UNIVERSITY OF TARTU

Institute of Computer Science

Computer Science Curriculum

Jane Õunaid

Investigating the Effect of Replay Attacks on Popular Car Models in Estonia

Bachelor's thesis (9 ECTS)

Supervisor: Danielle Melissa Morgan, MSc

Tartu 2023

Investigating the Effect of Replay Attacks on Popular Car Models in Estonia

Abstract:

Hackers have found different ways to exploit the vulnerabilities in remote keyless entry systems used in cars. This paper aims to give an overview of some of the attacks and assess whether some of Estonia's most popular car models are vulnerable to various forms of replay attacks.

As a result, this thesis will give an overview of which of the cars were vulnerable to the experiment attacks and why other cars were not vulnerable. Even though all cars tested used rolling code to thwart replay attacks, most of the cars were still vulnerable.

Keywords:

SDR, GNU Radio, HackRF, URH, Replay attack

CERCS:

P175 Informatics, systems theory

T121 Signal processing

Taasesitusrünnete mõju uurimine Eestis populaarsete automudelite vastu

Lühikokkuvõte:

Häkkerid on leidnud erinevaid viise kuidas ära kasutada nõrkusi võtmeta kaugjuhtimispulti (ingl *Remote Keyless Entry,* RKE) kasutavaid auto lukustussüsteeme. Selle töö eesmärgiks on anda ülevaade mõnedest rünnetest, mida saab selliste lukustussüsteemide vastu ära kasutada. Teiseks eesmärgiks on hinnata, kas valik Eestis populaarsetest automudelitest on nõrgad erinevate taasesitusrünnete vastu.

Selle töö tulemuseks on ülevaade sellest, millised katsetes olnud autodest on väljavalitud rünnete vastu nõrgad ning miks teised autod ei reageeri nendele rünnetele. Kuigi kõik katsetes osalenud autod kasutasid koodiveeretust, olid enamus autod ikka kaitsmata taasesitusrünnete vastu.

Võtmesõnad:

SDR, GNU Radio, HackRF, URH, Taasesitusrünne

CERCS:

P175 Informaatika, süsteemiteooria

T121 Signaalitöötlus

Table of Contents

Introduction

When cars were first introduced to the general public, they did not have any safety measures to keep them from being stolen, as starting the car was a complicated procedure that required precise knowledge of the car itself [1]. As time went on, car manufacturers started implementing safety features that would assure the car's owner that their precious vehicle would not get stolen. Most of the locking systems that were introduced used a simple lock-and-key mechanism, until the 1980s, when remote keyless entry was introduced [2]. Remote keyless entry systems made it possible for car owners to open their car doors easier because they could just press a button on a remote instead of having to fumble with a key.

Remote keyless entry systems introduced new ways for thieves to access people's cars. If the car's key fob uses the same code with each button press, an attacker could record the signal and use it themselves. Some car manufacturers have started implementing rolling code, that changes with each button press to deter such attacks, but not all manufacturers have done this.

Since public knowledge of the threats against remote keyless entry systems is low and these types of attacks can lead to significant financial loss, more awareness should be brought to this topic.

This paper aims to give an overview of replay and similar keyless entry attacks and to determine if popular car models in Estonia are vulnerable to these attacks. There will be an overview of the hardware and software used for the experiments as well as an overview of other gadgets that can be used.

This thesis is divided into six parts. Chapter 1 is dedicated to frequently used terminology. Chapter 2 describes keyless entry systems and what kinds of attacks they are vulnerable to. Chapter 3 describes the experiments in detail, from how the cars were chosen to how to conduct these attacks. Chapter 4 gives an overview of the results of the experiments. Chapter 5 discusses how to prevent falling victim to replay attacks. Chapter 6 is the final chapter which concludes this paper.

Grammarly[1] was used in the paper to detect small grammatical mistakes such as wrong comma placements or misspelt words.

[1] https://www.grammarly.com/

1 Terminology

Café attack - a type of replay attack where an attacker records a signal from a victim outside the range of the car's receiver, guaranteeing that the recorded signal is unused. The unused signal can then be used to unlock the car doors.

Remote Keyless Entry (RKE) - a type of electronic lock. A Remote Keyless Entry System in cars has two components – a key fob to transmit a lock or unlock signal and the car's receiver that obeys the received command [3].

Replay attack - also known as a playback attack, is an attack where an attacker records the signal emitted by the victim's car key fob and replays it to the car's receiver to gain access to the victim's car [3].

RollBack - an attack where an attacker replays a few recorded signals in the hopes of it triggering a rollback to previous valid codes [4].

Rolling code - also known as hopping code is a type of code that regenerates after use. In a car's central locking system, this means that the car's key fob generates a new signal with each button press [4].

RollJam - an attack where an attacker records a victim's car key fob signal while preventing it from reaching the victim's car [4]. Once the victim tries to use the key fob again, the attacker replays the previous signal and records the latest signal to replay it at a later time.

Software defined radio (SDR) - radio hardware whose functionality can be changed by the software in use [5].

2 Background

Around the year 1900, cars did not need any protection against theft, because the process of starting a car was rather complex. Due to this, protection against theft was not a big priority of car manufacturers and suppliers like Bosch [1]. Later on, in 1911 one of the first defence systems against thieves was developed when the company Bosch started adding ignition switches that needed a key. According to the source, turning the ignition knob was impossible without a key.

Before the 1920s car doors did not use to lock, and some cars even did not have any doors [1]. But when vehicles with canopy tops, doors, and closed roofs started gaining popularity, manufacturers started adding the option to lock the car doors, which meant that the owner of the car could safely store their possessions in their car. Unless a thief had the car's key or was willing to break the car's window, they could not enter the vehicle.

The first remote locking systems started to appear in the 1950s when garage doors could be opened with a radio signal [6]. These systems were very simple in design – every time a single signal was sent out the garage door would respond to it.

The first car to use remote central locking came out in 1982, featured on the Renault Fuego [7][8]. This remote keyless system used a key fob that emitted an infrared signal and a receiver on the car that could detect the signal.

In 1995 the frequency used for remote keyless entry systems in cars was standardized in Europe [8]. By that time infrared locking systems were being replaced by radio-controlled security systems in the car manufacturing world.

In the mid-1990s remote keyless entry systems started adapting rolling code to protect car owners against attackers who knew how to record the signal emitted by a car key fob [2]. Implementing rolling code in remote keyless entry systems means that every time a button on the car's key fob is pressed, it generates a new, single-use code.

The following subchapters describe different attacks against the remote keyless entry system and the tools used to implement attacks and assess the security of the car key fob.

2.1 Keyless entry system technologies

Remote keyless entry systems refer to electronic locks that compose of a transmitter that can send out commands, such as lock and unlock, and a receiver that can receive and react to the commands that were sent [3]. These systems either use simple signals which means that every button press on a car key fob sends out the same signal, or rolling code, which would mean that every button press generates a new signal.

2.1.1 Simple signals

Simple signals refer to remote entry systems that use a single-code system. Like each car has a unique physical key, car manufacturers also provide a unique code for every car, but this was not enough to keep cars safe as attackers could get hold of this signal and use it to their advantage [2]. Once they get a hold of the signal, they just need to send it out again. To make using car key fobs to lock/unlock cars safer, manufacturers started introducing rolling code [2].

2.1.2 Rolling code

Implementing rolling code in remote keyless entry systems means that every time a button on the car's key fob is pressed, a new unique code is generated [9]. The new codes can be generated by either using a counter-based approach or using pseudo-random number generators (PRNGs).

In a counter-based approach, both the car and the car's key fob have to have the same starting number, which means that they have to be synchronised before use [9]. Both the car and the key fob have to generate new signals using the same function to generate the code based on the counter. Figure 1 shows an illustration of the process from H. Li's rolling code explanation [9], where pushing the unlock/lock button on the key fob unlocks the car and uses the first code. To use the next code, the counter is increased on both the key fob and the car's side, making the previous codes invalid.

