



PTA - Practical Threat Analysis Calculative Tool

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.

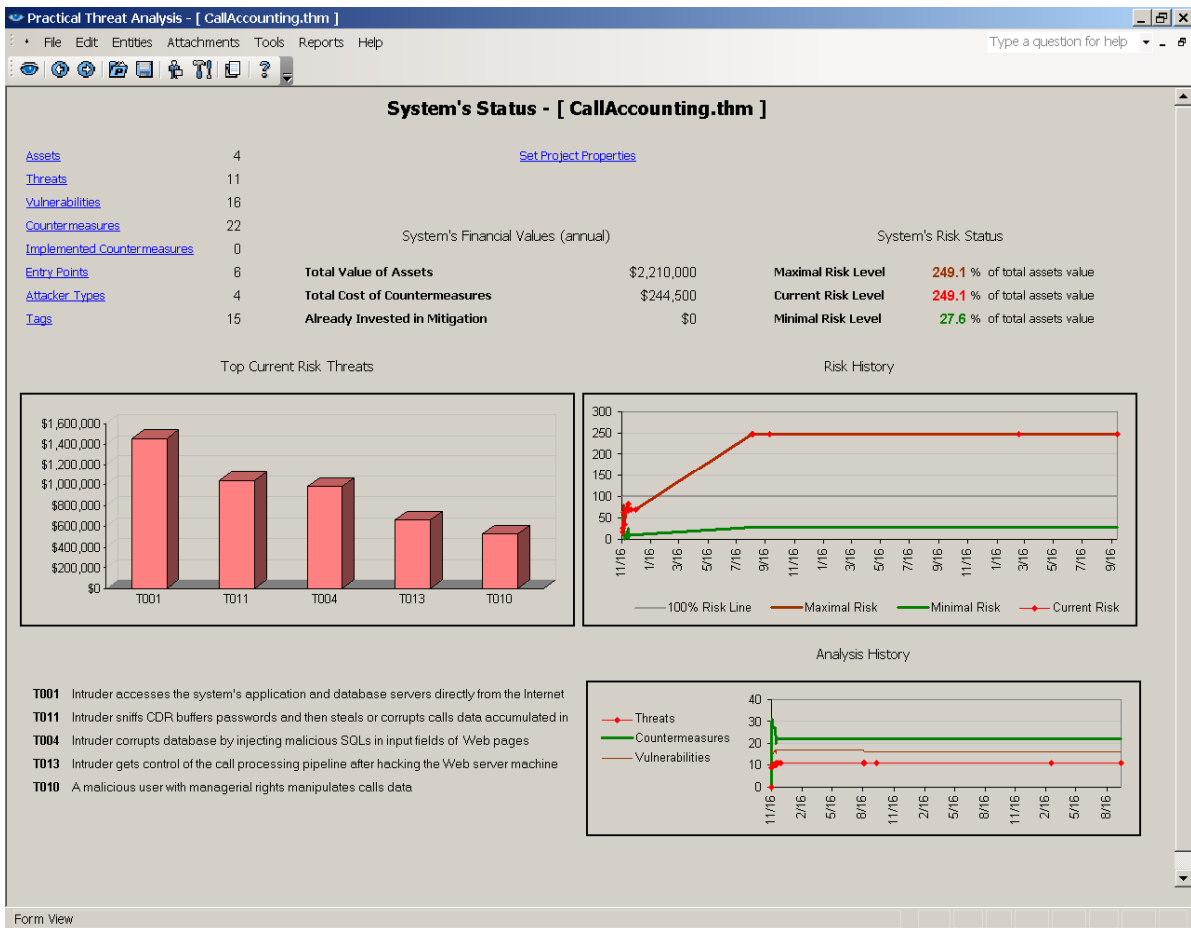
A Calculative Threat Analysis and Modeling Tool

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.

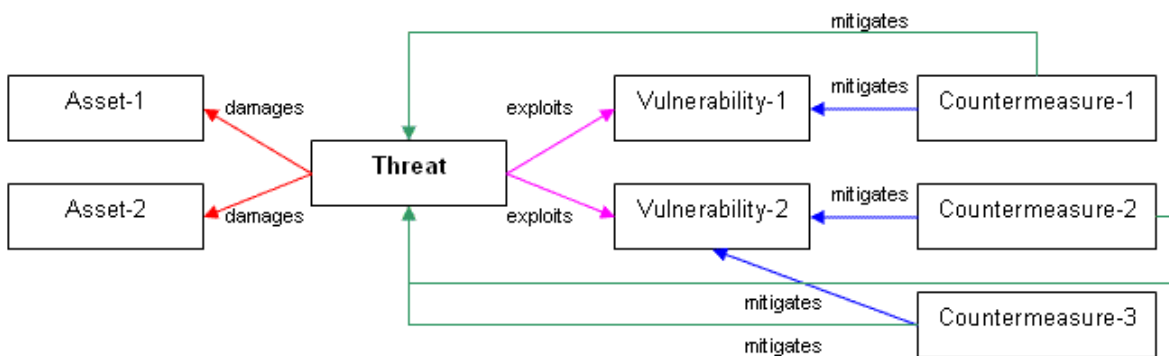


Figure 1: PTA data model sample scheme

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.

