

the security journal

www.TheSecurityJournal.com

ISSN: 1947-6973

Enjoy that summer vacation!



Just don't forget to mind the store...

...take some time and learn about:

- Protecting yourself from theft & disruption
 - Using honeypots in intrusion detection
 - Motivating teleworkers to be secure
- ...and the next installment of Noob's Corner!



Volume 28 - Summer 2009 Edition



Your global information security experts

5350 Tomah Drive
Suite 3200
Colorado Springs, CO 80918
www.securityhorizon.com

Editor in Chief: Greg Miles
Assistant Editor: Michele Fincher

Call for Articles!

- Interested in being published in a recognized periodical?
 - Need to earn CPE's?
 Contact us at
editor@securityhorizon.com

Would you like to advertise in The Security Journal?

Contact us at
editor@securityhorizon.com

A special thank you to **Ping Look** from **Look Designs** for the creation of the Security Horizon logo and masthead images for *The Security Journal*.

For more information on Look Designs:
www.republicofping.com
design@republicofping.com

Security Horizon, Inc. was founded in 2000 and is headquartered in Colorado Springs, Colorado. As a company, we believe that sound security services are based on education, experience, standards, ethics and unquestionable integrity.

Table of Contents

Notes from the Editor
greg miles.....p. 3

Information Security Against Theft and Disruption, Part 1
tim godlove.....p. 4

Intrusion Detection System Using Advanced Honeypots
ram kumar singh.....p. 10

IAM Course Schedule.....p. 21

IEM Course Schedule.....p. 21

Noob's Corner
dana rollins.....p. 22

Which Factors Motivate Teleworkers to Take Necessary Security Precautions?
tim godlove.....p. 26



Copyright ©2009 by Security Horizon, Inc.
All rights reserved. Reproduction without permission is prohibited. The views addressed in each article are those of the author and not necessarily those of The Security Journal or Security Horizon, Inc.
ISSN 1947-6973



Black Hat[®]

Briefings & Training

World Tour 2010

Black Hat Briefings & Training DC

Hyatt Crystal City • Virginia

January 31-February 3

Call for Papers and Registration Opens September 1, 2009.

Black Hat Briefings & Training Europe

Hotel Rey Juan Carlos Barcelona • Spain

April 12-15

Call for Papers and Registration Opens November 1, 2009.

Black Hat Briefings & Training USA

Caesars Palace Las Vegas • Nevada

July 24-29

Call for Papers and Registration Opens February 1, 2010.

Notes From the Editor

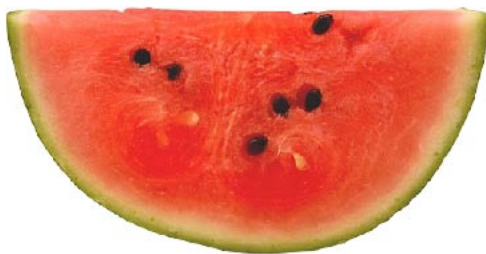


Welcome to another information packed edition of The Security Journal! We appreciate you joining us this quarter and hope you will continue to read our e-periodical.

In this journal, we are very happy to publish an article from an associate in India, this gives us a bit of an international flair focused around intrusion detection. We also have a good article on the impacts of telework on the security of an organization. Our Noobs corner continues with a great article on how to do some war walking.

For future issues, we are keeping our eyes on important changes in our industry, to include the introduction of a U.S. cyber czar, the importance of PCI standards, and the changes to information security due to possible healthcare initiatives that are in the works.

We are currently keeping the new format we used last quarter. We haven't received much in the way of comments on the format, positive or negative, so if you have thoughts on this, please pass them along. As always, we are open to feedback on improving our periodical as it is meant to be useful to you, our readers.



Gregory Miles, Ph.D. CISSP, CISA, CISM is the President and a Co-Founder of Security Horizon (www.securityhorizon.com), Editor-In-Chief of the Security Journal (www.thesecurityjournal.com), and a professor with the University of Advancing Technology. (www.uat.edu) You may contact him at gmiles@securityhorizon.com.

... and Disruption

~ The following is the first half of a two part article. ~

Introduction

Network security is an incredibly important issue, but the sheer importance often leads to an oversight: physical security. While millions are spent thwarting hackers and identity thefts, for example, much crucial data is no more physically secure than a laptop computer left in an unlocked car. Data is so easily copied that sensitive information can be purposefully or accidentally emailed or otherwise sent to someone – for solid, business-related purposes – whose own desktop or other data storage devices may lack the security necessary to protect crucial data from exposure.

Cyber attacks may be geared toward disruption or denial of service, or financial gain. Financial gain is sometimes associated with identity theft or reallocation of funds from accounts, both of which are considered white-collar crimes and do not receive much attention from law enforcement agencies or the general public. An example of financial loss was demonstrated in a survey of 611 companies doing business on the Internet in 2001. Results indicated that 83% of the companies experienced security breaches and 62% said there was some type of financial loss, with average damages of \$47.8 million, compared to \$26.6 million in 1999. These were the relatively early days of information security concerns, and the height of the dot.com boom. Surely the situation has improved since these days, now that the Internet is more fully integrated into economic life? Unfortunately, no. Information security failures are still a major economic fault line.

The costs of poor information security has increased since the 2001 dot.com boom: “In the 2006 CSI/FBI Computer Crime and Security Survey conducted by the Computer Security Institute and the Federal Bureau of Investigation, 313 computer security professionals reported a total of \$52.49 million in losses linked to computer security incidents for 2006.” This, despite the immense amount of money spent on computer security in the past decade and even the emergence of dedicated information technology security divisions within larger firms, as well as many number of vendor firms working as providers of various security protocols, training, and hardware/data management services.

Much of information security failure activity comes in the form of illegal access into a company or government network system. Some hackers start out as outsiders who use various password attacks in order to gain access as a user of the network. Many begin as insiders, in the form of disgruntled or former employees. They will use known weaknesses in the system to gain further access as an administrator or super user. Once these privileges are attained, a

hacker then can read or alter files, control a system, and insert a rogue code such as a virus to damage the infrastructure. Often, hackers may not even be motivated by gain or aware of what systems their viruses have infiltrated.

The costs of security breaches can be severe, and evolve into not only crime but literal “cyberterrorism.” There are several possible scenarios for cyberterrorism. In one, a cyberterrorist hacks into the processing control system of a cereal manufacturer and changes the levels of iron supplement. Customers suffer, some perhaps die, the product is recalled, and the firm suffers greatly. In another, a cyberterrorist attacks the next generation of air traffic control systems. Two large civilian aircraft collide. In a third, a cyberterrorist disrupts banks, international financial transactions, and stock exchanges. Economic systems grind to a halt, the public loses confidence, and destabilization is achieved.



As technology continues to evolve, so will opportunities for cyberterrorists and other malevolent actors whose goals may be financial, simply apolitical, or utterly inexplicable. The phenomenon of “cybercash”, in which nearly all money is electronic, and thus instantly transferable and exchangeable, is in the offing, and as Guttman (2003) notes:

Given the inherently unstable nature of self-regulation, cybercash will need external stabilizers for support. Facing a heterogeneous money form appearing in many variations, such stabilizers must contain central-control mechanisms which manage the organizational complexity of this new monetary regime. Those mechanisms have to ensure a systemic coherence and robustness of the electronic-money regime in the face of possible technological mishaps, cyberterrorism, incidences of financial crisis, and our economic system’s propensity to monetary instability.

Given the stakes, both for society as whole and individual firms, the security of information and of the information infrastructure are paramount. The very nature of information — it can only be shared via copying, for example, and not exchanged — limits its total security, and the fact that information must be used in order to have value means that information will be exposed to end users when transmitted. Both external loci (hackers, cyberterrorists), and internal loci (employees, vendors, physical objects such as hard drives and servers) for security vulnerabilities.

Risk Assessment

Risk assessment involves answering these seven questions:

1. What can go wrong? (threat events)
2. If it happened, how bad could it be? (single-loss exposure value)

3. How often might it happen? (frequency)
4. How sure are the answers to the first three questions? (uncertainty)
5. What can be done to remove, mitigate, or transfer risk? (safeguards and controls)
6. How much will it cost? (safeguard and control costs)
7. How efficient is it? (cost/benefit, or return on investment analysis)

There are six major steps involved in a risk assessment:

1. Inventory, definition, and requirements
2. Vulnerability and threat assessment
3. Evaluation of controls
4. Analysis, decision, and documentation
5. Communication
6. Monitoring

These steps are of course part of any sort of risk assessment and are not specific to information security. This paper will examine specifics of how a risk assessment for information security may look and how this could influence top management views on information security management.

