Introduction to the Common Criteria and the Underlying Concepts of Trust in Computer Systems

Michael McEvilley
SIGAda 2002 Tutorial SF3
December 8, 2002
Tutorial Objectives

Understanding

- Security concepts and the principles behind establishing trust in security functions
- The contents and concepts of the Common Criteria
- The philosophy behind the CC and the resultant limitations of the CC
The similarities and differences in establishing assurance for security critical and other critical application domains
  – Concepts vs. terminology
  – Development and verification processes
Discussion Topics

- Security Concepts & the CC
- CC Document Conceptual Walk-through
  - CC Part I – Introduction & General Model
  - CC Part II – Functional Requirements
    - Requirements Organization, Overview, Operations
  - CC Part III – Assurance Requirements
    - Requirements Organization, Overview, Operations
What Is the CC?

“Common Criteria for Information Technology Security Evaluation”

Common Criteria

- Meta-standard containing constructs and criteria used to develop security specifications
  - Specification constructs
    - Protection Profile (PP)
    - Security Target (ST)
  - Requirements criteria
    - Functional
    - Assurance

… in support of the evaluation of products and systems
CC Functional Criteria

- Specify the security properties of IT products and systems that address:
  - Unauthorized disclosure (confidentiality, privacy)
  - Unauthorized modification (integrity)
  - Loss of use (availability)
  - Verification of identity (Identification and Authentication (I&A))
  - Accountability for operations (audit, non-repudiation)

- Provides a basis for comparison of different design or implementation solutions
CC Assurance Criteria

- Specify the properties for verification of development life-cycle activities
- Specify the properties for accumulation and verification of a continuity of knowledge as systems evolve
  - Continuity of knowledge ~ maintenance
- Provides a basis for comparison of the results of independent evaluations
Application of the CC

Process Independence
CC constructs may be integrated with existing system life-cycle processes

Technology Independence
CC requirements are independent of technology and implementation – hardware, software, firmware

Functionality Independence
CC criteria is independent of requirements specific to any business or mission case

Goal Independence
Originally developed to support formal evaluation Being applied in new and diverse contexts
**Target of Evaluation (TOE)**

- An IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation
- Differentiation between product and system is not clear - think components
  - Single component TOE
  - Multi-component TOE
  - System TOE
CC Terms

- **TOE Security Policy (TSP)**
  - Set of rules that define how resources are managed, protected and distributed by the TOE

- **TOE Security Functions (TSF)**
  - The parts of the TOE implementation that are relied upon for the correct enforcement of the TOE Security Policy (TSP)

- **TSF Interfaces (TSFI)**
  - Interfaces to the TOE security functions
    - internal to the TOE
    - external to the TOE
CC Terms

- IT Environment
  - IT components that are not part of the TOE but with which the TOE shares a trusted relationship
    - Trust relationship – authentication of communication participants and secure methods to transfer information

- Non-IT Environment
  - The physical aspects of the location(s) in which the TOE is placed and operates
Illustration

TOE, TSF, TSFI

Target of Evaluation (TOE)

TSF Interfaces (TSFI)

TOE
Non-Security Functions

TOE Security Functions (TSF)
Non-IT environment consists of the physical aspects of the location(s) in which the TOE is placed and operates.
The general environment is enclosed inside the square, i.e., the ‘world’

- TOE Environment is enclosed inside the circle

Non-IT environment implemented by the physical world

IT Environment implemented by IT capabilities
Practical Illustration

Web Server (TOE) - Certificate Server (IT Environment)

Non-IT environment of the Web Server (TOE)

Non-IT environment of the Certificate Server (IT environment of the TOE)
Interfaces

- Rules for interaction between components
- Typically specified independent of functionality
  - message interface
  - programming interface (API)
  - services interface
  - plug-in interface
- May be internal or external
Trust Relationships

- Rules for secure interaction between components
  - special form of interface
  - subset of interface specification

