31st Annual International Conference of the IEEE EMBS
Minneapolis, Minnesota, USA, September 2-6, 2009

Integrity Mechanism for eHealth Tele-monitoring System in Smart Home Environment

Georgios Mantas, *Member, IEEE,* Dimitrios Lymberopoulos, *Member, IEEE*, and Nikos Komninos, *Member, IEEE*

***Abstract*—During the past few years, a lot of effort has been invested in research and development of eHealth tele-monitoring systems that will provide many benefits for healthcare delivery from the healthcare provider to the patient's home. However, there is a plethora of security requirements in eHealth tele-monitoring systems. Data integrity of the transferred medical data is one of the most important security requirements that should be satisfied in these systems, since medical information is extremely sensitive information, and even sometimes life threatening information. In this paper, we present a data integrity mechanism for eHealth tele-monitoring system that operates in a smart home environment. Agent technology is applied to achieve data integrity with the use of cryptographic smart cards. Furthermore, the overall security infrastructure and its various components are described.**

I. Introduction

NOWADAYS, the convergence of information and communication technologies has led to the emergence of assisted living applications in smart homes. Assisted living applications can apply smart home technology to provide health care services to persons with special needs, such as elderly people or people with chronicle diseases, who wish to lead an independent way of life staying at their own home with minimum intervention from healthcare professionals. In a smart home, health care services can be supported by smart in-home eHealth tele-monitoring systems which provide remote, non-invasive, real-time and continuous monitoring for patients [2]. However, the different communication technologies and devices incorporated in these systems pose great data integrity challenges. The heterogeneous and dynamic nature of smart home environment as well as the fact that the transmission of medical information between the smart home and the health care center is done through Internet are factors that raise many data integrity breaches. Data integrity can be compromised by malicious attackers who eavesdrop on the network traffic and attempt to modify or destroy the contents of legitimate messages. Hence, when designing eHealth Tele-monitoring systems, it is essential to define and design a data integrity mechanism to provide data integrity verification for transferred medical data between the patient and the central monitoring station in the health care center.

In this paper we propose a data integrity mechanism for an eHealth tele-monitoring system that operates in a smart home and supports transmission of medical data from the patient's home to the health care center. The proposed mechanism incorporates agent and smart card technology for protection of the transferred medical information from accidental or malicious alteration or destruction. Agents perform a number of tasks required in order to ensure integrity in transferred medical data. Furthermore, agents use cryptographic smart cards to provide extensive support for implementing state-of-the-art mechanisms for validating data integrity [5].

Following the introduction, this chapter is organized as follows. In section II, we briefly present the related work of techniques for ensuring data integrity in eHealth tele-monitoring systems. In section III, we describe the smart in-home eHealth tele-monitoring system in which we apply our proposed data integrity mechanism. Furthermore, the key elements of the proposed mechanism are discussed. In section IV, the proposed mechanism is described. Finally, section V concludes the paper.

II. Related Work

The advances in low power wireless communication technologies and sensor networks have contributed significantly to the emergence of eHealth tele-monitoring area [3]. However, there are many security requirements in eHealth tele-monitoring systems [2], [3]. Data integrity is one of the most important security requirements that should be satisfied in such systems since extremely sensitive patient information is transferred [1], [4]. In [1], it is discussed that during transit of medical information, data integrity protection can be ensured using lightweight message authentication and integrity check methods such as MACs and one-way hash functions. Furthermore, in [6] the local computation is proposed to provide privacy to the transferred data. In [7], encryption of data is proposed to protect sensor data from initial acquisition to final destination. Finally, the Cyber Security Industry Alliance has proposed data encryption, cryptographic checksums and signatures to ensure that transferred medical data have not been changed by unauthorized entities [8].

Georgios Mantas is with the Electrical & Computer Engineering Department, University of Patras, Rio Patras, GR-26500, Greece (phone: 0030-2610996852; e-mail: gman@upatras.gr).

Dimitrios Lymberopoulos is with the Electrical & Computer Engineering Department, University of Patras, Rio Patras, GR-26500, Greece (e-mail: dlympero@upatras.gr).

