Conceitos de Segurança da Informação

Gerência e Segurança de Redes

Objetivos de Aprendizagem

Introduzir conceitos básicos de segurança da informação

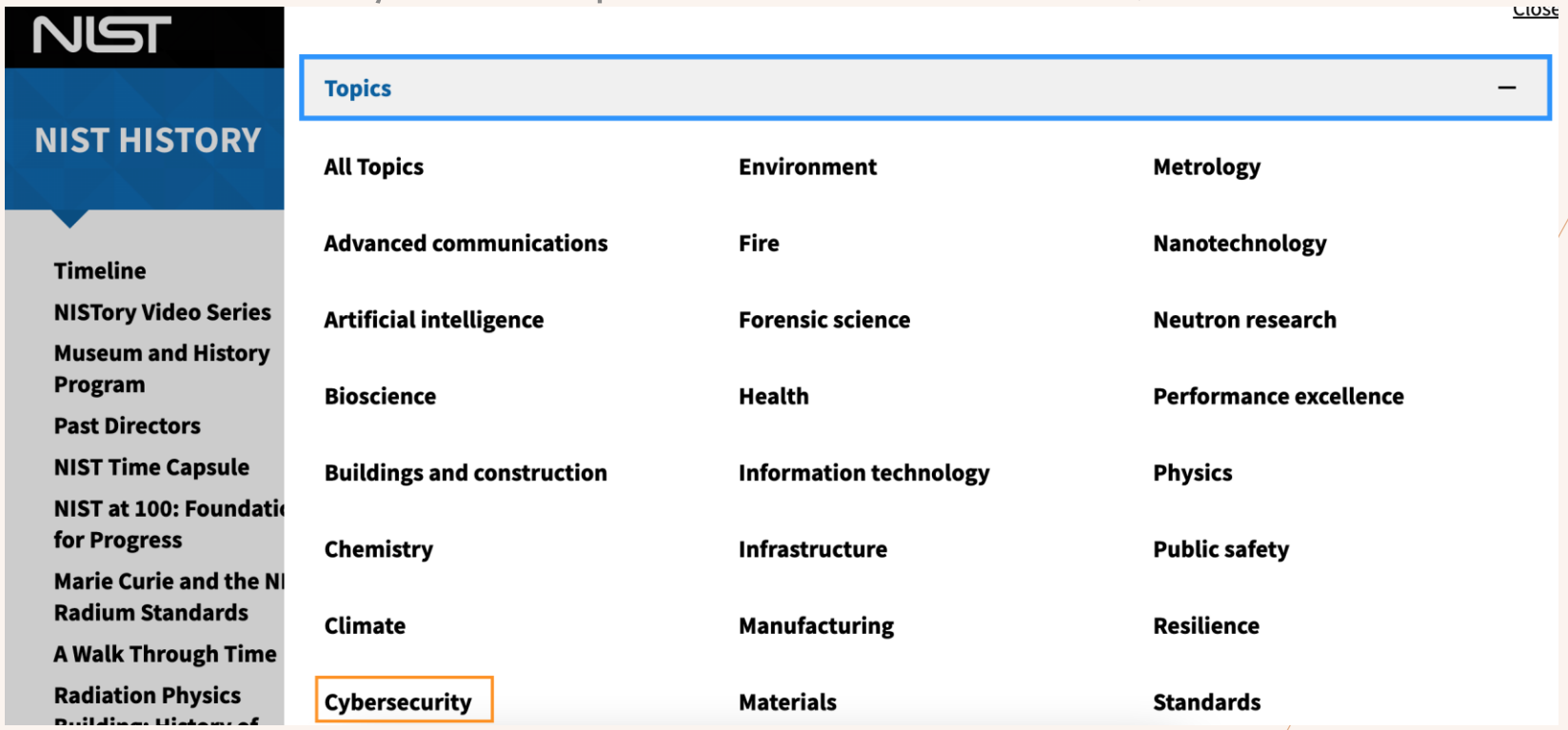
Agenda

1. Definição de segurança de computadores
2. Objetivos
3. Arquitetura OSI
4. Tipos de ataques
5. Serviços de Segurança
6. 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



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"

NIST

Objetivos

- 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

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

CONFIDENCIALIDADE

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

INTEGRIDADE

Integridade de dados assegura que informações e programas sejam modificados de forma específica e autorizada

Integridade do sistema assegura que um sistema execute suas funcionalidades de forma ilesa, livre de manipulações intencionais

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

DISPONIBILIDADE

Integridade de dados assegura que os sistemas 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

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

- **Moderada**

  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

  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

- ## Integridade

  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.

