Security Management System for 4G Heterogeneous Networks

Hani Alquhayz, Ali Al-Bayatti, Amelia Platt

***Abstract*—In recent years, there have been major developments in, and deployment of, diverse mobile technology. Security issues in mobile computing are now presenting significant challenges. The ability to move from one network to another, and from one provider to another creating thus vertical and horizontal handoffs, has increased the complexity of mobile security. There are many research groups, such as Hokey and Y-Comm, working on the design of security architectures for 4G networks. Heterogeneous networks are the convergence of wired and wireless networks, other diverse end user devices and other communication technologies which provide very high speed connections. Major security challenges in 4G heterogeneous networks are inherent in current internet security threats and IP security vulnerabilities. These new challenges are: IP address spoofing, user ID theft, Theft of Service, Denial of Service, and intrusion attacks. Therefore, it is necessary to design security solutions which are independent from the network, provider, and end user devices. Existing technique in 4G heterogeneous security networks has not achieved major mobile security requirements such as protecting the mobile equipment; integrity of the hardware, and software. They do not prevent access to the mobile data and the mobile equipment can be used as an attack tool. In addition, current researches in security 4G heterogeneous network do not consider a security management system based on ITU-T M.3400 TMN management functions or any other related standards. In this paper, we propose a management system which is responsible for enforcing security policies and ensuring that security policies continued to be followed. The objective of this security management system is to prevent the mobile equipment from being abused or used as a malicious attack tool. The proposed security management system is consistent with the security specifications defined by ITU-T recommendation M.3400 TMN management functions. Finally, this paper will present a policy-based architecture for the security management system of 4G heterogeneous networks focusing on detection and prevention of malicious attacks. This architecture will consist of intelligent agent, security engine, security policies database, and security administrator.**

***Index Terms*— Mobile Security, Heterogeneous Networks, Security Management System, 4G Networks**

Manuscript received March 05, 2012; revised March 27, 2012.

H.A. Alquhayz is with De Montfort University, Leicester, United Kingdom. (phone: 0447745364459; email: hani373@gmail.com)

A.H Al-Bayatti is with De Montfort University, Leicester, United Kingdom.(email: alihmohd@dmu.ac.uk).

A. Platt is with De Montfort University, Leicester, United Kingdom. (email: amp@dmu.ac.uk).

I. INTRODUCTION

4G is the next generation of mobile networks. The International Telecommunications Union (ITU) defined the International Mobile Telecommunications-Advanced (IMT-Advanced) standard as the global standard for 4G wireless communications. As specified by the International Telecommunication Union's Recommendation (ITU-R), 4G provides very high speed connections such as 100Mbps for outdoor environments and 1Gbps for indoor environments. Also, it is recommended that a 4G heterogeneous network should have high capacity, low cost, low latency, good quality of service, and good coverage [1]. There are many candidates such as LTE Advanced and Wireless MAN Advanced which are trying to achieve these requirements, especially high speed, while, other candidates are trying to build a 4G heterogeneous network as a convergence between wired and wireless networks. There are some new architectures such as, for example, Y-Comm for this heterogeneous network which is a new architecture comprising of a fast core network and a slower peripheral network. The core network contains wired technologies such as optical networks and peripheral networks consisting of wireless technologies such as 3G [5]. 4G security vulnerabilities have been addressed well [3] and [2] and include current IP internet threats and other threats due to the open architecture and the diversity of end user devices' security levels. Some security solutions such as Y-Comm and Hockey have been presented for 4G heterogeneous mobile networks. However, they do not take into account the security of end user devices, which causes many security vulnerabilities and they do not achieve the security requirements of 4G systems.

