EACH

Escola de Artes, Ciências e Humanidades
da Universidade de São Paulo

ACH2026
Redes de Computadores

Introdução a
Segurança da Informação

Profa. Dra. Cíntia B. Margi

Dezembro/2009

“A arte da guerra nos ensina a contar não com a probabilidade de o inimigo não chegar, mas com nossa própria prontidão para recebê-lo; não com a chance de não ser atacado, mas com o fato de tornar nossa posição inatacável.”

***A Arte da Guerra,* Sun Tzu**

Introdução

- Requisitos de segurança da informação mudaram nas últimas décadas...
- Tradicionalmente obtida através de meios físicos e administrativos:
  - armários e cadeados para armazenar documentos;
  - processo de contratação; etc.
- Uso de computadores requer ferramentas automatizadas para proteger arquivos e outras informações armazenadas.
- Uso de redes e enlaces de comunicação requer medidas para proteger dados durante a transmissão.

Segurança

- “Prevenir que atacantes alcancem seus objetivos através do acesso não autorizado ou uso não autorizado dos computadores e suas redes” (Howard).

Definições

- **Segurança de Computador –** nome genérico para conjunto de ferramentas projetadas para proteger dados e impedir *hackers*.
- **Segurança de Rede** – medidas para proteger os dados durante a transmissão.
- **Segurança da Internet (ou de Inter-rede)** - medidas para proteger os dados durante a transmissão através de uma coleção de redes interconectadas.

