Writing a Protection Profile for a Security Service Package

Donald Marks, John Hale
Center for Information Security
University of Tulsa

Donald-marks@utulsa.edu
John-hale@utulsa.edu

Disclaimer

- This is not an "official position" of any organization
- These are personal reflections based upon experiences in working with Protection Profiles for Security Service Packages (SSPs)

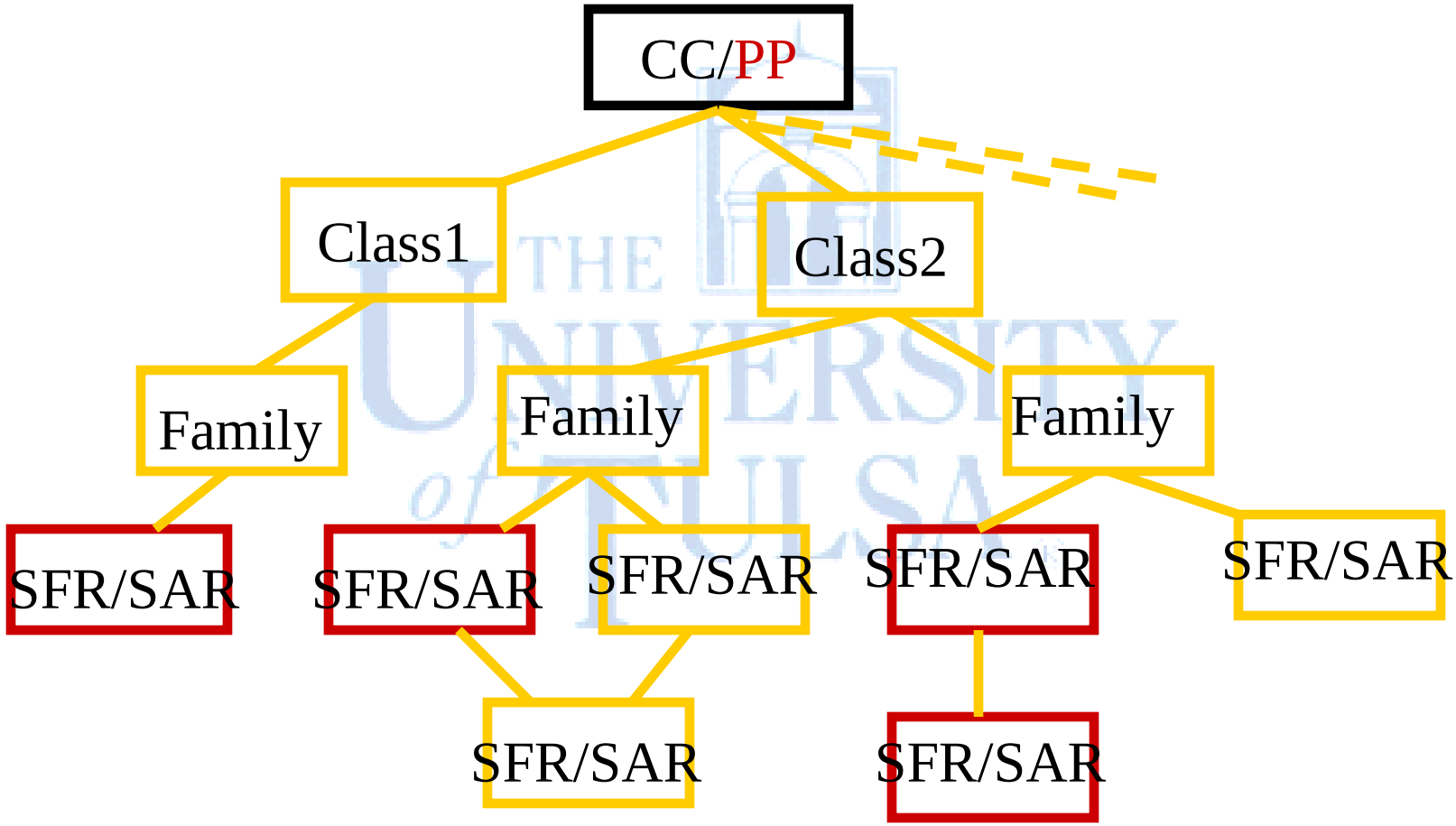
Experiences

- Develop a testable methodology for security service packages (SSP)
- Develop a security target for a smart card
- Teach CC to a graduate class
- Graduate class project to write PP for an SSP

