Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars

Aurélien Francillon, Boris Danev, Srdjan Čapkun
Department of Computer Science
ETH Zurich
8092 Zurich, Switzerland
{aurelien.francillon, boris.danev, srdjan.capkun}@inf.ethz.ch

Abstract

We demonstrate a relay attack on Passive Keyless Entry and Start (PKES) systems used in modern cars. The attack allows the attacker to enter and start a car by relaying messages between the car and the smart key. We build two setups, wired and wireless physical layer relays, showing that this attack is both inexpensive and practical. We further show that, for the attack to work, it is sufficient that the attacker's devices are placed within $\leq 1m$ of the key and of the car. Moreover, on the several cars we tested, relaying the signal in one direction only (from the car to the key) is sufficient as the replies are sent with UHF, which has a longer range. As the signals are relayed at the physical layer, the attack is completely independent of the modulation scheme, protocols or the presence of strong authentication and encryption. We demonstrate the attack on recent car models from several different manufacturers. Our attack works for a specific set of PKES systems that we tested and whose operation is described in this paper. However, given the generality of the relay attack, it is likely that PKES systems based on similar designs are equally vulnerable to the same attack.

In this work, we further propose simple countermeasures that minimize the risk of relay attacks and that can be immediately deployed by the car owners; however, these countermeasures also disable the operation of the PKES systems. Finally, we discuss countermeasures against relay attacks that were suggested in the open literature and we sketch a new PKES system that prevents relay attacks. This system preserves convenience of use for which PKES systems were initially introduced.

1 Introduction

Modern cars embed complex electronic systems in order to improve diver's safety and convenience. Domains of significant public and manufacturer interest are access to the car (i.e., entry in the car) and authorization to drive (i.e. start the car). Traditionally, access and authorization have been achieved using physical key and lock systems, where by inserting a correct key into the access and start locks, the user was able to enter and drive the car. In the last decade, this system has been augmented with remote access in which users are able to open their car remotely by pressing a button on their key fobs. In these systems, the authorization to drive was still mainly enforced by a physical key and lock system. Physical keys often also embedded immobilizer chips to prevent key copying.

Recently, car manufacturers have started to introduce Passive Keyless Entry and Start (PKES) systems that allow users to open and start their cars while having their car keys 'in their pockets'. This feature is very convenient for the users since they don't have to search for their keys when approaching or preparing to start the car. The Smart Key system was introduced in 1999 [1]. Since then, similar systems have been introduced by a number of manufacturers under different names; a full list of systems can be found in [2].

In this work, we analyze the security of PKES systems and show that they are vulnerable to relay attacks. In a relay attack, the attacker places one of its devices in the proximity of the key, and

Table 1: Key system types

Denomination	Entry	Start engine
Physical key	Physical key	Physical key
Physical key with RFID immobilizer	Physical key	Physical key + RFID
Keyless entry with RFID immobilizer	Remote active (press button)	Physical key + RFID
Passive Keyless Entry and Start (PKES)	Remote passive	Remote passive

the other device in the proximity of the car. The attacker then relays messages between the key and the car, enabling the car to be open and started even if the key is far from the car. This corresponds to the scenario where the key is e.g., in the owner's pocket in the supermarket, and the car is at the supermarket parking lot. We tested several recent car models from several manufacturers and we showed that PKES systems in the tested cars are vulnerable to relay attacks [1]. The attack allowed us to open and start the cars without physically compromising the key or raising any suspicion of the owner. For the attack to work it was sufficient to place one relay device within $1 - 2m$ from the key and the other relay device close to the car. We tested the attack with both wired and wireless relay setups and with different antennas and amplifiers. The cost of our relay setups was between 100$ and 1000$, depending on the choice of components. This shows that relay attacks on PKES systems are both inexpensive and practical. Although the possibility of relay attacks on PKES systems has been discussed in the open literature [3], it was not clear if these attacks are feasible on modern cars; in this paper, we demonstrate that these attacks are both feasible and practical.

Besides demonstrating relay attacks on PKES systems, we propose simple countermeasures that can be immediately deployed by the car owners and that minimize the risk of relay attacks; however, these countermeasures also disable the operation of the PKES systems. We further review countermeasures against relay attacks that were suggested in the open literature and discuss their effectiveness and appropriateness for car PKES systems.

We note that the main reason why relay attacks are possible on PKES systems is that, to open and start the car, instead of verifying that the correct key is in its physical proximity, the car verifies if it can communicate with the correct key, assuming that the ability to communicate (i.e., communication neighborhood) implies proximity (i.e., physical neighborhood). This is only true for non-adversarial settings - in adversarial settings communication neighborhood cannot be taken as a proof of physical proximity. Given this, any secure PKES system needs to enable the car and the key to securely verify their physical proximity. This is only natural since the car should open only when the legitimate user (holding the key) is physically close to the car. We outline a new PKES system, based on distance bounding, that achieves this goal, and preserves user convenience for which PKES systems were initially introduced. We note that relay attacks have been similarly used in other scenarios, e.g., in [13] as mafia-fraud attacks, in [21] as wormhole attacks. Equally, the relationship between secure communication and physical neighborhood notions has been previously studied in [31, 33, 37].

The rest of the paper is organized as follows. In Section 2 we first describe the evolution of car key systems from physical keys to Passive Keyless Entry Systems. In Section 3 we describe the implementation of both the wired and wireless physical layer relay attack. Section 4 describes the consequences and implications of those attacks, countermeasures are presented in Section 5 while related work is discussed in Section 6.

