Smart Locks Re-engineered : Securing IoT devices using Steganography

Project Guide: Dr. Anant Nimkar, Associate Professor
Project By : Ganesh Baleri
Chaitanya Bapat
Shivani Inamdar

Table of Contents

Introduction

- 21st century = Century for Internet of Things
- Phenomenal growth in interconnected devices -> Threats
- Result = Insecurity of Things
- Objective - Robust security solution to existing IoT devices like Smart Locks
- Reason -
  - Providing extra layer of security
  - Improve the existing architecture of IoT devices

Motivation

- Most IoT devices use Bluetooth Low Energy protocol.
- Number of vulnerabilities associated with the Bluetooth Low Energy (BLE).
- Primary vulnerability in BLE = Man in the Middle (MITM) attack
- Steganography overcomes MITM attack

Literature Review

Overview and Evaluation of Bluetooth Low Energy: An Emerging Low-Power Wireless Technology, Carles Gomez , Joaquim Oller and Josep Paradells, Sensors, ISSN 1424-8220, 2012	● BLE Protocol Stack explained ● Potential threats of BLE ● 3 phases in Bluetooth pairing. ● Vulerability of Just Works.
Secure Internet Banking Authentication Hiltgen, A., Kramp, T., Weigold, T. IEEE Security and Privacy 2006	● Prevention of MITM attack by using Short-term password solutions (OTP) E.g. VeriSign, Active Card

Literature Review

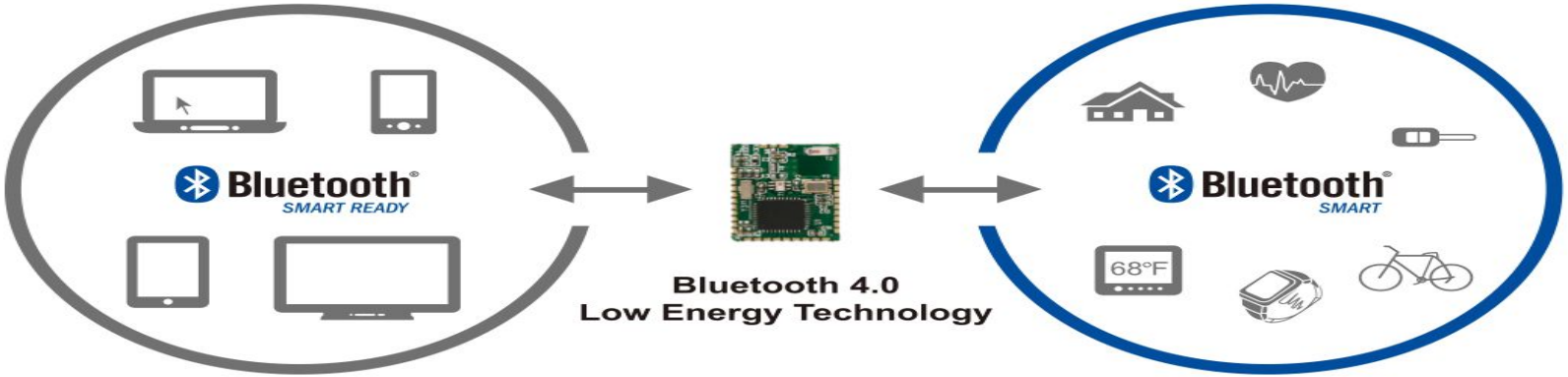
SMS-Based One time Password vulnerabilities and safeguarding OTP over network A. Karia, A. B. Patankar, and P. Tawde 2014	● Counter MITM and phishing attack on authentication and authorization ● Vulnerability - Wireless interception, Mobile phone trojans, SIM Swap attack
Stepping Up Internet Banking Security Using Dynamic Pattern Based Image Steganography P. Thiyagarajan, G. Aghila, and V. Prasanna Venkatesan Springer-Verlag Berlin Heidelberg 2011	● Utilizing Steganography for protection against MITM attack. ● Man-in-the-Middle attack principle ● Proposed - Stego-layer method ● Prevents MITM and Session Hijacking

Current Smart Lock System

- Smart Locks uses BLE protocol
- BLE protocol vulnerable to MITM attacks
- Just Works - Phase 2 of BLE Pairing - Vulnerability
- Less Secure

