Eric Clausing

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

Tracking Me, Tracking You. There is Nothing We can do…

Fitness Tracker - Bedrohungen und Angriffsmöglichkeiten unter Android und Bluetooth LE

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

Das AV-TEST Institut in Magdeburg – Hightech in historischem Ambiente

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

15 Jahre Erfahrung in der Viren-Forschung und der Analyse von Antiviren-Software

Wir sind ein weltweit agierender, unabhängiger Anbieter von Services im Bereich IT-Sicherheit und Antiviren-Forschung.

Wir haben 15 Jahre Erfahrung auf dem Gebiet Malware und Anti-Viren Software.

Wir verarbeiten mehrere Petabyte Testdaten mit hunderten Client- und Server-Systemen.

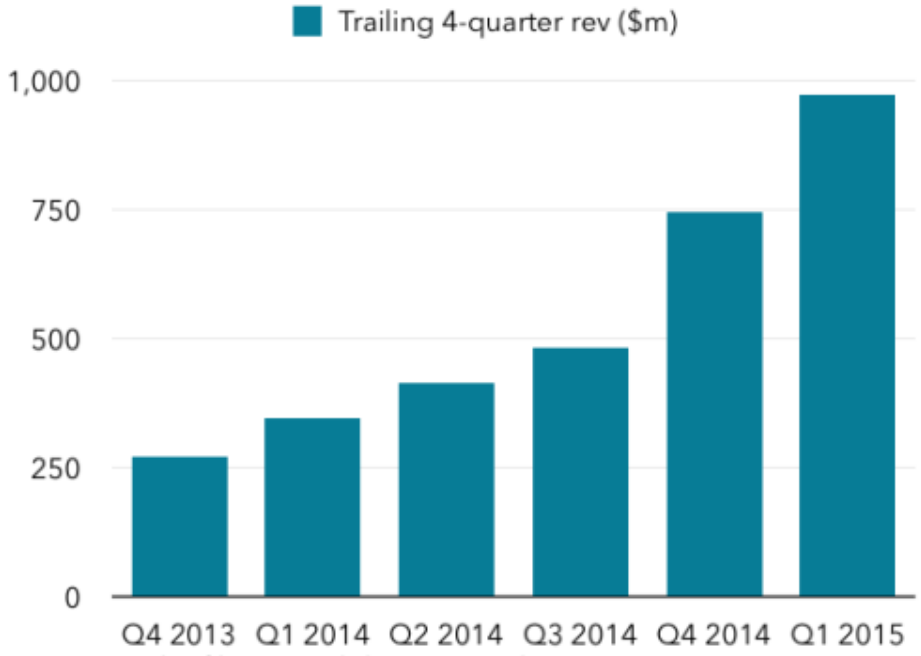
Wir haben unseren Fokus auf Anti-Malware Lösungen (Hard- und Software), blicken aber auch über den Tellerrand.

Inhalt

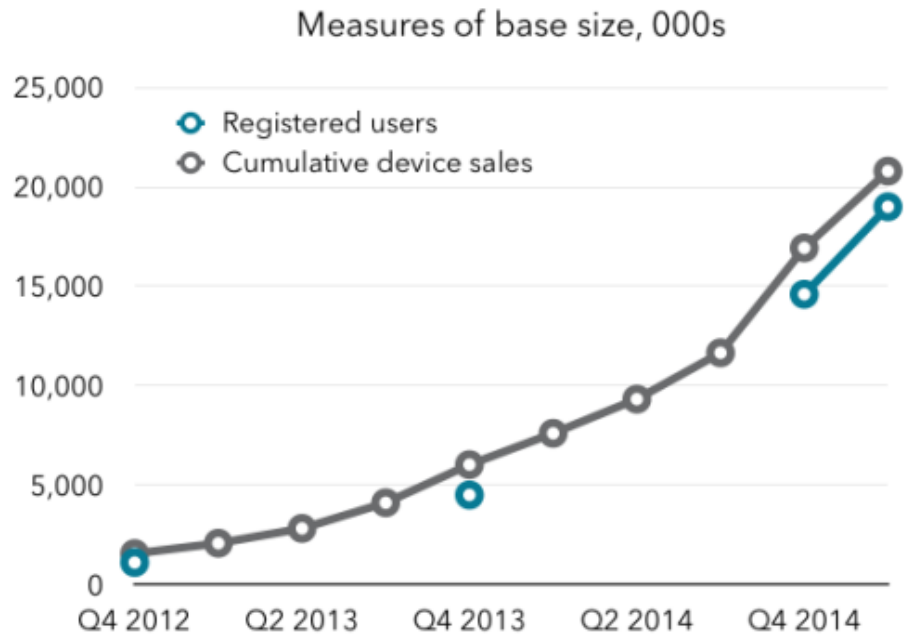
- Motivation
- Bluetooth Low Energy
- Testkonzept
  - Aufbau
  - Getestete Aspekte
- Testergebnisse
  - Häufigste Probleme
  - Ausgewählte Beispiele
- Schlussfolgerung

