Finding Optimal Attack Path Using Attack Graphs: A Survey

Supriya Khaitan, Supriya Raheja

Abstract— **As the traditional methods, the result of vulnerability scanning can't directly reflect complex attack routes existing in network, so the concept of attack graph comes. After analyzing host computer, devices link relation and the characteristic of attack, the model of network security status was built. Attack graphs are one of the important tools for analyzing security. A lot of research has been done on issues such as scalable and time efficient ways of generation of attack graphs. The intent of this paper is to study different ways to generate an attack graph and to provide future scope for research on these attack graphs.**

***Index Terms*— Attack Graph, Attack Path, Network Security, optimal attack path.**

I. INTRODUCTION

Our society has become increasingly dependant on the proper functioning and reliability of a huge number of interconnected information systems. Major issues in nowadays to secure such systems, it is necessary to measure the amount of security provided by various network configurations. Thus it is important to design automatic tools that can analyze the configuration of an enterprise network and find potential security vulnerabilities and the attack paths. In a network with critical resources, certain vulnerabilities may seem to be insignificant when considered in isolation. An attacker may take advantage of it and exploit sequences of related vulnerabilities.

Attack graphs can reveal such potential threats by enumerating all possible sequences of exploits that an attacker can follow to compromise given critical resources.

An *Attack Path* specifies an attack scenario that results in compromising organization values. It tells us how an attacker gains access to the victim computer; how and which vulnerability attacker can take advantage of and what kind of damage may be done that can impact the organization.

II. GENERATION OF ATTACK GRAPH

We have studied various research papers on finding attack path using attack graphs. In this paper, we have included some papers from the starting concept of attack graphs.

In 1999 Schneier [11] gave one of the first descriptions of a manual approach to generate an attack graphs. He explained that each graph has a goal node, and nodes below this represent actions that can reach this goal. Actions combine using either OR (disjunctive) or AND (conjunctive) logic. Weights can be assigned to action nodes that indicate if they are possible, if they require special equipment, the cost of the action, the likelihood of the action, and the probability of success. These values can be propagated to the goal state using the OR and AND nodes to compute the characteristics of paths from different starting actions to the goal state. Graphs were also termed as attack tree, can be applied in many fields. These graphs were generated by hand.

Year 2000 was the first when Ritchey, Amman [2] used a model checker to address the network vulnerability problem. Amman gave a thorough and explicit example that shows how model checking can be used to determine an attack path if a final goal state is reachable for an attacker starting with limited privileges on a network. The model checker is provides the information on network hosts, their vulnerabilities, reachability status between all hosts, the current state of the attacker, and exploits that can be used by the attacker. The model checker either offers assurance that the assertion is true on the actual network or provides a counterexample detailing each step of a successful attack.

Year 2001 a language, LAMBDA was described Cuppens, Ortalo [1]**.** LAMBADA can be used to describe attack scenarios as a combination of different actions. As in the case of JIGSAW model, each action has conditions or requirements that must be satisfied for the action to succeed, and successful actions affect the network and may satisfy conditions for other actions. Actions may be combined using operators that are used to specify sequencing, parallel unconstrained execution, absence of a condition, nondeterministic choice between multiple equivalent actions, and also for synchronized execution. The problem with this language is:

a) it is labor intensive to use
b) only a few examples are provided
c) an automated tool to create scenarios is not presented

In the same year Swiler, Phillips [3] gave first attack graph generation tool. In this tool each node in an attack graph represents an attack state and edges represent the action taken by the attacker. The method was better over other computer security risk methods are:

a) It considers the physical network topology and actual machine configurations in conjunction with the set of attacks possible against that configuration.
b) It builds attack graphs to determine the shortest path

Manuscript received June 09, 2011.

Supriya Khaitan, CSE Department, Sharda University, Greater Noida, India, (e-mail: supriyaKhaitan21@gamil.com).
Supriya Raheja, CSE Department, ITM University, Gurgaon, India, (e-mail: supriya.raheja@gmail.com).

to a specified target.

