Secure Communication and VoIP Threats in Next Generation Networks

M. Hossein Ahmadzadegan, M. Elmusrati, and H. Mohammadi

***Abstract*—VoIP services are among key issues in the Next Generation Network (NGN) for the telecommunication domain. This technology is comprised of positive and negative aspects like similar emerging technologies. Nowadays, telecom operators provide call waiting, conference calling, call transfer, caller ID and other VoIP services based on NGN and all IP solution. Thus, VoIP security is now one of the issues over which many debates take place. In this paper we have decided to concentrate on vulnerability categories for VoIP services in NGN. We try to present the common security threats and vulnerabilities of VoIP services. Determining the vulnerabilities and their classification, together with the risks that this system is threatened by clarifies the ways to penetrate this system and enables administrators to solve the problems.**

The debate on this matter would be misleading without having full recognition of various specifications. In addition, to make the importance of identifying these types of vulnerabilities clear, we will classify the probability threats for VoIP.

***Index Terms*—IMS, next generation networks, system security, VoIP**

I. Introduction

Nowadays, telecommunication networks have become an inseparable part of our life and play major roles in the exchange of information and news. This technology which dates back over 100 years, has taken advanced measures to adapt itself and cope with the new requirements of the new generations. The IP Multimedia Subsystem (IMS) provides real-time multimedia services based on an Internet Protocol (IP) which has been designed and developed by 3GPP (Third Generation Partnership Project).

The main goal of the IMS is to bring together cellular networks and the Internet. Convergence of these two principles enables providers to offer their customers access to Internet services almost wherever they go. The IMS is a distributed system which consists of several functions. Communication between these functions is based on an IP network which brings some advantages but also some disadvantages as security issues. The IMS has many advantages in comparison with other technologies. It is in accordance with an open standard, and has real-time and service-oriented architecture. It was designed considering its main target, which is providing services to customers. It combines these important technologies: mobility, quick Internet access, real-time multimedia services, easy management of the network, easy deployment of new services, access network independence (it supports fixed, cable and mobile access technologies including WCDMA, CDMA2000, GPRS, Wi-Fi, GSM, 3G), enabling Quality of Service in the IP environment, user and data security, charging capabilities, roaming support and the convergence of fixed and mobile networks into one unit.

A. The IMS Core

The core of the IMS is comprised of several functions interconnected by an IP network. In Fig. 1, you can find basic IMS architecture. It is commonly divided into three layers [1]:

- Transport layer - this layer is composed of the routers, switches and access elements which are situated at the edge of a provider's IMS network. The connectivity layer is the layer at which users are connected to the network via phones, PDAs, laptops and desktop computers.
- IMS layer - this layer comprises control servers. The control servers are the management authority for the call or data session set-up, modification and disconnect/release. The most important element in this layer is the Call Session Control Function (CSCF). The CSCF is the SIP server that is in charge of the call set-up between the end devices.

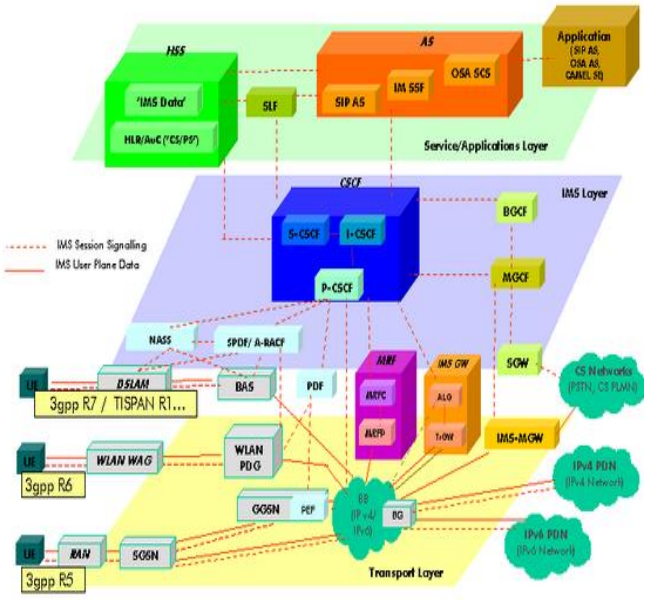

Fig. 1. 3GPP / TISPAN IMS architectural overview [2].

