Financial Institution Letters

Security Risks Associated with the Internet

FIL-131-97
December 18, 1997

TO: CHIEF EXECUTIVE OFFICER
SUBJECT: *FDIC Issues Paper on Risks Related to Internet Use*

In response to the ever-increasing number of financial institutions using the Internet, the FDIC has issued the attached paper identifying many of the risks to an institution's information system security associated with Internet use. The paper also describes several risk controls.

The Internet offers financial institutions a wide array of opportunities to access resources and to deliver information, products and services. However, the principal benefits of Internet access, namely its global reach and open architecture, also present significant security risks.

The paper, *Security Risks Associated with the Internet*, offers helpful information to financial institutions that are currently using or are planning to use the Internet as an information resource or delivery channel. The paper does not make specific recommendations as to which technical solutions an institution should deploy. This will depend on each institution's individual system design and objectives. However, bank management must recognize the risks that the Internet presents and implement appropriate controls. Further, given the dynamics of technology, risks and controls should continue to be evaluated on an ongoing basis.

This paper is designed to complement the FDIC's safety and soundness examination procedures for electronic banking activities. The safety and soundness procedures focus on non-technical functions such as planning, administration, internal controls, and policies and procedures. Technical examinations of these systems are referred to FDIC information systems specialists and electronic banking subject matter experts. The FDIC has initiated a comprehensive training program for these specialists and is developing technical examination work programs.

For further information, please contact your Division of Supervision Regional Office or Examination Specialist Cynthia A. Bonnette at (202) 898-6583.

Nicholas J. Ketcha Jr.
Director

Attachment

Distribution: FDIC-Supervised Banks (Commercial and Savings)

NOTE: Paper copies of FDIC financial institution letters may be obtained through the FDIC's Public Information Center, 801 17th St., NW, Room 100, Washington, DC 20434 (800-276-6003 or 202-416-6940).

Security Risks Associated with the Internet

Federal Deposit Insurance Corporation
Division of Supervision
December 1997

SECURITY RISKS ASSOCIATED WITH THE INTERNET

I. Purpose

This paper alerts financial institutions to the fundamental technological risks presented by use of the Internet. Regardless of whether systems are maintained in-house or services are outsourced, bank management is responsible for protecting systems and data from compromise. This paper is intended to provide foundational information to be considered by management, but should not be relied upon to identify all potential risk factors. Appendix A discusses applicable security measures.

II. Background

Continuing advances in technology and its prominent role in commerce are leading financial institutions toward the Internet in increasing numbers. Uses of the Internet may include information-only, information transfer, or fully transactional sites on the World Wide Web (Web), or the capability to access the Internet may exist from within the institution. Regardless of the use, numerous risks exist which must be addressed within the bank's risk management program. Security breaches due to some of the following factors may currently be rare, but as banks expand their role in electronic commerce they could potentially become prominent targets of malicious activities.

III. Security Risks

The Internet is inherently insecure. By design, it is an open network which facilitates the flow of information between computers. Technologies are being developed so the Internet may be used for secure electronic commerce transactions, but failure to review and address the inherent risk factors increases the likelihood of system or data compromise. Five areas of concern relating to both transactional and system security issues, as discussed below, are: Data Privacy and Confidentiality, Data Integrity, Authentication, Non-repudiation, and Access Control/System Design.

Data Privacy and Confidentiality

Unless otherwise protected, all data transfers, including electronic mail, travel openly over the Internet and can be monitored or read by others. Given the volume of transmissions and the numerous paths available for data travel, it is unlikely that a particular transmission would be monitored at random. However, programs, such as "sniffer" programs, can be set up at opportune locations on a network, like Web servers (i.e., computers that provide services to other computers on the Internet), to simply look for and collect certain types of data. Data collected from such programs can include account numbers (e.g., credit cards, deposits, or loans) or passwords.

Due to the design of the Internet, data privacy and confidentiality issues extend beyond data transfer and include any connected data storage systems, including network drives. Any data stored on a Web server may be susceptible to compromise if proper security precautions are not taken.

