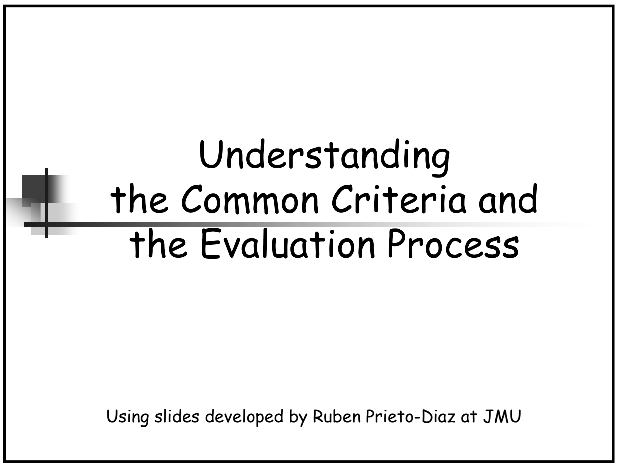
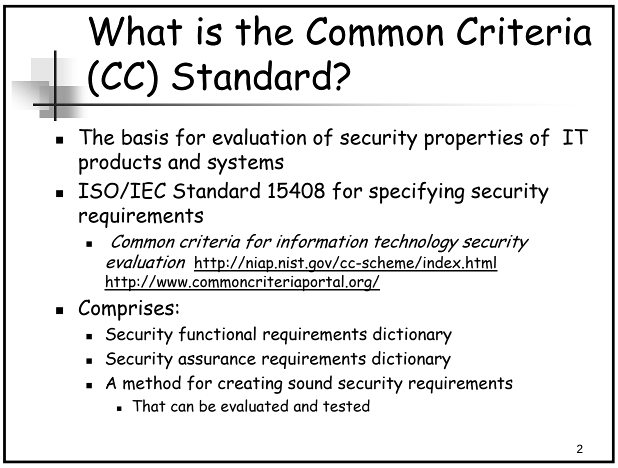


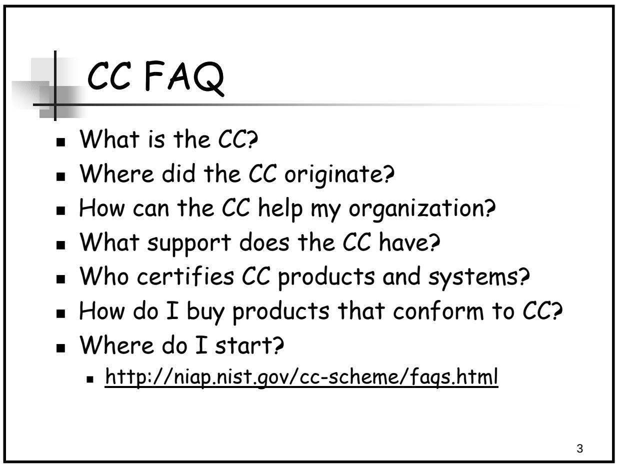
Understanding the Common Criteria and the Evaluation Process

Using slides developed by Ruben Prieto-Diaz at JMU



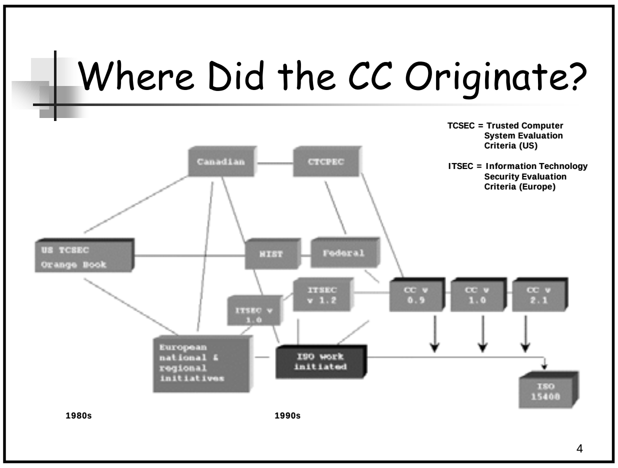
What is the Common Criteria (CC) Standard?

- The basis for evaluation of security properties of IT products and systems
- ISO/IEC Standard 15408 for specifying security requirements
  - *Common criteria for information technology security evaluation* http://niap.nist.gov/cc-scheme/index.html http://www.commoncriteriaportal.org/
- Comprises:
  - Security functional requirements dictionary
  - Security assurance requirements dictionary
  - A method for creating sound security requirements
    - That can be evaluated and tested



CC FAQ

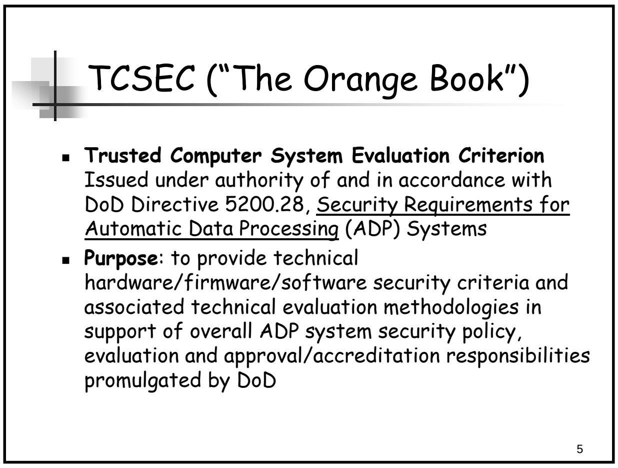
- What is the CC?
- Where did the CC originate?
- How can the CC help my organization?
- What support does the CC have?
- Who certifies CC products and systems?
- How do I buy products that conform to CC?
- Where do I start?
  - http://niap.nist.gov/cc-scheme/faqs.html



Where Did the CC Originate?

