Car security: remote keyless “entry and go”

Jarno van de Moosdijk, jarno.vandemoosdijk@os3.nl
Dick Visser, dick.visser@os3.nl

June 2009

Revision 232 , compiled at Sun Jul 5 14:40:02 CEST 2009

Research report for System and Network Engineering, University of Amsterdam, the Netherlands. Conducted under supervision of Stan Hegt, Pieter Ceelen and Hans IJkel from KPMG IT Advisory, ICT Security & Control.

Abstract

Modern cars all contain a Keyless Entry system to operate the door locks by radio signals. This can be a traditional car key with integrated remote control, or a smart card with more functions integrated into it. Based on the CIA model for information security, and the STRIDE model for security threats, a matrix of requirements is formulated that these systems should adhere to. This included the process to obtain new or spare keys. To determine whether these requirements are met, we examined the systems that are used by a number of major car brands in the Netherlands. Based on the results of these tests we put forward several recommendations.

Contents

1 Introduction

Modern cars are equipped with several security systems: door locks, ignition lock, steering lock, anti-theft alarm, electronic engine immobiliser and anti-carjacking systems. Many of these are common in modern vehicles, with others starting off as after market add-ons suited to older vehicles. The key provides the authorisation to the multiple layers of security that protect the car from unintended users.
Automobiles have been around since the beginning of the 20th century, however, the first cars were not equipped with any kind of locks.
Current door locks can be operated in various ways. While commonly utilising a mechanical pin tumbler lock, for the sake of convenience, has been entirely bypassed by using "keyless entry" remote locking system.
In addition, technological development has introduced different techniques that can be used to start a car.

The traditional (mechanical) key is gradually disappearing as a way to start the engine. It is being replaced by tokens that operate without user intervention. These systems - called keyless "entry and go" systems - automatically unlock the doors if the token is located within an n-meter radius of the car. Most cars equipped with such a system do not have a traditional ignition lock. They can be started using a "start" button, instead of turning a key.

There is no standard for remote keyless "entry and go" systems. Due to this, there is a lot of diversification on the market of those systems.

Because cars are used on a massive scale, any issues regarding the security systems of them are likely to have a significant social impact. Developments such as RFID historically have always been claimed to be highly secure, but in hindsight turned out to be trivial to break, copy, or otherwise tamper with [30] [7] [18].

In most – if not all – cases of remote keyless "entry and go" systems, proprietary techniques are used. Manufacturers do not publish technical implementation details regarding the security of their products. There is no way to check any claims about security by independent organisations.

1.1 Demarcation of the study

1.1.1 Research questions

Initially our research focused on the following questions:

- *What requirements should a keyless "entry and go" system adhere to?*
- *What systems are currently being used and do they meet these requirements?*

During the research project it turned out to be very difficult to obtain usable information about the security aspects of keyless "entry and go" systems. Almost every contact with manufacturers ended up in a formal statement that no information will be given. Because of this lack of cooperation it was only marginally possible to answer the two research questions stated above.

We therefore decided to do research on an extra topic related to car keys based on the following research questions.

- *What requirements should the new/spare key order procedure adhere to?*
- *What are current order procedures and do they meet these requirements?*

Scope

Car keys contain several security systems. We chose to limit the scope of the project by not taking RFID immobilisers into account, which are also part of every car key. We will only look at the keyless "entry and go" system.

There is an overwhelming set of techniques that can be used for communication between the car and the car key. We will not look into the low level safety characteristics of these techniques. There are numerous papers which describe these in detail [21] [22] [23].

1.1.2 Research methodology

Since there is no official standard for keyless "entry and go" systems, we start by defining a theoretical requirement set to which all systems should adhere. These requirements are constructed using the extended version of the CIA model [25]. In addition we will do a threat analysis based on the STRIDE model [5]. The output of these two models will be used to construct a set of practical requirements. We will do the same for the new/spare key order procedure that the car manufacturers employ.

To see whether these requirements are actually met by technology used in the field, we will make an inventory of the systems currently used by car manufacturers. We will do this by interviewing employees of major car brands in the Netherlands, and examining car keys.

1.1.3 Added value of this study

This research project is an inventory of the system security aspects of remote keyless "entry and go" systems and the new/spare key order procedure. It is largely theoretical, and because of the broad scope it does not contain any in-depth technological reviews. It will be a good starting point however for further research into those areas.

1.2 Structure of this report

Section 1 covers the demarcation of the study and the related work. section 2 contains an overview of all systems that are currently available on the market. The trend of future systems is also covered.

Section 3 covers the system architecture of both the car access and the new/spare key order procedure. This architecture will be used to understand the various attack routines as well as the requirements for any countermeasures to these attacks. Section 4 contains an overview of the CIA model. The three key concepts: confidentiality, integrity, and availability will be extended with various other concepts to be able to create a more complete requirement set.

The CIA model will be linked to the STRIDE threat model in section 5. In addition, the section contains a threat analysis based on the STRIDE model. Section 6 covers the practical requirements which are based on both models.

The practical requirements are used to assess systems currently used by the car brands. This is done in section 7. Based on this assessment, recommendations are formulated in section 8.

Considerations about how insurance companies handle theft without any sign of entry and the KeeLoq technology are covered in section 9. Lastly, section 10 contains the conclusion based on our research questions and ideas for further research.

1.3 Related work

We are not aware of any prior research done on car security in a broad sense. There are several papers that focus on specific details of car security (e.g. KeeLoq).

Keeloq is the proprietary block cipher that is used by a large number of car manufacturers in their keyless entry and keyless go systems. It attracted much attention in the academic world after the specification was leaked in 2006[8]. Since then researchers have described several attacks against it. These were mathematical attacks by Bogdanov[3], Courtois[6], and Indesteege[16].

In 2008 researchers from the Bochum university[10] succesfully conducted differential power analysis (DPA) attacks against KeeLoq. When certain specific conditions were met this resulted in 'a complete break of the cipher'.

2 Available systems

This section gives an overview of the systems that are currently used.

2.1 Mechanical keys

Figure 1:

This is the traditional form of car authentication. A physical key (blade) is used to gain access to the vehicle.

The first car ignition lock appeared in 1919. During this year, the first patent describing a car ignition lock was filed [13]. The invented lock blocked the steering column and disabled the power feed to the engine. As stated at the time:

> *The purpose of this invention is to prevent the theft of automobiles in so far as a mechanical lock can be made to increase the difficulty of moving an automobile or otherwise hampering the free propulsion or movement thereof.*

In the late 1920s ignition locks were standard on most cars. In addition to ignition locks, closed cars were equipped with door locks [26].

Various types of key blades are being used nowadays. Some manufacturers use a blade that is cut from the outside, others use a blade with a groove embedded into it. Figure 1 contains examples of both key blades.

Current cars contain an immobiliser system, which secures the car against hotwiring. Every car key that can be used to start the engine contains an immobiliser chip. This chip communicates with a receiver when the car is being started. The receiver is normally built into the steering column.

2.2 Remote keyless entry (RKE) systems

Figure 2:

Remote keyless entry (RKE) systems have been available since 1983[14]. Nowadays almost all new cars come with such a system. There are two basic types of form factors. The most common one is a remote control integrated into the car key itself. The alternative form factor is a separate small remote control. Figure 2 contains an example of both form factors.

RKE systems enable a car owner to open his car without using the physical lock of the car. The RKE system usually signals that it has either locked or unlocked the car through a combination of flashing indicator lights and a distinctive sound other than the horn. In addition to opening and closing the car, other features are also possible like opening and closing the trunk, windows, or rooftop. Some RKE systems also have a "panic button" which activates the car alarm.

