UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

Seguridad e Integridad de la transferencia de datos

Integrantes:

Diego Agulló

Rol: 201130047-5.

María Constanza Guerra

Rol: 201130013-0

Felipe Silva

Rol: 201130020-3

Ricardo Vivanco

Rol: 201130024-6

Vaparaíso, 23 de Julio de 2012

Resumen:

En este informe, se pretende dar a conocer cómo es posible interceptar o vulnerar la privacidad de las conexiones en las redes de computadores, cómo se llaman estos ataques y cómo operan, a su vez, y acorde a los cambios tecnológicos que permiten la mejora de la confiabilidad en estas conexiones, se pretende también mostrar las soluciones actuales frente a estos ataques.

Esta seguridad en las conexiones se verá a través de múltiples capas, ya sea en la capa aplicación, capa de transporte, capa de red y capa de enlace. No puede haber un método de seguridad global, que abarque todas las capas, debido a que todas ellas operan de manera independiente, por lo que no están involucradas las unas de las otras.

Introduccion:

En tiempos actuales, el tema de la transferencia confiable de datos ha sido un tópico amplio para desarrollar, debido a que cada vez la cantidad e intensidad de ataques informáticos, y esto conlleva a tener que estar constantemente mejorando las técnicas de seguridad en internet en general.

En este informe, empezaremos explicando las principales técnicas de ataques informáticos, enfocados principalmente a la transferencia de datos, para luego dar paso a las principales técnicas de seguridad en las capas involucradas en el proceso: Aplicación, Transporte, Red y Enlace.

Seguridad de transferencia de datos

Los problemas en seguridad de transferencia de datos más comunes no son sólo las pérdidas de paquetes sino que también lo son los distintos tipos de ataques informáticos o ciberataques siendo los siguientes tres tipos: DDoS, MItM, 0-day; los más comunes.

Ataque de denegación de servicios: Denial of Service (DoS) consiste en impedir el uso de un servicio de red a los usuarios que les compete. En general provoca la pérdida de conexión a la red por sobre consumo de ancho de banda o sobrecarga de recursos computacionales; haciendo que el servidor objetivo se sobrecargue impidiendo que éste entregue sus servicios. Se denomina DDoS a un ataque por denegación a mayor escala (Distributed Denial of Service) con un gran flujo de información desde varios puntos de conexión (generalmente haciendo uso de **botnet**)
Existen tres principales métodos de ataque DDoS: SYN FLOOD, ICMP FLOOD y UDP FLOOD; En términos generales, SYN FLOOD consiste en el envió de una gran cantidad de paquetes petitorios para establecer conexión cliente/servidor predispuestos a fallar debido a la falsificación del origen de estos (**IPSPOOFING**) consumiendo recursos y máximo de conexiones entrantes. ICMPFLOOD pretende agotar el ancho de banda con envíos continuos de **paquetes tipo ICMP** que obligan al objetivo a enviar una respuesta, su efectividad depende de la relación de la capacidad de procesamiento víctima/atacante. UDPFLOOD al igual que los anteriores actúa con el envió de gran cantidad de paquetes, esta vez son UDP fácilmente con suplantación de identidad.

Ataque Man In the Middle: Dentro de una red funcionando bajo un switch, mediante protocolos ARP esto es; verificación de dirección MAC e IP de la tarjeta de red de los ordenadores comprometidos. Su premisa básica es el redireccionamiento y reenvío (y posible modificación) de datos alterando dirección MAC en las tablas ARP de cada computador (**ARPSPOOFING**), esto es posible ya que el protocolo ARP no tiene ningún mecanismo de validación de datos por tanto si recibe nuevos datos simplemente los acepta y actualiza por parámetros ya existentes en la tabla . De esta forma el ordenador atacante se posiciona entre el tráfico las víctimas (de ahí el nombre). No se altera la dirección IP para no levantar sospechas.