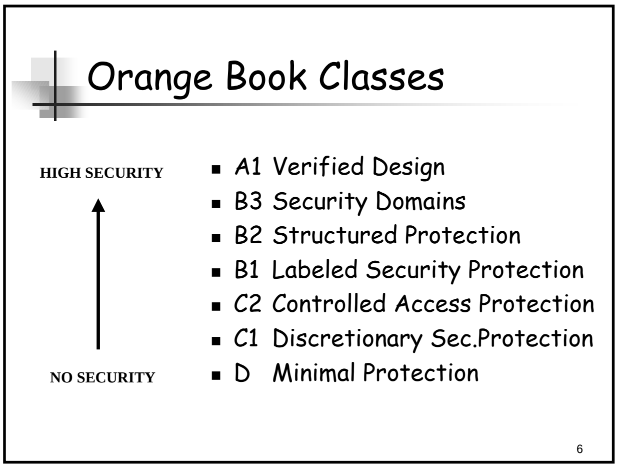
TCSEC = Trusted Computer System Evaluation Criteria (US)

ITSEC = Information Technology Security Evaluation Criteria (Europe)



TCSEC ("The Orange Book")

- **Trusted Computer System Evaluation Criterion** Issued under authority of and in accordance with DoD Directive 5200.28, Security Requirements for Automatic Data Processing (ADP) Systems
- **Purpose**: to provide technical hardware/firmware/software security criteria and associated technical evaluation methodologies in support of overall ADP system security policy, evaluation and approval/accreditation responsibilities promulgated by DoD

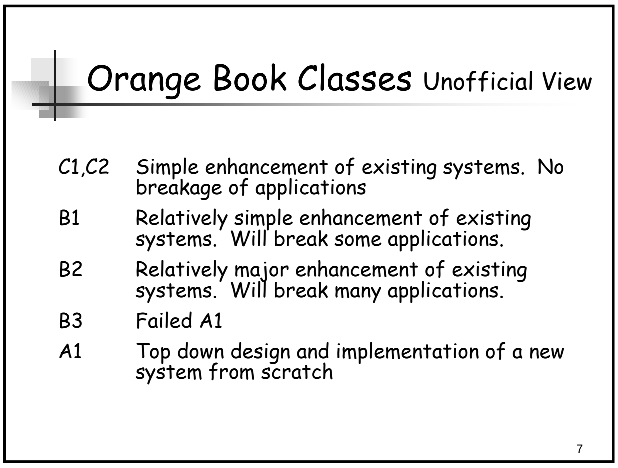


Orange Book Classes

HIGH SECURITY

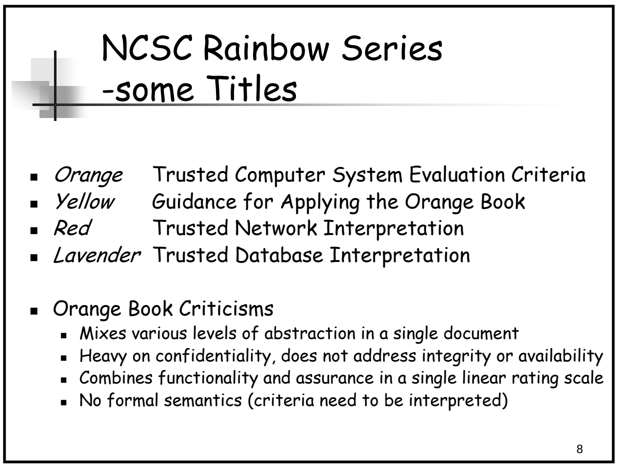
NO SECURITY

- A1 Verified Design
- B3 Security Domains
- B2 Structured Protection
- B1 Labeled Security Protection
- C2 Controlled Access Protection
- C1 Discretionary Sec.Protection
- D Minimal Protection



Orange Book Classes Unofficial View

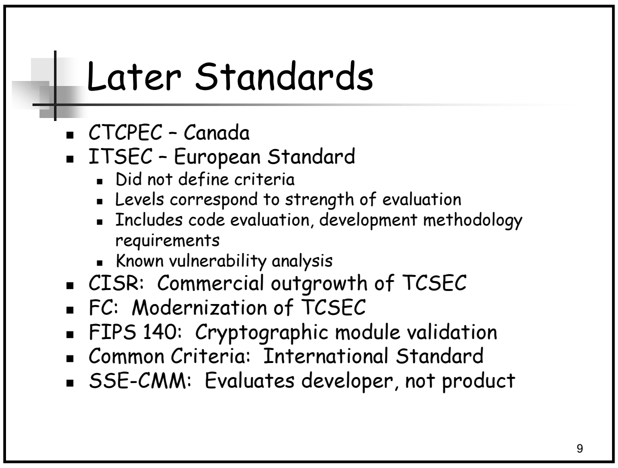
C1,C2	Simple enhancement of existing systems. No breakage of applications
B1	Relatively simple enhancement of existing systems. Will break some applications.
B2	Relatively major enhancement of existing systems. Will break many applications.
B3	Failed A1
A1	Top down design and implementation of a new system from scratch



NCSC Rainbow Series -some Titles

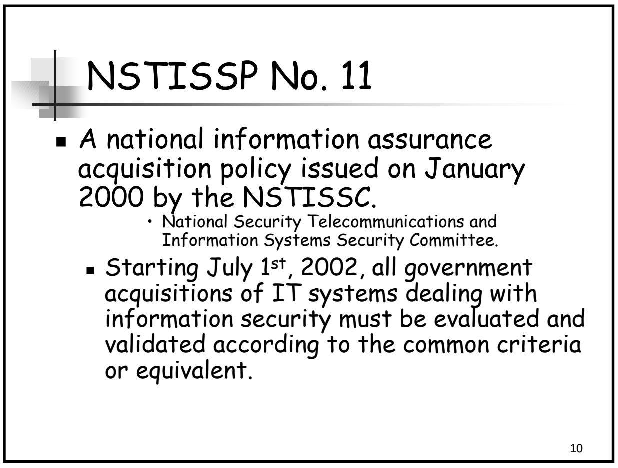
Orange	Trusted Computer System Evaluation Criteria
Yellow	Guidance for Applying the Orange Book
Red	Trusted Network Interpretation
Lavender	Trusted Database Interpretation

- Orange Book Criticisms
  - Mixes various levels of abstraction in a single document
  - Heavy on confidentiality, does not address integrity or availability
  - Combines functionality and assurance in a single linear rating scale
  - No formal semantics (criteria need to be interpreted)



