A Study of SIP Trunk Security and Challenges

Aws Naser Jaber¹, Selvakumar Manickam², Profossor Surerswaran Ramdas³

National Advanced IPv6 Centre (NAv6)
6th Floor, School of Computer and Mathematical Sciences Building Universiti Sains Malaysia
11800 Penang, Malaysia.
{aws, selva, sures}@nav6.org

Abstract— Several voice over internet protocol (VoIP) providers migrate to their services to session initiation protocol (SIP). SIP is a lightweight signaling protocol used to implement in wiled VoIP services. However, with the global spread of this service, we can see how VoIP is affected by the stealing of SIP trunk services. Thus, the VoIP Trade Company will exhaust it effort and income. Our survey shows how much SIP security is enforced when somebody cracks the SIP server, and looks for any VoIP process trunk IP to use the server as a legitimate user, or to try to harm the trunk by injecting it with a forged source code that will lead to a road map for the hacker. The latter will make it deny the server, or inject it with the SQL script effect to come with DDos attacks. Our study shows the interest of researchers and students on VoIP security. It also provides a road map between the hypotheses and implementation, particularly on how SIP is affected by the variety of attacks from the outside world and from inside the local network.

Keywords- SIP trunk; SBC; VoIP firewalls; cryptographic algorithms.

I. INTRODUCTION

Session initiation protocol (SIP) Session initiation protocol (SIP) is classified as one of the most important voices over internet protocol (VoIP) signaling protocols[1]. SIP shows the calls where to send the signals for their requests. From the mid-90s, IETF engineering realized that the SIP is one of the important signaling protocols that can overcome the voice signaling servers.

SIP became more vital when internet telephony was developed, particularly because of the low cost of international calls. Furthermore, SIP was useful for mobility and multimedia. Recently, over 70% of all variety of sold PBXs used IP bases on SIP. When VoIP PBX enterprise was developed, the use of SIP trunk resulted in better cost and benefit ration on a large scale[2]. The survey presents a study of SIP trunking security issues, and particularly focuses on the SIP security development, which still has some security weakness. From the data that gathered, we concluded that hardware security tools are not enough to get the rest of the form of the attacker. A high deployment for open source must be conducted to build not only the VoIP application, but also to develop the most important diversity of encryption.

II. SIP PROCESS

SIP was developed based on RFC 3216[3]. The network element can also be reliable from the end point of SIP servers. RFC 3261 shows an example for SIP peer-to-peer for network elements. Further, SIP is based on SIP text messaging, which has a similar appearance as HTTP. The SIP has a user agent (UA) and a user agent server (UAS).

A user agent is not the end of unified communication, such as softphone and X-lite [4], or the hardware user agent. We have two different kinds of SIP message transactions, namely, request and respond. Request is described in RFC 3261 as below Register, which is used by UA to receive calls. INVITE is used for establishing the media sessions between clients and servers. ACK is used for confirming the exchange of messages. CANCEL is used to terminate the pending session. BYE is used when there is a live session, and it has to terminate this session within this request. For the response, the following is used. Provisional (1xx) is a request to receive the beginning process. Success (2xx) is used when the request is already received. Redirection (3xx) is used for more action to be done depending on the sender and receiver. Client Error (4xx) is used as a bad syntax when configured on the server. Server Error (5xx) referred to when the server is disconnected and not reachable for SIP request. Global Failure (6xx) is the request that cannot be entertained at any time by the server. In Fig1. It shows the SIP process. In addition, SIP depends on real-time transport protocol (RTP)[5] for voice transaction between clients Trunk process

SIP trunks generally have a transmission media that carry out all types of communication between homes and offices. Basically, it carries thousands of VoIP connection by multiplexing the packet though the optical fibers or satellite connections.

SIP trunk servers are the bases for bridging unified communication infrastructures based on IP PBX and different VoIP systems. These services provide the signal number office that all users can dial to make PSTN calls or mobile calls.

From another point of view, the cost can be free by joining SIP servers among different overseas locations with the IP trunk. An example is a video conference. In comparison with the legacy of the PBX, we can emphasize that it will be enough to reduce the cost. The Internet Engineering Task Force (IETF) can replace the two main RFCs, which are

RFC5947 and RFC 4904, where one is informal and the other is the proposed standard.

Figure 1. SIP transaction process

Figure 2. Trunk service process.

The RFC4904 of the proposal is described as the trunk group parameters for SIP and telephony uniform resource identifiers (URI). When the trunk is provided, it can better configure the sip server to force by using Digest Authentication. For the SIP server, the registration side, and request to invite must be available upon registration. The Trunk process can see in Fig 2. And in Fig 3, we can notice the client's usage and cost.

