Human-to-Device (H2D) Authentication Using Biometrics

MohammadReza Hosseinzadehketilateh, Sara Tehranipoor, and Nima Karimian
Lane Department of Computer Science and Electrical Engineering
West Virginia University
Morgantown, USA
mh00136@mix.wvu.edu and nima.karimian@mail.wvu.edu

2024 Silicon Valley Cybersecurity Conference (SVCC) | 979-8-3503-8314-0/24/$31.00 ©2024 IEEE | DOI: 10.1109/SVCC61185.2024.10637372

***Abstract*—An increasing array of intelligent computing devices operate within vulnerable environments where they are susceptible to capture or physical assault. The data and intellectual property (IP) stored within these devices are often compassionate. This paper explores the potential advantages and challenges of integrating biometrics into electronic devices. By combining cutting-edge biometrics, such as physiological data, with innovative system-level obfuscation techniques, we aim to prevent hardware attacks. We term this approach human-to-device (H2D) authentication. ECG biometrics offer high security as they are difficult to replicate or guess, making them ideal for high-stakes applications. ECG biometrics are easy to use, as they only require a few seconds of ECG signal recording, making them a convenient option.**

***Index Terms*—H2D, Bimetrics, Security, Authentication, Obfuscation**

I. Introduction

The widespread adoption of smart computing devices (such as smartphones, smart glasses, and wearables) and the growing Internet of Things (IoT) ecosystem [1] have made secure operation in hostile and unprotected environments a top priority. In military contexts, smart devices play a crucial role in gathering information, rapid information dissemination, tracking troop health and safety, providing navigation and instructions (e.g., through augmented reality displays [2]), and more. In healthcare, the use of smart medical devices and wearables has revolutionized patient care, enabling remote monitoring and personalized treatment. However, these devices also pose significant security risks, as they often contain sensitive patient data and can be vulnerable to hacking. If compromised, these devices could compromise patient privacy and even put lives at risk. Therefore, it is essential to develop and implement robust security measures, such as encryption, secure authentication, and intrusion detection, to ensure the integrity and reliability of these critical systems.

However, most of the proposed countermeasures are vulnerable to physical attacks [3], leaving it vulnerable to tampering or reverse engineering [4] if it is captured by an adversary. In light of these threats, there is an urgent need to enhance the access control mechanisms of electronic devices. In this paper, we combine two innovative concepts - hardware obfuscation and biometric-based authentication - to address these challenges and threats. Our approach, dubbed human-to-device (H2D) authentication, offers the following advantages:

- We propose a comprehensive biometric template protection and hardware obfuscation based on physical unclonable function and biokeys.
- In contrast to conventional software methods, our approach eliminates the need to permanently store any biometric template or key on the device. This notably decreases the risk of compromising biometric data and keys.

II. Experiment Setup

A. Data Acquisition

In our study, we utilized three public ECG databases such as (MITDB), PTB Diagnostic ECG Database (PTDB), and The ECG identification database (ECG-ID). We used only a single ECG lead from collecting ECG for realistic scenarios.

B. Data Processing

ECG biometric system comprises filtering, segmentation, feature extraction, and matching [5], [6]. In this work, we used Savitzky-Golay filter to clean up the signal. Once the ECG signal is filtered, we segment it into different heartbeats. To address the existing study for feature extraction, we developed reliable mathematical models that capture ECG dynamics to estimate states like noise, emotion, and exercises and built a deep learning model based on the ECG model for a robust authentication framework.

We employed Bayesian estimation to model an ECG signal, extracting both its model parameters and observation noise. Assuming the ECG signal comprises a clean component and noise, represented as $x_i(t) = \tilde{x_i}(t;\boldsymbol{\theta}) + e_i(t)$, where $\tilde{x_i}(t;\boldsymbol{\theta})$ represents a parametric ECG model and $e_i(t)$ denotes measurement noise. To extract the dynamic parameters of the ECG, we applied autoregressive (AR) dynamics, defined as $x_i(t+1) = \gamma x_i(t) + e_i(t)$, where $x_i(t)$ corresponds to any of the 15 Gaussian parameters α_t, b_t, and θ_t, with $e_i(t)$ representing the corresponding ECG noise. To maintain valid equations, we set γ to 1, reflecting the expected variation between successive beats in a normal ECG within the Gaussian parameters. Estimation of the ECG noise is conducted using the extended Kalman filter (EKF), considering their dynamics (Haykin, 2004) [7]. Subsequently, after modeling the ECG signal to mitigate noise and variation, we delve into the time-frequency domain for feature extraction. Our proposed