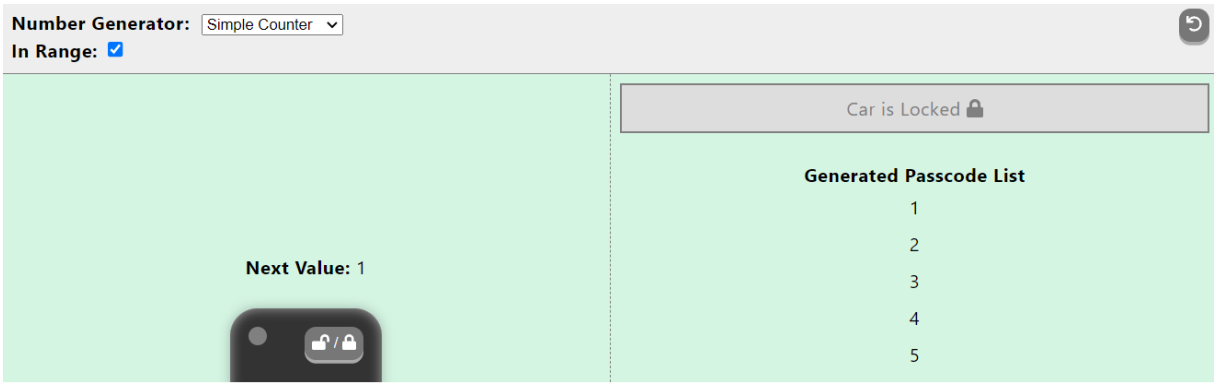

Figure 1. An illustration of a counter-based rolling code [9].

In a system that uses a pseudo-random number generator with each button press, a new, ideally unpredictable number sequence is generated [9]. Both the car and the key fob get the same starting value or an initial parameter (also known as a seed), that allows them to use a function to generate the same, seemingly random, codes. Figure 2 depicts a PRNG-based system, where pressing the unlock/lock button generates a new seemingly random code with each press on both the key fob and the car's side.

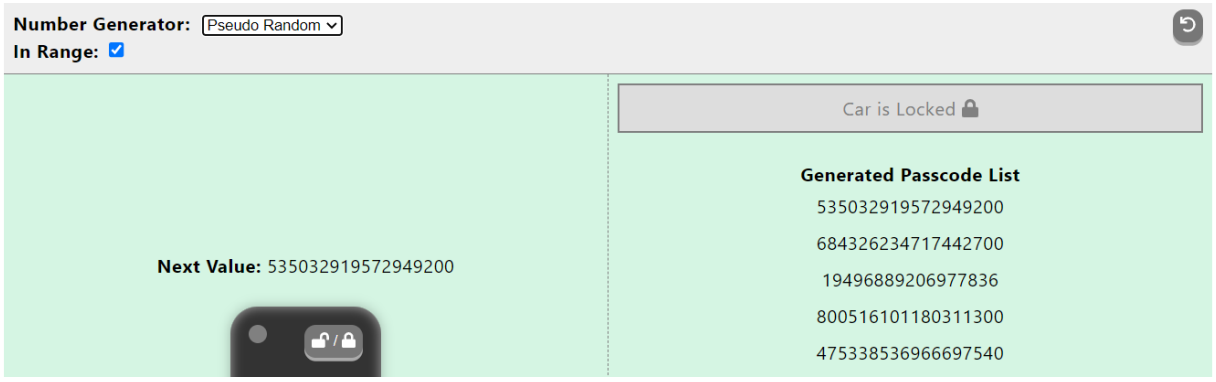

Figure 2. An illustration of a pseudo-random number generator based system [9].

To prevent desynchronising the system by accident, future valid codes are stored in the vehicle [4]. If a button on the car's key fob gets pressed outside the range of the car's receiver, the car still recognises the next signal as a valid signal. Using a code that is ahead of the valid code that the car expects next will invalidate all the codes that fall between the actual code and the expected code [9].

2.2 Attacks

In this section, different kinds of attacks against RKE systems will be reviewed. For each of the attacks, there will be a general idea of how they work.

2.2.1 Replay attack

A replay attack is one where the signal emitted by a radio transmitter device (of a transmitter/receiver pair) is captured by a foreign radio receiver and later sent back to the original receiver [4]. The attack is considered successful if the same action is performed when the signal is replayed. This attack generally only works on cars where the key fob always transmits the same signal. To thwart this type of attack, manufacturers implemented rolling code.

2.2.2 RollJam

RollJam is an attack technique that was created by Samy Kamkar in 2015 [4][10]. This attack aims to disable the protection offered by rolling codes and works by capturing the newest signal from the key fob while ensuring the signal never reaches the car's receiver.

Figure 3. Samy Kamkar's RollJam attacker [10].

A RollJam attack device, depicted in Figure 3, works by blocking the signal from reaching the car's receiver, and simultaneously recording it. When the car owner attempts to unlock the doors again, the attacker sends the previously recorded signal to the car and records the new signal to have a valid code to use later [10].

2.2.3 Relay attack

A relay attack is a type of replay attack that is targeted at cars that use key fobs that constantly emit a signal which can unlock the car when in the car's receiver's range [11]. The attacker records the signal that is constantly being emitted by the key fob. After recording the signal, the attacker could either go to the victim's car or send the recorded signal file to an accomplice.

In RKE systems the user of the car has to press a button on the car's key fob to unlock the car doors [3]. Since relay attacks are targeted at car locking systems that use a key fob that constantly is emitting a signal, key fobs in an RKE system cannot be tested against this.

2.2.4 Café attack

Inspired by the concepts of the RollJam attack and a relay attack, a Café attack is a type of replay attack where an attacker acquires a valid signal from a key fob that uses rolling code when the car's receiver is not in range of the transmitter. This guarantees an unused signal and imitates the real life situation where an attacker might have access to a car key fob outside the range of the car, for example in a café or an office. After recording the signal, an attacker can go to the car themselves or they can forward the file containing the signal to an accomplice who is waiting by the victim's car.

The name "Café attack" seemed to be suitable as it is possible to carry out this type of replay attack in any public space where an attacker could have access to the victim's car key fob.

2.2.5 Rollback

A RollBack attack is a type of replay attack where an attacker can record and replay some already used signals causing the system to synchronise to previously used codes assuming a fault in the synchronisation process which allows for an attacker to gain access to a victim's car [4]. With this type of replay attack, an attacker can use the already used signals as many times as they want without having to record new signals.

2.2.6 Attacks chosen

For the experiments, only replay attacks and café attacks were conducted. These attacks were chosen because they only involved recording a few signals and replaying these signals to the

cars, which means that causing the system to go out of synch (and therefore causing financial harm to the participants' cars) was less likely to happen than with the other attacks.

2.3 Devices used to assess security

Software defined radio (SDR) or software radio (SR) is a radio device whose functionality can be changed depending on the software used [3]. According to the source, a device is considered to be a radio if it can receive and/or transmit radio frequency (RF) signals.

The codes used in RKE systems to unlock the car doors are generated in the microchip of the car remote [6]. This would require an attacker to physically obtain the car remote. However, when the code is emitted as a signal an attacker can easily capture it without the victim noticing using radio hardware such as SDR.

The rest of this section focuses on giving an overview of different SDR platforms, both the software and hardware that can be used to assess the security of car key fobs. The hardware is compared by its functionalities and price points.

