I Know Where You Are: A Non-intrusive Geospatial–Electrical Authentication System.

HyeLim Jung
SysCore Lab
Sejong University
Seoul, Korea
hyello13@gmail.com

Sang-Hoon Choi
SysCore Lab
Sejong University
Seoul, Korea
csh0052@gmail.com

Mohsen Ali Alawami
SysCore Lab
Sejong University
Seoul, Korea
mohsencomm@sejon.ac.kr

Sung-Kyu Ahn
SysCore Lab
Sejong University
Seoul, Korea
yiimfn@gmail.com

Ki-Woong Park*
Department of Information Security
Sejong University
Seoul, Korea
woongbak@sejong.ac.kr

***Abstract*—The Zero Trust security model is being applied to IT systems recently, leading to changes in the security model. Zero Trust requires continuous authentication for all actions and elements, including users, computing devices, and data. This necessitates additional costs and policy changes, which can impact user convenience. In this paper, the GEA system is proposed, which performs geographical-electrical authentication between a building's power system and computing devices. By utilizing the building's power system to generate power patterns and detecting them on computing devices, geographical-electrical authentication is achieved. The feasibility and efficiency of this system are validated through experiments. The GEA system provides transparent authentication to users and offers advantages of cost savings and maintenance without modifying existing infrastructure. Additionally, it analyzes power patterns to determine geographical location and provides security measures.**

***Index Terms*—Zero Trust, Side Channel, Authentication, GPS.**

I. Introduction

Zero Trust has been increasingly applied as a security model in IT systems. Attacks that threaten IT systems have become increasingly targeted and sophisticated. Recently, cybercrimes have evolved to target victims, recruit insiders within organizations, and exploit vulnerabilities in programs and devices already installed within organizations. Consequently, the traditional security model, which focuses on securing the entry points of IT systems, is evolving toward a Zero Trust security model, which verifies and monitors all elements and behaviors of a given system without fully trusting them. [1] [2] Unlike traditional security models, Zero Trust does not grant authorization based on a single authentication but continuously demands authentication for all actions and elements. In a Zero Trust security model, elements such as users, computing devices, and data require authentication, monitoring, and control. [3] The scale of the system determines the increase in elements that require control and the complexity of security policies and facilities. To implement Zero Trust, rigorous security measures must be applied to each IT device and data source, and security levels must be maintained through management and monitoring.

However, the implementation of Zero Trust incurs significant costs and policy changes. [4] Additionally, replacing or upgrading existing security systems may result in additional expenses. Furthermore, it may require constructing new facilities or adopting security solutions. Unlike traditional security systems, Zero Trust requires identification and security measures for each element, such as users, computing devices, and data, which significantly increases the system complexity. This requires additional effort in terms of management and operations. Moreover, Zero Trust also imposes additional procedures on users, thus resulting in reduced convenience to end users, who must undergo verification to obtain access privileges and validate the reliability of their devices. Moreover, existing systems must be adapted to align with the Zero Trust security model, thus leading to potential compatibility issues and need for additional modifications.

In this study, we propose a geospatial–electrical authentication (GEA) system, which performs GEA between a building's power system and the computing devices within the facility. The proposed GEA system utilizes the building's power system to supply power to each floor and detects similar patterns within the computing devices connected to the building's power system, thus performing GEA between the building and computing devices. This enables the verification

[*] Corresponding author.

