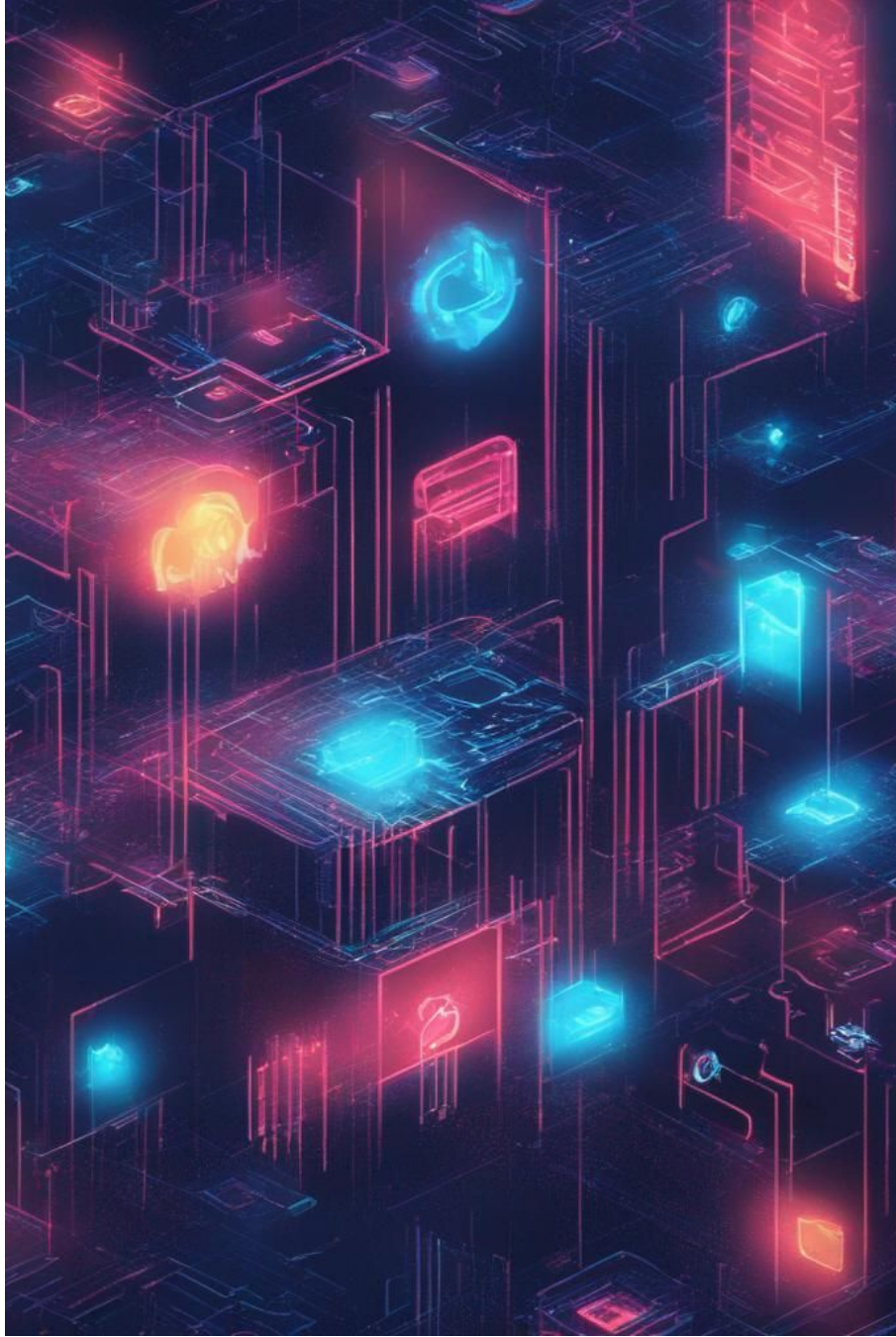
Securing the Foundation

A Comprehensive Exploration of Security Architecture and Design

CISSP Study Guide - III



Security Architecture and Design Fundamentals

Exploring the core principles of security models focusing on Confidentiality, Integrity, and Availability.

