International Journal
of Applied Information Technology
http://journals.telkomuniversity.ac.id/ijait/

A Security Analysis on OpenSIPS

Gandeva Bayu Satrya [a,*], Muhammad Caesara Nicovandia [b]

[a] *School of Applied Science, Telkom University, Indonesia.*
[b] *Project Management Officer, PT. Huawei Tech Investment, Indonesia.*
gbs@telkomuniversity.ac.id, m.nicovandia.ex@huawei.com

ARTICLE INFO

Received 27 January 2020
Revised 6 June 2020
Accepted 10 June 2020
Available online 30 June 2020

Keywords
VoIP, VPN gateway, TLS, attacks, OpenSIPS.

ABSTRACT

IP Telephony, Internet Telephony, Digital Phone or often also called VoIP (Voice Over Internet Protocol) is a technology that allows long-distance voice conversations with the Internet. The increasing number of VoIP users and other IP-based multimedia streaming services naturally raises security issues. Many users are likely to lose their privacy in communication. To overcome this security problem a security system must be implemented. Implementing a security system will use VPN Gateway using SSL and TLS encryption on the VoIP server. The VPN Gateway method is used to build a private network so that only certain users can use the private network. The TLS method is used to secure a user signaling session to the server. From the test results obtained that the VoIP server that uses VPN Gateway and TLS on the server can overcome the attacks e.g., eavesdropping, attacking authentication, teardown session, and denial of service.

Acknowledgment

This research was supported by School of Applied Science, Telkom University, and PT. Huawei Tech Investment Indonesia. The authors also wish to thank the person who does not want to be named for their technical support and provision in this research.

* Corresponding author at:
School of Applied Science, Telkom University,
Jl. Telekomunikasi No. 1, Terusan Buah Batu, Bandung, 40257
Indonesia.
E-mail address: gbs@telkomuniversity.ac.id

ORCID ID:
- First Author: 0000-0002-0243-9020
- Second Author: 0000-0002-5707-0427

https://doi.org/10.25124/ijait.v3i02.2503
Paper_reg_number IJAIT000030209 2020

1. Introduction

The development of technology has brought the communication business into a new era that offers the unification of all communications that are multimedia and sent via the internet. The next development of the Internet is the emergence of a concept known as Internet Telephony [1]. Internet Telephony or commonly known as Voice Over Internet Protocol (VoIP) can be interpreted as the ability to make telephone connections and all other capabilities performed by telephone networks and send faxes over IP-based networks with adequate service quality [1][2]. VoIP usually uses the Session Initiation Protocol (SIP) standard signaling protocol [3]. SIP is an application layer protocol used to make, modify, and end multimedia sessions or calls [4].

Of course, in the SIP server itself, there must be security threats that can make the SIP server's performance not as it should. The types of threats that occur in SIP are eavesdropping phone calls, attacking authentication, denial of service, and tear down sessions [4][5]. As is known during the signaling phase, several parameters are exchanged between users. Some parameters are very vulnerable, and confidentiality must be protected such as the user's location, username, and each user has his own identity.

Various types of threats to the SIP server, of course, must be taken seriously, so that all services from the SIP server run as it should. Based on the background above, this research will create a secured OpenSIP Server, where a security system will be embedded in this server to handle threats as mentioned previously using the Virtual Private Network (VPN) Gateway method with the Secure Socket Layer (SSL) encryption method, and OpenSIP Server with the Transport Layer Security (TLS) encryption method. The contributions of this research are as follows:

1. Implementing a VoIP server system by implementing VPN Gateway.
2. Developing OpenSIPS by implementing TLS.
3. Providing a recommendation for a secured infrastructure in the implementation of OpenSIPS.

The remaining sections are arranged as follows. Section 2 reviews OpenSIPS security issues and countermeasures. Section 3 describes our proposed infrastructure to improve the OpenSIPS security and compares it with a conventional strategy. Section 4 provides the implementation and analysis of this research. Finally, Section 5 highlights key take-away directive from this research.