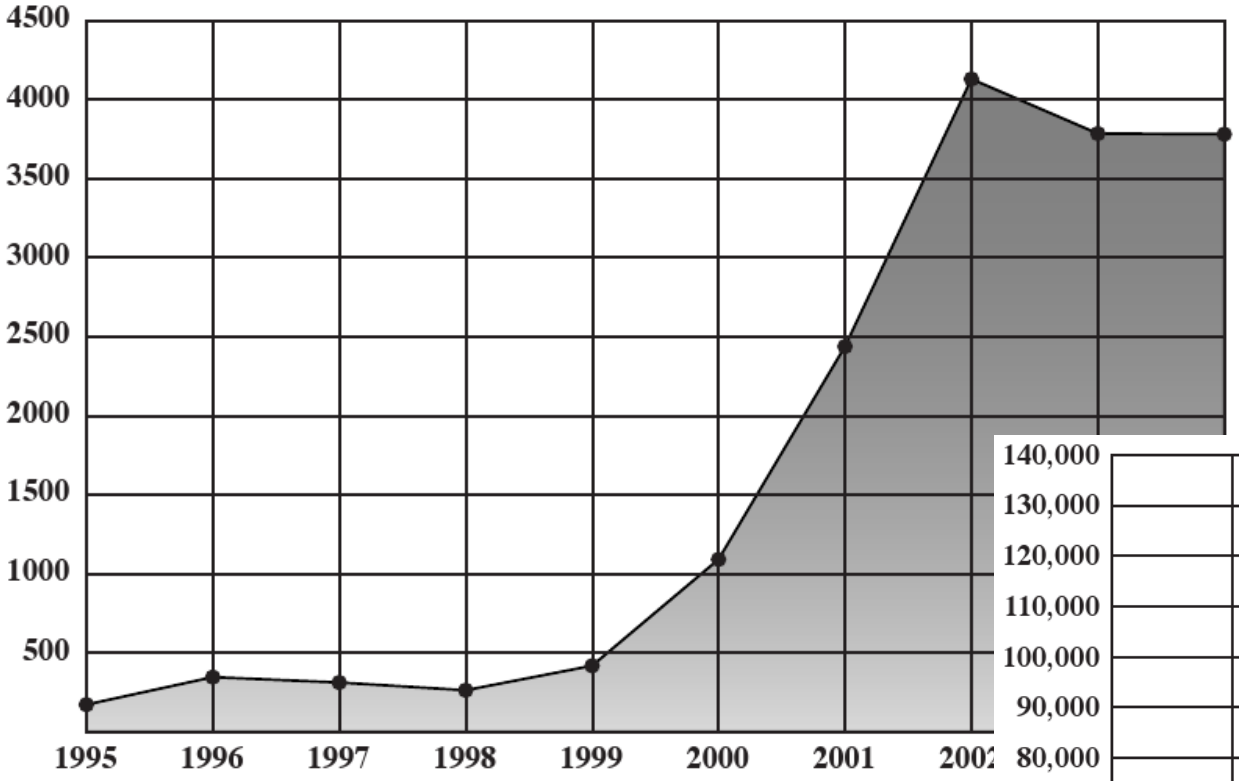
Objetivos

- **Segurança de Internet**:
  - consiste em medidas para desencorajar, impedir, detectar e corrigir violações de segurança que envolvam a transmissão de informações.