Y-Comm uses a multi-layer security model to provide a security solution. However, there are researches which show that, because 4G is an IP-based and heterogeneous network, there are several security threats which could cause service interruption and hijack the data. These researches indicated that the current security threats, and also new threats, were inherent in 4G technology [3][2]. The security requirements of 4G heterogeneous networks have been defined on two levels: firstly, these are on mobile equipment; and, secondly, on operator networks. Mobile equipment requirements include protecting the device's integrity, privacy and confidentiality, controlling access to data, and preventing the mobile equipment being stolen or compromised and the data being abused or used as an

ISBN: 978-988-19252-1-3
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

attack tool [4]. Existing research on security of 4G heterogeneous networks focused on the security such as authentication and authorization mainly, on the interface between the network and the operator. However, the protection of the mobile device from attacks and becoming an attack tool solves important security issues in the heterogeneous network.

Therefore, there is a demand to build security management systems for 4G heterogeneous networks. We are building a security management system which detects if the mobile device has been attacked and prevents using it as an attack tool by removing the user's access and severing the connection. We followed the ITU-T's definition of security management as detailed in standardization M.3400, where Security management is the combined function of groups of sets; these are Prevention, Detection, Containment, Recovery, and Security Administration.

The security policies can detect and prevent attacks on end user devices. Security management policy-based systems have a variety of mechanisms depending on the type and scale of the network. There is an increasing challenge when this is a large scale network which combines two different topologies. We propose a policy-based architecture which is independent from the network and can adapt to the changes to the network. Our proposal will achieve a security management system which maintains the security requirements of 4G heterogeneous mobile networks. The remainder of this paper is structured as follows. Section II presents background information about 4G heterogeneous network's security issues, ITU-T recommendations, and policy-based systems. Section III explains the approach and architecture of our security management system. Section IV provides an example of a security management system working in the case of an attack. Finally, Section V concludes this paper.

II. Background

A. Security of 4G Heterogeneous networks

The open nature of 4G means that the infrastructure is accessed from many external connection points through peer operators, through the internet and via third party technologies. All these elements are at risk from providing holes in security and vulnerabilities. Also, different service providers share the core network infrastructure which means that one single provider being compromised affects the whole network infrastructure [2]. 4G network security concerns have been addressed well by many research groups. Y-Comm & Hocky, have worked on designing security architectures such as Hokey and Y-Comm for 4G networks. Y-Comm uses a multi-layer security model to provide a security solution. This model is applied together on peripheral and core frameworks. The four security layers work together through both frameworks. Security services in Y-Comm include Authentication; Authorization; Auditing; and other services related to protecting the entity of the network [5].

However, Aiash et.al' research study was about the security challenges in 4G systems. Their research tried to address the security challenges by looking at the possibility of applying current security techniques on 4G networks. Their research indicated that the current security threats and, also, new threats were inherent to 4G technology. Their study used standard X.805 to investigate the possibility of applying the 3G's Authentication and Key Agreement (AKA) to a 4G communication framework. By applying X.805, they analyzed the AKA protocol in 4G networks. The result was that they found many threats to the network's security [3].

Yongsuk Park and Taejoon Park conducted another research study. They showed that, because 4G was an IP-based and heterogeneous network, there were a number of security threats which could cause service interruption and could hijack the data. They addressed, also, several outstanding open issues which required solutions. In a traditional network security procedure, the network is secured by preventing threats from accessing network entities. However, this is inefficient with an open architecture network such as 4G because the attackers try to find security vulnerabilities in the operating system and in the network protocols or applications. From these vulnerabilities, they can create malware which abuses the network.

According to the new architecture, there are possible threats within a 4G network system. These threats are: IP address spoofing, User ID theft, Theft of Service (ToS), Denial of Service (DoS), and intrusion attacks.

Due to the open architecture and IP based environment, 4G heterogeneous networks receive new security threats and inherit threats from the internet. These threats were unseen in 3G because the network infrastructure was owned by the service providers and access was denied to other network equipment. Also, the diversity in end user devices and security levels leads to greater security threats [1]. The experience of internet protection which says that the protection should involve not only data but, also, entities led us to believe that the 4G should protect both the entities and infrastructure [2].