2. Literature Review

Ganesan and Manikandan have proposed a two-tier model for the security, load mitigation, and distribution issues of the SIP server [6]. In the first tier, the proposed handler segregates and drops the malicious traffic. The second tier provides a uniform load of distribution, using the least session termination time (LSTT) algorithm. Besides, the mean session termination time is minimized by reducing the waiting time of the SIP messages. The efficiency of the LSTT algorithm is evaluated through the experimental testbed by considering with and without a handler. The experimental results establish that the proposed two-tier model improves throughput and CPU utilization.

Asgharian et al. have proposed a specification-based intrusion detection system by combining the SIP finite state machine and machine learning-based approaches [7]. They focused on SIP flooding attacks including denial of service and distributed denial of service attacks. After classifying various types of SIP attacks based on their sources, we extracted four specific feature sets to detect these

attacks. Each derived feature set is extracted from the specification of its attack group, and also, the normal behavior of the SIP state machine.

Segeč et al. used Public Key Infrastructure (PKI) for multimedia real-time communication (RTC) [8]. RTC is a type of communication service provided over IP, which introduced its specific security threats and security-related problems that may disturb an RTC communication environment. RTC communication consists of two parts i.e. signalization and multimedia data transfer. Within the signalization part, the SIP (Session Initialization Protocol) protocol became dominant. In the data transfer part, there is the RTP (Realtime Transport Protocol) protocol.

The deployment of Over-The-Top (OTT) Voice over IP (VoIP) applications has been accelerated after the adoption of high-speed communications technologies (e.g.: LTE) by mobile operators. Khoury et al. have minimized the termination call's cost by forwarding the CS calls to a VoIP system when the user is roaming outside the Home Public Land Mobile Network (HPLMN) [9]. They also proposed a method that secures a competitive edge for mobile operators over current OTT VoIP apps.

Yu have studied by capturing every incoming and outgoing SIP packet from the tcpdump data. In addition to the REGISTER flooding attack, we also identified the INVITE flooding attack [10]. Our major findings are (1) a REGISTER flooding rate of 200 msg/sec has the potential to deplete CPU resource and causes a Denial of Service (DoS) attack, and (2) an INVITE flooding rate with only 110 msg/sec could cause a DoS attack because of process stack overflow. He also has discussed different approaches to prevent DoS attacks against IP-PBX. The details of literature comparison can be seen in Table 1.

Table 1. Comparison with Relevant Studies

Authors	Focus	Drawback
[6]	Proposing a two-tier model for security, load mitigation, and distribution issues of the SIP server.	experimental testbed with and without a handler.
[7]	Proposing a specification-based intrusion detection system.	focused on SIP flooding attacks.
[8]	Proposing Public Key Infrastructure (PKI) for multimedia real-time communication (RTC).	RTC communication consists of two parts i.e. signalization and multimedia data transfer.
[9]	Deployment of Over-The-Top (OTT) Voice over IP (VoIP) applications.	global reachability only based on the E.164 standard.
[10]	Studying and capturing every incoming and outgoing SIP packet from the tcpdump data.	Preventing only the DoS attacks against IP-PBX.
Proposed	Improving VoIP security using VPN and TLS.	Using four common scenario attacks.

3. Proposed Architecture

The network to be implemented consists of 1 VoIP Server, 1 VPN Server, 2 routers, 1 switch, 2 PC-clients, and 1 PC that acts as an attacker in the laboratory environment. All clients and attackers are routed to VoIP Server. But only clients can use the VPN Gateway service. For more details, it can be seen in Figure 1. On the SIP server, the software used is OpenSIP 1.7-tls and on the VPN server using OpenVPN-2.2.0. The operating system used on the SIP server is Linux Fedora 10

and the operating system used on the VPN server is Linux OpenSuse. The tools that have been used for these scenarios e.g., Cain and Abel, Wireshark, SIP-Protos, and Inviteflood.

