ISSN : 0976-8491 (Online) | ISSN : 2229-4333 (Print)

Analysis of Security Threats in Voice Over Internet Protocol (VOIP)

[1]Mayank Patel, [2]B. V. Buddhdev
[1,2]Dept. of Computer Engineering, L. D. Collage of Engineering, Ahemdabad, Gujarat, India

Abstract
The VoIP system is build on the IP network, so it is affected by the IP network security problem. It has many security problems because of the security mechanism of VoIP system and other external factors. These effects relate to the following three aspects: confidentiality, integrity and availability. This paper makes a detailed analysis discussed several security potential threats by dividing it into several categories like social, eavesdropping, service abuse, etc. and finally shows how this threats are harmful to VoIP.

Keywords
VOIP, Security Threats

I. Introduction of VOIP

Voice Over Internet Protocol (VOIP) is a technology that allows users to make telephone calls using a broadband Internet connection instead of an analog phone line. VoIP holds great promise for lowering the cost of telecommunications and increasing the flexibility for both businesses and individuals. VoIP leverages existing IP-based packet-switched networks to replace the circuit-switched networks used for voice communications since the invention of the telephone [1]. The VoIP infrastructure consists of endpoints (telephones), control nodes, gateway nodes, and the IP-based network. The IP network can utilize various media including Ethernet, fiber, and wireless. The VoIP system interacts with both local and remote VoIP phones using the intranet and Internet as well as interacting with phones connected to the public-switched tele- phone network (PSTN) through gateways. As VoIP resides on the IP network, the vulnerabilities in VoIP encompass not only the flaws inherent within the VoIP application itself, but also in the underlying operating systems, applications, and protocols that VoIP depends on [5]. The unauthorized access, worms, viruses, Man-in-the-Middle, denial of service attacks which are not previously issues with the circuit-switched network are now easily implemented in VoIP.

II. VOIP Threat Classification

To classify the surveyed work, we use the taxonomy provided by the Voice over IP Security Alliance (VoIPSA) 3. VoIPSA is a vendor-neutral, not for profit organization composed of VoIP and security vendors, organizations and individuals with an interest in securing VoIP protocols, products and installations. The VoIPSA security threat taxonomy [7] aims to define the security threats against VoIP deployments, services, and end users. The key elements of this taxonomy are [1]:

- Social Threats
- Eavesdropping
- Interception and Modification
- Service Abuse
- Intentional Interruption of Service
- Other Interruptions of Service

A. Social Threats

Social threats focuses on how to manipulate the social context between communication parties so that an attacker can misrepresent himself as a trusted entity and convey false information to the target user [2]. This definition describes threats categorized under misrepresentation but theft of service and unwanted contact are also categorized as social threats. These threats can be seen in fig. 1.

Fig. 1: Social Threat

1. Misrepresentation

Misrepresentation is an assertion or manifestation by words or conduct that is not in accord with the facts. As can be seen in Figure 2 the attacker claims to be User A by presenting false information to User B (the victim) [3]. This is done e.g. in order to gain access to otherwise unreachable information, gain access to toll calls, call logs, files and for phishing purposes. The attacker may misrepresent his identity, authority, rights and/or content in order to fulfill his achievements.

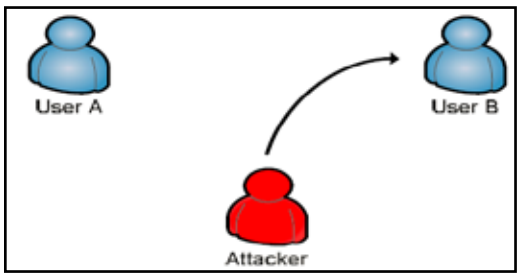

Fig. 2: Misinterpretation

2. Theft of Service

Theft of service stands for any use of service without proper payment. Toll frauds have been a part of the telephone system almost from start and VoIP is no different [4]. Typical theft of service is placing calls without payment. This may be done by hacking the system or changing billing information. More serious attack is the unlawful taking of service provider property. Over the years many cases have come up where computer criminals hack a service provider and sell his phone minutes on the black market. Attacks on private telecommunication stations are also increasing in number and magnitude. The number of minutes sold can be in thousands or even millions so the financial loss for the victim can be significant.

