A PROPOSED FRAMEWORK FOR BUSINESS INFORMATION SECURITY BASED ON THE CONCEPT OF DEFENSE-IN-DEPTH

by

MATTHEW K. BURNBURG

A MASTER'S THESIS

Submitted in partial fulfillment of the requirements for the degree
of Master of Science in Management Information Systems

SCHOOL OF BUSINESS AND MANAGEMENT

UNIVERSITY OF ILLINOIS AT SPRINGFIELD

SPRINGFIELD, ILLINOIS

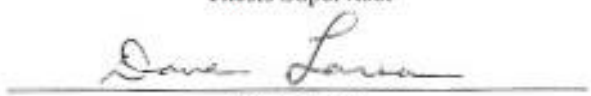
MAY 2003

GRADUATE THESIS ACCEPTANCE PAGE

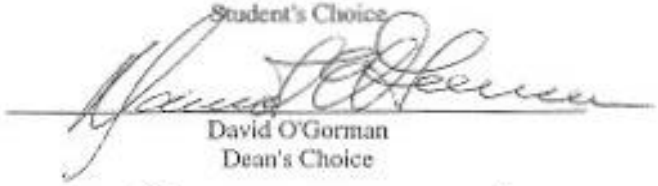
Submitted by Matthew K. Burnburg (ID# 662510527) in partial fulfillment of the requirements for the degree of Master of Science in Management Information Systems.

Accepted on behalf of the Faculty of the College of Business and Management by the project committee:

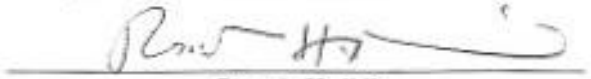
Rassule Hadidi
Thesis Supervisor



Dave Larson
Student's Choice



David O'Gorman
Dean's Choice



Rassule Hadidi
Department Chairperson

6-24-03
Date of Committee Approval

Ronald McNeil, Dean
College of Business and Management

6/27/03
Date of Dean's Approval

ABSTRACT

A PROPOSED FRAMEWORK FOR BUSINESS INFORMATION SECURITY BASED ON THE CONCEPT OF DEFENSE-IN-DEPTH

by

Matthew K. Burnburg

Chairperson of the Supervisory Committee: Professor Rassule Hadidi
Management Information Systems Department

Information systems security is a complex area of study and practice. Communication of security requirements to business executives is difficult due to the highly specialized nature of the field and the accelerating deployment of new technologies. This study proposes a framework based on generally accepted domains of information security and the temporal nature and locality of data and information. The proposed framework also accounts for the small world network characteristics of the Internet. This study evaluates this framework within the context of an operating financial industry network.

Table of Contents

LIST OF FIGURES

LIST OF TABLES

ACKNOWLEDGMENTS

The author wishes to thank the faculty and staff of the University of Illinois at Springfield for their support and mentorship during his time at the College of Business and Management. Specific thanks to Donna Dufner, Ph.D. for the motivation, Ojoung Kwon, Ph.D. for always accepting ideas with an open mind, David O'Gorman, Ph.D. for showing me that everything is complex, and Rassule Hadidi, Ph.D. for allowing me the opportunity to teach. Jeff Noble who created the visualizations of the proposed framework based on my descriptions. Separate thanks are warranted for the anonymous bank president who allowed this author to use internal data for this study. A special thanks to my wife, Cathy, who put up with long hours of not seeing me and always being supportive.

CHAPTER 1
Introduction

It seems unlikely that the Internet or its successor, the Internet II, will not be utilized by organizations of all kinds and individuals for their own purposes. However, the Internet's underlying protocols where designed to be resilient to catastrophic losses not to be secure. The news media continues to report on new types of technology-based crimes. Many of these crimes are facilitated by the Internet. As a result, many organizations and individuals are attempting to implement security to protect information resources and individual privacy. Governments are also attempting to enact new laws or extend old laws to protect individuals and organizations from crime and other activities that may adversely affect confidentiality, availability, and integrity of public, semi-public and private information stores on the Internet and its successors.

> *"Organizations must rely on their own defenses for now. Governments, industry and civil society must work together to develop consistent and enforceable national laws to deter future crime in cyberspace."*
>
> - Bruce McConnell, SC Magazine, April 2001

So, what are the problems associated with securing information assets? There are many levels of complexity associated with that simple question. Most organizational managers and few individuals are equipped with the requisite knowledge to make informed decisions about the adequacy of their security posture. The primary goal of this research is to put forth a framework in which to evaluate the efficacy of layered information systems security. Organizations are on their own from a security perspective, but so are individuals.

Statement of the Problem

The problem with information security processes for any organization is two-fold. First, the field of information security is very complex. Organizational managers outside information technology roles are not knowledgeable of the risks associated with specific technologies. This leads to information systems requirements that may expose the organization to unnecessary risks. Business line managers must have a simple model in order to understand how business decisions affect information technology deployments and the associated risks. Hardly a day goes by without the news media publishing cautionary tales of how company X has been hacked, cracked, or otherwise suffered some information security breach. The constant reporting of security breaches leads to the process of "Management by magazine" (Carson et al. 2000, Lee and Collar 2002). Whatever the latest article in Business Week or Inc. says that other organizations are doing to preserve the security of information resources must be the right thing to do at the executive's organization (Salkever 2000).

The second issue pertaining to information security is deployment of technologies that do not have a baseline of functional testing (Axelrod and Cohen 1999). In many cases, the organization deploys new information technology without considering the security issues. Many organizations also function under the misconception that a single line of defense is sufficient to protect the organization. In the past, user ID and password has been the defense. Today, the defense is some sort of firewall technology… usually the cheaper the better.

This research will focus on a theoretical model of information security applied to a commercial bank and trust company that addresses four basic considerations. First, information security exists within multiple domains. These domains cover everything from the business environment to technology considerations. Second, all data and information resources have a location property that exists in storage and transmission. Third, the model has a temporal quality that changes over time. Data, information, and

technology have a time dependent values. Finally, these factors contribute to the small world network nature of the Internet.

This leads to the following suppositions:

A1. The nature and volume of the hostile traffic will be impossible to predict for any given point in time.

A2. Filtering network traffic will reduce the total number of potential exploits and attacks against a target network.

A3. Filtering network traffic will not completely mitigate application and service attacks based on allowed network traffic.

A4. Use of multiple layers of security can reduce the overall risk of unauthorized access to systems.

A5. The configuration of the computers used to probe and attack the organization will be variable.

A6. The geographic location of the computers used to launch attacks and hostile probes will be much wider than the primary market area of the organization.

Purpose of the Study

The purpose of this study is to examine the efficacy of specific technical countermeasures and security postures at the edge of an organizational network. This study will evaluate the evolutionary security changes within a financial institution's data network with a specific evaluation of how changes to the security architecture have affected the overall security of environment. These changes were made over a seven-month period and in accordance with the proposed framework described in Chapter 2.

No matter what technological security measures are implemented, no matter what policies and procedures are in place, information security comes down to human nature and human beliefs. The field of memetics is useful in describing the spread of beliefs in any culture whether it is the sum total of human culture or the sub-culture known as organizational culture. There are two main views of what memes are and how they spread beliefs. The first view supported by Dawkins (1993) puts forth that a meme is much like a virus and spreads via an epidemiological process. The other main view is proposed by Aunger (2002) and suggests that memes are like genes. A number of memes compose any belief. Memes are spread according genetic replication and general fitness. Either view is acceptable for the purpose of this study in relation to how management beliefs are spread to the organization and become part of the organization's culture. The primary point is that management beliefs impact the organization's culture and drive information security as an overall process.

During the last twenty-four months, the management has changed basic security beliefs of the financial institution three times. The initial belief was "Our organization is too small to draw the interest of a hacker". The key problem with this position is that a significant number of hackers do not care why the organization placed resources on the Internet and wish to use the systems they find for other purposes. This belief changed when a spammer started using the organization's email server to send large quantities of email.

The external use of the email server resulted in the installation of a firewall. This action brought about the second security belief: "My organization has a firewall. We are secure." This belief fails to acknowledge the possibility that the firewall is appropriately configured and has no basic security flaws at an operating system or application level. At this point, an external security assessment was conducted by an independent auditor. The findings of this assessment showed a significant number of issues with the firewall configuration. These issues included a number of TCP and UDP service ports open (i.e. SNMP, RPC, FTP, etc) to the inside network. The external assessment, combined with

the federal and state regulatory agency reviews, brought about the implementation of a comprehensive set of security policies (see Appendix A). The first two beliefs or paradigm shifts required approximately twelve months and changes in the positions of the executive management of the financial institution. However, this brought about the third belief.

The third belief was "My organization has security policies, procedures and technical measures in place today. We are secure." This belief assumes that security measures currently employed have no holes or exploits now or in the future. This particular belief may be the most dangerous for an organization to adopt. In the specific case of this financial institution, this was only dangerous from a regulatory standpoint. The organization went through a regulatory review where the primary finding was that there were no documented internal reviews of the institution's security status. At this point in time (approximately May 2002), the organization has adopted monthly reviews of all relevant security logs and devices and semi-annual reviews of existing security policies and procedures. This institution has adopted the current belief: "Information security is an on-going process that requires continual testing and review".

This project will examine the data generated after the adoption of the final belief. The validity of this examination is based on the fact that changes to the total security framework of the organization were implemented over a six-month period between May 2002 and November 2002. These changes were incrementally implemented offering clear delineations within the data sets.

Significance

Hiltz and Turoff (1993) forecast that the United States would become a "network nation" in the near future. It may have been a better forecast to suggest a "network world". The world's economy continues to move toward an information economy. The value of information (even the raw data) becomes the very lifeblood of any organization. Financial institutions, as well as, many other public and private organizations, use safes,

alarm systems, and security guards to protect physical assets such as important documents, currency or negotiable instruments. However, information security is usually viewed as an evil, unnecessary, or unwarranted requirement by paranoid technologists. One wonders what the executives at Nike thought when they were sued by a small Internet service provider in Scotland because they had inadequate safeguards on their web site (Harrison 2000). Governments are moving to adopt legislation that mandates security processes for critical industries and market sectors. The public is beginning to understand some of the issues surrounding their privacy and demanding that organizations defend their private information and indicate how that information will be used.

Scope

This study will be limited to an evaluation of a theoretical security framework for defense-in-depth applied to a real-world financial institution. This institution was chosen because all the elements of the framework can be evaluated in microcosm.

Assumptions and Limitations

The primary assumption is that there is a credible risk to information systems from external sources. All security processes, procedures, and functions are put in place to assure the accessibility to information by authorized individuals and/or organizations. Human nature, however, always needs to know-especially what the individual is not supposed to know.

Second, the risk and nature of potential attackers increases as an organization moves toward greater connectivity. Today's organizations seek to increase connectivity to their customers, clients, vendors, suppliers, employees, and other stakeholders. This need to increase the capability to communicate is promulgated with the express purpose to improve productivity within the workforce of the organization.

Third, there exists a wide range of vulnerabilities to information systems. Whether an attacker chooses to perform a denial of service attack, send viral attachments, attempt to install Trojans, or simply gain unauthorized access, the tools available to even novices are extremely potent.

Finally, the small-world network nature of the Internet creates a broad range of complexities based on its size, inter-nodal connections, technology deployments, the relative security of other organizations and individual computers and devices with Internet access, human nature, and governmental regulations. These complexities, when taken in total, contribute to the premise that no system or group of systems can ever be totally secure.

Specific assumptions include:

- This project will focus on the technical measures used to create perimeter defenses for a network based on its security policies.
- The evaluated network is considered "high-risk" from a business perspective. The target network is part of the critical national infrastructure (i.e. financial, transportation, energy, etc.) as defined by the United States government.
- A security policy and the attendant procedures have been implemented, but will be subject to review in this project.
- A multilevel anti-virus solution is in place and running on all servers and workstations. All platforms are updated automatically on a weekly basis.
- A backup strategy is in place and is tested on a monthly basis.
- Nature and type of attack(s) are unknown prior to onset.
- As the implemented tactical security measures are implemented, internal network traffic is expected to decrease.

- No assumptions were made during the data collection period in relation to the nature and type of attacks this network would experience.

The principal limitation of this study is that the network under evaluation is an operational network. This limitation prevents the deployment of strategies and technologies that could potentially decrease the overall security risk to the network. In addition, certain technologies cannot be deployed due to budgetary constraints outside the control of this study.

Organization of the Paper

Chapter 2 will evaluate the threats to an organization's information systems infrastructure, the technical countermeasures that can be taken, defense-in-depth strategies, and map appropriate technologies to each layer of a theoretical defense-in-depth framework within the context of a generalized security framework. Chapter 3 will describe the overall architecture of the network to be evaluated and the changes that were implemented during the course of this study. The purpose of this approach is to show that layering various technologies will improve the overall security posture at the edge of an organization's network. Chapter 4 will evaluate the data collected and compare the effectiveness in the prevention of attacks. Chapter 5 gives concluding remarks and suggestions for future work. Several appendices are attached to provide sanitized security policies, technical configurations, and sample data sets.

CHAPTER 2

LITERATURE REVIEW

Why is Information Security Important?

Organizations are continuing to extend their information systems into the Internet. Several reasons for this extension include (Lederer et al. 2001):

- Improving business processes and communications effectiveness with investors, employees, suppliers, and vendors;
- Improving the productivity of the organization's employees;
- Improving the flexibility of the organization (i.e. virtual teams) in response to the changing business environment;
- Improve efficiencies by offering customers the ability to access customized information or place and track orders online.

The extension of private information systems onto the Internet poses several security challenges. First, the act of writing an Internet-based application is relatively easy. However, as is common, application developers very seldom consider security until the end of their project. Schneider (2000) makes the case that application developers should evaluate the total application environment including operating systems, authentication mechanisms, and other supporting programs to uncover the reasons for security lapses during operation. This is not a common meme or paradigm within the client server development community. Most client server environments do not have the same access control or development methodologies that mainframe programmers commonly use. As a result, client server development generally relies upon other authentication subsystems such as network operating systems user ID and passwords (Schneider 2000).

Second, Internet Protocol version 4 (IPv4) is intrinsically insecure. The underlying design was to ensure communications during catastrophic failures (i.e. nuclear war). The

protocol design is robust and capable of routing around failed nodes and circuits, but was not designed to be particularly secure.

Internet Protocol version 6 (IPv6) addresses the security limitations of IPv4 as well as addressing issues, automatic device configuration, quality of service and native multicasting support (Koprowski 1998). However, IPv6 is in limited deployment and generally limited to Intranet networks. At the present time, enterprise networks utilizing IPv6 must maintain IPv6-to-IPv4 enabled devices at the edge of the network (Bound 2001). Consequently, IPv6 vulnerabilities are not generally known to the Internet hackers and crackers.

Third, new technologies are being deployed before their security implications are known. This can lead to "chaotic" operations because an extensive knowledge base does not exist prior to deployment (Axelrod and Cohen 1999). Because there's a risk of failure with unknown technologies, information technology professionals tend to build in redundancy within their systems. This too can lead to unanticipated results.

Finally, business pressures to get new products and/or services to customers shorten timelines for deployment of new applications and services. Under these circumstances, executives tend to look at security as a necessary evil, but not an evil to take too seriously.

The results of these points are seen every day in the headlines of newspapers and trade magazines. New Internet worms are routinely deployed to the Internet causing havoc with email systems and loss of business critical information. Governments seem powerless to prevent the spread of these Internet worms. This is primarily due to a lack of governing international and national law. The European Union is working on a draft treaty on Cybercrime that will require all signatories to institute a variety of laws aimed at curbing Internet-based crimes (Radcliff 2001).

Internet-based attacks against organizations or individuals can be launched from anywhere on the Internet. There are many different types of attackers with many different reasons for launching an attack against a particular individual or organization. From the hacker that wants to learn about the target system(s) to nation states which are attacking a public infrastructure in an enemy state, the result is the same: the confidentiality, integrity, and availability of data may be impacted or lost.

Most business organizations tend to utilize military paradigms to describe how to sell their product and services (propaganda AKA advertising), compete within the marketplace against other vendors (battle plans AKA marketing plans), and how to survive for the long term (Foreign or Military Policy planning AKA Strategic planning).

> *"In strategy as well as in tactics, the defense enjoys the advantage of terrain, while the attacker has the advantage of initiative."*
>
> Carl von Clausewitz, On War

Information systems security is not immune from this trend. One of the first approaches to Internet security at the edge of the network was the Internet DMZ (demilitarized zone). The military definition of a DMZ is "a defined area in which the stationing or concentrating of military forces, or the retention or establishment of military installations of any description, is prohibited" (U.S. Department of Defense 12 April 2001). This implies a buffer zone between opposing forces. However, the Internet DMZ is the battlefield of the organization's Internet connection. It is in the Internet DMZ where the organization prepares its defenses against the unauthorized individuals, organizations, and nations that may attempt to breach security and steal or destroy private information. As von Clausewitz notes, the defender gets to decide where the battle will be fought, but the attacker gets to decide when and how the battle will begin.

Throughout history, mankind has fought countless battles and numerous wars. With each advance in technology, humanity has determined ways to use that 'new' capability to improve the odds of winning. Technology is the great equalizer in human conflict. Cyberspace or the Internet will be no exception. The ability for a small country to have a significant impact on a more powerful enemy has become a reality. Many nation states have already formed or advocate the formation of information warfare groups within their military organizations (Liang and Xiangsui 1999). The only real issue facing organizations and individuals on the Internet is how best to defend themselves. Survivability is the goal. The defense-in-depth paradigm may be the answer.

The military defines defense-in-depth as "the siting of mutually supporting defense positions designed to absorb and progressively weaken attacks, prevent initial observations of the whole position by the enemy, and to allow the commander to maneuver the reserve (U.S. Department of Defense 12 April 2001). From a technological perspective, the military definition evolves into an objective of implementing "defenses at multiple locations [within the network] so that critical enclave resources are protected and can continue to operate in the event that one or more defenses are circumvented (McKenney 2001)."

Why is this level of defense important for organizations? The answer lies in a simple evaluation presented to a business client during a standard security briefing. Many organizations have begun utilizing the Internet to virtualize their offices. Low cost, high speed (i.e. digital subscriber lines and cable access) Internet connectivity is now available to a significant percentage of households in the United States. Organizations are beginning to leverage this capability to move employees out of high cost office locations and back to their homes. The cost savings to organizations and improved employee productivity are significant. However, there are some issues from a security perspective.

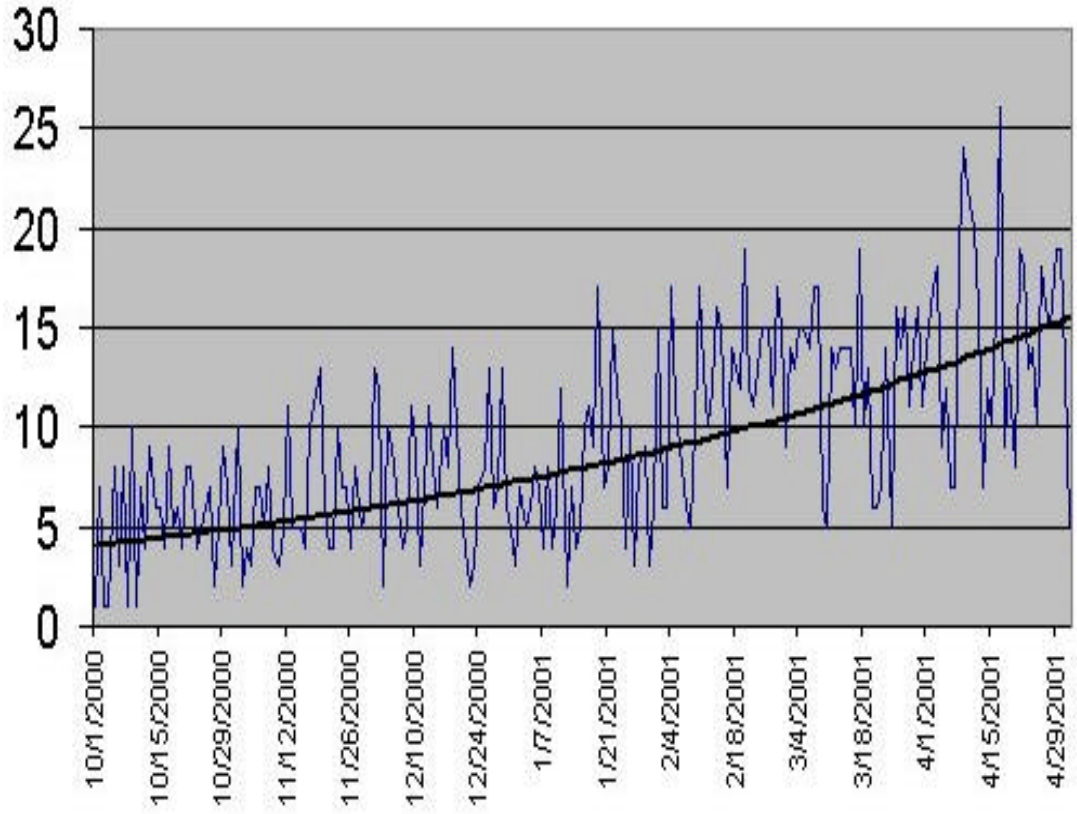


Figure 1 Discrete Attacking Hosts on Cable-Connected Home PC (Burnburg 2001)

Figure 1 shows the number of discrete IP addresses attacking a cable-connected personal computer over a seven-month period. The personal computer that gathered this data was a default installation of Windows 2000 Professional running the personal firewall - Black Ice. This personal computer was not used for any business purpose; its primary function was for surfing the Internet. While the rate of discrete attacking hosts is extremely variable, the exponential trend line shows a general rise over the duration of the data. It is interesting to note at both the trend line and the rate of attack fell off to zero immediately after applying a second firewall between the cable modem and the target personal computer (Burnburg 2001).

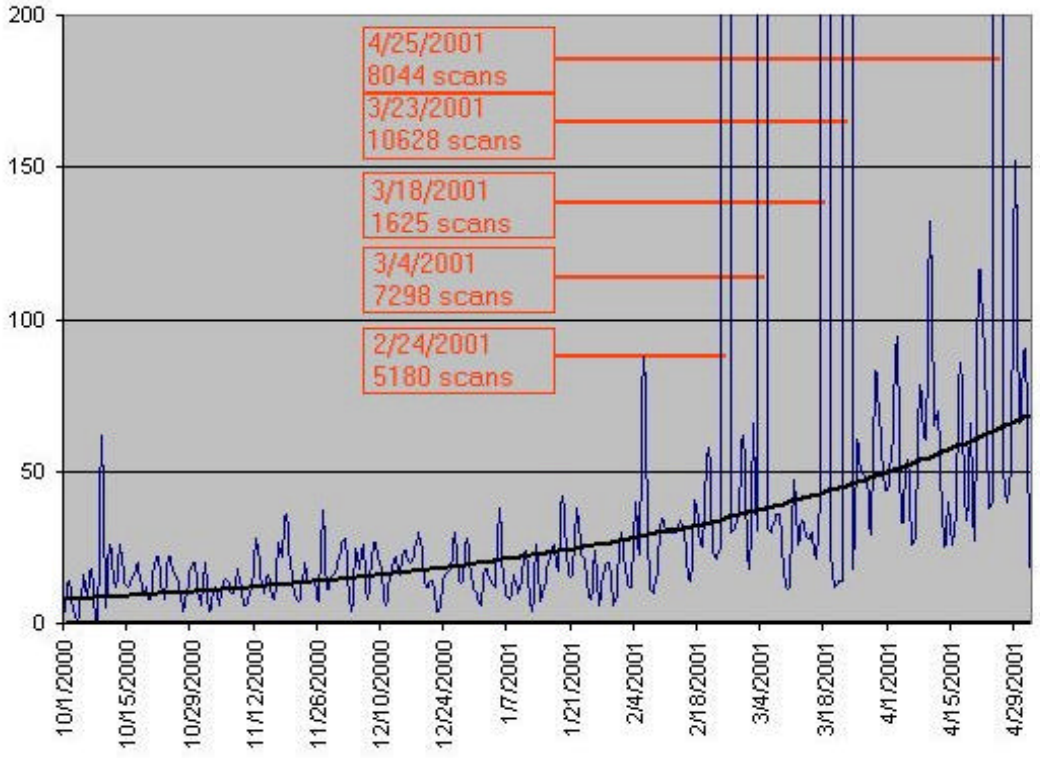


Figure 2 Numbers of Discrete Attacks, Probes or Scans on Cable-Connected PC (Burnburg 2001)

The rate of discrete port scanning over the same seven month period followed the same trend (see Figure 2). However, on the five days that are denoted in Figure 2, the intensity of the scanning had negative impacts on the user of the system. Over 85.2% of the total probes where executed on these five days. The user was not able to find information as quickly as they would have on other days.

The business implications are made clear when evaluating the type of attacks and scans launched against this user. Referring to Table 1, several types of probing (i.e. SubSeven port probes, Back Orifice) were encountered over 34% of the time.

Attack Type	Count	Attack Type	Count
SubSeven port probe	689	WhatsUp scan	6
RPC port probe	262	PCAnywhere ping	5
RPC TCP port probe	252	TCP Trojan horse probe	4
FTP port probe	146	POP3 login failed	3
TCP port probe	133	IMAP4 port probe	2
TCP OS fingerprint	122	POP3 port probe	2
DNS TCP port probe	67	SNMP port probe	2
UDP port probe	59	Trinoo master activity	2
DNS port probe	48	.url URL type	1
NetBus port probe	37	Back Orifice scan seen	1
Telnet port probe	37	DNS I-Query	1
Proxy port probe	30	IP fragment overlap	1
UDP Trojan horse probe	25	Scan by sscan program	1
NNTP port probe	18	SMTP attack	1
HTTP port probe	17	SQL port probe	1
Back Orifice ping	10	Trace route	1
IRC port probe	10	UDP port scan	1
SMTP port probe	7	XWINDOWS port probe	1
TCP port scan	6		
		Detected Attack Types	37
		Total Attacks	2011

Table 1 Attack Types Detected By IDS Software (Burnburg 2001)

Many of the probes indicate that the attacker was looking for security holes that the attacker may have attempted to initiate via email vectors. The SubSeven exploit will allow remote control of the target PC if successfully exploited (Chirillo 2001). The remaining attacks and probes are footprinting the services or daemons running on the target PC. Each service or daemon has its own security issues.

Remote Control Attacks	Count
SubSeven port probe	689
NetBus port probe	37
UDP Trojan horse probe	25
Back Orifice ping	10
PCAnywhere ping	5
TCP Trojan horse probe	4
Trinoo master activity	2
Back Orifice scan seen	1
Total	***773***

Remote Access Attempts	Count
RPC port probe	262
RPC TCP port probe	252
FTP port probe	146
Telnet port probe	37
Proxy port probe	30
POP3 login failed	3
.url URL type	1
Total	***731***

Denial of Service Attacks	Count
IP fragment overlap	1
SMTP attack	1
Total	***2***

Services Enumeration	Count
TCP port probe	133
TCP OS fingerprint	122
DNS TCP port probe	67
UDP port probe	59
DNS port probe	48
NNTP port probe	18
HTTP port probe	17
IRC port probe	10
SMTP port probe	7
TCP port scan	6
WhatsUp scan	6
IMAP4 port probe	2
POP3 port probe	2
SNMP port probe	2
Scan by sscan program	1
SQL port probe	1
Trace route	1
UDP port scan	1
XWINDOWS port probe	1
DNS I-Query	1
Total	***505***

Attack Class	%
Remote Control Attacks	38.4
Remote Access Attempts	36.4
Services Enumeration	25.1
Denial of Service Attacks	0.01

Table 2 Attack Classification (Burnburg 2001)

A further evaluation of this data by attack classification (Table 2) indicates that the majority of attacks were designed to gain remote control or remote access to this platform. Only 25.1% were service enumeration or mapping efforts. The most interesting part of this data was that only two events could be considered to be Denial of Service (DoS) attacks.

What is the goal?

The goal of any information security process is to maintain the confidentiality, integrity, and availability of information assets. Confidentiality is the process where access to

information is controlled and made available only to those individuals who require it. The integrity of data is concerned with those processes taken as a whole to prevent the intentional or unintentional alteration of information. Finally, availability of data seeks to provide the information requested by authorized personnel in a timely manner. Confidentiality, integrity, and availability are the classic and most easily recognized requirements within the field of information systems security (Tiller and Fish, 2001).

During the last five to ten years, additional requirements for information security processes have been enumerated. The most common additional requirements are Non-repudiation, identification and authentication. Non-repudiation is the concept that both the sender and receiver of information have proof of the others identity and receipt of the information (U.S. Department of Defense, 2000). The identification and authentication of authorized personnel is complex and without a clear standard proof. Many technologies and methods have been proposed including two and three factor authentication, biometric identification, and public key technologies. Each has strengths and weaknesses. As of the writing of this document, nothing is considered foolproof.

What is the risk?

Statistical analysis of computer crime and security is hampered by the lack of response from the victims (Refer to Figure 3). The primary reason most organizations refuse to acknowledge security incidents is the perception that the public will lose confidence in the organization. Other factors may include such things as the stockholders may sue us because we breached their fiduciary responsibility, Wall Street may adversely impact our market cap, other "hackers" may find out we're vulnerable, and old fashioned pride.

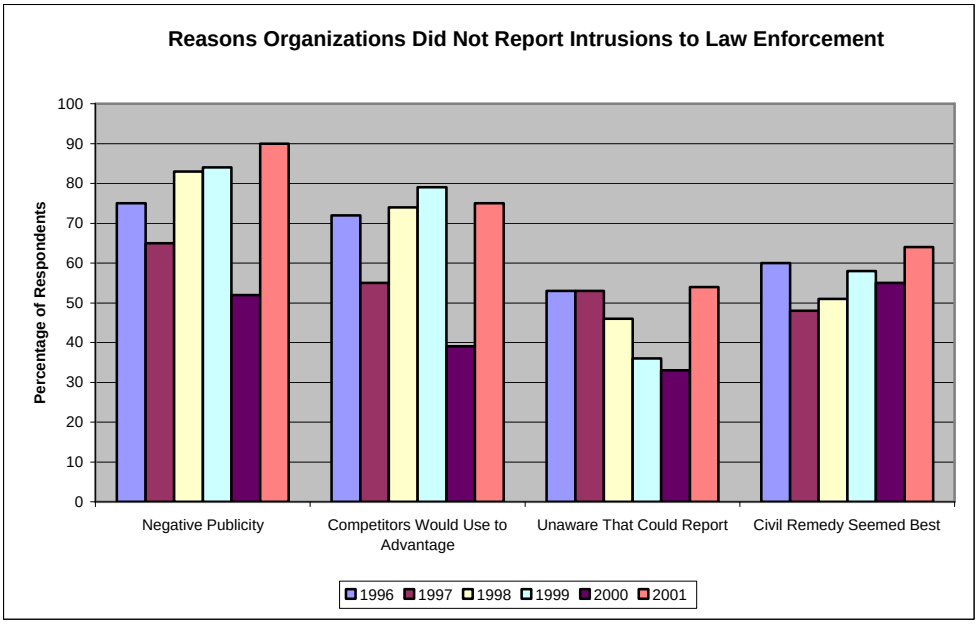


Figure 3 Reasons for not Reporting Intrusions (Computer Security Institute 2001)

The Computer Emergency Response Team (CERT®), located at Carnegie-Mellon University, maintains data on the number of reported security incidents and vulnerabilities on an annual basis. The information presented in Figure 4 shows that according to CERT® data the growth rate of reported incidents and vulnerabilities is growing exponentially.

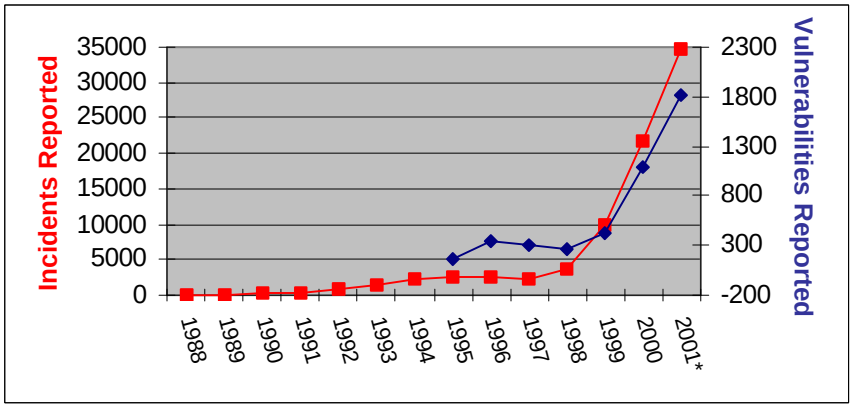


Figure 4 CERT Statistics through Q3 2001 (CERT®)

The reason for this trend is shown in Figure 5. Over the years, attacker knowledge necessary to effectively penetrate a system has declined. The availability of easy to use tools combined with the low cost of the necessary hardware, software, and Internet connectivity has resulted in attackers with little training or knowledge being able to effectively penetrate or attack any Internet connected system of their choice.

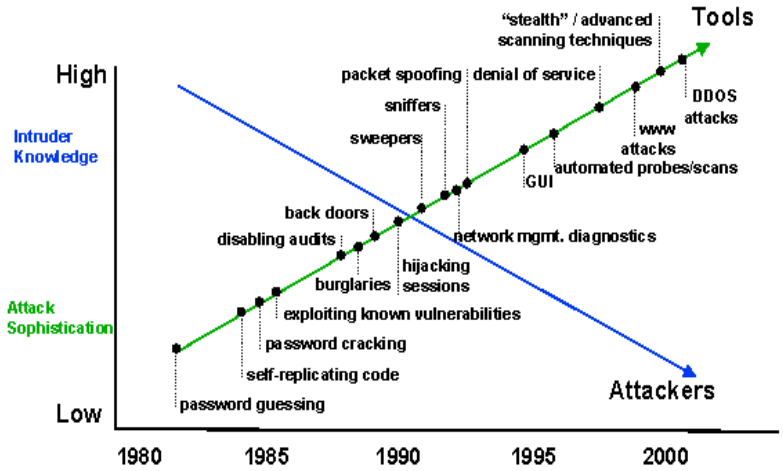


Figure 5 Attack Sophistication vs. Intruder Knowledge (Pethia 2001)

The most cited statistical analysis of computer crime and security is the annual report jointly issued by the Computer Security Institute (CSI) and United States Federal Bureau of Investigation (FBI). The CSI/FBI Computer Crime and Security Survey gives the first clues into what happens when an unauthorized intrusion takes place in most organizations. Referring to Figure 6, a qualitative trend can be seen in organization response to intrusions.

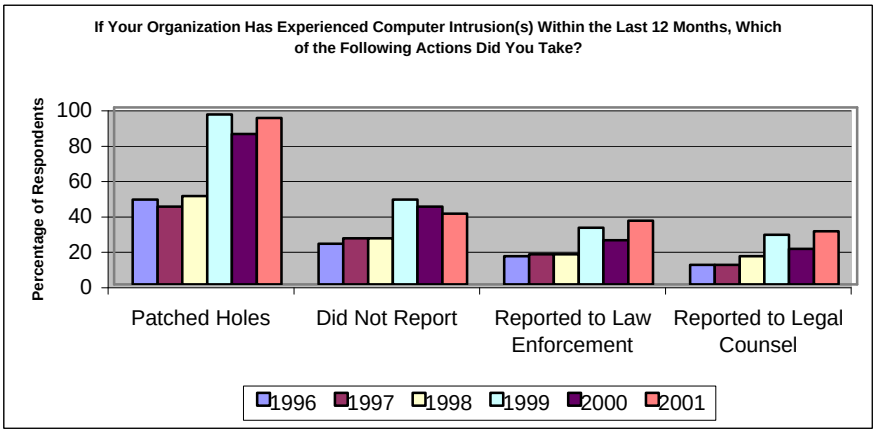


Figure 6 Actions Taken to Computer Intrusions (Computer Security Institute 2001)

Reporting of intrusions is trending upward over time; however, the majority of organizations continue not to report intrusions to external agencies. Most organizations appear to fix the vulnerability the intruder used.

The principal issue with this particular survey is that the respondents generally "pick and choose" which questions to answer. The highest response rate was for general organizational questions such as the number of employees, industry sector, and security technologies used. These questions had response rates between 99% and 100%. Response rate fell dramatically for questions (Computer Security Institute 2001) such as:

- Financial losses by type of attack or misuse (64%),
- Dollar amount of losses by type (34%),
- WWW site incidents: If yes, How Many Incidents? (40%),
- WWW site incidents: what type of unauthorized access or misuse? (14%)
- If your organization has experienced computer intrusions within the last twelve months, which of the following actions did you take? (64%)

While the 2001 CSI/FSI Computer Crime and Security Survey is suspect from a quantitative perspective, several qualitative trends can be seen.

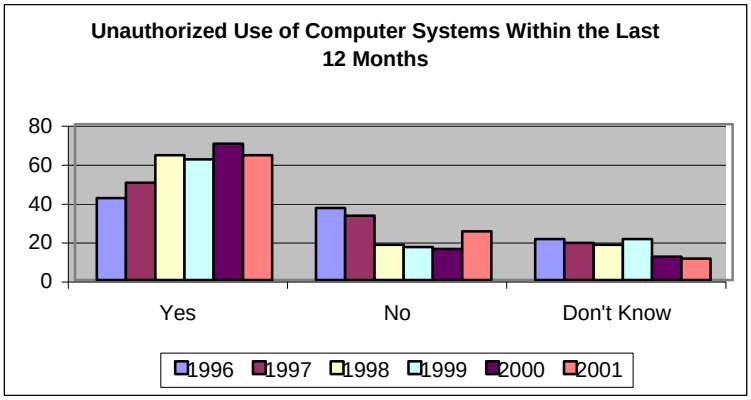


Figure 7 Unauthorized Use of Computer Systems Within the Last 12 Months (Computer Security Institute 2001)

Over a six year period, organizations are becoming more aware of whether or not their computer systems are being used in an unauthorized manner (see Figure 7). During the same time frame, organizations are reporting a generalized trend towards more unauthorized use of their systems. The information contained within Figure 7 had one of the highest response rates (> 91% for all years except 1997 which was 69%).

The recognition of unauthorized systems use has probably increased over the 1996-2001 period because of increased use of security technologies such as firewalls and intrusion detection systems (see Figure 8 on page 22). Figure 8 shows that organizations, over the last five years, have increased the use of security related technologies.

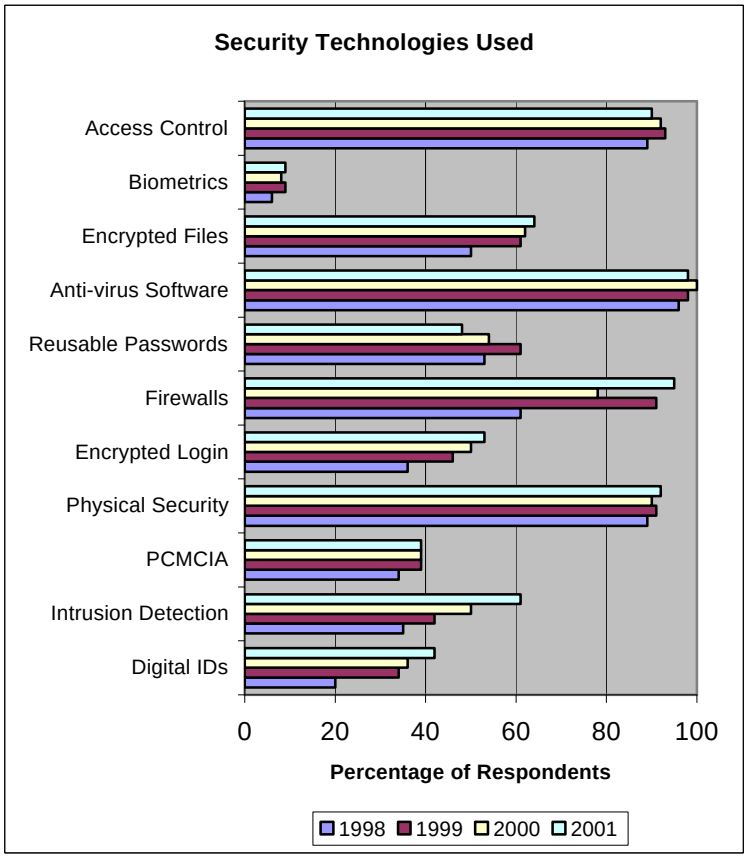


Figure 8 Security Technologies Used (Computer Security Institute 2001)

As in Figure 7, what security technologies are used (Figure 8) had a high response rate (> 96% in all years). A significant increase in the use of intrusion detection and firewall technologies is the probable factor showing increased situational awareness with regard to unauthorized use of systems (refer to Figure 7). Increased use of encryption technologies combined with firewalls and anti-virus, software does show that organizations are beginning to address basic security requirements. Many operating system vendors (Microsoft, Novell, etc.) have made encrypted logins the default option, so the increase in use of encrypted logins may be attributed to normal operating system upgrade processes.

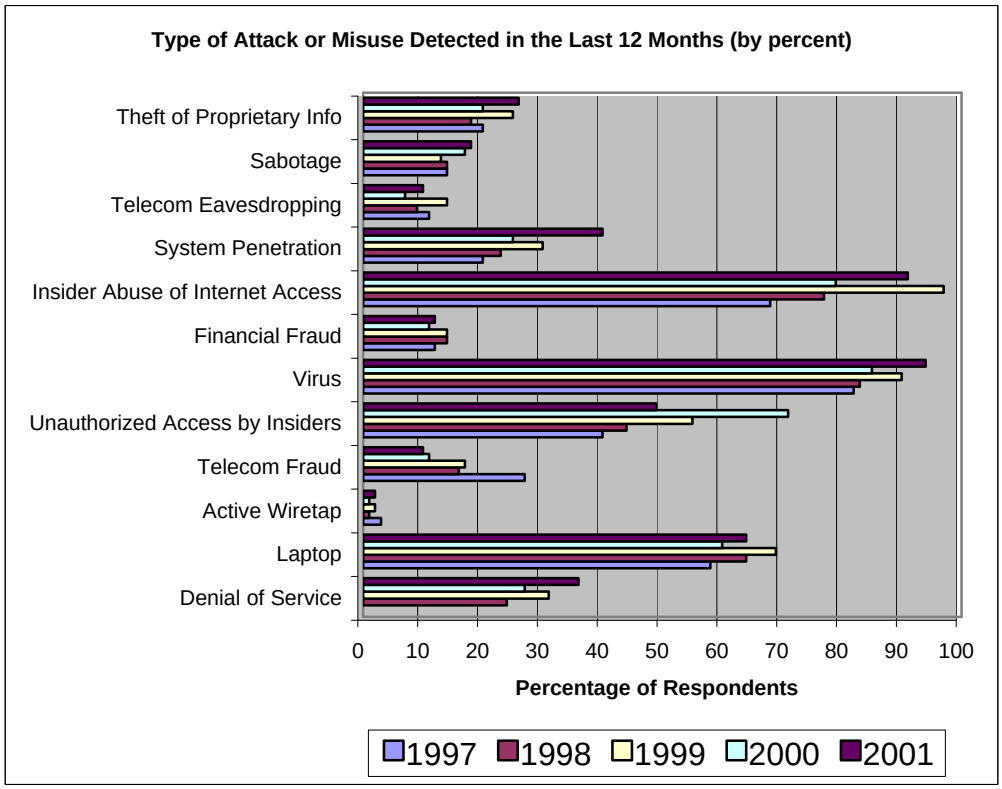


Figure 9 Type of Attack or Misuse Detected in the Last 12 Months (Computer Security Institute 2001)

Organization's reported a wide variety of misuse within their networks according to the Computer Crime Survey (Figure 9). While virus attacks were significant in 2001, insider abuse (i.e. employees) was significant. Denial of service attacks and the viral attacks continue to be on the rise. Most significant is the rate of increase in system penetrations; however, the Computer Crime Survey does not indicate how many penetrations have occurred from internal sources vs. external sources.

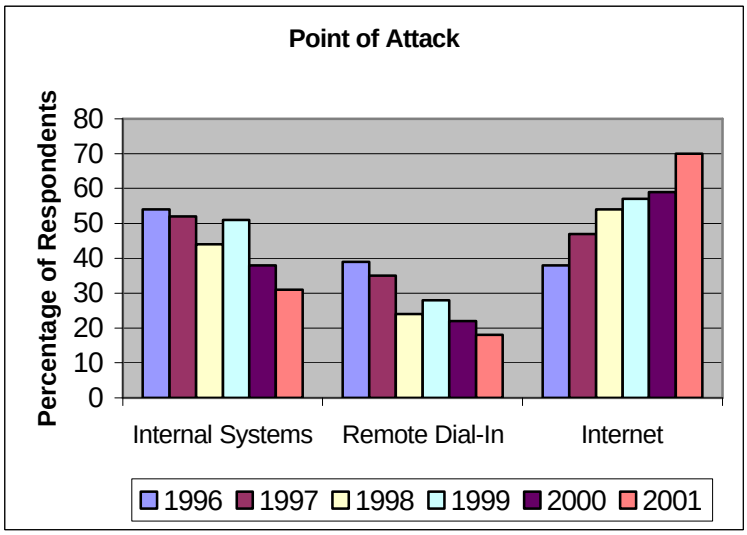


Figure 10 Point of Attack (Computer Security Institute 2001)

Organizational networks are attacked internally and externally. An internal attack is generally launched by an insider. Remote dial-in attacks are launched by insiders and outsiders. Figure 10 shows the perception of organizational respondents as to the point of attack. Most interesting aspect of this graph is the apparent disconnect between the perceived point of attack and the detected misuse pattern (refer to Figure 9).

Who are the players?

What becomes readily apparent reviewing the preceding information is that the high availability of quality tools combined with the rapid growth of Internet access around the world has resulted in a target rich environment for individuals, organizations, and governments to exploit. In an information economy, the primary value of any organization is the information it creates and maintains. That information is the target.

The two principle roles within the information security are the attackers and the defenders (Denning, 1999). This may seem to be a trivial statement. However, the attackers and the defenders are interchangeable depending on the associated group or

need of the organization over time. According to Schwartau, there are several categories of potential information warriors or hackers/crackers (1996):

- Organizational Employees
- Vendors and Contractors
- International, National, and Local Governments
- Government Employees
- Law Enforcement
- Terrorists
- Organized Crime and Individual Criminals
- Direct Mailers and Telemarketers
- Doctors, Hospitals and Insurance Companies
- Private Investigators
- Security Professionals
- Politicians and Political Action Groups
- Foreign and Domestic Intelligence Agencies
- Foreign and Domestic Competitors

With the exception of governmental bodies, both foreign and domestic, the vast majority of these groups either wants or needs to know a great deal of information about individuals. Most will collect information, disseminate information, or desire more information. Criminals, telemarketers, political groups, insurance companies and private investigators have a vested interest in violating individual privacy to reach their goals. They need this information in order to be successful. Schwartau (1996) effectively states that nearly everyone is an information warrior in some way.

However, a more balanced approach may be the perceptions of organizations that participate in the Computer Crime Survey. Figure 11 (on the next page) makes a very simple case. Most organizations believe that competitors, governments, hackers, and disgruntled employees are the most likely source of attack. For the purposes of the information security professional, this may be the more balanced approach.

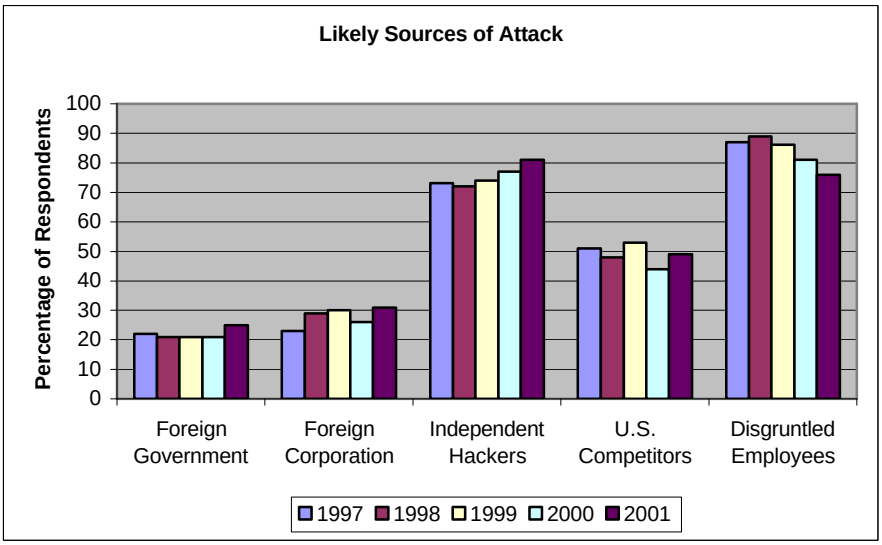


Figure 11 Likely Sources of Attack (Computer Security Institute 2001)

Attack Method

Despite the Hollywood image of a hacker, most hackers and crackers utilize an methodical approach to gain access to servers or services that they have no authorization to utilize. The approach is very systematic and requires little explanation. Scambray, McClure and Kurtz (2001) suggest a straightforward attack methodology:

- Footprinting - During this phase, the goal is to determine the IP address range, domain name of target, and general information gathering about the target.

- Scanning - This phase of the process begins target assessment. The goal is to determine all services that target system(s) have running. This helps the attacker to narrow his focus to avenues with the highest probability of success.

- Enumeration - At this point, the attacker becomes more intrusive. The principal goal during this phase is to identify user accounts and poorly defended resource shares (i.e. Windows drive mappings).

- Gaining access - The attacker has now gained enough information to attempt to gain access to the target. Access can be a low level user account with minimal privileges.

- Escalating privilege - Assuming system or root level access has not been gained; the attacker will now attempt to gain complete control over the compromised system.

- Pilfering - Information gathering begins again as the attacker attempts to gain access to trusted systems.

- Covering tracks - Once the target has been completely compromised, the attacker attempts to keep system administrators from determining this fact.

- Creating back doors - This is generally the last stage of attack. The attacker creates a variety of privileged accounts to regain control of the target should system administrators discovered his access.

- Denial of service - Depending on the nature of the attack and attacker, the target may be disabled through a variety of system exploits. The goal is to deny access to legitimate users. This may be the result of an attacker's failed attempt to gain control of the target.

Figure 12 shows a graphical representation of Scambray et al's (2001) attack methodology.

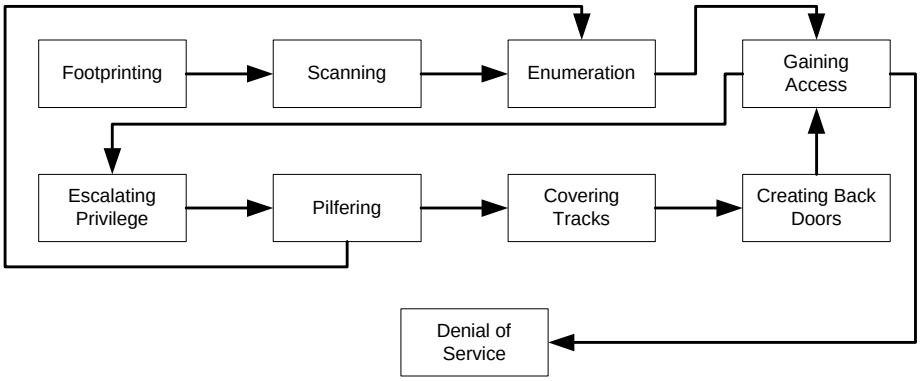


Figure 12 Attacker Methodology
(Scambray. McClure and Kurtz 2001)

From a security perspective, there is a very little that can be done concerning footprinting and scanning. The very nature of networking within a public environment, such as the Internet, precludes hiding server names or IP addresses on a wholesale basis. An organizational site, which has the goal of reaching external organizations and individuals, must advertise the presence and name of at least one server to the Internet community. The construction of the TCP/IP protocol stack generally precludes the ability to hide the ports that daemons use for communication.

Security Frameworks

Historically, security frameworks tend to address concepts without showing a relationship to the locality of data or technological infrastructure where the data is stored, transmitted or processed. Combined with a lack of understanding about the social and technological characteristics of information technologies, totally conceptual frameworks do not convey the necessary understanding to decision makers who approve changes.

The most basic security framework is known as the C-I-A triangle. The three corners of this framework are: Confidentiality, Integrity, and Availability (Parker 1981). Confidentiality refers to the requirement that only individuals with a need-to-know have

the ability to access the information. Integrity of data is the need to assure that the information is not altered in any manner, intentional or unintentional, which is inconsistent with normal processing. The availability of information necessitates that those who need the information have access when they require access. The key aspect of this framework is that all three factors are in balance with one another. Increase the confidentiality of information and the availability will decrease.

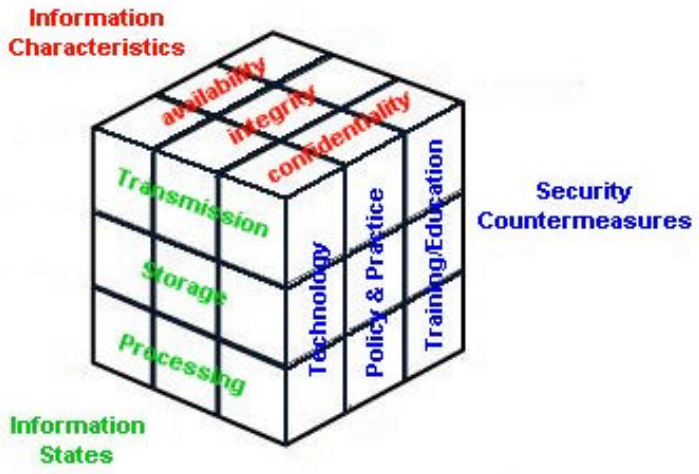


Figure 13 McCumber INFOSEC Model (1991)

The next framework of note is the McCumber INFOSEC Model proposed in 1991. This framework (Figure 13) maintains three core areas of concern. First, information characteristics are simply the C-I-A triangle. The confidentiality, integrity and availability of information are required in this model. The second area of concern is the state in which the information exists. Each information state has specific security concerns. Transmission of data is the simple movement of data or information between storage and processing or between multiple computing platforms. Information must be stored or maintained somewhere. This requirement speaks to the availability of information. Finally, processing of data transforms data values or presents data as information. This information state is where the consumer of information actually "sees" the information.

The final core area of the McCumber INFOSEC model addresses security countermeasures. Most people look to technology to provide the "security" for any organizational information system. McCumber would place all technologically-based security controls here. However, McCumber recognized that organizational policies and actual practices had a substantial impact on the overall security of any environment. This leads naturally to training and education as a security countermeasure. Individuals continue to be the largest single security issue for any organization. Unless the individual understands what is required of them (i.e. do not share user ids and passwords), they will continue to be the largest security risk to the organizational infrastructure.

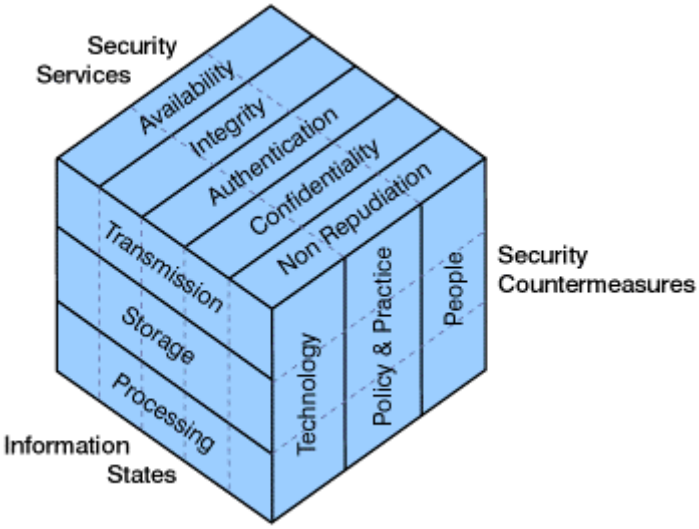


Figure 14 Information Assurance Model (Maconachy et al 2001)

Maconachy et al (2001) extended the McCumber INFOSEC Model by adding two additional information characteristics, authentication and non-repudiation (Figure 14), which are referred to as security services. Many believe that these services are the same. However, authentication seeks to provide a mechanism where an individual provides adequate proof of authorization to access different levels of information. Non-repudiation seeks to provide the sender of a message with proof of delivery and the

receiver of the message with confirmation of the sender's identity. In many definitions of non-repudiation, the message content is also confirmed to be "assent" through the use of message digests.

A General Framework for Conceptualization of Defense-In-Depth

As is readily apparent, any security architecture needs a framework in which to evaluate and conceptualize all the necessary issues and processes. Information systems security is complex from a number of different perspectives. First, no single technology can provide all the necessary protection an organization or even an individual requires. Second, the legal environment changes, in knee-jerk fashion, depending on the mood of the governmental body enacting the supporting legislation. Third, the rapid adoption and deployment of new technologies can lead to a number of unanticipated consequences (Axelrod and Cohen, 1999). Fourth, as organizations move to utilize public networks for business needs, small world network nature of the Internet induces a broad range of complexities to the network and security environments of the organization (Watts and Strogatz, 1998). These complexities are broadly grouped by Strogatz (2001) into six categories: structural complexity, network evolution, connection diversity, dynamical complexity, node diversity and meta-complications which are a combination of the first five categories. Finally, organizations, themselves, do not always act in their own best interest when evaluating the need for security of assets that cannot be touched.