Inventory —Threat Assessment

A compliance/policy management official explains the first step of developing an information risk management program:

“Overall, you need to know what your hardware-, operating system-, and application layer-security vulnerabilities are-and you need to know, generally, who uses what application and why. Then, you need to lock down these assets in a systematic way. This is simple but it isn’t easy.”

Larger organizations may not even know what they have. If one very large institution could not produce a network map in a reasonable time-that meant, they had servers and other digital assets that were unaccounted for and reliance on default controls at the hardware and operating system level and inconsistencies in response time to threats that can be dangerously complacent. Data are notoriously difficult to “rein in” once made available on certain networks. Data often end up stored on local files rather than being centralized, and once out of control of those in charge of it, data can end up virtually anywhere in the world. Not only is the Information Technology Department an important part of this initial assessment, so too is the Human Resource Department.

Indeed, risk assessment begins not necessarily with risk alone, but with a complete assessment of information technology capabilities and vulnerabilities. Often organizations fix point problems without looking at the overall picture. Large companies are the most notorious

for doing this, having separate business units that tend to fight more often than work together for the good of the company. Subsequently, without cooperation and an overarching plan, they end up vulnerable to attack. An initial assessment will also allow the firm to know where its data are, and what possible damage can be done via unauthorized access to these data. Clearly, a firm with trade secrets or even sales leads can be severely compromised by a disgruntled employee or a former executive taking information to a competitor. Firms with access to consumer retail information (e.g., credit card numbers, social security numbers, and other such information) may also be open to significant liability if proper protocols and industry standard protections are not followed. Staffers may need training on security protocols and even the basics of common hacker tactics (e.g., viruses, social engineering, etc.) However, just knowing these possibilities is not enough — a top-to-bottom security assessment must be put into place in order to understand what an organization's specific vulnerabilities are, and how exposure can be limited.

Subject-matter experts, including Certified Public Accountants, can also be brought in to deal with the non-technical ends of security issues. According a Certified Public Accountant understand internal controls and can assist companies in adapting control concepts to protect the confidentiality, availability, and integrity of valuable assets. ... Certified Public Accountants can perform trend analysis and search for patterns in security data. They can be assets in drafting policies and procedures for safeguarding financial and customer data and also play a role in training employees to abide by the rules. Certified Public Accountants can be useful as they often have interpersonal training that technical staffers and IT professionals lack, and have a greater professional understanding of data control and non-technical protocols in general.



In addition to the application/user layer, the operating system itself can often have vulnerabilities, especially as operating systems these days are often tied to specific applications, such as web browsers, or even databases such as the .mac storage facility that comes along with recent versions of some Mac operating systems.

Operating systems can be more or less vulnerable to viruses, Trojans (which do not attack a system, but simply draw information from the system), and other malevolent programs. Windows-based operating systems are especially vulnerable to such programs due partially to the widespread deployment of the systems (thus, more vectors from which to spread) and due to animosity toward Microsoft as a firm in the hacker community.

Hardware is also vulnerable. Many firms “give” employees laptops, pagers, palmtops and

other easily portable computer equipment, which can be stolen, destroyed, or delivered to an opponent for hard drive copying after hours. Old equipment can be disposed of without the data being erased from it — indeed it can be said that data never truly “goes away”; with sufficient resources virtually any hard drive or other information medium can be milked of “deleted” information if the equipment remains intact. Recommend contracting with asset disposal firms to ensure that old hardware does not end up on eBay, with information intact, or in the hands of a competitor, criminal, or terrorist who will often need little more than a Norton utility restoring program to retrieve “erased” data.

References

- Andress, A. (2003) *Surviving Security: How to Integrate People, Process, and Technology*. Boca Raton, FL: Auerbach.
- Bielski, L. (2004). Keep Proprietary Information in Its Place: Running an ‘Enterprise’ with Control, Insight, and an Eye on Risk Management. *ABA Banking Journal*, 96(4): 52-58. Retrieved May 5, 2008, <http://www.allbusiness.com/legal/laws/137657-1.html>
- Collin, B. (1997). The Future of Cyberterrorism. *Crime and Justice International*, March 1997:5–18. Retrieved May 1, 2008, <http://www.cjcenter.org/cjcenter/publications/cji/archives/cji.php?id=415>
- Guttman, R. (2003). *Cybercash: The Coming Era of Electronic Money*. New York: Palgrave MacMillan.
- Lineberry, S. (2007) “The Human Element: The Weakest Link in Information Society.” *Journal of Accountancy*, 204(5):44 –50. Retrieved May 1, 2008, http://www.aicpa.org/pubs/jofa/nov2007/human_element.htm
- Sharma, A. (2006) “A Holistic Approach to Physical and IT Security.” *Security Magazine*. 21 November. Retrieved April 28, 2008, http://www.securitymagazine.com/CDA/Articles/Feature_Article/c805be157db0f010VgnVCM100000f932a8c0

~ Look for Part 2 in our next edition! ~



Tim Godlove is currently a doctoral student in the field of Information Assurance Policy with many years as an information technology and security officer both on active duty with the U.S. Navy and in the Federal government. He may be reached through this publication.

SAINT®

Announcing SAINT 7

Securing your network
just got easier!



SAINT's crisp new interface makes it even easier to use.

- ✓ Integrated vulnerability scanning and penetration testing
- ✓ Payment Card Industry (PCI) Approved Scanning Vendor (ASV)
- ✓ Heterogeneous exploit and vulnerability coverage
- ✓ Exploit tools give you extra penetration testing capabilities including e-mail harvesting, social engineering trojan, e-mail forgery, and more
- ✓ Available as software for download or as a pre-configured appliance



Find out how SAINT can help you secure your network at www.saintcorporation.com
Contact SAINT's sales team at 1-800-596-2006 x0119 or sales@saintcorporation.com

Examine. Expose. Exploit.

Copyright ©2009 SAINT Corporation. All Rights Reserved.

...Using Advanced Honeypots

Abstract

As the number and size of the Network and Internet traffic increases the need for the intrusion detection grown in step to reduce the overhead required for the intrusion detection and diagnosis, it has made public servers increasingly vulnerable to unauthorized accesses and incursion of intrusions[2]. In addition to maintaining low latency and poor performance for the client, filtering unauthorized accesses has become one of the major concerns of a server administrator.

Hence implementation of an Intrusion Detection System (IDS)[2] distinguishes between the traffic coming from clients and the traffic originated from the attackers or intruders, in an attempt to simultaneously mitigate the problems of throughput, latency and security of the network. We then present the results of a series of load and response time in the terms of performance and scalability tests, and suggest a number of potential uses for such a system.

The exponential growth of computer/network attacks are becoming more and more difficult to identify the need for better and more efficient intrusion detection systems increases in step. The main problem with current intrusion detection systems is high rate of false alarms. Using honeypots[1] provides effective solution to increase the security and reliability of the network;

Keywords-Intrusion Detection Ssystem; Advanced Honeypots;Computer Attcks; Network Security;Information Security

Introduction

We hereby introduce the design and implementation of a load balancer that distinguishes between the traffic coming from clients and the traffic originated from the attackers. This system is an attempt to simultaneously solve the problems of load balancing[3] and unauthorized intrusion.

If, in the process of forwarding requests, the balancer detects traffic is an attack on the server ('an exploit'), it is then directed to an alternative server - a type of honeypot. Conventional detection and forensics methodology can then be used to gather information on the intruder, who will be unaware that they are not using a "real" server. Thus, the system will not only protect mission critical servers from unauthorized access in a manner transparent t the user, but allow for detailed data to be collected, which can later be used to take appropriate legal action against the incursion of intruders.

Background on IDS

An intrusion detection system (IDS) inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack from someone

attempting to break into or compromise a system.

There are several ways to categorize an IDS:

A. **Misuse detection vs. anomaly detection:** in misuse detection, the IDS analyzes the information it gathers and compares it to large databases of attack signatures. Essentially, the IDS looks for a specific attack that has already been documented. Like a virus detection system, misuse detection software is only as good as the database of attack signatures that it uses to compare packets against. In anomaly detection, the system administrator defines the baseline, or normal, state of the network's traffic load, breakdown, protocol, and typical packet size. The anomaly detector monitors network[12] segments to compare their state to the normal baseline and look for anomalies.

B. **Network-based vs. host-based systems:** in a network-based system, or NIDS, the individual packets flowing through a network are analyzed. The NIDS can detect malicious packets that are designed to be overlooked by a firewall's simplistic filtering rules. In a host-based system, the IDS examines at the activity on each individual computer or host.

