INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES TOULOUSE

REPORT SECURITY INNOVATIVE PROJECT

5A ISS - 2024/2025

By Brian Biendou
Achille Caute
Marie Brunetto
Timothé Bigot

Introduction

In simple or complex systems, any electronic device and digital system could be exposed to security issues, by malevolent attackers or simply by some untreated systemic issues. During the development of our Innovative Project, we have to question ourselves about potential weaknesses of our implementation. Through this report, we will explore our system, divided into sections, and question ourselves about security topics that could be associated, and which approach we should take to solve them.

Our report will be divided into two main sections: the bluetooth communication between the device and the confidentiality of the data that our system has or might implement. More specifically on BLE (Bluetooth Low Energy) that is suitable for our application with low power consumption objectives.

On the following figure, we can see an overview of the possible threats that may occur on the BLE protocol. We will not be able to cover the entire threats but we can have a global point of view of the risks that our system could face.

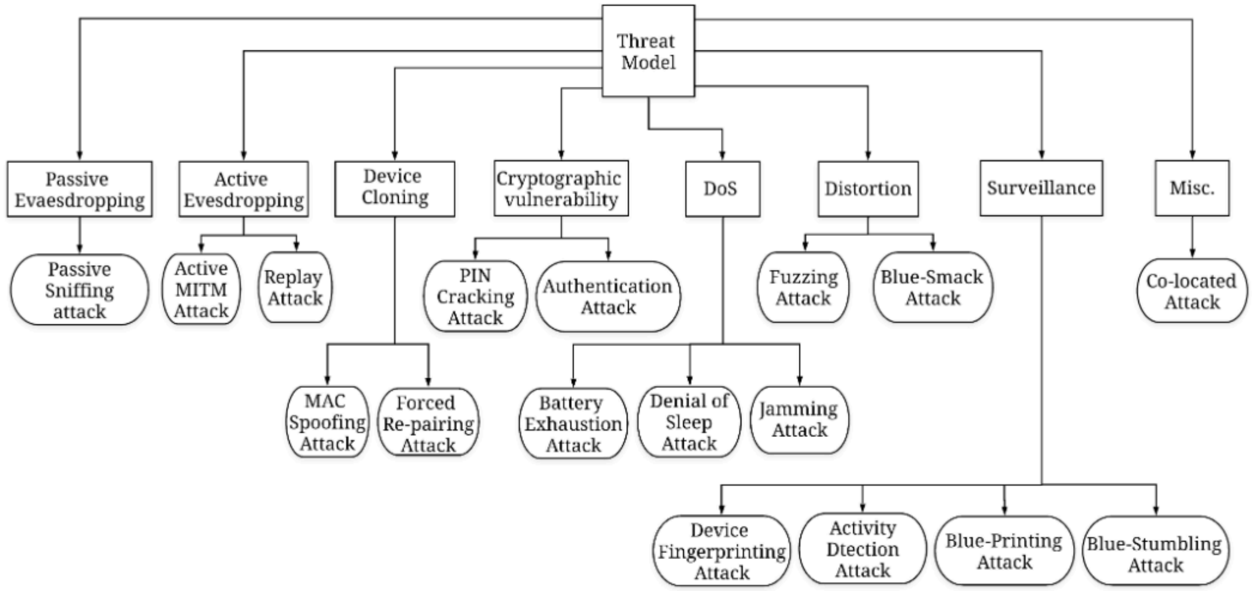

Figure 1 : BLE threat model on the basis of the attack domain [1]

Bluetooth connection between devices

Our project relies on a phone to support an application interfacing with the user and manage the communication between the devices. Although it allows us to create a complex application and facilitate the implementation of further communication, such as a potential database, it restricts the protocols that we can use for communication to Wi-fi, Bluetooth and Cellular (2G, 3G, 4G or 5G)

Due to the short range of our application, the energetic needs and the facility of development, our choice went to Bluetooth, more specifically Bluetooth Low Energy (BLE). BLE implements multiple security procedures, with levels of authentication and encryption.

Connection between the phone and the tricycle

The first connection that we need to securize is the one that the phone will have with the tricycle, more precisely with an ESP32 that will be embedded on the vehicle, that communicates directly with the motor. This development board integrates a Bluetooth module.

