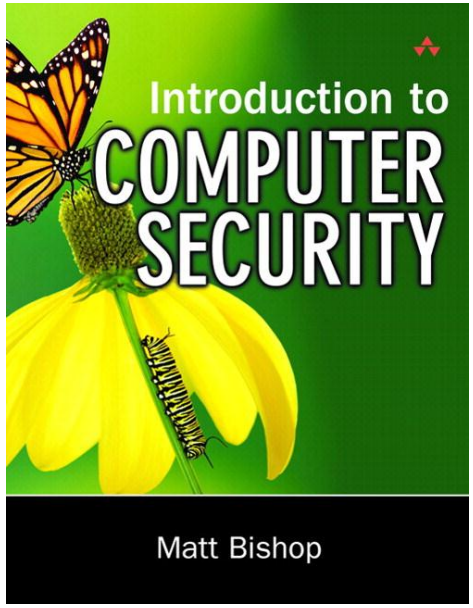
Segurança de sistemas informáticos

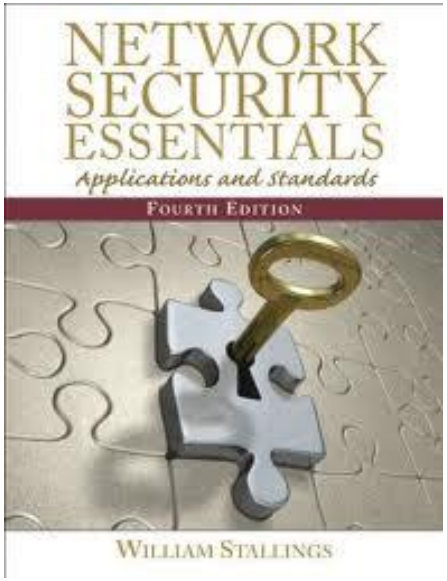
Bibliografia

- Título **Introduction to Computer Security**
- Autor **Matt Bishop**
- Edição 1
- Editora Addison-Wesley Professional
- ISBN **0321247442**
- Número de páginas 784 páginas



Bibliografia

- Titulo: Network Security Essentials: Applications and Standards (4th Edition)
- Author: William Stallings
- Publisher: Pearson Education;
- Language: English
- ISBN10: 0136108059
- ISBN13: 978-0136108054

