Editors: Patrick McDaniel, mcdaniel@cse.psu.edu
Sean W. Smith, sws@cs.dartmouth.edu

Voice-over-IP Security

Research and Practice

Angelos D. Keromytis
Columbia University

Consumers and enterprises alike are rapidly adopting voice-over-IP (VoIP) technologies, which offer higher flexibility and more features than traditional telephony infrastructures. They can also potentially lower costs through equipment consolidation and, for the consumer market, new business models. However, VoIP systems also represent high complexity in terms of architecture, protocols, and implementation, with a corresponding increase in the potential for misuse.

VoIP Vulnerabilities

As part of the Vampire project (http://vampire.gforge.inria.fr/)—funded by the French National Research Agency (ANR) and tasked to better understand the VoIP security problem space—I conducted a survey of all published vulnerabilities in the Common Vulnerabilities and Exposures (CVE) database and in two IETF RFC Internet drafts. In total, these included 221 problems disclosed from 1999 through November 2009. These issues ranged from relatively straightforward problems that can lead to server or equipment crashes (denial of service [DoS]) to more serious problems that let adversaries eavesdrop on communications, remotely take over servers or handsets, impersonate users, avoid billing or charge another user (toll fraud), and so on.

Figure 1a breaks down the vulnerabilities by type, using the VoIP Security Alliance (VoIPSA) taxonomy.[1] Most problems lead to DoS attacks, typically via server or equipment crashes, although less obvious DoS attacks that users or administrators wouldn't notice immediately have also been reported. Note that our classification likely underestimates the number of more serious, remote-takeover vulnerabilities: many CVE entries report a DoS vulnerability, indicating that attackers could also conduct a buffer overflow attack, but don't follow up with a thorough analysis.

What the graph doesn't show is that VoIP servers and clients (end devices) each account for roughly half the DoS vulnerabilities. Although we theoretically know how to conduct fault tolerance for server applications, it's less clear how we can protect end devices; worse, updating VoIP equipment's firmware occurs rather infrequently outside enterprise environments.

Another interesting lesson from this graph and the supporting analysis[2,3] is that traffic eavesdropping and hijacking constitutes roughly one-fifth of these vulnerabilities; digging a little deeper, most of these problems enable traffic analysis via access to a user device or server's call logs but don't directly let attackers eavesdrop on voice conversations.

Figure 1b shows these vulnerabilities' sources. Given CVE's nature, it isn't very surprising that most of the problems stem from implementation issues. However, a sizable and arguably undercounted source of problems is misconfigurations; these include default administrator credentials, insecure and undocumented services running on the device (such as remotely accessible debuggers running on VoIP handsets, with no authentication!), and access to otherwise restricted services through alternative interfaces (for example, a Web front end). Finally, a very few protocol vulnerabilities allow DoS attacks[4] or toll fraud.[5] These problems were discovered (or, at least, reported) only recently, which is surprising given how long the standards documents have been published.

Research into VoIP Security

Considering VoIP's importance, the scope of such systems (which include and depend on whole families of protocols, including the Dynamic Host Configuration Protocol, Domain Name System, and Web services) and the breadth of vulnerabilities, considerable research exists in this space. In conjunction with my vulnerability analysis, I surveyed all research papers I could find on VoIP security.[6] I started with papers I was personally familiar with, then those published in the proceedings of top security conferences, workshops, and journals from the past five years, and the results from

searching CiteSeer, IEEE Xplore, Google Scholar, and the ACM Digital Library. I used obvious keywords such as "VoIP security" and "SIP security" and recursively followed relevant cited papers. I omitted some that were only peripherally relevant to VoIP or VoIP security. In the end, I looked at 200 papers, which I classified using an augmented VoIPSA taxonomy, given that more than half didn't naturally fit in the VoIPSA scheme.

Figure 2a shows how I classified these papers using the VoIPSA taxonomy. What we see is a breadth of research but also a lack of attention to some problem areas that appear to dominate the set of known vulnerabilities. Specifically, only 21 percent of the papers focused on the DoS problem, which corresponds to 58 percent of disclosed vulnerabilities. Conversely, a large focus (50 percent) is on VoIP spam, also known as spam over Internet telephony (SPIT); although 18 percent of vulnerabilities fit in the same category (social threats), few were actually related to SPIT.

Figure 2b shows the breakdown of the remaining papers. Approximately 40 percent are surveys and overviews of VoIP problems and security mechanisms. Some could in fact help against specific problems (such as DoS), although much of the effort in both intrusion detection and architectures is focused on SPIT detection and prevention.

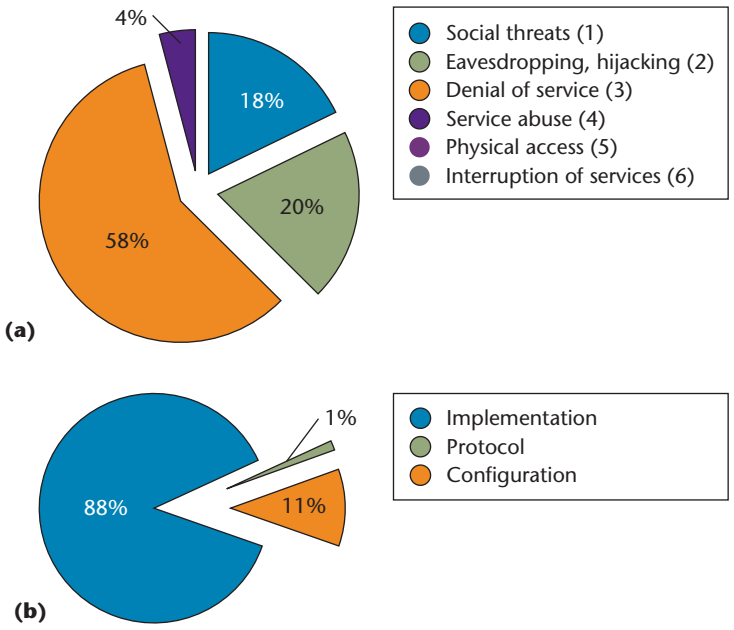

Figure 1. Vulnerabilities in voice over IP (VoIP). We can see (a) the vulnerability classification using the VoIP Security Alliance taxonomy and (b) the vulnerabilities' locations and causes.