Manuscript received March 16, 2013; revised May 16, 2013.

M. Hossein Ahmadzadegan and M. Elmusrati are with the Department of Computer Science, Communication and Systems Engineering Group, University of Vaasa, Vaasa, Finland (e-mail: hossein_classicguy@yahoo.com).

H. Mohammadi is with Pishgaman Kavir Co.

- Service/applications layer - this layer includes application and media servers offering a multitude of enhanced service features for IMS-enabled networks. This layer indicates which services are offered by particular IMS network.

B. Functional Model Description

As our researches do not focus on all IMS functions, we will give a brief description just for those which we are interested in.

Home Subscriber Server (HSS) – is a central repository for user-related information. It contains all the user-related subscription data required to settle multimedia sessions; such as location and security information, user profile information and S-CSCF devoted to user.

The Proxy Call/Session Control Function (P-CSCF) – is a point of connection of the user's terminal into the IMS network. It acts as an inbound/outbound SIP proxy server from the SIP point of view. P-CSCF is assigned to the terminal during IMS registration and does not change for the duration of the registration. P-CSCF ensures several functions e.g. security functions, compression/ decompression of SIP messages, verifying correctness of SIP messages and other.

Interrogating CSCF (I-CSCF) is a SIP proxy server located at the edge of the administrative domain. It serves as the inter-domain node which is considered to be a next hop for a SIP message when it is routed from other IMS domain to our domain.

Serving CSCF (S-CSCF) is the central node of the signaling IMS plane. It is a SIP server which also performs session control and maintains binding user location with the user's SIP address of record – it acts as SIP registrar. All SIP messages traveling from/to IMS terminal are settled by SCSCF server so it can decide whether or not route it to some Application Server. Among its chief functions is offering SIP routing service. Moreover, network operator policies are applied – if a user tries to perform unauthorized activity it basically prevents it.

Application Server (AS) is a SIP entity which hosts and executes services.

A session border controller (SBC) is a device regularly deployed in Voice over Internet Protocol (VoIP) networks to exert control over the signaling and usually also the media streams involved in operations like setup, conduct and tearing down telephone calls or other media communications. SBC's core utilization was concentrated on the borders between two service provider networks in a peering environment. This role has been extended to entitle significant deployments between a service provider's network and a backbone network to offer service to residential and/or enterprise customers.

Voice over Internet Protocol (VoIP) as one application of NGN has become a popular alternative to traditional public-switched telephone network (PSTN) networks that provides advantages of low cost and flexible "digital" features. VoIP system flexibility and the convergence of voice and data networks brings with it additional security risks. These are added to the common security issues encountered by the underlying IP data network facilities that a VoIP system relies on. The result is that the VoIP network further complicates the security assurance mission faced by enterprises employing this technology.

VoIP damage that is threatened is imposed in two different ways. One of them is VoIP infrastructure systems, on which activities such as networks, operating systems, web servers are taking place. The other is VoIP protocols, equipment and devices that are used for VoIP such as phone, voice gateway, media server, signaling controller and …

In this paper VoIP vulnerabilities have been divided into two categories, source of vulnerability and vulnerable component, which are separately presented [3].

II. Source of Vulnerability

Here common cases are presented:

- **IP-Based Network Infrastructure:** As a result of the fact that VoIP is a built-in IP-Based network infrastructure, damage which threatens the protocols unconsciously is transmitted to the VoIP system. These include: Transmission control protocol attacks, exhaustive floods, malicious IP fragmentation, network viruses and many other harms.
- **Open or Public Networks:** In networks like the internet which are open and public networks there is a large bomber that poses serious threats.
- **Open Standard Protocol:** Most VoIP protocols such as SIP and H.323 are standardization which the public are able to access. Anyone can produce a client or server in this base even for rogue purposes. Therefore, these open protocols due to can be exploited by the attacker.
- **Exposed Interface:** In VoIP due to random IP and ports scan this possibility is provided for the attacker to produce fake and nonsense traffic.
- **Real-time communication:** Because the communication must be without interruption and be real-time any effect from the attacker can reduce the QoS and also lost packets due to no retransmission mechanism.
- **Mobility:** VoIP allows its users to have virtual access to different locations. This property makes internet phone mobility more complicated to protect against attackers.
- **Lack of security features and devices:** Although to prevent VoIP systems from the attacks, a firewall is utilized nowadays because of complex risks which are threatening these systems using these skills alone are not enough.
- **Voice and data integration:** Adding data to voice causes new harms and in the absence of enough device performance, the QoS is reduced [3], [4].

