Classification of Attributes and Behavior in Risk Management Using Bayesian Networks

Ram Dantu, Prakash Kolan, Robert Akl, Kall Loper

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 network component vendors, system administrators require a barrage of tools for analyzing the risk due to vulnerabilities in those components. In addition, criticalities in patching some end hosts 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 keeping in view the everyday emerging new vulnerabilities. We hypothesize that sequence of network actions by attackers depends on their social and attack profile (behavioral resources such as skill level, time, and attitude). To estimate the types of attack behavior, we surveyed individuals for their ability and attack intent. Using the individuals' responses, we determined their behavioral resources and classified them as having opportunist, hacker, or explorer behavior. The profile behavioral resources can be used for determining risk by an attacker having that profile. Thus, suitable vulnerability analysis and risk management strategies can be formulated to efficiently curtail the risk from different types of attackers.**

Index Terms—**Attack Graphs, Behavior, Risk Management**

I. Introduction

With the increase in the number of hosts connected to the network, there is always a mounting risk for protecting computers from outside attacks. In addition to this, improper configuration of network hosts results in host vulnerabilities because of which the hosts are susceptible to outside attacks. For managing the security of a network, security engineers identify security holes by probing the network hosts, asses the risks associated with the vulnerabilities on the computer hosts and fix host vulnerabilities using patches released by the vendors.

We see frequent releases of patches from product vendors (Microsoft, IBM, and HP). 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. This process of patching end hosts requires a great deal of human intervention, time and money. The situation worsens when the already present state of the art monitoring tools are not effective in identifying new vulnerabilities. These everyday emerging vulnerabilities provide different attack probabilities depending on the type of attacker profile (e.g., script kiddie, hacker).

A considerable amount of work has been reported on attacker profiles and risk management on an individual basis. Jackson[4] introduces the notion of behavioral assessment to find out the intent behind the attack. 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 revealed about themselves during the attacks. There are several works in the literature on hacker profiles [5, 6, 9] but none of them tie the profiles to any exploits in the network. All the theories proposed account for the hacker behavior. To our knowledge, no work has been reported on integrating behavior-based profiles with sequence of network actions for computing the vulnerability of resources.

On the other hand, attack graphs are beginning to be used to formalize the risks of a given network topology and exploits. Sheyner[13] attempts to model a network by constructing an attack graph using symbolic model checking algorithms. Moore[12] 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 their desire of exploiting the host and ultimately the network. However, current research like [11-13] does not combine the behavior and risk management with these graph transitions.

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, 5] using attack profiles. A considerable amount of research has been reported on developing profiles of an attacker based on the evidence left behind during an attack. 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. This paper marries profiling with chain of exploits, and detects highly vulnerable resources in the network. Our work uses the theory from criminology, statistical analysis, behavioral-based security, and attack graphs for computing risk levels of network resources.

II. Attack Graphs

Attack graphs or attack trees have been increasingly formalized to be a model for representing system and network security based on various attacks. An attack graph can be created using network topology, interconnection between hosts, and various vulnerabilities of each host [11, 12, 13]. These attack graphs represent the sequence of network actions for exploiting each network resource and ultimately the whole network. Consider for example a network hosting ftp, ssh, and database services as shown in Fig. 1.

1-4244-1330-3/07/$25.00 ©2007 IEEE.

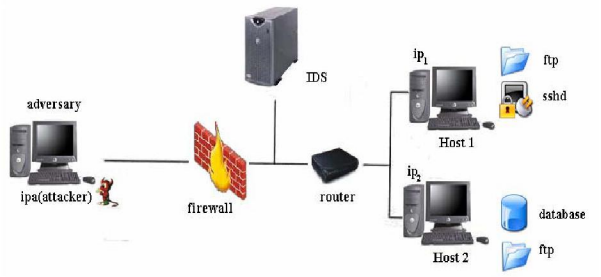


Fig. 1. Network Diagram

For the network diagram shown in Fig 1, we can construct an attack graph that represents all possible attacks as shown in Fig 2. Each node in the graph represents an event, and a path from root to leaf represents a successful attack.

