# Evaluating IoT Device Pairing Authentication Techniques

Group 2:
Niklas Bernardo Correa, Sarah Dill, Edwin Liu, Alison Nakai-Lackey, Andrea Pallotta

## Introduction and Motivation

Many essential systems—including smart-home devices, factories, cars, and blood glucose meters—require distinct instruments to exchange information reliably and securely. Device pairing is the first phase in establishing a communication channel between devices. Issues during the pairing phase can lead to system failure. This can have potentially ruinous consequences for the user and their security and privacy. For example, a malicious third party may obtain sensitive information or have control over the system.

The Internet of Things (IoT) landscape offers significant challenges for secure pairing, as sometimes it is performed between devices that differ both in terms of computation power and ability to interact with the surrounding environment. These devices might be located a few feet away or across the globe and might require the help of the user (manual pairing).

The broad scope of scenarios under which pairing must take place means that there is no one-size-fits-all pairing scheme. Thus, this project aims to understand the constraints and threat model for various IoT device-pairing authentication techniques and evaluate them in different environments.

## Background

The term “device pairing” (also known as “device association”) refers to the process of virtually tying two or more devices together to establish a secure communication channel. A device pairing scheme must provide a way for a device to verify that the other party is the device it intends to communicate with.

## Research Question

The following research questions have been devised:

- When IoT device pairing occurs within the LAN, what attacks must be protected against, and what schemes provide the best protection?
- What authentication techniques can be employed in pairing schemes involving power-constrained devices?
- When IoT device pairing occurs between a user and a device using biometric information, what are the most promising techniques in terms of effectiveness, privacy, and security?
    - What are the limitations of these techniques?
    - Which of these techniques do we believe is the “best”?

## Method

We will collect the necessary data from related papers on IoT pairing authentication and introduce the different types of authentication schemes and their limitations in terms of computational power, usability, environment, and the threat model they address. Our detailed methods are as follows.

- First, we will carefully read papers on IoT pairing authentication schemes to understand typical use cases and threat models.
- We will also collect information on security and privacy issues with established authentication schemes.
- Finally, we will compare how authentication schemes that overlap compare to one another and rank them according to their ability to strike a balance between security and usability.

## Preliminary findings

We have so far narrowed down the categories for IoT authentication schemes into:

- Local
    - Proximity-based [1] [11]
        - Motion-based
        - Signal strength-based
        - Ad-hoc IoT networks
    - Sound-based [8]
        - Acoustic signals / “reference signals”
- Remote
    - Blockchain-based [3] [7]
    - Hardware-based
        - PUF [2]
- Wearable [10]
    - Gait-based [9]
- Pairing-based Cryptography [6]
    - Full Dent IBE scheme
- Elliptic Curve Cryptography (ECC) [4]
- Multi-factor [10] [12]

## References

[1] A. A. S. AlQahtani, H. Alamleh and B. Al Smadi, "IoT Devices Proximity Authentication In Ad Hoc Network Environment," 2022 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS), 2022, pp. 1-5.

[2] B. Kim, S. Yoon, Y. Kang and D. Choi, "PUF based IoT Device Authentication Scheme," 2019 International Conference on Information and Communication Technology Convergence (ICTC), 2019, pp. 1460-1462.

[3] D. Li, W. Peng, W. Deng and F. Gai, "A Blockchain-Based Authentication and Security Mechanism for IoT," 2018 27th International Conference on Computer Communication and Networks (ICCCN), 2018, pp. 1-6.

[4] Hsiao-Ling Wu, Chin-Chen Chang, Long-Sheng Chen, Secure and anonymous authentication scheme for the Internet of Things with pairing, Pervasive and Mobile Computing, Volume 67, 2020, 101177.

[5] J. Zhang, Z. Wang, Z. Yang and Q. Zhang, "Proximity based IoT device authentication," IEEE INFOCOM 2017 - IEEE Conference on Computer Communications, 2017, pp. 1-9.

[6] Karantaidou, I., Halkidis, S.T., Petridou, S., Mamatas, L., Stephanides, G. (2018). Pairing-Based Cryptography on the Internet of Things: A Feasibility Study. In: Chowdhury, K., Di Felice, M., Matta, I., Sheng, B. (eds) Wired/Wireless Internet Communications. WWIC 2018. Lecture Notes in Computer Science(), vol 10866. Springer, Cham.

[7] L. Wu, X. Du, W. Wang and B. Lin, "An Out-of-band Authentication Scheme for Internet of Things Using Blockchain Technology," 2018 International Conference on Computing, Networking and Communications (ICNC), 2018, pp. 769-773.

[8] N. Z. Gong et al., "PIANO: Proximity-Based User Authentication on Voice-Powered Internet-of-Things Devices," 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS), 2017, pp. 2212-2219.

[9] P. Musale, D. Baek, N. Werellagama, S. S. Woo and B. J. Choi, "You Walk, We Authenticate: Lightweight Seamless Authentication Based on Gait in Wearable IoT Systems," in IEEE Access, vol. 7, pp. 37883-37895, 2019.

[10] S. Yu, N. Jho and Y. Park, "Lightweight Three-Factor-Based Privacy- Preserving Authentication Scheme for IoT-Enabled Smart Homes," in IEEE Access, vol. 9, pp. 126186-126197, 2021

[11] Sun, F., Mao, C., Fan, X., & Li, Y. (2019). Accelerometer-Based Speed-Adaptive Gait Authentication Method for Wearable IoT Devices. IEEE Internet of Things Journal, 6(1), 820–830.

[12] A. Ometov, V. Petrov, S. Bezzateev, S. Andreev, Y. Koucheryavy and M. Gerla, "Challenges of Multi-Factor Authentication for Securing Advanced IoT Applications," in IEEE Network, vol. 33, no. 2, pp. 82-88, March/April 2019.