2831-7203/23/$31.00 ©2023 IEEE
DOI 10.1109/AIKE59827.2023.00029

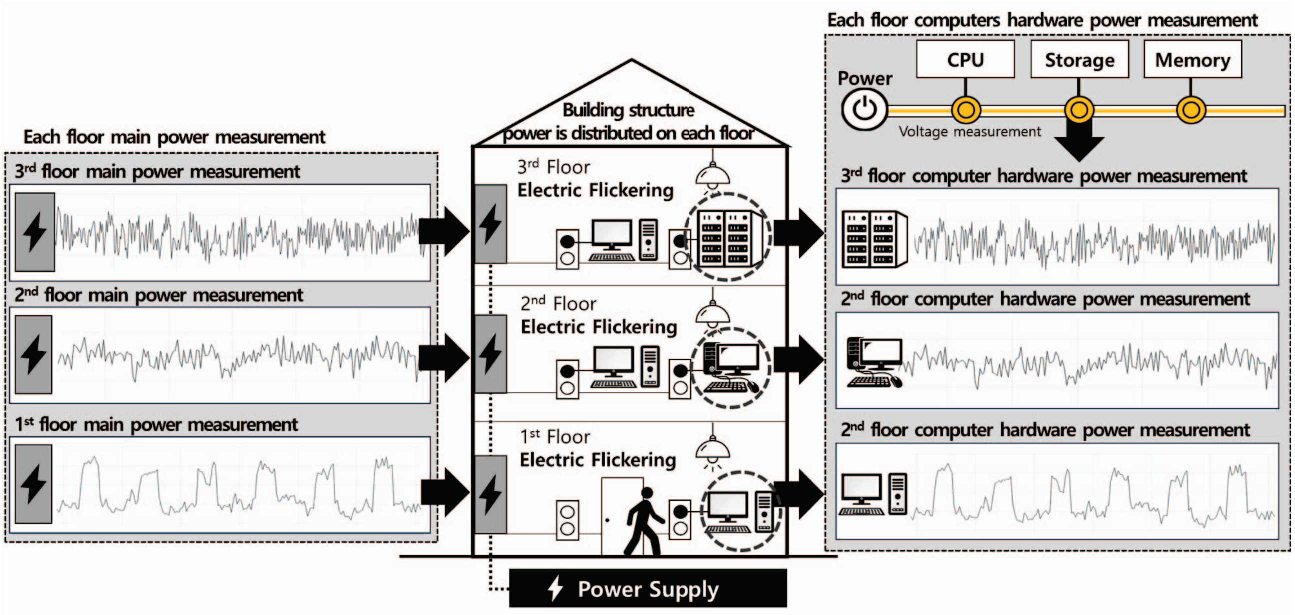
Each floor main power measurement
3rd floor main power measurement
2nd floor main power measurement
1st floor main power measurement
Building structure
power is distributed on each floor
3rd Floor
Electric Flickering
2nd Floor
Electric Flickering
1st Floor
Electric Flickering
Power Supply
Each floor computers hardware power measurement
Power
CPU
Storage
Memory
Voltage measurement
3rd floor computer hardware power measurement
2nd floor computer hardware power measurement
2nd floor computer hardware power measurement

Fig. 1: Overview of the GEA system

of the authenticated computing devices or files that are being accessed to operate within the authorized building.

As shown in Fig.1, the GEA system deploys power systems on each floor and generates power patterns for each floor's power system. Subsequently, these power patterns are detected on PCs connected to the power system on each floor, which serves as the main reference for the power patterns of that floor. When a PC connected to a floor requests PC usage or internal data access, the corresponding request is granted if the measured power pattern from that PC is similar to the main power pattern of the respective floor. Power patterns and their periodicity can function similarly to one-time password (OTP) based on security policies, thereby enabling continuous passive authentication by the continuous measurement of power patterns.

This approach partitions locations based on specific patterns using shared power resources within the power system of a building. This capability allows geographic information to be obtained when certain power patterns generated in a specific area match the connected power patterns, similar to GPS functionality. Malicious users experience difficulty in imitating specific patterns because of variations in the power-event patterns and cycles. This system provides convenience by passively performing continuous authentication. The GEA system simplifies the authentication process, reduces costs, and minimizes system maintenance by utilizing existing power infrastructure. Consequently, attempting malicious access to a PC from outside the building to generate patterns similar to a specific power signal at specific times becomes challenging. In addition, the GEA system proposed in this study determines the scope of the area to be authenticated based on the electrical patterns injected into the power system by the administrator. For instance, the injection of electrical patterns into the power system for each floor of a building enables the authentication patterns to change for each floor, thereby enabling the identification of the building and floor location of the PCs requesting authentication.

