Hardware Security Meets Biometrics for the Age of IoT

Zimu Guo
ECE Dept., University of Florida
Email: zimuguo@ufl.edu

Nima Karimian
ECE Dept., University of Connecticut
Email: nima@engr.uconn.edu

Mark M. Tehranipoor and Domenic Forte
ECE Dept., University of Florida
Email: {tehranipoor,dforte}@ece.ufl.edu

***Abstract*—The Internet of Things (IoT) is a concept that involves connecting endpoint devices and physical objects to the Internet. While IoT is envisioned to dramatically increase convenience in our daily lives, it could also result in catastrophic economic and safety issues. Considering the applications envisioned for IoT (smart cities, homes, retail, etc.), security must be handled with great care and should start from the bottom up (i.e., from the hardware level). As a good deal of IoT devices require interaction between devices and humans, biometrics provide an interesting opportunity for improving both the convenience and security in IoT applications. In this paper, we consider the potential benefits and challenges associated with incorporating biometrics into IoT. We combine novel biometrics, such as ECG and PPG, and system-level obfuscation approaches to prevent reverse engineering, tampering and unauthorized access of IoT devices and other electronic systems. Our preliminary results are promising and motivate future work in this area.**

I. Introduction

The Internet of Things (IoT) is a concept that involves networking of endpoint devices and physical objects to increase the convenience and efficiency of our everyday experiences [1]. The IoT ecosystem includes life-changing applications, such as smart homes, buildings, cities, retail, transportation, and public safety. Forward thinking organizations are also interested in the opportunities for new revenue made possible by IoT. That being said, critics are skeptical and question whether or not the world is ready to add IoT devices to the Internet. Our current cybersecurity landscape is already rife with well-publicized breaches, often committed remotely. IoT devices integrated into home and enterprise networks represent new, possibly dangerous entry points for malicious actors. Therefore, it is of the upmost importance that we design IoT devices and systems with security in mind.

While a large amount of research focuses on the security between IoT devices, the interaction of IoT devices with their owners is often neglected. Controlling IoT devices remotely is a fundamental aspect of IoT, but access to them must be handled carefully. For instance, IoT devices in industrial control applications could handle critical tasks such as monitoring of air toxic gases and air quality, temperature control of fridges with sensitive merchandise, etc. Tampering with such devices could lead to significant economic losses and even have life-threatening consequences. With the billions of IoT endpoints projected to exist in the near future [1], traditional forms of access control like passwords are outmoded. Strong passwords are already difficult to remember, let alone with so many devices. Passwords are also vulnerable to guessing. Although dongles, smart cards, etc. are becoming more popular, their theft and misuse are threats. Biometrics are a more appropriate option and have several major benefits: (i) they are more convenient than passwords, maintaining the spirit of IoT; (ii) if appropriately selected, they could have low probability of circumvention; (iii) besides access control, they could be used to enhance many IoT applications. Furthermore, the recent advancements in low cost sensor technologies makes the use of biometrics more feasible than ever.

In this paper, we discuss the opportunities and challenges for biometrics in IoT. In Section II, we discuss biometrics, including emerging ones such as electrocardiogram (ECG) and photoplethysmograph (PPG), and their application to IoT. In Section III, we discuss a recent approach we have developed that prevents unauthorized access to electronic systems through obfuscation, and then combine it with biometric-generated keys for enhanced security. Section IV discusses preliminary results for biometric keys and obfuscation. We conclude in Section V.

II. Biometrics in IoT

Biometrics have been investigated with respect to identification, authentication, and key generation for many years [2]. Fingerprints are very popular (e.g., login to modern laptops) due to their low-cost implementation and well-developed feature extraction approaches. Iris is acclaimed for its high accuracy and fast verification time, providing unique features even for identical twins. Face recognition systems, given their noninvasive nature, are more heavily utilized for surveillance purposes. While these biometrics are more common, many are vulnerable to circumvention. For example, fingerprints are very easy to obtain (they are left on everything we touch) and can be used to bypass biometric systems.

Electrocardiogram (ECG) and photoplethysmogram (PPG) are cardiovascular biometrics that are emerging as interesting choices for biometric systems. They are exceptionally difficult to acquire, copy, and circumvent without user approval. The ECG signal represents electrical activity related to heart muscle depolarization and can be measured using low cost smart devices and wearables these days. Similarly, PPG detects the heart depolarizing and blood pressure changes. Since these biometrics are physiological in nature, they may also provide information beyond simple identification, such as demographic (age, sex, etc.) and health related information [3].

