VoIP security threats

A. Mentsiev[1], A. Dzhangarov[2]

[1]Chechen State University, Grozny

[2]Kuban State University, Krasnodar

Abstract: Voice over Internet Protocol (VoIP) is a widely deployed service since the commencement of voice and data integration. This was done in a bid to reduce cost and management concerns. VoIP uses the same infrastructure as traditional data networks and thus, inherits all the security challenges of a data network. In addition, VoIP exhibit self-inflected problems resulting from network components and the protocol adopted. This paper present the security threats witnessed in VoIP telecommunication. The paper discusses the security threats in tandem with confidentiality, integrity and availability principle. Examples of security issues under consideration include; spamming, identity spoofing, call tempering, DoS, and Man-in-the-middle attacks among others. Finally, the paper will outline the common countermeasures adopted to mitigate the threats.

Keywords: VoIP, VoIP security, voice over IP security, DoS, spamming, identity spoofing, call tempering, Cybercrime, Computer security.

SECURITY THREATS

A. Confidentiality Threats

Confidentiality refers to the access of information by authorized parties alone. The confidential information of end users includes private documentation, financial information, security information such as passwords, conversion content, conversion history pattern among others. The confidential information for network components include operating systems, IP addresses, and protocols, address mapping, user records and data in the networks [1][2].

1. Eavesdropping

Conventional telephone eavesdropping requires either physical access to tap a line or penetration of a switch. With VoIP, opportunities for eavesdropping increase significantly as a result of the large number of nodes in the path of communicating entities. If the attacker comprises one of the nodes, it is easy to access the IP flowing through the nodes. Numerous network analyzers and tools can convert VoIP traffic to wave files. These tools give attacker ability to save conversations into the file systems and play them back on a computer. VoMIT is

an example of such a tool. Software such as Wireshark can be used to retrieve conversations. Wireshark is a powerful analytical tool used to track network traffic. As a network packet analyzer, Wireshark has the capability to peer inside the network and record the details concerning traffic at a variety of levels ranging from connection level stats to bits comprising a single packet. The flexibility and depth of analysis allows the user to analyze security events and trouble shoot network security device issues.

Peering into the traffic can reveal important information about packet details which aids in dissecting a network attack and designing remedies. For instance, in the case of a denial of service attack, Wireshark can identify the specific type of network attack and modify upstream firewall rules to block unwanted traffic. Troubleshooting security devices is another function of the tool. If systems running Wireshark are connected to either side of the firewall, it troubleshoots the firewall rules and determines which packets are traversing the device successfully and which are not. This aids in the identification of the origin of connectivity issues [2].

However, the software present challenges in terms of privacy and levels of exposure. As such, an organization must have a clearly defined policy detailing the rights and responsibilities of individuals using the network. It must also have clauses granting permissions to sniff traffic for security and troubleshooting issues and outline the organizations policy requirements for retrieving, analyzing and retaining network traffic dumps. Thus, before a tool such as Wireshark is used in any network, relevant permissions need to be granted to the user otherwise legal implications may occur [3].

2. Unauthorized access

Attackers can access information on a network that they do not authority to see. Multiple undocumented ports and services in certain VoIP phones provide the leeway for attackers. Vulnerabilities also occur due to implementation issues.

Networks rely on the truth and without accurate information, they do not work correctly. Attackers use lies to deceive networks and systems attached to a particular network thereby impacting their operation. Source address spoofing is a mechanism of lying about a packets return address.

Attackers have used source address spoofing to institute denial of service attacks against commercial servers and networks. Though the phenomenon is still widely misunderstood relevant measures have been undertaken to make the attacks unsuccessful. Users can become a victim of address spoofing and more worryingly a source of attacks based on source address spoofing unless the user understands how it works and take measures to prevent it.

In order to get spoof proof, ISP practice ingress filtering is applied to filter and drop any packets with spoofed source addresses. For instance, Cisco Express Forwarding is an advanced IP switching technology that is designed for high performance layer 3 IP switching with optimum performance [4].

There are systems for call control, administration, billing, and other VoIP RELATED telephone functions. These systems may contain passwords, user identities, phone numbers, private information, among others. Lots of gateways and switches are bought with default well known passwords. If these passwords are left without configurations, the attackers can easily go past them and institute attacks. Some switches contain TELNET remote access and the clear text protocol exposes everything to traffic sniffers. Some of the gateways or switches contain web server interface for remote control. Attackers capitalize to sniff on HTTP traffic in LAN and steal sensitive information. Attackers also make use of the ARP cache poisoning to forward all the traffic via their workstations to capture network traffic of the VoIP [5].

3. ID Spoofing

IP spoofing is a means of IP address forgery where an attacker masquerades as a trusted host to conceal his identity. An attacker obtains the IP address of the

legitimate host and alters packet headers so as to make it look like that of the source which is the legitimate host. A user who visits the sited is redirected to the spoofed content created by the attacker and as such the attacker gains access to sensitive information and network resources. Apart from this, the attacker could alter sensitive information, install malware and take control of the compromised computer in order to send out spam.

These are attacks that target vulnerabilities in the client applications that interact with a malicious server or data. The client can initiate a connection that could result in an attack. The client has to interact with the server in order to be affected. A client running mere FTP does not fall vulnerable but interaction such as instant messaging applications exposes the client to such attacks because clients are automatically configured to log into the remote server [4].

