



A Quick Tour of Attack Tree Based Risk Analysis Using Secur//Tree

Introduction

Every day we are forced to make decisions whether to take certain risks. Can we cross the street safely? It depends whether it is a busy ten lane Interstate or a quiet residential street. Can we lessen the risk by looking both ways before we cross? In most situations our intuition tells us the correct course of action. Many situations in modern life are less familiar. The lack of facts, and sometimes the overabundance of facts, makes it difficult to make well-reasoned decisions.

Attack Tree Analysis is a modeling technique for understanding risk in complex situations. A graphical model is constructed showing all the ways to attack or damage a system. Then, the capabilities of various classes of attackers are compared with the resources required to perform each attack. Attacks requiring resources beyond the capabilities of the attackers are removed. **The remaining attacks are those that must be worried about.**

Until recently, the lack of automated tools made attack tree analysis impractical. **Amenaza Technologies proudly introduces Secur//Tree, the first graphical attack tree modeling tool in the world.** Secur//Tree is straightforward to use but has an amazing capacity to help you draw very complex conclusions using capability-based modeling. The results are presented in a graphical format readily understood by anyone.

Although Secur//Tree can model very complex situations, we will illustrate using a simple example – burglary.



The Situation:

You have a system that may be the target of a hostile attack. There are many vulnerabilities that could be exploited. You don't have the time or the resources to fix all of them.

The Good News:

Your attackers will only use a small subset of the vulnerabilities.

The Bad News:

You don't know which ones they will use.

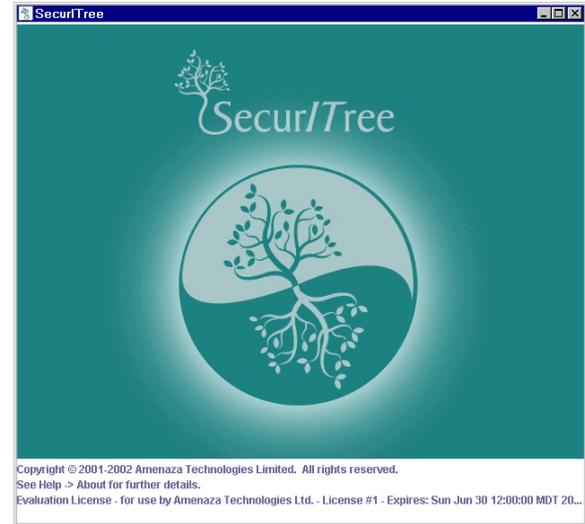
The Example:

Secur//Tree can model almost any kind of system. It is frequently used to analyze information (computer) systems. Secur//Tree has also been effective at understanding the protection of critical infrastructure such as buildings, pipelines and electrical transmission lines. To make this example meaningful to all audiences, we will study an example everyone can relate to – the different techniques that can be used to break into a typical, middle class residence – i.e., a house burglary.



