






Penetration testing for VoIP

Şevki Gani Şanlıöz 

National Defense University HEZARFEN Aeronautics and Space Technologies, İstanbul, Turkey

Muhammed Sadık Karabay 

National Defense University HEZARFEN Aeronautics and Space Technologies, İstanbul, Turkey

Aytuğ Boyacı 

National Defense University HEZARFEN Aeronautics and Space Technologies, İstanbul, Turkey

Submitted: 28.01.2021

Accepted: 13.02.2021

Published: 28.02.2021



Abstract:

Thanks to its economic advantages and flexibility, VoIP technology is spreading dramatically in recent years. This increase is happening much faster, especially due to the recent COVID-19 restrictions. However, the rapid spread also brings along some security threats. So, it is inevitable to take security measures specific to VoIP technology. These security measures specific to VoIP systems and devices will increase the benefit in terms of cost and performance. In this context, penetration tests to determine the required security measures should also be made specific to VoIP. In this paper, we proposed a penetration testing strategy for VoIP which ensure and analyzes the VoIP vulnerabilities. Furthermore, it provides an aspect of view on VoIP security precautions for VoIP administrators. This strategy provides proactivity to VoIP administrators before a possible attack. In our future studies, we aim to analyze them by implementing in a test environment.

Keywords: *Attack models, Penetration Test, VoIP, VoIP Security*

© 2021 Published by peer-reviewed open access scientific journal, CI at DergiPark (<https://dergipark.org.tr/tr/pub/ci>)

Cite this paper as: Şanlıöz Ş. G., Karabay M. S., & Boyacı A., Penetration testing for VoIP, *Computers and Informatics*, 2021, 1(1), 36-45.

1. INTRODUCTION

With the development of IP technology, most of the security systems, camera systems, communication systems and many other system infrastructures started to use this technology recently. With VoIP technology, IP-based voice communication has dramatically increased in recent years. The most important reason for this increase is that VoIP technology provides cost effectiveness and high performance. Considering the usage rates over time, the rate of VoIP usage to all voice calls was at the level of 1% in 1998; this rate reached 3% in the early 2000s and 25% in 2003 [1]. PSTN usage, which was 658 million in 2017, decreased to 612 million by the end of 2018; On the other hand, VoIP usage increased from 338 million to 359 million in the same period. It is estimated that the use of VoIP will exceed the use of PSTN by 2021 [2].

This increase in the use of VoIP also brings many security risks. When a VoIP hacking case that occurred at a company called Sunbelt Software in the United States examined, it can be seen that an attacker gained an unauthorized access on the VoIP system through remote access features, and then caused a huge financial damage to the company by making international calls. In addition to measures for general data communication, additional measures specific to VoIP technology needs to be taken. However, generally most of the measures taken are insufficient. One of the most important reasons for this issue is that the existing vulnerabilities cannot be fully identified. In this context, vulnerability analysis on VoIP systems plays a vital role in highlighting the protection methods to be determined.

The penetration test strategy has a vital importance on system security. It ensures the security mechanisms created against constantly evolving and renewed threats. The penetration test strategy should be specific to the system to be protected. For this reason, the protection strategy for the security of VoIP technology, which is different from traditional data communication, should be developed specifically for it. The security measures determined as a result of the penetration test strategy will affect the configuration of the relevant security devices as well as their positioning in the system.

This manuscript is organized as follows: Section 2 introduces the VoIP architecture and vulnerabilities. Section 3 describes the penetration tests. Section 4 analyzes the penetration tests in VoIP systems. Section 5 concludes the paper.

2. VOIP ARCHITECTURE AND VULNERABILITIES

It will be useful to understand the VoIP architecture and vulnerabilities to manage the VoIP Pentest process more effectively.

2.1. VoIP Architecture

VoIP is a technology that allows real-time voice transmission by using the advantage of existing internet infrastructure. VoIP technology basically consists of two different protocol groups as signaling (SIP) and media transmission protocols (RTP). Sample VoIP Architecture is presented in Fig. 2.

