A trust management model for Body Sensor Networks

Citation for published version (APA):

Bui, T. V. (2011). A trust management model for Body Sensor Networks. In *Proceedings of the 2011 IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM 2011, Lucca, Italy, June 20-24, 2011)* (pp. 1-3). Institute of Electrical and Electronics Engineers.
<https://doi.org/10.1109/WoWMoM.2011.5986201>

DOI:

[10.1109/WoWMoM.2011.5986201](https://doi.org/10.1109/WoWMoM.2011.5986201)

Document status and date:

Published: 01/01/2011

Document Version:

Publisher's PDF, also known as Version of Record (includes final page, issue and volume numbers)

Please check the document version of this publication:

- A submitted manuscript is the version of the article upon submission and before peer-review. There can be important differences between the submitted version and the official published version of record. People interested in the research are advised to contact the author for the final version of the publication, or visit the DOI to the publisher's website.
- The final author version and the galley proof are versions of the publication after peer review.
- The final published version features the final layout of the paper including the volume, issue and page numbers.

[Link to publication](#)

General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal.

If the publication is distributed under the terms of Article 25fa of the Dutch Copyright Act, indicated by the "Taverne" license above, please follow below link for the End User Agreement:

www.tue.nl/taverne

Take down policy

If you believe that this document breaches copyright please contact us at:

openaccess@tue.nl

providing details and we will investigate your claim.

A Trust Management Model for Body Sensor Networks

Vinh T. Bui

*Security and Embedded Networked Systems
Department of Mathematics and Computer Science
Eindhoven University of Technology, The Netherlands
Email: t.v.bui@tue.nl*

Abstract—Body Sensor Networks (BSNs) are used for diverse applications ranging from monitoring for medical purposes, sport coaching to computer gaming. A foreseen usage scenario for a BSN is the installation of third-party monitoring applications. Existing applications can also be extended by downloading and installing new components dynamically. Dependability and security properties must be preserved under these changes while the user of the BSN must have a transparent view on data usage and installed software. To that end we propose an efficient trust management model and we investigate policies and mechanisms to express and control the data usage.

Keywords—body sensor network; trust management; trust model; downloadable components;

I. INTRODUCTION

A BSN consists of a wide variety of wearable electronic devices, so-called body sensors, which measure body functions such as movement, location, and vital signs. While BSNs have been investigated and used in various types of monitoring applications, many of them are special purpose platforms which deliver the collected data directly to a central backend system [1]. At the backend system features are extracted and messages or warnings are issued, e.g., extraction of the heart rate from an ECG signal. Since raw sensor data is transferred over the network, the user is not in control of privacy sensitive information leaving his personal network, but must trust the integrity of the applications and the backend system.

In the VITRUVIUS project [2], we aim to develop a body sensor *platform*, on which applications and components can be uploaded and installed dynamically, which is self-contained and can connect to backend systems (e.g., a hospital system) if required [3]. The VITRUVIUS's BSN consists of sensors together with a more powerful device, called the *body hub*, that is capable of storing data and running software components (see Figure 1). New components are uploaded to the body hub in the form of executable code, execution of which leads to the configuration of the BSN towards specific services. For instance, an application may want to install and use its own decision support component, to get access to specifically tailored information.

The problem is then to preserve dependability and security characteristics of the system: new components might leak information, affect the overall resource distribution

amongst components, or jeopardize the correct execution of the device. There also exists other potential threats to the system security (e.g., wrong data from sensor, data loss, spoofing of sensor, and eavesdropping), which we analyzed and mentioned in [4]. To address these problems, we propose a trust management model, which monitors the trustworthiness of components and their data usage such that the user can transparently manage his BSN. We are interested in reasoning about the trustworthiness of the system with respect to system properties like integrity, resource usage, and data use, based on properties of the components and the composition. Input to this reasoning are, for example, code dependencies, presence of encryption mechanisms, or particular properties of the loaded components.

