IDG.net

NetworkWorld Reprint

The leader in network knowledge ■ www.nwfusion.com May 24, 2004 ■ Volume 21, Number 21

Breaking through VoIP security

In the first-ever public test of VoIP security, Cisco and Avaya set up secure VoIP networks in Network World Lab Alliance partner Miercom's facility in New Jersey. Then we set loose our four-person attack team. The results: Cisco's network was impenetrable; it survived dozens of attacks during a three-day bombardment. Of course, the setup also required six Cisco security gurus. Avaya's no-frills, out-of-the-box setup had some holes, but its more hardened security configuration performed much better.

CLEAR CHOICE TEST

VoIP security wares

Breaking through IP telephony

In tests, Avaya and Cisco attempt to strut VoIP security stuff.

■ BY EDWIN MIER, RANDALL BIRDSALL AND RODNEY THAYER, NETWORK WORLD LAB ALLIANCE

Can you hacker-proof your IP telephony network? The short answer — as demonstrated in the first-ever public test on this topic — is: Yes, pretty much. But it strongly depends on whose IP PBX you use and more importantly, whether you're willing to spend the dollars and the time it takes in terms of network security planning, network and personnel resources, and extra security gear.

In our tests, we developed a plan for realistically assessing how secure vendors' IP telephony packages are — or aren't — against a determined, malicious attacker. While we invited the top five vendors by VoIP market share to participate, only Cisco and Avaya stepped up to the challenge.

Cisco's "maximum-security" VoIP configuration — a midsize CallManager-based system, with call control, voice mail, gateway; a Catalyst 4500- and 6500-based Layer 2/Layer 3 infrastructure; a copious supply of intrusion-detection system (IDS) and PIX firewall security add-ons; plus a half-dozen Cisco security gurus supporting the test — earned our most Secure rating (see rating criteria, page 2). Our attack team couldn't disrupt, or even disturb, Cisco's phone operations after three days of trying.

Avaya submitted two configurations: A no-frills, out-of-the-box Avaya IP telephony deployment with no extra-priced security

options; and a maximum-security alternative — featuring the same VoIP gear, but with an added firewall and Layer 2/Layer 3 infrastructure switches from Extreme Networks. Security weaknesses earned the basic Avaya configuration a so-so Vulnerable rating, while the hardened package fared better with an overall Resistant rating.

The ground rules (see page 3) imposed some limitations on the four-member assault team. For example, only hacker tools and attacks that were available on the Internet could be used. Attacks had to be launched via an end-user data port or IP phone connection, as if the hacker had access to a standard office cube; attackers could not disassemble or dissect the vendor's IP phone — and so on.

The objective was to disrupt phone communications. Via the data and IP phone connections, the attack team used scanning tools and other techniques to see and learn what they could of the topology. The attack team was told nothing of the vendor's configuration beforehand. After discerning and identifying "targets," the hackers then systematically launched dozens of attacks, at times in combinations concurrently.

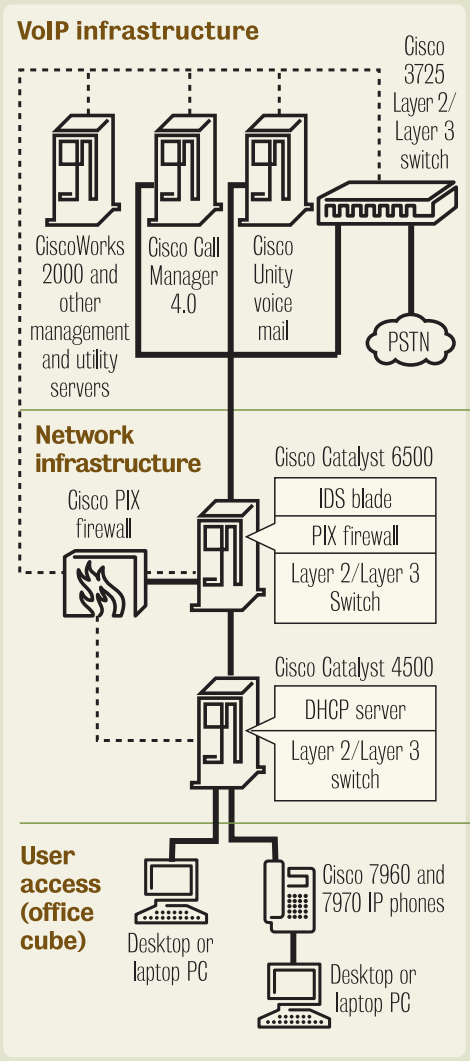
Given the limits set by our ground rules and the duration of the tests, it is important to note that the attacks launched against these products are not as severe as those that could be encountered in an actual deployment. We consulted with a half-dozen security experts regarding these attacks, and they concluded that the attacks were of moderate intensity.

