Master Thesis
Computer Science
Thesis no: MCS-2009:24
May 22nd 2009

Architecture for IMS Security to Mobile: Focusing on Artificial Immune System and Mobile Agents Integration

Author: Kalyani Chalamalsetty

School of Computing
Blekinge Institute of Technology
Soft Center
SE-37225 RONNEBY
SWEDEN

This thesis is submitted to the Department of Software Engineering and Computer Science, School of Engineering at Blekinge Institute of Technology in partial fulfillment of the requirements for the degree of Master of Science in Computer Science. The thesis is equivalent to 20 weeks of full time studies.

Contact Information:
Author(s):
Kalyani Chalamalasetty
E-mail: kaca07@student.bth.se
Department of Software Engineering and Computer Science

University advisor(s):
Dr. Bengt CarlssonAssociate professor
Email: Bengt.Carlsson@bth.se
Department of Software Engineering and Computer Science

Dr. Guohua Bai
Assistant professor
Email: Guohua.bai@ipd.bth.se
Department of Interaction and System Design

School of Computing
Blekinge Institute of Technology
Soft Center
SE-37225 RONNEBY
SWEDEN

- REGISTER request sent from User Equipment to P-CSCF.
- P-CSCF transfers REGISTER request to analyzer agent to verify for SQL injection.
- If SQL injection found, REGISTER request will be denied.
- If analysis agent found no SQL injection, then request sent to monitor agent.
- Monitor agent checks for CPU load and if load is normal, monitor agent will send the reply as normal.
- Under this normal load condition, analyzer agent forward REGISTER request to database agent
- If UE is existing, it will send back a message existing UE.

3.9.2 INVITE flooding attack design scenario

The design scenario of INVITE flooding attack is as follows and is shown in *figure 16*

- Initially INVITE request is sent by UE to P-CSCF.
- P-CSCF forward INVITE request to analyzer agent for SQL injection checking.
- If it contains SQL injection, INVITE request denied.
- If it contains no SQL injection, then request sent to monitor agent and INVITE flooding is verified by checking CPU load.
- If load is normal, it will be informed to analyzer agent.
- Analyzer agent will then forward INVITE secure and the request will enter IMS core.
- If load exceeded the CPU limit, the system is under attack.
- INVITE request rejected.

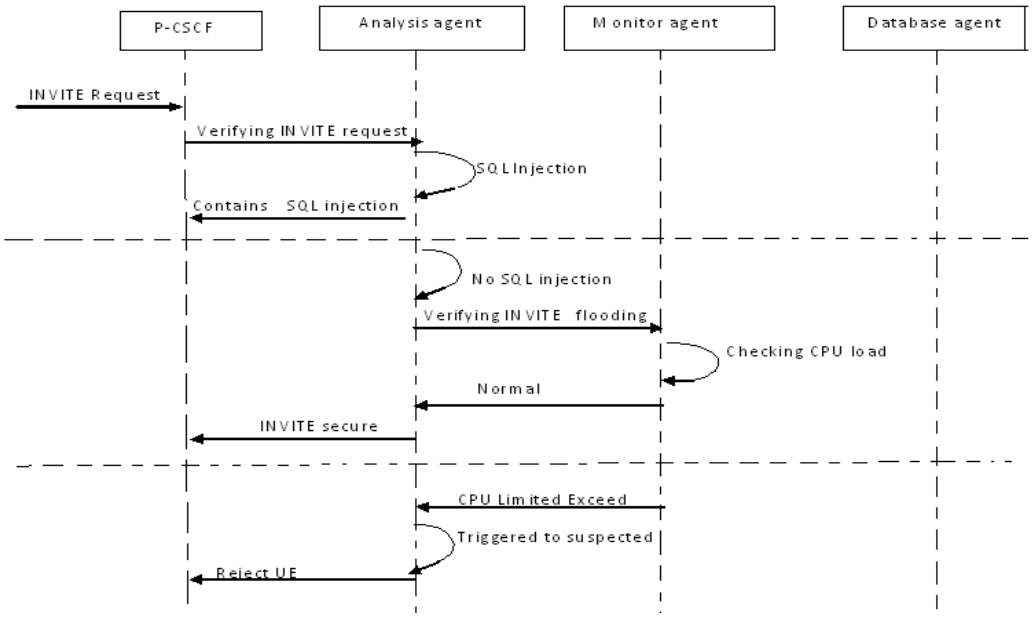

Figure 16: INVITE flooding attack design scenario

4 ARCHITECTURE EVALUATION

Architecture evaluation tells us the important properties of the system. By analyzing architecture well, one can find important interesting properties of the system. These important properties can be known before the existence of system in real. But some of the architecture properties could be evaluated only after building architecture in practice. Architects make design decisions because of the effects they will have on the systems they are building in the direction of current process of stream, and these effects are known and predictable. Architectural techniques and patterns bring known properties to the systems in which they are used. Hence, the design choices of architectures are analyzable. Assessing the architecture with an effective technique before it becomes accepted blueprint of project is very helpful in economic point of view. ATAM (Architecture Tradeoff Analysis Method) is a repeatable, structured method of architecture evaluation that can provide relatively a low-cost risk mitigation capability. The main reason behind choosing ATAM for architecture evaluation is that ATAM is appropriate when we evaluate architecture based on business goals, quality attributes and functional requirements. The IMS security architecture for mobile has its own business goals, constraints, quality attributes and functional requirements which is exactly suitable to be evaluated by ATAM. By using ATAM, the evaluation team confirms whether the proposed architecture is the right one or not. Another reason behind choosing ATAM is to verify the correctness of his architecture.