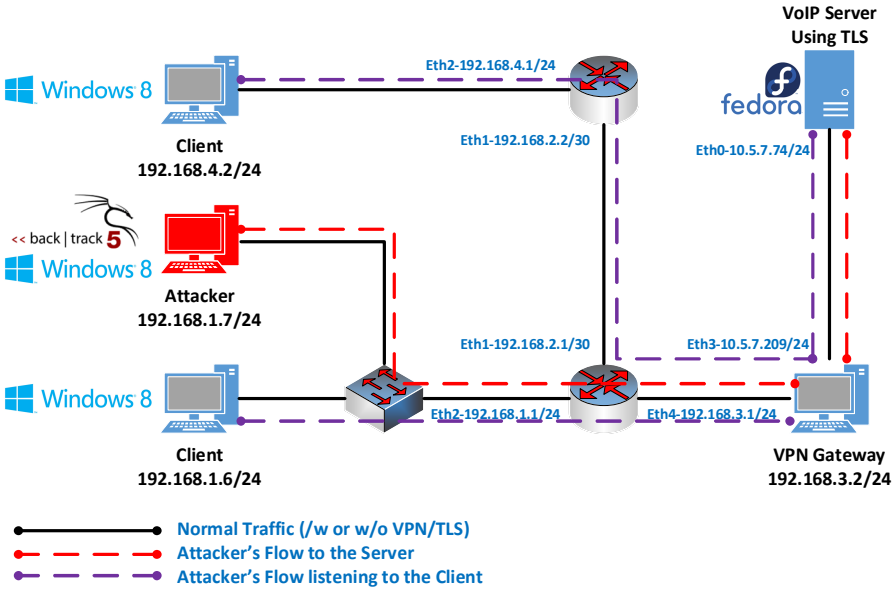

Figure 1 Design Network Architecture.

3.1. VPN in OpenSIPS

Virtual Private Network (VPN) is a popular technology among large organizations because it provides privacy in internal communication [6]. In principle, VPNs can be divided into 2 parts, they are trusted-based VPNs and secured-based VPNs. A trusted VPN is a virtual network that is built using a separate infrastructure from the internet network. In a secured VPN, VPN can be used on the internet, so it can send data across public networks. VPNs are also built on the network to secure certain communications from unwanted things on the network. In this research, a secure-based VPN using SSL will be used.

3.2. TLS in OpenSIPS

Transport Layer Security is a protocol that can be used by other protocols such as TCP to provide security for applications that are communicating on the network [13]. With TLS, all content of signaling information will be executed in the form of encrypted data. To form SIP communication using TLS in its signaling session, it requires the process of delivering the encryption key from the server to the client which is commonly called the TLS handshake.

3.3. Attacking models in OpenSIPS

Many threats commonly occur in VoIP services. Here are some common threats that occur in VoIP services.

3.3.1. Eavesdropping

In the case of the user sending a message using an encryption key that is recognized by the proxy. Although proxies can be trusted, attackers in these domains can decrypt encrypted text or even modify the encryption key. This can

be categorized as Man in the Middle Attack which changes the key characteristics according to the user's wishes.

3.3.2. Attacking Authentication

In this case, the attacker tries to break through the system authentication process by brute force password from a recognized user. If he is successful, he can conduct signaling sessions, communication sessions, and others. So, the system has been entered by individuals who are not recognized.

3.3.3. Teardown Session

After the dialog has been run, requests can be sent in a specific order to modify the status of the dialog or session. Using this attack method, the attacker can send a cancellation signal that can destroy the communication that is established between two clients.

3.3.4. Denial of Service (DoS)

This type of attack aims to use resources from network elements, usually by sending large numbers of packets to the target. Usually sends fake requests that include the sender's address to the target being attacked. Then requests are sent to many SIP elements. Eventually, the target will be met by responses from many SIP elements.

4. Implementation and Security Analysis

Security testing scenarios aim to evaluate the security system against threats or attacks. This research uses four attack scenarios from [11]. These scenarios will be explained in Table 2 below.