Figure 3. the Trunk clients usage [6]

A. Session border controller (SBC)

Is an essential tool for SIP trunk applications. In addition, it can provide high-security cover against many threats and attacks on both sides of the VoIP servers and their provider. In fact, SBC is feasible for IP address translation for different versions of VoIP servers. equally important, SBC can show the types of SIP attacks and what it offers Fig 4. It can generate reports to audit for the network system administrator.

The SIP Business-Trunking reference architecture is a five level hierarchical architecture divided into two domains. [7].

In fact, SBC has several benefit, for example, Billing, network topology hidings, quality of service (Qos) enforcement, NAT, H.323 and SIP interworking. Fig 4 describes SBC useful implementation.

Figure 4. benefits from implement Trunk series on SIP servers [8]

B. VoIP Software trunking support

Trunk has two main open source distributions that can offer SIP good trunking servers, namely, Asterisk and OpenSIPS.

Asterisk [9] is an open source for VoIP application issued by Digium. Asterisk acts as a register server with a state-full server support. That produces a free source code. Hence, this feature allows the client to modify and build his own dial plan policy. In fact, this server can save money and use open standards.

Furthermore, Asterisk hugely favors the VoIP application. Asterisk is used as specific configuration file for trunk. For instance, Zap Trunk, which provided the connection between old TDM systems[10], uses the analog lines (FXO) or Digitally interfaces (E1/T1) or IAX2-trunk specifically made for the Asterisk trunk. Within this trunk, each asterisk can talk to each other. The SIP trunk is a configuration file that can provide servers for Asterisk and other VoIPs.

For instance, OpenSIPS negotiate the sessions between the servers and use the Voice mail servers that come from VoIP servers back to the Asterisk. Finally, Asterisks can be more feasible for the software developer. Thus, the developer can make it his own custom trunk.[11].

When some VoIP servers do not support SIP, we need to make a custom trunk for other signaling protocols that are mainly used for video conferences, such as ISDN and H323. One of the major trunk attacks comes from misconfiguration. Misconfiguration means that the server configuration is still in default, and there has been no modification in the security policy of the Asterisk server. When clients install Asterisks, they can at the same time place the anti-attack filtering system and intrusion system.

Asterisks use a spastic configuration file for trunk, for example, Zap Trunk, which proved the straight connection between old TDM system that uses the analog lines (FXO) or digitally interfaces (E1/T1) or IAX2- Trunk, which is specific for asterisk trunk that each asterisk can talk to each other within this trunk.

SIP trunk- this configuration file can provide servers between Asterisk and Other VoIP servers, for example, OpenSIPS, to negations the session between then and use the Voice mail servers who come from VoIP servers to asterisk. Finally, Asterisks can be more feasible for the Developer software and make it his own custom Trunk, Asterisk as we know an open software, when some VoIP servers don't support SIP, we need to make a custom trunk for other signaling protocols such as ISDN and H323, which use mostly for Video conferences. In table 1. We can notice a trunk example from **Penang - Kuala Lumpur** Asterisk simple trunk configuration in **sip.conf** file (standers configuration without authentication). Table 2. Explain the trunk configuration with Authentication

TABLE I. TRUNK PATH FROM PENANG TO KL

Penang	Kuala Lumpur
[trunk-Penang- Kuala Lumpur] type=peer host=asterisk-Kuala Lumpur context=from-asterisk-Kuala Lumpur	[trunk- Kuala Lumpur - Penang] type=peer host=asterisk-Penang context=from-asterisk-Penang

TABLE II. TRUNK PATH PENANG- KL WITH AUTHENTICATION

Penang	Kuala Lumpur
[trunk-Penang- Kuala Lumpur] type=peer host=asterisk-Kuala Lumpur context=from-asterisk-Kuala Lumpur username=trunk-Kuala Lumpur - Penang secret=strong_password	[trunk- Kuala Lumpur - Penang] type=peer host=asterisk- Penang context=from-asterisk-Penang username=trunk-Penang-Kuala Lumpur secret=strong_password

III. SIP TRUNK THREAT

This threat refers to the brute force attack considered as a main VoIP attack to crack the SIP servers. One of the methods to get through VoIP system, the attacker may crack the SSH access through the brute force attack and be granted..

The privilege of becoming a legitimate user to exchange the SIP server resources. Thus, it may affect the SIP trunk provider. A good study that uses the encryption to protect VoIP servers against brute force attack is presented in. [12]. Another study shows the detection system against SIP-flooding attack that is caused by the brute force attack [13]–[14]. SIP security is enhanced against this attack through some modification of public key infrastructure[15].