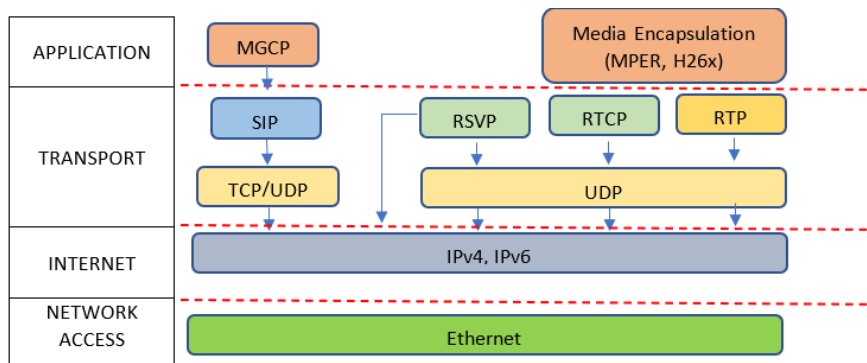


Figure 1. VoIP Architecture.

This architecture represents VoIP protocols including Session Initiation Protocol (SIP) that handles signaling process during media communication, Real Time Transfer Protocol (RTP) used for real-time data streaming and Real Time Control Protocol (RTCP) that provides control of this protocol, Resource Reservation Protocol (RSVP) used for resource allocation, Real Time Streaming Protocol (RTSP) that establishes and controls the flow of audio or video data between the server and the client and Media gateway Control protocol (MGCP) that handles audio transmission between different networks by making connections between media gates. Sample VoIP flow diagram is presented in Fig. 2.

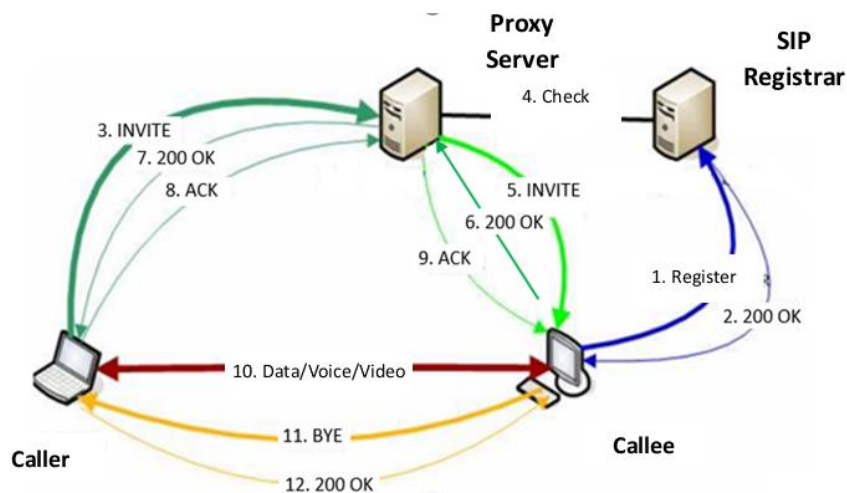


Figure 2. VoIP flow diagram.

As seen in Fig. 2, users must first be registered to a system to make a call in VoIP technology. Registration process is shown in 1st and 2nd steps. All users in the system are registered on the registrar server as shown in these steps. Then, when one of the parties makes a call, it is first checked whether the user he is calling is in the same system; If it is in the same system, it is directed directly to the relevant user, if not, it forwards the request to target system. These operations are shown between the 3rd and 9th steps. Then, as seen in the step 10, voice transfer between the parties takes place. Finally, in steps 11 and 12, one of the parties sends a request to end the session, and thus the call is terminated. In step 10, media transfer protocols are implemented, while all other steps are done through signaling protocols.

The most widely used signaling protocol today is the Session Initiation Protocol (SIP). After the session is initiated, media streaming is provided via the real-time data transmission protocol (Real Time Protocol- RTP). The termination of the session takes place via SIP again.

2.2. VoIP Vulnerabilities

Although VoIP technology provides advantages in terms of cost and performance, it also brings many security threats. When the literature is examined, it is seen that although the classification of the mentioned attacks is similar, they are classified in different ways. For example, VOIPSA (Voice Over IP Security Alliance), known as VoIP Security Association, classify these attacks in four group: wiretapping attacks (Eavesdropping), interception and modification, Intentional Interruption of Service and Social Threats [3]. In addition, IETF (Internet Engineering Task Force) classifies VoIP threats into four groups as Interception and Modification, Denial of Service, Abuse-of-service and Social Threats [4].

