A Security Approach using SIP Protocol in Imbedded Systems

Toniclay Andrade Nogueira, Adauto Cavalcante Menezes,
Admilson De Ribamar Lima Ribeiro and Edward David Moreno Ordonez
Computing Department, Segipe Federal University, Aracaju, Brazil

Keywords: VoIP, Asterisk, Embedded Systems, SIP, Safety.

Abstract: Voice over IP communication will dominate the world. However, given the growing demand for voice and data communication to make any and all communication reliable and secure, several attacks occur frequently in communication networks, so this work is based on verifying security, analyzing risks, vulnerabilities, such as verifying the attacks and proposing a security measure for voice over IP communication on embedded devices.

1 INTRODUCTION

The Voice Over Internet Protocol (VoIP) technology consists in the integration of the services in the telecommunication areas and the network services provided by computers. In this way, it enables the digitization and encoding of the voice signal and transforms it into data packages for communication in a network using UDP protocols.

In this context, the VoIP concept allows cost reduction in installations, maintenance and management of parallel networks. With this, a new concept of telephony is created (Sitolino 1999). However, it will be necessary equipment, techniques and specific human resources (Silva, 2016).

Stapko (2007) understands as information security the protection of personal or confidential information, as well as the computational resources of individuals or organizations. Without information security, malicious individuals can destroy or use such information for malicious purposes. The state-of-the-art security in VoIP telephony involves audio encryption between the two distinct points as well as interoperability between communication server manufacturers through indecipherable encryption and centralized management (Stallings, 2008).

According to Barr (1999), Car and Wagner (2003) and Marwedel (2011), embedded systems must be reliable, since failures can compromise their functionality and make system recovery unfeasible. Embedded systems use hardware platforms, which are driven by softwares. Several implementations of processors can be used, which implies a great reduction of costs.

Some reliability issues are found on embedded devices, as they cannot be safely shut down for repairs, the system must run continuously.

As its operating mode has reduced performance, the environment tends to fail if it is turned off (Akyildiz, 2002). Security in embedded systems was not always considered, since most of these systems were initially operated without Internet connectivity.

Information security and new embedded device paradigms are increasingly present in our lives. However, the communication between devices will have a great impact on global communication, which will increase the efficiency and security of VoIP communication.

This article is organized as it follows: section 2 is composed of theoretical grounding presentation, section 3 presents related works, section 4 has a description of the proposal, and section 5 show the expected contribution of the research.

2 THEORETICAL FOUNDATION

2.1 VoIP

According to Raake (2007) and Walker, (2004), VoIP is a technology that performs voice communication over an IP network.

The communication process consists of transforming the analog voice into digital, through the

Nogueira, T., Menezes, A., Ribeiro, A. and Ordonez, E.
A Security Approach using SIP Protocol in Imbedded Systems.
DOI: 10.5220/0006354403520355
In *Proceedings of the 13th International Conference on Web Information Systems and Technologies (WEBIST 2017)*, pages 352-355
ISBN: 978-989-758-246-2

fragmentation of the package and transport over the IP network. The process is becoming more modern, it is possible to mention some softwares that work with this technology, among them, Facebook, Messenger, Skype, Viber and WhatsApp.

In image 01 we can observe the operation of a VoIP application where the analog audio is converted into digital and grouped into packages that are transmitted to the IP network through the Real Time Protocol (RTP) protocol, after arriving at the receiver the packages are organized and then reproduced.

Figure 1: Scenario of the ideal operation of the VoIP application, Shigueoka, 2016.

2.2 Embedded Systems

Some data researched in high technology shows that more than 90% of microcomputers manufactured in the world are intended for machines that are not called computers, such as cell phones, automobiles, DVD players, among others.

According to Reis (2004), what comes to differentiate the set of devices from a computer is the project based on a dedicated set and specialist, consisting of Hardware, Software and Peripherals, i.e., embedded system.

For Ball (2005), the system is classified as embedded when it is dedicated to a single task and continuously interacts with the environment around it, by the use of actuators and sensors.

In their article, Siqueira, Menegotto, Weber, César Netto and Wagner (2006) comment on the use of embedded systems in critical applications, which comprises as applications in which the risks associated with the hazards involved are considered unacceptable and need to be handled.

The embedded system is commonly a solution formed from dedicated and specific microcontroller and software to performing the operational functions of equipment for which it was designed.

2.3 Session Initiation Protocol (SIP)

SIP has been developed to facilitate the implementation of the basic aspects of a session, which is a non-trivial process. Today it is used worldwide and it is also a strong “competitor” of H.323. Barbosa (2006) defines SIP as a protocol that signals client-server sessions, and that stands out for its simplicity and mobility; it has a primitives the initialization, modification and termination of sessions in a VoIP communication.

