Secure, Usable and Practical Authentication for the Internet of Things

By

Kyuin Lee

A dissertation submitted in partial fulfillment of
the requirements for the degree of

Doctor of Philosophy

(Electrical and Computer Engineering)

at the

UNIVERSITY OF WISCONSIN–MADISON

2022

Date of final oral examination: 04/25/2022

The dissertation is approved by the following members of the Final Oral Committee:

Younghyun Kim, Assistant Professor, Electrical and Computer Engineering
Suman Banerjee, Professor, Computer Sciences
Kassem Fawaz, Assistant Professor, Electrical and Computer Engineering
Rahul Chatterjee, Assistant Professor, Computer Sciences

ACKNOWLEDGMENTS

I would like to dedicate this dissertation to my beloved colleagues, friends and families who have influenced and motivated me to successfully complete my Ph.D. degree.

First and foremost, I want to thank my wonderful advisor, Professor Younghyun Kim, for his great support, guidance and effort to constantly motivate and guide me in every aspects of my life for the past five years. I am honored and I always realize how lucky I am to have such a wonderful advisor. I would also like to thank every members of my defense committee, Professor Banerjee, Professor Fawaz, and Professor Chatterjee for their valuable advice, feedback and comments to make this dissertation more concrete and solid in every ways.

I would also like to thank my beloved family members, Kwansup Lee, Soyeon Ahn, Dr. Jongho Ahn, Kwangja Yu, Dongchoon Lee, Sukhyun Shin and Kyuwon Lee. I am grateful for their positive outlook, support and unconditional love in helping me accomplish my academic goals in every ways for the past 30 years.

I also want to thank all of my colleagues, Setareh Behroozi, Jingjie Li, Tianen Chen, Di Wu, Yucheng Yang, Dr. Neil Klingensmith, Jack West, Hien Vu, Aishwarya Lekshmi Chithra, Omkar Prabhune, Victoria Schrimpf, Sujin Kim, John Rupel for their genuine characters, support and our wonderful interactions together.

Last but not least, I want to thank my dearest soulmate and friends, Songhee Hong, Dr. Juhwan Lee, Dr. Yongho Kwon, Dr. Inkyu Lee, Dr. YeiHwan Jung, Dr. Wonyup Song, Dr. Iksoo Kwon, Yooyoung Ko, Yonnho Oh, Taejin Kim, Chris Kim, Bohak Yoon, Jaesung Ahn, Teddy Ahn, Sangrok Shin, Bokyeon Hwang, and Jonghwi Park, for staying by my side and helping me get through my challenging times

with our enjoyable moments together. I could not have done it without you all. Thank you.

— Kyuin Lee

CONTENTS

LIST OF TABLES

LIST OF FIGURES

ABSTRACT

The explosive growth in the number of connected and Internet-of-Things (IoT) devices (e.g., smart speakers, lights, and thermostats) today calls for more convenient and yet secure ways to establish wireless connection between devices. Unfortunately, current device authentication method between typical IoT devices heavily involves manual human interaction by requiring the user to type in a pin or password to establish credentials between two devices. Considering highly distributed and heterogeneous nature of today's connected environment, this unwieldy authentication process particularly degrades the overall usability of IoT systems, which often causes device users to perform poor security practices such as choosing weak passwords or even reusing them. To overcome this usability challenge that leads to various security vulnerabilities, researchers have devised zero-interaction authentication (ZIA) technique which allow devices to autonomously authenticate with each other through common secret extracted from environmental contexts to prove co-existence of devices.

In this dissertation, I present series of works on designing and building novel ZIA techniques for spontaneous authentication of IoT devices based on their deployment environments. More specifically, I first propose two techniques named SyncVibe and ivPair, leveraging readily available accelerometer to sense physical vibration in the ambient environment and authenticate closely located wearable and mobile devices in various portable scenarios. Secondly, I present two authentication techniques named VoltKey and AeroKey, designed to seamlessly and continuously associate indoor IoT devices using ubiquitously observable power line noise and ambient electromagnetic radiation as a secret to authenticate co-located devices in a fully autonomous manner. Specifically tailored towards emerging mobile and resource-constrained IoT devices, the proposed works effectively result in higher overall security and usability than

traditional authentication approaches while maintaining high practicality to be directly applicable to today's already deployed devices. In addition, to address generic challenges and limitations that exist in the current state-of-the-art ZIA works, I present a framework to automatically determine proper key reconciliation parameters that provide optimal balance between security and usability.

