VULNERABILITY ANALYSIS OF IP MULTIMEDIA SUBSYSTEM (IMS)

NAURIS PAULINS, PETERIS RIVZA

Department of Computer systems, Latvia University of Agriculture, Latvia
nauris.paulins@llu.lv, peteris.rivza@llu.lv

Abstract: *NGN introduces the concept of fix-mobile convergence (FMC). NGN provides the IP multimedia subsystem (IMS) as platform to converge the wire and wireless networks. It is open and distributed architecture that can enable easy access to services, information and resources. But the same time there is lot of risks in such approach. Potential hackers can access IMS architecture to lunch some attacks on IMS network. IMS security is vital important and it is beneficial to be aware of possible vulnerabilities. This paper investigates current situation in IMS security regulations, potential threats and attacks facing to IMS deployment. We also provide vulnerability discovering and analysis method with Open Source IMS Core.*

Keywords: IP Multimedia Subsystem, security, IMS vulnerabilities.

Introduction

The IP multimedia subsystem (IMS) is a standardized next-generation networking architecture that has been conceived for telecom operators willing to provide advanced services on top of both mobile and fixed networks (Ahson and Mohammad, 2009). The Next Generation Network (NGN) will be based on IP technology and IMS is a common architecture to provide multimedia services. The main idea behind this framework is to merge to most successful communications paradigms – cellular networks and the Internet. It was designed by the Generation Partnership Project (3GPP) as a part of the vision for evolving 3G mobile networks to delivering "Internet services" in 3GPP Release 5. Now it is accepted by 3GPP2, ETSI, ITU-T and developed as a unified service architecture that allow fixed-mobile convergence, and as the core of the NGN, already now some countries in Europe and Asia-Pacific areas, operators are going on the deployment of IMS.

Complete migration on all-IP architecture enable convergence of voice, video, data and mobile network technologies, it is great achievement to maintain single communication platform for all communications, from another side it is big challenge to provide adequate security for such heterogeneous network environment. Security in telecommunication networks never have been major problem, telephone systems is characterized by strict rules and strongly guarded end-nodes. It is hard to access another end point of the system if you are not recognized by another end. Telephone numbers are given only to carriers and all jurisdictions is carefully controlled. The same time IMS and Internet is characterized by widely open architecture, open end-points, based on freely available standard with lot of threats and vulnerabilities, which comes from Internet world. With this new network infrastructure, information can be reachable whenever and wherever, by who needs it. Hence, in the corporate world, the border between traditional company and office environments will diminish. Naturally these developments will inevitably come with many still unknown vulnerabilities, threats, and security risk (Atay and Masera, 2011).

Vulnerability assessment has become important are in security, but there is still a lack of vulnerability analysis in this area, many of existing assessment methods are limited possibilities and do not cover all areas when applied to IMS. The aim of this paper is to discuss current situation in IMS security and propose IMS vulnerability analysis method based on ETSI threat, vulnerability and risk analysis method (eTVRA) and ITU-T.805 Security Architecture., which analysis based on Open Source IMS Core.

Materials and methods

This paper makes IMS security evaluation derived from two approaches; (1) eTVRA and (2) ITU-T.805 Security architecture. This paper also makes research on vulnerability of IMS network, making tests with open-source IMS (OpenIMS Core). The idea for users of this Open Source software is to enable the development of IMS services and the trial of concepts around core IMS elements that are based upon highly configurable and extendable software (Anon, 2011). The Open IMS is experiment environment for developers and designers and includes new concepts, paradigms and new technologies that make it one of the best tools worldwide for IMS testing. This project is popular in academic and industry community.

The IP Multimedia Subsystem (IMS) is the key enabler for integration of multiple loosely coupled features in technical and service level. And IMS has open architecture, but its network core consists of lot of entities for cooperation between different user equipment's. Architecture of IMS provided in Figure 1 (Anon, 2011). IMS is decomposed in many functional entities and interfaces between them, where each interface is specified as reference point, which defines both the protocol over the interface and functions which it does. Main components in IMS are (Ahson and Mohammad, 2009):

- Proxy call state control function (P-CSCF) – is the first contact point within the IP multimedia core network; all SIP signaling traffic from or to the user equipment (UE) traverse via the P-CSCF. Its address is discovered by the UE following the packet data protocol (PDP) context activation. The P-CSCF behaves like a proxy, accepting and forwarding requests and responses. It performs functions like authorizing the bearer resources for the appropriate QoS level, emergency calls, monitoring, header (de)compression, and identification of I-CSCF.

