SECURITY OF VEHICLE KEY FOBS AND IMMOBILIZERS

By Anna Richardson

TABLE OF CONTENTS

ABSTRACT

The first use of cryptography in automobiles has been immobilizer chips, since then car manufacturers have added to…. In this paper, I first discuss the use of RFID in immobilizer, then the security of different car types. The majority of the paper is on five attacks that can be used on key fobs and immobilizers. First, is the radio jamming attack where the attacker sends garbage data at the same frequency as the key fob to block the users signal from reaching the car. The result is that the car owner isn't able to lock or unlock the car. Next, the RollJam Wireless Attack. Here the RollJam device similarly blocks the key fob signal from reaching the car, but it also records it. The owner then presses the lock/unlock button again and this code is also stored by the RollJam, but the first code is released and the car locks/unlocks. The attack is then able to use the second code to gain access to the car at will. The third attack is the relay attack which carries the key fob signal over a greater distance such that the attacker can unlock and start the car. The next attack is an attack on the Megamos Crypto transponder. Here, the attack is able to figure out the code needed to unlock and start the car through weaknesses in the cryptography. Last, an attacker can attack the keypad on the driver's code using a long sequence detailed below which must include the password into the vehicle.

1. INTRODUCTION

In the 1990's, the government put pressure on car manufacturers to improve the security of vehicles. Thieves could steal cars very easily by hotwiring, making a copy of the key, or by other means. The first use of cryptography in cars is the placement of immobilizer chips based on RFID technology in key fobs. The first immobilizer alarm system was invented and patented in 1919 by St. George Evans and Edward Birkenbeuel[1]. Many car manufacturers started in producing cars with immobilizers chip in 1995. Immobilizers became mandatory in all new cars sold in German since

January 1, 1998 and in Canada since January 2007[2]. After the installation of immobilizers, there was a great decline in car theft. As car manufacturers install more technology and software into the car for security and convenience, thieves learn how to manipulate weakness in the technology, so vehicles can be stolen without the key.

2. TO THE COMMUNITY

I have written this paper to make the community aware of vehicle security risk. Technology has enable so many valuable conveniences and safety features in vehicles which have also provided many weaknesses to be exploited. Most people think their belongings and vehicle are safe when they hit the lock button on their key. Unfortunately, we make assumption about the technology we use, which often aren't true. I have outlined some of the attacks that can be carried out to unlock or even start vehicles without the possession on the key. According to an article written in October in The Telegraph, "Three Quarters of Cars Stolen in France 'electronically hacked' [3] This means that car thieves are learning how to exploit the car manufacturer weaknesses very quickly. There is very inexpensive equipment such as the HackRf and RollJam that are produced to aid attackers. As a consumer, you should be aware and know how to best protect yourself and your belongings by reviewing the counter measures in this paper. When buying a new car, look into the cars security features and check if the systems have been exploited by hackers. Some car manufacturers and models have more security risks than others.

3. RFID

RFID, Radio-Frequency IDentification is a general term for small, wireless devices that emit unique identifiers upon interrogation by RFID readers[4]. RFID's are mostly used in commercial supply chains and are known as EPC (Electronic Product Code) tag. Large companies use them to provide identification but not digital authentication. RFID's don't just denote EPC

tags, but a wide spectrum if wireless devices or varying capabilities. Higher end RFID devices can offer cryptographic functionality and can support authentication protocol.

Vehicle immobilizers are a type of RFID that did not originally provide cryptographic security, but now exclusively have that functionality. "Immobilizers deter vehicle theft by interrogating an RFID transponder embedded in the ignition key as a condition of enabling the fuel-injection system of the vehicle". Without the RFID signal, the engine will not start even if the thief has a copy of the key (without the immobilizer). This device has been credited with significant reductions in car theft.

4. TYPES OF CAR KEYS

Table 1. Key System Types

Denomination	Entry	Start engine
Physical key	Physical key	Physical key
Physical key with immobilizer	Physical key	Physical key + RFID
Remote Keyless Entry System	Remote active (press button)	Physical key + RFID
Remote Keyless Ignition System	Remote passive	Remote passive

4.1 PHYSICAL KEYS

According to Popular Science article, the key was introduced to cars in 1949 by the Chrysler Corporation as an ignition-key to start vehicles [5]. Previously, cars were started with 2 separate buttons, a starter and an ignition button, as seen in the picture. Aside from the convenience to the driver, the key was used to prevent children from starting a vehicle.

Figure 1. A car that has no key but two separate buttons – starter and ignition to start the car[2].

Although the key added some security, vehicles were easily hot-wired and stolen. Also, metallic keys were easily duplicated, providing an attacker access to the vehicle with previous contact with the key.

Figure 2. Chrysler Corporation car keys from 1949[2].

4.2 PHYSICAL KEYS WITH IMOBILIZERS

A key with an immobilizer has a metal key than an immobilizer (RFID transponder) imbedded into the plastic part of the key. The immobilizer communicates with the steering column to enable to fuel injection system. The immobilizer is a passive device that uses electromagnetic induction from interrogation signal transmitted by the reader. This system was created to

prevent car thefts such as hot wiring, because the car won't start unless it has the successful authentication by the RFID chip.

There are two types of immobilizers: Electronic and Cryptographic [2]. Electronic immobilizers were the first generation which used static signature type transponders. Although they lacked cryptography, they decreased car theft dramatically, see Figure X. The next immobilizer uses cryptographic protocols to prevent attackers from copying the electronic immobilizer with ease.

Figure 3. Key with immobilizer, showing the immobilizer chip embedded in the plastic top[2].

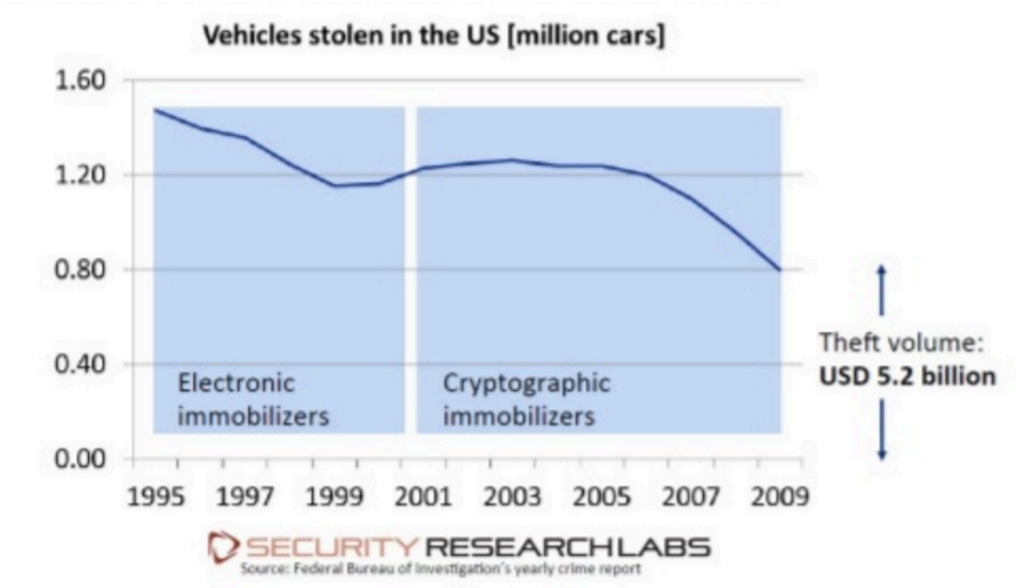

Figure 4. Motor Vehicle Theft in the United States 1995-2009 from the U.S. Department of Justice, Federal Bureau of Investigation, *Uniform Crime Reports* [2].