It is proposed, therefore, that a general framework for the evaluation of information security needs to be stated in order to have a reference point to ground the remaining discussion. This framework will center on the key information resource to be defended – the data. In most information systems, the data is accessed by a set host or group of hosts that exist within a greater context of (potentially) multiple networks. However, the specific organizational and technological needs will vary depending on the 'environmental context' of the organization.

Evaluation of the environmental context centers on several technology and organizational requirements or domains. The following domains are recognized by several sources as key areas that must be addressed (Tipton and Krause 2001):

1. Legal and Governmental Environment
2. Encryption
3. Access Controls
4. Physical Security
5. Application and Systems Development
6. Disaster Recovery and Business Continuity
7. Operational Security

An additional domain should be reviewed and acknowledged within the overall security framework – Organizational Environment. The organization defines the business and consequently the information systems to be utilized (Helms and Wright 1992).

Figures 15 and 16 (on the next page) serve to visually represent this relationship[1]. It is very important to note that no one domain has precedence over any other domain. Each domain exists whether or not an organization specifically recognizes it. Further, each domain is not sharply defined. Encryption technologies may be utilized within access controls or a new law may change the business environment of an organization. Each domain is part of the whole. An organization cannot ignore one without risking the others.

1. Figures 15, 16, 17 and 18 where created for this study to visualize the proposed framework, it structure and relationships.

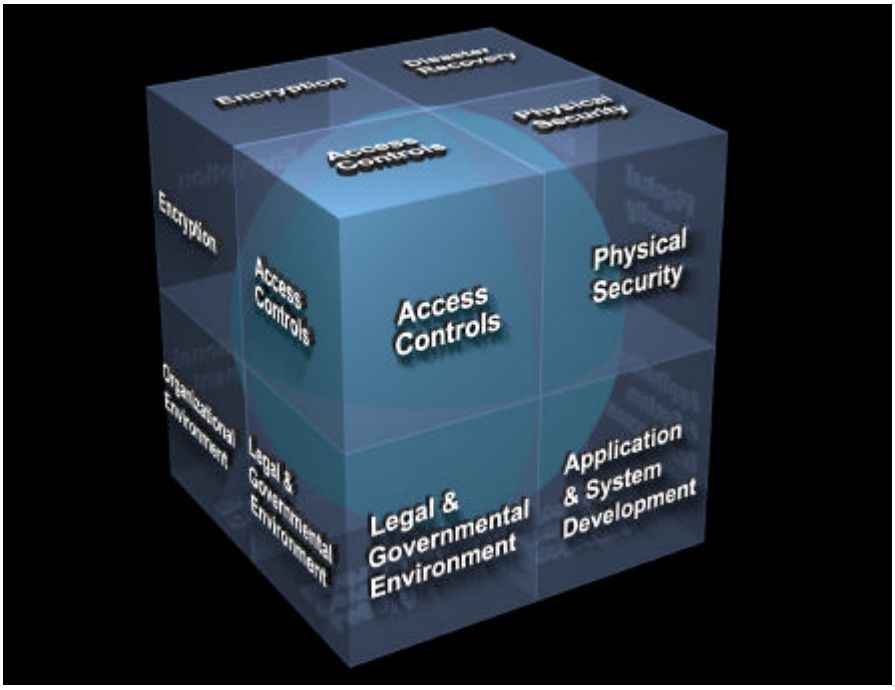


Figure 15 Proposed Framework (Front View)

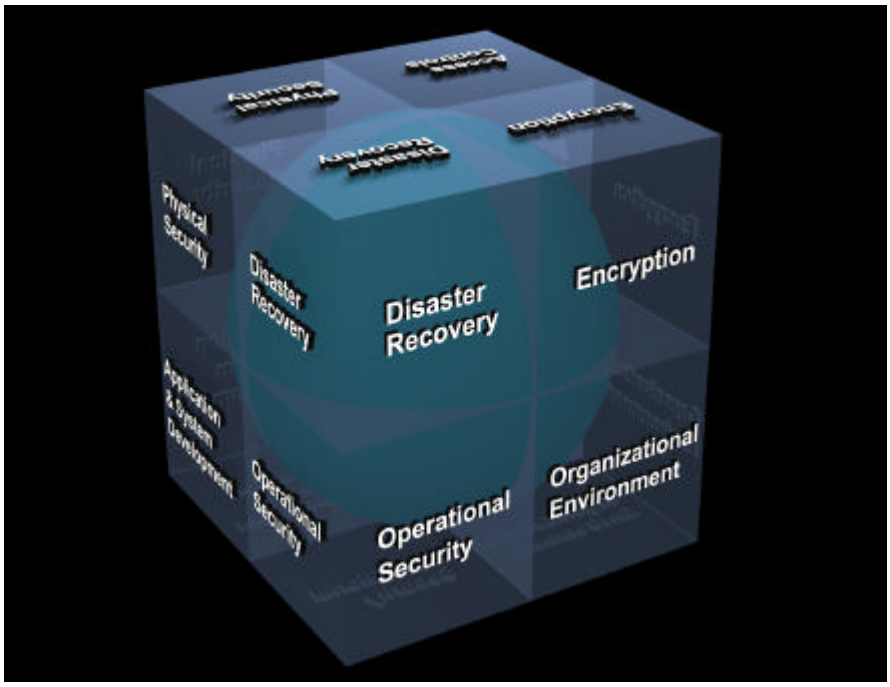


Figure 16 Proposed Framework (Rear View)

Organizational Environment

Other than the 'normal' business applications (i.e. office suites, desktop operating systems, etc.), the nature of the business drives the type of information to be processed and the applications that perform that processing. While there are similarities in business software requirements, specialty information is dependent upon:

1. What sector(s) is the organization operating business line(s)?
2. What level of competition exists within each sector?
3. How much governmental regulation exists for each sector?
4. How successful has the organization been in the past?
5. How successful is the organization now?
6. Is the organization utilizing technology and automation for competitive advantage?

These questions and their answers help drive what technologies and information are implemented and planned for any organization.

An organization's strategic mission statement drives strategic planning. Strategic planning drives tactical planning. Strategic and tactical planning drives policy creation and formulation. Therefore, by example, a credit card company wishes to increase shareholder equity by lowering operating costs and increase customer service. Strategic solution: Offer customers the ability to pay their bills via the Internet saving the organization manual bill and payment handling costs, postage, and printing costs. However, the credit card company must safeguard customer information and prevent unauthorized account access. In addition, there are legal and regulatory requirements.

Legal and Governmental Environment

The legal and governmental environment is extremely complex when viewed from an international perspective. Many governments have conflicting laws concerning what individual privacy rights are granted, what constitutes an illegal act, what encryption standards are allowed, what civil and criminal penalties will be leveled for specific acts, and whether or not data can cross international borders. Even within the United States there are conflicting laws and regulations that must be addressed by organizations with respect to information systems and security (Gallagher 2001).

Some of the laws that govern information systems security within the United States include:

- The Privacy Act of 1974 (5 U.S.C. § 552A)
- The Foreign Corrupt Practices Act of 1977 (15 U.S.C. §§ 78)
- The Comprehensive Crime Control Act of 1984 (Pub. L. No. 98-473, Title II)
- The Computer Fraud Abuse Act of 1986 (18 U.S.C. § 1030)
- The Electronic Communications Privacy Act of 1986 (18 U.S.C. § 2701)
- The Computer Security Act of 1987 (Pub. L. No. 100-235)
- The National Infrastructure Protection Act of 1996 (Pub. L. No. 104-294)
- The Economic Espionage Act of 1996 (18 U.S.C. § 90)
- The USA Patriot Act of 2001 (Pub. L. No. 107-56)

These acts cover a broad range of issues within information systems and telecommunications security. A quick synopsis of some of these acts with implications for information security follows.

The Privacy Act of 1974 governs the disclosure of identifiable individual information. This act prohibits the disclosure of personal information by governmental agencies outside the scope of the agency's mandate without permission of the person in question. There are sections that allow the individual to challenge erroneous, incomplete, or inaccurate information (United States Department of Justice 2001).

While the Privacy Act of 1974 applied to electronic files, the United States Congress passed the Electronic Communications Privacy Act of 1986 (ECPA). The ECPA extends the Privacy Act of 1974 in several key ways. First, the ECPA makes it a crime to illegally access, use, disclose, intercept or violate the privacy protections of electronic communications (United States Internet Industry Association 2000). In addition, the ECPA prevents governmental organizations from accessing, tapping, or copying electronic information without due process (e.g. a proper warrant).

Further extensions to privacy of individual information have been legislated in the United States through the Health Information Portability and Accountability Act of 1996 (Pub. L. No. 104-191) and the Graham-Leach-Bliley Act of 1999 (Pub. L. No. 106-102). These acts seek to prevent the dissemination of private health information (e.g. HIPAA) and financial information (United States Senate Committee on Banking, Housing, and Urban Affairs 1999).

Most of the privacy legislation in the United States is based on the concept of "opt-out". Opt-out requires that an individual must be presented with information concerning the use of their private information by an organization. However, HIPAA requires that informed consent must be granted prior to medical treatment unless there are substantial communications issues between the primary care provider and the patient and an

emergency situation exists. HIPAA does not allow the patient to "opt-out" if the patient wishes to receive medical care.

Information security personnel must be cognizant of the relevant privacy laws that affect their organization. There are specific liabilities, both criminal and civil, if the laws are not met. Full line insurance companies (life, accident, health, etc) have conflicting regulations to be resolved depending on which product line is under consideration.

Moving away from privacy legislation, the legal position for organizations is exacerbated by conflicting laws from multiple countries. The USA Patriot Act of 2001 and the European Union's Cybercrime Treaty define a variety of cybercrimes and illegal uses of information systems and the Internet. The USA Patriot Act of 2001 expanded the definition of what constitutes a cybercrime while dramatically expanding the scope and reach of governmental agencies in "pursuing" criminals.

This shows that the "problem" of cybercrime is being addressed internationally. However, most nations differ as to the seriousness of computer crime. Further, what constitutes an actual crime varies from nation to nation. Rules of evidence and law enforcement technical capabilities differ and there may be issues as to whether governments can work together on this problem.

The legal and regulatory environment is further complicated by contradictory requirements. HIPAA and Graham Leach Bliley Act (GLBA) are in conflict with each other on specifics of implementation. While both laws and their enabling regulations are designed to protect individual privacy, when an organization must comply with both; problems are bound to crop up. For example, GLBA requires that customers must opt-out in order to protect their privacy. This resulted in a variety of financial institutions sending out notices to their customers delineating their privacy policies and how (in the fine print) a customer could prevent information from being shared (sold) between organizations. With HIPAA, the patient (customer) had to opt-in for information to be

shared. This required organizations to get prior approval for information sharing. Now imagine an insurance company that offers financial services and health care insurance. If a customer had both health care insurance and a retirement account, the company would be by default out of compliance with one of the laws (HIPAA or GLBA).

Application and System Development

It can be argued that the application development process is the primary culprit for many security breaches. Software, whether internally or externally developed, does not generally receive adequate testing prior to use in production. In addition, the organizational desire to use common-off-the-shelf (COTS) applications and development environments add to common code vulnerabilities.

In a security context, software includes operating systems (end-user and network), device drivers, commercial application software, development environments, vendor implementations of network communications protocol stacks, and embedded software. Whether the software is called from read only memory or any of the variants or from storage, all software requires testing.

The minimum requirements (Murray 2001) that are generally accepted for application development and software testing include:

- Separation of duties between application development and production systems
- All changes to source code must be documented, tested, and approved
- All library code must be reviewed and tested

Some of the security challenges surrounding software development include;

- Reuse of objects to improve programmer productivity can induce unintended security holes

- Aggregation of objects that have not been tested together before may create security problems through improper operation, erroneous data manipulation, or inappropriate data communications

Most modern application development processes utilize code reuse to bring new applications to market or place into production on a shortened timeframe. To further shorten the application development process, many organizations utilize code sets developed by third parties. This can lead to multiple problems. Reuse of objects from object repositories or subroutines from libraries can propagate coding flaws because the developers of the new application may not know all of the internal processes being executed in those objects and/or subroutines. Potential problems can include intentional covert communication channels, trap doors, and back doors may allow unauthorized access to data and information.

With adequate code review and control of object repositories and subroutine libraries, the likelihood of many different application development threats can be reduced. Examples of controls for the application development process include:

- Separation of duties so that no one individual can place new code into the production environment,

- Separation of the production environment from the development environment to eliminate code testing on live data sets,

- Review of all source code to be included in object repositories and subroutine libraries to reduce the likelihood of processes that could allow unauthorized access to data and information,

- and peer review of all source code to be placed into production during the application development process to reduce the chance that a single individual could place malicious code into production or distribution.

Operational security

Operational security can be considered the tactical processes and procedures that are mandated by organizations security policies. Those involved with operational security will assist in the selection of access control systems. However, the aspects of operational security extend beyond information systems and can include voice systems, alarm systems, and other security systems.

Procedural control over the following types of assets is not uncommon:

1. communications hardware and software to include telephone switches, Voicemail Systems, and wide area networks and the attendant hardware and software

2. data storage systems and storage media to include storage area networks, network attached storage, CDR media, data tape, and any other potential storage media

3. network infrastructure to include all processing equipment, mainframes, minicomputers, workstations, personal computers, routers, hubs, switches and cable plant

4. applications including program libraries, source code, operating system software, proprietary software, and common off-the-shelf software

5. system utilities, logs, and audit trails

6. backup files and all data files

7. people

8. sensitive forms and printouts

The staff normally responsible for operational security includes the system operators and network administrators. This group should be monitored for all activities to watch for potential abuses, such as, fraud and operational interference.

Physical Security

Within the domain of physical security, there are three areas of concern: facilities security, administrative controls and procedures, and personnel security. Facilities security is concerned with managing access to buildings, controlling access to information systems platforms, and telecommunications infrastructure. Administrative controls and procedures for physical security are designed to control and audit who is physically within an area. These control systems and their attendant procedures may be integrated with the network security, but the function is organizationally separate. Personnel security limits physical access by job role. In some organizations, the network group may not have responsibility for the wide area network infrastructure. In this case, physical access to the routers and switches may be limited with locked telecommunications closets. An example of poor physical security controls would be a scenario where access to an automated teller machine (ATM) is located within the wiring closet for the network. Procedurally, no personnel could be in the closet while the ATM machine is being serviced or loaded with currency. This would prevent internal personnel from being able to observe the activities while non-staff personnel in the wiring closet.

Access Controls

The domain of access controls is extremely broad. However, for this discussion, access controls are discussed as technologies for implementation. Procedural processes for use

with these control technologies are within the domains of physical security and operations security.

Every layer of the logical and physical network (refer to Figure 16) may contain one to many access controls. Some access controls span multiple network layers, such as virtual private networks, and may make use of multiple systems to confirm authorized access (i.e. tokens with one time passwords). Broadly classed, access controls fall into three categories:

1. Edge Devices – Firewalls, VPN Concentrators, Proxy Servers, Load Balancers, Filter Platforms (Email, antivirus, etc.), Intrusion Detection Devices

2. Operating System Authentication including single, two and three factor authentication

3. Application Authentication

The edge of the network is where most organizations focus their security efforts even though insider threats are still the most serious. With that in mind, review of the edge devices is critical. It is important to remember that improper configuration of any security device is self-defeating. There are three basic firewalls technologies, packet filtering, stateful inspection and application (Fratto 2001). The filtering firewall either allows or denies traffic based on what protocols authorized. In other words, if a packet is destined for TCP port 80 on a HTTP (web) server and the traffic is allowed, then the packet is passed. If, however, a packet is destined for TCP 21 and a rule exists to drop all traffic but TCP port 80, then the packet is dropped. The filtering firewall does not evaluate whether or not the connection for a specific port is properly set up.

The stateful inspection firewall evaluates whether or not the connection is properly made for allowed ports or services. In other words, if a request comes into TCP port 80 and the TCP three-way handshake has not occurred, the packet is dropped. Application

firewalls take stateful inspection to a higher level. This technology evaluates the content or data load of each packet and makes decisions about allowing or denying traffic based on rule sets, attack signatures and learned traffic patterns. Depending on the requirements of the organization, all three types of firewalls may be used. The principle concern is throughput. Filtering and stateful inspection firewalls are the fastest. Application layer firewalls are the slowest since they inspect the data load of every packet.

Proxy servers are designed to support a number of functions. One on the most common proxy servers is the mail transfer agent. This platform isolates the internal Email server from public networks. The mail transfer agent or proxy server is designed to simply forward mail from the internal to the external network (CipherTrust 2001). This prevents direct attacks on the internal email server. There are other types of proxy servers, but their function is the same.

VPN concentrators create encrypted communication tunnels through a network. In most cases, virtual private networks are used in public network. There are some uses for VPNs on internal, high security networks, but most organizations do not have this need. VPNs are being utilized to move employees to home and create extranet business partnership connections (Cisco Systems 2001). VPNs suffer from a communications overhead due to the encryption/decryption requirements. However, this is outweighed by the cost savings generated by freeing up expensive office space and the ability to leverage inter-organizational communication channels over public networks.

Load balancers are designed to spread application load or network traffic across a number of devices. Microsoft describes the primary function of clustering services as load balancing. Many manufacturers have created devices that spread inbound network and application traffic (Anderson and James, 1999). One aspect of load balancers is the ability to evaluate inbound traffic and route specific traffic to specific platforms at an application level.

Anti-virus systems are designed to block malicious code. The systems can be used to scan all files on a particular system, all inbound and outbound traffic to a server, and all email and email attachments at the server and/or the workstation. The systems totally rely upon signature files as the principal means of detection of malicious code. However, some systems use heuristic algorithms for virus-like activity.

Other filters and detectors are designed to monitor where internal users go on the Internet and block inappropriate email traffic. The systems are primarily focused on human resource issues for the organization. The principal goal is to the liability under various sexual harassment laws and regulations at the local, federal, and state level in the United States and other countries.

Intrusion detection systems function as the alarm system of a network or host. The systems rely on signature files or heuristic algorithms for detection and recognition of attacks. Upon detection of an attack, the systems notify via email, pager, or telephone, appropriate personnel to review and decide on the response to the attack in progress. Some intrusion detection systems to allow for automated shunning of an attacker's IP address. This ability does provide some form of automated response that does not become an active measure.

Operating system authentication and other authentication systems comprise the next major area of access controls. The normal operating system requires a user ID and password for access. Most modern operating systems send the password over the network in an encrypted format. Storage of these passwords generally makes use of a one-way hash. However, there are software applications designed to brute force passwords. Each of these applications have differing success that cracking passwords.

Since user ID and password combinations are considered relatively insecure, other means have been developed to authenticate authorized users. This is generally referred

to as single-factor, two-factor, and three-factor authentication. The factors of authentication are:

1. Something the user knows,

2. Something the user has,

3. And something the user is.

Single-factor authentication requires the user to know something, namely, their password. Single-factor authentication is used by all operating systems and many applications.

Two-factor authentication makes use of two of the three authentication factors. The most common forms of two-factor authentication are:

1. Something the user has and knows

2. or something the user knows and is.

"Something the user has" typically refers tokens and access cards. These devices store information that is needed to authenticate to the application or operating system. Information stored in tokens could include PKI key sets, X.509 certificates, time-based passwords and single use passwords.

"Something the user is" refers to a physical aspect of the user. This is the realm of biometric devices. Hand geometry, retina scanning, fingerprint scanning and voiceprint recordings are the normal types of biometric authentication (Richards 2000).

In the first type of two-factor authentication, the user must have their token in order to be authorized access to the information system. In the second type, the user simply must be present and perform the required action to register their identity to the

authentication system. Many organizations that have HIPAA and GLBA requirements have started to utilize two-factor authentication for access. Two-factor and three-factor authentication also supports non-repudiation requirements in some systems.

Three-factor authentication uses all three factors for identification. The organizations that use three-factor authentication have high security access and non-repudiation requirements. Three-factor authentication is not generally deployed to all users within an organization.

Application authentication presupposes that the user ID and password is different from the network operating system or host user ID and password. This is a custom authentication process and is application specific. Any of the preceding access control technologies may be used within the application.

All access control systems should have the following characteristics:

1. Logging capability - the ability to establish an audit trail to enable reconstruction of events such as:
    a. Administrative access
    b. Configuration changes
    c. Changes to access levels
    d. Changes to passwords or authentication
2. Rule-based control - the ability to manage users and groups of users according to authorized to access levels
3. Administrative controls – organizational policies and procedures

Additional access control capabilities are dependent on specific requirements. Controls designed to limit and audit access to specific files or data of sensitive nature or the ability to encrypt and decrypt files on a specific user or user role.

The key problem with access controls is that security technologies change at a high rate. These same security technologies are deployed without a complete understanding of their capabilities at almost the same rate. It must also be noted that improperly configured access controls will not perform the intended task or tasks.

Encryption and Cryptography

Encryption and cryptography is a rapidly changing domain within the security framework. Research continues unabated as new ways to crack encryption keys are developed. Encryption is utilized in a number of technologies and devices. Encrypted telecommunications and data networks, non-repudiation of messages, file systems, password repositories, and individual file and messages are just a few of the applications.

Disaster Recovery and Organizational Continuity

Business continuity planning and disaster recovery planning addresses the integrity and availability of data. Business problems do not only arise from natural disasters. Technical failures, user errors and malicious attacks can also impact the availability and integrity of data maintained in information systems. Certain industry sectors in the United States, like banking and healthcare, have legislative mandates to maintain business continuity plans.

Any organization should (must) assess the risk to its information systems. Once the risks are understood, management can take actions design to mitigate the identified risks. Here is the first stumbling block. Managers may choose to mitigate risk by using only insurance products. This is a common practice in small to medium size organizations. This neglects the issue of client/customer service during a system outage.

Another common problem is that many organizations believe that disaster recovery and business continuity starts and stops with data backups. Frequently, these backup tapes are not tested for data recovery. This meme or paradigm also neglects the need to potentially replace hardware that has been damaged and may not be readily available.

The disaster recovery process typically focuses on the technical issues. This process has been extended to include business processes. When this extension occurs, the overall process is known as business continuity planning. Business continuity planning encompasses all the necessary business processes necessary to continue operations in a short period of time. This process extends the disaster recovery technical processes into other organizational areas such as human resources, accounting, customer service, and production of goods and services.

Business continuity and disaster recovery processes are highly individualized on an organizational basis. For large organizations, these processes may and probably will push down into business units.

Locality and Complexity of the Proposed Framework

In addition to the domains, data has a locality or position within the context of Internet and the organization's network of information resources (refer to Figure 16). Each locality envelopes the data until physical media is accessed, read, wrote or modified. These localities are (from storage to outside):

1. Data Storage
2. Host
3. Local Area Network (LAN)
4. Intranet
5. Wide Area Network (WAN)

   Boundary
6. Internet
7. Extranet

Data has one other quality that is not represented graphically within the framework. All data and information has a temporal quality. In other words, information changes over time. Representing this within the framework would be difficult, but it should be understood that this quality exists and cannot be ignored.

It should also be noted that not every organization will have resources located at each layer of internal framework structure. Many organizations do not have extranets connecting other organizations within their supply chain into their data resources. Some will not have intranets or Internet connections although this is rapidly changing within the small to medium organizations.

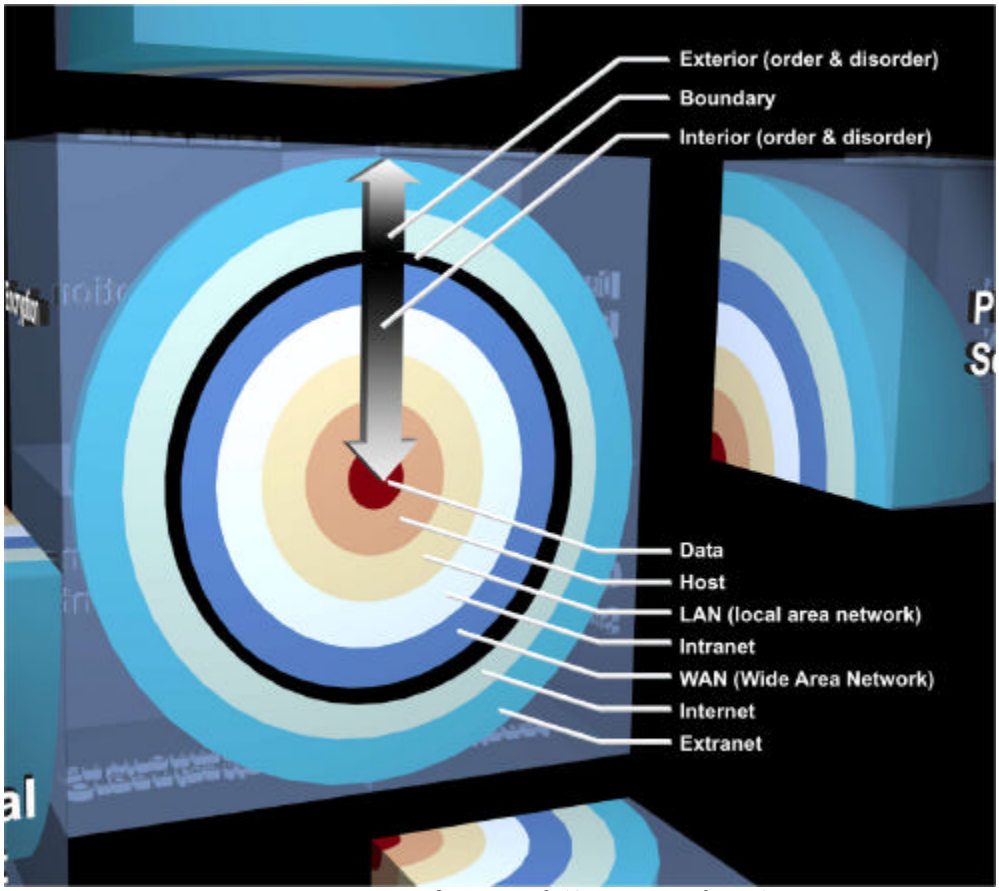


Figure 17 Proposed Framework (Cross-sectional View)

Data Storage

Traditionally, data storage has been direct attached storage (i.e. disk drives), floppy diskette, and tape. Today, the options for storing information have exploded. With this expansion of storage media types, security professionals have been faced with new challenges.

Storage Area Networks (SANs) have become the data platform of choice for large organizations. A SAN can present multiple hosts logical storage across high-speed fibre channels connections. This eases the data backup issue at the price of centralizing data storage. This creates the need to re-evaluate disaster recovery issues due to the highly customized nature of SANs.

CD\R, CDRW, and DVD/R have provided organizations with another potential security issue. With storage capacities reaching four gigabytes of data, a relatively small media form factor can transport vast quantities of data.

The most insidious storage media is flash RAM. This media format is extremely small and is the basis for most digital camera image storage. However, Microsoft has made this a plug and play 'feature' of the Windows family of operating systems. Most current Linux distributions also support this capability. The security issue is that data files may be transported on this media without impairing camera function. Merely seeing that a digital camera is working is not sufficient to guarantee that confidential data files are not on the device. Nearly all these devices do not require any device drivers for the operating system. Similar to flash RAM are the new USB attached external hard drives. These devices can easily store 40+ gigabytes of data and are about the size of a pack of cigarettes.

New forms of easily transportable storage media with higher and higher densities are being developed. The capability of storing 512 megabytes of data on a flash RAM module is a reality – one gigabyte is projected for early 2003.

Safeguarding storage and data against the new threats is a nearly impossible task. Some developers are beginning to address the USB storage issue, but no major vendor operating system vendor has done so as of this time.

Host

Nearly everyone recognizes the computer or host as the 'repository' of data transformation or processing. As noted in the prior section, traditional data storage has been confined to the host. While that may not be the case today, the host computer still performs the data processing function based on the applications available and running.

Security of the application programs occurs here. This is critical because it is the host that controls access via operating systems, applications, and any other controls to the data. It is the protection of the host that is the principle objective of the security process in most organizations.

Local Area Network

The lowest network layer is the local area network (LAN). The LAN provides for basic connectivity and communication between hosts. The most common networking protocol suite in use today is TCP/IP. In many organizations, multiple LANs are connected via a variety of wide area network technologies (frame relay, point-to-point, ATM, etc.) which allow interoperability with the TCP/IP protocol stack and services.

One area of concern in the LAN is the use of the Dynamic Host Configuration Protocol (DHCP). This is an administrative time savings, but allows minimally configured computers to be added and have basic TCP/IP connectivity within the organizational network. This allows an attacker with physical access to the network to gather data and other vital information without having to be authenticated to the organizations information systems.

Intranet

Intranets are usually intra-organizational in nature and extend across the boundaries of the LAN and WAN spheres. Therefore, within the proposed framework, the intranet sphere resides between the LAN and WAN spheres. Intranets generally utilize TCP/IP protocols and services to provide information to organizational members and to unify access to network data, services and applications. Intranets generally increase the complexity of information system architectures because access to legacy systems is commonly provided. The heterogeneous nature of the "back end" systems implies differing access control methodologies that may not be compatible or will be require alteration to provide intranet users with seamless access.

Wide Area Network

Traditionally, the WAN has been the boundary of the organizational information technology infrastructure. The main extension of the organization's infrastructure, in the past, has been dial-in access. Technologies and processes have been in place for many years to support this type of access to information resources. However, the business environment for many organizations has changed radically over the last ten to twelve years. Organizational requirements for Internet access and presence have driven the traditional boundary of the information infrastructure onto public and consequently anonymous networks.

The inter-organizational competition for customers and the need to improve the bottom line or reduce costs while increasing efficiencies has driven the increased access to internal resources via public networks for many organizations. In addition, international business pressures have forced many organizations to form business alliances and joint ventures that have information technology support and communications requirements. These issues have driven the formation of customer/client, vendor, joint venture partner, and other stakeholders to require the formation of extranets. The extranet is a secure connection between the organization and external stakeholders. In nearly every case, the extranet connects the resources of two or more organizations in a controlled

manner exposing only the information and data required to the other partners. Because many extranets utilize the Internet as the connecting network, the Internet sphere is placed between the WAN and the extranet.

Boundary

The boundary between the internal network of an organization and the Internet and extranets is commonly referred to as the 'edge of the network'. This is where the battle for information security is generally fought. It is also at this layer where maximum complexity occurs.

Firewalls, routers, another edge devices are deployed inside the boundary layer controlled general access into and out of the organizational network. Access control lists and authentication devices are the principal means of control. It is becoming a common practice for organizations to deploy content filtering of email and web access for legal reasons.

It is at the boundary layer where maximum complexity occurs. The internal complexities of an organization's information systems meet the external complexities of the Internet. Substantial research into the complexities involved had been summarized by Strogatz (2001). Strogatz enumerates the following complexity issues surrounding large networks exhibiting small-world network characteristics.

Structural Complexity – Taken as a snapshot, the physical complexity of an organization's network may be impossible to determine. In many cases, once a network cable has been installed, its physical location along its entire path is forgotten. This factor, combined with the need to see logical network diagrams, make understanding many physical networks nearly impossible.

Network Evolution – To paraphrase an old saying, "Wait ten minutes and the network will change". Networks and organizations evolve over time. This evolution is brought

about by the deployment of new services and the removal of services that are no longer needed. In large organizations, this can lead to systems that are running because they always have been there. This, in turn, can lead to security issues.

Connection Diversity – Not every organization is connected to the Internet with the same bandwidth, service provider, or services. An example would be that it is easier to perform a communications denial of service attack on an organization with a single 128 Kbps connection to the Internet than an organization with multiple T3 (45 Mbps) connections.

Dynamical Complexity – Simply put, not every node on the Internet receives the same level of traffic at the same time. There is a decidedly nonlinear nature to Internet communications paths and their related utilization.

Node Diversity – This is the easiest area to understand. While every organization may wish to maintain an Internet presence, there is no standard configuration for that presence. Multiple vendors' hardware and software will be combined in many unique configurations. Each configuration will have differing performance characteristics.

Meta-complications – Two or more of the proceeding areas combine to produce complications.

Internet

From a security perspective, the Internet is like having an open door in a storefront that is open twenty four hours a day. However, many organizations feel the advantages of having a web presence outweigh the potential dangers. This belief is prevalent throughout the business community because the Internet is the great equalizer. Every organization has an equal chance at being heard or seen no matter what their respective size.

This is also borne out by changes in society. It is now extremely commonplace to request someone's email address. The Internet as a interpersonal communications medium will continue to grow and organizations will continue to add access.

From a complexity perspective, the Internet is definitely a small-world network (Adamic 1999, Watts 1999). This results in nearly every accessible system being 4 to 5 links away independent of the underlying IP network route. This leads to greater exposure for the organization and a greater security risk.

Extranet

Organizations are utilizing extranets to automate their supply chains. Whether this is across the Internet or an extension of the wide area network of an organization, security issues abound. The primary concern is allowing another organization access to the data resources of the network. All layers and domains of the framework are brought into play when extranets are deployed.

An external organization's access must be limited to the information required by that organization to fill its obligation. This means from a policy perspective and a procedural process, access controls must be in place to manage access appropriately.

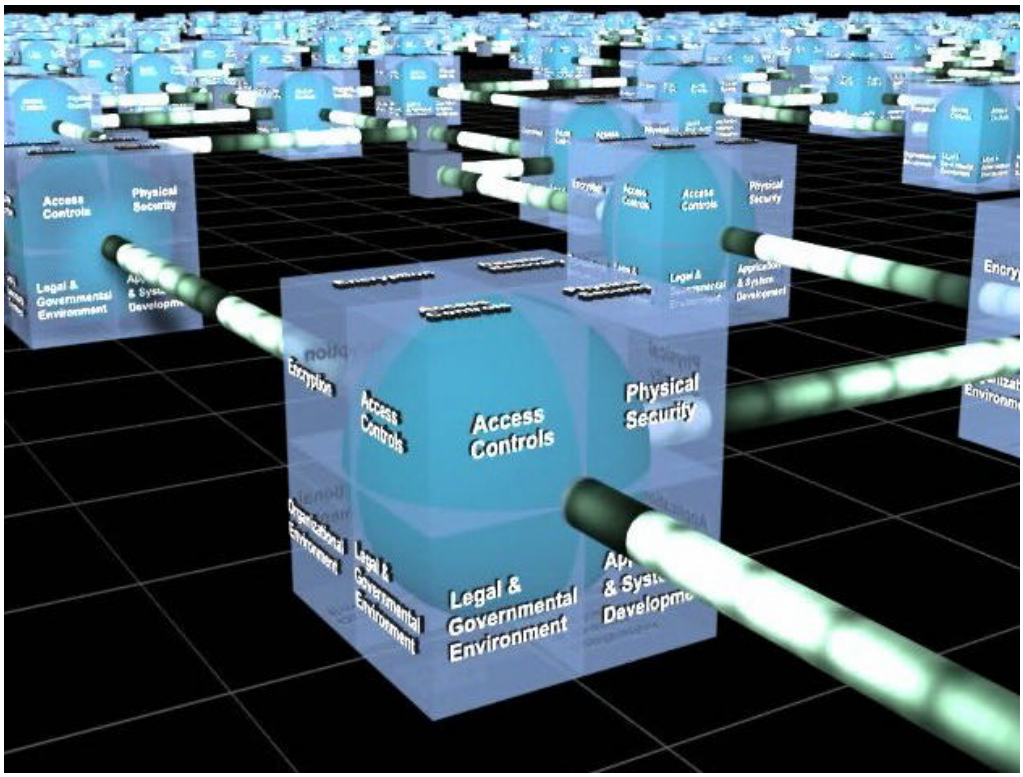


Figure 18 The security framework in relation to other organizations

Interaction on Public Networks

Public networks, such as the Internet, exist to ease and stimulate interaction between organizations and individuals. Networks are inherently social constructs linking individuals and organizations (Wellman 2001). Nearly any face-to-face event can occur on-line in cyberspace. Because of the social nature of the Internet, it is reasonable to assume that many human activities can be facilitated or enhanced in this environment. This leads to a key assumption: the Internet is the great equalizer.

Armed with the proper tools and knowledge, an individual can take on a large corporation, a third world country could wage economic warfare on the United States or Japan, or organizations could gain access to sensitive information about their

competitors. These are the wild cards for information systems security. It is impossible to know who or what may attack an organization's information systems via the Internet.

In addition, it is necessary to be a good neighbor when connected to the Internet. Any organization should take reasonable measures to secure their information systems so that others do not subvert their intended use. Email servers are prime targets when the server is configured to be an anonymous relay server. This allows spammers the ability to hide their "real" email address and prevents easy tracking of the true originator. Many of the technologies presently deployed to the Internet can be attacked and/or subverted. The failure of one organization to take appropriate security measures can have negative impacts on many other organizations.

Strogatz's list of potential complexities in small world networks could be extended to include social complexities. The interactions between individuals, businesses, and governments on the Internet are impossible to predict. The consequences of actions taken by these entities can be minor or massive. Your email may get lost on its way to the addressee, another Mafiaboy may choose to cause service outages resulting billions of dollars in damages (US Department of Justice 2000), or a terrorist may attack the control systems of the national power grid. It is impossible to predict the source and nature of an attack. While the attack may rely on technological tools, the reason for the attack depends on the motivation of the attacker.

CHAPTER 3

PROPOSED METHOD AND PROCEDURE

Data Collection

Data collection was performed over a seven-month period from May 2002 through November 2002. Log files are collected and archived for compliance reviews with bank regulators. The key log files are collected on a management platform and stored in multiple locations to monitor any changes. No log file should show signs of tampering. The log files maintained and used for this study include:

1. The firewall logs showing all levels of events and activities. These logs maintain source and destination IP address and port numbers.

2. Network operating system event logs showing system, user and application events. These logs are collected on an exception basis. These logs are generated by the internal email and file servers running Microsoft Windows 2000 Server.

3. Antivirus monitoring and detection logs show updates by platform and detected malicious code.

The internal logs are used in correlation with firewall logs to determine penetration events. Service provider audit logs are not examined within this study. There are no IP routes that allow access from the Internet or the AnyBank VPN to these services for this financial institution.

To review the nature the hostile hosts, NMAP will be utilized to scan all IP addressed that launch probes or attacks on the financial institution. A further determination will be performed to identify the host country of the IP address.

Data Analysis

Evaluation of the data collected falls into three timeframes. Prior to March 2002, this organization had no means of maintaining any data concerning the security of the network because no resources where in place to archive events. This situation prevented any analysis of security events beyond an average two week window depending on network activity. Between May 2002 and September 5, 2002, the initial firewall configuration was in operation and collecting data. In addition, internal monitoring of network activities was initiated and data collected for management and regulatory reporting functions. After September 5, 2002, an additional layer of packet filtering was enabled at the Internet router for the internal network. This filtering was designed to block private IP address ranges and various services that were security issues and not required by the organization for operation.

An independent auditing organization conducted an external penetration assessment during a two-week period during the second half of September 2002. The independent auditors conduct this testing according to regulatory requirements of the federal and state bank regulatory agencies. The findings of these reports will be discussed within the context of the data analysis.

An analysis of the organization's security policies and procedures in relation to the data sets will also be performed.

The Organization's Network

This financial organization maintains a single Internet connection for conducting business on the Internet. The organization also maintains a private connection to several third party service providers offering various banking service applications and information feeds. While the organization maintains a web presence, these services are hosted at another physical location and no direct connection exists to the internal network from the hosted Web servers. This configuration allows for the blocking of all inbound HTTP traffic to the organizational network.

The primary services that are allowed to transition the Internet boundary or edge of the network are:

1. Simple Mail Transfer Protocol
2. Post Office Protocol 3
3. Domain Name Service
4. Virtual Private Network Traffic

Wide Area Network connections maintained with two extranet service providers and the Federal Reserve System will not be examined.

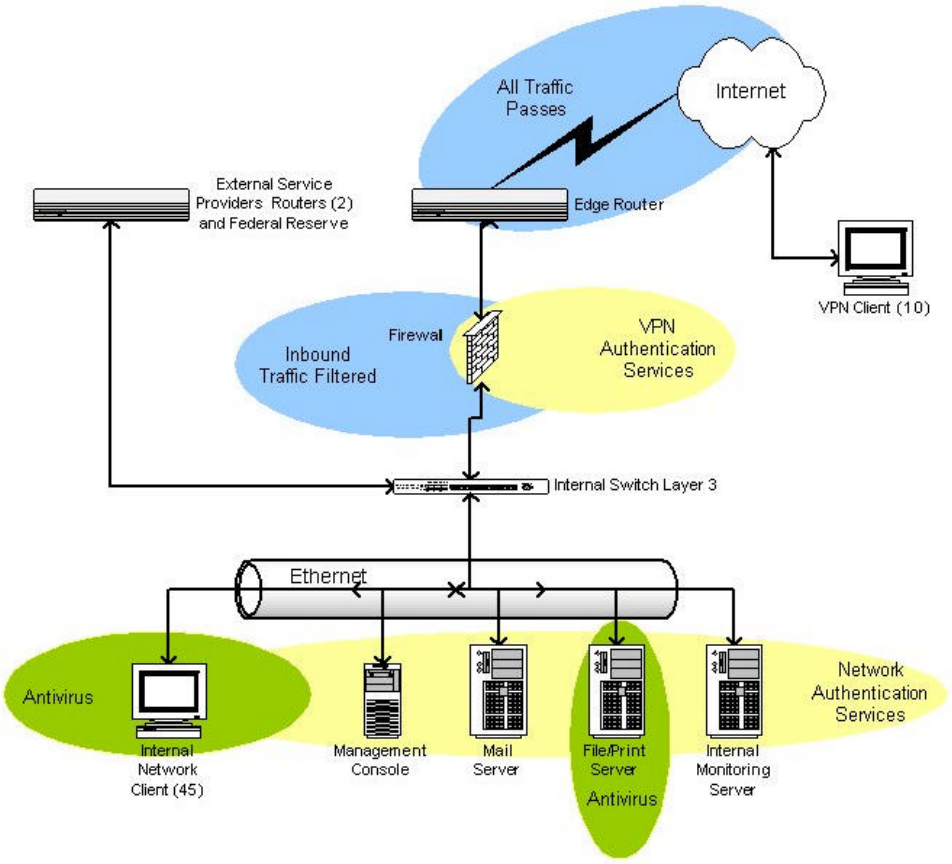


Figure 19 Organization Network before September 2002

Before March 2002, the organization network did not have any security layers beyond limited antivirus software and network authentication. Figure 19 shows the network security services implemented in March 2002 and in service until September 2002. The key aspects of the security environment during this time frame are:

1. The edge router is passing all traffic to the firewall.

2. Primary authentication occurs at the network operating system or host layer for all internal services.

3. All VPN traffic is limited to employees, but they have full access.

4. Antivirus services are manually updated on an ad hoc basis by the users at the workstations and automatically at the file and print server.

This network experienced one virus outbreak during this time frame and no detected intrusions.

Figure 20 (page 62) shows the changes that occurred in September 2002. This network remained stable structurally, but additional security layers were added. These alterations included:

1. The antivirus solution was extended to cover all host platforms inside the network. All email is scanned for malicious code and no executable attachments are allowed.

2. The edge router had access control lists added to block external access to all RFC 1918 private IP address ranges via directed routing. Further access controls were instituted to block access to Netbios/Netbeui ports, Simple Network Management Protocol ports, Remote Procedure Call ports, and Telnet ports.

3. VPN traffic was segregated to allow for granular control of external access. Since no web-based email services are allowed, simple email access is granted via VPN access. Dependent upon the user's access requirements, additional network-based file services are available via the VPN.

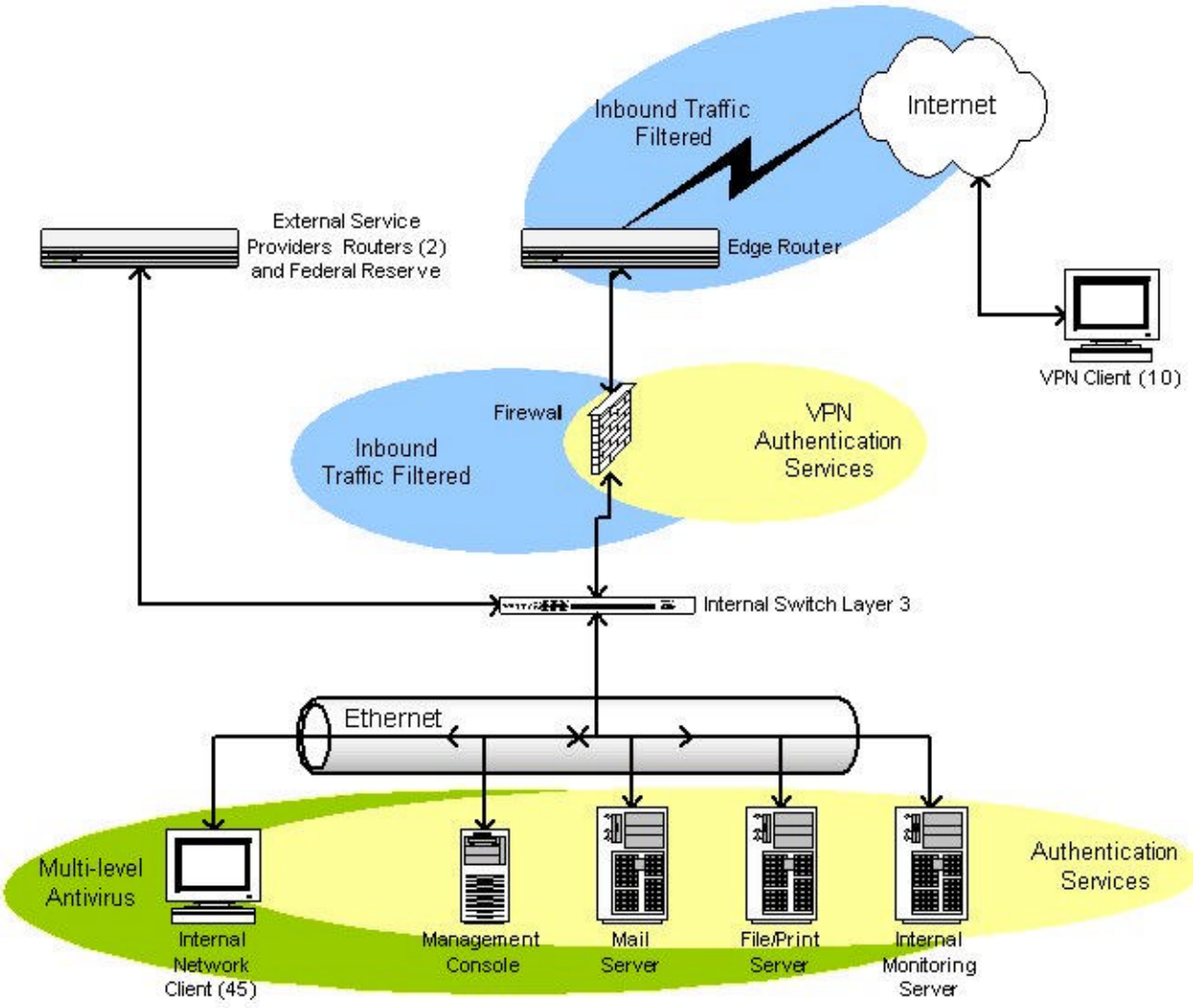


Figure 20 Organization Network after September 2002

CHAPTER 4

RESULTS

Data Sources

Data was generated or obtained from the following sources:

- Internal Event Logs – The security event logs record all successful and failed login attempts that occur on the network. The security logs also monitor the status of each user account for account lockouts.

- PIX Log Files – The firewall log files record all granted and denied traffic in and out of the network. These log files record:

    - Date and time the IP packet was presented to an inside or outside interface on the firewall,

    - Whether the frame passed or denied,

    - If the frame was denied, the level of concern from informational to critical,

    - If the frame was denied, a description of the reason for dropping the frame,

    - The source IP address and port number,

    - The destination IP address and port number,

    - And additional information as required.

- Server-based Anti-virus log files – These files record the viruses, Trojans, and other suspicious files that were detected and removed. The primary log files are from the core file server and the email server.

- Internet assigned IP address ranges – These files are issued monthly or on an as needed basis. These files include the IP networks allocated by the four regional authorities. These ranges were used to identify originating country of the source IP address. These authorities are:

    - American Registry of Internet Numbers (ARIN) – This authority issues IP address ranges for North and South America and Southern Africa.

    - Asia Pacific Network Information Centre (APNIC) – This authority issues IP address ranges for the Asia Pacific region.

    - Regional Latin-American and Caribbean IP Address Registry (LACNIC) – This is a newer authority which handles IP address ranges for Latin America and some Caribbean islands.

    - Réseaux IP Européens Network Coordination Centre (RIPE NCC) – This is the authority for Europe and surrounding areas.

- NMAP Log Files – Approximately 4215 IP addresses were identified as attacking hosts. These log files were generated by NMAP (a public-source enumerating software package) when scanning the attacking IP addresses to determine the DNS name and available (open and filtered) ports.

Overall Traffic

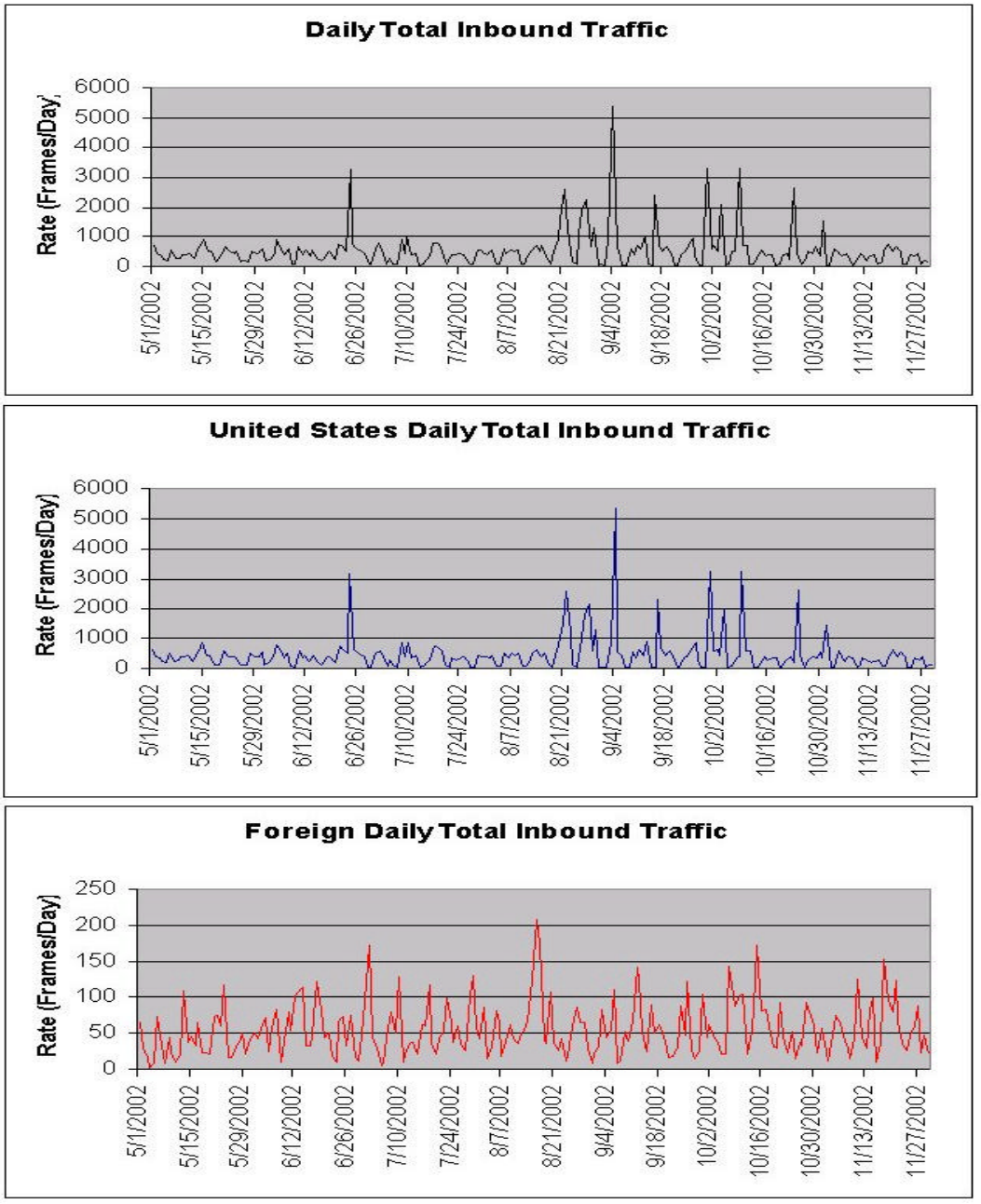


Figure 21 Total Daily Traffic

Figure 21 shows the total inbound traffic to the financial institution. The traffic is extremely variable. The traffic is further segregated into traffic originating from IP addresses in the United States and all other countries. The majority of traffic originates from IP addresses associated with IP networks assigned to the United States.

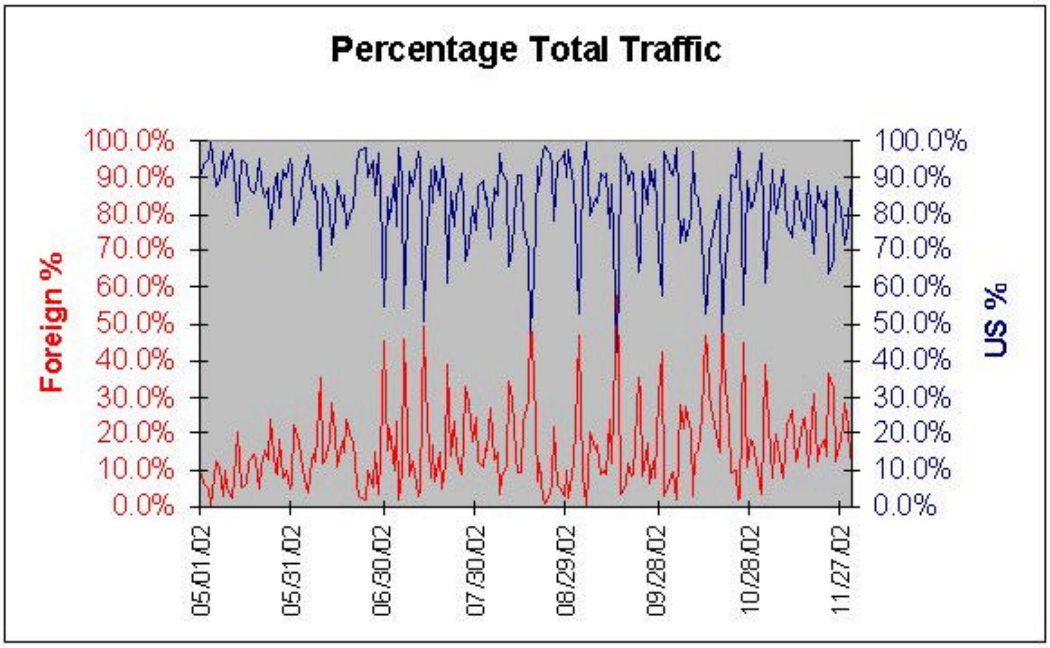


Figure 22 Percentage of Total Traffic (US vs. Foreign)

Figure 22 compares traffic originating from the United States versus all other countries as a percentage of the total daily traffic. While the majority of traffic consistently originates from the United States, on three occasions traffic from other countries actually exceeded the traffic coming from IP addresses assigned to networks in the United States.

	Foreign	United States	Total Packets
Average Daily Packets	55.7	486.9	542.6
Median Daily Packets	47	387	442
Maximum Daily Packets	209	5328	5372
Minimum Daily Packets	2	28	48

Table 3 Total Traffic

Table 3 bears out the wide variation in shown in figures 22 and 23. Traffic originating from foreign IP addresses consistently remains approximately 10% of the average US originating traffic. There were only three occasions foreign traffic exceeded US traffic (Table 4).

Date	Foreign Packets	US Packets	Total Packets	% Foreign	% US
08/17/02	175	160	335	52.2%	47.8%
09/14/02	55	40	95	57.9%	42.1%
10/19/02	31	28	59	52.5%	47.5%

Table 4 Foreign Total Traffic > Total US Traffic

Each of the dates where foreign traffic exceeded traffic originating from the United States was a Saturday. This is the exception when the total traffic is evaluated for the day of the week.

	Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
Foreign Average	29.3	73.9	77.3	59.2	62.0	61.4	27.2
Foreign Median	28.5	70.0	72.0	64.0	52.0	51.0	20.0
Foreign Maximum	54	154	172	128	140	209	175
Foreign Minimum	8	21	33	9	11	6	2
US Average	**113.3**	**667.3**	**534.7**	**823.7**	**558.8**	**583.1**	**122.5**
US Mean	**73.5**	**416.5**	**424.0**	**522.0**	**417.0**	**443.0**	**77.0**
US Maximum	**490**	**3,204**	**1,793**	**5,328**	**2,602**	**2,041**	**653**
US Minimum	**38**	**38**	**271**	**179**	**58**	**165**	**28**
Total Average	142.6	741.2	612.0	882.9	620.8	644.5	149.7
Total Mean	114.5	503.0	523.5	547.0	451.0	500.0	96.0
Total Maximum	500	3,309	1,880	5,372	2,655	2,078	671
Total Minimum	57	72	304	209	81	214	48

Table 5 Total Traffic Day of Week

The majority of traffic, whether originating in the United States or in a foreign country, occurs Monday through Friday. Traffic originating from US IP addresses remains at over 90% of the total by average day of the week analysis.

