Foundations of Computer Security

Lecture 78: Protection Profile Example

Dr. Bill Young
Department of Computer Sciences
University of Texas at Austin

PP Example: WBIS

German *Waste Bin Identification System* (WBIS) evaluated to EAL1.

Trash containers have ID tags, read via short-range radio by trucks that weigh them as trash is collected, stores the information and later transmits it to government offices for billing. ID tags contain numbers that are unique but not confidential.

What is the threat model? What are the assets being protected?

PP Example: WBIS

Assets
Records that a waste bin was cleared (trash collected) consisting of (bin ID, timestamp, weight).

Environmental Assumptions

- A.ID: the tag is attached to the waste bin
- A.Trusted: the crew is authorized and trustworthy
- A.Access: access to the system is protected
- A.Check: operator checks at intervals that the data transfer is complete
- A.Backup: operator makes backup copies of the data at intervals

PP Example: WBIS

Threats

- T.Man: attacker smashes the tag
- T.Jam1: attacker sends a signal to corrupt the data read by the truck
- T.Jam2: attacker corrupts data during processing and storage within the truck
- T.Create: attacker creates and broadcasts arbitrary data

Organizational Security Policies

- P.Safe: fault tolerant secondary backup of data within the truck

PP Example: WBIS

Security Objectives

- OT.Inv1: detect invalid ID tags
- OT.Inv2: detect invalid bin-cleared messages
- OT.Safe: fault tolerance

Security Requirements

- Data authentication (FDP_DAU.1)
- Internal transfer integrity protection (FDP_ITT.1)
- Stored data integrity (FDP_SDI.1)

Information from www.cceval.com

FDP_DAU.1 Basic data authentication
User application notes: This component may be satisfied by one-way hash functions (cryptographic checksum, fingerprint, message digest), to generate a hash value for a definitive document that may be used as verification of the validity or authenticity of its information content.

Operations:

> *In FDP_DAU.1.1, the PP/ST author should specify the list of objects or information types for which the TSF shall be capable of generating data authentication evidence.*
>
> *In FDP_DAU.1.2, the PP/ST author should specify the list of subjects that will have the ability to verify data authentication evidence for the objects identified in the previous element. The list of subjects could be very specific, if the subjects are known, or it could be more generic and refer to a "type" of subject such as an identified role.*

PP Example: WBIS

There is a mapping from threats / assumptions to security objectives / requirements:

	OT.Inv1	OT.Inv2	OT.Safe	OE.ID	OE.Trusted	OE.Access	OE.Check	OE.Backup
T.Man	X							
T.Jam1	X							
T.Create		X						
T.Jam2		X						
A.ID				X				
A.Trusted					X			
A.Access						X		
A.Check							X	
A.Backup								X
P.Safe			X					

Lessons

- The German WBIS illustrates the components of a protection profile.
- It doesn't relate to any specific product, but describes what security means for a particular class of systems.
- It provides a systematic way of deciding whether threats and assumptions are being addressed by mechanisms and requirements.

Next lecture: Security Target Example