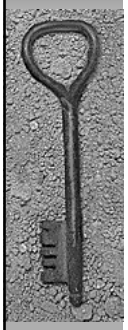
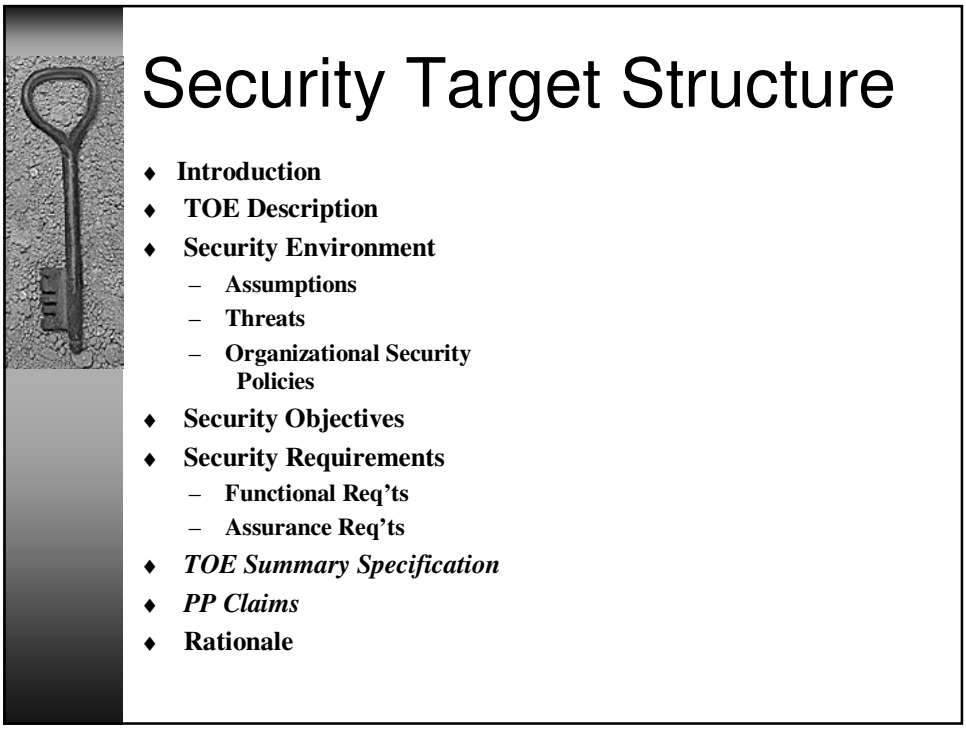
Developing A Common Criteria Security Target

- Quick Review of ST Contents
- Development
  - –Functional Requirements Rationalization
  - –Assurance Requirements Rationalization
  - –PP Compliance Claims
  - –TOE Summary Specification



