

Standards for Security Products

CSH5 Chapter 51

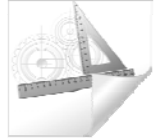
“Security Standards for Products” Paul J. Brusil and Noel Zakin

1

Copyright © 2012 M. E. Kabay. All rights reserved.

Selected Topics in CSH5 Ch 51

- Introduction
- Security assessment standards and security implementation
- Establishing trust and managing risk
- Common criteria paradigm
- Conclusion



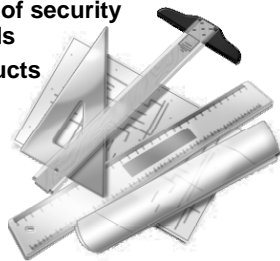
These notes are deliberately limited to focus on highlights of the chapter suitable for the introductory-level undergraduate course IS342 on management of information assurance taught at Norwich University

2

Copyright © 2012 M. E. Kabay. All rights reserved.

Introduction

- IT is vast; security standards essential
- Standards stipulate security needs and requirements
- Standards specify conventions
- Standards ensure interoperability
- Customers can specify level of security and assurance with standards
- Customers can assess products from different vendors with standards



3

Copyright © 2012 M. E. Kabay. All rights reserved.

Security Assessment Standards and Security Implementations

- Security Technology and Product Assessment Standards
- Standards for Assessing Security Implementers
- Combined Product and Product Builder Assessment Standards



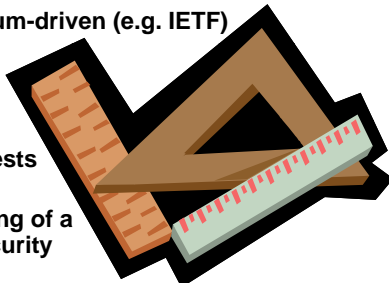
4

Copyright © 2012 M. E. Kabay. All rights reserved.

Security Assessment Standards and Security Implementations (1)

Security Technology and Product Assessment Standards

- Informal, consortium-driven (e.g. IETF)
- Security Proof of Concept Keystone (SPOCK) – NSA sponsored product-specific tests
- VPN consortium – conformance testing of a VPN to IETF IP security standard



5

Copyright © 2012 M. E. Kabay. All rights reserved.

Security Assessment Standards and Security Implementations (2)

Standards for Assessing Security Implementers

- Capability Maturity Model (CMM) family
 - Systems Security Engineering CMM (SSE-CMM) – framework of accepted security principles
- Quality (ISO 9000) – broad assessment of system quality



6

Copyright © 2012 M. E. Kabay. All rights reserved.

Security Assessment Standards and Security Implementations (3)



Combined Product and Product Builder Assessment Standards

- Competing National Standards
 - ❑ TCSEC (Trusted Computing System Evaluation Criteria) – Orange Book, US
 - ❑ ITSEC – EU
 - ❑ CTCSEC – Canada
- Common Consolidated Criteria Standard – New international standard Common Criteria (CC)



7

Copyright © 2012 M. E. Kabay. All rights reserved.

Establishing Trust and Managing Risks Topics



- Why Trust and Risk Management are Important
- Alternative Methods of Establishing Trust
 - ❑ Nonstandard Trust Development Alternatives
 - ❑ Standard-Based Trust Development Alternatives



8

Copyright © 2012 M. E. Kabay. All rights reserved.

Establishing Trust and Managing Risks (1)



Why Trust and Risk Management are Important

- New technology, new business models – players need confidence
- Trust against cyber-terrorism
- Presidential Decision Direction (PDD 63)
- Trust + Risk mitigation = more revenue
- Need Common Criteria paradigm



9

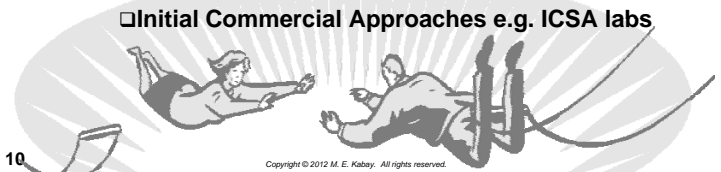
Copyright © 2012 M. E. Kabay. All rights reserved.

Establishing Trust and Managing Risks (2)



Alternative Methods of Establishing Trust

- Nonstandard Trust Development Alternatives
 - ❑ Vendor self-declarations
 - ❑ Proprietary in-house assessments e.g. Smart Card Security Users Group
 - ❑ Hacking (uncertain, unmeasurable)
 - ❑ Open Source e.g. Linux code
 - ❑ Trade press (reviews, recommendations)
 - ❑ Initial Commercial Approaches e.g. ICISA labs



10

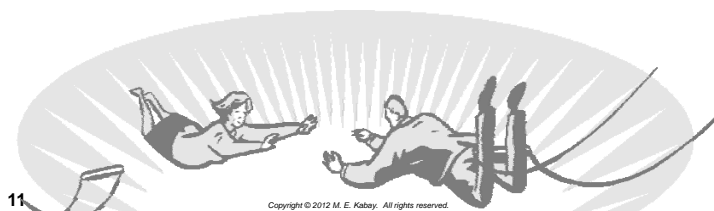
Copyright © 2012 M. E. Kabay. All rights reserved.

