Information Systems Security Architecture Professional (ISSAP)

Notes by Al Nafi

Domain 4

Security Architecture Analysis

Author:

Osama Anwer Qazi

Product Assurance Evaluation Criteria

Product assurance evaluation criteria are used to assess and validate the security features and reliability of IT products and systems. These evaluations provide structured methodologies for verifying the security claims of software, hardware, and cryptographic implementations. One of the most widely recognized frameworks for security evaluation is the Common Criteria (CC), which is an internationally accepted standard for certifying IT security products.

Common Criteria (CC) Part 1

Common Criteria (CC) is an international standard (ISO/IEC 15408) for evaluating the security of IT products. It provides a common framework for testing and certifying security functionalities based on defined requirements. CC Part 1 establishes the fundamental concepts and principles of security evaluation, including:

- **Security Functional Requirements (SFRs):** Defines what security functions the product must provide.
- **Security Assurance Requirements (SARs):** Defines how the security functions must be tested and verified.
- **Protection Profiles (PPs):** Standardized sets of security requirements tailored for specific categories of products (e.g., firewalls, encryption devices).
- **Security Targets (STs):** Vendor-defined security requirements for a product undergoing evaluation.

CC Part 1 serves as the foundation for evaluating the security strength, capabilities, and risks associated with IT products.

Common Criteria (CC) Part 2

CC Part 2 focuses on security functional requirements (SFRs) that products must meet to achieve certification. These requirements define the expected security behaviors of an IT product and include:

- **Identification and Authentication (IA):** Ensures that users and entities are correctly authenticated.
- **Access Control (AC):** Enforces rules on who can access what resources based on predefined security policies.
- **Cryptographic Support (CRY):** Defines encryption, key management, and secure communication standards.
- **Security Audit (AUD):** Enables logging and monitoring of security events.
- Security Management (SM): Establishes administrative controls for maintaining system security.

Products that comply with CC Part 2 demonstrate robust functional security controls designed to withstand cyber threats and unauthorized access.

The Target of Evaluation (TOE)

The Target of Evaluation (TOE) refers to the specific IT product, software, or system undergoing security assessment. The TOE defines the scope and boundaries of the evaluation, including:

- The security features being tested (e.g., authentication, encryption, access control).
- The evaluation environment (e.g., on-premises system vs. cloud-based security solution).
- Potential threats and attack vectors applicable to the product.

A well-defined TOE ensures that security assessments are conducted with clear objectives and consistent evaluation standards.

Evaluation Assurance Level (EAL) Overview

The Evaluation Assurance Level (EAL) is a standardized scale that measures the depth and rigor of security testing and verification. The higher the EAL level, the more extensive and formalized the security evaluation.

EAL1 - Functionally Tested

EAL1 represents the lowest assurance level, where products are tested for basic security functions without requiring extensive design reviews. This level is suitable for products that require minimal security assurance, such as non-critical applications or commercial software.

EAL2 - Structurally Tested

EAL2 involves structured security testing, including code analysis and vulnerability assessments. It provides moderate assurance and is commonly used for corporate applications, access control systems, and secure communication tools.

EAL3 - Methodically Tested and Checked

EAL3 requires formal security documentation, structured testing, and vulnerability assessment methodologies. This level is suitable for products that require controlled security features, such as enterprise authentication systems, VPNs, and security appliances.

EAL4 - Methodically Designed, Tested, and Reviewed

EAL4 is the highest assurance level achievable without specialized development requirements. It involves formal design reviews, penetration testing, and independent security audits. Government agencies and financial institutions often require EAL4 certification for security-critical applications.

EAL5 - Semiformally Designed and Tested

EAL5 involves formal security engineering practices and detailed vulnerability assessments. It is used for specialized security devices such as trusted platform modules (TPMs), hardware security modules (HSMs), and secure operating systems.

EAL6 - Semi Formally Verified Design and Tested

EAL6 provides high security assurance through rigorous verification of security architecture and cryptographic mechanisms. It is typically required for high-risk environments, such as classified government systems, financial transaction security, and military-grade encryption.

EAL7 - Formally Verified Design and Tested

EAL7 represents the highest level of security assurance, requiring formal mathematical verification of security properties. This level is used for top-secret government applications, cryptographic research, and national security systems.

Common Criteria (CC) Part 3: Assurance Paradigm

CC Part 3 focuses on security assurance requirements (SARs), which define the methods for evaluating the effectiveness of security implementations. It outlines the testing methodologies, documentation standards, and risk analysis procedures necessary to determine whether a product meets its security claims.

The assurance paradigm ensures that security evaluations are:

- Repeatable and measurable using defined testing methodologies.
- Consistent across different vendors and testing laboratories.
- Aligned with global security best practices for reliable certification.

Significance of Vulnerabilities

Security vulnerabilities can compromise the integrity, confidentiality, and availability of an IT system. The severity of a vulnerability is assessed based on:

- Potential exploitation impact (e.g., unauthorized access, data breach, privilege escalation).
- Likelihood of exploitation (e.g., availability of attack tools, ease of execution).
- Remediation complexity (e.g., patch availability, system dependencies).

Understanding the significance of vulnerabilities helps security professionals prioritize patching, mitigation strategies, and risk management.

The Causes of Vulnerabilities

Vulnerabilities arise due to design flaws, implementation errors, and misconfigurations. The most common causes include:

- **Poorly written code:** Unchecked input validation, buffer overflows, and insecure API calls.
- **Weak cryptographic implementations:** Use of outdated encryption algorithms (e.g., MD5, SHA-1).
- **Misconfigurations:** Weak access controls, open ports, and improperly managed authentication settings.
- **Lack of security testing:** Inadequate penetration testing, vulnerability scanning, and code audits.

Mitigating these causes requires secure software development practices, continuous monitoring, and adherence to cryptographic security standards.

Common Criteria Assurance

Common Criteria assurance ensures that IT products meet rigorous security and compliance requirements. Certified products are:

- **Independently verified** through accredited testing laboratories.
- **Evaluated against global security standards** such as ISO/IEC 15408.
- **Accepted across multiple countries** for interoperability and trust.

Organizations adopting Common Criteria-certified products gain confidence in the security and reliability of their IT systems, ensuring compliance with regulatory frameworks such as GDPR, HIPAA, and NIST.

Conclusion

The Common Criteria framework provides a structured approach to evaluating IT security products, ensuring that they meet defined security requirements and industry standards. By assessing the Target of Evaluation (TOE), Evaluation Assurance Levels (EALs), and vulnerability management processes, organizations can make informed decisions about product security, compliance, and risk mitigation strategies. Security architects must integrate Common Criteria principles into product evaluations to enhance overall IT security and resilience against cyber threats.