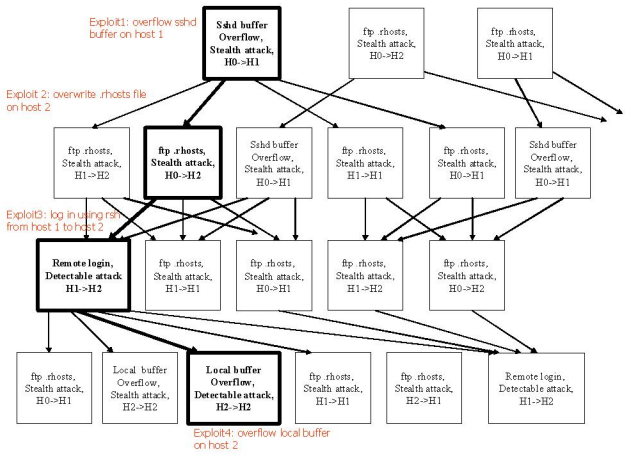


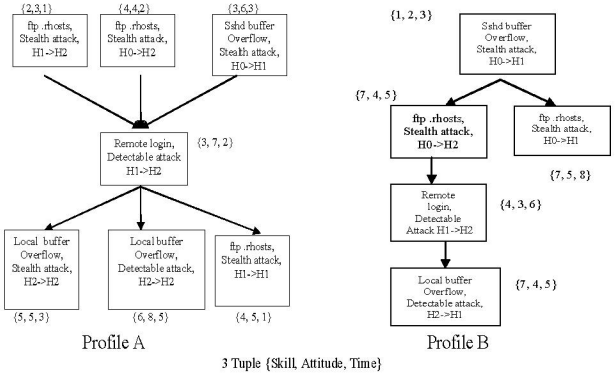
Fig. 2. An example attack graph with a chain of exploits

For each network action given in Fig 2, the attack probability is different for different types of attackers or attacker profiles.

III. ATTACKER PROFILES

An attacker profile gives the expendable resources associated with the attacker. These resources can include cost, computer and hacking skills, attitude, time, tenacity, perseverance, and motives like revenge and reputation that the attacker would expend to exploit a given 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 on a scale of 1-10 for a hacker is medium level of skill (e.g., 6), medium level of attitude (e.g., 5) and high level of time (e.g., 8).

For a given attacker profile, the nodes of the attack graph can be labeled using a set of behavior attributes like: i) computer skills, ii) hacking skills, iii) time, iv)attitude, and v) techniques for avoiding detection. We conducted a survey that helps in defining behavior attributes for different profiles (see Section V). Using the attribute values, we can derive profile based attack graphs that represent all attack paths that could be possible executed by that profile. These profile based attack graphs give a source of analysis for inferring profile based attacks. For example, Fig. 3 represents attack graphs constructed for two example profiles A & B respectively for three example attributes skill, attitude, and time.



3 Tuple {Skill, Attitude, Time}

Fig. 3. Attack paths based on profiles from Fig. 2

Using the profile based attack graphs, we can compute the risk level associated with that profile. This risk level represents the risk based on given network topology and profile behavior.

IV. RISK MANAGEMENT

Risk management refers to the process of making decisions that would help in minimizing the effects of vulnerabilities on network hosts. It can be very helpful to have an adaptive risk computation mechanism that helps in computing risk levels of network components during patch management and penetration testing processes for different attacker profiles.

