A Closer Look on Challenges and Security Risks of Voice Over Internet Protocol Infrastructures

Ahmed H. Al Omari[1*], Yazan A. Alsariera[1*], Hussam S. Alhadawi[2], Mahmoud A. Albawaleez[3], Sultan S. Alkhliwi[1, 3]

Corresponding author: ahmed.alomari@nbu.edu.sa | yazan.sadeq@nbu.edu.sa

[1] Department of Computer Science, Collage of Science, Northern Border University, Arar, Saudi Arabia.
[2] Department of Computer Techniques Engineering, Dijlah University College, Baghdad 10011, Iraq
[3] Deanship of Information Technology, Northern Border University, Arar, Saudi Arabia.

Summary
Voice over Internet Protocol (VoIP) has grown in popularity as a low-cost, flexible alternative to the classic public switched telephone network (PSTN) that offers advanced digital features. However, additional security vulnerabilities are introduced by the VoIP system's flexibility and the convergence of voice and data networks. These additional challenges add to the normal security challenges that a VoIP system's underlying IP data network infrastructure confront. As a result, the VoIP network adds to the complexity of the security assurance task faced by businesses that use this technology. It's time to start documenting the many security risks that a VoIP infrastructure can face, as well as analyzing the difficulties and solutions that could help guide future efforts in research & development. We discuss and investigate the challenges and requirements of VoIP security in this research. Following a thorough examination of security challenges, we concentrate on VoIP system threats, which are critical for present and future VoIP deployments. Then, towards the end of this paper, some future study directions are suggested. This article intends to guide future scholars and provide them with useful guidance.

Keywords:
VOIP Security, Attacks, SIP, Confidentiality, Integrity, availability.

1. Introduction

VoIP (Voice over Internet Protocol) has quickly become the de facto standard for Internet-based voice communication. Because VoIP makes use of an existing IP network, it drastically lowers the cost of communication compared to conventional PSTN (Public Switched Telephone Network). VoIP is also an appealing solution for voice communication via the Internet because of its ease of setup and low communication infrastructure [1, 2]. Furthermore, VoIP allows for the creation of customized solutions by allowing for the addition of personalized and value-added services. Hence, the adoption of VoIP communication infrastructure has shifted most of the control within the PSTN's central infrastructure to the end devices.

VoIP refers to a method of sending voice packets over an existing IP network. An IP network, unlike the PSTN, is packet switched. When a phone call is initiated between two parties on the PSTN, a physical circuit is established between the two communicating parties [1, 38]. The parties communicate after establishing the call through the circuit that has been reserved until the communication has ended between the parties. On an IP network, on the other hand, IP packets are used for all communication. When a communication is initiated by a party, the generated analog signals during the call is transformed back to analog signals at the receiving end after being digitized, encoded, and packed into an IP packet at the transmitting end.
VoIP, in addition to the PSTN and cellular networks, adds a third dimension to voice communication. VoIP allows you to make a call to any PSTN or mobile phone anytime anywhere in the world. Although some services require a computer or a specific VoIP phone to operate, others enable a caller to use a regular phone with an adaptor. The conversion of the present circuit switched PSTN to a PSN is expected to be possible with VoIP. Advanced functionalities have begun to emerge as VoIP has gained wide acceptance by most telecommunication provider [3]. The confluence of the voice and digital worlds, on the other hand, brings with it not just opportunities but security risks as well [4, 39].

VoIP security challenges are one-of-a-kind and, in most circumstances, rather complicated. This article seeks to provide a review of VoIP security challenges, covering basic VoIP architecture, current defence protocols and attacks, as well as a prediction for future attacks like SPIT. We'll go through the basic VoIP network architecture in this review to help with the conversation that follows. As seen in Fig 1, the three components of VoIP infrastructure are end user equipment, network components, and a gateway to the conventional phone network. Each of these layers is defined as follows:

Manuscript received February 5, 2022
Manuscript revised February 20, 2022
https://doi.org/10.22937/IJCSNS.2022.22.2.23

