VoIP Shield: A Transparent Protection of Deployed VoIP Systems from SIP-based Exploits

Ryan Farley *Member, IEEE* and Xinyuan Wang *Member, IEEE*
Department of Computer Science
George Mason University
Fairfax, Virginia 22030
Email: {rfarley3, xwangc}@gmu.edu

***Abstract*—In this paper, we present a lightweight defense mechanism against VoIP attacks, called *VoIP Shield*, that can detect counterfeit or MITM modified messages as well as replay attacks without ever changing the underlying VoIP protocol. We then empirically tested our design in conjunction with deployed Vonage VoIP services against a large body of attacks including billing, call redirection, voice pharming, and complex MITM exploits. The results demonstrate that advanced VoIP protection is practical, lightweight, and can be deployed even in systems where software upgrades are impossible.**

***Index Terms*—VoIP; SIP; Billing; Call Redirection; Defense;**

I. Introduction

Our previous research [1], [2], [3], [4], [5], [6] on leading US residential VoIP services (e.g., Vonage and AT&T who have had 53.9% and 5.5% of US residential VoIP market share respectively [7]) has demonstrated that currently deployed VoIP systems are far from secure and trustworthy. Specifically, we have empirically demonstrated that a MITM (man-in-the-middle) could transparently redirect any VoIP calls from targeted Vonage and AT&T VoIP subscribers to any phone chosen by the attacker. For instance, this could route a call from Citibank customer service to a fraudulent representative even if the caller dials the authentic Citibank customer service number. Given this, even the most cautious customers could be tricked into giving out sensitive information (e.g., account info, credit card number, PIN). Furthermore, our research [4] has empirically shown that a remote attacker who is thousands of miles away from the attack target could become the MITM even if he was not initially in the path of the victim's VoIP traffic. Therefore, the identified security vulnerabilities in currently deployed VoIP services are much more realistic than people previously thought in general.

One major challenge for current VoIP systems to face in defending against identified exploits is the difficulty to update underlying VoIP protocols used by the currently deployed VoIP providers. Not only does it takes years to standardize any VoIP protocol, but also the vendors are reluctant to upgrade. Therefore, it is desirable to have mitigation that does not require any changes to the existing protocols.

With such goals in mind, we present a practical VoIP attack mitigation system, called *VoIP Shield*, that can transparently protect currently deployed, vulnerable VoIP systems from almost all exploits we have identified without any changes on the protected VoIP systems. Essentially the VoIP shield is a thin proxy that transparently adds the missing security protection to VoIP traffic between the protected VoIP client and server. We have empirically validated the effectiveness of the VoIP shield with Vonage VoIP services and it can shield the vulnerable Vonage VoIP client from 22 otherwise working SIP-based exploits. In the remaining 23^{rd} case, DNS poisoning based, while the VoIP shield does not block the poisoning, it does prevent the SIP attack from being successful.

978-1-4673-0269-2/12/$31.00

II. Background

There is a significant body of pre-existing offensive and defensive SIP research. Geneiatakis et al. [8] examined several potential security problems in SIP and listed several potential threats (e.g., DoS attack) and their remedies. However, they did not consider any of the transparent call diversion attacks described in [3]. Cao and Malik [9] analyzed potential security threats to VoIP without empirical demonstration, and recommended the best practice.

This paper is the counterpart to a large body of offensive research previously conducted by our team. These attacks form the body of experiments we used to gauge the effectiveness of the VoIP shield. For instance, Zhang et al. [1] empirically demonstrated that users of currently deployed VoIP services are vulnerable to billing attacks, which incur overcharges to the victims on calls they have made. Wang et al. [3] systematically studied the trust of current SIP-based VoIP and demonstrated that a MITM can transparently redirect or divert any targeted Vonage and AT&T VoIP call to any VoIP device chosen by the attacker. Furthermore, Zhang et al. demonstrated that a remote attacker could launch all kinds of MITM based attacks on VoIP even if he is not initially in the path of the VoIP traffic. They also demonstrated [5] that a MITM or remote attacker could transparently: 1) hijack selected E911 calls and impersonate the Public Safety Answering Point (PSAP); 2) spoof the voicemail servers of both the callee and the caller of selected VoIP calls; and, 3) make spam calls to VoIP subscribers even if Do Not Disturb is enabled.

