Risk Management Using Behavior Based Bayesian Networks

Ram Dantu and Prakash Kolan

Department of Computer Science,
University of North Texas
{Rdantu, 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). We extended this and 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 attackers (script kiddies, hackers, criminals and insiders).

1 Introduction

The increase in the size of the enterprise network is an ever-growing process. With the increase in number of hosts connected to the 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. Accurate vulnerability analysis require a deep understanding of failure and attack modes and their impact on each of the network components, and the knowledge of how these components interact with each other during normal as well attack modes of operation. For managing the security of a network, security engineers identify security holes by probing the network hosts, asses the risk associated with the vulnerabilities on the computer hosts and fix host vulnerabilities by using patches released by the vendors.

P. Kantor et al. (Eds.): ISI 2005, LNCS 3495, pp. 115 – 126, 2005.

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 its components. We see frequent release of patches from product vendors (Microsoft, IBM, HP) etc. to reduce the effect of vulnerability once it is reported. The product vendors, for the process of vulnerability assessment, focus on active prevention methodologies of closing the vulnerabilities before they are exploited. But this process of patching end hosts requires a great deal of human intervention, time and money. It involves frequent monitoring of end systems using a set of monitoring tools by the admin staff to identify and prevent intrusion. The situation worsens when the already present state of the art monitoring tools are not effective in identifying new vulnerabilities.

Risk management refers to process of making decisions that would help in minimizing the effects of vulnerabilities on the network hosts. In context of high exploit probability, risk management is a nightmare to plan with. And also, it is very difficult to identify new exploits and vulnerabilities. For many years security engineers have been doing risk analysis using economic models for the design and operation of risk-prone, technological systems([1], [3], [4], [6]) 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. We believe that integrating this research could improve the process of risk analysis. Many articles explain how intruders break into systems ([14], [15]). Companies like *Psynapse, Amenaza*, and *Esecurity* have built products using the behavior of intruders. 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 attempted in integrating risk analysis with attacker behavior. Jackson[4] introduces the notion of behavioral assessment to find out the intent behind the attack. The proposed Checkmate intrusion detection system distinguishes legitimate use from misuse through behavior intent. But this does not propose any detail on vulnerable device identification based on the assessed behavior. Rowley[17] 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. There is a need of integrating risk mitigation strategies with attack behavior to 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. Categories of hackers like novices, crackers and criminals have been defined. Each of the hacker groups has their own knowledge and motivation for carrying on the attacks. Rogers[16] proposed different categorizations of a hacker community and advices derivation of hacker profiles using intruder behavior. Yuill[1] profiles detection of an on-going attack by developing a profile of the attacker using the information he reveals about himself during his attacks. Kleen[9] developed a framework by reviewing existing methods and advances in a way that hackers are classified and profiled, with the goal of better understanding their values, skills and approaches to hacking. There are several works in the literature on the hacker profiles ([6], [7], [8]) but none of them tie the profiles to any exploits in the network. All the theories proposed account for the hacker behavior, but don't attempt to relate the reasons behind hacker behavior to exploits and vulnerability utilization.

On the other hand, attack graphs are beginning to be used to formalize the risk for a given network topology and exploits. Sheyner[12]attempts to model a network by constructing attack graph for the model using symbolic model checking algorithms. Moore[11] 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 [10] [11] [12] does not combine the behavior with these graph transitions.

Loper[5][13] 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). 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 attack trees are been increasingly formalized to be a model for representing 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. Attack graphs can be drawn to represent the sequence of network actions for exploiting each network resource and ultimately the whole network. We use attack graphs for calculating the vulnerability level and risk of a critical resource in a given network for different attacker profiles. There are five steps in our procedure. The five steps are repeatedly executed until optimum security is achieved. *Our hypothesis is that there is a relation between network actions and social behaviour attributes.*

3.1 Step 1: Creation of an Attacker Profile

The profile an attacker gives the expendable resources associated with the attacker. These resources can be any of cost, computer and hacking skills, tenacity, perseverance, motives like revenge, reputation etc. that the attacker would expend to exploit a vulnerability. Different attack profiles have different behavioral attribute values for attacker resources. For example, a corporate espionage has more money compared to a script kiddie who tries to hack for fun with little money. A corporate insider has more knowledge regarding the enterprise network topology compared to a hacker. One example for assigning relative attributes for a profile is for a hacker who has low level of funding (e.g., 0.2), medium level of skill (e.g., 0.6) and high level of tenacity (e.g., 0.8).

