SECURITY ANALYSIS AND DELAY EVALUATION FOR SIP-BASED MOBILE MASS EXAMINATION SYSTEM

Ahmad Barnawi[1], Abdulrahman Altalhi[2], Nadine Akkari[3] and Muhammad Emran[4]

Faculty of computing and information technology, King Abdulaziz University, KSA
[1]ambarnawi@kau.edu.sa [2]ahaltalhi@kau.edu.sa [3]nakkari@kau.edu.sa
[4]memran@kau.edu.sa

ABSTRACT

IP Multimedia Subsystem (IMS) is considered to be one of the important features in Mobile Next Generation Networks (MNGN). It adds value to the mobile services and applications by integrating mobile network resources, such as location, billing and authentication. This is achieved by enabling a third party access to network resources. In previous work [1] we have presented a testbed to be used as platform for testing mobile application prior to actual deployment. We have chosen a novel IMS based MObile Mass EXamination (MOMEX) system to showcase the benefit of designing an IMS based mobile application. We identify two aspects essential to of the application namely security threats and delay analysis. In this paper we identify MOMEX security threats and suggest strategies to mitigate system vulnerabilities. We then evaluate the performance of MOMEX system in terms of delay and security threats and vulnerabilities. The results presented show system performance limitation and tradeoffs.

KEYWORDS

IMS, SIP, mobile application, performance evaluation

1. INTRODUCTION

Driven by competition from application warehouses i.e. Over the Top players, standardization body, such as 3GPP, has paid enormous attention to develop an interface for third parties to access the mobile network to deploy applications that will make life much easier for mobile users. This business model will also make sure that mobile operator can secure some revenues out of the traffic going through their networks [1]. IP Multimedia Subsystem (IMS) is considered as the cornerstone for NGN. IMS is best described as the glue between the "global" applications world (Internet) and the mobile world. The IMS was designed to enable third party developers to deploy their applications over mobile networks. According to the standards, IMS is defined in the form of reference architecture to enable delivery of next-generation communication services of voice, data, video, wireless, and mobility over an Internet Protocol (IP) network [1]. Signaling in IMS network is based on a Session Initiation Protocol (SIP). The SIP based architecture provides a multiservice environment with multimedia capabilities. IMS contains Home Subscriber Server (HSS), which is the central storage area for user-related information such as his/her security related information or the service to which the user is subscribed to. It is also consists of the Serving Call Session Control Function (S-CSCF) which acts as the central node of the signalling

DOI : 10.5121/ijngn.2012.4101

plane. S-CSCF on one hand is connected to the Application Server that hosts the application and on the other it is connected to HSS and the mobile IMS either through the Proxy CSCF (P-SCSF) if the client resides in its own area of serving or Interrogator CSCF (I-SCSF) if a client is being served by another S-CSCF.

This funded research project is aimed toward the development of a testbed for Next Generation Networks (NGN). The testbed is to be used for testing mobile applications prior to actual deployment. The benefits of such testbed are enormous. For start it would enable third party application developer to test applications in realistic environment prior to deployment. The testbed will also facilitate studying the traffic and signaling in NGN network to optimize system performance.

Along with testbed development, we showcase the advantages of IMS based mobile application by developing a Mobile Mass Examination (MOMEX) system. MOMEX System expedites the examination process for mass students by automating various activities in an examination such as exam paper setting, scheduling and allocating examination time and evaluation etc.

The MOMEX system will assess to students by conducting mobile based objective exam. This will be highly customizable for any university who acquired to adopt similar IMS based examination system and faculties to create their own dashboard (create set of questions, creates groups, adds related students into the groups, schedule exams, etc.). Further, the exams will be associated with specific groups so that only associated students can appear for the test; result will be notified to the student either through SMS/email as shown in Figure 1.

IMS based applications inherits several security challenges for both infrastructure providers and mobile users. Thus security for MOMEX system has to be taken care of due to the nature of the application. In this paper, we provide an overview of the IMS based application architecture and the security challenges that it raises. It is intended as a case study basis for assessing security threats and counter measures to secure NGN mobile applications.

As a distributed system, performance evaluation of a heterogeneous system such as the IMS is a none trivial problem. It also appears that signaling delay associated with SIP messages, have concerned mobile operators about the viability of SIP services over the UMTS air interface [2]. In this paper we provide an insight into the SIP based applications performance, focusing on the MOMEX system. We furthermore study the effect of security threats on the overall delay. Results of a performance evaluation of the registration and set up signaling scenarios are presented in terms of time delay through the IMS network components.

The paper is organized as follows. In section 2, an overview in Mobile Exam Examination system is presented. In section 3, Security Risk Analysis for SIP Based IMS Exam Application is conducted. In section 4, we summarize the system vulnerabilities and counter measures. In section 5, an application layer security gateway solution is proposed. Section 6 presents the delay analysis in function of the student's registration and set up phases. Next, the IMS delay is analysed to determine the delay bottleneck of the system. In section 8, performance evaluation and related results are presented. Finally related security vulnerabilities are studied in function of the delay analysis. At the end, we conclude and discuss future works.

2. MOBILE MASS EXAMINATION (MOMEX) SYSTEM

SIP based Mobile Examination scenario is based on the following High Level Operations which are illustrated in the following figure 1 and explained below [3].

- Step 1 & 2: The exam will be scheduled by the teacher to be triggered to specified recipients (UA) on the specified time.
- Step 3: User authentication by the application server and exam submission by the client will be carried out in this step.
- Step 4: Informing the students for the examination results.
- Step 5: After automated evaluation sending results back to the teacher for further clarifications or manual corrections.

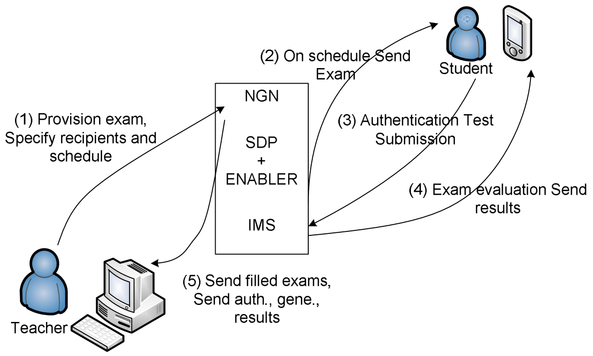
(2) On schedule Send Exam
Student
NGN
SDP
+
ENABLER
IMS
(1) Provision exam, Specify recipients and schedule
(3) Authentication Test Submission
(4) Exam evaluation Send results
(5) Send filled exams, Send auth., gene., results
Teacher

Figure 1. Mobile exam use case

The MOMEX will typically be deployed over IMS based system. The IMS main Components are listed as follows:

CSCF: The Call State Control Function (CSCF) is the heart and soul of the IMS. SIP (Session Initial Protocol) is used as signaling protocol for establishing, controlling, modifying and terminating sessions between two or more the SIP routing machinery. CSCF can be further divided into 3 subcomponents mainly P-CSCF, I-CSCF, S-CSCF.