RKE systems operate via radio frequencies: 315 MHz is used in North America and Japan, 433.92 MHz in Europe [31]. The operating range of RKE systems varies between manufacturers. For instance Ford RKE systems have a range of 20 meters for Europe and North America and only 5 meters for Japan and other markets where transmission power is more restricted by law. The range around the vehicle is not linear as corner pillars and small window apertures attenuate the

signal, hence reducing its range [34].

The same technology has been used to open garage doors since the 1950s [4]. Those transmitters were extremely simple, they sent out a single - non-encrypted - signal to the garage door opener, which would respond by opening or closing the garage door. Everyone with such a garage door opener could open all other doors that were fitted with the same equipment. As these systems became more common, so grew the need for security. Modern RKE systems claim that they use encryption to prevent car thieves from decoding the signal.

2.3 Passive keyless entry (PKE) systems

Evolution of the RKE technology has led to so-called *passive keyless entry* or PKE systems. The first PKE system was patented in the US on July 17, 1990 [32]. The system enables the owner to open his vehicle without the need for physical interaction (e.g. pushing a button on the remote control). The car is automatically unlocked if the key is within a certain radius of the car.

Some manufacturers use a slightly different technique. Once you are within the radius, the car does not unlock automatically. Instead the door handles contain motion sensors – when you touch one of the door handles the car checks if the associated key is in the "safe" radius. If the key is found, the door is unlocked.

In addition to the integrated normal RKE procedure to lock the car, the PKE system will automatically lock the car if the user carrying the key leaves the "safe" radius.

Figure 3:

RKE/PKE systems actively transmit radio signals and hence need a battery. All systems contain a backup key blade that can be used if battery is drained. Figure 3 contains two keys that are equipped with a PKE system. The aluminium part of the upper key can be removed. The backup blade is attached to it. The second - credit card shaped - key on the picture, shows the backup key blade slid out half way.

2.4 Keyless go systems

PKE systems are often combined with "keyless go" systems. A keyless go system removes the need for a normal ignition lock. Once the driver has entered his vehicle using one of mentioned entry systems, he can start and stop the engine without inserting a physical key into the ignition lock. The engine is started by pushing a button, rather than turning a key.

When the engine is started, the electronic control unit (ECU) will check if one of the associated car keys is available in the car. If one of the associated keys is found within the car, the immobiliser is disabled and the car is started.

Keys containing the keyless go system are generally named "SmartKeys", although, every manufacturer has its own name for it [33].

2.5 Future systems

All systems covered in the last subsections are currently used in the field. Several manufacturers announced new prototypes:

Figure 4:

In October 2008 NXP Semiconducters and BMW Group Research and Technology published the first multi-functional car key [29]. The new prototype uses the SmartMX P5CD081 series wireless chipset. It is compatible with the EMV (Europay Mastercard VISA [12]) electronic payment standard. It contains a dedicated cryptographic coprocessor. The same chipset is being used for the ePassport [28]. The car key has the following features:

- *Contactless payment using RFID.* This feature replaces the need for cash or additional cards. The payment technology can be used for ad-hoc transactions including general shopping, paying for petrol, public transport ticketing, parking and road tolls.
- *Personalised access control.* Stores the position of the seat and steering wheel in the key. Other personal settings that can be thought of are: radio presets and GPS navigation destinations.
- *One key for multiple cars.* The key can be temporarily registered with other cars. Renting or sharing cars becomes much more convenient this way. Personalised settings can be activated in the other car(s).

Other manufacturers are also working on new car "entry and go" systems. Lots of development seems to go into using different channels for communication between car and key, such as Bluetooth and ZigBee. In addition, there is a tendency to integrate more and more multimedia features into a car and the associated keys. This adds another dimension to the use of the key as an authorisation device to one of personalisation and customisation of vehicle functions.
Mazda introduced a concept car which has a USB stick integrated in the car key [24]. The car itself has an integrated hard drive. The USB key can be used to store personal settings, just like the key that was announced by NXP/BMW. Additionally, the key can be used to store multimedia files onto the car. Figure 4 displays a key equipped with an SD card, figure 5 displays an USB enabled car key.

Figure 5:

Sony Ericsson collaborated with Saab to enhance their concept car - the Saab 9-X BioHybrid - with Bluetooth [11]. A phone application pairs the with the car via Bluetooth and allows the vehicle owner to remotely control several functions using the phone's touchscreen:

- Control ambient lightning
- Control front and rear seat settings
- Lock the car
- Open the tailgate
- Switch the head lights and blinkers on and off

A similar example of such cooperation is a mobile phone with intelligent key that has been put together by Nissan, NTT DOCOMO, and Sharp.[9].

3 System architecture

To really understand the various attack routines as well as the requirements for any countermeasures to these attacks, we need to develop a more abstract view of the system and decompose it into its functional components:

- **Transmitter**. The transmitter of the RKE system is the car key itself[1].
- **Medium**. The medium that is used by transmitter and receiver is the air between them.
- **Receiver**. The receiver of the signal is the car. The car can contain various kinds of antennas to intercept signals.

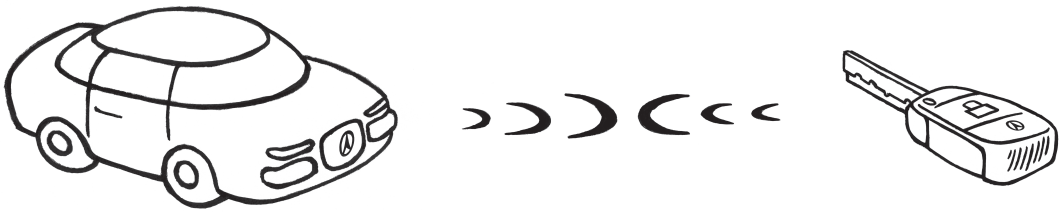

Figure 6: Car, transmission medium, and key

There is also the process of ordering a new or spare key. This procedure can be subdivided into the following components.

- **Requesting party**. The owner of the vehicle who is requesting a new or spare key.
- **Relaying party**. The party that relays the request from the vehicle owner to the issuing party (e.g. a dealer).
- **Medium**. The medium that is used by the requesting and issuing party. Examples of this medium are the Internet, phone, or fax.
- **Issuing party**. The party that is issuing the new/spare key set (e.g. car manufacturer).

Figure 7: Requesting party, relaying party, medium, and issuing party

[1]Nowadays both the key and the car can transmit and receive signals. For historic reasons however the key is still considered a transmitter and the car a receiver.

4 Requirements

The CIA triad is generally accepted as the base of information security for over twenty years [17][25][27]. The triad is built up out of three key concepts, namely: confidentiality, integrity and availability. Integrity can be split up into: data integrity, accountability, authenticity, and authorisation.

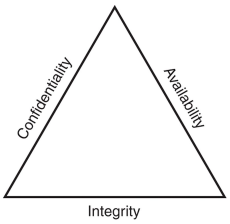

Figure 8: CIA triad

- **Confidentiality**. Confidentiality is the property of preventing disclosure of information or access to parts of the system to unauthorised entities. Entities that are authorised to access information or a specific part of the system, should be the only ones having access to it.
- **Integrity**. Integrity deals with the prevention of unauthorised modification of information, either intentional or by accident. It can be split up in the following four parts:
  - **Data integrity**. This means protecting data from being tampered with by unauthorized entities.
  - **Accountability**. All actions should be traceable to the entity that committed them.
  - **Authenticity**. Authenticity means that information and the system itself is genuine (authentic).
  - **Authorisation**. Takes place *after* authentication, and deals with different roles.
- **Availability**. Availability defines that the system must be available when it is needed.

