

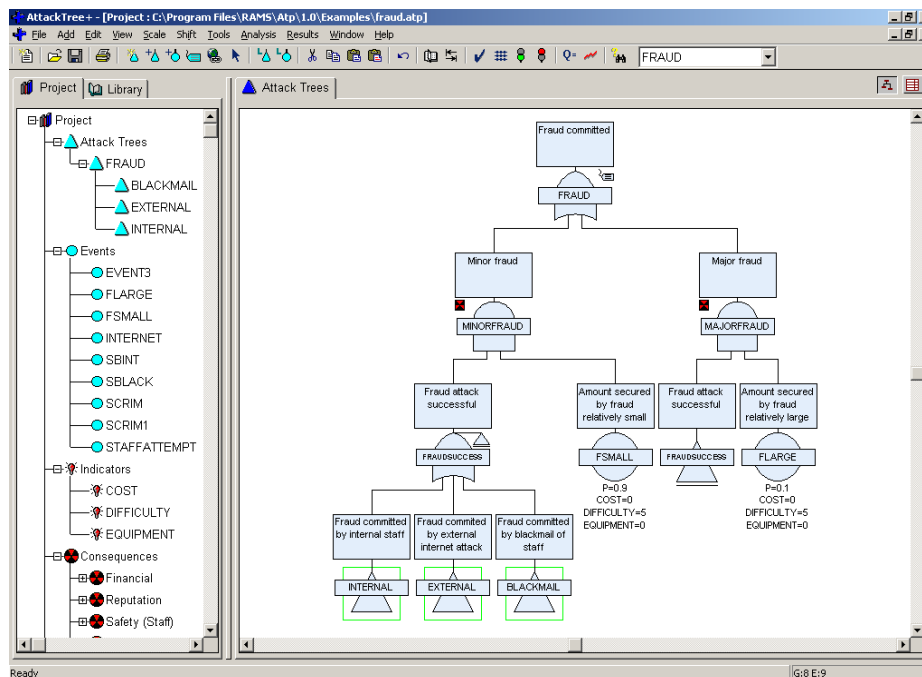
AttackTree+ V1.0 Technical Specification

Platform

Runs under Windows 95, 98, NT, 2000, Me and XP. Recommended host memory – minimum required for operating system, plus 32Mb.

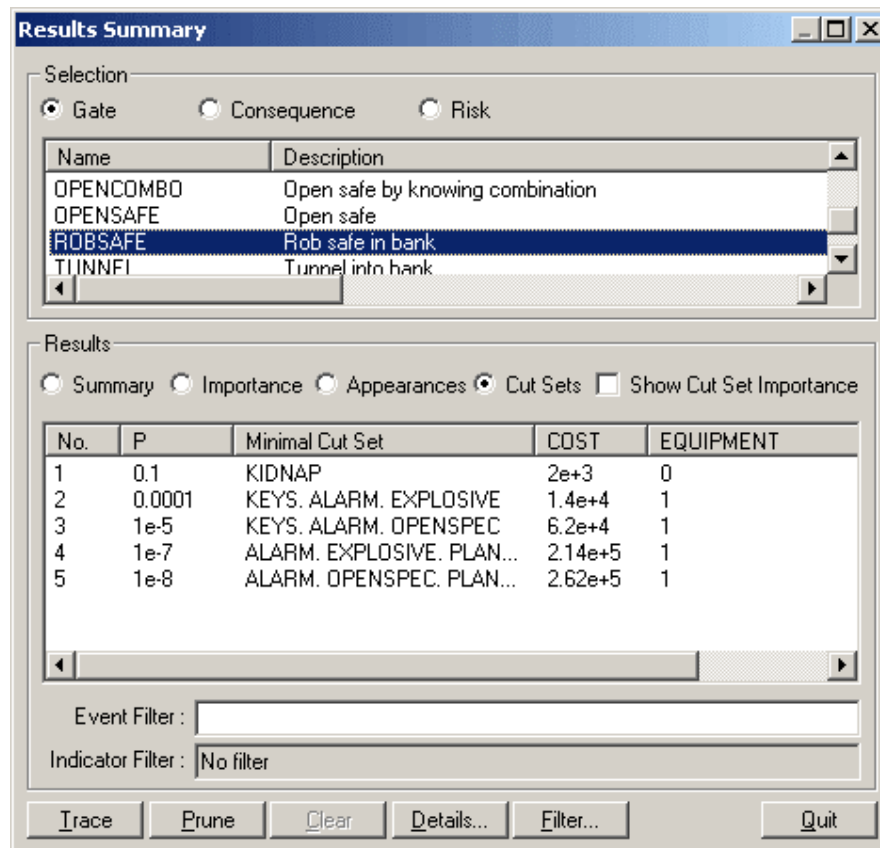
Summary of capabilities :

