Perspectiva general de la ciberseguridad en los OSI layers

Albert Bausili Fernández
Noa-Yu Ventura Vila

Índex

Introducción

Hoy en día vivimos en un mundo interconectado a través de Internet, y nos hemos acostumbrado a usarlo sin preocuparnos, en la mayor parte de los casos, de la implementación o el funcionamiento de éste.

Esa aparente ignorancia en la mayor parte de la población es una de las principales causas de vulnerabilidades y fallos de seguridad en los sistemas informáticos modernos.

En este trabajo hemos intentado realizar un repaso transversal recorriendo los 7 layers OSI y destacando las medidas de ciberseguridad implementadas en los principales protocolos de cada layer y por otro lado sus fallos y agujeros de seguridad, si los hay. También hemos incorporado información sobre posibles soluciones que se han desarrollado para combatir estos problemas.

Layer 1

Descripción

El layer 1 o layer físico es el primero y el mas cercano al hardware. Las implementaciones protocolos de este layer generalmente se implementan directamente en el hardware.

Esta característica limita en gran medida el desarrollo de protocolos “complejos” y/o la evolución de éstos, ya que al complicar los protocolos o actualizarlos requiere, en la mayor parte de casos de una fuerte inversión en nuevo hardware que a parte de los costes directos también comporta para las corporaciones costes formativos para los empleados que los usaran y mantendrán.

Estos motivos han sido en gran parte los causantes de los problemas de seguridad en este nivel, pero no los únicos, ya que el principal problema para la seguridad es que generalmente se tratan de protocolos definidos hace muchos años y, por lo tanto, están concebidos para unos propósitos y con unas necesidades que distan mucho de las actuales, pues en esos tiempos no se le daba mucha importancia a la ciberseguridad.

Esto ha provocado que hoy en día que los sistemas se hacen cada vez más robustos y se invierte más en seguridad los atacantes malintencionados hayan encontrado una “vía fácil” de encontrar agujeros que se trata de este primer layer.

En este layer se frecuenta el uso de ataques de “downgrade”.

Layer 2

Descripción

El layer 2, o layer de enlace de datos, es el segundo y centrado en la interconexión entre nodos adyacentes.

Esta capa se encuentra en una situación similar a la anterior, aunque sin llegar a la problemática de ésta. En éste caso el principal problema es que los propios desarrolladores de los protocolos, ya sea por su antigüedad o por sus ideas sobre donde se suelen situar los ataques provocan que se suela dejar muchas veces la seguridad de lado y en gran parte de los protocolos no hay directamente medidas de seguridad.

Por suerte, en los últimos años se ha empezado a coger conciencia de esto y fabricantes como Cisco, entre otros, han estado definiendo protocolos "parche" para intentar solucionar estos problemas, pues una brecha en este layer puede, y suele, comportar una brecha en parte o incluso todos los protocolos superiores. (Figura 1)

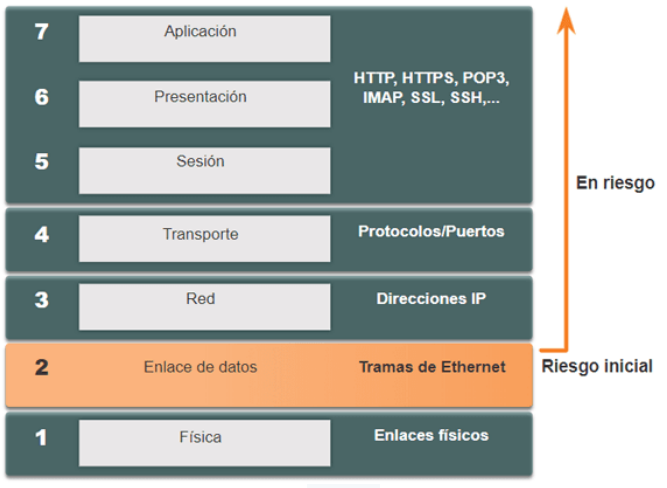

Figura 1. Representación gráfica del posible riesgo que comporta una brecha en el layer 2

Protocolos

ARP

El protocolo Address Resolution Protocol (ARP), es uno de los protocolos mas comunes y usados en el layer 2, pero debido a su antigüedad, éste es un protocolo de "texto en claro" sin ninguna medida de seguridad incluida.