Explotaciones día cero (0-day Exploits): Consiste en la búsqueda de fallas o vulnerabilidades en aplicaciones informáticas desconocidas por los desarrolladores para sacar provecho de éstas o atacar al sistema comprometido. Este tipo de explotación (**Exploit**), que puede ser una pieza de software o una secuencia de código con el fin de causar fallos o errores, circula entre los potenciales atacantes hasta que es publicado y posteriormente parchado por los desarrolladores. Este intervalo entre la publicación de la amenaza y del parche que la soluciona se conoce como la "ventana de vulnerabilidad" ; es aquí donde ocurren los ataques, por tanto el tiempo de la ventana depende de la reacción de los propios responsables del programa bajo amenaza.

Seguridad en la Capa Aplicación:

Una de las capas del stack TCP/IP en las cuales se trabaja la seguridad de transferencia de datos es en la Capa de Aplicación, donde el método principal es a través de los algoritmos de encriptación.

Los Algoritmos Criptográficos o de Encriptación en las redes de computadores son funciones que modifican un mensaje respecto a una clave y ciertos métodos aritméticos. La finalidad de dichos algoritmos es hacer que el mensaje sea ininteligible o no funcional sin la llave y el algoritmo, para evitar que se revele su contenido. El primer algoritmo de encriptación conocido data de los tiempos de Julio César, el cual consistía en tomar el número de orden de una letra, sumarle tres, y cambiarla por la letra en ese lugar. Por ejemplo, la palabra *"fortaleza"*, con el algoritmo de César, quedaría *"iruwdohcd"*.

Existen tres tipos de algoritmos de encriptación:

Algoritmos Simétricos: En esos algoritmos se usa una misma clave para cifrar y para descifrar. Las dos partes que se comunican mediante el cifrado simétrico deben estar de acuerdo en la clave a usar de antemano. Una vez de acuerdo, el remitente cifra un mensaje usando la clave, lo envía al destinatario, y éste lo descifra usando la misma clave. Un buen sistema de cifrado pone toda la seguridad en la clave y ninguna en el algoritmo. En otras palabras, no debería ser de ninguna ayuda para un atacante conocer el algoritmo que se está usando. Sólo si el atacante obtuviera la clave, le serviría conocer el algoritmo. Un ejemplo de este tipo de algoritmo es el algoritmo de Rijndael, el cual utiliza claves

entre 128 y 256 bits, que a la vez sean múltiplos de 32.

El principal problema con los sistemas de cifrado simétrico no está ligado a su seguridad, sino al intercambio de claves. Una vez que el remitente y el destinatario hayan intercambiado las claves pueden usarlas para comunicarse con seguridad, pero ¿qué canal de comunicación que sea seguro han usado para «comunicar» la clave entre ellos? Sería mucho más fácil para un atacante intentar interceptar una clave que probar las posibles combinaciones del espacio de claves.

Algoritmos Asimétricos: Los algoritmos asimétricos o de clave pública se inventaron con el fin de evitar por completo el problema del intercambio de claves. Un sistema de cifrado de clave pública usa un par de claves para el envío de mensajes. Las dos claves pertenecen a la misma persona a la que se ha enviado el mensaje. Una clave es *pública* y se puede entregar a cualquier persona. La otra clave es *privada* y el propietario debe guardarla para que nadie tenga acceso a ella. El remitente usa la clave pública del destinatario para cifrar el mensaje, y una vez cifrado, sólo la clave privada del destinatario podrá descifrar este mensaje. Los sistemas de cifrado de clave pública se basan en funciones-trampa de un sólo sentido. Una función de un sólo sentido es aquélla cuya computación es fácil, mientras que invertir la función es extremadamente difícil. Como con los sistemas de cifrado simétricos buenos, con un buen sistema de cifrado de clave pública toda la seguridad descansa en la clave. Por lo tanto el tamaño de la clave es una medida de seguridad del sistema, pero no se puede comparar el tamaño del cifrado simétrico con el de un cifrado de clave pública para medir la seguridad, ya que éste dependerá del tipo de cifrado. Un ejemplo de un algoritmo asimétrico es RSA, cuya manera de funcionar radica en la factorización de números enteros.

