**UNIVERSIDADE SÃO JUDAS TADEU – USJT**

**SISTEMAS COMPUTACIONAIS E SEGURANÇA**

VICTOR GONÇALVES VOLPI

**Segurança em Sistemas Computacionais**

"Explorando as Aplicações Práticas de Proteção de Dados e Infraestruturas Digitais”

SÃO PAULO – SP

2025

**Criptografia e Proteção de Dados**

A **criptografia** é uma técnica fundamental no campo da segurança computacional, usada para proteger informações sensíveis. Ela transforma dados legíveis em um formato cifrado, que só pode ser revertido para seu formato original por quem possui a chave de descriptografia.

**Exemplo**: Em sites de banco online ou lojas na internet, quando você faz uma compra e insere o número do seu cartão de crédito, por exemplo.

**Criptografia simétrica**: Utiliza uma chave única tanto para criptografar quanto para descriptografar os dados. O grande desafio aqui é garantir que a chave seja compartilhada de forma segura entre as partes envolvidas.

**Criptografia assimétrica**: Usa duas chaves: uma pública e uma privada. A chave pública é usada para criptografar os dados e a chave privada para descriptografá-los. Isso torna a criptografia assimétrica muito útil para ambientes como o de serviços bancários, onde a chave pública pode ser compartilhada sem comprometer a segurança dos dados.

**Explicação**: A criptografia é como uma "sela" que "tranca" suas informações, como senhas ou dados bancários, enquanto elas viajam pela internet. Isso evita que hackers possam ver ou roubar esses dados. É o que garante que suas informações fiquem seguras quando você está navegando na web.

**Autenticação e Controle de Acesso**

A **autenticação** é o processo de verificar a identidade de um usuário ou sistema, enquanto o **controle de acesso** define o que esses usuários ou sistemas podem fazer depois de serem autenticados. Ambas as técnicas são essenciais para garantir que somente pessoas autorizadas tenham acesso a dados e recursos sensíveis.

**Exemplo**: Quando você faz login no seu e-mail, nas redes sociais ou em sistemas da sua empresa.

**Autenticação por senha**: É o método mais tradicional, mas não é mais considerado totalmente seguro, pois senhas fracas podem ser facilmente comprometidas.

**Autenticação multifatorial (MFA)**: Adiciona uma camada extra de segurança ao exigir que o usuário forneça mais de uma prova de identidade. Isso pode incluir algo que o usuário sabe (a senha), algo que o usuário tem (um token gerado por um aplicativo ou enviado via SMS) ou algo que o usuário é (como impressão digital ou reconhecimento facial).

**Autenticação biométrica**: Tecnologias de autenticação biométrica, como o uso de impressões digitais, reconhecimento facial ou íris, estão se tornando cada vez mais comuns, especialmente em dispositivos móveis.

**Identidade do usuário**: Atribuição de permissões específicas com base no

Usuário (ex: "João pode acessar documentos financeiros").

**Função do usuário**: Controle de acesso baseado em papéis (ex: "Todos os gerentes têm acesso ao sistema financeiro").

**Atributos de segurança**: Controle de acesso mais dinâmico, considerando características do ambiente, como localização geográfica ou horário de acesso.

**Explicação**: Autenticação é o processo de garantir que você é realmente quem diz ser. Pode ser feito apenas com sua senha, mas hoje em dia também pode pedir mais, como um código enviado para o seu celular ou até reconhecimento facial. O controle de acesso, por sua vez, define o que você pode ou não fazer dentro de um sistema, como acessar certos arquivos ou configurações.

**Análise de Vulnerabilidades e Testes de Penetração**

A **análise de vulnerabilidades** envolve a identificação de falhas de segurança em um sistema ou rede, enquanto os **testes de penetração** são realizados para simular ataques reais, a fim de avaliar a resistência do sistema a invasões.

**Exemplo**: Empresas de tecnologia, como Google e bancos, fazem "testes" para garantir que seus sistemas não têm brechas que possam ser exploradas por hackers.

**Testes de Penetração (Pentesting):**

O pentesting simula ataques cibernéticos para testar como um sistema reagiria a uma invasão real. Isso pode ser feito de maneira "caixa-preta", onde os testadores não sabem nada sobre o sistema, ou "caixa-branca", onde eles têm total acesso às informações do sistema.

Exemplo de pentest: Um "hacker ético" pode tentar explorar falhas em um site para roubar informações de usuários ou obter acesso a dados confidenciais.

**Impacto da Análise e Testes de Penetração**: Essas técnicas são cruciais para descobrir vulnerabilidades antes que criminosos possam explorá-las. Ao realizar testes de penetração e análises de vulnerabilidades, as organizações podem proteger seus dados e sistemas contra-ataques, melhorar a confiança do cliente e cumprir com regulamentações de segurança, como o GDPR.

