EVERYTHING IS A TARGET - YOUR HEALTH DATA IS NEXT
THE AV-TEST INSTITUTE

- MORE THAN 30 IT-SPECIALISTS
- MORE THAN 15 YEARS EXPERIENCE IN ANTI-MALWARE-RESEARCH

- ONE OF THE LARGEST MALWARE REPOSITORIES WORLDWIDE
- STATIC AND DYNAMIC MALWARE ANALYSIS WITH IN-HOUSE TOOLS
- 400 CLIENT- AND SERVERSYSTEMS
- 1.000 TERABYTE TESTDATA
- MORE THAN 5.000 INIDIVIDUAL AND COMPARATIVE TESTS PER YEAR

- ANALYSIS, TESTING, DEVELOPMENT, CONSULTING & SERVICES FOR VENDORS, MAGAZINES, GOVERNMENT AGENCIES & COMPANIES

18.04.2016
Everything is a target - your health data is next
THE AV-TEST INSTITUTE

- MORE THAN 30 IT-SPECIALISTS
- MORE THAN 15 YEARS EXPERIENCE IN ANTI-MALWARE-RESEARCH
- ONE OF THE LARGEST MALWARE REPOSITORIES WORLDWIDE
- STATIC AND DYNAMIC MALWARE ANALYSIS WITH IN-HOUSE TOOLS
- 400 CLIENT- AND SERVERSYSTEMS
- 1.000 TERABYTE TESTDATA
- MORE THAN 5.000 INIDIVIDUAL AND COMPARATIVE TESTS PER YEAR
- ANALYSIS, TESTING, DEVELOPMENT, CONSULTING & SERVICES FOR VENDORS, MAGAZINES, GOVERNMENT AGENCIES & COMPANIES

18.04.2016

Everything is a target - your health data is next
Who
... wants access to the data?

Why
... would they want access to the data?
... should you care?

How
... can they get access to the data?
WHO WANTS ACCESS?

(Cyber) Criminals

18.04.2016

Everything is a target - your health data is next
WHO WANTS ACCESS?

Users

18.04.2016

Everything is a target - your health data is next
WHO WANTS ACCESS?

Multi Billion Dollar Companies
WHY WOULD THEY WANT ACCESS?

- Fitness Trackers may be the next big thing with millions of users
- None or weak security concepts
- Lots of interesting and sensitive data

---

Forecast unit sales of health and fitness trackers worldwide from 2014 to 2015 (in millions), by region

- Western Europe: 2014 - 4 million, 2015 - 7.1 million
- Asia Pacific: 2014 - 2.7 million, 2015 - 4.8 million
- North America: 2014 - 0.6 million, 2015 - 1.1 million
- Central and Eastern Europe: 2014 - 0.2 million, 2015 - 0.5 million
- China: 2014 - 0.9 million, 2015 - 1.3 million
- South America: 2014 - 0.3 million, 2015 - 0.6 million
- Middle East and Africa: 2014 - 0.2 million, 2015 - 0.2 million

Source: Statista, 2015

Forecast of health and fitness tracker market revenue from 2013 to 2020

- 2013: $5 billion
- 2014: $6.5 billion
- 2015: $7.5 billion
- 2016: $9 billion
- 2017: $10.5 billion
- 2018: $11 billion
- 2019: $11.5 billion
- 2020: $12 billion

Source: Analysys Mason, 2014
WHY WOULD THEY WANT ACCESS?

- What kind of **raw data** is there anyway?
  - Accelerometer
  - Pedometer
  - Heart Rate/Pulse
  - Blood Oxygen
  - GPS
  - UV Exposure
  - Ambient Light
  - Skin Temperature
  - Galvanic Skin Response
  - Notifications from the Smartphone (SMS, eMail, WhatsApp,… App Permissions!)

- What kind of **data** is derived from raw data?
  - Stress Level
  - Feeling
  - Sleep Tracking
  - Activity Form and Level (Walking, Running, Biking, Driving – Indoor / Outdoor)
  - Distance / Locations traveled to
WHY WOULD THEY WANT ACCESS?

