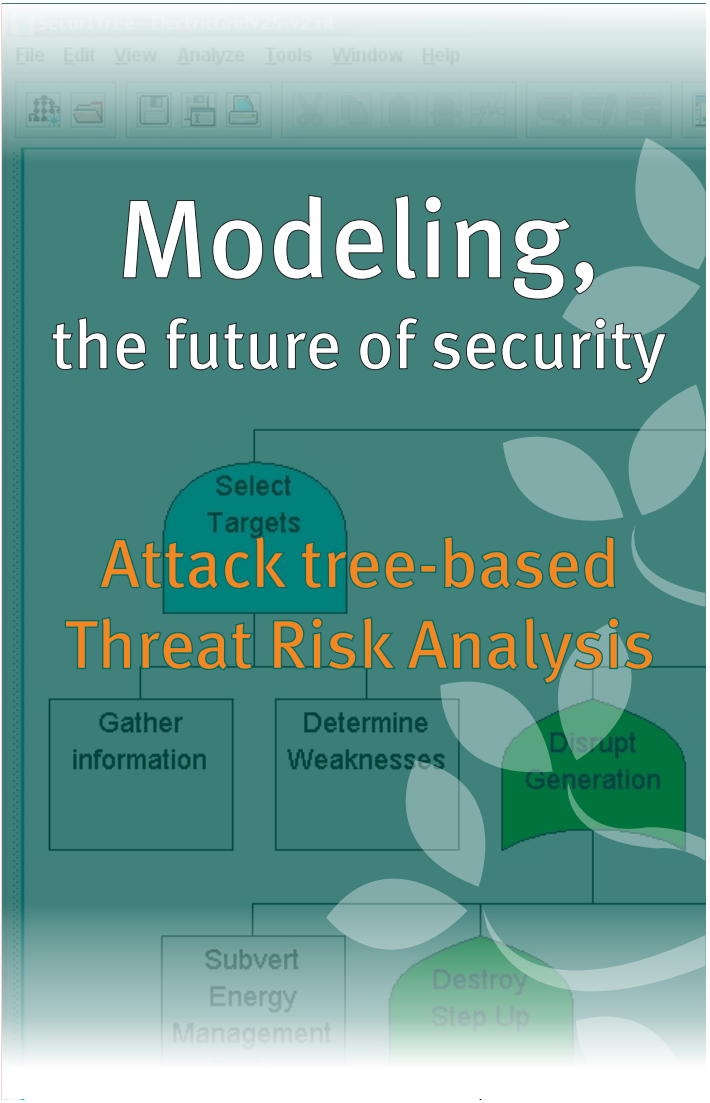
Amenaza®
TECHNOLOGIES LIMITED

Modeling, the future of security

Attack tree-based Threat Risk Analysis

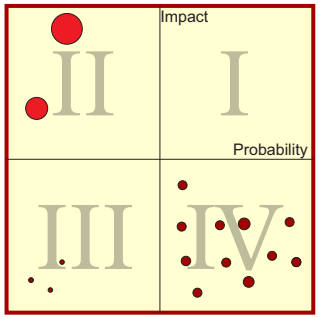


SecurITree

Advanced hostile threat risk analysis for
Information Technology & Industrial Control Systems

Quadrant II hostile risk

The risk of a harmful attack occurring is determined by its likelihood and potential impact. Plotting these two factors yields a graph that can be divided into four quadrants.



Since no operational IT or ICS environment experiences frequent, catastrophic events, quadrant I (Q-I) is empty.

Q-III represents seldom occurring attacks of marginal impact. Q-III can be safely ignored.

Q-IV events are the routine, low impact security incidents that occur regularly in any practical environment. They are identified and dealt with routinely. Dealing with Q-IV events often consumes considerable time and resources, but these nuisance events seldom have long term impact.

Q-II is the most difficult quadrant to deal with. While there are many hypothetical high impact events, most will never happen. The challenge is in distinguishing between the high impact attacks that will never occur (and require no mitigation), and those that have simply not occurred yet. Q-II includes Advanced Persistent Threat (APT) attacks. APT events are rare, but potentially devastating!

In a pure mathematical sense, the risk from Q-II attacks may appear acceptable. Their low probabilities can easily lull the unsuspecting into a false sense of security. However, a Q-II event in a high value IT environment might threaten the existence of the target organization. A Q-II event in an ICS system (such as a nuclear facility) would have devastating consequences not just to the ICS operator, but also to public safety.

The meteor impact that ended the reign of the dinosaurs was a low frequency event, but the impact was terminal (even though the annual risk was not excessive). Similarly, a failure of the industry to anticipate and deal with potential Q-II events may have irreversible consequences.

SecurITree®

Capabilities-based Threat Modeling

Amenaza's SecurITree software tool was specifically designed to analyze hostile risk. It is especially effective at identifying those potential quadrant II events that pose a concern.

