Introdução
Segurança - Conceitos

- Conforme a recomendação X.800 (Security Architecture for OSI) do ITU-T International Telecommunication Union (ITU), Telecommunication Standardization Sector (ITU-T)
- Ataque
  - Ação que compromete a segurança da informação de uma organização
- Mecanismo de Segurança
  - Um processo (ou dispositivo) utilizado para detectar, prevenir ou recuperar da ação de um ataque
- Serviço de Segurança
  - Um processo ou serviço de comunicação que aumenta a segurança de sistemas de processamento de dados e de transferência de informação de uma organização
  - O serviços atuam contra ataques e utilizam um ou mais mecanismos de segurança

Introdução
Ameaça x Ataque

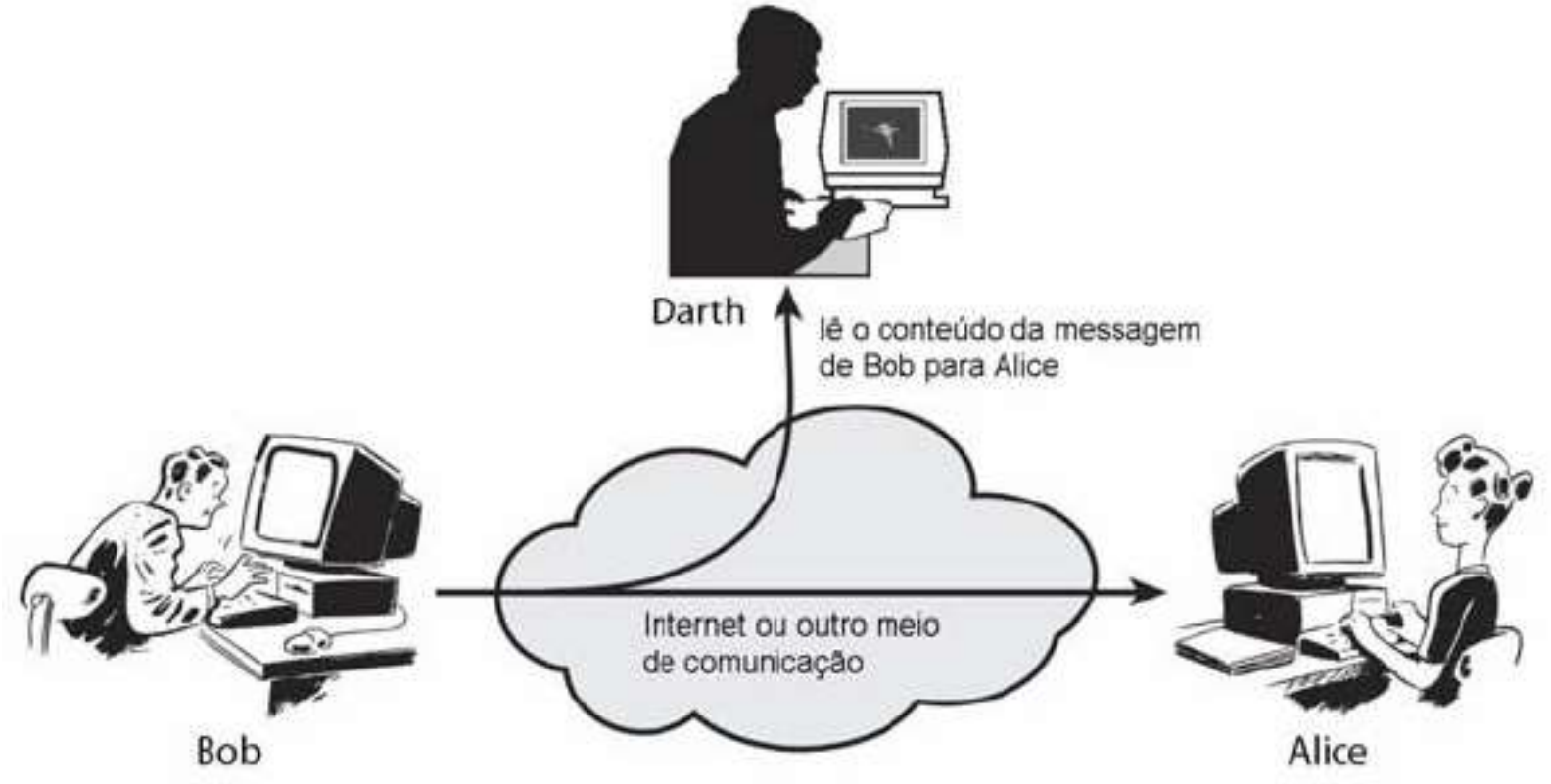
- Definições conforme a RFC 2828 (Internet Security Glossary)
- Ameaça (Threat)
  - Existência de um potencial para uma violação.
  - Ocorre devido a existência de uma circunstância, capacidade, ação ou evento que pode quebrar a segurança e causar danos
  - Um perigo possível que pode explorar uma vulnerabilidade
- Ataque (Attack)
  - Um assalto ao sistema de segurança causado a partir de uma ameaça
  - Um ato inteligente que é empreendido de forma deliberada para esquivar-se dos serviços de segurança e violar a política de segurança de um sistema
  - Os Ataques podem ser:
    - Passivos ou Ativos

