CETEPI - I
PAULO AFONSO

EDUCAÇÃO PROFISSIONAL DA BAHIA
Trabalho, Educação e Desenvolvimento

SEGURANÇA DE SISTEMAS E REDES

TÁSSIO JOSÉ GONÇALVES GOMES
www.tassiogoncalves.com.br
tassiogoncalvesg@gmail.com

CONTEÚDO

- **Serviços de Segurança**
  - Autenticação
  - Controle de Acesso
  - Confidencialidade dos Dados
  - Integridade de Dados
  - Irretratabilidade
- **Mecanismos de Segurança**
  - Mecanismos de Segurança Específicos
  - Mecanismos de Segurança Difusos
- **Um Modelo para Segurança de Rede**

SERVIÇOS DE SEGURANÇA

Segundo a RFC 4949, Serviços de Segurança é um serviço de processamento ou comunicação que é fornecido por um sistema para dar um tipo específico de proteção aos recursos do sistema; os serviços de segurança implementam políticas (ou diretrizes) de segurança e são implementados por mecanismos de segurança.

Esses serviços podem ser divididos em categorias e serviços específicos.

SERVIÇOS DE SEGURANÇA

AUTENTICAÇÃO	CONTROLE DE ACESSO	CONFIDENCIALIDADE DOS DADOS	INTEGRIDADE DE DADOS	IRRETRATABILIDADE
Autenticação de entidade pareada		Confidencialidade da conexão	Integridade da conexão com recuperação	Irretratabilidade, origem
Autenticação da origem de dados		Confidencialidade sem conexão	Integridade da conexão sem recuperação	Irretratabilidade, destino
		Confidencialidade com campo seletivo	Integridade da conexão com campo seletivo	
		Confidencialidade do fluxo de tráfego	Integridade sem conexão	
			Integridade sem conexão com campo seletivo	

AUTENTICAÇÃO

O serviço de autenticação refere-se à garantia de que uma comunicação é autêntica.

- Única mensagem;
- Interação em curso:
  - Início da conexão entre duas entidades;
  - Garantir que a conexão não sofra interferência.

AUTENTICAÇÃO

Dois serviços de autenticação específicos são definidos:

- **Autenticação da entidade pareada:** fornece autenticação para a identidade de uma entidade pareada em uma associação.
- **Autenticação da origem de dados:** fornece autenticação para a origem de uma unidade de dados.

CONTROLE DE ACESSO

No contexto da segurança de redes, o controle de acesso é a capacidade de limitar e dominar o acesso aos sistemas e aplicações por meio de links de comunicação.

CONFIDENCIALIDADE DOS DADOS

A proteção dos dados contra divulgação não autorizada.

- **Confidencialidade da conexão** - a proteção de todos os dados do usuário em uma conexão.
- **Confidencialidade sem conexão** - a proteção de todos os dados do usuário em um único bloco de dados.
- **Confidencialidade com campo seletivo** - a confidencialidade de campos selecionados dentro dos dados do usuário em uma conexão ou em um único bloco de dados.
- **Confidencialidade do fluxo de tráfego** - a proteção das informações que poderiam ser derivadas dos fluxos de tráfego.

CONFIDENCIALIDADE DOS DADOS

O outro aspecto da confidencialidade é a proteção do fluxo de tráfego contra análise. Isso exige que um atacante não consiga observar a origem e o destino, a frequência, o tamanho ou outras características do tráfego em uma comunicação.

INTEGRIDADE DE DADOS

A certeza de que os dados recebidos são exatamente conforme enviados por uma entidade autorizada (ou seja, não contêm modificação, inserção, exclusão ou repasse).

INTEGRIDADE DE DADOS

- **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 da conexão sem recuperação** - Como acima, mas 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 DE DADOS

- **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. além disso, pode haver uma forma limitada de detecção de repasse.
- **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

A irretratabilidade impede que o emissor ou o receptor neguem uma mensagem transmitida. Assim, quando uma mensagem é enviada, o receptor pode provar que o emissor alegado de fato a transmitiu. De modo semelhante, quando uma mensagem é recebida, o emissor pode provar que o receptor alegado de fato a obteve.

IRRETRATABILIDADE

Oferece proteção contra negação, por parte de uma das entidades envolvidas em uma comunicação, de ter participado de toda ou parte dela.

- **Irretratabilidade, origem** - prova de que a mensagem foi enviada pela parte especificada.
- **Irretratabilidade, destino** - prova de que a mensagem foi recebida pela parte especificada.

MECANISMOS DE SEGURANÇA

Os mecanismos são divididos entre aqueles implementados em uma camada de protocolo específica e aqueles que não são específicos a camadas de protocolo ou serviços de segurança em particular.

- **Mecanismos de Segurança Específicos**

- **Mecanismos de Segurança Difusos**

MECANISMOS DE SEGURANÇA ESPECÍFICOS

Podem ser incorporados à camada de protocolo apropriada a fim de oferecer alguns dos serviços de segurança OSI.