The Proxy –CSCF (P-CSCF): is the first point of contact for user with the IMS and act as an outbound/inbound SIP proxy server. This means that all the requests initiated by the IMS terminal or destined for the IMS terminal traverse the P-CSCF. The P-CSCF includes several functions, some of which are related to security. Since SIP is a text based protocol and sometimes SIP message can be large so the P-CSCF also includes a compressor and a de-compressor of SIP messages using SigComp, which reduces the round-trip over slow radio links. It may also include a PDF (Policy Decision Function), which authorizes media plane resources e.g. quality of service (QoS) over media plane.

Interrogating-CSCF (I-CSCF): I-CSCF is used to conceal network details from other operators, determining routing within the trusted domain and thus helps to protect the S-CSCF and the HSS from unauthorized access by other networks.

Serving-CSCF (S-CSCF): The S-CSCF acts as a registrar. It controls subscriber's service (handling registration processes, making routing decisions and maintaining session states, etc) on every session that the user initiates.

The Home Subscriber Server (HSS): Is the master data storage for all subscribers and service related data of the IMS. The main data stored include user identities, registration information, location of the subscriber device, the services a subscriber is allowed to access and other service-triggering information.

Application Server (AS): AS is not a part of IMS Core, AS is a SIP unit that hosts and executes services depending upon the services subscribed to and invoked by the user. The ASs offer APIs like SIP servlet, Parlay for application execution.

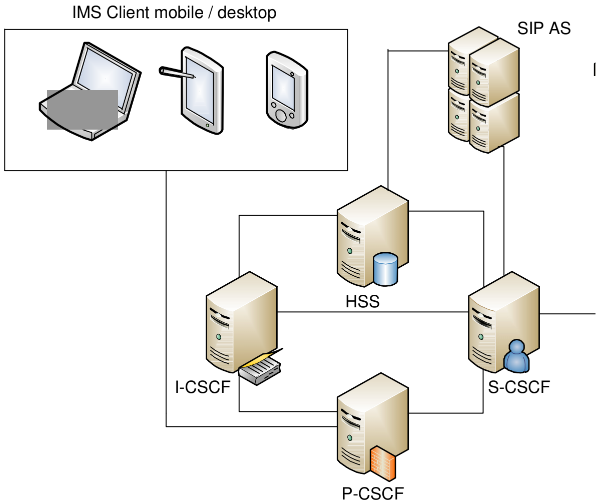

Figure 2. IMS-SIP based components of the Mobile Exam Application Infrastructure Source [3]

3. Security Risk Analysis for SIP Based IMS Exam Application

Here we conduct an analysis aimed at evaluating security threats for MOMEX system. We start with listing the threats and scenarios of occurrence and we end up with proposal addressing common security threats.

3.1. General Type of the possible attacks on the IMS components

The title is to Attack on SIP based network can be categorized into passive versus active attacks, Internal versus external attacks, single source versus multisource attacks. Security Analysis shows that following are the possible risk factors that should be taken care of in designing Mobile Exam Application.

3.1.1. Gateway attacks

Different access technologies are being converged on IMS platform which need conversion of the content from one access technology to the other. This conversion is achieved by the gateways that require some level of conversion in content forms, which is legitimate manipulation of the content. These are the most vulnerable hosts in the IMS network specifically, signaling gateway (SGW), Media Gateway Control Function (MGCF) and Media Gateway (MGW). [4] The content conversion should be integrity checked otherwise some intruder may perform an inverse conversion from a malicious script that may look legal contents which could harmful after conversion for the network.

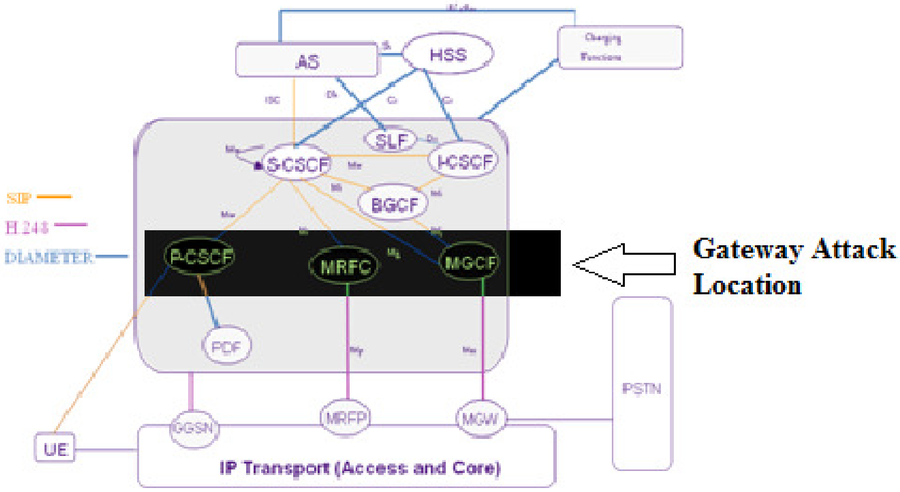

Figure 3. Gateway Attack

3.1.2. Denial of Service (DoS) attack on User Agent (UA)

In IMS infrastructure an individual user could be held under the DoS attack. Due to DoS attack the required bandwidth for the UA will be consumed by the attack initiating malicious machines. IMS security mechanism should be capable enough to guard against DoS attack especially when user is trying to access the exam [4]. An attacker can issue a large number of fake requests which can be targeted to SIP network device to consume its resources and not allow it to access the exam from the exam application server.

3.1.3. Application Servers security

As the third party application servers are accessible on the IMS network. The more are the chances that UAs are getting affected from suspicious attacks which indirectly can affect the security of the application servers. User agent security should be taken care of by applying the proper authentication mechanisms which is important for the security of application servers [4].

3.1.4. Presence Consideration and Identity Risk

Wide range of social networking applications on IMS network pose more security risks on IMS UAs. For example IMS user agent presence data may disclose some of the attributes of UA to others like current status, availability and location of UA. Presence data must be safeguard against eavesdropping and should only be accessible by legitimate users, who have permission to access private data [4]. In IMS HSS is the component which stores the user's profiles. User defined groups should be managed by the IMS instead of users so their security can be taken care off.

3.1.5. Hijacking of SIP Registration

The SIP registration session can be hijacked by a hijacker during the SIP user registration process:

1. By launching DOS attack on user machine the legitimate user's registration can be disabled.

2. Hacker can send a registration request with attacker's IP address instead of the legitimate user's address to get registered on.
3. Attacker changes the IP address in the header by replacing its own IP with the IP of the original user's IP.
4. By these steps the attacker can gain access to the network and SIP messages are read by the hacker clearly.
5. Because SIP messages are being sent in clear text and no SIP message authentication is built into the protocol that is why the attack is made possible.