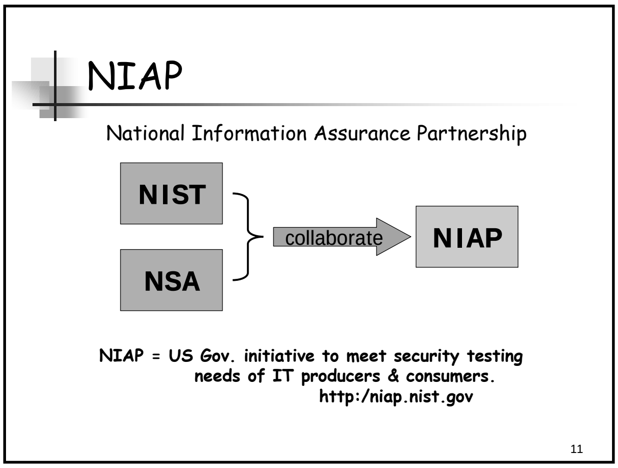
Later Standards

- CTCPEC – Canada
- ITSEC – European Standard
  - Did not define criteria
  - Levels correspond to strength of evaluation
  - Includes code evaluation, development methodology requirements
  - Known vulnerability analysis
- CISR: Commercial outgrowth of TCSEC
- FC: Modernization of TCSEC
- FIPS 140: Cryptographic module validation
- Common Criteria: International Standard
- SSE-CMM: Evaluates developer, not product



NSTISSP No. 11

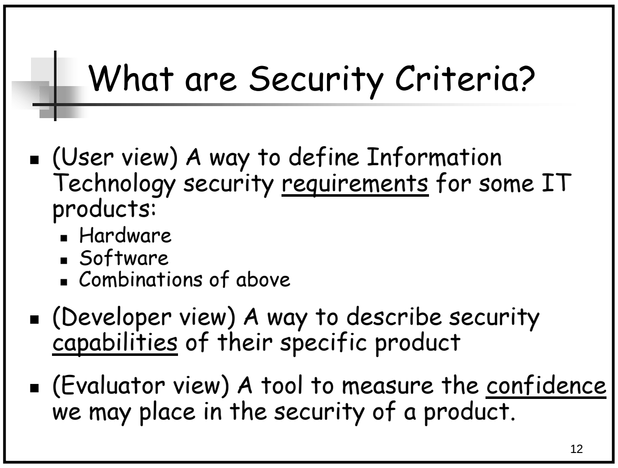
- A national information assurance acquisition policy issued on January 2000 by the NSTISSC.
    - National Security Telecommunications and Information Systems Security Committee.
  - Starting July 1st, 2002, all government acquisitions of IT systems dealing with information security must be evaluated and validated according to the common criteria or equivalent.



NIAP

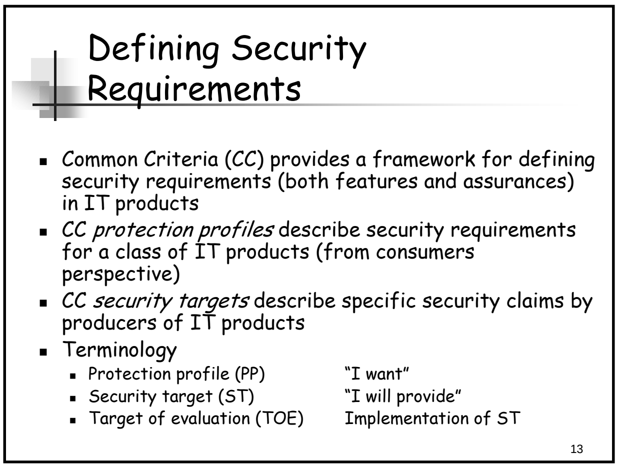
National Information Assurance Partnership

NIAP = US Gov. initiative to meet security testing needs of IT producers & consumers.
http:/niap.nist.gov



What are Security Criteria?

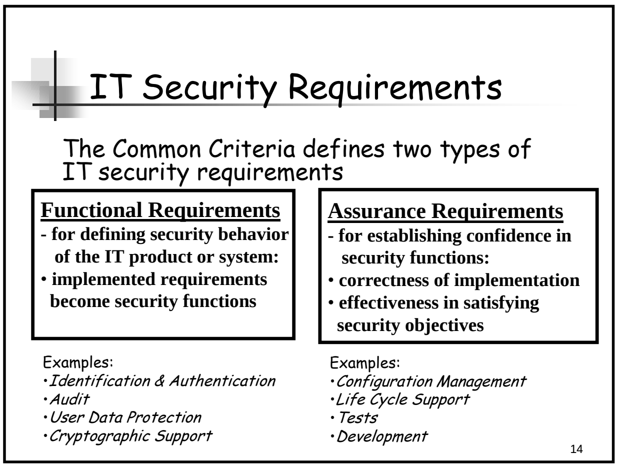
- (User view) A way to define Information Technology security <u>requirements</u> for some IT products:
  - Hardware
  - Software
  - Combinations of above
- (Developer view) A way to describe security <u>capabilities</u> of their specific product
- (Evaluator view) A tool to measure the <u>confidence</u> we may place in the security of a product.



Defining Security Requirements

- Common Criteria (CC) provides a framework for defining security requirements (both features and assurances) in IT products
- *CC protection profiles* describe security requirements for a class of IT products (from consumers perspective)
- *CC security targets* describe specific security claims by producers of IT products
- Terminology

Protection profile (PP)	"I want"
Security target (ST)	"I will provide"
Target of evaluation (TOE)	Implementation of ST



IT Security Requirements

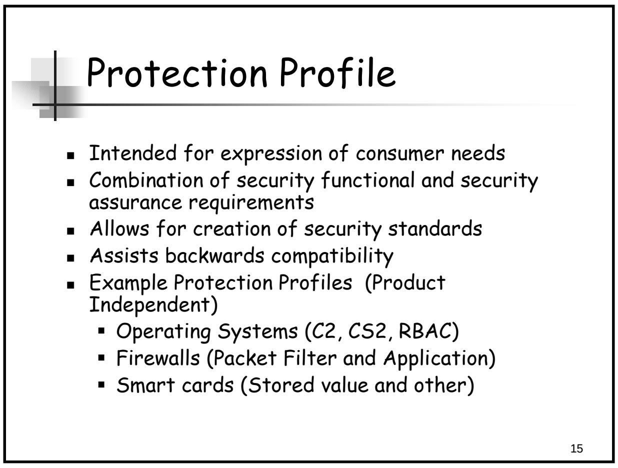
The Common Criteria defines two types of IT security requirements