Also, in mobile communications, another security problem is when the end user device is disconnected from the network for reasons such as battery exhaustion. The transition from level of disconnection to connection presents an opportunity for the attacker to show himself as a mobile device or a mobile support station [12].

There is an increasing importance in protecting the end user device due to the increasing danger of root kits. These are malware which can modify for malicious reasons operating system code and data. MacAfee stated that root kits had increased by 600% in the last few years [13]. Also, MacAfee stated that most malware targeted Android operating systems [9].

In addition, new end user devices are sources of denial of service attacks, viruses, worms, and so on. Smart phones have become attractive targets for attackers and this make the social implications of the attacks more harmful.

ISBN: 978-988-19252-1-3
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

B. ITU-T Recommendation

As specified by ITU-T, recommendation M.3400 belongs to the Telecommunications Management Network (TMN) recommendations. It provides the security management sets of specifications of TMN management function. It considers security management as a part of TMN Management which cannot be isolated from any telecommunication network [6]. Security Management includes four groups of function sets: these are Prevention, Detection, Containment and Recovery and Security Administration. In designing our system, we followed these specifications of security management. Specifications of security management contain many function sets but, as mentioned above, we considered which ones help us to achieve our security requirements. Some function sets, which met our requirements were, firstly, the Customer Security Alarm function set defined as "This set supports access to security alarm that indicates security attacks on their portion of network" [6]. We use this function set to detect if the mobile equipment had been attacked and it help us afterwards to prevent its use as an attack tool. Secondly, there was the Investigation of Theft of Service function set defined as "This set supports investigation of customer and internal users whose usage patterns indicate possible fraud or theft of service" [6]. Also, we use it to lead us to the attacked mobile equipment. Thirdly, there was the Software Intrusion Audit function set defined as "This set supports checks for signs of software intrusion in the network" [6]. This helped, also, to detect if there was a violation in the network which leads us to an attack on the mobile equipment.

C. Policy based system

A security policy is the rule which defines the functions to maintain security in a system. A procedure is the heuristic process to enforce the rule. Therefore, it is important, when we propose a security management system, to build a component which specifies the policies and another component which is responsible for ensuring that these policies have been followed. Another requirement for our system was to address the challenge of combining wired and wireless technologies.

The security management framework, used in a wired network, does not suit wireless networks because of the hosts' dynamic topology and mobility. Consequently, the construction of a security management system for both wired and wireless technologies increased the complexity. There are many solutions on wireless networks which existing researches have followed. Research on a WLAN security management framework follows the concept of dividing the network into wireless policy zones and, therefore, enforcement and validation policies are easier and more efficient [11]. However, a WLAN security management framework requires expensive management and equipment with regard to the need for a local server for each wireless policy zone. Also, scalability was an important challenge which our system needed to address. Many researches on different networks achieved this feature such in [7]. They maintained scalability issues in wireless networks by presenting wireless network policy managers with local policy autonomy. However, they explained neither what type of security policies should be enforced nor the formal validation of such polices. Consequently, we could obtain some idea of autonomous policies by building an auto system administrator with regard to these network changes. An auto system administrator is very fast and cannot be managed easily by human capabilities.

III. Our Approach

This research's goal was to design and implement a security management system which could detect an attack on a mobile in 4G heterogeneous networks and prevent this attacked mobile from being used an attack tool which could harm the network. In our system, we defined the attack as any malicious user who tried to access the system's configuration files such as the password file, the system log configuration file or the mail configuration file [14]. Our approach followed the M.3400 specifications of TMN management. As explained, the system requires detecting an attack on the mobile and preventing this attacked mobile from being used as an attack tool. There are function sets which achieve this requirement. These function sets are: Customer Security Alarm, Investigation of Theft of Service, Software Intrusion Audit, Exception Report Action, and Theft of Service Action.