Introdução
Tipos de Ataques - Passivos

- Baseados no monitoramento das transmissões
- Objetivo é obter a informação que está sendo transmitida
- De difícil detecção pois não envolvem nenhuma alteração de dados
- Maneiras usuais: Conhecimento Mensagem da Transmitida e Análise do Tráfego
- Conhecimento Mensagem da Transmitida
  - Basicamente a mensagem que contém informações confidenciais é conhecida pelo oponente
- Análise do Tráfego
  - Neste caso o oponente consegue identificar as partes existentes na comunicação (hosts) e observar a freqüência em que as mensagens são trocadas, seu comprimento e seus dados
  - A partir da análise desta informações é possível acessar as informações confidenciais (ativos)
- Uma maneira para prevenir contra tais ataques é através do uso de criptografia
- Neste tipo de ataque o mais importante é a sua prevenção

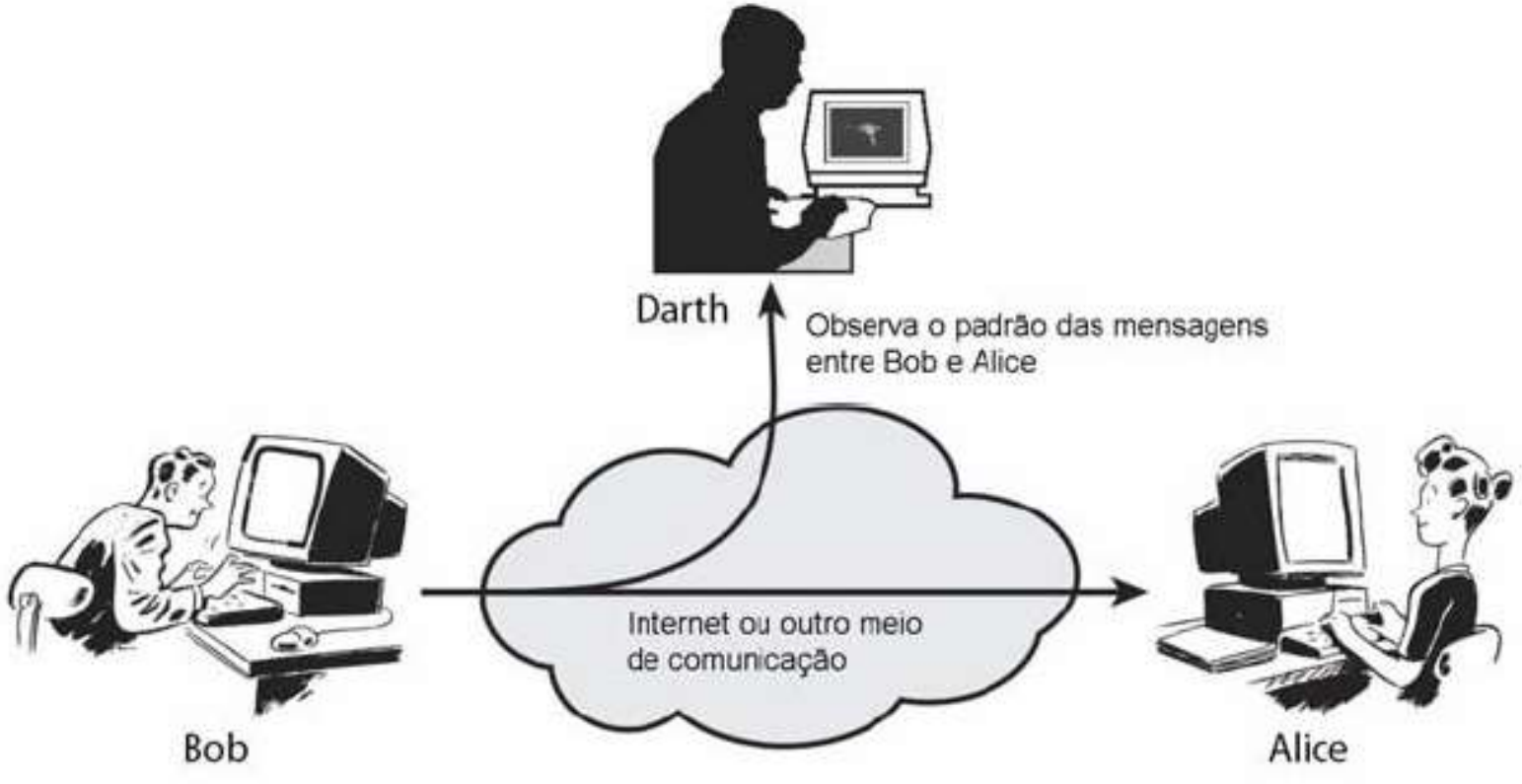
Introdução
Ataques Passivos

- Conhecimento Mensagem da Transmitida



Introdução
Ataques Passivos

- Análise do Tráfego



Introdução
Tipos de Ataques - Ativos

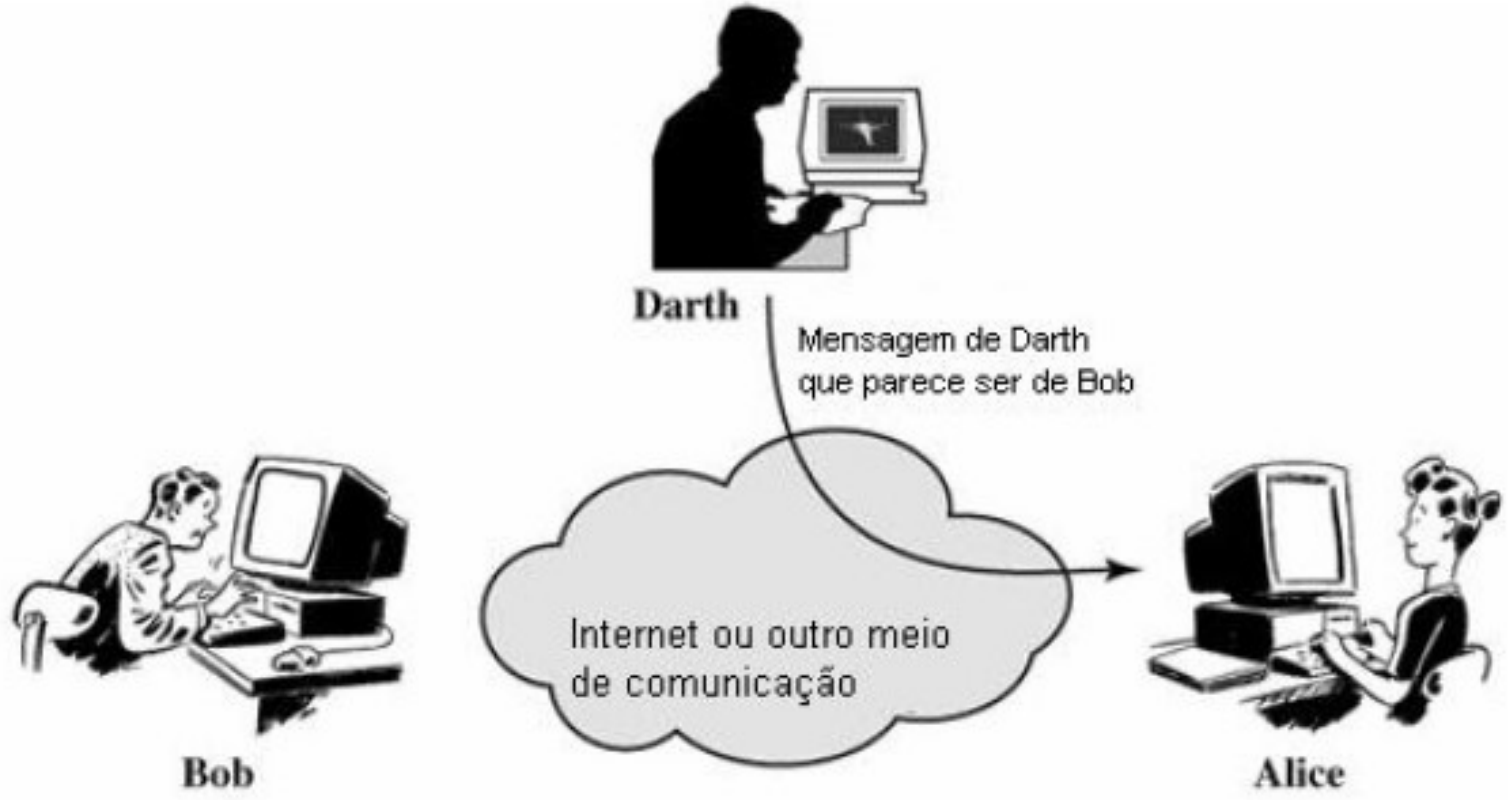
- Neste caso a mensagem é modificada ou um mensagem falsa é criada
- Existem quatro tipos de ataques ativos: Representação ; Reenvio; Modificação e Negação de serviço
- Representação (Mascarade)
  - Uma entidade finge ser outra, ou seja, representa um papel que não é o seu
  - Normalmente inclui outras formas de ataque ativo. Ex: Seqüência de autenticação valida é obtida e então reenviada. Neste caso o oponente finge ser quem não é.
- Reenvio (Replay)
  - Neste caso é executada uma captura passiva de dados e então é feita uma retransmissão produzindo efeitos danosos
- Modificação (Message Modification)
  - Neste casos partes de uma mensagem legítima é alterada ou então as mensagens são atrasadas ou reordenadas a fim de produzir novos efeitos

Introdução
Tipos de Ataques - Ativos

- Negação de Serviço (Denial of Service)
  - Impede o uso normal de um serviço proporcionado por um sistema
  - Exemplos:
    - Uma entidade impede que todas as mensagens direcionadas a um sistema de auditoria sejam enviadas
    - Interrupção de uma rede ou de um servidor, através da sobrecarga do mesmo com muitas mensagens a fim de degradar sua performance