4.3 REMOTE KEYLESS ENTRY SYSTEMS (RKE)

The Remote Keyless Entry System, RKE, send radio waves to the vehicle to lock and unlock door, open the trunk, or disarm the car alarm system. Older models used infrared band, but newer ones use radio waves. RKE systems typically run at 315MHz for North America and 433.92 MHz for Europe and Asia and the transmission range is between 10 and 100 meters [6]. The device has a power source and sends signals to the receiver in the vehicle which means this is an active system. The 1982 Renault Fuego was the first car to use a central locking system [2].

A typical RKE system (Figure 5) includes a microcontroller in the key or key fob. To unlock the car, you press a pushbutton in the key that wakes up the microcontroller, which then sends a stream of 64 or 128 bits to the key's RF transmitter, where it modulates the carrier and us radiated through a simple printed-circuit loop antenna. A loop antenna is inefficient but is inexpensive to produce and is widely used [10].

In the vehicle, an RF receiver captures that data and directs it to another microcontroller, which decodes the data and sends an appropriate message to start the engine or open the door. The digital data stream, transmitted between 2.4kbps and 20kbps usually consists of a data preamble, a common code, some check bits and a "rolling code" which ensure changes with each use to ensure the vehicles security. This prevents an attacker from capturing the signal once and being able to repeatedly gain entry[10].

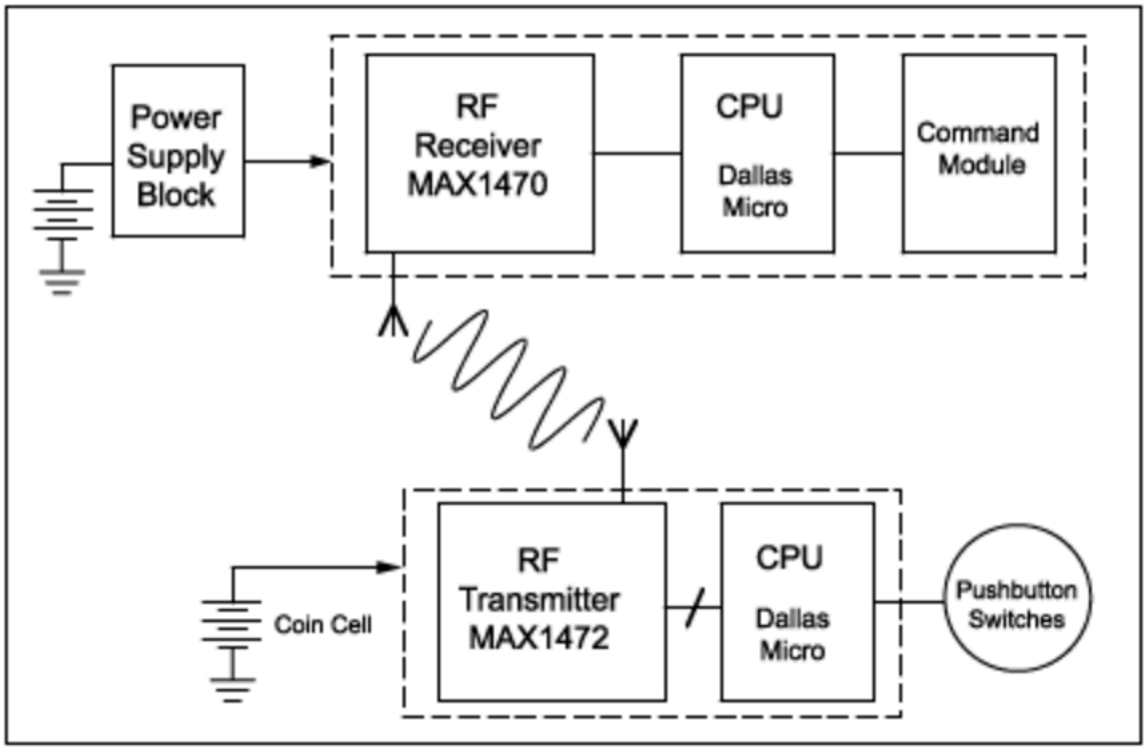

Figure 5. An RKE system consists of a key fob circuit (lower diagram) transmitting to a receiver in the vehicle (upper diagram) [10].

4.4 REMOTE KEYLESS IGNITION SYSTEMS (RKI)

Remote Keyless Ignition Systems (RKI), also called Passive Keyless Entry and Start Systems (PKES) or Smart Key, are devices that have the capabilities of a RKE but also do not require a metal to start the car. Doors are usually unlocked without pressing any button on the key (many cars with RKI systems allow the car owner to have the key in their pocket and touch a sensor on the door handle). Some cars require that the key fob be placed in the ignition slot, while other just require it to be inside the car to start the ignition.

The "automatic" car unlocking or ignition can be a security risk because an attacker may be able to steal the car when the car owner is nearby (i.e. filling up fuel or loading the trunk). The normal mode for the key uses two channel. After getting in close proximity to the car, the car

communicates via inductive coupling LF channel (120-135 kHz) to the key on one channel (in 1 – 2 meter vicinity) and the key will replay back on the second, UHF channel (315-433 MHz) even in the vicinity of 50 – 100 meters [2]. A car first periodically sends LF signals until the key sends its acknowledgment proximity UHF signal; then the car sends its Id number along with the challenge via LF signal, and finally, the key sends its response via the UHF signal. Battery depleted mode uses the passive component on the key and works in both directions. The passive component must be near the RFID reader and a metallic key must be used in the key fob to start the car.

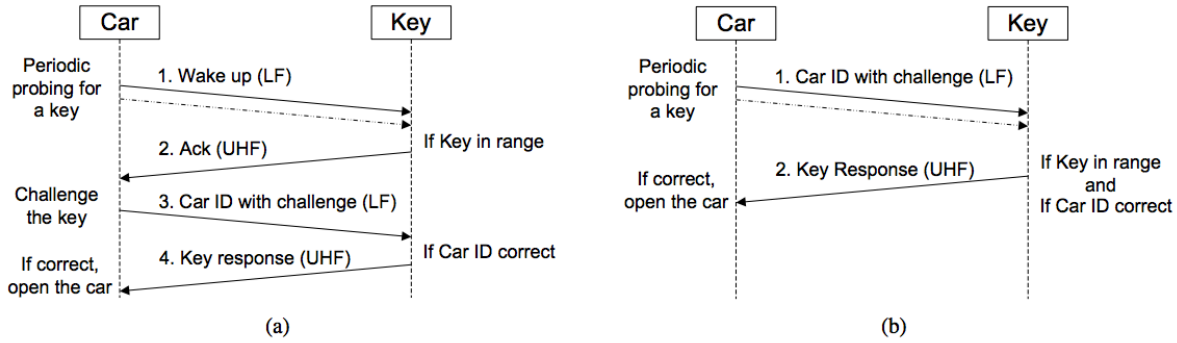

Figure 6. Examples of Passive Keyless Entry System protocol realizations. a) In a typical realization, the car periodically probes the channel for the presence of the key with short beacons. If the key is in range, a challenge-response protocol between the car and the key follows to grant or deny access. This is energy efficient given that the key relies on very short beacons. b) In a second realization, the car periodically probes the channel directly with larger challenge beacons that contain the car identifier. If the key is in range, it directly responds to the challenge.

PKES Access Control Summary

Key position	Authorization	Medium used	
		Car ⇒ Key	Key ⇒ Car
Normal mode: when the internal battery is present			
Remote	Active open/close	None	UHF
Outside	Passive open/close	LF	UHF
Inside	Passive start	LF	UHF
Backup mode: when the internal battery is exhausted			
Remote	Open/close	Impossible	
Outside	Open/close	With physical key	
Inside	Start	LF	LF

Figure 7. PKES/RKI Access Control Summary

5. RADIO JAMMING ATTACK

This is a relatively easy attack which jams the locking signal from the key to lock or unlock the car. The attacker just needs a radio transmitter that transmits garbage code at the same frequency as the key fob to block the signal. The attacker must be close to the car in order to block the signal which allows for easy detection. For this attack, the attacker can't start the car, but they can steal any possession left in the car by the owner. Most cars make a particular sound and/or flash their lights when they are locked, so the owner should notice when the car doesn't lock successfully which undermines this attack [6].

