Adaptive Information Security in Body Sensor-Actuator Networks

Krishna K. Venkatasubramanian and Craig A. Shue
Dept. of Computer Science
Worcester Polytechnic Institute
Worcester, MA, 10609
{kven, cshue}@wpi.edu

***Abstract*—A Body Sensor Actuator Network (BSAN) consists of a set of sensing and actuating devices deployed on a person (user) typically for health management purposes. Securing the information exchanged within a BSAN from unauthorized tampering is essential to ensure that such systems are *safe*, and thus do no harm, to the people using them. Current solutions for enabling information security in BSANs impose considerable overhead on the nodes. In order to make security viable in BSANs, one needs to move away from this one-size-fits-all solution and take a more adaptive approach where the level of security provided matches the level of threat present. In this regard, we present an adaptive information security scheme for BSANs that uses *honeypots* to measure the current *threat context*, by interacting with the adversaries trying to undermine user safety. The measurements made by the honeypot can then be used to determine the appropriate balance for the tradeoff between the level of security and associated overhead at any given time. This paper provides an overview of our approach and the associated research challenges in successfully implementing it.**

I. Introduction

Emerging Body Sensor Actuator Networks (BSANs) have demonstrated great potential in a broad range of applications in healthcare and wellbeing. A BSAN consists of a set of low-capability monitoring and actuation devices deployed on a user. These devices continuously monitor the user and provide sensor information to a sink entity called the base station for processing. The base station can then provide treatment to the user using the actuators in the network. As BSANs deal with personal health data, ensuring information security, especially over the communication channel is critical. Security vulnerabilities may potentially allow attackers to compromise patient safety by modifying actual physiological data, resulting in a wrong diagnosis and treatment [4].

One way of enabling information security in BSANs is to distribute (symmetric) cryptographic keys between the nodes in the BSAN in a secure manner. Numerous secure key distribution techniques have been proposed in the literature for BSANs [5], [4], [1], [2], [3]. Using the exchanged key, the devices can encrypt and verify the integrity of any subsequent data exchange with other BSAN nodes. Further, the devices can verify the authenticity of each other by requiring evidence that the remote party holds the key (e.g., through a message authentication code (HMAC)).

The secure key distribution and secure data communication protocols implemented on BSANs have two important characteristics: (1) *Overhead:* They add considerable computational and communication overhead to the limited capability platforms like BSANs. (2) *Static Nature:* The protocols proposed in these approaches never change; they are not aware of the user's current threat context nor do they respond to it.

We can reduce the overhead of these information security protocols by allowing them to employ protections commensurate with the prevalent threat context. It is well understood that, unlike traditional computing, for low capability systems such as BSANs the security vs. overhead tradeoff is particularly important. A "perfect" but computationally expensive security solution is not very useful if it quickly drains the battery of the nodes in turn affecting its usability of the system. However, this does not mean one can choose a security solution that is weak in the interest of being computationally cheap. What is needed is needed a hybrid solution where the security solution being used *adapts* to the threat context. They should use different versions of secure key distribution and secure data communication protocols depending on the prevailing threat context around the user. We measure the threat characteristics by using a *honeypot* to learn adversary intentions and capabilities. With such monitoring, we aim to find the right balance in the tradeoff between the security provided and the associated overhead.

II. Adaptive Security for BSANs

A honeypot is a trap set to detect attempts by malicious entities to gain unauthorized access to information systems. Traditional honeypots have been used in enterprise networks and consist of a group of machines that appear to be part of the enterprise's network, but are actually isolated and monitored. The honeypots are designed such that legitimate access to the enterprise network never leads the user a honeypot machine. Therefore, any access attempt observed at the honeypot is, by definition, unauthorized. The honeypot resembles a regular enterprise network machine and monitors the connected user to learn about the adversary's motivation and capabilities [6].

We can apply the honeypot concept to BSANs as well and use it in two modes: (1) *Passive-Mode:* In this use-case a honeypot is a dedicated BSAN device or an application on the base station that acts as an open node that accepts commands from anyone. If an adversary is present in the vicinity, then any interaction with the honeypot will allow the BSAN to get an understanding of their intention. In the bait-mode, the honeypot can only detect active adversaries who try to interact with the BSAN. (2) *Active-Mode:* To combat adversaries that attempt to intercept or manipulate messages in the BASN without interacting with the honeypot, we take a more active posture. In this regard, we send "honeypot messages" between the two entities in the BSAN acting together as honeypots. The

entities use a high security channel to indicate which messages are honeypot messages and then send those honeypot messages using a lower security channel. If the messages are altered, the nodes will know that an attacker is actively manipulating the messages. The active model has additional utility in that if an adversary passively monitors the channel, it will be unable to distinguish real messages from the false honeypot messages, leading to misinformation. For the honeypot to operate in both passive and active modes, in a single hop network like BSAN, it would need to be implemented at the base station and one or more additional *helper nodes* in the network.

