Impact of Security in QoS Signaling in NGN: Registration Study

RAOUYANE Brahim[1]
N&DP Team, IT&NT Laboratory,
Faculty of Sciences, Ain Chock, Casablanca, Morocco

BELMEKKI Elmostafa[2], KHAIRI sara[3],
BELLAFKIH mostafa[4]
RAISS Team, INPT
Rabat, Morocco

Abstract—**New generation networks (NGN) use an IP base to transmit their services as well as voice, video and other services. The IP Multimedia Subsystem (IMS) which represents the network core, allowed controls and accesses into various services through a set of signalling protocols, the most common of which is Session Initiation Protocol (SIP). After securing the most vulnerable interfaces in the core of the NGN: IMS architecture. The idea is to improve QoS in SIP signalling, especially in authentication and registration that represent the first step to access. The proposed approach is used as encryption asymmetry in the SIP registration process and study the performance of the system in terms of QoS parameters.**

Keywords—Quality of Service (QoS); Security; New Generation Network (NGN); IP Multimedia Subsystem (IMS); Session Initiation Protocol (SIP)

I. Introduction

The Next Generation Network (NGN) enables [1] the deployment of independent access services over fixed and mobile networks with agnostic convergence. NGN is based on packet switching and uses IP to transport different types of traffic (voice, video, data and signalling). The specifications were agreed that the EPC (Evolved Packet Core) would no longer have a circuit-switched domain and that the EPC should be an evolution of the packet switching architecture used in GPRS / UMTS. Indeed, this decision had consequences on the architecture itself but also on the way services were provided. Security in NGN is important, the main goal is to choose a sensitive scenario to deal with. According to security analysis and modelling, NGN can be divided into 3 boxes or boxes with their communication interfaces. The risk analysis with EBIOS (Expression of Needs and Identification of Security Objectives) designates three boxes: Client, IMS, and Server, the communication between these boxes is made by standard protocols signalling or service according to the customer need. The most commonly used services with the IMS is recording, calls, videos, messages. etc. The primary service performed by each connection is the registration, this operation is important also sensitive to faults that are related to the use or inherited from the packet switching network and others attached to the SIP signalling protocol. Our approach to remedy this registration problem is reinforced security in SIP before using the regular methods of IP (SSH, TLS). The approach is based on the Register scenario study as well as SDL (Specification and Description Language) modelling and finally demonstrates its theoretical and practical reliability in a test network.

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 (Internet Service Provider). 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 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 as well as [2][3].

In this work we will first present the IMS network architecture and we propose a state of the art of the IMS network. Second, we present our approach to secure the SIP registration after having identifying interfaces and sensitive entities in the architecture. Finally, we will analyse experimentally the operational of primordial protocols as SIP proposed compared to security standards to highlight all associated loopholes.

II. Presentation of the NGN Architecture

As Fig. 1, the 4G / LTE (Long Term Evolution) [4] network benefits from a large flow evolution and thus services that have a direct impact on topology and structure. A user (UE) connects via eNodeB, EPC and the IP Multimedia Subsystem (IMS). The EPC is combined with E-UTRAN (Evolved Terrestrial Radio Access Network) it is the communication part of a mobile network, these composite entities to form Evolved Packet System (EPS). The EPC contains the following components: Serving Gateway (S-GW), Mobile Management Entity (MME), Policy Control and RulesFunction (PCRF), and PDN Gateway (P-GW).

The integration of new features such as SDN and virtualization into the current EPC is a complex task that involves carefully evaluating 3rd Generation Partnership Project (3GPP) standardizations. The most important challenge is to preserve LTE (Long-Term Evolution) functionality in a new, flexible and centralized EPC architecture based on new features. The proposed architecture is to redefine the main procedures for control and data plans by relying on new techniques such as SDN and virtualization functions. First, firstly, the challenges of this new architecture are discussed and the proposed solutions are presented. Secondly, the possible improvements are studied in terms of flexibility, complexity and technology-based performance that could possibly optimize the design of the proposed system.

The proposed architecture aims at slightly modifying the existing 3GPP architecture in order to integrate existing core components, especially in the EPC and in the transport layer in order to integrate SDN [5] and OpenFlow [6] controller, also in the Service layer in order to perform changes to improve the performance of certain services with the principle of virtualization by complying with SLA (Service Level Agreement) constraints. The main basic interfaces: the S1-MME, S1-U, S6a and Gx functionalities are maintained, as well as 3GPP intra-3GPP authentication, authorization and mobility management by Mobility Management Entity (MME). The current Service Gateway (SGW) / Packet Data Network Gateway (PGW) selection mechanism based on the Domain Name System (DNS) has been changed. The MME queries the OpenFlow controller through the NorthBound interface (representation state transfer API) that can install transfer rules in OpenFlow switches.