C. **Passive system vs. reactive system:** in a passive system, the IDS detects a potential security breach, logs the information and signals an alert. In a reactive system, the IDS responds to the suspicious activity by logging off a user or by reprogramming the firewall to block network traffic from the suspected malicious source.

Though they both relate to network security, an IDS differs from a firewall in that a firewall looks out for intrusions in order to stop them from happening. The firewall limits the access between networks in order to prevent intrusion and does not signal an attack from inside the network. An IDS evaluates a suspected intrusion once it has taken place and signals an alarm. An IDS also watches for attacks that originate from within a system.

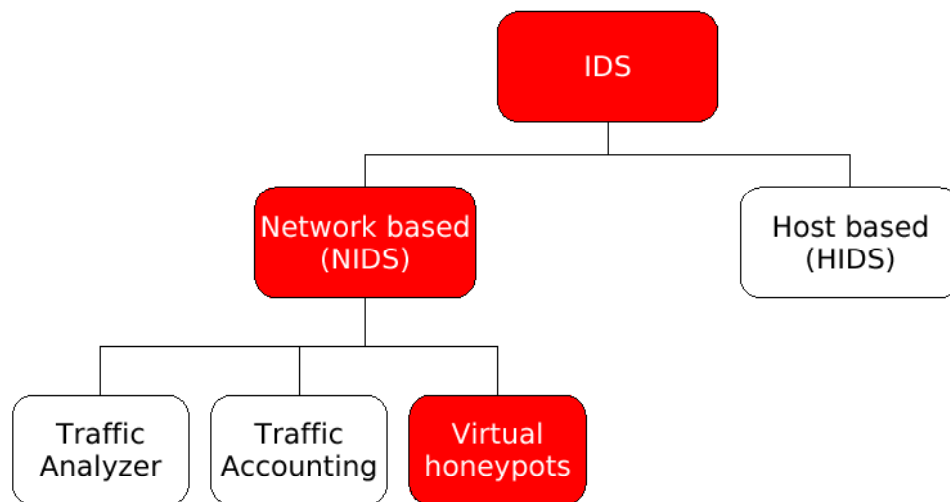


Figure 1: Intrusion Detection System heirarchy

Network Intrusion Detection Systems (NIDS)

Recent years have seen a drastic increase in the popularity of Network Intrusion Detection systems (NIDS). Intrusion Detection Systems (IDS) can be classified into two categories: Network-based Intrusion Detection Systems (NIDS) and Host-based Intrusion Detection Systems (HIDS). Existing products have substantial network monitoring capacity, and have been largely successful at providing accurate reports on unauthorized activity. While these products have gotten fairly good at monitoring and reporting on unusual activity, it has been stated, that the biggest problem with IDS is “intelligently reacting to their output”.

If an IDS detects an attack in progress, what action should be taken?. Furthermore, even if the organization deploying the IDS has the foresight create an attack response plan, if an administrator receives a page at 4:00 am, what are the chances that s/he will be able to react quickly enough to prevent the intrusion? Under most existing systems chances for timely prevention of the intrusion highly depend on the quick reaction of the human administrator. All too often IDS logs are only consulted long after the damage from an attack has been done.

Background on Honeypots

A honeypot is “an information system resource whose value lies in unauthorized or illicit use of that resource”[1].

A Honeypot is defined as being a security resource whose value lies in being probed or compromised” [1]. They can be either host and/or network based, but are more often than not network based as all interaction is typically performed over a network connection. A honeypot’s main utility comes from the fact that it simplifies the Intrusion Detection problem of separating “anomalous” from “normal” by having no legitimate purpose, thus any activity on a Honeypot can be immediately defined as anomalous. The characteristics of Honeypots make them well suited to the monitoring of malicious activity on networks, as well as being a valuable research tool in Computer Security.

Honeypot concepts are not particularly new, they can be traced back to early Computer Security papers such as Cliaord Stoll’s Stalking The Wily Hacker [2], however the study of Honeypots has recently been formalised. With this formalisation has come a focus on research of attackers’ methods and motivations [3], which has led to Honeypots being instrumental in the discovery of new security vulnerabilities [4].

Secure Direct

Secure Direct is an attempt to address this problem: by providing a fully automated response to specific network intrusions, it can eliminate the need for human decision making, and thus mitigate slow human response times.

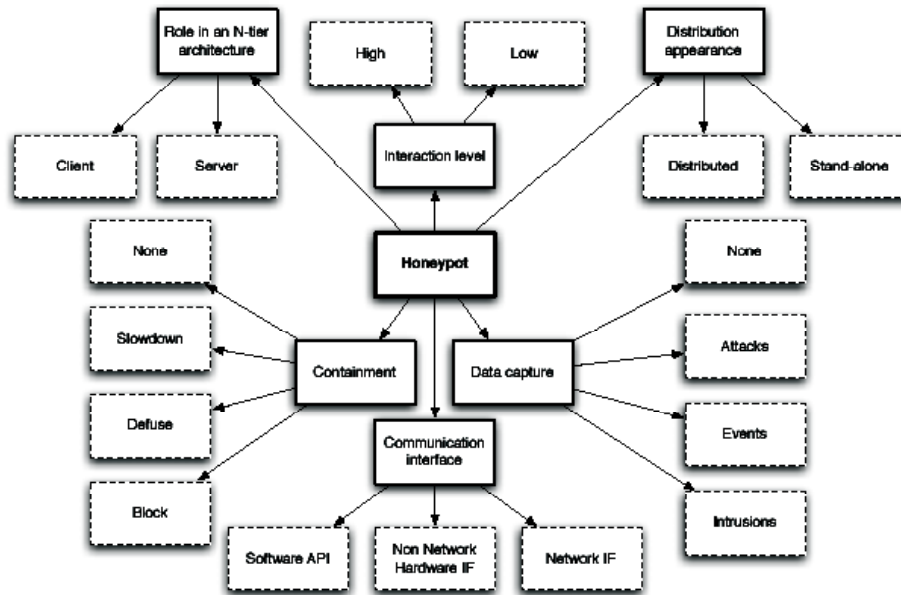


Figure 2. Taxonomy of Honeypot

Architecture of IDS Using Advanced Honeypot

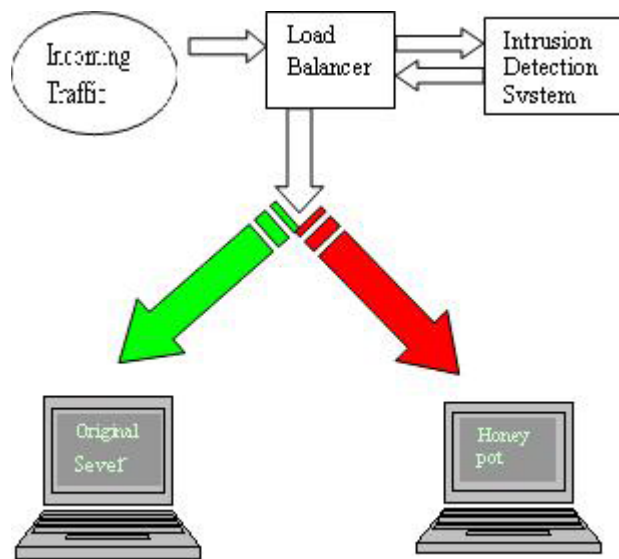


Figure 3. Architecture of IDS using Advanced Honeypot

The activity at each process in the above diagram can be described as follows:

1. The load balancer[3] receives the request to the virtual IP address. If the packet containing

the request has been fragmented, it is reassembled.

2. The Load balancer opens a TCP connection to the IDS Process, and sends the content of the packet (less the headers) over that connection.
3. The IDS process checks the content of the packet against its database of known attacks, and returns a Boolean result to the load balancer over the same TCP connection.
4. On receiving the result, the load balancer closes the TCP connection. If the result from the IDS was "true" (Indicating the presence of an attack) the packet is forwarded to the Honeypot. Otherwise, a server is selected from the active server pool in a round-robin fashion, and the packet is forwarded to the server.

The design of this system entailed overcoming a number of challenges. What these challenges were, and how they were addressed is discussed in the remainder of this section.

Honeypots are a highly flexible security tool with different applications for security. They don't fix a single problem. Instead they have multiple uses, such as prevention, detection, or information gathering. Honeypots all share the same concept, a security resource that should not have any production or authorized activity. In other words, deployment of honeypots in a network should not affect critical network services and applications. A honeypot is a security resource whose value lies in being probed, attacked, or compromised. There are two general types of honeypots: Production honeypots are easy to use, capture only limited information, and are used primarily by companies or corporations; and Research honeypots are complex to deploy and maintain, capture extensive information, and are used primarily by research, military, or government organizations.

