Creating Secure Systems through Attack Tree Modeling

Abstract: This document provides an overview of a highly advanced approach to evaluating and managing risk – capabilities-based attack trees.

Attack trees take their name from the fact that the methodology creates a graphical, tree structured model to describe the ways in which a system may be compromised or damaged. The technique is especially effective in assessing and managing the risks from hostile, intelligent adversaries. It is useful for analyzing threats against assets ranging from information systems to physical infrastructure.

Attack trees offer a scientific approach to a complex problem – predicting human behavior. By using capabilities-based attack tree analysis an organization can understand the ways in which they will be attacked, determine the likelihood and impact (damage) of these attacks and decide what action to take where the risks are unacceptable.

Attack tree modeling provides for effective security solutions, cost effective security solutions and defensible risk mitigation decisions.

Amenaza
TECHNOLOGIES LIMITED

Creating Secure Systems through Attack Tree Modeling

Building Complex Systems the "Hard Way"

People have been building complex systems for thousands of years. Until fairly recently, it was pretty much a trial and error process. Understanding all of the factors that might affect a real world system is sometimes very difficult. Success can be spectacular – as can failure!

This is not to say that great things were not accomplished through trial and error. The Great Pyramid of Cheops, the most massive secure structure ever built[1], was the culmination of a trial and error process. Archaeologists have found earlier, incomplete pyramids that were abandoned midway through construction when they collapsed. It apparently took several attempts to get the design right but it was not anything that could easily have been anticipated. Even the great Egyptian architectural genius, Imhotep, lacked the mathematics and computational tools to understand the limitations of construction materials and the stresses caused by a given design. Only by learning from previous failures was Imhotep able to build the Great Pyramid.

Estimates vary, but the nearly 6 million tons of stone used in its construction are thought to have taken almost 20 years to assemble! Between 20,000 and 100,000 workers were involved in the project. Sadly, the monumental engineering achievements of the Egyptian engineers were insufficient to protect the pyramid's contents from treasure hunters. Despite the mammoth construction effort, the contents of the Great Pyramid of Cheops were plundered. Fortunately for Imhotep, his employer was already dead when this happened or he might have asked for a refund!

A more recent example of the drawbacks of trial and error engineering is found in the ill-fated voyage of the RMS Titanic. The Titanic was a marvelous ship that incorporated numerous advanced safety features. Yet, the Titanic sunk with a tremendous loss of life. A century of analysis has identified a number of relatively minor design errors.

For example, the Titanic's rudder was small for a ship of its size. This prevented it from turning in time to miss the iceberg. The steel used was brittle and produced long cracks on impact. Gaps in watertight compartments allowed flooding to spread. These, and other problems, could have been easily resolved if the designers had been able to anticipate how their ship would perform in an abnormal situation.

Improving Designs through Modeling

Many of the Titanic's safety features are still used in today's ocean liners. What assurance do

[1] Some argue that the Hoover Dam, weighing in at 6,600,000 tons is a larger structure. However, unlike the Great Pyramid, the dam was not designed specifically to provide secure storage. So, we maintain that the Great Pyramid is the most massive security system ever created.

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

we have that they are any safer than the Titanic? The answer, according to some experts[2] lies in the use of computer models to simulate a ship's behavior under stress. A computer simulation allows shipbuilders to see how a design will perform under a variety of conditions before actually constructing the ship. Defects can be identified and corrected in a safe and cost effective fashion.

Naval architects are not the only ones to use models to verify the correctness of their designs. Buildings and bridges are almost always designed using Computer Aided Design/Computer Aided Modeling (CAD/CAM) and Finite Element Analysis (FEA). Aircraft designers use wind tunnels in conjunction with computer tools to produce efficient designs. Pharmaceutical companies use computer-based molecular modeling tools to create new wonder drugs. The very computer processors used to drive these simulations are themselves the product of computer modeling tools.

21st Century Threats versus 19th Century Defenses

Models are used to analyze and create all kinds of things. Except security systems. Security systems are largely constructed based on "expert opinion." Not only are experts scarce, but as was shown in the examples above, even experts may find it overwhelming to manage the details of a complex system in their heads. So, why are analytic tools and techniques not used to design secure systems?

