Journal of Theoretical and Applied Information Technology
10th May 2013. Vol. 51 No.1
© 2005 - 2013 JATIT & LLS. All rights reserved·
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

IP MULTIMEDIA SUBSYSTEM: SECURITY EVALUATION

[1]E.BELMEKKI, [2]N.BOUAOUDA, [1]B.RAOUYANE, [1]M.BELLAFKIH

[1] Networks Laboratory, Institut nationale de Poste et Télécommunication, RABAT, MOROCCO
[2]LR@II, Faculté des Sciences et Techniques, MOHAMMADIA, MOROCCO
E-mail: [1]mbelmekki@inpt.ac.ma

ABSTRACT

The IMS (IP Multimedia Subsystem) as network controller includes effective mechanisms for new services, regardless of the access technology. The network regroups all existing access IP-based technologies that unify access and minimize costs of service deployment. However, such architecture poses significant security challenges at network access and services providing. Indeed, the diversity of technologies used and entities included in the IMS control as well as user mobility and type of deployed services increase the risks and issues related to security. Thus, the paper proposes a state of the art of the IMS network security. Our focus is to highlight the most critical attacks at protocol level and access layer. The paper, then, illustrates in a test bed an effective way to secure a time sensitive application and evaluates the impact of the applied security measurements on the quality of service (QoS).

Keywords: *IP Multimedia System (IMS); Quality of services (QoS); Real-Time Protocol (RTP); Session Initiation Protocol (SIP).*

1 INTRODUCTION

Security issues in the IMS network is an important challenge as it includes a wide variety of services, protocols and components. This complexity enhances the number of vulnerabilities and risk for the IMS users and the ISP. Some of these vulnerabilities are inherent on one hand to protocols and services used and others are induced by the context of the IMS like users mobility. On the other hand, QoS is also a big challenge in any IMS network as this network is designed to offer time sensitive application like video, videoconferencing and so on. The main idea in this paper is to secure IMS services and evaluate the impact on QoS.

In this work we will first present the IMS network architecture and we propose a state of the art of the IMS network security. We will summarize the most critical attacks at the protocol level of the IMS architecture namely Session Initiation Protocol (SIP), RTP (Real-Time Protocol), Service Description Protocol (SDP), Domain Name System (DNS) and Dynamic Host Configuration Protocol (DHCP). At the access network level, we will focus on the analysis of the technologies used in wireless networks, which have several vulnerabilities. Second, we will analyze experimentally the operational of primordial protocols as SIP and RTP using security standards to highlight all associated loopholes.

The paper is organized as following. Section 2 outlines related work dealt with a security in IMS network. Then, the Sections 3 present IMS architecture and components. Section 4 describes the vulnerability and security in IMS with explications of each one. Section 5 then combines the results from work test and describes result and analyses. Finally, further steps are discussed in conclusions and future work.

2 RELATED WORKS

Chi-Yuan [1] proposed a key exchange protocol IMSKAAP, this work gives a procedure for opening IMS session to achieve end to end security. This mechanism, also, reduces spam impact over IP telephony (SPIT) using mutual authentication which meet requirement of lawful interception. The simulation result shows that proposed mechanism provides an efficient exchange session. EFORT [2] describes authentication procedure in IMS using private and public user identities. Kai Chuang and al [3] propose a multi-attribute stereo model based on X.805 standard, which focuses on a holistic, top-down, end-to-end perspective and analysis of IMS security, classification and evaluation. This standard, in addition, detail and analyze threats and vulnerabilities of IMS. The Model defined for this

© 2005 - 2013 JATIT & LLS. All rights reserved·
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

purpose is presented in [3], and it consists of three layers (security, and Security Security plan.).

The proposed solution of D.Slezak: [4] is based on definition of a security gateway for network interconnection between IMS and the Internet. The main function performed by the SEG is to ensure the confidentiality of data between client and IMS network.

The work of Frank S. Park [5] presents examples and systematic of security, as well the evaluation of IMS deployments using a modeling approach threats. It also offers suggestions for possible mitigation options if necessary.

3 IP MULTIMEDIA SUBSYSTEM ARCHITECTURE, COMPONENTS AND OPERATION

The IMS architecture is originally designed by 3GPP (3rd Generation Partnership Project) and later updated by 3GPP, 3GPP2 and TISPAN (Telecoms & Internet converged services and protocols for advanced networking) [6]. At the beginning, IMS has been designed for mobile networks. From the sixth version, the interaction with circuit-switched networks, IP networks and others with different access technologies has been achieved.

