

# The Common Criteria for Information Technology Security Evaluation (CC)

Real-Time and Embedded Systems Forum  
Security Working Group  
24 January 2002

Michael McEvilley



# Discussion Goals

- Establish a basis for continued discussion regarding application of the CC to meet Security Working Group objectives
  - Acquire a high-level understanding of what the CC is and how it is being used
  - Understand why the CC can support Security Engineering life-cycle processes
  - Address CC-related issues raised during morning session discussion

# What you're in for ...

- Good news
  - ... the CC addresses your concerns and questions
- Not so good news
  - ... you are responsible for figuring out the answers
- Bad news
  - ... the CC does not tell you how to do it!

# Motivation for Development

*“Support Formal Evaluation”*

- Consolidation of
  - differing international *security evaluation criteria* into a single standard (ISO/IEC 15408, CC)
- Establishment of
  - a *security evaluation methodology* based upon the international standard (Common Evaluation Methodology)
- Enforcement of
  - *national processes for security evaluation* based on a common *security evaluation methodology* utilizing a standard set of *security evaluation criteria*

# How is the CC being used?

- On the one hand ...
  - used *initially* to support formal evaluation in the context of an international program
    - Common Criteria Recognition Arrangement (CCRA)
- On the other hand ...
  - used *increasingly* to support security engineering activities associated with system life-cycle processes

# The CC Application Domain

## Process Independence

Constructs may be integrated into existing system life-cycle processes

## Technology Independence

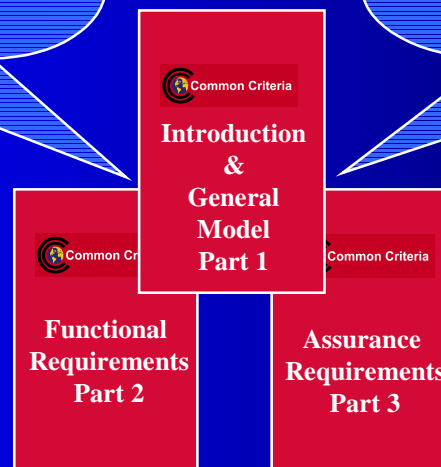
Criteria expressed independent of technology and implementation choices – hardware, software, firmware

## Domain Independence

Criteria is not specific to or optimized for any business or mission case

## Goal Independence

Suitable wherever there is need to articulate security criteria



# The CC is NOT

- ... a process
- ... a methodology

# The Common Criteria (CC)

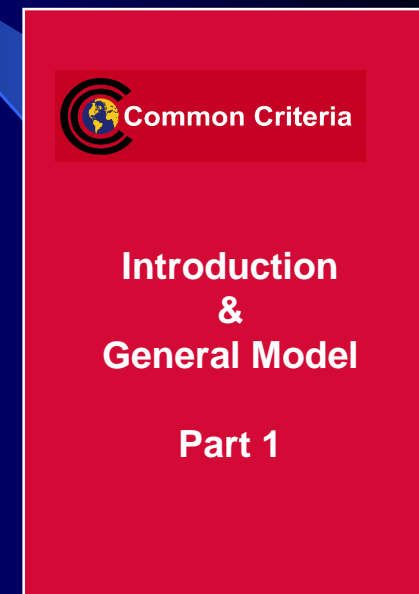
*“Common Criteria for Development of IT Security Specifications”*

- The CC is a meta-standard for development of security specifications
  - defines a requirements specification framework (Part 1)
    - Protection Profile, Security Target, Packages
  - contains criteria used to populate the framework
    - Security Functional Requirements (Part 2)
      - Applicable to any “problem space”
    - Security Assurance Requirements (Part 3)
      - Applicable to any “verification space”