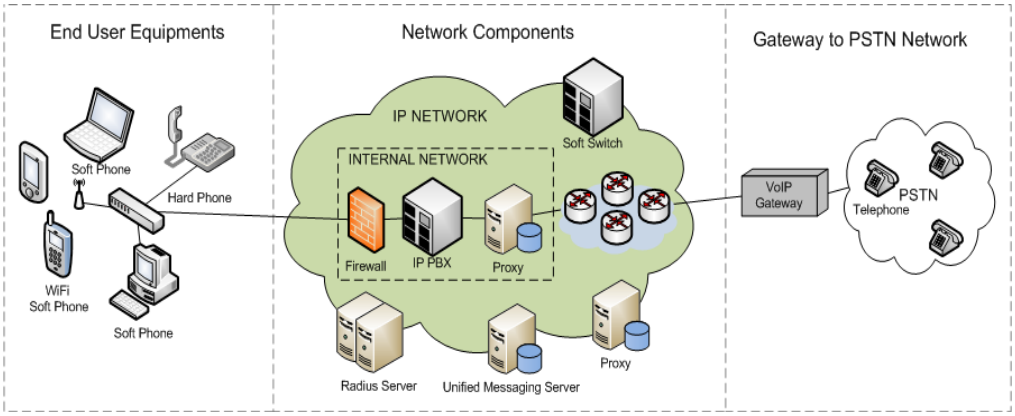


Figure 1. Typical VOIP network

1. End-user equipment: The end-user equipment provides an interface for users to communicate with other end users. Equipment could be "hard phones" with an interface similar to a conventional telephone or a "soft phone," software that emulates a telephone. The security of such end-user components depends upon how they are installed. Mostly, this end-user equipment often deployed in campus networks, at home, or in hotels. Rarely, however, does the equipment have security features built-in, making them vulnerable to exploitable flaws [5].
2. Network components: VoIP typically leverages the existing IP network, which means it inherits its flaws. Each component of the network has its own set of security problems that have emerged in recent years. When voice traffic is added to these components, their vulnerability increases. To ensure the security features specified for VoIP, the IP network components such as routers, firewalls, and switches must be VoIP-aware [6].
3. VoIP gateways: Due to the importance of the gateway in the integration of the IP network with the PSTN, it's necessary to ensure that its security features don't pose vulnerabilities. The role of the VoIP gateway is mainly voice compression/depression, call routing, packetization, and signal management. It is also possible to establish interaction between the VoIP gateways and the external controllers such as H434 Gatekeepers, SIP proxies, network management systems, and Media Gateway Controllers (MGC). Malicious attackers can utilize these interfaces to make free phone calls, making them a possible vulnerability. Any security architecture must be able to promptly and effectively counter these threats [4].

The primary goal of this article is to create a roadmap of existing work in securing VOIP. As well as to identify the gaps in existing research. This article will tackle the VOIP security constraints and requirements. Section 2, VOIP architecture will be presented. Next, section 3, deals with the security concerns in VOIP application. Then, attacks mechanism in VOIP systems will be discussed accordingly in section 4. Finally, the conclusion of the article will be demonstrated in section 5.

2. VOIP Protocols

Before we get into the security difficulties with VIOP, let's go over the foundations of the technology. This will aid us in comprehending the security implications of all VOIP-related protocols. Security was not considered when building VOIP protocols that can be classified as either media transport or signalling protocols.

2.1 Signaling protocols

These protocols can be used to set up signalling services such as initiating or terminating calls. Some examples of these protocols are skinny client control protocol (SCCP), session initiation protocols (SIP), and inter Asterisk eXchange (H.323, IAX). SIP and H.323 protocols before passing it on to the media transport protocols. They provide similar services but take different techniques. SIP utilizes a simple methodology like HTTP, wherein methods such as BYE, FORWARD, and REGISTER are used to start a call. In session setup, H.323 uses a group of sub-protocols such as H.239 and H.245. Furthermore, both protocols rely on supportive servers to establish a connection between two end points. The two protocols use RTP to send audio between two or more end points after establishing a call [7]. The IAX protocol, which isn't as well-known as SIP or H.323, is typically used between 2 asterisk servers. It can be used also for setting up calls between 2 end-locations, as well as voice transfers. As a result, IAX requires no RTP usage for media transfer [7]. The SCCP is used between the Cisco VoIP phone and Cisco call management [8].

2.2 Media Transport Protocol

Media Transport Protocols: In real-time communication, these protocols (such as RTP and RTCP) are used to decode, control, and order voice scripts. RTP is mainly used to provide services such as delivery monitoring, identification of payload type, & time stamping, as well as to establish the structure of the standard packet for transporting video and audio files across IP networks. The RTCP's major purpose is to provide information about the quality of the offered service by RTP [9].

3. Security concerns of VOIP applications

Security measures are defined for the description of the security problems, such as the triplets defined by the Central Intelligence Agency (CIA) which are confidentiality, integrity, and availability. The categorization of each security problem depends on how it affects the VoIP system's confidentiality, integrity, or availability [10, 11]. Confidentiality threats typically reveal the content of a two-party communication, but they can also reveal call data [12]. Threats to integrity jeopardize the ability to trust the caller's identity, the message, the recipient's identity, or the call log. Availability threat puts the ability to make or receive calls in jeopardy [12]. Table 1 illustrates the security concerns in VoIP and their impact based on these 3 metrics.