External traffic was designated as hostile or attack traffic when the traffic met one or more of the following characteristics:

- External traffic was directed against the two public IP addresses of the edge router.

- OR -

- External traffic was directed against the external interface of firewall.

- OR -

- External traffic was directed as the public IP address of the financial institution's email server.

- AND -

- External traffic was directed at a common TCP service port (File Transfer Protocol (FTP), Secure Shell (SSH), Domain Name Service (DNS), Hyper Text Transport Protocol (HTTP), Remote Procedure Call (RPC), Authentication Protocol, the TCP NetBIOS service ports (135-139), Simple Network Management Protocol (SNMP), or Microsoft SQL Server TCP service).

- OR -

- External traffic was directed at the financial institution's email service ports (Simple Mail Transfer Protocol (SMTP) or Post Office Protocol 3 (POP3)).

- OR -

- External traffic was probing well known Trojan/worm TCP ports.

With the exception of the email services of the financial institution, none of the services chosen for attack criteria are allowed beyond the firewall. Furthermore, the selected services are not running on any of the hosts with public IP addresses. This should catch most probes and attempted attacks against these services.

Originally, there was one other selection criterion for hostile traffic. If an external host was scanning a wide range of TCP service ports, then that host was defined as hostile and all traffic originating from that host's IP address would be considered attack traffic. This selection criterion was not met with the data collected for this study.

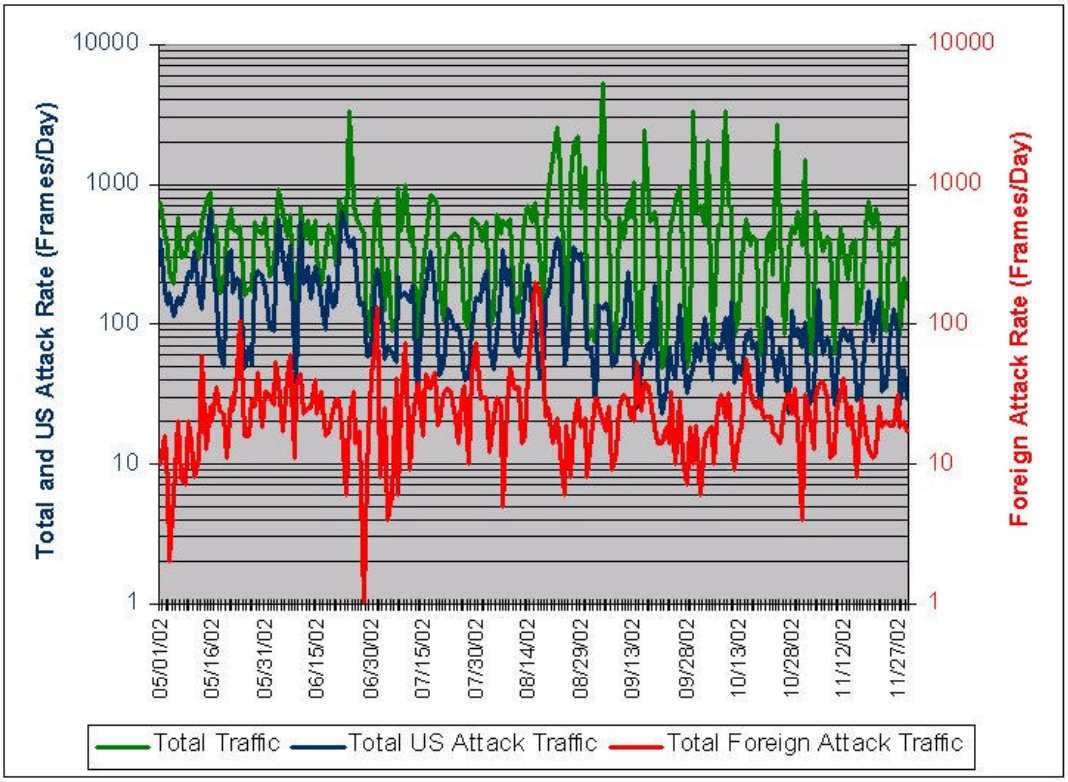


Figure 23 Daily Total and Attack Traffic

Figure 23 shows the relationship between the daily total traffic and attack traffic originating from US and foreign-based IP addresses. This financial institution only allows email traffic into the organizational network. All of this traffic is SMTP-based

traffic. No other services are allowed inbound from the Internet. It is immediately apparent that significant levels of hostile traffic were present over the course of this study.

The variability of the traffic, both total and attack, is high. Figure 23 shows the magnitude of the variability. Table 6 shows the standard descriptive statistics for the total traffic.

	Total Traffic	US Traffic	US Attack Traffic	Foreign Traffic	Foreign Attack Traffic
Mean	542.743	486.981	137.958	55.762	26.435
Standard Error	42.784	42.229	7.771	2.544	1.562
Median	442	387	97	47.5	22
Mode	500	267	66	44	18
Standard Deviation	625.870	617.760	113.686	37.221	22.846
Variance	391712.981	381626.854	12924.435	1385.412	521.928
Range	5324	5300	637	207	201
Minimum	48	28	23	2	1
Maximum	5372	5328	660	209	202
Sum	116147	104214	29523	11933	5657
Count	214	214	214	214	214
Largest(1)	5372	5328	660	209	202
Smallest(1)	48	28	23	2	1
Confidence Level(95.0%)	84.334	83.241	15.319	5.015	3.078

Table 6 Total Traffic vs. Attack Traffic

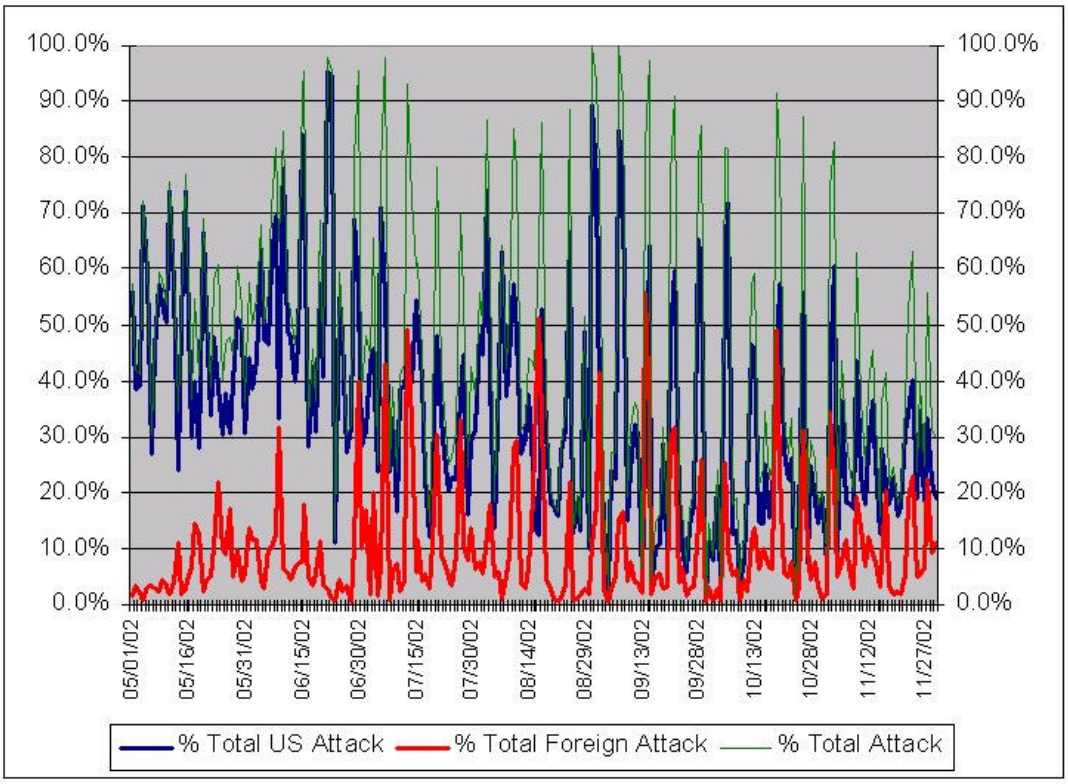


Figure 24 Percentage of Attack vs. Total Traffic

In order to evaluate the variability of the attack traffic to total traffic, all traffic gathered in this study was reduce to total daily percentages. Figure 24 shows the total attack, US attack, and foreign attack traffic as a percentage of the total traffic received by the financial institution. The percentage of traffic that is hostile is frequently > 50% of the total traffic.

User Password Controls

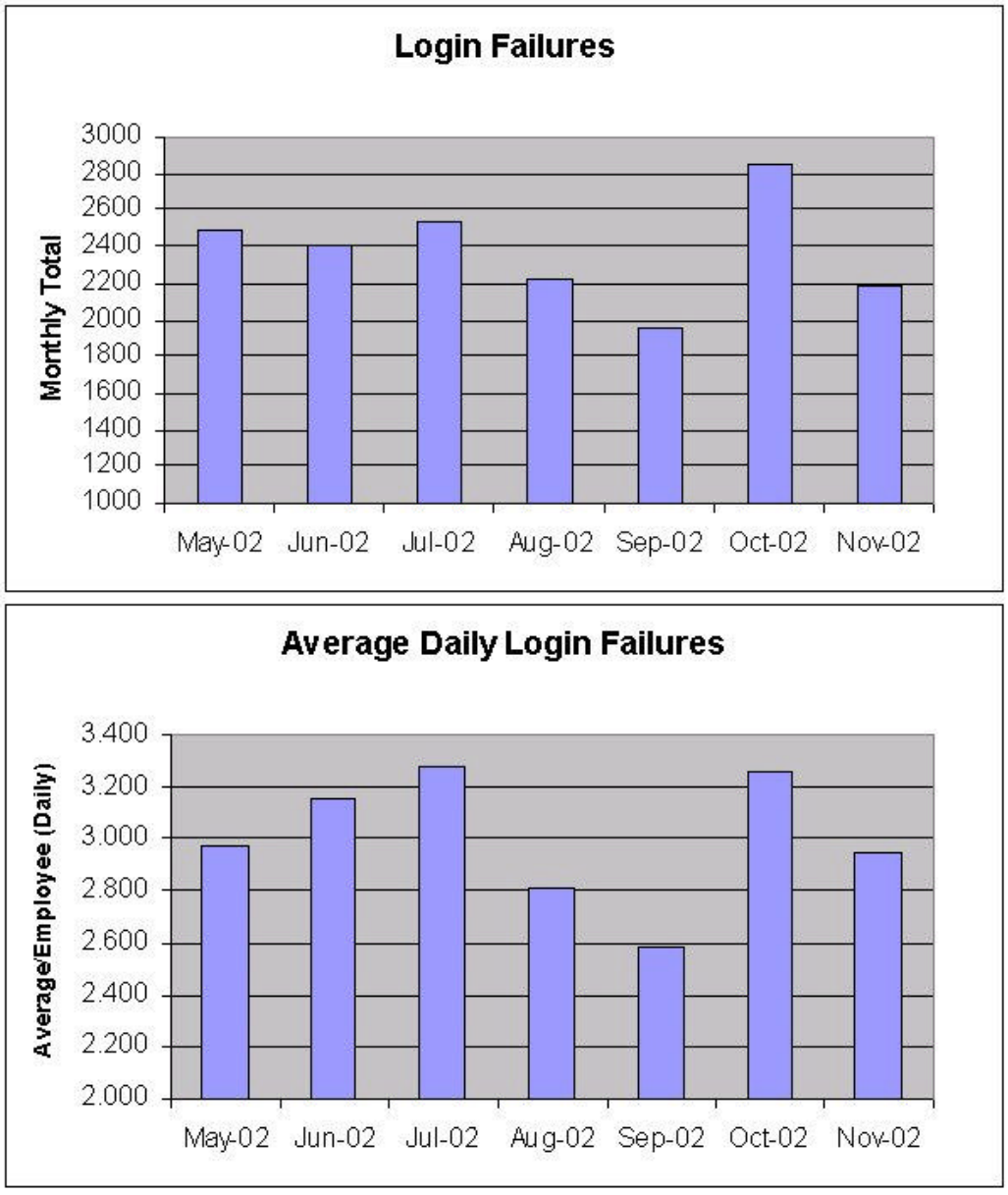


Figure 25 Network User Login Failures

Network user login failures were used as a means to determine whether or not unauthorized access was occurring. Anonymous access, administrator access, software

operating as the system (i.e. Microsoft Exchange), and normal user access were tracked. Anonymous and administrator access attempts were nonexistent. However, network users seemed to have a high number of login failures (see Figure 24).

Password security is a high priority at the financial institution. The following describes the network user password requirements (refer to Appendix A: Policies and Procedures):

1. Passwords must be changed every thirty (30) days. This is enforced by the network operating systems in use.

2. Passwords must have at least eight (8) characters. Every password must contain at least one uppercase, one lowercase and one numeric character. This is enforced by the network operating systems in use.

3. After three (3) incorrect attempts, the network operating systems will lock out the account requiring administrator intervention. The lock out time is 60 minutes and is enforced by the network operating systems.

4. Screen savers must automatically activate after fifteen (15) minutes of non-use and require the users or an administrator account to unlock. This is enforced by network group security policies that are checked and updated (if needed) every time a user logs into the network.

5. Network users are prohibited from writing down passwords within their work areas. This is enforced by periodic physical security sweeps through the building by independent security consultants.

Upon review of the system, security logs for login failures and lockouts, it was discovered only one account has been locked out during the seven-month period of this study. The high rate of login failures was suspicious until the employees were interviewed. It was determined that majority of the login failures resulted from simple

mistakes while entering the password or forgetting the password shortly after changing it.

Network Access Control Layers

From approximately May 1, 2002, through September 4, 2002, the financial institution maintained a Cisco PIX firewall between the Internet and internal network resources. On approximately September 4, 2002, the edge router connected to the Internet was reconfigured to drop specific traffic. The reconfiguration was done for two reasons. First, it was determined that certain types of network traffic (i.e. telnet sessions, etc.) would never be allowed to enter the internal network from the Internet. It was reasoned that this would result in an improved in the performance of the firewall because there would be less traffic to analyze. The second reason was to add another filter layer at the edge of the network. Review of the May through August 2002 firewall logs indicated that the highest level of hostile traffic was directed at the NetBIOS TCP service ports. In addition, remote procedure call (RPC), simple network management protocol (SNMP), Microsoft Active Directory Services, and telnet access was blocked from any traffic originating on the Internet.

Additional changes were made to disallow directed IP packets (packets that contain the complete path a packet must take), large IP packets (to prevent teardrop and other forms of denial of service attacks), small IP packets (to prevent fragmentation attacks), and traffic from any private IP address. The private IP addresses defined in RFC 1918 are used on many networks to make sure organizations have enough IP addresses for internal use. The IP address ranges blocked included: 10.0.0.0 – 10.255.255.255, 172.16.0.0 – 172.31.255.255, and 192.168.0.0 – 192.168.255.255. These IP addresses are not generally allowed to transit the Internet, but may be used if directed packets are used in the attack. This is a spoofing attack. It is designed to fool the target network into believing that IP packet is from a valid host.

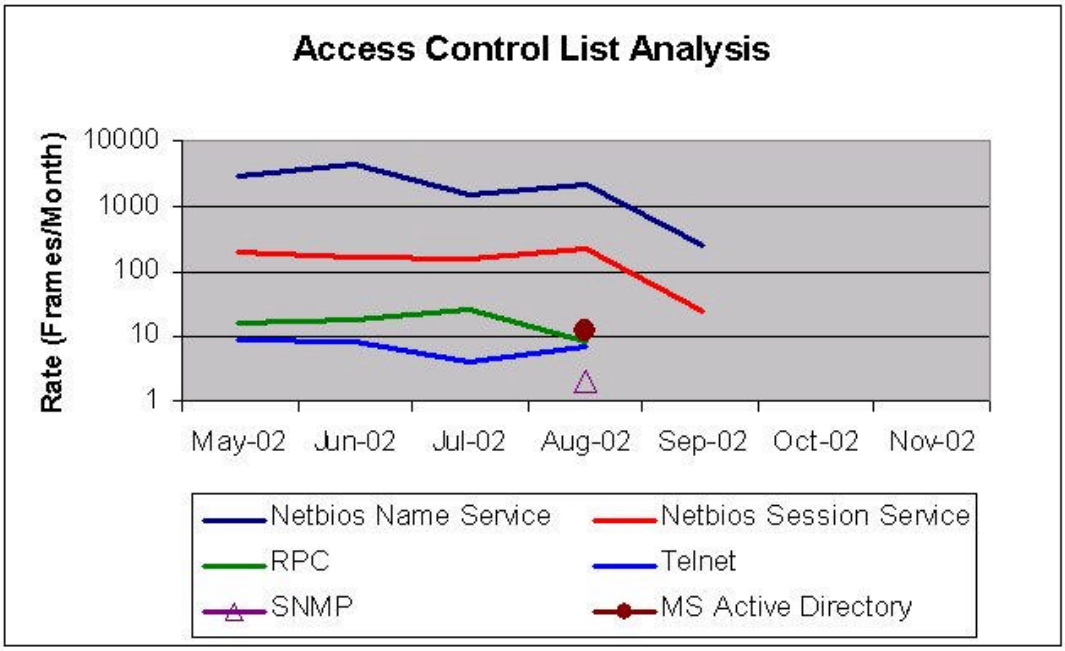


Figure 26 Network Access Control Services

The access control list (ACL) modification had the intended effect at the firewall. As of implementation of the new ACLs, traffic directed at the NetBIOS TCP ports fell to zero for all remaining months. Telnet, SNMP, Microsoft Active Directory, and RPC traffic had a much lower and sporadic frequency, but no further attacks were detected on these ports at the firewall. All other traffic (from non-private IP addresses) continued to be passed to the firewall.

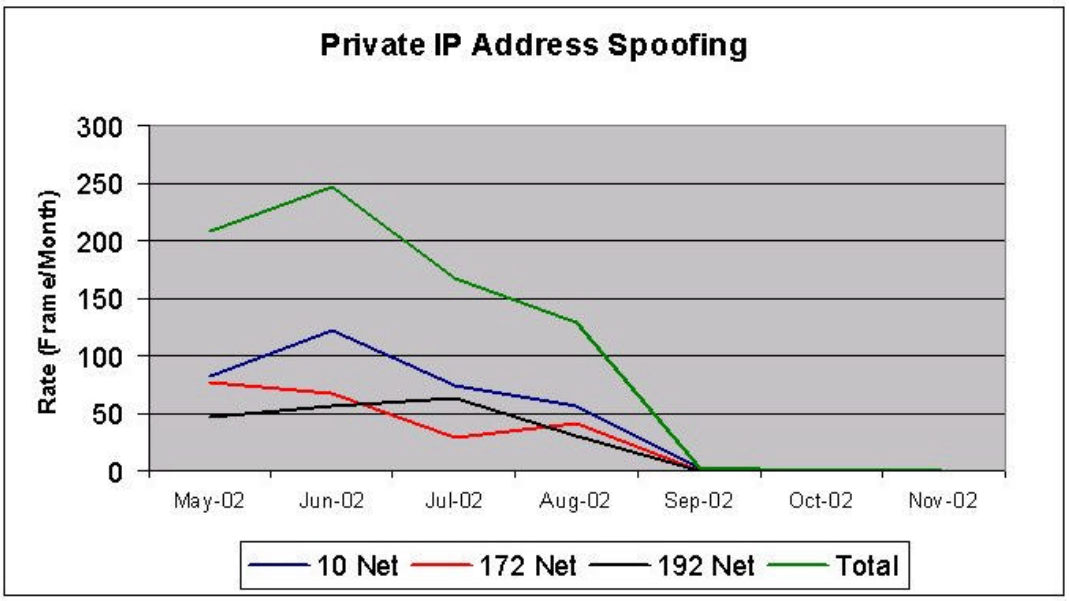


Figure 27 Private IP Address Spoofing Attempts

At the same time key ports were blocked, all RFC 1918 private addresses were blocked from entering the internal network from the Internet. Analysis of inbound traffic indicates from May through September 2002 significant spoofing of RFC 1918 private addresses was occurring. During the September through November 2002 timeframe, no further RFC 1918 private address spoofing occurred.

Anti-Virus Layers

The main file and print server was originally configured to be the principal anti-virus server. The server was also configured to scan all inbound and outbound traffic for viruses. All workstations were configured to obtain virus signature file updates individually. All workstations were configured to report virus detection to the file and print server. No email messages were scanned for viruses or other malicious code.

At the beginning of September 2002, the email server was configured to be the principal anti-virus server on the network. The file and print server and all workstations reconfigured to check with email server on a daily basis for new virus signature files.

The email server was configured to check with the software vendor for signature file updates every day. All servers and workstations were configured to report virus detection to the email server for reporting.

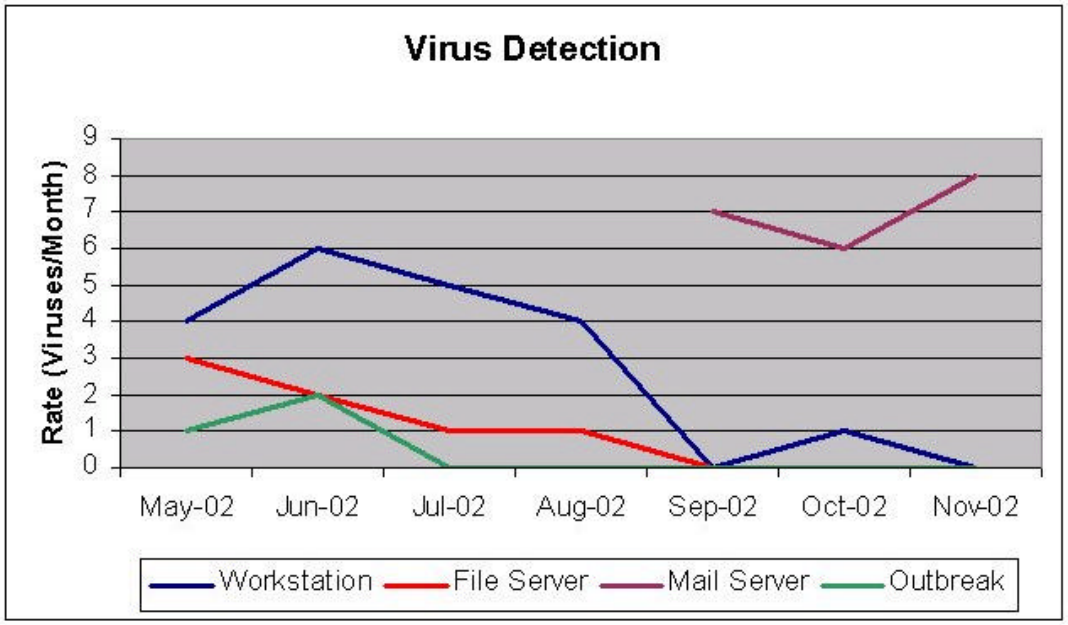


Figure 28 Virus Detection by Layer

Figure 27 illustrates the detection of viruses over the period of this study. The main file and print server did not detect significant numbers of viruses when compared to the viruses reported by the workstations. This indicates that core file server was probably not the primary vector for infection during the months of May through September 2002.

There were two outbreaks of viruses during the months of May and June 2002. These outbreaks occurred within three days of each other. An outbreak for the purpose of this study was defined as the same virus appearing on more the three workstations concurrently.

Figure 27 also shows that when the mail server became the primary anti-virus server and all email messages were scanned, the total number of viruses detected increased while the

number of viruses detected at the workstations and the file server decreased sharply. There was one virus detected on a workstation during the month of October 2002. This detection was made on an employee's diskette that was brought in from home. The employee's home PC was determined to be infected and was cleaned by the IT staff of the financial institution. It appears that the primary vector of viral infection in this financial institution's network is email messages and their associated attachments.

Complexity of Attack

There are two areas of complexity that were reviewed during the course of this study. The first area concerns the nature of the hosts originating the designated hostile or attack traffic. The second area concerns the attacks themselves. In the second area, the types of exploits were not evaluated except for known Trojan ports.

Month	Foreign	% Foreign	US	% US	Total
May-02	218	20.1%	867	79.9%	1085
June-02	249	24.5%	769	75.5%	1018
July-02	293	27.9%	758	72.1%	1051
August-02	224	20.7%	858	79.3%	1082
September-02	226	24.4%	699	75.6%	925
October-02	249	24.7%	759	75.3%	1008
November-02	244	25.6%	710	74.4%	954
Total	**1703**	**23.9%**	**5420**	**76.1%**	**7123**

Table 7 Unique IP Addresses

1. The total number of hosts detected over the course of this study is shown in table 7. In evaluating these addresses, only three IP addresses were found in more than one month. All repeating IP addresses were from foreign address ranges. The relative distribution of IP addresses (foreign vs. United States) is consistent with the percentages of allocated addresses reported by the various Internet Assigned Numbers Authority (IANA) approved Regional Internet Registries.

Registry	United States	Foreign
ARIN	1,845,863,507	341,055,304
APNIC		114,063,760
LACNIC		139,211,536
RIPENCC		135,172,608
Total	1,845,863,507	729,503,208
Percentage	72%	28%

Table 8 Allocated Addresses by Registry

Table 8 shows the allocated IPv4 addresses as of December 2002. When reviewing the overall distribution between foreign and US IP addresses, the percentages do not vary significantly. What is significant is that the financial institution does not have any foreign or overseas accounts.

Table 9 shows the number of unique hosts that were determined to meet the attacker criteria of this study. The evaluation is shown by attacked service or known Trojan port. With the exception of Simple Mail Transfer Protocol, none of the services shown in Table 9 are externally available.

Service / Trojan	Unique IP Addresses
Hyper Text Transport Protocol (HTTP)	2183
NetBIOS Name Service	608
Microsoft SQL Server	520
Authentication Protocol	293
File Transfer Protocol (FTP)	281
Secure Shell (SSH)	92
Domain Name Service (DNS)	83
Simple Mail Transport Protocol (SMTP)	52
GateCrasher Trojan	41
Remote Procedure Control (RPC)	31
NetBIOS Session Service	18
SubSeven Trojan	13
Total	**4215**

Table 9 Designated Attacker IP Addresses

Internally, the only services running on the financial institutions network are the NetBIOS and DNS services. The financial institution's Web Server is hosted off-site

and there is no linkage to the internal network. Web Server hosting is a common practice in the financial services industry to reduce the external exposure of the financial institution. Each of the services and Trojans shown in table 8 will be discussed in the next section.

NMapWin (freely available from www.insecure.org) was utilized to determine the nature of the host IP addresses that were designated as hostile. There were some basic assumptions made in the configuration of NMapWin:

1. The hostile host could be any platform including penetrated servers acting as proxies to dial-up account IP addresses. For this reason, SYN Stealth scanning was selected as the default method for penetration of firewalls.

2. An attempt to determine the hostile host operating system would be made depending on responses to the specific probes.

3. An attempt to determine the services (filtered and unfiltered by a firewall) would be made.

4. An attempt to resolve the hostile host's DNS name would be made to determine type of host (dial-up, broadband, or server).

5. All 4215 designated hosts were scanned.

	Count	% of Hostile Hosts	% of Detected Hosts
Resolved a DNS Name	1731	41.1%	24.3%
Resolved a dial-up DNS Name	485	11.5%	6.8%
Resolved a broadband DNS Name	538	12.8%	7.6%
Resolved an EDU Domain Name	109	2.6%	1.5%
Resolved non-EDU Domain Name	599	14.2%	8.4%
No DNS Name resolved	2484	58.9%	34.9%

Table 10 Hostile DNS Name Analysis

Table 10 shows the results of NMapWin scan for DNS names. Only 24.3% of all detected hosts resolved a DNS name. This is a common problem in the determination of the identity of the attacker. This is further illustrated by the number of hosts that resolved no DNS name.

Hostile hosts originating from dial-up accounts and broadband connections accounted for approximately 24.3% of all identified DNS names. These hosts have a high probability of being actual attackers. The hostile hosts that resolved to any other DNS name showed a wide variety of services available. Most the remaining DNS name identified platforms had a high likelihood of being servers for external organizations. The external servers that were identified by DNS name have a high likelihood of not being the primary attacker.

The 4215 hosts identified as hostile were also scanned for services that they were running. Table 11 summarizes the top services found to be running on the hostile hosts.

Service	Number of Hosts	Percentage of Hostile Hosts
Hyper Text Transport Protocol (HTTP)	994	23.6%
NetBIOS Name Service	987	23.4%
Microsoft SQL Server Service (MSSQL)	632	15.0%
File Transfer Protocol (FTP)	577	13.7%
Simple Mail Transfer Protocol (SMTP)	564	13.4%
HTTP over SSL (HTTPS)	494	11.7%
Microsoft Active Directory Services (MS-ADS)	480	11.4%
Domain Name Service (DNS)	333	7.9%
Post Office Protocol 3 (POP3)	167	4.0%
Secure Shell (SSH)	160	3.8%
Network News Transport Protocol (NNTP)	125	3.0%
Internet Message Access Protocol (IMAP)	125	3.0%
Telnet	90	2.1%
Spooler	61	1.4%
Remote Procedure Call (RPC)	48	1.1%
Identification Protocol (IDENT)	35	0.8%

Table 11 Hostile Host Services

Basic information can be gleaned from Table 11 about the structural complexity of the hostile hosts. Many of the services are considered to be server level services. In particular, a significant number of the hostile hosts appear to be email servers. This is indicated by the SMTP, POP3, and IMAP services.

Another group appears to be Microsoft Windows Services as indicated by the MSSQL and MS-ADS services running on these platforms. The NetBIOS Name Service does not necessarily indicate that the host is Windows-based platform. Many UNIX and Linux operating systems run SAMBA services. SAMBA service is a compatibility service that allows UNIX and Linux platforms to communicate with Windows-based platforms.

Traffic was collected on the basis of external source IP address and destination service port. With the exception of SMTP, none of the services examined are available for external use. The method for selection of a service for further analysis was based on the volume of total traffic received at the outside interface of the firewall of the financial institution over the seven month period of the study. SMTP traffic did not fit this profile, but was included for analysis because it is the only unauthenticated externally available service. The services selected are:

1. Simple Mail Transfer Protocol (SMTP)
2. File Transfer Protocol (FTP)
3. Secure Shell (SSH)
4. Domain Name Service (DNS)
5. Hyper Text Transport Protocol (HTTP)
6. Identification Protocol
7. Remote Procedure Call (RPC)

8. NetBIOS Name Service

9. NetBIOS Session Service

10. Microsoft SQL Server

NetBIOS Name Service and the other NetBIOS services are running internally at the financial institution. However, none of the remaining services are running on the internal network. All of this traffic is considered by definition to be hostile.

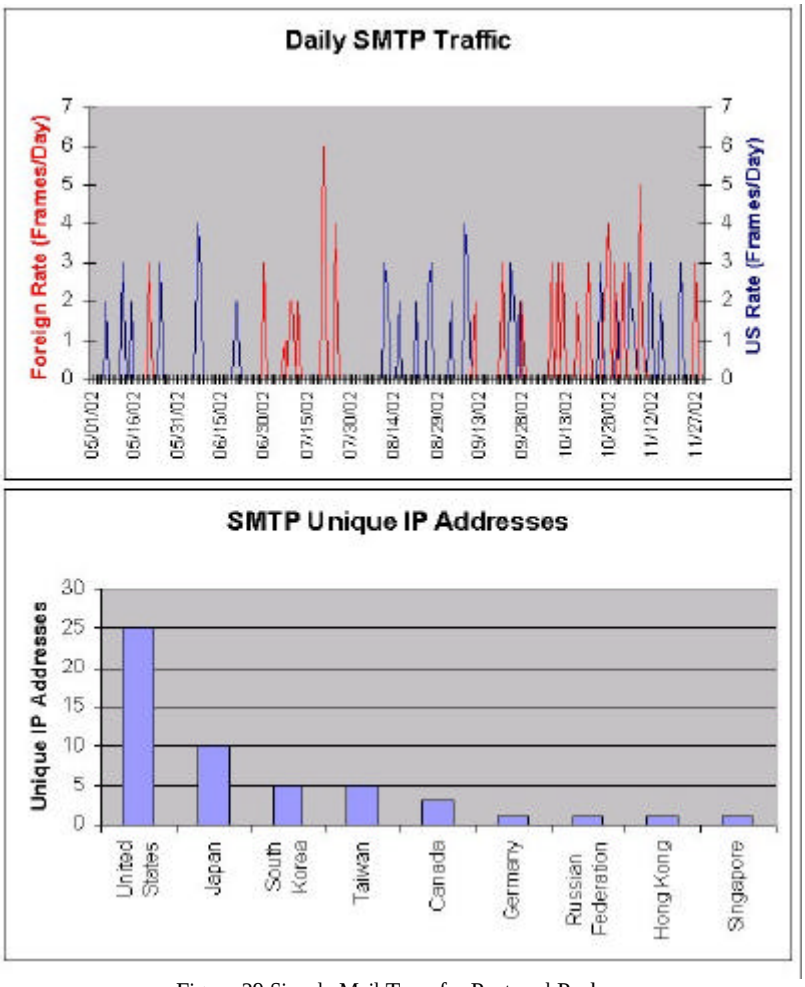


Figure 29 Simple Mail Transfer Protocol Probes

There are many reasons to break into a STMP server. Some of the more common reasons are:

- Compromising the server to relay email for a spammer,
- Denial of service,
- Or compromising the server to attempt further intrusion into the system.

In all cases, it is necessary to determine if the SMTP service is running on the target host. Table 12 looks at the number of frames sent by each hostile host on a session basis. There is consistentency in the number of frames, on average, from each attacking host. In the single event where six frames were sent to the financial institution's SMTP server, this was the only remote attempt to gain control over the server. These attacks are consistent with banner grabbing.

Simple Mail Transfer Protocol	Foreign	US
Average	2.48	2.88
Median	3	3
Mode	3	3
Maximum	3	6
Minimum	1	2
Unique IP Addresses	27	25

Table 12 Simple Mail Transfer Protocol Traffic by Unique IP Address

There was one instance were the attacking host sent more than three frames. In this case, the firewall blocked the attack. The attack was an attempt to determine if the financial institution's SMTP server was an open relay. This is indicative of an attempt to utilize the financial institution's server as a relay for spam email.

Figure 29 shows the daily rate of hostile traffic experienced by the financial institution over the period of this study and the source countries based on their IP addresses. The attack rate is sporadic and not constant. The countries attacking based on allocation of

IP addresses shows significance only in the total foreign IP addresses versus US IP addresses. The US to foreign allocation of IP addresses for the hostile SMTP traffic is 48.1% US to 52.9% foreign. However, total traffic shows that US-based IP addresses account for 51.1% of all frames while foreign-based IP addresses account for 48.9%.

	Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
Foreign Average Daily	0.40	0.23	0.27	0.32	0.29	0.23	0.45
Foreign Median Daily	0	0	0	0	0	0	0
Foreign Maximum	6	4	3	3	4	5	3
Foreign Minimum	0	0	0	0	0	0	0
US Average Daily	0.33	0.50	0.43	0.16	0.19	0.58	0.16
US Median Daily	0	0	0	0	0	0	0
US Maximum	4	3	3	2	2	4	3
US Minimum	0	0	0	0	0	0	0
Total Average Daily	0.73	0.73	0.70	0.48	0.48	0.81	0.61
Total Median Daily	0	0	0	0	0	0	0
Total Maximum	6	4	3	3	4	5	3
Total Minimum	0	0	0	0	0	0	0

Table 13 Simple Mail Transfer Protocol Day of Week

Table 13 shows that the foreign-based hostile hosts were more likely to attempt an attack on the weekend, while US-based attackers preferred Mondays and Fridays. Overall, the attacks based on day of week analysis are fairly constant. However, the total number of frames used by an attacker rarely rises to a significant level and could be easily missed in the logs of a firewall. The daily frequency histograms for US and Foreign SMTP hostile traffic (refer to Appendix 3) show that confirm the relative low number of days when attacks occur.

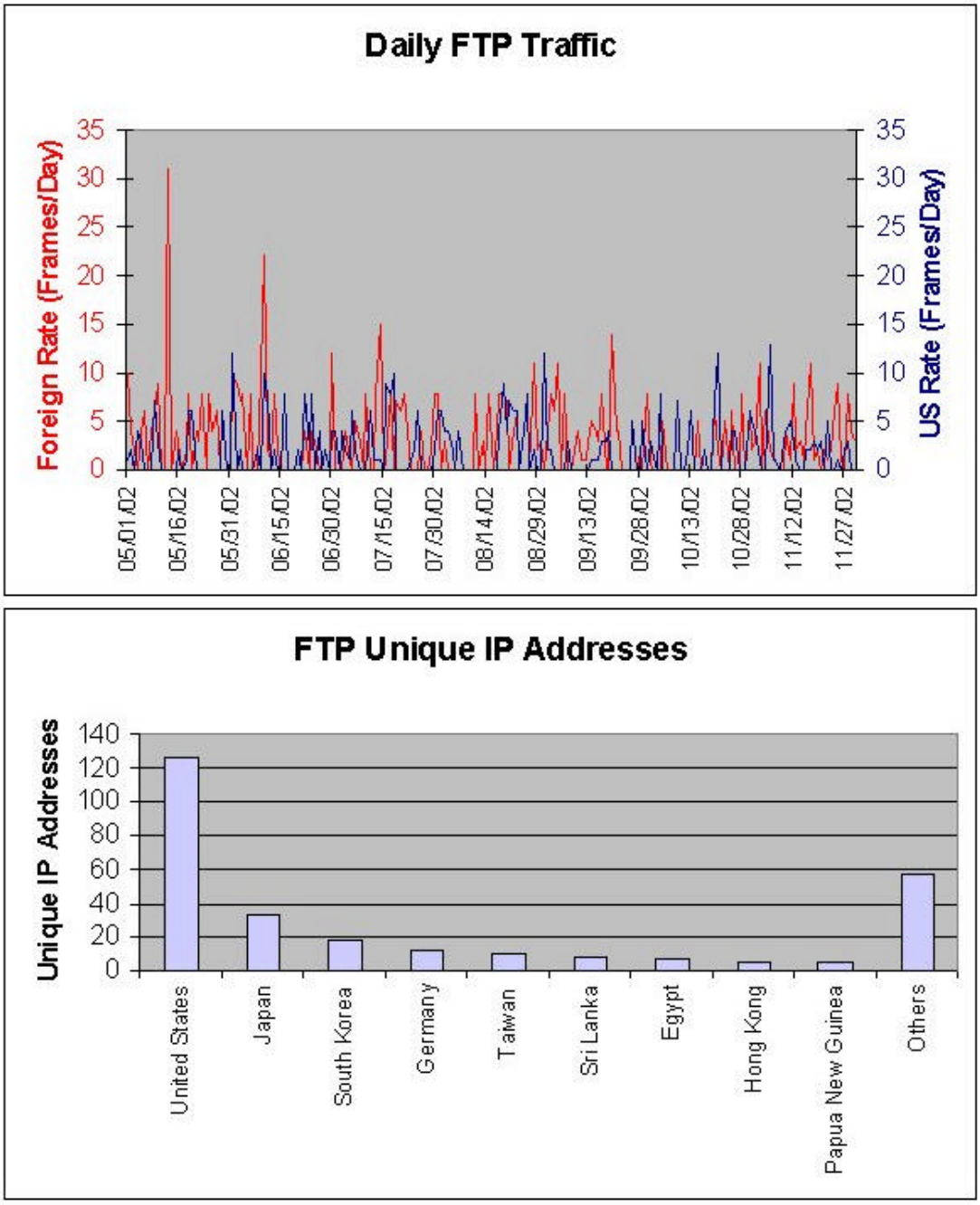


Figure 30 File Transfer Protocol Probes

External hosts are not allowed access to File Transfer Protocol (FTP) services on this internal network of the financial institution. Attackers are looking to exploit the service for

privilege escalation or file storage capability. On the internal network, FTP services are limited to a few network attached printers for firmware updates. However, as is indicated in Figure 30, frequent probes are made to determine if this service is available to external systems.

File Transfer Protocol	Foreign	US
Average	4.24	3.38
Median	4	3
Mode	4	2
Maximum	26	12
Minimum	1	1
Unique IP Addresses	155	126

Table 14 File Transfer Protocol Traffic by Unique IP Address

Table 14 shows the traffic generated by unique IP addresses on a session basis. The average frame count for both US and foreign originating traffic is skewed by a small number of hosts attempting more than one entry. Foreign-based IP addresses represent 55.2% of the total detected unique addresses while they account for 60.7% of the total FTP traffic. The US-based IP addresses represent 44.8% of the unique addresses and 39.3% of the traffic.

	Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
Foreign Average	4.3	4.7	2.5	2.7	2.4	2.5	2.5
Foreign Median	4.0	2.5	1.0	0.0	1.0	1.0	0.0
Foreign Maximum	15	31	9	11	8	14	11
Foreign Minimum	0	0	0	0	0	0	0
US Average	**2.1**	**2.4**	**1.7**	**2.1**	**2.3**	**1.2**	**2.1**
US Median	**1.5**	**0.0**	**0.0**	**1.0**	**2.0**	**0.0**	**1.0**
US Maximum	**8**	**12**	**13**	**8**	**10**	**8**	**12**
US Minimum	**0**	**0**	**0**	**0**	**0**	**0**	**0**
Total Average	6.4	7.1	4.2	4.8	4.7	3.7	4.6
Total Median	6.0	6.0	3.5	3.0	5.0	2.0	4.0
Total Maximum	16	32	15	16	13	14	22
Total Minimum	0	0	0	0	0	0	0

Table 15 File Transfer Protocol Traffic Day of Week

Day of week analysis for FTP intrusion attempts is shown in Table 15. The maximum rate for foreign traffic is on Sunday and Monday. However, US originating traffic appears to be spread more evenly throughout the week. Review of the daily frequency histograms for FTP shows a marked trend toward no attack versus attack (refer to Appendix 3).

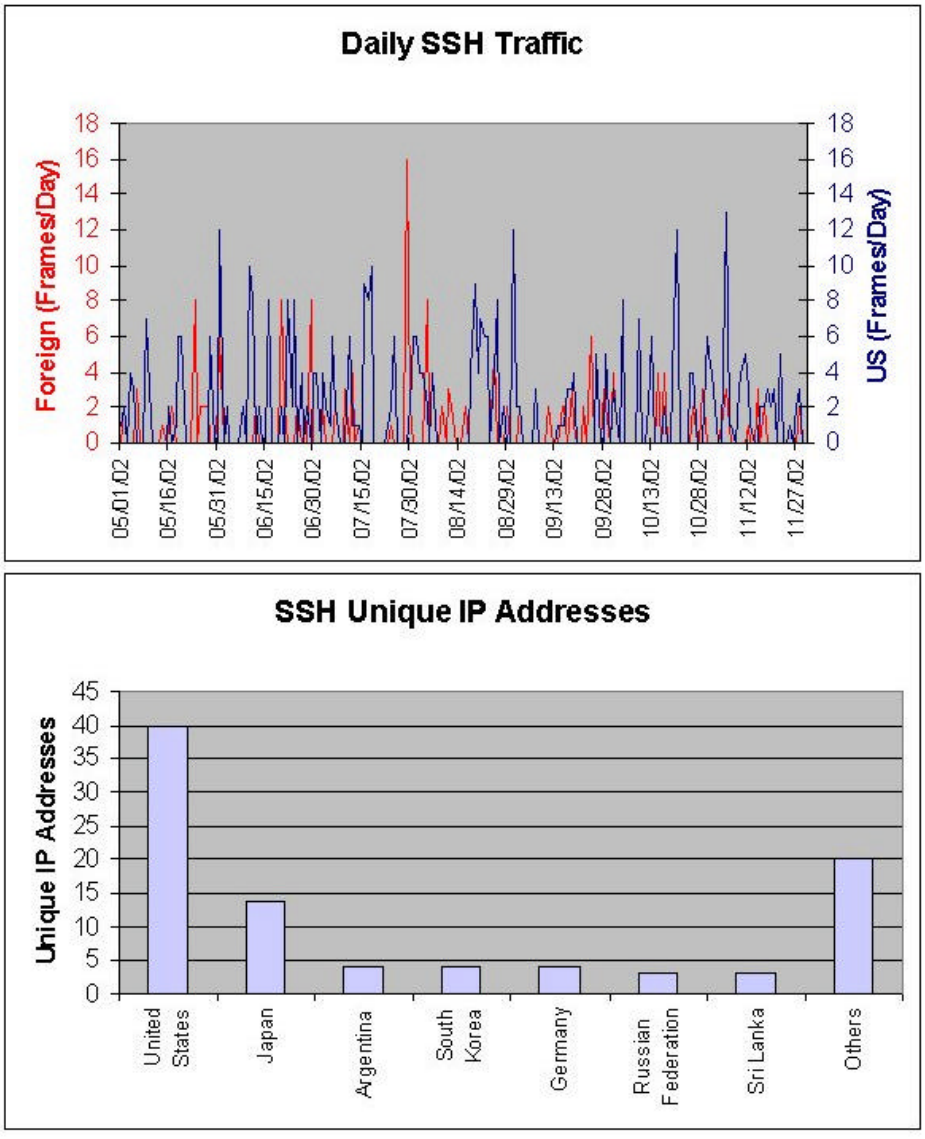


Figure 31 Secure Shell Probes

Secure Shell (SSH) was developed to provide a secure communications channel between two hosts. This service is typically deployed within UNIX environments and certain manufacturers of routers, switches and firewalls. By definition, SSH communications are trusted in the environments where deployed. This makes the penetration of a SSH service particularly attractive. There are a number of attacks that enable a penetration of the secure communications channel.

Figure 31 shows the random nature of the probing for a SSH host. The financial institution's firewall and edge router support this capability, but SSH is not enabled for external communications. As with the FTP traffic assessment, more foreign IP addresses probed for SSH than IP addresses originating in the United States. This is not consistent with the allocated IP addresses identified in Table 8. Foreign IP addresses account for approximately 56.5% of all attacking nodes and 60.2% of the hostile SSH traffic.

Secure Shell	Foreign	US
Average	3.17	2.73
Median	2	2
Mode	2	2
Maximum	16	9
Minimum	1	1
Unique IP Addresses	52	40

Table 16 Secure Shell Traffic by Unique IP Address

Table 16 shows the analysis of unique IP address probes. There is a high probability that all the SSH traffic was probe only and no active attempts where made to gain access.

	Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
Foreign Average	1.0	0.9	0.9	0.5	0.6	0.8	0.6
Foreign Median	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Foreign Maximum	8	16	6	3	8	8	8
Foreign Minimum	0	0	0	0	0	0	0
US Average	**2.1**	**2.4**	**1.7**	**2.1**	**2.3**	**1.2**	**2.1**
US Median	**1.5**	**0.0**	**0.0**	**1.0**	**2.0**	**0.0**	**1.0**
US Maximum	**8**	**12**	**13**	**8**	**10**	**8**	**12**
US Minimum	**0**	**0**	**0**	**0**	**0**	**0**	**0**
Total Average	3.1	3.3	2.7	2.6	2.9	2.0	2.7
Total Median	2.5	2.0	1.5	2.0	2.0	2.0	1.0
Total Maximum	10	16	16	8	10	8	18
Total Minimum	0	0	0	0	0	0	0

Table 17 Secure Shell Traffic Day of Week

Day of week analysis shows a constant rate of probing with no preference for a specific day to probe. When evaluating the daily frequency histograms (Appendix 3) for the SSH traffic, the trend is toward no attempts on any given day.

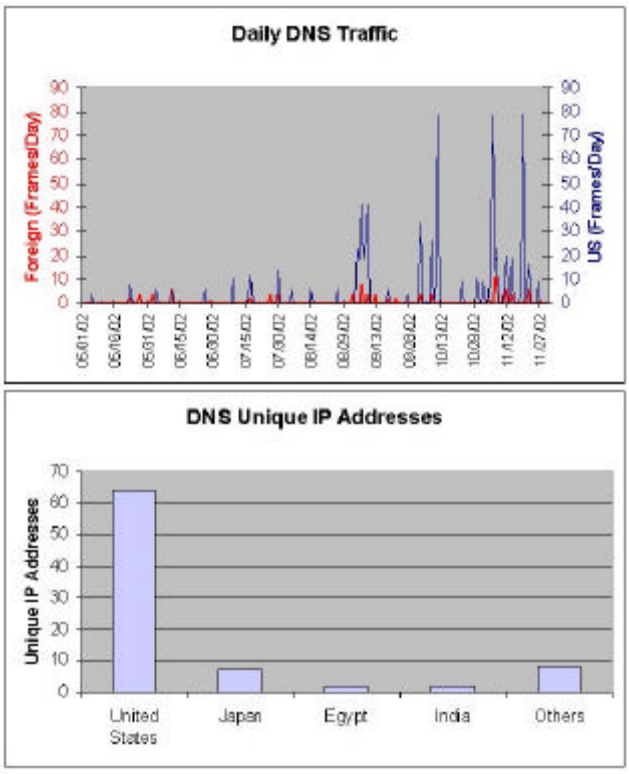


Figure 32 Domain Name Service Probes

Figure 32 shows the daily rate and sources of Domain Name Service probes. The principle reason for attacking an organization's DNS service is perform traffic redirection or denial of service. There are some exploits against some DNS daemons that will allow escalation of privilege, but these exploits are very old and mostly placed or replaced with daemons that are not susceptible.

The traffic originating from US IP addresses was substantially greater than the foreign-based traffic. The US-based attacks were twice the average duration, in terms of frames per attack per unique IP address (refer to Table 18). The unique IP address distribution is consistent with the allocated addresses in identified in Table 8. US-based IP addresses account for 77.1% of all unique IP addresses detected and 88.1% of all hostile DNS traffic.

Domain Name Service	Foreign	US
Average	5.21	11.44
Median	4	6.5
Mode	2	2
Maximum	18	45
Minimum	1	1
Unique IP Addresses	19	64

Table 18 Domain Name Service Traffic by Unique IP Address

	Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
Foreign Average	0.2	0.6	0.5	0.5	0.8	0.6	0.0
Foreign Median	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Foreign Maximum	4	6	6	10	11	8	0
Foreign Minimum	0	0	0	0	0	0	0
US Average	**1.1**	**3.0**	**8.5**	**2.2**	**3.8**	**4.8**	**0.6**
US Median	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**
US Maximum	**27**	**41**	**79**	**23**	**33**	**78**	**18**
US Minimum	**0**	**0**	**0**	**0**	**0**	**0**	**0**
Total Average	1.3	3.7	9.0	2.6	4.6	5.4	0.6
Total Median	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Total Maximum	27	45	80	24	37	78	18
Total Minimum	0	0	0	0	0	0	0

Table 19 Domain Name Service Traffic Day of Week

Analysis by day of week shows that the majority of DNS attacks and probes occurred during the business week. Rates are consistent with the rates shown by unique IP address. Again, the DNS daily frequency histograms (Appendix 3) show the tendency toward no DNS probes or attacks for any given day.

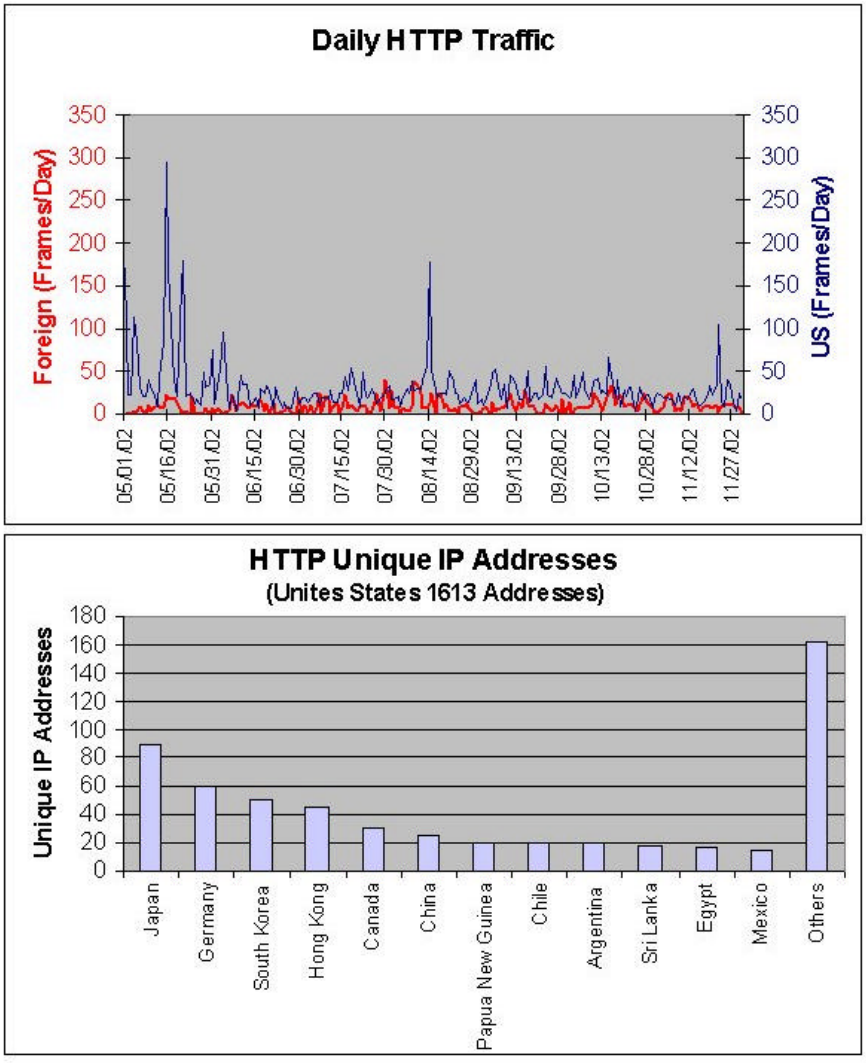


Figure 33 Hypertext Transport Protocol Probes

Hyper Text Transport Protocol (HTTP) is not running on the financial institution's internal network. The mail server does not have an enabled web interface. The financial institution's web server is located at a web hosting service in another state.

HTTP is the entry point for many potential exploits designed to create a denial-of-service, escalate privilege, deface the web site, gain confidential information (i.e. credit card numbers, etc.), or change the operation of web-based applications. Figure 33 shows the daily rate of probes/attempted attacks over the course of the study. The origin of the probes and attacks is primary from US-based IP addresses (73.9% of all unique IP addresses probing/attacking HTTP). This is consistent with allocated IP addresses identified in Table 8. US-based IP addresses accounted for 77.3% of all hostile HTTP traffic.

Hyper Text Transport Protocol	Foreign	US
Average	3.46	4.18
Median	3	2
Mode	3	2
Maximum	25	324
Minimum	1	1
Unique IP Addresses	571	1613

Table 20 HyperText Transport Protocol Traffic by Unique IP Address

The analysis of traffic generated by hostile hosts show that the average foreign host sends one more frame to probe for a web server than the average US-based host. However, in one case which skews the US average, an attacker attempted to gain access to any web server. This is indicative of a scripted attack trying a number of potential exploits. The HTTP service is more consistently probed/attacked than all other IP services except the NetBIOS Name Service. Review of the daily frequency histograms (Appendix 3) for HTTP shows that both foreign and US-based IP addresses tend toward attack versus no attack.

	Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
Foreign Average	9.9	9.6	11.7	8.9	8.2	8.7	8.0
Foreign Median	8.0	8.0	11.0	7.0	6.0	6.0	6.0
Foreign Maximum	26	27	40	34	28	37	34
Foreign Minimum	0	0	0	0	0	0	0
US Average	**21.6**	**31.6**	**37.2**	**43.5**	**31.6**	**31.4**	**23.5**
US Median	**18.0**	**25.0**	**25.0**	**26.0**	**27.0**	**25.0**	**20.0**
US Maximum	**84**	**151**	**180**	**294**	**169**	**105**	**112**
US Minimum	**7**	**6**	**7**	**6**	**4**	**6**	**5**
Total Average	31.5	41.2	48.9	52.4	39.7	40.1	31.5
Total Median	27.0	38.0	40.5	33.0	31.0	31.0	29.0
Total Maximum	86	153	182	316	185	107	114
Total Minimum	10	10	19	13	9	16	10

Table 21 HyperText Transport Protocol Traffic Day of Week

The day-of-week analysis for HTTP traffic shows a nearly uniform pattern. US-based hosts represent between 69% and 83% of all traffic on any given day for HTTP.