# Specification Constructs

*Protection Profile*

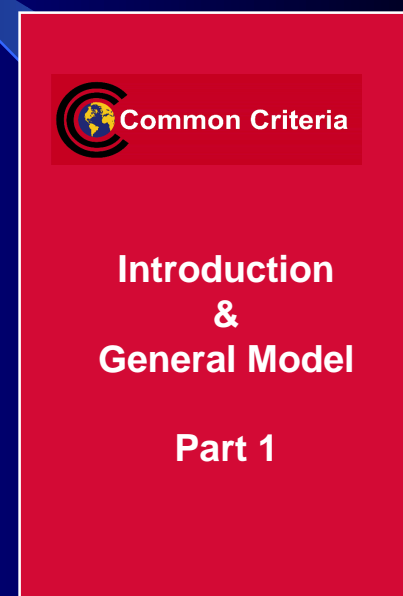
- An implementation-independent security specification that characterizes a security solution
- A means for stakeholders to articulate requirements
  - acquisition, development, integration
  - verification
  - establishment of security standards
  - to meet any need for documenting security requirements



# Specification Constructs

*Security Target*

- An implementation-dependent security specification that reflects the “as-built” or “as-to-be-built” solution
- A means for developers and system integrators to articulate the security requirements of components
  - in response to a PP
  - independent of a PP
- The basis for verification activities



# Specification Constructs

*Packages*

- Reusable specification units
- Used to compose PPs/STs



Common Criteria

Introduction  
&  
General Model

Part 1

# Other CC Terms - 1

- Target of Evaluation (TOE)
  - The IT component(s) and associated administrator and user guidance documentation that is the subject of an evaluation
- TOE Security Policy (TSP)
  - Set of rules that define how resources are managed, protected and distributed by the TOE

# Other CC Terms - 2

- 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

# Other CC Terms - 3

- 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

# Environments Illustrated

Non-IT Environment of  
the Trusted IT Product



Trusted  
IT Product

Unconstrained  
Space

Non-IT Environment  
of the TOE

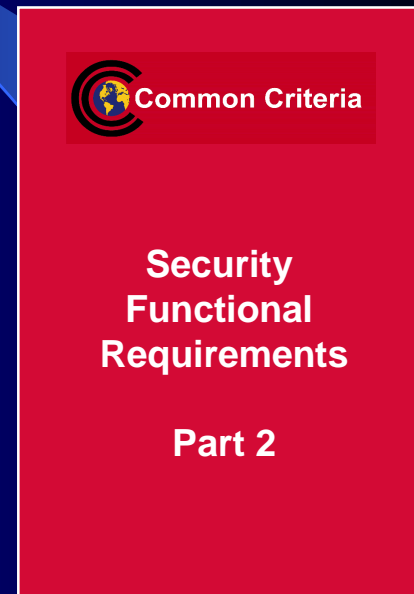


TOE



# Functional Criteria 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)



# Example Functional Requirement

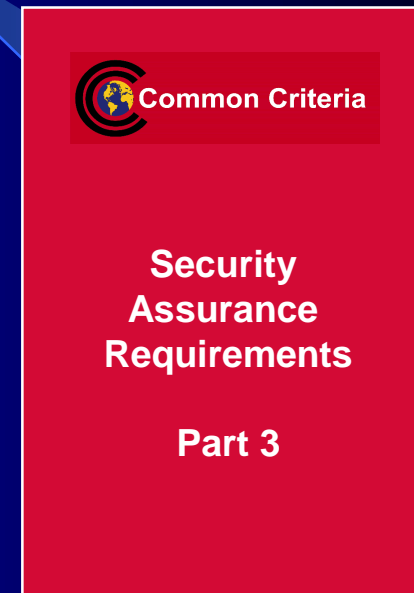
- **FPT\_SEP.2 SFP domain separation**

- FPT\_SEP.2.1 The unisolated portion of the TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.
- FPT\_SEP.2.2 The TSF shall enforce separation between the security domains of subjects in the TSC.
- FPT\_SEP.2.3 The TSF shall maintain the part of the TSF related to [**assignment: *list of access control and/or information flow control SFPs***] in a security domain for their own execution that protects them from interference and tampering by the remainder of the TSF and by subjects untrusted with respect to those SFPs.

