All Your Locks are BLEong to Us

Anthony Rose
Student
Air Force Institute of Technology
Agenda

- Goals
- What is Bluetooth Low Energy?
- Vulnerable BLE Devices
- How can it be fixed?
- Summary
- Apply It
- Questions?
Goals

- Identify vulnerabilities in BLE smart locks
- Release proof of concept exploits
- Put pressure on vendors to improve security
- Raise consumer awareness
What is Bluetooth Low Energy?

- Designed for apps that don’t need to exchange large amounts of data
- Minimal power consumption
- Operates 2.4 GHz
- Short range (<100m)
Why Should I Care?

- Widely used and gaining popularity
- Securing homes and valuables
- Current BLE security products:
  - Deadbolts
  - Bike locks
  - Pad locks
  - Safes
  - ATMs
What do I need?

- Ubertooth One – $100
- Bluetooth Smart USB dongle (Sena UD100) – $20
- Directional antenna – $50
Past exploited devices

- Quicklock Doorlock
  - Plaintext Password
- Quicklock Padlock
  - Plaintext Password
- iBlulock Padlock
  - Plaintext Password
- Plantraco Phantomlock
  - Plaintext Password
- Safetech Gunsafe
  - Plaintext Password
- Ceomate Bluetooth Smart Doorlock
  - Replay Attack
- Elecycle EL797 & EL797G Smart Padlock
  - Replay Attack
- Vians Bluetooth Smart Doorlock
  - Replay Attack
- Laguate Sciener Smart Doorlock
  - Replay Attack
- Okidokey Smart Doorlock
  - Command Fuzzing
- Poly control Danalock Doorlock
  - Hard-coded Password
- Mesh Motion Bitlock Padlock
  - Rogue Device & Relay Attack
New exploits

Mesh Motion Bitlock
- More passwords!
- DDOS Attack

Safetech Gunbox
- Plaintext password
Plaintext Passwords

- Yes...this is still a problem!!!
- Found on 5 devices
  - Quicklock Doorlock
  - Quicklock Padlock
  - Safetech Gunbox
  - iBluLock Padlock
  - Plantraco Phantomlock

- Threats
  - Easily sniffed
  - Brute forcible
  - Elevate admin privileges
Quicklock

- Unencrypted (by design)

**BLUETOOTH SECURITY NOTICE**

**BLUETOOTH SECURITY - DEFCON - QuickLock**

Anthony Rose recently discussed issues related to Bluetooth security and the Quicklock doorlock, & Padlock:

The Quicklock solution uses two mechanisms for opening and access: (RFID and Bluetooth). The electronic codes necessary to open are passed wirelessly and are unencrypted (by design) to allow vendors flexibility when integrating the Bluetooth device into existing platforms. Because keys are passed wirelessly, they are open to Bluetooth hacking only for a few seconds when a hacker is within range of the device. However, this level of security is similar to a standard lock and key scenario; Standard mechanical devices offer far fewer benefits than Bluetooth connected locks.

**Bluetooth Electronic keys:** To obtain the Bluetooth electronic key for quicklock, a Bluetooth hacker must setup a device within proximity of the lock and wait for the lock to be activated by the user. Standard quicklock protocol keeps the lock in low power mode to conserve battery life, so the hacker must wait or setup equipment within a few feet of the device in continual capture mode. Once the lock is activated, the hacker must then intercept the communication sent by the user. This transaction must be done in short range of the device and at the precise time. The probability of this occurring is debatable but it is admitted possible. This risk is reduced because the device is pushed to wake! The Quicklock electronic solution is better security than a standard mechanical key that can be easily taken and copied by any lock picker.

**Quicklock RFID Key security:** Every Quicklock system also has the ability to learn and use up to 50 RFID keys. These keys can be programmed to any lock. The electronic exchange for this transaction is much shorter (less than 2 inches), but it would be possible for a thief to steal a RFID key that is already programmed to a lock and then make a duplicate RFID key. Again, this threat is analogous to a standard mechanical key being stolen but a mechanical key offers far fewer benefits and does not require a high tech individual hack attack.

**The real threat:** With a standard padlocks and doorlocks users possess mechanical key to open. Keys can be copied or stolen but some effort must be taken to protect the key from falling into the wrong hands. Even with a digital keypad, like on most cell phones, a user must protect that no person with ill intentions is peaking over the shoulder to get the access code. With most Padlocks, thefts must often occur when the lock is cut. Many mechanical doorlocks can be bumped easily but thefts occur most often when a window is broken and entry is forced.