- Interrogating call state control function (I-CSCF) – is the first contact point within an operator's network. It contacts the HSS to get the address of S-CSCF to serve the user for registration. It forwards SIP requests and responses to S-CSCF. It also performs network topology hiding functionality.
- Serving call state control function (S-CSCF) – performs the session control services for the end point and maintains session state as needed by the network operator for support of the services. Within an operator's network, different S-CSCFs may have different functionalities. The important functions performed by S-CSCF include user registration/interaction with service platforms for the support of services. The S-CSCF decides whether an AS is required to receive information related to an incoming SIP session request to ensure appropriate service handling. The decision at the S-CSCF is based on filter information received from the HSS. This filter information is stored and conveyed on a per-application-server basis for each user.
- Home subscriber server (HSS) – is the equivalent of the HLR (home location register) in 2G systems but extended with two DIAMETER-based reference points. It is the master database of an IMS that stores IMS user profiles, including individual filtering information, user status information, and application server profiles.
- Application server (AS) – provides service platforms in IMS environments. It does not address how multimedia/value-added applications are programmed; only well-defined signaling and administration inter- faces (IMS service control and Sh) and SIP and DIAMETER protocols are supported. This enables developers to use almost any programming paradigm within a SIP AS, such as legacy intelligent network servers (i.e., CAMEL support environments); open service access (OSA)/Parlay servers/gateways; or any proven VoIP SIP programming paradigm like SIP servlets, call programming language (CPL), and common gateway interface (CGI) scripts. The SIP AS is triggered by the S-CSCF, which redirects certain sessions to the SIP AS based on the downloaded filter criteria or by requesting filter information from the HSS in a user-based paradigm. The SIP AS comprises filter rules to decide which of the applications deployed on the server should be selected for handling the session. During execution of service logic, it is also possible for the SIP AS to communicate with the HSS to get additional information about a subscriber or to be notified about changes in the profile of the subscriber
- Media resource function (MRF) – can be split into media resource function controller (MRFC) and media resource function processor (MRFP). It provides media stream processing resources like media mixing, media announcements, media analysis, and media transcoding as well as speech. The other three components are border gateway control function (BGCF), media gate control function (MGCF), and media gate (MG), which perform the bearer interworking between RTP/IP and the bearers used in the legacy networks.

More detailed about IMS Core component can be found in (Ahson and Mohammad, 2009; Poikselka et al., 2006). In architectural design of IMS is used layered approach where transport and bearer services are separated from IMS signaling network and session management services. IMS is split in three main layers – Service or Application layer, Control or Signaling layer, and User or Transport layer. Application layer provides an infrastructure for services development and management. Control plane routes signaling and tells the transport plane what traffic to allow, also this layer takes care of billing information. User plane provides core with access from User Equipment (UE) over mobile, Wi-Fi and broadband networks. Security organization in IMS consists of several parts – Network Domain Security (NDS), Authentication and Authentication and Key Agreement (AKA). NDS provides security between different nodes within a domain. NDS is concerned with a network that is controlled by a single administrative authority. The security domain refers to the network that is managed by a single network operator or provides IP security between different domains. Authentication provide identity management, if user wants to access the IMS network, the user will be authenticated. AKA allows organizing access security for SIP-based services. Challenge response protocols are intended to make the identification tests without having shared the password between two entities. Important component of IMS security is IPsec which provides security services for: data integrity, data origin authentication, anti,-replay protection and some protection against traffic flow analysis. The access into the IMS network must have enabled security mechanisms and features such the user equipment associations is protected. It is obvious that important role in security is authenticate each entity in network. Rest of security model will be analyzed in next chapter together within vulnerability evaluation process.

