International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)
Web Site: www.ijettcs.org Email: editor@ijettcs.org, editorijettcs@gmail.com
Volume 3, Issue 2, March – April 2014 ISSN 2278-6856

Analysis of various possible threats in VoIP in order to design network security mechanism

Navneet Kumar Verma[1] and Rahul Saxena[2]

[1&2]School of Computer & Systems Sciences, Jaipur National University,
Near New RTO, Jagatpura, Jaipur

Abstract- ***VoIP used for voice and data over internet. As the VoIP has the advantages of low cost implementation, portability and flexibility is has gain its usages in major organizations as compared to other communication media. It is a new way of communication with Public Switched Telephone Network (PSTN) and cellular network, with the benefit of using voice messaging, calling, video messaging as well as video conferencing with file sharing. We can see all the services in VoIP based application like Skype, Google talk, Yahoo Messenger etc. Due to these types of services like file sharing and data sharing this application is more prone to to lose, theft and security of data and information to various types of threats. In this paper we have discussed basics of VoIP, possible threats in VoIP and focused on main categories and methods which are useful to resolve these types types of vulnerabilities.***

Keywords- *VoIP, N/W Security, Possible threats.*

1. INTRODUCTION

VoIP stands for voice over internet, it is a facility provided to the customer for using telephone call service over the internet. *According to CISCO VoIP refers to a way to carry phone calls over an IP data network, whether on the Internet or your own internal network [7].* A primary attraction of VoIP is its ability to help reduce expenses because telephone calls travel over the data network rather than the phone company's network. It is rapidly used today and new way of communication with Public Switched Telephone Network (PSTN) and cellular Network [1]. VoIP can be used to call any PSTN telephone or mobile phone anywhere in the world. But there are some services which can be used by only a special computer or VoIP specific phone [2]. VoIP refers to a class of products that enable advanced communication services over data networks, with other capabilities like collaborative editing, whiteboard sharing, file sharing, calendaring, etc. and it works on packet switched network rather than traditional circuit and public switching telecommunication network. There are many advantages of VoIP other than as list in the abstract like extendibility which support multiple user at a time for using data and voice services, optimized utility of resources, ease of setup and implementation, mobility, simple user control interface and portability. Yahoo Messenger, Google Talk, Skype, and Face book Messenger etc are the best examples that make usages of VoIP services for its associated applications and they proved its attractions to the end users for their services and key features. Many papers has been published regarding VoIP and possible threats in VoIP but the main motive behind this paper is to presents the basic knowledge of VoIP, security measures for VoIP based applications and to find the solution to minimize the issues and challenges of possible threats and vulnerabilities in VoIP. This paper is structured as follow. In section 2 we discuss various literature reviews regarding selected problem. Section 3 presents the overview of possible attacks and threats in VoIP, section 4 represent the solutions of these threats and issues, in section 5 we will present result and discussion and finally section 6 gives conclusion and future work.

2. RELATED WORK

Protection of business private data is the most important concern for most of the commercial companies and institutions. VoIP is a new technology which emerged since late 90s. Although, this new technology was accomplished with many security risks; it is still considered more secure than a traditional telephone (e.g. PSTN) communication [4]. It is because of the new risks accomplished with the new technologies [3], merging voice with data to be transmitted in data network by using IP as an identifier is considered as an attractive area of research which is the basis of VoIP. In order to establish this communication using VoIP multiple protocols are combined together, each of these protocols servers their own features and properties; and that makes the area of attack wider for the attacker. Nowadays various businesses organizations are migrating from the legacy traditional enterprise telephone PSTN to VoIP, since VoIP provides the benefit of the class of technologies that enables multimedia (text/voice/video) traffic to be transmitted over IP networks. The fundamental concept of VoIP is the digitization and packet formation of the human voice. The speech (voice analogue signals) is converted into digital signals by appropriate coders/decoders and it is then broken into packets and transferred over Internet Protocol (IP)-based networks like the Internet [4]. Generally, VoIP uses the existing IP networks and therefore inherits their vulnerabilities. Adding voice traffic to IP networks complicates security issues and introduces a range of new vulnerabilities. This is because VoIP requires VoIP-specific configurable parameters in addition to the existing ones in the underlying IP networks, such as call. Security related to VoIP is used to protect the services to possible attacks and threats and attacks and their possible method for these attacks [4]. Due to network security it is essential to find out the reason and threats which can cause the information losses and modifications.

