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

- Revisão conceitos de segurança da informação
- Os desafios da segurança de computadores
- A arquitetura de segurança OSI
- Ataques à segurança

CONCEITOS

Informação:

RFC 4949 define informação como “fatos e ideias que podem ser representadas (codificadas) em vários formatos de dados”

CONCEITOS

- **Segurança de computadores:** a 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.

CONFIDENCIALIDADE

- **Confidencialidade de dados:** assegura que informações privadas e confidenciais não estejam disponíveis nem sejam reveladas para indivíduos não autorizados.
- **Privacidade:** assegura que os indivíduos controlem ou influenciem quais informações relacionadas a eles podem ser obtidas e armazenadas, da mesma forma que como, por quem e para quem essas informações são passíveis de ser reveladas.

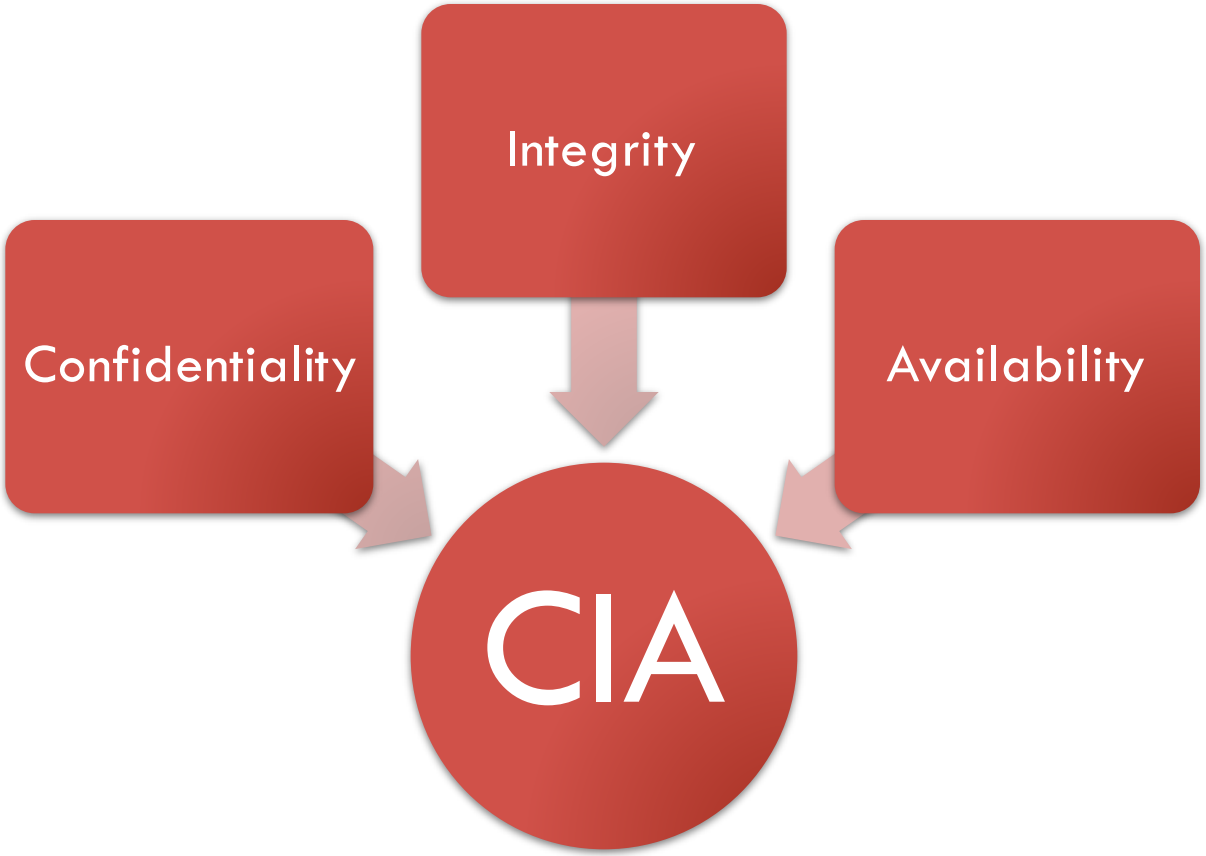
INTEGRIDADE

- **Integridade de dados:** assegura que as informações e os programas sejam modificados somente de uma maneira especificada e autorizada.
- **Integridade do sistema:** assegura que um sistema execute as suas funcionalidades de forma ilesa, livre de manipulações deliberadas ou inadvertidas do sistema.

DISPONIBILIDADE

- **Disponibilidade:** assegura que os sistemas operem prontamente e seus serviços não fiquem indisponíveis para usuários autorizados.

