Security in the Internet of Things (IoT)

Niklas Lensing
School of Electronic Information and
Electrical Engineering
Shanghai Jiao Tong University
Email: Niklas.Lensing@gmail.com

***Abstract*—This paper deals with security in the Internet of Things (IoT).**

In a brief introduction it will be elaborated about what the IoT is. Subsequently it will be explained why security in the IoT is important with the help of some examples.

The main focus of this paper is the analysis of the current status of security. Findings from different organizations are being discussed and then evaluated.

Finally some thoughts about improving the current security situation are expressed.

***Index Terms*—Internet of Things, IoT, security, security threats.**

I. Introduction

The Internet of things (IoT) is a trending topic. Some say that the IoT will shape our future lives. But what exactly is this Internet of Things?

The International Telecommunication Union (ITU) states that: "The Internet of Things is the network of physical objects or 'things' embedded with electronics, software, sensors, and network connectivity, which enables these objects to collect and exchange data." [1]

The Oxford University published a definition seeing the IoT as "a proposed development of the Internet in which everyday objects have network connectivity, allowing them to send and receive data." [3]

Furthermore HP observes that "suddenly, everything from refrigerators to sprinkler systems are wired and interconnected (...). These devices are now collectively called the Internet of Things (IoT)." [3]

As one can see from these three citations there is no fixed definition of what the Internet of Things is. Bringing the key points together one can learn that they all stress the idea of devices being connected to the Internet to exchange information. This is a quite spacious definition allowing lots of devices to count themselves into the range of IoT devices.

Another point that can be observed is the diversity of the entities being involved into the IoT. These three quotes are from an international standardization organization, a famous university and a big IT company. So it can be concluded that there are different stakeholders being involved into the IoT. It is a topic which affects several areas and therefore attracts so many different entities.

Due to the growing importance of IoT and it's seemingly endless possibilities it naturally also attracts the attention of hackers. As a consequence one might ask: What is done about security in the IoT? Do we actually need it all? These are the questions that this paper will focus on.

II. Why is security in the IoT important?

Not securing your IoT devices properly can have serious consequences. Hacked IoT devices can be very dangerous in the hands of people with bad intentions. They could either manipulate the device so that it causes damage to others or steal the information stored on this device.

What is more the IoT is becoming more and more interesting for hackers as it is growing fast and a lot of money is involved. Both factors that make it a lucrative target.

A. Hacked "things" can lead to serious problems - an example

A popular example for emphasizing that security in the IoT is very important is a security flaw in the Jeep Cherokee. The Jeep Cherokee is an all-terrain vehicle which features an infotainment system called UConnect. The US model features a modem which connects the car to the Internet. With the help of this modem hackers were able to hack over the Internet into UConnect which in turn had access to the car's central CAN bus system. This CAN bus can be found in a lot of modern cars and it is used to distribute information between the car's electronic devices. With access to the CAN bus the hackers were able to send instructions to the car's brakes, the gas and in reverse gear even to the wheel. [4]

One might ask how it is possible that the infotainment system was entitled to do so? Why was there no protection against such non authorized commands?

First of all it has to be stated that connecting the infotainment system to other electronic devices in a car is very useful. For instance the infotainment system of the Jeep Cherokee adjusts the volume of the music according to the speed of the car and to do so it needs to be connected to the CAN bus. However the CAN bus was not designed to be secure against hacker attacks. When the CAN bus was designed it was a closed system and attacks from outside were not an issue. It was not foreseeable that cars would get connected to the Internet.

This example shows one of the major problems of IoT devices. A lot of the "things" that are getting connected to the internet now were never designed to be secured against hacker attacks. As they were initially not designed to be secure, it is very hard to implement security afterwards.