[1] Instead of providing names of car models and manufacturers that we tested, we describe the operation of the PKES system that the tested models use. We leave it to the readers to verify with the manufacturers if the described or similar PKES system is used in specific car models.

2 Car Entry Systems

Car key systems have shown several evolutions from the simple physical keys, Table 1 presents the existing key systems in cars.

2.1 Remote Open and Close

Physical keys were enhanced with capabilities for remote opening and closing the car for convenience. Such enhanced keys have a button on the key fob to open or close the car remotely. This functionality usually requires the presence of a battery and rely on UHF (315 or 433 MHz) communications. UHF typically provides 10 to 100 meters communication range using a reduced amount of energy making the replacement of battery sufficiently infrequent.

2.2 Keys with Immobilizers

In a key with an immobilizer (also known as *transponder key*), RFID chips are embedded in the key bow. When the key blade is inserted in the ignition lock the RFID tag will be queried by the car to verify if the key is authorized. These *immobilizer* systems are designed to prevent a physical copy of the key as well as preventing stealing of the car by bypassing the lock. Only a key with a previously paired RFID tag would be authorized to start the engine. The RFID technology involved typically relies on LF technology (from 120 to 135 KHz). It can operate in both passive and active modes depending on the scenario. The active mode of operation is commonly used with PKES (see Section 2.3).

In the passive mode of operation, the RFID tag is powered by the car via inductive coupling before it communicates a challenge to the key. With the power transferred from the car, the key wakes up the microcontroller, demodulates the challenge, computes a response message and replies back on the LF channel. This mode of operation requires close proximity between key and car because the key has to harvest energy from the car to function and the decrease of the intensity of a magnetic field is inversely proportional to the cube of the distance.

2.3 Passive Keyless Entry Systems

The first proposal that describes Passive Keyless Entry Systems (PKES) appeared in [44]. In that work, the authors proposed a system that automatically unlocks the vehicle when the user carrying the key approaches the vehicle and locks the vehicle when the user moves away from the vehicle. The communication between the key and car is characterized by a magnetically coupled radio frequency signal. In this system, the car concludes that the key is in the close proximity when it is 'in the car's communication range'.

A PKES car key uses a LF RFID tag that provides short range communication (within 1-2 meters in active and a few inches in passive mode) and a fully-fledged UHF transceiver for longer range communication (within 10 to 100 meters). The LF channel is used to detect if the key fob is within regions *Inside* and *Outside* of the car. Figure 2(b) shows the areas in proximity of the car that must be detected in order to allow a safe and convenient use of the PKES system. The regions are as follows.

- M remote distance to the car (in general about 100 m) allows to actively open/close the car by pushing a button on the key fob.
- O outside the car but at a maximum distance of approximately 1 meter from the door handle.
- I inside the car.

The PKES access control protocols vary depending on the manufacturer. Typically two modes of operation are supported, namely *normal* and *backup* mode. The normal mode relies on a charged and working battery, while the backup mode operates without a battery (e.g., when the battery is exhausted). The locations and authorizations of the two modes are summarized in Table 2.

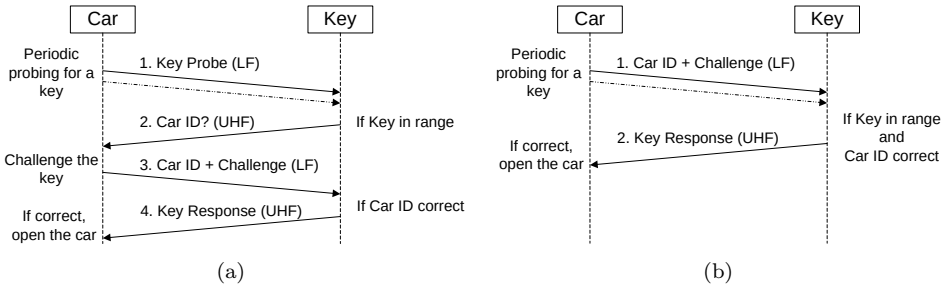
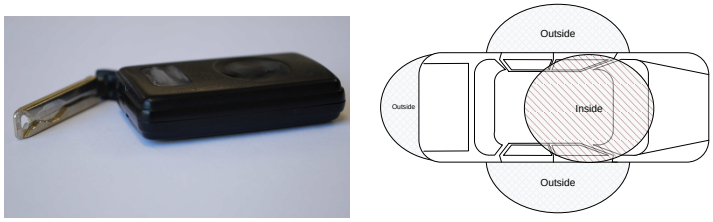


Figure 1: Examples of Passive Keyless Entry System protocol realizations. a) In a typical realization, the car periodically probes the channel for the presence of the key with short beacons. If the key is in range, a challenge-response protocol between the car and key follows to grant or deny access. This is energy efficient given that key detection 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.



(a) A PKES Key and it's backup physical key.

(b) Car LF coverage.

Figure 2: Backup key and LF coverage regions.

Figure 1 shows two example realizations of car opening in a normal mode. The car sends beacons on the LF channel either periodically or when the door handle is operated. These beacons could be either short wake-up messages or larger challenge messages that contain the car identifier. When the key detects the signal on the LF channel, it wakes up the microcontroller, demodulates the signal and interprets it. After computing a response to the challenge, the key replies on the UHF channel. This response is received and verified by the car. In the case of a valid response the car unlocks the doors. Subsequently, in order to start the car engine, the key must be present within the car (region *Inside* in Figure 2(b)). In this region, the key receives different types of messages that when replied will inform the car that the correct key is within the car itself. The car will then allow starting the engine. It should be noted that in normal mode the LF channel is only used to communicate from the car to the key as such operation requires a large amount of energy.

