Network and Complex Systems
ISSN 2224-610X (Paper) ISSN 2225-0603 (Online)
Vol.3, No.3, 2013
www.iiste.org

Prevalent Network Threats and Telecommunication Security Challenges and Countermeasures in VoIP Networks

Eze Elias Chinedum[1]*, Elechi Onyekachi O.[1], Sijing Zhang[2]

1. Department of Computer Science, Faculty of Physical Sciences, Ebonyi State University Abakaliki, P.M.B. 053, Ebonyi State, Nigeria.
2. Department of Computer Science and Technology, University Of Bedfordshire, United Kingdom.

*E-mail of the corresponding author: elias.eze@study.beds.ac.uk

Abstract

Due to the recent global popularity gained by VoIP network while many organisations/industries are employing it for their voice communication needs, optimal security assurance has to be provided to guarantee security of their data/information against present day teeming security threats and attacks prevalent in IP-based networks. This research paper has critically investigated and analysed most of the security challenges associated with VoIP systems and traditional IP data networks; and has proposed several defence measures which if designed and implemented will prevent most (if not all) of the security threats plaguing these networks.

Keywords: Network security, VoIP, Computer attack, Security threats, SIP, H.323, Defence measures, IPSec.

1. Introduction

Voice over Internet Protocol (VoIP) is a very rapid evolving communication technology which supports transportation of voice data via IP based networks. This technology has turned out to be a possible replacement to the conventional circuit switched PSTN. It consists of a web of communication protocols or technologies used in making telephone calls via a broadband access internet connection by a calling node (or endpoint) to a receiving node. VoIP is defined as a packetized Voice traffic sent over an IP network [1]. It is made up of IP-based network, control nodes, gateway nodes as well as endpoints or telephones. The VoIP networks use the intranet and internet to communicate with local and remote VoIP phones as well as communicate with phones that are connected to the traditional PSTN [2] through their gateway nodes.

VoIP networks provide a great advantage of minimal cost of telecommunication service provision. In their research work, Butcher *et al* claim that many organisations are using the VoIP technology in order to cut cost as well as to improve overall productivity. The wide adoption of VoIP systems no doubt stems from the fact that it provides far reaching benefits in terms of voice communications through internet with the minimal cost.

Internet is an open system with little or no security, hence, the teeming increase of security challenges in VoIP networks. Such security threats as eavesdropping and toll fraud as well as DoS/DDoS and many others are forms of attacks that are prevalent in VoIP and hosts of other related IP data networks.

VoIP technologies like the IP telephony system entails sending voice signal transmissions as data packets over private or public IP networks as well as re-assembling and decoding the packetized data on the receiving end [4]. The VoIP data processing is made up of the following three (3) steps:

- *Signalling* – signalling protocol is needed to establish and maintain connections or calls between endpoints (telephones). Session Initiation Protocol (SIP), Media Gateway Control protocol (MGCP), H.3232, [3, 14] etc are VoIP signalling protocols, but SIP and H.323 are two most generally used signalling standards for establishing and managing calls in IP telephony.

- *Encoding and transport* – when connection is established between two endpoints, voice streams are converted and transmitted in digital form, and segmented into a stream of digitised packets. An analog-to-digital converter (ADC) is used in converting the voice signal from analogue to digital together with the application of compression algorithms (voice codecs) to reduce volume of data for transmission and minimise bandwidth wastage. Real-time Transport Protocol (RTP) [5] is now used to carry the stream of packets over the internet, and these RTP packets use the header fields to hold the data which will be used to reassemble the packets into a voice signal at the other endpoint of the connection to enable the

recipient hear the sender's voice. User Datagram Protocol (UDP) carries the compressed voice packets by the application of suitable voice codec and transmits them as payload. This whole process is reversed at the other endpoint where the compressed packets are disassembled and put into the original order using a digital-to-analogue converter (DAC) to enable the called party's handset speaker to produce analogue voice message.