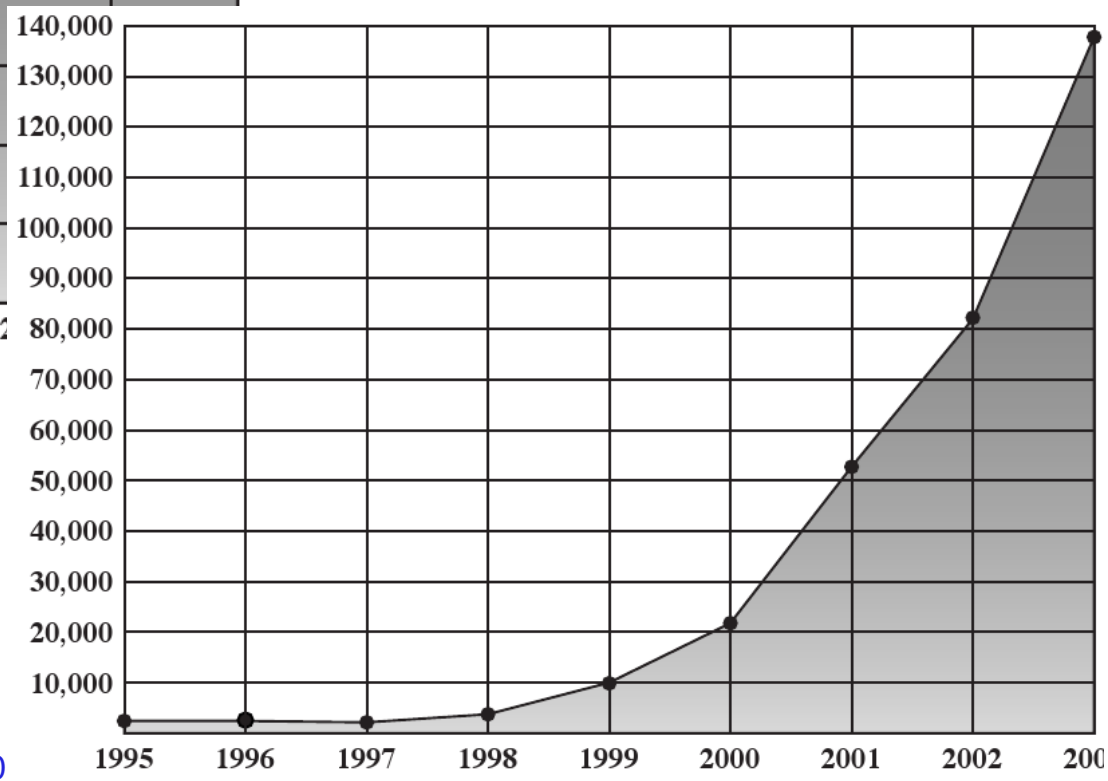
EACH

Escola de Artes, Ciências e Humanidades
da Universidade de São Paulo

Estatísticas do CERT



(a) Vulnerabilities reported

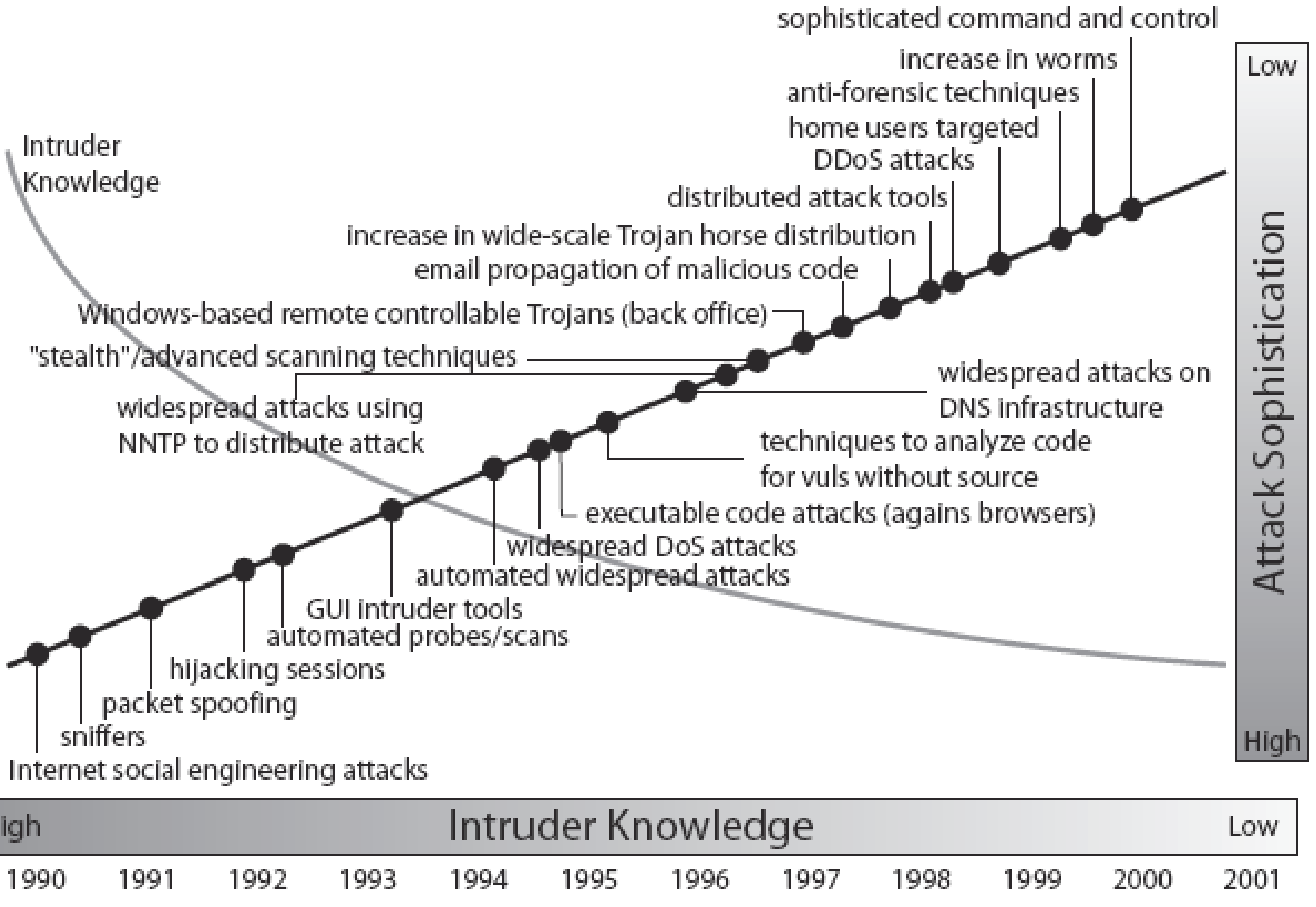


(b) Incidents reported

EACH

Escola de Artes, Ciências e Humanidades
da Universidade de São Paulo

Tendências de Segurança



Source: CERT

Arquitetura de Segurança OSI

- Recomendação ITU-T X.800 - “Security Architecture for OSI”:
  - define uma maneira sistemática para definir e prover requisitos de segurança, e caracterizar técnicas para satisfazer esses requisitos;
  - provê visão geral útil e abstrata dos conceitos que serão estudados.

