Securely Retrofitting Door Locks for Cheap Control through Mobile Devices

Read Sprabery, Güliz Seray Tuncay, Carl Gunter, Roy Campbell
University of Illinois at Urbana-Champaign
{sprabery2, tuncay2, cgunter, rhc}@illinois.edu

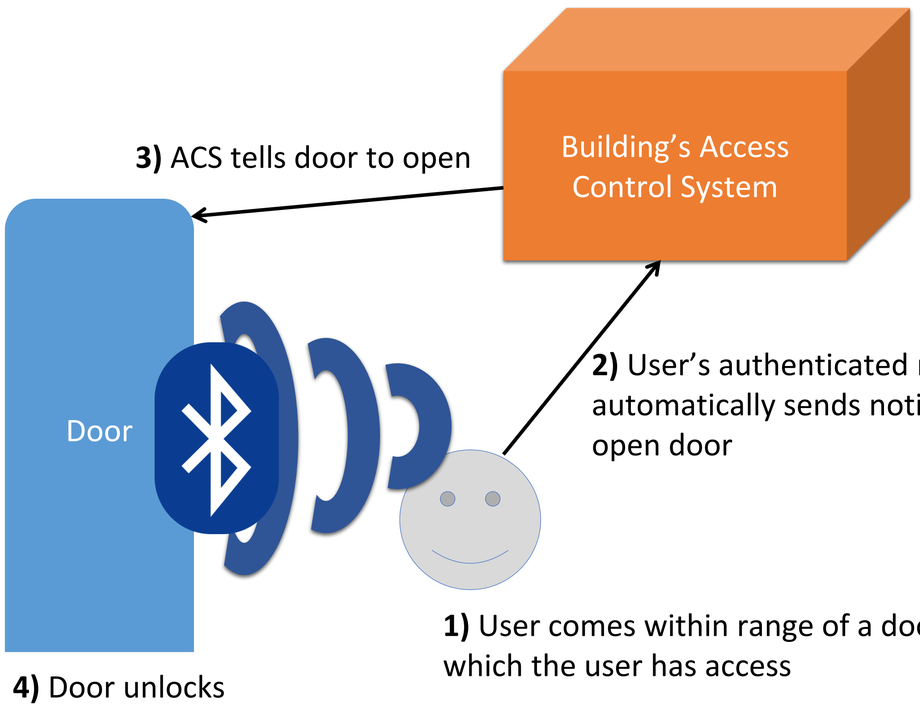
Introduction

- The internet of things is a fast growing space
  - Nonstandard Authentication mechanisms
- There is **a large install base** of existing infrastructure for **building automation**
- Bluetooth low energy beacons allow for affordable retrofitting of legacy systems
  - Secondary authentication mechanism necessary
- Contributions:
  - Attack model for BLE devices requiring authentication
  - **Low cost** method to retrofit door lock systems for mobile control
  - Prototype implementation of protocol