This paper describes the design of the proposed GEA system, outlines the environmental configuration required for its operation, and presents experimental results to demonstrate the feasibility and efficiency of the proposed system.

II. Related work

The proposed GEA system injects patterns into the power provided by the building and detects similar patterns in computing devices connected to that power, thus performing geolocation authentication when the computing device exists within the building. The analysis of power patterns and extraction of meaning from these patterns is known as side-channel analysis, and it has been extensively studied. In this section, we describe side-channel analysis studies and explain the power analysis performed in the proposed GEA system.

Side-channel analysis is based on the idea that information can be inferred from the power consumption or electromagnetic emissions of a computing system. Several techniques have been applied to assess various device types in the side-channel research area by analyzing the power consumption and study patterns throughout them, such as PCs, laptops, smartphones, and vehicle stations.

Because the run time and power consumption represent the main constraints of a real-life cryptographic device in exposing the device's secrets, Koeune [5] provided a detailed tutorial on side-channel attack cryptographic devices. The authors described physical security, the main types of attacks, and their principles. After collecting the physical characteristics of the device, such as running time and power patterns, attackers analyze the obtained patterns and exploit the findings to expose the device's secrets. Kocher [6] addressed the practicality of the assumption by cryptosystem designers that secrets are manipulated in closed, reliable computing environments. They presented methods for analyzing power consumption measurements to prove that computers and microchips leak information during their operations, and thereby developed approaches for building secure cryptosystems.

Alexander [7] found that current wireless charger transmitters are vulnerable to power-side channel attacks because they leak information related to smartphone activities. They proved this concept by conducting a website fingerprinting attack through a wireless charging side channel on iOS and Android devices. The scenario involves monitoring and drawing varying amounts of current as mobile websites from the Alexa Top Site list are loaded on the charging phone. Cronin [8] explained that a side-channel attack on touch-based devices such as smartphones and tablets poses security threats and leaks information through the power line. They collected power traces and built a side-channel attack on a passcode-unlock screen for 4-digit and 6-digit case studies on Android and iOS smartphones.

Bai [9] presented an approach to detecting anomalous behavior in IoT using side-channel analysis. They introduced remote access to side channels (RASC), which is an external monitoring printed circuit board (PCB) system that enables the monitoring of the power and electromagnetic (EM) traces of target IoT devices. Conti [10] focused on smart buildings, where all features in a building are controlled by network sensor readings to manage the environment and reduce cost. The author investigated the feasibility of identifying a pair of laptop users (*i.e.,*, the user is using his/her laptop) connected to a wall socket by collecting power traces produced by the user's laptop.

III. System design of the work

In this study, we introduce a GEA system and propose an innovative security authentication method based on a building's power system within the facility. The proposed system enables secure authentication by transmitting specific power patterns between computing devices that share power resources. The GEA system has the following features.

Each floor has its main power source connected to PCs. The main power source generates power patterns. The PCs measure the power consumption at the hardware level and compare the measured power consumption graph with the power graph of the main power source. If the power pattern generated by a PC is similar to that of the main power, the PC is granted authorization. Authorization refers to permission for PC usage and access to specific data.

To implement the proposed GEA system, power networks are arranged on each floor, thus allowing the differentiation of power patterns generated in different regions when power patterns vary on each floor. For instance, assume that different power patterns are generated on the 2nd and 3rd floors; this indicates the possibility of distinct power occurrences, such as electrical flickers, momentary power outages, or voltage fluctuations, in each region. Thus, the power within the PCs' internal hardware must be analyzed using sensors provided by the computer hardware to perform the authentication system in the proposed environment. In addition, PC power consumption is analyzed using side-channel techniques to detect power patterns from specific floors in a particular building and provide geographic information regarding the PCs.