6. ROLLJAM WIRELESS ATTACK

The RollJam hack was created by Samy Kamkar, known best for creating the first self-propagating cross-site scripting worm. The RollJam is a $32 radio device that is designed to defeat the "rolling codes" security in

keyless entry systems, alarm systems, and garage door opening systems. This device is meant to be hidden on or near the target vehicle or garage, where it waits for the victim to use his or her key fob within radio range. The key fob won't work on the first try, but will unlock or lock the vehicle on the second try. The RollJam first jams and stores the first signal from the key fob and fails to unlock the door, so the user naturally presses the button again. On the second press, the RollJam again jams the signal and records the second code and broadcasts its first code, unlocking the door [7]. The RollJam attacker can then return at anytime to retrieve the device and replay the intercepted code from the victim's fob to unlock the car or garage. Kamar says he has tested the RollJam successfully on Nissan, Cadillac, Ford, Toyota, Lotus, Volkswagen, and Chrysler vehicles.

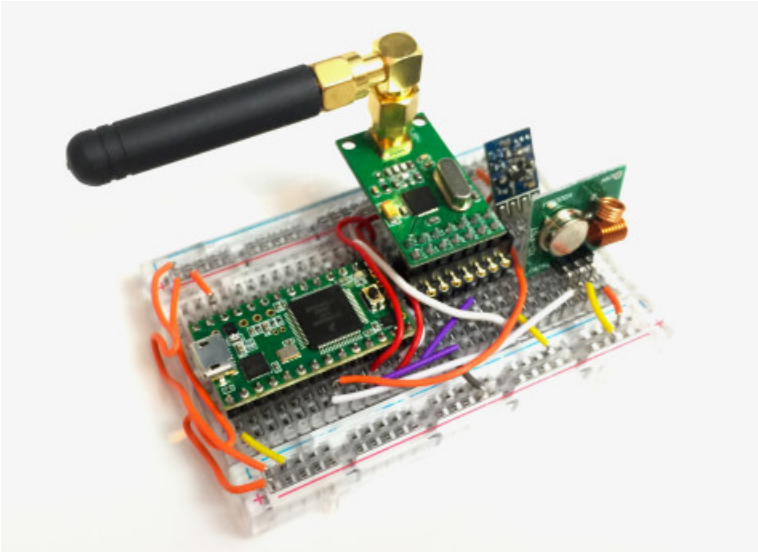

Figure 8. Samy Kamkar's RollJam device

Figure 9. The RollJam, detecting a signal, jams the vehicle's frequency. The code is intercepted and stored [7].

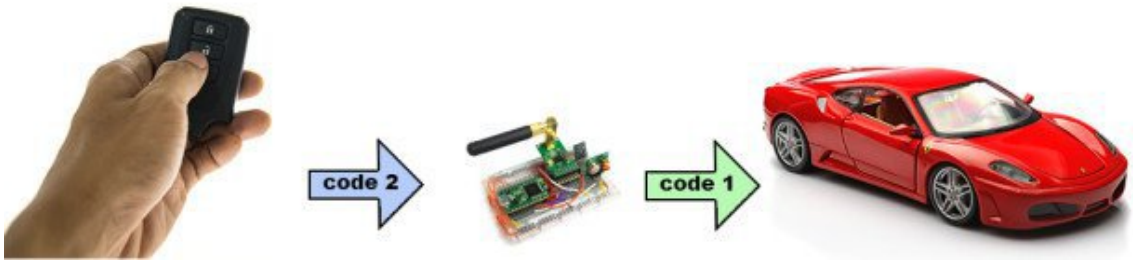

Figure 10. The user clicks the button again and the RollJam broadcasts the old code while simultaneously capturing the new one. The car unlocks [7].

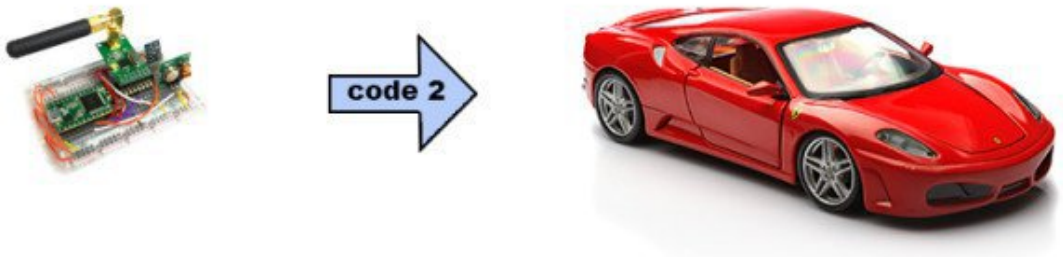

Figure 11. The RollJam device is retrieved, still holding the new unused code. The code can then be transmitted later to unlock the car [7].

7. RELAY ATTACK

This technique is relevant with only RKE and RKI systems where the attacker extends the range of the radio frequency transmitter to intercept the data being transmitted between the key fob and the vehicle. A paper on the security of Passive Keyless Entry and Start Systems (PKES) or Remote Keyless Ignition Systems (RKI), introduced this model of attacking modern cars using two variants of physical-level relays, wired and wireless [8]. The

results show that a signal relaying in one direction (from the car to the key) is sufficient to perform the attack and while the distance between the car and the key can be large (tested up to 50 meters, non line-of-sight). The researches tested 10 car models from 8 manufacturers which were concluded to be all vulnerable to the attack. This attack does not Even if the passive keyless entry system has strong cryptography (e.g. AES or RSA), it would still be vulnerable to this attack.

4.4 RELAY OVER-CABLE ATTACK

For the relay over-cable attack, the researchers used a relay composed of two loop antennas connected together with a cable that relays the LF signal between the antennas. An amplifier may be placed in the middle to improve the signal if needed. When the loop antenna is placed close to the door handle of the vehicle, it captures the car beacon signal as a local magnetic field. This fields excites the first antenna of the relay which creates an alternating signal at the output of the antenna. The electrical signal is then transmitted over the coaxial cable to reach the second antenna, which then creates a magnetic field in the proximity of the second antenna. The magnetic field excites the antenna of the key and recovers the original message from the car. In each system that they tested, this was sufficient to make the key send the *open* or *start* authorization message over the UHF channel. The attacker just needs to present the relaying antenna in front of the door handle for the key to send the *open* signal and bring the antenna inside the car and push the breaks or start engine button to send the *start* message.

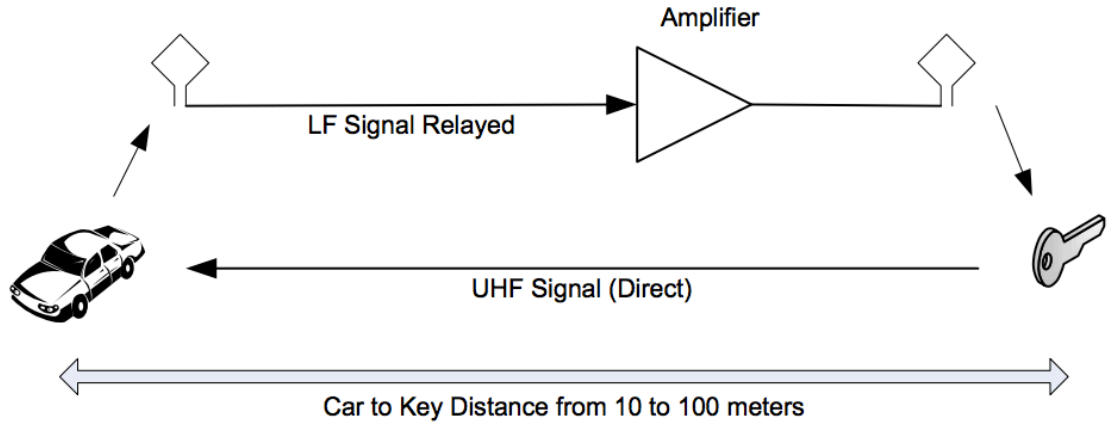

Figure 12. The relay with antennas, cables, and an (optional) amplifier [8].

