Risk Management using Behavior based Attack Graphs

Ram Dantu
University of North Texas
rdantu@cs.unt.edu

Kall Loper
University of North Texas
doc@unt.edu

Prakash Kolan
University of North Texas
prk0002@cs.unt.edu

Abstract

Security administration is an uphill task to implement in an enterprise network providing secured corporate services. With the slew of patches being released by Microsoft, HP and other vendors, system administrators require a barrage of tools for analyzing the risk due to these vulnerabilities. In addition to this, criticalities in patching some end hosts (eg., in hospitals) raises serious security issues about the network to which the end hosts are connected. In this context, it would be imperative to know the risk level of all critical resources (e.g., Oracle Server in HR department) keeping in view the everyday emerging new vulnerabilities. We hypothesize that sequence of network actions by an attacker depends on the social behavior (e.g., skill level, tenacity, financial ability). By verifying our hypothesis on hacker email communications, we extended this methodology and calculated risk level for a small network. Towards this goal, we formulated a mechanism to estimate the risk level of critical resources that may be compromised based on attacker behavior. This estimation is accomplished using behavior based attack graphs. These graphs represent all the possible attack paths to all the critical resources. Based on these graphs, we calculate the risk level of a critical resource using Bayesian methodology and periodically update the subjective beliefs about the occurrence of an attack Such a calculated risk level would be a measure of the vulnerability of the resource and it forms an effective basis for a system administrator to perform suitable changes to network configuration. Thus suitable vulnerability analysis and risk management strategies can be formulated to efficiently curtail the risk from different types of attacker (script kiddies, hackers, criminals and insiders).

1.Introduction

With the increase in number of hosts connected to the enterprise network, there is always a mounting risk of protecting computers from the outside attacks. In addition to this, improper configuration of network hosts result in host vulnerabilities because of which the hosts are susceptible to outside attacks. With increasing network scanning technologies and end host vulnerabilities, effective security policies have to be implemented along with cost effective vulnerability analysis techniques. It has to be supported with appropriate network optimization for at most security. For managing the security of a network, security engineers identify security holes by probing the network hosts, assess the risk associated with the vulnerabilities on the computer hosts, fix host vulnerabilities by using patches released by the vendors and ultimately come up with an advanced set of security policies to be implemented for effective management of the network. Patching up network hosts is a short-term solution for avoiding an attack, but this requires fixing the vulnerabilities in all of the network hosts and their components. But this process of patching end hosts requires a great deal of human intervention, time and money for frequently monitoring the end systems by using a set of monitoring tools to identify and prevent intrusion. The difficulty in patching end hosts worsens when the already present state of the art monitoring tools are not effective in identifying new vulnerabilities. Similarly, in the case of high exploitation probability on the network and its hosts, risk management is a nightmare to plan with, due to everyday emerging new exploits. However, it is possible to estimate the risk based on a sequence of network actions when they are grouped with an attack behavior. For many years security engineers have been doing risk analysis using economic models for the design and operation of risk-prone, technological systems [1] [2] [3] using attack profiles. Considerable amount of research has been reported in developing profiles of the attacker based on the evidence he leaves behind during an attack. The evidence collected can be used in estimating the type of attacker. Based on the type of attacker identified, effective risk management policies can be formulated for the network.

Simultaneously, a great deal of psychological and criminological research has been devoted to the subject; but the security engineers do not use these studies. To our knowledge, no work has been reported on integrating behavior-based profiles with sequence of network actions for computing the vulnerability of resources. *The overall* *goal of this research is to estimate the risk of a critical resource based on attacker behavior and a set of vulnerabilities that can be exploited.* This implies a more fine-grained repertoire of risk mitigation strategies tailored to the threat rather than blanket blocking of network activity as the sole response.