Functional Requirements
- for defining security behavior of the IT product or system:
• implemented requirements become security functions

Examples:
- *Identification & Authentication*
- *Audit*
- *User Data Protection*
- *Cryptographic Support*

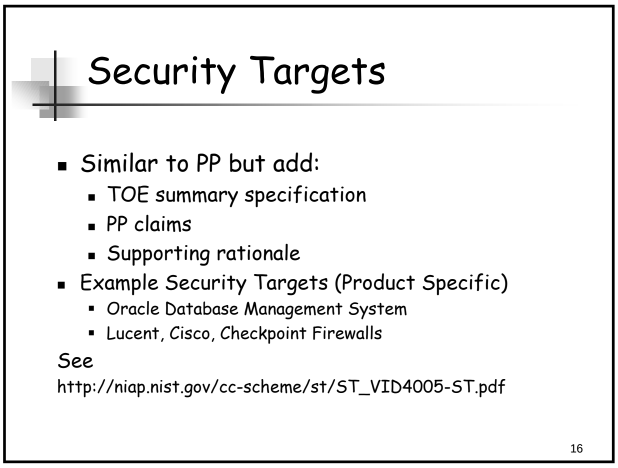
Assurance Requirements
- for establishing confidence in security functions:
• correctness of implementation
• effectiveness in satisfying security objectives

Examples:
- *Configuration Management*
- *Life Cycle Support*
- *Tests*
- *Development*



Protection Profile

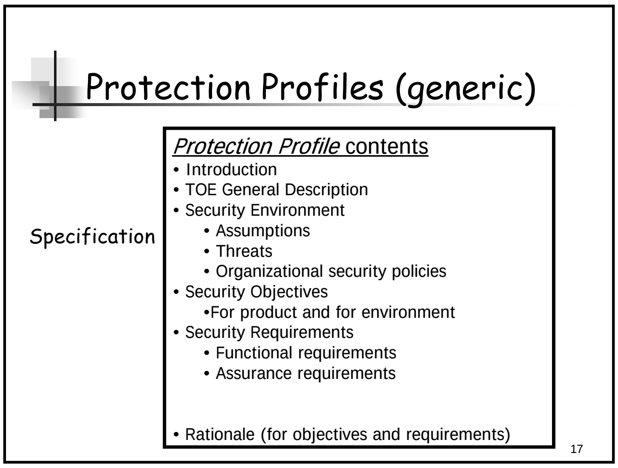
- Intended for expression of consumer needs
- Combination of security functional and security assurance requirements
- Allows for creation of security standards
- Assists backwards compatibility
- Example Protection Profiles (Product Independent)
  - Operating Systems (C2, CS2, RBAC)
  - Firewalls (Packet Filter and Application)
  - Smart cards (Stored value and other)



Security Targets

- Similar to PP but add:
  - TOE summary specification
  - PP claims
  - Supporting rationale
- Example Security Targets (Product Specific)
  - Oracle Database Management System
  - Lucent, Cisco, Checkpoint Firewalls

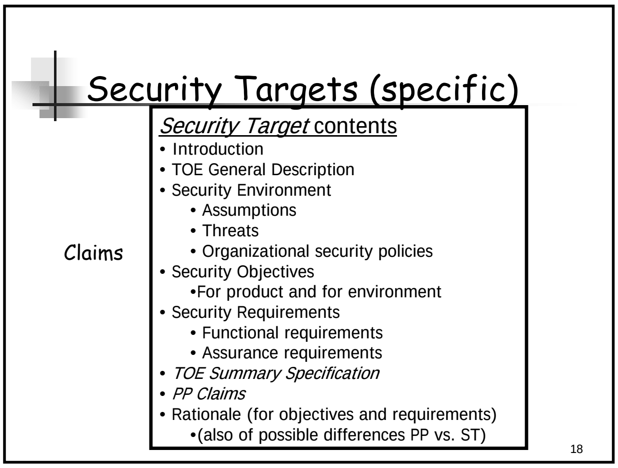
See
http://niap.nist.gov/cc-scheme/st/ST_VID4005-ST.pdf



Protection Profiles (generic)

Specification

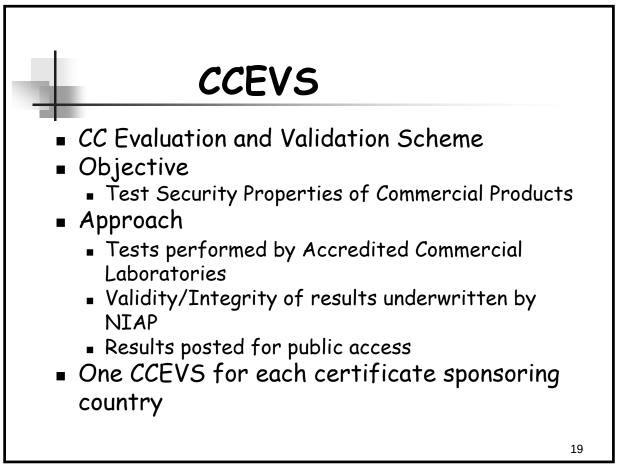
Protection Profile contents
- Introduction
- TOE General Description
- Security Environment
  - Assumptions
  - Threats
  - Organizational security policies
- Security Objectives
  - For product and for environment
- Security Requirements
  - Functional requirements
  - Assurance requirements
- Rationale (for objectives and requirements)



Security Targets (specific)