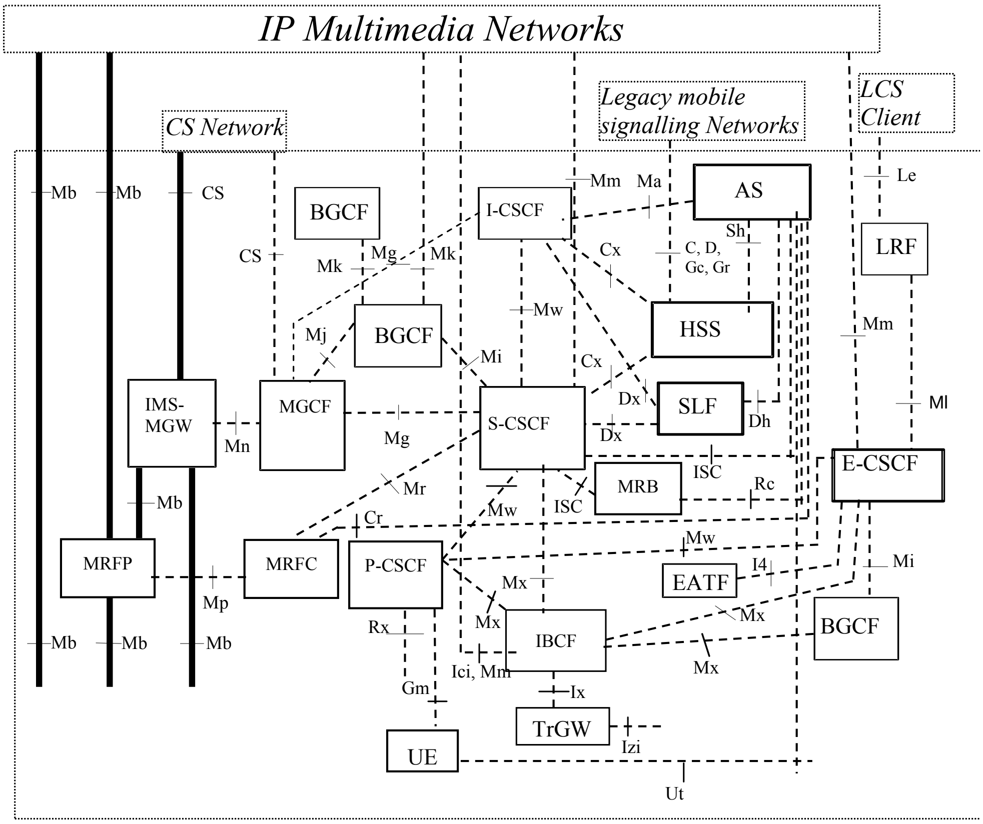


Fig. 1. **Architecture of IP multimedia core network**:

Bold lines - interfaces supporting user traffic; Dashed lines - interfaces supporting only signalling

Relationships in architectural structure can be found between IMS and ITU-T X.805 which is ITU-T recommendations for End-to-End communications. This X.800 series Recommendations identifies threats as destruction of information and resources, corruption or modification of information, data theft or removal, disclosure of information and interruption of services. They were proposed as the framework for NGN architecture for achieving end-to-end security in distributed applications (Atay and Masera, 2011). It is useful tool to comprehend a complex set of network architecture and services. The X.805 consist of 3 architectural parts – Security dimensions, Security layers and security planes, as shown in Figure 2 (Anon, 2011).

