Seguridad en redes 4G: Wimax o LTE

¿Cuál es más segura?

Autor: Roiman Valbuena. Ingeniero en Electrónica y Telecomunicaciones

Versión: 1.0 (20130914)

http://seguridaddigitalvenezuela.blogspot.com.ar/2013/06/seguridad-en-redes-4g-wimax-o-lte-cual.html

Edición y publicación: www.segu-info.com.ar

Introducción

La Seguridad de la Información en la futura generación de Telecomunicaciones 4G, dependerá en gran medida de los esfuerzos en el desarrollo de nuevas técnicas de Encriptación, Autenticación y Codificación por parte de las corporaciones involucradas, ello sin sacrificar eficiencia y desempeño del móvil. No obstante, se estima que habrá una competencia fiera por el perfeccionamiento de tal tecnología, y más aun, por el dominio de ese mercado.

En ese sentido, Intel desarrolla los Microprocesadores para Wimax que prometen acompañar al usuario no importa donde este se desplace, y con la visión de expandir dramáticamente su experiencia en el acceso a internet. En consonancia, hace uso de la Tecnología Centrino que ha mostrado excelentes resultados de desempeño en Smartphones, PC Ultralivianos, Notebooks y Tablets. Centrino es un Microprocesador de doble núcleo soportado en una Micro-Arquitectura tecnológica de apenas 45 nanómetros.

Centrino para Wimax ha sido diseñado para que la batería del móvil alcance su máximo, esto le ha permitido redefinir la palabra eficiencia. Centrino también es compatible con la tecnología Multi-Ruta MIMO (Multiple Input – Multiple Output), mostrando excelentes resultados en pruebas experimentales. Apreciándose un bien marcado diferencial de desempeño con respecto al rango de cobertura entre celdas inalámbricas, es bueno recordar que Wimax es una Tecnología inalámbrica suficientemente madura y probada (11 años), fue diseñada para operar como LAN o MAN con un alcance superior a las 31 millas (50km) y un ancho de banda compartido de hasta 70Mbps. El nuevo Wimax Advanced permite la convergencia con redes de banda ancha e incorpora **All IP** (todo IP).

Wimax soporta múltiples tecnologías de radio acceso, los Centros de Investigaciones Tecnológicas de Motorola y Samsung han logrado producir dispositivos Inalámbricos

Multimodo que pueden operar sobre Wimax y **EVDO** (Evolution data Only). Uno de los más impactantes resultados sobre Wimax como tecnología 4G, y que ha informado el Intel Research Center, ha sido el obtenido de las pruebas preliminares en lugares con sombra entre celdas, donde los Smartphones se mantuvieron casi inalterados con respecto a su ancho de banda aun cuando la velocidad de desplazamiento superó los 200km/h, los Handoff, Handover y Softer Handoff mostraron sus mínimos históricos, así como los videos 3D en tiempo real y con gran resolución no sufrieron impacto alguno.

Por otro lado, los más agrestes competidores de Intel para redes 4G son Motorola y algunas empresas de telecomunicaciones Chinas. Motorola es una empresa que en años recientes notificó el haber completado exitosamente el paso a Time Division Dúplex Long Term Evolution (**TD-LTE**) en China, y cuyos resultados fueron avalados por el Ministerio de Industria de Información y Tecnología (MIIT) de ese país. Los resultados presentados por Motorola evidencian haber obtenido un alto desempeño tanto en sus equipos como en su plataforma, donde se destacan: picos de transferencia que superaron los 100 Mbps; demostración exitosa en pruebas de desempeño de **TD-LTE** cuyas fases incluyeron Handover – Sistemas Multitarea – Pruebas con vectores ortogonales (MIMO), Calidad de Servicio (QoS), Control de Potencia y más.

Con estas métricas, Motorola junto a China Mobile, China Telecom y China Unicom, se ubican como líderes indiscutibles en la adopción de TD-LTE para 4G y que posteriormente les permitirá hacer uso extensivo de **OFDM** (Multiplexión por División de Frecuencias Ortogonales) en sus transmisiones. En cuanto al desarrollo de 4G LTE, los ojos de los inversionistas están puestos sobre Motorola, es bueno recalcar que esta empresa posee uno de los más desarrollados centros de investigaciones en tecnología a nivel mundial, además, es dueño de las patentes de explotación comercial de tecnologías de primera generación (AMPS) y (TACS). Así como las patentes de (CDMA y CDMA-ONE- IS-95), también se le conoce por haber desarrollado **EDGE** para **GPRS** en 2G y 2,5G.