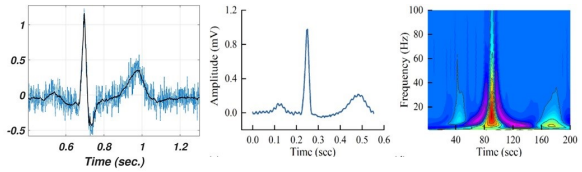

Fig. 1. Proposed method for noise cancellation and 2D-scalogram images extraction using wavelet transform.

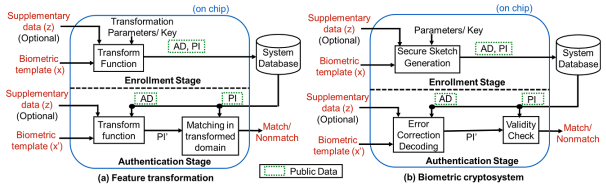

Fig. 2. Flow of operations in two major biometric template protection approaches.

methodology involves transforming the ECG signal into a 2D image scalogram, leveraging a family of wavelet functions for signal decomposition in the time-frequency domain. Specifically, we explore various mother wavelets such as Daubechies, Biorthogonal, Coiflets, Symlets, Morlet, and Mexican Hat. By transitioning the ECG signal from the time to frequency domain and extracting 2D-scalogram images using continuous wavelet transform, we can capture more discriminative image features from the ECG, facilitating the utilization of advanced deep learning architectures such as LSTM, Vision Transformers (Dosovitskiy et al., 2020) [8], Conv-CapsNet (Sabour et al., 2017) [9], and RBM-CapsNet models, among others.

III. Biometric Template Protection

The existing template protection schemes are broadly divided into two major categories: (i) biometric cryptosystems y [10] and (ii) feature transformation approaches [11].

As can be seen in Fig. 2(a)), upon receiving the input biometric template (x) from a user, the transformation parameters (AD) will be applied on x to create the protected biometric template (PI) [12] during enrollment stage [11].

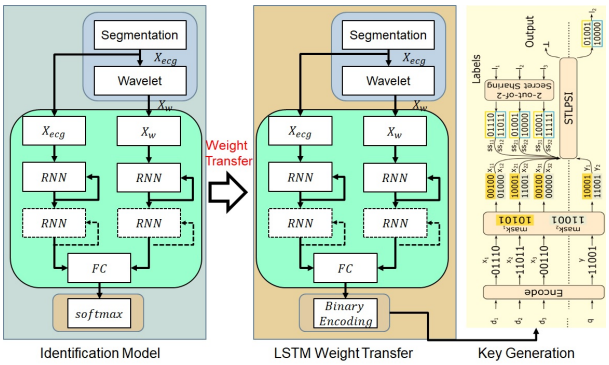

Fig. 3. Biokey generation scheme using LSTM weight transfer and homomorphic encryption.

In the authentication stage, when a biometric template (x') is queried, AD may be used to reconstruct a PI. After the transformation, another protected template, PI$'$ is constructed and compared to PI using a matcher module. Based on the match/no-match result, the query template is authenticated, and access is granted. Since AD is public here, it is possible to retrieve the x from the PI utilizing the AD; hence, the desired non-invertibility requirement can be violated. Non-invertible feature transformation using cancelable biometrics has been studied to tackle this issue. [13]). However, some of these techniques exhibit poor recognition performance in practice [14]. On the other hand, as shown in Fig. 2(b), the enrollment stage of biometric cryptosystems [11] involves a secure sketch generator (SSG) as AD. **Existing biometric templates are not only vulnerable to different described attacks, and have low performance, but studies on ECG biometrics are also very limited.**

Proposed work: Unlike other biometric systems where the matching module is implemented to compare similarity between enrollment and verification phase, our proposed schemes, however, rather than having an authentication step, use an *activation* step, where the obfuscated design is unlocked. To achieve this goal, we first generated binary strings (Biokey) from ECG biometric traits. Then, BioKey will be used as a challenge of strong physical unclonable function (PUF). The challenge is fed into the strong PUF model to compute a unique device and biometric-dependent response, which will behave as an obfuscation key (ObsKey). The obfuscated bitstream will be sent to the user and loaded into the device.

