

The Essentials of Network Security

Introduction

With the current growth of the Internet and e-commerce, networks are becoming increasingly vulnerable to damaging attacks. At the same time, downtime from networks that carry critical business applications can result in production losses and directly affect a company's bottom line. Computer viruses, denial-of-service (DoS) attacks, vindictive employees, and human error all present dangers to networks. No individual—whether a noncomputer user, a casual Internet surfer, or even a large enterprise—is immune to network-security breaches. With proper planning, however, network security breaches can often be prevented.

This paper provides a general overview of the most common network security threats and recommends steps you can take to decrease these threats and to mitigate exposure to risks through active design and prevention.

The Importance of Security

In 1999, the U.S. Federal Bureau of Investigation (FBI) reported U.S.\$265 million in verifiable losses due to computer security breaches in U.S. companies, more than double the losses in 1998. The following survey from the Computer Security Institute (CSI) documents the scope of the problem.

The CSI team surveyed 538 computer security practitioners in U.S. corporations, government agencies, financial institutions, medical institutions, and universities, and reported its results in the 2001¹ Computer Crime and Security Survey. The goal of this effort is to raise the level of computer security awareness and to help determine the scope of computer crime in the United States. The following statistics demonstrate that the threat from computer crime and other information security breaches continues unabated and that the financial toll is mounting.

- Thirty-five percent of respondents quantified their financial losses.
- Respondents reported a total of U.S.\$377,828,700 in financial losses. In contrast, the losses from the 249 respondents in the 2000 survey totaled only U.S.\$265,589,940. The average annual total from 1997-1999 was U.S.\$120,240,180.
- Eighty-five percent of respondents, primarily large corporations and government agencies, detected computer security breaches within the last 12 months.
- Sixty-four percent of respondents acknowledged financial losses due to computer security breaches.

¹ The 2001 Computer Crime and Security Survey was conducted by CSI with the participation of the San Francisco office of the FBI's Computer Intrusion Squad.



- Forty percent of respondents detected system penetration from outside sources. Only 25 percent reported this type of system penetration in the 2000 survey.
- Thirty-eight percent of respondents detected DoS attacks. Only 27 percent reported DoS attacks in the 2000 survey.
- Ninety-one percent of respondents detected employee abuse of Internet access privileges; for example, downloading pornography or pirated software, or inappropriate use of e-mail systems. Only 79 percent detected Internet abuse in the 2000 survey.
- Ninety-four percent of respondents detected computer viruses. Only 85 percent detected them in the 2000 survey.

Real and Imagined Threats from the Internet

The Internet has undoubtedly become the largest public data network in the world, enabling and facilitating both personal and business communications worldwide. The volume of traffic moving over the Internet and corporate networks is expanding exponentially every day as mobile workers, telecommuters, and branch offices use e-mail and the Internet to remotely connect to corporate networks. Commercial transactions completed over the Internet now account for a significant percentage of many companies' revenue.

Widespread use of the Internet has opened the door to an increasing number of security threats. The consequences of attacks range from inconvenient to debilitating. Important data can be lost, privacy can be violated, and several hours—or even days—of network downtime can ensue. Gartner Group expects that by 2003, more than 50 percent of small and midsize enterprises using the Internet for more than e-mail will experience a successful Internet attack.

The fear of a security breach, however, can be just as debilitating to a business as an actual breach. General fear and suspicion of computers still exists and with that comes a distrust of the Internet. This distrust can limit the business opportunities for companies, especially those that are completely Web-based. Giving credit-card information to a telemarketer over the phone or to a waiter in a restaurant can be more risky than submitting the information via a Web site. Electronic commerce transactions are usually protected by security technology, while waiters and telemarketers are not always monitored or trustworthy. Companies must enact security policies and incorporate safeguards that are not only effective, but are also *perceived* as effective.

Government Regulations

To combat abuse, national governments are currently developing laws intended to regulate the vast flow of electronic information found on the Internet. In an effort to accommodate government regulations, The network security industry has developed a portfolio of security standards to not only help to secure data, but also to prove that it is secure. Ultimately, businesses that do not demonstrate security policies that protect their data will be in breach of these standards.

Threats to Data

As with any type of crime, threats come from a minority of the population. However, while one car thief can steal only one car at a time, a single hacker working from a basic computer can damage a large number of computer networks and wreak havoc around the world.

Hackers

This generic and often glamorized term applies to computer enthusiasts who take pleasure in gaining access to other people's computers or networks. Many hackers are content with simply breaking in and leaving evidence of their intrusion; such evidence might consist of joke applications or messages on computer desktops. Other hackers, often referred to as "crackers," are more malicious, crashing entire computer systems, stealing or damaging confidential data, defacing Web pages, and ultimately disrupting business. Some amateur hackers cause damage by merely locating hacking tools online and deploying them without much understanding of how they work or their effects.

Employees

Most network security experts claim that employees who work inside corporations where breaches have occurred initiate the majority of network attacks. Employees, through mischief, malice, or mistake, often manage to damage their own companies' networks and destroy data. With the recent pervasiveness of remote connectivity technologies, the risk is even greater. Businesses are expanding to give larger numbers of telecommuters, branch offices, and business partners access to their networks. These remote employees and partners pose the same threats as internal employees. They risk creating security breaches, either intentionally or inadvertently. Companies must review their remote-networking assets to be sure they are properly secured and monitored.