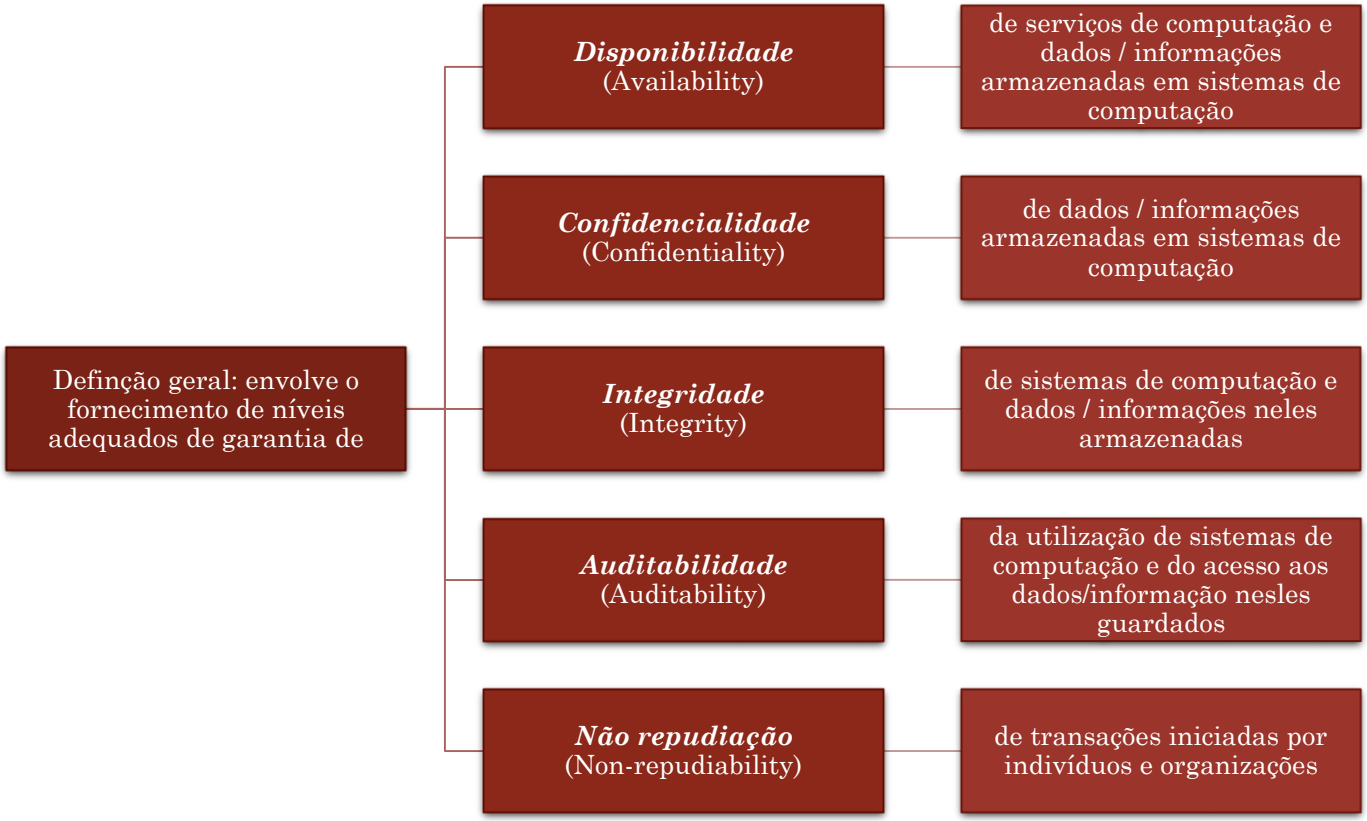


Introdução

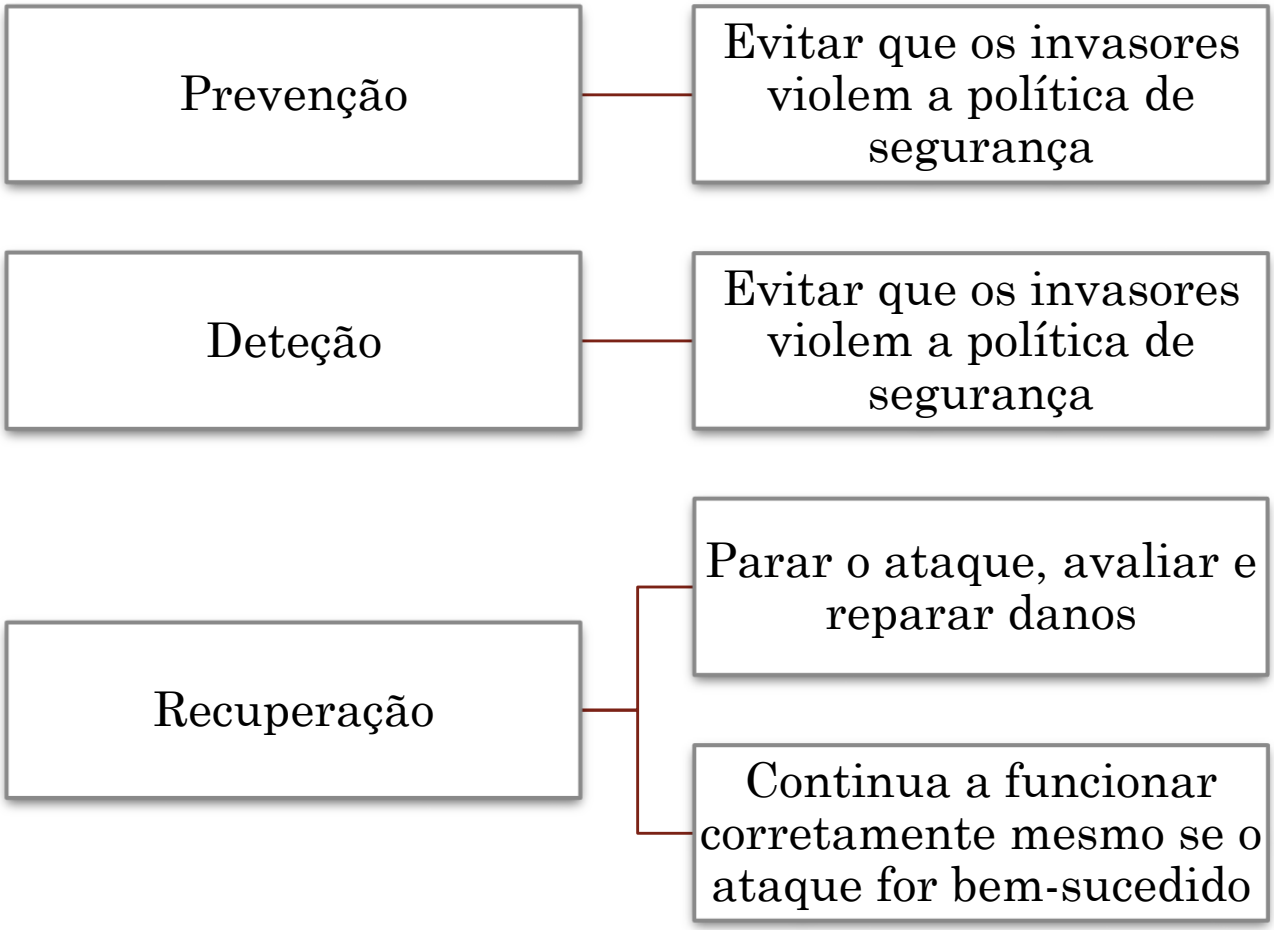
O que é a segurança

- Procedimentos que protegem
  - O próprio, seus funcionários e seus pares
  - Documentos ou meios eletrónicos
  - Hardware, software, e redes
- Proteger contra danos, roubo ou alteração
- Proteger os recursos contra
  - Erro humano
  - Intrusos (do exterior e do interior)
  - Empregados desonestos
  - Sabotagem