1 INTRODUCTION

The number of connected and Internet-of-Things (IoT) devices has been experiencing explosive growth, driven by emerging applications and advanced technologies, coupled with the active standardization of connected ecosystems. It is predicted that by the end of year 2024, there will be around 84 billion connected devices throughout the world, which is more than double the number of devices that existed in 2020 [63]. According to a former chief futurist of Cisco, there are around 127 newly introduced devices that are being connected to the internet every second [62].

With this overwhelming growth in its numbers, there are various environments in which these IoT devices are being deployed. As Figure 1.1 illustrates, the deployment environments can generally be categorized into two major sectors: *consumer and industrial*. In the consumer sector, personal, wearable, and home IoT devices, such as smart watches, smart

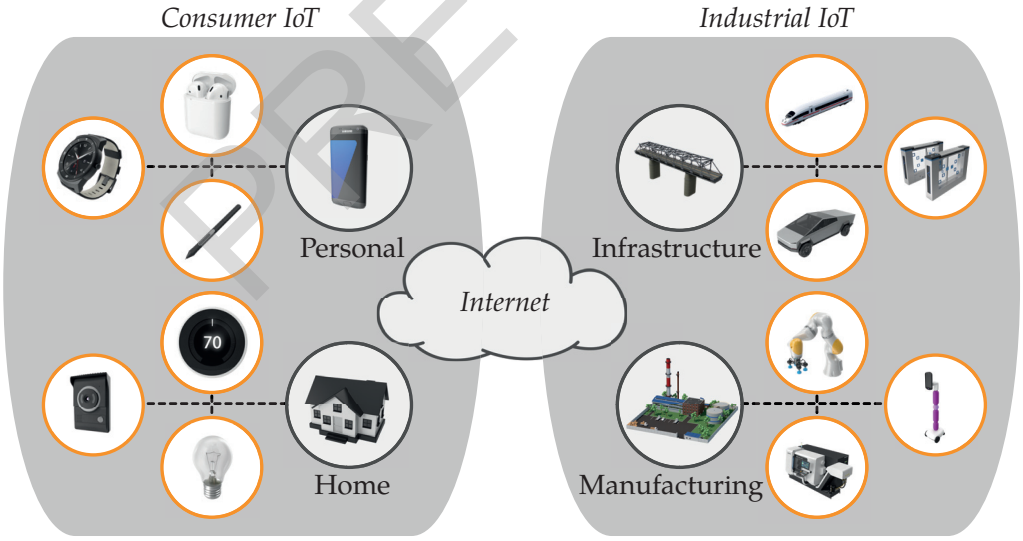

Figure 1.1: Wide deployment environments of the IoT devices are categorized into two sectors: *consumer and industrial*.

earbuds and speakers make our daily lives more efficient, effective, and healthy. On the other hand, devices deployed in the industrial sector, such as smart sensors and machines deployed in cities, warehouses, and manufacturing plants ensure higher level of automation to maintain good air quality, efficient traffic managements, and faster package deliveries. As the awareness of connected efficiency grows in the market, every industry and businesses of all sizes are thinking of ways to adopt IoT into their day-to-day activities. However, while this increased connectivity brings far too many benefits to our lives, adaptation of proliferating IoT devices leads to scalability challenges much like any other technology systems.