4.1 Benefits of Evaluating with ATAM

Software architecture is "the structure of the components of a program/system, their interrelationships, a principles and guidelines governing their design and evolution over time."[50]. The main benefit of using ATAM is to check whether the architecture reaches the user expectations i.e. it serves as a blueprint of the system. Using this, problem can be found in the initial stages so it is easy to correct and maintenance will become easier from economic point of view. ATAM is easy way to discover tradeoffs and sensitivity points. Using ATAM evaluation, one can document all the justifications for key architectural decisions. The communication among stakeholders is increased after ATAM evaluation.

4.2 About ATAM

ATAM (Architecture Tradeoff Analysis Method) describes how different architecture attributes interact to analyze the architecture. Its main purpose is to assess the consequences of architectural decisions based on quality attribute requirements. In fact it is not used to achieve quality but mainly to find the risks in advance. The main result of this ATAM is improved architecture. Other outputs includes a concise presentation of the architecture, articulation of the business goals, quality requirements in terms of a collection of scenarios, mapping of architectural decisions to quality requirements, a set of identified sensitivity and tradeoff points, a set of risks and non-risks and a set of risk themes. Other benefits include good documentation of architecture, reasoning for architectural decisions and quality attributes where requirements get clarified.

4.3 Architectural Evaluation using ATAM

The ATAM evaluation consists phase 0 to phase 2. In phase 0 preparations for evaluation is done i.e. selecting participants and plan logistics. In phase 0 the evaluation team with outside experts, project decision makers including project manager, architect, and customer and architecture stakeholders are formed [50]. The author has formed evaluation team of two cellular operators who constitute the first category, two retailers as second category and 2 users as third. The cellular operators chosen were experts in testing telecommunications like mobile applications, mobile embedded applications, customer care software, and wireless network protocols. The evaluation team is given with concise presentation of architecture. The architecture is clearly explained to evaluation team as described in section 3.

Now evaluation team continues with phase 1 and phase 2

Evaluation: Phase 1

STEP1-Present the ATAM:

It is important to clearly state what ATAM is [50] to the evaluation team. Here the assembled evaluation team is provided ATAM in detail. This way they know what the goals are. The outputs of evaluation are to confirm correctness of proposed architecture, to validate the architecture by analyzing quality attributes.

STEP2-Present the business drivers:

The business goals that motivated the development effort and primary architectural drivers, functional requirements, technical constraints, important stakeholders, the important quality attributes are presented [51]. Here the following *table 4* shows the output step 2.

Serial No.	Business Drives	In Project
1	Functional requirements	➢ Providing AIS based Security to mobile UE ➢ Securing the IMS core components using light weight mobile agents ➢ Securing SIP signal
2	Technical Constraints	➢ Architecture should be embedded into P-CSCF ➢ All incoming requests should be deviated into the proposed architecture without sending directly into IMS core
3	Major stakeholders	➢ Network operators ➢ System developers ➢ End users
4	Business Goals	➢ Ensuring network performance and integrity ➢ Flexible IMS security deployment
5	Architectural drives	➢ Distributability of the architecture ➢ Scalability ➢ Performance

		➢ Availability ➢ Interoperability ➢ Usability ➢ Maintainability

Table 4: Presenting business drivers for the proposed architecture

Among the architectural drives performance, scalability, interoperability are identified as high priority. Distributability, maintainability, availability, usability are also identified, but of lower priority because cellular system itself consists of these quality attributes and they are also being used in the proposed architecture.

STEP3- Present architecture:

The architect will describe the proposed architecture, focusing on how it addresses the business drivers [51].

- The analyzer agent is the brain of proposed architecture. It performs analysis and takes decision to protect IMS core against flooding and fuzzing attacks. The analysis procedure detects the reason of overloading and decides to stop further communication from illegitimate around defined time interval. The attacks detection algorithm identifies the reasons of overloading of IMS resources.
- The primary functionality of proposed architecture is to detect and protect the DoS/DDoS flooding attacks launched against IP Multimedia Subsystem (IMS) core network.
- The proposed architecture also detects and drops SQL injection attack during UE (User Equipment) and P-CSCF starts authentication procedure without effecting P-CSCF message procedure under normal load.
- The proposed architecture is based on AIS by using mobile agents.
- Proposed architecture mainly focuses security of mobiles.

There will be different questions posed by the evaluators regarding the inconsistencies and functioning of various modules for better understanding of architecture from architect's information notation. With layered view in *figure 13* and data flow architectural view in *figure 11*, the inconsistencies and quality attributes can be drawn to carry out analysis steps of ATAM.

