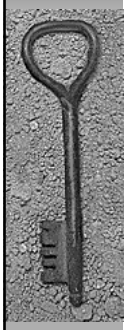
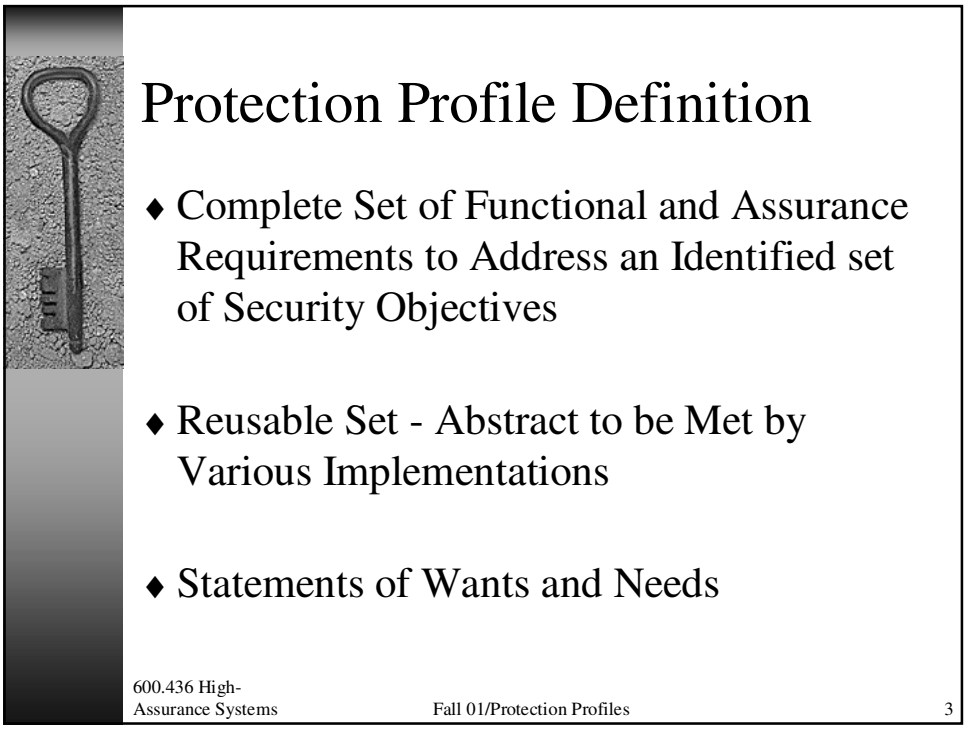
Developing A Common Criteria Protection Profile

- Overview
- Preparation
- Development



Overview

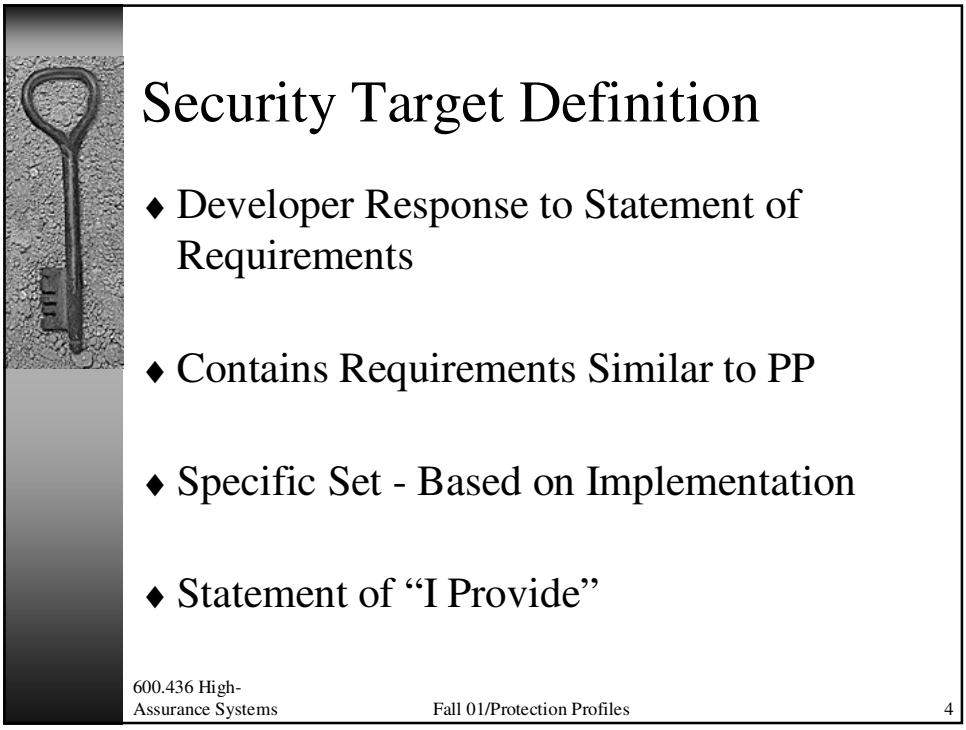
- What is a PP?
- What is a ST?
- How are they used?
- How are they Related?



Protection Profile Definition

- Complete Set of Functional and Assurance Requirements to Address an Identified set of Security Objectives
- Reusable Set - Abstract to be Met by Various Implementations
- Statements of Wants and Needs

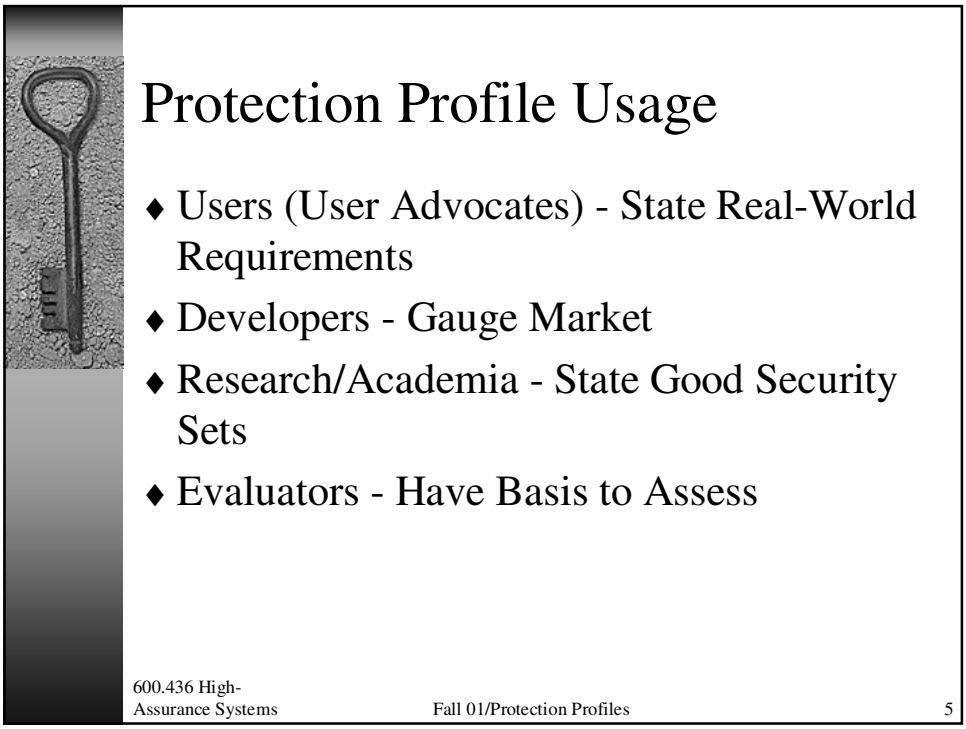
600.436 High-Assurance Systems Fall 01/Protection Profiles 3

