2.0 Architecture and Design

2.1 Explain the importance of security concepts in an enterprise environment.

- **Configuration management**
  - Diagrams
  - Baseline configuration
  - Standard naming conventions
  - Internet protocol (IP) schema
- **Data sovereignty**
- **Data protection**
  - Data loss prevention (DLP)
  - Masking
  - Encryption
  - At rest
  - In transit/motion
  - In processing
  - Tokenization
  - Rights management
- **Geographical considerations**
- **Response and recovery controls**
- **Secure Sockets Layer (SSL)/Transport Layer Security (TLS) inspection**
- **Hashing**
- **API considerations**
- **Site resiliency**
  - Hot site
  - Cold site
  - Warm site
- **Deception and disruption**
  - Honeypots
  - Honeyfiles
  - Honeynets
  - Fake telemetry
  - DNS sinkhole

2.2 Summarize virtualization and cloud computing concepts.

- **Cloud models**
  - Infrastructure as a service (IaaS)
  - Platform as a service (PaaS)
  - Software as a service (SaaS)
  - Anything as a service (XaaS)
  - Public
  - Community
  - Private
  - Hybrid
- **Cloud service providers**
- **Managed service provider (MSP)/ managed security service provider (MSSP)**
- **On-premises vs. off-premises**
- **Fog computing**
- **Edge computing**
- **Thin client**
- **Containers**
- **Microservices/API**
- **Infrastructure as code**
  - Software-defined networking (SDN)
  - Software-defined visibility (SDV)
- **Serverless architecture**
- **Services integration**
- **Resource policies**
- **Transit gateway**
- **Virtualization**
  - Virtual machine (VM) sprawl avoidance
  - VM escape protection

2.3 Summarize secure application development, deployment, and automation concepts.

- **Environment**
  - Development
  - Test
  - Staging
  - Production
  - Quality assurance (QA)
- **Provisioning and deprovisioning**
- **Integrity measurement**
- **Secure coding techniques**
  - Normalization
  - Stored procedures
  - Obfuscation/camouflage
  - Code reuse/dead code
  - Server-side vs. client-side execution and validation
  - Memory management
  - Use of third-party libraries and software development kits (SDKs)
  - Data exposure
- **Open Web Application Security Project (OWASP)**
- **Software diversity**
  - Compiler
  - Binary
- **Automation/scripting**
  - Automated courses of action
  - Continuous monitoring
  - Continuous validation
  - Continuous integration
  - Continuous delivery
  - Continuous deployment
- **Elasticity**
- **Scalability**
- **Version control**

2.4 Summarize authentication and authorization design concepts.

- **Authentication methods**
  - Directory services
  - Federation
  - Attestation
  - Technologies
    - Time-based one-time password (TOTP)
    - HMAC-based one-time password (HOTP)
    - Short message service (SMS)
    - Token key
    - Static codes
    - Authentication applications
    - Push notifications
    - Phone call
  - Smart card authentication
- **Biometrics**
  - Fingerprint
  - Retina
  - Iris
  - Facial
  - Voice
  - Vein
  - Gait analysis
  - Efficacy rates
  - False acceptance
  - False rejection
  - Crossover error rate
- **Multifactor authentication (MFA) factors and attributes**
  - Factors
    - Something you know
    - Something you have
    - Something you are
  - Attributes
    - Somewhere you are
    - Something you can do
    - Something you exhibit
    - Someone you know
- **Authentication, authorization, and accounting (AAA)**
- **Cloud vs. on-premises requirements**