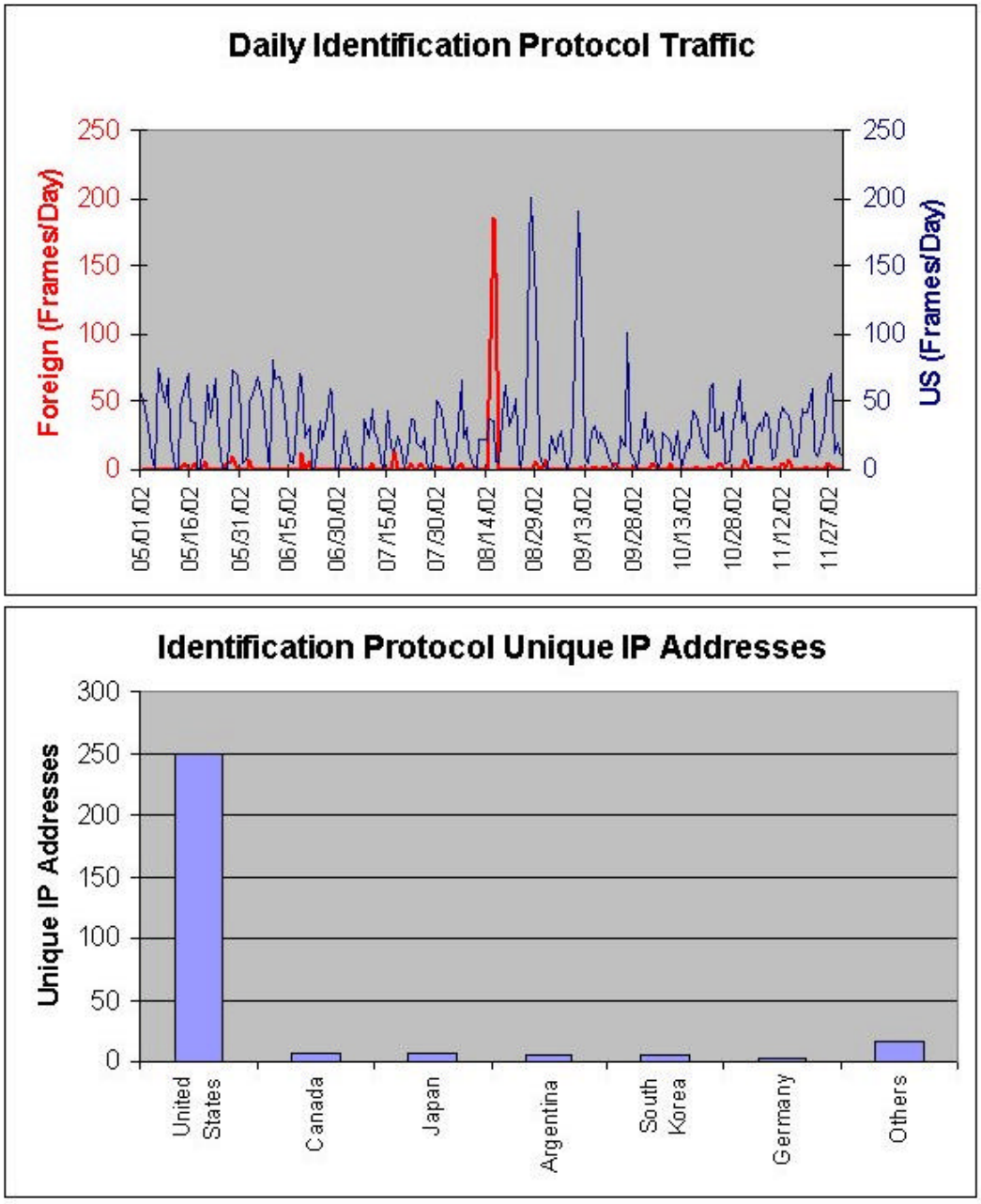


Figure 34 Identification Protocol Probes

Identification Protocol (IETF RFC1413) was originally known as the authentication protocol. It was renamed since it does not provide a means by which to prove a user's

identity. The primary purpose in exploiting this protocol is to crash the identd service performing a denial-of-service on an Internet Chat Relay server.

The financial institution does not use the Identification Protocol for any network service internally or externally. All traffic to this port is considered hostile. The majority of unique IP addresses probing the Identification Protocol port is US-based (85%) and does not correlate with the distribution of assigned IP addresses shown in Table 8. US-based IP addresses were responsible for 91.5% of all hostile Identification traffic.

Identification Protocol	Foreign	US
Average	13.82	26.26
Median	4	4
Mode	2	2
Maximum	378	1363
Minimum	1	1
Unique IP Addresses	43	250

Table 22 Identification Protocol Traffic by Unique IP Address

Reviewing the hostile traffic profile by unique IP address in Table 22 for the Identification Protocol, there is marked difference in the median and average. The key reason for the skewing of the average frames per IP address is the result of several foreign and US-based scripted attacks from six hosts.

	Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
Foreign Average	0.8	1.2	1.0	1.9	2.7	7.1	5.0
Foreign Median	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Foreign Maximum	8	7	4	14	51	186	146
Foreign Minimum	0	0	0	0	0	0	0
US Average	**5.3**	**33.0**	**48.2**	**49.8**	**44.6**	**28.6**	**5.2**
US Median	**2.5**	**33.0**	**44.0**	**41.0**	**37.0**	**28.0**	**4.0**
US Maximum	**28**	**80**	**164**	**201**	**126**	**57**	**16**
US Minimum	**0**	**1**	**16**	**12**	**0**	**4**	**0**
Total Average	6.1	34.2	49.2	51.7	47.3	35.6	10.2
Total Median	4.0	34.5	46.0	43.0	40.0	28.0	4.0
Total Maximum	30	80	164	201	128	222	152
Total Minimum	0	2	16	12	0	4	0

Table 23 Identification Protocol Traffic Day of Week

Day-of-week analysis indicates that there is a preference for probing during the business week. While foreign-based hosts seem to prefer Friday and Saturday probes, the comparatively overwhelming Identification Protocol traffic during the business week moves the window for attacks to the Monday through Friday period.

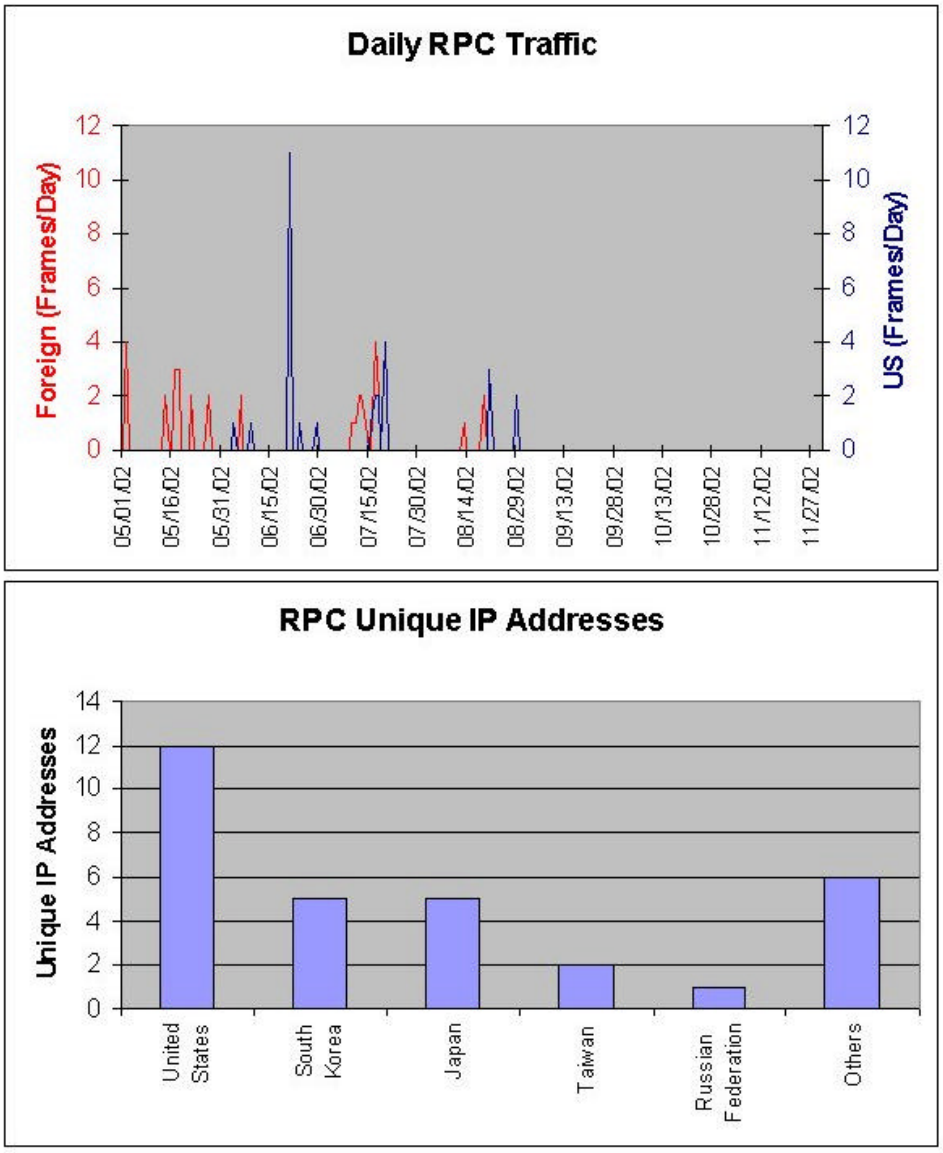


Figure 35 Remote Procedure Call Probes

Remote Procedure Call (RPC) was proposed for the TCP/IP protocol stack by Sun Microsystems in RFC 1050. RPC has many exploits and forms the basis for many client/server systems. Loss of data, corruption of data, denial-of-service, escalation of privilege, and application-specific attacks are just a few of the potential ways to exploit RPC.

The RPC traffic was very sporadic and infrequent. Further, the RPC traffic was included in the access control lists that implemented the packet filter layer at the edge router.

Remote Procedure Call	Foreign	US
Average	2.05	2.42
Median	2	1
Mode	2	1
Maximum	4	11
Minimum	1	1
Unique IP Addresses	19	12

Table 24 Remote Procedure Call Traffic by Unique IP Address

The average traffic originating from unique IP addresses shows probing and not attack characteristics. With a total of 68 frames prior to the implementation of the edge router access control lists and no traffic after, RPC probes did not pose a significant threat to the financial institution.

Review of the daily frequency histograms for the RPC traffic (Appendix 3) shows the same outcome as the rate graph in Figure 35, the tendency is toward no attacks based on RPC exploits for any given day. The traffic level was so low that day-of-week analysis was meaningless.

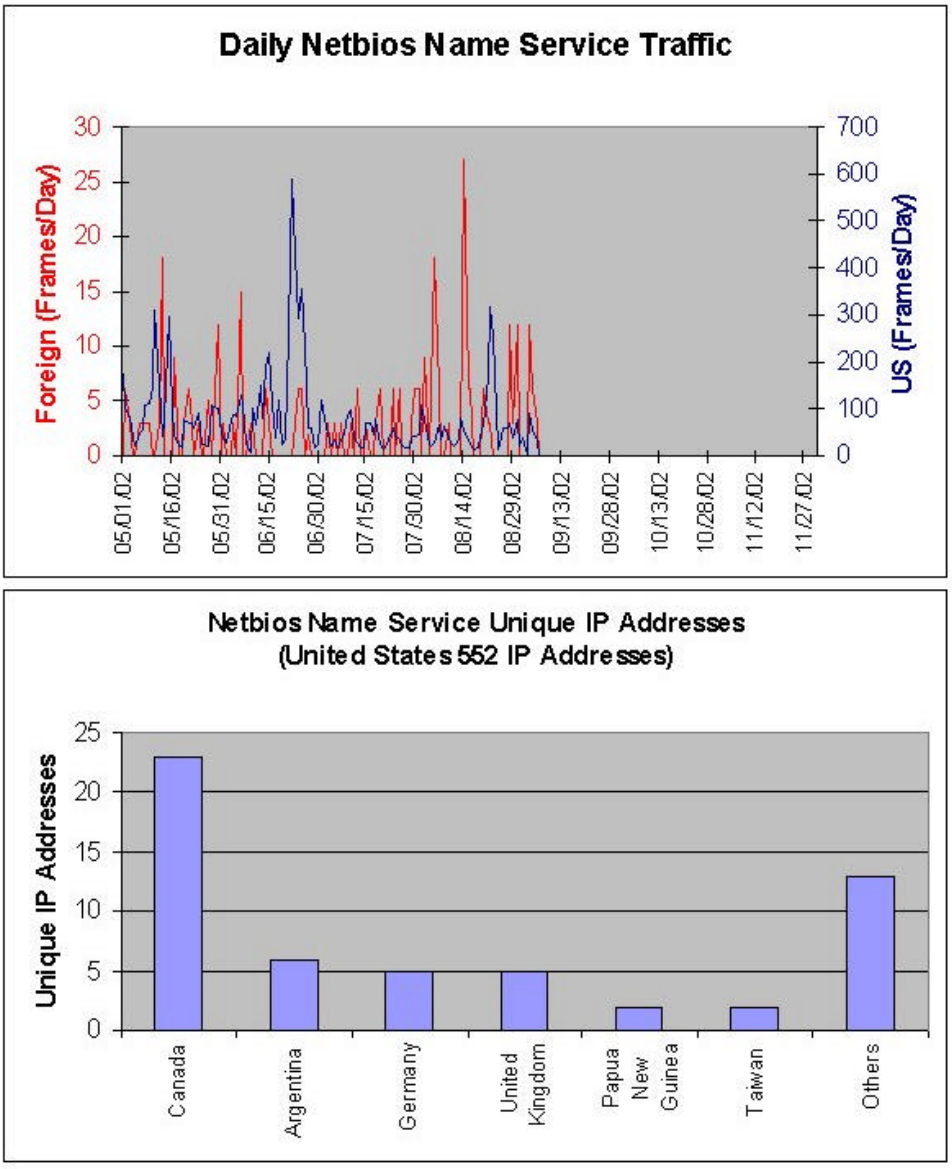


Figure 36 NetBIOS Name Service Probes

NetBIOS services are running on the internal network of the financial institution. All TCP and UDP ports associated with NetBIOS were dropped at the edge of the network commencing on September 5, 2002 with the implementation of the access control lists.

NetBIOS Name Service is also known as Windows Internet Name Services or WINS. This service was developed by Microsoft to map Windows computer names to IP addresses on Windows-based networks. Attackers attempt to gain access to WINS to rapidly enumerate an internal network.

Figure 36 shows the daily frame rates for NetBIOS Name Service (WINS) from foreign and US-based IP addresses for the period of this study. While US-based IP addresses (90.8%) where the overwhelming source of traffic (96.8%) destined for TCP port 137, foreign addresses (9.2%) accounted for approximately 3.2% of the total inbound traffic.

NetBIOS Name Service	Foreign	US
Average	6.02	18.70
Median	3	3
Mode	3	3
Maximum	27	2880
Minimum	2	2
Unique IP Addresses	56	552

Table 25 NetBIOS Name Service Traffic by Unique IP Address

Table 25 shows the analysis of the aggregate average traffic originating from unique IP addresses. The average shows some skewing away from the median due to several IP addresses sending substantially high traffic volumes. However, the median is fairly representative of the attempt to complete the TCP connection to WINS on the target. The distribution of unique IP addresses between foreign and US-based ranges is inconsistent with distribution of all IP addresses as shown in Table 8.

	Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
Foreign Average	0.6	2.1	1.8	2.2	2.0	2.1	0.2
Foreign Median	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Foreign Maximum	6	18	12	27	15	12	3
Foreign Minimum	0	0	0	0	0	0	0
US Average	**34.2**	**39.3**	**54.4**	**61.3**	**49.0**	**52.1**	**46.9**
US Median	**17.0**	**31.5**	**58.5**	**45.0**	**33.0**	**27.0**	**12.0**
US Maximum	**429**	**293**	**354**	**294**	**315**	**263**	**586**
US Minimum	**0**	**0**	**0**	**0**	**0**	**0**	**0**
Total Average	34.8	41.4	56.2	63.5	51.0	54.2	47.1
Total Median	17.0	36.0	61.5	45.0	36.0	33.0	12.0
Total Maximum	432	299	360	294	318	263	586
Total Minimum	0	0	0	0	0	0	0

Table 26 NetBIOS Name Service Traffic Day of Week

Day-of-week analysis of averages for foreign and US indicates that there is no particular preference for probing of WINS. However, the median shows a preference for the work week. Review of the daily frequency histograms (Appendix C) indicates that foreign-based IP addresses are less likely to launch a probe or attack than a US-based IP address.

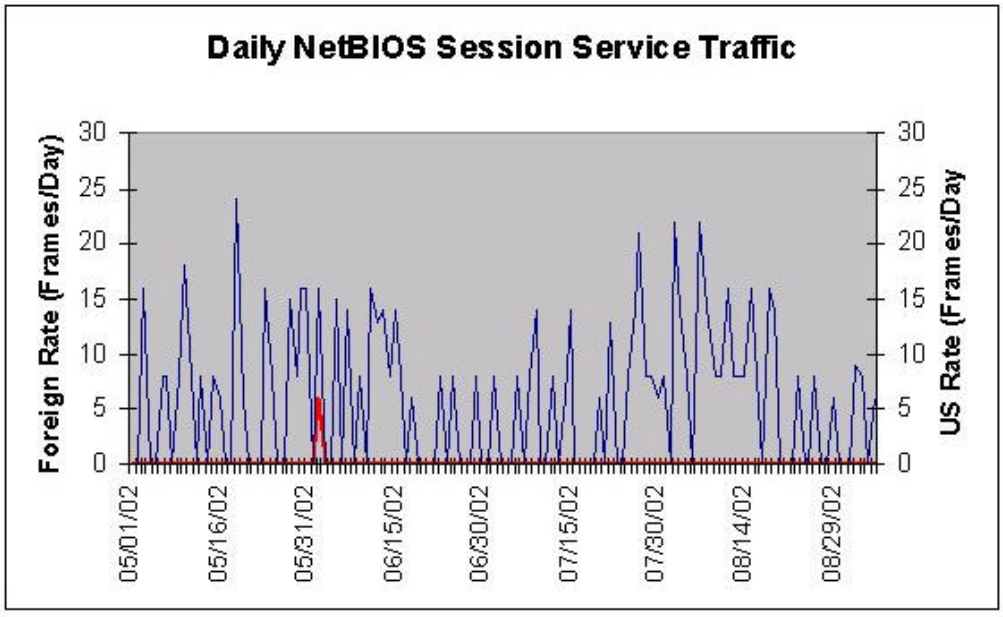


Figure 37 NetBIOS Session Service Probes

NetBIOS Session Service handles file transfers between computers. This service typically requires NetBIOS Name Service (WINS) to resolve the IP address of the system being attached to for file transfer operations. However, if the attacker or any legitimate user places the NetBIOS computer name with its IP address, WINS is not required. Figure 37 shows the daily frame rate of hostile traffic directed against TCP port 139 for the Internet. There is no country graph because only two origin countries were detected during the course of this study – the United States and Japan.

NetBIOS Session Service	Foreign	US
Average	N/A	3.38
Median	N/A	3
Mode	N/A	2
Maximum	6	12
Minimum	6	1
Unique IP Addresses	1	12

Table 27 NetBIOS Session Service Traffic by Unique IP Address

Table 27 shows that the average probe/attack rate per IP address is consistent. This three frames per unique IP address tends to indicate the attempt to force a NetBIOS Session Service connection. The US-based IP addresses accounted for 99.2% of all traffic directed against this TCP port and 92.3% of the unique IP addresses probing the financial institution.

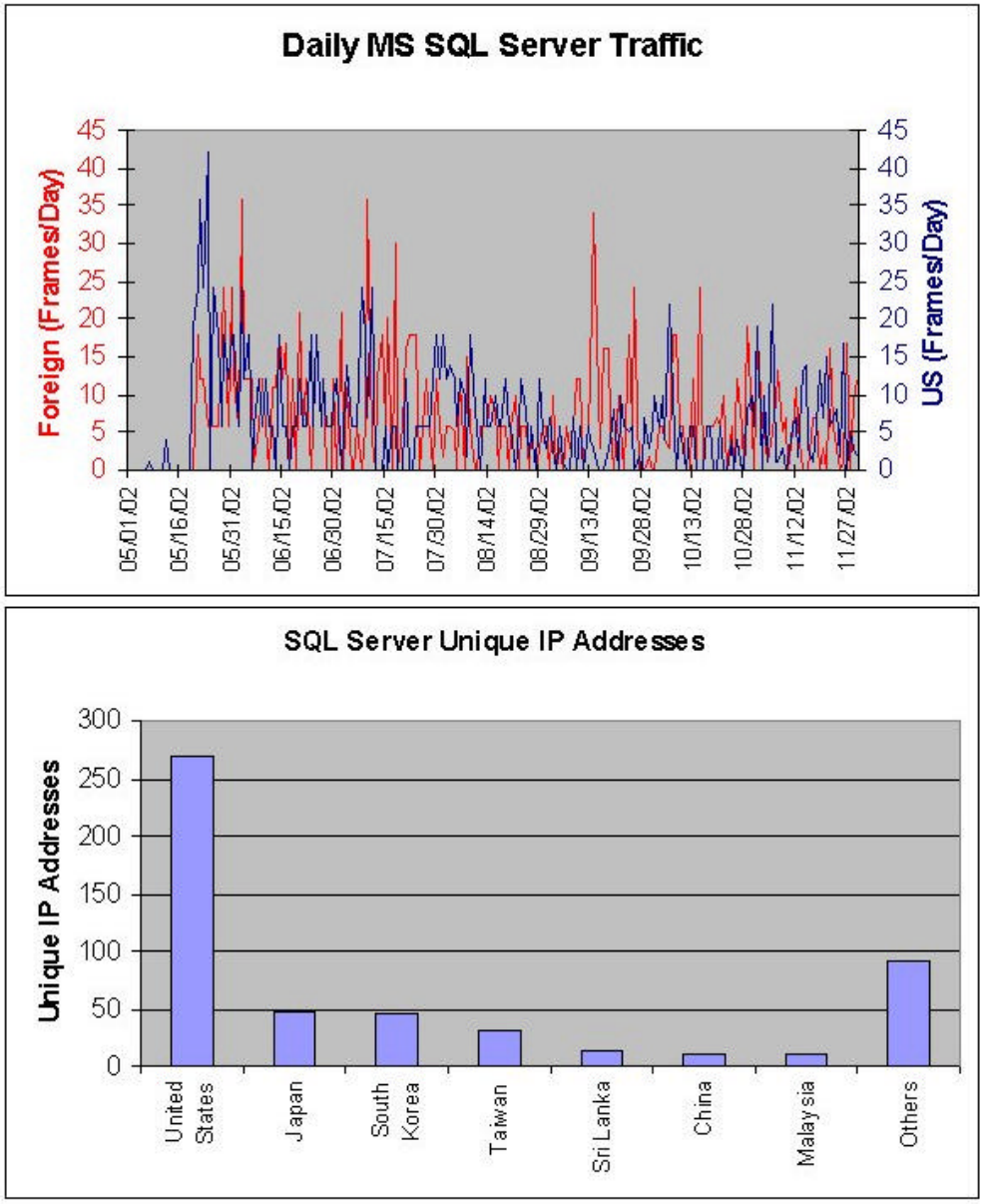


Figure 38 Microsoft SQL Server Probes

Client applications can connect to a Microsoft SQL Server via TCP port 1433. This service is designed to manage the connection and move data between the client application and the SQL server. As a result, this is a highly vulnerable service port if not properly secured. The financial institution is not running this service internally and

therefore all traffic directed to this port is considered hostile. Figure 38 shows the daily probe rates originating from US and foreign-based IP addresses. The traffic directed against TCP port 1433 is random. Of the IP addresses probing this port, 51.7% are US addresses account for 49.4% of the traffic.

Microsoft SQL Server	Foreign	US
Average	5.78	5.27
Median	6	6
Mode	6	6
Maximum	18	12
Minimum	1	1
Unique IP Addresses	251	269

Table 28 Microsoft SQL Server Traffic by Unique IP Address

The traffic coming from unique IP addresses is nearly uniform in terms of the number of frames per IP address. There is little variation whether the IP addresses are foreign or US-based. While US-based addresses account for 51.7% of all unique IP addresses probing for Microsoft SQL Server, they only account for 49.4% of all Microsoft SQL Server inbound traffic. The daily frequency histograms in Appendix C for Microsoft SQL Server traffic and Figure 38 agree that the trend is toward daily probing on TCP port 1433.

	Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
Foreign Average	6.0	5.1	10.4	6.7	7.5	5.3	6.3
Foreign Median	6.0	2.5	12.0	6.0	6.0	6.0	6.0
Foreign Maximum	18	36	24	36	30	24	34
Foreign Minimum	0	0	0	0	0	0	0
US Average	**7.0**	**6.5**	**7.6**	**6.5**	**7.0**	**7.5**	**4.3**
US Median	**6.0**	**6.0**	**6.0**	**6.0**	**6.0**	**6.0**	**3.0**
US Maximum	**24**	**24**	**24**	**36**	**24**	**42**	**18**
US Minimum	**0**	**0**	**0**	**0**	**0**	**0**	**0**
Total Average	13.0	11.7	18.1	13.2	14.5	12.9	10.6
Total Median	12.0	12.0	18.0	10.0	12.0	11.0	8.0
Total Maximum	30	60	42	48	36	48	37
Total Minimum	0	0	0	0	0	0	0

Table 29 Microsoft SQL Server Traffic Day of Week

Table 29 shows the day-of-week analysis for the Microsoft SQL Server traffic over the period of this study. There does not appear to be any preference for a particular day whether the hostile host is foreign or US-based.

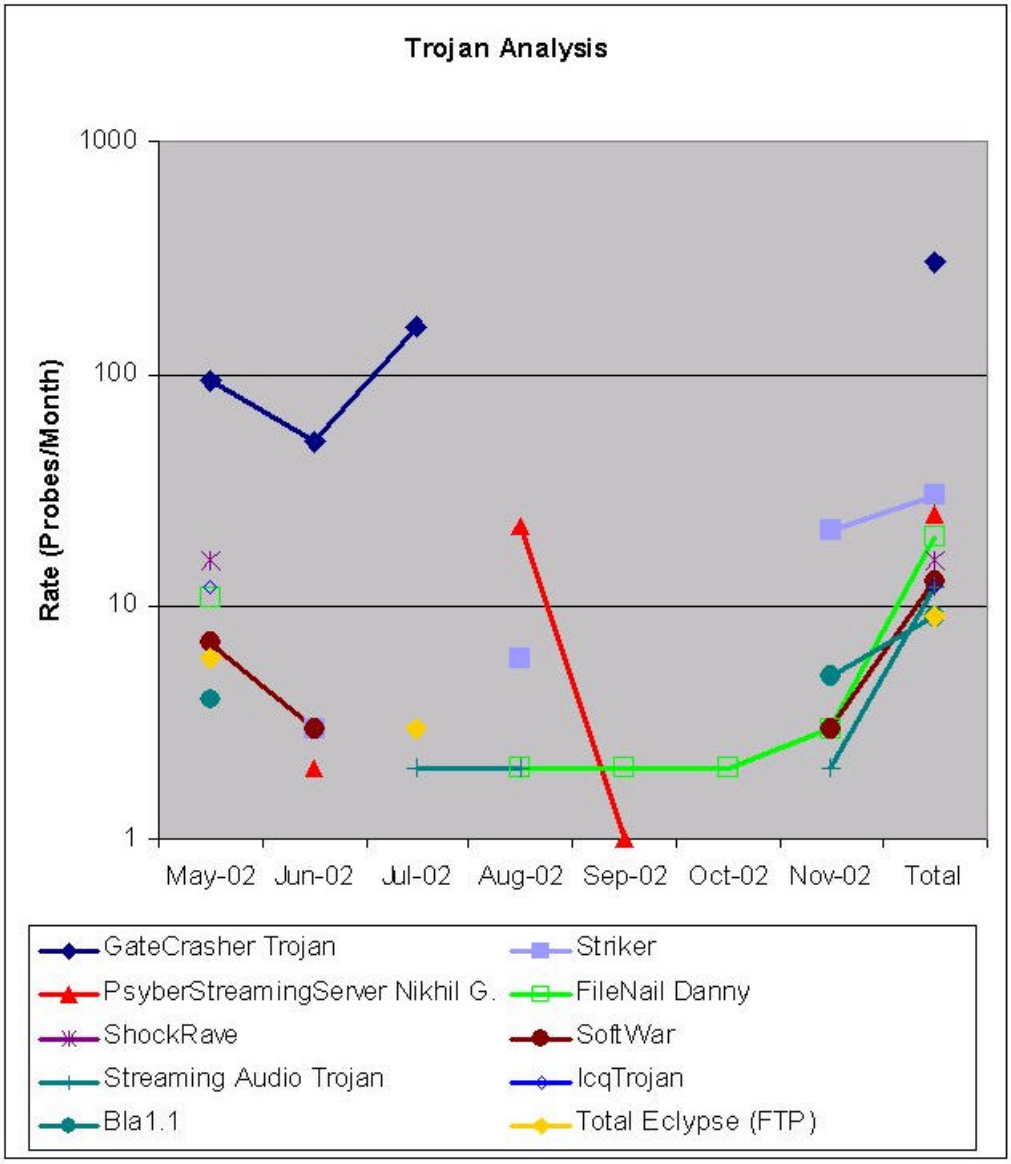


Figure 39 Top Ten Trojan Horse Probes

Trojan horse programs are a means by which attackers seek to gain access to the internal information technology resources of an organization. In the course of this study, a

number of probes where directed against the financial institution to determine if there were Trojan horse applications running on the internal systems. Because the firewall is setup to block all inbound traffic other the TCP port 25 (SMTP), these probes were blocked and logged. Two of the currently most popular Trojan horse programs on the Internet are SubSeven and GateCrasher. Each of these will be reviewed individually. Figure 39 shows the top ten Trojan horse probes experienced by the financial institution over the course of the study.

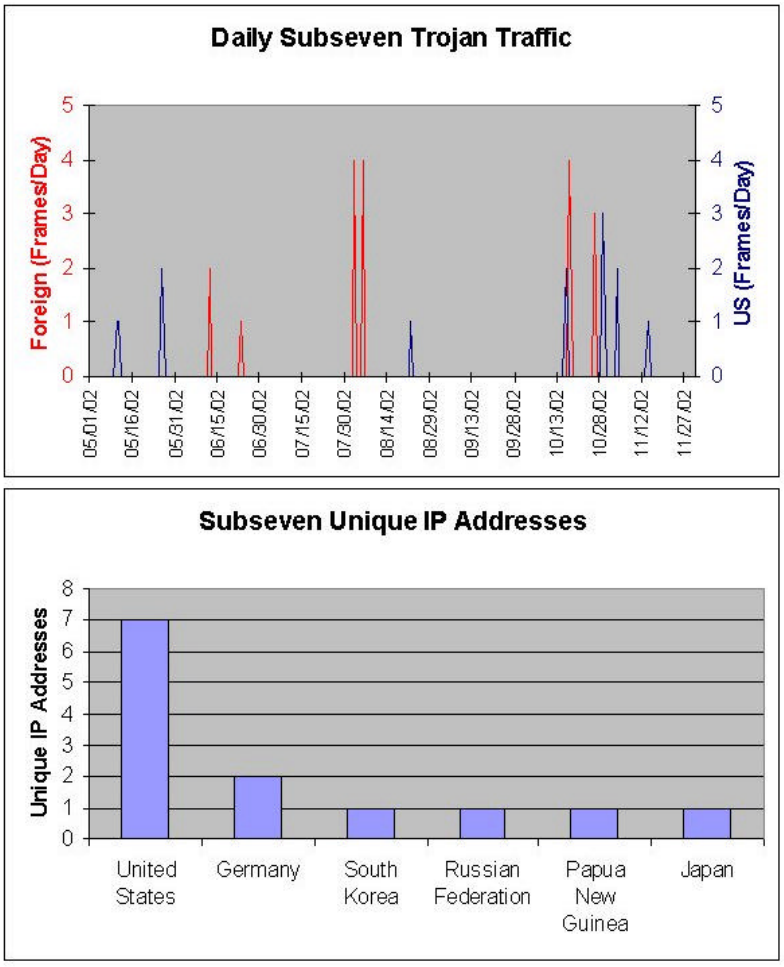


Figure 40 SubSeven Trojan Probes

SubSeven is designed to be a remote control and administration tool. The normal vector for attack is in Email messages as an attachment or via Internet Relay. This Trojan has the capability to capture the user's keystrokes, perform screen captures of the affected host, route the output of a computer's microphone to the attacker, read and write files, and perform limited packet sniffing on the network were the victim host is located. The other key capability of SubSeven is its ability to launch and participate in distributed denial-of-service attacks on systems that not infected with this malicious code.

.SubSeven Trojan	Foreign	US
Average	3.00	1.86
Median	3.5	2
Mode	4	1
Maximum	4	3
Minimum	1	1
Unique IP Addresses	6	7

Table 30 SubSeven Trojan Traffic by Unique IP Address

The financial institution experienced very limited probing of SubSeven's primary ports. This information is shown in Figure 40. The distribution between foreign and US-based hosts is not consistent with the distribution of IP addresses shown in Table 8 and Table 30. Foreign-based hosts probing for SubSeven appear to be sending more frames on the specific ports, but only marginally.

Given the relatively low number of frames the were used to probe for SubSeven, a day-of-week analysis reveals little relevant information. The daily frequency histograms for SubSeven (Appendix 3) confirm that are few days when probing occurs.

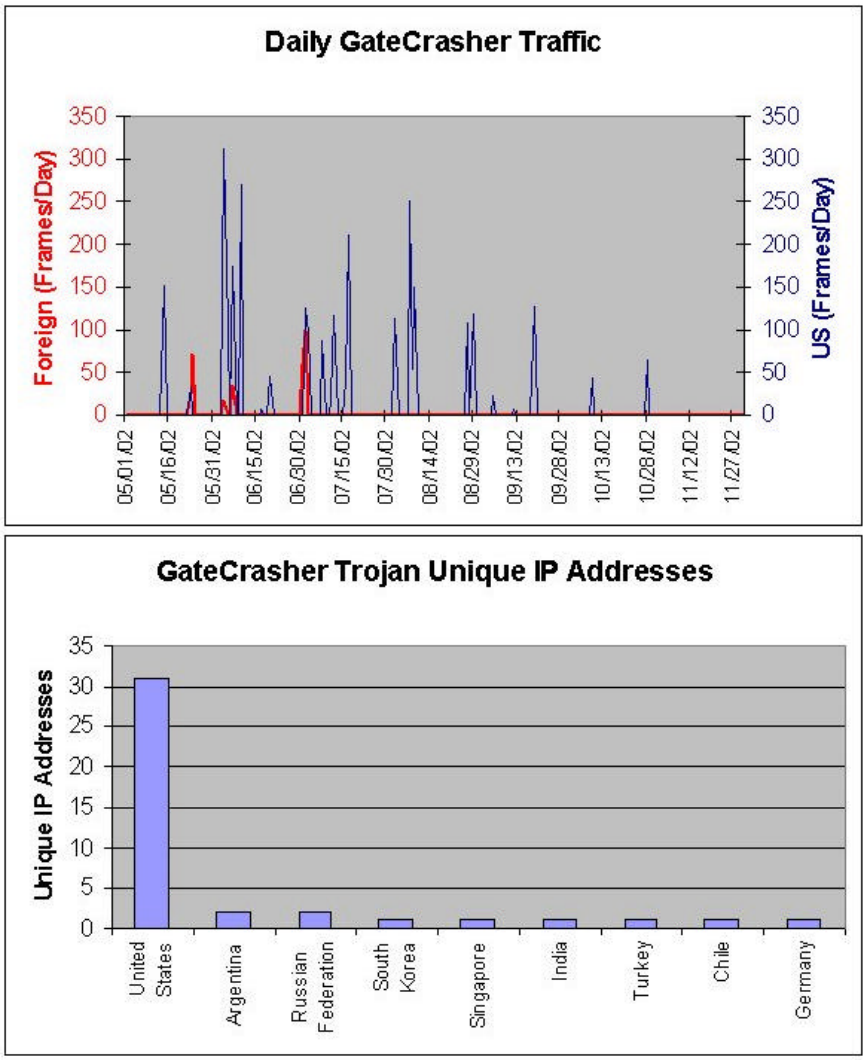


Figure 41 GateCrasher Trojan Probes

The Gatecrasher Trojan was one of the first Trojan horse applications to utilize a Microsoft Word document as the vector for attack. GateCrasher can also be spread by Internet Relay Chat (IRC). GateCrasher has a variety of capabilities aimed at controlling to victim host. These capabilities include file write and delete, window control, and send and receive files. Figure 41 shows the daily rate for probes of the GateCrasher Trojan port. The interval at which probes were launched against the financial institution is random.

GateCrasher Trojan	Foreign	US
Average	30.40	91.97
Median	30.5	44
Mode	N/A	20
Maximum	55	797
Minimum	13	1
Unique IP Addresses	10	31

Table 31 GateCrasher Trojan Traffic by Unique IP Address

The GateCrasher probes are not consistent with the other protocols that were probed or attacked during this study. The average and median traffic (Table 31) by unique IP address shows a large increase in the number of frames sent to probe the GateCrasher default TCP port. The distribution between US and foreign-based of unique IP addresses is consistent with the findings shown in Table 8. However, the US-based IP addresses accounted for 90.3% of the traffic probing for the GateCrasher TCP default port.

	Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
Foreign Average	0.0	2.0	3.9	0.0	0.8	3.4	0.0
Foreign Median	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Foreign Maximum	0	59	100	0	24	70	0
Foreign Minimum	0	0	0	0	0	0	0
US Average	**0.0**	**14.3**	**24.6**	**22.7**	**13.8**	**17.8**	**0.0**
US Median	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**
US Maximum	**0**	**270**	**313**	**249**	**127**	**174**	**0**
US Minimum	**0**	**0**	**0**	**0**	**0**	**0**	**0**
Total Average	0.0	16.3	28.5	22.7	14.6	21.2	0.0
Total Median	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Total Maximum	0	270	329	249	127	209	0
Total Minimum	0	0	0	0	0	0	0

Table 32 GateCrasher Trojan Traffic Day of Week

GateCrasher day-of-week analysis shows no activity occurred on the weekends. The daily frequency histograms in Appendix C and Figure 41 bear out the finding that GateCrasher probing tends not to occur on any given day.

CHAPTER 5

DISCUSSION AND FUTURE DIRECTIONS

Discussion

The security architecture of the financial institution is a direct result of the implementation of the information systems security policies (Appendix A). The security policies conform to the proposed model put forth in Chapter 2 in the following ways:

1. Regulatory and Legal Environment – The financial institution is required to comply with a variety of federal and state banking laws and regulation. The principle compliance issue for the financial institution is the Graham-Leech-Bliley Act and the USA Patriot Act which are at odds with each other concerning individual customer privacy. These privacy and security regulations are specified in the Privacy Policy attached in Appendix A.

2. Organizational Environment – The Information Protection Policy (Appendix A) supports the organizational need to control the content and flow of information to external sources and organizations. The financial institution also establishes ownership of the information systems and the data contained within the systems for the purpose of regulatory compliance and limiting liabilities. To this end, the Information Protection Policy authorizes officers of the financial institution to monitor and review all data and activity on the network and connections to the network. Monitoring systems include

    a. the application, system, security logs of the network file servers,

    b. the firewall system logging inbound and outbound activity to an internal syslog server,

c. a layered anti-virus solution at the workstation, server, and email server levels,

d. and a web activity monitor that tracks Internet usage by all employees and systems.

3. Access Controls – The principle access controls are

a. the network user ID and password which clears access for file, print, email and general Internet access,

b. User IDs for specific application access are separate from the network user ID which include access to FedLine (the Federal Reserve System for domestic and international inter-bank funds transfers) and main bank data systems which are provided by two separate vendors which store primary customer account information in out-of-state systems,

c. the firewall and the edge router on the Internet connection which filter and log inbound and outbound Internet traffic,

d. and the Virtual Private Network connections which require encrypted links with a minimum of 168-bit Triple DES key and separate authentication.

4. Disaster Recovery and Business Continuity processes are mandated by policy and implemented with backup dial-up connections for key service providers and the Internet. Full data backups are performed each day and the tapes removed to a secure off-site location. All data backup is monitored and reported on a monthly basis.

5. Encryption – The primary use of encryption technologies is limited to the virtual private network (VPN) connection of the financial institution. Encrypted messaging and email is presently not implemented due to a lack of standardization of encryption standards.

6. Operational Security is mandated through the Information Protection Policy and the Intranet and Internet Policy, which require updates to virus definition files (automated on the servers and pushed to the workstations), user ID password construction and 30-day change (enforced by the applications and network operating systems), and reporting of suspicious events to management.

7. Physical security is implemented in combination with the financial institution's monitored alarm system. Further physical security measures include the password-enabled screen saver function after fifteen minutes of inactivity at the workstation and controlled access to the network servers, network infrastructure, and telephone key systems.

8. Application and system development is avoided by the use of service providers for the principle enterprise information systems and off-the-shelf software for other applications. No application development occurs in-house.

This study was designed to evaluate the effectiveness of applying defense-in-depth processes to a financial institution's information systems. Layered defenses are easily evaluated through the analysis of the log files of various servers and monitoring applications. There were six suppositions evaluated during the course of this study and each will be addressed individually.

A1. The nature and volume of the hostile traffic will be impossible to predict for any given point in time.

Review of the results in Chapter 4, "Overall Traffic" and "Complexity of Attack", as well as, the "Histograms of Total and Attack Traffic" (daily frequencies) and the "Traffic By Destination Port" table in Appendix C, lend support to the supposition. Attack and probing traffic was extremely variable for the financial institution of the course of this study.

The nature of hostile traffic was also extremely variable. There were variances in inbound traffic loads that traditional statistical modeling cannot characterize. The financial institution has only two services presented to the Internet – SMTP and VPN access. The VPN access was not attacked at all during the course of this study. SMTP was probed and attacked multiple times, but without success. The key attacks against SMTP appear to focus on gaining access to the email relay function. The email relay function is critical to spammers seeking to obfusticate the origin of spam email traffic.

The remaining services probed shows that hostile hosts preferred attempting to exploit HTTP and NetBIOS. The first, HTTP, is arguably the protocol of choice for most attackers. There are a substantial number of exploits affecting nearly every web server deployed on the Internet. The number of HTTP exploits is not the only issue. Most attackers, once they have gained access to an internal system, will redirect services to port 80 which is not filtered in most networks when going outbound. Filtering or dropping outbound HTTP frames would effectively shutdown the organization's ability to use external web servers. Application layer filtering is available to analyze the contents of frames at a protocol level, but many organizations feel that this is too costly.

The probing activity for NetBIOS service ports is expected since Microsoft enjoys market dominance in shipped operating systems. Microsoft effectively ported the NetBIOS network communications processes on to the TCP/IP protocol stack utilizing

TCP ports 135 through 139. The lack of security inherent in NetBIOS and the historical Microsoft position on collaborative computing makes these ports of particular interest. The NetBIOS Session Service, for example, depends on the NetBIOS Name Service to resolve NetBIOS names into IP addresses. However, when requesting a drive share from a Windows server simply replacing the target computer's NetBIOS name with its IP address will eliminate this lookup process. For example, if a computer had a NetBIOS name of ANYBANK_FS and its IP address was 192.168.1.1, then the share command path element for the hidden share of drive c: would look like \\192.168.1.1\C$ as opposed to \\ANYBANK_FS\192.168.1.1.

The evaluation of the rates of probing traffic demonstrates dynamical complexity as defined by Strogatz (2001). The incoming traffic rates, whether evaluated in total or by service port, was extremely non-linear. Standard statistical evaluation fails characterize the traffic experienced by the financial institution. Limited characterization was possible when evaluating the traffic generated by individual hosts to determine the number of frames sent by a hostile host during probing operations. The day-of-week analysis was designed to evaluate average traffic loads for individual services, but this traffic is also non-linear.

A2. Filtering network traffic will reduce the total number of potential exploits and attacks against a target network.

In the fifth month (Spetember 2002) of the study, access control lists were applied to the edge router of the financial institution (Refer to Appendix B for changes to the router configurations). The purpose of the access control lists was to drop traffic the met specific criteria before the traffic reached the firewall effectively creating a second "firewall" outside the primary firewall. The criteria selected were:

1. No inbound IP traffic would be redirected to a specific router (no ip redirects),

2. No response to inbound ICMP traffic (ping, traceroute, etc.),

3. Disallow any inbound route-specific traffic,

4. Drop all inbound traffic with a private IP address (RFC 1918) as the source IP address,

5. Drop all inbound traffic with a multicast IP address as the source IP address,

6. Drop all inbound TCP and UDP traffic with destination ports 135 through 139 (NetBIOS Service ports),

7. Drop all inbound UDP traffic with a destination port of 161 (Simple Network Management Protocol),

8. Drop all inbound TCP and UDP traffic with a destination port of 111 (Remote Procedure Call),

9. Drop all inbound TCP and UDP traffic with a destination port of 445 (SMB block transmission for Microsoft Windows 2000 and Microsoft Directory Service),

10. And drop all inbound TCP traffic with a destination port of 23 (Telnet). The Telnet block was in place for the entire duration of the study.

While it can be argued that access control lists are security by fiat, the usefulness for the financial institution was immediately apparent in the firewall logs (Chapter4: Network Access Control Layers). Within 30 seconds of implementation of the access control lists at the edge router, traffic destined for TCP port 137 (NetBIOS Name Service) ceased. TCP port 137 was the most probed service in study until implementation of the access control lists. This event alone justified the implementation of the edge router access

control list by improving the performance of the financial institution's firewall by reducing the level of incoming traffic it had to evaluate.

Prior to the implementation of the access control lists on the edge router, the financial institution experienced some inbound traffic that had source IP addresses in the private IP address ranges as defined by RFC 1918. These attacks were most certainly directed broadcasts since all core Internet routers are configured to drop RFC 1918 addressed traffic. Dropping directed broadcast frames in combination with dropping all private IP addresses (RFC 1918) effectively eliminated this method to gain access to the financial institution's internal network.

The layering of access control with firewalls and routers increases the difficulty of penetration to the internal network of the financial institution. If the attacker is able to gain access to the internal network by other means (i.e. malicious code via email attachment) and redirect a filtered port to an open port, then the attacker can get around the filters and the firewall.

A3. Filtering network traffic will not completely mitigate application and service attacks based on allowed network traffic.

As noted on the prior page, there are ways to defeat filtering and stateful inspection of inbound traffic. However, the most common way into a network, like the financial institution in this study, is to exploit the open or unfiltered services. In the case of the financial institution used for this study, the only open or acceptable inbound traffic is limited to email and VPN access.

No attacks were detected against the VPN services of the financial institution during the course of this study. This does not imply that there are no ways to exploit the VPN service ports or execute a denial-of-service attack against these ports.

The primary inbound service for the financial institution is SMTP. This service is vulnerable to a number of different exploits and attacks. The financial institution experienced one critical attack and many probing attacks during the course of this study. The critical attack was an attempt to relay email from an outside server to outside destinations. This attack was blocked because the email server was configured not to accept outside, unauthenticate connections for email relay. A firewall alone would not have prevented this attack. Had the spammer attempting to exploit the financial institution's email server been successful, the most likely result would have been disruption of the financial institution's ability to send legitimate email to external organizations utilizing email blacklists to block spam email.

The email attack indicates that firewalls and multiple layers of filtering are not a sufficient means to defend a network against unauthorized access. Access controls on the hosts accessible from public networks must also have proper configurations in order to prevent attacks or misuse.

A4. Use of multiple layers of security can reduce the overall risk of unauthorized access to systems.

The financial institution has three multi-layer security mechanisms. The first, edge router access control lists and firewalls, has been discussed in the preceeding sections. The second multi-layer security posture is anti-virus detection and deletion.

The financial institution's original anti-virus layer was centered on the workstation level of the internal network and the primary file server. This posture allowed for two virus outbreaks to occur. While the outbreaks were limited to less than five workstations, the impacts cost the institution lost employee productivity while the workstations were cleaned and increased external costs because outside contractors were brought in to correct the issue. The source of the outbreaks was subsequently traced to emails with attachments containing malicious code.

In September 2002, the financial institution implemented three-layer anti-virus configuration. The first layer centered on the workstations, the second layer performed anti-virus scanning on all file activity on the main file servers, and the third layer focused on scanning all emails and email attachments for malicious code. All layers are updated on a daily basis when new virus definition files are available from the vendor of the anti-virus software. The primary finding for the approach is that the primary vector for malicious code is email (Chapter 4:Anti-Virus Layers). The one workstation detection of a virus after September 2002 was due to an infected CD brought in to office by an employee. This did not result in an outbreak.

The final multi-layer security mechanism is centers on user IDs and passwords. The financial institution enforces compliance with security policies through the nework operating system. The primary internal systems requiring authentication are the network file, print, and email systems. Outside the scope of this study are the external service providers which also require differing user ID and password construction.

The primary finding for user passwords (Chapter 4: User Password Controls) is that the users tend to incorrectly type their passwords frequently during the course of the average work day. This is due to the complexity of the passwords. Each password is required to have an uppercase, a lowercase, and a numeric character and be at least eight characters in length. However, review of the system security logs on the network domain controller show that only one user locked out their account during the period of this study. In order to lock out a user account, the password must be entered incorrectly three times within one hour. The lock out period is twenty four hours without administrator intervention.

These three interlocking multilayer security constructs make it difficult to attack the financial institution's internal network. The goal of any implemented security architecture is to make it cost too much in terms of resources to attempt to gain access while not rendering the systems unusable to the authorized users. Over the seven

months of this study, the financial institution did not have a single successful penetration.

A5. The configuration of the computers used to probe and attack the organization will be variable.

The result of scanning the hostile hosts (Chapter 4: Complexity of Attack) clearly demonstrates two forms of complexity as defined by Strogatz (2001): Connection diversity and Node Diversity. Connection diversity is demonstrated by the results of the reverse DNS lookups performed during services determination. The DNS names determined during the services scanning with NMAPWin infer the following types of connections:

1. Dial-up connections were used at minimum of 485 (11.5%) times. By definition, a dial-up connection is bandwidth limited to less than 56Kbps. Multiple Internet service providers were identified, both foreign and domestic.

2. Broadband connections were used at a minimum of 538 (12.8%) times. These are variable, shared bandwidth connections that can yield bandwidth speeds exceeding 3 Mbps depending upon a number of factors. Some of the factors affecting broadband bandwidth include the number of hosts on the network segment, whether or not the Internet service provider has capped the speed of connection, and the bandwidth aggregation that the Internet service provider utilizes to save costs.

3. Educational connections (EDU domains) were used 109 (2.6%) times. The bandwidth available to a hostile host originating from an EDU domain is also dependent on many of the same factors as broadband connections. It seems unlikely that the schools involved sanctioned hostile probes of the financial institution.

4. Non-EDU or commercial domain connections were used 599 (14.2%) times. Many of these hosts can be defined as web, FTP and email servers that were being used as launch points to obscure the real attacker's identity. These connections probably have the highest degree of connection diversity with the majority of connections falling between DS0 (64Kbps) and T1 (1.544 Mbps) bandwidth speeds.

The commercial and educational domains had a small number of hosts that were located behind firewalls or packet filters. This shows that having a firewall is no guarantee of protection.

The second form of complexity, Node Diversity, is demonstrated by the services found to be available on the attacking hosts. Characterization of the standard hostile host is impossible to determine. Even the definition of a range of probable service configurations is difficult.

Hostile hosts had identified operating systems such as UNIX (many different proprietary distributions and versions), Linux (every major distribution was identified), Windows operating systems from Windows 95 to Windows 2000 Advanced Server, and even a few Novell NetWare servers. The services running on these platforms were also variable. Potential services ran from two or three services to several thousand open ports.

A6. The geographic location of the computers used to launch attacks and hostile probes will be much wider than the primary market area of the organization.

The determination of the source country for an individual IP address was made be comparing the logged source IP addresses of hostile traffic to the assigned IP address ranges made by the four regional Internet address registries. This is not a foolproof method, but is the only available method for analysis.

The financial institution in this study has few account holders outside a two hundred mile radius from its primary location and no foreign accounts. The occurance of source IP addresses outside of the United States should have been minimal. However, 67 countries other than the United States were identified by source IP address.

The distribution of countries is also interesting. There are countries that were expected such as the Peoples Republic of China and the Russian Federation, but unexpected countries included many third world countries and allies of the United States. Refer to Chapter 4: Complexity of Attack and Appendix C: Source Country by IP address for further information on the source countries that were detected by the financial institution during the period of this study.

It must be noted that merely knowing the source IP address does not necessarily identify the source of attack or the attacker's motivation. Many attackers will penetrate foreign hosts to obscure their actual location and launch attacks from the comprised foreign hosts. The perceived technological capability of the source country must not be used to discount the hostile traffic originating from countries like Papua New Guinea and Iran. While these countries may not have extensive technological infrastructures or may have theological prohitbitions on certain uses of technology, the requirement for lauching a technological attack only requires knowledge and access to the Internet.

There was one unanticipated finding in this study. The attacker methodology (Scambray. McClure and Kurtz 2001) as shown in Figure 12 was not observed during the course of this study. This methodology implies that an attacker will select a target organization and then completely enumerate the hosts and available services.

The unique IP address analysis indicates that the hostile hosts probing or attacking the financial institution were interested in single service ports. This was strongly indicated by the fact that only three unique IP addresses were identified in more than one month

during the course of the study. It appears that the financial institution experienced directed individual service probes or attacks without wholesale enumeration of ports.

Future Directions

There are two key directions for this study to persue in the future. The first direction would be to further this study by continued incrementally enhancing the financial institution's security architecture. The first enhancement would be to add network and host intrusion deterction. The intrusion detection systems would be utilized to further characterize the nature of the hostile traffic into sepcfic exploits, provide for some degree alerting process for the financial institution's information systems personnel of attacks in progress, and to provide for active response to hostile traffic. The network intrusion detection systems should be placed between the edge router and the firewall and on the internal network. Host intrusion detection should be placed on all public servers located on the financial institution's network. All of the alerting and logging functions should be integrated to accurately track and mitigate hostile traffic and intrusion attempts.

The second direction would be to extend this study across industry sectors and the Internet as a whole. This would allow for generalizations to be formed characterizing attacker approaches, the efficacy of layering strategies, and the combination of the various complexity types suggested by Strogatz. This may not be practical in terms of time and resources. However, modeling the complexities of attacker behavior and security architectures would form the basis toward establishing novel solutions to today's information systems security problems and potential reduce the time necessary to determine if an attack is under way.

BIBLIOGRAPHY

Adamic, Lada A. "The Small World Web," Proceedings of the 3rd European Conference on Research and Advanced Technology for Digital Libraries, 1999 (accessed 13 December 2002, available at http://citeseer.nj.nec.com/adamic99small.html).

Anderson, Paul and James, Gail. "Performance Soars, Features Vary", NetworkWorld, June 14, 1999. (accessed 21 December 2001, available at http://www.nwfusion.com/reviews/0614rev.html)

Aunger, Robert. The Electric Meme: A New Theory of How We Think. New York: The Free Press, 2002.

Armstrong, Illena. "Legislators Turn Up the Heat on Cybercrime," SC Magazine April 2001: 33-34.

Axelrod, Robert and Cohen, Michael D. Harnessing Complexity: Organizational Implications of a Scientific Frontier. New York: The Free Press, 1999.

Bell, D.E. and LaPadula, L.J. "Secure Computer System: Unified Exposition and Multics Interpretation", MTR-2997, Rev. 1, MITRE Corp., Bedford, Mass., March 1976.

Bound, Jim. "IPv6 Implementation," ISOC Member Briefing #4, Internet Society: September 2001 (accessed 26 October 2001 available at http://www.isoc.org/briefings/004/index.html).

Burnburg, Matthew K. Broadband Security Concerns for Business. Client security briefing paper, electronic document, 15 May 2001.

Carson, Paula Phillips; Lanier, Patricia A Carson, Kerry David Guidry, Brandi N. "Clearing a Path through the Management Fashion Jungle", Academy of Management Journal, December 2000.

Chirillo, John. Hack Attacks Revealed: A Complete Reference with Custom Security Hacking Toolkit. New York: John Wiley & Sons, 2001.

Chirillo, John. Hack Attacks Encyclopedia: A Complete History of Hacks, Cracks, Phreaks, and Spies over Time. New York: John Wiley & Sons, 2001.

CipherTrust. How to Secure Email Servers. Alpharetta, GA: CipherTrust, October 22, 2002. (accessed October 31, 2002 available at http://www.ciphertrust.com/bitpipe/ciphertrust-how_to_secure_email_servers.pdf).

Cisco Systems. Virtual Private Networks: Your Guide to the New World Opportunity. San Jose: Cisco Systems, 2001 (accessed 21 December 2002, available at http://www.cisco.com/application/pdf/en/us/guest/netsol/ns193/c671/ccmigration_09186a00800a2fde.pdf).

Dawkins, Richard. "Viruses of the Mind." Dennett and His Critics: Demystifying Mind. Ed. Bo Dahlbohm. Oxford: Blackwell, 1993.