Understanding Defense in Depth within System Architecture.

Overview: Ensuring robust security from conceptualization to Maintenance Phase.

ISO/IEC 42010:2011 introduces critical terminologies shaping system security design.

System Architecture Lifecycle

1. **System Design Phase**: Requirements collection and solutions blueprint.

2. **Development Phase**: Assign component development tasks to respective teams.

3. **Maintenance Phase**: Ongoing evaluation of system and security functionality.

Architectural Concepts According to ISO/IEC 42010:2011

- **Architecture**: How systems components relate and evolve based on foundational principles.
- **Architectural Description (AD)**: Formal documentation of the architecture.
- **View**: How stakeholders perceive the system.
- **Viewpoint**: Framework aiding the creation of views tailored to stakeholder needs.

Computing Platforms Overview

Platform types ranging from Mainframe/Thin Clients to Mobile and Virtual Computing.

The role of Middleware and Embedded Systems in modern architecture.

The emergence of Cloud-based Virtual Machines and their security implications.

Integral Security Services

1. **Boundary Control**: Zones management to enforce security boundaries.
2. **Access Control Services**: Limiting user access to necessary areas.
3. **Integrity Services**: Verifying uncorrupted data traversal.
4. **Cryptographic Services**: Information encryption in transit.
5. **Auditing and Monitoring Services**: Enables usage and system process tracking.

Key System Concepts

- CPU functionalities including multiprocessing and privileged mode operations.
- **RAM Variants:** SDRAM, DDR, Laptop-specific SODIMMs.
- **ROM types:** Flash Memory, PLDs, FPGAs, and Firmware.
- Addressing schemes like Associative, Absolute, Indirect Accessing, and Logical Addressing.
- **Memory concerns:** Cache use, Virtual Memory utilization, preventing Memory Leaks.

Security-Enforcing Process and Multitasking

Understanding Privilege Levels and their impact on system security.

Segregation of Memory models: Symmetric vs. Asymmetric.

Multicore Processor Dynamics: Balance between User Threads and System Operations.

Trusted Computer System and Security Architecture Frameworks

1. Trusted Computer System Evaluation Criteria and how it relates to Bell-LaPadula concept.

2. Establishing a Security Perimeter and engaging a Reference Monitor coupled with a Security Kernel.

3. Using frameworks like Zachman, SABSA, ITIL, and TOGAF for a holistic approach to security design.

Slide 9: Security Architectural Development and Documentation

- TOGAF's iterative Architectural Development Method (ADM).
- Importance of ISO/IEC 27000 Series in maintaining standards.
- Navigating IT Governance with CobiT alongside myriad Security Models and Modes.

Models of Security

Bell-LaPadula: Ensuring confidentiality with no read up, no write down, and strong star property rules.

Biba and Clark-Wilson Models: Committing to data integrity.

Additional Models: Lipner, Brewer-Nash, Graham-Denning, and Harrison-Ruzzo-Ullman.

Handling System Security Evaluation and Security Modes

1. Explaining TCSEC's role and various Books related to system product security evaluation.

2. Dissecting ITSEC and Common Criteria ratings and assurance levels.

3. Discussing Certification and Accreditation including NIACAP and types like Type, System, and Site Accreditation.

Security Architecture Threats and Distributed System Security

- Identifying vulnerabilities from Maintenance Hooks to Web-Based Attacks.
- Mitigation tactics for Inference, Polyinstantiation, Aggregation, and Contamination.
- The necessity and challenge of securing Data Warehouses and Distributed Systems including Cloud, Grid, and Peer-to-Peer Computing.

Information Security Buzz

Discover more at our InfoSec Knowledge Hub