Data Integrity

Potentially, the open architecture of the Internet can allow those with specific knowledge and tools to alter or modify data during a transmission. Data integrity could also be compromised within the data storage system itself, both intentionally and unintentionally, if proper access controls are not maintained. Steps must be taken to ensure that all data is maintained in its original or intended form.

Authentication

Essential in electronic commerce is the need to verify that a particular communication, transaction, or access request is legitimate. To illustrate, computer systems on the Internet are identified by an Internet protocol (IP) address, much like a telephone is identified by a phone number. Through a variety of techniques, generally known as "IP spoofing" (i.e., impersonating), one computer can actually claim to be another. Likewise, user identity can be misrepresented as well. In fact, it is relatively simple to send e-mail which appears to have come from someone else, or even send it anonymously. Therefore, authentication controls are necessary to establish the identities of all parties to a communication.

Non-repudiation

Non-repudiation involves creating proof of the origin or delivery of data to protect the sender against false denial by the recipient that the data has been received or to protect the recipient against false denial by the sender that the data has been sent. To ensure that a transaction is enforceable, steps must be taken to prohibit parties from disputing the validity of, or refusing to acknowledge, legitimate communications or transactions.

Access Control / System Design

Establishing a link between a bank's internal network and the Internet can create a number of additional access points into the internal operating system. Furthermore, because the Internet is global, unauthorized access attempts might be initiated from anywhere in the world. These factors present a heightened risk to systems and data, necessitating strong security measures to control access. Because the security of any network is only as strong as its weakest link, the functionality of all related systems must be protected from attack and unauthorized access. Specific risks include the destruction, altering, or theft of data or funds; compromised data confidentiality; denial of service (system failures); a damaged public image; and resulting legal implications. Perpetrators may include hackers, unscrupulous vendors, former or disgruntled employees, or even agents of espionage.

The following topics represent potential areas of vulnerability related to access control and system design.

System Architecture and Design

The Internet can facilitate unchecked and/or undesired access to internal systems, unless systems are appropriately designed and controlled. Unwelcome system access could be achieved through IP spoofing techniques, where an intruder may impersonate a local or internal system and be granted access without a password. If access to the system is based only on an IP address, any user could gain access by masquerading as a legitimate, authorized user by "spoofing" the user's address. Not only could any user of that system gain access to the targeted system, but so could any system that it trusts.

Improper access can also result from other technically permissible activities that have not been properly restricted or secured. For example, application layer protocols are the standard sets of rules that determine how computers communicate across the Internet. Numerous application layer protocols, each with different functions and a wide array of data exchange capabilities, are utilized on the Internet. The most familiar, Hyper Text Transfer Protocol (HTTP), facilitates the movement of text and images. But other types of protocols, such as File Transfer Protocol (FTP), permit the transfer, copying, and deleting of files between computers. Telnet protocol actually enables one computer to log in to another. Protocols such as FTP and Telnet exemplify activities which may be improper for a given system, even though the activities are within the scope of the protocol architecture.

The open architecture of the Internet also makes it easy for system attacks to be launched against systems from anywhere in the world. Systems can even be accessed and then used to launch attacks against other systems. A typical attack would be a denial of service attack, which is intended to bring down a server, system, or application. This might be done by overwhelming a system with so many requests that it shuts down. Or, an attack could be as simple as accessing and altering a Web site, such as changing advertised rates on certificates of deposit.

Security Scanning Products

A number of software programs exist which run automated security scans against Web servers, firewalls, and internal networks. These programs are generally very effective at identifying weaknesses that may allow unauthorized system access or other attacks against the system. Although these products are marketed as security tools to system administrators and information systems personnel, they are available to anyone and may be used with malicious intent. In some cases, the products are freely available on the Internet.

Logical Access Controls

A primary concern in controlling system access is the safeguarding of user IDs and passwords. The Internet presents numerous issues to consider in this regard. Passwords can be obtained through deceptive "spoofing" techniques such as redirecting users to false Web sites where passwords or user names are entered, or creating shadow copies of Web sites where attackers can monitor all activities of a user. Many "spoofing" techniques are hard to identify and guard against, especially for an average user, making authentication processes an important defense mechanism.