Step 4- Catalog Architectural Approaches:

The evaluators bring out architectural approaches after pre-evaluation review of the submitted documentation based on their understanding [51]. The approaches that evaluation team observed are listed out after reviewing the proposed architecture document and are presented below in *table 5*

Layering	It enhances the system in layered structure as the controls follow in a layered format that achieving the ease of system modification. Thus, the system could grow or respond to changes easily by

	adding/removing a layer/component. Also, it helps to integrate the system with other existing systems. This not only shortens the time, but also helps in easy the modification work of system maintainers.
Client-Server Transaction processing	In proposed architecture with various agents embedded in it, analyzer agent interacts with database agent, monitor agent, killer agent and detection agent to detect and prevent attacks on IMS core. Client-server transaction processing is completely taken care by the architecture which is done by analysis agent by simple requests to other existing agents.
Optimized database	Anomaly based detection is used. A major advantage is it detects unknown attacks. Here all the information regarding existing user is stored and can be retrieved when needed.

Table 5: Description of architectural approaches in proposed architecture

Step 5- Generate quality attribute utility tree

A table containing utility tree will be generated in step 5 and is shown in *table 6*. Scenarios were drawn for each quality attribute that can explain inconsistencies clearly. In some situations there may not be refinements that can clearly explain inconsistencies used. This may be due to fact that mobile customers are sometimes able to think of reasonable refinement for quality attribute, but when pressed to initiate it in context of their own system, discover that it doesn't apply really [51].

The scenarios at the leaves of the utility tree are prioritized along two dimensions:

1. Importance to the system.
2. Perceived risk in achieving the particular goal.

The scenario priorities then drive the further analysis. These nodes are prioritized relative to each other using ranking pairs of High, Medium, and Low (H, M, and L), where the first value in the pair indicates the degree of importance to the system and the second indicates the degree of difficulty for the architecture to achieve it.

Not all the attribute concerns are filled in with elaborating scenarios. This is normal and reflects the fact that sometimes stakeholders can think of a broad description of a quality attribute but not a specific requirement for it.

I=Importance level

D=Difficulty to achieve

H, M, L = High, Medium, Low

Quality attribute	**Attribute Refinement**	**Scenarios**	**(I, D)**
Performance	Throughput	When there are more transaction requests simultaneously generated, the system should be able to handle them	(H,L)

		without any problem.	
	Synchronization	Synchronization has been achieved by architecture performing real-time monitoring in accordance with the needs and preferences of IMS network.	(H,L)
	Response time	Response time depends on quality of technique used. However the response time is less as different agents interact and reduce the response time.	(H, L)
	Accuracy of result	Accuracy of result is achieved by effective co-ordination of various mobile agents.	(H, M)
	Data base management	Database entities are used efficiently where necessary and part of data is retrieved upon request without searching for unnecessary data entities	(H,M)
Scalability	Problem growing	This is maintained by tactics that are used to implement SQL injection, REGISER flooding and INVITE flooding techniques used as problem size grows.	(H,L)
	Cost effectiveness	Low signaling cost of authentication for legitimate user.	(H,M)
Inter operability	Managing different service providers	Architecture similar for all service providers or cellular operators. Using security architecture and improving integration aspects are up to service providers. The research may change components responsibilities as the profit from this service increases.	(H,L)
Distributability	Integrity	Cellular centric operations are available and unauthorized controllers are restricted by architecture in case of sending SMS or voice calls. Operator has ability to control all events.	(M,L)
	Distributable	The various mobile agents interact locally to provide global protection. There is no single point of failure.	(H,H)
		Control access to the system before connection established.	(L,M)
Usability	Proficiency in using service.	Service is used by the subscriber who request services from IMS.	(M, H)
	Normal operations	Operations at UI are normal and can be controlled by subscribers themselves just like they usually navigate.	(L,H)
Maintainability	Database	Changes in the database can be controlled by analyzer agent (adding previously seen invader).	(M,L)
	Hotspots	New hotspots are identified by architecture detection algorithm and added to database.	(M,M)

Availability		The given architecture supports 24/7 access to mobile.	(M,L)

Table 6: Tabular form of utility tree for proposed architecture ATAM evaluation

Response time depends on attack detection methodology. It is as below.

The response time for each request under normal load.

Response time= service request time + processing time+ result response delivery time.

Else the response time for each request under over load

Response time= service request time+ processing time+ extra time + result response delivery time.

Where service request time =time taken to send request from UE to proposed architecture.

Request response time=time taken to receive reply from proposed architecture.

