SISTEMAS OPERACIONAIS

AULA 20 – SEGURANÇA DE SISTEMAS OPERACIONAIS

Prof.ª Sandra Cossul, Ma.

CONCEITOS BÁSICOS

- **Segurança de um sistema de computação**
  - Garantia de propriedades fundamentais associadas às informações e recursos do sistema

- **Informação –** todos os recursos disponíveis no sistema
  - Registros de banco de dados
  - Arquivos
  - Áreas de memória
  - Dados de E/S
  - Tráfego de rede
  - Configurações, etc.

CONCEITOS BÁSICOS

- A segurança de um sistema de computação pode ser expressa através de algumas propriedades fundamentais:
  - **Confidencialidade –** recursos do sistema só podem ser consultados por usuários autorizados
  - **Integridade –** recursos só podem ser modificados ou destruídos pelos usuários autorizados
  - **Disponibilidade –** recursos devem estar disponíveis aos usuários que tiverem direito de usá-los, a qualquer momento
  - **Autenticidade –** todas as entidades do sistema são autênticas (dados verdadeiros)
  - **Irretratabilidade –** todas as ações do sistema são conhecidas e não podem ser escondidas

PROTEÇÃO DO SO

- **Mecanismos de proteção**
  - É função do sistema operacional garantir a manutenção das propriedades de segurança para todos os recursos sob sua responsabilidade.

- Essas propriedades podem estar sujeitas a violações decorrentes de erros de software ou humanos, praticados por indivíduos mal intencionados, internos ou externos ao sistema.

PROTEÇÃO DO SO

- **Objetivos:**
  - Aumentar a confiabilidade de qualquer sistema que faça uso de recursos compartilhados
  - Impedir a violação maldosa e intencional de uma restrição de acesso por um usuário
  - Garantir que cada componente ativo no sistema utilize os recursos do sistema de forma consistente com as políticas estabelecidas

PRINCÍPIOS DE PROTEÇÃO

- **Princípio do privilégio mínimo –** determina que programas, usuários e sistemas recebam privilégios apenas suficientes para a execução de suas tarefas
  - Habilitação/desabilitação de serviços
  - O gerenciamento de usuários com o princípio do privilégio mínimo requer a criação de uma conta separada para cada usuário, apenas com os privilégios de que o usuário precisa
  - Ajuda a tornar o ambiente de computação mais seguro, minimizando os dados causados por erros ou ações maliciosas intencionais.

PRINCÍPIOS DE PROTEÇÃO

- **Separação de privilégios –** sistemas de proteção baseados em mais de um controle ou regra são mais robustos, pois se o atacante conseguir burlar um dos controles, mesmo assim não terá acesso ao recurso.
  - Autenticação de dois fatores

- **Mediação completa –** todos os acessos a recursos, tanto diretos quanto indiretos, devem ser verificados pelos mecanismos de segurança.

- **Default seguro –** o mecanismo de segurança deve identificar claramente os acessos permitidos e negar quando não permitido.

PRINCÍPIOS DE PROTEÇÃO

- **Economia de mecanismo -** o projeto de um sistema de proteção deve ser pequeno e simples, para que possa ser facilmente e profundamente analisado, testado e validado.

- **Compartilhamento mínimo -** mecanismos compartilhados entre usuários são fontes potenciais de problemas de segurança, devido à possibilidade de fluxos de informação imprevistos entre usuários.
  - Uso de mecanismos compartilhados deve ser minimizado

- **Facilidade de uso –** o uso dos mecanismos de segurança deve ser fácil e intuitivo, caso contrário eles serão evitados pelos usuários.

PRINCÍPIOS DE PROTEÇÃO

- **Projeto aberto –** o projeto do mecanismo de proteção deve ser público e aberto, dependendo somente do segredo de poucos itens, como listas de senhas ou chaves criptográficas.
  - torna possível a avaliação por terceiros independentes, provendo confirmação adicional da segurança do mecanismo.
  - Urnas eletrônicas

- **Proteção adequada –** cada recurso computacional deve ter um nível de proteção coerente com seu valor intrínseco.
  - nível de proteção de um servidor web de serviço bancário é bem distinto de um terminal público de acesso à internet

PRINCÍPIOS DE PROTEÇÃO

- **Eficiência –** os mecanismos de segurança devem ser eficientes no uso dos recursos computacionais, de forma a não afetar significativamente o desempenho do sistema ou as atividades de seus usuários.