- From the CC perspective
  - internal to the TOE
  - between the TOE and a remote trusted component
    - the IT environment
Establishing Trust Relationships

- Trusted channels provide mechanism for trust relationships between security components
  - authentication of endpoints
  - secure communication protocol
    - integrity, confidentiality, recovery
- Trusted channels provide mechanism for trust relationship between user and TSF
CC Trust Relationship Terms

- Trusted Channel
  - the means by which the TSF communicates securely with another part of the TSF or with a remote trusted IT product

- Trusted Path
  - the means by which a user communicates securely with the TSF
  - trusted paths are built on trusted channels
Trust relationship between TOE and IT environment requires
- establishment of trust between the communicants via two-way authentication
- protecting information from modification and disclosure
Trusted Relationship Concept

Networked/Distributed TOE

- No IT Environment - the TSF is a single logical entity although the parts are physically distributed
- Regardless, the requirements remain
  - establishment of trust between the distributed TSF components
  - protecting information from modification and disclosure
Security Evaluation Issues

- TSF consists of three subsystems
  - one external interface to TSF
  - three internal subsystem interfaces
Descriptive Walkthrough of the Common Criteria
Common Criteria
Part I

Introduction & General Model
The CC Requirements Specification Framework

Specification Constructs

Protection Profiles
Security Targets
Packages
Purpose

● Present a “Security Case”
  – Context problem statement
    ● Introduction
    ● TOE Description
    ● Environment information
      – Assumptions, Threats, Policies
  – Statement of solution
    ● Objectives
    ● Functional and assurance requirements
  – Rationale to substantiate the solution
CC Specification Constructs

- Protection Profile (PP)
  - An implementation-independent characterization of required security capabilities and verification activities

- Security Target (ST)
  - A implementation-dependent statement of security capabilities and verification activities used as the basis for the TOE evaluation
    - Complete requirement and implementation detail

- Package
  - Reusable set of functional and/or assurance requirements
Purpose of the PP

- To provide a means for statement of security requirement needs
  - for acquisition
  - for development
  - for certification & accreditation
  - for any unique security documentation requirement

- PPs establish ...
  - a basis for ST development
  - a common reference for ST comparison and assessment
Protection Profile Granularity

- Requirement detail granularity is the discretion of the PP author

Increasing detail & constraints - less options & flexibility
Purpose of the ST

- To provide a means for developers and system integrators to state the security requirement of a component, product or system
  - in response to a PP
  - independent of a PP

- STs establish
  - the basis for a TOE evaluation
PP/ST Contents/Comparison

Protection Profile
- Identification
- Overview
- TOE Description
- Security Environment
  - Assumptions, Threats, Policies
- Security Objectives
- Security Requirements
  - Functional, Assurance (EAL)
- Rationale

Security Target
- Identification
- Overview
- TOE Description
- Security Environment
  - Assumptions, Threats, Policies
- Security Objectives
- Security Requirements
  - Functional, Assurance (EAL)
- Rationale
- TOE Summary Specification
- CC Conformance Claim
- PP Claims
PP Evaluation

- Verifies that the PP meets the criteria defined by the APE assurance class
  - Technical correctness vs. applicability
- Establishes an approved specification repository from which compliant components may be developed or verified
  - Often referred to as a registry
  - Managed by a controlling [regulatory] organization
ST Evaluation

- Verifies that the ST serves as a suitable basis for the TOE evaluation
  - Technical correctness
- Verifies that the ST is an accurate instantiation of each profile to which it claims compliance
  - PP compliance claim is optional
- The ST is typically evaluated with the TOE
TOE evaluation includes ST, TOE and evaluation evidence

ST must be evaluated first to establish a basis for the TOE evaluation

ST evaluation is not complete until the TOE evaluation completes
  - ST must be *sufficiently complete* to enable the TOE evaluation
PP/ST Relationship

