Middleware de seguridad para el interworking WLAN-IMS

Security middleware for IMS-WLAN interworking

Oscar Caicedo[*]*, Edgar De La Cruz, Geovanni Taimal*

GIT, Universidad del Cauca, Calle 5ª N.° 4-70, Popayán, Colombia

(Recibido el 4 de abril de 2009. Aceptado el 20 de abril de 2010)

Resumen

El 3GPP plantea una arquitectura de seguridad para el *interworking* WLAN-3GPP, sin embargo ésta presenta ineficiencias en el procedimiento de autenticación, lo que produce un mayor: consumo de recursos de radio, procesamiento en los dispositivos y retardo en la autenticación. Debido a esto, en este artículo se propone un *middleware* de seguridad que reduce los pasos en la autenticación del *interworking* WLAN-3GPP y asegura la señalización SIP entre el equipo de usuario (UE, *User Equipment*) y el *Proxy* CSCF (P-CSCF, Proxy - Call State Control Function) del subsistema multimedia IP (IMS, *IP Multimedia Subsystem*).

----- *Palabras clave:* Autenticación, confidencialidad, IMS, integridad, *interworking*, seguridad, WLAN

Abstract

The 3GPP proposes security architecture for Interworking WLAN-3GPP. However, it presents inefficiencies in the authentication procedure, which bring a greater consumption of radio resources, processing on the devices and delayed authentication. Due to previous reasons, we propose a security middleware that reduces the steps in the authentication of the WLAN-3GPP interworking and ensures the SIP signaling between the user equipment and the first entry point to the IMS network (P-CSCF).

----- *Keywords:* Authentication, confidentiality, IMS, integrity, interworking, security, WLAN

* Autor de correspondencia: teléfono: + 57 + 2 + 820 98 00 ext. 2127, fax + 57 + 2 820 98 10, correo electrónico: omcaicedo@unicauca.edu.co. (O. Caicedo)

Introducción

La convergencia de redes planteada por IMS se orienta a facilitar la prestación de servicios desde una plataforma única para los distintos tipos de red de acceso (AN, *Access Network*). En esta vía, un caso importante y prometedor para el mercado de las telecomunicaciones es la integración de las redes inalámbricas de área local (WLAN, *Wireless Local Area Network*) con las redes móviles, lo que permite a las últimas brindar servicios en el ambiente de las primeras, pero con mayor contenido multimedia [1]. Sin embargo, poner todo el tráfico (señalización y servicios) de IMS sobre un núcleo de red IP en un ambiente inalámbrico genera vulnerabilidades, subsanables con tecnologías y arquitecturas que permiten incrementar los niveles de seguridad [2].

El 3GPP (3GPP, 3rd *Generation Partnership Project*) propone en [3] la arquitectura de seguridad para IMS, la cual define esquemas para la gestión de integridad, confidencialidad y autenticación, en esta red y consta de cinco partes que garantizan seguridad en distintos puntos de IMS. Los dos primeros permiten asegurar la comunicación entre el UE y el P-CSCF; los demás puntos hacen referencia a la protección entre entidades internas de una red IMS o entre redes IMS de distintos operadores.

El modelo de autenticación propuesto por el 3GPP, para soportar seguridad en un ambiente 3GPP-WLAN, estipula que para acceder a IMS se debe ejecutar el protocolo de autenticación y acuerdo de llaves (AKA, *Authentication and Key Agreement*) [4] en cada uno de los dominios del *interworking* WLAN-IMS (WLAN, 3G e IMS), lo que introduce sobrecarga a la red debido al intercambio de múltiples mensajes redundantes, causantes de [5-8]: retardo en la autenticación del usuario, aumento en el consumo de recursos de radio y mayor procesamiento de los dispositivos. Para solucionar los problemas mencionados, en este artículo se propone un *middleware* de seguridad que reduce los pasos en la autenticación del *interworking* WLAN-IMS, asegura la señalización SIP entre el UE y el P-CSCF, e implementa los dos primeros puntos de la arquitectura de seguridad planteada por el 3GPP para IMS. El *middleware* se validó en un ambiente WiFi-IMS, se eligió como WLAN una red WiFi debido a su amplia difusión y a que presenta gran cantidad de fallos de seguridad.