- ## Disponibilidade

  Sistemas financeiros, governamentais, inscrições online.

Arquitetura OSI

Recomendação X.800 (ITU-T)

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

  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

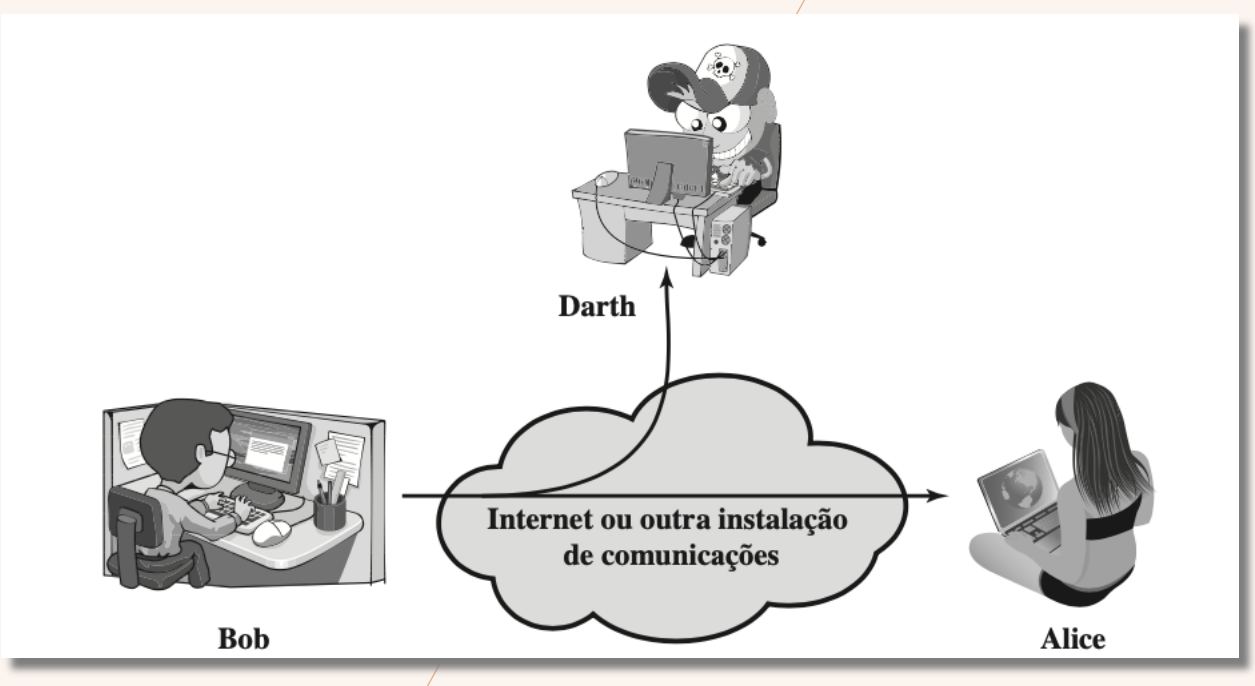
- ## Ataques passivos

  Visa acessar ou utilizar informações do sistema sem afetar os recursos.

- ## Exemplos

  Vazamento de conteúdo de uma mensagem eletrônica, ligação telefônica, 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