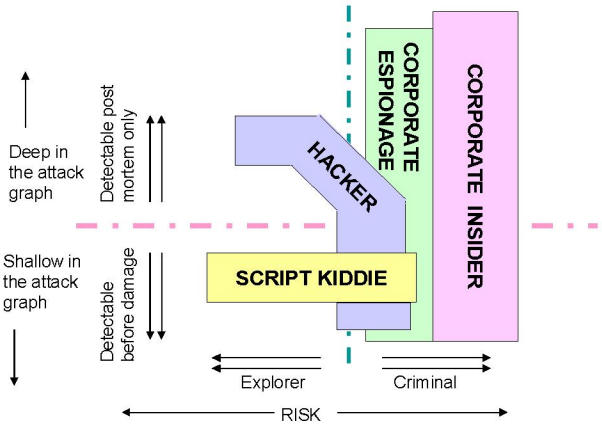


Fig 4. Relation between risk, behavior, and network penetration

However, the amount of risk for the network components is different for different attacker profiles. We have discussed an adaptive risk computation and network penetration inference mechanism using Bayesian estimation techniques in [7, 8]. In this paper, we present a method based on a survey for defining behavior attributes of attacker profiles such as opportunists, hackers and explorers. Using the attribute values and the above risk computation and network penetration inference mechanism, we can relate risk of network components to network penetration and attacker behavior as shown in Fig 4.

V. SURVEY AND CLASSIFICATION

The prime objectives of conducting the survey are to:

1. Define resource attribute values of different profiles for the network actions given in Fig 3.
2. Analyze the relationship between behavior and network actions for reducing profile based attacks.
3. Understand the relationship between risk, network penetration and behavior profiles.

All the participants had to take a survey with questions divided into two parts. The two parts are described in detail as follows:

Part I of the Survey (Network actions):

The 14 questions [17] represent network actions that are concerned with day-to-day operations for computer network penetration. The responses to these network actions can be used for inferring the resources that are required to carry out the network action. We identified three resources: skill (attacker's ability), attitude (attack intent) and time (for the attacker to carry out the network action).

For assigning attribute values for skill, attitude, and time for the survey participant, we analyzed the responses to the survey. Each option for a given question is assigned a score for skill, attitude and time. The sum of the scores of the selected options by the participant gives the amount of skill, attitude, and time available with the participant.

Part II of Survey (Behavior profiles):

The second part of the survey consists of 32 questions [17]. The responses to these questions can be used to infer the behavior of the survey participant. In this survey, we assumed that there are three kinds of people who attempt to penetrate or compromise network resources. These are people with hacker-behavior, opportunist-behavior, and explorer-behavior. People differ in the mindset for attack behavior. For example, a person with opportunist behavior may intend to be isolated and hidden, whereas a person with explorer behavior is someone who believes in open door principles.

For classifying the participant into one of the three profiles, we assigned a score to each option for every question in Part II of the survey. The sum of the selected option scores by the participant to all the 32 questions is used to classify the participant into one of the three profiles.

VI. RESULTS AND CONCLUSION

Using the responses given in Part II, we divided the participants into three groups: hacker, opportunist, and explorer-behavior. We analyzed the values of skill, attitude, and time for the people in the three groups based on Part I of the survey. For inferring these values, the median (or most probable responses) of all the people classified into one group are taken into consideration. A normalized set of values in the range of 1-10 for the people in three groups are given in Table I. From the computed score, we observed the following:

- Participants classified into the opportunist-behavior profile have higher attitude, skill and time compared to participants belonging to other profiles.
- Participants with hacking behavior had intermediate values of skill, attitude, and time among all the participants.
- Participants classified into the explorer-behavior profile have the least amount of attitude among the participants of all the three profiles.

These observations can be clearly seen in Fig. 5. The attribute values of skill and attitude are higher for opportunists followed by hackers and then by explorers. However, it can be observed that explorers have high values of attributes for question #10, which inquires about frequency with which the participants logs into a system as "root" or admin user. More explorers use "root" user to login compared to opportunists and hackers as they tend to believe in open door policies.

In Table II, we sorted the sum of scores for attribute values in a descending order of attitude, time (if any other participant have same value of attitude), and then by skill (if there are any participants with same skill and attitude). Based on the above sort order, we observed that all the higher order participants are the people with opportunist-behavior followed by people with hacking and explorer behavior. This order justifies the classification that high attitude are the ones with opportunist behavior and the ones with explorer behavior have lower values of attitude.

In, conclusion, we hope our research will help in better understanding the relationship between the attributes (such as skills, time, and attitude) for attacker profiles (such as hackers, opportunists, and explorer behavior) with risk and network penetration.