According to Defsip, together with Real-time Transport Protocol (RTP), Real Time Streaming Protocol (RTSP), Session Description Protocol (SDP), SIP establishes a complete multimedia architecture, providing complete services to the user.

SIP also provides participant management services in a multimedia session.

According to Cuervo (2000), due to the ability of working in conjunction with other protocols, it allows integration with public telephony, allowing not only the connection between IP extensions, but also for public network telephones.

2.4 Types of Attacks to SIP Protocol

2.4.1 Main-in-the-middle

For this attack, the attacker can use two techniques: ARP table poisoning, or DNS cloning. With either of these, permission is granted to be between the SIP server and the User Agent. With this type of attack, the intruder does not necessarily know valid usernames and passwords; they can simply route traffic between the server the and client and act intercepting the packages, preventing them from reaching their real destination, which is the SIP server (Nakamura, Emílio, Geus and Lício, 2007).

2.4.2 Subsection Titles

According to Thermos (2007), this attack aims to obtain credentials from valid users in a SIP telephony communication system using a brute-force attack, which is, sending multiple ID requests and passwords to from a dictionary.

2.4.3 Denial of Service

In attacks known as Denial of Service, it is possible to layers of infrastructure in VoIP environment. According to Thermos (2007) the DoS attacks have as main objective to cause the interruption of the target service. In this case, the attack is directed to both the operating system and also to the network services.

2.4.4 SIP Redirect

For Butcher, Li and Guo (2007), the attack employs a server that receives requests from a telephone or proxy and returns a redirect response, which indicates

where the request is to be repeated, thus enabling users to have a call redirected to another location rather than where they are located. However, the caller normally dials only the number to reach the user.

The attacker redirects the victim's calls to a specific number, so the attacker starts receiving the calls that were forwarded to the attacked user.

3 RELATED WORK

The work covered in this article contains a large amount of research. Thus, the IEEE Base has been used with works from the year 2012 to 2016.

3.1 The Communication System

In their article, Lomotey and Deters (2014) show that IP communication systems have been the target of attacks, such as call theft, attacks on servers, which allows access to users' data. Thus, the author proposed a solution to prevent the intrusion of attackers in the communication system built in VoIP Asterisk.

In his experiment, a complete platform for Asterisk was not used because he proposed a cloud-based middleware, which layer maintains the most sensitive part of the information call.

3.2 VoIP Security Analyses

Rehman and Abbasi (2014) analyzed security in the VoIP architecture with the Asterisk voice over IP communication system. It has been noted that most of the attacks are related to the fragility of the SIP protocol, espionage attacks, modification and involuntary interruption were detected.

The authors have proposed as solution of the presented problem, an efficient and secure mechanism of authentication for the protocol SIP, with this, it is possible to assure greater protection to the attacks.

It was suggested to assign a cryptographic token that would authenticate the users allowing their identification and providing greater security as well as there would be the need for the user to enter a password to use other available services.

3.3 VoIP Intrusion Detection with Snort

Číž, Lábaj, Podhradský and Londák (2012), have proposed in their experiment a model focused on DoS attack in order to cause a malfunction in Asterisk voice over IP communication software. The authors used the SIP tool, in order to verify the functionality of the detection system and cause anomalies in denial of service attacks, the Snort software tool was also used to detect open network attacks, capable of performing analysis of the Traffic and packet logging on IP networks.

4 DESCRIPTION OF THE PROPOSAL

The present proposal aims at creating a defense method for the IP asterisk over SIP protocol, in order to use embedded devices (Raspberry Pi3, Banana Pi M3 and Orange Pi Plus 2) as shown in image 2. The method will be based on the main attacks that occur in embedded systems, contemplated by authors in related works in diverse bases.

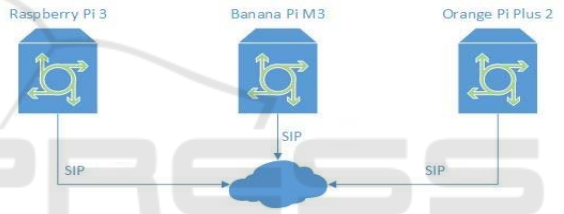

Figure 2: Architecture of the scenario.

With the result of the main attacks, simulations will be made in the device in order to propose security methods.

It will be necessary to study the SIP protocol to verify the vulnerabilities in order to apply the best configuration and defense methods to ensure the security of the device.

In order to achieve the objectives of this research, it will be necessary to elaborate a scenario that makes possible to carry out all the experiments as close as possible to a real production environment, so the scenario should include three low cost embedded devices already configured with the system, which must be directly connected to the Internet.