SecurITree does not use a conventional, checklist-based analysis approach to evaluate security. Instead, analysts create graphical, attack tree models describing their systems and the adversaries that threaten them. These models use quantitative metrics plus subject matter experts' ratings as a basis for analysing the threatscape. Specifically, SecurITree considers

1. The resources required to exploit a target's vulnerabilities and cause a security incident
2. The adversary's strengths and resources
3. The degree to which an attack satisfies the adversary's objectives

1) and 2) determine how feasible an attack is for a given adversary. 3) is a measure of whether the attack is desirable. Combined, the three factors, provide a mechanism for SecurITree to estimate the attack's probability and frequency.

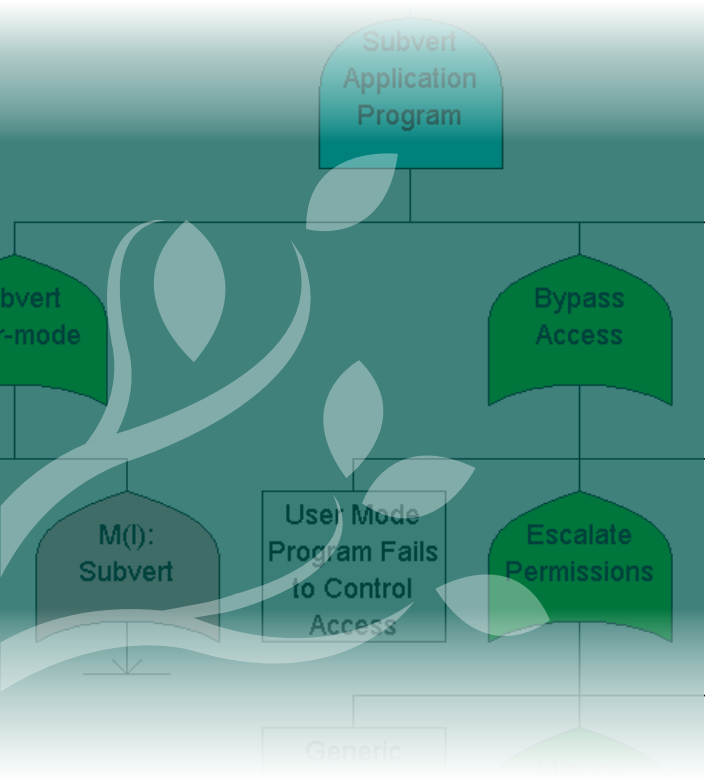
The attack model then considers the attack's impact on stakeholders. The combination of probability and impact provides a quantitative measure of risk.

This approach combines the "think like an attacker" philosophy used by military Red Teams with the analytical capabilities of computer models used to solve engineering problems. SecurITree's attack tree-based models can evaluate vast numbers of attack scenarios, including those too dangerous to ever be attempted by a conventional Red Team.

Documented Security

Good security is no longer good enough. SecurITree's attack tree models capture the factors and logic that lead to security decisions. They demonstrate that due diligence was performed.

Amenaza®
TECHNOLOGIES LIMITED



Contact Us

406 – 917 85th St SW, m/s 125
Calgary, AB Canada T3H 5Z9

TEL (403) 263-7737
FAX (403) 278-8437
TOLL-FREE 1-888-949-9797

E-MAIL info@amenaza.com

Who is Amenaza Technologies?

Amenaza Technologies Limited is a Canadian company based in Calgary, Alberta, Canada.

Incorporated in 2001, Amenaza produces highly specialized, security modeling tools that have been adopted in various high security fields.

Although Amenaza is a small company, it has unparalleled expertise in the field of attack tree analysis. Amenaza's SecurITree attack modeling software is the most advanced commercially available software package of its type in the world.

What is SecurITree® ?

The SecurITree threat risk modeling software tool is based on principles that originated in the intelligence community.

SecurITree models how physical, electronic and mixed systems respond to attackers. SecurITree helps defenders to find chinks in their armor and allows them to plan and test proposed solutions. It documents the process that has been used to secure a system.

Who uses SecurITree® ?

Most of Amenaza's customers are on the Fortune 500 list – many are in the Fortune 100. Five of the top eight aerospace/defense companies in the world are licensees of the SecurITree software. One of these customers recently commented, "SecurITree continues to be the best available tool for security risk assessments on our military programs."

SecurITree is gaining in popularity for the analysis of industrial control systems, particularly those involving critical infrastructure. One entity involved in the security and reliability of the power grid has used SecurITree to model over 1 billion attack scenarios! Others use SecurITree to model threats against nuclear power facilities.

SecurITree

Who are the people behind Amenaza Technologies?

Terrance R Ingoldsby is the President and Chief Technology Office at Amenaza. Terrance has almost thirty years experience in the fields of information technology and information security. He is the chief architect of the SecurITree software package.

In addition to his own technical expertise, he has long experience in participating in and managing cutting edge software projects.

Terrance holds a BSc(Physics) and a MSc(Computer Science). He also has the CISSP accreditation.

Christine M McLellan is Amenaza's Vice President of Software Development. With over thirty years of experience in multiple software development environments, Christine has overseen the development of the entire SecurITree software package since its inception.

Christine holds a BSc(Computer Science).

Amenaza®
TECHNOLOGIES LIMITED