4.4 RELAY OVER-THE-AIR ATTACK

Relaying over a cable may not be preferable because it may be inconvenient or be suspicious. The relay-over-the-air attack, relays the LF signal from the car over a purpose-built RF link (composed if the emitter and the receiver) with minimal delays. The emitter captures the LF signal and up-converts it to 2.5 GHz which is then amplified and transmitted over the air. The receiver receives the signal and down-converts it to obtain the original LF signal. The LF signal is then amplified again and sent to a loop LF antenna which reproduces the signal that the car emitted. The process of opening and starting the car is the same as with the over-cable attack.

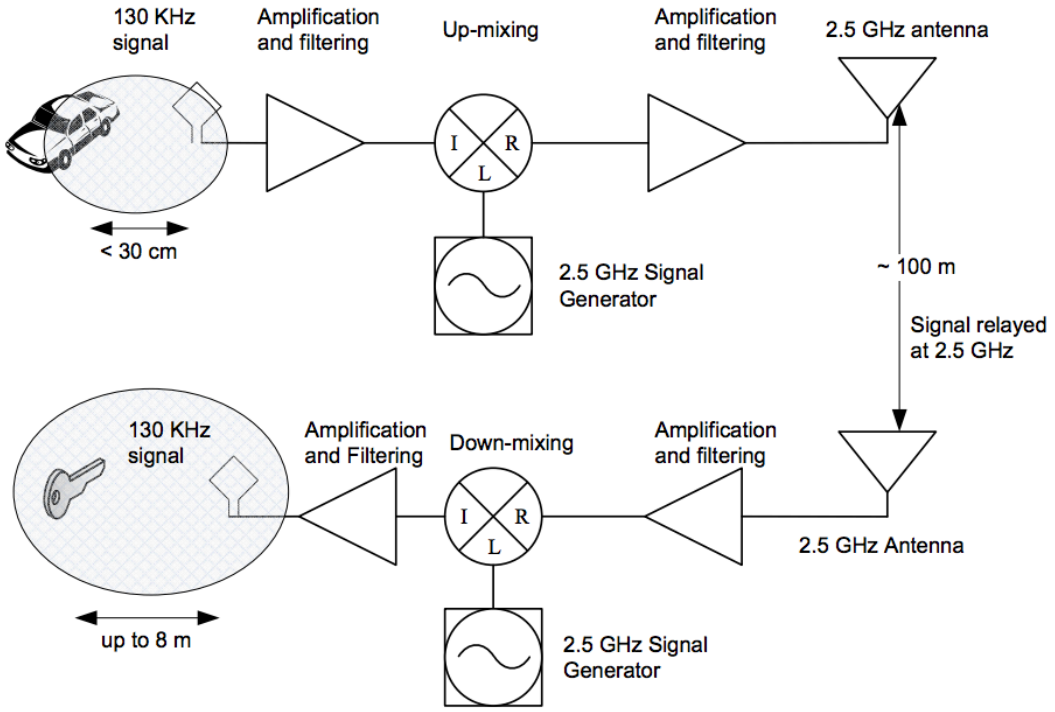

Figure 13. Simplified view of the attack relaying LF (130 KHz) signals over the air by up-conversion and down-conversion. The relay is realized in analog to limit processing time [8].

(a) Key side. (b) Car side.

Figure 14. Experimental wireless relay setup [8].

(a) Loop antenna placed next to the door handle. (b) Starting the engine using the relay.

Figure 15. The relay attack in practice: (a) opening the door with the relay. (b) starting the car with the relay, in the foreground the attacker with the loop antenna starts the car, in the background the table (about 10 meters away) with the receiver side of the wireless relay and the key. Emitter side of the wireless relay is not shown in this picture [8].

For this attack to be successful, the attacker must only allow for a small delay from relaying and should attack when the car owner is relatively far from the vehicle to avoid detection. As the distance of attack increases, the delay in transmission increases.

Table 2. Distance vs. Relay link delay: The measured delays are for the LF channel only. The UHF link delay is based on direct car-key communication and assumes wave propagation with the speed of light. The latter should be added to obtain the total relay delay [8].

Attack	Distance (m)	Delay (ns)	Comments
Relay over cable	30	160 ($\pm$20)	Opening and starting the engine works reliably
	60[1]	350 ($\pm$20)	With some cars signal amplification is not required
Wireless relay	30[2]	120 ($\pm$20)	Opening of the car is reliable, starting of the engine works

[1] With an amplifier between two 30 m cables.
[2] Tested distance. Longer distances can be achieved.

8. MEGAMOS CRYPTO TRANSPONDER ATTACK

The attacks on the Megamos Crypto are exploiting the cipher design, key-update mechanism, and weak cryptographic keys set by car manufacturers. In the research paper "Dismantling Megamos Crypto: Wirelessly Lockpicking a Vehicle Immobilizer", the researchers present the weakness in the cryptography and authentication protocol in the Magamos Crypo transponder[9]. The paper outline three attacks on the transponder to recover the 96-bit transponder secret key. According to Bloomberg "The Megamos is one of the most common immobilizer transponders, used in Volkswagen-owned luxury brands including Audi, Porsche, Bentley, and Lamborghini, as well as Fiats, Hondas, Volvos and some Maserati models.

Make	Models
Alfa Romeo	147, 156, GT
Audi	A1, A2, A3, **A4 (2000)**, A6, A8, Allroad, Cabrio, Coupé, Q7, S2, S3, S4, S6, S8, **TT (2000)**
Buick	Regal
Cadillac	CTS-V, SRX
Chevrolet	Aveo, Kalos, Matiz, Nubira, Spark, Evanda, Tacuma
Citroën	**Jumper (2008)**, Relay
Daewoo	Kalos, Lanos, Leganza, Matiz, Nubira, Tacuma
DAF	CF, LF, XF
Ferrari	California, 612 Schaglietti
Fiat	Albea, Doblò, Idea, Mille, Multipla, Palio, **Punto (2002)**, Seicento, Siena, Stilo, **Ducato (2004)**
Holden	Barina, Frontera
Honda	Accord, Civic, CR-V, FR-V, HR-V, Insight, **Jazz (2002)**, Legend, Logo, S2000, Shuttle, Stream
Isuzu	Rodeo
Iveco	Eurocargo, Daily
Kia	Carnival, Clarus, Pride, Shuma, Sportage
Lancia	Lybra, Musa, Thesis, Y
Maserati	Quattroporte
Opel	Frontera
Pontiac	G3
Porsche	911, 968, Boxster
Seat	Altea, Córdoba, Ibiza, Leon, Toledo
Skoda	**Fabia (2011)**, Felicia, Octavia, Roomster, Super, Yeti
Ssangyong	Korando, Musso, Rexton
Tagaz	Road Partner
Volkswagen	Amarok, Beetle, Bora, Caddy, Crafter, Cross Golf, Dasher, Eos, Fox, Gol, **Golf (2006, 2008)**, Individual, Jetta, Multivan, New Beetle, Parati, Polo, Quantum, Rabbit, Saveiro, Santana, **Scirocco (2011)**, Touran, Tiguan, Voyage, **Passat (1998, 2005)**, Transporter
Volvo	C30, **S40 (2005)**, S60, S80, V50, V70, XC70, XC90, XC94

Figure 16. Vehicles that used Megamos Crypto for some version/year. Boldface and year indicate specific vehicles researchers experimented with [9].