Introducing honeypots devices and messages into BSANs alone is only a part of the solution. The next step is to determine how to change the security primitives within a BSAN based on the measurements of the honeypot. This can be done by first defining a set of *security levels*. Each security level is characterized by a two parameters: (1) number of and type of protocol steps (e.g., nonce exchange, certificate exchange, vault exchange, master key generation) it involves, and (2) set of variables associated the security primitives exchanged during each of the protocol steps (e.g., key length, nonce usage, HMAC algorithm used). When the measured threat is low, the BSAN can be operated at a security level that is very cheap in terms of overhead and also provides minimal security. As the measured threat increases, the security level at which the BSAN operates also increases, providing adaptive security for BSANs. We believe that the number and characteristics of the security levels have to be customized for each user of the BSAN. This is because each user has a specific routine that may be different from others and require different security guarantees. Further, in the interest of keeping security configuration requirements to a minimum, the BSAN must determine the security level in a manner that is transparent to the user, perhaps even automatically changing over time based on user behavioral changes.

III. Research Challenges

There are four main research challenges that need to be met before adaptive security can be effectively used with BSANs, which we will discuss below.

Link-layer Issues: Implementing the honeypot highly depends on the link-layer protocol in place between the nodes and the base station. For example, we consider Bluetooth-based BSANs. Bluetooth is one of the most common link-layer protocols used in medical devices and personal area networks. Bluetooth mandates that a device be a master or a slave in only one piconet at a time. Therefore, in the passive mode of operation, the base station would have to interact with the malicious node to learn its capabilities. This would mean allowing malicious nodes to join the user's BSAN, yet isolate them from legitimate and helper nodes. This may be a challenge. This problem is further complicated if the nodes use different link layer protocols in the same BSAN.

Interaction Design: In the passive mode, the honeypot will have to interact with the malicious entity and determine its capabilities and intentions. The goal for the honeypot is to keep the malicious entity connected for a substantial period of time to learn its capabilities while not disclosing useful information. A signification research issue is determining what kind of interactions are permitted.

"Honeypot Message" Ratio: In the active mode, the base station and helped node will be exchanging low security honeypot messages with each other interspersed with higher security regular messages. Determining the exact percentage for the mixing of the two message types is a open problem. Too few honeypot messages might mean the adversary is not detected and too many of them might lower the goodput within the network. Further, this level of mixing might even have to adapted as the threat context changes around the user. Higher threat environments might need greater proportion of honeypot message, compared to lower threat environments. Finding the optimal number of honeypot messages for different situations is also an open problem.

Threat-Security level Mapping: Upon determining the threat present, we must map the honeypot measurements to an appropriate security level. One option is to have a *policy language* as a way to map the measurements to security levels. The language used should be extendable enough to deal with extensions to the entire system both in terms of what the honeypot measures (in passive and active mode) and the number of security levels that are defined.

Switching Costs: Switching between the different security levels in response to the measurements made by the honeypot has its own costs. Rapid switches between security-levels might not be good for the system stability and may impose significant overheads. As an example, a threat may require the distribution of new, longer keys for a more secure communication protocol. The BSAN must consider the overheads involved in security level changes.

IV. Conclusions

Preserving information security is essential for BSANs in order to ensure user safety. Current information security solutions are insufficient because they are computationally expensive and static in nature. In order to make information security viable in BSANs, we must take an adaptive approach where the level of security provided matches the threat present. Our approach uses a honeypot to monitor and interact with adversaries and used the information thus collected to change the level of security provided within the system. We then provide a list of challenges for designing the honeypots along with how to use the information provided by these honeypots to enable adaptive security for BANs.

References

[1] A. Banerjee, S. K. S. Gupta, and K. K. Venkatasubramanian. Pees: Physiology-based end-to-end security for mhealth. In *Proceedings of the 4th Conference on Wireless Health*, WH '13, pages 2:1–2:8, New York, NY, USA, 2013. ACM.

[2] C. Hu, X. Cheng, F. Zhang, D. Wu, X. Liao, and D. Chen. Opfka: Secure and efficient ordered-physiological-feature-based key agreement for wireless body area networks. In *INFOCOM, 2013 Proceedings IEEE*, pages 2274–2282, April 2013.

[3] C. C. Y. Poon, Y.-T. Zhang, and S.-D. Bao. A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health. *Communications Magazine, IEEE*, 44(4):73 – 81, April 2006.

[4] K. K. Venkatasubramanian, A. Banerjee, and S. K. S. Gupta. PSKA: Usable and secure key agreement scheme for body area networks. *Information Technology in Biomedicine, IEEE Transactions on*, 14(1):60 –68, Jan. 2010.

[5] K. K. Venkatasubramanian and S. K. S. Gupta. Physiological value-based efficient usable security solutions for body sensor networks. *ACM Trans. Sen. Netw.*, 6(4):31:1–31:36, July 2010.

[6] F. Zhang, S. Zhou, Z. Qin, and J. Liu. Honeypot: a supplemented active defense system for network security. In *Parallel and Distributed Computing, Applications and Technologies, 2003. PDCAT'2003. Proceedings of the Fourth International Conference on*, pages 231–235, Aug 2003.