A. Forward-Thinking Biometrics-based IoT Applications

Binding IoT devices with biometrics could improve the security and convenience of current IoT applications as well as enable new ones. Some of the services/applications we envision are shown in Figure 1. Note that we focus on ECG, PPG, face, and fingerprint which seem to be the most appropriate for IoT due to cost, ease-of-measurement, etc. Fundamentally, these biometrics carry information about user identity and

characteristics, which could have significant benefits to consumers, organizations, and general public safety. In consumer

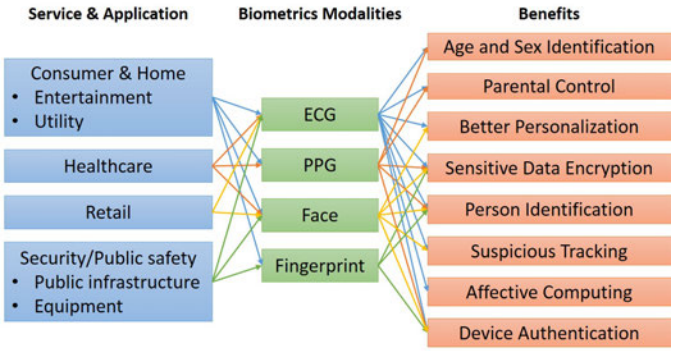

Fig. 1: IoT Related Applications

applications, biometric-based identity can enable seamless personalized experiences without the need for clumsy logins and passwords. Through biometrics-based access control, personal laptops, smart phones, implanted medical devices [4], etc. will be able to recognize their owners and only operate in their hands (more in next section). Biometrics like ECG and PPG are also correlated with user age and sex. One can imagine parental controls for smart computing devices and TVs that automatically restrict inappropriate content based on age. The health information contained in ECG and PPG could also be used to alert users to seek medical attention if cardiac issues and arrhythmias are detected. User information can be protected in previously unimaginable ways. For instance, keys generated from biometrics can encrypt sensitive data in a way that ensures that it may only be decrypted by the authorized user with high confidence.

The demographic information obtained by biometric systems embedded in electronics could be used by organizations to characterize the age or sex distributions of consumers and improve marketing. Similarly, biometrics that can be obtained non-invasively (e.g., face and possibly ECG) could be used by retailers to collect such information from customers as they walk through aisles. In the IoT-enabled world, long lines and registers may also be a thing of the past. By reading RFID tags embedded in products and user biometrics, customers can be automatically charged as they leave a store with items. Similar benefits extend to healthcare as well. For instance, patients that don't adhere to prescribed medication can cost billions of dollars per year [5]. Similar RFID+biometric enabled systems can be used to remotely monitor patients and ensure they take proper doses.

In the domain of public safety, biometrics and IoT can have substantial benefits too. The most straightforward benefit is access control for buildings, schools, campuses, military bases, etc. For example, electronic door locks can be controlled by biometrics. Disasters (such as those related to recent gun-violence) could be avoided entirely or mitigated with automated biometrics-based tracking and surveillance at entrances. Authorities could use the information to identify individuals that do not belong and locate them more quickly during a crisis. Biometrics can also be used for affective computing where information contained in biometrics (e.g., face, ECG) characterizes the emotional state of individuals. Those who are suicidal, violent, etc. could be identified to prevent crises [6].

B. Challenges

While the above applications are promising, incorporation of biometrics is challenging.

- *Biometric Reliability.* Noise introduced by the sensors capturing the biometric and the impact of stress, exercise, health, etc. (in physiological biometrics) reduce the accuracy of identification and key generation.
- *Biometric Template Protection and Revocability.* If passwords or dongles are hacked or stolen, it is possible to replace them. Biometrics on the other hand are permanent and more difficult to revoke if compromised.
- *Privacy.* Biometrics in the above applications could be used maliciously to invade user privacy. A careful balance needs to be met between use of biometrics and privacy through both policies and technological solutions.
- *Low Cost Signal Processing and Feature Extraction.* Most IoT devices are simple, low-cost devices with little power. Algorithms that extract unique and reliable features from biometrics for identification, key generation, etc. and can be deployed in resource constrained systems are needed.

In the next section, we present approaches that may partially address these challenges.

III. Human-to-Device (H2D) Authentication

In this section, we discuss an approach that we refer to as Human-to-Device (H2D) authentication where a system is locked in a way that it can only be unlocked by the appropriate user.

