Highly Effective Filtration and Prevention Framework for Secure Incoming VoIP Calls

Aws Naser Jaber[1], Supriyanto[1,2], Selvakumar Manickam[1] and Sureswaran Ramadass[1]

[1]*National Advanced IPv6 Center (NAv6), Universiti Sains Malaysia, Malaysia*
[2]*Universitas Sultan Ageng Tirtayasa (UNTIRTA), Indonesia*

aws@nav6.org, supriyanto@ft-untirta.ac.id,selva@nav6.org,sures@nav6.org

Abstract

In the past 10 years, numerous users have applied Voice over Internet Protocol (VoIP) with the rise of VoIP-oriented businesses. The system filters incoming calls through an intrusion detection system engine. If a call is accepted, the middle box signature inspection initiates a Session Initiation Protocol (SIP) proxy for the incoming call. A bridge is then used to send the call to the SIP server through a double virtual private network. If the call is rejected by the anomaly detection box, however, the box sends a report to the network administration and efficiently audits rejected calls. This paper examines the use of SIP as an integrated protocol for managing a specific multimedia service, including several aspects of configuration, coordination, and adaptation logic, to enable response with a session negotiation control of user sessions. The proposed innovation is a combined filtration and prevention security method, whose significance lies in its ability to execute object intrusion and encryption, as well as in the correspondence between the two methods without losing efficiency. The proposed framework focuses on DoS attacks, spoofing detection, and filtration. A new security model layer for SIP is also developed to supplement entire session initiations.

Keywords: *Snort, open SSL, VPN, OpenSIPS, Ourmon*

1. Introduction

Session Initiation Protocol (SIP) is a technology that reduces the cost of existing voice-based services and new multimedia services [1]. Many networks and service providers perceive SIP as a cost-cutting measure. Furthermore, the Voice over Internet Protocol (VoIP) infrastructure is an economic foundation on which new revenue-generating services are developed by providers [2]. The deployment of SIP technology is widely established as part of the competitive landscape shared among businesses. The successful achievement of this goal paves the way for enterprise goals.

Latently envisioned SIP services are called converged services, which effectively integrate the prominent features and functions of various existing services [3]. Some features are obtained from conventional voice-based telephony service and combined with the characteristics of data network services. For example, a user can access a click-to-dial service to control telephone calls, SMS, and call back via a web browser that runs on personal computer systems [4].

Converged services offer users integrated new media, such as multimedia conferencing [5], which enables users to communicate with one another through calls with effective exchange of audio and video information. The new versions of video phones are examples of such technologies.

Most cybercrimes today are directed toward mobility network servers that support SIP, public switched telephone networks (PSTNs), VoIP service providers, and the private branch exchange extensions in government offices and campuses. SIP can be used as an integrated protocol that manages a specific multimedia service, including several aspects of configuration, coordination, and adaptation logic, thereby enabling response with a session negotiation control of user sessions [6]. The various vulnerabilities inherited from IP affect consumer privacy, possibly resulting in system failures, also defined as system vulnerabilities [7].

SIP got six categories of responses process between their client s and server's which follows: **informational response** (1xx); **success**, in which information is already delivered and a request is successfully transmitted (2xx); **redirection**, in which a user can apply a proxy to search for an alternative service if an address has been permanently or temporarily moved (3xx); **client error**, wherein a request must proceed through a proxy (4xx); **server error**, which refer to server failures (5xx); and **global failure**, wherein a topical request cannot execute a response from a server (6xx) (Figure 1).

The SIP request also includes INVITE, which initiates a SIP session; ACK, which informs the recipient of a message; BYE, which terminates the session; and CANCEL, which cancels the session. The SIP server can act as a Registrar Server for services or user registration, or a Location Server that constantly monitors user locations [8]. SIP proxy servers can forward requests, such as forking and rewriting messages. The two types of SIP proxies are stateful proxies, which remember all requests, and stateless proxies, which forget requests after they have been forwarded [9].

Many SIP servers have built-in optional authentication procedures in software or hardware design. Nevertheless, activating or placing a security measure on standby depends on the user agent policy used. SIP can operate over different transport protocols, which are simultaneously reliable and unreliable. One of the reliable transport protocols is transport layer security (TLS) [10].

This paper aims to enable high security in VoIP servers and clients. We examine the capability of a framework to mitigate DoS attacks and the feasibility of VoIP detection of unusual activities from the traffic caused by attackers. Such a DoS attacks and eavesdropping are the major problems encountered by clients who depend on SIP for conventional telecommunications services.