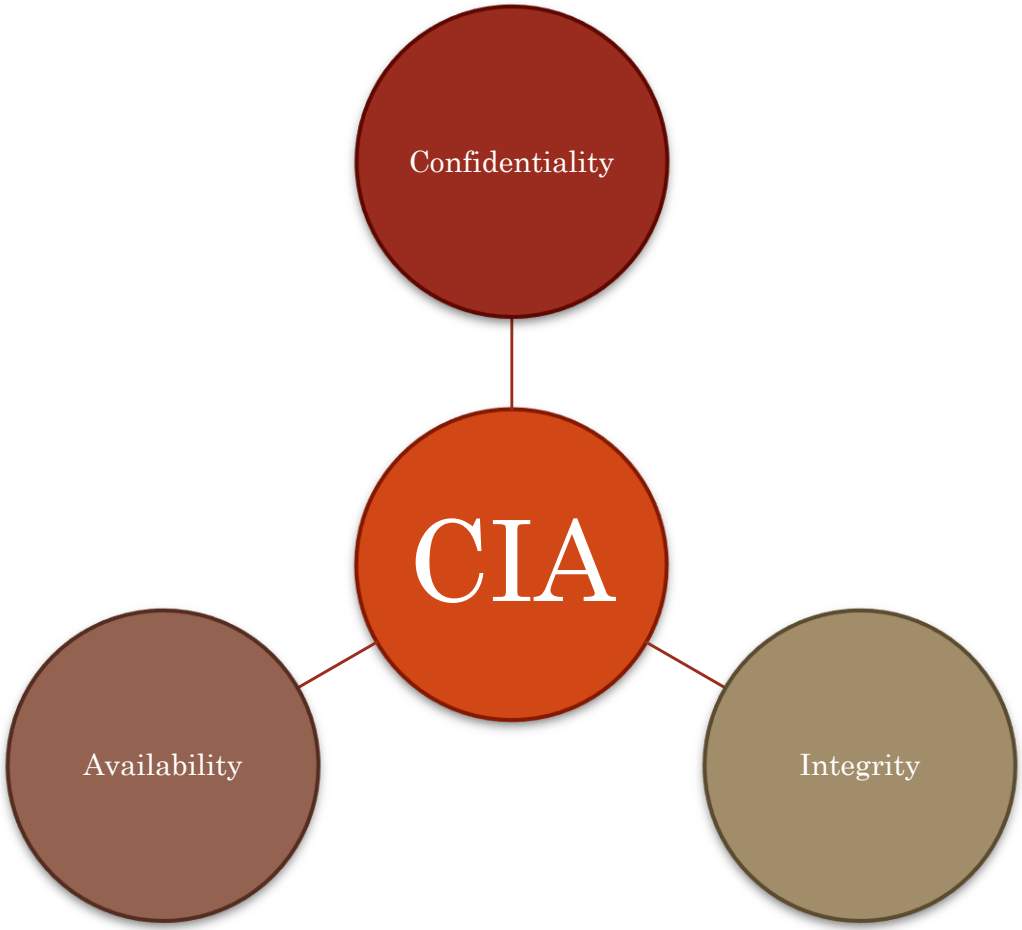
O que é a segurança informática



Objetivos da segurança



Termos importantes

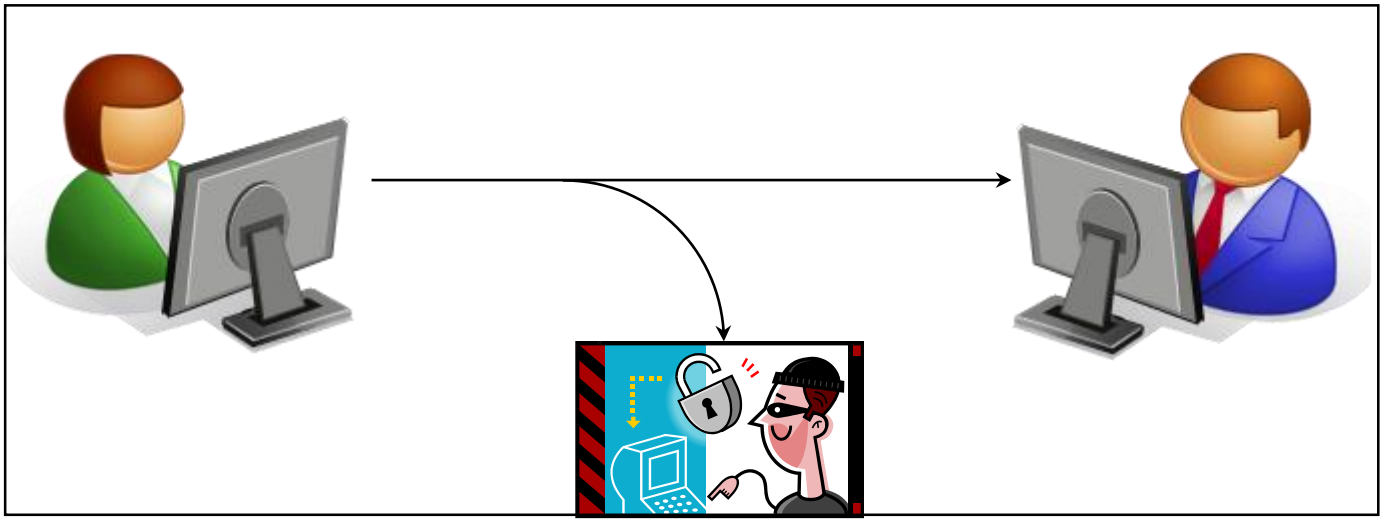


Termos importantes

- **Threat – Ameaça**
  Conjunto de circunstâncias que tem o potencial de causar perda ou dano. Ou uma violação potencial da segurança.
- **Vulnerability – Vulnerabilidade**
  Fraqueza no sistema que pode ser explorada para causar perda ou dano
- **Attack – Ataque**
  Quando uma entidade explora uma vulnerabilidade no sistema
- **Control – controlo**
  Um meio para evitar que uma vulnerabilidade seja explorada

