Secure and Usable Zero-interaction Pairing and Authentication Methods for the Internet-of-Things

Kyuin Lee
University of Wisconsin, Madison–Wisconsin
Advisor: Prof. Younghyun Kim, Graduation: May 2022, Field: Internet-of-Things (IoT), Past submission: None

I. Background and Motivation

For the past several years, enthusiastic and ambitious projections have been made for the rapid growth in the number of Internet-of-Things (IoT) devices. As this number is continuing to increase, efficient configuration and long-term management of these devices are becoming more time-consuming and labor-intensive. For instance, current *pairing* (mutually registering two devices with no prior knowledge) and *authentication* (verifying the authority of a device to access resources) methods between typical IoT devices (e.g., smart speakers, lights, and thermostats) heavily involves *human-in-the-loop* operations by requiring the user to manually type in a pin or password to establish credentials between two devices. Unfortunately, this process is particularly challenging for IoT systems because most low-cost IoT devices delegate the user interface to web- or mobile-based apps rather than using their own on-board interfaces (e.g., screen and keyboard), mainly due to form factor or cost constraints. They usually require the use of a third device, most commonly the user's mobile device, to configure devices and establish a secure network. When the devices do not support this complicated interaction, the security is often given up, leaving the communication vulnerable to a number of attacks.

Recently, efforts to reduce human involvement have lead researchers to introduce various *zero-interaction pairing or authentication (ZIPA)* techniques. ZIPA techniques exploit a spatially correlated, temporally uncorrelated environmental contexts to allow devices to authenticate with each other only when they are closely located at the same time as shown in Fig. 1. The main assumption of ZIPA is that if two devices observe substantially correlated environmental context signal, they are likely to be located in the same physical space, which implicitly means that they are owned by the same user and can be allowed to authenticate with each other using their measured context signal as a key. Since the environmental contexts are significantly different when measured at different locations, distant devices cannot generate the same key. Compared to traditional password-based authentication schemes, ZIPA is advantageous in terms of both security and usability. The randomly generated keys provide higher security than user-created passwords and it does not depend on the user to create, remember, and enter the password. Further, it allows devices to use a unique key for each device pair or re-establish fresh keys more frequently and autonomously.

In this work, I present series of our proposed works on multiple ZIPA techniques designed for spontaneous pairing and authentication of IoT devices based on their deployment environments. Further, I introduce two proposed frameworks to address some of the practical challenges and limitations that exist in the current state-of-the-art ZIPA works such as randomness distillation of the generated keys and automatic determination of proper reconciliation parameters. Other than the works related to ZIPA, I have actively worked on the field of approximate computing, hardware security and secure V2P communication systems [6]–[8].

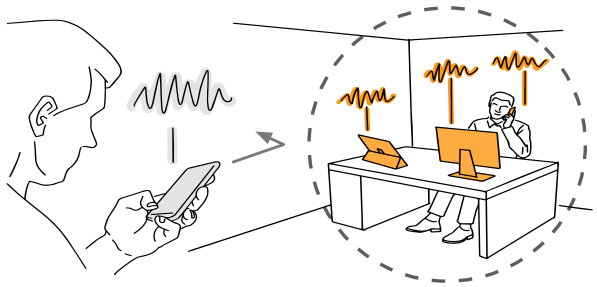

Fig. 1. ZIPA allows co-located devices to autonomously pair or authenticate each other while rejecting distant ones.

II. Approach

We mainly categorize the general IoT devices into two main categories (*mobile* and *stationary*) and present different methods based on the device's environmental characteristics. Mobile device refers to battery operated devices that are freely carried around by users (e.g., smartphones, smartwatches, etc) whereas stationary devices include constantly powered devices such as smart thermostats or speakers.

A. ZIPA for Mobile Devices

We proposed two usable and secure pairing protocols to address tedious and time-consuming nature of current pairing scheme between mobile devices. The first method, SyncVibe [1], utilizes a vibration motor and an accelerometer, that are already ubiquitously available or easy to embed in mobile and wearable devices, to transmit and receive pairing information. By simply keeping two devices in direct contact, the user can bootstrap a secure, high-bandwidth wireless connection without going through manual pairing procedures. Compared to previous vibratory communication schemes, SyncVibe significantly improves the effective throughput by maximizing bitrate and minimizing synchronization overheads through *vibration clock recovery* technique, which extracts timing information from the non-ideal vibration waveform of data bits by detecting the activation and deactivation of the vibration motor. When transmitting 150-bit pairing information, our prototype shows a reliable success rate of 92% with average pairing time of 6.74 s, achieving up to 2x faster

pairing time compared to previously proposed vibration based communication methods.

The second method, IVPAIR [2], specifically addresses pain of pairing mobile devices within intra-vehicular scenario. Using IVPAIR, users can pair a mobile device equipped with an accelerometer with the vehicle's in-vehicle infotainment (IVI) system or other mobile devices by simply holding it against the vehicle's interior frame. Contrary to SYNCVIBE, where arbitrarily generated pairing information is transmitted using vibration motor, IVPAIR extracts entropy from the road conditions and vibration of the vehicle to automatically generate pairing information for multiple devices within the same car. Under realistic driving experiments with various types of vehicles and road conditions, we demonstrate that all passenger-owned devices can expect a high pairing success rate (87%) with a short pairing time (11 s).

