

Conceitos de Segurança da Informação

Gerência e Segurança de Redes



Objetivo de Aprendizagem

- Conhecer conceitos básicos de segurança da informação

Agenda

- Definição de segurança de computadores
- Objetivos
- Arquitetura OSI
- Tipos de ataques
- Serviços de Segurança
- Mecanismos de segurança da X.800

Conceitos Segurança de Computadores

National Institute of Standards and Technology (NIST)

- Instituto americano existente desde 1901
- Promove inovação e competitividade na indústria, ciência e TI

What We Do

Segurança de Computadores

Proteção oferecida para um sistema de informação automatizado a fim de alcançar os objetivos de preservar a integridade, a disponibilidade e a confidencialidade dos recursos do sistema de informação.

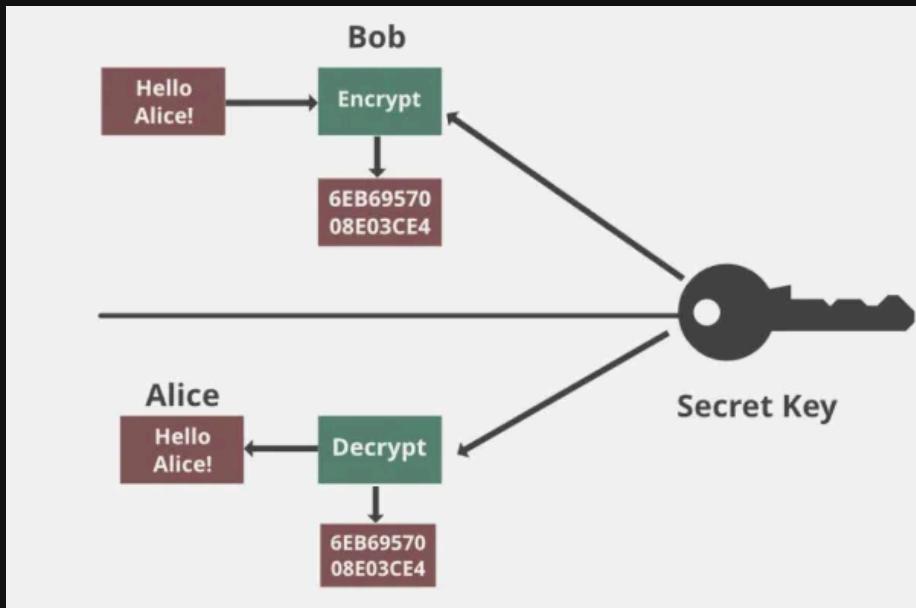
Objetivos

Cyber security

- Confidencialidade (*Confidentiality*)
- Integridade (*Integrity*)
- Disponibilidade (*Availability*)
- Tríade (CIA) da segurança cibernética

Confidencialidade

Confidencialidade de dados assegura que informações privadas e confidenciais não estejam disponíveis nem sejam revelados a terceiros



Confidencialidade

A perda de confidencialidade seria a divulgação não autorizada de informação de qualquer natureza a terceiros

Confidencialidade x Privacidade

Qualidade daquilo que é confidencial (que se diz ou que se faz com confiança e com segurança). Trata-se de uma **propriedade** da informação que pretende garantir o acesso unicamente às pessoas autorizadas

Privacidade assegura que os **indivíduos** controlem ou influenciem quais informações podem ser obtidas e armazenadas e quem pode ter acesso

Integridade

Integridade de dados assegura que informações e programas sejam modificados de forma específica e autorizada durante transmissão ou armazenamento

Integridade assegura que um sistema execute suas funcionalidades de forma íntegra, livre de manipulações intencionais de terceiros

Integridade

Prevenção contra a modificação ou destruição imprópria de informação, incluindo irretratabilidade e autenticidade. Perda de integridade seria a modificação ou destruição não autorizada da informação

Como garantir integridade?

Funções de *Hash* garantem a checagem da integridade de dados e programas

O que são hashes?

