WIRELESS NETWORKS AND CUSTOMER ACCESS

FIL-8-2002
February 1, 2002

TO: CHIEF EXECUTIVE OFFICER

SUBJECT: *Guidance on Managing Risks Associated With Wireless Networks and Wireless Customer Access*

Financial institutions are actively evaluating and implementing wireless technology as a means to reach customers and reduce the costs of implementing new networks. In light of this fast-developing trend, the Federal Deposit Insurance Corporation (FDIC) is providing financial institutions with the following information about the risks associated with wireless technology and suggestions on managing those risks. Please share this information with your Chief Information Officer.

Wireless Technology and the Risks of Implementation

Wireless networks are rapidly becoming a cost-effective alternative for providing network connectivity to financial institution information systems. Institutions that are installing new networks are finding the installation costs of wireless networks competitive compared with traditional network wiring. Performance enhancements in wireless technology have also made the adoption of wireless networks attractive to institutions. Wireless networks operate at speeds that are sufficient to meet the needs of many institutions and can be seamlessly integrated into existing networks. Wireless networks can also be used to provide connectivity between geographically close locations without having to install dedicated lines.

Wireless Internet access to banking applications is also becoming attractive to financial institutions. It offers customers the ability to perform routine banking tasks while away from the bank branch, automated teller machines or their own personal computers. Wireless Internet access is a standard feature on many new cellular phones and hand-held computers.

Many of the risks that financial institutions face when implementing wireless technology are risks that exist in any networked environment (see FIL-67-2000, "Security Monitoring of Computer Networks," dated October 3, 2000, and the 1996 FFIEC Information Systems Examination Handbook, Volume 1, Chapter 15). However, wireless technology carries additional risks that financial institutions should consider when designing, implementing and operating a wireless network. Common risks include the potential:

- Compromise of customer information and transactions over the wireless network;
- Disruption of wireless service from radio transmissions of other wireless devices;
- Intrusion into the institution's network through wireless network connections; and
- Obsolescence of current systems due to rapidly changing standards.

These risks could ultimately compromise the bank's computer system, potentially causing:

- Financial loss due to the execution of unauthorized transactions;
- Disclosure of confidential customer information, resulting in - among other things - identity theft (see FIL-39-2001, "Guidance on Identity Theft and Pretext Calling," dated May 9, 2001, and FIL-22-2001, "Guidelines Establishing Standards for Safeguarding Customer Information," dated March 14, 2001);
- Negative media attention, resulting in harm to the institution's reputation; and
- Loss of customer confidence.

Risk Mitigation

Security should not be compromised when offering wireless financial services to customers or deploying wireless internal networks. Financial institutions should carefully consider the risks of wireless technology and take appropriate steps to mitigate those risks before deploying either wireless networks or applications. As wireless technologies evolve, the security and control features available to financial institutions will make the process of risk mitigation easier. Steps that can be taken immediately in wireless implementation include:

- Establishing a minimum set of security requirements for wireless networks and applications;
- Adopting proven security policies and procedures to address the security weaknesses of the wireless environment;
- Adopting strong encryption methods that encompass end-to-end encryption of information as it passes throughout the wireless network;
- Adopting authentication protocols for customers using wireless applications that are separate and distinct from those provided by the wireless network operator;
- Ensuring that the wireless software includes appropriate audit capabilities (for such things as recording dropped transactions);
- Providing appropriate training to IT personnel on network, application and security controls so that they understand and can respond to potential risks; and
- Performing independent security testing of wireless network and application implementations.

Additional information about wireless networks and wireless customer access appears in the Appendix, available on the FDIC's Web site at www.fdic.gov. You may also contact Jeffrey M. Kopchik, Senior Policy Analyst, E-Banking Branch, Division of Supervision, on 202-898-3872.

Michael J. Zamorski
Director

Appendix

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 Street, NW, Room 100, Washington, DC 20434 (800-276-6003 or 202-416-6940).

APPENDIX

Wireless Networks and Customer Access

The following discussion addresses the critical components and supporting principles for implementing security and controls around a wireless network environment.

PART I. Risks Associated with Wireless Internal Networks
Financial institutions are evaluating wireless networks as an alternative to the traditional cable to the desktop network. Currently, wireless networks can provide speeds of up to 11Mbps between the workstation and the wireless access device without the need for cabling individual workstations. Wireless networks also offer added mobility allowing users to travel through the facility without losing their network connection. Wireless networks are also being used to provide connectivity between geographically close locations as an alternative to installing dedicated telecommunication lines.

