Federal Deposit Insurance Corporation
550 17th Street NW, Washington, D.C. 20429-9990

Financial Institution Letter
FIL-69-2005
July 27, 2005

VOICE OVER INTERNET PROTOCOL
Guidance on the Security Risks of VoIP

Summary: The FDIC is providing guidance to financial institutions on the security risks associated with voice over Internet protocol (VoIP). VoIP refers to the delivery of traditional telephone voice communications over the Internet.

Distribution:
FDIC-Supervised Banks (Commercial and Savings)

Suggested Routing:
Chief Executive Officer
Chief Information Security Officer

Related Topics:
Section 501(b) of the Gramm-Leach-Bliley Act

Attachment:
Voice Over Internet Protocol (VoIP) Informational Supplement

Contact:
Examination Specialist Kathryn M. Weatherby at Kweatherby@fdic.gov or (202) 898-6793

Note:
FDIC financial institution letters (FILs) may be accessed from the FDIC's Web site at www.fdic.gov/news/news/financial/2005/index.html.

To receive FILs electronically, please visit http://www.fdic.gov/about/subscriptions/fil.html.

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 (1-877-275-3342 or 202-416-6940).

Highlights:

- VoIP is susceptible to the same security risks as data networks if security policies and configurations are inadequate.
- The risks associated with VoIP should be evaluated as part of a financial institution's periodic risk assessment, with status reports submitted to the board of directors as mandated by section 501(b) of the Gramm-Leach–Bliley Act (GLBA). Any identified weaknesses should be corrected during the normal course of business.
- The attached "Informational Supplement" details the risks associated with using VoIP.

VOICE OVER INTERNET PROTOCOL
Guidance on the Security Risks of VoIP

The Federal Deposit Insurance Corporation (FDIC) is providing guidance to financial institutions on the security risks associated with voice over Internet protocol (VoIP). VoIP refers to the transmission of voice communications over the Internet rather than through the public switched telephone network (PSTN). When a telephone call is made, VoIP translates the caller's voice into a stream of data packets by an analog-digital converter. The data packets are transmitted over the Internet and converted to a voice signal on the other end of the communication.

VoIP can be an attractive alternative to traditional telephone networks because of the potential cost savings. For example, long distance charges incurred through the PSTN can be eliminated. In addition, only one network is managed for both voice and data, resulting in additional savings. However, the initial costs for implementation of VoIP can be significant. There are also increased data security risks associated with VoIP. Before making an investment in VoIP technology, a financial institution should weigh the benefits (lower communication expenses) against the disadvantages (substantial implementation costs and increased data security risks).

Risks and Vulnerabilities

VoIP is susceptible to the same risks as data networks that use the Internet, such as exposure to viruses, worms, trojans[1] and man-in-the-middle attacks.[2] Configuration weaknesses in VoIP devices and underlying operating systems can enable denial of service attacks, eavesdropping, voice alteration (hijacking) and toll fraud (theft of service), all of which can result in the loss of privacy and integrity. In addition, industry observers are concerned about the potential exploitation of SPAM using VoIP. In this situation, SPAM would refer to unwanted and potentially offensive phone calls.

Speed is imperative to the quality of transmission, and in order to achieve adequate voice quality, VoIP requires the highest priority access to available bandwidth. VoIP must be fast enough to avoid a delay, even by milliseconds, in the processing and delivery of voice packets. The loss, out-of-sequence delivery or non-delivery of data packets can also adversely affect the quality of VoIP.

[1] Trojans are malicious programs or programming code that either masquerade as or are inserted into innocuous applications.
[2] A man-in-the-middle-attack is when an intruder sits between two parties, monitors the transmission and is then able to impersonate one of the parties.

Recommendations

Financial institutions can access various publicly available sources to develop VoIP security policies and practices. Widely accepted best practices are published by the National Institute of Standards and Technology (NIST), the agency responsible for developing information security standards for federal agencies (Special NIST Publication 800-58, *Security Considerations for Voice over IP Systems*, can be found at http://csrc.nist.gov/publications/nistpubs/800-58/SP800-58-final.pdf).

Financial institutions contemplating the use of VoIP technology should consider the following best practices. Details of these best practices are further discussed in the attached "Voice over Internet Protocol Informational Supplement."

- Ensure that the institution has examined and can acceptably manage and mitigate the risks to information, systems operations and continuity of essential operations when implementing VoIP systems.

- Assess the level of concern about security and privacy. If warranted and practical, do not use "softphone" systems, which implement VoIP using an ordinary PC with a headset and special software.

- Carefully review statutory requirements for privacy and record retention with competent legal advisors.

- Develop appropriate network architecture.

- Use VoIP-ready firewalls and other appropriate protection mechanisms. Financial institutions should enable, use and routinely test security features included in VoIP systems.

- Properly implement physical controls in a VoIP environment.

- Evaluate costs for additional backup systems that may be required to ensure continued operation during power outages.

- Consider the need to integrate mobile telephone units with the VoIP system. If the need exists, consider using products implementing WiFi Protected Access (WPA), rather than Wired Equivalent Privacy (WEP).

- Give special consideration to emergency service communications. Automatic location services are not always as available with VoIP as they are with phone calls made through the PSTN.

When a financial institution decides to invest in VoIP technology, the associated risks should be evaluated as part of a financial institution's periodic risk assessment and discussed in status reports submitted to the board of directors as mandated by section

501(b) of the Gramm-Leach-Bliley Act. Any identified weaknesses should be corrected during the normal course of business.

Conclusion

If improperly implemented, VoIP can pose significant operational risks to financial institutions. Therefore, management should perform a comprehensive risk assessment before implementation to ensure the confidentiality, integrity and availability of voice communications using VoIP technology.

Michael J. Zamorski
Director
Division of Supervision and Consumer Protection