Hunting SIP Authentication Attacks Efficiently

Tomáš Jansky, Tomáš Čejka, Václav Bartoš

Hunting SIP Authentication Attacks Efficiently

Tomas Jansky[1], Tomas Cejka[2], Vaclav Bartos[2]

[1] CTU in Prague, FIT, Thakurova 9, 160 00 Prague 6, Czech Republic
jabsoluteskto1@fit.cvut.cz
[2] CESNET, a.l.e., Zikova 4, 160 00 Prague 6, Czech Republic
cejkat@cesnet.cz, bartos@cesnet.cz

Abstract. Extended flow records with application layer (L7) information allow for detection of various types of malicious traffic. Voice over IP (VoIP) is an example of technology that works on L7 and many attacks against it cannot be reliably detected using just basic flow information. Session Initiation Protocol (SIP), which is commonly used for VoIP signalling, is a frequent target of many types of attacks. This paper proposes and evaluates a novel algorithm for near real time detection of username scanning and password guessing attacks on SIP servers. The detection is based on analysis of L7 extended flow records.

1 Introduction

Voice over IP (VoIP) is a technology that replaces classic telephone services and is used to transfer multimedial data such as voice or video over common packet switched networks. One of the core protocols used in VoIP services is Session Initiation Protocol (SIP), which is used for signalling between communicating parties.

There are many types of attacks against SIP infrastructure. The most dangerous attacks often compromise Private Branch Exchange (PBX) devices and cause a significant financial loss to the owner of PBX. According to [3], a total worldwide loss due to VoIP hacking and calling to premium rate services goes to billions of dollars per year.

Even though there are standards that describe security considerations and extensions of the SIP protocol, it is still often observed unencrypted in real network traffic. This allows for security analysis of SIP traffic at a network level using a network passive monitoring. The analysis may detect malicious SIP traffic so that a network operator can inform owners of the target device about a potential threat or take appropriate actions to mitigate malicious traffic.

Network traffic monitoring in large networks is usually done using so called flow records, i.e. aggregated information about communicating hosts that is computed from observed packets. A typical flow record consists of information from packet headers up to the transport protocol. This approach is feasible and it allows for detection of various types of malicious traffic. However, as it was presented in [2], many types of attack at application protocol (L7) cannot be reliably detected using just the basic flow records. This paper shows usage of application layer flow records [6], in this case flows extended by L7 information about SIP traffic, for detection of brute-force password guessing and scanning for user accounts (called *extensions* in SIP terminology) on PBX. This work is a continuation of [2] and an improvement of detection abilities of the previous detection mechanism.

2 SIP attacks

This work focuses on two types of network attacks by an unauthenticated external attacker against a SIP server – extension scanning (i.e. finding valid usernames) and password guessing.

Both are based on sending large amount of requests (usually `REGISTER`) to the server. When a client sends the request requiring authentication, server challenges it with a response code `401 Unauthorized`. Normally, the client sends valid credentials and server responds with `200 OK`. If the username is not valid, server responds with `404 Not Found` or `401 Unauthorized`, depending on configuration[1]. In case of correct username but wrong password, `401 Unauthorized` is returned.

Therefore, both types of attacks are characterized by a high number of `REGISTER` requests and `401 Unauthorized` (or `404 Not Found`) responses, using either different extensions (extension scanning) or a single extension but different passwords (passwod guessing). Combination of both is also possible. More details about these SIP attacks can be found in [4].

3 Detection algorithm

In line with the L7 flow monitoring approach, our monitoring probes use a plugin which is able to extract necessary SIP information from traffic (*response code*, *To* and *CSeq*). As it is shown in Fig. 1, flow records are sent from probes to a collector in the IPFIX format and afterwards analyzed by the detection algorithm which is implemented as a part of the NEMEA [1] system.

The detection method is designed to work without any prior knowledge of VoIP infrastructure or existing extensions. It is based on an analysis of `401` responses from SIP servers. By aggregating these responses by a PBX IP address, an extension (username) and a client IP address, the detection algorithm can detect non-standard and potentially malicious traffic.

The algorithm shifts between two stages. In the first stage, it receives data and stores it into data structures. For each SIP server (i.e. IP address sending SIP responses), the following data is stored – a list of client IPs, a list of usernames, and a mapping between them that tells which clients tried which usernames and a number of such attempts.

[1] The former is considered insecure since it eases the extension scanning as it immediately discloses existence of the extension on the server.

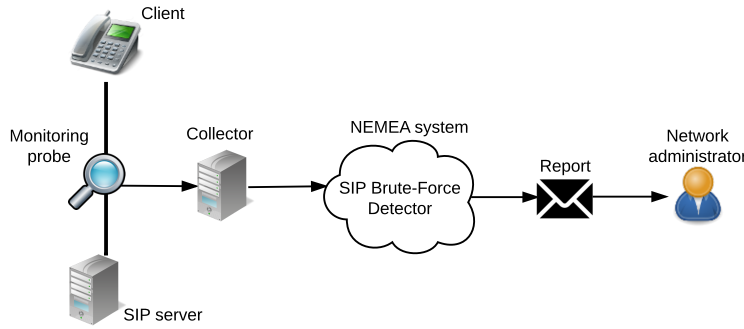

Fig. 1: Monitoring infrastructure.

After a certain time period, the algorithm gets to the second stage where it evaluates the stored data. First a type of (potential) attack is determined. If a single client attempts to register one certain extension, it is classified as a brute-force attack. This attack can be reclassified as a distributed brute-force attack if more clients attempt to register the particular extension on the same server. When a client tries to register more than one extension, the behavior is classified as a scan. When the number of attempts exceeds a threshold, the attack is reported. If `200 OK` response code is detected as part of the communication, the attack is considered successful. If no communication between the server and the client is observed for a certain amount of time, the corresponding structures are released from memory.

