Algerian Journal of Research and Technology
https://doi.org/10.58681/ajrt.23070201
A.J.R.T Volume 7 (N°2) (2023) 1 - 12

Involved Security Solution in Voice over IP Networks

K. Belbachir[1], R. Tlemsani[1]

[1]*Computer Sciences Department, University of Science and Technologies of Oran Algeria.*

Corresponding author: tlemsani.redouane@gmail.com;redouane.tlemsani@univ-usto.dz

Received. Juin 25, 2023. Accepted. July 29, 2023. Published August 16, 2023

DOI: https://doi.org/10.58681/ajrt.23070201

Abstract. In this paper, the work involves setting up a secure VoIP solution. At first, we presented some attacks scenarios affecting confidentiality, authenticity and integrity in the VoIP network. In the second part, we focused on VOIP security themes, so our work has focused on areas where enhancing VoIP security is essential. The convergence towards everything of IP is now a reality. The efforts made by infrastructure providers, whether fixed, mobile, and cabled or wireless. This is also evident in operators who now only design the services they offer in the context of everything IP. But with the increasing use of Voice over IP (VoIP) technology, services and protocols are becoming increasingly vulnerable. In this context work several organizations that promote the research and development of network security, warn users of the attacks risks that may affect the communications confidentiality. This work proposed to explore the security vulnerabilities associated with VoIP networks and to present some solutions to avoid and minimize these threats.

Keywords. Ignition time, Residence time, Incident heat flux, Vegetation.

INTRODUCTION

The opportunity to migrate from traditional telephony to IP telephony, has offered several advantages for companies, and allows them to integrate in the same network data and telephony services with a minimum cost of administration and communications, with minimization in the cost of administration has, greater flexibility and adaptability, and to benefit from a new services one of the main services is Voice over IP (VoIP).

Voice over IP is a telephony service offered over a telecommunications network, public or private, using mainly the IP network protocol. It defines the use of "Internet" to route Phone calls from one person to another. However, the major problem of this technology, which is not yet avoided, is the numerous attacks and risks in the IP network in terms: Protocol, software, operating system, physical infrastructure and human error.

These attacks are already present in conventional telephony, But the use of an IP network makes them more easily realizable (Remote access and wide spread of attack tools) and less costly immediately above the abstract; it sets the column format.

Today, several efforts have already been made to define security solutions for IP telephony. Recommendations have been established for the consolidation of architectures and implementation of protocols to maximize the level of security to apply to VoIP flows.

ATTACKS ON VOIP

As any technology, the VoIP has security issues aiming its communication protocols or services. The VoIP attacks can be classified into three categories: attacks against signaling, attacks against media transfer and attacks against supporting services (Fig. 1) (Dabbebi, 2013).

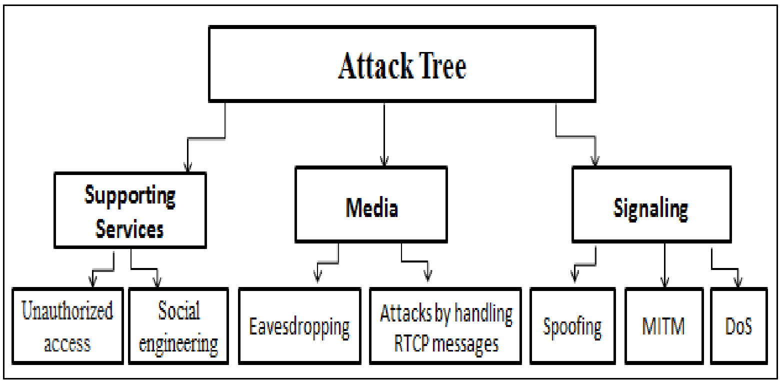

Fig. 1. Attacks Classification.

Attacks against signaling protocols

Denial of Service attack

In context of a VoIP solution, network elements such as IP phone, operating system, application, etc. can be attacked by through attacks called Denial of service (DoS) (Fig. 2).

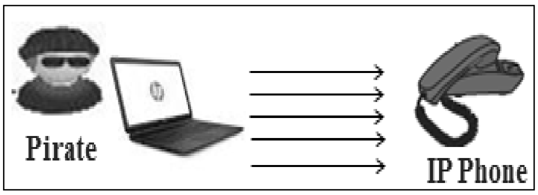

Fig. 2. Denial of Service attacks.

