Available online at www.sciencedirect.com

ScienceDirect

AASRI Procedia 4 (2013) 138 – 146

AASRI Procedia

www.elsevier.com/locate/procedia

2013 AASRI Conference on Intelligent Systems and Control

Towards a New Approach for Securing IMS Networks

E.Belmekki[a]*, B.Raouyane[b], M.Bellafkih[b], N.Bouaouda[a]

[a]*LR@II, Faculte des Sciences et Techniques, MOHAMMADIA, MOROCCO*
Networks Labotatory, Institut nationale de Poste et Telecommunication,RABAT, MOROCCO

Abstract

IMS presents an innovation in the world of telecommunications by providing a concrete Control Platform; the platform enables the delivery of multimedia services with high QoS range and with a soft convergence from circuit-switched services to the switching packet world. The IMS can unify access to multiple technologies and equipment-based IP. Indeed, the heterogeneity of access and technology imposes a challenge or repercussion in QoS, mobility and security. The article focuses on the importance of security, and it proposes a conceptual analysis on existing standards. Finally we propose an approach that meets the needs of a network such as IMS. The study focuses the main interfaces of IMS and security around and inside network with a sensitive context.

Keywords: IMS (IP Multimedia System); Security ; TVRA (Threat and Vulnerability Risk Assessments);RTP (Real-Time Protocol); SIP (Session Initiation Protocol).

1. Introduction

Security in IMS networks is an important issue [1], in addition to QoS [2], which will ensure the development of new services on its platforms. Security concerns the user, service provider over IMS and operator responsible for the core IMS. Several research works are concerned with this issue. In this sense, we

* Corresponding author. Tel.: 212538002783; fax: 212538002783.
E-mail address: mbelmekki@inpt.ac.ma.

doi:10.1016/j.aasri.2013.10.022

propose in this paper an analysis of the highlight work in this field, and an approach to cover the security issues in IMS networks. The approach is mainly directed towards the user and the service provider over IMS. An analysis of the security in this approach led to identify the critical interfaces that need more effort and concentration in order to strengthen security in IMS networks. The paper is organized into sections. Sections two and three respectively present the architecture and the risks related to IMS. The sections four and five present an analysis of existing work and our approach to secure the IMS network.

2. Architecture Of IP Multimedia Subsystem network

The IMS permit the convergence and the integration of data and multimedia services like voice over IP (VoIP), video, presence, instant messaging and so on. Multiple protocols are used with IMS but the main one is SIP protocol (Session Initiation Protocol). It provides method for configuring and controlling multimedia applications in IP network. The IMS architecture include four layers (Fig 1) [3], which work together to provide reliable service.

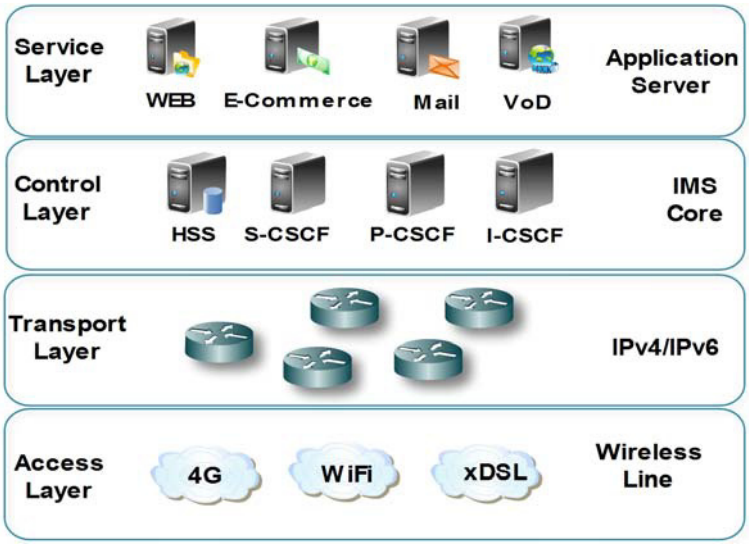

Fig. 1. IMS layered architecture.