Therefore service request time = request response time= half of call establishment time (assumed), which implies that

Service request time + request response time= half of call establishment time

Step 6-Analyze Architectural Approaches:

Based upon the high-priority factors identified in Step 5, the architectural approaches that address those factors are elicited and analyzed. The utility tree produced scenarios are ranked according to evaluation team analysis and are presented in *table 7*. We can see the pairs (H, H), (H, M), (H, L) (M, H), (M, M), (M, L), (L, H) and (L, M) with the specified scenarios of utility tree in *table 6*. The ranking pair (L, L) is omitted by evaluation team since there is no use in considering least important scenarios. Risks and non-risks are identified by evaluation team. The scenarios with high importance and more difficult or medium difficult to achieve are termed as risks i.e. (H, H) and (H, M). High importance and with low or medium difficulty to achieve were termed as non risks. There were tradeoffs identified as cost effectiveness, interoperability, integrity, distributability and availability. Therefore 8 risks, 8 non risks and 5 tradeoffs identified by evaluations team. The evaluation phase 1 ends here and evaluators proceed to phase 2.

Evaluation phase 2

Step 7-Brainstrom and prioritize scenarios:

The phase 2 starts here and evaluation team interact with architect in telephone to check their understanding of some technical points. The stakeholders were productive group and contributed some scenarios during this step. Since it is difficult to accumulate all the scenarios by stakeholders with the proposed architecture until it is implemented, the scenarios analyzed by the evaluation team are prioritized and presented in a table 7 form.

Priority	Scenario	Satisfied ?(YES/NO)
1	Synchronization has been achieved by architecture performing real-time monitoring in accordance with the needs and preferences of IMS network.	YES
2	When there are more transaction requests simultaneously generated, the	YES

	system should be able to handle that without any problem	
3	Response time depends on quality of technique used. However the response time is less as different agents interact and reduce the response time	YES
4	database entities are used efficiently where necessary and part of data is retrieved upon request without searching for unnecessary data entities.	YES
5	Architecture similar for all service providers or cellular operators. Using security architecture and improving integration aspects are up to service providers. The research may change components responsibilities as the profit from this service increases.	YES
6	Low signaling cost of authentication for legitimate user.	YES
7	Scalability is maintained by tactics that are used to implement SQL injection, REGISER flooding and INVITE flooding techniques used as problem size grows.	YES
8	Accuracy of result is achieved by effective co-ordination of various mobile agents.	YES
9	Cellular centric operations are available and unauthorized controllers are restricted by architecture in case of sending SMS or voice calls. Operator has ability to control all events	NO
10	The various mobile agents interact locally to provide global protection. There is no single point of failure.	YES
11	Service is used by the subscriber who request services from IMS	YES
12	Changes in the database can be controlled by analysis agent (adding previously seen invader).	YES
13	New hotspots are identified by architecture detection algorithm and added to database.	NO
14	Operations at UI are normal and can be controlled by subscribers themselves just like they usually navigate.	YES
15	The given architecture supports 24/7 access to mobile.	YES
16	Control access to the system before connection is established.	NO

Table 7: Brainstormed scenarios presented by evaluation team

Step 8- Analyze architectural patterns:

Table7 above shows 8 out of 8 risks found in step 6 were satisfied by the proposed architecture. There were few scenarios not satisfied by the proposed architecture. Even though, some non-risks are not satisfied as mentioned by evaluation team in above table, cellular system architecture inherently has ability to satisfy those scenarios. Therefore those scenarios were not taken into consideration. The

architecture is considered as consistent as most of the risks have been satisfied by the proposed architecture.

4.4 Results

We found the ATAM a useful method for assessing software architecture against known quality criteria established by the stakeholders. Evaluation of proposed architecture has been applied to confirm the correctness of proposed architecture and validate it by analyzing its quality attributes. The author has formed evaluation team of two cellular operators who constitute the first category, two retailers as second category and two users as third. The cellular operators chosen were experts in testing telecommunications like mobile applications, mobile embedded applications, customer care software, and wireless network protocols. The quality attributes that have been identified from the layered view of proposed architecture (*figure 12*) and data flow view are distributability, scalability, performance, availability, interoperability, usability, maintainability. Utility tree has been generated and evaluation team ranked and checked for the validity with the existing architecture. The scenarios are ranked based on two criteria and they have been shown in *table7*. The evaluation team found 8 risks, 8 non-risks and 5 tradeoffs in step 6 satisfied by the proposed architecture. 8 out of 8 identified in step 6 have been satisfied by proposed architecture according to ATAM which confirms consistency of the architecture. Mobile agents carry security policy in a fast and cost-effective way so the proposed architecture is thus cost effective.

5 DISCUSSION

IP Multimedia Subsystem (IMS) is an architectural framework for delivering Internet Protocol multimedia services [53].This 3GPP architecture integrates the IP network services with 3G devices such as 3G cellular phone. For this integration IMS uses IETF protocols like SIP (Session Initiation Protocol)[52]. Due to this reason it has advantages of IPV6 support, support for instant messaging, different event packages, and IPSec. At the same time it has the disadvantages of threats (which an SIP based communication like VOIP had)[54]. Unfortunately, the security mechanisms proposed by 3GPP are not enough to protect the IMS networks from flooding attacks. These flooding attacks lead to downfall of IMS resources and network services. Flood DoS and DDoS attacks cause a malicious user send tremendously large amount of random messages to core network elements from either a single location (DoS) or from multiple locations (DDoS)[55]. IMS security challenges and threats were discussed in section 2.