2.2.1. VoIP Vulnerabilities

Interception is the attacks made by the attacker by obtaining the communication signal or data between the parties. It includes attacks such as number harvesting, where user numbers or identities are compromised, call pattern tracking, where user search features are tracked, and conversation reconstruction, in which speech and / or additional data supplied with it are intercepted.

The modification is the types of attacks, such as the man in the middle attack, where the attacker changes the packets captured. Call black holing attack in which the transmission of packets required for proper communication is blocked, call rerouting attack that causes the transfer of calls to different users, conversation alteration attack where packets are changed to manipulate the conversation between two users and the overall quality of the conversation. An example of this threat is the conversation degrading attack where the packet was deliberately dropped or changed to drop it.

2.2.2. VoIP Vulnerabilities

Denial of service is a type of threat that is valid for all IP networks and its purpose is to render the system inoperable. Distributed DoS (DDoS), on the other hand, is a version of disruption attacks performed over multiple different sources [5]. Denial of service attacks specific to SIP protocol includes SIP malformed requests and messages, SIP requests and messages flooding, call hijacking and call tear down attacks.

2.2.3. VoIP Vulnerabilities

Attacks with the aim of fraud or billing reducing. Examples include identity theft attacks using other user's credentials to circumvent an authentication system or billing, attacks to increase resource utilization, and session replay attacks to access the same resources as the legitimate user.

2.2.4. VoIP Vulnerabilities

It includes the types of attacks carried out through unwanted communication and self-promotion for the purpose of gaining interest. Examples of this type of threat are unwanted communication attacks, such as a user identity / authorization attack or telemarketing (also called SPIT attack).

3. PENETRATION TESTS

Penetration test, which has a long history starting from the early 1970s, is used by organizations to proactively provide measures for the security of Information Systems and is becoming more common recently [6]. The protection of data, which is one of the most valuable resources nowadays, is of vital importance for organizations of all levels. Thanks to penetration tests that simulate many cyber-attacks,

companies can see their vulnerabilities prior to real attack. The measures they take according to risk analysis based on these vulnerabilities provide them financial gain as well as security [7]. Although each methodology used for penetration testing has different number of phases or different phases names, they all provide similar overview of the penetration testing. As one of the most popular methodology, kill chain, has 7 phases as follows [8]:

Information Gathering: Identifying the target system and collecting information about it (technologies used, potential vulnerabilities, etc.)

Weaponization: Developing malicious code to discover vulnerabilities, combining developed code with unexpected deliverables.

Delivery: Transferring the weaponized payload to the target system.

Exploitation: Use of the target system's vulnerability to execute malicious code.

Installation: Remote Access Trojan's (RAT) are generally installed which allows adversary to maintain its persistence in the targeted system.

Command and control (C2): Adversary require a communication channel to control its malware and continue their actions. Therefore, it needs to be connected to a C2 server.

Actions: It is the last phase in which adversary achieves its objectives by performing actions like data exfiltration. Defenders can be confident that adversary achieves this phase after passing through previous phases.



Figure 3. Phases of Penetration Testing.

Additionally, Advanced Persistent Threats (APT) which have a complex attack structure, has become popular recently. In the literature, Moonlight Maze [9], GhostNet [10], Hydraq [11] and STRONTIUM [12] has been analyzed comparatively with the help of the kill chain model [13,14,15,16].

4. PENTEST IMPLEMENTATION ON VOIP SYSTEMS

In addition to SIP server vulnerabilities, weaknesses on end-user devices (used in different models and software versions) also affect the overall security of the institution. VoIP, which is also described as one of the first examples of IoT technology [18], can be used in large-scale DDoS attacks by exploiting end-user devices. An example of this is Mirai botnet, built with 1,5 million cameras in 2016 and generated 660 Gbps traffic [19].

According to various sources, more than 50 billion devices are expected to exist in the coming years. The contribution of IoT, Artificial Intelligence, 5G and Beyond Communication systems is inevitable in the formation of this huge connection and device. All these developments raise the living standards of humanity. However, there is a point that is overlooked while these are taking place. This point is security. When we examine the cyber-attacks carried out in the last decade, we can clearly see this. 2016-Mirai botnet case is one of the biggest painful experiences of this situation.

