Princípios/Objetivos da Segurança

- Confidencialidade
- Autenticação
- Autorização (controle de acesso)
- Integridade
- Não-repúdio
- Auditoria/Registro (Accountability)
- Disponibilidade

Confidencialidade

Garantia de que uma informação permancerá confidencial àqueles que tem acesso autorizado a ela.

Desafio constante: inviabilizar a interceptação de mensagens

- Sobretudo em trocas de mensagens pela rede

Abordagem comum → criptografia

Autenticação

Autenticação → verificar/garantir a identidade de um objeto/sistema/usuário.

Mecanismos básicos de autenticação

- Algo que você sabe → ex: senha
- Algo que você tem → ex: smart card
- Alguma coisa que você é → ex: biometria

Cada mecanismo possui vantagens e desvantagens, com relação à aplicabilidade, possibilidade de fraude, erros.

Autorização

Ato de checar se um usuário ou sistema tem permissão para executar uma determinada ação.

Mecanismo geral de implementação: ACLs (listas de controle de acesso)

- Armazena uma lista dos usuários que podem realizar determinada operação

Implementado em diversos níveis complementares: SO, rede, aplicação

Integridade

Integridade de dado ou mensagem: garantia de que uma informação não foi modificada por terceiros (intencionalmente ou não).

Propriedade necessária para evitar ataques man-in-the-middle: alguém intercepta uma mensagem e a modifica de maneira a tirar proveito.

- Em redes → códigos de correção de mensagens (CRC),
- Não são suficientes para segurança

Em segurança devemos evitar modificações intencionais

Outra perspectiva: ao receber uma mensagem, como saber se alguém a modificou durante o caminho?

Não-repúdio

O objetivo do não-repúdio é garantir que nenhum usuário ou elemento do sistema possa negar a execução de uma ação.

Uma ação no sistema deve, por si só, provar que ela foi executada e por quem foi executada.

- **Exemplo**: Recibo digital de uma transação deve provar que ela de fato ocorreu → autenticação da fonte da transação

Também chamado **irrefutabilidade**

Auditoria/Registro (Accountability)

Accountability → responsabilização

Objetivo: garantir que será possível determinar quem gerou um ataque ou problema, caso algo dê errado no sistema ou uma transação equivocada seja identificada.

Auditoria/Registro → logs de sistema

Log seguro → difícil de ser adulterado

Disponibilidade

Um sistema **disponível** é um que responde às requisições de usuários em um tempo aceitável.

Geralmente associada ao requisito de desempenho, tem forte impacto na segurança.

Um ataque à disponibilidade (DoS) é um ataque que torna o uso de um sistema inviável para os usuários → acarreta perdas à empresa.

Ex: Fevereiro 2000: E*TRADE, Amazon, CNN, Yahoo fora do ar por 1 dia devido a ataque de DDoS. Perdas estimadas em US$ 1 bi