3. Unwanted Contact

Unwanted contact is any contact that either requires prior affirmative consent for incoming calls or bypasses a refusal of consent for outgoing calls (VoIPSA, 2005). Harassment, extortion and unwanted lawful content fall under this category. The biggest issue, of those three, for service providers and users is the unwanted lawful content. Unwanted lawful content may include lawful pornography, advertisements and/or other unwanted messages. In many cases the attacker sends out a bulk of session initiation attempts to the user in order to spam messages to him as can be seen in fig. 3. Everybody is familiar with the annoying e-mail spams that count for up to 95% of all email traffic. They have been countered with filters, which are capable of blocking about 90% of all spams, and the awareness of users. With VoIP came the possibility of spam over IP telephony or SPIT [4]. SPIT is somewhat comparable to PSTN-call spam in the form of telemarketer calls. The main difference is that through VoIP those sorts of calls are made much easier due to lower call cost, spam applications and so on. Attackers can even infect other users with viruses and utilise their bandwidth to generate spam.

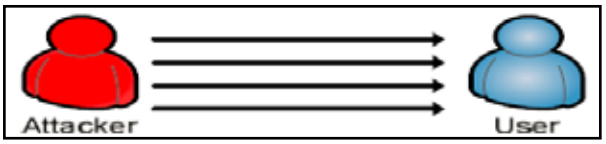

Fig. 3: SPIT Attack

SPIT is getting more popular due to the fact that it's much harder to counter than e-mail spam. Since voice is real-time media users can't recognize spam until they have listened to its content.

B. Eavesdropping

Eavesdropping is when an attacker intercepts a data stream between two or more users without altering the data [4]. The attacker does however gain access to the conversation between the users, as can be seen in fig. 4, making users vulnerable to the threats shown in fig. 5.

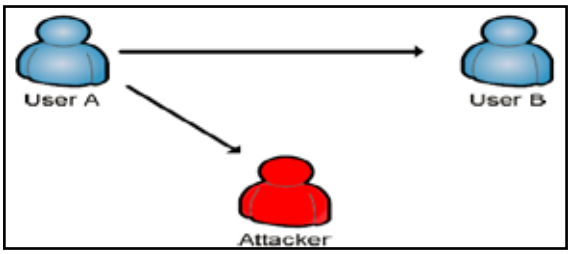

Fig. 4: Evasdropping Attack

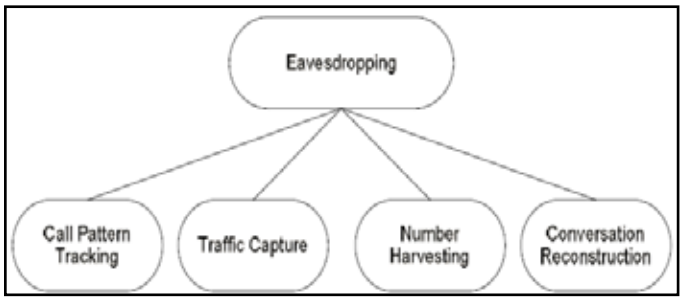

Fig. 5: Evasdropping Attack Threats

1. Call Pattern Tracking

Call pattern tracking is the unauthorized tracking of users' call pattern. This enables the attacker to capture and analyze victims' phone records and use it to his advantage. This means the attacker can see who the victim has been calling which can be helpful in many situations. Reasons for these attacks may include theft, extortion and espionage [4]. Traffic Capture In traffic capture, the attacker can capture ingoing/outgoing traffic and eavesdrop it. He however can't alter the traffic in any way. Number Harvesting Number harvesting is the unauthorised collection of IDs, usually in the form of phone numbers. The attacker monitors incoming/ outgoing calls in order to build a database of legitimate IDs. The databases can be used for other attacks such as SPIT, toll fraud calls and DoS attacks.

2. Reconstruction

Reconstruction refers to any unauthorized monitoring, recording, storage, reconstruction, recognition, interpretation, translation and/or feature extraction of any portion of a media session without consent of the owner (VoIPSA, 2005).

C. Interception and Modification

Threats in this category describe attacks where the attacker can intercept and modify the traffic between two or more endpoints [6]. In fig. 6, scenario is depicted where the attacker has intercepted traffic between two endpoints. The attacker now has the power to implement the threats shown in fig. 7. These attacks are also known as MitM attacks.