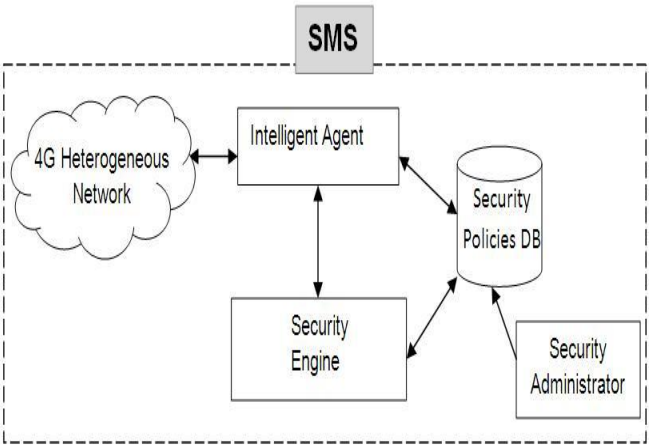

Fig. 1. Architecture of the Security Management System

As illustrated previously with regard to the security threats in a 4G heterogeneous network, we believe that there was a clear requirement for a security management system to address attacks on the end user device [4]. Based on these considerations, we present a policy-based concept of a security management system. Figure 1 shows the four main parts of the system's architecture, which consists of: (1) Intelligent Agent, (2) Security Engine, (3) Security Policies Database, and (4) Security Administrator. We believe that the policies should be able to detect an attack and prevent any damage to the network. The system contains assurance functions to prevent this by removing the user's access and severing the connection to the attacked mobile. Firstly, the Intelligent Agent collects

ISBN: 978-988-19252-1-3
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

information. Then, the Intelligent Agent obtains the policies from the Security Policies Database. Next, the Intelligent Agent analyses this information and sends the results to the Security Engine. Finally, the Security Engine finds that there is no attack and sends an instruction to execute the normal policy set and, when there is an attack, follows the appropriate procedures and stores a record in the database.

A. *Intelligent Agent*

The Intelligent Agent collects the information according to the Security Engine's management policies. It collects different kinds of information such as the mobile device's system information and files information. The system information contains hardware, operating system, etc.

As explained in Figure 2 below, the Intelligent Agent follows four main steps.

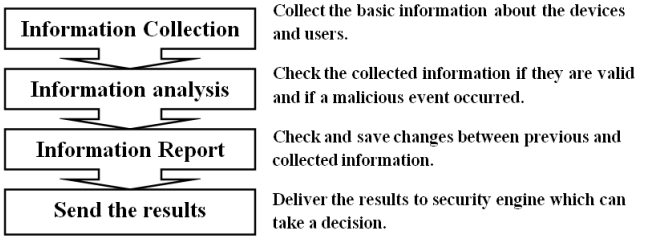

Fig. 2. Intelligent Agent Internal Processes

B. *Security Engine*

The Security Engine obtains from the Intelligent Agent information about the events and saves this information in the Security Policies Database. When the security management system's Security Engine receives event information that there is a violation, it should deny the network access to the mobile device.

The Security Engine makes the decision based on many factors such as the type of attack; the type of end user device; possible vulnerabilities in the same nodes; and previous records in the security database. The decision making process is heuristic and contains full details in order to generate a suitable security policy set. Figure 3 shows the functional diagram of the security management system.

C. *The Security Administrator*

The Security Administrator updates policies and generates new settings for the network when the policies are breached. The Security Administrator's roles are: (1) discovers the inconsistencies between the prescribed policies and current network status, and (2) confirms whether or not the policy rules, network domain and network entities are working together in consistent way.

If the Security Administrator detects a policy violation or inconsistency, it generates a new configuration setting and pushes a report to the security management system's Security Engine which will prevent the mobile device from accessing the network.

The Security Administrator validates the policies by using network topology, the configuration state and previous records about the network.

