December 2004

Empirical Test of Hacking Framework: An Exploratory Study

Alberto Bento
University of Baltimore

Regina Bento
University of Baltimore

Empirical Test of Hacking Framework: An Exploratory Study

Al Bento
University of Baltimore
abento@ubalt.edu

Regina Bento
University of Baltimore
rbento@ubalt.edu

ABSTRACT

This exploratory study is an empirical test of a model based on a hacking framework. Variables were measured using non-reactive, secondary data obtained from sixty months of official statistical data, instead of relying on self-reports and surveys. Using stepwise regression, we found support for several of the model predictions. Reconnaissance was positively related to the vulnerability represented by increased Broadband access. Reconnaissance seems to lead to Malicious Code. There was support for escalation of privilege, as Root Compromise was related to User Compromise. There was also support for the idea that hacker frustration at failing to gain control of a resource may lead to Denial of Service attacks (DoS was negatively related to Root Compromise). Environmental variables (Broadband and Number of hosts) are positively related to each other. The study has potentially significant implications for research and practice.

Keywords

Hacking framework, empirical test, security, network, Internet

INTRODUCTION

There is widespread public concern with network and Internet security, but empirical research in this area is only in its early stages. Most empirical work on computer security predates the explosion of the World Wide Web in the mid-1990's (Bookholdt, 1989; Loch, Carr & Warkenting, 1992; Straub & Nance, 1990), and thus fails to take into consideration the new dimensions that the Web added to computing security. This paper represents an attempt to explicitly consider those new dimensions, by proposing and empirically testing a model based on a hacking framework.

Networks and the Internet are decades old, but it was the advent of the World Wide Web that made them pervasive in businesses and homes. The exponential growth of the Web has meant that the Internet poses an ever-increasing security threat (Straub & Welke, 1998). Whereas in the past security professionals believed that most attacks on computers and networks came from inside the organization, outsiders are now considered to be the biggest threat (Pfeegler and Pfeegler, 2002). There was a significant growth in computer security incidents, and the CERT Coordination Center documented that incidents reported increased from 21,756 in 2000 to 137,529 in 2003 (CERT/CC, 2003). Alarming trends include a continuous increase in the speed and sophistication of attack tools, faster discovery of vulnerabilities, increasing permeability of firewalls, increasingly asymmetric threat, and increasing threat from infrastructure attacks (CERT/CC, 2002). The 2003 CSI/FBI survey found that 75% of the organizations in the sample had detected computer security breaches leading to financial losses (Richardson, 2003). In spite of the difficulties involved in measuring the costs of cyber crime, there is evidence that those costs are substantial (Garg et al., 2003) and may be growing at yearly rates of about 200% (Lukasik, 2000). These numbers may actually underestimate the phenomenon, given the tendency for cyber crime to be underreported (Bagchi & Udo, 2003).

The increased magnitude of the problem of network and Internet security has not been accompanied by a proportional increase in empirical research. Security breaches have received a lot of media attention (e.g., the hoopla surrounding Melissa, Nimda, etc.), and the trade literature offers substantial information about hacking methods, techniques, tools and countermeasures (McClure, Scambray & Kurtz, 2001). The recent academic literature is mostly limited, however, to case studies about specific incidents or organizations (e.g., Straub & Welke, 1998) and analytical studies based on data from surveys of self-reports of attacks, such as Bagchi and Udo's (2003) modeling of the growth of computer and Internet security breaches. A notable exception is an analysis of security incidents on the Internet that used data reported to CERT/CC (Howard, 1997).

In this paper we draw from a hacking framework to develop and test, in an exploratory study, a model of the variables related to the steps involved in hacking attacks. The following sections present an overview of a hacking framework, the model we developed to test it, and the research questions and hypotheses inspired by the model. Next comes a discussion of the data collection strategy, which used surrogate measures based on official, publicly available statistics from the Federal Computer

Incident Response Center (FCIRC), the Federal Communications Commission (FCC) and Netcraft, instead of the usual surveys of self-reports. This is followed by an analysis of the results and a discussion of the implications of this exploratory study for research and practice.

HACKING FRAMEWORK

The model developed and tested in this study is based on a framework for understanding the steps involved in hacking attacks. The framework includes elements which have been widely used as a basis for the development of practical tools for prevention and defense against hacking attacks (Bento, 2003; Howard, 1997; Howard and Longstaff, 1998; McClure et al., 2001; Panko, 2003; Pfleeger and Pfleeger, 2002). The framework identifies five steps involved in hacking attacks:

1. *Information Gathering for Target Acquisition*

This step includes activities comparable to a burglar "casing the establishment" (McClure et al., 2001:1). It involves three main types of activities: footprinting, scanning and enumeration.