Table 1. Security threats of VOIP applications

Threats	Confidentiality	Integrity	Availability
Toll fraud	-	✓	-
Accounting data manipulation	✓	✓	-
Alteration of voice stream	✓	✓	-
Eavesdropping	✓	-	-
Denial of service	-	-	✓
Caller ID impersonation	-	✓	-
Unwanted calls and messages	-	✓	✓
Redirection of call	✓	✓	✓

3.1 Toll Fraud

This is simply the situation of an unauthorized user using a legitimate VoIP network [13]. Toll fraud is a severe danger to VoIP networks because it raises the cost of doing business by utilizing its resources. Toll fraud is at the top of the list of threats linked with the fraudulent use of VoIP services, according to research published by the French National Research Agency (ANR) VAMPIRE Project on VoIP/SIP in 2009. Following allegations of stealing £11 million through VoIP toll fraud, 30 members of a criminal group were detained in Budapest and London in 2010. The gang made around half a million calls to premium rate numbers using stolen VoIP account data, and they were paid a percentage of the exorbitant call charges [14]. A service provider in Miami (USA) was also reported to have hacked into the networks of other service providers, diverting his customers' calls onto other networks and receiving payment from his customers [15]. This means that if a hacker gains access to VoIP infrastructure, his or her goal is to dial premium rate numbers, resulting in high call bills.

3.2 Accounting data manipulation

Each call placed through the system is recorded in the accounting database. These call data records (CDR) include information such as the phone numbers from which the call was made and to which it was made, as well as the time of the call, the duration, and other call details [16]. The attacker can observe call patterns by getting access to the CDR database. The attacker could acquire access to confidential information by monitoring the call patterns, such as the pattern of the calls repeatedly made from one company's executive to another company's executive. Also, the attacker could use this data to figure out if a strategic alliance or merger is in the works. It is possible for an attacker to change or delete call records if they get write access to the CDR database.

This could be done to avoid paying for services (toll fraud) or to hide other more serious illegal conducts. Tampering with the call log or changing phone numbers from which and to whom the calls were made, could be a way of concealing various behaviours that can be traced through the call records. The switched telephone network is also vulnerable to this type of attack. The conventional phone network has the benefit of separating the data network which houses the accounting database from the voice network. In a typical setup, the accounting database would most likely be on a private network that was physically isolated from any public networks. The data network serves as the underlying transport for both voice and call data in VoIP networks. When matched with a normal system, call logs protection in VoIP networks requires more effort [17].

3.3 Alteration of voice stream

This is referred to as a substitute or man-in-the-middle attack. The attacker can eavesdrop and manipulate the dialogue between the targeted victims. This involves replaying previously recorded speech to give the receiver a different message from what was sent by the sender [18]. Because human discussions are unpredictable, it may be difficult to utilize this technique to change the entire dialogue between the two parties. However, this might be

used to alter extremely small bits of a conversation. For instance, "no" can be changed to "yes" in response to a question, or "sell" to "purchase" in a financial conversation with an advisor; these would have a significant effect on the meaning of the discussion. When utilized with interactive voice response phone systems, an attacker may also benefit from it. An attacker may launch substitution attack may after collecting the passwords from users that use the interactive voice response system to check account balance after a transaction. A previous balance may be replayed by the attacker to give the victim the impression that no cash had been taken from the account.

3.4 Denial of service

This is regarded as one of the most dangerous attacks. A DoS attack [13]. is described as "an attack on a network system with the intent of causing a service interruption. The SIP is vulnerable to DoS attacks in two ways: (1) the SIP server can be flooded with bulk SIP messages by the attacker, thereby denying legitimate users access; and (2) the SIP requests with malformed SIP header fields can be sent by the attacker to exploit the vulnerabilities of the SIP server [19]. By flooding the network with traffic, attackers can overwhelm the resources of the attacked system and consume all the bandwidth.

Attack on the main network will affect the rest of the network due to the overloading of the routers and their subsequent failure. Owing to the distributed structure of the internet, tracing the source of an attack is extremely difficult; hence, DoS attacks are one of the most well-known issues with VoIP systems. Researchers are devoting a lot of time and effort to developing a solution that can stop or prevent DoS attacks, but so far, they've only had little success [13]. DoS attacks can make it impossible to make or receive phone calls, as well as shut down all operational apps, resulting in the loss of phone service in enterprises and service disruptions. Threats to VoIP security remains the most significant attack on service availability as customers can be affected, causing unproductivity due to system downtime [20].

3.5 Caller ID impersonation

Each phone has a unique identification number. The identity of a device can be impersonated to accept or make calls using the faked identity. To launch the impersonation attack, an attacker would need to configure the VoIP phone equipment to be able to use the device identity of the victim. Having done this, the device of the attacker registers with the phone system in a manner that any calls to the impersonated phone number would be forwarded to the attacker's phone. The attacker might then pick up the phone and pretend to be the victim [21]. Also, the attacker can use the faked device to make phone calls. ID of the caller on the phone of the recipient will show that the victim, not the attacker, is calling.