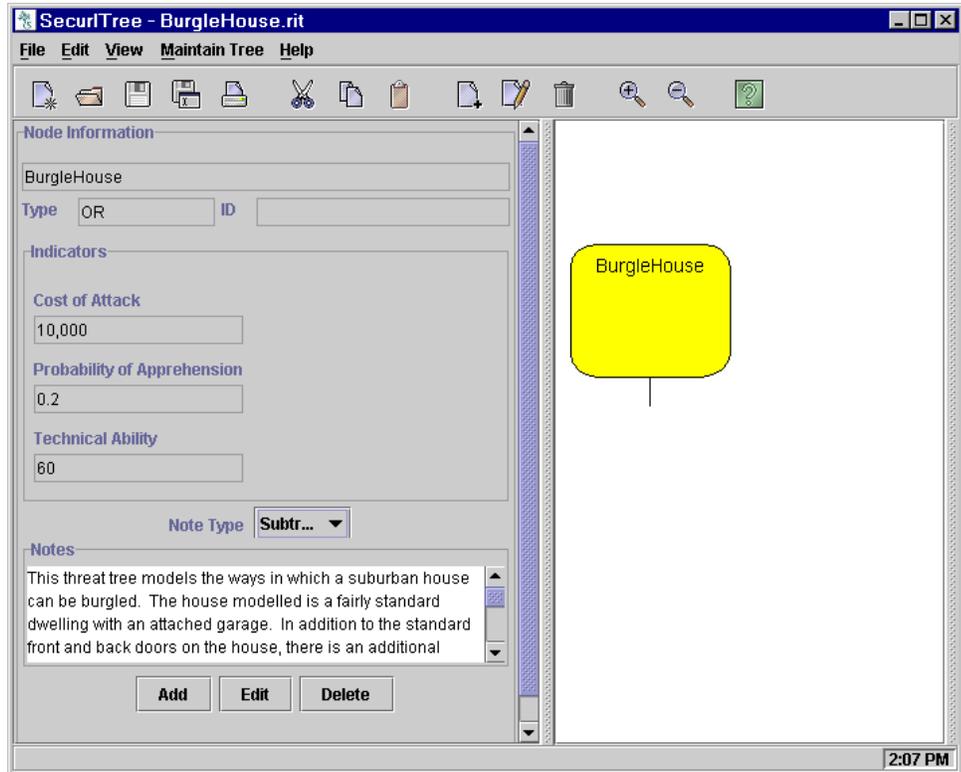
1. Secur/Tree

- a. This document consists of “screen shots” from an actual Secur/Tree session.
- b. If you would rather run Secur/Tree yourself, simply visit the Amenaza web site (www.amenaza.com) and request a free evaluation copy of the application. The accompanying tutorial loosely follows the demonstration shown in this document.
- c. Secur/Tree is a Java™ application. As such, it runs on all major computing platforms including Windows™ and Linux.





2. First, define the Attacker's Overall Goal.
 - a. In this case, the goal is to burglarize a house.
 - b. In other, more realistic analyses, it might be to steal information from a computer system or destroy a gas pipeline.

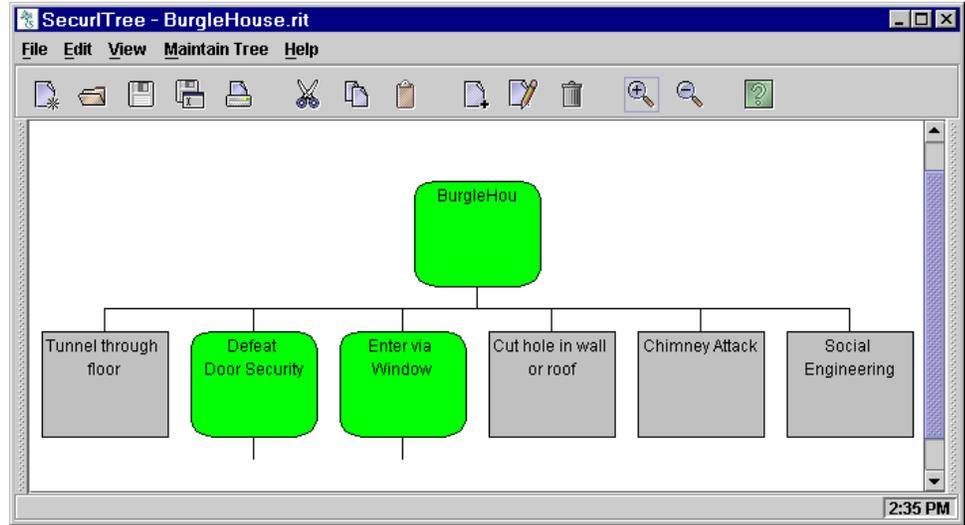




3. Decompose the overall goal into subgoals (represented by the boxes below the *BurgleHouse* box).

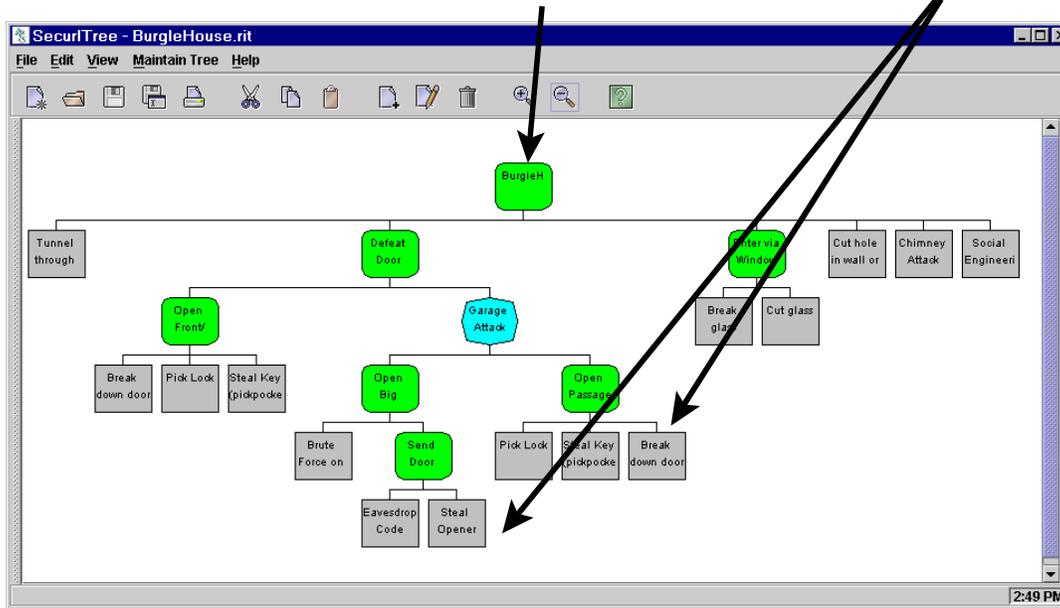
a. There are a variety of ways to achieve the high level goal.