Part of the reason is that there is great confusion over what is meant by *secure*. Without a precisely defined goal it is impossible to apply sophisticated analytic tools. So, security designers fall back on techniques such as:

- *Whack-a-mole* – a game frequently played at carnivals wherein the player attempts to hit a mechanical mole as it pops out of numerous mole holes. Unfortunately, the mole usually disappears just as the player swings and pops up somewhere else. In the information security field, system administrators play a variant of this game, known as *patch-a-hole*.
- *The Barn Door Approach* – the barn door is carefully secured and bolted after the horse has been stolen. Frequently used by corporations to justify after-the-fact security expenditures or to meet a condition imposed by the courts during litigation.
- *Blow the Budget* – security tools and services are purchased until the money runs out.
- *Best Practices* – this noble sounding term refers to the idea of building everything to the highest possible specification. Since no real project ever has the time or funding required to do this, when a security violation occurs it allows the security architect to declare with righteous indignation that the breach occurred because they "were not allowed to do the project properly."

---

[2] The PBS television network's Nova special on the Titanic stated that, "Today, materials engineers use computers to model the stresses on ship hulls and formulate steel able to withstand those stresses." For further information please see http://www.pbs.org/wgbh/nova/titanic/unsinkable.html

Amenaza
TECHNOLOGIES LIMITED

Risk Theory

Amenaza Technologies believes that what most people want when they ask for a "secure" system is one in which the level of risk is acceptable. To understand what is meant by this it is first necessary to understand the meaning of risk.

Risk (of a particular event) ≡ Event Probability × Resulting Damage

This formula is used, with slight variations, in many fields. It is often expressed as an Annualized Loss Expectancy (ALE) in $/year. In theory, it should be easy to determine the risk of a particular type of event. All that is needed is to find out how likely it is that the event will occur and how much damage it will cause. While it is usually straightforward to estimate the impact of an incident, coming up with a figure for *Event Probability* is more difficult.

The Problem with Probability

The probability of simple situations (such as tossing a coin or rolling dice) can be derived from mathematical principles. Unfortunately, real world situations are seldom this simple so this approach is of little practical value.

The probability of recurring events in a relatively static system can often be found from statistics. For example, historical records can be used to predict the frequency of floods, hurricanes and earthquakes. **Unfortunately, statistics do not work well for hostile attacks carried out by an intelligent, malicious adversary.** There may be no precedents which could be used to gather statistics or an insufficient number of samples may make the statistics unreliable. In some cases the dynamic nature of the environment makes previous cases irrelevant. For example, what was the probability that two airliners would strike the World Trade Center on September 11th, 2001? There were no precedents. What is the probability today? Airline security has changed considerably. Can conclusions be drawn from a single event? Or worse yet, when there are no precedents whatsoever?

This is the Achilles Heel of conventional risk assessment techniques. **They fail because of an inability to estimate the probability of hostile activities.**

Reality and the Law of Averages

Conventional risk assessment techniques also fail to recognize that, notwithstanding the mathematics of the risk equation, high probability/low impact events are not equivalent to low probability/high impact events. This lesson was learned some time ago by the former rulers of this planet, the dinosaurs.

Every year the earth receives thousands of collisions with meteoroids. The vast majority of these objects range in size from microscopic to a few metres in size. Overall, it is estimated that about 10,000 tonnes of debris falls to earth each year. Almost all of it burns up as it enters the atmosphere leaving only microscopic dust particles to reach the earth's surface.

About 65 million years ago a very large object is thought to have collided with the earth. Some estimates suggest the object was about 1.5×10^{12} tonnes! When averaged over the eons, the amount of material that fell per year from the colossus is not much different from the yearly

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

fallout from collisions today. However, the mega-meteorite wiped out the dinosaurs and formed the Caribbean Sea. Current meteors provide only an entertaining sky show.

There is another misconception that it is desirable to minimize risk. Risk minimization is easy to achieve. Simply turn off the lights, fire all the employees and bolt the doors. Risk (as well as productivity and profit) are negligible. What people really want is **optimized risk.**

Optimized risk occurs at the point where there is a balance between security and opportunity. When this balance is achieved productivity and profit will be maximized **over the long haul**. This is true even if occasional, minor security incidents do occur.