Vulnerable Component:

- Each component that is used by VoIP has specific vulnerabilities which affect it directly or indirectly. Some of the key requirements of VoIP with their vulnerabilities are mentioned.
- Operating system of the VoIP application: Because VoIP is run on operating systems like Windows, Linux, Unix and … their vulnerability is transmitted to VoIP. Provided security patch at each of these systems indicate vulnerability in them.
- Web client/server: VoIP application that provide web service, inherit vulnerabilities of web client/server such malicious traffic or worms.

- Access Devices (switch, router): If the attacker can switch into the router and access the system it would be able to damage the systems seriously. For example, an attacker can check all VoIP signals and media without having any effect on the working performance. As another instance, configuration errors in the 3rd layer of router can cause unnecessary broadcast and the attacker can achieve some information and through them will carry out the next attacks.
- Network: The network itself may be the vulnerable component because of vast and uncontrolled traffic, regardless of whether it is malicious or not.
- VoIP Protocol Stack: Security factors are not taken nito account while VoIP protocols (for example, SIP and H.323) are initialized. Therefore, these protocols recommend being combining with other security protocols (for example, Transport Layer Security [TLS], Secure/Multipurpose Internet Mail Extensions [S/MIME]) when implementing them [4].

After expressing vulnerabilities, we examine the classification of VoIP risks and threats.

III. The Classification of VoIP Threats

In this paper, we divided the VoIP threats to 4 categories:

1) Threats against availability
2) Threats against confidentiality
3) Threats against integrity
4) Threats against social context

Each of these categories includes some threat which we mention below.

A. Threats against Availability

Some groups of risks are created against services provided 24 hours a day and 7 days a week and causing system failure or interruption and disruption A famous example is the DoS (Denial of Service) attack. Among these risks we can point to the following example:

1) Call flooding

A well-known example from DoS is the simultaneous creation of call flooding where the attacker causes heavy traffic from valid or invalid calls (signal or media) and sends to a target system (such as VoIP server, client and underlying infrastructure), thereby significantly decreasing its efficiency or the system will break down [5]. Common methods are as follows:

- Valid or invalid registration flooding
- Valid or invalid request flooding
- Call control flooding after call setup
- Ping flooding

Not only noted intentional flooding but also unintentional flood can cause the failure of the system called a "self-attack". The following elements can be the cause of attack:

Regional power outage and restoration

- Incorrect configuration of device
- Misbehaving endpoints
- Legitimate call flooding

2) Malformed messages (protocol fizzing)

An attacker can create a malformed message and send it to a specific user with the intention of disrupting the work. This malformed message is similar to a protocol message but the text is written wrongly, and it causes confusion in related devices [6]. This threat takes place commonly due to the following reasons:

- Weakness of protocol specification
- Ease of creating the malformed message
- Lack of exception handling in the implementation
- Difficulty of testing all malformed cases

3) Spoofed messages

An attacker may insert a fake (spoofed) message to interrupt the services or steal the session. The typical examples are "call teardown" and " toll fraud".

a) Call teardown

In this method the attacker monitors an SIP dialog and obtains session information and the “From” and “To” tags, and sends a "SIP BYE" message to the communication device and unconsciously causing the call session to close [6].

4) Call hijacking

Call hijacking occur when some transaction between a VoIP endpoint and the network are taken over by an attacker. The typical cases are registration hijacking, server impersonation and media server hijacking [7].

In this case, the attacker identifies itself as a legitimate device, and steals all the contact and media sessions between two end points. The sender user thinks that, it is in conversation with the desired user, while the intended user has no access to message sender.

5) QoS abuse

In this method the attacker by using various tools, occupies a large bandwidth and the legitimate user is not able to use services or the quality of the service will face problems.