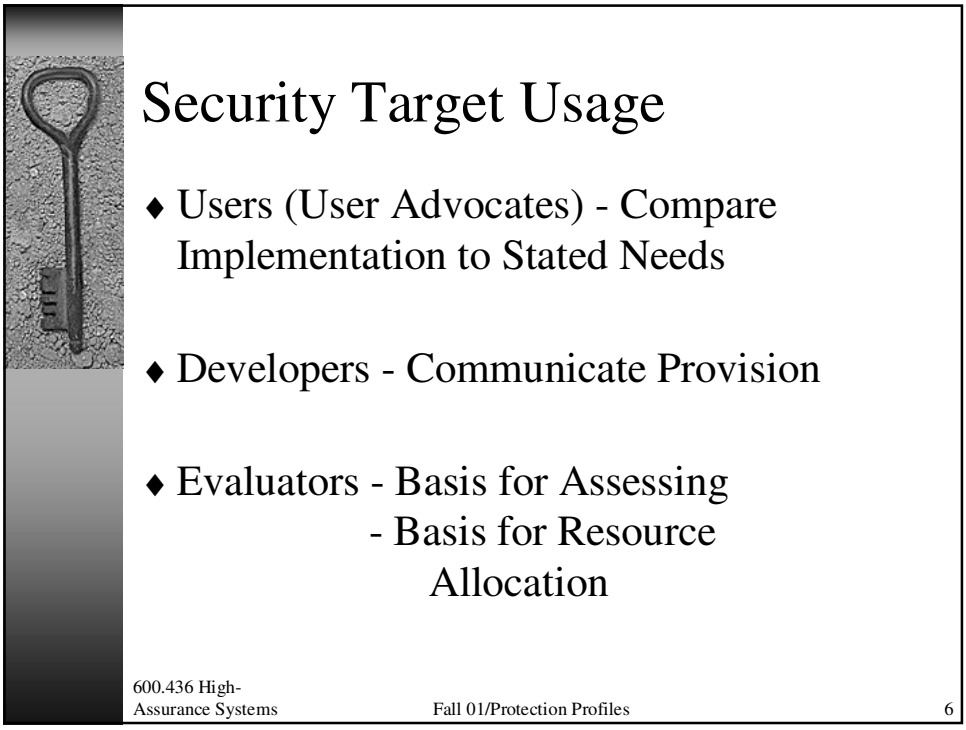


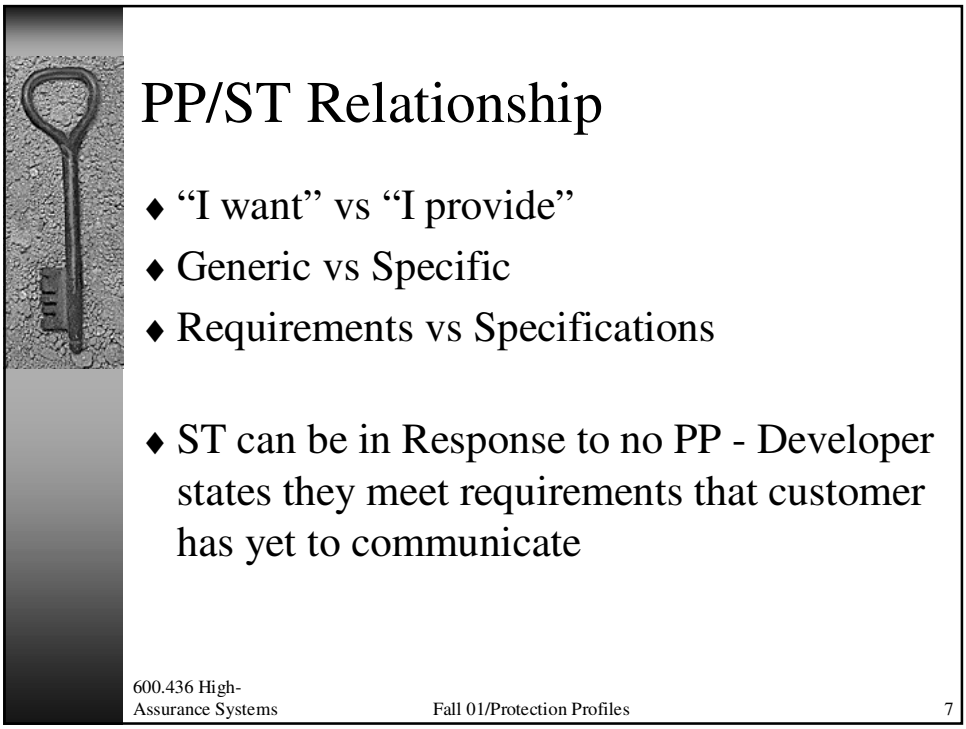
Security Target Definition

- Developer Response to Statement of Requirements
- Contains Requirements Similar to PP
- Specific Set - Based on Implementation
- Statement of “I Provide”

600.436 High-Assurance Systems Fall 01/Protection Profiles 4


Protection Profile Usage
♦ Users (User Advocates) - State Real-World Requirements
♦ Developers - Gauge Market
♦ Research/Academia - State Good Security Sets
♦ Evaluators - Have Basis to Assess
600.436 High-Assurance Systems
Fall 01/Protection Profiles
5


Security Target Usage
♦ Users (User Advocates) - Compare Implementation to Stated Needs
♦ Developers - Communicate Provision
♦ Evaluators - Basis for Assessing
- Basis for Resource Allocation
600.436 High-Assurance Systems
Fall 01/Protection Profiles
6

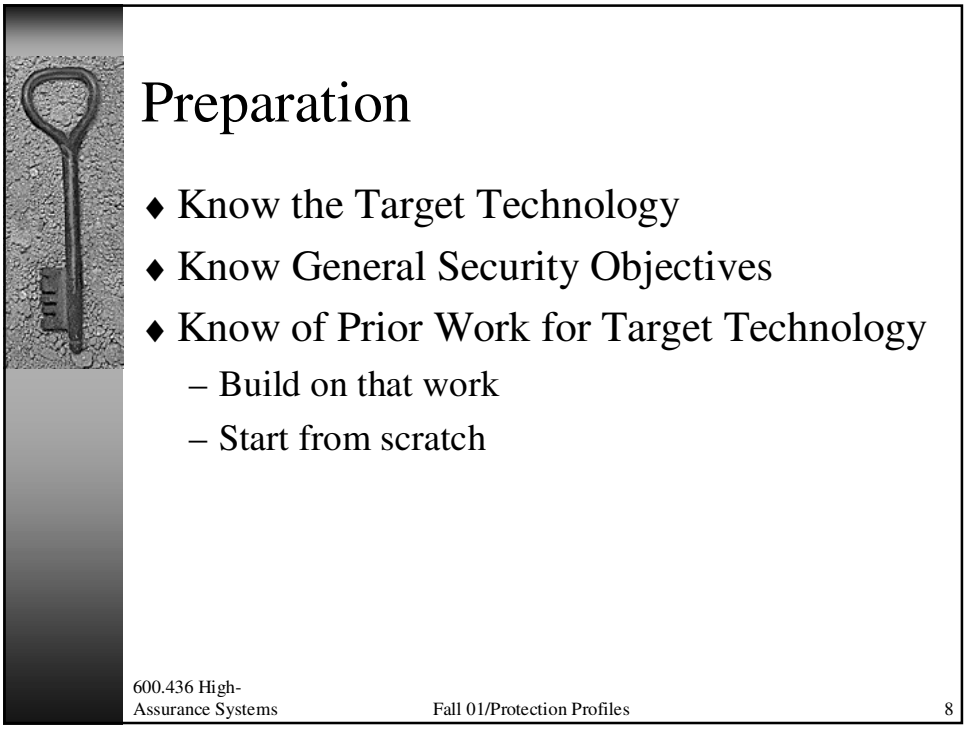


PP/ST Relationship

- "I want" vs "I provide"
- Generic vs Specific
- Requirements vs Specifications

- ST can be in Response to no PP - Developer states they meet requirements that customer has yet to communicate

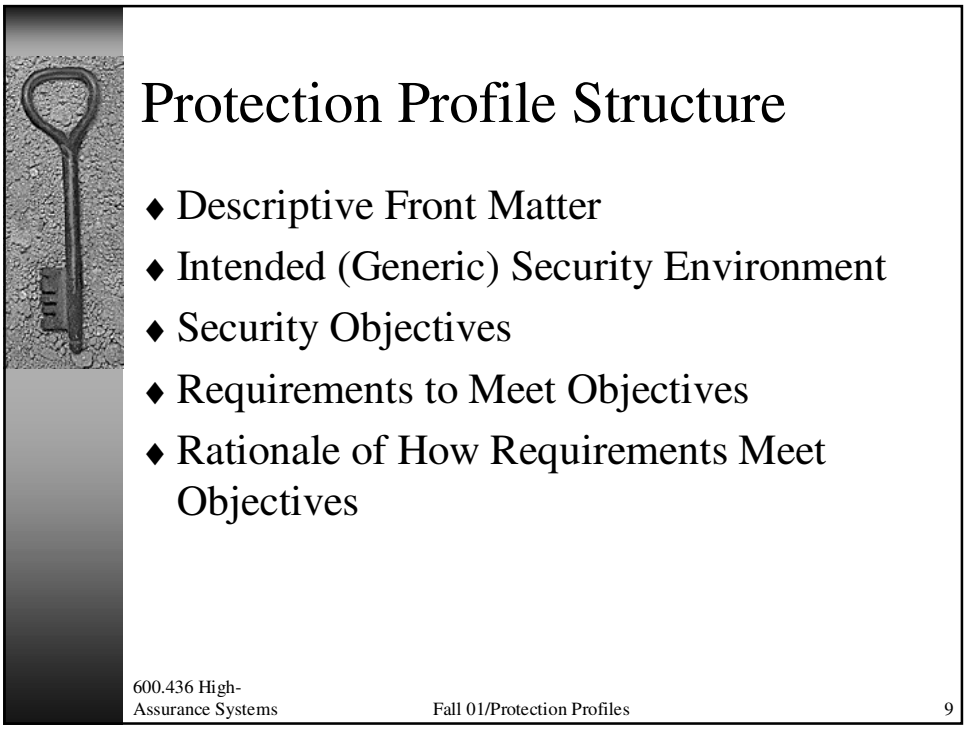
600.436 High-Assurance Systems Fall 01/Protection Profiles 7