3.2 Step 2: Creation of Attack Graphs

An attack graph can be created using network topology, interconnection between hosts, and various vulnerabilities of each host ([10], [11], [12]). 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 Fig. 1] can be a sequence of events like overflow *sshd* buffer on host1(H1), overwrite *.rhosts* file on host2(H2) to establish *rsh* trust between H1 and H2, log-in using *rsh* from H1 to H2, and finally, overflow a local buffer on H2 to obtain root privileges. An attack graph can be shown as a causal graph with each node representing a cause and its child node representing an effect. Each node in the graph represents an event, and a path from root to leaf represents a successful attack.

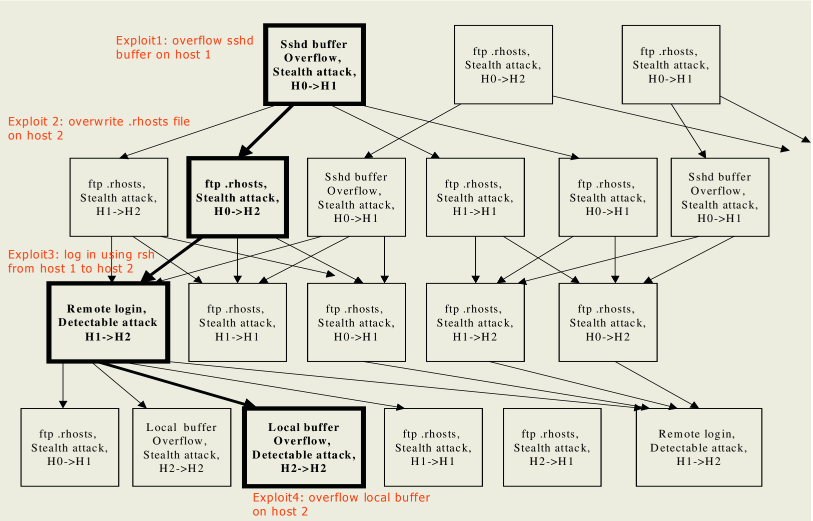

Exploit1: overflow sshd buffer on host 1
Sshd buffer Overflow, Stealth attack, H0->H1
ftp .rhosts, Stealth attack, H0->H2
ftp .rhosts, Stealth attack, H0->H1
Exploit 2: overwrite .rhosts file on host 2
ftp .rhosts, Stealth attack, H1->H2
ftp .rhosts, Stealth attack, H0->H2
Sshd buffer Overflow, Stealth 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

Fig. 1. An example attack graph with a chain of exploits

3.3 Step 3: Assigning Behavior Attributes to Attack Graph Nodes

For a given attacker profile, the nodes of the attack graph can be labelled using a set of behaviour attributes like: i) computer skills, ii) Hacking skills iii) tenacity iv) cost of attack v) techniques for avoiding detection etc. for carrying out the events represented by them. We are in midst of conducting a survey which would help in profiling attack behavioural aspects such as how different people would behave in attack scenarios given expendable resources at their disposal[20]. Using this, for a given profile, the attack graphs based on that profile are constructed by documenting all the attack paths that could be possibly executed by that profile. For example, Fig. 2 represents attack graphs constructed for two example profiles A & B respectively for three example attributes cost, skill and tenacity. These profile based attack graphs give a source of analysis for inferring profile based attacks.