5 EXPECTED CONTRIBUTION

This proposal presents as main contribution the elaboration of a security method for a VoIP communication central in an embedded device using the Asterisk system.

With the development of this proposal we intend

to obtain the following contributions: to survey the main techniques used to attack the communication systems, to survey the tools and materials necessary to simulate the most significant attacks on embedded devices; to perform a literature review of the SIP protocol, to analyze the vulnerabilities of the SIP protocol, to propose a defense for these attacks, to write the dissertation and present the results of the security analysis on the devices shipped with Asterisks.

REFERENCES

Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., and Cayirci, E. (2002). Wireless sensor networks: a survey. *Computer networks, 38(4):393–422.*

Ball, Stuart - ”Embedded Microproceessor Systems: Real Woard Desing”, *3º edition,* Editora:Mcpros, EUA, 2005.

Barbosa, Camila Soares. *Voz sobre IP em Redes Locais sem Fio*. CEFET – Centro Federal de Educação Tecnológica de Goiás. Goiânia, (2006).

Barr, M. (1999). *Programming embedded systems in C and C++*. O'Reilly.

Carro, L. and Wagner, F. R. (2003). Sistemas computacionais embarcados. *Jornadas de atualização em informática. Campinas:* UNICAMP.

Číž, P., Lábaj, O., Podhradský, P., & Londák, J. (2012). VoIP Intrusion Detection System with Snort. *In ELMAR, 2012 Proceedings (pp. 137-140).* IEEE.

Cuervo, F., Greene, N., Rayhan, C., Rosen, B., and Segers, J. (2000). *Megaco Protocol Version 1.0 RFC 3015 (Proposed Standrd)*. Obsoleted by RFC 3525.

D. Butcher, X. Li, and J. Guo. Security challenge and defense in VoIP infrastructures. *IEEE Transactions on Systems, Man, and Cybernetics, Part C:* Applications and Reviews, 37(6):1152–1162, November 2007.

DEFSIP. *Definindo o que é um protocolo de sinalização*. Disponível em http://www.gta.ufrj.br/grad/06_1/SIP/Definindooqueumprotocolodesinalizao.html, acessado em 27 nov 2016.

Lomotey, R. K. and DETERS, R. (2014). Intrusion Prevention in Asterisk-Based Telephony System. In 2014 *IEEE International Conference on Mobile Services, pages 116–123*.IEEE.

Marwedel, P. (2011). Embedded system design. Springer.

Nakamura, Emílio T.; *GEUS, Paulo Lício de. Segurança de rede em ambientes corporativos.* São Paulo: Novatec Editora, 2007.

Raake, *A. Speech quality of VoIP: assessment and prediction. [S.l.]:* John Wiley & Sons, 2007.

Rehman, U. U. and Abbasi, A. G. (2014). Security analysis of VoIP architecture for identifying SIP vulnerabilities. *In 2014 International Conference on Emerging Technologies (ICET), number i, pages 87–93*. IEEE.

Reis, Claiton – *"Sistemas Operacionais para Sistemas Embarcados",* Tutorial, Editora: EDUFBA, BRASIL, 2004.

Silva, Adailton. Qualidade de Serviço em VoIP – *Rede Nacional de Ensino e Pesquisa.* Maio/2000 – Disponível em: http://www.rnp.br/newsgen - Acessado em 18/11/2016.

Siqueira, Tórgan Flores de ; Menegotto, C. C. ; Weber, T. S. ; César Netto, João ; Wagner, F. R. . Desenvolvimento de Sistemas Embarcados para Aplicações Críticas. In: *Escola Regional de Redes de Computadores, 2006, Passo Fundo*. Escola Regional de Redes de Computadores. Porto Alegre : Sociedade Brasileira de Computação, 2006. v. 1. p. 1-10.

Sitolino, Cláudio Luiz., Voz sobre IP – *Um estudo experimental 1999.* http://www.inf.ufrgs.br/pos/SemanaAcademica/Semana99/sitolino/sitolino.html. Acessado 16/08/2016.

Stallings, W. (2008). *Criptografia e segurança de redes: princípios e práticas.* PRENTICE HALL BRASIL.

Stapko, T. (2011). Practical Embedded Security: Building Secure Resource-Constrained Systems. *Embedded technology series.* Elsevier Science.

Thermos, P.; Takanen, A. *Securing VoIP networks: threats, vulnerabilities, countermeasures.* Boston: Pearson Education, 2007.

Walker, J. Q.; HICKS, J. T. *Taking charge of your VoIP project. [S.l.]:* Cisco Press, 2004.