- A ST may be derived from a PP
- A ST may be developed independent of a PP
- The ST author has the option to establish the relationship between the ST and a PP
  - referred to as a PP Claim
  - one ST may be related to multiple PPs
  - each PP claim must be substantiated by the ST author
CC Requirements Specification Framework (PP/ST) Contents
ALL TOE security requirements ultimately arise from consideration of the purpose of the TOE and the context in which the TOE operates.
A specification framework with checks and balances to provide end-to-end correctness
PP/ST Development Activities

Establish Security Environment

TOE Physical (Non-IT) Environment
TOE IT Environment
Assets Requiring Protection
TOE Scope and Purpose
Establish Security Environment
Secure Usage Assumptions
Threats
Organizational Security Policies (OSP)s
PP/ST Development Activities

Establish Security Objectives

- Establish Security Objectives
  - Threats
    - Secure Usage Assumptions
    - Organizational Security Policies (OSPs)
  - TOE Objectives
    - Non-IT Environment Objectives
    - IT Environment Objectives
PP/ST Development Activities

Establish Security Requirements

- Non-IT Environment Objectives
- CC Part II & Part III Requirements Catalog
- TOE Objectives
- IT Environment Objectives
- TOE Functional Requirements
- TOE Assurance Requirements
- Interface to IT Environment Requirements
- Non-IT Environment Requirements
The Security Environment

Secure Usage Assumptions
Threats
Organizational Security Policy (OSP)
Security Environment Components

- **Assumptions**
  - The security aspects of the environment in which the TOE will be used or is intended to be used

- **Threats**
  - The ability to exploit a vulnerability by a threat agent

- **Organizational Security Policies (OSPs)**
  - A set of rules, procedures, practices, or guidelines imposed by an organization upon its operations
Assumptions are “assertions of expectations” regarding
- secure usage of the TOE
- scope and boundary of the TOE
- placement of the TOE in its environment
  - interaction with other IT (IT environment)
  - interaction with people (Non-IT environment)

Assumptions establish context for all that follows in the PP/ST

“The security aspects of the environment in which the TOE will be used or is intended to be used”
Using Assumptions

- Assumptions must not
  - impose requirements on the TOE or on its IT environment
  - have IT aspects of objectives mapped to them
  - be used to mitigate legitimate threats that are to be countered by the TOE or its IT environment

- Assumptions must
  - be considered as requirements for the Non-IT environment

- Assumptions always
  - result in objectives for the Non-IT environment
Assumption Examples

- **A.Physical_Protection**
  - The TOE is installed in a restricted and controlled access area sufficient to prevent unauthorized physical access to the TOE.

- **A.Dedicated_Network**
  - The TOE is installed on an isolated network that is dedicated to the TOE and that is not connected to any other network.
Threats

“The ability to exploit a vulnerability by a threat agent”

- Threat definition is accomplished through a Vulnerability Analysis that give insight to the threats
  - against the TOE
  - against the environment of the TOE (IT & Non-IT)
  - inherent to technology/personnel/operations

- Threats are countered
  - by the TOE
  - by the IT environment of the TOE
  - by the Non-IT environment of the TOE
Focus of Threat Statements

- Threats provide a basis for statement of countermeasures
- Threats SHALL address
  - the attack
  - the attacker
  - the assets
  - the implications of the successful attack
- Threats SHOULD address
  - attacker motivation, expertise
  - risk of threat being realized
T. Intercept

An individual obtains unauthorized access to controlled information by intercepting information transmitted to/from the TOE.

T. Authentication

An individual obtains unauthorized access to the TOE by

a. impersonating an authorized user of the TOE,

b. replaying a successful authentication session,

c. unauthorized use of an authorized users existing session
Organizational Security Policy

“A set of rules, procedures, practices, or guidelines imposed by an organization upon its operations”

- PP/ST author discretion to include/exclude policy
  - Policy required
    - If some aspect of the policy is to be enforced by the TOE or by the IT environment of the TOE
  - Policy optional
    - If no aspect of the policy is to be enforced by the TOE or by the IT environment of the TOE
P.Dedicated_Network

All mission-critical systems shall be installed on dedicated networks that are isolated from non-mission-critical systems in accordance with OPSEC 123.4.
Assumptions vs. Policy
  - it’s a style/preference issue
  - assumptions are mapped to non-IT objectives, and an equivalent policy statement will also be mapped to a non-IT objective

- **A.Dedicated_Network**
  The TOE is installed on an isolated network that is not connected to any other network.

