

Cyberspace security management

David C. Chou

St Cloud State University, St Cloud, Minnesota, USA

David C. Yen

Miami University, Oxford, Ohio, USA

Binshan Lin

Louisiana State University-Shreveport, Shreveport, Louisiana, USA

Philip Hong-Lam Cheng

Miami University, Oxford, Ohio, USA

Keywords

Internet, Computer security, Encryption

Abstract

Through the tremendous growth of Internet users during the last few years, organizations now realize the potential market of the information highway. However, these organizations now face the problem of Internet security. The open environment of the Internet contributes greatly to its success, but also plants inherent security problems. Discusses the security frameworks implemented in the cyberspace environment and the current developments and future trends involving this issue.

Introduction

With the astonishing growth of the Internet, corporations around the world now see a huge potential market for their products and services. Unfortunately, the Internet's rapid growth over the past few years comes with a high price tag as network users have to deal with the increased risk of data security.

According to a report made by the Defense Information System, a division of the US Defense Department, its network experienced 250,000 attacks last year. In nearly two-thirds of the cases, attackers gained entry to the agency's computer networks.

Network security issues fall into two categories: unauthorized attempts to access private data through Internet and internal networks, as well as the disruptions such as natural disasters and computer virus. While most attempts are made by accident, a number of people have less than honorable intentions.

Although network attacks are a growing concern, they are not yet unmanageable. This article identifies the major sources of threats, such as technology weaknesses, inherent risks in the network environment, and internal control problems. Classifications of Internet attacks will be investigated next. Tools developed in dealing with security issues such as authentication and encryption will be discussed next. Finally, this article will look into the future of the Internet and cybersecurity.

Causes of Internet security incidents

Understanding the causes of Internet security incidents is a good starting point toward knowing cybersecurity. This section

discusses five types of Internet security incidents:

- 1 inherent risks;
- 2 technology weaknesses;
- 3 policy weaknesses;
- 4 unauthorized intruders; and
- 5 legal issues.

Inherent risks

The Internet has its own vulnerability. The Internet connects millions of computers among users, companies, commercial service providers and governments around the world. Its size inherits vulnerability and incurs such problems as misrouting, transmission failure, data corruption, etc. Some computers use ISDN for communications and some still need a phone-line for connection. This diversity causes security flaws that are difficult to control. Moreover, when the Internet was first designed, its emphasis was compatibility instead of security.

The Internet Engineering Task Force (IETF), together with the Internet Activities Board (IAB), sets guidelines and standards for the Internet. Membership in the IETF is open to everyone interested in Internet issues. As the Internet becomes more commercial-oriented, the role of the IETF has become less clear-cut. Vendors may propose their own standards without IETF approval, and the emergence of these different standards worsens the problems of security.

Technology weaknesses

Technology weaknesses refer to deficiencies in software and hardware products. Technology weaknesses can be classified into two categories: those caused by inherent weaknesses in communications mechanisms and products, and those that result from the misconfiguration of operating systems and software.

Many Internet weaknesses can be traced back to communication protocols. Protocols define the set of rules by which networks interact with each other. The most common



protocol on the Internet is TCP/IP. Unfortunately, there are many vulnerable areas associated with this protocol. One of the biggest problems is its inability to verify the identity of communication parties. Another major shortcoming is its inability to protect the privacy of data on the Internet. Owing to the characteristics of TCP/IP protocols, it is possible for a given machine to monitor all of the traffic that passes along an attached network. As a result, a Telnet session or an FTP transfer can be captured by a third party.

Configuration weaknesses stem from the complexity of networked systems. Some systems that come with default settings may not be secure. Examples include unsecured user accounts (such as guest log-in or expired user accounts), system accounts with widely known default passwords, and misconfigured Internet services.

Policy weakness

Corporate security policies serve as the foundation of the computer security framework. These policies, often referred to as baseline controls, work together in establishing a certain level of security throughout a company. These security controls include:

- physical security controls;
- personnel security controls;
- administrative security controls;
- data communications security controls;
- computer security controls;
- disaster recovery and backup; and
- business continuity (Cross and Yen, 1989).

Each of these controls should be implemented consistently throughout the entire organization. Furthermore, multiple security measures should be used instead of a single one. Finally, a complete set of guidelines regarding passwords and user ID should be established and enforced accordingly.

