https://doi.org/10.26552/com.C.2013.2A.180-184

Filip Rezac – Jakub Safarik – Miroslav Voznak – Jan Rozhon – Karel Tomala – Jiri Vychodil *

BRUTEFORCE ATTACKS BLOCKING SOLUTION ON EMBEDDED SIP COMMUNICATION SERVER

This article deals with embedded SIP communication server with an easy integration into the computer network based on open source solutions and its effective defense against the most frequent attack in the present – Denial of Service. The article contains brief introduction into the Bright Embedded Solution for IP Telephony – BESIP and describes the most common types of DoS attacks, which are applied on SIP elements of the VoIP infrastructure including the results of defensive mechanism that has been designed.

Keywords: *BESIP, SIP, IP Telephony, DoS, IPS, Security, Embedded Solution.*

1. Introduction

Many large institutions operate small offices with tens or hundreds of employees. A common requirement is the full integration of these departments in the organization's environment (examples are libraries and branch offices). With our proposed solution BESIP (Bright Embedded Solution for IP telephony), the integration can be achieved easily with the use of IP telephony and supporting network infrastructure. The device is designed as a price acceptable solution that supports SIP (Session Initiation Protocol) IP telephony and also services such as ENUM (E164 NUmber Mapping) [1], secure communication using SRTP (Secure Real-time Transfer Protocol) and TLS (Transport Layer Security) [2], monitoring of call quality, tools for attacks detection, billing and clear configuration via a web interface. The whole solution is deeply described in the paper "Embedded multiplatform SIP server solution" [3].

The system consists of software PBX Asterisk [4] and a part of BESIP is also a module responsible for the safety. Today one of the most common attacks against these types of network elements is Denial of Service – DoS. It is because of high efficiency and relatively simple feasibility. It was therefore necessary to develop methods for security which can be used not only as part of our system, but also as a general solution for Asterisk.

The following chapters refer to the scheme of the system in more details, the vulnerability of Asterisk SIP proxy servers to DoS attacks and methods for server protection. For each attack, this paper describes their impact on a SIP server, evaluation of the threat and the way in which they are executed.

2. BESIP System Schemes and Modules

As mentioned above, the BESIP system is a modular solution where each element consists of several applications which are supported by core. (Fig.1). Modules are divided according to the function which they perform at Core, Security Module, Monitoring Module, PBX Module, and Module of Services.

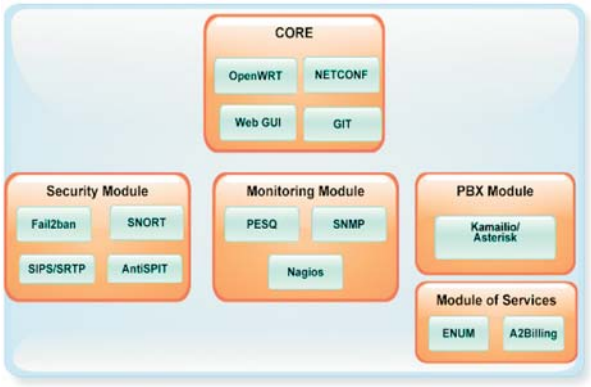

Fig. 1 BESIP Divided into Modules

2.1. Core

The core of the system consists of the Linux distribution OpenWRT [5] which is directly designed for embedded devices and has very low demands on computing power.

* **Filip Rezac, Jakub Safarik, Miroslav Voznak, Jan Rozhon, Karel Tomala, Jiri Vychodil**
Department of Telecommunications, Faculty of Electrical Engineering and Computer Science, VSB-TU Ostrava, Czech Republic,
E-mail: fillip.rezac@vsb.cz

To manage updates and revisions, Git [6] application is used. Another tool that is part of the core is the NETCONF protocol [7]. NETCONF provides mechanisms to install, manipulate, and delete the configuration of network devices.

The last part of the Core Module is Web GUI support. This is done using Lighttpd [8] which has a small memory demands and is therefore suitable for embedded devices.