II. RELATED WORK

Trust management can be specially useful for a sensor network in term of the security system design, but not much work has been done for BSNs. In [5] the authors introduce a security framework with trust management, i.e. establishment of a trustworthy network environment, to secure sensor networks. For trust management, a distributed trust model enabling recommendation-based trust and trust-based recommendation is proposed, to build reasonable trust relationship (e.g., trust values) among network entities. The authors in [6] propose a trust model without a central trust authority, to establish trust for wireless sensor networks. The approach combines several kinds of trust values together, including the direct and indirect trust values of nodes. The direct trust value is the type of trust value that can be established between an initial node (sponsor node) of the cooperation and a target node that provides a service to the sponsor node. The indirect trust value is established when a third-party node provides its trust value of the target node to the sponsor node. These presented models however focus more on the trust relationship during the interaction process among the nodes than the trust management with respect to the system properties and behavior of the application components running on the nodes.

The authors in [7] propose a trust management framework for embedded systems which, while acting on behalf of components, supervises the system's existing trustor-trustee relationships and preserves the overall system level of de-

pendability and security. Being different from the other models above, this approach supports a trust management model for application components and it implements both solutions for monitoring the behavior of a component and control mechanisms for that. Our trust management model is based on this model and is modified for the use in BSNs.

III. SYSTEM ARCHITECTURE

The system architecture of the VITRUVIUS project is shown in Figure 1. The body hub controls the BSN and is the primary access point. The BSN may connect to backend systems through the Internet, employing a secure connection between an *expert system* running in the backend and an access control service in the body hub, which is called the *body firewall*. Through the secure connection, the back end system communicates with the BSN for the purposes of retrieving data and installing software. The body firewall shields the body hub from the outside world and limits access to privacy-sensitive data according to the authorization level of the requesting party. For example, the user or his social care givers receive different information than doctors or professional sport coaches do.

Figure 1. The system architecture, addressed in the VITRUVIUS project.

The medical experts in the backend system determine the behavior of the BSN by giving parameters (e.g., data type, sampling frequency) to an expert system. The expert system generates instructions in the form of application components, which are then uploaded to the body hub. The components, in combination with resident run-time information in the body hub are capable of gathering the required data, analyzing relevant events and taking appropriate actions towards a certain monitoring and analysis task. The responsibilities of the different parts of the BSN are as follows.

A. Sensor nodes

At or near the body, a number of sensor nodes extract information from the body via dedicated sensors. The program of the sensor nodes determines the data which is sent to the body hub. Our special purpose sensor platform allows nodes to be programmed over the air by the body hub. There are also *single-sensor signal processing components* running on these sensors, which pre-process the data (through calibration, signal validation and compression).

Besides the trustworthiness of the whole BSN, we also consider security aspects of the wireless communication and the sensor resource management.

B. Body hub

The body hub receives data from the sensors, stores, and processes it according to the instructions from the loaded components. The body hub must be capable of autonomously responding to abnormal conditions found in the data, like contacting the user or the expert system in case of an emergency. Most importantly, the body hub maintains the trustworthiness of the system. Figure 2 presents a simplified component view of the body hub architecture.

Figure 2. The simplified component view of the body hub architecture.

Based on the sensor signals received from the *Sensor Abstract Layer*, the key physiological parameters (e.g., heart rate and temperature) are computed by signal processing components, and subsequently the key diagnostic information is extracted by the *Decision Support Engine* module. This processing is controlled by *Application specific components* uploaded to the body hub. To support the component upload and configuration in a secure and trust preserving manner, the body hub architecture contains two modules:

Secure Upload and Configuration Manager: This module provides means for run-time upload and installation of the application specific components. For example, an application may want to use its own signal processing component to process and get access to specifically tailored information. In this case, the application can request installation of this specific component on the body hub. The module checks the component's certificate, verifies the future system integrity, and installs the component on the system.

Trust and Ownership Monitor Engine: This module constantly monitors the components' behavior and the system properties, and also predicts and verifies these properties at system configuration time, thereby authorizing configuration changes.

Within the body hub, the raw incoming signals as well as the state values of the BSN can be collected in the *Data Storage* for inspection in special cases (e.g., liability

disputes) or at special moments (e.g. the body hub is disconnected from the backend system).

IV. TRUST MANAGEMENT MODEL

We define trust as follows: Trust is the degree to which a trustor has a justifiable belief that, in a given context, a trustee will live up to a given set of statements about its behavior.

