Amenaza TECHNOLOGIES LIMITED

Hostile Risk Decisions and Capabilities-based Analysis

Amenaza Technologies' capabilities-based attack tree analysis provides an objective way to improve decision making on issues related to hostile risk.

Background

From the risk definition, we see that for a single incident

$$\text{risk} \equiv (\text{incident probability}) \times (\text{incident impact})$$

Conventional risk analysis processes use this formula to generate an *Annualized Loss Expectancy (ALE)*. Mitigation is deemed appropriate if the annual cost of mitigation is less than the ALE for a given risk.

For situations involving risks from malicious attackers, applying ALE to the decision process is not as easy as it seems. Calculation of the ALE requires that applicable statistics be available for the types of incidents being considered. Such statistics generally exist for only a very narrow set of hostile attacks. They often describe frequently occurring attacks of low to moderate impact (such as computer virus infestations). It can be argued that formal analysis is unnecessary in these cases since the victim survives the attack but suffers repeated, obvious pain. This makes it obvious that mitigation should be performed.

It is more difficult, but also more important, to understand the risks from hostile incidents that occur infrequently (and may never have occurred before) but which carry a moderate to high potential impact. Unfortunately, it is very difficult to gather meaningful statistics for these risks precisely because of the events' rarity. Where statistics have been compiled, they may be inapplicable if the systems being considered have changed since information was gathered, or if the characteristics of the system's adversaries have evolved. Information technology is a prime example of a situation where these conditions apply.

Elimination of Improbable Incidents

In order for a hostile incident to occur, two conditions must exist:

1. The adversary must possess the means or capabilities to carry out the attack. Capabilities include money, equipment, knowledge, resources and overall willingness to pay all of the costs (including penalties) incurred by the attacker in carrying out the attack.

2. The adversary believes the projected benefits of a successful attack represent the best return for the resources they will expend[1].

[1] This accounts for the situation when the attacker has a choice of several targets. They will choose the target that brings them the greatest reward, or best reward per unit of expended resources.

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

Capabilities-based Elimination

Of the two conditions mentioned above, the first (capabilities) is the easiest to analyze objectively. An expert familiar with the technology used in the system's defenses and its vulnerabilities constructs an attack tree representing the various ways[2] in which attacks can occur. An attack tree is a graphical diagram consisting of a collection of nodes (boxes) with the overall attacker goal represented by the top or *root* node. The *root* goal is then decomposed into the various ways it can be accomplished. The substeps are represented by additional nodes in the tree. This successive decomposition process continues until the attacker's actions are described by finely detailed *leaf* nodes. Associated with the leaf nodes are estimates, based on expert opinion, of specific resources that will be required by the attacker to carry out the operation. While there is some uncertainty on the costs of a particular activity, most experts will agree on the order of magnitude of the estimate. This is sufficient for useful analysis.

Each possible attack is represented in an attack tree model by a path from one or more leaf nodes to the tree's root. Amenaza's SecurITree® modeling software quickly computes the set of all possible paths or *attack scenarios* and the resource costs that must be paid by the attacker for each kind of attack. Attack scenarios also reflect the impact on the victim.

Next, the analyst identifies the types of adversaries that plausibly threaten the system. Again, using expert opinion, estimates are made of the resources that will be possessed by a given class of enemies. For example, juvenile delinquents (typically adolescent males) are unlikely to have more than $50 at their disposal for an attack. Industrial spies, on the other hand, can be expected to have tens of thousands of dollars available. Terrorists are willing to pay the price of their lives for attacks; dishonest employees much less so. The exact numbers are debatable, but consensus is usually easy to achieve as to the correct order of magnitude.

SecurITree® compares the resources available to each type of adversary with those required to accomplish each attack scenario. All attack scenarios requiring more resources than those available to the adversary are classified as improbable and eliminated from consideration. The remaining scenarios are probable if the adversary finds the benefits of the attack sufficiently rewarding[3]. If the adversaries under consideration were chosen as having a plausible interest in harming the system then the remaining scenarios have a significant probability of occurrence. Although we do not have a precise probability value, the likelihood is sufficiently high that the projected impact of each attack should be evaluated for mitigation.

---

[2] Although there may be an infinite number of variations of how attacks can occur the number of classes of attacks against a given asset are usually much more restricted. Within an attack class the resources required from the attacker are usually similar.

[3] Although attack benefits may be financial, many adversaries have other interests such as creating bad publicity, harming a victim, creating terror.

Amenaza TECHNOLOGIES LIMITED

Attacker Motivation

The second condition which affects the probability of an incident is the attacker's level of motivation to perform the attack. An attacker's motivation to carry out an attack is related to:

1. The reward they will obtain from the attack.
2. The resources they will expend to carry out the attack.

Attacks only happen because the adversary believes they will receive some benefit through the attack. The higher the net reward the higher the degree of motivation. As discussed earlier, if the attacker's resources are insufficient, they will be incapable of mounting a particular attack. However, even if an attacker has sufficient resources to carry out an attack they may choose not to if they feel the return on their investment is inequitable. Attackers may be interested in absolute profit or in return on investment.

The positive benefits experienced by an attacker are easily incorporated into SecurITree models. SecurITree uses these benefits coupled with the attack scenario resource expenditures described previously to model attacker motivation.

Analysis at this level is tricky. It requires a high level of understanding of your adversaries' thought processes. Some adversaries are easier to understand than others. For example, bank robbers want money. Other attackers may have very complex objectives. It becomes necessary to understand the relative value an adversary may place on their resources. For example, would a terrorist group rather do an attack that is inexpensive, but costs a large number of attacker lives or would they prefer an expensive attack with no attacker casualties. It is not clear that these issues can be understood completely – particularly if the attacker is from a different culture or society than the analyst. This type of analysis is undertaken by national intelligence agencies, but they have an exceptional understanding of their adversaries.

Conclusion

Amenaza's capabilities-based attack tree analysis can be used effectively to identify high risk vulnerabilities in systems. Elimination of improbable attacks through a comparison of the adversaries' capabilities and the system's vulnerabilities is the primary analysis mechanism. Further analysis involving the attackers' motivation is possible, but requires a higher understanding of the adversary than is available to most analysts.

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