El ataque más común se llama ARP "spoofing", y consiste en la suplantación de la MAC de un dispositivo de la red recopilando o modificando información o hasta llegar a vulnerar firewalls o otras medidas de seguridad.

Su principal solución actualmente fue propuesta por Cisco, y se llama DAI.

DAI

DAI o Dynamic Arp Inspection, es una medida de seguridad sencilla pero eficaz en la mayor parte de casos. Consiste en comprobar la veracidad de la tabla de traducciones MAC-IP proporcionada por el DHCP snooping.

ATM

El protocolo ATM es un protocolo multi-layer desarrollado para implementar WANs y esta compuesto por conmutadores y enlaces punto a punto de larga distancia (Figura 2). Fue muy popular hasta finales del milenio que perdió popularidad en favor de las implementaciones TCP/IP, en parte, puede que fuera por la falta de posibilidad de añadir seguridad en el protocolo así como IP disponía del Ipsec.

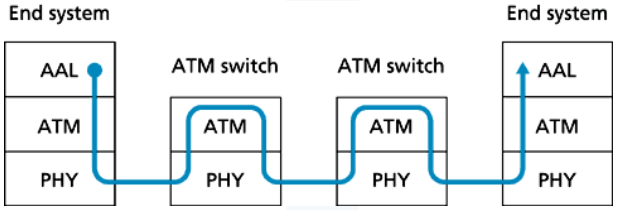

Figura 2. Representación esquemática del envío de un datagrama usando ATM.

CDP

CDP o Cisco Discovery Protocol, se trata de un protocolo desarrollado por cisco. Este protocolo envía información a dispositivos directamente conectados referente al nombre del dispositivo, plataforma, versión, dirección IP…

Es usado y implementado por empresas como VMware.

Pero debido nuevamente a su antigüedad no dispone de medidas de seguridad, pero esto Cisco lo solucionó años mas tarde con el lanzamiento de SCDP.

SCDP

SCDP o Secure Discovery Protocol, se trata de un protocolo totalmente equivalente al anterior, pero con la implementación y uso de campos TLV.

Estos campos se envían a través del protocolo permitiendo a los usuarios enviar el Type, Length i Value de la información que se envía a una interfaz en concreto, permitiendo filtrar la información que se envía a través del protocolo.

NDP

Neighbor Discovery Protocol, se trata de un protocolo utilizado principalmente en IPv6 y se encarga de recolectar la información necesaria para la comunicación de redes.

Debido a su antigüedad, se trata de un protocolo sin medidas de seguridad y por lo tanto, vulnerable.

Para solucionar esto se desarrollo y implemento el protocolo SEND.

SEND

Este protocolo funciona de forma equivalente al NDP tradicional pero añadiendo Cryptographically Generated Addresses (CGA) y Resource Public Key Infrastructure (RPKI) que le proporcionan un buen nivel de seguridad.

WIFI

WIFI o IEEE 802.11 es un popular estándar de conexión a nivel 2 Wireless, pero por su propia naturaleza es inseguro. Su funcionamiento es parecido al del ethernet. A lo largo de la historia ha tenido diversos protocolos de seguridad para intentar hacerlo seguro:

Wired Equivalent Privace (WEP):

Fue el primer intento de añadir seguridad al protocolo, pero debido a su antigüedad ya no es seguro. Funcionaba con encriptación.

WiFi Protected Acces (WPA):

Es un protocolo creado para intentar mitigar los fallos de su predecesor. Usa medidas de encriptación como TKIP y PSK. Hoy en día tampoco es seguro.