- **The access layer**: The IMS user can access to IMS services through different access network like mobile network, wireless network, DSL line, enterprise network, etc. User can use basically different end IP based terminal to have access to IMS network, but can also use no IP based device.
- **The transport layer**: This layer offer an abstraction of different access network used which can be vendor technology dependent. It provides a unified network operation based on IP, unlike access network that can connect a no IP network users. It's responsible for assigning IP address and registration for users. The upper layers in the IMS architecture use transport layer transparently without thinking to detail behind network access.
- **The control layer**: It is responsible for authentication, accounting and billing, routing SIP messages to the appropriate services and forwarding traffic (mainly associated with SIP) between transport and service layers and other IMS providers. The main components in this layer are: The CSCF (Call/Session Control

Function), responsible for SIP interaction Home Subscriber Service (HSS), application servers and media servers. The CSCF is itself composed by tree components, each one assume different operation: P-CSCF (Proxy CSCF), I-CSCF (Interrogation CSCF) and S-CSCF (Serving CSCF). This layer includes also HSS which content subscriber data required for handling SIP session. The other component in this layer is PCRF (Policy Control and Charging Rules Function) responsible for charging and control [4].

- **The service layer**: These layers provide multimedia service over IMS network. In the 3GPP specifications, the components of this layer are referred as service platforms. The communication between S-CSCF and the service layer component are based on SIP.

3. Risks associated with IMS networks

As can be deduced from the previous section, IMS is based principally on IP protocol. Therefore, it inherits the security issues of IP networks. The IMS architecture is open, distributed and it has the advantage of being flexible in its implementation and deployment. This generates a variety of communication interfaces, which can make the system very vulnerable to attack. Add to that, the services offered on the IMS network must be provided by ensuring confidentiality and respect the privacy of users. Therefore, it is necessary to secure the IMS network at every level of its architecture including the final customer or subscriber device [5].

To understand the risks associated with IMS networks, we present in the following some risks associated with each layer of the IMS [6].

- *Risks in service and application layer:* The most of applications located at servers running with traditional OS (Operating System), indeed this may represent same vulnerability and threats. The attacks can damage all services in enterprise; the most examples known are denial of service (DoS), viruses and worms, etc.
- *Risks in control layer:* The IMS core uses two main protocols SIP and DIAMETER. The SIP is messages-based protocol like HTTP. This is why SIP is vulnerable to attacks types DoS (Denial of Service).The most critical attacks against IMS core can target CSCF components, this attacks impact control function and will capture or modify sensitive messages
- *Risks in transport layer:* As Packet Switching (PS), the layer contains a stream of data packets that consuming the entire bandwidth of a network. The flooding attacks can occur using any available network protocols, such as TCP flood or UDP flood. In Circuit Switching (CS), the attack is especially in a telecommunications network (GPRS, 3G, etc.) by using the protocol GTP (GPRS Tunneling Protocol) to divert logged in user's network session.
- *Risks in access layer:* The layer contains a set of IP-based devices. This diversity requires that the control layer differentiate between wire-line and wireless network. The IMS must ensure the authentication of all users during the process of registration; after that, the IMS must avoid other threats from the equipment as viruses, spyware and spam.

The following section presents the approaches leading to security management in IMS networks.

4. Comparison between models and methods for security

Withregard to the importance of network security in general, IMS networks are also affected by this aspect. Several organizations (3GPP, ITU, ETSI, etc.) and others Research work made suggestions and recommendations to secure this type of network. We present in this section the recommendations of the organizations 3GPP, ITU and ETSI.

4.1. 3GPP Recommendations

The 3GPP recommend different mechanisms to improve security in IMS network. The security architecture proposed by 3GPP describes five associations, between IMS components, and defines needed protection for each association [7]:

1) **The UE (User Equipment) and IMS Core association:** it need mutual authentication of UE and IMS core. The keys used for this are generated and managed by HSS (Home Subscriber Server). The authentication itself is done by the S-CSCF component [8].

2) **The UE and P-CSCF association:** The 3GPP recommend authenticating the data origin in the communication between an UE and the proxy P-CSCF.

3) **The CSCF and HSS association:** The communication between HSS and CSCF (named Cx interface) is also concerned by security in 3GPP architecture. The DIAMETER protocol is used in this interface to ensure a secure and reliable channel for exchanging keys during an UE registration process [5].

4) **The P-CSCF and other SIP core services association:** During the roaming operations of an UE to one visited network it recommends to use IPsec to secure the communication with IKE protocol to negotiate security association. This interface is known as Za interface.

5) **The P-CSCF and other core SIP association:** This concern security of communication between P-CSCF and other service when the UE is operating in the home network. These communications are exchanged via Zb interface.

The implementation of these recommendations in IMS networks is limited to some initial deployment, when all of the standard requirements can be satisfied. As example, in IMS network, the IPv6 deployment is very easy compared to IPv4 an also reliable; another problem may prevent the deployment of the recommendations is that current EU devices, mobile phones in particular, cannot have capabilities of IPSec [9].