5 Threat identification using STRIDE

This section covers the threat identification based on the STRIDE model [5]. This model describes the following six threat categories:

- **Spoofing identity**. Cloning or stealing any entity of the system.
- **Tampering with data**. Unauthorised modification of information used in the system.
- **Repudiation**. The fact that an entity can deny that it performed an action. Since this is unwanted, the goal is to establish the opposite: *non-repudiation* – the ability to prove that the entity *did* perform the action.
- **Information disclosure**. The threat of leaking information in any way.
- **Denial of service (DoS)**. DoS attacks render a service unavailable when it is needed.
- **Elevation of privilege**. An unprivileged user that gains privileged access to the system. This user may gain sufficient access to compromise or destroy the entire system.

These categories can be mapped perfectly to the extended CIA model for IT security, covered in section 4. Table 1 shows this mapping.

	Confidentiality	Accountability	Authenticity	Authorisation	Data integrity	Availability
Spoofing identity			✓			
Tampering with data					✓	
Repudiation		✓				
Information disclosure	✓					
Denial of service						✓
Elevation of privilege				✓		

Table 1: CIA model vs STRIDE model

The following subsections cover attacks which are created by structurally mapping each item from the STRIDE model to the items of the system architecture (car, medium, key, and key order procedure).

5.1 Spoofing identity

STRIDE defines *spoofing identity* very broadly, and covers cloning or stealing any entity of the system. Possible threats to each of these entities are listed below:

Spoofing related threats regarding the **transmitter** (key) are:

- Unauthorised usage. This is especially important if a payment system is integrated into the car key.

Spoofing related threats regarding the **medium** (air) are:

- Replay and relay attacks. These attacks may be the most common because the medium that is used: air, is freely accessible for everybody that is located in the area covered by the signal.

Spoofing related threats regarding the **receiver** (car) are:

- A spoofed receiver may be used to collect signals from keys. These signals may be used to open the real car to which the key is associated.

Spoofing related threats regarding the **new/spare key order procedure** are:

- Spoofing the identity of the requesting party to request a key for a specific car.
- Unauthorised retrieval of a master key that is used to generate car keys. An algorithm may be used to generate car keys based on the VIN number [2].

5.2 Tampering with data

As described in section 5, *tampering with data* covers all unauthorised modification of information used in the system.

Threats related to tampering with the **transmitter** (key) are:

- Not applicable (since the key already works, any tampering with it could only result in the key not working any more).

Threats related to tampering with the **medium** (air) are:

- Not applicable.

Threats related to tampering with the **receiver** (car) are:

- Unauthorised altering of the receiver. The receiver stores keys codes that are able to open the car. Tampering could be achieved by introducing rogue key codes.

Threats related to tampering with the **new/spare key order procedure** are:

- Breaking into the manufacturer's key database and altering it. An example of this is adding a backdoor key which is added to every newly produced ECU. The attacker is then able to open every car that is produced. Another example is altering the database or production process so that none of the produced ECUs is associating the right key-pair.

5.3 Repudiation

As described in section 5, *repudiation* is the fact that an entity can deny or cannot prove that it performed an action.

Repudiation related threats regarding the **transmitter** (key) are:

- Suppose that assets get stolen from a car using a cloned key, and the car keeps a record of the open/close action. Then the owner might have to prove that he did not open the car with his own key. If his own key does not keep track of the performed open/close action then he will not be able to provide this proof.

Repudiation related threats regarding the **medium** (air) are:

- Not applicable.

Repudiation related threats regarding the **receiver** (car) are:

[2] VIN-number: vehicle identification number

- Insurance companies may require evidence of theft when assets get stolen from a car. If the car was opened with a cloned key or by using a relay attack, and the car does not keep any record of open/close actions, there will be no evidence and hence the car owner cannot prove theft.

Repudiation related threats regarding the **new/spare key order procedure** are:

- A car dealer employee can request keys of any car produced by the car manufacturer. He can use these keys to steal the cars to which the key is associated or supply them to third parties, and deny everything.
- A manufacturer employee may be able to access the key code database and supply the retrieved information to third parties, and then deny everything.

5.4 Information disclosure

As described in section 5, *information disclosure* is the threat of leaking information in any way.

Threats related to information disclosure regarding the **transmitter** (key) are:

- Retrieval of personal information through scanning for available transmitters in an area. It may be possible to identify your car brand and type by identifying the technology that is used in the transmitter.
- Cryptanalysis. Excessive use of the transmitter may leak information that can be used to do cryptanalysis, which might open up the system to several other threats such as spoofing or tampering with data.
- Cloning of keys in all imaginable ways. Examples of methods that can be used are raw copying and side channel attacks (e.g. differential power analysis).

Threats related to information disclosure regarding the **medium** (air) are:

- Insecure communication between the transmitter (key) and receiver (car) (e.g. the use of weak or no encryption).

Threats related to information disclosure regarding the **receiver** (car) are:

- Retrieval of keys that are associated to a receiver. If the storage of the receiver is not properly secured, it is possible to retrieve a list of associated keys.

Threats related to information disclosure regarding the **new/spare key order procedure** are:

- Insecure communication used between the requester (dealer) and the supplier (car manufacturer) when ordering a new/spare key. It may be possible to eavesdrop on the request of the new key. The retrieved information can be used to intercept the key during the delivery process.

5.5 Denial of service

As described in section 5, *DoS* attacks render a service unavailable.

DoS related threats regarding the **transmitter** (key) are:

- Key battery drainage. Excessive use may cause the battery to drain. This is worsened by the application of advanced cryptography, which uses more power.
- Altering the key in a way that would cause it to stop working, for instance by using physical force or burning out the chip with a strong burst of radiation.

DoS related threats regarding the **medium** (air) are:

- Interruption of the communication channel. This may be done using a jammer. This device sends a very strong signal of the same frequency so that regular communications will fail.

DoS related threats regarding the **receiver** (car) are:

- Tampering with the receiver equipment installed in the car (e.g. altering the ECU in such way that the system stops working).
- Tampering with the power source so that the ECU stops working.

DoS related threats regarding the **new/spare key order procedure** are:

- Physically destroying important parts of the new/spare key production process.
- Interrupting the communication channel between requesting (dealer) and issuing party (car manufacturer).

5.6 Elevation of privilege

As described in section 5, *elevation of privilege* means that an unprivileged user gains privileged access to the system. The user may gain sufficient access to compromise or destroy the entire system.

Threats related to elevation of privilege regarding the **transmitter** (key) are:

- If the car key has any additional functionalities integrated into it, they may be abused due to the use of weak authentication/authorisation.

Threats related to elevation of privilege regarding the **medium** (air) are:

- Not applicable.

Threats related to elevation of privilege regarding the **receiver** (car) are:

- It may be possible to use custom key association equipment to associate rogue keys to the car.

Threats related to elevation of privilege regarding the **new/spare key order procedure** are:

- Users may be able to order keys for which they were not authorised if the order procedure is not secured adequately.
- Employees of the car dealer may be able to use the key association equipment to associate rogue keys to customer cars.

6 Mitigating measures

Practical requirements are formulated for the keyless "entry and go" system and the spare/new key order procedure. The requirements in the next sections are based on both the CIA (section 4) and STRIDE model (section 5), as well as the possible threats covered in section 5.

There can be different sets of practical requirements depending on the environment in which it is being operated or the available budget. A basic set of requirements is formulated that should be seen as mandatory for all situations. Additional requirement sets - each with a different level of security - may be applicable in some situations.