Estado actual del conocimiento

Propuesta de arquitectura de seguridad 3GPP-WLAN definida por el 3GPP

La propuesta presentada en [3, 9] específica que un usuario WLAN debe acceder a los servicios IMS ejecutando el procedimiento de autenticación AKA de manera independiente para cada uno de los dominios WLAN, 3G e IMS: *i) Autenticación al dominio WLAN.* El UE y la WLAN se autentican uno al otro usando el protocolo de autenticación extensible-AKA (EAP-AKA, *Extensible Authentication Protocol*-AKA) [10,11]. *ii) Autenticación al dominio 3G.* En este caso se ejecuta el protocolo de intercambio de llaves (IKE, *Internet Key Exchange*) [12], el cual permite la autenticación mutua entre el UE y la pasarela de paquetes de datos (PDG, *Packet Data Gateway*), y el establecimiento de una asociación bidireccional de seguridad para la ejecución del protocolo EAP-AKA. También, utiliza certificados para la autenticación del PDG lo cual implica el despliegue de una PKI y un mayor procesamiento para el UE. *iii) Autenticación al dominio IMS.* Previo registro del usuario en el dominio IMS se autentican mutuamente el UE y el *Serving*-CSCF (S-CSCF), con el fin de obtener un enlace seguro en el punto de referencia Gm [13]. El procedimiento de autenticación por ejecutarse es IMS-AKA, el cual encapsula los mensajes AKA sobre la señalización SIP. La ejecución de los tres procedimientos AKA tiene un impacto adverso en la calidad de servicio (QoS, Quality of Service) ofrecida a los usuarios finales. Por esta razón, surgieron las siguientes propuestas.

Propuesta de autenticación SIP-Digest-AKA

En [8] se plantea migrar la funcionalidad de autenticación de capa 2 (802.1x/ EAP-AKA) al nivel de servicio (SIP-Digest-AKA) implementando la confidencialidad y el control de acceso en la capa IP a través de IPsec. De esta forma, con un solo proceso de autenticación se disminuye el retardo y con la migración de capa se proporciona mayor flexibilidad para la configuración a nivel de acceso. Esta propuesta tiene como principal aporte con respecto al sistema planteado por el 3GPP, un nuevo dispositivo (WLAN P-CSCF) en la AN con capacidades SIP, implementación de IPsec y control de acceso, que hace uso de filtrado de paquetes. Así, solo usuarios autenticados correctamente son dotados de conectividad IP, mientras que para usuarios no autenticados la única comunicación permitida es la conducente a realizar autenticación. Los principales problemas de [8] radican en que: i) la autenticación SIP-Digest-AKA no garantiza seguridad para la señalización entre el WLAN P-CSCF y la red IMS. ii) No tiene en cuenta en el proceso de registro a las entidades pasarela de acceso WLAN (WAG, *WLAN Access Gateway*) y PDG, por lo que requiere un intercambio adicional de mensajes para notificarles el resultado del proceso [5].

Propuesta de autenticación EAP-AKA (tres pasos)

La propuesta presentada en [6, 7] consiste en un solo proceso de autenticación AKA conformado por 3 pasos que dependen de la autenticación a la WLAN, lo cual representa su mayor debilidad ya que se debe repetir con cada *hand-off*. i) Primer paso, el usuario y la WLAN se autentican mutuamente ejecutando EAP-AKA. Además, el usuario y el servidor de autenticación generan y almacenan una llave maestra (MK, *master key*). ii) Segundo paso, el usuario es autenticado en el dominio 3G ejecutando IKE que omite la encapsulación de EAP-AKA, así, la autenticación entre el UE y la PDG está basada en la MK. iii) El tercer paso elimina la necesidad de ejecutar IMS-AKA para registrarse al dominio IMS, lo que resulta en menos procesamiento al disminuir el intercambio de mensajes y autenticaciones. La falta de autenticación del usuario por parte de IMS no implica un riesgo de seguridad, ya que el dominio 3G ha sido autenticado en pasos previos. Esta solución reduce la sobrecarga de las tres autenticaciones y soporta su seguridad en la privacidad de la llave MK.

Propuesta de autenticación EAP-AKA (un paso)

La solución presentada en [5] escoge la capa 2 para autenticación, principalmente por la escalabilidad del protocolo EAP, puesto que si una posible debilidad es encontrada en uno de los métodos de autenticación o en un algoritmo específico de integridad, éste podría ser fácil y rápidamente modificado. Provee una autenticación unificada, adicionando un nuevo encabezado en el mensaje EAP por medio del cual, el usuario puede escoger los servicios de la red que desea acceder y el nivel de seguridad con que lo quiere hacer. Sus principales desventajas son no considerar las entidades pertenecientes a IMS (por lo cual no establece un túnel seguro entre el UE y el P-CSCF), y como la anterior propuesta, repetirse con cada *hand-off*.

MidSEG

Características

- MidSEG trabaja en el escenario tres del *interworking* WLAN-IMS [13,14], de este modo, tiene en cuenta aspectos relacionados con la seguridad y el acceso a servicios IMS.
- MidSEG utiliza AKA, debido a que éste: i) Permite la deducción de las claves de integridad y de cifrado, y proporciona autenticación mutua entre el UE y el núcleo IMS. ii) Utiliza números de secuencia y contadores para evitar repeticiones en los datos de autenticación. iii) Es la recomendación del 3GPP para la autenticación de entidades móviles.