- **P.Dedicated_Network**
  All mission-critical systems shall be installed on dedicated networks that are isolated from non-mission-critical systems in accordance with OPSEC 123.4.
The Security Objectives

- Security Objectives for the TOE
- Security Objectives for the IT Environment
- Security Objectives for the Non-IT Environment
Security Objectives

- Objectives establish the basis for the selection of security requirements (functional & assurance)
- Objectives exist only to address the problem statement per the security environment section
  - Support Assumptions
  - Counter Threats (eliminate, minimize, monitor)
  - Enforce OSPs
- Justified by rationale
Types of Security Objectives

- **TOE Objectives**
  - Implemented by security requirements allocated to the TOE

- **IT Environment Objectives**
  - Implemented by security requirements allocated to the IT systems that interact with the TOE

- **Non-IT Environment Objectives**
  - Implemented by personnel and procedural means
  - Outside the scope of the CC
  - Statement of non-IT environment requirements is not required
Objective Example - Non-IT
(from Assumption)

- **OE.Physical_Protection**
  Those responsible for the TOE shall ensure that the TOE is installed in a restricted and controlled access area that prevents unauthorized physical access to the TOE.

- **A.Physical_Protection**
  The TOE is installed in a restricted and controlled access area sufficient to prevent unauthorized physical access to the TOE.
Objective Example - TOE  
(from Threat)

- **O.Impersonate**
  The TSF shall provide two-factor authentication employing hardware token technology and a unique identification attribute.

  Note: O.Impersonate addresses only one aspect of T.Authentication.

- **T.Authentication**
  An individual obtains unauthorized access to the TOE by
  
  a. impersonating an authorized user of the TOE,
  
  b. replaying a successful authentication session,
  
  c. unauthorized use of an authorized user's existing session
Objective Example - Non-IT
(from Policy)

- OE.NeNetwork
  Those responsible for the TOE shall ensure that the TOE is connected to a dedicated network that is isolated from non-mission-critical systems.

- P.Dedicated_Network
  All mission-critical systems shall be installed on dedicated networks that are isolated from non-mission-critical systems in accordance with OPSEC 123.4.
The Security Requirements

- Security Functional Requirements
- Security Assurance Requirements
Functional and Assurance Requirements

- Selected from the CC
  - Functional Requirements - Part 2
  - Assurance Requirements - Part 3
- May be explicitly stated
- Justified by rationale
Security Objectives
Security Requirements
TOE Summary Specification (ST only)
Security Objectives Rationale

- Justifies statement of security objectives through demonstration of
  - Necessity - coverage of security environment
    - through traceability to specific aspects of the environment
  - Sufficiency - suitability to
    - support the assumptions
    - counter the threats
    - enforce the OSPs
Security Requirements Rationale

- Justifies each security requirement through
  - Necessity - coverage of security environment
    - traceability to specific aspects of the objectives
  - Sufficiency
    - suitability to implement specific aspects of the objectives
TOE Summary Specification (TSS)

- Definition and mapping of
  - security functions to functional requirements
  - assurance measures to assurance requirements
- Rationale (necessity/sufficiency)
  - security functions meeting the security requirements
  - assurance measures meeting the assurance requirements
Reusable Constructs

Packages
Package Construct

- Reusable set of either functional or assurance components combined together to satisfy a set of identified security objectives
- CC provides no explicit criteria for evaluation of packages
Package Contents

- Objectives
  - establish context for requirements
- Requirements
  - implement objectives
- Rationale
  - presents informal argument to justify requirements in terms of the stated objectives
PP/ST Section Relationships