Establishing Trust and Managing Risks (3)



Alternative Methods of Establishing Trust contd..

- Standard-Based Trust Development Alternatives
 - ❑ Common Criteria (CC) paradigm



11

Copyright © 2012 M. E. Kabay. All rights reserved.

Common Criteria Paradigm Topics



CC paradigm is a scheme based on formal international standards

- Standards that shape Common Criteria (CC)
- Details about the CC
- Using CC to define security requirements and solutions
- Defining common text methodology
- Mutual recognition of testing and national testing schemes
- CC evaluation and validation scheme (CCEVS) of the US



12

Copyright © 2012 M. E. Kabay. All rights reserved.

Common Criteria Paradigm Topics (cont'd)



- Accredited testing
- Testing validation
- Recognizing validated products and profiles
- Summary of CC



13

Copyright © 2012 M. E. Kabay. All rights reserved.

Common Criteria Paradigm (1)



Standards that Shape CC Paradigm

- CC for Information Technology Security Evaluation
- Common Evaluation Methodology
- Mutual Recognition Agreement (MRA)
- CC Evaluation & Validation Scheme (CCEVS)



14

Copyright © 2012 M. E. Kabay. All rights reserved.

Common Criteria Paradigm (2)



Details about the CC Standard

- Models for Security Profiles
 - Protection Profile (PP)
 - Security Target (ST)
- Security Functional Requirements Catalog
 - 11 classes
- Security Assurance Requirements Catalog
 - 10 classes
- Requirements catalogs are comprehensive



15

Copyright © 2012 M. E. Kabay. All rights reserved.

Common Criteria Paradigm (3)



Using CC Standard to Define Security Requirements and Solutions (1)

- Constructing a protection profile (PP) - PP states security problem that product will solve.
- Steps involved in constructing PP
 - Identify threats, vulnerabilities (use CVE* & NVD**)
 - Describe operational environment
 - Enumerate policies
 - Set security objectives for product and environment



* <http://cve.mitre.org/cve/>
 ** <http://nvd.nist.gov/>

16

Common Criteria Paradigm (4)



Using CC Standard to Define Security Requirements and Solutions (2)

- Steps involved in constructing a PP (cont'd)
 - Refine security requirements from CC catalogs
 - Select assurance requirements from assurance catalog
 - Give rationale for all decisions and choices made in constructing a PP
 - Reuse existing PP if possible



17

Copyright © 2012 M. E. Kabay. All rights reserved.

Common Criteria Paradigm (5)



Using CC Standard to Define Security Requirements and Solutions (3)

- Security Targets (ST) – to document product security information
 - Steps involved in constructing an ST
 - Describe environment of product
 - Enumerate threats, policies, laws etc.
 - Delineate security objectives
 - Enumerate security requirements addressed
 - Give rationale for all decisions and choices
- So far, STs are like PPs*



18

Copyright © 2012 M. E. Kabay. All rights reserved.

Common Criteria Paradigm (6)



Using CC Standard to Define Security Requirements and Solutions (4)

- STs go beyond PPs because they:
 - ❑ Specify security functions offered to meet security requirements
 - ❑ Specify assurance measures taken to meet assurance requirements
 - ❑ Can conform to more than one PP
- STs beneficial – complete, unambiguous
- PP/ST development tools available



19

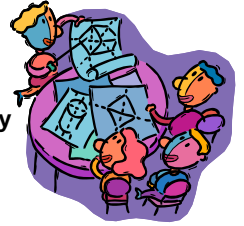
Copyright © 2012 M. E. Kabay. All rights reserved.

Common Criteria Paradigm (7)



Defining Common Text Methodology

- Common Evaluation Methodology (CEM)
 - ❑ Two-part standard
 - ❑ Part 1: general model, evaluation process, roles of stakeholders
 - ❑ Part 2: complete methodology information on general evaluation tasks
- Benefits of CEM
 - ❑ Common base for product assessment
 - ❑ Common floor of operational confidence



20

Copyright © 2012 M. E. Kabay. All rights reserved.

Common Criteria Paradigm (8)



Mutual Recognition of Testing and National Testing Schemes

- Mutual Recognition Arrangement (MRA)
 - ❑ Identifies conditions for mutual recognition of testing, validation, and certification among countries
 - ❑ Rooted in use of CC and CEM
- National schemes
 - ❑ Countries agreeing to the MRA have their own schemes



21

Copyright © 2012 M. E. Kabay. All rights reserved.