The equipment needed for these attacks are the Proxmark III to eavesdrop and communicate with the car and transponder. The Proxmark is a powerful general purpose RFID protocol analysis tool that supports raw data sampling from low frequency of 125kHz to High frequency of 13.56 MHz. The researchers also implemented a custom firmware and FPGA design for the modulation and encoding schemes of the Megamos Crypto transponders. The researchers reverse engineered they Megamos cipher in a semi-automatic way by observing the memory state changes and guessing the

intermediate cryptographic calculations. The researchers found a simple cryptanalysis that recovers the 96-bit secret key with a complexity of 2^{56} first and then optimize it to a complexity of 2^{48}. The full details of their cryptanalysis can be found in their research appear [9].

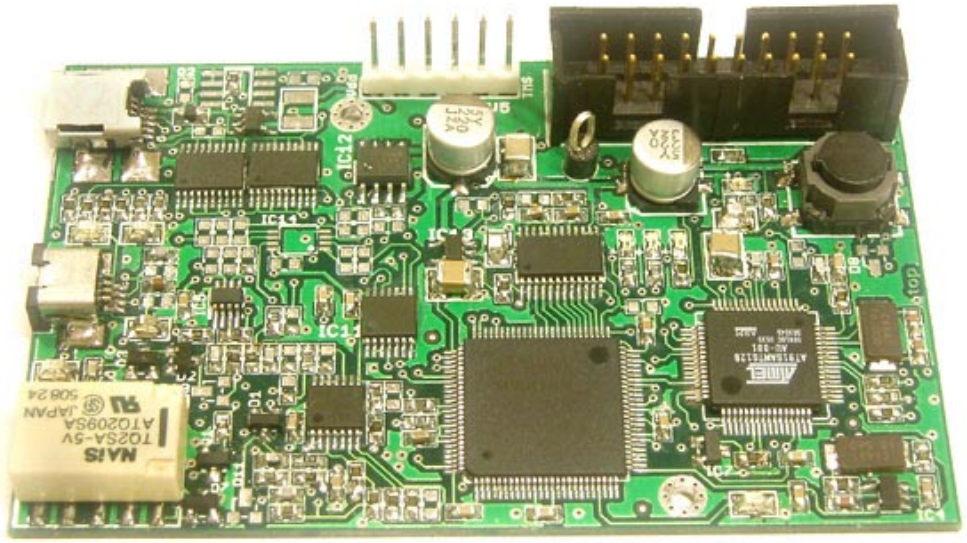

Figure 17. Proxmark III

4.4 PARTIAL KEY-UPDATE ATTACK

The first attack is a partial key-update attack. When the transponder is not locked, the Megamos Crypto transponder does not require authentication in order to write to memory. This makes the transponder vulnerable to a denial of service attack by an attacker flipping one bit of the secret key of the transponder to disable it. There is also another weakness in how the secret key is written to the transponder. The secret key is 96 bits long and these bits are stored in 6 memory blocks of 16 buts each (blocks 4 to 9), see Figure 18. It is only possible to write one block at a time to the transponder which constitutes a serious weakness since a secure key-update must be an automatic operation. The car authenticates by sending a nonce $n_C = Random$ and the corresponding authenticator $a_C = f(Rnd,K)$. When the car successfully authenticates itself, the Megamos Crypto transponder sends the

transponder authenticator $a_T = g(Rnd,f,K)$ back to the car, see Figure 19. The optimized attack can be completed as follows:

1. *The adversary eavesdrops a successful authentication trace, obtaining n_C, a_C, and a_T.*
2. *They adversary writes 0X0000 on memory block 9 which contains key bits $k_{80}…k_{95}$.*
3. *The adversary then increments the observes n_C value and attempts an authentication for each $n_C + inc \pmod{2^{56}}$, where $0 \leq inc < 2^{16}$.*
4. *Repeating step 3) at most 2^{16} times, the transponder will accept one ac value for a particular increment value inc and give an answer. Then the adversary knows that $k_{80}…k_{95} = inc$.*
5. *The adversary proceeds similarly for 8 blocks and 7. At this point the adversary has recovered key bits $k_{48}…k_{95}$.*
6. *Next the adversary guesses 15 key bits $k_{33}…k_{47}$.*
7. *Having $k_{33}…k_{95}$ the adversary is now able to initialize the cipher, obtain the initial state s_0 and run it forward up to state s_7. At this point the adversary has 2^{15} candidates for state s_7.*
8. *For each of these candidates, the adversary runs the cipher forward 33 steps up to state s_{40}. While running the cipher forward the adversary is able to determine input bits $k_{32}…k_0$ by comparing the output bits to a_C and a_T from the trace.*
9. *Then, forward each candidate state at s_{40} to s_{55} and produce another 15 output bits to test on, although this time, with the known input of 15 zero bits. On average only one candidate survives this test. The adversary has now recovered the complete key [9].*

This attack only requires one successful authentication trace. In total, we need to write three times on the memory of the transponder and perform 3 x 2^{16} authentications with the transponder. This can be done within 30 minutes using Proxmark III. The computational complexity of the last three steps is 2^{15} encryption which takes less than a second on a laptop.

Do to the complexity associated with this attack, it is not ideal for an attacker with limited programming skills. This however is a very fats attack

and could be a very effective way to unlock a car. The attacker would be, however, limited to attacking cars with a Megamos Crypto transponder.

Block	Content	Denoted by
0	user memory	$um_0 \dots um_{15}$
1	user memory, lock bits	$um_{16} \dots um_{29} l_0 l_1$
2	device identification	$id_0 \dots id_{15}$
3	device identification	$id_{16} \dots id_{31}$
4	crypto key	$k_0 \dots k_{15}$
5	crypto key	$k_{16} \dots k_{31}$
6	crypto key	$k_{32} \dots k_{47}$
7	crypto key	$k_{48} \dots k_{63}$
8	crypto key	$k_{64} \dots k_{79}$
9	crypto key	$k_{80} \dots k_{95}$
10	pin code	$pin_0 \dots pin_{15}$
11	pin code	$pin_{16} \dots pin_{31}$
12	user memory	$um_{30} \dots um_{45}$
13	user memory	$um_{46} \dots um_{61}$
14	user memory	$um_{62} \dots um_{77}$
15	user memory	$um_{78} \dots um_{93}$

read-only
write-only
read-write

Figure 18. Megamos Crypto transponder memory layout [9].

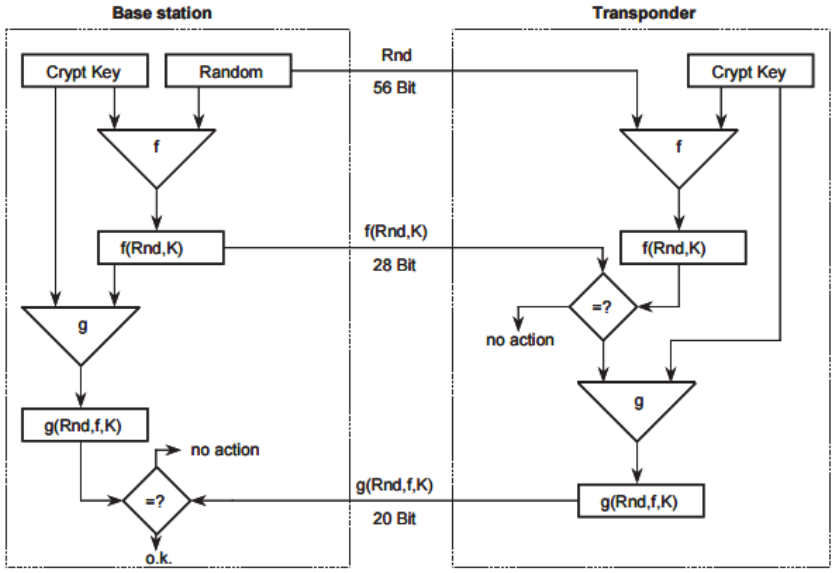

Figure 19. Authentication procedure [9].