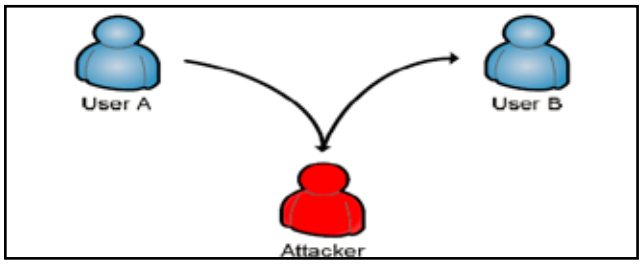

Fig. 6: Interception and Modification

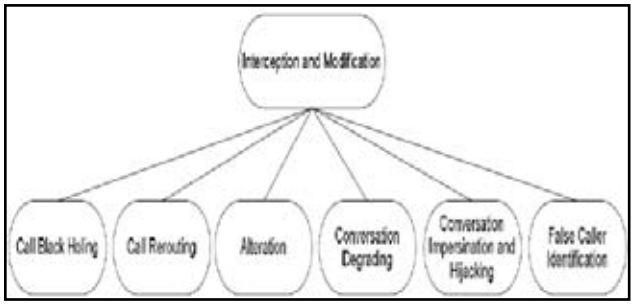

Fig. 7: Interception and Modification Threat

1. Call Black Holing

Call black holing stands for any unauthorized method of redirecting essential elements of any VoIP protocol, usually SIP or H.323. This results in delayed call setups, errors in applications, dropped calls and other denial of service [6]. One example of a black holing attack is when an attacker denies all incoming calls to a specific organization such as hospitals, banks or police stations.

2. Call Rerouting

In call rerouting the attacker changes the call direction from one or more endpoints by altering the routing information in the protocol message [12]. Reasons for rerouting are to either include illegitimate notes into a communication or exclude legitimate ones. Attacker can use this attack for scams. One example is when an attacker reroutes incoming calls, e.g. to a bank, to himself and attempts to gain critical information from the user in the process, e.g. PIN numbers [6].

3. Alteration

Alteration, as the name applies, refers to any unauthorized alteration of communication. The attacker will alter some or all of the communication between endpoints in order to e.g. misrepresent identity, or deliver undesired information. These attacks can be extremely dangerous for the users as, in many cases, they think they are talking to a trusted person and may give up critical information to the attacker.

4. Conversation Degrading

Conversation degrading stands for any unauthorized reduction in QoS of any communication. The attacker intercepts and manipulates the media packets in a communication in order to introduce latency, jitter and so on. Reasons for these attacks may be to frustrate users or undermine SP's reputation.

5. Onversation Impersonation and Hijacking

Conversation impersonation and hijacking includes any modification of a communication in order to impersonate a trusted user or hijack the traffic completely.

6. False Caller Identification

False caller identification is a threat where the attacker calls a user and manages to signal untrue identity [4]. One example is where an attacker represents a bank employee, or other trusted person, and asks for a PIN number or any other critical information. The victim may be more likely to give out this information if he sees the banks phone number calling him.

D. Service Abuse

Service abuse covers threats regarding any kind of fraudulent activity regarding VoIP. List of threats can be seen in Figure 8.

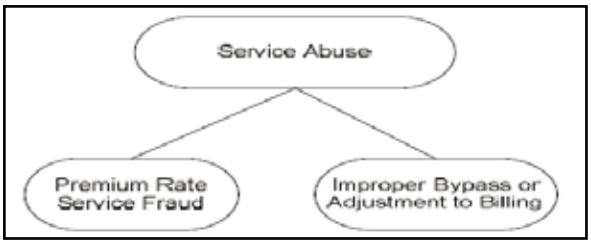

Fig. 8: Service Abuse Threat

1. Premium Rate Service Fraud

Premium rate service fraud is the act of deceiving someone to call a premium rate number without offering some reward or service for the process [8]. Premium rate numbers bear higher calling cost as portion of the fee goes to the owner of the number. Fraudsters have manyways of enticing users to call these numbers and one popular way is by false advertisement. Improper Bypass or Adjustment to Billing This threat describes any unlawful method to avoid service charges or bills.

