Fitness Trackers and Security

Amherst Security Group (@AmherstSec)
September 12, 2018
Robert Hurlbut

RobertHurlbut.com • @RobertHurlbut

Robert Hurlbut

Threat Modeling Architect, Trainer

Microsoft MVP – Developer Security 2005-2009, 2015-2019

(ISC)2 CSSLP 2014-2020

Co-host with Chris Romeo – Application Security Podcast

MeetUp Leader: Boston .NET Architecture Group, Amherst Security Group

Contacts

Web Site: https://roberthurlbut.com

Twitter: @RobertHurlbut, @AppSecPodcast

Agenda

- Fitness Trackers and their Uses
- Security Issues
- Case Study: Doping your FitBit
- Demo (maybe?)
- Resources

Fitness Trackers

- Wearable devices or a computer application that records a person's daily physical activity, together with other data relating to their fitness or health, such as the number of calories burned, heart rate, etc.

"I get five miles of walking in a day according to my fitness tracker"

Fitness Trackers

- Apple - Watch Series 3
- Fitbit - Charge 2
- Garmin - vívofit 3
- Huawei - Band 2 Pro
- Jawbone - UP3
- Lenovo - HW01
- Medion - Life S2000
- Moov - Now
- Nokia - Steel HR
- Polar - A370
- Samsung - Fit2 Pro
- TomTom - Spark 3
- Xiaomi - Mi Band 2

(List from https://www.av-test.org/en/news/fitness-trackers-13-wearables-in-a-security-test/)

Fitness Trackers

- Apple - Watch Series 3
- Fitbit - Charge 2
- Garmin - vívofit 3
- Huawei - Band 2 Pro
- Jawbone - UP3
- **Lenovo - HW01**
- **Medion - Life S2000**
- **Moov - Now**
- Nokia - Steel HR
- **Polar - A370**
- Samsung - Fit2 Pro
- TomTom - Spark 3
- **Xiaomi - Mi Band 2**

(List from https://www.av-test.org/en/news/fitness-trackers-13-wearables-in-a-security-test/)

NOTE: Issues with those marked in **red** : authentication issues, etc.

Fitness Trackers

Many fitness trackers …

- Do not encrypt **local connections**
- Apps require data upload **to the cloud**

In the news

- Researcher says Fitbit can be wirelessly hacked to infect PCs, Fitbit says not true (October 26, 2015)

  A researcher demonstrated a proof-of-concept to infect Fitbit with malware in about 10 seconds; the malware infection could then spread to a PC when the fitness tracker is plugged into it. FitBit denied it.

  https://www.computerworld.com/article/2997561/cybercrime-hacking/researcher-says-fitbit-can-be-wirelessly-hacked-to-infect-pcs-fitbit-says-not-true.html

In the news, continued

- U.S. military reviewing its rules after fitness trackers exposed sensitive data (January 29, 2018)

  Online "heat maps" from Strava showing where users jog, bike, and exercise, including military bases in strategic locations showing movements of workers and soldiers

  https://www.washingtonpost.com/world/the-us-military-reviews-its-rules-as-new-details-of-us-soldiers-and-bases-emerge/2018/01/29/6310d518-050f-11e8-aa61-f3391373867e_story.html

Attack examples from "Wearfit" case study:

examples of representative attacks that illustrate, but do not completely enumerate, ways that attackers might target the system.

Denial of service

- Render wearable unusable with fake firmware update.
- Drain battery, CPU, or other resources.
- Lockout user from website account.

Compromising device integrity

- Malicious firmware update.
- Buffer overflow on wearable to compromise paired mobile device.

Falsifying the user's own health data

- Physically manipulate the device.
- Tamper with data on mobile device before uploading to the webserver.
- Tamper with data in transit from wearable to mobile or mobile to website.

Falsifying another user's health data

- Rewrite health data on device.
- Tamper with data on a mobile device when used as a passthrough.
- Spoof data uploads using a known device or user identifier.
- Tamper with data in transit from wearable to mobile or mobile to website.
- Direct attacks against the website (for example, SQL injection).
- Phishing, cross-site request forgery (CSRF), and other indirect attacks against end users.