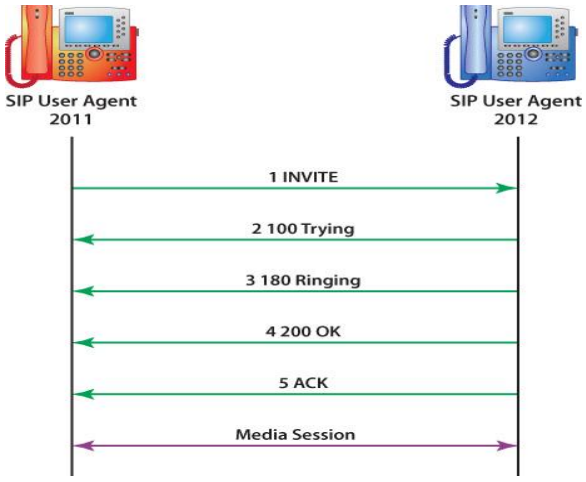

Figure 1. SIP Transaction: Request and Response

2. Related Works

For the literature review, we use the keywords “filtration” and “prevention” under VoIP services to identify related studies. One of the most comprehensive studies developed a prototype of a detection system for VoIP spam [11]. The system design is similar to packet filtering and email filtering system as viewed on Outlook Express.

Other researchers used a spam detection system [12], which is based on a multilayered fusion method for calls executed before a call session is established. A detection system based on VoIP Intrusion uses a state machine that is extended with input or output parameters, and has context variables, several predicates, and filtration operation [13].

An SIP intrusion system can prevent attacks, such as snooping [14], modification [15], spoofing [16], and DoS attacks [17]. Figure 2 shows the different methods of testing vulnerability to DoS attacks [18]. In an implemented fuzzer framework, two open-source SIP-based softphones are tested and their various security vulnerabilities are identified. The number of vulnerabilities identified shows that extensive security tests with additional scenarios and variations are required for softphone applications. Another work explored cross-infrastructure vulnerabilities that bridge VoIP and PSTN [19]. A general outline with high-level architecture was found for firewalls, including functionality and signaling trust management, encryption, authentication, and intrusion detection.

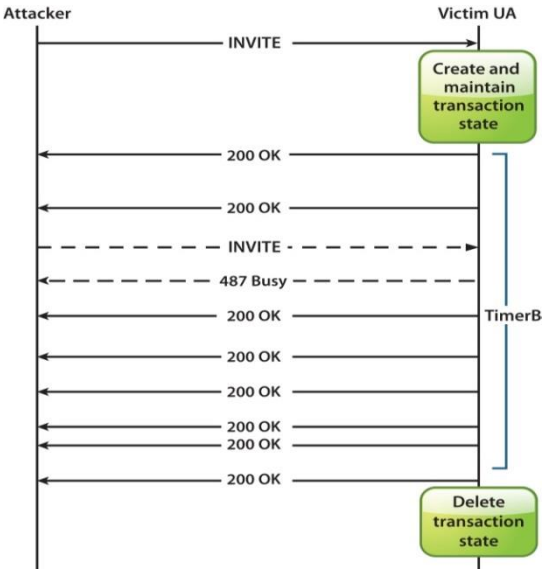

Figure 2. SIP DoS Attack Scenario

3. Proposed Framework

To explain the proposed scheme, we present a case in which an attacker can create a self-signature that initiates communication between an individual’s (“Bob”) softphone and a server (“Alice”); the self-signature is created using the TLS through an Open secure socket layer (OpenSSL) [20]. A virtual private network (VPN) [21] is provided to reduce VoIP traffic and send the filtered call from Bob to the required destination. The VPN secures incoming calls and isolates such calls from the outside world for secure transmission to Alice. Snort and OpenSSL integration are also considered. We use three PCs of high performance and a memory of up to 16 MB; several tests on DoS attacks are conducted using scanning tools for spoofing, in which penetration tools that accumulate on Backtrack are found [22].