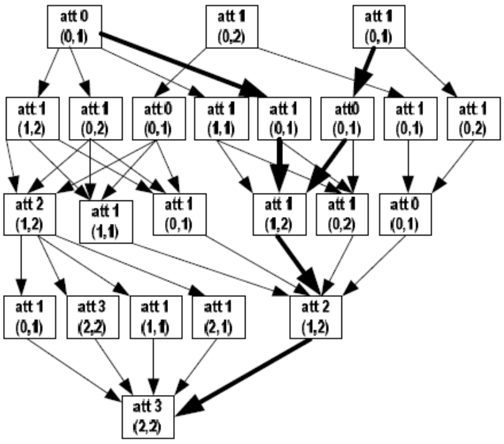

Fig. 1 Attack Graph generated by model checker

In 2002 Artz [8] developed a tool NetSPA (Network Security Planning Architecture) system that generates worst-case attack graphs. NetSPA was developed in C++. Different inputs information required by this tool is:

a) Software types and versions
b) Intrusion detection system placement, gateways between subnets
c) Firewall rules
d) Exploits.
e) Other information, including critical network resources and the attacker starting locations, is provided at run time.

Information on network vulnerabilities is collected using the vulnerability scanner Nessus [9], this information must be entered into the database by hand. Attack graphs are then built, using a depth-limited forward chaining depth-first search. This tool produced attack graphs that were identical to those produced by the model checker described in [10] for the same small test network. It was also evaluated using a realistic network with 17 representative hosts from an actual network, 21 unique vulnerability types. Although the largest graphs for the 17-host network took less than 90 seconds to produce when the graph depth was limited to three, scaling is poor because the graph produced is similar to a full graph.

In the same year Sheyner, Jha, Wing, Lippmann, and Haines [10] gave a thorough and detailed example of using a model checker to analyze the security of a small artificial network. A small artificial network with a few vulnerabilities is used to create a finite-state machine (by hand) that can be analyzed by a model checker. The run time was 5 seconds for this network, but it increased dramatically to 3 hours when the number of hosts was increased to only 5 and the number of vulnerabilities was increased to 8. The major drawback of Model checker is:

a) It scales poorly
b) It is difficult to create inputs for the 20 model checker and interpret the outputs.

Topological Vulnerability Analysis (TVA) [16] tool was developed in year 2003. It is one of the most comprehensive tools developed to date for the purpose of building and analyzing attack graphs. It worked with 3 hosts, 4 exploits, and a firewall with a total of 6 rules and network objects. Major limitations with the TVA approach include the following:

1. Exploit information must be entered by hand
2. Firewall and router rules are not imported and analyzed.
3. Poor scaling to large networks requires low-level attack details.

Dawkins [17] described a framework that can be used to create and analyze attack graphs in computer networks in year 2004. A proof-of concept tool is described that reads in network, vulnerability, and attacker models that are expressed in XML. The main features of this tool are:

1. It builds full attack graphs to a specified depth.
2. Allows a user to select a top-level goal.
3. Extracts paths that reach these goals and simplifies these paths to produce a minimum-cut-set graph.

Inputs to this tool are hand generated same as the other tools and it has only been applied to a small artificial network with 4 hosts and 4 vulnerabilities. Scaling results are not presented, but because a full graph is generated, scaling will be poor because the number of nodes in full graphs can grow combinatorial as the number of hosts in a network grows. The algorithm used to generate a minimum-cut-set graph from the full graph is also not specified. One useful idea presented in this paper is to store network state changes differentially along attack paths.

As in the traditional method, the result of vulnerability scanning can't directly reflect complex attack routes existing in network, so the T Zhang [18] in year 2005 presented an attack graph. After analyzing host computer, devices link relation and the characteristic of attack, the model of network security status was built. Zhang used a forward-search, breadth-first and depth-limited algorithm to produce an attack route and the tools to generate the attack graph was implemented.

In year 2006 Vaibhav Mehta [19] in his paper proposed ranking scheme for the states of an Attack Graph. It was one of the first such papers that gave rank to nodes of an attack graph. Rank of a state shows its importance based on factors like the probability of an intruder reaching that state. Given a Ranked Attack Graph, the system administrator can concentrate on relevant part of graph to figure out how to start deploying security measures. He also defined a metric of security of the measures. He also defined a metric of security of the system based on ranks which the system administrator can use to compare Attack Graphs and determine the effectiveness of various defense mechanisms.

Year 2007 Yue Chen [21] presented a quantitative threat modeling method, the Threat Modeling method based on Attack Path Analysis (T-MAP), which quantifies security threats by calculating the total severity weights of relevant Attack Paths for Commercial off the Shelf (COTS) systems. Compared to existing approaches, TMAP is sensitive to an organization's business value priorities and IT environment. It distills the technical details of thousands of relevant software vulnerabilities into management-friendly numbers at a high-level. T-MAP can help system designers evaluate the security performance of COTS systems and analyze the effectiveness of security practices. He demonstrated the steps of using T-MAP to analyze the cost-effectiveness of how system patching and upgrades can improve security. In addition, he introduced a software tool that automates the T-MAP.