A toll fraud through stealing the voice mail service was studied as well as the kinds of Dos attack. However, when the caller cannot get the recipient, the calls will be entered in a trunk-to-trunk shift. Then, call forwarding will start. Another example of the threat for SIP server hosting trunk servers is denial of services. [16] and Distributed denial of service attacks (DDos) [17].

For the DDos, “zombies” send a massive invitation traffic number through the UDP, thus downing the server. Apart from that activity, these attacks can send spam messages for the VoIP trunk provider. Another type of VoIP trunk attack is the physical trunk attack [18]. Physical attack can modify some portions of the SIP trunk servers who make the system more confusing for out bound calls. Meanwhile, Asterisks also suffer from brute force password guessing attacks.

Nevertheless, in the IAX2 configuration file, an option mentions on brute force attack enables “delay rejected.” This process means that if the clines and the server were under authentication levels, there would be a delay in the authentication time. Thus, the session will be rejected. However, most asterisk users forget about these open ports. Therefore, it may become a source code and be relied on by the attacker. Subsequently, the standard configuration will not work properly. In this case, we can also refer to these kinds of attacks as remount data tunneling. Furthermore, students study in more detail the Asterisks server support, their protocols, and their security [19].

IV. TRUNKS THROUGH SIP SERVER FIREWALL

A firewall guards against the different variety of attacks, especially those intrusions from outside networks to the private network. This firewall can be implemented on VoIP servers. The trunk can take over the back-to-back user agent server (B2bAs). It may be considered as a middle box acting as firewalls, especially when the two VoIP servers are overseas. One of the useful studies mentioned on the dynamic scale is for calls, especially when both servers use trunk servers to locate the middle box [20].

Firewalls, through the VoIP, can cause some delays. For instance, firewalls may be the main obstacles for the misunderstanding from the VoIP provider to the VoIP recipient. A study showed that the firewall encompassed private networks for the public access [21].

The study proved a special and secure tunnel for the firewall, which enabled the filter to address the parameter. This mechanism builds on a third party server acting as a gateway. Recently, several RFCs recommended a secure gateway box for the actual SIP proxy[22]. Some of them are based on software. Others are connected to the physical hardware layer, which comes from the session border controller. While a high section of service for VoIP firewalls with its trunk supported is complicated, a hardware solution named "Ingate" are embedded in firewalls [23]. For OpenSIPS, a trunk configuration policy is nearly the same, but the way of the security is different. our believe OpenSIPS has more chances to raise the security level. Open SIPS can act as a different variety of VoIP servers. Therefore, no Asterisk can register the server or PSTN gateway server. Hence, an encryption and authentication type can be applied in a feasible way. For instance, the RSA is used to implement the current session between servers and their clients, which can disable the attacker to be involved as the man in the middle attack who can listen to the conversation or to search the most valuable trunk that supports overseas calls.

Another studied cross infrastructure vulnerabilities that bridged VoIP and PSTN networks[24]. A general outline with a high-level of architecture was potentially found for firewalls, including functionality and signaling trust management, encryption, authentication, and intrusion detection.

V. TRUNK ENCRYPTION

Analysis is the VPN for VoIP services. However, encryption can be applied for authentication and encrypted to the server. IPSec is a good method to use between a server and its clients. Thus, it is considered a mutual method to raise the security trunk with a signal encryption packet through the IPSec. The IPSec is based on a cryptographic method to prevent eavesdropping and MiMT. Furthermore, there is a key negotiation between SSL and IPSec per session.

Hence, an encryption and authentication type can be applied in a feasible way. For instance, the RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman [25] is used to implement the current session between servers and their clients, which can disable the attacker to be involved as the man in the middle attack who can listen to the conversation or to Most SIP servers build in optional authentication procedures. However, it depends what the client's Policy to enable or disable the security measure. One of the method's

SIP can operate over different transport protocols, which are simultaneously certain and unreliable. Since a transport layer, security (TLS) is a trustworthy transport protocol[26].

In a commercial gateway sector. Configuration encryption to configure the Digest Authentication ability using Diffie-Helman key[27], for example, Cisco gateway[28]

As a result, a cryptographic algorithm can be applied, and authentication protocol also can be implemented to power up the security to the top priority of clean and secure uses..

VI. SUMMARY

Based on the results, the main problem is the security of VoIP and trusting all SIP trunks. The answer is in the affirmative because the big VoIP trade companies must ensure the quality of servers, they provide to their clients. Therefore, we believe that most trunk servers have effects that are like the flu virus because the server behavior is controlled by a hacker or a remote control access to the SIP server, which causes faulty information. This observation is reflected in two ways. First, there is an excuse to limit costs to a few thousand dollars. Second, the provider and recipient will suffer from the attack that harms both the server and clients.