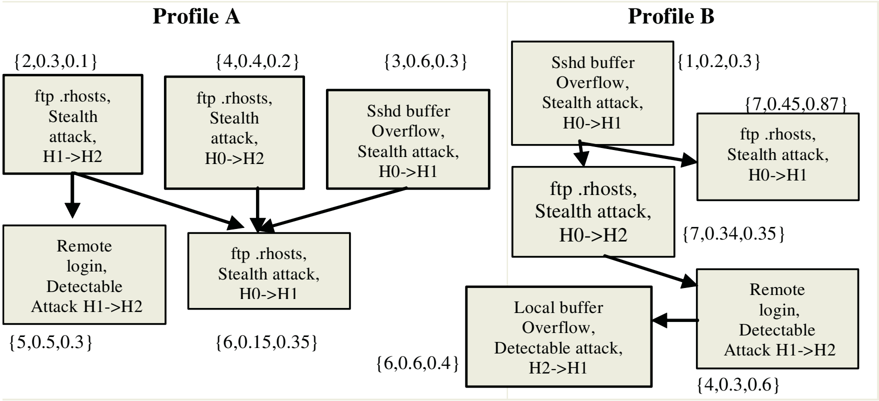

Profile A
{2,0.3,0.1}
ftp .rhosts, Stealth attack, H1->H2
{4,0.4,0.2}
ftp .rhosts, Stealth attack, H0->H2
{3,0.6,0.3}
Sshd buffer Overflow, Stealth attack, H0->H1
Remote login, Detectable Attack H1->H2
{5,0.5,0.3}
ftp .rhosts, Stealth attack, H0->H1
{6,0.15,0.35}
Profile B
Sshd buffer Overflow, Stealth attack, H0->H1
{1,0.2,0.3}
{7,0.45,0.87}
ftp .rhosts, Stealth attack, H0->H1
ftp .rhosts, Stealth attack, H0->H2
{7,0.34,0.35}
Remote login, Detectable Attack H1->H2
{4,0.3,0.6}
Local buffer Overflow, Detectable attack, H2->H1
{6,0.6,0.4}

Fig. 2. Attack paths based on profiles from Fig. 1 (3 Tuple{Cost, Skill, Tenacity})

3.4 Step 4: Risk Computation

In this step, a risk level for all the critical resources is calculated based on the set of paths, attributes and attacker type (e.g., script kiddie, hacker, corporate insider etc.). Bayesian networks based estimation can be 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.

3.4.1 Deriving Risk of an Attack Path

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. $\Theta = (f_1, f_2 \ldots fn)$ 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 Fig. 3(a) can be represented as in Fig. 3(b).

Table 1 describes all the behavioral attributes for each attack path and exploits. Given an attacker profile, all the attack paths that the attacker can move are described in this table. In this way we can derive the relationship between sequence of network actions and the social motives behind the attacker to carry out the attack.

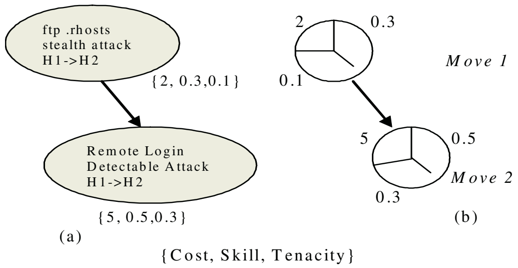


Fig. 3. An attack path of profile A in Fig. 2

Table 1. Probabilities for each move in Fig. 3

Path

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

3.4.2 Bayesian Networks for Risk Inference

A Bayesian network is a graphical model for showing probabilistic relationships among a set of variables (representing nodes) in a graph. Each node or variable is associated with a set of Probability Distribution Functions. Therefore the attack graphs can be modelled by reducing them to causal graphs and associate the nodes with probabilities. Using monitoring or intrusion detection systems, protocol state machines and traffic patterns observed between various states in the state machine, the initial subjective beliefs can be formulated. Any deviation from normal behaviour gives the evidence for calculating the posterior probabilities using Bayesian inference techniques. 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 distributions. 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 are patched to estimate the new risk level of the critical resources.

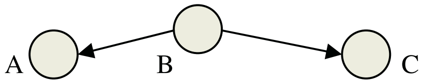


Fig. 4. Representing Conditional Probability

Fig. 4 is a simple Bayesian network with three nodes. The joint prob. distribution function for the figure can be shown to be P(A,B,C) i.e. P(A/B)*P(B)*P(C/B).

Therefore for set of variables in X = X_1, X_2,..........X_N, the prob. distribution would be

$$P(X_1,X_2,.....X_N) = \prod_{i=1}^{n} P(X_i / parent(X_i)) \tag{1}$$

3.4.3 Inference Based on Attacker Profiles

As shown in the previous sections the posterior probabilities of nodes converge depending upon the statistical dependencies existing due to various parent child relationships. Similarly, the attack graph for a given profile is initialized using expert knowledge and past observations[20]. Expert knowledge provides with profile information about all the probabilities of attack. The observations using expert knowledge can provide a basis for Bayesian probability estimation.

