VoIP Security Issues: The Grey Shades of Internet Telephony

Neha Tiwari

[1]*Department of CS & IT, The IIS University, Jaipur, (INDIA)*
E-mail: sneha.sh02@gmail.com

***Abstract*-Voice over Internet Protocol (VoIP) technology has gone viral over the packet switched network. It involves transmission of voice as data packets over public or private Inter Protocol (IP) Networks. The growing popularity has laid a big threat to making calls through the Public Switched Telephone Networks (PSTN). The convergence of networks behind this technology brings best and worst of them all together. Despite of providing a number of benefits, VoIP has some its own agonizing issues which it inherits from its Internet based execution. Whenever we talk of VoIP, our prime focus doesn't deviate from impairments associated with it and Quality of Service (QoS) issues. This paper converges on different types of security threats and vulnerabilities linked with VoIP.**

***Keywords*- VoIP, VoIP impairments, Qos, security.**

I. INTRODUCTION

Voice over IP (VoIP) has emerged as a strong global communications mode which integrates voice, data and images, and allows it to travel over existing packet data networks along with traditional data packets. Lower cost and greater flexibility adds more to its ever growing popularity. VOIP has a very different architecture contrary to the traditional circuit-based telephony, and these differences result in some significant deployment concerns. Therefore, despite of the promises of VOIP for the enterprise, it should not be installed without careful consideration of the problems that it introduces.

VOIP systems take a wide variety of forms, including traditional telephone handsets, conferencing and mobile units. In addition to the equipments used by the end-users VOIP systems include a variety of other components, including call processors/call managers, gateways, routers, firewalls, and protocols. Most of these components have counterparts used in data networks, but the performance demands of VOIP mean that ordinary network software and hardware must be supplemented with special VOIP components. Major cause behind the implementation of VoIP lies in the confusion of the assumption that because of digitization, voice travels in packets just like any other data and the existing network architectures and tools can be used for it without further change. However, VOIP adds a number of complications to the existing network technology, and these problems are exaggerated by security considerations. The convergence of data and voice in the same network brings both benefits and as well as constraints to the users. There are several issues that need to be addressed when we talk about deployment of this technology and security is one of the most critical one.

Internet Telephony suffers from many security issues ranging from infrastructure to users' perspective. Some of the most common and crucial of them are discussed in the coming sections.

II. TYPES OF INFORMATION SECURITY RISKS

Packet networks depend for their successful operation on a large number of configurable parameters for example, IP and MAC (physical) addresses of voice terminals, addresses of routers and firewalls, and VOIP specific software such as Call Managers and other programs used to place and route calls. Every time when a VOIP call is restarted or added to the network or a network component is restarted, many of the above mentioned network parameters are established dynamically. Because of the availability of various places in an IP network with dynamically configurable parameters, intruders have a wide array of potentially vulnerable points to attack.

The Information security risks can be broadly categorized into three types, which can be remembered as the mnemonic "CIA" [1]. They are:

- Confidentiality
- Integrity
- Availability

Additional risk types comprise of fraud and risk of physical damage to the switch, physical network, or telephone extensions.

A. Confidentiality and privacy:

Confidentiality refers to the need to keep information secure and private. For home computer users, this category includes security information such as passwords, confidential memoranda and financial information. In a telecommunications' switch, eavesdropping on

conversations is an issue of obvious concern, but the confidentiality of other information on the switch must be protected to defend against voice and data interception, toll fraud, and denial of service (DoS) attacks. Network IP addresses, operating system type, telephone extension to IP address mappings, and communication protocols are all examples of information that, while not critical as individual pieces of data, can make an attacker's job easier.

There are lot of vulnerabilities and problems related with confidentiality maintenance and privacy of user. Some of them are as below:

i. Switch Default Password Vulnerability:

Failing to change default passwords is one of the most common errors made by inexperienced users. It is common for switches to have a default login/password set, e.g., admin/admin, or root /root. This vulnerability allows for wiretapping conversations on the network with port mirroring or bridging. An attacker with access to the switch administrative interface can mirror all packets on one port to another, allowing the indirect and unnoticeable interception of all communications. If possible, remote access to the graphical user interface should be disabled to prevent the interception of plaintext administration sessions. Some devices provide the option of a direct USB connection in addition to remote access through a web browser interface. Port mirroring on the switch should also be disabled.

ii. Classical Wiretap Vulnerability:

A good physical security policy for the deployment environment is a general first step to maintain confidentiality. Attaching a "packet capture tool" or "protocol analyzer" to the VOIP network segment makes it easy to intercept voice traffic. Disabling the hubs on IP Phones as well as developing an alarm system for notifying the administrator when an IP Phone has been disconnected will allow for the possible detection of this kind of attack.

iii. ARP Cache Poisoning and ARP Floods:

Because many systems have little authentication, an intruder may be able to log onto a computer on the VOIP network segment, and then send ARP commands corrupting ARP caches on sender(s) of desired traffic, then activate IP. An ARP flood attack on the switch could render the network vulnerable to conversation "eavesdropping".