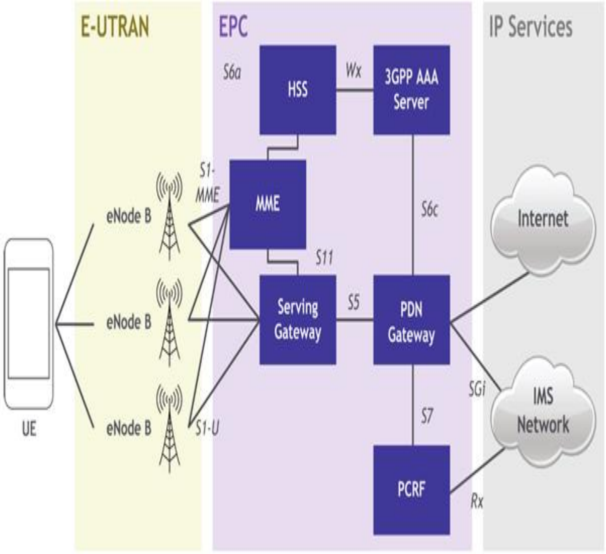


Fig. 1. IMS avec LTE-Evolved Packet Core [5].

A. SIP Security in NGN

The proposed new approach begins with an analysis of the IMS architecture to secure the communication interfaces. To this end, a study is made with the useful EBIOS to explore the main network entities as well as their communications interfaces (Fig. 2) [7].

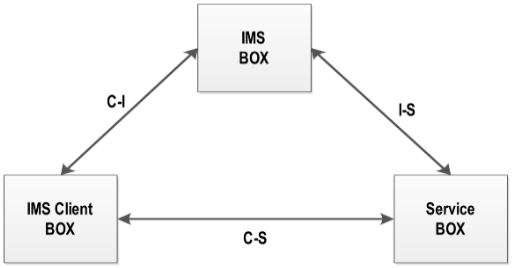


Fig. 2. Modelling of NGN / IMS Entities and their Communication Interfaces.

The resulting model consists of three entities:

- **IMS-Client BOX**: Represents the end user connected to the IMS to access network services. The IMS-Client can access it either through a packet or circuit network.
- **IMS-BOX**: represents the core of the IMS network with its different internal components with a direct and secure connection. The box represents an abstraction of the details of the communications and the different operations that take place at the heart.
- **Service-BOX**: Represents the service platforms provided by IMS for clients.
- The components communicate via 3 interfaces:
- **C-I interface:** Between the client and the IMS-BOX. The interface transports all signalling and access control traffic between the client and the IMS network. the most used protocol is SIP.
- **I-S interface:** An interface between the Service-BOX service platforms and the IMS-BOX IMS. It comprises, on the one hand, the signals that make it possible to verify that the service platform is authenticated and authorized to provide the service via the IMS network and, on the other hand, that the communication between a server and a client by the request for service access to a service. The I-S interface is based on the SIP protocol.
- **C-S interface:** Between the client and the service platforms, the interface contains the traffic of the service requested by the client. Multi-form traffic is **VoIP** communication, video conferencing, etc. The protocols used on this interface are related to the types of services.

The study proved that the communication between IMS core entities such as CSCF and HSS is very secure, since the communication link is direct as well as the security mechanism uses certificates with Diameter protocol, these assets ensure confidentiality, integrity and authentication. Nevertheless, the traffic or the flow of information, which circulates between the client and the IMS core or between the application server and the IMS core, remain vulnerable since they cross different others network entities. These communication interfaces have a critical degree of severity that classifies the risks on these interfaces as an operator security violation that must be handled first, in relation to the services that it may be SIP, HTTP, RTP, FTP traffic, or others [7].

TABLE I. PROTOCOLS AND COMMUNICATIONS INTERFACES IN NGN FOR VOLTE

Interfaces	**Protocols**	**Security Mechanism**
C-I	**SIP** **DHCP** **DNS**	**IPsec** **TLS**
C-S	**RTP** **SIP**	**sRTP** **IPsec**
I-S	**SIP**	**IPsec** **TLS**

3GPP's proposals for security in NGN / IMS architecture have difficulties and limitations, hence the need for convergence to other solutions to improve and enhance security in the three communication interfaces. The first step is to identify and analyse the traffic passing between the three components. Table I provides an overview of the set of signalling protocols and services in NGN as well as the security mechanisms recommended by the 3GPP and RFC standards.