Fig. 1. The infotainment system UConnect of the Jeep Cherokee

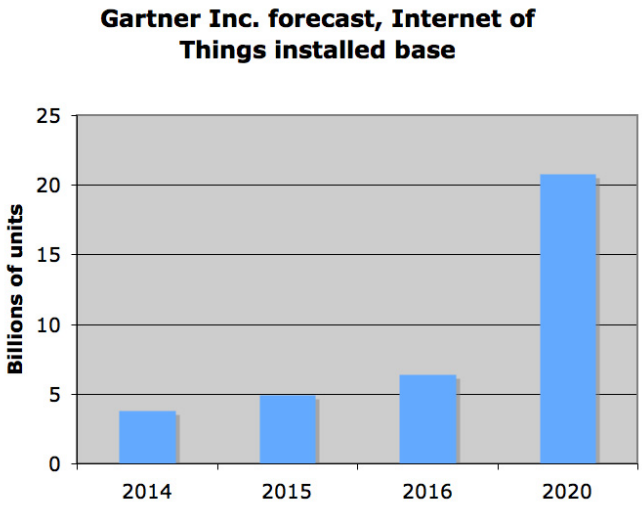

Fig. 2. Gartner forecasts more than 20 billion IoT units by 2020

B. Sensitive data processed by "things" should be protected

IoT devices help us in our everyday life. To do so, several of these devices have access to very sensitive personal data.

One example is the Apple Watch which gathers several sensitive information. The watch has an integrated heart beat scanner so it holds information about the user's health condition. What is more it can be used with Apple's payment system Apple Pay and therefore has access to banking information. With the help of an iPhone it can also obtain the current GPS position.

To sum it up an Apple Watch is able to hold information about one's health condition, banking and location data. All of these are data which surely a lot of people would like to be kept secret. And to keep these data secret proper security is necessary.

C. IoTs importance is growing fast

The IoT is currently a big trend. Researchers, organizations and companies engage themselves with the IoT and as a result it is growing fast. According to Gartner, by 2020 the IoT will include more than 20 billion units and it will generate incremental revenue exceeding $300 billion. [5]

These figures make it a very lucrative target for hackers. 20 billion units is a huge playground that can be hacked and hackers will even be more motivated as there is a lot of money involved. Hackers have already proven to be able to hack into IoT devices and they will continue to try. As a consequence IoT devices should be secured properly.

III. Current status of security in IoT

Regarding the arguments and examples from the previous section, security should be handled seriously in the IoT. In this section the current status of security in IoT will be elaborated.

To get an overview about the current status a study on security in IoT devices and the OWASP Top 10 list will be evaluated.

What is more it is discussed how IoT devices are being patched.

A. IoT security study

A current study ([3]) conducted by Hewlett Packard (HP) evaluated on the security of IoT devices. In this study HP searched for security issues in IoT devices. They tested 10 IoT devices for common security flaws. These 10 devices were:

- TV
- web cam
- home thermostat
- remote power outlet
- sprinkler controller
- hub for controlling multiple devices
- door lock
- home alarm
- scale
- garage door opener

Some of these devices have access to sensitive information about the user. The TV for example could tell a hacker which programs the user likes to watch. Spying on a web cam might give hackers a very intimate insight into the user's life.

Others of these devices are a lucrative target to be manipulated by an attacker. A hacked home alarm and door lock would for example facilitate a house robbery.

As a consequence one might anticipate that these devices were secured properly against attacks. However the HP study results show different facts.

HP found out that 7 of these 10 devices did not encrypt their network services. That means all the information being sent from and to these devices could easily be intercepted and read by an attacker.

Furthermore 6 of the devices had insecure web interfaces. HP found security loopholes in these web interfaces which allowed them to hack into the device. Hackers could have used

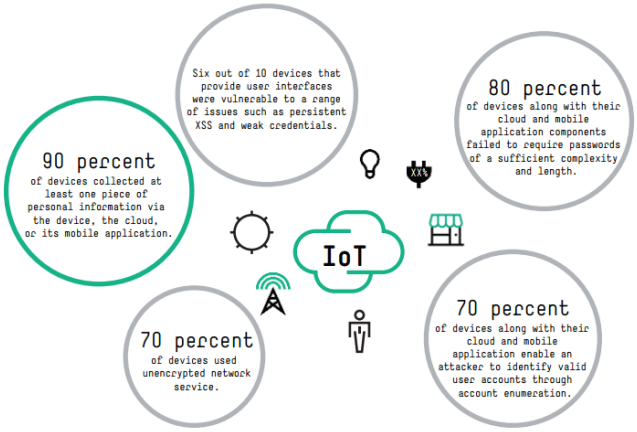

Fig. 3. HP study results

these loopholes to get access to the device's controls without having the permission to do so.