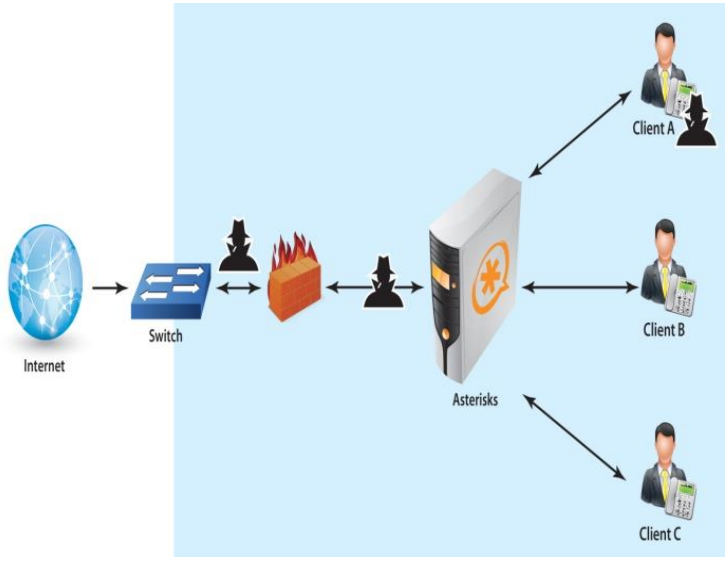

Figure 3. SIP User–Agent–Server (asterisks) attacked by Hacker

Figure 3 depicts a scenario wherein an external legitimate user and an attacker simultaneously act from outside the local network environment. The scenario attack proceeds as follows.

1. When Bob calls Alice, the entire SIP signal request from Bob is redirected to the SIP proxy server box in full design. The server acts as an intrusion box for Bob's SIP signal, which is forwarded to Alice; the server also determines whether the SIP signal originates from a legitimate user. If Bob is found in the proxy database, a second redirect to the proxy server that holds the certification magnet is executed. To detect network failure or attacks, separate Linux–Centos boxes [23] are used to capture anomalous calls and facilitate the creation of a network security solution. In addition, the system sends the blacklist packet to the anomaly box for verification, which is implemented using Ourmon, an open source technology for monitoring and anomaly detection [24].
2. After isolation and prevention are executed in the first level, the SIP invites Bob's call to the signature box, such as the OpenSIPS box with TLS privileges [25]. Thus, secure signaling is achieved, and certification between the client and the server is exchanged.
3. In the final stage, the filtered Call components aspects are securely forwarded to the VPN and Asterisk servers. Call quality is improved through the encapsulation of VoIP UDP packets, including SIP and RTP. The call is then established.

Figure 4 describes the proposed security scheme that uses different boxes, which also share the same operating system. Sequentially, each of the boxes understands one another under VoIP application; such understanding stems from the coding and configuration of the source code of SIP servers that are built by Centos and designed to be preventive by Linux.