Funciones Hash y Firmas Digitales: Una función hash es una función múltiple que asigna su entrada a un valor dentro de un grupo finito. Por regla general este grupo es un rango de números naturales. Una firma digital en un documento es el resultado de aplicar una función hash al documento. Para que sea de utilidad, la función hash necesita satisfacer dos propiedades importantes. Primero, debería ser difícil encontrar dos documentos cuyo valor para una función hash sea el mismo. Segundo, dado un valor hash debería ser difícil de recuperar el documento que produjo es valor. Como alternativa está el uso de funciones hash designadas para satisfacer estas dos importantes propiedades. MD5 es un ejemplo de este tipo de algoritmos. Al usar uno de estos algoritmos, un documento se firma con una función hash, y el valor del hash es la firma. Otra persona puede comprobar la firma aplicando también una función hash a su copia del documento y comparando el valor hash resultante con el del documento original. Si concuerdan, es casi seguro que los

documentos son idénticos.

Transferencia de datos en la capa de transporte

La Capa de transporte es la encargada de la comunicación lógica entre procesos
Dentro de los protocolos de esta capa en internet podernos encontrar el protocolo TCP (orientado a conexión), el cual se caracteriza por realizar una entrega confiable y en orden de los datos.

Protocolos de seguridad a nivel capa de transporte: SSL y TLS

SSL (Secure Sockets layer): Es un protocolo desarrollado por Netscape que utiliza certificados digitales para establecer conexiones seguras en internet.
Este protocolo fue sucedido por TLS (Transport Layer Security).Las versiones TLS están basadas en SSL y son similares en el modo de operar.

Protocolo TLS (Transport Layer Security): Es un protocolo que ofrece la privacidad e integridad de los datos entre dos aplicaciones que se comunican. Este protocolo está compuesto por dos capas: el protocolo TLS Record y el protocolo TLS Handshake.

- TLS Record: provee una conexión segura y cuenta fundamentalmente con dos propiedades: Conexión privada y confiable.
- TLS Handshake: permite que el cliente y el servidor negocien el cifrado de datos .Este protocolo posee 3 propiedades básicas: Autenticada asimétricamente o de clave pública además puede ser optativa la autenticación, negociación secreta y fiable.

Ambos protocolos permiten al usuario confiar información privada ya que los datos son
Ocultos mediante métodos criptográficos. Estos protocolos son utilizados en páginas web que necesiten resguardar información privada.

Funcionamiento de SSL: EL cliente y el servidor entran en el proceso de Handshake, cuando el Handshake termina se establece la conexión segura, posteriormente se utilizan llaves para cifrar o descifrar hasta que la conexión se termine

Certificados SSL: Certificado digital de seguridad utilizado por SSL, es otorgado por una autoridad certificadora la cual se encarga de verificar la identidad del poseedor del certificado. El navegador web recibe e interpreta este certificado, posteriormente verifica su validez e informa al usuario indicando que se realiza una conexión segura.

Punto débil de la conexión SSL/TLS: Es importante saber que aunque accedamos únicamente a sitios seguros los protocolos no garantizan un 100% de efectividad, ya que pueden ser vulnerados.

Seguridad en la capa de enlace y de red

En las redes de computadores, no basta con protegerse a nivel de la capa de aplicación, debido a que las capas funcionan como módulos independientes, cualquier intervención hecha en los routers o los switches pueden comprometer al resto de las capas, sin que ellas lo noten.

Es por eso, que en la actualidad la mayoría de los hubs y switches cuentan con la implementación frente a estos ataques maliciosos.

