Criptografía e Cifrado

Introducción

Introducción

A finalidade da criptografía é garantizar a confidencialidade, integridade, a autenticación, o non repudio e o sellado de tempo (Seguridade da Información). Os sistemas de cifrado poden ser:

- Simétricos
- Asimétricos ou de chave pública
- De un único sentido (hash)

Habitualmente se empregan sistemas híbridos que combinan a criptografía simétrica e asimétrica.

O cifrado consiste en ofuscar a información facéndoa incomprensible salvo para o seu destinatario.

Cifrado

O cifrado da información depende da chave de cifrado / descifrado (salvo as funcións hash). Esta chave debe ser robusta e se debe gardar de xeito seguro (a súa perda imposibilitará o acceso á información, e o seu roubo supón a perda da confidencialidade).

Parao o cifrado se utilizan varias ferramentas que dependerán do uso:

- Si se require o cifrado trasparente ou non
- Si o descifrado debe poder realizarse en calquera sitio
- Si o usuario ten un perfil técnico ou non

É particularmente importante cifrar a información crítica almacenada na nube ou en proveedores externos.

Cifrado Simétrico

- No cifrado simétrico se emprega unha única chave para cifrar e descifrar
- A chave de cifrado debe ser coñecida únicamente para as partes que se comunican
- O punto débil neste sistema e a comunicación da chave de cifrado a outra parte
- Os algoritmos máis utilizados son AES e DES. O DES é vulnerable e está substituíndose por 3DES, que é lento. Polo que o recomendado é **AES**. Outros algoritmos son RC4 (que se usa en TLS e para cifrado de arquivos) e RC5.

Cifrado Asimétrico

O cifrado asimétrico resolve o problema da comunicación da chave de cifrado mediante o emprego de dúas chaves relacionadas. O que cifra unha chave únicamente pode descifralo a outra.

- Unha das chaves se almacena de xeito seguro sin que ninguén salvo o propietario teña acceso a ella (chave privada).
- A outra chave se pode e debe distribuír libremente de xeito público (chave pública).
- Cando se necesita enviar unha mensaxe privada a alguén bastará con cifrala coa chave pública do destinatario. Únicamente o que dispón da chave privada correspondente poderá descifralo.
- O punto débil deste sistema é o xeito de asegurar que a chave pública pertence realmente ao destinatario que nos pensamos. Existen dous enfoques para resolver este problema: As autoridades de certificación e as cadeas de confianza.
- O cifrado asimétrico é lento para cifrar volumes de información grandes, polo que se recurre habitualmente ao ***cifrado mixto ou híbrido***, no que se emprega o cifrado asimétrico para a comunicación segura da chave de cifrado simétrico.
- Os algoritmos máis utilizados son ***Diffie-Hellman*** que se utiliza para o intercambio de chaves simetricas sen necesidade de transmitila mediante cálculos matemáticos con números primos, ***RSA/DSA*** que é o máis utilizado para cifrar e descifrar mensaxes pequenos, firmas dixitais, autenticación.. usando chaves de 1024, 2048 ou máis bits.

Cifrado Unidireccional (Hashing)

O cifrado unidireccional consiste en xerar unha chave única relativamente breve a partir da información orixinal. Distinta información idealmente debe dar lugar a distintas chaves (o que resulta matemáticamente imposible). Cando dúas informacións distintas producen a mesma chave decimos que se produce unha **colisión.**

Se emprega habitualmente para:

- Almacenar contrasinais: Para comprobar si unha contrasinal é correcta se lle aplica o algoritmo de hash e se comproba si a chave xerada coincide.
- Verificar a integridade da información: Si cando aplicamos o algoritmo de hash a unha información e a chave xerada non coincide coa orixinal é que a información orixinal foi alterada.

O punto débil das funcións hash é a facilidade coa que se poden lograr colisións aplicando o algoritmo. Si conseguimos crear unha información que produza unha chave concreta o algoritmo de hash deixa de ser válido dende o punto de vista da seguridade. Algoritmos coñecidos son:

- SHA2 (SHA2-256, SHA2-512 …) - Amplio uso, o número indica o número de bits da chave xerada. A máis bits máis seguro, pero a maior custo computacional.
- MD5 – Inseguro, se atoparon colisións. Se utiliza para a verificación de integridade de arquivos.

Data Masking

A tokenización consiste en protexer a información sensible mediante o uso dun “token” en lugar dos datos orixinais.