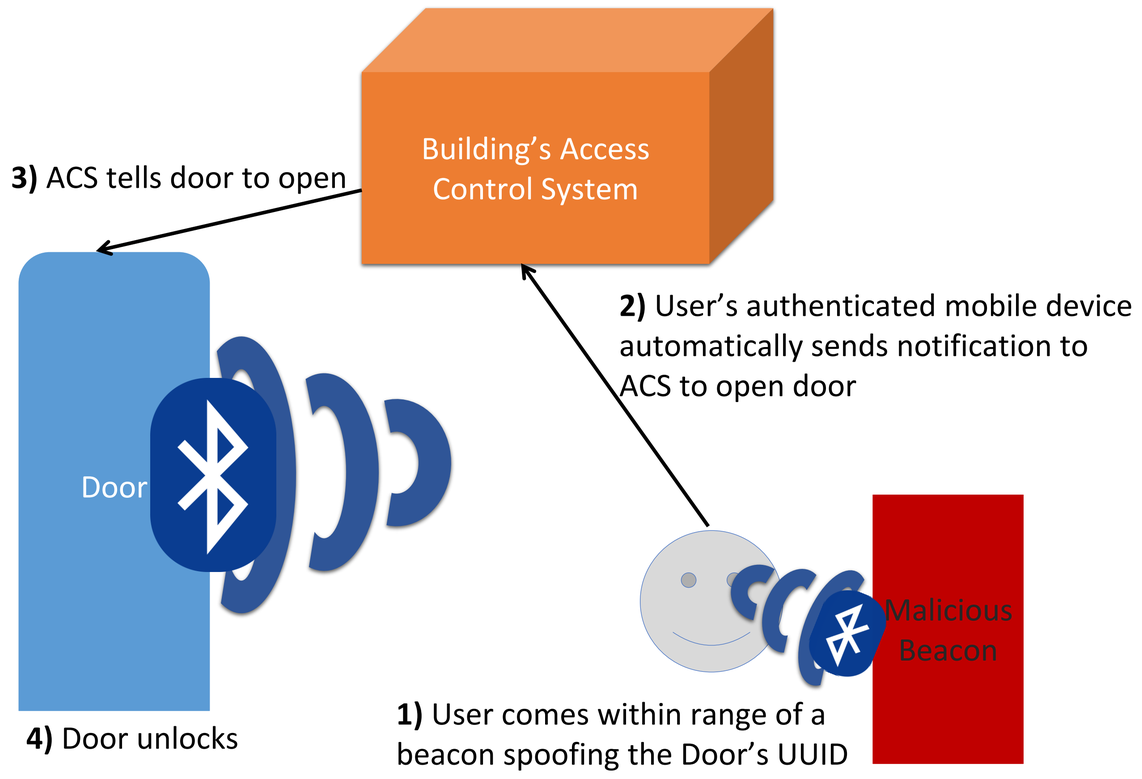
Overview & Components

- In a conventional door lock system, there are three actors:
  - The user, granted and revoked access to locks
  - The Access Control System (ACS)
  - An enterprise authentication mechanism
- Existing authentication:
  - Active directory syncs with building automation
  - Doors connected to via serial lines
  - Expensive to replace entire automation system
- Bluetooth Beacons:
  - Transmit a unique id & transmission power
  - No means of authentication
  - Passive Devices – no connections

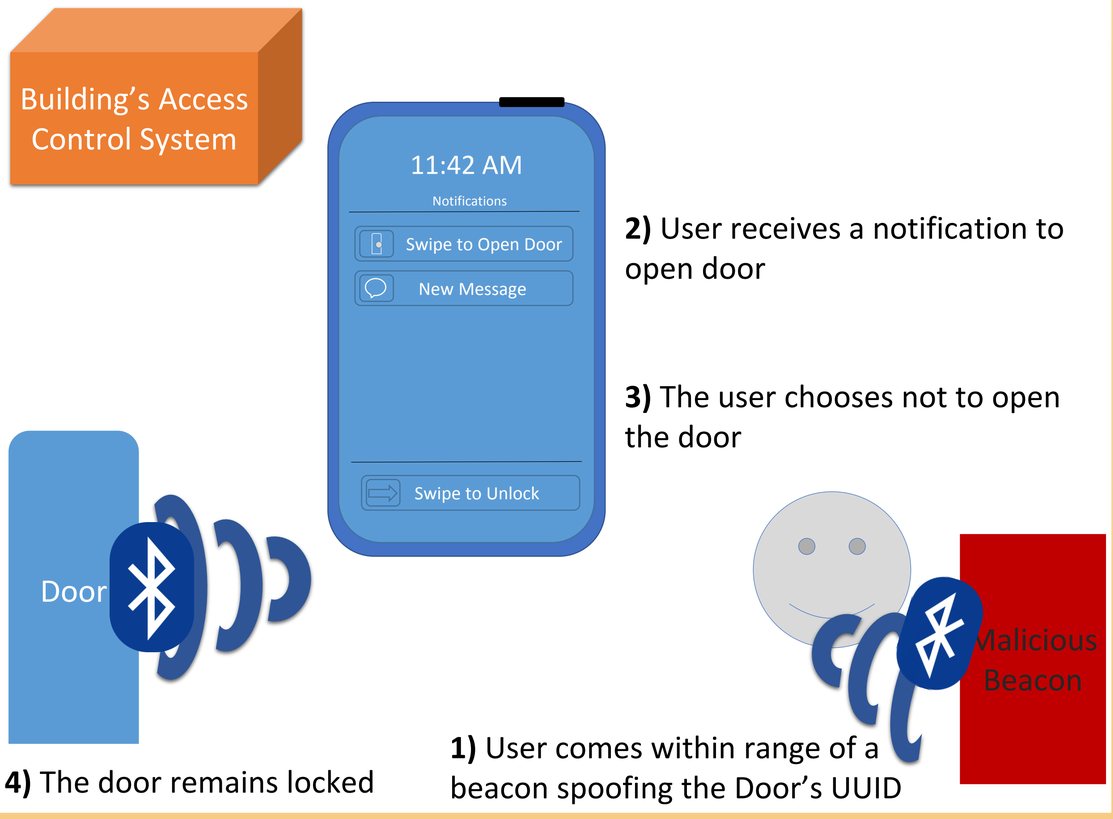
Naïve Protocol



Example Attack



Mitigation through User Interaction



Progress & Future Work

- Prototype implementation:
  - Building Automation & Serial Connection Representation
    - JSON API
  - System Authentication Representation
    - Ruby on Rails Backend
  - Legacy Door Lock
    - Raspberry Pi with LED as Lock
  - iBeacon for Retrofitting Door Lock
  - iBeacon as a Malicious Actor
    - First UUID intercepted and attack proven feasible
- Future Work:
  - Formally verified implementation
  - Integration into existing legacy systems
  - Alternative protocols:
    - RSA Token as UUID for beacon
    - Door locks with integrated Bluetooth receivers (active connection to devices)

Material based on research sponsored by the Air Force Research Laboratory and the Air Force Office of Scientific Research under agreement No. FA8750-11-2-0084 and National Science Foundation Graduate Research Fellowship Program under Grant Number DGE- 1144245. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author and do not necessarily reflect the views of the National Science Foundation, or other organizations.