Segurança em Sistemas Operacionais

Introdução **1**
Objetivos da Segurança 1
Ameaças à Segurança **2**
Mecanismos de Proteção **3**
Autenticação de Usuários 4
Segurança em Linux e Windows **5**
Segurança no Linux 5
Segurança no Windows 5
Conclusão **6**
Referências **6**

Introdução

A segurança é um aspecto cada vez mais crítico dos sistemas computacionais modernos. À medida que mais informações sensíveis são armazenadas e processadas digitalmente, e com a crescente interconexão de sistemas através de redes como a Internet, a necessidade de proteger os sistemas contra acesso não autorizado, modificação indevida, negação de serviço e outras ameaças tornou-se primordial. O sistema operacional desempenha um papel central na segurança do sistema, pois controla o acesso a todos os recursos de hardware e software. Este capítulo explora os objetivos da segurança em sistemas operacionais, as diversas ameaças que eles enfrentam, os mecanismos de proteção implementados para mitigar essas ameaças, as técnicas de autenticação de usuários e, finalmente, uma visão geral das funcionalidades de segurança específicas nos sistemas operacionais Linux e Windows.

Objetivos da Segurança

Os objetivos fundamentais da segurança da informação, frequentemente referidos pela tríade CIA, são cruciais para os sistemas operacionais:

- **Confidencialidade (Confidentiality):** Garantir que a informação seja acessível apenas por entidades autorizadas. Isso envolve proteger os dados contra divulgação não autorizada. Mecanismos como criptografia e controle de acesso são usados para alcançar a confidencialidade.
- **Integridade (Integrity):** Assegurar que a informação e os recursos do sistema sejam precisos e completos, e que só possam ser modificados de maneira autorizada. A integridade protege contra a alteração ou corrupção indevida de dados e software.

- **Disponibilidade (Availability):** Garantir que os recursos do sistema e os dados estejam acessíveis e utilizáveis por entidades autorizadas quando necessário. Ameaças como ataques de negação de serviço (Denial of Service - DoS) visam comprometer a disponibilidade.

Além da tríade CIA, outros objetivos importantes incluem:

- **Autenticidade (Authenticity):** Verificar a identidade de usuários, processos ou dispositivos para garantir que são quem afirmam ser.
- **Não Repúdio (Non-repudiation):** Garantir que uma entidade não possa negar ter realizado uma determinada ação (e.g., enviar uma mensagem, aprovar uma transação).
- **Responsabilização (Accountability):** Rastrear as ações dos usuários e processos para que possam ser responsabilizados por suas atividades, geralmente através de logs de auditoria.

Ameaças à Segurança

Os sistemas operacionais estão sujeitos a uma ampla gama de ameaças que podem comprometer seus objetivos de segurança. Essas ameaças podem originar-se de fontes internas ou externas e podem ser intencionais ou acidentais.

- **Malware (Software Malicioso):**
  - **Vírus:** Fragmentos de código que se anexam a programas legítimos. Quando o programa hospedeiro é executado, o vírus também é executado, podendo se replicar e infectar outros programas, além de realizar ações maliciosas.
  - **Worms (Vermes):** Programas autônomos que se replicam e se espalham através de redes, explorando vulnerabilidades em sistemas operacionais ou aplicações. Diferentemente dos vírus, não precisam de um programa hospedeiro.
  - **Cavalos de Troia (Trojan Horses):** Programas que parecem ter uma funcionalidade útil, mas que escondem código malicioso. Enganam o usuário para que os execute.
  - **Spyware:** Software que coleta informações sobre o usuário e suas atividades sem seu conhecimento ou consentimento (e.g., senhas, histórico de navegação).
  - **Ransomware:** Malware que criptografa os arquivos do usuário ou bloqueia o acesso ao sistema, exigindo um resgate (ransom) para restaurar o acesso.
  - **Rootkits:** Malware projetado para obter acesso de administrador (root) a um sistema e ocultar sua presença e atividades maliciosas do sistema operacional e de ferramentas de segurança.
- **Ataques de Rede:**

  - **Ataques de Negação de Serviço (Denial of Service - DoS):** Tentativas de tornar um recurso de rede ou sistema indisponível para seus usuários legítimos, sobrecarregando-o com tráfego ou explorando vulnerabilidades. Ataques de Negação de Serviço Distribuído (DDoS) usam múltiplas fontes comprometidas (botnets) para lançar o ataque.
  - **Sniffing (Interceptação de Pacotes):** Capturar e analisar pacotes de dados que trafegam em uma rede para obter informações sensíveis (e.g., senhas, dados não criptografados).
  - **Spoofing (Falsificação):** Disfarçar a origem de uma comunicação (e.g., IP spoofing, email spoofing) para enganar o destinatário ou contornar controles de acesso.
  - **Man-in-the-Middle (MitM):** Um invasor intercepta secretamente e possivelmente altera a comunicação entre duas partes que acreditam estar se comunicando diretamente.
- **Engenharia Social:** Manipulação psicológica de pessoas para que realizem ações ou divulguem informações confidenciais. Exemplos incluem phishing (e-mails fraudulentos para obter credenciais) e pretexting.
- **Ameaças Internas (Insider Threats):** Usuários legítimos (funcionários, ex-funcionários, parceiros) que abusam de seus privilégios de acesso para causar danos ou roubar informações.
- **Vulnerabilidades de Software:** Falhas ou fraquezas no design, implementação ou configuração de software (incluindo o SO) que podem ser exploradas por invasores. Exemplos incluem buffer overflows, SQL injection, cross-site scripting (XSS).

