Criptografia e Segurança em Rede Capítulo 1

De William Stallings

Apresentação por Lawrie Brown e Fábio Borges

Capítulo 1 – Introdução

A arte da guerra nos ensina a não confiar na probabilidade de o inimigo não chegar, mas na nossa própria capacidade para recebê-lo e não sobre a sua chance de não atacar, mas sim no fato de que fizemos a nossa posição inatacável.

—***The Art of War,*** **Sun Tzu**

Visão Geral

- as exigências da Segurnaça da Informação tem sido alteradas nos últimos tempos
- exigências tradicionalmente prestadas pela física e mecanismos administrativos
- a informática exige ferramentas automatizadas para proteger arquivos e outras informações armazenadas
- utilização de redes de comunicações altamente conectados requer medidas para proteger os dados durante a transmissão.

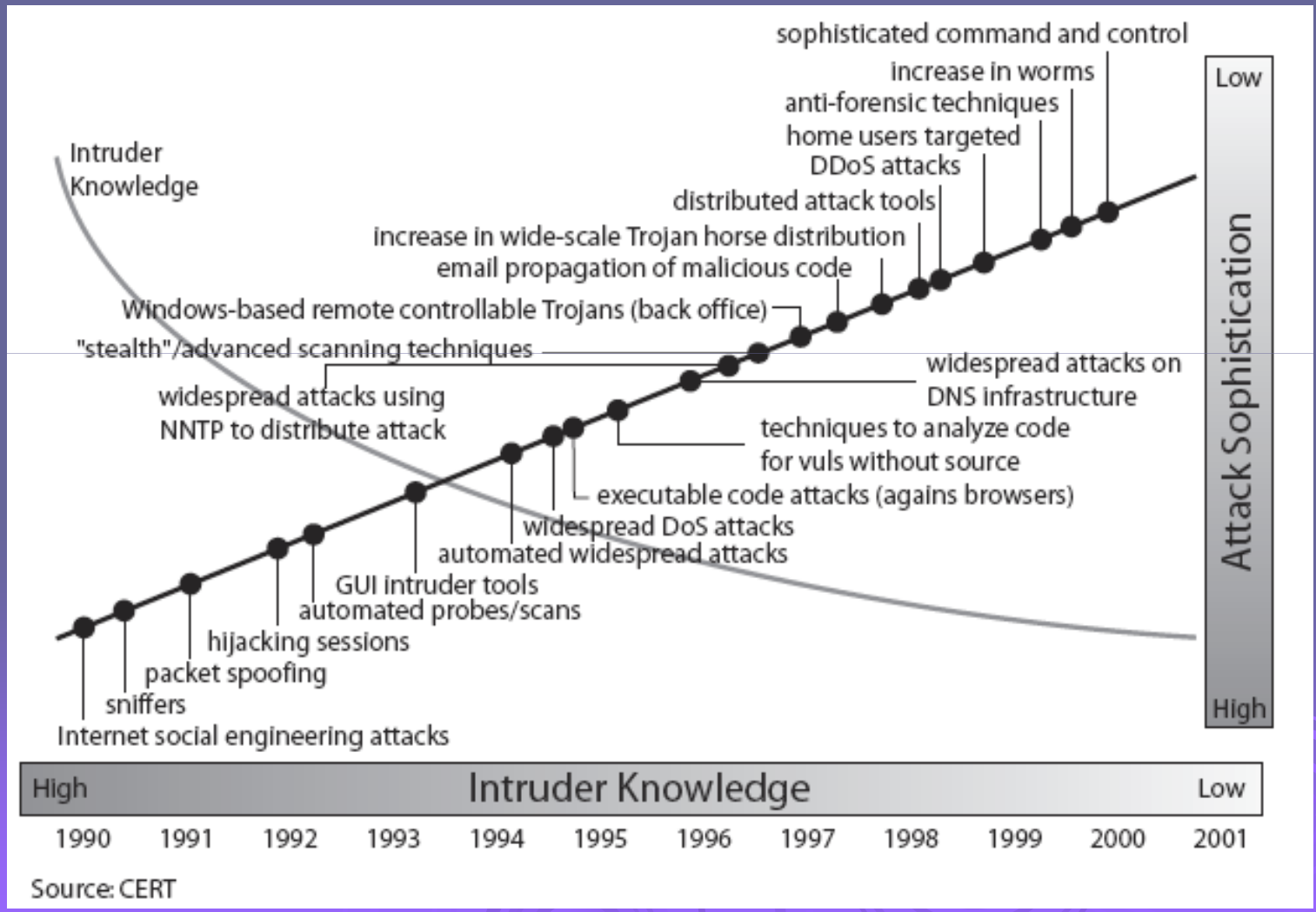
Definições