The attacker can also utilize this to mimic the victim. Caller ID information is being used for a variety of applications. Many banking programs now employ caller ID to confirm the customer's identification. An attacker could utilize a spoofing of a victim's phone ID to get access to banking or credit card details [22]. This type of attack is unlikely to affect a typical phone system. For the most part, the switched telephone network's centralized design of phone lines inhibits spoofing of caller ID information. Because of the widespread belief that caller ID can be trusted, applications that rely on caller ID to determine a person's identity have been developed. There is a need for a similar level of integrity in the VoIP-based phone network for it to be generally accepted [23].

3.6 Unwanted calls and messages

Spam is a term used to describe the millions of unsolicited emails that are sent out by an attacker at little or no cost to the recipients. Telemarketing could also use VoIP phone network to send Spam messages over Internet telephone (SPIT)in bulk [24]. To do this, the attacker has to first establish a server farm that has a lists of VoIP phone addresses. These servers establish connection with the addresses and send out many messages that can be either played over the victim's phone or left in the voice mail box of the victim. Telemarking has been shown to be irritant in the switched telephone network. New legislation to phase out traditional telephone from telemarketing lists has been drafted. The good attributes of VoIP, such as low cost, no legislation, and high throughput has made it suitable for telemarketing. Hence, the growth of VoIP adoption can be curtailed by an explosion in SPIT.

3.7 Redirection of call

Flexibility and a large feature set were two main design goals of the VoIP system. The ability to divert any phone number to wherever the owner is located, is a sophisticated feature that allows callers to quickly locate the person they are seeking for by simply calling a single phone number. If an adversary compromises the redirection functionality, this rich feature may become a possible risk as the victim's phone number can be diverted by an attacker to any address they want, perhaps allowing them to impersonate the victim by redirecting their calls elsewhere [19]. This feature is not yet available in the traditional phone systems, aside from simple call forwarding. A number of new features in VoIP network will provide a range of tools for end users to increase productivity while also providing opportunities for attackers to exploit [20].

4. Attack mechanism in VOIP

Table 2 summarized the classification of threats to VoIP systems into specific attack vectors that disrupt the system and the attacked system layer. In this table, the "Layer" column indicates the attack location within a data transmission network's system structure. Other classifications can place these attacks at end nodes (cellphones or PCs), servers, or other locations of the network. However, when compared to such a location categorization, the layer will represent a more accurate classification in this table. An attack mechanism leveraging OS vulnerabilities, for example, could occur at a terminal, server, or other areas of the network. This form of attack, on the other hand, occurs entirely at the application layer. This section will go through the attacks that are specific to VOIP apps and are crucial to VOIP security. General attacks on IP data networks and PTSN networks will also be covered in this section.

4.1 Physical attack

The attacker can have a significant impact on the system's availability and secrecy by physically altering components of the VoIP network, such as trunk lines, VoIP servers, handsets, etc. By securing the server rooms, wiring closets, and erecting physical barriers to barriers on the locations of the network core areas, the servers, cabling, and switches that make up the VoIP network will not be accessible to anybody except those that has administrative work to do in the system [25].

4.2 Network layer attacks

4.2.1 MAC spoofing

MAC spoofing introduces a new node with a cloned MAC address to the network. This allows the node of the attacker to appear as a legitimate node in the VoIP system in the absence or unavailability of the node that owns the MAC address. One of the most effective defences is to prevent new nodes from connecting to the network without first passing through an authentication step with the port that provides connectivity, as described in the IEEE 802.1xstandard.

Table 2. The impact of potential attacks to VOIP

Attack vector	Confidentiality	Integrity	Availability
Network Layer			
Physical attack	✓	-	✓
MAC spoofing	✓	✓	✓
ARP cache	✓	✓	✓
Data Link Layer			
Malformed packets	-	-	✓
Device IP spoofing	✓	✓	✓
Transport Layer			
TCP or UDP replay	✓	✓	-
TCP or UDP floods	-	-	✓
Application Layer			
DHCP starvation	-	-	✓
TFTP server insertion	-	✓	-
Buffer overflow	✓	✓	✓
Operating system	✓	✓	✓
Viruses and malware	✓	✓	✓
Database attacks	✓	✓	-
ICMP floods	-	-	✓
SIP attacks			
Message modification	✓	✓	-
Cancel/ Bye attack	-	-	✓
Registeration hijacking	✓	✓	✓
Redirect	✓	-	✓
RTP Attacks			
RTP tampering	✓	✓	✓
RTP payload	-	-	✓

4.2.2 ARP cache

The attacker can link the MAC address of the attacker with another IP address in the ARP cache of the victim node by delivering faked ARP packets. The attacker can exploit this situation in the VoIP system to impersonate either an endpoint or a control node [26]. Dynamic ARP inspection (DAI) prevents these attacks by intercepting all ARP packets on the switch, followed by checking the correct IP-to-MAC bindings before either updating the local ARP cache or sending them to the right destination.

