Security Enhancement Architectural Model for IMS based Networks

Ilyas Ed-daoui, Tomader Mazri and Nabil Hmina

1Systems Engineering Laboratory, ENSA Kenitra, Ibn Tofail University, Morocco; ilyas.ed-daoui@uit.ac.ma, hmina@univ-ibntofail.ac.ma
2Electrical and Telecommunication Systems Engineering Laboratory, ENSA Kenitra, Ibn Tofail University, Morocco; tomader20@gmail.com

Abstract

Objectives: The IP Multimedia Subsystem (IMS) is an architectural framework for delivering protocol-based services that enables an easy deployment of new rich multimedia services mixing voice and data. In fact, the IMS is vulnerable to several malicious uses that can be conducted by its users. We propose in this paper, a security enhancement architectural model to monitor the system and build a rapid and normal functioning retrieval after failing. Methods/Statistical Analysis: The weakness of the IMS network topology structure makes it a target for both normal cellular threats and IP-related threats. We propose a model that consists of dividing a complex set of end-of-end (IMS-based) network security related features into separate architectural components, layers and tiers in order to divide the system and to be more precise in the problems’ detection phase. Findings: Using the proposed approach, an effective evaluation study is investigated. The simulated network adopting our model showed an excellent behavior. The quality metric measuring call quality showed some excellent results. In other words, the adoption of the proposed model does not affect the normal frame delays, packet arrival durations and packet loss rates. The results showed how our proposed model is lightweight and effective in handling security issues. Application/Improvements: This paper fulfills a huge need of handling security using an effective lightweight architectural model adopting the proposed approach. Our methodology ensures designing a secure, flexible and easily monitored network with a rapid location of the affected areas and effective security supervision.

Keywords: Cellular Networks, IP Multimedia Subsystem (IMS), Network Security, Network Simulation, Threats

1. Introduction

We all agree that the cellular network has known a tremendous change during the last few years. We recently started talking about Next-Generation Networks (NGN) which packet-based networks are providing new practical features. However, even if the benefits of this migration are enormous, it is also true that such a fundamental change is full of challenges.

Regarding these so-called challenges, they are due to the different technical natures of the telephone and packet-based networks, in addition to the inherent need to hold the same or better performance of ancient generations.

Anyhow, the move towards all-IP architecture for voice, messaging and data services delivery appears to be a strong trend and an interesting evolution of telecommunication paradigms, but it does not ensure a high level of security (Section 3).

Actually, this move needs the implementation of new mechanisms, protocols and architectural frameworks in order to work securely. In our case, we chose to study the implementation of the IP Multimedia Subsystem, which is an architectural framework for delivering protocol-based
services that enable an easy deployment of new rich multimedia services mixing voice and data.

Although this solution provides a completely new effective manner to handle telecommunication services, it does not ensure a high level of security, which can lead us to the misadministration of the services provided. Surprisingly, this problem still unsolved.

Consequently, there is an immeasurable need to an architectural design in order to construct a secure network, in addition to security supervision, follow-up and threats management, in order to keep all entities, communications, traffic and data secure.

What we are about to introduce is this paper, is our approach in order to design a secure IMS-based network, with the ability to monitor and follow up security level of the network while it is working.

This paper is organized as follows:

• We give a description to the IP Multimedia Subsystem (IMS), its functional components and the reason why it is considered as a bright solution for Next Generation Networks (Section 2).
• We prove that this system can be far from the Eldorado, in fact, even if it is a promising solution, it has plenty of problems related to security, which can affect and disturb the normal use of this system (Section 3).
• We give the syntax and semantics of our new approach dedicated to handle security issues from the design phase to the implementation phase; in addition to a full description of its innovative features (Section 4).
• We have built a simulation that represents our new approach. And the results are outstanding regarding performance and network behaviour when it adopts our proposed design (Section 5).

2. Network Architecture

The IP Multimedia Subsystem was designed by the wireless standards body Generation Partnership Project in order to evolve mobile networks beyond its original formulation; it foresees a complete migration towards an all-IP architecture, in which both the user and the control plane are based on the IP protocol stack.