Unauthorized intruders

People who gain unauthorized access to organizational data files and resources are often viewed as intruders or “malicious crackers”. According to Barrett (1996), a cracker is a malicious person who uses password-guessing programs, packet sniffing, or other means to break into another person’s computer account or otherwise defeat the security of a computer. Crackers look for weaknesses in the network system and find ways to penetrate them. According to a study conducted by SRI International, intruder motives vary; however, the methods they use to pinpoint a security hole are similar. Therefore, a comprehensive security

system is essential for safeguarding your computer system in an open environment.

Legal issues

There are certain criminal activities that are pervasive on the Internet. These illegal activities derive from copyright infringements and pornography. These crimes stem from a lack of security and/or regulatory enforcement on the Internet. From these crimes, fraud, embezzlement, pirating and espionage can occur.

Copyright infringement

The growth of the Internet has provoked concern with copyright infringements among publishers, writers and others. The Internet exposes more data and information than ever before to more people. This exposure has made theft a primary consideration. The Internet’s structure is vulnerable and open to sabotage and abuse. The law has become concerned with the protection of copyright interests. The Copyright Act states that information must be “freely available”. To deter such activities the Criminal Copyright Improvement Act of 1995 was created. This law prohibits reproducing or distributing copyrighted material with a retail value of \$5,000 or more.

Copyrighted data can become safer with the use of digital-rights management. Digital-rights, another form of software security, trace the activities performed by the end user. Digital transmission can be traced to the millisecond. Digital-rights systems can be embedded into the code that provides proof of ownership and copy protection. The system detects any changes made to the data. Also, the system tracks, identifies and determines the appropriate royalties through serial codes. Serial codes can identify hackers and track them to their point of origin. The same process also applies to high-volume financial transactions.

Other solutions, such as digital watermarking software, can assist in establishing copyright ownership. Digital watermarking provides hidden messages in a random manner on the digital data. Digital-rights management has the potential to destroy the Internet’s range of free digital content. The legislative outcome is uncertain but the rule for distributing data will be an incentive-based opportunity. The acceptance of this system will transform the way content is distributed, consumed, and paid for on the Internet (Angell and Zelhka, 1997).

Revisions of copyright laws that employ the Dilution Act and pursue international agreements are necessary to guarantee copyright, trademark, and rights against pornographers. This revision also fosters the

creativity and growth of the Internet in a manner that serves the public well (Appelman, 1996).

Pornography

Pornography is a concern because a proliferation of provocative content exists on the Internet. Before the Decency Act was created, the decision of the *US v. Thomas* served as a test of online or Internet communications. The 6th US Circuit Court of Appeals upheld that electronic bulletin board operators might be liable for interstate transmissions of material deemed pornographic by the local standards of communities far from where that material originated (Appelman, 1996). To combat these activities on the Internet, the Telecommunications Reform Act was signed into law on February 8, 1995. This Philadelphia federal district court lawsuit challenged the Communications Decency Amendment (CDA). Senator Jim Exon, a Democrat of Nebraska, introduced this law. The amendment threatened the potential freedom of the Internet. To lawyers who defended First Amendment interest in cyberspace, the constitutional problems with the CDA, as well as the imminence of its threat to freedom of speech, were obvious. Thus, we quickly agreed on the basic themes of the case:

- 1 The terms of the law are vague and overboard. The legislation prohibits the public display or dissemination to a minor of “indecent” content or of any comment, request, suggestion, proposal, image, or other communication that, in context, depicts or describes, in terms patently offensive as measured by contemporary community standards, sexual or excretory activities and organs. The FCC defines Community Standards as national community of those who watch or listen to broadcast programming. Community standards define obscenity on the Internet as a subject open to interpretation. The Internet’s environment is subject to obscenity but the law will determine what is acceptable.
- 2 The government has no clearly established constitutional authority to regulate “indecent” content outside of broadcast media.
- 3 The legislation flunks the “least restrictive means” test.
- 4 The CDA’s “safe harbor” provisions are illusory.
- 5 The amendment of 18 USC 1462, which added a prohibition of computer transmission of “obscene” or “indecent” materials may have revived the long-dormant prohibition in that statute of information relating to inducing or obtaining an abortion (Godwin, 1996).