For Sip Registration Hijacking attack the security measure should be taken at the application level. The proper way of authentication and SIP Optimized firewall should be used to secure the SIP components. [5] SIP registration Hijacking is shown in figure 4.

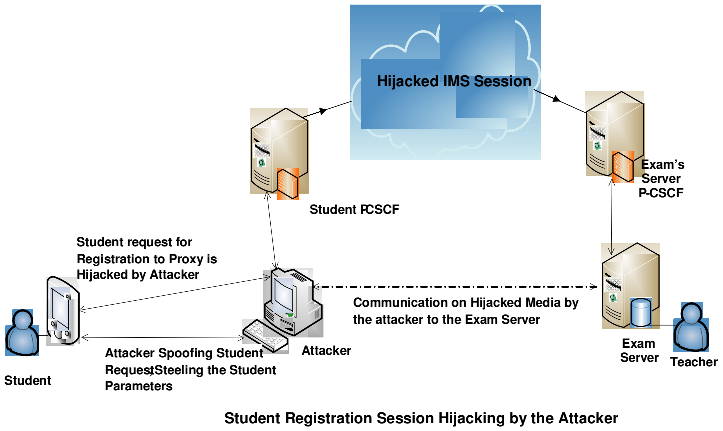
Hijacked IMS Session
Student PCSCF
Exam's Server P-CSCF
Student request for Registration to Proxy is Hijacked by Attacker
Communication on Hijacked Media by the attacker to the Exam Server
Attacker Spoofing Student Request,Steeling the Student Parameters
Attacker
Exam Server
Teacher
Student
Student Registration Session Hijacking by the Attacker

Figure 4. Student Registration Session Hijacking by Attacker

3.1.6. Eavesdropping

Internet tools like Ethereal and Wire shark could be used to make eavesdropping possible for the traffic based on SIP signaling protocol. SIP messages are sent in plain text which is easy to capture and analyzed by the sniffer.

By intercepting the signaling and associated media streams of a VOIP conversation could help in eavesdropping. Media streams are usually carried over UDP and RTP. Packet sniffing tools can capture and decode RTP packets.

IPSEC could be one solution for the IP packets secure encryption making them safe from unauthorized access or modifications. By using shared keys between the parties IPSEC can provide the secure path for communication between the SIP Users.

Eavesdropping should be handled at the application layer by applying proper security measures otherwise the rough UA can listen the conversation of the VOIP enabled UA [5].

3.1.7. Proxy Impersonation

In Proxy Impersonation attack the attacker can trick the proxies to communicate with the rouge proxy. If the attacker can successfully impersonate the proxy, he can have the full access to the SIP messages and is in complete control of the session. Lack of strong authentication and communication using UDP is the reason for proxy impersonation attack. A rouge proxy can insert itself into the communication by using either Domain Name Service (DNS) spoofing, Address resolution protocol (ARP) cache spoofing or by simply changing the proxy address for a SIP User Agent. Proxy Impersonation attack is shown in figure 5.

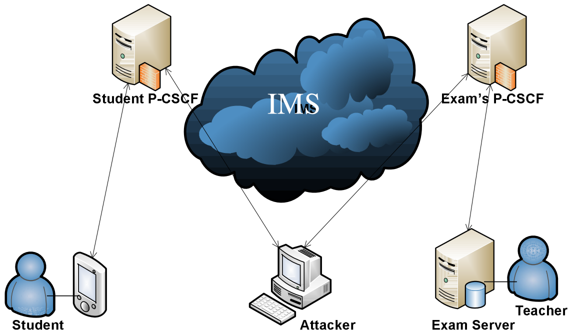

Figure 5. Proxy Impersonation Attack

DNS spoofing can be used to redirect the outgoing call to a particular domain. ARP cache spoofing is an attack on the internal switch which can trick the UA to communicate with a rough proxy on the internal network. The calls from the user agent can be intercepted by the attacker [6].

3.1.8. Session Tear down (Bye Attack)

The "Bye" message can be crafted and sent by an attacker as man in the middle attack to tear down the ongoing exam session. This message can be crafted by learning the necessary session parameters which are Session ID, RTP Port etc. To mitigate this type of attack the security for the session parameters must be made mandatory by encrypting the message. Either Transport Layer Security (TLS) or IPSec can be employed to provide security measures against such type of attack [7]. Session teardown or Bye attack is shown in the figure 6.

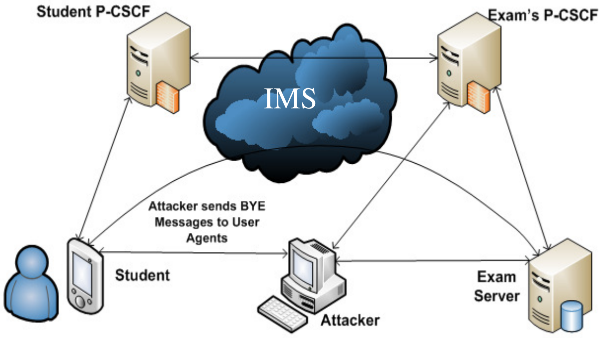

Figure 6. Session Tear down (Bye Attack)

3.1.9. DoS Attack on Application Server

SIP is susceptible to threats and vulnerabilities which exist in the Internet realm. [8]. SIP architecture components and devices should be made secure against denial of service attacks. One of the possible methods to create DOS attack can be launched by creating a large number of requests against any SIP component so it cannot provide useful service. The examination server can be the potential target of such attacks.

3.1.10. Reflection distributed DOS (RDDOS)

Reflection distributed DOS (RDDOS) attack can also be a threat and launched by using attack reflectors, which create a large number of requests against the target SIP component. Weak areas in SIP based network can be exploited as vulnerabilities of the network which could help the attacker to gain access to the network and could cause potential security threats for the system [7]. If no appropriate security mechanism is in place then attacker may easily find any appropriate parameter needed to launch any of the above mentioned types of attacks. Security analysis indicates that proper security mechanisms are required in SIP based networks for exam application to provide confidentiality, integrity, Authentication, Authorization and Accounting (AAA) services.

4. Summary of attacks and counter measures

The increasing need of security concerns have focused on securing both the components of IMS architecture and the application servers as well. In this part in the following table we have summarized the possible security threats and their vulnerabilities for mobile exam application. Also we discussed possible countermeasure for the security of mobile exam application. On Internet thousands of messages can be generated or tailored and sent to attack applications servers. To handle the multimedia sessions on Internet and 3G Networks SIP is adopted as signaling protocol. SIP specification does not include any specific security mechanisms. The utilization of other well-known Internet security mechanisms is suggested. Following security methods are described in [7] which can help us in securing our exam application.

