White Paper

VoIP Vulnerabilities

The malicious behavior that we have seen in other media already plagues Internet voice calls. In this report, we examine vulnerability trends as well as protocol- and application-layer attacks. We offer both a general and technical overview to the threats against Voice over Internet Protocol and how to protect and remediate against them.

By Kevin Watkins, McAfee Labs™

Table of Contents

Introduction

What is VoIP?

Voice over Internet Protocol (VoIP) is a method for making phone calls over the Internet or using private networks. Traditional phone calls must travel over a series of switches and circuits owned by the telephone companies, which control the process and the charges. By using VoIP, both businesses and individuals can enjoy a substantial cost savings, especially while making long-distance calls.

VoIP at a technical level is a communications method that uses the competing standards Session Initiation Protocol (SIP)[1] and H.323,[2] both of which are widely deployed. The two standards deal with the routing of voice conversations over the Internet, or IP-based networks. The standards define protocols that are derived from traditional phone systems. Signaling protocols replace the traditional private branch exchange (PBX) functions and are carried out by server-based IP PBXs with application software. Examples of this software include Cisco Call Manager, Nortel CallPilot, and Asterisk. The second type, media protocols, define the protocols used between two endpoints or VoIP phone devices. Examples include the Cisco 7900 series phones or a VoIP wireless phone. Vulnerabilities in VoIP have been found in the signaling and media protocols, the call management software, and in the VoIP phone devices themselves.

This report will discuss major VoIP vulnerabilities, how attacks occur, and how to protect your enterprise from VoIP attacks.

VoIP vulnerability trends and targets

McAfee Labs first observed an increase in VoIP vulnerabilities during the end of 2006 and that trend has continued through today. We can credit part of this increase to better tools for finding VoIP vulnerabilities, yet this upward trend should be largely attributed to the growing number of VoIP installations. According to a report by Infonetics Research, overall enterprise telephony grew more than 8 percent in the second and third quarters of 2008. Vendors Cisco, Avaya, and Nortel have been consistently in the top three of enterprise vendor deployment. Recently, Cisco took the top spot overall with growth of 19 percent in the third quarter of 2008. Avaya grew 10 percent, with Nortel completing the top three.[3] It's hardly surprising that products from these three vendors have the majority of known VoIP vulnerabilities.

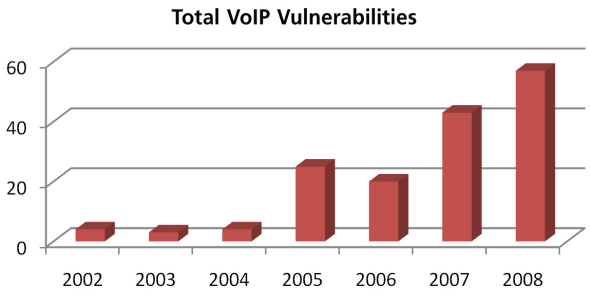

Figure 1: Total vulnerabilities have trended rapidly upward since 2006. (Source: NVD)

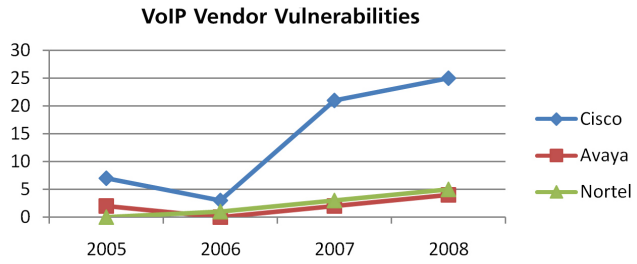

Figure 2: Cisco leads by far the three top vendors in this field. (Source: NVD)

How Do Attacks Happen?

Making VoIP calls

To understand how attacks happen, we need to understand how VoIP architecture works. Figure 3 shows the components of a call, starting with (1) the user initiating the call to another user. The request is sent, via an invite request, across the signaling protocol/SIP to the call-management software (2). After the invite, the call-management software locates and forwards the request to the receiver (3). At this point, control is passed to the two users and the media transport protocol/real-time transport protocol (RTP) encodes and transports the media conversation. This example uses SIP, although the steps in other VoIP environments are similar.

