Universidade Federal do Rio Grande do Norte
Unidade Acadêmica Especializada em Ciências Agrárias
Escola Agrícola de Jundiaí
Curso de Análise e Desenvolvimento de Sistemas
TAD0006 - Sistemas Operacionais - Turma 01

Segurança

Antonino Feitosa

antonino.feitosa@ufrn.br

Macaíba, junho de 2025

Aula Passada

- Princípios do Hardware de E/S
  - Tipos de Dispositivos
  - Controladores de Dispositivos
  - Tipos de E/S
- Princípios do Software de E/S
  - Objetivos do Software de E/S
  - E/S Programada
  - E/S Orientada por Interrupções
  - E/S Usando DMA
- Camadas de Software de E/S
  - Tratadores de Interrupção
  - Drivers dos Dispositivos
  - Software de E/S Independente de Dispositivo
  - Software de E/S do Espaço do Usuário

Roteiro

- Segurança
- Ambiente de Segurança
- Segurança de Sistemas Operacionais
- Malwares

Segurança

Segurança

- Como proteger informações contra o uso não autorizado?
  - Função do sistema operacional.

Segurança

- Sistemas isolados, sem conexão a rede alguma.
  - Modelos e mecanismos elaborados foram desenvolvidos para certificar-se de que nenhum usuário conseguisse direitos de acesso aos quais ele não era credenciado.
  - Assume que os sistemas estão corretos, livre de erros.

Segurança

- Sistemas de servidores compartilhados.
  - Interceptação das mensagens.
    - Criptografia.
  - Invasão do sistema.
  - Ameaças internas.

Segurança

- Sistemas operacionais podem apresentar defeitos de segurança.
  - Chamados de **vulnerabilidades**.

Segurança

- O software precisa ser “alimentado” com a sequência de bytes específicos para desencadear a vulnerabilidade.
  - Uma entrada que desencadeia um defeito assim normalmente é chamada de uma **exploração** (exploit).

Segurança

- Explorações podem ser desencadeadas por vírus e similares.
  - Intimamente relacionado com a segurança de redes.

Segurança

- Também podemos ter ameaças internas!

Ambiente de Segurança

Ambiente de Segurança

- Segurança: problemas gerais envolvidos em certificar-se de que os arquivos não sejam lidos ou modificados por pessoas não autorizadas, o que inclui questões técnicas, administrativas, legais e políticas, por um lado.

Ambiente de Segurança

- Mecanismos de proteção: mecanismos do sistema operacional específicos usados para fornecer segurança.

Ambiente de Segurança

- Podemos decompor a segurança em:
  - **Confidencialidade**: diz respeito a fazer com que dados secretos assim permaneçam.
    - O proprietário pode decidir quem deve acessar.
  - **Integridade**: significa que usuários não autorizados não devem ser capazes de modificar dado algum sem a permissão do proprietário.
    - Incluir remover ou atualizar dados.
  - **Disponibilidade**: significa que ninguém pode perturbar o sistema para torná-lo inutilizável.
    - Ataques de recusa de serviço (denial-of-service).

Ambiente de Segurança: Exemplos

1. Um atacante pode farejar o tráfego em uma rede de área local e violar a confidencialidade da informação, especialmente se o protocolo de comunicação não usar encriptação.
2. Um intruso pode atacar um sistema de banco de dados e remover ou modificar alguns registros, violando sua integridade.
3. Um ataque de recusa de serviços bem aplicado pode destruir a disponibilidade de um ou mais sistemas de computadores.

Ambiente de Segurança

- Há muitas maneiras pelas quais uma pessoa de fora pode atacar um sistema.
  - Ferramentas e serviços altamente avançados.
  - Hackers de “chapéu preto” (crackers): pessoas que tentam invadir sistemas computacionais que não lhes dizem respeito.
  - Hackers de “chapéu branco”.

Ambiente de Segurança

- Há uma variedade enorme de maneiras pelas quais atacantes podem comprometer a máquina de um usuário.
  - Podem oferecer versões gratuitas, mas contaminadas, de um software popular.
    - A instalação desses programas proporciona ao atacante o acesso completo à máquina.
      - Computador sob o controle do atacante: um bot ou zumbi.

Ambiente de Segurança

- Privacidade: proteger indivíduos do uso equivocado de informações a seu respeito.
  - O governo deve compilar dossiês sobre todos a fim de pegar sonegadores de X, onde X pode ser “previdência social” ou “taxas”, dependendo da sua política?
  - A polícia deve ter acesso a qualquer coisa e a qualquer um a fim de deter o crime organizado?
  - O governo pode monitorar os telefones celulares diariamente na esperança de pegar potenciais terroristas e criminosos?