2. Background

A considerable amount of work has been reported on attacker profiles and risk management on an individual basis. But none of them is successful in integrating risk analysis with attacker behavior. Jackson[3] introduces the notion of behavioral assessment to find out the intent behind the attack. This work advocates learning human behavior by analyzing the packet stream into "discrete bundles" in real time from a single IP address and report any abnormal behavior if detected. This is in contrast to the general signature and anomaly based intrusion detection methodologies where instead of depending on a set of rules governing the detection, it relies on packet information analysis in real time. But this does not propose any detail on vulnerable device identification based on the assessed behavior. Ian[15] views risk analysis to involve threat identification, risk assessment and steps to be taken for mitigating the risk. The issues that are identified to be of potential threats are identified and an estimate of damage the threat could pose is calculated. But there is a need to integrate attack behavior with risk mitigation strategies could help reduce the possibility of impending attacks.

The psychological and criminological research on hacker community attempts to define different categories of hackers based on their intent, skill and attack proficiency. Yuill [1] proposed deriving hacker profiles based on ongoing attack and intruder behavior. Using this, an identification of vulnerable devices in a network can be achieved which could subsequently help in repairing and securing the network. But the suggested proposal lacks quantitative analysis of attacker behavior attributes and sequence of network actions to recognize risk prone devices in the network There are several works in the literature on the hacker profiles [5] [6] [7] [8] but none of them tie the profiles to any exploits in the network.

On the other hand, attack graphs are beginning to be used to formalize the risk for a given network topology and given exploits. Sheyner [11] attempts to model a network by constructing attack graph for the model using symbolic model checking algorithms, which would help in analyzing the attacks that would be more cost-effective to guard against. Morre [10] documents attacks on enterprises in the form of attack trees, where each path from the root to the end node documents how an attacker could realize his desire of exploiting the host and ultimately the network. However, current research [9] [10] [11] does not combine the behavior with these graph transitions.

Loper [4] [12] indicates that mapping network actions to social motives is sustained by the available data. It is relatively well established in social science that measurable attitudes and observable actions can predict specified behavior (within a known level of error). Loper identified overreaching constructs like content, method, self-definitions, and culture. This work automates the analysis of data to build standard expressions or groups of expressions that indicate a meaning. The way hackers use these expressions are compiled into activity profiles that can be used to distinguish hacker from computer criminals.

This paper marries profiling with chain of exploits, and detects highly vulnerable resources in the network. In addition, behavior profiles are used for calculating the trust of a given attack path. Our work uses the theory from criminology, statistical analysis, behavioral based security, and attack graphs.

3. Methodology

Attack graphs or trees are been increasingly formalized to be a model for representation of system security based on various attacks. An attack tree can be visualized to be a graph consisting of a group of nodes with links interconnecting them. We use attack graphs to calculate vulnerabilities and risk of a critical resource in a given network configuration. There are five steps in our procedure. The five steps are repeatedly executed until optimum security is achieved.

Step 1->Creation of an attacker Profile: The profile of an attacker is created to relate the sequence of network actions that he might take during the course of an attack. The profile gives the expendable resources associated with the attacker. These resources can be any of cost, skill tenacity etc. that the attacker would expend to exploit a vulnerability. Different attack profiles have different behavioral attribute values for the attacker resources. Creating an attack profile would help in identifying the probable attacks and the probable network resources that can be compromised by the attacker.

Step 2->Creation of Attack Graph: To achieve Denial of Service or intrusion attack, malicious users take advantages of a series of exploits existing in the network. An attack graph can be created using network topology, interconnection between hosts, and various vulnerabilities of each host [9] [10] [11] . In this graph, each path identifies a series of exploits. Using this graph, we can learn how intruders culminate sequence of state transitions for achieving an attack. For example, an attack path in an attack graph (see Figure 1) can be a sequence of events like overflow *sshd* buffer on host1, overwrite *.rhosts* file on host2 to establish *rsh* trust between hosts1 and host2, log-in using *rsh* from host1 to host2, and finally, overflow a local buffer on host2 to obtain root privileges.

