



TEORIA GERAL DE SISTEMAS

Vulnerabilidade dos sistemas e uso indevido

- Um computador desprotegido conectado à Internet pode ser desativado em segundos
- **Segurança:**
 - Políticas, procedimentos e medidas técnicas usadas para prevenir acesso não autorizado, roubo ou danos físicos aos sistemas de informação.
- **Controles:**
 - Métodos, políticas e procedimentos organizacionais que garantem a segurança dos ativos da organização, a precisão e a confiabilidade de seus registros contábeis e a adesão operacional aos padrões administrativos.

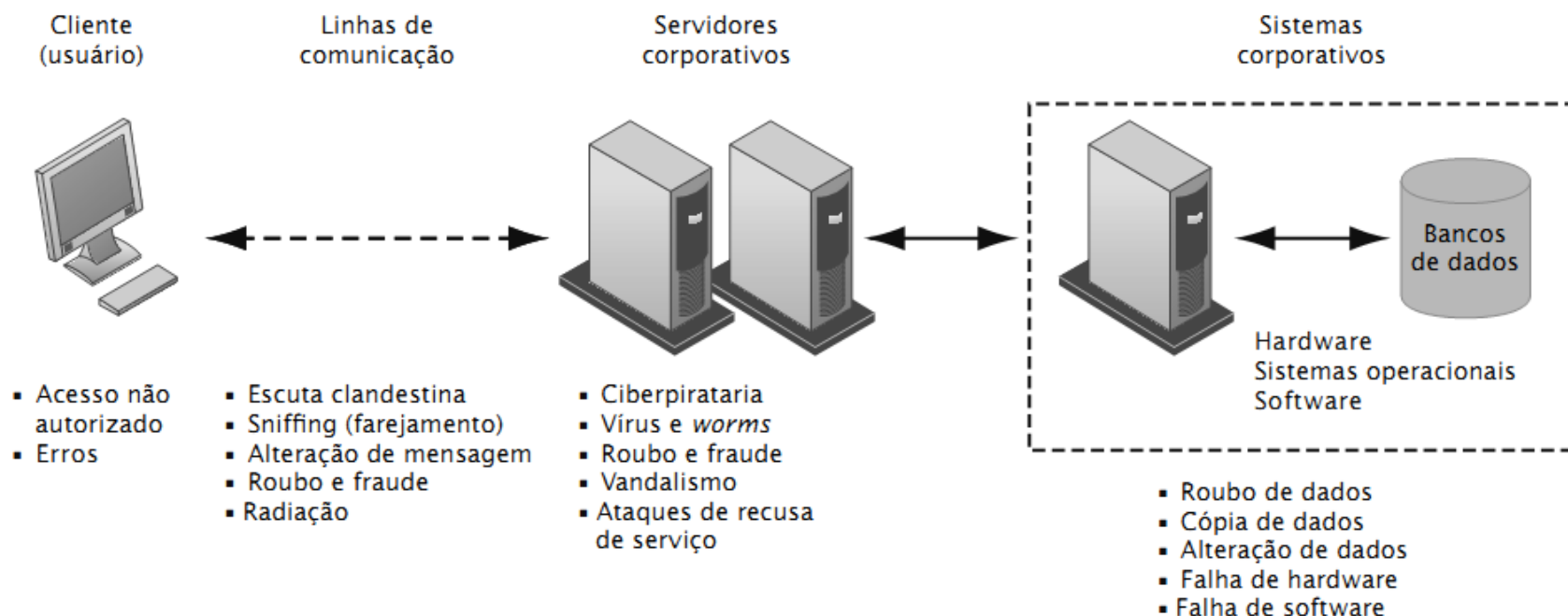
Vulnerabilidade dos sistemas e uso indevido

Por que os sistemas são vulneráveis

- **Problemas de hardware**
 - Avarias, erros de configuração, danos causados pelo uso impróprio ou por crimes.
- **Problemas de software**
 - Erros de programação, erros de instalação, mudanças não autorizadas.
- **Desastres**
 - Quedas de energia, enchentes, incêndios etc.
- **Uso de redes e computadores fora dos limites e do controle da empresa**
 - **Exemplo:** uso por fornecedores nacionais ou estrangeiros.

