Internet of Things Hacking

Simon Carlsson and Max Näf

***Abstract*—As the Internet of Things is gaining more traction in the market, people are becoming more comfortable with having their daily equipment connected to the internet, fewer are taking the security aspect seriously. By attempting an attack on the Telia Sense, an IoT device connected to a car, it is shown how an attacker could try to compromise this type of system and how developers and engineers in the field can test their devices. Information from the device was obtained, including debug information and program code. Telia Sense was found to be a well secured device with a lot of thought and consideration given towards cyber security, therefore a successful attack was not able to be performed. However, the methods and procedures described in this paper are still valid and does aid in securing a device.**

I. Introduction

TODAY smart devices are at high demand, Internet of Things (IoT), is one of the most popular buzzwords in the tech industry and with the launch of 5G approaching, IoT devices will only become more common. These new types of devices bring a promise of a better-connected future, with benefits never before possible. Ericsson estimates that 5G internet will hit the market in 2020 [1], but already there is a big market for IoT-devices. However, with an ever-growing market of smart, connected devices comes the question of cyber security. How safe are these devices? And is it possible to compromise an IoT device remotely to obtain user data or to gain control over the device?

In this paper, we aim to illustrate how the security of IoT devices can be examined and tested for by attempting to compromise a specific IoT system. This device promises to "Enhance your car". It is marketed for older cars, and aims to bring smart functionality to cars which previously had none. The device can provide the user with information about the car, such as: current position through GPS, driving data and even car service information. All of which can be viewed at any time by the user via a mobile application. However, connecting the cars internal network to the internet can pose a big problem if it were to be compromised. The car manufacturers had a mindset that you had to be physically connected to the car to manipulate it. It was not designed to be accessed via these kinds of devices. This results in the internal car network being quite exposed [2].

II. Background

A. The Smart Citys Cybersecurity

In this project, one aspect of the Smart City's Security is in focus, Cybersecurity. The market is pushing more and more connected devices in to our everyday life, smart- locks, lights and cars are only a few examples. With the constant expanding market, only limited by the imagination of developers. We as a society have built an infrastructure dependent on a stable internet connection and electricity. There are a lot of interesting topics and discussion to be made about this, in this paper, the focus is at IoT-devices, designed as a complement to older equipment and how they interact and handles safety in the smart city. One of these devices is Telia Sense.

B. Telia Sense

The Telia Sense is a device developed by ZTE as the VM6200S and marketed by Telia in Sweden, see figure 1. The same platform is sold in the USA and marketed by T-Mobile, an American mobile carrier, as the SyncUP DRIVE [3]. It is described as a way to modernize your car. The device is interesting since it connects directly to the cars internal network via the On-Board Diagnostics (OBD) port, and through its internet connection it is potentially accessible from the entire world. The device is part of a payed service with a bundled mobile data plan and mobile application. The device is marketed to the average consumer wanting more information about their car and also to gain 4G internet connection within the car. Possible tools to breach or secure this device could give a valuable lesson for future development of similar IoT products.

Fig. 1. The ZTE VM6200S, Telia Sense [4].

In order to attack, and or test the device for safety issues, the attack vantage point needs to be established. In the industry, it is common to categorize this vantage point into two categories, white box- and black box perspective.

C. White box Perspective

If the target device is known to the attacker i.e. the attacker has access to the source code, schematics, encryption keys, etc. This is known as a "White box perspective". This is typically the perspective a security tester at the manufacturer would have. By knowing everything about the device, the security of it can be very easily tested, and potential entry points in the software can be quickly spotted and taken care of. In addition, there are also multiple tools developed around white box security testing which can display potential security flaws and their likelihood of being exploited.

D. Black box Perspective

If the target device is not known to the attacker, i.e. the attacker has limited information about the device. Then it is known as the "black box perspective". This would typically be the case for a conventional hacker and is how this project sees its target. Working with a black box perspective poses a lot of challenges for the attacker. Since nothing is known, everything needs to be investigated and penetration tested in order to find potential vulnerabilities.

E. CAN

Modern cars use an internal network standard called Controller Area Network (CAN) [5]. The CAN bus was created by Bosch and introduced to the general consumers around 1990. The CAN network exists in two different versions, CAN A (11-bit) and CAN B (29-bit) [6]. The CAN transceiver system have migrated from cars to an increasing number of products, including railways, airplanes and medical equipment, and is a standard when using multiple transceivers. This network often consists of multiple independent agents communicating at the same time but with set rules for which one gets to transmit over the network and which to listen. It enables fast and stable communications, but relies heavily on that only the desired transceivers are connected to the network. Therefore, the manufacturers implementing the CAN network had no intention of allowing external third-party devices to be connected.

F. Threat Model

To be able to focus resources and time at the correct weaknesses in the system, a threat model is usually constructed. This model has two main benefits. For a black box perspective, it provides a better understanding of the device and the different functions connected to it. Also, it serves as a checklist for the attacker, and can help priorities possible vulnerabilities. For a developer in the white box perspective, the threat model can provide valuable information of possible threats that might have been overlooked. There are even possibilities to model a device or piece of software for security issues. One of these modelling tools is the Microsoft Threat Model Tool [7]. This gives the user a list of identified threats between the different connection points and also classifies weaknesses and which attacks are possible. This tool is marketed for software developers programming for Microsoft platforms, but it can still be useful for other projects.

