Toward a security model for a body sensor platform

Toward a Security Model for a Body Sensor Platform

Shervin Amini, Richard Verhoeven, Johan Lukkien, Shudong Chen
Department of Mathematics & Computer Science, Eindhoven University of Technology
P.O. Box 513, 5600 MB Eindhoven, the Netherlands

Abstract-- **Body Sensor Networks (BSNs) are used in the ubiquitous healthcare to measure human body functions like vital physiological data (e.g. heart beat). As the privacy-sensitive sensor data are transferred over the unreliable wireless connection and can be shared among various BSN applications, it is necessary to protect this data against potential threats. The purpose of this paper is to introduce an approach to design a lightweight security model with respect to limited resource constraints of our special purpose sensor platform.**

I. INTRODUCTION

Body Sensor Networks (BSNs) consist of wearable electronic devices known as body sensors which record human body functions including physiological, emotional and spatial aspects. BSNs can be used for a wide range of applications from monitoring for medical purposes and sports coaching to computer gaming [1]. While various types of BSNs have been investigated in this domain, most of the proposed BSNs are special purpose platforms which deliver the collected data directly to a (particular) data sink.

In the VITRUVIUS project[1], we aim to develop a body sensor platform, on which several BSN applications are installed dynamically, which is self-contained and which can connect to backend systems of choice. The facts that the sensor data are transferred over the wireless connection and shared among different applications lead to security concerns such as data alteration and violation to data authenticity.

The security requirements for the BSN are significantly different from those of typical Wireless Sensor Networks (WSNs). In contrast to the traditional WSNs which measure public information such as temperature and humidity, the BSNs are deployed to collect vital health data from human body such as heart beat and blood pressure. Since such data form a part of the personal Electronic Health Record (EHR), the BSN needs to be protected with a higher level of security which entails the use of precious resources (CPU and memory) of the sensors. Conventional security protocols for the WSNs rely on asymmetric cryptography techniques which exhaust computation power and memory of the sensors [2]. It is, therefore, a great challenge to design a lightweight security model which is both time and resource efficient for the resource-constrained sensors.

In this paper we present system architecture and we outline potential threats to the BSN as part of the overall system. With respect to the threats, we define a set of security requirements and summarize related solutions proposed by state-of-the-art security protocols in the WSN. Our aim will be to select the most efficient lightweight solutions with respect to resource limitations of our sensor hardware platform.

[1] The VITRUVIUS project is funded by the Dutch government in the IOP program *Generic Communication* which aims at building a generic platform for body sensor applications.

II. SYSTEM ARCHITECTURE

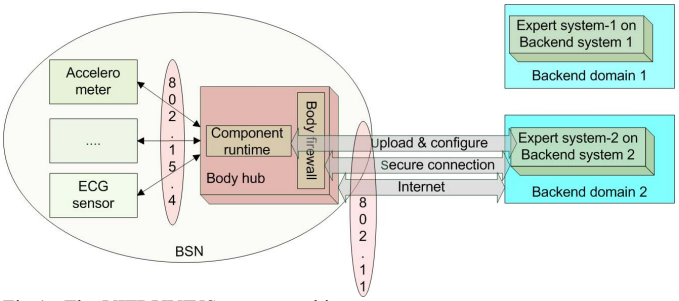

Fig 1. The VITRUVIUS system architecture

Fig 1. depicts the two-layer system architecture designed in the VITRUVIUS project. The first layer is composed of the wireless sensors attached to a person's body, measuring and sending the physiological data to the body hub (e.g. smart phone) for further processing. The set of sensors and body hub forms a person's Body Sensor Network (BSN). From the body hub the data are transported via a network connection to a backend system (e.g. hospital), in the second layer, where the data are analyzed and subsequent actions are taken when needed. Furthermore, the clinical staff in the backend system determines the behavior of the BSN by giving parameters (e.g. data type, frequency) to an expert system (decision support system). The expert system generates instructions in the form of application components which are executed with the help of the run-time platform on the BSN. The execution of the application components configures the BSN (hub and sensors) towards a certain monitoring and analysis task.

In this paper, we consider threats to the BSN with respect to the communication channel from sensors to body hub. The threats are instantiated by the attacks which are effective because of associated vulnerabilities (weaknesses) in the BSN. We examine the combination of the following attacks and vulnerabilities which help us to design a security model.

Wrong data from sensor. This might happen because of a faulty sensor, a noisy channel or malicious alteration of transmitted messages. Our security model must protect message transfer against the alteration.

Data loss. This might be caused by (malicious) interference or by a noisy wireless channel. We cannot simply avoid this, but our security method must be resilient to data loss.

Spoofing of sensor. Unintentionally or maliciously a sensor may be attached to a wrong person or a wrong sensor-body hub relationship may be established. Furthermore, the attacker may spoof the identity of the sensor. Our security method must make such spoofing impossible by using authentication.

Eavesdropping and replay. A malicious attacker might intercept messages for inspection or replay. Our security method, therefore, must encrypt messages and protect them against the replay.