In backup mode, e.g., when the battery is exhausted, the user is still able to open and start his car. The manufacturers usually embed a backup physical key within the key fob to open the car doors. These are shown in Figure 2(a)). In order to start the engine the system uses the passive LF RFID capabilities of the key. Given the very short communication range as discussed before, the user is required to place the key in the close proximity of some predefined location in the car (e.g., the car Start button). We discuss the security implications of that mode of operation in Section 5.

3 Relay Attack on Smart Key Systems

In this section we first describe generic relay attacks, and then we present the attacks that we implemented and tested on PKES systems of several cars from different manufacturers. In our experiments, we relayed the LF communication between the car and the key; the relay of the UHF communication (from the key to the car) was not needed since this communication is 'long' range

Table 2: PKES Access Control Summary

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

(approx. 100m) and is not used in PKES systems for proximity detection. However, similar relay attacks could equally be mounted on UHF communication channel if a longer relay than 100m would be required.

3.1 Relay Attacks

The relay attack is a well known attack against communication systems [20]. In a basic relay attack messages are relayed from one position to another in order to make one entity appear closer to the other. Examples of relay attacks have been shown on credit card transactions [14], between nodes in wireless sensor networks, known as a wormhole attack [21]. An example of relay attack on RFID [2] has been shown in [18]. The attack consists of first demodulating the signal, transmitting it as digital information using RF and then modulating it near the victim tag. In this experimental setup, the relay adds 15 to 20 μseconds of delay. This delay could be detected by a suitable key/car pair as the delay of signal propagation is of the order of nanoseconds for a short distance.

In this work, we design and implement a relay attack in the analog domain at the physical layer. Our attack does not need to interpret, nor to modify the signal, i.e., our attack only introduces the delays typical for analog RF components. It is completely transparent to most security protocols designed to provide authentication or secrecy of the messages. Although some attacks have been reported on key entry systems [22, 30, 10, 7], our attack is independent of such attacks, if a passive keyless entry system uses strong cryptography (e.g. AES and RSA), it would still be vulnerable to our proposed relay attack.

It should be noted that many relay attacks previously presented are modulating and demodulating the signal, in other words they often rely on fake reader and a fake RFID tag. An obvious advantage of such attacks is that they can be performed with commercial off-the-shelf (COTS) hardware. The same setup can also be used to perform replay or message forging. However, this approach has several drawbacks. First, modulation and demodulation significantly increases the response time of the attack; this extra time could be detected and used as a proof of the presence of a relay. Second, such a realization is dependent on the modulation and encoding of the signal, which makes the relay specific to some key model. Both drawbacks are avoided in our design and implementation of the relay attack.

3.2 Description of the Relay Over Cable Attack

In order to perform this attack, we used a relay (Figure 3) composed of two loop antennas connected together with a cable that relays the LF signal between those two antennas. An optional amplifier could be placed in the middle to improve the signal power. When the loop antenna is presented close to the door handle, it captures the car beacon signal and creates a local magnetic field. This field excites the first antenna of the relay, which induces an alternating signal at the output of the antenna. This electric signal is then transmitted over the a coaxial cable and reaches the second antenna via an optional amplifier. The need for an amplifier depends on several parameters such

[2] Although for a different RFID technology namely ISO 14443 at 13.56 MHz.

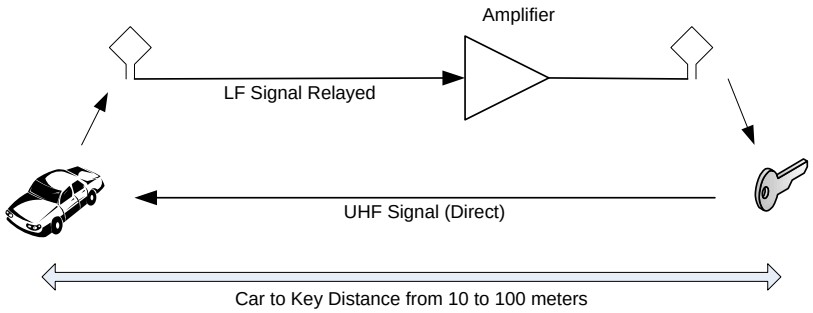


Figure 3: The relay with antennas, cables and an (optional) amplifier.

as the quality of the antennas, the length of the cable, the strength of the original signal and the proximity of the relaying antenna from the car's antenna. When the relayed signal reaches the second antenna of the cable it creates a current in the antenna which in turn generates a magnetic field in the proximity of the second antenna. Finally, this magnetic field excites the antenna of the key. The key then demodulates this signal and receives the original message from the car. In all the passive keyless entry systems we evaluated, this is sufficient to make the key sending the *open* or the *start* authorization message over the UHF channel. The message sent by the key will depend on what was originally sent by the car. The car will send *open* command to the key from the outside antennas and the *start* command form the inside antennas. Therefore, the attacker (e.g., car thief) first needs to present the relaying antenna in front of the door handle such that the key will send the open signal. Once the door is unlocked, the attacker brings the relaying antenna inside the car and after he pushes the brakes pedal or the start engine button the car will send the *start* message to the key.