- MidSEG permite reutilizar la autenticación a IMS en cada una de las entidades encargadas del control de acceso de cada dominio (WLAN, 3G e IMS), reduciendo los tres procesos de autenticación propuestos por el 3GPP a uno solo, así se disminuye: el tráfico de registro y el consumo de recursos tanto de red como de procesamiento. La unificación de la autenticación en el nivel de servicio trae como ventaja que la seguridad en la comunicación establecida entre el UE y la red IMS se independiza de la AN.
- La seguridad en sistemas inalámbricos tiene factores adicionales de riesgo ya que cualquiera puede tener acceso al medio de trasmisión y a su vez a la información transportada, además con la ayuda de antenas los ataques pueden ser realizados a grandes distancias, eliminando cualquier rastro físico. Con el objetivo de evitar este tipo de violaciones de seguridad, MidSEG cuenta con un subsistema de seguridad especial para la WLAN (SSW, *Subsystem Security WLAN*), encargado de garantizar confidencialidad e integridad de la señalización sobre la interfaz inalámbrica.
- Para asegurar la señalización hasta el dominio IMS, MidSEG cuenta con túneles de seguridad configurados entre el SSW y el subsistema de seguridad P-CSCF (SSP, *Subsystem Security P-CSCF*), el SSP se ubica como punto de entrada al núcleo IMS.
- Teniendo en cuenta que en cada uno de los seis escenarios descritos en [8] se define de forma incremental distintos aspectos para lograr un completo *interworking* WLAN-3GPP, se optó por trabajar con MidSEG en el escenario tres, debido a que trata aspectos como: i) El acceso a los servicios de PSS. ii) El acceso a los servicios de la AN. iii) La reutilización del mecanismo de autenticación 3GPP. De este modo, se incluyen en MidSEG aspectos asociados a: autenticación mutua, autorización a los servicios y el establecimiento de asociaciones de seguridad entre el UE y el P-CSCF.

Requisitos de la solución

- Controlar el acceso de paquetes a los dominios WLAN e IMS. MidSEG protege las entidades de la red contra abusos y permite tráfico diferente al registro, únicamente a usuarios registrados. Esta funcionalidad debe estar presente en cada uno de los tres dominios del *interworking* WLAN-IMS teniendo en cuenta que se pueden ofrecer servicios de distinto tipo.
- Permitir al UE registrarse a la red WLAN, 3GPP o IMS. MidSEG permite que: i) El usuario escoja el tipo de acceso y use los servicios a libre albedrio. ii) El operador realice una diferenciación de usuarios y ejecute el respectivo control de acceso.
- Obtener los desafíos que permitan al UE autenticar las redes WLAN, 3GPP e IMS. MidSEG evita que terceros suplanten a una o a todas las redes.
- Unificar la autenticación del UE en los dominios WLAN, 3GPP e IMS. Reutilizando la autenticación realizada por el núcleo IMS, MidSEG evita la suplantación de un usuario legítimo, es decir garantiza que la comunicación de la red es con el usuario apropiado.
- Actualizar el estado del usuario. MidSEG modifica el HSS como resultado de un registro satisfactorio con el fin de habilitar los servicios configurados en su perfil, de la misma forma notifica a la red cuando un usuario sale del sistema.
- Validar la integridad de los datos. MidSEG garantiza la integridad en la comunicación establecida entre el UE y el P-CSCF, así evita que alguien ajeno a la comunicación modifique, inserte o elimine información de acuerdo a su conveniencia.
- Cifrar la señalización. MidSEG garantiza la confidencialidad en la comunicación entre el UE y el P-CSCF. Cada usuario, al momento de registrarse, obtiene unas llaves

de cifrado que permiten el establecimiento de asociaciones de seguridad, las cuales garantizan la privacidad en la comunicación y evitan que información confidencial llegue a manos erróneas.

Arquitectura de referencia

Las funcionalidades de MidSEG se encuentran repartidas en los tres subsistemas mostrados en la figura 1 Arquitectura de referencia de MidSEG.

