Demo Abstract: Secure Pairing via Video and IMU Verification

Carlos Ruiz[1], Shijia Pan[1,2], Hae Young Noh[2], Pei Zhang[1], Jun Han[3]
[1] Carnegie Mellon University, Electrical and Computer Engineering, Moffett Field, CA, 94035
[2] Carnegie Mellon University, Civil and Environmental Engineering, Pittsburgh, PA, 15213
[3] National University of Singapore, Computer Science, Singapore, 117417
{carlosrd,shijiapan,noh,peizhang}@cmu.edu,junhan@comp.nus.edu.sg

ABSTRACT

Secure pairing is an important problem especially due to large number of IoT devices. In this paper, we propose *PosePair++*, to enable a camera to securely pair with IoT devices which are equipped with IMU sensors. Existing context-based pairing approaches do not adequately address this problem due to differing sensing modalities. To address this challenge, we propose to translate the signals from heterogeneous sensing modalities to a common space, namely 2D acceleration. In this demo, we present *PosePair++*'s robustness against different types of attackers (i.e., attackers that observe the user's motion, or attackers performing mimicking attack).

ACM Reference Format:
Carlos Ruiz[1], Shijia Pan[1,2], Hae Young Noh[2], Pei Zhang[1], Jun Han[3]. 2019. Demo Abstract: Secure Pairing via Video and IMU Verification. In *The 18th International Conference on Information Processing in Sensor Networks (co-located with CPS-IoT Week 2019) (IPSN '19), April 16–18, 2019, Montreal, QC, Canada.* ACM, New York, NY, USA, 2 pages. https://doi.org/10.1145/3302506.3312492

1 INTRODUCTION

Cyber-Physical Systems (CPS) and Internet of Things (IoT) are projected to increase in number to 24 billion by 2020 [4]. These interconnected devices provide various smart services, e.g., tracking fitness activities, biometrical mobile payments, public display sharing. With the growth of the smart devices, securely pairing across the devices are becoming a necessity to protect privacy-sensitive information (e.g., health status, credit card number, document).

Prior works on IoT device pairing mainly fall into the following categories: 1) direct inputs, such as passkey, touch screen, and button [1]. The security of these methods rely on manual user input of passkey. However, with the growth of the number of devices and reduction of their size, it becomes impractical to pair all of them manually; 2) Tag-based methods, such as NFC, RFID tag, barcode, QR code [7, 9]. The security of these methods exchange pairing messages while "tagging" the two devices together. However, they all make a strong assumption that the devices are all equipped with the tags, incurring additional deployment and procurement costs. 3) Sensing-based methods, such as co-located context aware sensing, motion detection based pairing [11]. The security of these methods rely on extracting common sources of entropy from the sensed information. However, they either do not support heterogeneous sensing or take a long time to achieve secure pairing [5]. Particularly relevant work such as UniverSense [8] and PosePair [10] explored the heterogeneous sensing based device identity association, however, these pairing methods cannot provide secure pairing.

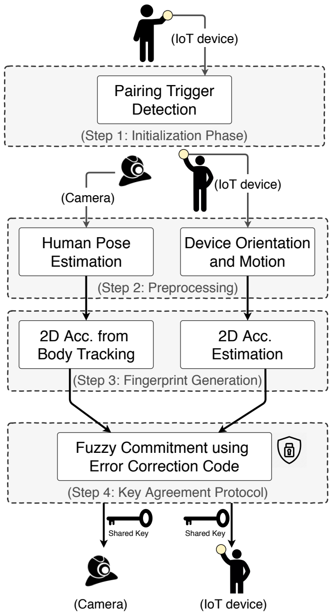
(IoT device)
Pairing Trigger Detection
(Step 1: Initialization Phase)
(Camera)
(IoT device)
Human Pose Estimation
Device Orientation and Motion
(Step 2: Preprocessing)
2D Acc. from Body Tracking
2D Acc. Estimation
(Step 3: Fingerprint Generation)
Fuzzy Commitment using Error Correction Code
(Step 4: Key Agreement Protocol)
Shared Key
Shared Key
(Camera)
(IoT device)

Figure 1: *PosePair++* system overview.