The IMS core is composed of two main elements: The Call Session Control Functions (CSCF) and the Home Subscriber Server (HSS). In fact, there are three different kinds of CSCF:

• Proxy Call Session Control Functions (P-CSCF): Compresses the signalling messages that the mobile exchanges with the IMS to reduce their load on the LTE transport network.
• Interrogating Call Session Control Functions (I-CSCF): Which is the first point of contact for signalling messages arriving from another IMS. In addition to the assignment of the adequate S-CSCF to the UEs.
• Serving Call Session Control Functions (S-CSCF): Handles all registration and authentication processes with the HSS.

The IMS Core may also contain other nodes such as:

• Application Server (AS): Which is a node or a network that can help provide more advanced network services.
• Policy and Charging Rules Function (PCRF): Which is a node designed to determine policy rules in a multimedia network.
• IMS Media Gateway (IM-MGW): Which is a node able to convert VoIP streams to circuit switched streams and vice versa.
• Media Gateway Control Function (MGCF): Carries out the same role for signalling messages, controls the IMS Media Gateway and is itself controlled by the serving CSCF.

3. Threat Model

The IMS network topology structure stills vulnerable and weak facing unwanted scans and malicious use by legitimate and illegitimate users, which conduct us later to the misadministration of users, the undesirable loss of data privacy and integrity, in addition, the bad control of the network and its services. Here is a list of the main threats targeting the IP-based cellular network and particularly, IMS-based networks (based on [2–5,9–11]):

• Eavesdropping: An intruder can intercept the traffic transiting the network without any detection.
• Masquerading: An intruder hoaxes an authorized entity into believing that they are the legitimate system to obtain confidential information from another entity.
• Traffic analysis: An intruder observes the time, rate, length, source, destination and many other
information related to messages, in order to determine a user’s location or to learn whether an important business transaction is taking place.

- Inference: An intruder observes a reaction from a system by sending requests.
- Manipulation of messages: Messages may be deliberately modified, inserted, replayed or deleted by an intruder.
- Intervention: An intruder may prevent an authorized user from using a service by jamming his traffic.
- Resource exhaustion: An intruder may prevent authorized user from using a service by overloading the service.
- Misuse of privileges: An entity may exploit its privileges to access unauthorized services or information.
- Abuse of services: An intruder may abuse some service to cause disruption to the network.
- Repudiation: A user denies actions that have taken place.

Eventually, the IP Multimedia Subsystem (IMS) is considered as a promising solution for handling data, voice and messaging services in the new generation of cellular networks, nevertheless, its security level is very low. And this is a very interesting problem.

“So how could we benefit from such a useful system without exposing our network to these threats?”

“How could it be possible to enhance security level and control the security aspect of the network?”

“How do we only need to add some security mechanisms to overcome this huge problem? Or do we need a whole new security design to manage the security aspect of this solution?”

These are the main questions that this paper explicitly answers.

4. Our Proposed Model

“If you take care of a problem while it’s small you won’t have a bigger problem to deal with later”.

Here is a famous quote that sums up our strategy to deal with security problems. According to our philosophy, the better tactic to deal efficiently with problems (like in our case, it can be security holes, attacks …) is to do it when it just starts small. That is why we see that dividing the network into three layers with the wise usage of checkpoints can lead to a rapid location of security holes and detection of malicious actions before it becomes bigger and harder to manage.

In this section, we give the syntax and semantics of our innovative proposition, inspired by the ITU-T recommendations X.805 and dedicated to the IMS-based networks.

Our approach consists of dividing a complex set of end-to-end (IMS-based) network security related features into separate architectural components, which are:

- System layers.
- Logical and physical tiers.
- Security checkpoints.

In addition to the ability to manage the massive users’ requests, our proposed approach aims to monitor and protect the system, help build a rapid normal functioning retrieval after every technical defect and counter malicious intrusions and internal dysfunctions.