CONCEITOS



CONCEITOS

Conceitos adicionais são necessários para apresentar um quadro completo.

Autenticidade: a propriedade de ser genuíno e capaz de ser verificado e confiável.

OS DESAFIOS DA SEGURANÇA DE COMPUTADORES

A segurança de computadores e redes é tão fascinante quanto complexa.

DESAFIO 1

Segurança não é tão simples quanto parece à primeira vista para o iniciante.

Os requisitos aparentam ser claros e diretos;

No entanto, os mecanismos usados para satisfazê-los talvez sejam bastante complexos e seu entendimento envolva razões bastante sutis.

DESAFIO 2

No desenvolvimento de um mecanismo ou algoritmo específico de segurança, deve-se sempre considerar potenciais ataques a essas funcionalidades.

DESAFIO 3

Por conta do ponto 2, os procedimentos usados para fornecer os serviços de segurança são muitas vezes nem um pouco intuitivos.

Normalmente, um mecanismo de segurança é complexo, e não fica óbvio na definição de seus requisitos que essas medidas são necessárias.

Só faz sentido elaborar mecanismos de segurança quando os vários aspectos de ameaças são considerados.

DESAFIO 4

Tendo projetado vários mecanismos de segurança, é necessário decidir onde eles devem ser usados.

Essa é uma verdade tanto em termos da localização física quanto do sentido lógico.

DESAFIO 5

Mecanismos de segurança normalmente envolvem mais do que um algoritmo ou protocolo em particular.

Eles também requerem que os participantes possuam algumas informações secretas (como chave de encriptação), o que levanta outras questões relacionadas à criação, distribuição e proteção delas.

DESAFIO 6

Segurança de computadores e redes é, essencialmente, uma batalha de inteligência entre um criminoso que tenta encontrar buracos e o projetista ou administrador que tenta fechá-los.

DESAFIO 7

Existe uma tendência natural de uma parte dos usuários e gerentes de sistemas a perceber poucos benefícios com os investimentos em segurança, até que uma falha nela ocorra.

DESAFIO 8

A segurança requer um monitoramento regular, ou até mesmo constante, e isso é algo difícil com os curtos prazos e nos ambientes sobrecarregados dos dias de hoje.

DESAFIO 9

Segurança ainda é muito frequentemente um adendo a ser incorporado no sistema após o projeto estar completo, em vez de ser parte do processo de sua criação.

DESAFIO 10

Muitos usuários, e até mesmo administradores de segurança, veem uma segurança forte como um impedimento à eficiência e à operação amigável de um sistema de informação ou do uso da informação.

A ARQUITETURA DE SEGURANÇA OSI

Para avaliar efetivamente as necessidades de segurança de uma organização e escolher diversos produtos e políticas de segurança, o gerente responsável precisa de algum meio sistemático de definir os requisitos para a segurança e caracterizar as técnicas para satisfazê-los.

A ARQUITETURA DE SEGURANÇA OSI

A recomendação X.800, Security Architecture for OSI, define tal técnica sistemática.

A ARQUITETURA DE SEGURANÇA OSI

A arquitetura de segurança OSI oferece uma visão geral útil, abstrata, de muitos dos conceitos.

Ela focaliza ataques, mecanismos e serviços de segurança.

A ARQUITETURA DE SEGURANÇA OSI

Ataque à segurança: qualquer ação que comprometa a segurança da informação pertencida a uma organização.

A ARQUITETURA DE SEGURANÇA OSI

Mecanismo de segurança: um processo que é projetado para detectar, impedir ou recuperar-se de um ataque à segurança.

A ARQUITETURA DE SEGURANÇA OSI

Serviço de segurança: um serviço de processamento ou comunicação que aumenta a segurança dos sistemas de processamento de dados e das transferências de informação de uma organização.

(RFC 4949) - AMEAÇA

Uma chance de violação da segurança que existe quando há uma circunstância, capacidade, ação ou evento que poderia quebrar a segurança e causar danos.

(RFC 4949) - ATAQUE

Um ataque à segurança do sistema, derivado de uma ameaça inteligente;