Sin embargo, y según WIPO (World Intellectual Property Organization), hasta el 2013 Motorola todavía no había presentado patentes importantes sobre LTE, en ese campo la mayoría han sido asignadas a la Corporación ZTE; a Ericsson y a Samsung. De hecho, las patentes más importantes y medulares en los sistemas de transmisión de LTE han sido concedidas a Qualcomm Corporation.

En un artículo reciente denominado: **From 2G to 4G LTE Facilitating Technology Leapfrog,** Motorola asegura que los operadores de LTE podrán entregar un mayor ancho de banda a un menor costo por bit. Incluso, sostiene que es más fácil pasar desde 2G hasta 4G sin tocar UMTS. No obstante, la batalla en el campo de la seguridad apenas comienza, si bien es cierto, ambas tecnologías son excelentes, las brechas de seguridad

sobre cada una pueden hacer tambalear su posición en el mercado. A continuación revisaremos las vulnerabilidades de cada una, preste atención a los detalles y al final del artículo saque sus propias conclusiones.

Vulnerabilidades en Wimax

Primeramente, una vulnerabilidad consiste en una falla en la seguridad de un sistema de transmisión de datos que representa un riesgo que debe corregirse, pudiendo ser usado por rivales en un ataque contra las prestaciones del mismo. En ese sentido, el establecimiento de la conexión entre una **Unidad Móvil** (**UM**) y la red Wimax usando IEEE 802.16, envuelve necesariamente la transmisión de datos sin cifrar, constituyéndose esta en una gran falla de seguridad. Los ataques **Man in The Middle** (un tipo de ataque donde un dispositivo intermedio permite interceptar y escuchar la transmisión) explotan esta vulnerabilidad a través del **Eavesdropping** (escucha secreta), permitiendo al interceptor la fabricación a gusto de sesiones de intercambio de mensajes, golpeando severamente la confiabilidad de la red.

En el ataque, el enemigo toma posesión de la transmisión haciéndosele posible el leer, cambiar o modificar parte de los mensajes transmitidos. El problema se mitigaría con el proceso de autenticación de mutua fuente, sin embargo, afectaría la calidad del servicio (QoS), su principal vulnerabilidad subyace en la interfaz de radio.

El estándar 802.16e-2005 introdujo una serie de complejos mecanismos que aseguran el radio acceso a la red empleando **Privacy and Key Management Protocol versión 2** (**PKMv2**), este brinda soporte a los mecanismos de autenticación mutua, y también introdujo **AES (Advanced Encryption Estándar)** para una interfaz aire. Aquí el proceso de autenticación mutua se ejecuta a través de un intercambio de códigos **HASH**, o lo que se denomina **Hash Based Message Autentication Code (HMAC)**, no obstante, a pesar de estos mecanismos, el ataque **Man in the Middle** sigue siendo la gran preocupación para los Analistas de Seguridad.

Para el año 2007, Andreas Deininger y algunos de sus compañeros del Laboratorio del Centro de Investigaciones KDDI R&D en Japón, informaron haber encontrado una serie de vulnerabilidades en IEEE 802.16e y sometieron a consideración del Wimax Fórum, algunas sugerencias para mitigarlas. Según ellos, el estándar 802.16e introdujo a su vez ciertas especificaciones que daban soporte a las unidades o estaciones móviles (MS), permitiendo un handover sin problemas en redes 2G y 2,5G.

No obstante, ya para **UMTS-3G**, por presentar características diferentes entre el móvil y la ahora denominada **UTRAN**, las especificaciones cambiaron. Informaron que si bien es cierto 802.16e eliminó muchas de las vulnerabilidades descubiertas en su predecesor, no

se sabe a ciencia cierta si fue que introdujo algunas nuevas, o los hackers y el negocio del Cibercrimen se volvieron más eficientes.