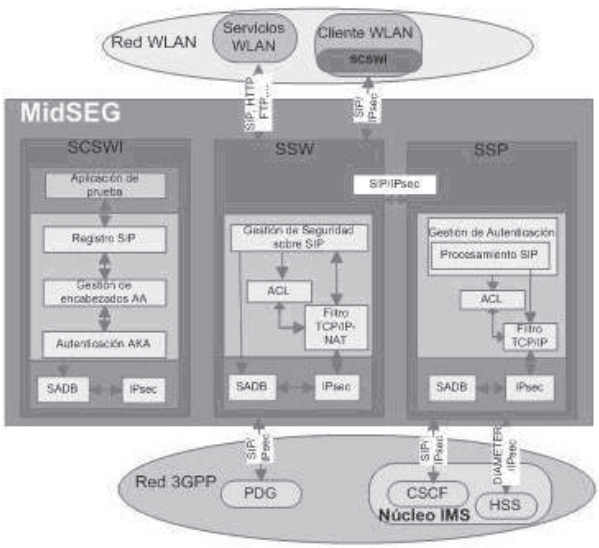

Figura 1 Arquitectura de referencia de MidSEG

SCSWI (Subsystem Client Security WLAN - IMS)

Se localiza en el UE y sus funciones son: i) Registrar el UE en los diferentes dominios (WLAN, 3GPP e IMS) que elija el usuario. ii) Autenticar a la red IMS. iii) Deducir las llaves de cifrado (CK, *Cipher key*) e integridad (IK, *Integrity Key*). iv) Establecer SA con el SSW. v) Utilizar SIP como protocolo de transporte de AKA. vi) Permitir la configuración de seguridad de la interfaz de radio.

Capa de aplicación

- *Aplicación de prueba:* en ella: i) El usuario puede iniciar el procedimiento de registro eligiendo a qué dominio quiere acceder y configurando la seguridad que requiere sobre la interfaz de radio. ii) Se informa el estado del proceso de registro.

Capa de Control

- *Registro SIP:* se encarga de retirar y adicionar los encabezados de autorización, autenticación y acceso, necesarios para el registro.
- *Gestión de encabezados AA (authentication, authorization):* construye los encabezados de acceso y de autenticación, basándose en la selección de los dominios y en el proceso de autenticación AKA, respectivamente. Además, entrega los parámetros necesarios para ejecutar la autenticación AKA a partir del encabezado SIP de autorización enviado por el S-CSCF, y provee las direcciones IP con las cuales el UE se puede comunicar con cada dominio**.**
- *Autenticación AKA:* se encarga de verificar la identidad de la red por medio del mecanismo AKA utilizando los algoritmos Milenage [15], comprueba la integridad del mensaje y la sincronización con el servidor de autenticación para evitar ataques por réplica de paquetes, además genera las llaves de cifrado e integridad (las cuales son utilizadas en IPsec) y una respuesta al desafío utilizando parámetros de seguridad como la llave compartida, un número de secuencia y un número aleatorio encontrado en el desafío.

Capa de transporte

- *SADB (Security Association Database):* aquí se configuran todos los parámetros de las SA de la base de datos de IPsec, entre los que se encuentran las direcciones IP de las entidades involucradas en la comunicación, las llaves y las políticas de seguridad que se aplicarán haciendo uso de las SA establecidas.

- *IPsec:* actúa sobre la capa de red lo que permite asegurar las comunicaciones sobre el protocolo IP y las capas superiores. Además, obtiene de la SADB las políticas con las cuales opera para proveer confidencialidad e integridad en la comunicación con el SSW.

SSW (Subsystem Security WLAN)

Cumple con las siguientes funciones: i) Controlar el acceso a la WLAN, la red IMS y la red 3GPP. ii) Establecer SA con el SCSWI, el PDG y el SSP.

Capa de control

- *Gestión de Seguridad sobre SIP:* procesa únicamente los mensajes SIP involucrados en el procedimiento de registro, del mensaje inicial SIP REGISTER del UE obtiene la dirección IP y los algoritmos de encapsulamiento seguro de la carga útil (ESP [16], *Encapsulating Security Payload*), para la configuración de IPsec; del mensaje SIP NO-AUTHORIZATION enviado por el SSP retira las llaves de CK e IK, para luego actualizar la SA IPsec de la señalización de registro; del mensaje SIP OK obtiene la autorización enviada por el SSP, para el acceso a los dominios, la configuración de la lista de control de acceso (ACL) y el establecimiento de nuevas SA para cada dominio registrado. Al mensaje SIP OK que envía al UE le agrega las direcciones IP con las cuales éste puede alcanzar los dominios requeridos. Las SA del último registro exitoso se mantienen hasta obtener las nuevas llaves de CK e IK que permiten establecer nuevas SA, lo que brinda mayor seguridad a solicitudes posteriores.

  En el caso de una solicitud de des-registro por parte del usuario, cuando llega la confirmación por parte del SSP con el mensaje SIP OK, configura la ACL para bloquear el tráfico, de este modo solo los mensajes REGISTER enviados desde el UE serán procesados.