4.3 Data Link Layer Attacks

4.3.1 Malformed packets

This is among the well-known examples of how to exploit the flaws of the text-based protocols. SIP headers to cause the malfunction of the proxy servers or User Agents (UAs). attacker actively injects fabricated information (payload) in the SIP message to either crash the system or create parsing overhead, the study by [27] and [28] characterized this technique as a SIP parser attack and SIP message payload manipulation, respectively. The authorization header field, for example, can be used to begin SQL code injection. Malformed message attacks also employ methods such as overflow-space, specific header deletion, overflow null, and the inclusion of non-ASCII code.

4.3.2 Device IP spoofing

This attack impersonates a trustworthy computer by leveraging an internal or external trusted IP address. IP spoofing attacks, according to [29], can be used as a platform for additional attacks, such as a DoS attack where the attacker can mask his identity by using falsified source addresses. When sufficient defence systems are not in place, this might cause the spoofing of the IP-address of the PBX, causing the swamping of the entire voice segment with the UDP packets.

4.4 Transport Layer Attacks

4.4.1 TCP or UDP replay

The attacker can retrieve information such as voice conversations, device authentication, and DTMF (touchtone) information from recorded packets. The collected data can then be uploaded to the network in preparation for a fresh connection. attacker can use the identity of another device to register a device in the system and initiate and receive calls, as well as play back segments of voice or data call [30]. This can be prevented by encrypting the sessions with a distinct sequence number. The encrypted message can only be decrypted by the receiving node; the sequence number is verified to be sure it is the next expected value

4.4.2 TCP or UDP floods

The attacker uses random source addresses and the TCPSYN flag set to send numerous packets to the receiving node, demanding a buffer allocation. Having depleted the buffer space by the attacker, the legitimate users cannot be able to connect to the victim machine [31]. The TCP transport is used by the VoIP signalling protocols (H.323 and SIP) to communicate between the nodes. The possible preventive measures could include properly configured firewalls, implementation of TCP that use SYN cookies, and delivering a SYN-ACK with a properly formed number sequence before allocating the buffer.

4.5 Application Layer Attacks

4.5.1 DHCP starvation

A DHCP request is issued by the attacker for MAC addresses; the IP address data is then modified in the system to prohibit nodes from obtaining IP addresses and force the server to seek IP addresses from another VoIP server. The IEEE 802.1x standard includes a way to protect against such attacks [32, 33].

4.5.2 TFTP server insertion

By taking advantage of the TFTP response race as the phone resets, the configuration of the target phone can be modified. It is possible that a rogue TFTP server can provide false information even before the legitimate server can answer to a request. An attacker can modify the phone IP configuration using this method. A state-based IDS can be used to filter out DHCP server packets from IP Phone ports to allow only valid server communication [34]. It is important that before adopting VoIP systems, organizations should seek for IP Phone instruments that can download signed binary files.

4.5.3 Buffer overflow

These attacks rely on software weaknesses that try to keep more data in a buffer than it was designed to handle. Such excess data overflows into nearby buffers or code, allowing the attacker to take control of the program. This type of attack can be launched against VoIP network control nodes and phone devices [35]. To reduce the danger of buffer overflow attacks, nodes running popular operating systems (Windows, Linux) should be kept up to date.

4.5.4 Operating system

There are numerous known and undisclosed vulnerabilities in the OS platforms that control VoIP network nodes and gateways. Softphones for VoIP phones can be installed on desktop or notebook computers. To reduce the danger of these attack types, the platforms must be updated with the recommended OS patches by the platform suppliers, and platform hardening ought to be considered for the gateway and control nodes.

4.5.5 Viruses and malware

Virus and malware susceptibility can be exploited in the same way an attacker exploits the vulnerabilities in OS platforms. The ability of VoIP network nodes to process call traffic can be reduced if affected by viruses and malware [12]. Antivirus software must be installed and updated on all nodes, in addition to maintaining OS patches current and hardening servers as previously described.

4.5.6 Database Attacks

Control nodes log call activities by storing CDR in commercial databases. The call logs can be exploited using known vulnerabilities in commercial database software such as Microsoft's SQL Server. By establishing the database on a different LAN or VLAN, the network must be designed to segregate the database from the signalling traffic. An attacker cannot send or receive data from the database server because of this separation.

4.6 SIP Attacks

4.6.1 Message modification

Because a SIP message has an intrinsic mechanism to check the integrity of the sent message, a man-in-the-middle (MITM) attack such as spoofing, IP spoofing, MAC, or SIP registration hijacking could allow an attacker to capture and modify a SIP message. As a result, the attacker can alter all or portion of the message's properties, impersonating the caller or redirecting a call to a different location without the caller's awareness [36].