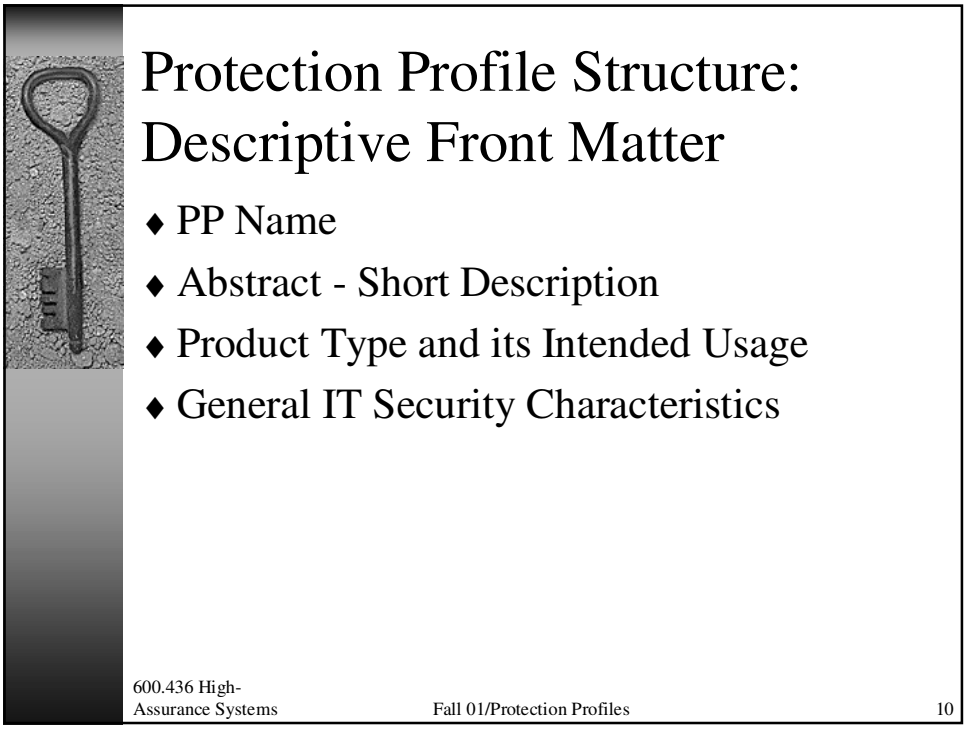


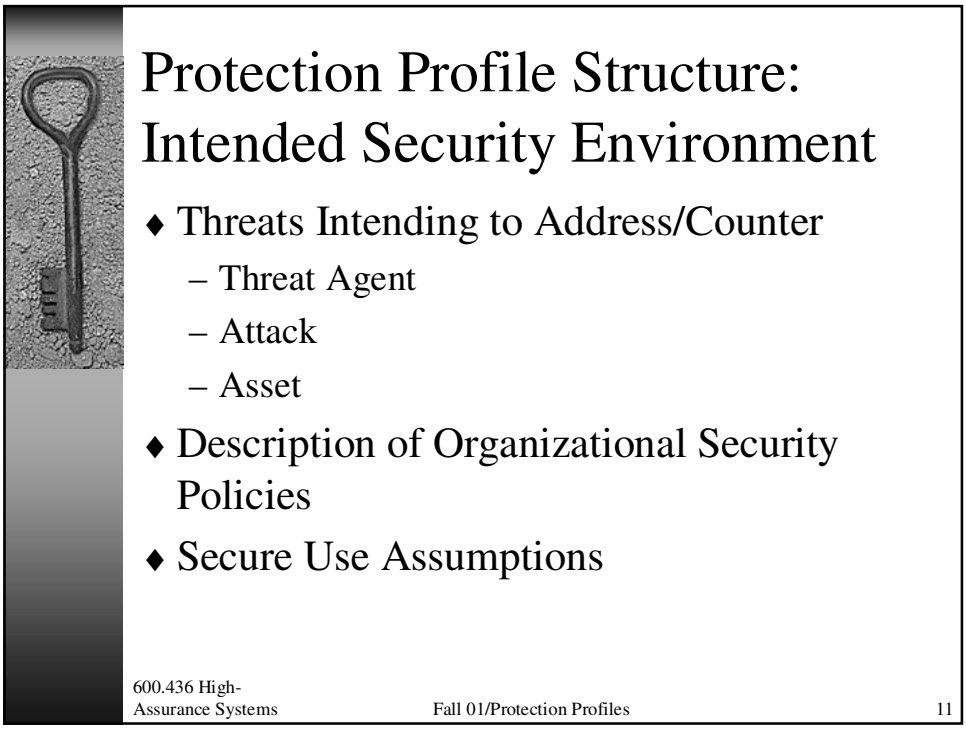
Preparation

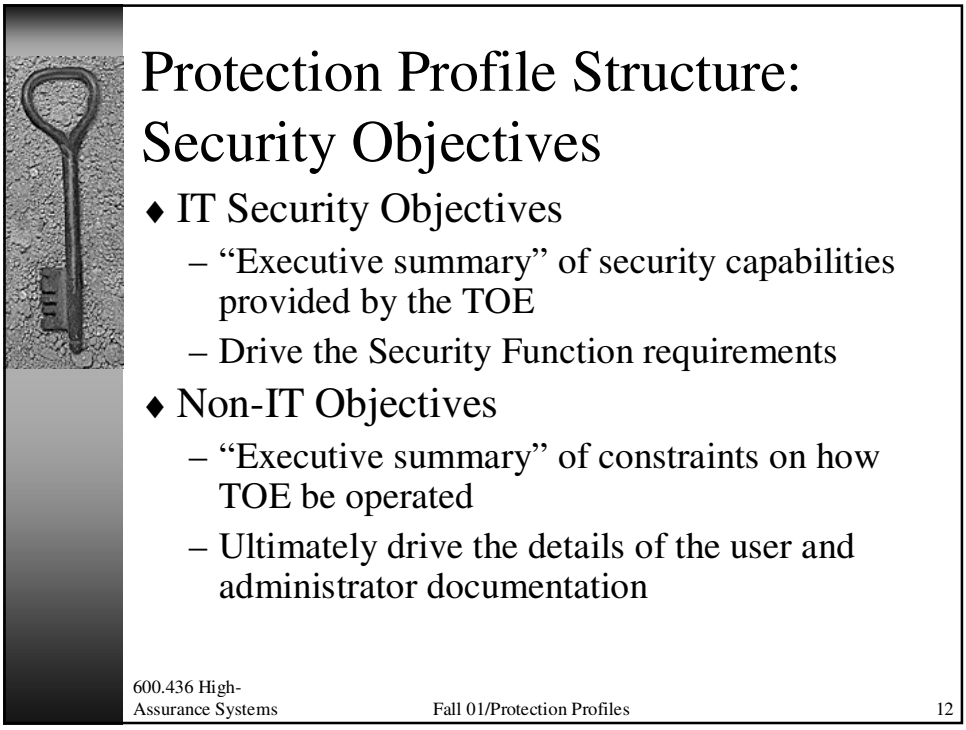
- Know the Target Technology
- Know General Security Objectives
- Know of Prior Work for Target Technology
  - Build on that work
  - Start from scratch

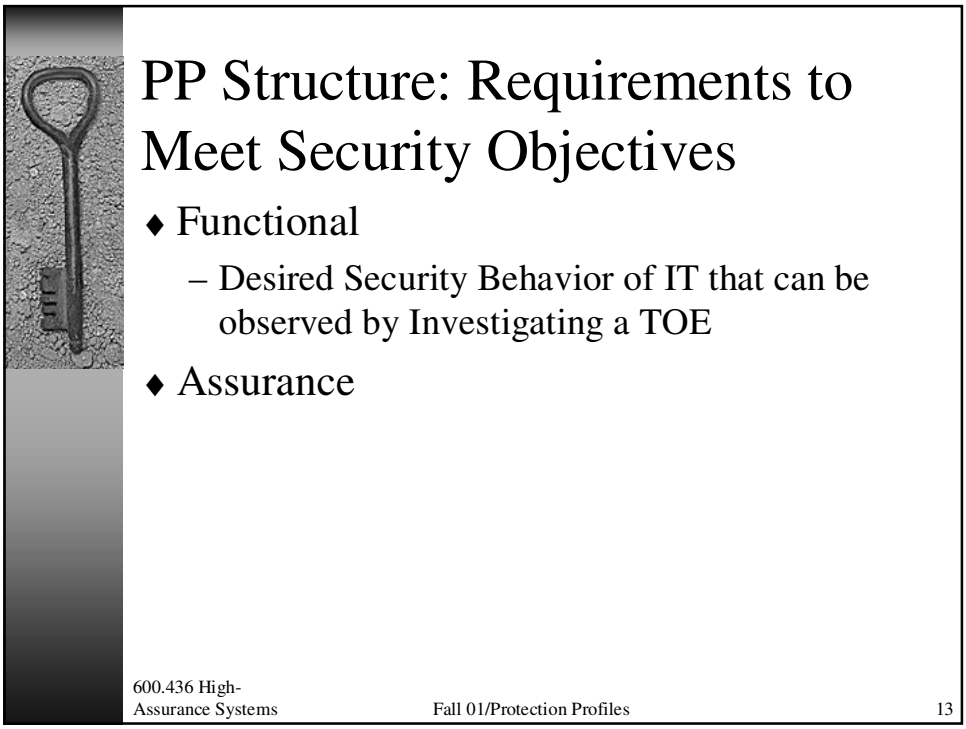
600.436 High-Assurance Systems Fall 01/Protection Profiles 8

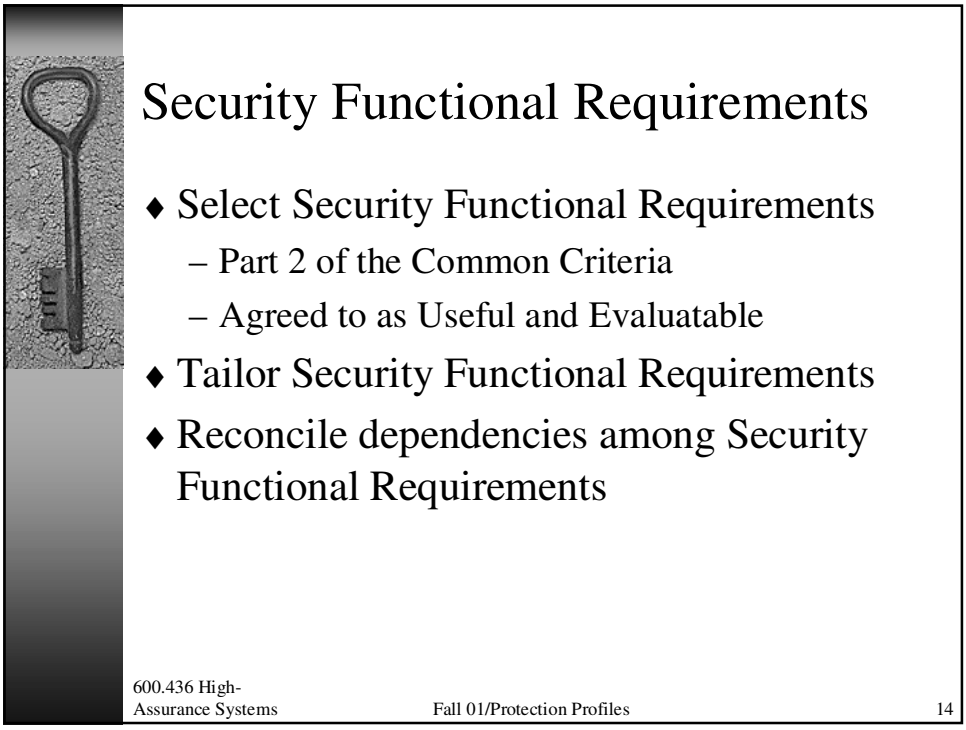

Protection Profile Structure
♦ Descriptive Front Matter
♦ Intended (Generic) Security Environment
♦ Security Objectives
♦ Requirements to Meet Objectives
♦ Rationale of How Requirements Meet Objectives
600.436 High-Assurance Systems
Fall 01/Protection Profiles
9