G. Testing and Report

The last step is to test the identified safety issues, here the threat model is used to make sure that important vulnerabilities have been tested for. This is highly dependent on the type of attack surface. A penetration test might be software injections in servers, reading data from chips and interfering communications to and from the device. Often, a combination of these are required for an actual attack. For example, information about a device's hardware might be needed to implement a software attack.

III. Threat Modelling

The simplified threat model map for the Telia Sense can be seen in figure 2. The complete threat model image was made in the Microsoft Threat model tool and can be seen under Appendix. The different parts of the model is explained in an enumerated list, with numbers correlating to the numbers in figure 2.

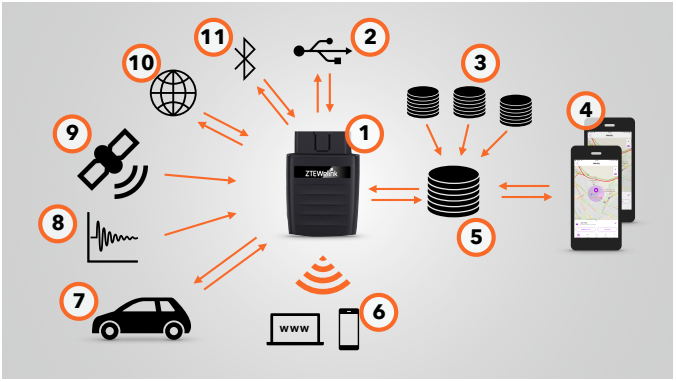

Fig. 2. Simplified threat model

This map shows how the Telia Sense communicates between the server, the car and its sensors and radios. All of which can be an interesting attack surface. Information was gained through general usage, Telias Website [8], information from ZTE [4] and third-party services [9]. This follows the methods introduced by Aaron Guzman and Aditya Gupta [10].

1) Telia Sense. This is the main device in this network.

2) The micro USB port. This can be seen in the promotional videos for the T-Mobile variant of the VM6200S [3]. This is a standard connection to a computer, likely used when servicing the unit. Therefore, the port could be closed for entrance, or it could possibly require specific drivers.

3) Secondary server. The Telia Sense communicates to other servers as well, including the connection to Trafikverket, where information about registered cars in Sweden is stored. This is likely a one-way communication, that is used at the registration of a new car in the application. There exist other services as well, including connection to the "Folksam drive safe" service, that rewards the user with better insurance. It is most likely that this is a one-way communication through the server.

4) The mobile application. The application communicates directly to the servers owned by Springworks [11], an affiliated company of Telia. Information is likely encoded using the https protocol, keeping information safe. The user of the application can change a few parameters, such as the router SSID and password.

5) Main server. Between the Telia Sense and the mobile application lies a server. The server processes the

information from the unit and stores it for all the users of that device. The data is likely to be transmitted at least by IPv4 standards.

6) The Car. This is the main target, directly connected via an OBD port, to the Telia sense.

7) Device sensors. The Telia Sense has a couple of sensors, including an accelerometer with a gyroscope that measures hard breaks and or when something collides with the car.

8) The GPS connection. It is probably used to send direct information about the unit's position. It can also be part of measuring the cars velocity, instead of reading it from the car. The GPS standard is developed by the United States military and spoofing by foreign nation have been speculated. The data is sent via circularly polarized EM-waves at 1575.42 MHz & 1227.6 MHz frequency [12].

9) The Wi-Fi router. The Wi-Fi router is a very interesting access point in the device, often protected by a password. However, IP addresses can be exploited as seen in previous cases of car hacking [13]. After gaining interesting IP addresses and passwords, entrance could be made via a computer from all around the world.

10) The internet connection. In this case Telia is the internet provider that also sells the unit in the name Telia Sense. In most cases this is a 4G LTE connection (in Sweden 83.65% is covered by LTE network) [14], this is a highly secure network and often comes encrypted with multiple keys around 128-bit in length [15].

11) The Bluetooth connection. The unit has Bluetooth possibility and it is stated to be a possible connection point. For Bluetooth 4.0 (present in the VM6200S), a P-192 Elliptic Curve function is used for generating the link key between the devices. Since the device lacks the possibility to enter a pin code, it is likely to use the "Just Work" protocol of Bluetooth [16].

IV. Identification of Vulnerabilities

With multiple connection points comes potentially multiple attack surfaces. It might only take one vulnerability in order to compromise the entire system. Therefore, it is important to consider all possible vulnerabilities.

A. Software Vulnerabilities

With IoT devices comes usually proprietary software, in the form of servers, web interfaces and mobile applications. These different types of software can all have their respective weaknesses and possible attack surfaces. By identifying what is used by that particular IoT device, and how the information is exchanged, the attacker can interfere transmissions and possibly modify or read the data sent. By looking at what data is transmitted between the server, the Telia Sense and the application. A proxy can be used to read data transmitted and also probably manipulate values. Bluetooth can also be a way to transmit malicious messages and possibly take control of the device. The attacker would need to breach the password to connect, but after that there could be a lot of possibilities, since these types of attacks have been seen to be very effective before [17].