Bluetooth Low Energy Protocol

- Wireless technology based on low power consumption
- Allows short range communication
- IoT devices (smart locks, proximity sensors, heart rate monitors) work on BLE
- BLE has greater deployment expectations than other low power technologies such as Zigbee, 6 LoWPAN, Z-Wave

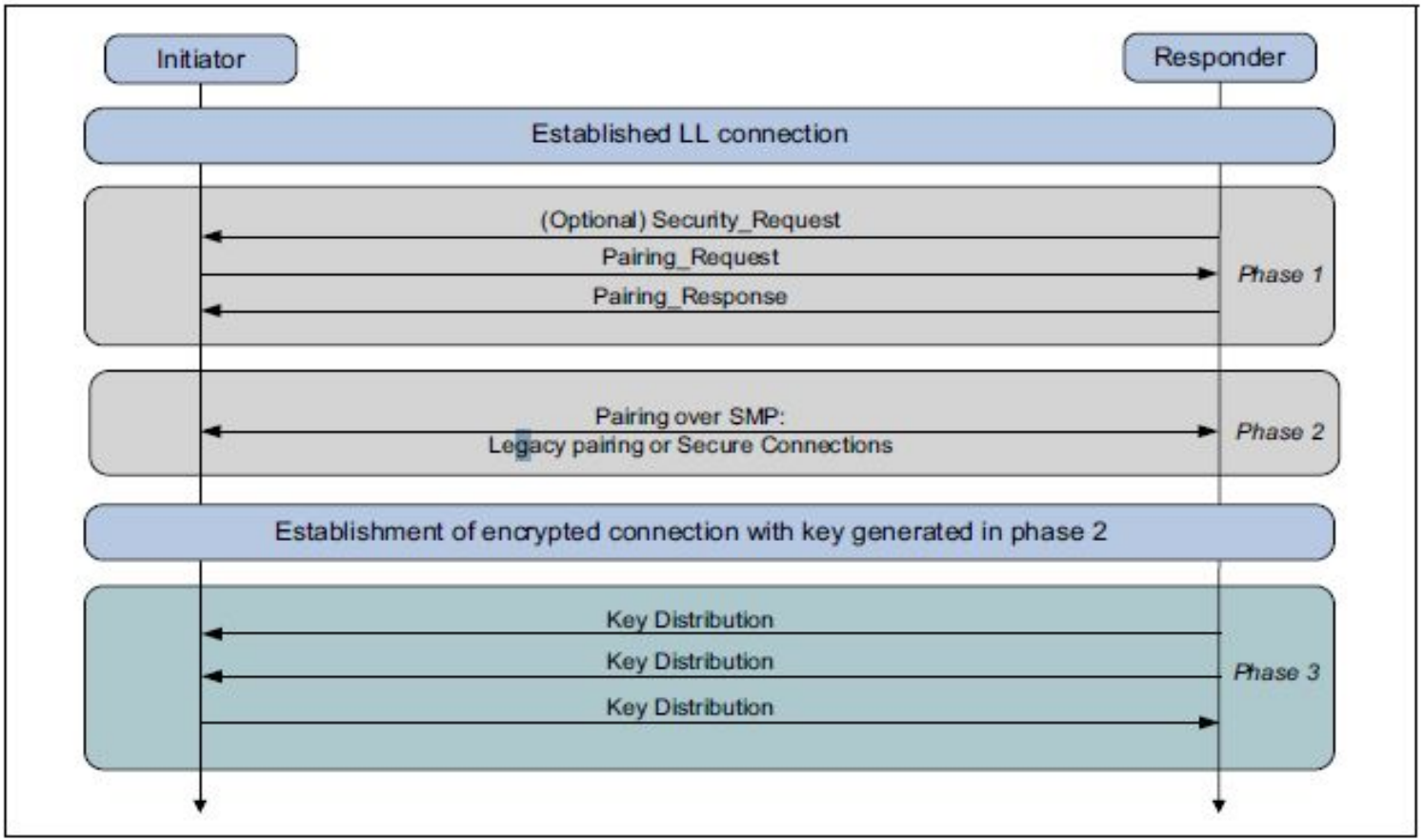


Security at the Link Layer

- 128-bit AES block cipher
- Cipher Block Chaining-Message Authentication Code (CCM) Protocol
- Secure pairing done in 3 phases:

1. **Phase 1**: Devices announce their I/O capabilities
2. **Phase 2**: Generation of STK (Short Term Key) and agreement on TK (Temporary Key)
3. **Phase 3: LTK (**Long Term Key**), CSRK** (Connection Signature Resolving Key)**, IRK** (Identity Resolving Key) are shared between end-points

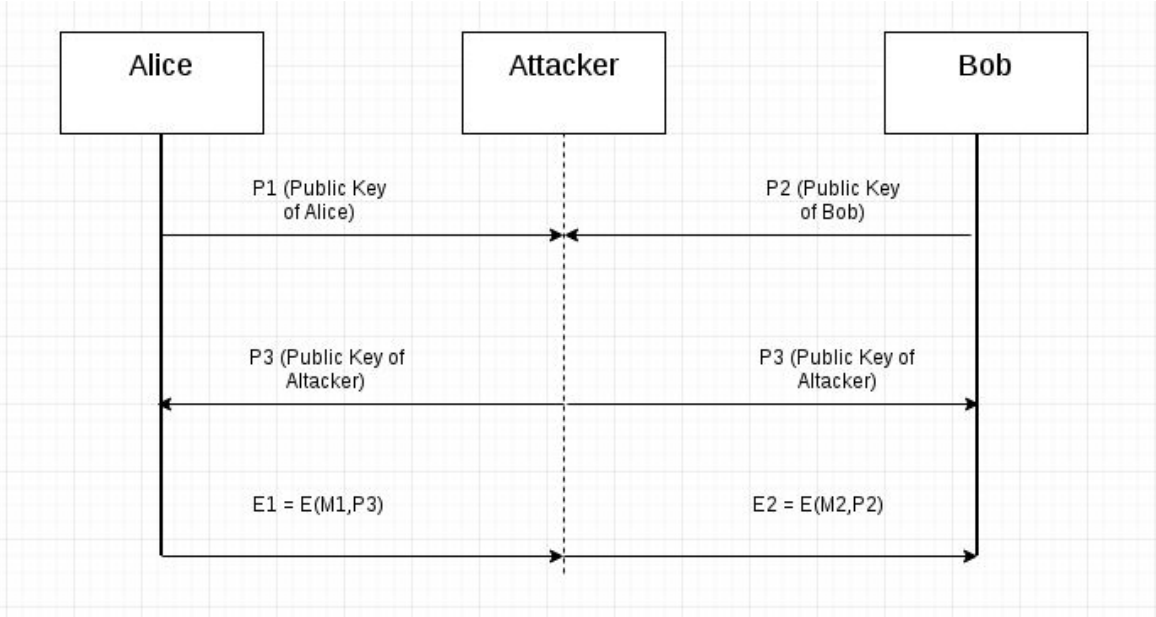