X Xiao, T Zhang, H Wang, [4] describes a comprehensive framework for a component-centric access graph based approach to network attack analysis in year 2008. The framework is comprised of the modeling substrates for network, hosts, vulnerabilities, and the component-centric access graph, access graph generation algorithm and correlative approaches to analyze network vulnerabilities and improve security of computer networks. The work done by Xiao is same as Amman with following improvements:

1. Redefines the access graph formally.
2. Improves the performance of the access graph generation algorithm by taking the preconditions of exploits into account when constructing the chained exploits.
3. Further reducing the algorithmic complexity by examining the possible hosts when generating the chained exploits.

In the same year Jan Magott, Marek Woda [5] defines a formal model of network attack. He also presented a model of intrusion detection system. The models of attack and intrusion detection system can be applied in simulation experiments of network with Service Oriented Architecture and within other organizations. They also gave detail of new features of atomic attack like:

a) Resource consumption
b) Host-processing time
c) Bandwidth of physical connections

M Frigault, L Wang [7] proposed to model probability metrics based on attack graphs as a special Bayesian Network. This approach provides a sound theoretical foundation to such metrics. It can also provide the capabilities of using conditional probabilities to address the general cases of interdependency between vulnerabilities.

In year 2009 Petreska [22] propose an alternative way to study robustness and vulnerability of complex networks by applying a modal analysis. The weights of the network nodes are considered as a measure for their busyness, which is further used for removal of nodes with less weights and attack simulation. Analyses of the attack vulnerability are carried out for several generic graphs, generated according to ER and BA algorithms, as well as for some examples of manmade networks. Petreska found that a modal weight based attack causes significant disintegration of manmade networks by removing a small fraction of the busiest nodes, comparable to the one based on the node degree and centrality.

Nirnay and Ghosh [23] proposed a methodology for finding out optimal risk prone attack path that attacker may choose to penetrate in a wireless network. He used PSO particle swarm optimization to find optimal attack path using attack vector metrics. This is the first such technique where warm optimization concept is used to generate attack graph.

III. FUTURE SCOPE

Various kinds of attack graphs have been proposed for analyzing network security. Although some of them addressed the scalability problem, none of the works has shown solid evidence that the graph generation tool can scale to an enterprise network with realistic sizes. In practice it is desirable to compute attack graphs for enterprise networks with 1000 to 10,000 hosts. It shows that “although research has made significant progress in the past few years, no system has analyzed networks with more than 20 hosts and computation for most approaches scales poorly and would be impractical for networks with more than even a few hundred hosts. Besides the scalability problem, many of the existing attack graph tools adopt an ad-hoc way to represent input information and output graph data structures. The graph generation tools often required various auxiliary inputs in custom-designed data format, and the resulting attack graphs are often hard to comprehend and use by a human. These have made those attack graph tools difficult to use in practice.

Now days the wireless communication revolution is bringing fundamental changes to data networking, telecommunication, and is making integrated networks a reality. Very little work has been done on wireless networks, as the wireless networks works in unpredictable manner. Future research should explore these and other approaches to develop attack graph construction and analysis algorithms that can be applied to large enterprise networks.

IV. CONCLUSION

A lot of research has been done on issues such as scalable and time efficient ways of generation of attack graphs in wired network in contrast to that in wireless scenario. In this Paper, we formulated research papers that describe the past methods to generate an attack graph in wired and wireless networks. For each study, information is provided on the number of attacker goals, how graphs are constructed, sizes of networks analyzed, how well the approach scales to larger networks. Overall, finding an optimal attack path is still facing very key challenges like scalability and mobility. This can be the base of further research on attack graphs.

REFERENCES

[1] F.Cuppens and R. Ortalo, “LAMBDA: A Language to Model a Database for Detection of Attacks,” Recent Advances in Intrusion Detection (RAID) 2000, Lecture Notes in Computer Science 1907, H. Debar, L. Me, and F. Wu, Eds., Berlin: Springer Verlag, 2001.

[2] R. Ritchey and P. Amman,”Using Model Checking to Analyze Network Vulnerabilities”, Proceedings of the IEEE Symposium on Security and Privacy, pp. 156-165, 2000.

[3] L. P. Swiler, C. Phillips, D. Ellis, and S. Chakerian, “Computer-Attack Graph Generation Tool,” Proceedings of the Second DARPA Information Survivability Conference & Exposition (DISCEX II), Los Alamitos, California, vol. II, pp. 307-321, IEEE Computer Society, 2001.