Algoritmos matemáticos que transformam qualquer bloco de dados em uma **código** de caracteres de tamanho fixo (*Message Digest*)

Exemplos:

- MD5, de 128bits
- SHA (*Secure Hash Algorithm*)
 - SHA-1, 160bits
 - SHA-256, 256bits
 - SHA-512, 512bits

Input	Digest
Fox	DFCD3454BBEA788A751A 696c24D97009CA992D17
The red fox jumps over the blue dog	008646BBFB7DCBE2823c ACC76CD190B1EE6E3ABC
The red fox jumps ower the blue dog	8FD8755878514F32D1C6 76B179A90DA4AEFE4819
The red fox jumps oevr the blue dog	FCD37FDB5AF2C6FF915F D401C0A97D9A46AFFB45
The red fox jumps oer the blue dog	8ACAD682D5884C754BF4 17997D88BCF892B96A6C

Disponibilidade

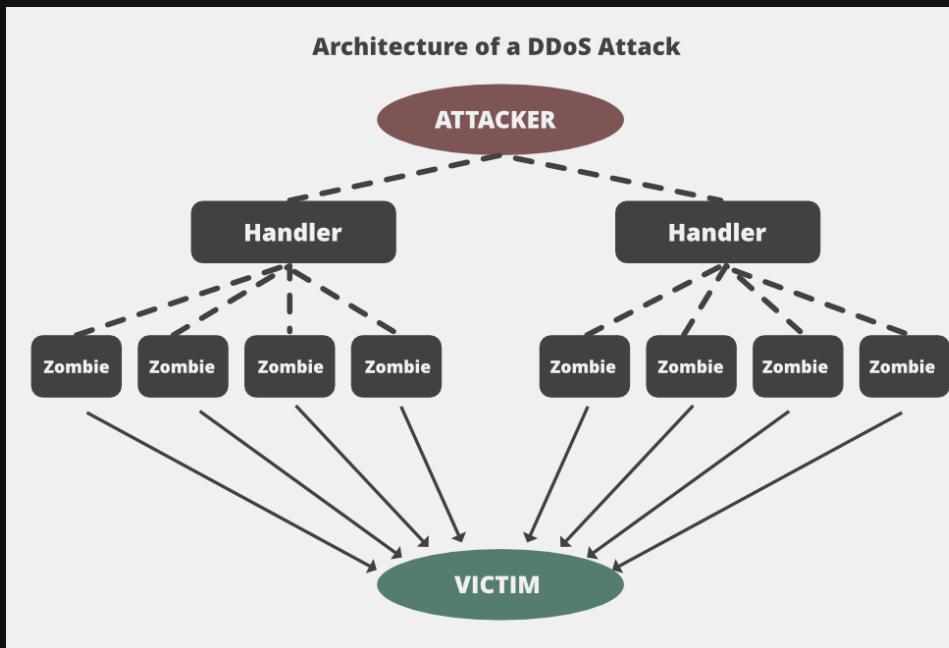
Integridade de dados assegura que os sistemas e dados operem prontamente e seus serviços não fiquem indisponíveis para usuários autorizados

Disponibilidade

Assegurar acesso e uso rápido e confiável da informação. Perda de disponibilidade é a perda de acesso ou de uso da informação ou sistema de informação

Riscos a Disponibilidade

- DoS (*Denial of Service*)
- Malwares



Níveis de Impacto

Baixo

- Considerado quando apenas um efeito adverso limitado nas operações é observado, tais como:
 - Degradação na capacidade de cumprir as funções primárias
 - Dano limitado aos recursos da organização
 - Perda financeira limitada

Níveis de Impacto

Moderado

- Considerado quando graves efeitos adversos nas operações ou recursos são observadas:
 - Degradação significativa na capacidade de cumprir as funções primárias
 - Dano expressivos aos recursos da organização
 - Perdas financeiras significativas

Níveis de Impacto

Alto

- Considerado quando efeitos adversos muito graves ou catastróficos nas operações ou recursos são observadas:
 - Perda da capacidade de cumprir as funções primárias
 - Danos grandes aos recursos da organização
 - Grandes perdas financeiras
 - Danos catastróficos aos indivíduos, risco de morte ou lesões

Exemplos

Confidencialidade (Impacto Baixo)

- FERPA (*Family and Education Rights and Privacy Act*), EUA. Protege informações relativas a notas de alunos.
- É pouco provável que esses dados sejam alvo de ataques e isso implica em menor dano se forem revelados

Exemplos

Integridade (Impacto Moderado)

- Dados de alergia de pacientes são um exemplo de informação que demandam um nível de integridade alto.
- Informações erradas podem levar a prescrições erradas podendo causar danos a saúde do paciente.