- **Segurança Computacional** - nome genérico para a recolha de instrumentos destinados a proteger os dados e para contra-atacar hackers
- **Segurança de rede** - medidas destinadas a proteger os dados durante a sua transmissão
- **Segurança da Internet** - as medidas para proteger os dados durante a sua transmissão por uma coleção de redes interconectadas

Objetivo do Curso

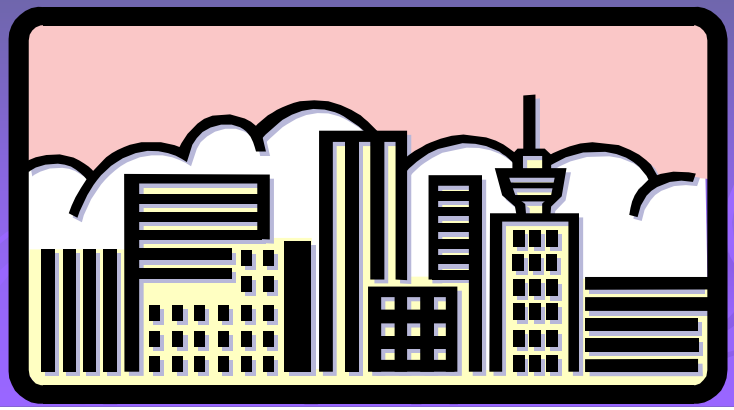
- nosso foco está na **Segurança da Internet**
- que consiste em medidas para dissuadir, prevenir, detectar e corrigir as violações de segurança que envolvem a transmissão e armazenamento de informações

Tendências da Segurança



Arquitetura de Segurança OSI

- ITU-T X.800 Arquitetura de Segurança OSI
- define uma forma sistemática para definir os requisitos de segurança
- fornecendo para nós um instrumento útil, se abstrato, resume os conceitos que vamos estudar