These attacks are under several forms. The most classic are those aiming the use of the entire available bandwidth or to abuse intrinsic TCP/IP problems (Fischbach, 2004). They aim to make damage (temporary shutdown, calls malfunction…) to the VoIP networks.

A DoS attack can be carried out at several levels:

- IP Flooding (Network layer): The goal is to send a large number of IP packets to the same destination so that the processing of these packets prevents a network entity (a router or the receiving station) from processing legitimate IP packets;
- UDP Flooding Attack (Transport layer): The principle is to send a multitude of UDP (User Data Protocol) requests to a machine. This attack type is able to promptly confuse and overwhelms the traffic transiting on the network and thus disturb the

most bandwidth. Almost all SIP (Session Initiation Protocol) devices work above the UDP protocol, making them a target;

- TCP SYN floods: Is an attack aiming the TCP (Transfer Control Protocol) protocol and more precisely the connection establishment phase. The attack consists of sending a large number of SYN packets. The victim will then respond with a SYN-ACK acknowledgment message. To complete the TCP connection, the victim will then wait for a period of time the response through an ACK packet. This is the heart of the attack because the final ACKs are never been sent, and then the system memory fills up quickly and consumes all resources available for these invalid requests. The final result is that the victim will not be able to distinguish between fake SYN and legitimate SYN of a real VoIP connection;
- SIP Flooding (application layer): In the case of SIP, a DoS attack can be directly conducted against the end users, or against the servers involved in the process, using the SIP protocol mechanism (Kuhn, 2014);

  We find three categories of SIP flooding attacks. The first category consists of flooding with correct SIP messages. This involves sending a large number of SIP messages such as SIP INVITE to perform a denial of services against a SIP terminal or proxy. The second category consists of flooding with malformed messages to bring down servers and the third category consists in sending malformed messages exploiting specific vulnerabilities (Zhang et al., 2017).

Attacks Man in The Middle

When there are no strong authentication mechanisms, many situations allow an attacker to position himself between a caller and a called and listen to their communication. These two interlocutors communicate and none of them can doubt that the channel of communication between them was compromised, this is called: the attack Man in the Middle (MITM).

Most MITM attacks consist in listening to the network using a tool called sniffer (Boursali, 2014). All SIP servers such as the proxy and the redirection server can authenticate a SIP client by a cryptographic challenge based on the shared secret (generally the password stored in the server) (Seedorf, 2006). This authentication is usually done in one way only, from the client to the server. The hacker then spoofs the MAC address of both ends by poisoning the ARP cache of the switch in order to be transparent in these exchanges. For example, two computers trying to engage (Fig. 3).

- The SIP client Keltoum sends an INVITE message to its SIP proxy server;
- The attacker intercepts the message and sends a forged response to Keltoum leading to its physical address;
- Since it did not authenticate the proxy server, the SIP client accepts the response and redirects the call tow the attacker;
- The true SIP proxy can be neutralized by a denial of service or exploiting a competition situation;
- At the same time, the attacker replaces the location of the sender with his IP address. Then, he sends the falsified message to the receiver Ahlem.

Thus all communication to Keltoum or Ahlem will pass through the pirate. The latter can thus intercept all traffic, namely sensitive information such as passwords (Dabbebi, 2013).

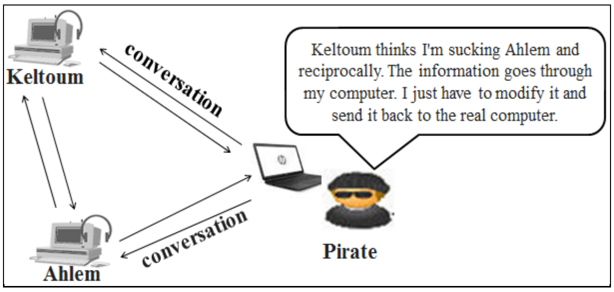
Keltoum
conversation
Keltoum thinks I'm sucking Ahlem and reciprocally. The information goes through my computer. I just have to modify it and send it back to the real computer.
Ahlem
conversation
Pirate

Fig. 3. Man In the Middle Attack.

