Network Security Optimization to Measure Security Risks using Attack Graph

Asmitha Shree [1], Manoj Kumar R [2], Naveen P [3]

Assistant Professor 1, UG Scholar [2, 3]

Sri Krishna College of Technology, Kovaipudur, Coimbatore-641042 [1, 2, 3]

ABSTRACT:

To provide security for large organizational networks is challenging due to the complex configurations and constraints. The main goal is to reduce the probability of a successful large-scale attack and measuring security risks in dynamically changing and complex network architecture. To accurately assess the security of networked systems, understand how vulnerabilities can be combined to stage an attack. It can be modeled through attack graphs. It is a success measurement model that measures and reduces the security risk as the probability of success in an attack. Attack graphs have been used to model the vulnerabilities of the systems and their potential exploits. The attack graph h measuring the likelihood that such residual paths may eventually be realized by attackers.

KEYWORDS - Network security, attack graph, probabilistic model, vulnerability analysis, optimization

I. INTRODUCTION

Network security refers to any activity designed to protect the usability and integrity of the network and data. It includes both hardware and software technologies. Effective network security manages efficient access to the network. It targets a variety of threats and stops them from entering or spreading on the network.

Network security combines multiple layers of defenses at the edge and in the network and implements policies and controls. Authorized users gain access to network resources, but malicious actors are blocked from carrying out exploits and threats.

Large organizations need rigorous security tools for Analysing potential vulnerabilities in their networks. However, managing large-scale networks with complex configurations is technically challenging. For example, organizational networks are usually dynamic with frequent configuration changes. These changes may include changes in the availability and connectivity of hosts and other devices, and services added to or removed from the network.

Network administrators also need to respond to newly discovered vulnerabilities by applying patches and modifications to the network configuration and security policies, or utilizing defensive security resources to minimize the risk from external attacks. For instance, a remote attack targeting a host can be prevented by Analysing the candidate defensive strategies in choosing installation and runtime parameters for one or several intrusion prevention systems (IPSs).

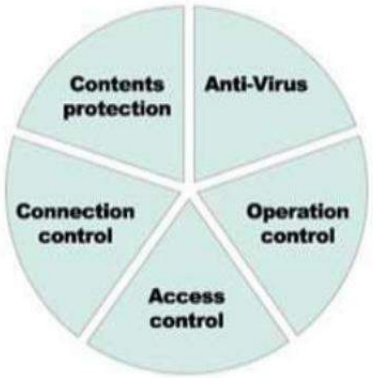

Fig.1. Network Security Threats

An intrusion prevention system (IPS) scans and monitors network traffic to actively block attacks. It is a preemptive approach to network security used to identify potential threats and response to them swiftly.

The very familiar and most common network security threat includes: Viruses, worms and Trojans, Spyware and adware, Zero-hour attacks, Hacker attacks, Denial of service attacks, Identity theft and Data interception theft

II. RELATED WORK

The literature has a significant number of attempts to provide methods, algorithms, and tools for the various problems concerning graph-based analysis of security in large networks. Graph-based analysis of networks represent a graph of attack stages in a network topology was introduced to analyze specific attacks in a network. In addition to producing attack graphs using model checking, introduced an analysis of guarding against the attacks. Unfortunately, some of the ongoing challenges facing automated network security analysis remain unresolved. Per our survey, the literature lacks a comprehensive and rigorous methodology for the assessment of a set of network security defense strategies with the goal of reducing the success of an attack.

ATTACK- In computer networks, an attack is any attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset. An attack via cyberspace, targeting of disrupting, disabling, destroying or maliciously controlling a computing environment/infrastructure or destroying the integrity of the data or stealing controlled information. An attack also defined as an assault on system security that derives from an intelligent threat, i.e., an intelligent act that is a deliberate attempt to evade security services and violate the security policy of the system. There are several attacks that are currently used by the intruders / attackers / hackers to breach the security in networks. It includes Active attack, Passive attack, Distributed attack, Insider attack. Close-in attack, Spoof attack, Phishing attack, Hijack attack, Buffer overflow, Exploit attack and Password attack.

III. ATTACK GRAPH

The attack graphs model how multiple vulnerabilities may be combined for an attack. They represent system states using a collection of security-related conditions, such as the existence of vulnerability on a particular host or the connectivity between di erent hosts. Vulnerability exploitation is modeled as a transition between system states. As an example, consider Fig .2. The left side shows a shows the attack graph for compromise of the database server by a malicious workstation is intended to help protect the internal transfer (ftp), secure shell (ssh), and remote shell (rsh) services. The internal database server o ers ftp and rsh services. c from a user workstation

to both servers, and blocks all other tra c. In the attack graph, attacker exploits are blue ovals, with edges for their pre- conditions and post conditions. The numbers inside parentheses denote source and destination hosts. Yellow boxes are initial network conditions, and the green tri- angle is induced by attacker exploits are plain text. The overall attack goal is a red octagon. The Fig 2. also shows the direct impact of blocking ssh or rsh tra through the attack graph.

