AVAR CONFERENCE 2015

You Are The Target In The Internet-of-Things

Maik Morgenstern
Chief Technology Officer (CTO)
AV-TEST GmbH,
Klewitzstr. 7, 39112 Magdeburg, Germany
Phone: +49 391 6075463, Fax: +49 391 6075469
Web: https://www.av-test.org

Content

Introduction

The Internet of Things brings comfort and many exciting new features to everyone. Smart Home systems make your life easier and fitness trackers will help you to live healthier. These are just two prominent examples. But with every good thing there come bad things as well. IT-Security is a major problem in many of the devices, sometimes nonexistent and sometimes badly designed or implemented.

In 2013 we have started to look into different kinds of devices and have since then analyzed over 30 different products. We have found numerous vulnerabilities that allow unauthorized access to data or even the manipulation of data and functionality.

Right now, users aren't suffering from attacks. Criminals have other ways of earning money and have still to figure out a business model when attacking IoT devices. But as we all know, the bad guys will find ways to get money out of their attacks sooner or later. Therefore it is necessary to be prepared.

This talk will present the experiences we have gathered in the last years and show which mistakes are repeatedly made by vendors of these devices. In the end it is all about the data that is generated or gathered by the different devices. We will discuss who would like to attack, what the targets and objectives are and why they want to do it. On top of that we will propose several steps in order to get more secure devices or at least to be able to use them more securely

Who wants access to your data?

Whenever hacking attacks and unauthorized access to data is being discussed everyone thinks about the obvious attackers: (Cyber-) Criminals. They have lots of different reason to do it and we have seen numerous attacks in the past. In fact the industry we work in does exist solely because of those criminals trying to hack into computer systems and infect them. Obviously they will not limit themselves to Windows PCs or Android smartphones but the Internet-of-Things is another interesting target for them.

However, there are at least two more groups to think about that would be interested in getting authorized or unauthorized access to the data:

1. The user itself
2. Multi-Billion companies

Both may look strange at first, but if you think about the data that is possibly generated by the usage of IoT devices and how this data might be used it becomes a lot clearer. Users may gain advantages by manipulating certain data or by manipulating the functionality of devices. Companies will use the generated user data for their purposes. This may not at all be a security issue. They will likely access the data in an authorized way and with consent of the user. Still this can pose a threat as will be shown in the paper.

Why would anyone want to have access?

There are several answers to this question. First it is important to mention that Gartner predicts 6.4 billion devices connected to the internet by 2016, see the tables for reference.

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**

Figure 1 Smart Home Devices Total and Spendings[1]

With these numbers it is obvious that a lot of potential is there for both people with good and bad incentives. On top of that we know that companies like Apple, Google or Samsung are heavily investing in the market and have released own products already. As you can easily guess, these companies are not only in there to sell their devices. They are particularly interested in the data that comes from the usage of these devices. For criminals there may be very simple reasons. As the figure below shows most of the users in the US would use a smart home system to make their home more secure. If a criminal would be able to hack such a system, then this would be an obvious motivation.