4.4 WEAK-KEY ATTACK

During the reasearchers experiements, they discovered that many of keys they recovered were from $k_0 = \ldots = k_{31} = 0$ and then more or less random looking bits for $k_{32} \ldots k_{96}$. Here are some example key for Car A and B with 0's at the front.

Car	Secret key
A.1	00000000**d8 b3967c5a3c3b29**
A.2	00000000**d9 b79d7a5b3c3b28**
B.1	0000000000 **0001040505090**5

Figure 20. Recovered keys from cars A and B. Besides the evident 32 leading zero bits, every second nibble seems to encode a manufacturer dependent value, which further reduces the entropy of the key [9].

If the Megamos Crypto uses weak keys like the ones above, the key can be recovered very quickly, even when the memory of the transponder is locked with a PIN code. A weak secret key has the bits $k_0 \ldots k_{31}$ fixed by the car manufacturer allows the attacker to know the input bits of the cipher states $s_8 \ldots s_{55}$. With a weak key, it is possible to pre-compute and sort on a 47 contiguous ouput bits for each internal state at s_8. This table (with 2^{56} entries) requires a huge amount of storage so a rainbow table would be advisable to shrink the store significantly. The researchers calculated that the rainbow would take $2^{18.7}$ seconds to build and complete which is less than 5 days [9].

Do to the complexity and time associated with this attack, it is not ideal for an attacker with limited programming skills or time.

9. KEYPAD ENTRY ATTACK

Some cars use a keypad entry on the B-pillar or under the driver's door handle that accepts a 5-digit code to unlock the car. The following Ford,

Lincoln, and Mercury SUVs have the SecuriCode keyless entry keypad: 2010 Ford Edge, 2010 Ford Flex, 2009 Ford Taurus X, 2010 Ford Expedition, 2009 Ford Escape, 2010 Ford Explorer, 2010 Lincoln MKX, 2010 Lincoln MKT, 2009 Mercury Mountaineer, and 2009 Mercury Mariner. The keypad has buttons labels 1/2, 3/4, 5/6, 7/8, 9/0. While this feature seems handy to the car owners, an attacker can enter the sequence below in about 20 minutes which will unlock the car door and allow access to the attacker. This long sequence will grant access because the keycodes roll, meaning that one code can continue into another without resetting or causing alerts.

9 9 9 9 1 1 1 1 1 3 1 1 1 1 5 1 1 1 1 7 1 1 1 1 9 1 1 1 3 3 1 1 1 3 5 1 1 1 3
7 1 1 1 3 9 1 1 1 5 3 1 1 1 5 5 1 1 1 5 7 1 1 1 5 9 1 1 1 7 3 1 1 1 7 5 1 1 1
7 7 1 1 1 7 9 1 1 1 9 3 1 1 1 9 5 1 1 1 9 7 1 1 1 9 9 1 1 3 1 3 1 1 3 1 5 1 1
3 1 7 1 1 3 1 9 1 1 3 3 3 1 1 3 3 5 1 1 3 3 7 1 1 3 3 9 1 1 3 5 3 1 1 3 5 5 1
1 3 5 7 1 1 3 5 9 1 1 3 7 3 1 1 3 7 5 1 1 3 7 7 1 1 3 7 9 1 1 3 9 3 1 1 3 9 5
1 1 3 9 7 1 1 3 9 9 1 1 5 1 3 1 1 5 1 5 1 1 5 1 7 1 1 5 1 9 1 1 5 3 3 1 1 5 3
5 1 1 5 3 7 1 1 5 3 9 1 1 5 5 3 1 1 5 5 5 1 1 5 5 7 1 1 5 5 9 1 1 5 7 3 1 1 5
7 5 1 1 5 7 7 1 1 5 7 9 1 1 5 9 3 1 1 5 9 5 1 1 5 9 7 1 1 5 9 9 1 1 7 1 3 1 1
7 1 5 1 1 7 1 7 1 1 7 1 9 1 1 7 3 3 1 1 7 3 5 1 1 7 3 7 1 1 7 3 9 1 1 7 5 3 1
1 7 5 5 1 1 7 5 7 1 1 7 5 9 1 1 7 7 3 1 1 7 7 5 1 1 7 7 7 1 1 7 7 9 1 1 7 9 3
1 1 7 9 5 1 1 7 9 7 1 1 7 9 9 1 1 9 1 3 1 1 9 1 5 1 1 9 1 7 1 1 9 1 9 1 1 9 3
3 1 1 9 3 5 1 1 9 3 7 1 1 9 3 9 1 1 9 5 3 1 1 9 5 5 1 1 9 5 7 1 1 9 5 9 1 1 9
7 3 1 1 9 7 5 1 1 9 7 7 1 1 9 7 9 1 1 9 9 3 1 1 9 9 5 1 1 9 9 7 1 1 9 9 9 1 3
1 3 3 1 3 1 3 5 1 3 1 3 7 1 3 1 3 9 1 3 1 5 3 1 3 1 5 5 1 3 1 5 7 1 3 1 5 9 1
3 1 7 3 1 3 1 7 5 1 3 1 7 7 1 3 1 7 9 1 3 1 9 3 1 3 1 9 5 1 3 1 9 7 1 3 1 9 9
1 3 3 1 5 1 3 3 1 7 1 3 3 1 9 1 3 3 3 3 1 3 3 3 5 1 3 3 3 7 1 3 3 3 9 1 3 3 5
3 1 3 3 5 5 1 3 3 5 7 1 3 3 5 9 1 3 3 7 3 1 3 3 7 5 1 3 3 7 7 1 3 3 7 9 1 3 3
9 3 1 3 3 9 5 1 3 3 9 7 1 3 3 9 9 1 3 5 1 5 1 3 5 1 7 1 3 5 1 9 1 3 5 3 3 1 3
5 3 5 1 3 5 3 7 1 3 5 3 9 1 3 5 5 3 1 3 5 5 5 1 3 5 5 7 1 3 5 5 9 1 3 5 7 3 1
3 5 7 5 1 3 5 7 7 1 3 5 7 9 1 3 5 9 3 1 3 5 9 5 1 3 5 9 7 1 3 5 9 9 1 3 7 1 5
1 3 7 1 7 1 3 7 1 9 1 3 7 3 3 1 3 7 3 5 1 3 7 3 7 1 3 7 3 9 1 3 7 5 3 1 3 7 5
5 1 3 7 5 7 1 3 7 5 9 1 3 7 7 3 1 3 7 7 5 1 3 7 7 7 1 3 7 7 9 1 3 7 9 3 1 3 7
9 5 1 3 7 9 7 1 3 7 9 9 1 3 9 1 5 1 3 9 1 7 1 3 9 1 9 1 3 9 3 3 1 3 9 3 5 1 3
9 3 7 1 3 9 3 9 1 3 9 5 3 1 3 9 5 5 1 3 9 5 7 1 3 9 5 9 1 3 9 7 3 1 3 9 7 5 1
3 9 7 7 1 3 9 7 9 1 3 9 9 3 1 3 9 9 5 1 3 9 9 7 1 3 9 9 9 1 5 1 5 3 1 5 1 5 5
1 5 1 5 7 1 5 1 5 9 1 5 1 7 3 1 5 1 7 5 1 5 1 7 7 1 5 1 7 9 1 5 1 9 3 1 5 1 9
5 1 5 1 9 7 1 5 1 9 9 1 5 3 1 7 1 5 3 1 9 1 5 3 3 3 1 5 3 3 5 1 5 3 3 7 1 5 3
3 9 1 5 3 5 3 1 5 3 5 5 1 5 3 5 7 1 5 3 5 9 1 5 3 7 3 1 5 3 7 5 1 5 3 7 7 1 5
3 7 9 1 5 3 9 3 1 5 3 9 5 1 5 3 9 7 1 5 3 9 9 1 5 5 1 7 1 5 5 1 9 1 5 5 3 3 1
5 5 3 5 1 5 5 3 7 1 5 5 3 9 1 5 5 5 3 1 5 5 5 5 1 5 5 5 7 1 5 5 5 9 1 5 5 7 3
1 5 5 7 5 1 5 5 7 7 1 5 5 7 9 1 5 5 9 3 1 5 5 9 5 1 5 5 9 7 1 5 5 9 9 1 5 7 1
7 1 5 7 1 9 1 5 7 3 3 1 5 7 3 5 1 5 7 3 7 1 5 7 3 9 1 5 7 5 3 1 5 7 5 5 1 5 7