E. Intentional Interruption of Service

Threats in this category all aim at interrupting users from using VoIP and/or other service as depicted in fig. 9. In most cases the attacker has no personal gain from these attacks so the biggest motivation for attacks in this category is to annoy the victim. Intentional interruption can be carried out in many ways. DoS threats, especially VoIP specific ones, count for the largest part of intentional interruption threats.

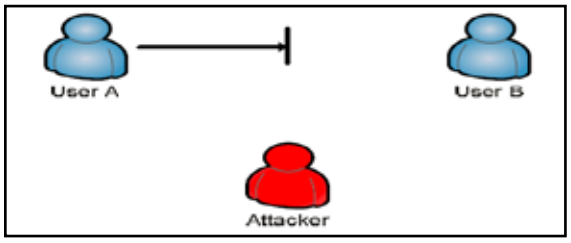

Fig. 9: Interruption of Service Threat

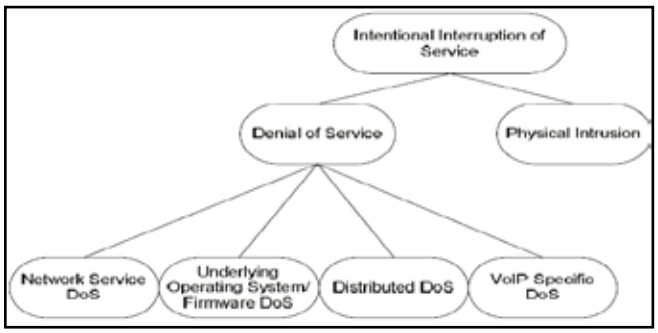

Fig. 10: Interruption of Service Categories

1. Denial of Service

Denial of service or DoS attacks are well known in the computer world as hackers, through the years, have applied various ways to deny users of some sort of service. DoS attacks are defined as attempts to make computer resources unavailable to their intended users and this is precisely what they do [4]. The hacker, through various measures, floods the system and makes it unable to function correctly in the process. Since VoIP is IP based it is also vulnerable to DoS threats. There are number of ways that an attacker can deny VoIP service but the threats can be divided into four categories. These categories will now be studied further.

2. Distributed DoS

DDoS is an attack where number, often thousands or even millions, of computers are utilized to attack a single target. Usually the attacker utilizes a number of computers without their owner consents to form a so-called botnet. These bonnets are then controlled by one master computer and their forces combined to attack a single target, flooding it with countless number of packets.

3. Underlying Operating System or Firmware DoS

Most of the underlying OS and firmware for VoIP is run on popular operating systems or firmware that regularly becomes vulnerable to new threats, e.g. viruses. Vendors update their products regularly but hackers are quick to find and exploit any sort of vulnerability in the underlying systems.

4. Network Services DoS

Network service DoS describes the threat that an attacker targets network components or services that the VoIP service depends on. For example the attacker can flood routers, switches, proxies, etc [10]. making them unable to function properly and therefore close down any VoIP service passing through these network components. The attacker can also target services that VoIP depends on like DNS and DHCP with the same results.

5. VoIP Specific DoS

Threats in this category are all VoIP specific i.e. they all utilize vulnerabilities in VoIP protocols, endpoint software, setup etc. to enable attacks. Physical Intrusion Physical intrusion describes the threat that an unauthorized person gains access to a protected premise [10]. If that premise is accessed the attacker can cause serious damage to a VoIP system by various methods. The premise can be in the form of a tangible asset such as a building or a facility. It can also be in the form of an intangible asset such as the physical layer of the OSI model.

F. Other Interruptions of Service

This category hosts other threats that interrupt VoIP service but aren't necessarily intentional. The threats can be seen in fig. 11.