6.1 Spoofing identity

As covered in section 5, "spoofing identity" is linked to "authenticity" from the extended CIA model. Authenticity ensures that information and the system itself is genuine (authentic). The following practical requirements should be taken to defend the system against the attacks covered in section 5.1.

Requirements for the **transmitter** (key) are:

- 1.1.1 The vehicle owner should authenticate himself to the key before using it. If the key has any additional functionalities like a payment system integrated to it, authorisation should also be used.
- 1.1.2 It should not be possible to clone a car key. It should be resistant against cloning methods like raw copying or side channel attacks like differential power analysis.

Requirements for the **medium** (air) are:

- 1.2.1 It should not be possible to reuse (replay) a stored communication pattern used to change the state of the car locks.
- 1.2.2 It should not be possible to relay a signal between the key and the car via different channels, especially not when a keyless "entry and go" system is being used.

Requirements for the **receiver** (car) are:

- 1.3.1 The key should request authentication from the ECU before performing any sensitive operations. This way the key knows that it is talking to the right ECU and hence the right car.

Requirements for the **new/spare key order procedure** are:

- 1.4.1 Only approved dealers should be able to order new/spare car keys.
- 1.4.2 A secure connection should be used between the requesting and issuing party. In the case of web based communication cryptography (HTTPS) should be used.
- 1.4.3 When approving a dealer, a static key delivery address should be agreed on. A rogue key request will not result in the key being sent to a custom address of the attacker.
- 1.4.4 Delivery should be into a secured mail box, separated from the normal mail OR the delivery should be accepted and signed by the employee who issued the request.
- 1.4.5 It should not be possible to break into the manufacturer's key database and read its content.

6.2 Tampering with data

As covered in section 5, "tampering with data" is linked to "data integrity" from the extended CIA model. Data integrity ensures that integrity of information is guaranteed at all times. The following practical requirements should be taken to defend the system against the attacks covered in section 5.2.

Requirements for the **transmitter** (key) are:

- 2.1.1 The key should be physically designed so that it is not possible to change the information stored on it.

Requirements for the **medium** (air) are:

- 2.2.1 Not applicable.

Requirements for the **receiver** (car) are:

- 2.3.1 The ECU should be installed in a safe place inside the car and not be accessible without entering the vehicle or opening the bonnet.

Requirements for the **new/spare key order procedure** are:

- 2.4.1 In addition to 1.4.5, it should not be possible to break into the manufacturer's key database and change its content.

6.3 Repudiation

As covered in section 5, "repudiation" is linked to "accountability" from the extended CIA model. Accountability deals with recording information about events. The following practical requirements should be taken to defend the system against the attacks covered in section 5.3.

Requirements for the **transmitter** (key) are:

- 3.1.1 The key should be equipped with logging functionality. These logs will show what cars were opened and closed, which can be used as evidence for insurance companies.

Requirements for the **medium** (air) are:

- 3.2.1 Not applicable.

Requirements for the **receiver** (car) are:

- 3.3.1 The car should be equipped with logging functionality. These logs will show what keys were used to open and close the car, which can be used as evidence for insurance companies.

Requirements for the **new/spare key order procedure** are:

- 3.4.1 A dealer employee should not be able to order keys on his own. At least two different employees should authorise key orders (four-eye principle).
- 3.4.2 The manufacturer back-end systems should log all key related actions.

6.4 Information disclosure

As covered in section 5, "information disclosure" is linked to "confidentiality" from the extended CIA model. Confidentiality ensures that disclosure of information or access to parts of the system to unauthorised entities is prevented. The following practical requirements should be taken to defend the system against the attacks covered in section 5.4.

Requirements for the **transmitter** (key) are:

- 4.1.1 The key should have a rate limiting mechanism to deny excessive use of the transmitter unit. This to prevent the ability to conduct cryptanalysis on the key.
- 4.1.2 As an addition to requirement 2.1.1, information on the key should not be readable by equipment other than the key itself. This is to prevent side channel attacks.
- 4.1.3 See requirement 1.3.1.

Requirements for the **medium** (air) are:

- 4.2.1 The communication between key and receiver should not disclose any information.
- 4.2.2 The mechanism to secure communications should be designed so that it will be secure during the entire lifetime of the car. This could be done by anticipating on future developments in computing power. Another option is to have an updating mechanism in place.

Requirements for the **receiver** (car) are:

- 4.3.1 In addition to the requirement from 2.3.1, it should not be possible to retrieve information about associated keys from the ECU.

Requirements for the **new/spare key order procedure** are:

- 4.4.1 See requirement 1.4.2.

6.5 Denial of service

As covered in section 5, "denial of service" is linked to "availability" from the extended CIA model. Availability ensures that a system can actually be used for its intended purpose. The following practical requirements should be taken to defend the system against the attacks covered in section 5.5.

Requirements for the **transmitter** (key) are:

- 5.1.1 The key should have a backup non-electrical mechanism to open and start the car, in case of a battery problem, interference with other keys, or when signal jamming equipment is used.
- 5.1.2 The battery unit of the key should be replaceable.
- 5.1.3 A nice to have, though not mandatory feature is an in-vehicle battery charging mechanism to charge the key battery while driving.
- 5.1.4 The key should have a rugged design.

Requirements for the **medium** (air) are:

- 5.2.1 The medium should be resistant against denial of service attacks or at least have a mechanism that detects denial of service. This mechanism should be built into the key. The owner should be alerted if the vehicle does not respond to the key.

Requirements for the **receiver** (car) are:

- 5.3.1 The antennas of the receiver and the power source of the car should be installed in a location which is not accessible from the outside of the car (without opening the bonnet).
- 5.3.2 See requirement 2.3.1

Requirements for the **new/spare key order procedure** are:

- 5.4.1 It should not be possible to interrupt the communication channel between the requesting and issuing party. This could be in the form of a backup communication channel using a different medium.

6.6 Elevation of privilege

As covered in section 5, "elevation of privilege" is linked to "authenticity" from the extended CIA model. Authorisation deals with different roles that are assigned after authentication. These roles grant or deny permission to an entity for a specific function or part of the system. The following practical requirements should be taken to defend the system against the attacks covered in section 5.6.

Requirements for the **transmitter** (key) are:

- 6.1.1 See requirement 1.1.1.

Requirements for the **medium** (air) are:

- 6.2.1 Not applicable.

Requirements for the **receiver** (car) are:

- 6.3.1 See requirements: 6.4.2-7

Requirements for the **new/spare key order procedure** are:

- 6.4.1 A vehicle owner should identify himself when ordering a new key. In addition, he has to prove that the car for which he is ordering the key, belongs to him. Ownership can be checked through the registration certificate of the car.
- 6.4.2 No undocumented authorisation codes or *back doors* should exist that give full access to the ECU.
- 6.4.3 Every ECU should be accessible by using a unique code.
- 6.4.4 Different authorisation levels should be used in the ECU, e.g. for engine maintenance/-monitoring and security functions.
- 6.4.5 The authorisation codes to access the security functions of the ECU should not be delivered together with the car. If this code is needed, it should be possible to request it through the manufacturer's (or importer's) back-end. To make this process even more secure, the ECU could be equipped with a one-time-password system, so that the password or PIN can only be used once. This way it is clear who accessed the ECU's security functions and when (in combination with requirement 3.4.2).
- 6.4.6 Key association equipment should be connected to the manufacturer's back-end during usage. This way the configuration of every ECU is logged at the back-end.
- 6.4.7 Not all car dealer employees should be able to request a code to gain access to the ECU's security functions. Different roles should exist that can perform different tasks on the back-end.
- 6.4.8 See requirement 3.4.1.

