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*—Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Etiam lobortis facilisis sem. Nullam nec mi et neque pharetra sollicitudin. Praesent imperdiet mi nec ante. Donec ullamcorper, felis non sodales commodo, lectus velit ultrices augue, a dignissim nibh lectus placerat pede. Vivamus nunc nunc, molestie ut, ultricies vel, semper in, velit. Ut porttitor. Praesent in sapien. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Duis fringilla tristique neque. Sed interdum libero ut metus. Pellentesque placerat. Nam rutrum augue a leo. Morbi sed elit sit amet ante lobortis sollicitudin. Praesent blandit blandit mauris. Praesent lectus tellus, aliquet aliquam, luctus a, egestas a, turpis. Mauris lacinia lorem sit amet ipsum. Nunc quis urna dictum turpis accumsan semper.**

I. Introduction

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Etiam lobortis facilisis sem. Nullam nec mi et neque pharetra sollicitudin. Praesent imperdiet mi nec ante. Donec ullamcorper, felis non sodales commodo, lectus velit ultrices augue, a dignissim nibh lectus placerat pede. Vivamus nunc nunc, molestie ut, ultricies vel, semper in, velit. Ut porttitor. Praesent in sapien. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Duis fringilla tristique neque. Sed interdum libero ut metus. Pellentesque placerat. Nam rutrum augue a leo. Morbi sed elit sit amet ante lobortis sollicitudin. Praesent blandit blandit mauris. Praesent lectus tellus, aliquet aliquam, luctus a, egestas a, turpis. Mauris lacinia lorem sit amet ipsum. Nunc quis urna dictum turpis accumsan semper.

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 electronical 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 electronical 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 forseeable 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.

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 sensitve 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 information 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 26 billion units and it will generate incremental revenue exceeding $300 billion. [5]

These figures make it a very lucrative target for hackers. 26 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. However, a study on security in IoT devices and the unsolved issue how to patch IoT devices show a different image.

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
- webcam
- home thermostat
- remote power outlet
- sprinkler controller
- hub for controlling muliple 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 webcam might gives 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 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.

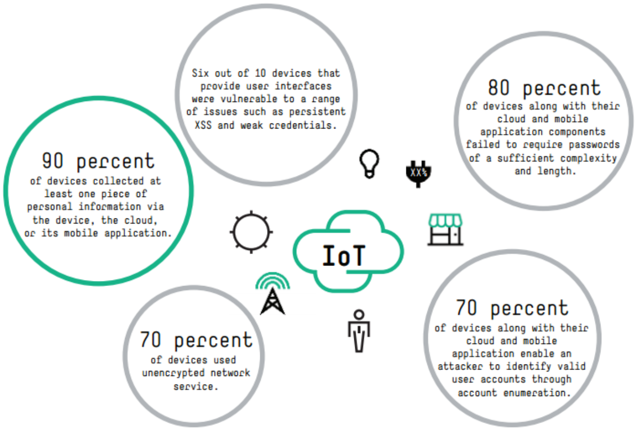

Six out of 10 devices that provide user interfaces were vulnerable to a range of issues such as persistent XSS and weak credentials.
80 percent of devices along with their cloud and mobile application components failed to require passwords of a sufficient complexity and length.
90 percent of devices collected at least one piece of personal information via the device, the cloud, or its mobile application.
XX%
IoT
70 percent of devices used unencrypted network service.
70 percent of devices along with their cloud and mobile application enable an attacker to identify valid user accounts through account enumeration.

Fig. 1. HP study results

Figure 1 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.

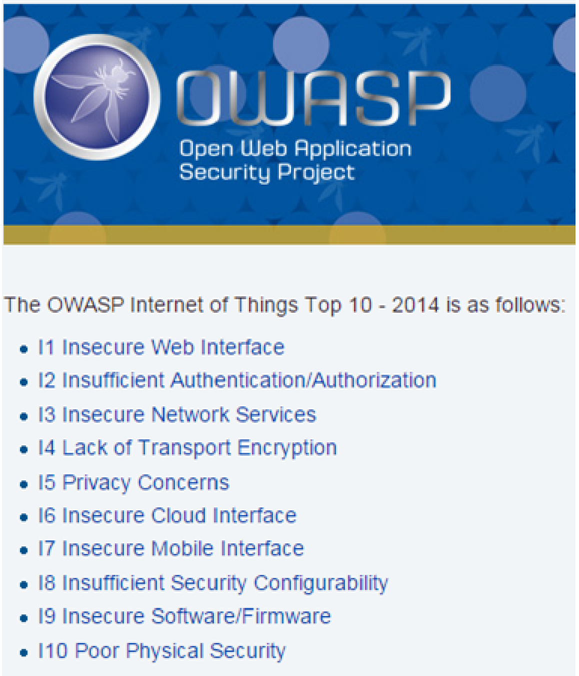
B. *OWASP Top 10*

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

Among these projects OWASP publishes a list of the top 10 security flaws in the iot. it lists the most common errors done about security ordered by their frequency of occurence. The list can be seen in figure.

with this list OWASP wnats to give developers a guideline which security issues are common and how they should be handled. To every of the top 10 security flaws a detailed page can be found 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 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



The OWASP Internet of Things Top 10 - 2014 is as follows:

- I1 Insecure Web Interface
- I2 Insufficient Authentication/Authorization
- I3 Insecure Network Services
- I4 Lack of Transport Encryption
- I5 Privacy Concerns
- I6 Insecure Cloud Interface
- I7 Insecure Mobile Interface
- I8 Insufficient Security Configurability
- I9 Insecure Software/Firmware
- I10 Poor Physical Security

Fig. 2. The OWASP Internet of Things Top 10

to the points of the top 10 list this study found that many of the devices tested had an insecure web interface, did not encrypt their network traffic and insufficient security configurability which means amongst other things that a sufficient password policy is missing. so as these points are also mentioned in this top 10 list is another indicator that results of the study are accurate.

insufficient authentication/authorization -¿ ct S.90, Abschnitt Typische Fehler vermeiden

insecure network services -¿ unsichere network services with security flaws -¿ ct S.90, Abschnitt Typische Fehler vermeiden

privacy concerns? -¿ ct S.90, Abschnitt Typische Fehler vermeiden

punkt 9/10 -¿ ct S.90, Abschnitt Typische Fehler vermeiden

analyzing this list; kommentar zu der liste, einfache oben, schwere unten -¿ underlines not a lot of care is taken about security in iot

erwhnen in Einleitung

C. Patching problems

Security updates are an important means to fix security 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 pratice 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 exmaple 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 untackled patching problems remain unsolved in many business areas of the IoT.

IV. Conclusion

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Etiam lobortis facilisis sem. Nullam nec mi et neque pharetra sollicitudin. Praesent imperdiet mi nec ante. Donec ullamcorper, felis non sodales commodo, lectus velit ultrices augue, a dignissim nibh lectus placerat pede. Vivamus nunc nunc, molestie ut, ultricies vel, semper in, velit. Ut porttitor. Praesent in sapien. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Duis fringilla tristique neque. Sed interdum libero ut metus. Pellentesque placerat. Nam rutrum augue a leo. Morbi sed elit sit amet ante lobortis sollicitudin. Praesent blandit blandit mauris. Praesent lectus tellus, aliquet aliquam, luctus a, egestas a, turpis. Mauris lacinia lorem sit amet ipsum. Nunc quis urna dictum turpis accumsan semper.

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.