For example, consider one segment of attack graph shown in Fig. 1. Fig.5 represent the quantifying variables {cost, skill, tenacity} required by a profile to exploit the remote login and ftp .rhosts attacks. With the available initial knowledge, we compute the inferred probability for observed evidence at node E. Assume each of the nodes to be in two states "yes" or "no", and the probability values obtained from expert knowledge to the nodes are

P(A = yes) = 0.1, P(B = yes) = 0.35, P(C = yes) = 0.2
P(D=yes |A=yes)=0.3,   P(D=yes |A=no)=0.4
P(E=yes |C=yes ,B=yes ,A= no) = 0.25   P(E=yes |C=yes ,B=yes ,A=yes) = 0.15

Then, if an attacker is using the *.rhosts* stealth attack at node E, then prob. that .rhosts attack at node A was carried out can be calculated by P(A/E, D,C,B).

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

$$= \frac{P(E / C, B, A) * P(D / A) * P(A)}{\sum P(E / C, B, A^1) * P(D / A^1) * P(A^1)} \tag{2}$$

$$= \frac{(0.15 * 0.7 * 0.1)}{(0.15 * 0.7 * 0.1) + (0.25 * 0.6 * 0.9)} = 0.0721 \tag{3}$$

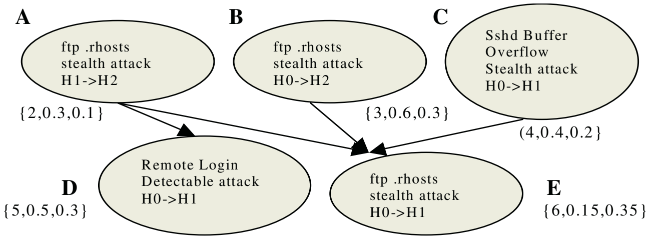


Fig. 5. A small Bayesian Causal graph

The probability before was 0.1, but the inferred probability is 0.0721 based on the values of other variables. For a given resource, we document all attack paths and calculate Bayesian probabilities of the root nodes of each attack path when the evidence regarding the leaf is available. Tab. 2 describes inferred probabilistic values for a given profile and attack path AE of Fig. 5. This procedure is carried out for all attack paths and profiles that are capable for carrying out an attack. Hence, for a given resource, all probable attack paths that can lead to the exploitation of it can be inferred.

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

Path	Skill	Tenacity	Cost	…	…	…	…
1	0.072	0.33	1.82				
2							
….							

3.4.4 Relating Risk, Behavior and Penetration

As we described before we believe that sequence of network actions carried out by an attacker relate to social behaviour. We attempt to derive the relation between vulnerability of a given resource and the penetration an attacker can achieve in exploiting the network. This can be achieved by defining the probability of each event in the attack path and inferring the posterior probability given evidence at a node, usually the leaf node i.e. the node representing the final event for a successful attack. Fig. 6 is a part of an attack graph of Fig. 1 and the prob. of the nodes are represented using Conditional Probability Tables (CPT). The CPT tables give the probability of nodes given the value of its parents. Assume each node to be in two states "yes" or