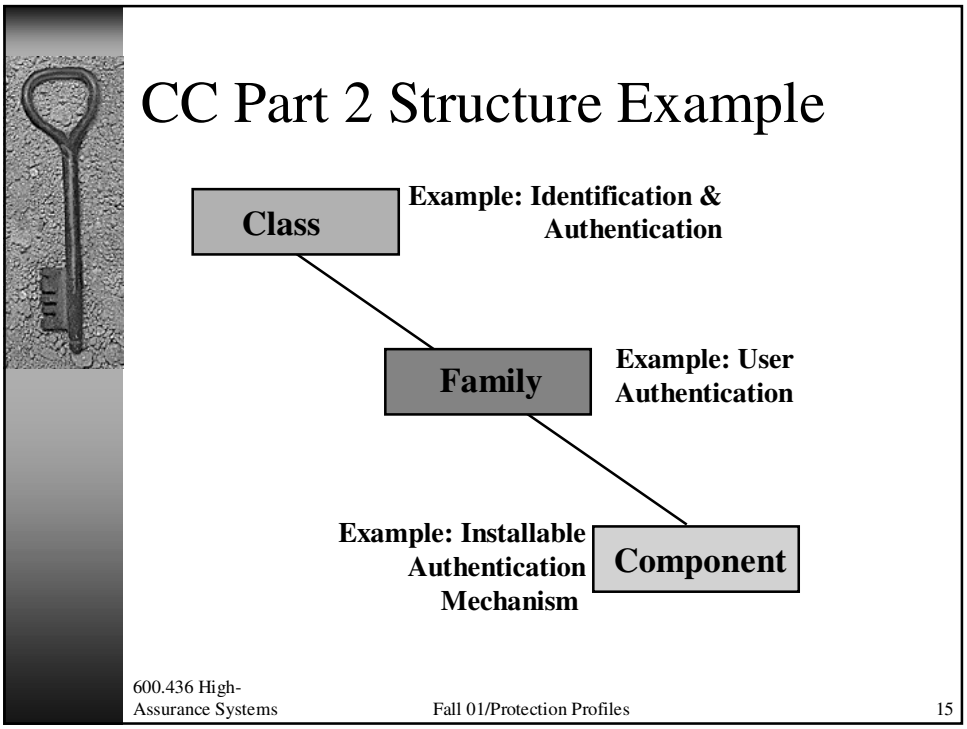

Protection Profile Structure: Descriptive Front Matter
♦ PP Name
♦ Abstract - Short Description
♦ Product Type and its Intended Usage
♦ General IT Security Characteristics
600.436 High-Assurance Systems
Fall 01/Protection Profiles
10

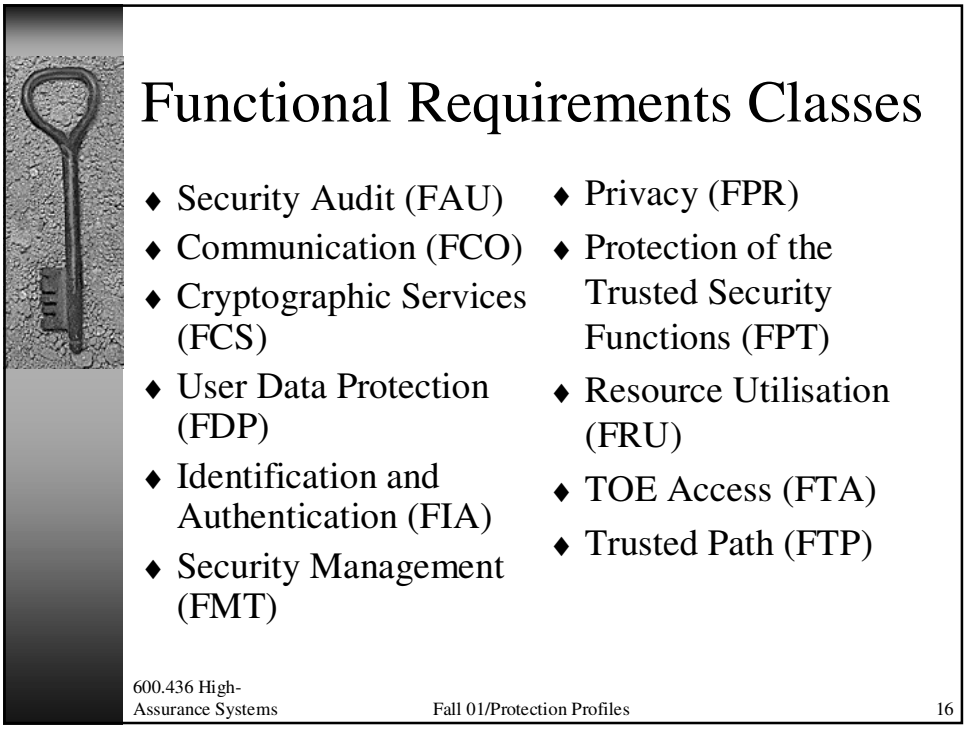

Protection Profile Structure: Intended Security Environment
♦ Threats Intending to Address/Counter
– Threat Agent
– Attack
– Asset
♦ Description of Organizational Security Policies
♦ Secure Use Assumptions
600.436 High-Assurance Systems
Fall 01/Protection Profiles
11

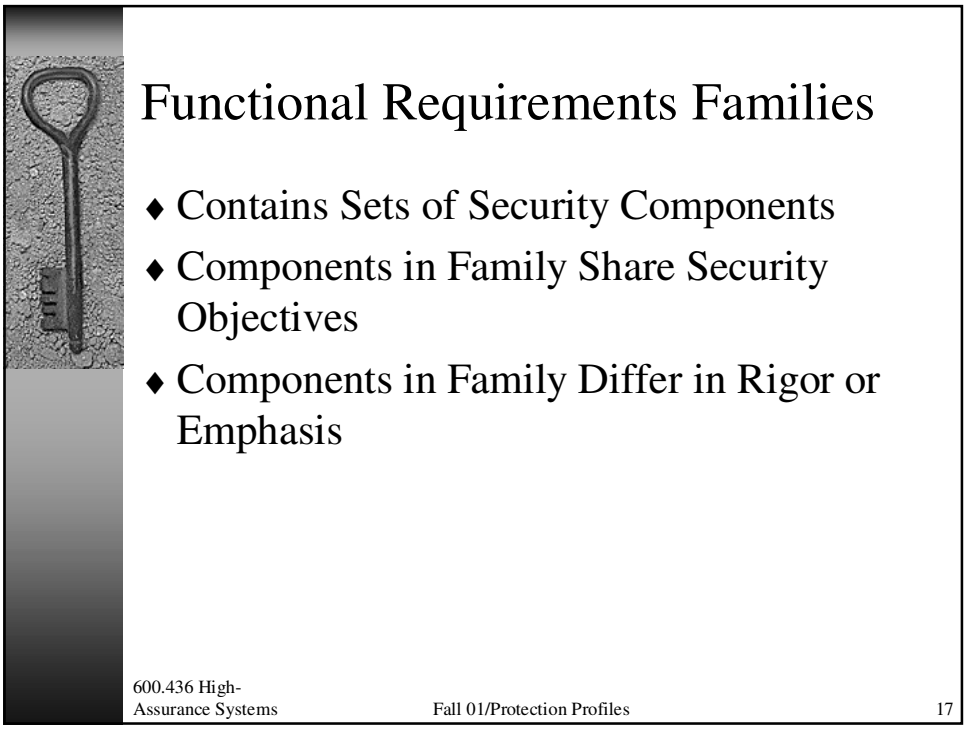

Protection Profile Structure: Security Objectives
♦ IT Security Objectives
– "Executive summary" of security capabilities provided by the TOE
– Drive the Security Function requirements
♦ Non-IT Objectives
– "Executive summary" of constraints on how TOE be operated
– Ultimately drive the details of the user and administrator documentation
600.436 High-Assurance Systems
Fall 01/Protection Profiles
12

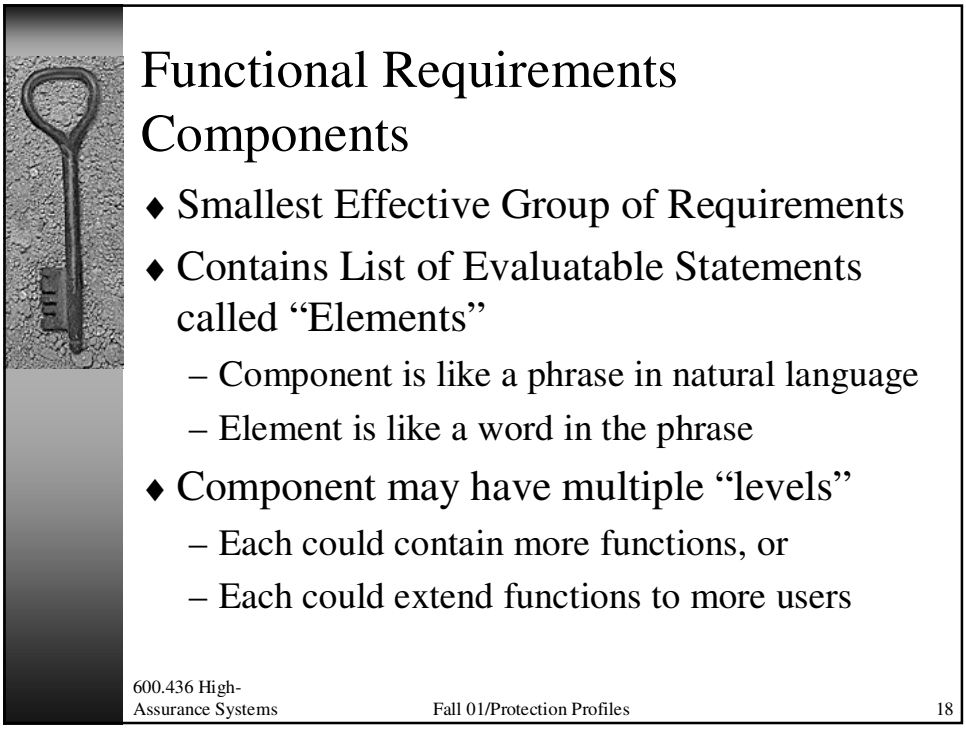

PP Structure: Requirements to Meet Security Objectives
♦ Functional
– Desired Security Behavior of IT that can be observed by Investigating a TOE
♦ Assurance
600.436 High-Assurance Systems
Fall 01/Protection Profiles
13