Denning, Dorothy E. Information Warfare and Security. New York: ACM Press, 1999.
Fratto, Mike. "Buyers Guide: Enterprise Firewalls", Network Computing, 10 December 2001:90-2.
Gallagher, Christopher. "Health Information Privacy: The Federal Floor's State Elevator," Glasser LegalWorks Conferece – HIPAA Privacy Compliance, Washington, DC. 25 July 2001 (accessed 6 January 2003, available at http://www.gcglaw.com/resources/healthcare/healthprivacy.pdf).
Harrison, Ann. "Companies point fingers over Nike Web site hijacking", NetworkWorld, June 30, 2000. (accessed 12 February 2001, available at http://www.nwfusion.com/news/2000/0630nike.html).
Helms, Marilyn M. and Wright, Peter. "External considerations: Their influence on future strategic planning," Management Decision v30n8, 1992.
Hiltz, Starr Roxanne and Turoff, Murray. The Network Nation: Human Communication via Computer. Cambridge, Massachusetts: MIT Press, 1993.
Internet Engineering Task Force. RFC 1700: Assigned Numbers. October 1994. (accessed 18 April 2002, available at http://www.ietf.org/rfc/rfc1700.txt)
Kabay, Michael E. The NCSA Guide to Enterprise Security: Protecting Information Assets. New York: McGraw-Hill, 1996.
Koprowski, Gene. "Emerging Uncertainty Over IPv6," Computer November 1998: 16-7+.
"Laying Down the Law", Technology Review May 2001: 65-8.
Lederer, Albert L., Mirchandi, Dinesh A., and Sims, Kenneth. "The Search for Strategic Advantage from the World Wide Web," International Journal of Electronic Commerce, Summer 2001.
Lee, Jintae and Collar, Emilio. "Information Technology Fashions: Building on the Theory of Management Fashions", MIT Center for Coordination Science, Working Paper #219, June 2002 (accessed 31 December 2002 at http://ccs.mit.edu/papers/pdf/wp219.pdf).
Levy, Stephen. Crypto: How the Code Rebels Beat the Government – Saving Privacy in the Digital Age. New York: Viking, 2001.
Liang, Qiao and Xiangsui, Wang. Unrestricted Warfare. Beijing: PLA Literature and Arts Publishing House, 1999.
Maconachy, W. Victor, Schou, Corey D., Ragsdale, Daniel, and Welch, Don. "A Model for Information Assurance: An Integrated Approach". West Point: Proceedings of the 2001 IEEE Workshop on Information Assurance and Security, June 2001.
McCumber, John. "Information Systems Security: A Comprehensive Model", Proceedings of the 14th National Computer Security Conference. Baltimore: National Institute of Standards and Technology, October 1991.

McKenney, Brian. “Defense in Depth,” The Edge: The Mitre Advanced Technology Newsletter, February 2001, v5, #1 (accessed 15 September 2001 available at http://www.mitre.org/pubs/edge/february_01/mckenney.htm).
Murray, William Hugh. “Common System Design Flaws and Security Issues.” Information Security Management Handbook. Ed. Harold F. Tipton and Micki Krause. 4th Edition, Volume 2. Boca Raton: Auerbach Publications, CRC Press, 2001.
Parker, Donn B. Computer Security Management. Reston: Prentice-Hall, 1981
Pethia, Rich. Internet Security Trends. Pittsburgh: Carnegie-Mellon University, Software Engineering Institute, 2001. (accessed 12 September 2001, available from http://www.cert.org/present/internet-security-trends/sld016.htm)
Power, Richard. Tangled Web: Tales of Digital Crime from the Shadows of Cyberspace. Indianapolis: Que, 2000.
Power, Richard, ed. “2001 CSI/FBI Computer Crime and Security Survey,” Computer Security Issues & Trends, Spring 2001
Radcliff, Deborah. “Playing by Europe’s Rules,” ComputerWorld, 9 July 2001.
Richards, Donald R. “Biometric Identification.” Information Security Management Handbook. Ed. Harold F. Tipton and Micki Krause. 4th Edition, Volume 1. Boca Raton: Auerbach Publications, CRC Press, 2000.
Salkever, Alex. “Cyber-Extortion: When Data is Held Hostage,” Business Week, August 22, 2000.
Scambray, Joel; McClure, Stuart; and Kurtz, George. Hacking Exposed: Network Security Secrets and Solutions (Second Edition). New York: McGraw-Hill, 2001.
Schneider, Dave. "Security Management," Internet Management. Jessica Keyes, editor, New York: CRC Press, 2000.
Schneier, Bruce. “Attack Trees: Modeling Security Threats,” Dr. Dobb’s Journal, December 1999.
Schneier, Bruce. Secrets and Lies: Digital Security in a Networked World. New York: John Wiley & Sons, 2000.
Schwartau, Winn. Information Warfare: Cyberterrorism: Protecting Your Personal Security in the Electronic Age. 2nd ed. New York: Thunder Mouth Press, 1994.
Strogatz, Steven H. “Exploring Complex Networks”, Nature: 8 March 2001.
Sun-tzu. The Art of War. Trans. Ralph D. Sawyer. New York: Barnes & Noble Books, 1994.
The Ideahamster Organization. The Open Source Security Testing Methodology Manual. 26 February 2002. (accessed 14 March 2002, available from http://www.ideahamster.org/osstmm-description.htm)
Tiller, James S. and Fish, Bryan D. “Packet Sniffers and Network Monitors.” Information Security Management Handbook. Ed. Harold F. Tipton and

Micki Krause. 4th Edition, Volume 2. Boca Raton: Auerbach Publications, CRC Press, 2001.
Tipton, Harold F. and Krause, Micki. Information Security Management Handbook. Ed. Harold F. Tipton and Micki Krause. 4th Edition, Volume 2. Boca Raton: Auerbach Publications, CRC Press, 2001.
U.S. Department of Defense. Department of Defense Dictionary of Military and Associated Terms. Joint Publication 1-02. 12 April 2001. (accessed 14 September 2001, available from http://www.dtic.mil/doctrine/jel/new_pubs/jp1_02.pdf)
U.S. Department of Defense. Information Assurance Through Defense-In-Depth. February 2000. (accessed 14 September 2001, available from http://www.infowar.com/mil_c4i/01/InformationAssurance.pdf)
U.S. Department of Justice Federal Bureau of Investigation. "MAFIABOY", Press Release, 7 August 2000 (accessed 13 December 2002, available at http://www.fbi.gov/pressrel/pressrel00/mafia080700.htm).
U.S. Department of Justice. The Privacy Act of 1974. June 2001. (accessed 15 February 2002, available from http://www.usdoj.gov/foia/privstat.htm)
United States Internet Industry Association. The Electronic Communications Privacy Act. March 2001. (accessed 15 February 2002, available from http://usiia.org/legis/ecpa.html)
United States Senate Committee on Banking, Housing, and Urban Affairs. Conference Report and Text of the Graham-Leach-Bliley Act. November 1999. (accessed 15 February 2002, available from http://www.senate.gov/~banking/conf/confrpt.htm)
Von Clausewitz, Carl. On War. Trans. Michael Howard and Peter Paret. New York: Knopf, 1993.
Watts, Duncan J. Small Worlds: The Dynamics of Networks between Order and Randomness. Princeton: Princeton University Press, 1999.
Watts, Duncan J. and Strogatz, Steven H. "Collective Dynamics of 'Small-World' Networks", Nature: 4 June 1998.
Wellman, Barry. "Computer Networks as Social Networks", Science: 14 September 2001.

APPENDIX A: POLICIES AND PROCEDURES

Note: All references that identify the financial institution have been removed from these appendices.

ANYBANK

INTRANET AND INTERNET SECURITY POLICY

AUGUST 2002

Introduction

This is an Acceptable Use Policy that provides rules and guidelines for Internet and e-mail use within AnyBank.

Our electronic mail capabilities have become integral to our internal communications. Increasingly, however, e-mail is becoming a preferred medium for external business communication, either via the Internet or other public computer systems. Further, Internet access has become increasingly important to many employees conducting business on behalf of the company. While the Internet provides tremendous business and learning opportunities, it is important that employees be aware of the risks associated with external e-mail and Internet access. The Internet and External E-mail Acceptable Use Policy (AUP) was developed to help employees optimize their use of the Internet, protect confidential information of the company and others, preserve and enhance the company's image, and minimize costs associated with Internet usage.

Scope

The AUP was developed for all personnel who access, either directly or indirectly, the Internet or any public networked or dial-in system. The AUP applies under these circumstances:

When company personnel provide or acquire information through access to any external public computer system using company provided access accounts or company provided equipment.

When people identify themselves as associated with the company (i.e., officers, employees, and contractors) in their personal use of individually acquired access accounts to public computer systems.

Providing information includes:

- Answering questions
- Sending e-mail
- Uploading files
- Posting information
- Creating personal web pages

Acquiring information includes:

- Asking questions and searching for information
- Receiving e-mail
- Downloading files
- Surfing the World Wide Web (WWW)
- Reading newsgroups

Examples of public computer systems include:

- Internet e-mail
- Internet service providers
- Bulletin boards
- Real-time chat sessions
- Online services (i.e., CompuServe, America Online, MSN, Europe Online UK, etc.)
- UseNet newsgroups

- World Wide Web (WWW)
- File Transfer Protocol (FTP)
- All other publicly accessible computer systems and on-line services

General Security Policy

Prohibited Activities

The following are prohibited when using company-provided access accounts or equipment, or when identifying yourself as associated with the company using an individually acquired access account:

- Downloading, transmission, and possession of pornographic and sexually explicit materials.
- Transmitting libelous, slanderous, threatening or abusive messages, or any messages that may be construed as such.
- Sending or otherwise participating in chain letters.

Proprietary Information

Obey all copyright laws. Questions concerning copyright compliance should be directed to the legal group in your region. Special note: Although material may be available for "free" on the Internet, you do not have the legal right to copy it. Compare the Internet to a bookstore - you are free to browse as much as you like, but you are not welcome to make copies. Obtain the copyright holder's written permission before copying from the Internet or other public computer system.

Do not transmit proprietary or confidential materials of the company over any public computer system unless properly encrypted. Electronic communications between people within the company should be made using the company's e-mail system as opposed to individual Internet addresses.

No client-related information of any kind and no confidential information pertaining to others (i.e., suppliers, vendors, or alliance partners) is to be sent over any public computer system unless the client or other third party has specifically agreed, in writing and in advance, to the company's use of the public computer system for confidential communications, and then only if the agreed upon procedures are observed (i.e., encryption).

Electronic Mail Policy

When communicating via e-mail or any public computer system, all of the company's existing professional standards for written communications apply.

Accessing the Internet and other public computer systems for non-business use is generally not allowed when using either company provided access accounts or company provided equipment. Please contact the CIO organization for exceptions.

Always obtain the approval of your group's management team before any messages representing the company are posted to the Internet or to any other public computer system. Posting messages to public computer systems includes subscribing to mailing lists and participating in newsgroups.

When communicating with a broad public audience that has reason to know of your association with the company, using either an individually acquired or a company provided account, the following disclaimer must appear on all communications: "The views expressed herein are the personal views and opinions of the current user and are not made on behalf of his or her current employer." Users communicating with a specific person already known to them from face-to-face professional interaction are not required to use this disclaimer.

Ensure that the addressed recipients of your e-mail are really the intended recipients. There is no way to verify users' names or affiliations from their e-mail addresses.

Confirm recipients' ability to receive attachments prior to sending an attachment.

Internet Access Policy

Mailing Lists

Requests for mailing lists or other similar services should be made for business purposes only. Exercise caution and be very selective when subscribing to any of these services.

Check all internal sources for information before subscribing to any mailing list.

Ensure that you know how to unsubscribe from a mailing list before requesting a subscription.

Forums

When participating in a forum, obey all rules and ensure that you read 'Frequently Asked Questions' (FAQ's). FAQ's are often posted within a particular newsgroup.

Personal web pages

When creating a personal web page, company personnel may state where they are employed and their specific responsibilities, in addition to providing a link to the company's main web site. Personnel should not attempt to describe any other aspect of the company's services. The following disclaimer must also appear on the personal web page: "The views expressed herein are the personal views and opinions of the current user and are not made on behalf of his or her current employer."

Security

Immediately inform the IT services group of any communication, system problem or other circumstance that you think may indicate a breach of security or other risk to the integrity of the company's system.

The Internet is not a secure environment. Do not assume any activities are private.

There is no way to prevent the redistribution of e-mail messages. Never assume that any message is a one-time, one-to-one communication.

Do not enable any program or macro/agent to automatically forward e-mail to or via the Internet or any other external system.

If you suspect that your Internet password and ID have become compromised, immediately request a new password and ID from your local administrator. (Internet passwords and IDs should be treated with the same precaution as a telephone calling card number or an Automatic Teller Machine personal identification number).

Do not transmit IDs, passwords, internal network configurations or addresses, or system names over the Internet.

Unauthorized bypass or any attempt to circumvent any security system is prohibited.

Do not leave your computer unattended while connected to the Internet.

When possible, users should connect to the Internet through the company's Internet gateway, not via a modem.

System Integrity

Verify that the company's current standard antivirus software is installed on your computer. Ensure that you scan all files attached to external e-mail as well as any files downloaded from an external system.

No workstation may maintain a peer-to-peer connection with any other workstation while connected to the Internet or any other external system.

Exercise caution when downloading large files (i.e., over 1 MB, including text and multimedia files) should be taken. Downloading large files can take a long time and therefore degrade network performance for everyone on the network.

The company's computer networks (including all media and data paths facilitated by the company), and the messages and information residing on or exchanged through them, are the property of the company. Management tools are used to track usage and log network activity, which is audited by company personnel.

Compliance and Guidance

Company personnel are expected to exercise good judgment and act in a professional manner whenever accessing the Internet or any other external system. Please be aware that disciplinary actions, ranging from the revocation of your Internet access to dismissal, may result from failure to adhere to any policy contained in the AUP. If there is any doubt or question concerning whether to use the Internet or another external system, please contact Jane Doe or John Doe.

The AUP is in addition to, and is not meant to supersede, any other policies, procedures, or standards applying to communications between the company and others. The AUP may be modified or replaced as circumstances change and/or as assessments of risks and benefits develop.

ANYBANK

INFORMATION PROTECTION POLICY

VERSION 1.4

AUGUST 2002

CHANGE RECORD

Date	Version	Changes	Made By
4/15/01	1.0	Initial version	JD – mmm
4/30/01	1.1	Minor revisions	JD – mmm
5/2/01	1.2	Included Introduction Section	JD – mmm
4/2/02	1.3	Minor revisions	JD – mmm
4/11/02	1.3	Minor revisions	JD – nnn
5/24/02	1.3	Formatting revisions	nnn
8/21/02	1.4	Revisions to align new IS env and policies	JD-mmm

INTRODUCTION

PURPOSE

The purpose of this policy is to establish management direction, procedures, and requirements to ensure the appropriate protection of AnyBank information handled by computer networks.

SCOPE

This policy applies to all employees, contractors, consultants, temporaries, and other workers at AnyBank, including those workers affiliated with third parties who access AnyBank computer networks. The policy also applies to all computer and data communication systems owned by and/or administered by AnyBank.

RESPONSIBILITIES

The IT Committee is composed of Jane Doe, Assistant Vice President – Bank, and John Doe, Executive Vice President and Cashier–Bank. At quarterly and ad hoc meetings, this committee will: (a) periodically review the status of AnyBank's computer and network security, (b) as needed, review and monitor remedial work related to computer and network security incidents, (c) authorize and later judge the results of major projects dealing with computer and network security, (d) approve new or modified information security policies, standards, guidelines, and procedures, and (e) perform other high-level information security management activities. This committee is responsible to the AnyBank Bancorp, Inc. Board of Directors.

End User Policies

PASSWORD UTILIZATION

Minimum Password Length–The length of passwords must always be checked automatically at the time that users construct or select them. All passwords must have at least 8 characters.

User-Chosen Passwords Must Not Be Reused–Users must not construct passwords that are identical or substantially similar to passwords that they had previously employed.

Passwords Must Contain both Alphabetic And Non-Alphabetic Characters–All user-chosen passwords must contain at least one uppercase, one lowercase, and one numeric character. This will help make passwords difficult-to-guess by unauthorized parties such as hackers and industrial spies. The use of control characters and other non-printing characters is forbidden because they may inadvertently cause network transmission problems or unintentionally invoke certain system utilities.

Users are prohibited from constructing fixed passwords by combining a set of characters that do not change, with a set of characters that predictably change. In these prohibited passwords, characters which change are typically based on the month, a department, a project, or some other easily-guessed factor. For example, users must not employ passwords like "X34JAN" in January, "X34FEB" in February, etc.

Writing Passwords Down and Leaving Where Others Could Discover–Passwords must not be written down and left in a place where unauthorized persons might discover them.

Password Sharing Prohibition–Regardless of the circumstances, passwords must never be shared or revealed to anyone else besides the authorized user. To do so exposes the authorized user to responsibility for actions that the other party takes with the password. If users need to share computer resident data, they should use electronic mail, public directories on local area network servers, and other mechanisms.

Users Responsible for All Activities Involving Personal User-Ids–Users are responsible for all activity performed with their personal user-IDs. User-IDs may not be utilized by anyone but the individuals to whom they have been issued. Users must not allow others to perform any activity with their user-IDs. Similarly, users are forbidden from performing any activity with IDs belonging to other users (excepting anonymous user-IDs like “guest”).

Leaving Sensitive Systems without Logging-Off – If the computer system to which they are connected contains sensitive or valuable information, users must not leave their microcomputer (PC), workstation, or terminal unattended without first logging-out.

USE OF SYSTEMS

Games May Not Be Stored or Used On AnyBank Computer Systems

Incidental Personal Use of Business Systems Permissible–AnyBank information systems are provided for, and must be used only for business purposes. Incidental personal use is permissible if the use: (a) does not consume more than a trivial amount of resources that could otherwise be used for business purposes, (b) does not interfere with worker productivity, and (c) does not preempt any business activity. Permissible incidental use of an electronic mail system would, for example, involve sending a message to schedule a luncheon.

Prohibition Against Non-Approved System Uses–Subscribers to AnyBank computing and communications services must not use these facilities for soliciting business, selling products, or otherwise engaging in commercial activities other than those expressly permitted by AnyBank management.

OTHER PRIVILEGE RESTRICTIONS

Unbecoming Conduct and the Revocation of Access Privileges – AnyBank management reserves the right to revoke the privileges of any user at any time. Conduct that interferes with the normal and proper operation of AnyBank information systems, which adversely affects the ability of others to use these information systems, or which is harmful or offensive to others will not be permitted.

Prohibition against Testing Information System Controls – Workers must not test, or attempt to compromise internal controls unless specifically approved in advance and in writing by the IT Committee.

LOGGING

Logs Of User-Initiated Security Relevant Activities – To assure that users are held accountable for their actions on AnyBank production computer systems, one or more logs tracing security relevant activities to specific users must be securely maintained for a reasonable period of time.

COMPUTER VIRUSES AND WORMS

Virus Eradication Requires Support of Systems Administrator – Users are prohibited from attempting to eradicate a computer virus from their system unless they do so while in communication with a systems administrator. This communication will help minimize damage to data files and software, as well as ensure that information needed to detect a re-infection has been recorded.

Approved Virus Checking Programs Required on PCs and LAN Servers – Virus checking programs approved by the IT Committee must be continuously enabled on all local area network (LAN) servers and networked personal computers (PCs). Workers are not allowed to disable any virus protection software running on any AnyBank computer or server.

All User Involvement With Computer Viruses Prohibited – Users must not intentionally write, generate, compile, copy, collect, propagate, execute, or attempt to introduce any computer code designed to self-replicate, damage, or otherwise hinder the performance of or access to any AnyBank computer, network, or information. Such software is known as a virus, bacteria, worm, Trojan horse, and similar names.

RESTRICTIONS OF PRIVACY RIGHTS

Right of Management to Examine Data Stored on AnyBank Systems – All messages sent over AnyBank computer and communications systems are the property of AnyBank. To properly maintain and manage this property, management reserves the right to examine all information stored in or transmitted by these systems. Since AnyBank's computer and communication systems must be used for business purposes only, workers should have no expectation of privacy associated with the information they store in or send through these systems.

Disclosure Of Information On AnyBank Systems To Law Enforcement – By making use of AnyBank systems, users consent to allow all information they store on AnyBank systems to be divulged to law enforcement at the discretion of AnyBank management. Release of information will be in compliance AnyBank policies and procedures concerning client privacy.

OVERALL DATA CONFIDENTIALITY POLICIES

Confidentiality Agreements Required for All AnyBank Workers – All employees and contractors (temporaries, consultants, outsourcing firms, etc.) must personally sign a AnyBank non-disclosure agreement. The provision of a signature must take place before work begins, or if a worker has been working without a non-disclosure agreement, a signature must be provided as a condition of continued employment.

Default Restrictions on Dissemination of AnyBank Information – All AnyBank internal information must be protected from disclosure to third parties by default. Third parties may be given access to AnyBank internal information only when a demonstrable need-to-know exists, and when such a disclosure has been expressly authorized by AnyBank management.

Disclosure of System Vulnerability Exploitation and Victim Data – AnyBank staff must not publicly disclose information about the individuals, organizations, or specific systems that have been damaged by computer crimes and computer abuses. Likewise, the specific methods used to exploit certain system vulnerabilities must not be disclosed publicly. All disclosures, including law enforcement, must be approved by AnyBank management prior to the release of any information.

MISCELLANEOUS CONFIDENTIALITY POLICIES

Browsing on AnyBank Systems and Networks Prohibited – Workers must not browse through AnyBank computer systems or networks. For example, curious searching for interesting files and/or programs in the directories of other users is prohibited. Steps taken to legitimately locate information needed to perform one's job are not considered browsing.

CONTINGENCY PLANNING

Expected Employee Assistance during Business Restoration – Employees are expected to be present, and to assist to the best of their abilities, with the restoration of normal business activity after an emergency or a disaster disrupts AnyBank business activity. After an employee's family and personal assets are determined to be safe, employees are expected to put in overtime, work under stressful conditions, and otherwise do what it takes to maintain AnyBank as a going concern.

BACKUP, ARCHIVAL STORAGE, AND DISPOSAL OF DATA

What Data to Backup and Minimum Backup Frequency – All critical business information and critical software resident on AnyBank computer systems must be periodically backed-up. These backup processes must be performed at least daily, and with sufficient frequency to support documented contingency plans.

Off-Site Storage of Backup Media - Backups of essential business information and software must be stored in an environmentally-protected and access-controlled site which is a sufficient distance away from the originating facility to escape a local disaster.

Regular Testing of Used Data Media Employed for Archival Storage–The computer data media used for storing sensitive, critical, or valuable information must be high quality and must be tested monthly to ensure that it can properly record the information in question. Used data media that can no longer reliably retain information must not be used for archival storage.

DIAL-UP COMPUTER COMMUNICATIONS

Use of Cable Modems for Business Communications – Cable modems must not be used for any AnyBank business communications unless a firewall and a virtual private network (VPN) is employed on the involved computers.

Prohibition against Personal Computer Modems In Auto-answer Mode – Users must not leave modems connected to personal computers in auto-answer mode, such that they are able to receive in-coming dial-up calls.

Approval Required For Systems Accepting In-Coming Dial-Up Calls – AnyBank workers must not establish any communications systems which accept in-coming dial-up calls unless these systems have first been approved by the IT Committee.

ELECTRONIC MAIL SYSTEMS

Using an Electronic Mail Account Assigned to another Individual – Workers must not use an electronic mail account assigned to another individual to either send or receive messages. If there is need to read another's mail (while they are away on vacation for instance), message forwarding and other facilities must instead be used.

Forwarding Externally Provided Electronic Mail Messages – Workers must not create their own, or forward externally provided electronic mail messages which may be considered to be harassment or which may contribute to a hostile work

environment. Among other things, a hostile work environment is created when derogatory comments about a certain sex, race, religion, or sexual preference are circulated.

Privacy Expectations And Electronic Mail – Workers must treat electronic mail messages and files as private information. Electronic mail must be handled as a private and direct communication between a sender and a recipient.

Treat Electronic Mail As Public Communications – Consider electronic mail to be the electronic equivalent of a postcard. Unless the material is encrypted, users must refrain from sending credit card numbers, passwords, research and development information, and other sensitive data via electronic mail.

Authorization To Read Electronic Mail Messages Of Other Workers – When AnyBank management collectively agree to it, electronic mail messages flowing through AnyBank systems may be monitored for internal policy compliance, suspected criminal activity, and other systems management reasons. Unless AnyBank Management has specifically delegated electronic mail monitoring tasks, all workers must refrain from this activity.

Profane, Obscene or Derogatory Remarks in Electronic Mail Messages – Workers must not use profanity, obscenities, or derogatory remarks in electronic mail messages discussing employees, customers, or competitors. Such remarks—even when made in jest—may create legal problems such as trade libel and defamation of character. Special caution is warranted because backup and archival copies of electronic mail may actually be more permanent and more readily accessed than traditional paper communications.

Message Content Restrictions For AnyBank Information Systems – Workers are prohibited from sending or forwarding any messages via AnyBank information systems that a reasonable person would consider to be defamatory, harassing, or explicitly sexual. Workers are also prohibited from sending or forwarding messages or images via AnyBank systems that would be likely to offend on the basis of race, gender, national origin, sexual orientation, religion, political beliefs, or disability.

Electronic Mail Messages Are Company Records – The AnyBank electronic mail system is to be used only for business purposes. All messages sent by electronic mail are AnyBank records. The Company reserves the right to access and disclose all messages sent over its electronic mail system, for any purpose. AnyBank Management may review the electronic mail communications of workers to determine whether they have breached security, violated Company

policy, or taken other unauthorized actions. The Company may also disclose electronic mail messages to law enforcement officials without prior notice to the workers who may have sent or received such messages.

Personal Use Of Electronic Mail Systems – Electronic mail systems are intended to be used primarily for business purposes. Any personal use must not interfere with normal business activities, must not involve solicitation, must not be associated with any for-profit outside business activity, and must not potentially embarrass AnyBank.

INTERNET CONNECTIONS

Internet Representations Including AnyBank Affiliation – When engaged in discussion groups, chat rooms, and other Internet offerings, only those individuals authorized by management to provide official support for AnyBank products and services may indicate their affiliation with AnyBank. This may be accomplished explicitly by adding certain words to their messages. Alternatively, it can be accomplished implicitly via the use of an electronic mail address. In either case, unless they have received instructions to the contrary, whenever workers disclose an affiliation with AnyBank, they must clearly indicate that "the opinions expressed are my own, and not necessarily those of my employer."

Internet Discussion Group And Chat Room Participation Forbidden – Unless expressly authorized by senior management, when using AnyBank information systems, all AnyBank workers are forbidden from participating in Internet discussion groups, chat rooms, or other public electronic forums. This prohibition also covers the use of Instant Messaging software provided by any organization other than AnyBank.

AnyBank Blocks Certain Non-Business Internet Web Sites – AnyBank information systems routinely prevents users from connecting with certain non-business web sites. Workers using AnyBank information systems who discover they have connected with a web site that contains sexually explicit, racist, or other potentially offensive material must immediately disconnect from that site. The ability to connect with a specific web site does not in itself imply that workers are permitted to visit that site. AnyBank management reserves the right to monitor and log all Internet usage without prior worker notification.

Request to Download Software from Internet – All software and files downloaded from non-AnyBank sources via the Internet (or any other public network) must be approved prior to download by a system administrator.

Handling Software And Files Down-loaded from Internet – All software and files down-loaded from non-AnyBank sources via the Internet (or any other public network) must be screened with virus detection software. This screening must take place prior to being run or examined via another program such as a word processing package.

Posting AnyBank Material On The Internet – Users must not place AnyBank material (software, internal memos, press releases, etc.) on any publicly accessible Internet computer system unless the IT Committee has first approved the posting.

Exchanges Of Information Over The Internet – AnyBank software, documentation, and all other types of internal information must not be sold or otherwise transferred to any non-AnyBank party for any purposes other than the business purposes expressly authorized by management and in accordance to all relevant internal policies, procedures, and governmental regulation. Exchanges of software and/or data between AnyBank and any third party may not proceed unless a vice president has first signed a written agreement. Such an agreement must specify the terms of the exchange, as well as the ways in which the software and/or data is to be handled and protected. Regular business practices—such as shipment of technical information in response to a customer purchase order—need not involve such a specific agreement since the terms of the exchange are already defined.

REPORTING OF SECURITY PROBLEMS

Required Reporting of Information Security Incidents – All suspected information security incidents must be reported as quickly as possible to the IT Committee.

Internal Reporting Of Information Security Violations & Problems – AnyBank workers have a duty to report all information security violations and problems to the IT Committee on a timely basis so that prompt remedial action may be taken.
Protection Of Workers Who Report Information Security Problems – AnyBank will protect workers who report in good faith what they believe to be a violation of laws or regulations, or conditions that could jeopardize the health or safety of other workers. This means that such workers will not be terminated, threatened, or discriminated against because they report what they perceive to be a wrongdoing or dangerous situation. Before taking any other action, these workers must report the problem to their manager or the Internal Auditing Department, and then give the organization time to remedy the situation.

Immediate Reporting Of Suspected Computer Virus Infestation – Computer viruses can spread quickly and need to be eradicated as soon as possible to limit serious damage to computers and data. Accordingly, if workers report a computer virus infestation to the IT Committee immediately after it is noticed, even if their negligence was a contributing factor, no disciplinary action will be taken. The only exception to this early reporting amnesty will be those circumstances where a worker knowingly caused a computer virus to be introduced into AnyBank systems. However, if a report of a known infestation is not promptly made, and if an investigation reveals that certain workers were aware of the infestation, these workers will be subject to disciplinary action including termination.

HUMAN RESOURCES MATTERS–DISCIPLINE AND TERMINATION

Disciplinary Measures For Information Security Non-Compliance – Non-compliance with information security policies, standards, or procedures is grounds for disciplinary actions up to and including termination.

IT COMMITTEE ROLE

Information Security Is Every Worker's Duty – Responsibility for information security on a day-to-day basis is every worker's duty. Specific responsibility for information security is NOT solely vested in the IT Committee.

Management & Technical Policies

PASSWORD UTILIZATION–MANAGEMENT & TECHNICAL

Periodic Forced Password Changes – All users must be automatically forced to change their passwords at least once every thirty (30) days.

Limits on Consecutive Unsuccessful Attempts to Enter A Password – To prevent password guessing attacks, the number of consecutive attempts to enter an incorrect password must be strictly limited. After three (3) unsuccessful attempts to enter a password, the involved user-ID must be suspended until reset by a system administrator.

Unique Passwords for Each Internal Network Device – All AnyBank internal network devices (routers, firewalls, access control servers, etc.) must have unique passwords or other access control mechanisms. A compromise in the security of one device will therefore not automatically lead to a compromise in other devices.
Changing Vendor Default Passwords – All vendor-supplied default passwords must be changed before any computer or communications system is used for AnyBank business.

Forced Change of All Passwords – Whenever an unauthorized party has compromised a system, system managers must immediately change every password on the involved system. Even suspicion of a compromise requires that all passwords be changed immediately. Under either of these circumstances, a trusted version of the operating system and all security-related software must also be reloaded. Similarly, under either of these circumstances, all recent changes to user and system privileges must be reviewed for unauthorized modifications.

USE OF SYSTEMS–MANAGEMENT & TECHNICAL

Granting User-IDs To Outsiders – Individuals who are not employees, contractors, or consultants must not be granted a user-ID or otherwise be given privileges to use AnyBank computers or communications systems unless the written approval of the IT Committee has first been obtained.

Third Party Access To AnyBank Systems Requires Signed Contract – Before any third party is given access to AnyBank systems, a contract defining the terms and conditions of such access must have been signed by a responsible manager at the third party organization. Both the IT Committee and the General Counsel must also approve these terms and conditions.

Information Systems Access Privileges Terminate When Workers Leave – All AnyBank information systems privileges must be promptly terminated at the time that a worker ceases to provide services to AnyBank.

SPECIAL PRIVILEGES–MANAGEMENT & TECHNICAL

Supports For Special Privileged Type Of Users – All network systems must support a special type of user-ID which has broadly-defined system privileges. This user-ID will in turn enable authorized individuals to change the security state of systems.

Restriction Of Special System Privileges – Special system privileges, such as the ability to examine the files of other users, must be restricted to those directly responsible for system management and/or security. These privileges must be granted only to those who have attended an approved systems administrator training class.

Limited Number Of Privileged User-IDs – The number of privileged user-IDs must be strictly limited to those individuals who absolutely must have such privileges for authorized business purposes.

Multi-user systems administrators must have at least two user-IDs – One of these user-IDs must provide privileged access and be logged; the other must be a normal user-ID for the day-to-day work of an ordinary user.

All user-ID creation, deletion, and privilege change activity performed by systems administrators and others with privileged user-IDs must be securely logged and reflected in periodic management reports.

LOGGING–MANAGEMENT & TECHNICAL

Inclusion Of Security Relevant Events In System Logs – Computer systems handling sensitive, valuable, or critical information must securely log all significant security relevant events. Examples of security relevant events include: password guessing attempts, attempts to use privileges that have not been authorized, modifications to production application software, and modifications to system software.

Computer System Logs Must Support Audits – Logs of computer security relevant events must provide sufficient data to support comprehensive audits of the effectiveness of, and compliance with security measures.

Resistance Of Logs Against Deactivation, Modification, Or Deletion – Mechanisms to detect and record significant computer security events must be resistant to attacks. These attacks include attempts to deactivate, modify, or delete the logging software and/or the logs themselves.

Persons Authorized To View Logs – All system and application logs must be maintained in a form that cannot readily be viewed by unauthorized persons. A person is unauthorized if he or she is not a member of the internal audit staff, systems security staff, systems management staff, or if he or she does not clearly have a need for such access to perform regular duties. Unauthorized users must obtain written permission from the IT Committee prior to being granted such access.

Regular And Prompt Review Of System Logs – To allow proper remedial action, computer operations or information security staff must review records reflecting security relevant events on multi-user machines in a periodic and timely manner.

COMPUTER VIRUSES AND WORMS–MANAGERIAL & TECHNICAL

Virus Checking At Firewalls, Servers, And Desktop Machines – Virus screening software must be installed and enabled on all AnyBank firewalls, FTP servers, mail servers, intranet servers, and desktop machines.

COMPUTER OPERATIONS–MANAGERIAL & TECHNICAL

Computer Operator Logs Required For Multi-User Production Systems – All AnyBank multi-user production systems must have computer operator logs which show production system configuration changes, system errors and corrective actions taken.

Computer Operator Logs Must Be Periodically Reviewed – The IT Committee must regularly review the logs from all AnyBank multi-user production systems. These reviews are intended to ensure that operators are following established procedures and to identify problems in need of remedial action.

OVERALL DATA CONFIDENTIALITY POLICIES–MANAGERIAL & TECHNICAL

Presentation Of Low-Profile And Secure Image – AnyBank must at all times present a low profile and secure image to both the public and third parties.

Information about the existence and nature of significant assets must be accessible only to those persons with a demonstrable need-to-know.

RIGHT TO KNOW–MANAGERIAL & TECHNICAL

Disclosure Of Privacy Related Information Security Policies & Procedures – As a general rule, information security policies and procedures should be revealed only to AnyBank workers and selected outsiders (such as auditors) who have a legitimate business need for this information. A notable exception involves private data about individuals. In these cases, AnyBank has a duty to communicate the privacy related policies and procedures employed. In addition, AnyBank has a duty to disclose the existence of systems containing private information and the ways this information is used.

CONTINGENCY PLANNING–MANAGERIAL & TECHNICAL

Three Category Application Criticality Classification Scheme – All production computer applications must be placed into one of three criticality classifications, each with separate handling requirements: highly critical, required, and deferrable. This criticality classification system must be used throughout AnyBank, and must form an integral part of the system contingency planning process.

Preparation And Maintenance Of Computer Emergency Response Plans – For computer and communications systems, management must prepare, periodically update, and regularly test emergency response plans. These plans must provide for the continued operation of critical systems in the event of an interruption or degradation of service.

Organization/Maintenance Of Computer Emergency Response Team – Management must organize and maintain an in-house computer emergency response team (CERT) that will provide accelerated problem notification, damage control, and problem correction services in the event of computer related emergencies such as virus infestations, hacker break-ins, and the like.

Information Security Alert System – IT Committee management must establish, maintain, and periodically test a communications system allowing workers to promptly notify appropriate staff about suspected information security problems. These problems include computer virus infestations, hacker break-ins, and improper disclosure of internal information to outsiders, system service interruptions, and other events with serious information security implications.

Expected Employee Assistance During Business Restoration – Employees are expected to be present, and to assist to the best of their abilities, with the restoration of normal business activity after an emergency or a disaster disrupts AnyBank business activity. After an employee's family and personal assets are determined to be safe, employees are expected to put in overtime, work under stressful conditions, and otherwise do what it takes to maintain AnyBank as a going concern.

Preparation And Maintenance Of Computer Disaster Recovery Plans – Management must prepare, periodically update, and regularly test a disaster recovery plan that will allow all critical computer and communication systems to be available in the event of a major loss such as a flood, earthquake, or tornado.

Preparation And Maintenance Of Business Contingency Plans – Management must prepare, periodically update, and regularly test a business recovery plan. This recovery plan must specify how alternative facilities such as offices, furniture, telephones, and copiers will be provided so workers can continue operations in the event of either an emergency or a disaster.

Business And Computer Continuity Planning Process – A standard organization-wide process for developing and maintaining both business contingency plans and computer contingency plans must be documented and maintained by the IT Committee.

Reversion To Manual Procedures Where Cost-Effectively Possible – If AnyBank critical business activities could reasonably be performed (even for a short while) with manual procedures rather than computers, a manual computer contingency plan must be developed, tested, and periodically updated. In most circumstances, this contingency plan should be integrated into computer and communication system contingency plans.

Contact Numbers For IT Committee Staff – All members of the IT Committee who travel out of town must carry a cellular phone. These staff members must additionally provide both their manager and their group secretary with telephone numbers where they can be reached. These phone numbers must be provided in advance of the travel, and are required regardless of the reasons for travel.

BACKUP, ARCHIVAL STORAGE, AND DISPOSAL OF DATA– MANAGERIAL & TECHNICAL

Specification Of Backup Process And Frequency – Incremental backups for all end-user files must be performed by the system starting at 10:00PM each

business day. An exception to this will be each Friday (or if this is a holiday, the first business day thereafter) when a full backup of all files must be performed.

Off-Site Storage Of Backup Media – Backups of essential business information and software must be stored in an environmentally protected and access-controlled site that is a sufficient distance away from the originating facility to escape a local disaster.

FIREWALLS & EXTERNAL NETWORKS–MANAGEMENT & TECHNICAL

Internal Network Addresses Must Not Be Publicly Released – The internal system addresses, configurations, and related system design information for AnyBank networked computer systems must be restricted such that both systems and users outside AnyBank's internal network cannot access this information.

All Internet Web Servers Must Be Firewall Protected – All web servers accessible via the Internet must be protected by a router or firewall approved by the IT Committee.

Internet Commerce Servers Must Be In Demilitarized Zone (DMZ) – All Internet commerce servers including payment servers, database servers, and web servers must be protected by firewalls in a demilitarized zone.

Real-Time External Network Connections Require Firewalls – All in-bound real-time external connections to AnyBank internal networks and/or multi-user computer systems must pass through an additional access control point (aka a firewall, gateway, or access server) before users can reach a login banner.

Firewalls Must Run On Firewall Appliance – All firewalls used to protect AnyBank's internal network must run on approved Firewall Appliance.

Firewall Configuration Change Requires Information Security Approval – Firewall configuration rules and permissible service rules have been reached after an extended evaluation of costs and benefits. These rules must not be changed unless the permission of the IT Committee has first been obtained.

TRAINING AND AWARENESS–MANAGEMENT & TECHNICAL

Information Security Training For All Workers - All workers (employees, consultants, contractors, temporaries, etc.) should be provided with sufficient

training and supporting reference materials to allow them to properly protect AnyBank information resources.

Work According To Information Security Policies & Procedures – Every worker must understand AnyBank's policies and procedures about information security, and must agree in writing to perform his or her work according to such policies and procedures.

REPORTING OF SECURITY PROBLEMS–MANAGEMENT & TECHNICAL

Annual Analysis Of Information Security Violations & Problems – An annual analysis of reported information security problems and violations must be prepared by the IT Committee.

Issuance Of Cease And Desist Messages To Attackers – A stern cease and desist message must be sent to the source of all attacks mounted against AnyBank computers whenever the source or intermediate relay points can be identified.

HUMAN RESOURCES MATTERS–DISCIPLINE AND TERMINATION–MANAGEMENT & TECHNICAL

When To Prosecute Or Seek Restitution – To communicate that abusive and criminal behavior will not be tolerated; AnyBank management must seriously consider prosecution for all known violations of the law.

SECURITY ROLES–MANAGEMENT & TECHNICAL

Centralized Responsibility For Information Security – Guidance, direction, and authority for information security activities is centralized for the entire organization in the IT Committee.

Who Must Comply With Information Security Requirements – Outside consultants, contractors, and temporaries must be subject to the same information security requirements, and have the same information security responsibilities, as AnyBank employees.

Incident Management Responsibilities – To ensure a quick, effective, and orderly response to incidents, the individuals responsible for handling information systems security incidents must be clearly defined. These people are in turn responsible for defining procedures for handling incidents.

PHYSICAL SECURITY–MANAGEMENT & TECHNICAL

Computer Or Communications Systems In Locked Rooms – All network servers and communications equipment must be located in locked rooms to prevent tampering and unauthorized usage.

Propped-Open Doors To Network Room Requires Monitoring – Whenever doors to the network are propped-open (perhaps for moving computer equipment, furniture, supplies, or similar items), the entrance must be continuously monitored by an employee.

RESPONSIBILITY FOR INFORMATION SECURITY–MANAGEMENT & TECHNICAL

Information Security Management Responsibilities – An IT committee composed of Officers or their delegates will meet quarterly to: (a) review the current status of AnyBank's information security, (b) review and monitor security incidents within the Company, (c) approve and later review information security projects, (d) approve new or modified information security policies, and (e) perform other necessary high-level information security management activities.

Policy Accepted by Board: April 24, 2002
Secretary / Assistant Secretary: _____

ANYBANK COMPANY
RIGHT TO FINANCIAL PRIVACY POLICY AND PROCEDURES

Employees of AnyBank Company have a duty to protect the confidential nature of customers' financial records. Employees will not release customer financial information to any source other than a credit bureau without written authorization from the customer, a subpoena, summons, or warrant.

The Right to Financial Privacy Act (12 USC 3401, 12 CFR 219, 29 CFR 19, 31 CFR 14) establishes specific procedures for federal government authorities to follow when seeking customer records. Our employees will follow the procedures contained in this policy **when a federal agency requests customer financial information**. Under the privacy provisions of Illinois Banking Act (205 ILCS 5), AnyBank will not release any information to any other entity without prior authorization of the customer except as allowed by law.

APPLICABILITY

The act covers individuals or partnerships, if the partnership consists of five or fewer individuals. **Corporations or partnerships of six or more individuals are not covered by the act**. In addition, the act excludes access by state government agencies, state or local law enforcement officials, or private individuals.

REQUIREMENTS

To gain access to a customer's records, the act requires, with certain exceptions, that the federal government agency obtain one of the following:

- An authorization, signed and dated by the customer, which identifies the records being sought, the reasons the records are being requested, and the customer's rights under the Right to Financial Privacy Act (The agency's request should be on an official form and contain the required customer authorization.)
- An administrative subpoena or summons
- A search warrant
- A judicial subpoena

- A formal written request by a government agency (to be used only if no administrative summons or subpoena authority is available)

If we receive a request for information from a federal agency, we may not release the financial records of a customer until the federal government authority seeking the records certifies in writing that it has complied with the applicable provision of the Right to Financial Privacy Act. Documents will not be furnished to the federal agency for at least 14 days after a request is received.

RECORD RETENTION

We maintain a file of all federal government agency requests for customer records and copies of the furnished documents. The file contains the agency's official request, a summary of the information provided, the date provided, and the name of the employee providing the information. The act does not specify how long to keep copies. We keep copies for three years.

This file will contain all requests covered by the Right to Financial Privacy Act as well as requests from state and local governments and the Internal Revenue Service.

COST FOR PRODUCTION

The act permits charging the federal agency for labor and reproduction costs. The authorized labor rate (rounded to quarter hours) is $10 per hour and $.15 per copy. We will keep detailed records of the time it takes to produce documents for each request, subpoena, or summons. An itemized statement will be provided to the agency requesting the records.

EXCEPTIONS

Certain requests by federal agencies are exempt from the Right to Financial Privacy Act, as follows:

- Requests from federal law enforcement offices for information relevant to violations of the law or crimes

- Requests from a court or agency when perfecting a security interest, proving a claim in bankruptcy, or collecting a debt

- An agency's request for records that do not individually identify a particular customer

- A supervisory agency's request for records sought in connection with its supervisory, regulatory, or monetary function

- Specific reports required by federal statute or rules, such as the Home Mortgage Disclosure Act report

- Grand jury subpoenas

Exception to Notice Requirement But Where Certification Is Required

In certain instances, the act does not require a federal agency to provide a written notice to a customer if the agency requests financial information for the following purposes:

- Records incidental to a government loan, loan guaranty, loan insurance agreement, or default on a government-guaranteed or -insured loan

- Government-authorized foreign intelligence activities or the Secret Service conduct of protective functions

- Securities and Exchange Commission request with an order from a United States district court

In these instances, the federal government agency must provide written certification that it has met all requirements of the Right to Financial Privacy Act before we will release the requested information. The customer may examine these records.

CONDITION OF DOING BUSINESS

The act prohibits us from refusing to do business with a customer without the customer's prior authorization to disclose financial records. Therefore, this is not a condition of doing business with our Trust Company.

SUMMARY AND PROCEDURES

The Right to Financial Privacy Act establishes specific procedures for federal government authorities to follow when seeking customer financial records from financial institutions and imposes certain duties on institutions prior to releasing such information. In almost all instances, the federal agency must obtain written authorization from the customer or must serve us with a subpoena, summons, or warrant.

The federal agency must notify the customer that his or her records are being requested. We must receive written certification that the agency has complied with the act prior to our Trust Company releasing the information.

The Trust Company's employees who receive a release of financial records from any government agency or court will immediately notify a Senior Trust Officer.

Policy Accepted by Board: April 24, 2002.

Assistant Secretary: _____

APPENDIX B: CONFIGURATIONS

Firewall Configuration

```
PIX Version 6.1(1)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 FinancialNews security10
enable password ********** encrypted
passwd ********** encrypted
hostname AnyBankpix
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
fixup protocol skinny 2000
names
access-list Internet permit tcp any host 999.999.999.30 eq smtp
access-list Internet permit tcp any host 999.999.999.30 eq pop3
access-list FinancialNews permit ip host 10.10.10.52 28.13.16.0 255.255.255.0
access-list FinancialNews permit ip host 10.10.10.52 19.10.76.0 255.255.248.0
access-list FinancialNews permit ip host 10.10.10.52 5.83.24.0 255.255.255.0
access-list FinancialNews permit ip host 10.10.10.52 99.1.14.0 255.255.254.0
access-list nonat permit ip 10.0.0.0 255.0.0.0 192.168.200.0 255.255.255.0
pager lines 24
logging on
logging trap debugging
logging history debugging
logging host inside 10.10.10.124
logging host inside 10.10.10.64
interface ethernet0 auto
interface ethernet1 auto
interface ethernet2 auto
mtu outside 1500
mtu inside 1500
mtu FinancialNews 1500
ip address outside 999.999.999.18 255.255.255.240
ip address inside 10.10.10.125 255.255.255.128
ip address FinancialNews 10.10.10.129 255.255.255.128
ip audit info action alarm
ip audit attack action alarm
ip local pool vpnpool 192.168.200.1-192.168.200.100
pdm history enable
arp timeout 14400
global (outside) 1 999.999.999.19
global (FinancialNews) 1 10.10.10.131
```

```
nat (inside) 0 access-list nonat
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
static (inside,outside) 999.999.999.30 10.10.10.123 netmask 255.255.255.255 10 1 0
access-group Internet in interface outside
access-group FinancialNews in interface FinancialNews
route outside 0.0.0.0 0.0.0.0 999.999.999.17 1
route inside 10.165.1.0 255.255.255.0 10.10.10.1 1
route FinancialNews 19.10.76.0 255.255.248.0 10.10.10.130 1
route FinancialNews 99.1.14.0 255.255.254.0 10.10.10.130 1
route FinancialNews 5.83.24.0 255.255.255.0 10.10.10.130 1
route FinancialNews 28.13.16.0 255.255.255.0 10.10.10.130 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h323
0:05:00 si
p 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
url-server (inside) host 10.10.10.124 timeout 5 protocol TCP version 1
filter url http 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 allow
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
sysopt connection permit-ipsec
no sysopt route dnat
crypto ipsec transform-set strong esp-3des esp-md5-hmac
crypto dynamic-map strongmap 10 set transform-set strong
crypto map vpnmap 10 ipsec-isakmp dynamic strongmap
crypto map vpnmap interface outside
isakmp enable outside
isakmp identity address
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption 3des
isakmp policy 10 hash md5
isakmp policy 10 group 2
isakmp policy 10 lifetime 86400
vpngroup AnyBankVPN address-pool vpnpool
vpngroup AnyBankVPN dns-server 10.10.10.120
vpngroup AnyBankVPN default-domain anybank.local
vpngroup AnyBankVPN idle-time 1800
vpngroup AnyBankVPN password ********
telnet 10.10.10.124 255.255.255.255 inside
telnet 10.10.10.120 255.255.255.255 inside
telnet 10.10.10.64 255.255.255.255 inside
telnet timeout 15
ssh timeout 5
terminal width 80
Cryptochecksum:eeaeecdf2632033562070628faf7d62
```

Edge Router Configuration (before ACL modification)

```
version 12.0
service timestamps debug uptime
service timestamps log uptime
service password-encryption
!
hostname ab2600
!
enable secret 5 ******************
!
ip subnet-zero
no ip finger
ip domain-name anybank.com
ip name-server 1.17.16.6
ip name-server 2.12.17.2
!
interface FastEthernet0/0
 description AnyBank LAN
 ip address 999.999.999.17 255.255.255.240
 duplex auto
 speed auto
!
interface Serial0/0
 description T1 to Internet
 ip address 1.19.26.7 255.255.255.252
 ip access-group 101 in
 encapsulation ppp
 no ip mroute-cache
 service-module t1 remote-alarm-enable
!
interface FastEthernet0/1
 shutdown
 duplex auto
 speed auto
!
interface Serial0/1
 shutdown
!
ip classless
ip route 0.0.0.0 0.0.0.0 999.999.999.77
no ip http server
!
```

```
access-list 1 permit 192.168.1.7
access-list 101 deny   tcp any any eq telnet
access-list 101 permit ip any any
!
line con 0
 transport input none
line aux 0
line vty 0
 password 7 ******************
 login
line vty 1 2
 login
line vty 3 4
 password 7 ******************
 login
!
end
```

Edge Router Configuration (after ACL modification)

Changes noted in **BOLD**

```
version 12.0
service timestamps debug uptime
service timestamps log uptime
service password-encryption
!
hostname ab2600
!
enable secret 5 ******************
!
ip subnet-zero
no ip finger
ip domain-name anybank.com
ip name-server 1.17.16.6
ip name-server 2.12.17.2
!
interface FastEthernet0/0
 description AnyBank LAN
 ip address 999.999.999.17 255.255.255.240
 no ip directed-broadcast
 duplex auto
 speed auto
!
```

```
interface Serial0/0
 description T1 to Internet
 ip address 1.19.26.7 255.255.255.252
 ip access-group 101 in
 no ip redirects
 no ip unreachables
 no ip directed-broadcast
 encapsulation ppp
 no ip mroute-cache
 service-module t1 remote-alarm-enable
!
interface FastEthernet0/1
 shutdown
 duplex auto
 speed auto
!
interface Serial0/1
  shutdown
!
ip classless
ip route 0.0.0.0 0.0.0.0 999.999.999.77
no ip http server
!
access-list 1 permit 192.168.1.7
access-list 101 remark Deny traffic to this router.
access-list 101 deny   ip 10.0.0.0 0.255.255.255 any
access-list 101 deny   ip 127.0.0.0 0.255.255.255 any
access-list 101 deny   ip 172.16.0.0 0.15.255.255 any
access-list 101 deny   ip 192.168.0.0 0.0.255.255 any
access-list 101 deny   ip 224.0.0.0 15.255.255.255 any
access-list 101 deny   tcp any any range 135 139
access-list 101 deny   udp any any range 135 netbios-ss
access-list 101 deny   udp any any eq snmp
access-list 101 deny   tcp any any eq sunrpc
access-list 101 deny   udp any any eq sunrpc
access-list 101 deny   udp any any eq 445
access-list 101 deny   tcp any any eq 445
access-list 101 deny   tcp any any eq telnet
access-list 101 permit ip any any
!
line con 0
 transport input none
```

```
line aux 0
line vty 0
 password 7 ******************
 login
line vty 1 2
 login
line vty 3 4
 password 7 ******************
 login
!
end
```

APPENDIX C: SELECTED DATA SETS

Firewall Log Excerpt (Sanitized)

8/30/2002 14:43	Local4.Error	PIX.anybank.local	%PIX-3-106011: Deny inbound (No xlate) tcp src outside:66.163.172.132/80 dst outside:X.Y.Z.19/41524
8/30/2002 14:43	Local4.Error	PIX.anybank.local	%PIX-3-106011: Deny inbound (No xlate) tcp src outside:63.240.15.139/80 dst outside:X.Y.Z.19/41227
8/30/2002 14:43	Local4.Error	PIX.anybank.local	%PIX-3-106011: Deny inbound (No xlate) tcp src outside:63.240.15.139/80 dst outside:X.Y.Z.19/41259
8/30/2002 14:43	Local4.Error	PIX.anybank.local	%PIX-3-106011: Deny inbound (No xlate) tcp src outside:63.240.15.139/80 dst outside:X.Y.Z.19/41293
8/30/2002 14:43	Local4.Error	PIX.anybank.local	%PIX-3-106011: Deny inbound (No xlate) tcp src outside:63.240.15.139/80 dst outside:X.Y.Z.19/41336
8/30/2002 14:44	Local4.Error	PIX.anybank.local	%PIX-3-106011: Deny inbound (No xlate) tcp src outside:63.240.15.139/80 dst outside:X.Y.Z.19/41372
8/30/2002 14:44	Local4.Error	PIX.anybank.local	%PIX-3-106011: Deny inbound (No xlate) tcp src outside:207.68.178.253/80 dst outside:X.Y.Z.19/1443
8/30/2002 14:44	Local4.Error	PIX.anybank.local	%PIX-3-106011: Deny inbound (No xlate) tcp src outside:63.240.15.139/80 dst outside:X.Y.Z.19/41420
8/30/2002 14:44	Local4.Error	PIX.anybank.local	%PIX-3-106011: Deny inbound (No xlate) tcp src outside:207.68.178.253/80 dst outside:X.Y.Z.19/1453
8/30/2002 14:44	Local4.Error	PIX.anybank.local	%PIX-3-106011: Deny inbound (No xlate) tcp src outside:207.68.178.253/80 dst outside:X.Y.Z.19/1458
8/30/2002 14:44	Local4.Error	PIX.anybank.local	%PIX-3-106011: Deny inbound (No xlate) tcp src outside:63.240.15.139/80 dst outside:X.Y.Z.19/41042
8/30/2002 14:44	Local4.Error	PIX.anybank.local	%PIX-3-106011: Deny inbound (No xlate) tcp src outside:63.240.15.139/80 dst outside:X.Y.Z.19/41130
8/30/2002 14:44	Local4.Error	PIX.anybank.local	%PIX-3-106011: Deny inbound (No xlate) tcp src outside:63.240.15.139/80 dst outside:X.Y.Z.19/41202
8/30/2002 14:44	Local4.Error	PIX.anybank.local	%PIX-3-106011: Deny inbound (No xlate) tcp src outside:66.163.172.132/80 dst outside:X.Y.Z.19/41524
8/30/2002 14:44	Local4.Error	PIX.anybank.local	%PIX-3-106011: Deny inbound (No xlate) tcp src outside:63.240.15.139/80 dst outside:X.Y.Z.19/41245
8/30/2002 14:44	Local4.Error	PIX.anybank.local	%PIX-3-106011: Deny inbound (No xlate) tcp src outside:63.240.15.139/80 dst outside:X.Y.Z.19/41288
8/30/2002 14:44	Local4.Error	PIX.anybank.local	%PIX-3-106011: Deny inbound (No xlate) tcp src outside:63.240.15.139/80 dst outside:X.Y.Z.19/41320
8/30/2002 14:45	Local4.Error	PIX.anybank.local	%PIX-3-106011: Deny inbound (No xlate) tcp src outside:63.240.15.139/80 dst outside:X.Y.Z.19/41345
8/30/2002 14:45	Local4.Error	PIX.anybank.local	%PIX-3-106011: Deny inbound (No xlate) tcp src outside:63.240.15.139/80 dst outside:X.Y.Z.19/41393
8/30/2002 14:45	Local4.Error	PIX.anybank.local	%PIX-3-106011: Deny inbound (No xlate) tcp src outside:63.240.15.139/80 dst outside:X.Y.Z.19/41443

Table 33 Firewall Log Excerpt (Sanitized)

NOTE: This is an extract of the PIX log files used in the data analysis. The organizational IP addresses were changed to X.Y.Z.number and the PIX identifier was changed to anybank. This was done in order to protect the organization from external security breaches based on this study.

