

# HEIGHTENED

# Level of Alert



By Leonard Klie

**As more risks become associated with VoIP, companies that did not take security into account before will need to start**

A recent CIO Index report found that 23 percent of companies currently use some Voice over Internet Protocol (VoIP) services. Those numbers are expected to rise dramatically as more corporate entities discover the cost savings and the increased flexibility, efficiency, and mobility that the technology provides. But, as VoIP call volumes increase, so too do security threats.

“Enterprise VoIP deployments will continue to ramp in 2007, and the frequency and severity of VoIP-specific attacks will increase as well,” warns Mark Collier, chief technology officer at SecureLogix Corp., an enterprise telephony management and security company.

Collier and other network security experts warn that corporate VoIP networks are subject to the same kinds of viruses, spyware, denial-of-service attacks, spam, and phishing as traditional data networks. “While these attacks may not directly target VoIP systems, they will disrupt operations because the underlying platforms are vulnerable to the attack,” Collier explains.

As VoIP technology grows and becomes more commonplace, “we will also start to see more VoIP-specific attacks, particularly aimed at the enterprise,” he continues. “There is more scrutiny of VoIP systems and attackers will find more issues that are unique to VoIP and the systems that enable it. Attackers will also be developing more tools to exploit these issues. Even now, there are plenty of tools out there, but you can expect to see more tools and extensions to the tools currently available.”

Worse than that, the attacks are likely to be aimed at a specific organization or network, according to many security experts. Dan Blum, a senior vice president and



## “Nearly three quarters of the corporate deployments we have audited have been exploitable from the inside.”

research director at IT research firm Burton Group, for example, states that the IT security threats today are “very sinister,” in which the majority of attacks are not random but rather, are targeted and intentional.

A single attack to a company’s VoIP network could knock out phone service for hours, or even days. Calls can be monitored, intercepted, and recorded, putting company trade secrets and confidential client information at risk. Incoming calls to a corporate call center can be rerouted to an unauthorized external location. Call centers and networks can be flooded, causing them to crash. A hacker can access the network and use it

to make unauthorized calls, register rogue IP phones, or spoof the addresses of authorized personnel within the network to send VoIP spam or call on customers to get them to divulge personal information.

This last threat, dubbed vishing (short for VoIP phishing), is a concern that is growing in leaps and bounds, especially as more financial organizations replace traditional telephone services with VoIP. In fact, the Federal Deposit Insurance Corp. warned early last year that, “if improperly implemented, VoIP can pose significant risks to financial institutions.”

“Credit card companies are especially vulnerable. Phishing is always a problem,”

says John Burns, chief operating officer of ERF Wireless, a company that specializes in creating secure wireless broadband networks. Most of his clients are in the financial arena, where information security is an especially urgent concern.

VoIP spam is another growing problem, and a lot harder to detect than email spam, primarily because most VoIP telephone systems lack filters. Email filters can scan documents and attachments for certain words or phrases and block them before they are ever opened, but it’s impossible to determine the contents of a phone call before the conversation starts.

Any of these attacks can cost a company dearly. Loss of credibility for the company, corporate espionage and blackmail are just a few of the risks a company faces when running an unsecured VoIP setup.

And, none of these kinds of attacks are hard to pull off, warns Sheran Gunasekera, an engineer with Belgian Internet security firm Scanit. “You do not need to be very highly skilled. You just need to have a basic understanding of how VoIP

works and a little bit of network knowledge,” he says.

Typically, anyone who knows the IP address of a VoIP phone can tap into calls made with it. Specific underground programs, called sniffers, are available as well to intercept, analyze, and record VoIP traffic. Or legitimate programs for internal security and quality assurance can also be used for malevolent purposes.

Think it couldn’t happen to you? Don’t be so sure, according to the experts.

Scanit estimates that as many as 70 percent of all VoIP calls could be subject to attack by hackers. “Nearly three quarters of the corporate deployments we have audited have been exploitable from the inside,” Gunasekera says.