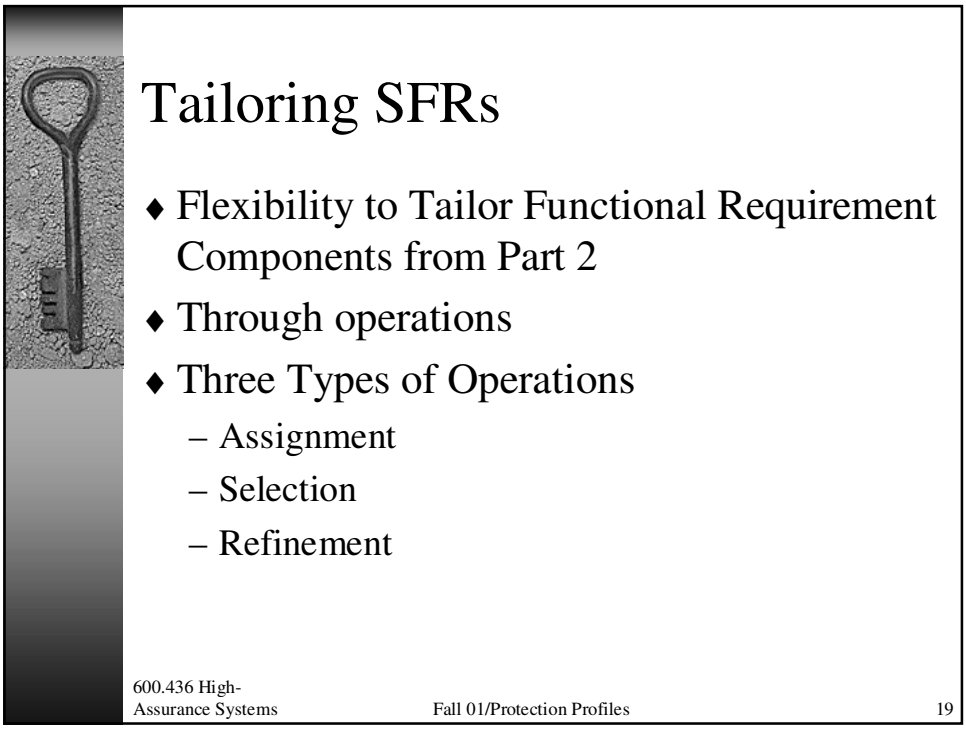

Security Functional Requirements
♦ Select Security Functional Requirements
– Part 2 of the Common Criteria
– Agreed to as Useful and Evaluatable
♦ Tailor Security Functional Requirements
♦ Reconcile dependencies among Security Functional Requirements
600.436 High-Assurance Systems
Fall 01/Protection Profiles
14

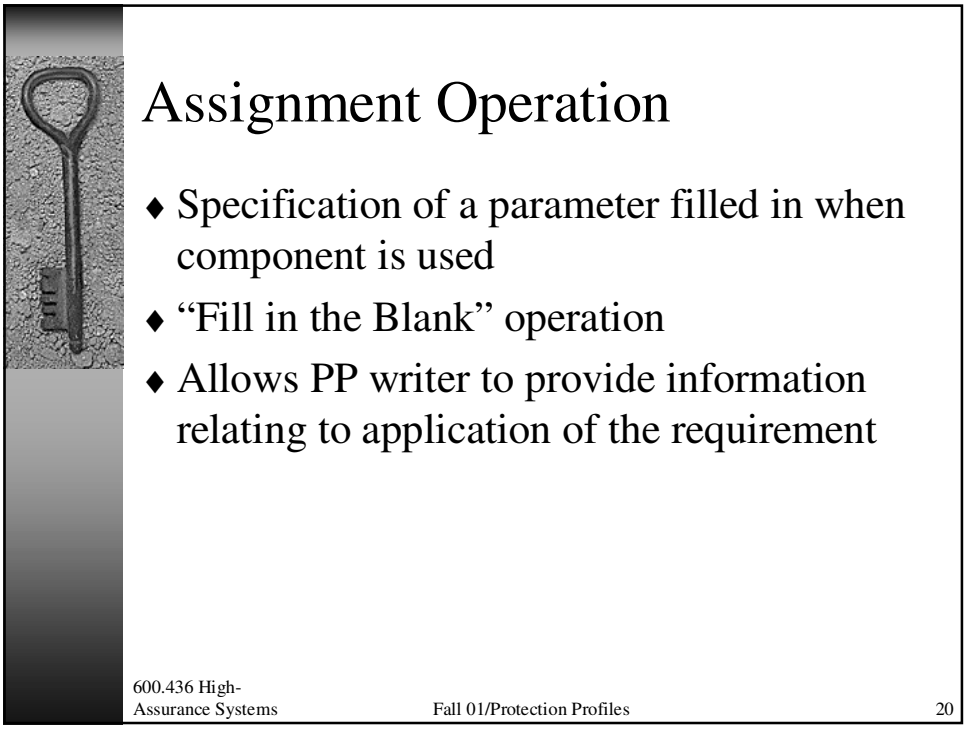

CC Part 2 Structure Example
Class
Example: Identification & Authentication
Family
Example: User Authentication
Example: Installable Authentication Mechanism
Component
600.436 High-Assurance Systems
Fall 01/Protection Profiles
15

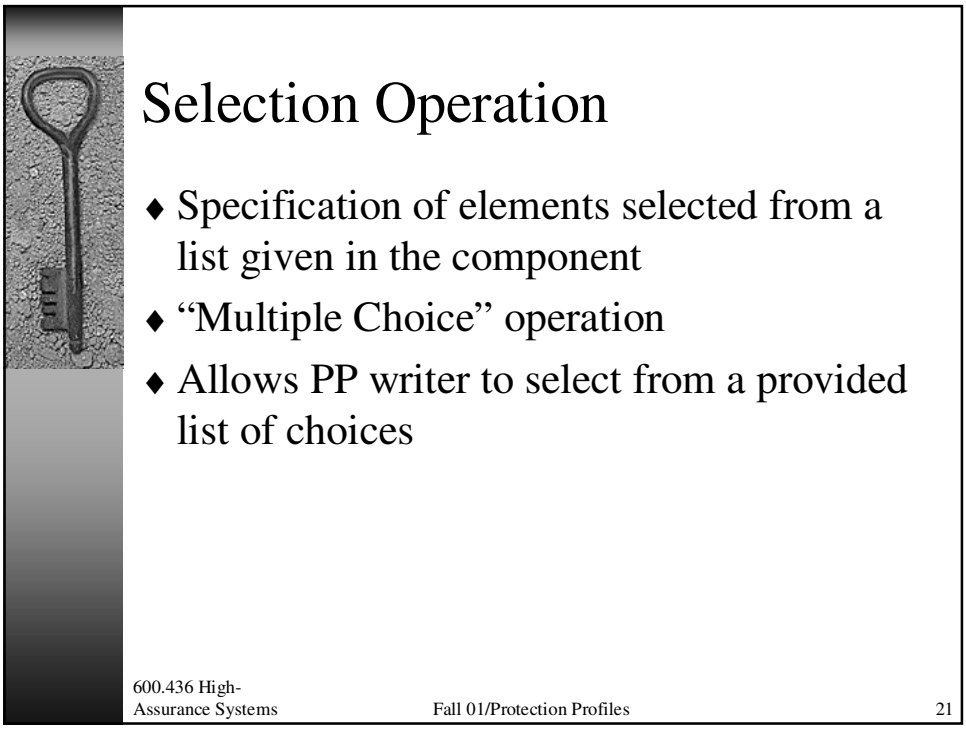

Functional Requirements Classes
Security Audit (FAU)
Communication (FCO)
Cryptographic Services (FCS)
User Data Protection (FDP)
Identification and Authentication (FIA)
Security Management (FMT)
Privacy (FPR)
Protection of the Trusted Security Functions (FPT)
Resource Utilisation (FRU)
TOE Access (FTA)
Trusted Path (FTP)
600.436 High-Assurance Systems
Fall 01/Protection Profiles
16

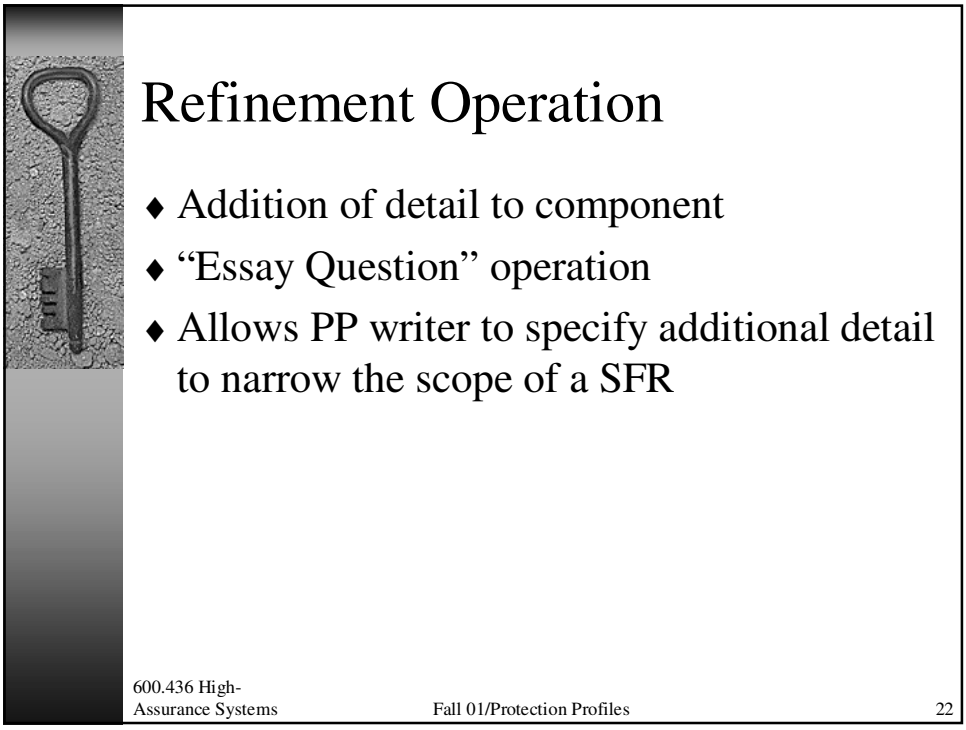

Functional Requirements Families
♦ Contains Sets of Security Components
♦ Components in Family Share Security Objectives
♦ Components in Family Differ in Rigor or Emphasis
600.436 High-Assurance Systems
Fall 01/Protection Profiles
17