The signalling protocols always carry out the services, for this it is necessary to secure these protocols upstream and downstream. SIP is the primary signalling protocol that will be our goal in the IMS context. Indeed, SIP is a signalling protocol that specifies the exchange of information to manage multimedia sessions in the IMS. The protocol describes the power to establish, modify and terminate a multimedia session [8].

The IMS benefits from RFC specifications and uses mechanisms to provide communication between these Client/Server/Proxy entities. The text-based SIP and uses HTTPDigest for authentication and user registration, also to secure TLS, S/MIME and IPsec signalling. On the other hand, these solutions guarantee a security on a domain or on a link but not on the whole of an end-to-end communication [8].

Before accessing the various services of the IMS, it is necessary to go through the first step which is essential authentication. The operation of authenticating a user is based on a simple challenge / response that contain several risks [9].

The TLS or S / MIME solutions guarantee security but require an intervention with certificates, which is not possible in the IMS infrastructures. As well as HTTPDigest remains simple, to the opposition of specifications of 3G with AKA [10] which impose that an authentication must be mutual systematically. Our contribution is to strengthen authentication at the signalling level either by decreasing the vulnerabilities of simple authentication, or by offering another form of mutual authentication with HTTP Digest [11].

B. *Approach to securing SIP Authentication*

The problem exists in IMS resides in the REGISTER method of the SIP protocol especially in the sensitive parts in the authentication messages, so our objective is to reinforce the mutual security between the two communicating parties without modifying the communication via the SIP protocol as well as infrastructural interoperability, while minimizing the impact on QoS. The proposed solution makes it possible to hide the sensitive fields in the SIP messages, the asymmetric encryption guarantees mutual reliable communication between the two parties (Client / Server). A partial or radical change in an existing protocol requires behavioral and static modelling to keep the properties of it. The modeling is followed by a verification test to ensure no changes in the content and SIP message only the content.

Firstly, our objective is to propose a solution to reinforce the security with a mutual authentication, what follows is to integrate the solution in the SIP protocol, secondly it is the integration in the NGN network and finally to measure the impact on the QoS. Integration is a difficult operation considering its composition of a set of processes resulting from modeling followed by a formal validation with SDL (Specification Description Language) [12], and also by a behavioral validation with the use of the MSC (Message Sequence Chart) to validate the interactions of approach [13], while respecting the IMS network components.

The user must be subscribed to an IMS network before starting any service offered by the network providers. As much as a control subsystem, IMS following an internal communication registration procedure between CSCF and HSS, and with the EU external user.

By focusing only on the signalling exchanged with UE, since the internal communications are direct and secure by a kernel. Communication between the EU and the IMS takes into account 4 messages (Fig. 3):

1) A Registration Request with Register Is Sent Contains EU Identity.

2) The IMS responds with a 401Unauthorized message with a random nonce value.

3) The client sends a response that contains Response, after a key calculation.

4) The IMS server responds with OK 200 if the answer is correct.

The method used in the registration is challenge / response authentication with HTTPDigest. In the challenge phase, a sensitive field "WWW-Authenticate is clear in the form of a "NONCE" [13]. Then, the UE generates a response based on the previous information in two "Authorization" fields with a response value in the SIP message in the form:

$$response = H\ (username\ ||\ realm\ ||\ password)\ ||\ ness\ ||\ H\ (METHOD\ ||\ Request\text{-}URI)) \quad (1)$$

A simple catch can expose SIP messages that are text-based and clearly accessible, sensitive information such as nonce values, and the response generated by the client during recording appear clearly during the communication. Indeed, the knowledge of these values can generate dictionary type attacks to easily calculate the shared secret value between UE and IMS. Therefore, it is necessary to secure the communication between EU and IMS on the one hand and on the other hand to strengthen the registration between the two parties. Our idea is to generate a significant value of nonce instead of a random value. The value of nonce generated depends on the value CallID, realm, URI, secret key and Timing [14].

The approach is without change in the procedure, it adds additional functions next to Server and SIP Client (encryption / decryption).

The reinforcement scenario is illustrated in Fig. 4. This scenario, which consists of different phases, is the same as the old one.

