

The PTA (Practical Threat Analysis) Methodology in a Nutshell

A Calculative Threat Modeling Methodology

The PTA calculative threat analysis and threat modeling methodology enables effective management of operational and security risks in complex systems. It provides an easy way to maintain dynamic threat models capable of reacting to changes in the system's assets and vulnerabilities. With PTA an analyst can maintain a growing database of threats, create documentation for security reviews and produce reports showing the importance of various threats and the priorities of the corresponding countermeasures.

PTA calculates threats and countermeasures priorities and provides decision makers with updated risk mitigation plan that reflects changes in threat realities. Countermeasure's priorities are a function of the system's assets values, level of potential damage, threats probabilities and degrees of mitigation provided by countermeasures. The recommended mitigation plan is composed of the countermeasures that are the most cost-effective against the identified threats.

The Practical Analysis Threat Model

The scheme below describes the interrelations between a threat and the assets, vulnerabilities and countermeasures.

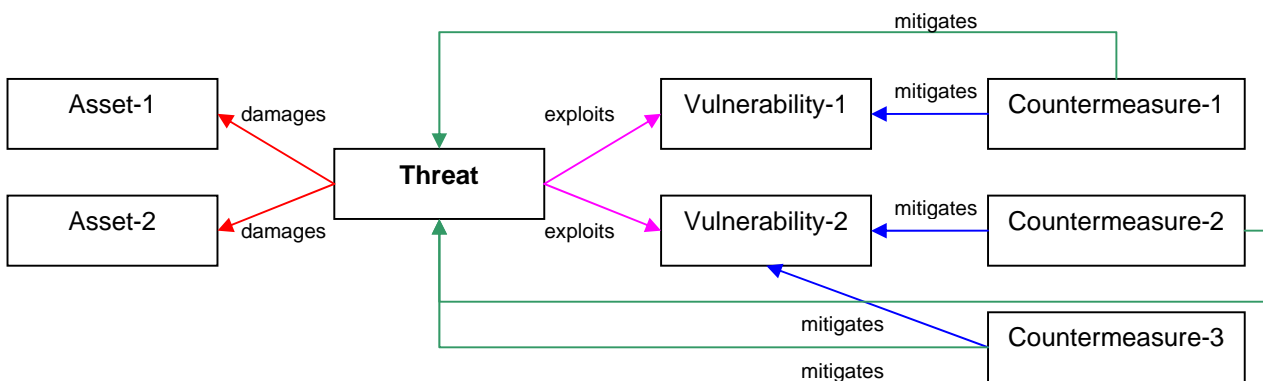


Figure 1: PTA data model sample scheme

In a nutshell:

- **Threats** exploit **Vulnerabilities** and damage **Assets**.
- **Countermeasures** mitigate **Vulnerabilities** and therefore mitigate **Threats**.

The Practical Threat Analysis Process

In the following we present an abbreviated description of the PTA threat modeling steps.

1. **Identifying Assets.** Mapping of system asset's financial values and potential losses due to damages. Asset's values are the basis for calculating threats, risks and countermeasures priorities.
2. **Identifying Vulnerabilities.** Identifying potential system vulnerabilities requires knowledge of the system's functionality, architecture, business and operational procedures and types of users. This is a continuous iterative task coupled with the step of identifying threats (step 4).
3. **Defining Countermeasures.** Defining the countermeasures relevant to system vulnerabilities. The countermeasure's cost-effectiveness is calculated according to its estimated implementation cost.
4. **Building Threat Scenarios and Mitigation Plans.** Composing the potential threats scenarios and identifying the various threat's elements and parameters as follows:
 - Entering a short description of the threat scenario.
 - Identifying the threatened assets and the level of damage caused to each asset.
 - Identifying system's vulnerabilities exploited by the threat. Identification of system's vulnerabilities automatically populates a list of proposed countermeasures.
 - Setting the threat's probability. The threat's risk level is automatically calculated based on the total damage that may be caused by the threat and the threat's probability.
 - Deciding on the actual mitigation plan by selecting the most effective combination of countermeasures.

Starting with Predefined Vulnerabilities and Threats

The threat analysis process can start with predefined entities of assets, vulnerabilities and countermeasures typical to the system being analyzed.

Reviewing the Threat Analysis Results

Reviewing the threat analysis results can help improve the threat model and refine the model entities parameters. The basic analysis outcomes are described below.

- List of threats, their risk and potential damage to assets when threats materialize.
- List of assets and the financial risk that threatens them.
- List of countermeasures, their overall mitigation effect and cost-effectiveness relative to their contribution to system risk reduction.
- The maximal financial risk to the system, the final risk to the system (after all mitigation plans were implemented) and the current level of system risk according to the status of countermeasure's implementation.

It is also recommended to examine how the model behaves in response to changes in parameters and to run various "what if" scenarios that might provide additional insight on the system's realities.

PTA is free of charge for students, researchers, software developers and independent security consultants.

© PTA Technologies 2005 - 2008

www.ptatechnologies.com

+972 3 5443085