- **Elo mais fraco -** a segurança do sistema é limitada pela segurança de seu elemento mais vulnerável, seja ele o SO, as aplicações, a conexão de rede ou o próprio usuário.

- **Esses princípios devem pautar a construção, configuração e operação de qualquer sistema computacional com requisitos de segurança.**
- **A imensa maioria dos problemas de segurança dos sistemas atuais provém da não observação desses princípios.**

DOMÍNIO DE PROTEÇÃO

- Os sistemas de computação contêm muitos **objetos**, e eles precisam ser protegidos contra a má utilização

- Os **objetos** podem ser de **hardware** (tais como memória, tempo de CPU e dispositivos de I/O) ou de **software** (tais como arquivos, programas e semáforos)

- Um processo deve ter permissão para acessar apenas os recursos para os quais ele tenha autorização e além disso, apenas os recursos de que precisa para executar sua tarefa.

ESTRUTURA DE DOMÍNIO

- Um processo opera dentro de um **domínio de proteção**, que especifica os recursos que ele pode acessar
- Cada domínio define um **conjunto de objetos e os tipos de operações** que podem ser invocadas sobre cada objeto

- A capacidade de executar uma operação sobre um objeto é o **direito de acesso**.
- **Domínio** – conjunto de direitos de acesso

ESTRUTURA DE DOMÍNIO

- Os **processos** são executados em **domínios** e podem usar qualquer um dos direitos de acesso do domínio para acessar e manipular objetos.

- Durante seu tempo de vida, um processo pode ficar limitado a um domínio de proteção ou ter **permissão para trocar de um domínio para outro**.

SEGURANÇA

- Segurança requer um sistema de proteção adequado e também a consideração do ambiente externo dentro do qual o sistema opera

- Garante a autenticação dos usuários do sistema para **proteger a integridade da informação** guardada no computador (programas e dados)

- Os recursos do computador devem ser protegidos contra **acesso não autorizado, destruição ou alteração maliciosa e introdução acidental de inconsistências.**

SEGURANÇA

- Dizemos que um sistema é **seguro** quando seus **recursos são usados e acessados como esperado** sob todas as circunstâncias

- **Violações** (ou a má utilização) da segurança do sistema podem ser categorizadas como **intencionais** (maliciosas) ou **acidentais**.

- **Ameaça** é a possibilidade de uma violação de segurança, tal como a descoberta de uma vulnerabilidade
- **Ataque** é a tentativa de violar a segurança.

NÍVEIS DE MEDIDAS DE SEGURANÇA

- **Físico –** os locais que contêm os sistemas de computação devem ser fisicamente protegidos contra a entrada não autorizada de pessoas. Isso inclui as salas dos computadores e todos os terminais de acesso
- **Humano -** A autorização deve ser feita cuidadosamente para assegurar que apenas usuários apropriados tenham acesso ao sistema.
- **SO -** O sistema deve proteger a si próprio contra brechas de segurança acidentais ou propositais.
- **Rede –** Os dados nos sistemas modernos são compartilhados via Internet, o que pode gerar ataques remotos.

AMEAÇAS – TIPOS DE VIOLAÇÕES ACIDENTAIS E MALICIOSAS DE SEGURANÇA

- **Brecha de sigilo/confidencialidade** – leitura não autorizada de dados ou roubo de informações sensíveis (números de cartão de crédito, senhas, e-mails privados, etc.)
- **Brecha de integridade –** modificação não autorizada de dados (alterar senhas, instalar programas, drivers), visando obter o controle do sistema, roubar informações ou impedir o acesso de outros usuários
- **Brecha de disponibilidade –** um usuário alocar para si todos os recursos do sistema, como a memória, o processador ou o espaço em disco, para impedir que outros usuários possam utilizá-lo.
- **Roubo de serviço –** uso não autorizado de recursos
- **Recusa de serviço –** envolve o impedimento do uso legítimo do sistema