IMS is a network architecture that is actually using the principles of NGN SIP (Session Initiation Protocol) (Figure 1). IMS network has its own characteristics. It is not a separate network, but the sum of the functions that the system must support. The core of the IMS network is defined as a layered network. It consists of Access Layer, Control Layer and Service or Application Layer [7].

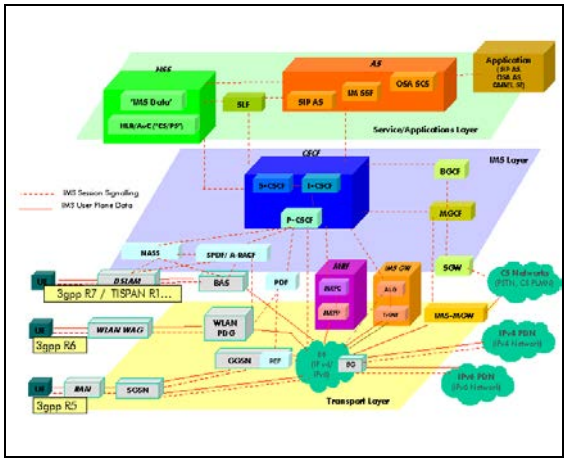

Figure 1. IP Multimedia Subsystem Architecture [9]

The Access layer is responsible for allows different user's devices IP-based to connect to the IMS network; the transport of information is also part of this layer. In the control layer, there are tree Call Session Control Functions (CSCF) and HSS (Home Subscriber Server) database. These two layers provide an integrated and standardized network platform to allow service providers to offer a variety of multimedia services in the service layer. The application servers provide an interface within control layer using SIP and Diameter protocol [8].

The IMS provides any type of service and inherits the problems related to the Internet such as QoS and security. The QoS management [10] can be solved using a PCRF (Policy and Charging Rule Function) and PCEF (Policy and Charging Enforcement Function), but the subject of security is very recent and must detail the IMS standard and all existing troubles and their solutions.

4 IP MULTIMEDIA SUBSYSTEM'S SECURITY AND VULNERABILITIES

4.1 Basic security services

Security service is a service provided by a communication protocol between open systems. It provides adequate security for communicating systems and data exchanged between the systems. These services can be classified into six categories [11]:

- *Authentication:* This service provides the authenticity of a communication. It ensures that two entities from same association are authentic, that certify the identity of each entity. Also, the service ensures that the received message has been originated from the source it claims to be from. It provides no protection against duplication or alteration of messages.
- *Access Control*: This is to limit and control access to systems or applications via communication interfaces. To do this, each entity must be authenticated in order to adapt access rights for each case.
- *Data confidentiality*: It is the protection of transmitted data against passive attacks. Several levels of protection are identified. The most general service protects all data transmitted between two entities. Restricted forms of this service can also be defined, including the protection of a whole message or even specific fields within a message. The other aspect of confidentiality is the protection against the flow of traffic analysis. This requires that an attacker can observe sources and destinations, frequency, length or other characteristics of the traffic [12].

© 2005 - 2013 JATIT & LLS. All rights reserved·
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

– *Data Integrity*: It is the protection of transmitted data against active attacks. This is to detect such attacks rather than prevent them. A connection-oriented integrity service ensures that messages sent are received rather than sent immediately without duplication, insertion, modification, reorganization, repetition and destruction. Service integrity undirected connection provides protection against data modification.

– *No-repudiation*: This prevents any end of a communication (sender or receiver) to deny having sent a message. Thus, when E sender sends a message to a receiver R, it can prove that the message was sent by the sender E. Similarly, when the receiver R receives a message, the sender of this message can prove that the message has been received by the receiver R.

– *Availability*: is the ability to access a system and can use its resources by an authorized entity. Loss or reduction of availability is a form of attack. Some of these attacks are against-automatic measurements, such as authentication and encryption, while others require human intervention to recover from the loss of availability.

The security services are implemented by mechanisms and security protocols. The most protocols used to secure exchanges will be presented in the next section.

4.2 Security protocol

The previous section presents security services; the following section will present some security protocols used to overcome attacks. When the exchange involves IP networks, security services can be offered using security protocols. Indeed, several protocols can mitigate the security vulnerabilities of communications. The best known are IPSec (IP Security Protocol), SSL (Secure Sockets Layer)/TLS (Transport Layer Security) and DTLS (Datagram TLS). These protocols are used to add security in different ways because they operate at different layers of the protocol stack. IPsec enables secure data transfer at the network layer, while SSL/TLS and DTLS operate at the transport layer to protect services based on TCP and UDP respectively [13].