- *Gateway control* – it is the task of IP network to carry-out the transmission of the converted voice packets across the IP telephony system.

VoIP network architecture like every other IP telephony/data network technologies that use the Internet as medium of signal transmission presents a myriad of vulnerabilities because of the loose security over Internet transactions. Figure 1 depicts a typical VoIP network architecture with the necessary network elements required to design, configure and implement effective VoIP system. Some typical threats prevalent in VoIP networks as well as their proposed defence measures are dissected in detail in the following sections.

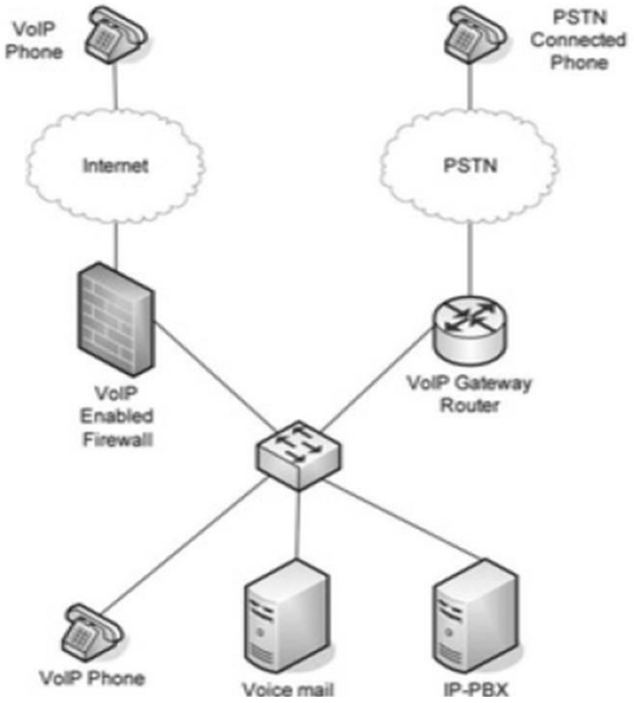

Figure 1. A typical VoIP network architecture [3]

2. Literature Review

Network attacks in forms of malicious codes, denial of service (DoS), pharming, toll fraud as well as distributed DoS (DDoS) [1-3, 5] are among the security threats observed in VoIP networks as a result of their vulnerabilities. In VoIP networks, these attacks create adverse effects on the system by taking over the system's resources, denying legitimate users access, corrupting codes and data as well as compromising confidentiality of the entire system [6]. Every system that is connected to the Internet just like the VoIP system is always sensitive to malicious codes such as worms, viruses, Trojan, and so on, which infect several hosts by way of creating congestion in network system. The challenges of VoIP network security and provision of set of guidelines for those organisations using IP telephony technology have been investigated in [3, 5, 7].

VoIP phones (or other VoIP network devices) using Bluetooth wireless technology are also directly attacked by such malicious codes like Ralea Odenga virus. Many other groups of malicious codes and security threats prevalent in VoIP network propagates widely and are always difficult to detect especially when those malicious software used by the intruders are encrypted and changes its representation on each new infection. Intrusion Detection Systems (IDS) [19, 20] are already in place to detect and prevent malicious codes attacks on VoIP systems.

Spam over Internet Telephony [6, 8, 9], also called SPIT is another security threat against VoIP network which is the transmission of unwanted bunk of messages over Internet Telephony. Several techniques have been proposed in [10, 11] to resist and fight SPIT in VoIP systems such as filtering, caller's reputation and black/white lists.

Denial of service (DoS) and distributed denial of service (DDoS) [1, 5-7, 9, 11] attacks are also noticed in VoIP systems where an attacker denies legitimate users access to system resource by making it difficult to place or receive a call. These attacks may come in the form of preventing calls to sensitive phone numbers in an attempt to disrupt business or block effective communications to facilitate another event like delaying an emergency response to anti-social activities such as robbery attack. A number of VoIP network infrastructures' defensive mechanisms are proposed in [3, 6] such as fair bandwidth share and throttling techniques to classify packets following a combined criterion involving source hosts and packet sizes as a defensive measure to lessen disruptive traffic situations in VoIP systems.