The IMS client needs to establish association with P-CSCF for communication. The emerging standard for third generation (3G) wireless communications, has adopted, is an enhanced Authentication and key Agreement (AKA) protocol resulted from the Third-Generation Partnership Project (3GPP)[56]. The AKA is used for authentication between UE and P-CSCF. The 3GPP/IMS authentication and key agreement protocol has been reported and claimed to be secure. But [46] demonstrate that 3GPP AKA is vulnerable to a variant of false base station attack.

The standard architectural frameworks could not prevent application layer attacks like SIP message flooding, SIP message flow, and fuzzing and SQL injection. The major contribution of my thesis is IMS security extension by providing solution for the threats and vulnerabilities which are not addressed by standard architectural frameworks. This research work incorporates the ideas of immune system and multiagent architecture. In this thesis security architecture is proposed based on immune system framework that is capable of detecting and identifying an attack, and recovering from an attack. Simulating biological immune system, author placed certain amount of immune cells[57] (viz .,mobile agents) into the networks . These mobile agents host on the network provide forensic analysis on the network. The proposed security model based on immune system is capable of detecting, identifying an attack and recovering from an attack. In addition, it has same learning and adaptive capability of human immune system, so it is able to react to unknown attacks. To protect the IMS core from identified attacks as mentioned in section 2.3 and 3.2 all the incoming and out going messages should pass through proposed architecture. Section 3 concentrated on securing IMS core components from SQL injection, REGISTER and INVITE flooding attacks.

The current security architecture is been conceptually evaluated by the evaluation team using ATAM which is a theoretical technique. The proposed architecture investigates attacks in two levels based on CPU load conditions. In the first level i.e. CPU under normal load all requests were investigated to detect and prevent SQL injection. Second level considers Denial of Service (DOS) attacks when CPU load exceeds threshold limit. The request or message is blocked if it matches the defined attacks. The evaluation team found 8 risks, 8 non risks and 5 tradeoffs were in step 6 satisfied by the proposed

architecture. 8 out of 8 identified in step 6 of evaluation have been satisfied by proposed architecture according to ATAM which confirms consistency of the architecture.

6 CONCLUSIONS AND FUTURE WORK

In this article the author identified and categorized various types of SIP-oriented threats, including flooding attacks, security vulnerabilities and attacks exploiting vulnerabilities on the signaling-application level. It is stressed that, no matter how strong the existing security prevention mechanisms employed in current SIP-based VoIP services are, there is always the possibility for a malicious user to manage to bypass them. The author focused to protect network resources and applications from the potential attacks causing downfall of next generation multimedia services. The author designed security mechanism against these attacks.

In this part author accumulates answers to research questions mentioned under section 1.2. Finally the author concludes section by explaining unaddressed research gaps in present thesis as future work.

6.1 Addressing research questions and Objectives

RQ (1): WHAT ARE THE BASIC SECURITY REQUIREMENTS IN IMS SIP APPLICATION?

The open architecture of the Internet and the use of open standards like Session Initiation Protocol (SIP) constitute provisioning of services (e.g., Internet telephony, instant messaging, presence, etc.) vulnerable to known internet attacks, while at the same time introducing new security problems based on these standards that cannot been tackled with current security mechanisms. Those security attacks include DoS/DDoS flooding attacks launched against IP Multimedia Subsystem (IMS) core network. The identified problem areas need to be resolved rather quickly for IMS. These attacks are resolved in the proposed architecture. My architecture main focus is on SIP message flooding, SIP message flow, and fuzzing and SQL injection.

RQ (2): HOW CAN THE EXISTING SECURITY BE IMPROVED

The development of new services for the establishment of multimedia sessions over internet requires security enhancements to secure data flowing against internal and external threats like eavesdropping and interception, man-in- middle attacks , DoS and SQL injection. These type of harmful attacks take place either during signaling phase or during transmission of media packets (e.g. ., voice). Therefore both the signaling and media packets transmission demand certain security mechanisms utilization.

Despite the diverse security mechanisms that have been proposed for SIP-based infrastructures [26], there are still vulnerabilities that affect this architecture with an intension of consuming the network resources like memory, CPU performance [27], thus preventing legitimate IMS users from receiving services with some minimal performance. Unfortunately, the security mechanisms proposed by 3GPP are not enough to protect the IMS networks from flooding attacks [28]. The low level attacks could be prevented by using low level mechanisms like encryption in Transport Layer Security (TLS) and to IP Security (IPSec). The task of proposed architecture is to detect and block SQL injection, DoS at application level.

The objective of architecture is to protect IMS application server and to secure SIP signaling. The proposed architecture is based on open core IMS and is integrated within P-CSCF. It is placed in between IMS client and IMS core as shown in *figure 12*. To protect the IMS core from identified

attacks as mentioned in section 2.3 and 3.2 all user requests were bypassed into proposed architecture before entering IMS core.

RQ (3): WHAT ARE THE ADVANTAGES WITH THE PROPOSED ARCHITECTURE?