Source Country by IP Address

Country	May-02	Jun-02	Jul-02	Aug-02	Sep-02	Oct-02	Nov-02	Total	%	Non-USA %
United States	12077	14298	11119	19729	20827	16808	9236	104094	89.7%	
Canada	296	505	364	644	943	913	389	4054	3.5%	33.8%
Japan	106	140	226	517	136	186	115	1426	1.2%	11.9%
Australia	10	13	35	45	13	125	463	704	0.6%	5.9%
Private Addresses	205	215	152	129	3	0	0	704	0.6%	5.9%
South Korea	86	117	141	51	74	84	115	668	0.6%	5.6%
Germany	57	67	118	124	47	125	88	626	0.5%	5.2%
Taiwan	37	53	135	66	35	31	57	414	0.4%	3.5%
Argentina	85	24	39	21	16	24	54	263	0.2%	2.2%
Hong Kong	61	7	35	20	24	46	30	223	0.2%	1.9%
Ireland	1	108	61	10	2	19	10	211	0.2%	1.8%
Egypt	10	20	33	25	24	32	52	196	0.2%	1.6%
Sri Lanka	22	27	16	26	49	37	19	196	0.2%	1.6%
China	24	36	39	23	7	27	26	182	0.2%	1.5%
Russian Federation	23	5	88	6	5	43	5	175	0.2%	1.5%
Turkey	14	43	26	8	36	22	14	163	0.1%	1.4%
Papua New Guinea	10	30	25	33	21	26	12	157	0.1%	1.3%
United Kingdom	12	33	37	27	11	17	13	150	0.1%	1.3%
Mexico	35	16	8	19	10	34	12	134	0.1%	1.1%
Chile	4	12	28	7	37	21	22	131	0.1%	1.1%
Norway	23	19	9	19	17	7	17	111	0.1%	0.9%
Italy	11	20	9	8	20	16	7	91	0.1%	0.8%
Malaysia	12	18	24	11	10	3	13	91	0.1%	0.8%
Singapore	20	6	25	7	8	10	5	81	0.1%	0.7%
Denmark	3	15	13	9	11	18	7	76	0.1%	0.6%
France	3	9	8	6	23	10	14	73	0.1%	0.6%
India	3	20	17	0	6	8	13	67	0.1%	0.6%
Switzerland	0	5	6	2	10	14	29	66	0.1%	0.6%
Belgium	4	6	6	10	0	16	16	58	0.0%	0.5%
Great Britain (UK)	18	4	3	12	6	0	6	49	0.0%	0.4%
Netherlands	3	13	6	3	4	0	14	43	0.0%	0.4%
Sweden	0	5	8	4	7	18	0	42	0.0%	0.4%
Finland	2	2	0	11	14	4	8	41	0.0%	0.3%
Iran	6	6	3	9	0	0	4	28	0.0%	0.2%
Saudi Arabia	0	8	3	0	6	0	11	28	0.0%	0.2%
New Zealand	3	6	2	0	12	2	0	25	0.0%	0.2%
South Africa	6	11	6	0	0	0	1	24	0.0%	0.2%
Poland	0	0	0	0	0	2	19	21	0.0%	0.2%
Austria	0	0	3	0	0	4	10	17	0.0%	0.1%
Barbados	0	0	0	6	8	0	3	17	0.0%	0.1%
Thailand	10	1	3	3	0	0	0	17	0.0%	0.1%
Colombia	0	3	2	1	0	4	2	12	0.0%	0.1%
Spain	0	3	0	3	6	0	0	12	0.0%	0.1%
Guatemala	0	0	8	0	0	0	0	8	0.0%	0.1%
Philippines	0	2	0	6	0	0	0	8	0.0%	0.1%
Greece	0	0	7	0	0	0	0	7	0.0%	0.1%
Venezuela	3	0	0	1	3	0	0	7	0.0%	0.1%
Bolivia	0	0	0	0	0	0	6	6	0.0%	0.1%
Luxembourg	0	6	0	0	0	0	0	6	0.0%	0.1%
Puerto Rico	0	0	0	0	0	0	6	6	0.0%	0.1%
El Salvador	0	0	0	0	0	0	6	6	0.0%	0.1%
Kuwait	3	0	0	0	2	0	0	5	0.0%	0.0%

Country	May-02	Jun-02	Jul-02	Aug-02	Sep-02	Oct-02	Nov-02	Total	%	Non-USA %
Viet Nam	2	0	3	0	0	0	0	5	0.0%	0.0%
United Arab Emirates	0	4	0	0	0	0	0	4	0.0%	0.0%
Costa Rica	0	0	0	0	4	0	0	4	0.0%	0.0%
Estonia	0	1	3	0	0	0	0	4	0.0%	0.0%
Peru	0	0	2	0	0	0	2	4	0.0%	0.0%
Romania	0	0	0	0	4	0	0	4	0.0%	0.0%
Tunisia	0	0	0	0	0	0	4	4	0.0%	0.0%
Brazil	0	0	0	3	0	0	0	3	0.0%	0.0%
Cyprus	0	0	3	0	0	0	0	3	0.0%	0.0%
Lithuania	0	0	0	0	0	3	0	3	0.0%	0.0%
Haiti	0	0	2	0	0	0	0	2	0.0%	0.0%
Indonesia	0	2	0	0	0	0	0	2	0.0%	0.0%
Israel	0	0	2	0	0	0	0	2	0.0%	0.0%
Slovenia	0	0	0	0	0	0	2	2	0.0%	0.0%
Slovak Republic	0	0	0	2	0	0	0	2	0.0%	0.0%
Ukraine	0	0	0	2	0	0	0	2	0.0%	0.0%
Hungary	0	0	0	0	0	1	0	1	0.0%	0.0%
Totals	**13310**	**15964**	**12911**	**21668**	**22501**	**18756**	**10957**	**116071**		
Totals (non-USA)	**1233**	**1666**	**1792**	**1939**	**1674**	**1952**	**1721**	**11977**		
Non-USA %	**9.3%**	**10.4%**	**13.9%**	**8.9%**	**7.4%**	**10.4%**	**15.7%**	**10.3%**		

Traffic by Destination Port (IP)

Port	TCP/UDP Ports Description	May-02	Jun-02	Jul-02	Aug-02	Sep-02	Oct-02	Nov-02	Total	Percentage
	All Ports Total Monthly Frames	**13310**	**15964**	**12911**	**21668**	**22501**	**18760**	**10957**	**116071**	**100.00%**
ICMP	Internet Control Message Protocol	2833	911	1869	2548	479	910	1822	14434	12.44%
137	NETBIOS Name Service	2890	4186	1484	2092	246	0	0	10898	9.39%
80	World Wide Web HTTP	2141	936	1059	1307	1085	1220	977	8725	7.52%
113	Authentication Service	1216	1098	644	1557	883	842	931	7171	6.18%
6970	GateCrasher	280	962	977	793	155	108	0	3275	2.82%
1433	Microsoft-SQL-Server	384	563	513	391	318	332	367	2868	2.47%
37628	Undetermined	0	2524	0	0	0	0	0	2524	2.17%
21	File Transfer Protocol [Control]	171	184	172	157	130	116	157	1087	0.94%
53	Domain Name Server	19	29	46	18	202	174	343	831	0.72%
3024	WinCrash	809	0	1	1	0	0	0	811	0.70%
139	NETBIOS Session Service	197	162	158	227	23	0	0	767	0.66%
27374	Sub-7 2.1	84	69	291	92	41	69	100	746	0.64%
33435	Undetermined	0	0	0	0	0	97	442	539	0.46%
22	SSH Remote Login Protocol	37	36	54	54	35	34	24	274	0.24%
443	https MCom	3	0	0	0	43	84	99	229	0.20%
1080	Socks	11	23	16	27	27	46	42	192	0.17%
25	Simple Mail Transfer	13	13	18	14	23	30	29	140	0.12%
111	SUN Remote Procedure Call	16	18	26	8	0	0	0	68	0.06%
8080	Standard HTTP Proxy	11	2	6	8	15	14	7	63	0.05%
17300	Kuang2 Trojan	0	0	19	40	0	0	4	63	0.05%
37852	Undetermined	7	8	4	15	2	2	23	61	0.05%
515	spooler	1	8	17	11	0	8	10	55	0.05%
12416	Undetermined	0	0	0	0	0	2	50	52	0.04%
5664	Undetermined	0	0	0	0	0	0	50	50	0.04%
27795	Undetermined	0	0	0	0	0	50	0	50	0.04%
8167	Undetermined	0	17	0	0	7	12	0	36	0.03%
63774	Undetermined	0	0	0	9	12	0	12	33	0.03%
63875	Undetermined	0	0	0	12	7	0	12	31	0.03%
3128	Squid Proxy/SubSeven	4	3	0	9	0	12	3	31	0.03%
4590	ICQ Trojan Horse	0	0	0	8	22	0	0	30	0.03%
37630	Undetermined	0	0	0	0	0	23	6	29	0.02%
64346	Undetermined	0	0	0	0	29	0	0	29	0.02%
37097	Undetermined	0	0	0	0	17	12	0	29	0.02%
1243	SubSeven	0	0	2	1	0	0	26	29	0.02%
63992	Undetermined	0	0	0	0	16	0	12	28	0.02%
23	Telnet	9	8	4	7	0	0	0	28	0.02%
54769	Undetermined	0	0	0	0	15	12	0	27	0.02%

Port	TCP/UDP Ports Description	May-02	Jun-02	Jul-02	Aug-02	Sep-02	Oct-02	Nov-02	Total	Percentage
23550	Undetermined	25	0	0	0	0	2	0	27	0.02%
10234	Undetermined	0	0	0	0	14	12	0	26	0.02%
8240	Undetermined	0	0	0	0	13	0	13	26	0.02%
15371	Undetermined	0	0	0	0	25	0	0	25	0.02%
37108	Undetermined	0	0	0	0	25	0	0	25	0.02%
54685	Undetermined	0	0	0	0	25	0	0	25	0.02%
54708	Undetermined	0	0	0	0	25	0	0	25	0.02%
54755	Undetermined	0	0	0	0	25	0	0	25	0.02%
24519	Undetermined	0	0	0	12	13	0	0	25	0.02%
59932	Undetermined	0	0	0	0	24	0	0	24	0.02%
59946	Undetermined	0	0	0	0	24	0	0	24	0.02%
60880	Undetermined	0	0	0	0	24	0	0	24	0.02%
61928	Undetermined	0	0	0	0	24	0	0	24	0.02%
62882	Undetermined	0	0	0	0	24	0	0	24	0.02%
63702	Undetermined	0	0	0	0	24	0	0	24	0.02%
58147	Undetermined	0	0	0	0	23	1	0	24	0.02%
7984	Undetermined	0	0	0	0	13	11	0	24	0.02%
63760	Undetermined	0	0	0	0	12	0	12	24	0.02%
1524	ingres	0	7	7	2	1	7	0	24	0.02%
6112	dtspcd	0	4	5	6	3	0	2	20	0.02%
8000	iRDMI/Shoutcast Server	1	0	0	3	9	3	0	16	0.01%
4447	N1-RMGMT	0	0	0	2	0	13	0	15	0.01%
1534	micromuse-lm	0	0	1	1	1	12	0	15	0.01%
1386	CheckSum lic mgr	2	1	2	2	7	0	0	14	0.01%
8893	Desktop Data TCP 5: NewsEDGE	0	0	0	0	13	0	0	13	0.01%
6143	Watershed lic mgr	0	0	0	0	0	12	0	12	0.01%
1345	VPJP	1	8	1	0	2	0	0	12	0.01%
6672	vision_server	0	0	0	0	0	12	0	12	0.01%
1799	NETRISK	11	0	0	0	0	1	0	12	0.01%
6147	Montage lic mgr	0	0	0	0	0	12	0	12	0.01%
445	Microsoft-DS	0	0	0	12	0	0	0	12	0.01%
7201	DLIP	0	0	0	0	0	12	0	12	0.01%
1428	Informatik lic mgr	0	7	1	0	2	1	0	11	0.01%
1998	cisco X.25 service (XOT)	0	0	1	0	0	3	7	11	0.01%
1434	Microsoft-SQL-Monitor	0	1	2	2	1	4	0	10	0.01%
1528	micautoreg	0	0	1	0	0	9	0	10	0.01%
1611	Inter Library Loan	0	0	1	1	1	0	7	10	0.01%
2065	Data Link Switch Read Port Num	0	0	2	7	0	1	0	10	0.01%
2140	The Invasor Nikhil G.	0	1	0	0	7	1	0	9	0.01%

Port	TCP/UDP Ports Description	May-02	Jun-02	Jul-02	Aug-02	Sep-02	Oct-02	Nov-02	Total	Percentage
1486	nms_topo_serv	0	1	4	0	2	2	0	9	0.01%
1482	Miteksys lic mgr	0	1	0	0	0	1	7	9	0.01%
1640	cert-responder	0	0	1	0	0	1	7	9	0.01%
1381	Apple Network lic mgr	0	0	0	1	7	1	0	9	0.01%
1536	ampr-inter	0	0	0	1	0	8	0	9	0.01%
6912	Shitheep	0	0	0	0	8	0	0	8	0.01%
8888	NewsEDGE server TCP (TCP 1)	1	0	2	0	5	0	0	8	0.01%
9989	iNi-Killer	0	0	0	0	0	0	8	8	0.01%
1359	FTSRV	0	0	7	0	1	0	0	8	0.01%
1508	diagmond	0	0	0	0	0	8	0	8	0.01%
1506	Universal Time daemon (utcd)	0	1	1	1	2	2	0	7	0.01%
1599	simbaservices	0	1	1	2	1	2	0	7	0.01%
1693	rrirtr	2	0	1	1	2	1	0	7	0.01%
1603	pickodbc	0	1	2	1	2	1	0	7	0.01%
9993	Palace	0	0	0	0	7	0	0	7	0.01%
9996	Palace	0	0	0	0	7	0	0	7	0.01%
1394	Network Log Client	0	3	2	2	0	0	0	7	0.01%
1493	netmap_lm	0	1	3	1	2	0	0	7	0.01%
2286	NAS-Metering	0	0	3	2	1	1	0	7	0.01%
50766	Fore	0	0	0	0	0	7	0	7	0.01%
1689	firefox	0	1	2	2	1	1	0	7	0.01%
1560	asci-val	0	1	2	2	0	2	0	7	0.01%
1546	abbaccuray	0	1	2	2	1	1	0	7	0.01%
1716	xmsg	0	1	3	0	0	2	0	6	0.01%
1462	World lic mgr	0	0	3	1	2	0	0	6	0.01%
1565	WinDD	0	0	2	1	0	3	0	6	0.01%
12345	Win95/NT Netbus backdoor	0	0	6	0	0	0	0	6	0.01%
1457	Valisys lic mgr	0	1	2	1	1	1	0	6	0.01%
1580	tn-tl-r1	0	0	1	3	1	1	0	6	0.01%
1170	Streaming Audio Trojan	0	0	0	2	3	1	0	6	0.01%
1911	Starlight Networks Multimedia	0	0	4	0	2	0	0	6	0.01%
1681	sd-elmd	0	1	4	0	0	1	0	6	0.01%
1813	RADIUS Accounting	0	1	0	1	4	0	0	6	0.01%
1552	pciarray	0	0	2	0	4	0	0	6	0.01%
5631	pcANYWHEREdata	0	0	6	0	0	0	0	6	0.01%
1529	oracle	0	0	2	1	1	2	0	6	0.01%
1388	Objective Solutions DB Cache	0	1	2	3	0	0	0	6	0.01%
1688	nsjtp-data	0	1	0	3	0	2	0	6	0.01%
1458	Nichols Research Corp.	0	2	1	2	1	0	0	6	0.01%

Port	TCP/UDP Ports Description	May-02	Jun-02	Jul-02	Aug-02	Sep-02	Oct-02	Nov-02	Total	Percentage
1364	Network DataMover Server	2	0	0	1	1	2	0	6	0.01%
1907	IntraSTAR	0	1	0	3	0	2	0	6	0.01%
1379	Integrity Solutions	0	0	1	0	0	5	0	6	0.01%
1404	Infinite Graphics lic mgr	0	1	3	1	0	1	0	6	0.01%
2239	Image Query	0	0	3	0	1	2	0	6	0.01%
1494	ica	0	0	0	0	0	6	0	6	0.01%
1715	houdini-lm	0	0	0	5	1	0	0	6	0.01%
1909	Global World Link	0	0	0	6	0	0	0	6	0.01%
1620	faxportwinport	0	0	3	1	2	0	0	6	0.01%
1455	ESL lic mgr	0	1	2	1	0	2	0	6	0.01%
1488	DocStor	0	2	1	2	1	0	0	6	0.01%
9000	CSlistener	0	0	6	0	0	0	0	6	0.01%
1566	CORELVIDEO	0	1	1	1	0	3	0	6	0.01%
1400	Cadkey Tablet Daemon	0	0	1	1	2	2	0	6	0.01%
1375	Bytex	0	0	2	1	1	2	0	6	0.01%
1422	Autodesk lic mgr	0	1	1	1	1	2	0	6	0.01%
5305	# HA Cluster Test	0	0	0	0	0	6	0	6	0.01%
1946	tekpls	0	1	1	1	2	0	0	5	0.00%
1733	sipat	0	2	2	0	0	1	0	5	0.00%
3143	Sea View	0	2	0	0	1	2	0	5	0.00%
1698	RSVP-ENCAPSULATION-1	0	1	0	1	1	2	0	5	0.00%
1541	rds2	0	0	1	1	0	3	0	5	0.00%
1735	PrivateChat	0	1	0	0	4	0	0	5	0.00%
1395	PC Workstation mgr software	0	2	1	0	0	2	0	5	0.00%
1571	Oracle Remote Data Base	0	1	1	2	0	1	0	5	0.00%
1025	network blackjack	0	0	0	0	4	1	0	5	0.00%
1664	netview-aix-4	0	1	3	0	0	1	0	5	0.00%
2592	netrek	0	0	1	1	0	3	0	5	0.00%
2288	NETML	3	0	1	0	1	0	0	5	0.00%
1683	ncpm-hip	0	0	0	2	0	3	0	5	0.00%
1731	MSICCP	0	0	1	1	0	3	0	5	0.00%
1680	microcom-sbp	0	0	3	1	0	1	0	5	0.00%
1682	lanyon-lantern	0	0	1	1	2	1	0	5	0.00%
1706	jetform	0	0	1	2	1	1	0	5	0.00%
2233	INFOCRYPT	0	0	2	1	1	1	0	5	0.00%
1725	iden-ralp	0	0	3	1	1	0	0	5	0.00%
1746	ftrapid-1	0	1	0	1	1	2	0	5	0.00%
1561	facilityview	0	0	4	0	0	1	0	5	0.00%
2287	DNA	0	0	1	1	0	3	0	5	0.00%

Port	TCP/UDP Ports Description	May-02	Jun-02	Jul-02	Aug-02	Sep-02	Oct-02	Nov-02	Total	Percentage
1471	csdmbase	0	0	1	2	2	0	0	5	0.00%
1991	cisco STUN Priority 2 port	0	0	1	2	1	1	0	5	0.00%
1997	cisco Gateway Discovery Prot	0	0	2	1	2	0	0	5	0.00%
1721	caicci	0	1	2	0	0	2	0	5	0.00%
1769	bmc-net-adm	1	0	1	0	1	1	1	5	0.00%
1346	Alta Analytics lic mgr	0	1	0	0	0	4	0	5	0.00%
2222	Allen-Bradley unregistered port	0	1	1	2	1	0	0	5	0.00%
1481	AIRS	0	1	0	2	2	0	0	5	0.00%
2583	Wincrash V2.0 trojan	0	0	2	1	0	1	0	4	0.00%
1498	Watcom-SQL	0	1	2	0	0	1	0	4	0.00%
1589	VQP	0	0	1	0	1	2	0	4	0.00%
1516	Virtual Places Audio data	0	0	1	1	2	0	0	4	0.00%
1398	Video Active Mail	0	1	0	2	1	0	0	4	0.00%
1771	vaultbase	0	0	0	2	1	1	0	4	0.00%
1737	ultimad	0	1	1	0	2	0	0	4	0.00%
1588	triquest-lm	0	1	0	0	0	3	0	4	0.00%
1420	Timbuktu Service 4 Port	0	1	0	1	2	0	0	4	0.00%
1418	Timbuktu Service 2 Port	0	0	1	1	1	1	0	4	0.00%
1758	tftp-mcast	0	1	2	1	0	0	0	4	0.00%
1047	Sun's NEO Object Request Broker	0	0	0	1	3	0	0	4	0.00%
1607	stt	0	1	0	1	0	2	0	4	0.00%
1543	simba-cs	0	0	1	2	1	0	0	4	0.00%
1714	sesi-lm	0	0	0	2	0	2	0	4	0.00%
1436	Satellite-data Acquisition System 2	0	0	0	3	1	0	0	4	0.00%
1696	rrifmm	0	0	1	0	2	1	0	4	0.00%
1522	Ricardo North America lic mgr	0	1	2	1	0	0	0	4	0.00%
2501	Resource Tracking system client	0	2	0	1	0	1	0	4	0.00%
1353	Relief Consulting	0	0	1	3	0	0	0	4	0.00%
1540	rds	2	0	1	0	1	0	0	4	0.00%
1531	rap-listen	0	0	2	1	0	1	0	4	0.00%
1445	Proxima lic mgr	0	0	2	1	1	0	0	4	0.00%
1403	Prospero Resource mgr	0	0	3	0	0	1	0	4	0.00%
1526	Prospero Data Access Prot	0	0	1	3	0	0	0	4	0.00%
1723	pptp	0	0	2	1	0	1	0	4	0.00%
1916	Persoft Persona	0	2	0	0	1	1	0	4	0.00%
1449	PEport	0	1	0	0	2	0	1	4	0.00%
1480	PacerForum	0	0	1	1	1	1	0	4	0.00%
1384	Objective Solutions Lic Mgr	0	1	2	0	0	1	0	4	0.00%
1617	Nimrod Inter-Agent Communication	0	0	2	2	0	0	0	4	0.00%

Port	TCP/UDP Ports Description	May-02	Jun-02	Jul-02	Aug-02	Sep-02	Oct-02	Nov-02	Total	Percentage
1666	netview-aix-6	0	1	1	0	0	1	1	4	0.00%
1676	netcomm1	0	0	1	1	2	0	0	4	0.00%
138	NETBIOS Datagram Service	0	0	0	0	0	4	0	4	0.00%
1574	mvel-lm	0	1	1	2	0	0	0	4	0.00%
1123	Murray	0	0	0	3	0	1	0	4	0.00%
1755	ms-streaming	0	1	0	2	0	1	0	4	0.00%
1700	mps-raft	0	0	1	1	0	2	0	4	0.00%
1801	Microsoft Message Que	0	0	2	0	0	2	0	4	0.00%
1824	metrics-pas	0	1	0	0	2	1	0	4	0.00%
1555	livelan	0	0	0	2	1	1	0	4	0.00%
2213	Kali	0	0	2	1	0	1	0	4	0.00%
1567	jlicelmd	0	0	1	2	1	0	0	4	0.00%
1949	ISMA Easdaq Live	0	0	0	2	1	1	0	4	0.00%
2042	isis	0	0	2	0	1	1	0	4	0.00%
1641	InVision	0	0	1	2	1	0	0	4	0.00%
1490	insitu-conf	0	1	1	0	0	2	0	4	0.00%
1412	InnoSys	0	0	3	0	0	1	0	4	0.00%
1586	ibm-abtact	0	0	1	2	0	1	0	4	0.00%
1376	IBM Person to Person Software	0	0	3	0	1	0	0	4	0.00%
1803	HP-HCIP-GWY	0	0	0	0	2	2	0	4	0.00%
1409	Here lic mgr	0	0	3	0	1	0	0	4	0.00%
1720	h323hostcall	0	1	0	2	0	1	0	4	0.00%
1383	GW Hannaway Network Lic Mgr	0	1	0	0	3	0	0	4	0.00%
1542	gridgen-elmd	0	1	2	0	1	0	0	4	0.00%
1453	Genie lic mgr	0	0	1	2	1	0	0	4	0.00%
1786	funk-logger	0	0	0	1	1	2	0	4	0.00%
1514	Fujitsu Systems Business of USA	0	0	0	2	2	0	0	4	0.00%
1513	Fujitsu Systems Business of USA	0	0	3	1	0	0	0	4	0.00%
1807	Fujitsu Hot Standby Protocol	0	0	0	1	3	0	0	4	0.00%
1371	Fujitsu Config Protocol	0	0	2	2	0	0	0	4	0.00%
1985	Folio Remote Server	0	0	0	1	1	2	0	4	0.00%
1717	fj-hdnet	0	1	0	2	1	0	0	4	0.00%
4567	FileNail Danny	0	0	3	1	0	0	0	4	0.00%
1798	Event Transfer Protocol	1	1	1	0	1	0	0	4	0.00%
1772	EssWeb Gateway	0	0	2	2	0	0	0	4	0.00%
1691	empire-empuma	0	0	1	1	1	1	0	4	0.00%
1357	Electronic PegBoard	0	0	1	2	1	0	0	4	0.00%
1440	Eicon Service Location Protocol	0	1	1	0	1	1	0	4	0.00%
1438	Eicon Security Agent/Server	0	2	1	1	0	0	0	4	0.00%

Port	TCP/UDP Ports Description	May-02	Jun-02	Jul-02	Aug-02	Sep-02	Oct-02	Nov-02	Total	Percentage
1945	dialogic-elmd	0	0	1	3	0	0	0	4	0.00%
1456	DCA	0	1	2	0	1	0	0	4	0.00%
1467	CSDMBASE	0	2	0	1	1	0	0	4	0.00%
1484	Confluent lic mgr	0	0	2	1	1	0	0	4	0.00%
1741	cisco-net-mgmt	0	0	1	2	0	1	0	4	0.00%
1992	cisco STUN Priority 3 port	0	0	1	1	0	2	0	4	0.00%
1766	cft-5	0	0	0	2	0	2	0	4	0.00%
1756	capfast-lmd	0	1	0	0	2	1	0	4	0.00%
1563	Cadabra lic mgr	0	0	2	1	1	0	0	4	0.00%
1636	CableNet Control Protocol	0	0	1	1	0	2	0	4	0.00%
1031	BBN IAD	0	1	0	0	3	0	0	4	0.00%
1544	aspeclmd	0	0	2	1	1	0	0	4	0.00%
1557	ArborText lic mgr	0	0	2	1	0	0	1	4	0.00%
1491	anynetgateway	0	2	0	0	1	1	0	4	0.00%
2223	Allen-Bradley unregistered port	0	0	0	0	1	3	0	4	0.00%
1742	3Com-nsd	0	0	1	1	0	2	0	4	0.00%
2279	xmquery	0	0	0	1	0	2	0	3	0.00%
1559	web2host	0	1	0	1	1	0	0	3	0.00%
1581	vmf-msg-port	0	0	0	1	0	2	0	3	0.00%
1500	VLSI lic mgr	0	1	1	0	1	0	0	3	0.00%
1545	vistium-share	0	0	1	1	1	0	0	3	0.00%
1519	Virtual Places Video control	0	1	0	1	1	0	0	3	0.00%
1517	Virtual Places Audio control	0	1	0	1	0	1	0	3	0.00%
4445	UPNOTIFYP	0	0	1	1	1	0	0	3	0.00%
1823	Unisys Natural Language Lic Mgr	0	0	2	0	1	0	0	3	0.00%
1568	tsspmap	0	0	2	1	0	0	0	3	0.00%
2700	tqdata	0	0	1	1	1	0	0	3	0.00%
1584	tn-tl-fd2	0	0	0	0	1	2	0	3	0.00%
1380	Telesis Network lic mgr	0	0	2	0	1	0	0	3	0.00%
1390	Storage Controller	0	0	1	1	0	1	0	3	0.00%
1759	SPSS lic mgr	0	0	1	1	1	0	0	3	0.00%
1207	SoftWar	0	0	0	1	1	1	0	3	0.00%
1621	softdataphone	0	0	0	0	2	1	0	3	0.00%
1594	sixtrak	0	0	1	0	1	1	0	3	0.00%
3048	Sierra Net PC Trader	0	0	0	0	1	2	0	3	0.00%
1368	ScreenCast	0	1	0	2	0	0	0	3	0.00%
1811	Scientia-SDB	0	0	0	1	1	1	0	3	0.00%
1501	Satellite-data Acquisition System 3	0	0	2	0	1	0	0	3	0.00%
1646	sa-msg-port	0	0	0	1	0	2	0	3	0.00%

Port	TCP/UDP Ports Description	May-02	Jun-02	Jul-02	Aug-02	Sep-02	Oct-02	Nov-02	Total	Percentage
1745	remote-winsock	0	2	0	0	1	0	0	3	0.00%
3142	RDC WH EOS	0	0	1	1	0	1	0	3	0.00%
1587	pra_elmd	0	0	1	2	0	0	0	3	0.00%
1465	Pipes Platform	0	1	1	0	0	1	0	3	0.00%
2787	piccolo - Cornerstone Software	0	0	0	1	1	0	1	3	0.00%
1575	oraclenames	0	0	1	2	0	0	0	3	0.00%
1525	oracle	0	0	1	1	0	1	0	3	0.00%
2237	Optech Port1 lic mgr	0	0	0	1	1	1	0	3	0.00%
1473	OpenMath	0	0	0	1	2	0	0	3	0.00%
1622	ontime	0	0	2	0	1	0	0	3	0.00%
1463	Nucleus	0	0	0	3	0	0	0	3	0.00%
4454	NSS Agent mgr	0	0	1	1	0	1	0	3	0.00%
1687	nsjtp-ctrl	0	0	0	2	0	1	0	3	0.00%
4134	NIFTY-Serve HMI protocol	0	0	2	0	0	1	0	3	0.00%
1365	Network Software Associates	0	0	1	0	1	1	0	3	0.00%
1155	Network File Access	0	0	0	0	2	1	0	3	0.00%
1669	netview-aix-9	0	1	0	0	2	0	0	3	0.00%
1665	netview-aix-5	0	1	0	1	0	0	1	3	0.00%
1406	NetLabs lic mgr	0	0	2	0	0	1	0	3	0.00%
4008	NetCheque accounting	0	0	0	0	2	1	0	3	0.00%
1616	NetBill Product Server	0	1	0	2	0	0	0	3	0.00%
1521	nCube lic mgr	0	0	1	0	1	1	0	3	0.00%
1591	ncpm-pm	0	0	1	1	0	1	0	3	0.00%
1744	ncpm-ft	0	1	0	2	0	0	0	3	0.00%
1790	Narrative Media Streaming Protocol	0	0	1	2	0	0	0	3	0.00%
1477	ms-sna-server	0	0	1	0	1	1	0	3	0.00%
1532	miroconnect	0	0	0	1	1	1	0	3	0.00%
1360	MIMER	0	0	1	0	0	2	0	3	0.00%
1510	Midland Valley Exploration Ltd. Lic. Man.	0	0	2	1	0	0	0	3	0.00%
2789	Media Agent	0	0	1	0	1	1	0	3	0.00%
1269	Maverick's Matrix	0	0	0	2	0	1	0	3	0.00%
3985	MAPPER TCP/IP server	0	0	3	0	0	0	0	3	0.00%
2908	mao	0	0	0	1	1	1	0	3	0.00%
1752	Leap of Faith Research Lic Mgr	0	0	1	1	1	0	0	3	0.00%
1578	Jacobus lic mgr	0	0	0	1	0	2	0	3	0.00%
2241	IVS Daemon	0	1	1	0	1	0	0	3	0.00%
1539	Intellistor lic mgr	0	0	1	0	1	1	0	3	0.00%
1443	Integrated Engineering Software	0	0	2	1	0	0	0	3	0.00%
1550	Image Storage lic mgr 3M Comp	0	1	1	1	0	0	0	3	0.00%

Port	TCP/UDP Ports Description	May-02	Jun-02	Jul-02	Aug-02	Sep-02	Oct-02	Nov-02	Total	Percentage
1515	ifor-protocol	0	0	1	1	1	0	0	3	0.00%
1430	Hypercom TPDU	0	0	1	2	0	0	0	3	0.00%
1424	Hybrid Encryption Protocol	0	0	2	0	1	0	0	3	0.00%
1789	hello	0	0	1	0	1	1	0	3	0.00%
3000	HBCI	0	0	2	0	1	0	0	3	0.00%
1590	gemini-lm	0	0	2	0	0	1	0	3	0.00%
1421	Gandalf lic mgr	0	0	3	0	0	0	0	3	0.00%
1505	Funk Software	0	0	1	2	0	0	0	3	0.00%
1657	fujitsu-mmpdc	0	0	2	0	0	1	0	3	0.00%
1904	Fujitsu ICL Term Emulator Prog C	0	0	1	1	0	0	1	3	0.00%
1902	Fujitsu ICL Term Emulator Prog B	0	1	1	1	0	0	0	3	0.00%
1372	Fujitsu Config Protocol	0	0	1	2	0	0	0	3	0.00%
1504	EVB SW Engineering Lic Mgr	0	0	0	1	0	2	0	3	0.00%
1569	ets	0	0	2	1	0	0	0	3	0.00%
2912	Epicon	0	0	0	1	1	1	0	3	0.00%
1818	Enhanced TFTP	0	0	0	0	1	2	0	3	0.00%
1396	DVL Active Mail	0	1	1	0	0	1	0	3	0.00%
1489	dmdocbroker	0	1	1	0	0	1	0	3	0.00%
2234	DirectPlay	0	0	2	1	0	0	0	3	0.00%
1351	Digital Tool Works (MIT)	0	1	1	0	1	0	0	3	0.00%
1702	deskshare	0	0	0	1	1	1	0	3	0.00%
3883	Deep Throat 2 trojan	0	1	0	2	0	0	0	3	0.00%
1656	dec-mbadmin-h	0	1	0	1	1	0	0	3	0.00%
1367	DCS	0	0	0	1	0	2	0	3	0.00%
1407	DBSA lic mgr	0	0	1	0	0	2	0	3	0.00%
1973	Data Link Switching RAS Protocol	0	1	0	1	1	0	0	3	0.00%
2067	Data Link Switch Write Port #	0	1	0	1	0	1	0	3	0.00%
2401	cvspserver	0	0	1	0	0	1	1	3	0.00%
1468	CSDM	0	0	0	2	0	1	0	3	0.00%
1358	CONNLCLI	0	0	1	2	0	0	0	3	0.00%
1802	ConComp1	0	0	0	0	2	1	0	3	0.00%
1757	cnhrp	0	0	0	0	2	1	0	3	0.00%
1476	clvm-cfg	0	0	0	1	2	0	0	3	0.00%
1993	cisco SNMP TCP port	0	0	0	1	1	1	0	3	0.00%
1989	cisco RSRB Priority 3 port	0	0	0	3	0	0	0	3	0.00%
1995	cisco perf port	0	0	2	0	1	0	0	3	0.00%
1762	cft-1	0	1	1	0	0	1	0	3	0.00%
1918	Candle Directory Service - NDS	0	0	1	2	0	0	0	3	0.00%
1770	bmc-net-svc	0	0	0	1	1	1	0	3	0.00%

Port	TCP/UDP Ports Description	May-02	Jun-02	Jul-02	Aug-02	Sep-02	Oct-02	Nov-02	Total	Percentage
2911	Blockade	0	0	1	1	0	1	0	3	0.00%
1951	bcs-lmserver	0	0	0	2	1	0	0	3	0.00%
1411	AudioFile	0	1	1	0	1	0	0	3	0.00%
1397	Audio Active Mail	0	0	2	0	0	1	0	3	0.00%
1385	Atex Publishing lic mgr	0	0	1	0	1	1	0	3	0.00%
1556	AshWin CI Tecnologies	0	0	1	1	0	1	0	3	0.00%
1447	Applied Parallel Research LM	0	0	0	3	0	0	0	3	0.00%
1800	ANSYS-lic mgr	0	0	1	1	1	0	0	3	0.00%
1781	answersoft-lm	0	0	2	0	0	1	0	3	0.00%
1535	ampr-info	0	0	2	0	1	0	0	3	0.00%
2102	Zephyr server	0	0	1	0	0	1	0	2	0.00%
2104	Zephyr hostmgr	0	0	2	0	0	0	0	2	0.00%
1558	xingmpeg	0	0	0	2	0	0	0	2	0.00%
7100	X Font Service	0	0	0	2	0	0	0	2	0.00%
1760	www-ldap-gw	0	0	1	0	0	1	0	2	0.00%
2784	world wide web - development	0	0	2	0	0	0	0	2	0.00%
1739	webaccess	0	0	0	1	1	0	0	2	0.00%
1245	Vodoo	0	0	0	1	0	1	0	2	0.00%
1796	Vocaltec Server Administration	0	1	0	0	0	1	0	2	0.00%
1518	Virtual Places Video data	0	0	1	1	0	0	0	2	0.00%
1533	Virtual Places Software	0	0	0	1	0	1	0	2	0.00%
5800	Virtual Network Computing server	0	0	2	0	0	0	0	2	0.00%
1707	vdmplay	0	0	1	1	0	0	0	2	0.00%
3456	VAT default data	0	0	1	0	1	0	0	2	0.00%
1370	Unix Shell to GlobalView	0	0	1	0	1	0	0	2	0.00%
1470	Universal Analytics	0	1	1	0	0	0	0	2	0.00%
1912	Unassigned	0	0	1	0	0	1	0	2	0.00%
1797	UMA	0	0	0	0	0	2	0	2	0.00%
1753	Translogic lic mgr	0	0	1	1	0	0	0	2	0.00%
3791	Total Eclypse (FTP)	0	0	2	0	0	0	0	2	0.00%
1417	Timbuktu Service 1 Port	0	0	0	2	0	0	0	2	0.00%
1728	TELINDUS	0	0	0	1	0	1	0	2	0.00%
1610	taurus-wh	0	0	0	1	0	1	0	2	0.00%
1751	SwiftNet	0	0	0	1	0	1	0	2	0.00%
1625	svs-omagent	0	0	1	0	0	1	0	2	0.00%
1048	Sun's NEO Object Request Broker	0	0	1	0	0	1	0	2	0.00%
1736	street-stream	0	0	0	1	0	1	0	2	0.00%
1391	Storage Access Server	0	0	0	0	1	1	0	2	0.00%
133	Statistics Service	0	0	0	0	0	2	0	2	0.00%

Port	TCP/UDP Ports Description	May-02	Jun-02	Jul-02	Aug-02	Sep-02	Oct-02	Nov-02	Total	Percentage
1654	stargatealerts	0	0	0	1	0	1	0	2	0.00%
161	SNMP	0	0	0	2	0	0	0	2	0.00%
1222	SNI R&D network	0	0	0	1	1	0	0	2	0.00%
1684	SnareSecure	0	0	0	0	1	1	0	2	0.00%
1553	sna-cs	0	0	2	0	0	0	0	2	0.00%
1660	skip-mc-gikreq	0	0	0	1	0	1	0	2	0.00%
1750	Simple Socket Library's PortMaster	0	1	1	0	0	0	0	2	0.00%
1583	simbaexpress	0	1	0	0	0	1	0	2	0.00%
1659	Silicon Grail lic mgr	0	0	1	0	1	0	0	2	0.00%
1651	shiva_confsrvr	0	0	1	0	0	1	0	2	0.00%
1426	Satellite-data Acquisition System 1	0	1	0	0	0	1	0	2	0.00%
1606	Salutation mgr (SLM-API)	0	0	0	0	1	1	0	2	0.00%
1793	rsc-robot	0	1	1	0	0	0	0	2	0.00%
1697	rrisat	0	0	0	0	1	1	0	2	0.00%
1695	rrilwm	0	0	1	0	0	1	0	2	0.00%
1497	rfx-lm	0	0	0	2	0	0	0	2	0.00%
1431	Reverse Gossip Transport	0	0	1	0	1	0	0	2	0.00%
1530	rap-service	0	1	0	0	1	0	0	2	0.00%
1812	RADIUS	0	0	0	0	2	0	0	2	0.00%
1596	radio-sm	0	1	0	0	1	0	0	2	0.00%
1595	radio	0	0	0	1	0	1	0	2	0.00%
1732	proxim	0	1	1	0	0	0	0	2	0.00%
1402	Prospero Resource mgr	0	0	1	0	0	1	0	2	0.00%
1460	Proshare Notebook Application	0	1	0	0	1	0	0	2	0.00%
1678	prolink	0	0	0	1	0	1	0	2	0.00%
1778	prodigy-internet	0	0	0	2	0	0	0	2	0.00%
1711	pptconference	0	0	1	0	0	1	0	2	0.00%
1562	pconnectmgr	0	0	0	1	0	1	0	2	0.00%
9997	Palace	0	0	0	2	0	0	0	2	0.00%
1675	Pacific Data Products	0	0	0	1	0	1	0	2	0.00%
1597	orbplus-iiop	0	0	0	1	0	1	0	2	0.00%
1570	orbixd	0	0	0	1	1	0	0	2	0.00%
1808	Oracle-VP2	0	0	1	1	0	0	0	2	0.00%
1754	oracle-em2	0	1	0	0	0	1	0	2	0.00%
1446	Optical Research Assoc Lic Mgr	0	0	0	2	0	0	0	2	0.00%
4453	NSS Alert mgr	0	0	1	0	0	1	0	2	0.00%
1416	Novell LU6.2	0	0	1	0	1	0	0	2	0.00%
1917	nOAgent	0	0	0	2	0	0	0	2	0.00%
1690	ng-umds	0	1	0	1	0	0	0	2	0.00%

Port	TCP/UDP Ports Description	May-02	Jun-02	Jul-02	Aug-02	Sep-02	Oct-02	Nov-02	Total	Percentage
2788	Netware NLM - Seagate SW	0	0	1	0	0	0	1	2	0.00%
1662	netview-aix-2	0	0	1	0	1	0	0	2	0.00%
1661	netview-aix-1	0	0	0	0	2	0	0	2	0.00%
21848	NetSpeak Automatic Call Distrib	0	0	0	2	0	0	0	2	0.00%
1613	NetBill Key Repository	0	0	0	1	0	1	0	2	0.00%
2236	Nani	0	0	0	0	1	1	0	2	0.00%
1806	Musiconline	0	0	0	1	0	1	0	2	0.00%
1348	multi media conferencing	0	0	0	1	0	1	0	2	0.00%
1347	multi media conferencing	0	0	0	1	1	0	0	2	0.00%
1478	ms-sna-base	0	1	1	0	0	0	0	2	0.00%
1464	MSL lic mgr	0	1	0	1	0	0	0	2	0.00%
1582	MSIMS	0	0	1	0	0	1	0	2	0.00%
1576	moldflow-lm	0	0	0	0	0	2	0	2	0.00%
1512	MS's Windows Internet Name Serv	0	0	1	0	0	1	0	2	0.00%
1444	Marcam lic Management	0	0	1	0	1	0	0	2	0.00%
1593	mainsoft-lm	0	0	0	0	1	1	0	2	0.00%
1352	Lotus Note	0	0	0	2	0	0	0	2	0.00%
1487	LocalInfoSrvr	0	0	1	1	0	0	0	2	0.00%
1903	Local Link Name Resolution	0	0	0	0	0	1	1	2	0.00%
2284	LNVMAPS	0	0	2	0	0	0	0	2	0.00%
2281	LNVCONSOLE	0	1	0	0	0	1	0	2	0.00%
1496	liberty-lm	0	0	1	0	1	0	0	2	0.00%
1547	laplink	0	0	2	0	0	0	0	2	0.00%
1701	l2f	0	0	1	0	0	1	0	2	0.00%
4444	KRB524	0	1	0	1	0	0	0	2	0.00%
1773	KMSControl	0	0	0	0	1	1	0	2	0.00%
1810	Jerand lic mgr	0	0	1	0	1	0	0	2	0.00%
1623	jaleosnd	0	0	0	1	0	1	0	2	0.00%
1573	itscomm-ns	0	1	0	0	0	1	0	2	0.00%
1609	isysg-lm	0	0	2	0	0	0	0	2	0.00%
2043	isis-bcast	0	2	0	0	0	0	0	2	0.00%
1537	isi-lm	0	0	1	1	0	0	0	2	0.00%
7999	iRDMI2	0	0	2	0	0	0	0	2	0.00%
1585	intv	0	0	0	0	2	0	0	2	0.00%
1355	Intuitive Edge	0	0	1	0	0	1	0	2	0.00%
1454	interHDL lic mgr	0	0	1	1	0	0	0	2	0.00%
1674	Intel Proshare Multicast	0	0	0	1	0	1	0	2	0.00%
2202	Int. Multimedia Teleconferencing	0	0	0	1	0	1	0	2	0.00%
1413	Innosys-ACL	0	0	1	1	0	0	0	2	0.00%

Port	TCP/UDP Ports Description	May-02	Jun-02	Jul-02	Aug-02	Sep-02	Oct-02	Nov-02	Total	Percentage
1710	impera	0	0	0	2	0	0	0	2	0.00%
1027	ICQ?	0	0	1	0	1	0	0	2	0.00%
1461	IBM Wireless LAN	0	0	0	1	0	1	0	2	0.00%
1405	IBM Remote Execution Starter	0	0	1	1	0	0	0	2	0.00%
1435	IBM CICS	0	0	1	0	1	0	0	2	0.00%
1782	hp-hcip	0	0	0	2	0	0	0	2	0.00%
2564	HP 3000 NS/VT block mode telnet	0	0	0	1	1	0	0	2	0.00%
1410	HiQ lic mgr	0	1	1	0	0	0	0	2	0.00%
1719	h323gatestat	0	0	0	1	0	1	0	2	0.00%
1677	groupwise	0	0	1	0	0	1	0	2	0.00%
1708	gat-lmd	0	0	0	2	0	0	0	2	0.00%
1738	GameGen1	0	0	0	0	1	1	0	2	0.00%
1901	Fujitsu ICL Terminal Emulator Prog A	0	0	0	0	2	0	0	2	0.00%
1499	Federico Heinz Consultora	0	0	1	0	1	0	0	2	0.00%
1776	Federal Emergency MIS	0	0	0	1	0	1	0	2	0.00%
3047	Fast Security HL Server	0	0	0	1	0	1	0	2	0.00%
1915	FACELINK	0	0	0	0	0	2	0	2	0.00%
1374	EPI Software Systems	0	0	0	2	0	0	0	2	0.00%
1439	Eicon X25/SNA Gateway	0	0	1	0	1	0	0	2	0.00%
1791	EA1	0	1	0	0	0	1	0	2	0.00%
1795	dpi-proxy	0	0	0	1	1	0	0	2	0.00%
1389	Document mgr	0	1	0	0	1	0	0	2	0.00%
1479	dberegister	0	1	0	0	1	0	0	2	0.00%
1908	Dawn	0	2	0	0	0	0	0	2	0.00%
1645	datametrics	0	0	0	2	0	0	0	2	0.00%
1679	darcorp-lm	0	0	0	1	0	1	0	2	0.00%
1686	cvmon	0	0	0	0	1	1	0	2	0.00%
4451	CTI System Msg	0	0	0	0	0	2	0	2	0.00%
3145	CSI-LFAP	0	0	0	0	1	1	0	2	0.00%
1472	csdm	0	0	0	0	1	1	0	2	0.00%
1713	ConferenceTalk	0	1	0	0	1	0	0	2	0.00%
1387	CAD Software Inc LM	0	0	1	1	0	0	0	2	0.00%
1944	close-combat	0	1	0	0	0	1	0	2	0.00%
1729	CityNL lic Management	0	0	2	0	0	0	0	2	0.00%
1990	cisco STUN Priority 1 port	0	0	0	0	0	2	0	2	0.00%
1996	cisco Remote SRB port	0	1	0	0	0	1	0	2	0.00%
1377	Cichlid lic mgr	0	0	1	1	0	0	0	2	0.00%
1572	Chipcom lic mgr	0	0	0	1	0	1	0	2	0.00%
1768	cft-7	0	0	0	0	2	0	0	2	0.00%

Port	TCP/UDP Ports Description	May-02	Jun-02	Jul-02	Aug-02	Sep-02	Oct-02	Nov-02	Total	Percentage
1765	cft-4	0	0	0	1	0	1	0	2	0.00%
1764	cft-3	0	0	0	2	0	0	0	2	0.00%
1763	cft-2	0	0	0	0	1	1	0	2	0.00%
1709	centra	0	0	0	1	0	1	0	2	0.00%
3264	cc:mail/lotus	0	0	2	0	0	0	0	2	0.00%
4450	Camp	0	0	0	2	0	0	0	2	0.00%
1734	Camber Corporation Lic Mgmt	0	0	0	1	0	1	0	2	0.00%
1399	Cadkey lic mgr	0	0	1	0	0	1	0	2	0.00%
1441	Cadis lic Management	0	1	0	1	0	0	0	2	0.00%
1554	CACI Products Company Lic. Mgr	0	0	0	2	0	0	0	2	0.00%
1637	CableNet Admin Protocol	0	0	0	1	1	0	0	2	0.00%
3421	Bull Apprise portmapper	0	0	0	1	0	1	0	2	0.00%
1042	Bla1.1	0	0	0	0	2	0	0	2	0.00%
1032	BBN IAD	0	0	0	0	2	0	0	2	0.00%
2238	AVIVA SNA SERVER	0	0	1	0	0	1	0	2	0.00%
1749	aspen-services	0	1	0	0	1	0	0	2	0.00%
1913	armadp	0	0	0	0	1	1	0	2	0.00%
4449	ARCrypto IP	0	0	1	1	0	0	0	2	0.00%
6588	AnalogX Web Proxy	0	0	0	0	0	2	0	2	0.00%
5190	America-Online	0	0	0	0	2	0	0	2	0.00%
2786	aic-oncrpc - Destiny MCD DB	0	0	0	1	0	1	0	2	0.00%
1483	AFS lic mgr	0	0	1	1	0	0	0	2	0.00%
2201	Advanced Training System Prog	0	0	0	2	0	0	0	2	0.00%
1469	Active Analysis Ltd lic Mgr	0	2	0	0	0	0	0	2	0.00%
1601	aas	0	0	0	1	1	0	0	2	0.00%
1511	3l-l1	0	0	1	0	1	0	0	2	0.00%
1652	xnmp	0	1	0	0	0	0	0	1	0.00%
1727	winddx	0	0	0	0	1	0	0	1	0.00%
22347	WIBU dongle server	0	0	0	0	0	1	0	1	0.00%
3457	VAT default control	0	0	0	0	1	0	0	1	0.00%
3900	Unidata UDT OS	0	0	1	0	0	0	0	1	0.00%
4343	UNICALL	0	0	0	0	0	0	1	1	0.00%
1624	udp-sr-port	0	0	1	0	0	0	0	1	0.00%
1906	TPortMapperReq	0	1	0	0	0	0	0	1	0.00%
1362	TimeFlies	0	0	0	1	0	0	0	1	0.00%
1419	Timbuktu Service 3 Port	0	1	0	0	0	0	0	1	0.00%
3010	Telerate Workstation	0	0	1	0	0	0	0	1	0.00%
1474	Telefinder	0	1	0	0	0	0	0	1	0.00%
61466	Telecommando	1	0	0	0	0	0	0	1	0.00%

Port	TCP/UDP Ports Description	May-02	Jun-02	Jul-02	Aug-02	Sep-02	Oct-02	Nov-02	Total	Percentage
1	TCP Port Service Multiplexer	0	0	0	0	1	0	0	1	0.00%
1450	Tandem Distrib Workbench Facility	0	1	0	0	0	0	0	1	0.00%
1475	Taligent lic mgr	0	0	1	0	0	0	0	1	0.00%
2565	Striker	0	0	0	1	0	0	0	1	0.00%
6145	StatSci lic mgr - 2	1	0	0	0	0	0	0	1	0.00%
1692	sstsys-lm	0	0	0	0	0	1	0	1	0.00%
11000	SSTROJG trojan	0	0	0	0	0	1	0	1	0.00%
1408	Sophia lic mgr	0	1	0	0	0	0	0	1	0.00%
1089	SocksServer trojan	0	0	0	1	0	0	0	1	0.00%
1705	slingshot	0	0	0	1	0	0	0	1	0.00%
1618	skytelnet	0	0	0	0	0	1	0	1	0.00%
1658	sixnetudr	0	0	1	0	0	0	0	1	0.00%
1549	Shiva Hose	0	0	1	0	0	0	0	1	0.00%
1502	Shiva	0	0	0	0	1	0	0	1	0.00%
1905	Secure UP.Link Gateway Protocol	0	0	0	1	0	0	0	1	0.00%
1644	Satellite-data Acquisition Sys 4	0	0	0	0	1	0	0	1	0.00%
4500	sae-urn	0	0	0	0	1	0	0	1	0.00%
1699	RSVP-ENCAPSULATION-2	0	1	0	0	0	0	0	1	0.00%
1694	rrimwm	0	1	0	0	0	0	0	1	0.00%
1730	roketz	0	0	0	0	1	0	0	1	0.00%
1509	Robcad	0	0	1	0	0	0	0	1	0.00%
1712	resource monitoring service	0	0	0	0	0	1	0	1	0.00%
4321	Remote Who Is	0	0	0	1	0	0	0	1	0.00%
4672	remote file access server	0	0	0	1	0	0	0	1	0.00%
1349	Registration Network Protocol	0	0	0	0	1	0	0	1	0.00%
1350	Registration Network Protocol	0	0	0	0	1	0	0	1	0.00%
3001	Redwood Broker	0	1	0	0	0	0	0	1	0.00%
2011	raid	0	0	0	0	0	1	0	1	0.00%
1788	psmond	0	0	0	0	1	0	0	1	0.00%
1459	Proshare Notebook Application	0	0	0	1	0	0	0	1	0.00%
8032	ProEd	0	1	0	0	0	0	0	1	0.00%
1777	powerguardian	0	0	1	0	0	0	0	1	0.00%
9875	Portal of Doom	0	1	0	0	0	0	0	1	0.00%
1819	Plato lic mgr	0	0	0	0	1	0	0	1	0.00%
1598	picknfs	0	1	0	0	0	0	0	1	0.00%
2801	Phineas trojan	0	0	1	0	0	0	0	1	0.00%
1779	pharmasoft	0	0	0	0	1	0	0	1	0.00%
2307	pehelp	1	0	0	0	0	0	0	1	0.00%
1564	Pay-Per-View	0	0	1	0	0	0	0	1	0.00%

Port	TCP/UDP Ports Description	May-02	Jun-02	Jul-02	Aug-02	Sep-02	Oct-02	Nov-02	Total	Percentage
1809	Oracle-VP1	0	0	1	0	0	0	0	1	0.00%
1748	oracle-em1	0	0	0	1	0	0	0	1	0.00%
1448	OpenConnect lic mgr	0	0	1	0	0	0	0	1	0.00%
1466	Ocean Software lic Mgr	0	0	1	0	0	0	0	1	0.00%
4132	NUTS Daemon	0	0	1	0	0	0	0	1	0.00%
1366	Novell NetWare Comm Service	0	0	0	0	1	0	0	1	0.00%
1059	nimreg	0	0	0	0	0	1	0	1	0.00%
1672	netview-aix-12	0	0	0	1	0	0	0	1	0.00%
1671	netview-aix-11	0	0	0	0	1	0	0	1	0.00%
1670	netview-aix-10	0	0	0	1	0	0	0	1	0.00%
1033	Netspy	0	0	0	1	0	0	0	1	0.00%
30100	NetSphere	0	0	0	1	0	0	0	1	0.00%
1612	NetBill Transaction Server	0	1	0	0	0	0	0	1	0.00%
1615	NetBill Authorization Server	0	0	0	1	0	0	0	1	0.00%
4446	N1-FWP	0	0	0	0	0	1	0	1	0.00%
2009	n	0	0	0	0	0	1	0	1	0.00%
5050	multimedia conference control tool	0	0	0	0	0	0	1	1	0.00%
1815	MMPFT	0	0	1	0	0	0	0	1	0.00%
2105	MiniPay	0	0	0	1	0	0	0	1	0.00%
20000	Millenium	0	0	0	0	0	1	0	1	0.00%
1820	mcagent	0	1	0	0	0	0	0	1	0.00%
3984	MAPPER network node mgr	0	0	1	0	0	0	0	1	0.00%
2283	LNVSTATUS	0	0	0	0	1	0	0	1	0.00%
2282	LNVALARM	0	0	1	0	0	0	0	1	0.00%
1361	LinX	0	1	0	0	0	0	0	1	0.00%
1485	LANSource	0	0	1	0	0	0	0	1	0.00%
2232	IVS Video default	0	0	0	0	1	0	0	1	0.00%
1950	ISMA Easdaq Test	0	1	0	0	0	0	0	1	0.00%
1643	isis-ambc	0	1	0	0	0	0	0	1	0.00%
1642	isis-am	0	0	1	0	0	0	0	1	0.00%
1579	ioc-sea-lm	0	1	0	0	0	0	0	1	0.00%
1673	Intel Proshare Multicast	0	0	0	0	1	0	0	1	0.00%
1602	inspect	0	0	0	0	1	0	0	1	0.00%
25002	icl-twobase3	0	0	0	0	0	0	1	1	0.00%
1792	ibm-dt-2	0	0	0	0	1	0	0	1	0.00%
1414	IBM MQSeries	0	0	0	0	0	1	0	1	0.00%
1451	IBM Information Management	0	0	0	1	0	0	0	1	0.00%
1726	IBERIAGAMES	0	0	0	0	0	1	0	1	0.00%
1577	hypercube-lm	0	0	0	0	0	1	0	1	0.00%