A. Board-level Obfuscation

Printed Circuit Boards (PCBs) are used extensively to provide mechanical support and electrical connections to system chips and components in nearly every electronic system. IoT devices will be no different. We have developed a novel PCB level approach [7] (shown in Figure 2) which could be extremely useful against reverse engineering and unauthorized access of electronic systems. The only requirement is one additional chip that acts as a permutation block between programmable component (MCU, DSP, FPGA, etc.) and other non-programmable components. Through the permutation block, the true connections between components (and the overall system functionality) are obscured. Not all the connections will be obfuscated since some of the connections are associated with some dedicated ports on MCU and obvious to tell from the documentation. A key is loaded into the permutation block in order to establish the correct connections in the system and enable correct functionality. Provided that the key remains protected, our approach could therefore prevent attackers from learning the design through reverse engineering. The strength of obfuscation is evaluated on several industrial benchmarks in Section IV.

H2D can be accomplished as follows. Firmware is downloaded to the chip and obfuscates the PCB so that only the system owner's biometric will unlock it. Instead of directly inputting the key to the permutation chip, the biometric is used as input instead. Features are extracted from the biometric within the permutation chip to generate the key that unlocks the PCB. Depending on the biometric modality used, it could be very difficult for an attacker to obtain the owners biometric and use/access the system. Note that the proposed H2D approach is very different from other system or software level

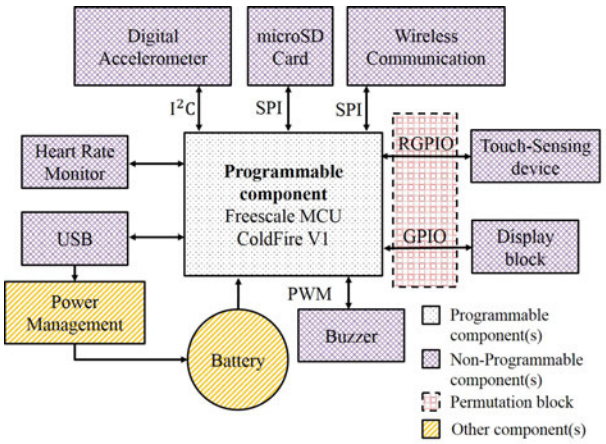

Fig. 2: Block diagram of Freescale's activity monitor reference design based on Freescale ColdFire V1 MCF51MM256CLL MCU

approaches. Traditional methods for user authentication require comparing the input credentials/keys with the ones stored in a systems non-volatile memory. However, for IoT devices, traditional methods could be risky since credentials/keys could be invasively extracted [8]. In the proposed approach, the key is only temporarily stored in the IoT device's volatile memory. Any attack on the system is likely to require removal of power which would destroy the key. We assume that the user unlocks the device at every use with his/her biometric. The key can timeout after a prespecified time.

B. Biometrics Based Key Generation

As mentioned earlier, keys generated from biometrics may suffer from environment/measurement noise, internal instability, and so on which could introduce binary errors during key generation process and make it impossible for even the system owner to access/use the system. In order to overcome these detriments, we have developed a statistical approach to mitigate or eliminate the intra-subject variance while preserving privacy and generating long keys.

Our approach begins with an initialization phase. Raw ECG or other biometric signals are preprocessed to remove noise and features are extracted from a large population of users. The feature distribution of population is normalized to $\mathcal{N}(0,1)$ after enrollment and the feature distributions of subjects (e.g. Sub 1 to 3) are normalized by the parameters pre-computed during population normalization. These statistical parameters generated from each feature and designer-defined control parameters are used to determine thresholds and boundaries. The number of quantized bits for one feature depends on the boundaries, and can vary from feature to feature. The boundaries (b_0, b_1, b_2) and thresholds (t_0, t_1) are calculated by satisfying two constraints at the same time. The first constraint is randomness. This constraint can be realized by making selected features have equal probabilities when quantized to different binary symbols. The second constraint is reliability which can be realized by minimizing the shaded region (shown in the insight area in Figure 3). Boundaries and thresholds of an arbitrary feature for a 2-bit quantization case are shown in Figure 3. Once these boundaries are determined, users can be enrolled. Since certain features may be reliable for some but unreliable for others, our approach will only use reliable features from each individual. Reliable features are determined based on the above thresholds. The features selected for a user are stored as helper data for each enrolled subject. The thresholds and helper data from initialization and enrollment phases are used with the supplied biometrics to handle key regeneration in the permutation block at run-time.

