
A Study of Attack Tree Analysis Using a SQL Based Simulation

Michael S. Pallos

Walden University

Abstract

This research evaluated the effectiveness of attack tree analysis incorporated into an information system computer security risk assessment methodology by evaluating the effectiveness of using attack tree analysis to assist with costing decisions, probability analysis, and the viability of using structured query language (SQL) computer program simulation model developed as part of this research. A pre- and post-assessment instrument was developed to ascertain the effectiveness of using attack tree analysis. The data gathering technique included a purposeful sample of 56 computer security experts and leading academic authorities of attack tree analysis. Many facets of society that utilize complex systems, such as Public Policy and Home Land Security efforts, may benefit from this research.

Introduction

Businesses such as insurance and financial institutions once had the luxury of maintaining control over their business and client data by dictating how that data could be used and accessed (Rosall, 2002). The ubiquitous presence of the Internet and the customer demands and regulatory requirements for doing business via the Internet have forced most businesses and entire industries to change their paradigm in order to remain competitive. This paradigm has created a lucrative target for hackers and other

information “thieves,” while at the same time giving these individuals an entirely new set of access points into corporate databases. Information managers are challenged with incorporating risk assessment and threat analysis models as a baseline to assist with identifying potential penetration points. Unfortunately, most risk assessment models (Andrews & Moss, 2002) such as fault tree analysis (Elliott, 1998; Ericson, 1999; Helmer et al., 2000) and failure mode and effect analysis (Elliott, 1998; Huang, Shi, & Mak, 1999) were created to identify failure points within a system, or to perform postmortem analysis of catastrophic events.

What information systems managers appear to be lacking is a methodology which takes a holistic perspective of a system’s penetration points, including, but not limited to, access points external to the system (Schneier, 2000). An example of a system attacker who uses more than the Internet as a means of gaining sensitive corporate data is a hacker who rummages through an organization’s dumpster searching for documents containing vital information. One risk assessment model that considers the holistic perspective of system penetration points is attack trees.

Schneier (1999, 2000) first introduced the concept of attack trees in a paper co-authored with the National Security Agency (Salter, Saydjari, Schneier, & Wallner, 1998), and expanded on the notion in an article in *Dr. Dobbs Journal* the following year (Schneier, 1999). Attack trees provide a process for identifying penetration points throughout all components of a system.

Problem Statement

This study researched the ability to perform calculations based on costing and probability claims made by Schneier (2000, p. 323) regarding the uses of attack trees in

risk assessment and security analysis in an attempt to partially fill this gap. The literature review did not produce a link between application and theory with attack trees (Ellison & Moore, 2001, 2003; Salter, Saydjari, Schneier, & Wallner, 1998; Schneier, 1999, 2000). This research attempted to address the perceived application and theory chasm. Its focus included risk assessment costing analysis, quantifying system vulnerabilities using mathematical formulas, the automation of attack tree costing, and vulnerability assessment built algorithms contained in a software application. Risk assessment costing analysis provided a computer program for information managers as they decide where to invest their budget in order to achieve the greatest benefit from that expenditure. The use of mathematical formulas provided a similar tool for these same managers to identify critical components of their system and efficiently allocate countermeasures in the form of time, money, and human resources. Finally, the use of the software application provided an automated means to implement these methodologies in order to make the process accurate and efficient.

Purpose of the Study

The purpose of this study was to research the effectiveness of attack trees, using costing and probability, incorporated into an information system computer security risk assessment methodology. This research evaluated the effectiveness of using a computer program incorporating attack tree analysis to assist with costing decisions and probability analysis. To assist information systems managers with the above-mentioned process, a deliverable from this study included the creation of a computer program that assisted with the costing and probability decisions information systems managers made with the use of attack trees.