The algorithm was implemented as a module for open-source NEMEA system and published at GitHub[2].

4 Evaluation

Since the algorithm is threshold based, it was necessary to estimate some key values based on the behavior on a real network. We temporarily captured SIP traffic from CESNET2 network[3].

After the analysis of the captured data, we discovered that more than **99.9 %** of all successful register attempts use **20** messages or less. We therefore set 20 attempts as a threshold for deciding whether the communication is malicious or not.

We also examined the frequency of malicious requests in individual attacks and discovered that only **0.01 %** have more than **30 minutes** delay between individual requests. Therefore an information about a communication is released from the program memory if no new message is observed for 30 minutes. It also

[2] `https://github.com/CESNET/Nemea-Detectors/`

[3] CESNET2 network is monitored at all its 7 peering links at the 10 and 100 Gbps wire speeds. Average total amount of traffic: 110,000 flows/s, average SIP traffic: 1,500 flows/s.

means that an elapsed attack is reported after this delay since the last observed message.

Finally, we counted unique extensions attempted by every client in 30 minute windows. Most observed clients attempted to register as less than **10** unique extensions on a certain server. This value is surprisingly high, but it is possible that the client is actually a proxy server or there are multiple SIP clients hidden behind NAT. We used 10 distinct extensions as a threshold for extension scanning detection.

First, the detection module was tested on a real network with generated malicious traffic using auditing tool SIPVicious [5]. All generated attacks were successfully distinguished from other SIP communication and reported.

Then, the module was run for one week to capute real attacks in the CESNET2 network. Total number of 7,008 events were reported. Table 1 shows some statistics about reported events. One of the most interesting findings is that **46.3 %** of all `200` and `401` SIP responses to `REGISTER` requests are a malicious traffic and are directly related with one of reported alerts.

Tab. 1: Statistics after one week of flow detection

Brute-force events	6,488 (92.6 %)
Extension scanning events	520 (7.4 %)
Successful brute-force events	7
Strongest brute-force	6,930,911 attempts
Largest scan	9,360 extensions
SIP flows observed	718,627,758
SIP flows analyzed (401 & 200 responses)	40,909,352 (5.7 %)
Number of malicious flows	18,945,291 (46.3 %)

Detection results were stored to a log file during the the week. Thorough examination showed that most attackers perform either brute-force attacks or extension scanning. However, some of the attackers combine these two attacks to one, usually trying a small number of password guesses (between 20 to 100) to a large number of extensions. This behavior indicates that these attackers use some sort of a set of common and frequently used passwords.

To confirm that the detection module is working correctly, we manually analyzed traffic of some of the reported attacks. Most of them are certainly scanning or brute-force attempts. In just a few cases were the traffic did not look like any of the attacks and can be viewed as false positive (we estimate total FP rate to 0.1%), however, it was still an unusual traffic, probably caused by misconfiguration of some devices, which is worth inspecting. To prove practical usefulness of the detection, we chose one of the attacks marked as successful and contacted the administrator of the attacked PBX. He confirmed that, indeed, the account was compromised and informed us that appropriate steps to fortify the PBX will be taken.

5 Conclusion

We designed a method for detection of SIP attacks, namely username scanning and password guessing, based on an analysis of SIP headers in extended flow records. The algorithm works without any prior knowledge of VoIP infrastructure. Its key parameters and thresholds can be adjusted by network administrators in accordance to the characteristics of their network to reach optimal detection results. It is efficient and it is able to process data from an NREN-sized network (several 10 and 100 Gbps links) in real time.

Using the algorithm, we were able to detect thousands of scanning and password guessing against SIP infrastrucutre. The software is also capable of detecting distributed guessing of user's password, however, this type of attack was not observed in our network yet. Some of the attacks, which were identified as successful, were reported to network administrators who subsequently confirmed the attacks. Analysis of detection results showed only a small amount of false positive reports with frequency around 0.1 % of all reported events. Most of the false positives are caused by a few clients that communicate in an unusual way and can be easily filtered using a whitelist.

6 Acknowledgments

This work was supported by *Packet analysis based network diagnostics (DISTANCE)* project No. TH02010186 granted by Technology Agency of the Czech Republic, project Reg. No. CZ.02.1.01/0.0/0.0/16_013/0001797 co-funded by the MEYS of the Czech Republic and ERDF and the CTU grant No. SGS17/212/OHK3/3T/18 funded by the MEYS of the Czech Republic.

References

1. Cejka, T., Bartos, V., Svepes, M., Rosa, Z., Kubatova, H.: NEMEA: a framework for network traffic analysis. In: 12th International Conference on Network and Service Management (CNSM 2016). Montreal, Canada (Oct 2016)
2. Cejka, T., Bartos, V., Truxa, L., Kubatova, H.: Using application-aware flow monitoring for sip fraud detection. In: Intelligent Mechanisms for Network Configuration and Security (AIMS 2015). pp. 87–99. Springer (Jun 2015)
3. Communication Fraud Control Association: Global fraud loss survey (2015), `http://www.cfca.org/pdf/survey/2015_CFCA_Global_Fraud_Loss_Survey_Press_Release.pdf`
4. Dwivedi, H.: Hacking VoIP: protocols, attacks, and countermeasures. No Starch Press (2009)
5. Gauci, S.: SIPVicious. Tools for auditing sip based voip systems (2012), `https://code.google.com/p/sipvicious/`
6. Velan, P., Celeda, P.: Next generation application-aware flow monitoring. In: Monitoring and Securing Virtualized Networks and Services, LNCS, vol. 8508, pp. 173–178. Springer (2014)