Critical Health Monitoring with Unreliable Mobile Devices

Minho Shin

Myongji University

Abstract. As the nation's healthcare information infrastructure continues to evolve, new technologies promise to provide readily accessible health information that can help people address personal and community health concerns. Concerns about privacy and information quality, however, may impede the development and deployment of these technologies for remote health monitoring. In this research we plan to design a framework for secure remote health-monitoring systems. Specifically, we want to *(i)* build a realistic risk model for sensor-data quality, by interacting with health professionals, *(ii)* develop protocols and mechanisms for data protection and quality assurance, and *(iii)* propose a new health-monitoring architecture that is secure despite the weaknesses of common personal devices.

1 Introduction and Relevance

The nation has an urgent need to build a national healthcare information infrastructure (NHII) that provides health information to all who need to make sound decisions about health [1]. Readily accessible and reliable health information would greatly improve everyone's ability to address personal and community health concerns. Health emergencies also require prompt and authoritative information about the situation to be readily available to those involved. Fortunately, present information technology brings us the hope that significant improvements in the public's health and well-being are not only possible but close at hand. In this research we propose to design a framework for secure remote health-monitoring systems, cutting across two core research areas of the I3P Cyber Security Research and Development Agenda: *Trust Among Distributed Autonomous Parties* and *Wireless Security*, and addressing information-security challenges in one of the nation's critical infrastructures: healthcare.

Wearable and implantable medical sensors and portable computing devices present many opportunities for providing timely health information to health providers, public health professionals, and consumers [2]. By supplying real-time health information, or extensive measurements collected continuously, a sensor-based health-monitoring system complements the current healthcare information infrastructure – which is based on relatively static, sparsely collected information in the patient's medical records. A remote health-monitoring system may help to reduce the *cost* of healthcare [3] and to simultaneously improve the *quality* of the healthcare; patients may spend less time in the hospital and yet have more detailed health data, measured by wearable sensors as they go about their daily activities; caregivers can more quickly react to the medical emergencies of elders; trainers can analyze a trainee's fitness level; and consumers can maintain their own health and wellness.

Privacy and information quality, however, are two major concerns in the development and deployment of remote health-monitoring systems [4, 5]. To be viable, any such system must provide *usable* devices that respect patient *privacy* while also retaining data *quality* required for the medical purpose it serves. There are many opportunities for the data to become lost, damaged, forged, or exposed: patients may fail to apply sensors correctly, leading to medically incorrect readings; the patient's device may be misplaced, stolen, or compromised, causing the medical data stored in the device to be divulged [6]; the sensor data may travel across multiple devices and networks before it is presented to the medical team. The problem is especially challenging, given the difficulty of hardening low-cost sensors and the personal devices that collect, process, and forward the medical data, and given that all such devices will communicate over wireless networks.

In our research, we will address these issues by designing a framework for secure remote health-monitoring systems. Given the time available (one year), we will focus most on the data-quality issues. Specifically, we want to *(i)* build a realistic risk model for sensor-data quality, by interacting with health professionals, *(ii)* develop protocols and mechanisms for data protection and quality assurance, and *(iii)* propose a new health-monitoring architecture that is secure despite the weaknesses of common personal devices. For evaluation, we will implement a proof of concept for secure health monitoring.

2 Challenges and our Approach

2.1 Risk Analysis

To design a secure health-monitoring system, we first need to understand what determines the quality of the medical sensor data and how we can quantify the degree of the data quality. Specifically, we want to identify factors that affect the data quality and then analyze to what extent they influence the data quality. Others have described overall security challenges in health-monitoring systems [4], and initial ideas for protecting health-data integrity [7], but an in-depth and realistic analysis of the problem is lacking in the literature.

As a preliminary analysis, we recently identified eleven factors that can affect the quality of medical sensor data [5] (see next section for detail). To ensure or evaluate the data quality of a health-monitoring system, one should take these factors into account. Without knowledge of physiology and practical concerns, however, it is difficult to quantify to what extent each factor will contribute to the data quality.

In our research, we plan to exploit the collaboration to hold conversations with health professionals there, refining the above list of risk factors and developing our data-quality risk model so it can answer the following questions:

- “What are the high-priority concerns for achieving high-quality medical data?”
- “How much does each factor contribute to the data-quality problem?”
- “How can we evaluate and possibly improve the data quality?”

