On Usable Authentication for Wireless Body Area Networks

Cory Cornelius
Department of Computer Science
Dartmouth College
cory.t.cornelius@dartmouth.edu

David Kotz
Department of Computer Science; Institute for Security, Technology, and Society
Dartmouth College
kotz@cs.dartmouth.edu

Abstract

We examine a specific security problem in wireless body area networks (WBANs), what we call the *one body authentication problem*. That is, how can we ensure that the wireless sensors in a WBAN are collecting data about one individual and not several individuals. We explore existing solutions to this problem and provide some analysis why these solutions are inadequate. Finally, we provide some direction towards a promising solution to the problem and how it can be used to create a *usably secure WBAN*.

1 Introduction

As the population of the world grows, it will become increasingly necessary to use technology to monitor, diagnose, and treat populations. We imagine, for example, that WBANs will become the dominant means of collecting longitudinal health-related data, which will enable physicians to make better medical decisions. By their very nature, WBANs also present unique security and privacy challenges. If we expect WBANs to become a solution to monitoring the world's aging population, then it is imperative that we are mindful of their security and privacy implications. Many researchers have noted that WBANs are energy scarce, and, in doing so, have made significant steps towards developing energy-aware security solutions where the overhead of security is minimal if not nil [4, 8]. Furthermore, we must also remind ourselves that secure solutions should be usable, because the target population for these kind of systems is often the elderly.

2 One body authentication problem

Although one can find many security related problems in WBANs, we focus on one particular problem. In WBANs there are typically multiple wireless sensors collecting data about a particular user and transmitting this data to a particular base station. One can easily imagine cryptographic schemes to pair wireless sensors with a base station such that all communication is confidential and the sensor data's integrity is preserved. Even with these security precautions, there is an assumption that the wireless sensors are all attached to the same human body. An even stronger assumption is that the wireless sensors are attached to a particular human body. Collectively, we call this the *one body authentication problem*, the latter being the strong version and the former being the weak version. For now, we set aside the strong version and focus on the weak version. We limit ourselves to the weak version because we treat the user not as malicious adversary but a forgetful one. That is, a user might forget to re-pair a wireless sensor already paired with another user, or they might accidentally swap wireless sensors.

This problem matters for at least one important reason. If we expect physicians to make decisions about health data collected from WBANs, then they are going to need some confidence that all the data they are examining has come, at the very least, from the same body. It is risky to make medical decisions without said confidence, and until such measures are in place, physicians should be wary of using data from WBANs.

3 Solutions and shortcomings

In the following sections we present some existing solutions and their shortcomings.

Low-tech

A simple solution is to put labels on the wireless sensors to indicate with which user they are logically paired. While this does provide some confidence to the user that they are wearing the correct wireless sensors, it does not provide the physician with the same confidence. Thus, we require a kind of proof that confirms the wireless sensors were attached to the same body.

Wireless localization

Another simple solution is to provide some means of localizing the wireless sensors to make sure they are within bodily distances. This fails for several reasons. First, it does not provide a proof as we required above. One might argue the base station could be a trusted entity to do such a localization radio traffic. However, users might not always be near the base station and the data collected away from the base station (the wireless sensors, for example, might store collected data and transmit when it range) would have no proof. Second, this trivially fails when users are close together because of the granularity of wireless localization. Finally, depending upon the frequency at which the wireless sensors communicate, the body may block all or some of the wireless signal necessary for the localization scheme.

Body-coupled communication

Prior work has explored the use of body-coupled communication is means for transmitting sensor data [2]. Body-coupled communication is means of transmitting data by way

Presented at HealthSec, August 2010.

Funded in part by NSF Trustworthy Computing award 0910842.

of the physical human body. Although this is a promising solution, the security of these types of communications is wholly unexplored. What happens, for example, if two users touch each other? The security properties of these kinds of communication channels are not well understood, and until they are we should be wary of their use.

Data-based authentication

Previous work has shown an approach for securing communications using biometrics extracted from the data of wireless sensors [3]. That is, a combination of biometrics can be used to seed a random number generator, which then can be used to derive keys. This is a promising solution because it sidesteps the problems mentioned above and it also provides a kind of proof (the derived key). Ignoring the problem of the amount of randomness in the chosen biometric data, this solution, and similar ones, fail for a simple reason: any solution that uses the data from the wireless sensors must find ways of correlating the data coming from each sensor. While it might be possible to find such correlations, it is impossible to know a priori which type of wireless sensors will be present on the body. If we expect WBANs to have heterogenous sensor types, then this problem is even more difficult. Finally, it is questionable whether every sensor can produce a biometric. For such sensors, it will be necessary to physically couple them with a sensor that can produce a biometric.

