

Practical Threat Analysis

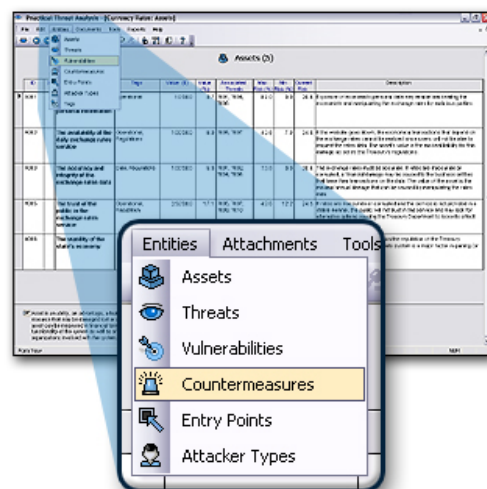
PTATechnologies

What is PTA ?

PTA (Practical Threat Analysis) is a risk assessment methodology and a suite of tools that enable users to find the most beneficial and cost-effective way to secure their systems and applications according to their specific functionality and environment.

How does it work?

The threat analysis process begins by describing the specific threats and vulnerabilities of the system. The threats are then associated with assets that might be damaged. The process continues by finding the exact countermeasures that will fit different threats. The risk level, potential damage and countermeasures required are all presented in real \$ values. PTA automatically calculates the level of risk and the maximum available mitigation and advises on the most cost effective way to mitigate threats and reduce overall system risk.

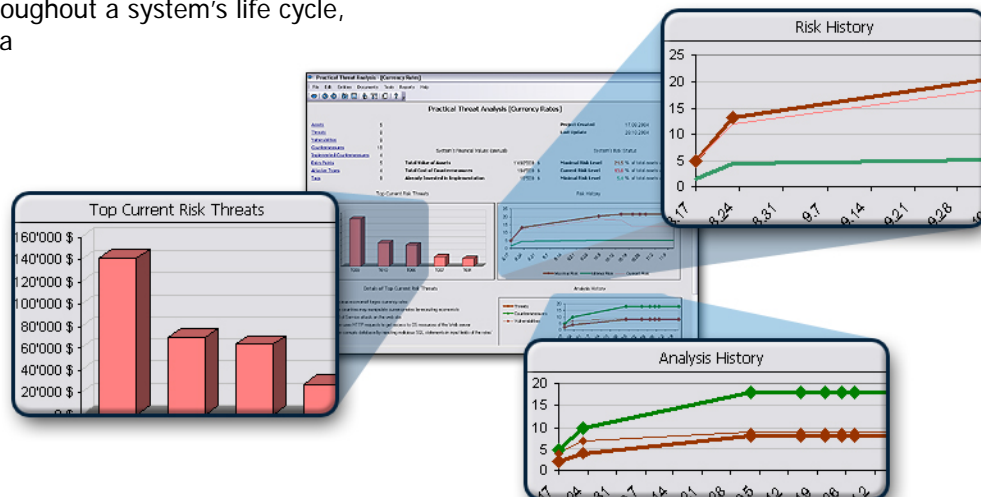


Who should use PTA?

PTA was designed to assist the work of security consultants, software security engineers and information security officers.

When should threat analysis be done?

The best time to use PTA is during system design phase. Potential losses and security countermeasures may be defined at the start and prevent future problems. For systems already in operation, PTA can identify areas of corrective actions. Since threats, vulnerabilities and countermeasures vary throughout a system's life cycle, threat analysis should be a continuous task.



What are the common problems arising during system threat analysis?

- Analyzing only a particular 'environment', for example networking, makes it difficult to thoroughly explore threats. This is especially true in complex applications with many interfaces.
- Analyzing a system only once during its life cycle.
- There is no quantitative valuation of the severity of threats in real \$ value.
- The outcome of the analysis does not include clear recommendations on the most efficient and cost-effective countermeasures required.
- Threat analysis models are not dynamic; changes in any parameter of the model will not be immediately reflected in the countermeasures recommended.

#T001 Hacker corrupts database by injecting malicious SQL statements in input fields of the rates Web page

Assets (2)

ID	Asset	Threat's Damage to Asset
A001	The confidentiality of economists' personal information	90 %
A003	The accuracy and integrity of the exchange rates data	90 %

Vulnerabilities (1)

ID	Vulnerability
V006	SQL server is prone to injection of malicious code via Web pages

Countermeasures (4)

ID	Countermeasure	Mitigation Level
C005	Database login accounts should be given the minimal rights that are necessary for their functionality	85 %
C006	Implement validation of input fields in rates web pages	80 %
C007	Enforce data access via stored procedures with formal parameters content validation	80 %
C009	Enforce security code review	33 %

The solution

Using PTA, analysts can quickly build threat models, analyze risks and manage risk mitigation policies relevant to the application's domain. Inputs are obtained from a variety of external sources e.g. vulnerability scanners, real-time network analyzers, security event repositories and security standards databases. The information can be entered manually as well as automatically.

PTA will save you time and money. In addition to recommending the most cost effective countermeasures, PTA presents the current level of security of the monitored system. Once used, PTA enables dynamic changes in each of the defined threats, vulnerabilities, assets and countermeasures parameters. This allows an effective and continuous security management, throughout the application's life cycle without duplicating efforts and at minimal cost.