Seguridad en la virtualización de Redes Definidas por Software: revisión por dimensión a virtualizar

Graciela Becci[1], Miguel Morandi[1], Luis Marrone[2]

[1] Universidad Nacional de San Juan, Av Libertador San Martín Oeste 1109, San Juan, J5400ARL Argentina.
[2]Universidad Nacional de La Plata, Facultad de Informática, Calle 50 y Av 120, La Plata, Buenos Aires, B1900ASF.
gbecci@unsj.edu.ar, morandi@unsj.edu.ar, lmarrone@linti.unlp.edu.ar

Resumen. En las Redes Definidas por Software (SDN), donde el Plano de Control está separado del Plano de Datos (hardware), la red es configurada y administrada en forma dinámica y centralizada desde el controlador. Esto permite flexibilidad en la programación del flujo de la red y variedad en los servicios a desarrollar, para mejorar la performance y seguridad de la red, tales como ruteo y firewalling. El protocolo de comunicación de SDN, OpenFlow ofrece una abstracción del Plano de Datos que permite virtualizar los recursos de la red, ancho de banda, topología, tabla de flujo de datos, etc, tarea inimaginable en el modelo de red tradicional con dispositivos administrados en forma individual. No obstante las ventajas del control centralizado existen temas de seguridad inherentes a SDN, OpenFlow en particular y a la virtualización de la red, que justifican un análisis de la seguridad de la red en este escenario. El enfoque de este artículo se basa en las vulnerabilidades de los protocolos usados por FlowVisor para virtualizar, en la administración de la red por parte de FlowVisor como proxy y el comportamiento del controlador OpenFlow. Se obtuvo un panorama integrador de los aspectos de seguridad que afectan a la red SDN virtualizada, y las medidas que se pueden tomar para contrarrestar las vulnerabilidades señaladas.

Palabras clave: redes definidas por software, virtualización de redes SDN, seguridad en redes de datos

1 Introducción

Una Red Definida por Software SDN es un paradigma alternativo a las redes tradicionales, donde cada dispositivo ejecuta su propio sistema operativo y donde la configuración debe hacerse en forma individual por cada equipo. En este tipo de redes el Plano de Control está separado del Plano de Datos (hardware), y la red es configurada y administrada en forma dinámica y centralizada desde el controlador [1]. El control de la red se realiza mediante interfaces y plataformas estandarizadas que permiten la creación de servicios para los diferentes planos. Esto permite flexibilidad en la programación del flujo de la red y variedad en los servicios a desarrollar, para mejorar la performance y seguridad de la red, tales como ruteo, firewalling, network Address translation, balance de cargas, etc. OpenFlow es el protocolo de comunicación de la red SDN que además de sus funciones específicas ofrece una abstracción del Plano de Datos, condición necesaria para el desarrollo y florecimiento de plataformas de virtualización de la red. Para este artículo se seleccionó FlowVisor

como el hypervisor para analizar los temas de virtualización y seguridad, por ser el proyecto fundamental en el área, y base para el desarrollo de otras plataformas.

El enfoque de este artículo para el análisis de seguridad en la virtualización de la red SDN se basa en las vulnerabilidades de los protocolos usados por FlowVisor para virtualizar y por la administración de la red por parte de FlowVisor como proxy y del controlador de OpenFlow.

En las secciones siguientes se describe el paradigma SDN y los aspectos más relevantes del protocolo de comunicación OpenFlow que puedan servir para el análisis de seguridad en la virtualización. Se describe la forma en que FlowVisor realiza la virtualización para cada una de las cinco dimensiones de virtualización y cómo asegura el aislamiento. Se resumen los temas de seguridad más relevantes que afectan a cada dimensión y las medidas sugeridas en la literatura. Por último se presenta la conclusión y temas de interés más relevantes.

2 Virtualización de SDN

Para el análisis de seguridad en la virtualización de SDN de este artículo se tienen en cuenta la arquitectura de SDN, el comportamiento de OpenFlow en relación a la estrategia de virtualización de FlowVisor, que dan como resultado las dimensiones en las cuales se puede virtualizar la red. A continuación se describen estos agentes para luego dar un detalle de las dimensiones de virtualización y los temas de seguridad relacionados.

2.1 SDN: Paradigma y Arquitectura

La necesidad de controlar el tráfico de la red en forma flexible, la necesidad de aprovechar los recursos de la red en forma eficiente mediante la virtualización de la red y la necesidad de asignar recursos en forma flexible sin causar disrupción a la red, son sólo algunos de los factores que impulsaron el desarrollo del paradigma de SDN.

Como solución, SDN propone una arquitectura donde las funciones de control (Control Plane) están separadas de los dispositivos de red (Data Plane), descriptos en **Figura 1**.

Los controladores pueden residir en servidores estándar y la abstracción del Plano de Datos permite que la infraestructura de la red sea considerada como una entidad lógica [3]. Esto da lugar a que en el Plano de Datos coexistan diferentes tipos de dispositivos de red, comunicándose mediante protocolos en diferentes capas, realizando tareas estándar de recepción y envío de paquetes. El controlador se encarga de tareas complejas como ruteo, definición de políticas, sistemas de nombres y funciones de seguridad. Los controladores y switches SDN pueden implementar switches Ethernet de Capa 2, Internet Routers de Capa 3, transporte en Capa 4 y conmutación y ruteo mediante aplicaciones de Capa 7 [2].