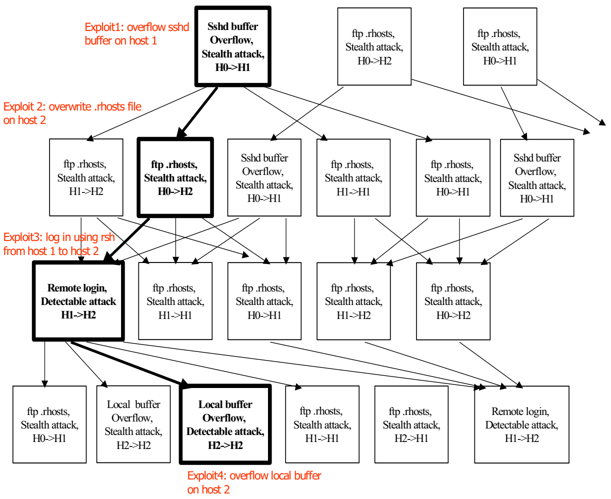
Exploit1: overflow sshd buffer on host 1
Sshd buffer Overflow, Stealth attack, H0->H1
ftp .rhosts, Stealth attack, H0->H2
ftp .rhosts, Stealth attack, H0->H1
Exploit 2: overwrite .rhosts file on host 2
ftp .rhosts, Stealth attack, H1->H2
ftp .rhosts, Stealth attack, H0->H2
Sshd buffer Overflow, Stealth attack, H0->H1
ftp .rhosts, Stealth attack, H1->H1
ftp .rhosts, Stealth attack, H0->H1
Sshd buffer Overflow, Stealth attack, H0->H1
Exploit3: log in using rsh from host 1 to host 2
Remote login, Detectable attack H1->H2
ftp .rhosts, Stealth attack, H1->H1
ftp .rhosts, Stealth attack, H0->H1
ftp .rhosts, Stealth attack, H1->H2
ftp .rhosts, Stealth attack, H0->H2
ftp .rhosts, Stealth attack, H0->H1
Local buffer Overflow, Stealth attack, H2->H2
Local buffer Overflow, Detectable attack, H2->H2
ftp .rhosts, Stealth attack, H1->H1
ftp .rhosts, Stealth attack, H2->H1
Remote login, Detectable attack, H1->H2
Exploit4: overflow local buffer on host 2

Figure 1: An example attack graph with a chain of exploits

Step3-> Labeling Attack Paths with Behavior Attributes : In this step, the attack graph with attacker attributes will generate a list of attack paths related to these attributes(Figure 2). For example, the attributes can be : i) Computer-skills, ii) Hacking skills iii) Tenacity iv) cost of attack, and iv) techniques for avoiding detection, etc.

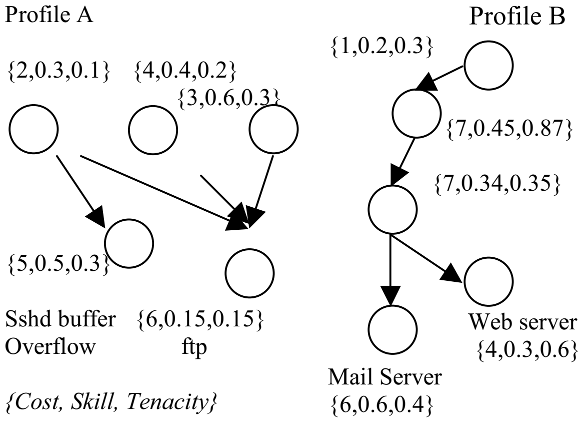

Figure 2: Attack paths based on profiles

We construct profile based attack graphs by documenting all the attack paths for a given attacker profile. Figure **2** represents attack graphs constructed based on the profiles of A & B respectively. A sequence of network actions can be constructed that are possible to be undertaken by the attacker for whose profile the attack graph has been drawn. Based on the type of the attacker, the attack paths are considerably different depending on the type of quantifying variable in consideration. The eventual path of the attacker would be his optimized use of the quantifying variables such as cost, skill , tenacity etc. Thus the final attack path "Θ" taken by the attacker would be a function of individual attack paths i.e Θ = (f_1,f_2,…f_n) where each f_i is the attack path that an attacker would take for an identifier variable "i". Each f_i can be calculated by documenting individual attack paths of the attack graph. An attack path with nodes of "n" number of attributes in figure 3(a) can be represented as in figure 3(b).