Environment of Internet security

The players on the Internet are the users, business sectors, and regulatory agents.

Users are classified as individuals, the community, and non-business concerns. Business sectors represent all businesses for profit and non-profit who operate as a growing concern. Regulatory agents are those agencies synonymous with the law. Each player is impacted by similar security constraints.

The user

The user is any person whose computer connects to the Internet. The user has a lot to fear because of the anonymity of people on the Internet. This anonymity makes it easy for criminals to continually shift their activities when they sense trouble. Anonymity provides a sense of security high and dangerous for the users.

The educators, parents, and the community have an increased alarm towards the Internet, because various Web sites promote sexually provocative material as well as drugs. Web sites allow the exploration of information never before achieved. Every user seeks a safer Internet environment. Embedded security deters provocative Web sites from growing.

Business sectors

Corporations understand that the Internet provides a competitive advantage. The Internet provides an opportunity to make a company more responsive to its customers. The Internet provides an instant way of communicating ideas among buyers, suppliers and customers. However, the risk of using the Internet is high.

The company’s fear is to be intruded by hackers and cyberpunks. A corporate information systems administrator’s nightmare is that intruders will breach the root system and gain control over the whole system. The interaction on the Internet will be a virtual gamble without security protection.

Risks occur when hackers intercept messages, sniff programs, steal passwords and break codes. These negative activities cause fear. Three fundamental security issues prominent in the business world are:

- 1 *Confidentiality*. This indicates that all secrets should be kept secret. Companies want to prevent confidential information from leaving the organization. Encryption controls and password systems can resolve these problems.
- 2 *Integrity*. This assures that data are not altered or modified undesirably. Altered data can be a breach of the corporate ideas, activities and goals.

- 3 **Availability.** A company's resources and systems must be up and running whenever needed.

The company must protect the data in their information systems. The lack of security on the Internet generates vulnerability on a company's information systems.

Regulatory agents

Laws have a monumental effect on the Internet. Laws must be reconfigured to meet the Internet environment. Subsequently, Congress and the judicial branches would be advised to revise existing laws and enable courts to address rights more effectively via the Internet. It has been suggested that "cybercourts" could be established to arbitrate and settle Internet crimes. The law plays an important role in assisting users during the due process as well as determining conformance rules and regulations for all providers. The law monitors and restricts illegal activities.

Security on the Internet is not only important to users and businesses. It also affects the legal fiber of our nation. Many regulatory agencies have found the criminal intent and actions on the Internet pervasive enough to build a legal framework around these infractions. The Department of Justice defines computer crimes as any violations of the law that involve knowledge of computer technology for their perpetration, investigation, or prosecution. Computer crimes can be broken down into three major categories: the computer role in the crime, the target or object of a crime, and the physical site of the crime and/or the instrument used to commit the crime. Congress considered the parameters of a computer crime and drafted the *Counterfeit Access Device and Computer Fraud Law of 1984*. This act prohibits unauthorized access to any federal interest computer. The law includes not only computers of federal interest but computers used or owned by the government or financial institutions. This law also affects the amount of hardware used to commit the crime. Computer crimes are far more prevalent and are becoming more serious. The Department of Justice has formed a criminal section to combat computer crimes. This division has been expanded to include Internet piracy.

Types of Internet attacks

Internet security breaches can be classified in the following ways: password-based attacks, IP spoofing, attacks that exploit trusted access, network snooping, and

attacks that exploit technology vulnerabilities.

Password-based attacks

Password-based attacks involve exploiting passwords in certain ways. A cracker will try every combination of a password in order to access a network. This brute-force strategy (the use of a computer to attempt all possible keys) succeeds with many types of UNIX systems that do not logout the user after several attempts of login failure. Crackers sometimes learn passwords by accessing electronic mails which contain passwords via a tool such as "crack", which locates a hole in the UNIX system. Crackers could use the FTP to obtain a publicly readable password file in the UNIX system. Although the file is in an encrypted form, the encryption algorithm is widely available. Since the process of obtaining passwords is very time-consuming, crackers steal passwords from real people.