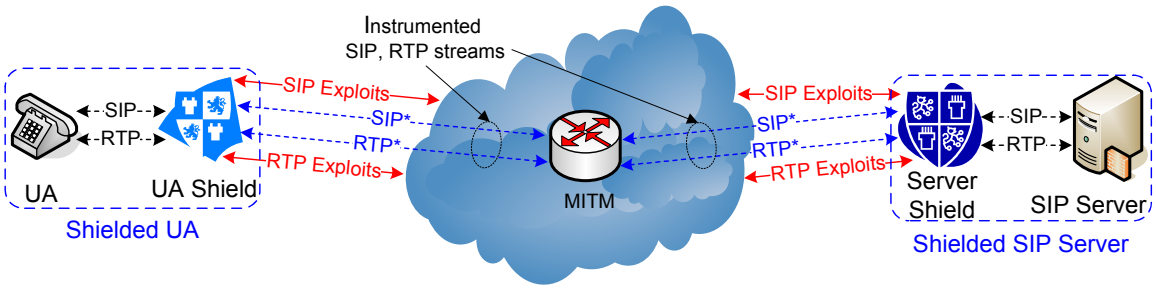

Fig. 1: The VoIP shield provides transparent protection against exploits between SIP user agents, even for existing implementations without modifications.

On the defense side, Arkko et al. [10] proposed a new way for negotiating the security mechanisms (e.g., IPSec [11] and TLS [12] HTTP authentication [13]) used between a SIP UA and its next-hop SIP entity. Reynolds and Goshal [14] proposed a multi-layered protection scheme against flooding DoS attacks on a VoIP network. The DoS detection method was based on measuring the difference between the number of attempted connection establishments and the number of completed handshakes. Wu et al. [15] proposed a stateful, cross protocol VoIP intrusion detection system, called SCIDIVE, to detect attacks on VoIP systems. Sengar et al. [16], [17] extended the cross protocol VoIP intrusion detection method by using Hellinger distance to detect flooding DoS attacks that may use a combination of SIP, RTP and IP streams. Specifically, the learning phase of their detection method trains with the normal traffic pattern and the detection phase uses the Hellinger distance to detect abnormal deviations from the normal behaviors. While existing VoIP defense mechanisms help to protect VoIP systems, none of them are able to detect or prevent the unauthorized call redirection attacks presented in work [3] which, as detailed later, our VoIP shield can.

Salsano et al. [18] evaluated the performance of SIP digest authentication and showed that implementing SIP digest authentication would incur significant processing overhead. McGann and Sicker [19] analyzed several VoIP security tools and showed that there is a large gap between known VoIP security vulnerabilities and the tool's detection capability.

III. VoIP SHIELD

The VoIP shield provides protection against malicious SIP packet manipulation between the end user and their proxy server. The VoIP shield is a lightweight SIP aware transparent gateway that augments the current SIP protocol and can be deployed on any existing VoIP network without changes to the user agent (UA) code.

The most basic structure of the VoIP shield consists of at least two shields with a pre-distributed shared key: one adjacent to the end user, called the phone shield, and another adjacent to the end user's proxy server, called the server shield, as in figure 1. A server shield is capable of pairing with many phone shields, but each phone shield can only pair with a single server shield. We use pre-shared keys so that no sophisticated key management or distribution system is needed. As detailed later, a cryptographic hash function uses the key to generate a message authentication code (MAC). Alternative methods, such as hash-based MAC (HMAC), could be substituted, but were not evaluated in our proof of concept in order to focus on functionality and performance. The MAC is appended to all SIP packets between the shields and allows each shield to authenticate the origin of the message and verify that the message is unaltered. If the MAC indicates a fake or altered packet, then it is dropped, otherwise the MAC is stripped off and the message is forwarded to the UA.