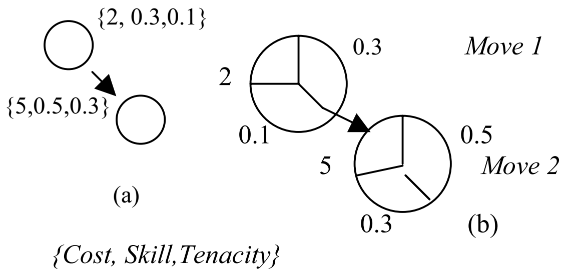

Figure 3 An attack path of a given profile

Path

Move	Skill	Tenacity	Cost	….
1	0.3	0.1	2	
2	0.5	0.3	5	
….				

Table 1: Probabilities for exploiting a vulnerability for each path in the attack graph.

Table 1 documents all the behavioral attributes for each attack path and exploit. Therefore, given an attacker profile, all the attack paths that the attacker can move are known. This helps us in deducing all the vulnerable resources in a network for a given attack profile.

Step4->Risk Computation: In this step, a risk level for all the critical resource is calculated based on the set of paths, attributes and attacker type (e.g., script kiddie, hacker, corporate insider etc.). Bayesian networks based estimation is used for calculating the aggregated risk value of the resource. Next, a resource is marked as attack prone if this value is more than a threshold. In some cases, the resource may be marked for more than one kind of attack. For example, the web portal may be attacked either by hacker or a criminal.

A Bayesian network is a graphical model for showing probabilistic relationships among a set of variables in a Directed Acyclic Graph (DAG). Each node(symbolizing a variable) in a Directed Acyclic Graph is associated with a set of Probability Distribution Functions and therefore a

Bayesian network can be used to encode the joint probability distribution for a set of variables. Bayesian statistics helps us to quantify the available prior probabilities or knowledge based on the evidence colleted at any node in the network. The evidence thus collected updates the subjective belief of all the other random variable probability distribution using Bayesian Inference.

Bayesian networks encode the probability relationships between various random variables or nodes in a causal graph and therefore we can model the attack trees by reducing them to causal graphs and associating the nodes or random variables with probabilities. Using monitoring or intrusion detection systems, protocol state machines and the traffic patterns observed between various states in the state machine, the initial subjective beliefs can be formulated and the new posterior probabilities are calculated. The new posterior probability distributions designate the updated subjective beliefs or the possibilities of the intermediate network actions to achieve the overall goal of exploiting the vulnerabilities existing in the network and its components. *These posterior probability calculations are done before and after the exploits or vulnerabilities are patched to estimate the new risk level of the critical resources.* The following procedure shows the calculation of the posterior probabilities based on new evidence.

Consider an attack graph in the figure below

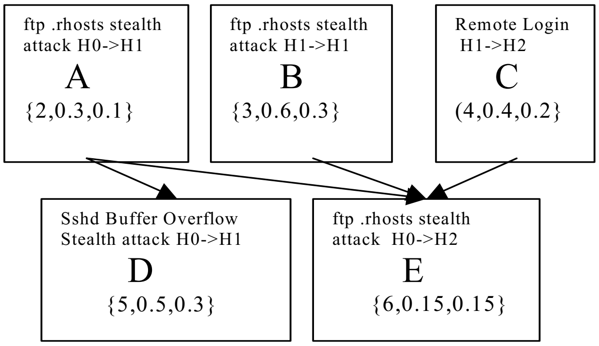
ftp .rhosts stealth attack H0->H1
A
{2,0.3,0.1}
ftp .rhosts stealth attack H1->H1
B
{3,0.6,0.3}
Remote Login H1->H2
C
(4,0.4,0.2}
Sshd Buffer Overflow Stealth attack H0->H1
D
{5,0.5,0.3}
ftp .rhosts stealth attack H0->H2
E
{6,0.15,0.15}