4.1. IPSec and SIP

For lack of authentication mechanism in SIP, proper security measures should be taken care of at application development time. “IPSec in SIP can safeguard signaling and data from various network vulnerabilities, provided that some sort of trust (e.g. pre-shared keys, certificates) has been established beforehand between the communicating parties.” [7] .This could be achieved by the use and sharing of proper keys during the authentication phase between the student agent and exam application server.

4.2. Transport Layer Security (TLS)

TLS support is not yet fully implemented in current SIP UAs [7]. On SIP components, Transport Layer Security (TLS) standard should be enforced to provide strong authentication and encryption between these SIP components. Secure RTP (SRTP) can also be used as a standard for media gateway protection. The firewalls should also support TLS as a security measure to incorporate the secure authentication.

4.3. Authentication, Authorization and Accounting Services in SIP

It is more convenient for SIP entities to communicate with an authentication, authorization and accounting (AAA) server than attempting to store users’ credentials and profiles locally as required by the HTTP digests [7]. In hardware based solutions for the sack of IMS security numerous devices such as SIP optimized firewalls can be used to protect the SIP systems from attacks. Session border controllers (SBC) and other application specific gateways are all part of the proposed security measures which could be taken to protect the exam application from the above mentioned threats.

5. PROPOSED SOLUTION

In our proposed solution we have deployed Application Level Gateway (ALG) and firewall in order to make secure communication on IMS network. ALG is deployed exact before SIP application server and packet filtering firewall is deployed between the Internet client and IMS network. Firewall could help in packet filtering or can provide state full firewall functionalities. SIP traffic should be passed through the firewall and directed towards the ALG in order to be checked by the ALG before getting into SIP application server.

Application Level Gateway will help in deep packet inspection of all the packets directed towards it. Application specific protocols are being supported by the ALG. An ALG can allow firewall traversal with SIP back to back user agent (B2BUA). SIP sessions can be passed to the ALG instead of the firewall if the firewall has its SIP traffic terminated on an ALG. NAT traversal is another issue for SIP which can also be solved with ALG. Information within the SIP messages can be rewritten by a NAT with a built in ALG and can hold address bindings until the session terminates.

An ALG plays here the roll similar to a proxy as it is being deployed between the client and the server and it facilitates the information exchange. The only difference between the Proxy and the ALG is that ALG performs its function by intercepting the messages without the application being configured to use it whereas the Proxy needs to be configured in the client application to be used by the client. In case of Proxy the client explicitly connects to the proxy rather than the real server [8].

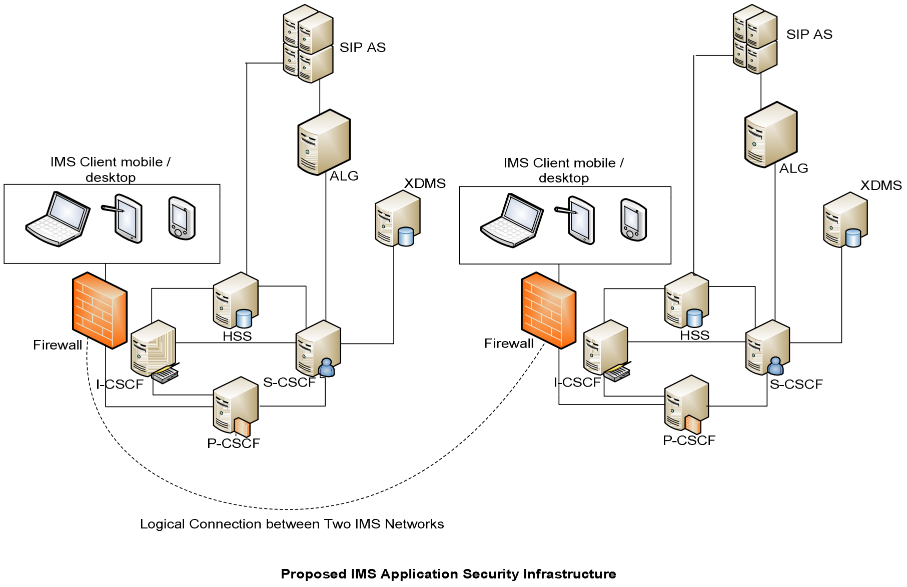
SIP AS
ALG
XDMS
IMS Client mobile / desktop
Firewall
HSS
I-CSCF
S-CSCF
P-CSCF
SIP AS
ALG
XDMS
IMS Client mobile / desktop
Firewall
HSS
I-CSCF
S-CSCF
P-CSCF
Logical Connection between Two IMS Networks
Proposed IMS Application Security Infrastructure

Figure 7. Firewall and ALG Deployment in IMS Networks

Table 1. Security Threats Comparison

Security Threat	Target	Vulnerability
SIP Registration Hijacking	UAs, Media Gateway (MG), Interactive Voice Response (IVR), VOICE Mail System	User Agent Messages Spoofing
Eavesdropping	SIP Message	User Agent / Proxy Message Spoofing
Proxy Impersonation	Proxy	Proxy Messages Spoofing
Session Tear Down Attack (Bye Attack)	User Agent (UA)	Lack of Authentication
VOIP Server Attack	User Agent (UA)	Lack of Authentication

6. DELAY ANALYSIS

In order to evaluate the performance of the exam system, the end-to-end delay from the access network to the Exam AS over the IMS network will be analyzed. The IMS-based exam will be based on the core IMS for student registration and the Exam server for exam delivery. Accessing the system will be through the access network where the mobile is launching the request. This Student-to-server delay is calculated starting from the student registration with the SCSCF and ending up with the exam being delivered to the student. This process includes students accessing the Exam access server from any access network and then requesting the exam. According to the exam system, student should first register and be authenticated before the AS accept the student invitation and to open the exam session. At this point all the http and RTP messages will be exchanged. Thus the total delay in study is the signaling delay composed of the registration and set up phases that took place before the user starts the exam session. Accordingly, the total delay is viewed to be equal to the time taken by the registration and set up signaling in the access network and IMS network as per equation (1).

$$\text{Total delay} = \text{Access network delay} + \text{IMS delay} \quad (1)$$

From equation (1), the IMS delay and the access network delay need to be considered for both the registration and the set up phases. The access network delay will be considered as negligible as we will assume the students will be accessing the IMS through a high data rates network.
We will evaluate the total delay in the IMS networks considering separately the registration and the set up phases.

We will build our model based on the queuing theory and we will study the system performance in function of the related parameters such as arrival rate, waiting probability, number of students, etc. The purpose of the study is to specify what will be the bottleneck of the system, which system parameters will contribute in the total delay and what could overflow the serving points of the system.