Ahora procederé a describir paso a paso, el proceso de establecimiento de una comunicación entre una unidad móvil (**UM**) y una estación base **BTS (Base Transceiver Station)**, no pierda detalle del sumario pues todo se produce en la interfaz de aire.

La Arquitectura de seguridad de Wimax soporta dos tipos de transmisiones dúplex, **TDD** (**Time Division Duplex**) y **FDD** (**Frequency Division Duplex**). Em ambos modelos de transmisión las conexiones son programadas usando técnicas de acceso multipameo **DL-MAP** (**Downlink Mapping**) y **UL-MAP** (**Up Link Mapping**). Debido a que la BTS envía periódicamente un mapeo de Broadcast sobre su área de cobertura, la unidad móvil hace espera del mensaje en el downlink adecuado.

Este Frame se denomina Identificador de Conexión de Alcance Inicial; I**nitial Ranging Conection Identifier** o simplemente (**CID**). Posteriormente, este identificador se asocia a un Slot de tiempo que permitirá iniciar el proceso. Paso seguido, la unidad móvil debe incrementar su potencia de transmisión con cada petición de conexión inicial hasta recibir respuesta de la BTS (Base Station Transceiver), tal proceso es muy similar a los ACK en Ethernet.

Durante el intento de conexión, el móvil busca información sobre la sincronización, la identificación del canal, el tipo de modulación, el tipo de código de corrección de errores hacia adelante, el tiempo de uso y la identificación de la radio base. Cuando la estación base responde al móvil, le incluye una petición de ajuste de conexión (sobre todo de potencia), a este proceso se le denomina **Negociación de las Condiciones Básicas de Conexión**. Como hasta el momento no se ha producido ningún tipo de autenticación, es donde los Cyber-Delincuentes aprovechan la ocasión haciendo uso de estaciones base falsas (**FAKE BTS**), estas consisten en un equipamiento electrónico capaz de simular una estación base real y cuyo proceso de autenticación permite dejar ver datos particulares y comprometedores de cada usuario.

Instalada y funcionando la BTS falsa, se produce el denominado <<**Ataque Selectivo**>>, en este paso ya los delincuentes tienen información de conexión asociada a la tarjeta SIM. Para ejecutar efectivamente el ataque, la BTS falsa debe rechazar cualquier intento de conexión de otros móviles dentro de su radio de alcance. A los atacantes les conviene estafar a la menor cantidad de usuarios posible, pero con la mayor rentabilidad, pues, se arriesgan a ser descubiertos no por la policía local del país en cuestión, sino por otros grandes grupos de Cyber Delincuentes organizados que buscan defenderse y pueden

perder parte del terreno que ocupan, debe evitarse una posible guerra entre bandas, la policía perdona la mafia no.

Para evitar que otros usuarios se autentiquen, se configura la BTS falsa con el denominado **Código de Causa de Rechazo** que presenta el error en hexadecimal **0x0C** <<**Location Update Procedure Reject**>> este código lo establece la norma **3GPP 24.008** y la norma **3GPP TSG-GRAN W4** para GPRS, funciona para las BTS de 2G y 2,5G que operan en Modo I. Estando ya el atacante enfocado hacia un solo objetivo, es entonces cuando busca apoderarse de dos parámetros básicos que le permitirán dominar a la víctima, el **International Mobile Subscriber Identity** (**IMSI**) de GSM y que forma parte de la SIM de la víctima; y el (**LAI**) **Location Area Identifier**. Habiendo obtenido ya el IMSI, este debe ser guardado en la estación base falsa, de manera que cada vez que lo desee puede interceptar sus transmisiones, ya entonces los delincuentes pueden apagar la BTS e intentar cuando sea necesario.

Este tipo de ataques es muy común en el mundo del espionaje militar, político o industrial. Si se quieren evitar, la organización de inteligencia que protege a la posible víctima tiene un equipo móvil especial, este consiste en un duplicado del móvil que se desea evitar ser interceptado más otras aplicaciones, y si espera saber si ha sido interceptada la comunicación, basta con sólo cambiar el modo de conexión a la red, bien sea del modo “A”, del modo “B”, o del “C”.