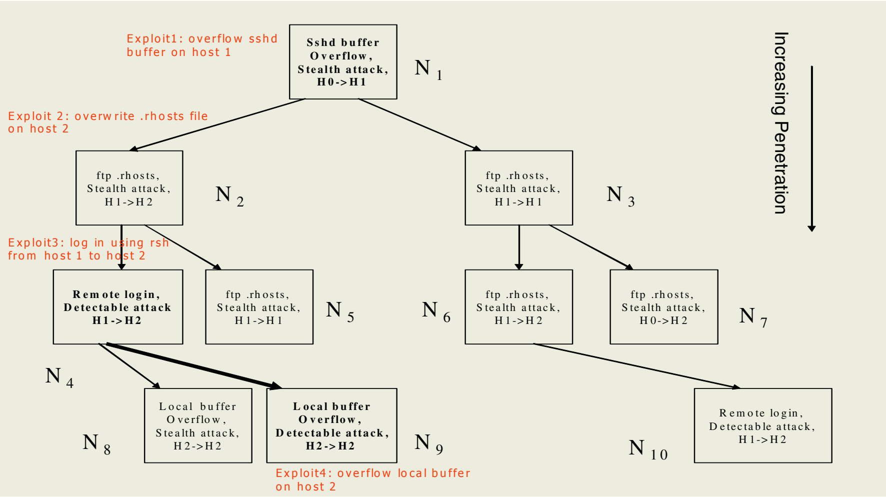

Exploit1: overflow sshd buffer on host 1
Sshd buffer Overflow, Stealth attack, H0->H1
N 1
Increasing Penetration
Exploit 2: overwrite .rhosts file on host 2
ftp .rhosts, Stealth attack, H1->H2
N 2
ftp .rhosts, Stealth attack, H1->H1
N 3
Exploit3: log in using rsh from host 1 to host 2
Remote login, Detectable attack H1->H2
ftp .rhosts, Stealth attack, H1->H1
N 5
N 6
ftp .rhosts, Stealth attack, H1->H2
ftp .rhosts, Stealth attack, H0->H2
N 7
N 4
Local buffer Overflow, Stealth attack, H2->H2
Local buffer Overflow, Detectable attack, H2->H2
N 8
N 9
N 10
Remote login, Detectable attack, H1->H2
Exploit4: overflow local buffer on host 2

Fig. 6. Example Sub-Attack Graph from Fig. 1

"no". Representing Node 1 as N_1, Node 2 as N_2 etc. and probability of Node X as $P(N_X)$. For the four different profiles Corporate Insider, Corporate espionage, hacker and script kiddie, and five nodes in analysis N_1, N_2, N_4, N_8 *and* N_9, the CPT tables would be as in Tab 3a and Tab 3b. (*In reality, initialisation of CPT tables is carried out by analysing a statistical data from an interview or a survey*[20]).

Table 3a. Prob. of nodes N_1, N_2 ,N_4 of Fig. 6 given their parents (N1 does not have a parent)

Probability Profile	$P(N_1)$	$P(N_2)$ given N_1 = yes	$P(N_2)$ given N_1 = no	$P(N_4)$ given N_2 = yes	$P(N_4)$ given N_2 = no
Corp. Insider	0.8	0.75	0.82	0.85	0.70
Corp. Espionage	0.62	0.65	0.71	0.67	0.63
Hacker	0.6	0.7	0.31	0.51	0.46
Script Kiddie	0.4	0.52	0.36	0.48	0.32

Table 3b. Prob. of nodes N_8 and N_9 of [Fig. 8] given their parents

Probability Profile	$P(N_8)$ given N_4 = yes	$P(N_8)$ given N_4 = no	$P(N_9)$ given N_4 = yes	$P(N_9)$ given N_4 = no
Corp. Insider	0.71	0.83	0.69	0.77
Corp. Espionage	0.7	0.65	0.72	0.64
Hacker	0.3	0.57	0.52	0.63
Script Kiddie	0.62	0.41	0.44	0.62

The values given by the CPT tables describe the behaviour of each of the profiles. For example, a corporate insider who is in the enterprise has more profound knowledge of the corporate network topology and thus the risk posed by the corporate insider is more compared to a corporate espionage. The probabilities of the hacker are understandingly less because a hacker tries to compromise the network resources and the risk associated with this is much less compared to corporate espionage and an insider. Script Kiddie has the least skill, tenacity and knowledge of an enterprise network and hence with limited attributes tries to hack into the network by downloading some network scanning and monitoring tools.

Table 4. Bayesian Inference for directly affected nodes due to evidence at node N_9. N_1 represents minimum and N_4 the maximum penetration

Profile	$P(N_1)$	$P(N_2)$	$P(N_4)$	$P(N_8)$
Corp. Insider	0.8002	0.7609	0.7975	0.7343
Corp. Espionage	0.6199	0.6738	0.6829	0.6841
Hacker	0.5991	0.5416	0.4395	0.4513
Script Kiddie	0.3980	0.4112	0.3102	0.4751

In the figure, if evidence regarding the happening of the event represented by Node 9 is known to happen, nodes N_1, N_2, N_4, N_8 are directly inferred. For example, what is the probability of a hacker penetrating through N_I-N_2-N_4-N_9 given an event that N_9 is attacked. The inferred probabilities of the nodes directly affected by this evidence using our analytical model (See Sec 3.4.3) are given in Tab. 4. Network Penetration is given by the extent to which the attacker would be able to penetrate i.e., the level of the graph on the attack path.

