Amenaza SecurITree has a different view of risk analysis

Imagine that you are an attacker planning how to penetrate a major network. Put all of your information security skills into the exercise and plan how you would approach the project. This is a tiger team's thinking before it conducts a round of sophisticated penetration tests.

Consider the technical issues, social engineering and rogue employees that you might be able to compromise, as well as information that you might be able to gather on the internet that would help you. Now, draw an attack or threat tree taking all of these plans into account. Figure out what the cost of each step is to you as the attacker. Consider the cost to the victim if you are successful. Finally, examine the amount of effort and skill that each step of your plan would require. Now, after you have done all of that, analyze your results and determine the most likely path to success.

Although greatly simplified, this is exactly what SecurITree does. Although it may appear at first blush to be yet another way to model information security risk, in fact, it is discipline agnostic. If you can define the steps of an attack of any kind you can create an attack tree. And if you can create an attack tree you can predict the most likely — and risky — path of the attack. That helps you mitigate the risk with a higher level of certainty that you are going after those things that really matter, while giving less emphasis to those threats that are less likely.

Quantifying risks

From the perspective of the information security pro, this allows us to mix elements of risk that we accept but rarely quantify. For example, while we consider the results of penetration tests as contributing to risk, we rarely factor in physical security threats and vulnerabilities, even though we know they exist. SecurITree allows you to include and quantify all the elements that would lead to a successful attack. The result is a clear picture of risks in general, and the most likely risks in particular.

Like all sophisticated tools that solve difficult problems, SecurITree is not trivial to use. Conceptually, the product is straightforward. However, its real power is in its ability to allow the user to characterize each step of the attack quantitatively. The problem is not the tool. Rather, it is understanding what you are doing with the tool that requires thought.

Getting the know-how

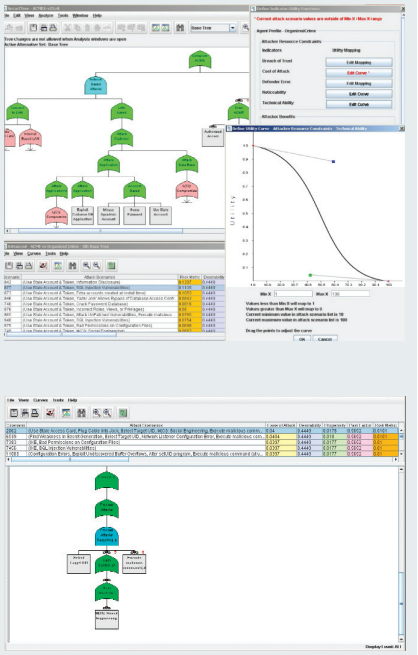
The application uses well-known "and" and "or" gate logic in setting up the attack/threat tree. Each gate represents a step in the attack process and each gate carries with it the characteristics assigned by the user. The user can build standard attack/threat steps that can be connected together in any tree. If there is not an appropriate step in the existing collection, the user simply creates the need gate and adds appropriate characteristics. They then insert the new gate into the tree at the desired location.

When the tree is complete, SecurITree calculates the weakest path to success and that path is the one that represents the greatest risk. That risk includes the combination of the low cost to the attacker, ease of performing the attack, and high cost to the victim of the successful attack.

We found SecurITree to be an excellent approach to understanding threats and vulnerabilities to an enterprise. While this is not the sort of tool that collects live data and makes calculations on the fly, it has the distinct advantage of allowing thoughtful analysis of the risk posture of a system at any time in the target's lifecycle. This is a significant benefit during the pre-implementation phases when there is no live system to test. It has the additional benefit of being able to analyze information that normally would not generate data for a risk or threat analysis tool. An example is the inclusion of physical security information, operator skill levels, costs involved with attacks, etc.

We liked this tool and look forward to seeing how it performs in the marketplace. It is powerful, flexible and it allows users to understand the threats against virtually any information system in the context of both qualitative and quantitative risk to that system. With the added benefit of not being limited to information systems risk, this is a formidable entry in the overall risk analysis category. — *Peter Stephenson*

AT A GLANCE



Product: SecurITree

Company: Amenaza Technologies Limited
Calgary, AB Canada
www.amenaza.com

Availability: Now

Price: $7,000 plus $3,000 for libraries — includes one year of maintenance. Also available on GSA.

What it does: SecurITree models qualitative and quantitative risks to virtually any type of system using threat/attack trees as the analysis mechanism.

What we liked: We liked the power, flexibility, and completeness of solutions to risk problems. We also liked the ease of use of the tool and the simplicity of displaying and explaining the results of an analysis to a lay audience.

What we didn't like: There was simply nothing about the tool that we did not like. However, like any powerful tool, if you don't understand what you are using it for it is not of much use to you. While the attack tree metaphor is fairly well known, it and the application of logic gates may be a new paradigm for some users.

Verdict: SecurITree from Amenaza Technologies Limited is a first rate risk analysis/modeling tool. At the moment, it's in a class by itself.