Figure 4: A small Bayesian Causal graph

Consider each of the nodes might be in two states "yes" and "no" and assume some of the probabilities to be given as

P(A = yes) = 0.1	P(A = no) = 0.9
P(B = yes) = 0.3	P(B = no) = 0.7
P(C = yes) = 0.2	P(C = no) = 0.8
P(D=yes |A=yes)=0.3	P(D=yes |A=no)=0.4
P(D=no |A= yes)=0.7	P(D=no |A=no) = 0.6

P(E=yes |C=yes ,B=yes ,A= no) = 0.25
P(E=no |C=yes ,B=yes ,A= no) = 0.75
P(E=yes |C=yes ,B=yes ,A=yes) = 0.15
P(E=no |C=Yes ,B=yes ,A= yes) = 0.85

Then, if an attacker is using the *.rhosts* stealth attack at node E and not the *buffer overflow* vulnerability, then with the available values of B,C, D and E, the probability that .rhosts attack at node A was undertaken can be calculated by P(A/E, D,C,B).

$$\text{P(A/E, D,C,B)} = \frac{P(E,D,C,B,A)}{\sum P(E,D,C,B,A^{1})}$$

$$= \frac{P(E=Yes/C=Yes,B=Yes,A=Yes)*P(D=No/A=Yes)*P(A=Yes)}{\sum P(E=Yes/C=Yes,B=Yes,A^{1})*P(D=No/A^{1})*P(A^{1})}$$

$$= \frac{(0.15*0.7*0.1)}{(0.15*0.7*0.1)+(0.25*0.6*0.9)}$$

$$= 0.0721$$

The probability before was 0.1, but the inferred probability is 0.0721 based on the values of other variables. Thus the Bayesian networks help in identifying the attack paths that the attacker would probably take during the course of an attack.

Therefore, we document all the attack paths for a given resource and calculate the Bayesian probabilities of the root nodes of each attack path when the evidence regarding the leaf is available. For example, Table 2 describes probabilistic values for a given profile and attack paths. For a given profile P_i, we calculate the Least Square Error (LSE_i) for all attack paths with the available prior knowledge. This is carried out for all the profiles that are capable for carrying an attack. Hence, given an attack profile and a resource, all the probable attack paths that can lead to the exploitation of the resource can be inferred. Using this information, the risk associated with a resource is calculated.

Path	Skill	Tenacity	Cost	LSE_1	LSE_2	…..
1	0.072	0.33	..			
2						
….						

Table 2: Bayesian probabilities at the root node of attack path given the evidence at the leaf.

Step5->Optimizing the risk level: In a typical network, patching a vulnerability may impact other network elements. For example, after patching some exploits and changing the network configuration (e.g., moving the firewall to another location in the topology or changing the firewall rules, deploying Intrusion detection systems etc.), steps 1-4 need to be performed repeatedly for an optimum risk value**.** .Figure 5 shows the relation between behavior, risk, depth in the graph (relates to sequence of moves) and critical resources. Certain behaviors overlap regardless of the type of threat (e.g. corporate insiders may share some behaviors with outside espionage).