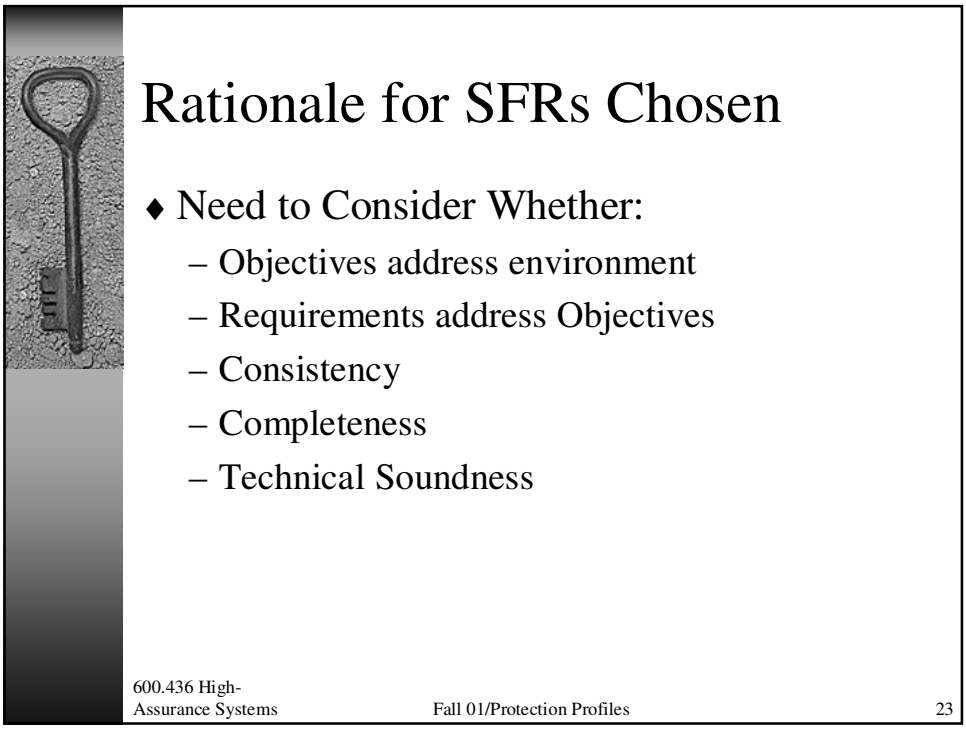

Functional Requirements Components
♦ Smallest Effective Group of Requirements
♦ Contains List of Evaluatable Statements called “Elements”
– Component is like a phrase in natural language
– Element is like a word in the phrase
♦ Component may have multiple “levels”
– Each could contain more functions, or
– Each could extend functions to more users
600.436 High-Assurance Systems
Fall 01/Protection Profiles
18

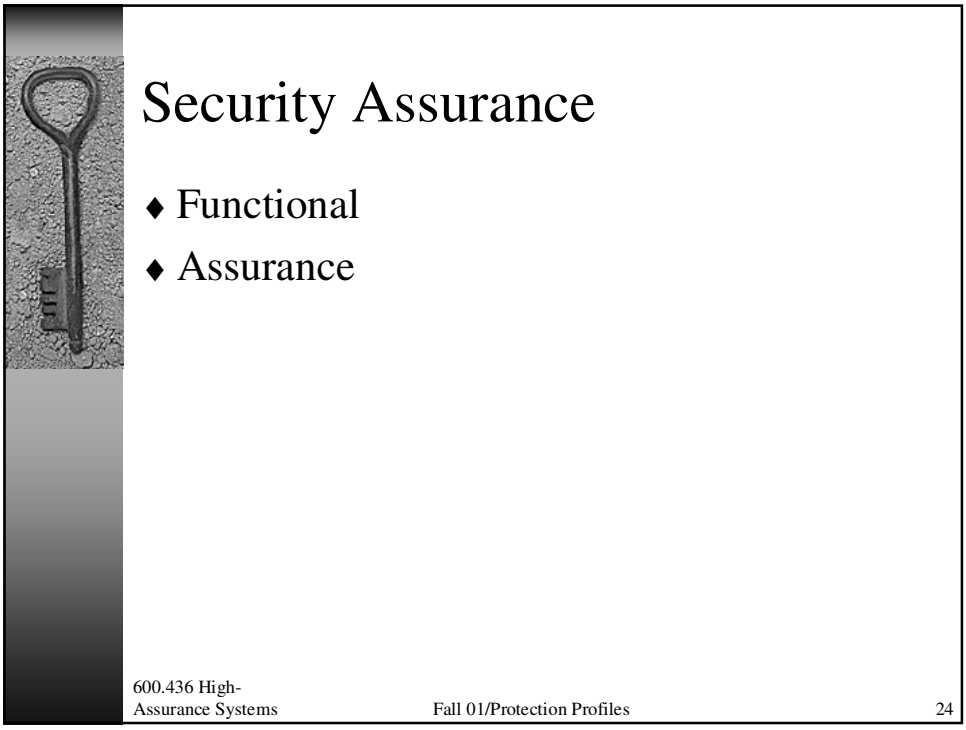

Tailoring SFRs
♦ Flexibility to Tailor Functional Requirement Components from Part 2
♦ Through operations
♦ Three Types of Operations
– Assignment
– Selection
– Refinement
600.436 High-Assurance Systems
Fall 01/Protection Profiles
19

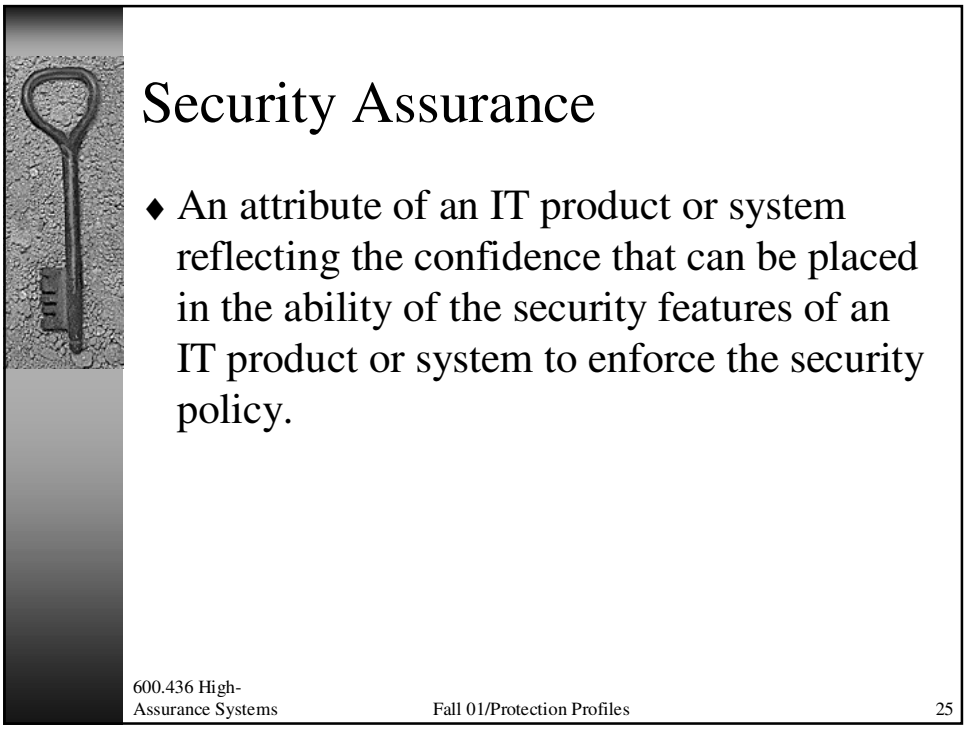

Assignment Operation
♦ Specification of a parameter filled in when component is used
♦ “Fill in the Blank” operation
♦ Allows PP writer to provide information relating to application of the requirement
600.436 High-Assurance Systems
Fall 01/Protection Profiles
20

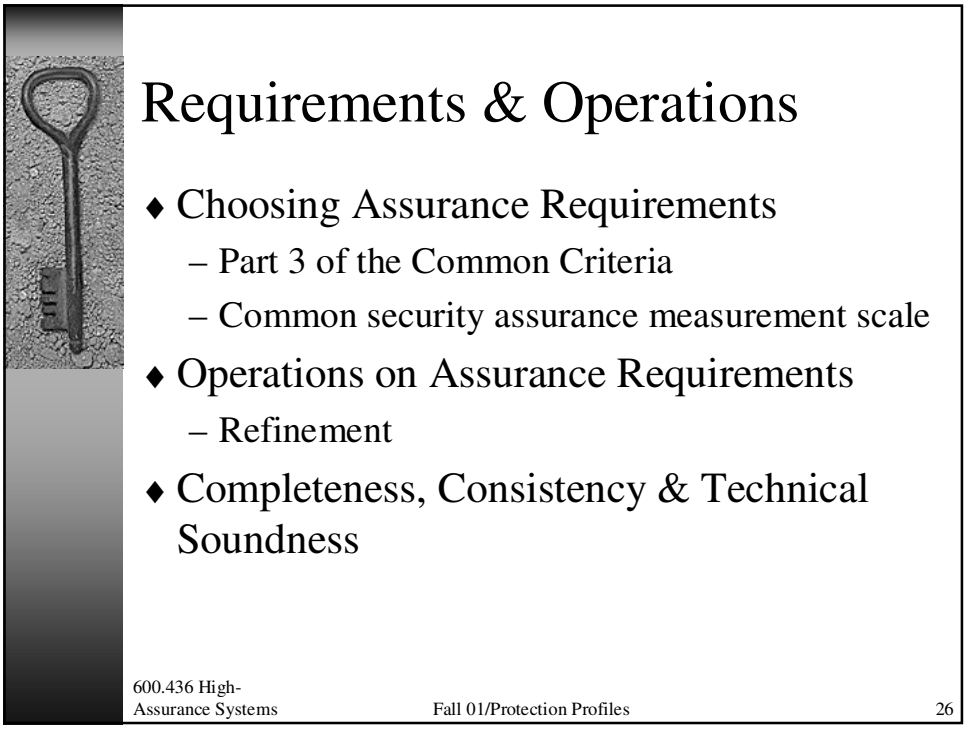

Selection Operation
♦ Specification of elements selected from a list given in the component
♦ "Multiple Choice" operation
♦ Allows PP writer to select from a provided list of choices
600.436 High-Assurance Systems
Fall 01/Protection Profiles
21