2.2 Quality control

To design a quality-control framework, we first analyzed the health-monitoring system as a sequence of processes, assigned related factors to each process, and then identified possible methods for the quality control of individual factors. Medical sensing begins with sensing the physiology of the patient (*Sense* process). Each sensor generates sensor data at a certain rate and transmits them to the device through a wireless connection (*Transfer* process). The monitoring device collects data from sensors, processes them as needed (*Collect* process), and then forwards them to the provider (*Transfer* process). Upon receiving the data from the device, the provider’s server evaluates the validity of the data (*Verify* process) and then presents the data to the provider. When it presents the data, the server also presents the level of the data quality to the provider (*Assess* process). In the following, we discuss our analysis in more detail. (For brevity, we skip the factors that are self-explanatory.)

- *Accuracy*: the accuracy of a sensor depends on its design and manufacturer (i.e., sensor profile), the time since the latest calibration, and the age of the sensor. The data quality depends on the accuracy expressed by the expected error bound.
- *Granularity*: the quality of sensor data also depends on the level of detail that a sensor can provide.
- *Application*: the data quality also depends on correct application of the sensor to the body; if the sensor is not correctly applied to the body, it generates incorrect sensor data. If the patient is responsible for the application, the quality of sensor application depends on the patient’s ability and diligence. The patient’s ability depends on the education, age, and prior experience. When a sensor is incorrectly applied, the data is likely to deviate from the range of values that are considered *reasonable* as a physiological value. We call this reasonableness of the medical data *soundness*. The soundness of data includes physiological soundness and contextual soundness; we explain these in more detail below where we explain the verification process.
- *Synchronization*: it is often medically necessary to collect multiple sensor readings of different modalities, and a health professional can derive a medical condition from their combination. For the combination to be useful the sensor readings should be temporally synchronized. If sensors cannot timestamp each data, the device should do so, but it should also make sure that the sensor data is sampled at that moment (i.e., not replayed by an adversary). The data quality depends on the granularity of the synchronization.
- *Information loss by aggregation*: communication is costly. To save the amount of information to be sent, the device can aggregate sensor readings before

sending (e.g., reporting the average per minute). However, every aggregation loses some information in data and the quality of data depends on the amount of information lost by the aggregation.

Most factors related to sense, collect, and transfer processes are syntactic (except sensor application); they depend little on the semantics of the medical data. For example, one can protect message integrity without knowing the meaning of the data contained in the message. However, medical data has rich semantics that can determine what data is *sound* as medical data. The verification process exploits the semantics of the medical sensor data to verify if the data is appropriate, useful, or acceptable for the purpose of health monitoring.

- *Patient authentication*: patient authentication verifies whether the sensors are monitoring the right person. Biometric data (e.g., fingerprint) is simple and accurate but its permanence can raise a privacy issue. We can also compare the data with the patient's past data or the medical profile (e.g., disease or weakness) to verify the patient's identity. The data quality depends on the likelihood that we are monitoring the right person.
- *Physiological soundness*: a physiological data cannot take arbitrary values. One can check if the value falls in a reasonable range (*range check*), if it is coherent with the known probability distribution (*probability distribution*), if its temporal change exhibits a reasonable behavior (*auto-correlation*), or if sensor values of different modalities accord with the known correlations between them.[1]
- *Contextual soundness*: Like physiological soundness, we can verify the data quality by comparing the medical data with some context data such as body movement, location, or temperature. For example, the acceptable values for heart-rate or blood pressure are different when the patient is running or sleeping.

When quality verification fails, the quality of incoming data becomes uncertain. Even if all the verifications succeed, there are many opportunities for data to become incorrect (see Figure **??**). To deal with the uncertainty, the providers need to know how much they can trust the data and what is causing the problem. The *assessment* process takes all the factors into account and judges the current level of the data quality, and presents that judgment to the provider.

Prior work on data integrity in health-monitoring systems focused on detecting packet loss [8], improving false positives using sensor correlation [9], or categorizing the data quality into four discrete states based on observed error and lack of data [10]. Giani et al. [7] proposed a broad range of methods for data validation but only basic concepts were proposed. Compared to prior work, our approach attempts to provide a generic framework for the quality control of a health-monitoring system.

[1] Such an anomaly can also signify a medical problem of the patient, and the verification methods can also apply to the problem of anomaly detection. However, such "emergency detection" is outside the scope of this work.

DS-Theory has many uses; for example, it was recently used for evaluating the performance of intrusion detection systems (IDS) [11]. While they simply combined the partial judgments that are provided by existing IDS schemes, our work will actually define belief functions for each factor and also explore other possibilities for combining partial results, seeking methods that fit better to health-monitoring applications.

2.3 Architecture

So that patients need not carry a dedicated monitoring device, we want to leverage the mobile device they already carry: their cellphone. Mobile phones are increasingly powerful, effectively personal computing devices with substantial computation, storage, and networking capabilities. Furthermore, they are increasingly able to sense location (GPS), motion (accelerometer), light, proximity, temperature, sound (microphone), and video (camera). The use of existing devices has advantages in deployment cost and usability [12].