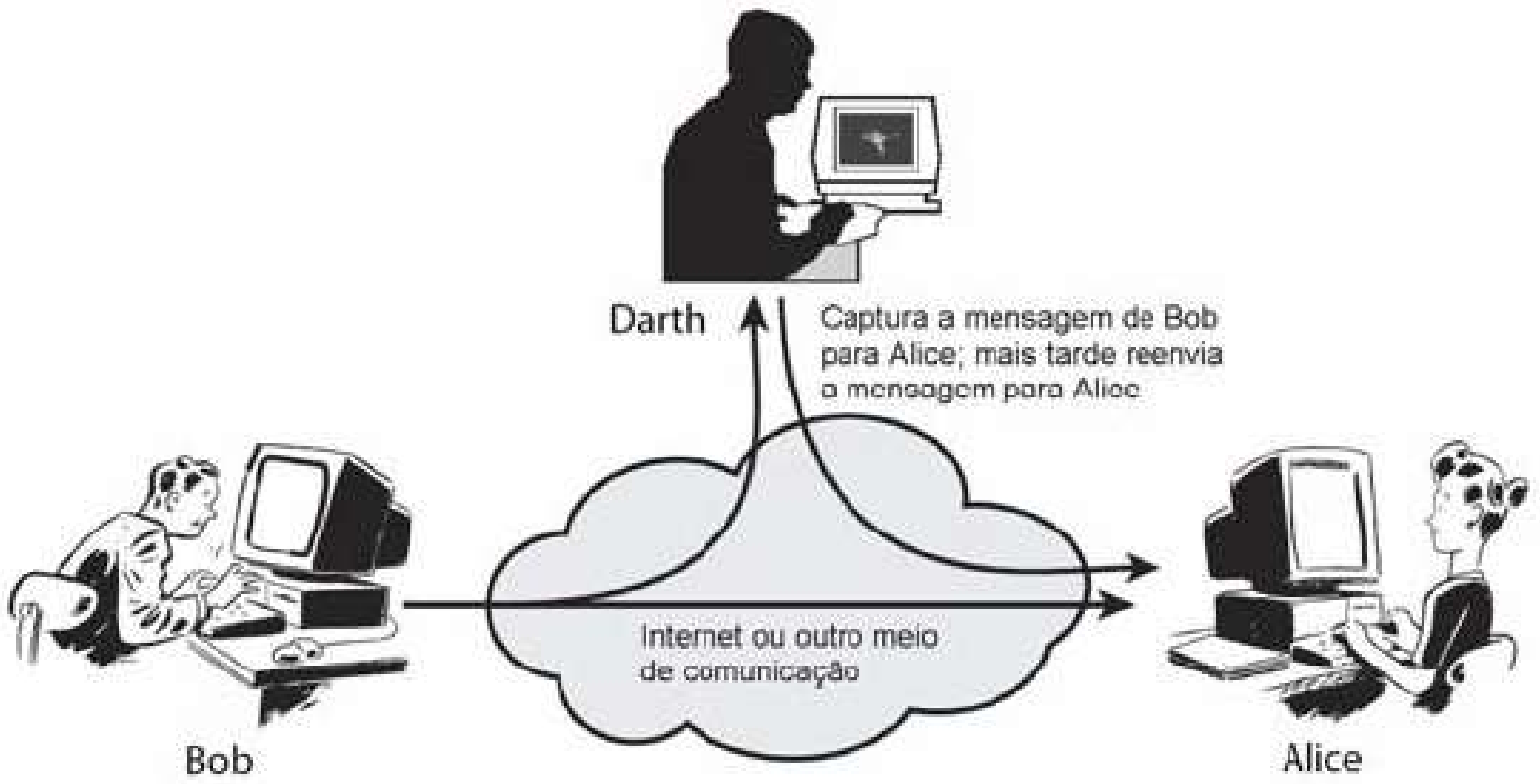
Introdução
Tipos de Ataques - Ativos

- Representação (Mascarade)