The goal of *footprinting* is to gather as much information as possible about all aspects of the target and its security, just as a bank robber would find out about armored car routes and delivery times, video cameras, number of tellers, escape routes, etc. (McClure et al., 2001:2). Using a variety of techniques, the attacker uncovers information about the target's environments: IP addresses reachable through the Internet, TCP and UDP services, system architecture, access control mechanisms, remote access, extranet, etc.

Scanning allows the attacker to focus on those systems in the target that are "alive" and actually reachable through the Internet, just as a burglar choosing doors or windows (McClure et al., 2001:30). Scanning involves techniques such as "ping sweep" (to find which IP addresses have active hosts), TCP/UDP port scanning (to find out which ports have active server programs running), and operating systems detection.

Enumeration is an intrusive probe to identify valid user accounts, network resources and shares not adequately protected, applications and versions, etc. Given their intrusive nature, with active connections to systems and directed queries, enumeration activities can potentially be logged and detected.

2. *Initial Access*

This step includes attempts to get access to the target's system, and to compromise it as much as possible after obtaining user-level privileges.

Attempts to gain access often involve malicious coding, such as viruses that infect files in a single system, worms that spread infections across different systems (such as BubbleBoy, IloveYou, etc.), and blended worms or snakes, which can carry viruses and "trojan horses" (Code Red, Code Red II, Sircam, Nimda). A "Trojan horse" (or "trojan," for short) is a program that pretends to be legitimate software, such as a game, but "performs unintended (and often unauthorized) actions, or installs malicious or damaging software behind the scenes when launched." (McClure et al., 2001:578). Hacker attempts to gain access to a user's system may also employ techniques such as brute force password guessing and buffer overflows (Panko, 2003:315; McClure et al., 2001:161). Physical access is also possible, but rare (eg., when users' computers at work are left unattended).

Once the "door" to a user's computer is open through malicious code, brute force or physical access, the hacker proceeds to breach the security of the user's computer and compromise its confidentiality, integrity and availability (Pfeegler and Pfeegler, 2002).

3. *Privilege escalation*

In this step the attacker tries to gain complete control over the system by acquiring privileges above the simple user-level. The hacker tries to acquire administrator or root privileges (through techniques such as password cracking and trojans), and to consolidate power by obtaining other accounts, and accessing other resources (hosts, networks). The hacker is now in a position to wreak havoc, by reading or altering sensitive information, changing or deleting key files, wiping out the hard drive, using the compromised target to launch attacks against other targets, etc. (Panko, 2003).

4. *Covering tracks and creating back doors*

Having acquired administrator-level control of the target, the hacker then tries to avoid being detected by the real systems administrators. This involves techniques such as deleting or modifying logs, hiding tools and disguising trojans.

The hacker may also set backdoors, to ensure that access can easily be regained later, even if the password is changed. This is done through techniques such as creating rogue user accounts, scheduling batch jobs, infecting startup files, planting remote control services, installing monitoring mechanisms and replacing applications with Trojans.

Step sequencing, alternative paths and Denial- of- Service

The framework implies a logical sequence of steps (gathering information, then breaking in to gain user-level access, then using this level of access to gain higher level privileges, and finally covering the tracks and leaving backdoors open for return intrusions). It is important to note, however, that some steps might be skipped (e.g., gaining access without having bothered to gather information; or getting administrator privileges already in the initial access) or repeated (e.g., going back for more elaborate enumeration after getting administrator privileges).

It is also important to note that not all attacks succeed. When hackers are unable to achieve control of the target, they often express their frustration by launching Denial-of-Service (DoS) attacks (such as Smurf, Fraggle and Syn) that disrupt services or make them inaccessible to legitimate users, networks, systems, etc. Techniques for DoS attacks may involve bandwidth consumption, resource starvation, taking advantage of programming flaws, and launching routing and DNS attacks. An even more vicious form of attack is Distributed Denial-of-Service (DdoS), where handler programs and zombies or slaves are planted in several other compromised clients or servers, which are then used to attack the target. This form of attack has succeeded in temporarily paralyzing targets such as Yahoo, eBay, CNN.com, E*Trade, ZDNeT and others, causing severe financial losses (McClure et al., 2001:504).