WiFi Protected Acces (WPA2):

Usa medidas de encriptación y creación de claves únicas a partir del SSID del usuario i la password. Hoy en día es moderadamente seguro, aunque se recomienda evitarlo.

WiFi Protected Acces (WPA3):

Usa medidas innovadoras de seguridad que le otorgan una protección adicional contra ataques de fuerza bruta, protocolos de hand-shaking y encriptación individualizada de datos.

WIMAX

WIMAX es un protocolo que se desarrollo para intentar mejorar la distancia y la velocidad del estándar WIFI tradicional. Debido a su utilidad pese a tener diversos problemas de vulnerabilidades, se están desarrollando protocolos y parches para este protocolo.

La principal ventaja en cuanto a ciberseguridad respecto al protocolo WIFI tradicional es el soporte que ofrece para la encriptación AES.

Layer 3

Descripción

El layer 3, o capa de red, es el tercer layer y se encarga del envío de paquetes a través de routers adyacentes.

Este es el primer nivel que una gran parte de los protocolos incluyen medidas de seguridad.

VRRP

VRRP o Virtual Router Redundancy Protocol, es un protocolo no propietario creado, como bien indica su nombre, para poder realizar implementaciones con redundancia de routers y así minimizar el impacto de la caída de uno de estos. (Figura 3)

Los paquetes pasan generalmente por un proceso de autentificación (En VRRPv2) a través de hashes MD5 y de verificaciones del paquete para evitar que se envíen datos que no correspondan con los necesarios.

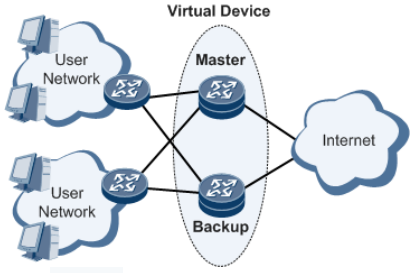

Figura 3. Representación esquemática del protocolo VRRP.

IP

IP o Internet Protocol, es el popular y conocido protocolo de comunicación para transmitir datos.

Debido a su antigüedad en el estándar Ipv4 no habían medidas de seguridad aplicadas y no fue hasta el estándar Ipv6 que ya se empezaron a aplicar, así que para asegurar Ipv4 se creo Ipsec.

IPsec

Ipsec se trata de un conjunto de protocolos con el objetivo de asegurar las comunicaciones usando IPv4.

Se encargan de autenticar y cifrar cada paquete IP y también incluyen la opción de establecer claves de cifrado.

OSPF

OSPF o Open Shortest Path First es el protocolo mas utilizado para el enrutamiento de paquetes dentro de los AS y especialmente a dentro de redes de consumidores y corporaciones.

Debido a su antigüedad no incorpora demasiada seguridad.

Incluye principalmente herramientas de autentificación.

IS-IS

IS-IS se trata de un protocolo muy similar a OSPF, creado para intentar remediar sus principales problemas. En referencia a seguridad, incorpora mejoras como por ejemplo el uso de TLV y mejoras en la autentificación de éstos.

Layer 4

Descripción

El layer 4, se tarta del nivel de transporte, este nivel es el que usan las aplicaciones para comunicarse.

TCP

TCP o Transmission Control Protocol, se trata de uno de los principales protocolos de internet moderno. Se trata de un protocolo orientado a conexión, mediante el uso del 3-way handshaking (Figura 4), y que representa la base de muchos otros protocolos de layers superiores. Debido a su antigüedad solo incorpora medidas de checksumming, insuficientes para hacerlo seguro.

La principal manera para solucionar sus problemas es mediante el uso de Firewalls.

