SHARED DETECTION OF CYBERATTACKS ON VOIP EXCHANGES.

Jiri Jezek
Doctoral Degree Programme (1), FEEC BUT
E-mail: xjezek13@vutbr.cz

Supervised by: Pavel Silhavy
E-mail: silhavy@feec.vutbr.cz

Abstract: In the last decade, security in Voice over IP raises on importance. This article focuses on shared defence systems in VoIP, summarizes the existing work related to this topic. In standard systems with basic security, it is common to monitor attacks and prevent them with certain countermeasures. A problem occurs when multiple PBXs are connected to one network because the individual PBXs do not know that other network entities are attacked. It can lead to the attack spreading to other devices connected to one network and significantly slowing the whole network. This paper proposes a solution focused on sharing information about an attacker with other network entities by using method MESSAGE from SIP protocol.

1 INTRODUCTION

Voice over IP (VoIP) is a technology designed to transmit multimedia (mostly audio) data over Internet Protocol (IP) networks. VoIP systems gradually replace traditional telecommunication systems. The main reason is that VoIP offers low cost and high quality of service for multimedia communications. Thanks to the development of 5G networks, VoIP is expected to become the dominant technology for communication based on voice [1].

For implementing VoIP, we can use plenty of protocols. Today mostly used is SIP (Session Initial Protocol) for signalling [9] in cooperation with SDP (description of relation) [10] and RTP (transmission of voice data) [11].

VoIP is a growing industry, and it makes it an attractive target for attackers. In 2017, a 29.2 billion US dollar loss was reported related to VoIP attacks, according to the Communications Fraud Control Association (CFCA). One of the leading causes of telecom fraud is Private Branch Exchange (PBX) hacking and toll fraud [8],[1]. Securing PBX is demanding for many organizations. Due to their usage attacks in popular services like web, email, ssh, traditional intrusion detection systems are not primarily meant to be used on PBX, so they are not as sufficient as they may be. Even with the Session Border Controller or edge gateway, PBX is still susceptible to a brute-force attack on SIP accounts with weak passwords. To secure the PBX and SBC correctly, human expertise is required to calibre rules and analyze the logs for abnormalities.

There can be a problem with detection attacks. PBX must detect the upcoming attack and apply defence mechanisms, and this will take some time. For higher efficiency of defence mechanisms, there can be some form of shared defence, where one PBX can contact others in the network and provide them with information about the attack and how to defence against it [2].

2 RELATED WORKS

Researchers have been investigating the options of shared defence mechanisms for PBX. In the experiment with VoIP based PBX honeypot, researchers confirmed that attacks on PBX are growing. This study has found out that almost 19 million SIP messages occurred on the experimental honeypot

in only ten days. This experiment also reacted to a similar experiment from 2009 to 2012, where between 3 years was realized 47.5 million SIP messages. We can see a considerable increase in attacks in this experiment. [3].
In another study, the authors proposed a solution with the database, which were connected nodes, which should be protected. For preventing attacks, was used system fail2ban. The proposed solution was for the general use of any systems, not specially for VoIP systems [4].
The next study is focused on the decentralized type of database – blockchain. The concrete solution runs on Ethereum blockchain. In their study, they also use fail2ban for preventing attacks. This work focuses especially on VoIP systems where information about attackers are written by smart contracts to Ethereum blockchain, to where are connected other PBX by a special interface [2].