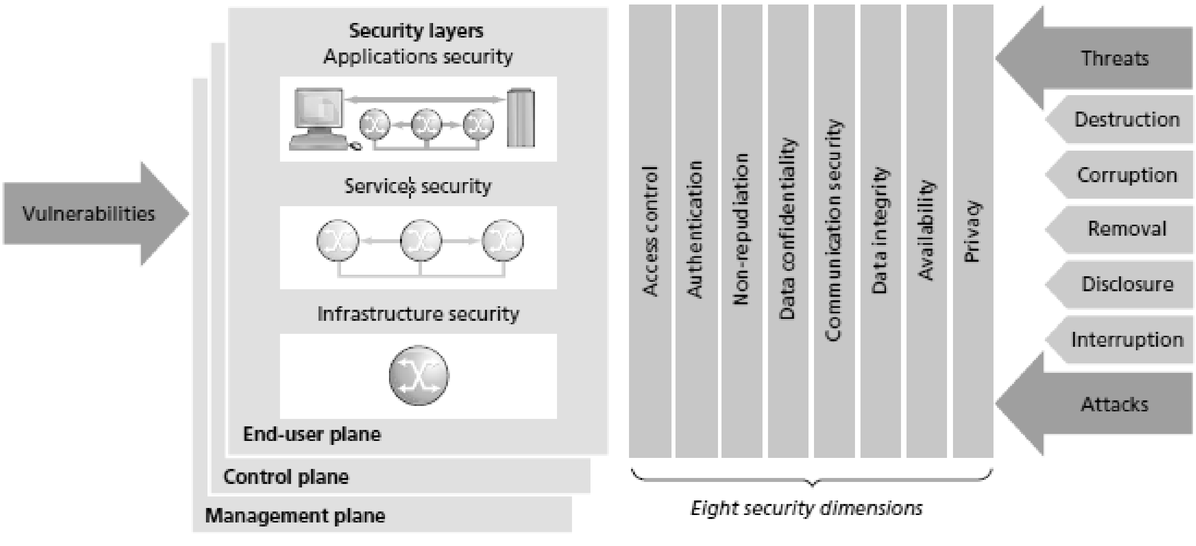


Fig. 2. **ITU-T X.805 Security Framework**.

Security layers also consist of 3 layers – infrastructure layer, service security layer, service security layer which all together are hierarchy of equipment and facilities grouping. But security planes show the activities that occur on a network – management security plane, Control security plane and End-User security plane. Security

Dimensions are security methods addressed to protection – Access control, Authentication, Nonrepudiation, Data confidentiality, Communication flow security, Data integrity, Availability and Privacy. Each layer is relates to unique vulnerabilities, threats and mitigation measures.

One of standards for security evaluation is ISO 15408:2009 Common Criteria for Information Technology Security Evaluation, but this standard is time and resource costly, and security guidelines are not accessible for non-security experts. For this reason, the Telecoms and Internet converged Services & Protocols for Advanced Networks (TISPAN) program at European Telecommunications Standards Institute (ETSI), a major European Telecommunication (Telco) standardization organization with worldwide influence, developed a threat, vulnerability, risk analysis (eTVRA) method to support Telco companies in a Common Criteria security evaluation. eTVRA builds on CORAS (Braber et al., 2003) and is structured to provide output that can be directly fed into a security evaluation thus easing the evaluation process (Morali et al. 2009). The vulnerability assessment in eTVRA consist of 7 steps witch shown in Figure 3 (Morali et al., 2009). The process starts with identification of the security objectives of a system or a system component, out of which security requirements are extracted. Later an inventory of the assets in the system is drafted. The purpose of using the eTVRA is to be able to identify vulnerabilities that exist in the system. Therefore, after identifying assets and their vulnerabilities, threats that exploit those vulnerabilities and cause incidents are determined. The security requirements and the threats are then extended ac- cording to threats and vulnerabilities. Then, the occurrence likelihood of the threats and their impact is analyzed and quantified. This is used in the following step to calculate the risk. Consequently, the countermeasures for treating the risk are identified. This process is applied iteratively, until the risk of unwanted incidents is reduced to an acceptable level, or whenever there are changes in the environment (Rosseb et al., 2006).