- **Fitness Tracker**
  - Wearables in **Clip-** oder **Armbandform**
  - Erfassen typischerweise **relativ unkritische Daten**, wie gelaufene Schritte, zurückgelegte Strecke und verbrannte Kalorien
  - **Drahtlose Synchronisierung** der gesammelten Daten mit dem Smartphone (**über Bluetooth Classic/Low Energy**)
  - **Synchronisierung** mit der **Cloud (Dritt-/Anbieter)** über Internetverbindung des Smartphones

- Immer **größere Beliebtheit** und **steigende Verkaufszahlen**
  - **Millionen von Nutzern** als potentielle Angriffsziele und Überwachungsopfer
  - Ständig neue Produkte in diesem Bereich auf den Markt „geworfen“, die teilweise **kein (nennenswertes) Sicherheitskonzept** aufweisen
  - Mit fortschreitender Entwicklung **zunehmende Erfassung sensibler Daten** (Puls, Schlaf, Stress)

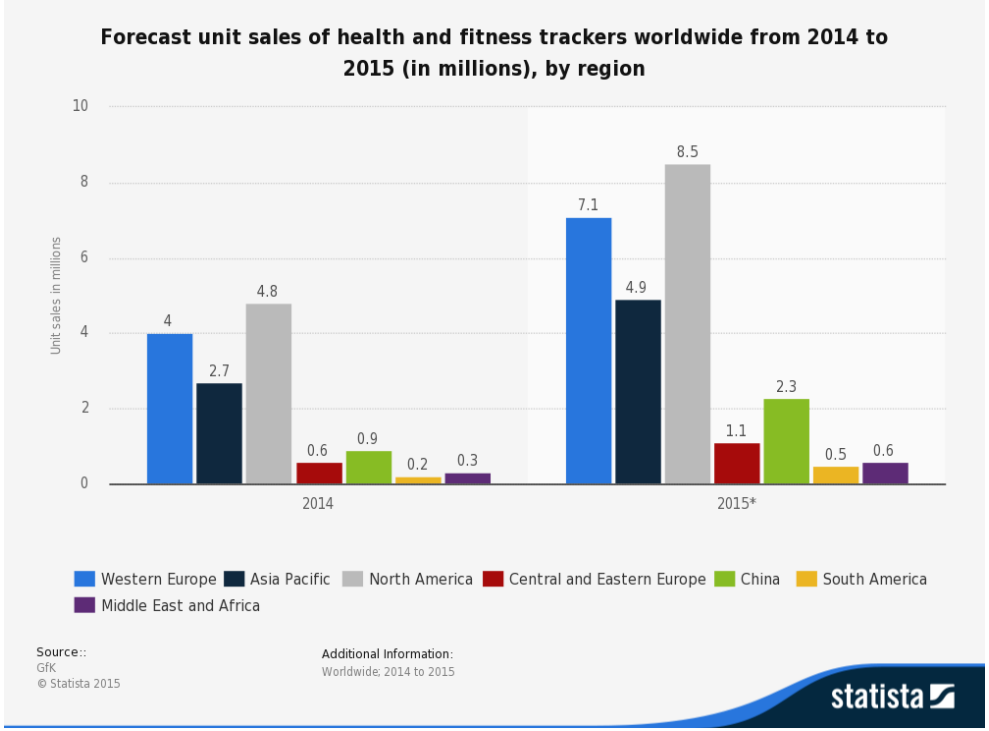


Source: Fitbit filings, Jackdaw Research



Source: Fitbit filings, Jackdaw Research