Risk Modeling Requirements

Amenaza Technologies believes that designing effective, defensible security solutions is best accomplished through the use of modeling. Modeling frequently requires the support of specialized tools. Effective modeling techniques and tools promote a number of important characteristics.

Simplicity

The whole point of a model is to present information in such a way that complex material becomes understandable. It has been said that a picture is worth a thousand words. We would suggest that a good model is worth a thousand pictures. Modern science centers are based on this premise. The Smithsonian Air and Space museum in Washington, D.C. has a section where people get hands on experiences with aerodynamic models. This is far more instructive than a gallery of pictures of airfoils.

Even an expert's brain is limited in the number of different factors it can grasp at one time. By creating a security model an analyst is forced to organize information in a systematic, understandable way. When it comes time to explain the information to others (who are frequently less well versed in the subject) the model must be an effective way of convincing them of the soundness of the analyst's conclusions. This can be crucial since non-experts are usually the people who approve or reject the recommendations of a risk analysis study.

Relevance

A security model should organize and interpret information such as to make it relevant to solving real world problems. This means that it must help an analyst identify solutions which represent the best balance of opportunities, controls and costs. The model must highlight solutions that are optimal over the long run and eliminate the dinosaur killers that can destroy an organization in a single event.

The model should help analysts construct solutions which have an architecture that is resilient to

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

isolated component failures[3]. Where deficiencies exist in a proposed design the model should make obvious which solutions are the most cost effective.

Know Thine Enemy

Military strategists have long advocated the need to understand one's enemy. The model must take into account the characteristics of the adversary.

Risk Prioritization Based on Attack Prediction

Most security solutions are reactive in nature. They respond to activities carried out by the adversary. A more useful security model will predict how, where and by whom an attack will occur. By factoring the effect of the attack on the defender into the analysis it is possible to correctly prioritize proactive defensive measures. This allows all of an organization's resources to be directed to the problems that matter, instead of diluting risk mitigation efforts by squandering funds on unnecessary defenses.

Self Documenting, Defensible Results

No model will ever be a perfect representation of reality. This is particularly true when analysis deals with human behavior. Sometimes a security incident occurs even when all of the recommendations of a risk assessment have been followed. When this happens it may become necessary to defend the analysis. In the extreme, this could take place in a court of law where millions of dollars are at stake in a "due diligence" lawsuit.

Although no one can make any guarantee how the courts will decide a hypothetical lawsuit, it is generally agreed that the chances that the defenders' actions will be found to have been reasonable are greatly enhanced if they are able to document

- The vulnerabilities and threats that were considered in the analysis.
- The assumptions made in the analysis.
- The reasoning that was used to discount certain attacks as low risk.

Attempting to explain these issues using reams of notes and foggy memories is unlikely to be persuasive to a jury! The model should intrinsically record and document these issues. It should be possible for an independent group of analysts to examine the work that was done and understand the process used to arrive at conclusions.

A Five Step, Capabilities-based Attack Tree Method of Risk Assessment

Amenaza believes these requirements can be met through a simple five step process:

1. Create an attack tree model showing possible ways to attack the system.

---

[3] Metal bridges incorporate thousands of fasteners and welds. Although every effort is made to ensure that the construction is of the highest standard, the reality is that not every weld and fastener is perfect. Nonetheless, bridges do not fall down. The reason for this is that the engineers use designs that tolerate a certain amount of imperfection. Security systems should behave similarly.

Amenaza TECHNOLOGIES LIMITED

2. Predict how adversaries will attack using *Capability-based Analysis*.

3. Identify the impact associated with each *attack scenario.* An attack scenario is the set of events that characterize a particular attack.

4. Determine the level of risk associated with each *attack scenario*.

5. Monitor the system for signs that an attack scenario is in progress.

Each step will now be explained in greater detail.

Step One – Create an Attack Tree Model

An attack tree model is a graphical representation of the various ways in which a system can be attacked. Nodes (depicted as boxes of various shapes) in an attack tree represent goals or states that an attacker wishes to achieve. At the top of the tree is a *root* node that represents the overall (malicious) goal of the attacker. The goal will vary depending on the type of system being analyzed and may be broad or narrow depending on the attacker's purpose. Examples of root goals include: Steal data from computer system; Contaminate water supply; Conquer Europe.