- ## Ataques ativos

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

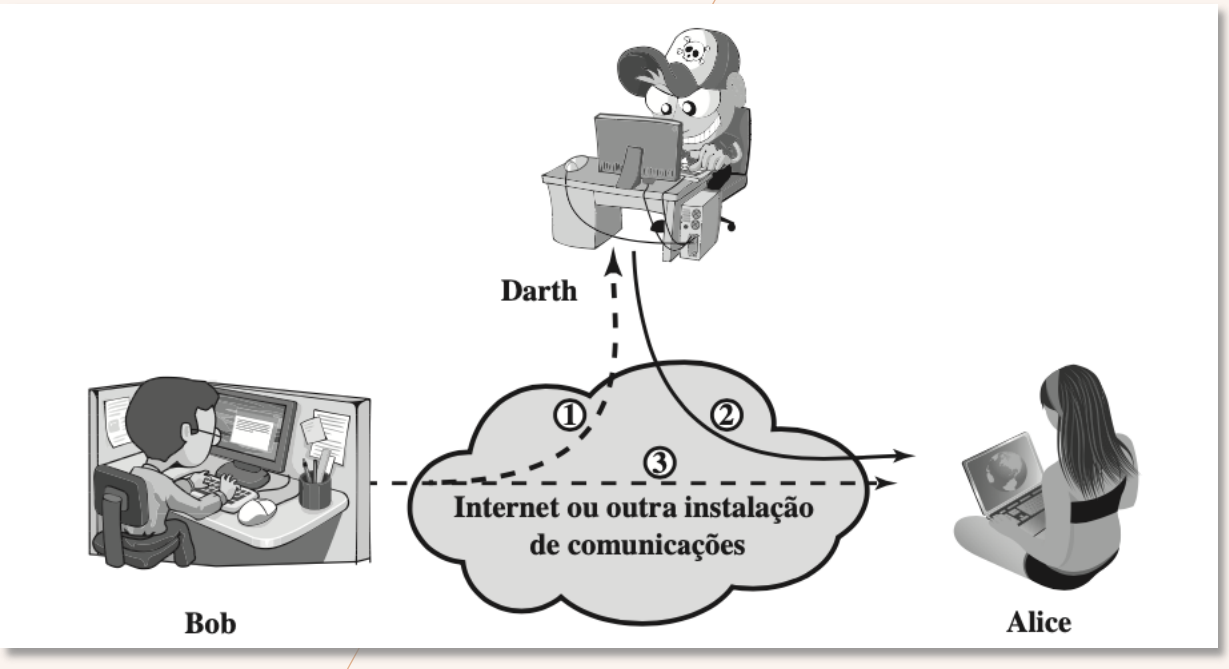
- ## Categorias

  Disfarce quando uma entidade finge ser outra com privilégios maiores.

  Repasse 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

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

- Autenticação
  - entidade pareada
  - origem de dados
- Controle de Acesso
- Confidencialidade dos Dados
  - Conexão
  - Sem conexão
  - Campo Seletivo
  - Fluxo de tráfego
- Integridade dos Dados
  - Conexão com recuperação
  - Conexão sem recuperação
  - Campo seletivo
  - Sem conexão
  - Sem conexão + Campo Seletivo
- Irretratabilidade
  - Origem
  - Destino

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

- **Confidencialidade sem conexão**

  Protege dos dados do usuário em um único bloco de dados

- **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

- **Confidencialidade do fluxo de tráfego**

  Protege as informações derivadas dos fluxos de tráfego

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.

- **Integridade de conexão sem recuperação**

  oferece apenas detecção sem tentativa de recuperação.

- **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.

- **Integridade sem conexão**

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

- **Integridade sem conexão com campo seletivo**

  providencia a integridade de campos selecionados dentro de um único bloco de dados sem conexão; determina se os campos selecionados foram modificados.

Irretratabilidade

- **Irretratabilidade de origem**

  Prova que a mensagem foi enviada pela parte especificada

- **Irretratabilidade de destino**

  Prova que a mensagem foi recebida pela parte especificada

Mecanismos de Segurança

- Incorporados a camadas de protocolos específicos
  - Codificação
  - Assinatura Digital
  - Controle de Acesso
  - Integridade dos Dados
  - Troca de Autenticação
  - Preenchimento de Tráfego
  - Notarização

CODIFICAÇÃO

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.