- i. Tunnel through the floor.
- ii. Force open the door.
- iii. Enter via a window.
- iv. Cut a hole in the wall or roof.
- v. Come down the chimney (like Santa Claus).
- vi. Fool someone into authorizing access.





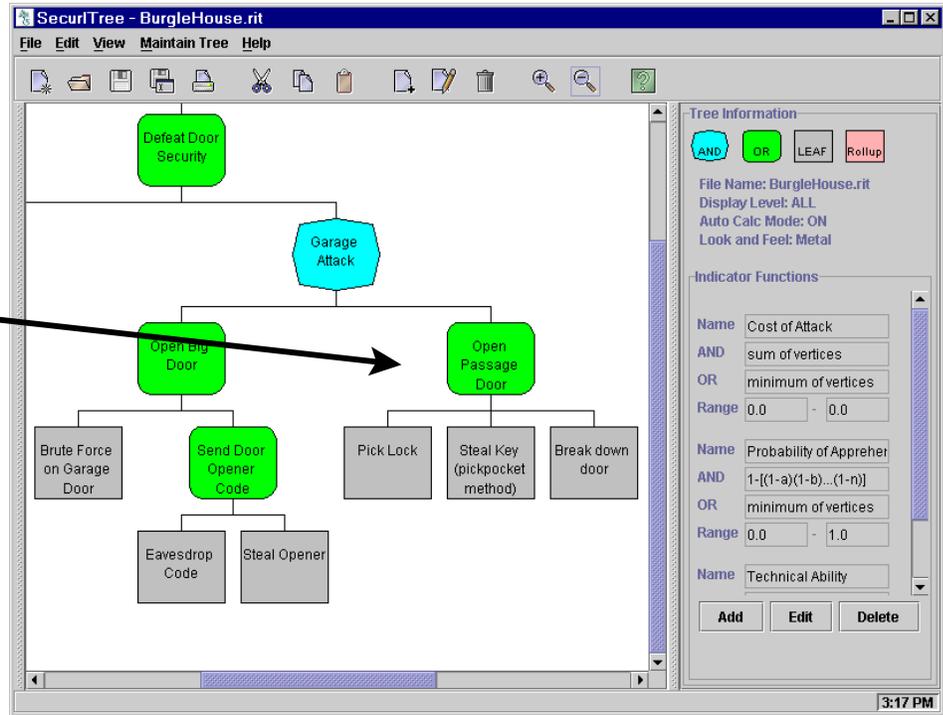
4. Continue the step-wise decomposition into smaller and smaller tasks.
 - a. The completed diagram of attacks and **sub-attacks** is called an *Attack Tree*.
 - b. The tree is upside-down; i.e., we call the top node the *root* and the bottom nodes the *leaves*.





5. Different classes of goals are represented by shapes.

- a. **OR** indicates that the goal or state can be achieved by performing any of the subgoals directly below it.
- b. For example, the goal *Open Passage Door* could be accomplished by
 - i. Picking the lock, OR
 - ii. Stealing the key, OR
 - iii. Breaking down the door.



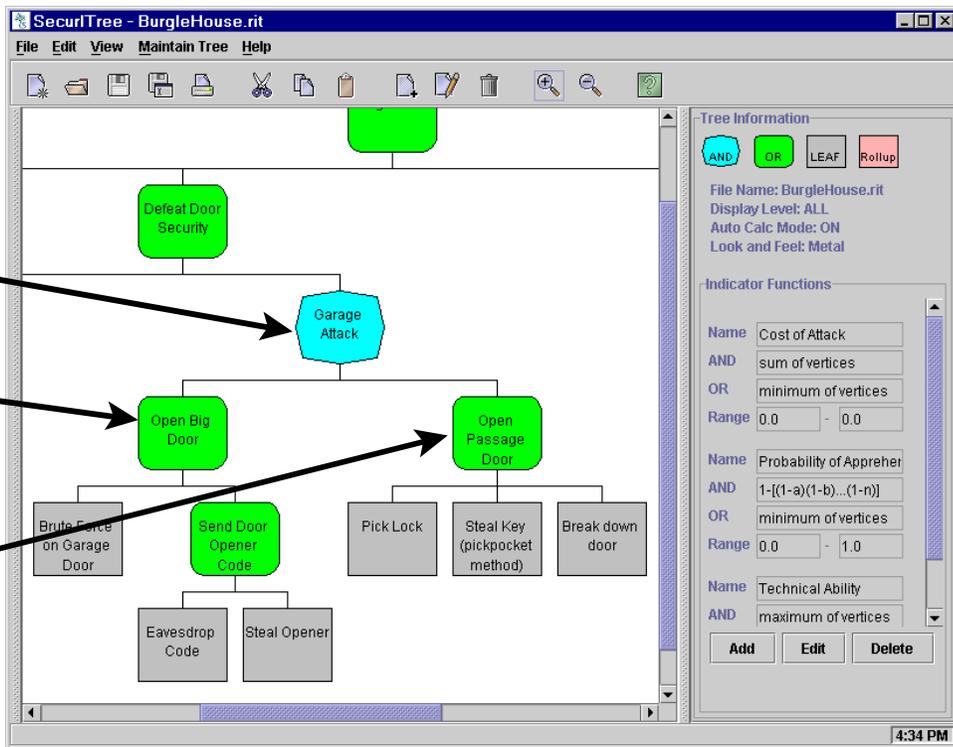


c. **AND** indicates that the goal or state can only be achieved by performing all of the subgoals directly below.