Ambiente de Segurança

- Atacantes (ou intrusas, ou adversárias): pessoas que se intrometem em lugares que não lhes dizem respeito.
- Diferentes de motivações: roubo, ativismo cibernético, vandalismo, terrorismo, guerra cibernética, espionagem, spam, extorsão, fraude, exibição, expor a fragilidade de segurança, etc.

Segurança de Sistemas Operacionais

Segurança de Sistemas Operacionais

- O sistema pode ser comprometido de várias maneiras.
  - Senhas padrões: admin, 12345, 0000;
  - Senhas complexas, porém, escritas em papel de fácil acesso;
  - Perda de pen-drives com informações sensíveis;
  - Discos rígidos descartados sem serem apagados.
- Estamos interessados em ataques ao sistema operacional.
  - Existem outros: engenharia de pessoas, ataques de sistemas de redes de computadores, ataques em banco de dados, em sistemas web, etc.

Segurança de Sistemas Operacionais

- Conceitos:
  - Ataques **passivos**: tentam roubar informações;
    - Ex.: Um adversário que fareja o tráfego de rede e tenta violar a codificação (se houver alguma) para conseguir os dados.
  - Ataques **ativos**: tentam fazer com que um programa de computador comporte-se mal.
    - Ex.: o intruso pode assumir o controle do navegador da web de um usuário para fazê-lo executar um código malicioso, a fim de roubar detalhes do cartão de crédito.

Segurança de Sistemas Operacionais

- Conceitos:
  - **Criptografia**: diz respeito a embaralhar uma mensagem ou arquivo de tal maneira que fique difícil de recuperar os dados originais a não ser que você tenha a chave.
    - Envio de dados, armazenamento de arquivos, armazenamento de senhas de acesso.
  - **Endurecimento de software**: acrescenta mecanismos de proteção a programas a fim de dificultar a ação de atacantes que buscam fazê-los comportar-se inadequadamente.
    - Evita que atacantes injetem códigos novos em softwares em execução;
    - Certificar-se de que cada processo tem exatamente os privilégios de que ele precisa para fazer o que deve fazer e nada mais; etc.

Segurança de Sistemas Operacionais

- É possível construir um sistema computacional seguro?
  - Os sistemas atuais não são seguros, mas os usuários não estão dispostos a jogá-los fora.
    - Exemplo do windows.
  - A única maneira segura de construir um sistema seguro é mantê-lo simples.
    - Funcionalidades são o inimigo da segurança.
      - Mais complexidade, mais códigos, mais defeitos e mais erros de segurança.

Segurança de Sistemas Operacionais

- Sistemas confiáveis: sistemas que têm exigências de segurança declaradas e atendem a essas exigências.
  - Forças armadas.
- Base Computacional Confiável (TCB — Trusted Computing Base): hardware e software necessários para impor todas as regras de segurança.
  - Se a base de computação confiável estiver funcionando de acordo com a especificação, a segurança do sistema não pode ser comprometida, não importa o que mais estiver errado.