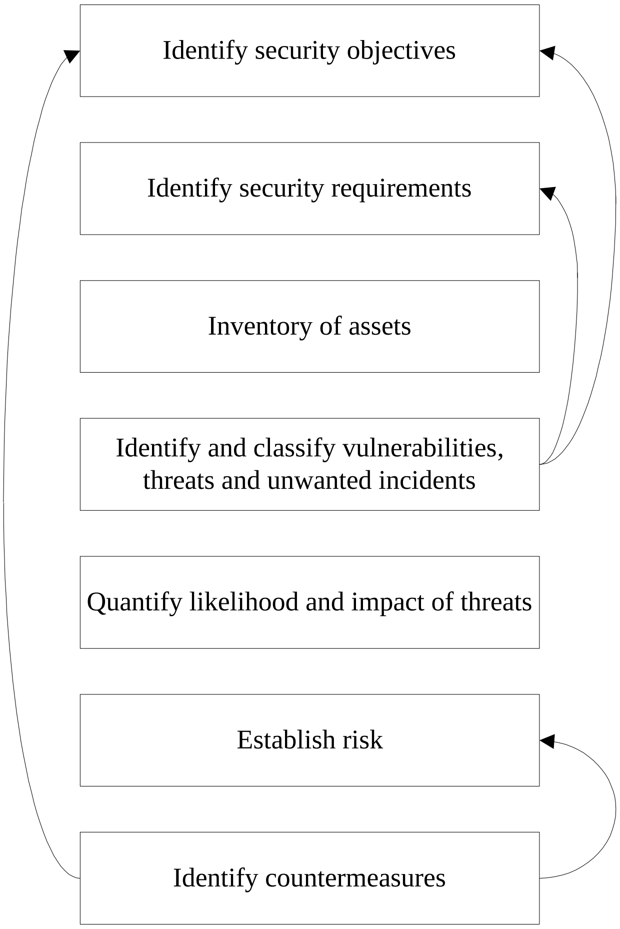
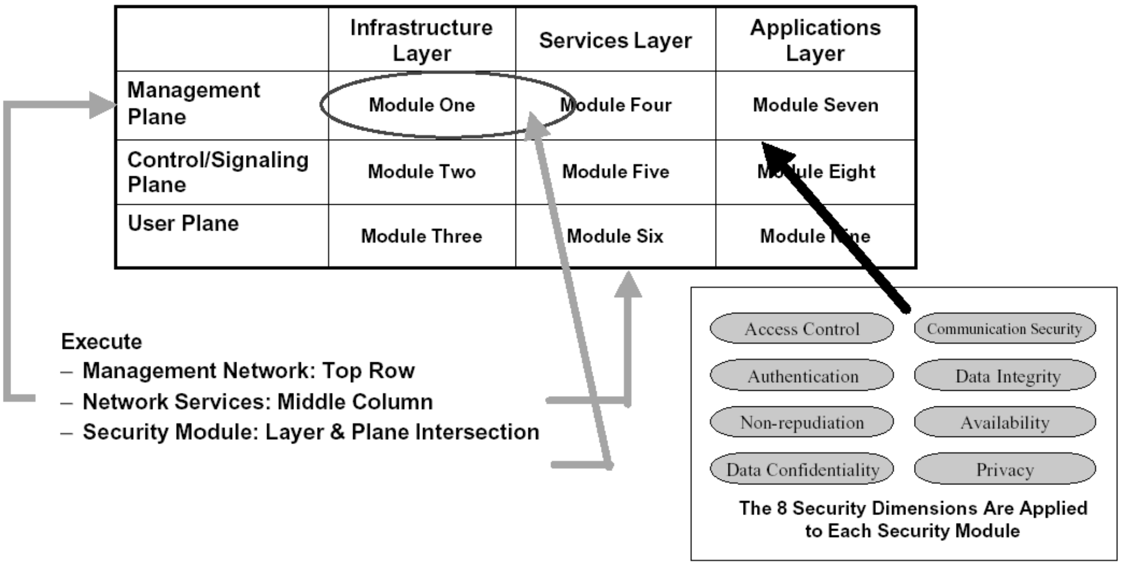

Identify security objectives
Identify security requirements
Inventory of assets
Identify and classify vulnerabilities, threats and unwanted incidents
Quantify likelihood and impact of threats
Establish risk
Identify countermeasures

Fig. 3. **Main steps of eTVRA.**

.This research propose use X.805 modular security perspectives which shown in Figure4 (Anon, 2011.) to IMS Core vulnerability analysis which is extended with eTVRA.



	Infrastructure Layer	Services Layer	Applications Layer
Management Plane	Module One	Module Four	Module Seven
Control/Signaling Plane	Module Two	Module Five	Module Eight
User Plane	Module Three	Module Six	Module Nine

Execute
– Management Network: Top Row
– Network Services: Middle Column
– Security Module: Layer & Plane Intersection

Fig. 4. **Modular security perspectives from X.805** (Anon, 2011.)

