Study of the security aspect of networks based on SIP and H323 protocols

Ed-daoui Ilyas, Mazri Tomader
Systems Engineering Laboratory, National School of Applied Sciences, Kenitra, Morocco

Abstract
Mainly represented by SIP or H323 VoIP protocols and implementations involve a number of vulnerabilities, particularly related to their complexities and in the face of interoperability of telephony equipments. One of them is the absence of clear standard for negotiating voice encryption keys, resulting in large deployments significant gaps in terms of confidentiality and integrity of conversations and availability service. Our job is to study these protocols dedicated to VoIP applications and offer security solutions to cure the vulnerabilities of these networks.

Keywords:
SIP, H323, VoIP threats, VoIP Vulnerabilities, security.

1. Introduction

The opportunity to migrate from traditional telephony to IP telephony, offered several advantages for businesses, and allowed them to benefit from new services such as video conferencing and data transmission. However, the integration of these services in one platform requires more security.

The attacks on VoIP networks can be classified into two types: internal attacks and external attacks. External attacks are launched by individuals other than those belonging to the same LAN, and they usually occur when VoIP packets traverse an unreliable network and/or the call go through a third party during the transfer of network packets. Internal attacks are made directly on the local network.

There are two main classes of vulnerabilities on a VoIP environment. The first depends on the used protocol (SIP, H323 ...) and the second is connected to the systems where the VoIP is implemented. Each protocol or service has its own vulnerabilities.

2. Threats targeting the VoIP

A VoIP phone call consists of two parts: signaling, which establishes the call and the media stream that carries the voice.

Signaling, managed by SIP transmits the headers and the payload of the packet in plain text, allowing an attacker to read and to falsify packages. It is therefore vulnerable to attacks that try to steal or disrupt the telephone service, and eavesdropping seeking information on a valid user account to make free calls, for example. Signaling uses, in general, the default port UDP/TCP 5060.

The RTP protocol, used for the transport of media flow, also presents several vulnerabilities due to the lack of authentication and encryption. Each header of an RTP packet contains a sequence number that allows the recipient to reconstruct the voice packets in the correct order.

However, an attacker can easily inject artificial packet with a higher sequence number. Therefore, these packets will be broadcast instead of the true packet. The usual threats tale flow of voice are the interruption of transport and eavesdropping.

2.1 VoIP servers localisation

There are several methods for the collection of information here are some of the most used:

Whois servers: Whois services are offered free online to obtain information about a particular field of an email address.

Web site sniffer: If the target has a website , the hacker must travel in search of email addresses , and account passwords or other specific information . Browse the source code can also identify information that could help trace the sources. The sites cleaners automate this research.

Search engines and intelligent agents: A major advantage of Internet search engines is their enormous potential to discover the most obscure details of the Internet. One of the biggest security risks today is the enormous potential of search engines to discover the details on the internet.

Voip network scan: In order to identify each component of the network, you must decipher and understand many packets to recognize for example the IP address and ID.

The necessary tool to scan a network is called a network sniffer. It is a software, used to discover the devices and services in a network.

Manuscript received September 5, 2016
Manuscript revised September 20, 2016

2.2 Threats targeting confidentiality

The most known threat targeting the network's transactions confidentiality is the Eavesdropping. In VoIP network, an attacker typically uses two methods. The first method is the capture session packets from the same broadcast domain as the same direction on the support. The second is a limitation of an accessibility system (e.g., Layer 2 Switch) and sending (duplicating) media development to an intrusion system.

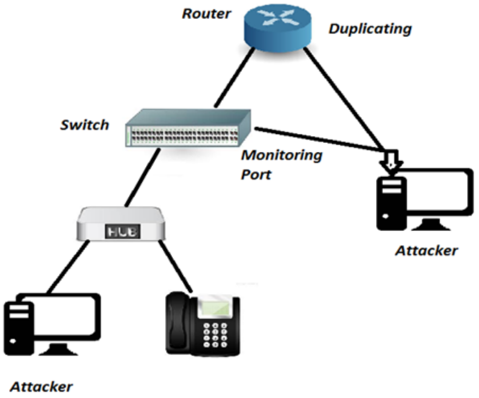


Fig. 1 Different location for an attacker

In figure 1, the attacker device that is in the same broadcast domain as IP phone of a user who has the ability to capture all of the signals through the Hub. The figure also reveals the possibility that external interference can connect to a switch or router, and sets up a monitoring port for audio, video and transmits the same media to capture a jammer sensor.