– *Protocol IPSec:* IPSec (IP Security Protocol) is used to protect the traffic at the IP (IPv4 or IPv6). The security services offered by this protocol are integrity, origin authentication, data protection against replay and confidentiality. IPSec can be implemented in the user terminal or a security gateway (SG Security Gateway). Thus, it enables secure communication between two terminals, two security gateways or a terminal and a security gateway. To provide security, IPSec uses two protocols: AH (Authentication Header) and ESP (Encapsulating Security Payload). The AH protocol provides integrity and authentication of data origin, with optional protection against replay attacks. The ESP protocol provides the same set of services, and also offers privacy. Both protocols can be applied alone or combined to provide security services want. Each mechanism supports two modes: transport mode in which only protects the data transported and tunnel mode protects the IP header plus.

– *Protocol EAP/TLS:* EAP uses TLS to provide secure authentication. This method relies on digital and electronics certificates. Thus, each party (server and client) must have a certificate to prove its identity. The use of certificates has advantages and disadvantages. They are often considered more secure than passwords, however, certificate management and operations (creation, deletion, revocation lists etc...) can be tedious. This requires a public key infrastructure (PKI) to redistribute certificates to clients is also constraint that must not be overlooked [14].

4.3 IMS Vulnerability

The analysis of the IMS protocol shows several weaknesses; with some threats being exploited to damage the IMS. The threats are divided into seven families; each family breaks a security objective [15].

– *Network snoop:* Network snoop breaks confidentiality. Without the protection with SSL/TLS or IPsec, it will be easy for attacker to capture SIP signaling and RTP traffic. Tools like Wireshark [16] can be used to realize this attack. Another attack against confidentiality can be realized by using scan tools to gather sensitive and valuable information about IMS components, operating systems and network topology.

– *Session hijacking*: The session hijacking impact the integrity of session. The attacker can insert malicious packets to this session and can even substitute some traffic. Par example the attacker can send SIP Re-Invite bogus request to modify the session parameters.

© 2005 - 2013 JATIT & LLS. All rights reserved·
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

- *Denial of Service attack*: this is an attack against availability. The attacker launches a large number of datagram such as TCP connection to network system in a short period of time. This attack increase network traffic and system load causing a degradation of performance or completely stopping services. TCP SYN floods, UDP floods, Smurf attack floods are some examples of this common attacks on the Internet. As IMS is also IP-based network, this type of attacks can be also lunched against IMS components [17].
- *P-CSCF Discovery Attacks*: this attack concerns integrity and availability. The P-CSCF is the entry point for UE (User Equipment). The DHCP (Dynamic Host Control Protocol) and DNS (Domain Name System) are commonly used to discover P-CSCF. In this attack, an attacker can break the process of discovering P-CSCF through DNS by poisoning DNS cache so that fake IP or domain name will be returned to UE. The result is that the UE cannot be registered to IMS network or it will be with fake server [18].
- *Service Abuse Attacks*: This attack impact availability and integrity of IMS. Authorized users can use services more than what it is expected. IMS authorized users try to gain more privileged access to services that are not normally permitted for them.
- Toll Fraud: This attack is against accountability. When session between tow UE A and B is established by IMS core, media flow is directly exchanged between A and B. In the common scenario, when UE sends or receives the SIP Bye request, it will release media streams actively. But, an attacker can forge UE A and B in the way that when one UE sends Bye request to CSCF, and CSCF will think that the session is end, and stop accounting at this time the two UEs don't release the media streams. That mean that UE A and B can continue this session and media stream continue to be exchanged. This threat calls media theft, and use the weakness of lack of effective control of media streams.
- *Permission Acquisition Attacks*: The permission acquisition attacks concerns authentication. The attacker can obtain authorization by password cracking or other methods. Basically, UE use HTTP Digest authentication during access to IMS services. This method is based on username and password which is not high level security method. The specification of HTTP digest lists several potential attacks such as replay attack and brute force attack.

Mitigate IMS and SIP vulnerabilities require structured and proactive security approach. To summarize the main axes of safety considerations, I quote:

- The subscriber access to the IMS network with strong authentication.
- Network security: the flow exchanged between clients and application servers must be secured.
- Systems and applications must be secured.

In this work we will be interested in securing Video on Demand (VoD) as service proposed by IMS network. And because VoD is a sensitive time application, we will be interested in the impact of security implementation to QoS. The next section presents our approach, implementation and experimental results of this work.