THE MODEL

The model we developed to conduct an empirical test of the hacking framework is presented in Figure 1. It provides a basis for exploring the variables inspired by the framework, and adds two other variables that the literature suggests might have an impact on the growth in security breaches: number of hosts in the Internet, and broadband access to the Internet by home and small business users.

Reconnaissance

This variable corresponds to the first step in the hacking framework: target acquisition and information gathering (footprinting, scanning and enumeration). The objective of this step is to identify potential victims for the hacking attacks to follow, by obtaining information such as the number and type of computers, their operating systems, servers, applications, and resources like shared files, databases, etc. If the hackers find enough interesting resources in a given site or organization, they are then more likely to attempt initial access.

Malicious Code

Malicious Code is the tool of choice for hackers to attempt initial access to user and administrator accounts. As discussed before, Malicious Code attacks include worms, viruses, and similar computer code, and typically deliver trojan horse payloads to a target's computer. Malicious Code attacks may exploit software vulnerabilities in popular operating systems, server software and application software, or rely on visit to a web site which delivers the malicious code directly. They can also rely on having a user or administrator open an e-mail attachment and/or render a HTML formatted message which replaces a valid element type with a disguised malicious code. A Malicious Code attack may also be an end in itself, intended to bring havoc to a network and cause either a server or network shutdown, working similarly to a DoS attack.

User Compromise

This variable represents what happens in the second step in the hacking framework (initial access), once the door to a user's computer has been opened through malicious code, brute force, or physical access. While Malicious Code is a measure of attempts to compromise computer systems, User Compromise is a measure of actual breaches of user computer systems. According to the literature (e.g. McClure et al., 2002), User Compromise should increase with the growth in Internet high-speed access, due to computers being on seven days a week, twenty four hours a day (24/7).

Root Compromise

Root Compromise corresponds to the third step in the hacking framework, privilege escalation. Once hackers succeed at User Compromise, they try to gain administrator or root-level privileges, and to consolidate power by obtaining other accounts, and accessing other resources. Root Compromise may also be achieved directly, through Malicious Code that takes advantage of operating systems, server and application vulnerabilities, typically using buffer overflows to deliver the malicious payload.

Denial of Service

As mentioned before, Denial-of-Service attacks represent attempts to make a service inaccessible to legitimate users. Recent examples include attacks against Yahoo, Microsoft and other anecdotal cases. The literature (McClure et al, 2001; Panko, 2003; Pfleeger and Pfleeger, 2002) suggests that when hackers are not able to achieve Root Compromise, they express their frustration by launching DoS attacks, where they flood a network or disrupt connections or services. The rationale here is that if hackers cannot achieve control of the resource, they will try to at least make it inaccessible.

Hosts and Broadband

The literature (e,g, Pfleeger and Pfleeger, 2002) suggests that two variables in the environment might help explain the growth in security threats: number of hosts in the Internet (Hosts) and broadband access for households and small business (Broadband). The increase in the number of hosts represents an increase in the potential for attack by hackers. The increase in broadband access for households and small businesses means that now there are millions of computers working on a 24/7 basis, with little or no protection. Because households and small businesses typically lack the security protections used by large businesses, there is anecdotal evidence that malicious code attacks are being broadcast through broadband DSL and cable users, just as spammers are also doing. There are probably other environmental factors that might have a bearing on the growth of security threats, but given the exploratory nature of this study these are the only two that will be considered here.

RESEARCH QUESTIONS AND HYPOTHESES

The following research questions were addressed in this exploratory study:

- Are the relationships presented in the model observable in practice? If so, which variables should system administrators be concerned with?
- Do environmental variables such as number of hosts and broadband access help explain the increase in security threats?

These research questions led to the formulation of the following hypotheses:

Hypothesis 1: Reconnaissance is positively related to Broadband and Hosts.

> Increase in Broadband access and number of Internet Hosts may increase the number of potential hacker targets, which in turn may increase the activities of information gathering for target acquisition (i.e., Reconnaissance).

Hypothesis 2: Malicious Code is positively related to Reconnaissance.

> Increase in Reconnaissance activities may increase the number of potential victims selected, which in turn may increase hacker activities for distributing Malicious Code.

Hypothesis 3: User Compromise is positively related to Malicious Code, Reconnaissance and Broadband.

> Increase in Malicious Code activities may open the door for an increase in User Compromise. Increase in Reconnaissance means that more potential desired targets are identified, which may then lead to an increase in initial access and contribute to User Compromise. Increase in Broadband access may increase the number of users with lower computer security in place, which in turn may increase User Compromise.