The main idea is the generation of the new value of "nonce" with a significant value. The generated nonce is random and invisible according to the specifications [15], the elaboration of the "nonce" is the following one:

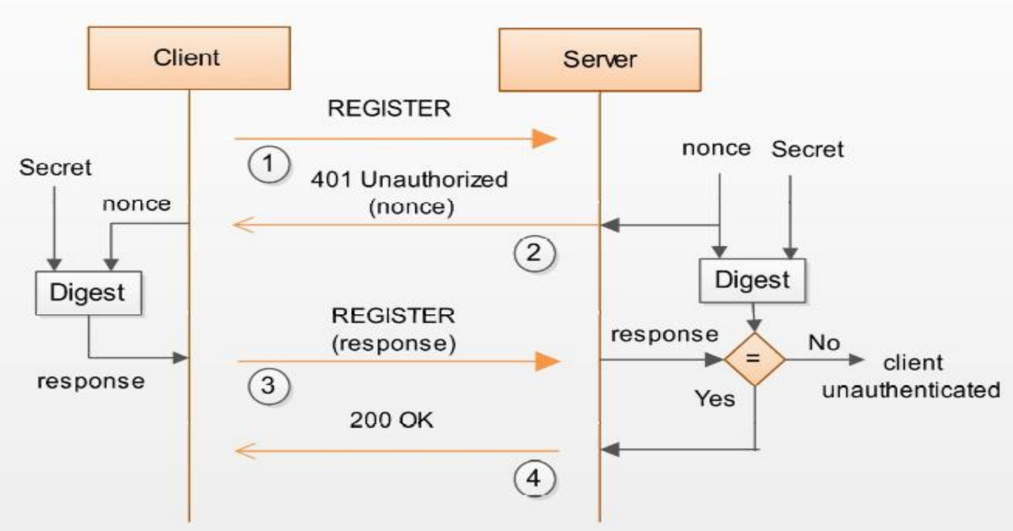


Fig. 3. Classical Registration in the IMS Network.

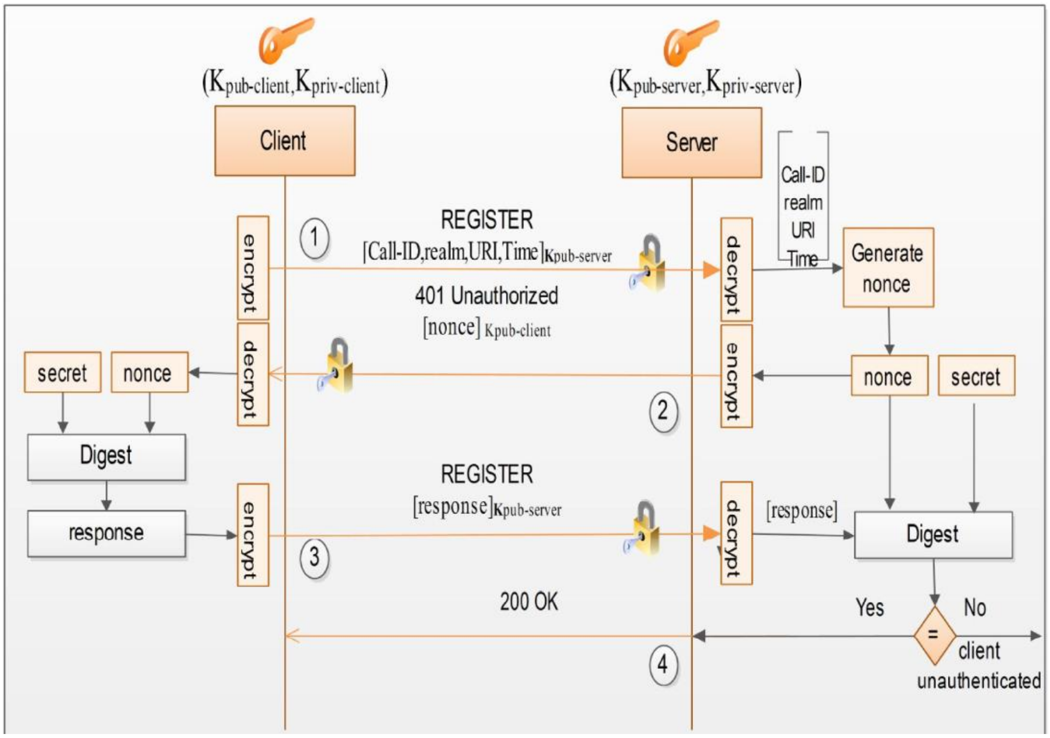


Fig. 4. Enhanced Registration in the IMS.

The registration process offers several advantages, the most important is the mutual authentication, to ensure the integrity and confidentiality of the information exchanged during the registration phase between the client and the server. This procedure also enhances security and prevents attacks that can exploit sensitive information: nonxe, call-ID, domain and response. Note that the communication architecture and messages remain as they were before [16].