Mecanismos de Proteção

Os sistemas operacionais implementam vários mecanismos de proteção para controlar o acesso aos recursos do sistema e impor políticas de segurança.

- **Domínios de Proteção (Protection Domains):** Um domínio é um conjunto de pares (objeto, conjunto de direitos de acesso). Um processo executa em um domínio e pode acessar apenas os objetos especificados nesse domínio com os direitos permitidos. A troca de domínios (domain switching) permite que um processo altere seu conjunto de direitos (e.g., quando um processo de usuário faz uma chamada de sistema e entra no modo kernel).
- **Anéis de Proteção (Protection Rings):** Uma forma hierárquica de domínios de proteção, onde anéis internos têm mais privilégios que anéis externos. O kernel do SO geralmente roda no anel mais interno (e.g., anel 0), enquanto aplicações de usuário rodam em anéis menos privilegiados (e.g., anel 3).
- **Matriz de Acesso (Access Matrix):** Um modelo abstrato para descrever os direitos de proteção. As linhas da matriz representam domínios (ou sujeitos, como processos ou usuários), e as colunas representam objetos (e.g., arquivos, dispositivos). A entrada Matriz[i, j] especifica o conjunto de operações que um processo no domínio i pode invocar no objeto j.
- **Implementações da Matriz de Acesso:**

  - **Listas de Controle de Acesso (Access Control Lists - ACLs):** Para cada objeto, uma ACL especifica os usuários (ou grupos) e os tipos de acesso permitidos. É como armazenar as colunas da matriz de acesso com os objetos.
  - **Listas de Capacidades (Capability Lists - C-Lists):** Para cada domínio (ou sujeito), uma lista de capacidades especifica os objetos que podem ser acessados e as operações permitidas. Uma capacidade é como um token que concede acesso. É como armazenar as linhas da matriz de acesso com os sujeitos.
- **Princípio do Menor Privilégio (Principle of Least Privilege):** Programas e usuários devem operar usando o menor conjunto de privilégios necessários para completar suas tarefas. Isso limita o dano que pode resultar de um acidente, erro ou exploração.
- **Sandboxing:** Isolar processos em um ambiente restrito (sandbox) onde eles têm acesso limitado aos recursos do sistema. Usado para executar código não confiável de forma segura.
- **Firewalls:** Filtram o tráfego de rede de entrada e/ou saída com base em um conjunto de regras de segurança, ajudando a proteger contra acessos não autorizados e certos tipos de ataques de rede.
- **Sistemas de Detecção/Prevenção de Intrusão (IDS/IPS):** Monitoram o tráfego de rede ou atividades do sistema em busca de sinais de atividades maliciosas ou violações de políticas. Um IDS alerta sobre possíveis intrusões, enquanto um IPS tenta bloqueá-las ativamente.

Autenticação de Usuários

A autenticação é o processo de verificar a identidade de um usuário antes de conceder acesso ao sistema. Existem três fatores principais de autenticação:

1. **Algo que o usuário sabe (Knowledge Factor):**
   - **Senhas (Passwords):** O método mais comum. A eficácia depende da força da senha (comprimento, complexidade) e de como ela é protegida (e.g., armazenada como hash com salt).
   – **PINs (Personal Identification Numbers).**
2. **Algo que o usuário tem (Possession Factor):**
   - **Tokens de Segurança:** Dispositivos físicos (e.g., smart cards, tokens USB, chaves de segurança) que geram senhas de uso único (One-Time Passwords - OTPs) ou contêm certificados digitais.
   - **Telefones Celulares:** Usados para receber códigos OTP via SMS ou através de aplicativos autenticadores.
3. **Algo que o usuário é (Inherence Factor):**
   - **Biometria:** Usa características físicas ou comportamentais únicas do indivíduo, como impressões digitais, reconhecimento facial, reconhecimento de íris, reconhecimento de voz.

- **Autenticação Multifator (Multi-Factor Authentication - MFA):** Requer que o usuário forneça evidências de dois ou mais fatores de autenticação diferentes para aumentar a segurança. Por exemplo, senha (algo que sabe) mais um código OTP de um aplicativo autenticador (algo que tem).

Segurança em Linux e Windows

Ambos os sistemas operacionais implementam uma variedade de mecanismos de segurança.