We implemented both the phone and server shields on dual homed FreeBSD transparent gateways by modifying packets as they traverse the packet filter, ipfw, using the divert sockets kernel module. A more transparent version could be made with an ethernet bridge, but we observed that divert sockets breaks ethernet bridge functionality when the packets are re-injected into the networking stack. An alternative would be bpf, FreeBSD's raw packet filter, or a custom kernel module. We may consider this in the future, but for now our version is functionally the same yet more platform agnostic, as divert sockets is supported on a variety of Unix platforms.

If arriving packets match a firewall rule specifying SIP traffic, then the kernel module writes them to a raw socket. Divert sockets stores the packet's arrival interface name within the unused socket data structure, `sin.sin_zero`. We use this metadata in userspace to determine if the packet is from the trusted (the shielded UA) or untrusted network.

The VoIP shield remains invisible to potential malicious agents while filtering all VoIP traffic. The ideal location for this is the UA's next hop, but it is also acceptable to locate the shield anywhere between the UA and its last trusted hop. For instance, if you only need to protect traffic while it is routed through an established untrusted network, then the shield may be installed at the UA's side of that network's edge.

Once the VoIP shield function receives the packet and its metadata (length, maximum length, shield mode, trusted origin flag) the code enters into a scope that has access to a packet modification and SIP parser library that we designed. The first step is to use the trusted origin flag to determine which direction the packet is headed.

If the message m is from the UA, then the shield will tag it with MAC a to make m', i.e. $m' = m + a$, and forward this along. MAC a is the SHA-1 hash H of the concatenation of message m and the pre-shared key k, i.e. $a = H(m + k)$.

For Vonage, replay prevention is accomplished though existing nonces that are SIP tags within m. We relied on this observation of the Vonage protocol to greatly simplify our

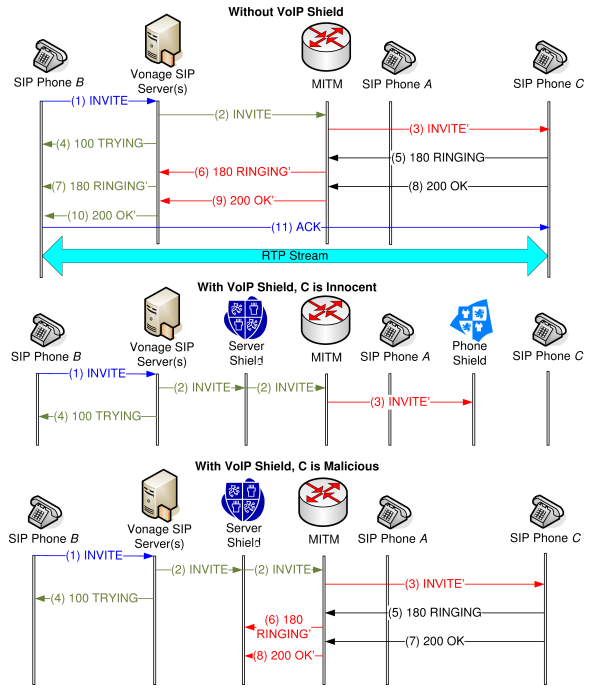

Fig. 2: Call Redirection attack. A's VoIP shield is omitted for space. C's VoIP shield does not have to be paired with the server shield shown. If C is innocent, then C's VoIP shield detects the fake Invite. If C is malicious, then the server shield detects the fake 180 Ringing and 200 OK packets.

design. For other service providers, the combination of the call ID and the call sequence number is sufficient.

Since the MAC is a known length and at a known location—the tail of m'—the program can easily extract the components. The program calculates the hash H of the concatenation of m and the pre-shared key k. If the hash does not equal a, then the packet is fraudulent and dropped.

