
# 3.0 Security Engineering and Cryptography

## 3.1 Given a scenario, apply secure configurations to enterprise mobility.

- **Managed configurations**
  - Application control
  - Password
  - MFA requirements
  - Token-based access
  - Patch repository
  - Firmware Over-the-Air
  - Remote wipe
  - WiFi
    - WiFi Protected Access (WPA2/3)
    - Device certificates
  - Profiles
  - Bluetooth
  - Near-field communication (NFC)
  - Peripherals
  - Geofencing
  - VPN settings
  - Geotagging
  - Certificate management
  - Full device encryption
  - Tethering
  - Airplane mode
  - Location services
  - DNS over HTTPS (DoH)
  - Custom DNS
- **Deployment scenarios**
  - Bring your own device (BYOD)
  - Corporate-owned
  - Corporate owned, personally enabled (COPE)
  - Choose your own device (CYOD)
- **Security considerations**
  - Unauthorized remote activation/ deactivation of devices or features
  - Encrypted and unencrypted communication concerns
  - Physical reconnaissance
  - Personal data theft
  - Health privacy
  - Implications of wearable devices
  - Digital forensics of collected data
  - Unauthorized application stores
  - Jailbreaking/rooting
  - Side loading
  - Containerization
  - Original equipment manufacturer (OEM) and carrier differences
  - Supply chain issues
  - eFuse

## 3.2 Given a scenario, configure and implement endpoint security controls.

- **Hardening techniques**
  - Removing unneeded services
  - Disabling unused accounts
  - Images/templates
  - Remove end-of-life devices
  - Remove end-of-support devices
  - Local drive encryption
  - Enable no execute (NX)/ execute never (XN) bit
  - Disabling central processing unit (CPU) virtualization support
  - Secure encrypted enclaves/ memory encryption
  - Shell restrictions
  - Address space layout randomization (ASLR)
- **Processes**
  - Patching
    - Firmware
    - Application
  - Logging
  - Monitoring
- **Mandatory access control**
  - Security-Enhanced Linux (SELinux)/ Security-Enhanced Android (SEAndroid)
  - Kernel vs. middleware
- **Trustworthy computing**
  - Trusted Platform Module (TPM)
  - Secure Boot
  - Unified Extensible Firmware Interface (UEFI)/basic input/ output system (BIOS) protection
  - Attestation services
  - Hardware security module (HSM)
  - Measured boot
  - Self-encrypting drives (SEDs)
- **Compensating controls**
  - Antivirus
  - Application controls
  - Host-based intrusion detection system (HIDS)/Host-based intrusion prevention system (HIPS)
  - Host-based firewall
  - Endpoint detection and response (EDR)
  - Redundant hardware
  - Self-healing hardware
  - User and entity behavior analytics (UEBA)

## 3.3 Explain security considerations impacting specific sectors and operational technologies.

- **Embedded**
  - Internet of Things (IoT)
  - System on a chip (SoC)
  - Application-specific integrated circuit (ASIC)
  - Field-programmable gate array (FPGA)
- **ICS/supervisory control and data acquisition (SCADA)**
  - Programmable logic controller (PLC)
  - Historian
  - Ladder logic
  - Safety instrumented system
  - Heating, ventilation, and air conditioning (HVAC)
- **Protocols**
  - Controller Area Network (CAN) bus
  - Modbus
  - Distributed Network Protocol 3 (DNP3)
  - Zigbee
  - Common Industrial Protocol (CIP)
  - Data distribution service
- **Sectors**
  - Energy
  - Manufacturing
  - Healthcare
  - Public utilities
  - Public services
  - Facility services

## 3.4 Explain how cloud technology adoption impacts organizational security.

- **Automation and orchestration**
- **Encryption configuration**
- **Logs**
  - Availability
  - Collection
  - Monitoring
  - Configuration
  - Alerting
- **Monitoring configurations**
- **Key ownership and location**
- **Key life-cycle management**
- **Backup and recovery methods**
  - Cloud as business continuity and disaster recovery (BCDR)
  - Primary provider BCDR
  - Alternative provider BCDR
- **Infrastructure vs. serverless computing**
- **Application virtualization**
- **Software-defined networking**
- **Misconfigurations**
- **Collaboration tools**
- **Storage configurations**
  - Bit splitting
  - Data dispersion
- **Cloud access security broker (CASB)**

## 3.5 Given a business requirement, implement the appropriate PKI solution.

- **PKI hierarchy**
  - Certificate authority (CA)
  - Subordinate/intermediate CA
  - Registration authority (RA)
- **Certificate types**
  - Wildcard certificate
  - Extended validation
  - Multidomain
  - General purpose
- **Certificate usages/profiles/templates**
  - Client authentication
  - Server authentication
  - Digital signatures
  - Code signing
- **Extensions**
  - Common name (CN)
  - Subject alternate name (SAN)
- **Trusted providers**
- **Trust model**
- **Cross-certification**
- **Configure profiles**
- **Life-cycle management**
- **Public and private keys**
- **Digital signature**
- **Certificate pinning**
- **Certificate stapling**
- **Certificate signing requests (CSRs)**
- **Online Certificate Status Protocol (OCSP) vs. certificate revocation list (CRL)**
- **HTTP Strict Transport Security (HSTS)**

## 3.6 Given a business requirement, implement the appropriate cryptographic protocols and algorithms.

- **Hashing**
  - Secure Hashing Algorithm (SHA)
  - Hash-based message authentication code (HMAC)
  - Message digest (MD)
  - RACE integrity primitives evaluation message digest (RIPEMD)
  - Poly1305
- **Symmetric algorithms**
  - Modes of operation
    - Galois/Counter Mode (GCM)
    - Electronic codebook (ECB)
    - Cipher block chaining (CBC)
    - Counter (CTR)
    - Output feedback (OFB)
  - Stream and block
    - Advanced Encryption Standard (AES)
    - Triple digital encryption standard (3DES)
    - ChaCha
    - Salsa20
- **Asymmetric algorithms**
  - Key agreement
    - Diffie-Hellman
    - Elliptic-curve Diffie-Hellman (ECDH)
  - Signing
    - Digital signature algorithm (DSA)
    - Rivest, Shamir, and Adleman (RSA)
    - Elliptic-curve digital signature algorithm (ECDSA)
- **Protocols**
  - Secure Sockets Layer (SSL)/ Transport Layer Security (TLS)
  - Secure/Multipurpose Internet Mail Extensions (S/MIME)
  - Internet Protocol Security (IPSec)
  - Secure Shell (SSH)
  - EAP
- **Elliptic curve cryptography**
  - P256
  - P384
- **Forward secrecy**
- **Authenticated encryption with associated data**
- **Key stretching**
  - Password-based key derivation function 2 (PBKDF2)
  - Bcrypt

## 3.7 Given a scenario, troubleshoot issues with cryptographic implementations.

- **Implementation and configuration issues**
  - Validity dates
  - Wrong certificate type
  - Revoked certificates
  - Incorrect name
  - Chain issues
    - Invalid root or intermediate CAs
    - Self-signed
  - Weak signing algorithm
  - Weak cipher suite
  - Incorrect permissions
  - Cipher mismatches
  - Downgrade
- **Keys**
  - Mismatched
  - Improper key handling
  - Embedded keys
  - Rekeying
  - Exposed private keys
  - Crypto shredding
  - Cryptographic obfuscation
  - Key rotation
  - Compromised keys