Biometrics for Authentication in Resource-Constrained Systems

Nima Karimian, *Student Member, IEEE*, Mark Tehranipoor, *Senior Member, IEEE*,
Damon Woodard, *Senior Member, IEEE,* and Domenic Forte, *Member, IEEE*

***Abstract* — Remote healthcare monitoring (RHM) can be more convenient and alleviate health care costs, but is currently limited by the growing need for security under heavy resource constraints. A complete paradigm shift in how we design algorithms, architectures, and tools is needed to overcome these issues.**

I. Introduction

With the rapid growth in population of persons over the age of 65, the cost of health care is increasing at an alarming rate. Remote healthcare monitoring (RHM) [1], such as wireless body area sensor network (WBSN) and mobile health monitoring systems [3], promises to alleviate these costs and could have a variety of benefits to both patients and health care providers. While there has already been some progress in developing preliminary and prototype systems for RHM (e.g., portable ECG [5], blood oxygen saturation measurement [3]. efficient microcontroller units (MCUs) for wearable sensing [2], etc.), many critical security and resource related challenges remain. These include

- *Privacy:* Health related data is personal and must be kept private, thereby requiring cryptographic algorithms, protocols, and authentication policies for access control.
- *Risks of Fraud:* Due to the lack of physical presence at the time of collection, the identity of the user that transmits the respective information is uncertain, which increases the risk of identity fraud in health care [7]. The best form of mitigation is through continuous biometric measurement which can be captured along with medical information. To date, many suitable biometrics (e.g., ECG and PPG) suffer from considerable noise. This demands more processing and secure storage of biometric templates.
- *Hardware Attacks:* RHM systems can be involved in sensitive and life-critical tasks, and are therefore susceptible to a growing number of hardware issues such as counterfeit electronics and hardware Trojans [8]. In addition, side channel attacks (SCAs) can extract secret information (such as keys) based on physical implementation of the hardware- though timing, power, electromagnetic emanation and faults analysis [4].

The devices used for RHM are predominantly implantables, wearables, and/or smart phones which have a range of different resource constraints (hardware, size, weight, power sources, etc.). Thus, managing these security issues under such constraints is a challenging task.

II. Potential Solutions

The above security needs and requirements for continuous monitoring and wireless transmission are coupled, but have been dealt with independently until now. To address these challenges, what is needed is a complete paradigm shift that supports co-optimization of these competing elements in RHM systems. In this paper, we highlight potential solutions at the hardware level as instances of this paradigm shift:

1) *HW Personalization of Biometrics:* The traditional methods for biometric authentication aim to find a universal process for all users in a population, but this is ineffective and inefficient. We have recently developed an approach that is adaptable to the population itself (to preserve entropy) while also being adaptable to individual users (to improve reliability). Our approach was recently demonstrated on ECG, iris, and face data from publically available databases and produced strong results [9]. We are currently developing noise analysis methods and extending the above paradigm to achieve improved trade-offs between pre-processing and post-processing hardware on a user-to-user basis through reconfigurable hardware.
2) *Secure HW Design Tools:* The rapid scaling and time-to-market for today's semiconductors (with billions of transistors) are enabled by electronic design automation (EDA) tools. Such tools are capable of balancing area, power, timing, etc. requirements, but not yet security. We are currently developing metrics, rules, and tools that expand the capabilities of EDA to include hardware security as an additional design parameter. In doing so, co-optimization of security vs. resources will finally be possible.

Together, we expect these approaches to obtain better biometric authentication accuracy and greater levels of security in a more resource efficient manner.

References

[1] S. Sharma and V. Balasubramanian. "A biometric based authentication and encryption Framework for Sensor Health Data in Cloud." *ICIMU,* 2014.
[2] Chen et al. "Wireless body sensor network with adaptive low-power design for biometrics and healthcare applications." *IEEE Systems Journal*, 2009.
[3] Walker et al., "Mobile health monitoring systems." *Engineering in Medicine and Biology Society*, 2009.
[4] D.L. Delivasilis and S. K. Katsikas. "Side Channel Analysis on Biometric-based Key Generation Algorithms on Resource Constrained Devices." *IJ Network Security*, 2006.
[5] Moulton et al. "Ambulatory health monitoring and remote sensing systems to be used by outpatients and elders at home: User-related design considerations." *Healthcom*, 2009.
[6] M. Kamaraju and P. A. Kumar, "DSP based embedded fingerprint recognition system," *HIS*, 2013.
[7] Agrafioti et al., "Secure Telemedicine: Biometrics for Remote and Continuous Patient Verification, *Journal of Computer Networks and Communications*, 2012.
[8] M. M. Tehranipoor et al. *Counterfeit Integrated Circuits: Detection and Avoidance*. Springer, 2015.
[9] Guo et al., "Hardware Security Meets Biometrics for the Age of IoT", to appear *ISCAS*, 2016.

N. Karimian, is with the department of Electrical and Computer Engineering, University of Connecticut, CT, 06269 USA (corresponding author to provide e-mail: nima@engr.uconn.edu).

M. Tehranipoor, D. Woodard, and D. Forte, are all with the department of Electrical and Computer Engineering, University of Florida, FL, 32611 USA (e-mail: tehranipoor@ece.ufl.edu, dwoodard@ufl.edu, dforte@ece.ufl.edu.).