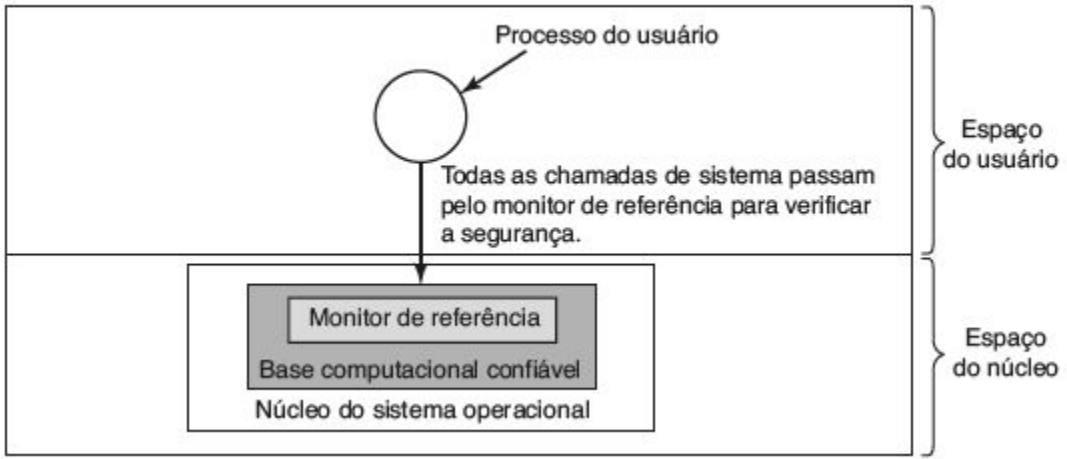
Segurança de Sistemas Operacionais

- Monitor de referência: parte do TCB.
  - O monitor de referência aceita todas as chamadas de sistema envolvendo segurança, como a abertura de arquivos, e decide se elas devem ser processadas ou não.
  - Permite que todas as decisões de segurança sejam colocadas em um lugar, sem a possibilidade de desviar-se dele.
    - A maioria dos SOs não seguem esse projeto.

Segurança de Sistemas Operacionais

- Monitor de referência

FIGURA 9.2 Um monitor de referência.



Controlando o Acesso aos Recursos

Controlando o Acesso aos Recursos

- A segurança é muito mais fácil de atingir se há um modelo claro do que deve ser protegido e quem tem permissão para fazer o quê.
- Um sistema computacional contém muitos recursos, ou “objetos”, que precisam ser protegidos.
  - Recursos possuem um nome único e um conjunto de operações.
  - Mecanismos para permitir acesso, indicando o subconjunto de operações.

Controlando o Acesso aos Recursos

- Domínio: é um conjunto de pares (objetos, direitos).
  - Cada par especifica um objeto e algum subconjunto das operações que podem ser desempenhadas nele.
  - Direito: permissão para desempenhar uma das operações.
- POLA (Principle of Least Authority — Princípio da Menor Autoridade).
  - Cada domínio tem os objetos e os privilégios mínimos para realizar o seu trabalho e nada mais.

Controlando o Acesso aos Recursos

- Como o sistema controla quais objetos pertencem a qual domínio.
  - Podemos visualizar uma matriz, em que as linhas são os domínios e as colunas os objetos.

FIGURA 9.4 Uma matriz de proteção.

	Objeto							
	Arquivo1	Arquivo2	Arquivo3	Arquivo4	Arquivo5	Arquivo6	Impressora1	Plotter2
Domínio 1	Leitura	Leitura Escrita						
2			Leitura	Leitura Escrita Execução	Leitura Escrita		Escrita	
3						Leitura Escrita Execução	Escrita	Escrita

Autenticação

Autenticação

- Todo sistema computacional seguro deve exigir que todos os usuários sejam autenticados no momento do login.
- Princípios gerais de identificação:
  - Algo que o usuário conhece (senhas, informações, etc.).
  - Algo que o usuário tem (cartões magnéticos).
    - Cartão inteligente (processador simples e memória).
      - Operam offline.
  - Algo que o usuário é (biometria).
    - Cadastramento e identificação.
    - A característica deve variar entre as pessoas.
    - A característica deve persistir em um tempo razoável.

Autenticação

- Feedback de login: deve exibir somente sucesso ou falha.
  - Não deve indicar se o usuário existe ou não.
    - Pode revelar um login válido para o sistema.

FIGURA 9.17 (a) Um login bem-sucedido. (b) Login rejeitado após nome ser inserido. (c) Login rejeitado após nome e senha serem digitados.

(a)	(b)	(c)
LOGIN: mauro	LOGIN: carolina	LOGIN: carolina
SENHA: qualquer	NOME INVÁLIDO	SENHA: umdois
LOGIN COM SUCESSO	LOGIN:	LOGIN INVÁLIDO
		LOGIN:

Ataques Internos

Ataques Internos

- São executados por programadores e outros empregados da empresa executando o computador a ser protegido ou produzindo um software crítico.

Ataques Internos: Bomba Lógica

- Bomba lógica: é um fragmento de código escrito por um dos programadores da empresa e secretamente inserido no sistema de produção.
- Se bomba lógica não for alimentada com sua senha diária então ele é detonada (a detonação pode ser agendada).
  - Alimentação por login no sistema, nome na folha de pagamento, etc.
  - Detonar poderia envolver limpar o disco, apagar arquivos de forma aleatória, cuidadosamente fazer mudanças difíceis de serem detectadas em programas fundamentais, ou criptografar arquivos essenciais.

Ataques Internos: Back door

- Back door (porta dos fundos): código inserido no sistema por um programador para driblar alguma verificação normal.
- Revisões de código minimizam o problema.