In this definition, trustor and trustee can be any entity (e.g., a user, a computer, or a process); 'justifiable' refers to the ability to explain the reasoning or computation behind the trust. According to this view, trust is a value (or vector) in the range 0 through 100% determined by trustor, trustee, and context. The context includes elements that determine the trustee's behavior (e.g., available resources or competing applications) as well as information that influences the trustor's judgement (e.g., history). In general we model this context as some state vector.

For the scope of this work we specialize the *Trust Model* (see Figure 3) for the scenario of a component (C) uploaded into the body hub (B). The trustor is B , the trustee is C , and the context is given by the current state of B , $B.S$. We only consider explicit statements about the behavior of C , the *Quality Profile*, represented as a list $C.X$. An example of such statement is: " C uses at most 10Kb of memory." One of the statements includes the functional properties of C . Components may have several modes of operation like "secure" or "resource efficient", which may have different qualities. The *Trust Profile*, specified by the trustor, is a vector of weights ($B.W$) that give the relative importance of $C.X$ to B . The Trust Profile may have modes that describe different modalities of judgements in different contexts.

Figure 3. The functional block diagram of the trust management model.

The Quality Profile may also be evaluated by an authority A . The opinion of A about the quality statements of C is represented by a vector of trust values ($C.T$) associated with $C.X$. In this way the trust is delegated to A allowing B to trust C on behalf of A . The problem of how A develops this trust is out of scope for this paper.

The trust value is then evaluated by the *Trust Evaluation* function, based on $C.X$, $C.T$, $B.W$, and $B.S$. Subsequently, decisions are converted into control actions which can, for example, install a new component, reduce the priority of

a certain component, or signal it to change to a different mode of operation. The user can also transparently intervene and enforce his decisions. The monitor keeps checking the compliance of the component's actual behavior against its declared behavior and it may trigger a re-evaluation and a new decision making process.

V. CONCLUSION AND FUTURE WORK

We have introduced the system architecture and a trust management model for our body sensor platform. The trust management model is used to enhance the dependability and security of the system under dynamic changes in applications (e.g., the applications can be extended by downloading and installing new components dynamically).

Our current work is to specify the Trust Model more precisely and to specify the evaluation functions.

ACKNOWLEDGEMENT

This work has been conducted within the VITRUVIUS project supported by the Dutch Ministry of Economic Affairs under the Innovation Oriented Research Program. The author would like to thank to Johan Lukkien, Shudong Chen, and Richard Verhoeven, in developing the presented concepts and for their useful comments in improving the quality of this paper. My thanks are also to all other members of the project for their contributions so far.

REFERENCES

- [1] B. Lo and G. Z. Yang, "Key technical challenges and current implementations of body sensor networks," in *Proc. 2nd International Workshop on Body Sensor Networks*, Apr. 2005.
- [2] "Vitruvius project official website." [Online]. Available: <http://vitruvius-project.com/>
- [3] J. Linnartz, J. d. Groot, J. Lukkien, and H. Benz, "A novel architectural concept for trustworthy and secure access to body sensor information," in *Proc. 4th International Conference on Intelligent Systems and Knowledge Engineering*, vol. 2, November 2009, pp. 417–423.
- [4] S. Amini, R. Verhoeven, J. Lukkien, and S. Chen, "Toward a security model for a body sensor platform," in *29th International Conference on Consumer Electronics*, 2011.
- [5] Z. Yao, D. Kim, I. Lee, K. Kim, and J. Jang, "A security framework with trust management for sensor networks," in *Security and Privacy for Emerging Areas in Communication Networks, 2005. Workshop of the 1st International Conference on*, sept. 2005, pp. 190 – 198.
- [6] G. Han, D. Choi, and W. Lim, "A reliable approach of establishing trust for wireless sensor networks," in *Proc. the 2007 IFIP International Conference on Network and Parallel Computing Workshops*, ser. NPC '07. Washington, DC, USA: IEEE Computer Society, 2007, pp. 232–237.
- [7] G. Lenzini, A. Tokmakoff, and J. Muskens, "Managing trustworthiness in component-based embedded systems," *Electronic Notes in Theoretical Computer Science*, vol. 179, pp. 143–155, 2007.