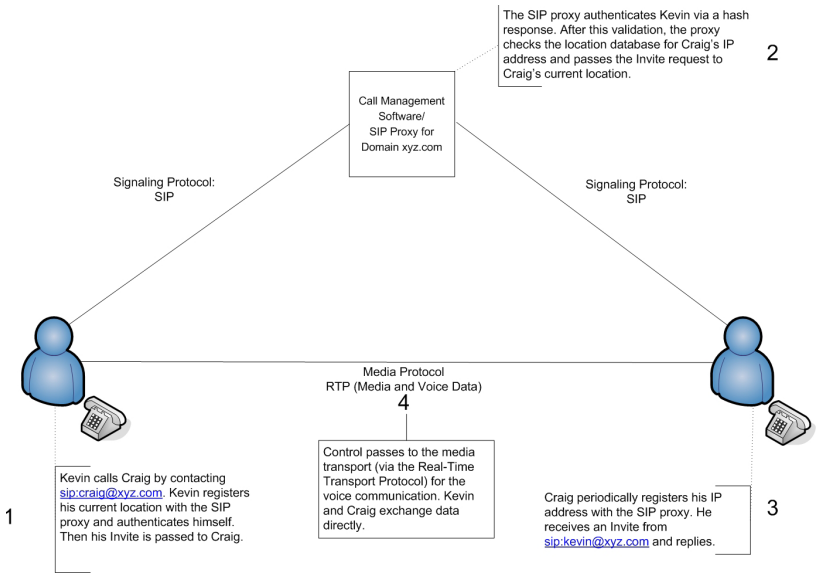

Figure 3: VoIP in action, using SIP.

Various steps in this process are open to vulnerabilities, from denial of service of the invite requests, to eavesdropping on the media conversation between the two users, and to holes in the call-management software. Let's look at those attacks and vulnerabilities.

Protocol-Level Attacks

Eavesdropping

In 2001, we first saw VOMIT (Voice Over Misconfigured Internet Telephones).[4] This tool takes the network traffic dump of a Cisco IP phone conversation and converts it to a file that can be played on ordinary sound players. The tool supported only H.323/G.711, or Cisco IP phones, although tools such as VoIPong work for SIP and the media transport protocol/RTP.[5]

Figure 4 shows SIP/RTP sniffing between two IP phones, and the default configuration of Asterisk. The example uses WireShark (formerly Ethereal), an open-source network-analysis tool (or sniffer).

Eavesdropping attacks can occur because the media transport protocol that carries the conversation lacks encryption in many default configurations. This is the case when using RTP as the media transport layer. For a superior solution, you should use secure RTP (SRTP), which provides both encryption and authentication.[6]

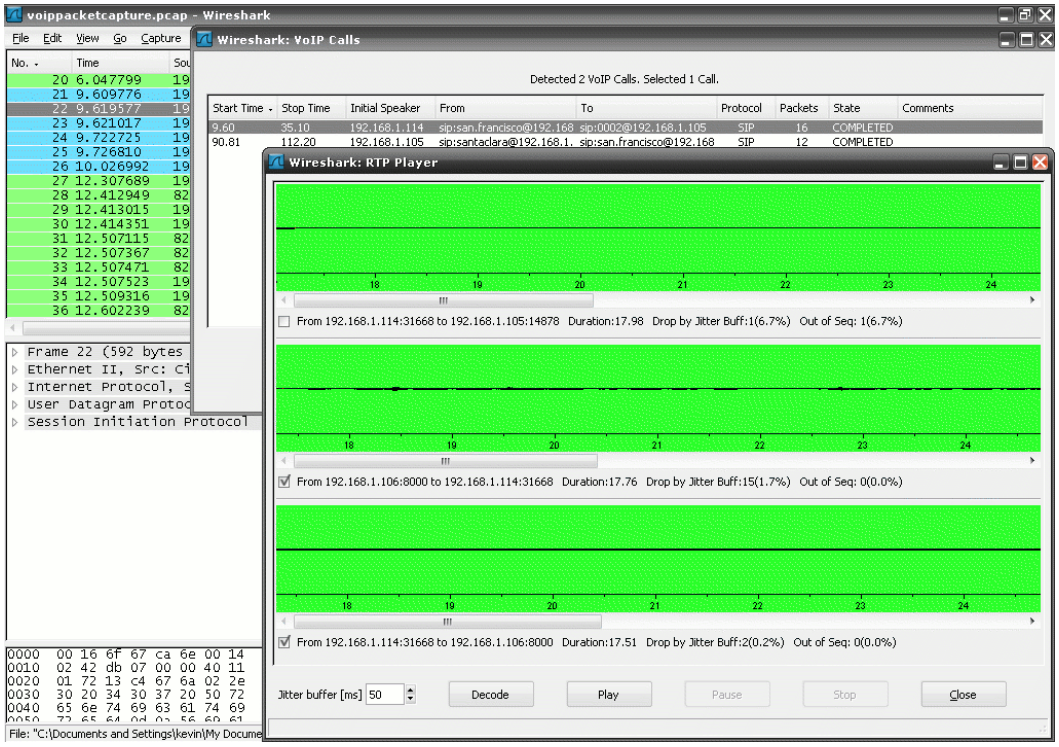

Figure 4: Eavesdropping on a VoIP call.

