Is VoIP Secure?

You Make the Call

Is your network equal to the task? Are you willing to risk exposing data *and* voice on the Internet?

by STEVEN TAYLOR

Voice over IP (VoIP) is no longer tomorrow's technology. High-speed networks that support quality-of-service (QoS) technology have come a long way in mitigating performance and availability issues.

But what about security? If your network is robust enough, securing VoIP is manageable. But if you're contemplating Internet telephony, you're entering dangerous territory.

"That's really the wild, wild West," says Doug Haluza, director of engineering and

illustration by GEOFF McCORMACK

new technology at Lexent, an enterprise telecommunications solutions provider. "There's no way to control how packets are routed, how many carriers they go across. Basically, doing Internet telephony is a risky proposition." *(see "This Line's Secure," p. 80)*

Internally, voice running over your data lines is essentially no more or less secure than any other application in your IP infrastructure. And, in some respects, it's at least as secure as traditional telephony. VoIP is here, now, and growing. When we examine VoIP in the context of well-known issues of IP data and traditional telephone security, implementation remains a security challenge—but not necessarily a nightmare.

VoIP on the Rise

Most major corporations are starting to look at their next generation of telephony technology. Almost without exception, they're looking at VoIP.

The process of transporting voice conversations using the IP protocol isn't a radical new idea. In fact, the basic technology for using advanced packet services like frame relay, ATM and IP for transporting voice between corporate sites is several years old. Historically, the most common application for this technology has been for toll bypass—using less-expensive data services rather than by-the-minute voice services. This has been especially cost effective for international calls.

That's no longer the case. Extremely low toll rates have removed a lot of the incentive to bypass toll charges. Long distance voice in the United States is already essentially free. Cutting the price of phone calls in half saves far less when you're paying 3 cents per minute rather than the 15 cents per minute of a few years ago.

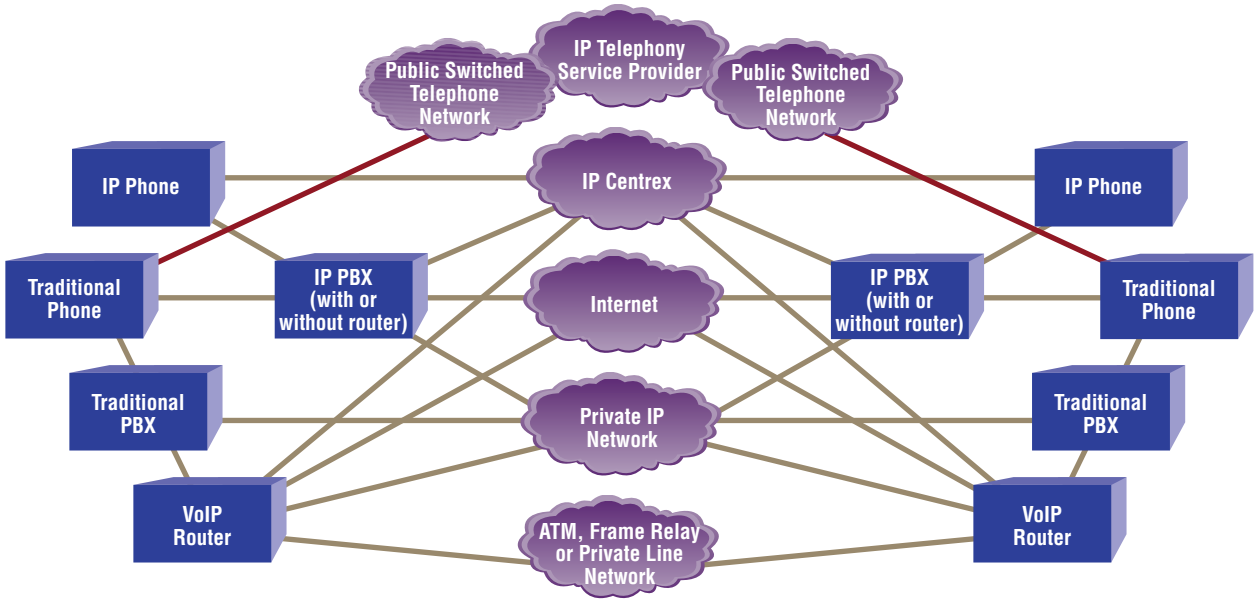
Nevertheless, VoIP is taking off as the focus moves from simple toll savings to reengineering the entire voice infrastructure. As organizations move through the normal cycle of replacing their PBXes, VoIP can be viewed as a logical choice for converged messaging, call centers and interactive multimedia collaboration.