Estos modos aparecen en el Release 97 del 3GPP, se dice que se está operando en modo “A” cuando un móvil soporta operaciones simultáneas GPRS y GSM. El modo de operación clase “B” es cuando el móvil está conectado simultáneamente con ambas redes, pero sólo se le permite operar un conjunto de servicios a la vez. En el modo clase “C” el móvil solo opera los servicios GPRS. Cuando el equipo de inteligencia cambia el modo de conexión, inmediatamente se producen mensajes de error en respuesta a operaciones indebidas y que son captadas por el dispositivo especial. Pues, el móvil ha violado el proceso de negociación de conexiones básicas previamente establecido, además, las ranuras de tiempo cambian drásticamente provocando asincronía en la transmisión. De esta manera, los delincuentes quedan al descubierto.

Wimax ha demostrado también ciertas vulnerabilidades a nivel de su capa física, allí es débil ante los **Ataques de Interferencia** (**Jamming Attacks**), a estos ataques, aunque no son muy sofisticados, se les considera dentro de los ataques de denegación de servicios (**DoS**). Así como también, como un ataque de interferencia por fuerza bruta. Su objetivo consiste en aplicar la mayor cantidad de interferencia a un canal previamente identificado, se envuelve a la frecuencia central del canal con dos frecuencias más, una superior y una

inferior, ambas con al menos el doble de la potencia de la señal del canal, a esta técnica se le denomina **Intento de Hijacking por Perturbación Electrónica**.

Esta añadidura de frecuencias y potencia hace que la relación señal a ruido del canal, sea superior a la potencia de los RX y TX envueltos en la transmisión original. Como uno de los primeros pasos para el establecimiento de la conexión entre BTS y móvil es la codificación del canal, los códigos de detección de errores se activarán como no conformes, ocasionando la caída de un enlace autentico.

Explicaré ahora el proceso de autenticación, manténgase atento pues aquí la cosa se complica. 802.16e provee un mecanismo simple de autenticación por algoritmos de clave pública basado en **RSA (Rivest, Shamir y Adleman),** o un soporte de autenticación basado en **EAP (Extensible Autentication Protocol).** De este último se conocen alrededor de 38 variantes, una de las más efectivas es la EAP basada en **MD5,** consiste en un algoritmo que permite reducir formulas criptográficas y fue desarrollado por el mismo Ronald Rivest del Instituto Tecnológico de Massachusetts. RSA tiene algunas prestaciones que otros algoritmos no, por ejemplo, provee autenticación en capas altas, estas características según los analistas de riesgo, lo convierten en un modelo bastante seguro.

La seguridad y capacidad operativa de 802.11e es puesta al descubierto por Rijmen Vincent, investigador de Teorías Matemáticas para el Diseño de Criptografía Simétrica Primitiva, Rijmen fue condecorado en años anteriores y nombrado Co-Diseñador de AES. Este investigador publica un artículo denominado: **Timing Attacks on AES** (Ataques de Sincronización sobre el Estándar Avanzado de Encriptación), artículo que aparece publicado en la prestigiosa revista Hakin9 de junio de 2012.

Rijmen asegura que si bien es cierto nadie esta habilitado para desencriptar textos encriptados con AES, si el atacante tiene acceso a operaciones adicionales de AES, entonces un ataque potencial se torna realmente plausible. Lo demuestra haciendo una simple implementación en el campo de operación de Columnas Mixtas de AES. Para ello se requiere de la ejecución simultánea de programas que provean información sobre el canal, AES ha demostrado también ser débil ante ataques basados en la medición del consumo de potencia del móvil, debido a que durante el proceso de encriptación se presentan patrones electromagnéticos diferentes a los de una transmisión normal.

Para el año 2005, y luego de la presentación de 802.16e-2005, Daniel Bernstein, investigador del Departamento de Matemáticas y Estadística de la Universidad de Illinois, demostró el proceso de extracción exitosa de una clave completa AES desde un servidor de la red hacia un simple PC. Bernstein utilizó para ello ataques de sincronismo sobre la caché de AES.