7 Examining current situation

As covered in section 1.1.1, research is conducted on several topics related to the security of car keys and the secureness of the new/spare key order procedure.

Section 7.1 covers the research into the hardware that is being used by the different car manufacturers in their keys. We chose to investigate the top 10 car brands based on the 2008 sales numbers[2]. We added some alternative brands which we thought would use a different system.

The researched hardware will be assessed against our the requirements in section 7.2. Section 7.3 covers the assessment of the key order procedure against the requirements. Section 7.4 covers the manufacturer's view on the Kerckhoffs principle [19].

7.1 Key properties

To determine if the requirements regarding the car and keys are met, we first need to know the technical details of car keys used by every car brand. We assume that not every car brand uses its own specific technology, but that there are instead a few chip manufacturers that sell products to several car manufacturers.

We visited several major brand car dealers, where we interviewed service personnel and examined the imprinted codes on different car keys. After explaining the goal of our research, most dealers were willing to cooperate.

Dealers do not have detailed information about the inner working of car keys at their disposal. They do not need this information because it does not have any added value for them. If a car key or ECU does not work, it is simply replaced by a new one.

For detailed information, all dealers redirected us to the importer/distributer of their car brand or to the main factory. Unfortunately none of the importers was willing or able to cooperate.
Table 7.1 contains information about the used systems collected while conducting the interviews at the car dealers and looking at numerous car keys.

Brand	Example imprint information	Transponder brand	Frequency
Audi	`4D0 837 231K`	Hella	433/315 MHz
BMW			
Citroën	`BF433`	Delphi	433 MHz
Fiat	`210401,5105`	TRW	
Ford	`5WK4 725/8686 (frq1)` `5WK4 8025 (frq2)`	Siemens	433 MHz
Honda	`800 87-A` `12147-SMG-E110-M1`	Valeo	

Hyundai	`Transmitter Assy (PA) HA-T001`
	`FCC ID: PINHA-T001 CMII`
	`ID: 2007DJ0420 v1.0, S/N: 00000`
	`Hyundai Autonet/made in Korea`		

Mazda	`5WK43449E` `HP433Mhz 092609`	Siemens	433 MHz
Mercedes			433 MHz
Opel	`G3 AM433TX v1.0` `13189118`	Delphi	433 MHz

Peugeot [3]	`HF433 ASK indice S 31/10/07`
	`HF433 ASK indice U 09/06/08`
	`HF433 F8K Indice J 25/03/09`
	`HF433 ASK Indice T 11/12/07`
		Delphi	433 MHz

Peugeot [4]	`HF434 21674002-9 ED13 13/07/07`
	`HF434 28113204-4 ED13 03/07/07`
	`HF434 28119725-6 ED10 09/04/09`
		JCAE	434 MHz

Renault		JCI	433 MHz
Seat	`HLO 1J0 959 753CT` `5FA 009 259 00`	Hella	433 MHz
Toyota		Tokai Rika	
Volkswagen		Hella	434 MHz
Volvo	`SWK49259 SIEMENS VDO 8D23`	Siemens-VDO	

Even with various blank spots in the table it is clear that several car manufacturers indeed use chipsets from the same company. We contacted these vendors to obtain further information on their products. We were especially interested in what security techniques are used (if any), and in which cars the products are used. However, none of the vendors was willing to disclose any information related to the security of their products.
After further investigation on the chipset brands, we discovered the following additional information:

- Car brands that use 433 or 434 MHz actually are using 433.92 MHz as their center frequency. This is the center frequency of the range 433.05–434.79 MHz, specified in the industrial, scientific and medical (ISM) band [31].
- Both JCI and JCAE are abbreviations for the same company, namely: Johnson Controls Inc. [15].
- All systems labeled with Siemens or Siemens-VDO are part of Continental AG [1].

[3] Models 607, 407SW, 308CC, 307CC
[4] Models 208, 207CC, 3008

7.2 Assessing discovered systems

Requirement	Audi	BMW	Citroën	Fiat	Ford	Honda	Hyundai	Mazda	Mercedes	Opel	Peugeot	Renault	Seat	Toyota	Volkswagen	Volvo
Key uses authentication (1.1.1)	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Key uses authorisation (1.1.1)	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Clone protection (1.1.2)																
Side channel attack protection (1.1.2)																
Replay protection (1.2.1)																
Relay protection (1.2.2)																
Key requests authentication from ECU (1.3.1)	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Key is read only (2.1.1)	+	-[5]	+	+	+	+	+	+	+	+	+	+	+	+	-[6]	+
Key is not readable by other devices (4.1.2)		-[5]		+	+	+	+	+	+	+	+	+	+	+	+	-
Key is rugged (5.1.4)	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ECU installed in a tamper-proof place (2.3.1)	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
Key has logging functionality (3.1.1)	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Car has logging functionality (3.3.1)	-	+	-	-	-	+	-	-	+	-	-	-	-	-	+	-
Key does rate limiting (4.1.1)																
Key-car communication is secured (4.2.1)	+[7]	+[7]	+[7]	+[7]	+[7]		+[7]	+[7]	+	+[7]		+	+[7]	+[7]	+[7]	
Security mechanism outlives car lifetime (4.2.2)																
Key security mechanism can be updated (4.2.2)	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
ECU is protected against key read-outs (6.4.2-7)	+	+	+[8]	+[8]	+[8]		+[8]	+[8]	-	+[8]	+[8]	+[8]	+[8]	+[8]	+	+
Key has non-electrical backup (5.1.1)	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
Key battery is replaceable (5.1.2)	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
In-vehicle key battery charge method (5.1.3)	-	+	-	-	-	-	-	-	-	-	-	-	-	-	+	-
Key gives alert if vehicle does not respond (5.2.1)	-	+	-	-	-	-	-	-	-	-	-	-	-	-	+	-
Car battery in a tamper-proof place (2.3.1)	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+

Table 2: Key requirements results

[5] Diagnostic data is written to the key every 5 minutes, which can be read by dealer equipment.
[6] Key contains user preferences such as steering wheel and chair position.
[7] "Rolling code", which indicates that KeeLoq "Code Hopping Mode"[8] is used.
[8] Not applicable because no logging takes place.

7.3 Key order procedures

In order to investigate the key order procedure, we followed the same procedure: visit major brand car dealers and interview their personnel. The basic procedure seems to be similar for most car brands:

1. The vehicle owner requests a new key at a dealer.
2. The dealer orders the new key or key set.
3. Manufacturer makes the key and sends it to the dealer.
4. Dealer reprograms ECU to accept the new key or key set.

It turns out that the shape of the physical key is linked to the car's VIN. Therefore any key generating party needs to have the database or algorithm that enables them to carve the right physical shape. Once this is done, the key can be used to open the vehicle by physically putting it in one of the locks. It is not possible to start the car using this newly created physical key because the immobiliser – which is located inside the key – is not yet known by the car.

The electronic IDs of the key - the immobiliser and/or RKE/PKE ID - have to be associated to the car. This is done by programming both IDs into the car's ECU ('learning') which is mostly done by dealers using special handheld devices. More and more dealers are replacing these special handheld devices by regular laptops.