We will not disclose in this story complete details of vendors' specific vulnerabilities uncovered and exploited, so as not to put customers using these products at risk. These exploits are therefore discussed in general terms.

VoIP security rating scale

Overall rating	Maximum impact that assault team could achieve
Secure	No perceptible disruption to voice service.
Resistant	Only minor and/or temporary disturbance(s).
Vulnerable	Phone service affecting many phone users could be disrupted for a protracted period, via a sophisticated or coordinated attack.
Open	Phone service affecting most phone users could be significantly disrupted, indefinitely, via a fairly straightforward assault.
Unsecure	Phone system or service affecting all users could be readily and indefinitely disabled.

Cisco maximum-security VoIP topology



Key security components

- Cisco Security Agent integrated on all servers.
- Firewall-protected, out-of-band management access to all servers and infrastructure boxes.
- Aggressive monitoring of security related events.
- Built-in denial-of-service protection in Catalyst IOS, including rate-limiting.
- Dynamic Address Resolution Protocol Inspection; other attack suppression in Catalyst IOS.
- Multiple firewalls at strategic locations.
- Separate voice and data VLANs throughout.
- Certificate-authenticated, encrypted VoIP call control and signaling.
- Media (VoIP Real-time Transfer Protocol stream) encryption on 7970 IP phone.
- Local IP phone administrative.

Like a rock

Cisco proved it could build a VoIP network that a sophisticated hacker assault team could not break or even noticeably disturb. The elaborate IP-telephony package — with underlying Layer 2 and Layer 3 infrastructure and assorted security add-ons (see "Cisco maximum-security topology," above) — is the most secure that Cisco's collective network security expertise could muster, and employs every defensive weapon in the Cisco arsenal.

The Cisco topology tested certainly represents more security options and stricter security settings than most users currently employ, but all are available today for a price. The optional components included: two standalone PIX firewalls (about $8,000 each); another firewall on a blade in the backbone Catalyst 6500 (about $35,000); an IDS blade also in the 6500 (about $30,000); an entirely separate, out-of-band management subnet and various security-management applications. The price for the firewall and IDS pieces came to slightly more than $80,000. Cisco says, though, that it threw in systems that it could readily get its hands on, and that the same job could be done with less-expensive firewall and IDS models from Cisco.

The firewalls brought some very useful, high-level security features to the table. One is the notion of trusted vs. untrusted sides — and the untrusted interfaces were always pointed toward our hackers. Another is a stateful understanding of protocols, so that only specific VoIP protocols required for VoIP were allowed, with

Ground rules for VoIP security testing

Before the test, these ground rules were adopted as a means of setting a level playing field for consistent testing practices across all vendors tested.

1. The vendor has complete control over the IP telephony environment and underlying network infrastructure — which products to include and how everything would be configured.

2. A midsize, local-only VoIP environment (campus or building) would be simulated. No VoIP traffic would be carried via WAN between remote, distributed locations.

3. After setup, IP telephony and Layer 2/Layer 3 data networking could not be functionally limited because of security settings, including normal IP phone calling out to/from the PSTN.

4. After setup, vendors could not actively manipulate or reconfigure their network. They could, however, continue to passively monitor security alert/alarm logs.

5. Assaults would all be attempted via these specific attack points:

a. Via an "office-cube" data-LAN port, which the assailant can legitimately access (for example a valid MAC address).

b. Via an "office-cube" IP phone, which the assailant is authorized to use, including the "data switch port" on the back of the phone, for a desktop or laptop. These scenarios represent typical "insider-attack" scenarios.

6. All assaults would employ or be based on tools and attacks that are publicly available via the Internet. No new programming or other unique or custom attacks could be applied.

