On Line With...
Haviland Telephone Company, Inc.

VoiP an uphill walk?

Like many other traditional telephone companies, we've been internally using and experimenting with Internet calling, sometimes called Voice Over Internet Protocol, or VoiP. A June 8 Wall Street Journal article ("VoiP Security Problems," Dionne Searcey and Shawn Young) really scared lots of technical people. It reported the arrests of VoiP company personnel in Miami for hacking into the networks of as many as 15 other Internet phone providers for fraudulently routing customers' calls. The company in question was alleged then to have billed one of the Internet telephone companies for more than 500,000 unauthorized calls. The company did this by hacking into routers to disguise the calls' origins, and then selling the fake call records to their own customers. Say, what?

Like most new technologies, Internet calling presents opportunity and risk. For over 5 years, the risk has been a concern. Today, companies such as the SANS Institute make a living in computer security training. Annually, several national and international VoiP security workshops are held, concentrating on security issues for VoiP and Instant Messaging (IMS).

There are 4 basic vulnerabilities: Eavesdropping, fraud, interruption of service attacks, and unsolicited calls, according to Saverio Nicolini, Senior Researcher at NEC's Network lab in Heidelberg, Germany, in a presentation at the 3rd Global VoiP security workshop in Berlin last month. In fact, he names and describes nearly 30 specific kinds of fraudulent or unintended uses of VoiP. To make matters worse, experts project that the nature of the threats will evolve as viruses and worms have in the computer data world.

Unsolicited calls are expected to be so bad, they've evolved a nasty acronym: SPIT: Spam over Internet Telephony. Spam, of course, is unwanted e-mail. It's anything you didn't ask for. It could be as innocuous as credit card sales offer, mass e-mail from your high-school class, or a newsletter from a current company you do business with. If the content is illegal (obscenity, for example), it isn't just *unwanted* e-mail. SPIT is just like that, only using voice on the Internet. SPIM is Spam over Instant Messaging. SPIT is projected to be worse than Spam, since it interrupts the caller immediately, and prevents the VoiP phone from being used for any other purpose. Similar problems are projected to affect Instant Messaging.

Today, few of the protections that have been implemented for e-mail Spam are in place to protect us against SPIT. However, SPIT travels much of the same data pathways that e-mail travels. With Spam the e-mail doesn't actually interrupt the receiver. SPIT would actually ring the phone. The caller wouldn't be just another person, as in much of today's marketing phone calls. It may be just a computer-generated message or solicitation. Just as an e-mail server is a computer that can generate millions of e-mails in very little time, a computer can generate millions of phone calls over a VoiP network much faster (and cheaper) than calls could be generated over a traditional circuit-switched network.

New approaches are needed. Most of today's e-mail filtering is content-based. Printed content is easy to check compared to voice content. Filtering probably won't work, since a voice call is real time, while e-mail can be delayed a few minutes without degrading the service, while it runs to a filtering proxy, much as Postini e-mail filtering works.

Globally, new ideas are being tested. The most promising approaches to SPIT and SPIM protection are white and black listing. Under these approaches calls coming from acceptable parties are permitted, or calls from unacceptable sources are denied. Cryptography is the best approach today for content protection. Stronger identity assertion is a

VoiP Continued...

key to future, too. Using this method, an outbound proxy is used to protect the identity of the domain name. The inbound proxy checks with a third party who vouches for the domain name identity. This is like regular call set up with CallerID. All these fixes cost money, on a service whose chief claim is lower price. As the number of VoiP providers increase, finding workable methods that all providers will use becomes more difficult.

Most companies that retail VoiP do offer some kind of protection. Some, for example, report using encryption to protect content privacy, but not encrypt call setup. Generally, small business systems are not aggressive in protecting themselves, as are many retail systems. Each business must protect voice traffic as it protects its data.

Experts suggest several tactics: Encrypt Voice. Put it on a VPN. Use your firewalls. Separate voice and data by using a virtual LAN. Use proxy servers in front of firewalls for incoming and outgoing voice data. Protect you IP phone system against viruses and denial-of-service attacks. Here's another suggestion: be careful.

More details: http://csrc.nist.gov/publications/nistpubs/800-58/SP800-58-final.pdf for a 2005 report from a governmental agency with technical recommendations; http://www.sans.org/reading_room/whitepapers/voip/ has 5 papers with VoiP security ideas; http://www.voipsa.org is a large U.S. VoiP security alliance; and a more down-played report at http://www.thevoicereport.com/telecomjunkies.html.

Ending Support for 98

Microsoft recently announced that they will no longer support Windows 98 and Windows ME. What this means to you as a user is that these products are outdated and can cause security risks to your computer if not upgraded.

It is recommended that if you are running either one of these systems that you upgrade to a newer, more secure operating system.

If you would like further information on this subject visit their web-site www.microsoft.com and follow the links for Windows 98 information.

These older operating system are not optimised for today's computer services and threats.

News Updates

• On page 41 Bennett Agency's toll-free number is listed as 1-800-456-2247. It should be 1-866-456-2247. We sincerely apologize.
• We will be changing the way we handle after-hours calls during the next few months. Customers will continue to call either 800 number, but the answering service will change.
• Our sister company, Giant Communications, has moved 2 employees from Pratt to Haviland. Giant provides our Internet customer help. They can still be reached via 866-70-GIANT.
• Our basic DSL speed is moving again. Our east towns' now have basic DSL at 3 megabytes downstream. Our west towns' will be moving over the next few months.
• Just a reminder that our post office box is still the same, although the street address has changed. Please not the correct address and make the appropriate changes:

104 N. Main St.
PO Box 308
Haviland, KS 67059

• Thank you for your generous donation to the Haviland After Prom Party 2006. Your support is very much appreciated.

Feature of the Month!
"CALLER ID"

Sign up for **Caller ID** today!
For only $7.00 a month
you can know who's calling before
you answer the phone.