- Mehrere Konzepte in der Entwicklung, die die **Verwendung** von Fitness Trackern auf **wirtschaftlicher Ebene** vorsehen
  - **Krankenversicherungen** (z.B. Generali[1]) planen **Bonussystem**, das Belohnung besonderer Sportlichkeit und Fitness mit Beitragsrabatten, Sachpreisen und Gutscheinen vorsieht
  - **Große Unternehmen** (z.B. BP[2] und Autodesk) planen ähnliche Nutzung mit dem Ziel der **Senkung der Healthcare-Kosten**
- **Anreiz für Manipulation** zum eigenen Vorteil oder fremden Nachteil dementsprechend **groß**

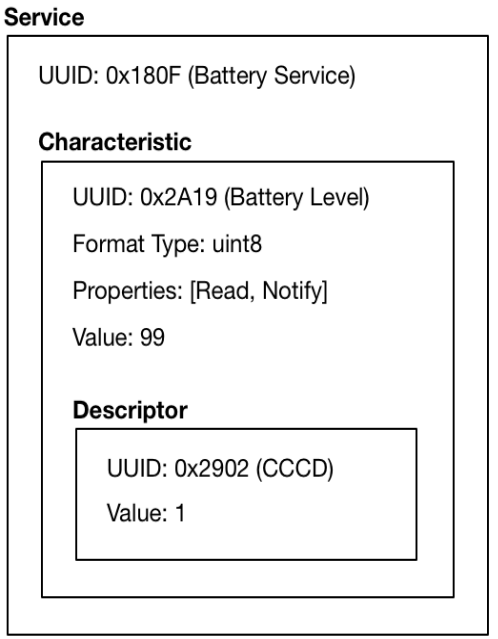


[1]http://www.heise.de/newsticker/meldung/Direkter-Draht-von-der-Kasse-zur-Versicherung-2791960.html

[2]http://hr.bpglobal.com/LifeBenefits/Shared/Pages/BP-Life-benefits/BP-Wellness-Programs/Program-Information.aspx

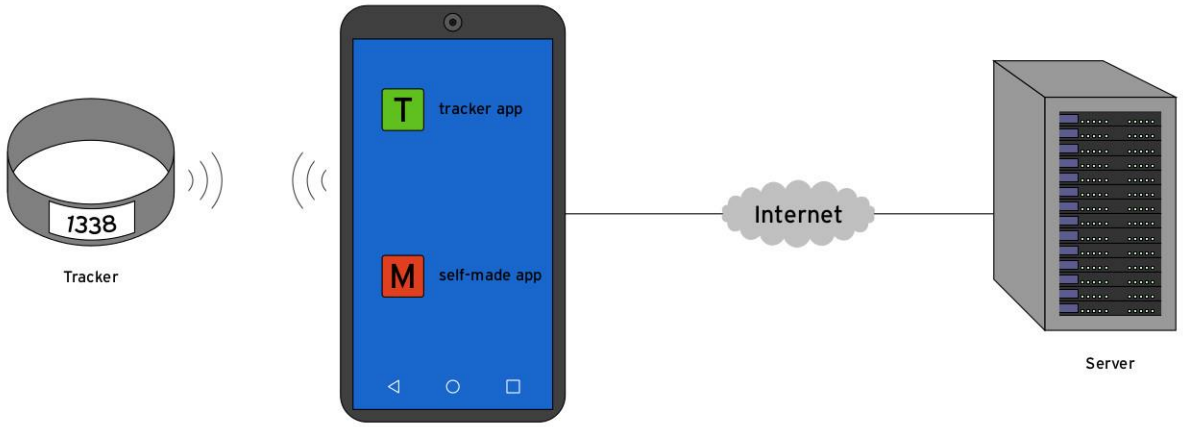
Quelle: http://www.statista.com/statistics/413265/health-and-fitness-tracker-worldwide-unit-sales-region/