7. Assailants could not procure or disassemble and dissect a vendor IP hard phone.

requests and responses passing only in the appropriate directions. Other firewall features that came into play during this test included:

- Stateful inspection of VoIP call control, and the ability to network address translation and tunnel call control through the firewall.
- TCP intercept, which makes sure TCP connections are completed. This can prevent certain denial-of-service (DoS) assaults on the CallManager.
- Secure Skinny Call-Control Protocol (Secure SCCP) support. This is the newer, more secure form of Cisco's proprietary SCCP that the company used in this VoIP network. Secure SCCP uses a TCP connection rather than User Datagram Protocol (UDP) and encrypts call control information.

Enter CallManager

Version 4.0 of CallManager, which handles call control and is the heart of Cisco's IP telephony package, includes some new security-related features. Key among them is the company's first VoIP encryption implementation. At this time voice-stream (Real-time Transfer Protocol [RTP]) encryption is supported only on Cisco's newer 7970 IP phone sets. The latest CallManager also has been additionally hardened, along with the underlying Windows 2000 operating system, according to Cisco. For our tests, this meant that open ports were closed and unnecessary services disabled.

An impressive array of network self-defense features is included in the Catalyst IOS versions tested. Specifically, we had IOS 12.2(17b)sxa on a core Catalyst 6500, and IOS 12.1(20)ew on an access Catalyst 4500. These capabilities did more to thwart our assaults than any other component in the Cisco topology because they were the first line of defense. They include:

- Traffic policing and committed access rate, which were very successful in fending off our DoS assaults.
- Layer 2 port security, which restricts the number of media access control (MAC) addresses on a port.
- Layer 2 Dynamic Host Configuration Protocol snooping, which prevents dynamic host configuration protocol exhaustion attacks.
- Dynamic Address Resolution Protocol inspection, which stops ARP poisoning and ARP spoofing attacks. This, too, frustrated a number of our attack team's more insidious assaults.
- IP Source Guard, which prevents impersonation attacks.
- Virtual LAN (VLAN) access control lists, which restrict the traffic that can reach IP phones.

Cisco Security Agent (CSA) is a host-based intrusion-prevention system (IPS), and is now an integral security component in CallManager IP telephony servers. It was also on Cisco's Unity voice mail server and all other Win 2000 servers (seven CSA agents in all) deployed throughout Cisco's network topology. The CSA agent runs automatically and unattended, and provides some powerful safeguards at the server, including:

- Buffer overflow protection, which protects the server's protocol stack from attacks involving malformed data packets.
- Network worm and Trojan prevention (not tested).
- Prevention of unauthorized application from running.
- Protection against synflood attacks — a family of DoS attacks against the server's TCP processing.
- Detection of port scans, which all hackers employ to determine vulnerabilities based on a server's responses to specific services and port numbers.

Bottom line

After three days, the attack team could not find a perceptible disruption to phone communications. We only had two minor concerns about the Cisco system as tested.

First, our hackers could readily insert a passive probe into an IP phone station connection. From that vantage point they could observe and collect full traffic details — protocols, addresses, and even capture RTP, which is the VoIP protocol that runs above UDP and carries all voice samples in all VoIP systems. VoIP streams to/from Cisco 7970 phones can be 128-bit encrypted, however. Our hacker team readily acknowledged that it could not hope to decrypt those streams.

Second, with the network information collected via the inserted probe, the hackers could insert their own computer, gain access to the voice virtual LAN and send traffic to other devices on the VLAN. They could not impersonate an IP phone or spoof an IP phone call, however. With all the other controls in place, they could not further exploit the system.

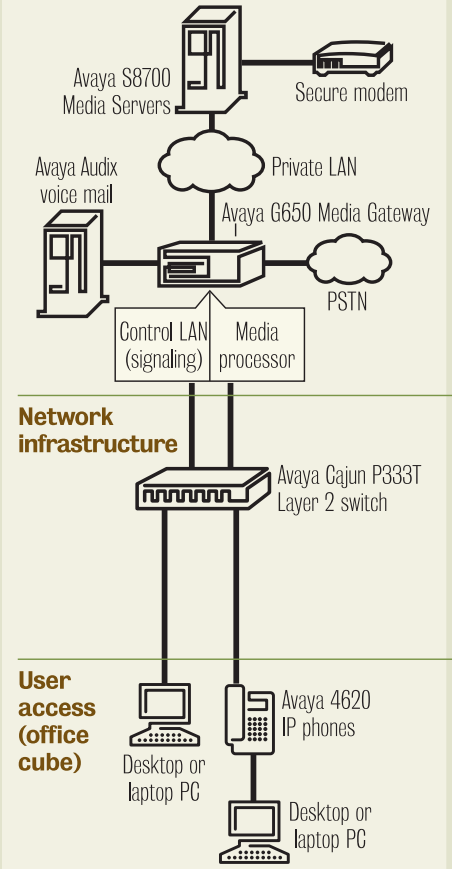
Achieving what Cisco did — orchestrating effective security across so many layers and platforms — is no mean feat. The subtle inter-relationships and correct setup of all these security pieces is daunting. But despite all the Cisco security experts on hand to tune, monitor and configure the various systems, we still uncovered configuration problems.