3 Aspectos de Segurança

- **Ataque à segurança**
- **Mecanismo de Segurança**
- **Serviço de Segurança**

Ataque à Segurança

- Qualquer ação que comprometa a segurança da informação pertencente a uma organização.
- Segurança da Informação tem como objetivo impedir ataques, ou se isso falhar, detectá-los.
- Ataque e ameaça são comumente usados como sinônimos, mas...

Ameaças e Ataques

Table 1.1 Threats and Attacks (RFC 2828)

Threat

A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit a vulnerability.

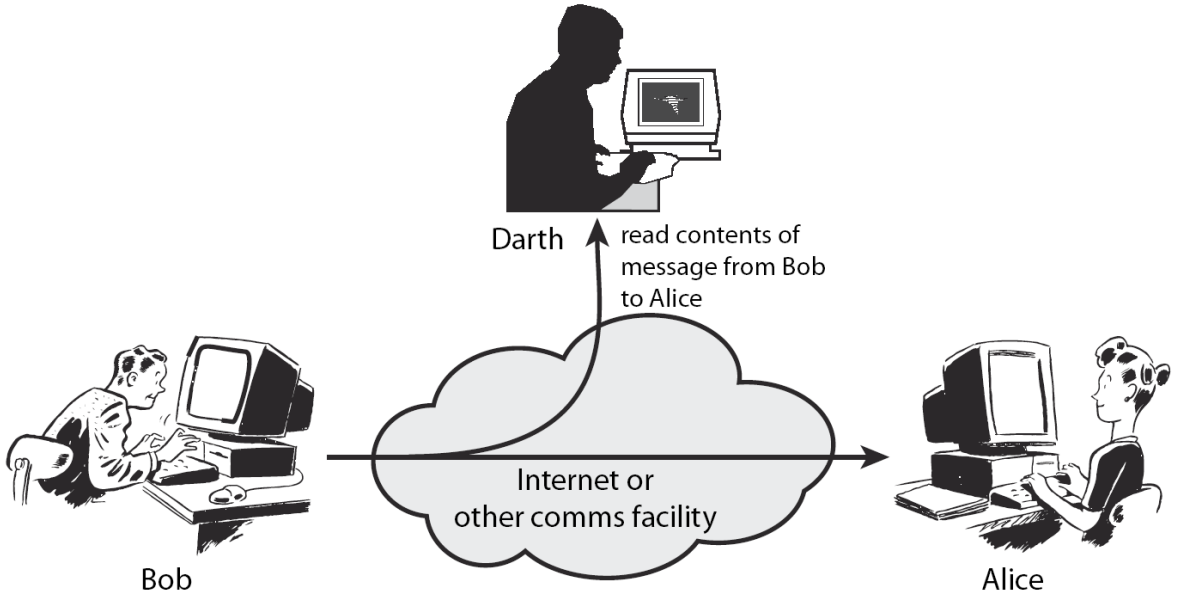
Attack

An assault on system security that derives from an intelligent threat; that is, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.