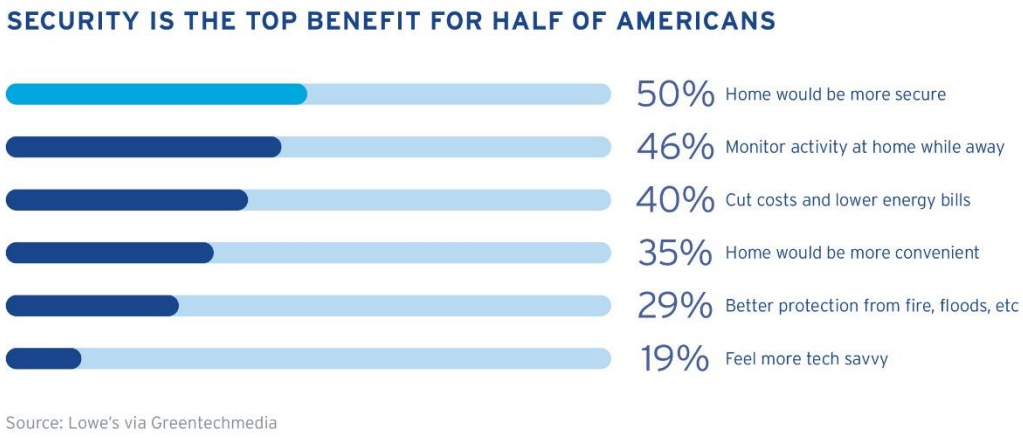

Figure 2 Top motivation to buy Smart Home devices[2]

One of the next big things in the IoT may be fitness trackers with millions of devices sold and more important it is generating lots of sensitive data. The figure below illustrates the sales and registered users of Fitbit devices only. We are talking about more than 20 million devices already.

[1] http://www.zdnet.com/article/six-billion-connected-devices-by-next-year-the-internet-of-things-takes-shape/?linkId=18826980

[2] http://www.greentechmedia.com/articles/read/What-Americans-Really-Want-from-Their-Smart-Homes

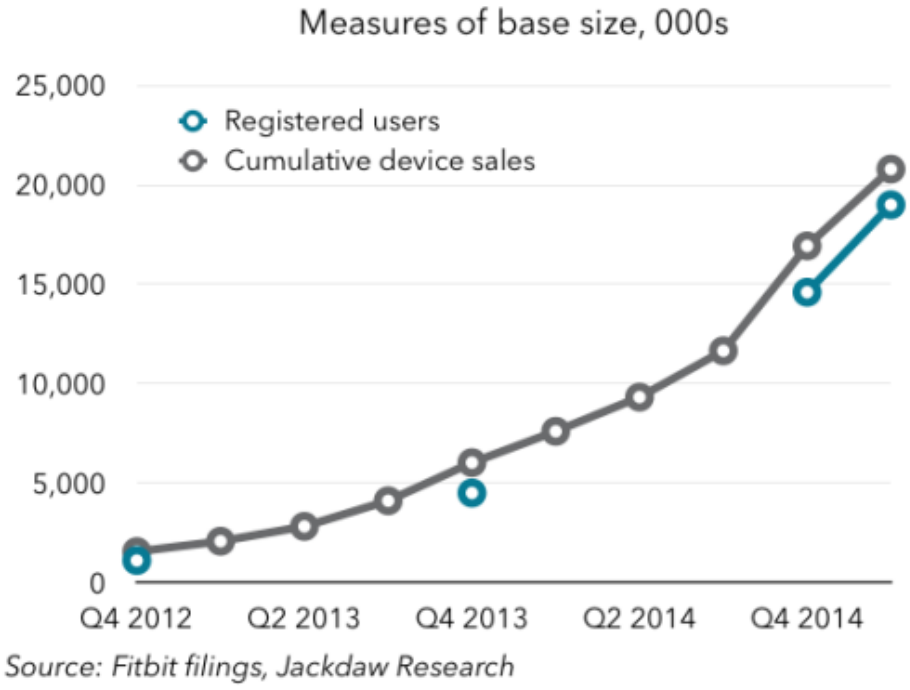

Figure 3 Registered Fitbit users and device sales

And now think about the data that can already be extracted from those devices:

X-axis accelerometer, Pedometer, Activity Tracker (Walking, Running, Biking), Sleep Tracker, Heart Rate/Pulse, Oxygen, GPS, Skin Temperature, Galvanic Skin Response, Stress Level, Notifications from the Smartphone

It is not too difficult to come up with ideas how this data alone could be abused by criminals or even insurance companies. Companies like Facebook, Google or Yahoo are making money with user data already, e.g. by providing advertisement opportunities to companies. The Forbes magazine calculated how much one user is worth to these companies. The numbers are shown in the table below.