Hypothesis 4: Root Compromise is positively related to User Compromise, Malicious Code, and Hosts.

> Increase in User Compromise followed by privilege escalation may increase Root Compromise. Increase in Malicious Code activities may also lead directly to an increase in Root Compromise. Increase in the number of Internet Hosts may create a larger number of computer systems with administrator or root privileges, which in turn may also increase Root Compromise.

Hypothesis 5: Denial of Service is negatively related to Root Compromise, and positively related to Malicious Code and Number of Hosts.

> If hackers achieve little or no Root Compromise, frustration may lead to an increase in the number of DoS attacks. Increase in Malicious Code may also lead to increase in DoS attacks (e.g., the SCO Denial- of- Service attack caused by MyDoom). Increase in the number of Internet Hosts may lead to a larger number of servers, which in turn may increase DoS attacks.

Hypothesis 6: Broadband is positively related to Number of Hosts.

The growth of the Internet (reflected in the growth in Number of Hosts) may affect the demand and availability of broadband access.

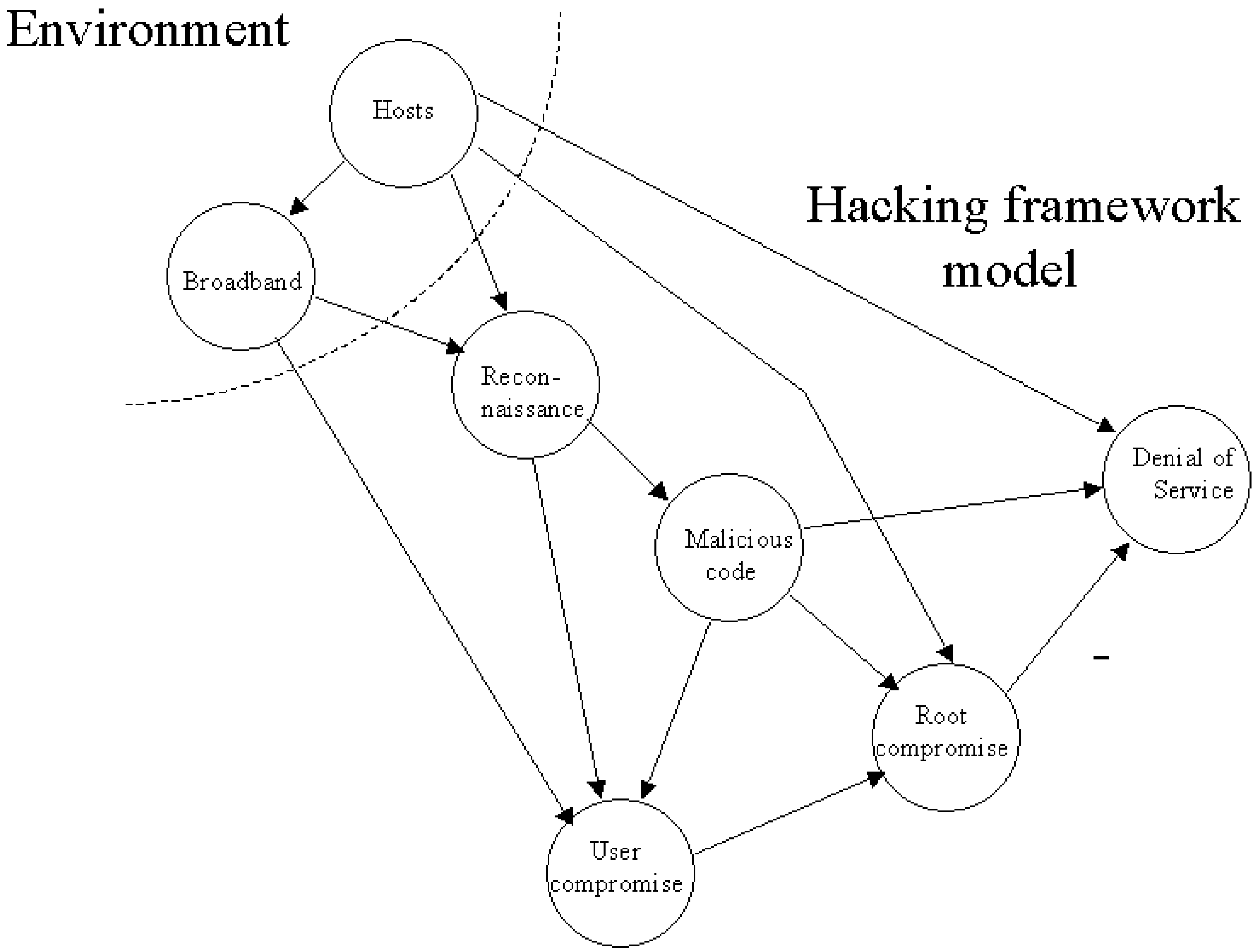

Figure 1. Model for Empirical Test of Hacking Framework

MEASUREMENT AND DATA COLLECTION

This exploratory study used non-reactive measures based on available official descriptive statistics of the whole population, rather than self-reports collected through the use of samples and surveys. The federal government only recently started collecting those statistics, so there is no long historical series to draw from. Therefore, the findings of this exploratory study are based on 60 months of statistical data. In the future, the accumulation of data over the years will allow more sophisticated analyses (e.g., testing for the possibility of cyclical phenomena that peak at certain times of the year).

Reconnaissance, Malicious Code, User Compromise, Root Compromise, and Denial of Service were measured using the data collected for the similarly named categories in the statistics published by the Federal Computer Incident Response Center (available at http://www.fedcirc.gov/incidentAnalysis/incidentStatistics.html) . Although the FCIRC data represents the best information available for the last 60 months, it might underestimate the actual incidence of the phenomena, because the data is based on reported incidents, which represent an unknown fraction of total incidents.

There are no reliable worldwide statistics for the number of hosts in the Internet, so a surrogate measure was used here, the number of web servers on the Internet. Although not necessarily a perfect surrogate, this study assumes that the number of web servers is related to the number of computers in the Internet, because it reflects the expansion in the use of the web and access to the Internet. We were interested in the overall expansion, the growth curve, and not in the different types of web servers. The total number of web servers was therefore used as a measure of the number of Hosts variable in the model. The source for this data was Netcraft, which obtains the number of web servers by querying all servers in the Internet (http://news.netcraft.com/archives/web_server_survey.html).