Ataque à Segurança

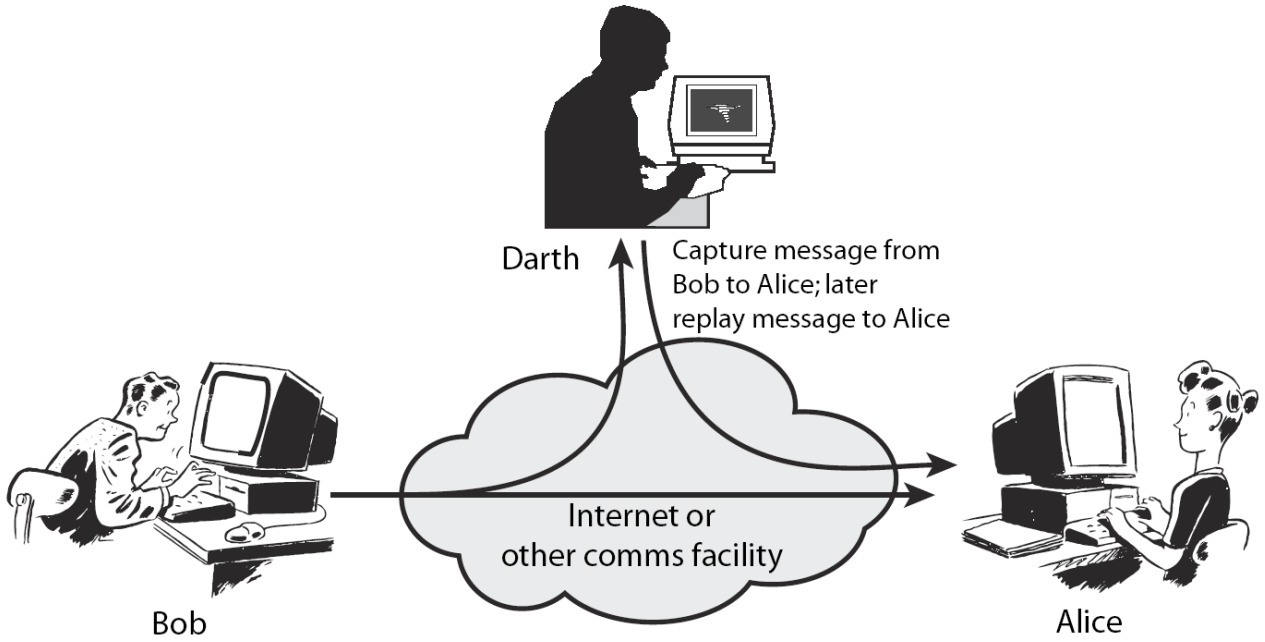
- Classificação de ataques (tanto X.800 como RFC2828):
  - passivo;
  - ativo.
- Qualquer um destes tipos de ataque irá alterar o fluxo normal da informação.

Ataques Passivos



- São aqueles onde a mensagem é apenas observada ou copiada.
- Um exemplo deste tipo de ataque é a interceptação.

Ataques Ativos



- São aqueles onde a mensagem sofre alterações ou é desviada.
- Exemplos: disfarce, repetição, modificação e negação de serviço.

Serviços de Segurança

- **X.800**: serviço fornecido por uma camada de protocolo de comunicação de sistemas abertos, que garante a segurança adequada dos sistemas ou das transferências de dados
- **RFC2828**: serviço de processamento ou comunicação que é fornecido por um sistema para prover 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.

Serviços de Segurança (X.800)

- **Autenticação**
- **Controle de Acesso**
- **Confidencialidade dos dados**
- **Integridade dos dados**
- **Irretratabilidade (Non-Repudiation)**

- **Disponibilidade** – de acordo com a recomendação, é uma propriedade associada aos serviços.

Serviços de Segurança

Autenticidade

- Requer que a origem ou o originador de uma mensagem seja corretamente identificado.
- A verificação de autenticidade é necessária após todo processo de identificação, seja de um usuário para um sistema, de um sistema para o usuário ou de um sistema para outro sistema.

Serviços de Segurança

Controle de Acesso

- Consiste na capacidade de se permitir ou negar acesso aos serviços e recursos oferecidos pelo sistema.
- Acessos desconhecidos ou feitos por pessoas não autorizadas podem significar a necessidade de uma verificação de todos os recursos envolvidos em busca de possíveis estragos que possam ter sido causados ao sistema, mesmo que nada tenha ocorrido.

Serviços de Segurança

Confidencialidade

- Consiste em proteger a informação contra leitura ou cópia por alguém que não tenha sido explicitamente autorizado pelo proprietário daquela informação.
- A informação deve ser protegida qualquer que seja a mídia que a contenha: impressa, digital, etc...

Serviços de Segurança

Integridade

- Consiste em proteger a informação (ou programas do sistema) contra modificação sem a permissão explicita do proprietário daquela informação.
- A modificação inclui ações como escrita, alteração de conteúdo, alteração de *status*, remoção, criação e o atraso de informações transmitidas.

Serviços de Segurança

Irretratabilidade

- Requer que o originador de uma mensagem (ou ação) não possa negar futuramente o envio da mensagem (ou a realização da ação).
- Do mesmo modo, o receptor de uma mensagem (ou ação) não deve ser capaz de negar o recebimento da mensagem (ou ação).

