



# Information Security Evaluation Criteria

Prof. Joon S. Park, Ph.D

School of Information Studies

Syracuse University



# Security Evaluation

- ◆ Product Evaluation
  - ITSEC, TCSEC, CC, etc.
  - Expensive (time & cost)
- ◆ Engineering Process Evaluation
  - SPICE, CMM, etc.
  - Save cost for product evaluation



# TCSEC

- ◆ Known as Orange Book, DoD 5200.28-STD
- ◆ Four trust rating divisions (classes)
  - D: Minimal protection
  - C (C1,C2): Discretionary protection
  - B (B1, B2, B3): Mandatory protection
  - A (A1): Highly-secure



# Common Criteria

- ◆ CC is the outcome of a series of effort to develop criteria for evaluation of IT security
- ◆ The International Organization for Standardization (ISO) has developed a set of international standard security evaluation criteria
- ◆ It opens the way to worldwide mutual recognition of evaluation results
- ◆ The CC defines seven Evaluation Assurance Levels (EALs) for ranking the criteria.



# Security Functionality Classes in CC

- ◆ Audit (FAU)
- ◆ Cryptography Support (FCS)
- ◆ Communications (FCO)
- ◆ User Data Protection (FDP)
- ◆ Identification and Authentication (FIA)
- ◆ Security Management (FMT)
- ◆ Privacy (FPR)
- ◆ Protection of the TOE Security Functions (FPT)
- ◆ Resource Utilisation (FRU)
- ◆ TOE Access (FTA)
- ◆ Trusted Path/Channels (FTP)



# Examples of CC Certified Products

- ◆ Oracle 8 Release 8.1.7: EAL4, Oracle Corporation Certified in 2001/07
- ◆ Symantec Enterprise Firewall v7.0: EAL4, Symantec, Certified in 2002/05
- ◆ Gemplus 64k Java Card™: EAL5, Gemplus, Certified in 2002/02
- ◆ Many other products



# Common Criteria

- ◆ The security properties of the Target of Evaluation (TOE) are captured in the Protection Profile (PP) and Security Target (ST)
  - PP
    - An implementation-independent set of security requirements for a category of TOEs (goal specification)
    - intended to be reusable
    - Written by anyone who wants to state IT security needs
  - ST
    - An implementation-dependent set of security requirements and specifications used as the basis for evaluation of the identified TOE (~as-built specification)
    - Written by vendors, developers, integrators (with knowledge of implementation details)



# Common Criteria

- ◆ The usefulness of CC depends on the quality of PP and ST
  - However, the process for writing a good PP and ST has not been thoroughly described
  - The CC provides only limited guidance on how to write PPs and STs
- ◆ It is not easy to understanding the CC document in one reading
  - Consumers, developers and assessors may have a lot of questions about CC evaluations because of the lack of concise information about using the CC



# SSE-CMM (1995)

- ◆ Intended to be used
  - to evaluate an organization (provider)'s security engineering process
- ◆ Covers
  - Entire life cycle
    - Requirements analysis, development, installation, operation, maintenance, etc.
  - Current interactions with other disciplines
    - Hardware, software, test, management, other organizations, etc.
- ◆ Defines
  - Capability dimension (applied to all processes)
    - five capability levels of generic practices
  - Domain dimension
    - 11 groups of security base practices
    - 11 groups of project and organizational practices