Wireless differs from traditional hard-wired networking in that it provides connectivity to the network by broadcasting radio signals through the airways. Wireless networks operate using a set of FCC licensed frequencies to communicate between workstations and wireless access points. By installing wireless access points, an institution can expand its network to include workstations within broadcast range of the network access point.

The most prevalent class of wireless networks currently available is based on the IEEE 802.11b wireless standard. The standard is supported by a variety of vendors for both network cards and wireless network access points. The wireless transmissions can be encrypted using "Wired Equivalent Privacy" (WEP) encryption. WEP is intended to provide confidentiality and integrity of data and a degree of access control over the network. By design, WEP encrypts traffic between an access point and the client. However, this encryption method has fundamental weaknesses that make it vulnerable. WEP is vulnerable to the following types of decryption attacks:

- Decrypting information based on statistical analysis;
- Injecting new traffic from unauthorized mobile stations based on known plain text;
- Decrypting traffic based on tricking the access point;
- Dictionary-building attacks that, after analyzing about a day's worth of traffic, allow real-time automated decryption of all traffic (a dictionary-building attack creates a translation table that can be used to convert encrypted information into plain text without executing the decryption routine); and
- Attacks based on documented weaknesses in the RC4 encryption algorithm that allow an attacker to rapidly determine the encryption key used to encrypt the user's session).

Using WEP by itself to provide wireless network security may lead a financial institution to a false sense of security. Information traveling over the network appears secure because it is encrypted. This appearance of security, however, can be defeated in a relatively short time.

Through these types of attacks, unauthorized personnel could gain access to the financial institution's data and systems. For example, an attacker with a laptop computer and a wireless network card could eavesdrop on the bank's network, obtain private customer information, obtain access to bank systems and initiate unauthorized transactions against customer accounts.

Another risk in implementing wireless networks is the potential disruption of wireless service caused by radio transmissions of other devices. For example, the frequency range used for 802.11b equipment is also shared by microwave ovens, cordless phones and other radio-wave-emitting equipment that can potentially interfere with transmissions and lower network performance. Also, as wireless workstations are added within a relatively small area, they will begin to compete with each other for wireless bandwidth, decreasing the overall performance of the wireless network.

Risk Mitigation Components -- Wireless Internal Networks

A key step in mitigating security risks related to the use of wireless technologies is to create policies, standards and procedures that establish minimum levels of security. Financial institutions should adopt standards that require end-to-end encryption for wireless communications based on proven encryption methods. Also, as wireless technologies evolve, new security and control weaknesses will likely be identified in the wireless software and security protocols. Financial institutions should actively monitor security alert organizations for notices related to their wireless network devices.

For wireless internal networks, financial institutions should adopt standards that require strong encryption of the data stream through technologies such as the IP Security Protocol (IPSEC). These methods effectively establish a virtual private network between the wireless workstation and other components of the network. Even though the underlying WEP encryption may be broken, an attacker would be faced with having to defeat an industry-proven security standard.

Financial institutions should also consider the proximity of their wireless networks to publicly available places. A wireless network that does not extend beyond the confines of the financial institution's office space carries with it far less risk than one that extends into neighboring buildings. Before bringing a wireless network online, the financial institution should perform a limited pilot to test the effective range of the wireless network and consider positioning devices in places where they will not broadcast beyond the office space. The institution should also be mindful that each workstation with a wireless card is a transmitter. Confidential customer information may be obtained by listening in on the workstation side of the conversation, even though the listener may be out of range of the access device.

The financial institution should consider having regular independent security testing performed on its wireless network environment. Specific testing goals would include the verification of appropriate security settings, the effectiveness of the wireless security implementation and the identification of rogue wireless devices that do not conform to the institution's stated standards. The security testing should be performed by an organization that is technically qualified to perform wireless testing and demonstrates appropriate ethical behavior.

Part II. Risks Associated with Wireless Internet Devices

As wireless Internet devices become more prevalent in the marketplace, financial institutions are adopting wireless application technologies as a channel for reaching their customers. Wireless Internet services are becoming available in major cities across the United States. Through wireless banking applications, a financial institution customer could access account information and perform routine non-cash transactions without having to visit a branch or ATM.