Serviços de Segurança

Disponibilidade

- Consiste na proteção dos serviços prestados pelo sistema de forma que eles não sejam degradados ou tornem-se indisponíveis sem autorização.
- Um sistema indisponível quando um usuário autorizado necessita dele pode resultar em perdas tão graves quanto as causadas pela remoção das informações daquele sistema.

Mecanismos de Segurança

- Um processo (ou um dispositivo incorporando tal processo) que é projetado para detectar, impedir ou permitir a recuperação de um ataque a segurança.

Tabela 1.3 Mecanismos de segurança (X.800)

MECANISMOS DE SEGURANÇA ESPECÍFICOS

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

Cifragem

O uso de algoritmos matemáticos para transformar os dados em um formato que não seja prontamente decifrável. A transformação e subseqüente recuperação dos dados depende de um algoritmo e zero ou mais chaves de criptografia.

Assinatura digital

Dados anexados a (ou uma transformação criptográfica de) uma unidade de dados que permite que um destinatário da unidade de dados comprove a origem e a integridade da unidade de dados e proteja-se contra falsificação (por exemplo, pelo destinatário).

Controle de acesso

Uma série de mecanismos que impõem direitos de acesso aos recursos.

Integridade de dados

Uma série de mecanismos utilizados para garantir a integridade de uma unidade de dados ou fluxo de unidades de dados.

Troca de informações de autenticação

Um mecanismo com o objetivo de garantir a identificação de uma entidade por meio da 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 permite mudanças de roteamento, especialmente quando existe suspeita de uma brecha de segurança.

Certificação

O uso de uma terceira entidade confiável para garantir certas propriedades de uma troca de dados.

MECANISMOS DE SEGURANÇA PERVASIVOS

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

Funcionalidade confiável

Aquela que é considerada como sendo correta em relação a alguns critérios (por exemplo, conforme estabelecido por uma política de segurança).

Rótulo de segurança

A marcação vinculada a um recurso (que pode ser uma unidade de dados) que nomeia ou designa os atributos de segurança desse recurso.

Detecção de evento

Detecção de eventos relevantes à segurança.

Registros de auditoria de segurança

Dados coletados e potencialmente utilizados para facilitar uma auditoria de segurança, que é uma revisão e exame independentes dos registros e atividades do sistema.