B. Threats against Confidentiality

Unlike the service interruption in the previous section, threats against confidentiality do not impact current communications generally but by stealing and recording media the attacker gets the information needed for the next threat. This introduces the most popular types of confidentiality threats.

1) Eavesdropping media

Eavesdropping media is carried out in two ways. One is sniffing media packets in the same broadcasting domain as a target user’s. The other is compromising an access device (for example, a layer2 switch) and forwarding and duplicating to an attacker device [7].

2) Call pattern trucking

In this method, the attacker proceeds in an unauthorized analysis of VoIP service and obtains the necessary information. For example, knowing that a company’s CEO and CFO have been calling the CEO and CFO of another company could indicate that an acquisition is under way.

3) Traffic capture

Traffic Capture is the unauthorized recording of traffic by any means and includes packet recording and logging packet snooping for unauthorized purposes. Traffic capture is a basic method for recording communication without the consent of all the parties.

4) Data mining

Collect information like user name, phone number, URL address, email address or any other identifiers that the attacker uses for the following reason: Toll fraud calls, spam calls, service interruptions, phishing.

5) Service abuse

Service abuse is a large category of improper use of services and includes:

a) Call conference abuse

Call Conference Abuse is an abuse of a VoIP call service as a means to hide identity for the purpose of committing fraud.

b) Premium rate service (PRS) fraud

Premium Rate Service Fraud is a method of artificially increasing traffic without consent or purpose other than to maximize billing.

c) Improper bypass or adjustment to billing

Improper Bypass or Adjustments to Billing are methods of avoiding authorized service charges or for concealing other fraud by altering billing records [8].

C. Threats against Integrity

After the attacker has intercepted the message as a network interface, it tries to change. The alteration can consist of deleting, injection or replacing certain information in the VoIP message or media.

This section is divided into two types:

- Threats against message integrity (message alteration)
- Threats against media integrity (media alteration)

The threat against message integrity (message alteration) happens by the following methods:

1) Call Rerouting

The attacker access, by an unauthorized to call routing information, changes the call direction and instead of reaching the desired user, the call is transferred elsewhere.

2) Call black holing

Any unauthorized method of deleting or refusing to pass any essential elements of protocol message. The consequence is to delay call setup, refuse subsequent messages, make errors on application, drop call connections and so on.

3) False caller identification

False Caller Identification is the signaling of an untrue identity or presence.

The threats against media integrity (media alteration) happen by the following method:

a) Media injection

In this method the attacker injects new media into an active media channel or replaces media in an active media channel. As a consequence the user (victim) may hear an advertisement, noise or silence in the middle of conversation.

b) Media degrading

The attacker manipulates media control packets and causes reduction of QoS of any communication.

D. Threats against Social Context

This threat is somewhat different from other threats. In this method the attacker misrepresent itself as a trust entity and convey false information to the target user (victim) in order to gain personal information and accomplish the next threat.

Typical threats against social context are as follows:

- Misrepresentation of identity, authority, rights, and content
- Spam of call (voice), IM, and presence
- Phishing

1) Misrepresentation of identity, authority, rights, and content

By the presentation of false identity, the user (victim) may be deceived and the attacker obtains access to password, key, certificate and so on.

2) Spam of call (voice), IM, and presence

A Massive amount of unsolicited requests to create an audio or video session, most utilized in internet marketing.[9] This section is divided into three types:

- Call Spam (SPIT)
- Spam over Instant Messaging or IM Spam (SPIM)
- Presence spam (SPPP)

IV. Conclusion

VoIP can be affected by many different kinds of threats in an Internet environment. The main cause is that most of the attacks cannot be followed and all networks are obvious for any type of spoofing and sniffing. Hence, in this paper, we have categorized VoIP vulnerabilities and possible threats. Vulnerabilities are divided into two categories, source of vulnerability and vulnerability components, and they have been analyzed separately.