To intercept VoIP, the scrambler should catch, first, the RTP stream. In a network, an attacker is between the caller and the called party, must employ ARP spoofing. An attacker can easily access the VoIP VLAN, because the phone is usually connected to the computer. After identifying the RTP stream by the jammer, we must find the codec that could also be used to encode voice. To find the codec that could be used to also encode the voice. This information can be found in the PT field (Payload Type) UDP flow field in the MP (Media Format) when SIP change to find format. VoIP calls can be diverted by diverting to a third party with proxy settings called "man-in -the –middle" that is configured to monitor the call.

2.3 Threats targeting integrity

2.3.1 RTP packet injection

This attack is at the LAN / VPN. It targets the server "Registrar" and aims to disrupt an ongoing communication. The attacker must first listen to an RTP stream of the caller to the called, analyze its content and generate an RTP packet containing a similar header but with a larger sequence number and timestamp so that packet is reproduce until the other packages (if they are really reproduced). So communication will be disrupted and the call will not complete successfully.

To perform this attack, the attacker must be able to listen to the network to locate and identify communication and timestamps of RTP packets.

2.3.2 Caller ID Spoofing

Caller ID is usually a service provided by most telephone companies reveals that users phone number of an incoming call. Caller ID Spoofing is the setting of Caller ID on outgoing calls to a 10-digit number of the choice of the caller. Several websites provide a service Caller ID Spoofing eliminating the need for any special hardware. The list includes www.spooftel.com, www.telespoof.com, www.callnotes.net, www.spoofcard.com, etc.

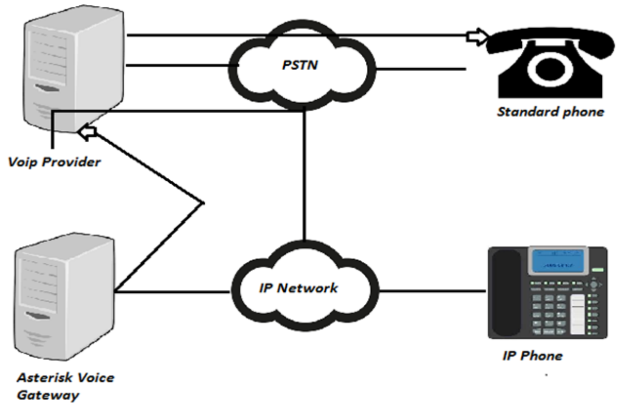


Fig. 2 Caller ID Spoofing

2.3.3 Proxy Impersonation

Proxy Impersonation bypasses the victim to communicate with a proxy created by the attacker. Once an attacker impersonates a proxy, he has complete control of the call.

The attacker deceives the caller to end it communicates with its server instead of communicating with a legitimate proxy. Proxies usually communicate with other proxies. The attack can succeed through several techniques, including DNS spoofing, ARP spoofing, spoofing Cache, DHCP spoofing or completely change the proxy address for a SIP phone.

2.4 Threats targeting availability (DoS attacks)

The applications of Voice over IP (VoIP) and Unified Communications (UC) is based on IP networks. This means that these real-time communication applications are vulnerable to DoS attacks that same data applications. However, the complexity of the protocols used to run these applications also make them vulnerable to a series of DoS attacks entirely new.

Submerging systems differently, these attacks based on sending requests at a volume that can not be distinguished from normal traffic.

VoIP and UC systems are also targets of attacks by flooding, but the success threshold of a DoS attack is much lower than for a data application.

3. Vulnerabilities related to infrastructure

A VoIP infrastructure is composed of IP phones, Gateway server (proxy, registrar, etc.). Each item, either an embedded system or a standard server running on an operating system, is accessible via the network like any computer; and can be attacked or used as a launching point for a deeper attack.

3.1 Weaknesses in the configuration of VoIP devices

Several devices of VoIP in their default configuration can have a variety of TCP and UDP ports. The services running on these ports may be vulnerable to DoS attacks or buffer overflow.

