Securing your in-ear fitness coach: Challenges in hardening next generation wearables

Kavya Racharla
Sumanth Naropanth
Who are we?

- Kavya Racharla
  - Security Research Manager — Sports Group, Intel
  - Oracle & Qualcomm

- Sumanth Naropanth
  - Founder and CEO — Deep Armor
  - Intel, Palm/HP, Sun Microsystems

- Security consulting, vulnerability testing, SDL and training services for emerging technologies
- www.deeparmor.com  |  @deep_armor
Security problems in New Devices

How do we address them?
Agenda

- Introduction to an in-ear fitness coach
- Unshackling from traditional SDL methods
- Securely designing a software fitness coach
- Hardware, Firmware & Software paradigms
- Ecosystem Security
- Real world problems - weaknesses and demos
- Privacy
IoT/Wearable Ecosystem

Gateway

Node

Node

Node

Sensors

Sensors

Sensors

HTTP/HTTPS

HTTP/HTTPS

HTTP/HTTPS

BT/BLE/WiFi/NFC

BT/BLE/NFC

BLE/ANT+

Zigbee/Z-wave

Back End Services
Case Study: In-ear fitness coach

Wearable = Comfortable

Smart

Untethered

Continuous Learning

Data/Analytics

Better Quality of Life
Securing an in-ear fitness coach
Unshackling from traditional SDL
Challenges: Securing a never-before gadget

- Lack of tactical SDL frameworks for rapid time-to-market products with constantly evolving requirements
- Diverse, non-standard and evolving communication protocols
- Weaknesses in adoption of protocol specifications
- Long lives for IoT products
- Privacy
- Nascent research in IoT security
Challenges - Technical

• Collection of personal data and PII is higher
  • Geo-location information
  • Biometric data
  • Sensor data
  • Payment services

• Limited SW stack —> security may get compromised
  • Often FW running on micro-controllers
  • Field updates are difficult
  • Asymmetric key crypto, TEEs, etc. are heavy

• Multi-tier, multi-tenant product architecture
  • Cross-domain flows
  • Multiple exposure points as a consequence
Proposal: Securing a never-before gadget

- Next-gen SDL
  - For IoT, wearable and cloud technologies. Especially when they all come together
  - Ecosystem security
  - Agile

- Security, Privacy and Legal woven into the development cycle

- Leveraging industry standards
Introducing SPDL

- Architecture Reviews
- Threat Modeling & Attack Trees
- Security Code Reviews & Static Code Analysis
- Penetration Testing
- Privacy Sign-off, Data Availability
- Legal sign-off & Incident Response

Product Development Lifecycle:
- Program Conception to Pre-Alpha
- Alpha
- Beta
- Launch to Post Launch
Designing SPDL
Hardware & Firmware Security Paradigms

Device Hardware
- Port access restrictions & lockdown

Device Software
- Service layer security
- Protocol security
- Data sandboxing
- Secure Erase
- Signed libraries
- Key Management
- Secure Boot
- Secure FOTA
- TEE
- Data At Rest Encryption
- Secure Debug
- Secure Storage

Protocol layer
- Service layer security
- Protocol security
- Data sandboxing
- Secure Erase
- Signed libraries
- Key Management
- Secure Boot
- Secure FOTA
- TEE
- Data At Rest Encryption
- Secure Debug
- Secure Storage

Device Hardware
- Port access restrictions & lockdown

Device Software
- Service layer security
- Protocol security
- Data sandboxing
- Secure Erase
- Signed libraries
- Key Management
- Secure Boot
- Secure FOTA
- TEE
- Data At Rest Encryption
- Secure Debug
- Secure Storage

Device Hardware
- Port access restrictions & lockdown

Device Software
- Service layer security
- Protocol security
- Data sandboxing
- Secure Erase
- Signed libraries
- Key Management
- Secure Boot
- Secure FOTA
- TEE
- Data At Rest Encryption
- Secure Debug
- Secure Storage

