Topics

- What is the Common Criteria?
- Key concepts
  - Targets of Evaluation
  - Security Requirements
  - Assurance Requirements
  - Environmental Requirements
- Testing
- Other Information Resources

ANSI Shared Public Documents – Common Criteria

What is the Common Criteria?

- An international standard (ISO/IEC15408) for computer security evaluation
- A framework in which...
  - Computer system purchasers and users can specify their security requirements
  - Vendors can make claims about the security attributes of their products
  - Testing laboratories can evaluate products to determine if they actually meet the claims.

Targets of Evaluation

- A system design which claims to satisfy security requirements
- A product or system for which security claims are made

Note: The term “target of evaluation” is typically abbreviated as “TOE”.

ANSI Shared Public Documents – Common Criteria

Security Requirements

- **Derived from**
  - **Policies**, e.g., desired states and outcomes of privacy protections, confidentiality, and assurance of security within the TOE.
  - **Risk analysis**, identifying threats for which mitigation is required within the TOE
  - **Environmental analysis**, identifying factors that may influence the formation of policy or mitigate risks, but which are generally outside the TOEs' scope.

Security Requirements

- **Document artifacts**
  - **Protection Profile (PP)** - identifies detailed security requirements relevant to a particular purpose, e.g. a set of related use cases.
  - **Security Functional Requirements (SFRs) -** the individual security functions to be provided within a TOE.
  - **Security Target (ST)** - a document that identifies the security properties of the TOE.

ANSI Shared Public Documents – Common Criteria

Assurance Requirements

- **Assurance** is the level of confidence that the policies are enforced and risks are mitigated within the TOE.
- Assurance requirements must be supported by the TOE
- Assurance activities are ongoing, often periodic, and typically performed in the course of system operation

Assurance Requirements

- **Security Assurance Requirements (SAR)** describe the detailed actions during development, implementation, and operation the TOE that will assure its compliance with the claimed security functionality.
- **Evaluation Assurance Level (EAL)** is a numerical rating assigned to the TOE to reflect the SARs to be fulfilled. EALs are predefined packages (in ISO/IEC 15408-3) of SARs with a given level of strictness.

Testing

- NIST's National Voluntary Laboratory Accreditation Program (NVLAP) accredits Common Criteria testing laboratories in the US.
  - CCHIT security criteria are derived, in part, from the Common Criteria. However, the rigor of the testing laboratories was deemed too expensive.
- Use of the Common criteria in US Federal system procurement is mandatory.

ANSI Shared Public Documents – Common Criteria

Resources

- Common Criteria Project Portal
  https://www.commoncriteriaportal.org/cc/