The author identified various SIP-oriented security threats, including flooding attacks, and vulnerabilities on signaling application level. Moreover, these types of attacks can also exist in other signaling like diameter; H.248 and so on (refer section 2 for more details on these protocols). It is stressed that, no matter how strong the existing security mechanisms employed in current SIP-based VoIP services are, there is always the possibility for a malicious user to manage to bypass them. The detection, identification and recovery of these attacks substantially increase performance, availability, scalability, usability, availability, usability and maintenance security robustness of the offered VOIP service. Since the security is based on immune based mobile agents it is more comprehensive solution.

RQ (4): HOW AIS HELP TO FETCH THE RESULT?

Now in this thesis author proposed bio-inspired Artificial Immune System (AIS) named "Architecture for IMS Security to Mobile". This architecture is capable of detecting, identifying an attack and recovering from attack. All these activities are done by mobile agents. The author also illustrated the advantages of immune model over traditional models in section 2. An interesting reader can find more applications in [41]. The light weight AIS will provide integrated solution against all types of attacks on IMS with low computational complexity. The proposed architecture presented in *figure 13* and explained in section 3.5. The key objective is to control/secure access to the IMS network and to protect its core and the underlying infrastructure.

RQ (5): DOES THE PROPOSED ARCHITECTURE SATISFY ALL THE IDENTIFIED REQUIREMENTS OF IMS SIP?

The proposed architecture is designed by the author to satisfy all the identified requirements. The proposed architecture is evaluated using ATAM as mentioned in section 4 to check the identified requirements are satisfied or not. The Scenarios identified by the evaluation team are mentioned in utility tree in *table 6* in step5. The scenarios are ranked and checked against proposed architecture. A total of eight risks were found and all of them have been satisfied by the architecture which means that the architecture satisfies the requirements identified. The scenarios that have been drawn according to the requirements as well as quality attributes help us to check the ability of proposed architecture.

RQ (6): DOES THE PROPOSED ARCHITECTURE THEORETICALLY AND CONCEPTUALLY PROVE VIABLE FOR ITS IMPLEMENTATION?

Viability of the proposed architecture is tested by applying a popular and successful evaluation method called ATAM. This evaluation is held by the evaluation team and documented in section 4. The author formed an evaluation team of two cellular operators, two retailers and two users. The cellular operators chosen are experts in testing telecommunication areas like mobile applications, mobile embedded applications, customer care software, and wireless network protocols. The evaluation team is given with concise presentation of architecture by the author. The architecture is clearly explained as described in section 3. Evaluation has been exactly done according to the phases and steps in ATAM. Utility tree is

generated by evaluation against architectural requirements and analyzed during steps 6 through 8. The stakeholders were productive group and contributed some scenarios during evaluation. Since it is difficult to accumulate all the scenarios by stakeholders with the proposed architecture until it is implemented, the scenarios analyzed by the evaluation team were prioritized and presented in a *table 7*. This priority is based on decision of people who have relevant experience in testing mobile embedded applications, wireless protocols and mobile server applications. The results obtained and presented in section 4.4 confirm consistency of the architecture. Hence the architecture has conceptually proved its viability.

6.2 Future work

The proposed architecture satisfies all the identified requirements and can form an efficient solution for SQL injection, Denial of Service attacks and effective result set achievement. The memory agent is used to identify the attacker launching SIP message flooding. This approach is suitable for preventing DoS attacks. However there are certain limitations for the work like the memory agent(available memory may not be enough) may not be suitable for distributed DoS attacks due to increase of faked and spoofed address lists. The future enhancement could be to extend this component architecture with additional approach for protection against DDoS.

On the other hand the architecture is evaluated using ATAM which is totally a theoretical approach. The prototype implementation of the designed architecture would be considered as good future work. In future the author will try to implement designed architecture and evaluate if the architecture fulfils all the architectural drivers. Thus, this will facilitate to compare results of the present evaluation, with results of before implementation to results of after implementation. Therefore the consistency of proposed architecture can be checked and the resulting architecture would be more valuable. Additionally, finding more quality attributes from mobile applications and integrating these attributes with in the designed architecture would result in more efficient and effective architecture for IMS security. The future work is to extend this work to include different intelligent traffic features that would improve the performance of AIS in terms of detection accuracy. A case study would be more effective to find the remaining defects in the implemented architecture which helps in improving the architecture.

REFERENCES

[1] 3rd Generation Partnership Project, "IMS Security Framework", IETF RFC 3261, 2003.

[2] Rebecca Elisa CY Su, Victor Sc Shen, Yi-Hong Wang, "Introduction to IP Multimedia Subsystem (IMS) ", 3GPP Project, 2006.

[3] J. J.Rosenberg, H.Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Spark, M.Handley, and E. Schooler, "Session Initiation Protocol",June 2002, <http:www.ietf.org/rfc/rfc3261.txt>.

[4] M.Sher, F.Gouveia, T. Magedanz, "IP Multimedia Subsystem (IMS) for Emerging All-IP Networks", Encyclopedia of Internet Technologies and Applications" Pub. IGI Global, formerly Idea Group Inc. 701 East Choclate Avenue, Suite 100, Hershey, PA 17033-1240, USA, 2007.