Fig. 7 represents the relationship between risk, behaviour and network penetration for all the profiles for a given attacker skill level. In reality, the CPT values will be a range instead of single value. The values for two profiles are given in Table 5a and Tab. 5b (α/β for each node represents the range of probabilities of given profile in which the prob. for all attributes of the profile fall into[5]). The range of probabilities of the nodes that are directly inferred by the event at node N_9 are given in Tab 6.

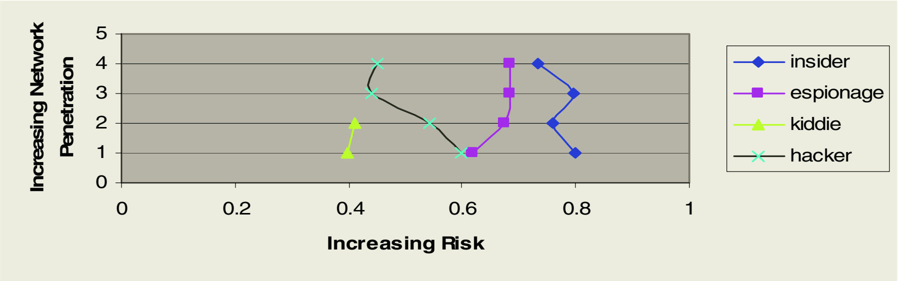


Fig. 7. Relating risk, behavior and penetration for an attribute of all profiles

Table 5a. For given two profiles, range of probabilities of nodes $N_{1,}$ N_2 and N_4 of Fig. 8

Profile	$P(N_1)$	$P(N_2)$ given N_1 = yes	$P(N_2)$ given N_1 = no	$P(N_4)$ given N_2 = yes	$P(N_4)$ given N_2 = no
Corp. Insider	0.8/0.92	0.75/0.87	0.82/0.94	0.85/0.97	0.70/0.82
Script Kiddie	0.4/0.65	0.52/0.71	0.36/0.56	0.48/0.73	0.32/0.67

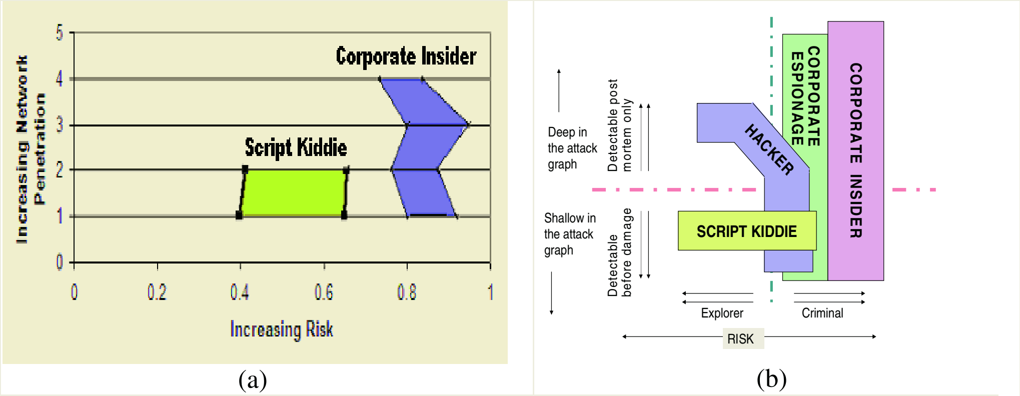
Table 5b. For given two profiles, range of prob. of nodes N_8 , N_9 of Fig. 8 given their parents

Profile	$P(N_8)$ given N_4 = yes	$P(N_8)$ given N_4 = no	$P(N_9)$ given N_4 = yes	$P(N_9)$ given N_4 = no
Corp. Insider	0.71/0.83	0.83/0.94	0.69/0.82	0.77/0.89
Script Kiddie	0.62/0.84	0.41/0.63	0.44/0.68	0.62/0.81

Table 6. Inferred prob. range of all the attributes for the given two profiles for directly affected nodes N1, N_2, N4, and N8. N_1 represents minimum and N_4 the maximum penetration

Profile	$P(N_1)$	$P(N_2)$	$P(N_4)$	$P(N_8)$
Corporate Insider	0.8/0.92	0.76/0.874	0.7975/0.974	0.734/0.835
Script Kiddie	0.398/0.649	0.411/0.655	0.310/0.672	0.475/0.771

From Tab. 6, we infer that for all attributes, the probability of node N_1 falls in the range [0.8, 0.92] for the corporate insider and in the range [0.398, 0.649] for the script kiddie. For the given two profiles and two attributes, the relation between the risk, behaviour and penetration looks as in Fig. 8(a). Fig. 8(a) can be extrapolated for all the four profiles and attributes, and can be shown as in Fig. 8(b). Fig. 8(b) shows the relation between behaviour, risk, depth in the graph (relates to sequence of moves) and critical resources. Certain behaviours overlap regardless of the type of threat (e.g. corporate insiders may share some behaviour with outside espionage).