Claims

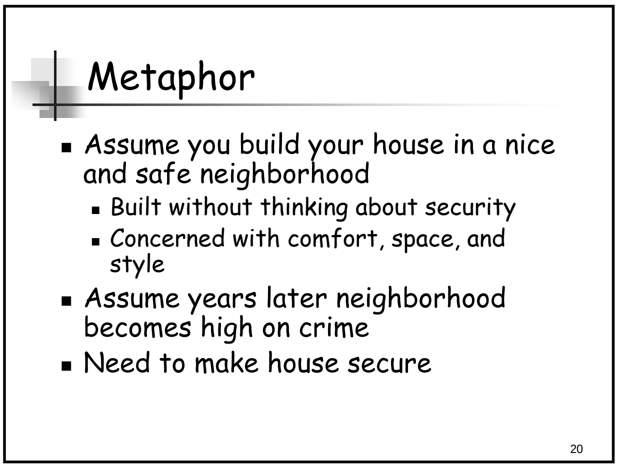
Security Target contents
- Introduction
- TOE General Description
- Security Environment
  - Assumptions
  - Threats
  - Organizational security policies
- Security Objectives
  - For product and for environment
- Security Requirements
  - Functional requirements
  - Assurance requirements
- *TOE Summary Specification*
- *PP Claims*
- Rationale (for objectives and requirements)
  - (also of possible differences PP vs. ST)



CCEVS

- *CC Evaluation and Validation Scheme*
- Objective
  - Test Security Properties of Commercial Products
- Approach
  - Tests performed by Accredited Commercial Laboratories
  - Validity/Integrity of results underwritten by NIAP
  - Results posted for public access
- One CCEVS for each certificate sponsoring country

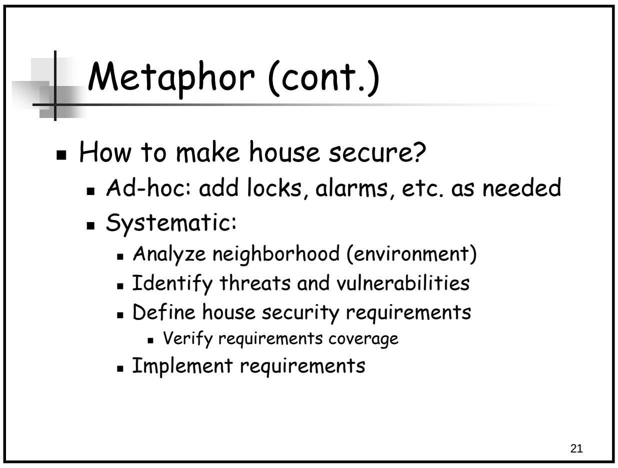
19



Metaphor

- Assume you build your house in a nice and safe neighborhood
  - Built without thinking about security
  - Concerned with comfort, space, and style
- Assume years later neighborhood becomes high on crime
- Need to make house secure

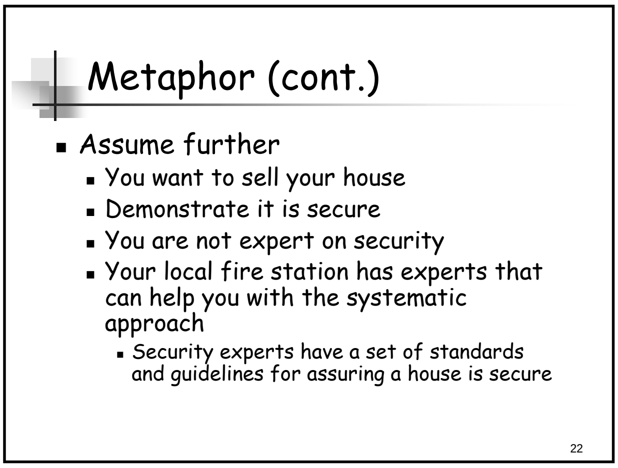
20



Metaphor (cont.)

- How to make house secure?
  - Ad-hoc: add locks, alarms, etc. as needed
  - Systematic:
    - Analyze neighborhood (environment)
    - Identify threats and vulnerabilities
    - Define house security requirements
      - Verify requirements coverage
    - Implement requirements

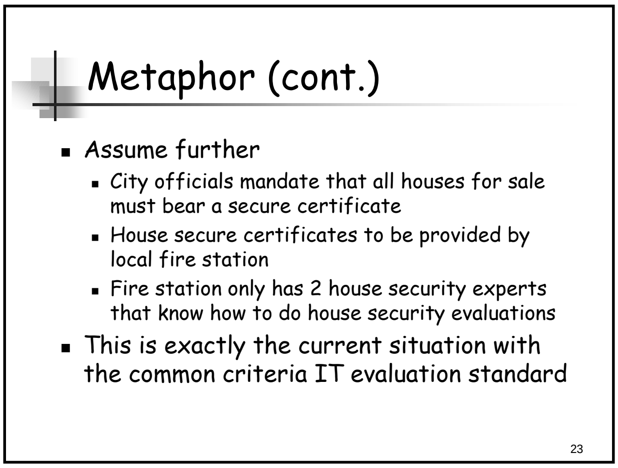
21



Metaphor (cont.)

- Assume further
  - You want to sell your house
  - Demonstrate it is secure
  - You are not expert on security
  - Your local fire station has experts that can help you with the systematic approach
    - Security experts have a set of standards and guidelines for assuring a house is secure

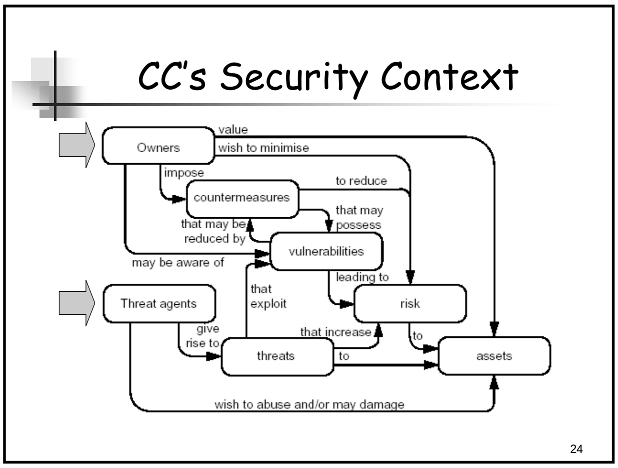
22



Metaphor (cont.)