Spoofing attacks

The Spoofing is one of the major attacks on the authentication of an individual (LoPucki, 2001). It refers to the stolen identity from a SIP client by the listening to SIP traffic or acquiring via another route of the couple (user name and password) (Sisalem et al., 2009).

This is the possibility that a person trying to take over the virtual account of another person, organization or company in order to retrieve necessary information such as the identifier and the password and get access to personal information, including bank accounts, and credit cards numbers, etc.

Identity theft can be done by MITM attack type, the attacker places himself between the SIP user and the access point, and he follows the exchange of the traffic between them and retrieves back the authentication coordinates. And he can record and modify the transmitted data at will.

There are some types of usurpation such as: spoofing e-mails, spoofing WEB, and spoofing IP address, etc.

The latter is the best known. It consists in sending IP packets with an unsigned address to the sender (Bellovin, 1996). The goal may be to hide its own identity in an attack on a server, or to spoof somehow the identity of another device on the network to access the services to which they has access. And this is done in two different ways:

- The first utility is the falsification of the source of an attack. For example, during a DoS attack, the source IP address of sent packets will be forged in order to avoid locating the attack source allowing the attacker to be anonymous (Senet, 2010);
- The second use allows exploiting a trusted relationship between two machines through their IP addresses to take control of one of the two. That is the only authentication made at the level of the waiter consists of a check of the IP address of the customer. That is, the only authentication made at the server levels a verification of the IP address of the client. For example: the client has established a connection to the server with a user authentication based on IP address, the hacker will try to impersonate the client to the server. To do this, he will prevent the client from interacting with the server and responding in his place.

Attacks against media protocols

Eavesdropping

Eavesdropping is a technique that has an impact on the data confidentiality. It refers to unauthorized monitoring, which may intervene on the VOIP network in order to listen to or record a conversation in progress.

Several tools can be used to perform this attack, such as VOMIT (Voice Over Misconfigured Internet Telephones) and Wires hark. The latter converts sniffed packets into a .wav file that can be replayed with any sound files player (Fig. 4) (Bouzaida, 2011).

The attacker get access to the physical network and uses tools to spy directly on the cables. He can do this between a UA and a switch or between two switches. He can then replay on the contents of packets (Schulzrinne et al., 1996).
The principle of the eavesdropping is shown as follows:

- Determine the MAC addresses of the victims (clients and server) by the attacker;
- Sending unsolicited ARP (Address Resolution Protocol) requests to clients and the server, to inform them of the change in the address MAC (Media Access Control);
- Disable checking MAC addresses on the attack machine so that traffic can flow between the two victims (Benchikh and Mechernene, 2015).

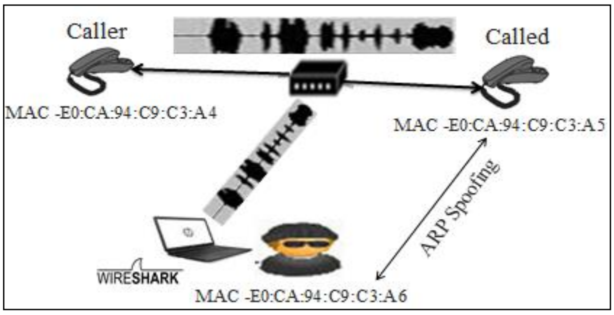

Fig. 4. Attack Eavesdropping.

RTCP messages handing Attacks
RTCP (Real Time Control Protocol) is a protocol integrated into RTP (Real Time Protocol). It regularly transmits control packets containing various statistics between participants in a session. When listening and analyzing traffic, the operation of the RTCP protocol may disrupt, the attacker intercepts the control reports. Then, he modifies the content and parameters in these reports to send false information about RTP exchanges. The receivers use RTCP to send a Quality of Service reports back to the transmitters. These reports contain the number of lost packets, if the attacker sends reports indicating that there is no message loss during the audio conversation, we find messages loss much larger and therefore it makes communication incomprehensible (Dabbebi, 2013).