2.5 Given a scenario, implement cybersecurity resilience.

- **Redundancy**
  - Geographic dispersal
  - Disk
    - Redundant array of inexpensive disks (RAID) levels
    - Multipath
  - Network
    - Load balancers
    - Network interface card (NIC) teaming
  - Power
    - Uninterruptible power supply (UPS)
    - Generator
    - Dual supply
    - Managed power distribution units (PDUs)
- **Replication**
  - Storage area network
  - VM
- **On-premises vs. cloud**
- **Backup types**
  - Full
  - Incremental
  - Snapshot
  - Differential
  - Tape
  - Disk
  - Copy
  - Network-attached storage (NAS)
  - Storage area network
  - Cloud
  - Image
  - Online vs. offline
  - Offsite storage
    - Distance considerations
- **Non-persistence**
  - Revert to known state
  - Last known-good configuration
  - Live boot media
- **High availability**
  - Scalability
- **Restoration order**
- **Diversity**
  - Technologies
  - Vendors
  - Crypto
  - Controls

2.6 Explain the security implications of embedded and specialized systems.

- **Embedded systems**
  - Raspberry Pi
  - Field-programmable gate array (FPGA)
  - Arduino
- **Supervisory control and data acquisition (SCADA)/industrial control system (ICS)**
  - Facilities
  - Industrial
  - Manufacturing
  - Energy
  - Logistics
- **Internet of Things (IoT)**
  - Sensors
  - Smart devices
  - Wearables
  - Facility automation
  - Weak defaults
- **Specialized**
  - Medical systems
  - Vehicles
  - Aircraft
  - Smart meters
- **Voice over IP (VoIP)**
- **Heating, ventilation, air conditioning (HVAC)**
- **Drones**
- **Multifunction printer (MFP)**
- **Real-time operating system (RTOS)**
- **Surveillance systems**
- **System on chip (SoC)**
- **Communication considerations**
  - 5G
  - Narrow-band
  - Baseband radio
  - Subscriber identity module (SIM) cards
  - Zigbee
- **Constraints**
  - Power
  - Compute
  - Network
  - Crypto
  - Inability to patch
  - Authentication
  - Range
  - Cost
  - Implied trust

2.7 Explain the importance of physical security controls.

- **Bollards/barricades**
- **Access control vestibules**
- **Badges**
- **Alarms**
- **Signage**
- **Cameras**
  - Motion recognition
  - Object detection
- **Closed-circuit television (CCTV)**
- **Industrial camouflage**
- **Personnel**
  - Guards
  - Robot sentries
  - Reception
  - Two-person integrity/control
- **Locks**
  - Biometrics
  - Electronic
  - Physical
  - Cable locks
- **USB data blocker**
- **Lighting**
- **Fencing**
- **Fire suppression**
- **Sensors**
  - Motion detection
  - Noise detection
  - Proximity reader
  - Moisture detection
  - Cards
  - Temperature
- **Drones**
- **Visitor logs**
- **Faraday cages**
- **Air gap**
- **Screened subnet (previously known as demilitarized zone)**
- **Protected cable distribution**
- **Secure areas**
  - Air gap
  - Vault
  - Safe
  - Hot aisle
  - Cold aisle
- **Secure data destruction**
  - Burning
  - Shredding
  - Pulping
  - Pulverizing
  - Degaussing
  - Third-party solutions

2.8 Summarize the basics of cryptographic concepts.

- **Digital signatures**
- **Key length**
- **Key stretching**
- **Salting**
- **Hashing**
- **Key exchange**
- **Elliptic-curve cryptography**
- **Perfect forward secrecy**
- **Quantum**
  - Communications
  - Computing
- **Post-quantum**
- **Ephemeral**
- **Modes of operation**
  - Authenticated
  - Unauthenticated
  - Counter
- **Blockchain**
  - Public ledgers
- **Cipher suites**
  - Stream
  - Block
- **Symmetric vs. asymmetric**
- **Lightweight cryptography**
- **Steganography**
  - Audio
  - Video
  - Image
- **Homomorphic encryption**
- **Common use cases**
  - Low power devices
  - Low latency
  - High resiliency
  - Supporting confidentiality
  - Supporting integrity
  - Supporting obfuscation
  - Supporting authentication
  - Supporting non-repudiation
- **Limitations**
  - Speed
  - Size
  - Weak keys
  - Time
  - Longevity
  - Predictability
  - Reuse
  - Entropy
  - Computational overheads
  - Resource vs. security constraints