Valid messages are parsed for call ID and call sequence number. The SIP call ID is an alphanumeric string and domain or IP address that uniquely identifies calls. The call sequence number is a monotonically increasing integer that allows a logical ordering of signals independent of arrival time for the session. This couplet roughly defines the current state of the call. The VoIP shield maintains a list of previously seen call IDs and their last known call sequence number. If a call ID has been previously seen and the call sequence is not greater than latest seen, then m is dropped.

We have observed that our Vonage UAC employed the same call ID and sequence number for Registration messages and a special exception exists for this case. Otherwise at this point in the program all invalid messages will have been dropped, and any valid m is forwarded to the shielded UA.

IV. Experiments

We have tested the VoIP shield in conjunction with deployed Vonage VoIP services against 23 previously developed VoIP attacks, listed in this section. The VoIP shield successfully defends against 22 and prevents advanced functionality of the 23^{rd} (Vonage DNS Hijacking [4]).

The experimental environment consisted of five virtual machines: a Windows installation with the Vonage softphone; a VoIP shield gateway; a second VoIP shield, the server shield, stationed at the network edge closest to the proxy server; a MITM; and, a remote attacker. The adversaries were on the network between the phone and server shields. The server shield had a secondary duty of protecting the commercial networks by blocking outgoing unethical packets.

For space we detail four attacks, each representative of a group within the total 23 attacks. The first, Fake Call [1], represents attacks which do not employ a MITM. Others in this group are Nuisance Call [2] and Caller Spoofing [1]. In Fake Call, the remote attacker rings a victim's SIP phone with spoofed caller ID information. When the victim answers, the attacker records the victim's audio stream. The VoIP shield protects against this attack because the attacker cannot create the necessary hash to append to the spoofed Invite packet. When A's shield sees the invalid hash, it knows that the packet is not from its proxy and drops the packet.

The second detailed attack is Extended Caller Side Callee Redirection [3], representing attacks where a MITM transparently forwards calls to an arbitrary third party. This also includes: Callee/Caller Side Callee Redirection [3], as with E911 [5]; Callee/Caller Side Voicemail Capture [5]; Voicemail Server Spoofing [5]; and, Voicemail PIN Capture [5].

Extended Caller Side Call Redirection highlights the VoIP shield's effectiveness against more complex attacks. Our experiment redirected outgoing calls for a telephone banking service. If redirected, the remote bot uses voice PIN code prompts we recorded from the same bank we pretend to be. The victim enters their PIN, the bot records this via the RTP stream, then gives a generic error to have the caller hang up.

Given the level of transparency with which a MITM would be capable of performing the redirection, this attack provides an excellent proof bed to show VoIP shield resiliency. As in figure 2 (except that C is malicious), the shield stops the attack on the first fraudulent packet without any assistance from the proxy server. Depending on T's implementation, the precise packet is either the fraudulent 180 Ringing or 200 OK. The packets' hashes indicate to A's VoIP shield that they were not calculated by A's proxy's shield, and therefore dropped.

Other MITM attacks protected as in the above groups are Realtime Caller ID Spoofing [2] and the billing attacks, which include: Invite Replay Billing [1]; Fake Busy Billing Callee/Caller [1]; Bye Delay Billing Callee/Caller [1]; and, Bye Drop Billing Callee/Caller [1]. Two somewhat related MITM attacks, Busy and Bye Termination [1], rely on DoS. For the billing and termination attacks, the VoIP shield drops all attack packets, but the attacker's goal of extending the billing period or DoS is still accomplished, due to uncontrollable issues inherent to network design related to packet loss, such as the two army problem. Similarly, while the Vonage DNS Hijacking [4] uses non-SIP signals and is undetectable by the shield, the attacker must then send SIP signals to initiate any advanced features. All these packets are detected as fraudulent and dropped, protecting the UA.