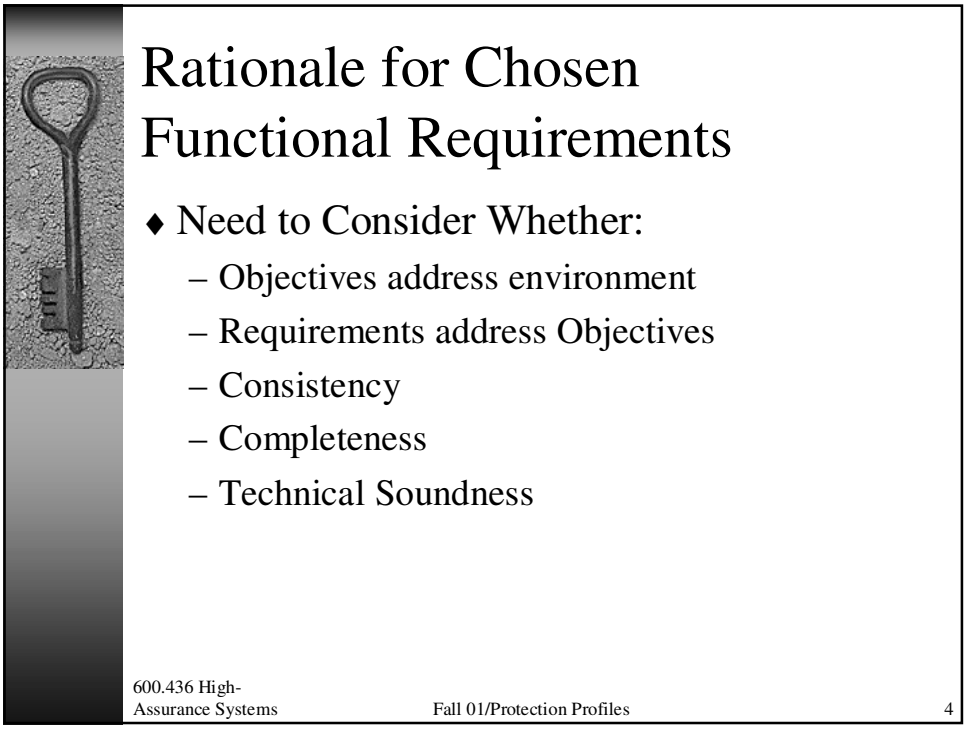
Security Target Definition

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



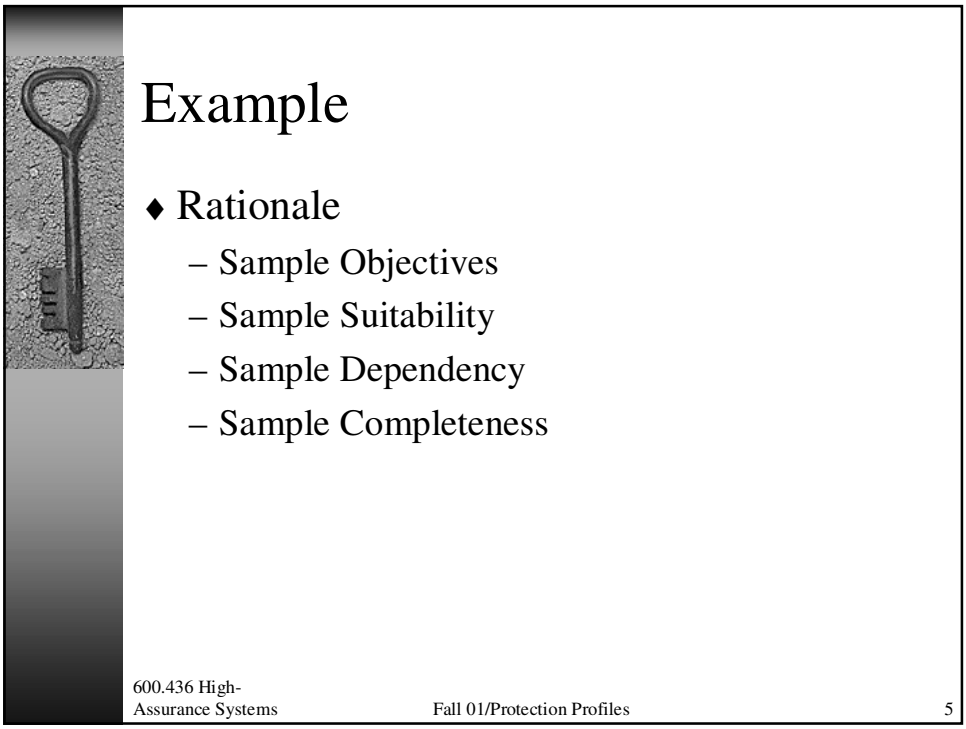
Security Target Structure

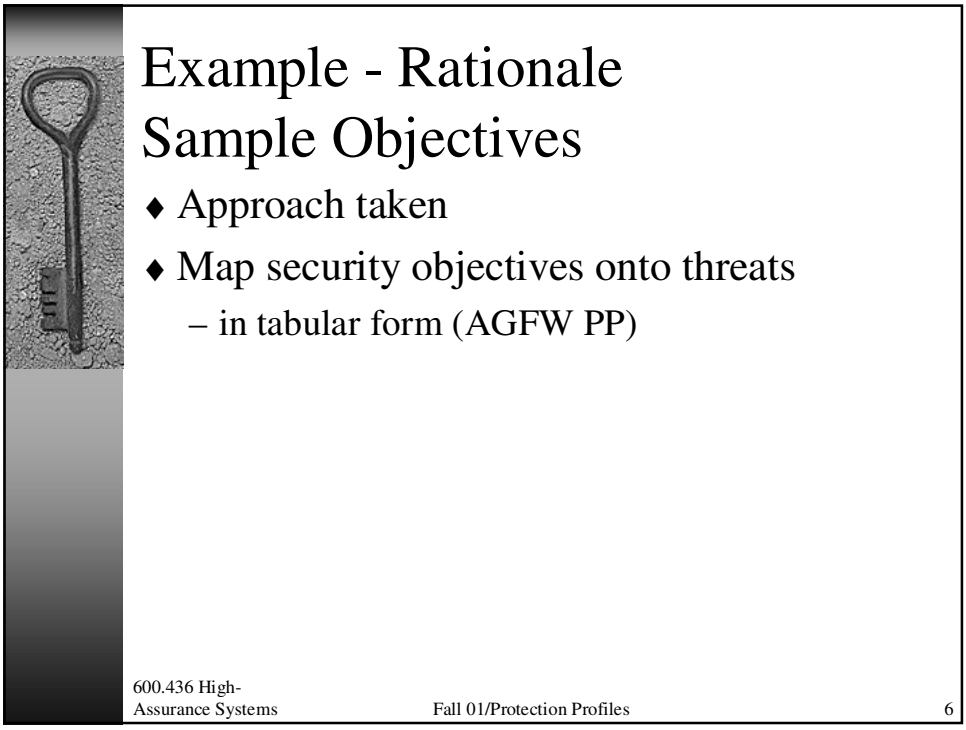
- **Introduction**
- **TOE Description**
- **Security Environment**
  - **Assumptions**
  - **Threats**
  - **Organizational Security Policies**
- **Security Objectives**
- **Security Requirements**
  - **Functional Req'ts**
  - **Assurance Req'ts**
- ***TOE Summary Specification***
- ***PP Claims***
- **Rationale**

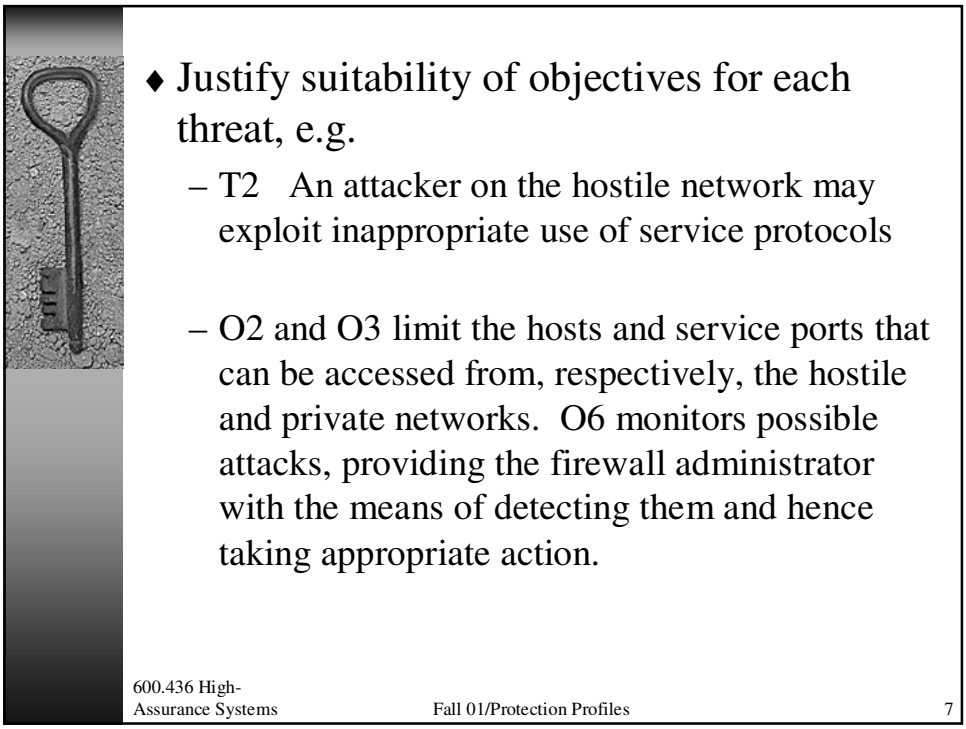


Rationale for Chosen Functional Requirements

- Need to Consider Whether:
  - Objectives address environment
  - Requirements address Objectives
  - Consistency
  - Completeness
  - Technical Soundness