- Security Environment
- Assumptions
- Threats
- OSPs
- Non-IT
- TOE
- IT
- Functional
- Assurance
- Functional
- Assurance
- Security Functions
- Assurance Measures
- Security Target Only
Security Functional Requirements
Functional Requirements
Organization

- **Class** - organizational purposes
  - all members share a common focus (e.g., Audit, I&A)

- **Family** - organizational purposes
  - all members share security objectives but may differ in emphasis (e.g., Audit event definition, Audit event review)

- **Component** - smallest selectable requirement set
  - contains a set of elements

- **Element** - “shall” statements
  - members of a component
  - elements cannot be selected individually
Interpreting Functional Requirement Names

FIA_UID.1.1

F = Functional

Class Name

Family Name

Component Number

Element Number
Operations on Requirements

- Assignment
- Selection
- Refinement
- Iteration

Functional requirements have placeholders indicating where Assignment and Selection operations are allowed.

Refinement and iteration may be performed on any functional requirement.
Assignment Operation

- Specification of a parameter filled in when component is used
- “Fill in the Blank” operation
- Allows PP/ST writer to provide information relating to application of the requirement
- The PP writer may defer completing assignments, but the ST writer must complete all assignments
Assignment Operation Example

As Written in the Common Criteria:

- FMT_SMR.1.1 The TSF shall maintain the roles: [assignment: the authorized identified roles].

After Assignment Operation:

- FMT_SMR.1.1 The TSF shall maintain the roles: [assignment: authorized administrator, security officer, operator].
Selection Operation

- Specification of elements selected from a list given in the component
- “Multiple Choice” operation
- Allows PP/ST writer to select from a provided list of choices
- The PP writer may defer completing selections, but the ST writer must complete all selections
As Written in the Common Criteria:

- **FTA_TAH.1.1** Upon successful session establishment, the TSF shall display the [selection: *date, time, method, location*] of the last successful session establishment to the user.

After Selection Operation:

- **FTA_TAH.1.1** Upon successful session establishment, the TSF shall display the [selection: *date, time, and location*] of the last successful session establishment to the user.
Selection Operation Example #2

As Written in the Common Criteria:

- **FTP_TRP.1.3** The TSF shall require the use of the trusted path for [selection: initial user authentication, [assignment: other services for which trusted path is required]].

After Selection Operation:

- **FTP_TRP.1.3** The TSF shall require the use of the trusted path for [selection: initial user authentication [assignment: and password changes]].
Combined Selection and Assignment Example

As Written in the Common Criteria:

- **FMT_MTD.1.1** The TSF shall restrict the ability to [selection: change_default, query, modify, delete, clear, [assignment: other operations]] the [assignment: list of TSF data] to [assignment: the authorized identified roles].

After Selection Operation:

- **FMT_MTD.1.1** The TSF shall restrict the ability to [selection: delete, [assignment: and create]] the [assignment: user authentication database] to [assignment: the authorized administrator].
Refinement Operation

- A mechanism to tailor a requirement by specifying additional detail in order to meet a security objective.

- Rules for refinement:
  - The refinement shall only restrict the set of possible acceptable functions used to implement the requirement.
  - The refinement may not levy completely new requirements.
  - The refinement may not increase the list of dependencies of the requirement being refined.
As Written in the Common Criteria:

- **FAU_SAA.1.1** The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the TSP.

After Refinement Operation:

- **FAU_SAA.1.1** The **Server-TSF** shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the TSP.
Iteration Operation

- Repetitive use of the same component to address different aspects of the requirement being stated (e.g., identification of more than one type of user).

- Can be performed on any functional component.
Iteration Operation Example

As Written in the Common Criteria:

- **FMT_MTD.1.1** The TSF shall restrict the ability to [selection: change_default, query, modify, delete, clear, [assignment: other operations]] the [assignment: list of TSF data] to [assignment: the authorized identified roles].