Segurança no Linux

- **Permissões de Arquivo Tradicionais (rwx):** Para proprietário, grupo e outros.
- **Listas de Controle de Acesso (ACLs POSIX):** Permitem um controle de acesso mais granular do que as permissões tradicionais.
- **SELinux (Security-Enhanced Linux):** Uma implementação de Controle de Acesso Obrigatório (Mandatory Access Control - MAC) que permite definir políticas de segurança detalhadas sobre o que processos e usuários podem fazer. Pode confinar processos a domínios restritos.
- **AppArmor:** Outro sistema MAC, mais focado em perfis por aplicação, definindo quais recursos um programa específico pode acessar.
- **Capabilities (Capacidades POSIX):** Permitem dividir os privilégios de root em unidades menores, de modo que um processo possa receber apenas as capacidades específicas de que necessita, em vez de todos os privilégios de root.
- **Firewall (iptables/nftables):** Ferramentas poderosas para configurar regras de firewall no nível do kernel.
- **Criptografia de Disco (e.g., LUKS/dm-crypt):** Para proteger dados em repouso.
- **PAM (Pluggable Authentication Modules):** Uma estrutura flexível para gerenciar a autenticação de usuários, permitindo que diferentes módulos de autenticação sejam usados.

Segurança no Windows

- **Listas de Controle de Acesso (ACLs):** O NTFS usa ACLs extensivamente para controlar o acesso a arquivos, diretórios e outros objetos do sistema. Cada entrada em uma ACL é uma ACE (Access Control Entry) que especifica um trustee (usuário ou grupo) e suas permissões.
- **Controle de Conta de Usuário (User Account Control - UAC):** Ajuda a prevenir alterações não autorizadas no sistema, solicitando permissão ou credenciais de administrador antes de permitir que tarefas potencialmente perigosas sejam executadas, mesmo que o usuário esteja logado como administrador.
- **BitLocker Drive Encryption:** Criptografia de volume completo para proteger dados em repouso.
- **Windows Defender (Antivírus e Firewall):** Ferramentas de segurança integradas.

- **AppLocker / Windows Defender Application Control:** Permitem que administradores controlem quais aplicações podem ser executadas no sistema (whitelisting).
- **Integridade de Código (Code Integrity):** Garante que apenas drivers e componentes do sistema assinados digitalmente e confiáveis possam ser carregados.
- **Autenticação:** Suporte robusto para senhas, smart cards, Windows Hello (biometria e PINs), e integração com Active Directory para gerenciamento centralizado de identidades e políticas.
- **Security Development Lifecycle (SDL):** Um processo que a Microsoft usa para construir software mais seguro.

Conclusão

A segurança em sistemas operacionais é um campo complexo e em constante evolução, essencial para proteger os ativos digitais e garantir a operação confiável dos sistemas. Os SOs modernos empregam uma abordagem de defesa em profundidade, combinando múltiplos mecanismos de proteção, autenticação robusta e ferramentas para mitigar uma ampla gama de ameaças. Desde a proteção da confidencialidade, integridade e disponibilidade dos dados até o controle granular do acesso aos recursos do sistema, o sistema operacional é a primeira e mais importante linha de defesa. A conscientização sobre as ameaças e a correta configuração e utilização das funcionalidades de segurança disponíveis são cruciais tanto para administradores de sistemas quanto para usuários finais.

Referências

- Silberschatz, A., Galvin, P. B., & Gagne, G. (2018). *Operating System Concepts* (10th ed.). Wiley. (Capítulo sobre Segurança)
- Tanenbaum, A. S., & Bos, H. (2015). *Modern Operating Systems* (4th ed.). Pearson Education. (Capítulo sobre Segurança)
- Stallings, W. (2018). *Operating Systems: Internals and Design Principles* (9th ed.). Pearson. (Capítulos sobre Segurança do Computador)
- Garfinkel, S., & Spafford, G. (2003). *Practical Unix & Internet Security* (3rd ed.). O'Reilly Media.
- Russinovich, M. E., Solomon, D. A., & Ionescu, A. (2017). *Windows Internals, Part 1 & 2* (7th ed.). Microsoft Press. (Seções sobre mecanismos de segurança do Windows)
- National Institute of Standards and Technology (NIST). (Várias datas). *Special Publications (SP) on Cybersecurity*. Recuperado de https://csrc.nist.gov/publications/sp

foi elaborado para fins educativos e de referência, e todos os créditos foram devidamente atribuídos aos respectivos autores e fontes originais.

Qualquer utilização comercial ou distribuição do conteúdo aqui compilado deve ser feita com a devida autorização dos detentores dos direitos autorais originais. Os compiladores deste documento não assumem qualquer responsabilidade por eventuais violações de direitos autorais ou por quaisquer danos decorrentes do uso indevido das informações contidas neste documento.

Ao utilizar este documento, o usuário concorda em respeitar os direitos autorais dos autores originais e isenta os compiladores de qualquer responsabilidade relacionada ao conteúdo aqui apresentado.