On the contrary, turning a personal device to a health-monitoring device also has challenges. First, personal devices are diverse in software platform and security mechanism. The developer must adapt to the wide variety of features (and varying degrees of security) on mobile platforms such as Windows Mobile, Mac OS X, and Symbian. Although some future platforms may have strong security support such as a TPM [13, 14], a TPM may not allow the patient to install monitoring software without going through a complicated platform-certification process.

To address these challenges and yet still leverage the patient's mobile phone as a platform, we plan to design a novel architecture that decouples the monitoring component from the personal device. Suppose the health provider distributes small *health-monitoring units* (HMU) to patients and asks them to keep the unit plugged into the device through a common interface such as SD card, miniUSB, or SIM card.[2] The HMU can store secret keys and compute some cryptographic functions (as SIM card can do in today's GSM phones). As shown in The unit can authenticate sensors (*authenticator*) and verify the authenticity of sensor data forwarded by the monitoring software (*auditor*). When needed, it aggregates sensor data before sending to the provider (*fusor*). The HMU adds message authentication codes to messages sent to the provider and, without HMU, the device cannot prove authenticity of the sensor data to the provider. The HMU makes the health-monitoring portable from device to device, easy to manage, and hard to compromise; there are many opportunities for adversaries to access the device through software attacks [6], while it requires a hardware attack to compromise the HMU [15].

[2] Although not all current phones have expansion slots, and GSM phones only have one SIM-card interface, we imagine next-generation mobile phones that have a standard expansion slot of similar form factor and capability to these examples.

References

1. Detmer, D.E.: Building the national health information infrastructure for personal health, health care services, public health, and research. BMC Med. Inform. Decis. Mak. **3** (January 2003)
2. Jurik, A.D., Weaver, A.C.: Remote medical monitoring. Computer **41**(4) (2008) 96–99
3. Dimmick, S.L., Burgiss, S.G., Robbins, S., Black, D., Jarnagin, B., Anders, M.: Outcomes of an integrated telehealth network demonstration project. Telemedicine Journal and e-Health **9**(1) (March 2003) 13–23
4. Stanford, V.: Pervasive health care applications face tough security challenges. IEEE Pervasive Computing **1**(2) (2002) 8–12
5. Sriram, J., Shin, M., Kotz, D., Rajan, A., Sastry, M., Yarvis, M.: Challenges in data quality assurance in pervasive health monitoring systems. In Gawrock, D., Reimer, H., Sadeghi, A.R., Vishik, C., eds.: Future of Trust in Computing. Lecture Notes in Computer Science. (July 2009)
6. Ghosh, A.K., Swaminatha, T.M.: Software security and privacy risks in mobile e-commerce. Communications of the ACM **44**(2) (2001) 51–57
7. Giani, A., Roosta, T., Sastry, S.: Integrity checker for wireless sensor networks in health care applications. In: Proceedings of the Second International Conference on Pervasive Computing Technologies for Healthcare. (2008) 135–138
8. O'Donoghue, J., Herbert, J., Fensli, R., Dineen, S.: Sensor validation within a pervasive medical environment. In: Proceedings of the IEEE Conference on Sensors. (Oct. 2006) 972–975
9. Chen, C.M., Agrawal, H., Cochinwala, M., Rosenbluth, D.: Stream query processing for healthcare bio-sensor applications. In: Proceedings of the 20th International Conference on Data Engineering. (April 2004) 791–794
10. Peter, C., Ebert, E., Beikirch, H.: A wearable multi-sensor system for mobile acquisition of emotion-related physiological data. In Tao, J., Tan, T., Picard, R.W., eds.: ACII. Volume 3784 of Lecture Notes in Computer Science., Springer (2005) 691–698
11. Thomas, C., Balakrishnan, N.: Mathematical analysis of sensor fusion for intrusion detection systems. In: The First International Conference on Communication Systems and Networks. (January 2009)
12. Mann, W., Helal, S.: Smart phones for the elders: Boosting the intelligence of smart homes. In: Proceedings of the AAAI Workshop "Automation as Caregiver: The Role of Intelligent Technology in Elder Care", AAAI Press (2002) 74–79
13. : Mobile Phone Work Group, Trusted Computing Group https://www.trustedcomputinggroup.org/groups/mobile.
14. : TCG Mobile Trusted Module Specification, Revision 1 https://www.trustedcomputinggroup.org/specs/mobilephone/tcg-mobile-trusted-module-1.0.pdf.
15. Clavier, C.: Side channel analysis for reverse engineering (SCARE) – an improved attack against a secret A3/A8 GSM algorithm. Cryptology ePrint Archive, Report 2004/049 (2004)