Welcome to Practical Threat Analysis (PTA) - a calculative threat modeling methodology and software technology that assist security consultants and analysts in assessing system risks and building the most effective risk reduction policy for their system.

**What is practical threat analysis?**

Practical threat analysis identifies threats and defines the most cost-effective risk mitigation policy for a specific architecture, functionality and configuration. It involves mapping assets, modeling threats and building a mitigation plan that lowers system risk to a minimal, acceptable level. The mitigation plan is composed of countermeasures that are considered to be the most effective against the identified threats.

**A Calculative Threat Analysis and Modeling Tool**

PTA Professional Edition is a calculative desktop tool which 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.

PTA was designed to assist the work of security analysts in building practical threat models for computerized systems. It includes features such as threat builder, risk calculator, risk reduction optimizer, countermeasures cost-effectiveness ranking and controls implementation tracking.

PTA automatically recalculates threats and countermeasures priorities and provides decision makers with updated 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 following picture is a screen shot of PTA’s System Status "bottom lines monitor" which provides an updated view of the security status of the analyzed system as well as indications of the progress of the threat analysis process.
The PTA Threat Model

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

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

See the Practical Threat Analysis in-depth page for a detailed description of the PTA Threat Model and the definitions of Entry Points, Attacker Types and Security Entity Tags.

**The Practical Threat Analysis Process**

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

1. **Identifying Assets**

The correct mapping of assets, their financial value and the evaluation of financial loss to the system's owner when these assets are damaged or stolen, is one of the most critical tasks in the threat analysis process. The assets value is used as the basis for calculating threat risks and countermeasures priorities.
The screen above shows a list of 4 assets identified in a threat analysis case study for a call accounting solution. See the [TACS Call Accounting Case Study](#) for a detailed description of the sample analyzed system.

In some cases the value of assets is less intuitive especially when they are intangible. For example, the confidence of the public in an electronic trading system may be damaged by the appearance of non-relevant text on the system’s Web site. No money is lost, no information is disclosed, all technical resources are still functioning but the site reputation and the shopper's trust are shaken. An indirect financial loss should be set for this type of damage.

Due to the importance of asset mapping, we recommend that the asset list and corresponding values be regularly checked by non IT personnel, such as the company’s CFO, marketing officers and legal consultants. Analysts can quickly perform a “what-if” analysis by modifying asset values and obtaining insights on the model’s accuracy and completeness.

In practice, it is often easier for the analyst to identify system assets through analyzing specific threats (as described in the following). A fact of human nature is that we don’t realize how valuable things are until we lose them. This implies an iterative approach of mapping assets and threats.

### 2. Identifying Vulnerabilities – the real ones

Identifying vulnerabilities requires that the analyst be intimate with the system’s functionality, architecture, implementation and deployment details. The analyst should also be familiar with business and operational procedures and the types of users and other parties involved in system operation.

An analyst can use the Web to find generally known vulnerabilities as published by software vendors and security consultants. Most of the items in these check lists are, in many cases, irrelevant to the specific system or may be easily solved by a simple comprehensive routine such as “always install most updated vendor’s security patches”. The thing that should concern us here is that such a list will draw the attention of the analyst away from the real vulnerabilities that are specific to the analyzed system.

Therefore we highly recommend that the analyst should investigate the system's architecture and implementation details and collaborate with architects, developers, installers and support engineers as well as with the system business managers to discover the real vulnerabilities that are unique to the system and may not be identified without this intimate knowledge. **From experience – the most severe vulnerabilities reside in the interfaces, junctures and stitches between the various elements in complex systems and rarely appear in the standard lists.**
3. Defining Countermeasures

Defining countermeasures produces two outputs:

- A list of countermeasures that protect vulnerabilities. The list includes the implementation cost of each countermeasure. If the countermeasure is already applied it should be marked as (‘already implemented’) to enable producing updated statistics of the current system risk level.
- A map of the relationships between countermeasures and vulnerabilities. This map shows which vulnerability may be mitigated by a specific countermeasure. Sometimes a countermeasure is introduced as a solution to a specific vulnerability, but after additional consideration it turns out that it may help in mitigating other vulnerabilities too.

The accurate identification of countermeasures and their relations with vulnerabilities is the basis for building risk mitigation plans as described in the next step.
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's scenario.
- Identifying the threatened assets and the level of potential damage.
- 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.
- Identifying the vulnerabilities exploited by the threat. Identification of system's vulnerabilities automatically populates a list of proposed countermeasures.
- Deciding on the actual mitigation plan by selecting the most effective combination of countermeasures.

Since threats are the most complex entities in the model, the process of identifying and constructing the threat's elements and parameters has a 'decomposition' nature. During this process the analyst will have to return to previous analysis steps in order to create missing entities, such as assets and vulnerabilities referred by the constructed threat. The screen above presents the GUI that supports the sub-steps of building a threat scenario and a mitigation plan for a single threat.
Reviewing the Threat Analysis Results

Reviewing the threat analysis results can help improve the threat model and refine the model entities parameters. For a detailed description of the analysis results see the Threat Analysis Results and Reports page. 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.
- The optimized mitigation plan which is composed of the countermeasures that are the most cost-effective against the identified threats

The analyst is encouraged 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 Free Program

PTA Free Program is intended for students, researchers, software developers and independent security consultants. As a member of PTA Free Program you may use, free-of-charge, a single instance of PTA Professional Edition for your professional and academic aims - it is our contribution to the security community.

PTA can be downloaded, installed and operate within minutes. We believe that high availability of a calculative practical threat analysis technology will have positive impact on the numerous systems that are responsible for the quality of our life by enabling consultants and engineers to provide better/safer systems. We wish to encourage our users to publish their threat models and customized security entities libraries and to share their experience with the community.