Attacks against support services

Attack of unauthorized access
The attack of unauthorized access is a category of attack that affects the support service. It involves accessing a service, feature, or network element without appropriate authorization by exploiting the weak points of that element; for example, weak firewall rules, buffer overflow attacks, weak configurations, etc. (Allsopp, 2009).
This type of attack is a critical for telecommunication operators and providers. It can be used to support other attacks, including denial of service attack, and spoofing attack (Dabbebi, 2013).
Social engineering
The social engineering is the ability to abuse or on joy VoIP services for a personal or financial gain (Deuss, 2016).
This type of attack is a critical for VoIP operators and providers and is an important security and privacy concern.
Attackers use various forms to trap their victim, including by telephone, social networks, instant messaging, or e-mail, etc. (Hadnagy, 2011). For example, Phishing e-mails of have a

link to follow for further instructions. This link often leads to a site that seems reliable. But it is generally only a stratagem of more invented by the cybercriminals to steal confidential and sensitive data, such as Social Security number, bank details, etc. (Boursali, 2014).

SECURITY MECHANISMS RESULTS

Many efforts have already been done to define the solutions for VoIP security.

Basic Security and good practices

Going back to our focus on the VoIP security, it is important to lead the security reflection upstream in phase with the design of the architecture of VoIP. The improvement of the levels of security passes, among others, by the respect for good practices and the application of efficient solutions of which here are some examples:

- THE IPBX (Internet Private Branch exchanges), Hard Phones and Soft Phones contain all software. The code of this software can contain faults (buffer overflow) and can be vulnerable to various attacks. It is therefore very important to maintain the version of these software’s up to date, notably when a security fault concerning them is discovered. To do this, you have to regularly consult the sites of the manufacturers of the equipment hardware/software introduced in the VoIP infrastructure, or better, you have to be subscribed to their newsletters in manner which automatically informs you of new version and patch available;
- Do not test the rectifications on the server itself (test the rectifications on the testing equipment); it is very important to test all the software updates in a testing laboratory before applying them on the production system;
- Update the equipment of production if the previous test is decisive (Doswald et al., 2017);
- It is well known that all the unstable applications surely contain errors and vulnerabilities. To reduce the risks, it is imperative to use a stable version;
- Do not install a client application in the server;
- Do not use the default configurations which serve just to establish calls. They do not contain any protection against attacks (Bouzaida, 2011);
- Once the configuration of harp hones/softphones is established, it is important to put in place a real political password to lock this configuration in order to avoid a user modifying the settings (deactivating the authentication, etc.) and to forbid employers from all configuration modifications of the VoIP infrastructure equipment’s (Doswald et al., 2017);
- Suppression of old/useless accounts, suppression of useless software’s and units of IPBX and work stations;
- Put into practice the surveillance and exploitation of infrastructures, etc. On the WAN side, never expose its IPBX to a public IP even if it is "natted", or in a public DMZ (DeMilitarized Zone) and / or directly outside even a specific module for this purpose is proposed (Huré, 2011).

Data Separation and VoIP equipment

The separation of DATA and VoIP equipment allows it to prepare a big part of attacks, notably the attacks concerning the eavesdropping.

Separation on IP level (layer 3)

This choice consists of assigning a group of addresses per network; for a network, meaning a group of addresses for a data network and a group for voice network.

Once this separation is done, it is possible to define ACLs (Access Control Lists) on the devices so as not to allow communications only between allowed IP addresses. This option requires that each network (VoIP or DATA) has its own Dynamic Host Configuration Protocol (DHCP), Domain Name Server (DNS), or Network Time Protocol (NTP) servers. These servers are dedicated to voice, and distinct from data servers to avoid a denial of service that affect the entire network (Huré, 2011).

Separation with VLANs (layer 2)

The second step of our in-depth defense is to define a VLAN DATA (Virtual Local Area Network) dedicated to the network equipment's present in the DATA network and a VoIP VLAN dedicated to VoIP equipment. This is done at level 2 of the OSI model. VLANs can be represented as a logical separation of the same physical network. This logical separation of voice and data flows using VLAN is a highly recommended measure. It must be such as to prevent the incidents encountered on one of the flows from disturbing the other.

In order to achieve better separation, it is advisable to create a VLAN for each category of VoIP equipment, such as VoIP Hard phones VLANs, VoIP Softphone VLANs, and VoIP Servers VLANs instead of the VoIP VLAN (Telephony, 2004).