# Assurance Criteria Classes

*Component 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)



# Assurance Criteria Classes

*Specification Evaluation*

- PP Evaluation (APE)
- ST Evaluation (ASE)



**Security  
Assurance  
Requirements**

**Part 3**

# CC Specification Philosophy

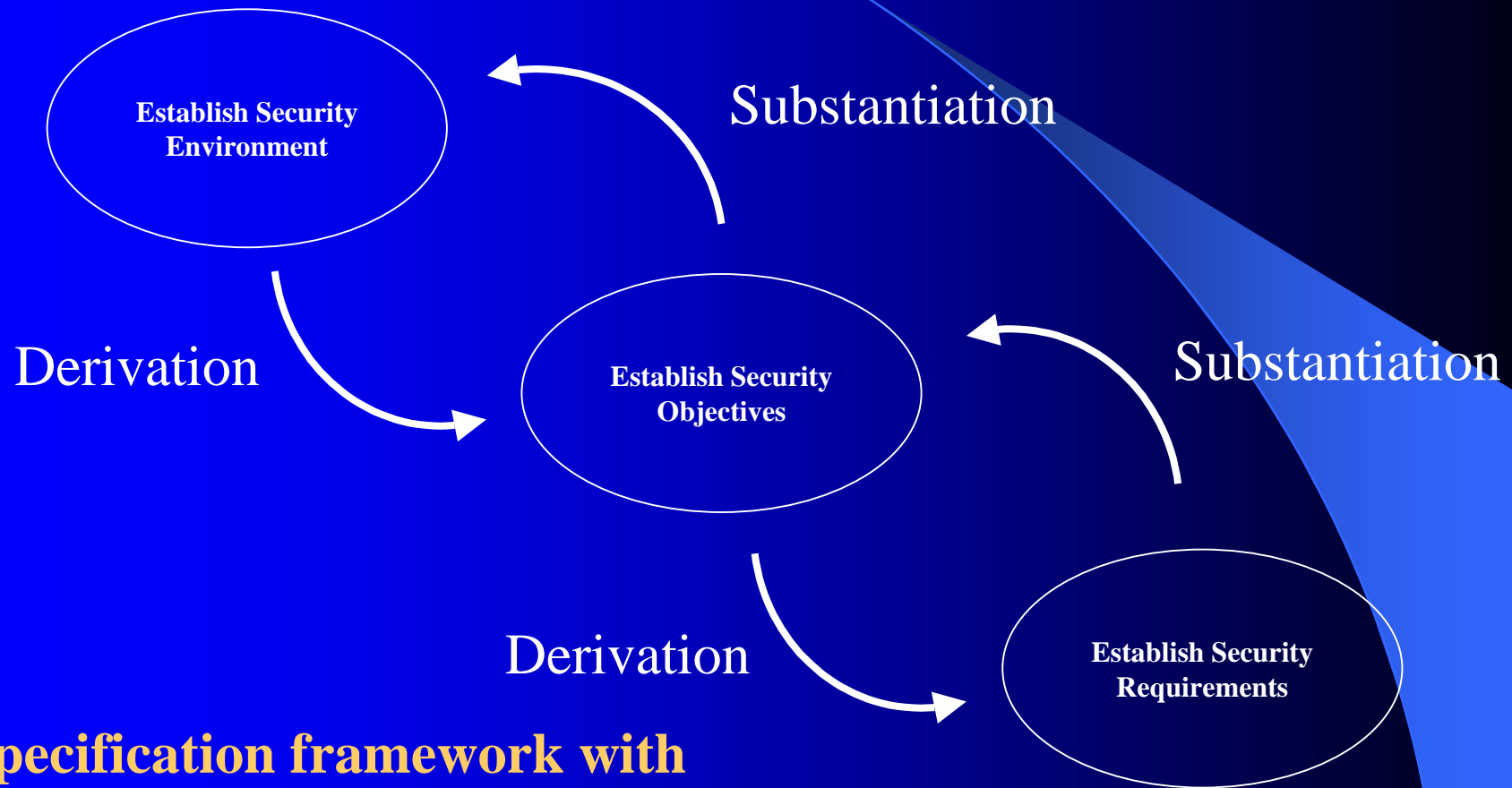
*“One-Stop Shopping”*

- All the information you need to know in one place
  - Security problem definition
  - Security problem solution
  - Substantiation of the appropriateness of the solution
- Information context and volume defined by stakeholders

# Requirement Specification Framework

- Security component description
  - Security component application domain
    - Secure usage assumptions
    - Organizational security policies
    - Threats
  - Security Objectives
  - Security Requirements
    - Functional, Assurance
  - Rationale
- Statement of problem
- Statement of solution
- Substantiation of solution