3 PROPOSED SOLUTION

This paper proposes a solution that focuses on giving information about potential attacks using SIP protocol. Firstly, we need Intrusion Prevention System (IPS), which can identify and react to incoming attacks by applying defined rules. Based on previous researches on this topic, it seems that the best IPS in our case is Fail2ban. Fail2ban scans log files and ban IP addresses reporting too many failed login attempts. This happens by updating firewall rules to disable attempts for connection from those IP addresses for a configurable time [5].
The proposed solution is focused on sending information about an attacker using SIP protocol. If we look at SIP methods, concrete on requests, we can find some methods that can be used to provide information about an attacker, which was detected by IPS. To provide information about an attacker seems to be the best method MESSAGE, which can be easily detected and readable. Method MESSAGE is normally used for instant messaging. On image 1 you can see the flow of SIP MESSAGE request. Using MESSAGE method have also advantage that the recipient only accepts the message

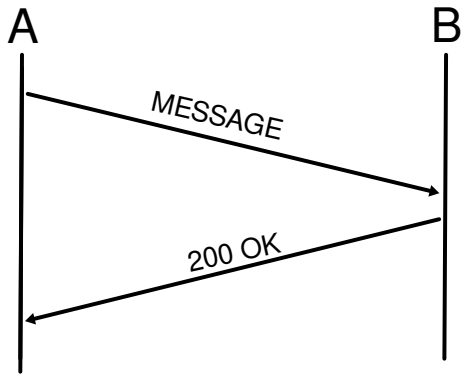

Figure 1: SIP message flow

and responds by 200 OK (when the message was sent correctly) [6]. In this case, we do not need to devise a feedback system because it is provided natively by SIP protocol (200 OK response). With 200 OK response, is sender informed that every PBX on the network got his message with information about the attacker.
Now we know in what method we will provide data with to others PBX in the network. We need to define the format of information about attackers sent by the method MESSAGE. The main information is the attacker IP address, which is the key for subsequent blocking of attackers by the firewall. The next field can be the type of detected attack (for example, Toll Fraud). Important information can be the rate of attack in attempts per second. For correct receive, it is needed to distinguish if it is a message used by a user for instant messaging or an alert message signalising that PBX is under attack. For this, we will need the format message body starting with some special characters, which

Table 1: Main fields in SIP MESSAGE

Field	Description
ipattacker	Attacker IP address.
attack	Type of attack (i.e Toll Fraud,...)
rate	Reported attempts per second

are recognisable for receiving party. Special characters to recognise can be practically anything important is recognizability for both participants of the session. The final body of request MESSAGE then can look like this:

```
<sipdeff>ipattacker=192.168.0.1;attack=tollFraud;rate=10000;<sipdeff>
```

SIP protocol is a text-based protocol. So practically anybody can read and modify them (i.e. Man in the middle attack). This might be a big problem because we send an important message leading to blocking attackers IP addresses. This vulnerability of SIP can be abused for blocking legit users IP addresses instead of attacker IP address. For securing data exists protocol SIPS (Secured SIP). In this protocol are SIP messages encrypted by using TLS (Transport Layer Security) protocol. Securing SIP messages is necessary for the correct function of the proposed solution.
In table 1, you can see the proposed data, which will be sent by PBX, which is under attack. In the end, it is needed to detect the message with the IP address of the attacker. This depends on the used PBX system. We will need several scripts. First to generate and send a message to other PBXs in our network. To generate SIP MESSAGE, we need to use the SIP message generator, for example, open-source tool SIPp [7], where we can define SIP message format. The MESSAGE method's body must be defined with the correct format to be recognizable for other PBXs. On PBXs must also be defined script, which after receiving information about the attacker, will apply firewall rules.
In figure 2 you can see the scheme of proposed solution. In the first step, the attacker wants to attack PBX2. After some time, IPS reads from logs that there can be malicious activity and add a firewall rule to block the attacker IP address. Then PBX2, with the help of their scripts, generate SIP MESSAGE which will be encrypted by TLS protocol, with information about the attacker and send it to other PBX in the network (PBX1 and PBX2). Other PBXs, by using the scripts, add new firewall rules to attacker IP address. At this moment, the attacker cannot access any PBX in the network by his IP address.