The attacker's overall (root node) goal is then decomposed into increasingly detailed subtasks. The basic premise of an attack tree model is that insight can be achieved by decomposing the high level parent goals into the smaller subtasks needed to achieve them.

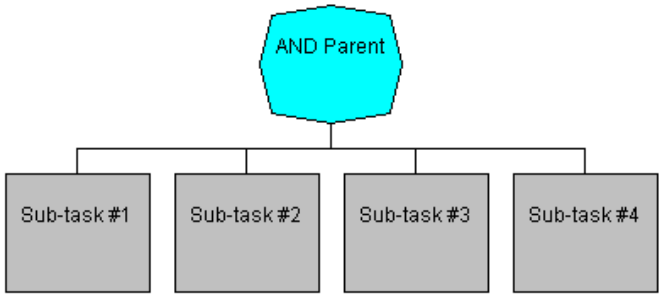

Figure 1

Nodes below a particular node represent subtasks and are referred to as *children.* Conversely the nodes above a given node are referred to as *parents.* Nodes two levels above are called *grandparents* and so on. In **Figure 1** the grey, rectangular boxes (labeled as subtasks #1-#4) are children of the cyan colored, eight-sided polygon node. The eight sided polygon is the parent of the subtask nodes.

If all of the child subtasks beneath a parent must be achieved in order to realize the goal, then the parent is called an *AND* node. The diagrams used in this paper depict *AND* nodes as eight-sided, cyan polygons (e.g., **Figure 1**).

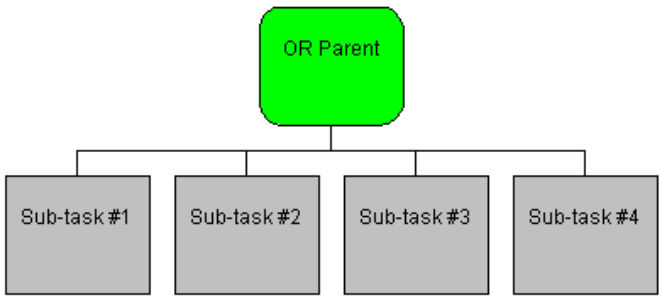

Figure 2

In other cases, successfully performing any one (or more) of the subtasks will cause the parent goal (known as an *OR* node) to be achieved. *OR* nodes are shown in diagrams as rounded, green rectangles (e.g., **Figure 2**).

The decomposition of tasks and goals into smaller components can continue to any desired level (each goal being represented

by a separate node). At some point, however, the analyst decides that the level of detail in a node is sufficient. These nodes are considered to be *atomic*[4]. That is, the description of the task is precise enough for someone skilled in the art to perform the activity. These atomic nodes are known as *leaf* nodes and are represented as square cornered, grey rectangles. Leaf nodes represent the actual actions performed by an attacker. **Figure 3** illustrates, in a perhaps oversimplified fashion, the ways in which a residence (with an attached garage) could be burglarized[5].

