Amenaza
TECHNOLOGIES LIMITED

The Value Proposition for Attack Tree Risk Modeling

The Business Need for Improved Threat Risk Analysis (TRA) Tools

Risk analysis is nothing new. Businesses of all types have long had formal risk analysis processes to evaluate a variety of financial, investment, environmental and liability exposures. Until recently, however, it has been unusual for an organization to formally consider operational risks due to hostile, malicious adversaries. If any thought was given to the subject at all it was usually in the form of a burglar alarm or security guard.

Four significant societal changes have made this informal view of hostile threats inadequate.

1. The widespread dependence of society on infrastructure and technology has greatly increased the amount of damage that can potentially be inflicted on businesses and citizens.
2. The accessibility to and familiarity with infrastructure by large numbers of people have greatly increased the level of threat.
3. Changes in the world order have resulted in a large number of people, unrestrained by moral barriers, that are motivated and capable of inflicting damage on infrastructure systems.
4. Increasingly, legislative controls[1] hold organizations responsible for breaches in security.

These issues have an impact in many different disciplines. Electrical generation and transmission facilities, gas pipelines, water treatment plants and nuclear facilities are all exposed as never before.

The dangers are especially visible in the area of information technology. Businesses of all sizes are now accessible to millions of potential *hackers* via the Internet. Employees now have potential access and control of information that, just a few years ago, might have been accessible only to senior company officials. Some studies have shown that a major failure in company's information systems often leads to the business's demise. The relative immaturity of the information technology field (compared to other engineering disciplines) has resulted in many questionable security practices. This has driven many governments to create legislation (e.g., HIPAA, PIPEDA) mandating information security.

The need for rigorous risk assessment tools and methodologies seems clear. Unfortunately, **existing techniques are almost all probability-based and do not work well for understanding hostile threats**. For this reason Amenaza has created a product (Secur*IT*ree®) that uses a completely different mechanism, known as *capabilities-based attack tree analysis.* It

[1] Recent US legislation includes the Gramm Leach Bliley Act governing financial institutions, the HIPAA regulations in the health care arena and California state legislation making it mandatory for companies to notify customers whose personal data have been disclosed through a security breach. The Canadian PIPEDA rules govern privacy issues. In some cases company officers and directors may be held personally responsible for breaches in security.

Amenaza Technologies Limited
550, 1000 8th Ave SW
Calgary, AB, Canada
T2P 3M7

Tel: (403)263-7737
Fax: (403)278-8437
Toll Free: 1-888-949-9797
http://www.amenaza.com

Amenaza TECHNOLOGIES LIMITED

is designed specifically for analysing the threats posed by intelligent, malicious adversaries.[2]

Amenaza believes that, at a business level, corporate management needs three things from risk assessment:

1. Defensible mitigation decisions.
2. Effective security solutions.
3. Cost-effective security solutions.

These are described in greater detail below.

Defensible Mitigation Decisions

Conventional threat-risk-assessments (TRAs) involve a lot of discussion which is never captured or recorded. The reasoning process that was used to arrive at certain confusions is often lost when analysts leave the company or simply forget what they were thinking. Later, when an incident occurs, no one can say for sure what was considered or why certain decisions were made.

While no one can guarantee how a particular court case will turn out, it is generally accepted that a defense that presents solid information about

- which system vulnerabilities were considered,
- the types of threats that were examined,
- the projected impacts of the incidents that were discussed
- the reasoning that led to particular mitigation decisions

is more likely to succeed than one that does not.

Amenaza's Secur*I*Tree captures all of these assumptions in a graphical, mathematical model. This model can be re-examined at any time – whether or not the original analysts are available – thus providing a clear description of the efforts the organization took to ensure their systems were secure.

Effective Security Solutions

Conventional risk assessments often generate recommendations which, when implemented, do not work. Because Secur*I*Tree can model the effect of a proposed solution before it is purchased or implemented, management can have strong assurances that the desired result will be obtained.

Cost Effective Security Solutions

Without a proper risk assessment, it is impossible to tell whether or not it is better to accept the risk or if it should be mitigated. Many million dollar solutions end up protecting a few thousands of dollars of assets. Secur*I*Tree's attack scenario analysis allows the organization to

[2] Secur*I*Tree also supports probabilistic analysis for threats such as floods, hurricanes and equipment failures.

produce a cost (or impact) prioritized list of various attack scenarios. These costs are easily evaluated against the costs of proposed solutions.

Capabilities-based Attack Tree Analysis is the Gold Standard

Capabilities-based attack tree analysis is the preferred approach for analyzing hostile threats of all kinds against all types of assets. The tool and technique can handle situations ranging from the simple (such as the house burglary example shown in **Figure 1**) to extremely complex problems where millions of dollars of assets, data and even human lives are at stake.

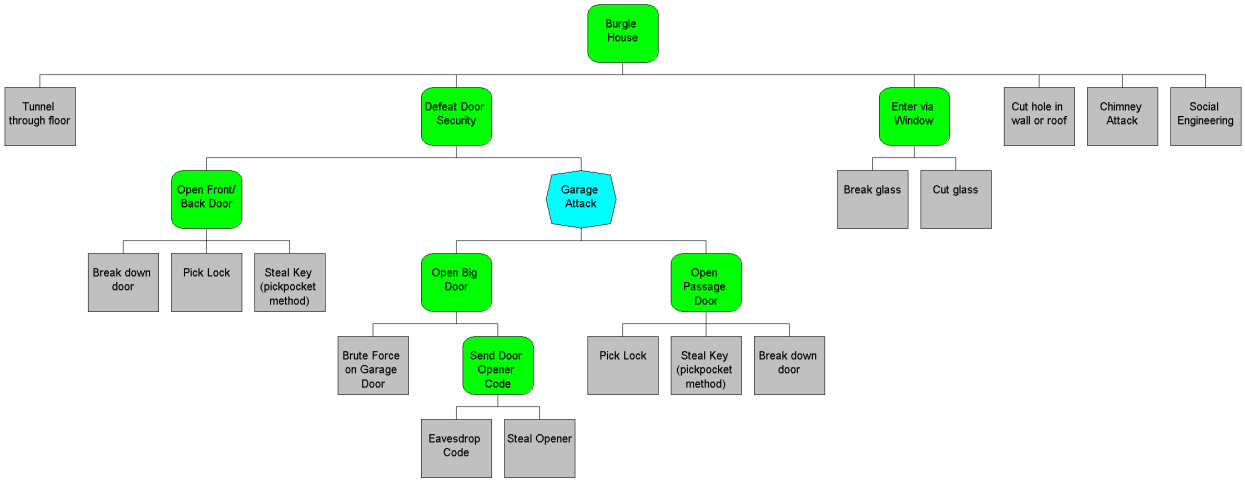

Figure 1 – Simple Attack Tree Describing Ways to Burgle a House

SecurITree® – Dare you risk IT?

Amenaza Technologies Limited has developed the world's most advanced Attack Tree based vulnerability assessment tool, SecurITree®. *When used with the accompanying methodology and attack tree libraries,* SecurITree *allows enterprises to discover which weaknesses are most likely to be used against them by attackers .* SecurITree *turns the tables on the attackers by enabling enterprises to quickly and efficiently invest in those security measures that result in the greatest reduction of risk.*

Learn more about Amenaza Technologies and SecurITree at http://www.amenaza.com

The information and product features described in this document are subject to change without notice. Any discussion of product features or enhancements must not be construed as a commitment by Amenaza Technologies Limited.