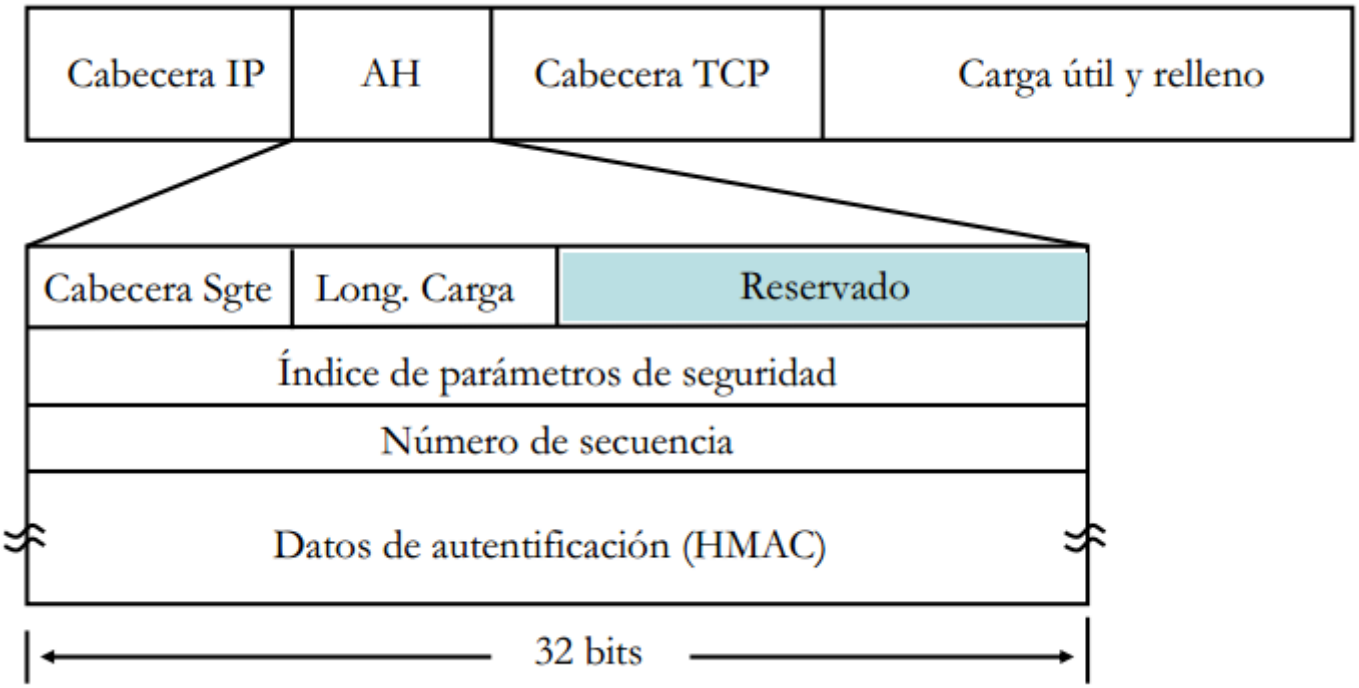
Dentro de la capa de enlace, para ataques basados en la falsificación de MAC y de tablas ARP, tales como el DDoS y Man In The Middle, la solución se encuentra en el control y bloqueo de puertos. Esto se encuentra en la mayoría de los switches de gama media y alta, y permite:

- Restringir el acceso a los puertos según la MAC.
- Restringir el número de MACs por puerto.

- Reaccionar de diferentes maneras a violaciones de las restricciones anteriores (ya sea enviando una alerta o deshabilitando el puerto).
- Establecer la duración de las asociaciones entre MAC y puerto.

También, a nivel de enlace, se ha tratado de definir dónde establecer la seguridad de la conexión en el canal. El resultado: IPsec (Internet Protocol Security), un conjunto de protocolos que aseguran las conexiones en la capa IP. Entre estas medidas, se incluye una cabecera de autenticación (Authentication Header) a nivel IP, esta cabecera ocupa un largo de 32 bits.

IPsec funciona mediante el intercambio de claves entre los comunicadores, de esta manera, se negocian las opciones y se llega al intercambio de una clave para la sesión.



Entre los datos de la cabecera de autentificación se encuentran:

- Cabecera siguiente: indica qué protocolo se ocupa para transferir los datos
- Longitud de carga: Tamaño del paquete AH
- Espacio reservado para uso futuro.