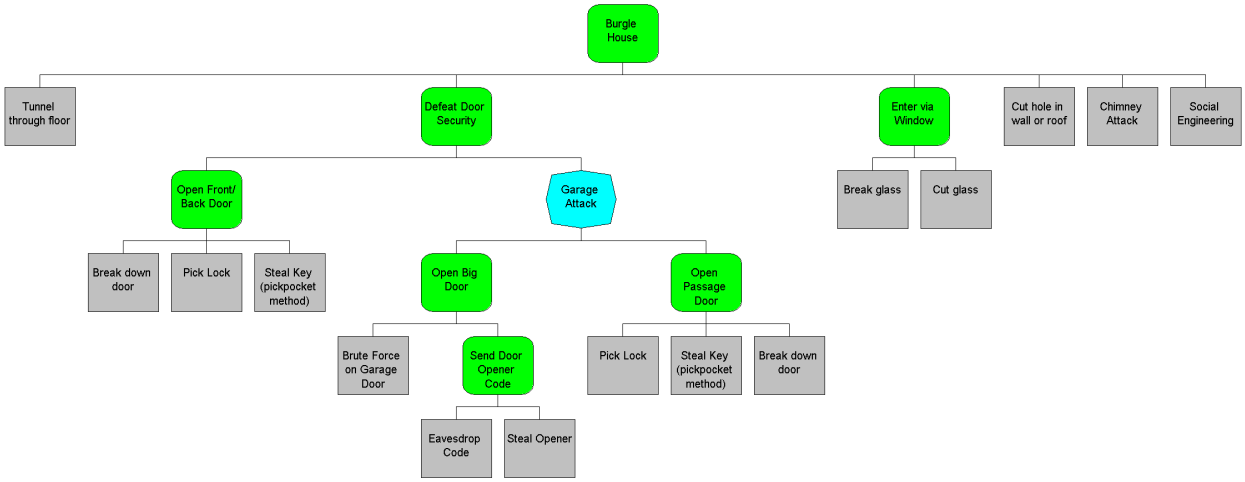

Figure 3 – Simple Attack Tree Describing Ways to Burgle a House

Step Two – Identify Probable Attacks using Capability Analysis

As was discussed earlier, the use of statistics to determine the probability of hostile activities is ineffective. Estimates based on first principles are only practical for extremely simple situations, such as rolling dice or flipping a coin. *Capabilities-based analysis* overcomes the limitations of these techniques.

Capabilities-based analysis is based on a simple premise

***IF* they want to *AND* they can *THEN* they will**

In other words, if someone has the motivation to commit a hostile act and they have all the

[4] We said that capabilities-based analysis was powerful! However, in this context the term *atomic* refers to the original Greek meaning of the word *atomos* (indivisible). *Atomic* simply means that the goal cannot be subdivided.

[5] An attack tree model of a house burglary is probably overkill. However, our purpose here is simply to provide an illustrative simple example that most people can relate to.

necessary capabilities (money, skill, willingness to accept the consequences, etc.) then they may reasonably be expected to attack. This holds for all kinds of attackers – vandals, hackers, state-sponsored terrorists, criminals, employees, industrial spies, lunatics and fanatics.

Motivation

Many factors determine whether or not people will behave in a certain way. We can make some predictions about groups of rational people. Unfortunately, whether or not someone is perceived as rational is partly determined by cultural biases. Prior to 11 September 2001 many people discounted the possibility of kamikaze style airplane attacks because it would require the attacker to give up their life. We now know that this assumption was incorrect.

Any type of person that would benefit from a successful attack should be considered a potential *threat agent.* Fortunately, intuition is a pretty good guide as to who are our enemies. In case of doubt, the most prudent course of action is to assume a somewhat conservative, defensive posture. Therefore, for purposes of analysis we should presume that any group whose intentions are uncertain, to be hostile.

Capability

It takes more than just motivation to carry out a successful attack. The attacker has to possess a variety of resources in order to perform the attack. These resources include money, time, technical ability and a tolerance for the consequences that may result from the attack. Amazingly, highly diverse types of people are constrained by similar resources.

Of course, the level of resources required varies dramatically depending on the weaknesses present in a particular system. Assaulting an 85 year old senior citizen is likely to be much easier than attacking a 30 year old karate instructor. Whether or not an attack will take place is therefore determined by a combination of the strength of the threat and the size of the vulnerability. The risk equation, which we have written as

Risk (of a particular event) ≡ Event Probability × Resulting Damage

is often rewritten as

Risk ≡ Threat × Vulnerability × Resulting Damage

In other words,

Event Probability = Threat × Vulnerability

Conventional analytic techniques require that the *threat* variable be a value representing the frequency with which adversaries attack. Once again, this seems to require non-existent statistics to calculate, so the formula is of little practical value. A different approach is required.

Capabilities-based Tree Pruning

Although it is not possible to determine a precise mathematical value for event probability, it is possible to get a good estimate from an attack tree. When the analyst creates a particular attack tree, they associate with each leaf node the approximate level of resources required to carry out

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

that specific attack. Depending on the nature of the resource, it is possible to define formulae that will calculate the resources needed to reach any point in the tree. For example, **Figure 1** shows an *AND* parent node with four child leaf nodes representing a number of subtasks, all of which must be accomplished in order to reach the parent's state. If subtasks 1 through 4 cost $10, $20, $50 and $5 respectively then it would cost an attacker $10 + $20 + $50 + $5 to reach the *AND* node. Similar calculations can be done for other kinds of resources and for *OR* nodes. **The resource requirements at any node in the tree are a direct reflection of the size of the vulnerability at that point.**