d. For example, the goal *Garage Attack* can only be achieved if someone

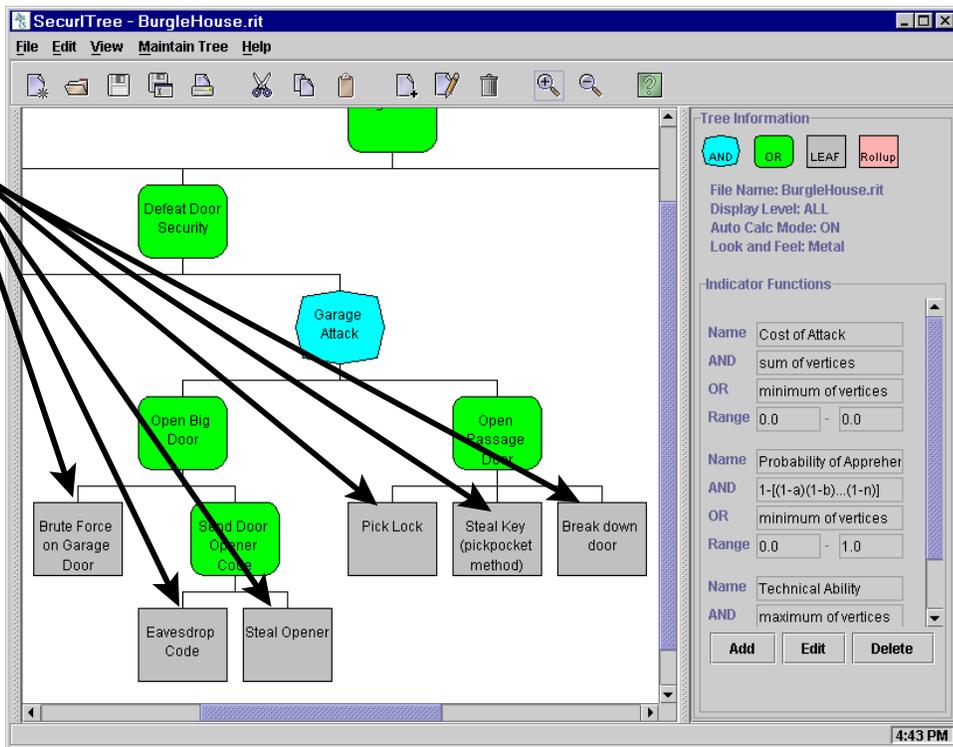
i. breaks into the garage through the large, car door, AND

ii. then continues on into the house through the small, passage door.





- e. **LEAF** goals are the most detailed descriptions of the activities required to carry out the attack.
- f. An attacker always begins an attack by performing the tasks described in one or more of the leaf goals.
- g. The symbols used to represent the OR, AND and LEAF goals are referred to as *nodes*.





6. Each node (goal) has associated with it additional information that can be displayed by double-clicking on it.
 - a. Textual notes explain what the node represents.

Edit Node

Title: Brute Force on Garage Door

Type: LEAF

Indicators

Cost of Attack	150
Probability of Apprehension	0.6
Technical Ability	25

Note Type: Node *

Notes

Unlike ordinary (person) doors, no puny little battering club is going to open a big, solid core garage door. Double width doors are also very heavy - at least 150 Kg (330 lb). It might be possible to lift the door using a hydraulic floor jack, but how do you get it under the lip of the door? You can drive a vehicle through the door, but that is *really* noticeable and tends to make a mess of the vehicle. After some thought, the most cost effective scheme is to take a circular saw, plug it into the ubiquitous outdoor receptacle and cut through the door.

Default Indicator Values and Rationale
Cost of Attack: \$150 - for this price you can get a really good circular saw, blade and extension cord.
Probability of Apprehension: 0.6 (or 60%) - your neighbors would have to really hate you to ignore such a blatant attack.
Technical Ability: 25 - It is a bit tricky to start a saw cut in the middle of a board.

OK Apply Cancel



- b. *Indicator* values represent the effort or resources that must be expended by the attacker in order to carry out the attack or achieve the state.
- c. To break down the (big) Garage Door this node indicates that
- it will cost \$150 (apparently for power tools),
 - there is a 60% (0.6) probability the attacker will be caught (because it is a noisy, obvious attack),
 - on a scale of 1-100, this attack requires skill rating of 25 (to operate the power tools).
- d. The *indicators* are factors that influence human behavior. Not everyone is willing or able to take a 60% chance of being caught. Only very risk tolerant burglars would try this attack.