Vulnerabilidade dos sistemas e uso indevido

Vulnerabilidades e desafios de segurança contemporâneos



Normalmente, a arquitetura de uma aplicação baseada na Web inclui um cliente, um servidor e sistemas de informação corporativos conectados a bancos de dados. Cada um desses componentes apresenta vulnerabilidades e desafios de segurança. Enchentes, incêndios, quedas de energia e outros problemas técnicos podem causar interrupções em qualquer ponto da rede.

Vulnerabilidade dos sistemas e uso indevido

- Vulnerabilidades da Internet
 - Rede aberta a qualquer usuário
 - O tamanho da Internet propicia que os abusos tenham um alto impacto
 - Uso de endereços de Internet fixos com conexões permanentes à rede mundial facilita a identificação por *hackers*
 - Anexos de e-mail
 - E-mails usados para transmissão de segredos de negócios
 - Mensagens instantâneas não são seguras e podem ser facilmente interceptadas

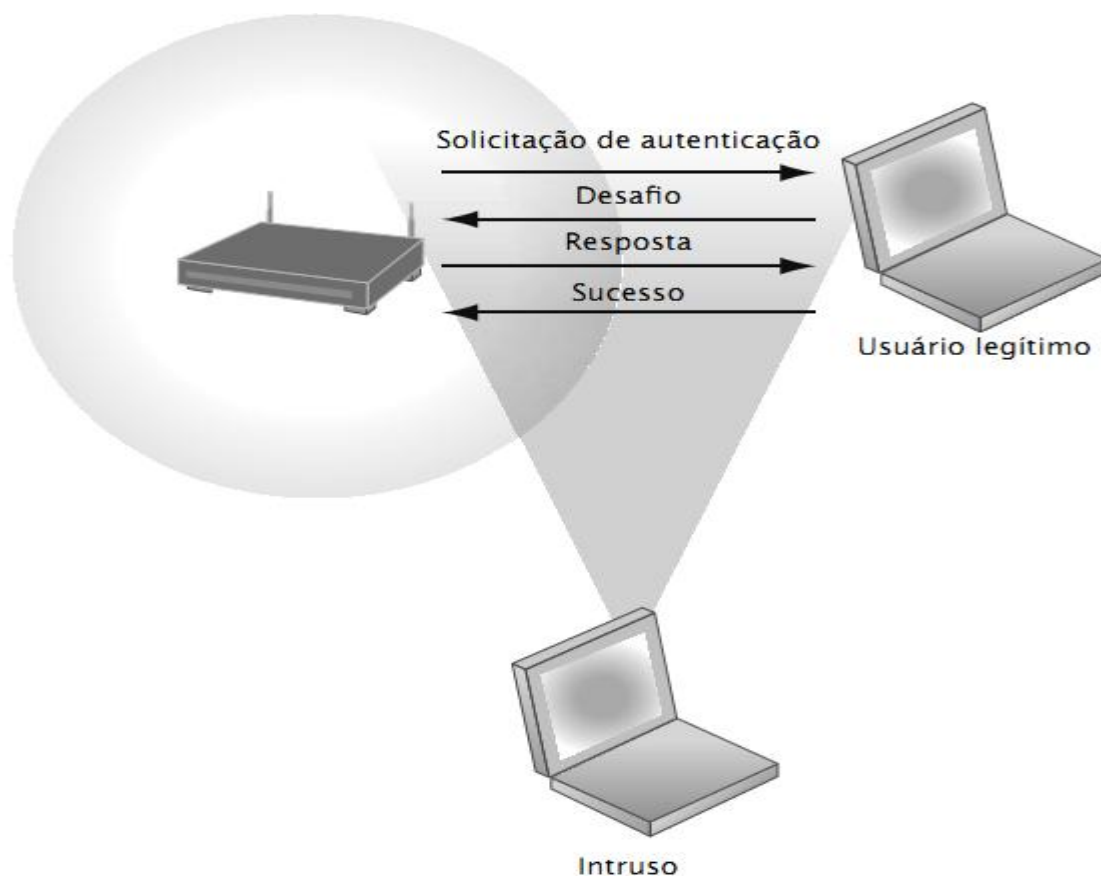
Vulnerabilidade dos sistemas e uso indevido