[5] Chistian W.Dawson, The Essensce of computing projects: A students Guide, Prentice Hall, ISBN: 978-0131219725, september 1999, pages:12-13.

[6] Joshua S.Gans, Stephen P.King and Julian Wright , "Wireless Communications, , Handbook of Telecommunications Economics", university of Melbourne , volume 2, 2007.

[7] 3rd generation partnership project. TS 22.279: Combined Circuit Switched (CS) and IP Multimedia Subsystem (IMS) sessions – stage 1, release 7, 2005.

[8] UMTS Forum, http://www.umts-forum.org/

[9] 3GPP TS 23.221; 3rd Generation partnership project; Technical specification group services and system aspects; Architectural requirements.

[10] Rakesh Khandelwal, "The importance of standard IMS Architecture", TATA consultancy service limited, May 2007, http://www.iec.org/newsletter/may07_2/analyst_corner.pdf

[11] 3GPP. Access security in for IP-based services (release 7). Technical Report TS 33.203 V7.6.0, June 2007.

[12] 3GPP TS 24.229 IP Multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP).

[13] 3GPP TS 23.228 Technical Specification Group services and system aspects IP Multimedia subsystem.

[14] M. Poikselkae, G. Mayer, H. Khartabil, A. Niemi, *"*The IMS, IPMultimedia Concepts and Services in the Mobile Domain*",* 2nd Edition, John Willey & Sons Ltd, West Sussex, England, 2006.

[15] M. Poikselkae, G. Mayer, H. Khartabil, A. Niemi, *"The IMS, IP Multimedia Concepts and Services in the Mobile Domain*" , John Willey & Sons Ltd. West Sussex , ISBN 0-470-87133-X, , England, 2004

[16] http://www.openimscore.org/

[17] 3GPP TS 24.228 - 3rd Generation Partnership Project; Technical Specification Group Core Network; Signaling flows for the IP multimedia call control based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3 (Release 5)

[18] Gonzalo Camarlio, Miguel A. Garcia-Martin, The 3G IP Multimedia Subsystem (IMS): Merging the internet and cellular worlds, John Wiley & Sons, ISBN:0470018186, 2006.

[19] Dimitris geneiatakis, Tasos dagiuklas, Georgios kambourakis, Costas lambrinoudakis, and Stefanos gritzalis, "Survey of Security Vulnerabilities in Session Initiation Protocol", *IEEE Communications Surveys & Tutorials*, 2006,pages:68-81.

[20] P. Calhun, J. Loughney, E.Guttman, G.Zorn," RFC3588: Diameter Base Protocol", *International Journal of Internet Protocol Technology(portal.acm.org)*, volume 1, November 2005, pages:109-116

[21] Miikka Poikselka, Georg Mayer, Hisham Khartabil, Aki Niemi ,"IMS", 3rd Edition, John Wiley & Sons Ltd, ISBN 0470721960, 9780470721964, 2006.

[22] Ericsson - Introduction to IMS white paper, Revision A, 2007

[23] 3GPP TS 24.229 - 3rd Generation Partnership Project; Technical Specification Group Core Network; IP Multimedia Call Control Protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage3 (Release6)

[24] Dragos Vingarzan, Peter Weik, " IMS Signal over Current Wireless Networks", *IEEE explore communications magazine*, march 2007.

[25] Himanshoo Kumar Saxena, "Introduction to IMS-IP Multimedia Subsystem", http://www.requestfill.com/article/112_Introduction.pdf.

[26] J. Rosenberg et al., "Sip: Session Initiation Protocol," RFC 3261, June 2002.

[27] D. Sisalem et Al, "Denial of Service Attacks Targeting a SIP VoIP Infrastructure", *To appear in IEEE Networks Magazine: Securing Voice over IP*

[28] D. Geneiatakis, T. Dagiuklas, G. Kambourakis, C. Lambbrinoudakis, S. Gritizalis, S. Ehlert, D. Sisalem, "Survey of Security Vulnerabilities in SIP Protocol", IEEE Communication Surveys Volume 8, No.3 ISBN 1553-877X, 2006, ppages: 68-81.

[29] Sipera Systems, "Protecting IMS networks from attack", February 2007 http://www.sipera.com.

[30] Muhammad Sher, Thomas Magedanz, "Protecting IP Multimedia Subsystem (IMS) Service Delivery Platform from Time Independent Attacks", *IEEE computer society*, 2007.

[31] D. Geneiatakis, T. Dagiuklas, G. Kambourakis, C. Lambbrinoudakis, S. Gritizalis, S. Ehlert, D. Sisalem, "Survey of Security Vulnerabilities in SIP Protocol*", IEEE Communication Surveys Volume* 8, No.3 ISBN 1553-877X, 2006, pages: 68-81.

[32] M. Sher, S. Wu, T. Magedanz, "Security Threats and Solutions for Application Serverof IP Multimedia Subsystem (IMS-AS)", *IEEE/IST Workshop on Monitoring, Attack Detection and Mitigation.*

[33] Chi-Yuan Chen , Tin-Yu Wu, Yueh-Min Huang , Han-Chieh Chao, "An efficient end-to-end security mechanism for IP multimedia subsystem", *Computer Communications archive.* Volume 31 , Issue 18 ,December 2008, pages:68-81.