B. Hardware Vulnerabilities

Sometimes it is not enough just to attack the system remotely. It might be to many unknown parameters, such as encryption keys, passwords or IP addresses. It is common to store this type of information inside the device's program memory. Therefore, manufacturers usually design in several ways to prevent attackers from getting to this information. For instance: It is possible to read the program memory of a microcontroller, this is usually done via a Joint Test Action Group (JTAG) programmer/reader [18]. However, there is an option to disable the JTAG line completely. This is a so-called fuse and cannot be reset, preventing the attacker from reading the memory.

Although the entirety of the program memory might be blocked, there might still be other ways for an attacker to compromise the hardware. By analyzing data flow inside the unit, other memory locations might be found which are unprotected.

V. Main Critical Points

By analyzing the threat model and the unit through disassembling, a better understanding of the unit was gained and the devices vulnerabilities could be categorized using the STRIDE system [10]. Some attack surfaces have been chosen as the main weaknesses, and are then scored using the DREAD threat scoring system [10]. These paths would be the final way an attack could be performed. However, information needed to execute the attack may be extracted through other exploits such as the software or hardware vulnerabilities mentioned previously.

A. STRIDE

Here the different threats are classified into categories for better understanding of how different weaknesses could affect the device.

Spoofing of user identity

- *By claiming to be admin, an attacker can gain access to the router network through an IP address.*
- *Getting access to the device by acting as the host server.*
- *Open access to Bluetooth by cracking password, ECC key.*

Tampering

- *Read data sent on the CAN network.*
- *Read data sent from the processor.*

– *Set up proxy to read data between the mobile Application and the server.*

Repudiation

– *Enable data transmission via USB.*

Information Disclosure

– *Use a proxy to read information sent via the Application to server.*
– *Read sent and received data between device and server.*
– *Read data sent on the device directly by probing.*

Denial of Service

– *Overload CAN network and disable other communication between transceivers.*

Elevation of Privilege

– *Get admin privileges by finding relevant data in the code.*

B. DREAD

The DREAD system helps in scoring the different suspected vulnerabilities:

Damage potential: How great is the damage if exploited?
Reproducibility: How easy is it to reproduce the attack?
Exploitability: How easy is it to perform the attack?
Affected users: How many users are affected?
Discoverability: How easy is it to find the vulnerability?

The DREAD model has a risk rating system from 1-3. where 1 is a low risk, 2 is medium and 3 is a high risk.

Execute CAN commands sent via the local Wi-Fi hotspot.

Damage potential: 3
The ability to send commands over the hotspot would enable arbitrary commands to be sent over the CAN network.
Reproducibility: 2
If one gain access through the hotspot it is highly likely that all other units will have the same weakness.
Exploitability: 2
This requires a lot of knowledge about IP hacking, but it will probably be manageable by someone with moderate knowledge.
Affected users: 3
This affects all devices sold under the name Telia Sense or perhaps all VM6200S units.
Discoverability: 2
The method of getting access to IP addresses are well known, but how to use this to manipulate the processor is not well documented.

Dread score: 12

Note this is in the case of a hacker in the proximity of the router Wi-Fi, in the case with a hacker exploiting a device thought an Android phone the R, E, A is scaled down to 1 due to the extra steps and smaller install base and change the Dread score to 8.

Send information by acting as the host server.

Damage potential: 3
By acting as the host server, the attacker could tell the unit that new CAN-commands are available for the car. This means that for example an arbitrary command can be loaded instead of the "check engine" command.
Reproducibility: 2
Since all the devices connect to the server in a similar way, hacking one would make it possible to hack multiple. However, depending on how messages are sent it is not possible to state that all could be controlled simultaneously.
Exploitability: 1
Acting as the server in of its self is a difficult task. Then, getting the unit to talk to a computer instead of the real server when both are live at the same time is a big challenge.
Affected users: 3
Since all devices communicate to the same server, acting as this server would apply to all units.
Discoverability: 1
Working from a "black box" perspective, very little of the actual server and what it would take to mimic it is known. It might be very difficult to take over the communication to the real server.

Dread score: 10

Modify data sent from the application.

Damage potential: 1
Since the web server probably has a white list of what commands can and cannot be sent the damage potential will be quite low. If the server doesn't have such a function the damage potential could be huge.
Reproducibility: 2
Since the server is always active and ready to receive commands, uploading and receiving commands can be done whenever. One might need to know the user-ID and password for each attack scenario.
Exploitability: 1
Since the server needs to validate the user, one probably would need to know the user-ID and password in order to communicate with the server.
Affected users: 3
All users are connected to the same servers which implies that all users are exposed to the threat. At least for the Telia Sense service.
Discoverability: 1
Since the communication between the application and the server are very limited, there is very little information to be modified.

Dread score: 8

Direct connection via Bluetooth.

