Segurança em sistemas distribuídos

Sistemas Distribuídos

Eduardo Furlan Miranda

2025-10-07

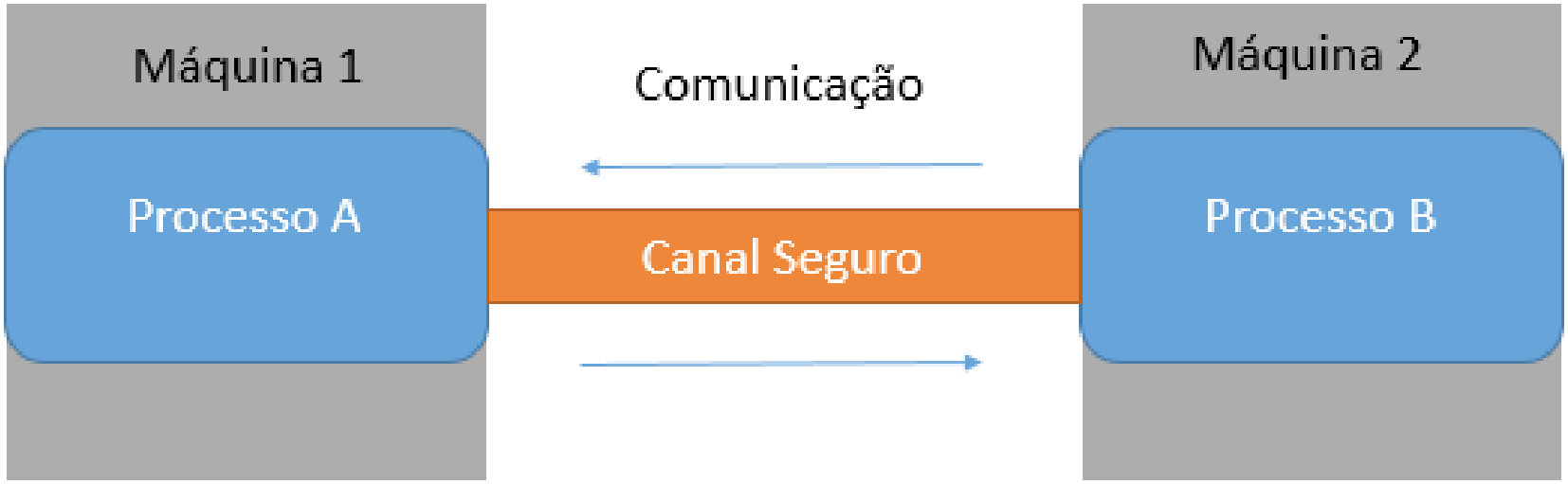
Adaptado de: PEREIRA, C. S. Sistemas Distribuídos. Londrina: EDE SA, 2019. ISBN 978-85-522-1443-4.

- Uma das formas mais funcionais de prevenir os sistemas atualmente é utilizar uma estratégia de segurança multicamada
- Caso ultrapassem alguma camada, deverão ser barradas pelas camadas seguintes
- Vírus, spyware, malware, phishing, invasão de redes, spam e vazamento de dados, Trojan Banking, e-mails e sites infectados
- Fatores: hardware, software, humano

- Em sistemas distribuídos podemos dividir a parte de segurança em duas
  - Permissão de acessos a serviços e recursos disponíveis no sistema
  - Comunicação entre máquinas que contém mais de um processo e usuários diferentes

- 5 fatores relacionados a segurança de um sistema distribuído
  - Confidencialidade - apenas pessoas/máquinas autorizadas
  - Integridade - a informação está acessível
  - Autenticidade - somente usuários e máquinas autenticadas
  - Disponibilidade - a informação está sempre disponível
  - Não repúdio - autenticidade de uma informação utilizada por sistemas distribuídos

- Uma das principais formas de proteção é deixar a comunicação permitida apenas em máquinas com usuários autenticados, em nosso sistema, e com somente as permissões necessárias