If the available services are not configured with a password, an attacker can gain unauthorized access to this device.
Several of VoIP devices are configured to periodically download a configuration file from a TFTP server or by other mechanisms. An attacker can potentially divert or mystify this connection and fool the device will download a malicious configuration file instead of the actual file.

3.2 IP phones

A hacker can compromise a telephony over IP device, such as an IP phone, a softphone or other programs or hardware client. Generally, it gets the privileges that allow it to fully control the functionality of the device.

Compromising an endpoint (IP phone) can be done remotely or by physical access to the device.
To compromise the availability of the endpoint, for example, it can automatically reject all call requests, or, eliminate trigger notification such as a sound, visual notification to the incoming call. Calls may also be interrupted unexpectedly.

The acquisition of unauthorized access over an IP telephony device may be the result of another element compromise on the IP network, or information collected on the network.

3.3 Servers

A hacker may target the servers that provide the IP telephony network. Compromising such an entity generally will jeopardize the entire phone network whose server part. For example, if a signaling server is compromised, an attacker can completely control the signaling information for different calls. This information is routed through the server compromise. Having control of the signaling information allows an attacker to change any parameter on the call.

If an IP telephony server is installed on an operating system, it can be a target for viruses, worms, or any malicious code.

4. Proposed solutions for VoIP network security

4.1 Securing the transport layer: SRTP

VoIP datagrams are usually transported using RTP. SRTP is an RTP profile that aims to provide authentication and confidentiality to the message, and strengthen the protection of RTP data and control traffic. SRTP uses a unique passkey (symmetrical) to get the hardware input via a secure cryptographic hash function.

In SRTP, a cryptographic context refers to the state of cryptography information maintained by the sender and receiver for the media streams. This includes the master key, session key, encryption identifiers and authentication algorithms of the message, the session key lifetime and a RollOver Counter (OCR).

A cryptographic context for SRTP is identified by the triple (SSRC, the destination address, port of destination).

Moreover, for data encryption, SRTP uses a single algorithm, Advanced Encryption Standard (AES).

SRTP uses a secure cryptographic pseudorandom function (PRF) to generate encryption, Master Salt and authentication session keys from the master key and the packet sequence number. The sender selects the packet sequence number. The master key and Master Salt are derived by applying HMAC, rigged with the material received by the key exchange protocol.

4.1.1 SRTP packet

SRTP packet format is almost the same RTP packet format. The SRTP packet header is identical to the RTP, but with two new optional fields: MKI and authentication tag. Figure 3 shows the SRTP packet format.

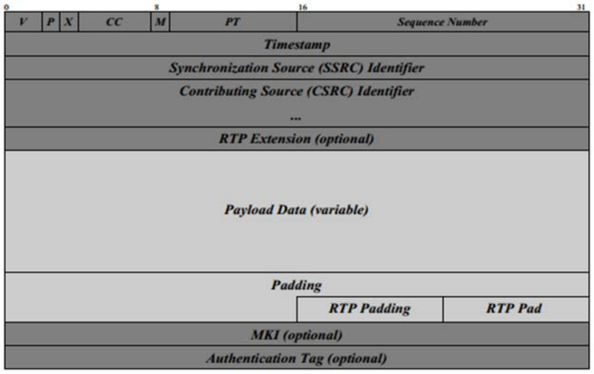


Fig. 3 SRTP packet format

In the figure, the dark gray field at the top of the packet corresponds to the header SRTP (identical to the RTP header). The gray part of the packet is the payload, which is the part covered by the encryption operation (this part is also known as the "encrypted part"). The MAC message authentication operation calculates the above these two parts and locations This Mac from the authentication tag (Tag Authentication).

The new optional fields are placed at the end of the packet. First, the MKI field is used by the key management protocol. It identifies the master key from which session keys were derived. It can be used during the re-entry to identify a master - especially key in the cryptographic context. Initially, since the master key will be shared by both SRTP and SRTCP. Both users are expected to share the master key, which has an indefinite life.

Only the RTP payload is encrypted (called encrypted part), along with the possible padding, if necessary, of the payload. To provide a confidentiality RTP header, political "end-to –end" should be considered.

