Segurança e Auditoria de Sistemas

Fundamentos e Segurança para SI

Prof. Flávio Murilo de Carvalho Leal
Centro Universitário Paraíso

Definição

Requisitos de segurança são especificações técnicas e organizacionais que definem como um sistema deve proteger ativos informacionais contra ameaças internas e externas.

Importante

Segurança não é um recurso adicional — é requisito não funcional essencial.

Escopo da Aula

- Segurança em aplicações
- Segurança em bases de dados
- Segurança em comunicações
- Segurança de dispositivos físicos e móveis
- ~~Estruturação de check-lists técnicos~~

Requisitos Funcionais

Descrevem o que o sistema faz.

Requisitos Não Funcionais

Descrevem como o sistema opera (desempenho, escalabilidade, segurança).

Segurança

Segurança é tipicamente classificada como requisito não funcional, mas impacta diretamente o desenho arquitetural.

Principais Vetores de Ataque em Aplicações

- Injeção (SQL, NoSQL, LDAP)
- Cross-Site Scripting (XSS)
- Cross-Site Request Forgery (CSRF)
- Broken Authentication
- Controle de acesso inadequado
- Desserialização insegura
- Upload de arquivos maliciosos

1. Autenticação
   - Políticas de senha
   - MFA
   - Bloqueio por tentativas
2. Autorização
   - RBAC
   - ABAC
   - Princípio do menor privilégio

Boas Práticas

- Validação no cliente e no servidor
- Uso de prepared statements
- Sanitização
- Whitelisting ao invés de blacklisting

Erro comum

Confiar apenas na validação do front-end.

Requisitos Técnicos

- Uso de hash forte (bcrypt, Argon2)
- Uso de salt
- Não utilizar SHA1 ou MD5
- Não armazenar senha em texto puro

Requisitos

- Registro de eventos críticos
- Logs protegidos contra alteração
- Correlação de eventos
- Monitoramento contínuo

- SQL Injection
- Credenciais fracas
- Exposição direta à internet
- Backup desprotegido
- Falta de criptografia

Controle de Acesso

- Usuários com permissões mínimas
- Separação entre usuário de aplicação e administrador
- Revogação periódica de privilégios

Em Repouso

- TDE (Transparent Data Encryption)
- Criptografia de disco

Em Trânsito

- TLS
- Certificados válidos

Requisitos

- Backup criptografado
- Teste de restauração
- Armazenamento segregado
- Controle de acesso ao arquivo de backup

- Man-in-the-Middle
- Sniffing
- Replay Attack
- DNS Spoofing

Web
HTTPS (TLS 1.2+)

E-mail
SPF, DKIM, DMARC

VPN
IPSec, OpenVPN

Configurações Técnicas Importantes

- Desativar SSL antigo
- Desabilitar TLS 1.0/1.1
- Certificados válidos
- HSTS
- Perfect Forward Secrecy

- Furto
- Acesso físico não autorizado
- Malware móvel
- Engenharia social

Configurações Essenciais

- Criptografia de disco
- Bloqueio automático
- Senha forte ou biometria
- Atualizações automáticas

Funcionalidades

- Controle remoto
- Apagamento remoto
- Políticas obrigatórias
- Controle de aplicativos

Camadas de Segurança

- Hardware (Secure Enclave / Trusted Execution Environment)
- Sistema Operacional
- Camada de Aplicação
- Rede e Comunicação
- Gestão Corporativa (MDM)

Princípio

A segurança móvel é baseada em defesa em profundidade (Defense in Depth).

Aspecto	Android	iOS
Modelo	Mais aberto	Ecossistema fechado
Instalação de Apps	Play Store + fontes externas	App Store (restrito)
Customização	Alta	Limitada
Fragmentação	Alta	Baixa
Controle do Fabricante	Variável	Centralizado (Apple)

Camada	Android	iOS
Isolamento de Apps	Sandbox por UID	Sandbox rígido
Execução Segura	TEE (Trusted Execution Env.)	Secure Enclave
Boot Seguro	Verified Boot	Secure Boot Chain
Root/Jailbreak	Root possível	Jailbreak restrito

Observação

Ambos utilizam sandboxing, mas o iOS possui controle mais centralizado de integridade.

Android

- Depende do fabricante
- Fragmentação de versões
- Patch variável por modelo

iOS

- Atualização centralizada
- Alta taxa de adoção rápida
- Correções distribuídas simultaneamente

Aspecto	Android	iOS
Permissões em tempo de execução	Sim	Sim
Granularidade	Alta	Alta
Controle de rastreamento	Limitado	App Tracking Transparency
Instalação fora da loja	Permitida	Não permitida (oficialmente)

Android

- File-Based Encryption
- Full Disk Encryption (versões antigas)
- Armazenamento protegido via Keystore

iOS

- Criptografia automática por padrão
- Proteção vinculada ao código de desbloqueio
- Chaves armazenadas na Secure Enclave

- Mistura de dados pessoais e corporativos
- Vazamento via aplicativos não confiáveis
- Backup automático em nuvem pessoal
- Jailbreak ou Root
- Conexões Wi-Fi inseguras

Impacto

Comprometimento de dados corporativos sensíveis.

Políticas Técnicas

- Criptografia obrigatória
- Bloqueio automático 5 minutos
- MFA para acesso corporativo
- Proibição de root/jailbreak
- VPN obrigatória fora da rede interna

Android vs iOS – Perspectiva Corporativa

Critério	Android	iOS
Controle Centralizado	Médio	Alto
Fragmentação	Alta	Baixa
Gerenciamento MDM	Amplo suporte	Forte integração nativa
Risco de Modificação	Maior (root)	Menor (jailbreak raro)
Padronização Corporativa	Mais difícil	Mais simples

Não existe sistema invulnerável

- Android oferece maior flexibilidade
- iOS oferece maior controle centralizado
- Segurança depende de:
  - Configuração
  - Política corporativa
  - Atualizações
  - Conscientização do usuário

Definição

Ferramenta estruturada de verificação sistemática de conformidade com requisitos previamente definidos.

Função

Reduz falhas humanas, padroniza auditorias e garante cobertura mínima.

Características de um Bom Check-list

- Objetivo
- Mensurável
- Baseado em norma (ISO 27001, OWASP)
- Adaptado ao contexto
- Versionado

Modelo Estrutural

- Identificação do sistema
- Categoria (Aplicação, BD, Rede, Dispositivo)
- Requisito avaliado
- Evidência coletada
- Status (Conforme/Não Conforme)
- Risco associado
- Responsável

Exemplo – Check-list para Aplicação Web

Item	Status	Evidência
Senha com hash forte		
Prepared Statements		
HTTPS obrigatório		
Controle de sessão		
Logs ativos		

Exemplo – Check-list para Banco

Item	Status	Evidência
Usuário com privilégio mínimo		
Backup criptografado		
TLS ativo		
Auditoria habilitada		

- Uso em auditorias internas
- Uso em revisão de código
- Uso antes de deploy
- Uso em homologação
- Uso periódico em produção

Síntese

- Segurança deve ser requisito desde a concepção
- Aplicações, bancos e comunicações precisam de controles específicos
- Dispositivos físicos são ponto crítico
- Check-lists operacionalizam a governança de segurança