3. OVERVIEW AND POSSIBLE ATTACKS

Statement of the Problem:

Possible threats in VoIP and enhancement of network security. There are many possible threats in VoIP.

3.1 Denial of Service or VoIP Service Disruption

Denial-of-service (DoS) attacks can affect any IP-based network service, and is the most challenging treat in VoIP applications since not only data but also the voice are transferred on the same channel. Denial of Service is the type of attack in which packets can simply be flooded into or at the target network from multiple external sources and may result the complete network blockage at extreme conditions.

3.2 Call Hijacking and Interception

Call interception and eavesdropping are other major concern on VoIP networks which cause theft of information and services on VoIP networks (Benini and Sicari, 2008). The existence of this threat in VoIP applications is because of the fact that a VoIP service does not use any authentication measures before establishing communication and application use. This threat demonstrates the need for security services that enable entities to authenticate the originators of requests and to verify that the contents of the message and control streams have not been altered in transit [3].

3.3 H.323 Specific attacks

H.323 is signaling protocol in VoIP communications which is encoded according to ASN.1 PER encoding rules. The implementation of H.323 massage parser, rather than the encoding rules themselves cause vulnerabilities in H.323 suits (Porter, 2006). So for resolving these types of threats several methodologies have been approved for VoIP security. Some have worked on the tools, others have given theoretical frameworks, models, some have given simulations, others have proposed algorithms or modified a protocol, some have dealt with the problem in a theoretical manner, others have built a prototype etc.

3.4 Eavesdropping

The VoIP eavesdropping in principle is different from the traditional eavesdropping in data networks, but the general concept of eavesdropping remains the same. In VoIP the eavesdropping is the process of intercepting the signaling messages and associated multimedia streams of a conversation. The signaling messages use separate network protocols like UDP or TCP and ports from the media itself, while the multimedia streams typically are carried over UDP using the Real Time Streaming Protocol.

3.5 Password authentication

Circumventing password authentication using dictionary or brute force attacks will always be possible given a large user base combined with poor security practice. Using the client/server mode of authentication is not, on its own, a strong method to ensure that only legitimate endpoints communicate with each other before the communication commences. It can only provide a basic first step toward a secure architecture.

3.6 VoIP Phishing (Vishing)

Vishing is the act of using the telephone in an attempt to scam the user into surrendering private information that will be used for identity theft. It will not take long until criminals discover the potential monetary benefits of social engineering attacks as exemplified by e-mail spam. Even though phishing is not an attack on a computer system itself, it gives the attacker access to it by using social engineering techniques on legitimate users of the VoIP system.

4. SOLUTIONS

4.1 Solution against Denial of Service attack

Any VoIP network can be targeted for a DoS attack. Preventative measures include strengthening authentication safeguards, removing unnecessary network services, avoiding link ups with unauthenticated components and using strong firewalls. All of this may not stop a mass DoS attack, but it will give your system a fighting chance at survival.

4.2 Solution against call hijacking and interception attack

Call interception and eavesdropping are major concerns on VoIP networks. This family of threats relies on the absence of cryptographic assurance of a request's originator. Endpoints must be authenticated, and end users must be validated in order to ensure legitimacy.

4.3 Solution against H.323 specific attack

To solve H.323 attack we need to update organizational existing security policies, practices, and procedures to meet the need of the new requirements for converged networks, and its proper distribution, communication and to enforce these policies, ensure that all networked systems are patched, and virus scanners are up to date, install and monitor IDS, IPS, and Honeypots. Exercise diligence in analyzing logs from intrusion detection systems, firewalls, routers, servers and other network devices, create strategies for secure offsite backups and develop disaster recovery plans, encrypt H.323 traffic, utilize VPNs wherever possible. Employ H.323-ready firewalls and other appropriate protection mechanisms, and properly configure them [13]. Consider segmenting voice and data traffic by using a virtual LAN, limiting the threat posed by packet-sniffing tools and minimize disruption in the event of an attack.