AMEAÇAS DE PROGRAMAS

- **Malware –** software projetado para explorar, desabilitar ou danificar sistemas de computadores.
  - Ex.: cavalo de tróia, spyware, ransomware

- **Injeção de código –** código executável é adicionado ou modificado.
  - Ataque explora um bug no código e direciona o código após a interrupção

- **Vírus –** fragmento de código embutido em um programa legítimo
  - são autorreplicáveis e projetados para infectar outros programas
  - podem modificar ou destruir arquivos
  - se espalham pelo download de programas virais

AMEAÇAS DE SISTEMAS E REDES

- **Interceptação do tráfego da rede –** obtenção de informação útil sobre o conteúdo de uma sessão

- **Recusa de serviço -** não visam à obtenção de informações ou ao roubo de recursos, e sim à interrupção do uso legítimo de um sistema ou instalação

- **Varredura de portas -** não é um ataque e sim um meio de um cracker detectar as vulnerabilidades de um sistema para atacar

VULNERABILIDADES

- Uma vulnerabilidade é um **defeito ou problema presente na especificação**, **implementação, configuração ou operação de um software** ou sistema, que possa ser explorado para violar as propriedades de segurança do mesmo.

  - Erro de programação do serviço de compartilhamento de arquivos (não verificar a conformidade dos dados recebidos de um usuário ou da rede)

  - Uma conta de usuário sem senha, ou com uma senha predefinida pelo fabricante (vai permitir acesso não autorizado)

ATAQUES

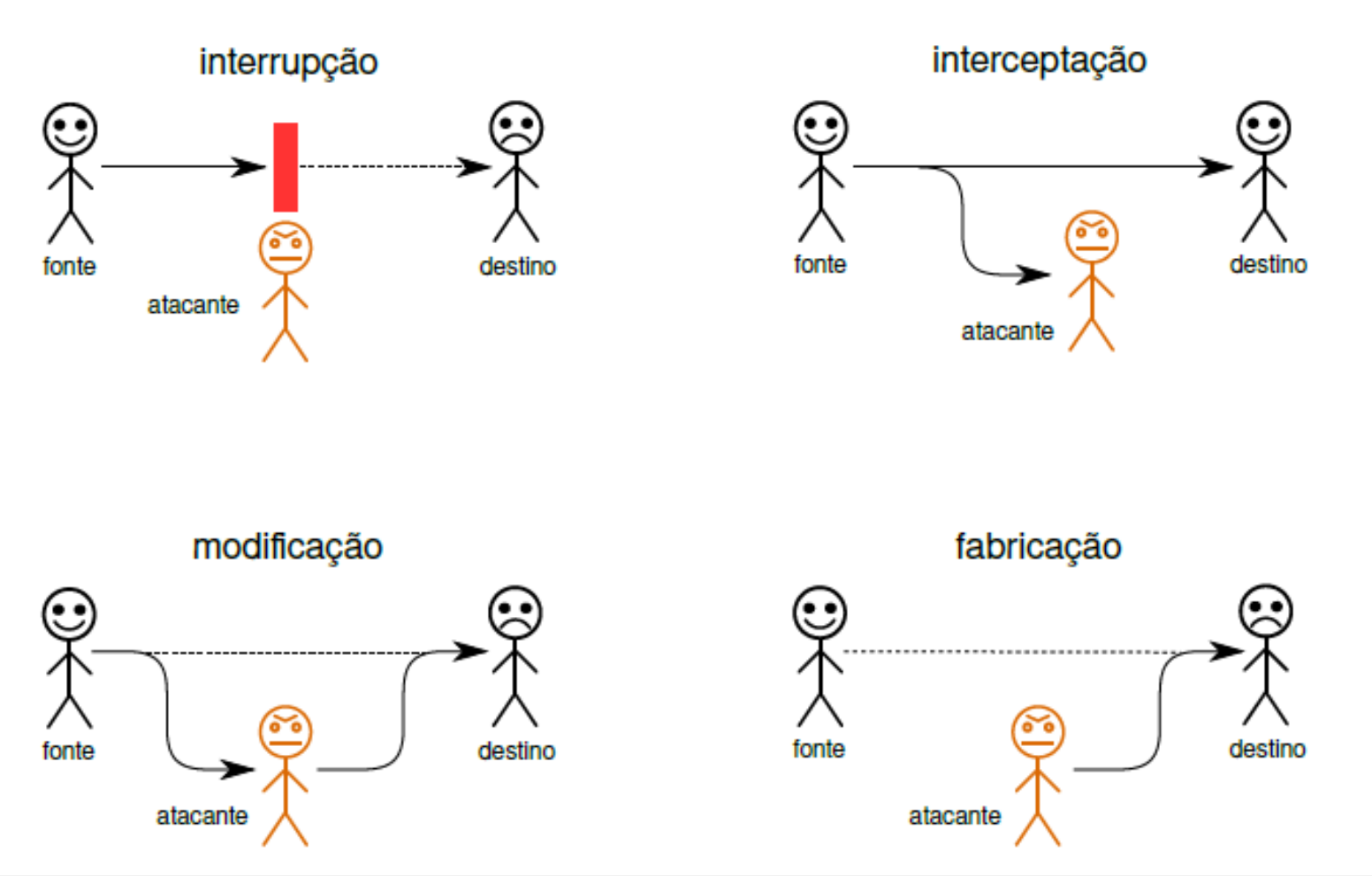
- Um ataque é o ato de **utilizar (ou explorar) uma vulnerabilidade** para **violar uma propriedade de segurança** do sistema