Unaware Staff

Employees often overlook standard network security rules. For example, they might choose passwords that are simple to remember, to log on to their networks easily. Such passwords might be easy to guess or to crack by hackers using simple common sense or a widely available password-cracking software utility.

Employees can also cause security breaches by accidentally contracting and spreading computer viruses. Two of the most common ways to pick up a virus are from a floppy disk or by downloading files from the Internet. Employees who transport data via floppy disks can inadvertently infect corporate networks with viruses they picked up from computers in copy centers or libraries, without even knowing the viruses are on their PCs. Employees who download files from the Internet, including JPEG files, jokes, and executable images, risk infecting corporate networks.

Companies must also be wary of human error. Employees, whether computer novices or computer savvy, can erroneously install virus protection software or accidentally overlook warnings regarding security threats. Security-conscious companies take the time to document security policies and educate every employee.

Disgruntled Staff

Far more unsettling than the prospect of employee error causing harm to a network is the potential for an angry or vengeful staff member to inflict damage. Angry employees, often those who have been reprimanded, fired, or laid off, might intentionally infect corporate networks with viruses or delete crucial files. This population is especially dangerous because it is generally far more aware of the network, the value of the information within it, and the location of and safeguards protecting high-priority information.

Snoops

Employees known as “snoops” sometimes partake in corporate espionage, gaining unauthorized access to confidential data in order to provide competitors with otherwise inaccessible information. Snoops might be simply satisfying their personal curiosities by accessing private information, such as financial data, a romantic e-mail correspondence between coworkers, or the salary of a colleague. Some of these activities are relatively harmless, but others, such as previewing private financial or human resources data, are far more serious and can be damaging to reputations and cause financial liability for a company.

Known Security Holes

Individuals or groups who are intent on exploiting a network do not need to create new ways to attack; they can easily leverage known, published problems. In fact, most issues relating to hacker attacks are traceable to a small number of well-documented security holes that may be months, if not years, old. Fixing known security holes can completely prevent these attacks.

For example, SANS Institute known as the System Administration, Networking and Security—<http://www.sans.org> found that in 1999, as many as 50 percent of Domain Name System (DNS) servers were running vulnerable copies of the popular Berkeley Internet Name Domain program, yet this same warning appears on the SAN’s watch list today, several years later.

A little over a year ago, the SANS Institute and the National Infrastructure Protection Center (NIPC) released a document summarizing the Ten Most Critical Internet Security Vulnerabilities. Thousands of organizations used that list to prioritize their efforts so they could close the most dangerous holes first. This new list, released on October 1, 2001, updates and expands the Top Ten list. Cisco Systems along with many other credible security teams in the U.S. participated in this research and is helping to determine what should be on this list. With this new release they have increased the list to the Top Twenty vulnerabilities, and have segmented it into three categories: General Vulnerabilities, Windows Vulnerabilities, and Unix Vulnerabilities.

The SANS/FBI Top Twenty list is valuable because the majority of successful attacks on computer systems via the Internet can be traced to exploitation of security flaws on this list. For instance, system compromises in the Solar Sunrise Pentagon hacking incident and the easy and rapid spread of the Code Red and NIMDA worms can be traced to exploitation of unpatched vulnerabilities on this list.

During a briefing at FBI headquarters in July 2001, security expert John Collingwood, FBI Assistant Director for Public Affairs, stated that the Russian Mafia had infiltrated many businesses in the former Soviet Union. These types of groups are becoming more sophisticated and are extending their reach to the United States and other western countries. Collingwood further stated that these hackers are exploiting unpatched Microsoft Windows NT operating systems through holes that have been documented and that have had fixable patches since 1998.

Destructive Code

It is easy to pass destructive viruses to an unsuspecting client. Many would-be hackers use this method to spread problems, expose critical content or put the performance of a network at risk.

Viruses

Viruses are the most widely known security threats because they often generate extensive press coverage. Viruses are computer programs designed to replicate themselves and infect computers when triggered by a specific event. For example, viruses called *macro viruses* attach themselves to files that contain macro instructions (routines that can be repeated automatically, such as mail merges) and are activated every time the macro runs. The effects of some viruses are relatively benign and cause annoying interruptions such as displaying a comical message when striking a certain letter on the keyboard. Other viruses are more destructive and cause problems such as deleting files from a hard drive or slowing down a system.

A virus can only infect a network if the virus enters the network through an outside source—most often through an infected floppy disk or a file downloaded from the Internet. When one computer on the network becomes infected, the other computers on the network are highly susceptible to contracting the virus.

Trojan Horse Programs

Trojan horse programs, known as “Trojans,” are delivery vehicles for destructive code. Trojans appear to be harmless or even useful software programs, such as computer games, but are actually enemies in disguise. Trojans can delete data, mail copies of themselves to e-mail address lists, and open up computers to additional attacks. Trojans can be contracted only by copying the Trojan horse program to a system via a disk, downloading from the Internet, or opening an e-mail attachment. Neither Trojans nor viruses can be spread through an e-mail message itself—they are spread only through e-mail attachments.

