Predicting Adversarial Behavior with Secur*IT*ree

We live in a risky world! When you consider all the things that **might** happen, it is a miracle that any of us ever reach retirement. Considering all of life's hazards, it is astounding that we're even willing to get out of bed in the morning. If it weren't for the belief that accidents happen to "the other guy" we would probably just cocoon!

Not all risks are equal. According to the National Safety Council, the lifetime odds of drowning in a bathtub are only about 1 in 10,000. Most of us (fortunately) continue to take baths (with only our rubber ducky as a life preserver)! The same source informs us that it is more than a hundred times more likely we will die in an automobile accident than in the bathtub. Not surprisingly, more effort has gone into improving the safety of automobiles than bathtubs. Due to the well known risk of an automobile accident, auto manufacturers have spent millions of dollars finding ways to build more crashworthy cars. Almost everyone agrees that these efforts have been worthwhile. The automotive industry demonstrates that we've gotten pretty good at dealing with hazards for which probabilities are well known. The fact that statistics exist for a given peril means that we have a lot of experience with it. Our intuition is arguably as good a tool as any for these situations.

The pace of change in the world now presents threats that are quite outside of our experience. Unlike automobile accidents, these threats are far from random. Terrorists threaten our way of life by using common instruments against us. In a less dramatic, but no less hazardous fashion, tools such as the Internet and wireless technology can become weapons in the hands of our adversaries. Hackers, disgruntled employees, competitors, radical social groups and enemies of the state all have the means and motivation to actively disrupt our information technology (IT) services.

The IT industry has tools to scan networks and hosts looking for vulnerabilities. Unfortunately, these tools all too often produce an overwhelming volume of cryptic data. Various security organizations deluge us with advisories warning of all kinds of dangers. Correcting all of the deficiencies identified is beyond the capability (and budget) of even the most dedicated and knowledgeable security professional.

Since it is impossible for businesses to "cocoon" (short of ceasing operations) there are two choices.

- Ignore the vulnerabilities and hope it happens to "the other guy."
- Prioritize which vulnerabilities are most likely to affect your company.

The first strategy is tantamount to IT Russian Roulette. Sooner or later your luck will fail (and the odds aren't good). The second approach of prioritizing vulnerabilities requires an understanding of two things: how much damage a particular attack will inflict in a given situation and which vulnerabilities are most likely to be used by an organization's adversaries. Knowing how IT fits in a company means that it isn't too difficult to estimate the possible damages of a security incident. Until recently, however, anticipating adversarial behavior has been impossible.

Fortunately, recent developments in threat analysis now make it possible to predict the adversaries' behavior. This allows us to focus on thwarting our enemies by protecting the most likely points of attack.

In the late 1990s, the noted computer security expert, Bruce Schneier, described a method for modelling hostile activity. He called this approach *Attack Tree Analysis*[1]. Although the technique was clearly a step ahead in understanding threats, adoption of *Attack Tree Analysis* was stymied by the lack of detailed process instructions and the absence of an automated tool.

Attack (or Threat) Tree Analysis is based upon a graphical, hierarchical tree model. A "root" node is defined representing the ultimate goal of the attacker. In most cases several different approaches to achieving this goal are possible. These alternatives are represented by breaking the high level goal into more detailed sub-goals, each represented by an additional threat node[2]. As far as is possible, all plausible attacks are described without consideration of whether they are likely to occur.

Each threat node includes indicator values showing the resources required by the attacker to carry out the assault to that point. Many different types of resources can be specified, however the popular choices are:

- cost of the attack
- technical difficulty of carrying out the attack
- the likelihood of being caught using a particular attack

Indicators are chosen as being things that influence people's behavior.