5 7 1 5 7 5 9 1 5 7 7 3 1 5 7 7 5 1 5 7 7 7 1 5 7 7 9 1 5 7 9 3 1 5 7 9 5 1 5
7 9 7 1 5 7 9 9 1 5 9 1 7 1 5 9 1 9 1 5 9 3 3 1 5 9 3 5 1 5 9 3 7 1 5 9 3 9 1
5 9 5 3 1 5 9 5 5 1 5 9 5 7 1 5 9 5 9 1 5 9 7 3 1 5 9 7 5 1 5 9 7 7 1 5 9 7 9
1 5 9 9 3 1 5 9 9 5 1 5 9 9 7 1 5 9 9 9 1 7 1 7 3 1 7 1 7 5 1 7 1 7 7 1 7 1 7
9 1 7 1 9 3 1 7 1 9 5 1 7 1 9 7 1 7 1 9 9 1 7 3 1 9 1 7 3 3 3 1 7 3 3 5 1 7 3
3 7 1 7 3 3 9 1 7 3 5 3 1 7 3 5 5 1 7 3 5 7 1 7 3 5 9 1 7 3 7 3 1 7 3 7 5 1 7
3 7 7 1 7 3 7 9 1 7 3 9 3 1 7 3 9 5 1 7 3 9 7 1 7 3 9 9 1 7 5 1 9 1 7 5 3 3 1
7 5 3 5 1 7 5 3 7 1 7 5 3 9 1 7 5 5 3 1 7 5 5 5 1 7 5 5 7 1 7 5 5 9 1 7 5 7 3
1 7 5 7 5 1 7 5 7 7 1 7 5 7 9 1 7 5 9 3 1 7 5 9 5 1 7 5 9 7 1 7 5 9 9 1 7 7 1
9 1 7 7 3 3 1 7 7 3 5 1 7 7 3 7 1 7 7 3 9 1 7 7 5 3 1 7 7 5 5 1 7 7 5 7 1 7 7
5 9 1 7 7 7 3 1 7 7 7 5 1 7 7 7 7 1 7 7 7 9 1 7 7 9 3 1 7 7 9 5 1 7 7 9 7 1 7
7 9 9 1 7 9 1 9 1 7 9 3 3 1 7 9 3 5 1 7 9 3 7 1 7 9 3 9 1 7 9 5 3 1 7 9 5 5 1
7 9 5 7 1 7 9 5 9 1 7 9 7 3 1 7 9 7 5 1 7 9 7 7 1 7 9 7 9 1 7 9 9 3 1 7 9 9 5
1 7 9 9 7 1 7 9 9 9 1 9 1 9 3 1 9 1 9 5 1 9 1 9 7 1 9 1 9 9 1 9 3 3 3 1 9 3 3
5 1 9 3 3 7 1 9 3 3 9 1 9 3 5 3 1 9 3 5 5 1 9 3 5 7 1 9 3 5 9 1 9 3 7 3 1 9 3
7 5 1 9 3 7 7 1 9 3 7 9 1 9 3 9 3 1 9 3 9 5 1 9 3 9 7 1 9 3 9 9 1 9 5 3 3 1 9
5 3 5 1 9 5 3 7 1 9 5 3 9 1 9 5 5 3 1 9 5 5 5 1 9 5 5 7 1 9 5 5 9 1 9 5 7 3 1
9 5 7 5 1 9 5 7 7 1 9 5 7 9 1 9 5 9 3 1 9 5 9 5 1 9 5 9 7 1 9 5 9 9 1 9 7 3 3
1 9 7 3 5 1 9 7 3 7 1 9 7 3 9 1 9 7 5 3 1 9 7 5 5 1 9 7 5 7 1 9 7 5 9 1 9 7 7
3 1 9 7 7 5 1 9 7 7 7 1 9 7 7 9 1 9 7 9 3 1 9 7 9 5 1 9 7 9 7 1 9 7 9 9 1 9 9
3 3 1 9 9 3 5 1 9 9 3 7 1 9 9 3 9 1 9 9 5 3 1 9 9 5 5 1 9 9 5 7 1 9 9 5 9 1 9
9 7 3 1 9 9 7 5 1 9 9 7 7 1 9 9 7 9 1 9 9 9 3 1 9 9 9 5 1 9 9 9 7 1 9 9 9 9 3
3 3 3 3 5 3 3 3 3 7 3 3 3 3 9 3 3 3 5 5 3 3 3 5 7 3 3 3 5 9 3 3 3 7 5 3 3 3 7
7 3 3 3 7 9 3 3 3 9 5 3 3 3 9 7 3 3 3 9 9 3 3 5 3 5 3 3 5 3 7 3 3 5 3 9 3 3 5
5 5 3 3 5 5 7 3 3 5 5 9 3 3 5 7 5 3 3 5 7 7 3 3 5 7 9 3 3 5 9 5 3 3 5 9 7 3 3
5 9 9 3 3 7 3 5 3 3 7 3 7 3 3 7 3 9 3 3 7 5 5 3 3 7 5 7 3 3 7 5 9 3 3 7 7 5 3
3 7 7 7 3 3 7 7 9 3 3 7 9 5 3 3 7 9 7 3 3 7 9 9 3 3 9 3 5 3 3 9 3 7 3 3 9 3 9
3 3 9 5 5 3 3 9 5 7 3 3 9 5 9 3 3 9 7 5 3 3 9 7 7 3 3 9 7 9 3 3 9 9 5 3 3 9 9
7 3 3 9 9 9 3 5 3 5 5 3 5 3 5 7 3 5 3 5 9 3 5 3 7 5 3 5 3 7 7 3 5 3 7 9 3 5 3
9 5 3 5 3 9 7 3 5 3 9 9 3 5 5 3 7 3 5 5 3 9 3 5 5 5 5 3 5 5 5 7 3 5 5 5 9 3 5
5 7 5 3 5 5 7 7 3 5 5 7 9 3 5 5 9 5 3 5 5 9 7 3 5 5 9 9 3 5 7 3 7 3 5 7 3 9 3
5 7 5 5 3 5 7 5 7 3 5 7 5 9 3 5 7 7 5 3 5 7 7 7 3 5 7 7 9 3 5 7 9 5 3 5 7 9 7
3 5 7 9 9 3 5 9 3 7 3 5 9 3 9 3 5 9 5 5 3 5 9 5 7 3 5 9 5 9 3 5 9 7 5 3 5 9 7
7 3 5 9 7 9 3 5 9 9 5 3 5 9 9 7 3 5 9 9 9 3 7 3 7 5 3 7 3 7 7 3 7 3 7 9 3 7 3
9 5 3 7 3 9 7 3 7 3 9 9 3 7 5 3 9 3 7 5 5 5 3 7 5 5 7 3 7 5 5 9 3 7 5 7 5 3 7
5 7 7 3 7 5 7 9 3 7 5 9 5 3 7 5 9 7 3 7 5 9 9 3 7 7 3 9 3 7 7 5 5 3 7 7 5 7 3
7 7 5 9 3 7 7 7 5 3 7 7 7 7 3 7 7 7 9 3 7 7 9 5 3 7 7 9 7 3 7 7 9 9 3 7 9 3 9
3 7 9 5 5 3 7 9 5 7 3 7 9 5 9 3 7 9 7 5 3 7 9 7 7 3 7 9 7 9 3 7 9 9 5 3 7 9 9
7 3 7 9 9 9 3 9 3 9 5 3 9 3 9 7 3 9 3 9 9 3 9 5 5 5 3 9 5 5 7 3 9 5 5 9 3 9 5
7 5 3 9 5 7 7 3 9 5 7 9 3 9 5 9 5 3 9 5 9 7 3 9 5 9 9 3 9 7 5 5 3 9 7 5 7 3 9
7 5 9 3 9 7 7 5 3 9 7 7 7 3 9 7 7 9 3 9 7 9 5 3 9 7 9 7 3 9 7 9 9 3 9 9 5 5 3
9 9 5 7 3 9 9 5 9 3 9 9 7 5 3 9 9 7 7 3 9 9 7 9 3 9 9 9 5 3 9 9 9 7 3 9 9 9 9
5 5 5 5 5 7 5 5 5 5 9 5 5 5 7 7 5 5 5 7 9 5 5 5 9 7 5 5 5 9 9 5 5 7 5 7 5 5 7
5 9 5 5 7 7 7 5 5 7 7 9 5 5 7 9 7 5 5 7 9 9 5 5 9 5 7 5 5 9 5 9 5 5 5 9 7 7 5 5