- Auch bekannt als ***Bluetooth SMART***
- Eingeführt mit der Bluetooth 4.0 Spezifikation (2010)
- **Vorteile** gegenüber *Classic*
  - Niedriger Energieverbrauch
  - Niedrige Herstellungskosten
  - Niedrige Latenz
    - **Verbindungslos** (Verbindungsaufbau, Übertragung und Verbindungsabbau in unter 10ms)
  - Hohe **Reichweite** von theoretisch **über 100m**
- **Nachteile** (aus Security-Sicht)
  - Geräte standardmäßig für jeden **auffind-** und **verbindbar**
  - **Service discovery** erlaubt jedem den Überblick über laufende **Services**, deren **Characteristics** und deren **Descriptors**
  - Stark vereinfachtes Pairing **erfordert nicht** mehr zwangsläufig **physischen Zugang** (Pin)



Quelle:
http://www.heikomaass.de/2015/07/01/bluetooth-le-gatt-profile/

- Testaufbau
  - Android Smartphones mit **Android 4.4.4** und **5.0.1**
  - Analyse der **Kommunikation** zwischen **Tracker/Smartphone** und **Smartphone/Cloud**
  - Unterscheidung zwischen
    - **Tracker-bekanntem Smartphone** mit **Original-App**
    - **Tracker-fremdem Smartphone** mit **Angreifer-App**
    - **Tracker-bekanntem Smartphone** mit **Angreifer-App**
  - **Kein Angriff** auf das **Bluetooth-Protokoll** oder **HTTPS** selbst!



- Werkzeuge
  - Apktool
    - https://ibotpeaches.github.io/Apktool/
  - APKAnalyser
    - http://developer.sonymobile.com/knowledge-base/tools/analyse-your-apks-with-apkanalyser/
  - APKSmash
    - https://github.com/intrepidusgroup/APKSmash
  - dex2jar
    - https://github.com/pxb1988/dex2jar
  - CFR
    - http://www.benf.org/other/cfr/
  - Android Studio / Android Device Monitor
  - Java IDE nach Wahl
  - Wireshark

- Getestete Aspekte
  - **Bluetooth**
    - Sichtbarkeit
    - Konnektivität
  - **Authentifizierung**
    - Tracker → App/Smartphone
    - App/Smartphone → Tracker
  - **Datenspeicherung**
    - Auf dem Tracker
    - Auf dem Smartphone
  - **Datenübermittlung zur Cloud**
  - **App-Sicherheit** allgemein
    - Obfuscation
    - Debug vs. Release
    - Logging

App name	Version
Acer Liquid Leap	
Leap Manager	1.0.292p
FitBit Charge	
Fitbit Mobile	2.4.2
Garmin Vivosmart	
Garmin Connect Mobile	2.11.2
Huawei TalkBand B1	
Huawei Wear	12.03.02.01.00
Huawei Wear	12.04.03.01.00
Jawbone UP24	
UP - Requires UP/UP24/UP MOVE	4.2.0
LG Lifeband Touch FB84	
LG Fitness	2.5.23
Polar Loop	
Polar Flow	2.1.0
Sony Smartband Talk SWR30	
Lifelog	2.6.A.0.10
SmartBand Talk SWR30	3.0.0.102
Withings Pulse O_x	
Health Mate	2.04.40
Health Mate	2.04.50
Mobile Action Q-Band	
i-gotU Life	1.2.1506.947
Striiv Fusion	
Striiv Activity Tracker	1.0.1024p (nicht verwendet)
Xiaomi MiBand	
Mi Fit	1.5.453