2.3.1 Hardware

The most affordable SDR hardware is usually receivers only, such as the RTL-SDR, pictured in Figure 4 [12]. This device sells for approximately 30 dollars and has an operating range of 24MHz to 1766MHz, which means that it can record the signals emitted by a car key fob as the key fobs work on frequency 433.92MHz or 868MHz [13]. The sample rate is low hence sample sizes are small and will not overload computer storage. Since this device is a receiver only, it cannot transmit signals, meaning this device is not sufficient to conduct replay attacks on its own.

Figure 4. The RTL-SDR [14].

The RTL-SDR is a good device for capturing the signal emitted by a car key fob, as it can operate on the frequencies used by car key fobs. The device itself is small and easy to hide, which helps an attacker to remain inconspicuous.

The YARD (Yet Another Radio Dongle) Stick One by Great Scott Gadgets, illustrated in Figure 5, is a "sub-1 GHz wireless test tool controlled by your computer" [15]. This device is both a receiver and a transmitter. Official operating frequencies are 300 to 348 MHz, 391 to 464 MHz and 782 to 928 MHz, these are guaranteed to work according to the creators. These frequency ranges align with the ones necessary to conduct a replay attack. The YARD Stick One costs $99.95 [16].

Figure 5. The YARD Stick One [15].

As shown in Figure 6, the Flipper Zero is a toy-like multi-tool, that can be used as a sub-1 GHz transceiver among other functionalities [17]. The official frequency bands for the Flipper One are 315MHz, 422MHz, 868MHz and 915MHz, which makes this device suitable for conducting replay attacks on cars. This device costs $169 [18].

Figure 6. The Flipper Zero [18].

One of the other cheaper options for transmitting is the HackRF One, illustrated in Figure 7, which is an SDR platform by Great Scott Gadgets that is marketed as test equipment for RF systems [19]. The supported frequency range is from 1MHz to 6GHz. This device costs $339.95 [20]. The HackRF One was used to conduct the replay attacks and café attacks for this thesis paper.

Figure 7. The HackRF [19].

Since the HackRF One's supported range is compatible with the frequencies car key fobs use and it can both receive and transmit a signal, it was an efficient tool for conducting the experiments.

In addition to the HackRF One, a Portapack can be purchased. A PortaPack, shown in Figure 8, is a device which attaches to the HackRF One to add a touchscreen, user control and more features to be able to use the HackRF One without a computer [21]. This would make the HackRF One easier to use for an attacker, as it would not be necessary to carry a computer with them. The PortaPack costs $200 (HackRF not included) [21].

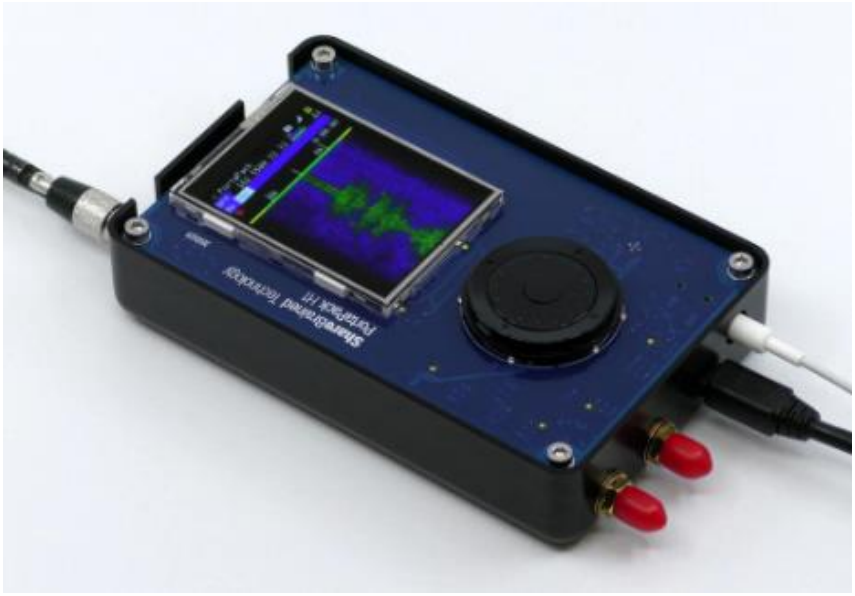

Figure 8. The PortaPack [21].

The bladeRF, illustrated in Figure 9, is an SDR platform for both professionals and hobbyists to explore radio frequency (RF) communication [22]. The bladeRF makers offer tutorials, documentation and the source code of the project, to make using this product as convenient as possible for their target audience. The device is portable and supports USB 3.0 SuperSpeed. The supported frequency range is from 300MHz to 3.8GHz. Prices can range from 540 to 1850 dollars, which makes this device expensive [22].

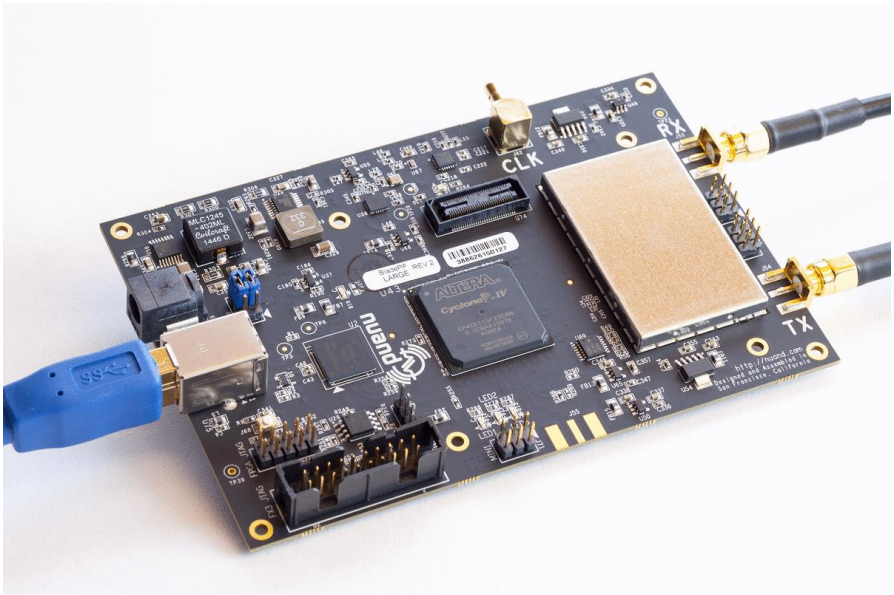

Figure 9. The bladeRF [22].

The LimeSDR, shown in Figure 10, is an SDR platform that is claimed to be usable for anyone who has an interest in RF communication [23]. The supported frequency range is from 100kHZ to 3.8GHz. This device costs $399 [24].

Figure 10. The LimeSDR [23].

Both the BladeRF and LimeSDR are on the expensive side of SDR platforms, but they have their benefits – both are full-duplex devices, which means that they can transmit and receive signals simultaneously.

The HackRF was chosen to conduct the experiments, as it was more affordable than the bladeRF and the LimeSDR. The RTL-SDR and YARD Stick One are more affordable than the HackRF, but the RTL-SDR can act only as a receiver and could not transmit signals which would also be necessary for conducting replay attacks. The YARD Stick One has less software support than the HackRF One.

2.3.2 Software

A spectrum analyser of, which there are many, would be needed to find the frequency used. Some examples of software that could be used for this purpose:

- GNU Radio [25]
- HackRF spectrum analyser [26]
- SDR# [27]
- HDSDR [28]
- Spectrum Lab [29]

In this paper, GNU Radio was used to confirm the car's key fob's signal frequency. On the GNU Radio website, the software is described as "a free & open-source software development toolkit that provides signal processing blocks to implement software radios" [25]. For this reason, GNU Radio was selected for this paper as it offered the freedom to create a custom spectrum analyser instead of using a ready-made option. Usually, GNU Radio programs are written in Python [30].