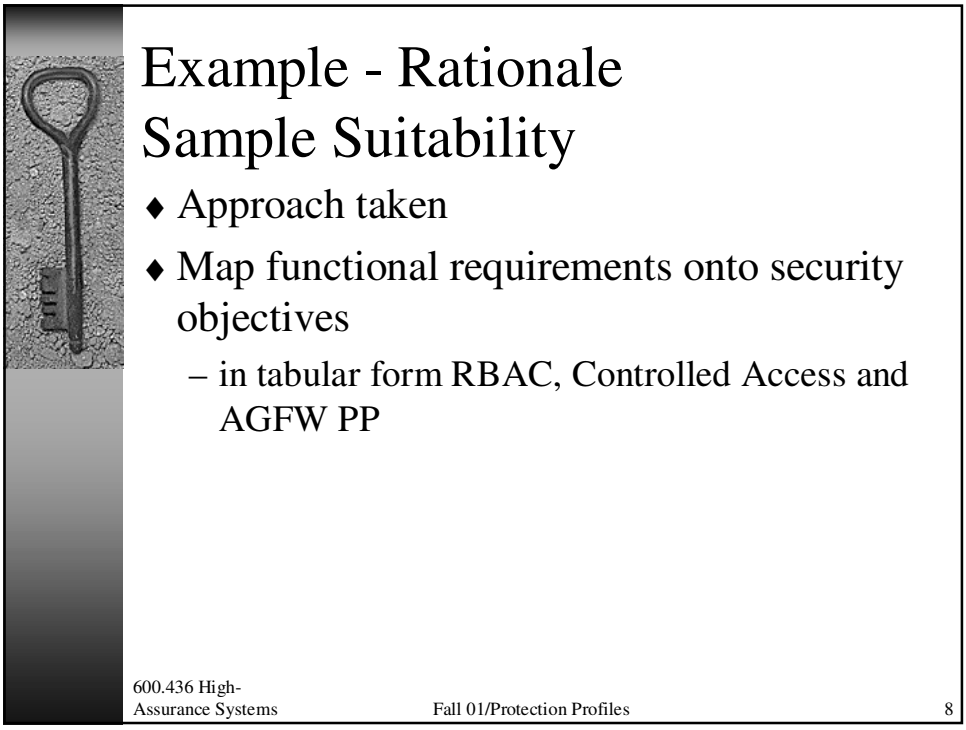

Example
♦ Rationale
– Sample Objectives
– Sample Suitability
– Sample Dependency
– Sample Completeness
600.436 High-Assurance Systems
Fall 01/Protection Profiles
5


Example - Rationale
Sample Objectives
♦ Approach taken
♦ Map security objectives onto threats
– in tabular form (AGFW PP)
600.436 High-Assurance Systems
Fall 01/Protection Profiles
6



- Justify suitability of objectives for each threat, e.g.
  - T2 An attacker on the hostile network may exploit inappropriate use of service protocols
  - O2 and O3 limit the hosts and service ports that can be accessed from, respectively, the hostile and private networks. O6 monitors possible attacks, providing the firewall administrator with the means of detecting them and hence taking appropriate action.

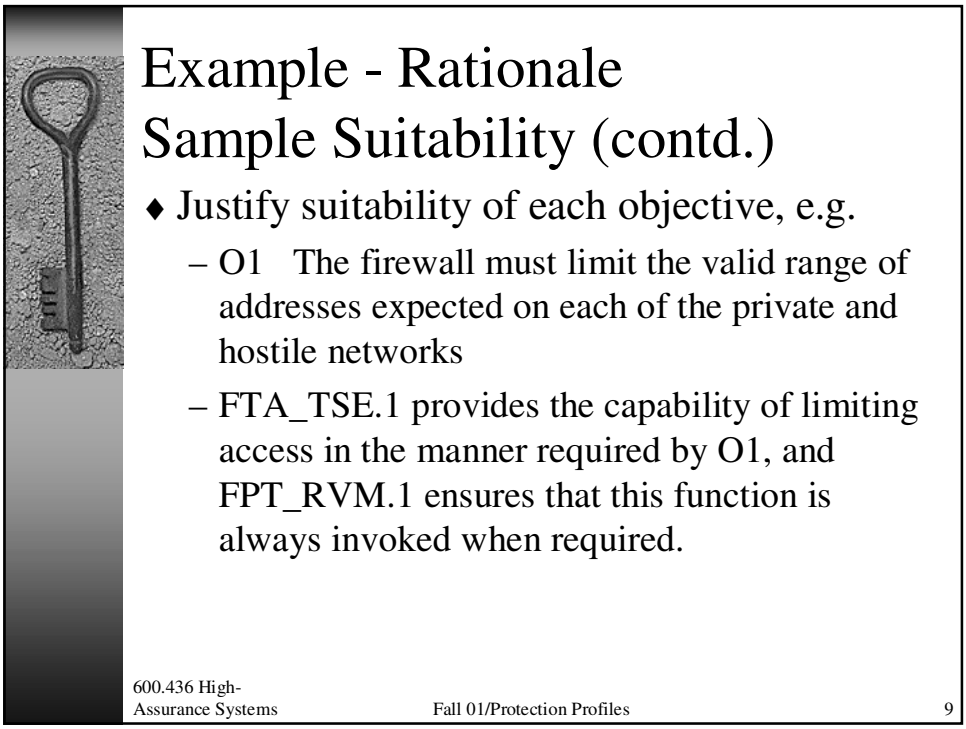
600.436 High-Assurance Systems Fall 01/Protection Profiles 7



Example - Rationale Sample Suitability

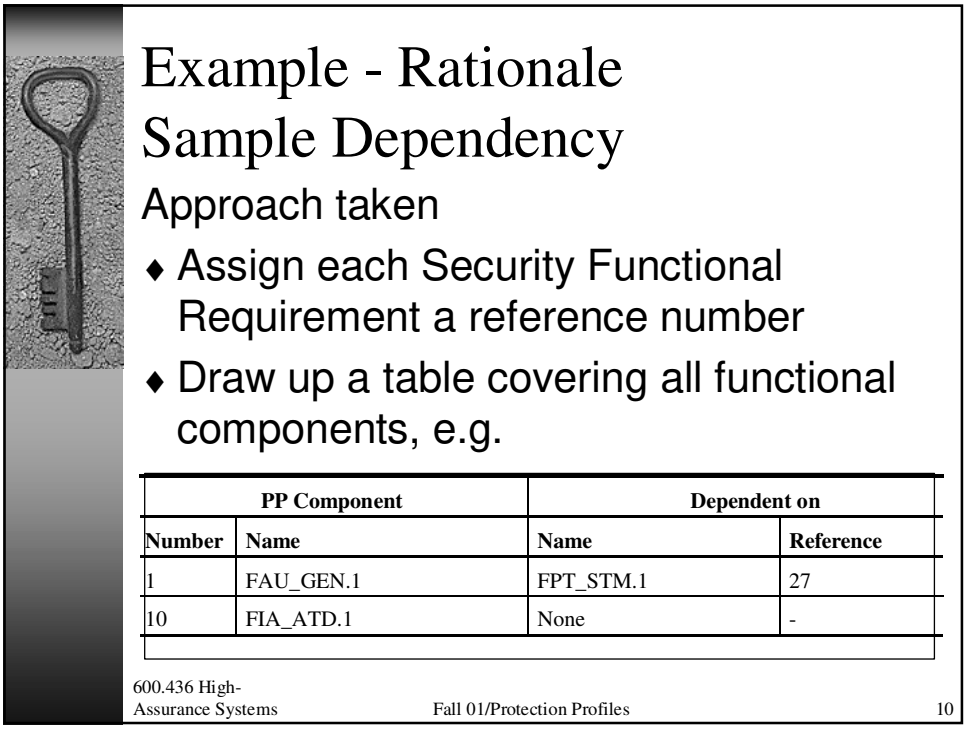
- Approach taken
- Map functional requirements onto security objectives
  - in tabular form RBAC, Controlled Access and AGFW PP

600.436 High-Assurance Systems Fall 01/Protection Profiles 8



Example - Rationale Sample Suitability (contd.)