- Bluetooth
  - Mehrheit der Tracker implementiert **kein adäquates Pairing / Bonding**
    - Tracker sind **immer auffind-** und für beliebige Geräte **verbindbar**
    - Nutzer hat **keine Kontrolle** darüber, ob und mit welchen Geräten gerade eine **Kommunikation** stattfindet
- Datenspeicherung
  - Mehrheit der Apps verlässt sich auf den **Zugriffsschutz von Android**
    - **Nutzerdaten** (teilweise mit Nutzerpasswort) liegen im **Klartext** im Appverzeichnis → **Problem auf gerooteten Geräten**
  - Verwendung des freien Speicherbereichs (z.B. SD-Card) um **Log-files** und **temporäre Daten ungeschützt** abzulegen → **Zugriff von Dritt-Apps**

- Authentifizierung
  - Nur einseitig
    - Oft **nur Authentifzierung des Trackers** gegenüber der App
    - Tracker überprüfen aber **in den wenigsten Fällen** die **Authentizität der App/des Smartphones**
  - Hohe **Anfälligkeit** für **Replay**-Attacken
    - Viele Tracker arbeiten mit **festem Auth-Befehl**
    - Selbst scheinbar randomisiert berechnete funktionieren **beliebig oft**
  - **Unvollständige** Authentifizierung
    - **Wichtige Funktionen** von Authentifizierung **ausgenommen**
    - Authentifizierung **in Programmablauf zu spät**
  - **Fehlende** Authentifizierung
    - Teilweise ist sogar die **Nutzung eines Trackers** mit **mehreren Accounts** möglich (Data sharing)

- Datenübermittlung zur Cloud
  - **Keine (wirklichen) Probleme** feststellbar
    - **Sensible Kommunikation** bei allen getesteten Apps **über gesicherte Kanäle**
    - Zusätzliche eine große Menge an **ungesicherter Kommunikation** (mit unsensiblen Daten)
    - **Anfälligkeit** der **gesicherten Kommunikation** sowie potentielle Anfälligkeit über **ungesicherte Kommunikation** nicht getestet
- App Sicherheit allgemein
  - Etwa 50% aller Apps setzen keine oder **keine adäquate Obfuscation** ein
    - **Reverse Engineering erheblich erleichtert** und damit Aufwand für Angriff deutlich gesenkt
  - Einige Apps im vollständigen oder teilweisen **Debug-Status** ausgeliefert
    - Beinhalten noch **Debug-Ausgaben**
    - Legen Debug **Log-files** an
    - Ausführliches **Logcat-Logging**

- Live-Data
  - „Feature“
  - Liefert **Fitnessdaten ohne Authentifizierung**
  - Aktivierbare **Notifizierungen** erlauben Erhalt der Daten in (beinahe) **Echtzeit**

```
// ... 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();
}
```

12 A3 40 55 8C 00
steps

00 00 F0 8B 01 00
floor

59 01 0A 00 00 00
calories

- Synchronisierung Datum / Zeit / Alarm / User-Info
  - **Ohne Authentifizierung** aber (teil-)verschlüsselt / geschützt
  - **Replay-Attacke** möglich
    - Characteristic
      - `adabfb00-6e7d-4601-bda2-bffaa68956ba`
    - Sync-Anfrage über festen Init-Befehl
      - `C0 0A 0A 00 08 00 10 00 00 00 C8 00 01`
    - Tracker bestätigt mit (MAC-Adresse)
      - `C0` / `C0` / `C0 14 0C 0A 00 00` `67 B3 E9 02 6A DA` `17 00`
    - Befehl für Sync-Umfang (Mini-Dump, Mega-Dump)
      - `C0 10 0D` / `C0 10 03`
    - Befehl für Sync des Trackers
      - `C0 24 04 A6 01 00 00` `0A A3` `64`
    - Bestätigung Sync
      - `C0 12 04 00 00 64`