It is necessary to have software to capture and analyse the signal. A few of these would be:

- URH [31]
- GNU Radio
- Inspectrum [32]
- SDRangel [33]

Universal Radio Hacker (URH) was used to record and replay the signal. URH is a software tool used for wireless protocol investigation [31]. This tool offers support for a variety of SDR devices. Some of the features listed are the demodulation of signals and automatic detection of modulation parameters which help to identify the bits transmitted by the signal source (in this paper, by a car key fob). The bits are the code that the car key fob generates and the signal is what is emitted as radio waves. Demodulation of the signal means that the radio waves get converted into the generated code [34]. For the reasons listed above, URH proved to be the easiest-to-use choice for capturing the signal, analysing the signals and replaying the signal.

3 Experiments

In this chapter, there is an overview of the cars which were chosen for the experiments based on how popular these specific cars are in Estonia. After explaining why these particular cars were chosen to be in the experiments, there will be an overview of how the replay attacks were carried out and which tools were used for it.

To carry out a replay attack, it is necessary to capture the car's key fob's signal and then analyse whether the car uses rolling code or not. After that, it is possible to replay the signal to the car and attempt to perform a replay attack. Since the process of verifying the key fob's signal frequency and later recording it is very similar with all the cars, the process is described using examples from recording the 2012 Skoda Fabia's key fob's signal.

3.1 Cars chosen

For the experiments, friends and family members of the author were offered an opportunity to find out if their cars were vulnerable to replay attacks or café attacks. Participants were required to sign a consent form (see Appendix I).

The chosen cars were ranked based on make and model popularity. The make of the car refers to its brand and the model refers to the specific vehicle model[2]. For a Ford Focus, Ford is the make and Focus is the model.

All of the chosen cars except for one (a Lexus LS460) are in the top 20 of popular makes and most of the cars are in the top 50 of popular models based on Estonia's Transport Administration's data [35].

Of the chosen cars, the Lexus LS460 is not considered to be popular based on the make (ranking at the 29th position) or model (1187th place), but it was more expensive than an average costing car in 2007. While an average new car cost $23,892 in 2007[3], the Lexus LS460 had a starting price of $61,000[4]. This makes the Lexus an interesting test subject regardless of its popularity. The Lexus' key fob features a lock and unlock button as shown in Figure 11.

[2] https://www.progressive.com/answers/what-does-make-and-model-mean/
[3] https://www.energy.gov/eere/vehicles/fact-744-september-10-2012-average-new-light-vehicle-price-grows-faster-average-used
[4] https://www.cars.com/research/lexus-ls_460-2007/

Figure 11. The key fob of the 2007 Lexus LS460.

The data from Estonia's Transport Administration includes five main age categories for cars (and one for unknown ages), in descending order by popularity they are:

- 10 to 20 years old
- Older than 20 years
- 5 to 10 years old
- 2 to 5 years old
- 0 to 2 years old

The cars chosen for this thesis mostly fall under the 10 to 20-year-old car category, this includes the Lexus.

Based on both make and model, the most popular car chosen for these experiments is the 2008 Volkswagen Passat Variant, which ranks at number 1 based on the make and number 5 based on the model [35]. As shown in Figure 12, this car's key fob has the functionality to lock and unlock the car doors and it also has a button to open the car's trunk.

Figure 12. The key fob of the 2008 Volkswagen Passat Variant.

Other cars that fall under the most common age group for cars in Estonia include both a 2005 and a 2012 Ford Focus, which are the 3rd most popular cars based on the make and 11th based

on the model [35]. Both of these cars' key fobs' can lock and unlock the doors and they can also open the trunk, as illustrated in Figure 13.

Figure 13. The key fob of the 2005 Ford Focus (left) and the key fob of the 2012 Ford Focus (right).

The remaining cars in the most common age category include a 2006 Audi A6 Avant which is 4th most popular based on the make and 9th based on the model, a 2008 Honda Civic which is 12th most popular based on the make and 17th based on the model and a 2012 Skoda Fabia which is 8th most popular based on the make and 22nd based on the model [35]. All of these cars feature lock and unlock buttons, but only the Honda Civic does not have a button for opening the car's trunk. The key fobs of these cars are shown in Figure 14, where the key fob on the left belongs to the 2006 Audi A6 Avant, the middle one belongs to the 2008 Honda Civic and the rightmost key fob belongs to the 2012 Skoda Fabia.

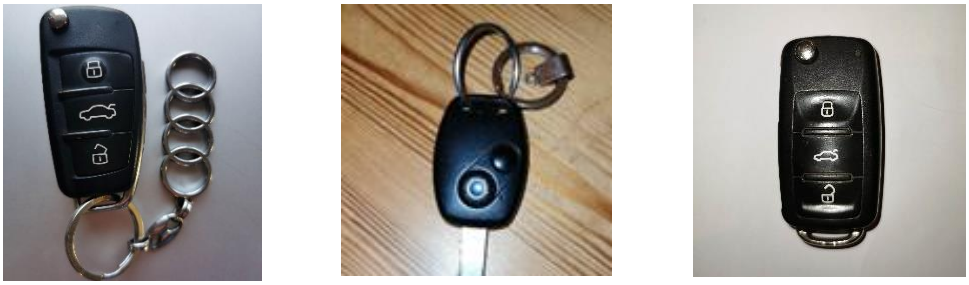

Figure 14. The key fobs of the 2006 Audi A6 Avant (left), 2008 Honda Civic (middle) and 2012 Skoda Fabia (right).

The cars that fell under the other age categories were a 1998 Audi A6 Avant (ranked 4th based on the make and 9th based on model), a 2015 Ford Galaxy (ranked 40th based on the model), a 2015 Honda Accord (ranked 58th based on the model), a 2016 Mazda 6 (ranked 16th based on make and 24th based on the model) and a 2018 Opel Astra (ranked 9th based on the make and

36th based on the model) [35]. The 2016 Mazda 6 and the 2018 Opel Astra have lock and unlock buttons on their key fobs, as shown in Figure 15. The rest of the cars also have a button for opening the trunk which can be seen in Figure 16.

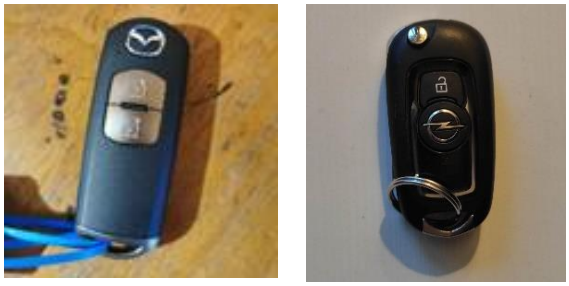

Figure 15. The key fobs of the 2016 Mazda 6 (left) and the 2018 Opel Astra (right).

Figure 16. The key fobs of the 2015 Ford Galaxy (left), the 1998 Audi A6 Avant (middle) and the 2015 Honda Accord (right).

The car ranking information is summarised in Table 1. The first column lists the cars in random order, the second column indicates the popularity of the make, the third column indicates the popularity of the model and the final column shows the cars' ranking based on the age groups.

Table 1. The popularity of the cars chosen for the experiment.

Car make and model	**Popularity based on the make**	**Popularity based on the model**	**Popularity based on age group**
2005 Ford Focus	3	11	1
2012 Ford Focus	3	11	1
2015 Ford Galaxy	3	40	3

1998 Audi A6 Avant	4	9	2
2006 Audi A6 Avant	4	9	1
2008 Honda Civic	12	17	1
2015 Honda Accord	12	58	3
2007 Lexus LS460	29	1187	1
2008 Volkswagen Passat Variant	1	5	1
2012 Skoda Fabia	8	22	1
2016 Mazda 6	16	24	3
2018 Opel Astra	9	36	3

For these experiments, only the unlock signals were tested, as an attacker might only be interested in gaining access to the car. By unlocking the car doors, an attacker would have access to the contents of the trunk as well, and locking the car probably would not be their priority.