- Codificação
- Assinatura digital
- Controle de acesso
- Integridade de dados
- Troca de autenticação
- Preenchimento de tráfego
- Controle de roteamento
- Notarização

MECANISMOS DE SEGURANÇA DIFUSOS

Mecanismos que não são específicos a qualquer serviço de servidor OSI ou camada de protocolo específica.

- Funcionalidade confiada
- Rótulo de segurança
- Detecção de evento
- Trilha de auditoria de segurança
- Recuperação de segurança

RELACIONAMENTO ENTRE SERVIÇOS E MECANISMOS DE SEGURANÇA

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			

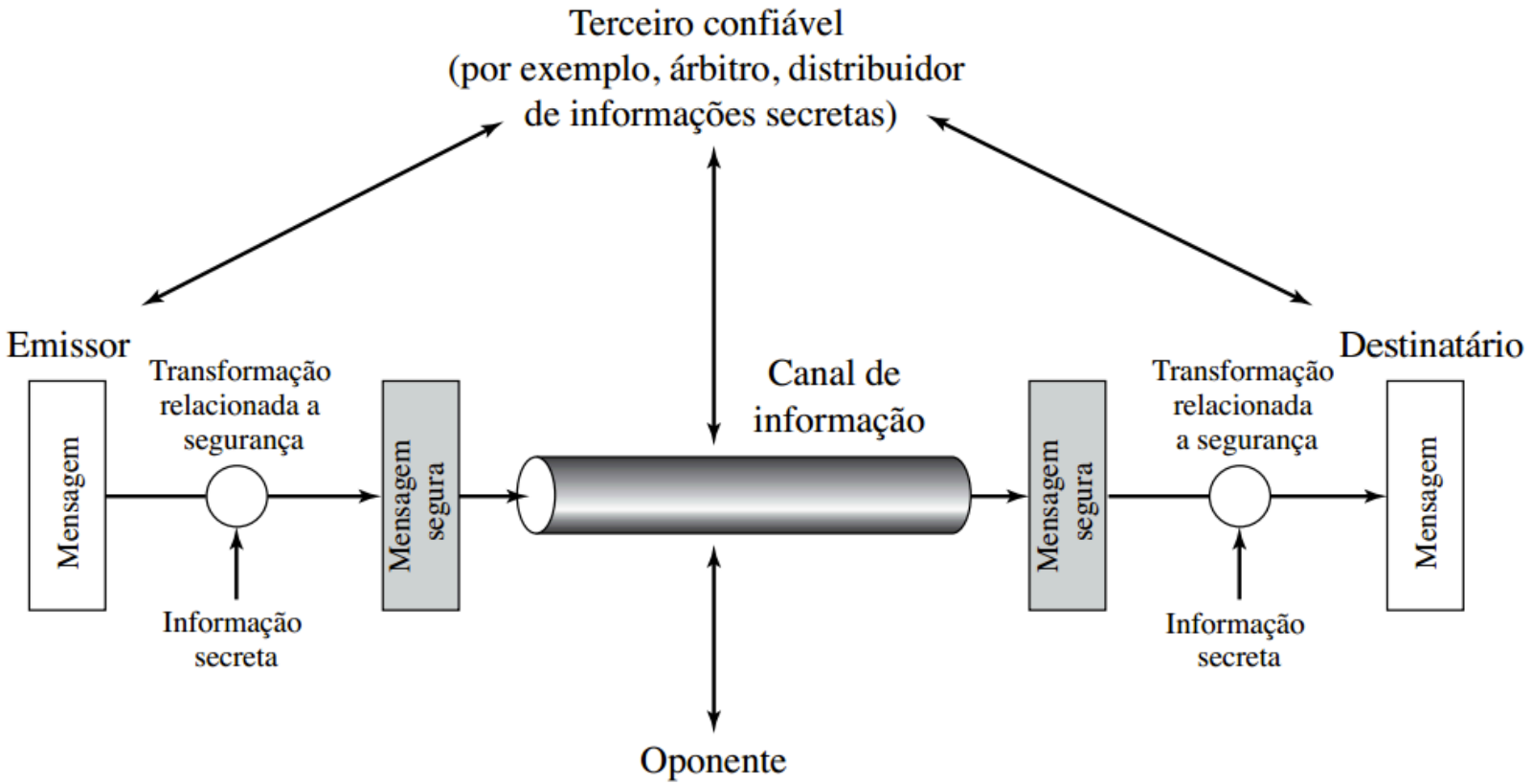
MODELO PARA SEGURANÇA DE REDE

Uma mensagem deve ser transferida de uma parte para outra por meio de algum tipo de inter-rede.

As duas partes, que são os principais nessa transação, precisam cooperar para que a troca ocorra.

Um canal de informação lógico é estabelecido definindo-se uma rota pela inter-rede da origem ao destino, e pelo uso cooperativo de protocolos de comunicação (por exemplo, TCP/IP) pelos dois principais

MODELO PARA SEGURANÇA DE REDE



MODELO DE SEGURANÇA DE ACESSO À REDE