<http://www.honeypots.net> Honeypots are increasingly used to provide early warning of potential intruders, identify flaws in security strategies, and improve an organization's overall security awareness. "Honeypots can simulate a variety of internal and external devices, including Web servers, mail servers, database servers, application servers, and even firewalls. As a software development manager, I regularly use honeypots to gain insight into vulnerabilities in both the software my team writes and the OS upon which we depend."

<http://www.windowsitpro.com/Windows/Article/ArticleID/44711/44711.html> A honeypot is a security resource whose value lies in being probed, attacked, or compromised. This means that whatever we designate as a honeypot, it is our expectation and goal to have the system probed, attacked, and potentially exploited. A honeypot also is a detection and response tool, rather than prevention which it has a little value in. (<http://www.securitydocs.com/library/2692>) A better way to think of a honeypot is as an Internet-attached server that acts as a decoy, luring in potential hackers in order to study their activities and monitor how they are able to break into a system.

Honeypots are designed to mimic systems that an intruder would like to break into but limit the intruder from having access to an entire network. If a honeypot is successful, the intruder will have no idea that s/he is being tricked and monitored. Most honeypots are installed inside firewalls so that they can better be controlled, though it is possible to install them outside of firewalls. A firewall in a honeypot works in the opposite way that a normal firewall works:

instead of restricting what comes into a system from the Internet, the honeypot firewall allows all traffic to come in from the Internet and restricts what the system sends back out. By luring a hacker into a system, a honeypot serves several purposes: The administrator can watch the hacker exploit the vulnerabilities of the system, thereby learning where the system has weaknesses that need to be redesigned. The hacker can be caught and stopped while trying to obtain root access to the system. By studying the activities of hackers, designers can better create more secure systems that are potentially invulnerable to future hackers. (<http://www.securitydocs.com/library/2692>)

Load Balancing

In designing a load balancer[3] for Secure Direct we have three main focuses, namely, to provide High-Availability by handling hardware failure in the web-cluster, maintain high speed access to the cluster, and ensure the balancer itself does not become a security hole. High availability is achieved by simply pinging the servers at regular intervals, and removing them from the server pool if no response is received.

The second challenge is to secure the load balancer. Our strategy is to protect it from any irrelevant traffic. Only traffic to a specific port on the virtual IP will be processed by the load balancer and any other malicious access is simply ignored. The load balancer uses a technique known as 'Proxy-ARP' to respond to ARP requests from the router to the virtual IP address.

The web servers have their loop back interface3 configured with the virtual IP address, but are set not to respond to ARP packets. This, at the network layer, there is no way to tell which servers are configured with the virtual IP.

The load balancer process is implemented as a multi-threaded process in Java. The main thread is responsible for reading packets off the wire and if they are destined to virtual IP and their destination port is our desired service port, it hands them to the control thread. The control thread then communicates with the IDS process and decides to pass the packet to the production servers or direct it to the Honeypot.

In case of TCP applications, after redirecting a request to a server, the load balancer process should hold the information about which request is forwarded to which server in order to forward all of the ACK packets in a particular session. We keep the information about each connection in a table. As the load balancer only passes the traffic from client to server, it is unable to see the last FIN sent by the server, and therefore there is no way that the load balancer can find out when the conversation between two hosts is over. Therefore we define a time stamp for each connection. Each time a packet is received on a connection its time stamp is updated. The connections will be removed from the table if its time stamp is not updated for a certain amount of time (which has been set at arbitrarily at 4 minutes during our tests).

Intrusion Detection

Internally, the implementation of the IDS portion of Secure Direct is very simple. The IDS process runs as a concurrent TCP server, and listens for client requests on a specified port. When a connection is made, the IDS fork a child process when receives the content of the packet, and then checks it against a database of known attacks. It then returns the result of

this check to the load balancer process, which makes the decision on whether to forward the request to the production server cluster, or the Honeypot.

The multithreaded design of the load balancer ensures that multiple requests from a client will not get 'mixed up'; however, it is possible that an attack would occur from a single IP at the same time as a valid request. In this case, the initial, harmless packets may be safely forwarded to the real servers until the IDS process finds the attack-packet and detects the signs of intrusion. At this point, it immediately informs the load balancer process to discontinue forwarding packets to the real server, and to send an RST packet to the corresponding server to end the connection. Thus, the server will never receive the attack. In the attacker side, observing silence from the server side causes it to assume the server has crashed and possibly causes it to try to re-connect. However from this point, after detecting the intrusion, all the incoming traffic from the attacker's IP will be forwarded to the Honeypot.

One of the key points in maintaining speed of this system is that, once an IP is recognized as an Attacker IP, packets coming from that source are not passed to the IDS process any more. The load balancer process directs the incoming traffic from attackers to the Honeypot.

The TCP Layer

Secure Direct is implemented for applications that use TCP/IP as their transport protocol. Secure Direct is designed (like any good security product) to be failed-closed system, which means if it crashes, it is no longer possible to access either web server through the virtual IP. Consequently the attackers can not crash Secure Direct and access the unprotected system.

One of the major challenges for Secure Direct is to deal with attackers who try to fool the system by forcing it to analyze the packets inconsistent with what is received in the end-system. In the cases that the intrusion detection system runs at the different host-OS than the end-system, this can be a serious concern. The attacker can take advantage of differences between the IDS and the end-system in dealing with the packets that do not fully comply with the standard protocols, and send some packets that are discarded by the end-host but accepted by the IDS, or vice versa. If Secure Direct uses TCP/IP, the inconsistency between the IDS and the end-host may appear in IP level or TCP level [5]. TCP protocol uses sequence numbers to preserve the order of the incoming packets. The end-system waits until it receives all the sequence numbers required for re-assembling the data. If there is a missing sequence number, the end-system will not accept the consequent packets and waits until it receives the packet with the sequence number it is waiting for. Therefore one way to try to fool the system is to send two packets with the same sequence numbers, one containing false data to be accepted by the IDS and discarded by the end-host, and the other one containing the attackers desired data to be accepted by the end host, and skipped by the IDS. Thus, whenever it detects two different packets with the same sequence number (and a sane checksum) for one connection, it considers it as an attack and prevents the load balancer from sending that packet to the end-host. Furthermore it marks the source IP of this packet, as an attacker IP, causing the load balancer to forward all the consequent packets originated from this IP to the Honeypot.

An alternative way to break into the system is using IP fragmentation, hoping that IDS and the end-host follow two different methods for re-assembling IP fragments. Secure Direct however re-assembles the IP fragmented packets in the load balancer and forwards the assembled packet to the end-host. Therefore what IDS analyzes is completely consistent with what end-host sees. This type of implementation should drastically reduce the chances of an attacker breaking into the system.

Experimental Results

I chose Windows 2003 Server and professional systems with a 2.0GHz processor and 512 MB of RAM with a CDROM drive. Windows 2003 was the best choice to since it can be secured the most from the operating systems I had available to chose from, Windows XP, Windows 2000 Server and Windows 2003 Professional. .To archives the findings for evidence if needed and also to see if a pattern would develop over time to the probability of an attack and what type of attack.

The experimental results we describe the detail of this experiment conducted with network simulator NS2 and configuration of a system 3.0GHz processor and 512 MB of RAM.

Test Environment

A simple test environment requires a minimum of 3 servers and 4 IP addresses. Each server is assigned a single IP address for basic TCP/IP connectivity, while the fourth is used as a virtual IP, which will be accessed by clients, and balanced by the balancer to either of the two servers depending on the contents of the client request.

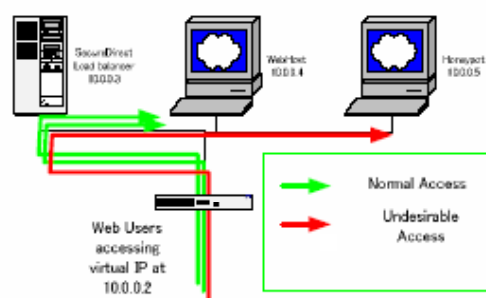


Figure 4. Test Network Environment

Some intrusion correlation systems do not use a raw data stream (like network or audit data) as input, but instead rely upon alerts and aggregated information reports from IDSs and other sensors [20, 21]. We need to develop systems that can generate realistic alert log files for testing correlation systems. A solution is to deploy real sensors and to “sanitize” the resulting alert stream by replacing IP addresses. Sanitization in general is difficult for network activity

traces but it is relatively easy in this special case since alert streams use well defined formats and generally contain little sensitive data (the exception being IP addresses and possibly passwords). Alternately, some statistical techniques for generating synthetic alert datasets from scratch are presented by [16].