The Broadband variable in the model was measured using 60 months of data about the growth of broadband access for household and small businesses, from available statistics collected by the FCC (http://www.fcc.gov/wcb/iatd/comp.html). The FCC collects data every six months, not in a monthly basis. We used the data for each semester as if it were the data for each month in that semester. This underestimates the number of users with broadband access within a semester, but captures the trend for long-term use of broadband. As discussed before, high-speed access to the Internet, with its 24/7 availability for home and small business users, has been suggested as an important environmental variable affecting the increase of security attacks and compromise.

ANALYSIS AND RESULTS

Descriptive Statistics

Table 1 shows the descriptive statistics for the variables from the hacking framework, which were included in the model. Reconnaissance and Malicious Code account for 97% of the incidents reported. Malicious Code and Denial of Service, however, are also important because they impact a larger number of users and computers. Once a server is unavailable (as in the case of the Denial of Service attack at Microsoft), an incalculable number of users were affected by the inability to obtain information, download latest updates and patches, etc. Malicious Code aimed at delivering viruses to mail users (as in the case of Melissa) lead to the shutdown of mail servers, affecting not only the infected users, but all other users accessing the mail server. And although User and Root compromise correspond to small percentages of the attacks, the results still mean that almost every day either a root or user compromise occurs. Root compromises have the potential to affect a large number of computers in an organization, for the root or administrator can access most of the other computers in his or her local area network and Internet. Of course, User compromise can also lead to Root compromise by escalation of privilege.

Variable	Mean	Total	%
User compromise	16	961	.07
Root compromise	11	633	.04
Denial of Service	15	891	.06
Malicious Code	3,272	196,335	13.69
Reconnaissance	19,921	1,195,186	83.35
Total incidents(*)	23,899	1,394,006	

(*) This does not include other unclassified incidents

Table 1. Descriptive Statistics

Note: it seems that there are large variability in a month-to-month basis in each of the variables, but there are not enough data to indicate if there is seasonably, or not, in the incidents.

Simple Correlations

Table 2 shows the simple correlations among all the variables in the model. The correlations marked in bold were found to be significant, and the letters in parentheses indicate their level of significance. Some correlations were both high and highly significant (e.g., Broadband and Hosts), while other correlations were low and with low significance (e.g., Denial of Service and Hosts).