Replay

A replay attack replays a legitimate session (usually captured by sniffing the network traffic) against a target. For VoIP, replay attacks can occur in the signaling protocol SIP. One well-known attack uses replay techniques for registration hijacking. The SIP employs the register command to tell the call-management software where a user is located, based on the IP address. An attacker can replay this request and substitute another IP address, thereby redirecting all calls to the attacker. Replay attacks occur because parts of SIP are communicated in plain text. To protect against this type of attack we can now use SIPS (SIP over transport-layer security). SIPS provides integrity and authentication between the user and call-management software.

Denial of service

Because VoIP is a service on the IP network, it is open to the same flooding attacks that affect other IP-based services. Infrastructure attacks include TCP SYN/User Datagram Protocol floods of VoIP IP PBX and VoIP phone devices. Signaling and media protocol attacks are also well known in the hacker community, with tools such as the SIP Invite flooder, which sends a flurry of SIP invite requests to an IP phone, thus exhausting its resources; or the "bye teardown" attack, which injects a "bye" into the network stream, thereby ending the call.[7, 8]

Denial-of-service attacks such as these have been a source of blackmail by attackers. Traditional phone service is considered 99.999 percent available (the "five nines" of telephony) and we expect similar uptime for VoIP. Yet VoIP is open to flooding attacks (using botnets and other tools), and numerous denial-of-service vulnerabilities lie in VoIP equipment.

Signal and media manipulation

Again, because VoIP is a service on the IP network, it is vulnerable to the same network-manipulation attacks as other network services. One such attack is "RTP InsertSound," which allows an intruder to inject sound files into an RTP media stream (a voice conversation between two or more IP phones).[9]

Application-Level Attacks

VoIP devices with open services

Many phones expose a service port that allows administrators to gather statistics, information, and remote configuration settings. These ports open the door to information-disclosure theft that attackers can use to gain more insight to a network and identify the VoIP phones.

VoIP phone web services

Many of the service ports on VoIP phones that expose data also interact as web services and thus are prone to common vulnerabilities such as cross-site request forgeries and cross-site scripting. The former occur when a link is inserted in a web page that uses the credentials, usually in a cookie, of the victim. One example is a vulnerability that was recently found in Snom Technology's SIP phones, which allow users to change device settings, view call history, or even make phone calls via a built-in web interface. An attack can occur if the attacker knows the IP address of the VoIP device. By luring a phone user to a malicious site, the attacker can grab the user's credentials and access the phone via its IP address, accessing the phone as its owner. This method is particularly insidious because it defeats the firewall.

Vishing

We have long verified personal information by phone, and we're generally accustomed to trusting that the callers are who they claim to be. With traditional phone calls we can often track a caller to a physical location and we often rely on caller ID to provide identification. With VoIP these safeguards are gone. Calls can come from anywhere on the Internet and the caller-ID verification can easily be spoofed. Cybercriminals are now exploiting this anonymity using "vishing" techniques, the combination of VoIP and caller-ID spoofing. Much like phishing, a vishing attack often looks like a financial institution that is asking for personal information such as credit card and social security numbers. We have seen reports of a few of these attacks. In one recent example an email appeared to be from a bank and offered a local VoIP number for contact. Because the number was local, it added legitimacy to the email.[10] With caller IDs so easily spoofed and VoIP numbers so easily created, we anticipate there will be many more of this type of social engineering attack.

VoIP spam

VoIP, like standard phone service, is also vulnerable to unsolicited and unwanted communications. VoIP spam is also known as SPIT (spam over Internet telephony). Telemarketers have noticed VoIP and the potential of using automation to reach thousands of users. Such unwelcome calls can rapidly consume resources and create a denial-of-service attack. Using the lessons we have learned (authentication, whitelists, etc.) from email and traditional phone service, we can lessen the risks of SPIT.

