COLABORACIÓN DE IMS Y SDN-OPENFLOW

Una arquitectura para mitigar problemas de seguridad en redes futuras

Por: Ing. Yanko Antonio Marín Muro, Especialista de la Unidad de Control de la Dirección Territorial de Sancti Spíritus (DTSS), ETECSA; DrC. Ing. Félix Florentino Álvarez Paliza, Profesor Titular, Jefe de la disciplina de Sistemas de Telecomunicaciones, ISPJAE; Ing. Abel A. López Carbonell, Especialista principal del Departamento de Control de la División de Servicios Fijos (DVSF), ETECSA.
yanko.marin@etecsa.cu; fapaliza@uclv.edu.cu; abel.lopez@etecsa.cu

RESUMEN

IMS es una arquitectura basada en el protocolo SIP que sirve como una infraestructura para el control de llamadas, sesiones y servicios en redes futuras. El Subsistema Multimedia IP (IMS) es una arquitectura de control para las redes de próxima generación (NGN). Se espera que esta arquitectura de red proporcionará nuevos servicios multimedia en entornos de redes convergentes. Las redes definidas por software (SDN) han surgido como un enfoque para fomentar la innovación en la red a través de una mayor flexibilidad, capacidad de programación, gestión y rentabilidad.

En este trabajo se propone la colaboración de las arquitecturas IMS y SDN para mitigar problemas de seguridad en redes futuras. Para ello se empleo una plataforma de código abierto como laboratorio de pruebas para la enseñanza, el aprendizaje y la evaluación del desempeño de los principales elementos de esta arquitectura.

Palabras clave: IMS, IP Multimedia Subsystem, SDN, OpenFlow, Open IMS Core

ABSTRACT

IMS is a SIP protocol-based architecture deployed as an infrastructure for call, session and service management in future networks. IP Multimedia Subsystem (IMS) is a management architecture for next generation networks (NGN). It is expected that this network architecture provides new multimedia services in scenarios of converged networks. Software-defined networks (SDN) have emerged as an approach to promote network innovation comprising higher flexibility, programming, management and profitability capacity.

This paper aims at proposing IMS and SDN architectures collaboration in order to mitigate security problems in future networks. To do so, an open-source platform as a testing lab is deployed for teaching, learning and performance assessment of the main elements of this architecture.

Key words: *IMS, IP Multimedia Subsystem, SDN, OpenFlow Open IMS Core*

Introducción

La industria de las telecomunicaciones está experimentando una gran revolución y el catalizador de este cambio son los nuevos modelos de negocio y las tecnologías de Internet. El acceso ubicuo a servicios de voz, datos, video, multimedia, juegos, entretenimiento, etc, basados en IP, está conduciendo a la convergencia de industrias, servicios, redes y modelos de negocio.

La seguridad es un factor clave en las redes, por lo que es uno de los requisitos básicos a cumplir para el buen funcionamiento de las mismas. Con el desarrollo de las Tecnologías de la Información y las Comunicaciones (TIC), los teléfonos inteligentes —*smartphones*—, la convergencia de servicios, la seguridad de la red IMS afronta muchas amenazas y retos. [3]

El motivo de esta investigación está encaminado a analizar las arquitecturas IMS y SDN basada en el protocolo *OpenFlow*; identificar las principales medidas para garantizar la seguridad en IMS; así como identificar algunos beneficios que desde el punto de vista de la seguridad pueden ser utilizados mediante la colaboración entre las dos arquitecturas.

Medidas para garantizar la seguridad en redes IMS

El subsistema multimedia IP (IMS) para defenderse utiliza políticas de seguridad rigurosas y así prevenir ataques a la red. Con el objetivo de evitar agresiones a los elementos de la red en IMS se utilizan los controladores de borde de sesión (SBC). Los SBC —*Session Border Controller*— usualmente se despliegan en la frontera de red IP para controlar las sesiones de audio, datos y video. Estas arquitecturas también se utilizan para esconder la topología de la red y para garantizar que las sesiones VoIP solamente se realicen contra los controladores autorizados. Las principales medidas que deben ser adoptadas son las siguientes:

División por zonas de seguridad

Según los principios de división por zona de seguridad definidos en ITU E.408, la red IMS está dividida en las siguientes áreas lógicas:

- Tipo entidad de red (NE)
- Objetivos de seguridad
- Políticas de seguridad

Las subredes o los dispositivos que comparten los requerimientos de seguridad tienen estrechas relaciones de confianza y por tanto requieren iguales o similares políticas de control de acceso. Cada área lógica pertenecerá a una zona segura o de confianza, no segura o desmilitarizada.