So, there's a good chance VoIP is coming to your organization, probably sooner rather than later. The good news is that VoIP in a well-designed corporate IT environment is at least as secure as conventional telephony. Then again, conventional telephony isn't exactly secure.

Voice Over Ethernet

You may be concerned that VoIP LAN or WAN traffic will be carried over an Ethernet backbone and broadcast over the

VoIP Network Architecture



As shown by this basic reference architecture, a typical VoIP implementation consists of many functionally independent elements, each of which presents its own security risks. The good news, though, is that few of these risks are unique to VoIP.

entire local network, making it easy for anybody to eavesdrop. Not so.

It's true that 15 years ago almost all Ethernet traffic was broadcast over a single coaxial cable and was available to all users on the network. Today, however, virtually all Ethernet traffic is switched. Even though all network points may be reached—just as you can call anyone connected to the traditional telephony network—the individual packets exchanged between two network points are available only to those two points.

So, the architecture is the same as that of traditional telephony. The VoIP packets that comprise a conversation between two network points are available to the workstations or IP phones at those endpoints, on the physical cabling to the nearest Ethernet switch and in the switching infrastructure.

Can this infrastructure be compromised? Sure, if your switches aren't protected from unauthorized access. Someone with the right equipment can tap in—but the risk, as we'll see later, is significantly less than with traditional telephony.

Voice Over the Internet

OK, you're feeling pretty good about VoIP running over your private network; corporate intranets are a closed system, and any breaches of security must come from within. But what about letting VoIP out into the world? How does the security of Internet VoIP compare with your current phone system?

Network connections to the outside world—and to business partners, suppliers, etc.—open your servers to access from unfriendly and unknown people. Unlike traditional telephone numbers, there's very little centralized control over the use of IP addresses. This anonymity creates a fertile environment for address spoofing, which enables distributed denial-of-service (DDoS) attacks and other network compromises that could bring down your call-processing capabilities. By definition, VoIP is vulnerable to all of the intrinsic security problems in IP.

DDoS is a virtual "busy signal" on an IP phone system. VoIP's dependence on continuous, reliable packet flow makes availability an issue in the face of attacks. The high levels of packet loss inflicted by January's SQL Slammer worm, for example, raised concerns about VoIP reliability.

When you conduct business on the Internet, you're turning control of your data and/or voice transmission to other people's networks—and some of those networks are more secure than others.

Traditional data networks depend on a few well-known—and trusted—entities. There's a local service provider at each end of the connection and an interexchange carrier connecting them. So, for instance, a connection between Atlanta and Boston might involve BellSouth, Verizon and AT&T. You know these

Case Study

THIS LINE IS SECURE

If you want VoIP to work, the pros say do your homework and roll up your sleeves. by ANNE SAITA

In many ways, Doug Haluza, director of engineering and new technology at Lexent, is just like any other IT professional who's recently deployed VoIP throughout his company. Since he was implementing a new WAN and changing service providers, he did his research and made sure Lexent's network could support VoIP.

But rather than rely on perimeter security, as many VoIP adopters apparently do, Lexent, which knows a thing or two about IP telephony as a solution provider to both enterprises and telecommunications companies, has taken additional steps to prevent voice transmissions over its LAN and WAN from being intercepted.

VoIP is an option that more organizations are considering, particularly those that make a lot of international calls.