- Merkel mahnt, es mit dem Datenschutz nicht zu übertreiben (Don‘t overdo data privacy)
  
  http://heise.de/-2812931

- German Chancellor Angela Merkel: „Daten sind der Rohstoff der Zukunft“ (Data: The Resource of the Future)
WHY WOULD THEY WANT ACCESS?

- Personal Data is worth a lot of money

<table>
<thead>
<tr>
<th>Company name</th>
<th>Facebook</th>
<th>LinkedIn</th>
<th>Yahoo</th>
<th>Google</th>
</tr>
</thead>
<tbody>
<tr>
<td>Market cap (in billions)</td>
<td>$100.56</td>
<td>$31.31</td>
<td>$27.67</td>
<td>$282.20</td>
</tr>
<tr>
<td>Number of users (in millions)</td>
<td>1,110</td>
<td>225</td>
<td>627</td>
<td>1,300</td>
</tr>
<tr>
<td>Revenue (in billions)</td>
<td>$1.813</td>
<td>$0.366</td>
<td>$1.135</td>
<td>$13.110</td>
</tr>
<tr>
<td><strong>Per user valuation</strong></td>
<td>$90.59</td>
<td>$131.55</td>
<td>$44.13</td>
<td>$217.08</td>
</tr>
<tr>
<td>Average Revenue per User (ARPU)</td>
<td>$1.63</td>
<td>$1.53</td>
<td>$1.81</td>
<td>$10.09</td>
</tr>
</tbody>
</table>
WHY WOULD THEY WANT ACCESS?

- **Insurance Companies provide Discounts**
  - Vitality (Insurance Company, UK): „The healthier you get, the more we're able to offer you. It's a virtuous circle that's good for you, good for us, and good for society.“

- **German Insurance Companies will pay subsidies:**
  - „Nach der AOK Nordost hat inzwischen auch die Techniker Krankenkasse Wearables und Fitnesstracker offiziell in ihr Bonusprogramm aufgenommen – darunter auch die Apple Watch.“ [http://heise.de/-2817046](http://heise.de/-2817046)
  - They claim they are not interested in the data (yet)

- **Users** may want to **manipulate** the data for better discounts

- **Attackers** may **hold the data to ransom** and threaten the user with loss of their discounted rates
WHY WOULD THEY WANT ACCESS?

- **Tracking of users** becomes even easier
  - “Security Expert Warns of Criminals Using Facebook to Plan Home Burglaries”
  - You don’t even need to actively post, attackers will read the GPS of your fitness tracker
  - „Health-Schufa“ (consumer reporting agency) may prevent you from getting the job, the bank loan or the wife you wanted

- **“Wearable tech will transform sport – but will it also ruin athletes' personal lives?”**
  - By faking data you could manipulate careers or even destroy them

- **Use** of fitness trackers **as evidence at court**

---

**Fitbit Data to Be Submitted as Court Evidence**

*Wearable tech numbers used for personal injury claim*

**Fitbit data increasingly used as court evidence**

*Police: Woman’s fitness watch disproved rape report*
WHY WOULD THEY WANT ACCESS?

- University of Illinois: Using a **homegrown app** on a Samsung Gear Live smartwatch, the researchers were able to **guess what a user was typing** through data "leaks" produced by the watches' motion sensors. [https://www.ece.illinois.edu/newsroom/article/11762](https://www.ece.illinois.edu/newsroom/article/11762)
  - Researchers were essentially able to **guess passwords**
  - **Android malware** is on the rise. It could simply implement this as well

---

**Number of Android Malware in AV-TEST's Database**

- **New Android samples per month**
- **Total number of Android samples**

HOW CAN THEY GET ACCESS?