- Security Parameters Index (SPI): Indica los parámetros de seguridad que, en combinación con la dirección IP, identifican la asociación de seguridad implementada con este paquete.
- Número de secuencia: Utilizado para evitar ataques de repetición.
- HMAC: Contiene el valor de verificación de integridad (ICV) necesario para autenticar el paquete, puede contener relleno.

Pero, ¿qué sucede con la seguridad en la capa de enlace, es importante también?

Sí, es igual de importante, sobre todo si el medio es inalámbrico, es por eso, que en un primer instante se definió el WEP (Wired Equivalence Privacy) que ocupa un algoritmo de cifrado de tipo RC4, al poco tiempo, por la simplicidad de este algoritmo, fue desaprobado como un mecanismo de privacidad inalámbrico en el año 2004, para luego dar paso a WPA (Wi-Fi Protected Access), donde el servidor reparte claves diferentes a los usuarios. WPA implementa TKIP (Temporal Key Integrity Protocol), que utiliza el mismo algoritmo que WEP (RC4), pero construye las claves de manera diferente.

Actualmente el estándar a nivel de capa de enlace es WPA2, el sucesor que corrige las vulnerabilidades que se encuentran en WPA, WPA2 utiliza el algoritmo de encriptado AES.

Conclusion:

Las actuales implementaciones de seguridad en múltiples capas ha permitido generar una mayor confianza en la transferencia de datos, sobre todo en estos tiempos, cuando se es más vulnerable a ataques debido a la gran facilidad que se tiene para obtener software malicioso. Es por eso que las medidas de seguridad que han sido certificadas por el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE en inglés), son cada vez más exigentes.

Con la masificación del Wi-fi a nivel comercial y residencial, se ha tenido que ser más estricto en cuanto a seguridad a nivel de capa de red, ya que las ondas electromagnéticas que fluyen en el medio en el que operan las redes inalámbricas son fácilmente interceptables por cualquier tercero que pueda “escuchar” estas ondas.

Anexos:

Glosario:

- Botnet: Término que hace referencia a un conjunto de *robots informáticos*, que se ejecutan de manera autónoma y automática. El artífice de la botnet (llamado pastor) puede controlar todos los ordenadores/servidores infectados de forma remota.
- IP Spoofing: Suplantación de IP. Consiste básicamente en sustituir la dirección IP origen de un paquete TCP/IP por otra dirección IP a la cual se desea suplantar. Esto se consigue generalmente gracias a programas destinados a ello.
- Paquetes ICMP: es el sub protocolo de control y notificación de errores. Como tal, se usa para enviar mensajes de error, indicando por ejemplo que un servicio determinado no está disponible o que un router o host no puede ser localizado.
- ARP Spoofing: Suplantación de identidad por falsificación de tabla ARP. Se trata de la construcción de tramas de solicitud y respuesta ARP modificadas con el objetivo de falsear la tabla ARP (relación IP-MAC) de una víctima y forzarla a que envíe los paquetes a un host atacante en lugar de hacerlo a su destino legítimo.
- Exploit: Es una pieza de software, o una secuencia de comandos con el fin de causar un error o un fallo en alguna aplicación, a fin de causar un comportamiento no deseado o imprevisto en los programas informáticos, hardware, o componente electrónico (por lo general computarizado). Con frecuencia, esto incluye cosas tales como la toma de control de un sistema de cómputo o permitir la escalada de privilegios o un ataque de denegación de servicio.

Algoritmo de Rijndael:

El algoritmo de Rijndael es un algoritmo simétrico de cifrado por bloques, por lo que utiliza la misma clave tanto para descifrar como para encriptar. en el estándar avanzado de encriptación (AES) se utiliza una clave de 128 bits, pero puede ser cualquier clave múltiplo de 32, entre 128 y 256 bits.