Segregación de los servicios

Para asegurar la transmisión de datos entre las zonas de seguridad, en IMS se adopta el principio de segregar los servicios. Con esta política de seguridad se garantiza que un servicio no pueda afectar a otro. Estas políticas utilizan las tecnologías de redes de área local virtual (VLAN) y redes privadas virtuales (VPN) para aislar los flujos de datos de diferentes zonas. Mediante la segregación de los servicios, la red IMS puede funcionar de una forma más estable y segura.

Codificación IPSec

IMS utiliza una red portadora dedicada para la transmisión IP y que generalmente es segura. Sin embargo, en algunos escenarios pueden existir algunos riesgos y tal es el caso de cuando se transmiten datos entre dos redes IMS. Para evitar los riesgos de seguridad en este tipo de entornos, la tecnología IPsec —*IP security*— puede ser utilizada para codificar la información sobre esta red.

Medidas de seguridad en el plano de control

En el plano de control se deben proteger la topología de la red, cuentas, claves, información personal y autentificación de los usuarios. En IMS la protección contra usuarios no autorizados se garantiza con los mecanismos de autentificación. La protección contra la divulgación de la topología de la red es una de las medidas de seguridad más importantes que no pueden omitirse en el diseño de un sistema.

Campo de pruebas IMS

En este trabajo proponemos la implementación de un campo de pruebas de IMS sobre el sistema operativo Debian 7 Wheezy que ayudará a los investigadores a crear su propio núcleo IMS con el objetivo de estudiar los protocolos de estas redes; así como evaluar el comportamiento de las mismas ante los diferentes tipos de ataques que fueron presentados anteriormente. Conocer la naturaleza de cada uno de los ataques permitirá crear implementaciones de redes más seguras en cualquier nivel de la red de telecomunicaciones.

Para ello utilizamos la plataforma Open IMS Core que es una implementación de código abierto del núcleo de una red IMS, y que consiste de un P-CSCF, I-CSCF, S-CSCF, y un HSS (Figura 1). Open Source IMS Core System es un sistema multimedia IP para pruebas desarrollado por el Instituto Fraunhofer Fokus y no está concebida para aplicaciones comerciales. El subsistema creado por FOKUS es un entorno ideal para desarrolladores que desean crear aplicaciones y servicios basados en IMS. Los componentes del CORE IMS de FOKUS están basados en el software de código abierto SIP Express Router (SER). En esta etapa inicial de la investigación fue instalado Open IMS Core en un servidor Debian 7 Wheezy y se configuraron cada uno de los nodos IMS para trabajar localmente el propio servidor. En la segunda etapa de la investigación, se instalará cada

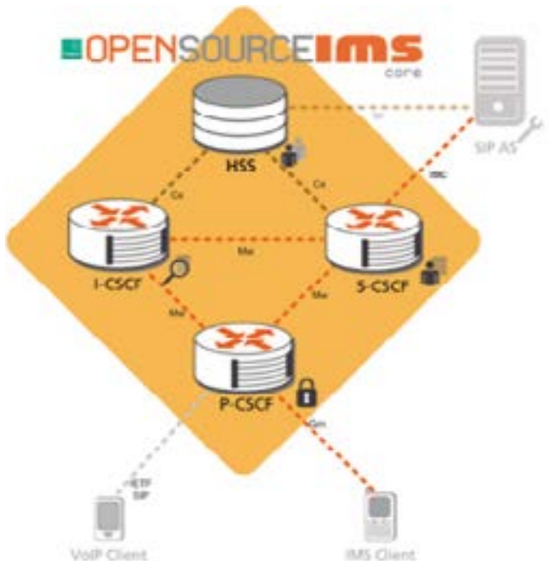

Figura 1. FOKUS OPEN IMS CORE. Fuente: Open IMS FOKUS.

nodo en un servidor diferente para aumentar el rendimiento del núcleo de IMS y disminuir el tiempo de respuesta de la red. En la Figura 2, se puede observar el topológico de la prueba de campo propuesta. Después de configurado el núcleo de IMS se procederá a instalar un cliente IMS en las PC1 y PC2. SP1 y SP2 serán dos teléfonos SIP MITEL 5212. Los ordenadores WF1 y WF2 accederán a la red vía WiFi y tendrán instalado clientes IMS. Los teléfonos inteligentes 555555 y 888888 accederán a la red vía WiFi utilizando la aplicación IMSDROID.