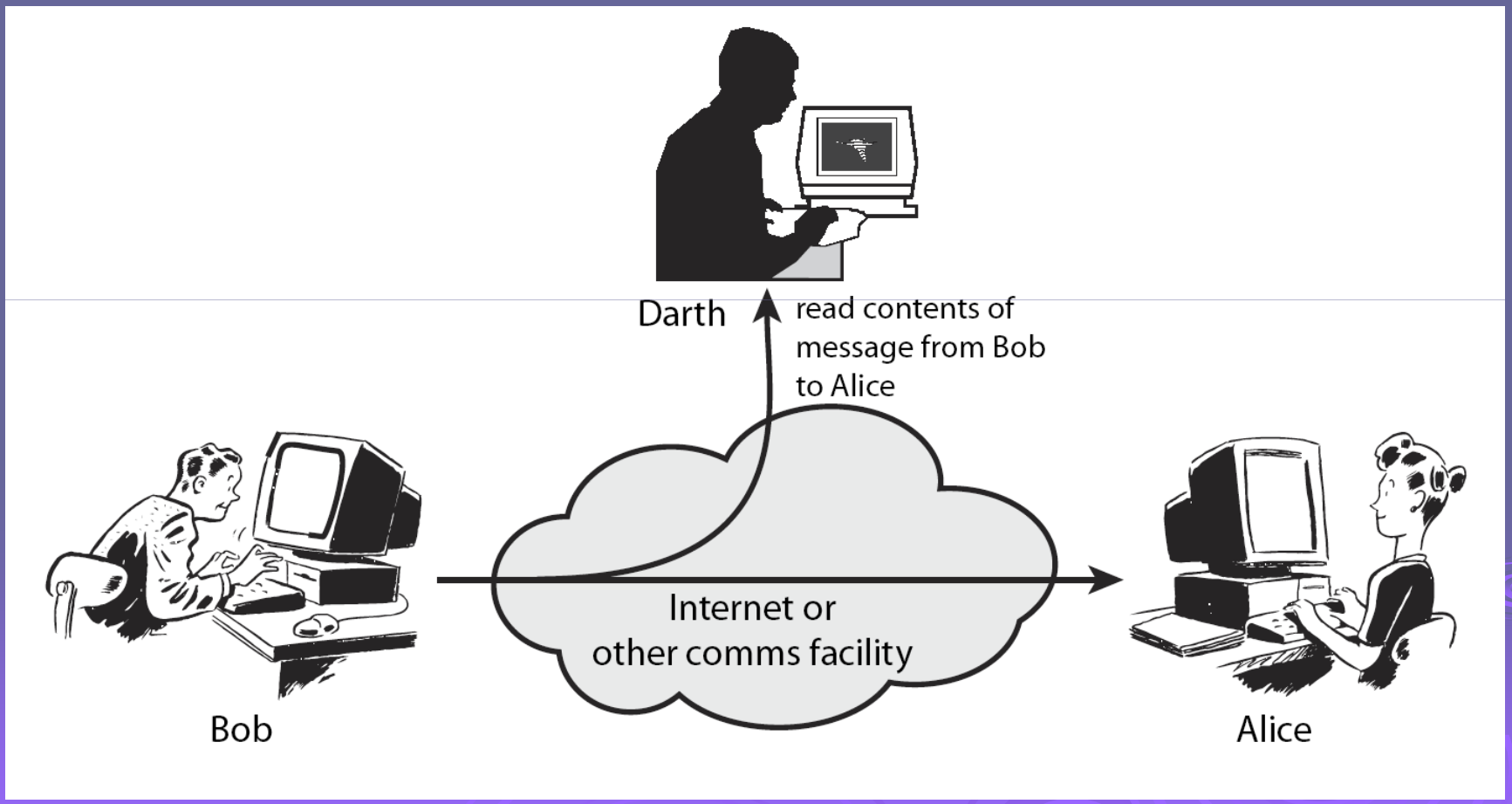
Aspectos de Segurança

- considerar 3 aspectos de segurança da informação:
  - ataque à segurança
  - mecanismo de segurança
  - serviço de segurança