- *ACL:* establece los permisos con los cuales trabaja el Filtro TCP/IP-NAT que da acceso a los dominios WLAN, 3GPP e IMS.

Capa de transporte

- *Filtro TCP/IP–NAT:* su objetivo es filtrar tráfico de acuerdo con la ACL y, si es necesario, hacer traducción de direcciones de red (NAT, *Network Address Translation*). Para usuarios no registrados, el filtro está configurado para permitir únicamente tráfico dirigido al puerto por el que escucha la señalización SIP, y para usuarios registrados el filtro permite el reenvío de paquetes a los dominios autorizados utilizando el NAT.
- *SADB:* descrito en el anterior subsistema.
- *IPsec:* actúa sobre la capa de red permitiendo asegurar las comunicaciones sobre el protocolo IP, estableciendo SA con el SCSWI y el SSP. De la SADB obtiene sus políticas de operación, para proveer confidencialidad e integridad en la comunicación.

SSP (Subsystem Security P-CSCF)

Es el punto de entrada al dominio IMS y se encarga de: i) Establecer el control de acceso a los diferentes SSW. ii) Procesar los mensajes SIP entrantes. iii) Mantener temporalmente los dominios por registrar. iv) Acceder al HSS para recuperar las llaves de CK e IK que necesita enviar al SSW. v) Actualizar los dominios en los cuales el cliente WLAN fue registrado en el HSS.

Capa de control

- *Gestión de Autenticación:* gestiona los encabezados SIP adicionales, mantiene temporalmente los dominios en los cuales el usuario quiere registrarse, agrega un encabezado con las CK e IK, las cuales se usan en el túnel IPsec entre el SCSWI y el SSW. Solicita del HSS las CK e IK y actualiza los dominios en los que se registró satisfactoriamente el UE.
- *ACL:* descrito previamente.

Capa de transporte

- *Filtro TCP/IP:* su objetivo es filtrar tráfico de acuerdo con la ACL, la cual se configura para permitir únicamente la comunicación con los SSW con los que se han establecido acuerdos.
- *IPsec:* permite establecer SA con el SSW, con el fin de garantizar confidencialidad e integridad en la comunicación

Definición de las interfaces entre los subsistemas

- *SCSWI – SSW.* Con el fin de establecer las SA de la interfaz IPsec utilizada en la comunicación entre estos dos subsistemas, el SCSWI y el SSW obtienen las llaves CK e IK, de la ejecución del procedimiento AKA y del mensaje NO-ATHORIZATION enviado por el SSP, respectivamente.
- *SSW – SSP.* Estos dos subsistemas también se encuentran unidos a través de una interfaz de comunicación IPsec, la cual utiliza IKE para el establecimiento dinámico de las SA. Su seguridad es fundamental ya que el SSP envía a través de ella las CK e IK con el fin de establecer la interfaz SCSWI – SSW.

  Las interfaces SCWI-SSW, SSW-SSP, junto con el filtro configurado en el SSP garantizan la confidencialidad e integridad de la comunicación entre el UE y el P-CSCF ya que los subsistemas intermedios son autenticados y utilizan conexiones IPsec dinámicas, la primera por medio de AKA-SIP y la segunda con IKE.
- *Interfaz SIP, HTTP, FTP, etc.* Hace referencia a la comunicación que tiene el SSW con los servicios prestados por la WLAN, los cuales únicamente son alcanzables por un usuario autenticado a través del SSW.
- *SSP-CSCF.* Habilita al SSP para manejar señalización SIP, lo que le permite interactuar con el P-CSCF. Es asegurada con el establecimiento de una interfaz IPsec.
- *SSP-HSS.* Permite al SSP interactuar con el HSS, con el fin de solicitar las CK e IK de un usuario y actualizar el registro a los dominios WLAN, 3GPP e IMS. Se asegura con el establecimiento de una interfaz IPsec.

Implementación de referencia

En la figura 2 Modelo de Implantación del Sistema, se puede ver el prototipo de MidSEG:

- Usuario, el cual conoce la llave compartida y la configuración necesaria para acceder a la red IMS que gestiona su registro a los dominios de red.
- UE que contiene al SCSWI, se implantó en un equipo con las siguientes características: SO Ubuntu 8.04, jdk-1.6, jain-sip 1.2 [17], ipsec-tools R0.7.1 [18], y tarjeta para la conexión WLAN.
- AP WLAN que permite la conexión inalámbrica con el UE. Se realizaron pruebas con un AP Linksys modelo WAP54G utilizando WEP, WPA y sin seguridad.
- Servidor Middleware de Seguridad WLAN que contiene al SSW, se implantó en un equipo con las siguientes características: SO Ubuntu 8.04, jdk-1.6, jain-sip 1.2, ipsec-tools R0.7.1, mysql-server 5.0.51a, mysql-connector-java-3.1.12-bin, ip-tables 1.3.8 [19] y tres interfaces Ethernet de comunicación. Es el único camino físico que tiene el AP para alcanzar los servicios de la WLAN e IMS.
- IPv4: nube que representa las redes IP que se encuentran entre IMS-WLAN. Correspondió tanto a la *intranet* como la *extranet* de la Universidad del Cauca.
- Servidor Middleware de Seguridad P-CSCF, equipo de red con las siguientes características SO Kubuntu 8.04, jdk-1.6, jain-sip 1.2, ipsec-tools R0.7.1, mysql-connector-java-3.1.12-bin, ip-tables 1.3.8, racoon [20] y dos interfaces Ethernet de comunicación. Contiene al SSP, es el único

camino por el cual un SMSW puede alcanzar el núcleo IMS.

- Red IMS, simulada con el OpenIMSCoreKDE2008-12-08.r608 [21]. El servidor de implantación tiene las siguientes características: SO Kubuntu 8.04, jdk-1.6, ipsec-tools R0.7.1, mysql-server 5.0.51a, racoon, bind9 1:9.4.2 [22], y una interfaz de comunicación Ethernet.

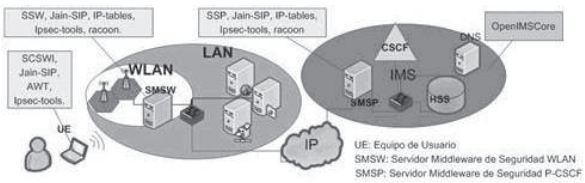

Figura 2 Modelo de Implantación del Sistema

Experimentación

Seguridad

Para la elaboración de las pruebas se definió el escenario de la figura 3 Ambiente de evaluación de MidSEG y se siguió la OSSTMM (OSSTMM, *Open-Source Security Testing Methodology Manual*) [23]. A continuación se presentan los resultados de las pruebas realizadas y su respectivo análisis.

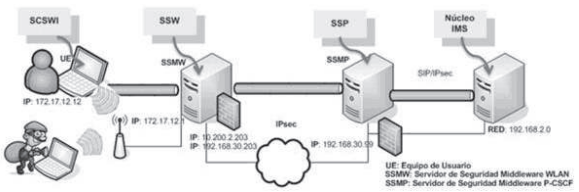

Figura 3 Ambiente de evaluación de MidSEG

- *Controlar el acceso de paquetes a los dominios WLAN e IMS***.** Si un usuario no registrado desea acceder a Internet desde la WLAN a través de IMS no lo puede hacer, porque el *firewall* que define MidSEG en el SSW se lo impide, ya que el reenvío de paquetes por defecto tiene la política de denegar todos los paquetes. Únicamente si el usuario se registra exitosamente el *firewall* se modifica automáticamente para permitirle acceder a los servicios de los dominios elegidos. Si un atacante utiliza la dirección IP de alguien que está registrado, no puede acceder a las autorizaciones otorgadas al cliente WLAN registrado, debido a que existe un túnel IPsec entre el cliente WLAN y el SSW por lo que a cada paquete que llega al SSW se le verifica su integridad y su confidencialidad con las respectivas SA. Para que el atacante tenga éxito debería conocer las SA, las cuales cambian con cada registro.

- *Validar la integridad y confidencialidad de los datos para garantizar la seguridad en la comunicación establecida entre el UE y el P-CSCF***.** Sin el uso de IPsec, se comprueba que la confidencialidad y la privacidad de la señalización IMS puede ser fácilmente vulnerada, ver figura 4 Señalización sin uso de MidSEG, ya que ésta viaja en texto plano, razón por la cual puede ser interceptada por alguien que use un analizador de protocolos como *Wireshark* [24]. Para solventar ésta vulnerabilidad MidSEG protege la señalización SIP por medio de IPsec que utiliza el protocolo ESP para proporcionar confidencialidad e integridad. Ver figura 5 Señalización utilizando MidSEG.