Another latent DDoS threat specific to VoIP networks is pharming attacks which is an advancement of attack called phishing [12], where an attacker attempts to maliciously acquire sensitive information such as usernames, passwords, personal identification number (PIN) and credit card details by appearing to be a trustworthy partner via electronic communication. Pharming, in the other hand, entails taking advantage of Domain Name Server (DNS) vulnerabilities [3, 14] to manipulate the communication between a remote server and a client, thereby stealing sensitive information from the clients of a given organisation by the attackers deceiving the customers to believing that they are interacting with the organisation's representatives. According to [5, 9], there is another form of pharming attack against VoIP where large numbers of calls are misdirected to a specific domain in order to carry out distributed denial of service.

Flash crowd is another form of attack that can cause congestion in VoIP networks by making simultaneous massive number of requests to the same server. Several control measures have been proposed to mitigate flash crowd attacks by using its characteristics to design a vigorous load-balancing algorithm [3, 15] for web caches. Another flash crowd prevention approach based on requests regulation on web servers [13] is to always scrutinize high bandwidth applications where specific applications request rate is higher than pre-defined threshold because they are more related to flash crowd as opposed to low bandwidth requests.

The VoIP network architecture like other IP telephony/data network technologies that use the Internet as medium of signal transmission presents a myriad of vulnerabilities because of the loose security over the Internet transactions and this has attracted all these above mentioned attacks and even more from existing teeming internet fraudsters.

3. Security Issues common to VoIP Applications and PSTN Networks

The key factor that borders on the industries and deters many organisations from employing VoIP technologies for their voice communications needs is the overwhelming security issues which this paper tends to address in this section by dwelling richly on those new emerging security threats in VoIP applications and proffering feasible defensive mechanisms that will prevent most if not all of the security challenges associated with VoIP networks.

VoIP systems components have a lot of potential security holes or vulnerabilities thereby creating rooms for attackers to tap in and exploit the system. These vulnerabilities in VoIP systems are much in strong semblance to those found in the public-switched telephone network (PSTN) where eavesdropping can be achieved through physical attachment of a listening device on the telephone line [3]. The VoIP infrastructure's control and gateway servers [16] are built based on existing computing platforms such as Linux and Windows [2] which are constantly under attack; and these attacks would as well be applicable to VoIP networks thereby giving the attackers a wide range of possible vulnerable points (or an opening) for potential attacks.

Security challenges could be categorized based on their effects on the three fundamental security requirements such as confidentiality, integrity and availability [6] of VoIP networks where threats against confidentiality endangers the overall content of the interaction between two endpoints which can as well expose the call data such as telephone numbers dialled and call durations. Security threats against integrity tend to strongly affect the trust issues on the caller's identity, the recipient's identity, the messages transferred, or the call record logs [5]; while those against the availability of the network resources tend to deny legitimate users access to system resources thereby making it extremely difficult to make or receive a call. These three fundamental security requirements as tabulated in Table 1 review some of the VoIP networks security threats and their affected

components of the system.

Table 1. Security threats and their effects in VoIP systems.

Security threats	Confidentiality	Integrity	Availability
DoS			✓
Eaves-dropping	✓		
Caller ID Impersonation			
Toll Fraud		✓	
Alteration of Voice Stream	✓	✓	
Unwanted Calls and Messages		✓	✓
Redirection of Calls	✓	✓	✓

4. Prevalent Attacks (Threats) on VoIP Applications and Proposed Defensive Measures

In this section, emphasis is laid on several security threats that are specific to VoIP applications and feasible defensive approaches that may guarantee VoIP applications security assurance as italicized below under the following subsections.