Damage potential: 2

If connection and control are given via Bluetooth a close proximity attack could be likely.
Reproducibility: 1
The Bluetooth connection is not active by default, it must be activated by third-party services.
Exploitability: 2
The encryption system for Bluetooth is known, (ECC for 4.1), and also there is a lack of confirmation on the device so it will probably use the "Just Work" authentication.
Affected users: 1
It is not likely that the devices will have a activated Bluetooth connection and if not it will have to be started by the user in some way.
Discoverability: 1
The ECC encryption needs to be broken, which is very difficult.

Dread score: 7

VI. Penetration Testing and Results

When the device's functionality has been thoroughly mapped and ranked, it is time to test the highest risk vulnerabilities.

A. Test Platform

A test platform was made to enable easy manipulation of JTAG, UART and Flash memory. The platform contains connectors to the CPU that enables fast and sturdy connection for the different protocol wires. With this platform, reading data with the unit plugged in to a car is possible. The platform made it easier for testing and reading various transmissions of data. The platform can be seen in figure 3.

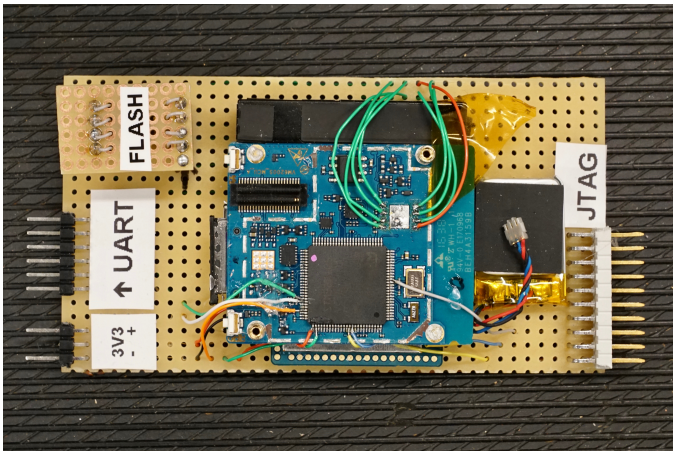

Fig. 3. Here the test platform is showed with the top PCB removed to expose the soldered-on connections.

B. Direct Device Communication

The direct communication is any communication directly to the unit.

1) Communication Between Device and Server: The most interesting part of the Telia Sense Application is its communication to the server. This is the main way information gets sent to and from the device, and it is also via this connection information from the car is transferred. One big possibility for an attack is the CAN command the application sends to read information from the car, e.g. battery voltage. If another command could be sent instead, there would be a direct way to control the car, and a fairly easy exploit. By using the software OWASP ZAP [19], it was possible to set up a proxy. Then, by installing a certificate on an Android phone, it was possible to read the communication between the server and the Android application for the Telia Sense. This included communication to the "Machine to Human server" (M2H), hosted by Springworks. In figure 4, one "get request" from the application is shown.

```
PATCH https://users.machinetohuman.com/v1--
    HTTP/1.1
X-M2H-OS-Type: Android
X-M2H-OS-Version: 4.4.2
X-M2H-Client-Version: 1.29.6016
X-M2H-Model-Manufacturer: samsung
X-M2H-Model-Name: mondrianwifixx
X-M2H-Partner: Telia
X-M2H-Market: telia-se
Authorization: Bearer
    eyJhbGciO--6IkpXVCJ9-z-4g
Accept-Language: sv
Content-Type: application/json; charset=UTF-8
Content-Length: 24
Connection: Keep-Alive
User-Agent: okhttp/3.6.0
Host: users.machinetohuman.com
```

Fig. 4. OWASP ZAP, get request to the M2H server. I.e. the Android application is requesting data from the server Machine to Human. A response followed, which is non important. This figure only aims to convey a general idea of the communicationl.

Unfortunately, no direct CAN messages was sent and only Wi-Fi router names and passwords was actually possible to type in and send. The proxy made it possible to change some values, like the Wi-Fi standby timer, and they were visible in the UART study (discussed later). However, the device did not accept arbitrary characters and or arbitrary lengths. Therefore, we can conclude, information is passing through the server, but it does not really affect the device in any meaningful way.

2) Reading of CAN Port: By connecting the direct CAN output pins, CAN High (6) and CAN Low (14), on the Telia Sense OBD port shown in figure 5, to an oscilloscope. Readings was possible to extract from the device. This is evidence that the car do receive direct commands from the device and if they where to be tampered with one could probably control or interfere the car. However, to actually read the message is difficult as cars uses different commands for the same function. Information can however be decoded, but that is outside the scope of this paper. This confirms the threat model CAN communication and enables hacking of the car.

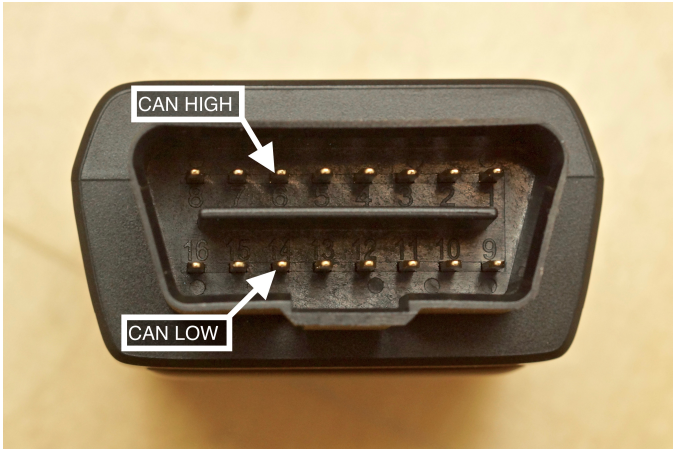

Fig. 5. Telia Sense standard OBD-II port with the two pins of the CAN bus highlighted.