The *threat* variable can be easily estimated by estimating the magnitude of resources available to each kind of threat agent under consideration. Continuing with the house burglary example given earlier, the following table might apply:

Threat Agent	Available Resources		
	Money	Technical Ability (1-100)	Tolerance of Apprehension
Juvenile Delinquent	$25	20	50%
Cat Burglar	$500	75	10%

The portion of the house burglary attack tree that deals with attacks against passage doors describes three ways of opening a door (shown in **Figure 4**):

1. Break down the door – this attack is very inexpensive. A $10 piece of scrap iron (such as an anvil) will break the door jam on most locks. It does not take much skill to wield this tool, but we have set the skill requirement at 20 (you have to be strong enough to lift the anvil). Finally, even if the attacker waits until there is no one in sight to swing his battering ram, the noise may still attract some attention. So the probability that such an attack will result in apprehension is set to 30%.

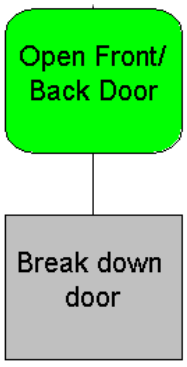

Figure 5 – Delinquent

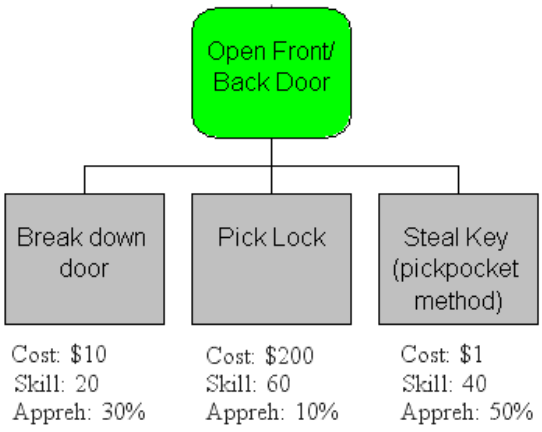

Figure 4 – Subtree with Attack Resources

2. Pick the lock – good burglary tools (dentist pick, file, specialized tools) are not free. High quality steel is expensive so the cost has been estimated at $200. The skill required to pick a good quality house lock is considerable, so the skill level is judged to be 60. This is a fairly stealthy attack and the chances of getting caught are minimal (10%).

3. Pickpocket key – there are really no costs involved in this attack. It does require a bit of finesse to pinch a key, so the skill is set to 40. Contrary to popular belief, pickpockets are frequently detected – they just run fast. So, the probability of apprehension is estimated at 50%.

Comparing the chart showing the adversaries' capabilities with the resources required to exploit the vulnerabilities we see that the only attack available to the juvenile delinquent is to break down the door. Our misunderstood adolescent has neither the money nor the skill to pick a lock. They can almost pickpocket the key but have not developed the necessary skill yet.[6] This is shown graphically in **Figure 5**.

The sophisticated cat burglar, on the other hand, is also constrained by his resources. Although he certainly has the skill and money to use the battering ram, he is unwilling to accept the odds of getting caught. The same holds true for the pickpocket approach. For the cat burglar this is a business and there is nothing like a stint in the slammer to ruin profitability. The only attack available is to pick the lock (**Figure 6**).

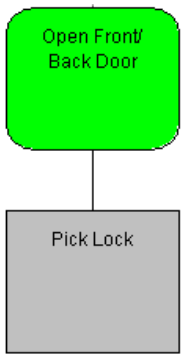

Figure 6 – Cat Burglar

In these somewhat simplistic examples, attacks beyond the capabilities of adversaries were *pruned* away from the original attack tree. **The attacks that remain are highly probable.**

Assumptions

Whether or not the results of the analysis are actually true depends entirely on the correctness of our assumptions. Specifically, assumptions were made as to:

- Which adversaries posed a threat.
- What resources were possessed by the adversaries.
- How much resources were required to carry out the various attacks.
- The set of possible attacks.

For this we make no apology. Any analysis technique that attempts to predict the future (particularly of human behavior) must intrinsically make assumptions. **Capabilities-based attack tree analysis automatically captures and records these assumptions in the model.**

It is essential that the assumptions be clearly recorded in case the analysis ever needs to be defended. Courts of law base their judgements on issues of due diligence by determining whether the assumptions that were made and the actions that were taken were reasonable. A major part of the battle is in proving what was considered and why certain threats were eliminated as inconsequential. Capabilities-based attack tree analysis facilitates this.