**The Advantage of QuickLock:** Users of the quicklock system recognize the benefit of quick access and the ability to use multiple keys. Many users of the products never update the default password and when they call for tech support our first option is to have them try the default Bluetooth password—which often works. With Bluetooth the Quicklock can keep record and report who is opening when and on what platform. The device is great for inventory tracking and Lock-out-tag-out where many of our customers are concerned about traceability and access more than security. Having multiple ways to open also offers users “immediate access” in times where getting the lock open must be done in milliseconds and fumbling for a key isn’t an option! The Bluetooth interface also enables unique ways to interact with the electronic device using a users cell phone interface. It’s not about just pushing the button on the app to open the device. It is often about programmability, accountability, tech support and visibility into the electronic device. For enterprise applications and custom locking solutions, higher levels of security are enabled as required.
Quicklock

- **Bluetooth Attribute Protocol**
  - **Opcode**: Write Request (0x12)
  - **Handle**: 0x0029 (Unknown)
  - **Value**: 001234567812345678
Quicklock

**Bluetooth Attribute Protocol**

- **Opcode**: Write Request (0x12)
- **Handle**: 0x0029 (Unknown)
- **Value**: 001234567812345678

**OpCode**
Quicklock

**Bluetooth Attribute Protocol**

- **Opcode**: Write Request (0x12)
- **Handle**: 0x0029 (Unknown)
- **Value**: 001234567812345678

**Opcode Current Password**
Quicklock

Bluetooth Attribute Protocol

- Opcode: Write Request (0x12)
- Handle: 0x0029 (Unknown)
- Value: 001234567812345678

Op,code | Current Password | New Password
Quicklock

LE Scan ...
61:84:14:FA:72:18 (unknown)
61:84:14:FA:72:18 (unknown)
42:2B:E7:4C:E9:05 (unknown)
42:2B:E7:4C:E9:05 (unknown)
56:D2:A7:61:CE:EB (unknown)
56:D2:A7:61:CE:EB (unknown)
C5:F0:2F:98:C3:28 Tile
C5:F0:2F:98:C3:28 (unknown)
D4:80:D6:53:DF:4C (unknown)
5E:16:15:B1:03:16 (unknown)
F8:45:28:A7:56:CD (unknown)

- Bluetooth Attribute Protocol
  - Opcode: Write Request (0x12)
  - Handle: 0x0029 (Unknown)
  - Value: 006969696969696969

Password is 69696969???
Quicklock

- Communication must be within a “few” feet
Quicklock

- Communication must be within 2,640 feet
“Many users of the products never update the default password and when they call for tech support our first option is to have them try the default password – which often works”

- No need to brute force
- Default password is 12345678
User Behavior Analytics

- Vulnerabilities give adversaries access to:
  - Lock functionality
- Device & user history logs
- Intelligence Value
  - Activity by Time, Week, Day, Month, etc.
  - User activity
  - Cross reference with open-source material
Gunbox

- Gun Storage Safe
- Biometrics, RFID, Bluetooth, and Z-Wave
- Auto-open feature
Gunbox

- “Hidden in plain sight, the Gunbox allows for quick access and safe storage.”
- “The GunBox’s Mission is to Keep Kids Safe”
Gunbox

- Listens for Gunbox
- Connects to Gunbox as soon as the button is pressed (advertising)
- Sends unlock command
- Profit

- Build slide with child pressing button on gunbox
Bitlock

- Bikesharing lock
- Utilizes a web server to generate password
- Requires internet to communicate and retrieve passwords (has an offline mode)
- Current firmware uses a predictable nonce
- Application is always running in the background
Bitlock

(1) Connect
(2) 0
(3) 1
(4) 2

(5) 0
(6) Enc(0)
Bitlock

(6) Enc(0) 0

(5) Connect n

(7) Enc(0)
(8) Enc(1)
(9) Enc(2)

Enc(n)
No command 'lear' found, did you mean:
Command 'pear' from package 'php-pear' (main)
Command 'lear' from package 'ecrire-dev' (universe)
Command 'bear' from package 'bear' (universe)
Command 'lear' from package 'unar' (universe)
Command 'lear' from package 'ncurses-bin' (main)
lear: command not found
opt@opt:~$ clear
opt@opt:~$ sudo node Bitlock.js
[sudo] password for opt:
on: stateChange: power: on
on: advertisingStart: success
on: servicesSet
Bitlock DDOS Attack

Why?
- Bikeshare program
- Requires access to the internet (web server)

Outcome
- Eliminates ability to generate a profit
- Disrupts customers
Bitlock DDOS Attack

- Stop communication between Bitlock and their servers
- What happens if the web server is unreachable?
- Will it enter an offline mode?
Bitlock DDOS Attack

- Utilize Burp to intercept packets
- Drop packets directed to Bitlock API
- App waits for response from server
- Lock never opens
Bitlock DDOS Attack

- What happens if the web server is unreachable?
  - The lock becomes unopenable
- Will it enter an offline mode?
  - No
Next week you should:
- Identify affected Bluetooth devices

In the first three months following this presentation you should:
- Safetech – Develop alternative security measures (encryption)
- Bitlock – Limit amount of requests to web server
- Bitlock – Newest firmware implements random number generator

Within six months you should:
- Safetech – Release firmware update to add encrypted communication
- Bitlock – Application requires option to switch to offline mode after a timeout
Questions?

Anthony.Rose@AFIT.edu