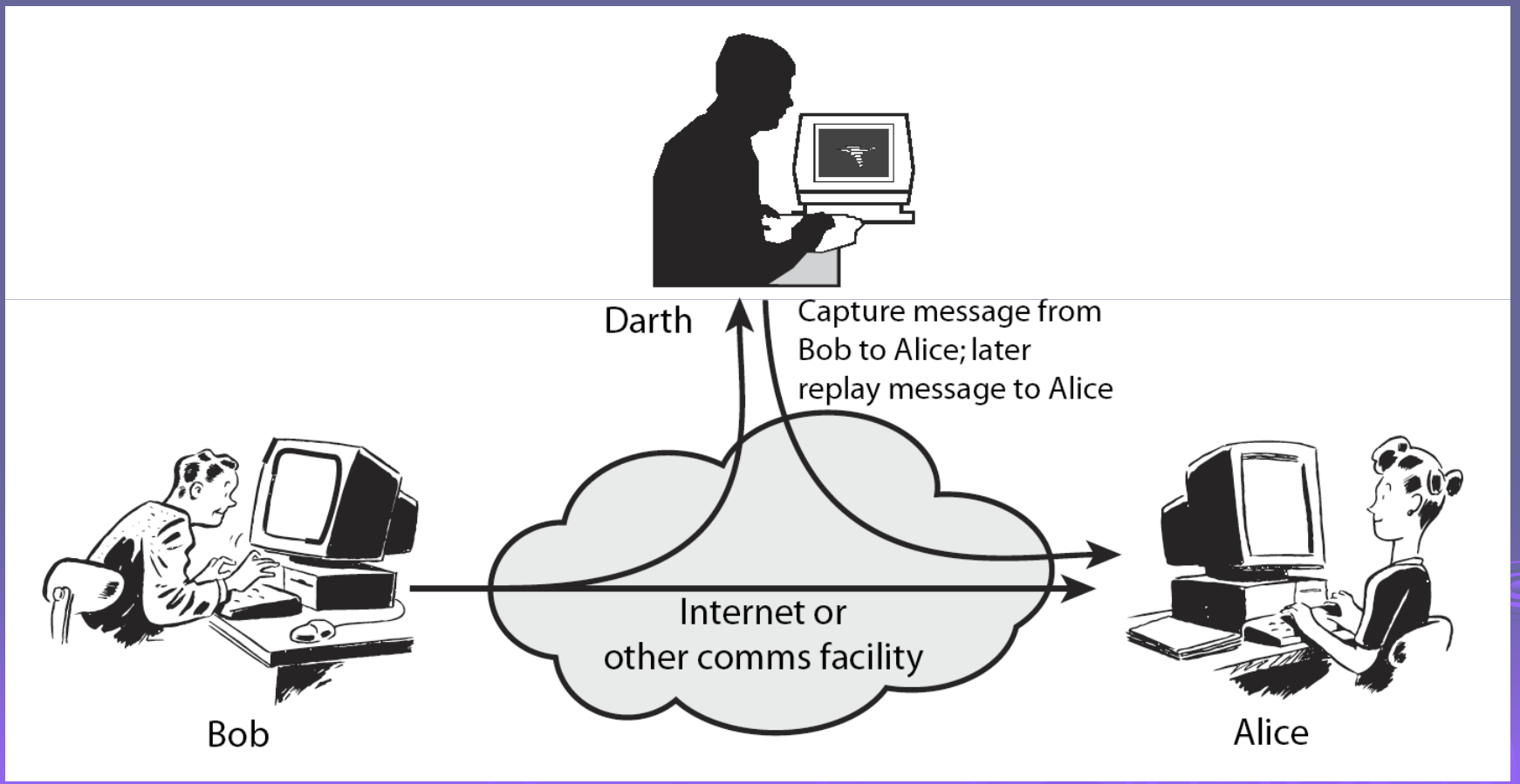
Ataque à Segurança

- qualquer ação que comprometa a segurança da informação detida por uma organização
- segurança da informação é versa sobre como evitar os ataques, ou na falta desta, a fim de detectar os ataques aos sistemas de informação
- frequentemente ameaça & ataque são utilizados para significar mesma coisa
- existe uma ampla gama de ataques
- podem centrar-se em tipos genéricos de
  - Ataques passivos
  - Ataques ativos

Ataques Passivos



Ataques Ativos



Serviços de Segurança

- reforçar a segurança dos sistemas de processamento de dados e informações das transferências de uma organização
- destinados a segurança contra ataques
- utilizando um ou mais mecanismos de segurança
- muitas vezes repetições de funções normalmente associadas a documentos físicos
  - que, por exemplo, tem assinaturas, datas, proteção contra a divulgação, alteração ou destruição; autenticação ou testemunha; ser armazenados ou licenciados

Seviços de Segurança

- X.800:

  "um serviço prestado por uma camada de protocolo de comunicação de sistemas abertos, que garante a segurança adequada dos sistemas ou de transferências de dados"

- RFC 2828:

  "Um serviço de processamento ou comunicação prestado por um sistema para dar um tipo específico de proteção aos recursos do sistema"

Serviços de Segurança(X.800)

- **Autenticação** - garantia de que a entidade está comunicando com a entidade alegada
- **Controle de acesso** - a prevenção do uso não autorizado de um recurso
- **Confidencialidade dos dados** - proteção de dados de divulgação não autorizada
- **Integridade do dados** - garantia de que os dados recebidos como foi enviado por uma entidade autorizada
- **Não repúdio** - a proteção contra a negação de uma das partes em uma comunicação