2.2. Security Module

Security module is responsible for protecting the system itself against attacks from external subjects, as well as the analysis of these threats.The module is responsible also for signaling and media encryption.

The protection of system against threats is provided by Fail2ban [9] application. It is a tool which is able to block IP addresses in the firewall based on the logs scan. Another way to protect the system against attacks directed at an IP telephony service is the implementation of Snort and IPS (Intrusion Protection System) [10]. Snort and its sub-applications are the main defense used to protect against DoS, as described below. Protection against Spam over Internet Telephony – SPIT attacks is solved by the AntiSPIT [10] tool which was also developed as an original solution by the authors of article. The last element of the security module is the ability to encrypt calls using SRTP and TLS protocol. This security is ensured directly by communication server, in our case, the SIP PBX Asterisk in version 1.8.4.4 [10].

2.3. Monitoring Module

This module is able to monitor the speech quality for individual IP calls, as well as provide other monitoring of network devices in the network using SNMP (Simple Network Management Protocol) and Nagios tools [11].

2.4. PBX Module

This module is one of the most important of the entire system, as it contains the actual communication server for IP telephony calls. All other modules are interconnected with Asterisk because instead of sending or retrieving data, Asterisk is also responsible for encrypting and comparing call quality using algorithm which is based on PESQ (Perceptual Evaluation Speech Quality) method [9].

2.5. Module of Services

Module of services contains tools for providing additional services, such as billing or ENUM. End user can also define additional services that he/she needs, but above mentioned are part of the system by default.

2.6. Hardware

Since the beginning of the development, the BESIP was planned as the most mobile, portable and especially low cost device. Outside of these conditions it also had to offer sufficient computing power for smooth operation of all modules, applications and participants.

After a series of tests and analyses a standard desktop PC with Atom processor was chosen. It consists of the Intel Packton D410PT setwith the following configuration: CPU: x86 Intel Atom D410 - 1,66 GHz, chipset: Intel NM10 Express, NIC: Realtek 10/100 Mbps, USB 2.0: 8 ports, max. RAM: 4 GB, memory: Kingston 1GB 667MHz CL 5, HDD: Kingston 16GB SSD, interface: SATA 3 Gb/s 2,5" , case: Eurocase Mini ITX Wi-05, Size: 265 × 90 × 270 mm, power Supply: 200 W, number of 2,5" positions: 1.

3. Classification of the DoS Attacks

Denial of service can be achieved in several ways – flooding a server with malformed, damaged or useless packets as a result of which the server runs out of its resource capacity. The affected server is then unable to communicate with its regular users or process regular requests. DoS attacks can be divided into three general classes [12, 13] - Flooding Attacks which are targeting on server resources (CPU, memory or link capacity), Misuse Attacks specified by the hacker uses of a modified SIP message to cancel or redirect calls or misuses of the service and Unintentional Attacks where the attacker targets the supporting services (DNS, call billing, etc.) in order to distort or restrict the service. These attacks typically affect a small group of users only.

The impact of a DoS attack depends on the target. Targeting a particular client can lead to denying the service to this user only but when a SIP server such as BESIP is the target, no user can use its services.

4. BESIP Security Technology Used

Attacks against the embedded systems are more dangerous due to their relatively lower performance which makes the attacks more efficient. That is because we tried to use an effective secure solution in BESIP system. We chose an IPS system, consisting of three applications.

4.1. Snort

The core of the entire IPS solution is IDS (Intrusion Detection System) system Snort which detects malicious activity in the network. The detection is based on signatures or detection of anomalies. The whole IDS system is modular. The most important components are Packet Decoder that captures packets from network interfaces, prepares them for pre-processing. Pre-processor is responsible for processing or modification of the packets before processing (packet Defragmentation, URI decoding, reassembling TCP

streams, etc.). Other modules are also important. Detection Engine is responsible for attack detection, Logging and Alerting System is linked to the Detection Engine and is used to log the activity or generate an alert. Plenty of plugins and extensions that enhance its features are also available for Snort.