Exemplos

Disponibilidade (Impacto Alto)

- Sistemas financeiros, governamentais, inscrições *online*.
- Sistemas críticos de infra-estrutura

Arquitetura OSI

Recomendação X.800 (ITU -T)

- Metodologia para avaliar as necessidades de segurança de uma organização
- Organiza a tarefa de prover segurança

Concentra-se em:

- Ataques à segurança
- Mecanismos de segurança
- Serviços de segurança

Ataques à Segurança

Qualquer ação que comprometa a segurança da informação de uma organização.

Mecanismos de Segurança

Um processo ou dispositivo que é projetado para detectar, impedir ou recuperar-se de um ataque.

Serviços de Segurança

Serviço de processamento ou comunicação que aumenta a segurança dos sistemas de processamento e ou transferência de informação de uma organização. Servem para frustrar ataques à segurança utilizando um ou mais mecanismos.

Tipos de Ataques

Classificação (X.800)

- Ataques passivos
 - Visa acessar ou utilizar informações do sistema sem afetar os recursos.
- Ataques ativos
 - Tem como objetivo alterar, danificar, afetar a operação do sistema e/ou seus recursos.

Ataques Passivos

Exemplos

- Vazamento de conteúdo de uma mensagem eletrônica, ligação telefônica ou arquivos. Visa capturar informações sensíveis, reservadas ou confidenciais.
- Análise de tráfego busca identificar padrões na troca de mensagens, tais como frequência, tamanho, origem, destino da comunicação.

Ataques Ativos

Envolvem **modificação** no fluxo dos dados e/ou criação de fluxo falso

Categorias

- **Disfarce** quando uma entidade finge ser outra com privilégios maiores
- **Repasso** envolve a captura de dados e criação de uma nova retransmissão
- **Modificação** de mensagens envolve a captura de dados e retransmissão modificada
- **Negação de serviço** impede ou inibe a utilização normal das instalações

Serviços de Segurança

A X.800 define serviço de segurança como aquele fornecido por um protocolo de comunicação

São divididos em cinco categorias:

- Autenticação
- Controle de Acesso
- Confidencialidade dos Dados
- Integridade dos Dados
- Irretratabilidade

Existem 14 serviços definidos nas 5 categorias

X.800

Categorias

- Autenticação
- Controle de Acesso
- Confidencialidade dos Dados
- Integridade dos Dados
- Irretratabilidade

Autenticação

- **Autenticação de entidade pareada**, usada em associação com uma conexão lógica para fornecer confiança na identidade das entidades conectadas
- **Autenticação da origem de dados**, em uma transferência sem conexão, oferece certeza de que a origem dos dados recebidos é conforme alegada.

Controle de Acesso

Prevenção de uso não autorizado de um recurso, ou seja, esse serviço controla quem pode ter acesso a um recurso, sob que condições o acesso pode ocorrer e o que é permitido àqueles que acessam o recurso.

Confidencialidade

Confidencialidade da conexão

Garante a confidencialidade de todos os dados do usuário durante o uso da conexão

- **Exemplo**, uso de TLS (SSL) em uma conexão HTTPS, que garante que todo o fluxo entre cliente e servidor é cifrado.

Confidencialidade

Confidencialidade sem conexão

Protege dos dados do usuário em um único bloco de dados (PDU, *Protocol Data Unit*) sem exigir que uma conexão seja estabelecida

Exemplo, envio de um e-mail criptografado, onde cada mensagem é protegida individualmente e não necessariamente os meios de acessar o e-mail

Confidencialidade

Confidencialidade em campo seletivo,

Garante a confidencialidade dos dados em campos selecionados dentro dos dados dados do usuário em uma conexão ou bloco de dados

```
1  {
2    "idTransacao": "98372",
3    "agencia": "1234",
4    "conta": "567890-1",
5    "valor": 2500.75,
6    "moeda": "BRL",
7    "descricao": "Pagamento fornecedor",
8    "timestamp": "2025-09-14T13:45:00Z"
9  }
```