After Iteration Operation:

- **FMT_MTD.1.1** The TSF shall restrict the ability to [selection: modify] the [assignment: password file] to [assignment: the authorized administrator].

- **FMT_MTD.1.1** The TSF shall restrict the ability to backup/restore the password file to the authorized operator.
Explicitly Stated Requirements

“Rolling Your Own Requirements”

- CC component catalogues are extensive but not comprehensive
  - Requirements evolve over time
- CC does not mandate exclusive use of component catalogues
- CC contains criteria for correctness of extended requirements
- CC terms
  - Extensibility ~ Extended requirements ~ Explicitly stated requirements
CC Part II

Functional Requirement Classes
Functional Requirement Classes

- Security Audit (FAU)
- Communication (FCO)
- Cryptographic Support (FCS)
- User Data Protection (FDP)
- Identification & Authentication (FIA)
- Security Management (FMT)
- Privacy (FPR)
- Protection of the TOE Security Functions (FPT)
- Resource Utilization (FRU)
- TOE Access (FTA)
- Trusted Path/Channels (FTP)
Class FAU: Security Audit

The 6 families in this class address...

- recognizing and responding to (FAU_ARP)
- recording (FAU_GEN, FAU_SEL)
- storing and protecting (FAU_STG)
- review and analysis of (FAU_SAA, FAU_SAR)

... security-relevant events and activities.
Class FCO: Communication

- The 2 families in this class address ...
  - proof of origin (FCO_NRO)
  - proof of receipt (FCO_NRR)

... of transmitted information.
The 2 families in this class address ... 
- generation, distribution, access, and destruction (FCS_CKM) 
- operational use (FCS_COP) 
... of cryptographic keys.
Class FDP: User Data Protection

The 13 families in this class address ...
- security function policies (FDP_ACC, FDP_IFC)
- access control and information flow control functions (FDP_ACF, FDP_IFF)
- authenticity and integrity (FDP_DAU, FDP_ITT, FDP_SDI)
- reuse and rollback (FDP_RIP, FDP_ROL)
- import/export (FDP_ETC, FDP_ITC)
- inter-TSF communications (FDP_UCT, FDP_UIT)

... for protection of user data.
The 6 families in this class address ...
  – establishing (FIA_ATD, FIA_SOS, FIA_USB)
  – verifying (FIA_UAU, FIA_UID)
  – failures when authenticating (FIA_AFL)

... claimed user identity.
The 6 families in this class address ... 
  – management of TSF data (FMT_MTD) 
  – management of security attributes (FMT_MSA, FMT_REV, FMT_SAE) 
  – management of the security functions (FMT_MOF) 
  – security roles (FMT_SMR) 
... of the TOE.
The 4 families in this class address ...
  - discovery and misuse (FPR_ANO, FPR_PSE, FPR_UNL, FPR_UNO)
... of an individual’s identity or activities by others.
The 16 families in this class address ...
- testing (FPT_AMT, FPT_TSF)
- physical/anti-tamper protection (FPT_PHP)
- secure TSF data transfer (FPT_ITA, FPT_ITC, FPT_ITI, FPT_ITT, FPT_RPL, FPT_TDC, FPT_TRC)
- failure and recovery (FPT_RCV, FPT_FLS)
- state and timing (FPT_SSP, FPT_STM)
- reference mediation and domain separation (FPT_RVM, FPT_SEP)

... of the TSF mechanisms and data.
The 3 families in this class address ... 
- availability (FRU_FLT)
- allocation (FRU_PRS, FRU_RSA)

... of resources.
Class FTA: TOE Access

The 6 families in this class address ...
- attributes (FTA_LSA, FTA_TAB, FTA_TAH)
- establishment (FTA_MCS, FTA_SSL, FTA_TSE)
... of a user session.
The 2 families in this class address...
- trusted communication paths (FTP_TRP)
- trusted communication channels (FTP_ITC)

...between users and the TSF and between the TSF and other trusted IT products, respectively.
CC Part 3
Security Assurance Requirements
Part 3
What is Assurance?