- **Interrupção –** impedir o fluxo normal das informações ou acessos (ataque à disponibilidade do sistema)
  - Ataques de negação de serviços (DoS – Denial of Service)
  - Comum em ambientes de rede (impedir o acesso a servidores)
  - No SO – objetivo de consumir todos os recursos locais (CPU, memória, arquivos, etc.)

ATAQUES

- **Interceptação –** obter acesso indevido a um fluxo de informações, sem necessariamente modificá-las (ataque à confidenciabilidade)
  - spywares
- **Modificação –** modificar de forma indevida informações ou partes do sistema, violando sua integridade
- **Fabricação –** produzir informações falsas ou introduzir módulos ou componentes maliciosos no sistema (ataque à autenticidade)

ATAQUES


interrupção
fonte
atacante
destino
interceptação
fonte
atacante
destino
modificação
fonte
atacante
destino
fabricação
fonte
atacante
destino

ATAQUES

- **Passivos –** visam capturar informações confidenciais
- **Ativos –** visam introduzir modificações no sistema para beneficiar o atacante ou impedir seu uso pelos usuários válidos

- **Locais –** quando executados por usuários válidos do sistema
- **Remotos –** realizados através da rede, sem fazer uso de uma conta de usuário local

- **Um programa especialmente construído para explorar uma determinada vulnerabilidade de sistema e realizar um ataque é denominado exploit.**

ATAQUES

- **Intrusão/Invasão –** ataque bem sucedido, que dá ao atacante acesso indevido a um sistema
  - Enviar spam
  - Atacar outros sistemas
  - Minerar moedas digitais

- **Elevação de privilégio –** intruso executa novos ataques para aumentar seu nível de acesso no sistema
  - Exploram vulnerabilidades em programas do sistema (que executam com mais privilégio) ou do próprio núcleo, através de chamadas de sistema, para alcançar os privilégios do administrador

MALWARES

- Denomina-se genericamente malware **todo programa cuja intenção é realizar atividades ilícitas**, como realizar ataques, roubar informações ou dissimular a presença de intrusos em um sistema.

TIPOS DE MALWARES

- **Vírus -** trecho de código que se infiltra em programas executáveis existentes no SO, usando-os como suporte para sua execução e replicação
  - Quando um programa "infectado" é executado, o vírus também se executa, infectando outros executáveis e eventualmente executando outras ações danosas.

- **Worm -** um "verme" é um programa autônomo, que se propaga sem infectar outros programas.
  - A maioria dos vermes se propaga explorando vulnerabilidades nos serviços de rede, que os permitam invadir e instalar-se em sistemas remotos.