Edit Node

Title: Brute Force on Garage Door

Type: LEAF

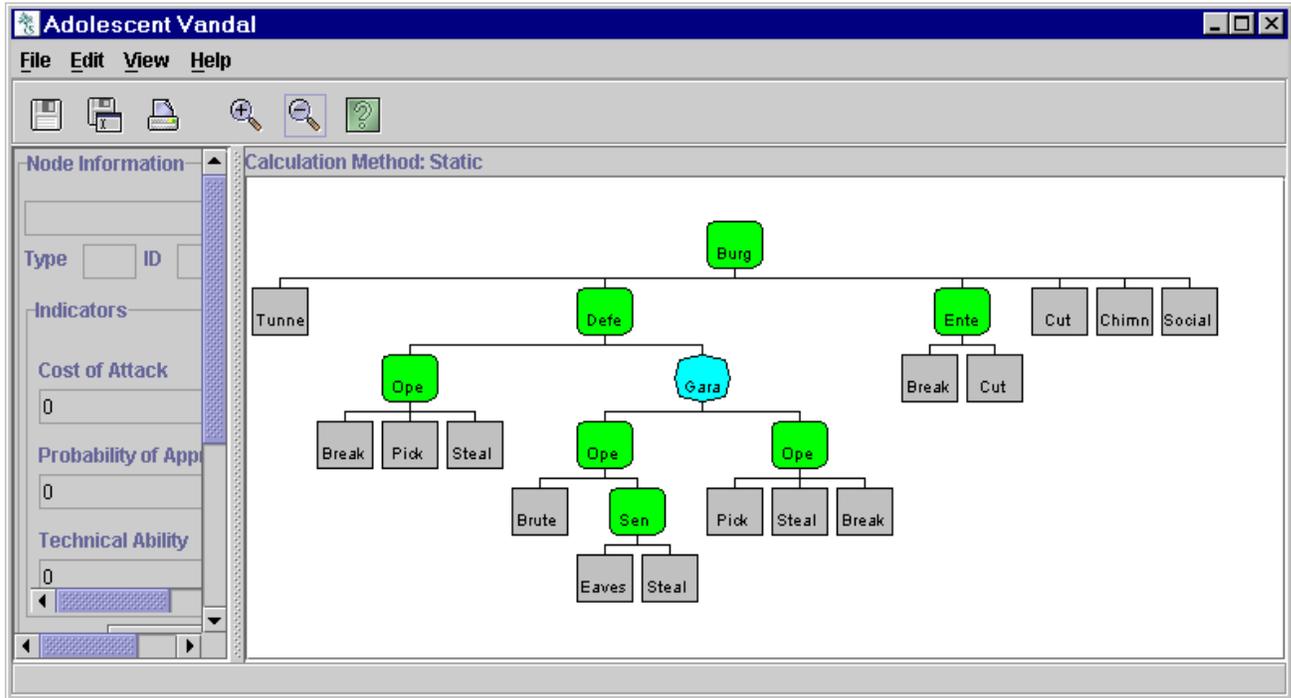
Indicators

Cost of Attack	150
Probability of Apprehension	0.6
Technical Ability	25

- 
7. **By comparing the resources required to perform an attack with those available to an attacker, we can deduce which attacks are worth worrying about.**
- a. All attacks begin with leaf nodes.
 - b. If an attacker doesn't have the "right stuff" to perform a particular attack (represented by one or more leaf nodes) then they will not use that attack!
 - c. Identify different groups or categories of attackers that concern you. We call these groups, *threat agents*.
 - d. The *threat agents* will vary depending on the situation.
 - e. In the House Burglary example, the average homeowner is worried about
 - i. Adolescent vandals,
 - ii. Career criminals (who make a living by stealing small non-identifiable valuables).
 - f. In special situations, other *threat agents* may be applicable. For example, if you are wealthy and have expensive jewelry, you might want to include Cat Burglars. If you are an actor or a rock star, you may be genuinely concerned about obsessive fans.

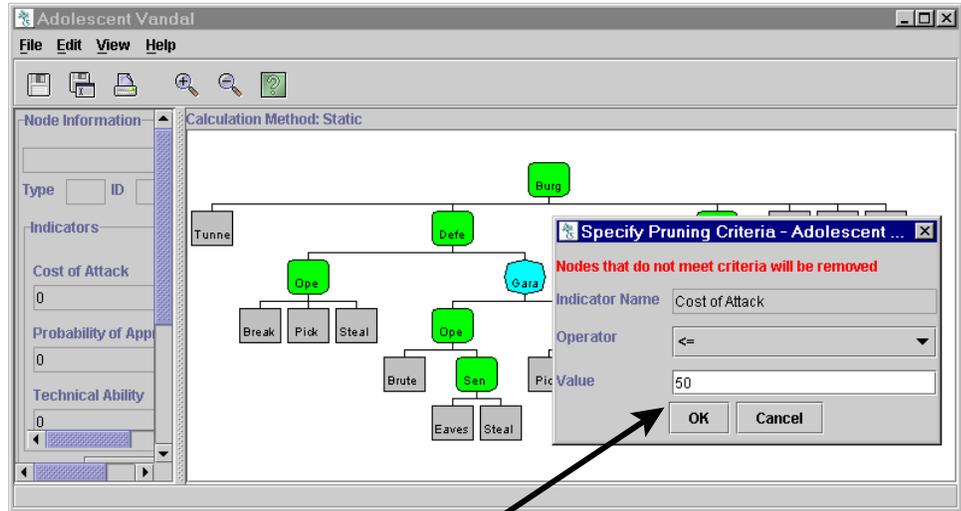


- For each distinct *threat agent*, create a new window to perform analysis.