En la tercera etapa de la investigación, se instalará el núcleo de IMS en la plataforma de virtualización PROXMOX con el objetivo de incrementar el rendimiento de la red. Para lograr lo anterior se crean máquinas virtuales realizando funciones específicas de P-CSCF, S-CSCF. Al incrementar la cantidad de nodos del núcleo de la red se garantiza un incremento de la capacidad de procesamiento de sesiones así como la mejora de la fiabilidad del sistema ante el fallo de algún nodo.

Colaboración de IMS y SDN-*OpenFlow*. Una arquitectura para mitigar problemas de seguridad en redes futuras

Las Redes Definidas por Software (SDN) —*Software Defined Network*— se presentan como un nuevo paradigma de red que tiene el objetivo de solucionar los problemas de complejidad, escalabilidad y dependencia de proveedores de las redes actuales. Las SDN han surgido como un enfoque para fomentar la innovación en la red a través de una mayor flexibilidad, capacidad de programación, gestión y rentabilidad. En las SDN se separa la lógica de control de los *routers* y *switch* de la conmutación de tramas y paquetes. Con esta separación los *routers* se convierten en dispositivos simples especializados en el reenvío de tramas y paquetes. [4], [5]

La seguridad de la red es una parte notable de la seguridad cibernética y está ganando atención constantemente. Las prácticas tradicionales relacionadas con la seguridad de red se implementan desplegando firewalls, SBC, servidores proxy para proteger una red física. [6]

En este aspecto, SDN ofrece una plataforma conveniente para centralizar, combinar y controlar las políticas y configuraciones para asegurarse de que la implementación cumple con la protección requerida. De esta manera de una forma proactiva se evitan brechas de seguridad [7]. Por otra parte, SDN proporciona mejores métodos para detectar y defenderse de ataques de forma reactiva. Debido a que SDN tiene la capacidad de recopilar estado de la red, se pueden analizar los patrones de tráfico en busca de amenazas de seguridad potenciales. Los ataques, como ataques de ráfaga de baja velocidad y distribuidos de denegación de servicio (DDoS), se pueden detectar simplemente mediante el análisis de patrones de tráfico. [5]

Al mismo tiempo, SDN proporciona un control programático sobre los flujos de tráfico. En consecuencia, el tráfico de interés puede ser dirigido explícitamente a Sistemas Prevención de Sistemas Intrusos (IPSs) para los sistemas de Inspección Profunda de Paquetes (DPI). Si estos sistemas detectan ataques, la SDN puede instalar reglas de reenvío de paquetes a los dispositivos de conmutación para bloquear el tráfico malicioso cuando esté entrando o propagando por la red. [8]

El control centralizado de SDN permite poner en cuarentena dinámica a los *host* atacantes y obligarlos a pasar por un nuevo proceso de autenticación. Por último, SDN es más capaz de proporcionar un control directo y preciso sobre las redes, y le da la oportunidad de poner en práctica nuevas estrategias de protección de la seguridad. [8]

Al analizar las potencialidades relativas a las aplicaciones de calidad de servicios, balance de carga y seguridad de las redes SDN que fueron abordadas muy brevemente, es evidente que la arquitectura IMS debe colaborar con la arquitectura SDN para que los elementos que las componen puedan en tiempo real realimentarse como por ejemplo de situaciones de seguridad en toda la red. Los dispositivos conmutadores de paquetes de la red deben soportar *Openflow* que es el protocolo estándar entre la capa de infraestructura y la de control. Bajo

