Marin Aranitasi, et. al. International Journal of Engineering Research and Applications
www.ijera.com
ISSN: 2248-9622, Vol. 12, Issue 4, (Series-III) April 2022, pp. 09-15

RESEARCH ARTICLE OPEN ACCESS

Increasing the vehicle security by improving the Remote Key System

Marin Aranitasi*, Igli Tafa**
**(Department Basics of Informatics, Polytechnic University of Tirana, Albania)*
*** (Department of Informatics Engineering, Polytechnic University of Tirana, Albania)*

ABSTRACT
These days the number of vehicles that are being used is incredibly high compared to the number of the population. The advantages that this tool gives the users comes with the need to increase its security. The locking technology in modern vehicles is called Remote Keyless System (RKS) and it is composed by two subsystems, one that is responsible for the locking/unlocking and the other responsible for the ignition. The key fob, as an integral part of the RKS generates signals to control the vehicles functionality. Even though the theft rate has decreased in the last decades, the introduction of new technology contributes to a higher risk of theft in the future. The focus of this article is the detailed analysis of the vehicle locking system: design, functionality and mostly the vulnerabilities. We will show the main methods that are currently used to attack the vehicle security using the Remote Keyless System (RKS) and what measurements we could take to prevent some of these attacks. In the end we present one of the possible techniques that can increase the vehicle security by limiting access on the communication between fobs and cars.

Keywords - security, vehicles, RKS, RKE, immobilizer, attacks

---

Date of Submission: 09-04-2022 Date of Acceptance: 26-04-2022

I. INTRODUCTION

Nowadays we have the largest number of vehicles on road since the creation of the first automobile. A precise number is difficult to calculate but according to [1] we could have more than 1.4 billion vehicles all around the globe. For a population of 7.9 billion people, that means a car for every 5-6 people. This means that it's much likely that we have a car for almost every two families (an average family of 4 members). The number of cars is likely to double in the next 15 years. The likelihood that you or your family are or are going to be the owner of a car is great. But your asset is constantly at threat of being stolen. Even though the theft rate has dropped in the last years when we can see [2] 43% drop from the year 1991 to 2019 in the US, the improvement of technology which allowed the addition of smart gadgets to vehicles is increasing the surface which intruders can use to access and stole your car. All those smart features of modern cars are controlled by ECUs (Electronic Control Units). All ECUs are connected by a wired network called the Controller Area Network (CAN). Hackers can exploit some vulnerable ECUs and use them to access and control the whole system. Some attacks can be found in [3], [4], and [5].

Even though those attacks are practical they require from adversary to have high technical knowledge and the target car to be a high-end model with remote connectivity features. In this paper, the focus is the locking system and what methods are being used to overcome it

II. VEHICLE SECURITY

Car security consists of measurements that should prevent primarily the possibility to enter the vehicle and start the engine. So modern cars have multiple systems to guarantee this level of security. We have the RKE (Remote Keyless Entry System) which primarily handles the functions of locking and unlocking the vehicles. Also, the immobilizer system handles the engine start-up.

As detailed in article [6] we have transmitted from simple lock keys to key-less technology. Picking locks in the past ("pre-YouTube era") needed techniques like "bumping" (inserting a blank key for the specific car model and hitting it with a hammer). Nowadays even modern locks can be picked with the right set of tools and the correct technique.

After the simple locks system from the year 1998, most of the new cars came with a new type of key: transponder key. This type of key also known

as chip key has a small chip on its body. To start the engine of the motor, first, the key should be inserted into the ignition module, when the key is rotated the chip inside is provided with energy which is used to send a signal to the immobilizer system ECU. If this signal contains the correct code, the engine will start running. So even with an identical physical key but with a different chip code, a theft cannot steal that car. The introduction of this technology also prevented thieves to start a car by hot-wiring it or breaking the ignition module. Stealing a car with a chip key security system is hard even for thieves. As explained in [7] thieves need to act as the owner of the car, go to their dealership, and get a copy of the physical key with a not programmed chip. Using this key, they can unlock the car's doors. If he wanted to just access your car and steal anything that you have left inside it, he accomplished the task. To steal the car, he needs to start the vehicle's engine, which can be achieved by possessing a professional scanner to program the blank key's chip. This action can take up to 15 minutes which can be considered a lot of time for someone who is trying to not be seen from breaking the law.