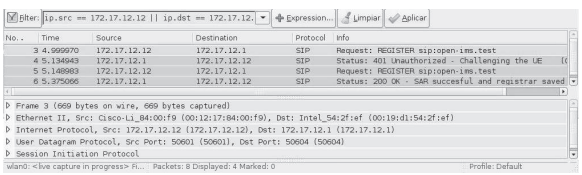

Figura 4 Señalización sin uso de MidSEG

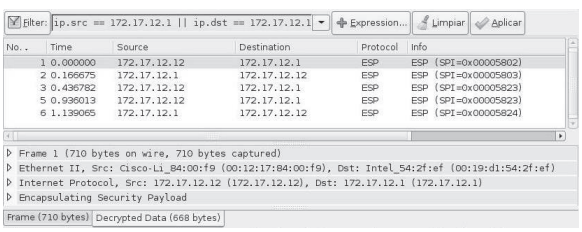

Figura 5 Señalización utilizando MidSEG

- *Evaluar la seguridad de MidSEG en la WLAN*. Se realizó con el fin de verificar la seguridad prestada por MidSEG en los paquetes de la interfaz inalámbrica. Para esto se utilizó la herramienta CommView for WiFi 6.1 [25], la cual permite analizar el tráfico inalámbrico sin estar conectado directamente a un AP. Se capturaron paquetes de un AP configurado sin seguridad, que es el peor de los casos en 802.11 y se obtuvo que ningún paquete puede ser descifrado debido al uso de IPsec (figura 6 Captura de paquetes con y sin la seguridad inalámbrica de MidSEG). También es importante señalar que las llaves utilizadas en las SA entre MidSEG y el SCSWI son diferentes para cada usuario y son renovadas con cada autenticación, por lo que los usuarios que estén conectados al mismo AP no pueden acceder al tráfico de los demás.

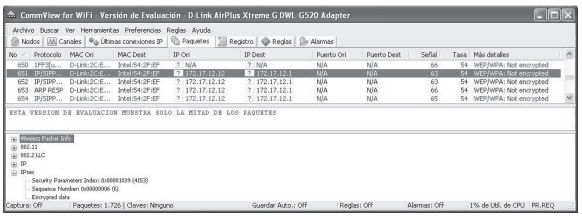

Figura 6 Captura de paquetes con y sin la seguridad inalámbrica de MidSEG

- *Evaluar el establecimiento de sesiones para el servicio de VoIP utilizando MidSEG*. La prueba consistió en registrar dos usuarios a través de MidSEG, con lo cual se estableció la seguridad en la comunicación entre cada UE y el P-CSCF, posteriormente uno de los usuarios realizó una llamada al otro usando el cliente IMS OpenICLite, de esta forma se verificó el establecimiento de una sesión SIP, la seguridad prestada por MidSEG, el correcto funcionamiento del servicio y la independencia de MidSEG.

Rendimiento

Tiempos de registro del SCSWI con y sin seguridad. Primero se llevo a cabo la sin seguridad, ésta se repitió cien veces y se obtuvo un promedio de 265,9 milisegundos para el proceso de registro. Posteriormente se efectuó la prueba con el SCSWI, que en el proceso de registro, hace dos solicitudes SIP REGISTER y obtiene las respuestas SIP UNAUTHORIZED y SIP OK, lo que equivale a dos viajes de ida y vuelta (RTT, *Round-Trip Time*). De esta forma, se obtuvo un tiempo total de registro de 532,9 milisegundos y un RTT promedio de 266,45, valor superior al obtenido sin el MidSEG pero por debajo del umbral correspondiente para este parámetro (500ms) [26].

Conclusiones y trabajos futuros

- La confidencialidad e integridad en la señalización SIP prestada por MidSEG es alta debido a que utiliza IPsec ESP con autenticación, la cual no ha sido a vulnerada.
- La seguridad de MidSEG es escalable, ya que ante posibles vulnerabilidades encontradas en el algoritmo de cifrado y/o de autenticación utilizado en IPsec, éste puede ser cambiado.
- Utilizar IPsec garantiza la confidencialidad e integridad en los datos de protocolos pertenecientes a capas superiores a IP, lo que hace que MidSEG sea una solución independiente de las aplicaciones. Esto permite que todo el tráfico en la interfaz inalámbrica sea cifrado.
- La unión del Filtro TCP/IP con las políticas de seguridad de IPsec garantiza el acceso a los dominios 3GPP, WLAN e IMS, únicamente a los usuarios que están autorizados y autenticados.
- La implementación de referencia de MidSEG es independiente de la tecnología de acceso debido a que la autenticación se trasladó al nivel de servicio.
- Unificar la autenticación a los dominios WLAN, 3GPP e IMS permite reducir: el consumo de recursos de radio y el procesamiento en los dispositivos y el retardo global en el proceso de autenticación.

- MidSEG aprovecha las SA establecidas entre los clientes y el servidor SMSW para garantizar la confiabilidad e integridad del tráfico entre los UE que pertenezcan a la WLAN.
- El diseño e implementación de la interfaz Java para la configuración dinámica de IPsec permite aprovechar de forma transparente para el UE la seguridad brindada por éste protocolo.