3.3 Description of the Wireless Relay Attack

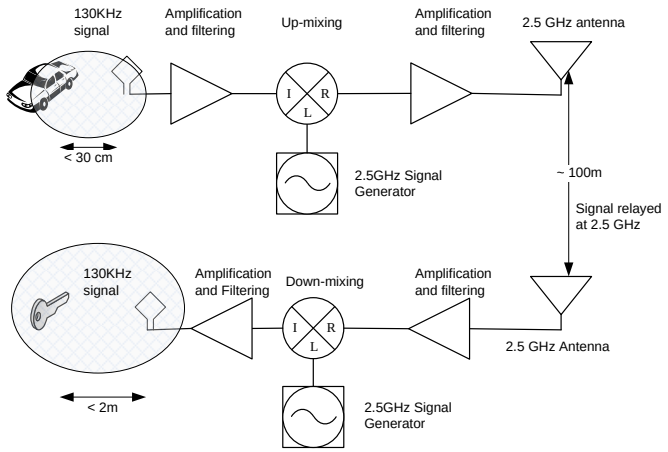


Figure 4: Simplified view of the attack relaying LF (130 kHz) signals over the air by upconversion and downconversion. The relay is realized in analog to limit processing time.

Relaying over a cable might be inconvenient or suspicious. For example, the presence of walls or doors could prevent it. We therefore design and realize a physical layer relay attack over the air. Our attack relays the LF signals from the car over a purpose-built RF link with minimal delays. The link is composed of two parts, the *emitter* and the *receiver*. The *emitter* captures the LF signal and up-converts it to 2.5 GHz. The obtained 2.5 GHz signal is then amplified and transmitted over the air. The *receiver* part of the link receives this signal and down-converts it to obtain the original

LF signal. This LF signal is then amplified again and sent to a loop LF antenna which reproduces the signal that was emitted by the car in its integrity. The procedure for opening and starting the engine of the car remains the same as discussed above.

Using the concept of analog up and down conversion allows the attacker to reach larger transmission/reception relay distances, while at the same time it keeps the size, the power consumption and the price of the attack very low (see Section 3.4) [3].

3.4 Experimental Results

We experimented those attacks against several recent car models from different manufacturers. Both the cable relay and the wireless relay were successful to open the car and start the engine. Some preliminary measurement results on the delay versus distance are reported in Table 3 for both relay attacks.

In the cable LF relay, the delay is primarily introduced by the wave propagation speed in solid coaxial cables which is approximately 66% of that speed in the air. The delay of our amplifier is of the order of a few nanoseconds. In the wireless LF relay, our measurements show a delay of approximately 15-20 ns in both emitter and receiver circuitries, the remaining delay being due to the distance between the antennas, i.e., approximately 35 ns for 10 m. Therefore for larger distances, using the air relay should be preferred in order to keep the delay as low as possible. In order to compute the total delay of the relay attack, i.e., including both the LF and UHF links, we should add the UHF car-key communication which assumes wave propagation with the speed of light and will only depend on the distance.

Figure 5(b) shows the part of the wireless relay that receives messages from the car. Signals are received using the white loop antenna (right on the picture) which must be approached to the car emitting antennas, near the door handle or the start button (Figure 6) in order to obtain a good signal from the car. This signal is amplified, up-mixed and sent at 2.5 GHz with a dipole antenna (black in front of the image).

The receiver, Figure (a) shows the key side of the relay. The antenna (in front) receives the up-mixed signal, in back the signals are relayed to the key using a loop antenna. While the setup on those pictures is made of experimental equipment, it could easily be reduced to two small and portable devices.

Table 3: 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.

Attack	Distance (meters)	Delay (ns)	Comments
Relay over cable	30	160 (±20)	Opening and starting the engine works reliably
	60[1]	350 (±20)	With some cars signal amplification is not required
Wireless relay	10[2]	50 (±20)	Opening of the car is reliable, starting of the engine works[3]

[1] With an amplifier between two 30 m cables.

[2] Tested distance. Longer distances can be achieved.

[3] Starting of the engine is reliable when the clocks are better synchronized.

[3]It could even be possible to transmit in the LF band over large distance, however this would require large antennas and a significant amount of power.

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

Figure 5: Experimental wireless relay setup.

(a) Loop antenna placed in front of the door handle (b) Starting the engine using the relay

Figure 6: The relay attack in practice: (a) openning 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 (from Figure 5(a)) of the wireless relay and the key. Emitter side (Figure 5(b)) of the wireless relay is not shown on this picture.

4 Implications of the Relay Attack on PKES Systems

In this section we discuss implications of relay attacks on PKES systems.

Common Scenario: Parking Lot. In this scenario, the attackers can install their relay setup in an e.g., underground parking, placing one relay antenna close to the passage point (a corridor, a payment machine, an elevator). Once that the user parks and leaves his car, the Passive Keyless Entry System will lock the car. The user then leaves the parking confident that his car is locked (feedback form the car is often provided to the owner with indicator lights or horn). Once that the user leaves the car and it is no longer in its sight, the attackers can place the second antenna to the door handle. The signals will now be relayed between the passage point and the car. When the car owner passes in front of this second antenna with his key in the pocket, the key will receive the signals from the car and will send the *open* command to the car. As this message is sent over UHF it will reach the car even if the car is within a hundred meters[4]. The car will therefore unlock. Once that the attacker has access to the car, the signals from within the car are relayed and the key will now believe it is inside the car and emit the *allow start* message. The car can now be started and driven. When the attacker drives away with the car, the relay will no longer be active. The car may detect the missing key; however, for safety reasons, the car will not stop but is will continue running. Equally, the car might detect a missing key for several other reasons including if the key battery is depleted. Some car models will not notify the user if the key is not found when the car is on course, while some will emit a warning beep. None of the cars we experimented with stops the engine if the key is not detected anymore after the engine is started.

This attack therefore enables the attackers to gain access (open) and to get authorization to drive (start and drive) the car without the possession of appropriate credentials.