	User Compromise	Root Compromise	Denial of Service	Malicious Code	Reconnaissance	Broadband	Hosts
User Compromise	1	**.1743** (e)	-.0630	.1090	.0025	**.2223** (d)	.1809
Root Compromise	**.1743** (e)	1	**-.2980** (e)	-.1142	.0256	-.0347	-.0297
Denial of Service	-.0630	**-.2980** (e)	1	-.0432	-.1109	.0021	**.1505** (e)
Malicious Code	.1090	-.1142	-.0432	1	**.6230** (a)	**.4015** (b)	**.3240** (c)
Reconnaissance	.0025	.0025	-.1109	**.6230** (a)	1	**.5135** (a)	**.4195** (b)
Broadband	**.2223** (d)	-.0347	.0021	**.4015** (b)	**.5135** (a)	1	**.9022** (a)
Hosts	**.1809** (e)	-.0297	**.1505** (e)	**.3240** (c)	**.4195** (b)	**.9022** (a)	1

(a) significant at .0001 (b) significant at .001 (c) significant at .01 (d) significant at .1 (e) significant at .2

Table 2. Simple Correlations

Hypotheses Testing

The hypotheses inspired by the model were tested using stepwise regression, which generated the results highlighted in Table 3. Given the exploratory nature of this study, there was no attempt to use more sophisticated tools such as causal analysis to measure the hypotheses as a recursive system.

HYPOTHESES	**VARIABLES**		**BETA**	**T Significance**	**R^2**
	Dependent	**Independent**			
H1	Reconnaissance	Broadband	.513476	.00001	.26366
H2	Malicious Code	Reconnaissance	.622971	.00001	.38809
H3	User Compromise	Broadband	.222302	.0878	.04942
H4	Root Compromise	User Compromise	.174308	.1829	.03038
H5	Denial of Service	Root Compromise Hosts	-.293751 .141746	.0224 .2619	.10886
H6	Broadband	Hosts	.902162	.00001	.81390

Table 3. Results of Stepwise Regression

Hypothesis 1 was partially supported. Reconnaissance is positively related to the growth in Broadband access, and almost 30% of the variation on Reconnaissance is explained by the variation on Broadband. The association between Reconnaissance and Hosts, however, is not significant.

Hypothesis 2 was supported. Malicious Code is positively related to the increase in Reconnaissance, and almost 40% of the variation on Malicious Code is explained by the variation on Broadband.

Hypothesis 3 was partially supported. User Compromise is positively related to Broadband, probably reflecting unprotected computers of home and small business users. Surprisingly, User Compromise is not related to increase in Reconnaissance or Malicious Code. Given that only about 5% of the variation on User Compromise is explained by the variation of Broadband, it seems that other factors not considered in the Model may have a greater influence in User Compromise (e.g. number of vulnerabilities found in popular operating systems and applications).

Hypothesis 4 was partially supported. Root Compromise is not affected by Malicious Code or Hosts, and is rather modestly (3%) affected by User Compromise, probably through privilege escalation from user to root. Again, it seems that other factors not considered in the model may have a greater influence in Root Compromise.

Hypothesis 5 was supported. Denial of Service is positively related to Hosts and negatively related to Root Compromise, as expected, but Root Compromise and Hosts explain only about 10% of the variation of Denial of Service. While this means that DoS has other main causes, the results still seem to indicate that the inability to compromise systems leads hackers to attempt to make the resource inaccessible, as proposed in the hacking framework.

Hypothesis 6 was supported. The environmental variables used in the model, Broadband and Hosts, are strongly positively related, and more than 80% of the variation in Broadband is explained by the variation in Hosts.

The effect of each variable on the others is shown in Figure 2, with the BETA values obtained for the relationships that were found to be significant. Once more, this study is too exploratory in nature to allow a full causal path analysis, and therefore no causality is to be inferred from these results.

DISCUSSION AND CONCLUSION

The results obtained in this exploratory study provide preliminary corroboration for the value and potential of the model. As expected, Reconnaissance (Step 1) was positively related to the vulnerability represented by increased Broadband Internet access by home and small business users. Reconnaissance (Step 1) seems to lead to Malicious Code (Step 2). There was support for escalation of privilege, as Root Compromise (Step 3) was related to User Compromise (Step 2). There was also support for the idea that hacker frustration at failing to gain control of a resource may be the impetus for trying to sabotage it through Denial of Service (DoS was negatively related to Root Compromise). However, it seems that other variables not in the model might help explain User Compromise, Root Compromise and Denial of Service, and more research is needed to identify and test those missing variables.

Given the exploratory nature of the study, system administrators should perceive its practical implications as suggestive rather than prescriptive. The results indicate that increase in the level of Reconnaissance is related to increase in Malicious Code. Therefore Systems Administrators may use the detection of Reconnaissance activities as an early signal of future attacks using Malicious Code. This early signal should allow them to be prepared and to strengthen their defenses ahead of those Malicious Code attacks.