4.6.2 Cancel Bye attack

Here, an attacker creates a SIP message in a way that the message's payload contains the Bye or Cancel command. Then, the message is delivered to the intended recipient (an end-node or phone). When a steady stream of these packets is forwarded to the target phone, it may interrupt end-node services, preventing the phone from making or receiving calls. A distributed DoS (DDoS) can occur if the attack space is expanded to include more phones [32, 37].

4.6.3 Registration hijacking

SIP is a control protocol in the application layer that allows you to start, stop, and change user sessions. A user agent (UA)/IP phone must first register with a SIP proxy/registrar before the inbound calls can be redirected by the proxy to the phone in SIP. When a genuine UA has been impersonated by an attacker and changes the original registration of the genuine user with its own, this is known as registration hijacking. In this case, all incoming calls that are intended for the UA will be routed to the impersonated UA as a result of this attack [19].

Calls to a genuine UA may be lost due to registration hijacking. This could be a single user, a group of users, or a resource with a large volume of traffic, such as a voice mail system or media gatewayAll outgoing calls can be stopped or otherwise influenced by hijacking calls to a media gateway. The calls can also be recorded by a rogue UA in the middle of a call. The registration detail is currently transmitted between the control node and UA using UDP and TCP. SIP registration hijacking can be avoided by using TLS to provide an authorized secure connection instead of an open connection.

4.6.4 Redirect

The SIP redirect server can be attacked by an attacker just to reroute the calls intended for a victim to any number he chooses. This is due to the ability of the SIP server application to receive phone queries and respond with a redirect answer that includes information on where to repeat the request. The ability to reroute a call to a different phone can be used by an attacker to destroy a phone network via redirecting all the users' phone numbers to a non-existent device [19].

4.7 RTP Attacks

4.7.1 RTP tampering

The packets can be re-sequenced or rendered worthless by manipulating the sequence number and time stamp fields in the header of the RTP packet. This attack may decide to either render the discussion incoherent or crash the node receiving the packets in some protocol stack implementations; this puts it offline until the software is recycled. The receiving node will be able to tell if the RTP header has been changed thanks to the SRTP protocol. The packet will be destroyed before being processed, preventing strange behaviour from the application software [19]. Keeping VoIP traffic segregated from non-VoIP traffic on LAN or VLAN will assist prevent this type of attack. The separation of the VoIP traffic from the data network makes it difficult to access the VoIP traffic, making it difficult to monitor or modify the traffic.

4.7.2 RTP payload

The encoded voice communication is sent between the two callers using the RTP protocol. It's only a simple addition of sequencing information to the UDP protocol. An attacker can modify or inspect the message payload using a man in the middle attack to access the RTP media stream between 2 nodes. In this instance, inspection becomes eavesdropping on a conversation. An attacker that has access to the message payload can use it to insert noise or their own message [19]. In the case of noise, this would either degrade or prevent dialogue between the persons on the call; the attacker can also change the meaning of the conversation. This kind of attack can be avoided by using the secure RTP (SRTP) protocol. The transmitter encrypts RTP packets, which remain encrypted throughout the network until decrypted by the receiver. The SRTP protocol prohibits eavesdropping and packet alteration to include new messages.

5. Conclusion

VoIP has evolved as a crucial enabling technology on the IP network for multimedia communication. Considering that the Internet is an open network, VoIP has removed virtually the issue of geographic restrictions for making phone conversations. VoIP leverages the existing IP network and as such, inherits its flaws. To research on VoIP security challenges, one must first understand the underlying VoIP architecture and existing protection mechanisms, as well as the current and potential VoIP network threats and assaults. In this article, we'll go over the essential differences between VoIP and PSTN, as well as the basic VoIP architecture, which includes network components, end-user equipment, and VoIP gateway. The signalling and media transport protocols used in VoIP systems, such as H.323 and SIP, as well as RTP and RTCP, have been detailed. Future efforts will also entail preventing software attacks by enforcing strong security policies. In addition, intrusion detection systems must be designed to be able to handle emerging encrypted & polymorphic malicious code. DoS and DDoS attacks are a persistent threat that numerous systems have yet to be able to stop. The continued popularity of VoIP has highlighted the importance of effective defence mechanisms against these attacks.

Acknowledgment

The work reported in this study is funded by the Deanship of Research for the project No.: SCI-2018-3-9-7572, from the Northern Border University (NBU), KSA. We thank NBU for the contribution and support. Additionally, the first author would like to thank NBU for its invaluable supports to this study.

References

[1]. Chakraborty, T., I.S. Misra, and R. Prasad, *Overview of VoIP Technology*, in *VoIP Technology: Applications and Challenges*. 2019, Springer. p. 1-24.

[2]. Prasad, J.K. and B.A. Kumar. *Analysis of SIP and realization of advanced IP-PBX features*. in *2011 3rd International Conference on Electronics Computer Technology*. 2011. IEEE.