9 7 9 5 5 9 9 7 5 5 9 9 9 5 7 5 7 7 5 7 5 7 9 5 7 5 9 7 5 7 5 9 9 5 7 7 5 9 5
7 7 7 7 5 7 7 7 9 5 7 7 9 7 5 7 7 9 9 5 7 9 5 9 5 7 9 7 7 5 7 9 7 9 5 7 9 9 7
5 7 9 9 9 5 9 5 9 7 5 9 5 9 9 5 9 7 7 7 5 9 7 7 9 5 9 7 9 7 5 9 7 9 9 5 9 9 7
7 5 9 9 7 9 5 9 9 9 7 5 9 9 9 9 7 7 7 7 7 9 7 7 7 9 9 7 7 9 7 9 7 7 9 9 9 7 9
7 9 9 7 9 9 9 9 9

Figure 21. A sequence to enter into a vehicle's keypad to unlock the door. This sequence is 3129 key presses long and was creating using de Bruijn sequence [6].

Although this attack is fairly easy and only takes 20 minutes to complete at most, the obvious drawback is that there are few cars that have keypad entry systems. In addition, typing digits into the car's keypad for 20 minutes may rise suspicion.

10. COUNTER MEASURES

10.1 FARADAY'S CAGE

Any RFID based wireless system should be put in aluminum foil or protective metal sheath to prevent it from sending or receiving any radio communication signals. A Faraday's cage should be used for keys with immobilizers, RKE systems, or RKI systems. The car owner would have place and remove the key from the Faraday's cage for every use with takes away from the convenience of the keyless system. This counter measure would prevent the relay attack, because the user would not be able to capture your key fob signal.

10.2 REMOVING BATTERY FROM KEY

This is a safer solution than the Faraday's cage because some signals could potentially be captures through the cage. By removing the battery, the system would completely turn off. This countermeasure will work for RKE and RKI systems which have power sources, but not with immobilizers. There is usually a hidden key within the key fob in case the battery becomes dead which should be used if suspicious of an attack.

10.3 CHANGES BY MANUFACTURERS

Since the systems themselves are insecure, a car owner can only limit security risks. In order to have more secure systems, the manufacturers themselves must implement more secure protocols, better cryptography, stronger keys and authentication, and inform car owners about the possible security risks.

Instead of having to use a Faraday's cage or remove the battery of the key, car manufacturers could make an on/off switch on the key to disable it when the car owner is not using the key. Also there should be an option for PKES systems to turn off the automatic locking/unlocking when near by. If the owner is in a private and safe place, then this feature could be used, but it could also be disabled, forcing the owner to press the lock/unlock button when in an unknown, insecure place.

10. CONCLUSION

Although RFID in car keys have been used for more than a decade and have significantly reduced the number of car thefts, new ways of attack are growing and car manufacturers need to resolve these weaknesses. While car manufacturers slowly change the weaknesses in their systems, car owners must learn how to spot and prevent attacks. Although I have outlined three different attacks, there are many other insecurities with key fobs and immobilizer that can be exploited and many more ways attackers can gain access and start your car.

12. RESOURCES

[1] Patents: Automobile-theft preventer US 1300150 A. [online] Accessed 12/10/15. Available from: http://www.google.com/patents/US1300150.

[2] Security of car keys. Andrej Simko. 04/25/14. Accessed 12/10/15. Available from: http://www.slideshare.net/Andrejimko/security-of-car-keys.

[3] Samuel, Henry. Three Quarters of Cars Stolen in France 'Electronically Hacked.' The Telegraph. 10/29/15. Accessed 12/10/15. Available from: http://www.telegraph.co.uk/news/worldnews/europe/france/11964140/Three-quarters-of-cars-stolen-in-France-electronically-hacked.html

[4] Exploiting RFIDs Car Immobilizers and the ExxonMobil Speed pass. Bono, Stephen and Green, Mathew and Stubblefield, Adam and Rubin, Avi. Accessed 12/10/15. Available from: https://securityevaluators.com/knowledge/case_studies/rfid/

[5] LOZIER, Herbert. 90 Firsts in American Automotive History. Popular Science. New York: Time4 Media, 1964, pp. 81-83. Accessed 12/10/15. Available from: https://encrypted.google.com/books?id=_iwDAAAAMBAJ&pg=PA80&lpg=PA80&dq=automotive+firsts&sour ce=bl&ots=HmsMDH-dRn&sig=7e_6YR85hodR-Wm50gtphsei23s&hl=en&ei=G1NwTLPRG8Tflgf68OTODg&sa=X&oi=book_result&ct=result&resnum=8&ve d=0CDcQ6AEwBw#v=onepage&q&f=false

[6] Open Garage. Car Hacker's Handbook. Accessed 12/10/15. Available from: http://opengarages.org/handbook/2014_car_hackers_handbook_compressed.pdf

[7] Kraft, Caleb. Anatomy of the RollJam Wireless Car Hack. Make: We Are All Makers. 10/11/15. Accessed 12/10/15. Available from: http://makezine.com/2015/08/11/anatomy-of-the-rolljam-wireless-car-hack/

[8] Francillion, Aurelien and Danev, Boris, and Capkun, Srdjan. Relay Attack on Passive Keyless Entry and Start Systems in Modern Cars. 2010. Accessed 12/10/15. Available from: https://eprint.iacr.org/2010/332.pdf.

[9] Verdult, Roel and Flavio Garcia. Dismantaling Megamos Crypto: irelessly Lockpicking a Vehicle Immobilizer. 10/16/13. Accessed 12/10/15. Available from: https://www.usenix.org/sites/default/files/sec15_supplement.pdf

[10] Requirements of Remote Keyless Entry Systems. Maxim Integrated. Accessed 12/10/15. Available from: https://www.maximintegrated.com/en/app-notes/index.mvp/id/3395