- Justify suitability of each objective, e.g.
  - O1 The firewall must limit the valid range of addresses expected on each of the private and hostile networks
  - FTA_TSE.1 provides the capability of limiting access in the manner required by O1, and FPT_RVM.1 ensures that this function is always invoked when required.

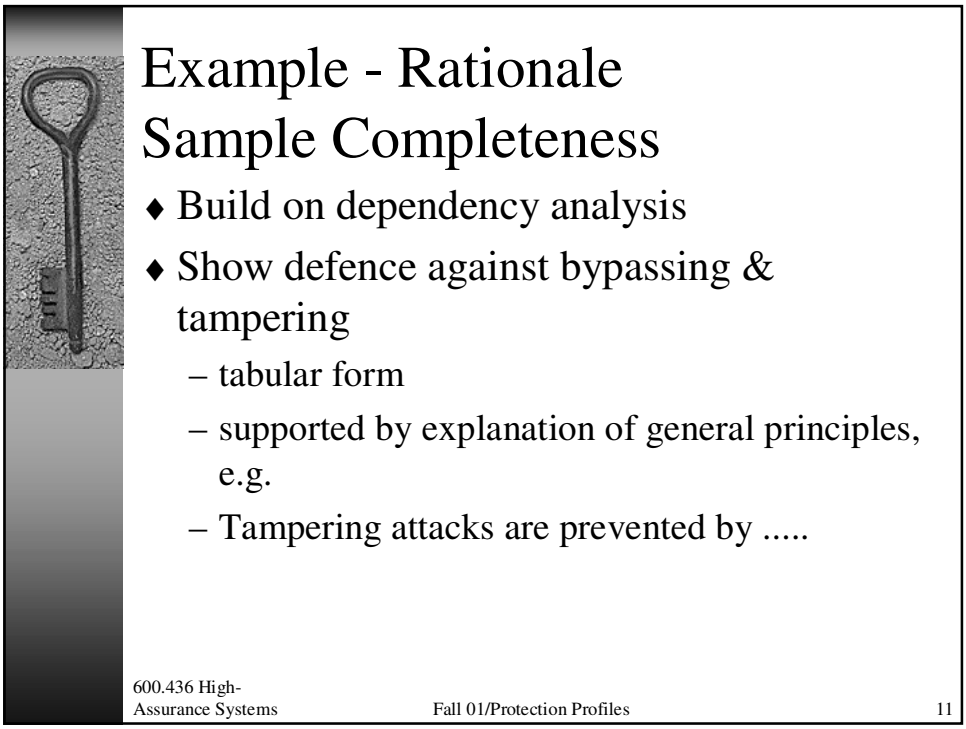


Example - Rationale Sample Dependency

Approach taken

- Assign each Security Functional Requirement a reference number
- Draw up a table covering all functional components, e.g.

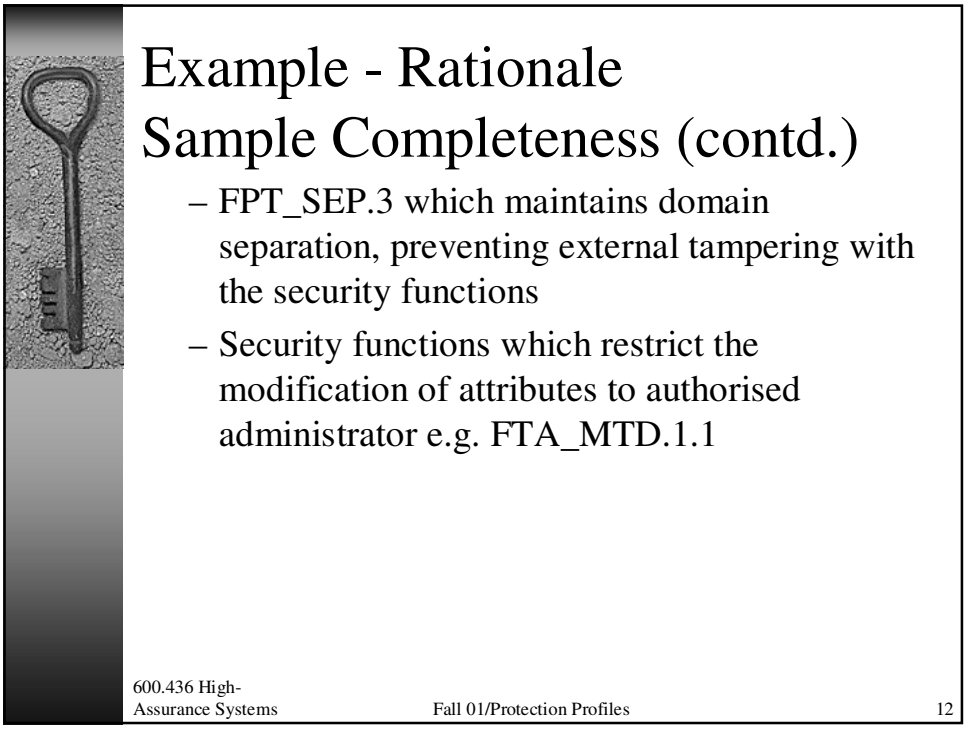
PP Component		Dependent on	
Number	**Name**	**Name**	**Reference**
1	FAU_GEN.1	FPT_STM.1	27
10	FIA_ATD.1	None	-



Example - Rationale Sample Completeness

- Build on dependency analysis
- Show defence against bypassing & tampering
  - tabular form
  - supported by explanation of general principles, e.g.
  - Tampering attacks are prevented by .....

600.436 High-Assurance Systems Fall 01/Protection Profiles 11



Example - Rationale Sample Completeness (contd.)