Port	TCP/UDP Ports Description	May-02	Jun-02	Jul-02	Aug-02	Sep-02	Oct-02	Nov-02	Total	Percentage
6110	HP SoftBench CM	0	1	0	0	0	0	0	1	0.00%
81	HOSTS2 Name Server	1	0	0	0	0	0	0	1	0.00%
1947	hlserver	0	0	0	0	1	0	0	1	0.00%
1722	HKS lic mgr	0	0	0	0	0	1	0	1	0.00%
1551	HECMTL-DB	0	0	0	0	0	1	0	1	0.00%
1703	hb-engine	0	0	0	0	0	1	0	1	0.00%
1718	h323gatedisc	0	0	1	0	0	0	0	1	0.00%
1452	GTE Govt Systems lic Mgr	0	0	0	1	0	0	0	1	0.00%
1401	Goldleaf lic mgr	0	1	0	0	0	0	0	1	0.00%
1369	GlobalView to Unix Shell	0	1	0	0	0	0	0	1	0.00%
1774	global-dtserv	0	0	0	1	0	0	0	1	0.00%
21554	GirlFriend trojan	0	0	0	0	0	1	0	1	0.00%
21544	GirlFriend	0	0	1	0	0	0	0	1	0.00%
1787	funk-lic	0	1	0	0	0	0	0	1	0.00%
1747	ftrapid-2	0	0	0	0	0	1	0	1	0.00%
1784	Finle lic mgr	0	0	1	0	0	0	0	1	0.00%
1948	eye2eye	0	1	0	0	0	0	0	1	0.00%
3002	EXLM Agent	0	0	0	0	0	1	0	1	0.00%
1423	Essbase Arbor Software	0	0	0	0	0	1	0	1	0.00%
1822	es-elmd	0	1	0	0	0	0	0	1	0.00%
1805	ENL-Name	0	0	0	0	0	1	0	1	0.00%
1804	ENL	0	0	0	0	0	1	0	1	0.00%
1740	encore	0	0	0	1	0	0	0	1	0.00%
1914	Elm-Momentum	0	0	0	1	0	0	0	1	0.00%
1378	Elan lic mgr	0	0	0	0	0	1	0	1	0.00%
12701	Eclipse 2000	0	1	0	0	0	0	0	1	0.00%
1821	donnyworld	0	0	0	0	0	1	0	1	0.00%
1655	dec-mbadmin	0	0	1	0	0	0	0	1	0.00%
1415	DBStar	0	0	1	0	0	0	0	1	0.00%
1503	Databeam	0	0	0	0	0	1	0	1	0.00%
1495	cvc	0	0	0	0	1	0	0	1	0.00%
1356	CuillaMartin Company	0	0	0	0	1	0	0	1	0.00%
1724	csbphonemaster	0	0	0	0	0	1	0	1	0.00%
1648	concurrent-lm	0	0	0	0	1	0	0	1	0.00%
2301	Compaq Insight mgr	0	0	1	0	0	0	0	1	0.00%
1110	Cluster status info	0	1	0	0	0	0	0	1	0.00%
1994	cisco serial tunnel port	0	0	0	0	0	1	0	1	0.00%
1999	cisco identification port	0	0	1	0	0	0	0	1	0.00%
1743	Cinema Graphics lic Mgr	0	0	0	0	0	1	0	1	0.00%

Port	TCP/UDP Ports Description	May-02	Jun-02	Jul-02	Aug-02	Sep-02	Oct-02	Nov-02	Total	Percentage
1523	cichild	0	0	1	0	0	0	0	1	0.00%
1373	Chromagrafx	0	0	0	1	0	0	0	1	0.00%
4009	Chimera HWM	0	0	0	0	0	0	1	1	0.00%
1767	cft-6	0	0	1	0	0	0	0	1	0.00%
1761	cft-0	0	0	0	0	0	1	0	1	0.00%
1639	cert-initiator	0	0	0	0	0	1	0	1	0.00%
1920	Candle Directory Service-FERRET	0	0	0	1	0	0	0	1	0.00%
1442	Cadis lic Management	0	0	1	0	0	0	0	1	0.00%
1638	CableNet Info Protocol	0	0	1	0	0	0	0	1	0.00%
1313	BMC_PATROLDB	0	0	1	0	0	0	0	1	0.00%
1432	Blueberry Software lic Mgr	0	0	1	0	0	0	0	1	0.00%
1548	Axon lic mgr	0	1	0	0	0	0	0	1	0.00%
5005	avt-profile-2	0	0	0	1	0	0	0	1	0.00%
1520	atm zip office	0	0	1	0	0	0	0	1	0.00%
4448	ASC Licence mgr	0	0	1	0	0	0	0	1	0.00%
3454	Apple Remote Access Protocol	0	0	0	0	1	0	0	1	0.00%
1084	Anasoft lic mgr	0	0	0	0	1	0	0	1	0.00%
1653	alphatech-lm	0	0	1	0	0	0	0	1	0.00%
2785	aic-np	0	0	0	0	1	0	0	1	0.00%
1538	3ds-lm	0	0	0	0	1	0	0	1	0.00%
	All Other Ports	**2118**	**4015**	**5094**	**11832**	**17947**	**14050**	**5332**	**60388**	**52.03%**

NMAP Scan Sample Data

nmap (V. 3.00) scan initiated Sun Dec 29 21:07:44 2002 as: nmap -sS -PT -PI -R -F -O -T 3 -iL C:\Program Files\NMapWin\ipaddress.txt -oN Scan1
Interesting ports on (63.240.15.170):
(The 1142 ports scanned but not shown below are in state: closed)

Port	State	Service
22/tcp	open	ssh
80/tcp	open	http
137/tcp	filtered	netbios-ns
138/tcp	filtered	netbios-dgm
139/tcp	filtered	netbios-ssn
554/tcp	open	rtsp
7070/tcp	open	realserver
9090/tcp	open	zeus-admin

Remote OS guesses: Linux kernel 2.2.13, Linux 2.2.14

Interesting ports on (63.240.15.179):
(The 1142 ports scanned but not shown below are in state: closed)

Port	State	Service
22/tcp	open	ssh
80/tcp	open	http
137/tcp	filtered	netbios-ns
138/tcp	filtered	netbios-dgm
139/tcp	filtered	netbios-ssn
554/tcp	open	rtsp
7070/tcp	open	realserver
9090/tcp	open	zeus-admin

Remote OS guesses: Linux 2.1.19 - 2.2.20, Linux kernel 2.2.13, Linux 2.2.14
Uptime 410.744 days (since Wed Feb 20 02:24:00 2002)

Interesting ports on (63.240.15.187):
(The 1142 ports scanned but not shown below are in state: closed)

Port	State	Service
22/tcp	open	ssh
80/tcp	open	http
137/tcp	filtered	netbios-ns
138/tcp	filtered	netbios-dgm
139/tcp	filtered	netbios-ssn
554/tcp	open	rtsp
7070/tcp	open	realserver
9090/tcp	open	zeus-admin

Remote OS guesses: Linux kernel 2.2.13, Linux 2.2.14

Uptime 264.293 days (since Tue Jul 16 14:15:14 2002)

Warning: OS detection will be MUCH less reliable because we did not find at least 1 open

and 1 closed TCP port
Insufficient responses for TCP sequencing (0), OS detection may be less accurate
Insufficient responses for TCP sequencing (0), OS detection may be less accurate
Insufficient responses for TCP sequencing (0), OS detection may be less accurate
Interesting ports on real.cbsig.net (63.240.56.43):
(The 1146 ports scanned but not shown below are in state: filtered)
Port State Service
80/tcp open http
554/tcp open rtsp
7070/tcp open realserver
8080/tcp open http-proxy
Too many fingerprints match this host for me to give an accurate OS guess

Interesting ports on (207.188.15.156):
(The 576 ports scanned but not shown below are in state: closed)
Port State Service
1/tcp filtered tcpmux
2/tcp filtered compressnet
3/tcp filtered compressnet
5/tcp filtered rje
7/tcp filtered echo
9/tcp filtered discard
11/tcp filtered systat
13/tcp filtered daytime
15/tcp filtered netstat
17/tcp filtered qotd
18/tcp filtered msp
19/tcp filtered chargen
20/tcp filtered ftp-data
21/tcp filtered ftp
22/tcp filtered ssh
23/tcp filtered telnet
24/tcp filtered priv-mail
25/tcp filtered smtp
27/tcp filtered nsw-fe
29/tcp filtered msg-icp
31/tcp filtered msg-auth
33/tcp filtered dsp

35/tcp filtered priv-print
37/tcp filtered time
38/tcp filtered rap
39/tcp filtered rlp
41/tcp filtered graphics
42/tcp filtered nameserver
43/tcp filtered whois
44/tcp filtered mpm-flags
45/tcp filtered mpm
46/tcp filtered mpm-snd
47/tcp filtered ni-ftp
48/tcp filtered auditd
49/tcp filtered tacacs
50/tcp filtered re-mail-ck
51/tcp filtered la-maint
52/tcp filtered xns-time
53/tcp filtered domain
54/tcp filtered xns-ch
55/tcp filtered isi-gl
56/tcp filtered xns-auth
57/tcp filtered priv-term
58/tcp filtered xns-mail
59/tcp filtered priv-file
61/tcp filtered ni-mail
62/tcp filtered acas
63/tcp filtered via-ftp
64/tcp filtered covia
65/tcp filtered tacacs-ds
66/tcp filtered sql*net
67/tcp filtered dhcpserver
68/tcp filtered dhcpclient
69/tcp filtered tftp
70/tcp filtered gopher
71/tcp filtered netrjs-1
72/tcp filtered netrjs-2
73/tcp filtered netrjs-3
74/tcp filtered netrjs-4
75/tcp filtered priv-dial
76/tcp filtered deos
77/tcp filtered priv-rje
78/tcp filtered vettcp
79/tcp filtered finger

80/tcp open http
81/tcp filtered hosts2-ns
82/tcp filtered xfer
83/tcp filtered mit-ml-dev
84/tcp filtered ctf
85/tcp filtered mit-ml-dev
86/tcp filtered mfcobol
87/tcp filtered priv-term-l
88/tcp filtered kerberos-sec
89/tcp filtered su-mit-tg
90/tcp filtered dnsix
91/tcp filtered mit-dov
92/tcp filtered npp
93/tcp filtered dcp
94/tcp filtered objcall
95/tcp filtered supdup
96/tcp filtered dixie
97/tcp filtered swift-rvf
98/tcp filtered linuxconf
99/tcp filtered metagram
100/tcp filtered newacct
101/tcp filtered hostname
102/tcp filtered iso-tsap
103/tcp filtered gppitnp
104/tcp filtered acr-nema
105/tcp filtered csnet-ns
106/tcp filtered pop3pw
107/tcp filtered rtelnet
108/tcp filtered snagas
109/tcp filtered pop-2
110/tcp filtered pop-3
111/tcp filtered sunrpc
112/tcp filtered mcidas
113/tcp filtered auth
114/tcp filtered audionews
115/tcp filtered sftp
116/tcp filtered ansanotify
117/tcp filtered uucp-path
118/tcp filtered sqlserv
119/tcp filtered nntp
120/tcp filtered cfdptkt
121/tcp filtered erpc

122/tcp filtered smakynet
123/tcp filtered ntp
124/tcp filtered ansatrader
125/tcp filtered locus-map
126/tcp filtered unitary
127/tcp filtered locus-con
128/tcp filtered gss-xlicen
129/tcp filtered pwdgen
130/tcp filtered cisco-fna
131/tcp filtered cisco-tna
132/tcp filtered cisco-sys
133/tcp filtered statsrv
134/tcp filtered ingres-net
135/tcp filtered loc-srv
136/tcp filtered profile
137/tcp filtered netbios-ns
138/tcp filtered netbios-dgm
139/tcp filtered netbios-ssn
140/tcp filtered emfis-data
141/tcp filtered emfis-cntl
142/tcp filtered bl-idm
143/tcp filtered imap2
144/tcp filtered news
145/tcp filtered uaac
146/tcp filtered iso-tp0
147/tcp filtered iso-ip
148/tcp filtered cronus
149/tcp filtered aed-512
150/tcp filtered sql-net
151/tcp filtered hems
152/tcp filtered bftp
153/tcp filtered sgmp
154/tcp filtered netsc-prod
155/tcp filtered netsc-dev
156/tcp filtered sqlsrv
157/tcp filtered knet-cmp
158/tcp filtered pcmail-srv
159/tcp filtered nss-routing
160/tcp filtered sgmp-traps
161/tcp filtered snmp
162/tcp filtered snmptrap
163/tcp filtered cmip-man

164/tcp filtered cmip-agent
165/tcp filtered xns-courier
166/tcp filtered s-net
167/tcp filtered namp
168/tcp filtered rsvd
169/tcp filtered send
170/tcp filtered print-srv
171/tcp filtered multiplex
172/tcp filtered cl-1
173/tcp filtered xyplex-mux
174/tcp filtered mailq
175/tcp filtered vmnet
176/tcp filtered genrad-mux
177/tcp filtered xdmcp
178/tcp filtered nextstep
179/tcp filtered bgp
180/tcp filtered ris
181/tcp filtered unify
182/tcp filtered audit
183/tcp filtered ocbinder
184/tcp filtered ocserver
185/tcp filtered remote-kis
186/tcp filtered kis
187/tcp filtered aci
188/tcp filtered mumps
189/tcp filtered qft
190/tcp filtered gacp
191/tcp filtered prospero
192/tcp filtered osu-nms
193/tcp filtered srmp
194/tcp filtered irc
195/tcp filtered dn6-nlm-aud
196/tcp filtered dn6-smm-red
197/tcp filtered dls
198/tcp filtered dls-mon
199/tcp filtered smux
200/tcp filtered src
201/tcp filtered at-rtmp
202/tcp filtered at-nbp
203/tcp filtered at-3
204/tcp filtered at-echo
205/tcp filtered at-5

206/tcp filtered at-zis
207/tcp filtered at-7
208/tcp filtered at-8
209/tcp filtered tam
210/tcp filtered z39.50
211/tcp filtered 914c-g
212/tcp filtered anet
213/tcp filtered ipx
214/tcp filtered vmpwscs
215/tcp filtered softpc
216/tcp filtered atls
217/tcp filtered dbase
218/tcp filtered mpp
219/tcp filtered uarps
220/tcp filtered imap3
221/tcp filtered fln-spx
222/tcp filtered rsh-spx
223/tcp filtered cdc
242/tcp filtered direct
243/tcp filtered sur-meas
244/tcp filtered dayna
245/tcp filtered link
246/tcp filtered dsp3270
247/tcp filtered subntbcst_tftp
248/tcp filtered bhfhs
256/tcp filtered FW1-secureremote
257/tcp filtered FW1-mc-fwmodule
258/tcp filtered Fw1-mc-gui
259/tcp filtered esro-gen
260/tcp filtered openport
261/tcp filtered nsiiops
262/tcp filtered arcisdms
263/tcp filtered hdap
264/tcp filtered bgmp
265/tcp filtered maybeFW1
280/tcp filtered http-mgmt
281/tcp filtered personal-link
282/tcp filtered cableport-ax
308/tcp filtered novastorbakcup
309/tcp filtered entrusttime
310/tcp filtered bhmds
311/tcp filtered asip-webadmin

312/tcp filtered vslmp
313/tcp filtered magenta-logic
314/tcp filtered opalis-robot
315/tcp filtered dpsi
316/tcp filtered decauth
317/tcp filtered zannet
321/tcp filtered pip
344/tcp filtered pdap
345/tcp filtered pawserv
346/tcp filtered zserv
347/tcp filtered fatserv
348/tcp filtered csi-sgwp
349/tcp filtered mftp
350/tcp filtered matip-type-a
351/tcp filtered matip-type-b
352/tcp filtered dtag-ste-sb
353/tcp filtered ndsauth
354/tcp filtered bh611
355/tcp filtered datex-asn
356/tcp filtered cloanto-net-1
357/tcp filtered bhevent
358/tcp filtered shrinkwrap
359/tcp filtered tenebris_nts
360/tcp filtered scoi2odialog
361/tcp filtered semantix
362/tcp filtered srssend
363/tcp filtered rsvp_tunnel
364/tcp filtered aurora-cmgr
365/tcp filtered dtk
366/tcp filtered odmr
367/tcp filtered mortgageware
368/tcp filtered qbikgdp
369/tcp filtered rpc2portmap
370/tcp filtered codaauth2
371/tcp filtered clearcase
372/tcp filtered ulistserv
373/tcp filtered legent-1
374/tcp filtered legent-2
375/tcp filtered hassle
376/tcp filtered nip
377/tcp filtered tnETOS
378/tcp filtered dsETOS

379/tcp filtered is99c
380/tcp filtered is99s
381/tcp filtered hp-collector
382/tcp filtered hp-managed-node
383/tcp filtered hp-alarm-mgr
384/tcp filtered arns
385/tcp filtered ibm-app
386/tcp filtered asa
387/tcp filtered aurp
388/tcp filtered unidata-ldm
389/tcp filtered ldap
390/tcp filtered uis
391/tcp filtered synotics-relay
392/tcp filtered synotics-broker
393/tcp filtered dis
394/tcp filtered embl-ndt
395/tcp filtered netcp
396/tcp filtered netware-ip
397/tcp filtered mptn
398/tcp filtered kryptolan
399/tcp filtered iso-tsap-c2
400/tcp filtered work-sol
401/tcp filtered ups
402/tcp filtered genie
403/tcp filtered decap
404/tcp filtered nced
405/tcp filtered ncld
406/tcp filtered imsp
407/tcp filtered timbuktu
408/tcp filtered prm-sm
409/tcp filtered prm-nm
410/tcp filtered decladebug
411/tcp filtered rmt
412/tcp filtered synoptics-trap
413/tcp filtered smsp
414/tcp filtered infoseek
415/tcp filtered bnet
416/tcp filtered silverplatter
417/tcp filtered onmux
418/tcp filtered hyper-g
419/tcp filtered ariel1
420/tcp filtered smpte

421/tcp filtered ariel2
422/tcp filtered ariel3
423/tcp filtered opc-job-start
424/tcp filtered opc-job-track
425/tcp filtered icad-el
426/tcp filtered smartsdp
427/tcp filtered svrloc
428/tcp filtered ocs_cmu
429/tcp filtered ocs_amu
430/tcp filtered utmpsd
431/tcp filtered utmpcd
432/tcp filtered iasd
433/tcp filtered nnsp
434/tcp filtered mobileip-agent
435/tcp filtered mobilip-mn
436/tcp filtered dna-cml
437/tcp filtered comscm
438/tcp filtered dsfgw
439/tcp filtered dasp
440/tcp filtered sgcp
441/tcp filtered decvms-sysmgt
442/tcp filtered cvc_hostd
443/tcp filtered https
444/tcp filtered snpp
445/tcp filtered microsoft-ds
446/tcp filtered ddm-rdb
447/tcp filtered ddm-dfm
448/tcp filtered ddm-ssl
449/tcp filtered as-servermap
450/tcp filtered tserver
451/tcp filtered sfs-smp-net
452/tcp filtered sfs-config
453/tcp filtered creativeserver
454/tcp filtered contentserver
455/tcp filtered creativepartnr
456/tcp filtered macon-tcp
457/tcp filtered scohelp
458/tcp filtered appleqtc
459/tcp filtered ampr-rcmd
460/tcp filtered skronk
461/tcp filtered datasurfsrv
462/tcp filtered datasurfsrvsec

463/tcp filtered alpes
464/tcp filtered kpasswd5
465/tcp filtered smtps
466/tcp filtered digital-vrc
467/tcp filtered mylex-mapd
468/tcp filtered photuris
469/tcp filtered rcp
470/tcp filtered scx-proxy
471/tcp filtered mondex
472/tcp filtered ljk-login
473/tcp filtered hybrid-pop
474/tcp filtered tn-tl-w1
475/tcp filtered tcpnethaspsrv
476/tcp filtered tn-tl-fd1
477/tcp filtered ss7ns
478/tcp filtered spsc
479/tcp filtered iafserver
480/tcp filtered loadsrv
481/tcp filtered dvs
482/tcp filtered bgs-nsi
483/tcp filtered ulpnet
484/tcp filtered integra-sme
485/tcp filtered powerburst
486/tcp filtered sstats
487/tcp filtered saft
488/tcp filtered gss-http
489/tcp filtered nest-protocol
490/tcp filtered micom-pfs
491/tcp filtered go-login
492/tcp filtered ticf-1
493/tcp filtered ticf-2
494/tcp filtered pov-ray
495/tcp filtered intecourier
496/tcp filtered pim-rp-disc
497/tcp filtered dantz
498/tcp filtered siam
499/tcp filtered iso-ill
500/tcp filtered isakmp
501/tcp filtered stmf
502/tcp filtered asa-appl-proto
503/tcp filtered intrinsa
504/tcp filtered citadel

505/tcp filtered mailbox-lm
506/tcp filtered ohimsrv
507/tcp filtered crs
508/tcp filtered xvttp
509/tcp filtered snare
510/tcp filtered fcp
511/tcp filtered passgo
512/tcp filtered exec
513/tcp filtered login
514/tcp filtered shell
515/tcp filtered printer
516/tcp filtered videotex
517/tcp filtered talk
518/tcp filtered ntalk
519/tcp filtered utime
520/tcp filtered efs
521/tcp filtered ripng
522/tcp filtered ulp
523/tcp filtered ibm-db2
524/tcp filtered ncp
525/tcp filtered timed
526/tcp filtered tempo
527/tcp filtered stx
528/tcp filtered custix
529/tcp filtered irc-serv
530/tcp filtered courier
531/tcp filtered conference
532/tcp filtered netnews
533/tcp filtered netwall
534/tcp filtered mm-admin
535/tcp filtered iiop
536/tcp filtered opalis-rdv
537/tcp filtered nmsp
538/tcp filtered gdomap
539/tcp filtered apertus-ldp
540/tcp filtered uucp
541/tcp filtered uucp-rlogin
542/tcp filtered commerce
543/tcp filtered klogin
544/tcp filtered kshell
545/tcp filtered ekshell
546/tcp filtered dhcpv6-client

547/tcp filtered dhcpv6-server
548/tcp filtered afpovertcp
549/tcp filtered idfp
550/tcp filtered new-rwho
551/tcp filtered cybercash
552/tcp filtered deviceshare
553/tcp filtered pirp
554/tcp open rtsp
555/tcp filtered dsf
556/tcp filtered remotefs
557/tcp filtered openvms-sysipc
558/tcp filtered sdnskmp
559/tcp filtered teedtap
560/tcp filtered rmonitor
561/tcp filtered monitor
562/tcp filtered chshell
563/tcp filtered snews
564/tcp filtered 9pfs
565/tcp filtered whoami
566/tcp filtered streettalk
567/tcp filtered banyan-rpc
568/tcp filtered ms-shuttle
569/tcp filtered ms-rome
570/tcp filtered meter
571/tcp filtered umeter
572/tcp filtered sonar
573/tcp filtered banyan-vip
574/tcp filtered ftp-agent
575/tcp filtered vemmi
576/tcp filtered ipcd
577/tcp filtered vnas
578/tcp filtered ipdd
579/tcp filtered decbsrv
580/tcp filtered sntp-heartbeat
581/tcp filtered bdp
582/tcp filtered scc-security
583/tcp filtered philips-vc
584/tcp filtered keyserver
585/tcp filtered imap4-ssl
586/tcp filtered password-chg
587/tcp filtered submission
588/tcp filtered cal

589/tcp filtered eyelink
590/tcp filtered tns-cml
591/tcp filtered http-alt
592/tcp filtered eudora-set
593/tcp filtered http-rpc-epmap
594/tcp filtered tpip
595/tcp filtered cab-protocol
596/tcp filtered smsd
597/tcp filtered ptcnameservice
598/tcp filtered sco-websrvrmg3
599/tcp filtered acp
600/tcp filtered ipcserver
606/tcp filtered urm
607/tcp filtered nqs
608/tcp filtered sift-uft
609/tcp filtered npmp-trap
610/tcp filtered npmp-local
611/tcp filtered npmp-gui
628/tcp filtered qmqp
631/tcp filtered ipp
634/tcp filtered ginad
636/tcp filtered ldapssl
637/tcp filtered lanserver
660/tcp filtered mac-srvr-admin
666/tcp filtered doom
691/tcp filtered resvc
704/tcp filtered elcsd
706/tcp filtered silc
709/tcp filtered entrustmanager
729/tcp filtered netviewdm1
730/tcp filtered netviewdm2
731/tcp filtered netviewdm3
740/tcp filtered netcp
741/tcp filtered netgw
742/tcp filtered netrcs
744/tcp filtered flexlm
747/tcp filtered fujitsu-dev
748/tcp filtered ris-cm
749/tcp filtered kerberos-adm
750/tcp filtered kerberos
751/tcp filtered kerberos_master
752/tcp filtered qrh

753/tcp filtered rrh
754/tcp filtered krb_prop
758/tcp filtered nlogin
759/tcp filtered con
760/tcp filtered krbupdate
761/tcp filtered kpasswd
762/tcp filtered quotad
763/tcp filtered cycleserv
764/tcp filtered omserv
765/tcp filtered webster
767/tcp filtered phonebook
769/tcp filtered vid
770/tcp filtered cadlock
771/tcp filtered rtip
772/tcp filtered cycleserv2
773/tcp filtered submit
774/tcp filtered rpasswd
775/tcp filtered entomb
776/tcp filtered wpages
780/tcp filtered wpgs
781/tcp filtered hp-collector
782/tcp filtered hp-managed-node
783/tcp filtered hp-alarm-mgr
786/tcp filtered concert
799/tcp filtered controlit
800/tcp filtered mdbs_daemon
801/tcp filtered device
871/tcp filtered supfilesrv
873/tcp filtered rsync
888/tcp filtered accessbuilder
901/tcp filtered samba-swat
950/tcp filtered oftep-rpc
953/tcp filtered rndc
975/tcp filtered securenetpro-sensor
989/tcp filtered ftps-data
990/tcp filtered ftps
992/tcp filtered telnets
993/tcp filtered imaps
994/tcp filtered ircs
995/tcp filtered pop3s
996/tcp filtered xtreelic
997/tcp filtered maitrd

998/tcp filtered busboy
999/tcp filtered garcon
1000/tcp filtered cadlock
1008/tcp filtered ufsd
7070/tcp open realserver
9090/tcp open zeus-admin
Remote operating system guess: Solaris 8 early access beta through actual release
Uptime 5.148 days (since Tue Apr 01 17:16:47 2003)

Interesting ports on loa-lvl3-wa09.rbn.com (63.214.137.50):
(The 1142 ports scanned but not shown below are in state: closed)
Port State Service
22/tcp open ssh
80/tcp open http
137/tcp filtered netbios-ns
138/tcp filtered netbios-dgm
139/tcp filtered netbios-ssn
554/tcp open rtsp
7070/tcp open realserver
9090/tcp open zeus-admin
Remote OS guesses: Linux Kernel 2.4.0 - 2.5.20, Linux 2.4.19-pre4 on Alpha, Linux Kernel

2.4.3 SMP (RedHat)

Interesting ports on (63.240.15.178):
(The 1142 ports scanned but not shown below are in state: closed)
Port State Service
22/tcp open ssh
80/tcp open http
137/tcp filtered netbios-ns
138/tcp filtered netbios-dgm
139/tcp filtered netbios-ssn
554/tcp open rtsp
7070/tcp open realserver
9090/tcp open zeus-admin
Remote OS guesses: Linux kernel 2.2.13, Linux 2.2.14
Uptime 38.387 days (since Thu Feb 27 11:39:08 2003)

Interesting ports on (63.240.15.184):
(The 1142 ports scanned but not shown below are in state: closed)
Port State Service
22/tcp open ssh

80/tcp open http
137/tcp filtered netbios-ns
138/tcp filtered netbios-dgm
139/tcp filtered netbios-ssn
554/tcp open rtsp
7070/tcp open realserver
9090/tcp open zeus-admin
Remote OS guesses: Linux kernel 2.2.13, Linux 2.2.14

Warning: OS detection will be MUCH less reliable because we did not find at least 1 open

and 1 closed TCP port
Interesting ports on real.cbsig.net (63.240.56.42):
(The 1146 ports scanned but not shown below are in state: filtered)
Port State Service
80/tcp open http
554/tcp open rtsp
7070/tcp open realserver
8080/tcp open http-proxy
No exact OS matches for host (test conditions non-ideal).
TCP/IP fingerprint:
SInfo(V=3.00%P=i686-pc-windows-windows%D=4/6%Time=3E90ECE4%O=80%C=-
1)
TSeq(Class=RI%gcd=1%SI=5D14D6%IPID=Z)
TSeq(Class=RI%gcd=1%SI=5FD8A8%IPID=Z)
TSeq(Class=RI%gcd=2%SI=37C8F9%IPID=Z)
T1(Resp=Y%DF=Y%W=16A0%ACK=S++%Flags=AS%Ops=MNNTNW)
T1(Resp=Y%DF=Y%W=16A0%ACK=O%Flags=AS%Ops=MNNTNW)
T2(Resp=N)
T3(Resp=N)
T4(Resp=N)
T5(Resp=N)
T6(Resp=N)
T7(Resp=N)
PU(Resp=N)

Interesting ports on (207.188.15.144):
(The 574 ports scanned but not shown below are in state: closed)
Port State Service
1/tcp filtered tcpmux

2/tcp filtered compressnet
3/tcp filtered compressnet
5/tcp filtered rje
7/tcp filtered echo
9/tcp filtered discard
11/tcp filtered systat
13/tcp filtered daytime
15/tcp filtered netstat
17/tcp filtered qotd
18/tcp filtered msp
19/tcp filtered chargen
20/tcp filtered ftp-data
21/tcp filtered ftp
22/tcp filtered ssh
23/tcp filtered telnet
24/tcp filtered priv-mail
25/tcp filtered smtp
27/tcp filtered nsw-fe
29/tcp filtered msg-icp
31/tcp filtered msg-auth
33/tcp filtered dsp
35/tcp filtered priv-print
37/tcp filtered time
38/tcp filtered rap
39/tcp filtered rlp
41/tcp filtered graphics
42/tcp filtered nameserver
43/tcp filtered whois
44/tcp filtered mpm-flags
45/tcp filtered mpm
46/tcp filtered mpm-snd
47/tcp filtered ni-ftp
48/tcp filtered auditd
49/tcp filtered tacacs
50/tcp filtered re-mail-ck
51/tcp filtered la-maint
52/tcp filtered xns-time
53/tcp filtered domain
54/tcp filtered xns-ch
55/tcp filtered isi-gl
56/tcp filtered xns-auth
57/tcp filtered priv-term

58/tcp filtered xns-mail
59/tcp filtered priv-file
61/tcp filtered ni-mail
62/tcp filtered acas
63/tcp filtered via-ftp
64/tcp filtered covia
65/tcp filtered tacacs-ds
66/tcp filtered sql*net
67/tcp filtered dhcpserver
68/tcp filtered dhcpclient
69/tcp filtered tftp
70/tcp filtered gopher
71/tcp filtered netrjs-1
72/tcp filtered netrjs-2
73/tcp filtered netrjs-3
74/tcp filtered netrjs-4
75/tcp filtered priv-dial
76/tcp filtered deos
77/tcp filtered priv-rje
78/tcp filtered vettcp
79/tcp filtered finger
80/tcp open http
81/tcp filtered hosts2-ns
82/tcp filtered xfer
83/tcp filtered mit-ml-dev
84/tcp filtered ctf
85/tcp filtered mit-ml-dev
86/tcp filtered mfcobol
87/tcp filtered priv-term-l
88/tcp filtered kerberos-sec
89/tcp filtered su-mit-tg
90/tcp filtered dnsix
91/tcp filtered mit-dov
92/tcp filtered npp
93/tcp filtered dcp
94/tcp filtered objcall
95/tcp filtered supdup
96/tcp filtered dixie
97/tcp filtered swift-rvf
98/tcp filtered linuxconf
99/tcp filtered metagram
100/tcp filtered newacct

101/tcp filtered hostname
102/tcp filtered iso-tsap
103/tcp filtered gppitnp
104/tcp filtered acr-nema
105/tcp filtered csnet-ns
106/tcp filtered pop3pw
107/tcp filtered rtelnet
108/tcp filtered snagas
109/tcp filtered pop-2
110/tcp filtered pop-3
111/tcp filtered sunrpc
112/tcp filtered mcidas
113/tcp filtered auth
114/tcp filtered audionews
115/tcp filtered sftp
116/tcp filtered ansanotify
117/tcp filtered uucp-path
118/tcp filtered sqlserv
119/tcp filtered nntp
120/tcp filtered cfdptkt
121/tcp filtered erpc
122/tcp filtered smakynet
123/tcp filtered ntp
124/tcp filtered ansatrader
125/tcp filtered locus-map
126/tcp filtered unitary
127/tcp filtered locus-con
128/tcp filtered gss-xlicen
129/tcp filtered pwdgen
130/tcp filtered cisco-fna
131/tcp filtered cisco-tna
132/tcp filtered cisco-sys
133/tcp filtered statsrv
134/tcp filtered ingres-net
135/tcp filtered loc-srv
136/tcp filtered profile
137/tcp filtered netbios-ns
138/tcp filtered netbios-dgm
139/tcp filtered netbios-ssn
140/tcp filtered emfis-data
141/tcp filtered emfis-cntl
142/tcp filtered bl-idm

143/tcp filtered imap2
144/tcp filtered news
145/tcp filtered uaac
146/tcp filtered iso-tp0
147/tcp filtered iso-ip
148/tcp filtered cronus
149/tcp filtered aed-512
150/tcp filtered sql-net
151/tcp filtered hems
152/tcp filtered bftp
153/tcp filtered sgmp
154/tcp filtered netsc-prod
155/tcp filtered netsc-dev
156/tcp filtered sqlsrv
157/tcp filtered knet-cmp
158/tcp filtered pcmail-srv
159/tcp filtered nss-routing
160/tcp filtered sgmp-traps
161/tcp filtered snmp
162/tcp filtered snmptrap
163/tcp filtered cmip-man
164/tcp filtered cmip-agent
165/tcp filtered xns-courier
166/tcp filtered s-net
167/tcp filtered namp
168/tcp filtered rsvd
169/tcp filtered send
170/tcp filtered print-srv
171/tcp filtered multiplex
172/tcp filtered cl-1
173/tcp filtered xyplex-mux
174/tcp filtered mailq
175/tcp filtered vmnet
176/tcp filtered genrad-mux
177/tcp filtered xdmcp
178/tcp filtered nextstep
179/tcp filtered bgp
180/tcp filtered ris
181/tcp filtered unify
182/tcp filtered audit
183/tcp filtered ocbinder
184/tcp filtered ocserver

185/tcp filtered remote-kis
186/tcp filtered kis
187/tcp filtered aci
188/tcp filtered mumps
189/tcp filtered qft
190/tcp filtered gacp
191/tcp filtered prospero
192/tcp filtered osu-nms
193/tcp filtered srmp
194/tcp filtered irc
195/tcp filtered dn6-nlm-aud
196/tcp filtered dn6-smm-red
197/tcp filtered dls
198/tcp filtered dls-mon
199/tcp filtered smux
200/tcp filtered src
201/tcp filtered at-rtmp
202/tcp filtered at-nbp
203/tcp filtered at-3
204/tcp filtered at-echo
205/tcp filtered at-5
206/tcp filtered at-zis
207/tcp filtered at-7
208/tcp filtered at-8
209/tcp filtered tam
210/tcp filtered z39.50
211/tcp filtered 914c-g
212/tcp filtered anet
213/tcp filtered ipx
214/tcp filtered vmpwscs
215/tcp filtered softpc
216/tcp filtered atls
217/tcp filtered dbase
218/tcp filtered mpp
219/tcp filtered uarps
220/tcp filtered imap3
221/tcp filtered fln-spx
222/tcp filtered rsh-spx
223/tcp filtered cdc
242/tcp filtered direct
243/tcp filtered sur-meas
244/tcp filtered dayna

245/tcp filtered link
246/tcp filtered dsp3270
247/tcp filtered subntbcst_tftp
248/tcp filtered bhfhs
256/tcp filtered FW1-secureremote
257/tcp filtered FW1-mc-fwmodule
258/tcp filtered Fw1-mc-gui
259/tcp filtered esro-gen
260/tcp filtered openport
261/tcp filtered nsiiops
262/tcp filtered arcisdms
263/tcp filtered hdap
264/tcp filtered bgmp
265/tcp filtered maybeFW1
280/tcp filtered http-mgmt
281/tcp filtered personal-link
282/tcp filtered cableport-ax
308/tcp filtered novastorbakcup
309/tcp filtered entrusttime
310/tcp filtered bhmds
311/tcp filtered asip-webadmin
312/tcp filtered vslmp
313/tcp filtered magenta-logic
314/tcp filtered opalis-robot
315/tcp filtered dpsi
316/tcp filtered decauth
317/tcp filtered zannet
321/tcp filtered pip
344/tcp filtered pdap
345/tcp filtered pawserv
346/tcp filtered zserv
347/tcp filtered fatserv
348/tcp filtered csi-sgwp
349/tcp filtered mftp
350/tcp filtered matip-type-a
351/tcp filtered matip-type-b
352/tcp filtered dtag-ste-sb
353/tcp filtered ndsauth
354/tcp filtered bh611
355/tcp filtered datex-asn
356/tcp filtered cloanto-net-1
357/tcp filtered bhevent

358/tcp filtered shrinkwrap
359/tcp filtered tenebris_nts
360/tcp filtered scoi2odialog
361/tcp filtered semantix
362/tcp filtered srssend
363/tcp filtered rsvp_tunnel
364/tcp filtered aurora-cmgr
365/tcp filtered dtk
366/tcp filtered odmr
367/tcp filtered mortgageware
368/tcp filtered qbikgdp
369/tcp filtered rpc2portmap
370/tcp filtered codaauth2
371/tcp filtered clearcase
372/tcp filtered ulistserv
373/tcp filtered legent-1
374/tcp filtered legent-2
375/tcp filtered hassle
376/tcp filtered nip
377/tcp filtered tnETOS
378/tcp filtered dsETOS
379/tcp filtered is99c
380/tcp filtered is99s
381/tcp filtered hp-collector
382/tcp filtered hp-managed-node
383/tcp filtered hp-alarm-mgr
384/tcp filtered arns
385/tcp filtered ibm-app
386/tcp filtered asa
387/tcp filtered aurp
388/tcp filtered unidata-ldm
389/tcp filtered ldap
390/tcp filtered uis
391/tcp filtered synotics-relay
392/tcp filtered synotics-broker
393/tcp filtered dis
394/tcp filtered embl-ndt
395/tcp filtered netcp
396/tcp filtered netware-ip
397/tcp filtered mptn
398/tcp filtered kryptolan
399/tcp filtered iso-tsap-c2

400/tcp filtered work-sol
401/tcp filtered ups
402/tcp filtered genie
403/tcp filtered decap
404/tcp filtered nced
405/tcp filtered ncld
406/tcp filtered imsp
407/tcp filtered timbuktu
408/tcp filtered prm-sm
409/tcp filtered prm-nm
410/tcp filtered decladebug
411/tcp filtered rmt
412/tcp filtered synoptics-trap
413/tcp filtered smsp
414/tcp filtered infoseek
415/tcp filtered bnet
416/tcp filtered silverplatter
417/tcp filtered onmux
418/tcp filtered hyper-g
419/tcp filtered ariel1
420/tcp filtered smpte
421/tcp filtered ariel2
422/tcp filtered ariel3
423/tcp filtered opc-job-start
424/tcp filtered opc-job-track
425/tcp filtered icad-el
426/tcp filtered smartsdp
427/tcp filtered svrloc
428/tcp filtered ocs_cmu
429/tcp filtered ocs_amu
430/tcp filtered utmpsd
431/tcp filtered utmpcd
432/tcp filtered iasd
433/tcp filtered nnsp
434/tcp filtered mobileip-agent
435/tcp filtered mobilip-mn
436/tcp filtered dna-cml
437/tcp filtered comscm
438/tcp filtered dsfgw
439/tcp filtered dasp
440/tcp filtered sgcp
441/tcp filtered decvms-sysmgt

442/tcp filtered cvc_hostd
443/tcp filtered https
444/tcp filtered snpp
445/tcp filtered microsoft-ds
446/tcp filtered ddm-rdb
447/tcp filtered ddm-dfm
448/tcp filtered ddm-ssl
449/tcp filtered as-servermap
450/tcp filtered tserver
451/tcp filtered sfs-smp-net
452/tcp filtered sfs-config
453/tcp filtered creativeserver
454/tcp filtered contentserver
455/tcp filtered creativepartnr
456/tcp filtered macon-tcp
457/tcp filtered scohelp
458/tcp filtered appleqtc
459/tcp filtered ampr-rcmd
460/tcp filtered skronk
461/tcp filtered datasurfsrv
462/tcp filtered datasurfsrvsec
463/tcp filtered alpes
464/tcp filtered kpasswd5
465/tcp filtered smtps
466/tcp filtered digital-vrc
467/tcp filtered mylex-mapd
468/tcp filtered photuris
469/tcp filtered rcp
470/tcp filtered scx-proxy
471/tcp filtered mondex
472/tcp filtered ljk-login
473/tcp filtered hybrid-pop
474/tcp filtered tn-tl-w1
475/tcp filtered tcpnethaspsrv
476/tcp filtered tn-tl-fd1
477/tcp filtered ss7ns
478/tcp filtered spsc
479/tcp filtered iafserver
480/tcp filtered loadsrv
481/tcp filtered dvs
482/tcp filtered bgs-nsi
483/tcp filtered ulpnet

484/tcp filtered integra-sme
485/tcp filtered powerburst
486/tcp filtered sstats
487/tcp filtered saft
488/tcp filtered gss-http
489/tcp filtered nest-protocol
490/tcp filtered micom-pfs
491/tcp filtered go-login
492/tcp filtered ticf-1
493/tcp filtered ticf-2
494/tcp filtered pov-ray
495/tcp filtered intecourier
496/tcp filtered pim-rp-disc
497/tcp filtered dantz
498/tcp filtered siam
499/tcp filtered iso-ill
500/tcp filtered isakmp
501/tcp filtered stmf
502/tcp filtered asa-appl-proto
503/tcp filtered intrinsa
504/tcp filtered citadel
505/tcp filtered mailbox-lm
506/tcp filtered ohimsrv
507/tcp filtered crs
508/tcp filtered xvttp
509/tcp filtered snare
510/tcp filtered fcp
511/tcp filtered passgo
512/tcp filtered exec
513/tcp filtered login
514/tcp filtered shell
515/tcp filtered printer
516/tcp filtered videotex
517/tcp filtered talk
518/tcp filtered ntalk
519/tcp filtered utime
520/tcp filtered efs
521/tcp filtered ripng
522/tcp filtered ulp
523/tcp filtered ibm-db2
524/tcp filtered ncp
525/tcp filtered timed

526/tcp filtered tempo
527/tcp filtered stx
528/tcp filtered custix
529/tcp filtered irc-serv
530/tcp filtered courier
531/tcp filtered conference
532/tcp filtered netnews
533/tcp filtered netwall
534/tcp filtered mm-admin
535/tcp filtered iiop
536/tcp filtered opalis-rdv
537/tcp filtered nmsp
538/tcp filtered gdomap
539/tcp filtered apertus-ldp
540/tcp filtered uucp
541/tcp filtered uucp-rlogin
542/tcp filtered commerce
543/tcp filtered klogin
544/tcp filtered kshell
545/tcp filtered ekshell
546/tcp filtered dhcpv6-client
547/tcp filtered dhcpv6-server
548/tcp filtered afpovertcp
549/tcp filtered idfp
550/tcp filtered new-rwho
551/tcp filtered cybercash
552/tcp filtered deviceshare
553/tcp filtered pirp
554/tcp open rtsp
555/tcp filtered dsf
556/tcp filtered remotefs
557/tcp filtered openvms-sysipc
558/tcp filtered sdnskmp
559/tcp filtered teedtap
560/tcp filtered rmonitor
561/tcp filtered monitor
562/tcp filtered chshell
563/tcp filtered snews
564/tcp filtered 9pfs
565/tcp filtered whoami
566/tcp filtered streettalk
567/tcp filtered banyan-rpc

568/tcp filtered ms-shuttle
569/tcp filtered ms-rome
570/tcp filtered meter
571/tcp filtered umeter
572/tcp filtered sonar
573/tcp filtered banyan-vip
574/tcp filtered ftp-agent
575/tcp filtered vemmi
576/tcp filtered ipcd
577/tcp filtered vnas
578/tcp filtered ipdd
579/tcp filtered decbsrv
580/tcp filtered sntp-heartbeat
581/tcp filtered bdp
582/tcp filtered scc-security
583/tcp filtered philips-vc
584/tcp filtered keyserver
585/tcp filtered imap4-ssl
586/tcp filtered password-chg
587/tcp filtered submission
588/tcp filtered cal
589/tcp filtered eyelink
590/tcp filtered tns-cml
591/tcp filtered http-alt
592/tcp filtered eudora-set
593/tcp filtered http-rpc-epmap
594/tcp filtered tpip
595/tcp filtered cab-protocol
596/tcp filtered smsd
597/tcp filtered ptcnameservice
598/tcp filtered sco-websrvrmg3
599/tcp filtered acp
600/tcp filtered ipcserver
606/tcp filtered urm
607/tcp filtered nqs
608/tcp filtered sift-uft
609/tcp filtered npmp-trap
610/tcp filtered npmp-local
611/tcp filtered npmp-gui
628/tcp filtered qmqp
631/tcp filtered ipp
634/tcp filtered ginad

636/tcp filtered ldapssl
637/tcp filtered lanserver
660/tcp filtered mac-srvr-admin
666/tcp filtered doom
691/tcp filtered resvc
704/tcp filtered elcsd
706/tcp filtered silc
709/tcp filtered entrustmanager
729/tcp filtered netviewdm1
730/tcp filtered netviewdm2
731/tcp filtered netviewdm3
740/tcp filtered netcp
741/tcp filtered netgw
742/tcp filtered netrcs
744/tcp filtered flexlm
747/tcp filtered fujitsu-dev
748/tcp filtered ris-cm
749/tcp filtered kerberos-adm
750/tcp filtered kerberos
751/tcp filtered kerberos_master
752/tcp filtered qrh
753/tcp filtered rrh
754/tcp filtered krb_prop
758/tcp filtered nlogin
759/tcp filtered con
760/tcp filtered krbupdate
761/tcp filtered kpasswd
762/tcp filtered quotad
763/tcp filtered cycleserv
764/tcp filtered omserv
765/tcp filtered webster
767/tcp filtered phonebook
769/tcp filtered vid
770/tcp filtered cadlock
771/tcp filtered rtip
772/tcp filtered cycleserv2
773/tcp filtered submit
774/tcp filtered rpasswd
775/tcp filtered entomb
776/tcp filtered wpages
780/tcp filtered wpgs
781/tcp filtered hp-collector

782/tcp filtered hp-managed-node
783/tcp filtered hp-alarm-mgr
786/tcp filtered concert
799/tcp filtered controlit
800/tcp filtered mdbs_daemon
801/tcp filtered device
871/tcp filtered supfilesrv
873/tcp filtered rsync
888/tcp filtered accessbuilder
901/tcp filtered samba-swat
950/tcp filtered oftep-rpc
953/tcp filtered rndc
975/tcp filtered securenetpro-sensor
989/tcp filtered ftps-data
990/tcp filtered ftps
992/tcp filtered telnets
993/tcp filtered imaps
994/tcp filtered ircs
995/tcp filtered pop3s
996/tcp filtered xtreelic
997/tcp filtered maitrd
998/tcp filtered busboy
999/tcp filtered garcon
1000/tcp filtered cadlock
1008/tcp filtered ufsd
4045/tcp open lockd
7070/tcp open realserver
9090/tcp open zeus-admin
32771/tcp open sometimes-rpc5
Remote operating system guess: Solaris 8 early access beta through actual release
Uptime 28.826 days (since Sun Mar 09 01:36:13 2003)

Interesting ports on (63.111.71.48):
(The 1142 ports scanned but not shown below are in state: closed)
Port State Service
22/tcp open ssh
80/tcp open http
137/tcp filtered netbios-ns
138/tcp filtered netbios-dgm
139/tcp filtered netbios-ssn
554/tcp open rtsp
7070/tcp open realserver

9090/tcp open zeus-admin
Remote OS guesses: Linux 2.1.19 - 2.2.20, Linux kernel 2.2.13, Linux 2.2.14
Uptime 51.424 days (since Fri Feb 14 11:17:37 2003)

Interesting ports on (211.95.72.22):
(The 1140 ports scanned but not shown below are in state: closed)
Port State Service
21/tcp open ftp
135/tcp open loc-srv
137/tcp filtered netbios-ns
138/tcp filtered netbios-dgm
139/tcp filtered netbios-ssn
445/tcp open microsoft-ds
1025/tcp open NFS-or-IIS
1026/tcp open LSA-or-nterm
3372/tcp open msdtc
5631/tcp open pcanywheredata
No exact OS matches for host (If you know what OS is running on it, see

http://www.insecure.org/cgi-bin/nmap-submit.cgi).
TCP/IP fingerprint:
SInfo(V=3.00%P=i686-pc-windows-windows%D=4/6%Time=3E90F171%O=21%C=1)
TSeq(Class=RI%gcd=1%SI=3D37%TS=0)
TSeq(Class=RI%gcd=1%SI=371D%TS=0)
TSeq(Class=RI%gcd=1%SI=3730%TS=0)
T1(Resp=Y%DF=Y%W=FAF0%ACK=S++%Flags=AS%Ops=MNWNNT)
T2(Resp=N)
T3(Resp=Y%DF=Y%W=FAF0%ACK=S++%Flags=AS%Ops=MNWNNT)
T4(Resp=N)
T5(Resp=Y%DF=N%W=0%ACK=S++%Flags=AR%Ops=)
T6(Resp=N)
T7(Resp=N)
PU(Resp=N)

Interesting ports on (194.226.201.199):
(The 1141 ports scanned but not shown below are in state: closed)
Port State Service
25/tcp open smtp
110/tcp open pop-3
137/tcp filtered netbios-ns

138/tcp filtered netbios-dgm
139/tcp filtered netbios-ssn
1434/tcp filtered ms-sql-m
2001/tcp filtered dc
3306/tcp open mysql
10000/tcp open snet-sensor-mgmt
No exact OS matches for host (If you know what OS is running on it, see

http://www.insecure.org/cgi-bin/nmap-submit.cgi).
TCP/IP fingerprint:
SInfo(V=3.00%P=i686-pc-windows-windows%D=4/6%Time=3E90F227%O=25%C=1)
TSeq(Class=TR%IPID=RD%TS=U)
TSeq(Class=TR%TS=U)
T1(Resp=Y%DF=N%W=FFFF%ACK=S++%Flags=AS%Ops=M)
T2(Resp=N)
T3(Resp=Y%DF=N%W=FFFF%ACK=S++%Flags=AS%Ops=M)
T4(Resp=N)
T5(Resp=Y%DF=N%W=0%ACK=S++%Flags=AR%Ops=)
T6(Resp=N)
T7(Resp=N)
PU(Resp=N)

Interesting ports on (210.83.18.98):
(The 1105 ports scanned but not shown below are in state: closed)
Port State Service
7/tcp open echo
9/tcp open discard
13/tcp open daytime
19/tcp open chargen
21/tcp open ftp
23/tcp open telnet
25/tcp open smtp
37/tcp open time
79/tcp open finger
111/tcp open sunrpc
137/tcp filtered netbios-ns
138/tcp filtered netbios-dgm
139/tcp filtered netbios-ssn
256/tcp open FW1-secureremote
257/tcp open FW1-mc-fwmodule

259/tcp open esro-gen
264/tcp open bgmp
265/tcp open maybeFW1
445/tcp filtered microsoft-ds
512/tcp open exec
513/tcp open login
514/tcp open shell
515/tcp open printer
540/tcp open uucp
587/tcp open submission
1720/tcp filtered H.323/Q.931
2201/tcp open ats
4045/tcp open lockd
5800/tcp filtered vnc-http
5900/tcp filtered vnc
6000/tcp open X11
6112/tcp open dtspc
7100/tcp open font-service
32771/tcp open sometimes-rpc5
32772/tcp open sometimes-rpc7
32773/tcp open sometimes-rpc9
32774/tcp open sometimes-rpc11
32775/tcp open sometimes-rpc13
32776/tcp open sometimes-rpc15
32777/tcp open sometimes-rpc17
32778/tcp open sometimes-rpc19
32779/tcp open sometimes-rpc21
32780/tcp open sometimes-rpc23
32786/tcp open sometimes-rpc25
32787/tcp open sometimes-rpc27
Remote operating system guess: Solaris 8 early access beta through actual release
Uptime 6.079 days (since Mon Mar 31 19:45:47 2003)

Warning: OS detection will be MUCH less reliable because we did not find at least 1 open

and 1 closed TCP port
All 1150 scanned ports on p508F3FF2.dip.t-dialin.net (80.143.63.242) are: filtered
Too many fingerprints match this host for me to give an accurate OS guess

Warning: OS detection will be MUCH less reliable because we did not find at least 1 open

and 1 closed TCP port

Interesting ports on dnvr-dsl-gw32-poolb235.dnvr.uswest.net (65.102.250.235):
(The 1146 ports scanned but not shown below are in state: closed)
Port State Service
80/tcp filtered http
137/tcp filtered netbios-ns
138/tcp filtered netbios-dgm
139/tcp filtered netbios-ssn
Too many fingerprints match this host for me to give an accurate OS guess

Warning: OS detection will be MUCH less reliable because we did not find at least 1 open

and 1 closed TCP port
Interesting ports on p508F2CDF.dip.t-dialin.net (80.143.44.223):
(The 1136 ports scanned but not shown below are in state: closed)
Port State Service
21/tcp filtered ftp
23/tcp filtered telnet
25/tcp filtered smtp
79/tcp filtered finger
110/tcp filtered pop-3
135/tcp filtered loc-srv
137/tcp filtered netbios-ns
138/tcp filtered netbios-dgm
139/tcp filtered netbios-ssn
143/tcp filtered imap2
443/tcp filtered https
445/tcp filtered microsoft-ds
5000/tcp filtered UPnP
5303/tcp filtered hacl-probe
Too many fingerprints match this host for me to give an accurate OS guess

Interesting ports on (216.86.160.183):
(The 1142 ports scanned but not shown below are in state: closed)
Port State Service
135/tcp open loc-srv
137/tcp filtered netbios-ns
138/tcp filtered netbios-dgm
139/tcp filtered netbios-ssn
445/tcp open microsoft-ds
1025/tcp open NFS-or-IIS
3389/tcp open ms-term-serv
5000/tcp open UPnP

No exact OS matches for host (If you know what OS is running on it, see

http://www.insecure.org/cgi-bin/nmap-submit.cgi).
TCP/IP fingerprint:
SInfo(V=3.00%P=i686-pc-windows-
windows%D=4/6%Time=3E90F74A%O=135%C=1)
TSeq(Class=RI%gcd=1%SI=43D0%IPID=I%TS=0)
TSeq(Class=RI%gcd=1%SI=416E%IPID=RD%TS=0)
TSeq(Class=RI%gcd=1%SI=43B6%IPID=I%TS=0)
T1(Resp=Y%DF=Y%W=FAF0%ACK=S++%Flags=AS%Ops=MNWNNT)
T2(Resp=N)
T3(Resp=Y%DF=Y%W=FAF0%ACK=S++%Flags=AS%Ops=MNWNNT)
T4(Resp=N)
T5(Resp=Y%DF=N%W=0%ACK=S++%Flags=AR%Ops=)
T6(Resp=N)
T7(Resp=N)
PU(Resp=N)

Interesting ports on sl-gex-burt-1-0.sprintlink.net (144.223.30.134):
(The 1146 ports scanned but not shown below are in state: closed)
Port State Service
23/tcp open telnet
137/tcp filtered netbios-ns
138/tcp filtered netbios-dgm
139/tcp filtered netbios-ssn
No exact OS matches for host (If you know what OS is running on it, see

http://www.insecure.org/cgi-bin/nmap-submit.cgi).
TCP/IP fingerprint:
SInfo(V=3.00%P=i686-pc-windows-windows%D=4/6%Time=3E90F805%O=23%C=1)
TSeq(Class=TR%IPID=Z%TS=U)
T1(Resp=Y%DF=N%W=1020%ACK=S++%Flags=AS%Ops=ME)
T1(Resp=Y%DF=N%W=1020%ACK=S++%Flags=A%Ops=)
T1(Resp=Y%DF=N%W=1020%ACK=S++%Flags=AS%Ops=ME)
T2(Resp=N)
T3(Resp=Y%DF=N%W=1020%ACK=S++%Flags=AS%Ops=M)
T4(Resp=N)
T5(Resp=Y%DF=N%W=0%ACK=S++%Flags=AR%Ops=)
T6(Resp=N)
T7(Resp=N)

PU(Resp=N)

Interesting ports on pc154247.kyunghee.ac.kr (163.180.154.247):
(The 1132 ports scanned but not shown below are in state: closed)