Once an *attack tree* model (complete with the resource requirements needed to reach each threat node) has been built, the next step is to identify classes of people interested in attacking the modelled system. Amenaza calls these people, *threat agents.* The resources available to the *threat agents* are estimated. For each class of *threat agent*, the *threat agent's* capabilities are compared to the resources required to accomplish the various kinds of attacks. Attacks (nodes) beyond the capabilities of the *threat agent* are removed from the tree. Those nodes remaining are the attacks most likely to be carried out by that *threat agent.* **In this way, threat tree analysis predicts how various types of people will behave.**

[1] B. Schneier, Secrets and Lies: Digital Security in a Networked World, pp 318-333, 14 August 2000, John Wiley & Sons; ISBN 0471253111
B. Schneier, Attack Trees, Dr. Dobb's Journal, v. 24, n. 12, December 1999, pp. 21-29.
B. Schneier, Attack Trees: Modeling Actual Threats, SANS Network Security 99 – The Fifth Annual Conference on UNIX and NT Network Security, New Orleans, Louisiana.
B. Schneier, Seminar session at the November 1997 Computer Security Institute conference held in Washington DC.

These references do not imply endorsement of Amenaza's tools or processes by Mr. Schneier.

[2] Following the convention usually used with other types of tree models, the root is at the top and the tree grows downwards toward the leaf nodes.

In the past, security analysts attempted to understand threats using *threat vulnerability assessment* (TVA) methodologies based on checklists or spreadsheets. Conventional TVAs are manpower intensive, slow, tedious and error prone. Due to the significant effort involved, they are seldom completed. If carried out, ordinary TVAs suffer from serious shortcomings:

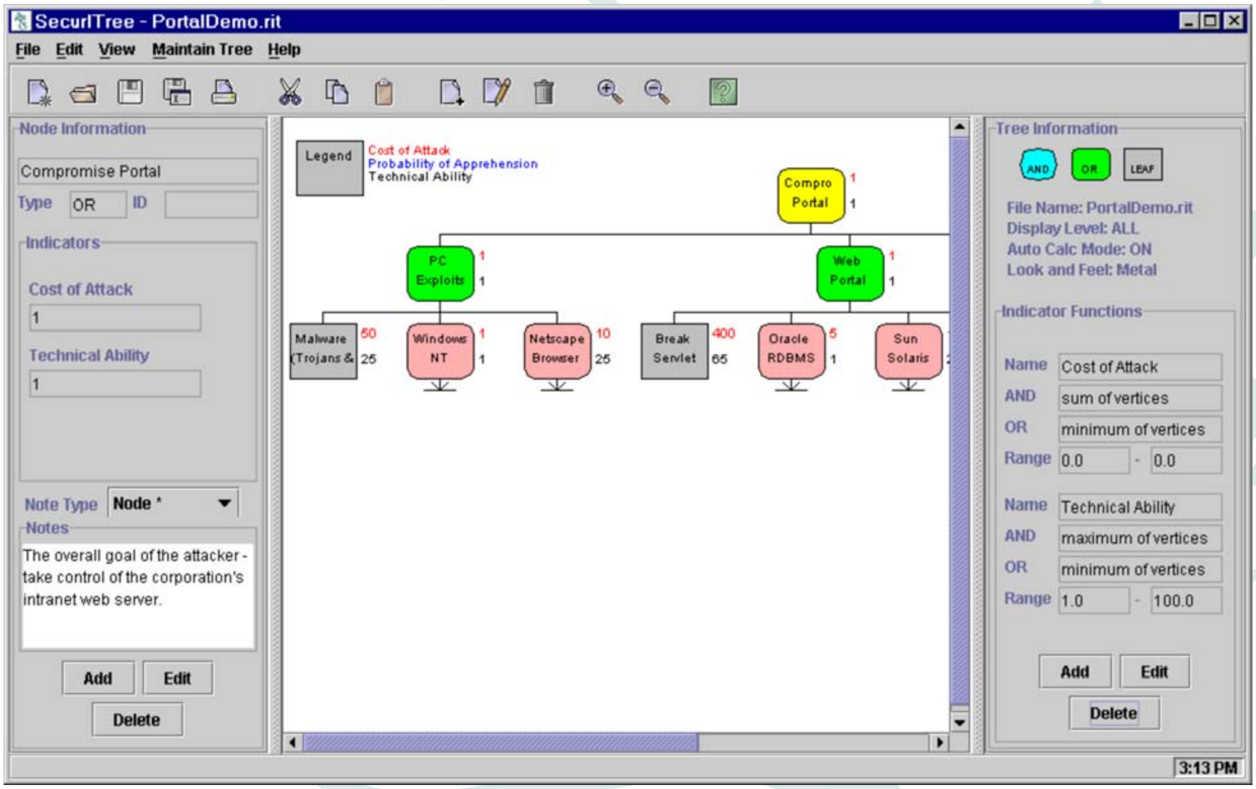
- "what-if" analysis is difficult to perform
- threat prioritization is not possible or extremely subjective
- the results represent a snapshot in time
- a true picture of the risk is not presented