Vandals

A “vandal” is a software application or applet that causes destruction of varying degrees. It can destroy just a single file, or a major portion of a computer system. Web sites have come alive through the development of software applications such as ActiveX and Java Applets. These devices enable animation and other special effects to run, making Web sites more attractive and interactive. However, the ease with which these applications can be downloaded and run has provided a new vehicle for inflicting damage.

Network Attacks

Network attacks are commonly classified in three general categories: reconnaissance attacks, access attacks, and DoS attacks.

Reconnaissance Attacks

Reconnaissance attacks are information-gathering activities by which hackers collect data that is later used to compromise networks. Usually software tools such as sniffers and scanners are used to map out network resources and exploit potential weaknesses in targeted networks, hosts, and applications. For example, software exists that is specifically designed to crack passwords. This software was created for network administrators to assist employees who have forgotten their passwords or to determine the passwords of employees who have left the company without disclosing their passwords. Placed in the wrong hands, however, this software can become a dangerous weapon.



Access Attacks

Access attacks are conducted to exploit vulnerabilities in network areas such as authentication services and File Transfer Protocol (FTP) functionality. Access attacks are used to gain entry into e-mail accounts, databases, and other sources of confidential information.

Denial of Service Attacks

DoS attacks prevent access to part or all of a computer system. DoS attacks are usually achieved by sending large amounts of jumbled or otherwise unmanageable data to a machine that is connected to a corporate network or the Internet, blocking legitimate traffic from getting through. Even more malicious is a distributed denial of service attack (DDoS), in which the attacker compromises multiple machines or hosts.

In its May 24, 2001 newsletter, *ISP World News* reported on a study, conducted by Asta Networks and the University of California, San Diego, that assessed the number of DoS attacks in the world and characterized DoS attack behavior. According to the study, attacks range from large Internet companies—such as AOL, Akamai, and Amazon.com—to small ISPs that serve small to medium-sized businesses. The study showed that a significant percentage of attacks are directed against network infrastructure components, including domain-name servers and routers.

The following are some of the findings from the Asta study:

- DoS attacks can range from minutes to several days; most attacks are short in duration, less than 10 minutes to less than 1 hour
- No country is immune; Web sites in Romania were hit as frequently as .net and .com sites; Brazil was targeted more than .edu and .org sites combined; targets in Canada, Germany, the UK, Belgium, Switzerland, New Zealand, and China were all compromised
- Most targets are attacked multiple times, as high as 70 to 100 times per incident

Data Interception

Data transmitted via any type of network can be subject to interception by unauthorized parties. The perpetrators might eavesdrop on communications or alter the data packets being transmitted. Perpetrators can use various methods to intercept the data. IP *spoofing*, for example, entails posing as an authorized party in the data transmission by using the Internet Protocol (IP) address of one of the data recipients.

Social Engineering

Social engineering, in this context, is the increasingly prevalent act of obtaining confidential network security information through non-technical means. For example, a social engineer might pose as a technical-support representative and make calls to employees to gather password information. Other examples of social engineering include bribing a coworker to gain access to a server or searching a colleague's office to find a password that has been written in a hidden spot.

Unsolicited Mail

Spam is the commonly used term for unsolicited e-mail or the action of broadcasting unsolicited advertising messages via e-mail. Spam is usually harmless, but it can be a nuisance, taking up the recipient's time, costing company money in wasted human-resource time, and compromising network storage space allotted for business use.

Security Tools

No matter what tools and gadgets you purchase to help secure your network, whether it is expensive, sophisticated software, a secure firewall, or an intrusion detection system (IDS), you cannot overlook the damage that can be created by human error. Technology and networks are prone to human failure. How do you best protect your networks from the humans needed to manage them?

People-security and technical-security are often treated separately, yet both must be considered in putting together your corporate strategy. For example, does your network know if a user tries to log on in two separate locations at the same time? This would be a clear indication that something may be compromised. Can an employee who forgot to log off in the office access the network from home or from someone else's machine? Can a technically savvy user bypass or remove anti-virus software without being detected? Whether these events are malicious or errant policy, the results are the same: improper security implementation.

Biometrics

More and more companies are using highly sophisticated technologies to track employees and increase security. To have a truly secure environment and reduce your security risk, you must know where your users are, electronically and physically, and whether they are following defined security policy.

For example, biometric security systems that verify a person's identity by scanning fingers, hands, faces or eyes are predicted to grow from revenues of U.S.\$228 million in 2000 to more than U.S.\$520 million by 2005. This growth is coming primarily from government entities in the law enforcement arena, but large enterprise companies are starting to show interest in using it as well.

Magnetic-Strip Systems

Less expensive, but still quite effective, are magnetic-strip authentication systems. These systems allow users to access buildings or physical company resources, and can track if a person is in one building while their computer is being accessed simultaneously from a different location. Magnetic-strip systems can limit access to vaults, network operations centers (NOCs), partner locations, or corporate virtual private networks (VPNs).

Security Staff

Your IT staff may not be the best people to put in charge of security, since they are usually the people who build the infrastructure and it is difficult to audit your own work. The design and development engineers and the daily operations people may feel that they have "designed in" best solutions, and may feel that discovering flaws in their own designs reflects negatively on their reputations. The skills to understand the requirements of keeping a network secure are unique and time consuming. Additionally, the complexities of network security and network operations are vast. Today's infrastructure and potential risks are much too complicated to be someone's part-time responsibility. The complexity of network-security technologies and how hackers can exploit them must be thoroughly understood in order to develop a strong defense. This task takes a significant amount of specific knowledge that the normal operations staff simply do not have. It is recommended that you hire qualified and dedicated security staff armed with sophisticated hardware and software tools and complement these resources with the services of an outside security specialist.