The lesson to draw from the juxtaposition of these two surveys is that further research is needed into DoS attacks against VoIP systems. Furthermore, the research community and security professionals should better address configuration problems and emergent properties, especially those arising from unexpected interactions among different services, such as cross-site scripting attacks on Web management interfaces implemented by injecting code through the SIP `Caller` field.

One limitation of my work to date is that it represents a view that's potentially detached from what's actually happening on the Internet with respect to malicious activity and VoIP devices. Thus, some of the next steps in the Vampire project include designing, implementing, and deploying a distributed VoIP honeynet that will give us some insight as to the operational significance of different vulnerability types and the potential impact of various research thrusts. In the meantime, VoIP users and operators must remain vigilant and follow best practices, including the timely application of firmware and patch updates, the use of VoIP-aware firewalls and intrusion-detection systems, and the overall hardening of the critical services on which their VoIP infrastructures depend. □

Acknowledgments

The work described in this article was performed while the author was on sabbatical with Symantec Research Labs Europe.

References

1. "VoIP Security and Privacy Threat Taxonomy," VoIP Security Alliance, Oct. 2005; www.voipsa.org/Activities/VOIPSA_Threat_Taxonomy_0.1.pdf.
2. A.D. Keromytis, "A Look at VoIP Vulnerabilities," *login; The USENIX Magazine*, vol. 35, no. 1, 2010; www.usenix.org/publications/login/2010-02/pdfs/keromytis.pdf.
3. A.D. Keromytis, "Voice over IP: Risks, Threats and Vulnerabilities," *Proc. Cyber Infrastructure Protection (CIP) Conf.*, 2009; www.cs.columbia.edu/~angelos/Papers/2009/cip.pdf.
4. R. Sparks et al., *Addressing an Amplification Vulnerability in Session Initiation Protocol (SIP) Forking Proxies*, IETF RFC 5393, Dec. 2008; www.rfc-editor.org/rfc/rfc5393.txt.
5. R. State et al., "SIP Digest Authentication Relay Attack," IETF

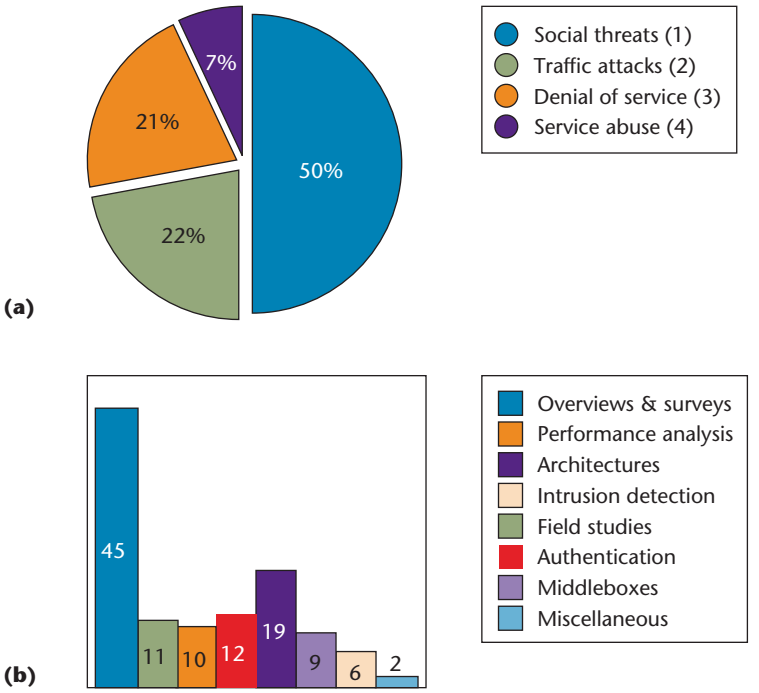

Figure 2. Voice-over-IP (VoIP) security papers. I classified (a) 43% of the 200 papers I surveyed using the VoIP Security Alliance taxonomy. I conducted an informal classification on (b) the remaining 57 percent of the papers (bars indicate the number of papers).

Internet draft, work in progress, Mar. 2009.

6. A.D. Keromytis, "A Comprehensive Survey of Voice over IP Security Research," *Security in Computing and Networking Systems: The State-of-the-Art*, W. McQuay and W.W. Smari, eds., to be published, Wiley & Sons, 2010.

Angelos D. Keromytis *is an associate professor with the Department of Computer Science at Columbia University, and director of the Network Security Lab. His research interests revolve around most aspects of security, with particular interest in systems and software security, cryptography, and access control. Keromytis has a PhD in computer science from the University of Pennsylvania. He's a senior member of the ACM and IEEE. Contact him at angelos@cs.columbia.edu.*