Editors: Elias Levy, aleph1@securityfocus.com
Iván Arce, ivan.arce@coresecurity.com

Voices, I Hear Voices

No, I'm not interested in developing a powerful brain. All I'm after is just a mediocre brain, something like the President of the American Telephone and Telegraph Company. —*Alan Turing*

Through pride we are ever deceiving ourselves. But deep down below the surface of the average conscience a still, small voice says to us, something is out of tune. —*Carl G. Jung*

In 1876 Alexander Graham Bell received US patent number 174,465 for his "improvement in telegraphy," triggering a revolutionary change in human communications and the emergence of a new industry with technology at its very foundation. Today, more than 130 years after the telephone's invention, we face the difficult task of reconciling the prodigal children of the two great men quoted above within the confines of our computer networks. The assignment is far from easy, considering that men from telephony and computing worlds have substantially different philosophies, idiosyncrasies, technologies, business models, entry barriers, and operational characteristics.

Iván Arce
Core Security Technologies

The clash between these two worldviews in the realm of computer networks already plagued with security and privacy concerns is a fertile ground for both offensive and defensive information security practitioners. In this installment of Attack Trends, I delve into the new security and privacy challenges the ongoing widespread adoption of IP telephony and voice over IP (VoIP) pose.

Phreaky styley

Arguably, many of today's information technologies, defensive security mechanisms, and attack patterns came from organizations and individuals with deep roots in the telecommunications world of the 1970s and '80s. The information security folklore is filled with stories, anecdotes, and facts that link known personalities with security and privacy improvements and setbacks in the telephony industry.

In 1971, for example, Steve Wozniak (www.woz.org/letters/general/03.html) and Steve Jobs jerry-rigged an ingenuous device called the "Blue Box," which gave its users control of long-distance trunks on the public switched telephony network (PSTN) by manipulating the session teardown, call routing, and session establishment protocols (http://en.wikipedia.org/wiki/Blue_box). The Blue Box proved to be a useful tool for exploring a PSTN's obscure and proprietary corners and making prank calls or engaging in phone fraud in the form of "free" long-distance calls. It also demonstrated the commercial viability of new types of electronic consumer products: Wozniak and Jobs went on to found Apple Computer in 1976.

In his account of the Blue Box story, Wozniak cites an inspiring and supposedly fictional article featuring Joe Engressia and John Draper that appeared in *Esquire* in 1971 (www.webcrunchers.com/crunch/esq-art.html). Draper was called "Captain Crunch" because of his most valuable tool: a toy whistle included in Captain Crunch cereal boxes that produced the exact signal—an audible tone with a 2,600-Hz frequency—required to disrupt telephone signaling systems and take control of the telephony trunk. Calling a random phone number and blowing the whistle at any point during the call would grant trunk control to the caller and open up the PSTN's front gate.

The practice of exploring, experimenting, and exploiting PSTN and telephone equipment vulnerabilities came to be called *phreaking*, and phreakers soon learned that messing around with a telephone company's assets didn't necessarily lead to success stories or happy endings. Draper was arrested on charges of toll fraud in 1972 and sentenced to five years' probation; later, in 1977, he was arrested again and convicted of wire fraud. He made better use of his idle time by writing EasyWriter, one of the earliest word processor programs for Apple and IBM PC computers. In the years to come, many other phreakers and hackers would follow similar paths.

In the 1980s, the advent of PCs and the general availability of relatively low-cost modems popularized by bulletin board systems (BBS) helped a new generation of computer users explore the confines of both their own computers and the vast technological world that lay at the end of the phone line. Telephony companies worldwide operated business-oriented data networks on the physical circuits of their PSTNs

using the ITU-T X.25 protocol suite for wide area networks (WANs) over phone lines (http://en.wikipedia.org/wiki/X.25). Interconnectivity, open protocols, and free access to data networks belonged to "toy networks" such as the Internet, not the serious business-oriented infrastructures of X.25 networks.

