ANALYSING REMOTE KEYLESS ENTITY SYSTEMS

KiranRaj KG[1], Shahikant Khot[2], Ananya Choudhary[3], Ratan Singh[4]
Ajeenkya DY Patil University – Pune

Abstract

For many years, security has been extensively studied for immobilizers and remote keyless entry systems. Apart from relay threats, there was little attention paid to active, keyless entry and start devices that are commonly used for luxury vehicles. In this venture we completely reverse engineer and complete a Passive Keyless Entry & Start Program. Our analysis shows several vulnerabilities in security. In keeping with a previously adopted strategy, Jam-listen-replay, our new attack strategy requires only a jammer and a signal logger. We conducted attacks on six different car models that are shown to be effective. In all the cases tested and with a broad range of system parameters, the attack is successful. We also contrast our approach with state-of-the-art assaults, demonstrate that the found weaknesses improve in past attacks, and conclude that remote keyless entity system implementations are not secure.

Keywords: *Remote Entity Attacks, Modern supercar vulnerability, Supercars hijacking.*

1. Introduction

Renault developed the first Remote Keyless Entry (RKE) system for cars in 1982. Instead of Radio Frequency (RF), these systems used infrareds at the time. Today, the vehicles usually have a Remote Keyless Entity system and often have a Passive Keyless Entry (PKE) system. The first enables users, by pressing a button, to lock and unlock a key-fob their vehicle. When the primary fob is nearby, the latter releases the vehicle automatically

However, cars use an immobilizer, which tests whether the user's key fob is valid before starting the engine. The use of immobilizer devices substantially decreased the number of car thefts, according to Van Ours and Vollaard. Although two distinct systems traditionally were without key input and immobilization, today, luxury cars often combine this into a one-way passive keyless input and Start (PKES) system.

Mainly a request-response protocol is enforced with minimal security coverage between the fob and the car radio transceiver. Many security vulnerabilities were found over the years, and the RKS has been evolving to prevent these assaults. This enables the vehicle to be unlocked and the immobilizer to be unlocked without any user interaction. Moving to PKES systems results in higher user convenience, but could also facilitate some attacks as no legitimate user interaction is required.

2. ATTACK OUTLINE

Three objects are involved in our attack scenario: the vehicle, the owner of the car (user), and the opponent who wants to steal the car from the client.

The opponent applies his plan in the following 3 phases:

1. Setup
2. Recording and Jamming
3. Hijacking

The attack takes place in a series of 3 steps:

1. Jammer set-up and activation.
2. Jamming the interaction between the user and the car and forcing the user to use the mechanical button or the key. Leaving the car unattended, the opponent hijacks the vehicle.

2.1 SETUP

This is the intermediate step that the competitor requires when the vehicle is left unattended by the client. In reality, the opponent has a jammer to put on the vehicle. As can be seen below, the Jammer is a very portable device composed predominantly of a Raspberry Pi V3 (RPiv3) attached to a HackRF One, a very inexpensive Software Defined Radio (SDR), ready to be deployed. In several locations outside of the vehicle, the total machinery may be stored, for instance, by using a magnet under the car frame.

2.2 JAMMING AND RECORDING

The device must be switched on after activation by jamming a specific frequency or blocking the contact between the fob and the engine. Because the driver can not unlock the car with the fob, he returns to the mechanical key after several tries. In comparison, by eavesdropping the fob-car communication channel, the adversary can capture one or more code sequences emitted by the fob (and never accessed by the car).

2.3 HIJACKING

Finally, the owner of the car must push the car forward utilizing the mechanical button or keys. We should inform you that a jammer is mounted on the vehicle, stopping the fob from accessing the lock mechanism of the car. The four opponents will then execute the attack by replaying one of the code sequences already documented to allow the car to be hijacked. The interaction rate followed by the car brand is the only uncertain variable to the previous method. By performing a session that senses fractions of the radio spectrum, the opponent can easily discriminate. The bulk of the cars we used have a Frequency band nearly 433MHz. Our experiments show.

3 REQUIREMENTS AND CONFIGURATIONS

Our system is composed of two components: the Jammer and the Logger code series.

3.1 JAMMER

In conjunction with the HackRF One and a power bank, as shown in Fig.2, we used a handheld jammer.

HackRF One: HackRF One is a Great Scott gadget-developed open-source, semi-duplex Radio Defined System with the capacity to receive or transmit radio signals starting from 1 MHz to 6 GHz.
ANT500: The ANT500 antenna, typically designed to operate from 75 MHz to 1 GHz, is a telescopic antenna built by great Scott gadgets. The length can be changed between 20 cm and 88 cm.

Raspberry Pi v3: We installed GNU Radio on the RPiv3 and exploited the Python SDK to control the Hack RF One. The result is a script to transmit white Gaussian noise on a target frequency.