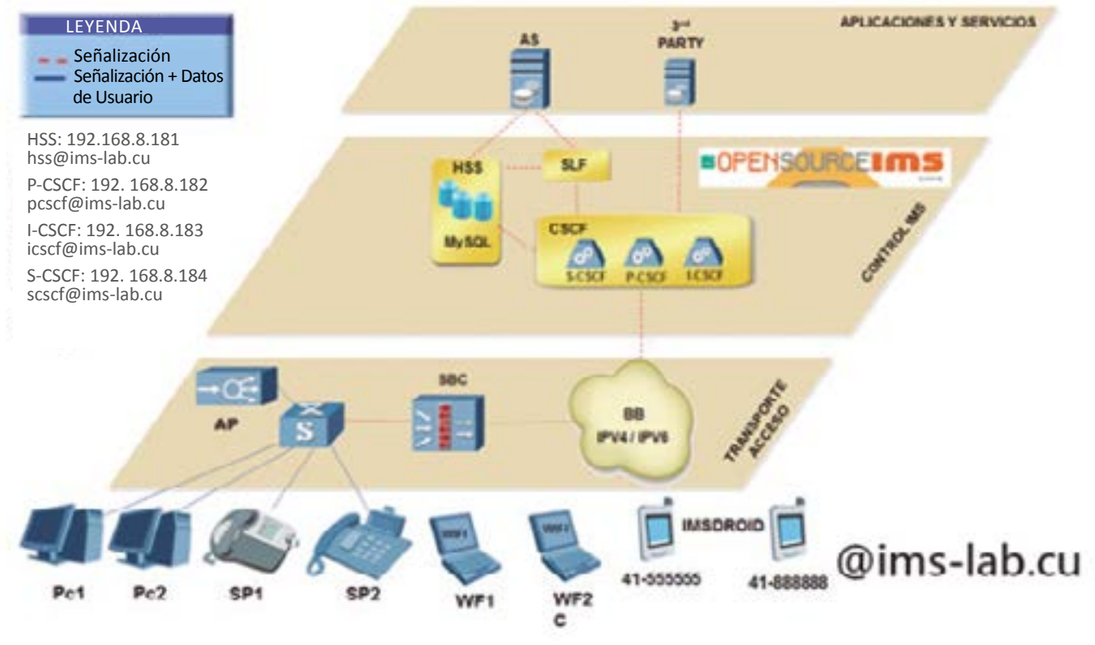

Figura 2. Laboratorio de pruebas. Dominio ims-lab.cu. Fuente: Elaboración propia.

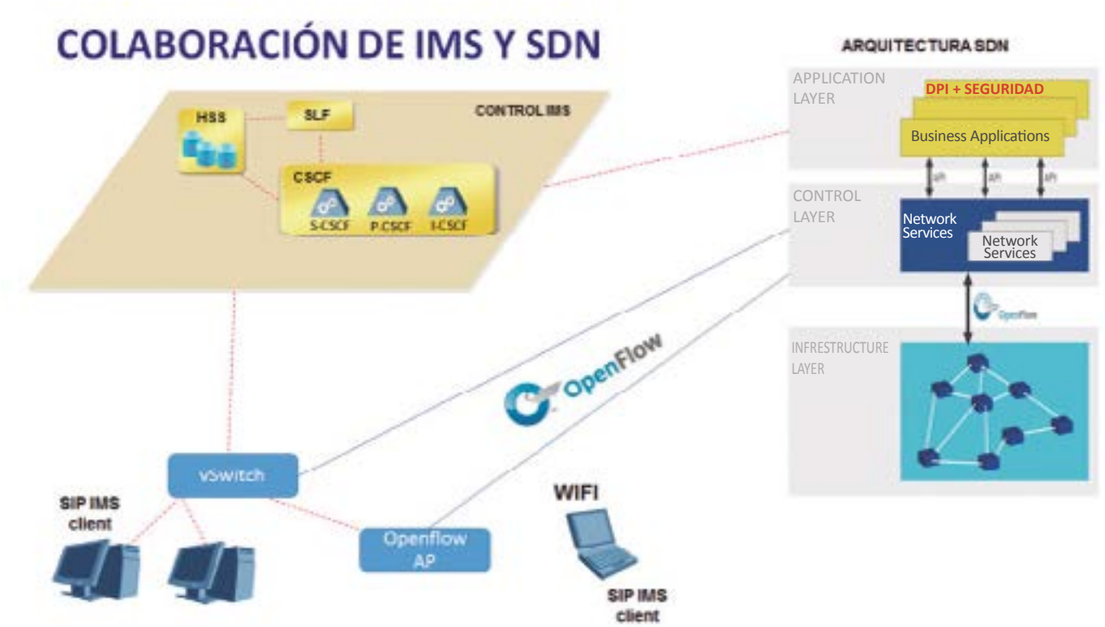

Figura 3. Colaboración de IMS, SDN basada en el protocolo OpenFlow. Fuente: Elaboración propia.

este escenario es necesario pensar en la integración de las dos arquitecturas de forma tal que permita la creación de servicios IMS novedosos mediante el intercambio de señalización entre el control de IMS y aplicaciones de SDN. En redes donde el servicio IMS no sea virtual se pueden sustituir los *switch* y *router* por equipamientos que soporten el protocolo *OpenFlow*. De esta forma se puede realizar una migración de los servicios IMS sin necesidad de cambiar el núcleo de la red.

Para el caso especial de la seguridad en IMS para mitigar los ataques de denegación de servicio y paquetes mal formados se propone la creación de una aplicación SDN especializada en este tipo de ataques (Figura 3). La aplicación SDN podrá a partir de la información estadística que está concebida en el propio protocolo *OpenFlow* chequear las velocidades de señalización en múltiples puntos de la red, aplicar reglas de denegación a usuarios maliciosos o transferir los datagramas a otras aplicaciones DPI antes de que los mensajes SIP sean enviados al P-CSCF.