Table 2 Testing Scenarios

Type of Attacks	Codes	VPN	TLS
Eavesdropping (E)	E1	disable	disable
	E2	disable	enable
	E3	enable	disable
	E4	enable	enable
Attacking Authentication (AA)	AA1	disable	disable
	AA2	disable	enable
	AA3	enable	disable
	AA4	enable	enable
Teardown Session (TS)	TS1	disable	disable
	TS2	disable	enable
	TS3	enable	disable
	TS4	enable	enable
Denial of Service (DoS)	DoS1	disable	disable
	DoS2	disable	enable
	DoS3	enable	disable
	DoS4	enable	enable

4.1. Dealing with Eavesdropping

It can be seen in Figure 2 that the Cain and Abel tools are conducting an attack. Even though the attacker managed to get into the network, but the attacker still cannot retrieve data between client 1 and client 2, this is because the data

communication between clients is always through a VPN server. As previously known, all data that enters or exits the VPN Server is encrypted data and requires authentication to open it which the attacker certainly does not have. Then, the security certificate used for authentication differs between client 1 and client 2. That's what makes it difficult for an attacker to retrieve communication data.

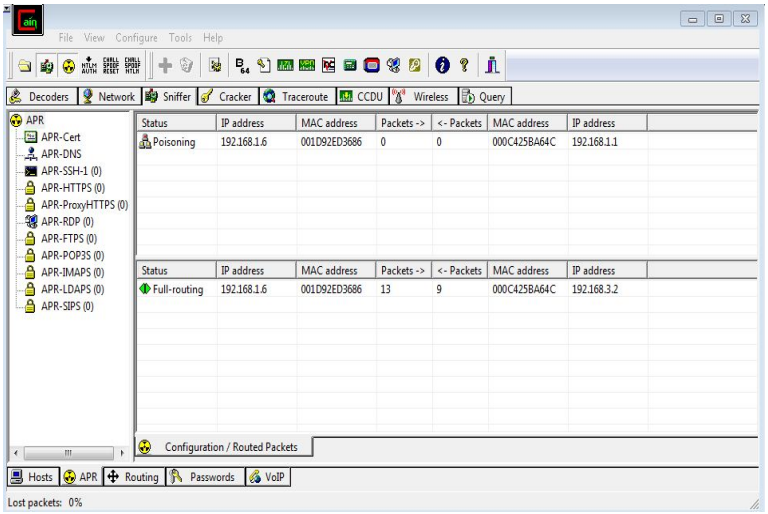

Figure 2 Attack OpenSIPS with VPN Enable, and TLS Enable.

4.2. Dealing with Attacking Authentication

Then the attack is carried out against OpenSIPS using VPN Gateway and TLS. The attacker will try to retrieve client data in the form of a username and password. It can be seen in Figure 3, that there is nothing that can be done by Cain and Abel. This is because Cain and Abel cannot enter the VPN Gateway network. After all, the network is specifically for clients who have security certificates and security keys. These certificates and security keys are not owned by the attacker.

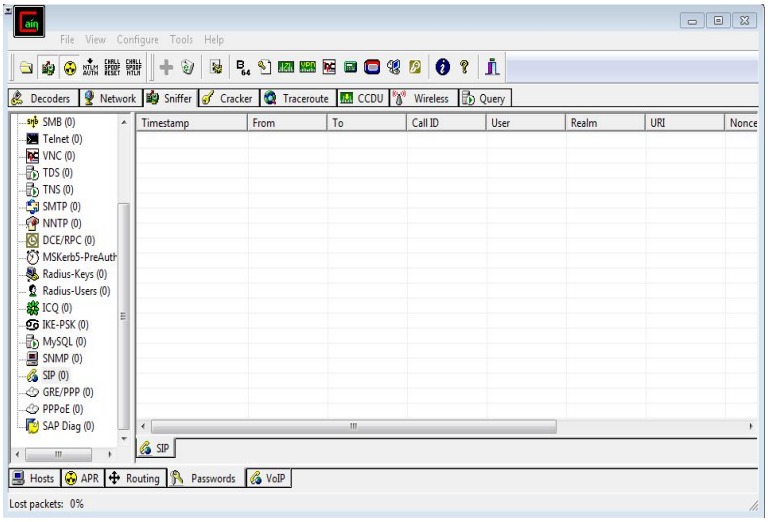

Figure 3 Attack OpenSIPS with VPN Enable, and TLS Enable.

4.3. Dealing with Teardown Session

The results of attacks carried out this time will not be much different from the results of previous attacks. That the attacker still cannot send the cancel signal

packet due to VPN Gateway encryption. This information can be seen in Figure 4 below, that the packet sent never arrives at its destination because it has a different network (VPN network). Not arriving at the package is indicated by the message "Network Unreachable".