3.2 Capturing the signal

Before capturing the car's key fob's signal, it is necessary to verify the emitted signal's frequency. This can be done using a spectrum analyser. For these experiments, GNU Radio and a HackRF were used to build the spectrum analyser. Figure 17 depicts the spectrum analyser used. This flow chart consists of 5 blocks:

- Options, in which the language and script name are configured.
- Variable, which specifies the sampling rate the HackRF should use. It was set to 5Msps to have a broad view of the spectrum to detect any signals the remote may emit.
- QT GUI Range gives the freedom to scroll through radio frequencies. Its values (upper and lower) were set to the HackRF's operating frequency.
- Osmocom Source block was used to receive data from the HackRF. The frequency is set to 433MHz because the most commonly used frequency used for car key fob transmitters is 433.92 MHz [13].
- QT GUI Waterfall Sink displays a waterfall plot, which shows the signal's frequency over time. Figure 18 is an example of how the key fob's signal looks on the waterfall plot. The signal is marked with a pink circle.

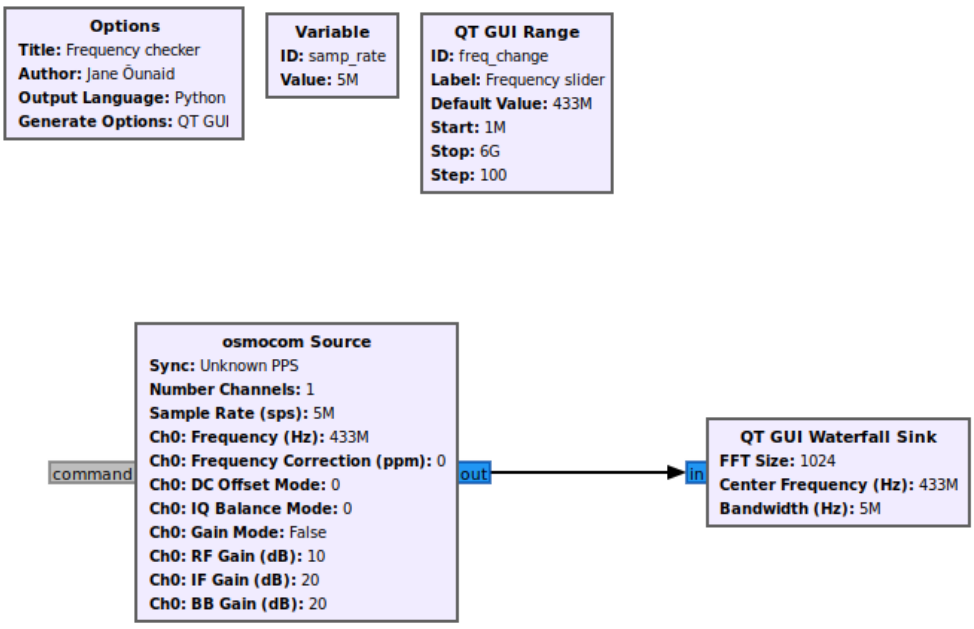

Figure 17. A simple frequency checker in GNU Radio

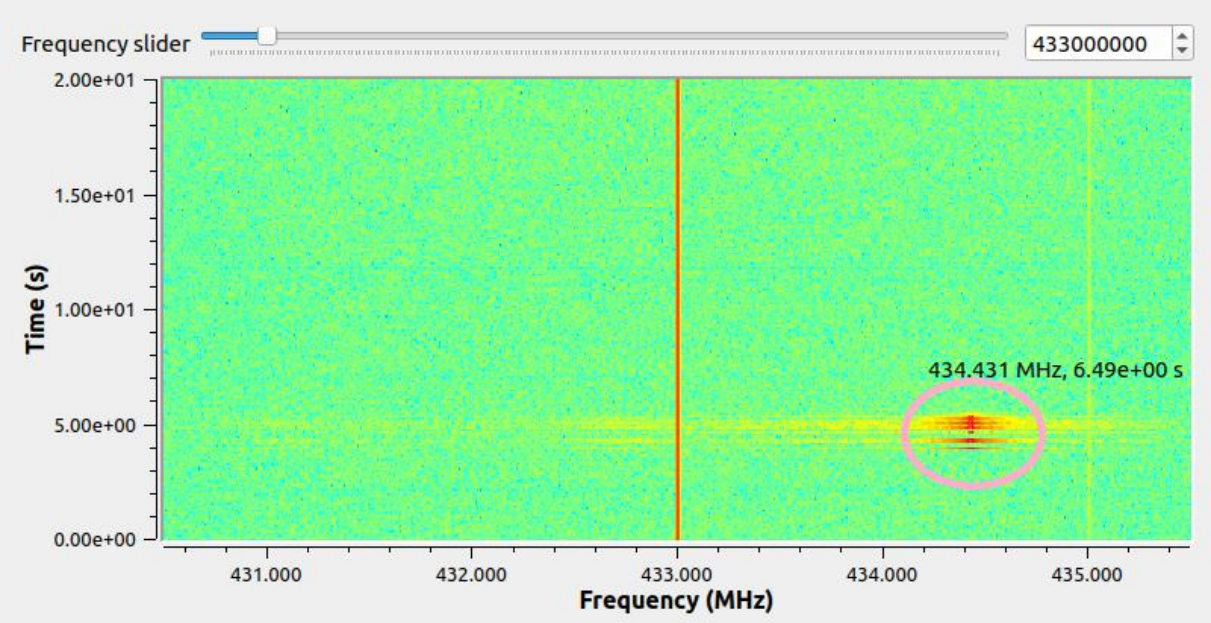

Figure 18. Skoda Fabia's key fob frequency.

After confirming the car's frequency, URH was used to record the signal. This was done by selecting "Record Signal" from the "File" menu, which is depicted in Figure 19. This action opened a window where the settings needed to record the device's signal were specified. Figure 20 shows the settings that were entered for the Skoda Fabia's key fob signal.

As the HackRF was also used to capture the signal, the "Device" option was set to HackRF. The frequency was set to the value discovered by the spectrum analyser, which was 434,43 MHz. For cases where the car's remote had a weak signal, the Gain was increased to the maximum value to amplify the signal. Everything else was kept at their default values.

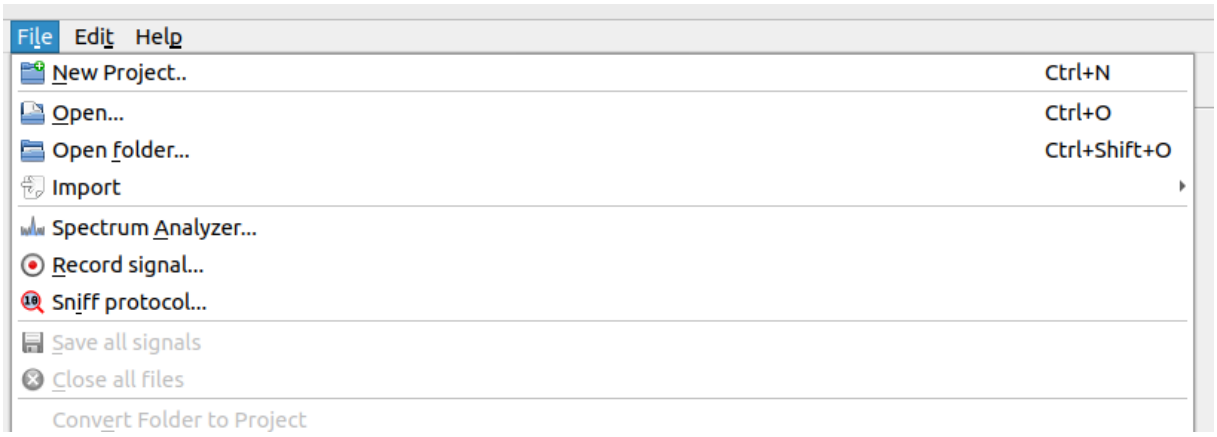

Figure 19. The "File" menu in URH.