C. Modelling the New Approach

The specialization of a language (SDL) follows a three-step methodology: specification, design and implementation with code generation. The first step concerns the expression of constraints and needs by the specification. At this level several languages can be used as UML, SDL. The second step concerns the definition of the execution model it is the design stage. At this level, languages like SDL-RT, LACATRE, UML-RT can be used.

The methodology must follow four essential steps:

a) Definition of constraints and specifications

b) Definition of the Structural model

c) Definition of the Behavioral Model

d) Verification and Validation

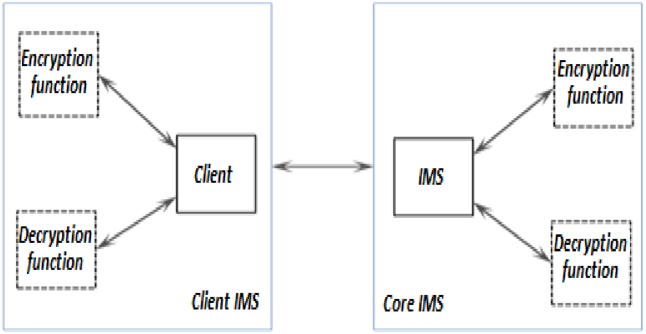
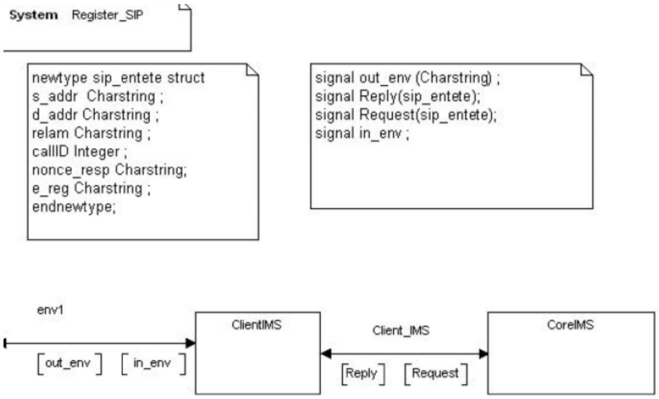


Fig. 5. All Blocks and Sub-Blocks of System.

The objective is to first enhance security by validating the registration process approach of the REGISTER SIP method.

The specifications of SDL must take into consideration all the compositional structures and links in the NGN and especially the IMS, it allows to give a concrete view in the implementation of an external operation launched by a customer such as registration or service request. In this formalism, two resulting processes: a block for the IMS network with all these components, and the second block is the client with all its activities. Likewise, each block is subdivided into three blocks relating to the authentication operation processed. The IMS block contains a master block with the functions (CSCF) of the IMS with two sub-blocks for the encryption and decryption of sensitive information. The client block has a sub-block to simulate the functionality of a client in terms of registration, the other two block aims to encrypt / decrypt information. The blocks in Fig. 5 and the sub-blocks communicate with each other via interfaces and messages [11].

The structural model is a static view, which represents the relationship between modelled entities, their interfaces, and attributes according to SDL. The communication channels between the different block instances specify the signals as SIP messages between the clients and the IMS core. Blocks and processes are used to represent entity types such as client and core IMS with the Cinderella tool. The two main IMS entities according to the definition of constraints and specifications are shown in Fig. 6.



```
newtype sip_entete struct
s_addr  Charstring ;
d_addr Charstring ;
relam Charstring ;
callID Integer ;
nonce_resp Charstring;
e_reg Charstring ;
endnewtype;
```

```
signal out_env (Charstring) ;
signal Reply(sip_entete);
signal Request(sip_entete);
signal in_env ;
```

Fig. 6. System Interaction between ClientIMS and CoreIMS.

The model contains the elements:

- **IMS Client Block**
- **Block Core IMS**
- **4 signals:** outenv, inenv, reply and request
- **2 interfaces env1 and clientIMS**: to ensure communication between the entities and their environment.

The system contains mainly four sub-blocks, these blocks are detailed according to their communication and their role of each sub-block:

- **Client Block**: This system block represents all IMS clients, these clients communicate with their environment by signals that activate processes within the block. To register in the IMS network, the block sends a signal to the Client block to activate the process. After a phase of external exchanges, the client process informs the environment of the result received from the IMS core. The process inside the client block contains the different communication interfaces and the signals between this process and the external environment.
- **Block CoreIMS**: The block is very important for the IMS, it includes all the functionalities of the entities: P-CSCF, I-CSCF, S-CSCF and HSS. The signals and the behaviors of each entity are taken into consideration in order to give a better modeling of the block. The block contains only a single process inside it is the process "IMS_process" which ensures the task of recording as well as the interactions between the 4 IMS core entities. The "CI_pr" interface ensures communication between the process and the external environment (Client or Application Server).
- **Block encryption function**: Asymmetric encryption is a communication protocol based on asymmetric mathematical functions with private keys. These mechanisms make it possible to obtain functionalities: confidential data protection, a digital signature or the exchange of secrets [16]. In an RSA crypto-system, each IMS client element and IMS core must build its own RSA module like [17]:

Algorithm 1: Module Manufacturing

```
Input : A size t for the RSA cryptosystem module.
Output : An RSA N module of size t.
1: Take a first random number p in the range $[2^{\frac{t}{2}}, 2^{\frac{t+1}{2}}]$,
2: Take a random prime number q in the meantime $[2^{\frac{t}{2}}, 2^{\frac{t+1}{2}}]$,
3: If p = q
4:     Next step 2.
5: Else if
6:     N = pq.
7: Fi
```

p and q are in the meantime $[2^{\frac{t}{2}}, 2^{\frac{t+1}{2}}]$, so we have

$$2^t < pq < 2^{t+1}$$

Which shows that $N = pq$ is size t.

After having made an RSA module, each of the participants must prepare a secret key d and a public key e:

In some cases, specific values may be taken for the public key for example: $e = 3$ ou $e = 2^{16} + 1$. In this case, steps 2 to 5 of algorithm 2 are not executed.

The function $\emptyset$ plays a central role in the RSA cryptosystem and is called the Euler function. Definition of the function of Euler: Let n be an integer. The indicator function (2) of Euler is:

$$\emptyset(n) = \#\{a|0 \leq a \leq n-1, pgcd(a,n) = 1\} \qquad (2)$$

```
Algorithm 2: Key Making
Input : Two prime numbers p and q.
Output : A private key d and a public key e
1: Calculate $\emptyset(n) = (p-1)(q-1)$.
2: Prendre un nombre aléatoire e dans l'intervalle [1; Ø(N)].
3: If pgcd(e,Ø(N))≠1
4:     Next step 2.
5: Ifelse
6:     Calculate $d \equiv e^{-1}(mod\ \emptyset(N))$
7: Fi
```

The function is defined for any integer n≥2. If the decomposition into primitive factors is

$$n = \prod_{i=1}^{s} p_i^{x_i}$$

So we have $\emptyset(n) = \prod_{i=1}^{s} p_i^{x_i} (p_i - 1)$

```
Algorithm 3: Encrypting a message
Entry: a clear message and the public key. ($N_B$,$e_B$).
Output: An encrypted message C
1: Transform the message into an integer M of the interval [2,$N_B$]
2: Calculate $C \equiv M^{eB}(mod\ N_B)$.
3: Send the message C
```

- **Block decryption function**: If the IMS receives an encrypted message C from the client. Then the decryption in message B is done using its secret key d_B as in this algorithm:

```
Algorithm 4: Decrypting a message
Entry: an encrypted message C and the private key ($N_B$, $d_B$).
Output: A clear message M.
1: Calculate $M \equiv C^{dB}(mod\ N_B)$
2: Transform the number M into a clear message.
```

III. Implementation

A. Description of Testbed

The test bench contains four layers of NGN and implements open source solutions (Fig. 7).

1) Service layer: The layer contains control entities to access IMS services (CSCF) with open source OpenIMSCore [18]; this layer can expose two types of service, the IMS service with VoD AS [19] - UCT IP TV the IMS server. Video on Demand (VoD) services allow users to watch video content of their choice at a time. And another traditional Web server Iperf [20], Iperf and an open source performance measurement tool used to test the bandwidth, the bit rate between two hosts so that one host acts as a server and the other as a client. Performance parameters can be measured with either TCP or UDP packets.

2) Control layer: This layer exposes control services with the HSS database, as well as the two QoS political entities (PCRF, PCEF) implemented in java code called UCT Policy Control Framework PCRF [21]. The layer also contains a controller that allows QoS management in SDN. We choose Floodlight [22] is a range of the Beacon Controller, a Java-based OpenFlow Controller with Apache license. FloodLight is chosen as the OpenFlow controller to be used to coordinate stream inputs and the NGN / IMS architecture. This controller is chosen because it is a robust and powerful controller.