4 DISCUSSION

The work proposes the theoretical solution to the growing problem of VoIP attacking. The proposed solution is focused on the network with a larger amount of PBXs. The disadvantage of the solution with one centralized database [4] is that attacker can directly attack that database and disable communication with PBXs (by DoS attacks), or even worse, gain access to the database and by adding some false data harm legitimate users. This is solved by sending messages with information about detected attacks to other PBXs directly by SIP, where is also a back control mechanism by confirmation received message by SIP protocol.
As mentioned above, the disadvantage also removes the second solution proposed in SIPChain [2]. There is a problem solved by the decentralized database, concrete by using Ethereum blockchain. The disadvantage of using SIPChain is that it must use another interface to communicate with the blockchain. This could lead to a potential security issue. There can also be a problem if some attacker starts providing false information about attackers to blockchain used as a database, and legit users can be blocked, or it can cause a large overhead.
The proposed solution's disadvantages can be compatibility between PBXs and processing information about attackers obtained from the message method. There is also the need to secure SIP messages,

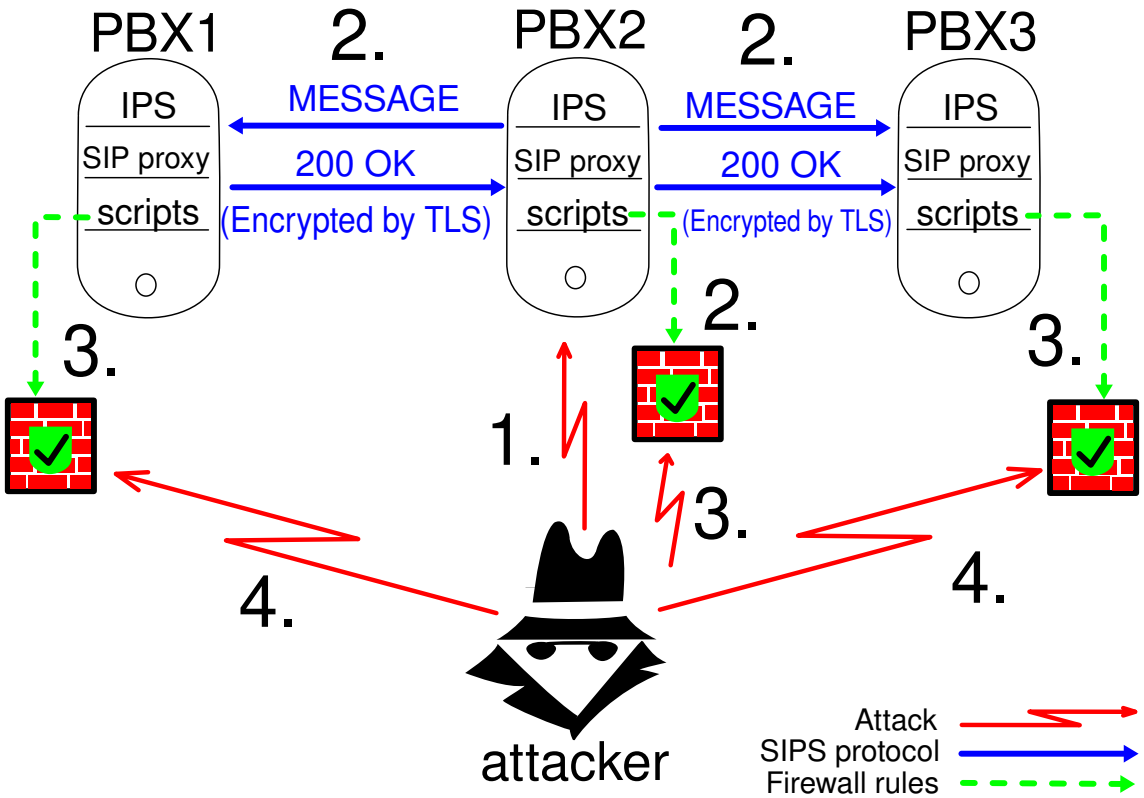

Figure 2: Scheme of proposed solution

as was mentioned in the previous chapter. This will be probably a little slower than with not secured SIP messages, but it is necessary.