Several dealers use a third party company to order keys. Three of such companies were mentioned during the interviews: Jutkey[9], Car Lock Systems [10], and EuroKey[11].
Jutkey is a key maker which is making key fobs for business customers as well as normal private customers.
Car Lock Systems is a key maker which specialises in car key fobs. Only official car brand dealers, or dealers certified by FOCWA[12]/BOVAG [13] are able to order keys at Car Lock Systems. For several brands it is possible to order keys just by VIN.
Every dealer has his own username and password (authentication) which grants the dealer access to his private area where he can order keys of the car brands he is allowed to (authorisation). The login page uses normal HTTP which sends the username and password in plain text over the Internet. Dealers can request key codes associated to VIN numbers for at least Citroën, Hyundai, Mazda and Peugeot.
The following section contains information specific to the key order and association procedure of each car brand.

1. **Audi**. All keys are ordered at the manufacturer. All security related operations require a network connection with the manufacturer.
2. **BMW**. All keys are ordered at the manufacturer. All security related operations require a network connection with the manufacturer.
3. **Citroën**. Keys are either ordered at the manufacturer, but mostly via third party Car Lock Systems.
4. **Fiat**. Keys are ordered exclusively at Car Lock Systems.
5. **Ford**. Network connection needed to learn key to ECU. Keys are ordered at manufacturer or ordered at Jutkey.
6. **Honda**. All keys are exclusively ordered via third party Eurokey. ECU does not use any PIN code.
7. **Hyundai/Seat**. All keys are ordered via Car Lock Systems.

[9] Jutkey, Amsterdam. http://www.jutkey.nl
[10] Car Lock Systems, Sleeuwijk. http://www.carlock.nl
[11] Eurokey, Eindhoven. http://www.eurokey/nl
[12] FOCWA: "Federatie van Organisaties in de Carrosserie- en Wagenbouw en Aanverwante bedrijven".
[13] BOVAG: "Bond van Autohandelaren en Garagehouders".

8. **Mazda**. There are no ECU PIN codes, instead the ECU gives a challenge (OUT code) that needs to be typed in at the manufacturers intranet site. This will give a response code (IN code) that needs to be typed in on the dedicated equipment connected to the car. Keys are ordered exclusively at Car Lock Systems.
9. **Mercedes**. All keys are ordered at the manufacturer. All key related procedures require an online connection with the manufacturer.
10. **Opel**. Sometimes key are ordered at the manufacturer, sometimes at Car Lock Systems. ECU programming requires hardware dongle.
11. **Peugeot**. Keys are ordered exclusively at Car Lock Systems.
12. **Renault**. Network connection needed to learn key to ECU.
13. **Toyota**. This is different than all the order brands that we investigated. With each Toyota come two keys: one black master key, and one grey regular key. New keys are cut using the VIN, and can be learned by the ECU with the master key. One very important implication of this system is that if the master key is lost, there is no way of adding any extra keys to the car. You can still use the car with any regular keys, but if that one is lost you will have to replace the entire ECU and all the locks, which is a very costly operation. The problem is worsened because most car owners are under the impression that the grey key is the master key, and drive around using the black key. If they misplace that they are in for an expensive surprise. Another thing that is different is that you can add keys one at time, you do not need to program all the keys together in one go. Recently the 'standard way' of learning keys by connecting dedicated equipment to the ECU is used. The intranet web site that is used to order spare parts and keys is also used to order keys.
14. **Volkswagen**. All keys are ordered at the manufacturer. All security related operations require a network connection with the manufacturer.
15. **Volvo**. All keys are ordered at the manufacturer. All security related operations require a network connection with the manufacturer.

Requirement	Audi	BMW	Citroën	Fiat	Ford	Honda	Hyundai	Mazda	Mercedes	Opel	Peugeot	Renault	Seat	Toyota	Volkswagen	Volvo
Only access for approved dealers (1.4.1)	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
Secure connection during request process (1.4.2)		+	+-[14]	-	+-[14]	-	-	-	+	+-[14]	-	+	-	+	+	+
Static key shipping address (1.4.3)	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
Delivery to secured mailbox (1.4.4)	-	-	-	+	+	+	+	+	+	+	+	+	+	+	-	-
Secure key database (1.4.5)																
Four-eye principle key order procedure (3.4.1)	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Back-end key association logging (3.4.2)	+	+	-	+	+	-	-	-	+	+	-	-	+		+	+
Backup medium for request process (5.4.1)	+	-	+	+	+	+	-	-	+	+	+	+	-	+	-	-
Vehicle owner identification (6.4.1)	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
Back-door ECU authorisation codes (6.4.2)	-	-	-	-	-	-	-		-	-	-	-	-	-	-	-
Unique code for each ECU (6.4.3)	+	-	+	+	+	-[15]	+	-[15]	-[16]	+	+	-[15]	+	-[15]	-[16]	-[16]
Different ECU authorisation levels (6.4.4)	-	-	-	+		-[15]	+	-[15]	-[16]	+	+	-[15]	+	-[15]	-[16]	-[16]
ECU access code delivered with car (6.4.5)	-[16]	-[16]	+	+	+	-[15]	-	-[15]	-[16]	+	+	-[15]	-	-[15]	-[16]	-[16]
ECU one-time access codes (6.4.5)	-[16]	-[16]	-	-	-	-[15]	-	-[15]	-[16]	-	-	-[15]	-	-[15]	-[16]	-[16]
Online key association equipment (3.4.2)	+	+	-	-	+	-	-	+[17]	+	-	-	+	+	-	+	+
ECU configuration logged at back-end (6.4.6)	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ECU modifications logged at back-end (6.4.6)	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
Dedicated key request employees (6.4.7)	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+

Table 3: Key order requirements results

[14] Mixed situation: sometimes keys are ordered via manufacturer, sometimes via third party.
[15] No ECU code at all.
[16] Network connection with manufacturer is needed.
[17] Semi-online: challenge/response, entered manually in reading device and back-end system.

7.4 Manufacturer view on Kerckhoffs principle

We tried to find out what the reason was for the chipset manufacturers refusal to give security information on their products, by asking them this question:

> In case you cannot answer some of our questions, we would like to have a short reaction on the Kerckhoff principle:
>
> "A Cryptosystem should be secure even if everything about the system, except the key, is public knowledge."

Only Hella gave an actual answer:

> "If everything, except the key, is known, a car would become unsecure very soon due to the fast growing computing power of IT technology compared to automotive technology and their life cycle."

8 Recommendations

Based on the assessment covered in chapter 7 we have several recommendations to improve overall security. The following recommendations deal with the keys:

- Implement PIN codes on keys. This way stolen keys will not lead directly to a stolen car.
- Implement logging facilities in both key and car. This will enable car owners to prove what actions they performed, or what actions were performed on the car.
- Equip the key with a rechargeable battery and implement an in-vehicle battery charge mechanism. This prevents battery drainage and thereby DoS attacks.
- Let the key signal the user if the car did not respond. This helps reducing the effect of jammers in keeping the car unlocked.
- All systems used to gain access to the car should be certified by an independent party. This might be done by a European-wide organisation.
- The market should consolidate to less but better solutions. We already saw that some of the car brands use the same end manufacturer of key hardware.

The following recommendations deal with the key ordering process, the key association process and back-end systems:

- Use secure connections for online ordering of keys. None of the third party key manufacturers (e.g. Car Lock Systems) use HTTPS, but it is trivial to implement and costs practically nothing.
- Change processes to enforce the 'four-eye principle' when ordering keys. This prevents rogue employees from ordering keys without someone else knowing about it.
- Personalised dealer employee accounts should be used in the back-end, instead of global dealer accounts. This way a key request can be associated to a single employee, rather than a dealer.
- Design the ECU with different access levels so that different roles can be used (e.g. for engine related maintenance and the key association procedure).
- Use network enabled key association equipment. Some manufacturers already require connecting to their back-end systems when associating keys to a car. This can be used to store changes to the security functions of the car in the back-end, and also prevents unauthorised changes to the ECU.