We noticed this trend from the VoIP servers. The VoIP hacker went further away from the standard hacking tools. They used these tools on other servers and fired up what they could find along the way. Thus, soon we hope to reveal more solutions that are not costly such as SBC, and indicate such a solution with the VoIP server as one platform.

ACKNOWLEDGEMENTS

The authors would like to thank the anonymous reviewer for their valuable comments and suggestions to improve the quality of the paper .This work is supported by grand *RUT 2011916 –unversity science Malaysia* .

REFERENCES

- [1] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, and E. Schooler, "SIP: session initiation protocol," 2002.
- [2] C. Hattingh, D. Sladden, and A. T. M. Z. Swapan, *Sip trunking*: Cisco Systems, 2010.
- [3] C. Elliott, D. Harrington, J. Jason, J. Schoenwaelder, and F. Strauss, "W. Weiss," "SMIng Objectives", RFC 32162001.
- [4] K. Singh and H. Schulzrinne, "Peer-to-peer internet telephony using SIP," 2005, pp. 63-68.
- [5] H. Schulzrinne, "RTP: A transport protocol for real-time applications," 1996.
- [6] <http://www.nojitter.com/feature/231600052>.
- [7] I. Gaboli and V. Puglia, "SIP Trunking the route to the new VoIP services," in *Kaleidoscope: Beyond the Internet? - Innovations for Future Networks and Services, 2010 ITU-T*, 2010, pp. 1-8.
- [8] S. Opinions, "2012 SIP Trunking State-of-the-Market Report."
- [9] P. Mahler, *VoIP Telephony with Asterisk*: Signate, 2005.
- [10] B. Goode, "Voice over internet protocol (VoIP)," *Proceedings of the IEEE*, vol. 90, pp. 1495-1517, 2002.

- [11] J. Rudinský, M. Vozňák, and J. Růžička, "Asterisk and SS7," Technical report 26/20064, CESNET2006.
- [12] K. Lohiya, N. Shekokar, and S. R. Devane, "End to End Encryption Architecture for Voice over Internet Protocol," *International Journal of Computer Applications*, vol. 41, pp. 31-34, 2012.
- [13] J. Tang, Y. Cheng, and Y. Hao, "Detection and prevention of SIP flooding attacks in voice over IP networks," 2012, pp. 1161-1169.
- [14] M. Alshingiti, "Security Enhancement for SIP in Ad Hoc Networks," CARLETON UNIVERSITY, 2012.
- [15] P. C. K. Hung and M. V. Martin, "Security issues in VoIP applications," 2006, pp. 2361-2364.
- [16] Y. Wang and Y. Yang, "A Practical Method for SIP-DoS Attack Effect Evaluation*," *Journal of Information & Computational Science*, vol. 9, pp. 333-345, 2012.
- [17] N. Jeyanthi and N. C. S. N. Iyengar, "An Entropy Based Approach to Detect and Distinguish DDoS Attacks from Flash Crowds in VoIP Networks."
- [18] M. Sain and H. Rai, "Analysis and Design of a reliable packet transfer mechanism for WIMAX," 2012, pp. 500-504.
- [19] I. K. O. DETKEN and I. E. EREN, "VoIP Security regarding the Open Source Software Asterisk."
- [20] N. Janssens, X. An, K. Daenen, and C. Forlivesi, "Dynamic Scaling of Call-Stateful SIP Services in the Cloud," *NETWORKING 2012*, pp. 175-189, 2012.
- [21] S. H. Christie IV, "Firewall control for secure private networks with public VoIP access," ed: Google Patents, 2007.
- [22] J. Hautakorpi, G. Camarillo, R. F. Penfield, A. Hawrylyshen, and M. Bhatia, "Requirements from Session Initiation Protocol (SIP) Session Border Control (SBC) Deployments," IETF RFC 5853, April2010.
- [23] S. Beer and C. William, "Application Notes for Ingate Firewall using SIP Trunking with ITSPs," 2009.
- [24] H. Sengar, R. Dantu, and D. Wijesekera, "Securing voip and pstn from integrated signaling network vulnerabilities," 2006, pp. 1-7.
- [25] Y. Lindell, "Introduction to Cryptography," *Algorithms*, vol. 1, pp. 89-220, 2005.
- [26] C. Shen, E. Nahum, H. Schulzrinne, and C. Wright, "The impact of TLS on SIP server performance," 2010, pp. 59-70.
- [27] M. Steiner, G. Tsudik, and M. Waidner, "Diffie-Hellman key distribution extended to group communication," 1996, pp. 31-37.
- [28] A. Headquarters, "Cisco Unified Communications Manager Security Guide," 2007.