Besides, every layer is composed of two other tiers: Physical Components Tier (PCT) and Logical Operations Tier (LOT) and all this conceptual design is protected by a set of checkpoints: Confidentiality, integrity, non-repudiation, access rules, traceability, authentication and availability; which will help making a precise security situational analysis and a complete follow-up of security level of the network.

Figure 1. Our approach’s design to handle security issues.

5. Network Division into Layers

5.1 The Access Layer (ALay)

The PCT of the Access Layer is composed of the E-UTRAN Network in addition to the User Equipment (UE). The E-UTRAN (for Evolved Universal Terrestrial Radio Access Network) is also referred to as the 3GPP work item on the Long Term Evolution (LTE), while the UE is a device used directly by an end-user to communicate and connect to the
E-NodeB, which is responsible for all radio-related functions in one or several cells.

5.2 The Transmission Layer (TLay)
The Transmission Layer is represented by the Evolved Packet Core Network (EPC). The EPC supports access to the packet-switched domain only, with no access to the circuit-switched domain.

5.3 The Service Layer (SLay)
Figure 2 illustrates perfectly the different approaches delivering the voice and message services over the LTE network. In our study case, we aim to deliver the voice using Voice over IP server that lies outside the LTE network, with the usage of IP Multimedia Subsystem, in order to keep all the service components under the oversight of the network operator and inside its territory.

5.4 The Security Checkpoints
In this subsection, we present the eight fundamental security checkpoints for a high and sustainable security level.

The general purpose behind the use of security checkpoints is, actually, twofold:
- From the system perspective: They ensure a combined and homogeneous security scan by processing like in Figure 3, it eases both the monitoring and protection tasks, by checking every security state of every checkpoint for every single layer, which consequently will help to have an overall idea about security level of the entire network and, of course, a proactive look to malicious usage or some adapted exploitations.
- From a user perspective: A user request will be filtered (like it is shown in Figure 1) and verified with these checkpoints, in the reverse direction of the Figure 3, (starting from availability to finish with confidentiality and integrity checkpoints).

6. Network Performance and Behavior Analysis
In this simulation, we have built the Access Layer with 25 User Equipment (UEs) related to a single cell managed by one eNodeB. The Service Layer appears as an external server representing IMS and handling monitoring service, a router replacing the EPC core and standing for the transmission layer and the ENodeB stands for the Access Layer.

We consider that some of the UEs are in movement around the eNodeB. The UEs’ speeds considered in this simulation are between 0 m/s and 20 m/s and have a normal access to voice, messaging and data services.
The table below represents mechanisms used for the implementation of every security checkpoint:

| Security checkpoint                  | Mechanism used | Comments                                                                 |
|--------------------------------------|----------------|--------------------------------------------------------------------------|
| Data and communication confidentiality| 128 bits       | EEA3 algorithm is based on a new stream cipher called ZUC<sup>2</sup>     |
|                                      | EEA3           |                                                                          |
| Data and communication integrity     | 128 bits       | EIA3 algorithm is based on a universal hashing and a one-time-pad masking and uses the GMAC<sup>2</sup> |
|                                      | EIA3           |                                                                          |
| Non-repudiation                      | Traces database| the database is implemented in the server                                 |
| Traceability                         | Traces database| the database is implemented in the server                                 |
| Authentication                        | EPS-AKA        |                                                                          |

7. Simulation Results

One of the most important metrics is the MOS, which is a quality metric that measures subjective call quality for a call. It scores range from 1 for acceptable to 5 for excellent. In Figure 5(A), we can clearly see that the MOS values in our simulation are generally between 4 and 5, with of course some small exceptions varying between 1 and 4 and that’s only due to the random movement of the UEs that makes them get far from the eNodeB station sometimes. However, the MOS metric stays excellent for users staying in the eNodeB’s coverage zone, in addition, that issue can certainly be solved in a real implementation with a lot of eNodeBs using handover.

Moreover, and according to Figure 5(B), the frame delays, which is the duration needed for a packet to arrive from a UE to the other UE, are between 5 ms and 25 ms which is a very excellent result because generally, it needs to be less than 150 ms. In Figure 5(C), the playout delays of this simulation are generally null and does not exceed 15 ms.

