Síntesis conceptual

Grado: Administración de Sistemas Informáticos en Red
Asignatura: Seguridad y alta disponibilidad
Unidad: 2. Seguridad activa

Resumen

La criptografía se basa en el empleo de códigos para ocultar el mensaje real, desde complejos esquemas a un simple desplazamiento de las letras a través del abecedario. Pero ningún código es imposible de resolver, ya sea mediante diversas técnicas para encontrar la clave del código o mediante "fuerza bruta" probando todas las combinaciones hasta descubrir la correcta.

Desde la antigüedad se encriptan mensajes, Julio Cesar ya lo hacía, hoy en día es un proceso llevado a cabo continuamente con nuestros mensajes de texto. Podemos encontrar dos tipos principales de este proceso concreto:

- Algoritmos simétricos o clave privada: Usan la misma clave para cifrar y descifrar, por lo que se requiere que ambos lados posean la misma clave.
- Algoritmos asimétricos o de clave pública: Se requiere de dos claves, la pública y la privada, para poder descifrar el mensaje.

Otro tipo de sistema de seguridad es la huella digital. La huella digital se genera a partir del documento, de modo que si el documento se modifica su huella cambiará, sin posibilidad de eliminar los cambios para volver hacia atrás o de recrear el documento a partir de la huella.

El protocolo de seguridad permite una segura transmisión de la información con la encriptación del tráfico de datos, no se debe confundir con los algoritmos de cifrado. El primer protocolo de este tipo para la red wifi fue el ya obsoleto WPA.

Otros grandes elementos de seguridad son la firma electrónica y el certificado digital.

La firma electrónica es un conjunto de autenticaciones electrónicas involucradas en un documento de manera digital, que pueden ser utilizadas como medio de identificación, Ese fichero electrónico es el equivalente al DNI en el mundo informático.

Con el fin de que estas sean realmente auténticas debemos generarlas apropiadamente a través de autoridades certificadoras de confianza. Todas las páginas web HTTPS deberían poseerlo, en caso contrario el navegador nos avisará con el mensaje "Your connection is not private".

Las CA, autoridades certificadoras, pueden emitir y quitar estos certificados, mientras que también pueden habilitar a agentes intermedios para que realicen esta acción en su nombre.

Todos los sistemas operativos y algunas aplicaciones, como el navegador Google Chrome, poseen un almacén de certificados propio donde se almacenan todos los certificados, actualizándose con el tiempo.

Algunos posibles problemas al obtener la certificación son:

- Falta de conocimiento por parte del usuario.
- La FNMT no se tiene en cuenta como raíz de confianza.
- Los navegadores trabajan con algoritmos de cifrado diferentes.
- El software que permite la firma electrónica es escaso.
- Falta de información oficial, clara e inequívoca.

Existen diferentes tipos de *malware*, como son:

- *Malware* infeccioso: virus y gusanos: Infección de ficheros ejecutables o sistemas a través de la red y ejecuta su cometido hostil. El virus necesita la intervención del usuario para ejecutarse e iniciar su infección, el gusano aprovecha ciertas vulnerabilidades del sistema para instalarse en él y autoejecutarse.
- Puerta trasera: Método para iniciar sesión en un sistema esquivando el proceso de autenticación, requiere de su instalación por un virus que ya se encuentra en el sistema.
- *Drive-by downloads, adware, hijackers, phishing*: Si se trata de una descarga no consentida, se trata de ***undrive-by downloads***; la aparición de ventanas de publicidad emergente de forma descontrolada se llama ***adware***, ***hijack***, es un tipo de malware que secuestra de alguna manera la configuración del navegador pudiendo mostrar publicidad; ***Phishing*** consiste en páginas web falsas que suplantan la identidad a las verdaderas para que el usuario, sin darse cuenta, introduzca información sensible.
- Troyanos: Es un *malware* oculto dentro de un *software* que invita a ser ejecutado por parte del usuario.
- *Keyloggers, stealers y spyware*: Un keylogger es un tipo de malware que registra las pulsaciones de teclado del usuario en busca de patrones repetidos, pudiendo ser contraseñas o números de tarjetas de crédito. Los stealers obtienen los datos de los repositorios en los que los navegadores guardan la información referente a contraseñas y autorellenado de formularios. Los spyware se dedican a recopilar información sobre diversas actividades del usuario para venderla posteriormente a empresas de publicidad.
- *Ransomware*: Suele infectar los equipos a través de puertas traseras como los troyanos y una vez acceden al sistema, se encargan de la encriptación de todos los ficheros que puedan contener información vital.

Para evitar estas amenazas se recomienda contar con un *software* de seguridad y mantenerlo actualizado. Se recomienda también que se realicen periódicas revisiones, así como la eliminación o puesta en cuarentena de cualquier *malware* o archivo infectado.

Otro problema junto a los *malware* es el *spam* el cual podemos controlar con:

- Software antispam.
- Registros SPF: Sistema para evitar que correos legítimos se confundan con *spam*.
- Correo legítimo: Comprobar si el correo es legítimo.

Un elemento imprescindible para mantener la seguridad de las aplicaciones son las actualizaciones, pudiéndose realizar desde:

- Windows Server Update Services (WSUS): en Windows.
- Repositorios locales: en Linux.

Sistemas de *Hardening,* endurecimiento de las defensas, llevados a cabo por parte por entidades como la fundación OWASP, el consorcio WASC y CIS. Es recomendable también el empleo de auditorías de seguridad para las grandes empresas.

De especial relevancia es la seguridad en las redes corporativas, sin importar su tipo, donde podemos emplear múltiples elementos:

- Seguridad en redes cableadas:
    - Control por dirección MAC: Emplear una lista de direcciones IP fija y deshabilitar la asignación dinámica.
    - Servidores rogue DHCP: No está controlado por un administrador, por lo que a través de él no se podrá acceder a la red de los servidores de la empresa.
    - Registro de equipos en un dominio: El administrador es el único que da acceso a los dominios Active Directory.
    - IEEE 802.1X: Protocolo que requiere de diversos elementos para la identificación.
    - VLAN: Cada paquete incorpora en su cabecera una dirección IP origen y su dirección destino.
    - SNMP: Simple Network Management Protocol.
- Seguridad de redes inalámbricas:
    - WEP, WAP y WAP2: WEP utiliza un cifrado RC4 con claves de 64 bits para wifi, fue mejorado por sus sucesores.
    - WAP3: Es el más reciente, contando con un cifrado de 192 bits.
    - WPS: Requiere de un botón WPS en el punto de acceso para obtener acceso.
    - Hotpots: Variante de un punto de acceso inalámbrico que necesita un firmware especial que utilizan las empresas.
- Monitorización del tráfico de red.

Conceptos fundamentales

- **Autenticidad**: garantía de la identidad de nuestro interlocutor.
- **Criptoanálisis**: ciencia de estudio de la criptografía y sus posibles vulnerabilidades.
- **Confidencialidad**: garantía de que el receptor destinatario será el único capaz de leer el mensaje.
- **Integridad**: propiedad que garantiza que un mensaje o archivo no ha sido alterado.
- **No repudio**: el receptor no puede mentir sobre la llegada de un mensaje al receptor.