One of the firewalls as configured by Cisco was passing no traffic in either direction — which might be secure, but not very practical. Also a vulnerable service mistakenly was left running on one node. While these things, and others, were promptly fixed, the point is that even the best-laid security plan can be affected, even compromised, because of improper or incorrect settings.

Avaya, Part one

The first configuration Avaya submitted for security assessment had a minimal network infrastructure (see "Avaya no-frills VoIP security topology," page 4). In fact, there was no Layer 3 network infrastructure at all. All IP communications traversed a single, flat, switched Layer 2

Avaya no-frills VoIP security topology



Key security components

- Private LAN separates call controller (S8700) from user network.
- Remote management is via secure modem link; not IP.
- Voice mail connected by analog trunks, accessible from public switched telephone network independent of IP network.
- IP management access to switch disabled (console access only).
- Separate voice and data VLANs; and no routed connectivity between voice and data VLANs.
- Switch "locked down"; media access control addresses, once learned, can't change.
- Media (Real-time Transfer Protocol stream) encryption supported on all IP phones (but call-control signaling is not encrypted).
- Static IP addresses for all IP phones and hosts.
- Password-based authentication of IP phones.

network, segregated into two isolated VLANs, one for voice and the other for data. No firewalls were employed.

Despite this minimal network infrastructure, the Avaya VoIP package does feature various inherent security mechanisms. Consider the VoIP infrastructure, for example:

● Call control, in the form of a set of redundant S8700 Media Servers, connect the call control to a private LAN, which isolates and insulates them from the production network. The servers connect only to a specialized IP System Interface module, running Version 5 housed in the G650 Media Gateway chassis.

● Voice mail connects via analog trunks, which Avaya says is a plus when there are problems with or threats promulgating from the IP network. Even if all phones are IP, calls still can be received from the public switched telephone network and routed to voice mail, regardless of the state of the IP network.

● Rather than connect via the Internet, Avaya endorses a secure-modem connection for remote diagnostics and testing. But while this certainly avoids IP-based assaults, it hardly represents the state of the art in data networking or security.

● System software uploads involve a two-step process: The administrator downloads new software onto a laptop and then uploads the software from the laptop into the call-control system.

However, the Avaya topology call-control information is not encrypted, and the passwords used for IP phone authentication are not very strong.

The Avaya Cajun P333 switch does offer some security features. Those applied in our test environment were:

● For port security the administrator can lock down the port to one, two or three MAC addresses, once the switch has learned the MAC(s). This was applied in our environment, locking the switch port to one MAC. If a user moves with his PC to another location and switch port, the administrator has to manually release and then relock the switch ports. But because we readily could observe and record traffic on our data and voice links, we could have our hacker computer use a legitimate MAC address. The switch never knew the difference.

● Management-access restrictions, such as closing out all IP-based management access to the switch (Web and Telnet), allow access only via the serial console port.

● SNMP traps can be issued for VLAN violations and for any configuration changes.

Our hackers learned quite a bit by querying Avaya's IP phones via SNMP, using the universal default SNMP community name "public." But the phones could not be reconfigured, disabled or otherwise exploited via SNMP sets (writes).

Bottom line

Two of our attack team's main penetration and surveillance tricks that were successful in getting into the Cisco system worked equally well in this Avaya environment. The hackers could readily insert a passive probe into an IP phone station connection, and observe and collect full traffic details. VoIP streams to/from the Avaya 4620 IP phones also were encrypted. The hackers also could insert their own computers, gain access to the voice VLAN and contact other devices on the VLAN — but could not impersonate an IP phone or spoof an IP phone call.

The attack team then uncovered two serious vulnerabilities that could be exploited to disrupt voice communications.