VoIP toll fraud

Toll fraud is the act of gaining access to a VoIP network (call manager or gateway) and making unauthorized calls (usually long distance or international). Attackers exploit weak usernames and passwords, open gateways, and other application-level attacks mentioned in this report. Toll fraud is one of the most frequent attacks against VoIP. We have seen attackers targeting small businesses—such as in Perth, Australia, where they made 11,000 calls costing more than US$120,000[11]—to attackers stealing more than 120 million VoIP minutes and making $1.2 million from Verizon and AT&T.[12]

Conclusion

Securing the VoIP network requires combing two primary practices:

- Design the VoIP network with optimized security in mind—using encryption, firewalls, and virtual LANs. For instance, use SRTP to secure the network from eavesdropping and separate the VoIP network into its own VLAN. If possible, use SIPS. Employ industry best practices and baseline standards to insure that call controllers and VoIP phones are secure from the start. Insure effective patch management: Take countermeasures and immediately update all systems with the latest available software patches as soon as an exploit or vulnerability is announced. Use a vulnerability management service to identify VoIP phones and call controllers that are exposed to vulnerabilities or are not up to date.
- Understand current VoIP vulnerabilities. Learn the nature of VoIP security threats, and employ the latest proactive security products at the network perimeter and core to protect against zero-day attacks and exploits. Especially guard the connection at the gateway between the internal VoIP and external traditional networks.

With the right amount of security and precautions VoIP can be even more secure than traditional phone service.

Kevin Watkins *is a security researcher at McAfee Labs. He leads the regulatory compliance content and mappings across McAfee products. Watkins has led the implementation of VoIP at McAfee and contributes to working groups that are bringing VoIP to the Secure Content Automation Protocol. He has served in the security industry for more than ten years and has designed security software and content used by many Fortune 100 companies and government agencies. In his free time Watkins enjoys biking in the California mountains or snowboarding at Lake Tahoe.*

About McAfee Labs

McAfee Labs is the global research team of McAfee, Inc. With the only research organization devoted to all threat vectors— malware, web, email, network, and vulnerabilities—McAfee Labs gathers intelligence from its millions of sensors and its cloud-based reputation technologies such as Artemis and TrustedSource. McAfee Labs' 350 multidisciplinary researchers in 30 countries follow the complete range of threats in real time, identifying application vulnerabilities, analyzing and correlating risks, and enabling instant remediation to protect enterprises and the public.

About McAfee, Inc.

McAfee, Inc., headquartered in Santa Clara, California, is the world's largest dedicated security technology company. McAfee is relentlessly committed to tackling the world's toughest security challenges. The company delivers proactive and proven solutions and services that help secure systems and networks around the world, allowing users to safely connect to the Internet, browse, and shop the web more securely. Backed by an award-winning research team, McAfee creates innovative products that empower home users, businesses, the public sector, and service providers by enabling them to prove compliance with regulations, protect data, prevent disruptions, identify vulnerabilities, and continuously monitor and improve their security. www.mcafee.com.

Endnotes

1. "Session Initiation Protocol," Internet Engineering Task Force. *http://tools.ietf.org/html/rfc3261*
2. "H.323: Packet-based multimedia communications systems," International Telecommunication Union. *http://www.itu.int/rec/T-REC-H.323/e*
3. "Is Anyone Really Buying Unified Communications?" TMCnet. *http://intellicom-analytics.com/PressRelease/PDFs/1.pdf*
4. "Vomit—Voice Over Misconfigured Internet Telephones," Monkey.org. *http://vomit.xtdnet.nl/*
5. EnderUnix. *http://www.enderunix.org/voipong/index.php*
6. "The Secure Real-time Transport Protocol (SRTP)," IETF. *http://tools.ietf.org/html/rfc3711*
7. *http://www.hackingvoip.com/tools/inviteflood.tar.gz*
8. *http://www.hackingvoip.com/tools/teardown.tar.gz*
9. David Endler and Mark Collier, "Hacking Exposed VoIP: Voice Over IP Security Secrets & Solutions." *http://www.hackingvoip.com/sec_tools.html*
10. " 'Vishing': Beware of e-mail asking you to phone your bank," The Age. *http://www.theage.com.au/news/Technology/Vishing-Beware-of-email-asking-you-to-phone-your-bank/2006/07/24/1153593241137.html*
11. "VoIP hackers strike Perth business," ZDNet Australia. *http://www.zdnet.com.au/news/communications/soa/VoIP-hackers-strike-Perth-business/0,130061791,339294515,00.htm?ocid=nl_SEC_21012009_fea_l1&omnRef*
    "VoIP toll fraud attack racks up a £57K bill in two days," ITProPortal. *http://www.itproportal.com/security/news/article/2009/1/28/voip-toll-fraud-attack-racks-57k-bill-two-days/*
12. "Men Charged with Stealing More Than 120 Million VoIP Minutes from Verizon, AT&T," TMCnet.com. *http://hosted-voip.tmcnet.com/feature/articles/53861-men-charged-with-stealing-more-than-120-million.htm*

McAfee, Inc.
3965 Freedom Circle
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

7528wp_labs_voipvuln_1109