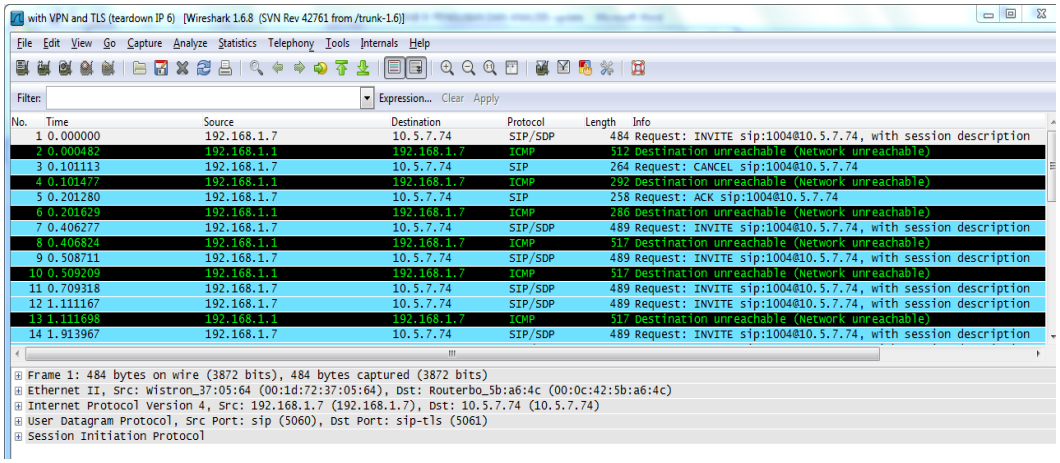

Figure 4 Attack OpenSIPS with VPN Enable, and TLS Enable.

4.4. Dealing with Denial of Service

The attack carried out by the attacker this time will also fail because the path used between the client and server is in the privacy path built by the VPN Gateway. Packets sent by the attacker will never reach the destination because different networks are marked with the message "Network Unreachable", therefore the client will remain safe in using existing services. Packets sent will be discarded on the network because it never reaches its intended destination. The proof can be seen from Figure 5.

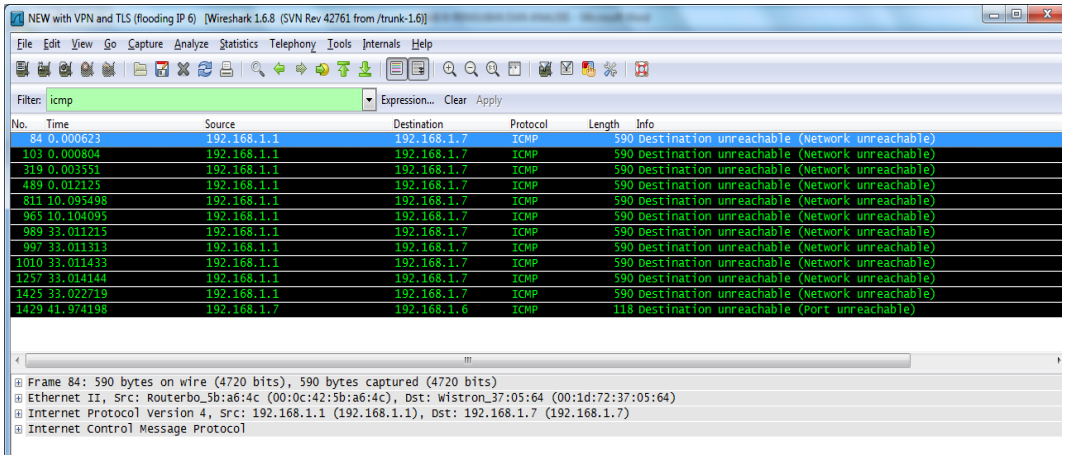

Figure 5 Attack OpenSIPS with VPN enable, and TLS enable.