Exchange between VLANs must be strictly controlled. Devices such as switches or firewalls must be able to filter inter-VLAN traffic. So you should also take precautions on the switches:

- Disable unused ports;
- Place unused ports on an unused VLAN;
- Allow only known MAC addresses;
- Provide for authentication of the machines.

These measures enable the reduction of the broadcast domains thus reducing the traffic on the network, thus releasing more bandwidth for useful applications and reducing processing times on network devices.

Enhanced security can be achieved by implementing inter-VLAN filtering, allowing only users of a VLAN to access it. The risk of DoS can thus be reduced.

Secure access to Switch ports

To protect the network from DoS, or other attacks, access restrictions on networking equipment such as Switches and mandatory servers. This limitation is achieved by managing Access Control Lists to restrict access to sensitive portions of the network by denying packets based on MAC addresses or source and destination IP addresses or TCP / UDP ports.

Port security (prohibit port mirroring, non-active ports will be disabled) may restrict access to an Ethernet port based on the MAC address of the device to which it is connected. This method can also limit the total number of devices connected to a switch port, protecting the switch from MAC flooding attacks and reducing the risks associated with wireless access points or hackers (Remazeilles, 2009).

Authentication

One of the most important methods for anticipating an attack on the telephony system is to clearly determine the identity of the peripherals or the people participating in the conversation, in order to authorize their access to the resources (system, Network, application) (Benchikh, 2015). It allows therefore validating the authenticity of the entities. In the case of the ToIP, this property allows for example a server to verify that it is providing services to a rightful user;

The procedure of authentication of a pair of computer entities consists typically of exchanging the identities (IDTA and IDTB) of a couple of interlocutors (called client / server), two random numbers (RA, RB) form a unique identifier of the session (RA||RB), then to perform a cryptographic calculation (F, a function of the Pseudo Random Function (PRF)). This last product, with the help of a key value (KS), a key master (KM), from which we deduce (with the help of function g, of the type Key Data Function (KDF)) the keys Encryption (KC) and key integrity (KI) allows us to create a secured channel (Urien, 2015).

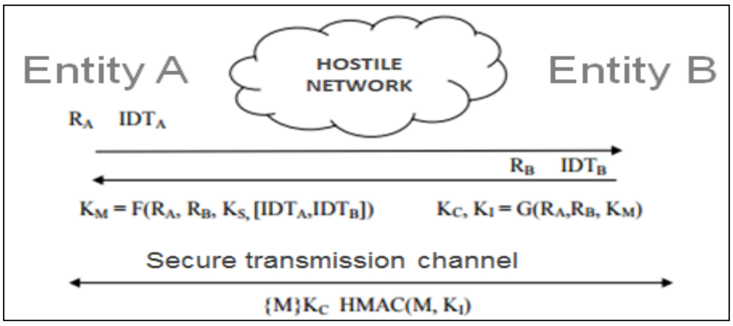
Entity A
HOSTILE NETWORK
Entity B
R_A IDT_A
R_B IDT_B
$K_M = F(R_A, R_B, K_S, [IDT_A, IDT_B])$
$K_C, K_I = G(R_A, R_B, K_M)$
Secure transmission channel
$\{M\}K_C$ HMAC(M, K_I)

Fig. 5. Authentication between two entities.

Encryption

The encryption is a process of cryptography concerns signaling flows (ask to put in relation calling it and the conscript) and media flows (transport of the information). It is an effective means to protect these data. Many solutions can be used: the encryption of the signaling flows with TLS (Transport Layer Security) and SIPS (SIP Secure), the encryption of media flows with SRTP (Secure RTP). The external communications can be also forwarded via VPN (Virtual Private Network) tunnels (Mehadji and Kahouadji, 2013).

TLS Protocol

It is a protocol of security of the exchanges on the Internet at the level of transport layer. Formerly, TLS is called SSL (Secure Sockets Layer), it is a modular protocol which the goal is to secure the exchanges of the data between client and server independently of every type of application. TLS acts as an additional layer over TCP.

TLS works according to a mode client-server. It supplies the following objectives of security:

- Authentication of the server;
- Confidentiality of exchanged data (encrypted session);
- Integrity of exchanged data;
- Optionally, the strong authentication of the client with the use of a digital certificate;
- The spontaneity, that is to say a client can transparently connect to a server to which it connects for the first time (Abdoulaye, 2013).

