se ha utilizado ya el mismo SQN.

Conclusiones

Definitivamente, como resultado de que la transferencia y el uso de los vectores son acciones independientes hay varias razones para que estos se empleen en un orden diferente al orden en el que se han generado. La razón más importante es que las funciones de la gestión de la movilidad (MM) para los dominios de conmutación de circuitos (CC) y la conmutación de paquetes (CP) son independientes entre sí y esto representa el gran logro de la arquitectura UMTS. Por tal motivo, los vectores de autenticación llegan al VLR y SGSN por separado y también se utilizan de forma independiente.

Para el caso del sistema GSM, el equipo móvil se reconoce mediante su identificación personal (IMEI), pero esta identidad no está directamente asociada al usuario, porque la tarjeta SIM fácilmente puede cambiar de un teléfono a otro, sin embargo, existen algunas características importantes en la red que únicamente se basan en el valor del IMEI, y este caso se observa en las llamadas de emergencia, que los celulares no necesariamente cuenten con una tarjeta SIM, y esta arquitectura fue heredable en UMTS, dando a concluir que en ninguna de las dos plataformas (GSM y UMTS) no existe ningún mecanismo que realmente autentique de manera segura el IMEI facilitado y es por esto que los algoritmos enfocan su desarrollo en el extremo del terminal. Hay que conseguir que sea supremamente difícil modificar el terminal para que facilite el IMEI cuando la red móvil lo solicite.

Referencias bibliográficas

Eberspächer, V. Jörg, Hans, Jörg, C. Bettestetter. *GSM Switching, Services and Protocols*, 2nd ed., New York: Ed.John Wiley & Sons Ltd. 2001.

GSM 04.04. *Digital cellular telecommunications system* (Phase Layer 1; General requirements.

GSM 05.01. *Digital cellular telecommunications system* (Phase Physical layer on the radio path; General description.

UMTS Digital cellular telecommunications system (Phase Functions related to Mobile Station (MS) in idle mode and group receive mode.

European digital cellular telecommunications system; Attachment requirements for UMTS mobile stations.

Heikki Kaarannen. Network UMTS (Arquitectura, movilidad y servicios). Editorial AlfaOmega.