Security Processes

To be effective, security processes must be comprehensive and well communicated to your entire organization's network of users. General security policy and procedures define an overall framework for security and provide the security teams with leverage to enforce security measures. After the potential sources of threats and the types of damage that can occur have been identified, putting the proper security policies and safeguards in place becomes much easier. Organizations have an extensive choice of technologies, ranging from antivirus software packages to dedicated network-security hardware such as firewalls and IDSs to provide protection for all areas of the network.

Be sure to consider all types of users on the network. Diversity of users on the network makes the task of network security more complicated. Outside access is normally necessary for employees on the road, vendors, and customers. While most users dial in to the corporate network, some gain access via the Internet. This scenario leaves potential entry points for hackers and other individuals to enter the network for illegitimate purposes. Good security processes must be in place to make sure that entry points are closely controlled for authorized access only. Procedures that can quickly and completely prohibit an individual's network access upon termination must also be established, and integrated with departments such as Human Resources.

A good security process should also employ an IDS that can alert network security if an attack or unauthorized access is in progress. The complexity of the network and the sophistication of hackers can present considerable challenges. Given enough time and attempts, a good hacker can find entry points into a network. Intrusion detection helps eliminate this risk by enabling network security to take immediate preventive action.

Table 1
Facts and Figures*

Did you know that:	
7	Is the number of Red Hat 6.2 servers that were attacked within three days of connecting to the Internet?
24 hours	Is the time elapsed before a Windows 98 system, deployed Oct 31, 2000, was compromised?
525	Is the number of unique Net Bios scans recorded in a 30-day period?
1398	Is the number of intrusion alerts recorded in February 2001 (an 890% increase from the previous year)?

* Source: project.honeynet.org/papers/stats/

Honeypots

Many companies are implementing a new concept in dealing with would-be hackers called “honeypots” or “honeynets.” Honeypots are tempting targets installed on the network with the sole intention of attracting hackers to them and keeping them occupied and away from valuable corporate resources. These machines appear to be normal, functional hosts but actually do not have legitimate users or network traffic. They exist for the sole purpose of being a false target aimed at uncovering the attackers’ tracks. An alarm on a honeypot is a clear indication that something is happening. Hackers can hide in legitimate network traffic and masquerade as common anomalies and errors. By hiding in what looks like normal network traffic or creating what looks like a typical network issue that self-corrects as traffic adjusts, the hacker can creep in stealthily and create a major attack. It is not uncommon for the network administrator to see slight abnormalities and ignore these common errors. Some network administrators will go as far as to turn off the alarms set up in IDS systems to track these types of issues thus leaving the network even more exposed.

Honeypots are excellent at ferreting out internal hackers as well. Technically savvy internal users can often work around IDSs, but have no way of knowing that the honeypots exist. Honeypots are exceptionally effective in collecting detailed information about an attack once it is detected, documenting forensic data that can prove invaluable in the case of legal action.

There are two kinds of honeypots, the *sacrifice box* and the *service simulator*. The *sacrifice box* consists of a fully functioning operating system with a suite of applications to busy the hacker while recording activity and limiting access to other network resources. The sacrifice box is an attractive and convincing target for hackers. This device is placed in a production environment, behind a firewall, and modified to allow inbound traffic while filtering outbound traffic. The *service simulator* is a software application that watches for inbound traffic and mimics the applications that are actually functioning on the server. Service simulators are much cheaper to deploy and are designed to limit access only. The service simulator approach is much easier for a savvy hacker to detect, and normally will not hold an attacker’s attention for very long. Information gathering is also more limited in this approach. If all your network needs is a smart burglar alarm, the service simulator is a cost-effective approach. Networks requiring a more comprehensive system because of the nature of the network or data should consider deploying a sacrifice-box honeypot or even a honeynet (multiple honeypots throughout the network).

After such solutions are installed, tools can be deployed that periodically detect security vulnerabilities in the network, providing ongoing proactive security. In addition, professional network security consultants can be engaged to help design the proper security solution for the network or to ensure that the existing security solution is up to date and safe. With all the options currently available, it is possible to implement a security infrastructure that allows sufficient protection without severely compromising the need for quick and easy access to information.

Virus Protection Software

Virus protection software is packaged with most computers and can counter many virus threats if the software is regularly updated and correctly maintained. The anti-virus industry relies on a vast network of users to provide early warnings of new viruses so that antidotes can be developed and distributed quickly. With thousands of new viruses being generated every month, it is essential that the virus database is kept up to date. The virus database is the record held by the antivirus package that helps it to identify known viruses when they attempt to strike.



Reputable antivirus software vendors publish the latest antidotes on their Web sites and the software can prompt users to periodically collect new data. Network-security policy should stipulate that all computers on the network are kept up to date and, ideally, are all protected by the same antivirus package—if only to keep maintenance and update costs to a minimum. It is also essential to update the software itself on a regular basis. Virus authors often make getting past the antivirus packages their first priority.