4.1.2 SRTCP packet

SRTCP adds four new fields in RTCP packet. These are SRTCP index, an encryption flag (referred to as S -flag), the authentication tag, and the MKI; Only the latter is optional. As it is a control protocol, authentication of messages must be ensured, and that is why the "Authentication Tag" field is mandatory.

The encrypted part of SRTCP package consists of the payload consists of the equivalent encrypted RTCP packet. The sworn portion consists of the entire equivalent RTCP packet, the E -Flag, and the index of SRTCP after all encryption applied to the payload. Figure 4 shows the packet format SRTCP. The SRTCP header is the same as the RTCP packet.

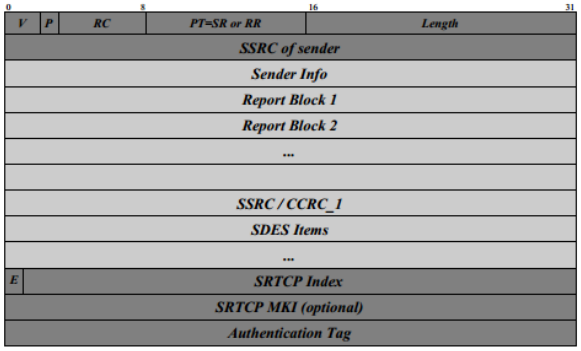


Fig. 4 SRTCP packet format

The dark gray colored portion at the beginning of the packet corresponds to the header of SRTCP. The encrypted part is the light gray part of the package, while the authentication coverage includes the entire package except SRTCP MKI and, of course, the Authentication - Tag itself, where the MAC is stored.

The index of SRTCP is a 31-bit counter explicitly included in the package SRTCP (note that the index of SRTP was made implicitly in the SRTP packet). Its value must be zero before the first packet is sent and increased by 1 modulo 231 after each packet is sent. We should keep in mind that while it would be recaptured, this index should not be reset.

4.1.3 Authentication and message integrity

Authentication and message integrity are ensured by the calculation and verification of the Authentication Tag , optional for SRTP traffic but mandatory for SRTCP packages.

For SRTP data, the sender computes the MAC authenticated portion of the chained with the ROC parameter, and adds to the package. The receiver checks the tag by performing a new message authentication and calculation of integrity on the same parameters using the same algorithm and compares it to that associated with the received packet. If the two are equal, the message is valid, and if not, then the receiver must reject this package, record the event, and an audit message “authentication error” is returned in the side of the receiver .

This procedure is almost identical for SRTCP traffic, with only one difference: since the ROC parameter is missing for the control protocol, the tag will be calculated only on the portion authenticated.

4.1.4 Encryption

The algorithm used to encrypt the RTP payload is AES, and two different modes of operation are specified: Counter Mode (AES - CM) and f8 Mode (AES - f8). The first mode is mandatory to implement.

We should also consider the null - Cipher encryption algorithm, as it is also mandatory to implement. It will be used in the absence of RTP or RTCP for securing.

5. Transport Layer Security (TLS)

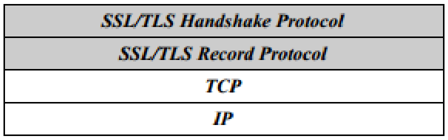
Transport Layer Security (TLS) is the IETF standard for version 3 of Secure Socket Layer (SSLv3), developed by Netscape mainly to protect traffic World Wide Web, so that the protocol may also be referred to as SSL/TLS.

TLS is between the application layer and TCP in the Internet protocol stack, and has been designed to provide a secure and reliable service throughout.

TLS is designed to secure the end to end associations, and it is closely related to the use of public key infrastructure (PKI), therefore, it is bound to the public key cryptography. The establishment of a PKI infrastructure to support TLS gives us an important advantage of TLS IPSec: unlike IPSec, TLS can provide strong authentication (mutual) peer entities solidly associated with TLS and management key because TLS defines a protocol in which the entity suffered a chained encryption suite (for more confidentiality and integrity), established necessary key material and authenticates each other. Regarding applications, they must be slightly modified to support the TLS service.

5.1 SSL/TLS architecture

As said above, TLS is designed to make the use of secure and reliable TCP, and consists of two layers of protocols: Registration protocol and negotiation protocol, as shown in Figure 5.