One particularly effective attack involved just the IP phones. This was a fairly sophisticated, two-step assault. By sending a high rate of a particular traffic type to an IP phone for a few minutes, the phone in many cases would reboot. Rebooting made the phone susceptible to the second part of the assault, delivery of a handful of special packets, which disabled the phone for 20 minutes. Many phones could be disabled in this manner, one at a time. By repeating the part-two packet stream during the 20-minute period, affected phones could be disabled indefinitely.

Other vulnerabilities were exposed, too, but time did not permit them to be fully exploited. One of these is that the switch data port on the back of Avaya's IP phone accepts and passes user traffic with VLAN tags appended. This makes the hacker's job easier. For example, the hacker computer could then plug in the back of the phone and start sending spoofed voice traffic — with the appropriate voice-VLAN tag; you don't even need to unplug the phone.

We also observed that certain traffic types sent to particular ports on the call-control equipment could increase the time it takes for calls to be processed. And in the hacker world, if you can cause it to slow down, it indicates a vulnerability that you can, with enough time, exploit to gum up the whole works.

Avaya, Part two

Avaya took home the lessons it learned from the first round and returned with a more hardened, more secure configuration (see "Avaya maximum-security topology," right).

Officially, Avaya says its IP-telephony package is switch-agnostic, with regard to the Layer 2 and Layer 3 equipment that underlies the VoIP infrastructure. So the Avaya Cajun P333 switch employed in the first test round was replaced in the second round with Layer 2/Layer 3 switches from Extreme, with which Avaya partners.

The key new components, all additions to the network infrastructure, included: an Avaya SG208 Security Gateway ($15,000); an Extreme Summit 300-48 Layer 2/Layer 3 switch ($8,000); and an Extreme Alpine 3804 Layer 3 switch ($10,000). The Avaya VoIP equipment was unchanged. In fact, the same software loads were run in this retest, for the Avaya S8700, the G650 Media Gateway, the Control LAN (CLAN) and media processing modules, and even the same IP phone firmware release. The CLAN module ran firmware Version 9; the media processing module ran firmware Version 75, and the IP phone ran Version 2.0 firmware.

The Avaya Cajun P333 switch used in the first round was replaced with Summit 300-48. So, the frills necessary to shore up Avaya's security story in the second test round amount to about $30,000.

Architecturally, the addition of Layer 3 IP routing and other key configuration changes prevented the type of attack that was developed in the first test round, where a rogue hacker computer directly assaulted other IP phones.

The changes that enhanced security were:

- Rate limiting of IP traffic by the Summit switch prevented any TCP, UDP or broadcast packet stream from exceeding 1M bit/sec.
- Individual VLANs per IP phone port were set up. An IP phone cannot directly assault another IP phone if it is on a different VLAN. Then any traffic between phones has to be routed. And then it can be examined, blocked by protocol, even rate-limited, as noted. Managing per-port VLANs also can be an administrative nightmare, especially when IP phones number several hundred or more. So the scalability of this approach in large VoIP deployments is dubious.
- A process Avaya calls "shuffling" is disabled. Shuffling is the ability of an IP phone to directly exchange RTP voice streams with another IP phone. With shuffling disabled, all VoIP streams must pass through the media processing module. So disabling shuffling provides for good control and network security, but it makes the media processing module a bottleneck. An Avaya source says a media processing module can handle up to about 64 concurrent calls. So the scalability of this approach is questionable.

The Extreme Alpine can restrict traffic it passes to known IP phone MAC addresses. That means a hacker has to spoof a legitimate IP phone's MAC address to send traffic through the Alpine. That is exactly what our attack team did. The passive monitoring insert cable our team developed lets all active network addresses be seen and captured, even in this hardened Avaya configuration.

The SG208 firewall was configured to let only traffic of specific ports pass to and from the call-control equipment. Only traffic within a narrow, specific UDP port range was allowed to pass to the media processing module, and only the ports and protocols associated with Avaya's H.323-based call-control signaling were passed to the CLAN module. It didn't take the hackers long, with straightforward techniques, to figure out which ports were open. Their surveillance confirmed that call processing was H.323, and that meant certain ports had to be in use. And using borrowed real-phone IP identities, they were able to contact the call-control infrastructure and get responses.