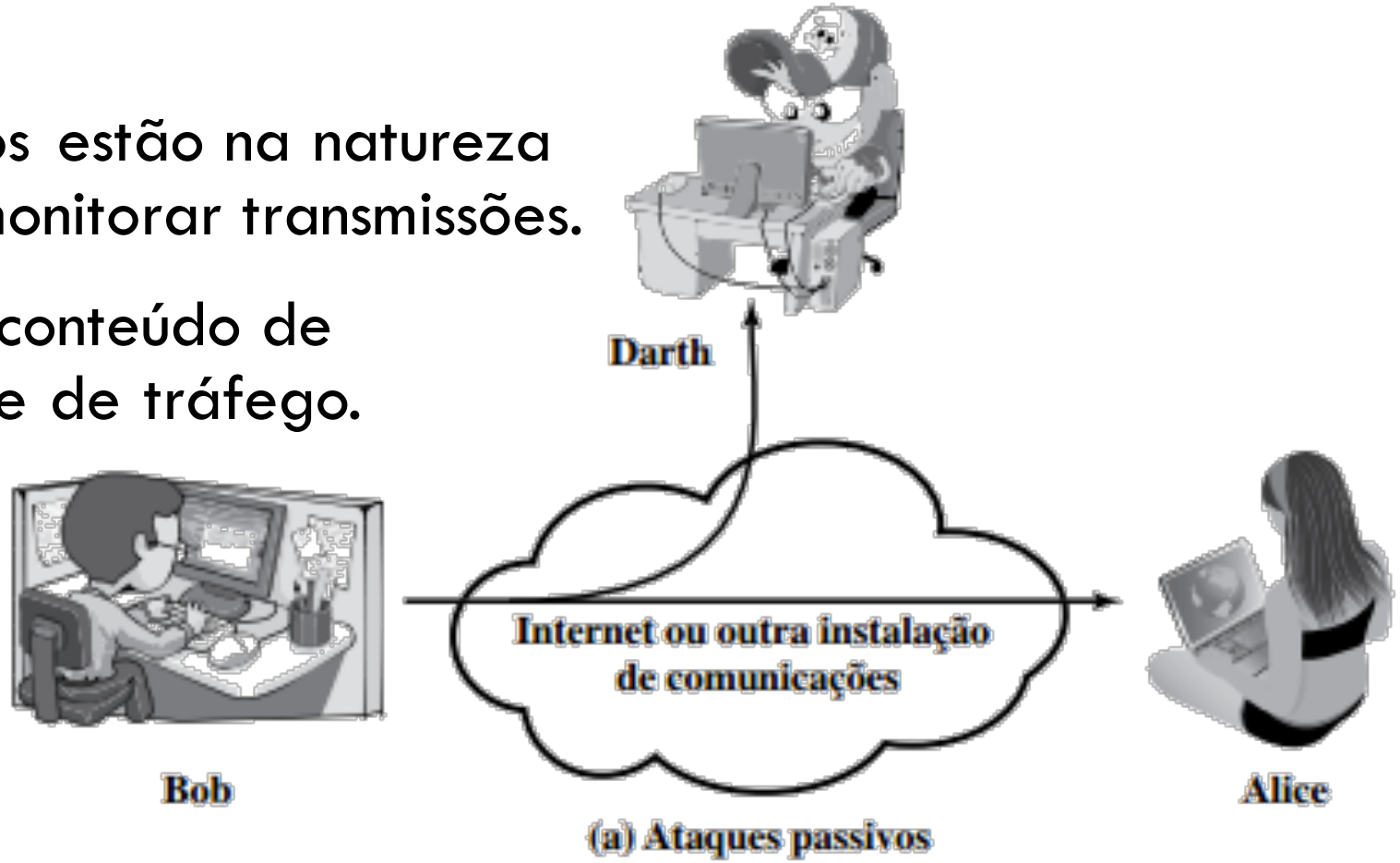
ATAQUES À SEGURANÇA

Uma maneira útil de classificar os ataques à segurança, usada tanto na X.800 quanto na RFC 4949, é em termos de **ataques passivos** e **ataques ativos.**

ATAQUES PASSIVOS

Os ataques passivos estão na natureza de bisbilhotar ou monitorar transmissões.

Ex: Vazamento de conteúdo de mensagem e análise de tráfego.