9 Considerations

Some things not directly related to our research qustions became evident.

9.1 Keys by default have limited utility

In almost all cases if someone is able to obtain a valid key this key will be able to open the doors only. In order to actually use the car and drive away the keys will have to be programmed into the car. We have seen a tendency to make this programming dependent on a network connection with the manufacturer. This way the intelligence is moved to a central place, which is easier to manage and is less prone to abuse. Several of the high-end car brands (BMW, Mercedes, Audi, VW) employ such techniques already, and several mid-range brands will implement this in the near future.

9.2 Do insurance companies refund theft of assets?

Section 6.3 covers a threat in which the car is unlocked by using a relay attack. Insurance companies may require physical evidence of theft when assets get stolen from a car. If an attack is used in which the car is opened through radio frequency, there are no physical signs of break in. In fact, even a jamming device could be used to block the owner from locking his car using any of the remote's buttons. If the car, nor the key, log state changes of the locks, the car owner can not prove that he really closed his car. Insurance companies may require this evidence.

We called several Dutch insurance companies to ask if physical evidence of theft is needed to get a refund of stolen assets.

- **OHRA**. Does not refund stolen assets if the car owner in question can not prove the theft.
- **Centraal Beheer Achmea**. No physical signs of entry needed, they always refund.
- **Interpolis**. No physical signs of entry needed, they always refund.

Below a quote from the conditions as utilised by OHRA.

> 1. *File a report at the police.*
> 2. *Signs of physical break-in of the car are not mandatory in the conditions, though if not present the insured party has to prove or to make plausible that the theft actually happened. If the insured party can not prove the theft, no refund will be done. If the car was not locked, the user has been careless. This is an exclusion in the conditions and no refund will be done.*

The conditions by OHRA stated above show that logging on both the key and the car are necessary. This way the vehicle owner can prove that he closed his car at a certain point in time. In addition to the the logging functionality, the key should notice if the car is not reachable/responding when an attempt is made to close to car. This way, the user is alerted that the car is not actually locked.

9.3 Microchip statements on KeeLoq

As mentioned in 1.3, several weaknesses have been discoverd in KeeLoq, the cipher that is used to secure communications in RKE/PKE system. Microchip made a public statement about this on their website:

> *Microchip Technology Inc., a leading provider of microcontroller and analog semiconductors, today announced that, after a thorough evaluation of recent claims made by cryptographic researchers, the Company concluded that its KEELOQ ©security system, in its recommended real-world implementation, is secure. Microchip recognizes that the highly talented researchers have been successful at a theoretical attack of a*

> *block cipher. However, the KEELOQ security system implementation involves much more than just the cryptographic algorithm. The researchers' claims that vehicles can be stolen, based on their cryptographic findings related to the KEELOQ algorithm, are incorrect due to several mistaken assumptions.*
>
> *Microchip does not believe a public debate on how to steal vehicles benefits consumer security. In addition, for reasons of customer confidentially, Microchip cannot disclose specific information regarding the errors in the claims being made.*

In addition to the RKE/PKE systems, cars also use an immobiliser, so the claim that cars can be stolen with breaking only the RKE/PKE part does indeed seem to be incorrect.

The second part of the statement is the most interesting. When someone finds flaws in their proprietary technology, Microchip says these claims are incorrect, however they can not say what the real errors are.
Microchip does seem to react however to external developments. Several months after the differential power attacks against KeeLoq in 2008[10] they introduced the KeeLoq 3 [20] development kit:

> *The kit provides new enhanced features over the KeeLoq II system such as a patented secure-learning algorithm that prevents differential power-analysis attack techniques.*

We did not investigate any cryptographic algorithms used by car manufacturers because this is out of the scope of this research project.

10 Conclusion

Reviewing our first research question:

> ***What requirements should a keyless "entry and go" system adhere to?***

Requirements have been set up using the CIA and STRIDE model. One of the most important requirements is the ability do authenticate and authorise the user prior to usage of the key. This is especially important if the key has additional integrated features (e.g. payment functionalities).

Another important requirement that should be adhered to by both the key and the ECU is: logging. Both the key and the ECU should log lock status changes. This information can be used as proof in insurance cases. All formulated requirements can be found in section 6.

Reviewing our second research question:

> ***What systems are currently being used and do they meet these requirements?***

During our research we saw that several car brands use key equipment from the same end manufacturer. Audi, Seat, Skoda, and Volkswagen all use equipment manufactured by Hella. Citroën, Opel, and Peugeot all use equipment manufactured by Delphi. In addition, Peugeot uses an additional manufacturer, namely: JCI, which is also used by Renault. It is not clear why Peugeot uses two different manufacturers. Ford, Mazda, and Volvo all use equipment from Continental, formerly known as Siemens or Siemens-VDO.

We were not able to test all systems in detail because none of the car brands, nor the end manufacturers were willing to supply security related details. Because proprietary systems are being used, it was not feasible to reverse-engineer any of the systems ourselves within the available time period.

None of the keys require authentication/authorisation before use. None of the keys are capable of logging their usage. The majority of the ECUs do not log which key changed the status of the locks. The complete results can be found in section 7.2.

Reviewing our third research question:

> ***What requirements should the new/spare key order procedure adhere to?***

Requirements concerning the new/spare key order procedure have also been set up using the CIA and STRIDE model. One of the most important requirements is the authentication and authorisation concerning the request procedure. A car owner has to prove that he is the rightful owner of the vehicle before a key is ordered. Personalised dealer employee user accounts should be used to request new keys at the manufacturer. The car manufacturer can thereby link all key requests to a person, rather than a dealer.

Another important requirement is the necessity of a connection with the back-end during the new key associating procedure. It should not be possible to associate new keys without a connection to the manufacturer's back-end. This way, the car manufacturer can log all modifications to the security configuration of a car's ECU.

All formulated requirements can be found in section 6.

Reviewing our fourth research question:

What are current order procedures and do they meet these requirements?

The key order and association procedure varies a lot per car brand. Some car brands obligate their dealers to order keys through third parties like Car Lock Systems (e.g. Peugeot and Mazda), others obligate their dealers to only order keys at the manufacturer (e.g. Mercedes and BMW). None of the third parties use HTTPS encryption on their website.

All car dealers require the end user to prove his identity and that he is the rightful owner of the vehicle. None of the car dealers use the four eye principle. If the car dealers use personal employee logins on the back-end, and if the system requires a connection with the manufacturer's network, all key related actions can be logged at the manufacturer's back-end.

Not all car brands require a connection to their back-end network when associating new keys to a car. Such a connection is currently used by: Audi, BMW, Mercedes, Seat, Volkswagen, and Volvo. The complete results can be found in section 7.3.

10.1 Further research

Based on our experiences we think that future research might be done in these areas:

Car key usage

Conduct practical experiments to find out how users actually use their car keys and remote controls. What do they expect from their car and keys? Do they understand what happens, and are they aware of the implications if things do not work as expected?

Relay attacks

Create a Proof of Concept of a relay attacks on a keyless go system. This could be done by relaying the radio signal between the key and the car. It might not be neccessary to do any (de)modulation, which makes the attack easier.

Security certification

Especially in Europe there seem to be a lot of different national regulation on radio frequencies, transmission power, security requirements, and so on. In the Netherlands SCM (Stichting Certificering Motorrijtuigen) is one of the bodies that deals with various aspects of car security regulation. There may be other (European) bodies that do similar things. Investigate what certification institutions exist, what their legal status is, and what the technical relevance of their certification is. Investigate the legal aspects of related topics such as radio frequencies and transmission power. Could it be that a system is legal in one country and illegal in another?