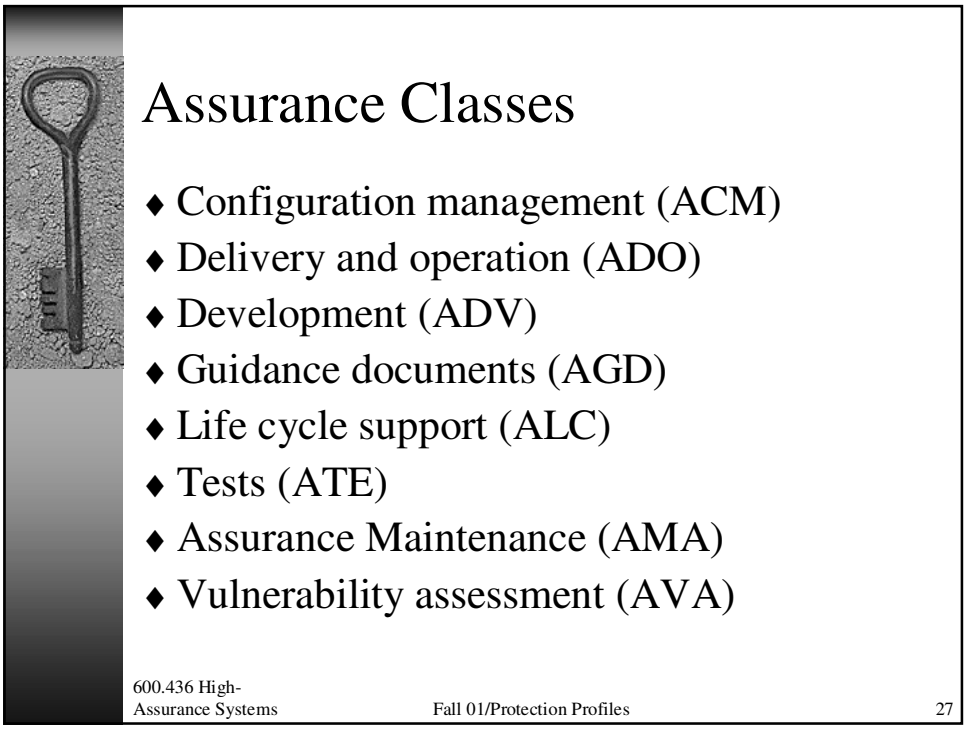

Refinement Operation
♦ Addition of detail to component
♦ "Essay Question" operation
♦ Allows PP writer to specify additional detail to narrow the scope of a SFR
600.436 High-Assurance Systems
Fall 01/Protection Profiles
22


Rationale for SFRs Chosen
♦ Need to Consider Whether:
– Objectives address environment
– Requirements address Objectives
– Consistency
– Completeness
– Technical Soundness
600.436 High-Assurance Systems
Fall 01/Protection Profiles
23


Security Assurance
♦ Functional
♦ Assurance
600.436 High-Assurance Systems
Fall 01/Protection Profiles
24


Security Assurance
♦ An attribute of an IT product or system reflecting the confidence that can be placed in the ability of the security features of an IT product or system to enforce the security policy.
600.436 High-Assurance Systems
Fall 01/Protection Profiles
25

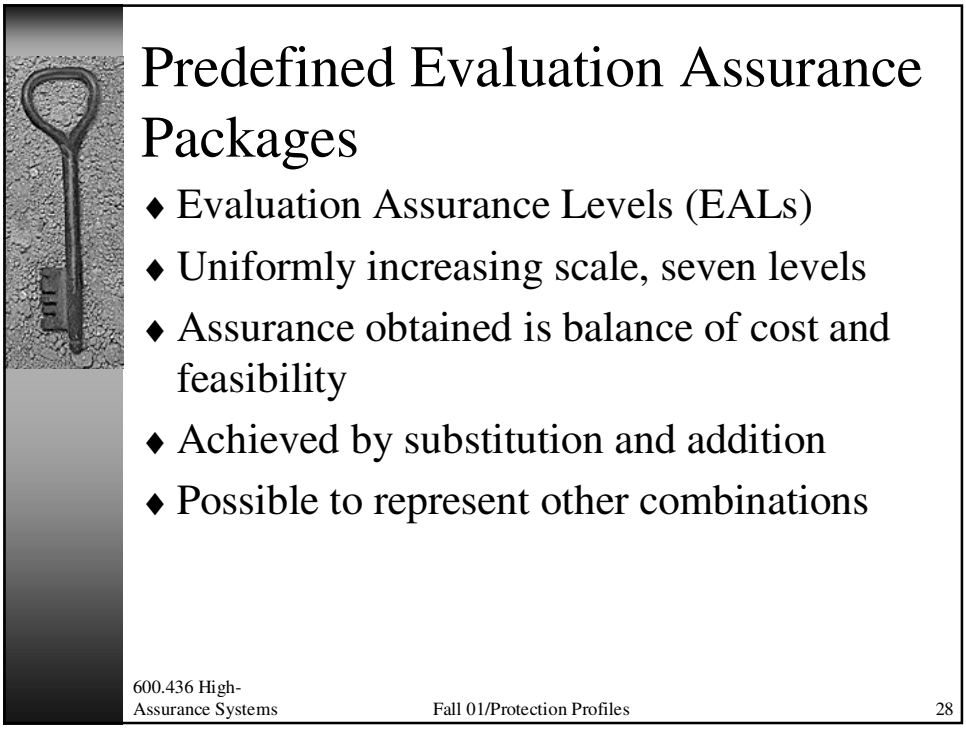

Requirements & Operations
♦ Choosing Assurance Requirements
– Part 3 of the Common Criteria
– Common security assurance measurement scale
♦ Operations on Assurance Requirements
– Refinement
♦ Completeness, Consistency & Technical Soundness
600.436 High-Assurance Systems
Fall 01/Protection Profiles
26



Assurance Classes

- Configuration management (ACM)
- Delivery and operation (ADO)
- Development (ADV)
- Guidance documents (AGD)
- Life cycle support (ALC)
- Tests (ATE)
- Assurance Maintenance (AMA)
- Vulnerability assessment (AVA)

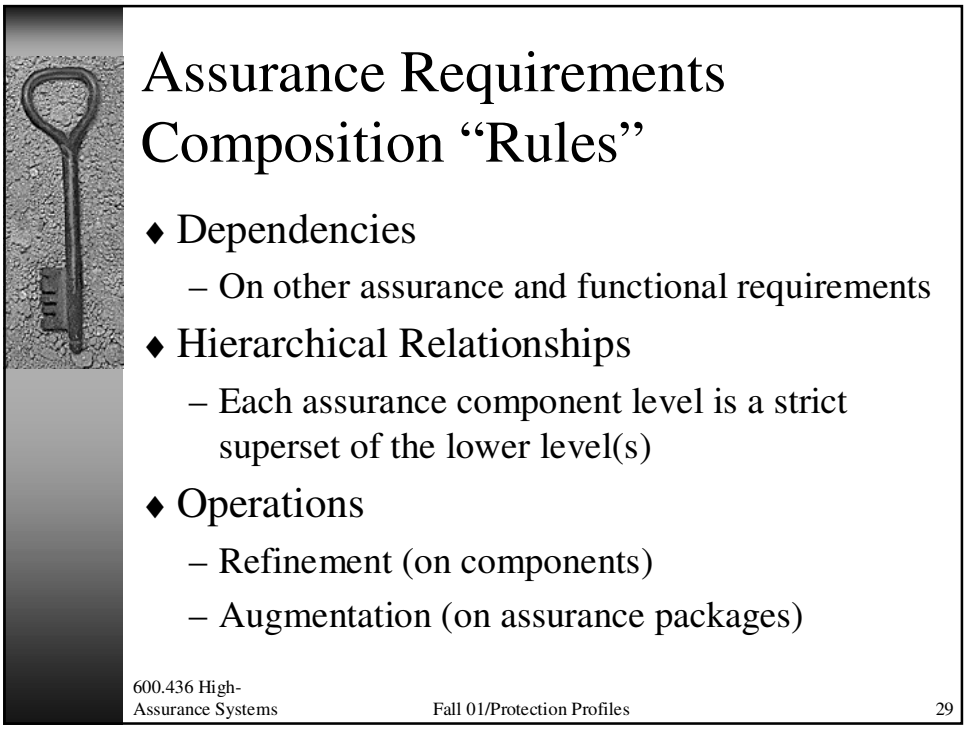
600.436 High-Assurance Systems Fall 01/Protection Profiles 27



Predefined Evaluation Assurance Packages

- Evaluation Assurance Levels (EALs)
- Uniformly increasing scale, seven levels
- Assurance obtained is balance of cost and feasibility
- Achieved by substitution and addition
- Possible to represent other combinations