A. Phase I: Binary Encoding

Our approach begins with an initialization phase. ECG identification using the LSTM model and feature encoding. To generate a reliable feature vector, we first implemented ECG-based identification based on the novel ECG identification model. We propose novel ECG identification techniques that consist of wavelet transformation and multiple, long short-term memory (LSTM) recurrent neural networks (RNN). To better capture the ECG patterns, we used both classical features, i.e., wavelet, and LSTM at the same time. The reliable and discriminate features of ECG is learned through identification techniques with wavelet transform and multiple long short-term memory (LSTM). We employed multiple smaller parallel RNNs instead of one larger RNN, which will increase the accuracy without significantly increasing the computational costs. The outputs of the two branches are concatenated and fed into a fully connected neural network layer in order to produce the probability score for identification. Then, the **weights for the identification model layers is transferred from a model trained for identification to the key generation model where each reliable feature is encoded into binary strings**. The difference is that the last layer after a fully-connected layer is replaced by an encoding technique. Fig. 3).

The training methodology of transferring weights from an identification model aimed to take advantage of the training

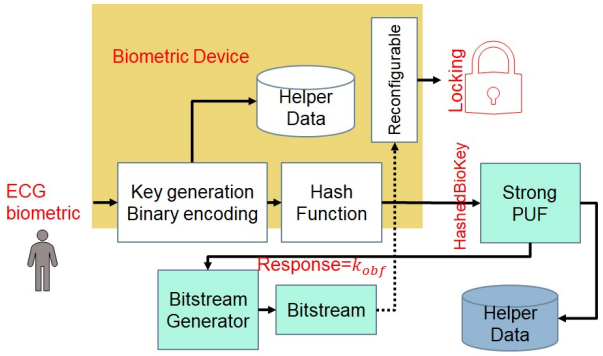

Fig. 4. Proposed ECG biometric Template Protection mechanism using PUF and Hardware Obfuscation.

process of identifying deep neural networks and assess how it could benefit a neural network for BioKey generation. Next, we used the Fuzzy Labeled Private Set Intersection (FLPSI) protocol for binary key generation. To build an FLPSI protocol, we adopted the AES block cipher, homomorphic encryption, garbled circuits, and t-out-of-T secret sharing suggested in USENIX Security [15] to handle noisy data. To eliminate noisy bits in BioKey, we used a hash function to generate HashedBioKey. The HashedBioKey is considered as the challenge of a strong PUF.

B. Phase II: Integrating PUF & Hardware Obfuscation

In order to generate the strong PUF challenge, the BioKey generated in Phase I is processed by the hash function to the desired length.

The designer builds a strong PUF model using HashedBioKey. A hash function is any function that can be used to map data of arbitrary size to data of fixed size. Due to the non-invertible property of PUF, the original biometric feature can not be reconstructed. To address issues with noisy behavior (voltage variation, aging, temperature variation) of the PUF, helper data is employed for performing error correction at the output of the PUF. We used provable strong PUF as designing strong PUFs does not fall within the scope of this career. The response from a strong PUF is to behave as an obfuscation key (ObsKey) which produces an obfuscated bitstream (sequence of bits). The obfuscated bitstream is sent to the user and loaded into the device to lock the device. The bitstream obfuscation allows the key to change for every chip/user due to the configurable hardware. This is an essential feature since a biometric-derived key will be different from user to user. The proposed ECG biometric template protection is depicted in Fig. 4. During the authentication phase, the user provides his/her biometric as an input. The process in phases I and II of the enrollment process is applied to generate the Bio-Key with respect to error correction and helper data. A correct ObsKey unlocks the obfuscated bitstream and brings the device into functional (unlocked) mode. Without the correct key, the device could not work correctly. Since our proposed work does not store any raw iometric data, which addresses the irreversibility property,. It will allow the user to re-issue a new template if the system is compromised, confirming the revocability of the system. The system parameters (AD) are not public in our proposed model. Therefore, the attackers cannot take advantage of AD to find links among multiple templates of a user.