Address spoofing

Spoofing is a situation in which the attacker steals a legitimate address and uses it to impersonate the owner of the system. One example is the IP spoofing attack. Assuming two machines are linked, an intruder replaces a computer without allowing the other to notice the redirection of their connection to a third party. This jeopardizes the original users of these two machines. In Web spoofing, a hacked server attracts the victim's browser and then sends requests for the Web page. A hot link on the hacked server redirects the request to the spoof server. The spoof server rewrites the page and sends the altered information to the user so that any information transmitted by the user can be intercepted. Spoofing is a dangerous and growing threat, but it is relatively easy to prevent. The best way to handle IP spoofing is to configure routers and to reject any inbound packets that claim to originate from a host within the internal network. Clicking on a bookmark or choosing "open location" from the file menu prevents Web spoofing because both of these are in parts of the browser that cannot be manipulated by a Java applet. However, no complete solution exists without a fundamental change on how the WWW and Java work.

Attacks that exploit trusted access

Several operating systems (such as UNIX, VMS and Windows NT) have trusted access mechanisms designed to facilitate access to other systems. The UNIX operating system allows access to trusted host files without a password. The user must enter the "rlogin"

or a similar command with some appropriate arguments. A person who has the name of the machine thus can access the machine that allows trusted access. An intruder needs only to gain access to one machine to get onto the other, thus increasing the threat of unauthorized access.

Network snooping

Thousands of files are transmitted from one end to the other of the network. At any point in the network, an attacker can intercept a file. This is known as network snooping or packet sniffing. Network snooping is one of the most serious threats to corporations, even if corporate networks do not connect to the Internet.

Attacks that exploit technology vulnerabilities

Operating systems such as UNIX and VMS are not security designed. Numerous loopholes and security problems have been found after their release, yet no one seems willing to completely rewrite them. Thus, one patch after another is developed to address new problems. Renewing the system will be extremely expensive because not every patch is compatible with the existing environment.

Internet security breaches cause many problems for Internet commerce. One important concern is the denial of service by the host. The denial of service prevents network resources from functioning to their intended purposes. The denial of services may lead to unauthorized destruction, modification, or delay of service. The “Syn” floods serve as an example. These floods lock the user out of an Internet connection by flooding the server with requests for connection – all from the hacker’s computer, which generates a phoney IP address and overloads the server, causing legitimate requests to be ignored. Crackers can also use security holes to commit fraud, such as using stolen credit card numbers to commit crimes. Internet security is, by far, the greatest threat posed to Internet commerce. Without a secure environment, it is difficult for companies to conduct business on the Internet and the potential of the Internet will not be fully utilized.

The Internet security techniques

As business communities realize potential opportunities on the Internet, business strategists predict that cyberspace will be the notable market of the next century. However, the biggest obstacles to Internet commerce so far are security issues. Since attacks make

the Internet a relatively unsafe place for investment, most companies use the Internet for advertising purposes only.

Internet security involves the application of both technical and non-technical countermeasures. The non-technical ways of pursuing Internet security include formulating a corporate security policy and educating and training users about that policy. On the other hand, major technical measures consist of access controls, authentication, encryption, firewall, audit, anti-virus tools, and self-assessment tools.

Access controls

To users, password control is the key control element. The one-time password can avoid sniffing; however, it is difficult to handle such a policy within a big corporation. On the other hand, to hosts, IP-address-based access control can be utilized. Unfortunately, this method can be easily subverted by crackers in comparison with the text password method. One common solution to this weakness is the use of encryption. Encryption avoids sniffing and hijacking, but is not well standardized. One example is Kerberos, which is a third-party trusted host authentication system devised at MIT within Project Athena. The Kerberos authentication server is a central system that knows about every principal and its passwords. It issues tickets to principals who successfully authenticate one principal (e.g. a user) to another (e.g. a server application). Moreover, Kerberos sets up a session key for the principals that can be used to protect the privacy and the integrity of communication.

Authentication

Authentication is a way to verify information senders through passwords, PIN, or cryptographic key. However, authentication is vulnerable to password attacks, address spoofing and bypasses. A new product of International Series Research, Inc. called CyberLocator™ uses space geodetic methods to authenticate the physical locations of intruders. This technique is accomplished through a location signature sensor, which uses signals from the satellite to find out a location on the earth. This new product is not vulnerable to many kinds of attacks because there is no password, PIN, etc. It will be accompanied with other security techniques to provide a higher assurance level of security.