Algunos de los trabajos que se pueden desarrollar a partir de MidSEG son: i) Evaluar a MidSEG en un ambiente IMS con otras tecnologías de acceso, y de ser necesario, realizar la adaptación respectiva. ii) Proveer a MidSEG de funcionalidades que permitan prestar calidad de servicio. iii) Extender MidSEG a los puntos 4 y 5 de la arquitectura de seguridad de IMS.

Referencias

1. S. Muhammad, T. Magedanz. "3G-WLAN Convergence: Vulnerability, Attacks Possibilities and Security Model". *The Second International Conference on Availability, Realiability and Security*. Vienna. 2007. pp. 198-205.
2. T. Wilder. "como estar seguro en un mundo IMS". *Revista auditoría y seguridad*. Vol. 10. 2007. pp. 83-85.
3. 3GPP TS 33.203. *3G security; Access security for IP based services*. Ed. 3GPP, Valbonne (Francia). 2008. pp. 7-28.
4. IETF. *HTTP Digest AKAv2*. Ed. IETF, Fremont (USA). 2005. pp. 2-11.
5. D. Celentano, A. Fresa, M. Longer, A. L. "Robustelli. Improved authentication for ims registration in 3G/ WLAN interworking". Personal, Indoor and Mobile Radio Communications. *2007.* PIMRC 2007. *IEEE 18th International Symposium on Publication.* Vol. 3-7. 2007. pp. 1-5.
6. C. Ntantogian, C. Xenakis. "Reducing authentication traffic in 3G-WLAN integrated networks". Personal, Indoor and Mobile Radio Communications 2007. PIMRC 2007. *IEEE 18th International Symposium on*. Vol. 3-7. 2007. pp. 1-5.
7. C. Ntantogian, I. Stavrakakis, C. Xenakis. "Reducing the User Authentication Cost in NextGeneration Networks". *Wireless on Demand Network Systems and Services*. 2008. pp. 65-72. WONS 2008.IEEE Fifth Annual Conference on Publication. Garmisch-Partenkirchen (Alemania). Vol. 23-25. 2008.
8. L. Veltri, S. Salsano, G. Martiniello. "Wireless LAN-3G Integration: Unified Mechanisms for Secure Authentication based on SIP". *Communications, 2006. ICC '06. IEEE International Conference*. Vol. 5. 2006. pp. 2219-2224.
9. 3GPP TS 33.234. 3G Security. *Wireless Local Area Network (WLAN) Interworking security Release*. Vol. 8. 2008. pp. 9-58.
10. IETF. *Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)*. RFC 4187. Ed. IETF, Fremont (USA). 2006. pp. 4-30.
11. IETF. *PPP Extensible Authentication Protocol (EAP)*. RFC 2284. Ed. IETF, Fremont (USA). 1998. pp. 2-12.
12. IETF. *Internet Key Exchange (IKEv2) Protocol*. RFC 4306. Ed. IETF, Fremont (USA). 2005. pp. 3-27.
13. 3GPP TR 22.934. *Feasibility study on 3GPP system to Wireless Local Area Network (WLAN) Interworking*. Vol. 7. 2007. pp. 42-53.
14. C. C. Yang, K. H. Chu, Y. W. Yang. "3G and WLAN Interworking Security: Current Status and Key Issues". *International Journal of Network Security*. Vol. 2. 2006. pp. 1-13.
15. 3GPP TS 35.206. *Specification of the MILENAGE algorithm set*. Ed. 3GPP, Valbonne (Francia). 2008. pp. 6-12.
16. IETF. *IP Encapsulating Security Payload (ESP). IETF. RFC 2406.* Ed. IETF, Fremont (USA). 1998. pp. 3-17.
17. https://jain-sip.dev.java.net. Consultada el 30 de Marzo de 2009.
18. http://ipsec-tools.sourceforge.net/. Consultada el 30 de Marzo de 2009.
19. http://www.netfilter.org/projects/iptables/index.html. Consultada el 30 de Marzo de 2009.
20. http://netbsd.gw.com/cgi-bin/man-cgi?racoon++NetBSD-current. Consultada el 30 de Marzo de 2009.
21. http://www.openimscore.org/. Consultada el 30 de Marzo de 2009.
22. http://www.bind9.net/. Consultada el 30 de Marzo de 2009.
23. P. Herzog. *OSSTMM - Manual de la Metodología Abierta de Testeo de Seguridad*. Ed. Universidad del Cauca. Popayán. 2008. pp. 31-85.
24. http://www.wireshark.org. Consultada 30 de Marzo de 2009.
25. http://www.tamos.com/products/commwifi/. Consultada el 30 de Marzo de 2009.
26. IETF. SIP: *Session Initiation Protocol*. IETF RFC 3261. Ed. IETF, Fremont (USA). 2002. pp. 264.