TIPOS DE MALWARES

- **Trojan horse –** um "cavalo de Tróia" computacional é um programa com duas funcionalidades: uma funcionalidade lícita conhecida de seu usuário e outra ilícita, executada sem que o usuário a perceba.
  - Muitos cavalos de Tróia são usados como vetores para a instalação de outros malwares. Uso de engenharia social.

- **Exploit -** é um programa escrito para explorar vulnerabilidades conhecidas, como prova de conceito ou como parte de um ataque
  - São disseminados sem a necessidade da ação de um usuário

TIPOS DE MALWARES

- **Packet sniffer –** um "farejador de pacotes" captura pacotes de rede do próprio computador ou da rede local, analisando-os em busca de informações sensíveis como senhas e dados bancários.
  - Criptografia resolve parcialmente esse problema: no entanto, a captura de dados pode acontecer antes da criptografia ou depois de descriptografar

- **Keylogger -** software dedicado a capturar e analisar as informações digitadas pelo usuário na máquina local, sem seu conhecimento.
  - Essas informações podem ser transferidas a um computador remoto periodicamente ou em tempo real, através da rede.

TIPOS DE MALWARES

- **Rootkit –** conjunto de programas destinado a ocultar a presença de um intruso no sistema operacional.
  - Como princípio de funcionamento, o rootkit modifica os mecanismos do SO que mostram os processos em execução, arquivos nos discos, portas e conexões de rede, etc., para ocultar o intruso.
  - Detecção e remoção complexa

- **Backdoor -** um "porta dos fundos" é um programa que facilita a entrada posterior do atacante em um sistema já invadido.
  - Geralmente a porta dos fundos é criada através um processo servidor de conexões remotas (usando SSH, telnet ou um protocolo ad-hoc).
  - Muitos backdoors são instalados a partir de trojans, vermes ou rootkits.

TIPOS DE MALWARES

- **Ransomware** – categoria recente de malware, que visa sequestrar os dados do usuário.
  - O sequestro é realizado cifrando os arquivos do usuário com uma chave secreta, que só será fornecida pelo atacante ao usuário se este pagar um valor de resgate.
  - Pagamento normalmente exigido em criptomoedas
  - Uma forma de se proteger é manter backup dos dados

ATAQUES RECENTES DE RANSOMWARE

- **Ataque ao Colonial Pipeline**: Em maio de 2021, a Colonial Pipeline, uma importante rede de oleodutos que fornece combustível para grande parte da costa leste dos Estados Unidos, foi atingida por um ataque de ransomware. O ataque interrompeu as operações da empresa por vários dias, levando a escassez de combustível e aumentos de preços.

- **Ataque ao JBS:** Em junho de 2021, a JBS, uma das maiores empresas de processamento de carne do mundo, sofreu um ataque de ransomware que forçou o fechamento temporário de suas operações em todo o mundo.

- **Ataque à CNA Financial:** Em março de 2021, a CNA Financial, uma grande seguradora dos Estados Unidos, foi atingida por um ataque de ransomware que levou à interrupção de seus sistemas por vários dias.

- **Ataque à Universidade de Vermont Health Network**: Em outubro de 2020, a rede de saúde da Universidade de Vermont foi atingida por um ataque de ransomware que levou à interrupção de suas operações por várias semanas.

- **Ataque ao Grupo Fleury:** Em junho de 2021, o Grupo Fleury, uma das maiores empresas de diagnóstico médico do Brasil, foi atingido por um ataque de ransomware que afetou seus sistemas de tecnologia da informação.

- **Ataque a lojas Renner**: Em agosto de 2021, um ataque de ransomware afetou os sistemas da empresa, interrompendo as operações de lojas físicas, online e de atendimento ao cliente em todo o país.