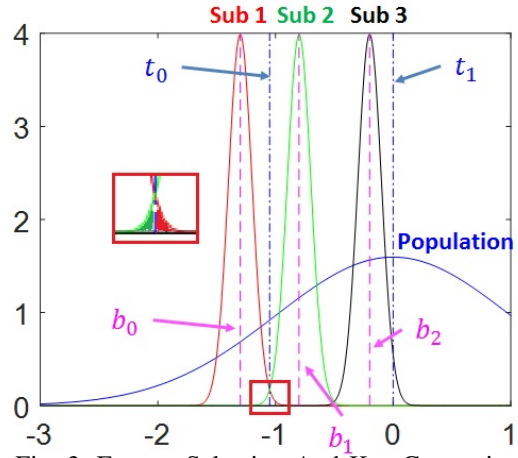

Fig. 3: Feature Selection And Key Generation

We should also note that using biometrics for personal identification does raise three systematic privacy concerns [9]: unintended functional scope; unintended application scope, and covert recognition. These privacy concerns can be solved in several ways [9]: legislation by governments and the public; assurance of self-regulation and autonomous enforcement by independent regulatory organizations. Additionally, in certain applications, using the biometrics can be mandatory by law.

IV. Simulation Results

A. Board-Level Obfuscation

We implement the board-level obfuscation suggested in Section III-A on 5 industrial benchmarks from Texas Instruments (TI). The outcomes are shown in Table I. **I/O** column represents the numbers of input and output signals handled by the permutation block (based on the original system design). **R only** and **R&D** imply the types of original connections the obfuscation algorithm would accept. **R** refers that the algorithm only considers the connections originally connected before the obfuscation scheme is applied, while **R&D** means the algorithm exploits all connected and unconnected ports on MCU (i.e., dummies). Generally speaking, the more ports are engaged in obfuscation, the better the performance is. **Combinations** shows the total input/output combinations the attacker needs to try in order to find the true connections.

TABLE I: Obfuscation strength evaluation

Design #	I/O	Combinations	
1	35/35	R only	1.0e40
2	30/13	R&D	7.5e17
3	34/24	R&D	8.1e31
4	17/17	R only	3.6e14
5	32/28	R&D	1.1e34

TABLE II: Multiple keys and probability analysis

	# of multi. keys	Probability
Min.	32768	1.47E-39
Max.	1.8E+19	8.27E-25
Mean	8.2E+07	3.67E-36

According to Table I, most of the designs offer huge numbers of the combinations excluding design number 4. Since the algorithm carefully chooses the obfuscation candidates, attackers could only examine all possible combinations. We

expect the time for an attacker to break the obfuscation scheme through brute force to be thousands of years.

To implement the permutation block, Benes network is selected for the reason of full permutation capacity and acceptable area overhead. Benes network is composed by an array of 2-to-2 switches. Each switch is controlled by one key bit (1-bit binary number). According to the nature of Benes network, the key space is much larger than the input/output combinations space. In other words, one input/output combination can be realized by multiple keys. This phenomenon is defined as the multiple-key effect, which may potentially benefit the attackers in breaking the obfuscation. In order to study the effect of multiple keys, we achieved 1e6 random input/output configurations as proposed in [10] on a 32-bit Benes network. In Table II, we provided the minimal, maximal and expected numbers of multiple keys and the probabilities of breaking the obfuscation with a single attempt. The total input/output combinations of a 32-bit Benes networks is $32! = 2.63E35$ and the corresponding breaking probability is $1/32! = 3.80E-36$. Comparing this value with the expected probability in Table II, the breaking probability becomes even smaller by implementing Benes network. As a result, we can conclude that Benes network will not diminish the obfuscation strength. The attacker would always try to examine the input/output combinations instead of the keys.