TABLE I
ATTRIBUTE VALUES OF NETWORK ACTIONS FOR THE BEHAVIOR PROFILES

Profile	Hacker-Behavior			Opportunist-Behavior			Explorer-Behavior		
Question	Skill	Attitude	Time	Skill	Attitude	Time	Skill	Attitude	Time
1	9.198	8.431	9.043	10.000	8.796	10.000	8.221	8.686	7.913
2	8.346	7.628	7.913	10.000	8.796	10.000	5.414	6.058	4.957
3	9.198	8.431	9.043	10.000	8.796	10.000	6.817	7.372	6.435
4	8.346	7.628	7.913	10.000	8.796	10.000	4.010	4.745	3.478
5	7.494	6.825	6.783	6.917	7.263	6.087	5.414	6.058	4.957
6	7.494	6.825	6.783	10.000	8.796	10.000	4.010	4.745	3.478
7	7.494	6.825	6.783	7.945	7.774	7.391	5.414	6.058	4.957
8	7.494	6.825	6.783	10.000	8.796	10.000	4.010	4.745	3.478
9	7.494	6.825	6.783	6.917	7.263	6.087	5.414	6.058	4.957
10	9.198	8.431	9.043	7.945	7.774	7.391	9.624	10.000	9.391
11	7.494	6.825	6.783	6.917	7.263	6.087	4.010	4.745	3.478
12	7.494	6.825	6.783	6.917	7.263	6.087	4.010	4.745	3.478
13	6.642	6.022	5.652	6.917	7.263	6.087	4.010	4.745	3.478
14	6.642	6.022	5.652	5.890	6.752	4.783	4.010	4.745	3.478

REFERENCES

[1] J. Yuill, S. F. Wu, F. Gong, H. Ming-Yuh, "Intrusion Detection for an on-going attack", *RAID symposium*.

[2] B. Scheiner, "Attack Trees: Modeling Security Threats", *Dr. Dobb's Journal*, Dec 1999.

[3] J. Desmond, "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] Modern Intrusion Practices, CORE security technologies.

[6] Know Your Enemy: Motives, The Motives and Psychology of the Black-hat Community, http://www.honeynet.org/papers/motives/, June, 2000.

[7] R. Dantu and P. Kolan, "Risk Management using Behavior Based Bayesian Networks", Lecture Notes in Computer Science, 2005

[8] R. Dantu, K. Loper and P. Kolan, "Risk Management Using Behavior Based Attack Graphs", IEEE International Conference on Information Technology (ITCC), April 2004

[9] M. Rogers, "Running Head: Theories of Crime and Hacking", *MS Thesis*, University of Manitoba, 2003.

[10] L. Kleen, "Malicious Hackers: A Framework for Analysis and Case Study", *Ph.D. Thesis*, Air Force Institute of Technology, Ohio, 2001.

[11] L. P. Swiler, C. Phillips, D. Ellis, S. Chakerian, "Computer-Attack Graph Generation Tool", *IEEE Symposium on Security and Privacy* 2001.

[12] A. P. Moore, R. J. Ellison, R. C. Linger, "Attack Modeling for Information Security and Survivalility", *Technical Note,CMU/SE1-2001-TN-001*, March 2001.

[13] O. Sheyner, J. Joshua Haines, S. Jha, R. Lippmann, J. M. Wing, "Automated Generation and Analysis of Attack Graphs", *IEEE Symposium on Security and Privacy*, 2002.

[14] A. Chandler, "Changing definition of hackers in popular discourse", *International Journal of Sociology and Law*, 24(2), 229-252, 1996.

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

[16] M. Rogers, " A New Hacker's Taxonomy" University of Manitoba.

