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

Smart locks make use of the Bluetooth Low Energy (BLE) protocol to communicate with other IoT devices and smartphones. BLE is designed to be power efficient and has been popular for transporting data. However, one vulnerability of BLE protocol is the Man-in-the-Middle (MITM) attack. We examine existing techniques that are aligned with BLE to ensure fundamental security requirement and protect communication. We propose the combination of Image Steganography and Cryptography for transferring keys over BLE, thus overcoming its vulnerabilities.

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 Man-in-the-Middle (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

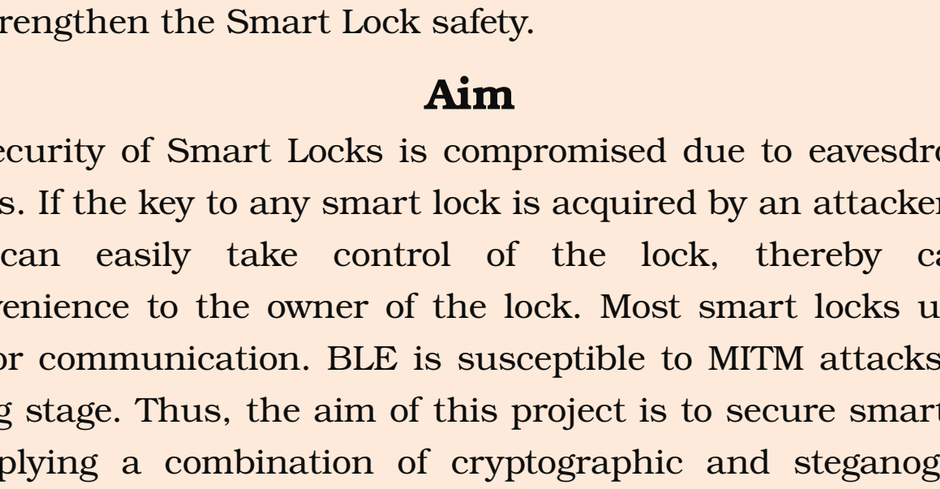
The security of Smart Locks is compromised due to eavesdropping attacks. If the key to any smart lock is acquired by an attacker, then they can easily take control of the lock, thereby causing inconvenience to the owner of the lock. Most smart locks use the BLE for communication. BLE is susceptible to 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

The following are the two objectives of our project :-

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

Problem Definition



BLE is vulnerable to MITM in which the attacker can intercept and corrupt the messages between the two parties. This takes place in the second stage of the pairing phase when the JustWorks security system is deployed.

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 MITM and Eavesdropping.

Design

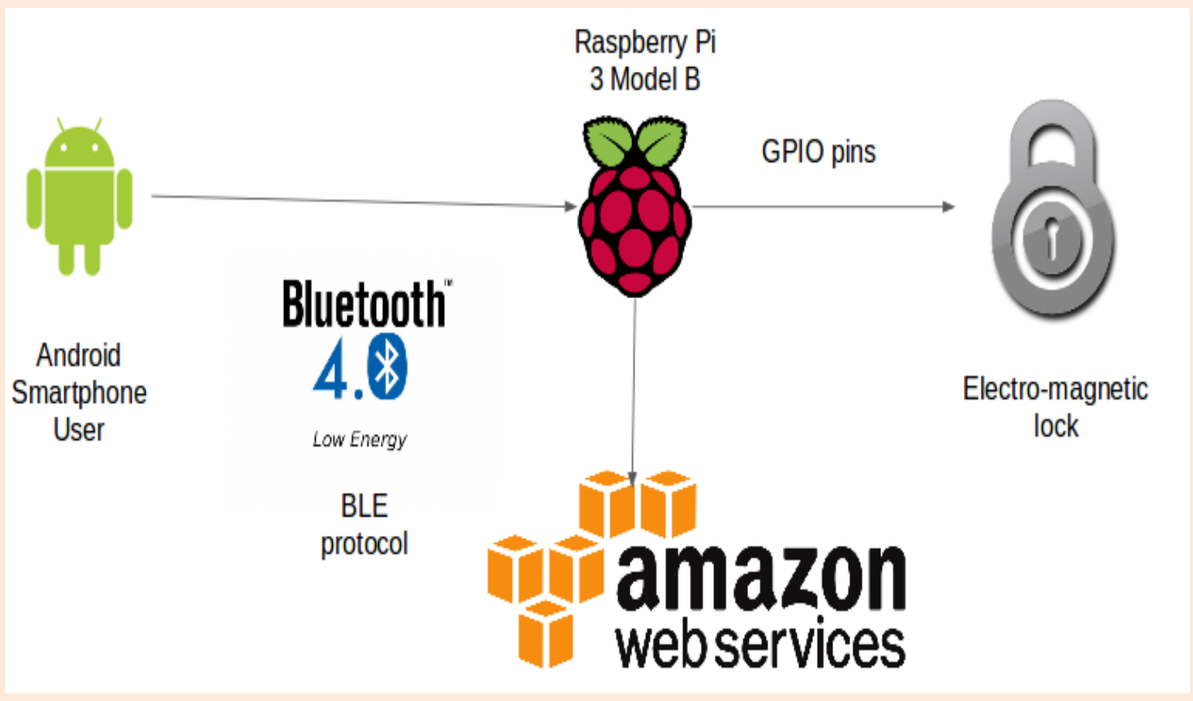


Fig 1 - System Design of Smart Locks with Raspberry Pi, Android smartphone over BLE protocol

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] Gomez C, Oller J, Paradells J. Overview and Evaluation of Bluetooth Low Energy: An Emerging Low-Power Wireless Technology. Sensors (Basel, Switzerland). 2012;12(9):11734-11753. doi:10.3390/s120911734.

[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, Springer-Verlag Berlin Heidelberg, 2011