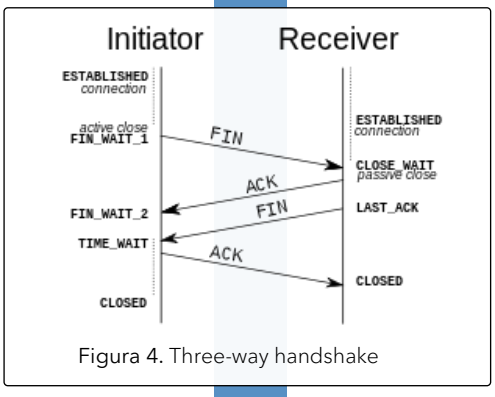

Figura 4. Three-way handshake

Layer 5

Descripción

Este layer permite establecer y gestionar conexiones entre el usuario y las aplicaciones. Principalmente consisten en packet requests and replies entre las aplicaciones.

NCP

NCP está compuesto por otros protocolos según el uso que le quieras dar. Por ejemplo, Encryption Control Protocol (ECP) es uno de ellos y se usa para configurar, gestionar y controlar algoritmos de encriptación. También están Compression Control Protocol (CCP) para configurar, gestionar y controlar la compresión de datos en una conexión, y Briding Control Protocol (BCP) para configurar, gestionar y controlar módulos.

Layer 6

Descripción

Este layer es lo que los programadores describiríamos como bajo nivel, porque el presentation layer es el que contiene y traduce las estructuras de datos a los bytes, strings, etc. También es donde comúnmente se hace la encriptación de paquetes, aunque ésta también se puede hacer previamente en los layers 7, 3, 4 y 5.

SSL/TLS

SSL/TSL cifra los datos que se transmiten por la red, tiene un proceso de autenticación entre dispositivos y verifica la integridad de los datos antes de alcanzar el destinatario asignado. La diferencia entre SSL y TLS en cuanto a implementación, uso y utilidad es nula.

Layer 7

Descripción

Este layer especifica la abstracción de aplicaciones. Se usan dos modelos distintos: Internet Protocol Suite (TCP/IP) y Open Systems Interconnection (OSI model).

TCP/IP:

Protocolos de comunicación y establecimiento de conexiones, los cuales dependen de las tecnologías y protocolos implementados en el layer 3 para establecer conexiones host-to-host.

OSI model:

En este caso el layer 7 está más enfocado a mostrar en la interfaz del usuario la información que ha llegado a través de los otros layers.

DHCP

Este protocolo no tiene implementado ningún tipo de seguridad, ya que por ejemplo un tercero podría tomar control del servidor y enviar a sus usuarios información no legítima.

HTTP/HTTPS

HTTP no es completamente seguro, aunque dispone de headers de seguridad que pueden hacerlo más seguro: strict-transport-security (HSTS) fuerza la conexión a ussar HTTPS en vez de HTTP, content-security-policy (CSP) te permite controlar muchos parámetros de tu web, así que es útil contra ataques XSS, x-frame-options, etc.

FTP/SFTP

FTP se usa muy poco hoy en día, pero aún hay gente que lo usa. No es demasiado seguro enviar archivos, pero tiene autorización a nivel de usuario, ya que el fichero /etc/ftpusers contiene los usuarios de la máquina que no pueden acceder a FTP.

La solución más sencilla es combinar ftp con ssh, lo que significa que estaríamos usando el protocolo SFTP, que dispone de los servicios de ftp con un incremento de seguridad adicional: encriptar los mensajes que se envían. Otra opción sería usar SSL conjuntamente con FTP.

Telnet

Es un protocolo inseguro, ya que la información enviada no está encriptada. Aun así, se puede combinar con ssh para hacer la conexión más segura. Para hacer telnet más seguro puedes proteger el puerto que usa telnet con SSL, pero esta solución no resuelve la posibilidad de una tercera persona capturando tus paquetes en la red.

SSH

Este protocolo es el método de acceso remoto a un servidor más seguro contra ataques de cifrado que hay hasta la fecha, ya que la información que se envía está cifrada. También sirve como un soporte para asegurar protocolos inseguros.