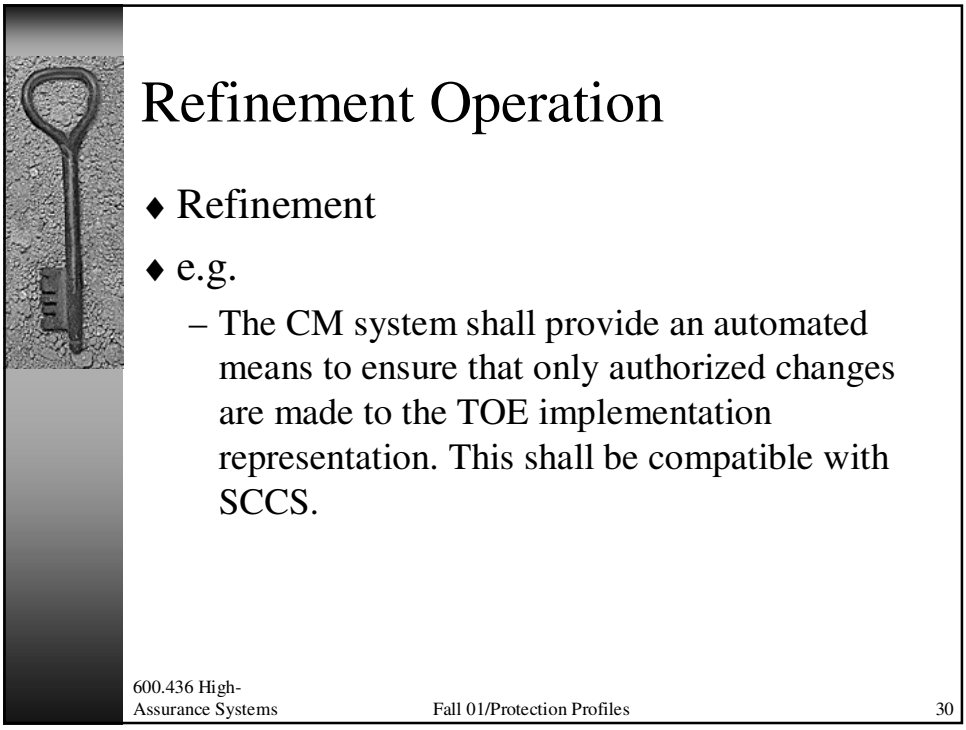
600.436 High-Assurance Systems Fall 01/Protection Profiles 28



Assurance Requirements Composition "Rules"

- Dependencies
  - On other assurance and functional requirements
- Hierarchical Relationships
  - Each assurance component level is a strict superset of the lower level(s)
- Operations
  - Refinement (on components)
  - Augmentation (on assurance packages)

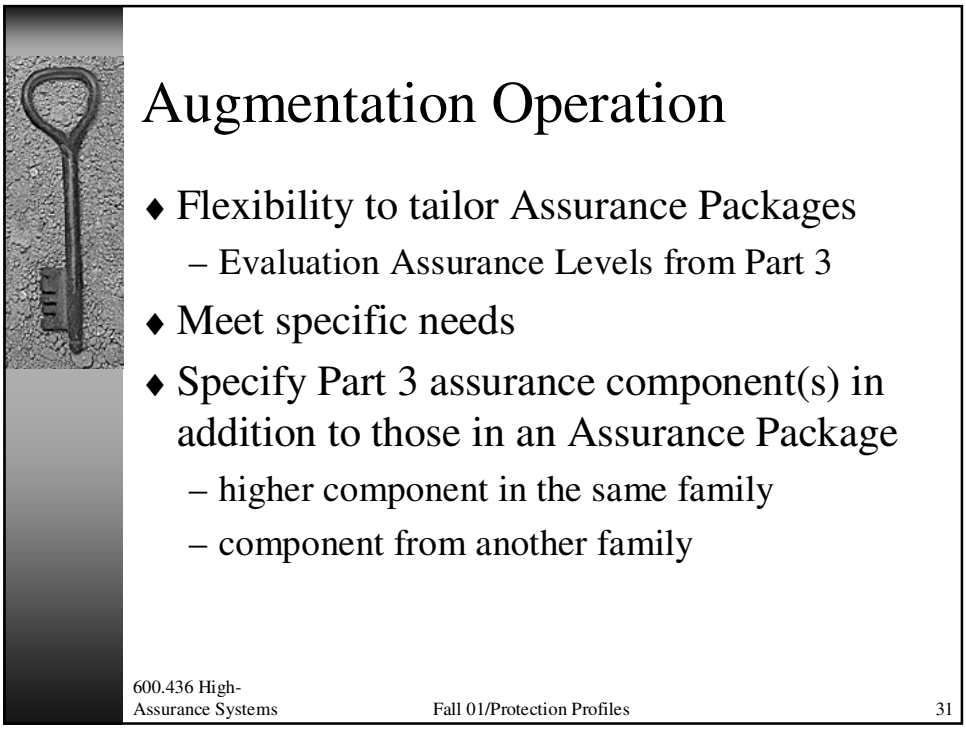
600.436 High-Assurance Systems Fall 01/Protection Profiles 29

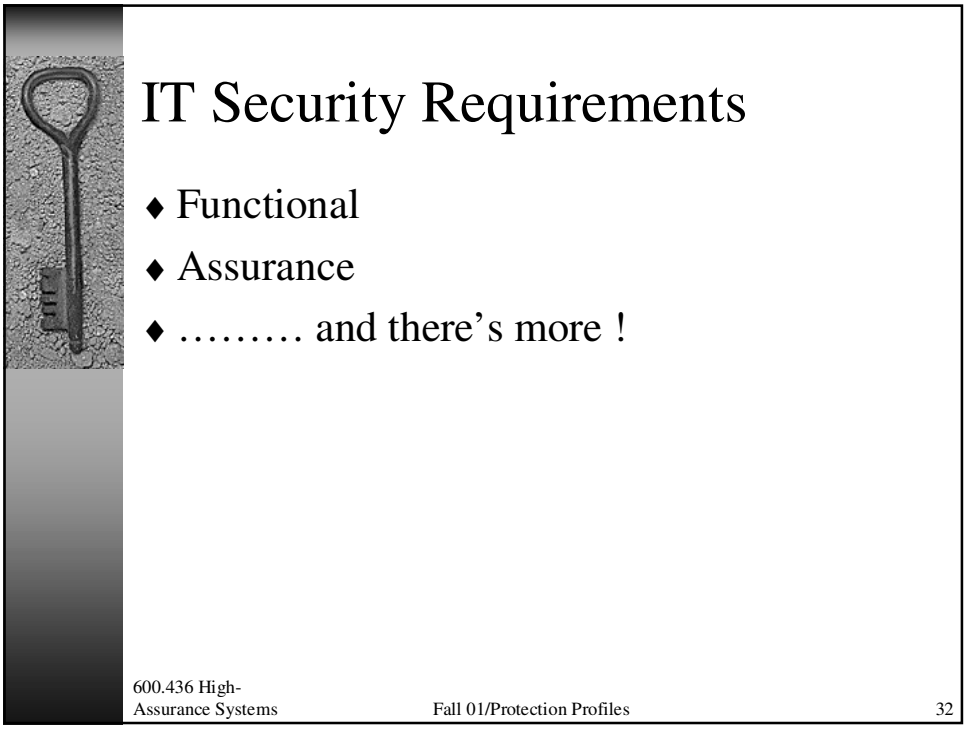


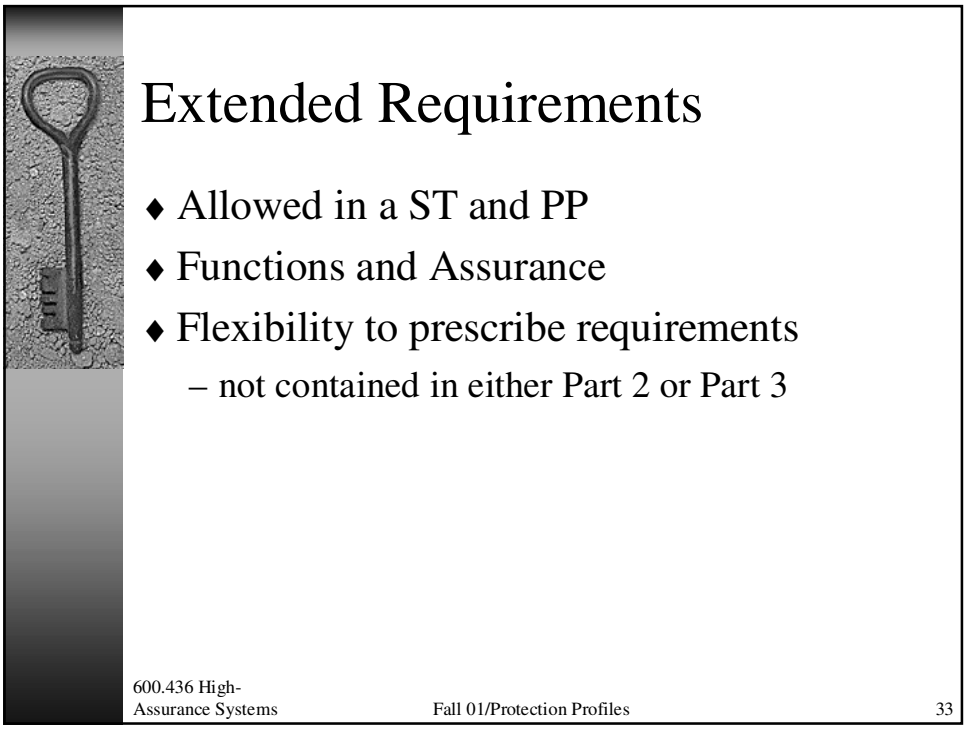
Refinement Operation

- Refinement
- e.g.
  - The CM system shall provide an automated means to ensure that only authorized changes are made to the TOE implementation representation. This shall be compatible with SCCS.

600.436 High-Assurance Systems Fall 01/Protection Profiles 30


Augmentation Operation
♦ Flexibility to tailor Assurance Packages
– Evaluation Assurance Levels from Part 3
♦ Meet specific needs
♦ Specify Part 3 assurance component(s) in addition to those in an Assurance Package
– higher component in the same family
– component from another family
600.436 High-Assurance Systems
Fall 01/Protection Profiles
31


IT Security Requirements
♦ Functional
♦ Assurance
♦ …… and there's more !
600.436 High-Assurance Systems
Fall 01/Protection Profiles
32


Extended Requirements
♦ Allowed in a ST and PP
♦ Functions and Assurance
♦ Flexibility to prescribe requirements
– not contained in either Part 2 or Part 3
600.436 High-Assurance Systems
Fall 01/Protection Profiles
33