CLASE 10 – 06/11/23 – Seguridad en Redes

Introducción

La seguridad hoy es una parte integral en cualquier red.
Hay protocolos, tecnologías, dispositivos, herramientas y técnicas para asegurar los datos y reducir las amenazas → hay que tratar de llegar al ideal.
Hay organizaciones de seguridad que crean estándares, fomentan la colaboración.
Ataques a las redes con virus, troyanos y gusanos son ataques específicos.
Los ataques se clasifican en reconocimiento, de acceso o denegación de servicios.

Requisitos de seguridad

Confidencialidad: garantiza que la información solo es accesible para quienes tienen la autorización.
Integridad: garantiza que la información no sea modificada.
Disponibilidad: garantiza que se pueda acceder a la información cada vez que se necesita.

Vulnerabilidad: debilidad en un activo
Amenaza: violación potencial. No es necesario que haya una violación para que al amenaza exista. Explotan la vulnerabilidades.

Tipos de Amenazas

A la confidencialidad: acceder, revelar, observar, monitorear, copiar, robar.
A la integridad: producir datos falsos, modificar los datos, generar representaciones falsas, repudiar (rechazar como falso), usar indebidamente.
A la disponibilidad: destruir, dañar, contaminar, denegar, prolongar el uso o el acceso.

Incidente

Evento adverso que puede afectar a un sistema o a una red de computadoras. Puede ser causado por una falla en algún mecanismo de seguridad o un intento o amenaza de romper estos mecanismos.

Causas de aumento de las amenazas

El crecimiento exponencial de las redes y de los usuarios y la dependencia de los mismos hace que haya crecido de la misma forma la cantidad de problemas en la seguridad de redes. Nuevas técnicas de ataque distribuido, técnicas de ingeniería social. Insuficiencia de capacitación y rentabilidad de los ataques.

Ataques Pasivos

Escuchar las transmisiones para obtener la información. Se puede hacer análisis del tráfico aunque esté encriptado. Es muy difícil de detectar. Puede ser prevenido.

Ataques Activos

Enmascaramiento, simular ser otro, modificación de mensajes, rechazo de servicio. Son más fáciles de detectar, pero difíciles de prevenir

Ataques Típicos

Interrupción: sale el mensaje del emisor, se interrumpe el mensaje y no le llega al receptor. Afecta la DISPONIBILIDAD.
Interceptación: el mensaje es escuchado, llega a destino. Afecta a la CONFIDENCIALIDAD.
Modificación: el mensaje es tomado, modificado y el receptor recibe cualquier cosa menos lo que le envió el emisor. Afecta a la INTEGRIDAD.
Falsificación: el atacante envía el mensaje directamente y el receptor lo recibe pensando que es el emisor quién se lo mandó. Afecta a la AUTENTICIDAD.

Política de Seguridad Informática (mal empleado – caer con todo el peso de la ley – denunciar)

DA 669/2004 → Todos los organismos de la administración pública nacional tienen que contar con una PSI aprobada e implementada, tiene que tener un responsable de la SI y tiene que haber un Comité de la SI para el tratamiento de dichos temas.
Objetivo: aumentar los niveles de seguridad, determinar que conductas son permitidas y cuáles no.
Ventajas: ahorra tiempo y dinero y genera mayor confianza fortaleciendo la imagen institucional.

Acceso a los Sistemas de Información

Identificación → indicarle al sistema cuál es la cuenta de usuario a utilizar
Autenticación → colocación de usuario/clave. Algo que se posee (tarjeta) o algo que es: huella digital, rostro. Lo ideal es la combinación de dos.
Autorización → tengo permiso para acceder a ese recurso

Clave de Acceso

Conjunto de caracteres definido por el usuario. Tiene que ser personal, secreta, intransferible, difícil de averiguar. Colocar caracteres, mayúscula, número y carácter especial. No cambiar cada 15 días ni todos los meses.
Riesgos Inherentes a la clave: pérdida, sustracción por parte de terceros, no renovación periódica (6 meses), descuidos en su operación.