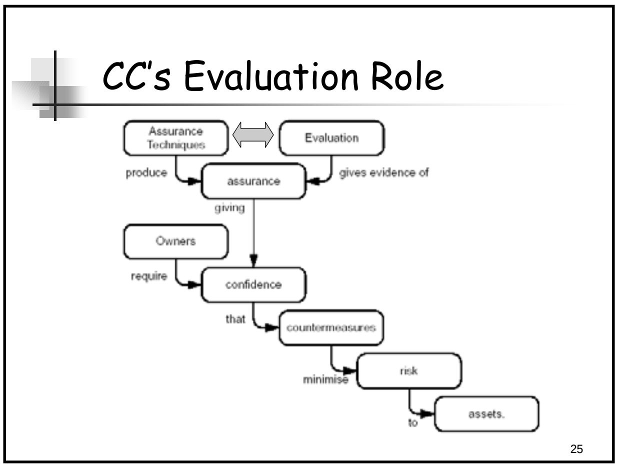
- Assume further
  - City officials mandate that all houses for sale must bear a secure certificate
  - House secure certificates to be provided by local fire station
  - Fire station only has 2 house security experts that know how to do house security evaluations
- This is exactly the current situation with the common criteria IT evaluation standard

23



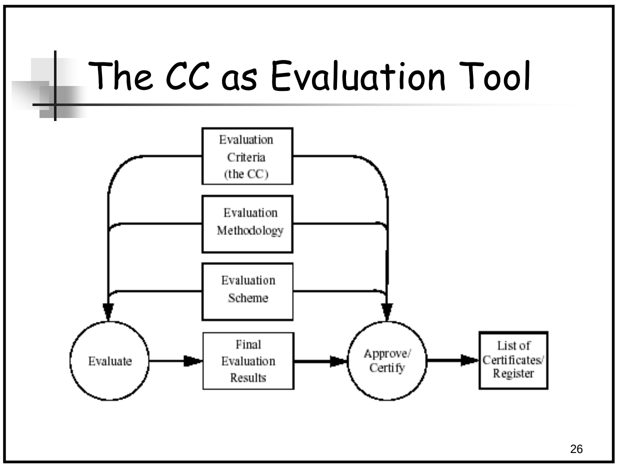
CC's Security Context

24



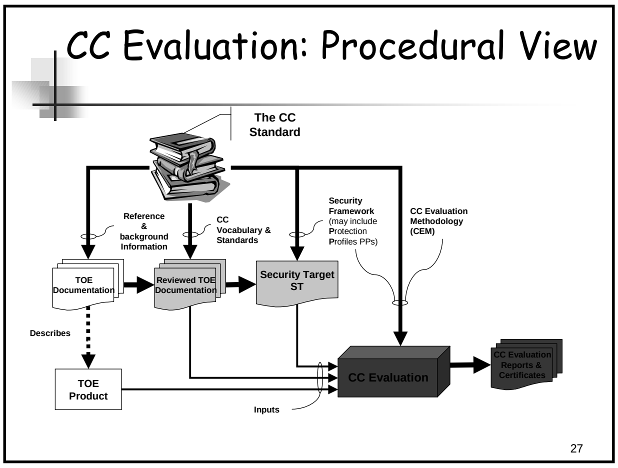
CC's Evaluation Role

25



The CC as Evaluation Tool

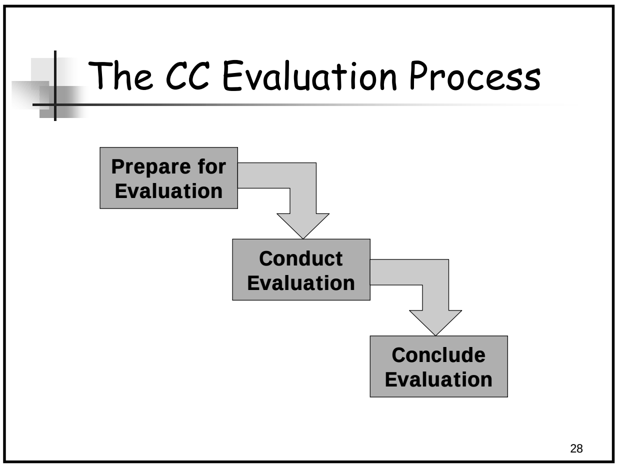
26



CC Evaluation: Procedural View

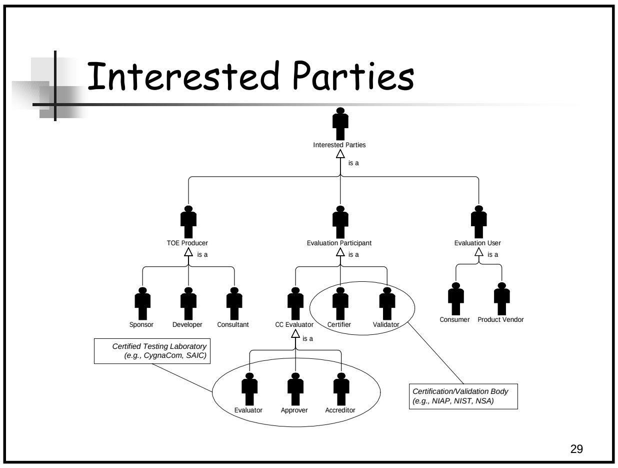
The CC Standard
Reference & background Information
CC Vocabulary & Standards
Security Framework (may include Protection Profiles PPs)
CC Evaluation Methodology (CEM)
TOE Documentation
Reviewed TOE Documentation
Security Target ST
Describes
TOE Product
CC Evaluation
CC Evaluation Reports & Certificates
Inputs