4.2. ITU-X Recommendations

ITU recommendations are intended to any type of telecommunications network and are generic. This model defines two main security concepts: layers and plans. Securities layers relate to rules, these rules are applied to network elements and systems that constitute End-to-End network. Security plans recovering security activities performed in a network (Fig 2) [10].

This layered model adopts hierarchical subdivision rules between the layers to ensure E2E security. The three layers are:

- *Infrastructure layer*: includes network transmission facilities and the various elements in network. It includes routers, switches and servers as well as theirs communication links.
- *Service layer*: examines network security of each service that is offered to customers. These services provide basic connections such as private network or connection services to value-added services.
- *Application layer*: related to requirements for network applications used by customers. These applications can be as simple as email or as complex as collaborative visualization, etc.

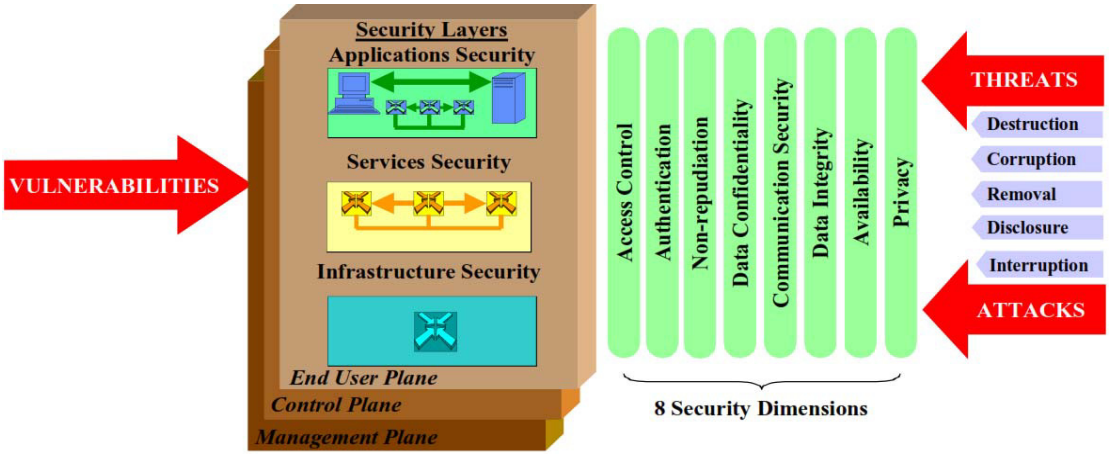

Fig. 2. : ITU X805 Model [10]

The model defines three security plans: management, control and End-user. They are designed to meet specific safety management activities associated with network operations and control signaling network and the corresponding end-user activities. Three types of activities are performed on network and are represented by three security planes:

- *Management Plane* is relates to all management operations like administration, maintenance and configuration
- *Control Plane* is associated with signalling aspects for establishment and modification of the communication from End-to-End in the network, regardless of carrier and technology used in the network.
- End User Plane related to security of access network used by customer. It also relates to the protection of data stream end user.

The model contain 8 Security Dimensions and it represent the classes of actions or technologies, a set of reactive actions which can be deployed to counter potential threats or attacks by each safety layer or plane:

- *Access Control:* Consists to protect against unauthorized use of network resources. This control ensures that only authorized people or devices can access to network core.
- *Authentication*: is to verify the identity presented by one entity, which may be human user, device, service and application, is correct and accurate
- *Non-Repudiation*: maintains that can help to proof the origin oh incident, act or data.
- *Data Confidentiality:* relating to the protection against unauthorized access to data content.
- *Communication Security*: ensures that information is flowing between allowed end points.
- *Data Integrity:* means that all data stored or in communication remains unchanged while stored or transmitted. Although, the authorization of change is possible if network administrator authorized.
- *Availability:* ensures that services and applications are deployed and functional as we expected.
- *Privacy:* protects information that might be sensible in network activities

In order to build more secure network including IMS network, it's recommended to use ITU-T X.805 security architecture framework during design, deployment, integration and maintenance phase of network life cycle [11].

4.3. TVRA (Threat and Vulnerability Risk Assessments) Model

Threat Vulnerability and Risk Analysis (TVRA) is used to identify risk to the system, TVRA is a method defined by ETSI TISPAN to analyze the threats, risks and vulnerabilities of a system of telecommunications TVRA. The method is derived from the model shown in [12].