[17] R. Dantu, K. Loper, P. Kolan, Survey of Behavior Profiles, University of North Texas Internal Document (http://secnet.csci.unt.edu/risk), 2004

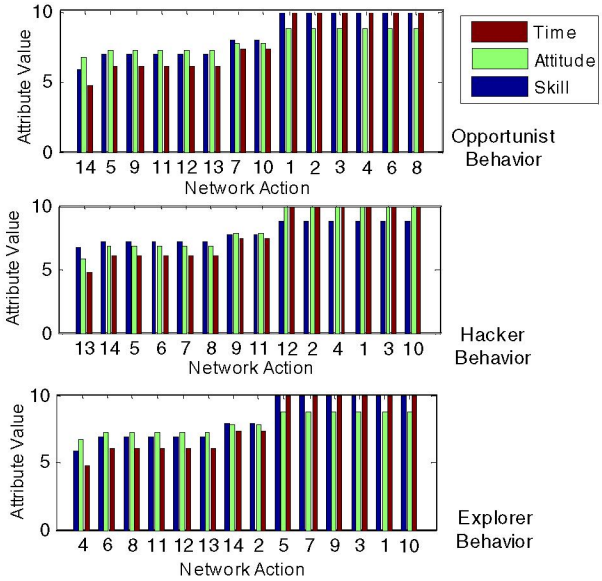


Fig. 5. Results of the survey and classification of participants

TABLE II
ATTRIBUTE VALUES AND BEHAVIOR CLASSIFICATION OF SURVEY PARTICIPANTS

Participant ID	Attitude	Skill	Time	Behaviour Classification	Participant ID	Attitude	Skill	Time	Behaviour Classification
13	10.000	10.000	9.559	Opportunist	24	6.232	7.262	6.618	Hacker
27	9.855	9.405	10.000	Opportunist	3	6.232	7.738	6.324	Hacker
45	9.420	8.333	8.824	Opportunist	34	6.087	7.381	7.941	Hacker
50	8.696	8.452	9.412	Opportunist	40	6.087	7.024	7.353	Hacker
32	8.406	8.929	7.794	Opportunist	53	6.087	7.143	5.882	Hacker
26	8.261	8.690	8.235	Opportunist	23	5.942	7.024	9.706	Hacker
4	8.261	7.381	6.618	Opportunist	58	5.942	6.667	7.647	Hacker
43	7.971	8.452	7.500	Opportunist	39	5.942	6.548	6.029	Hacker
10	7.971	7.857	6.765	Opportunist	48	5.652	6.905	6.765	Hacker
57	7.826	8.571	7.647	Opportunist	46	5.507	6.905	7.500	Hacker
7	7.536	7.738	8.088	Opportunist	59	5.507	6.190	6.029	Hacker
25	7.536	8.333	7.353	Opportunist	38	5.507	6.071	5.735	Explorer
30	7.391	8.214	8.088	Opportunist	51	5.362	6.548	7.941	Hacker
29	7.246	8.214	8.235	Opportunist	56	5.362	6.310	6.765	Hacker
33	7.246	7.738	6.912	Opportunist	42	5.362	6.310	6.471	Hacker
6	7.246	7.619	6.618	Opportunist	2	5.072	7.024	6.765	Hacker
49	7.101	7.857	7.794	Opportunist	12	5.072	6.071	6.324	Explorer
20	6.957	7.619	8.235	Opportunist	5	4.928	5.595	6.471	Explorer
1	6.957	7.500	6.029	Opportunist	28	4.928	6.190	5.441	Hacker
52	6.667	7.500	8.382	Opportunist	9	4.783	5.833	7.500	Explorer
18	6.667	7.262	6.765	Opportunist	54	4.783	4.762	5.294	Explorer
21	6.522	7.738	8.529	Opportunist	31	4.638	5.714	6.176	Explorer
19	6.522	6.190	6.324	Opportunist	55	4.638	5.238	5.588	Explorer
37	6.522	6.905	5.882	Opportunist	15	4.348	5.833	5.588	Explorer
14	6.377	6.905	7.353	Opportunist	36	4.348	5.357	5.000	Explorer
11	6.377	7.500	7.206	Opportunist	41	4.058	5.357	5.294	Explorer
17	6.377	7.500	6.324	Opportunist	35	4.058	5.714	5.147	Explorer
47	6.232	7.500	8.235	Hacker	44	3.768	4.762	4.559	Explorer
8	6.232	6.429	7.647	Hacker	22	3.478	3.810	4.706	Explorer
16	6.232	6.071	7.059	Hacker					