**Explicação**: A análise de vulnerabilidades é como um "check-up" nos sistemas, procurando por falhas de segurança. Já os testes de penetração são como se fossem "hackers éticos" tentando invadir o sistema para ver se conseguem encontrar esses pontos fracos. O objetivo é corrigir essas falhas antes que alguém mal-intencionado as descubra.

**Firewall e Proteção de Redes**

O **firewall** é uma barreira de segurança projetada para monitorar e controlar o tráfego de dados entre redes, como a internet e uma rede corporativa interna. Seu objetivo é bloquear tráfego malicioso e permitir o tráfego legítimo.

**Exemplo**: Em empresas, o firewall é como um "porteiro" que decide o que pode ou não entrar na rede interna.

**Aplicação: Empresas e Redes Corporativas**

Em empresas, o firewall é uma ferramenta essencial para proteger a rede interna contra acessos não autorizados da internet. Ele age como um "porteiro", decidindo quais dados podem entrar e sair da rede com base em regras predefinidas.

**Funcionamento do Firewall:**

**Firewall de filtragem de pacotes**: Analisa os pacotes de dados individuais que entram e saem da rede e verifica se eles atendem às regras de segurança.

**Firewall de aplicação**: Atua na camada de aplicação e filtra o tráfego com base em protocolos de aplicativos, como HTTP, FTP, ou DNS.

**Firewall de próxima geração (NGFW)**: Combina as funcionalidades dos firewalls tradicionais com outras ferramentas de segurança, como inspeção profunda de pacotes (DPI), prevenção de intrusão (IPS) e filtragem de aplicativos.

**Impacto do Firewall**: O firewall é uma camada de defesa essencial contra-ataques como invasões externas e tentativas de sobrecarga de servidores (ataques DDoS). Ele ajuda a minimizar o risco de acessos não autorizados e a proteger dados confidenciais dentro das organizações.

**Explicação**: O firewall é uma barreira que controla o tráfego de dados entre a internet e a rede interna de uma empresa. Ele impede que informações indesejadas ou maliciosas entrem na rede e possa bloquear ataques, como aqueles que tentam sobrecarregar o sistema, impedindo que os serviços funcionem corretamente.

**Sistemas de Detecção de Intrusão (IDS)**

Um **Sistema de Detecção de Intrusão (IDS)** é projetado para monitorar redes e sistemas em busca de atividades suspeitas ou maliciosas. Ele identifica comportamentos anômalos que possam indicar que um sistema foi comprometido por um invasor.

**Exemplo**: Empresas usam sistemas de monitoramento para ficar de olho em qualquer movimento suspeito em suas redes, como se fossem câmeras de segurança para a internet.

**Aplicação: Monitoramento de Redes Corporativas**

Em grandes organizações, onde várias conexões e dados estão em constante movimento, um IDS é fundamental para identificar e responder a ameaças cibernéticas em tempo real. Esses sistemas ajudam as equipes de segurança a detectar ataques rapidamente, como tentativas de invasão ou roubo de dados.

**Tipos de IDS:**

**IDS baseado em rede (NIDS)**: Monitora o tráfego de rede em busca de sinais de intrusão, como pacotes de dados anômalos ou padrões de tráfego que indiquem um ataque.

**IDS baseado em host (HIDS)**: Monitora atividades em um único computador ou servidor, procurando por comportamentos incomuns, como tentativas de acesso não autorizado a arquivos ou configurações.

**IDS em grandes empresas**: Uma empresa de telecomunicações pode usar um IDS para monitorar todas as conexões em sua rede e detectar atividades suspeitas, como um número excessivo de tentativas de login falhadas.

**IDS em sistemas de segurança pública**: Organizações governamentais podem usar IDS para proteger dados sensíveis relacionados à segurança nacional, detectando qualquer tráfego incomum ou invasões

**Impacto dos IDS**: O uso de IDS permite uma resposta rápida a ataques, mitigando os danos potenciais. Ao detectar intrusões em tempo real, esses sistemas ajudam a proteger informações sensíveis e a garantir a continuidade dos serviços.

**Explicação**: O IDS é como um alarme que dispara quando algo fora do comum acontece. Ele fica "observando" tudo o que acontece na rede e, se detectar algo estranho, avisa os responsáveis para que eles possam investigar e evitar problemas maiores, como invasões ou roubos de dados.

VICTOR GONÇALVES VOLPI

**Segurança em Sistemas Computacionais**

“Explorando as Aplicações Práticas de Proteção de Dados e Infraestruturas Digitais”

Trabalho apresentado a Universidade São Judas Tadeu – USJT como requisito para conclusão do trabalho de Sistemas Computacionais e Segurança

Orientador: Prof. Robson Calvetti

SÃO PAULO - SP

2025