- Sophisticated environment for constructing and analyzing attack trees
- Automatic drawing facilities produce high quality diagrams without any effort from the user
- Time saving features such as double mouse clicks to bring up gate and event attributes
- Drag and drop add mode for fast tree construction
- Tree control for easy project navigation
- Extensive diagram scale and shift options, including manual shifting of sub-trees and automatic alignment to the screen edit area
- Global and local font selection, allowing highlighting of labels and descriptions
- Automatic paging facilities - simply identify gates with a new page tag and the program takes care of pagination
- Automated attack tree symbol positioning
- Pop-up hyperlinks and notes
- Highlight event types with colour codes and symbol types
- Switch events represent true/false logic
- OR, AND and VOTE (m out of n) logic gates
- Full probabilistic analysis
- Risk Analysis
- Probability frequency and conditional probability models
- Full cut set analysis, including repeated events



AttackTree+ Sample Screen Shot

- User-defined indicators
- Various logical expressions for calculating gate indicator values
- Multiple consequence categories, including option to add user-defined categories
- Importance analysis with contribution and sensitivity factors
- Flexible labelling formatting allows the user to place descriptive text anywhere within an attack tree page
- Project database tables may be easily edited using direct and dependency filtering
- Library facility for storage of common attack tree structures, events, indicators and consequences
- Event and gate names may be globally edited
- Cut, copy and paste facilities for attack trees
- Hyperlinks available for gates and events
- Undo and automatic backup facilities
- Delete hidden data facility for tidying-up large projects
- Cut set tracing and pruning in attack tree diagrams
- Status facility to indicate whether analysis results are out-of-date with respect to project data
- Incorporate custom bitmap pictures for diagram enhancement
- Spell-checker for text fields, including user-definable dictionaries
- Extensive on-line help facilities, including keyword search
- Customisable reports interfacing with Microsoft Office products
- Graphs, plots, pie charts and time profile histograms
- Swift creation of metafiles for attack tree diagrams
- Powerful Import/Export facility, allowing data to be transferred with common database and spreadsheet formats



AttackTree+ Results Summary Dialog

Isograph Reliability Software

www.isograph-software.com

Overview

Attack trees allow threats against system security to be modelled concisely in a graphical format. The effectiveness of internet security, network security, banking system security, installation and personnel security may all be modelled using attack trees. With the increased risk of terrorist attacks on homeland security, hacking attacks on computer systems and computer-based fraud on banking systems, AttackTree+ is an invaluable tool to system designers and security personnel.

AttackTree+ provides a method to model the threats against a system in a graphical easy-to-understand manner. If we understand the ways in which a system can be attacked, we can develop countermeasures to prevent those attacks achieving their goal.