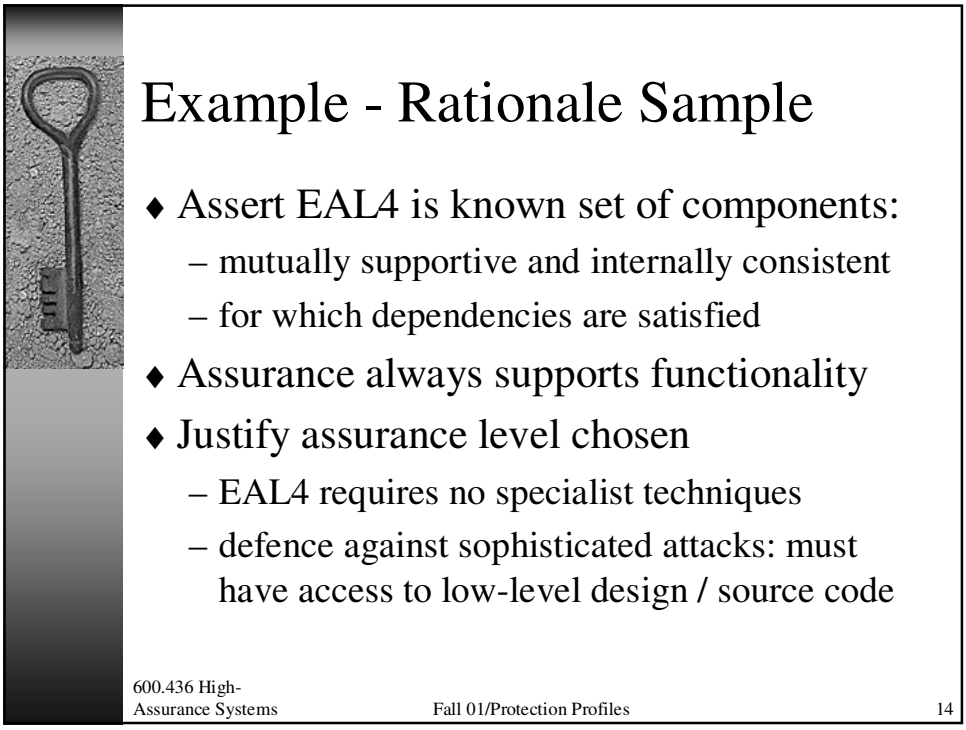
- FPT_SEP.3 which maintains domain separation, preventing external tampering with the security functions
- Security functions which restrict the modification of attributes to authorised administrator e.g. FTA_MTD.1.1

600.436 High-Assurance Systems Fall 01/Protection Profiles 12

Rationale for Chosen Assurance Requirements

- Need to Consider Whether:
- Objectives address environment
- Requirements address Objectives
- Consistency
- Completeness
- Technical Soundness

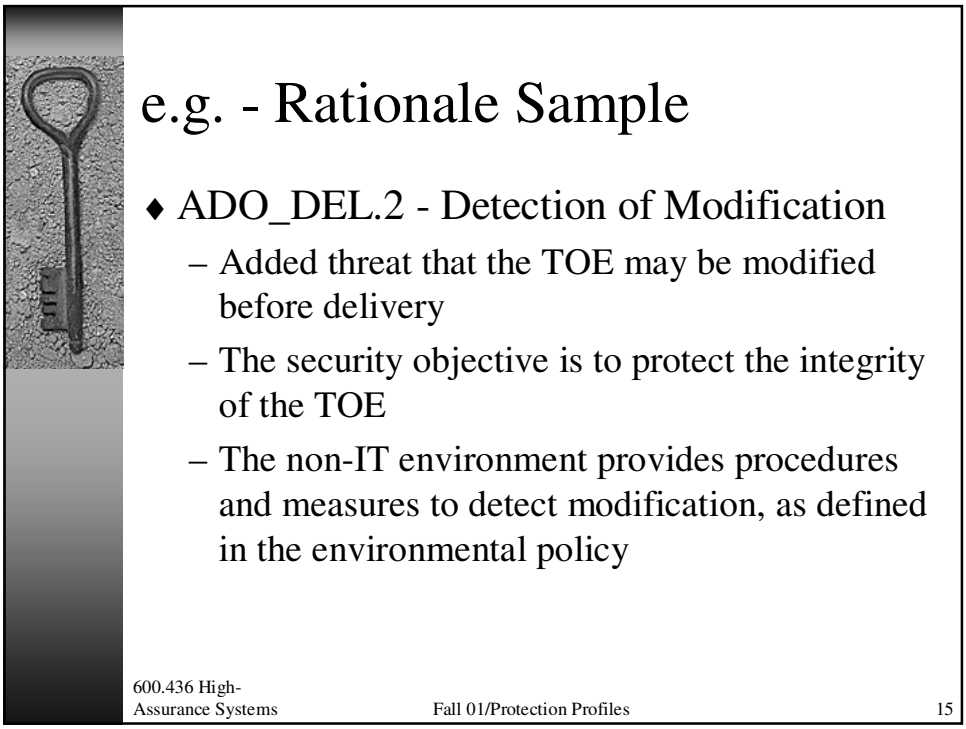
600.436 High-Assurance Systems Fall 01/Protection Profiles 13



Example - Rationale Sample

- Assert EAL4 is known set of components:
  - mutually supportive and internally consistent
  - for which dependencies are satisfied
- Assurance always supports functionality
- Justify assurance level chosen
  - EAL4 requires no specialist techniques
  - defence against sophisticated attacks: must have access to low-level design / source code

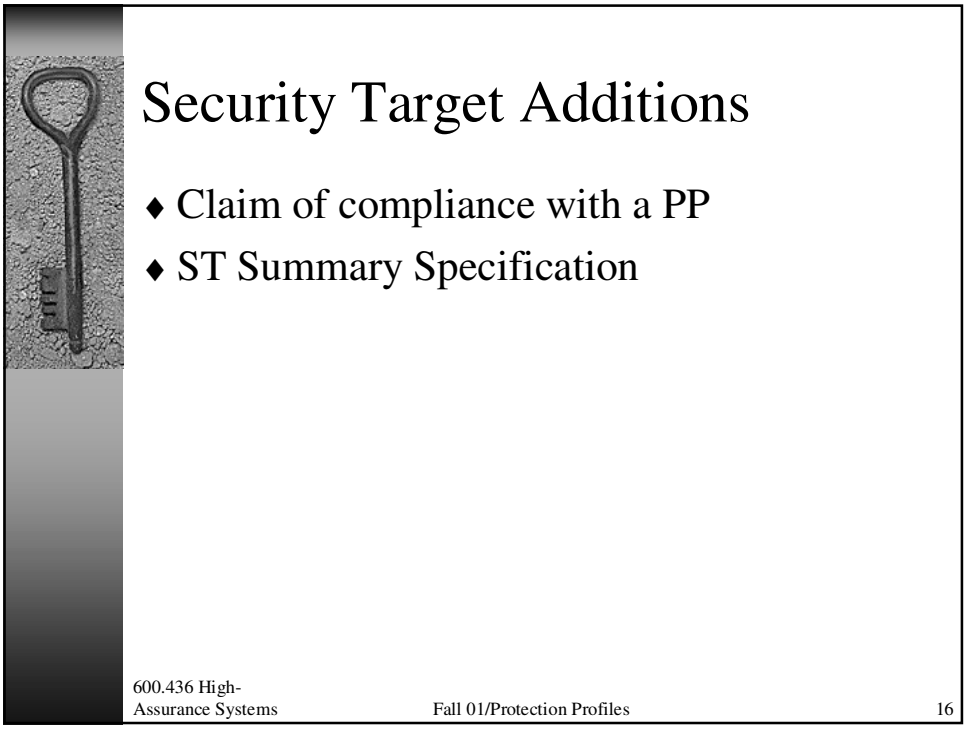
600.436 High-Assurance Systems Fall 01/Protection Profiles 14