The wireless Internet devices available today present attractive methods for offering and using financial services. Customers have access to financial information from anywhere they can receive wireless Internet access. Many of the wireless devices have built-in encryption through industry-standard encryption methods. This encryption has its limits based on the processing capabilities of the device and the underlying network architecture.

A popular standard for offering wireless applications is through the use of the Wireless Application Protocol (WAP). WAP is designed to bring Internet application capabilities to some of the simplest user interfaces. Unlike the Web browser that is available on most personal computer workstations, the browser in a wireless device (such as a cell phone) has a limited display that in many cases can provide little, if any, graphical capabilities. The interface is also limited in the amount of information that can be displayed easily on the screen. Further, the user is limited by the keying capabilities of the device and often must resort to many key presses for simple words.

The limited processing capabilities of these devices restrict the robustness of the encryption network transmissions. Effective encryption is, by nature, processing-intensive and often requires complex calculations. The time required to complete the encryption calculations on a device with limited processing capabilities may result in unreasonable delays for the device's user. Therefore, simpler encryption algorithms and smaller keys may be used to speed the process of obtaining access.

WAP is an evolving protocol. The most recent specification of WAP (WAP 2.0 - July 2001) offers the

capability of encrypting network conversations all the way from the WAP server (at the financial institution) to the WAP client (the financial institution customer). Unfortunately, WAP 2.0 has not yet been fully adopted by vendors that provide the building blocks for WAP applications. Previous versions of WAP provide encryption between the WAP client and a WAP gateway (owned by the Wireless Provider). The WAP gateway then must re-encrypt the information before it is sent across the Internet to the financial institution. Therefore, sensitive information is available at the wireless provider in an unencrypted form. This limits the financial institution's ability to provide appropriate security over customer information.

Risk Mitigation Components - Wireless Internet Devices

For wireless customer access, the financial institution should institute policies and standards requiring that information and transactions be encrypted throughout the link between the customer and the institution. Financial institutions should carefully consider the impact of implementing technologies requiring that a third party have control over unencrypted customer information and transactions.

As wireless application technologies evolve, new security and control weaknesses will likely be identified in the wireless software and security protocols. Financial institutions should actively monitor security alert organizations for notices related to their wireless application services. They should also consider informing customers when wireless Internet devices that require the use of communications protocols deemed insecure will no longer be supported by the institution.

The financial institution should consider having regular independent security testing performed on its wireless customer access application. Specific testing goals would include the verification of appropriate security settings, the effectiveness of the wireless application security implementation and conformity to the institution's stated standards. The security testing should be performed by an organization that is technically qualified to perform wireless testing and demonstrates appropriate ethical behavior.

Part III. Risks Associated with Both Internal Wireless Networks and Wireless Internet Devices

Evolution and Obsolescence

As the wireless technologies available today evolve, financial institutions and their customers face the risk of current investments becoming obsolete in a relatively short time. As demonstrated by the weaknesses in WEP and earlier versions of WAP and the changes in standards for wireless technologies, wireless networking as a technology may change significantly before it is considered mature. Financial institutions that invest heavily in components that may become obsolete quickly may feel the cost of adopting an immature technology.

Controlling the Impact of Obsolescence

Wireless internal networks are subject to the same types of evolution that encompass the computing environment in general. Key questions to ask a vendor before purchasing a wireless internal network solution include:

- What is the upgrade path to the next class of network?
- Do the devices support firmware (Flash) upgrades for security patches and upgrades?
- How does the vendor distribute security information and patches?

The financial institution should also consider the evolving standards of the wireless community. Before entering into an expensive implementation, the institution should research when the next major advances in wireless are likely to be released. Bank management can then make an informed decision on whether the implementation should be based on currently available technology or a future implementation based on newer technology.

The potential obsolescence of wireless customer access can be controlled in other ways. As the financial institution designs applications that are to be delivered through wireless devices, they should

design the application so that the business logic is not tied to a particular wireless technology. This can be accomplished by placing the majority of the business logic on back-end or mid-tier servers that are independent of the wireless application server. The wireless application server then becomes a connection point between the customer and the transactions performed. As the institution decides to upgrade or replace the application server, the business logic can remain relatively undisturbed.