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

Figure 4 How much is an user worth?[3]

So the usual browsing behavior and usage of certain social networks already generates enough data that this is worth between 44$ up to over 200$. If more sensitive data such as Fitness tracker data or data from smart home systems are added you can easily imagine that this data gets even more interesting more valuable. And this is the point where criminals play a role again. The user that gives

[3] http://www.forbes.com/sites/tristanlouis/2013/08/31/how-much-is-a-user-worth/

away the data to these companies usually consented to it by agreeing to certain Terms and Conditions and gets some service back in return: You can use Facebook free of charge to stay in contact with your friends and share photos. You can use Google for your search queries, use Google Maps or G Mail and all the other services from Google, again free of charge.

So this is a mutual contract. The user pays with his data, possibly unwittingly, and receives a service free of charge for this.

If cyber criminals steal the same data and users don't receive something in return then this is already a loss to the user. Additionally, the interest of those multi-billion $ companies shows that this data is highly interesting and there is the risk that it could by abused by cyber criminals.

Following are a few examples how this data is already used and could be abused in future:

Example 1

Insurance companies provide discounts based on Fitness Tracker data. Vitality (Insurance Company, UK) says: „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."

As long as you put it this way it sounds good. But instead of doing something for the customer, companies would rather earn more money. The consequences might be that insurance companies won't pay a bonus for healthy living anymore but instead punish unhealthy behavior, according to your fitness tracker data.

Either way, a customer would always be interested in having optimal data to provide to the insurance company. If there is a way to easily hack the device and generate the wanted data, then this might actually happen.

And last but not least, attackers could try to hack into the devices or connected apps and hold the data to ransom: They could delete or manipulate them so the customer would lose the bonus or would have to pay more to the insurance company.

Example 2

User tracking is already practiced by different companies. You search for a certain product on the Internet and the next four weeks you will see advertisements for this product. With more data coming from your IoT devices this can go even further. One possibility is the usage of health data for a consumer reporting agency: These companies take publicly and non-publicly available data to provide consumer credit information. This could make it difficult for certain users to get for example bank loans since banks might argue that the user has a higher mortality probability and might not be able to pay back the loan, all because of fitness tracker data.

Again users might be interested in manipulating this data to get better scores and cyber criminals could again try to hold this data ransom or manipulate it.

Example 3

Researchers from the University of Illinois created a homegrown app to get data from a Samsung Gear Live smartwatch[4]. With this data it was possible to guess what a user was typing through data leaks produced by the watches motion sensors. In the end, researchers were essentially able to guess passwords that were being typed in by users.

[4] https://www.ece.illinois.edu/newsroom/article/11762

Example 4

Following our Research of Fitness Trackers we got inquiries of different public authorities:

- A Pathologist that was working on a case of a dead person wearing a fitness tracker. He tried to extract data to answer several questions he had. 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?

Again it is obvious why users or criminals would have an interest to manipulate this data in order to commit crimes without getting caught.

Example 5

The University of Applied Sciences Münster published research on Smart Meters that allow "Multimedia Content Identification through Smart Meter Power Usage Profiles"[5]. The figure below shows different results for different movies.