e.g. - Rationale Sample

- ADO_DEL.2 - Detection of Modification
  - Added threat that the TOE may be modified before delivery
  - The security objective is to protect the integrity of the TOE
  - The non-IT environment provides procedures and measures to detect modification, as defined in the environmental policy

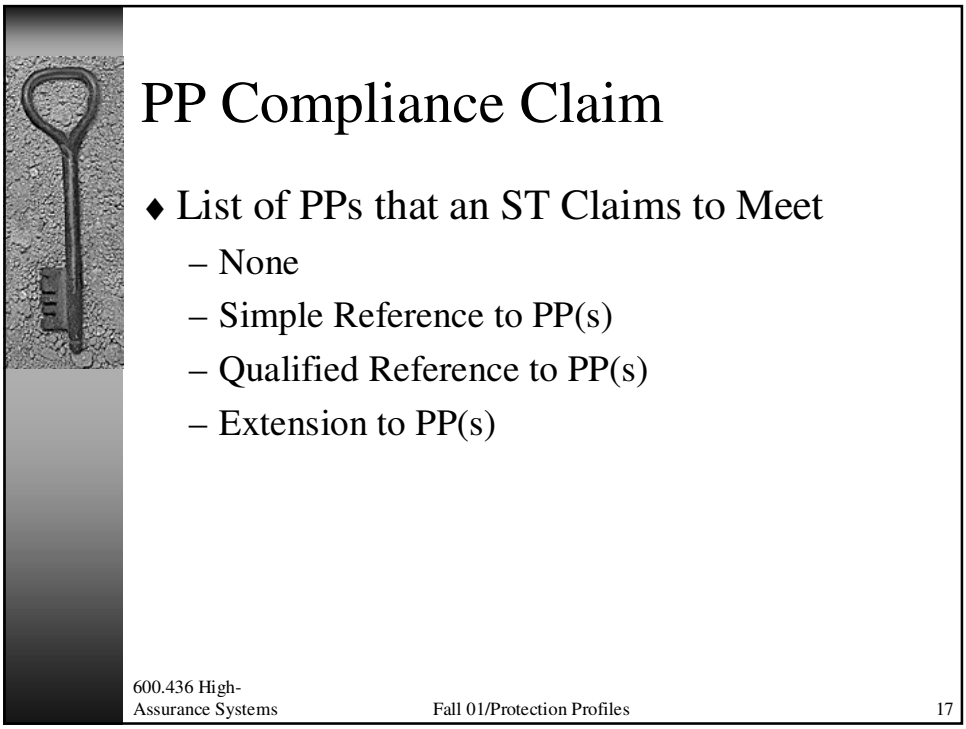
600.436 High-Assurance Systems Fall 01/Protection Profiles 15