Abusing health data that are intentionally shared

- Employer or insurer penalizes behavior seen through *WearFit Corporate Benefits*.
- Users of the *WearFit Social System* unintentionally view sensitive activities.
- Advertising partners target over-personalized ads.
- Share configuration that becomes out-of-sync with changes in real-world relationships.

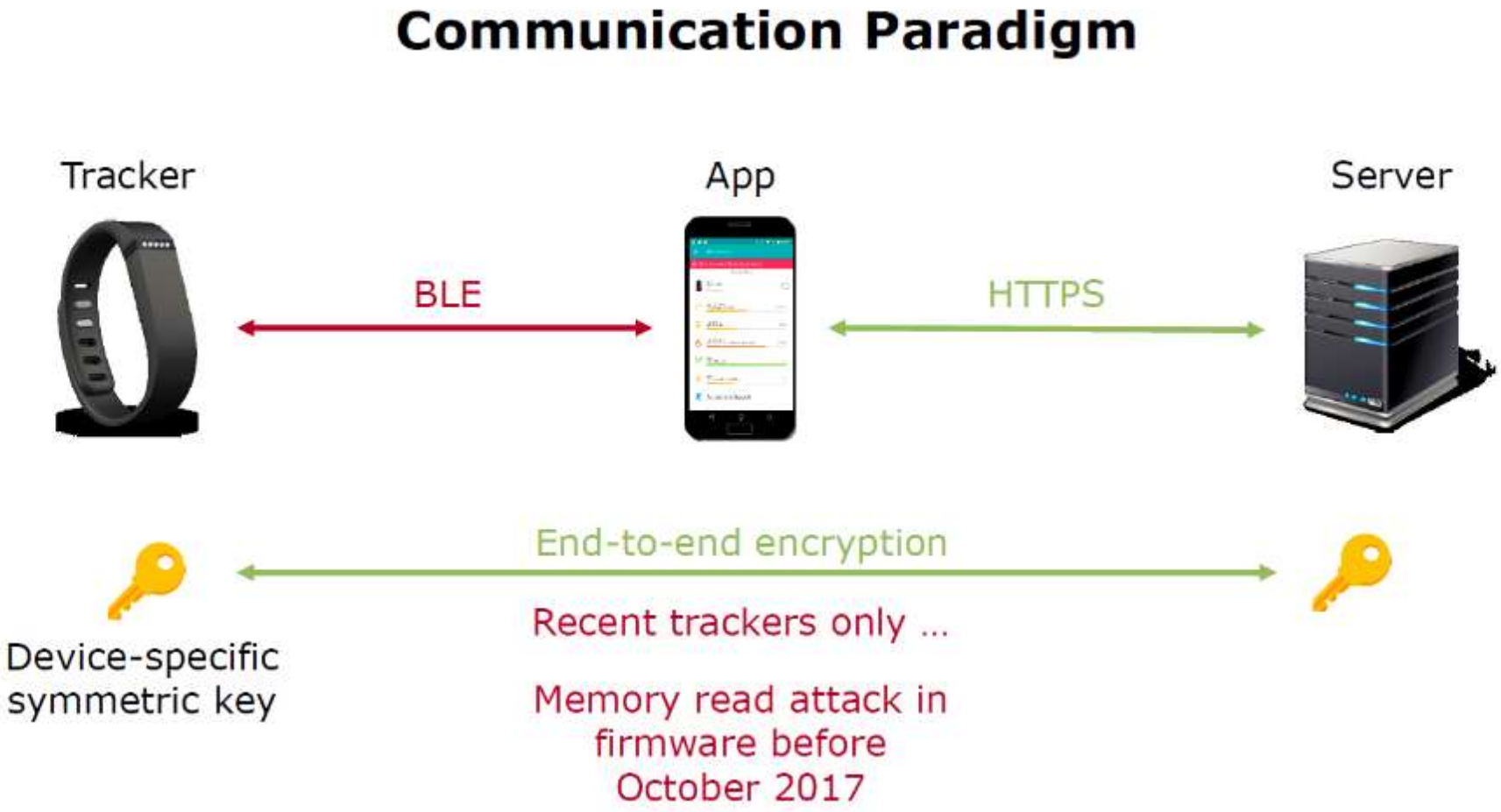
Stealing a user's health data

- Guess or steal a user's authentication credentials.
- Direct attacks against the website (for example, SQL injection).
- Eavesdrop on communication on mobile device when used as a passthrough.
- Eavesdrop on communication from wearable to mobile or mobile to website.
- Malicious insider uses internal, or otherwise "privileged," access.
- Phishing, CSRF, and other indirect attacks against end users.

