

Literature Review of Voice-over-IP Security Vulnerabilities

Abdulhai Naqvi, Dixit Paudel, and Mark Weber
The University of California, Davis
{abdulhainaqvi, meondav, marweber}@ucdavis.edu

February 19, 2018

1 Background

Migrating the telephone system away from a very centralized Public Switched Telephone Network (PSTN) system to a much more distributed Voice over IP (VoIP) system has a lot of benefits. These come from allowing developers the freedom of innovation and creativity to develop their own solutions. However, precisely because of this added freedom security becomes a problem. Malformed code and misconfiguration can become a huge issue and thus open up new security vulnerabilities [4]. It is worth noting that a staggering 88% of the security vulnerabilities arise from implementation details of VoIP [2].

In the traditional PSTN model the security vulnerabilities are strongly limited by physical resource access, but in the case of VoIP systems the weakest link can be present on any layer of the system: the transport protocols, the VoIP devices, the VoIP application, or even the operating system. The user thus has to rely on additional security measures such as encryption [4].

Additionally, attack techniques such as Denial of Service (DoS) suddenly become more relevant in a VoIP system because of the structure of the Internet Protocol. Places which allow cross communication between VoIP and PSTN systems will affect both the systems in ways not thought of before [4].

In a survey done on VoIP vulnerabilities [2], the three major security issues were : DoS attacks, man-in-the-middle-attack, social threats. However, the proportion of research papers to the importance of the issue (by occurrences) was not equal. For example, the DoS attack accounted for 58% of the issues, but only 21% of papers addressed the problem. Conversely, social threats such as Spam over Internet Telephony (SPIT) accounted for 18% of the issues, but only 50% of papers focused on this problem.

2 Related Work

Because no central authority controls the how VoIP is implemented vulnerabilities related to confidentiality, integrity, and availability (CIA) arise in all potentially all

protocol layers ranging from physical, internet, transport to application. [3].

SIP (Session Initiation Protocol) is the application layer protocol used in VoIP here at UC Davis for signaling calls. The SIP specification is devoid of any security mechanism, and instead suggests importing well-known method [1]. Thus, in the absence of such a mechanism, there are possibilities of attacks such as spoofing, session hijacking, privacy, and several others.

Even with security mechanisms in place, SIP based VoIP is vulnerable to DoS attacks. The flooding attack technique can be used to the various terminals in a VoIP network which includes the registrar server, the proxy server or the end-user terminal [1].

References

- [1] D. Geneiatakis, T. Dagiuklas, G. Kambourakis, C. Lambrinouidakis, S. Gritzalis, K. S. Ehlert, and D. Sisalem. Survey of security vulnerabilities in session initiation protocol. *IEEE Communications Surveys & Tutorials*, 8(3):68–81, 2006.
- [2] A. D. Keromytis. Voice-over-ip security: Research and practice. *IEEE Security & Privacy*, 8(2), 2010.
- [3] S. McGann and D. C. Sicker. An analysis of security threats and tools in sip-based voip systems. In *Second VoIP security workshop*, 2005.
- [4] D. C. Sicker and T. Lookabaugh. Voip security: Not an afterthought. *Queue*, 2(6):56–64, Sept. 2004.