Introducción a la Ciberseguridad

Ciberseguridad – FPUNA

Aplicaciones de Criptografía y PKI

Criptografía

La criptografía es una de las disciplinas más relevantes dentro del campo de la seguridad de la información. A la hora de proteger los datos y la información que manejan las organizaciones, tanto física como digital, las técnicas criptográficas están ganando mucho peso en la actualidad.

La aplicación de la criptografía consiste en convertir un mensaje que se quiere intercambiar en otro mensaje cuya información es incomprensible. Es decir, que su lectura sólo está al alcance de los responsables de este cifrado.

Principales términos en criptografía

- **Texto plano**: es el mensaje original que desea intercambiarse, contiene información legible.
- **Texto cifrado**: se corresponde con el mensaje resultante de aplicar una técnica criptográfica sobre el texto plano, y contiene información ilegible. El proceso de convertir texto plano en texto cifrado se conoce como cifrar.

Principales técnicas en criptografías

- **Critpografía de clave simétrica**: Se basa en la premisa de que tanto el emisor como el receptor de un mensaje que contiene una determinada información poseen la misma clave privada. De esta manera, el emisor puede cifrar el mensaje original utilizando la clave privada y enviárselo al receptor. El problema, sin embargo, es que el envío de esa clave ha de realizarse mediante texto plano, cuya lectura podría estar al alcance de cualquiera.
- **Criptografía de clave asimétrica**: En este caso, el emisor y el receptor que desean intercambiar mensajes cifrados, eligen una clave privada que solamente ellos conocen. A partir de la clave privada que ambos han elegido, mediante la aplicación de un algoritmo matemático, tanto el emisor como el receptor, generan una nueva clave que se denomina clave pública.

Public Key Infrastructure (PKI) 1/2

- Es un grupo de componentes y servicios informáticos que permiten gestionar, controlar y administrar la tarea de generar, brindar, revocar y validar toda clase de certificados digitales.
- En síntesis, es una combinación de hardware y software aplicada en políticas y tareas de seguridad digital. Lo que hace especial a la PKI sobre otros métodos de cifrado, es que puede integrar los certificados digitales junto a la criptografía de la clave pública y las diferentes autoridades de certificación dentro de una misma plataforma.

Public Key Infrastructure (PKI) 2/2

- Su arquitectura está conformada por una infraestructura de confianza que abarca los siguientes actores o componentes:
  - **Autoridad de certificación**
  - **Autoridad de registro**
  - **Autoridad de validación**
  - **Autoridad de repositorio**
  - **Software y políticas**

Autoridad de certificación

- Certificate Authority o CA
- La PKI permite que las instituciones o autoridades que se encargan de emitir y determinar la validez de los certificados estén incluidos en su estructura.

Autoridad de registro

- Registration Authority o RA
- Es en resumen el intermediario entre el usuario final de los certificados y la autoridad de certificación en la tarea de expedir y/o renovar los certificados.