Confidence Estimates

Assumptions about resources and threats can be adjusted slightly to see what effect, if any, is

[6] Pickpocket skills will be learned after they serve time in one of the government's finest institutions!

observed in the results. This is known as *sensitivity analysis*. In some cases, small variances in resources and threats will produce no change in the list of possible attacks. In other situations, the possible attacks can change greatly.

Through sensitivity analysis it is easily determined which resource or resources are constraining a particular type of attacker. This provides an estimation of the confidence level of a prediction. "What-if" thought experiments are trivial.

Attack Trees are Dynamic in Nature

Most threat, vulnerability and risk assessment techniques are so cumbersome that they are essentially static. An evaluation is done at a single point in time. The results are never updated despite changes to the system being defended and evolutions in adversarial capabilities.

An attack tree model makes it easy to see what architectural changes will be most effective. System changes or mitigation strategies can be modeled for effectiveness before they are implemented. The attack tree is updated to reflect the proposed changes, then capability-based pruning is reapplied. No longer do companies need to fund complex and expensive security projects only to discover upon completion that risk has not been reduced. Attack tree-based solutions are gold standard, not gold plated.

Factors external to the system being evaluated can result in new adversaries becoming a threat, or old adversaries gaining different levels of resources. The results of these changes can be known in moments by re-pruning the attack tree model.

Step Three – Evaluate the Impact of Attack Scenarios

It is often the case that a given adversary can achieve the overall goal of the attack tree in various ways. In the house burglary example shown earlier, the juvenile delinquent could burglarize the house in three different ways (shown in **Figure 7**, **Figure 8** and **Figure 9**). Although each of these attacks would result in the house being broken into, the impact on the victim is slightly different in each case.

For example, if the intruder breaks a window (**Figure 7**), the cost of repairing the damage is approximately $150. If they break down the outside passage door (**Figure 8**), a replacement door and lock set will cost at least $400. The attack (**Figure 9**) that involves stealing the garage door opener (from an unattended vehicle) with a value of $50 and then destroying the passage door inside the garage ($400) will total to $450. This, in our oversimplified example, ignores the damage that may occur once the intruder enters the house.

A more realistic example would be causing an essential computer system to crash. This might be caused by someone pulling the plug on the computer or it could occur when someone uses a diesel fuel/fertilizer bomb to level the building which houses the computer. In the first case, the impact damage would be a short loss of service until the computer is rebooted. In the latter, it would involve the loss of a multimillion dollar building, quite possibly a number of lives and, of course, a significant computer outage.