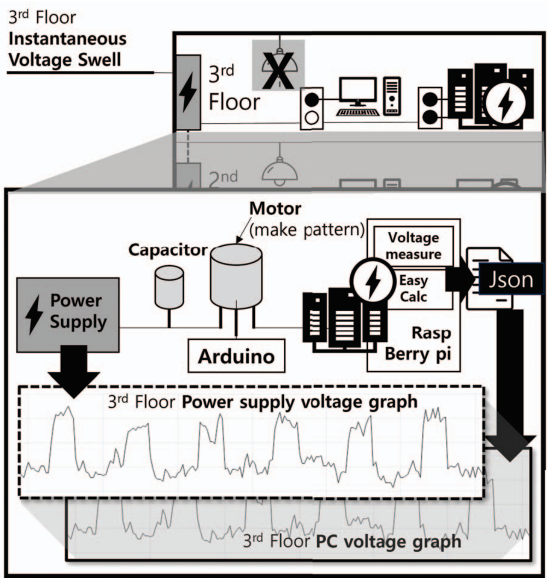

Fig. 2: Experiment design of GEA system

IV. Experiments and Results

The proposed GEA system verifies the presence of a PC within a specific geographical area by connecting it to a power supply. In this section, the GEA system is experimentally configured, as shown in Fig.2, and the feasibility of the GEA system implementation is explained by conducting a side-channel analysis. As shown in Fig.2, the proposed GEA system comprises power supplies on each floor. These power supplies generate electrical patterns and are connected to a PC undergoing authentication. For the experiments, a 5.7-V power supply was provided and a motor was attached to generate a potential drop, causing a momentary decrease in voltage from the existing power state. A Raspberry Pi board version 4 was used to authenticate the PC. Because the Raspberry Pi cannot measure the power consumption voltage, the voltage measurement was performed using its 3.3 V pin. In addition, to prevent PC shutdown owing to insufficient power caused by frequent power pattern generation, a capacitor was attached to supplement the power. The experiments measured DC voltage, but with frequency adjustments, AC voltage could also be obtained. Furthermore, in real PC power analysis, the use of voltage measurement components within the PC hardware or measurement from the PC's power source can increase the accuracy of the power pattern analysis. Fig.3. shows the injection of different power patterns on the 2nd and 3rd floors, as configured in Fig.2, and the measurements obtained from the PCs connected to each power supply. As presented in the

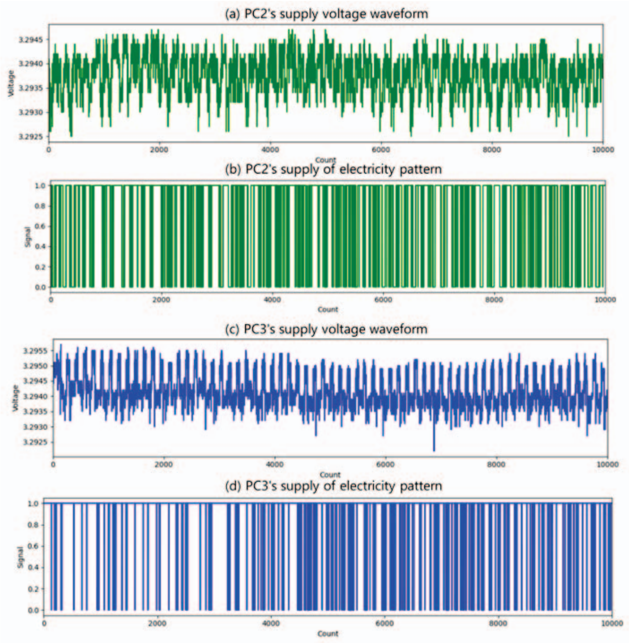

Fig. 3: Experiment result of GEA system

table, the similarity between the power pattern generated on the 2nd floor and PC2's power pattern can be observed, as well as the similarity between the power pattern generated on the 3rd floor and PC3's power pattern. This demonstrates the analysis of power patterns and the ability to provide geographical information by comparing similarities. Fig.3.3(a) presents the wave information of the voltage measured by the PC. The voltages were collected at 30-ms intervals. Fig.3.3(b) shows the electrical pattern delivered to PC2. Essentially, by comparing (a) and (b), we can see that the delivered electrical signal causes a specific pattern in PC2. Consequently, we delivered different patterns to PC2 and PC3, as shown in (b) and (c), and we can see that they produce specific voltage patterns, as shown in (a) and (c). By analyzing the waves, as shown in the Fig.3, we can classify the similarity as 99%. This experiment can be further enhanced by performing side-channel and similarity analyses using AI to achieve more accurate measurements.