4.1 *SIP Registration Hijacking*

The Session Initiation Protocol (SIP) is an application layer control protocol used in establishing, modifying or terminating VoIP applications over sessions. The SIP proxy/registrar enables registration of user agent/IP phone in SIP and other associated VoIP protocols thereby permitting the proxy to direct incoming calls to the user agent or IP phone. SIP registration hijacking takes place when an attacker replaces the legitimate registration of a valid user IP phone to an SIP control node/registrar with its own address, hence causing user IP phone's incoming calls to be forwarded to the attacker's IP phone, which results to a loss of calls for the intended legitimate user agent. With SIP registration hijacked, all outgoing calls can be blocked or manipulated if attackers hijack calls to a media gateway. In order to stop attackers from hijacking SIP registration, SIP registration of user agent to the SIP proxy/control node should be implemented using User Datagram Protocol (UDP) [18] and TCP as well as the application of Transport Layer Security (TLS) in establishing an authenticated secure connection as opposed to open connection approach of SIP registration process.

4.2 *SIP Message Modification*

An attacker can intercept and alter an SIP message by using any of the man-in-the-middle (or substitution) attacks such as IP spoofing, MAC spoofing or SIP registration hijacking [3]. SIP message modification by attackers can actually be prevented by using TLS to protect UDP and TCP transport mechanisms thereby protecting the confidentiality of the SIP message contents.

4.3 *SIP Redirect*

Session Initiation Protocol server application receives requests from a mobile station and returns a redirection response to specify where the request should be retried thereby creating room for attackers to attack the SIP redirect server by commanding it to redirect victim's calls to a number that will be provided by the attacker, hence enables the attacker to receive calls intended for the victim [8]. This weakness (or vulnerability) of SIP server application exist because of inadequate authentication in the SIP protocol which could be surmounted by using strong authentication system like transport layer security (TLS) with robust passwords to protect the SIP server application redirection from attackers.

4.4 *Real-time Transport Protocol (RTP) Payload*

RTP conveys (or transmits) the actual encoded voice signal (message) between the two callers. By using Man-in-the-middle attacks such as eavesdropping, the attackers can penetrate the RTP media stream between two nodes

with the intension of modifying the payload (or content) of the voice message [1]. When those attackers gain access to modify the payload of the voice message, they may introduce noise or even their own message into the packet. The application of secure Real-time Transport Protocol (SRTP) will prevent attackers from using Man-in-the-middle attacks such as eavesdropping and utter modification of the packets to avoid injection of noise or entirely new messages.

5. Security Threats Associated with IP Data Networks

This section identifies those security threats that are general to IP data networks, their modus operandi and proposed feasible defensive mechanisms to counter the ugly effects of those attacks as outlined under the following sub-headings.

5.1 Physical Attacks

VoIP network infrastructures such as trunk lines, headsets, VoIP servers, switches, and so on, could be modified physically by attackers in order to affect the availability and confidentiality of VoIP system resources; and this form of attack can be curtailed by the installation of physical access control or physical barriers to VoIP system servers, switches and cabling to control unauthorized access.

5.2 ARP Cache Poison

Attackers can combine their own MAC address with another IP address in the Address Resolution Protocol (ARP) cache of the victimized node by sending forged ARP packets while parading as either an SIP registrar or an endpoint in that particular VoIP system [19]. The use of a Dynamic ARP Inspection (DAI) to stop all the ARP packets on the switch in order to verify valid IP-to-MAC bindings [3] prior to updating the local ARP cache or before forwarding them to appropriate destination would prevent this type of attack.

5.3 MAC Spoofing

This is a situation where an attacker displaces an existing node in a VoIP network by duplicating its MAC address thereby allowing that attacker's malicious node to appear as an already configured and authorized node in that particular VoIP network. The defensive mechanism of using port authentication specified in IEEE 802.1 x standards [18] to verify authenticity of every new node with the port that connects it to the VoIP network will completely prevent MAC address spoofing by attackers.

