

SONY

Policies vs Threats

by Albert Dorofeev, Sony Corporation

10th International Common Criteria Conference, 2009

10th ICC, 2009

Policies vs Threats

Contents

SONY

- Security Problem Definition
 - Assets
 - Assumptions
 - Threats
 - Policies
- SPD through the use of Threats
- SPD through the use of Policies
- Examples of SPD to compare
- What happens to attacks and Threats
- Effect of using Policies

Security Problem Definition

SONY

- Assets
- Assumptions
- Threats
- Policies

Assets

SONY

- “assets - entities that the owner of the TOE presumably places value upon.”
- Asset is an object that a customer places into our hands for safekeeping
- (yes, we also have our own secrets to keep)
- The security functionality of a product is usually mainly concerned with the operations on assets

Assumptions

SONY

- Assumptions are made on the operational environment in order to be able to provide security functionality
- Assumption = Limitation of the scope
- Assumption = Risk
 - Once an assumption does not hold, there is no guarantee that the product operates in a secure manner
- Always a trade-off between cost and risk
- Fewer assumptions = Lower risk

Threats

SONY

- An adverse action performed by a threat agent on an asset
- Threats are always evolving as new attacks are discovered
- The list of threats is outdated as soon as published
- The solution applied by the schemes:
 - ST specifies the threats that are very specific for the product
 - The lab applies all the “usual” threats for the category of the product automatically

SPD through Threats

SONY

- Ideally: specific threats against the specific product
 - Really: a disguise for the list of known attacks
 - Result: immediately outdated at completion
 - More: does not fit into the design flow
-
- Side effect is that the ST becomes larger with every new attack and every new customer who has a peculiar threat

Traditional design flow

SONY

Intention

Assumptions/Threats



Objectives



Requirements



Design

Reality

Design



Requirements



Objectives



Assumptions/Threats

Using security policies

SONY

- A positive forward statement of the product's security capabilities, purpose and strengths
- Describe the functionality instead of attacks
- Describe the security functionality relevant to the customer, not for self-defence
- Directly translate into positive Security Objectives

Example : Assumptions/Threats

SONY

- A.Process-Card – Dedicated security procedures are assumed to be established for the delivery of the TOE between the parties and for the protection of the TOE outside of the control of the Developer before the final delivery to the User.
- A.Secure-Key - The cryptographic keys generated outside the TOE are assumed to be reliable, secret and adequately protected from disclosure.
- T.Logical_Attack – Since the TOE allows for software download, an attacker may attempt to use this capability to mount an attack against the TOE.
- T.Eavesdropping – The TOE and its communication channels may be monitored and an attacker may attempt to inject data to mount an attack against the TOE.
- T.Physical_Probing – The TOE may be subjected to an attempt of a physical modification to bypass the protection.
- P.Access_controls - The Administrator can configure an access control policy that links the access control mechanisms with the TOE assets.
- P.Mode - The Administrator sets up the TOE and switches it to the Operational Mode before delivering to the User.

Example : Policies

SONY

- P.Confidentiality - The TOE must provide means to protect the confidentiality of the stored assets.
- P.Integrity - The TOE must provide means to protect the integrity of the stored assets.
- P.TransferSecret - The TOE must provide means to protect the confidentiality of assets during transfer to and from the outside of TOE.
- P.TransferIntegrity - The TOE must provide means to protect the integrity of assets during transfer to and from the outside of TOE.
- P.Configure - The TOE must provide means to configure the level of protection for each of the assets.
- P.Keys - The keys generated for the use by TOE must be secure. The keys for the use by TOE must be generated and handled in a secure manner.

Attacks and resulting Threats?

SONY

- The lab is responsible for
 - checking if the product operates in a useful manner
 - checking that the claimed functionality operates in the stated environment
 - checking that the product remains secure under the known attacks
- The lab is going to verify all these things whether you include them into the Security Target or not
- Best concentrate on the product, not on trying to do the job of the evaluation lab

Effect of using Policies

SONY

- Security Target explains what the product does instead of what it does not do.
- Security Target talks about the security functionality for the customer, not about the security functionality of self-protection.
- Security Target becomes more streamlined, easier to write, understand and evaluate.
- This approach fits perfectly with the “top-down” security design.
- Ultimately saves the cost of both preparation and evaluation

SONY

Thank you!

Albert Dorofeev
General Manager
Sony Secure Communications Europe
albert.dorofeev@eu.sony.com

10th ICC, 2009

Policies vs Threats