In this context, several publications, such as *Phrack* (www.phrack.org) and *2600 The Hacker Quarterly* (www.2600.org), and organizations such as the German Chaos Computer Club (www.ccc.de) and the Dutch Hack-Tic Group (www.hacktic.nl), emerged as the telltale signs of a subculture linked together via a string of BBSs, informal technical publications, prototypical chat systems, and social gatherings. The line separating harmless and legitimate activity from harmful and illegal deeds rapidly blurred and soon confronted the apparent lack of legal, regulatory, and technical preparedness to address security and privacy concerns. Science-fiction author Bruce Sterling's novel epitomizes the dazzled and confused times of this new subculture and its clash with law and order ("The Hacker Crackdown: Law and Disorder in the Electronic Frontier" is available online at http://gopher.well.sf.ca.us:70/0/Publications/authors/Sterling/hc).

Meanwhile, the Internet and IP protocol suite marched on to become the de facto standard for interconnecting research and academic organizations, building local area networks (LANs), and reaching out to the users who would transform it into a global nerve system for business and leisure. With it came a new crop of security and privacy problems: Web site defacements, data privacy breaches, distributed denial-of-service attacks, proliferation of computer worms and other malware, and spam.

The convergence of voice and data communications over IP-based networks is developing steadily despite the iterative cycle of praise and dismissal that has raged since the mid 1990s. As the process unfolds, it's increasingly obvious that security and privacy concerns, attackers, and attack patterns have carried over from both the telephony and computer network worlds.

Like Ma Bell, I've got the ill communications

A cursory review of the foundations of PSTNs and IP-based networks reveals two opposing views on how to use technology for voice and data communications. The telephony networks were built on the assumption of complete ownership of almost all communications. A handful of providers deployed and ran communications over physical links and tightly controlled international standards and proprietary protocols. Most important, these providers maintained closed networks whose operational characteristics couldn't be tampered with because users were physically isolated from the systems that controlled them.

The Blue Box story is a particular example of how the discovery and exploitation of design weaknesses in signaling systems invalidate the isolation assumption and expose entire telephony networks to the whim of technically savvy users. The Blue-Boxing phreaker exploited the fact that telephony trunks were operated via in-band signaling, a system in which network command and control and user data is sent over the same medium. Abuse of in-band signaling prompted the move to out-of-band signaling systems such as the Common Channel Interoffice Signaling (CCIS, or Signaling System 7 as it came to be known internationally [http://en.wikipedia.org/wiki/Signalling_System_7]), which is an effective countermeasure for separating signaling and voice circuits. Nonetheless, Micah Sheer, Eric Cronin, Sandy Clark, and Matt Blaze showed—more than a decade later—that in-band signaling vulnerabilities remain a valid security and privacy concern today.[1]

The use of computers and terminals to manage and operate telephony equipment and networks weakened another major premise—that PSTNs were closed networks. This proved to be invalid when the equipment became remotely accessi-

ble via modems attached to regular, although unlisted, phone lines. The practice of systematically calling a set of phone numbers in search of an auto-answering modem attached to a computer system became a popular hobby for home computer users. *War Games*, a popular 1983 film, exposed this hacker "folklore" and introduced the term *war dialing* (www.imdb.com/title/tt0086567). The process was later automated with the development of ad hoc programs such as ToneLoc (www.textfiles.com/hacking/tl-user.txt), a functional predecessor to early TCP port-scanning tools such as Strobe (http://ftp.cerias.purdue.edu/pub/tools/unix/scanners/strobe/).

The use of the Private Branch Exchange (PBX) by government agencies and research, education, and businesses organizations implied the deployment of telephony equipment, owned and operated by PSTN customers, once again breaking the closed-network assumption and casting some light on the software and hardware used in telephony equipment. Further addition of IP-capable interfaces for management of PBX and central office switching equipment paved a road that would eventually lead to the IP protocol suite's adoption for the only component of the telecommunications infrastructure that remained isolated from data networks: voice transmissions.