3) Port Scanning: By reading the UART and flash memory, strings referring to IP addresses was found. The IP addresses are of private IPv4 type, they have a Machine to Machine (M2M) tag and was not possible to ping or access by a computer. These were scanned for open ports using Nmap. The command "nmap -T4 -A -v -Pn" was used to scan the first 1000 ports. The scan showed the highest level of security and no open ports. The Nmap showed interesting connections between the hard-coded messages and the one appearing when booting. The topology is showed in figure 6 and is done from the Wi-Fi hotspot generated by the Telia Sense to minimize the risk of being stopped by internal security such as firewalls. In Nmap, the service was categorized as having less than one open port. And thus rated as very secure.

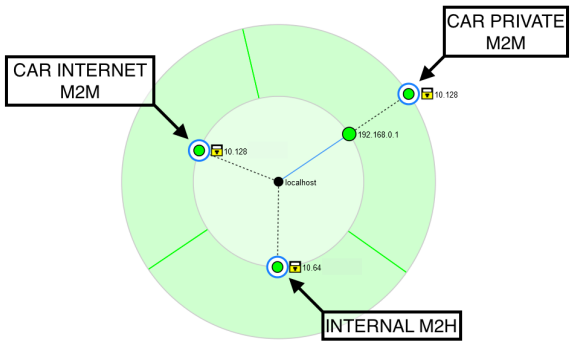

Fig. 6. Topology of the Nmap scan from the hotspot to the three servers. Hotspot (localhost) in the center and then the three servers.

4) Bluetooth Connection: Hardware exposing and distributor pages shows that there exists a Bluetooth antenna inside the device. Testing showed that this connection is most likely hidden and or turned off since it could not be found by any devices. There exists an extra payed service where the user connects a small device to the Telia Sense that warns the driver if the local speed limit is broken. This device could activate the Bluetooth and possible provide an access point. This was not tested since it requires the service to be coupled with personal insurance information. There are other ways to find hidden Bluetooth networks as describes in [20]. However, articles regarding finding a hidden Bluetooth examines older versions of Bluetooth.

5) JTAG Readings: By using the datasheet for the processor [21], the JTAG port was located. In order to communicate with the processor, signal wires were soldered on to the chip. These wires were then connected to a Segger J-Link [18]. In theory if the ports were active this could be a way to extract program code, passwords and possibly also write code to the processor [22]. However as previously mentioned, it is common practice to close the JTAG port in an end use product to prevent tampering and access by unauthorized users. For the Telia Sense, the JTAG protection was engaged thus preventing this attack.

6) UART Readings: By using the datasheet for the processor, the UART port was found. Similarly, to the JTAG readings, wires were soldered to the processor. There are several UART connections on the board, one was identified as a debug console. These types of debug consoles can provide very helpful information about the device in real time. The read was successful and the information could be read at a baud rate of 115200 baud. The extracted information gave more insight in how the device actually worked, also there existed messages to the server, one example is seen in figure 7. However, these messages were encrypted and were not possible to be decrypted, since the key and receiving system was unknown. Fortunately, other types of information were able to be extracted, like the three different IP-addresses that connected to the device, clear text communication for Wi-Fi passwords and username as well as the current/last known GPS location. However, this was strictly a print console, and no information were able to be sent to the device. This helped to strengthen the understanding for the product and validate our threat model. Especially the IP addresses was made to attempt hacking the Wi-Fi environment.

C. Hardware Exploits

The Telia Sense device is also equipped with hardware that can be manipulated in a few ways. These could be used to reach main functions and possibly internal files.

1) Micro USB port: A Micro USB port was found underneath the plastic cover, see figure 8. It was not mentioned by Telia, but it is shown on the T-Mobile variant of the VM6200S. Attempts to reach files or information via USB was made using both a Windows and a Mac computer. However, the device did not appear connectable without proper drives. Information about the device was extracted by using the Windows USB analyzing tool, USBview, developed by Microsoft for analyzing USB ports [23]. This program stated that it should be user connectable but not debug capable as seen in figure 9.

```
* send pack frame features:
* type: 3
* frame no: 14h
* effective data length: 8
   * msg total length: 61
      * msg data type: 0403
         * time: 486581
*/
before enc data:(L=32)<58 AB 22 AF 4D 33 24
    B7 03 00 14 00 08 04 03 5A 97 E9 E9 77 05
    F1 97 0B 97 43 96 94 A4 29 94 4A >

CBC iv: (L=8)<A0 25 3B 2A 0E 58 24 15 >

after enc data:(L=32)<DC B1 0A 45 94 85 59 10
    EC 46 22 8A A8 AA DA 8C EF B2 73 C0 1F 25
    5F B2 11 F8 59 42 5B 91 22 29 >

****processing has receives the data
    frame......
```

Fig. 7. UART dump with AES encrypted (CBC) communication to the server.