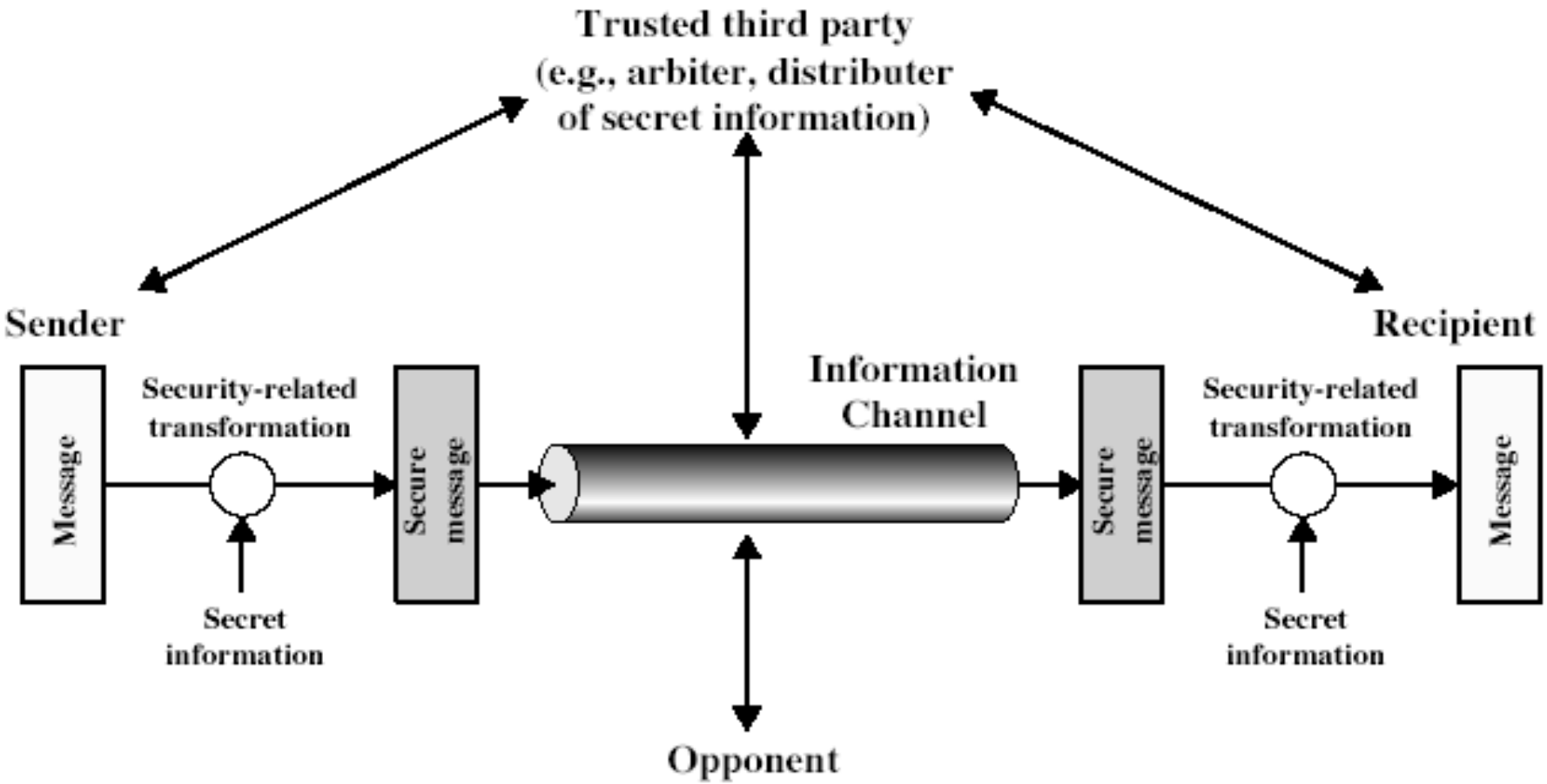
Recuperação de segurança

Lida com solicitações de mecanismos, como funções de tratamento e gerenciamento de eventos, e toma medidas de recuperação.