Outline of Talk

- Background
- SSP features
- Differences between PPs & SSPs
- Testing an SSP
- Case study: Smart Card
- Conclusions

CC Organization



Common Criteria

- The CC is viewed as a dictionary of possible security and assurance functions
- CC lists smallest possible increments of these security and assurance functions
- CC organized hierarchically by function
- Wide choice in building PPs, and STs

Protection Profiles

- Protection Profiles (PPs) define an implementation-independent set of security requirements for a class of TOEs.
- Protection Profile document structure (same structure for an SSP)
  1. PP Introduction
  2. TOE Description
  3. TOE Security Environment (Threat, Assumption, Policy)
  4. Security Objectives
  5. Security Requirements (Functional and Assurance)
  6. Application Notes
  7. Rationale
- But, users may need a grouping by purpose, objectives, or "services"

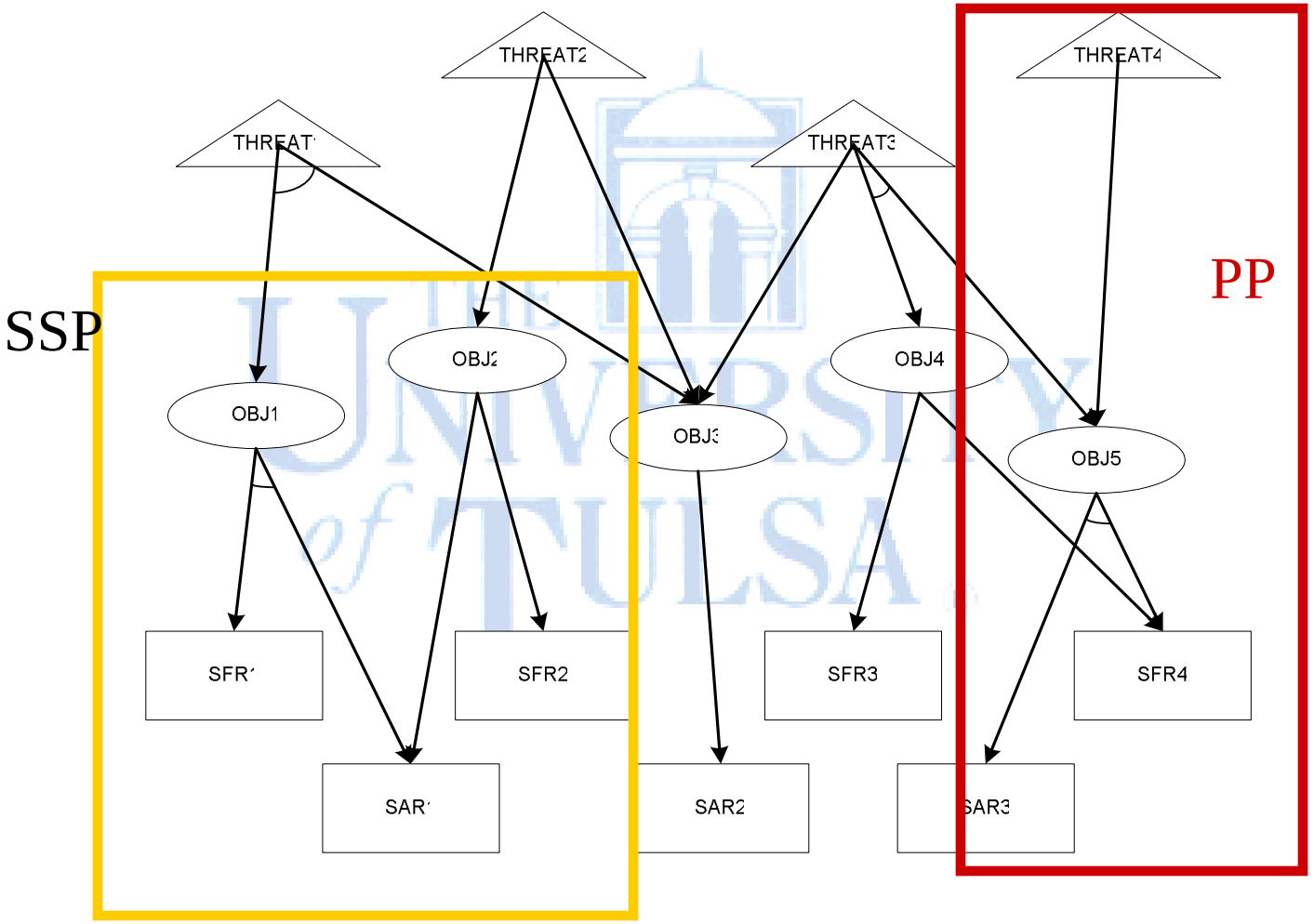
Assurance Grouping

- *Assurance* requirements grouped in Consistency Instruction Manuals (CIMs)
  - Basic, medium robustness, etc
- Grouping makes PPs easier to write
- We need to group security functional requirements into "services"
  - Then write a PP for those *Security Service Packages* (SSPs)

Security Service Packages

- SSPs are distinct forms of Protection Profiles in that they are not intended to identify a concrete or complete set of threats for a TOE.
- SSPs aim at meeting a set of security *objectives*
- Designed as modular elements for constructing PPs
- SSP organization - identical to that of a regular PP
- SSP contents and narrative text broadly characterize essential elements of a security service

PP/SSP Elements



Features of Security Service

- The CC meets all possible situations, a PP meets a specific class of situations, a security service is in between these in generality
- Meets a set of specific security *objectives*, defining threats is less important.
- Should be a specific service, not a general property

Examples

- Access Control
- CC classes for a specific class of use
  - Security auditing for Sarbanes-Oxley compliance
- Any sort of security engineering template
- Other Examples
  - Authentication for military systems
  - Non—repudiation for e-mail
  - Confidentiality for HIPAA

Example: Access Control SSP

- Requirements
  - User identification
  - User authentication
  - Validate access requests
  - System management of security features
  - Protection of security system
- Supplemental requirements
  - Auditing
  - Role and domain management
  - Session security

Scope of Protection Profile for SSP