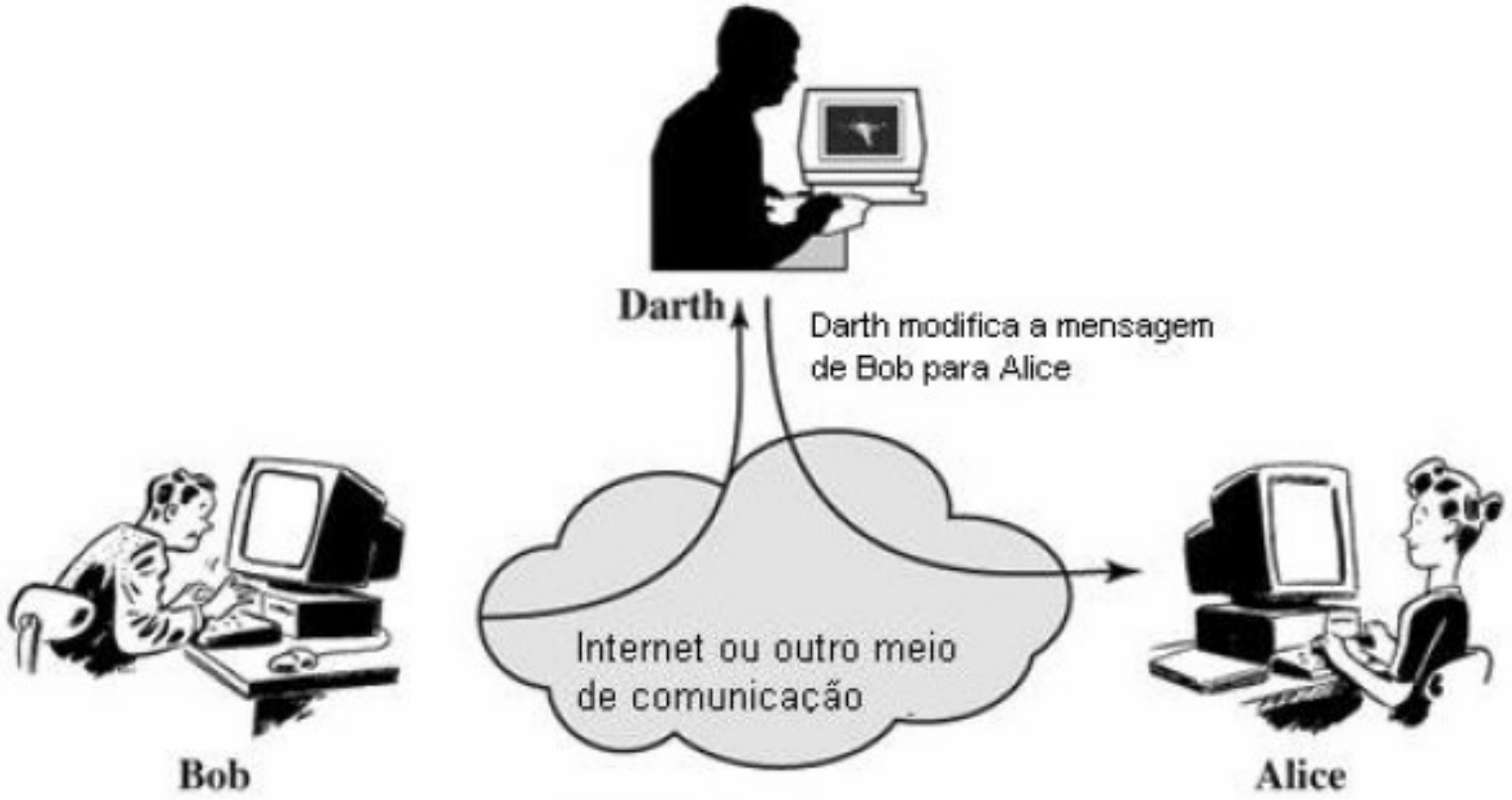
Introdução
Tipos de Ataques - Ativos

- Reenvio (Replay)



Introdução
Tipos de Ataques - Ativos

- Modificação (Message Modification)



Introdução
Tipos de Ataques - Ativos

- Negação de Serviço (Denial of Service)