[5] https://epic.org/privacy/smartgrid/smart_meter.pdf

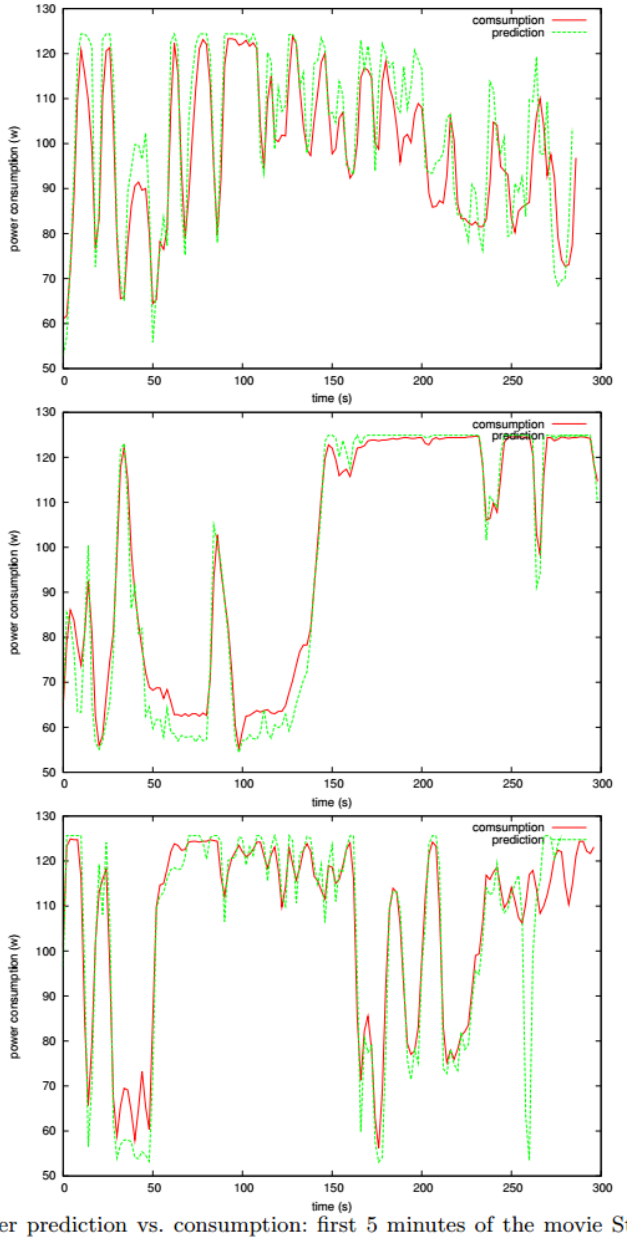

Fig. 5. power prediction vs. consumption: first 5 minutes of the movie Star Trek 11 (top), of episode 1, Star Trek TNG season 1, of the movie Body of Lies (bottom)

Figure 5 Power prediction vs. consumption[6]

Essentially 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".

There have been many more examples in the media that have shown how vulnerable different IoT devices. Sometimes it is not obvious how this could harm the user, sometimes actual harm has

[6] https://epic.org/privacy/smartgrid/smart_meter.pdf

happened. But we can be sure that criminals will find a way to earn money with the data and with the security holes sooner or later.

How could someone get access?

AV-TEST examined the security of over 30 IoT devices during the last two years. This includes 18 Smart Home Devices and 14 Fitness Trackers. The 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/*
- *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 researchers Eric Clausing and Michael Schiefer.

We found that the majority of devices had security issues that allowed unauthorized local or remote access to the data or even the manipulation of data. It is interesting to note that we are seeing the same kind of problems in different product categories. Also we have found that 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

We have reported all found security issues to the vendors. However only a few actually responded and out of those only some acknowledged the security issues and fixed them. Many others didn‘t reply at all and devices are still vulnerable. We will present several examples of the security issues that we have found.

Example 1

Device: Fitness Tracker

A fitness tracker has a feature called Live-Data which provides data without any authentication. It is possible to enable notifications so that data would be shared in real-time. The problem is, that any device could connect to the tracker and get this data all the time. The program code below shows how this is implemented. This issue has been fixed after we notified the vendor and the data will be transmitted encrypted from now on. This disables any unauthorized user from being able to read the data.