The unauthorized or unsuspected acquisition of data such as passwords, user IDs, e-mail addresses, phone numbers, names, and addresses, can facilitate an attempt at unauthorized access to a system or application. If passwords and user IDs are a derivative of someone's personal information, malicious parties could use the information in software programs specifically designed to generate possible passwords. Default files on a computer, sometimes called "cache" files, can automatically retain images of such data received or sent over the Internet, making them a potential target for a system intruder.

Security Flaws and Bugs / Active Content Languages

Vulnerabilities in software and hardware design also represent an area of concern. Security problems are often identified after the release of a new product, and solutions to correct security flaws commonly contain flaws themselves. Such vulnerabilities are usually widely publicized, and the identification of new bugs is constant. These bugs and flaws are often serious enough to compromise system integrity. Security flaws and exploitation guidelines are also frequently available on hacker Web sites. Furthermore, software marketed to the general public may not contain sufficient security controls for financial institution applications.

Newly developed languages and technologies present similar security concerns, especially when dealing with network software or active content languages which allow computer programs to be attached to Web pages (e.g., Java, ActiveX). Security flaws identified in Web browsers (i.e., application software used to navigate the Internet) have included bugs which, theoretically, may allow the installation of programs on a Web server, which could then be used to back into the bank's system. Even if new technologies are regarded as secure, they must be managed properly. For example, if controls over active content languages are inadequate, potentially hostile and malicious programs could be automatically downloaded from the Internet and executed on a system.

Viruses / Malicious Programs

Viruses and other malicious programs pose a threat to systems or networks that are connected to the Internet, because they may be downloaded directly. Aside from causing destruction or damage to data, these programs could open a communication link with an external network, allowing unauthorized system access, or even initiating the transmission of data.

IV. Conclusion

Utilization of the Internet presents numerous issues and risks which must be addressed. While many aspects of system performance will present additional challenges to the bank, some will be beyond the bank's control. The reliability of the Internet continues to improve, but situations including delayed or misdirected transmissions and operating problems involving Internet Service Providers (ISPs) could also have an effect on related aspects of the bank's business.

The risks will not remain static. As technologies evolve, security controls will improve; however, so will the tools and methods used by others to compromise data and systems. Comprehensive security controls must not only be implemented, but also updated to guard against current and emerging threats. Security controls that address the risks presented in this letter are discussed in Appendix A.

APPENDIX A

SECURITY MEASURES

PART ONE: Discusses the primary interrelated technologies, standards, and controls that presently exist to manage the risks of data privacy and confidentiality, data integrity, authentication, and non-repudiation.

I. Encryption, Digital Signatures, and Certificate Authorities

Encryption techniques directly address the security issues surrounding data privacy, confidentiality, and data integrity. Encryption technology is also employed in digital signature processes, which address the issues of authentication and non-repudiation. Certificate authorities and digital certificates are emerging to address security concerns, particularly in the area of authentication. The function of and the need for encryption, digital signatures, certificate authorities, and digital certificates differ depending on the particular security issues presented by the bank's activities. The technologies, implementation standards, and the necessary legal infrastructure continue to evolve to address the security needs posed by the Internet and electronic commerce.

Encryption

Encryption, or cryptography, is a method of converting information to an unintelligible code. The process can then be reversed, returning the information to an understandable form. The information is encrypted (encoded) and decrypted (decoded) by what are commonly referred to as "cryptographic keys." These "keys" are actually values, used by a mathematical algorithm to transform the data. The effectiveness of encryption technology is determined by the strength of the algorithm, the length of the key, and the appropriateness of the encryption system selected.

Because encryption renders information unreadable to any party without the ability to decrypt it, the information remains private and confidential, whether being transmitted or stored on a system. Unauthorized parties will see nothing but an unorganized assembly of characters. Furthermore, encryption technology can provide assurance of data integrity as some algorithms offer protection against forgery and tampering. The ability of the technology to protect the information requires that the encryption and decryption keys be properly managed by authorized parties.

Symmetric and Asymmetric Key Systems

There are two types of cryptographic key systems, symmetric and asymmetric. With a symmetric key system (also known as secret key or private key systems), all parties have the same key. The keys can be used to encrypt and decrypt messages, and must be kept secret or the security is compromised. For the parties to get the same key, there has to be a way to securely distribute the key to each party. While this can be done, the security controls necessary make this system impractical for widespread and commercial use on an open network like the Internet. Asymmetric key systems can solve this problem.