6.1 SIP registration phase

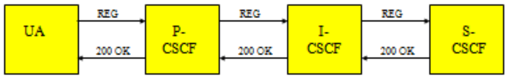

Figure 8. SIP signaling example for registratioon phase

The main components of the IMS network is as shown in figure 8. The P-CSCF is the entry proxy point for all SIP messages from end-points to the rest of the IMS network. It could be in the home network or may reside in the visited network. The P-CSCF determines what I-CSCF to send SIP messages to, which could be an I-CSCF in its own network or another I-CSCF across an administrative domain [9]. The Interrogating-CSCF (I-CSCF) is responsible for finding the S-CSCF at registration. The main function of the I-CSCF is to proxy between the P- and S-CSCF [9]. The Serving-CSCF (S-CSCF) is responsible for interfacing with the Application Servers (AS).

When receiving a registration request as a SIP message from an I-CSCF, the S-CSCF will query the HSS via Diameter protocol to register the terminal as being currently served by itself [9].
The Home Subscriber Server HSS provides information to the I-CSCF for locating the S-CSCF. It provides service profile information to the S-CSCF. The registration phase is made of a "REG" SIP messages sent from P, C, to S –CSCF. A UA client sends REGISTER message to inform a SIP server of its location. While processing the message, the response is "401 Unauthorized" as the user agent needs to authenticate. It therefore resends the REGISTER request again with authentication information and thus receives "200 OK" SIP message sent on the reverse way as shown in figure 8.

6.2 SIP set up phase

As per figure 9, a student has to register with the IMS core network per every mobile exam session setup. After registration, the user selects the exam service by sending to the S-CSCF an INVITE message, which is forwarded to the appropriate AS after resolving its destination address [10]. In the INVITE message, a caller sends this message to request that another endpoint join a SIP session such as AS. AS is the Application Server where Mobile Exam service is applied. The S-CSCF sends a SIP TRYING message "100 OK' to the user for a waiting state. SIP INVITE is processed toward the AS as shown in figure 9. 200 OK response means that the request was successful. ACK is a SIP UA response to an INVITE.

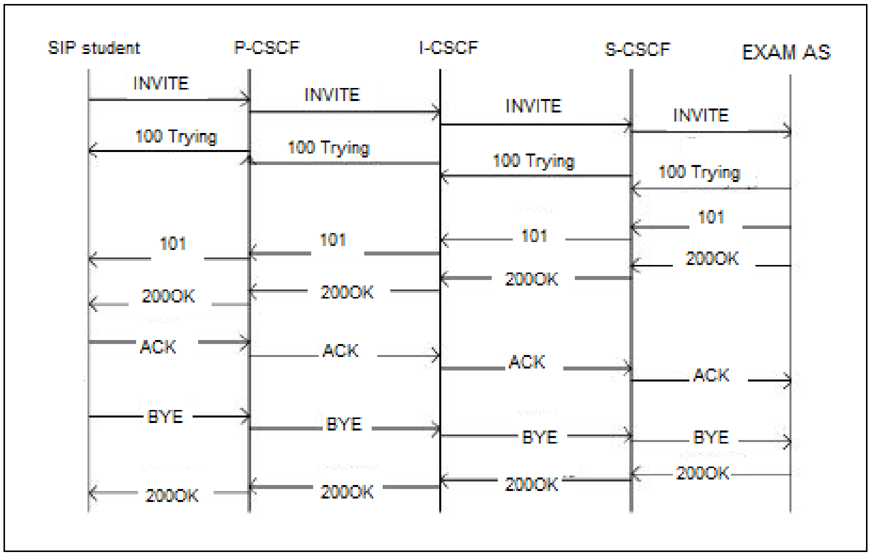

Figure 9.SIP set up messages

7. IMS DELAY ANALYSIS

As per (1), the total delay consists of calculating the Access network delay and the IMS delay where the access network delay will be considered negligible with the assumption that the students will be accessing the IMS through a high data rates network.
We will evaluate the total delay in the IMS networks as per equations (2) considering separately the registration and the set up phases.

$$\text{IMS delay} = (\text{queuing delay} + \text{propagation delay})\text{reg} \\ + (\text{queuing delay} + \text{propagation delay})\text{setup}\ (2)$$

The propagation delay is affected by the distance between the nodes and the channel characteristics. This parameter is considered negligible.

7.1 Queuing delay

In order to evaluate the queuing delay which contributes in both the registration and setup phases, each entity in the IMS network is modelled as M/M/1 as P,C and I-CSCF are responsible to process SIP messages and forward them from one node to another as per figure 11. Thus, we modelled the PCSCF as M/M/1 since PCSCF will be the first node that will accept the REG message from the UE. In this case, this system will not have loss due to the infinite buffer which will handle all the registration requests. Other CSCF nodes are modelled as the M/M/1/ as well contributing in M/M/1 cascaded model.

Figure 10 shows the overall scenario illustrated in the given queuing system. In this model, the total delay will be equal to the serving delay and the queuing delay within every node. In addition, the following assumptions were made:

- The students initiate a connection to the network as a Poisson process with an intensity of λ where λ is the arrival rate.
- The service time distribution of the CSCF nodes is exponentially distributed with mean of mean service rate assumed to be greater than the mean arrival rate.

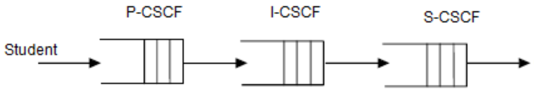

Figure 10. Queuing system for registration

The registration end-to-end delay is equal to the queuing delay in P-CSCF, I-CSCF, SCSCF and the serving delay in P-CSCF, I-CSCF, S-CSCF. The communication with the AS consists of sending SIP Invite message from UE to AS. The end-to end queuing delay:

Queueing delay = waiting time $_{(P,I,S,)}$ (3)

Where P,I, and S denotes P-CSCF, I-CSCF, and S-CSCF respectively. As per [11], waiting time at a node n is given by:

$$Wn = \lambda/[\mu * (\mu - \lambda)]\ (3.1)$$

Where λ denotes the arrival rate of P-CSCF and the P denotes the service rate of P_CSCF.

$$\text{The IMS registration queuing delay} = \text{waiting at } (UE + PCSCF + ICSCF + SCSCF)$$
$$= 2 * Wua + 4 * Wp + 4 * WI + 2 * Ws \quad (3.2)$$

Where the coefficients 2, 4, 4, and 2 are the number of messages that are to be processed by the involved node such as the UA, P-SCSF, ICSCF and S-CSCF respectively. In the same way, the queuing delay could be calculated for the IMS setup delay as:

$$\text{IMS Setup delay} = 4 * Wua + 7Wp + 7 * WI + 7 * Ws + 3 * WAS \quad (3.3)$$

Where W_n is the packet queuing delay at node n, and the coefficients are the numbers of messages that are to be processed by the involved nodes such as UA, P-SCSF, ICSCF and S-CSCF and AS respectively. Based on the above equations, the total delay could be finally calculated in function of the waiting time, in both the registration and the set up processes.