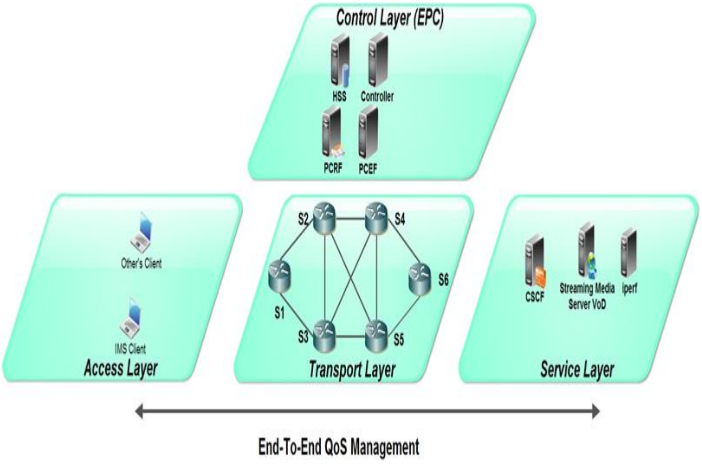


Fig. 7. TestBed Architecture.

3) Transport layer: This layer contains a set of switches that provide the interconnection with the two access and service layers. The topology is created with Mininet [23]. Mininet is used in this project to emulate the topology and to test traffic flows. A Python script is used to create the topology in Mininet, and traffic streams are received from a remote OpenFlow controller. In this layer, we defined two types of core and edge switches to implement DiffServ. The edge switch provides classification, measurement, queuing and scheduling operations; The core switch, at the input, performs a class flow and applies the PerHop Behavior (PHB). The TC traffic control tool [24] is used to show and manipulate traffic control settings. The queues are deployed in TC to ensure that each queue receives the level of service required for its class. A set of queue disciplines is implemented: First-In-First-Out (FIFO), pending class (CBQ) [24], HTB [25]. And iptables to classify all packages.

4) Access layer: The layer contains ordinary clients and an IMS client, the latter is UCT IMS Client [26] - The IMS client. The UCT IMS client support VoD / IPTV services. Our objective in this test bed is to secure client WiFi access to server via IMS network. For that we have to perform two actions:

- The Wi-Fi Client/User authentication: we use a centralized authentication server RADIUS [27] with EAP/TLS.
- Secure Client\Server communication: basically, SIP and RTP flows.

The Confidentiality, the integrity and the mutual authentication are the services we need to achieve our goal. We chose to use IPsec tunnel because it's 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. And also, our solution proposed is integrated into OpenIMScore and Clients.

B. *Experience & Test*

The objective of the test is to verify the impact of the SIP enhancement solution in the authentication operation, although check the correct integration in the IMS opensource solution. According to the test the authentication is done correctly with our new method, it remains to check the direct impact of the authentication mechanism on the response time as key of QoS.

For this it was necessary to highlight the platform response for a consistent number of users with several security solutions proposed which gives Fig. 8. The graph represents the response time or registration delay is represented in tree case: None, IPsec, TLS, and finally with SIP_Renforced which is represent our proposition for enforcing security in SIP.

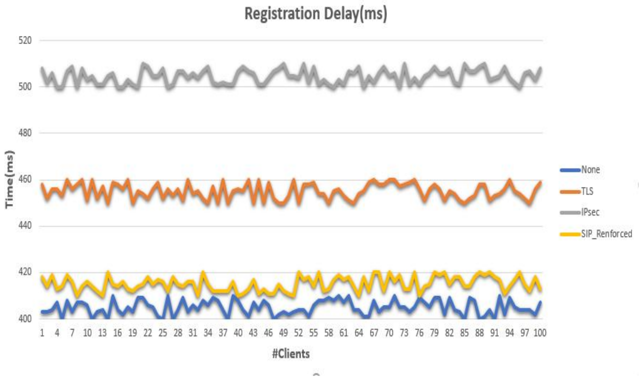


Fig. 8. Registration Delay in IMS: None, TLS, IPsec and SIP_Renforced.

The measured time is End-to-End between the client and the platform. The solutions proposed with TLS and IPsec contain security problems as well as a significant delay relative to the SIP protocol. On the other hand, the delay is less important in SIP authentication, especially with our solution that is close to values without the use of a security mechanism.

IV. Conclusion

Registration with an NGN is a sensitive and necessary operation before the request for any services. The new 4G or 5G generation offers SIP, because of its simplicity, as a primary signalling protocol. Nevertheless, in the basic registration operation, the same vulnerabilities exist with security solutions like IPsec or TLS for SIPs, these mechanisms have an impact not only by the lack of total security but also on the QoS and especially the time of reply.

In our work, instead of using traditional solutions like IPsec and TLS, we do an analysis of the NGN architecture as well as the registration procedure with SIP. The study shows that it is possible to modify the key supply principle (private and public) without changing the exchange messages or the protocol followed by authentication. After the analysis, comes the modelling step that we used SDL to integrate our solution with test bed to first test the feasibility and actual operation of our proposal and second to know the impact of direct on the response time.