[3]. Shin, D.-H., *What makes consumers use VoIP over mobile phones? Free riding or consumerization of new service.* Telecommunications Policy, 2012. **36**(4): p. 311-323.

[4]. Akinbami, J., S. Virtanen, and P. Sainio, *Developing Best Practices for Securing VoIP Communication for a non-profit Organization.* 2018.

[5]. Martin, M.V., P.C. Hung, and A. Brown, *Security Issues of VoIP*, in *VoIP Handbook*. 2018, CRC Press. p. 379-400.

[6]. Chakraborty, T., I.S. Misra, and R. Prasad, *VoIP Technology: Applications and Challenges*. 2019: Springer.

[7]. Dwivedi, H., *Hacking VoIP: protocols, attacks, and countermeasures*. 2009: No Starch Press.

[8]. Dantu, R., et al., *Issues and challenges in securing VoIP.* computers & security, 2009. **28**(8): p. 743-753.

[9]. Sarker, Z., et al., *RTP Control Protocol (RTCP) Feedback for Congestion Control.* Internet RFC, 2021(8888).

[10]. Kumar, V. and O.P. Roy. *Security and Challenges in Voice over Internet Protocols: A Survey*. in *IOP Conference Series: Materials Science and Engineering*. 2021. IOP Publishing.

[11]. Ahmed, H.A.S., N. Sulaiman, and M.N. Mohammed, *Performance Analysis of VoIP Quality of Service in IPv4 and IPv6 environment.* International Journal of Digital Content Technology and its Applications, 2014. **8**(2): p. 40.

[12]. Kolhar, M., A. Alameen, and M. Gulam, *Performance evaluation of framework of VoIP/SIP server under virtualization environment along with the most common security threats.* Neural Computing and Applications, 2018. **30** (9): p. 2873-2881.

[13]. Kumar, V. and O. Roy, *Reliability and security analysis of VoIP communication systems*, in *Rising Threats in Expert Applications and Solutions*. 2021, Springer. p. 687-693.

[14]. Anderson, R., et al., *Measuring the changing cost of cybercrime.* 2019.

[15]. Alabdan, R., *Phishing attacks survey: types, vectors, and technical approaches.* Future Internet, 2020. **12**(10): p. 168.

[16]. Iqbal, M.S., et al., *Development of origin–destination matrices using mobile phone call data.* Transportation Research Part C: Emerging Technologies, 2014. **40**: p. 63-74.

[17]. Rathore, M.M., et al., *Exploiting encrypted and tunneled multimedia calls in high-speed big data environment.* Multimedia Tools and Applications, 2018. **77**(4): p. 4959-4984.

[18]. Zhang, R., et al., *Billing Attacks on SIP-Based VoIP Systems.* WOOT, 2007. **7**: p. 1-8.

[19]. Naeem, M.M., I. Hussain, and M.M.S. Missen, *A survey on registration hijacking attack consequences and protection for Session Initiation Protocol (SIP).* Computer Networks, 2020. **175**: p. 107250.

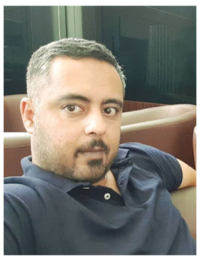
[20]. Malik, J.K. and S. Choudhury, *A Brief review on Cyber Crime-Growth and Evolution.* Pramana Research Journal, 2019. **9**(3): p. 242.

[21]. Sheoran, A., et al. *NASCENT: Tackling caller-ID spoofing in 4G networks via efficient network-assisted validation*. in