8. PERFORMANCE EVALUATION

As we calculated the queuing delay for both the registration and the setup phases, each entity in the IMS has its own unit processing cost in addition to the cost of searching within the information table such as in HSS node. We need to consider the HSS processing delay that depends on the address lookup delay. As the processing cost will increase with respect to the number of users which corresponds to an increase in the number of entries in the table thus an increased processing time as per [12]. The processing time for the HSS node is given by:

$$\text{Processing cost} = CIMS\_NODE + K' (\log k + 1N + R) \quad (4)$$

Where C_{IMS_NODE} is the processing cost per IMS node, K' is in function of the unit processing cost value for every entity and the number of packets per request, K is the system dependent constant, R is the ration of the number of bits in the address to the machine word size in bits and N is the number of entries per table [10]. Figure 11 shows the effect of increasing the number of users on the processing time. The processing time will double for a 10 times increase in the number of users N.

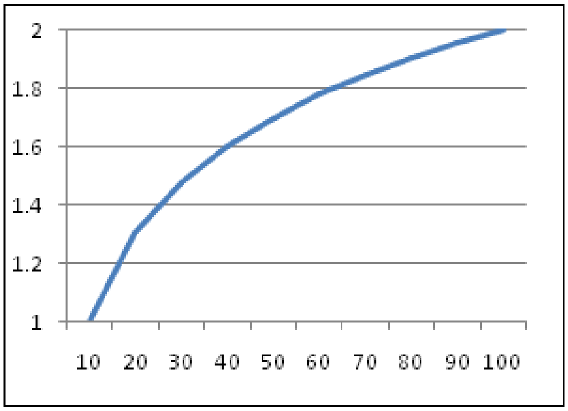

Figure 11. Processing time (sec) Vs Number of users

The waiting time depends on the integer coefficients which show that not only the arrival rate will affect the waiting time but also the number of the SIP exchanged messages processed at each node. Thus to minimize the registration delay, the bottleneck is to reduce the waiting time at each node which is in turn affected by the arrival rata. An increased arrival rate will result in an increase in the queue size and increase in the queuing time. On the other hand, the reduction of the SIP messages could result in less waiting time. Similarly, for the setup delay, the waiting time will increase with the increased arrival rate but will be mainly affected by the coefficient corresponding to the number of messages exchanged at each IMS node. Thus the waiting time is higher due to the higher number of messages involved in the setup delay. In addition, an increase in the arrival rate will affect more the setup time as compared to the registration time. Thus the total delay is highly affected by the setup delay rather than the registration delay as per figure 12. Thus the total signaling delay is due to the setup delay.

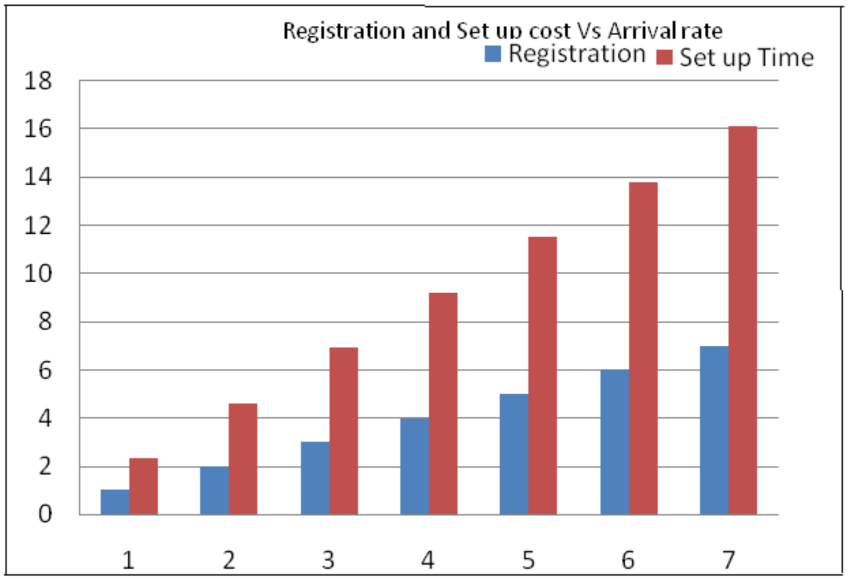

Figure 12. Registration and set up queuing cost versus arrival rate

9. SECURITY VIOLATIONS

For both registration and setup delay as calculated in the cascaded queuing model, we will study first the delay conditions at the system entry P-SCSCF and at the AS EXAM that may indicate a possible security violation. As per figure 13, we will consider security violation at the main entry point P-CSCF of the IMS queuing system. The I-CSCF and S-CSCF nodes will not be considered in this study since they will simply forward the messages from the P-CSCF to the AS exam server. At the end of the queue, the AS will be considered as another possible point possible security violations where delay should be evaluated in order to study the server performance.

At the P-CSCSF node we will consider the following measures: First the number of accepted registration should be controlled. When the number of students is known, the registration requests number could be limited. When denial of service is launched, more registration requests will be initiated toward the P-CSCF thus security violation could be recorded. Thus the probability of keeping the number of accepted registration less than the number of students n should be highly tracked.

Second, the time required to access the P-CSCF is critical since more time means possible violation of user account which results in more processing at P-CSCF node and more waiting time for the registration request in the P-CSCF system (buffer+ server).

Accepted registration: The maximum number of users in the system should be less than a number n after which no more users will be accepted in the system.

When a denial of service occurs, a number of registration requests may flood the system. Due to the PCSCF being over flowed, the number of users in the system should be less than a number n. Thus in order to ensure all the registration will be accepted, we need to calculate:

$$\text{P (number of registration requests in system} \leq \text{n)} = 1 - \rho\, n + 1 \qquad (5)$$

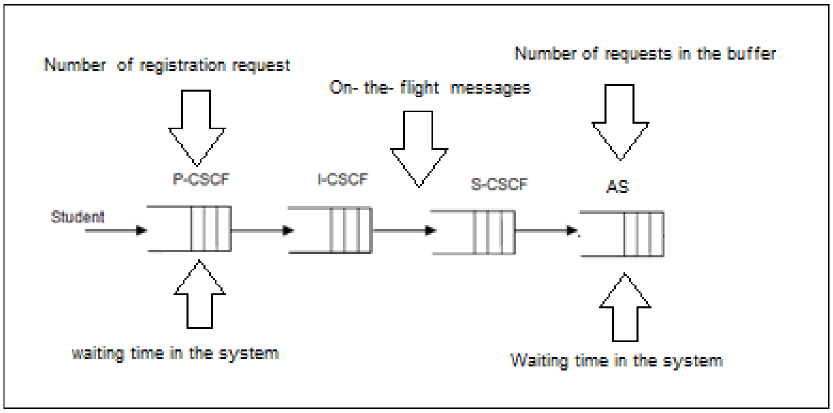
Number of registration request
On- the- flight messages
Number of requests in the buffer
P-CSCF
I-CSCF
S-CSCF
AS
Student
waiting time in the system
Waiting time in the system