ID	Excluded	Name	Tags	Associated Threats	Fixed Value (\$)	Recur. Value (\$)	Annual Value (\$)	Value (%)	Description
A002		The privacy of call details information	Data, Liability	T001, T002, T010, T011, T014	150,000	0	150,000	6.8	Calls details, especially the dialed and the caller numbers are considered private information that should be protected. The asset's value reflects the maximal liability according to the state's privacy-keeping regulations.
A003		The availability / integrity of the system's passwords	Data	T001	10,000	0	10,000	0.5	If passwords are disclosed then there is a need to run a password change procedure for users passwords as well as CDRs buffers passwords. Note that the asset in this case are the passwords themselves and not the damage that may be caused by a malicious use of the passwords.
A011		The availability of the system's Web application and service	Availability, Reputation	T001, T007, T009, T013, T016	0	50,000	50,000	2.3	If the Web application goes down, phone users and managers cannot view phone usage and utilization data. The value reflects the frustration, break of users confidence and cost of manual handling of users' queries.
A012		The accuracy and integrity of the data in the system's database	Data, Financial	T001, T004, T010, T011, T012, T013, T016	0	2,000,000	2,000,000	90.5	The database includes call records and pricing programs that affect the billing and has direct financial values. The value of the asset reflects the maximal annual loss of income caused by corrupted data.

IF An asset is an ability, an advantage, a feature, a financial or a technical resource that may be damaged, lost or disrupted. Damage to an asset may affect the normal function of the system as well as that of individuals and/or organizations involved with the system. Potential damage level is measured in financial terms.

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.**

Practical Threat Analysis - [CallAccounting.thm]

File Edit Entities Attachments Tools Reports Help

Type a question for help

Vulnerabilities (16)

ID	Excluded	Name	Tags	Associated Threats	Relevant Countermeasures	Description
V001		Application servers are vulnerable to exploits via the Internet	Networking, Application Servers	T001	C001, C013	Anyone can reach the server machines by scanning the organization network from the internet. This vulnerability can be mitigated by controlling incoming network traffic.
V003		The database passwords may be sniffed from the LAN when establishing connection with the database server	Networking, Application Servers	T002, T016	C003	Insider may learn passwords that are transferred in plain text by using sniffing equipment.
V004		Insiders and power users can access or modify data	Users / Employees	T002, T010	C019, C020, C021	Super-users such as technicians and administrators can modify data.
V005		System data can be extruded via email/http/ftp protocols	Data, Users / Employees	T001, T002	C006, C007	For example: since the application is managed in a campus-external site by an ASP (application service provider) party, there is always the possibility that ASP employee disclose calls sensitive information.
V009		The Web server and the database server machines may be reached from the LAN	Networking, Application Servers, Users / Employees	T002, T016	C002, C003, C004	Unauthorized personnel that have access to LAN can reach the server machines.
V010		MS SQL server is prone to injection of malicious code via Web pages	Data, Application Servers	T004	C011, C012, C014	Malicious SQL code may be injected via input fields and may cause damage to the data and the structure of the database.
V011		MS Server 2003 and IIS 6.0 have deficiencies that enable to exploit OS resources via HTTP protocol	Application Servers	T009, T013	C013, C014	For example: security exploits such as buffer overrun, url canonicalization and other weaknesses that enable malicious activities through HTTP requests.

V Vulnerability is a weakness, limitation or defect in one or more of the system's elements. It can be exploited to disrupt the normal function of the system. The weakness or defect may be in specific areas of the system, its layout, its users, its operators and/or in its associated regulations, operational and business procedures.

Form View

The screen displays some of the vulnerabilities identified in the sample call accounting system. As mentioned before, the identification of relevant vulnerabilities is a continuous iterative task bundled with the step of identifying threats (described below) - the real sophisticated vulnerabilities are identified when building threat scenarios.

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.

Threat Details

ID: T001 Name: **Intruder accesses the system's application and database servers directly from the Internet**

An intruder gains access to the system's computers and database, steals or modifies data and disrupts system operation. This attack may damage most of the system's assets.

Assets | Vulnerabilities | Entry Points | Attackers | Tags | Attached Documents

Assets that may be damaged by the threat		Asset's Value (\$)	Damage (%)
A002	The privacy of call details information	150,000	100
A003	The availability / integrity of the system's passwords	10,000	100
A011	The availability of the system's Web application and service	50,000	100
A012	The accuracy and integrity of the data in the system's database	2,000,000	100

Buttons: Add Asset..., Edit Asset..., Remove Asset, Threat's Damage to Asset ...

Temporarily Excluded from threat model and risk calculation

Recommended Countermeasures		In Mitigation Plan	Implemented
C001	Install firewall	V	
C006	Install content leakage prevention system	V	
C007	Create acceptable use policy for email and Internet access		
C013	Enforce deployment of latest security patches for OS, database and Web server	V	

Buttons: Edit Countermeasure..., Include Countermeasure in Mitigation Plan...

Value At Risk (VAR)

	in %	in \$
Max	66.0	1,458,600
Current	66.0	1,458,600
Min	3.3	72,900

Probability and Damage

Num of Annual Incidents: 0.66

Damage of a Threat Incident:

	in %	in \$
	100.0	2,210,000

Mitigation Plan

C001, C006, C013

Max Available Mitigation: 95 %

Current Mitigation 0 %

Buttons: Threat's Probability..., Threat's Mitigation Level...

Buttons: Apply, Cancel

Record: 5 of 11
Form View

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.