Common Criteria Paradigm (9)



Common Criteria Evaluation Scheme of the United States

- Purpose
 - ❑ Establish and maintain quality of CC-based security testing, validation, certification infrastructure
 - ❑ Define policies, procedures, processes for CC-based, MRA-recognized security testing, validation, certification
- See next slide for screen shot
 - ❑ <http://www.niap-ccavs.org/>

22

Copyright © 2012 M. E. Kabay. All rights reserved.

The screenshot shows the NIAP website with several sections:

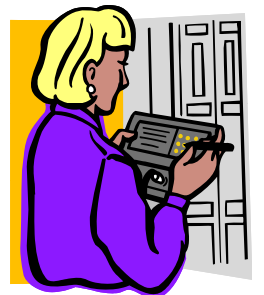
- CCAVS Big Picture**: Announcements, CCEVS Objectives, CC Testing Labs (CCTL), Candidate CCTLs, CCEVS Interpretations, CCEVS Validation Body, CORA and Partners, Defining the CCEVS, Evaluation/Validation Primer, Events, Guidance to Consumers, Historical Perspective, Terms and Acronyms.
- CCAVS Products**: Products in Evaluation, U.S. Government Approved Protection Profiles, U.S. Government Protection Profiles in Development, Validated Products List.
- Docs & Guidance**: CC/CBM Documentation, Consistency Instruction Manuals, FAQs, Forms and Templates, LabOrams, PP Development Process, Scheme Policy Letters, Scheme Publications, VOR Schedule.
- CCPP User's Links**: Common Criteria Portal, International Interop Database.
- Web Site Updates (22 January 2014)**:
 - NIAP POLICY LETTER UPDATES**: The NIAP Program Office updated the Scheme Policy Letters. Click here for a summary of the updates. Click here to view the current Policy Letters.
 - PROTECTION PROFILE UPDATES**: Click here for the latest Protection Profile status.
 - OTHER INFORMATION**: Previous announcements, Questions and Answers on the IBAP's Evolution (21 October 2009).
- Available products to assist in making a more secure infrastructure**: Validated Products List.
- Boosting consumer confidence through evaluation and testing of vendor products**: Finding a CCTL, Getting a CCTL Accredited, Getting a Product Evaluated.
- Policy that influences our adherence to the Common Criteria**: CCEVS Directive #502, DOD Directive #500.01E, DOD Directive #500.01, DOD Instruction #500.2, NISTOSP No. 11, Revised FAQs (March 2005).

Common Criteria Paradigm (10)



Accredited Testing

- Testing products and profiles
 - ❑ Benefits of accredited testing and evaluation
 - ❑ Helping customers
 - ❑ Preparing for testing
 - ❑ Conducting testing
 - ❑ Testing oversight
- Accrediting security testing laboratories
 - ❑ What is accreditation?
 - ❑ Benefits of accreditation



24

Copyright © 2012 M. E. Kabay. All rights reserved.

Common Criteria Paradigm (11)



Testing Validation

- Validating test results
 - ❑ Security assessment conforms to CCEVS
 - ❑ Conclusions follow from evidence
 - ❑ CC and CEM applied correctly
- Operating and maintaining the validation service
 - ❑ NIAP validation body conducts validation
 - ❑ Develops report
 - ❑ Bestows validated product status



25

Copyright © 2012 M. E. Kabay. All rights reserved.

Common Criteria Paradigm (12)



Recognizing Validated Products and Profiles

- Issue CC certificates to confirm evaluation
- Posting validations – validated profiles placed in a national registry of PPs



26

Copyright © 2012 M. E. Kabay. All rights reserved.

Common Criteria Paradigm Summary



- CC paradigm a powerful, flexible, standards-based mechanism
- Facilitates defining IT security and confidence requirements
- Facilitates stipulating IT product security specifications
- Facilitates testing and test verification
- Provides cost-effective value
- Helps users understand risks, vulnerabilities
- Assures better-engineered, more acceptable products



27

Copyright © 2012 M. E. Kabay. All rights reserved.

Review Questions: Extra credit for posting responses to NUoodle Discussion Board



1. Why do we use standards for security products?
2. Compare and contrast alternatives to formal standards for security certification of products.
3. Outline the history of security standards leading to the Common Criteria
4. Summarize the components of the CC framework.

28

Copyright © 2012 M. E. Kabay. All rights reserved.

Extra points available



- For 10 extra points added to your quiz-points total
- Use the Kreitzberg Library, Google Scholar, and the WWW to research current industry views about the *Common Criteria*
- Write a 1 page report (500 ± 50 words) on findings
 - ❑ Single-spaced, following guidelines for essays
 - ❑ Put following in UPPER RIGHT CORNER of report:
Your Name
Common Criteria Today
IS342
- Upload the DOCX, DOC, RTF or ODT file to NUoodle in the upload function available in this week's section
- Submit by the deadline shown in NUoodle

29

Copyright © 2012 M. E. Kabay. All rights reserved.

DISCUSSION



30

Copyright © 2012 M. E. Kabay. All rights reserved.