Device Hardware
- Port access restrictions & lockdown
SW Security Paradigms: application SW

- Multi-app <-> multi-device communication
- Secure storage of app specific data, keys, logs, databases and user specific data
- 3rd Party SDK security
- HW backed keystore/keychain
- Secure implementation: Spec and Code
- App Store Scanning
- Privacy: Opt-in/Opt-out policy enforcement
Cloud Software & Infrastructure Security

- Secure storage of user and enterprise data, At Rest Encryption
- Secure Key Management and Provisioning
- User & Roles management
- Micro-services security
- Infrastructure hardening Secure configuration
- Privacy: Data storage, sharing and retention policies
- Security DevOps
- Web Portal Security (HTML/JS attacks)
Ecosystem security challenges

Design weaknesses in comms protocol adoption

Secure key negotiation and distribution

Gateway/Node Updates

Secure Provisioning

Network Security

Design weaknesses in comms protocol adoption

Secure key negotiation and distribution

Gateway/Node Updates

Device Software

- Secure Boot
- Secure FOTA
- TEE
- Data Anon: Data Anonymization
- Signed Libraries
- Secure Storage
- Security Escope
- Remote factory reset
- Firmware

Device Hardware

- Key Management
- Secure Boot
- Secure FOTA
- TEE
- Data Anon: Data Anonymization
- Signed Libraries
- Secure Storage
- Security Escope
- Remote factory reset
- Firmware

Secure key negotiation and distribution

Secure Provisioning

Design weaknesses in comms protocol adoption
Real world security problems
Demo 1: Ecosystem Challenges
Demo 1: Ecosystem overview

Back End Services

BT/BLE/ANT+

BT/BLE

HTTPS
Device commands:
- Put device into recovery mode
- Do a FW update
- Change Device (BLE) name

Notifications:
- Social apps
- Calls and texts

Information:
- User activity data
- User profile updates
- Application action (calls, music control)
- Call/text/social updates (sometimes)
The Problem – Prelude

Device Commands:
- Put device into recovery mode
- Do a FW update
- Change Device (BLE) name

Notifications:
- Social apps
- Calls and texts

Information:
- User activity data
- User profile updates
- Application action (calls, music control)
- Call/text/social updates (sometimes)

BLE - ENCRYPTED
ATTACKER
The Problem

Device Commands:
- Put device into recovery mode
- Do a FW update
- Change Device (BLE) name

Notifications:
- Social apps
- Calls and texts

Information:
- User activity data
- User profile updates
- Application action (calls, music control)
- Call/text/social updates (sometimes)

ATTACKER

BLE - ENCRYPTED
Root Cause

All applications on Android and iOS can subscribe to the BT service and get the data on the same BT channels or BLE characteristics as the legitimate app.

- **Android**
  - android.permission.BLUETOOTH
  - android.permission.BLUETOOTH_ADMIN – quote:

    If you want your app to initiate device discovery or manipulate Bluetooth settings, you must also declare the Bluetooth_ADMIN permission. Most applications need this permission solely for the ability to discover local Bluetooth devices. *The other abilities granted by this permission should not be used* unless the application is a “power manager”.

- **iOS**
  - Core Bluetooth (CB) Framework
  - Centrals (client/phone) and Peripherals (server/wearable) classes
Example – Wearable Ecosystem 1

- Uses BLE
- Proprietary code
- Existing market research for format of messages and headers
- Malware app subscribes to the known BLE characteristics gets data synced with the legit app
Example – Wearable Ecosystem 1
Example – Wearable Ecosystem 2

- Similar, but with a twist
- Malware application cannot send commands to the wearable by itself
- Legitimate app opens a connection to the device
- The malware app piggybacks to send commands to the wearable

**Moral: Partial security does not help**
- Protect not just the handshake but every message
Example – Wearable Ecosystem 2
Demo 2: Protecting User data in logs
The Problem

• Coach commentary, language definitions and dialogue stored as **PLAIN TEXT** files

• FIT files and JSON files stored in **public storage**
  • Due to private storage limitations