Introdução
Serviços de Segurança

- Um serviço ou processo de comunicação oferecido por um sistema a fim de oferecer uma proteção específica a recursos de um sistema. (Definição RFC 2828)
- Serviços de segurança implementam políticas de segurança
- Serviços de segurança utilizam mecanismos de segurança
- Serviços de Segurança
  - Autenticação
  - Controle Acesso
  - Confidencialidade
  - Integridade
  - Não-Repúdio
  - Disponiblidade

Introdução – Serviços Segurança Autenticação

- Envolve a capacidade de identificar e garantir que um usuário, um sistema ou a informação é realmente quem afirma ser
  - Normalmente o consumidor do serviço precisa provar que ele realmente é quem afirma ser.
  - Do mesmo modo, é importante que o comprador tenha certeza que o vendedor é quem afirma ser.
  - Autenticação de uma Entidade
    - Utilizada em ambientes com conexão a fim de garantir a identidade das partes na comunicação
  - Autenticação da Origem dos Dados
    - Utilizada em ambientes sem conexão a fim de garantir que a origem dos dados é quem afirma ser
- A autenticação é crítica, pois normalmente é a porta de entrada para a maioria dos sistemas
- Um agente mal intencionado, poderia acessar os mais variados ativos e produzir grandes prejuízos.

Introdução – Serviços Segurança Autorização

- Após autenticar uma entidade (usuário ou um sistema) é necessário determinar quais operações o mesmo está autorizado a realizar.
- O processo de autorização passa então por estabelecer quais os privilégios que a entidade autenticada pode usufruir naquele domínio.

Introdução – Serviços Segurança Confidencialidade

- A confidencialidade é a capacidade de garantir que o conteúdo de uma mensagem não seja observado por partes alheias à comunicação.
  - Serviço Orientado à conexão
    - Proteção de todos os dados na conexão (todas as mensagens)
  - Serviço Sem conexão
    - Proteção de todos os dados do usuário existentes em uma mensagem
  - Confidencialidade Seletiva
    - Confidencialidade de partes selecionadas da mensagem em uma conexão ou um bloco simples
  - Confidencialidade do tráfego
    - Proteção da informação, evitando o observação do fluxo de dados
- Um meio usualmente utilizado para garantir a confidencialidade é a criptografia
- Outra forma de garantir a confidencialidade é garantir o acesso a dados e sistemas somente para partes devidamente autorizadas

Introdução – Serviços Segurança Integridade

- Consiste na capacidade de garantir que as mensagens estão intactas e que não foram alterados de maneira deliberada, ou acidental.
- Desta forma as mensagens são recebidas da maneira que foram enviadas uma entidade autorizada não contendo modificações; inserções; remoções ou mesmo reenvio
  - Serviços com Conexão Íntegros e com Recuperação
    - Integridade de todos os dados da conexão, com a detecção de modificações, inserções, remoções e reenvio de mensagens.
    - Em caso de problemas as mensagens originais são recuperadas
  - Serviços com Conexão Íntegros sem Recuperação
    - Neste caso ocorre apenas a detecção de falha na integridade, sem as necessárias correções
  - Serviços com Conexão e Integridade Seletiva
    - Integridade de partes da mensagem transferida em uma conexão
  - Serviços sem Conexão Íntegros
    - Integridade de um bloco de dados (mensagem), com a detecção de alterações
    - Adicionalmente uma forma de detecção de reenvio pode ser oferecida
  - Serviços sem Conexão e com Integridade Seletiva
    - Integridade de partes da mensagem transferidas, determinando a modificação nas mesmas

Introdução – Serviços Segurança Não-Repúdio

- Capacidade que uma entidade ou sistema possui de garantir que determinada parte, realizou alguma operação e, portanto não pode negá-la em um momento posterior.
- Desta forma é possível afirmar que um determinado consumidor realizou as operações e deve ser responsabilizar pelos resultados da mesma.
- Não-Repúdio da Origem
  - Prova de que a mensagem foi enviada por uma entidade específica
- Não-Repúdio do Destino
  - Prova de que a mensagem foi recebida por uma entidade específica
- A autenticação tem um papel importante no não-repúdio, pois a garantia de que o cliente é ele mesmo é uma condição fundamental para o não repúdio a outra é a capacidade de armazenar registros de segurança como autenticação, assinaturas, a fim de realizar uma auditoria futura no sistema.