With the rapid development of IoT devices, the use of VoIP systems will also increase, and security weaknesses will occur accordingly. Researchers at Microsoft Threat Intelligence Center have discovered the attack on the vulnerabilities of a VoIP phone, an office printer and a video decoder, which are called three IoT devices in an enterprise system. In the investigation, it was determined that the attacker (STRONTIUM group as suspect) used these devices in order to access the corporate network. This incident shows the importance of end user devices, like IP phones, on system security. At this point, we will discuss about VoIP Penetration Tests in this study.

Fig. 4 depicts an example of simplified security precaution for VoIP penetration test flow chart. Before the implementation of VoIP penetration testing, a strategy should be developed to conduct this test effectively. Then analysis of the VoIP system and its components is made to determine the appropriate attack tools. Afterwards, the effects on the security measures taken are observed using the determined attack tools. Finally, the necessary security updates are implemented on the system accordingly.

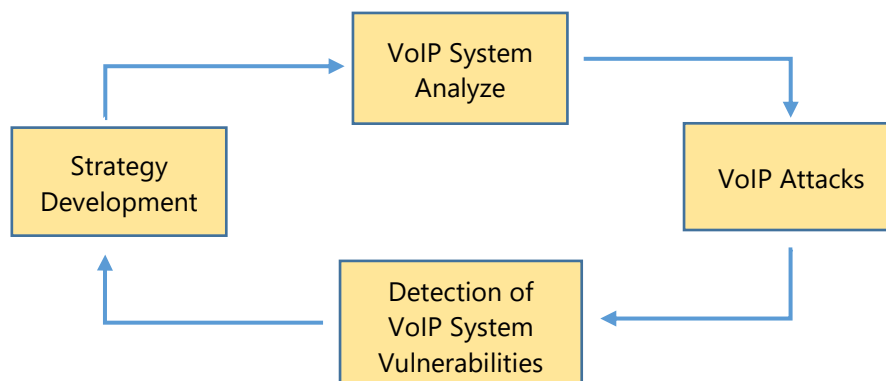


Figure 4. Security Precaution for VoIP Penetration Test Steps.

Although the attack methods used for Pentest are very similar to each other, they differ according to the features of the platform they are applied to. In this context, the attack methods used in VoIP contain their own unique methods. There are some stages when performing VoIP penetration tests. These are [17];

Table 1. VoIP Penetration Test List.

VoIP Penetration Test
Application Scoping
Vulnerability Analysis
Reconnaissance and Enumeration
Mapping and Service Identification
Application Scanning
Application Analysis
Strategic Mitigation
Patch Verification

Determining the measures to be taken to ensure the security of the system depends on the effective implementation of the penetration tests. There are many tools that can be used during a penetration test. Determining the measures to be taken to ensure the security of the system depends on the effective implementation of the penetration tests. While penetrating VoIP systems, many tools are used according to various methods. Related methods can be analyzed according to the classes given the following properties;

VoIP Sniffing Tools:

- Determine the password of a user by analyzing SIP traffic,
- Capability to reconstruct RTP media calls,
- CommView that is suited for real-time capturing and analyzing VoIP events (such as call flow, signaling sessions, registrations, media streams, errors, etc.)

VoIP Scanning Tools:

- IAX2 (Asterisk) login enumerating with using REGREQ messages,
- Network vulnerability scanners,
- Network port scanners,
- Enumerating open SCTP ports without establishing a full SCTP association with the remote host,
- SIP protocol login cracking,
- Finding SIP devices with potentially vulnerable Web GUIs,

VoIP Packet Creation and Flooding Tools:

- Creating IAX packets,
- Sending a flurry of SIP INVITE messages to a phone or proxy,
- Creating "well formed" RTP Packets that can flood a phone or proxy

VoIP Fuzzing Tools:

- Setting of malformed SIP methods (INVITE, CANCEL, BYE, etc.) that can be crafted to send to any phone or proxy

VoIP Signaling Manipulation Tools:

- Trying to disconnect an active VoIP conversation by spoofing the SIP BYE message from the receiving party,
- In a SIP signaling environment, to monitor for an INVITE request and respond with a SIP redirect response, causing the issuing system to direct a new INVITE to another location