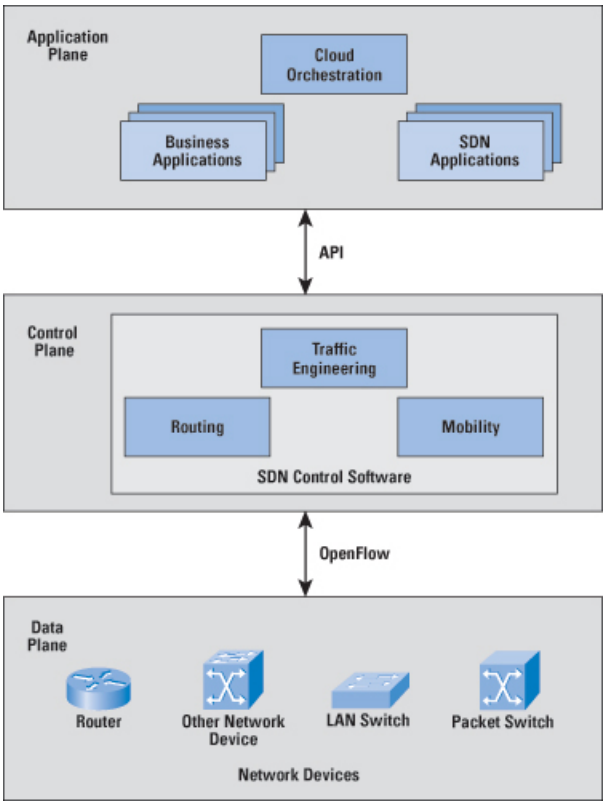

Fig 1. Arquitectura de una red SDN, donde se muestran los planos de Datos y Control comunicados entre si mediante el protocolo OpenFlow. El Plano de Contros se considera compuesto por el Plano de Aplicaciones y el Plano que contiene el controlador [2].

2.2 OpenFlow: Protocolo de comunicación de SDN

OpenFlow es el protocolo de comunicación entre el Plano de Control y el Plano de Datos de una red SDN, define parte del comportamiento del Plano de Datos, pero no especifica el comportamiento del controlador [4], y es al momento el único protocolo de dominio público que define la comunicación entre ambos planos.

Un sistema OpenFlow se compone de un controlador OpenFlow que se comunica con uno o más switches OpenFlow. El protocolo OpenFlow que define los mensajes intercambiados entre el controlador en el Plano de Control y los dispositivos en el Plano de Datos.

Un switch OpenFlow además de las funciones de un switch estándar de recibir paquetes por un puerto y transferirlos por otro, realizando algunas modificaciones a la trama si es necesario, tiene la función de comparación de paquetes, específica de OpenFlow, ver **Figura 2**. El switch contiene una Tabla de Flujo, cuando un paquete arriba al switch es comparado con las entradas en la Tabla de Flujo, de acuerdo al resultado de la lógica de comparación se ejecutan una de las acciones que pueden ser: transferir el paquete, descartarlo o enviarlo al controlador.

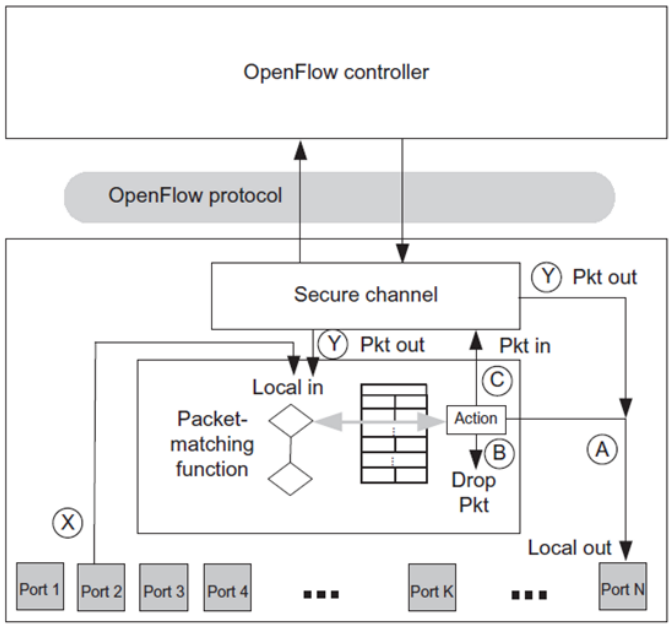

Fig 2. Estructura lógica de un OpenFlow Switch: se observan los puertos de acceso (x), la comunicación con el controlador mediante un canal seguro (y), y la lógica de comparación de paquetes. El resultado de esta última puede ser (A) packet forward, (B) packet drop, (C) forward to control logic [4].

Una implementación de switch OpenFlow puede ser OpenFlow puro o híbrido. Un switch OpenFlow puro sigue la lógica del protocolo OpenFlow, mientras que el switch híbrido puede también conmutar paquetes en modo Ethernet o ruteo IP. Este tipo de switch híbrido requiere un pre-procesamiento que determine si los paquetes son enviados en la forma tradicional o según el mecanismo de OpenFlow.

OpenFlow usa doce campos de la cabecera del mensaje para buscar las coincidencias, que referidas al modelo OSI son: Capa 1 física, Capa 2 de enlace de datos, Capa 3 de red, y Capa 4 de transporte, tales coincidencias pueden ser el puerto de entrada, la dirección IP y MAC de origen y destino y los rótulos de VLAN de Identificación y prioridad (PCP Priority Code Point, VID VLAN Identifier), entre otros. La **Figura 3** muestra la lista completa de los doce campos y su correspondencia con el modelo OSI.