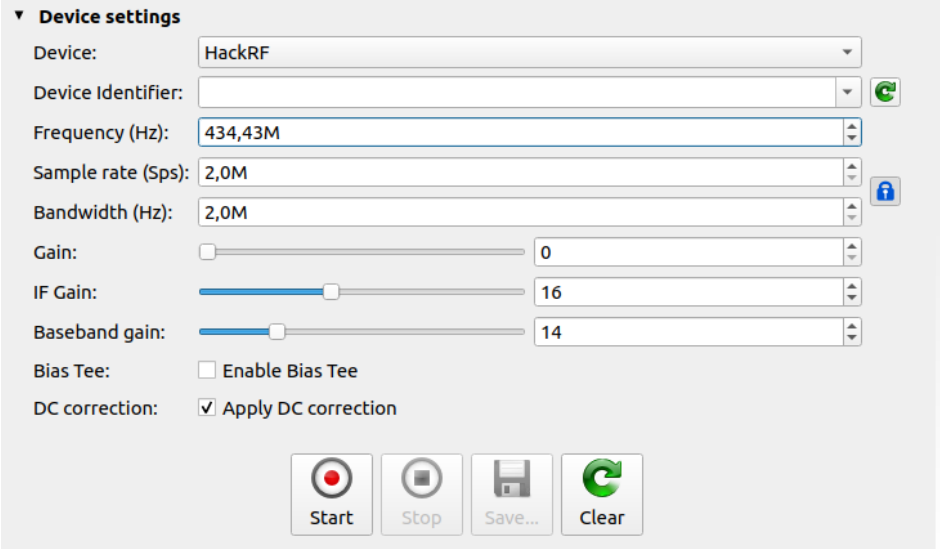

Figure 20. Device settings used to record car fob signals in URH.

Figure 21 shows both the wave pattern and the bits of the recorded signal. The upper window shows the captured signals; the highlighted part is one button press on the key fob. Two button presses were recorded to find out if the car's key fob uses rolling code. The lower window showed the signals as bits. Comparing the bits of the two button presses shows that each press generates a new unlock signal. This was used to determine if the car used rolling code.

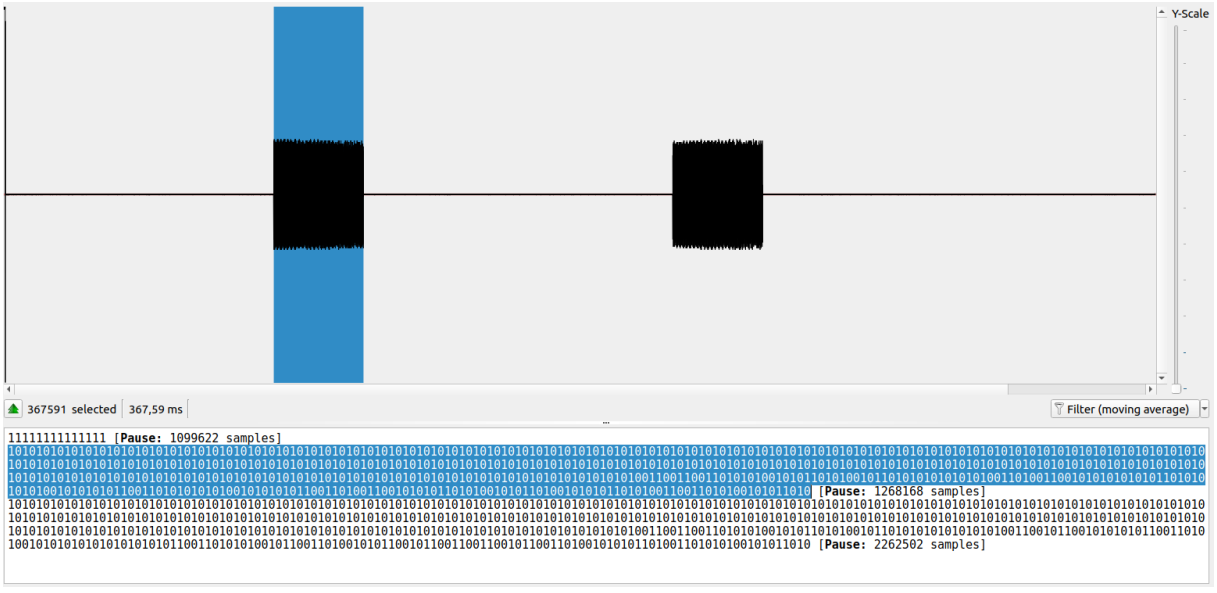

Figure 21. Skoda Fabia key fobs unlock signals

After determining if the car uses rolling code, both a simple replay attack and a café attack were conducted. The replay attacks were conducted by replaying the same signal that was recorded

in the range of the car's receiver. This was done by selecting the "Replay signal" option in URH.

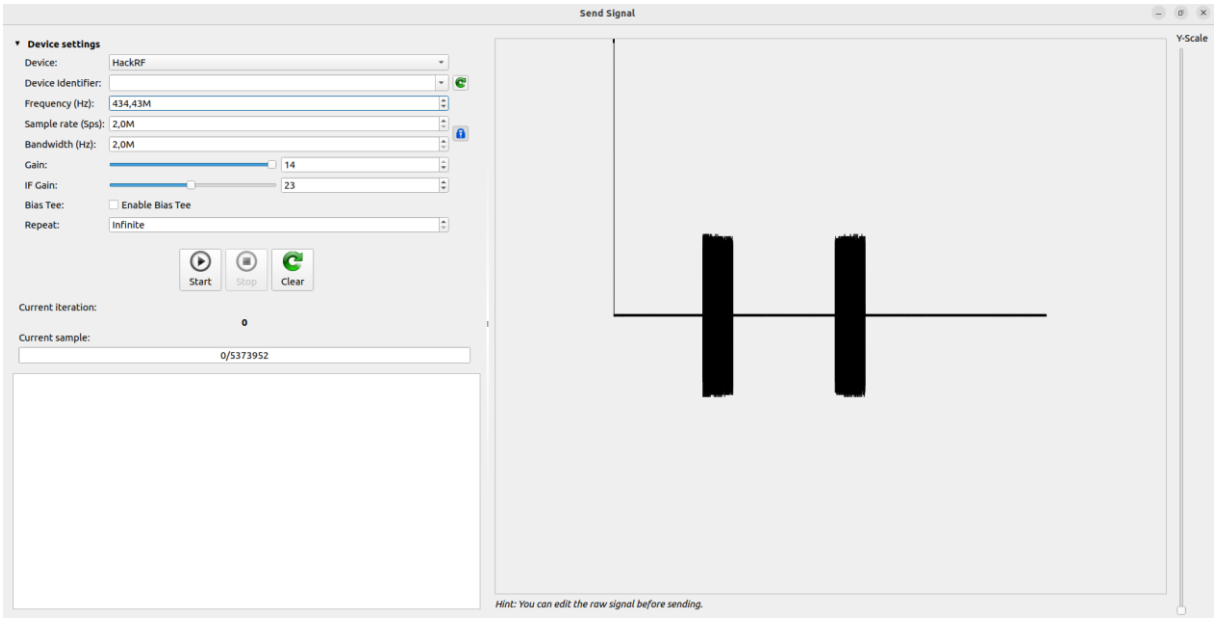

Figure 22. Replaying the Skoda Fabia's key fob's signal to the car.