[4] Xiaochun Xiao, Tiange Zhang, Huan Wang, Gendu Zhang “A Component-Centric Access Graph Based Approach to Network Attack Analysis,” in International Seminar on Future Information Technology and Management Engineering pp.171-176, 2008

[5] Jan Magott, Marek Woda “Evaluation of SOA security metrics using

attack graphs," Third International Conference on Dependability of Computer Systems DepCoS-RELCOMEX pp. 277-284 ,IEEE Computer Society , 2008

[6] P. Ammann, D. Wijesekera, and S. Kaushik, "Scalable, Graph-Based Network Vulnerability Analysis," Proceedings of the 9th ACM Conference on Computer and Communications Security, New York: ACM Press, 2002, 217–224.

[7] Marcel Frigault, Lingyu Wang " Measuring Network Security Using Bayesian Network-Based Attack Graphs " Computer Software and Applications, 2008. COMPSAC'08. 32nd Annual IEEE International, pp.698-703, 2008

[8] M. Artz, NETspa, A Network Security Planning Architecture, M.S. Thesis, Cambridge: Massachusetts Institute of Technology, May 2002.

[9] Nessus, "Nessus Security Scanner,"

[10] O. Sheyner, S. Jha, J. M. Wing, R. P. Lippmann, and J. Haines, Automated Generation and Analysis of Attack Graphs," in 2002 IEEE Symposium on Security and Privacy. Oakland, California, 2002.

[11] B. Schneier, "Attack Trees," Dr. Dobbs Journal, December, 1999.

[12] T. Tidwell, R. Larson, K. Fitch, and J. Hale, "Modeling Internet Attacks," Proceedings of the Second Annual IEEE SMC Information Assurance Workshop, United States Military Academy, West Point, New York, June 2001: IEEE Press, 2001, pp. 54–59.

[13] A. Wool, "A Quantitative Study of Firewall Configuration Errors," IEEE Computer, vol. 37, pp.62–67, 2004.

[14] D. Turner, S. Entwisle, O. Friedrichs, D. Hanson, M. Fossi, D. Ahmad, S. Gordon, P. Szor, E. Chien, F. Perriot, and P. Ferrie, "Symantec Internet Security Threat Report, Trends for January 1,2004–June 30, 2004," vol. VI, September 2004.

[15] G. Cohen, M. Meiseles, and E. Reshef, "System and Method for Risk Detection and Analysis in a

[16] Computer Network," USA: Skybox Security Ltd., 2004.

[17] S. Jajodia, S. Noel, and B. O'Berry, "Topological Analysis of Network Attack Vulnerability," Managing Cyber Threats: Issues, Approaches and Challenges, Kumar, Kluwer Academic Publisher, 2003.

[18] J. Dawkins and J. Hale, "A Systematic Approach to Multi-Stage Network Attack Analysis,"Proceedings of the Second IEEE International Information Assurance Workshop (IWIA'04), IEEE Computer Society, 2004.

[19]]T.Zhang, Ming-Zeng, Dong, Liang Sun," An Effective method to generate Attack Graph" Proceedings of the Fourth International Conference on Machine Learning and Cybernetics, Guangzhou, 2005

[20] Vaibhav Mehta, Constantinos Bartzis, Haifeng Zhu, " Ranking Attack Graphs", IEEE Computer Society, 2006.

[21] Somak Bhattacharya, S. K. Ghosh "An Attack Graph Based Risk Management Approach of an Enterprise LAN" " Journal of Information Assurance and Security 119-127, 2008

[22] Yue Chen, Barry Boehm Luke Sheppard "Value Driven Security Threat Modeling Based on Attack Path Analysis" Proceedings of the 40th Hawaii International Conference on System Sciences , 2007

[23] Irina Petreska, Igor Tomovski, Eugenio Gutierrez " Application of modal analysis in assessing attack vulnerabilityof complex networks" Commun Nonlinear Sci Numer SimulatScience Direct pp. 1008-1018,2009

[24] N Ghosh, S Nanda, S.K Ghosh ,"A quantative approach towards detection of an optimal attack path in wireless network using modified PSO technique" , IEEE proceedings , 2009

Supriya Khaitan, Sharda university is masters from GGSIPU in Information Technology and Btech form Punjab Technical University. Her area of interest is network security.

Supriya Raheja, ITM University, is pursuing her PhD in Computer Science from Banasthali University. She had done her engineering from Hindu college of Engineering, Sonepat and masters from Guru Jambeshwar University of Science and Technology, Hisar. She is working as a Reviewer/Committee member of various International Journals and Conferences. Her total Research publications are six.