Normas para construir una clave

- No usar palabras comunes ni nombres de fácil adivinación por parte de un tercero (nombre de la mascota)
- No vincularla con algo personal (patente, dni, fecha nacimiento, teléfono)
- No usar terminología técnica conocida (admin/admin)
- Combinar mayúscula/minúscula/carácter especial/números
- No usar menos de 8 caracteres
- Usar una acrónimo de fácil recuerdo → NorCarTren09: Norma y Carlos viajan en tren + la edad del hijo

Normas para el uso de las claves

- Cuidar que no estén mirando el teclado cuando se tipean las mismas

- No escribir las claves en papel ni en archivos sin cifrar
- No compartir las claves con otros
- No pedir las claves de otros
- No habilitar la opción de guardado de claves en los programas que se usan
- Nunca dejar la clave a mano
- Cambiarla de forma regular

Normas para el administrador

- No debe existir cuentas que no tengan contraseña
- Revisar el sistema de claves y utilizar fechas de vencimiento
- Obligar al cambio cuando se da de alta el usuario
- No dudar nunca en cambiar la clave si sospecho que alguien la puede conocer
- Escritorio Limpio: cuando se retira el personal no debe quedar nada sobre los escritorios, se debe llevar todo, guardar bajo llave o desechar.
- Pantalla Blanca: nunca dejar la computadora sin bloqueo cuando nos alejamos de ella.
- Ingeniería Social: MUY IMPORTANTE. Ejemplo: tirar el papel con la clave a la basura. El de limpieza revisa y encuentra la clave, puede acceder a mi cuenta. El factor humano es el eslabón más débil de la seguridad de la información.
- Reporte de Incidentes: una debilidad en la seguridad hay que comunicar y registrar al responsable de la SI del organismo.
- Como usuarios debemos registrar los síntomas del problema, ver los mensajes, alertar a los responsables de SI. NO debemos desinstalar el SW que aparentemente tiene una anomalía, realizar pruebas para detectar la falla de seguridad, tratar de solucionar por motus propio los problemas que aparecen.

Código Malicioso

Programa de computadora preparado para producir inconvenientes, destrucción, violar las políticas de seguridad. Hay virus (necesitan la instalación del usuario), troyanos (doble funcionalidad: una conocida y una oculta), gusanos (autreplicables). Importante: NINGÚN ANTIVIRUS PUEDE DETECTAR UN PROGRAMA MALICIOSO.
Estos programas pueden borrar archivos para que la computadora se vuelva inoperable, infectar una computadora y usarla para atacar a otras, obtener información, capturar conversaciones usando el micrófono, ejecutar comandos, robar archivos con información personal o financiera, bloquear la computadora.

Navegación WEB

En algunas ocasiones el enlace no coincide con el sitio de la empresa. Ante la duda chequear en propiedades o enviarlo a SPAM.
Siempre se debe entrar a sitio seguros verificando el certificado del mismo (candado cerrado con https)

HTTS

Protocolo de red basado en HTTP. Agregado cifrado en información sensible de usuario y clave. Usa el puerto 443 en TCP y tiene una RFC 2818.

Seguridad con el correo electrónico y mensajería instantánea

Los virus se propagan usando las libretas de direcciones y las direcciones existentes en los correos enviados. No es conveniente abrir adjuntos de origen desconocido ni aquellos que tengan extensión ejecutable. Chequear siempre el remitente. Evitar el reenvío de mensajes, en caso de ser necesario borrar la direcciones de los remitentes que no son necesarios o copiar el contenido original y armar uno nuevo usando la CCO si es para más de una persona

Redes P2P (peer to peer)

No tiene clientes ni servidores fijos. Consta de una serie de nodos que se comportan simultáneamente como clientes y servidores de los demás nodos de la red. Da servicios de telefonía y videoconferencia (Skype, zoom) y también de SW para descargar música, juegos, videos (emule).

Seguridad y Redes P2P

Mayor exposición de la estación de trabajo. Consumo excesivo del ancho de banda, el usuario puede estar compartiendo archivos que no desea compartir, hay una descarga no intencional del código malicioso, etc.