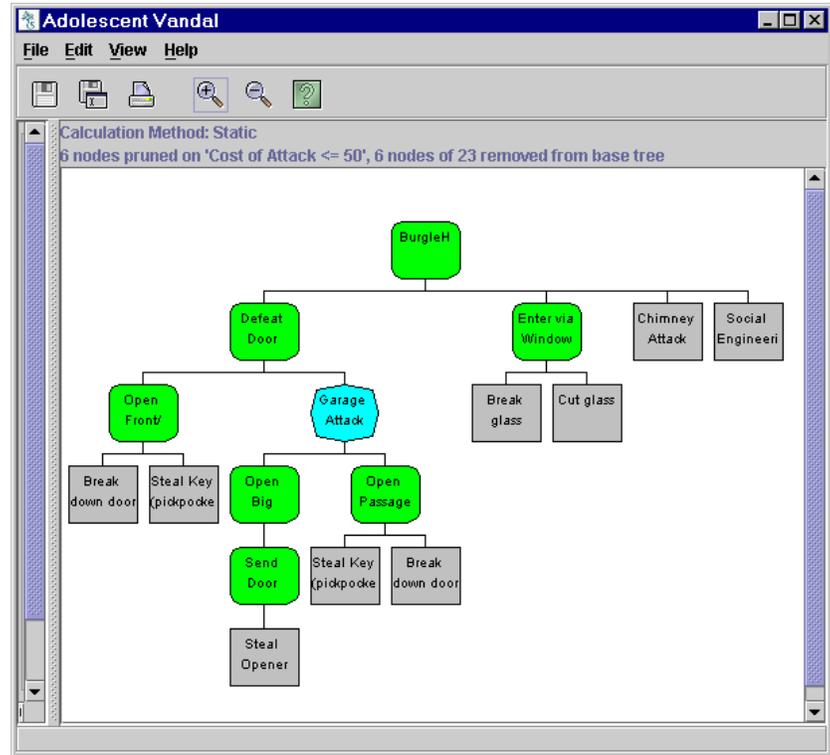


9. Specify the resources available to each *Threat Agent*.
 - a. These are assumptions based on expert opinion.
 - b. Like any assumptions, they may be incorrect.
 - c. Because the assumptions are explicit, the analyst is definitely aware of the factors that will influence the analysis.
 - d. Secur/Tree makes “What If” experiments easy.
 - e. Define assumptions for each *Behavioral Indicator*. In this figure we are asserting that an adolescent vandal will not spend more than \$50 to break into a house.



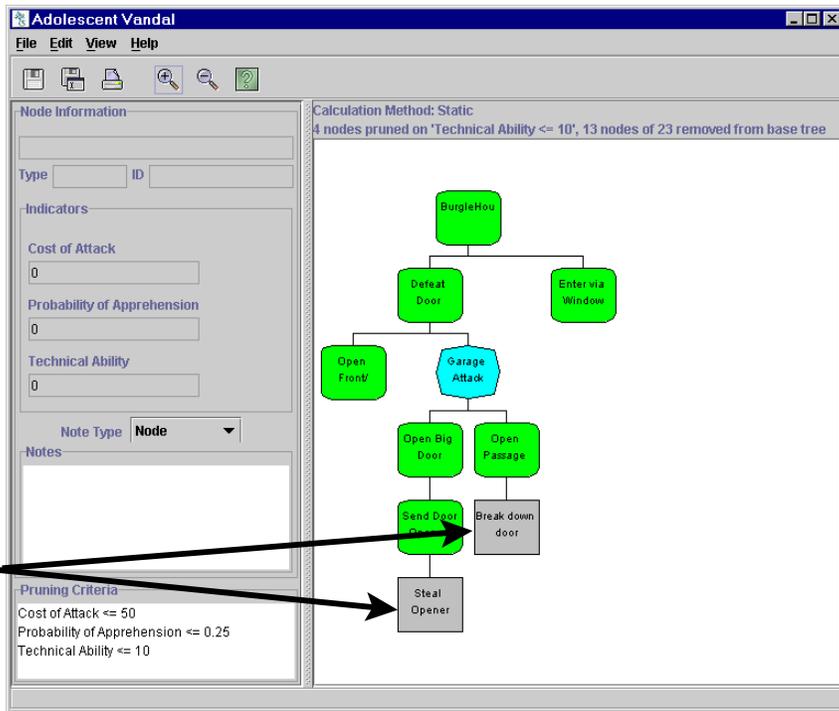


10. Secur/Tree removes all nodes from the tree that are beyond the *Vandal Threat Agent's* capability.
 - a. Remaining nodes indicate attacks that can be carried out by the *threat agent*.