Ataques Internos: Mascaramento de Login

- Mascaramento de login (login spoofing).
  - Usuário legítimo que está tentando conseguir as senhas de outras pessoas.
  - Empregada em organizações com muitos computadores públicos em uma LAN usados por múltiplos usuários.
- O usuário malicioso cria um programa que apresenta uma tela similar a tela do sistema.
  - Após coletar o login e senha, o programa encerra, apresentando o sistema real.
  - O usuário presume que cometeu um erro de digitação e simplesmente conecta-se de novo.

Malware

Malware

- Malware: software malicioso como vírus, worms, cavalos de Tróia e similares.
- Atualmente são usados por criminosos para infectar máquinas de forma sutil.
  - Instalação de software e porta dos fundos.
    - Máquina zumbi ou botnet.
  - Exemplos de uso: spams comerciais, ataques de recusa de serviço, ransomware, keylogger.

Malware

- Malware no sistema de um adversário, diminuindo a qualidade dos produtos produzidos.
- Malware para ataques pessoais: comprometimento de dados operacionais.
- Malware para comprometer os dados da UEFI.
  - Se o chip de memória flash estiver soldado na placa-mãe, provavelmente a placa inteira terá de ser jogada fora, e uma nova, comprada.

Malware

- Por que o malware se dissemina tão facilmente?
  - Cerca de 70% dos sistemas do mundo usam o windows.
  - Windows foi projetado para facilidade de uso em detrimento da segurança.

Cavalos de Tróia

- Cavalos de Tróia: qualquer malware escondido no software ou em uma página da web que as pessoas baixam voluntariamente.
  - Também certificam-se de que ele seja reiniciado sempre que a máquina for reinicializada.
- Como fazer com que as pessoas os instale?
  - Escrever algum programa genuinamente útil e embutir o malware dentro dele.

Vírus

- Vírus: é um programa que pode reproduzir--se anexando o seu código a outro programa, de maneira análoga à reprodução dos vírus biológicos.
  - Como os vírus funcionam?

Vírus

- O programador desenvolve o vírus e o insere em um programa na sua própria máquina.
  - O programa deve ser algo desejável: último jogo lançado, etc.
- As pessoas baixam o programa e o instalam.
- Quando o programa for executado, o vírus também será, infectando outros programas e então executando sua carga útil.
  - A execução da carga útil pode ser programada com um atraso para garantir que várias máquinas sejam infectadas.

Vírus:

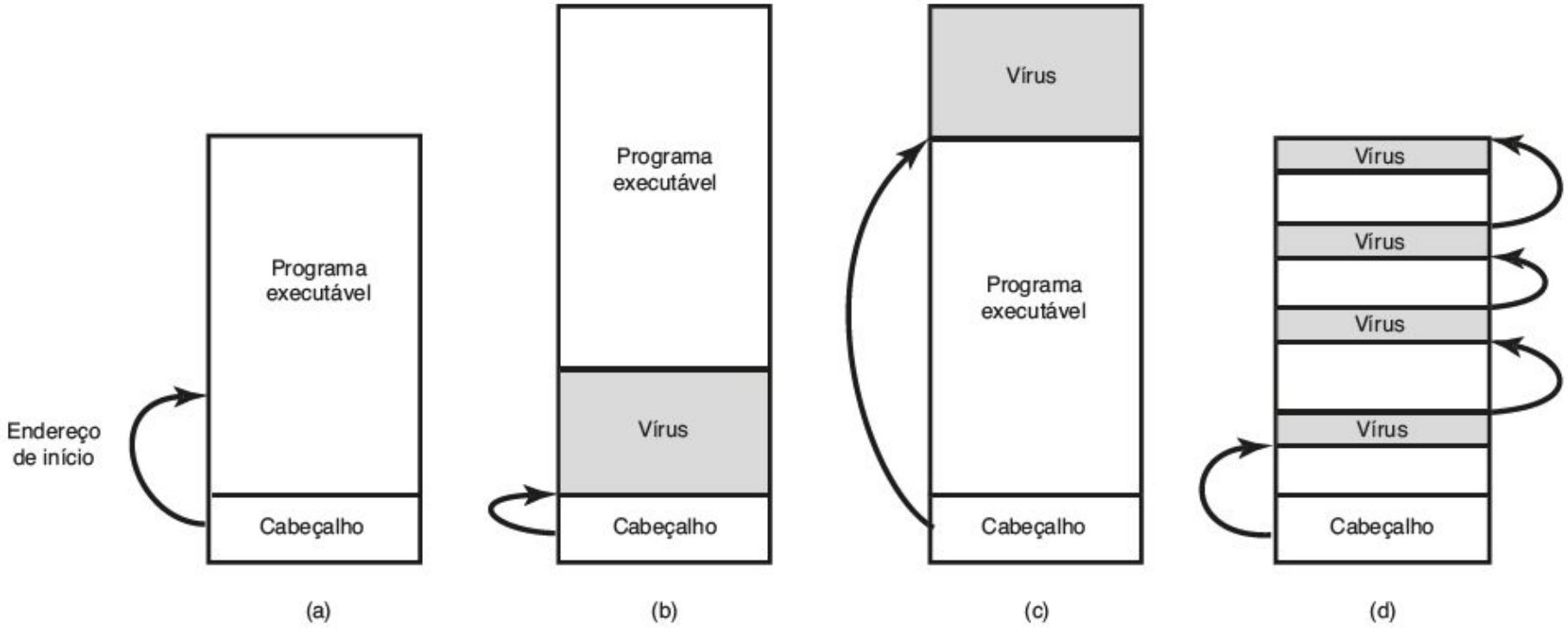
- Vírus companheiro: não infecta de fato um programa, mas é executado quando o programa for executado.
  - Ex.: alteração do atalho para um aplicativo.
- Vírus de programas executáveis: sobrescreve o programa executável com ele mesmo.
  - Facilmente detectado.