Dos años más tarde, para el 2007, y posterior a algunas modificaciones en 802.16e-2005, los investigadores: Onur, Werner y Celtin, de la Universidad de Oregón; el Instituto de Información de Alemania y el Centro de Investigaciones en Seguridad de la Información del Instituto de Comercio de Estambul en Turquía respectivamente, ejecutaron experimentos sobre AES usando los mismos ataques de sincronismo sobre su caché. Los resultados del experimento mostraron evidencias concretas de haber obtenido claves secretas y completas ubicadas en criptosistemas remotos, y cuyo servidor bajo ataque operase simultáneamente multitareas y Multi-lecturas con una gran carga de trabajo. Tal como en el **Mobile Switching Center Server (MSCS) de GRPS/GSM**.

En este artículo sólo se menciona al IEEE 802.16e-2005, sin embargo existen otros más nuevos y actualizados: el IEEE 802.16-2009; el IEEE 802.16j-2009; el IEEE 802.16h-2010 y el IEEE 802-16m-2011. El lector se preguntará el porqué no se trató sobre el resto de los estándares, la respuesta es simple, con excepción del IEEE P802-16n que no se presenta en la lista y se encuentra todavía en desarrollo, el resto no incluye mejoras significativas en cuanto a la seguridad, contrariamente, introducen mayores velocidades y optimización de procesos.

El IEEE 802.16m-2011, introduce nuevas prestaciones de seguridad, el **Private Key Management 3** (**PKMv3**) es uno de ellos. Pero sigue usando esquemas vulnerables como los ya explicados, **RSA**, **AES**, y **EAP** sin variaciones de importancia. Su arquitectura de seguridad se divide ahora en dos entidades lógicas: Security Management Entity y Encription and Integrity Entity. Provee mejoras en los soportes a Femtoceldas, soporta **DL MIMO** (Downlink Multiple Input Multiple Output) en modo TDD, así como **UL MIMO** dual, TDD y FDD.

En fin, si alguien no estaba convencido o creía que Wimax era segura, espero que realmente comience a dudar. He omitido intencionalmente los siguientes procesos de transferencia de datos entre los proveedores de servicio de telefonía celular: el Key Management, proceso importante y bastante vulnerable que asigna y desasigna claves a usuarios. Además de las fallas en 802.16e en cuanto al proceso de Multi – Broadcast Service (MBS) y sus sistemas de compartición de claves entre otros. Procedamos ahora a investigar las vulnerabilidades de LTE y comparemos.

Vulnerabilidades en Long Term Evolution (LTE)

LTE presenta una interfaz de radio altamente flexible, LTE Avanzado o LTE Advanced IMT (**International Mobile Telecommunications – Advanced**), como lo denomina el 3GPP, además de ofrecer altas velocidades de transferencia, baja latencia y mayor eficiencia espectral, presenta uno de los aspectos más novedosos e interesantes de las **NGMN** (**New Generation Mobile Networks**). Y es que está basada en una arquitectura de red todo IP, a esto se le conoce como **EPC** (**Evolution Packet Core).** Esta arquitectura para LTE hereda riesgos de seguridad derivados de sus predecesoras como Wimax ya explicados, es decir, exhibe como amenazas los ataques contra los recursos de radio acceso; es vulnerable a los sofisticados ataques Man in the Middle; y se ha demostrado que es posible acceder a datos e identidades de usuarios a través del Eavesdropping.

La arquitectura de seguridad de LTE presenta 5 niveles: el primero consiste en el **Nivel de Acceso a la Red**; el segundo viene representado por la **Seguridad del Dominio de la Red**; el tercero por la **Seguridad en el Dominio del Usuario**; el cuarto por la **Seguridad en los Dominios de Aplicaciones** y el quinto consiste en un **Dominio de Seguridad Non 3GPP**. En este último, se habilita a los equipos de usuario (UE´s) (User Equipment) a tener acceso al Evolution Packet Core (EPC), usando estrategias de proveedores privados, pero que aseguren las comunicaciones por el canal en la interfaz aire.

En cuanto a los mecanismos de seguridad, LTE maneja 5 sólo en el primer nivel: el Celular Security; el Handover Security; el **IMS** (Internet Multimedia Subsystem) Security; el **HeNB** Security (Para arquitecturas Femtoceldas LTE) y el **MTM** o simplemente **M2M** (Machine 2 Machine) Security. Este último ejecuta las revisiones de seguridad cuando las transmisiones de datos se producen entre máquinas, es decir, no hay interacción con humanos.