Haluza limits the company's exposure to the Internet, sending outbound voice through a single carrier's IP backbone. And all IP telephone devices have private addresses, so they're not globally routable. "You can't make a call [from the outside] using our gateway, because you can't get to it," Haluza explains.

In addition, packetized voice is encrypted with a Cisco IPSec-compliant VPN as it moves from one location to another. "IPSec obviously is not for the faint of heart," he warns. "It's complicated, and you have to be able to stick with it until you get it right."

And older VPN software wasn't designed to handle the traffic that VoIP generates. Pushing voice through a VPN can, in some cases, degrade quality of service to the point of being unacceptable, experts say.

Lexent avoided this problem by using new Cisco routers with hardware encryption. "Once you have IPSec running, it's actually harder not to encrypt the voice," Haluza said, "As long as the encryption is done in hardware, there's no performance penalty for encrypting voice."

Those that have dabbled in both voice and data should have fewer problems moving their telephony away from traditional environments, Haluza says. "If you're used to working with both technologies, then voice really does become just another application. At the end of the day, that's all it is—a real-time application."

Since August, Joel Pogar, national practice manager for information security at **Siemens** (**www.siemensenterprise.com**), has evaluated networks for numerous clients wanting to deploy VoIP. "None of them passed our initial assessment," he says.

That's not surprising. "Networks have to be designed

"If you're used to working with both [voice and data] technologies, then voice really does become just another application."

–**DOUG HALUZA**, director of engineering and new technology at Lexent

to support VoIP. We're looking at a lot of networks designed three to five years ago, when VoIP was not a mainstream technology."

The trick with VoIP is to reconfigure a network to accommodate the technology without compromising security, Pogar says. For Siemens customers, Pogar goes through several pages of potential holes or problems to be addressed. The older the network, the more time and money the deployment is likely to cost.

"If you're deploying a VoIP system, continually test and monitor it…to stay one step ahead of the potential bad guys who are out there."

–JOEL POGAR, national practice manager for information security at Siemens

At Lexent, IPSec-compliant VPNs with VoIP already has paid off in savings, from $48,000 monthly with a fully managed service provider to less than $20,000 in monthly expenses doing the work in-house. Future consolidation is expected to bring the monthly tab closer to $10,000.

While address spoofing and packet sniffing are frequently cited as chief security concerns, Pogar believes the biggest vulnerabilities lie within call-handling software, which usually resides on Linux or Windows servers, and other VoIP necessities, such as call-routing switches, which are increasingly subject to denial-of-service attacks.

"If you're deploying a VoIP system, continually test and monitor it," Pogar says. "As standards evolve and new security weaknesses are discovered, you'll want to be sure to stay one step ahead of the potential bad guys who are out there." ◗

providers and are confident they're transmitting your information securely.

Not so on the Internet. You can choose your local ISP, but your traffic between points on the Internet involve several ISPs, and these can change. For example, a simple Traceroute command usually shows at least three of four different carriers involved in a given data conversation.

So, the safest route is limiting VoIP to internal use. Simply add VoIP as an additional application on a secure corporate intranet.

If you're planning to deploy VoIP, you'll need to take some steps to make the data network more secure, especially if you haven't performed an overall security audit recently.

But you might be shortchanging yourself. When it comes to outside communications with VoIP, weigh the potential cost savings and efficiencies gained by converging technologies against the risk. If you're already transmitting and receiving sensitive data over the Internet, you've gone to considerable lengths to protect that data, which is almost surely more sensitive than your voice traffic and no less vulnerable to attack. These safeguards can be leveraged to help secure VoIP over the Internet.

But What About Packet Sniffing?

While it's technically possible to sniff voice packets, it's a lot more difficult than tapping into a traditional phone transmission. Let's consider what it would take to tap into VoIP.

The first step in sniffing a conversation is to gain physical access to the packets. This means having access to the switches and/or the corporate backbone network. But those same switches carry critical corporate data, which is far more sensitive than your conversations. If you've secured data against sniffing, you've secured voice. If you haven't protected your data, voice packet sniffing isn't your most serious security problem.