Several devices also lacked a sufficient password policy: 8 of the devices allowed the user to set passwords like "123" or "abc". A hacker would have no problems to find out these passwords and get access to the device.

Finally 7 of the 10 devices allowed attackers to identify valid accounts through account enumeration. This means that these devices would tell an attacker whether a certain account exists or not. This can be misused to find a valid user account and then perform a directed attack on this account.

Figure 3 shows a summary of all the results from the HP study.

Although these results are concerning one might argue that a study on 10 devices is not representative for the whole IoT business. It could not be proven that these concerning flaws were common in IoT devices. To contradict this argument HP argues in [3, p. 6]: "While there are certainly large numbers of IoT devices already on the market, and that number continues to grow on a daily basis, we believe the similarity in results of this subset provides a good indicator of where the market currently stands as it relates to security and the internet of things."

Even if this study might not be representative for the whole IoT business: Many of the security flaws found by the study are simple flaws. They would not need much work to be fixed. So it seems there is either a lack of time or will to handle security in at least some IoT business areas.

B. OWASP Top 10

The Open Web Application Security Project (OWASP) is a foundation which tries to enforce security throughout the Internet. To do so, it runs several projects which aim to establish a safer Internet.

Among these projects OWASP publishes a list of the top 10 security flaws in the IoT. It lists the most common mistakes done about security ordered by their frequency of occurrence. The list can be seen in figure 4.

Fig. 4. The OWASP Internet of Things Top 10

With this list OWASP wants to give developers an overview about which security issues are common and how they should be handled. To every of the 10 security flaws exists a detailed page which gives further information on how to take counter measures against the threat. Developers who are unfamiliar with security topics are supposed to use this page as an information source to secure their software properly.

Point 1, 4 and 8 on the Top 10 list were also mentioned in the study which was discussed in the previous section: Similar to the points on the Top 10 list the HP study found out that many of the devices tested had an insecure web interface, did not encrypt their network traffic and featured insufficient security configurability which means amongst other things that a sufficient password policy is missing. That these points are also mentioned in this Top 10 list is another indicator that the results of the study are accurate.

According to the top 10 list insufficient authentication/authorization is a common security flaw in IoT devices. This flaw comprises bad or non existing password encryption and the lack of user roles.

Passwords should always be encrypted. This includes both, when they are saved in a database as well as when they are sent over the network. If this is not done a hacker could easily extract the password from network traffic or try to steal the database and get the password from there without any effort.

User roles are essential to a securely working environment. Not all user accounts for a system should have the same rights. There should be a distinction between different roles. Otherwise every user could change passwords or delete users which facilitates the work for attackers.

The third point on the list, insecure network services, is

referring to open ports on network devices which could be closed as they are not needed. Hackers often look for well known ports which are known to offer insecure network services. To minimize the risk of being attacked all ports which are not absolutely necessary for proper operation should be closed.

Another point mentioned on the list are privacy concerns. When collecting user data it should be carefully determined which information are absolutely necessary to be stored. User data which is not needed should be discarded to make a theft have less impact on the user's privacy. In addition to that it should also be clearly determined who is allowed access to sensitive user data. Only persons who really need access to the data should get it.

Point 9 and 10 on the Top 10 list are topics which demand a rather high effort to be met.

Insecure software/firmware refers to security holes in software. OWASP states that there should be a mechanism to update software on IoT devices. As the devices are exposed to the Internet hackers will eventually find security holes in the software and exploit these holes. Hence there has to be a mechanism to fix them.

The last point on the list, poor physical security, states that the devices should be stored in a secured place where attackers cannot easily get access to. This minimizes the risk of direct physical intervention on the device by an attacker.

Analysing the points on the Top 10 list, one can see that the upper points on the list are simple security flaws which can be met with rather little effort. The more complex and expensive security issues such as an update mechanism or ensuring physical security are the last points on the list. Taking into account that the points are ordered by their frequency of occurrence it can be concluded that not a lot of effort is put into ensuring security in IoT. This reflects the findings of the HP study mentioned above which also stated similar facts.