De acuerdo al Doctor Maode Ma, Investigador destacado de la IEEE y perteneciente a la Escuela de Ingeniería Eléctrica y Electrónica del Instituto Tecnológico de Nanyang en Singapur. La seguridad a nivel del Cellular System que implica el proceso de autenticación mutua entre la unidad móvil y el EPC, al igual que en Wimax, representa uno de los esquemas de seguridad más importantes para 4G. No obstante, en esta sesión el procedimiento se lleva a cabo usando **AKA** (**Authentication and Key Agreement)** en vez de RSA. AKA consiste en un protocolo de seguridad diseñado para redes 3G, se usa para la autenticación y esta basado en criptografía simétrica.

Cuando la unidad móvil se conecta al EPC sobre E-UTRAN, el **MME** (**Mobility Management Entity**) representa al EPC y se le permite realizar una autenticación mutua con el móvil bajo el esquema dual EPC-AKA. No obstante, Fosberg et all, (2012),

aseguran que existen al menos 12 tipos de ataques conocidos que explotan esta vulnerabilidad en el proceso de autenticación entre el móvil y el MME. A continuación mencionaré sólo 4 de ellas: 1-) Amenazas contra la manipulación y control de data plana. 2-) Amenazas contra los protocolos de radio acceso. 3-) Amenazas relacionadas a los handover y 4-) Amenazas relacionadas al tracking o seguimiento de unidades móviles.

En ese mismo orden, Joe Kai y Stig Mjolsnes del Departamento de Telemática de la Universidad Noruega de Ciencia y Tecnología, afirman que el protocolo AKA presenta fallas aunque de naturaleza simbólica. Las debilidades fueron encontradas en pruebas experimentales usando un software computacional denominado **Prover CryptoVerif,** que consiste en un modelo computacional de verificación para criptografías integradas en protocolos. Debido a esta vulnerabilidad de AKA, un Insider puede hacerse pasar por un usuario autentico, y durante la ejecución del protocolo, copia la clave de sesión (**Hijacking de Sesión**) y la usa posteriormente para acceder a servicios inalámbricos en nombre del usuario real. Ataques muy comunes en sistemas UMTS-AKA y LTE-AKA.

Sin embargo, y según la National Vulnerability Database de EE.UU, en el sumario CVE-2013-1189 del año 2013, AKA ocasionó la interrupción en el servicio de un Router Cisco universal de banda ancha (aka uBR) de la serie 10.000, cuando al utilizar un módem de doble pila IPv4/IPv6, permitió a atacantes remotos provocar una denegación de servicio (recarga en el motor de enrutamiento) a través de cambios no especificados a las asignaciones de direcciones IP, también conocido como Bug ID CSCue15313. Según reporta la misma empresa Cisco System, el vector de acceso fue ubicado en una red adyacente, especificado como un ataque con nivel de complejidad medio y con clasificación 5,7. No se reportaron métricas importantes de impacto, pero provocó la denegación de servicios e interrupción de procesos.

Para el año 2011 los Investigadores: Anand; Hong; Chandramouli; Sengupta y Subbalakshmi. Investigadores del Instituto Tecnológico Stevens, y del Departamento de matemáticas y Computación de la Universidad de Nueva York, reportaron ciertas vulnerabilidades en la seguridad debido a la unión y agregación de canales (Aggregation/Bonding Channels) que produce **HSPA+** (**High Speed Data Access**) en redes LTE, estos resultados fueron publicados por **IEEE Spectrum Magazine** para el año 2011.

Según los investigadores, esta vulnerabilidad se presenta cuando, en la ejecución propia de HSPA+, se dan lugar a una gran cantidad de interrupciones del servicio debido a las métricas que relacionan a los parámetros electromagnéticos de radio acceso y la ubicación del usuario. Esta vulnerabilidad puede ser explotada por quien desee causar la interrupción del servicio. No obstante, para ejecutarlo necesitará operar en la misma banda del usuario, algo para nada complejo. De manera general, la unión de canales

(Channel Bonding) se ha utilizado como medida para mejorar el flujo de datos y ampliar el ancho de banda a los usuarios. Sin embargo, este efecto podría dar lugar a la pérdida de ortogonalidad dentro de la banda del espectro de servicio.