Pairing in BLE protocol using SMP



Vulnerabilities in BLE

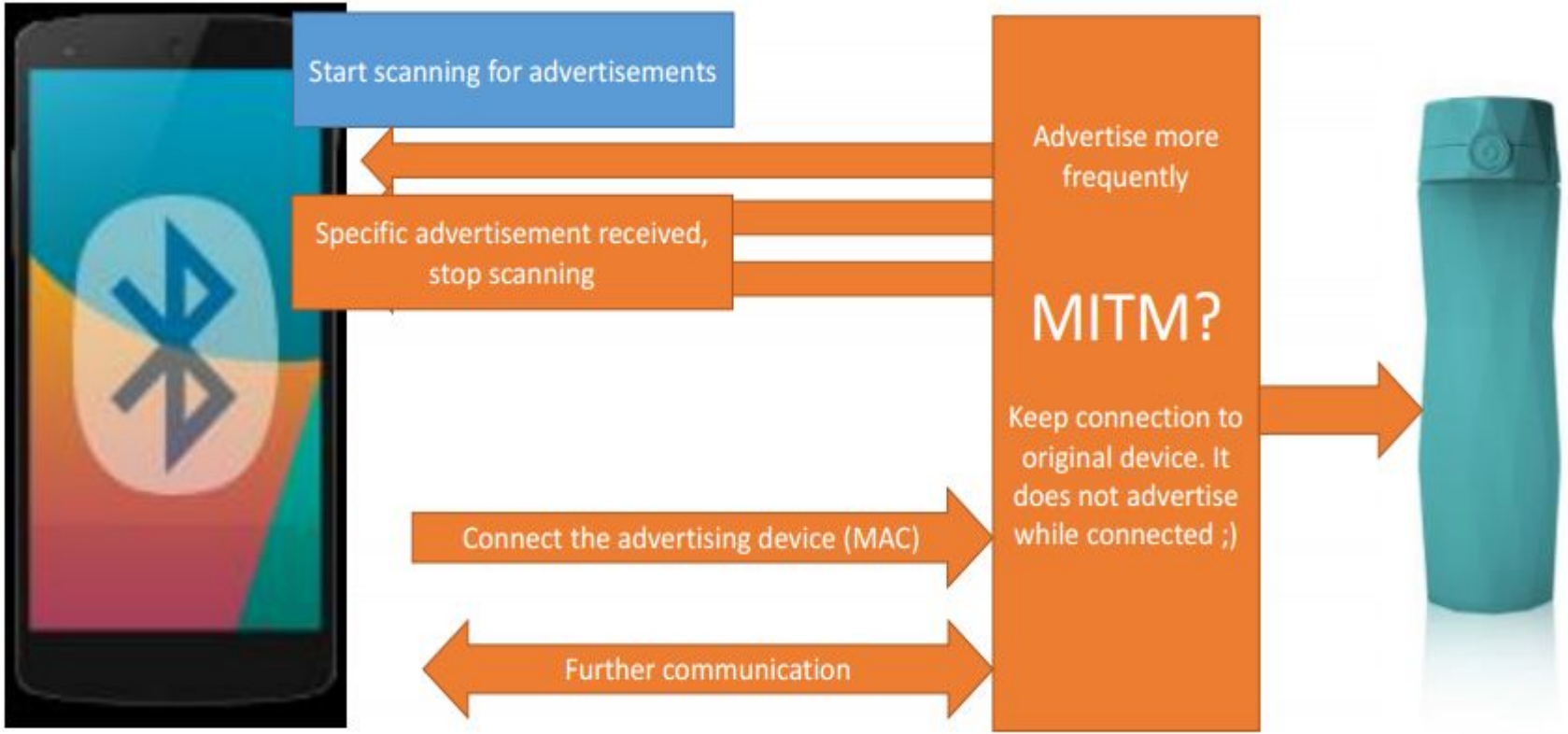
- In the 2nd Phase of pairing, 3 methods can be used- JustWorks, PassKey Entry, Out of Band Communication (NFC)
- Using JustWorks makes BLE susceptible to Man-in-the-Middle attack
- Eavesdropping
- Denial-of-Service