Although the original PSTNs relied on a set of assumptions that defined a specific threat model, IP-based networks suffered from security and privacy issues that derived from their own set of assumptions. The adoption of open protocols helped make interoperation possible with many implementations that were running on low-cost hardware and rapidly evolving software. Communications over a shared medium with no single entity enforcing standards, regulating use, or policing abuse yields, at least initially, a substantially different threat model. At the heart of the IP protocol suite is an almost total disregard for security and an explicitly stated spirit of openness to foster interoperation among cooperative parties, which elicits a constantly changing threat model due to the rapid development and adoption of new protocols, technologies, and applications. On the other hand, the technological foundations of traditional telephony networks indicate a conscious attempt to maintain control of all the variables in an almost unchanged and unchangeable threat model, demanding security by obscurity and slower adoption and deployment of new technologies and innovative business models.

These two conflicting visions were on a collision course 20 years ago, and the possible outcomes of the impending crash are increasingly evident today in both the corporate network and consumer market realms.

I sit around and watch the phone, but no one is calling

As IP telephony and VoIP become integral parts of modern enterprise networks, security and privacy concerns are on the rise. On the security front, several groups have pointed out several design and implementation flaws in VoIP's building blocks and in its relatively new protocols, such as the H.323 protocol suite (www.packetizer.com/voip/h323/standards.html), the Session Initiation Protocol (SIP, www.ietf.org/rfc/rfc3261.txt), Real-time Transport Protocol and Real-time Transport Control Protocol (RTP and RTCP, www.ietf.org/rfc/rfc3550.txt), and the Media Gateway Control Protocol (MGCP, www.ietf.org/rfc/rfc3435.txt).

In February 2003, the Oulu University Secure Programming Group (OUSPG) found an "alarming failure rate" when it performed security testing of various SIP implementations (www.cert.org/advisories/CA-2003-06.html) with the PROTOS security testing framework (www.ee.oulu.fi/research/ouspg/protos/testing/c07/sip/). A year later, in April 2004, the UK National Infrastructure Security Coordination Centre (NISCC) worked jointly with OUSPG to uncover multiple vulnerabilities in implementations of the H.323 protocol suite that affect various vendors (www.cert.org/advisories/CA-2004-01.html). The Secure RTP specification of March 2004 (www.ietf.org/rfc/rfc3711.txt) seeks to address the lack of confidentiality, message authentication, and replay protection mechanisms in the original RTP and RTCP standards, a substantial privacy concern because these protocols are used for voice transmission over IP networks.

Protocol-level attacks are no longer theoretical possibilities, as Peter Thermos indicates in his detailed account of two plausible attack scenarios against VoIP (www.securityfocus.com/infocus/1862), but a more mundane type of security flaw plagues VoIP devices and software. Insecure default configurations and software riddled with buffer overflows and other trivial flaws characterize many VoIP devices being deployed in corporate networks as you read this article. Specific IP telephony and VoIP vulnerability metrics and statistics aren't compiled as a single class in the lists maintained by the Open Source Vulnerability Database (OSVDB; www.osvdb.org), MITRE (http://cve.mitre.org), SecurityFocus.com (www.securityfocus.com/vulnerabilities), or Secunia (www.secunia.com), but a quick search for vulnerabilities with the keywords "voip," "phone," and "SIP" reveals a mounting number of IP-telephony products with a growing history of security flaws.

Operator, number please

Although deployment of IP-telephony and VoIP systems on enterprise networks pose security and privacy challenges with no precise or

clear-cut solutions, the increasing adoption of VoIP in the consumer and small-enterprise markets doesn't appear free of problems either. Signaled by eBay's US$3,200 million acquisition of Luxembourg-based software developer Skype Group in 2005, the race to prevail in the VoIP communications market seems to be gaining speed when we look at initial public offering (IPO) tribulations of the US-based Internet telephony company Vonage Holdings (www.businessweek.com/technology/content/feb2006/tc20060209_519496.htm), the availability of instant messaging software with voice communications capabilities such as Google Talk (www.google.com/talk/), America Online's TotalTalk service (www.totaltalk.com), and the new VoIP service offerings from incumbent US phone companies such as AT&T-SBC, Qwest, and Verizon and cable-modem operators such as Cox Communications and Comcast.