Of course, the transmission medium makes a difference. Wireless Ethernet is far more susceptible to sniffing than copper wire. The most secure is fiber-optic cabling, which doesn't emit radio frequencies as does copper wiring.

But let's say an intruder gains physical access, despite your best efforts. If it's a traditional phone line, he's practically listening already. But if you're using VoIP, he really has his work cut out for him.

First, consider what it takes to tap a traditional phone line. If the conversation is still in analog format, the intruder simply taps onto the line using a "butt set"—which was formerly reserved for telephone repairmen, but now available at hardware stores—and starts listening. Traditional telephony uses time-division multiplexing for trunk groups—as opposed to packet multiplexing—so picking out a single conversation from a digitally multiplexed bundle of conversations and decoding the 64 Kbps pulse code

modulation (PCM) is relatively easy.

Compare that with pulling a conversation out of an IP transmission. Voice packets are buried deep inside a sophisticated protocol stack. The intruder has to know what the physical format of the information is; decode the Ethernet packets to find a single flow between two points; decode the IP layer; decode the transport-layer (layer 4) protocol—probably UDP—and then, finally, decode the voice packets, which could be encoded in a wide range of formats. And he has to do it in real time.

Typically, tools for this type of analysis are applied to an archived stream as opposed to real time. If this isn't hard enough, the actual payload of the IP stream—possibly including a secondary level of IP addressing—could be encrypted via IPSec. (If you plan to use IPSec to protect your VoIP traffic, factor in its possible impact on performance. QoS may be a greater challenge than security in deploying VoIP.)

So, Is VoIP Secure?

It's a lot easier to listen to a conversation over a cubicle wall than it is to tap a VoIP call. Before you get excited about encoding all your IP telephony with IPSec, take some simple precautions like telling the sales force not to discuss key negotiations on their cellphones in a crowded airport. And lock the doors to the equipment rooms!

If you're planning to deploy VoIP, you'll need to take some steps to make the data network more secure, especially if you haven't performed an overall security audit recently. But the bottom line remains that for most corporations, we're already crossing the threshold where there's a higher level of security needed for data applications than for phone conversations. The odds are that you actually could improve your level of telephony security as compared with traditional telephony simply by piggybacking your voice onto the more secure data network.

There's even a question as to how secure VoIP should be. For instance, there are legitimate concerns from the law enforcement community about whether advanced voice networks are "too secure" for court-sanctioned wiretapping.

VoIP is probably as secure as traditional telephony and a lot more secure in most cases than your cellphone. Balance sufficient security against risks and benefits. If the effort of required to obtain the information in a VoIP call is greater than the intrinsic value of the information, VoIP could be considered "secure enough." ◗

VoIP Protocols

Two protocols are gaining popularity in the VoIP arena, with both able to support encryption but under different circumstances.

- **Session Initiation Protocol** (SIP), sponsored by Cisco Systems and Microsoft, is designed to set up a session, or "call," between two endpoints. SIP supports VoIP encryption via SSL, PGP or S/MIME. Its biggest deficiency may be the lack of authentication mechanisms, which could lead to identity theft. Also, it has no means of handling delivery failure of intermediary network devices or load balancing, which could be problematic for larger enterprises with a lot of traffic. However, inter-operability among SIP systems is fairly widespread.

- **H.323**, designed to support multimedia over IP for Web-based video conferencing, addresses some of SIP's call-handling issues, such as its ability to reroute calls around failed gateways so the call isn't disrupted. But such service comes at a cost. In addition to more overhead, voice data may not move as quickly, which could influence quality of service. It supports encryption via H.235 and can use SSL under certain conditions. ◗

–ANNE SAITA

STEVEN TAYLOR (**taylor@webtorials.com**) is president of Distributed Networking Associates, and editor and publisher of Webtorials.com, a Web site for technology-based tutorials.