Autoridad de validación

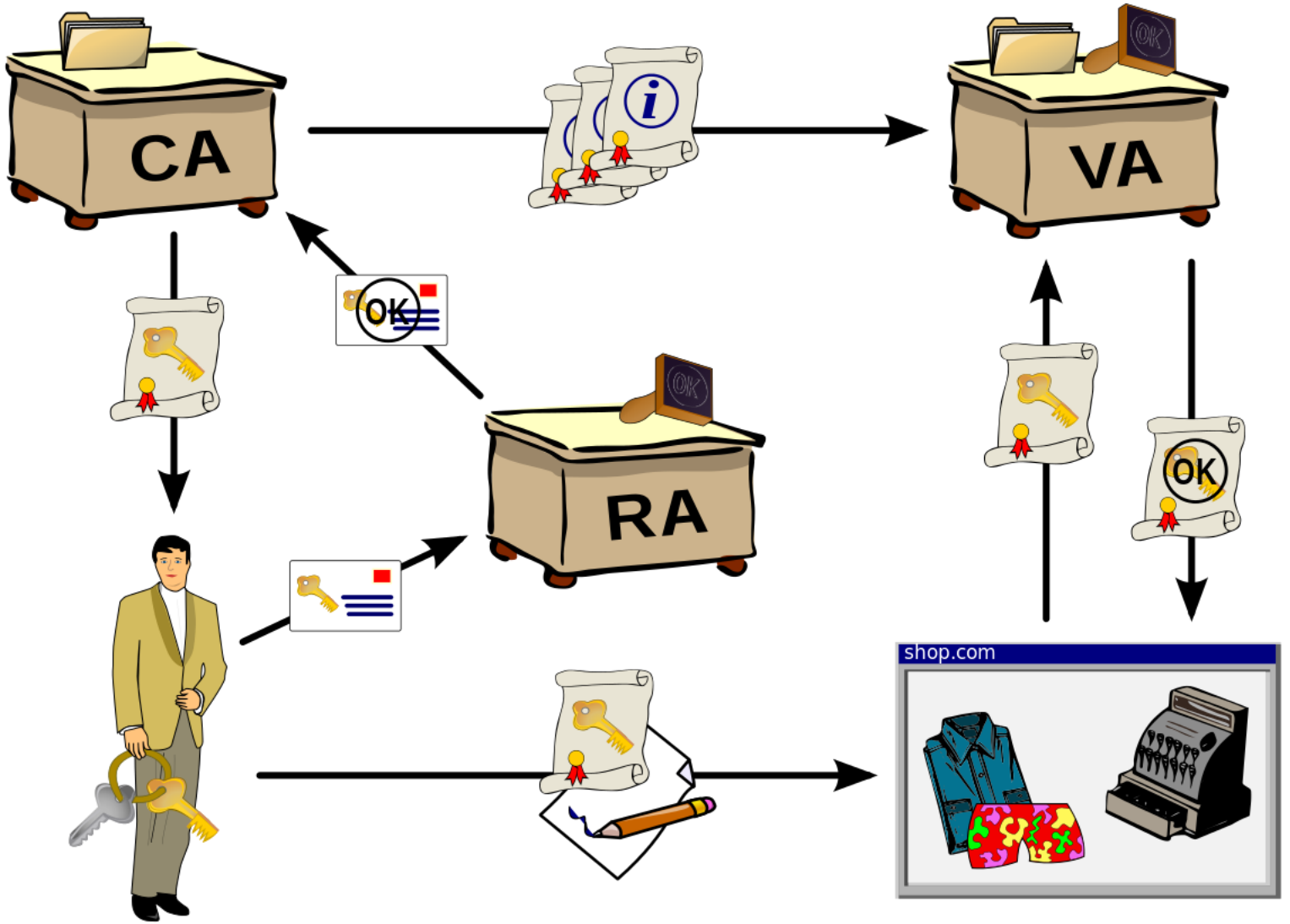
- Validation Authority o VA
- Son aquellos actores que se encargan de centralizar, organizar y controlar la lista de todos los certificados digitales emitidos, vencidos o revocados. Asimismo, permitiendo que toda esta información sea visible para los usuarios.

Autoridad de repositorio

- El “lugar” donde se almacenan todos los certificados emitidos, los caducados o revocados por cualquier razón.

Software y políticas

- Por último, la PKI integra a todos los productos de software que están destinados para usar los certificados digitales y, por supuesto, aquellas reglas o políticas definidas para la comunicación de la información en este aspecto.


CA
VA
RA
OK
OK
shop.com

Utilidad de la PKI

- La confidencialidad de la información es factor fundamental de las transacciones comerciales y la PKI se encarga de garantizar la protección y seguridad de todos los mensajes, su integridad, autenticación y el no repudio. De hecho, la Infraestructura de Clave Pública está presente en varias áreas o herramientas comerciales, por ejemplo: **Firma Electrónica**

Seguridad de datos

¿Qué es la Seguridad de Datos? 1/3

La seguridad de datos es la práctica que consiste en proteger la información digital contra el **acceso no autorizado**, **la corrupción** o **el robo** durante todo su ciclo de vida. Es un concepto que comprende todos los aspectos de la seguridad de la información, desde la seguridad física del hardware y los dispositivos de almacenamiento hasta los controles administrativos y de acceso, así como la seguridad lógica de las aplicaciones de software. También incluye las políticas y los procedimientos de la organización.

¿Qué es la Seguridad de Datos? 2/3

Cuando se implementan correctamente, las estrategias de seguridad de datos sólidas protegerán los activos de información de una organización contra actividades de ciberdelincuentes, pero también contra amenazas internas y errores humanos, que siguen siendo una de las causas principales de la vulneración de datos.

¿Qué es la Seguridad de Datos? 3/3

La seguridad de datos implica el uso de herramientas y tecnologías que ofrecen mejoras a la organización en cuanto a visibilidad del lugar donde se encuentran los datos críticos y cómo se usan. Idealmente, estas herramientas deben ser capaces de aplicar protecciones como el cifrado, el enmascaramiento de datos y la redacción de archivos confidenciales, así como de automatizar la generación de informes para agilizar las auditorías y cumplir los requisitos normativos.