Primero traspasa el bloque de B bits a una matriz estado de 4 filas y N_B columnas, donde N_B está dado por la expresión B/32 (el bloque de datos también debe tener un tamaño múltiplo de 32 bits y estar entre 128 y 256 bits), y la clave de tamaño K bits la asociamos a una matriz similar, de 4 filas y N_k columnas (N_k está dado por la misma

expresión). Luego, para un número de rondas dado se realizan cuatro transformaciones:

- SubByte: en este paso se realiza una sustitución no lineal donde cada byte es reemplazado con otro de acuerdo a una tabla de búsqueda definida.
- ShiftRow: en este paso se realiza una transposición donde cada fila del «state» es rotada de manera cíclica un número determinado de veces.
- MixColumns: operación de mezclado que opera en las columnas de la matriz estado, combinando los cuatro bytes en cada columna usando una transformación lineal.
- AddRoundKey: cada byte de la matriz estado es combinada con la clave de ronda; cada clave de ronda se deriva de la clave de cifrado usando una iteración de clave.

Se inicia con un AddRoundKey, luego se procede a las rondas, y se finaliza con un SubByte, ShiftRow y AddRoundKey. Para descifrar se realiza el proceso inverso.

Algoritmo Rivest, Shamir y Adleman:

RSA es un algoritmo criptográfico asimétrico desarrollado en 1977. Es el primer y más utilizado algoritmo de este tipo y es válido tanto para cifrar como para firmar digitalmente. La seguridad de este algoritmo radica en el problema de la factorización de números enteros. el receptor R escoge dos números primos p y q muy grandes (de unas 100 cifras cada uno), y los multiplica, obteniendo n = pq. También en privado, el receptor obtiene el valor de la función multiplicativa de Euler, $\varphi(n) = (p-1)(q-1)$. Luego R se guarda en secreto el par de números (d,n), lo cual es la llamada clave privada, y hace público el par de números (e,n), a los que llamaremos su clave pública. e es determinado arbitrariamente, mientras que d debe responder a la expresión $d = e^{-1} \bmod \varphi(n)$, es decir, debe ser el inverso multiplicativo modular de e mod φ(n). E, que desea enviarle el mensaje confidencial x a R, lo encripta del siguiente modo: $Enc(x) = (x_e)_n$. E envía el número resultante de la operación Enc(n), R recibe un número y = Enc(x) y ejecuta con el la siguiente operación: $Des(y) = y_{dn}$ Lo que consigue es: $Des(y) = (x_e)_{dn} = x_{(ed)n} = (x)_n$, puesto que d y e eran inversos en módulo φ(n).

Referencias:

Guía de ``Gnu Privacy Guard'' - http://www.gnupg.org/gph/es/manual.html

Algoritmo RSA, Facultad de Informática Universidad de Valparaíso - http://informatica.uv.es/iiguia/MC/Teoria/mc_capitulo12.pdf

Seguridad Europea para EEUU: Algoritmo de Rijndael, Alfonso Muñoz, Madrid, 2004 - http://www.openboxer.260mb.com/asignaturas/criptografia/rijndael.pdf

Gabriel Arellano: Seguridad en capa 2. Universidad Tecnológica Nacional - Facultad Regional Concepción del Uruguay, Argentina, Julio 2005 - www.gabriel-arellano.com.ar/file_download/13

Ingeniería de Sistemas y Automática, Universidad de Oviedo, España: Seguridad en Redes, Protocolos Seguros, Junio 2009 - http://www.isa.uniovi.es/docencia/redes/protocolos_seguros.pdf

Interlink Networks: Link Layer and Network Layer Security for Wireless Networks. Interlink Networks Inc, MI, United States, Mayo 2003 - http://www.lucidlink.com/media/pdf_autogen/Link_and_Network_Layer_Whitepaper.pdf (En inglés)

Revista .Seguridad:El Cifrado Web (SSL/TLS) , Dante Ramírez y Carmina Espinoza,Mexico, Mayo 2011. http://revista.seguridad.unam.mx/numero-10/el-cifrado-web-ssltls

About.com:Guia de About.com ¿Que es SSL?,por Luis Castro. http://aprenderinternet.about.com/od/ConceptosBasico/a/Que-Es-Ssl.htm

RFC 2246
http://tools.ietf.org/html/rfc2246