In this demo, we present *PosePair++*, a heterogeneous sensing based secure pairing approach that utilizes the motion pattern detected via video and the IMU on the smart device to perform key agreement protocol, ultimately to share a symmetric cryptographic key between the participating devices. These two types of measurements, despite their differences in sensing modalities, can be converted to the same signal space – acceleration – to produce a similar fingerprint. *PosePair++* is robust against attackers that utilize their cameras to observe the motion from angles that are not directly in front of the user. This is because *PosePair++* is able to ignore the acceleration in the legitimate camera's viewing direction for fingerprint similarity. Our demo shows the robustness of our approach against two types of attackers: visual (camera looking at the legitimate user) and mimicking (attacker with another IoT device trying to imitate the legitimate user's pattern).

Hence, the contributions of *PosePair++* are twofold:

- We design *PosePair++*, a heterogeneous sensing based secure pairing protocol, which leverages the spatial relationship between the legitimate camera and user to achieve security.

IPSN '19, April 16–18, 2019, Montreal, QC, Canada
© 2019 Copyright held by the owner/author(s).
ACM ISBN 978-1-4503-6284-9/19/04.
https://doi.org/10.1145/3302506.3312492

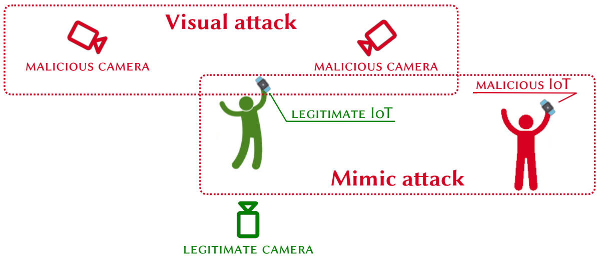

Figure 2: *PosePair++* demo overview where legitimate camera and IoT device sense motion of the legitimate user, thus generating similar fingerprints (green). Also, two different attackers attempt to produce the same fingerprint, through a) visual observation of motion pattern via attacker cameras from different angles; b) mimicking legitimate user's (red). *PosePair++* is robust against the attacks due to the difficulty of estimating acceleration in the depth axis of a camera and difficulty of replicating imperfections of human motion.

- We implement and demonstrate its robustness to two types of attacks: camera-based and mimicking attacks.

2 SYSTEM DESIGN

We present the system design of *PosePair++*. The main goal of our system is to enable a usable secure pairing of camera and IoT devices. Specifically, each device first translates *non-equal* numerical signals (i.e., video and IMU) into *similar* fingerprint bits. Subsequently, the devices conduct key agreement protocol by utilizing the extracted fingerprint bits to result in a *shared cryptographic key*.

We depict in Figure 1 the *PosePair++*'s system overview diagram. The user initiates *PosePair++* protocol by shaking the IoT device in a predefined pattern, triggering the *Pairing Trigger Detection* in the *Initialization Phase (Step 1)*. Once the protocol initiates, both the camera and the IoT device perceive the motion and subsequently pre-process each of their sensed data as depicted in *Step 2*. In this step, the camera performs *human pose estimation* from the video signal, while the IoT device performs *orientation and motion* estimation from the IMU signal. The pre-processed data are then subsequently input to *Fingerprint Generation (Step 3)* module, where the human pose information (from video) as well as the orientation and motion (from IMU) are both converted to 2D acceleration values. Specifically, user's motion is projected onto a 2D plane parallel to the camera's image plane (perpendicular to its viewing direction). *PosePair++* leverages the observation that it is extremely challenging for an attacker to estimate the acceleration of an object in the depth axis of an RGB camera. Finally, both devices undergo a key agreement protocol in *Step 4* by taking as input the estimated 2D acceleration from both devices to output the final shared symmetric cryptographic key. Specifically, *PosePair++* utilizes the fuzzy commitment scheme that leverages error correction code [3, 6]. The shared key can be used as a master key to derive subsequent session keys for authentication and encryption.

3 DEMO

We exhibit the robustness of our proposed multi-modal IoT secure pairing scheme by conducting two different attacks, as shown in Figure 2. A member of the audience will wear the legitimate IoT device (a wearable smartwatch) and stand in front of the legitimate camera he or she is trying to pair to, while one or more attacker cameras also observe from different angles. At the same time, a second member of the audience will play a mimic attack by trying to imitate the pattern of the legitimate user.