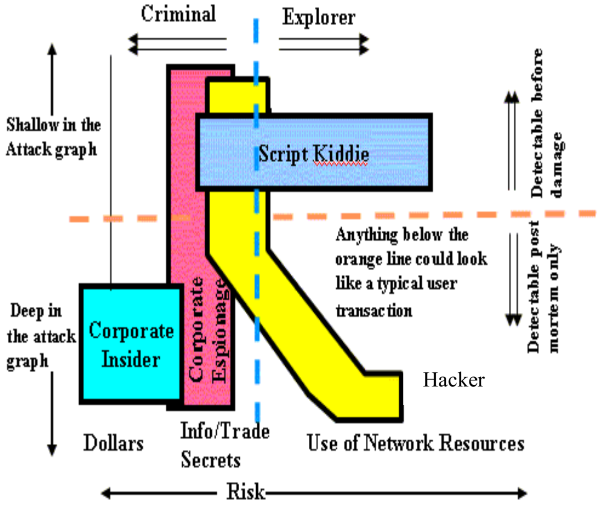

Figure: 5 Relation between risk, behavior and network configuration .

4. Conclusion

We have proposed a methodology for vulnerability analysis of a network based on attacker behavior. This analysis is based on the sequence of actions carried out by the attackers and their social attributes. We used attack graphs for representing all possible attacks on a critical resource in the network. We have described a five-step model of vulnerable device detection and risk estimation of a network using attack graphs and attack behavior. The creation of attack graphs helps us in identifying the possible attacks on a network component and formulated a mechanism through the use of multiple regression and Bayesian estimation to quantitatively analyze the attack graphs and derive the attack paths based on attacker attributes. In the final step, we propose the optimization of the network by patching the identified vulnerable devices or reconfiguration of network components for guaranteed security. Using this method along with a set of security policies can reduce the vulnerability of a network and its hosts to external attacks. Future work includes applying our method to real-world network configurations and testing the methodology on data collected during past attacks.

5. Bibliography

[1] Jim Yuill, S. Felix Wu, Fengmin Gong, and Ming-Yuh Huang, "Intrusion Detection for an on-going attack", RAID symposium, 1999.

[2] John Desmond, "Checkmate IDS tries to anticipate Hackers Actions", www.esecurityplanet.com/prodser, 12th June, 2003.

[3] Gary Jackson, "Checkmate Intrusion Protection System: Evolution or Revolution", Psynapse Technologies, 2003.

[4] Kall Loper, "The Criminology of Computer Hackers: A qualitative and Quantitative Analysis", Ph.D. Thesis, Michigan State University, 2000.

[5] Modern Intrusion Practicies, CORE security technologies,

[6] Know Your Ennnemy: Motives, The Motives and Psychology of the Black-hat Community, 27th June, 2000.

[7] Marc Rogers, "Running Head: Theories of Crime and Hacking", MS Thesis, University of Manitoba, 2003

[8] Christopher Wrobleski, "Computer Hacking and Intellectual Property,", Squad C-37, FBI, New York Office, 2003.

[9] Laura P. Swiler, Cynthia Phillips, David Ellis, and Stefan Chakerian, "Computer-Attack Graph Generation Tool", IEEE Symposium on Security and Privacy 2001.

[10] Andrew P. Morre, Robert J. Ellison, Richard C. Linger, "Attack Modeling for Information Security and Survivalility", Technical Note, CMU/SE1-2001-TN-001, March 2001.

[11] Oleg Sheyner, Joshua Haines, Somesh Jha, Richard Lippmann, Jeamnnette M. Wing, "Automated Generation and Analysis of Attack Graphs", IEEE Symposium on Security and Privacy, 2002.

[12] S. McQuade and D.K. Loper, "A Qualitative Examination of the Hacker Subculture Through Content Analysis of Hacker Communication", American Society of Criminology, November, 2002.

[13] Chandler. A., " Changing definition of hackers in popular discourse", International Journal of Sociology and Law, 24(2), 229-252, 1996.
Jasanoff. S., "A sociology of Hackers", The Sociological Review, 46(4), 757-780, 1998.

[14] Jasanoff. S., "A sociology of Hackers", The Sociological Review, 46(4), 757-780, 1998.

[15] Ian Rowley, "Managing In An Uncertain World: Risk Analysis And The Bottom Line", Systems Engineering Contribution to Increased Profitability, IEE Colloquium on , 31 Oct 1989