Man-in-the-Middle Attack



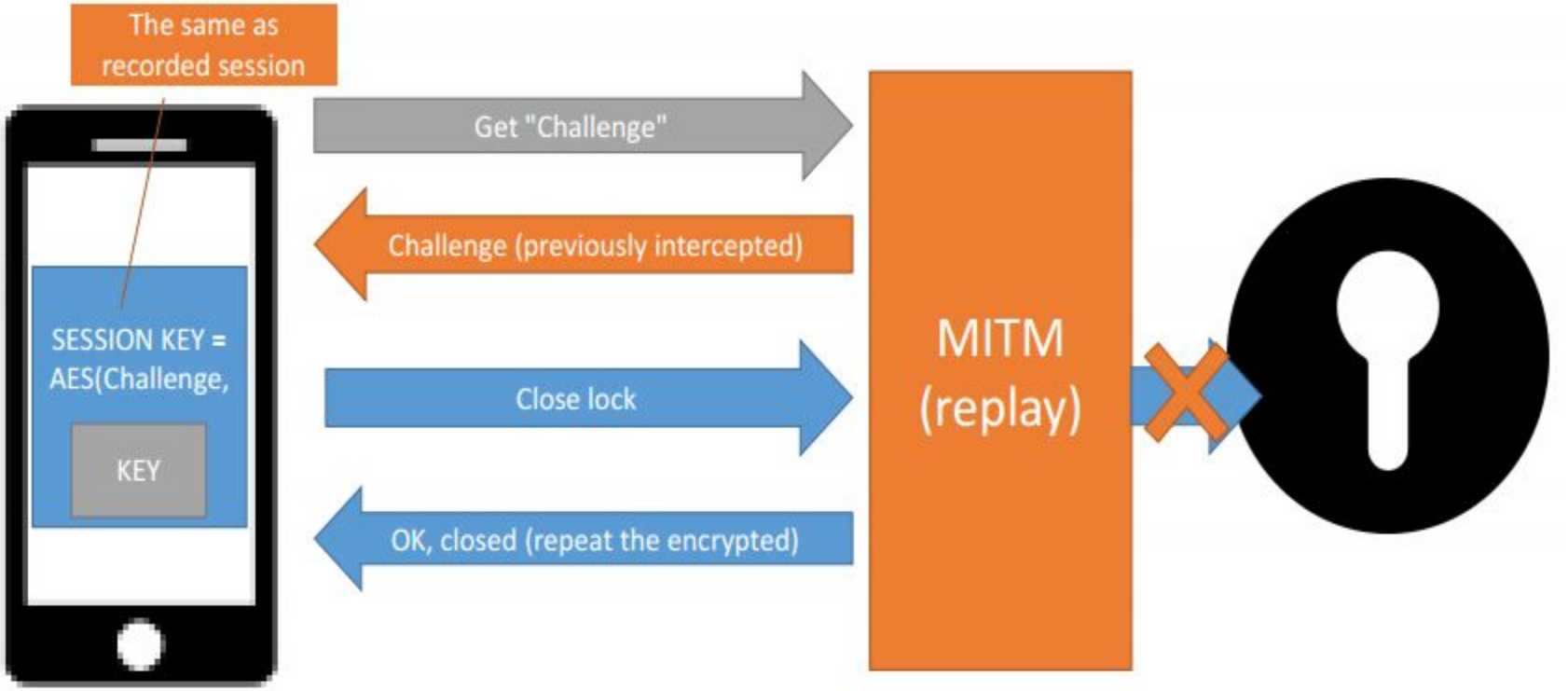
- Intruder secretly relays and possibly alters communication between 2 devices
- BLE devices susceptible to MITM in the pairing phase

MITM



Reference - GATTACKING BLUETOOTH SMART DEVICES Author - Slawomir Jasek, SecuRing Year - 2016

Smart lock – attack



Reference - GATTACKING BLUETOOTH SMART DEVICES Author - Slawomir Jasek, SecuRing Year - 2016