IEEE INFOCOM 2019-IEEE Conference on Computer Communications. 2019. IEEE.
[22]. Sahin, M., et al. *Sok: Fraud in telephony networks*. in *2017 IEEE European Symposium on Security and Privacy (EuroS&P)*. 2017. IEEE.
[23]. Ahson, S.A. and M. Ilyas, *SIP Security: Threats, Vulnerabilities and Countermeasures*, in *SIP Handbook*. 2018, CRC Press. p. 453-474.
[24]. Mullet, V., P. Sondi, and E. Ramat, *A Review of Cybersecurity Guidelines for Manufacturing Factories in Industry 4.0.* IEEE Access, 2021. **9**: p. 23235-23263.
[25]. Jang-Jaccard, J. and S. Nepal, *A survey of emerging threats in cybersecurity.* Journal of Computer and System Sciences, 2014. **80**(5): p. 973-993.
[26]. Conti, M., N. Dragoni, and V. Lesyk, *A survey of man in the middle attacks.* IEEE Communications Surveys & Tutorials, 2016. **18**(3): p. 2027-2051.
[27]. Geneiatakis, D., et al., *Survey of security vulnerabilities in session initiation protocol.* IEEE Communications Surveys & Tutorials, 2006. **8**(3): p. 68-81.
[28]. Ehlert, S., D. Geneiatakis, and T. Magedanz, *Survey of network security systems to counter SIP-based denial-of-service attacks.* computers & security, 2010. **29**(2): p. 225-243.
[29]. Coulibaly, E. and L.H. Liu. *Security of Voip networks*. in *2010 2nd International Conference on Computer Engineering and Technology*. 2010. IEEE.
[30]. Simonson, E.L. and B. McDaniel, *Protecting the Telephone System Against Toll Fraud*, in *The Network Manager's Handbook*. 2021, Auerbach Publications. p. 305-318.
[31]. Chakraborty, T., I.S. Misra, and R. Prasad, *VoIP over wireless LANs—Prospects and challenges*, in *VoIP Technology: Applications and Challenges*. 2019, Springer. p. 71-93.
[32]. Butcher, D., X. Li, and J. Guo, *Security challenge and defense in VoIP infrastructures.* IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), 2007. **37**(6): p. 1152-1162.
[33]. Hubballi, N. and N. Tripathi, *A closer look into DHCP starvation attack in wireless networks.* Computers & Security, 2017. **65**: p. 387-404.
[34]. Thomas Porter, C., C. CCNP, and M. Gough, *How to cheat at VoIP security*. 2011: Syngress.
[35]. Tiwari, N. and O. Rishi. *Quality Efficiency of VoIP Application Using Hybrid Co-ordination Function*. in *Data Driven Approach Towards Disruptive Technologies: Proceedings of MIDAS 2020*. 2021. Springer Singapore.
[36]. Hamdaqa, M. and L. Tahvildari. *ReLACK: a reliable VoIP steganography approach*. in *2011 Fifth International Conference on Secure Software Integration and Reliability Improvement*. 2011. IEEE.
[37]. Tang, J., Y. Cheng, and Y. Hao. *Detection and prevention of SIP flooding attacks in voice over IP networks*. in *2012 Proceedings IEEE INFOCOM*. 2012. IEEE.
[38] Ahmad H. Al-Omari, A Lightweight Dynamic Crypto Algorithm for Next Internet, Engineering, Technology & Applied Science Research, Vol. 9 No. 3 (2019): June, 2019, eISSN: 1792-8036, Greece
[39] Ahmad H. Al-Omari, Dynamic Crypto Algorithm for Real-Time Applications DCA-RTA, Key Shifting, International Journal of Advanced Computer Science and *Applications (IJACSA), Volume 7 Issue 1, 2016, ISSN: 2156-5570, UK*

Ahmad H. Al-Omari (PhD) received his B. Sc. In Computer Science in 1985, M.Cs of Computer Science in 2001, and he received his Ph.D. in Computer Information Systems in 2004. He was the acting dean, dean, department head in the faculty of Information Technology FIT, Applied Science University, Amman-Jordan. He supervised many master students, he participated in many masters' examination and discussion committees. His main research interest includes MANET, Encryption, RTA, e-government, supply chain and the tendering process.

Yazan A. Alsariera (PhD) received his BSc. from Mut'ah University, Jordan, in 2010. Master of Science in Computer Science (Minor in Software Engineering) from University of Putra Malaysia (UPM), Malaysia, in 2013. A Ph.D. degree in Software Engineering from University of Malaysia Pahang (UMP), Malaysia, in 2018. He is an Assistant Professor in the department of computer sciences at Northern Border University. His main research interest includes artificial intelligence, combinatorial intelligence optimization, secure software development, cybersecurity, and high-performance computing.



Hussam S. Alhadawi (PhD) received the M.Sc. degree in information technology from University Tun Abdul Razak (UNIRAZAK), in 2012, and the Ph.D. degree from University Malaysia Pahang (UMP), Malaysia, in 2018. He is currently a Senior Lecturer and a Senior Researcher in the field of computer engineering with Dijlah University College. His research interests include multimedia security, chaos-based cryptography, cryptanalysis, and optimization techniques. He has served as a reviewer and a technical program committee member of many international conferences. He also served as referee of some renowned journals, such as Physica B, Information Sciences, and IEEE ACCESS.

Mahmoud A.Albawaleez (PhD) is Assistant Professor of Network and Communication in the Deanship of IT at Northern Border University. He obtained Bachelor of Computer Science from Mut'ah University, Jordan, in 2006. Master of Information Technology from Universiti Utara Malaysia (UUM), Malaysia, in 2009. A Ph.D. degree in Science (Network and Communication) from university of / University Sciences Islamic Malaysia (USIM), Malaysia, in 2018.

Sultan Alkhliwi (PhD) received the B.E. degree, from Northern Border University in 2008. He received the M.Sc. and PhD. From University of Manchester- U.K in 2013 and 2018 respectively. Currently, he works as assistant professor in the Department of Computer Science- Faculty of Science- Northern Border University in Saudi Arabia. His research interest includes multi-hop communication networks, cryptography, network security, information security.