(a) Ataques passivos

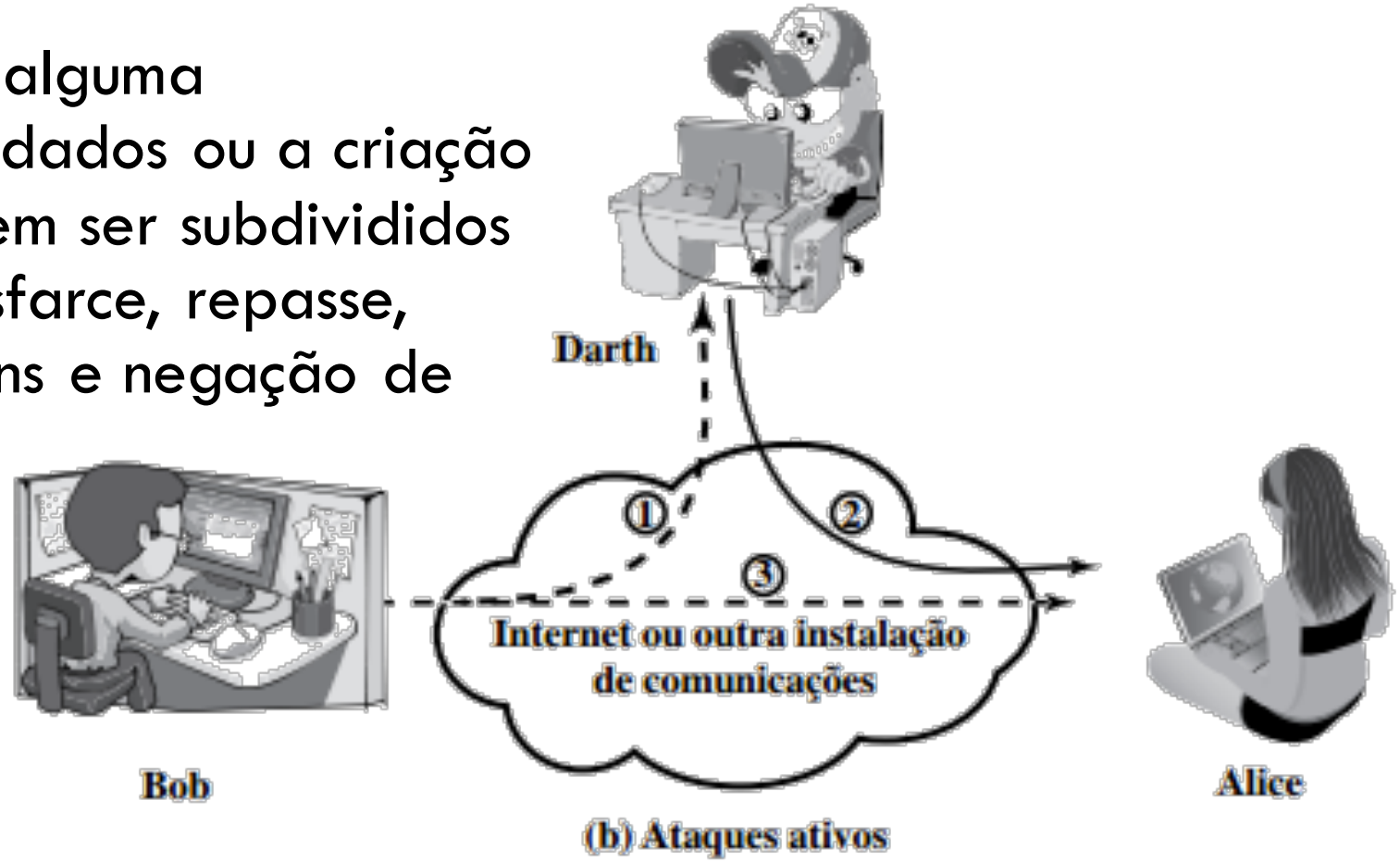
ATAQUES PASSIVOS

O **vazamento de conteúdo de mensagem** é facilmente compreendido.

Análise de tráfego, é mais sutil. Suponha que tivéssemos uma maneira de disfarçar o conteúdo das mensagens ou outro tráfego de informações, de modo que os oponentes, mesmo que capturassem a mensagem, não pudessem extrair as informações dela.

ATAQUES ATIVOS

Ataques ativos envolvem alguma modificação do fluxo de dados ou a criação de um fluxo falso, e podem ser subdivididos em quatro categorias: disfarce, repasse, modificação de mensagens e negação de serviço.



(b) Ataques ativos

ATAQUES ATIVOS

Um **disfarce** ocorre quando uma entidade finge ser outra diferente (caminho 3 ativo).

Repasse envolve a captura passiva de uma unidade de dados e sua subsequente retransmissão para produzir um efeito não autorizado (caminhos 1, 2 e 3 ativos).

ATAQUES ATIVOS

Modificação de mensagens simplesmente significa que alguma parte de uma mensagem legítima é alterada, ou que as mensagens são adiadas ou reordenadas, para produzir um efeito não autorizado (caminhos 1 e 2 ativos).

A negação de serviço impede ou inibe o uso ou gerenciamento normal das instalações de comunicação (caminho 3 ativo).

EXERCÍCIOS

1. Qual é a diferença entre ameaças à segurança passivas e ativas?
2. Liste e defina resumidamente as categorias de ataques passivos e ativos à segurança.
3. Considere um caixa eletrônico, no qual os usuários fornecem um cartão e um número de identificação pessoal (senha). Dê exemplos de requisitos de confidencialidade, integridade e disponibilidade associados com esse sistema.
4. Aplique o problema anterior para um sistema de comutação de telefonia que faz o direcionamento de chamadas baseado no número do telefone requisitado por quem iniciou a ligação.