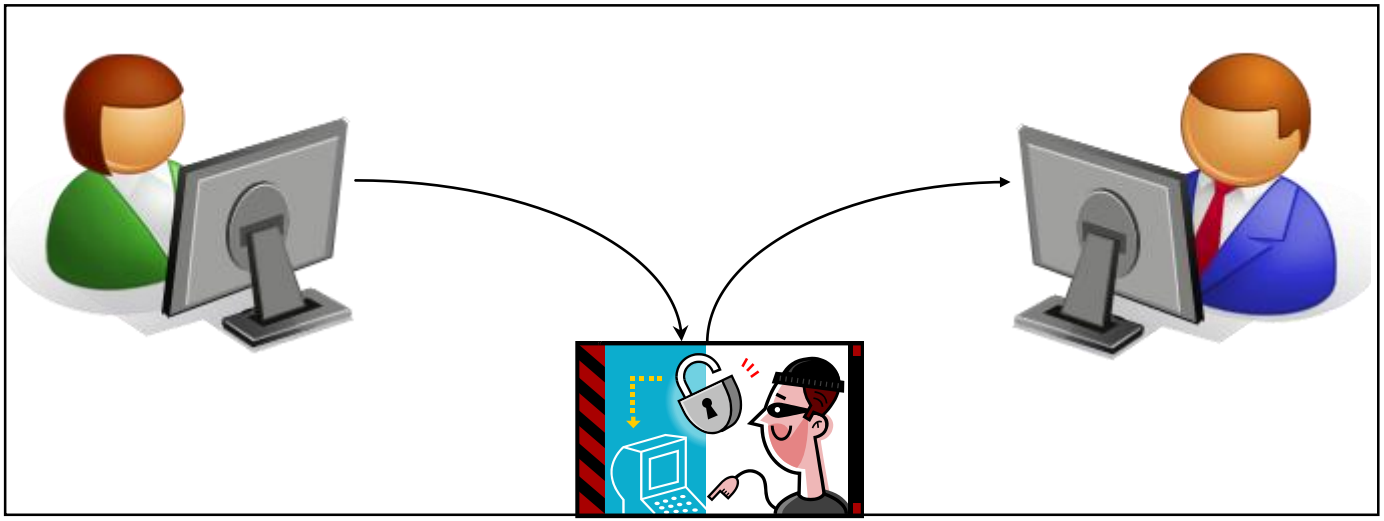
Ataques

- **Eavesdropping**
  Interceção da mensagem
  (Ataque da confidencialidade)
  - Acesso não autorizado à informação
  - Sniffers and wiretappers (escuta nos cabos)
  - Cópia ilícita da ficheiros e programas