Cuando el flujo de datos ingresa al switch se busca la coincidencia de alguno de estos campos con los flujos instalados en la Tabla de Flujos. Cuando se encuentra la primera coincidencia se detiene la búsqueda y se ejecutan las acciones asociadas a ese paquete que puede ser su envío al destino o descarte. Si se llega al final de la tabla de flujo de datos sin encontrar una coincidencia se envía el paquete de datos al controlador para que tome una decisión con respecto al paquete que puede ser incluirlo en la tabla de flujo de datos. El controlador puede determinar el envío de un paquete a una determinada cola asociada a un puerto con el propósito de Calidad de Servicio

Field	Description	Layer
Ingress Port	Incoming port for the frame	Physical
Ether source	Source MAC address	Data Link
Ether dst	Destination MAC address	
Ether type	Encapsulated Protocol in the payload. For IPv4, it is 0x0800	
VLAN id	VID field in the VLAN tag	
VLAN priority	PCP field in the VLAN tag	
IP src	Source IP address	Network
IP dst	Destination IP address	
IP proto	Transport layer protocol	
IP ToS bits	Type of Service field	
TCP/UDP src port	Source transport port (or ICMP type field)	Transport
TCP/UDP dst port	Destination transport port (or ICMP code field)	

Fig 3. Campos de comparación en la Tabla de Flujo de un switch OpenFlow y su correspondencia con el modelo OSI. [5]

2.3 FlowVisor: Virtualización en SDN

Al igual que sucede con la virtualización del hardware, donde una buena definición de la abstracción del hardware permite que los sistemas operativos huéspedes compartan los recursos físicos como si fueran dedicados, en la virtualización de la red, una adecuada definición de la abstracción de la red (switches, routers, access points, etc) permitiría que diferentes redes funcionen simultánea e independientemente entre sí. En redes convencionales, si bien existe la posibilidad de virtualizar recursos particulares como es el caso de las VLAN que virtualizan la Capa 2 de enlace de datos, no se cuenta con una capa de abstracción de hardware común a todos los dispositivos.

Existen varias plataformas de virtualización de red para SDN [6], de las cuales este artículo se focaliza en FlowVisor por ser el proyecto seminal de la virtualización de SDN. FlowVisor se basa en la abstracción del hardware (Plano de Datos) que ofrece OpenFlow para virtualizar la red en cinco dimensiones: ancho de banda, topología, CPU del switch, tráfico, tablas de ruteo [7], ver **Figura 4**. FlowVisor actúa como proxy entre el Plano de Control y el Plano de Datos, transcribiendo y reenviando los mensajes de control, de forma tal de refinar la definición de las tablas de ruteo de los dispositivos de red. Al poder virtualizar en cinco dimensiones es posible optimizar el uso de recursos de la red y segmentarla para su mejor uso.

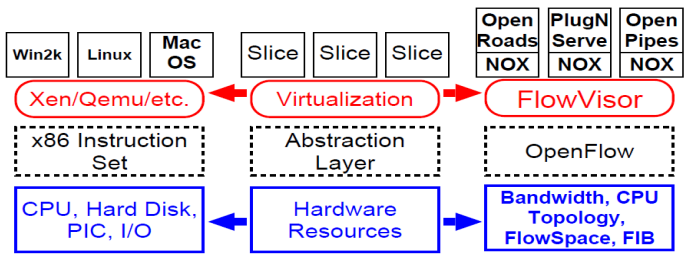

Fig 4. FlowVisor: comparación con la virtualización de computadora estándar. En el caso de FlowVisor se indican los recursos de una red a ser virtualizados, ancho de banda, CPU, topología, tráfico y tabla de flujo. En el Plano de Control se indica a

NOX como el sistema operativo de red para alojar las diferentes aplicaciones [7].

Seguridad en la Virtualización y Aislamiento

No obstante las ventajas del control centralizado de la red mediante la separación de los planos de control y de datos en redes SDN, existen temas de seguridad inherentes al paradigma de SDN, al protocolo OpenFlow en particular y a la administración de la red SDN. En la **Figura 5** se observan las diferentes funciones de cada plano y cómo interactúan entre sí, además de la administración a través del protocolo SNMP. Este protocolo en sí mismo introduce vulnerabilidades además de la comunicación entre planos vulnerable a ataques del tipo man-in-the-middle si no se encripta el canal.

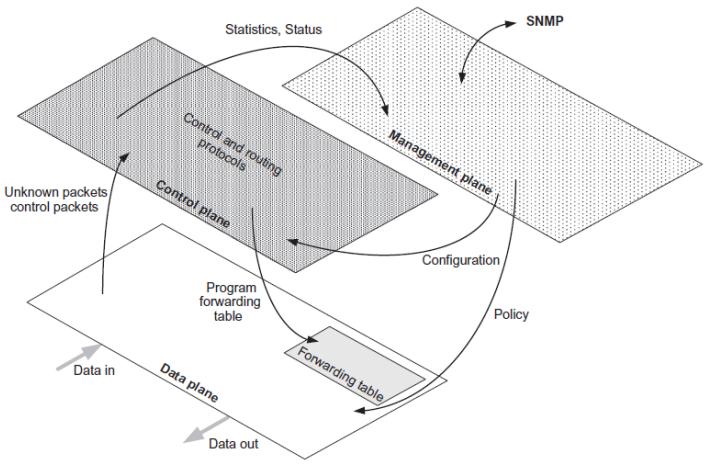

Fig 5. Planos de una red SDN y sus funciones: interacción entre planos y acceso de administración mediante SNMP [8].