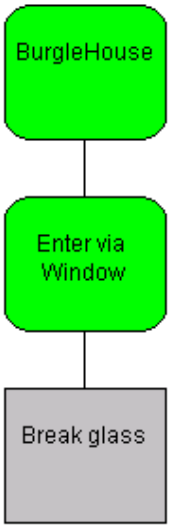

Figure 7 – Window Attack

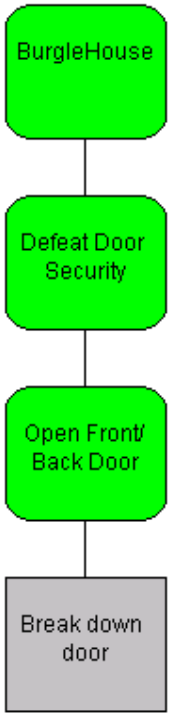

Figure 8 – Door Attack

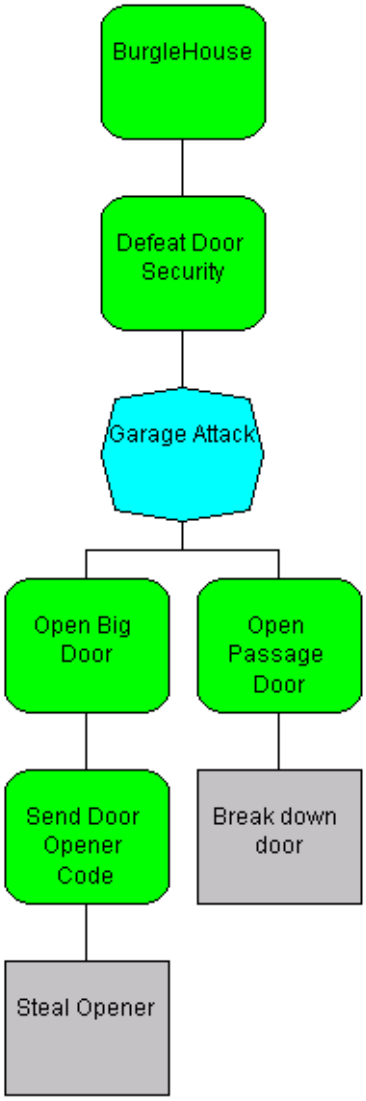

Figure 9 – Garage Door/Passage Door Combo

The scenarios for a simple house burglary can easily be generated by hand. A more complex attack tree might very well have hundreds or thousands of attack scenarios. At this point it becomes imperative to have an automated tool that can produce a scenario listing.

Unlike the resource requirements values, which are calculated from values entered by the analyst for leaf nodes, the impact values must be determined by examining the business and associating them with each attack scenario. In some cases an analyst may use a combination of directly entered values and values computed from formulas.

Step Four – Determine the Risk Level of Each Attack Scenario

As was discussed earlier, risk is a combination of the likelihood and impact of an event. Recall that an attack tree that has been pruned based on the capability of an adversary shows which attacks are reasonably probable. Therefore, **if the attack scenarios for a pruned tree are sorted based on impact, the result is (to a close approximation) a prioritized list of risks for a given adversary.** In other words, it is possible to read risk levels directly from an attack tree!

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

This is of great assistance in deciding where limited resources should be applied to mitigate risks and when the risk should be accepted. It can also be used to defend the choices an organization makes in due diligence situations.

Step Five – Attack Detection

Sometimes it is not practical to modify a system's architecture to make all attacks unattainable. In these cases, it may suffice to be able to quickly detect when an attack is in progress so as to take the appropriate response.

The leaf nodes in a given attack scenario describe the actions that must be performed by an attacker in order for the attack to succeed. By monitoring for these activities (perhaps with specialized sensors) it is possible to create a sophisticated intrusion detection system (IDS).

Most intrusion detection systems incorporate hard coded logic. Changes to a conventional IDS require programming changes. With an attack tree-based IDS, logic changes are made through modifications to the tree model. This means that the security analyst can update the IDS without, in most cases, the assistance of a programmer. Programmer assistance is only needed when new sensor inputs are required.

The Need for a Tool

While attack tree solutions can be created manually, an automated tool greatly increases the effectiveness of the approach. This is comparable to the traditional *spreadsheets* used in many aspects of business. Although, in principle, there is no reason why a spreadsheet cannot be calculated by hand, in practice almost everyone uses Microsoft's Excel® program.

Amenaza Technologies Secur*I*Tree® software is specifically designed to support the activities described above. Steps 1 through 4 of the attack tree analysis process are fully supported in the tool. Step 5 will be supported in a future product release. Secur*I*Tree® takes care of the modeling computations and allows the analyst to focus on the problem at hand.

Conclusion

Attack tree analysis is a leading edge solution to understanding the risks associated with hostile adversaries. Through attack prediction it is possible to focus protective efforts on the vulnerabilities in a system that are most critical. The self documenting nature of attack tree models makes it possible to mount a credible defense in due diligence situations. Attack tree models make it possible to detect attacks in progress.

In hostile situations, attack tree analysis is a significant step ahead of conventional, probabilistic analysis techniques. Attack trees bring a rigor to the problem that has not existed previously. In the words of Lord Kelvin, "when you can measure what you are speaking about, and express it in numbers, you know something about it; but when you cannot measure it, when you cannot express it in numbers, your knowledge is of a meager and unsatisfactory kind; it may be the beginning of knowledge, but you have scarcely, in your thoughts, advanced to the stage of science, whatever the matter may be."

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

References

Attack Modeling for Information Security and Survivability, Andrew Moore, Robert J. Ellison, Richard C. Linger, March 2001, Carnegie Mellon Technical Note CMU/SEI-2001-TN-001

Attack Trees: Modeling Security Threats, Bruce Schneier, Dr. Dobb's Journal, December 1999

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.

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