Power bank: We have a generic 5000mA power bank that guarantees our system a long-term lifespan (about half a day).

We used the embedded WiFi to access it via SSH and turned on and off the various jamming parameters in the RPiv3. It can be noticed that the jamming frequency (433MHz) is far from the WiFi (2.4GHz), which makes it possible to monitor the jammer remotely. We also set all the gains for the 40dB HackRF One system, i.e., the RF band, the IF band and the BAB. Eventually, we set the rate of sampling (SPS) to 2 M to jam the contact with fob-cars without disrupting other community communications.

3.2 LOGGER

The logger is mainly made up of a mobile platform capable of documenting the fob string.
The following framework has been adopted:
Laptop: A laptop with a Linux-based Ubuntu and the GNU Radio Companion has been installed.
HackRF One and ANT500 Antenna: a HackRF One was attached to the laptop to capture all of the neighborhood's software signals.
Our logger configuration and main links are outlined in Figure 3.

The SDR specification they tested was 434 MHz peaks, 2 M sample speed (SPS), 10dB RF, 20 dB IF, and 20 dB BB. We note that the logger's profit statistics differ significantly from those used by the jammer. In addition, to decipher the fob-transmitted code string, the logger must minimize the noise power of the jammer. The values above are the products of several experiments and also bring the relative distances between a jammer, the fob, and the logger into consideration.

4 MEASUREMENTS

In our university, we have done some experiments in the parking area, while the parking is vacant and not to compete with other users (AJEENKYA DY PATIL UNIVERSITY, PUNE, MAHARASHTRA).

The first phase of our assault is to define the rate of contact that the interaction between fob and car. Although different car manufacturers may use different frequencies, globally, there are two primary frequencies: 315MHz for North America at 433.92MHz for Europe and Asia. An attacker can, therefore, quickly detect the frequency band in a few consecutive checks. Other unknown parameters such as ASK, FSK, PSK can be found by using simple tools like gqrx [1],

Skoda Yeti (2016), Skoda Octavia (2009), Mazda6 (1999), Toyota Rav4 (2014), Mitsubishi Pajero (2015), and Nissan Sunny (2014) we have checked the attack on these cars. Another small challenge that we have to face with our attack is to find the most effective jammer position in the car. The best position, obviously, is close the siginal receiver of the car. The jammer should remain hidden from the consumer, and an ideal place has proven to be on the back of the car (for all car models). They have tested multiple locations throughout the target car

5 RESULTS

Six separate displacements have been listed, i.e., dCF{5,10} and dFL{1, 2, 3, 4}, each of them running as shown in Table 1 twenty-four times. Secondly, we notice that if the gap between the logger and the fob (dFL) increases the odds of the attack are diminished. They illustrate the limited protection of the logger from the existence of the jammer itself. Indeed, this is proved by the fact that when the distance between the jammer/car and the fob (dCF) gets larger, the logger can record a 7 good code sequence at 3 meters from the fob (that distance is reduced to 50cm when the fob is 5m away from the jammer).

Table 1. Results

DCF (M)	DFL (M)	Attack Frequency
5	1	1
5	2	0.4
5	3	0.05
10	2	1
10	3	1
10	4	0.1

6. CONCLUSION

We suggested a new scenario assault with a modern jamming technique and a remote-controlled signal recorder for remote keyless entry systems. In light of various delivery approaches, we check the assault on six different models. The cheap HW, quick attack installation and efficiency always efficient, even for a wide range of device parameters demonstrate that RKS remains unsafe.

References

[1] Gqrx sdr, http://gqrx.dk.

[2] Remote keyless systems, https://en.wikipedia.org/wiki/Remote_keyless_ system.

[3]van de Beek, S., Vogt-Ardatjew, R., Leferink, F.: Robustness of remote keyless entry systems to intentional electromagnetic interference. In: 2014 International Symposium on Electromagnetic Compatibility. pp. 1242–1245 (Sept 2014).

[4] Di Pietro, R., Oligeri, G.: Jamming mitigation in cognitive radio networks. IEEE Network 27(3), 10–15 (May 2013)

[5] Di Pietro, R., Oligeri, G.: Freedom of speech: Thwarting jammers via a probabilistic approach. In: Proceedings of the 8th ACM Conference on Security & Privacy in Wireless and Mobile Networks. pp. 4:1–4:6. WiSec '15, ACM, New York, NY, USA (2015).

[8] Di Pietro, R., Oligeri, G.: Silence is Golden: Exploiting jamming and radio silence to communicate. ACM Trans. Inf. Syst. Secure. 17(3), 9:1–9:24 (Mar 2015)

[9] Kamkar, S.: Drive it as you hacked it: New attacks and tools to wirelessly steal cars. In: DEFCON 23 (2015)