I am calling long distance, don't worry 'bout the cost

In April 2006, Nicholas Fischbasch, senior manager of network engineering security at COLT Telecom, a European Internet service provider in 14 countries, described carrier VoIP security as both a present concern and a difficult-to-solve puzzle at the CanSecWest security conference in Vancouver, Canada (www.cansecwest.com/slides06/csw06-fischbach.pdf). A day later at the same venue, German researcher Hendrik Scholz provided the flip side of the coin with a presentation that gave a panoramic view of attack scenarios against VoIP networks (www.wormulon.net/files/pub/csw06-attacking-voip-networks.pdf).

The skeptics needed only to wait just over a month to read about a real-world example of VoIP-related attacks motivated by quick profits. On 8 June, 2006, *New York Times* reporters Ken Belson and Tom Zeller Jr. broke the story of a set of VoIP scams that were worth one million US dollars to Edwin Andrés Pena, a 23-year old Miami Fla., resident who was arrested a day earlier on fraud charges (www.nytimes.com/2006/06/08/technology/08voice.html?ex=1307419200&en=ae6b91a86dc4d7fa&ei=5088)

If phishing and spam are any indication of real and present threats for "traditional" IP networks and initial reports of use of these nefarious techniques over VoIP are confirmed (www.newscientist.com/article.ns?id=dn6445 and http://blogs.pcworld.com/staffblog/archives/001921.html), no further wakeup calls for information security practitioners should be necessary to address IP-telephony threats proactively. Several guidelines and resources are already available:

- In April 2006, the first IEEE workshop on VoIP management and security occurred in Vancouver, Canada, at the 10th IEEE Network Operations and Management Symposium (www.noms2006.org/content/workshop.html#voip). The initiative is promising and, hopefully, will continue to gather research, industry, and service provider experts from around the world.
- In January 2005, the US National Institute of Standards and Technology (NIST) published special report 800-53, "Security Considerations for Voice over IP Systems" (http://csrc.nist.gov/publications/nistpubs/800-58/SP800-58-final.pdf).
- The Voice over IP Security Alliance (VOIPSA, www.voipsa.org), an industry consortium of VoIP and information security vendors, runs a mailing list dedicated to VoIP security and provides several security resources.
- David Piscitello, ICANN Security and Stability Advisory Committee fellow and coauthor of "Understanding Voice over IP Security" (www.amazon.com/gp/product/1596930500/104-5238401-7578347) maintains a comprehensive IP telephony security site. An extensive and regularly updated set of resources is also available at http://hhi.corecom.com/voipsecurity.htm.

Our networks are converging rapidly to become a single medium for all communications. We're lured by the siren songs that praise countless benefits and new business opportunities, but if we don't seal our ears with wax and listen carefully, we'll not miss a voice saying that something is out of tune. It's in our hands to test the VoIP waters, hold steady at the helm of our networks, and pilot our way to tranquil shores where we can take advantage of this innovative communications technology without having to do it at the expense of our privacy and security. □

Reference

1. M. Sheer et al., "Signaling Vulnerabilities in Wiretapping Systems," *IEEE Security & Privacy*, vol. 3, no. 6, 2005, pp. 13–25.

Iván Arce *is chief technology officer and cofounder of Core Security Technologies, an information security company based in Boston. Previously, he worked as vice president of research and development for a computer telephony integration company and as information security consultant and software developer for various government agencies and financial and telecommunications companies. Contact him at ivan.arce@coresecurity.com.*

Feedback

Like what you just read? Hate it? If you'd like to share your opinions on this or any other material you've read in this issue of *IEEE S&P* magazine, please contact lead editor Kathy Clark-Fisher, kclark-fisher@computer.org. Be sure to include "Letter to the Editor" in your subject line.