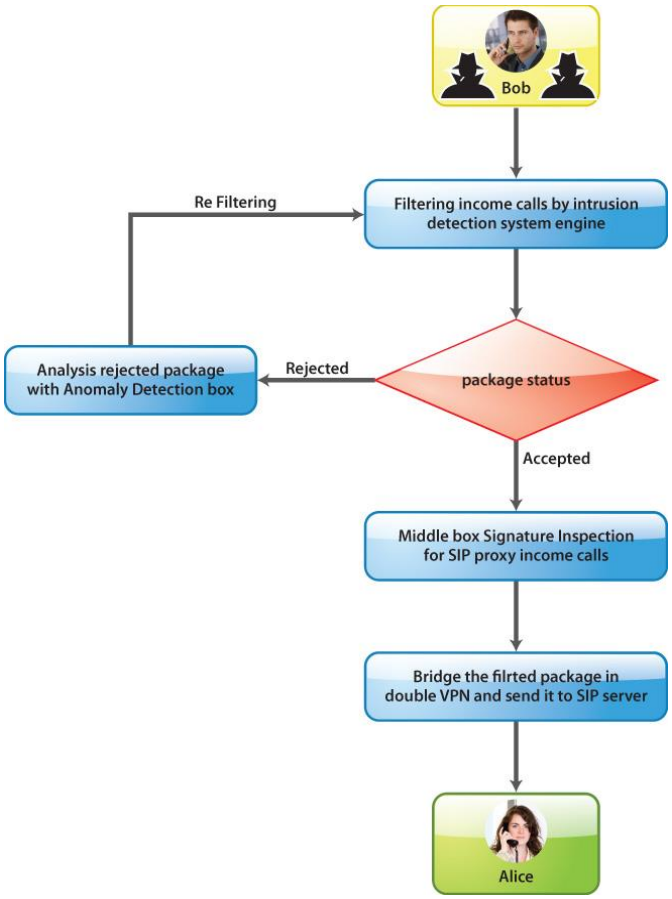

Figure 4. The SIP Proposed Scheme for Filtration and Detection

4. Framework Results and Discussion

Upon registration of the User–Agent–Client and the User SIP, the server is redirected and negotiation messages are transmitted for notification and referral to IP options [26]. SIP headers are used to identify other clients or SIP proxy directions (identified through Request-URI). The forwarding of SIP IP, prevention, isolation, and signal securing are input in the VPN. Thus, for each SIP-Proxy that begins from Proxy servers 1, 2, and 3, integration among them is implemented for the proxies to understand one another, thereby enabling signaling. Furthermore, the outcome from SIP Server-1 is excluded for major network security attacks (*e.g.*, DoS attacks, signaling spoofing). Meanwhile, SIP Server-2 must integrate the other SIP-Proxies to enhance signals, and SIP Server-3 must use a built-in RTP Proxy [27] to improve the quality of VoIP based on the VPN. A concession from this framework is the third-party box used for monitoring and anomaly detection. A Gray box is used to identify blocked malformed SIP messages caused by attackers; this box can also identify penetration features [28]. Table 1 summarizes the framework policy.

Table 1. Framework Policy

Proxy type	Purpose	Tool	Policy	Privilege
SIP redirect proxy-1	Detection and prevention	Snort	Snort VoIP rules	DoS attacks , signaling spoofing
Centos anomaly box	SIP auditing	Ourmon	Monitoring and anomaly detection	Gray box test
SIP redirect server-2	SIP signalling integration	OpenSSL	TLS - mutual authentication, session reuse	Signaling integrity
SIP register server-3	Enhancing call quality	VPN	Packet encapsulation	Voice quality

The proposed filtration and prevention module for securing incoming SIP calls requires additional time to establish a session. Table 2 shows that our proposed SIP security core needs three thresholds. The Receiver Operating Characteristics enable accurate analysis of signal detection theory. To verify the effectiveness of our scheme, we consider different durations for before the time of attack, during the attack, and detection and prevention of attacks.

Table 2. Results for false and true positives.

True positive	False positive	True positive rate
0.0000	0.0000	0.0000
0.0050	0.2301	0.0169
0.0100	0.3135	0.0430
0.0200	0.4168	0.0996
0.0300	0.4860	0.1545

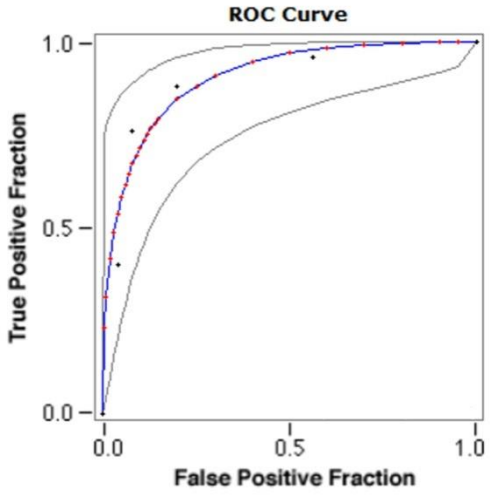

Figure 5. Randomly Selected Number for DoS and Eavesdropping Attacks

Confounding variables are found among different security aspects such Dos attack. Table 2 shows the variables that should be controlled by three major elements, namely, True Positive

(TP), False Positive (FP) for false alarms, and False Negative (FN) for missed alarms. The True Positive Rate (TPR) for the sensitivity alarm is defined as:

$$\text{TPR} = log\left(\frac{T\,P}{T\,P+F\,p}\right). \quad (1)$$

Predicting the duration of TP and FP generates important results for randomly selected attacks, and may be used to verify the extent to which the security core withstands DoS attacks and eavesdropping (Figure 5).

5. Conclusion

The discussion in the previous sections indicates that no limits are imposed on preventing VoIP attacks. The best way to detect these risks is to develop a framework that enables high filtration and prevention; these features are achievable through the integration of several methods. Naming authorities can be used to formulate an appropriate declaration solution mitigates the forged messages that ensures the prevention and filtration of VoIP attacks, in which anomaly codes are released to final destinations.

Our method enables the transmission of requests to the next SIP proxy server. A highly secure session policy is determined, constituting a more feasible solution for large companies that depend on VoIP calls and for campus infrastructure. The proposed framework aims to serve as a general guide that can be implemented and extended to include alternative steps such as session border. The other benefits of this framework are the implementation of an intrusion detection and prevention box. TLS for securing SIP identification is also implemented. TLS is suitable for implementation, and termination is sufficiently strong to enable added privacy. The VPN for SIP is currently being implemented and integrated to establish calls and multimedia services.