Además de la evidente vulnerabilidad que implica el control centralizado de ser un single-point-of-failure y por ende incrementar la vulnerabilidad a un ataque de denegación de servicio, existe la vulnerabilidad de usar texto plano para los mensajes entre el controlador y el Plano de Datos. A partir OpenFlow v1.0 el estándar recomienda el uso de encriptación asimétrica TLS entre switch OpenFlow y el controlador OpenFlow, en versiones anteriores, era mandatorio [4]. Si se implementara TLS, haría falta también implementar la autenticación de los switches para evitar ataques del tipo de reconocimiento de la red que dejen vulnerable a la topología [9]. Este tipo de reconocimiento puede detectar puertos de switches en modo escucha (listener), lo que dejaría vulnerable el dispositivo para insertar reglas que afecten al resto de la topología.

La seguridad de la virtualización está dada por el aislamiento entre los segmentos virtualizados. Este aislamiento debe darse tanto en el Plano de Control como en el Plano de Datos. Teniendo en cuenta esta premisa, la naturaleza de los recursos y los protocolos a disposición se pueden distinguir tres técnicas de aislamiento, segmentación, encapsulamiento y reescritura de paquetes [5]. En líneas generales, segmentación ocurre cuando los recursos son demarcados en base a información, atributos, características, etc que posean. El uso del contenido de la cabecera del mensaje es un ejemplo de segmentación de recursos. La encapsulación se produce cuando se usan rótulos para demarcar el tráfico como es el caso de VLAN. La reescritura de paquetes puede darse en el Plano de Control, reescribiendo los mensajes de control, o a nivel de Plano de Datos reescribiendo la cabecera del mensaje.

FlowVisor, en su calidad de proxy, ofrece ventajas en tema de seguridad al poder refinar las reglas entre el controlador y el Plano de Datos, pero introduce otras

vulnerabilidades propias de la virtualización que son analizadas en la siguiente Sección.

3 Seguridad y Virtualización: Dimensiones

3.1 Virtualización del Ancho de Banda

La virtualización de la red que lleva a separar los recursos de la red en canales de ancho de banda separados, no tan sólo sirve para la organización y administración de los recursos, sino también para la optimización de la capacidad del ancho de banda.

OpenFlow v1.0 no tiene un método particular para virtualizar la red pero permite la marcación de VLAN [10] lo que permite la distribución del flujo en colas por ancho de banda y la asignación de prioridades para manejo de Calidad de Servicio.

Virtualización del Ancho de Banda: Aislamiento

Dentro de la trama Ethernet, VLAN tag se compone de campos de 4 bytes, VLAN ID Identifier (2 bytes) y VLAN PCP Priority Code Point (2 bytes) [10], **Figura 6**.

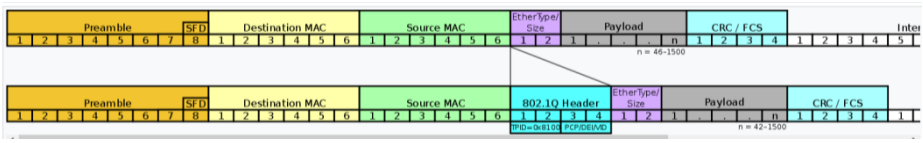

Fig 6. Estructura de la trama Ethernet y VLAN tagging según estándar IEEE 802.1Q, usado por FlowVisor para virtualizar usando la técnica de aislamiento de Reescritura de paquete [11].

FlowVisor asegura el aislamiento del ancho de banda mediante la reescritura de los rótulos de VLAN y puede asignar prioridades a las colas con el objetivo de Calidad de Servicio [12]. No obstante VLAN tagging fue creado para separación de redes LAN y no para garantizar la seguridad, por lo que las vulnerabilidades de las redes VLAN siguen vigentes en una red SDN virtualizada con FlowVisor.

Virtualización del Ancho de Banda: Vulnerabilidades y mitigación

Las vulnerabilidades de la virtualización del ancho de banda están relacionadas con las vulnerabilidades de las VLAN y todos los protocolos que intervienen en su administración. La mayoría de los ataques a VLANs se desarrollan en la Capa 2 de enlace de datos. Los ataques más comunes son VLAN Hopping, Double Encapsulation VLAN Hopping, VLAN Trunking Protocol, VLAN Management Policy Server / VLAN Query Protocol VQP, entre otros [13].

El ataque de VLAN Hopping consiste en acceder en forma no autorizada al tráfico y los recursos de otras VLAN, tiene como consecuencia que los paquetes traspasan de una VLAN a otra en el mismo switch. Esto puede ocurrir de dos formas [13]. En la primera forma, se ha establecido una comunicación TCP/IP en la misma VLAN, y se logra configurar el switch de forma tal que uno de los puertos pertenezca a una VLAN diferente. La comunicación no se interrumpe pues cada extremo tiene la dirección MAC del otro en la caché ARP y el bridge conoce la dirección MAC destino en el puerto señalado.

La segunda forma de VLAN Hopping ocurre cuando se introduce intencionalmente una entrada estática en la tabla ARP, esto requiere el conocimiento de la dirección MAC destino tal vez por acceso directo.

Mitigación. Este tipo de vulnerabilidad se puede mitigar deshabilitando la capacidad de autonegociación de las VLANs y filtrando la información sensible. Otra de las medidas es dehabilitar la característica de Auto-trunking para desalentar los ataques basados en una configuración troncal de los switches favorable.