IDS testing efforts vary significantly in their depth, scope, methodology, and focus. The characteristics of some of the more developed efforts listed in chronological order. This demonstrates that evaluations have increased in complexity over time to include more IDSs and more attack types, such as stealthy and denial of service (DoS) attacks. Only research evaluations have included novel attacks designed specifically for the evaluation, evaluated the performance of anomaly detection systems, and generated curves. Evaluations of commercial systems have included measurements of performance under high traffic loads. Traffic loads were generated using real high-volume background traffic mirrored from a live network and also with commercial load testing tools. The remainder of this section provides details concerning all the evaluations, as well as for a few other more limited evaluations. Evaluations of research systems are described first, followed by descriptions of commercial system evaluations.

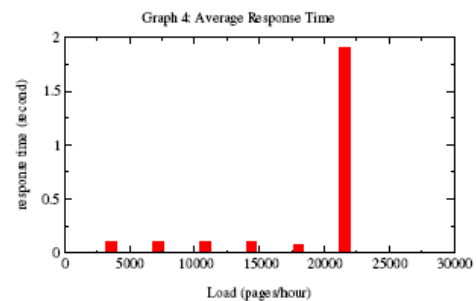
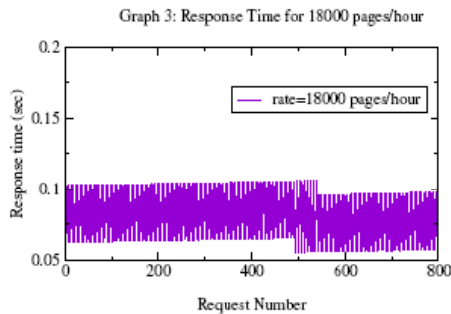
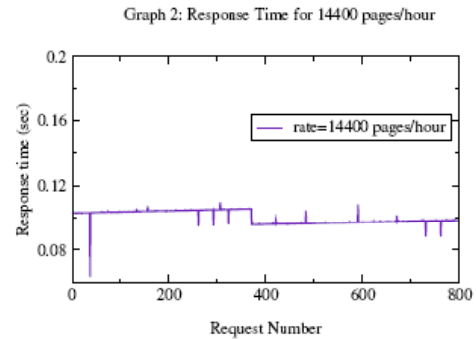
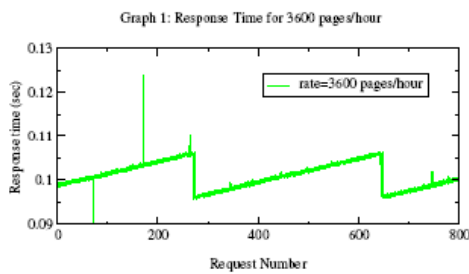
The load balancer itself doesn't gather any information internally, the addition of a Network Based Intrusion Detection System (NIDS) on the network can be used to perform this task, while the intruder is harmlessly attacking the Honeypot server.

However, some difficulties exist when using this approach:

1. Sanitization attempts may end up removing much of the content of the background activity thus creating a very unrealistic environment.
2. Sanitization attempts may fail causing an accidental release of sensitive data. This scenario is very possible since it is infeasible for a human to verify the sanitization of a large volume of data. We feel that this risk is one that most organizations will not tolerate for the sake of a research project.
3. Since attacks have to be injected somewhat artificially into the sanitized data stream (regardless of the method used), the attacks will not realistically interact with the background activity. For example, buffer overflow attacks may be launched against a web server and cause the server to crash, but normal background requests to the web server may continue. This lack of interaction between the attacks and the background activity could be a problem when testing IDSs.
4. When sanitizing real traffic, it may be difficult to remove attacks that existed in the data stream. If one is merely testing hit rates, then having unidentified attacks in the data is an inconvenience but not a major problem. However, having unidentified attacks in the background activity would pose a problem for any false positive testing. Further, sanitizing data may remove information needed to detect attacks.

Results

While the basic functionality of a content-based load balancer is relatively easy to achieve, such a system is only useful to the extent that it is scaleable and stable under load. At a modest load, the balancer showed very stable performance:



Conclusions

In this work, we have described some of the previous efforts to measure IDS, and we have outlined some of the difficulties that have been encountered. We believe that a periodic, comprehensive evaluation of IDSs could be valuable for network managers, information security officers and data managers. However, because both normal and attack traffic are so variable from site to site, and because normal and attack traffic evolve over time

Solving the problem of high availability and security simultaneously offers the opportunity for more reliability than systems which solve the problems separately, in addition to being easier to implement, and offering increased opportunity for recording and data analysis.

The integration of these two technologies, however, is a non-trivial task. A fine balance must be achieved between speed and robustness of IDS features – it is equally bad to have the web server crash because an attack was missed, or drop large amounts of traffic due to an overly through IDS becoming a bottleneck. Additionally, while a content-based load balancer offers many advantages over separate Load Balancing and IDS solutions, it also suffers from the drawbacks of both.

It has been said that the three things most important to a server manger are Security (the ability to withstand hacking), High-Availability (the ability to withstand hardware failure), and low-latency (the ability to service requests quickly). With the current implementation of secure direct, the first two criteria, security and high availability, are satisfied. In regards to latency, our experiments have (once again) shown that there is a trade-off between security and performance.

While improving the efficiency of the programming can mitigate this problem to an extent, the trade-off is certain to remain, and choosing the right balance will likely continue to be a difficult task for the system administrator. It is the authors' opinion that this type of system could provide a much needed additional security tool, however, a good deal of streamlining work remains before it could be widely deployed.

ACKNOWLEDGMENT

The Success of this research work would have been uncertain without the help and guidance of a dedicated group of people. I would like to express my true and sincere acknowledgements as the appreciation for their contributions. I also express my sincere thanks to Dr. Ajay Sharma, Director General, KIET, Ghaziabad, India and Prof. Verges Mudamattam, Director, ISBAT, Kampala, Uganda, East Africa, for their encouragement and support.

References

- [1] The HoneyNet Project. Know Your Enemy : HoneyNets (May 2005) <http://www.honeynet.org/papers/honeynet/>.
- [2] Clifford Stoll. Stalking the Wily Hacker. Communications of the ACM. pp 484- 497. 1988.
- [3] HoneyNet Research Alliance. Project HoneyNet Website. Retrieved May 16th 2003 from the World Wide Web: <http://project.honeynet.org>
- [4] Computer Emergency Response Team. dtscpd Exploit Advisory. Advisory CA-2002-01 Exploitation of Vulnerability in CDE Subprocess
- [5] Balance, An open Source Load Balancing TCP Proxy: <http://balance.sourceforge.net>
- [6] BigIP: <http://www.bigip.com/bigip/>
- [7] J.E. Balas and C. Viecco, "Towards a Third Generation Data Capture Architecture of Honeypots," Proceedings of the 6th IEEE Information Assurance Workshop, West Point (IEEE, 2005)
- [8] Bruce Schneier, Deceits and Lies: Digital Security in a Networked World, Wiley Publications, 2005
- [9] Hogwash: <http://hogwash.sourceforge.net/>
- [10] HoneyPot Project: <http://www.honeypot.org>
- [11] ManTrap: <http://www.recourse.com>
- [12] Martin Roesch, Snort- Lightweight Intrusion Detection for Networks, Proceedings of LISA'99 : 13th System Administration Conference, Seattle, Washington USA, 2005
- [13] Pen A load balancer for simple tcp based protocols such as http or smtp for Unix: <http://siag.nu/pen/>
- [14] Thomas Ptacek, Timothy N. Newsham, Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection, Technical Report, Secure Networks Inc. 2000
- [15] The HoneyNet Project. Know Your Enemy : Sebek (November 2003) <http://www.honeynet.org/papers/sebek.pdf>.
- [16] Haines J.A., Rossey L.M., Lippmann R.P., and Cunningham R. K.. Extending the DARPA Off-Line Intrusion Detection Evaluations in Darpa Information Survivability Conference and Exposition (DISCEX) II. 2001. Anaheim, CA: IEEE Computer Society.
- [17] Lance Spitzner. Honeypots: Tracking Hackers. Addison-Wesley, Boston. 2002.
- [18] Kinsella, J. (January 2005). Build a PC Honeypot. Retrieved November 5, 2005, from Windows IT Pros Website: <http://www.windowsitpro.com/Windows/Article/ArticleID/44711/44711.html>
- [19] Noordin, M. (November 5, 2004). Honeypots Revealed. Retrieved November 5, 2005, from Security Docs. com Website: <http://www.securitydocs.com/library/2692>
- [20] Vigna G., Kemmerer R.A., Blix P. "Designing a Web of Highly-Configurable Intrusion Detection Sensors", Recent Advances in Intrusion Detection (RAID 2001), Davis, CA, October 2001.
- [21] Valdes A., and Skinner K. "Probabilistic Alert Correlation", Recent Advances in Intrusion Detection (RAID 2001), Davis, CA, October 2001



Ram Kumar Singh [M.Tech.(Comp. Sci. & Engg.), B.Engg. (Electronics and Communication Engg.), CCNA, Polyt Echnichnic Diploma in Computer Science] is Senior Lecturer and CISSP Trainer in Department of Information Technology, International School of Business and Technology, Kampala,Uganda. His research area is Network Security and Information Security.