In an asymmetric key system (also known as a public key system), two keys are used. One key is kept secret, and therefore is referred to as the "private key." The other key is made widely available to anyone who wants it, and is referred to as the "public key." The private and public keys are mathematically related so that information encrypted with the private key can only be decrypted by the corresponding public key. Similarly, information encrypted with the public key can only be decrypted by the corresponding private key. The private key, regardless of the key system utilized, is typically specific

to a party or computer system. Therefore, the sender of a message can be authenticated as the private key holder by anyone decrypting the message with a public key. Importantly, it is mathematically impossible for the holder of any public key to use it to figure out what the private key is. The keys can be stored either on a computer or on a physically separate medium such as a smart card.

Regardless of the key system utilized, physical controls must exist to protect the confidentiality and access to the key(s). In addition, the key itself must be strong enough for the intended application. The appropriate encryption key may vary depending on how sensitive the transmitted or stored data is, with stronger keys utilized for highly confidential or sensitive data. Stronger encryption may also be necessary to protect data that is in an open environment, such as on a Web server, for long time periods. Because the strength of the key is determined by its length, the longer the key, the harder it is for high-speed computers to break the code.

Digital Signatures

Digital signatures authenticate the identity of a sender, through the private, cryptographic key. In addition, every digital signature is different because it is derived from the content of the message itself. The combination of identity authentication and singularly unique signatures results in a transmission that cannot be repudiated.

Digital signatures can be applied to any data transmission, including e-mail. To generate a digital signature, the original, unencrypted message is run through a mathematical algorithm that generates what is known as a message digest (a unique, character representation of the data). This process is known as the "hash." The message digest is then encrypted with a private key, and sent along with the message. The recipient receives both the message and the encrypted message digest. The recipient decrypts the message digest, and then runs the message through the hash function again. If the resulting message digest matches the one sent with the message, the message has not been altered and data integrity is verified. Because the message digest was encrypted with a private key, the sender can be identified and bound to the specific message. The digital signature cannot be reused, because it is unique to the message. In the above example, data privacy and confidentiality could also be achieved by encrypting the message itself. The strength and security of a digital signature system is determined by its implementation, and the management of the cryptographic keys.

Certificate Authorities and Digital Certificates

Certificate authorities and digital certificates are emerging to further address the issues of authentication, non-repudiation, data privacy, and cryptographic key management. A certificate authority (CA) is a trusted third party that verifies the identity of a party to a transaction. To do this, the CA vouches for the identity of a party by attaching the CA's digital signature to any messages, public keys, etc., which are transmitted. Obviously, the CA must be trusted by the parties involved, and identities must have been proven to the CA beforehand. Digital certificates are messages that are signed with the CA's private key. They identify the CA, the represented party, and could even include the represented party's public key.

The responsibilities of CAs and their position among emerging technologies continue to develop. They are likely to play an important role in key management by issuing, retaining, or distributing public/private key pairs.

Implementation

The implementation and use of encryption technologies, digital signatures, certificate authorities, and digital certificates can vary. The technologies and methods can be used individually, or in combination with one another. Some techniques may merely encrypt data in transit from one location to another. While this keeps the data confidential during transmission, it offers little in regard to authentication and non-repudiation. Other techniques may utilize digital signatures, but still require the encrypted submission of sensitive information, like credit card numbers. Although protected during transmission, additional measures would need to be taken to ensure the sensitive information remains protected once received and stored.

The protection afforded by the above security measures will be governed by the capabilities of the technologies, the appropriateness of the technologies for the intended use, and the administration of the technologies utilized. Care should be taken to ensure the techniques utilized are sufficient to meet the required needs of the institution. All of the technical and implementation differences should be explored when determining the most appropriate package.

PART TWO: Discusses the primary technical and procedural security measures necessary to properly govern access control and system security.

I. System Architecture and Design

Measures to address access control and system security start with the appropriate system architecture. Ideally, if an Internet connection is to be provided from within the institution, or a Web site established, the connection should be entirely separate from the core processing system. If the Web site is placed on its own server, there is no direct connection to the internal computer system. However, appropriate firewall technology may be necessary to protect Web servers and/or internal systems.