VLAN Management Policy Server VMPS / openVMPS / VLAN Query Protocol VQP. Es un switch server que tiene mapeada la información de la VLAN y permite asignar dispositivos a cada VLAN en base a la dirección MAC y asignar puertos del switch a cada VLAN. Está destinado a la administración de la red pero se usa para implementar medidas de seguridad de bloqueo de acceso a direcciones MAC desconocidas. Cisco desarrolló el cliente VQP para consultar al server VMPS, y FreeRadius ha desarrollado la versión libre OpenVMPS. El sistema puede ser vulnerado mediante la ejecución remota de código debido a la falta de autenticación [14].

Mitigación. Para solucionar este tipo de problemas se recomienda el uso del estándar IEEE 802.1X Port-based Network Access Control (PNAC) que define los mecanismos de autenticación de los dispositivos que se conectan a una red LAN [15].

Estos son sólo algunos ejemplos de ataques que pueden completarse con ataques Media Access Control MAC, envenenamiento de ARP, ataques a Spanning Tree Protocol STP, etc, etc. En líneas generales los protocolos de administración deben ser seguros SSH, SCP, SSL a cambio de SNMP, TFTP, FTP, telnet. Otra de las recomendaciones es usar una VLAN dedicada para la administración de la red y que sólo lleve tráfico de administración, configurar VLAN Access Control List ACL para tener un registro de acceso, y configurar el acceso por IP set IP permit para los protocolos de administración.

3.2 Virtualización de la Topología

En una red SDN el controlador reconstruye la topología de la red en base a la información brindada por los protocolos de descubrimiento usados por los dispositivos en el Plano de Datos. OpenFlow Discovery Protocol OFDP es la aplicación de descubrimiento que se ejecuta en el sistema operativo de red NOX en una red SDN, basándose en el protocolo LLDP Link Layer Discovery Protocol [16].

LLDP Link Layer Discovery Protocol es un protocolo de Capa 2 de Enlace (Data Link Layer), de descubrimiento de dispositivos de red, independientemente del fabricante, que permite que los dispositivos conectados a la red LAN publiquen su identidad, capacidades y estado a sus vecinos, y descripto en el estándard IEEE 802.1AB [17]. Es un protocolo que no solicita respuesta y se ejecuta mediante la publicación del mensaje LLDPDU (LLDProtocol Data Unit) a una de las direcciones destino MAC Multicast (01:80:C2:00:00:00 - 01:80:C2:00:00:03 - 01:80:C2:00:00:0E), con Ether Type 0x88CC, dirigido a todos los nodos vecinos de la red. Estas direcciones MAC pertenecen al grupo definido en el estándar IEEE 802.1D como Bridge Filtered, significando que los paquetes con destino a estas direcciones no son retransmitidos [18]. Esto implica que el mensaje LLDP sólo se transmite a los nodos adyacentes y no es retransmitido.

Los paquetes de datos LLDP se componen de atributos de la forma tipo-longitud-valor TLV (Type-Length Value) que contienen información del dispositivo origen. Existen campos obligatorios y otros opcionales. Los obligatorios son Chassis ID TLV, Port ID TLV (puerto origen), TTL TLV y END of LLPDU TLV. Mediante TTL (Time to Live) se determina si el dispositivo está activo en la topología, TTL TLV distinto de cero, actualizándose la información periódicamente, o si se retira de la topología, TTL TLV igual a cero. END of LLPDU (Link Layer Protocol Data Unit) TLV determina el fin de la trama del protocolo. Los TLV opcionales son usados por

protocolos propietarios como Cisco Discovery Protocol, Foundry Discovery Protocol de Brocade y variantes como LLDP-MED (Media Endpoint Devices) que permite el descubrimiento de dispositivos de telefonía IP VoIP, video en tiempo real y localización de llamadas de emergencia. Los TLV opcionales están agrupados en tres categorías: administración básica (Port description, System capability, etc), específicos para organización según IEEE 802.1 (administración de VLANs) y específicos para organización según IEEE 802.3 (MAC/PHY configuración, LINK aggregation, etc). La **Figura 7** muestra los campos LLDPDU dentro de la trama MAC.

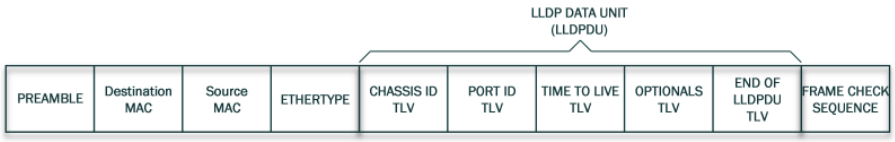

Fig 7. Estructura LLDP contenida en la trama MAC, mostrando los atributos TLV obligatorios.

Los paquetes LLDP se envían mediante el protocolo SNMP como se vio en la **Figura 5.** La información es almacenada en la base de datos MIB Management Information Base del dispositivo destino y un agente LLDP aprende la información guardada en las bases de datos de los dispositivos de la red y reconstruye la topología de la red en su totalidad [17]. De esta forma las aplicaciones de administración de la red descubren automáticamente los dispositivos conectados a la red mediante una consulta a la topología de la misma.

El protocolo OFDP al igual que LLDP tampoco solicita respuesta y se basa en los paquetes LLDP para crear una aplicación de descubrimiento de dispositivos de red que se comunican mediante OpenFlow u otro protocolo, lo que permite armar una topología híbrida. OFDP logra esto mediante la publicación de los mensajes a una dirección destino MAC Multicast estándar (01:23:00:00:00:01) con Ether Type 0x88CC. Esto implica que el switch retransmite los paquetes OFDP al resto de switches del backbone [19]. De esta manera un dispositivo habilitado con OFDP obtiene la información de toda la red no tan sólo de los dispositivos adyacentes. OFDP coexiste con LLDP dado que utilizan diferentes direcciones MAC para publicación de los mensajes.