- **Replayed Daten** werden vom Tracker **angenommen und bestätigt**
  - **Systemzeit** wird umgesetzt
  - **Weckzeiten** werden umgesetzt
  - Wenn die neue Systemzeit wenigstens ein Tag vor oder nach der alten Zeit liegt werden **Fitnessdaten auf 0 zurückgesetzt**
- Erst **nach Sync** des Trackers erfolgt **Authentifizierung**
  - **MAC-Challenge** um zu verifizieren dass es sich um Fitbit Device handelt („Tracker is not encrypted, we just assume it's authed“)
  - Erst dann Empfang der Fitnessdaten
  - **Vollständiger Sync** vorher, komplett **ohne Authentifizierung**

```
2D020000 00000100 00002D02 00000000 51100000
00000000 000099A8 02702852 09002911 00D402A6
03000000 00000000 20011000 00000020 20202020
20202020 20535445 50474545 4B202048 49205448
45524520 20484F57 44592020 20202000 00000000
00000000 00000000 00000000 0000 45B2 4C55 0000
00000000 00000000 00000000 00000000 00000000
04000000 14820000 1C020110 0DFC0FC0 FC0FC0FF
FFC0FC0F C0FC0000 BC7F0000 1C020110 0DFC0FC0
FC0FC0FF FFC0FC0F C0FC0001 907E0000 1C020110
0DFC0FC0 FC0FC0FF FFC0FC0F C0FC0002 E8800000
1C020110 0DFC0FC0 FC0FC0FF FFC0FC0F C0FC0003
04000000 05 45B24C 550238B2 4C550124 B24C5504
38B24C55 04000000 01102700 80000000 000AFFF0
3F03F03F 03F0381C 00000000 02000000 00E71400
000AFFF0 3F03F03F 03F0381C 00000000 03000000
00000000 000AFFF0 3F03F03F 03F0381C 00000000
04000000 00000000 000AFFF0 3F03F03F 03F0381C
00000000 02007924 A8060000 00000900 01234798
06000000 0009006D 37000000 00000000 00000087
E4000000 00000000 0000002A 20000000 00000091
0100
C002
```

Klartext Begrüßungstexte „STEPGEEK HI THERE HOWDY“

UNIX Epoch → Trackersystemzeit

UNIX Epoch → Weckzeiten

- Bluetooth Konnektivität
  - **Verbindungsaufbau** sollte **eigentlich(!) Hardwarezugang** voraussetzen (durch Betätigung einer Taste am Tracker soll dieser „aktiviert“ werden)
  - **Verbindung** kann allerdings über kurze Distanz **trotzdem aufgebaut** werden (egal ob mit originaler oder eigener App, bekanntem oder unbekanntem Smartphone)
- Authentifizierung
  - Original-App liest/überprüft die Informationen einiger **frei lesbarer Characteristics**
    - Serial-Nummer von `00002a25-0000-1000-8000-00805f9b34fb`
    - Software-Version von `00002a26-0000-1000-8000-00805f9b34fb`
    - Type-Bezeichnung von `00002a27-0000-1000-8000-00805f9b34fb`
    - Hardware-Version von `00002a28-0000-1000-8000-00805f9b34fb`
    - Company Name von `00002a29-0000-1000-8000-00805f9b34fb`
  - Tracker scheint **keinerlei Überprüfung** des **Smartphones** oder der **App** vorzunehmen