IMPLEMENTANDO DEFESAS DE SEGURANÇA

- O SO emprega várias técnicas complementares para garantir a segurança, divididas em áreas:
  1. **Autenticação**
  2. **Controle de acesso**
  3. **Auditoria**

1. AUTENTICAÇÃO DE USUÁRIOS

- Como determinar se uma identidade de usuário é autêntica?
  - **Posse de algo** (chave ou cartão) por parte do usuário
  - **Conhecimento de algo** (identificador e uma senha) pelo usuário
  - **Atributo do usuário** (impressão digital, assinatura, etc)

2. CONTROLE DE ACESSO

- Técnicas usadas para definir quais ações são permitidas e quais são negadas no sistema

- Para cada usuário do sistema devem ser definidas regras descrevendo as ações que este pode realizar no sistema, ou seja, que recursos este pode acessar e sob que condições

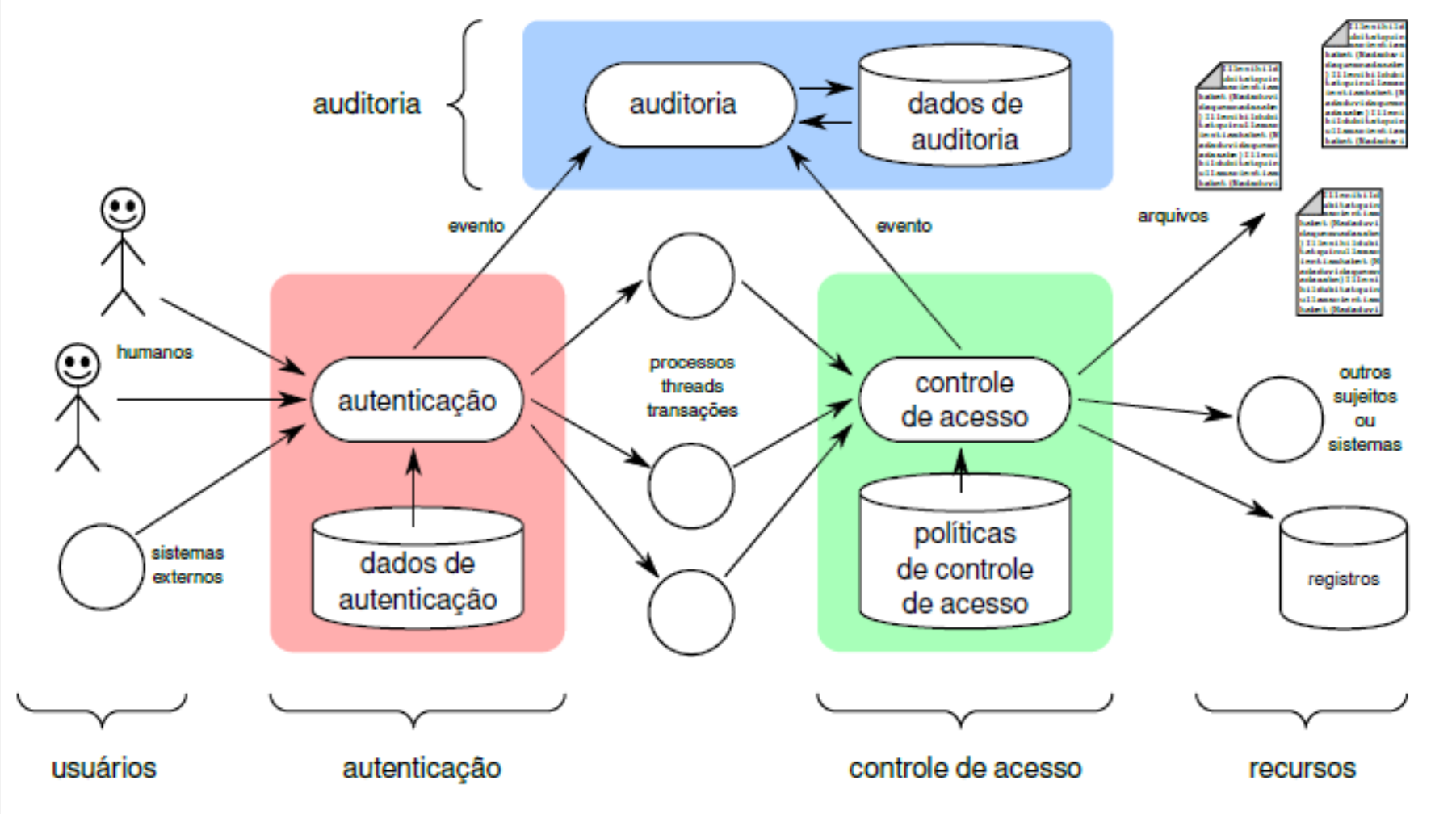
- **Política de controle de acesso –** imposta a todos os acessos que os usuários efetuam sobre os recursos do sistema

3. AUDITORIA

- Técnicas usadas para manter um registro das atividades efetuadas no sistema, visando a contabilização de uso dos recursos

- A análise posterior de situações de uso indevido ou a identificação de comportamentos suspeitos.