Encryption

Encryption is a process of making information indecipherable except to those who possess a decoding key. Messages are

David C. Chou, David C. Yen,
Binshan Lin and
Philip Hong-Lam Cheng
*Cyberspace security
management*

Industrial Management &
Data Systems
99/8 [1999] 353–361

scrambled using a shared secret key, and unscrambled through the same secret key. Unfortunately, this method does not work well in general because exchanging secret keys between sender and receiver is almost impossible. A breakthrough to this technique was the invention of the public key in the 1970s. In the public key cryptography, one key (the public key) is used to encrypt a message and another (the private key) is used to decrypt the same message. While electronic encryption secures information, it also creates the possibility that criminals could electronically hide important evidence. Encryption is widely used in national security. As a result, there are strict export controls over encryption technology beyond the US borders.

Firewall

Firewall is a gateway between a private network and the Internet that keeps the private network secure from intruders while allowing private users transparent and uninhibited access to the Internet. It is frequently placed between an organization's internal network and the Internet, with the objective of keeping intruders out of the network. There are several advantages associated with the firewall. You do not need to rely on the cooperation of all users. Furthermore, it is quicker and easier to establish and maintain. However, the firewall is a locked door. After an intruder breaks the lock and gets into the system, the firewall can do nothing to stop it.

Software companies have developed filtering software to restrict access to objectionable areas of the Internet. This software is similar to the V-chip that is used to prevent cable access. This is promising but it does not hold the solution. Effective filtering can assist in promoting a freer exchange of ideas and information, but it does not protect others from material they find offensive. The filtering process is performed by a database of undesired sites that are installed into a program to prevent their entrance into your Net environment. The system essentially places a firewall around all specified sites to prohibit access. This activity must be updated continuously. This process is also costly. Alta Vista and Infoseek help perform this filtering process by collecting abstracts of sites by looking for tags or Web page origins. The origin of the site is determined by HTML<META>. Using these terms, many of the keyword searches are blocked from finding pornographic material.

Audit

An Audit is a service that keeps a detailed record of network events, such as the number of unsuccessful user logins to the system. It can be used with the intrusion monitoring system to detect the abnormal use of the system and to pinpoint the intrusion as soon as it happens. Audit tools such as Tripwire, Swatch and Argus are available in the market.

Anti-virus tools

A virus is a piece of software designed and written to adversely affect your computer by altering the way it works without your knowledge or permission. Computer viruses spread by attaching themselves to another program or to the boot sector of a diskette. When an infected file is executed, or the computer is booted from an infected disk, the virus itself is executed. Viruses have the capability of moving from one computer to another, especially through the network environment. Commercial software such as Dr Solomon and Norton Anti-virus are the anti-virus tools. The real threat comes from newly-created viruses that have not been reported. One solution is to back up all files, while another is to make sure that each disk contains no unknown files after use.

Self-assessment tools

Security holes exist no matter how you set up the network. Therefore, a self-assessment test is very important. Software such as COPS and Tiger are used to analyze the system and to reveal possible weaknesses. Also, SATAN can be used to evaluate the network. However, many intruders also employ these tools to penetrate the system.

Rating system

Rating is also another procedure that prevents the reception of unwanted Internet sites. The problem with rating systems is that Web administrators are bombarded with unrated sites. In most cases, the unrated sites require most monitoring. The rating method has great potential and may prove to prevent censorship and guide users. Today, the rating tool system is slowly catching on, but it is cumbersome to create. At this time there are fewer than 200,000 Web sites that are rated out of the 30 million total pages. SafeSurf has rated 40,000 sites, while the Recreational Software Advisory Council (RSAC) has rated 150,000. The rating system also provides a methodology for blocking specific sites while granting access to others. Microsoft has

assisted in supporting the ratings devices by the RSAC standard in the Explorer.

Flexibility

Flexibility is simply each user self-regulating their Web site options while applying their own vigilance until Web developers invent a better method. When surfing the Net a user must remain flexible but discriminatory as well. All Web sites are not for every user. When deciding to use the Net a user must be cognizant of the various types of sites available and use his or her best judgment.