Many software companies are looking to form alliances with companies that specialize in security—Microsoft with VeriSign Secure, for example. These security alliances will help push a wider adoption of basic security packages in the home. However, alliances such as these can also have disadvantages. Although beneficial to the average user, the concern from a vendor's point of view is the establishment of a de facto standard on security.

Security Policies

When setting up a network, whether it is a LAN, virtual LAN (VLAN), or WAN, it is important to initially set the fundamental security policies. Security policies are rules that are electronically programmed and stored within security equipment to control areas such as access privileges. Security policies are also written or verbal regulations by which an organization operates. You must decide who is responsible for enforcing and managing these policies, and determine how employees are informed of them.

What Are the Policies?

Policies should control who has access to which areas of the network and how unauthorized users are prevented from entering restricted areas. For example, only members of a human resources department should have access to employee salary histories. Passwords usually prevent employees from entering restricted areas, but only if the passwords remain private. Written policies, even as basic as warning employees against posting their passwords in work areas, can often preempt security breaches. Customers or suppliers with access to certain parts of the network must be adequately regulated by the policies as well.

Who Will Enforce and Manage the Policies?

The individual or group of people that polices and maintains the network and its security must have access to every area of the network. Therefore, the security policy management function should be assigned to people who are extremely trustworthy and have the technical competence required. As noted earlier, the majority of network security breaches come from within, so this person or group must not be a potential threat. Once assigned, network managers can take advantage of sophisticated software tools that can help define, distribute, enforce, and audit security policies through browser-based interfaces.

How Will You Communicate the Policies?

Policies are essentially useless if all of the involved parties do not know and understand them. It is vital to have effective mechanisms in place for communicating existing policies, policy changes, new policies, and security alerts regarding impending viruses or attacks.

Identity Technologies

Once your policies are set, identity methods and technologies must be employed to help positively authenticate and verify users and their access privileges.

Passwords

Making sure that certain areas of the network are password-protected—accessible only by those with particular passwords—is the simplest and most common way to ensure that only those who have permission can enter a particular part of the network. In the physical-security analogy above, passwords are analogous to badge-access cards. However, the most powerful network-security infrastructures are virtually ineffective if people do not protect their passwords. Many users choose easily remembered numbers or words as passwords, such as birthdays, phone numbers, or pets' names, while others never change their passwords and are not very careful about keeping them secret. The guidelines, or policies, for passwords are:

- Change passwords regularly
- Make passwords as meaningless as possible
- Never divulge passwords to anyone until leaving the company

In the future, some passwords may be replaced by biometric security systems, as described in an earlier section.

Digital Certificates

Digital certificates or public-key certificates are the electronic equivalents of driver's licenses or passports and are issued by designated certificate authorities. Digital certificates are most often used for identification when establishing secure tunnels through the Internet, such as VPNs.

Access Control

Before a user gains access to the network with a password, the network must evaluate if the password is valid. Access-control servers validate the user's identity and determine which areas or information the user can access based on stored user profiles. In the physical-security analogy, access-control servers are equivalent to the gatekeeper who oversees the use of the access card.

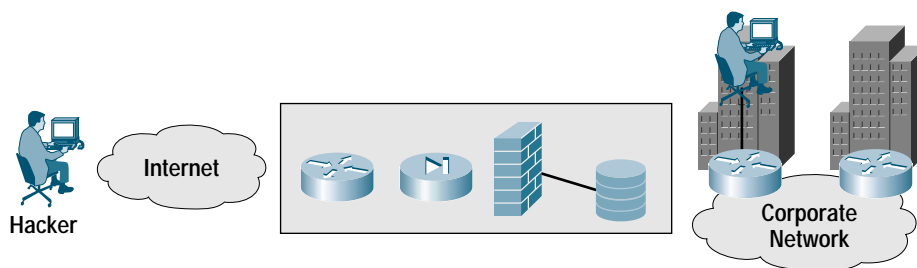
Firewalls

A firewall is a hardware or software solution implemented within the network infrastructure that contains a set of programs designed to enforce an organization's security policies by restricting access to specific network resources. In the physical-security analogy, a firewall is the equivalent to a door lock on a perimeter door, or on a door to a room inside of the building. It permits only authorized users, such as those with a key or access card, to enter. Firewall technology is even available in versions suitable for home use. The firewall creates a protective layer between the network and the outside world. In effect, the firewall replicates the network at the point of entry so that it can receive and transmit authorized data without significant delay. However, it has built-in filters that can disallow unauthorized or potentially dangerous material from entering the real system. It also logs an attempted intrusion and reports it to the network administrators.

Firewalls should be configured to block Internet Control Message Protocol (ICMP) pings that originate externally and tunnel through in that protocol's echo reply, or outgoing ICMP pings, to avoid unnecessary risk to a distributed DoS attack.

The FBI reported in 1999 a verifiable loss of U.S.\$256 million dollars due to computer security breaches. Gartner Group expects that by 2003 more than 50 percent of small and mid-sized enterprises using the Internet for e-mail will experience a successful, damaging attack, yet these mid-sized companies resist implementing even the most basic of security measures—namely a firewall.

Figure 1
Firewall Configuration



Change Management

Change management is a set of procedures that are developed by the network operations staff and adhered to whenever changes are made to a network. Companies that implement a software-based change management system are able to provide NOC technicians with valuable troubleshooting data about the change and react more efficiently to issues when needed.