The integration is done without problem as well as the measurement results show that the delay is close to what existed before. Our next research jobs focus on other type of signalling and other SIP message or other usual service in NGN (5G). The security aspect is still a persistent problem in the IP world.

References

[1] https://www.itu.int/ITU-T/studygroups/com13/ngn2004/working_definition.html

[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] 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.

[4] ETSI TS 123 272 V13.3.0 (2016-04) Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; Circuit Switched (CS) fallback in Evolved Packet System (EPS); Stage 2 (3GPP TS 23.272 version 13.3.0 Release 13

[5] SDN Architecture Overview Version 1.0 December 12, 2013 available via https://www.opennetworking.org/wp-content/uploads/2013/02/SDN-architecture-overview-1.0.pdf

[6] OpenFlow Switch Specification Version 1.5.1 (Protocol version 0x06) March 26, 2015 ONF TS-025, available via https://www.opennetworking.org/wp-content/uploads / 2014 / 10 /openflow-switch-v1.5.1.pdf

[7] Bellafkih.M. Belmekki.E. "efficient light model for securing IMS network". Intelligent Systems: Theories and Applications (SITA), 9th International Conference on Date 8-9 May 2013. EMI. Rabat Maroc IEEE, (8-9), May 2013.

[8] Bouaouda.N; Raouyane.B; Belmekki.E; Bellafkih.M. "IP Multimedia Subsystem : Security evaluation". Journal of Theoretical and Applied Information Technology, Vol. 51, No.1(10), May 2013.

[9] Belmekki.E. " Analyse des risques par EBIOS et validation d'une approche pour la sécurisation dans un réseau IMS". thèse de doctorat soutenu a la FST Mohammedia, Université Hassan 2, septembre 2015.

[10] 3GPP. "network domain security, IP network layer security". TS 33.210 (Release 5), March 2008.

[11] Garcia-Martin.M. Camarillo.G. "the 3g IP Multimedia Subsystem (IMS) : Merging the internet and the cellular worlds". John Wiley et Sons, ISBN : 9780470516621, 2008.

[12] ITU-T. "recommendation z.100. specification and description language (sdl).technical report z-100". International Telecommunication Union Standardization Sector, Genève, 1994.

[13] Bellafkih.M. Belmekki.E, Raouyane.B. "secure sip signalling service in IMS network". Intelligent Systems: Theories and Applications (SITA),

9th International Conference on Date 8-9 May 2014.Rabat Morocco IEEE, (8-9), May 2014.

[14] Bouaouda.N; Belmekki.E; Bellafkih.M. ”towards a new approach for securing IMS networks”. AASRI Conference on Intelligent Systems and Control (ISC 2013) Vancouver, Canada, proceeding published by AASRI Procedia (ISSN : 2212-6716) by ELSEVIER, which will be indexed by ScienceDirect and Scopus, Vol. 4(17-18), April 2013.

[15] J. Rosenberg And el , "SIP: Session Initiation Protocol", RFC 2361, June 2002

[16] Belmekki E.; Bellafkih M.; Belmekki A. «Enhances security for IMS client» Fifth International Conference on Next Generation Networks and Services (NGNS) 28-30 May 2014, Casablanca, Morocco IEEE

[17] Dobbertin.H.”The status of md5 after a recent attack”. cryptoBytes, vol 2 n.2(p 1-6), 1996.

[18] OpenIMSCore home page, [online] Available: htp://http://www.openimscore.org/

[19] Uct ip tv home page, [online] Available:https://linuxstgo.wordpress.com/2012/04/30/how-to-setup-uct-advanced-iptv/

[20] IPerf home page, [online] Available: https://iperffr/.

[21] PCRF home page, [online] Available: https://developer.berlios.de/project/showfiles.php?group_id=7844

[22] Floodlight Queues home page, [online] Available: https://floodlight.atlassian.net/wiki/display/floodlightcontroller/How+to+Use+OpenFlow+Queues

[23] Mininet home page, [online] Available: http://mininet.org/walkthrough/.

[24] Linux TC home page, [online] Available: http://linux.die.net/man/8/tc.

[25] Linux HTB home page, [online] Available: man7.org/linux/man-pages/man8/tc-cbq.8.html

[26] D. Waiting, R. Good, N. Ventura, The UCT IMS Client”, 2008. Uct ims client home page, [online] Available: https://yulexs.wordpress.com/tag/uct/.

[27] Rigney, C., Willens, S., Rubens, A., and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, June 2000.