1.1 MOTIVATION

One of the most paramount scalability challenges that has continued to vex researchers is the question of how to quickly, securely, and seamlessly verify the authenticity between connecting devices. Unfortunately, conventional device authentication methods profoundly rely on manual human involvement. For example, Bluetooth pairing activity or connecting a wireless device to an access point in a WiFi network require human verifiers to type in a pin or password to verify that associating devices are trustworthy. Compared to traditional computing systems, this process can be considered particularly more labor-intensive and usability degrading when applied to current IoT systems for two reasons: i) Stringent constraints in the cost and the form factor have forced the manufactures to build IoT devices with limited or no usable interfaces such as touchscreens or keyboards (i.e., smart pens, smart bands). As a result, users are often forced to introduce and use secondary device, most commonly the user's smart phones, to configure devices or to establish secure connection with authorized devices. This makes traditional password- or pin-based authentication significantly more tedious, difficult, and time-consuming [15].

ii) Because device manufacturers do not consider overloading number of devices from the user's perspective, there currently exist no efficient and usable form of collective device management, and the burden of managing collection of devices falls on the user. For instance, in a typical home IoT scenario, communication network comprises of multiple edge devices connected to a single, centralized access point (WiFi router). To newly introduce or to re-authenticate devices into this network setting, users need to individually interact with different apps for different devices, which results the overall device configuration and management process to be labor-intensive and mentally overloading.

Usability is a key aspect of the authentication mechanism for IoT systems that are deployed and maintained by non-professional users. The lack of usable authentication scheme has forced many personal and mobile devices to choose usability over security and resulted in failures in properly securing critical data. For instance, without a user interface to enter a password, Bluetooth 5 devices use a common default password to encrypt the communication messages used to establish an authentication token [47, 22]. If a malicious adversary manages to gain physical access to a Bluetooth 5 headset and unpair it, they can intercept the pairing messages and extract the authentication token, ultimately gaining perpetual access to the plaintext of all subsequent communications at a distance [60]. In the case of home IoT systems, some IoT device manufacturers have inadvertently chosen usability over security and miserably failed in providing even a minimum level of security. For instance, it was reported a few years ago that 73,000 private unsecured smart cameras, including 11,000 in the U.S. alone, were being streamed on the Internet because it was not mandated to change the default password [20]. Despite the federal government's consumer advisory [29], more than 15,000 private smart cameras are still unknowingly being streamed. In the industrial sector, according to report by Palo Alto Networks' threat intelligence team, out of 1.2 million IoT

devices in thousands of physical locations across information technology and healthcare organizations in the United States, 98% of all IoT device's traffic remains unencrypted, leaving data communications vulnerable to eavesdropping by any adversary within the wireless range [13]. This vulnerability can lead to catastrophic leakage of sensitive personal data such as medical imaging, video monitoring footage, etc. Unfortunately, authenticating devices with the password does not adequately address this concern. Difficulties of authentication results in inexperienced users opting not to change default or old WiFi passwords that leads to imminent threat as disclosed in the 2016 Data Breach Investigations Report — 63% of the confirmed data breaches are attributed to using weak, default, or stolen passwords [69]. Also, in current IoT systems, once a common password is leaked, all devices using the same password must undergo tedious and error-prone password update procedures which is burdensome and sluggish. As the number of IoT devices that each user has to manage increases, combined with their heterogeneous and distributed nature, employing traditional security solutions fails to address the current problems in terms of both security and usability.

1.2 OBJECTIVES AND CONTRIBUTIONS

In this dissertation, I propose series of novel device authentication techniques towards the goal of improving usability of current IoT device authentication, so that people who have limited or no skills to operate computers can easily keep a secure connected environment. The proposed techniques successfully give users an enhanced user experience by eliminating inconveniences of conventional methods without compromising the overall security. Furthermore, the proposed techniques require minimal or no extra hardware overheads, which implies that they can easily be adopted to wide range of resource-limited devices within today's dynamic