With conventional telephones, eavesdropping usually requires either physical access to tap a line, or penetration of a switch. Attempting physical access increases the intruder's risk of being discovered, and conventional PBXs have fewer points of access than VOIP systems. With VOIP, opportunities for eavesdroppers increase dramatically, because of the many nodes in a packet network. Broadcasting ARP replies blind is sufficient to corrupt many ARP caches. Corrupting the ARP cache makes it possible to re-route traffic to intercept voice and data traffic. Use authentication mechanisms provided wherever possible and limit physical access to the VOIP network segment.

iv. Web Server interfaces:

Both VOIP switches and voice terminals are likely to have a web server interface for remote or local administration. An attacker may be able to sniff plaintext HTTP packets to gain confidential information. This would require access to the local network on which the server resides. If possible, do not use an HTTP server. If it is necessary to use a web server for remote administration, use the more secure HTTPS (HTTP over SSL or TLS) protocol.

v. IP Phone Netmask Vulnerability:

A similar effect of the ARP Cache Vulnerability can be achieved by assigning a subnet mask and router address to the phone crafted to cause most or all of the packets it transmits to be sent to an attacker's MAC address. Standard IP forwarding makes the intrusion all but undetectable.

A firewall filtering mechanism can reduce the probability of this attack. Remote access to IP phones is a severe risk.

vi. Extension to IP Address Mapping Vulnerability:

Discovering the IP address corresponding to any extension requires only calling that extension and getting an answer. A protocol analyzer or packet capture tool attached to the hub on the dialing instrument will see packets directly from the target instrument once the call is answered. Knowing the IP address of a particular extension is not a compromise in itself, but makes it easier to accomplish other attacks. For example, if the attacker is able to sniff packets on the local network used by the switch, it will be easy to pick out packets sent and received by a target phone. Without knowledge of the IP address of the target phone, the attacker's job may be much more difficult to accomplish and require much longer, possibly resulting in the attack being discovered. Disabling the hub on the IP Phone will prevent this kind of attack. However, it is a rather simple task to turn the hub back on.

B. Integrity issues:

Integrity of information means that information remains unaltered by unauthorized users. For example, bank account or passwords should be changed only by the user or an authorized security administrator. Integrity threats include any in which system functions or data may be corrupted, either accidentally or as a result of malicious actions.

Telecommunication switches must protect the integrity of their system data and configuration. Because of the affluence of feature sets presented on switches, an attacker who can conciliate the system configuration can accomplish nearly any objective. Damaging or deleting information about the IP network used by a VOIP switch results in an immediate denial of service [2].
The security system itself provides the capabilities for system abuse and misuse. That is, compromise of the security system not only allows system abuse but also allows the elimination of all traceability and the insertion of trapdoors for intruders to use on their next visit. For this reason, the security system must be carefully protected. Misuse may involve legitimate users (i.e. insiders performing unauthorized operations) or intruders.

A legitimate user may perform an incorrect, or unauthorized, operations function (e.g., by mistake or out of malice) and may cause deleterious modification, destruction, deletion, or disclosure of switch software and data. This threat may be caused by several factors including the possibility that the level of access permission granted to the user is higher than what the user needs to remain functional.

i. Intrusion threats –

An intruder may masquerade as a legitimate user and access an operations port of the switch. There are a number of serious intrusion threats. For example, the intruder may use the permission level of the legitimate user and perform damaging operations functions such as:

- Disclosing confidential data
- Causing service deterioration by modifying the switch software
- Crashing the switch
- Removing all traces of the intrusion (e.g., modifying the security log) so that it may not be readily detected

ii. Insecure state –

At certain times the switch may be vulnerable due to the fact that it is not in a secure state. For example:

- After a system restart, the old security features may have been reset to insecure settings, and new features may not yet be activated. (For example, all old passwords may have reverted to the default system-password, even though new passwords are not yet assigned.) The same may happen at the time of a disaster recovery.
- At the time of installation the switch may be vulnerable until the default security features have been replaced.

iii. DHCP Server Insertion Attack:

It is often possible to change the configuration of a target phone by exploiting the DHCP response race when the IP phone boots. As soon as the IP phone requests a DHCP response, a rogue DHCP server can initiate a response with data fields containing false information [3].
This attack allows for possible man in the middle attacks on the IP-media gateway, and IP Phones. Many methods exist with the potential to reboot the phone remotely, e.g. “social engineering”, ping flood, MAC spoofing (probably SNMP hooks, etc.).