Confidencialidade

Confidencialidade em campo seletivo,

Garante a confidencialidade dos dados em campos selecionados dentro dos dados dados do usuário em uma conexão ou bloco de dados

```
1  {
2    "idTransacao": "98372",
3    "agencia": "1234",
4    "conta": "ENCRYPTED(4f7a8b ... )",
5    "valor": "ENCRYPTED(d2a3e1 ... )",
6    "moeda": "BRL",
7    "descricao": "ENCRYPTED(a9c4d6 ... )",
8    "timestamp": "2025-09-14T13:45:00Z"
9  }
```

Confidencialidade

Confidencialidade do fluxo de tráfego

Protege as informações derivadas dos fluxos de tráfego que possam identificar padrões de comunicação mesmo sem acesso às informações

Exemplo uso de redes anônimas como Tor, redes militares, as VPNs.

Técnicas padding, padronização de tamanhos de pacotes e encaminhamento por múltiplos caminhos

Integridade

Integridade da conexão com recuperação

Providencia a integridade de todos os dados do usuário em uma conexão e detecta qualquer modificação, inserção, exclusão ou repasse de quaisquer dados dentro de uma sequência inteira, com tentativa de recuperação

Exemplo

Um canal TLS com código de verificação (HMAC, *Hash-based Message Authentication Code*) em cada pacote, que permite detectar se houve alteração, além de retransmissão em caso de erro

Integridade

Integridade da conexão sem recuperação

Garante apenas que os dados não foram alterados ou inseridos de forma não autorizada, mas não corrige a falha

Exemplo

Protocolos que usam MAC (Message Authentication Code) para detectar alterações, mas encerram a sessão se um erro for detectado.

Integridade

Integridade da conexão com campo seletivo

Providencia a integridade de campos selecionados nos dados do usuário de um bloco de dados transferido por uma conexão e determina se os campos selecionados foram modificados, inseridos, excluídos ou repassados

Exemplo

Em um cabeçalho de protocolo, aplicar integridade apenas sobre os campos de controle, não sobre a carga útil

Integridade

Integridade sem conexão com recuperação

Providencia a integridade de um único bloco de dados sem conexão e pode tomar a forma de detecção da modificação de dados

Exemplo Sistemas de e-mail seguro (S/MIME ou PGP) que podem detectar e solicitar retransmissão de mensagens corrompidas

Integridade

Integridade sem conexão sem recuperação

Garante a integridade de mensagens individuais, mas apenas detecta a necessidade de alteração, sem corrigir.

Exemplo Assinatura digital em um contrato eletrônico em que caso o documento seja alterado, a assinatura não valida, sem a recuperação do original

Irretratabilidade (*non-repudiation*)

Irretratabilidade de origem

Garante que o remetente não possa negar ter enviado a mensagem

Exemplo

Uma assinatura digital em um e-mail ou contrato eletrônico; o emissor não pode negar autoria pois a assinatura depende de sua chave privada.

Irretratabilidade (*non-repudiation*)

Irretratabilidade de destino

Garante que o destinatário não possa negar ter recebido a mensagem

Exemplo

Protocolos de entrega de e-mail com confirmação assinada digitalmente, ou sistemas de mensagens corporativas que exigem recibo autenticado.

X.800

Mecanismos de Segurança

São incorporados a camadas de protocolos específicos

- Codificação
- Assinatura Digital
- Controle de Acesso
- Integridade dos Dados
- Troca de Autenticação
- Preenchimento de Tráfego
- Notarização

Mecanismos de Segurança

Codificação, criptografia ou *encipherment*

Aplicação de algoritmos matemáticos para transformar os dados para um formato que não seja prontamente inteligível. A transformação e subsequente recuperação dos dados depende de um algoritmo com zero ou mais chaves de encriptação

Mecanismos de Segurança

ASSINATURA DIGITAL

Dados anexados a uma unidade de dados que permite que um destinatário prove sua origem e integridade protegendo-se contra falsificação.