Our adversaries today are constantly developing more sophisticated tools for probing and penetrating our defenses. Shouldn't our TVA tools and methodologies adapt as well?

After several years of research and development, **Amenaza Technologies Limited has broken the barriers to attack tree analysis with the introduction of a totally new software tool, Secur*I*Tree.** With Secur*I*Tree, a rapid prediction can now be made of

- who will attack a given system
- where they will attack
- how they will carry out the attack
- what resources the attacker must expend to compromise the system

By knowing your enemies' most probable avenues of attack, you can quickly and efficiently



Node Information

Compromise Portal

Type: OR ID:

Indicators

Cost of Attack: 1

Technical Ability: 1

Note Type: Node *

Notes: The overall goal of the attacker - take control of the corporation's intranet web server.

Tree Information

File Name: PortalDemo.rit
Display Level: ALL
Auto Calc Mode: ON
Look and Feel: Metal

Indicator Functions

Name: Cost of Attack
AND: sum of vertices
OR: minimum of vertices
Range: 0.0 - 0.0

Name: Technical Ability
AND: maximum of vertices
OR: minimum of vertices
Range: 1.0 - 100.0

invest your limited security budget in measures that result in the greatest reduction of risk!

Secur/Tree's intuitive, graphical risk representations are a quantum leap forward in their ability to communicate complex security issues to a broad range of stakeholders. Senior managers will appreciate the clarity of a Secur/Tree model. Technical gurus will welcome the tool's ability to model threats at any level of detail. **Secur/Tree models are the easiest and best way to explain risk to people regardless of job title or position.** Secur/Tree has the flexibility to model almost any type of hostile threat against any kind of system. The secret to the rapid and efficient modeling of the hostile threats is the Secur/Tree threat libraries. The threat libraries are easily customized for any IT environment or potential threat. Amenaza has developed numerous libraries containing predefined attack trees for popular technologies such as Netscape, Oracle, Solaris and Windows NT. Additional libraries will be added in the near future. These libraries are included with the Secur/Tree product. Regular updates are provided electronically to customers who have purchased technical support (a one year subscription is bundled with the initial purchase).

Secur/Tree can be used throughout all phases of system development. Attack tree models can even be constructed and analyzed before the equipment is ordered. **This allows security risks to be identified when they can be most economically corrected – at the design phase.** Conversely, deficiencies identified by vulnerability scanning tools you may already own can be used as a source of input for your Secur/Tree models. The Secur/Tree product enhances, rather than replaces, tools that already exist in your environment.

Secur/Tree is written in Java™ and runs on most popular computing platforms. It has been tested on all Windows™ operating systems from Windows 95™ onward. It has also been tested on Linux and FreeBSD.

Just as your adversaries use their knowledge about you to attack your systems, Secur/Tree allows you to understand your adversaries' capabilities and forecast where and how they will attack. Armed with this understanding, you can focus your efforts, your resources and your budget, on the most appropriate defenses.

Secur/Tree – Dare you risk IT?

Amenaza Technologies Limited has developed the world's most advanced Attack Tree based vulnerability assessment tool, Secur/Tree. *When used with the accompanying methodology and attack tree libraries,* Secur/Tree *allows enterprises to discover which weaknesses are most likely to be used against them by attackers .* Secur/Tree *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 Secur/Tree *at www.amenaza.com*