Now let's consider how the system's technical design can affect its security.

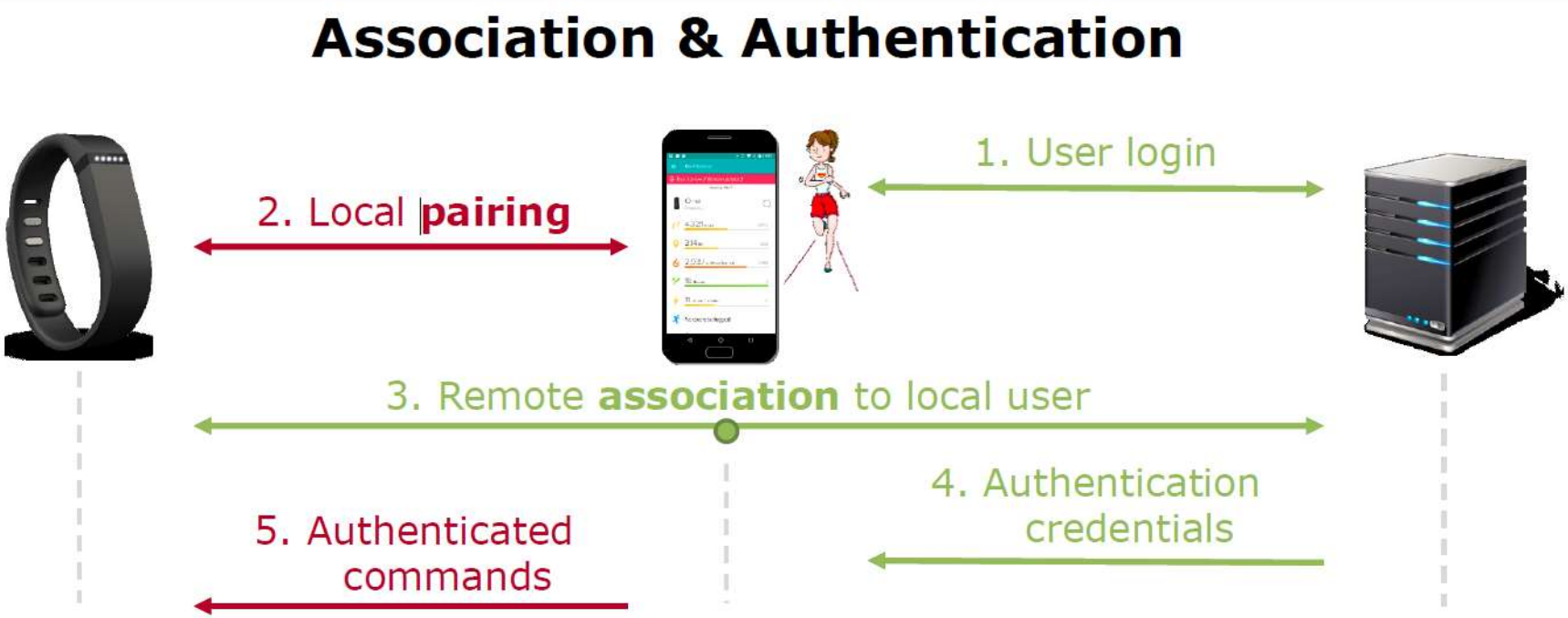
BACK TO TOP OF DOCUMENT

Case Study: Doping your FitBit*



* Jiska Classen & Daniel Wegemer
https://media.ccc.de/v/34c3-8908-doping_your_fitbit

Case Study: Doping your FitBit*



- User **associates local tracker** with remote server account
  - Requires entering a code displayed on tracker or physical tapping
- App receives **authentication credentials** and stores them locally
- App can use authentication credentials for **authenticated local commands**

* Jiska Classen & Daniel Wegemer
https://media.ccc.de/v/34c3-8908-doping_your_fitbit

Case Study: Doping your FitBit*

Remote Association Replay

Associating a tracker should require physical presence!