Correo Electrónico: Hoax

Engaño/Broma. Hay alertas sobre virus, mensajes religiosos, cadenas de la suerte, leyendas urbanas, métodos para hacerse millonario, regalos, rifas

SPAM

Mensajes no solicitados del tipo publicitario enviado en cantidades masivas. Los spammers usan distintas técnicas para armar las listas eternas de correo a la cuáles luego envían el spam. Capturan direcciones en páginas web y foros, en cadenas de correo y suscripciones de listas de correo y sobre todo compran bases de datos de direcciones de correo. Como recomendación se sugiere no dejar nuestro correo en cualquier página de internet o foro, no responder estos correos, dejar que vayan a SPAM y luego borrarlos. Hacer reglas de mensaje, no hacer respuestas automáticas, no responder acuses de recibo

Phishing

Normalmente se reciben correos de empresas conocidas solicitando información personal y confidencial pidiendo enviar información a páginas camufladas. Recomendaciones: llamar personalmente a la empresa, verificar el origen del correo y los enlaces.

Encriptación Simétrica

Tengo un Texto Plano + un Algoritmo de Encriptación + una clave secreta compartida y enviada. Envío el mensaje cifrado. El otro usuario tiene la misma llave, se desencripta (con un Algoritmo de Desencriptación) y se obtiene el texto plano original. Tengo que asegurarme que esa clave no ande dando vueltas y que llegue cifrada

Encriptación Asimétrica

Conocida como encriptación de clave pública. Los extremos puedan utilizar el mismo algoritmo o uno diferente. Hay dos valores de clave diferente: una pública y una privada

Requisitos para Seguridad en Encriptación

Debemos buscar que sea un algoritmo fuerte en encriptación, que aunque sea conocido no se pueda desencriptar sin clave. Las claves secretas deben ser distribuidas de manera segura. La clave tiene que ser conocida por la organización.

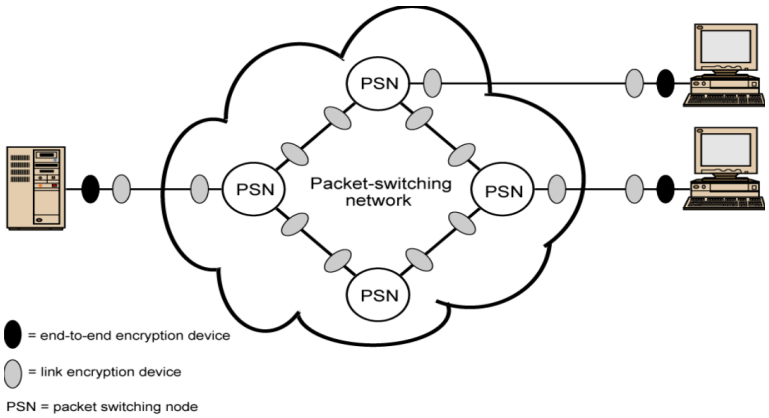
Ataque a la Encriptación

- Se analiza el encriptado
- Se requiere conocimiento de la naturaleza del algoritmo
- Se requiere conocimiento de características generales de texto plano
- Se intenta deducir texto o clave
- Fuerza bruta: prueba con cada clave distinta hasta obtener el texto plano

Algoritmos → procesan el texto plano en bloques de tamaño fijo. Producen bloques de texto cifrado de igual longitud.

1- DES: Data Encryption Standard: ya no se utiliza. Fue preparado en 1998. Usan 53 bits de clave.
2- TDES: Triple DES. Cumple la norma ANSI. Incorpora una norma de la DEA. Utiliza tres claves y tres ejecuciones del algoritmo DEA. Las claves son de 112 o 168 bits. Es lento según la máquina que esté usando. El tamaño de bloque es de 64 bits (pequeño).
3- AES: Advanced Encryption Standard. Tiene una norma NIST y una norma de FIPS. Es más seguro y más eficiente que el anterior. Tiene una adaptación del SW y el HW por lo que da mayor flexibilidad. Características:
    a. Las claves son de 128 bits
    b. La entrada es un bloque simple de 128 bits
    c. Las claves se presentan como una matriz cuadrada
    d. Hay 44 palabras claves de 128 bits
    e. Los bytes están ordenados por columna
    f. Formado por 4 etapas: una permutación y tres sustituciones