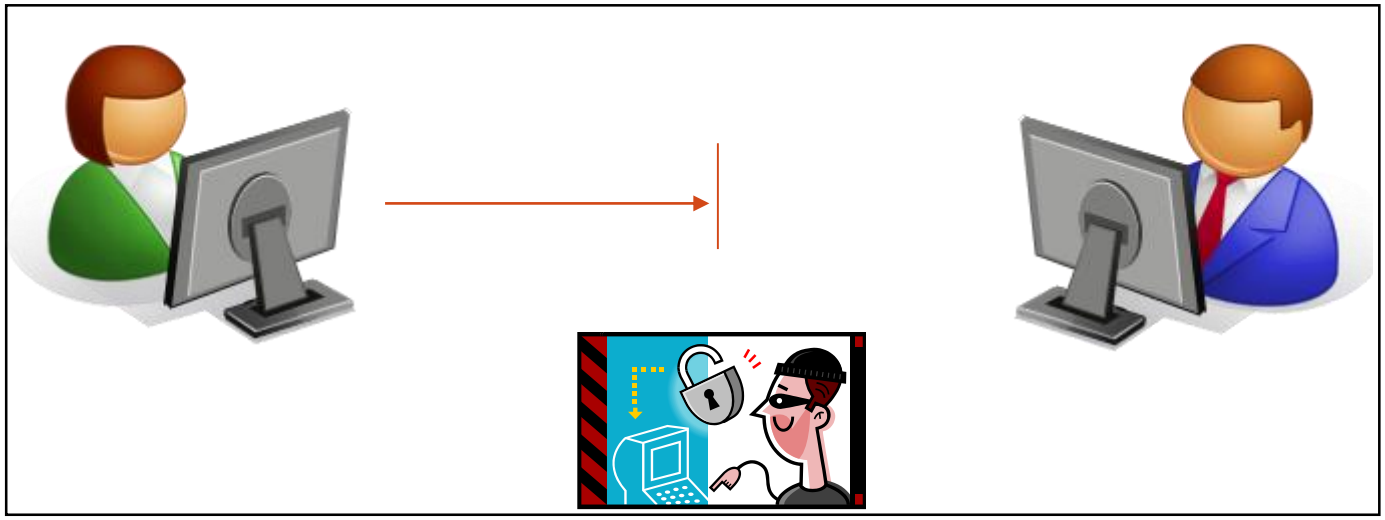
Ataques

- **Tampering**
  Interceção da mensagem
  (Ataque da integridade)
  - Interrompe o fluxo de mensagem
  - Atraso e, opcionalmente, modificação da mensagem
  - Disponibiliza a mensagem de novo