- Desafios da segurança sem fio
 - Bandas de rádiofrequência são fáceis de serem escaneadas
 - Identificadores de conjunto de serviços (SSIDs)
 - Identificar pontos de acesso
 - Transmitidos várias vezes
 - *War driving*
 - Espião dirige um carro entre edifícios ou estaciona do lado de fora e tenta interceptar o tráfego por redes sem fio
 - Quando os *hackers* obtêm acesso ao SSID, conseguem acessar os recursos da rede
 - WEP (Wired Equivalent Privacy)
 - Padrão de segurança para protocolo 802.11
 - Especificações básicas compartilham a mesma senha tanto para usuários quanto para os pontos de acesso
 - Usuários não fazem uso de recursos de segurança

Vulnerabilidade dos sistemas e uso indevido

Desafios de segurança em ambientes Wi-Fi

Muitas redes Wi-Fi podem ser facilmente invadidas por intrusos. Eles usam programas *sniffers* para obter um endereço e, assim, acessar sem autorização os recursos da rede.



Vulnerabilidade dos sistemas e uso indevido

Software mal-intencionado: vírus, *worms*, cavalos de Troia e *spywares*

- Malware
 - Vírus
 - Programa de software espúrio que se anexa a outros programas de software ou arquivos de dados a fim de ser executado
 - Worms
 - Programas de computador independentes que copiam a si mesmos de um computador para outro por meio de uma rede
 - Cavalos de Tróia
 - Software que parece benigno, mas depois faz algo diferente do esperado

Vulnerabilidade dos sistemas e uso indevido

Software mal-intencionado: vírus, *worms*, cavalos de Troia e *spywares*

- Malware (continuação)
 - Spyware
 - Pequenos programas que se instalam sorrateiramente nos computadores para monitorar a atividade do internauta e usar as informações para fins de marketing.
 - Key loggers
 - Registram cada tecla pressionada em um computador para roubar números seriais de softwares, senhas, deflagrar ataques na Internet.

Vulnerabilidade dos sistemas e uso indevido

Hackers e cibervandalismo

- Hackers X Crackers
 - Hacker: Indivíduo com grande conhecimento, utiliza-o para melhoria da segurança da infraestrutura, dos aplicativos e softwares em geral.
 - Cracker: Indivíduo com grande conhecimento, ao contrário do Hacker, utiliza esse conhecimento para benefício próprio ou de um grupo, ou seja, para invadir, roubar, transferir dados e informações.
- Atividades incluídas:
 - invasão de sistemas;
 - danos a sistemas; e
 - cibervandalismo.
 - Interrupção, a alteração da aparência ou até mesmo a destruição intencional de um site ou sistema de informação corporativo.

Vulnerabilidade dos sistemas e uso indevido

Hackers e cibervandalismo

- ***Spoofing***

- Apresenta-se de maneira disfarçada, usando endereços de e-mail falsos ou fingindo ser outra pessoa.
- Redirecionamento de um link para um endereço diferente do desejado, estando o site “disfarçado” como o destino pretendido.

- ***Sniffer***

- Programa espião que monitora as informações transmitidas por uma rede.
- Permite que os *hackers* roubem informações de qualquer parte da rede, inclusive mensagens de e-mail, arquivos da empresa e relatórios confidenciais.

Vulnerabilidade dos sistemas e uso indevido

Hackers e cibervandalismo

- **Ataque de recusa de serviço (DoS)**
 - Sobrecarregar o servidor com centenas de requisições falsas, a fim de inutilizar a rede
- **Ataque distribuído de recusa de serviço (DDoS)**
 - Uso de inúmeros computadores para iniciar um DoS
 - *Botnets*
 - Redes de PCs “zumbis” infiltradas por um *malware* robô

Vulnerabilidade dos sistemas e uso indevido

Hackers e cibervandalismo

- Crimes de informática
 - Definidos como “**quaisquer violações da legislação criminal que envolvam conhecimento de tecnologia da informática em sua perpetração, investigação ou instauração de processo**”
 - Computadores podem ser alvo de crimes:
 - Violar a confidencialidade de dados computadorizados protegidos
 - Acessar um sistema de computador sem autorização
 - Computadores podem ser instrumentos de crimes:
 - Roubo de segredos comerciais
 - Usar e-mail para ameaças ou assédio