ASSINATURA DIGITAL

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

CONTROLE DE ACESSO

Conjunto de mecanismos que impõe direitos de acesso aos recursos

INTEGRIDADE DOS DADOS

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

TROCA DE AUTENTICAÇÃO

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

PREENCHIMENTO DE TRÁFEGO

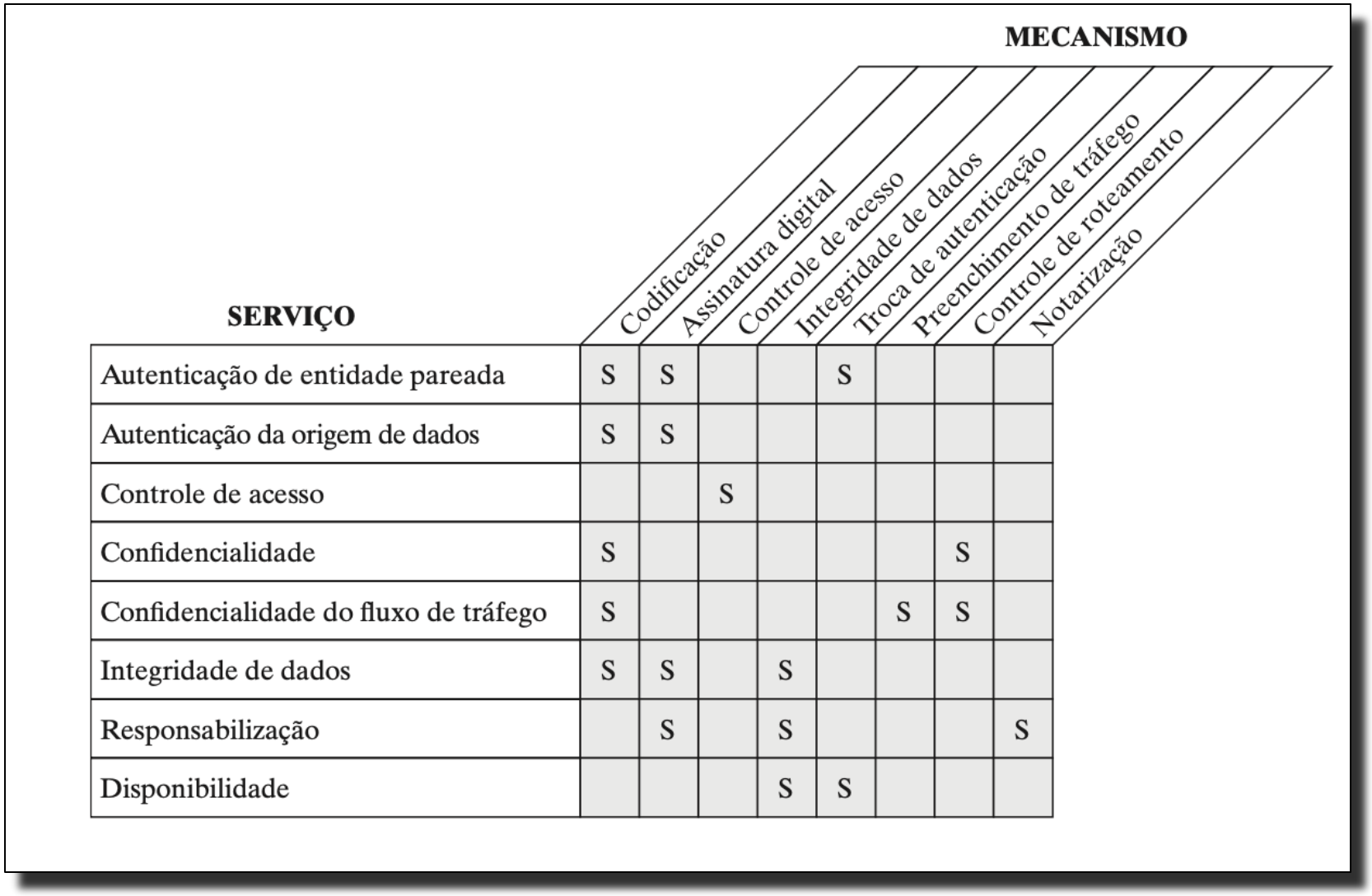
A inserção de bits nas lacunas de um fluxo de dados para frustrar as tentativas de análise de tráfego.

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.

