



White Paper

13 Reasons to be Worried About Voice Over IP Phone Calls...and What You Can Do About It



See, Act, Deliver

May 7, 2006

Contents

VoIP Security Vulnerabilities for Government.....	2
An attacker eavesdrops on your calls	2
Your call is denied	3
Your call gets altered	3
An attacker impersonates you	3
You get someone else's calls.....	3
An attacker breaks into your voicemail.....	3
Your phone or hand-set gets a virus.....	3
Your call is garbled	4
Your phone keeps ringing, and you keep answering it—but no one is there.....	4
Your calls end abruptly	4
Your voicemail box is filling up with "junk" mail	4
Your phone is filling up with "junk" text messages	4
What You Can Do About It.....	4

This paper discusses VoIP security vulnerabilities for the federal government and what you can do about them.

VoIP Security Vulnerabilities for Government

Voice over Internet Protocol (VoIP) offers a great many advantages over legacy POTS (plain old telephone systems) in terms of cost, features and service integration. However, it also means increased exposure on the Internet, which can translate into a risk of attack through inherent security vulnerabilities.

VoIP phone calls use the same kind of network that data has been using for years. Although network security products are mature, very few security solutions exist just for VoIP. Add connectivity to existing, traditional phone systems, and vulnerabilities increase. And in government, security concerns increase when your calls require privacy or relate to national security. Although there are numerous, potential security problems, here is a baker's dozen of possible VoIP security vulnerabilities—and what can be done about them.

An attacker eavesdrops on your calls

With POTS, eavesdropping usually means tapping a phone line or a phone switch, using low-tech "jumper cables" and a handset. With VoIP, attackers can eavesdrop and listen in on calls by tapping into any node in the network between phones. VoIP eavesdropping, unlike POTS phone taps, are virtually impossible to detect.

When eavesdropping, an attacker hijacks packets from your phone call. Also called a "man-in-the-middle" attack, the attacker can receive all the call information that your call server provides. You may not even know that your call is being intercepted.

A variation on this theme is when the attacker redirects all call information from your phone to the intruder's phone. In this case, the intruder operates at the application layer, which is much more difficult to detect.

The only reliable protection against eavesdropping is end-to-end encryption of the data stream.

Your call is denied

There are several attack scenarios that lead to denial of service (DoS), including attacks against the call server, voicemail server, PSTN (public switched telephone network) gateways or the VoIP phone itself. DoS attacks are not easy to identify: the phone may indicate that it cannot connect to the CallManager, you may not get a dial tone when you pick up the receiver, you may not be able to dial an outside number, or you may get a “fast busy” for all call attempts. This problem becomes critical if you need to place an emergency E911 call.

Given the breadth of the attack scenarios, it is not easy to devise a single protection strategy for DoS.

Your call gets altered

Once inside a VoIP network, an attacker can inject voice packets or delete packets from a call stream, changing the content and integrity of your call.

An attacker impersonates you

An attacker can appear as a legitimate user, including yourself, by using your permission level and creating damage, such as crashing the phone switches, causing call service and quality to deteriorate, and disclosing confidential data. Or more simply, the attacker may only make calls that are attributed to your phone (that is, toll fraud charges or nuisance phone calls.)

You get someone else’s calls

An attacker can disrupt the VoIP network in a way that the IP address for your phone is changed, making you get calls for someone else. On the face of it, this doesn’t seem like that big of a deal. You can always tell the caller that it is a wrong number. However, it may be the right number, and you could access the other user’s voicemail, which could contain confidential or secure information.

An attacker breaks into your voicemail

With VoIP, voicemail messages get stored as network data, subject to intrusion. Your own confidentiality and privacy are breached when an attacker can access these messages.

Your phone or hand-set gets a virus

An attacker can tamper with data that your phone downloads when it initializes, disrupting your phone. In this case, the attacker can inject a Trojan horse program or virus into the phone. The attacker can also entice you to download a “cool” upgrade for your phone that contains a malicious virus.

Your call is garbled

The attacker sends a number of bogus packets to your phone. As a result, your call quality may greatly deteriorate, and you may think your phone is not working properly. Your phone may even become completely disabled.

Your phone keeps ringing, and you keep answering it—but no one is there

The attacker sends a number of call requests to one or more victim phones and keeps ringing them or making users answer the call.

Your calls end abruptly

In this case, an attacker may be sending a flood of bogus messages and forcing already established calls to end. The attacker may also be redirecting calls to somewhere else.

Your voicemail box is filling up with “junk” mail

Known as SPIT (SPAM over Internet Telephony), an attacker automatically generates a number of voicemail SPAM calls. Think of it as telemarketing on steroids!

Your phone is filling up with “junk” text messages

Another variation of SPIT, the attacker can also automatically generate a number of SPAM text messages to appear on the LCD display of your VoIP phone.

What You Can Do About It

The first step in addressing these security risks and preventing problems from happening is to know that these risks can happen. If you notice any symptoms of potential security breaks affecting your IP phone calls, contact your IT department. Being proactive and vigilant can save a lot of crisis management down the road.

Check that your IT department is using good security solutions for the data network. Many VoIP security risks that affect VoIP calls can be addressed through good network security solutions.

VoIP application security requires a new set of solutions. While security management solutions for VoIP are still emerging, key to being proactive is to have a good VoIP network and call management solution operating in your VoIP network. Your IT department should have the management capabilities to see what is happening in the VoIP network, track IP phones and VoIP equipment, and to identify when call quality is degrading. Using management software to detect potential problems is crucial in preventing them from happening in the first place and is the foundation for providing secure, optimal IP phone call quality.

About Qovia, Inc.

Qovia® significantly eases the complexity of planning, monitoring and managing enterprise Internet phone networks. Providing dynamic discovery of VoIP resources and unmatched, minute-by-minute visibility into how IP telephony networks are performing, the Qovia IP Telephony Manager aggregates and analyzes IP telephony information to deliver timely call-by-call quality. Its intuitive dashboard shows a VoIP-centric view of critical IP telephony resources, allowing IT organizations to meet business objectives. Customers can use Qovia to increase the reliability and utilization of their IP telephony investments, increase end-user satisfaction and better manage the bottom line. Qovia was founded in 2002 and is backed by Canaan Partners; BlueRun Ventures (formerly Nokia Venture Partners); Anthem Capital; and the State of Maryland. The company, which has earned nearly two dozen industry awards, can be found online at www.qovia.com.

For More Information

www.qovia.com

e-mail: sales@qovia.com

© 2006 Qovia, Inc. The information contained herein is subject to change without notice. The only warranties for Qovia products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Qovia shall not be liable for technical or editorial errors or omissions contained herein.

Qovia is a trademark or registered trademark of Qovia, Inc., in the U.S. and other countries and is used under license.

05/2006