4.1 Future work

Future work will focus on developing a protocol working above SIP, based on the proposed solution in this paper. The whole solution will also be practically tested and evaluated with the chosen software PBXs. Depending on the results will be the solution subsequently modified or added more security features.
We can write this into several points:

- Implement IPS to work with our chosen PBX system.
- Define the full format of the data in MESSAGE body.
- Write scripts to control receiving and sending SIP MESSAGES.
- Practically tests the whole solution.
- Make corrections in response to the tests.

5 CONCLUSION

This work focuses on the problem of shared security in the network of PBX. In the second chapter are briefly described already existing works on this topic. The first mentioned work is about the increase in the number of PBX attacks in the last years. The other two works focus on different solutions related to this topic. The next chapter proposes a theoretical solution, which focuses on

sending information about the attacker using the SIP protocol. The main idea is that when some PBX is under attack, with the help of IPS blocks the attacker IP address and generate and send SIP MESSAGE to others PBXs in the network. In SIP MESSAGE method are encapsulated information about the attacker in the defined format. When PBXs accept SIP MESSAGE, they apply firewall rules according to the obtained information. This theoretical solution will lay the foundation for future work, which will be focused on the implementation of the proposed solution. The effort is to create a shared defence protocol working above the SIP protocol by using method MESSAGE for carrying these data. This paper also discussed the advantages and disadvantages of the proposed solution to compare with existing methods, which have been described in the second chapter.

ACKNOWLEDGEMENT

The research was supported by the project FEKT-S-20-6312 “Research on electronic communications and information and systems and their use to secure critical infrastructures”.

REFERENCES

[1] Nazih, W.; Elkilani, W.S.; Dhahri, H.; Abdelkader, T. Survey of Countering DoS/DDoS Attacks on SIP Based VoIP Networks. Electronics 2020, 9, 1827. https://doi.org/10.3390/electronics9111827

[2] A. Febro, H. Xiao and J. Spring, “SIPchain: SIP Defense Cluster With Blockchain,” 2019 Principles, Systems and Applications of IP Telecommunications (IPTComm), Chicago, IL, USA, 2019, pp. 1-8, doi: 10.1109/IPTCOMM.2019.8920874.

[3] McInnes, N., G. Wills and E. Zaluska. ’Analysis of threats on a VoIP based PBX honeypot.’ (2019).

[4] M. Ford et al., “A process to transfer Fail2ban data to an adaptive enterprise intrusion detection and prevention system,” SoutheastCon 2016, Norfolk, VA, USA, 2016, pp. 1-4, doi: 10.1109/SECON.2016.7506771.

[5] Fail2ban. Fail2ban [online]. 2016 [cit. 2021-03-07]. Available from: http://www.fail2ban.org/wiki/index.php/Main_Page

[6] SIP method message. VoIP-info [online]. [cit. 2021-03-07]. Available from: https://www.voip-info.org/sip-method-message/

[7] GAYRAUD, Richard a Olivier JACQUES. SIPp. SIPp [online]. 2014, 04/20/2014 [cit. 2021-03-07]. DostupnĂ© z: http://sipp.sourceforge.net/

[8] J. Osenbaugh, “Telecom fraud on the rise: What enterprises need to know.” https://www.nojitter.com/security/telecom-fraud-rise-what-enterprises-need-know, February 2019. Web. [cit. 2021-03-07].

[9] SIP: Session Initiation Protocol [online]. Network Working Group, 2002 [cit. 2021-03-07]. DostupnĂ© z: https://tools.ietf.org/html/rfc3261

[10] SDP: Session Description Protocol [online]. Network Working Group, 2006 [cit. 2021-03-07]. DostupnĂ© z: https://tools.ietf.org/html/rfc2327

[11] RTP: a Transport Protocol for Real-Time Applications [online]. Network Working Group, 2003 [cit. 2021-03-07]. DostupnĂ© z: https://tools.ietf.org/html/rfc3550