The main issue that we might encounter for this communication is the identification of the user: we want to make sure that the BLE connection is made with the associated vehicle, and not by a nearby one. We could imagine that a potential attacker could try to connect the vehicle we drive, and control some aspect of the driving regardless of what we wish for.

Currently, the ESP allows only one Bluetooth connection. We could ensure that the connection is the appropriate one by associating an identification number to the displayed bluetooth name. In case this one is not found, it means that it is currently associated with another device, and the user should be able to reset the connection.

Finally, if the user does not want to use the cardiac rhythm functionality, they should be able to turn it off. The system should be able to work without any information from the phone, without having issues or errors.

Key based security

A way to implement the security regarding the proper identification is the use of asymmetrical encryption, using an identification number and a pair of keys to ensure the identity of the phone/device pair. The public key would be available on a web server, while the private key would be stored directly on the tricycle. The key exchange would involve 3 actors: a web server, a tricycle and a phone:

1. The phone asks the public key assigned to this specific tricycle to the web server
2. The web server gives the key
3. The Phone encrypts a challenge (random number) using the public key
4. This encrypted challenge is sent to the tricycle, which deciphers it through its own private key.
5. The challenge is returned to the phone. If it matches the original one, the connection can be established, as both devices are recognized.

However, this implementation still have some issues:

- The generation of the private and public key needs to be defined before use.
- The tricycle (ESP32) needs to be able to store the private key. Currently, there is no persistence of the data when the system is turned off, making it tricky to have a private key. Otherwise, it might need to be generated at activation and be able to communicate with the website to give it. An internet connection would then be required.
- Each tricycle needs to have a proper identification to be able to get the matching public key on the website.

Connection between the phone and the watch

To get the information of the heart rate, we decided to use a smart watch. The smart watch offers an API that allows to get the data gathered by the watch. We are currently using a Garmin Watch that requires a connection by entering the username and password.

We are still not sure if this account would be the one from the user to which the watch belongs, or the company's account to which a paid API key might be applied. In both cases, we need to ensure that the credentials will be kept confidential and in case they need to be stored, will be encrypted.

Another solution we had to get the heart rate was the direct use of a sensor that would get the rhythm. In that case, a system would embed the sensor, and the communication would be managed by us. In that case, we would also need to ensure the availability, confidentiality and integrity of the transferred data by using a reliable protocol. In that case, BLE would remain the best option.

Machine learning and Blockchain to improve security

We can expect to improve bluetooth communication with the recent development and applications of machine learning. Currently, there is an open research opportunity to protect the BLE mesh network from zero-day vulnerability, DoS attacks, spoofing attacks using intrusion detection systems and intrusion prevention systems, and watchdogs.Introducing new aspects of machine learning algorithms is a promising area of research for enhancing the security and privacy of IoT devices.In the wrong hands, the power of AI can be exploited. AI is frequently used by attackers to uncover and exploit flaws far faster than developers can repair them.[1]

BLE enabled smart wearable and IoT devices have been seamlessly integrated into our everyday life. So secure data management and robust access control of IoT devices are becoming very important. The idea of using a server to connect with an IoT device rather than connecting with an individual device directly may enhance device management and users' privacy significantly. This server will store users preferences, thus preventing IoT devices from accessing personal information. But if the network/server is breached, then every device connected to that network will be compromised. So there is a research opportunity to use decentralized block-chain technology to secure IoT devices connected in a BLE mesh network. [1]

Data confidentiality

Information relative to the calculation

A functionality we did not implement is the ability for the user to enter their age and weight to adapt with more precision the model. If done, as this information is personal, we should ensure confidentiality in case we decide to keep it stored so the user does not have to enter them at each connection. In our case, as we developed a website, this information could be kept as a cookie. Using Json Web Tokens (JWT), we could properly store and even encrypt the data so it might not be gathered by other agents.

Conclusion

We saw that a system as simple as the effort on a tricycle adapted from the heart rate has many security threats and risks. However, due to the lack of time, we were not able to implement any proper security prevention, outside of the use of the BLE protocol, embedding some solution to keep the integrity and availability of our data.

Sources

[1] 1. Barua, M. A. Al Alamin, M. S. Hossain and E. Hossain, "Security and Privacy Threats for Bluetooth Low Energy in IoT and Wearable Devices: A Comprehensive Survey," in *IEEE Open Journal of the Communications Society*, vol. 3, pp. 251-281, 2022, doi: 10.1109/OJCOMS.2022.3149732.