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

Figure 6 Code to retrieve the Live Data

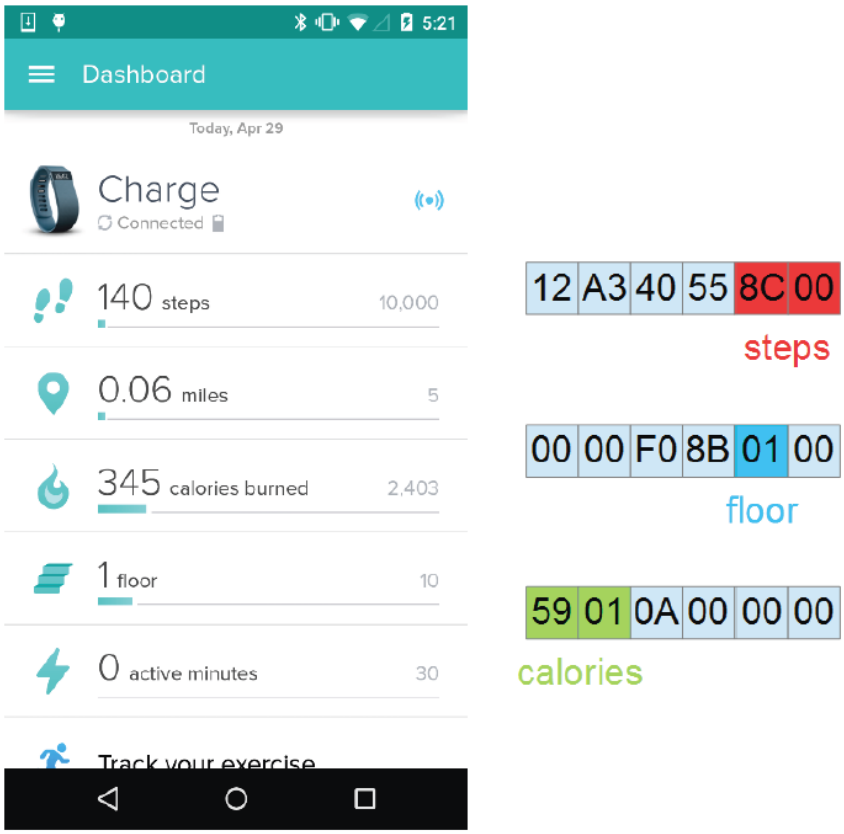

Figure 7 The actual retrieved live data

Example 2

Device: Fitness Tracker

Most devices enable some kind of authorization on the device and the smart phone when trying to connect the devices. There was one tracker that required the user to enter a PIN which is a good thing, because people without the PIN would not be able to connect to the tracker. The problem was

that the PIN could easily be derived from the device name shown in the Bluetooth connection window. See the screenshot below.

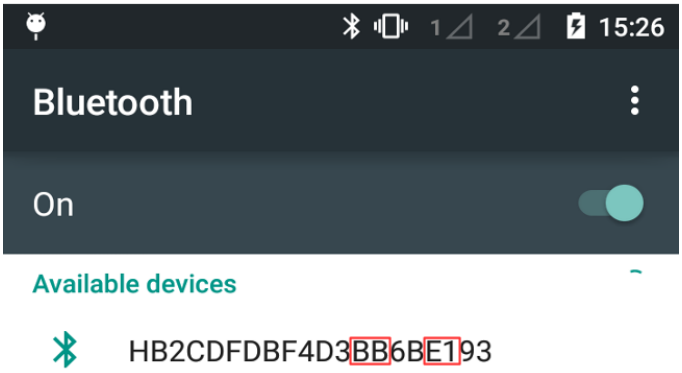

Figure 8 Name of the device and the included PIN

Example 3

Device: Fitness Tracker

For this product pairing with a smart phone should (!) require hardware access by pressing a button on the tracker. Pairing and connecting was possible anyway. No matter if we used the original or a fake App on a previously known or unknown Smartphone.

The authentication step was only done from the smartphone to the device to check whether it is a legit device. However the device didn't check which smartphone is trying to connect. So any smartphone was allowed to connect and data could be retrieved or manipulated.