IV. USE OF ATTACK GRAPH

Attack graphs have been used to model the vulnerabilities of the systems and their potential exploits. The successful exploits

leading to the partial/total failure of the systems are subject of keen security interest. Considerable effort has been expended in exhaustive modeling, analyses, detection and mitigation of attacks. One prominent methodology involves constructing attack graphs of the pertinent system for analysis and response strategies. This not only gives the simplified representation of the system, but also allows prioritizing the security properties whose violations are of greater concern, for both detection and repair.

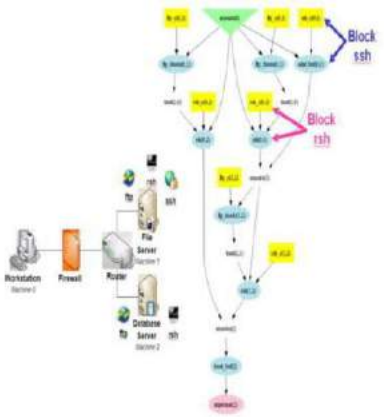

Fig.2. Example Network, Attack Graph and Network Hardening choices

V. MEASURING ATTACK LIKELIHOOD

In practice, vulnerabilities often remain in a network, even after they are discovered. Vendors may be slow to release software patches, or deployment may be delayed because of excessive cost or e ort. Attackers often leverage even correctly functioning network services to gain new capabilities. An organization will often trade security risk for availability of services. The attack graph measuring the likelihood that such residual paths may eventually be realized by attackers. When a network is more secure, attack likelihood is reduced. Preventing exploits as in Fig.2., removes certain paths, in turn reducing attack likelihood. When the attacker cannot reach the goal, the metric is zero. When the attacker is completely assured of reaching the goal, the metric is unity.

VI. CHALLENGES FOR SECURITY RISK ANALYSIS FOR NETWORK

A. Security vulnerabilities are rampant: Computer emergency report technology reports about hundred new security vulnerabilities each week. It become a difficult to manage the security of the network(with hundreds of hosts and different operating system and applications on each host) in the presence of software vulnerabilities that can be exploited.

B. Attackers launch complex multi-step cyber attack: Cyber attackers can launch multi-step and multi-host attacks that can be incrementally penetrate the network with the goal of eventually compromising critical systems. It is a challenging task to protect the critical systems from such attacks.

C. Current attack detection methods cannot deal with the complexity of attacks: Computer systems are increasingly under attack. When new vulnerabilities are reported attack programs are available short amount of time. Traditional approaches to detecting attacks(using an intrusion detection system) have problems such as too many false positives, limited scalability and limits on detecting attacks.

VII. RISK ANALYSIS USING ATTACK GRAPHS

In practice, vulnerabilities often remain in a network, even after they are discovered. Vendors may be slow to release software patches, or deployment may be delayed because of excessive cost or e ort. Attackers often leverage even correctly functioning network services to gain new capabilities. An organization will often trade security risk for availability of services. Removing attack paths reduces options for an attacker, but at what cost to the organization? For example, in Fig.2., blocking ssh or rsh tra c disables certain initial network conditions, preventing exploits that depend on these vulnerable connections, thereby reducing the number of attack paths. But what is lacking is a clear measure of exactly how security has been improved in each case.

VIII.SUCCESS MEASUREMENT MODEL

The module compute the expected chance of a successful attack on a network with respect to the success measurement model computes probabilities as a function of initial belief probabilities without the need for specifying conditional. The set of initial belief values required by the model is small and can be obtained from standard vulnerability assessment systems. This model measures the success of an attacker based on the attack dependencies determined by a logical attack graph.

IX. SECURITY IMPROVEMENT MODEL

To achieve the main goal of reducing the probability of success in an attack, and thus optimizing the overall security of the network, point out the necessity to model this problem as an optimization problem. Further, attempt to model an important feature that is to consider the availability of machines in the network.

Optimizing the security of the network: Given a set of security hardening products (e.g., a host based firewall), compute an optimal distribution of these resources subject to given placement constraints. Using the rigorous probabilistic model, this is the first work in which a logical attack graph is transformed into a system of linear and nonlinear equations with the global objective of reducing the attack goal. This transformation is performed efficiently and naturally and directly captures the goal.

Machine availability and the effect of mobile devices: This explain how to represent and assess devices with variable availability (frequently joining and leaving the network), which is one of the characteristics of mobile devices with variable connectivity.