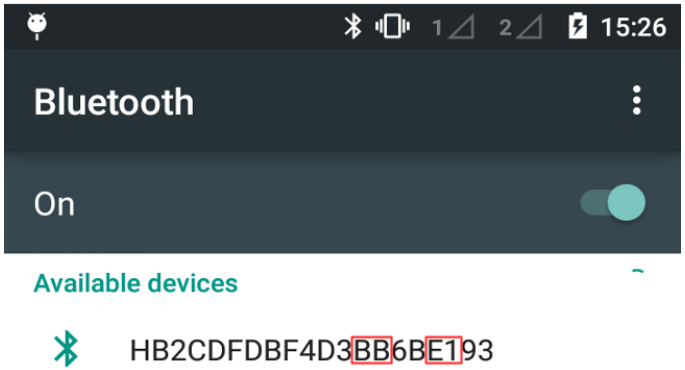
- Steuerung/Manipulation/Auslesen
  - **Steuerungsbefehle** direkt über **00002aff-0000-1000-8000-00805f9b34fb** geschrieben
  - Von jedem **beliebigen Smartphone** das Verbindung aufbauen kann
  - **Steuerbefehle**
    - 00 00 00 70 D5 01 70 17 A4 06 46 00 19 00 10 0E 00 00 1B 00
      (70 17: Gewicht in g/10; A4 06: Größe in cm*10; 46 00: Schrittweite in cm; 19: Alter)
    - 00 00 00 71 FF FF FF FF FF FF FF FF 00 00 00 00 00 00 00 00
      (FF FF FF FF FF FF FF FF: Weckzeiten in min; 00 00 00 00 00 00 00 00: Wiederholungen)
    - 00 00 00 72… - Daily Goals
    - 00 00 00 73-76… - Alarm Labels
    - 1F 00 80 16 - Factory Reset
  - **Fitnessdaten** von Characteristic **00002a53-0000-1000-8000-00805f9b34fb**
    - Einfache **Notifizierung** des Chars **genügt für Erhalt** in Form von 18 Byte Feld mit Daten inklusive Schritte, Kadenz, Geschwindigkeit, Distanz, Kalorien…

- Bluetooth Konnektivität
  - **Einmal bonded** ist der **Tracker** für andere Geräte **nicht mehr auffindbar**
  - **Tracker speichert** MAC-Adresse des **bekannten Smartphones** und ignoriert alles andere
- Authentifizierung
  - Auch das **bonded Smartphone** muss sich **authentifizieren**
  - Authentifizierung besteht aus 20 Byte Feld geschrieben auf `0000ff04-0000-1000-8000-00805f9b34fb` und 12 Byte Feld geschrieben auf `0000ff0a-0000-1000-8000-00805f9b34fb`

    - Tracker-intern wird **nur mithilfe** des **Prüfbytes** authentifiziert (Tracker speichert die User-Infos also vermutlich nicht)
    - Scheinbar randomisiert berechnetes 12 Byte Feld `0F 06 1C 09 1f 02 FF FF FF FF FF FF` (kann allerdings **mehrfach verwendet** werden → Replay)

- Steuerung/Auslesen
  - Steuer-Characteristic **`0000ff05-0000-1000-8000-00805f9b34fb`**
    - **`08 02`** – Vibration
    - **`03 01`** – Schritte in Echtzeit (Notification)
    - **`12 01`** – Sensordaten (Notification)
    - **`09`** – Factory Reset
    - **`0C`** – Reboot
    - **`0B`** – Sync
    - **`0E`** – Farbschema (RGB + Flash)
  - Lesen von mehreren Characteristics (**`0000ff05`**, **`0000ff06`**, **`0000ff0c`**)
    - Schritte, Kalorien, Schlafdaten, (Tief-)Schlafzeit, Batteriestatus, Device Info, User Info…
  - App legt im **Debug Modus** auf SD-Card **Log-File** an mit sämtlicher Kommunikation (Bluetooth + URLs), extrahierten Daten und aufgerufenen Klassen

- Tracker hergestellt von Striiv und **umgelabelt** vertrieben von Acer
- Pairing
  - Nimmt nur Verbindungsanfragen nach **Pairing mit Pinabfrage** an
  - 4-stelliger Hex-Code
  - Problem: **„Code“** wird aus dem **Device-Namen** erstellt




```
public String getCode() {

    if (this.name != null && this.name.length() >= 20) {

        return this.name.substring(12, 14) + this.name.substring(16, 18);
    }

    return "";
}
```

- Manipulation
  - **Original-App liefert** extern verwendbare **Library zur Kommunikation** mit dem Tracker
  - **Keine Obfuscation** → API vollständig und einfach nutzbar
  - Verschiedene Funktionen **ohne Authentifizierung** remote ausführbar
    - **Factory Reset**
      - Registrierter **User** auf Tracker **gelöscht**
      - **Fitnessdaten** auf **Null** gesetzt
      - Tracker **uninitialisiert**
    - **Weckzeiten**
      - Da Anzahl setzbarer Weckzeiten nur durch internen Speicher begrenzt → ca. 120 Weckzeiten möglich (alle 10min von 0-20Uhr)
      - Wiederholfunktion für jeden Alarm (**jede Minute im Zeitraum 0-20Uhr**)