If possible, use static IP addresses for the IP Phones. This will remove the necessity of using a DHCP server. Further, using a state based intrusion detection system can filter out DHCP server packets from IP Phone ports, allowing this traffic only from the legitimate server.

iv. TFTP Server Insertion Attack:

It is possible to change the configuration of a target phone by exploiting the TFTP response race when the IP phone is resetting. A rogue TFTP server can supply spurious information before the legitimate server is able to respond to a request. This attack allows an attacker to change the configuration of an IP Phone. Using a state based intrusion detection system can filter out DHCP server packets from IP Phone ports, allowing such traffic only from the legitimate server. Organizations looking to deploy VOIP systems should look for IP Phone instruments that can download signed binary files.

C. Availability and Denial of Service (DoS):

Availability refers to the notion that information and services be available for use when needed. Availability is the most obvious risk for a switch. Attacks exploiting vulnerabilities in the switch software or protocols may lead to deterioration or even denial of service or functionality of the switch. For example: if unauthorized access can be established to any branch of the communication channel (such as a CCS link or a TCP/IP link), it may be possible to flood the link with bogus messages causing severe deterioration (possibly denial) of service. A voice over IP system may have additional vulnerabilities with Internet connections. Because intrusion detection systems fail to intercept a significant percentage of Internet based attacks, attackers may be able to bring down VOIP systems by exploiting weaknesses in Internet protocols and services [4].

Out of the box VoIP implementations may leave TCP/UDP ports unnecessarily open and without sufficient monitoring. These, along with other default services, could create a habitat suitable for a DoS or distributed DoS attack. A distributed DoS attack is a concerted, coordinated effort to flood a network with requests. Though the attacked network may not be penetrated, these attacks can “busy” a system, rendering it unusable. To combat these attacks, security experts must ensure that

unnecessary ports and services are shut down, and that the network is properly patched for newly discovered vulnerabilities [5].

Any network may be vulnerable to denial of service attacks, simply by overloading the capacity of the system. With VOIP the problem may be especially severe, because of its sensitivity to packet loss or delay.

i. CPU Resource Consumption Attack without any account information:

An attacker with remote terminal access to the server may be able to force a system restart (shutdown all/restart all) by providing the maximum number of characters for the login and password buffers multiple times in succession. Additionally, IP Phones may reboot as a result of this attack.

In addition to producing a system outage, the restart may not restore uncommitted changes or, in some cases, may restore default passwords, which would introduce intrusion vulnerabilities. The deployment of a firewall disallowing connections from unnecessary or unknown network entities is the first step to overcoming this problem. However, there is still the opportunity for an attacker to spoof his MAC and IP address, circumventing the firewall protection.

ii. Default Password Vulnerability:

It is common for switches to have a default login/password set, e.g., admin/admin, or root /root. Similarly, VOIP telephones often have default keypad sequences that can be used to unlock and modify network information. This vulnerability would allow an attacker to control the topology of the network remotely, allowing for not only complete denial of service to the network, but also a port mirroring attack to the attacker's location, giving the ability to intercept any other conversations taking place over the same switch. Further, the switch may have a web server interface, providing an attacker with the ability to disrupt the network without advance knowledge of switch operations and commands.

In most systems, telephones download their configuration data on startup using TFTP or similar protocols. The configuration specifies the IP addresses for Call Manager nodes, so an attacker could substitute another IP address pointing to a call manager that would allow eavesdropping or traffic analysis. Changing the default password is crucial. Moreover, the graphical user interface should be disabled to prevent the interception of plaintext administration sessions.

iii. Exploitable software flaws:

Like other types of software, VOIP systems have been found to have vulnerabilities due to buffer overflows and improper packet header handling. These flaws typically occur because the software is not validating critical information properly. For example, a short integer may be used as a table index without checking whether the parameter passed to the function exceeds 32,767, resulting in invalid memory accesses or crashing of the system.

Exploitable software flaws typically result in two types of vulnerabilities: denial of service or revelation of critical system parameters. Denial of service can often be implemented remotely, by passing packets with specially constructed headers that cause the software to fail. In some cases the system can be crashed, producing a memory dump in which an intruder can find IP addresses of critical system nodes, passwords, or other security-relevant information. In addition, buffer overflows that allow the introduction of malicious code have been found in VOIP software, as in other applications [6].