System Administrators should also be aware of their fellow employees who have home broadband access and connect to the company's network from home. Although the link was not very strong, the results suggest that User Compromise at home may lead to Root Compromise at work.

Broadband Internet service providers should also heed the fact that User Compromise was related to increase in broadband access. The implication is that service providers should create security mechanisms in their networks in order to prevent User Compromise, in order to make up for the lack of computer security training that can be reasonably expected from their home customers (non computer experts).

Future research should use more rigorous methods to test for causality, using causal path analysis. It should also test for serial correlations (given the historical nature of the data), for multicolinearity (given a high level of correlation among the environmental variables used in the model), and for non-linearity of the relationships between some of the variables (given the seemingly exponential growth of the Internet).

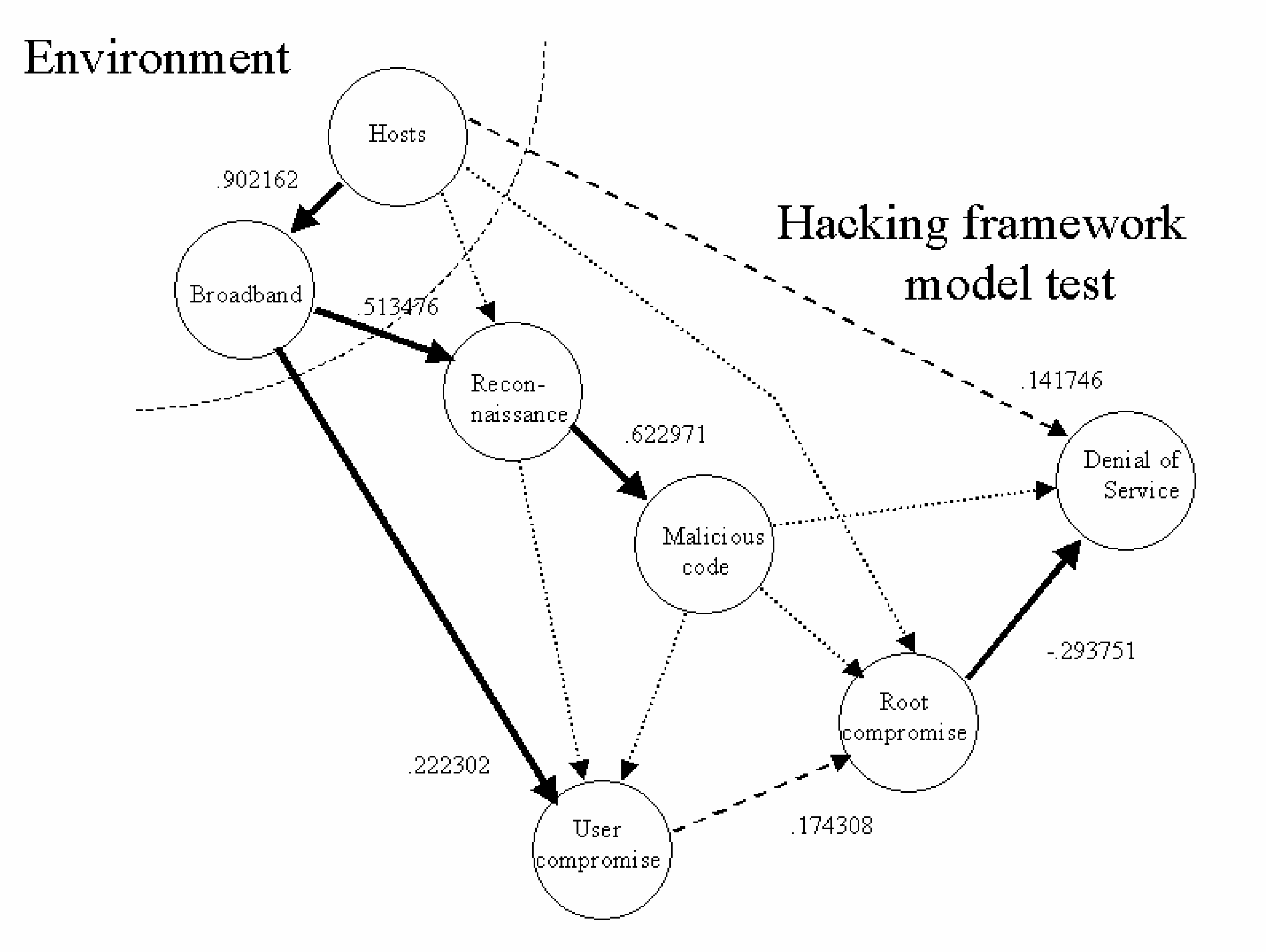

Figure 2. Test of model inspired by hacking framework

This study used secondary data, based on official statistics, which are non-reactive and collected at the time of the event, not retroactively. There seems to be significant promise in this data collection strategy of using secondary data from available longitudinal series of statistics of the whole population under study, rather than relying on surveys and samples. For example, future research to identify additional environmental variables to explain User and Root Compromise may use archives from Microsoft, RedHat, Sun, Symantec and other sources to identify the frequency and nature of discovered vulnerabilities, and the number and security threat levels of malicious code created to exploit these vulnerabilities. Using industry statistics, researchers will then be able to relate the number of computers using different operating systems, servers and applications to successful Root or User Compromise.

A limitation of this study is that only used 60 months of data, because statistics only started being compiled five years ago. Also, this study had to use monthly data, which can be more variable. The accumulation of data over the next several years should enable researchers to examine questions such as the possible cyclical nature of hacking attacks (for example, whether they peak at certain times of the year, such as the holiday shopping season). In the next ten years, as the government and other centers continue collecting data, researchers will have much longer historical series, and thus be able to study in much greater detail the phenomena associated with the hacking framework.

