Literature Review of Voice-over-IP Security Vulnerabiltiies

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

February 17, 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 innvoation 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 [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 this has to rely on additional security measures such an encryption [2].

Additionaly, 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 [2].

2 Related Work

As found by [1]...

References

[1] S. McGann and D. C. Sicker. An analysis of security threats and tools in sip-based voip systems. In *Second VoIP security workshop*, 2005.

[2] D. C. Sicker and T. Lookabaugh. Voip security: Not an afterthought. *Queue*, 2(6):56–64, Sept. 2004.