(a) (b)

Fig. 8. Relation between risk, behavior and network penetration

3.5 Step 5: Optimizing the Risk Level

In a typical network, patching 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.), the steps (Sec 3.1 to 3.4) outlined need to be performed repeatedly for an optimum risk value**.** This estimated risk value would help in processes like patch management and penetration testing etc.

4 Conclusion

Our *hypothesis* is that there is a relation between sequence of network actions and attacker behaviour and that the behaviour can be used for network risk analysis.. This analysis is based on sequence of actions carried out by an attacker and his 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 attacker behaviour. The creation of attack graphs helps us in identifying the possible attacks on a network component. We formulated a mechanism through Bayesian estimation to quantitatively analyze the attack graphs and derive attack paths based on attacker attributes. Risk computation is carried out using Bayesian probability distributions of a set of identifiers at each node in an attack graph. This gives a more appropriate prediction of risk and threat identification. Finally we suggest optimizing the network by patching the identified vulnerable devices or reconfiguration of network components till a comfortable security level is achieved. Using this methodology, a set of security policies can be formulated to 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.

References

1. Jim Yuill, J., Wu, S.F., Gong, F., Ming-Yuh H.: “Intrusion Detection for an on-going attack”, RAID symposium.
2. Scheiner, B.: “Attack Trees: Modeling Security Threats”, Dr. Dobb’s Journal Dec 99.
3. Desmond, J.: “Checkmate IDS tries to anticipate Hackers Actions”, www.esecurityplanet.com/prodser, 12th June, 2003.
4. Jackson, G.: “Checkmate Intrusion Protection System: Evolution or Revolution”, Psynapse Technologies, 2003.
5. Loper, K.: “The Criminology of Computer Hackers: A qualitative and Quantitative Analysis”, Ph.D. Thesis, Michigan State University, 2000.
6. Modern Intrusion Practicies, CORE security technologies,
7. Know Your Ennnemy: Motives, The Motives and Psychology of the Black-hat Community, 27th June, 2000.
8. Rogers, M.: “Running Head: Theories of Crime and Hacking”, MS Thesis, University of Manitoba, 2003
9. Kleen, L.: “Malicious Hackers: A Framework for Analysis and Case Study”, Ph.D. Thesis, Air Force Institute of Technology, Ohio, 2001.
10. Swiler, L.P., Phillips, C., Ellis, D., Chakerian, S.: “Computer-Attack Graph Generation Tool”, IEEE Symposium on Security and Privacy 2001.
11. Moore, A.P., Ellison, R.J., Linger, R.C.: “Attack Modeling for Information Security and Survivalility”, Technical Note,CMU/SE1-2001-TN-001, March 2001.
12. Sheyner, O., Joshua Haines, J., Jha, S., Lippmann, R., Wing, J.M.: “Automated Generation and Analysis of Attack Graphs”, IEEE Symposium on Security and Privacy, 2002.
13. McQuade S., Loper, D.K.: “A Qualitative Examination of the Hacker Subculture Through Content Analysis of Hacker Communication”, American Society of Criminology, November, 2002.
14. Chandler, A.: “Changing definition of hackers in popular discourse”, International Journal of Sociology and Law, 24(2), 229-252, 1996.
15. Jasanoff, S.: “A sociology of Hackers”, The Sociological Review, 46(4), 757-780, 1998.
16. Rogers, M.: “ A New Hacker’s Taxonomy” University of Manitoba
17. Rowley, I.: “Managing In An Uncertain World: Risk Analysis And The Bottom Line”, Systems Engineering Contribution to Increased Profitability, IEE Colloquium on , 31 Oct 1989
18. WINBUGS - http://www.mrc-bsu.cam.ac.uk/bugs
19. HUGIN DEMO - http://www.HUGIN.com/
20. Dantu, R., Loper, K., Kolan, P.: Survey of Behavior Profiles, University of North Texas Internal Document 2004.