Furthermore, the packet loss rates of this simulation are generally null and do not exceed 0.7 like in Figure 5(D).

8. Related Works

Like it has been described in the third section, this new tendency is not very safe. The traffic transiting the network is not confidential and should be protected and always available to entities that have rights to access it. As a result, many research works have been done concomitantly, in order to enhance the security level of the network.

The most notable one is the solution proposed by the International Telecommunication Union Telecommunication Standardization Sector (ITU-T)<sup>5</sup>, a security architecture that logically divides a complex set of end to end network security-related features into separate architectural components called: Security dimensions, security layers, security planes and security threats. Actually, this solution was inspirational for us. Because it gave us the idea of a need for separation in order to handle security in a better way.

However, the difference between our approach and the X805 recommendations is that our proposed model is not only designed to identify such sets that should be applied in order to face some major security threats, it is also designed to create a homogeneous orchestra of checkpoints. Because, in our opinion, security holes can have more chances to occur in a system, if the design of the latter does not respect homogeneously its security checkpoints. In addition, it also aims to facilitate the monitoring of the network and to be flexible in order to adapt to implemented networks.
9. Conclusion

As far as the security is concerned, we see that the best way to ensure a high-level security in a system is by studying the compatibility of the solutions used for security checkpoints and this compatibility should not be done randomly. And our approach is the best way to create the harmony researched in a telecommunication network and we see that the system should proceed in this manner to keep services, information data, nodes and the system secure and available while providing the service.

Following this tactic, we can ensure designing a secure, flexible and easily monitored network. Moreover, it will seem easy, rapid and effective to locate affected areas and to supervise the security level of the network while the network is operating, by verifying, periodically the security checkpoints. In addition, it can smartly be adapted to implemented networks. And the most important thing about it is that the simulation results are outstanding regarding performance and network behavior when it adopts our proposed design.

10. References

1. Slezak D, Gelogo YE. Securing IP Multimedia Subsystem with the appropriate security gateway and ipsec tunneling. Journal of Security Engineering. 2011; 8(3):385–96.
2. Chalamalasetty K. Architecture for IMS Security to Mobile: Focusing on Artificial Immune System and Mobile Agents Integration. 2009.
3. Wang D, Liu C. Model-based vulnerability analysis of IMS network. Journal of Networks. 2009 Jun; 4(4):254–62.
4. Belmekki E, Bouaouda N, Raouyane B, Bellafkih M. IP multimedia subsystem: Security evaluation. Journal of Theoretical and Applied Information Technology. 2013; 51:73–9.
5. Wu YS, Bagchi S, Garg S, Singh N. SCIDIVE: A Stateful and Cross Protocol Intrusion Detection Architecture for Voice-over-IP Environments. International Conference on Dependable Systems and Networks (IEEE); 2004. p. 433–42.
6. ETSI/SAG. Specification of the 3GPP confidentiality and integrity algorithms 128-EEA3 and 128-EIA3. Document 1: 128-EEA3 and 128-EIA3 specification. Version 1.5. Tech. rep, ETSI; 2011 Jan.
7. Hussein S. Lightweight security solutions for LTE/LTE-A Networks. [Doctoral dissertation]. Universite Paris Sud-Paris X; 2014.
8. ITU-T Recommendation X.805. Security architecture for systems providing end-to-end communications; 2003.
9. Wang D, Liu C. Model-based vulnerability analysis of IMS network. Journal of Networks. 2009 Jun; 4(4):254–62.
10. Cuevas A, Moreno JI, Vidales P, Einsiedler H. The IMS service platform: A solution for next-generation network operators to be more than bit pipes. IEEE Communications Magazine. 2006 Aug; 44(8):75–81.
11. Henrydoss J, Boult T. Critical security review and study of DDoS attacks on LTE mobile network. 2014 IEEE Asia Pacific Conference on Wireless and Mobile; 2014 Aug.