- **PIN** displayed on tracker is entered into the app, **server-side comparison**.
- Tapping-only trackers send **local confirmation of tapping**.

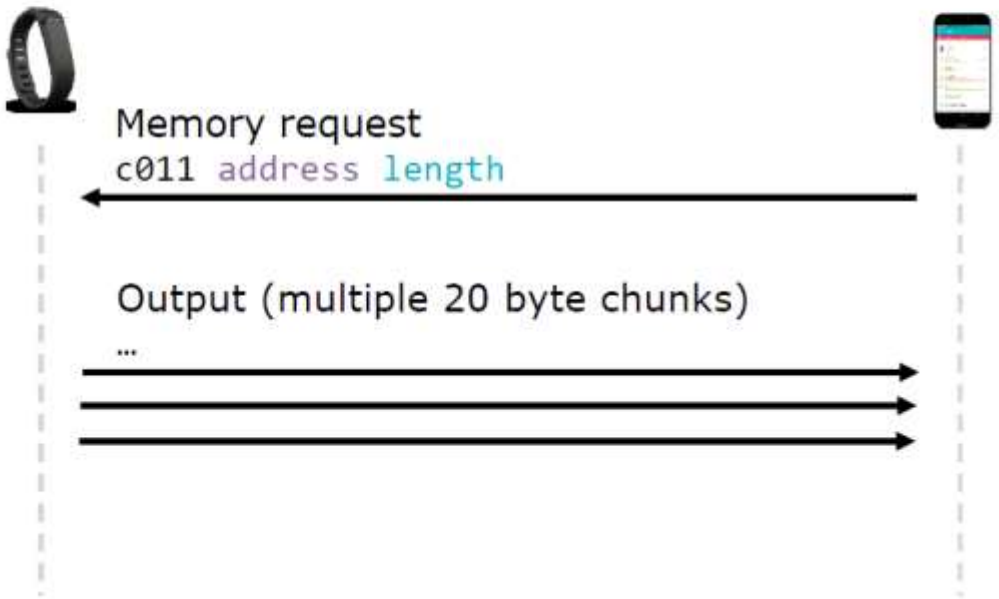
- No confirmation of freshness, **replay possible**.
- Plaintext associations only require knowledge of **serial number**, which is **printed** on the original packing.
- **Authentication credentials** depend on persistent device key, they stay **valid forever**.

* Jiska Classen & Daniel Wegemer
https://media.ccc.de/v/34c3-8908-doping_your_fitbit

Case Study: Doping your FitBit*

Authenticated Memory Readout

- Present in old Charge and Charge HR firmware, discovered by binary diff of firmware update: Read memory, including configurations.
- Update 6.44 and 7.88 (October 2017): **Fix for One & Flex**



Reading encryption key enables:

- Server independence
- Encrypted fake packets

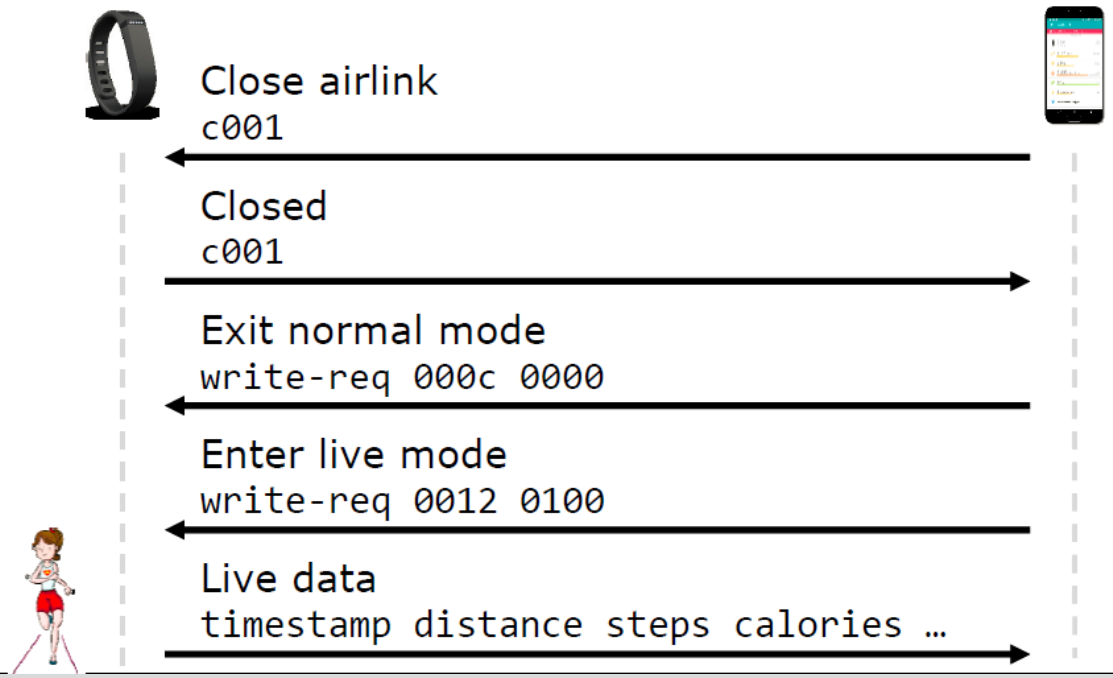
M. Schellevis, B. Jacobs, C. Meijer, J. de Ruiter: **Getting access to your own Fitbit data.** *2016.*

* Jiska Classen & Daniel Wegemer
https://media.ccc.de/v/34c3-8908-doping_your_fitbit

Case Study: Doping your FitBit

Authenticated Live Mode

- Local **plaintext connection** to the app, showing current activity summary.
- Update for all trackers, Alta … Surge (October 2017): **Optionally disable live mode**, but we even saw live mode in Ionic smartwatch logs…



* Jiska Classen & Daniel Wegemer
https://media.ccc.de/v/34c3-8908-doping_your_fitbit

Tools

- RedFang - small proof-of-concept application to find non discoverable Bluetooth devices

  https://tools.kali.org/wireless-attacks/redfang

- BlueSniff – proof-of-concept tool for Bluetooth wardriving

  https://github.com/auraltension/bluesniff (also available on iOS App Store)

- BTScanner – Bluetooth-scanning program that can perform inquiry and brute-force scans, identify devices, export scan results to text file

  https://packages.debian.org/sid/net/btscanner

- BlueBug – tool to exploit Bluetooth security loophole on some cellphones

  https://en.wikipedia.org/wiki/Bluebugging

Demo

Conclusions

- Understand what data is being tracked
- Some fitness trackers have apps that help you manage what data is sent to a paired device or the cloud (i.e. FitBit Live Data, etc.)
- Review any security issues with your fitness tracker (or one you intend to use/buy)
- Keep up to date on security patches/updates

Resources

Collect Your Own Fitbit Data with Python

https://towardsdatascience.com/collect-your-own-fitbit-data-with-python-ff145fa10873

FitBit Web Api

https://dev.fitbit.com/build/reference/web-api/

Getting access to your own FitBit data (Martin Schellevis)

https://www.cs.ru.nl/bachelors-theses/2016/Maarten_Schellevis___4142616___Getting_access_to_your_own_Fitbit_data.pdf

Resources

WearFit: Security Design Analysis of a Wearable Fitness Tracker

https://www.computer.org/cms/CYBSI/docs/WearFit.pdf

Doping your FitBit

https://media.ccc.de/v/34c3-8908-doping_your_fitbit

https://youtu.be/ccbwtrrB4lk?t=0s

Resources

- Here Are the Most (and Least) Secure Fitness Trackers (May, 2018)

  https://www.tomsguide.com/us/fitness-tracker-security,news-27166.html

Questions?

Contacts

Web Site: https://roberthurlbut.com

Twitter: @RobertHurlbut, @AppSecPodcast