Example 4

Device: Smart Home Product

This device does everything completely unencrypted. The login to the web portal via the Smartphone App is done in plain HTTP and username as well as passwords are transmitted 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=
```

Figure 9 App Login to the Webservice

The same is true for the actual usage of the device. Anyone in the network can take control with simple HTTP requests. There is absolutely no authentication or other security measures.

Example 5

Device: Smart Home Product

This Smart Home device offers backup of the configuration file in the cloud. It is possible to crawl this cloud for ALL backups of all users by just providing the serial number of the device which is easy to guess.

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 the available 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 received the ID you can download the given backup. In fact it looks like the IDs are just incremented one by one and could just be brute-forced.

Now that you know the IDs you can not only download the backups but also delete or replace them. Replacing is actually very easy because the configuration database is a simple LiteSQL Database. You could easily add users by copying the information from your own device and it is possible to change the privileges of a normal user to a super user for example.

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 > >|

Figure 10 SQLite Database containing the configuration

Now you would have to get the user of the device to use the manipulated backup somehow and you would have full access to the device.

Example 6

Device: Smart Home Product

A smart home product that uses SSL for the remote connection but doesn‘t verify the connection, so man-in-the-middle attacks are easily possible. Once the man-in-the—middle attach has been carried out it is possible to read the encrypted network traffic including an access token that can be used to take over the connection. No further logins are necessary once you got the access token which can be used to take full control over the device by using the remote functionality. The access token remains valid even after the user logs out of the active session.

Figure 11 Access Token

It is further possible to retrieve user information including the PIN for local access to the device, resulting in full control over the box.

Why are IoT devices so insecure?

There is no general answer to that, but there are a few things to consider.

A general observation is that many vendors don‘t think about security at all. One remarkable reply we got from a vendor: „Why would anyone hack a fitness tracker?“ While it is true that it is sometimes difficult to see the possible harm or damage this should not be an excuse to keep a device insecure.