There are two main security policy levels which are: (1) normal level; and (2) danger level. When there is no attack, the security management system works on normal level with continuous monitoring. The security level moves to the danger level whenever an attack occurs. Also, the Security Engine should take a procedure from the Security Policies Database depending on its analysis and policies. When the security management system recovers from an attack, it moves the security policy level to the normal level and keeps a record in the database for future use.

D. *Justification for using an Automated Security Administrator*

Due to the network and topology changes in wireless networks, human capabilities cannot match the rapid movements in network management movements.

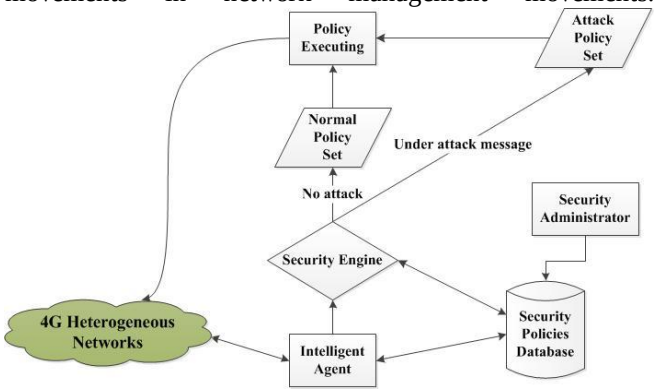

Fig. 3. SMS Functional Diagram

The security policy management needs to be automated to prevent any malicious access to the network after any changes to it [1]. Also, because the limits of static policies are well known, there is a demand for dynamic policies. A dynamic policy is effective and responsive to the changes. Also, separating policy specification from policy management can offer robustness and automation of policies [7].

IV. Example

We show an example of the security management system working in the case of an attack on a mobile device. The example assumes that there is a mobile device connected to the 4G heterogeneous network; this mobile device has an Android operating system. This Android device contains system image located in /system/etc and this image contains Android configuration files. The device files can be accessed with READ and WRITE functions. In the environment of a heterogeneous network, the mobile device is connected via Bluetooth with other mobiles. The Android mobile device receives an attack from another device; the attacker is trying to access the configuration files and modify them [14]. The operating system provides events recognized by the Intelligent Agent; these events are triggered by changes in the configuration files. Therefore, the Intelligent Agent recognizes when a process is trying to access the configuration files. The Intelligent Agent knows

ISBN: 978-988-19252-1-3
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

that there is a malicious attack and sends a message to the Security Engine. This contains the Mobile's IP address, attack type and date and time of the attack. The Security Engine finds that there is danger from this mobile from being abused or used as an attack tool. As explained above, this is a clear security requirement. In this case of attack, the security management system should follow the TMN M.3400 Exception Report and Theft of Service actions function sets. These function sets state that the security breach should be limited by isolating the equipment to prevent the corruption from being propagated and removing the user's access. Therefore, the Security Engine makes a decision to isolate the mobile and remove the user's access to the network. The Security Engine is going to prevent the user's access to the network by contacting the service and application layer in Y-Comm security model. This layer is responsible for authenticating the users, so we can prevent the user's access and isolate the malicious device. Then, the Security Engine keeps a record in the database and the Security Administrator updates the policies for fast detection in case of the same attack happening in the future. Figure 4 shows the sequence of the functions inside the security management system.

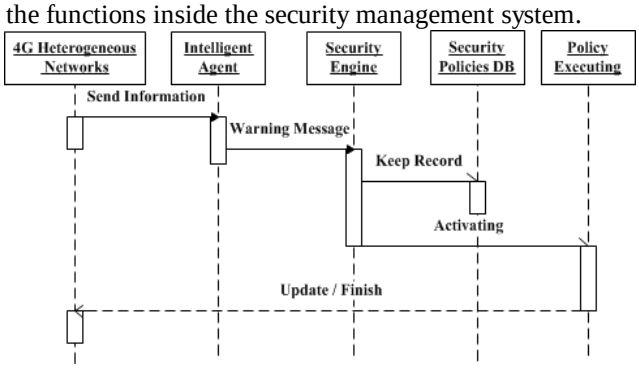

Fig. 1. Sequence of the functions in the proposed system

V. Conclusion

This research defined the architecture of a security management system. This security management system was policy-based and aimed to achieve the security requirements for protecting end user devices in 4G heterogeneous mobile networks. This system could be extended to achieve other requirements targeted at protecting the mobile entity from other attacks. We introduced the automatic security administrator which was reliable in addressing the challenges of fast changing networks. The system's processes are being implemented and the results will be published later.