27



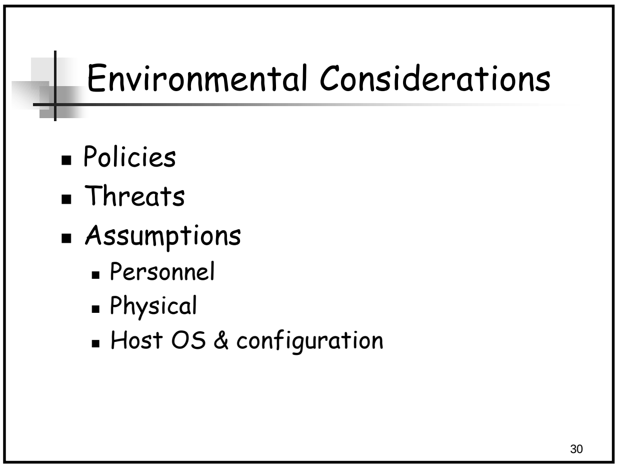
The CC Evaluation Process

28



Interested Parties

29

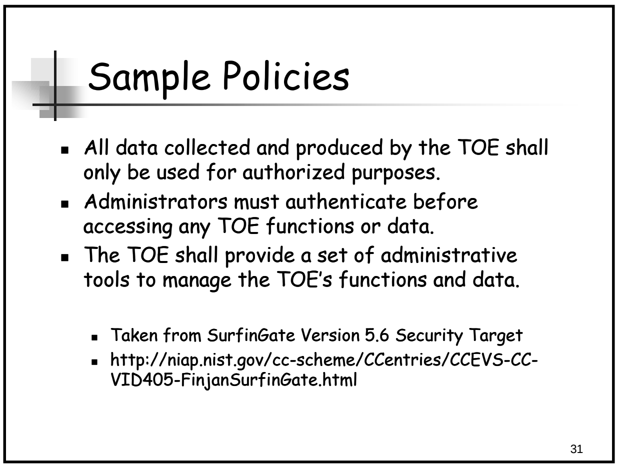


Environmental Considerations

- Policies
- Threats
- Assumptions
  - Personnel
  - Physical
  - Host OS & configuration

30

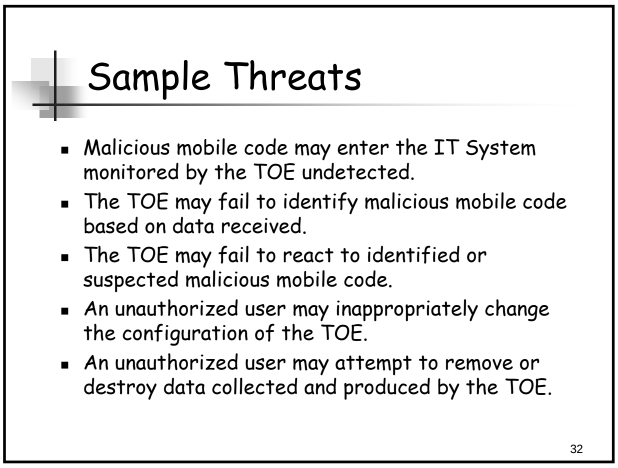
Based on slides by Ruben Prieto-Diaz



Sample Policies

- All data collected and produced by the TOE shall only be used for authorized purposes.
- Administrators must authenticate before accessing any TOE functions or data.
- The TOE shall provide a set of administrative tools to manage the TOE's functions and data.
  - Taken from SurfinGate Version 5.6 Security Target
  - http://niap.nist.gov/cc-scheme/CCentries/CCEVS-CC-VID405-FinjanSurfinGate.html

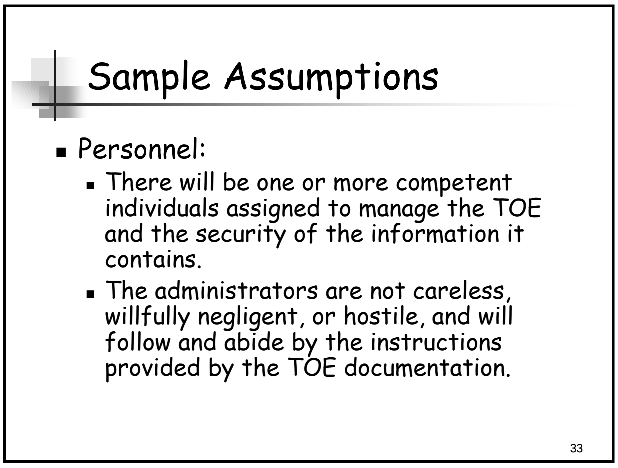
31



Sample Threats

- Malicious mobile code may enter the IT System monitored by the TOE undetected.
- The TOE may fail to identify malicious mobile code based on data received.
- The TOE may fail to react to identified or suspected malicious mobile code.
- An unauthorized user may inappropriately change the configuration of the TOE.
- An unauthorized user may attempt to remove or destroy data collected and produced by the TOE.

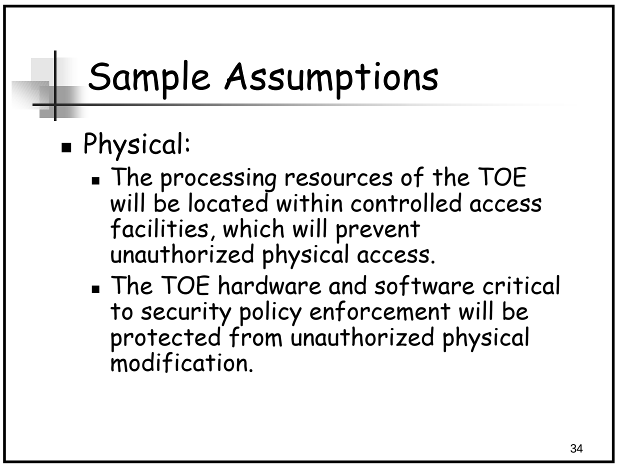
32



Sample Assumptions

- Personnel:
  - There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
  - The administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.

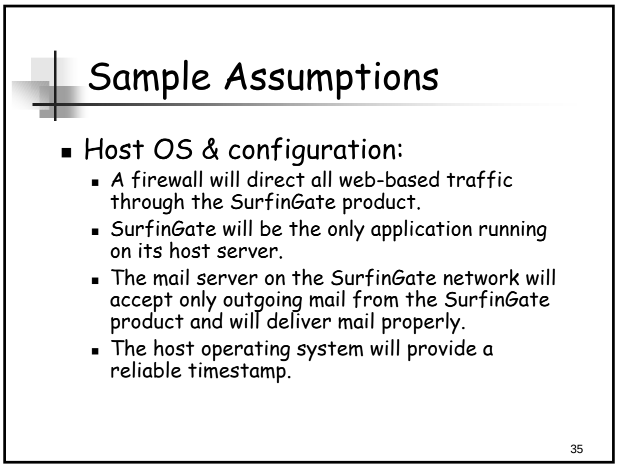
33



Sample Assumptions

- Physical:
  - The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
  - The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.