IV. Conclusion

This paper examines the potential benefits and challenges of integrating biometrics into electronic devices, proposing the concept of human-to-device (H2D) authentication. Utilizing advanced biometrics, such as physiological data like Electrocardiogram (ECG), along with innovative obfuscation techniques at the system level, aims to deter hardware attacks. ECG biometrics offer high security due to their uniqueness, resistance to spoofing, and ease of use, making them suitable for high-stakes applications.

References

[1] R. H. Weber, "Internet of things–new security and privacy challenges," *Computer law & security review*, vol. 26, no. 1, pp. 23–30, 2010.

[2] R. T. Azuma, "A survey of augmented reality," *Presence: teleoperators & virtual environments*, vol. 6, no. 4, pp. 355–385, 1997.

[3] J. A. Halderman, S. D. Schoen, N. Heninger, W. Clarkson, W. Paul, J. A. Calandrino, A. J. Feldman, J. Appelbaum, and E. W. Felten, "Lest we remember: cold-boot attacks on encryption keys," *Communications of the ACM*, vol. 52, no. 5, pp. 91–98, 2009.

[4] M. Fyrbiak, S. Strauß, C. Kison, S. Wallat, M. Elson, N. Rummel, and C. Paar, "Hardware reverse engineering: Overview and open challenges," in *2017 IEEE 2nd International Verification and Security Workshop (IVSW)*, pp. 88–94, IEEE, 2017.

[5] R. Cordeiro, D. Gajaria, A. Limaye, T. Adegbija, N. Karimian, and F. Tehranipoor, "Ecg-based authentication using timing-aware domain-specific architecture," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 39, no. 11, pp. 3373–3384, 2020.

[6] N. Karimian, Z. Guo, M. Tehranipoor, and D. Forte, "Highly reliable key generation from electrocardiogram (ecg)," *IEEE Transactions on Biomedical Engineering*, vol. 64, no. 6, pp. 1400–1411, 2016.

[7] S. Haykin, *Kalman filtering and neural networks*, vol. 47. John Wiley & Sons, 2004.

[8] A. Dosovitskiy, L. Beyer, A. Kolesnikov, D. Weissenborn, X. Zhai, T. Unterthiner, M. Dehghani, M. Minderer, G. Heigold, S. Gelly, *et al.*, "An image is worth 16x16 words: Transformers for image recognition at scale," *arXiv preprint arXiv:2010.11929*, 2020.

[9] S. Sabour, N. Frosst, and G. E. Hinton, "Dynamic routing between capsules," *Advances in neural information processing systems*, vol. 30, 2017.

[10] E. Uzun, C. Yagemann, S. Chung, V. Kolesnikov, and W. Lee, "Cryptographic key derivation from biometric inferences for remote authentication," in *Proceedings of the 2021 ACM Asia Conference on Computer and Communications Security*, pp. 629–643, 2021.

[11] K. Nandakumar and A. K. Jain, "Biometric template protection: Bridging the performance gap between theory and practice," *IEEE Signal Processing Magazine*, vol. 32, no. 5, pp. 88–100, 2015.

[12] S. Rane, "Standardization of biometric template protection," *IEEE MultiMedia*, vol. 21, no. 4, pp. 94–99, 2014.

[13] S. Wang, W. Yang, and J. Hu, "Design of alignment-free cancelable fingerprint templates with zoned minutia pairs," *Pattern Recognition*, vol. 66, pp. 295–301, 2017.

[14] V. M. Patel, N. K. Ratha, and R. Chellappa, "Cancelable biometrics: A review," *IEEE Signal Processing Magazine*, vol. 32, no. 5, pp. 54–65, 2015.

[15] E. Uzun, S. P. Chung, V. Kolesnikov, A. Boldyreva, and W. Lee, "Fuzzy labeled private set intersection with applications to private {Real-Time} biometric search," in *30th USENIX Security Symposium (USENIX Security 21)*, pp. 911–928, 2021.