SIPS protocol

A SIPS is a security mechanism defined for sending SIP messages over the TLS security protocol (Mehadji and Kahouadji, 2013).

IPsec protocol

IPsec (Internet Protocol Security) is a set of protocols designed to secure communications at the network layer of the OSI model between distant sites (Mehadji and Kahouadji, 2013). It was originally developed within the framework of the future version of protocol IP; namely IPv6.

There are two basic protocols defined for IPsec; ESP (Encapsulating Security Payload) and AH (Authentication Header). These two models provide the security, integrity, authentication and anti-replay services (Mehadji and Kahouadji, 2013).

IPsec can operate in two modes; the transport mode and the tunnel mode. The latter aims making the tunneling VPN, that is to say IP encapsulation which allows it among other things to create virtual private networks (VPN). The objective of this technology is to establish a secure communication (the tunnel) between remote entities, separated by an untrusted network, such as Internet.

The main properties of VPNs tunnels are:

- Transmitting data is encrypted (confidentiality) and protected (integrity), that is to say the flow can only be understood by the final receiver and the modification of data by intermediaries can't be possible;
- Both ends are authenticated;
- Source and destination addresses are encrypted;
- They can present (according to the protocol) anti-replay qualities or prevent MITM attacks (Bassil, 2005).

But in practice, IPsec has many problems because it works in the network layer and not in the session or application layer. Indeed, in order to be able to work normally, IPsec must be implemented in the kernel of the operating system either directly compiled or linked as a downloadable module. This protocol is not appropriate for working in any datagram exchange. In addition, if many communications must be encrypted, performance problems may arise (McGrew et al., 2014). Then, it is necessary to look other solutions (the SRTP protocol).

SRTP protocol

SRTP is the secure real-time transport protocol. It defines an RTP profile, which is intended to provide protection against repetition of RTP traffic and control traffic for RTP. SRTP is ratified by the IETF to secure the future multiplication of multimedia exchanges on networks. It covers the gaps of existing security protocols (IPsec), whose key exchange mechanism is too cumbersome (Abdoulaye,2013; McGrew et al., 2014). The main services offered by SRTP are:

- Be able to make confidential the RTP data, whether it is the header and payload or only the payload;

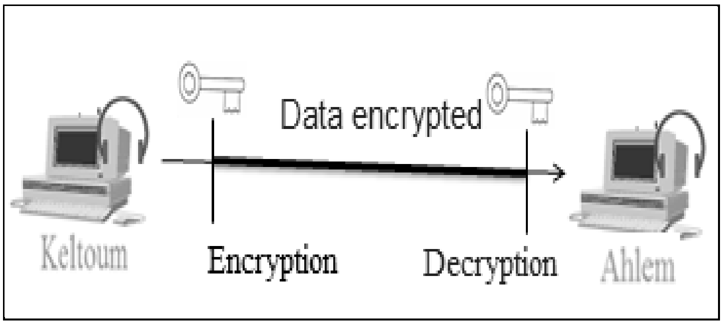

Fig. 6. Data encryption.

- Authenticate and verify the integrity of RTP packets (Fig. 7); the sender calculates an imprint of the message to be sent, then sends it with the same message;

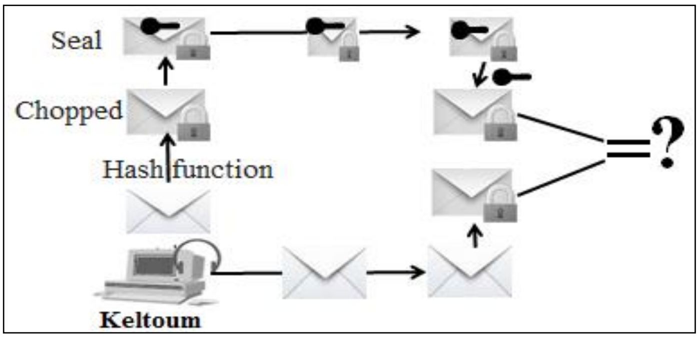

Fig. 7. Transmitter authentication and data integrity.

- Protection against packet replay: each receiver maintains a list of all the indices of received and well-authenticated packets (Kharrat, 2015);
- SRTP is an extension of RTP in which security options have been added. It proposes algorithms which will monopolize at least the resources and the use of the memory. Especially, it makes it possible to render RTP independent from other layers as regard the application of security mechanisms (Fig. 8).