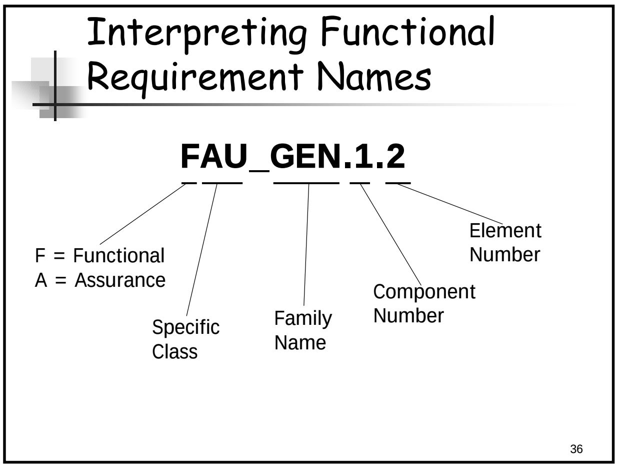
34



Sample Assumptions

- Host OS & configuration:
  - A firewall will direct all web-based traffic through the SurfinGate product.
  - SurfinGate will be the only application running on its host server.
  - The mail server on the SurfinGate network will accept only outgoing mail from the SurfinGate product and will deliver mail properly.
  - The host operating system will provide a reliable timestamp.

35



Interpreting Functional Requirement Names

FAU_GEN.1.2

F = Functional
A = Assurance

Specific Class

Family Name

Component Number

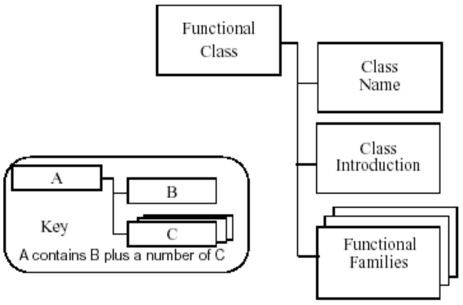
Element Number

36

CC's Security Functional Classes

1. Security Audit (4)
2. Communication (2)
3. Cryptographic Support (2)
4. User Data Protection (13)
5. Identification and Authentication (6)
6. Security Management (6)
7. Privacy (4)
8. Protection of Security Functions (16)
9. Resource Utilization (3)
10. Access (6)
11. Trusted Path/Channels (2)

CC's Functional Class Structure

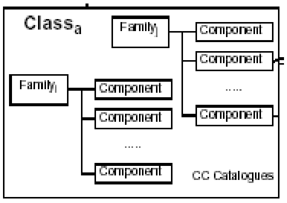


CC's Security Assurance Classes

1. Protection Profile Evaluation (6)
2. Security Target Evaluation (8)
3. Configuration Management (3)
4. Delivery and Operation (2)
5. Development (7)
6. Guidance Documentation (2)
7. Life Cycle (4)
8. Tests (4)
9. Vulnerability Assessment (4)
10. Maintenance of Assurance (4)

CC's Organization of Security Requirements

- **Class**
- **Family**
- **Component**
  - Describes a specific set of security requirements
  - Smallest selectable set of security requirements



Approach to Evaluation

- The principal input to an evaluation is a Security Target.
- The ST is the basis for agreement between the TOE developers, consumers, and evaluators as to what security a TOE offers.

Evaluation Assurance Levels

- EAL0 - Inadequate assurance
- EAL1 - Functionally tested
- EAL2 - Structurally tested
- EAL3 - Methodically tested and checked
- EAL4 - Methodically designed, tested and reviewed
- EAL5 – Semi-formally designed and tested
- EAL6 – Semi-formally verified designed and tested
- EAL7 - Formally verified designed and tested

EALs1-4

- EAL1 is the entry level.
- Up to EAL4 increasing rigor and detail are introduced, but without introducing significantly specialized security engineering techniques.
- EALs 3-4 commonly requested by governments and security-demanding organizations
- EAL 4 evaluation typically costs $1 million
- EAL1-4 can generally be retrofitted to pre-existing products (TOEs).

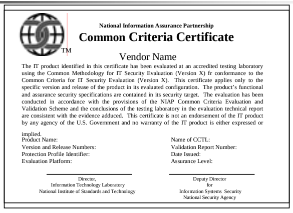
EALs5-7

- TOEs meeting the requirements of these levels will have been designed and developed with the intent of meeting those requirements.
- At EAL7 there are significant limitations on the practicability of meeting the requirements:
  - Substantial cost impact
  - Require state-of-the-art techniques for formal analysis.

Relationship to TCSEC

- With respect to assurance, roughly
  - EAL0 and EAL1 ~ D
  - EAL2 ~ C1
  - EAL3 ~ C2
  - EAL4 ~ B1
  - EAL5 ~ B2
  - EAL6 ~ B3
  - EAL7 ~ A1

What is a Validation Certificate?



National Information Assurance Partnership

Common Criteria Certificate

TM

Vendor Name

The IT product identified in this certificate has been evaluated at an accredited testing laboratory using the Common Methodology for IT Security Evaluation (Version X) fr conformance to the Common Criteria for IT Security Evaluation (Version X). This certificate applies only to the specific version and release of the product in its evaluated configuration. The product's functional and assurance security specifications are contained in its security target. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the IT product by any agency of the U.S. Government and no warranty of the IT product is either expressed or implied.

Product Name:	Name of CCTL:
Version and Release Numbers:	Validation Report Number:
Protection Profile Identifier:	Date Issued:
Evaluation Platform:	Assurance Level:

Director,
Information Technology Laboratory
National Institute of Standards and Technology

Deputy Director
for
Information Systems Security
National Security Agency

- **Validation that product met Common Criteria requirements for which it was evaluated/tested**
- **Not an NSA, NIST, or NIAP endorsement of the product**

Mutual Recognition

- **Parties commit to "recognize the certificates which have been issued by any one of them"**

  "Recognize" = accept the validity of the evaluation process

- **Two Categories of membership:**

"Certificate Producing"

"Certificate Consuming"

Common Criteria
(Capabilities and Limitations)

- Provides a common security specification language for IT products and systems
- Offers great flexibility in tailoring security requirements to specific needs
- Requires technical expertise in formulating protection profiles and security targets from generic catalogues
- Requires some interpretation due to lack of formal specification model