Virtualización de Topología: Aislamiento

FlowVisor actúa de proxy entre el switch y el controlador y asegura el aislamiento entre segmentos virtualizados mediante la marcación de paquetes [7]. FlowVisor accede a la información de la topología de la red que mantiene OFDP y también accede a los paquetes enviados por el protocolo de descubrimiento LLDP, por lo que marca los mensajes del controlador y dispositivos pertenecientes a cada partición virtualizada.

Virtualización de la Topología: Vulnerabilidades y mitigación

En la implementación del protocolo LLDP ha sido reportada la vulnerabilidad referida particularmente al protocolo CDP [20]. El ataque afecta la integridad de la topología de la red (topology poisoning) llevando a disrupción del servicio. El atacante debe encontrarse dentro de la misma red y el objetivo es toda la red a la que pertenece. La causa de la vulnerabilidad ha sido clasificada como CWE-20 (Common Weakness Enumeration) debida a que el programa realiza una validación inadecuada de algún campo de atributo TLV [21]. El envenenamiento de la topología puede

llevarse a cabo de dos maneras, mediante la alteración de la localización del host (host location hijacking), o mediante la fabricación de un enlace (link spoofing).

El conjunto de protocolos de descubrimiento es cuestionado por exponer información de la red en texto plano que puede ser usada en forma maliciosa para ataques a la seguridad [22]. Los atributos TLV que contienen información sensible son los de administración y organización que llevan datos de direcciones IP de administración, descripción del sistema, VLAN tagging, etc.

Mitigación. Dadas las vulnerabilidades que presentan los protocolos de descubrimiento, existe el debate sobre las ventajas de deshabilitar el protocolo, pero los expertos recomiendan aprovechar los beneficios de contar con la topología de la red y usar solamente los campos de atributos que sean necesarios, deshabilitando el resto [23].

En el caso particular del protocolo de descubrimiento de Cisco CDP, todos los atributos TLV están habilitados por defecto para ser enviados en el mensaje del protocolo, por lo que es conveniente usar sólo los necesarios. También este protocolo permite configurar listas de atributos para ser aplicadas como filtros de atributos por interface con la que se realiza la comunicación [24]. Lo que indica que el administrador de red tiene las herramientas para realizar un ajuste fino de lo que el protocolo muestra y a quién lo muestra. Para esto hace falta un buen estudio del protocolo para entender su funcionamiento.

Con respecto a la vulnerabilidad de transmitir los atributos TLV en texto plano

Existen propuestas de agregar un código de autenticación criptográfico a cada paquete LLDP para proveer autenticación e integridad al paquete usando código HMAC basado en una clave que cambia en forma aleatoria [25].

3.3 Virtualización de CPU del Switch

Los dispositivos en el Plano de Datos tienen una capacidad limitada de procesamiento, por lo que las operaciones que requieren el uso de CPU deben ser monitoreadas para evitar agotamiento del recurso y disrupción del servicio.

Virtualización de CPU del Switch: Aislamiento

Los recursos de CPU de los switches son limitados, si a esto se le suma una alta demanda puede llevar a una disrupción de la red. Aunque el envío de paquetes continúa, la comunicación con OpenFlow se interrumpe, y lleva a un timeout del protocolo de descubrimiento LLDP, lo que lleva al controlador a creer que existe una disrupción en la red [12]. Las tareas de mayor carga para la CPU son [4]: mensajes de setup de un flujo nuevo, manejo de solicitudes del controlador, envío de paquetes en “slow path”, log de estado interno del dispositivo.

Flujo de mensaje nuevo. El establecimiento de un nuevo flujo significa que se envía al controlador un mensaje, esto consume recursos de CPU si es elevado el número de mensajes nuevos, originados tal vez por ataques a la seguridad. FlowVisor previene esta situación controlando la tasa de arribos, cuando supera un umbral FlowVisor usa OpenFlow para insertar una regla para descartar estos paquetes hasta que la tasa de arribos se normalice.

Solicitudes del controlador. FlowVisor limita la tasa de mensajes OpenFlow, no obstante no hace una discriminación por tipo de mensaje o de hardware.

Operaciones en el Slow-path. A diferencia de las operaciones en el fast-path realizadas en el kernel, las realizadas en el slow-path son las que se ejecutan en el espacio del usuario [5]. Este tipo de operaciones consume gran cantidad de recursos. FlowVisor previene estas situaciones reescribiendo las reglas para que el paquete sea enviado de la forma más directa usando operaciones del kernel.

Log de estatus. La CPU se usa para administrar contadores internos, procesos de eventos, etc. FlowVisor supervisa que estas tareas no consuman recursos de CPU destinados a funciones, no obstante esta tarea no está lo suficientemente diferenciada en FlowVisor.

Virtualización de CPU del Switch: Vulnerabilidades y mitigación

Según lo visto en la sección previa, FlowVisor se vale de OpenFlow para evaluar el aislamiento de la virtualización de CPU por lo que los temas de seguridad se centran en este protocolo.

3.4 Virtualización de Tráfico

La virtualización de tráfico permite asociar un determinado tráfico a una red virtual, segmentando el tráfico por direcciones de origen o destino, por usuarios, protocolo o clasificado por algún tipo de rótulo, en el espacio de la cabecera del mensaje.

