[in]security

by Gary McGraw

Is VoIP Secure Enough For Prime Time? : : :

VoIP is hot, but VoIP security is not. Security risks abound in current commercial VoIP solutions, including Denial of Service (DoS) attacks, eavesdropping, and a host of new vectors for intrusion and malware propagation. As it stands now, the benefits of VoIP—cheaper phone bills and converged voice and data applications—may not be worth the risks.

CAN YOU HEAR ME NOW?

When you migrate voice from a circuit-switched medium to a packet-switched one, you expose that voice traffic to a pair of serious security risks: DoS attacks and eavesdropping.

Unlike traditional uses of IP networks (think downloading files), VoIP is ultrasensitive to latency. Seemingly small delays of 150ms can transform a high-quality call into unintelligible gobbledygook. Jitter, a phenomenon where network-induced delays cause packets to arrive out of sequence, can also be problematic. Losing a single packet isn't a big deal because VoIP packets are small and contain only 12 to 62ms worth of data. But packet loss as low as 1 percent can make a call hard to understand, and a 5 percent loss turns VoIP into toast.

> "Consider the business impact of an attack that derails data and phone service in one swoop."

The upshot is that VoIP networks are easy prey for DoS attacks. Network architects should strongly consider the business impact of a simple attack that can completely derail both data applications and phone service in one fell swoop. And note that not all DoS problems are packet-based. A simple power outage will silence a VoIP dial tone as effectively as any black hat.

VoIP also makes it easier for attackers to eavesdrop. The kind of physical access to a line or a switch required to tap a phone isn't required to tap a VoIP call. Common network sniffing tools, including Ethereal (www.ethereal.com) and tcpdump (http://sourceforge.net/projects/tcpdump), have plug-ins for both the Session Initiation Protocol (SIP) and H.323. The hilariously named vomit tool (an acronym for "voice over misconfigured Internet telephones," http://vomit.xtdnet.nl) converts tcpdump files into .wav files that can be played on any PC.

To protect against eavesdropping, VoIP users can use SSL/TLS, a VPN, or possibly IPSec. However, packet size, ciphering latency, and a lack of cryptographic engines designed for packet throughput efficiency and ordering affect the trade-off. In its present form, cryptography introduces a severe and unworkable bottleneck in most VoIP systems.

THE EASE OF BUILDING EXPLOITS

As with other elements of computer security, software exploits present a real problem for VoIP. Network architects should assume that software exploiters can obtain VoIP software, disassemble it, build exploits, and even make malicious modifications. In addition, a number of academics have uncovered and published SIP implementation flaws that, when exploited, allow remote code execution, unauthorized access, and software failure, all through malformed packets. Finally, H.323 systems make use of ASN.1 parsing, which has been particularly hard hit by software exploits.

Most VoIP network installations involve many parts, from endpoints to proxies to location servers and registrars. Because many of these nodes include or support dynamically configurable parameters, attackers are presented with a large set of potential targets, just as in a normal data network. Mobile unit systems exacerbate this risk by adding IEEE 802.11 wireless security issues to the mix.

VoIP is a cool technology with a host of benefits, but the security risks are very real. Network architects considering a VoIP solution must account for these risks in their deployment calculations. If security is important to you, it may be too early for VoIP in your enterprise.

Gary McGraw is CTO of Cigital, a software quality management consultancy. He is co-author of *Exploiting Software* (Addison-Wesley, 2004), *Building Secure Software* (Addison-Wesley, 2001), and *Java Security* (Wiley, 1996). Reach him at gem@cigital.com.