Stealth Attack. The described relay attack is not easily traced. Unless the car keeps a log of recent entries and records exchanged signals (e.g., for further analysis in search of relay fingerprints), it will be difficult for the owner to know if his car was entered and driven. Equally, it will be difficult for the user to prove that he is not the one that actually opened and used the car. This is since there will be no physical traces of car entry. This can have further legal implications for car owners in case that their cars or property from their cars are stolen due to this PKES vulnerability.

Combination with Other Attacks. Significant security vulnerabilities have been identified in computer systems of modern cars [23], allowing for example to control safety systems such as brakes or lights from the car internal communication bus. One of the most dangerous results of this study is the demonstration of *rootkits* on car computers that allow an attacker to take control of the entire car. Moreover, the malicious code could erase itself leaving no traces of the attack. The practical risks of such attacks is reported to be reduced as the attacker needs access to the ODB-II communication port, which requires to be able to open the car. The relay attack we present here is therefore a stepping stone that would provide an attacker with an easy access to the ODB-II port without leaving any traces or suspicion of his actions. Moreover, as the car was opened with the original key if an event log is analyzed it would show that the car owner did open the car.

5 Countermeasures

In this section we discuss countermeasures against relay attacks on PKES systems. We first describe immediate countermeasures that can be deployed by the car owners. These countermeasures largely reduce the risk of the relay attacks but also disable PKES systems. We then discuss countermeasures against relay attacks that were suggested in the open literature. We finally outline a new PKES system that prevents relay attacks. This system also preserves the user convenience for which PKES systems were initially introduced.

[4]UHF signal could be equally relayed, which could even further extend the distance from which this attack can be mounted.

5.1 Immediate Countermeasures

Shielding the Key One obvious countermeasure against relay attacks is to prevent the communication between the key and the car at all times except when the owner wants to unlock the car. The users of PKES-enabled cars can achieve this by placing the car key (fob) within a protective metallic shielding thus creating a Faraday cage around the key. A small key case lined with aluminum might suffice for this purpose. While the key is in the key case, it would not receive any signals from the car (relayed or direct). When the user approaches the car, it could take the key out of the case and open and start the car using the PKES system. The users who would opt for this countermeasure would loose only little of the convenience of PKES. Similar countermeasures have been proposed to block the possibility of remote reading of RFID tags embedded in e-passports. However, an attacker might be able to increase the reading power sufficiently to mitigate the attenuation provided by the protective shield. We note that designing a good Faraday cage is challenging [32]. Still, this countermeasure would make the relay attack very difficult in practice.

Removing the Battery from the Key Another countermeasure against relay attacks is to disable the active wireless communication abilities of the key. This can be simply done by removing the battery that powers the radio from the key. As a consequence, the UHF radio of the key will be deactivated. The key will then be used in the "dead battery" mode, which is provided by the manufacturers to enable the users to open the car when the key battery is exhausted. In this case, the car cannot be opened remotely but only using a physical key (the backup physical key is typically hidden within the wireless key fob). Given that the cars that use PKES cannot be started using a physical key, in order to start the car in the "dead battery" mode, the user needs to place the key in the close proximity of some predesignated location in the car (e.g., the car Start button). The car then communicates with the key's passive LF RFID tag using short-range communication. Typically, wireless communication with the LF RFID tags is in the order of inches, thus making the relay attack more difficult for the attacker; however, depending on the attacker capabilities relay from a further distance cannot be fully excluded. This defense disables the PKES for opening the car, but is still reasonably convenient for starting the car engine. With such a defense, the realization of a relay attack becomes very difficult in practice.

A combination of the two countermeasures would provide the highest protection, but would also be the least convenient for the users. It would essentially reduce the usability of a PKES key to the one of the physical key.

5.2 Countermeasures in the Open Literature

Several countermeasures against relay attacks were proposed in the open literature [5]. We examine them here and analyze their effectiveness and appropriateness for PKES systems.

One of the first countermeasures proposed against relay attacks is to rely on the signal strength to indicate the proximity between the devices. This is in fact the countermeasure that is used in today's PKES systems; the car transmits a short range LF signal such that only if the key is in its close proximity ($\leq 1m$) will it hear the signal. Similarly, the car could measure the strength of the signal that the key transmits in order to infer the distance to the key. This countermeasure is very weak and can be simply defeated since the attacker can fully mimic the car and the key by relaying signals using expected signal levels. Other countermeasure that rely on the measurements of signal properties, like those using complex modulation schemes, measure group delay times or measure intermodulation products suffer from similar shortcomings. Namely, an attacker equipped with a good antenna and waveform generator can mimic expected signal features [5] or can simply relay the observed signals without demodulating them. In [5] signal corruption is also reported as a possible countermeasure against relay attacks. However, the authors note that this countermeasure can be overcome by an attacker using a good amplifier.

Relay attacks can equally be prevented using multi-channel communication, where typically out-of-band channels are used to verify if the relay occurred [16]. However, these approaches require

[5] See [11] for an example of signal fingerprint replay.

human involvement, and as such are not well suited for PKES systems.

5.3 Our Proposal: PKES that Relies on RF Distance Bounding

Like other car entry and start systems, the main purpose of PKES is to allow access to the car and authorization to drive to the user that is at the time of entry and start physically close to the car. By being close to the car, the user indicates its intention to open the car and by being in the car, to drive the car. The car therefore needs to be able to securely verify if the user is close to the car to open the car and if the user is in the car to start the car.

Given this, a natural way that can be used to realize secure PKES systems is by using distance bounding. Distance bounding denotes a class of protocols in which one entity (the verifier) measures an upper-bound on its distance to another (trusted or untrusted) entity (the prover). This means that given that the verifier and the prover and mutually trusted, the attacker cannot convince them that they are closer than they really are, just further [6].