C. Patching problems

Security updates are an important means to fix holes that were not known when a software got released. For software which has been exposed to the web for a longer time such as operating systems and browsers it is common practice to release security patches at least once a month. These patches are then distributed over the Internet.

The software update process in IoT is still an unsolved problem in a lot of cases. The problem in IoT is that a lot of the devices where the software runs on are difficult to update or were not initially designed to get software updates.

One example are cars. For software updates cars normally need to be send back to the car manufacturer as only he has the know how to perform software updates. However, implementing the practice of sending the car back to the car manufacturer every month for security updates is for obvious reasons not possible. A different approach is needed.

Another aspect is that several IoT devices are being used a longer time than common devices that are connected to the Internet nowadays. As technology is developing fast, it is hard to maintain security and interoperability for old devices with other, newer web devices. In [6] one example of this problem is given: "We have one customer monitoring HVAC systems chilling a data center, and these industrial chillers last a long time - some are 80 years old. But the technology for monitoring has a much faster upgrade cycle. How do you build an architecture for things like that that's enabled for upgradability?"

These unsolved patching problems are still unsolved in many business areas of the IoT.

IV. Conclusion

It can be stated that currently there is a lack of experience and/or will to deal with security in IoT properly. Developers seem to invest their time rather into new features than into security. This is reflected by the results of the HP study and the OWASP Top 10 list. Also the unsolved problem of developing an update mechanism shows that there is little motivation to deal with security related topics.

No matter where this lack of motivation comes from - no experience or no will - security in IoT should and can be dealt with.

Assuming that there is a lack of experience there are means to get information such as the OWASP Top 10 list which gives a good introduction into the topic. Developers could use the information from this project to secure their IoT devices against the most common threats with little effort.

Developers might argue that right now they do not want to deal with security and rather prefer to focus on implementing new features. Security could be dealt with later. However this way of thinking has proven to be wrong: The problems with the CAN bus in the Jeep Cherokee show that implementing security after the design phase can be difficult or even impossible.

As a result security has to be considered in the design of IoT devices. Implementing security later is complicated and costs a lot more or is even infeasible. It is cheaper - time and money wise - to implement security now.

One might also ask if really all these "things" being connected to the Internet right now, do need this connection. Does for instance an iron need an Internet connection? There are some which do have one. Perhaps part of the solution for the IoT security issues is quite simple: Just do not connect some "things" to the Internet at all. A proper thought about the benefits of connecting a device to the Internet might help to reduce security issues.

The aim of this paper is not to condemn the IoT or to make it look as a bad idea. This paper just wants to emphasize that security should be considered more carefully in the design of IoT devices. The IoT bears a lot of fascinating opportunities but while exploring these, security issues should be considered and included into the design. Ignoring security threats can lead to severe problems as this paper pointed out.

ACKNOWLEDGMENT

The author would like to thank Hewlett Packard (HP) and the Open Web Application Security Project (OWASP) for providing the foundation that this paper is based on.

REFERENCES

[1] International Telecommunication Union (ITU), *Internet of Things Global Standards Initiative*, http://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx, last access: 2015-11-03.

[2] Open Web Application Security Project (OWASP), *OWASP Internet of Things Top Ten Project*, https://www.owasp.org/index.php/OWASP_Internet_of_Things_Top_Ten_Project#tab=OWASP_Internet_of_Things_Top_10_for_2014, last access: 2015-11-03.

[3] Hewlett Packard (HP), *Internet of things research study*, http://www8.hp.com/h20195/V2/GetPDF.aspx/4AA5-4759ENW.pdf, last access: 2015-11-03.

[4] B. Benz and F. A. Scherschel, *Der Feind im Innern* c't - Magazin fuer Computer und Technik, Germany: Heise Verlag, 21/15.

[5] Gartner, *Gartner Says the Internet of Things Installed Base Will Grow to 26 Billion Units By 2020*, http://www.gartner.com/newsroom/id/2636073, last access: 2015-11-08.

[6] arstechnica, *The future is the Internet of Things-deal with it*, http://arstechnica.com/unite/2015/10/the-future-is-the-internet-of-things-deal-with-it/, last access: 2015-11-10.