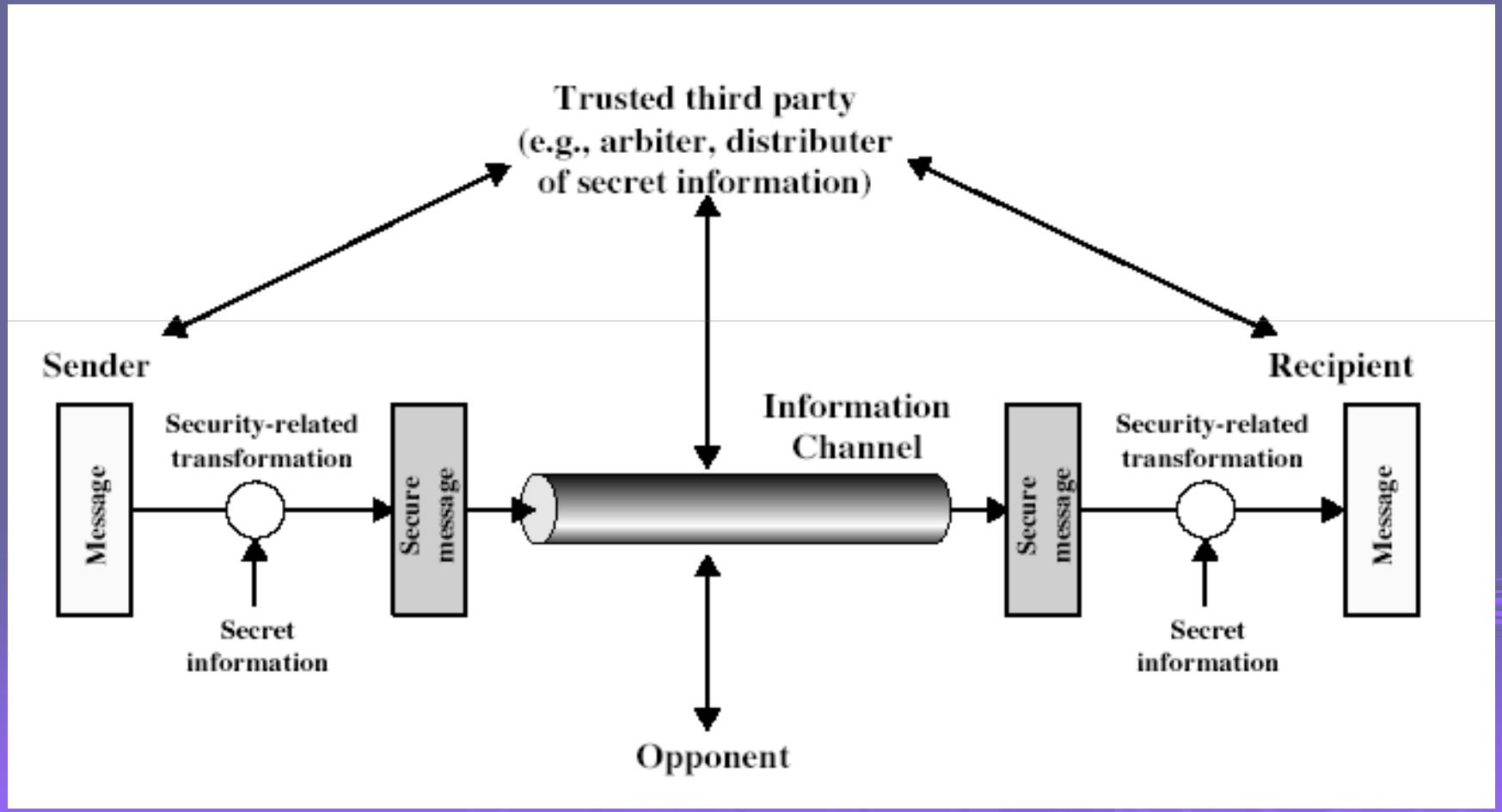
Mecanismos de Segurança

- recurso destinado a detectar, prevenir ou recuperar de um ataque à segurança
- nenhum mecanismo irá suportar todos os serviços requeridos
- no entanto, um determinado elemento subjacente a muitos dos mecanismos de segurança em uso:
  - técnicas criptográficas
- daí o nosso foco sobre este tema

Mecanismo de Segurnaça (X.800)

- mecanismos de segurança específicos:
  - encriptação, assinaturas digitais, controles de acesso, integridade dos dados, autenticação das partes, o tráfego coberto, controle de rota, testemunho
- mecanismos de segurança pervasivos:
  - funcionalidade confiável, etiquetas de segurança, detecção de evento, pistas de auditoria de segurança, recuperação de segurança