Though most of the firms he’s audited have been in the Middle East, the security threats are not unique to that region. “The technology remains the same throughout the world,” he warns. “The only variable would be the skill levels of the administrators at each location and the attention paid to deploying a secure VoIP setup.”

To date, few companies that have deployed VoIP technology have done so with the proper level of security in place beforehand. Many network administrators and IT professionals have mistakenly assumed that VoIP is just another plug-and-play application to be added to an existing data network, Gunasekera says,

ERF Wireless’ Burns also notes that especially in the banking and financial services sectors, demand is very high not only for VoIP and high-speed Internet connections, but also for digital image sharing, video surveillance, video conferencing, and more. In many cases, the banks and other institutions will have many branches scattered over hundreds of miles, and need to have them all connected. “The problem in the past has been how to properly secure a high-speed wireless network for these advanced digital products in regulated industries,” he says.

“Primarily, the reason for [security shortfalls] has been the fact that the system integrator or implementer had not paid much attention to the security of the entire setup,” Gunasekera says. “The most common reason in large companies is because no one under-

## VoIP Security Still a Concern for SMBs

Concerns about the security of Voice over Internet Protocol (VoIP) telephony solutions continue to persist among small and medium-sized businesses (SMBs), research commissioned by the Computing Technology Industry Association (CompTIA) reveals.

A survey of 350 businesses with fewer than 500 employees each found that just half of the businesses trust the security offered today by IP telephony product and solution vendors. That’s a slight improvement from a year ago, when 48 percent of SMBs surveyed said they trusted IP telephony security.

Conversely, other communications methods scored much higher in terms of security confidence levels. Eighty-two percent said they trusted traditional telephone services; 72 percent trust Ethernet data networks; and 60 percent trust wireless local area networks, according to the CompTIA survey.

“People are much more sensitized to disruptions in voice communications than they are with data communications,” says John Venator, president and CEO of CompTIA. “If the delivery of an email is delayed by 30 seconds, neither the message sender nor the receiver is likely to notice. But a 30-second gap in the middle of a phone call is another story entirely.

“Even a brief interruption in voice service can have disastrous consequences for an organization, in lost business, downtime, customer dissatisfaction, or negative publicity,” Venator adds. “That’s why it is incumbent on IP telephony vendors and solution providers to place security at the forefront of their offerings, and not leave it as an afterthought.” —L.K.



## Staying Securely

### Hotel VoIP installation has security covered

When the Four Diamond Seaport Hotel in Boston began installing in-room Web access portals, complete with Voice over Internet Protocol (VoIP) capabilities, security was a primary concern.

“It was critical. We would not have started it if we couldn’t do it securely,” says John Burke, vice president of technology for the Seaport Hotel and the adjoining Seaport World Trade Center, a conference and convention facility.

The in-room offering, provided by BlueNote Networks and AGN Networks, is part of the hotel’s Seaportal system. Seaportal provides guests with free, direct-dialed local and

domestic long distance VoIP calls, but also allows them to access the Web, send and receive email, view hotel and local attraction information, watch movies, listen to music, check travel information, and more. Users connect to the system through a touch-screen computer, complete with flat-panel monitor, wireless mouse, and keyboard.

For the hotel’s many business travelers, Seaportal is a great benefit because it allows them to leave their laptops at home. But, guests would not use the service if their privacy could not be ensured, Burke notes.

To that end, the hotel outfitted the entire system with triple-layer, 128-bit encryption and placed it behind multiple firewalls that protect not only the voice network but also the integrated back-office applications, such as guest services and property management. “When a call leaves Seaportal over the IP network, it is secure,” Burke says.

“We believe in protecting all of our guests’ information, and we wanted to give them at least the same level of service and security as they would get in a traditional PBX network,” he adds.

The Seaport Hotel was expecting to have Seaportal units installed in 100 of its 426 guest rooms by mid-February. Deployment throughout the entire hotel is expected to be completed by the end of this year or early in 2008. —L.K.





matures,” Mehta maintains. But for now, the flaws require vendors to put out patches to correct them, and therefore, it is important for network administrators to check often for software updates and patches.