5 IMPLEMENTATION AND TEST RESULTS

Our goal is to securing WiFi access and service in IMS network, for this we choose an application QoS sensitive as VoD (Video on Demand). We also focus on the impact of implementing security on QoS expressed by delay.

In our point of view, three security services are important in this context to secure VoD. Basically, confidentiality and integrity of flow exchanged between WiFi client and VoD server. The third service is authentication of the VoD client at IMS access layer. When implemented, this security measurement will impact QoS of service as we will develop in the next paragraphs.

5.1 Test bed description

To proof our approach and result we implement a test bed (Figure 2), it contain: IMS network, a VoD application server, an authentication server and Wi-Fi access network.

Our objective in this test bed is to secure client WiFi access to VoD server via IMS network. For that we have to perform two actions:

(1) The Wi-Fi Client/User authentication: we use a centralized authentication server RADIUS with EAP/TLS. The aim of this step is to grant access to VoD server to authenticated client only.

Journal of Theoretical and Applied Information Technology
10th May 2013. Vol. 51 No.1
© 2005 - 2013 JATIT & LLS. All rights reserved·
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

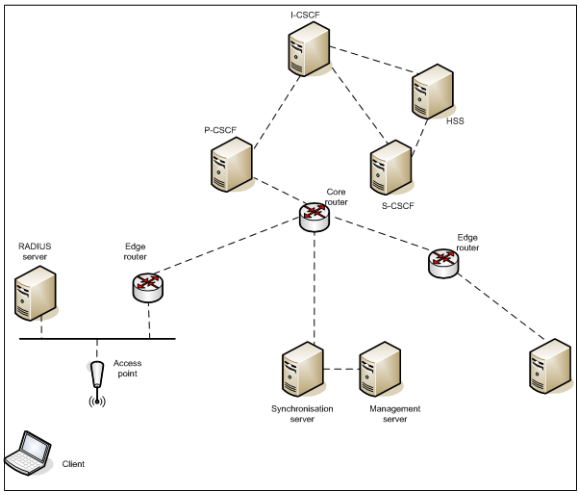

Figure 2. Test bed

(2) Secure Client\Server communication: basically SIP and RTP flows. Confidentiality, integrity and mutual authentication are the services we need to achieve our goal. We chose to use IPsec tunnel because it has the best advantage of securing all applications data and media transparently in IP layer. The test bed implements IPsec on tunnel mode with ESP as security protocol, AES-128 as algorithm for confidentiality, SHA-1 as algorithm for integrity, and pre-shared key for mutual authentication.

5.2 Results

Three critical parameters are used to evaluate QoS for time sensitive application: Jitter, Delay and response time. In the test bed, we compared the values of only delay before and after implementing the security measurements in both cases: signaling as registration and Service as RTP flow. We have proven with this test that the QoS is degraded by introducing authentication and IPSec versus flow number. The technical details of the implementation are not presented her to increase readability of the paper.

5.2.1 Security Impact in signaling:

In the first test, we focus in the impact of the authentication mechanism on the response time. We illustrate that when we introduce it, the response time become more important and it ingress with the number of user as illustrated in Figure 3. In the graph, the response time or registration delay is represented in tree case: None, IPsec and TLS.

The inspection of the results presented above shows that the delay of end-to-end gradually increases relative to the number of session.

The delay value varies from end to end security solution between IPsec and TLS (Figure 3). Although, the TLS solution is close to normal period-end delay is also slightly higher. This may be unnoticed by the user during registration. As expected, the highest delay is observed with security associations completed hop-by-hop IPSec solution.

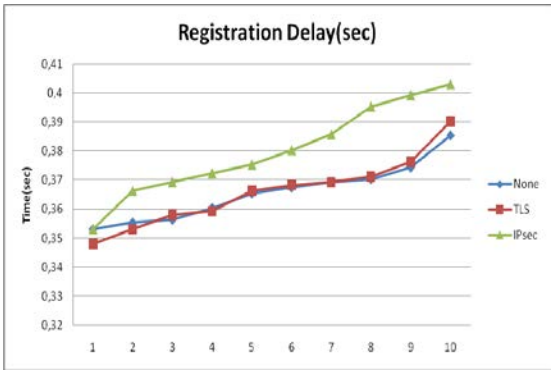

Figure 3. Registration Delay in IMS: None, TLS and IPsec

5.2.2 Security Impact in service

In the second test, we focus in the impact of using security between the client and the VoD application server. As illustrate in the graph, the values in the horizontal axis indication the number of session.