- The SSP can rarely be used, *without modification*, in any real PP
- Minimum case: all systems implementing access control must have these functions
  - PPs for most real systems will require additional security functional requirements
- Normal case: requirements for the most common implementation of this function
  - PPs for some systems will require deletion (or more rarely, addition) of some security functional requirements

Testable Methodology

- Protection Profiles are tested for completeness and accuracy
  - Common Evaluation Methodology (CEM)
    - Requires a level of completeness not found in SSPs
  - Consistency Instruction Manual (CIM)
    - Lacks necessary detail for evaluating security functional requirements
- Methods updated, applied, integrated, and changes suggested for SSP
- CEM preferred for a formal evaluation

Case Study: Smart Card ST

- Cryptoflex smart card – identification function
  - Access control needed to prevent changing credentials

Case Study: Cryptoflex

- CryptoFlex incorporates a limited OS to manage smart card resources
  - User memory
  - CPU, internal memories
  - Security features
- Features it offers to a reader
  - A secure file architecture
  - A communication interface
  - A set of commands based on ISO 7816-3,4 standards

Use of Access Control SSP

- Cryptoflex is Minimal system – only required 60% of the SFRs in the PP written for a "typical" system
- Still easier than writing PP "from scratch"

Case Study: Minimal AC

- Access control implementation lacking
  - Banners
  - Clocks and time stamps
  - Audit mechanisms
  - Interactive sessions
- As a result. Deleted or modified related
  - Assumptions
  - Policies
  - Objectives
  - SFRs

Case Study: Observations

- STs for some systems will require augmenting SSP security requirements; others (such as the smart card) will require deleting requirements
- SSP for AC limited the number of objectives and requirements that had to be considered
- Promoted consistency in development and writing processes (should promote consistency across STs as well)
- Saved an estimated 30% on development time

Findings, Recommendations and Conclusions

- SSPs cannot simply be inserted into PPs or STs, they must be modified to fit the situation
  - SSPs should address a small set of stated *objectives*
  - SSPs may include threat classes, not specific threats
  - SSPs may address a typical or a minimal system
  - SSPs should not be used as procurement specifications
- SSPs simplify writing PPs and STs
  - Additionally, these documents are more uniform and thus easier to understand and evaluate
- Evaluation similar to conventional evaluation