“It is really the responsibility of the security teams of the various organiza-

checking mechanism, and encrypt the actual voice data on the network,” Gunasekera says.

Of those, one of the most important in terms of data protection is the segregation of voice and data networks. “Segregation is a good idea. If VoIP is not separated from the rest of the data, some-

of a major power outage or electrical service disruption.

Such activities are, of course, limited by the capacity of the existing networks in place. Experts also warn that running separate networks, subnets, gateways, and servers can be an expensive proposition and may require additional space and IT to support them.

#### First Line of Defense

Whether sending transmissions over closed networks or the Internet, encryption is the first and most important line of defense. “With encryption, the actual data is scrambled so that if anyone gets into it, it comes back as gobbledy-gook,” says Burns of ERF Wireless, which offers a proprietary CryptoVue encryption system with biometric controls developed exclusively for customers who need high levels of security in their voice and data networks. Its primary customers are banks and other financial institutions.

“The best ways to prevent casual wiretapping are to ensure that voice communications are encrypted so that even if captured, they do not make sense when played back,” Scanit’s Gunasekera asserts as well.

The more layers of encryption, the more secure the network, and it’s better to have the transmission encrypted across the entire pathway between the caller’s phone and that of the person on the other end of the line. That means at both ends as well as all points in between.

Most VoIP service vendors provide built-in encryption, along with the ability to authenticate user information and block those without proper credentials from accessing the system. Skype, the VoIP calling service owned by eBay, is one service in particular that has been singled out by independent auditors and consultants for its high level of security. The service provider not only encrypts transmissions over its networks from end to end at the session layer, but also relies heavily on digital credential authentication to ensure that access to internal networks is limited only to valid subscribers. Each person on the call must verify his digital identity before a Skype session can begin. Together, the encryption and authentication “really reduce the opportunity for the high volume of

fraud,” says Kurt Sauer, Skype’s chief security officer.

Beyond those provided by the VoIP services providers directly, there are also add-on encryption products on the market. Many of these encryption engines also come with the ability to authenticate the caller and inspect the data stream during transmission for outside tampering.

“Encryption gives confidentiality to the calls and integrity validation so that you know the voices you’re hearing on the other end of the phone are from the requested callers,” Mehta advises.

It is also a good idea to position network servers behind a firewall. By their very nature, firewalls look at IP addresses, port numbers, and protocol types to determine a data packet’s legitimacy and block traffic deemed invasive, intrusive, or malicious from ever getting into the servers. Acceptable traffic is determined by a set of rules programmed into the firewall by network administrators. When properly designed and configured, no information will get through without first passing through the firewall.

Organizations that use VoIP today should also try to limit the use of softphones (a headset connected to a PC through an audio port) wherever possible. Many government agencies have rules against employees on a VoIP network using softphones because they are connected to a PC, which is subject to all sorts of malware, and because PCs are necessarily connected to the data network, they conflict with the need to separate voice and data networks.

#### Constant Monitoring

Also highly recommended is for network administrators to continually monitor traffic over the VoIP network. This means looking through traffic patterns and checking for abnormal data flow in terms of size, syntax, or content. Scrutinizing call logs can also bring to light irregularities such as high volumes of calls made at odd hours, calls to foreign countries in which the firm has no dealings, multiple failed log-in attempts (which could indicate that someone is trying to hack into the system), calls being made from locations and devices outside the network, and more. Adminis-

## NEC Develops VoIP Spam Blocker



While some have discounted its estimates as overstating the risk, NEC is warning businesses that telephony spam levels could soon soar, and has developed a software add-on that it says will stop up to 99 percent of spam phone calls.

Called VoIP Seal, the software uses a variety of techniques to

detect spam calls. When the system detects an incoming call, it can create a “fake” ring tone to trigger machine-generated messages and block them before the recipient’s phone ever rings. Once a VoIP spam call is logged, the system creates a blacklist of callers by caller ID or IP address and can automatically block those calls altogether or route them to voicemail.