Virtualización de Tráfico: Aislamiento

Para que el tráfico quede confinado en cada segmento virtualizado, FlowVisor reescribe los mensajes para que la red tenga control sobre su propio tráfico y no afecte otros segmentos virtualizados [7]. En el caso de reglas de control que no puedan ser reescritas, FlowVisor puede limitar la incidencia de estas reglas de control para que se ejecuten solamente sobre el tráfico de la red virtualizada. En el caso que las reglas no puedan ser modificadas, FlowVisor envía un mensaje al controlador indicando que esa entrada de flujo no va a ser agregada a la Tabla de Flujos.

Virtualización de Tráfico: Vulnerabilidades y mitigación

Para el aislamiento de tráfico FlowVisor usa recursos de OpenFlow por lo que las vulnerabilidades y su mitigación son las descriptas en la sección de OpenFlow. Dado que FlowVisor asegura el aislamiento de tráfico mediante la rotulación de paquetes, se han detectado vulnerabilidades donde el ataque proveniente de un controlador malicioso puede alterar los rótulos y por ende tener un controlar arbitrario de la totalidad del tráfico [26]. Si se limitara la acción del controlador impidiendo que sobreescriba la cabecera de los paquetes, aún tendrían la posibilidad de generar acciones, provocando inyección de paquetes en el tráfico de otra red virtual.

Una de las soluciones propuestas es usar virtualización del controlador para que cada controlador virtualizado tenga acción solamente sobre el tráfico que le corresponde.

Si se exceptúa como causante de controller spoofing a man-in-the-middle mediante algún tipo de control de acceso, queda por detectar la aplicación que pueda estar generando el ataque. Una forma de limitar la incidencia de las aplicaciones en las acciones del controlador es usando el paradigma de rol-based access control RBAC [27], que determina qué comandos se le permiten a cada aplicación en función del rol a cumplir.

3.5 Virtualización de las Tablas de Flujo

En redes SDN virtualizadas donde se comparten los recursos físicos de los routers entre los usuarios huéspedes también se comparten las Tablas de Flujo. Existen dos estratégias básicas para seleccionar la partición de las tablas, hard-partitioning que

asigna un número fijo de entrada de flujo a cada usuario, y soft-partitioning que asigna un número de entradas a la tabla de acuerdo a la demanda del usuario. Se han desarrollado métodos para evitar el monopolio que puede traer aparejada la alta demanda de entradas en la tabla de flujos [28].

Virtualización de las Tablas de Flujo: Aislamiento

El aislamiento en la virtualización de las tablas de flujo está dada por el hecho que cada huésped pueda hacer uso de la cuota que se le ha asignado sin que sea accedida por otro huésped. FlowVisor cuenta el número de entradas por cada segmento virtualizado y asegura que el número de entradas en la tabla de flujo no exceda un determinado límite [7]. Si esto ocurre se genera un mensaje de tabla llena.

FlowVisor incrementa un contador cuando una regla es insertada por el controlador en el switch, y decrementa el contador cuando la regla expira. Si una regla hace referencia a varios puertos de entrada, el caso es tratado en forma particular.

Virtualización de las Tablas de Flujo: Vulnerabilidades y mitigación

FlowVisor usa el protocolo OpenFlow para asegurar el aislamiento en la partición de las tablas de flujo por lo que las vulnerabilidades a la seguridad son las descriptas en la respectiva Sección.

4 Conclusión y temas de interés

Se ha mostrado un análisis de la seguridad en la virtualización de redes SDN discriminado por dimensión a virtualizar con el objetivo de brindar un panorama integrador de las potenciales amenazas en tema de seguridad. Si bien el análisis no es exhaustivo, da las pautas básicas en tema de seguridad para administrar una red SDN y aprovechar las ventajas de la virtualización.

La flexibilidad en la programación del flujo de la red y variedad en los servicios a desarrollar para mejorar la performance y seguridad de la red, tales como ruteo, firewalling, network Address translation, balance de cargas, etc trae aparejado el tema de la seguridad. La seguridad en una red SDN virtualizada parte de la base que las aplicaciones que se ejecutan en el plano de control han sido correctamente verificadas y validadas, no tan solo para cumplir con las especificaciones funcionales sino también con la no-funcionales en especial las referidas a seguridad. Al respecto se vieron las vulnerabilidades a la seguridad originadas en el desarrollo de aplicaciones en el Plano de Control que pueden desencadenar ataques al controlador del tipo controller spoofing [26] causando una denegación de servicio a la red en su totalidad. Otro aspecto importante a tener en cuenta es la compatibilidad y la interoperabilidad entre dispositivos en el Plano de Datos, que presenta desafíos para su integración y en temas de seguridad [3], y son posibles fuentes de futuros trabajos de investigación.

Referencias

[1] "RFC 7426 - Software-Defined Networking (SDN): Layers and Architecture Terminology." [Online]. Available: https://datatracker.ietf.org/doc/rfc7426/. [Accessed: 14-Apr-2019].

[2] "Software-Defined Networks and OpenFlow - The Internet Protocol Journal, Volume 16, No. 1," *Cisco*. [Online]. Available: https://www.cisco.com/c/en/us/about/press/internet-protocol-journal/back-issues/table-contents-59/161-sdn.html. [Accessed: 06-May-2019].

[3] Y. Jarraya, T. Madi, and M. Debbabi, "A Survey and a Layered Taxonomy of Software-Defined Networking," *IEEE Commun. Surv. Tutor.*, vol. 16, no. 4, pp. 1955–1980, Fourthquarter 2014.