B. ZIPA for Stationary Devices

For stationary devices, we proposed VOLTKEY [3], which transparently and continuously generates secret keys for colocated devices, leveraging spatiotemporally unique noise contexts observed in commercial power line infrastructure. VOLTKEY introduces a novel scheme to extract randomness from power line noise and securely convert it into the same key by a pair of devices. The unique noise pattern observed only by trusted devices connected to a local power line prevents malicious devices without physical access from obtaining unauthorized access to the network. VOLTKEY utilizes low-cost microcontroller to measure and extract power line noise, which can easily be implemented as a modular addition to standard USB or AC/DC power supplies shipped with IoT devices. Under various realistic deployment scenarios in home, laboratory, and office environments, VOLTKEY successfully authenticates over 90% of trusted pairs of devices while effectively rejecting adversarial devices leveraging temperature, time, dominant electrical noise, and access to nearby locations.

C. Limitations and challenges of ZIPA

Currently in most ZIPA works, there are gaps in our understanding of the theoretical limitations of environmental noise harvesting, making it difficult for researchers to build efficient algorithms for sampling environmental noise and distilling keys from that noise. To address this challenge, we presented MOONSHINE [4], an efficient algorithm to improve the quality of the environmentally extracted keys and evaluate it on real key extraction hardware. Compared to commonly used commonly-used key extraction algorithms, MOONSHINE can nearly double the quality of keys as measured by the randomness test suite, producing keys that can be used in real-world authentication scenarios.

Another limitation of current ZIPA works is the lack of a "systematic" design towards tunable authentication range (range at which devices are allowed to authenticate). To address this, we proposed a generic key reconciliation framework [5] that determines the proper reconciliation parameter based on a user-given authentication range. We also analyze and compare the two most commonly used reconciliation schemes used in ZIPA in terms of security and usability to select the better scheme with the best parameters to set the balance between them and estimate the computation overhead.

III. POTENTIAL LONG-TERM IMPACT

As devices continue to become smaller and more ubiquitous, it is unreasonable to utilize the current pairing and authentication paradigm. The presented works will not only give the users enhanced user experience by eliminating inconveniences of conventional methods, but also ultimately result in more robust security of overall system by enabling periodic fresh key generation. More importantly, our works does not require significant hardware modification or overhead that allows them to be easily implemented on the already deployed sets of devices. Currently, most ZIPA works lack systematic pipeline design, which leads different groups of work using different schemes, hindering coherence and fair comparison of many existing ZIPA techniques. Our two proposed frameworks can potentially be used as a standardized frameworks to address current limitations and serve as a major step towards the systematic design of many future ZIPA schemes.

AWARDS AND ACHIEVEMENTS

- Student Research Grants Competition, UW-Madison, 2019
- Richard Newton Young Fellow Award, DAC, 2019
- NSF Travel Grant, ICCD, 2018
- The Best Demonstration Award in SIGDA University Demonstration, DAC, 2018
- ECE Wisconsin Distinguished Graduate Fellowship, UW-Madison, 2017
- Osher Award, Meeting of the Minds Research Symposium, 2016

REFERENCES

[1] **Kyuin Lee**, Vijay Raghunathan, Anand Raghunathan and Younghyun Kim. 2018. SyncVibe: Fast and Secure Device Pairing through Physical Vibration on Commodity Smartphones. In *International Conference on Computer Design (ICCD).*

[2] **Kyuin Lee**, Neil Klingensmith, Dong He, Suman Banerjee and Younghyun Kim. 2020. ivPair: Context-Based Fast Intra-Vehicle Device Pairing for Secure Wireless Connectivity. In *Conference on Security and Privacy in Wireless and Mobile Networks (WiSec).*

[3] **Kyuin Lee**, Neil Klingensmith, Suman Banerjee and Younghyun Kim. 2019. VoltKey: Continuous Secret Key Generation Based on Power Line Noise for Zero-Involvement Pairing and Authentication. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies 3* (2019).

[4] Jack West, **Kyuin Lee**, Suman Banerjee, Younghyun Kim, George K. Thiruvathukal and Neil Klingensmith. 2021. Moonshine: An Online Randomness Distiller for Zero-Involvement Authentication. In *International Conference on Information Processing in Sensor Networks (IPSN).*

[5] **Kyuin Lee** and Younghyun Kim. 2021. Balancing Security and Usability of Zero-interaction Pairing and Authentication for the Internet-of-Things. To be appeared in *Workshop on CPS & IoT Security and Privacy (CPSIoTSec).*

[6] Yucheng Yang, **Kyuin Lee**, Younghyun Kim and Kassem Fawaz. 2021. PEDRO: Secure Pedestrian Mobility Verification in V2P Communication using Commercial Off-the-shelf Mobile Devices. To be appeared in *Workshop on CPS & IoT Security and Privacy (CPSIoTSec).*

[7] Younghyun Kim, Joshua San Miguel, Setareh Behroozi, Tianen Chen, **Kyuin Lee**, Yongwoo Lee, Jingjie Li and Di Wu. 2020. Approximate Hardware Techniques for Energy-Quality Scaling Across the System. In *International Conference on Electronics, Information, and Communication (ICEIC).*

[8] Yongwoo Lee, **Kyuin Lee** and Younghyun Kim. 2018. Demo Abstract: CAMPUF: Physically Unclonable Function based on CMOS Image Sensor Fixed Pattern Noise. In *SIGDA University Demonstration at DAC.*