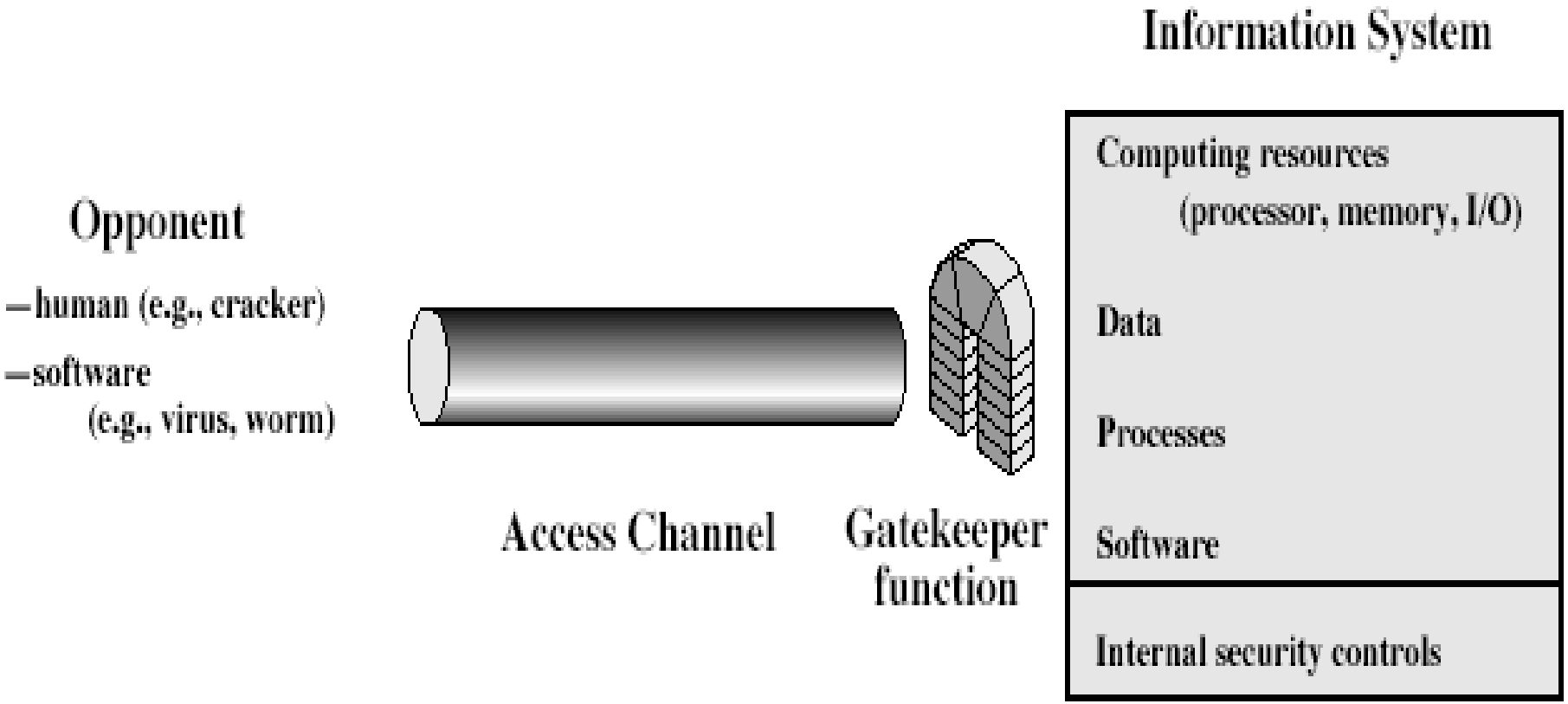
Table 1.4 Relationship Between Security Services and Mechanisms

Service	Mechanism							
	Enciph-erment	Digital signature	Access control	Data integrity	Authenti-cation exchange	Traffic padding	Routing control	Notari-zation
Peer entity authentication	Y	Y			Y			
Data origin authentication	Y	Y						
Access control			Y					
Confidentiality	Y						Y	
Traffic flow confidentiality	Y					Y	Y	
Data integrity	Y	Y		Y				
Non-repudiation		Y		Y				Y
Availability				Y	Y			

Modelo para Segurança da Rede



Modelo de Segurança de Acesso a Rede



CERT.br

- http://www.cert.br/
- Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil.
- Mantido pelo NIC.br.
- É responsável por receber, analisar e responder a incidentes de segurança envolvendo redes conectadas à Internet no Brasil.

CERT.br (cont.)

- Disponibiliza estatísticas sobre incidentes no Brasil.
- Cartilha de Segurança para Internet: http://cartilha.cert.br/
- Projeto: HoneyPots Distribuídos.

Vídeos - Antispam.br

- 1. Navegar é preciso
  - O vídeo trata do funcionamento da Internet, com suas vantagens, riscos e necessidade de proteção, principalmente mecanismos como o firewall.
- 2. Os Invasores
  - Apresenta os tipos de códigos maliciosos e como eles podem entrar no computador do usuário, reforçando que a maioria dos códigos têm mais de um vetor de entrada e por isso mais de uma proteção é necessária.

Vídeos – Antispam.br (cont.)

- 3. Spam
  - Aborda os tipos de spam existentes, suas diferenças e malefícios, incluindo códigos maliciosos e fraudes.
- 4. A Defesa
  - O objetivo do vídeo é mostrar ao usuário como se proteger de ameaças e navegar com mais segurança na rede.

Bibliografia

- Livro-texto:
  - Capítulo 8 - Segurança em redes de computadores
- William Stallings; “Criptografia e Segurança de Redes – Princípios e Práticas”, Quarta edição. Pearson/Prentice Hall, São Paulo, 2007.
- Matt Bishop; "Introduction to Computer Security". Addison Wesley, 2005.

EACH

Escola de Artes, Ciências e Humanidades
da Universidade de São Paulo

Dúvidas?