Voice over IP Security: Research and Practice

Angelos D. Keromytis[1]
Symantec Research Labs Europe *and* Columbia University
angelos@cs.columbia.edu

Voice over IP (VoIP) technologies are rapidly adopted by consumers and enterprises alike. They offer Higher flexibility and more features than traditional telephony infrastructures, as well as the potential for lower cost 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.

As part of the VAMPIRE project[2], funded by the French National Research Agency (ANR)

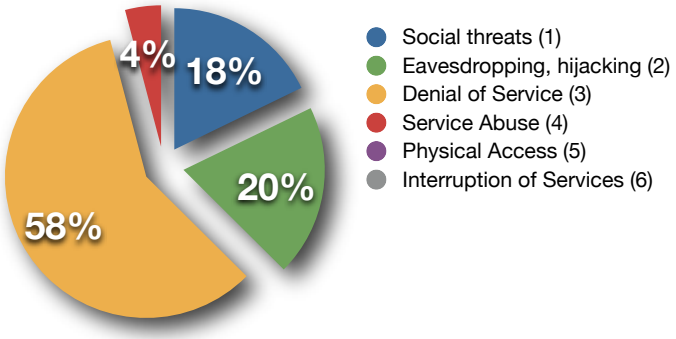

Figure 1: Vulnerability classification using the VoIPSA taxonomy

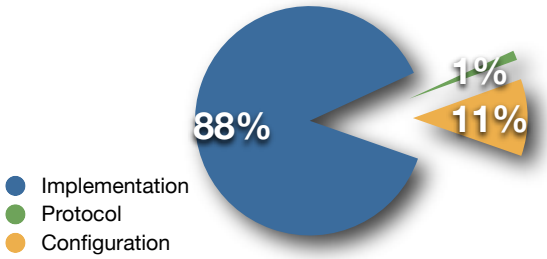

Figure 2: Vulnerability Location / Cause

and tasked to better understand the VoIP security problem space, we conducted a survey of all the published vulnerabilities in the Common Vulnerabilities and Exposures (CVE) database and in 2 IETF Request for Comments/Internet Drafts. In total, these included 211 problems that were disclosed from 1999 until November 2009. These issues ranged from relatively straightforward problems that can lead to server or equipment crash (denial of service) to more serious problems that allow adversaries to eavesdrop on communications, remotely take over servers or handsets, impersonate users, avoid billing or charge another user (toll fraud), *etc.*

Figure 1 shows a breakdown of the vulnerabilities by type, using the VoIP Security Alliance (VoIPSA) taxonomy [1]. The majority of problems lead to denial of service (DoS) attacks, typically via server or equipment crash, although less obvious DoS attacks that would not be noticed immediately by the users or administrators have also been reported. We should also note that our classification likely underestimates the number of more serious, remote-takeover vulnerabilities: many of the CVE entries report a DoS vulnerability, indicating that it may be possible to also conduct a buffer overflow attack but not following up with a thorough analysis.

Not shown on this graph is the fact that VoIP servers and clients (end-devices) each account for approximately half of the DoS vulnerabilities. While we theoretically know how to do fault tolerance for server applications, it is less clear how end devices can be protected; worse, updating the firmware of VoIP equipment is rather infrequent outside of enterprise environments.

---

[1] The work described in this article was performed while the author was on sabbatical with Symantec.

[2] http://vampire.gforge.inria.fr/

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

Figure 2 shows the source of these vulnerabilities. Given the nature of CVE, it is perhaps not very surprising that the overwhelming majority of problems stems from implementation issues. A sizable and arguably under-counted 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 (*e.g.*, a web front-end). Finally, there exist a very small number of protocol vulnerabilities that allow DoS attacks [4] or toll fraud [5]. These problems were only discovered (or, at least, reported) recently, which is surprising given how long the standards documents have been published.

Considering the importance of VoIP, the scope of such systems (which include and depend on whole families of protocols, including DHCP, DNS, web services, *etc.*) and the breadth of

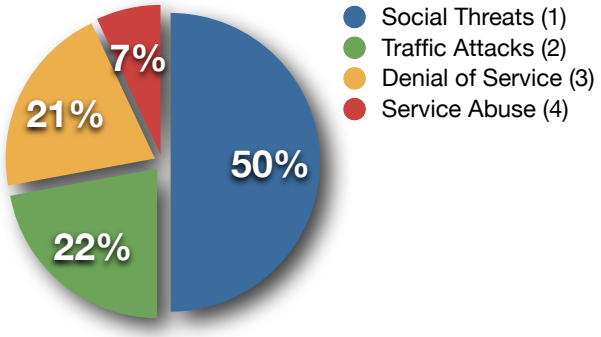

Figure 3: Paper classification using the VoIPSA taxonomy (43% of all papers)