- Grounds for confidence that implemented countermeasures meet their security objectives
  - CC focus is the IT countermeasures
  - Comprehensive approach includes the environment
- Assurance measures
  - Provide a basis for a security argument
  - Do not add functionality to the TOE
- Assurance is subjective
Why Assurance is Needed?

To address vulnerabilities arising from
- Requirements
  - Incorrect, insufficient, ineffective
- Design and Implementation
  - Incorrect design decisions
  - Errors in implementation
- Operational Controls
  - Inadequate or overly complicated
  - Poorly documented
Where Assurance is Needed

- Verification and Validation of the Specification
  - Protection Profile
  - Security Target
- Verification of the implementation (TOE)
- CC defines 3 evaluations
  - Protection Profile (PP) evaluation
    - mandatory criteria
  - Security Target (ST) evaluation
    - mandatory criteria
  - Target of Evaluation (TOE) evaluation
    - criteria as specified in the Security Target
Concept of TOE Evaluation

CC Approach to Verification

- Analysis of processes and procedures
- Checking that processes and procedures are being applied
- Analysis of the correspondence between TOE design representations
- Analysis of the TOE design representations against the requirements
- Verification of mathematical proofs
- Analysis of guidance documents
- Analysis of functional tests and results
- Independent functional testing
- Analysis for flaws
- Penetration testing
Balance 3 variables
- Scope - how much is assessed
- Depth - to what degree is it assessed
- Rigor - in what manner is it assessed

Greater Evaluation Effort (Scope, Depth, Rigor)
Greater Assurance
Interpreting Assurance Requirement Names

ADV_LLD.3.1(D,C,E)

A=Assurance

Specific Class

Family Name

Component Number

Element Number

Element Identifier
Security Assurance Classes

**TOE Evaluation:**
- Configuration Management (ACM)
- Delivery and operation (ADO)
- Development (ADV)
- Guidance documents (AGD)
- Life Cycle Support (ALC)
- Maintenance of Assurance (AMA)
- Tests (ATE)
- Vulnerability assessment (AVA)

**PP Evaluation:**
- PP Evaluation (APE)

**ST Evaluation:**
- ST Evaluation (ASE)
The families in this class address the CM system used in the development of the TOE.

- ACM_AUT CM automation
- ACM_CAP CM capabilities
- ACM_SCP CM scope
Class ADO: Delivery and Operation

The families in this class address documentation focused on correct delivery, installation, generation, and start-up of the TOE.
Class ADV: Development

The families in this class define requirements for the design documentation of the TOE security functions at various levels of abstractions.

- ADV_FSP Functional specification
- ADV_HLD High-level design
- ADV_IMP Implementation representation
- ADV_INT TSF internals
- ADV_LLD Low-level design
- ADV_RCR Representation correspondence
- ADV_SPM Security policy modeling
Class AGD: Guidance Documents

AGD defines requirements for the coherency, coverage, and completeness of the user and administrative guidance documentation.
Class ALC: Life Cycle Support

ALC defines requirements for the establishment of discipline and control in the process of TOE development and maintenance.

- ALC: Life cycle support
  - ALC_DVS Development security
  - ALC_FLR Flaw remediation
  - ALC_LCD Life cycle definition
  - ALC_TAT Tools and techniques
AMA defines requirements for the maintenance of the level of assurance that the TOE will continue to meet its security target as changes are made to the TOE or its environment.

- **AMA: Maintenance of assurance**
  - **AMA_AMP** Assurance maintenance plan
  - **AMA_CAT** TOE component categorization report
  - **AMA_EVD** Evidence of assurance maintenance
  - **AMA_SIA** Security impact analysis
ATE defines testing requirements that demonstrate the TOE satisfies its functional requirements.