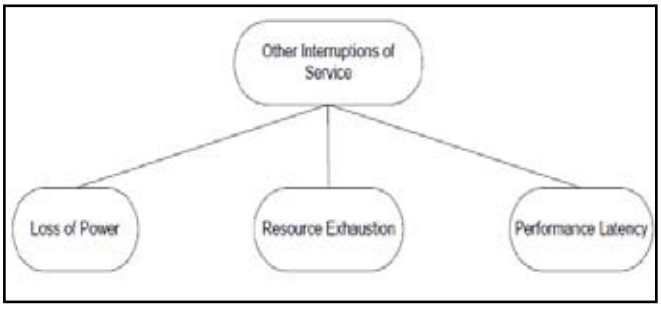

Fig. 11: Other Interruption

1. Loss of Power

Since VoIP is data network based, power loss will deny users of any service unless they have some backup power in place. Power loss can have various causes, both intentional and unintentional. Intentional causes include vandalism, theft, terrorism etc. often in the form of direct physical damage to power stations or other power sources. Regular power outage will deny endpoint devices of service since they rely on external power sources and are seldom UPS-protected.

2. Resource Exhaustion

Resource exhaustion is a simple denial of service condition which occurs when the resources necessary to perform an action are entirely consumed, therefore preventing that action from taking place. (OWASP, 2009). Resource exhaustion can origin from various causes. Attackers can flood a victim's system with various requests, depleting all CPU memory in the process. Faults in software/hardware and viruses may also cause resource exhaustion in various ways [7].

3. Performance Latency

Latency, or delay, is measured as the time it takes a packet to travel from its origin to its final destination. The delay can be divided into three categories: Propagation delay, handling delay and serialization delay [4]. Propagation delay is caused by the length that a signal has to travel in packet networks. Handling delay describes the delay caused by devices that forward the packet through a network (e.g. packetization, compression, and packet switching). Finally serialization delay is the time it takes to place a bit/byte onto an interface.

III. Conclusion

Because VoIP is on the application of the Internet, It has the inevitable problem of Internet security. With the VoIP system, the popularity of it brings more prominent security issues. This paper introduces VoIP system which may be subjected to attacks. VoIP systems can build a security system as a supplementary means of enhancing the security of VoIP in order to achieve the traditional telephone the safety of the system level. In the practical applications, VoIP security, which involves many aspects of protocol, network equipment, code writing, operating system security, user security awareness, and many other aspects, is a comprehensive project.

References

[1] D. Keromytis,"Voice over IP: Risks, Threats and Vulnerabilities", in Proc. Cyber Infrastructure Protection (CIP) Conference, June 2009.

[2] A. D. Keromytis,"A Look at VoIP Vulnerabilities", USENIX ;login: Magazine, Vol. 35, pp. 41–50, February 2010.

[3] A. D. Keromytis,"Voice over IP Security: Research and Practice", IEEE Security Privacy Mag., Vol. 8, pp. 76–78, March/April 2010.

[4] VoIP Security Alliance (2005),"VoIP Security and Privacy Threat Taxonomy, version 1.0.", [Online] Available: http://www.voipsa.org/Activities/taxonomy.php

[5] R. Zhang, X. Wang, R. Farley, X. Yang, X. Jiang,"On the Feasibility of Launching the Man-In-The-Middle Attacks on VoIP from Remote Attackers", in Proc. 4th International ACM Symposium on Information, Computer, and Communications Security (ASIACCS), pp. 61–69, March 2009.

[6] M. Petraschek, T. Hoeher, O. Jung, H. Hlavacs, W. N. Gansterer,"Security and Usability Aspects of Man-in-the-Middle Attacks on ZRTP", Journal of Universal Computer Science, Vol. 14, No. 5, pp. 673–692, 2008.

[7] R. MacIntosh, D. Vinokurov,"Detection and Mitigation of Spam in IP Telephony Networks Using Signaling Protocol Analysis", in Proc. IEEE/Sarnoff Symposium on Advances in Wired and Wireless Communication, pp. 49–52, April 2005.

[8] R. Baumann, S. Cavin, S. Schmid,"Voice Over IP - Security and SPIT", KryptDet Report FU Br 41, Swiss Army, August/September 2006.

[9] A. Madhosingh,"The Design of a Differentiated SIP to Control VoIP Spam", Masters Thesis Report SPIT, CAPTCHA, Florida State University, Computer Science Department, 2006.

[10] C. Wieser, J. R¨oning, A. Takanen,"Security analysis and experiments for Voice over IP RTP media streams", in Proc. 8th International Symposium on Systems and Information Security (SSI), November 2006.

[11] F. Palmieri, U. Fiore,"Providing True End-to-End Security in Converged Voice over IP Infrastructures", Computers & Security, Vol. 28, pp. 433–449, September 2009.