Further to that most vendors have no experience or knowledge in the IT Security field. We have seen attempts to implement security, but vendors failed, e.g. by implementing encryption on their own instead of using industry accepted libraries. Similar cases happened with authentication and were described above. In other cases vendors didn’t think about encryption at all and data is being transmitted in plain text, even passwords.

In general one could say that many IoT devices repeat mistakes that we have seen 10 or 15 years ago in the traditional IT field already.

Another possible reason why this happens may lie in tight deadlines, market demands and that features have to come first making security an afterthought. But as well know fixing security after something happened is always more work and more expensive

What should be done to fix this?

In order to answer this question we have to make clear what we are looking at:

1. Security issues in devices
2. Sensitive data that may be abused

The following picture describes what this is about.

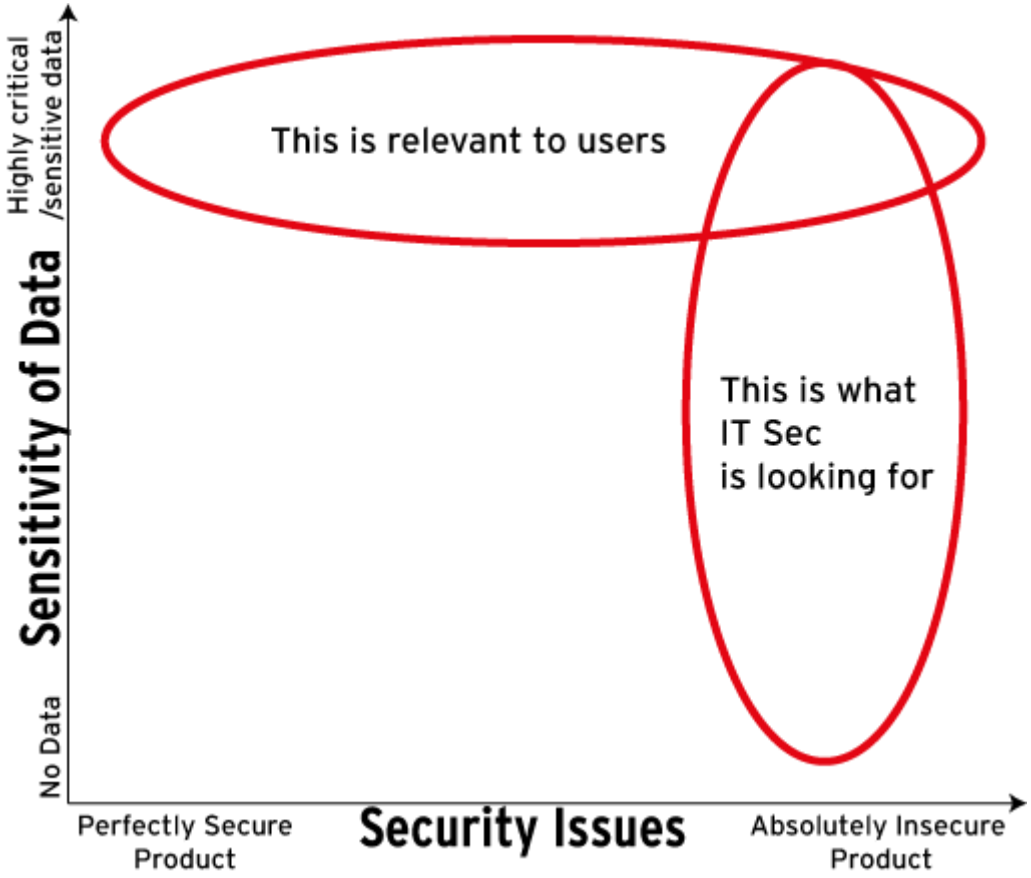

Figure 12 Security Issues vs. Sensitive Data (1)

When talking about the insecurity of IoT devices, we usually refer to the right hand side of this graph: Looking for security vulnerabilities in the device, the apps or the cloud services in order to extract/manipulate data or get control over the device. But as we pointed out above, there may be devices where it is difficult to do any actual harm, even if they have security issues and on the other hand there may be devices that are perfectly secure but share very sensitive data which could still cause harm to an user.

The following representation illustrates this some more.

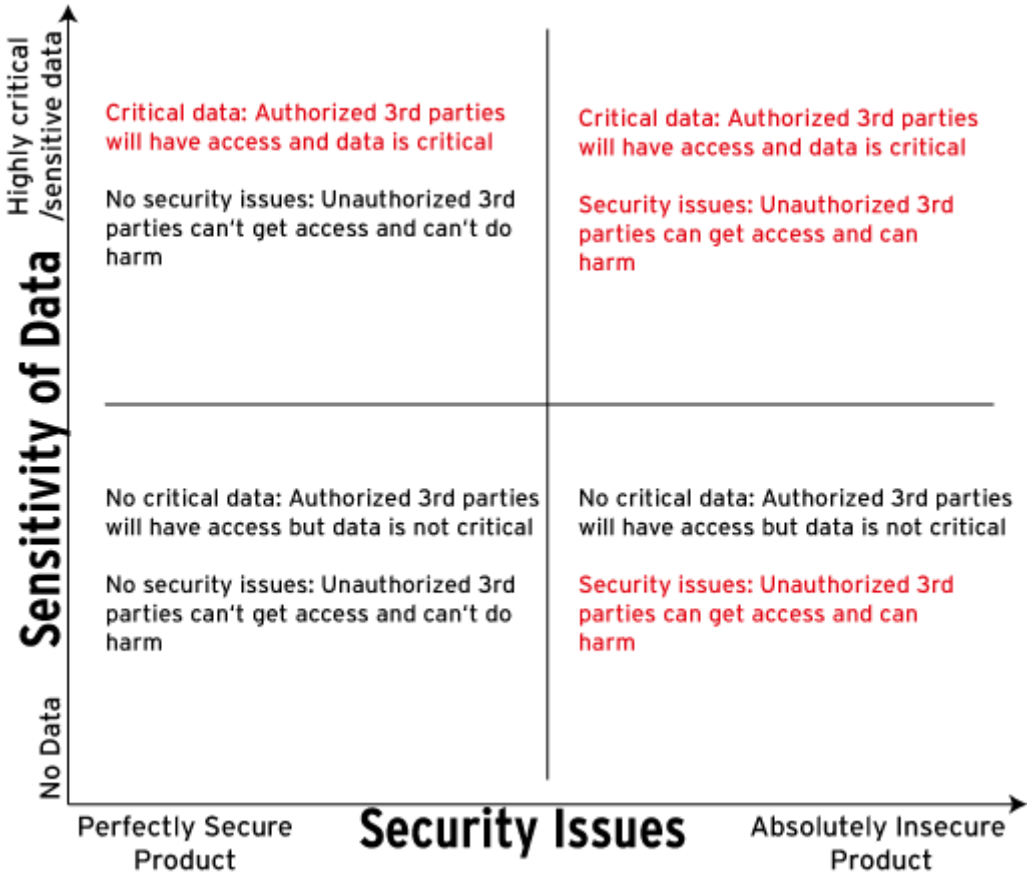

Figure 13 Security Issues vs. Sensitive Data (2)

This illustrates that you always have to think about two issues:

1. What kind of data is being shared? Sensitive or not sensitive?
2. Who could possibly get access to the data and the device? Authorized or Unauthorized 3rd parties?

Therefore different approaches are required to cope with these two problems. Certainly a lot of technology improvements are required to minimize the risk of security vulnerabilities in the products, this includes but is not limited to:

- **Threat Modeling**: Be aware what the attack surface of the device is and what kind of data is being generated/collected.
- **Security-by-Design**: Security has to be integral part of the development and implementation process.
- **Robust implementation**: Not every vendor can be an IT Security expert. There are a lot of well know and documented best practices for IT security. Use industry accepted security measures and libraries that provide the functionality you need in a secure way.
- **External penetration/security testing**: Even if you try your best, you will make mistakes here and there. External security testing will help to catch those before release.
- **External verification/certification**: This shows the public that your product has been tested/certified for security and passed the tests. This provides a marketing advantage but also forces other vendors to get their products tested for security, resulting in a higher overall security level.