Dispositivos de encriptación



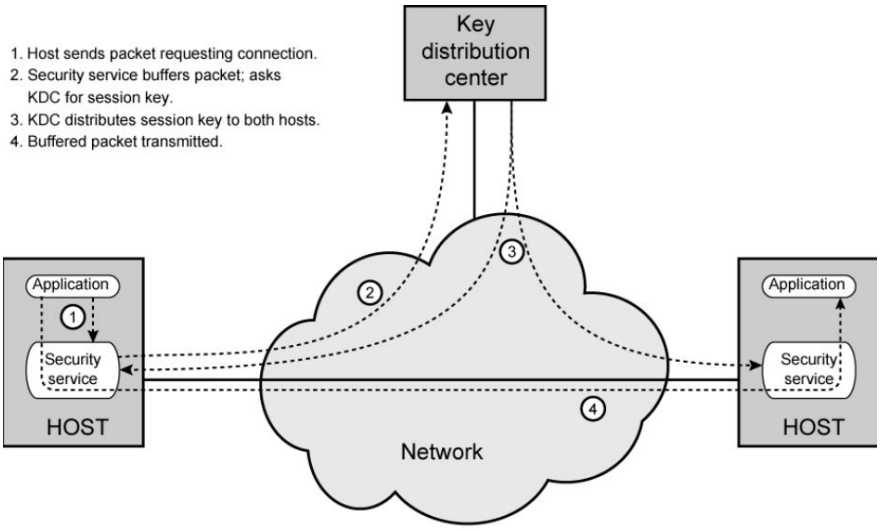
Encriptación de enlaces

- Se hace de extremo a extremo.
- Se utiliza para el tráfico de alto nivel de seguridad.
- Hay muchos dispositivos de encriptación.
- Los mensajes deben ser desencriptados en cada switch.
- Comparten una clave.
- Lo que va encriptado solo es el contenido de usuario para que el switch pueda leer el encabezado y las rutas

Métodos de distribución de claves

Una clave que selecciona el usuario A y lo quiere entregar al B. Un tercero puede seleccionar esta clave y la distribuirá a ambos. Utilizar una clave vieja para encriptar y transmitir la clave nueva de A a B. Utilizar una clave vieja para transmitir la nueva a ambos. ´

Distribución Automática



Elementos:

- *Clave de sesión*: usada durante una conexión lógica y se destruye al final de la sesión. Es usada para los datos de usuario.
- *Clave permanente*: usada para la distribución de claves.
- *Centro de distribución de claves*: determina cuál sistema puede comunicarse, provee la clave de sesión para la conexión.
- *Módulo de servicios de seguridad* (SSM): realiza la encriptación entre extremos y obtiene claves para los hots.

Relleno de Tráfico

Produce texto cifrado continuamente. Si no hay texto para codificar envía datos aleatorios. Esto hace imposible el análisis de tráfico.

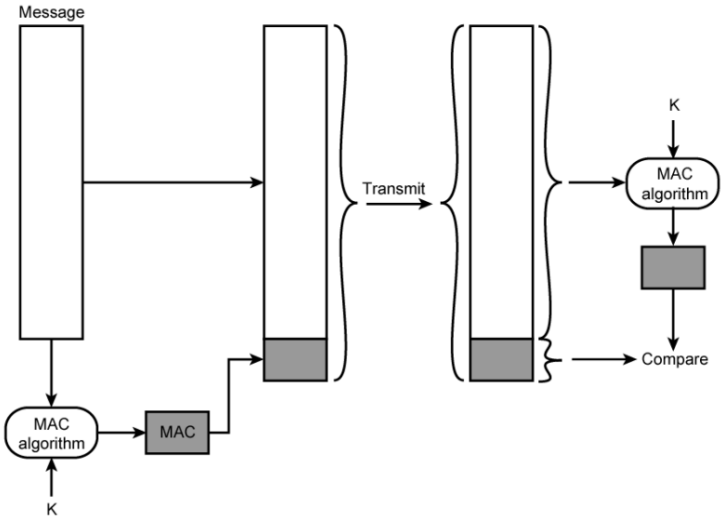
Autenticación de Mensajes

- Nos protege contra ataques activos.
- Si el mensaje es auténtico y proviene de una fuente confiable.
- La autenticación permite verificar que el mensaje es auténtico, que no fue alterado y que proviene de esta fuente segura.
- La autenticación encriptada supone que solo transmisor y receptor conocen la clave.
- El mensaje incluye un código de detección de error, un número de secuencia y el timestampt

- La autenticación sin encriptación se genera una marca de autenticación se agrega cada mensaje. El mensaje no se encripta. Es muy útil para estos casos: mensajes a múltiples destinos, aliviar la carga de procesamiento dado que autentica al azar y los programas se ejecutan sin decodificar.