To implement the various security services, SRTP uses the following main components:

- A master key used to generate session keys; the latter will be used to encrypt or authenticate packets;
- A function used to calculate session keys from the master key;
- Random keys used to introduce a random component to counter possible replay or memory effects (Bouzaida, 2011);
- An SRTP packet is generated by transforming an RTP packet through security mechanisms (Fig. 9).

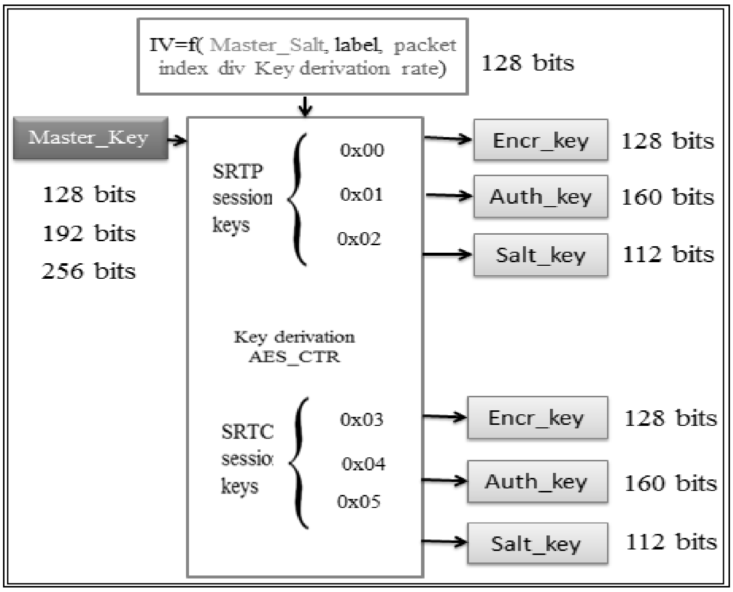

Fig. 8. Generating Session Keys.

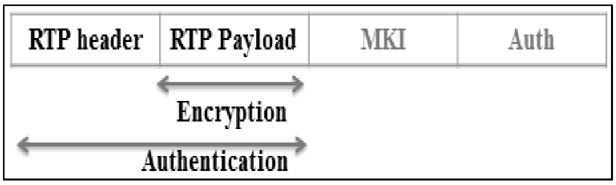

Fig. 9. Format of the SRTP package.

Note that the SRTP packet is realized by adding two fields to the RTP packet:

- SRTP MKI (SRTP Master Key identifier) is used to re-identify a particular master key in the cryptographic context. The MKI can be used by the receiver to retrieve the correct primary key when the need for a key renewal occurs;
- Authentication tag is an inserted field when the message has been authenticated. It provides the authentication of header and data RTP and indirectly provides protection against packet replay by authenticating the sequence number (Benchikh, 2013).

CONCLUSION

It is obvious that VoIP technology is a rapidly expanding service in the world, one of the techniques of recent years among the most promising is becoming a new flagship Internet application with the continued growth of attacks against this technology.

We covered this topic in order to discover the flaws and vulnerabilities of this communication system, and to correct these errors and carry out a modern communication reliable and accessible.

We concluded that the quality of VOIP networks is low especially in the context of using public internet and that their safety is not only a necessity but rather an obligation but be aware that it is impossible to have perfect security at the level of VIOP network and generally on all networks.

Only a rigorous risk analysis can guarantee the success of this VIOP infrastructure to an acceptable level.

Currently, many methods have been developed to secure network infrastructures and communication on the Internet, including the use of firewalls, encryption and private virtual networks (VPN) but these methods remain insufficient.

Therefore, the transition to new strategies more reliable and more efficient to compensate the weaknesses of conventional methods is inevitable.

Finally, our future research work, concerning the security of VoIP networks, by setting up an MPLS solution instead of VPN, and integration of a strong authentication server, using detection methods intrusion and machine learning such as Artificial Neural Networks, and Evolutionary algorithms.

REFERENCES

Abdoulaye, H. M. (2013). Audit d'un réseau VoIP et implémentation d'un client SIP sécurisé, Thesis of Master1 TDSI, University Cheikh-Anta-Diop Dakar, Senegal.