**ATE: Tests**

- **ATE_COV** Coverage
- **ATE_DPT** Depth
- **ATE_FUN** Functional tests
- **ATE_IND** Independent testing
AVA defines requirements for the identification of exploitable vulnerabilities introduced in the construction, operation, misuse, or incorrect configuration of the TOE.

- **AVA:** Vulnerability assessment
  - **AVA_CCA** Covert Channel analysis
    - 1 2 3
  - **AVA_MSU** Misuse
    - 1 2 3
  - **AVA_SOF** Strength of functions
    - 1
  - **AVA_VLA** Vulnerability analysis
    - 1 2 3 4
Operations on Assurance Requirements

Iteration
Refinement
Assurance Iteration and Refinement

- As stated in the CC …
  - ADV_FSP.1.3C The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing details of effects, exceptions and error messages, as appropriate.

- After applying iteration for software and hardware …
  - ADV_FSP.1.3C:1 For software implementations, the functional specification shall describe the purpose and method of use of all external TSF interfaces, providing details of effects, exceptions and error messages, as appropriate.

  - ADV_FSP.1.3C:2 For hardware implementations, the functional specification shall describe the purpose and method of use of all external TSF interfaces, providing details of effects, input and output signal levels, error indications and reset conditions, as appropriate.
Assurance Refinement

- As stated in the CC …
  - ADV_SPM.1.2C  The TSP model shall describe the rules and characteristics of all policies of the TSP that can be modeled.

- After applying iteration for software and hardware …
  - ADV_SPM.1.2C  The TSP model shall describe the rules and characteristics of all policies of the TSP as a finite state machine to include the following:
    - definition and transition from non-secure to secure initialization state
    - definition and transition from secure operational state to secure fail-state
    - recovery transition from fail-secure to operational secure state
    - definition of transition to known insecure fail states
Assurance Packages

- Reusable set of functional or assurance components combined together to satisfy a set of identified security objectives

- Currently, there are 7 assurance packages called Evaluation Assurance Levels (EAL1 - EAL7)
Evaluation Assurance Levels

Provide an increasing scale that strives to maintain a balance
# Assurance Component to EAL Mapping

<table>
<thead>
<tr>
<th>Assurance Class</th>
<th>Assurance Component by EAL Level</th>
<th>EAL1</th>
<th>EAL2</th>
<th>EAL3</th>
<th>EAL4</th>
<th>EAL5</th>
<th>EAL6</th>
<th>EAL7</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration management</td>
<td>ACM AUT</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>ACM CAP</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>ACM SCP</td>
<td></td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Delivery and operation</td>
<td>ADO DEL</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>ADO I GS</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Development</td>
<td>ADV FSP</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>ADV HLD</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>ADV IMP</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>ADV INT</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ADV LLD</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>ADV RCR</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>ADV SPM</td>
<td>1</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Guidance documents</td>
<td>AGD ADM</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>AGD USR</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Life cycle support</td>
<td>ALC DVS</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>ALC FLR</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ALC LCD</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ALC TAT</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tests</td>
<td>ATE COV</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>ATE DPT</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>ATE FUN</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>ATE I ND</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>Vulnerability assessment</td>
<td>AVA CCA</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>AVA MSU</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>AVA SOF</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>AVA VLA</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>Assurance maintenance</td>
<td>AMA AMP</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>AMA CAT</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>AMA EVD</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>AMA SIA</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
EAL Augmentation
The Tailoring of an Existing Evaluation Assurance Level (EAL)

- Allowed augmentation operations
  - Replace an existing component in the EAL with a higher component
  - Add additional component(s) from other EALs
  - Add additional component(s) not in any EAL
  - MRA does not recognize augmentation with components not in EAL 1-4

- Disallowed augmentation operation
  - Remove a component from an EAL definition
Thank you for your attention.

Please do not hesitate to follow-up with any questions are issues that arise subsequent to this session.

Michael McEvilley
703.414.5002 (voice)
703.414.5066 (fax)
michael.mcevilley@dac.us
www.commoncriteri.com