The TVRA method considers a system as a set of properties that can be physical or logical. Property in the model may have weaknesses that can be exploited by threats. The realization of a threat can lead to a security incident that violates the security objectives. The vulnerability, according to the definition given in ISO, is modelled as a combination of weakness that can be exploited by one or more threats. The method recommends against-measures to protect the system against threats, vulnerabilities and reduce risks [13].

5. The Proposed approach for IMS security

5.1. The Proposed Approach for IMS security

We present in this section our approach to address security in the IMS network. To approach this problem, which is likely very complicated and varied, we propose to model the network architecture of IMS as illustrated in Fig 3.

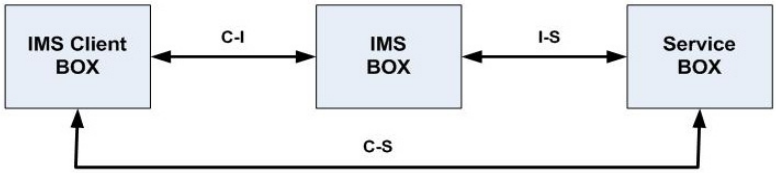

Fig. 3. The Proposed model for IMS security architecture

This model includes the following components:

- **IMS client**: it represents any user who connects to the IMS network in order to access a particular service offered by the network. A client accesses the IMS network via an access network which may be a telecommunication network or an IP network. In the case of the telecommunication network, the user has a SIM card [14] that includes information used for authentication. In the case of IP network, wired or wireless, the user does not have a SIM card.
- **IMS-BOX** is the core of the IMS network with its various internal components. We ignore the details of the communications and the various operations taking place in the core of the IMS network.
- **Service-BOX**: represents the services in the IMS network for end customers. Basically, one IMS user connects in order to use service offered by Service-BOX.

These components communicate with each other via three interfaces:

- *C-I Interface*: between the IMS client and the IMS-BOX. It carries all the signaling and control traffic associated with client access to the IMS network. It is basically based on the SIP protocol.
- *I-S interface*: used between service platforms represented in the diagram by "Service-BOX" and the IMS core represented as “IMS-BOX”. The traffic exchanged in this interface concern the verification of authenticity of the service platform. It also includes the authorization to offer service on IMS network. It is also based on SIP protocol.

• *C-S interface*: the interface is used to exchange media content between the client and the service platforms. This traffic can be a VoIP, video conferencing, video streaming or other. Protocols used on this interface depend on the service; it can be a HTTP, RTP and other.

5.2. Rationale of our approach

Representation of the IMS network used in this approach has several advantages and also disadvantages. The advantages of the representation are simplicity and efficiency. It allows focusing on the essential for security. Indeed points of interest on which we focus in our analysis of the security of the IMS network interfaces are the three interfaces C-I, I-S and C-S. These interfaces are the most vulnerable and exposed to several attacks. It represents a significant risk in terms of the likelihood of being attacked. For user and provider of service on IMS network, the most important in security is that the access will be secure. From the IMS provider perspective, the important is that the service must be available each time user need it. And the user who access to this service must be authenticated and has authorization to use service. From user perspective, the important is that it can access to needed service each time he want. The user need also to have guaranteed that the provider is authentic and authorized. For both, user and service provider, when confidentiality and integrity are need, the communication between them must guarantee this two security service.

As a drawback, we can say that the detail of what is happening in the IMS core is not taken into account. The impact of this decision on the analysis of security in this model is not very important compared to the advantages. We advance hypothesis that the IMS core network is a closed network in the security perimeter of one provider. The access to IMS internal components is not easy because they are often located in a single server or group of servers not accessible from the outside of the IMS core. The three IMS interfaces presented in Fig 5 are the most exposed in reality to external attacks.

5.3. Basic analysis of IMS network security with our approach

We identify, in our analysis of IMS network security, three critical interfaces namely I-C, I-S, and C-S. The traffic exchanged via these interfaces uses public network infrastructures which are unsafe and insecure. It makes these interfaces most vulnerable and exposed the attacks compared to interface within IMS core network. Indeed, the IMS IP-based client is connected to home network, enterprise network or Wi-Fi public hotspot network in open areas. These networks are also interconnected to the Internet service provider to have access to Internet. So when such IP-based client join IMS network, all the traffic generated by this access is forwarded over an IP network. The risk of attack in this context is more important than inside the IMS core. Similarly, the interface C-S established over IP public network, forward media traffic between the IP-based client and the service platforms represented in the diagram by "service-BOX".