NOTARIZAÇÃO

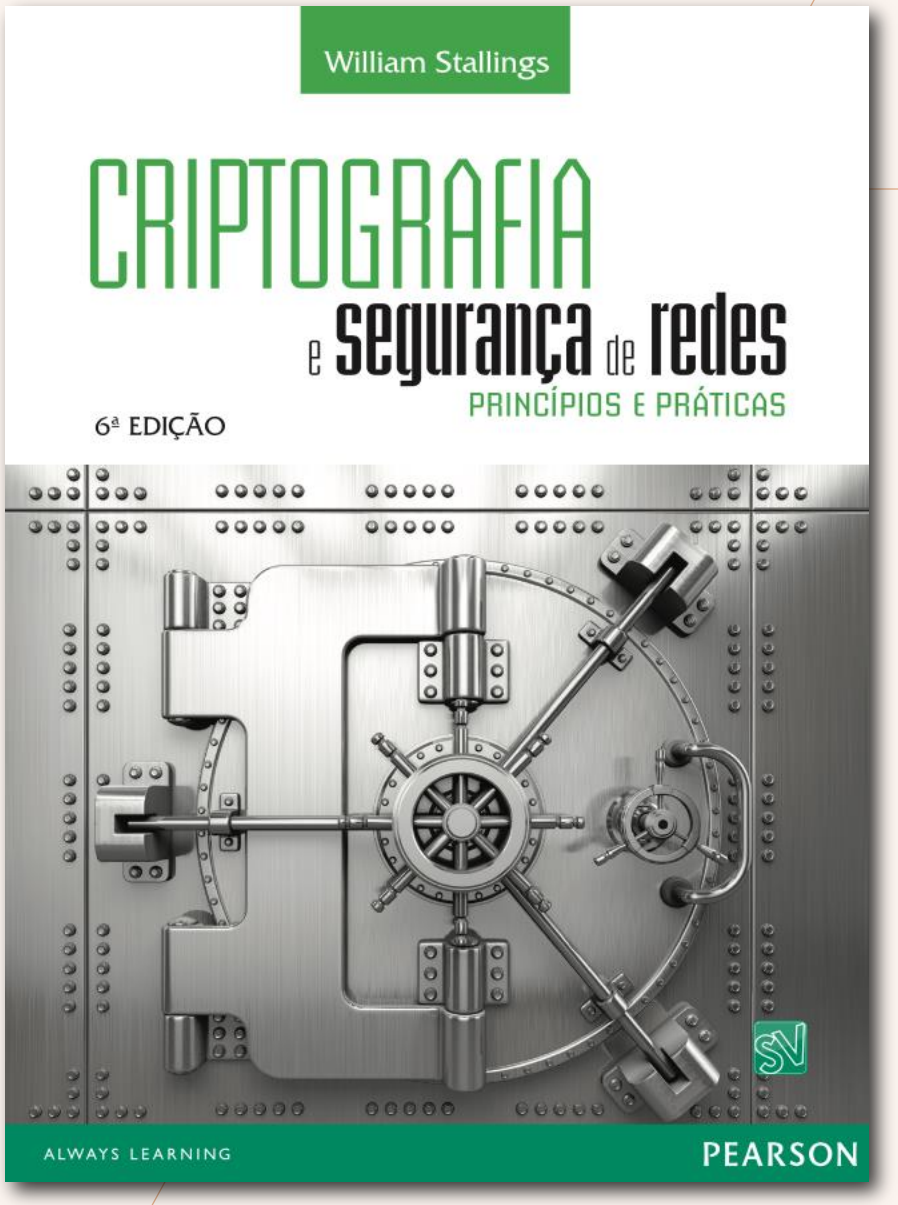
Uso de um terceiro confiável para garantir determinadas propriedades de uma troca de dados.



SERVIÇO \ MECANISMO	Codificação	Assinatura digital	Controle de acesso	Integridade de dados	Troca de autenticação	Preenchimento de tráfego	Controle de roteamento	Notarização
Autenticação de entidade pareada	S	S			S			
Autenticação da origem de dados	S	S						
Controle de acesso			S					
Confidencialidade	S						S	
Confidencialidade do fluxo de tráfego	S					S	S	
Integridade de dados	S	S		S				
Responsabilização		S		S				S
Disponibilidade				S	S			

Referências

- **Capítulo 1**. Criptografia e Segurança de Redes. *William Stallings*. 6ª. Edição. Editora Pearson.



Referências

- https://fedscoop.com/nist-drops-controversial-encryption-algorithm/
- https://www.nist.gov/cybersecurity

FIM

Prof. José Roberto Bezerra

jbroberto@ifce.edu.br

IFCE – *Campus* Fortaleza