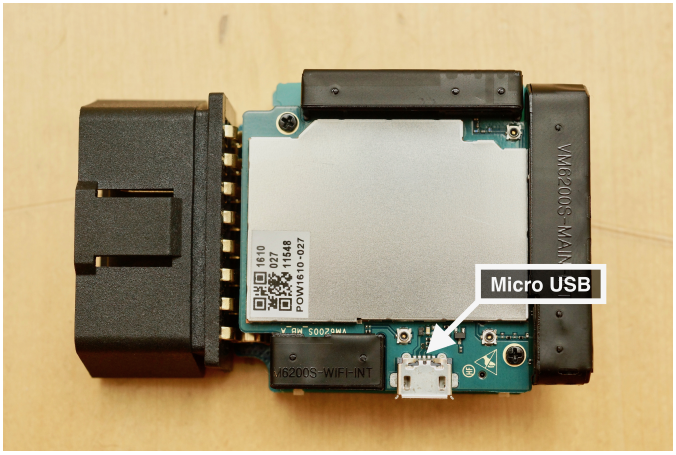

Fig. 8. One of 3 PCB's inside the Telia Sense showing the hidden USB port.

2) Flash Memory: When inspecting the Printed Circuit Boards (PCBs), it was found that the processor's boot mode was set to external boot. The boot memory was identified as a 2 MB Macronix flash memory [24]. This meant, by reading the flash memory contents, one could extract the firmware directly. This was later done by de-soldering the chip and reading its contents with a universal programmer/reader, TL866CS. In order to make the output file more readable, it was translated into ASCII. Here, hard coded numbers and values along with text strings could be read directly. These types of data can provide very useful information about the device, especially if the manufacturer has hard coded a password or an encryption key. In this instance, no passwords or keys was found, but the servers IP address was possible to read. By changing this IP address to something else, the communication to the server could potentially be piped through a computer and read directly, which might expose a new attack surface. Apart from what mentioned above, not a lot of information can be extracted from the firmware without decompiling it. This

```
[Port2] : USB-enhet (sammansatt)

Is Port User Connectable: yes
Is Port Debug Capable:    no
Companion Port Number:    11
Companion Hub Symbolic Link
    Name:USB#ROOT_HUB30#4&19393024&0&0#
{f18a0e88-c30c-11d0-8815-00a0c906bed8}
Protocols Supported:
 USB 1.1:                 yes
 USB 2.0:                 yes
 USB 3.0:                 no

Device Power State:       PowerDeviceD0

     ------>Device Information<------
English product name: ''ZTE Technologies MSM''

ConnectionStatus:
Current Config Value:     0x01 -> Device Bus
    Speed: High (is not SuperSpeed or higher
    capable)
Device Address:           0x09
Open Pipes:                 3
```

Fig. 9. Information about the USB connection extracted by USBview.

gives the hacker the ability to read the source code. Due to the compiling process, a lot of information is lost and the resulting code is far from readable, and next to useless unless the attacker knows exactly what to look for.

VII. Conclusion

We have shown how IoT devices work from a cyber security point of view. In addition we have shown were these type of devices may have weaknesses and how one can go about testing for them. The fact that we did not succeed in an attack on the Telia Sense, maybe has less to do with our methods being bad, and more to do with the Telia Sense being a well made IoT device, with cyber security in mind throughout the entire system.

VIII. Discussion

The initial assumption was that the Telia Sense was a fairly secured device with a few overlooked safety issues. However, after first deconstruction, it was clear that the device was professionally built with quality and high value components. Test after test showed that the device was more secure than initially thought. Especially the fact that UART readings showed encrypted messages to the server and no seemingly hidden passwords was to be found reading through the translated binary file from the flash memory. The locking of the JTAG port together with hidden and turned off Bluetooth, and inactive USB port greatly hinders intruders and raises the bar for hacking the device.

We are not professional hackers, nor safety tester with experience in the field. Hence we might have missed a couple of safety issues. When reading the FLASH memory, a lot of information was gained. We made the conclusion that we did

not obtain any more information about the device that would of aided in hacking it. But this may fall as being false, since there might be information that we overlooked. This is true for all of our testing, were somethings may have been overlooked. However, that does not change the conclusion of this report. We believe that almost any system may be hacked, the question is only how difficult. Hacking the Telia Sense is still not a task for a novice attacker.

The term hacking is one of the more interesting parts of this project. It is a word loaded with a lot of assumptions, negativity and stigma. Hacking could be lots of different things, spanning from government programs attacking infrastructure, self-employed hackers trying to find vulnerabilities in bigger companies or an interested customer trying to figure out how to gain more of their new product. The course "Ethical Hacking" has been introduced to KTH this last year and have gained immense publicity and interest. This is a first great step to reshape the image of the hacker and establish a safer software environment for the future. The next important step is to form a better regulation of what is legal and what is not. Arguments can be made that the customer can manipulate their own product at will. But there are also counter arguments, that it disturbs patents, user agreements and introduces new potential attack surfaces. If we want to investigate the security of a given system by attempting to hack it, we must do so without harming the system and or tampering with others property, such as another users data. And any findings should be reported before published, so as no one can take advantage of the security flaws found.