4.5. Discussion

From Table 3 it can be seen that for unsuccessful *eavesdropping* attacks is for E3 and E4 scenarios. As for the *attacking authentication* attack that does not work are the AA2, AA3, and AA4 scenarios. For *teardown session* attacks that are not successful are TS2, TS3, and TS4 scenarios. Not much different from *denial of service* attacks, which did not work was the DoS2, DoS3, and DoS4 scenarios.

Table 3 The Results of Testing Scenarios

Type of Attacks	Codes	VPN	TLS	Hypothesis	Result
Eavesdropping (E)	E1	disable	disable	V	V
	E2	disable	enable	V	V
	E3	enable	disable	X	X
	E4	enable	enable	X	X
Attacking Authentication (AA)	AA1	disable	disable	V	V
	AA2	disable	enable	X	X
	AA3	enable	disable	X	X
	AA4	enable	enable	X	X
Teardown Session (TS)	TS1	disable	disable	V	V
	TS2	disable	enable	X	X
	TS3	enable	disable	X	X
	TS4	enable	enable	X	X
Denial of Service (DoS)	DoS1	disable	disable	V	V
	DoS2	disable	enable	X	X
	DoS3	enable	disable	X	X
	DoS4	enable	enable	X	X

5. Conclusions

This research successfully implemented the OpenSIPS infrastructure using VPN gateways and TLS. It has also been proven by four types of attack categories e.g., eavesdropping, attacking authentication, teardown session, and denial of service with disable or enable features for VPN gateways and TLS. This research proposal also recommends using a VPN gateway and TLS to provide the secured features of the four types of attacks. To neglect eavesdropping attacks other than using VPN Gateways, SRTP (Secure Real-time Transport Protocol) might be an option to use. For further research can add types of attacks i.e., registration hijacking, proxy impersonation, and message tampering.

Bibliography

[1] Goncalves, Flavio E., and Bogdan-Andrei Iancu. Building Telephony Systems with OpenSIPS. Packt Publishing Ltd, 2016.

[2] Aliwi, Hadeel Saleh Haj, and Putra Sumari. "A comparative study of VoIP protocols." *International Journal of Computer Science and Information Security* 11.4 (2013): 97.

[3] Agrawal, Hemant, Radhika R. Roy, and Vipin Palawat. "Method and apparatus for SIP/H. 323 interworking." U.S. Patent No. 9,420,009. 16 Aug. 2016.

[4] Gavilanez, Oscar, Franklin Gavilanez, and Glen Rodriguez. "Audit Analysis Models, Security Frameworks and Their Relevance for VoIP." arXiv preprint arXiv:1704.02440 (2017).

[5] Hasan, Muhammad Zulkifl, and Muhammad Zunnurain Hussain. "Collective Study On Security Threats In VOIP Networks." *International Journal of Scientific and Technology Research* 6.01 (2017).

[6] Ganesan, Vennila, and Manikandan MSK. "A Secured Load Mitigation and Distribution Scheme for Securing SIP Server." Security and Communication Networks 2017 (2017).

[7] Asgharian, Hassan, Ahmad Akbari, and Bijan Raahemi. "Detecting Flood-based Attacks against SIP Proxy Servers and Clients using Engineered Feature Sets." *International Journal of Information and Communication Technology Research* 8.1 (2016): 33-41.

[8] Segeč, P., et al. "Securing SIP infrastructures with PKI—The analysis." 2017 15th *International Conference on Emerging eLearning Technologies and Applications* (*ICETA*). IEEE, 2017.

[9] Khoury, David, et al. "Method for Securing and Terminating a CS Call over a VoIP System with Multi-Device Support." *2019 42nd International Conference on Telecommunications and Signal Processing* (*TSP*). IEEE, 2019.

[10] Yu, James. "An empirical study of denial of service (DoS) against VoIP." *2016 15th International Conference on Ubiquitous Computing* and *Communications and Symposium on Cyberspace and Security* (*IUCC*-CSS). IEEE, 2016.

[11] Naeem, Makhdoom Muhammad, Intesab Hussain, and Malik Muhammad Saad Missen. "A survey on registration hijacking attack consequences and protection for Session Initiation Protocol (SIP)." Computer Networks (2020): 107250.