Change management is often overlooked as a security tool. Most companies, when focused on security, focus on the servers; yet routers make up the backbone of the network infrastructure and are accessible over the entire network. For example, consider a router problem in January 2001 that occurred at Microsoft. It took Microsoft 22 hours to track down the problem and fix it.

The initial problem was caused when a network technician changed the router configuration from Microsoft's network border to the internal network that housed all four of its DNS servers. Packets could still reach the DNS servers, and Microsoft's internal network still worked properly. Web traffic could not reach Microsoft's networks via the DNS servers, but could reach the servers directly by requesting access using the exact IP address assigned to the site they were trying to access. (Typically, access is configured via domain names, masking the actual IP address being used.) As a result, outside traffic could not gain access to resources requested in this fashion.

Microsoft made two key errors. The first was that it did not apply controlled change management processes. Had the technician used a documented change management procedure, Microsoft technicians would have been able to quickly resort to the previous router configurations and restore service quickly. Hackers immediately capitalized on the problem and used this vulnerable time to hit Microsoft's network with DoS attacks.

Secondly, the Microsoft network did not have system-engineered security designed in. All of the public DNS servers were on the same subnet. Hackers immediately discovered this situation by using a simple tool, and then capitalized on Microsoft's vulnerability by attacking the network with DoS attacks. The DoS attacks were solved when additional name servers were applied to the network. Had this configuration been part of the initial design, the exposure would have been significantly reduced.

Changes should be made to the network by adhering to proper change-ticket or emergency change-ticket procedures, followed by immediate update of associated documentation. Companies that implement a software-based change management system are able to provide NOC technicians with valuable troubleshooting data.

Encryption

Encryption technology ensures that messages cannot be intercepted or read by anyone other than the authorized recipient. Encryption is usually deployed to protect data that is transported over a public network and uses advanced mathematical algorithms to "scramble" messages and their attachments.

Encryption provides the security necessary to sustain the increasingly popular VPN technology. VPNs are private connections, or tunnels, over public networks such as the Internet. They are deployed to connect telecommuters, mobile workers, branch offices, and business partners to corporate networks or to each other. All VPN hardware and software devices support advanced encryption technology to provide the utmost protection for the data that they transport.

Several types of encryption algorithms exist, but some are more secure than others. The U.S. government this year has replaced the current data encryption standard, Triple DES, with AES. AES is fundamentally more secure than previous methodologies. The National Institute of Standards (NIST) created a task force to develop this new standard and to focus on areas such as improving mobility by reducing the number of passes from three to one per scan. Scanning a single piece of data three times may create a process that is relatively hard to break; but this solution is also CPU-intensive and cumbersome to available computing power.

With the rise in the use of the Internet and devices such as cellular phones and personal digital assistants (PDAs), the need to communicate securely will increase, but these smaller devices require a different approach to encryption, demanding a smaller footprint that uses fewer resources.



The NIST selected a research team to focus on the issue of effective encryption. This team is currently writing a formal standard where AES seems to be the solution of the future. Mathematically solid, AES requires only one pass to encrypt data and is designed to be fast, making it significantly more efficient. The biggest benefit to companies who plan to use AES is that the standardization will reduce cost, increase compatibility, and allow for more innovation in taking on this more robust security protocol and integrating the smaller, faster footprint onto new technologies.

Cisco released a paper in February 2001 stating its position to support AES, although this support won't be widely implemented until AES moves through the Internet Engineering Task Force (IETF). For VPNs, the IETF needs to specify how AES should be implemented within the IP security standard to maintain compatibility with multivendor networks.

The table below shows the differences in the two approaches to encryption.

Table 2
AES versus Triple DES*

Service Provider	Business Focus	Service Area
Type of algorithm	Symmetric, block cipher	Symmetric, feistel cipher
Key size (in bits)	128, 192, 256	112, 168
Speed	High	Low
Time to crack (assuming a machine could try 255 keys per second)	149 trillion years	4.6 billion years
Resource consumption	Low	Medium
NIST standard	N/A	FIPS 46-3

* Source: Network World, July 30, 2001

Intrusion Detection Systems

Organizations continue to deploy firewalls as their central gatekeepers to prevent unauthorized users from entering their networks. However, no single technology serves all needs. Organizations are increasingly looking to intrusion detection systems (IDSs) to counter the risk and vulnerability that firewalls alone cannot address. An IDS provides around-the-clock network surveillance and analyzes packet-data streams within a network, searching for unauthorized activity—such as attacks by hackers—and enabling users to respond to security breaches before systems are compromised. When unauthorized activity is detected, an IDS can send alarms to a management console with details of the activity and can often order other systems, such as routers, to cut off the unauthorized sessions. In the physical security analogy, an IDS is equivalent to a video camera and motion sensor; detecting unauthorized or suspicious activity and working with automated response systems, such as watchguards, to stop the activity.

There are two general types of IDSs: host-based and network-based. Host-based systems are installed on the server or desktop and protect and monitor log files for certain events or key changes. Many host-based IDSs are hybrid and also monitor network traffic sent to the host where they are installed. Network-based IDSs (NIDSs) sniff network traffic using a system called a sensor. The sensor collects all packets and evaluates both the network headers and data and looks for signs of misuse or a data pattern that matches a known attack. Some sensors go further by attempting to match traffic with correct Layer 4 and Layer 7 protocols.