Background on Distance Bounding Protocols In recent years, distance bounding protocols have been extensively studied: a number of protocols were proposed [8, 19, 14, 28, 42, 21, 36, 25, 17, 41] and analyzed [9, 38, 15, 35]. These proposals relied on ultrasonic or RF only communication. Since ultrasonic distance bounding is vulnerable to relay attacks [39], RF distance bounding is the only viable option for use in PKES systems.

Regardless of the type of distance bounding protocol a distance bound is obtained from a rapid exchange of messages between the verifier and the prover. The verifier sends a challenge to the prover, to which the prover replies after some processing time. The verifier measures the round-trip time between sending its challenge and receiving the reply from the prover, subtracts the prover's processing time and, based on the remaining time, computes the distance bound between the devices. The verifier's challenges are unpredictable to the prover and the prover's replies are computed as a function of these challenges. In most distance bounding protocols, a prover XORs the received challenge with a locally stored value [8], uses the received challenge to determine which of the locally stored values it will return [19, 41], or replies with a concatenation of the received value with the locally stored value [34]. Authentication and the freshness of the messages prevents the attacker from shortening the measured distance.

Recently, two RF distance bounding implementations appeared, showing the feasibility of the implementation of distance bounding protocols. One implemented XOR resulting in a processing time at the prover of approx. 50ns [24] and the other implemented concatenation with the prover's processing time of $< 1ns$ [34].

PKES Requirements for Distance Bounding Implementation Accurate Measurement of the distance is crucial to defending against relay attacks. The distance is directly proportional to the time of flight of the exchanged messages between the key and the car. Even more important than the actual processing time at the key is the variance of this processing time. If the key responds in a constant time then the actual duration of time taken by the key to respond is not important. Here, we naturally assume that the car trusts the key. This holds as long as the attacker is unable to advance neither the challenge messages from the car nor the response messages from the key, i.e. messages are fresh and authenticated.

Assuming that the delay incurred by the relay attack is dependent only on the relay cable length (or relay distance in the case of a wireless setup), the additional delay added by the relay attack is proportional to the speed of the signal in the cable and the length of the cable. For a standard *RG 58* coaxial cable, the specification provides that a speed of signal in that cable is equal to 2/3 of the speed of light in vacuum (that we denote by c). Therefore assuming that the UHF reply propagates at the speed of light in vacuum, the relay with a 30m long cable adds $30/c + 30/(2c/3) = 250ns$ of delay to the measured round-trip time between the car and the key.

[6] In the analysis of distance bounding protocols the attack by which an attacker convinces the verifier and the prover that they are closer than they truly are is referred to as the Mafia Fraud Attack [13].

Thus, if the round-trip time measurement in the distance bounding implementation shows a variance higher than $250ns$ then it will be impossible to detect the above described attack. If this variance is few orders of magnitude smaller than the delay introduced by the relay then the verifier will be able to deduce the response time of the key and therefore be able to compute the distance to the key reliably. Given that the maximum distance at which the key should be able to open the door (without action from the user) is at most $1m$, the maximum standard deviation of the measured round-trip time should be less than $2/c = 6ns$.

One recent implementation of RF distance bounding [34] showed that the processing time of the prover (key) can be stable with a rather small variance of $62ps$. This suggest that current and upcoming distance bounding implementations will be able to meet the requirements of PKES systems.

Sketch of the Solution A PKES system based on RF distance bounding would therefore work in the following way. When the user approaches the car, the key and the car would perform a secure distance bounding protocol. If the key is verified to be within $2m$ distance, the car would unlock and allow the user to enter. In order to start the car, the car will verify if the key is in the car. This can be done using a verifiable multilateration protocol proposed in [43], which allows the car to securely compute the location of a trusted key. Verifiable multilateration requires that at least three verifying nodes are placed within the car, forming a verification triangle, within which the location of the key can be securely computed.

6 Related Work

Low-Tech Attacks on Car Entry and Go Systems Low-tech attacks such as lock-picking physical locks of car doors or using hooks can be used to open a car. The hook is pushed between the window and the door and the thief tries to open the door by hooking the lock button or command. However, these low-tech attacks are less reliable on new car systems or when an alarm system is present. Lock-picking also leaves traces which can be analyzed by a forensics investigator [12].

Cryptographic Attacks A significant amount of research has been performed on the cryptographic algorithms used by remote key entry systems such as Keeloq [22, 30, 10], TI DST [7]. Vulnerabilities are often the consequence of too short keys, weak encryption algorithms that were not publicly reviewed by the community or side channel weaknesses. Consequently, manufacturers are moving towards more secure and well established ciphers (e.g., Atmel documentation recommends AES [26]). However, solving such issues by moving to the best cipher to date will not solve physical-layer relay attacks. The relay attack is independent of the cipher used; no interpretation or manipulation of the data is needed to perform a relay attack.

Jamming and Replay A well known attack against keyless car opening systems is to use a simple radio jammer. When the user step away from his car he will push the key fob button to lock the car. If the signal is jammed, the car won't receive the *lock* signal and will therefore be left open. If the car owner did not notice that his car didn't lock, the thief will be able to access it. However a jammer can not help a thief to start the car. Another related attack is to eavesdrop the message from the key fob and replay it (e.g., using on a fake reader/key pair). Standard cryptographic protocols using a counter or a challenge-response technique provide defense against message replay.

