

VoIP SECURITY

As of this writing, security threats to VoIP are more hypothetical than real; there have been no significant instances of breached VoIP security. This is because most VoIP deployments are closed systems; almost no organization exposes its VoIP system to the Internet. However, once organizations begin to publicize SIP addresses on business cards and Web sites, for example, security will become an issue.

The history of the Internet teaches that it is wishful thinking to believe that there will never be threats to VoIP. So use this time to build defenses that will work when the security threats arrive.

Although a number of threats have been identified, four are most significant:

- Spam over Internet Telephony (SPIT)
- Denial of Service (DoS) attacks
- Toll fraud
- Eavesdropping

SPIT is unsolicited bulk messages broadcast over VoIP to phones connected to the Internet. Marketers can use spambots to collect VoIP addresses or hack into a computer used to route VoIP calls. Furthermore, because calls routed over IP are much more difficult to trace, the potential for fraud is significantly greater. Finally, IP telephony makes it possible to send messages in bulk, rather than dialing each number separately.

DoS A successful DoS attack renders computer resources unavailable. It generally consists of the concerted, malevolent efforts to prevent an Internet site or service from functioning efficiently or at all, temporarily or indefinitely. DoS attacks either force the targeted computers to reset, or consume its resources so that it can no longer function.

Toll Fraud occurs when a hacker gains access to a VoIP network and allows unauthorized users to make repeated long distance calls, especially to international toll numbers. VoIP systems are particularly vulnerable to toll fraud because they form an integral part of an organization's IP network, unlike PBX systems that are closely monitored and managed by separate groups. VoIP toll fraud attacks can lead to serious financial damage in a remarkable short period of time.

Eavesdropping is when unauthorized parties monitor VoIP packets. By eavesdropping, they can listen in on conversations, and learn user names, passwords, and phone numbers, thereby gaining control over calling plans, voicemail, call forwarding, and billing information.

Unfortunately, eavesdropping is relatively simple. VoIP expert Peter Cox has released a proof-of-concept program demonstrating the vulnerability of VoIP-based calls to eavesdropping. The software, called SIPtap, can monitor multiple VoIP calls and record them as .wav files. A hacker would be able to infect a single PC on a network with a Trojan incorporating the program. This hack would also work at the ISP level.

An Ounce of Prevention

Because voice is essential to every company or organization, these threats – especially DoS and SPIT – represent the key threats to VoIP because they can literally bring voice services down. Toll fraud is important because of the economic implications of others using an organization’s VoIP system to make costly long distance calls. And eavesdropping carries the obvious risk of making private and confidential information accessible.

Fortunately, the steps required to secure VoIP are well understood. These are shown in the conceptual drawing and include:

- Intrusion protection, firewall
- Network segmentation into Virtual Local Area Networks (VLANs) and into separate VLANs for voice and data if possible
- Traffic analysis

Traffic analysis (that is, watching network traffic for anomalies) enables administrators to spot problems as soon as they arise. With data, delays are annoying but not necessarily disastrous. But voice is real-time, so it is essential to address issues as rapidly as possible, before voice communication is brought to its knees.