Deploying an IDS requires many support and design considerations. Your network administrators and security teams must have procedures that outline how to handle an IDS and what needs to be considered when launching new programs (does the IDS auto-find network changes, for example). Look for an IDS that provides detailed information, not terse logs. You need to get information about what the alert means, if it is a real event, and how to patch it.

Network Scanning

Network scanners conduct detailed analyses of network systems to compile an electronic inventory of the assets and detect vulnerabilities that could result in a security compromise. This technology allows network managers to identify and fix security weaknesses before intruders can exploit them. In the physical security analogy, scanning is like conducting a periodic building walk-through to ensure that doors are locked and windows are closed. Scanning helps to evaluate and understand risk, thereby allowing corrective action to be taken.

Expertise

While electronic scanning tools can be very thorough in detecting network-security vulnerabilities, they may be complemented by a security assessment from professional security consultants. A security assessment is a concentrated analysis of the security posture of a network, highlighting security weaknesses or vulnerabilities that need to be improved. Periodic assessments are helpful in ensuring that, in the midst of frequent changes in a network, the security posture of the network is not weakened. In the physical security analogy, a periodic security assessment such as scanning is like a guard periodically patrolling an entire secure area. The tools are only half the solution; specialized expertise is needed to fully understand the secure status of the network. Without a solid security team to help keep watch over the corporate network, a company can easily miss important security issues, be overwhelmed in trying to understand the larger impact a vulnerability may cause on their business. This lack of expertise, not having the knowledge or ability to act on the threats can result in significant productivity loss as well as compromising confidential corporate information.

Managed Security Services

Learning all the options for securing your network and keeping one step ahead of the threats can be time consuming and expensive for companies. One option is to turn to security intelligence professionals to help you identify internal and external risks.

Table 3
Cisco Powered Network Managed Security Providers

Service Provider	Business Focus	Service Area
Avasta, Inc.	Small, medium, large businesses	United States
Broadwing, Inc.	Small, medium, large businesses Consumers Service providers	United States
Cervalis	Small, medium, large businesses	United States
EXENET Technologies	Small, medium, large businesses Service providers	Partial United States
Exodus	Small, medium, large businesses Consumers Service providers	Canada, Japan, United Kingdom, United States
Genuity	Large businesses	United States
Inflow, Inc.	Small, medium, large businesses Service providers	United States
Pointshare	Large businesses	Partial United States
SBC	Small, medium, large businesses Consumers Service providers	Partial United States
Sprint	Small, medium, large businesses Consumers Service providers	Canada, United States
XO Communications	Large businesses	Partial United States

Conceptually, Internet-security intelligence services are modeled after government military intelligence-gathering apparatus. Many security service firms are started by ex-military security personnel who are finding that few IT teams really understand the complete security picture and are prepared to deal with its unique challenges.

Security intelligence services are different from managed-security services, which take operational responsibility for securing a customer Web site or network. The resources (time and money) needed to hire specialized security combined with the cost of the infrastructure and resources to manage the security on a 24x7x365 basis—hackers never sleep—can be debilitating to a normal IT budget. By purchasing a managed security service from a trusted service provider, companies can save on resources while employing leading-edge security techniques.

Table 4
Outsourced versus In-House Security

Hardware and Software	In-House (U.S.\$)	Outsourced
Firewall purchase	\$4995	0
Installation expense	\$1200	399
Hardware and software	\$1500	0
Vulnerability assessments	\$1800	0
SubTotal	\$9495	\$399
Management Costs		
Firewall management/monthly	4 hours	0 hour
Monthly costs @ 150.00/hour	\$600	\$499
Yearly management costs	\$7200	\$5988
Total fixed-year cost	\$16,695	\$6387

Managed-security services range from simple firewall deployment and management to full-blown vulnerability assessments that include looking for intrusion detection to virus protection. The best-managed security service companies offer a wide range of services.

Typical Services from a Security Service Provider

Network Monitoring 24x7x365

Security service providers should operate multiple network-monitoring centers that are staffed around the clock by experienced security engineers to monitor all aspects of network security for each of their customers.

Firewall Configuration/Installation Support

Service providers should perform firewall configuration and installment at the customer's site and then remotely manage one or more firewalls via the Internet using a VPN connection.

Vulnerability Assessments

Service providers should recommend performing a comprehensive assessment of the company's network before and after installation of security solutions. Additionally, a company should repeat the assessment every six months to ensure that the networks do not show new weakness.



Monthly Usage/Trend Reporting

Service providers should provide detailed, confidential summary reports so that their customers can actively track network activities, determine a normal baseline, and uncover security issues. The baseline is especially useful in helping to define security policies.

Web Site Filtering

As an option, the service providers should enable companies to block Web access to certain types of traffic and schedule appropriate Web access times.

Virus Protection

Service providers should offer virus protection services to stop the spread of viruses and other malicious content at the Internet gateway.

Technical Training and Support

Many service providers offer technical training and awareness seminars, and help establish policies and procedures to keep their customers' networks secure and their staff aware.