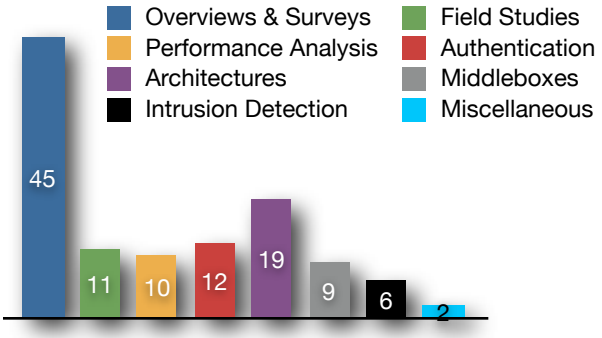

Figure 4: Informal classification of remaining (57%) papers (bars indicate number of papers)

vulnerabilities, there is considerable research in this space. In conjunction with our vulnerability analysis, we conducted a survey of all research papers that we could find on the subject of VoIP security [6]. We started from papers that we were personally familiar with, papers published in the proceedings of top security conferences, workshops and journals from the past 5 years, and the results from searching CiteSeer, IEEE Xplore, Google Scholar and the ACM Digital Library using obvious keywords such as “VoIP security” and “SIP security”, and recursively followed relevant cited papers. We omitted some papers that were of peripheral relevance to VoIP or VoIP security. In the end, we looked at 200 papers, which we classified using an augmented VoIPSA taxonomy, since more than half of them did not naturally fit in the VoIPSA scheme.

Figure 3 shows the classification of these papers using the VoIPSA taxonomy. What we see if the breadth of research, but also the lack of attention to some of the problem areas that appear to dominate the set of known vulnerabilities. Specifically, only 21% of the papers focused on the problem of denial of service, which corresponds to 58% of disclosed vulnerabilities. Conversely, there is a large focus (50%) on VoIP SPAM, also known as SPIT; although 18% of vulnerabilities fit in the same category (Social Threats), very few of them were actually related to SPIT.

Figure 4 shows the breakdown of the remaining papers. Approximately 40% are surveys and overviews of VoIP problems and security mechanisms. Some of the remaining work 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.

The lesson to draw from the juxtaposition of the two surveys is that further research is needed on the problem of denial of service attacks against VoIP systems. Furthermore, more attention is needed in addressing configuration problems and emergent properties, especially those arising from unexpected interactions of different services, *e.g.*, cross-site scripting attacks on the web management interface by injecting code through the SIP Caller field.

One limitation of our work to date is that it represents a view that is potentially detached from what is actually happening on the Internet with respect to malicious activity and VoIP devices. Thus, some of our next steps in the VAMPIRE project is to design, implement and deploy a distributed VoIP honeynet that will give us some insight as to the operational significance of the different vulnerability types and the potential impact of the various research thrusts. In the meantime, users and operators of VoIP services and devices 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 infrastructure depends.

Bibliography

[1] *"VoIP Security and Privacy Threat Taxonomy"*, VoIP Security Alliance, October 2005. Available at http://www.voipsa.org/Activities/VOIPSA_Threat_Taxonomy_0.1.pdf

[2] *"A Look at VoIP Vulnerabilities"*, Angelos D. Keromytis. In *USENIX ;login: Magazine*, vol. 35, no. 1, February 2010. Available at http://www.usenix.org/publications/login/2010-02/pdfs/keromytis.pdf

[3] *"Voice over IP: Risks, Threats and Vulnerabilities"*, Angelos D. Keromytis. In Proceedings (electronic) of the Cyber Infrastructure Protection (CIP) Conference. June 2009, New York, NY. *(Invited paper)* Available through the VAMPIRE project web site.

[4] *"Addressing an Amplification Vulnerability in Session Initiation Protocol (SIP) Forking Proxies"*, R. Sparks, S. Lawrence, A. Hawrylyshen, and B. Campen. RFC 5393, December 2008. Available at http://www.rfc-editor.org/rfc/rfc5393.txt

[5] *"SIP Digest Authentication Relay Attack"*, R. State, O. Festor, H. Abdelanur, V. Pascual, J. Kuthan, R. Coeffic, J. Janak, and J. Floroiu. Available as draft-state-sip-relay-attack-00, March 2009. Available through the VAMPIRE project web site.

[6] *"A Comprehensive Survey of Voice over IP Security Research"*, Angelos D. Keromytis. Chapter in *"Security in Computing and Networking Systems: The State-of-the-Art"*, W. McQuay and W. W. Smari (eds.), Wiley & Sons, 2010. Available through the VAMPIRE project web site.

Author Biography

Angelos D. Keromytis is an Associate Professor with the Department of Computer Science at Columbia University, and Director of the Network Security Lab. He is a Senior Member of the ACM and the IEEE. His research interests revolve around most aspects of security, with particular interest in systems and software security, cryptography, and access control. He received his M.Sc. and Ph.D. in Computer Science in 1997 and 2001 respectively from the University of Pennsylvania, and his B.Sc. from the University of Crete in 1996.