4 Proposed solution

In proposing a solution, we must remind ourselves of the requirements and potential shortcomings. Our first requirement is that the proposed solution should be energy-aware. That is, we should try to do as little sensing, computation, and transmission as necessary to accomplish the solution. Our second requirement is that we should be able to provide some proof to a physician that the data is indeed coming from the same body. Because physicians will make medical decisions based on the data collected from the WBAN, they need to have some confidence that the data is collected from the same user.

Our proposed solution takes a data-based authentication approach, but with a clever modification to the sensors. The typical problem with data-based approaches is that it is impossible to know a priori which wireless sensors the user will be carrying. However, we make the assumption that each wireless sensor will be coupled with an accelerometer. We choose an accelerometer for several reasons. They are small, cheap, require little energy to power, and, unlike some sensors, they can be placed anywhere on the body. Additionally, previous research has shown accelerometers to be effective for activity recognition [1], recognizing on-body positions of wearable wireless sensors [5], as a means for authentication [7], and even for a restricted version of the problem presented [6].

Prior work has proven a technique that can accurately detect when two devices are carried at the same position on the same body while a user is walking [6]. The solution uses coherence, a measure of how related two signals are in the frequency domain, to achieve 100% accuracy. They do provide some figures for accelerometers carried on different positions on the body (pocket/wrist) and show that they can achieve 70% success rate with the technique. Our own improved technique for locations for pocket/wrist and wrist/wrist locations achieves accuracies of 90%. However, it remains to be seen if any technique can be applied for the extreme positions on the body. One can easily imagine users wearing wireless sensors on their ankles, knees, waist, wrists, elbows, torso and head. Being able to show some correlation in acceleration for the extreme examples is an open research problem.

5 Conclusion

While we have explored only one specific problem, we believe solutions can be applied towards *usably secure WBANs*. In a usably secure WBAN, users would just fasten sensors to their body and the WBAN would secure itself with no human intervention. The sensors, for example, would determine they are collectively placed on the same body. Next, they would extract key material to secure communication channels. Finally, one or more of the sensors could identify the user using biometrics so the data can be tagged appropriately. Ideally, such a complete solution would work on a diverse population since the user is out of the loop, and, as a result, would drive the adoption of WBANs as a solution to helping monitor the health of the world's aging population.

6 References

[1] Ling Bao and Stephen S. Intille. Activity Recognition from User-Annotated Acceleration Data. In *Pervasive*, pages 1–17, 2004.

[2] Adam T. Barth, Mark A. Hanson, Harry C. Powell, Jr., Dincer Unluer, Stephen G. Wilson, and John Lach. Body-Coupled Communication for Body Sensor Networks. In *BodyNets*, pages 1–4, 2008.

[3] Sriram Cherukuri, Krishna K. Venkatasubramanian, and Sandeep K. S. Gupta. BioSec: A Biometric Based Approach for Securing Communication in Wireless Networks of Biosensors Implanted in the Human Body. In *WiSPr*, pages 432–439, 2003.

[4] Mark A. Hanson, Harry C. Powell Jr., Adam T. Barth, Kyle Ringgenberg, Benton H. Calhoun, James H. Aylor, and John Lach. Body area sensor networks: Challenges and opportunities. *Computer*, 42(1):58–65, 2009.

[5] Kai Kunze, Paul Lukowicz, Holger Junker, and Gerhard Tröster. Where am I: Recognizing On-body Positions of Wearable Sensors. In *LOCA*, pages 264–275, 2005.

[6] Jonathan Lester, Blake Hannaford, and Gaetano Borriello. "Are You with Me?"–Using Accelerometers to Determine If Two Devices Are Carried by the Same Person. In *Pervasive*, pages 33–50, 2004.

[7] Rene Mayrhofer and Hans Gellersen. Shake Well Before Use: Authentication Based on Accelerometer Data. In *Pervasive*, pages 144–161, 2007.

[8] Chiu C. Tan, Haodong Wang, Sheng Zhong, and Qun Li. IBE-Lite: A Lightweight Identity-Based Cryptography for Body Sensor Networks. *IEEE Transactions on Information Technology in Biomedicine*, 13(6):926–932, November 2009.