Analyse used cryptography

Investigate what cryptography is used in car-key communication by different car brands and types. Which systems use KeeLoq? Are there other systems in use? This probably means analysing the radio signals because none of the munufacturers wants to disclose information on this.

11 Thanks

While conducting this research project, we received the generous help from the following people, to whom we would like to express our gratitude for their help, information, and guidance:

- Stan Hegt, Pieter Cielen and Hans IJkel (KPMG) for supervising our project.
- Vincent Poeze (www.almostdaily.com) for the artwork.
- Rebecca van Nieuwkerk (Automotive-centre van Nieuwkerk, Amsterdam)
- Paul Abraham (A-point Groep, Amsterdam)
- Michael Westland (Furness Car, Amsterdam)
- Pieter Groeneveld (Arend Auto, Amsterdam)
- Gerard van Dijk (Merel Auto, Amsterdam)
- Mo Bouljir (Ford Amsterdam)
- Herman Brouwer (Mazda Nederland)
- Menno Lambrechts and Cees Hermes (Pouw Peugeot, Amsterdam)
- Louis Antunes (Dirk Barten Amsterdam)
- Sven Ties (Toyota Louwman Amsterdam)
- D. Visbeek (Audi Centrum Amsterdam)
- Stefan Broersen (Maaral BMW, Alkmaar)
- R. Nuisker (A-Point Groep, Amsterdam)
- Wim Blom (Vanderlinden Groep Hyundai/Seat, Waddinxveen)
- Dave van Swam (EMA Automobielgroep/Mercedes, Weert)

References

[1] Continental AG. Continental ag en siemens vdo automotive ag bundelen hun krachten. http://www.conti-online.com/generator/www/be/nl/continental/automobiel/algemeen/corporation/hidden/siemens_take_over_nl.html.

[2] Autoweek. Verkoopcijfers 2008, 2008. http://www.autoweek.nl/verkoopcijfers.php?verkoopjaar=2008.

[3] Andrey Bogdanov. Cryptanalysis of the KeeLoq block cipher. Cryptology ePrint Archive, Report 2007/055, 2007. http://eprint.iacr.org/2007/055.pdf.

[4] Marshall Brain. How remote entry works. http://auto.howstuffworks.com/remote-entry1.htm.

[5] Microsoft Corporation. The STRIDE threat model. http://msdn.microsoft.com/en-us/library/ms954176.aspx.

[6] Nicolas T. Courtois, Gregory V. Bard, and David Wagner. Algebraic and slide attacks on KeeLoq. Cryptology ePrint Archive, Report 2007/062, 2007. http://eprint.iacr.org/2007/062.pdf.

[7] Nicolas T. Courtois, Karsten Nohl, and Sean ONeil. Algebraic attacks on the crypto-1 stream cipher in mifare classic and oyster cards, 2008. http://eprint.iacr.org/2008/166.pdf.

[8] Steven Dawson. Code hopping decoder using a PIC16c56, 1998. http://www.keeloq.boom.ru/decryption.pdf.

[9] NTT DOCOMO. Nissan, ntt docomo and sharp jointly develop world's first mobile phone with built-in intelligent key, 2008. http://www.nttdocomo.com/pr/2008/001415.html.

[10] Thomas Eisenbarth, Timo Kasper, Amir Moradi, Christof Paar, Mahmoud Salmasizadeh, and Mohammad T. Manzuri Shalmani. On the power of power analysis in the real world: A complete break of the KEELOQ code hopping scheme. In *Advances in Cryptology - EUROCRYPT 2008 - 27th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 203–220. Springer Berlin / Heidelberg, 2008. http://www.crypto.ruhr-uni-bochum.de/imperia/md/content/texte/publications/conferences/crypto2008_keeloq.pdf.

[11] Sony Ericsson. Sony ericsson and saab: P1 application interacting with the saab 9-x biohybrid concept car, 8 2008. http://developer.sonyericsson.com/site/global/newsandevents/latestnews/newsaug08/p_saab_uiq3app_conceptcar.jsp.

[12] Visa Europe. Wat is EMV? http://www.visa.nl/visavoorwinkeliers/emv/main.jsp.

[13] Clarence U. Folster. US patent 1329391 - auto-lock, 1920.

[14] M Hobbs. What is an Automotive Keyless Entry Remote System. http://www.articlesbase.com/cars-articles/what-is-an-automotive-keyless-entry-remote-system-456455.html.

[15] Johnson Controls Inc. Jci/jcae website. http://www.johnsoncontrols.com.

[16] Sebastiaan Indesteege, Nathan Keller, Orr Dunkelman, Eli Biham, and Bart Preneel. A practical attack on KeeLoq. In *Advances in Cryptology - EUROCRYPT 2008 - 27th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 1–18. Springer Berlin / Heidelberg, 2008. http://www.cosic.esat.kuleuven.be/publications/article-1045.pdf.

[17] ISO/IEC 27002:2005. *Information technology Security techniques Code of practice for information security management*. ISO, Geneva, Switzerland.

[18] A. Juels. Rfid security and privacy: a research survey, 2 2006. http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=1589116.

[19] Auguste Kerckhoffs. La cryptographie militaire. *Journal des sciences militaires*, IX:5–38, January 1883. http://www.petitcolas.net/fabien/kerckhoffs/crypto_militaire_1.pdf.

[20] Microchip. Keeloq 3 development kit. http://www.microchip.com/keeloq.

[21] N Navet, Y Song, F Simonot-Lion, and C Wilwert. Trends in automotive communication systems, 2005. http://ieeexplore.ieee.org/iel5/5/30937/1435746/1435746.html.

[22] T Nolte, H Hansson, and LL Bello. Automotive communications-past, current and future. IEEE: Emerging Technologies and Factory Automation, 2005. http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=1612631.

[23] T Nolte, H Hansson, and LL Bello. Wireless automotive communications, 2005. http://www-ivs.cs.uni-magdeburg.de/bs/tagungen/paper/rtn05S3_nohalo-WAC.pdf.

[24] LD Paulson. Concept car uses USB, 2005. http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?tp=&arnumber=1556479.

[25] C.F. Pfleeger. *Security in Computing*. Prentice Hall, 1989.

[26] Bill Phillips. *The complete book of locks and locksmithing*. 2005.

[27] D. Russel. *Computer Security Basics*. O'Reilly, 1991.

[28] NXP Semiconductors. Nxp ships 100 millionth epassport chip, 11 2008. http://www.nxp.com/news/content/file_1504.html.

[29] NXP Semiconductors. The world's first "smart" car key prototype, 10 2008. http://www.nxp.com/news/content/file_1487.html.

[30] P Siekerman and M van der Schee. Security evaluation of the disposable ov-chipkaart, 4 2008. http://staff.science.uva.nl/~delaat/sne-2006-2007/p41/Report.pdf.

[31] International Telecommunication Union. What is meant by ISM applications and how are the related frequencies used?, 03 2007. http://www.itu.int/ITU-R/terrestrial/faq/index.html.

[32] T.J. Waraksa, K.D. Fraley, R.E. Kiefer, D.G. Douglas, and L.H. Gilbert. US patent 4942393 - passive keyless entry system, 1990.

[33] Wikipedia. Advanced key. http://en.wikipedia.org/wiki/Advanced_key.

[34] Wikipedia. Remote keyless entry systems. http://en.wikipedia.org/wiki/Remote_keyless_system.