Corsec®

Fully Utilizing the Threat Model

Presented to:

September 29th, 2005, by Adam O'Brien

Outline

1. Explain the threat model.
2. Outline the problem with the threat model.
3. Show the value of the threat model.
4. Propose a methodology for analysis of the threat model.

The Threat Model

The security requirements in a Security Target derive from a threat model.

A security problem is postulated in terms of Assumptions, Threats and Organizational Security Polices.

A set of Security Objectives are developed which address the security problem.

The Security Functional Requirements for the TOE are derived from the security objectives.

The Problem

How much value does the threat model add?

Options:

1. Exclude the threat model for lower EALs.

2. Learn to love the threat model. Find ways to gain more from the analysis.

The value of Common Criteria

Any testing program adds value in two main ways:

1. By assessing products
2. By improving products – finding and correcting flaws

   Statistics on the improvements to products from the Common Criteria process are starting to be gathered.

Two Types of Flaw

1. **Design Flaw** - The security functionality of the product isn't a coherent or robust solution to a realistic security problem.

2. **Implementation Flaw** - The security functionality was poorly implemented.

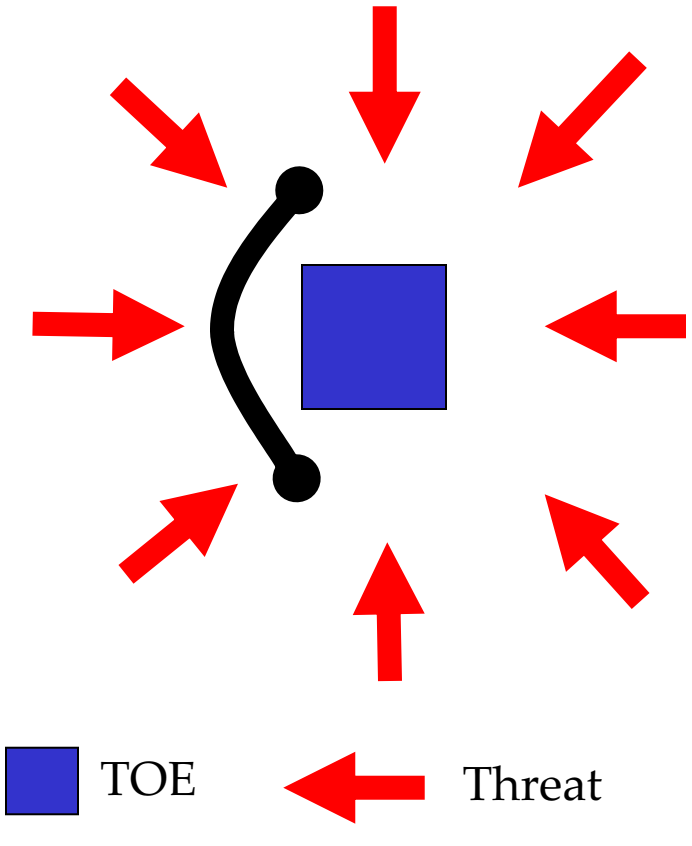
Detecting Design Flaws

Design flaws are detected primarily through the Security Target evaluation.

ASE_REQ.1.12C 'demonstrates that the IT security requirements meet the security objectives'.

The value of the threat model is that it gives a basis for determining that the security requirements are complete and coherent.

An analysis methodology



1. Determine the full range of threats.
2. Understand the assumptions and the environment.
3. Finalize the threats to security.

The Analysis of Threats

- This approach gives a new focus on threat analysis. It needs to determine if the statement of threats is complete.
- The skill is less about analyzing the existing threats than in discovering the missing threats.

Proposals

- Encourage more focus on the analysis of the threat model for completeness.
- Develop methodologies for doing this.

This should result in more design flaws being identified, earlier in the evaluation process.