Códigos de autenticación de mensajes

- Se generan a partir de claves en ambos extremos.
- Si solo el tx y el rx conocen la clave y el código coincide entonces el rx se asegura que el mensaje no fue alterado y que proviene del tx correcto. Si tiene mensaje tiene un nro de secuencia , el rx asegura la secuencia correcta.



Función de Hash unidireccional

- ✓ Hash: proceso por el cuál se encripta.
- ✓ Acepta mensajes de longitud variable.
- ✓ Produce tags de longitud fija.
- ✓ Desventaja: autenticación sin encriptación.

Funciones de Hash seguras

- ✓ Aquellas cuyas propiedades se pueden aplicar a cualquier tamaño de datos
- ✓ Produce salidas de longitud fija.
- ✓ Fácil de procesar.
- ✓ No se puede reversar.
- ✓ No es posible hallar dos mensajes con el mismo hash.

SHA-1 Secure Hash Algorithm 1

- ✓ Mensaje de entrada de por lo menos 2^{64} bits.
- ✓ Son procesados en bloques de 512 bits.
- ✓ La salida tiene 160 bits.

Encriptación de Claves Públicas

- ➢ Está basada en algoritmos matemáticos.
- ➢ Es simétrica.
- ➢ Usa dos claves separadas.
- ➢ Elementos: texto plano, algoritmo de encriptación, clave pública, clave privada y algoritmo de desencriptación.
- ➢ Para encriptar se usa la clave pública y luego la privada para desencriptar.

- Para autenticar se utiliza la privada y luego la pública para obtener el texto plano.

Firma digital – Ley 25.506

- El tx encripta el mensaje con su clave privada.
- El rx puede desencriptar usando una clave pública conocida.
- Sirve para autenticar al tx que es el único que tiene la clave correcta.
- No da privacidad a los datos, sí a las comunicaciones.
- Permite identificar a los usuarios.
- Repudio en términos legales.
- Garantiza la integridad del documento.
- Se usa el algoritmo RSA
- Certificado digital: usa la clave pública, genera un código, se lo pego, se encripta con la privada, lo desencripta con la pública.

Firma Digital y Certificado Digital

Firmar un documento es agregarle un objeto que permite con una clave pública verificar que nadie ha modificado el documento. La clave pública corresponde a la firma.
Un certificado es una clave pública firmada por una autoridad en la que confiamos (organismo de certificación).

Algoritmos Simétricos

Inconveniente:

- Los mensajes no son irrepudiables
- Es más sencillo de implementar.
- No puedo garantizar el manejo seguro de claves sin un canal seguro

Algoritmos Asimétricos

- Quebrarlos equivale a calcular la función inversa

Seguridad en Redes

Seguridad se refiere a la confianza en que los datos no serán accedidos por personal no autorizado. La autenticación de direcciones IP es insuficiente. Se usa encriptación para la seguridad perimetral. IPSEC opera en IPv4 e IPv6. Define un marco pero no define algoritmos

AH: IPSEC Authentication Header: agregado después del encabezado IP, no es opcional del IP. El encabezamiento IP se cambia el campo protocol. Usa IPv6. No envía toda la información sino algunos índices pre-asignados.

ESP: IPSEC Encapsulation Header: encripta el contenido de los mensajes y agrega un encabezado de 8 octetos con una cola de autenticación. Algunos campos del IP se cambian para implementar el IPSEC. Todos los algoritmos están respaldados en una RFC.

SSL: Secure Socket Layer: es un protocolo que provee autenticación y encriptación por medio del browser. Sobre TCP (no darle bola a esto)

TLS: Transport Layer Security: reemplaza al SS. RFC2246. Sobre TCP

Seguridad Perimetral: en las conexiones a internet insertamos firewall con políticas coordinadas centralmente.

Firewall: filtro de paquetes que corre en un router. Bloquea la información según la dirección IP, el protocolo o el puerto.

Acceso Proxy: Permite el acceso de determinados clientes a determinados servicios y detecta virus.

Statefull Firewall: Registra pedidos salientes para permitir ingresos de respuestas entrantes. Trabaja bien con TCP pero NO con UDT.