4.2. SnortSam

This application operates on the client-server model. It allows Snort to dynamically intervene into iptables rules. To ensure its proper operation, we need to first upgrade our Snort installation with a SnortSam plugin. The user communicates with the Snort's sensor, sends commands to the server (where incident has been detected). The server listens on port 898, applying information from clients to iptables rules (see Fig. 2). Iptables is an open-source firewall for Linux-based operation systems. It is used to block malicious traffic on a server.

SnortSam messages are transferred as encrypted. A whitelist of non blockable IP addresses is also available. The detected traffic is then blocked for some time. Once the attack is over and timed out, the blocked IP is allowed to communicate again. Thus, only malicious traffic that poses a threat to our server is blocked.

5. Results

We created a testing topology to measure DoS and security solution effectiveness. It contained a BESIP system, hacker's PC and some endpoint devices registered on BESIP.

The malicious tools applied were as follows: Sipp, Inviteflood, Udpflood, Flood2, Juno.

5.1. Attacks on BESIP's CPU Using Sipp

The Sipp programme is primarily used to simulate calls and to carry out SIP proxy stress tests. But with a simple upgrade of the call scenarios, it can make malicious calls on SIP proxy. These calls are intended to overload system's CPU. Figure 3 shows the impact of these attacks on the BESIP. The attack scenario applied was the same for each attack. Sending malicious packets started in 10 s and continued for 60 s. Other 30 s shows the time for which the system is still inhibited by the attack.

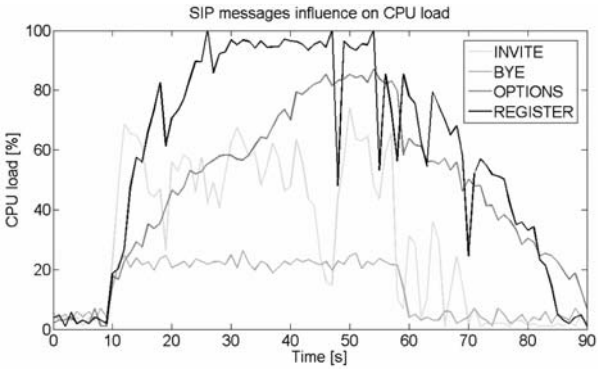

Fig. 3 The impact of different attack SIP message types on a BESIP's CPU load

To enable the comparison of the efficiency of individual malicious SIP messages, the messages had been sent to the SIP server with the same rate (250 messages per second). Clearly, the most effective SIP messages to attack a SIP server are REGISTER and OPTIONS. In the first case, the endpoint could not register or make calls, though running calls was not affected (the RTP stream only between endpoints). OPTIONS flood caused merely a delay in request processing, yet the situation deteriorated as the attack continued. In the end, not a single endpoint was able to register or make calls. The relatively long time necessary for the BESIP to recover (in both cases) was rather surprising.

The delay in connection was evident in the attack performed by means of INVITE messages. Some calls failed to be connected at all. The attack was performed by a non-existing source user.

Attacks performed by means of BYE, CANCEL and ACK messages returned almost the same results (the figure illustrates only the attack by means of the BYE message). During the attack, no call or registration was affected. BYE and CANCEL were not sent to end a particular call.

Security precautions against all these attacks include Snort rules tracking the number of messages sent to the SIP server from a particular source address. Where the limit for messages was exceeded, the blocking rule was activated on the firewall. The CPU load with the activated IPS system was about 9% during these attacks (Fig. 4.).

```
alert udp $EXTERNAL_NET any -> $SIP_PROXY $SIP_PORT (msg:"SIP DoS
attempt(registerflood)"; content:"REGISTER sip";detection_filter:track by_src,
count 50, seconds 5; classtype:misc-attack; sid:1000001; rev:1; fwsam:src, 5min;)

alert tcp $EXTERNAL_NET any -> $SIP_PROXY $SIP_PORT (msg:"SIP DoS
attempt(registerflood tcp)"; content:"REGISTER sip"; detection_filter:track by_src,
count 50, seconds 5; classtype:misc-attack; sid:1000007; rev:1; fwsam:src, 5min;)
```

Fig. 2 The example of the Snort rules - tracking the number of SIP REGISTER messages from one source

