**🔐 Criptografia: Conceitos e Aplicações**

**📌 Definição**

Criptografia é o processo de **codificar dados** de forma que apenas partes autorizadas possam acessá-los, garantindo a **confidencialidade** da informação.

**🔄 Tipos de Criptografia**

**🔒 Criptografia Simétrica**

* Utiliza a **mesma chave** para criptografar e descriptografar.
* É **mais rápida**, ideal para grandes volumes de dados.
* **Exemplos de algoritmos:**
  + **DES (Data Encryption Standard)**
  + **3DES (Triple DES)**
  + **AES (Advanced Encryption Standard)** → padrão da indústria; recomendado com chaves de **128 bits ou mais**.

**🔑 Criptografia Assimétrica**

* Utiliza **duas chaves distintas**:
  + **Pública** (para criptografar)
  + **Privada** (para descriptografar)
* **Mais lenta**, mas ideal para troca segura de chaves e autenticação.
* **Exemplos de algoritmos:**
  + **RSA (Rivest–Shamir–Adleman)**
  + **ECC (Elliptic Curve Cryptography)**
* **Aplicações comuns:** criptografia de chave simétrica durante troca de sessão e **assinaturas digitais** (autenticidade e integridade).

**🔄 Estados dos Dados e Criptografia**

Os dados podem existir em **três estados distintos**. Todos devem ser protegidos com criptografia adequada.

**🚚 Dados em Movimento (Data in Transit)**

**➤ Definição:**

Dados transferidos entre sistemas, redes ou dispositivos (ex: e-mails, uploads, mensagens).

**➤ Tecnologias de criptografia:**

* **TLS (Transport Layer Security)** – substitui o SSL.
* **HTTPS** (HTTP sobre TLS)
* VPNs e túneis seguros

**➤ Processo:**

1. Estabelecimento de sessão segura (criptografia assimétrica).
2. Transmissão de dados criptografados com chave simétrica.

**➤ Ameaças:**

* **Eavesdropping** (espionagem)
* **Sniffing** de pacotes não criptografados

**🖥️ Dados em Uso (Data in Use)**

**➤ Definição:**

Dados que estão sendo acessados, processados ou usados ativamente (ex: arquivos abertos, dados em RAM).

**➤ Proteções:**

* **Autenticação forte**:
  + MFA (Autenticação Multifator)
  + SSO (Single Sign-On)
* **Controle de acesso baseado em função** (RBAC)
* **Virtualização criptografada segura (SEV)**:
  + Utiliza **AES-128** na criptografia da memória RAM
  + Ex: AMD EPYC, Intel SGX

**➤ Ameaças:**

* **Ataques de autenticação** (brute-force, phishing)
* **Cold boot attacks**: extração de dados da RAM após desligamento

**💾 Dados em Repouso (Data at Rest)**

**➤ Definição:**

Dados armazenados e não utilizados ativamente (ex: bancos de dados, arquivos em HDs, SSDs, unidades USB, buckets de nuvem).

**➤ Técnicas de criptografia:**

* **Criptografia de disco completo (FDE)**
* **Criptografia de arquivos/sistema de arquivos**
* **Criptografia de banco de dados**
* **Criptografia de ativos em nuvem**

**➤ Boas práticas:**

* Usar algoritmos padrão da indústria (**AES**)
* Chaves fortes e rotacionadas periodicamente
* Armazenamento seguro das chaves:
  + **HSMs (Hardware Security Modules)**
  + **Cloud KMS** (Azure Key Vault, AWS KMS, GCP Cloud KMS)

**➤ Ameaças:**

* **Exfiltração de dados**
* **Acesso físico não autorizado** (dispositivos perdidos ou roubados)
* **Força bruta em chaves criptográficas**

**🔑 Gerenciamento de Chaves Criptográficas (Key Management)**

* Assegurar **armazenamento seguro** das chaves.
* Separar chave e dados.
* Utilizar **serviços dedicados**:
  + HSM local
  + Azure Key Vault / AWS KMS / GCP KMS

**✅ Resumo Rápido**

| **Tipo** | **Exemplos de Proteção** | **Principais Ameaças** |
| --- | --- | --- |
| **Em Movimento** | TLS, HTTPS, VPN | Sniffing, espionagem |
| **Em Uso** | SEV, MFA, SSO | Bypass de autenticação, cold boot |
| **Em Repouso** | AES, FDE, KMS, HSM | Exfiltração, roubo físico |