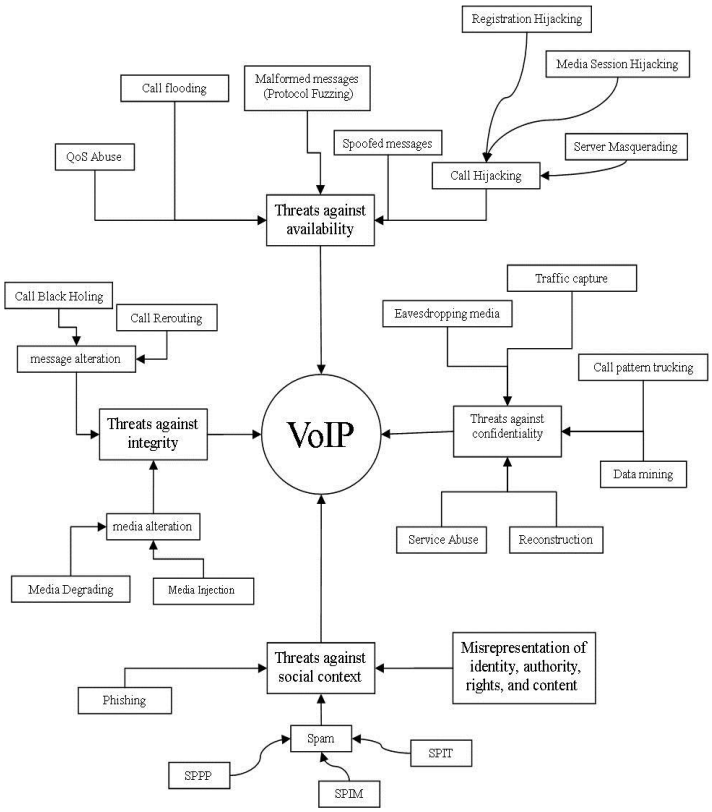

Fig. 2. VoIP Threats

REFERENCES

[1] T. Kovacik and I. Kotuliak, "TrafficCharacterization in IP Multimedia Subsystem," in *Proc. 16th International Conference on Systems, Signals and Image Processing*, 2009.

[2] IP Multimedia Subsystem and Architecture. [Online]. Available: http://en.wikipedia.org/wiki/IP_Multimedia_Subsystem.

[3] Keromytis, "Voice over IP: Risks, Threat and Vulnerabilities," in *Proc. Cyber Infrastructure Protection (CIP) conference*, June 2009.

[4] S. A. Ahson and M. Ilyase, *Security Issues of VoIP, VoIP Handbook*, CRC Press, Taylor & Francis Group, 2009.

[5] P. Park, *Voice over IP security*, cisco press, 2009.

[6] D. Sisalem, *SIP Security*, A John Wiley and Sons Ltd, 2009.

[7] J. F. Ransome, *CISM, CISSP, VoIP security*, Elsevier Digital Press, 2005.

[8] *VoIP Security Alliance, VoIP Security and Privacy Threat Taxonomy*, version 1.0.

[9] T. Koon. Phishing and Spamming via IM (SPIM). Internet Storm Center. [Online]. Available: http://isc.sans.org/diary.php?storyid=1905

M. Hossein Ahmadzadegan received his Diplom Ing. And Master from Politehnica University of Bucharest, Romania from Faculty of Engineering in Foreign languages with major field being Telecommunication in 2008 and 2010 respectively.
He previously held various positions in academia and industrial companies. He worked as network security researcher in Persian Telecommunication Research Center (ITRC). Currently he is with the Department of Computer Science, Communication and Systems Engineering Group, University of Vaasa, Vaasa, Finland working toward his PhD.

Mohammed Elmusrati received the B.Sc. (with honors) and M.Sc. (with high honors) degrees in telecommunication engineering from the Electrical and Electronic Engineering Department, Benghazi University, Libya, in 1991 and 1995, respectively, and the Licentiate of Science in technology (with distinction) and the Doctor of Science in Technology degrees in control Currently, Elmusrati is full professor and Head of communications and systems engineering group at University of Vaasa - Finland. Moreover, Elmusrati has Adjunct Professor Position at Automation and Systems Technology Department at Aalto University.

H. Mohammadi received the B.Sc. and M.Sc. degrees in Network engineering from Isfahan University of Technology and Azad University Tehran Central Branch, in 2006 and 2010, respectively.
He is currently a network expert in Pishgaman Kavir Co.