Placing a "screening router" between the firewall and other servers provides an added measure of protection, because requests could be segregated and routed to a particular server (such as a financial information server or a public information server). However, some systems may be considered so critical, they should be completely isolated from all other systems or networks. Security can also be enhanced by sending electronic transmissions from external sources to a machine that is not connected to the main operating system.

II. Firewalls

Description, Configuration, and Placement

A firewall is a combination of hardware and software placed between two networks which all traffic, regardless of the direction, must pass through. When employed properly, it is a primary security measure in governing access control and protecting the internal system from compromise.

The key to a firewall's ability to protect the network is its configuration and its location within the system. Firewall products do not afford adequate security protection as purchased. They must be set up, or configured, to permit or deny the appropriate traffic. To provide the most security, the underlying rule should be to deny all traffic unless expressly permitted. This requires system administrators to review and evaluate the need for all permitted activities, as well as who may need to use them. For example, to protect against Internet protocol (IP) spoofing, data arriving from an outside network that claims to be originating from an internal computer should be denied access. Alternatively, systems could be denied access based on their IP address, regardless of the origination point. Such requests could then be evaluated based on what information was requested and where in the internal system it was requested from. For instance, incoming FTP requests may be permitted, but outgoing FTP requests denied.

Often, there is a delicate balance between what is necessary to perform business operations and the need for security. Due to the intricate details of firewall programming, the configuration should be reassessed after every system change or software update. Even if the system or application base does not change, the threats to the system do. Evolving risks and threats should be routinely monitored and considered to ensure the firewall remains an adequate security measure. If the firewall system should ever fail, the default should deny all access rather than permit the information flow to continue. Ideally, firewalls should be installed at any point where a computer system comes into contact with another network. The firewall system should also include alerting mechanisms to identify and record successful and attempted attacks and intrusions. In addition, detection mechanisms and procedures should include the generation and routine review of security logs.

Data Transmission and Types of Firewalls

Data traverses the Internet in units referred to as packets. Each packet has headers which contain

information for delivery, such as where the packet is from, where it is going, and what application it contains. The varying firewall techniques examine the headers and either permit or deny access to the system based on the firewall's rule configuration.

There are different types of firewalls that provide various levels of security. For instance, packet filters, sometimes implemented as screening routers, permit or deny access based solely on the stated source and/or destination IP address and the application (e.g., FTP). However, addresses and applications can be easily falsified, allowing attackers to enter systems. Other types of firewalls, such as circuit-level gateways and application gateways, actually have separate interfaces with the internal and external (Internet) networks, meaning no direct connection is established between the two networks. A relay program copies all data from one interface to another, in each direction. An even stronger firewall, a stateful inspection gateway, not only examines data packets for IP addresses, applications, and specific commands, but also provides security logging and alarm capabilities, in addition to historical comparisons with previous transmissions for deviations from normal context.

Implementation

When evaluating the need for firewall technology, the potential costs of system or data compromise, including system failure due to attack, should be considered. For most financial institution applications, a strong firewall system is a necessity. All information into and out of the institution should pass through the firewall. The firewall should also be able to change IP addresses to the firewall IP address, so no inside addresses are passed to the outside. The possibility always exists that security might be circumvented, so there must be procedures in place to detect attacks or system intrusions. Careful consideration should also be given to any data that is stored or placed on the server, especially sensitive or critically important data.

III. Product Certification and Security Scanning Products

Several organizations exist which independently assess and certify the adequacy of firewalls and other computer system related products. Typically, certified products have been tested for their ability to permit and sustain business functions while protecting against both common and evolving attacks.

Security scanning tools should be run frequently by system administrators to identify any new vulnerabilities or changes in the system. Ideally, the scan should be run both with and without the firewall in place so the firewall's protective capabilities can be fully evaluated. Identifying the susceptibility of the system without the firewall is useful for determining contingency procedures should the firewall ever go down. Some scanning tools have different versions with varying degrees of intrusion/attack attempts.