References

[1] N. Seddigh, B. Nandy, R. Makkar, and J.F. Beaumont, "Security advances and challenges in 4G wireless networks ," in *Privacy Security and Trust (PST), 2010 Eighth Annual International Conference*, Ottawa, ON , 2010 , pp. 62 - 71.

[2] Y. Park and T. Park, "A Survey of Security Threats on 4G Networks ," in *Globecom Workshops, 2007 IEEE* , Washington, DC , 2007 , pp. 1-7.

[3] M. Aiash, G. Mapp, A. Lasebae, and R. Phan, "Providing Security in 4G Systems: Unveiling the Challenges," in *Telecommunications (AICT), 2010 Sixth Advanced International Conference*, Barcelona , 2010 , pp. 439 - 444.

[4] Y. Zheng, Dake He, Weichi Yu, and Xiaohu Tang, "Trusted Computing-Based Security Architecture For 4G Mobile Networks ," in *Parallel and Distributed Computing, Applications and Technologies, 2005. PDCAT 2005. Sixth International Conference*, Sichuan, 2006, pp. 251 - 255.

[5] G. Mapp, Mahdi Aiash, Aboubaker Lasebae, and Raphael Phan, "Security models for heterogeneous networking," in *Security and Cryptography (SECRYPT), Proceedings of the 2010 International Conference*, Athens, Greece , 2011, pp. 1 - 4.

[6] ITU, "ITU-T Recommendation M.3400," 2001.

[7] G. Lapiotis, Byungsuk Kim, S. Das, and F. Anjum, "A policy-based approach to wireless LAN security management ," in *Security and Privacy for Emerging Areas in Communication Networks, 2005. Workshop of the 1st International Conference*, 2006 , pp. 181 - 189.

[8] J. Burns et al., "Automatic management of network security policy," in *DARPA Information Survivability Conference & Exposition II, 2001. DISCEX '01. Proceedings* , Anaheim, CA , USA , 2002, pp. 12 - 26 vol.2.

[9] T. Greene. (2011, November) CSO. [Online]. HYPERLINK "http://www.csoonline.com/article/694728/mcafee-android-is-sole-target-of-new-mobile-malware-in-q3" http://www.csoonline.com/article/694728/mcafee-android-is-sole-target-of-new-mobile-malware-in-q3

[10] S. Maity, P. Bera, and S. K. Ghosh, "A mobile IP based WLAN security management framework with reconfigurable hardware acceleration," in *Proceedings of the 3rd international conference on Security of information and networks*, Taganrog, Rostov-on-Don, Russian Federation, 2010, pp. 218--223.

[11] P. Bera, S. K. Ghosh, and P. Dasgupta, "A Spatio-Temporal Role-Based Access Control Model for Wireless LAN Security Policy Management," *Communications in Computer and Information Science*, pp. 76-88, 2010.

[12] T. and Seberry, J. Hardjono, "Information security issues in mobile computing," 1995.

[13] J. Bickford, R. O'Hare, Ar. Baliga, V. Ganapathy, and L. Iftode, "Rootkits on smart phones: attacks, implications and opportunities," in *Proceedings of the Eleventh Workshop on Mobile Computing Systems \& Applications*, 2010, pp. 49--54.

[14] J. R. Vacca, *Network and System Security*. Oxford, UK: Elsevier, 2010.

ISBN: 978-988-19252-1-3
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)