Prof. T. Ramanujam is Director of Krishna Institute of Engineering and Techology, Mohan Nagar, Ghaziabad, U.P., India.



7/25 - 7/26, 2009 Las Vegas, NV

7/27 - 7/28, 2009 Las Vegas, NV

Black Hat

9/1 - 9/4, 2009 Panama City, FL

Special IAM/IEM Bootcamp - SecureInfo

9/15 - 9/16, 2009 Tempe, AZ

9/20 - 9/22, 2009 Miami, FL

Special IAM/IEM Bootcamp - Hacker Halted

The IAM is a two-day course for experienced Information Systems Security analysts who conduct, or are interested in conducting, INFOSEC assessments of information systems using NSA's methodology. It is a high-level, non-intrusive process for identifying and correcting security weaknesses in information systems and networks.

FREE 1 Year license to the SAINT Vulnerability Scanner just for attending any of our courses!

To register for one of these courses or to get additional information, please contact us at:

(719) 488-4500
info@securityhorizon.com
http://www.securityhorizon.com



We speak CVE®!

The INFOSEC Evaluation Methodology (IEM) is NSA's hands-on process for conducting evaluations of customer networks utilizing common technical evaluation tools. Students can expect to learn an easily repeatable methodology that provides each customer a roadmap for addressing their security concerns and increasing their security posture.

7/25 - 7/26, 2009

Las Vegas, NV

7/27 - 7/28, 2009

Las Vegas, NV

Black Hat

9/1 - 9/4, 2009

Panama City, FL

Special IAM/IEM Bootcamp - SecureInfo

9/17 - 9/18, 2009

Tempe, AZ

9/20 - 9/22, 2009

Miami, FL

Special IAM/IEM Bootcamp - Hacker Halted

To register for one of these courses or to get additional information, please contact us at:

(719) 488-4500
info@securityhorizon.com
http://www.securityhorizon.com

Budget Tight? Need to get training and gain new knowledge? Consider attending the NSA IAM and/or IEM at one of the following locations and receive a free pass to the associated conference.

HackerHalted USA 2009, Miami FL
Training: September 20-22, 2009
Conference: September 23-24, 2009

Techno Forensics 2009, Gaithersburg MD
Training: October 21-24, 2009
Conference: October 26-28, 2009



The 2009
Techno Forensics &
Digital Investigations
Conference

GAITHERSBURG, MARYLAND • OCTOBER 26 - 28, 2009

Mapping Your Wireless Signal

Welcome back, Noobs! This article is the first in a series designed to introduce you to several basic wireless security activities: signal strength mapping, and WEP cracking. By working through these exercises, you will gain a better understanding of wireless security and the tools and techniques used.

So, you have a wireless access point in your home. Have you ever wondered how far your router's signal emanates? Organizations have an interest in knowing where their wireless signal is in order to identify security risks. This exercise is going to show you how to map your own wireless signal using freeware and some readily available hardware, as well as introducing you to a Linux operating system and its Terminal window.

Required hardware:

A laptop with wireless access

A wireless adapter with a chipset that is capable of rfmon (I use an Edimax ew-7318usg)

Required software:

Linux OS (I use Fedora Core 10)

Kismet

Google Earth

Optional:

I use a nifty contraption called "Connect-a-Desk," available from www.Thinkgeek.com. You strap it on much like a backpack, the difference being that it gives you a flat surface for your laptop that you place in the front rather than on your back. You look like an uber geek walking around your neighborhood with a laptop attached to you, but it gives you the ability to operate your laptop without having to use one hand to carry it.

Another thing to consider is having a friend assist you. You will be looking at your laptop screen to note the changes in your wireless signal strength as you walk. An assistant can mark the signal locations on your map print-out, as well as help you avoid walking off a curb or into a tree (which I would have rapidly done if it weren't for a friend assisting me!).

So, before beginning, let's cover a few basics. First off, the most important aspect to consider when testing your wireless signal strength is your wireless adapter. This needs to be stressed due to the fact that some wireless adapters aren't as capable as others. You want to look for an adapter that is capable of "monitor mode" or rfmon. Atheros-based cards, Prism-based cards, and Ralink-based cards are very popular for the exercises I will cover in this series because they support rfmon. To find a wireless card suitable for your tests, check out madwifi's website and determine which wireless cards are compatible.

The next thing to address is Kismet. Kismet is a free, open source wireless network detector, sniffer, and can also be used as an intrusion detection system. Kismet can detect other wireless networks within range and report valuable information, including the SSID and MAC address. Kismet is also capable of channel hopping and decloaking hidden network SSIDs. The biggest advantage of using Kismet is its ability to operate in rfmon mode; this enables a computer with a wireless adapter to monitor all traffic received from the wireless network. Compared to promiscuous mode, which has to associate itself with an access point (AP), rfmon mode can capture packets without having to associate with an access point. This means Kismet can capture all packets covered by the 802.11 protocols, including ad-hoc, infrastructure, etc. Rfmon only applies to wireless networks, while promiscuous monitoring applies to wireless and wired networks. Rfmon is the magic ingredient that allows Kismet to sniff packets; it enables us to capture all the packets within range of the wireless adapter, not just those of the access point. Rfmon is also what allows Kismet to run passively, sniffing packets without being detected. All you need is a wireless adapter containing one of the aforementioned chip sets (madwifi, Prism, and Ralink are a few); these cards are capable of running in rfmon mode. These features make Kismet an ideal tool for wardriving and what I call "warwalking," which is what you will be doing in this exercise.



When used in conjunction with a supported GPS device, Kismet can assign GPS coordinates to detected APs. This enables us to use a number of tools to map out APs and even map out the signal strength of our own AP. GPSdrive, for example, will map Kismet data. There are also a number of scripts that will translate Kismet data onto a Google Earth map. In this exercise, however, we aren't using a GPS device in order to keep the cost down.

Let's get started! First, go to Google Earth to print out a map of your location. If you don't have Google Earth downloaded, you can download it from www.googleearth.com. Or you can use a map from your favorite mapping site. Be sure to make your map large enough to give you a graphic representation of your wireless signal. For example, if you live in a house, make sure you include the surrounding areas where you suspect your wireless signal reaches.

Next, you must download and install Kismet. Recall that these instructions are for Fedora Core 10. If you are using another Linux OS, use the applicable command for installing software.

- In the Terminal window, enter **yum install Kismet**
- When prompted for confirmation, enter **y** for yes. Kismet will automatically install in `/etc/Kismet`

Next, you must install the driver for the wireless adapter. Recall that I used an Edimax adapter, so these instructions apply to that specific adapter. The Edimax adapter contains a Ralink

chipset. You must download the driver for this chipset.

- At the time of this writing, I was able to download the driver from the following web site: <http://www.ralinktech.com/ralink/Home/Support/Linux.html>
- Click on the **RT2501USB (RT73 : RT2571w/RT2573/RT2671)** driver link. An **Archive Manager** window will appear. Click the **Save As** radio button. That driver will now be saved in **root/Download**
- In the Terminal window, cd to **/Download**, where you should see the driver file.
- Enter **tar -xvf** and the **file name of the driver file**

Next, you must configure Kismet to use the Edimax adapter. All configurations occur in the Kismet.conf file. The first thing to do is determine which source your laptop is using for the adapter. My laptop used wlan0, but if you're not sure, run the command **iwconfig** in the Terminal window. This will tell you if your adapter is using wlan0, wlan1, ra0, etc. Make note of the results as you will need this information for the Kismet.conf file.

- In the Terminal window, enter **vi /etc/Ksismet Kismet.conf**
- Scroll through this file so you are familiar with its contents. Make the following changes to the file:
 - o **Change suiduser = Kismet**
 - o **Change networkmanagersleep=true**

The next change is where you will use the results of your iwconfig query. The first portion of the "Source" statement is the driver. The second portion is for the wireless source. As I noted, my adapter used wlan0. The last portion is for the name of the adapter.