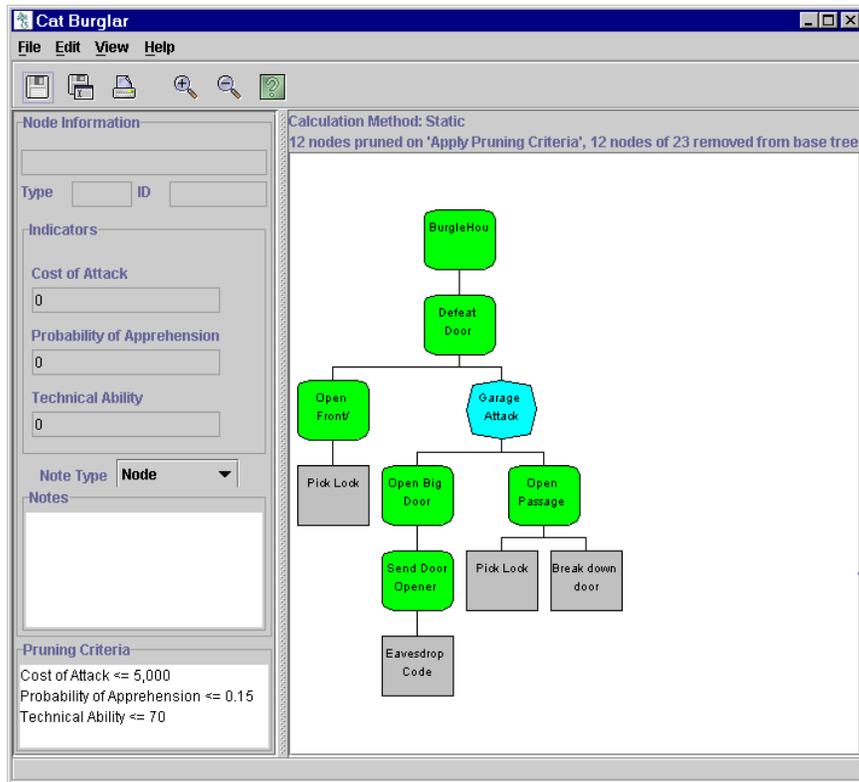


11. Repeat for all defined behavioral indicators.
 - a. Cost of Attack \leq \$50.
 - b. Probability of Apprehension \leq 0.25 (i.e., vandal is willing to do anything that has less than a 25% chance of getting caught).
 - c. Technical Ability \leq 10 (on a scale of 1-100). We are assuming that most adolescent vandals are not skilled. If they were busy studying, or had good job skills, they probably wouldn't be vandals.
 - d. Only two attacks are available to an adolescent vandal. Together they are sufficient to achieve the *Garage Attack*.





12. Compare these results with the analysis for a high end Cat Burglar or jewel thief.
- A Cat Burglar views theft as a job. He or she is willing to spend money on tools if they will get the job done in a cost effective fashion (up to \$5000).
 - The Pro is unwilling to take as much risk as the adolescent vandal (no more than 15% chance of getting caught).
 - The Pro's technical ability is much better (up to 70) than the vandal. He or she has special lockpicking skills and knows a lot about security systems.