Allsopp, W. (2009). Unthorised Access : Physical Penetration Testing for IT Security Teams. *John Wiley & Sons*. 308.

Bassil, C. (2005). SVSP (Secure Voice over IP Simple Protocol): une solution pour la sécurisation de la voix sur IP, Ph.D. Thesis, Institute of Science and Technology ParisTech, Paris, France.

Bellovin, S. (1996). Defending against sequence number attacks. Technical report, RFC 1948.

Benchikh, A., Mechernene, K. (2015). Etude de la sécurité dans la VOIP, Master Thesis, Dept. Informatique, University of Abou Bakr Belkaid, Tlemcen, Algeria.

Boursali, D. (2014). Une approche à base d'URL pour la détection des sites phishing, Master Thesis, Dept. Informatique, University of Abou Bakr Belkaid, Tlemcen, Algeria.

Bouzaida, R. (2011). Étude et Mise en place d'une Solution VOIP Sécurisée, Master Thesis, Virtual University of Tunis (UVT), Tunis, Tunisia.

DABBEBI, O. (2013). *Gestion des risques dans les infrastructures VoIP*. Thesis. University of Lorraine, France.

Deuss, K. (2016). Mécanismes de Social Engineering (phishing) : étude technique et économique. Thesis of Bachelor, High School of Management (HEG-GE), Geneva, Swiss.

Doswald, A., Ehrensberger, J., Hahn, X. (2017). Best Practice -Sécurité VoIP. Specialized High School of Western Switzerland (HES-SO). 56.

Fischbach, N. (2004). (In)sécurité de la Voix sur IP (VoIP), Actes du symposium sur la Sécurité des Technologies de l'Information et des Communications (SSTIC04). 4-6.

Hadnagy, C., Wilson, P. (2011). Social engineering: The art of human hacking. Indianapolis, Wiley Publishing Inc.

Huré, D. (2011). Attention aux techniques de hack de la téléphonie sur IP!, Journal Du Net(JDN).

Kharrat, B. (2015). Client Peer To Peer Pour Le Streaming Video Securise, University of Versailles-Saint-Quentin-en-Yvelines (UVSQ), Versailles, France.

Kuhn, L. (2014). Voip And Securite: IPS, Ph.D. Thesis, Dept. Informatics, University of applied Sciences, Western Switzerland.

LoPucki, L. M. (2001). Human identification theory and the identity theft problem. *Texas Law Review*. 80, 89–134.

McGrew, D., Carrara, E., Norrman, K., Baugher M., Naslund, M. (2014). Protocole sécurisé de transport en temps réel (SRTP). Technical report, RFC 3711, Cisco Systems, Inc, Ericsson Research.

Mehadji, M., Kahouadji, M. (2013). Conception et installation d'un système téléphonique sur IP basé sur Asterisk pour une entreprise multi sites, Master Thesis, University of Siences and Technology Mahamed Boudiaf, Oran, Algeria.

Remazeilles, V. (2009). *La sécurité des réseaux avec Cisco*. Editions ENI.

Schulzrinne, H., Fokus, G. M. D., Casner, S., Frederick, R., Jacboson, V. (1996). RTP: A Transport Protocol for Real-Time Applications, RFC 1889.

Seedorf, J. (2006). Using Cryptographically Generated SIP-URIs to protect the Integrity of Content in P2P-SIP, In Proc, of the 3rd Annual VoIP Security Workshop (VSW'06), Berlin.

Senet, R. (2010). Attaque par IPSpoofing, Site: http://www.regis-senet.fr.

Sisalem, D., Floroiu, J., Kuthan, J., Abend, U., Schulzrinne, H. (2009). *SIP Security*. John Wiley & Sons

Telephony, D. I. (2004). Voice over IP-Security Technical Implementation Guide ver2.

Urien, P. (2015). Introduction à la Sécurité des Réseaux et des Applications, Institute of Science and Technology ParisTech, Paris, France.

Zhang, G., Ehlert, S., Magedanz, T., Sisalem, D. (2017). Denial of Service Attack and Prevention on SIP VoIP Infrastructures Using DNS Flooding. In Proc. of the Principles, Systems and Applications of IP Telecommunications conference (IPTComm'07).