These problems require action from the software vendor, and distribution of patches to administrators. Intruders monitor announcements of vulnerabilities, knowing that many organizations require days or weeks to update their software. Regular checking for software updates and patches is essential to reducing these vulnerabilities.

Automated patch handling can assist in reducing the window of opportunity for intruders to exploit a known software vulnerability.

iv. Account Lockout Vulnerability:

An attacker will be able to provide several incorrect login attempts at the telnet prompt until the account becomes locked out. (This problem is common to most password-protected systems, because it prevents attackers from repeating a login attempt until the correct password is found by trying all possible combinations.)

The account is unable to connect to the machine for the set lockout time. If remote access is not available, this problem can be solved with physical access control.

v. Spam over IP telephony (SPIT):

Spam over IP telephony (SPIT), involves pre-recorded, unsolicited messages sent to the VoIP handset. SPIT owes its existence to the standard communications protocol called Session Initiated Protocol (SIP). SIP acknowledges the presence of a VoIP handset. The dialer programs can deliver an unsolicited programmed message, and have a better chance of a recipient picking up the call. SPIT carries with it other risks, such as DoS attacks, and the unauthorized use of resources (bandwidth), making SPIT much more than a nuisance.

SPIT's effects are lessened by a solid patch management solution, VoIP enabled firewalls are likely capable of

identifying SPIT, and create an authentication mechanism to identify true authorized callers. In short, the philosophy of combating SPIT is very similar to current day methods used to combat SPAM; it is impossible to stop it, you can only hope to control it [7].

vi. Limited gateway security options:

Securing VoIP traffic at the firewall level presents certain challenges because not all firewalls are VoIP aware. An older firewall may not recognize VoIP protocols such as SIP, MGCP or any other proprietary protocol, and may incorrectly block the traffic. Most of the firewalls actively scan traffic packets as an intrusion detection or prevention system. Due to the time-critical nature of VoIP traffic, this sort of scanning is not recommended. Experts set a threshold of 300 milliseconds to setup a call, and 100 milliseconds end-to-end packet delivery. Given these performance constraints, many security measures implemented in traditional data networks are simply not applicable to VoIP. The industry does not have a good answer to active packet scanning on VoIP implementations at this time. The best advice is to attempt full traffic scanning, measure the results, and determine if the IDS/IPS system is able to scan without performance issues.

III. CONCLUSION

Every good thing comes with a cost associated with it and IP Telephony is no more exception to it. The most popular VoIP communication technology has lot many security concerns attached to it, which needs to be taken care of before implementing it. The paper has highlighted various VoIP security issues, vulnerabilities and their importance in current scenario. Due to convergence of many networks IP Telephony has more complications contrary to their underlying data or telecommunication networks. This communication network therefore requires more cautious and serious attention for maintaining reliability and quality.

REFERENCES

[1] Thomas J.; Kuhn D.R.; Fries S. (2005) "Security Considerations for Voice over IP systems", *Technology Administration U.S. Department of Commerce*, National Institute of Standards and Technology NIST, Special publication, NIST SP 800-58

[2] Patrick C.K. Hung; Miguel Vargas Martin (2006), "Security Issues in VoIP Applications", *IEEE Conference publication, Canadian conference on Electrical and Computer Engineering*, CCECE '06, pp. 2361-2364.

[3] Butcher, D.; Xiangyang Li; Jinhua Guo (2007), "Security Challenge and Defence in VoIP Infrastructures", "*IEE Journals and Magazines*", Year 2007, vol. 37, issue 6, pp. 1152-1162

[4] Coulibaly, E.; Lian Hao Liu (2010), "Security of VoIP Networks", *IEEE Conference Publications, 2nd International Conference on Computer Engineering and Technology*, ICCET 2010, vol. 3, pp. v3-104-v3-108

[5] Feng Cao; Malik, S. (2005), "Security analysis and solutions for deploying IP Telephony in the critical infrastructure," *Workshop of 1st International Conference on Security and Privacy for Emerging Areas in Communication Networks*, pp. 171 – 180

[6] Ruck M. (2010), "Top Ten Security Issues Voice over IP (VoIP)", White Paper, www.designdata.com, Technology Consultants and Network Engineers

[7] Xiaohui Yang, Ram Dantu, DumindaWijesekera, "Security Issues in VoIP Telecommunication Networks", Chapter 30