# Framework Concepts Relationship



**A specification framework with checks and balances to provide end-to-end correctness**

# Applying the CC

Flexibility  
Extensibility  
Scalability



# Operations on Requirements

- Framework-defined operations allow flexibility through tailoring
  - Assignment - Fill-in-the-blank
  - Selection - Multiple choice
  - Iteration - Multiple instantiation
  - Refinement - Elaboration/Customization

# Explicitly Stated Requirements

*“Rolling Your Own Requirements”*

- Component catalogues are extensive but not comprehensive
  - Requirements evolve over time
  - Scope constrained by author focus on evaluation
- 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

# Protection Profile Granularity

Requirement detail granularity is the discretion of the PP author

Abstract  
High Level  
Conceptual  
PP



Capability  
or  
Technology  
Focused  
PP



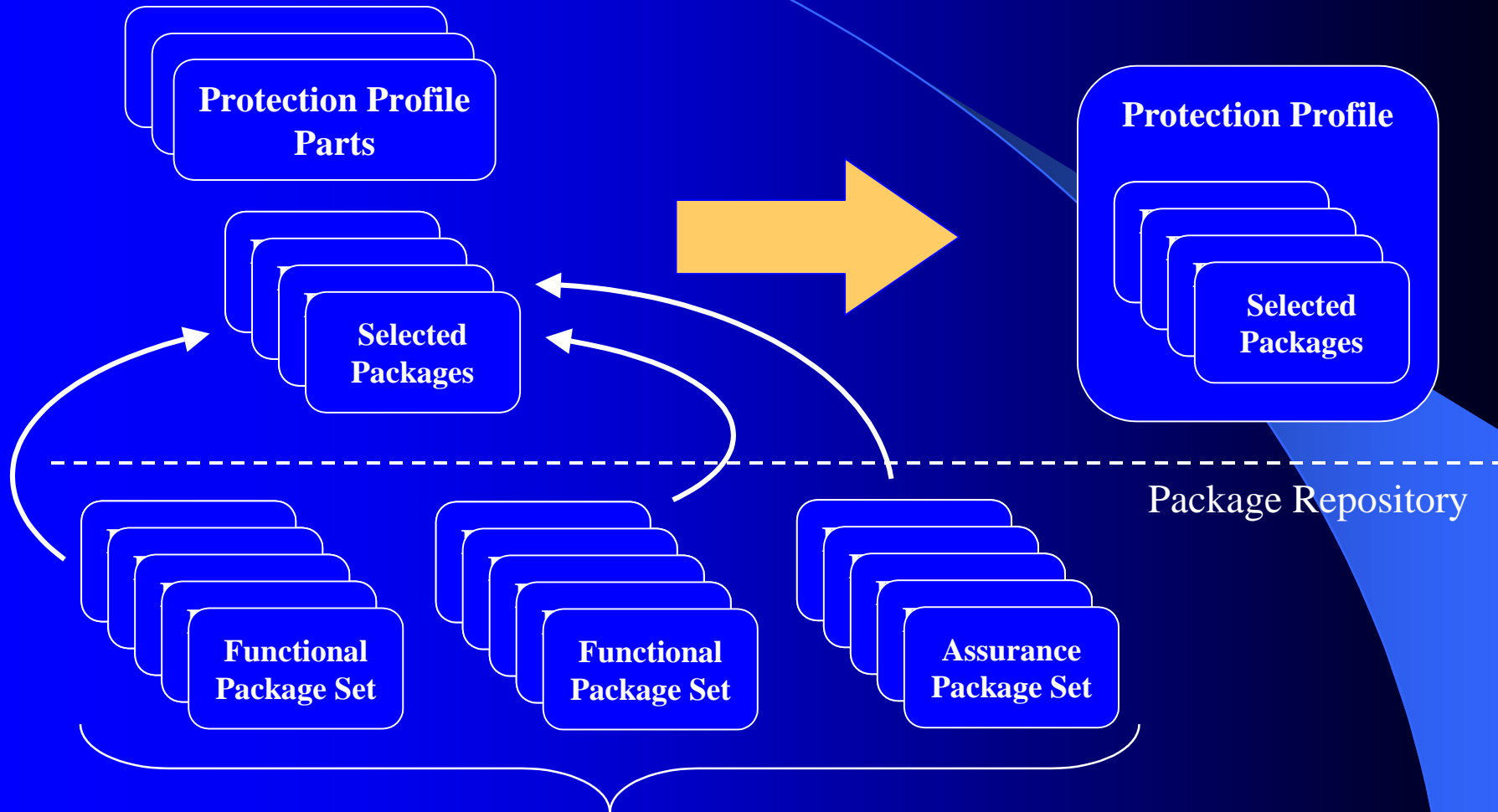
Increasing detail & constraints - less options & flexibility