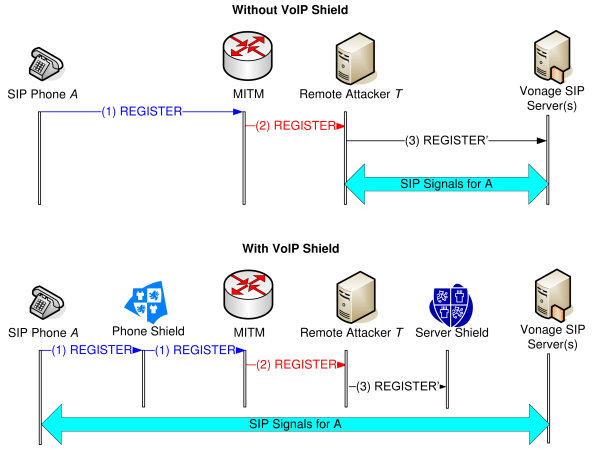

Fig. 3: Registration Hijacking attack. The server's VoIP shield detects the fake registration.

The third detailed attack, Registration Hijacking [2], demonstrates escalating any remote attacker into an MITM, as shown in figure 3. An existing MITM intercepts a Register and forwards it to the remote attacker, T. After changing the Register IP address and port number to reflect its information, T sends the modification to A's proxy, which subsequently sends A's signals to T. Taken further T can coordinate with A's MITM to establish itself as A's proxy and become a MITM. With a proxy shield, T's Register modifications are detected and the packet is dropped, preventing the hijack.

The fourth detailed attack is Remote Wiretap [4] and illustrates the VoIP shield's effectiveness against extraordinary attacker advantage. The MITM intercepts A's Invite to B. The MITM changes the SDP RTP IP address and port number to point to a remote attacker T, then forwards this modified Invite to B. B now believes that in order to talk with A it must send its RTP stream to T. B sends a 200 OK to A which is intercepted by the MITM. The MITM also changes this SDP RTP IP address and port number to point to T, and forwards this modified 200 OK to A. A now believes that in order to talk with B it must send its RTP stream to T. T can hear both sides, and as long as it forwards each side to the other A and B have no clue they are being eavesdropped on.

This is a different story with the shield enabled. If the MITM is adjacent to A, then the modified Invite will have an invalid hash when it arrives at A's proxy and will be dropped. If the MITM is adjacent to B, then the modified invite will have an invalid hash when it arrives at B and will be dropped. In both circumstances the attack is successfully detected and blocked.

V. Conclusion

People depend on credible voice communication for many critical and sensitive demands, such as emergency 911 and financial service calls. However, currently deployed VoIP services have serious security vulnerabilities that allow attackers to transparently spoof, hijack or redirect targeted VoIP calls. For instance, a victim could end up talking to a fraudulent customer representative collecting private data even if dialing the authentic number. These VoIP exploits could shake the long-held trust people have in voice communication.

As a mitigation of these attacks for currently deployed VoIP systems, we have designed the VoIP shield—a mechanism which does not require any changes to the underlying VoIP protocols and can be deployed even when software modification is not an option. We have empirically validated the VoIP shield with leading VoIP service provider implementations.

Our experimental results demonstrate that the VoIP shield defeats all 22 SIP-based exploits tested. While it does not block a 23^{rd} DNS-based attack, it does prevent the attack from achieving its SIP related goals. This practical, lightweight, and effective methodology provides a reasonable way to alleviate dependence on current and future producers of VoIP software which may be unable to maintain up-to-date security.

References

[1] R. Zhang, X. Wang, X. Yang, and X. Jiang, "Billing Attacks on SIP-Based VoIP Systems," in *the 1st USENIX Workshop On Offensive Technologies*, Aug. 2007.

[2] X. Wang, "Research Challenges in Securing VoIP," Tutorial in *the 14th ACM Conf. on Computer and Commun. Security*, Nov. 2007.