Para los ataques de lógica de servicio la aplicación SDN puede emplear filtros para verificar que los mensajes SIP cumplen con lo definido en los estándares de este protocolo. Las aplicaciones SDN corren sobre servidores y plataformas de virtualización que ante ataques y sobrecargas pueden auto ajustarse por ejemplo incrementando la cantidad de memoria o de procesamiento sin necesidad de incrementar *hardware* en el núcleo de la red IMS.

Criterios a tener en cuenta en la arquitectura para mejorar la seguridad de la red:

- Delegar las tareas a varios controladores SDN (en lugar de un solo controlador)

- Separar en el controlador SDN las funciones de control de las de monitoreo con el objetivo de evitar sobrecargas

- Desarrollar procedimientos a nivel de aplicación para distinguir entre ataques de alta y baja resolución

- Detectar ataques de alta resolución como el envenenamiento ARP Cache (ARP Cache Poisoning), y ARP Spoofing, que no pueden ser identificados sin tener acceso a todos los paquetes entrantes de un dispositivo de red

- Detectar ataques de baja resolución como DoS, DDoS y amplificación DNS, sin analizar 100% de los paquetes entrantes a un dispositivo

- Crear una API que permita la comunicación entre los elementos de control de la arquitectura IMS del 3GPP y las aplicaciones de la arquitectura SDN para que exista colaboración entre las dos arquitecturas

- Crear una API que permita la comunicación entre los PRCF, PCEF de la arquitectura IMS y las aplicaciones encargadas de garantizar la calidad del servicio (QoS) de la arquitectura SDN

Conclusiones

Para implementar redes que satisfagan los requerimientos de los usuarios de aquí en adelante, se hace necesario un cambio en la concepción de las arquitecturas de telecomunicaciones actuales. IMS llegó para cumplir con el sueño de las redes completamente IP, convergencia fijo-móvil e Internet, así como para resolver los problemas de calidad de servicio y seguridad de las redes anteriores. Como toda arquitectura, IMS posee sus propias amenazas de seguridad y es por eso que en esta investigación fueron abordadas las principales medidas que deben ser tomadas.

También se propone la implementación de un banco de prueba que ayudará a los investigadores a crear su propio núcleo IMS con el objetivo de estudiar los protocolos de estas redes; así como evaluar el comportamiento de las mismas ante diferentes tipos de ataques. Finalmente, se propone la colaboración de las arquitecturas IMS y SDN para mitigar problemas de seguridad en redes futuras.

Referencias bibliográficas

[1] Qadeer, M. A.; Khan, A. H.; Ansari, J. A. y Waheed, S. “IMS Network Architecture”. International Conference on Future Computer and Communication. ICFCC, pp. 329-333, 2009.

[2] Boucadair, M. y Jacquenet, C. “Software-Defined Networking a Perspective from within a Service Provider Environment”. Acceso: Octubre 2015. Disponible en: https://tools.ietf.org/html/rfc7149

[3] Natouri, S. y Lac, C. “IMS threats taxonomy: Survey and proposal”. International Conference on Computing, Management and Telecommunications (ComManTel), pp. 315-320, 2013.

[4] "Software-Defined Networking (SDN) Definition - Open Networking Foundation”. Acceso: Octubre 2015. Disponible en: https://www.opennetworking.org/sdn-resources/sdn-definition

[5] Xia, W.; Wen, Y.; Foh, C. H.; Niyato, D. y Xie, H. “A Survey on Software-Defined Networking”. IEEE Commun. Surv. Tutor. Vol. 17, No. 1, pp. 27-51, Firstquarter 2015.

[6] Yan, Q.; Yu, R.; Gong, Q. y Li, J. “Software-Defined Networking (SDN) and Distributed Denial of Service (DDoS) Attacks in Cloud-Computing Environments: A Survey, Some Research Issues y Challenges”. IEEE Commun. Surv. Tutor. Vol.17, No. 99, p.1, 2015.

[7] Nguyen, V.-G.; Do, T.-X. y Kim, Y. “SDN and virtualization-based LTE mobile network architectures: A comprehensive survey”. Wirel. Pers. Commun.. Vol. 86, No. 3, pp. 1401–1438, 2016.

[8] Ali, S. T.; Sivaraman, V.; Radford, A. y Jha, S. “A Survey of Securing Networks Using Software Defined Networking”. IEEE Trans. Reliab., Vol. 64, No. 3, pp. 1086-1097, 2015.

(Artículo recibido en noviembre de 2015 y aprobado en enero de 2016)