Firewall and router combined method

Another technique that a company can use for infiltration is the adoption of the router and firewall systems simultaneously. In using the firewall, the company could shelter itself while the router filters data from the Internet. Filtering is based on prefix packets at the header of the address. A company could prevent access to sites such as “.edu”, for example, if the company determined that these sites were less secure. The modification of header packets is easy to make by a technique known as spoofing. The act of spoofing is akin to a wolf in sheep’s clothing. The façade of appearing to be another address is simple to a hacker, but is indeed troublesome and detrimental to a company or user occupying that address. The detriment is derived owing to an address being twofold, one as identification of the Web site, and the other as a front door into a company’s system. The result is that a company can lose its confidentiality, integrity and availability. Remedies stem from companies such as American Express, who collaborate with other companies to reduce risk by creating a sheltered environment. The environment integrates each partner and creates a firewall for the user. This method is a step in the right direction but is not fool-proof.

A comparison of Internet attacks and security techniques

Table I shows the suitability of Internet security techniques for various Internet attacks identified in this article. The technique of access control is good for password-based attacks, and network snooping. It is satisfactory for address spoofing. However, this technique is limited to attacks that exploit trusted access since the host computer and network have no control to the external network’s attack. It is also limited to attacks that exploit technology vulnerabilities since this technique centers on access

control only. In order to handle these attacks, we need to educate the user with more business ethics and privacy.

The authentication technique verifies information senders through passwords, PIN, or cryptographic key. It works well with password-based attacks. It is satisfactory for attacks that exploit trusted access. However, this technique is limited to address spoofing, network snooping, and attacks that exploit technology vulnerabilities since the senders of these attacks are difficult to identify. This is not a state-of-the-art technique in preventing Internet attacks.

The encryption technique encodes a message so that meaning is not obvious. It is good for password-based attacks, attacks that exploit trusted access, and network snooping, since the hacker is unable to read such information. It is satisfactory for attacks that exploit technology vulnerabilities since the hacker may find a way of decrypting the message from technology impediment. However, this security technique is limited to address spoofing since the victim’s browser is attracted by a hacked server and this technique has no way to prevent it.

The firewall technique works well with address spoofing, attacks that exploit trusted access, and network snooping, since this technology can separate corporate networks from Internet access. However, it is limited to password-based attacks and attacks that exploit technology vulnerabilities. We need to educate the user base about business ethics and privacy. The government could play a stronger role in setting security regulations against these attacks.

The audit technique works well on password-based attacks, and it is satisfactory for address spoofing, attacks that exploit trusted access, network snooping, and attacks that exploit technology vulnerabilities since this technology keeps a detailed record of network events. Any abnormal use of and intrusion into the system will be detected as soon as it happens.

The use of anti-virus tools works on password-based attacks, address spoofing, attacks that exploit trusted access, network snooping, and attacks that exploit technology vulnerabilities, since any virus attacks from the above sources can be detected and prevented easily. However, a good anti-virus tool must identify and keep up with each new virus as soon as it comes into existence.

The use of self-assessment tools is good for address spoofing and attacks that exploit trusted access, and it is satisfactory for password attacks, network snooping, and attacks that exploit technology vulnerabilities since these tools analyze the system to reveal

David C. Chou, David C. Yen,
Binshan Lin and
Philip Hong-Lam Cheng
*Cyberspace security
management*

Industrial Management &
Data Systems
99/8 [1999] 353-361

possible weaknesses. The early warning systems can prevent possible Internet attacks.

The use of a rating system can prevent the reception of unwanted Internet sites. This approach is satisfactory for password-based attacks, address spoofing, attacks that exploit trusted access, network snooping, and attacks that exploit technology vulnerabilities since the rating system provides a methodology for blocking specific sites while granting access to others, thus preventing these attacks from gaining access to certain important sites.

The use of flexibility on Internet security control is limited to all attacks mentioned before. This technique is simply a self-regulated approach on accessing user Web sites until Web developers invent a better method. It is not a state-of-the-art technique; however, the awareness of business ethics and privacy and the inclusion of government regulations are the keys of success.