A. ZTE and their status today

At the time of writing this report, multiple news about ZTE and the suspicion of them extracting user data and leaving backdoors in the user's devices is circulating. ZTE is based in Shenzhen, China and multiple American internet providers are now in the process of removing their devices from the American market. Finding something to strengthen this accusation could be a huge breakthrough, especially in such a heavily connected device as the ZTE VM6200S [25].

B. Future work

For future projects, there now exist a test platform. Information have been extracted in the form of a Flash memory and UART readings. This Flash can easily be unmounted and rewritten, and new data can be read. The JTAG port could be examined again with a different method. There also exist Bluetooth that could be activated by using the Folksam drive safe add-on. Also, there could be more experiments by writing the driver for the USB and enable access that way. However, there would probably be more interesting to look at another device such as the ELM327, this comes in different configurations but is easier to access and already have connection via multiple mobile applications.

ACKNOWLEDGMENT

Special thanks goes to our supervisor, Professor Pontus Johnson. He has pushed us to greater lengths, to challenge the limits of our knowledge and supported us in our overwhelming task to ensure a safer future for us all.

REFERENCES

[1] Ericsson. (2018, feb) 5G open for business. Ericsson, Stockholm, Sweden. [Online]. Available: https://www.ericsson.com/en/5g
[2] M. Schellekens, "Car hacking: Navigating the regulatory landscape," *Computer Law & Security Review*, vol. 32, no. 2, pp. 307–315, 2016.
[3] T-Mobile. (2018, Apr) SyncUP DRIVE. Bellevue, Washington, USA. [Online]. Available: https://www.t-mobile.com/offers/syncup
[4] Z. Corporation. (2018, Apr) VM6200S, 4G OBD Device. Shenzhen, China. [Online]. Available: http://www2.ztewelink.com/en/products/telematics/20161226/138192.html
[5] S. Corrigan. (2016) Introduction to the Controller Area Network (CAN). Dallas, Texas, USA. [Online]. Available: http://www.ti.com/lit/an/sloa101b/sloa101b.pdf
[6] R. I. Davis, A. Burns, R. J. Bril, and J. J. Lukkien, "Controller area network (can) schedulability analysis: Refuted, revisited and revised," *Real-Time Systems*, vol. 35, no. 3, pp. 239–272, 2007.
[7] Microsoft. (2018, Apr) Microsoft Threat Modeling Tool. Redmond, Washington, USA. [Online]. Available: https://docs.microsoft.com/en-us/azure/security/azure-security-threat-modeling-tool
[8] Telia. (2018, Apr) Telia Sense. Box 50077, 973 22 Lule, Sweden. [Online]. Available: https://www.telia.se/privat/bredband/tjanster/teliasense
[9] Gurtam. (2018, Apr) ZTEWelink VM6200S. 220140, Minsk, Belarus. [Online]. Available: https://gurtam.com/en/gps-hardware/auto/ztewelink-vm6200s#parameters
[10] A. Guzman and A. Gupta, *"IoT Penetration Testing Cookbook"*. Birmingham, UK: Packt Publishing Ltd., 2017.
[11] Springworks. (2018, Apr) Springworks Spark. Sveavägen 52, 111 34 Stockholm, Sweden. [Online]. Available: https://www.springworks.se
[12] F. A. A. Department of Transportation. (2018, Apr) Global Positioning System Wide Area Augmentation System (WAAS) Performance Standard. DC, Washington, USA. [Online]. Available: https://www.gps.gov/technical/ps/2008-WAAS-performance-standard.pdf
[13] I. D. Foster, A. Prudhomme, K. Koscher, and S. Savage, "Fast and vulnerable: A story of telematic failures." in *WOOT*, 2015.
[14] OpenSignal. (2018, feb) The State of LTE. London, UK. [Online]. Available: https://opensignal.com/reports/2017/06/state-of-lte
[15] S. Banescu and S. Posea, "Security of 3g and lte," *Faculty of Computer Science, Eindhoven University of Technology*, 2011.
[16] J. Padgette, "Guide to bluetooth security," *NIST Special Publication*, vol. 800, pp. 13–17, 2017.
[17] C. Miller and C. Valasek, "Remote exploitation of an unaltered passenger vehicle," *Black Hat USA*, vol. 2015, 2015.
[18] Segger. (2018, Apr) J-Link EDU. 101 Suffolk Lane Gardner, MA 01440, USA. [Online]. Available: https://www.segger.com/products/debug-probes/j-link/models/j-link-edu/
[19] OWASP. (2018, Apr) OWASP Zed Attack Proxy Project. [Online]. Available: https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project
[20] D. Cross, J. Hoeckle, M. Lavine, J. Rubin, and K. Snow, "Detecting non-discoverable bluetooth devices," in *International Conference on Critical Infrastructure Protection*. Springer, 2007, pp. 281–293.
[21] STMicroelectronics. (2017) Stm32f105xx, stm32f107xx datasheet. Geneva, Switzerland. [Online]. Available: http://www.st.com/content/ccc/resource/technical/document/datasheet/e4/f3/1a/89/5a/02/46/ae/CD00220364.pdf/files/CD00220364.pdf/jcr:content/translations/en.CD00220364.pdf
[22] K. Rosenfeld and R. Karri, "Attacks and Defenses for JTAG," *IEEE Design & Test of Computers*, vol. 27, no. 1, 2010.
[23] Microsoft. (2018, Apr) USBView. Redmond, Washington, USA. [Online]. Available: https://docs.microsoft.com/en-us/windows-hardware/drivers/debugger/usbview
[24] Macronix. (2017, Nov) MX25L1606E Datasheet. No.16, Li-Hsin Road, Science Park, Hsin-chu, Taiwan, R.O.C. [Online]. Available: http://www.macronix.com/Lists/Datasheet/Attachments/6786/MX25L1606E,%203V,%2016Mb,%20v1.9.pdf/
[25] E. Rumney. (2018, Feb) Senators propose bill to block U.S. from using Huawei, ZTE equipment. London, United Kingdom. [Online]. Available: https://www.reuters.com/article/us-china-usa-telecoms/senators-propose-bill-to-block-u-s-from-using-huawei-zte-equipment-idUSKBN1FR35U