Mecanismos de Segurança

CONTROLE DE ACESSO

Conjunto de mecanismos que impõe direitos de acesso aos recursos

Mecanismos de Segurança

INTEGRIDADE DOS DADOS

Conjunto de mecanismos aplicados para garantir a integridade de uma unidade de dados ou fluxo unidades de dados.

Mecanismos de Segurança

TROCA DE AUTENTICAÇÃO

Conjunto de mecanismos aplicados para garantir a identidade de uma entidade por meio de troca de informações.

Mecanismos de Segurança

PREENCHIMENTO DE TRÁFEGO

A inserção de bits nas lacunas de um fluxo de dados para frustrar as tentativas de análise de tráfego.

Mecanismos de Segurança

CONTROLE DE ROTEAMENTO

Permite a seleção de determinadas rotas fisicamente seguras para certos dados e mudanças de roteamento, sobretudo quando uma brecha de segurança é suspeitada

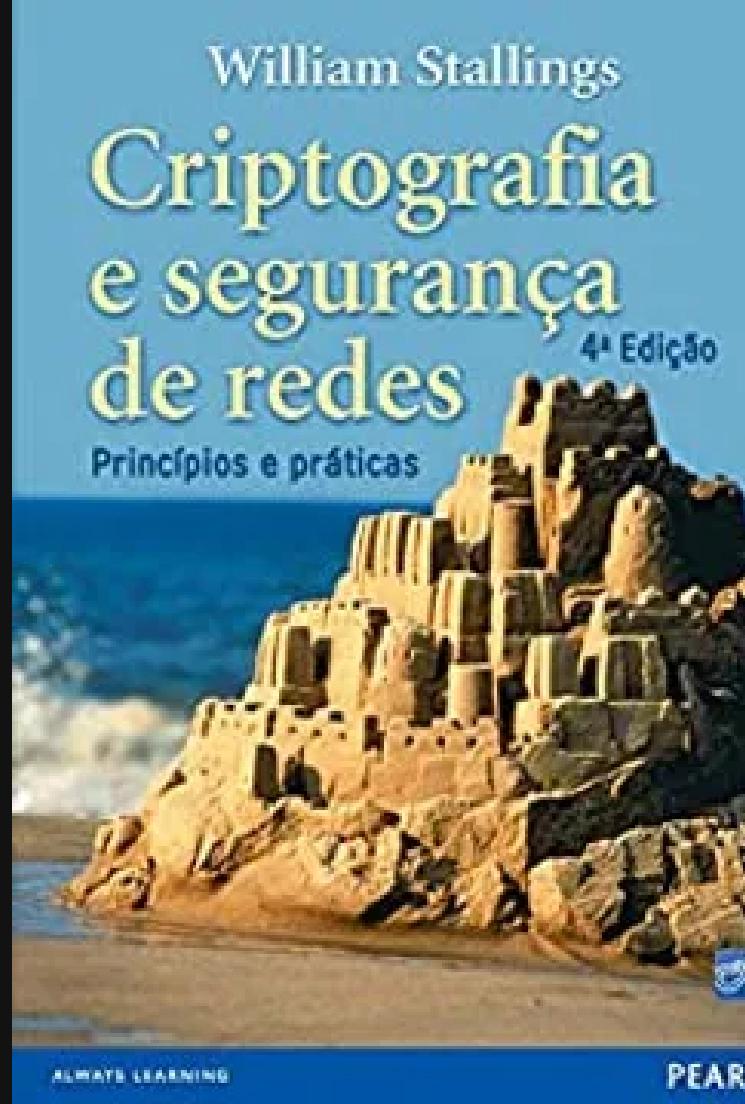
Mecanismos de Segurança

NOTARIZAÇÃO

Uso de um terceiro confiável para garantir determinadas propriedades de uma troca de dados

Referências

- Capítulo 1 . Criptografia e Segurança de Redes. William Stallings. 4a. Ed. Editora Pearson.
- NIST
- NIST drops controversial encryption algorithm



José Roberto Bezerra

jroberto@ifce.edu.br

<https://github.com/jroberto76>

Powered by  Sliddev

Foto da capa by Mona Bernhardsen na Unsplash