• Contains PII and IP

• Attacker can tamper with or copy over the text files
  • DoS
  • Code execution
  • Accessible by malicious apps
Our Recommendation

• Avoid public storage whenever possible

• Support for encryption
  • Keys must be user specific or application specific to prevent BORE

• Support for signing dialogue files or any sensitive information in public storage

• Capability to delete/ opt-out of dialogue logging
  • Cloud
  • App
Demo 3: Admin portal takeover
Demo 3: Ecosystem overview

User portal: Login and sign-up
User portal: Connect with friends
User portal: Comment on friends profile
User portal: Profile and activity mgmt.
Admin portal: Remote Device mgmt.
Admin portal: Data mgmt.
Target: Sign-up and Profile pages
Exploit Scenario

• Attacker uses the “friend request” functionality on user portal

• “Friend request” loads when victim logs into his/her account
  • Victim takes no action to view the invite/accept the invite

• Attacker exploits a XSS vulnerability in the user portal/ sign-up pages

• Uses two accounts to launch the attack
  • Gives 2X number of characters for the exploit code
  • Exploit code expandable up to 5 notifications (or 5 “friend” requests)
Exploit Scenario: The attack

First Name: Arya
Last Name: Stark
Email: aryastark.com

First Name: Jon
Last Name: Stark
Email: jonstark.com
Victim - logs in
Attacker’s c&c

Victim’s cookies and UA

Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_2) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/47.0.2526.73 Safari/537.36

GA1.2.1543537304.1450072994; _ga=GA1.2.1543537304.1450072994; _gat=1; _ga=GA1.2.1543537304.1450072994; _gat=1; 
_ads9hnrfj7a3uhd9cnd8esa4g7; _ra=0.100149.1450085069; 
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_2) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/47.0.2526.73 Safari/537.36
Access to admin portal

• Victim = Admin!

• Cloud -> Remote device management

ATTACKER’S BROWSER SEAMLESSLY LAUNCHES ALL PAGES OF THE VICTIM
The Attack

- Stolen admin credentials used to access admin portal
  - Remote device take-over
  - Unauthorized access to user profile data
  - Unauthorized access to user accounts
  - Malicious FW updates rolled-out

- Several Security and privacy violations!
Privacy

- Live on your body or vicinity => access to wealth of PII/sensitive data
- What is PII or personal data?

Data Management
- Collector/owner/processor/...
- 3rd party data access

Data retention and deletion policies
Regulatory Guidelines and Privacy Laws

- Geo/Country based restrictions for collecting, storing and retaining data
- US
- GDPR
- ...

- Data breaches and disclosures

The greater of €20 million or 4% of global annual turnover

In the case of non-compliance with key provisions of the GDPR, regulators have the authority to levy a fine in an amount that is up to the GREATER of €20 million or 4% of global annual turnover in the prior year. Examples that fall under this category are non-adherence to the core principles of processing personal data, infringement of the rights of data subjects and the transfer of personal data to third countries or international organizations that do not ensure an adequate level of data protection.

The key word is “greater”
Privacy Breaches

VTech to Pay FTC $650k Over Kids Privacy Violations in Connected-Toy Hack

January 9, 2018 15:45  by Elizabeth Montalbano

Strava Fitness App Can Reveal Military Sites, Analysts Say

By RICHARD PEREZ-Peña and MATTHEW ROSENBERG  JAN, 29, 2018

2 more wireless baby monitors hacked: Hackers remotely spied on babies and parents

Two more wireless baby monitors were hacked. One family heard voices as the camera followed them about the room; the second mom was freaked out and scared as a hacker remotely controlled the camera to follow her movements.
Quantifying Privacy Vulnerabilities

- Security Vulnerabilities are scored and rated
- Privacy vulnerabilities?
Summary

• Rethink SDL
  • Shift-left
  • Agile

• Old Vulnerabilities manifest in new ways

• Data and Privacy
Thanks!
(and Q&A)

@kavyarachcharla and @snaropanth