Figure 22 shows that in the newly opened window, the "Device" was set to the HackRF, "Frequency (Hz)" was set to "434,43M" and the "Gain" slider was set to the highest value. The button with the text "Start" was pressed. None of the cars responded to this, as all of them used rolling code.

3.3 Conducting a Café attack

To conduct a Café attack, a signal was recorded outside the range of the car's receiver. To look more discreet while conducting these experiments, the HackRF and laptop were kept in a handbag just so the HackRF's antenna would barely stick out of the bag. The programs necessary for the experiments were executed from a phone that had access to the laptop over a TeamViewer[5] session. The used setup is illustrated in Figure 23, where the left side shows that the laptop's screen is broadcasted to the smartphone and on the right side it is shown that the smartphone can still control the laptop even when it is in the bag.

[5] https://www.teamviewer.com/en/

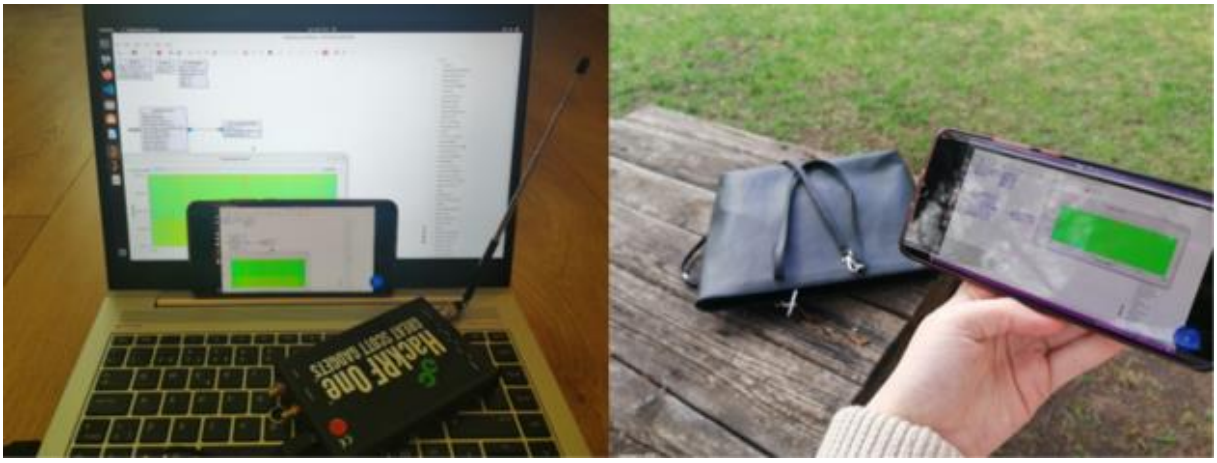

Figure 23. HackRF and a laptop in a bag can be controlled with a smartphone.

After an unused signal was acquired, it was replayed in the range of the car's receiver. The car was considered to be vulnerable against a Café attack if it responded to the replayed signal. If the car did not respond to the signal being replayed, it had additional safety measures in addition to rolling code.

4 Results

None of the tested cars were vulnerable to a simple replay attack, because all of them used rolling code. Only three cars (2012 Ford Focus, 2006 Audi A6 Avant and 2008 Volkswagen Passat Variant) were not vulnerable to the Café attack. Table 2 gives an overview of the results of checking whether a car's locking system used rolling codes or not and which attacks the car was vulnerable against. The first column shows the car make, model and year, the second column shows the operating frequency discovered with the spectrum analyser, the third column shows whether the key fob used a simple signal or rolling code, the fourth column shows if the car was vulnerable to a simple replay attack and the last column shows whether the car was vulnerable to a Café attack.

Table 2. Comparison of the car fob models.

Car make and model	Signal frequency	Code type	Vulnerable to a simple replay attack?	Vulnerable to a Café attack?
2005 Ford Focus	433.92 MHz	Rolling code	No	Yes
2012 Ford Focus	433.92 MHz	Rolling code	No	No
2015 Ford Galaxy	434.43 MHz	Rolling code	No	Yes
1998 Audi A6 Avant	433.92 MHz	Rolling code	No	Yes
2006 Audi A6 Avant	868.26 MHz	Rolling code	No	No
2008 Honda Civic	433.92 MHz	Rolling code	No	Yes
2015 Honda Accord	433.92 MHz	Rolling code	No	Yes
2007 Lexus SL460	433.92 MHz	Rolling code	No	Yes

2008 Volkswagen Passat Variant	434.43 MHz	Rolling code	No	No
2012 Skoda Fabia	434.43 MHz	Rolling code	No	Yes
2016 Mazda 6	433.92 MHz	Rolling code	No	Yes
2018 Opel Astra	433.92 MHz	Rolling code	No	Yes

The cars that were not vulnerable to the Café attack in all probability used other safety measures in addition to the rolling code. These measures could include a timer-based system, where the signal emitted by the car's key fob has to reach the car's receiver within a specific time window [36]. Another safety measure could be a signal strength measure, where the signal emitted by the key fob has to have the right signal strength [11].

For example, the 2012 Ford Focus sent out two signals on frequencies 433.57MHz and 433.92MHz. Sending out two signals could mean that the car's receiver expected to receive two simultaneous signals, but only got one. Future work could explore this further by analysing both of the signal values individually and testing if recording and replaying these two signals simultaneously would make the car vulnerable to a Café attack.

5 Discussion

The experiments showed, that rolling code alone is not enough to protect car owners from falling victim to replay attacks. There are a few different ways to prevent falling victim to attacks against RKE systems. One of them would be to use a physical key instead of the car's key fob. An attacker cannot record the signal of a car key fob unless a button on the key fob is pressed.

There are also suggestions for car owners that help lessen the risk of falling victim. One of these suggestions is to use a signal-blocking bag or box to protect the car's key fob's signal from being recorded without consent [37]. These bags or boxes could also protect a user from accidentally pressing the key fob's buttons while it is in a bag. In the source, it is also mentioned that there is a possibility to re-program the car's key fob to prevent a situation where a previous owner lost one of the car's key fobs or is planning to use a spare key fob with malicious intent.

Car owners can prevent attackers from recording their car key fobs' signals by making sure to not leave anyone unattended with the key fob. Owners should also avoid playing with the buttons on the car's key fob, as an attacker could be nearby to record the emitted signal.

6 Conclusion

In this thesis, some of the attacks used against remote keyless entry systems were described, of which replay attacks and café attacks were conducted on some of Estonia's most popular car models.

The preparation for the attacks and afterwards conducting the replay attacks and Café attacks was done using the HackRF. GNU Radio was used to verify the signal frequency and once the signal frequency was confirmed, the Universal Radio Hacker software was used to record signals emitted by the key fobs and replay the recorded signals to the corresponding cars.

Results of the conducted attacks showed that none of the cars were vulnerable to a simple replay attack, which means the average car owner probably does not need to worry about falling victim to such an attack. However, most of the cars were vulnerable to a Café attack, so it would be wise for car owners to keep an eye out for their car's key fob while in public.

In the future, research can be done on analysing the rolling code used in a selection of the most popular car models in Estonia or implementing other types of attacks against remote keyless entry systems. These attacks could be for example RollJam and RollBack.

References

[1] Kuhlgatz D. From car keys to perfectly keyless. Over 100 years of Bosch car locking technology. Bosch. https://www.bosch.com/stories/history-car-locking-systems/ (18.12.2022).