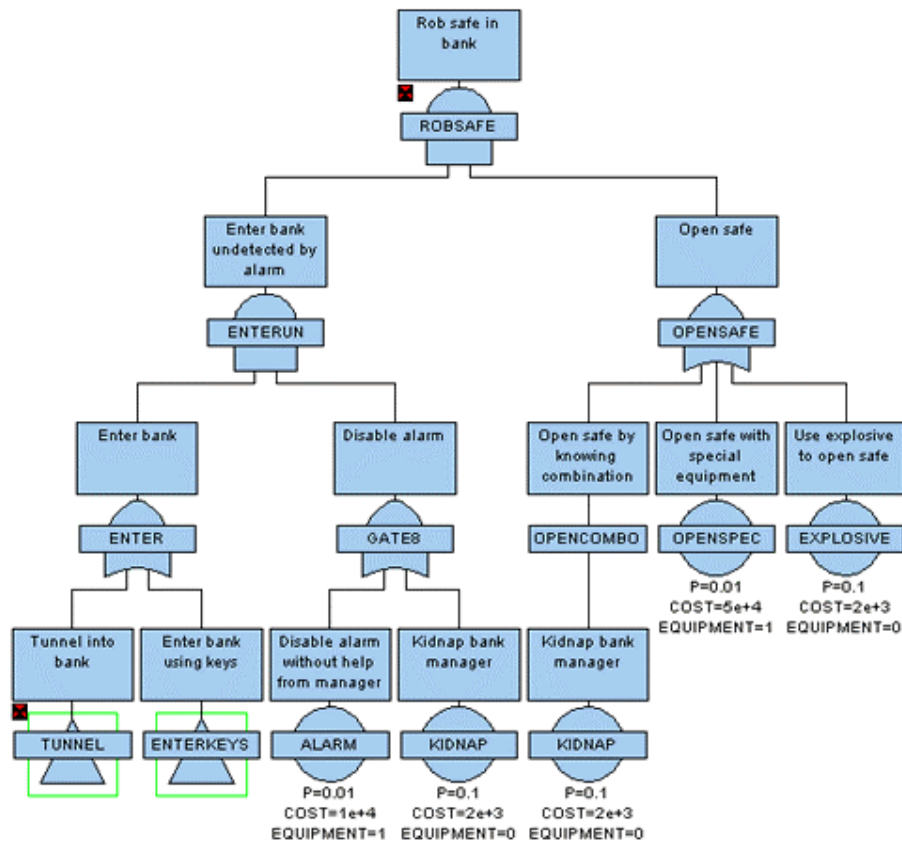
In order for an attack to succeed, the attack has to be initiated and various barriers overcome by the attacker. There may be different ways in which an individual or team could mount an attack on a system and there may be different levels of defence against different types of attack. Attack trees provide a graphical representation of how attacks might succeed and allow a probabilistic analysis of which attacks are most likely to succeed. The methodology can also reveal the vulnerability of your system, under specified constraints. For example, what are the most probable ways in which an attack will succeed in its objective at a relatively low cost to the attacker?

AttackTree+, through the use of attack tree models, allows the user to model the probability that different attacks will succeed. AttackTree+ also allows users to define indicators that quantify the cost of an attack, the operational difficulty in mounting the attack and any other relevant quantifiable measure that may be of interest. Questions such as ‘which attacks have the highest probability of success at a low cost to the

attacker?’ or ‘which attacks have the highest probability of success with no special equipment required?’ can be answered using AttackTree+. In AttackTree+, different categories and levels of consequence may also be assigned to nodes in the attack tree. A successful attack may have financial, political, operational and safety consequences. A partially successful attack may have a different level of consequence to a totally successful attack. All these types of consequence measure may be modelled in AttackTree+.

Diagram Construction

The process involved in constructing the attack tree for your target system begins with the identification of the goals of possible attacks. Due to the fact that different attacks may contain similar methods, this may result in inter-linked attack trees. The next stage is to identify all possible attack methods that may result in the goals being achieved. These first two stages will produce the top level of the system model. Each attack may consist of a large number of conditions that need to be met to allow the attack to be successful, or it may simply consist of a single quantifiable event. Therefore, the next step in the construction of the attack tree is to break down each attack into the basic conditions. This will result in a full attack tree structure with every 'branch' ending in a single quantifiable event.



A Basic Attack Tree Structure

Once the structure is complete, it is necessary to specify the likely frequency for each attack. Next, each event probability must be specified. That is to say, how probable each aspect of the attack is to succeed.

In addition to analyzing how likely an attack is to succeed, attack trees can also employ indicators to describe the cost to the attacker, whether any special equipment is needed, etc. A value for each indicator type is assigned to each event.

Finally, AttackTree+ allows users to define consequences and attach them to any gate within the attack tree. In this way, it is possible to model the consequences of successful attacks on the target system. This is a particularly useful feature when there are many Top Events representing different types of attack, or there are gates in the attack tree representing partial success of an attack.

Analysis

During the analysis process, AttackTree+ will perform the following tasks (NB: a minimal cut set is simply a combination of events that will result in the gate event occurring):

Isograph Reliability Software

www.isograph-software.com

- Determine the minimal cut sets for each gate
- Determine the probability of each cut set
- Determine the indicator values for each cut set
- Calculate the probability of each gate
- Calculate indicator values for each gate
- Determine the minimal cut sets for each consequence
- Determine the probability for each consequence
- Determine risk values for each consequence category

This process will allow the user to view all combinations of events that will lead to a successful attack, ranked in the probability of success. This list may be filtered according to indicator values (e.g. cut sets where the cost to an attacker is low). It is possible to 'prune' the attack tree to easily identify the route by which attack would succeed. Also, importance rankings may be viewed to identify how security may be improved most efficiently.

Available inside AttackTree+, the Report Generator allows the production of completely user-definable, professional reports.