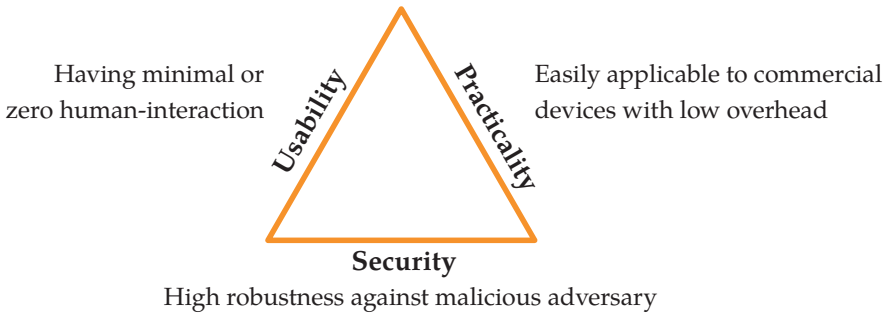

Figure 1.2: The three design aspects of the proposed device authentication techniques.

IoT deployment and usage scenarios.

Overall, the proposed authentication methods successfully improves upon conventional techniques in terms of the following three design aspects as illustrated in Figure 1.2.

1. Usability: The device authentication process can take place more quickly and efficiently with minimal or no human involvement.

2. Practicality: The authentication technique requires minimal or no hardware modifications to seamlessly be implemented into deployed devices with various form factors.

3. Security: The authentication technique provides robust protection against malicious adversaries attempting to gain unauthorized authentication.

With the three design aspects in mind, the proposed techniques are systematically evaluated in various real-world settings to demonstrate their effectiveness. Moreover, while building these series of techniques, I find that there currently exist no efficient way for the end users to balance the trade-off between usability and security of existing authentication techniques. As such, this dissertation additionally presents the generic

framework to automatically determine proper authentication parameter that balances the security and usability of device authentication schemes.

This dissertation presents different techniques designed for IoT devices that are classified into two deployment categories: *mobile* and *indoor*. Devices that are in the mobile category refers to the battery operated devices that are freely carried around by users such as smart phones, smart watches, and wearable devices. On the other hand, devices within the indoor category include all types of devices (including mobile) that are used indoors, including constantly powered devices such as smart thermostats or speakers that are designed to be mounted or not moving.

The rest of this dissertation is outlined as the following. Chapter 2 presents the background information and previous efforts of the research, as well as defining the commonly used terminologies. Next, Chapter 3 details the two device authentication techniques named SyncVibe [40] and ivPair [39] designed towards authentication between mobile and wearable devices using physical vibration that can be sensed with ubiquitously available accelerometers. In Chapter 4, I describe the techniques named VoltKey [38] and AeroKey [41] to address indoor IoT device authentication using power line noise and ambient electromagnetic radiation that are omnipresent in the indoor environment. Followed by presenting solutions to balance between security and usability of usable device authentication [37] in Chapter 5, I discuss the future works and conclude the dissertation in Chapter 6 and Chapter 7, respectively.

2 BACKGROUND

This Chapter provides the underlying background information and define the terminologies used to describe the presented works. In addition, I comprehensively provide and discuss previous efforts to improve the usability and security of device authentication through an emerging notion called zero-interaction device authentication.

2.1 DEVICE AUTHENTICATION

Device authentication is a fundamental security process where two or more devices that share no prior knowledge of each other build trust to establish a secure wireless channel to communicate with each other [76]. Traditionally, the most basic form of device authentication leverages shared secret (e.g., pre-shared key (PSK) or password), a something that only the owner "knows", to verify each others identity [21]. For IoT devices, device authentication is most commonly used to establish communication protocol such as WiFi or Bluetooth, which is the standard backbone of the wireless communication in IoT systems. For instance, in a typical smart home setting, WiFi access points and IoT end-point devices mutually authenticate each other through WiFi PSK (i.e., WiFi access point password) to agree on cryptographic keys used to encrypt and decrypt packets within the secure wireless channel [79]. Another example of device authentication which takes place between mobile devices (e.g., smart phone, smart watches) is during the Bluetooth pairing procedure. Similar to WiFi PSK, devices leverage a manually typed secret called pairing pin, typically much shorter in length, to mutually agree on the cryptographic keys for secure communication between devices.

However, secrets like PSK and passwords are usually recycled or easily gets passed around, which makes the entire network susceptible to