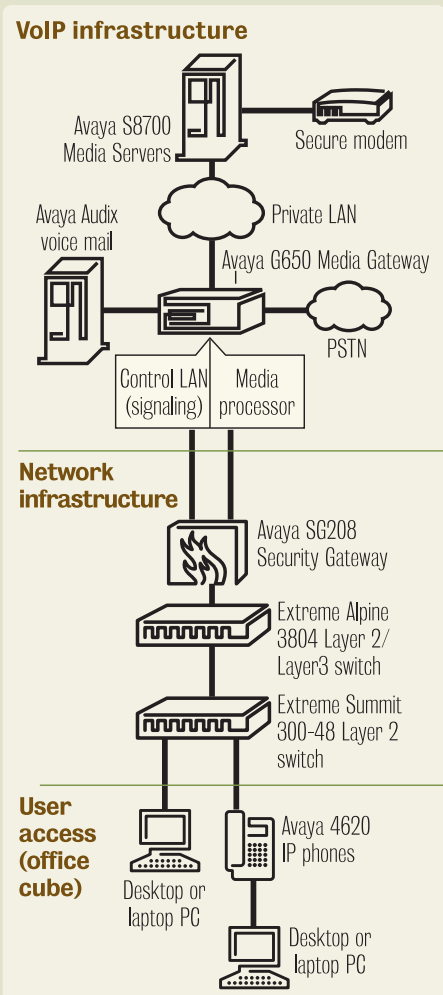
It is not necessary to emulate all aspects of a legitimate IP phone's operation, or even to know its password, for example, to penetrate the call-control infrastructure. Full emulation of an IP phone's password, protocols and packet streams is necessary to place an unauthorized phone call. But most hackers have more sinister objectives.

Bottom line

As in the first Avaya test and the Cisco test before that, the attack team readily could insert its passive probe into an IP phone station connection, and observe and collect full traffic details but not decipher the encrypted voice streams.

Similarly, with the network information they collected, the hackers successfully could insert their own computer and — using the MAC, IP and VLAN tag of a legitimate IP

Avaya maximum-security topology



Key security components

- Private LAN separates call controller (S8700) from user network.
- Remote management is via secure modem link; not IP.
- Voice mail connected by analog trunks, accessible from public switched telephone network independent of IP network.
- No direct phone-to-phone VoIP (shuffling); all streams go through media processor.
- Firewall rules restrict access to VoIP infrastructure; local even logging.
- Each IP phone isolated on its own unique VLAN.
- Static media access control addresses "locked down" to port and VLAN; static Address Resolution Protocol supported.
- Summit Layer 3 rate limiting.
- Media (Real-time Transfer Protocol stream) encryption supported on all IP phones (but call-control signaling is not encrypted).
- Static IP addresses for all IP phones and hosts.
- Password-based authentication of IP phones.

phone — gain access to the voice infrastructure and contact other devices within the VoIP infrastructure.

The attack that worked in the previous test round against other IP phones no longer worked with this Avaya configuration. But the attack team did turn up another vulnerability. By issuing a very low volume of packets, using a specific protocol and port to the call-control equipment, IP phones could be prevented from registering. In normal circumstances this would affect just a small number of phones: An IP phone registers only when it's first plugged in.

So unless a phone was moved or unplugged, it normally wouldn't need to re-register. Still, phones could be prevented from registering for as long as the very low-volume traffic stream continued to be sent to the call controller.

Avaya determined that a software patch to its call-control software was necessary to address this vulnerability. The company committed to fixing the problem.

In the final analysis, and given the relatively minor nature of this security hole, we gave Avaya an overall resistant rating for this maximum-security configuration.

Conclusion

Our findings underscore a tenet of network security: Effective security has to address all layers. Cisco applied effective measures at Layers 2 and 3 (Catalyst switches), Layers 4 and 5 (firewalls and IPS), Layer 6 (RTP voice stream encryption, still limited to certain phones, though), and Layer 7 (with server-based software such as the Cisco Security Agent).

The first Avaya configuration had limited Layer 2 defenses and very few defenses at Layers 3 and above, except for Layer 6. To its credit, Avaya does have good RTP encryption (Layer 6) support on all its phones. Avaya's hardened, maximum-security configuration addresses Layers 3, 4 and 6 more effectively, but still left some holes.

VoIP security, spawned by the popularity and proliferation of IP telephony, is a critical issue, and we challenge other IP telephony providers to throw their hats into the ring.

Mier is a network technologist, consultant, author and founder of Miercom, a network product test center in Cranbury, N.J. Birdsall is senior test engineer with Miercom. Thayer is principal investigator with Canola & Jones, a security research firm based in Mountain View, Calif. They can be reached at edmier @miercom.com, rbirdsall@miercom.com and rodney@canola-jones.com, respectively.