REFERENCES

1. Bagchi,K. and Udo,G.(2003). An Analysis of the Growth of Computer and Internet Security Breaches. *Communications of the Association for Information Systems*,12,684-700.
2. Bento,A.(2003). Soho Security: A Technical Briefing. *Proceedings of the Americas Conference on Information Systems.* Tampa,Florida.
3. Bookholdt,J.L.(1989). Implementing Security and Integrity in Micro-Mainframe Networks. *MIS Quarterly*,13,135-144.
4. CERT/CC (2002). Overview of Attack Trends. (http://www.cert.org/archive/pdf/attack_trends.pdf). Accessed 2/22/04.
5. CERT/CC (2003). CERT/CC Statistics 1988-2003. (http://www.cert.org/stats/cert_stats.html). Accessed 2/22/04
6. Federal Communications Commission (http://www.fcc.gov/wcb/iatd/comp.html). Accessed 2/22/04
7. Federal Computer Incident Response Center (http://www.fedcirc.gov/incidentAnalysis/incidentStatistics.html). Accessed 2/22/04
8. Garg,A., Curtis,J. and Halper,H.(2003). Quantifying the Financial Impact of IT Security Breaches. *Information Management & Security*,11,74-83.
9. Howard,J.D.(1997). *An Analysis of Security Incidents on the Internet*. Ph.D. Dissertation, Carnegie Mellon University.
10. Howard,J.D. and Longstaff,T.A.(1998). A Common Language for Computer Security Incidents. Albuquerque, New Mexico:Sandia.
11. Krol,E. and Ferguson,P.(1995). *The Whole Internet*. Sebastopol, CA: O'Reilly.
12. Landwehr,C.E., Bull,A.R., McDermott,J.P. and Choi,W.S.(1994). A Taxonomy of Computer Program Security Flaws. *ACM Computing Surveys*,26,211-233.
13. Loch,K.D., Carr,H.H. and Warkentin,M.E.(1992). Threats to Information Systems. *MIS Quarterly*,16,173-186.
14. Lukasik, S.J.(2000). Protecting the Global Information Commons. *Telecommunication Policy*,24,519-531.
15. McClure,S., Scambray, J.& Kurtz,G.(2001). *Hacking Exposed*. New York:McGraw-Hill.
16. Netcraft (http://news.netcraft.com/archives/web_server_survey.html). Accessed 2/22/04.
17. Panko, R.(2003). *Business Data Networks and Telecommunications*. Upper Saddle River, NJ:Prentice-Hall.
18. Pfleeger,C,P, and Pfleeger,S,L.(2002). *Security in Computing*. Upper Saddle River, NJ:Prentice-Hall
19. Richardson, R. (2003). *The 2003 CSI/FBI Computer Crime and Security Survey*. San Francisco: Computer Security Institute.
20. Straub,D.W. and Nance,W.D.(1990). Discovering and Disciplining Computer Abuse in Organizations. *MIS Quarterly*, 14,45-60.
21. Straub,D.W. and Welke,R.J.(1998). Coping with Systems Risk. *MIS Quarterly*,22,441-469.