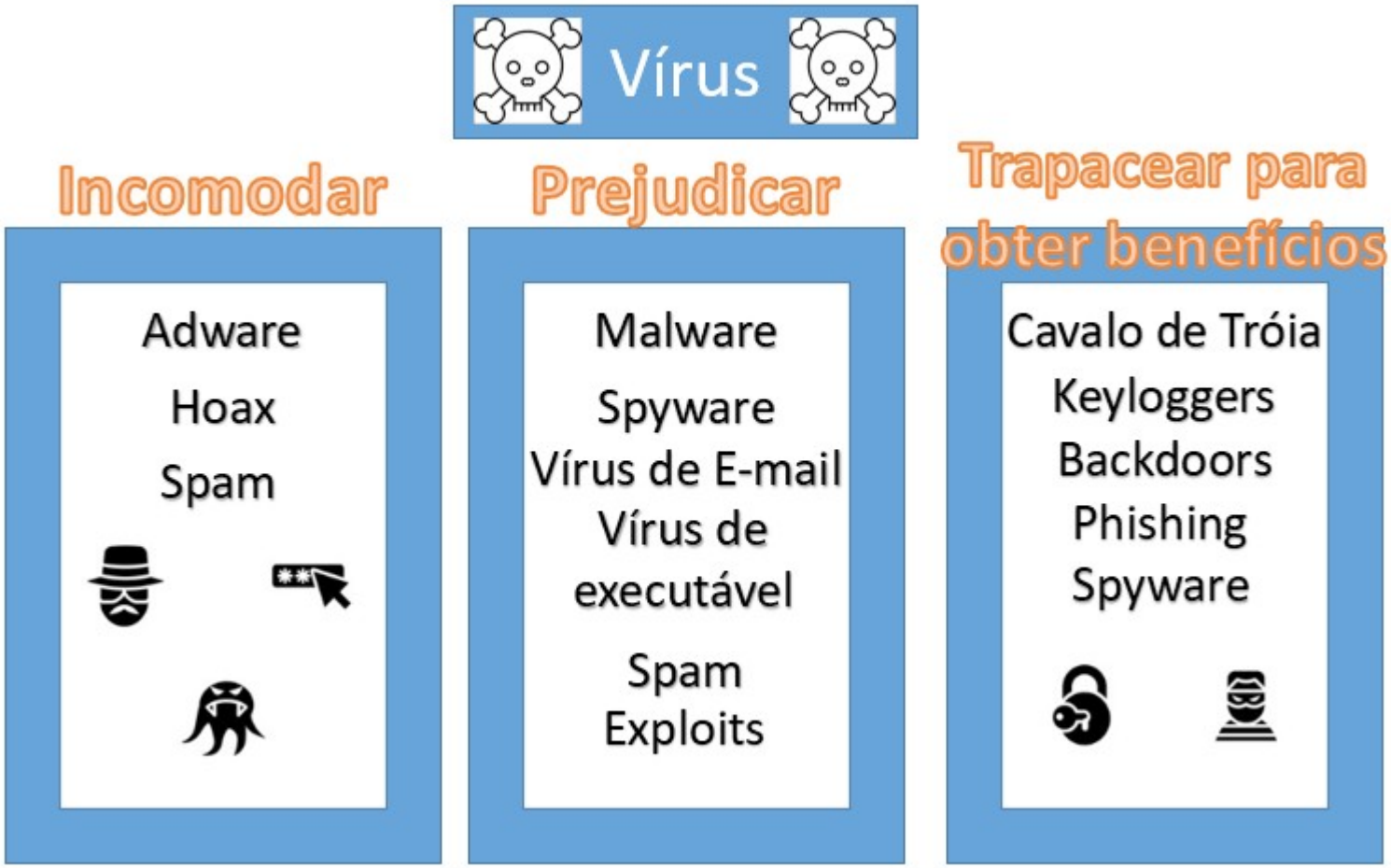
- Classificação das ameaças e seus métodos de ataque
  - Leakage (vazamento): acesso à informação por agentes não autorizados
  - Tampering (falsificação): modificação não autorizada de uma informação
  - Vandalism (vandalismo): interferência no funcionamento de um sistema

- Geralmente, todas as máquinas que compõem um sistema distribuído têm canais de comunicação para acesso autorizado às suas facilidades
  - Através desses canais de comunicação que o acesso não autorizado pode ocorrer

- Estratégias de violação de segurança em sistemas distribuídos
  - Eavesdropping - captura de mensagens da rede
  - Masquerading (disfarce) - mensagens utilizando a identidade de outra máquina
  - Message tampering (falsificação de mensagem) - captura, alteração do conteúdo da mensagem, e transferência ao destinatário
  - Replaying - capturar uma comunicação válida e reenviá-la posteriormente para enganar o sistema e fazê-lo repetir uma ação

- Método simples de infiltração: programas de quebra de senhas para obter as chaves de acesso de algum usuário do sistema
- Outras maneiras mais sutis
  - Vírus - instala em um hospedeiro
  - Worm - replica e se propaga através de redes, de forma autônoma
  - Trojan Horse - disfarçado de programa autêntico
  - Spyware - roubo de informações (espião)
  - Keylogger - grava as teclas digitadas
  - Backdoor - acesso por meios “não oficiais”
  - Spam - email indesejável
  - Adware - anúncios sem autorização
  - Exploit - trecho de código ou sequência de comandos que se aproveita de uma falha de segurança (vulnerabilidade)
  - Hoax - falsas mensagens
  - Phishing - técnica de engenharia social

Ameaças


Vírus
Incomodar
Adware
Hoax
Spam
Prejudicar
Malware
Spyware
Vírus de E-mail
Vírus de executável
Spam
Exploits
Trapacear para obter benefícios
Cavalo de Tróia
Keyloggers
Backdoors
Phishing
Spyware

- O que acontece em muitas empresas, é que às vezes há algum servidor mais vulnerável, com suas portas de acesso liberadas
- E através dessa porta de entrada todo o sistema web é contaminado
- Ex.: uma máquina antiga com um serviço de Wordpress (blogs) quase esquecido, é utilizada como porta de entrada para hackers acessarem boa parte dos arquivos web importantes da empresa

- FTP (File Transfer Protocol)
- SSH (Security Shell)
- Necessidade de atualização constante
- Cópias de segurança
- Protocolo para resposta a incidentes
- Estar preparado antes de acontecer (não é “se”, é “quando”...)