Nikos Komninos is with the Athens Information Technology, Peania, GR-190 02, Greece (e-mail: nkom@ait.edu.gr).

III. Proposed Data Integrity Mechanism for Smart In-Home e-Health Tele-monitoring System

Our proposed data integrity mechanism is applied on a smart in-home eHealth tele-monitoring system consisting of a Body Area Network (BAN), a Wireless Personal Area Network (WPAN), a Wireless Local Area Network (WLAN) and a public communication network (i.e. Internet).

The BAN is a network placed on patient's body and usually consists of a number of wearable sensors acquiring various vital parameters from the patient's body. Additionally, the BAN includes a wearable unit, called Body Gateway (BG), which gathers the biomedical data from the wearable sensors and transmits them to the base station wirelessly via the WPAN. The BG plays the role of the bridge between the BAN and the WPAN.

The WPAN is a personal wireless network for interconnecting the BG with the base station in order to transmit the biomedical data through wireless technologies to the base station. Typically, a wireless personal area network uses technology that permits communication within about 10 meters.

The WLAN is used to connect the base station to the Residential Gateway (RG). The RG is located in smart home and bridges the internal network of the smart home and the outside world. It integrates all the different networking technologies that exist in the internal network as well as provides access from the internal network to Internet and vice versa. The medical data transmitted to the base station are forwarded to the RG of the smart home over the WLAN.

Finally, a public communication network, such as Internet, is used to transfer the medical data from the RG to the heath care center where the data can be monitored by medical professionals, be analyzed by specific algorithms or be stored in databases.

The network infrastructure of the smart in-home eHealth tele-monitoring system is shown in the following Fig. 1:

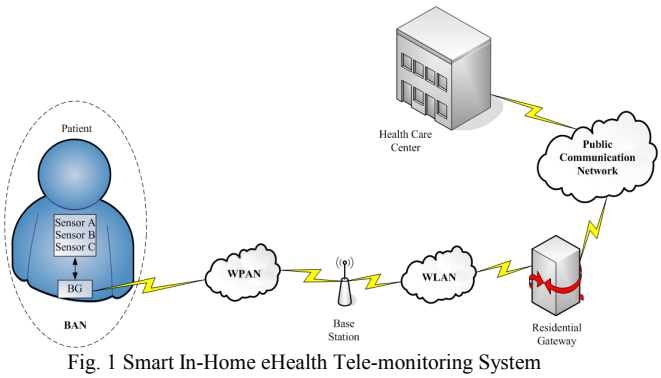

Fig. 1 Smart In-Home eHealth Tele-monitoring System

In our proposed data integrity mechanism, agents are hosted in the BG, the RG and the PC in the health care center. The BG hosts an agent devoted to receive and transmit messages as well as make use of cryptographic primitives. An agent is also located in the RG for receiving and sending messages as well as using cryptographic primitives and executing an encryption process. Finally, the PC of the healthcare professional hosts an agent for receiving messages, using cryptographic primitives and executing a decryption process. The agents in the RG and the PC of the caregiver execute the functions of the cryptographic primitives and the encryption/decryption processes on the cryptographic smart cards connected to the RG and the PC. Each smart card stores a pair of secret keys. The one, called k_m, is for the cryptographic primitives used in the RG and the PC and the other, called k_e, is for the encryption process used in the RG and decryption process used in the PC. As cryptographic primitives, we use a distinct category of keyed hash functions, called Message Authentication Codes (MACs). MAC algorithms and encryption/decryption algorithms are stored on the smart cards. Furthermore, we consider that the MAC-address of each sensor is known a priori to the BG, the RG and the PC in the health care center. Also, the MAC-address of the BG is known a priori to the RG and the PC in the heath care center. Moreover, we suppose that there is a secret pre-shared key, called master key, known a priori to each sensor, the BG, the RG and the PC in the health care center. Thus, we assume that the secret MAC key of each sensor is generated by the following formula:

$$sensor\_key = sensor\_MAC\_address \oplus Master\_Key \quad (1)$$

Additionally, the secret MAC key of the BG is given by the following formula:

$$BG\_key = BG\_MAC\_address \oplus Master\_Key \quad (2)$$

The architecture of our proposed data integrity mechanism is shown in the following Fig.2:

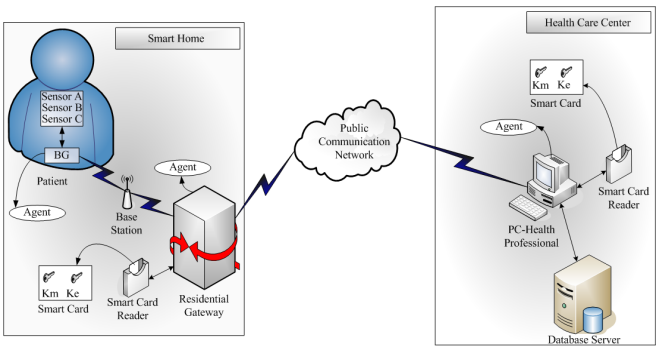

Fig. 2 Proposed Data Integrity Mechanism Architecture

IV. Operation of the Proposed Data Integrity Mechanism

In our proposed data integrity mechanism, we take into consideration two scenarios. In the first one, biomedical data are transferred from a sensor to the PC in the health care center. The first scenario includes four processes. In the second one, a notification message is transferred from the BG or the RG to the health care center.

A. Scenario A

1) Process 1

Each time that a sensor is going to send biomedical data, *x*, to the BG, the sensor firstly computes a MAC, $H_{sensor\_key}(x)$, over the biomedical data, *x*, using its secret MAC key. Then, the sensor sends a message including both the current biomedical data, *x*, and its corresponding MAC, $H_{sensor\_key}(x)$, to the BG.

2) Process 2

The agent of the BG, upon receiving the message, separates the received MAC, $H_{sensor\_key}(x)$, from the received biomedical data, *x*, and independently computes a MAC over the received biomedical data using the secret MAC key of the sensor. Then, the agent compares the computed MAC to the received MAC and if they match, it means that the transferred data have not been altered during the transmission from the sensor to the BG.

Following that, the agent computes the MAC, $H_{BG\_key}(x)$, over the received biomedical data, *x*, using the secret MAC key of the BG. Then, the agent sends a message including both the received biomedical data, *x*, and its corresponding computed MAC, $H_{BG\_key}(x)$, to the base station, which forwards the message to the RG.

3) Process 3

In the RG, the located agent receives the message from the base station and separates the received MAC, $H_{BG\_key}(x)$, from the received biomedical data, *x*, and independently computes a MAC over the biomedical data using the secret MAC key of the BG . The computation of the MAC is executed on the smart card where the MAC algorithm is stored. The agent sends the received biomedical data, *x*, and the secret MAC key of the BG to the smart card where the MAC algorithm is executed and the computed MAC is sent back to the agent that compares it to the received MAC. In case that they match, it means that the transferred data have not been altered during the transmission from the BG to RG.

Then, the agent of the RG uses the smart card to create the message that should be sent to the health care center. Firstly, in the smart card, the agent computes the MAC, $H_{km}(x)$, over the received biomedical data, *x*, using the secret key, k_m, as the secret MAC key. Then, the new computed MAC, $H_{km}(x)$, is sent back to the agent. In the next step, the agent encrypts the received biomedical data, *x*. The encryption takes place on the smart card using the encryption algorithm (e.g. AES) and the secret key, k_e. The encrypted biomedical data, $E_{ke}(x)$, are sent back to the agent. The agent sends the encrypted biomedical data, $E_{ke}(x)$, and the MAC, $H_{km}(x)$, to the PC of the caregiver. The block diagram of Process 3 is depicted in the following Fig. 3:

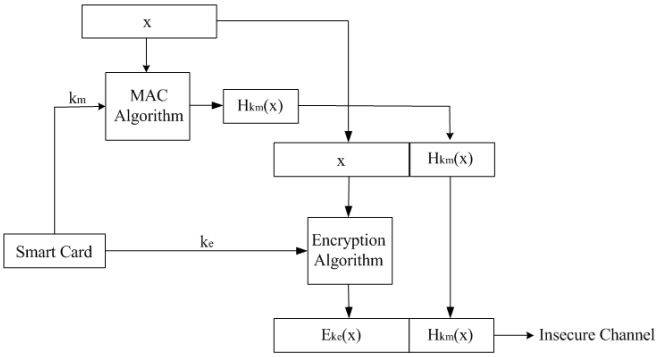

Fig. 3 Process 3 Block Diagram

4) Process 4

In the healthcare center, the PC of the caregiver hosts a local agent and is equipped with the smart card that stores the secret keys, *km* and *ke*, as well as the MAC and decryption algorithms stored on the RG's smart card. The agent receives the message from the RG and separates the received MAC, $H_{km}(x)$, from the received encrypted biomedical data, $E_{ke}(x)$ and sends them to the smart card where they are decrypted using the secret key, *ke*. Then, the agent computes a MAC over the decrypted data using the secret key, *km*, as the secret MAC key. The computation of the MAC is executed on the smart card. Then, the computed MAC is sent back to the agent that compares it to the received MAC. In case that they match, it means that the transferred biomedical data have not been tampered during the transmission from the RG to the health care center.

B. Scenario B

In this scenario, a notification message is transferred from the BG or the RG to the health care center in case that the BG or RG detects that the received data have been changed by unauthorized parties. The notification message includes an alarm code known to the other nodes as well as a MAC computing over the alarm code using the secret MAC key of the node whose data have been tampered. This MAC will be used by the PC's agent to identify the node whose data have been changed.

In case that the BG's agent detects that the received message from a sensor has been changed, the agent sends a notification message (notif_msg) to the RG. The notification message includes the alarm code and a MAC, $H_{sensor\_key}(alarm\_code)$, computing over the alarm code using the secret MAC key of the sensor, whose data have been tampered. Then, the agent computes another MAC, $H_{BG\_key}(notif\_msg)$, over the notification message using the secret MAC key of the BG and sends a message including both the notification message and its corresponding MAC, $H_{BG\_key}(notif\_msg)$, to the base station. The base station forwards the received message to the RG. The above processes, that agent performs, are presented in the following Fig. 4:

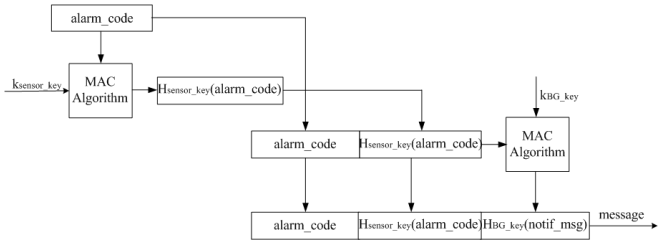

Fig. 4 Processes performed by the agent located in the BG

In the RG, the local agent receives the message from the base station and separates the received MAC, H_{BG_key}(notif_msg), from the received notification message and computes a MAC over the notification message using the secret MAC key of the BG. Thus, the agent sends the received notification message and the secret MAC key of the BG to the smart card where the MAC algorithm is executed and the computed MAC is sent back to the agent that compares it to the received MAC. In case that they match, the agent computes a MAC, H_{km}(notif_msg), over the notification message using the secret key, k_m, as the secret MAC key. Then, the agent sends a message including the notification message from the BG as well as its corresponding MAC, H_{km}(notif_msg), to the PC in the health care center.

