

Finding a secure voice



The increasing uptake of VoIP has uncovered security risks that need to be taken into account when considering implementation. Alan Harstein reports on these vulnerabilities and how to plug the gaps.

The ability to make phone calls over the internet using voice over internet protocol (VoIP) technology, where traditional public switched telephone networks (PSTN) are merged with IP and wireless systems, has opened up a huge range of possibilities for end users. Not only are vastly cheaper phone calls, both local and international, now possible, but there is also the potential to save vast amounts in network support and administration. Add the possibilities for merging all voice, video and data over the one central network architecture and the possibilities for productivity improvements seem limitless.

However, as is becoming increasingly more apparent with the accelerated pace of end-user uptake, VoIP has also brought with it a potential Pandora's Box of security risks. Would-be hackers can now exploit both old and new network vulnerabilities operating over the one network, and risks that had previously only been associated with traditional data IP technologies have been inherited by voice networks. What this effectively means is that VoIP security over the public internet is now only as safe as that provided for traditional web traffic and email.

"Like data networks, security vulnerabilities in VoIP can be susceptible to common targets for viruses, worms, trojans etc, which previously didn't exist in traditional PSTN phone systems," Sydney-based IP telephony services provider Allcom Networks director, Andrew Leigh said. IP PBXs (private branch exchanges) are now far less secure than traditional PBXs because traditional PBXs are connected to a telephony provider, whereas IP PBXs are connected to both the telephony provider and the open internet.

Furthermore, whilst a new set of protocols supporting VoIP technology are still in the process of being developed, new vulnerabilities are continuing to emerge. As a consequence, threats to security will continue to appear both from existing internet vulnerabilities and the old telephone network, as hackers attempt to exploit whatever vulnerabilities may come their way. So where does that leave end users, equipment vendors and service providers and what sorts of threats are likely to emerge over the next few years?

Cisco Australia's unified communications manager, Peter Hughes believes the nature of VoIP security has changed over the last few years, because the higher uptake has led to more frequent and vicious attacks over IP networks in general and, as voice is part of those networks, it too has been subject to those attacks.

Erik Rudin, VoIP solutions specialist at security and systems management software vendor NetIQ, said that while VoIP or IP telephony has created new targets for security

over the net



attacks, the traditional objectives of hackers have remained the same. "Whether you run a TDM or IPT phone system, the attacker has common goals; hurt the carrier, disrupt or degrade service (eg, deny dial tone), steal service (eg, toll fraud), hurt the subscriber, identity fraud (eg, use a stolen phone, access card), steal information (eg, eavesdrop) or compromise information (eg, change voicemail)."

Colin Lim, ANZ regional sales manager for security vendor Fortinet, said that as with all new technologies, once adoption rates improve, attackers also begin to focus their interests on the technology. "New threats evolve from old threats, and this is certainly true of VoIP." Evidence of this, Lim added, could be seen in the evolution of 'spit', or voice spam and phishing attacks using a bogus voicemail system rather than a bogus website.

The nature of the threats

As VoIP converts voice signals from the telephone into digital signals (data packets) that travel over the internet, from a security perspective it is just as vulnerable to other data traversing the internet. This has opened it up to a range of old data network threats.

As Lim pointed out, since VoIP involves placing IP handsets on the LAN, the attacks that plague all other LAN connected hosts will apply. "This means that DoS, virus/worm, trojans, spam, phishing, eavesdropping, spoofing and MITM attacks are all capable of finding their way into VoIP deployments as attackers begin turning their attention to it," Lim said.

VoIP technology has also added many new devices and components to a standard IP network. Each of these has brought with it potential operating system, application and configuration vulnerabilities. As a consequence, new targets have emerged, such as exploiting IPT operating systems on phones, attacking IPT infrastructure, exploiting IPT servers (gateways, call managers) and exploiting media servers (eg, voicemail). Spying, theft and data manipulation can also give

a savvy hacker the opportunity to potentially gain access to user account information, including IDs and passwords. This can then be potentially used to make unauthorised network modifications, from changing profiles to altering calling plans and even listening to voice messages, making eavesdropping a major VoIP security concern.

As Rudin said, in many organisations, a lot of focus, time and money are directed towards 'hardening' the perimeter so that intruders can't get inside the enterprise network. "Firewalls do a good job of protecting the perimeter. However, many times the real security threats to an organisation are internal. This means an employee or contractor could intentionally sabotage or accidentally bring down your VoIP service."

Another challenge with VoIP has to do with technology protocol adoption within the marketplace. The best example of this is the SIP signalling protocol used by VoIP devices to set up a call between endpoints.

Session initiation protocol (SIP) is a signalling protocol for IP telephony. SIP voice protocols provide a standard for authenticating users, a critical component of VoIP security,

As Rudin said, in many organisations, a lot of focus, time and money are directed towards 'hardening' the perimeter so that intruders can't get inside the enterprise network. "Firewalls do a good job of protecting the perimeter. However, many times the real security threats to an organisation are internal. This means an employee or contractor could intentionally sabotage or accidentally bring down your VoIP service."

Another challenge with VoIP has to do with technology protocol adoption within the marketplace. The best example of this is the SIP signalling protocol used by VoIP devices to set up a call between endpoints.

Session initiation protocol (SIP) is a signalling protocol for IP telephony. SIP voice protocols provide a standard for authenticating users, a critical component of VoIP security,

Agreeing to new standards

Another challenge with VoIP has to do with technology protocol adoption within the marketplace. The best example of this is the SIP signalling protocol used by VoIP devices to set up a call between endpoints.

Session initiation protocol (SIP) is a signalling protocol for IP telephony. SIP voice protocols provide a standard for authenticating users, a critical component of VoIP security,