Part Providers Major electronic parts suppliers provide components for passive keyless entry systems [26, 40, 29, 27], those components are then used buy various car manufacturers. Although variations exists in the protocols and cryptographic blocks (Keeloq in [27], TI DST in [40], AES in [26]), all manufacturers provide systems based on the same combined LF/UHF radio technology as we discussed in Section 2. Therefore, those systems are likely to be impacted by the attack we have presented.

Attacks on Keyless Systems The closest work to our investigation can be found in [5, 6]. The authors perform security analysis of Keyless Car Entry systems including relay attacks. While the performed analysis identifies the relay problem, the proposed relay attack consists of two separate UHF relay links to relay messages in both directions. The proposed abstract setup has the problem of creating a feedback loop as the car will also receive the relayed signal from the second link. We show that such a realization is not needed in modern PKES systems and demonstrate it experimentally. Moreover, the authors do not propose any hardware design, nor practical implementation of the attack. Finally, no adequate countermeasures are proposed.

Some practical attacks on PKES systems have been recently reported [4]. However, no detailed information is available and it is not possible to understand the details of the attack. It is unclear if the attack relies on a modulation/demodulation relay or on a physical-layer relay attack. Moreover, it is impossible to verify the reported claims and if the attack is indeed real.

7 Conclusion

In this paper, we showed that the introduction of PKES systems raises serious concerns for the security of car access and authorization to drive systems. We demonstrated on several cars from different manufacturers that PKES systems in some modern cars are vulnerable to relay attacks. This attack allows an attacker to open the car and start the engine by placing one antenna close to the key holder and the second antenna close to the car. We demonstrated the feasibility of this attack using both wired and wireless setups. Our attack works for a specific set of PKES systems that we tested and whose operation is described in this paper. However, given the generality of the relay attack, it is likely that PKES systems based on similar designs are equally vulnerable to the same attack.

We proposed simple countermeasures that minimize the risk of relay attacks and that can be immediately deployed by the car owners; however, these countermeasures also disable the operation of the PKES systems. We further discussed countermeasures against relay attacks that were suggested in the open literature and we sketched a new PKES system that prevents relay attacks. This system preserves convenience of use for which PKES systems were initially introduced.

References

[1] *http://www.mercedes-benz.com/.*

[2] *http://en.wikipedia.org/wiki/Smart_key.*

[3] *http://en.wikipedia.org/wiki/Keyless_Go.*

[4] *http://vintrack.com/SIU.html.*

[5] A. Alrabady and S. Mahmud. Some attacks against vehicles' passive entry security systems and their solutions. *Vehicular Technology, IEEE Transactions on*, 52(2):431 – 439, march 2003.

[6] A. Alrabady and S. Mahmud. Analysis of attacks against the security of keyless-entry systems for vehicles and suggestions for improved designs. *IEEE Transactions on Vehicular Technology*, 54(1):41–50, january 2005.

[7] S. C. Bono, M. Green, A. Stubblefield, A. Juels, A. D. Rubin, and M. Szydlo. Security analysis of a cryptographically-enabled RFID device. In *Proceedings of the 14th USENIX Security Symposium*, Berkeley, CA, USA, 2005. USENIX Association.

[8] S. Brands and D. Chaum. Distance-bounding protocols. In *EUROCRYPT '93*, pages 344–359, Secaucus, NJ, USA, 1994. Springer-Verlag New York, Inc.

[9] J. Clulow, G. P. Hancke, M. G. Kuhn, and T. Moore. So near and yet so far: Distance-bounding attacks in wireless networks. In *Proceedings of the European Workshop on Security and Privacy in Ad-hoc and Sensor Networks (ESAS)*, 2006.

[10] N. T. Courtois, G. V. Bard, and D. Wagner. Algebraic and slide attacks on KeeLoq. In *Fast Software Encryption: 15th International Workshop, FSE 2008, Lausanne, Switzerland, February 10-13, 2008, Revised Selected Papers*, pages 97–115, Berlin, Heidelberg, 2008. Springer-Verlag.

[11] B. Danev, H. Luecken, S. Čapkun, and K. Defrawy. Attacks on physical-layer identification. In *WiSec '10: Proceedings of the 3th ACM Conference on Wireless Network Security*, pages 89–98. ACM, 2010.

[12] Datagram. Lockpicking forensics. Black Hat USA Briefings, 2009.

[13] Y. Desmedt, C. Goutier, and S. Bengio. Special uses and abuses of the Fiat-Shamir passport protocol. In *CRYPTO*, pages 21–39, 1987.

[14] S. Drimer and S. J. Murdoch. Keep your enemies close: distance bounding against smartcard relay attacks. In *Proceedings of 16th USENIX Security Symposium*, Berkeley, CA, USA, 2007. USENIX Association.

[15] M. Flury, M. Poturalski, P. Papadimitratos, J.-P. Hubaux, and J.-Y. Le Boudec. Effectiveness of Distance-Decreasing Attacks Against Impulse Radio Ranging. In *3rd ACM Conference on Wireless Network Security (WiSec)*, 2010.

[16] F.-L. W. Frank Stajano and B. Christianson. Multichannel protocols to prevent relay attacks. In *Financial Cryptography*, 2010.

[17] S. Gezici, Z. Tian, G. Giannakis, H. Kobayashi, A. Molisch, H. Poor, and Z. Sahinoglu. Localization via ultra-wideband radios: a look at positioning aspects for future sensor networks. *Signal Processing Magazine, IEEE*, 22(4):70–84, July 2005.

[18] G. Hancke. Practical attacks on proximity identification systems (short paper). In *IEEE Symposium on Security and Privacy*, 2006.

[19] G. P. Hancke and M. G. Kuhn. An RFID distance bounding protocol. In *SecureComm '05: Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks*, pages 67–73, Washington, DC, USA, 2005. IEEE Computer Society.