El **Carrier Bonding** se refiere a la combinación de bandas espectrales contiguas, por ejemplo: 2 bandas de 20MHZ cada una para proveer al usuario una sola de 40MHZ de ancho de banda. Alternativamente, el proceso implica añadir también bandas no contiguas del espectro (a esto se denomina agregación de portadoras) y que posteriormente son asignadas a un usuario. Los resultados fueron explicados usando el software Spider-Radio Workbench, habiendo demostrado la pérdida de energía de otros canales debido al efecto agregación que produce HSPA+. Para IEEE, este consistió en uno de los primeros intentos por identificar y analizar vulnerabilidades significantes sobre sistemas de Redes LTE con servicios HSPA+.

En ese sentido, la empresa T-Mobile (www.t-mobile.com), anunció el haber logrado la unión de dos canales adjuntos de 5MHZ cada uno en HSPA+, y cuyo resultado fue un canal que logró rendir la velocidad de 21Mbps, con un flujo teórico de transferencia sin experimentar que alcanzaba los 42Mbps. En fin, LTE realmente tiene riesgo que habrán de correrse en pos de alcanzar un mayor avance tecnológico, no obstante, y para concluir, explicaré a los riesgos que se enfrenta cuando acepta el 3GPP que LTE sea totalmente IP, eso conlleva el luchar contra todo lo ya conocido y lo hasta el momento desconocido. Creo realmente que una de las principales desventajas que acarreará será el tener que adoptar a IPV6, a continuación el compendiado.

Bajo el sumario de vulnerabilidad VCE-2012-0179, la National Vulnerability Database informa de una vulnerabilidad de doble liberación detectada en el proceso **tcpip.sys** sobre Microsoft Windows Server 2008 Release 2 y Service Pack 1, además de Windows 7 Gold Service Pack 1. Esta vulnerabilidad permite a usuarios locales ganar privilegios mediante una aplicación que une las direcciones IPv6 con la interfaz local AKA-TCP/IP. Su vector de acceso se considera local, implica bajo nivel de complejidad y no se requiere autenticación para explotarla. Su métrica de impacto es alta con un factor de 7,2.

Otro sumario que aporta la National Vulnerability Database, consiste en el CVE-201-0413, y cuyo nivel de impacto alcanzó el score de 7,8. Esta vulnerabilidad se presenta en los servidores que manejan **DHCPv6 (Dinamic Host Configuration Protocol versión 6),** permitiendo a los atacantes remotos causar la denegación de servicios y deteniendo los procesos **DAEMON.** Esto sucede haciendo envío de mensajes sobre IPv6 para que ciertas direcciones sean declinadas y abandonadas.

En sistemas operativos multitareas como Windows Server, un Daemon es sencillamente un programa que se ejecuta internamente, por lo general, casi todos los programas que terminan con la letra “d” son subprocesos Daemon, por ejemplo: **syslogd** y **sshd**. Cuando el atacante no conoce el sistema operativo o la plataforma bajo la cual opera el sistema víctima, procede primeramente con Windows y subsiguientemente actúa sobre los programas **ProFTPd** y el **Pure-FTPd** que corren bajo distribuciones Linux.

Tanto el ataque anterior como este, no se ejecutan sobre la interfaz aire sino sobre el Core de la red, generalmente los atacantes ejecutan pruebas experimentales basadas en simulaciones hasta lograr cierto grado de perfección, para ello existe varias herramientas de simulación, una de las más efectivas es el software **MAPS™ MAP Protocol Emulator,** MAPS = MA (Message Automation) + PS (Protocol Simulation). Este software viene predeterminado para operar simulaciones las Interfaces de Radio Acceso como sobre todas las Interfaces del Core Network de LTE.