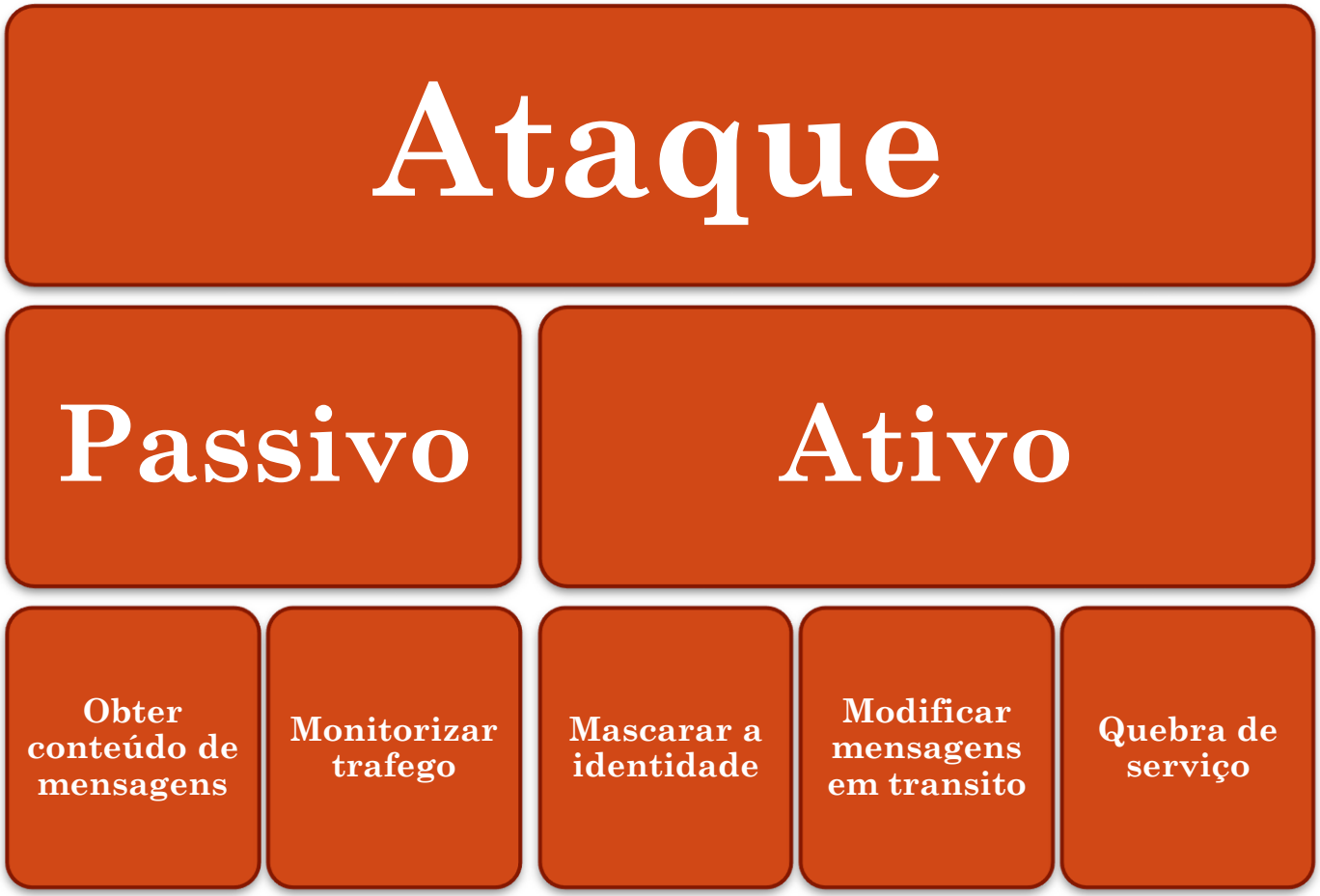


Ataques

- **Ataque na disponibilidade**
  - Destruição do hardware
  - Corromper informação em transito
  - Crash de um servidor/posto de trabalho



Ataques


Ataque
Passivo
Ativo
Obter conteúdo de mensagens
Monitorizar trafego
Mascarar a identidade
Modificar mensagens em transito
Quebra de serviço

Ameaças de segurança

Security threats

1. Trojan horse programs
2. Back door and remote administration programs
3. Denial of service
4. Being an intermediary for another attack
5. Unprotected Windows shares
6. Mobile code (Java, JavaScript, and ActiveX)
7. Cross-site scripting
8. Email spoofing
9. Email-borne viruses
10. Hidden file extensions
11. Chat clients
12. Packet sniffing

Fonte: CERT

Ameaças de segurança

Cavalos de Troia (Trojan Horse Programs)

- Cavalos de Troia são programas que são instalados sem o conhecimento do utilizador
- Programas cavalo de Troia podem executar uma grande variedade de conversações secretas, tais como modificar e apagar arquivos, transmissão de arquivos para o intruso, instalar programas, instalação de vírus e outros programas cavalo de Troia, etc.

Ameaças de segurança

Back door e programas de administração remota

- Instalação secreta de programas de administração remota como o BackOrifice e Netbus, SubSeven
- Esses programas dão acesso remoto ao computador de qualquer lugar na Internet

Ameaças de segurança

Intermediário para outros ataques

- O computador atacado é utilizado para lançar ataques de negação de serviço em outros computadores
- Um agente é normalmente instalado utilizando um programa de cavalo de Troia para lançar o ataque de negação de serviço em outros computadores

Ameaças de segurança

Partilhas de Windows não protegidas

- Código malicioso pode ser guardado nas partilhas não protegidas do Windows ;
- Partilhas não protegidas permitem a terceiros a cópia de ficheiros

Ameaças de segurança

Código móvel – Java, javascript ActiveX

- A possibilidade de códigos móveis, em Java, JavaScript e ActiveX poderem ser executados por um navegador da web (browser) é geralmente útil, mas também pode ser utilizada para executar código mal-intencionado no computador cliente.
- Desabilitar a execução de scripts em Java, JavaScript e ActiveX no navegador Web deve ser considerado se se pretender aceder a sites que não sejam confiáveis
- As mensagens de e-mail recebidas em formato HTML também são suscetíveis ao ataque de código móvel, porque estas também podem transportar código móvel