- Manipulation
  - User-Infos zu Größe, Gewicht, Schrittlänge lassen sich auf mehr als **unrealistische Werte** ändern
  - Sogar über die **Original-App** möglich
  - Werte werden **ohne Plausibilitätstest** für die **Berechnung** der zurückgelegten **Strecke** und verbrannten **Kalorien** verwendet

07-07 07:57:02.270 19725-19725/de.avt.bluesearch I/native-activity: JNI updating user profile
07-07 07:57:02.270 19725-19725/de.avt.bluesearch I/native-activity: JNI Updating user to user with ID 356291
07-07 07:57:02.270 19725-19725/de.avt.bluesearch I/native-activity: JNI updating name SHSK.avt@googlemail.com, ID 356291, user weight is 14121.300000, height is 7866.929170, stride is 9027.708676, units is 0, lang is 3, custom is

  - Von Characteristic `0000fff1-0000-1000-8000-00805f9b34fb` erhält man dann Fitnessdaten

Gegangene Schritte | Gelaufene Schritte | Aktive Zeit | Distanz | Kalorien

```
FF F1 07 00 01 CC 00 02 28 00 00 00 08 02 C5 D8 03 CA 00 00 05 62
```

  - Also: 460 Schritte gegangen, 552 Schritte gelaufen, **8min** dafür aufgewandt, **2,9 Meilen** zurückgelegt und dabei 970 Kalorien verbrannt (Weltrekord 5000m: 12,37:35min)

- Manipulation
  - **Initialisierung/Registrierung** des Trackers lässt sich **mit eigener App** (und von Original-App mitgelieferter Lib) vollständig **nachstellen**
    - Tracker liefert Status über Registrierung (nach Factory Reset immer Status= 5=unregistriert)
    - Start der Registrierung veranlasst Tracker Token zu berechnen und zu übergeben
      - Trackerbezeichnung / Version / Token Teil 1
        - `H77E85F147CBEA29D39A:5.1:A117E248D54E6BC8F5A5517A AAC3B073:9D4A87BFE56C9C90ECE5D31094E6186E`
      - Token Teil 2
    - Server antwortet mit encrypted Token
      - `9b261e9d7f3bafce3fbb515ba69977b1:c4be9ad76b4ed35f 27fd1787e30de54e:358c026ec8d4a5f41ca3abd82e75b177`
    - Encrypted Token an Tracker übergeben schließt Registrierung ab
  - An die Registrierungsfunktion müssen **Initialfitnesswerte** übergeben werden, die dann **als Startwerte vom Tracker** übernommen werden
    - → Mit **Factory Reset + Registrierung** lassen sich **beliebige Werte** für Schritte, Distanz etc. auf Tracker setzen

- Im derzeitigen Zustand **nur wenige Tracker** für ernsthaften Einsatz in Bonusprogrammen **geeignet**
  - Großteil der Probleme ließe sich durch **adäquate Authentifizierung** zwischen Tracker und Smartphone / App lösen
- Einige **gute Ansätze** zur Absicherung des Trackers, allerdings zu großen Teilen ungenügend umgesetzt / konzipiert
  - **Design** lückenhaft
  - **Implementation** unvollständig
  - **Reverse Engineering** zu einfach
- **Onlinekommunikation** nach heutigem Stand der Technik **abgesichert**, **keine gravierenden Probleme** feststellbar
  - HTTPS abgesicherte Kommunikation von sensiblen Daten
- **Bedrohung für Privatsphäre** durch fortschreitende Weiterentwicklung der Tracker (GPS, Pulsmessung, Stresslevel usw.) nicht zu unterschätzen

Vielen Dank für Ihre Aufmerksamkeit!