FDIC

Division of Supervision and Consumer Protection

Voice over Internet Protocol (VoIP)

Informational Supplement

June 2005

Summary

In an attempt to control expenses, consumers and businesses are considering voice over Internet protocol (VoIP) technology. VoIP is an attractive technology because, generally, phone service using VoIP costs less than equivalent service from traditional providers. VoIP provides a mechanism for subscribers to leverage their existing high-speed Internet connection to provide telephone service.

This document supplements Financial Institution Letter-69-2005, "Guidance on the Security Risk of VoIP," and provides additional information about best practices. Due to the potential exposure of customer data from the risks associated with VoIP, financial institution boards of directors should include VoIP in their Gramm-Leach-Bliley Act risk assessment.

Vulnerabilities

VoIP sessions can be established with a variety of protocols. H.323 (International Telecommunications Union standard for real-time communication) and SIP (Session Initiation Protocol) are the most commonly used protocols. VoIP-enabled telephones, software and other network equipment should be compatible with more than one protocol to ensure future interoperability. Security vulnerabilities have been reported in these VoIP protocols. For more information, refer to the US-CERT vulnerability hyperlinks below, which describe the specific impact of the vulnerability and the systems affected.

http://www.kb.cert.org/vuls/id/528719

http://www.kb.cert.org/vuls/id/749342

Best Practices

Nine best practices cited by the National Institute of Standards and Technology (NIST) were listed in FIL-69-2005. NIST noted that "the integration of voice and data in a single network, establishing a secure VoIP and data network is a complex process that requires greater effort than that required for data-only networks." Additional information about the best practices is listed below.

1. *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.*

An especially challenging security environment is created when new technologies are deployed. Risks often are not fully understood, administrators are not yet experienced with the new technology, and security controls and policies need to be updated. Therefore, institutions should carefully consider their level of knowledge and training in the technology, the maturity and quality of their security practices, controls, policies, and architectures, and their understanding of the associated security risks. These issues

should be considered for all systems but are especially important with VoIP since voice communications are essential.

VoIP can provide more flexible service at a lower cost, but there are significant tradeoffs to consider. VoIP systems can be expected to be more vulnerable than conventional telephone systems, in part because they are tied into the data network, resulting in additional security weaknesses and avenues of attack. Confidentiality and privacy may be at greater risk in VoIP systems unless strong controls are implemented and maintained. An additional concern is the relative instability of VoIP technology compared with PSTN systems. Today, VoIP systems are still maturing and dominant standards have not emerged. This instability is compounded by VoIP's reliance on packet networks as a transport medium. While the PSTN is extremely reliable, Internet service is generally much less so. In addition, VoIP cannot function without Internet connections, except in the case of large corporate or other users who may operate a private network. Essential telephone services, unless carefully planned, deployed and maintained, will be at greater risk if based on VoIP.

2. *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*.

Because PCs are necessarily on the data network, using a softphone system conflicts with the need to separate voice and data networks. Also, worms, viruses and other malicious software are extraordinarily common on PCs connected to the Internet, and very difficult to defend against. Well-known vulnerabilities in Web browsers make it possible for attackers to download malicious software without a user's knowledge, even if the user does nothing more than visit a compromised Web site. Malicious software attached to e-mail messages can also be installed without the user's knowledge, in some cases even if the user does not open the attachment.

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

Be aware that the laws and rulings governing interception or monitoring of VoIP lines, and retention of call records, may differ from those of conventional telephone systems. Review these issues with legal advisors.

4. *Develop appropriate network architecture*.

Separate voice and data on logically different networks, if feasible.

Disallow VoIP protocols from the data network at the voice gateway that interfaces with the public switched telephone network (PSTN). Use strong authentication and access controls on the voice gateway system.

Use Internet Protocol Security (IPsec) or Secure Shell (SSH) for all remote management

and auditing access. If practical, avoid using remote management and use Internet Protocol Private Branch Exchange (IPPBX) access for a physically secure system.

Encrypt VoIP communications at the router or other gateway, not at the individual endpoints. Since some VoIP telephones are not powerful enough to perform encryption, placing this burden at a central point ensures all VoIP traffic emanating from the enterprise network will be encrypted. Newer VoIP phones are able to provide Advanced Encryption System (AES) encryption at a reasonable cost.

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

Because of the inherent vulnerabilities when operating telephony across a packet network, VoIP systems incorporate an array of security features and protocols. The institution's security policy should ensure that these features are used. In particular, firewalls designed for VoIP protocols are an essential component of a secure VoIP system.

6. *Properly implement physical controls in a VoIP environment.*

Unless the VoIP network is encrypted, anyone with physical access to the office's local area network (LAN) could potentially connect network monitoring tools and tap into telephone conversations. Although conventional telephone lines can also be monitored when physical access is obtained, in most offices there are many more points to connect to a LAN without arousing suspicion. Even if encryption is used, physical access to VoIP servers and gateways may allow an attacker to do traffic analysis (i.e., determine which parties are communicating). Adequate physical control should be in place to restrict access to VoIP network components. Physical security measures, including barriers, locks, access control systems, and guards, are the first line of defense. Proper physical countermeasures need to be in place to mitigate some of the biggest risks, such as the insertion of sniffers or other network monitoring devices. Otherwise, the installation of a sniffer could result in not just data being intercepted, but all voice communications as well.

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

A careful assessment must be conducted to ensure that sufficient backup power is available for the office VoIP switch as well as each desktop instrument. Costs may include uninterrupted power supply (UPS) battery systems or diesel powered electric generators.

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

The security features of WEP provide little or no protection because WEP can be compromised with publicly available software. The more recent WPA offers significant improvements in security and can aid the integration of wireless technology with VoIP.

9. *Give special consideration to emergency services communications (E-911) because the E-911 automatic location service is not always available with VoIP*.

Unlike traditional telephone connections, which are tied to a physical location, VoIP's packet-switched technology allows a particular telephone number to be anywhere. This is convenient for users because calls can be automatically forwarded to their locations. But there is also a tradeoff: this flexibility severely complicates the provision of E-911 service, which normally provides the caller's location to the dispatch office. Although most VoIP vendors have workable solutions for E-911 service, government regulators and vendors are still working out standards and procedures for E-911 services in a VoIP environment.