There are 9 security perspectives or modules where is necessary to identify software and hardware entities in each perspective, as third factor in vulnerability analysis must be included human factor, which mean, that should be evaluated all kind of activities as well. Such solution should provide not just vulnerabilities analysis, but also better security implementation and improvement, because such model allows update security when vulnerabilities are identified.

Results and discussion

Current IMS security standards do not cover all security solutions and risk management possibilities for IMS core network. All security layers have their risks and vulnerabilities. It is important identified IMS hardware and software components and their security solutions in particular infrastructure and functional role. 3GPP IMS and ETSI have draft series of security to protect IMS, but it is still vulnerable to several attacks. ITU-T X.805 is good solution to provide fully covered, comprehensive security. Proposed model consist of eight steps (Figure 5), which basically taken from eTVRA, but some of the steps are extended with ITU-T X.805 security dimensions, layers and planes. The extensions made in proposed model are discussed in following steps description:

- **Identify context/location** – it is critical important to identify location of entity in core network and it’s functional context with other entities. Aim of this step is discover location of entity or reference point and analyze it relationships with other entities in particular context.
- **Set module** – After identification of entity or reference point it should be analyzed in which module it is located and with which layer and plane it is related. That will help correctly identify security objectives.
- **Identify security objectives and requirements** - to protect IMS against vulnerabilities, it should meet all security objectives which mentioned as ITU-T X.805, but here can be exceptions which will come from context analysis.
- **Inventory of assets** – Identify hardware and software components. And categorization by security layers and planes.
- **Identify and classify vulnerabilities, threats and unwanted incidents** – combine assets with security dimensions, discovering threats, vulnerabilities and possible unwanted incidents.
- **Analyze vulnerabilities and unwanted incidents between modules** – each combination of several components can include new risks. So overall situation must be analyzed as well. During research was discovered, that eTVRA do not provide guidelines for this process.
- **Quantify likelihood and impact of threats** – in this step is established the risk of attack against any vulnerability
- **Identify countermeasures** – this is the place how to achieve goals and the provision of security dimensions.

Standards and protocols are changing all the time. IMS is quite new in networks and are in development study, it will be changed, patched and will evolve new features. That means that vulnerability analysis must be continuously updated and monitored with every change in system.