The above list is not comprehensive. Each provider offers a unique approach to its security services. Networks vary, so when looking for managed-security services, look to a provider that offers a full range of services. Make sure that the provider has adequate staff and understands your company's unique situation. Start with a secure design for your infrastructure and recommendations for suitable policies that support the recommended design. Choose a provider that is flexible and that won't unnecessarily disrupt your network during peak times. Finally, make sure that the provider offers best-of-breed software and hardware and has the educated staff to ensure full operability.

Cyber-insurance

Cyber-insurance is a new concept for companies that want to insure against the losses that can occur in a security breach. More and more companies are being held liable when unauthorized access to customer data occurs. Offered by companies such as American International Group, Lloyds of London, and The St. Paul Companies, cyber-insurance protection could eventually become commonplace. For now, companies are struggling with how to quantify how much financial loss is possible due to security violations. There are little or no precedents. Many factors need to be considered when determining the risk, from company size to the nature of business transactions. Prices for cyber-insurance can vary from thousands to millions of dollars per network. If someone is using credit cards to do business with you and you don't take due diligence to protect that data, you can be held accountable.

Summary

You have scoured your network from end to end, found the holes, read the reports, and applied the patches. Your network is secure, at least until some savvy hacker invents a new way to slip packets through your firewalls. Vulnerability scanning and network security are not one-time fixes. Industrious hackers will find ways to breach all that you have built and to exploit your valuable assets wherever possible.

Networks are not static. Software and hardware must be constantly updated and new employees must be hired. The overall network design, the frequency of your security scans, and the policies and procedures you have in place must be reviewed regularly, along with special attention to more sensitive or at-risk areas of your network. By using multiple forms of protection and educating your staff and network users to maintain high security standards and report all questionable activities to the appropriate security support teams, you can provide a secure working environment for your company and a stable place where customers will feel comfortable doing business.

As time passes, new technologies will be developed to further improve the efficiency of business and communications and improve network security. If you stay abreast of emerging security technologies, and the latest security threats and dangers, the benefits of running your business applications over networks will most certainly outweigh the risks.

A secure network requires a dedication to protecting corporate resources. Companies must be prepared with the best tools, stringent procedures, and competent staff who are focused on the security of the network.

For More Information

For further information on network security and how Cisco products and technologies help customers address security problems and take advantage of the many benefits networks have to provide, visit: <http://www.cisco.com/go/security>

Other Useful Sites

- For more information about encryption using AES: http://www.nist.gov/public_affairs/releases/aesq&a.htm
- For a list of the top 10 security threats: www.sans.org/toptem.htm
- For more information on the CSI/FBI report: http://www.gocsi.com/prelea_000321.htm
- To see the top 20 most critical networking vulnerabilities, go to <http://www.sans.org/top20.htm>.
- IDS resources: http://www.icsa.net/html/communities/ids/buyers_guide/guide/technology/technology.shtml

<http://secinf.net/info/ids/idspaper/idspaper.html>

- Asta Resources

Newsfront: July 16, 2001,

Communications News: September 2000

The Industry Standard: July 23, 2001 (aye for an Eye)

- For more information on AES Encryption: http://www.nist.gov/public_affairs/releases/aesq&a.html

Hacker Web Sites

- Cult of the Dead Cow were the developers of BackOrifice: <http://www.cultdeadcow.com/>
- Kevin Mitnick supporters: <http://www.2600.com/mindex.html>
- Chaos Computer Club, German/English: <http://www.ccc.de/>
- Site that provides info on what operating system a site is running: <http://www.ussrback.com>
- Site that hosts registration and info for the annual hackers' convention: <http://www.defcon.org/>
- Hackers Hall of Fame: <http://www.discovery.com/area/technology/hackers/hackers.html>
- E-mail anonymizers and remailers: <http://www.activism.net/cypherpunk/>
- Interesting tidbits: <http://www.happyhacker.org/>
- Tools: <http://www.netsecurity.about.com/computer/netsecurity/cs/hackertools/>
- Tools and more: <http://www.technotronic.com>

**Corporate Headquarters**

Cisco Systems, Inc.
 170 West Tasman Drive
 San Jose, CA 95134-1706
 USA
www.cisco.com
 Tel: 408 526-4000
 800 553-NETS (6387)
 Fax: 408 526-4100

European Headquarters

Cisco Systems Europe
 11, Rue Camille Desmoulins
 92782 Issy-les-Moulineaux
 Cedex 9
 France
www.cisco.com
 Tel: 33 1 58 04 60 00
 Fax: 33 1 58 04 61 00

Americas Headquarters

Cisco Systems, Inc.
 170 West Tasman Drive
 San Jose, CA 95134-1706
 USA
www.cisco.com
 Tel: 408 526-7660
 Fax: 408 527-0883

Asia Pacific Headquarters

Cisco Systems Australia, Pty., Ltd
 Level 9, 80 Pacific Highway
 P.O. Box 469
 North Sydney
 NSW 2060 Australia
www.cisco.com
 Tel: +61 2 8448 7100
 Fax: +61 2 9957 4350

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the Cisco.com Web site at www.cisco.com/go/offices.

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Czech Republic • Denmark • Dubai, UAE
 Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico
 The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia
 Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Copyright © 2002, Cisco Systems, Inc. All rights reserved. Cisco, Cisco IOS, and the Cisco Systems logo, are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company (0202R)
 Printed in the USA SB/JSI/02.02