Port	State	Service
25/tcp	open	smtp
119/tcp	open	nntp
135/tcp	open	loc-srv
137/tcp	filtered	netbios-ns
138/tcp	filtered	netbios-dgm
139/tcp	filtered	netbios-ssn
443/tcp	open	https
445/tcp	filtered	microsoft-ds
563/tcp	open	snews
1025/tcp	open	NFS-or-IIS
1029/tcp	open	ms-lsa
1030/tcp	open	iad1
1521/tcp	open	oracle
3372/tcp	open	msdtc
3389/tcp	open	ms-term-serv
5800/tcp	filtered	vnc-http
5900/tcp	filtered	vnc
6666/tcp	filtered	irc-serv

No exact OS matches for host (If you know what OS is running on it, see
http://www.insecure.org/cgi-bin/nmap-submit.cgi).
TCP/IP fingerprint:
SInfo(V=3.00%P=i686-pc-windows-windows%D=4/6%Time=3E90F954%O=25%C=1)
TSeq(Class=RI%gcd=1%SI=2FD9%IPID=I%TS=0)
TSeq(Class=RI%gcd=1%SI=489C%IPID=I%TS=0)
TSeq(Class=RI%gcd=1%SI=2A13%IPID=I%TS=0)
T1(Resp=Y%DF=Y%W=FAF0%ACK=S++%Flags=AS%Ops=MNWNNT)
T2(Resp=N)
T3(Resp=Y%DF=Y%W=FAF0%ACK=S++%Flags=AS%Ops=MNWNNT)
T4(Resp=N)
T5(Resp=Y%DF=N%W=0%ACK=S++%Flags=AR%Ops=)
T6(Resp=N)
T7(Resp=N)
PU(Resp=N)

Warning: OS detection will be MUCH less reliable because we did not find at least 1 open

and 1 closed TCP port
Interesting ports on (211.224.198.97):
(The 1144 ports scanned but not shown below are in state: closed)
Port State Service
137/tcp filtered netbios-ns
138/tcp filtered netbios-dgm
139/tcp filtered netbios-ssn
445/tcp filtered microsoft-ds
5800/tcp filtered vnc-http
5900/tcp filtered vnc
Too many fingerprints match this host for me to give an accurate OS guess

Warning: OS detection will be MUCH less reliable because we did not find at least 1 open

and 1 closed TCP port
Interesting ports on (211.239.151.200):
(The 1148 ports scanned but not shown below are in state: filtered)
Port State Service
53/tcp closed domain
7007/tcp closed afs3-bos
Too many fingerprints match this host for me to give an accurate OS guess
Warning: OS detection will be MUCH less reliable because we did not find at least 1 open and 1 closed TCP port
All 1150 scanned ports on (211.212.196.246) are: filtered
Too many fingerprints match this host for me to give an accurate OS guess

Interesting ports on (210.12.79.125):
(The 1128 ports scanned but not shown below are in state: closed)
Port State Service
7/tcp open echo
9/tcp open discard
13/tcp open daytime
17/tcp open qotd
19/tcp open chargen
21/tcp open ftp
25/tcp open smtp
42/tcp open nameserver
53/tcp open domain
80/tcp open http

135/tcp open loc-srv
137/tcp filtered netbios-ns
138/tcp filtered netbios-dgm
139/tcp filtered netbios-ssn
443/tcp open https
445/tcp open microsoft-ds
1025/tcp open NFS-or-IIS
1029/tcp open ms-lsa
1032/tcp open iad3
1723/tcp open pptp
3372/tcp open msdtc
3389/tcp open ms-term-serv
Remote OS guesses: FreeBSD 2.2.1 - 4.1, Windows Millennium Edition (Me), Win 2000, or WinXP

Insufficient responses for TCP sequencing (0), OS detection may be less accurate
Interesting ports on (212.38.93.242):
(The 1130 ports scanned but not shown below are in state: closed)
Port State Service
21/tcp open ftp
25/tcp open smtp
53/tcp open domain
80/tcp open http
88/tcp open kerberos-sec
135/tcp open loc-srv
137/tcp filtered netbios-ns
138/tcp filtered netbios-dgm
139/tcp filtered netbios-ssn
389/tcp open ldap
445/tcp open microsoft-ds
464/tcp open kpasswd5
593/tcp open http-rpc-epmap
636/tcp open ldapssl
1026/tcp open LSA-or-nterm
1029/tcp open ms-lsa
3268/tcp open globalcatLDAP
3269/tcp open globalcatLDAPssl
5631/tcp open pcanywheredata
65301/tcp open pcanywhere
Remote OS guesses: F5 labs BigIp Load balancer Kernel 4.1.1PTF-03 (X86), FreeBSD 2.2.1 -

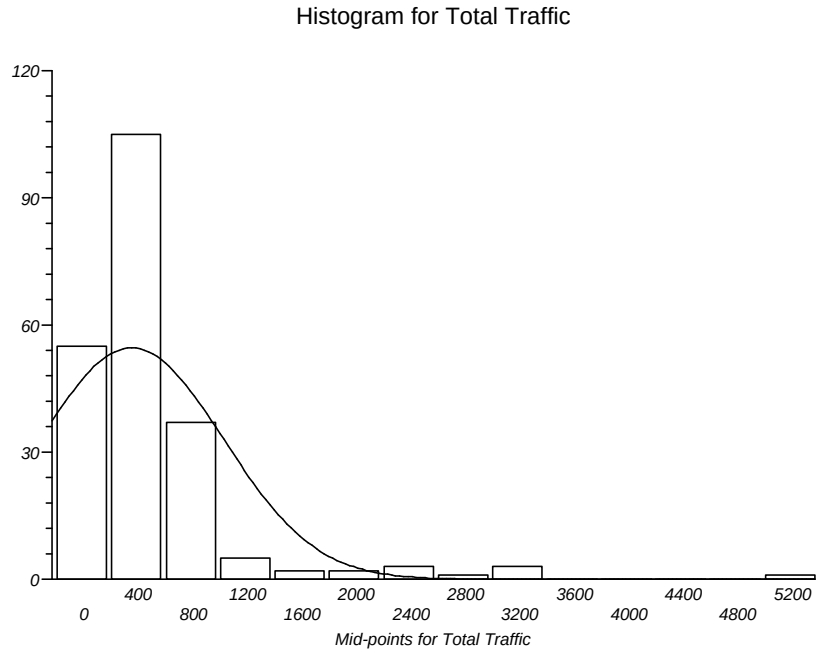
4.1, FreeBSD 2.1.0 - 2.1.5, Windows Millennium Edition (Me), Win 2000, or WinXP

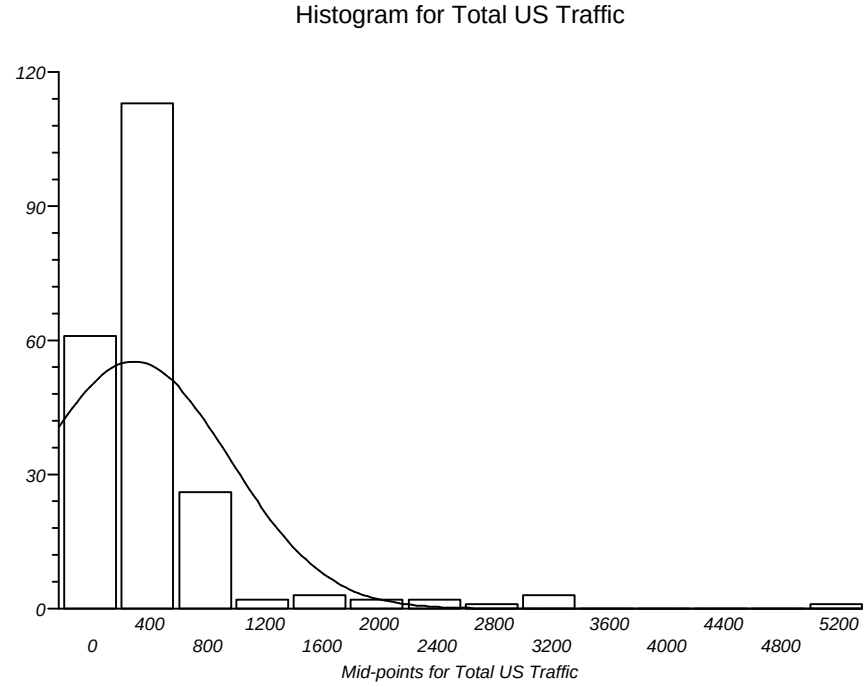
Warning: OS detection will be MUCH less reliable because we did not find at least 1 open and 1 closed TCP port
All 1150 scanned ports on (203.235.98.2) are: filtered
Too many fingerprints match this host for me to give an accurate OS guess

Interesting ports on (211.49.46.194):
(The 1139 ports scanned but not shown below are in state: closed)
Port State Service
20/tcp filtered ftp-data
80/tcp filtered http
135/tcp open loc-srv
137/tcp filtered netbios-ns
138/tcp filtered netbios-dgm
139/tcp filtered netbios-ssn
445/tcp open microsoft-ds
1025/tcp open NFS-or-IIS
5000/tcp open UPnP
6699/tcp filtered napster
8080/tcp filtered http-proxy
No exact OS matches for host (If you know what OS is running on it, see http://www.insecure.org/cgi-bin/nmap-submit.cgi).
TCP/IP fingerprint:
SInfo(V=3.00%P=i686-pc-windows-windows%D=4/7%Time=3E9107E9%O=135%C=1)
TSeq(Class=RI%gcd=1%SI=2CAC%TS=0)
TSeq(Class=RI%gcd=1%SI=3B1B%TS=0)
TSeq(Class=RI%gcd=1%SI=70C4%TS=0)
T1(Resp=Y%DF=Y%W=FAF0%ACK=S++%Flags=AS%Ops=MNWNNT)
T2(Resp=N)
T3(Resp=Y%DF=Y%W=FAF0%ACK=S++%Flags=AS%Ops=MNWNNT)
T4(Resp=N)
T5(Resp=Y%DF=N%W=0%ACK=S++%Flags=AR%Ops=)
T6(Resp=N)
T7(Resp=N)
PU(Resp=N)

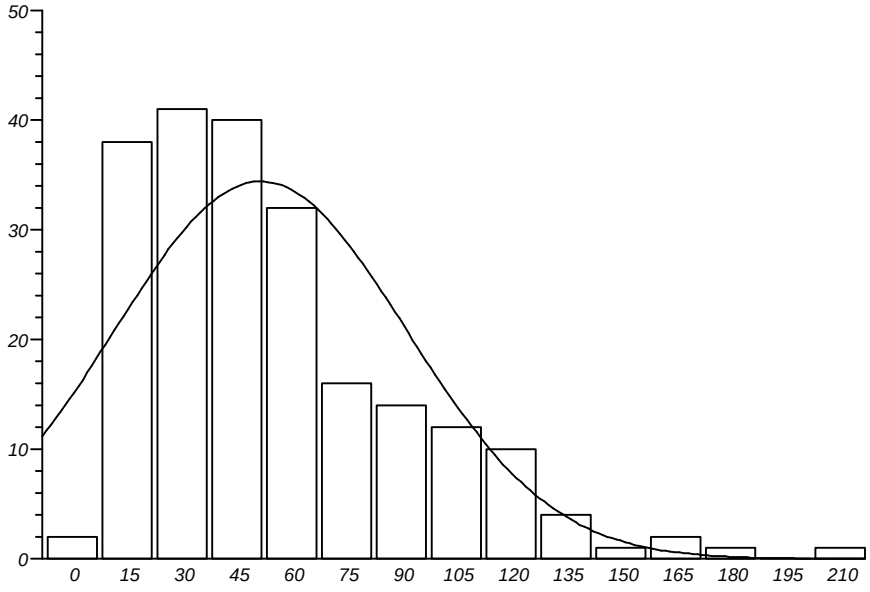
Nmap run completed at Mon Dec 30 00:08:57 2003 -- 99 IP addresses (27 hosts up) scanned in 10873 seconds

Histograms of Total and Attack Traffic

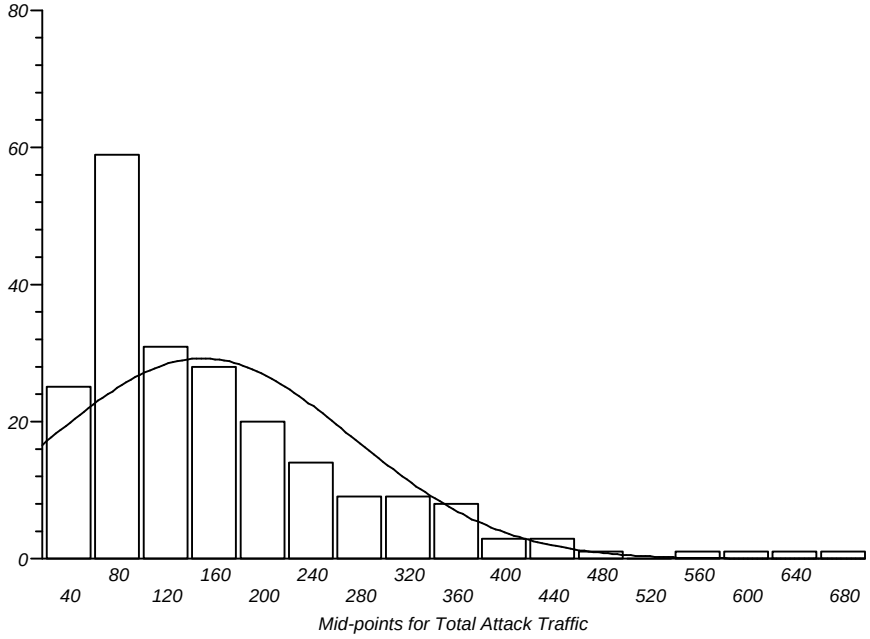




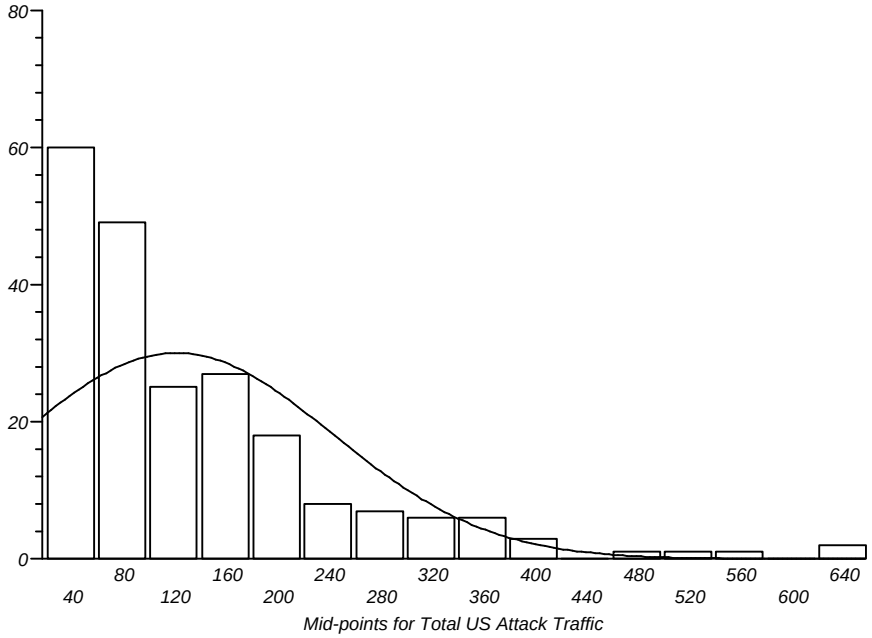
Histogram for Total Foreign Traffic



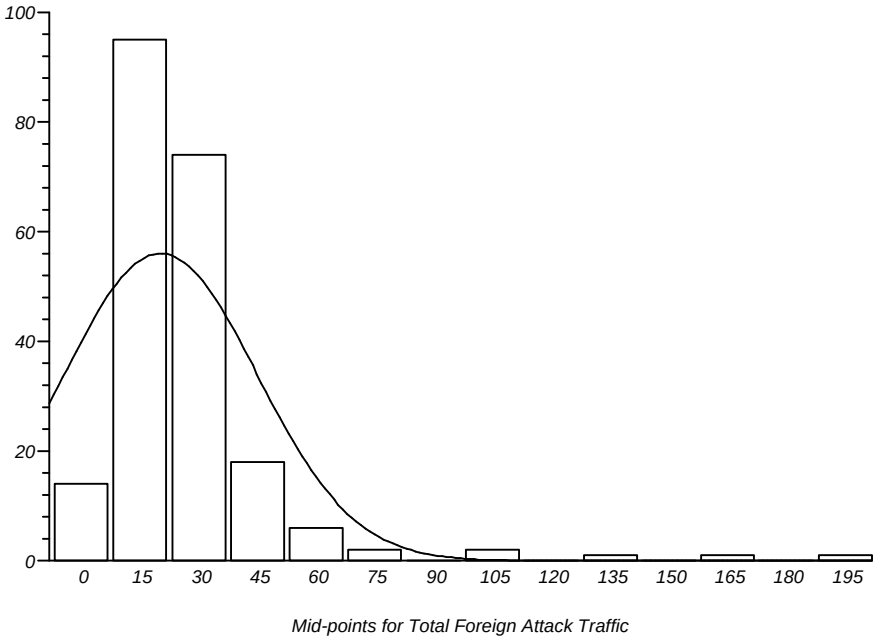
Histogram for Total Attack Traffic



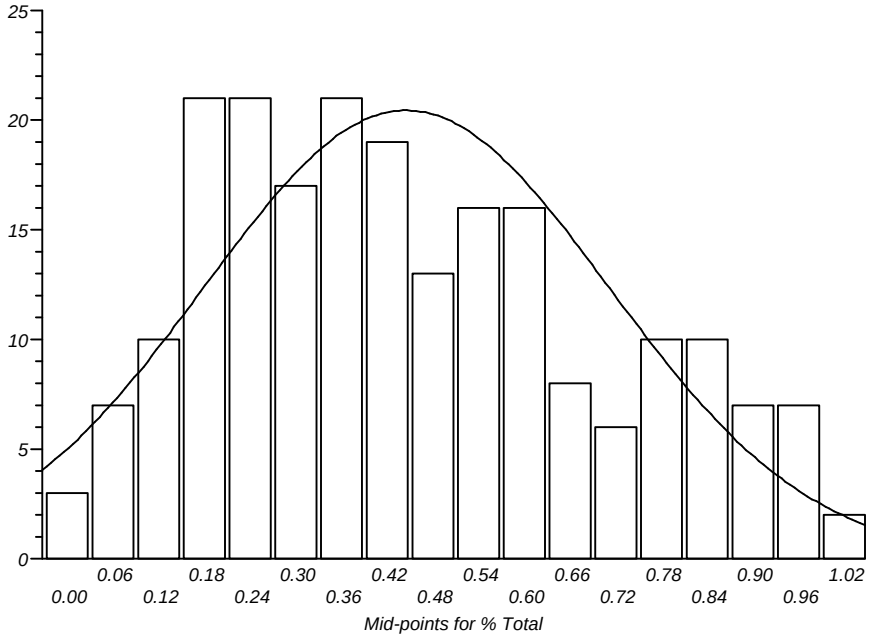
Histogram for Total US Attack Traffic



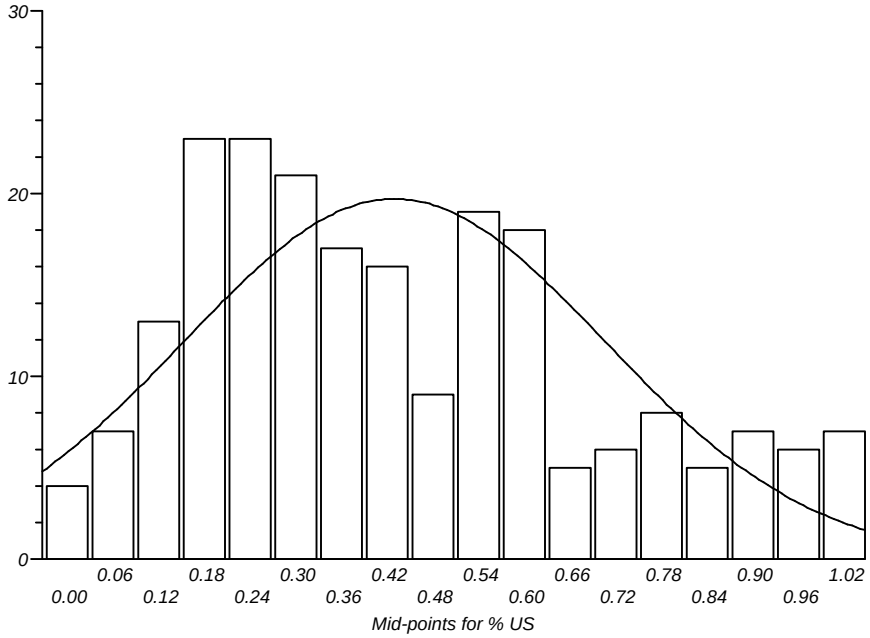
Histogram for Total Foreign Attack Traffic



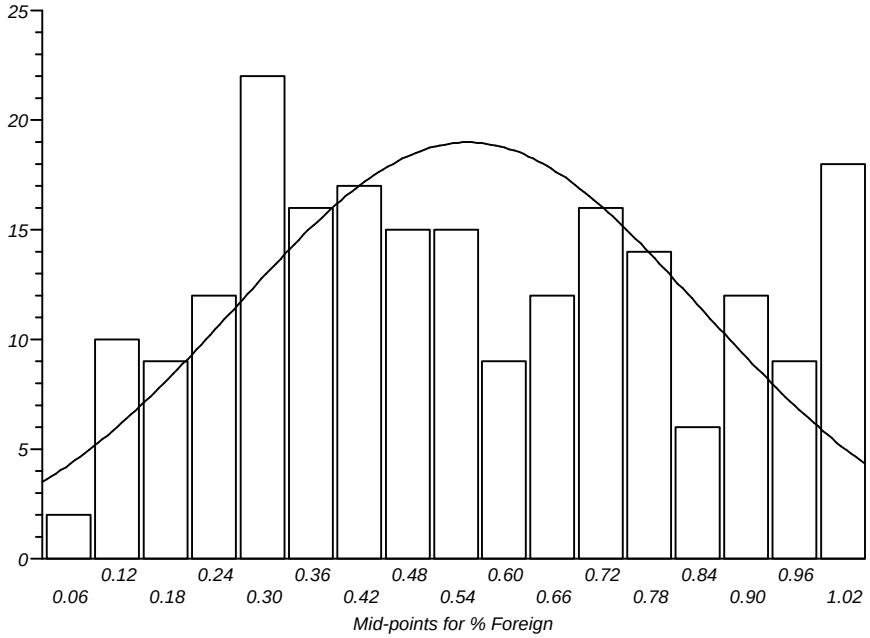
Histogram for % Total



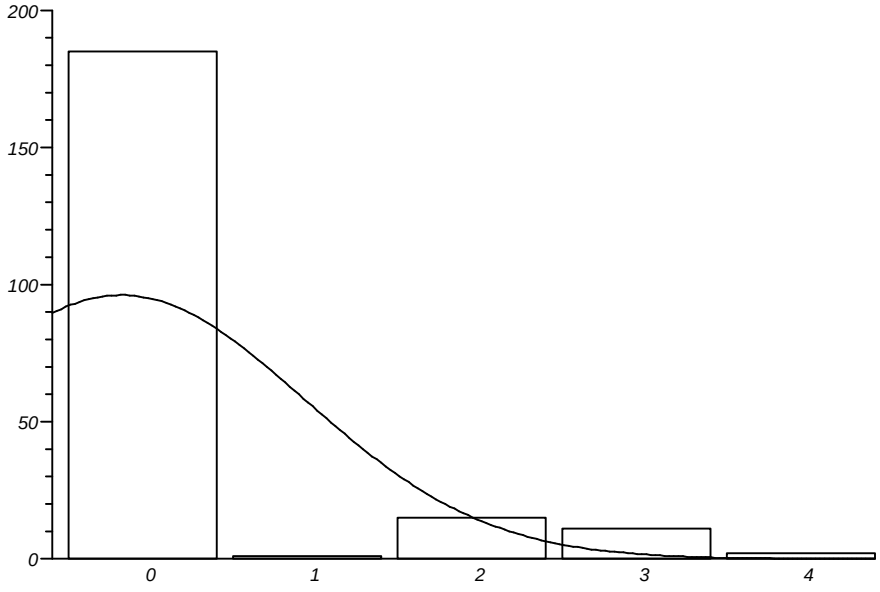
Histogram for % US



Histogram for % Foreign

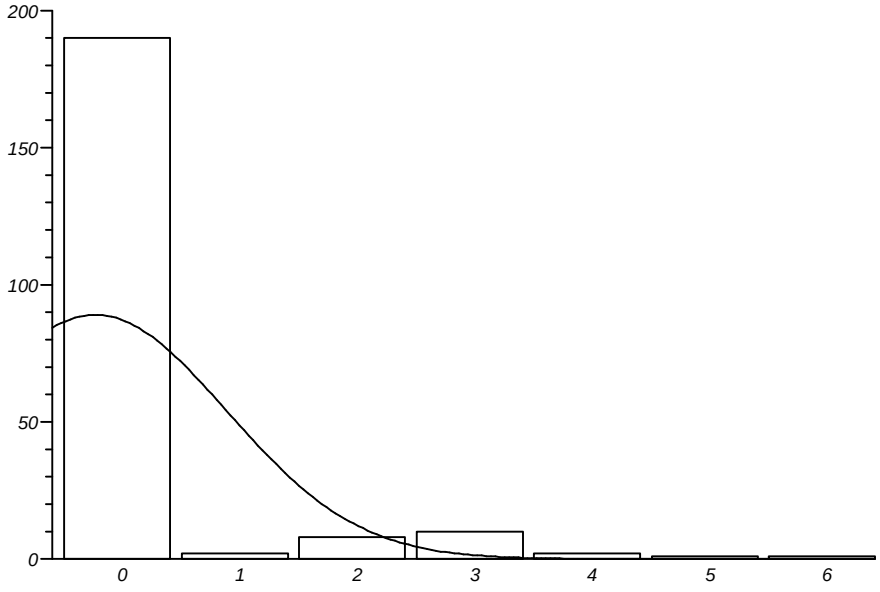


Histogram for US SMTP Traffic



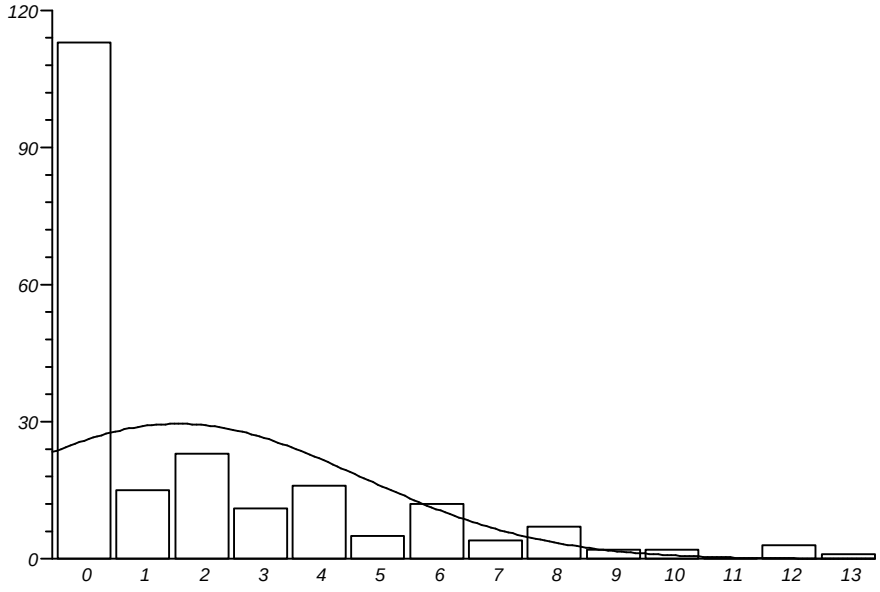
Mid-points for US SMTP Traffic

Histogram for Foreign SMTP Traffic

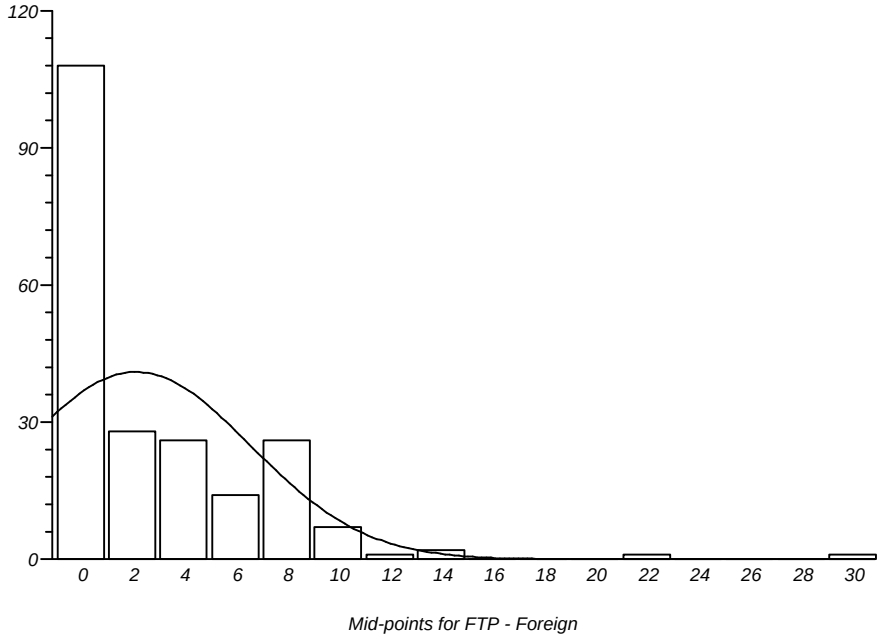


Mid-points for Foreign SMTP Traffic

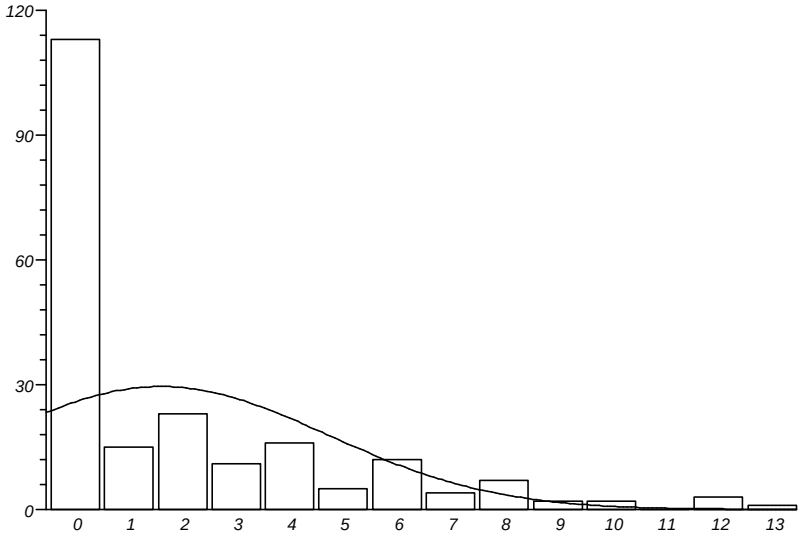
Histogram for FTP - US



Histogram for FTP - Foreign

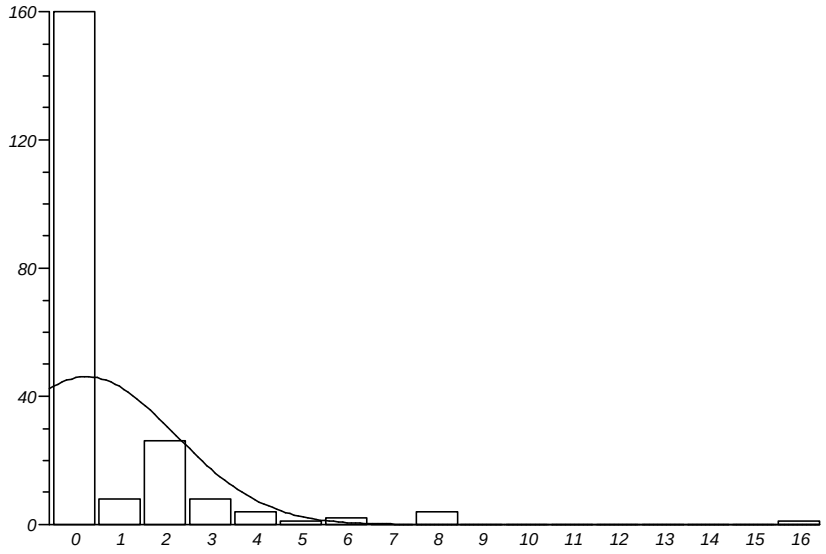


Histogram for SSH - US



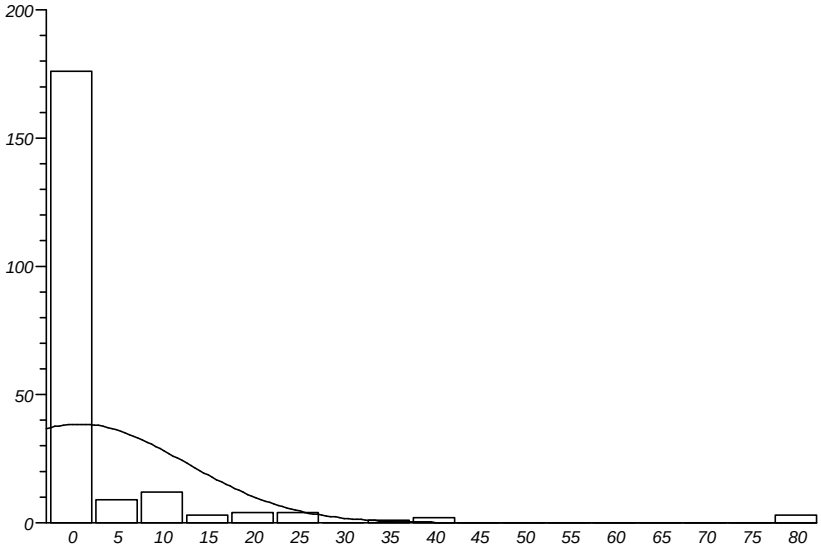
Mid-points for SSH - US

Histogram for SSH - Foreign

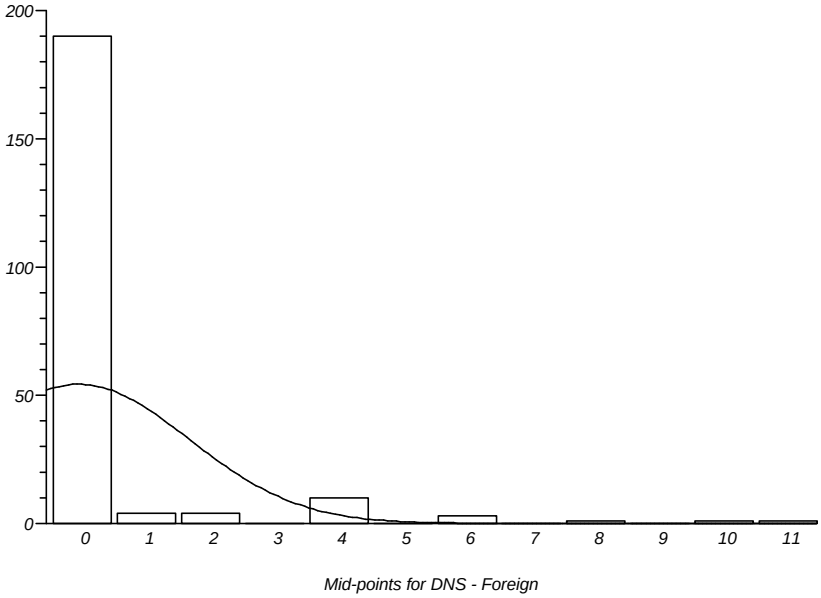


Mid-points for SSH - Foreign

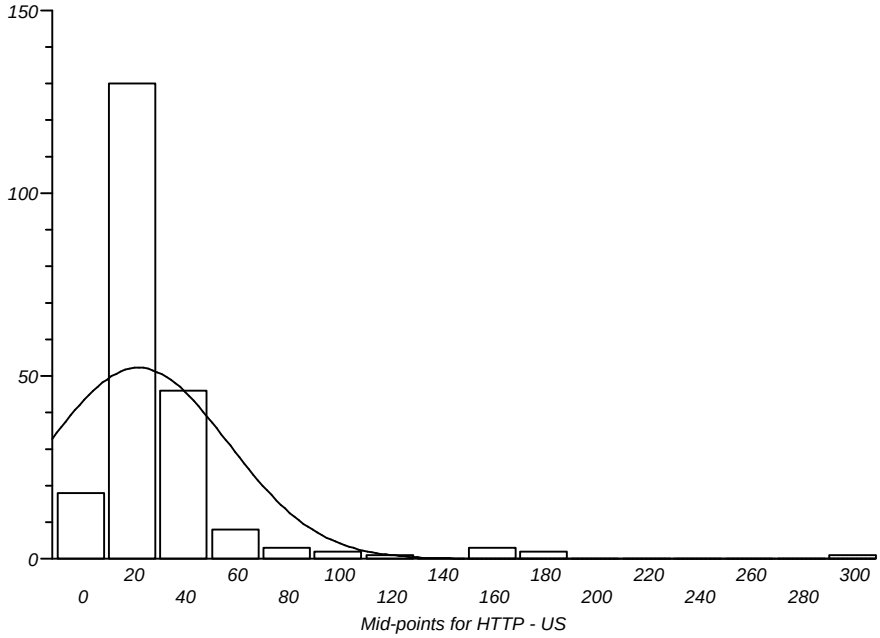
Histogram for DNS - US



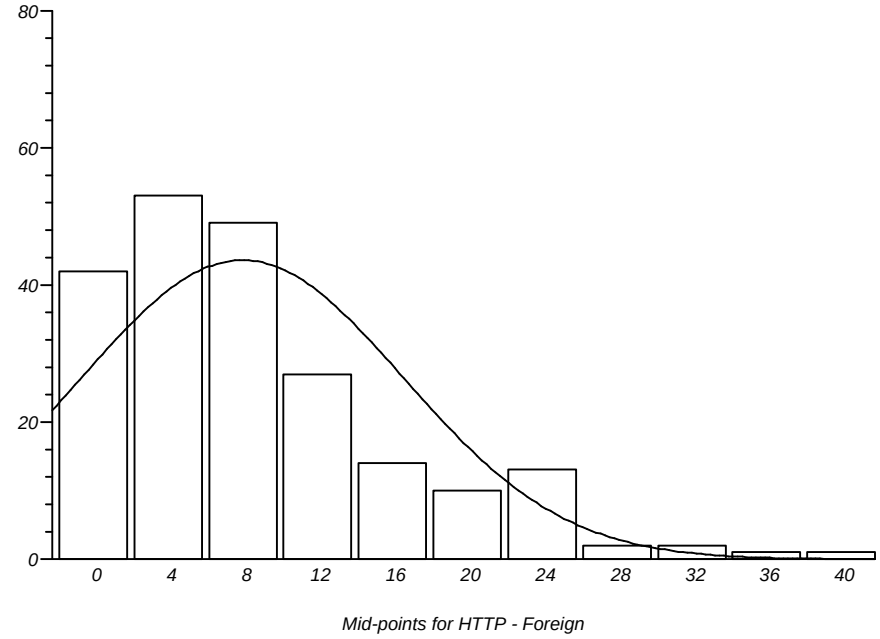
Histogram for DNS - Foreign



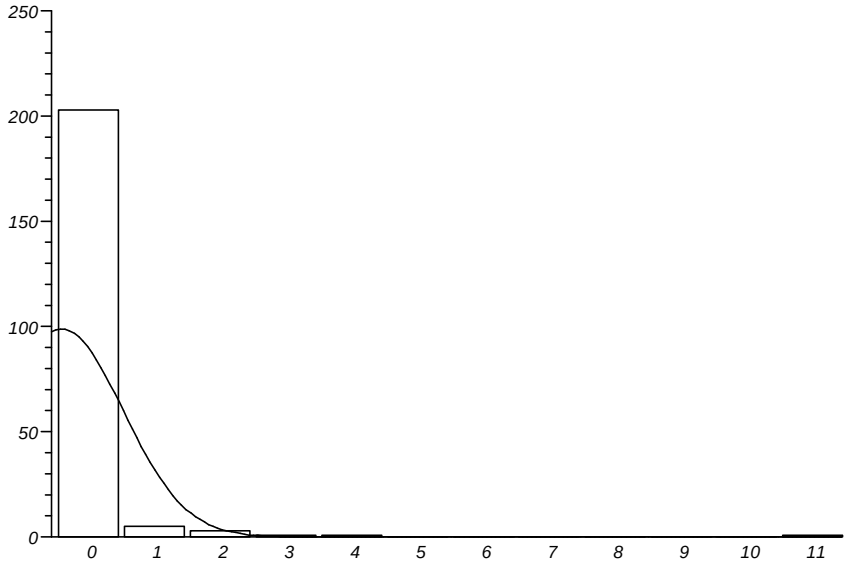
Histogram for HTTP - US



Histogram for HTTP - Foreign

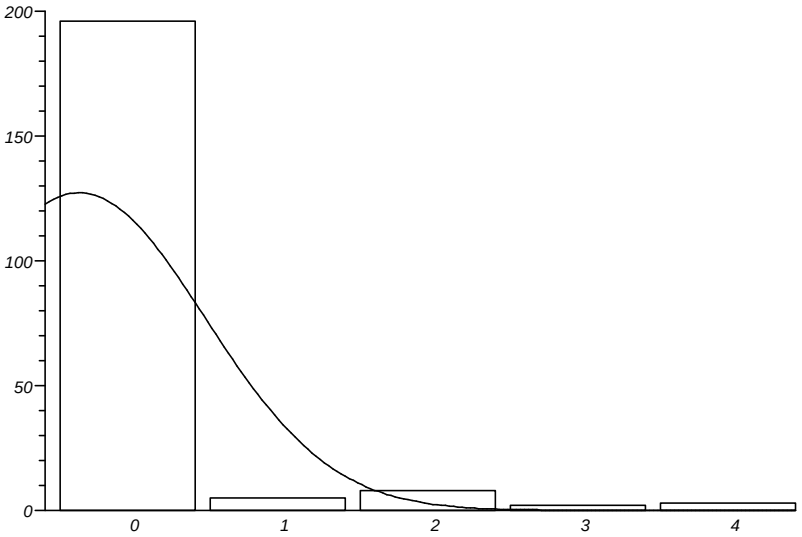


Histogram for RPC - US



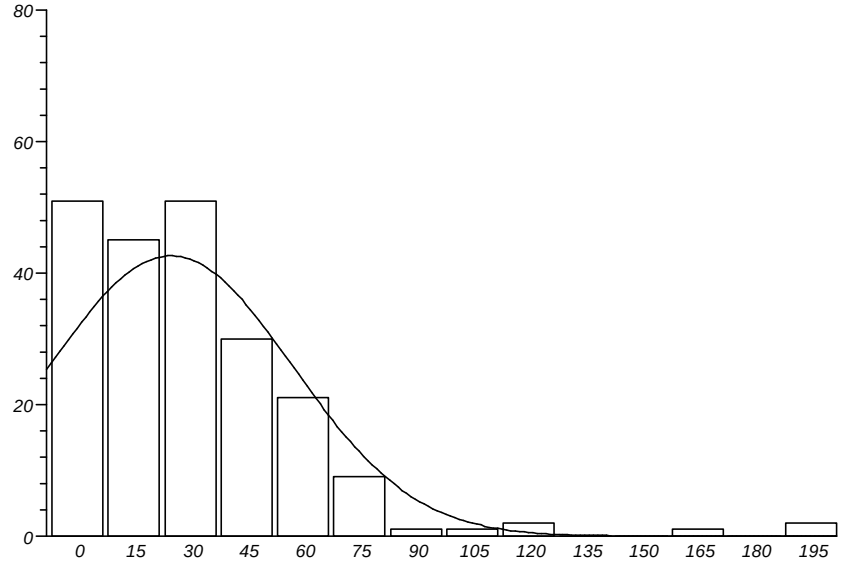
Mid-points for RPC - US

Histogram for RPC - Foreign

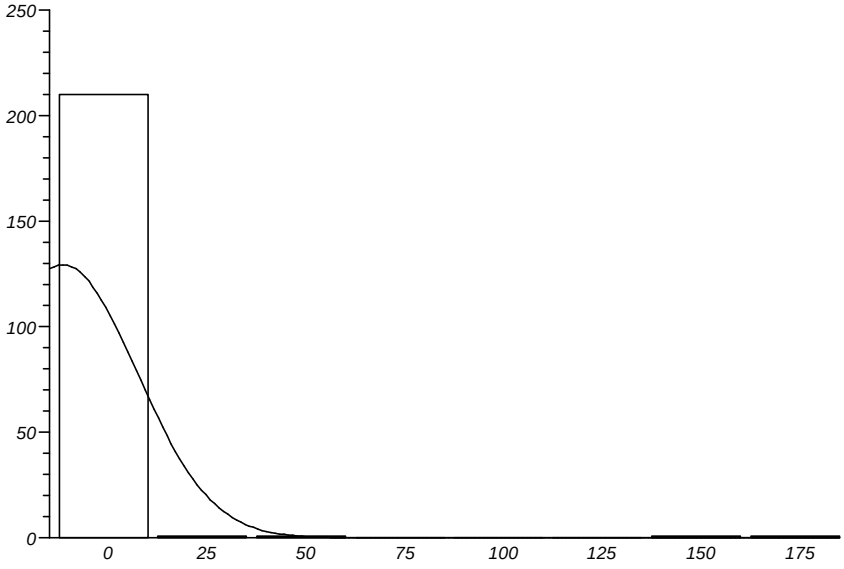


Mid-points for RPC - Foreign

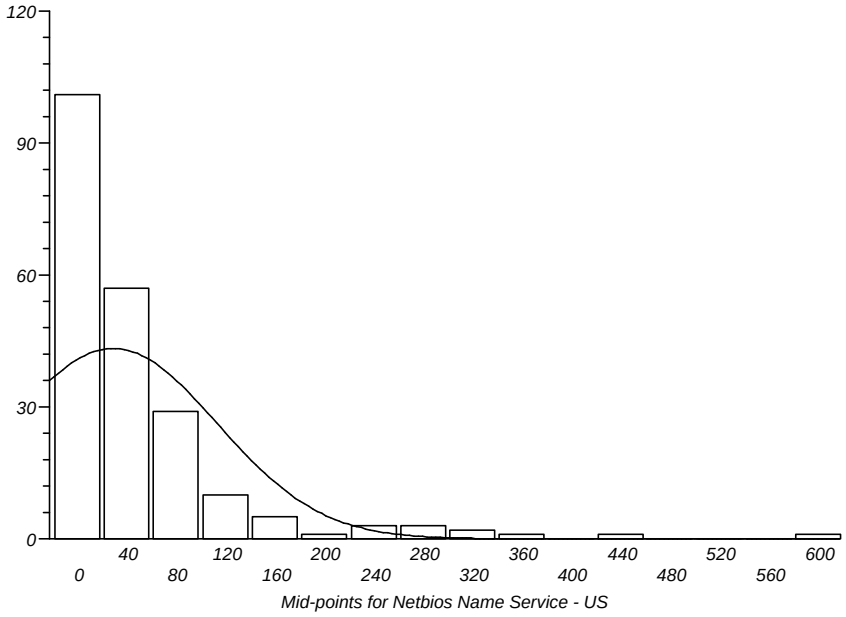
Histogram for Authent - US



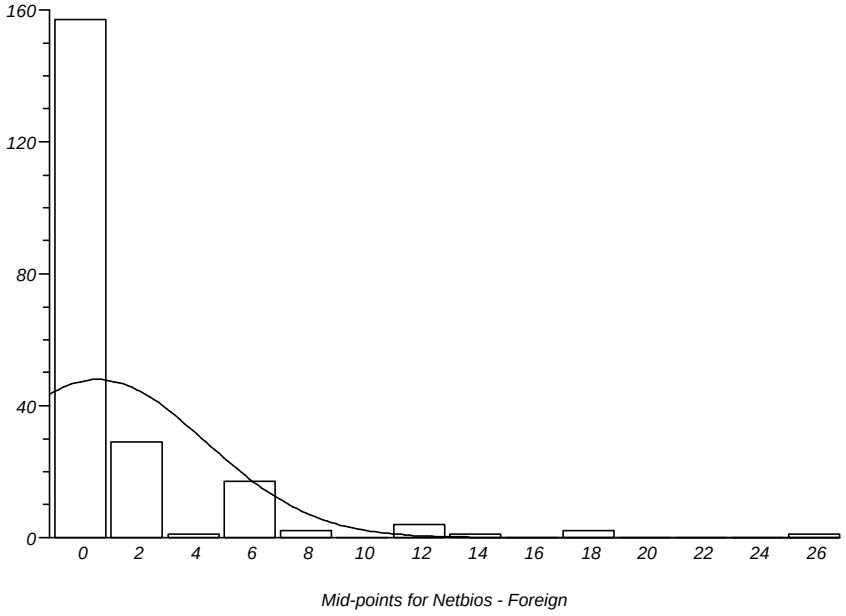
Histogram for Authent - Foreign



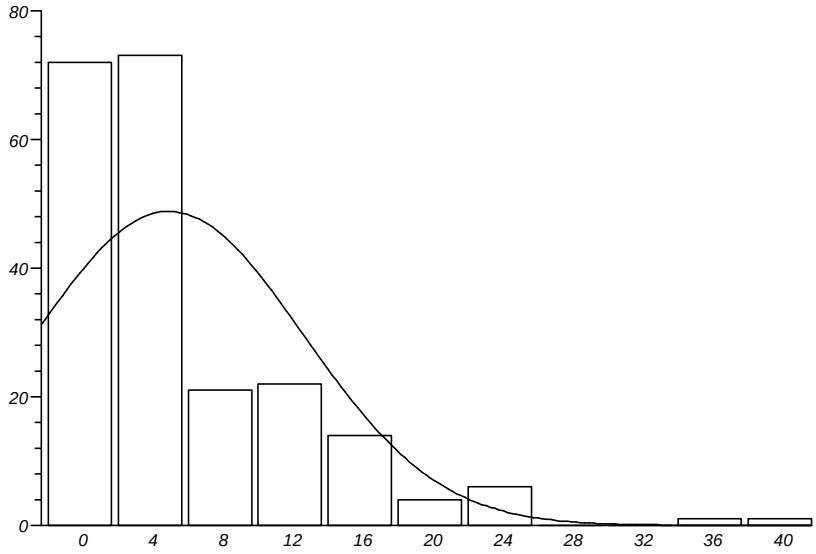
Histogram for Netbios Name Service - US



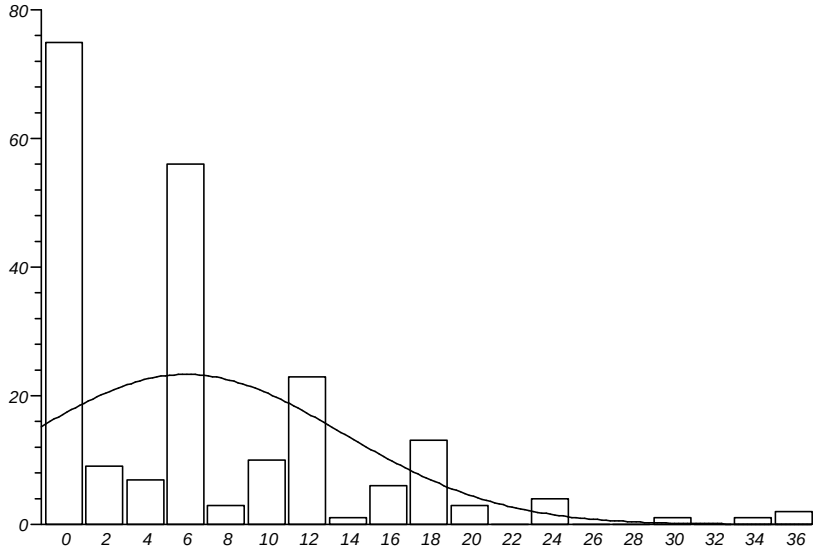
Histogram for Netbios Name Service - Foreign



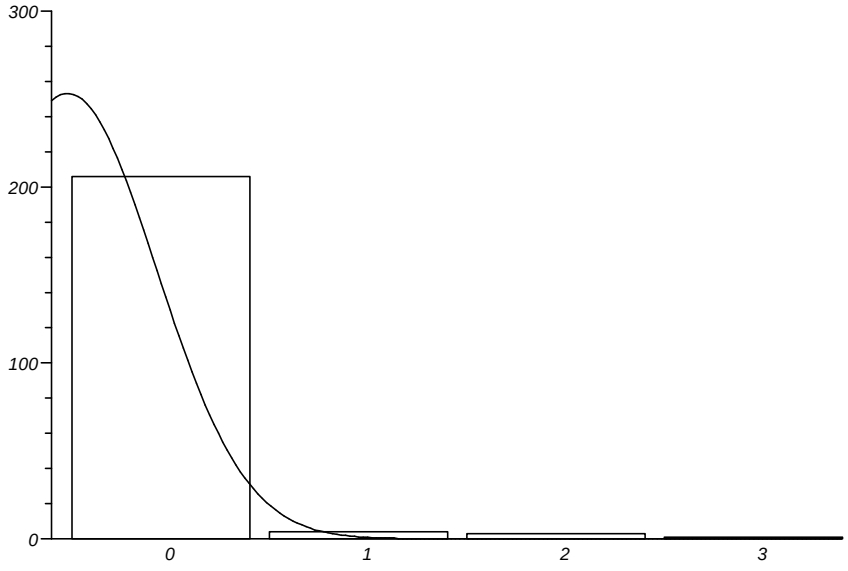
Histogram for MS-SQL - US



Histogram for MS-SQL - Foreign

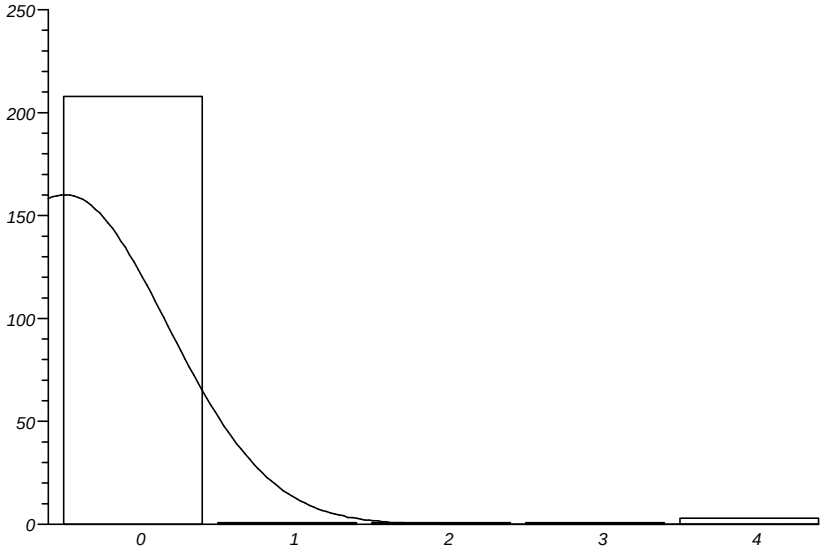


Histogram for SubSeven - US



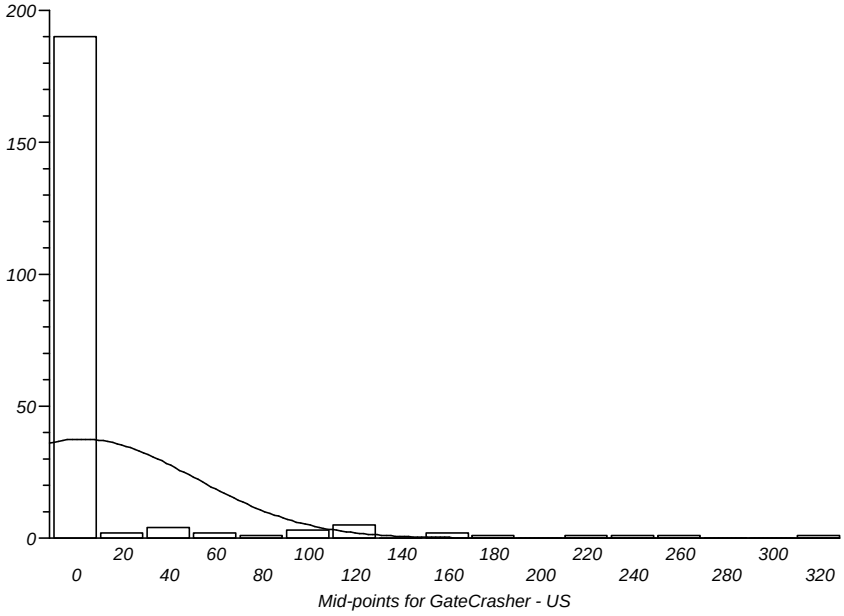
Mid-points for SubSeven - US

Histogram for SubSeven - Foreign



Mid-points for SubSeven - Foreign

Histogram for GateCrasher - US



Histogram for GateCrasher - Foreign