VoIP Media Manipulation Tools:

- Taking the contents of a .wav or tcpdump format file and inserting the sound into an active conversation

Miscellaneous Tools:

- Dictionary attack tools
- Tiny command-line based Script
- Spam testing

Related tools are included in Table 2 according to the above classes. By using these tools, many efficiencies can be obtained in penetration tests. We can maintain comprehensive security of VoIP systems with penetration tests. The limits of the system can be determined, and vulnerabilities can be

detected. With the results, measures are taken against possible attacks and VoIP system hardening can be complete. The relevant tools are also used for testing other systems, apart from VoIP penetration tests. The Nmap tool is one of the most obvious examples.

Table 2. VOIP Security Tool List.

VoIP Sniffing Tools	• AuthTool	• rtpBreak
	• Cain & Abel	• SIPomatic
	• CommView VoIP Analyzer	• SIPv6 Analyzer
	• Etherpeek	• UCSniff
	• ILTY ("I'm Listening To You")	• VoiPong
	• NetDude	• VoIPong ISO Bootable
	• Oreka	• VOMIT
	• PSIPDump	• Wireshark
VoIP Scanning Tools	• WIST	
	• EnableSecurity VoIPPack for CANVAS	• SIP-Scan
	• enumIAX	• SIPcrack
	• iaxscan	• Sipflanker
	• iWar	• SIPSCAN
	• Nessus	• SIPVicious Tool Suite
	• nmap	• SiVuS
	• Passive Vulnerability Scanner	• SMAP
VoIP Packet Creation and Flooding Tools	• SCTPScan	• VLANping
	• SIP Forum Test Framework (SFTF)	• VoIPAudit
	• IAXFlooder	• Scapy
	• INVITE Flooder	• Seagull
	• iThinkTest FlowCoder: SiPBlast	• SIPBomber
	• kphone-ddos	• SIPNess
	• NSAUDITOR - SIP UDP Traffic	• SIPp
	• RTP Flooder	• SIPsak
VoIP Fuzzing Tools	• Asteroid	• PROTOS H.323 Fuzzer
	• Codenomicon VoIP Fuzzers	• PROTOS SIP Fuzzer
	• Fuzzy Packet	• SIP Forum Test Framework (SFTF)
	• Interstate Fuzzer - VoIP Fuzzer	• Sip-Proxy
	• Mu Dynamics VoIP, IPTV, IMS Fuzzing	• Spirent ThreatEx
	• ohrwurm	• VoIPER
VoIP Signaling Manipulation Tools	• BYE Teardown	• Registration Eraser
	• Check Sync Phone Rebooter	• Registration Hijacker
	• H225regreject	• SIP-Kill
	• IAXAuthJack	• SIP-Proxy-Kill
	• IAXHangup	• SIP-RedirectRTP
	• iThinkTest FlowCoder: SiPCPE	• SipRogue
	• RedirectPoison	• vnak - VoIP Network Attack Toolkit
	• Registration Adder	• VoIPHopper
VoIP Media Manipulation Tools	• RTP InsertSound	
	• RTP MixSound	
	• RTPInject	
	• RTPProxy	
	• SteganRTP	
	• Vo2IP	

Miscellaneous Tools	<ul style="list-style-type: none">• IAX.Brute• SIP-Send-Fun• SIP.Tastic• Spitter• VoIP Security Audit Program (VSAP)• Xtest
------------------------	--

5. CONCLUSION

VoIP is becoming more popular thanks to the advantages it provides. Especially, due to Covid-19 restrictions, the obligation of working at home has highlighted the importance of video and phone communication for the collaboration of employees. It is also the same for students. Almost all lessons are conducted online. However, this rapid progress caused for some individuals and organizations to be vulnerable to attacks. Because traditional data security measures are insufficient for VoIP telephone and video communication. On the other hand, the high cost of security measures and the complexity of these security structures make it necessary to detect the weaknesses of the system before taking security measures. This reveals the requirement for Pentest, especially VoIP-specific Pentest.