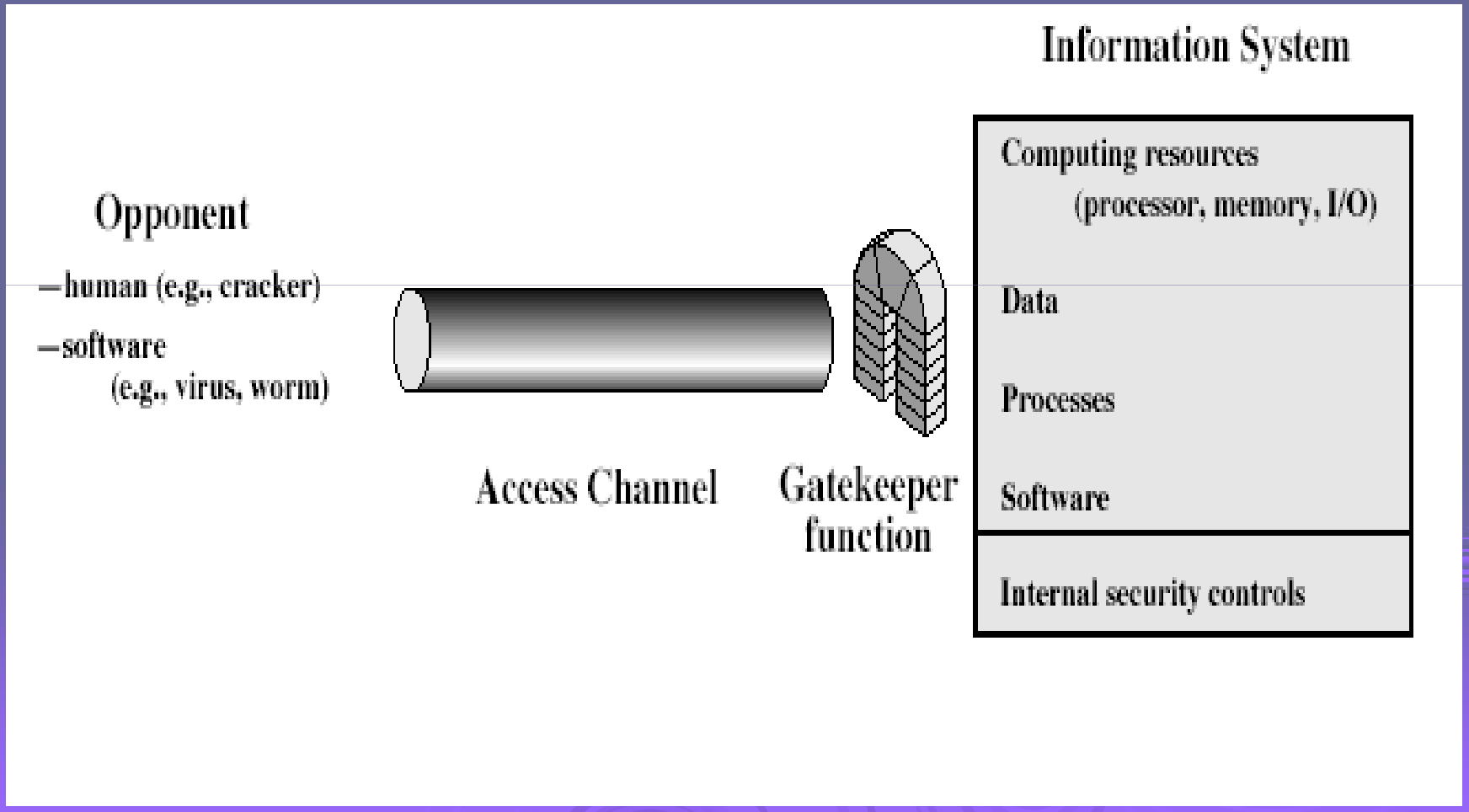
Modelo de Segurança de Redes



Modelo de Segurança de Redes

- utilizar este modelo exige-nos que:
  1. a concepção de um algoritmo apropriado para a transformação segurança
  2. gerar as informações secretas (chaves) utilizados pelo algoritmo
  3. desenvolver métodos para distribuir e compartilhar a informação secreta
  4. especificar um protocolo que permite aos usuários a utilizarem a transformação e informações secretas para um serviço de segurança

Modelo de Acesso à Rede de Segurança



Modelo de Acesso à Rede de Segurança

- utilizando este modelo exige-nos que:
  1. selecione uma função adequada para o gatekeeper identificar os utilizadores
  2. aplicar controles de segurança para garantir somente acesso de usuários autorizados a designados recursos ou informações
- sistemas computacionais confiáveis podem ser úteis para ajudar a implementar este modelo

Sumário

- ter considerado:
  - definições para:
    - computador, rede, segurança da internet
- Norma X.800
- ataques à segurança, serviços e mecanismos de segurança, modelos seguro (para acesso a rede)