4.4 Solution against eavesdropping

Long (2002) recommends four strategies to prevent eavesdropping:

- Employing flawless hardware.
- Ensuring that access to wiring closets is restricted to authorize personnel only.
- By implementing address securities using port-based MCA address filtering on any vulnerable network point; for example, on reception courtesy phone.
- Initiating a procedure to regularly scan the network for devices running in promiscuous mode.

4.5 Solution against password authentication

There is a password for each user for authentication. So when he/she access his account or accessing his/her information he set his/her password and easily accesses his/her information. Each user has its own and unique password for authentication purpose and for uniqueness a digital signature and cryptography scheme also used.

4.6 Solution against VoIP phishing attack

Catching VoIP phishers is no less difficult than snaring their e-mail counterparts. Enterprise VoIP system managers can fight VoIP phishers with the same technology which they use to detect SPITters: software that examines records for abusive calling patterns. Managers also need to alert system users to the phishing threat, telling them to treat unexpected phone calls with the same skepticism they apply to out-of-the-blue emails.

5. Result And Discussion

As a result of this paper we give a survey of possible attacks in VoIP for further enhancement of network security and solution of these attacks. This survey represent goal towards network security in VoIP.

6. Conclusion And Future Scope

The main motive behind this paper is to know more about the VoIP and the network security. In this paper possible threats which affect the VoIP services are discussed and also their solutions are given. So this paper is useful to find out the additional threats and give a future scenario to resolving those threats. In future we supposed to build a model which is used to configure and find out possible threats and vulnerabilities, in any educational institutions

References

[1] Mehdi Jahanirad, Yahya AL-Nabhani and Rafidah Md. Noor, "Security measures for VoIP application: A state of the art review", *International Journal on Scientific Research and Essay*, 6(23), Pages 4950-4959, (2011).

[2] Ram Dantua, Sonia Fahmyb, Henning Schulzrinnec, Joa˜o Cangussud, "Issues and challenges in securing VoIP", *Computer Security*, (2009).

[3] Porter T, Threats to VoIP Communication Systems, Syngress Force Emerging Threat Analysis, p. 3-25.

[4] Thermos P, Two attacks against VoIP, Symantec, Retrieved March 13, 2011 Web Reference http://www.symantec.com/connect/articles/twoattacks-against-voip

[5] Alireza Heravi, Sameera Mubarak, "Evaluation of Users' Perspective On VoIP's Security Vulnerabilities", *9th Australian Information Security Management Conference*, Australia, 94(2011).

[6] Porter T, Gough M, "How to cheat at VoIP security", Syngress Publishing, (2007)

[7] Park P, "Voice over IP security", Cisco Press, (2009).

[8] Igor Jouravlev, "Mitigating Denial-of-Service Attacks on VoIP Environment", *The International Journal of Applied Management and Technology*, 6(1), Pages 182-223, (2008).

[9] Muhammad Tayyab Ashraf, John N. Davies and Vic Grout, "An Investigation into the Effect of Security on Performance in a VoIP Network", *Proceedings of the Fifth Collaborative Research Symposium on Security, E-Learning, Internet and Networking*, Germany, 15(2009).

[10] Angelos D. Keromytis, "A Survey of Voice over IP Security Research", *Communications Surveys & Tutorials*, IEEE, 14(2), Pages 514-537, (2012).

[11] Florian Fankhauser, at. al., "Security Test Environment for VoIP Research", *International Journal for Information Security Research (IJISR)*, 1(1/2), Pages 53-60, (2011).

[12] Santi Phithakkitnukoon, et. al., "VoIP Security - Attacks and Solutions", *Information Security Journal: A Global Perspective*, 17(3), Pages 114-123, (2008).

[13] Thomas P., H.323 Mediated Voice over IP: Protocols, Vulnerabilities; Remediation, updated 2 November 2010, [online] Available: http://www.symantec.com/connect/articles/h323-mediated-voice-over-ip-protocols-vulnerabilities-amp-remediation.