SSL/TLS Handshake Protocol

SSL/TLS Record Protocol

TCP

IP

Fig. 5 SSL/TLS architecture

The Record Protocol provides basic security services to higher-level protocols such as Hypertext Transfer Protocol (HTTP), while the encryption protocol provides negotiation, key management, and mutual authentication between the entities involved.

5.2 SSL/TLS record protocol

The registration protocol TLS connections provides two basic security services:

Confidentiality: Using Conventional Encryption loads, based on a shared secret key defined by the negotiation protocol .

Integrity: using a message authentication code (MAC) based on a second shared secret key, also defined by the negotiation protocol.

The overall operation of the SSL / TLS record protocol is shown in Figure 6.

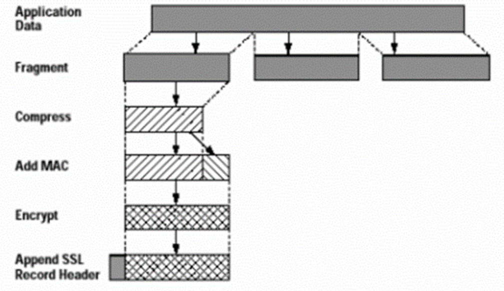


Fig. 6 Overall operation of the SSL/TLS protocol

The recording protocol takes application data to be transmitted and breaks up into manageable blocks (214 bytes), optionally compresses the block 13 calculates a MAC on the compressed data (TLS standard defines the use of HMAC), and encrypts the Message plus the MAC calculated using symmetric encryption (in light gray in Figure 7). The most important is defined as the cryptogram allows DES and 3DES. Finally, the registration protocol adds a specific registration header for SSL/TLS of each block (dark gray in the figure below). This header contains the following fields:

- Content Type (8 bits)
- Major Version (8 bits)

- Minor Version (8 bits)
- Compressed Length (16 bits)

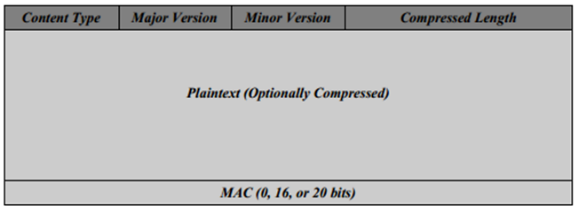


Fig. 7 SSL/TLS recording blocks format

6. Additional security and best practices

6.1 Software security

Several methods can be used to secure the application; these methods vary according to the type of application (server or client). To secure the server requires:

- The use of a stable release, It is well known that any unstable implementation probably contains errors and vulnerabilities. To minimize risk, it is imperative to use a stable release.
- Test software's updates in a test lab. It is very important to test any update of the application in a test lab before applying them to the system in production.
- Do not test patches on the server itself.
- Do not use the default configuration that is used just to establish calls. It contains no protection against attacks.
- Do not install a client application on the server.

Some parameters should be applied selectively. These settings increase security of the application, you can enable or prohibit the general configuration of the application, as can just use the parameters needed for definite clients and depending on the course need. These parameters generally protect against denial of service and these different variants. It is advisable to use the settings that uses hashing passwords, and it ensures confidentiality.

6.2 Operation System Security

It is very important to secure the system that is implemented VoIP server. Indeed, if the system is compromised, the attack can spread on the server application. This may affect the configuration files containing information on registered clients.

There are several security measures taken to protect the operating system:

- Use a stable operating system . New versions still contain bugs and flaws that must be corrected and controlled before .
- Update the operating system by installing security patches recommended for safety.
- Develop complex and robust passwords. They are fundamental against intrusion. And they should not be birth dates , names or telephone numbers . A password should be long enough to form a combination of letters , numbers and punctuation .
- Do not run the VoIP server with a user privilege . If an attacker manages to access the operating system via a vulnerability in the VoIP server, it will inherit all the privileges of that user.
- Asterisk in CHROOT : prevent the VoIP server to have full visibility of the tree of the disc, by running in a secure environment that prevents him from freely interact with the system.
- Backing up files remotely log : log files are very large , it is advisable to store them on a remote server.
- Install only the components required: To reduce the threats to the operating system. It is better to install on the machine's operating system and the server.
- Remove all programs, software or things that do not matter and can be a target of attack for accessing the system.
- Strengthen security of the operating system by installing patches that enhance the overall security of the kernel.