The company tested the software add-on during simulated VoIP spam attacks using botnets—a network of computers or servers that have been compromised and programmed remotely to initiate spam calls or perform other malevolent tasks. It has not given a timeline for when the product would be commercially available, but was due to demonstrate it at several upcoming conferences and trade shows.

Several other companies are also developing techniques for blocking VoIP spam. Included among them are Checkpoint and Eyeball Networks. —L.K.

**“Primarily, the reason for [security shortfalls] has been the fact that the system integrator or implementer had not paid much attention to the security of the entire setup.”**

tions to keep updated with regard to current trends in security and the newest threats that affect their equipment. It needs to be a continuous cycle where the administrator checks vulnerabilities of his products and implements the patches released by the vendors of the products. This needs to be done continuously,” Gunasekera states.

If you are currently running a VoIP network and have not implemented the necessary security measures, it’s still not too late. “If you already have VoIP in place, most security technologies can be dropped in without much effort,” Mehta says, “but there are some advantages that you may lose if you put up a network before putting proper security in place.”

“I personally think that security should be considered during the planning stage of a VoIP installation—when it’s still an idea in someone’s head,” Gunasekera adds. “Yes, it is possible to retrofit after an installation, but you’re looking at costly changes in the way of downtime, loss of productivity, and network changes.”

While there is no red button that will make all VoIP vulnerabilities go away entirely, there is plenty that a company can do to protect the integrity and security of its VoIP network. “A few basic things that I can recommend are to ensure the voice network is adequately segregated from the data network, ensure that signaling traffic contains an integrity

one can plug in a laptop and have access to both phone and corporate data networks,” Mehta adds.

Running separate servers and subnets for voice and data streams will keep traffic on one hidden from those that access the other, thereby minimizing the risk to one if the other is compromised. It will also speed up transmissions over both networks since voice traffic does not have to compete with data for limited bandwidth and vice versa.

Experts also recommend routing internal VoIP transmissions through dedicated, closed-loop local area networks or virtual private networks rather than across the Internet. Because they provide limited access to only those persons and devices that are authorized for the network, they are a lot harder to access from the outside. They are also faster and more reliable than Internet connections because data and voice streams do not have as far to travel.

Another suggestion is to increase the reliability of VoIP networks by creating redundancies. That can mean multiple Internet service providers or connection means, multiple VoIP providers, multiple VoIP gateways within a network, clustered VoIP servers so that one takes over if another goes down, and even redundant links to call centers connected to a VoIP network. Secondary electrical power sources can also provide the energy needed to run servers and hardware in the event

trators should prepare a list of permitted call destinations to prevent unauthorized calls or people using the network for VoIP spam or vishing.

“In order to correctly monitor and secure VoIP applications, customers need to be able to unify their view of the network, the applications on that network, and the security products that defend those applications,” says Tom Turner, vice president of marketing for Q1 Labs, a network security management company that launched the QRadar program to monitor VoIP communications, analyze the ability of a VoIP network to handle specific threats, and prepare daily, weekly, or monthly reports on all activity over a network.

Implementation of security measures like these, though, do not come without a cost. They are not only expensive, but their use often results in a marked deterioration of service quality and speed

because they create extra layers through which the data streams must pass.

The National Institute of Standards and Technology at the U.S. Department of Commerce’s Technology Administration has concluded that “VoIP can be done securely, but the path is not smooth. It will likely be several years before standards issues are settled and VoIP systems become mainstream. Until then, organizations must proceed cautiously and not assume that VoIP components are just peripherals for the local network. Above all, it is important to keep in mind the unique requirements for VoIP, acquiring the right hardware and software to meet the challenges of VoIP security.”

“There are ways to make VoIP more secure, but they are an inconvenience, so a lot of organizations do not use them,” Mehta concludes. “A lot more are pushing towards security now, though, because of the prevalence of VoIP attacks.” ☐