Ameaças de segurança

Cross-site Scripting (XSS)

- São ataques que visam os sites web que afixam dinamicamente conteúdo do utilizador sem efetuar controlo e codificação das informações apreendidas pelos utilizadores
- Um script malicioso pode ser injetado por um utilizador em páginas que vão ser visualizadas por outros utilizadores.
- Quando outro utilizador visualiza o site o código é executado pelo seu brower.

http://www.cgisecurity.com/xss-faq.html

Ameaças de segurança

E-mail spoofing

- E-mail "spoofing" engana o utilizador ao fazer acreditar que o e-mail foi enviado por um utilizador em vez de outro, por exemplo o administrador, embora ele realmente tenha sido enviado por de um hacker
- Normalmente este tipo de mails solicitam informação pessoal, tal como números de cartões de credito, palavras-chave
- Examinar o cabeçalho do email fornece informação adicional sobre a origem da mensagem

Ameaças de segurança

Vírus enviados por mail

- O código malicioso é muitas vezes distribuído recorrendo aos anexos das mensagens de mail
- Anexos de mensagens de mail devem ser abertos com cuidado

Ameaças de segurança

Extensões de ficheiros escondidas

- Um anexo pode ter uma extensão de arquivo oculto
  - Tais arquivos podem executar o anexo
- Exemplo:
  - MySis.avi.exe
  - TIMOFONICA.TXT.vbs
  - AnnaKournikova.jpg.vbs
    - A extensão escondida é .vbs

Ameaças de segurança

Clientes de chat

- As aplicações de “Internet chat” tais como IM podem incluir a troca de informação e ficheiros que podem conter código malicioso
- O cuidado que se deve ter ao abrir anexos de mail deve-se aplicar aos ficheiros recebidos por chat

Ameaças de segurança

Escuta de pacotes (packet sniffing)

- Programas de packet sniffing capturam o conteúdo de pacotes que podem incluir passwords e outras informações confidenciais que mais tarde podem ser usadas para comprometer o computador do cliente
- A encriptação do tráfego da rede é uma das defesas contra a escuta de pacotes

Níveis de segurança

- A Defense Advanced Research Projects Agency (DARPA) dos Estados Unidos definiu 7 níveis de segurança para os sistemas operativos dos computadores
- Os níveis são usados para definir diferentes níveis de proteção para hardware, software e informações armazenadas.
- O sistema é aditivo - classificações mais elevadas incluem a funcionalidade dos níveis inferiores.

Níveis de segurança

D1

- É a menor forma de estados de segurança disponível (sistema não é confiável)
- Uma classificação D1 nunca é concedido porque esta é essencialmente nenhuma segurança

Níveis de segurança

C1

- C1 é o menor nível de segurança.
- O sistema tem de **ficheiros e diretórios**, **controles de ler e escrever e autenticação** através de login do utilizador. No entanto, a raiz é considerada uma função não segura e a auditoria (logs do sistema) não está disponível.

Níveis de segurança

C2

- C2 possui uma função de auditoria para registrar todos os eventos relacionados com a segurança e oferece maior proteção em ficheiros de sistema, como por exemplo o ficheiro de palavras chave.

Níveis de segurança

B1 e B2

- B1 suporta segurança **multi-nível**, como por exemplo secreto e ultra-secreto, e **controle de acesso obrigatório**, que afirma que um **utilizador não pode alterar as permissões** de ficheiros ou diretórios
- B2 exige que cada objeto e ficheiro seja rotulado de acordo com seu nível de segurança e que esses rótulos mudam dinamicamente dependendo do que está sendo usado.

Níveis de segurança

B3 e A1

- B3 estende os níveis de segurança para dentro do hardware de sistema. Por exemplo, os terminais só podem ser ligados através de caminhos de cabos confiáveis e hardware especializado de forma a garantir que não haja acesso não autorizado
- A1 é o mais alto nível de segurança validado através da Orange Book. O projeto deve ser matematicamente verificado; todo o hardware e software devem ser protegidos durante o transporte para evitar adulterações.