In this approach, we give less importance to interfaces and other components inside the IMS core network. This choice is dictated by two reasons: the first is that the internal components of IMS core cannot be joined from the outside of the IMS network. They are internal to a private network protected by filtering mechanisms and access control. The probability of attacks against these components remains low compared to the risks on the three external interfaces we focus on in this article. The second reason is that by giving more importance to the most vulnerable interfaces we enhance the security overall the network.

The analysis of the security of these three interfaces uses the main security services: integrity, confidentiality and availability. We conclude that improving IMS security need necessary to strengthen these three services in the interfaces C-I, I-S and C-S. The following table summarizes the security service required on each interface according to our analysis.

The availability concerns the three interfaces. All security mechanisms involved in this service must allow exchanging traffic via these interfaces with a good quality of service.

The confidentiality concerns all interfaces. It must ensure that the content offered in the service platforms should be accessible by only permitted client. It also implies that when the client access to service, the media traffic must be confidential if the two end of communication decide to have this service active.

Table 1. Security service by interface.

Security service	C-I	I-S	C-S
Availability	Yes	Yes	Yes
Integrity	Yes	Yes	Yes
Confidentiality	Yes	Yes	Yes
Authentication	Yes	Yes	Yes

The integrity concerns any traffic exchanged via these interfaces. The mechanisms for integrity must guarantee to the end user that service platforms is authentic and provide authentic contents. In the other side, these mechanisms must guarantee for service provider that client is an authorized one and has the required permission. To ensure the integrity and confidentiality it is necessary to use another service security is authentication.

6. Conclusion

The article presents a synthesis of models and pioneering work related to security in IMS networks. It also presents a new simple, but effective, approach to address the security of IMS network. This approach identifies the critical and the most vulnerable interfaces on IMS network. The approach gives more importance to the relationship between a user and a service provider over IMS. The future of this work is to provide adequate security mechanism for each critical interface identified in this approach.

References

[1] 3GPP TS 23.228 V8.5.0 (2008-06)-IP Multimedia Subsystem (IMS); Stage 3 (Release 8).
[2] B.RAOUYANE, M.BELLAFKIH, D.RANC, “QoS management in IMS: DiffServ model”. NGMAST 2009 : 3rd International Conference and Exhibition on Next Generation Mobile Applications, Services and Technologies, IEEE Computer Society, 15-18 september 2009, Cardiff, Wales, United Kingdom, 2009, pp. 39-43, ISBN 978-0-7695-3786-3
[3] K Shuang, S Wang “IMS Security Analysis using Multi-attribute Model”JOURNAL OF NETWORKS, VOL. 6, NO. 2, FEBRUARY 2011
[4] B.RAOUYANE, M.BELLAFKIH, M.ERRAIS, M.RAMDANI, “IMS management and monitoring with eTOM framework and composite web service”, International Journal of Next-Generation Computing (IJNGC) - ISSN 2229-4678, eISSN 0976-5034Vol. 2, No. 2, 2011.
[5] 3GPP TR 33.978: Security aspects of early IP Multimedia Subsystem (IMS) (Release 7). June 2007.
[6] Dong Wang and Chen Liu, "Model-based Vulnerability Analysis of IMS Network", Journal of Networks, vol. 4, no.4, June 2009.ETSI TS 102 165-1 V4.2.3 (2011-03)
[7] 3GPP TS 29.328: IP Multimedia (IM) Subsystem Sh interface; Signaling flows and message contents (Release 5). March 2005.
[8] 3GPP TS 33.203: Access security for IP-based services (Release 8). March 2008.
[9] ETSI TS 102 165-1 V4.2.1 “Method and Performa for Threat, Risk, Vulnerability Analysis”. (2006-12).

[10] 3GPP TS 33.210: Network Domain Security; IP network layer security (Release 5). March 2002.
[11] International Telecommunication Union, Telecommunication Standardization Sector, "Security Architecture for Systems Providing End-to-End Communications," ITU-T Rec.X.805, Oct. 2003
[12] ETSI “Method and proforma for Threat, Risk, Vulnerability Analysis”TS 102 165-1 V4.2.3 (2011-03)
[13] C.Chen, Y.Huang,” An efficient end-to-end security mechanism for IP multimedia subsystem” Computer Communications 31 (2008) 4259–4268
[14] IMS avance : enregistrement et authentification EFORT
http://www.efort.com/r_tutoriels/AUTHENTIFICATION_IMS_EFORT.pdf