Sardar Patel Institute of Technology

Department of Computer Engineering
Academic Year 2016-17

Smart Locks Re-engineered : Security in IoT devices

Ganesh Baleri, Chaitanya Bapat, Shivani Inamdar, B.E.(Comp.)
Project Guide: Dr. Anant V. Nimkar

Abstract

To connect a lock with a key in Internet of Things(IoT) we need to use Bluetooth Low Energy(BLE) protocol. BLE protocol is designed to be power efficient and has been popular for transporting data between smartphones and IoT devices. One vulnerability of BLE protocol is the Man-in-the-Middle(MITM) attack. We examine different techniques that are aligned with BLE to ensure fundamental security requirement and protect communication and some research challenges. As a possible solution, we propose combination of Image Steganography and Cryptography to overcome vulnerabilities of BLE protocol.

Introduction

The Internet of Things (IoT) is a vast field where devices communicate with each other over predefined protocols, without manual intervention of humans. Smart Locks obviate the need to access traditional physical locks. They communicate over BLE protocol. It is a wireless personal area network technology designed for low power consumption for IoT devices. However, BLE is susceptible to network security threats and attacks. Attacks like MITM are those where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other. Hence, we have proposed a system to overcome these vulnerabilities and strengthen the Smart Lock safety.

Aim

The security of Smart Locks is compromised due to eavesdropping attacks. If the key to any smart lock is acquired by an attacker, then they can easily take control of the lock, thereby causing inconvenience to the owner of the lock. Most smart locks use the BLE for communication. BLE is susceptible to MITM attacks in its pairing stage. Thus, the aim of this project is to secure smart locks by applying a combination of cryptographic and steganographic techniques.

Objectives

Following are the two objectives of our project :-

1. Configure the communication between smart lock and Android phone using Raspberry Pi
2. Apply encryption and steganographic techniques to add a layer of security to smart locks

Problem Definition

BLE protocol uses Cryptography as a security mechanism. However, BLE is still vulnerable to security attacks like eavesdropping and MITM. In the pairing phase, there exists a loophole that needs to be addressed to fortify the system. The sole application of encryption leaves the system still exposed to threats and attacks. Hence, an extra layer of security and privacy needs to be added to support complete protection to IoT devices, particularly smart locks, which communicate over BLE. This system adds a steganographic layer to smart lock security, thus making it difficult for the attacker to even detect the existence of a message.

Methodology

Cryptography is a technique of jumbling or changing the form of the message. Steganography is a method of hiding the message in such a way that its existence cannot be perceived. As a result, the attacker is unable to detect the presence of message (key of the smart lock). Combining the concepts of Cryptography and Steganography, message will first be encrypted using encryption algorithm and further will be hidden inside an image using Steganography technique. This will protect our Smart Lock from security attacks like Man-in-the-middle and Eavesdropping.

Design

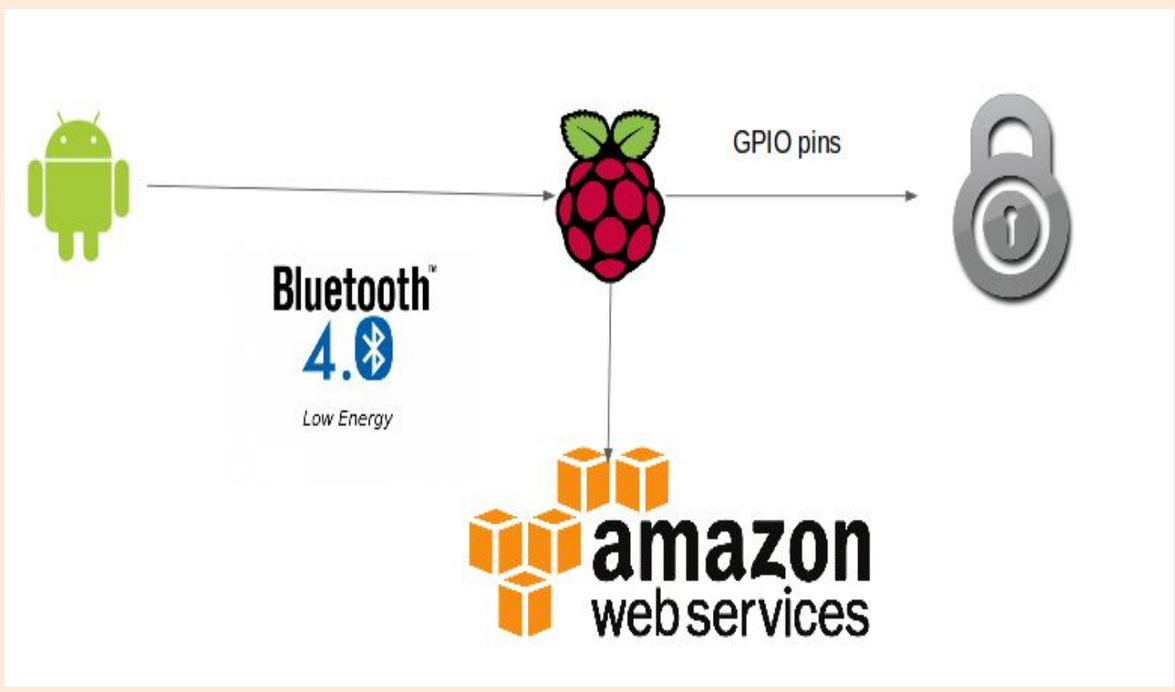

Fig 1 - System Design of Smart Locks with Raspberry Pi, Android smartphone over BLE protocol

Raspberry Pi will act as an interface between the smart lock and a smartphone (user). BLE 4.0 protocol is employed at the Android smartphone – Raspberry Pi interface. General Purpose Input Output (GPIO) pins used at Raspberry Pi – Smart Lock interface.

Conclusion

In order to tackle the vulnerability of Man-in-the-middle attack in Bluetooth Low Energy protocol, we combined the techniques of Cryptography with Steganography.

References

[1] Carles Gomez, Joaquim Oller and Josep Paradells, “Overview and Evaluation of Bluetooth Low Energy: An Emerging Low-Power Wireless Technology ”, ISSN 1424-8220, Sensors, 2012

[2] P. Thiyagarajan, G. Aghila, and V. Prasanna Venkatesan, “Stepping Up Internet Banking Security Using Dynamic Pattern Based Image Steganography”, Advances in Computing and Communications: First International Conference, ACC 2011, Kochi, India, July 22-24, 2011, Proceedings, Part IV, 978-3-642-22726-4, Springer-Verlag Berlin Heidelberg, 2011