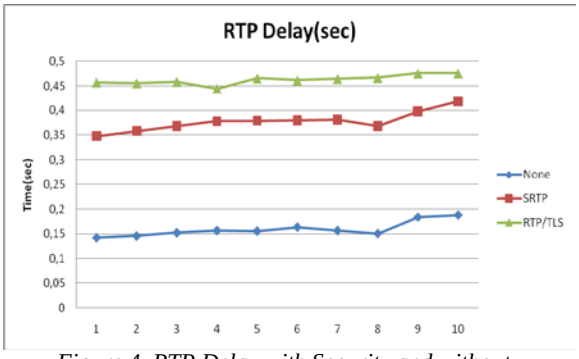

Figure 4. RTP Delay with Security and without

The security service implements SRTP and RTP over DTLS. For a VoD service, if the latency is too high, end users will begin to see problems like corrupted images, image blocking, and frozen frames on their terminals. For this, the processing time in each hop must not exceed a threshold.

Without security, the video can only compete with other flux, but the inclusion of SRTP and RTP/TLS increases the time especially with the latter (Figure 4). This

© 2005 - 2013 JATIT & LLS. All rights reserved·
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

supports SRTP due to its security mechanism from the RTP/TLS or without security.

5.2.3 Analysis of result

The different test realized in this test bed proof that securing sensitive time application impact negatively the critical QoS parameters. So the values recommended as threshold for these parameters in literature should not be used when implement security. We should take on consideration the supplementary time induced when securing this type of application.

For IPSec, the delay in both cases signaling and service is too big as well as Video, this will explained by the constitution of mechanism, the IPSec use large overhead that will surcharge the bandwidth, also there certainly a timing problem between source and destination. Moreover, to setup IPSec for End to end it's difficult (NAT/P-CSCF); but it still feasible for VoIP services.

The SRTP provide encryption, SRTP only encrypts the payload, making it a highly efficient protocol for transporting media packets, and some minor header changes for SRTCP. All SRTP keys derived from master key independent. Thereby, the network has no impact on the encrypted voice application, especially under varying QoS settings. But SRTP does not provide key management functionality; it instead depends on external key management to exchange secret master keys, and to negotiate the algorithms. So, the SRTP present a security failure in exchange with QoS.

The experiences made on the signaling and service plan with security protocols is necessary but not sufficient. Firstly, given the existence of several security mechanisms and the IMS network is not only a set of protocols but three distinct layers. Secondly, the study must takes into consideration the security patterns and prevention of attacks. Taking into account these two major points, we focus in the future the definition of a model for security services and signaling in IMS.

6 CONCLUSION

In this paper, we discuss a state of the art of IMS network security. The aim idea in the paper is who to secure sensitive service in IMS and evaluate the impact on QoS. As example, we chose wireless client users accessing to VoD service via IMS network. To proof the approach and illustrate the result, we implement a test bed, in which we use authentication by EAP/TLS and IPsec as security mechanism to ensure confidentiality and integrity of the access to VoD service. The test demonstrates that QoS is degraded when we implement security measurement particularly with IPsec in signaling. This degradation becomes more important when the number of simultaneous connected users increase.

It appears obviously to realize network security as IMS, but this network contains a number of features and protocols as well as several deferent type of access. This requires, as future work, the definition of an approach that will developed to a platform of security and attack prevention for IMS network. For that we choose ITU standards as X 805.

The ITU-T X 805[20] recommendations permit End-to-End security of distributed applications. The objective of this security model is to answer to the five threats telecommunications networks: Destruction of information, Corruption or modification of information, Removal, theft, or loss of information, Disclosure of information and Interruption of services

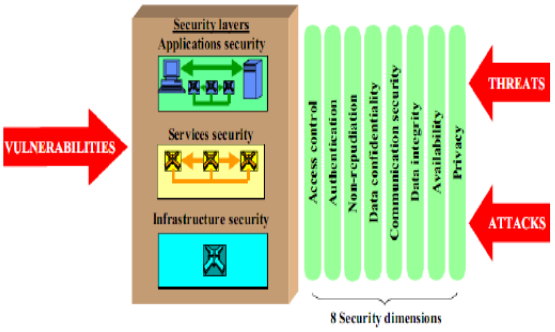

Figure 5. Illustrates plans, dimensions and layers of security architecture [14]

This model is defined on the basis of two main concepts, security layers and plans. Security layers relate to the rules that apply to the network elements and systems that constitute the End-to-End network. Security plans recovering security activities performed in a network.