Tipos de seguridad de datos

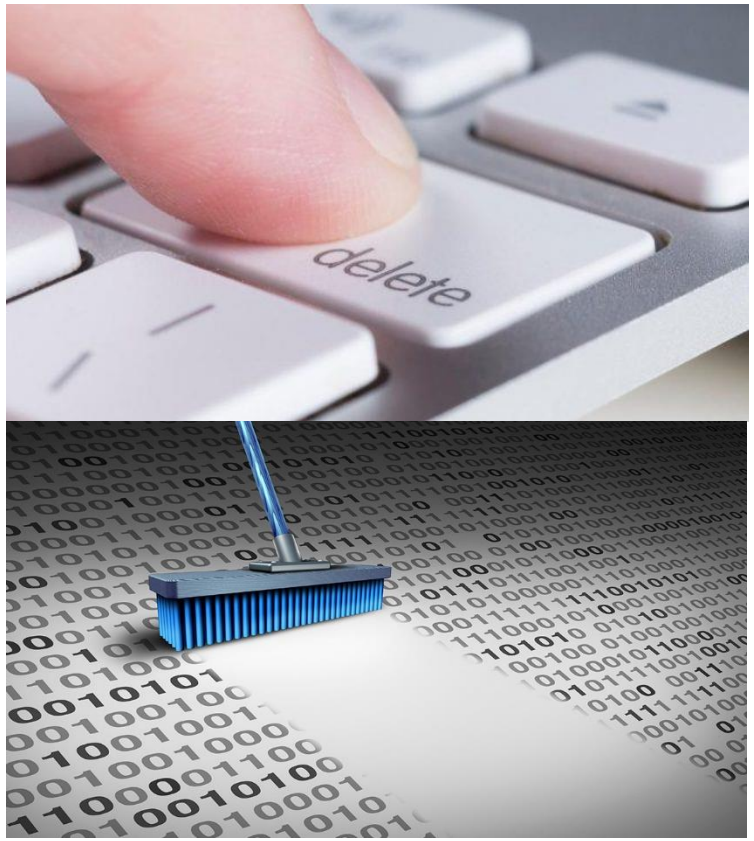
Tipos de Seguridad de Datos

- Cifrado
- Borrado de datos
- Enmascaramiento de datos
- Resiliencia de datos

Cifrado

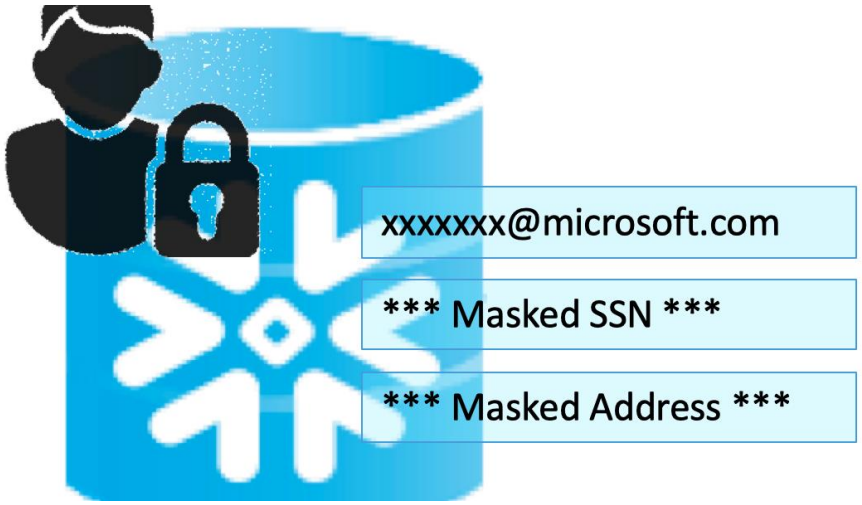
- Mediante un algoritmo que transformar los caracteres de texto normal en formato no legible, las claves de cifrado mezclan los datos para que solo los usuarios autorizados puedan leerlos. Las soluciones de cifrado de bases de datos y archivos son una última línea de defensa para volúmenes confidenciales, ya que ocultan su contenido a través del cifrado o la simbolización. La mayoría de las soluciones también incluyen prestaciones de gestión de claves de seguridad.

Borrado de datos



- El borrado de datos, que es más seguro que la eliminación estándar de datos, usa software para sobrescribir los datos en cualquier dispositivo de almacenamiento. Verifica que los datos no se puedan recuperar.

Enmascaramiento de datos



- Al enmascarar los datos, las organizaciones pueden permitir a los equipos que desarrollen aplicaciones o formen a las personas usando datos reales. Enmascara la información de identificación personal (PII) cuando es necesario para que el desarrollo pueda llevarse a cabo en entornos que cumplen la normativa.

Resiliencia de datos

- La resiliencia se determina según lo bien que una organización resista cualquier tipo de anomalía o se recupere de ella, ya sea un problema de hardware, un corte de suministro eléctrico u otro evento que pueda afectar a la disponibilidad de los datos. La velocidad de recuperación es fundamental para minimizar el impacto.