- AV-TEST evaluated the security of 9 popular fitness trackers, results are available at

- Majority of devices had security issues that allowed unauthorized local or remote access to the data or even the manipulation of data

- Security issues were reported to several vendors
  - Fitbit released a firmware update fixing two critical security issues after working on this with us for a few weeks
  - Others did not reply at all and devices are still vulnerable

18.04.2016 Everything is a target - your health data is next
HOW CAN THEY GET ACCESS? (Example 1)

- **Live-Data**, provides Fitness Data without authentication
- Notifications can be enabled to share the data in (near) real time
- **Fixed!**

```java
// Initialize Bluetooth LE scanning via standard Bluetooth LE protocol
// Establish connection to "Charge" via standard Bluetooth LE protocol
// Discover services running on tracker via standard Bluetooth LE protocol

public void onServicesDiscovered(BluetoothGatt gatt, int status) {
    //Fitness data service; UUID from service discovery
    BluetoothGattService service = gatt.getService(UUID.fromString("558dfa00-4fa8-4105-9f02-4eaa93e62980"));

    //Enable notifications to retrieve fitness data whenever it has changed;
    BluetoothGattCharacteristic serviceCharacteristic = service.getCharacteristic(UUID.fromString("558dfa01-4fa8-4105-9f02-4eaa93e62980"));

    setCharacteristicNotification(gatt, serviceCharacteristic, true);
    // ... Be notified whenever updated fitness data is available
}

public void onCharacteristicChanged(BluetoothGatt gatt, BluetoothGattCharacteristic characteristic) {
    //Fetch the data
    byte[] data = characteristic.getValue();
}
```
HOW CAN THEY GET ACCESS? (Example 1)

- **Replay Attack** to manipulate data
  - Device Time and Alarm clock can be changed
  - Fitness Data can be erased
- Fixed!

---

<table>
<thead>
<tr>
<th>2D020000 00000100 00002D02 00000000 51100000 00000000 000099A8 02702852 09002911 00D402A6</th>
</tr>
</thead>
<tbody>
<tr>
<td>03000000 00000000 20011000 00000000 20202020 20535445 50474545 4B202048 49205448</td>
</tr>
</tbody>
</table>

Welcome Text „STEPGEEK HI THERE HOWDY“

UNIX Epoch → Tracker Systemtime

UNIX Epoch → Alarm Clock time
HOW CAN THEY GET ACCESS? (Example 2)

- Rebranded and distributed by several vendors (e.g. Acer)
- Pairing
  - Requires a PIN
  - 4-digit Hex-Code
  - Problem: „Code“ can be extracted from the device name
- Manipulation
  - Original App uses a library to communicate with the tracker, this library can be (ab)used by anyone, no obfuscation, no other security measures
  - It was possible to write a fake App that has full access to the tracker and is able to manipulate the data
    - New World Record 5000m Run: 8min with 1000 steps!

18.04.2016
Everything is a target - your health data is next
HOW CAN THEY GET ACCESS? (Example 3)

- **Authentication**
  - Original-App checks **Characteristics** and **MAC-Address** (first few bytes) to verify **authenticity of the device**
  - Tracker does not perform any checks of **Smartphone** or **App** → **Anyone can connect**

- **After successful connection (and without authentication)** **data / tracker functions can be manipulated**
  - User information (height, weight, etc.)
  - Factory reset
HOW CAN THEY GET ACCESS?

- Why is that so?
  - **Vendors don’t think about security** at all. One reply we got from a vendor: „Why would anyone hack a fitness tracker?“
  - Vendors have **no experience or knowledge** in the IT Security field
    - Even if they try to implement security, they fail
    - Old mistakes are repeated over and over again:
      - No authentication, broken authentication implementation
      - No encryption, bad encryption implementation
      - Mistakes we have seen 10 or 15 years ago in the traditional IT
  - **Tight deadlines**, market demands, **features** always come first
    - Fixing security after something happened is always more work and more expensive
Final Remarks

- Should users completely abandon these devices?  
  - No, but they should be aware that a lot of devices will give away more information than they expect  
  - There are devices that have a robust security implementation  
  - Right now there are no known real-world attacks to fitness trackers. The possibility is there, but attacks will only be carried out on a larger scale when someone gains benefit from this.

- Should insurance companies really give discounts based on fitness tracker data? Should fitness data be used as court evidence?

- There is much more to come. Criminals (and companies) are way more creative and better in finding ways to monetarize this data

- Even legitimate ways to get (more or less) unauthorized access to your data are imaginable (The resource of the future!)
Thank you very much for your attention!