V. Conclusion

Recently, Zero Trust security models have been implemented to enhance the security of IT systems. Unlike traditional models, this model continuously requires authentication for every action and element, distrusting and monitoring all security components such as users, computing devices, and data. Implementing Zero Trust is expensive and demands policy changes, which can lead to increased system complexity and reduced user convenience. This study introduced a GEA system that performs GEA between building power systems and computing devices. The proposed GEA system detects power patterns on each floor using the building's power system, and verifies them within the computing devices by comparing them with expected patterns. This approach enables authentication between the building and the computing devices, essentially allowing access only within authenticated premises. This approach utilizes shared power resources within a building to partition locations based on specific patterns, thus making it difficult for malicious users to imitate patterns owing to variations in power event patterns and frequencies. In addition, the proposed GEA system aims to enhance the authentication process by considering various variables and systematically training a power analysis system to perform authentication even during disruptions caused by natural disasters.

Acknowledgment

This work was supported by the Institute of Information & Communications Technology Planning & Evaluation (IITP) ,(Project No. RS-2022-00165794, Development of a Multi-Faceted Collection-Analysis-Response Platform for Proactive Response to Ransomware Incidents, 30%), (Project No.2022-0-00701, 10%, Project No.RS-2023-00228996, 10%), the ICT R&D Program of MSIT/IITP, (Project No. 2021-0-01816, A Research on Core Technology of Autonomous Twins for Metaverse, South Korea, 10%), and a National Research Foundation of Korea (NRF), South Korea grant funded by the Korean government (Project No. RS-2023-00208460, 40%).

References

[1] VA Stafford. Zero trust architecture. *NIST special publication*, 800:207, 2020.

[2] Yuanhang He, Daochao Huang, Lei Chen, Yi Ni, and Xiangjie Ma. A survey on zero trust architecture: Challenges and future trends. *Wireless Communications and Mobile Computing*, 2022, 2022.

[3] Christoph Buck, Christian Olenberger, André Schweizer, Fabiane Völter, and Torsten Eymann. Never trust, always verify: A multivocal literature review on current knowledge and research gaps of zero-trust. *Computers & Security*, 110:102436, 2021.

[4] Songpon Teerakanok, Tetsutaro Uehara, and Atsuo Inomata. Migrating to zero trust architecture: Reviews and challenges. *Security and Communication Networks*, 2021:1–10, 2021.

[5] François Koeune and François-Xavier Standaert. A tutorial on physical security and side-channel attacks. *International School on Foundations of Security Analysis and Design*, pages 78–108, 2004.

[6] Paul Kocher, Joshua Jaffe, and Benjamin Jun. Differential power analysis. In *Advances in Cryptology—CRYPTO'99: 19th Annual International Cryptology Conference Santa Barbara, California, USA, August 15–19, 1999 Proceedings 19*, pages 388–397. Springer, 1999.

[7] Alexander S La Cour, Khurram K Afridi, and G Edward Suh. Wireless charging power side-channel attacks. In *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*, pages 651–665, 2021.

[8] Patrick Cronin, Xing Gao, Chengmo Yang, and Haining Wang. {Charger-Surfing}: Exploiting a power line {Side-Channel} for smartphone information leakage. In *30th USENIX Security Symposium (USENIX Security 21)*, pages 681–698, 2021.

[9] Yunkai Bai, Andrew Stern, Jungmin Park, Mark Tehranipoor, and Domenic Forte. Rascv2: Enabling remote access to side-channels for mission critical and iot systems. *ACM Transactions on Design Automation of Electronic Systems (TODAES)*, 27(6):1–25, 2022.

[10] Mauro Conti, Michele Nati, Enrico Rotundo, and Riccardo Spolaor. Mind the plug! laptop-user recognition through power consumption. In *Proceedings of the 2nd ACM International Workshop on IoT Privacy, Trust, and Security*, pages 37–44, 2016.