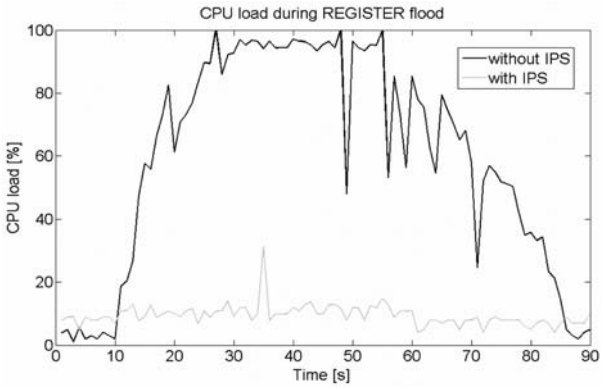

Fig. 4 The impact of an attack with (SSI) and without the protection

The attacker could be sending all the above mentioned malicious messages at a higher rate. In this way each malicious message can consume up to 100% of the BESIP's CPU. Just to compare, the INVITE messages need 10 times higher rate than the REGISTER messages to consume a similar load of the affected machines CPU. The INVITE messages can also send the inviteflood application and create a situation very similar to the flooding with UDP packets (the same is true for any attack with a high rate of packets sent).

5.2. Link Flooding Attacks

Unlike the above mentioned attacks, udpflood only floods the target destination with useless UDP packets. These packets contain a sequence from 1 to 9, followed by zeros. The packet size is 1400 bytes, and the tool can spoof the source address.

The CPU load is very low during the attack but all communication with the BESIP is blocked due to a high volume of traffic. Blocking the traffic on BESIP's interface is useless as the link would still be flooded. There is no efficient protection to be applied on the system, it is only possible to eliminate the impact of such an attack.

5.3. TCP SYN Flood Attacks

The last type of attack against BESIP tested was to flood it with TCP SYN flag set packets. We used flood2 and Juno applications. The Juno tool is especially dangerous as it can be easily upgraded to spoof the source address and ports. When the attack was launched, the connection with the system was lost almost instantly. Detecting this attack is simple but surprisingly useless. Even with an active firewall rule, Snort still analyzes the malicious traffic and the system's CPU load approaches 100%.

5.4. Assessment of Results

The performed tests clearly indicate that SIP proxy is rather vulnerable to DoS attacks. As the BESIP runs on a limited physical machine, only very basic protection mechanisms against certain DoS attacks can be implemented. This system consists of the following applications: Snort, SnortSam and Iptables. The tests proved that the analysis of the BESIP's traffic does not significantly affect system's performance (except for TCP SYN flood attack).

The most dangerous attacks include flooding with REGISTER, INVITE and OPTIONS messages, link bandwidth depletion using udpflood and TCP SYN flood attack. The attacks using malicious ACK, BYE or CANCEL messages are harmless at lower rates, with the same impact as udpflood at higher rates. No effective protection to be applied directly on the BESIP exists against certain attacks. In this case, a more secure network topology is the only solution (Fig. 5).

The main change in this topology is the inclusion of a demilitarized zone – DMZ. It is located between two firewalls (inner and outer). The purpose of this zone is to separate the safe inner part from the rather dangerous outer part of the network. Both firewalls run SnortSam agents so rules can be dynamically applied on both machines.

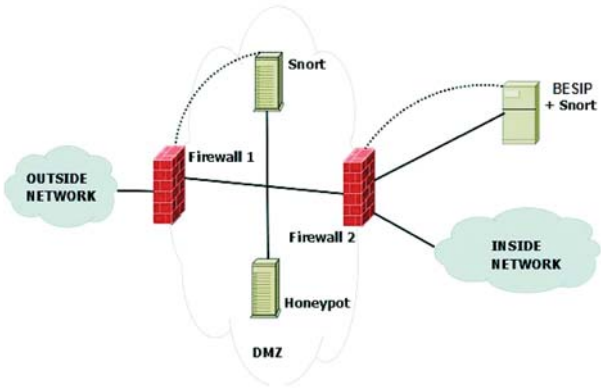

Fig. 5 The proposal of a safer topology

The inner firewall (marked as Firewall 2) serves to protect the BESIP system against the attacks from inside the network. All traffic to the BESIP has to pass through at least one firewall. The safe inner network should be implemented as a matter of course. The potential attack from inside the network would affect many users. Using encryption, VoIP VLANs and methods such as ARP inspection and DHCP snooping should provide an adequate response to possible security breaches. The implementation of a QoS mechanism should further reinforce the protection.