Bibliografía

- Acnicmez, Onur; Shindler, Wender y Koc, Cetin. (2007). **Cache Based Remote Timing Attack on the AES.** Revisado el 21-06-2013. Disponible en: http://cryptocode.net/docs/c38.pdf
- Anand, S.; Hong, K.; Sengupta, S.; Subbalakshmi, K. (2011). Security Vulnerability due to Channel Aggregation/Bonding in LTE and HSPA+ Networks.
- Bernstein J, Daniel. (2005). **Cache-timing attacks on AES**. Disponible en: http://cr.yp.to/antiforgery/cachetiming-20050414.pdf Revisado el: 20-06-2013.
- Bilogrevic, Igor; Jadliwala, Murtuza y Hurbaux, Jean-Pierre. (2010). **Security Issues in Next Generation Mobile Networks: LTE and Femtocells.** Revisado el: 12-06-2013. Disponible en: http://infoscience.epfl.ch/record/149153/files/secu-LTE-femtocells-BJH-final.pdf
- Daode, Ma. (2012). **Security Investigation in 4G LTE Wireless Networks.** Revisado el: 15-06-2013. Disponible en: http://www.ieee-globecom.org/2012/private/T10F.pdf
- Deininger, Andreas; Kiyomoto, Shinsaku; Kurihara, Jur y Tanaka, Toshiaki. **Security Vulnerabilities and Solutions in Mobile WiMAX.** IJCSNS International Journal of Computer Science and Network Security, VOL.7 No.11, November 2007. Revisado el 21-06-2013. Disponible en: http://paper.ijcsns.org/07_book/200711/20071102.pdf
- Forsberg, Don; Horn, Günter; Moeller, Wolf-Dietrich y Niemi, Valtteri. (2012). **LTE Security: A Concise, Updated Guide to the 3GPP LTE Security Standarization Specifications**. Editorial Wiley & Son. EE.UU.
- Han, Tao; Zhang, Ning; Liu, Kaiming; Tang, Bihua y Liu, Yuan´an. (2008). **Analysis of Mobile WiMAX Security: Vulnerabilities and Solutions.** Revisado el: 18-06-2013. Disponible en: http://web.njit.edu/~th36/published%20paper/Analysis%20of%20Mobile%20WiMAX%20Security%20Vulnerabilities%20and%20Solutions.pdf
- Kai, Joe; Mjolsnes, Stig. (2012). **A Vulnerability in the UMTS and LTE Authentication and Key Agreement Protocols**. Revisado el: 10-06-2013. Disponible en: http://ntnu.diva-portal.org/smash/get/diva2:584129/FULLTEXT01
- Komu, Beth; Mzyece, Mjumo y Djouani, Karin. (2011). **Formal Verification of Initial Network Entry in WiMAX Networks**. Revisado el 21-06-2013. Disponible en: http://www.satnac.org.za/proceedings/2011/papers/Protocols/134.pdf
- Narayana, Prasad; Chen, Ruiming; Zhao, Yao; Chen, Yan; Fu, Zhi y Zhou, Hai. **Automatic Vulnerability Checking of IEEE 802.16 WiMAX Protocols through TLA+**. Northwestern University, Evanston IL, USA y Motorola Labs, Schaumburg IL, USA. Revisado el: 20-06-2013. Disponible en: http://www.cs.northwestern.edu/~ychen/Papers/Narayana-wimax.pdf

- Niemi, Valtteri. (2009). **3GPP security hot topics: LTE/SAE and Home (e)NB.** Revisado el 19-06-2013. Disponible en: http://docbox.etsi.org/workshop/2009/200901_securityworkshop/nokia_valtteriniemi_3gppsecurityhottopics_ltesaeandhome%28e%29nb.pdf
- **OVERVIEW OF IEEE P802.16m TECHNOLOGY AND CANDIDATE RIT FOR IMT-ADVANCED** IEEE 802.16 IMT-Advanced Evaluation Group Coordination Meeting 13 January 2010. La Jolla, CA, USA. Revisado el: 20-06-2013. Disponible en: http://www.ieee802.org/16/liaison/docs/L80216-10_0002.pdf
- Parish, D.J. y Aparicio-Navarro, J. (2010). **Misbehaviour metrics in WiMAX networks under Attack.** Revisado el 21-06-2013. Disponible en: http://www.cms.livjm.ac.uk/pgnet2010/MakeCD/Papers/2010018.pdf
- Taha, Abd-Elhamid; Ali, Najah Abu y Hassanein, Hossan. (2011). LTE, LTE-Advanced and Wimax: A Consice Introduction to IMT-Advanced Systems Including LTE-Advanced and Wimax. Editorial John Wiley & Son. EE.UU.