Methodology and Results

A pre- and post-assessment instrument was developed to ascertain the effectiveness of using attack tree analysis. The data gathering technique included a purposeful sample of 56 computer security experts and leading academic authorities of attack tree analysis. The hybrid methodology incorporated quantitative data analysis using the chi-square test of homogeneity and the test for the equality of proportions; while qualitative data analysis include the use of grouping of data creating bar graphs, discussions, conclusions, and other narrative components.

The quantitative research findings suggested a strong support base for attack tree analysis ranging from 71.4% to 92.9%. While only 21.4% to 28.6% of participants are considering implementing attack tree analysis. The qualitative data suggests the transition from theory to implementation may not be achievable.

Conclusions and Recommendations

This study has added to the existing body of knowledge for the risk assessment of computer security systems by providing an academic evaluation of attack trees whose viability and usefulness may extend to information systems managers, government agencies, military organizations, and private citizens who have home computers connected to the Internet. As requested by Salter, Saydjari, Schneier, and Wallner (1998, p. 2), this study provided a step in bridging the gap and facilitating “dialog among academia, industry, and government toward securing the global information infrastructure.”

The process of developing attack trees was automated by a computer program that housed the mathematical properties contained within computer algorithms that

incorporated probability, Boolean algebra, and cost benefit analysis that may have aided information systems managers and security consultants in system analysis (Schneier, 1999, 2000). This program and process may aid in the ability to run countermeasure scenarios and “what-ifs” also adding to the security of information systems.

Further research is required to evaluate the use of attack tree analysis in a large complex setting. The data indicated that attack tree analysis added value as a risk assessment model assisting with costing and probability analysis; however, the data also suggested that attack trees, though useful in theory, may reach a point of uselessness in large organizations. A large attack tree implementation is required to explore this hypothesis.

References

- Andrews, J. D., & Moss, T. R. (2002). *Reliability and risk assessment* (2nd ed.). Fairfield, NJ: American Society of Mechanical Engineers.
- Elliott, J. B. (Ed.). (1998). *Risk analysis*. Booth Scientific, Incorporated Hendersonville, NC: The Validation Consultant.
- Ellison, R. J., & Moore, A. P. (2003, March). *Trustworthy refinement through intrusion-aware design (TRIAD)* (CMU/SEI-2003-RT-002). Pittsburg, PA: Carnegie Mellon University.
- Ellison, R. J., & Moore, A. P. (Eds.). (2001). *Architectural refinement for the design of survivable systems*. Pittsburg, PA: Carnegie Mellon University.
- Ericson, C. A. (Ed.). (1999). *Fault tree analysis - a history*. The Boeing Company; Seattle, Washington: Proceedings of the 17th International System Safety Conference.
- Helmer, G., Wong, J., Slagell, M., Honavar, V., Miller, L., & Lutz, R. (Eds.). (2000). *A software fault tree approach to requirements analysis of an intrusion detection system*. Ames, IA: Iowa State University.
- Huang, G. Q., Shi, J., & Mak, K. L. (Eds.). (1999). *Failure mode and effect analysis (FMEA) over the WWW*. Hong Kong: Department of Industrial and Manufacturing Systems Engineering, The University of Hong Kong.

Rosall, J. (2002). *E-commerce software market forecast and trends, 2002-2006*. Stamford, CT: Gartner Group.

Salter, C., Saydjari, O. S., Schneier, B., & Wallner, J. (1998). *Toward a secure engineering methodology*. : National Security Agency.

Schneier, B. (1999). Attack trees, Modeling security threats. *Dr. Dobb's Journal*, December, 21-29.

Schneier, B. (2000). Attack trees. In C. Long (Ed.), *Secrets & lies, digital security in a networked world* (pp. 318-333). New York: John Wiley & Sons, Incorporated.

About the Author: Dr. Michael S. Pallos is an alumnus of AMDS program with Information Systems Management specialization at Walden University. This dissertation study was chaired by Dr. Pamela Wilson. Correspondence for the author may be sent to e-mail: mpallos@waldenu.edu