- **Source = rt73,wlan0,Edimax**
- **wq!** to save the changes to Kismet.conf

Now test that you configured Kismet correctly. In the terminal window, enter **start Kismet**. If everything was configured correctly, the Kismet window will open and Kismet will begin searching for SSIDs. Otherwise it will post an error message. If you did not list the correct wireless source, you will see an error similar to "wlan0 not recognized." Google is a great source for resolving any Kismet configuration errors. If you are getting errors, just search for the error for your particular environment. And remember that while frustrating, trouble shooting is a great learning experience for noobs on configuring and using a standard security tool.

Assuming all went well, you should see your Kismet window, and you should see it populating the space with discovered SSIDs. A note for those of you in heavily populated areas: if there are a very large number of SSIDs being discovered, you may want to limit Kismet to only discovering SSIDs on your own channel, otherwise your system might hang. This happened to me when mapping a signal in a densely populated area consisting mostly of apartments. Kismet rapidly discovered hundreds of SSIDs and caused my system to hang. The default channel on most residential wireless access points is 6. To lock on to one channel, arrow up or down to highlight your SSID and enter **Shift-L** to lock on to that channel. This can be tricky, as

the item you highlighted might change as more SSIDs are discovered, so make sure you are indeed locking on to the correct channel. Also note that pressing the “h” key while in Kismet will open the list of key commands Kismet uses.

Once you have your SSID highlighted, you are ready to begin your warwalk. Bring your map print-out and a writing utensil. Start Kismet by entering **start Kismet**. You can sort the data by SSID by entering “s.” Expand the window until you see the Signal Strength column by clicking and dragging on the window border. Kismet indicates signal strength with “x.” A strong signal strength will look like this: **xxxxxxx**. Conversely, low signal strength will look like this: **x**. If there is no signal strength, you won't see any x's.

Begin walking around your location and note the changes in your signal strength. When the signal strength gets low, walk one step away from your location and see if the signal disappears. If it does, that may be the point where your signal drops off. To confirm this, take one step towards your location. If the signal returns, you can mark that spot on your map. Continue with this process until you have mapped your signal. Keep in mind that things like buildings, glass windows, temperature, and weather conditions will affect your signal strength. Once you're finished, connect the dots on your map and you have an idea of your signal map!

So how does this apply in the real world? Well, look at your map. Does your signal cover other homes, buildings, etc. where other users likely have wireless access points? If you're using WEP encryption or, worse, no encryption, those users could crack your encryption and/or use your access point. Organizations care about their wireless signal map for these very reasons. While the average home user will likely not have a router that lets you “tone down” the signal, large organizations could modify their access points to minimize their signal emanation. The bottom line is that if an attacker can get within range of your signal, they could attempt to crack your key and sniff your web traffic, potentially compromising the confidentiality, integrity, and availability of your data.

That concludes this exercise! The next article in this series will address WEP cracking, so stay tuned, Noobs!



Dana Rollins is a security consultant with Security Horizon. She may be reached at drollins@securityhorizon.com

... to Take Necessary Security Precautions?

~ The following is the first half of a two part article. ~

Telework--the practice of using off-site or portable computers to perform company or agency-related duties--has become increasingly commonplace during this first decade of the 21st century. This ever-growing use of telework is convenient and popular with workers but the jury is still out on whether it increases productivity. Telework arrangements can, however, have significant implications on an organization's data security and information technology operational strategies. A greater reliance on telework raises numerous information security concerns, including everything from breaches of confidentiality, increased opportunities for unauthorized viewing of data, data theft, and data leakage. Is there a solution? As the need for flexible work arrangements continue to be an important factor for workforce management, this article will highlight for management to have clearer understanding of how security policy are received, perceived by their end users, and the use of technology for organization data protection.

Telework is undoubtedly on the rise, especially for Government agencies. Because it is a mandated program, Federal employees are almost three times as likely as private sector employees to have an option of working from home. Until recently many Federal teleworkers had no choice but to use their own computers and equipment simply because some Government agencies either could not afford to supply their teleworkers with secure, Government-issued models or were not willing to take on the expense or complications involved. However, it is becoming increasingly more evident that the price of the equipment is minimal compared with the cost of dangerous security leaks that occur as a result of using non-secure, unauthorized technology.

To address the problems related to telework data security, some key terms must be adequately defined. In general, teleworkers are employees who work outside of the official workplace by way of a technological connection during regularly scheduled work hours—at home or an alternative workplace—on full-time, part-time, or situational basis. Non-teleworkers are considered employees working at the official workplace during regularly scheduled work hours. An unofficial teleworker is an employee who works at an official workplace, yet also performs work-related duties off-site on nights or on weekends.

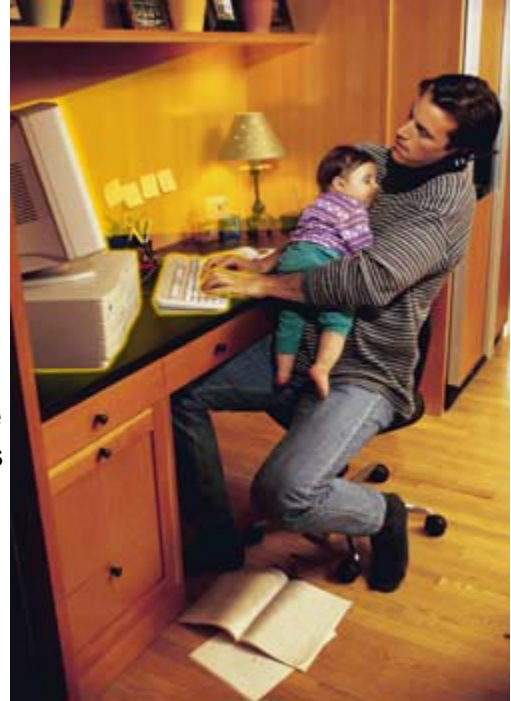
Teleworkers use various client devices, such as desktop and laptop computers, cell phones, and personal digital assistants (PDAs) to read and send e-mail, access Web sites, review and edit documents, or perform other tasks. Most teleworkers use some type of remote access to an organization's resources and data from locations other than its facilities. In many instances, teleworking has become an extension of mobile working, rather than being simply one or a few workers based outside the organizational perimeter and accessing the network from time to time. Organizations now have both teleworkers and mobile workers and require support for information technology devices.

Which Factors Motivate Teleworkers, cont.

tim godlove

The ability to be productive outside traditional office hours means that work can be extended in the dimension of time, and the fact that it is possible to work outside the office means that work can also be extended in the dimension of space. As the temporal and spatial territories of office work are being extended, so too are the boundaries of the organization. Certain items of technology, which we call work extending technology (WET), facilitate expansion of an organization's borders. Mobile phones, laptops, and BlackBerry devices provided to staff make working anywhere at any time quite simple, thereby affecting the traditional boundaries between two separate spheres or experiential categories identified as "home" and "work."

Telework has a critical attribute that differentiates it from other types of work organization, and of portable information and communication technologies allows it to be "delocalized." In other words, work is free from the confines of a particular physical work environment. The growth of the new technologies has created a distinct phenomenon: when a corporate identity requires only an e-mail address and a Web site, there is no need to be physically based in any particular location. In the course of a day, work can be conducted in a home, in a car, at a client's office, in a restaurant or café, walking on a street, on a park bench—literally anywhere. The convergence of the computer, television, and telephone allows these communication tools to offer increasingly broad coverage.



http://www.telerepsathome.com/telecommute_dad.jpg

The social meanings of home and work environments are beginning to merge as they become informationally similar. Convergence, a seemingly benign term, entails a whole host of technological dependencies that affect our daily lives. In the context of telework it implies an increasing lack of differentiation between our work lives and our domestic lives.