In this study, we tried to explain the penetration test methodology that should be followed and tools that can be used by considering the types of attacks that have become important for VoIP recently. Because, with an effective penetration test on the relevant platform, the necessary security measures can be provided in a cost-effective way. And, excessive security measures may restrict the communication capabilities of the employees. Pentest helps us to take security measures that meet security requirements and have minimal negative impact on employees.

For better understanding of the penetration test methodology specific to VoIP and develop effective counter measures against them, a test environment should be established, and the described VoIP penetration test methodology should be applied. In our future studies, we aim to implement and analyze a penetration test of VoIP systems, especially phones, which are seen as one of the first examples of IoT devices, in a test environment.

REFERENCES

- [1] Hallock J.A. Brief history of VoIP. Evolution and Trends in Digital Media Technologies, 2004. http://www.joehallock.com/edu/pdfs/Hallock_J_VoIP_Past.pdf.
- [2] Bell, P. (2019). No Lifeline for Wireline: Fixed Voice Continues to Fall. <https://blog.telegeography.com/no-lifeline-for-wireline>.
- [3] Coulibaly, E., Liu, L. Security of VoIP networks. In: *2nd International Conference on Computer Engineering and Technology (IC CET)* 2010, pp. 104-108. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5485790
- [4] Thermos, P., Takanen, A., *Securing VoIP Networks: Threats, Vulnerabilities, and Countermeasures*. Boston, USA. Adison-Wesley, 2007.
- [5] Porter, T. Threats to VoIP Communications Systems'. Syngress Force Emerging Threat Analysis. 2006, pp. 3-25.
- [6] Mirjalili, M., Nowroozi, A., & Alidoosti, M. A survey on web penetration test. *Advances in Computer Science: An International Journal*, 3(6), No.12, November 2014, pp. 107-121
- [7] Samant, N. Automated penetration testing. PhD, San Jose State University, United States, 2011.
- [8] Bhatt, P., Yano, E., & Gustavsson, P. Towards a framework to detect multi-stage advanced persistent threats attacks. *2014 IEEE 8th international symposium on service oriented system engineering*. IEEE, 2014.
- [9] Guerrero-Saade, J.A., Raiu, C., Moore, D., & Rid, T. Technical Report. Penquin's moonlit maze: The Dawn of Nation-State Digital Espionage. Kaspersky Lab. 2017.

- [10] Deibert, R. J., Rohozinski, R., Manchanda, A., Villeneuve, N., & Walton, G. Tracking ghostnet: Investigating a cyber espionage network. 2009.
- [11] McClure, S., Gupta, S., Dooley, C., Zaytsev, V., & Chen, X.B., Kaspersky, K., Spohn, M., Perme, R., 2010. Protecting your critical assets-lessons learned from operation aurora. Technical Report, 2010.
- [12] Accessed: 2020-12-29, <https://msrc-blog.microsoft.com/2019/08/05/corporate-iot-a-path-to-intrusion/>.
- [13] Alshamrani, A., Myneni, S., Chowdhary, A., & Huang, D. A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities. *IEEE Commun. Surveys and Tutorials*, 2019: 21(2), 1851–1877. doi: 10.1109/COMST.2019.2891891.
- [14] Chen, P., Desmet, L., & Huygens, C. A study on advanced persistent threats. *IFIP International Conference on Communications and Multimedia Security*. 2014, Springer, pp. 63–72.
- [15] McWhorter, D. Mandiant exposes APT1 - One of China's cyber espionage units & releases 3,000 indicators. Mandiant February 18, 2013.
- [16] Ussath, M., Jaeger, D., Cheng, F., & Meinel, C. Advanced persistent threats: Behind the scenes. *Annual Conference on Information Science and Systems (CISS)*. 2016, IEEE, pp. 181–186.
- [17] VoIP Penetration Testing. (2019, November 8). Essential Infosec Private Limited. <https://www.essentialinfosec.com/services/voip-penetration-testing/>
- [18] R. Pepper. The History of VoIP and Internet Telephones. <https://getvoip.com/blog/2014/01/27/history-of-voip-and-internet-telephones/>, 2014.
- [19] Vice. How 1.5 Million Connected Cameras Were Hijacked to Make an Unprecedented Botnet. <https://www.vice.com/en/article/8q8dab/15-million-connected-cameras-ddos-botnet-brian-krebs> 2016.