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 28, 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 [7]. It is worth noting that a staggering 88% of the security vulnerabilities arise from implementation details of VoIP [5].

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 [7].

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 [7].

In a survey done on VoIP vulnerabilities [5], 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 way VoIP is implemented, vulnerabilities related to confidentiality, integrity, and availability (CIA) arise in potentially all protocol layers ranging from physical, internet, transport to application. [6].

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 [3]. 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 [3]. SIP follows a 3-way handshake, so attackers can create spoofed IP addresses and request connections to the SIP server [8]. Since it is an invalid request, the search from the sever will fail. If an attacker repeats this procedure a lot within a small time frame, the servers will be drained up. While this research is interesting for the operators of the UC Davis network, our focus relies more on attacking the confidentiality and integrity of the network rather than the availability. Shihari et al. describe also methods for registration hijacking [8]. In our case, all clients get their certificates they use for registration offline. Therefore, this group of techniques will not work for us.

Vuong and Bai describe possible attacks on alternative protocols H.323, SIGTRAN and Megaco [9]. These attacks include spoofing, DoD and snooping, similar to the one described above, but are specific to the protocols. Since these are not used within the UC Davis campus network, we direct the reader to the original source for further details.

Keromytis explains several attacks against encrypted VoIP streams [**?**]. These include flow analysis, in which either certain bytes are added to the stream to follow it or certain parts are artificially delayed by a few milliseconds to de-anonymize communication partners. Another proposal is to use machine learning techniques to predict language from encrypted streams. Since these attacks are more advanced, they will become more interesting for us in a later stage of our project. Our focus lies on man-the-middle and privacy attacks on SIP.

Another important protocol that is often used to secure the VoIP stack is ZRTP [10]. ZRTP is a key exchange protocol that is used for end to end call security. ZRTP is based on the Diffie-Hellman key exchange [1]. The DH key exchange works based on the hardness of the discrete logarithms problem. It is the cornerstone of public key cryptography. However, by itself, the protocol provides neither forward secrecy nor authentication. This opens the door to Man in the middle (MITM) attacks, where an adversary could listen in on a conversation and save the parameters sent by one party and use them to obtain the secret key by posing as that party. ZRTP solves this problem by including a short authentication string (SAS) that is relayed to both parties, is the same and can be confirmed by both parties (presumably by voice in a VoIP call). The SAS value is a hash value based on both parties' DH parameters and a known nonce value. Perfect forward secrecy is ensured by using new keys for each separate session.

ZRTP is considered relatively safe against MITM attacks due to the SAS. However, the SAS needs to have a transfer mechanism such as a GUI display for both parties to see and agree on the SAS. However, not all VoIP phones necessarily have this capability. Gupta and Shmatikov [4] have demonstrated that a successful MITM attack can be carried out against ZRTP enabled VoIP clients. The attack relies on a shortcoming in the standard in the absence of an SAS.

Another attack described by Schurman et al. [2] descibes a mutually trusted party that goes rogue. Since this party's SIP address is not associated with its ZID (the identifier to store previous keys in cache), an attacker could substitute his own ZID instead of a legitimate participant and be an active MITM.

Despite the presence of MITM attacks on ZRTP, it is relatively safe when used as recommended. This is further shown by the number of applications employing ZRTP successfully in end to end communication and their relative foolproofness as analyzed by Schurman et al. [2].

References

[1] W. Diffie and M. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6):644–654, Nov 1976.

[2] S. et al. Wiretapping end-to-end encrypted voip calls: Real-world attacks on zrtp. *Proceedings of Privacy Enhancing Technologies*, 2017.

[3] D. Geneiatakis, T. Dagiuklas, G. Kambourakis, C. Lambrinoudakis, 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.

[4] Gupta and Shmatikov. Security analysis of voice-over-ip protocols. *Computer Security Foundations Symposium*, 2007.

[5] A. D. Keromytis. Voice-over-ip security: Research and practice. *IEEE Security & Privacy*, 8(2), 2010.

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

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

[8] V. Srihari, P. Kalpana, and R. Anitha. Security aspects of sip based voip networks: A survey. In *Second International Conference on Current Trends In Engineering and Technology - ICCTET 2014*, pages 143–150, July 2014.

[9] S. Vuong and Y. Bai. A survey of voip intrusions and intrusion detection systems. In *The 6th International Conference on Advanced Communication Technology, 2004.*, volume 1, pages 317–322, Feb 2004.

[10] J. Zimmerman and Callas. ZRTP: Media Path Key Agreement for Unicast Secure RTP. RFC 6189, 2011.