# Flexibility in the use of PPs

- The CC framework defines correctness of a PP as a complete and static entity
- The CC framework neither mandates its application nor application of developed PPs
- Creative use of the CC framework and resulting PPs can increase the effectiveness of security specifications that support system life-cycle processes

# Conceptual PP Application

*An Illustration*



Repository of functional packages based on mix of component, technology, service or application type or policy or threat environments

# The Weakest Link

## *The IT Security Specification*

- The specification establishes a basis for correctness and provides the means to communicate
- The activities based upon a specification are only as good as the specification
- IT security engineering has typically been a “back end” activity
  - engineer solutions after the foundation is poured
- IT Security engineering starts with development of the security specification
  - aided through leveraging the benefits of the CC

# Practical CC Application

*Truth, Constraints and Issues*

- The CC serves as a communication medium
- The CC may be applied in a practical sense to serve multiple stakeholders
- The CC provides no guidance for its use outside the context of evaluation
- Effective application of the CC in new ways requires
  - complete understanding of its concepts and constructs
  - a strategy for its application

# Practical CC Application

*Strategy and Process*

- Strategy

- What are the objectives to be met?
- How will the document be used?
- Who are the users of the developed documents?
- What information must be captured?

- Process

- First, integrate the CC into existing processes
- Otherwise, define management, development, configuration control and approval processes

# CC Issues

- Orange Book vs. the CC
- Evaluation - myth vs. reality
- Assumptions and the CC
- Composability and the CC

# CC and ISO 15408 Relationship

- CC managed by the Common Criteria Project (CCP)
  - Major release with quarterly updates
- ISO 15048 managed by International Organization for Standardization (ISO)
  - Major release every three years
- The CC and ISO versions “sync-up” upon ISO releases



# Questions?

**Thank you  
for your attention.**

**Michael McEvilley**

703.414.5002 (voice)

703.414.5066 (fax)

[mam@decisive-analytics.com](mailto:mam@decisive-analytics.com)

[www.commoncriteria.com](http://www.commoncriteria.com)