Estrategias de Seguridad de Datos

Estrategia de seguridad de datos

Una estrategia de seguridad de datos exhaustiva incorpora personas, procesos y tecnologías. Establecer controles y políticas apropiados es tanto una cuestión de cultura organizativa como de implementación del conjunto correcto de herramientas. Esto significa priorizar la seguridad de la información en todas las áreas de la empresa.

1. Seguridad física de servidores y dispositivos de usuarios.
2. Gestión y controles de acceso.
3. Seguridad y parcheado de aplicaciones.
4. Copias de seguridad.
5. Formación de los empleados.
6. Supervisión y controles de seguridad de redes y endpoints.

Seguridad física de servidores y dispositivos de usuarios

- Independientemente de que los datos se almacenen de forma local, en un centro de datos corporativo o en el cloud público, debe asegurarse de que las instalaciones estén protegidas contra intrusos y cuenten con medidas de extinción de incendios y controles climáticos adecuados. Un proveedor de cloud asumirá por usted la responsabilidad de estas medidas proactivas.

Gestión y controles de acceso

- El principio de "privilegio mínimo" debe aplicarse en todo el entorno de TI. Esto significa otorgar acceso a las bases de datos, redes y cuentas administrativas a la menor cantidad de personas posible, y solo a quienes lo necesiten realmente para hacer su trabajo.

Seguridad y parcheado de aplicaciones

- Todos los programas de software deben actualizarse con la última versión lo antes posible una vez que se estén disponibles parches o versiones nuevas.

Copias de seguridad

- Mantener copias de seguridad utilizables y comprobadas minuciosamente de todos los datos críticos es indispensable en cualquier estrategia de seguridad de datos sólida. Además, todas las copias de seguridad deben estar sujetas a los mismos controles de seguridad físicos y lógicos que rigen el acceso a las bases de datos principales y a los sistemas centrales.

Formación de los empleados

- Capacitar a los empleados sobre la importancia de tener buenas prácticas de seguridad y contraseñas seguras, así como enseñarles a reconocer ataques de ingeniería social, los convierte en un “firewall humano” que puede jugar un rol crítico en la protección de sus datos.

Supervisión y controles de seguridad de redes y endpoints

- Implementar un conjunto exhaustivo de herramientas y plataformas de gestión, detección y respuesta a amenazas en todo su entorno local y sus plataformas cloud puede mitigar los riesgos y reducir la probabilidad de una vulneración.

Modelos de control de acceso

Modelos de Control de Acceso

- Un modelo de control de acceso es un conjunto definido de criterios que un administrador del sistema utiliza para definir derechos/permisos de los usuarios del/al sistema.
- Hay tres modelos principales de control de acceso:
  - Control de Acceso Obligatorio (Mandatory Access Control - MAC),
  - Control de Acceso Discrecional (Discretionary Access Control - DAC), y
  - Controles de Acceso Basado en Roles (Rule Based Access Control - RBAC).
- Además, una regla de control de acceso basado en roles (RBAC) es útil para la gestión de permisos a través de sistemas múltiples.

Control de Acceso Obligatorio

En el modelo de control de acceso obligatorio se asignan las funciones de los usuarios estrictamente de acuerdo con el indicado por el administrador del sistema. Este es el método de control de acceso más restrictivo, porque el usuario final no puede establecer controles de acceso en los archivos. El Control de acceso obligatorio es muy popular en ambientes/instalaciones altamente secretas, como la industria de defensa donde los archivos «perdidos» pueden afectar a su seguridad nacional.

Control de Acceso Discrecional

- El control discrecional de acceso esta en el otro extremo del espectro de acceso, diferente del modelo de acceso obligatorio, ya que es el menos restrictivo de los tres modelos. En el marco del modelo de acceso discrecional el usuario final tiene total libertad para asignar los derechos a los objetos que desea.
- Este nivel de control completo sobre los archivos puede ser peligroso porque si un atacante o algún Malware compromete la cuenta a continuación, el usuario malicioso o código tendrá un control completo también.

Controles de Acceso Basado en Roles

- La Función de control de acceso basado en permisos o Roles crea la asignación de derechos/permisos de acceso a funciones o trabajos específicos dentro de la empresa; RBAC a continuación, asigna funciones a los usuarios, con lo que le concede privilegios.
- Este modelo de control de acceso a las funciones de manera efectiva en las organizaciones reales es, debido a que a los archivos y los recursos se le asignan los permisos de acuerdo a las funciones que lo requieran. Por ejemplo, un administrador del sistema puede crear una función de acceso para los gerentes solamente. Así, un usuario se le tendría que ser asignado el papel de un gerente para utilizar esos recursos.