[4] P. Göransson, C. Black, and T. Culver, "Chapter 5 - The OpenFlow Specification," in *Software Defined Networks (Second Edition)*, P. Göransson, C. Black, and T. Culver, Eds. Boston: Morgan Kaufmann, 2017, pp. 89–136.

[5] A. Ranjbar, M. Antikainen, and T. Aura, "Domain Isolation in a Multi-tenant Software-Defined Network," in *2015 IEEE/ACM 8th International Conference on Utility and Cloud Computing (UCC)*, 2015, pp. 16–25.

[6] A. Blenk, A. Basta, M. Reisslein, and W. Kellerer, "Survey on Network Virtualization Hypervisors for Software Defined Networking," *IEEE Commun. Surv. Tutor.*, vol. 18, no. 1, pp. 655–685, Firstquarter 2016.

[7] R. Sherwood *et al.*, "FlowVisor : A Network Virtualization Layer," 2009.

[8] P. Göransson, C. Black, and T. Culver, "Chapter 1 - Introduction," in *Software Defined Networks (Second Edition)*, P. Göransson, C. Black, and T. Culver, Eds. Boston: Morgan Kaufmann, 2017, pp. 1–21.

[9] P. Porras, S. Shin, V. Yegneswaran, M. Fong, M. Tyson, and G. Gu, "A Security Enforcement Kernel for OpenFlow Networks," in *Proceedings of the First Workshop on Hot Topics in Software Defined Networks*, New York, NY, USA, 2012, pp. 121–126.

[10] "IEEE Standard for Local and Metropolitan Area Network--Bridges and Bridged Networks," *IEEE Std 8021Q-2018 Revis. IEEE Std 8021Q-2014*, pp. 1–1993, Jul. 2018.

[11] "IEEE 802.1Q," *Wikipedia*. 12-Feb-2019.

[12] R. Sherwood, G. Gibb, K. Yap, M. Casado, N. Mckeown, and G. Parulkar, "FlowVisor: A Network Virtualization Layer," 2009.

[13] A. Abdou, P. C. van Oorschot, and T. Wan, "Comparative Analysis of Control Plane Security of SDN and Conventional Networks," *IEEE Commun. Surv. Tutor.*, vol. 20, no. 4, pp. 3542–3559, Fourthquarter 2018.

[14] "CVE-2005-4714 : Format string vulnerability in the vmps_log function in OpenVMPS (VLAN Management Policy Server) 1.3 allows remote attac." .

[15] "IEEE 802.1X," *Wikipedia*. 06-Mar-2019.

[16] N. Gude *et al.*, "NOX: Towards an Operating System for Networks," *SIGCOMM Comput Commun Rev*, vol. 38, no. 3, pp. 105–110, Jul. 2008.

[17] "IEEE Standard for Local and Metropolitan Area Networks– Station and Media Access Control Connectivity Discovery," *IEEE Std 8021AB-2009 Revis. IEEE Std 8021AB-2005*, pp. 1–204, Sep. 2009.

[18] "IEEE Standard for Local and metropolitan area networks: Media Access Control (MAC) Bridges," *IEEE Std 8021D-2004 Revis. IEEE Std 8021D-1998*, pp. 1–281, Jun. 2004.

[19] "OpenFlowDiscoveryProtocol – GENI: geni." [Online]. Available: https://groups.geni.net/geni/wiki/OpenFlowDiscoveryProtocol#no1. [Accessed: 02-May-2019].

[20] "NVD - CVE-2018-0395." [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2018-0395#. [Accessed: 30-Apr-2019].

[21] "CWE - CWE-20: Improper Input Validation (3.2)." [Online]. Available: http://cwe.mitre.org/data/definitions/20.html. [Accessed: 30-Apr-2019].

[22] T. Alharbi, M. Portmann, and F. Pakzad, *The (In)Security of Topology Discovery in Software Defined Networks*. 2015.

[23] "Is there any reason for CDP to be disabled in the Network?," 20-Apr-2011. [Online]. Available: https://community.cisco.com/t5/switching/is-there-any-reason-for-cdp-to-be-disabled-in-the-network/m-p/1687301#M174654. [Accessed: 03-May-2019].

[24] "Catalyst 4500 Series Switch Software Configuration Guide, 12.2(53)SG - Configuring LLDP and LLDP-MED [Cisco Catalyst 4500 Series Switches]," *Cisco*. [Online]. Available: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/53SG/configuration/config/swlldp.html. [Accessed: 29-Apr-2019].

[25] S. Hong, L. Xu, H. Wang, and G. Gu, "Poisoning Network Visibility in Software-Defined Networks: New Attacks and Countermeasures.," in *NDSS*, 2015, vol. 15, pp. 8–11.

[26] V. T. Costa and L. H. M. K. Costa, "Vulnerabilities and solutions for isolation in FlowVisor-based virtual network environments," *J. Internet Serv. Appl.*, vol. 6, no. 1, p. 18, Aug. 2015.

[27] P. A. Porras, S. Cheung, M. W. Fong, K. Skinner, and V. Yegneswaran, "Securing the software defined network control layer.," in *NDSS*, 2015.

[28] Y. Lin, T. Liu, J. Chen, and Y. Lai, "Soft Partitioning Flow Tables for Virtual Networking in Multi-Tenant Software Defined Networks," *IEEE Trans. Netw. Serv. Manag.*, vol. 15, no. 1, pp. 402–415, Mar. 2018.