Figure 13. Delay measures at security violations points

Where ρ is the system utilization given by equation (6) as:

$$\rho = \text{Arrival rate/Service rate} \quad (6)$$

Thus the probability that the number of registration requests exceeds a threshold n after which the calls will be denied is:

Probability (Overflow)=1 - P(number of registration requests in system $\leq n = \rho^{n+1}$) (7)

Figure 14 shows that, for a given n, the overflow probability will increase with increased ρ (varying from 0.1 to 0.9). Thus, higher utilization means busy server, less probability of being within the accepted number of registrations, more probability to exceed the threshold. Thus when ρ exceeds 0.75, the overflow probability will increase indicating a server being busy starting to reject student's registrations.

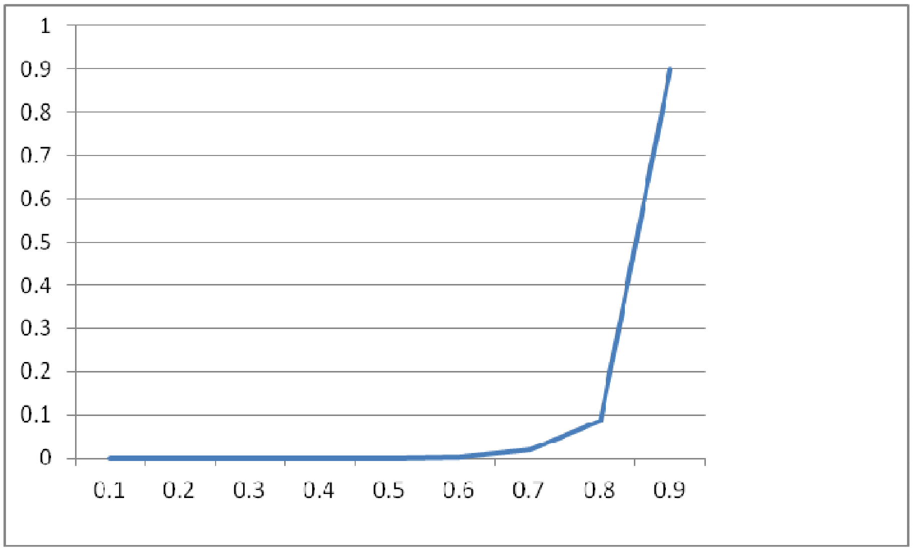

Figure 14. P-CSCSF node Overflow Probability Vs ρ

For the time required to access the P-CSCF node, the time spent in the system is to be controlled. Based on the following:

Waiting time in the system (T_q) = Waiting time buffer+ Waiting time server

The probability of the waiting time should be kept less than a threshold T where T corresponds to maximum waiting time for registration requests at the P-CSCG node, when this threshold is exceeded, the probability of the server being busy is higher which will contribute in more waiting time thus the probability of a possible security violation is exceeded when the threshold is not maintained.

$$\text{Probability (waiting time in the system} < t) = 1 - \exp(-t/Tq) \quad (8)$$

Where t is chosen to be less than a threshold T considering that a security attack would result in higher waiting time. Thus “t” is simply the value below the threshold corresponding to normal conditions of processing (waiting time) of the P-CSCF with no proxy overflow.

If t is exceeded, this means that server processing time is higher and a possible attack (student account violation, for example) has been encountered. Figures 15 and 16 show the probability of the waiting time in function of t for a low value of ρ (0.1) and high value of ρ (0.9) respectively. With increasing t, the waiting time will increase. Higher probability of exceeding T is in case ρ is high where the probability to be less than t is low and accordingly the system may be under attack. On the other hand, low ρ, the system will encounter less waiting time thus higher probability to stay within the threshold hence lower probability for the system to be overflowed or vulnerable to risks.

Exam AS: On the AS, we need to control number of registration requests in the buffer since after the buffer stage, requests will be served at the AS. So in order not to overflow the AS and before the server is overflowed, the number of registration requests in the buffer should be controlled. Thus the probability of the number of registration requests in the buffer should be kept less than n where n is the number of students as per the following equation:

$$\text{Probability (number of registration requests in buffer} \leq n) = 1 - \rho\, n + 2 \quad (9)$$