APPENDIX
THREAT MODEL

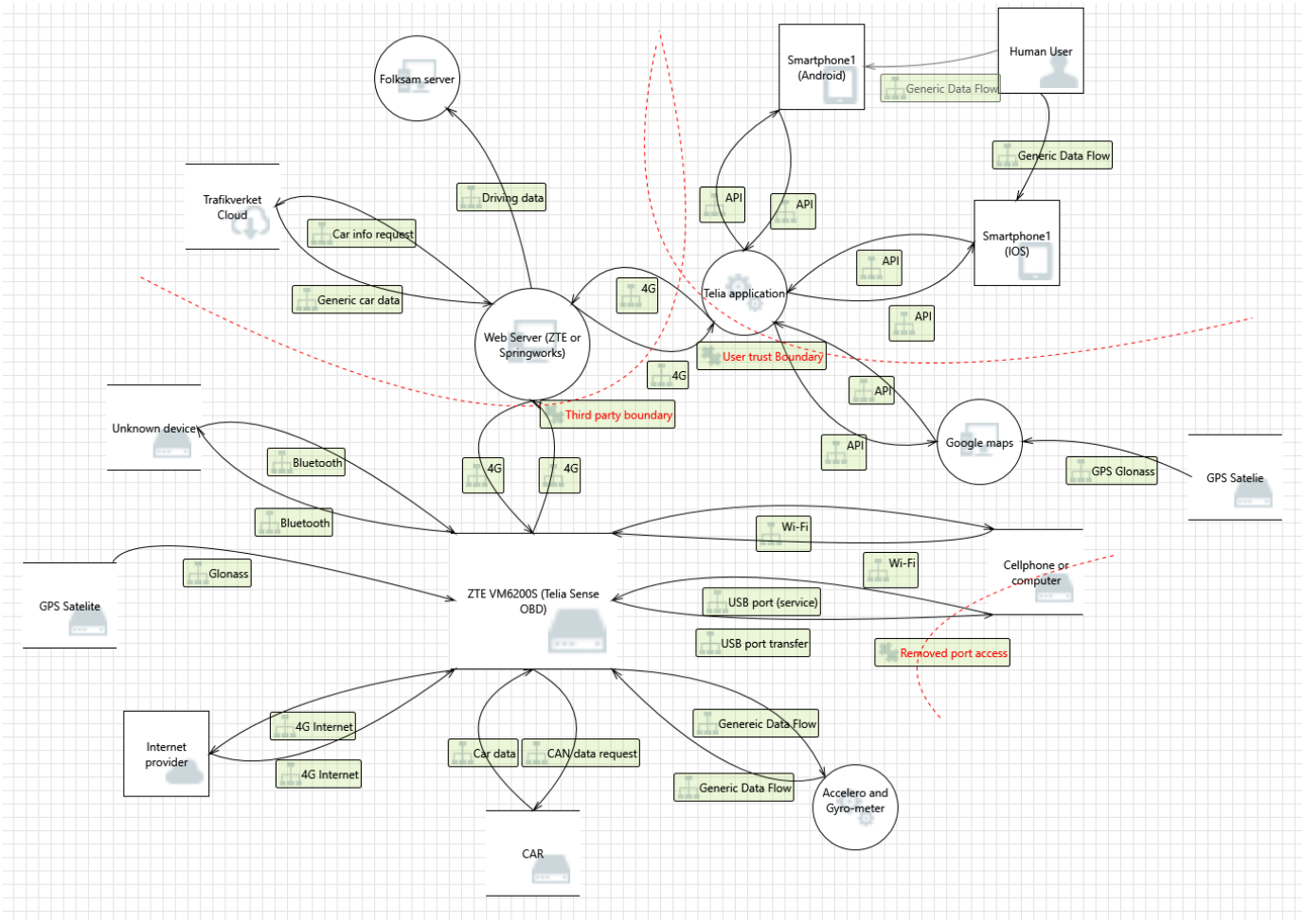

Fig. 10. The complete threat model for the Telia Sense