References

[1] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley and E. Schooler. "RFC 3261 SIP: Session initiation protocol", **(2002)**.
[2] P. Koutroumpis, "The economic impact of broadband on growth: a simultaneous approach", Telecommunications Policy, vol. 33, no. 9, **(2009)**, pp. 471-485.
[3] M. Adeyeye, N. Ventura and L. Foschini, "Converged multimedia services in emerging Web 2.0 session mobility scenarios", Wireless Networks, vol. 18, no. 2, **(2012)**, pp. 185-197.
[4] J. Rosenberg, J. Peterson, H. Schulzrinne and G. Camarillo, "Best current practices for third party call control (3pcc) in the session initiation protocol (SIP)", http://rfc. net/rfc3725. html, **(2004)**.
[5] W. Su, B. Cheng and J. Chen, "The design and implementation of sip control for Multimedia Conference system", pp. 223-226.
[6] M. A. Akbar and M. Farooq, "Application of evolutionary algorithms in detection of SIP based flooding attacks", pp. 1419-1426.
[7] R. K. C. Chang, "Defending against flooding-based distributed denial-of-service attacks: a tutorial", Communications Magazine, IEEE,vol. 40, no. 10, **(2002)**, pp. 42-51
[8] J. Rosenberg and H. Schulzrinne, "Session initiation protocol (SIP): locating SIP servers", **(2002)**.
[9] E. M. Nahum, J. Tracey and C. P. Wright, "Evaluating SIP server performance", pp. 349-350.
[10] J. Lennox, "Connection-Oriented Media Transport over the Transport Layer Security (TLS) Protocol in the Session Description Protocol (SDP)", **(2006)**.
[11] J. Nafe, B. Raybon and H. Nguyen, "Content Based SPAM Detection and Filtration Prototype for VoIP",
[12] H. Chen, F. Chen and S. Li, "A Multilayered Fusion Method for SPITs Detection", pp. 30-33.
[13] T. S. Chow, "Testing software design modeled by finite-state machines", IEEE Transactions on Software Engineering, vol.3, **(1978)**, pp. 178-187.
[14] Z. Bin, Y. Lu and C. ZhiChen, "A network intrusion detection system with the snooping agents", pp. V3-232-V3-236.

[15] A. Bremler-Barr, R. Halachmi-Bekel and J. Kangasharju, "Unregister Attacks in SIP", pp. 32-37.
[16] H. Sengar, "Overloading vulnerability of VoIP networks", pp. 419-428.
[17] T. Jin and C. Yu, "Quick Detection of Stealthy SIP Flooding Attacks in VoIP Networks", pp. 1-5.
[18] S. Taber, C. Schanes, C. Hlauschek, F. Fankhauser and T. Grechenig, "Automated Security Test Approach for SIP-based VoIP Softphones", pp. 114-119.
[19] H. Sengar, R. Dantu and D. Wijesekera, "Securing VoIP and PSTN from integrated signaling network vulnerabilities", pp. 1-7.
[20] J. Viega, M. Messier and P. Chandra, Network security with OpenSSL: O'Reilly Media, **(2002)**.
[21] V. Consortium, "VPN technologies: definitions and requirements", VPN Consortium, **(2006)**.
[22] S. Ali and H. Tedi, "Backtrack 4: Assuring security by penetration testing", Packt Pub Limited, **(2011)**.
[23] I. Voras, B. Mihaljevic, M. Orlic, M. Pletikosa, M. Zagar, T. Pavic, K. Zimmer, I. Cavrak, V. Paunovic and I. Bosnic, "Evaluating open-source cloud computing solutions", pp. 209-214.
[24] J. Binkley and B. Massey, "Ourmon and Network Monitoring Performance".
[25] F. Goncalves, "Building Telephony with OpenSIPS 1.6", Packt Publishing Ltd., Birmingham, United Kingdom, **(2010)**.
[26] R. J. Sparks, "The session initiation protocol (SIP) refer method", **(2003)**.
[27] P. Koski, J. Ylinen and P. Loula, "The SIP-based system used in connection with a firewall", pp. 203-203.
[28] C. Shepherd, C. Clegg and C. Stride, "Opening the black box: a multi-method analysis of an enterprise resource planning implementation", Journal of Information Technology, vol. 24, no. 1, **(2009)**, pp. 81-102.