B. Biometrics Based Key Generation

We employ proposed key generation algorithm on ECG, iris and face in this section. Public databases are available for ECG [11], iris [12] and face [13]. We compare the quality of generated keys by two evaluation criteria: (i) **Reliability**, which is the bitwise similarities between enrolled key and regenerated keys. The reliability (R) can be computed using (1).

$$R = 1 - \frac{1}{N}\sum_{n=1}^{N} HD(key_{en}, key_{re}^{n}) \tag{1}$$

where key_{en} and key_{re} indicate the enrolled and N regenerated keys respectively. HD (Hamming distance) means the percentage of bitwise difference between two binary chains. (ii) **Min-entropy** (E), which is a randomness indicator calculated by (2).

$$E = \frac{1}{N}\sum_{n=1}^{N} \log_p \min_{k=1}^{K}(Prob\{sym_k^n\}) \tag{2}$$

where p is a parameter specified by different quantization scenarios (1 bit, 2 bits or 3 bits). $Prob\{sym_k^n\}$ represents the probabilities of different symbols during nth key regeneration. Symbols are defined as the binary entries, which feature elements can be quantized to. For example, the symbols are '1' and '0' for 1-bit quantization case. For 2-bit case, the symbols are '00', '01', '10' and '11'. Since only a small number of features will be quantized into 2 or 3 bits by the nature of the feature elements, the entropy estimate is not accurate. Hence, we only compare the entropy denoted by 1-bit case for performance evaluation.

Reliability and entropy are both desired to be close to 1 for a good intra-class stability and inter-class randomness. We fix the control parameters and present the results in Table III. These control parameters let the designer control the expected randomness and reliability. Fixing these parameters means the expected key generation performances for different biometric modalities are the same.

TABLE III: Reliability and Entropy Analysis of Biometric Based Key Generation Algorithm

Biometric Modalities		Normal ECG	Iris	Face
Reliability	Average	0.994	0.953	0.959
	Minimal	0.979	0.906	0.826
	Maximal	1.000	1.000	1.000
Entropy	1-bit	0.7431	0.8550	0.7723
	2-bit	0.5187	0.0100	0.4898
	3-bit	0.2826	0.0000	0.1342
Average Key length		418	168	71

Comparing the three biometric modalities on average, ECG provides the longest key and highest reliability while iris exhibits the highest 1-bit entropy. ECG is likely the best candidate for our key generation approach due to its high quality and difficulty to circumvent. Comparing with the cumbersome high-definition cameras utilized to capture iris images, capturing ECG signals only requires small and lightweight sensors.

V. Conclusion and Future Work

This paper presented various benefits and challenges introduced from biometrics in IoT. The approach we demonstrate for access control is promising and will be investigated more in future work. By incorporating physical obfuscation, the biometric template need not be stored in the IoT device making it more resistant to attack. Keys generated from ECG by our algorithm exhibit encouraging reliability and leak little information for attackers. In the future, we will focus on multi-user access of one obfuscated device. We will also try to improve the reliability and entropy of abnormal ECG signals.

VI. Acknowledgment

Portions of the research in this paper use the CASIA-IrisV1 collected by the Chinese Academy of Sciences' Institute of Automation (CASIA) [12].

References

[1] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of things (iot): A vision, architectural elements, and future directions," *Future Generation Computer Systems*, 2013.
[2] R. Kannavara and K. Shippy, "Topics in biometric human-machine interaction security,," *Potentials, IEEE,*, 2013.
[3] S. Ergin, A. Uysal, E. Gunal, S. Gunal, and M. Gulmezoglu, "Ecg based biometric authentication using ensemble of features," in *CISTI*, 2014.
[4] M. Rostami, A. Juels, and F. Koushanfar, "Heart-to-heart (h2h): authentication for implanted medical devices," in *CCS*, 2013.
[5] M. T. Brown and J. K. Bussell, "Medication adherence: {WHO} cares?" *Mayo Clinic Proceedings*, 2011.
[6] P. K. Davis, W. L. Perry, R. A. Brown, D. Yeung, P. Roshan, and P. Voorhies, *Using Behavioral Indicators to Help Detect Potential Violent Acts*. RAND Corporation, 2013.
[7] Z. Guo, M. Tehranipoor, J. Di, and D. Forte, "Investigation of obfuscation-based anti-reverse engineering for printed circuit boards,," in *DAC*, 2015.
[8] S. P. Skorobogatov, "Semi-invasive attacks: a new approach to hardware security analysis," Ph.D. dissertation, 2005.
[9] S. Prabhakar, S. Pankanti, and A. K. Jain, "Biometric recognition: Security and privacy concerns," *IEEE S & P*, 2003.
[10] D. Nassimi and S. Sahni, "Parallel algorithms to set up the benes permutation network," *Computers*, 1982.
[11] A. L. Goldberger, "PhysioBank, PhysioToolkit, and PhysioNet: Components of a new research resource for complex physiologic signals," *Circulation*.
[12] "Casia-irisv1, http://biometrics.idealtest.org/," 2015.
[13] "Face recognition grand challenge (frgc)," 2015.