Introdução – Serviços Segurança Disponibilidade

- A disponibilidade da informação permite que:
  - Possa ser acessada no momento em que for necessário utilizá-la;
  - Esteja ao alcance de seus usuários ou destinatários.
- Refere-se à toda a informação e de toda a estrutura física e tecnológica que permite o acesso, a transmissão e o armazenamento.
- Indica o quanto o sistema estará em funcionamento, independente ou não de erros.
- Um serviço de disponibilidade garante o sistema contra a falta de disponibilidade

Introdução
Mecanismos de Segurança

- Recomendação X.800 divide os mecanismos de segurança em dois grupos
- Os mecanismos de segurança específicos (Utilizados em uma camada ou serviço de segurança específicos)
  - Cifragem (Encipherment)
  - Assinatura Digital (Digital Signature)
  - Controle de Acesso (Access Control)
  - Integridade de Dados (Data Integrity)
  - Permuta de Credenciais (Authentication Exchange)
  - Inserção de Bits (Traffic Padding)
  - Controle de Rotas (Routing Control)
  - Terceiros Confiáveis (Notarization)
- Mecanismos de Segurança Genéricos (Não estão associados a uma camada de específica ou serviço de segurança)
  - Funcionalidade Confiável (Trusted Functionality)
  - Rótulos de Segurança (Security Label)
  - Detecção de Eventos (Event Detection)
  - Log de Segurança (Security Audit Trail)
  - Recuperação da Segurança (Security Recovery)

Introdução – Mecanismos de Segurança Específicos

- Cifragem (Encipherment)
  - Uso de algoritmos matemáticos a fim de transformar os dados e impedir o seu reconhecimento. Recuperar estes dados através de 0 ou mais chaves
- Assinatura Digital (Digital Signature)
  - Dados que são adicionados e criptografados que permitem ao destinatário provar a origem e a integridade dos mesmos
- Controle de Acesso (Access Control)
- Integridade de Dados (Data Integrity)
- Permuta de Credenciais (Authentication Exchange)
  - Mecanismo que garante a identidade de uma entidade pela troca de informações
- Inserção de Bits (Traffic Padding)
  - Inserção de bits entre mensagens a fim de frustar a análise de tráfego
- Controle de Rotas (Routing Control)
  - Escolha e alteração de rotas em caso de suspeita de quebra da segurança
- Terceiros Confiáveis (Notarization)
  - Uso de terceiros confiáveis para garantir certas propriedades na troca de dados

Introdução - Mecanismos de Segurança Genéricos

- Funcionalidade Confiável (Trusted Functionality)
  - Funcionalidade que é percebida como confiável em relação a alguma política de segurança
- Rótulos de Segurança (Security Label)
  - Rótulos que são adicionados à mensagem indicando os atributos de segurança de um recurso
- Detecção de Eventos (Event Detection)
  - Detecção de eventos relacionados à segurança
- Log de Segurança (Security Audit Trail)
  - Dados que são obtidos e que podem facilitar uma auditoria da segurança, que consiste em examinar os registros do sistema e suas atividades
- Recuperação da Segurança (Security Recovery)
  - Mecanismos a fim de restabelecer a segurança de um sistema

Introdução
Mecanismos x Serviços

Serviço de Segurança	Mecanismos de Segurança							
	Cifragem	Assinatura Digital	Controle Acesso	Integridade de Dados	Permuta de Credenciais	Inserção de Bits	Controle de Rotas	Terceiros Confiáveis
Autentição de uma Entidade	S	S			S			
Autenticação da Origem dos Dados	S	S						
Controle de Acesso			S					
Confidencialidade	S						S	
Confidencialidade do tráfego	S					S	S	
Integridade de dados	S	S		S				
Não-Repúdio		S		S				S
Disponibilidade				S	S			