The combination of firewall and router methods prevent address spoofing, attacks that exploit trusted access, and network snooping, since the environment integrates each partner and creates a firewall for the user, and it also increases the flexibility of Internet access. However, this technique is limited to password-based attacks and attacks that exploit technology vulnerabilities because firewall-based security prevents only outside hackers.

In addition to the security techniques mentioned above, any corporate-wide procedures or policies can be adopted to strengthen cyberspace security. We need to educate users on business ethics and privacy concerns. The government needs to place more regulations on cyberspace security. These non-technique approaches are the alternatives of securing cyberspace.

Future implications and conclusion

Organizations such as the National Fraud Information Center (NFIC) provide an online service to alert Internet users. The NFIC has joined forces with the Attorney-General's Office, the Federal Trade Commission, and the National Consumers League to keep a problem diary. Companies such as American Express have partnered with technology companies to create a safer environment for cardholders to perform electronic shopping.

When we look into the future, we will see further improvements in Internet security. New security protocols are under development by the Internet Engineering Task Force. Newly-proposed IP security protocols combine authentication, integrity, access control, and confidentiality in their network layers. The network system will be flexible enough to support different algorithms as required. The trend shows that firewall will provide greater security, with more features and lower cost. Recently, Sun Microsystems released Java, which contains many security characteristics ideal for use on the Internet. At the same time, hacking techniques will also be improved, and Internet security will be a never-ending challenge. Every company should conduct a cost-benefit analysis before they adopt any type of security system.

The law and the user are faced with a critical decision on how to make the Internet a legal and safe environment for the user. Virtual reality must have regulations similar to the other environments. Security is necessary and will promote usage and better quality. The law can determine liability and responsibility for Internet infractions. But the law and Internet providers will have to decide how to create a structure for user privacy and reasonable safety on the Internet.

Table I

Techniques for Internet attacks

Techniques	Attacks				
	Password-based attacks	Address spoofing	Trusted access exploitation	Network snooping	Technology vulnerabilities exploitation
Access control	Good	Satisfactory	Limited	Good	Limited
Authentication	Good	Limited	Satisfactory	Limited	Limited
Encryption	Good	Limited	Good	Good	Satisfactory
Firewall	Limited	Good	Good	Good	Limited
Audit	Good	Satisfactory	Satisfactory	Satisfactory	Satisfactory
Anti-virus tools	Satisfactory	Satisfactory	Satisfactory	Satisfactory	Satisfactory
Self-assessment tools	Satisfactory	Good	Good	Satisfactory	Satisfactory
Rating system	Satisfactory	Satisfactory	Satisfactory	Satisfactory	Satisfactory
Flexibility	Limited	Limited	Limited	Limited	Limited
Firewall and router combined method	Limited	Good	Good	Good	Limited

David C. Chou, David C. Yen,
Binshan Lin and
Philip Hong-Lam Cheng
*Cyberspace security
management*

Industrial Management &
Data Systems
99/8 [1999] 353-361

Quality is adversely affected without security guidelines. Security is the minimum requirement that users deem important. Without a formalized structure to prevent unsecured data from entering or exiting the system, quality is at risk. At this time the Internet is filled with various Web sites that are subjective, commentary and factual. The user must determine the relevance of the data.

A secure Internet will perpetuate higher quality input and output. Quality output is only derived when there is quality input. Quality at this time is a subjective measure based on the user's ability to access and retrieve information. Accessibility, site locations, and content are the quality concerns related to "security". Quality will become more important to "the players" when secure parameters are established. Until this time,

the Internet is one of the freest environments for communications.

References

- Angell, D. and Zelhka, E. (1997), "The copyright question", *Internet World Magazine*, pp. 65-6.
- Appelman, D. L. (1996), "Internet law: policing the Net's red light district - efforts to combat obscenity imperil on-line providers", *The National Law Journal*, March 25, Section C, pp. 21-2.
- Barrett, D.J. (1996), *Bandits on the Information Superhighway*, O'Reilly & Associates, Inc., Sebastopol, CA.
- Cross, R.H. and Yen, D.C. (1989), "Security in the network environment", *Journal of Computer Information Systems*, Vol. 29 No. 1, pp. 14-20.
- Godwin, M. (1996), "Law of the Net: an ill-defined Act", *Internet World Magazine*, June, pp. 90-2.