In the health care center, the local agent hosted in the caregiver's PC receives the message from the RG and separates the received MAC, H_{km}(notif_msg), from the received notification message and sends it to the smart card where the agent computes a MAC over the notification message using the secret key, k_m, as the secret MAC key. The computation of the MAC is executed on the smart card where the MAC algorithm is stored and the computed MAC is sent back to the agent that compares it to the received MAC. In case that they match, the agent separates the alarm code from the MAC of the sensor, H_{sensor_key}(alarm_code). Then, the agent computes MACs over the alarm code using all the known secret MAC keys of the sensors. When a MAC is computed, it is compared to the MAC, H_{sensor_key}(alarm_code), included in the notification message. When the computed MAC is equal to the H_{sensor_key}(alarm_code), it means that the agent has identified the sensor whose data have been changed as the agent has identified its unique secret MAC key.

In case that the agent hosted in RG detects that the received message from the BG has been changed, the agent sends a notification message to the PC. The notification message includes the alarm code and the MAC, H_{BG_key}(alarm_code), computing over the alarm code using the secret MAC key of the BG. Thus, the agent sends the alarm code and the secret MAC key of the BG to the smart card where the MAC algorithm is executed and the computed MAC is sent back to the agent that creates the notification message. Then, the agent sends the notification message to the smart card where the agents computes the MAC, H_{km}(notif_msg), over the notification message using the secret key, k_m, as the secret MAC key. Then, the agent sends a message including the notification message and its corresponding MAC, H_{km}(notif_msg), to the PC in the healthcare center. There, the local agent performs the same processes as in the previous case to identify that the BG is the node whose data have been changed.

V. Conclusion & Future Work

In this paper, we have proposed a data integrity mechanism for eHealth Tele-monitoring system that operates in smart homes. In the proposed data integrity mechanism, agent technology is suggested to achieve data integrity for the transferred medical data making use of cryptographic smart cards and MACs. The main advantage regarding the use of agents is that they perform all required cryptographic processes as well as exchange the sensitive medical information from the patient to the health care center over a heterogeneous and insecure network without any user interference. Furthermore, MACs are proposed since they are energy efficient secure cryptographic primitives that conserve resources of the sensor nodes.

In our proposed mechanism, we have assumed that the length of the MAC value is n bits. Thus, in both scenarios the overhead is n bits. Additionally, in both scenarios the computational complexity is $O(2^{n/2})$, considering the birthday attack.

Finally, we are in the process of studying the behavior of the proposed data integrity mechanism by simulating our model into the OPNET modeling tool.

References

[1] F. Kargl, E. Lawrence, M. Fischer, Y. Y. Lim, "Security, Privacy and Legal Issues in Pervasive eHealth Monitoring Systems," *7th International Conference on Mobile Business*, 2008.

[2] G. Brettlecker, C. Cáceres, A. Fernández, N. Fröhlich, A. Kinnunen, S. Ossowski, H. Schuldt, M. Vasirani, "Technology in Healthcare," Book Chapter in *CASCOM: Intelligent Service Coordination in the Semantic Web*, Springer, 2008.

[3] M. Meingast, T. Roosta, S. Sastry, "Security and Privacy Issues with Health Care Information Technology," Proceedings of the 28th IEEE EMBS Annual International Conference, New York City, USA, 2006.

[4] C. Meinel, R. AlNemr, "Security Issues and Aspects in Healthcare Pervasive Systems," Quality Control in Biobanking, CATAI 2008, ISBN: 978-84-612-1364-1.

[5] N. Komninos and G. Mantas, "Intelligent Authentication and Key Agreement Mechanism for WLAN in e-Hospital Applications," Book Chapter in Wireless Networks: Research Technology and Applications, Jia Feng (editor), Nova Science Publishers Inc., ISBN: 978-1-60456-895-0, 2009.

[6] J. M. Eklund, T. R. Hansen, J. Sprinkle, S. Sastry, "Information Technology for Assisted Living at Home: building a wireless infrastructure for assisted living," EMBC 2005, Shanghai China, September, 2005.

[7] S. Warren, J. Lebak, J. Yao, J. Creekmore, A. Milenkovic, E. Jovanov, "Interoperability and Security in Wireless Body Area Network Infrastructures," EMBC 2005, Shanghai China, September 2005.

[8] Cyber Security Industry Alliance Technical report, "Ten Steps for Securing Electronic Health Care Systems," April 2005.