Proxy de aplicaciones: Detecta los virus de forma integral ya que un firewall solo ve los datagramas.

Firewall

- Es un elemento de HW o de SW.
- Controla las comunicaciones en base a políticas.
- Ante la duda siempre DENEGAR TODO. Para dar permiso hay tiempo, por las dudas decir que no y después se ve.
- Se ubica entre el punto de conexión entre las redes internas e internet.
- Se puede conectar una tercera red llamada DMZ.
- Operan en distintas capas
- Está normalizado en la RFC 2979

Seguridad en IPV4 e IPV6

- Se realiza a través del protocolo IPSEC.
- Permite una conexión segura entre la casa central y sus sucursales.
- Permite acceso remoto seguro.
- Cubre la conectividad entre la intranet y la extranet.
- Mejora la seguridad para el comercio electrónico.
- Descripto en RFC 2401, 2402, 2406, 2408.
- Hay encabezamiento y autenticación.
- Los datos de usuario van encapsulados.
- Hay un intercambio de claves.
- Security Association: SA. Es una relación unidireccional entre tx y rx. Para que sea bidireccional hay que usar dos SA. Hay tres parámetros para identificarlo:
    - 1- Índice de seguridad.
    - 2- Dirección IP de destino.
    - 3- Identificador de protocolo de seguridad.
    - Contador de nro de secuencia.
    - Contador de desborde de secuencia.
    - Ventana contra respuesta.
    - Información de Autentication Header.
    - Información de ESP. → encapsulation security payload (permite servicios confidenciales, da autenticidad de origen, integridad, asociación de confidencialidad en un solo paquete, etc)
    - Tiempo de vida de la asociación.
    - Modo de protocolo ipsec.
    - Máximo MTU de la ruta.

Ejemplo de ataque: En 2017 el ransomware conocido como WannaCry conmocionó al mundo con un ataque fulgurante: en un solo día infectó más de 230 000 PC con Windows en 150 países, muchos de ellos pertenecientes a agencias gubernamentales y hospitales.

Criptografía

- Es el estudio y práctica de ocultar información muy utilizada.
- Los datos inalámbricos pueden ser cifrados utilizando varias aplicaciones.
- Se puede cifrar una conversión entre 2 teléfonos IP y ocultarse con criptografía los archivos de una computadora.
- Asegura confidencialidad, integridad y disponibilidad

Inundación TCP/SYN

1. Es un ataque donde se envía una inundación de paquetes SYN.
2. Cada paquete es un mensaje con solicitud de conexión.
3. El servidor contesta devolviendo un paquete SYN ACK esperando la respuesta
4. Como la dirección es falta la respuesta no llega nunca
5. Con esto se logra saturar el número de conexiones disponibles haciendo que los intentos de conexión legítimas no lleguen

Ataque DDoS - Ataque Distribuido de Denegación de Servicio

- Se envía un paquete malicioso o una seguidilla de mensajes que colma el ancho de banda del enlace
- Se usa una red zombie o bootnet (red capaz de controlar muchos ordenadores de usuario en forma remota para propagar virus, generar spam y cometer algún otro delito o fraude en la red.) para lanzar el ataque.
- El ping de la muerte: ataque a la denegación de servicios donde el atacante desestabiliza la máquina objetivo al enviar un paquete de mayor tamaño que el máximo permitido haciendo que esta máquina se congele o deje de funcionar.
- Ataque Smurf: ataque a la denegación de servicios distribuido que deja fuera de servicio a las redes informáticas.
- Ataque al cifrado simétrico: usar claves de 128 ya que necesito sólo 10 horas para descifrar una clave de 56 bits.

Esteganografía → técnica de cifrado alternativa que oculta un mensaje secreto, encerrándolo en un archivo ordinario, como un archivo gráfico de película o de sonido (Google)

Seguridad en Redes Inalámbricas

WPA2: Wifi Protective Acces
AES: en página 5.
TKIP: protocolo de seguridad dinámico que cambia las claves a medida que se utiliza
PSK: oficinas domésticas pequeñas donde se comparte la clave
WEP: Se trata de una clave estática, por lo que todo el tráfico se cifra con una única clave, sin importar el dispositivo (128/64)
MAC: usado mucho en los móviles de empleados del banco.