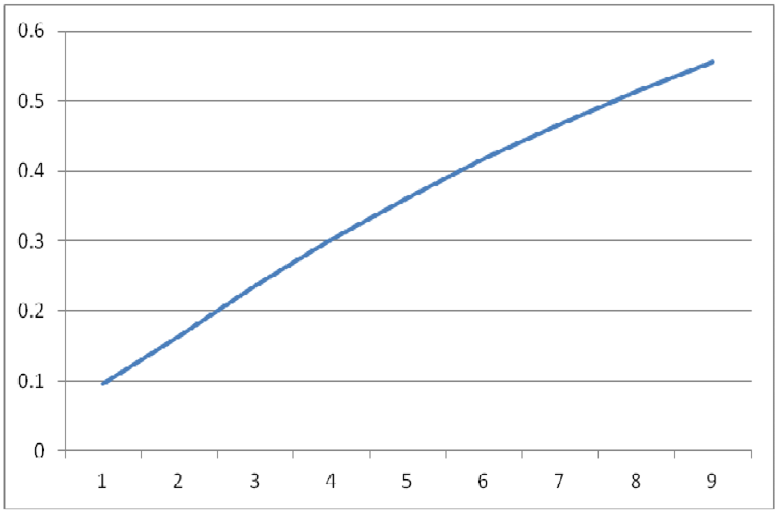

Figure 15. Waiting Probability Vs t with low ρ

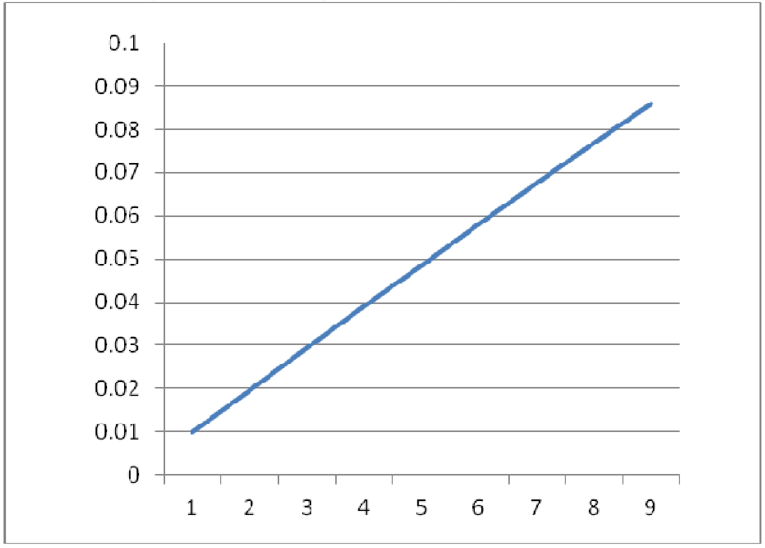

Figure 16. Waiting Probability Vs t with high ρ

Thus the probability of exceeding the number n of registration requests is ρ^{n+2}as per the P-CSCSF analysis, the overflow probability is increased with increasing n. Thus n should be kept less than the threshold that may overflow the server and cause the AS not to respond to the student's requests. In this context, exceeding the threshold will occur at higher system utilization ρ. Thus when kept at a low level the system should not suffer from any delay. In addition the AS server should not reject any registration or set up request due to server overflow. In addition, as per the P-CSCF delay limitations, the total time spent in the system (AS) should be less than a threshold t otherwise more security measures should be taken (possibility of security attacks). The time spent in the system (buffer + server) should be less than the normal condition time t. Thus probability (waiting time in the system ≤ t) will give the same results as per P-CSCF node. Table 2 summarizes the delays effects and related management based on the specified sources.

Table 2. Delay effects and management

Source of latency	Latency effect	Latency management
Propagation	Negligible at the node level	Shorter distance between the nodes
Transmission	Negligible at the access network level	Faster access networks
Queuing	Waiting time for both registration and set up	Accept invitation up to threshold n Registration waiting time do not exceed T
Increased waiting time	AS overflow or P-CSCF Overflow	Check for possible violations.
Increased service time	System may start to reject new requests	Check for possible violations before no more requests could be accepted.

10. CONCLUSIONS

In this paper we have analyzed different security threats for IP Multimedia Subsystem architecture. A detailed analysis of security threats is presented and proposed a solution for the security of Mobile Exam Application by deploying the firewall and Application Level Gateway. The proposed solution can better secure the IMS infrastructure by providing the security in two folds first firewall can filter the malicious traffic on network and transport layer and later ALG can help in mitigating the application layer attacks. In addition, a delay analysis was conducted to study the system performance and eliminate the possible security vulnerabilities based on the type of latency and the possible source of delay. Results showed that the security violations could be avoided by limiting the number of accepted registrations that the system will process and defining the maximum waiting time that a request could take based on the current number of students and related waiting time under normal system conditions.

ACKNOWLEDGEMENTS

The authors would like to thank King Abdulaziz City for Science and Technology (KACST), Saudi Arabia for funding this ongoing research project number 29-324.

REFERENCES

[1] Thoren, " Rethinking mobile communication: It's not about bit speed", Feb. 2007 (http://www.ericsson.com/ericsson/corpinfo/publications/ericsson_business_review/pdf/207/not_about_speed.pdf)

[2] Dirk Pesch, Maria Isabel Pous, Gerry Foster, "Performance evaluation of SIP-based multimedia services in UMTS", Computer Networks, Volume 49, Issue 3, 19 October 2005, Pages 385-403

[3] Barnawi, "Deploying SIP-based Mobile Exam Application onto Next Generation Network testbed", Electronics, Communications and Photonics Conference (SIECPC), 2011 Saudi International, 16 June 2011.

[4] Hunter, "Security Issues with the IP Multimedia Subsystem (IMS)", Version 1.0, September 1, 2007.

[5] Mark, "VOIP Vulnerabilities – Registration Hijacking" Secure Logix Corporation, 01 June 2005.

[6] Mark, “Basic Vulnerability Issues for SIP Security” Secure Logix Corporation, 01 March 2005.

[7] Geneiatakis, “Survey of Security Vulnerabilities Session Initiation Protocol”, IEEE Communications Survey & Tutorials, Volume 8, No.3, 3rd Quarter 2006.

[8] http://en.wikipedia.org/wiki/Application_Layer_Gateway accessed on 24th December 2011.

[9] Keith Drage, SIP and the application of SIP as used in 3GPP, Lucent Technologies.

[10] W.Jianhui, J.Hao, Wu Wenguang, “A novel queuing model for IMS- based IPTV system”, IC-BNMT2009.

[11] J. Medhi, Stochastic Models in Queueing Theory. Academic Press, 2003.

[12] N.Psimogiannos, A.ggeliki, D.Vergados,”An IMS-based network architecture for WiMAX-UMTS and WiMAX-WLAN interworking”, Conputer Communications, 2010.

Authors

Dr. Ahmed Barnawi received his BSc in Electrical Engineering from King Abdul-Aziz University in 2000, his degree in Communication Engineering from University of Manchester Institute of Science and Technology (UMIST) in 2002, and his PhD degree in Mobile Communications from Bradford University in 2006. Currently, Dr. Barnawi is an Assistant Professor at the Department of Computer Science, King Abdul-Aziz University, Jeddah, Saudi Arabia. His current research interests include Mobile Next Generation Network, Cognitive Radio and Wireless Ad hoc and Sensor Networks.

Dr. Abdulrahman Altalhi is an assistant professor of Information Technology at King Abdul-Aziz University. He has obtained his Ph.D. in Engineering and Applied Sciences (Computer Science) from the University of New Orleans on May of 2004. He served as the chairman of the IT department for two years (2007-2008). Currently, he is the Vice Dean of the College of Computing and Information Technology. His research interest include: Wireless Networks, Software Engineering, and Computing Education.

Dr. Nadine Akkari received his BSc and Msc in computer engineering from University of balamand, Lebanon in 1999 and a diploma in specialized study in telecommunications networks from Engineering School of Beirut, Saint Joseph University, Lebanon in 2001. She received her PhD degree in Mobility and QoS Management in next generation networks in 2006 from National Superior School of telecommunications (ENST), Paris, France. Currently, Dr. Akkari is an Assistant Professor at the Department of Computer Science, King Abdulaziz University, Jeddah, Saudi Arabia. Her current research interests include Next Generation Networks, mobility management and Cognitive Radio.

Muhammad Emran is working as Lecturer in Computer Science Department of King Abdul Aziz University, Jeddah, Saudi Arabia. He has completed Master in Computer Science from Quaid-i-Azam University, Islamabad Pakistan in 1997. Then he completed his MS (CS) with specialization in Computer Networks from COMSATS Institute of Information Technology, Lahore Pakistan in 2006. His research interests are in IP Multimedia Subsystem, Wireless and Mobile Computing and Network Security.