For cameras from other angles, reconstructing the acceleration on that plane is difficult and thus the fingerprint similarity with respect to the legitimate IoT device will be low, which will prevent the visual attack. Likewise, it is complicated for a human to perfectly replicate the motion pattern followed by another person, hence the mimic attack's fingerprint similarity should also be low – i.e., it would not lead to the same shared key.

4 IMPLEMENTATION

PosePair++'s implementation leverages open-source libraries such as OpenCV to interact with the cameras, PyTorch to run deep learning models, and OpenPose [2] to obtain 2D human pose estimation. The video feeds are processed on a MacBook Pro 2017 connected to an eGPU setup (Akitio Node Thunderbolt 3 eGPU with an Nvidia Titan Xp GPU). For the IoT devices, we use two Fossil Sport Smartwatch FTW4019P due to the wide availability of libraries for real-time data collection on Android WearOS devices. They are equipped with a 9-axis Inertial Measurement Unit (3-axis accelerometer, gyroscope and magnetometer), as well as Bluetooth 4.2 Low Energy and WiFi 802.11 b/g/n for communication. Furthermore, we implemented a Python client on the computer for data acquisition, fingerprint generation and visualization.

REFERENCES

[1] Adeola Bannis and Jeffrey A Burke. 2015. Creating a secure, integrated home network of things with Named Data Networking.

[2] Zhe Cao, Tomas Simon, Shih-En Wei, and Yaser Sheikh. 2017. Realtime Multi-Person 2D Pose Estimation using Part Affinity Fields. In *CVPR*.

[3] Yevgeniy Dodis, Rafail Ostrovsky, Leonid Reyzin, and Adam Smith. [n. d.]. Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data. *SIAM J. Comput.* ([n. d.]).

[4] Jayavardhana Gubbi, Rajkumar Buyya, Slaven Marusic, and Marimuthu Palaniswami. 2013. Internet of Things (IoT): A vision, architectural elements, and future directions. *Future generation computer systems* 29, 7 (2013), 1645–1660.

[5] Jun Han, Albert Jin Chung, Manal Kumar Sinha, Madhumitha Harishankar, Shijia Pan, Hae Young Noh, Pei Zhang, and Patrick Tague. 2018. Do you feel what I hear? Enabling autonomous IoT device pairing using different sensor types. In *Do You Feel What I Hear? Enabling Autonomous IoT Device Pairing using Different Sensor Types*. IEEE, 0.

[6] A. Juels and M. Sudan. 2002. A fuzzy vault scheme. In *Information Theory, 2002. Proceedings. 2002 IEEE International Symposium on.*

[7] Peter Kieseberg, Manuel Leithner, Martin Mulazzani, Lindsay Munroe, Sebastian Schrittwieser, Mayank Sinha, and Edgar Weippl. 2010. QR code security. In *Proceedings of the 8th International Conference on Advances in Mobile Computing and Multimedia*. ACM, 430–435.

[8] Shijia Pan, Carlos Ruiz, Jun Han, Adeola Bannis, Patrick Tague, Hae Young Noh, and Pei Zhang. 2018. UniverSense: IoT Device Pairing through Heterogeneous Sensing Signals. In *Proceedings of the 19th International Workshop on Mobile Computing Systems and Applications*. ACM.

[9] Jukka Riekki, Timo Salminen, and Ismo Alakarppa. 2006. Requesting pervasive services by touching RFID tags. *IEEE Pervasive computing* (2006).

[10] Carlos Ruiz, Shijia Pan, Alberto Sadde, Hae Young Noh, and Pei Zhang. 2018. PosePair: pairing IoT devices through visual human pose analysis: demo abstract. In *Proceedings of the 17th ACM/IEEE International Conference on Information Processing in Sensor Networks*. IEEE Press, 144–145.

[11] Ahren Studer, Timothy Passaro, and Lujo Bauer. 2011. Don't bump, shake on it: The exploitation of a popular accelerometer-based smart phone exchange and its secure replacement. In *Proceedings of the 27th Annual Computer Security Applications Conference*. ACM, 333–342.