[3] X. Wang, R. Zhang, X. Yang, X. Jiang, and D. Wijesekera, "Voice Pharming Attack and the Trust of VoIP," in *Proc. of the 4th Intl. Conf. on Security and Privacy in Commun. Netw.*, Sept. 2008.

[4] R. Zhang, X. Wang, R. Farley, X. Yang, and X. Jiang, "On the Feasibility of Launching the Man-In-The-Middle Attacks on VoIP from Remote Attackers," in *Proc. of the 2009 Symp. on Information, Computer & Commun. Security*. ACM, March 2009, pp. 61–69.

[5] R. Zhang, X. Wang, R. Farley, X. Yang, and X. Jiang, "An Empirical Investigation into the Security of Phone Features in SIP-based VoIP Systems," in *Proc. of the 5th Information Security Practice and Experience Conf.*. Springer, April 2009, pp. 59–70.

[6] X. Wang and R. Zhang, "VoIP Security: Vulnerabilities, Exploits and Defenses," in *Advances in Computers*. Elsevier, 2010.

[7] ZDNet Research, "US VoIP Market Shares," Aug. 2006, http://blogs.zdnet.com/ITFacts/?p=11425.

[8] D. Geneiatakis, G. Kambourakis, T. Dagiuklas, C. Lambrinoudakis, and S. Gritzalis, "SIP Security Mechanisms: A State-of-the-art Review," in *Proc. of the 5th Intl. Netw. Conf.*, July 2005, pp. 147–155.

[9] F. Cao and S. Malik, "Vulnerability Analysis and Best Practices for Adopting IP Telephony in Critical Infrastructure Sectors," *IEEE Commun. Mag.*, vol. 44, no. 4, pp. 138–145, April 2006.

[10] J. Arkko, V. Torvinen, G. Camarillo, A. Niemi, and T. Haukka, "Security Mechanism Agreement for the SIP," *RFC 3329*, IETF, Jan. 2003.

[11] S. Kent and R. Atkinson, "Security Architecture for the Internet Protocol," *RFC 2401*, IETF, Nov. 1998.

[12] T. Dierks and C. Allen, "The TLS Protocol," *RFC 2246*, IETF, 1999.

[13] J. Franks, P. Hallam-Baker, J. Hostetler, S. Lawrence, P. Leach, A. Luotonen, and L. Stewart, "HTTP Authentication: Basic and Digest Access Authentication," *RFC 2617*, IETF, June 1999.

[14] B. Reynolds and D. Ghosal, "Secure IP Telephony Using Multi-layered Protection," in *Proc. of the 2003 Netw. and Distributed System Security Symp.*, Feb. 2003.

[15] Y.-S. Wu, S. Bagchi, S. Garg, N. Singh, and T. Tsai, "SCIDIVE: A Stateful and Cross Protocol Intrusion Detection Architecture for Voice-over-IP Environments," in *Proc. of the 2004 Intl. Conf. on Dependable Systems and Netw.*, July 2004, pp. 433–442.

[16] H. Sengar, D. Wijesekera, H. Wang, and S. Jajodia, "VoIP Intrusion Detection Through Interacting Protocol State Machines," in *Proc. of the 2006 Intl. Conf. on Dependable Systems and Netw.*, June 2006.

[17] H. Sengar, H. Wang, D. Wijesekera, and S. Jajodia, "Fast Detection of Denial of Service Attacks on IP Telephony," in *Proc. of the 14th IEEE Intl. Workshop on Quality of Service*, June 2006, pp. 199–208.

[18] S. Salsano, L. Veltri, and D. Papalilo, "SIP Security Issues: the SIP Authentication Procedure and its Processing Load," *IEEE Netw.*, vol. 16, no. 6, pp. 38–44, April 2002.

[19] S. McGann and D. C. Sicker, "An Analysis of Security Threats and Tools in SIP-Based VoIP Systems," in *The 2nd VoIP Security Workshop*, 2005.