B. Integrity issues

Integrity refers to the alteration of information by the unauthorized users. A legitimate user may perform an incorrect or unauthorized operations functions causing delirious modifications, deletion, destruction, or disclosure of switch software or functions. Intruders masquerading as legitimate users can access the operation ports of the switch.

a. Caller ID

Caller ID is a service provided by telecommunication companies that notify users of an incoming call. Caller ID spoofing is the process of setting the caller ID on the outgoing calls to a 10-digit number of the caller choice. Some websites provide Caller ID spoofing services thus there is no need for special hardware to be implemented on the spoofed VoIP.

If the attacker can manage to take control of the gateway server, he can change the “From” header to a number he desires. The recipient will respond positively to the proxy server which in this case is just like the “via” field. The

proxy server then forwards the acknowledgement to the legitimate user since it knows its IP address of its phone [6].

Automated or manual caller ID verification systems like those used by credit card companies can sent false information. Caller ID spoofing websites are used by fraudsters using stolen credit card information. They call the service provider such as Money gram, setting the caller ID to appear as if it originates from card holders home, and use the credit information to order cash transfers that they will finally pick up. Likewise, spammers can use this information to spam or run as trusted entities such as banks [7].

b. DoS Attacks

Attackers can abuse the signaling protocols to conduct denial of service attacks - attackers create large number of call setup requests that elapse the processing power of proxy server of terminals. For instance, an attacker initiates too many invite requests to another party that cannot take the requests. It only requires large number of requests to flood the victim network thereby impacting on its services. Likewise, attackers can launch distributed denial of service to cover trace and aggregate requests.

VoIP media attack occurs when attackers flood the gateway, IP phone, and other media VoIP components with excessive number of RTP packets. If the target is forced to deny the packets, VoIP quality degrades significantly. The attacker tampers with the key components of the gateway putting it offline. Since RTP is encapsulated in UDP, it is not difficult to craft. A failure in one of the devices leads to a network failure [6].

c. Call Redirection or Hijacking

Another security problem of VOIP is the interception of calls. This is so because VOIP phone calls are very easy to capture and decode if the person has a physical access to the LAN segments that VOIP packets are travelling across. Even so, this can be counter measured by physical security or by implementing

encryption process or by use of secure wireless networks. There is also another security issue of denial of service attacks [5]. This occurs by sending fake traffic to the VOIP services or the normal end points hence disrupting the normal service. This can be overcome though by installing session border controllers that have DoS countermeasures that are built in [8]. With the use of VOIP, an attacker may obtain your confidential information by simply introducing a bug into your phone, or somewhere he can easily tap the information from you very easily hence becoming not as secure as we would want. An attacker may easily also hack into to the VOIP servers and hence redirect the calls to where he wants or even can obtain the users call details hence breaching to the persons secure confidential information hence this is a very bad crime. By so breaching, the attacker may use you network subsequently to obtain long distance calls at free and at your cost and expenses. This makes it not as secure as it results in users' charges [9].

Recommended countermeasures

To countermeasure availability issues, stronger authentication is required. VoIP components need to ensure that they are communicating with legitimate users. The same applies to integrity issues. Other not trusting the caller ID strong authentication schemes is necessary. Software patches are also necessary to fix any unknown vulnerability issues. Encryption through IPSec, SSH and SRTP provide confidentiality and replay protection [7]

References

1. Coulibaly, Elhalifa, and Lian Hao Liu. "Security of Voip networks." Computer Engineering and Technology (ICCET), 2010 2nd International Conference on. Vol. 3. IEEE, 2010. pp. 219-238.

2. Gallo Patrik, Dusan Levicky, and Gabriel Bugar. “Authentication threats in PSTN-VoIP architecture using multi-service gateways.” ELMAR, 2012 Proceedings. IEEE, 2012. pp. 153-156.

3. Nassar Mohamed, et al. “Risk management in VoIP infrastructures using support vector machines.” Network and Service Management (CNSM), 2010 International Conference on. IEEE, 2010. pp. 48-55.

4. Patel Mayank, and B. V. Buddhdev. “Analysis of Security Threats in Voice Over Internet Protocol (VOIP).” Control Theory and Informatics 3.5, 2013. pp. 30-37.

5. Rezac, F., Voznak, M., Tomala, K., Rozhon, J., Vychodil, J. Security Analysis System for Detection Security Threats on a SIP VoIP Infrastructure Elements, In Journal Advances in Electrical and Electronic Engineering, Volume 9, Number 5, 2011, pp. 225-232.

6. Thomas Porter, et al. “Practical VoIP Security.” Syngress, 2006. 362 p.

7. Yeun Chan Yeob, and Salman Mohammed AlMarzouqi. “Practical Implementations for Securing VoIP Enabled Mobile Devices.” Network and System Security, 2009. NSS'09. Third International Conference on. IEEE, 2009. pp. 409-415.

8. Zhang Ge. Unwanted Traffic and Information Disclosure in VoIP Networks: Threats and Countermeasures. “A Survey on Anonymous Voice over IP Communication: Attacks and Defences”. Diss. Umae University, 2012. pp. 203-234.

9. Abramov E.S., Tarasov Y.V. Inženernyj vestnik Dona (Rus). 2017. №3. URL: ivdon.ru/ru/magazine/archive/n3y2017/4354

10. Mokhov V.A., Georgitsa I.V., Goncharov S.A. Inženernyj vestnik Dona (Rus). 2013. №3. URL: ivdon.ru/ru/magazine/archive/n3y2013/1852