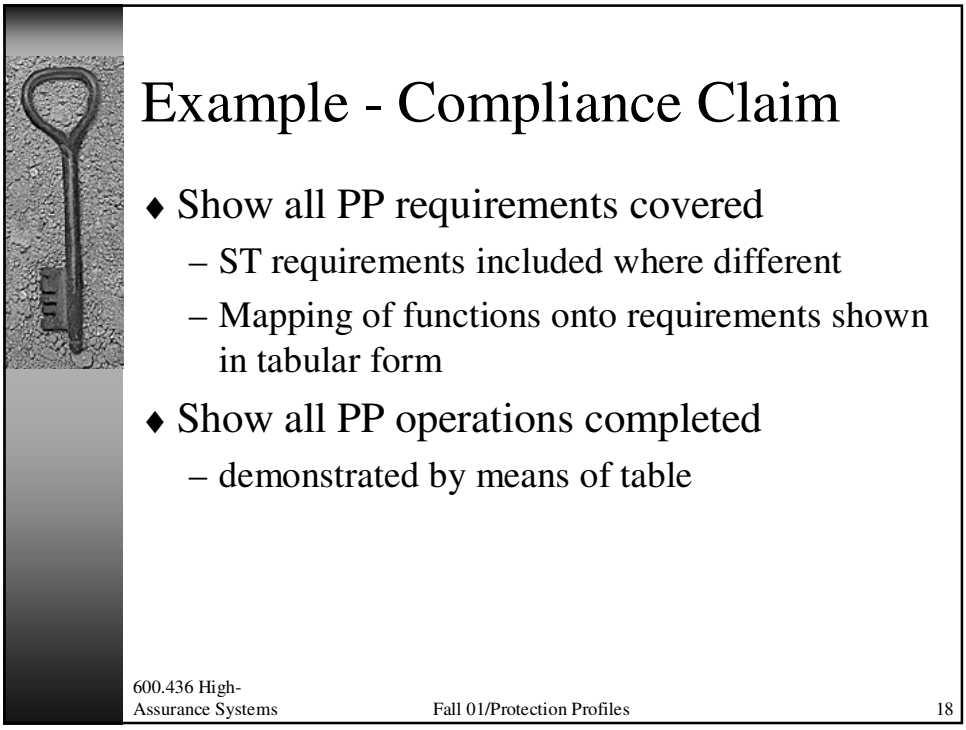


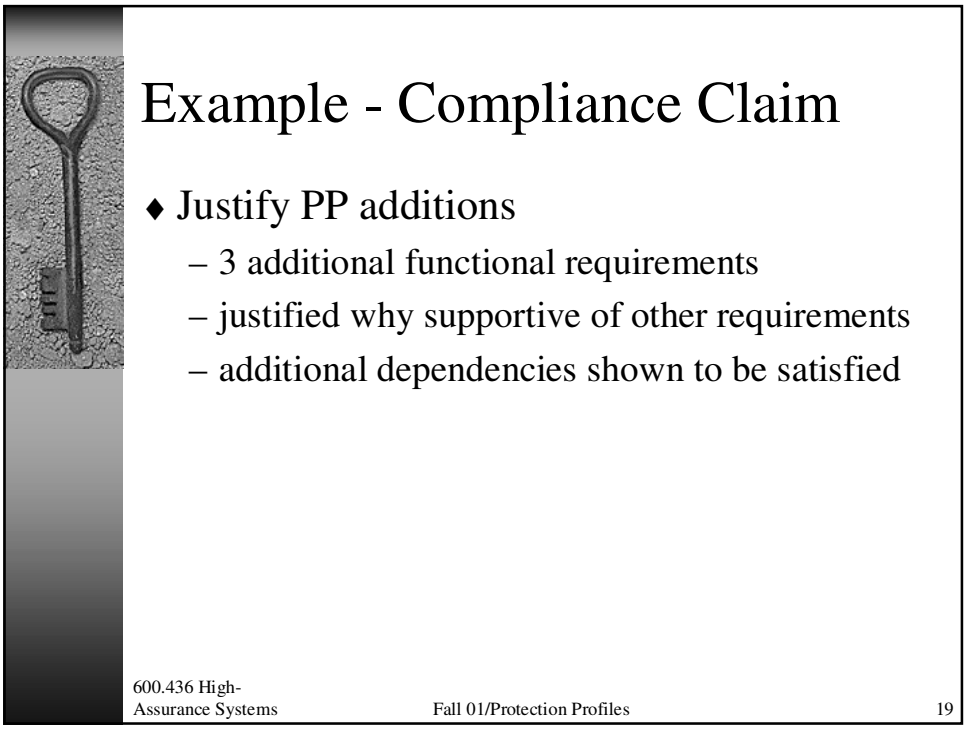
Security Target Additions

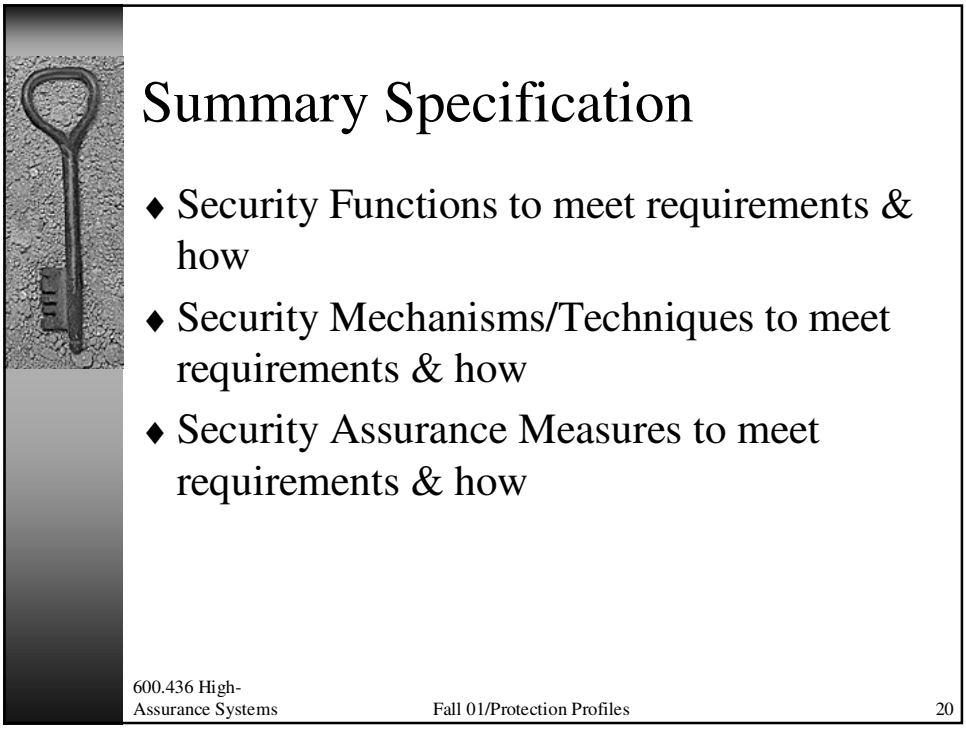
- Claim of compliance with a PP
- ST Summary Specification

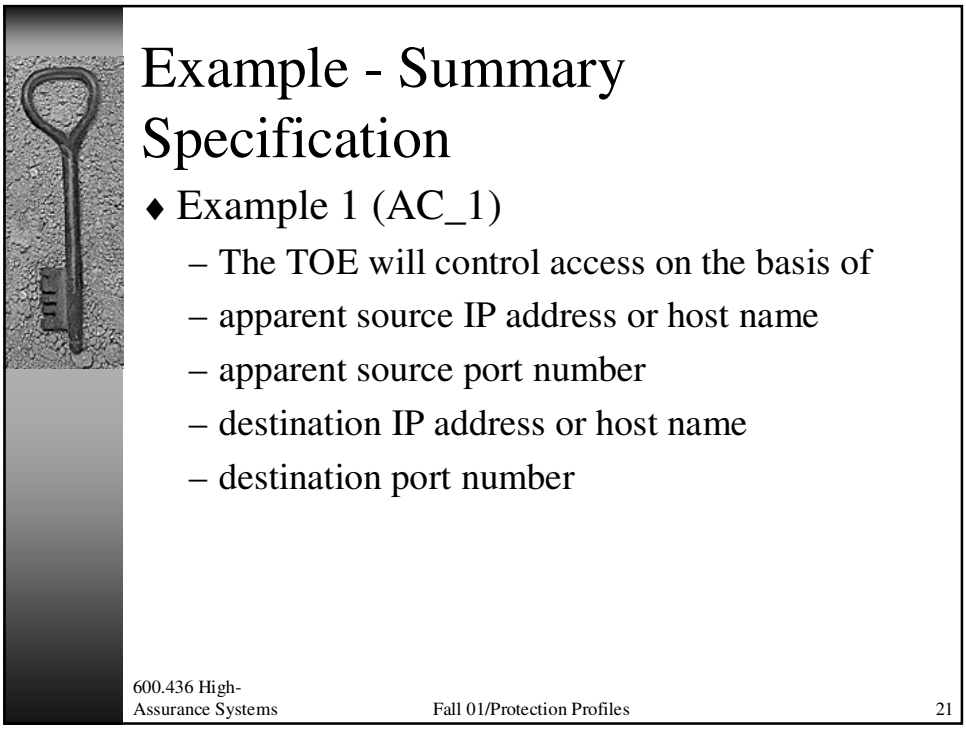
600.436 High-Assurance Systems Fall 01/Protection Profiles 16