5.4 Internet Protocol (IP) Spoofing

In IP spoofing [3], the attackers use the same approach as in MAC spoofing except that here the IP address is targeted as opposed to MAC address of the VoIP network nodes, and such security threat as this could be prevented by configuring routers to reject any inbound packets whose source addresses are not in the local address range (or domain) of that particular VoIP network.

6. Other Effective Defensive Measures against Security Threats in VoIP Networks

Some control measures against security challenges that are prevalent in VoIP and indeed other related IP data networks can actually prevent multiple attacks or threats when put in place. As seen in section 4 of this paper, the port authentication defensive mechanism could be used to protect nodes in VoIP networks from several threats. Other defense techniques that can be applied to VoIP networks in order to forestall activities of VoIP network fraudsters are discussed in the following sub-headings.

6.1 VoIP Media Encryption

Media encryption is one of the best VoIP network practices of establishing a secure tunnel transmission using the Real-time Transport Protocol (RTP) between two nodes that are entering or engaging in a voice conversation in a VoIP telephony system by applying secret key cryptographic algorithms because of low computational needs in

key exchange. Growing number of organizations using VoIP applications in their business transaction has shown serious concerns as it affects the protection of voice conversation contents from such an attack as eavesdropping which normally results in massive compromise of confidentiality of the transmitted payload.

The improved version of RTP, known as secure RTP (or SRTP) published by Internet Engineering Task Force (IETF) as RFC 3711, is used in providing authentication and confidentiality of the payload (voice conversations) that is transported by RTP protocol. SRTP uses Multimedia Internet Keying protocol (MIKEY) [21] to provide simple but dynamic protocol capable of generating and exchanging pre-shared session keys in an ad-hoc environment such as VoIP systems. The session keys are used to encrypt the messages sent via the SRTP protocol and containing voice data.

6.2 VoIP Signaling Authentication

Servers in a VoIP network use SIP to establish connection between two nodes (phones) thereby ensuring that the node's identity is ascertained as it registers with the VoIP SIP server using identifiers including MAC and IP addresses of the nodes [3]. Authentication and encryption mechanisms for voice signals in a VoIP network can as well be achieved by the use of IP security (or IPSec) protocol. Strong signal authentication between the VoIP phone and the call manger are established by using IPSec protocol. IPSec is made up of a number of related protocols such as the Authentication Header (AH) protocol [10] which it uses in establishing data origin authentication and connectionless integrity as well as the prevention of VoIP network voice conversation payload replays. When this IPSec AH protocol is used between the nodes and the servers, the voice signal authenticity and integrity of the call can be achieved through the identification of the caller, the phone number called, and the call manger. This control measure (signal authentication), in turn, prevents attackers from impersonating genuine callers as well as protects the inbound calls to a particular recipient from being received by a rogue node.

7. Conclusions

VoIP is a very rapid evolving communication technology which supports transportation of voice data via IP based networks. This technology, if properly secured using these stipulated defense measures, can provide voice communication needs to various sectors at a very minimal cost. This survey paper has critically investigated and analyzed most of the security challenges associated with VoIP systems and traditional IP data networks; and has also proposed several defense measures, which if designed and implemented, will prevent most of the security threats and challenges facing these networks.

In order to make VoIP systems the central and dominant technologies in IP telephony systems, future research work should be geared towards: i) The design and implementation of IPSec related protocols that will lessen or eradicate the difficulty in key sharing for encryption and decryption of voice conversation payload for large-scale deployments; ii) The design and implementation of robust Intrusion Detection System (IDS) that can withstand emerging polymorphic and encrypted malicious codes; and iii) Provision of reliable security policies and their implementation to foster software attacks prevention in VoIP telephony systems.

References

[1] B. Collier. (2010, Feb. 20). VoIP vulnerabilities: Denial of service. [Online]. Available at: http://www.voip-magazine.com/index.php?option, viewed 21 Nov. 2012.