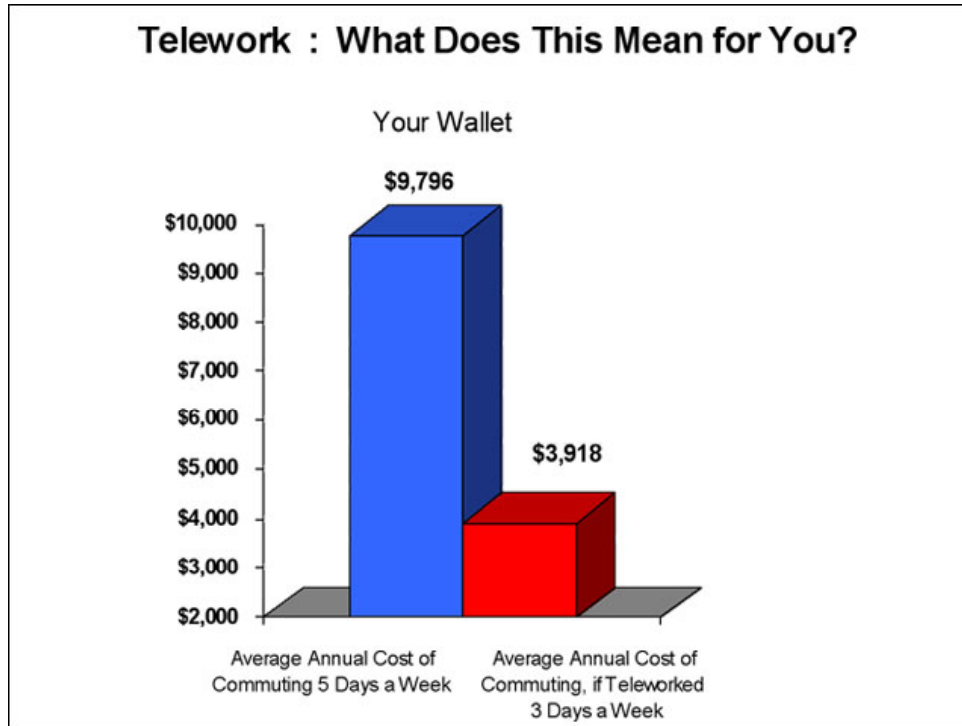
Challenges

Teleworkers--official and unofficial--present unique challenges for an organization due to the information technology needed to provide them with a secure working environment while implementing security controls. Yet despite the ongoing information security issues related to telework, as shown in the chart below, the purported cost- and time-savings are making it an increasingly popular choice in Government agencies.

In fact, there is currently an attempt to make telework an even more significant part of the Federal workforce, by introducing H.R. 4106, which is the Telework Improvement Acts of 2008 bill and if enacted would mandate the option of a telework arrangement unless an agency can prove that such an option was not viable. H.R 4106 would also require that Federal agencies incorporate telework into the continuity of operations planning and for mission critical personnel

Which Factors Motivate Teleworkers, cont. *tim godlove*

to be equipped to telework in time of a catastrophe.



Source: Auten, C. (2008, March 3) Ready, set, go: How to put telework in the fast lane, eWeek.com, <http://www.eweek.com/c/a/Enterprise-Applications/Ready-Set-Go-How-to-Put-Telework-in-the-Fast-Lane/>

In fact, there is currently an attempt to make telework an even more significant part of the Federal workforce, by introducing H.R. 4106, which is the Telework Improvement Acts of 2008 bill and if enacted would mandate the option of a telework arrangement unless an agency can prove that such an option was not viable. H.R 4106 would also require that Federal agencies incorporate telework into the continuity of operations planning and for mission critical personnel to be equipped to telework in time of a catastrophe.

There are several reasons why the Government is pushing for more teleworkers. Telework offers substantial savings of physical facility related costs including rent, storage, electricity, including decreased energy consumption and less traffic (resulting from eliminating the need to drive back and forth to work), as well as a greater level of personal contentment for employees who are not forced to deal with the stresses of office life. This is, of course, is expected to result in greater productivity. Opportunities for productivity improvements as workers no longer suffer from the tiredness associated with physical commuting and are removed from many of the distraction of a traditional office. Telework has our interest in the potential for a dramatic shift in the workplace and work process based on evolving telecommunication technology--the history of the world is the history of change.

Telework has caused the line between personal time and work time to become blurred in such

Which Factors Motivate Teleworkers, cont. *tim godlove*

a way that it seems natural for a person to take care of personal business at a time when the person should be taking care of work business. Telework brings the public domain (work) into the private domain (home). This raises a number of issues for teleworkers, for example, the importance of separating being at work from the family time. This, of course, results in a decrease in productivity and also raises the problem of requiring a workforce that is highly self-motivated – something that is often easier said than done.

As a theoretical construct, telework works well. However, a problem in its application exists in that expansion of teleworking employment arrangements can have significant implications on an organization's data security and information technology operational strategies. Increased reliance on telework increases risks for information security.

Security threats in a telework infrastructure are often related to the computers literacy of the teleworker accessing the network rather than the actual corporate network. Or computer-savvy teleworkers who link an organization's laptop to high-speed cellphone networks simply to avoid paying for special cards and service plans because they are able to easily access Wi-Fi hot spots when at home or traveling. In addition there is that unknown activity by employees at home, when information can be damaged, copied, or simply assessed in an unauthorized manner. And unethical employees can engage in activity against the business's best interests.

Information technology departments do have less control and oversight of remote users. Most organizations have facilities with physical control safeguards in place for onsite employees. Other concerns, who is also in the teleworkers home and what are their intentions, shoulder surfing watching entered IDs and password? Who else has access to the company equipment and the data being used, do children play on the equipment and able to access the organizations network?

With the increased benefits afforded by teleworking come increased information security risks. When taking into account the negative aspects of information security concerns and combining them with the questionable benefits of increased productivity, a question can be posed about why telework is on such a steady rise. When a teleworker combines personal business and office business on the same computer, not only do lines between personal and business matters blur, but more importantly, information security can be more easily compromised. A sophisticated intruder may find it easier to attack the laptop of a teleworker logged on to the corporation network than attacking the corporation network itself. The results are very costly and damaging to the reputation of the organization.

With the lines between work and home becoming increasingly blurred, some of the most challenging questions faced by organizations relate to the difficulty in identifying and assessing the continued information security risk and the need to develop and implement effective information technology security controls to secure the data of employees who work from home with permission and without permission.

Which Factors Motivate Teleworkers, cont. *tim godlove*

References

Antonopoulos, A. M. (2007, October 10) Combining work and play threatens business security. Network World, <http://www.networkworld.com/columnists/2007/101007-risk-reward.html?fsrc=rss-antonopoulos>

Auten, C. (2008, March 3) Ready, set, go: How to put telework in the fast lane, eWeek.com, <http://www.eweek.com/c/a/Enterprise-Applications/Ready-Set-Go-How-to-Put-Telework-in-the-Fast-Lane/>

Ajzen, I. (2005) Attitudes, personality and behavior, Maidenhead, England: Open University Press

Bain, B. (2007, September 13) Justice says no to private PCs for telework, FCW.com, <http://www.fcw.com/online/news/150044-1.html>

Flood, K. (2001, February 5). The forgotten side of network security. Network World, 12, 276-283.

Hines, M. (2007, August 21) Mobile workers still struggling with security; A new study shows that even as the business use of mobile devices increases, many users are unconcerned or uninformed about security issues and practices." InfoWorld, http://www.infoworld.com/article/07/08/21/Mobile-workers-still-struggling-with-security_1.html

Jones, K.C. (2007, November 5) Businesses more concerned about mobile, remote security, but still ignore training, InformationWeek, <http://www.informationweek.com/news/showArticle.jhtml?articleID=202802456>

Kilpatrick, I (2007, November). Dam data leakage at source: how unified encryption management (UEM) is changing the threat landscape, Software World, 12(4).

Lampson, B. (2005). Microsoft, Accountability and Freedom, <http://research.microsoft.com/lampson/slides/accountabilityAndFreedomAbstract.htm>.

Mears, J. (2007, April) Legislation promotes Federal teleworkers; Telework Enhancement Act of 2007 would open more doors to telecommuting. Network World, <http://www.nwwsubscribe.com/news/2007/040307-telework-legislation.html>

National Institute of Standards & Technology. (2007). SP 800-114, User's Guide to Securing External Devices for Telework and Remote Access: National Institute of Standards and Technology.

Sternstein, A. (2007, June 4) Survey: Unauthorized teleworkers a security risk, National Journal's Technology Daily, http://www.govexec.com/story_page.cfm?articleid=37105

~ Look for Part 2 in our next edition! ~



Tim Godlove is currently a doctoral student in the field of Information Assurance Policy with many years as an information technology and security officer both on active duty with the U.S. Navy and in the Federal government. He may be reached through this publication.

Master the ghost in the machine.

Some may dream in code. We program the dreams. Gain comprehensive knowledge of application development, object oriented graphical programming. Conjure your calling as an innovator in the realm with a Bachelor of Science in Software Engineering degree.



Discover yourself and make the software spirits dance. UAT.edu/majors

Artificial Life Programming > Technology Management > Computer Forensics > Game Programming > Network Engineering > Network Security > Software Engineering > Web Architecture > Robotics and Embedded Systems > Digital Animation > Digital Art and Design > Digital Video > Game Design > Game Art and Animation