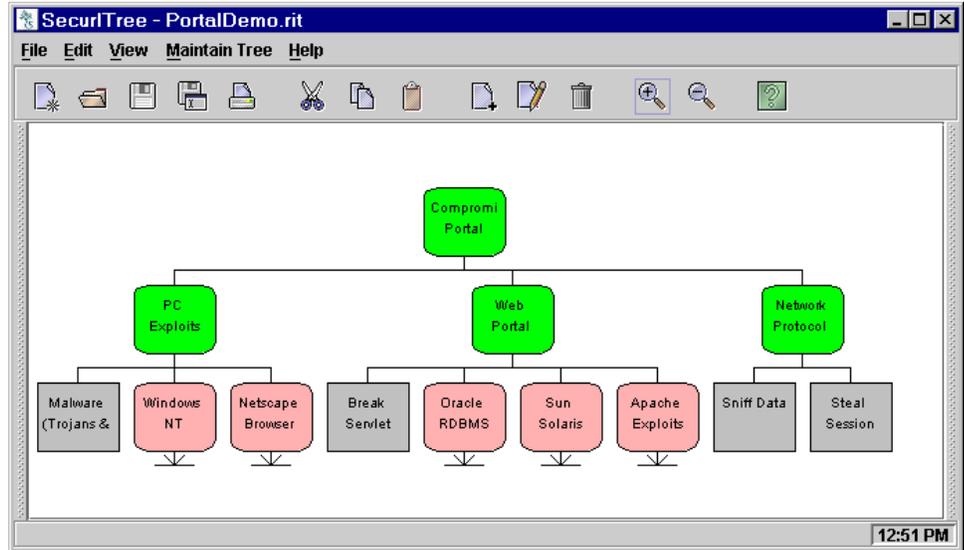




13. Applying Secur//Tree to problems we are familiar with may be overkill.
 - a. Attacks which happen frequently (such as house break-ins) are well understood and intuitive.
 - b. Many attacks are not as easy to understand.
 - c. We need a technique that forces us to state our assumptions explicitly.
 - d. An automated tool is the only way to quickly perform “what-if” thought experiments.
 - i. *What if* our attacker is smarter than we assume? (Find out by increasing their “technical ability”.)
 - ii. *What if* our attacker has more money? (See what new attacks are viable with a bigger budget.)
 - iii. *What if* our indicators do not influence our attacker’s behavior? (Experiment with other indicators.)
 - e. Secur//Tree can analyze problems in many different domains
 - i. Oil/gas pipelines,
 - ii. Chemical Plants,
 - iii. Information Technology,
 - iv. Infrastructure,
 - v. Facilities.

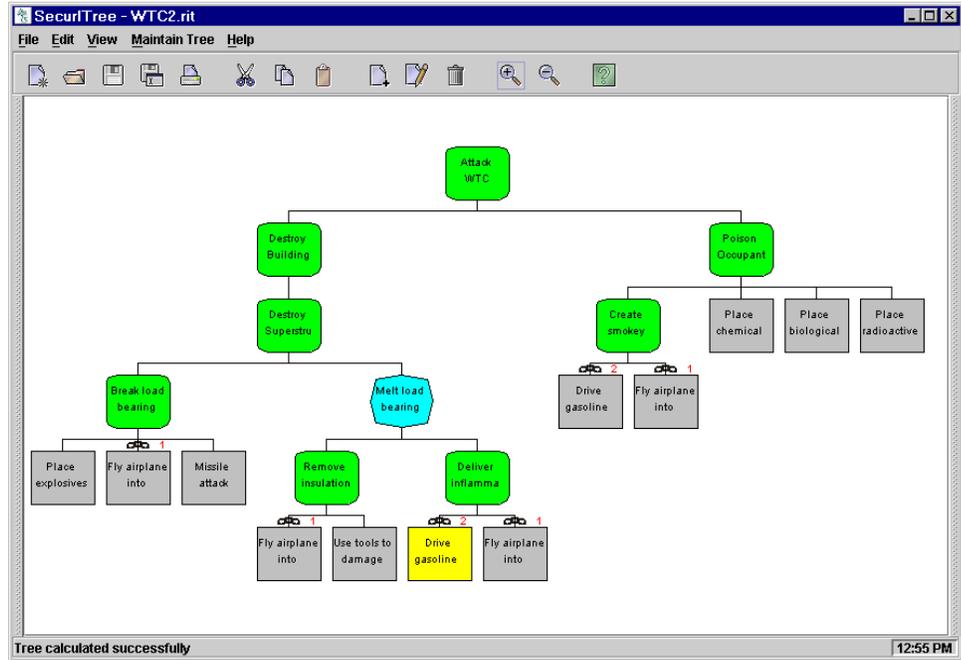


14. Example: an information system.
- Consider the popular corporate intranet web portal application.
 - It consists of many different technologies, each with its own subtle weaknesses.
 - Analysis is simplified using the information technology attack tree libraries that are included with Secur//Tree.
 - The attacks used by professionals, hackers and employees are often very different.





15. Example: the 9/11 attack against the World Trade Center.
- a. Secur/Tree accurately identifies the attack used by the terrorists.
 - b. Hindsight is great – could we have predicted the attack before it occurred using attack tree analysis? We think so.
 - c. Even terrorists and madmen are constrained by the resources at their disposal.
 - d. Know where and how to protect your assets.





16. **It's all about time.**

- a. Every real system has many possible attack points.
 - i. Even with unlimited resources correcting all of the vulnerabilities will take time.
 - ii. Your enemies will attack before you complete your efforts.

17. **It's all about money.**

- a. Do you have unlimited money?
- b. Do you ever wonder whether you actually benefit from the security systems you implement?
- c. How do you calculate Return On Investment (ROI) for security systems?

18. Forewarned is forearmed.

- a. During World War II the Allies gained the upper hand by breaking German Enigma ciphers.
- b. The National Security Agency has said, “Information from the decrypted messages was used by the Allies time after time to outmaneuver German armies. Some ask why, if we were reading the Enigma, we did not win the war earlier. One might ask, instead, when, if ever, we would have won the war if we hadn't read it.” (See <http://www.nsa.gov/museum/enigma.html>)
- c. Will you win your battles without knowing what your enemy is planning?
- d. **Know your enemies' plans with Secur/Tree's easy to understand attack tree analysis.**



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 www.amenaza.com