[34] Hayzelden and Bigham," Agents for Future Communication Systems", *Springer*; 1 edition , June 11, 1999, pages:68-81.

[35] A. Niemi, J. Arkko, V. Torvinen, "HTTP Digest Authentication Using AKA", IETF RFC 3310 , 2002.

[36] A.somayali, S.Hofmeyr. and S.forrest, Principles of computer immune system. *In proceedings of second new security paradigms workshop*, 1997, pages :75-82.

[37] D.Dasgupta. Immunity-based intrusion detection system: A general framework. *In the proceedings of the 22nd National Information Systems Security Conference (NISSC)*, 1999, pages:79-89.

[38] R.L.King , A.B. Lambert, S.H Russ, and D.S Reese,"The biological basis of the immune system as amodel for intelligent agents". *Second workshop on Bio-Inspired Solutions to parallel Processing Problem*s., 1999 ,Pages: 156-164.

[39] S. Forrest, A. S. Perelson, L. Allen, and R. Cherukuri, " Self-nonself discrimination in a computer", *In Proceedings of the IEEE Symposium on Research in Security and Privacy*, Los Alamos, 1994, pages:1341-1346 .

[40] J. O. Kephart, R. A. Brooks and P. Maes " A biologically inspired immune system for computers", *Proceedings of the Fourth International Workshop on the Synthesis and Simulation of Living Systems*, Cambridge, MA, 1994, pages: 130–139.

[41] Leandro N. de Castro and Jonathan Timmis,"Artificial Immune Systems: A New Computational Intelligence Approach*", Springer*, 2002.

[42] S. Forrest, S. Hofmeyr, and A. Somayaji, "Computer immunology." *Communications of the ACM*, Dec. 1996, pages: 89-98.

[43] AvTravis Russell, "The IP Multimedia Subsystem (IMS): Session Control and Other Network Operations", McGraw-Hill Professional, ISBN 0071488537, 9780071488532, 2007.

[44] Henning Schulzrinne, Jonathan Rosenberg, "The Session Initiation protocol:Internet-centric signaling", *IEEE Communications magazine* , 0ct 2000, Pages:134 – 141.

[45] 3rd Generation Partnership Project; Technical Specification Group SA; 3G Security, "Security Architecture", version 4.2.0, Release 4, 3GPP, TS 33.102, 2001.

[46] Muxiang Zhang; Yuguang Fang; "Security analysis and enhancements of 3GPP authentication and key agreement protocol", Volume 4, *IEEE Communications magazine*, March 2005, Pages:734 – 742.

[47] Yauhui Lei, Samuel Pierre and Alejandro Quintero,"Enhancing UMTS Authentication and Key Agreement with Vector Combination", *UbiCC Journal* , Volume 3April 2008

[48] D. Geneiatakis, T. Dagiuklas, G. Kambourakis, C. Lambbrinoudakis, S. Gritizalis, S. Ehlert, D. Sisalem, "Survey of Security Vulnerabilities in SIP Protocol", *IEEE Communication Surveys Volume 8*, No.3 ISBN 1553-877X, 2006, pages: 68-81 .

[49] D. Geneiatakis, T. Dagiuklas, G. Kambourakis, C. Lambbrinoudakis, S. Gritizalis, S. Ehlert, D. Sisalem, "Survey of Security Vulnerabilities in SIP Protocol*", IEEE Communication Survey, Volume 8,* No.3 ISBN 1553-877X, pp 68-81 2006

[50] Garlan and Perry, guest editorial to the *IEEE Transactions* on Software Engineering, April 1995

[51] Len Bass, Paul Clements, Rick Kazman, Software Architecture in Practice, 2nd Edition, ISBN 0321154959, 9780321154958, Addison-Wesley, 2003.
[52] Marcus Wong, "IMS Security Framework", 3GPP, 2003
[53] Rebecca Chen, Elisa CY Su, Victor Sc Shen, Yi-Hong Wang, "Introduction to IP Multimedia Subsystem (IMS), 3GPP Project, 2006
[54] Gonzalo Camarillo, Miquel-angel Garcia-Martin, "The 3G IP Multimedia Subsystem", 2nd Edition, ISBN 0470871563, 9780470871560, WileyBlackwell, 16 Dec 2005.
[55] Erik E.Anderland, David W.Faucher, Eric H.Grosse, Daniel N. Heer, Andrew R. McGee, David P.Strand, and Robert Thornberry Jr, *" IMS Security*" , Wiley, 2006
[56] 3GPP vision, Ashok chatterjee, Eriksson INC. chairman, 3GPP project co-ordination group, ITU seminar, Ottawa, may 2002, http://www.itu.int/osg/imt-project/docs/2.2_Chatterjee.pdf\
[57] S. Forrest, S. Hofmeyr, A. Somayaji, and T. Longstaff, "A sense of self for UNIX processes", *In Proceedings of the IEEE Symposium on Computer Security and Privacy,* IEEE Press, 1996.