[20] G. P. Hancke, K. Mayes, and K. Markantonakis. Confidence in smart token proximity: Relay attacks revisited. *Computers & Security*, 28(7):615–627, 2009.

[21] Y.-C. Hu, A. Perrig, and D. B. Johnson. Wormhole attacks in wireless networks. *IEEE Journal on Selected Areas in Communications*, 24(2):370–380, 2006.

[22] S. Indesteege, N. Keller, O. Dunkelman, E. Biham, and B. Preneel. A practical attack on KeeLoq. In *EUROCRYPT'08: Proceedings of the theory and applications of cryptographic techniques 27th annual international conference on Advances in cryptology*, pages 1–18, Berlin, Heidelberg, 2008. Springer-Verlag.

[23] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, and S. Savage. Experimental security analysis of a modern automobile. In *Proceedings of the 31st IEEE Symposium on Security and Privacy*, May 2010.

[24] M. Kuhn, H. Luecken, and N. O. Tippenhauer. UWB impulse radio based distance bounding. In *Proceedings of the Workshop on Positioning, Navigation and Communication (WPNC)*, 2010.

[25] J.-Y. Lee and R. Scholtz. Ranging in a Dense Multipath Environment Using an UWB Radio Link. *IEEE Journal on Selected Areas in Communications*, 20(9), December 2002.

[26] P. Lepek and P. Hartanto. RF design considerations for passive entry systems. Atmel automotive compilation, Volume 6, page 20. Online: http://www.atmel.com/dyn/resources/prod_documents/article_passive_entry_s.pdf.

[27] Microchip. Passive keyless entry (PKE) reference design, users manual. Online: ww1.microchip.com/downloads/en/DeviceDoc/DS-21986A.pdf.

[28] J. Munilla, A. Ortiz, and A. Peinado. Distance bounding protocols with void-challenges for RFID. Printed handout at the Workshop on RFID Security – RFIDSec 06, July 2006.

[29] NXP Semiconductors. Passive keyless entry. Online: http://www.nxp.com/#/aip/aip=[aip=147]—pp=[t=aip,i=147].

[30] C. Paar, T. Eisenbarth, M. Kasper, T. Kasper, and A. Moradi. KeeLoq and side-channel analysis-evolution of an attack. *Fault Diagnosis and Tolerance in Cryptography, Workshop on*, 0:65–69, 2009.

[31] P. Papadimitratos, M. Poturalski, P. Schaller, P. Lafourcade, D. Basin, S. Čapkun, and J.-P. Hubaux. Secure Neighborhood Discovery: A Fundamental Element for Mobile Ad Hoc Networking. *IEEE Communications Magazine*, 46(2):132–139, February 2008.

[32] A. Perrig, M. Luk, and C. Kuo. Message-in-a-bottle: User-friendly and secure key deployment for sensor nodes. In *Proceedings of the ACM Conference on Embedded Networked Sensor System (SenSys 2007)*, October 2007.

[33] M. Poturalski, P. Papadimitratos, and J.-P. Hubaux. Towards Provable Secure Neighbor Discovery in Wireless Networks. In *Proceedings of the 6th ACM workshop on Formal methods in security engineering*, 2008.

[34] K. B. Rasmussen and S. Capkun. Realization of RF distance bounding. In *to appear in USENIX Security Symposium 2010*.

[35] K. B. Rasmussen and S. Čapkun. Location privacy of distance bounding protocols. In *CCS '08: Proceedings of the 15th ACM conference on Computer and Communications Security*, pages 149–160, New York, NY, USA, 2008. ACM.

[36] N. Sastry, U. Shankar, and D. Wagner. Secure verification of location claims. In *WiSe '03: Proceedings of the 2nd ACM workshop on Wireless security*, New York, NY, USA, 2003. ACM.

[37] P. Schaller, B. Schmidt, D. Basin, and S. Capkun. Modeling and verifying physical properties of security protocols for wireless networks. In *22nd IEEE Computer Security Foundations Symposium*, pages 109–123. IEEE Computer Society Washington, DC, USA, 2009.

[38] P. Schaller, B. Schmidt, D. Basin, and S. Capkun. Modeling and verifying physical properties of security protocols for wireless networks. In *CSF '09: Proceedings of the 2009 22nd IEEE Computer Security Foundations Symposium*, pages 109–123, Washington, DC, USA, 2009. IEEE Computer Society.

[39] S. Sedighpour, S. Čapkun, S. Ganeriwal, and M. Srivastava. Implementation of attacks on ultrasonic ranging systems (demo). In *Proceedings of the third ACM International Conference on Embedded Networked Sensor Systems (Sensys)*, 2005.

[40] Texas Instruments. Car access system: Car access solutions from Texas Instruments. Online: http://focus.ti.com/docs/solution/folders/print/528.html.

[41] N. O. Tippenhauer and S. Čapkun. Id-based secure distance bounding and localization. In *In Proceedings of ESORICS (European Symposium on Research in Computer Security)*, 2009.

[42] S. Čapkun, L. Buttyán, and J.-P. Hubaux. SECTOR: Secure Tracking of Node Encounters in Multi-hop Wireless Networks. In *Proceedings of the ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN)*, Washington, USA, October 2003.

[43] S. Čapkun and J.-P. Hubaux. Secure positioning in wireless networks. *Selected Areas in Communications, IEEE Journal on*, 24(2):221–232, Feb. 2006.

[44] T. Waraksa, K. Fraley, R. Kiefer, D. Douglas, and L. Gilbert. Passive keyless entry system. US patent 4942393, 1990.