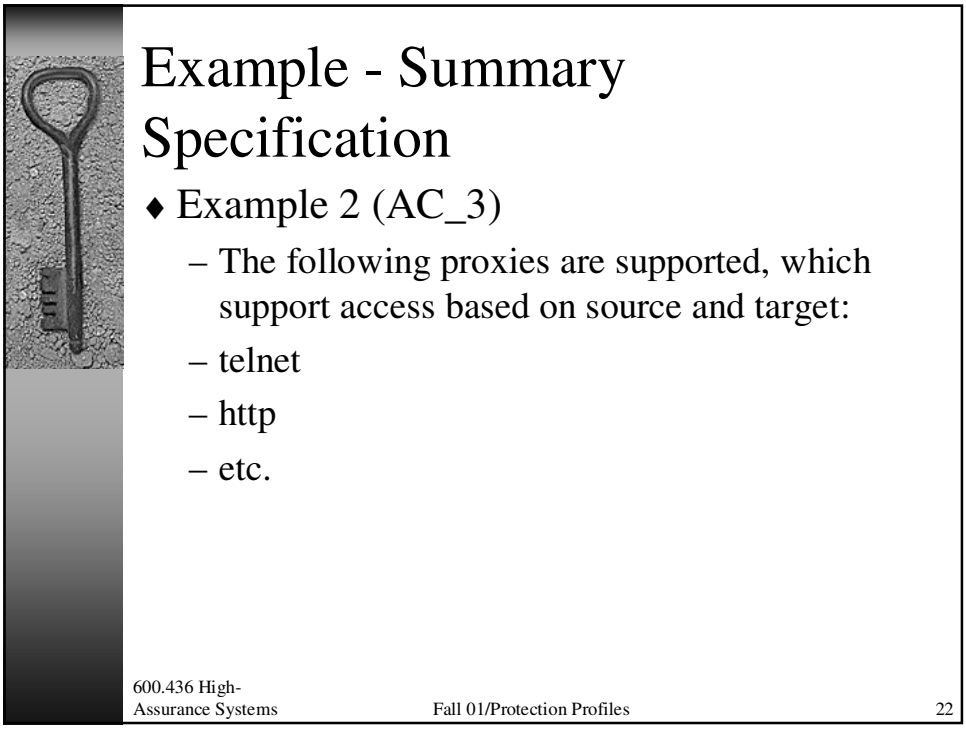

PP Compliance Claim
♦ List of PPs that an ST Claims to Meet
– None
– Simple Reference to PP(s)
– Qualified Reference to PP(s)
– Extension to PP(s)
600.436 High-Assurance Systems
Fall 01/Protection Profiles
17

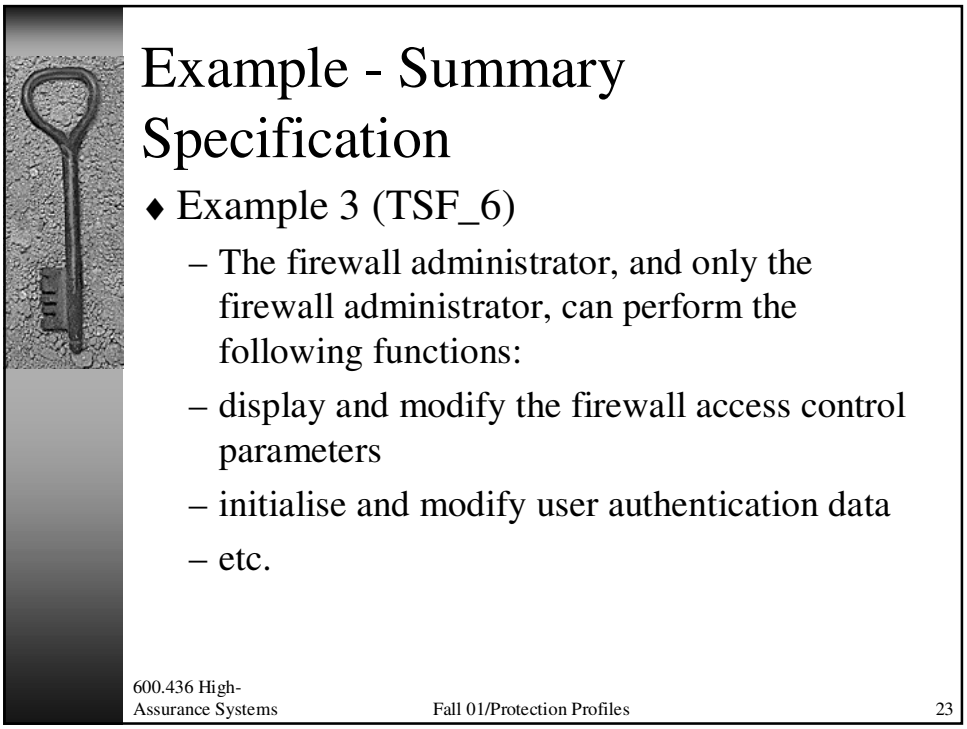

Example - Compliance Claim
♦ Show all PP requirements covered
– ST requirements included where different
– Mapping of functions onto requirements shown in tabular form
♦ Show all PP operations completed
– demonstrated by means of table
600.436 High-Assurance Systems
Fall 01/Protection Profiles
18


Example - Compliance Claim
♦ Justify PP additions
– 3 additional functional requirements
– justified why supportive of other requirements
– additional dependencies shown to be satisfied
600.436 High-Assurance Systems
Fall 01/Protection Profiles
19


Summary Specification
♦ Security Functions to meet requirements & how
♦ Security Mechanisms/Techniques to meet requirements & how
♦ Security Assurance Measures to meet requirements & how
600.436 High-Assurance Systems
Fall 01/Protection Profiles
20


Example - Summary Specification
♦ Example 1 (AC_1)
– The TOE will control access on the basis of
– apparent source IP address or host name
– apparent source port number
– destination IP address or host name
– destination port number
600.436 High-Assurance Systems
Fall 01/Protection Profiles
21


Example - Summary Specification
♦ Example 2 (AC_3)
– The following proxies are supported, which support access based on source and target:
– telnet
– http
– etc.
600.436 High-Assurance Systems
Fall 01/Protection Profiles
22


Example - Summary Specification
♦ Example 3 (TSF_6)
– The firewall administrator, and only the firewall administrator, can perform the following functions:
– display and modify the firewall access control parameters
– initialise and modify user authentication data
– etc.
600.436 High-Assurance Systems
Fall 01/Protection Profiles
23