You can also use the firewall and/or ACLs to limit access to people definite and close unnecessary ports and leave only the ports used (5060 , 5061 , 4569 ...). The firewall (firewall) is a software or hardware that serves to secure a network or computer against intrusion from other machines. The firewall uses packet filtering system after analyzing the header of the IP packets is exchanged between the machines.

The firewall can be implemented with an ACL is a list of Access Control Entry (ACE) or access control entry giving or removing access rights to an individual or group. ACL will be needed to give rights to many people determined according to their needs and their authorities.

For a VoIP server, it is important to implement ACLs to secure the server by restricting access to unwanted people. For example, only registered agents can send requests to the server. Furthermore, the access control list can be installed on network pares fire or routers, but they also exist in operating systems.

7. Conclusions

VoIP becomes more focused day after day. As we have seen in this chapter, there are several attacks threatening the security of VoIP networks, more infrastructure- related vulnerabilities. But by following some best practices and safety recommendations that we have seen in this paper we can create a well-secured network.

References

[1] Aditya Dakur, Shruthi Dakur, “Eavesdropping and Interception Security Hole and Its solution over VoIP Service”, IEEE 2014.
[2] An Overview on Security Analysis of Session Initiation Protocol in VoIP network International Journal of Research in Advent Technology, Vol.2, No.4, April 2014 E-ISSN: 2321-9637.
[3] Butcher, D., Xiangyang Li, Jinhua Guo, "Security Challenge and Defense in VoIP Infrastructures," Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions vol.37, no.6, pp.1152, 1162, Nov.2007.
[4] Sipera Systems, “DoS/DDoS Attacks and Protection on VoIP/UC”, 2008.
[5] Internet Security Systems, “Multi-layered Security Solutions for VoIP Protection”, 2005.
[6] Igor Jouravlev, “Mitigating Denial-of-Service Attacks on VoIP Environment”, The International Journal of Applied Management and Technology, Vol 6, Num 1, 2009.
[7] Gaston Ormazabal; Sarvesh Nagpal; Eilon Yardeni; Henning Schulzrinne, “Secure SIP: A Scalable Prevention Mechanism for DoS Attacks on SIP Based VoIP Systems”, 2008.
[8] Niccolini S., Garroppo R.G, Giordano S., Risi, G; Ventura, S., “SIP Intrusion Detection and Prevention: Recommendations and Prototype Implementation”, In: IEEE Workshop on VoIP Management and Security, April 2006).
[9] SANS Institute InfoSec Reading Room, “Security Issues and Countermeasure for VoIP”, 2007.
[10] Prateek Gupta; Vitaly Shmatikov, “Security Analysis of Voice-over-IP Protocols”.
[11] D. Richard Kuhn; Thomas J. Walsh; Steffen Fries, “Security Considerations for Voice Over IP Systems”, Recommendations of the National Institute of Standards and Technology.
[12] McAfee Intel Company, “Protect your VoIP/SIP Servers”, 2011.
[13] designDATA, “Top Ten Security Issues Voice over IP (VoIP)”, White paper series, 2010.
[14] LMLabs, “Combating Denial of Service Attacks for VoIP and Unified Communications”, October 2014.
[15] Alex Talevski, Elizabeth Chang, Tharam Dillon, “Secure Mobile VoIP”, International Conference on Convergence Information Technology, 2007.

Ed-daoui Ilyas Received the Master’s Degree in Information System Security 2015 in the National School of Applied Sciences, Kenitra, Morocco, and the Bachelor’s Degree in software engineering in Med V University, Rabat, Morocco.

Tomader Mazri Received the Ph.D. degrees in Microelectronics & Telecommunication from FST-Fez and of the National Institute of Posts and Telecommunications in Morocco 2012, Master’s Degree in Microelectronics & Telecommunication systems 2007, Bachelor’s Degree in Telecommunication 2005. She is currently a professor at the National School of Applied Sciences, Kenitra, Morocco. His major research interests microwave system and antennas.