IMPLEMENTANDO DEFESAS DE SEGURANÇA



IMPLEMENTANDO DEFESAS DE SEGURANÇA

- **Política de segurança –** define o que está sendo protegido e o nível de segurança

- **Avaliação de vulnerabilidades –** avaliação de riscos tenta determinar as chances de um incidente de segurança verificando alguns aspectos do sistema (senhas, programas não autorizados, processos de execução longa, etc.)

- **Detecção de invasões -** empenha-se em detectar invasões tentadas ou bem-sucedidas nos sistemas de computação e em iniciar respostas apropriadas aos intrusos

IMPLEMENTANDO DEFESAS DE SEGURANÇA

- **Proteção contra vírus –** uso de programas anti-vírus
  - funcionam inspecionando todos os programas em um sistema em busca de um padrão específico de instruções conhecido por compor o vírus
  - possuem catálogos com milhares de vírus

- **Auditoria, contabilização e registro em log**
  - todas as execuções de chamadas de sistema podem ser registradas em log para análise do comportamento (ou mau comportamento) do programa.
  - O mais comum é que eventos suspeitos sejam registrados em log. Falhas de autenticação e falhas de autorização podem nos dizer muita coisa sobre tentativas de invasão.

CRIPTOGRAFIA COMO UMA FERRAMENTA DE SEGURANÇA

- A **criptografia** é usada para restringir os emissores e/ou receptores potenciais de uma mensagem.

- Baseia-se em dados secretos chamados **chaves** que são distribuídos seletivamente aos computadores em uma rede e usados para processar mensagens.

CRIPTOGRAFIA COMO UMA FERRAMENTA DE SEGURANÇA

- A criptografia habilita o receptor de uma mensagem a verificar se a mensagem foi criada por algum computador que possua determinada chave.

- Da mesma forma, um emissor pode codificar sua mensagem para que somente um computador com determinada chave possa decodificá-la.

- As chaves são projetadas para que não seja computacionalmente factível derivá-las a partir das mensagens geradas com o seu uso ou a partir de qualquer outra informação pública.

FIREWALL

- Um **firewall** pode ser utilizado para proteger sistemas e redes
- É um computador, um equipamento ou roteador que se posiciona entre o que é confiável e o que não é confiável

- Um **firewall de rede** limita o acesso à rede entre os dois domínios de segurança além de monitorar e registrar todas as conexões em log

- Ele também pode limitar conexões com base no endereço de origem ou destino, na porta de origem ou destino ou na direção da conexão.

FIREWALL

- O firewall pode ser **implementado tanto em software quanto em hardware** e pode usar várias técnicas, como filtragem de pacotes, inspeção de estado, listas de controle de acesso e outros métodos para permitir ou bloquear o tráfego de rede.

- Ele é uma parte fundamental da **segurança de rede** e é frequentemente usado em conjunto com outras soluções de segurança para proteger as redes de computadores contra ameaças cibernéticas.

BIBLIOGRAFIA

- Tanenbaum, A. S. **Sistemas Operacionais Modernos.** Pearson Prentice Hall. 3rd Ed., 2009.
- Silberschatz, A; Galvin, P. B.; Gagne G.; **Fundamentos de Sistemas Operacionais.** LTC. 9th Ed., 2015.
- Stallings, W.; **Operating Systems: Internals and Design Principles**. Prentice Hall. 5th Ed., 2005.
- Oliveira, Rômulo, S. et al. **Sistemas Operacionais** - V11 - UFRGS. Disponível em: Minha Biblioteca, Grupo A, 2010.