- E moito máis rápido e consume menos recursos que o cifrado
- Ten aplicación na xeración de xogos de datos de proba

Este tipo de protección forma parte do estándar **PCI-DSS** (*Payment Card Industry Data Security Standard*) de protección de datos da tarxetas de crédito. A *RGPD* (Regulación General de Protección de Datos) e a *LODGCC* (Ley de Protección de Datos e Garantía de Dereitos Dixitais) tamén establecen o uso de esta técnica para evitar a posibilidade de identificación das persoas.

O Data-Masking se pode realizar mediante varias técnicas como:

- Cifrado simétrico
- Funcións hash
- Substituíndo parte dos datos (MAIL: ric****@****.com, IP: ***.***.12.1/16)
- Creando un diccionario de cadeas aleatorias

Cando realizamos Data Masking, os datos resultantes (tokens) deben:

- Parecer reais no seu formato
- Manter a integridade referencial nas bases de datos
- O enmascaramento debe ser repetible e dinámico. O enmascaramento dinámico se refire a presentación, mentres que o enmascaramento persistente se refire ao almacenamento.

Xestión de chaves de cifrado

A xestión das chaves de cifrado se refire ao proceso de xestión do ciclo de vida das chaves:

- Xeración e activación
- Uso
- Almacenamento e Custodia
- Arquivado
- Caducidade e renovación
- Destrucción

A xestión de chaves é un aspecto esencial. E esencial xestionar de modo seguro as nosas chaves criptográficas.

Sistemas de Xestión de Chaves

Os sistemas de xestión de chaves poden ser:

- Descentralizados
  - Os usuarios son responsables da súa propia xestión de chaves
- Distribuídos
  - Cada departamento da organización establece un protocolo de xestión de chaves.
- Centralizados
  - Toda a organización utiliza o mesmo protocolo de xestión. **É o modo recomendado.**

Os protocolos de xestión de chaves abranguen a tecnoloxía utilizada (aplicacións, servidores, algoritmos criptográficos…), as políticas (criterios de xestión de chaves) e o persoal especializado encargado. E importante o uso de seguridade física para protexer as chaves, e control dual / segregación de funcións.

TPM (Trusted Platform Module)

Hoxe en día os ordenadores dispoñen dun módulo hardware con capacidades criptográficas denominado ***TPM*** (*Trusted Platform Module*) que e esencial para o arranque seguro (***Secure Boot***) nos sistemas Microsoft Windows.

O Módulo TPM pode almacenar artefactos utilizados para autenticar a plataforma, que poden incluír contrasinais, certificados e chaves de cifrado.

Si activamos ***Secure Boot***, a UEFI/Bios se negará a cargar calquera Kernel ou drivers críticos que non estén firmados dixitalmente cunha chave recoñecida polo sistema TPM. Deste xeito se evita que se podan cargar drivers falsificados que permitan comprometer a seguridade do sistema. A activación de Secure Boot precisa que os sistemas que arranquemos teñan un kernel firmado cunha chave privada válida.

O hardware TPM pode crear, almacenar e utilizar chaves asimérticas RSA (sin a necesidade de cargalas en memoria), verificar o estado do software da plataforma mediante hashes e moito máis.

Os módulos TPM proporcionan:

- Capacidade de executar algoritmos de cifrado
- Un xerador de números aleatorios (*RNG – Random Number Generator*)
- Creación e almacenamento seguro de chaves de cifrado que poden utilizar diverso software e aplicacións
- Control do software que pode cargar a plataforma verificando criptográficamente o seu estado.

Os módulos TPM veñen cunha parella de chaves asimétricas RSA-2048 gravadas de fábrica (*Endorsement keys* ou ***EK***). A chave privada non é posible extraela do chip, todas as operacións se realizan no seu interor. A chave pública se utiliza para cifrar datos sensibles que se envían ao chip. Outras chaves de cifrado son:

- **SRK** (*Storage Root Key*): Creada a partir das **EK** e dunha password específica do propietario
- **AK** (*Attestation Key*): Se utiliza para cifrar información crítica do sistema e asegurar que esa información ven realmente do módulo TPM.

Software que pode facer uso do TPM aparte do Secure Boot: StrongsWan, Cisco AnyConnect, TrustedGRUB, Microsoft BitLocker, PGP/OpenPGP/GnuPG, Thunderbird, Microsoft Outlook, Chrome, Firefox…

TPM v2.0 será un requisito obrigatorio para a instalación de Windows 11, aínda que actualmente pode conseguirse instalar sin él
https://computerhoy.com/tutoriales/tecnologia/podras-instalar-windows-11-ordenador-no-tiene-chip-tpm-20-895355