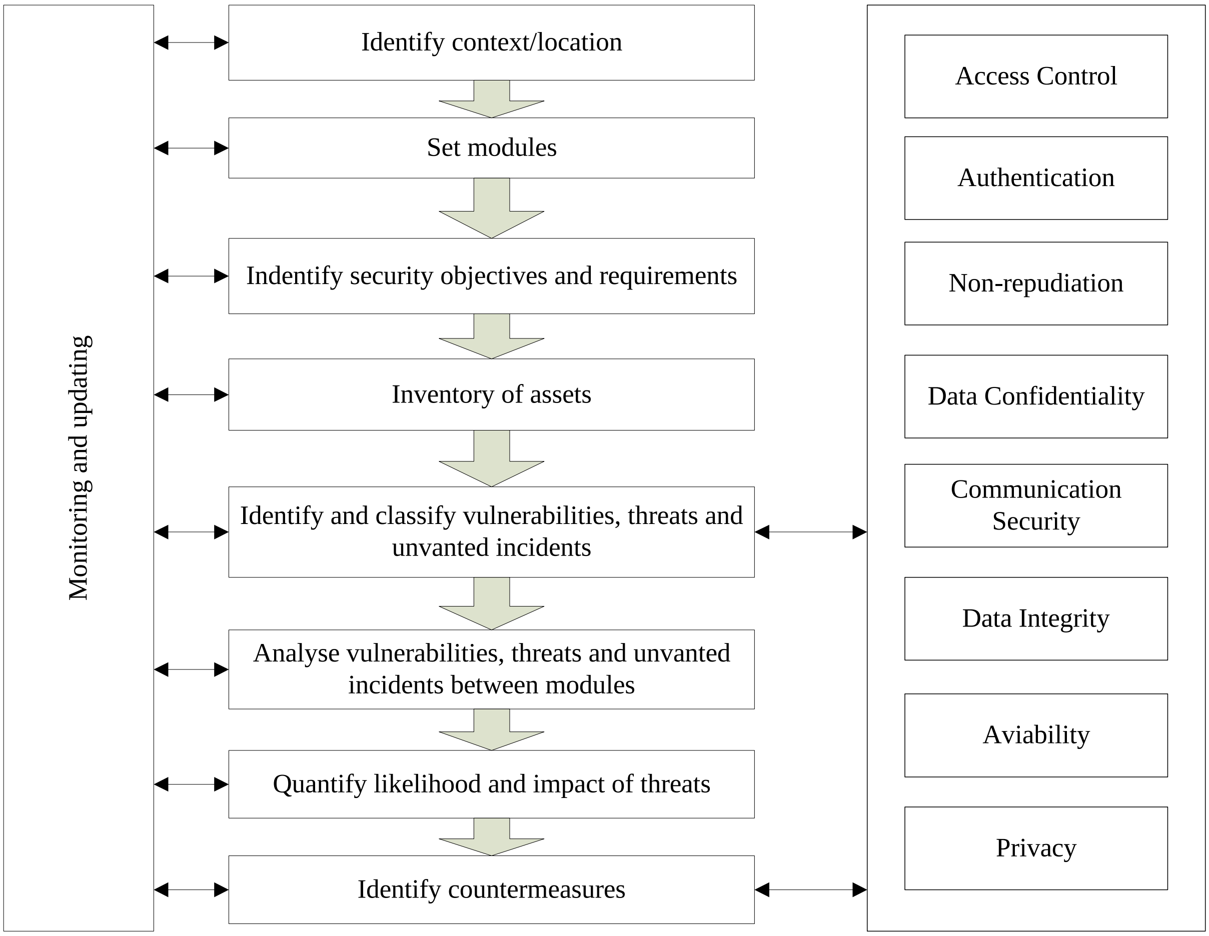

Monitoring and updating
Identify context/location
Set modules
Indentify security objectives and requirements
Inventory of assets
Identify and classify vulnerabilities, threats and unvanted incidents
Analyse vulnerabilities, threats and unvanted incidents between modules
Quantify likelihood and impact of threats
Identify countermeasures
Access Control
Authentication
Non-repudiation
Data Confidentiality
Communication Security
Data Integrity
Aviability
Privacy

Fig. 5. **Extended IMS vulnerability testing model**

Research process shown, that not all security dimensions can be addressed to each module, but anyway, it must be analyzed in context of infrastructure and assets. Any entity with some functional value in this architecture can be analyzed as asset, which must be grouped according it particular security layer and plane, what is shown in Table 1. IMS vulnerability analyses were done according asset categorization below.

Table 1

IMS assets by modules

	Infrastructure Layer	**Service Layer**	**Application Layer**
Management plane	CTF, CDF, CGF, PDF	Diameter (Rf, Rx, Ro) COPS (Go)	HTTP (Ut)
Control plane	CSCF, MGCF, MRFC, BGCF, IBCF, SLF, AS, DNS, ENUM	SIP/SDP(Gm, Mw, Mg, Mi, Mj,Mk, Mr), Diameter(Ch, Dx), H248 (Mp, Mn)	SIP(ISC), Diameter(Sh, Dh)
End-user plane	IM-MGW, MRFP, HSS, UE	RTP/RTCP(Mb), User profile	Voice, IM, VIDeo, State(XCAP)

Analysis of IMS vulnerabilities shown, that IMS may be exposed by different types of attacks. Vulnerability testing was done on OPEN IMS test-bed. This project source core is part of the Open IMS playground and is used to set up test-bed in order to simulate a practical scenario. Current research summarized different security vulnerabilities below in Table 2:

Table 2

IMS vulnerability list

Vulnerability	Weakness	Security dimension	Asset module	Impact
Message spoofing	IMS has absence of IPsec protection between user equipment and P-CSCF	Authentication	Service layer Control plane	Fraud of trust
SIP SQL injection	SIP authentication controllability is unsecure	Availability	Service layer User plane	Deniel of service
Media theft	Not enough control on media streems	Non-repudiation	Infrastructure layer Management plane	Theft of sercices
SIP flooding	Unable effectively prevent REGISTER and INVITE message flooding	Availability	Infrastructure layer Control plane	Loss of QoS for users
RTP data sniffing	No default confidentiality from data streem	Confidentiality	Application layer User plane	Theft of information
CANCEL attack	Possibility to fake SIP CANCEL request	Integrity	Service layer Control plane	Session disruption
RTP injection	RTP protocol missing media integrity protection mechanisms	Integrity	Service layer User plane	Session disruption
Man in the Middle P-CSCF attack	Authentication using SIP must be improved	Authentication	Service Layer Control plane	Impersonation of a server
Dictionary attack	Inadequate identity protection and AKA chipper algorithm use	Authentication	Application layer Control plane	Identity theft
BYE attack	Possibility to fake SIP BYE request/ not enough confidentiality protection	Integrity	Service layer Control plane	Disruption of session
DNS Cache Poisoning	Not enough connection integrity protection	Integrity	Infrastructure plane Control plane	Loss of service
Network topology disclosure	Not protected SIP messages	Confidentiality	Infrastructure layer Control plane	Leak of network topology
HTTP Parse Attack	Improperly data ContentLenght regulation	Availability	Infrastructure layer Control plane	Loss of services
User equipment configuration tampering	Probability lack of user education in security questions	Availability	Infrastructure layer Control plane	Denial of services

Evaluation of potential threats and vulnerabilities must be repeated obligatory, so it must be monitored and updated. Most of treats are discovered by current mechanisms, like IPSec and TLS or Authentication and authorized. But such attacks like SQL injections and data flooding can't be protected and requiring extra tool implementation most effective toll for such protection should be intrusion detection and prevention tool." That would help improve protection of human related threats.

Conclusion

This paper proposes implementation of eTVRA model in IMS vulnerability analysis which is extended with ITU-T X.805 security recommendations. This paper proposes method for fully covering vulnerabilities testing. Threats and vulnerabilities of IMS core was made on Open IMS test-bed at Focus Fraunhofer. One of major protocols which is facing with many vulnerabilities is SIP protocol. In this paper was shown major threats and future quantifying of vulnerabilities analysis should be made. Also as promising technology for such treat prevention could be implementation of intrusion detection and prevention system. Research show that much vulnerability related to Application layers and control plane, what means that this parts should have extra attention for protection.

Acknowledgements

This research has been supported by the European Social Fund within project "Support for the Implementation of Doctoral Studies at Latvia University of Agriculture", /2009/0180/1DP/1.1.2.1/09/IPIA/VIAA/017.

References

3GPP, 2011. 3GPP TS 23.002 V11.1.0 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Network architecture (Release 11)

Atay, S. & Masera, M., 2011. Challenges for the security analysis of Next Generation Networks. Information Security Technical Report, 16(1), pp.3-11. Available at: http://linkinghub.elsevier.com/retrieve/pii/S136341271000035X, 11.10.2011

Folker, B., Dimitrakos, T., Gran, A., Stolen, K., Aagedal, J., 2003. Model-based risk management using UML and UP, Section 3, pp.332-372.

Fraunhofer Fokus, OSIMS - The FOKUS Open Source IMS Core.Available at: http://www.fokus.fraunhofer.de/en/fokus_testbeds/open_ims_playground/components/osims/index.html, 11.01.2011

ITU-T, 2011, Recommendation X.805 Security Architecture for System providing End-to-End Communications.

Morali, A., Zambon, E., Houmb, S., Sallhammar, K., Etalle, S., 2009. Extended eTVRA vs. security checklist: Experiences in a value-web. 2009 31st International Conference on Software Engineering - Companion Volume, pp.130-140. Available at: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5070971. 19.12.2012.

Poikselka, M., Mayer, G., Khartabil, H., Niemi, A., 2006. IP Multimedia Concepts and Services Second., John Wiley & Sons Ltd, England, 439 p.

Rosseb, J.E.Y., Cadzow, S. & Sijben, P., 2006. eTVRA: a threat, vulnerability and risk assessment tool for eEurope. Proceeding iTrust'06 Proceedings of the 4th international conference on Trust Management.

Syed, A., S. Mohammad, I., 2009. IP Multimedia Subsystem (IMS) Handbook, Taylor & Francis Group, USA, 562 p.