Gartner

Research

Publication Date: 28 June 2005 **ID Number: G00127848**

IP Telephony Security Demystified

Lawrence Orans, Bjarne Munch, John Pescatore

Organizations with secure data networks shouldn't delay introducing IP phone systems because of security concerns. We show that, with a few key exceptions, securing these systems is very like securing data-only networks.

WHAT YOU NEED TO KNOW

The same security processes that protect data networks from worms and denial-of-service attacks will protect IP telephony applications. For networks that have an acceptable level of business security, the value of IP telephony will outweigh the risks. Organizations that cannot yet protect their data networks should not deploy IP telephony until they can.

ANALYSIS

Many organizations cite concerns about security as a key reason for delaying Internet Protocol (IP) telephony implementations. These concerns are understandable given that, in most organizations, the telephony application is the most mission-critical, the most widely deployed, and, historically, the most reliable of all applications. Organizations that have not yet deployed critical security processes to protect their data networks against worms and denial-of-service (DoS) attacks are right to proceed cautiously (see "Agile Processes Improve Enterprise Corporate Security Programs"). However, making enterprise networks secure enough for business-quality IP telephony is not rocket science — it is well within the capabilities of most businesses.

Many of the recommendations for making IP telephony secure are already proven best practices in data-only networks. This is because the expected attacks in the IP telephony world are similar to those that we are familiar with in the data world — a perspective which is driven by the fact that, with IP telephony, voice is another application on the data network. In the traditional data network, attacks are targeted at servers, endpoints (PCs), or the network itself. As converged networks become more commonplace, attacks will be targeted at the IP-PBX server, the endpoints (IP telephony handsets or PC-based softphones), or the network itself.

Two key issues that dictate extra focus in a converged environment are:

- **Real-time nature of voice traffic.** For example, a DoS attack could increase network latency to the point where voice traffic becomes unusable or completely unintelligible.
- **Emerging signaling protocols.** Most organizations that adopt IP telephony will introduce protocols that are new to their networks, like Session Initiated Protocol (SIP) and proprietary signaling protocols from IP-PBX vendors. By manipulating signaling protocols, hackers can steal services, disrupt sessions or launch other malicious attacks.

Organizations can protect themselves from these and other threats by implementing the following best practices recommendations.

Protect the IP-PBX Server

The same best practices and protective measures that apply to other mission-critical servers should also apply to the IP-PBX server.

- **Firewalls.** The behavior of voice over IP (VoIP) signaling protocols dictate the need for firewalls that are "IP telephony-aware." For example, SIP and H.323 use ports that are allocated dynamically during call set up. The firewall must scan VoIP messages and open ports dynamically only for calls approved by the call control server. At call disconnection, the firewall must close the session as well as any open ports. Since most IP-PBXs use proprietary protocols (most are based on versions of H.323) to speak with

their family of IP phones, organizations must use firewalls that provide explicit support for that proprietary protocol.

- **Network-based intrusion prevention.** To complement firewalls, use a network-based intrusion prevention system (IPS) to protect the IP-PBX against DoS and other attacks. The IPS solution should be able to block signaling protocol attacks (for example, recognize anomalous behavior in the signaling protocol).

- **Host-based IPS.** Protect the underlying operating system of the IP-PBX via host IPS (see "Host-Based Intrusion Prevention: Ready for Servers, Not PCs").

For IP Centrex solutions, where the equivalent of an IP-PBX is hosted by a carrier, the access link to the carrier should be protected via a firewall and network-based IPS that support IP telephony signalling protocols.

Protect the Network

Given the real-time nature of voice traffic, it is necessary to protect against network-based DoS attacks.

- **VLANs.** Separate voice traffic from data traffic using virtual LANs (VLANs). This is only possible when using IP telephony handsets. With Windows-based softphones, voice and data traffic is tagged with the same VLAN identifier, due to Window's inability to support 802.1Q VLAN tagging. Thus, traffic originating from softphones is more susceptible to DoS attacks than traffic originating from IP telephony handsets.

- **Quality of service.** Prioritize traffic in the voice VLAN to be sure that it cannot be "overrun" via bandwidth utilization spikes from malicious data traffic. Include the ability to lower the priority of unknown traffic or filter traffic that matches the profile of known attacks.

Protect the IP Phones

Most organizations will deploy a combination of IP telephony handsets and Windows-based softphones (primarily for mobile users and contact centers).

- **IP telephony handsets.** Endpoint security is presently not necessary for IP telephony handsets, nor does independent agent-based software exist for these devices. Most end users do not use their IP phones to surf the Internet or to download executables, so the risk to IP telephony handsets is negligible.

- **Softphones.** Use best practice laptop security configurations and endpoint security solutions. Currently, this is centrally managed personal firewalls and antivirus software. By the end of 2006, best practices will be the integration of desktop host-based intrusion prevention capabilities.

Emerging unified communications applications will drive more softphone deployments, but because of the underlying Windows-based PC platforms, softphones remain inherently more vulnerable to mass attacks. Unless there is a strong business case for softphones, always deploy IP telephony handsets as a first priority.

Selectively Deploy Encryption

The best protective measure against IP telephony eavesdropping is to encrypt voice traffic. However, eavesdropping is unlikely in most environments. In fact, it is no more difficult to eavesdrop on voice packets than it is data packets. Eavesdropping in a LAN-based IP telephony environment is done using an intermediate device that is able to monitor packets between two

endpoints. It is a Layer 2-based attack (a classic "man in the middle" attack that modifies address resolution protocol tables) which requires the eavesdropper to have direct physical access to the LAN segment containing the device that they wish to monitor. So, an employee or contractor could eavesdrop on other IP telephones within their physical proximity, but such a physical connection to the network would allow them to launch much more dangerous attacks than collecting gigabits of voice data. As a general rule, Gartner advises that if you already encrypt data traffic, then encrypt voice traffic. If you are not encrypting data traffic, then don't encrypt the voice traffic. Organizations that use encryption should test its performance to ensure that the overhead associated with the encryption and decryption process (for example, latency and jitter) does not mean that the voice quality deteriorates.

Key Issues

How will the enterprise communications equipment market evolve in the next five years?

REGIONAL HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters
Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters
Level 7, 40 Miller Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Latin America Headquarters
Av. das Nações Unidas 12.551
9 andar—WTC
04578-903 São Paulo SP
BRAZIL
+55 11 3443 1509

Gartner