Vírus:

- Vírus parasitas: se anexam ao programa, mas preservam as suas funcionalidades.
  - Podem ligar-se na frente: copiar o programa para RAM, colocar-se na frente e então copiá-lo de volta da RAM após si mesmo.
    - Necessário realocar os endereços do programa.
  - Podem ligar-se no fim: necessita deslocar as instruções para o seu espaço de endereçamento que precisa ser relativo.
  - Podem ligar-se no meio: explora a fragmentação interna de sistemas com segmentos de tamanho fixo.
    - Difícil detecção.

Vírus:

FIGURA 9.29 (a) Um programa executável. (b) Com um vírus na frente. (c) Com um vírus no fim. (d) Com um vírus espalhado pelos espaços livres ao longo do programa.



Vírus:

- Vírus residentes na memória: permanece na memória (RAM) o tempo inteiro.
  - Pode sobrescrever o vetor de interrupções para executar vírus.
    - Executado em toda chamada do sistemas.

Vermes (worms)

- Verme: programa que se autorreplica.
- A primeira violação de computadores da internet em grande escala começou na noite de 2 de novembro de 1988, quando um estudante formado pela Universidade de Cornell, Robert Tappan Morris, liberou um programa de verme na internet.

Spyware

- Spyware: é um software que, carregado sorrateiramente no PC sem o conhecimento do dono, executa no segundo plano fazendo coisas por trás das costas do proprietário.
  - Se esconde, de maneira que a vítima não pode encontrá-lo facilmente.
  - Coleta dados a respeito do usuário (sites visitados, senhas, até mesmo números de cartões de crédito).
  - Comunica a informação coletada de volta para seu mestre distante.
  - Tenta sobreviver a determinadas tentativas para removê-lo.

Spyware

- Três categorias:
  - Marketing: o spyware simplesmente coleta informações e as envia de volta para seu mestre, normalmente para melhor direcionamento da propaganda para máquinas específicas.
  - Vigilância: empresas intencionalmente colocam spywares em máquinas dos empregados para rastrear o que eles estão fazendo e quais sites eles estão visitando.
  - Botnet: a máquina infectada torna-se parte de um exército zumbi esperando por seu mestre para dar a ela suas ordens de marcha.

Spyware

- Como um computador se infecta com spyware?
  - Por um cavalo de Tróia.
  - Contágio por contato: apenas visitando uma página na web infectada.
    - A página na web pode redirecionar o navegador para um arquivo (.exe) executável. O navegador solicitará permissão para executá-lo.
    - Barra de ferramentas de navegadores infectada: instalação voluntária.
    - Controles activeX: tecnologia da Microsoft.
      - Dependendo do nível de segurança, podem ser instalados automaticamente.

Leitura Complementar

Leitura Complementar

- Sistemas Distribuídos: seção 8.3
- Exploração de Software: seção 9.7
- Defesas: seção 9.10

- Livro de Sistemas Operacionais Modernos, 4 ed., Tanenbaum.

Resumo

Resumo

- Segurança
- Ambiente de Segurança
- Segurança de Sistemas Operacionais
  - Controle de Acesso aos Recursos
  - Autenticação
  - Ameaças Internas
- Malwares
- Exploração de Software
- Defesas

Dúvidas?