X. PROBABILISTIC ANALYSIS OF ATTACK GRAPHS

One way to incorporate probabilities into attack graphs is to choose a subset of states and make transitions out of those states probabilistic. Suppose that the graph has a state s with only two outgoing transitions. In

a regular attack graph, the choice of which transition to take when the system is in state s is nondeterministic. However, some empirical data that enables to estimate that whenever the system is in state s, on average it will take one of the transitions four times out of ten and the other transition six remaining times. Probabilities 0:4 and 0:6 can be placed on the corresponding edges in the attack graph. Intuitively, probability of the transition s ! s0 represents the likelihood that the atomic attack corresponding to the transition will succeed. A state with known probabilities are called for outgoing transitions probabilistic. When all known probabilities are assigned in this way, left an attack graph that has some probabilistic and some nondeterministic states in it. Then such mixed attack graphs probabilistic attack graphs are called. Use probabilistic attack graphs to evaluate the reliability of a network. Note that probabilities of all the transitions might not be available because of lack of data, e.g., a new type of atomic attack. Since the attack graph includes only those states and transitions that can lead to success states, it excludes some transitions that exist in the complete model M. These excluded transitions can have non-zero probability, so that the sum of probabilities of transitions from a probabilistic state will be less than 1. To address this problem, model the rest of M in AG (Sun safe some way. A - Escape state se to the attack graph. A probabilistic states in the attack graph will have a transition to se if and only if in M there is a transition from s to some state not in the attack graph. The probability of going from s to se will be 1 minus the sum of the probabilities of going to other states. There are no transitions out of se except a self-loop (which preserves the totality of the transition relation).

In an attack graph containing the escape state se attacks are allowed to terminate in se. It can be called as escape attacks, or attacks that were preempted by the intruder.

XI. ALGORITHM FOR GENERATING ATTACK GRAPHS

Input:

S set of states

R _ S _ S transition relation S0 _ S set of initial states

L : S -> 2AP labeling of states with propositional formulas

p = AG(unsafe) (a safety property)

Output:

attack graph GP = (Sunsafe ,RP,SP0,SPS,L)

Algorithm:

GenerateAttackGraph(S,R, S0, L, p)

(Use model checking to find the set of states thatviolate the safety property unsafe). *)*

Sunsafe = modelCheck (S,R, S0, L, p).

(Restrict the transition relation R to states in the set Sunsafe *)*

Rp = R (Sunsafe × Sunsafe).

SP0 = S0 Sunsafe

SPS = {s|s Sunsafe ^ s|= unsafe } return(Sunsafe ,RP,SP0,SPS,L)

XII. ATTACK GRAPH PROPERTIES

An attack graph G generated by the above algorithm is exhaustive and succinct with respect to states and edges.

Proof is straightforward and following properties of the attack graph G are true:

(a) exhaustive

(b) succinct with respect to states

(c) succinct with respect to edges

XIII. CONCLUSION AND FUTURE ENHANCEMENT

A probabilistic model called Attack graph was formalized for measuring and reducing the security threats in large enterprise networks. It has the ability to quantitatively analyze and reduce the chance of successful attack in the presence of uncertainties about the configuration of a dynamic network and routes of potential attacks.

After the analysis of attacks, the future enhancement is to use the security improvement model and optimal security placement algorithm to reduce the security in the network. Noise elimination is the other important factor in the security of the network which is to be focused for obtaining more accurate results.

XIV.REFERENCES

[1]. Hussain M.J. Almohri, Layne T.Watson Dynamic Networks with Probabilistic Graph July/August 2016.

[2]. Y. Dou, K. Zeng, Y. Yang, and D. Yao, Malware detection for cognitive radio, Proc. IEEE Conf.,2015.

[3]. L. Wang, S. Jajodia, A. Singhal, P. Cheng, -zero daysafety: A network security metric for measuring the risk of Dependable Sec. Comput.,vol. 11, no. 1, pp. 30 44, Jan./Feb. 2014.

[4] Dynamic Security risk management usingIEEE Trans.Dependable Secure Comput., Jan 2012.

[5]. M. Albanese, S. Jajodia, A. Pugliese, and V. Subrahmanian, is of attack Proc. 16th Eur. Conf. Res. Comput. Security, 2011, pp. 416 433.

[6]. S. Noel and S. Jajo sensor placement and alert prioritization using Systems Management, Sep. 2008.

[7] Critical attacks assets in Dependency attack proc Eur. Symp. Res. Comput. Security, 2008.

[8]. X. Ou, W. F. Boyer, and M. A. McQueen, attack graph Proc. 13th ACM Conf. Comput. Commun. Security, 2006, pp. 336 345.

[9]. M. S. Bazaraa, H. D. Sherali, and C. M. Shetty, Nonlinear Programming.New York, NY, USA: Wiley, 2005.

[10]. O. Sheyner, J. Haines, S. Jha, R. Generation and Proceedings of the IEEE Computer Society, 2002.