III. SECURITY REQUIREMENTS

Fig. 2 shows a use case in which sensor sends messages, which contain data, to body hub via a pre-established wireless connection. After the sensor transfers the recorded data (1, 2), the body hub stores and checks the correctness of the data (3, 4) with respect to security requirements (4.1-4.4) before processing (5). Based on the mentioned threats, we summarize the security requirements and examine the solutions.

A. Confidentiality. During the message transfer, raw/processed sensor data must be kept confidential in order to protect them against eavesdropping by unauthorized entities. Typically in the WSN the confidentiality is achieved via an encryption method using a shared secret key. The amount of confidentiality gained, depends on the type of cipher scheme and mode of operation.

B. Authenticity. Exchanged messages must be authenticated according to the partnerships setup in the initialization phase. Message authenticity is typically achieved when the sender attaches a message authentication code (MAC) to the message. However, it may also be combined with confidentiality.

C. Replay protection. Upon receiving a message, the receiver (body hub) must ensure that the message is fresh and not replayed by an attacker. A typical defense against the replay attack is to include a monotonically increasing counter with every message and reject messages with old counter values.

D. Tolerance to message loss. With respect to the noise and the presence of the attacker in the communication channel, the receiver must be aware of the message loss. The number of the lost messages can be detected by using the counter.

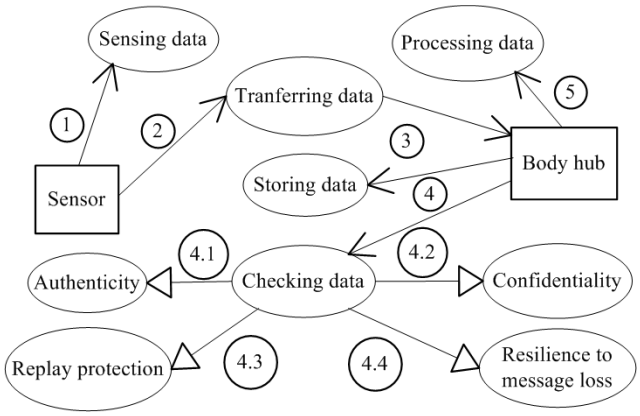

Fig 2. The use case for sensor data collection and reporting to body hub

IV. A SELECTIVE APPROACH FOR A SECURITY MODEL

Our approach to design the lightweight security model is based on state-of-the-art security protocols in the WSN. A comparison of these protocols with respect to the security requirements (B, C, and D) is illustrated in Table I. As the choice of a cipher affects the time and resource efficiency of our security model, we measured the resource usage of ciphers, which provide confidentiality (A), in terms of RAM, ROM (bytes), and clock cycles per byte (CPB) as shown in Table I. The measurements are based on the 16-bit MSP430 microprocessor with 48kB ROM, 10kB RAM and performed using the instruction-level platform simulator Wsim.

TABLE I
COMPARISON OF PROTOCOLS AND RESOURCE USE OF CIPHERS

Protocols	A				B	C	D
	Cipher	RAM	ROM	CPB			
TinySec [3]	Skipjack	276	3798	186.54	✓		
MiniSec [4]					✓	✓	✓
LLSP [5]	AES	4344	5865	306.5	✓	✓	
RC4-based [6]	RC4	1068	1494	62.23	✓	✓	✓

From the table above, we can observe that RC4 and Skipjack are the most efficient ciphers in terms of encryption/decryption speed and RAM size, respectively. As such, RC4 and Skipjack can be used to provide lightweight message confidentiality for our security model.

V. CONCLUSION

We have described the BSN architecture in the VITRUVIUS and have introduced the potential threats to its security. To examine the threats, we have identified the security requirements and the related solutions. Inspired by the state-of-the-art security protocols in the WSN, we found that RC4 and Skipjack are the efficient ciphers to provide the message confidentiality. We intend to investigate the most efficient approaches toward the remaining security requirements in our subsequent paper.

REFERENCES

[1] B. Lo and G. Z. Yang. "Key technical challenges and current implementations of body sensor networks," In: IEE Proceedings of the 2nd International Workshop on Body Sensor Networks (BSN 2005), Apr. 2005, pp. 1-5 (2005).

[2] H. S. Ng, M. L. Sim, and C. M. Tan, "Security issues of wireless sensor networks in healthcare applications," BT Technology Journal, vol. 24, no. 2, pp. 138–144, 2006.

[3] C. Karlof, N. Sastry, and D. Wagner, "TinySec: a link layer security architecture for wireless sensor networks," In SenSys, ACM, 2004.

[4] Luk, M., Mezzour, G., Perrig, A., Gligor, V.: "MiniSec: a secure sensor network communication architecture," In IPSN, Cambridge, Massachusetts, USA, Apr. 25-27 (2007).

[5] Leonard E. Lighfoot, Jian Ren, Tongtong Li, "An energy efficient link-layer security protocol for wireless sensor networks," In IEEE EIT, Nov. 2007.

[6] Yu, Qian, Chang N. Zhang, "A lightweight secure data transmission protocol for resource constrained devices," Security Comm. Networks, Sep. 2009.