- **External security measures**: Sometimes it is not possible to fix problems in a product, for whatever reason. In that case 3rd parties could provide solutions such as security appliances

that protect the network where the IoT device runs in. Another example is the usage of security software on the device that is used to access the IoT device, this usually refers to smartphones, tablets and PCs.

Those technology improvements should be well know and more and more IoT vendors hopefully implement them. But as we have shown there is not only the risk of unauthorized access to the device. Another risk is the uncontrolled or unwanted but authorized access of 3rd parties to critical/sensitive data. Users are often not aware what kind of data is being shared and which company has access to the data and what the possible harm could be. Therefore we also propose a discussion about non-technical improvements. We see two main areas here:

1. Privacy Laws
    a. What data is allowed to be collected?
    b. What data is allowed to be transmitted?
    c. What data is allowed to be processed?
    d. Who is allowed to collect the data?
    e. Who is allowed to receive the data?
    f. What is allowed to do with the data?
    g. Is this opt-in, opt-out or even mandatory?
2. Education of users
    a. Tell them about possible abuse of their data
    b. Give guidelines on how to secure their systems and devices

These are of course very broad fields and very general topics. Laws will differ from country to country and it will be difficult to ever find a solution. But we feel that this part of the discussion is currently underrepresented and research focuses too much on the security issues alone. As we pointed out, even a perfectly secure product that shares sensitive data with an authorized 3rd party could cause harm to the user.

Therefore we want to emphasize that it is important to secure the devices but also to discuss about the abuse or misuse of sensitive user data. This topic becomes more relevant every day, with new IoT devices and new functionality that will affect all of us in only a few years.

Conclusion

One question that should come into mind is whether users should completely abandon IoT devices? The answer is: No. Even if you wanted, you would probably not be able to because you won't be able to live without IoT devices sooner or later anyway. But you should be aware what risks exists around IoT devices. Also there are actually secure devices and we are seeing improvements in the 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.

However we should be aware that there is much more to come. Criminals (and companies) are way more creative and better in finding ways to monetarize this data.

That's why this should be an ongoing discussion and we have to make sure that both the security of the devices and the protection of the data is part of the future developments.