The model adopts a hierarchical subdivision rules between the layers to ensure End-to-End security. The three layers are as follows:

– *Infrastructure layer:* comprises network transmission facilities and various elements. It includes routers, switches and servers as well as communication links.

– *Services layer:* it include services security which are offered to customers. These services offer basic connection such as leased line services to value-added services.

© 2005 - 2013 JATIT & LLS. All rights reserved·
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

– *Application layer:* concerns the requirements for network applications used by customers, these applications can be as simple as email or as complex as collaborative visualization.

The security model defines three security plans. They are designed to meet specific security needs associated to activities of network management, activities and signaling network control and activities related to end-user. The three layers are as follows:

– *Management plan:* Refers to operations, administration, maintenance and configuration.

– *Control plan:* This plan is associated with the signaling aspects for the establishment and modification of the End-to-End communication regardless the technology used in the network.

– *End user plan:* It relate to the protection of data stream end user and access security at user side.

The Recommendation defines eight sets that protect against all major threats. These measures are not limited to the network, but also include applications and end-user information. Security measures comprise: Access control, authentication, non-repudiation, the confidentiality of data, security communication flow, Data integrity, availability, privacy.

Our future work, will be concerned the projection of this module ITU on IMS network. This projection gives birth to a platform that not only allows secure access to IMS service but rather the prevention of attacks.

REFRENCES:

[1] C.Chen, Y.Huang," *An efficient end-to-end security mechanism for IP multimedia subsystem*" Computer Communications 31 (2008) 4259–4268

[2] IMS avance : enregistrement et authentification EFORT

[3] K Shuang, S Wang "*IMS Security Analysis using Multi-attribute Model*"JOURNAL OF NETWORKS, VOL. 6, NO. 2, FEBRUARY 2011

[4] D Slezak E.Yvette. " *Securing IP Multimedia Subsystem with the appropriate Security Gateway and IPSec Tunneling*" Security Engineering Research and Engineering, Volume 8, N 3 Juin 2011

[5] S.Frank. Park, Devdutt Patnaik, Chaitrali Amrutkar, Michael T. Hunter "*A Security Evaluation of IMS Deployments*" IMSAA '08, Dec 10-12th, 2008, Bangalore, India

[6] 3GPP TS 23.228 V8.5.0 (2008-06)-"*IP Multimedia Subsystem (IMS)*"; Stage 3 (Release 8).

[7] 3GPP TS 23.228 V9.4.0: "*IP Multimedia Subsystem (IMS); Stage 2*", (Release 9)

[8] C. Wieser, J. Roning and A. Takanen, *"Security analysis and experiments for Voice over IP RTP media streams*", Proceedings of the 8th International Symposium on System and Information Security (SSI'2006), Sao Jose dos Campos,Sao Paolo, Brazil, November 2006.

[9] 3GPP TS 33.203 V12.0.0 (2012-06)-"*access security for IP-based services*"; (Release 12)

[10] Dong Wang and Chen Liu, "*Model-based Vulnerability Analysis of IMS Network*", Journal of Networks, vol. 4, no 4, June 2009.

[11] C. K. Chan and H. Pant, "*Reliability and Security Modeling in Upgrading Wireless Backbone Networks*," Bell Labs Tech. J., 8:4 (2004), 39–53.

[12] 3GPP TS 33.203 V7.9.0 (2008-04)-"*Access security for IP based services* ";(Release 7).

[13] 3GPP TS 33.203 V7.9.0 (2008-04)-"*Access security for IP based services* ";(Release 7).

[14] ETSI TS 102 165-1 V4.2.1 "*Method and Performa for Threat, Risk, Vulnerability Analysis*". (2006-12).

[15] www.wireshark.org

[16] T. Dierks, C. Allen, "*The TLS Protocol Version 1.0*," RFC 2246, Juanary.1999.

[17] H. Schulzrinne et al., "*RTP: A Transport Protocol for Real-time Applications*," RFC 3550, July.2003

[18] M. Handley and V. Jacobson, "*SDP: Session Description Protocol*," RFC 2327, Apr. 1998

[19] 3GPP TS 24.229 V8.5.0 (2008-06)-*IP Multimedia Subsystem (IMS)*; Stage 3 (Release 8)

[20] ETSI TS 102 165-1 V4.2.3 "*Method and Performa for Threat, Risk, Vulnerability Analysis*". (2011-03).