Steganography

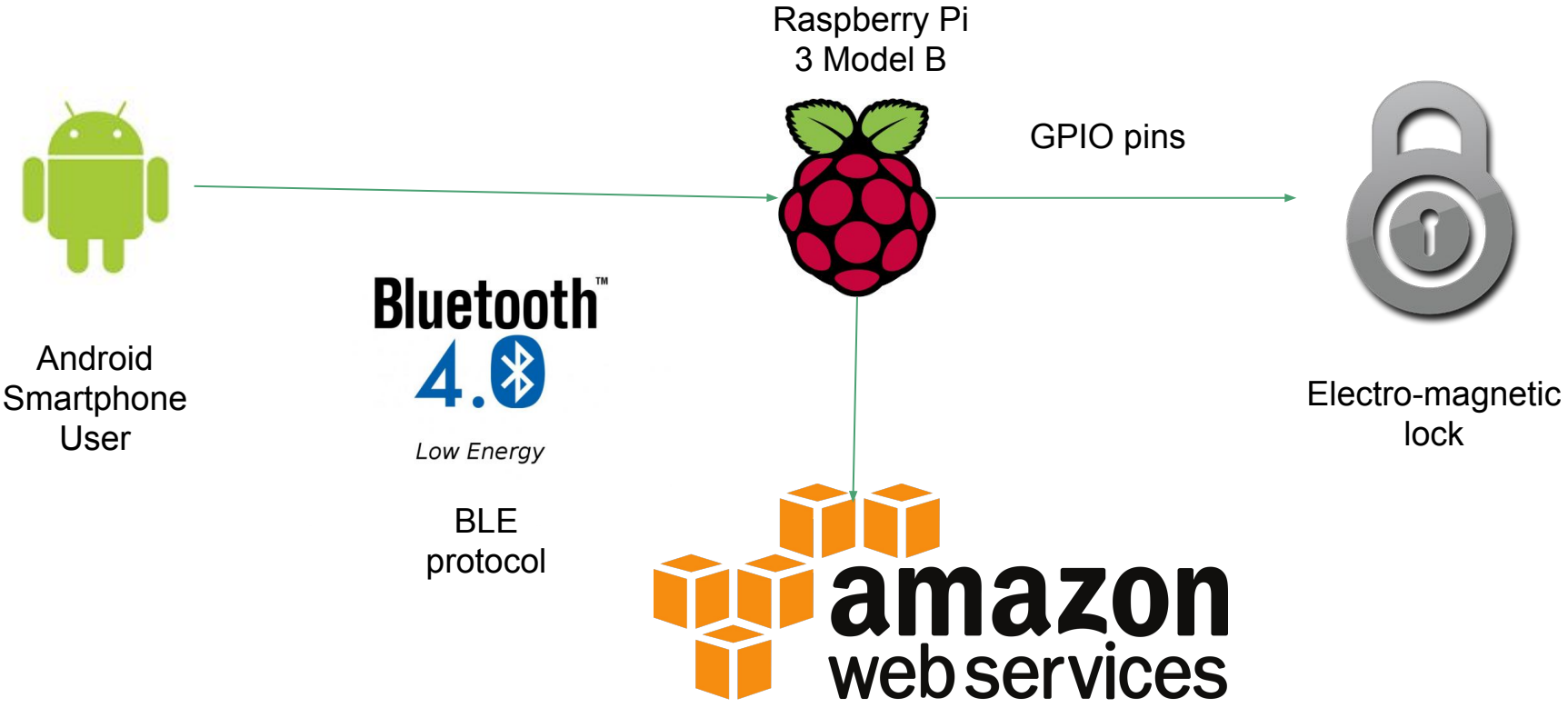
- Definition - “art of hiding a message”
- History - German spies in 1914-18
- Techniques -
  - Technical
    - Hiding in Stego-files (audio.video,image)
  - Text
    - Hiding in text
      - Format-based
      - Random & statistical

Observation

- Aim- Resolve the shortcomings of the existing Bluetooth Low Energy (BLE) protocol used in the IoT devices (Smart lock).
- Steganography - hiding the message in a larger message or image so as to hide the existence of the message itself
- Cryptography - the study of hiding information i.e. converting data into gibberish form and sending it.
- Our AIM,

Improved security = Cryptography + Steganography

System Design



Hardware & Software Requirements

- Hardware Requirements:
  - Smartphone
  - Raspberry Pi 3 Model B
  - Electro-magnetic Lock

- Software Requirements
  - Python 2.7 and Java SE 1.8 (programming on Raspberry Pi)
  - Android application

Circuit Diagram

References

1. Gomez, C., Oller, J., & Paradells, J. (2012). Overview and evaluation of Bluetooth low energy: An emerging low-power wireless technology.Sensors, 12(12), 1173411753. doi:10.3390/s120911734
2. OSullivan, Harry. ”Security Vulnerabilities of Bluetooth Low Energy Technology (BLE).” Tufts University.
3. Anderson, Hugh. ”Introduction to Computer Security.” (2004).
4. Conti, Mauro, Nicola Dragoni, and Viktor Lesyk. ”A Survey of Man In The Middle Attacks.” IEEE Communications Surveys & Tutorials 18, no. 3 (2016): 2027-2051.
5. Thiyagarajan, P., G. Aghila, and V. Prasanna Venkatesan. ”Stepping up internet banking security using dynamic pattern based image steganography.” In International Conference on Advances in Computing and Communications, pp. 98-112. Springer Berlin Heidelberg, 2011.
6. A. Karia, A. B. Patankar, and P. Tawde, ”SMS-Based One time Password vulnerabilities and safeguarding OTP over network,” vol. Vol. 3 - Issue 5 (May - 2014), no. Vol. 3 - Issue 5 (May - 2014), Jan.2017. [Online]. Available: http://www.ijert.org/view-pdf/9806/sms-based-one-time-password-vulnerabilities-and-safeguarding-otp-over-network. Accessed: Jan. 20, 2017

THANK YOU