IV. Logical Access Controls

If passwords are used for access control or authentication measures, users should be properly educated in password selection. Strong passwords consist of at least six to eight alpha numeric characters, with no resemblance to any personal data. PINs should also be unique, with no resemblance to personal data. Neither passwords nor PINs should ever be reduced to writing or shared with others.

Other security measures should include the adoption of one-time passwords, or password aging measures that require periodic changes. Encryption technology can also be employed in the entry and transmission of passwords, PINs, user IDs, etc. Any password Directories or databases should be properly protected, as well.

Password guessing programs can be run against a system. Some can run through tens of thousands of password variations based on personal information, such as a user's name or address. It is preferable to test for such vulnerabilities by running this type of program as a preventive measure, before an unauthorized party has the opportunity to do so. Incorporating a brief delay requirement after each incorrect login attempt can be very effective against these types of programs. In cases where a potential attacker is monitoring a network to collect passwords, a system utilizing one-time passwords would

render any data collected useless.

When additional measures are necessary to confirm that passwords or PINs are entered by the user, technologies such as tokens, smart cards, and biometrics can be useful. Utilizing these technologies adds another dimension to the security structure by requiring the user to possess something physical.

Tokens

Token technology relies on a separate physical device, which is retained by an individual, to verify the user's identity. The token resembles a small hand-held card or calculator and is used to generate passwords. The device is usually synchronized with security software in the host computer such as an internal clock or an identical time based mathematical algorithm. Tokens are well suited for one-time password generation and access control. A separate PIN is typically required to activate the token.

Smart Cards

Smart cards resemble credit cards or other traditional magnetic stripe cards, but contain an embedded computer chip. The chip includes a processor, operating system, and both read only memory (ROM) and random access memory (RAM). They can be used to generate one-time passwords when prompted by a host computer, or to carry cryptographic keys. A smart card reader is required for their use.

Biometrics

Biometrics involves identification and verification of an individual based on some physical characteristic, such as fingerprint analysis, hand geometry, or retina scanning. This technology is advancing rapidly, and offers an alternative means to authenticate a user.

V. Security Flaws and Bugs

Because hardware and software continue to improve, the task of maintaining system performance and security is ongoing. Products are frequently issued which contain security flaws or other bugs, and then security patches and version upgrades are issued to correct the deficiencies. The most important action in this regard is to keep current on the latest software releases and security patches. This information is generally available from product developers and vendors. Also important is an understanding of the products and their security flaws, and how they may affect system performance. For example, if there is a time delay before a patch will be available to correct an identified problem, it may be necessary to invoke mitigating controls until the patch is issued.

Reference sources for the identification of software bugs exist, such as the Computer Emergency Response Team Coordination Center (CERT/CC) at the Software Engineering Institute of Carnegie Mellon University, Pittsburgh, Pennsylvania. The CERT/CC, among other activities, issues advisories on security flaws in software products, and provides this information to the general public through subscription e-mail, Internet newsgroups (Usenet), and their Web site at www.cert.org. Many other resources are freely available on the Internet.

Active Content Languages

Active content languages have been the subject of a number of recent security discussions within the technology industry. While it is not their only application, these languages allow computer programs to be attached to Web pages. As such, more appealing and interactive Web pages can be created, but this function may also allow unauthorized programs to be automatically downloaded to a user's computer. To date, few incidents have been reported of harm caused by such programs; however, active content programs could be malicious, designed to access or damage data or insert a virus.

Security problems may result from an implementation standpoint, such as how the languages and developed programs interact with other software, such as Web browsers. Typically, users can disable

the acceptance of such programs on their Web browser. Or, users can configure their browser so they may choose which programs to accept and which to deny. It is important for users to understand how these languages function and the risks involved, so that they make educated decisions regarding their use. Security alerts concerning active content languages are usually well publicized and should receive prompt reviews by those utilizing the technology.

VI. Viruses

Because potentially malicious programs can be downloaded directly onto a system from the Internet, virus protection measures beyond the traditional boot scanning techniques may be necessary to properly protect servers, systems, and workstations. Additional protection might include anti-virus products that remain resident, providing for scanning during downloads or the execution of any program. It is also important to ensure that all system users are educated in the risks posed to systems by viruses and other malicious programs, as well as the proper procedures for accessing information and avoiding such threats.