[2] Butcher, D.; Xiangyang Li; Jinhua Guo; "Security Challenge and Defense in VoIP Infrastructures," *Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on communication*, vol.37, no.6, pp.1152-1162, Nov. 2007.

[3] C. Bilien, E. Eliasson, J. Orrblad, and J.O. Vatn, ―Secure VoIP: Call establishment and media protection,‖ presented at the 2nd Workshop Secur. Voice IP, Washington, DC, Jun. 2005.

[4] Cisco Systems. (2010, Feb. 20). How to secure Internet telephony media with SRTP and SDP [Online].Available at: http://www.cisco.com/en/us/ about/security/intelligence/voip.html. Viewed 21 Nov 2012.

[5] Edelson, ―Voice over IP: Security pitfalls, *Netw. Security*, no. 2, pp. 4–7, Feb. 2010.

[6] Garretson. (2011, Jul.). VoIP security threats: Fact or fiction? *Networking World.* [Online]. Available at: http://www.networkworld.com/voip-security.html. Viewed 20 Nov. 2012.

[7] H. Debar, M. Dacier, and A. Wespi, ―Towards a taxonomy of intrusion detection systems,‖ *Comput. Netw.*, vol. 31, pp. 805–822, 1999.

[8] J. Bartlomiejczyk and M. Phipps. (2007, Feb. 20). Preventing Layer 2 security threats [Online]. Available at: http://searchnetworking.techtar.com/, viewed 21 Nov 2012

[9] J. Kaavi, ―Group key distribution in ad-hoc networks using MIKEY,‖presented at the Helsinki Univ. Technol. Semin. Internetw., Apr. 2005.

[10] James. (2007, Feb. 20). Using IEEE 802.1x to enhance network security. [Online]. Available at: http://www.foundrynet.com/pdf/wp-ieee- 802.1x-enhance-network.pdf. viewed 22 Nov., 2012.

[11] N. Dadoun, ―Security framework for IP telephony, ANSI Accredited Eng. Committee TR41.4 Standards Commission, Rep. TR-41.4-02-02-12, Feb. 2002.

[12] P. Hunter, ―VoIP the latest security concern: DoS attack the greatest threat, *Networking Security*, no. 11, pp. 5–7, Nov. 2009.

[13] P. Mehta and S. Udani, ―Overview of voice over IP‖, Dept. Comput. Inf. Sci., Univ. Pennsylvania, Philadelphia, PA, Rep. MS-CIS-01-31, Feb. 2001.

[14] P. Rowe, ―VoIP—extra threats in the converged environment, *Networking Security*, no. 7, pp. 12–16, Jul. 2009.

[15] P. Thermos and G. Hadsall, ―Vulnerabilities in SOHO VoIP gateways, in *Proceeding 1st IEEE/CREATE-NET Workshop Security, QoS Communication, Networking (SecQoS 2009)*, Athens, Greece, Sep. 2009, pp. 236–245.

[16] S. Axelsson, *Intrusion Detection Systems: A survey and Taxonomy*, Dept. Comput. Eng., Chalmers Univ., Goteborg, Sweden, Rep. 99-15, 2000.

[17] S. McGann and D. Sicker, ―An analysis of security threats and tools in SIP-based VoIP systems, presented at the 5th Annual Workshop on VoIP Security Washington, DC, Jun. 2011.

[18] Sicker and T. Lookabaugh, ―VoIP security: Not an afterthought,‖ *ACM Queue*, vol. 2, no. 6, pp. 56–64, Sep. 2004.

[19] SIP: Session initiation protocol, The Internet Society RFC-3261. [Online]. Available at: http://rfc-ref.org/RFC-TEXTS/3261/index.html. Viewed 21 Nov. 2012.

[20] W. Stallings, *Cryptography and Network Security*. Upper Saddle River, NJ: Prentice-Hall, 2003.