[2] Lake M. HOW IT WORKS; Remote Keyless Entry: Staying a Step Ahead of Car Thieves. The New York Times. 6.7.2001; https://www.nytimes.com/2001/06/07/technology/how-it-works-remote-keyless-entry-staying-a-step-ahead-of-car-thieves.html (20.4.2023)

[3] Djinko IAR, Kacem T, Girma A. Blockchain-based Approach to thwart Replay Attacks targeting Remote Keyless Entry Systems. In: 2022 International Conference on Engineering and Emerging Technologies (ICEET). Kuala Lumpur, Malaysia: IEEE; 2022. page 1–6. https://ieeexplore.ieee.org/document/10007335/ (6.5.2023)

[4] Levente Csikor, Hoon Wei Lim, Jun Wen Wong, Soundarya Ramesh, Rohini Poolat Parameswarath, Mun Choon Chan. RollBack: A New Time-Agnostic Replay Attack Against the Automotive Remote Keyless Entry Systems. 14.9.2022;1–4.

[5] What is Software Defined Radio? Wireless Innovation Forum. https://www.wirelessinnovation.org/Introduction_to_SDR (25.4.2023)

[6] Marshall Brain. How Remote Entry Works. howstuffworks. 15.8.2001;2,3.

[7] 1980-1985 RENAULT Fuego Turbo. Octane. https://web.archive.org/web/20121027091155/http:/www.classicandperformancecar.com/front_website/octane_interact/carspecs.php/?see=3341 (19.4.2023)

[8] James Mills. KEYLESS WONDER: HOW DID WE END UP WITH “SMART” WIRELESS KEYS FOR OUR CARS? The Sunday Times Driving. 2014. https://www.driving.co.uk/features/keyless-wonder-how-did-we-end-up-with-smart-keys-for-our-cars/ (19.4.2023)

[9] Harry Li. Rolling Code Securing keyless entry systems. https://harryli0088.github.io/rolling-code/ (20.4.2023)

[10] Andy Greenberg. This Hacker’s Tiny Device Unlocks Cars And Opens Garages. Wired. 8.6.2015; https://www.wired.com/2015/08/hackers-tiny-device-unlocks-cars-opens-garages/ (21.4.2023)

[11] Aurelien Francillon, Boris Danev, Srdjan Capkun. Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars. IACR Cryptology ePrint Archive. 1.2010;2010. https://www.researchgate.net/publication/220333841_Relay_Attacks_on_Passive_Keyless_Entry_and_Start_Systems_in_Modern_Cars (20.4.2023)

[12] ABOUT RTL-SDR. RTL-SDR.COM. https://www.rtl-sdr.com/about-rtl-sdr/ (5.1.2023)

[13] Remote Keyless Entry Systems Overview. ANALOG DEVICES. 2002. https://www.analog.com/en/app-notes/remote-keyless-entry-systems-overview.html (20.4.2023)

[14] RTL-SDR BLOG V3 R860 (R820T2) RTL2832U 1PPM TCXO SMA SOFTWARE DEFINED RADIO (DONGLE ONLY). RTL-SDR.COM. 2017. https://www.rtl-sdr.com/product/rtl-sdr-blog-v3-r820t2-rtl2832u-1ppm-tcxo-sma-software-defined-radio-dongle-only/

[15] YARD Stick One. GREAT SCOTT GADGETS. https://greatscottgadgets.com/yardstickone/ (20.4.2023)

[16] YARD Stick One - Sub-1 GHz Wireless Test Tool. adafruit. https://www.adafruit.com/product/3586 (20.4.2023)

[17] Flipper Zero. FLIPPER. https://flipperzero.one/ (3.7.2023)

[18] Flipper Zero Shop. Flipper Zero Shop. https://shop.flipperzero.one/ (9.5.2023)

[19] HackRF One. GREAT SCOTT GADGETS. https://greatscottgadgets.com/hackrf/one/ (20.4.2023)

[20] Great Scott Gadgets HackRF One - Software Defined Radio. adafruit. https://www.adafruit.com/product/3583 (20.4.2023)

[21] PORTAPACK FOR HACKRF ONE, KIT. ShareBrained Technology. https://store.sharebrained.com/products/portapack-for-hackrf-one-kit (20.4.2023)

[22] bladeRF. nuand. https://www.nuand.com/bladerf-1/ (20.4.2023)

[23] LimeSDR. Lime microsystems. https://limemicro.com/products/boards/limesdr/ (20.4.2023)

[24] LimeSDR Mini 2.0. CROWDSUPPLY. https://www.crowdsupply.com/lime-micro/limesdr-mini-2#products (20.4.2023)

[25] About GNU Radio. GNURadio. https://www.gnuradio.org/about/ (20.4.2023)

[26] Sakac P. Spectrum Analyzer GUI for hackrf_sweep for Windows/Linux. 2023. https://github.com/pavsa/hackrf-spectrum-analyzer (9.5.2023)

[27] SDRSharp | Amateur Radio – PEØSAT. https://www.pe0sat.vgnet.nl/sdr/sdr-software/sdrsharp/ (9.5.2023)

[28] HDSDR Homepage. https://www.hdsdr.de/ (9.5.2023)

[29] HOME PAGE - SPECTRUMLAB. SpectrumLab. https://www.spectrumlab.eu/ (9.5.2023)

[30] What is GNU Radio? Wiki GNURadio. https://wiki.gnuradio.org/index.php/What_is_GNU_Radio%3F (21.4.2023)

[31] Johannes Pohl, Andreas Noack. Universal Radio Hacker: A Suite for Analyzing and Attacking Stateful Wireless Protocols. [Baltimore, MD]: University of Applied Sciences Stralsund; 2018. https://www.usenix.org/system/files/conference/woot18/woot18-paper-pohl.pdf (5.1.2023)

[32] Walters M. inspectrum. 2023. https://github.com/miek/inspectrum (9.5.2023)

[33] SDRangel – Open-source TX & RX Software Defined Radio. https://www.sdrangel.org/ (9.5.2023)

[34] What is Demodulation? Learn History, Process, Techniques & Applications. testbook. https://testbook.com/physics/demodulation (5.7.2023)

[35] Sõidukite statistika. Transpordiamet. 2023. https://www.transpordiamet.ee/soidukite-statistika (20.4.2023)

[36] Alrabady AI, Mahmud SM. Some attacks against vehicles' passive entry security systems and their solutions. IEEE Transactions on Vehicular Technology. 3.2003;52(2):3.

[37] Prevent Keyless Car Theft – 8 Quick Prevention Tips. Master Locksmiths Association. https://www.locksmiths.co.uk/faq/keyless-car-theft/(18.12.2022)

Appendix

I. Consent form

Nõusolek uurimistöö katsetes osalemiseks

Mina, _____, annan enda nõusoleku osaleda katsetes, mille raames lindistatakse minu auto võtmepuldi signaal ning taasesitatakse see minu autole. Katsete tulemusi analüüsitakse lõputöös ning signaalide lindistused kustutatakse lõputöö valmimisel.

Lõputöö pealkiri on „Taasesitusrünnete mõju uurimine Eestis populaarsete automudelite vastu“ ja töö autor on Jane Õunaid.

Allkiri: _____

Kuupäev: _____

II. Licence

Non-exclusive licence to reproduce the thesis and make the thesis public

I, Jane Õunaid,

1. grant the University of Tartu a free permit (non-exclusive licence) to

reproduce, for the purpose of preservation, including for adding to the DSpace digital archives until the expiry of the term of copyright, my thesis

Investigating the Effect of Replay Attacks on Popular Car Models in Estonia,

supervised by Danielle Melissa Morgan.

2. I grant the University of Tartu a permit to make the thesis specified in point 1 available to the public via the web environment of the University of Tartu, including via the DSpace digital archives, under the Creative Commons licence CC BY NC ND 4.0, which allows, by giving appropriate credit to the author, to reproduce, distribute the work and communicate it to the public, and prohibits the creation of derivative works and any commercial use of the work until the expiry of the term of copyright.

3. I am aware of the fact that the author retains the rights specified in points 1 and 2.

4. I confirm that granting the non-exclusive licence does not infringe other persons' intellectual property rights or rights arising from the personal data protection legislation.

Jane Õunaid
09/05/2023