A honeypot located in the DMZ is an inspiration for further security precaution to be implemented.

6. Conclusion

We have developed and implemented a system with the working title BESIP, which allows easy integration of SIP IP telephony

infrastructure to branch offices of large companies. On this solution were also implemented security solutions, which should reduce or completely eliminate the attacks, mostly DoS threats. We tested their efficiency in practice and documented the results. This article maps the most frequently used DoS attacks of today and evaluates the risk inherent to each of them. On the other hand the solution proposed in this article should ensure only a basic level of protection suitable for small and middle-size offices or detached workplaces for which the BESIP is intended. The contribution of this paper includes the performed comparison of the DoS attacks' efficiency. It was tested both without any protection and then with implemented Snort and SnortSam applications as proposed in our solution.

Acknowledgement

The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7/2007-2013) under grant agreement No. 218086.

References

[1] BRADNER, S., CONTROY, L., FUJIWARA, K.: *The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM)*, RFC 6116, URL: http://tools.ietf.org/html/rfc6116, 2011.

[2] DUHA, J., DADO, M., JARINA, R.: Communication Technologies and Services, *Communications - Scientific Letters of the University of Zilina,* vol. 5, No. 3, pp. 33-35, 2003.

[3] MACURA, L., VOZNAK, M., TOMALA, K., SLACHTA, J.: *Embedded Multiplatform SIP Server Solution,* 35th Intern. Conference on Telecommunications and Signal Processing, TSP 2012, Prague, pp. 263-266, 2012.

[4] KLIMO, M., KOVACIKOVA, M., SEGEC, P.: Selected Issues of IP Telephony, *Communications - Scientific Letters of the University of Zilina,* vol. 6, No. 4, pp. 63-70, 2004.

[5] SURHONE, L. M., TENOE, M. T.: *OpenWrt,* Betascript Publishing, ISBN-13: 978-6135271591, 2011.

[6] LOELLIGER, J.: *Version Control with Git: Powerful Tools and Techniques for Collaborative Software Development,* O'Reilly Media; 1 edition, ISBN-13: 978-0596520120, 2009.

[7] ENNS, R.: *NETCONF Configuration Protocol,* RFC 474, URL: http://tools.ietf.org/html/rfc4741, 2006.

[8] BOGUS, B.: *Lighttpd,* Packt Publishing, ISBN-13: 978-1847192103, 2008.

[9] VOZNAK, M., HALAS, M., REZAC, F., KAPICAK, L.: *Delay Variation Model for RTP Flows in Network with Priority Queueing,* 10th WSEAS Intern. Conference on EHAC'11 and ISPRA-11, Cambridge, pp. 344-349, 2011.

[10] REZAC, F., VOZNAK, M., TOMALA, K., ROZHON, J., VYCHODIL, J.: *Security Analysis System to Detect Threats on a SIP VoIP Infrastructure Elements,* Advances in Electrical and Electronic Engineering, vol. 9, No. 5, pp. 225-232, 2011.

[11] BARTH, W.: *Nagios: System and Network Monitoring,* No Starch Press; Second Edition, ISBN-13: 978-1593271794, 2008.

[12] ENDLER, D., COLLIER, M.: *Hacking Exposed VoIP,* McGraw-Hill Osborne Media, p. 321-363, 2009.

[13] SISALEM D., KUTHAN J., ELHERT T. S., FRAUNHOFER, F.: *Denial of Service Attacks Targeting SIP VoIP Infrastructure: Attack Scenarios and Prevention Mechanisms,* IEEE Network, 2006.