The mainstream locking technology found in our cars today is Remote Keyless System (RKS), this technology was introduced after chip keys. This system usually is built by two subsystems, the Remote Keyless Entry System (RKE) and the Remote Keyless Ignition System (RKI). RKE primarily handles the functions of locking and unlocking vehicles. The RKI or the immobilizer system handles the engine start-up. With the RKS systems, now we have a physical key plus a fob. The fob allows to perform the same actions as the key and even more. A key fob is an RF device that can generate signals and broadcast them to communicate with the vehicle. By using the fob, you can lock/unlock the car, start the engine, set the alarm system, open the truck, etc. When a user pushes a button, the fob generates a signal which contains the command code, an id, and other fields necessary for authentication and security. To guarantee the safety of communication the signal is encrypted through a cryptographic mechanism. This technology has increased car user's commodity because cars can execute a command in a range as far as 100 meters. It is important to notice that to start the car the physical key should be inserted into the ignition module. A more advanced form of keyless entry technology is the Passive Keyless Entry System and Passive Keyless Entry and Start System (PKE and PKES). The fob which is part of this system is called Smart Key. This type of key is found usually in luxury brand cars. The user just needs to have the fob with himself, and the car is going to be automatically opened when user pulls the door's handle, and the engine can start by pushing a button on the car. This is achieved because the fob is constantly releasing a signal to communicate with the car. When the car detects that the user is close enough it fires its unlocking system to open the doors. When user is in the driver's seat the car still detects the proximity of the fob and starts the engine when the user presses the start-up button. Also, through this technology, if the car detects that the user is at a fair distance from the vehicle it automatically locks the doors if the user has forgotten.

The most advanced type of key in the present is the digital key. Or more specifically the usage of a smartphone with a vehicle device as a key fob. On [8] [9] we can see implementations of this technology from Hyundai and Apple. This technology is applied even from companies as Tesla, GM, Volvo, Lincoln, Ford, BMW. But what can this technology provide better compared to fobs? Smartphones have better hardware components and performing more complex cryptographic algorithms is possible. Another benefit is the fact that sharing keys can be achieved flawlessly. Imagine being in another country and you ask a friend to take your car and go somewhere. You first need to send the key to him wasting a lot of time and some money through postal services. A digital key can be shared instantly with no physical barrier. The key can be set to be temporary to allow access to a specific user only for some time. Another entry system of the future is the biometric system when the key to access your vehicle and start the engine can be your biometric data [8]. Doors can be opened only by your fingerprints and additional inputs can be required as iris identification, voice, and facial recognition. It should be noted even though those systems are primarily designed to use fobs all the time to interact with vehicles, most of the manufacturers provide a physical-mechanical key as a backup in case of fob's battery is dead. This key can be used to open automobile doors on RKE systems, although the ability to start the engine depends on the fact if the immobilizer chip has the same power source as the RKE system

III. RKE USAGE

Most of the cars produced nowadays are designed with a remote keyless entry system [10]. Let's explain how this technology works:

1. When a user presses a button on the key fob, this turns on its CPU.
2. CPU creates and sends a data stream to the radio frequency transmitter which generates a radio signal based on this data and broadcasts it through an antenna.

3. On the vehicle side, we have a receiver that captures the signal and sends it to the car's CPU.

CPU decodes the data and sends the appropriate commands to the command module of the vehicle

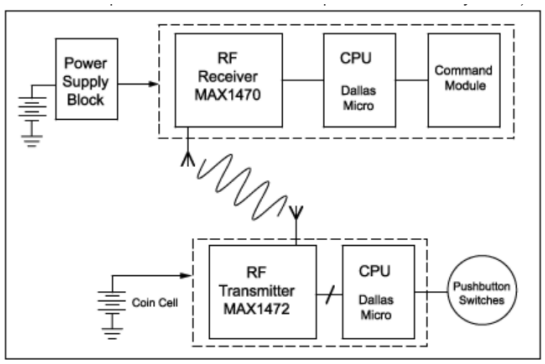

Fig 1. An RKE system consists of a key fob circuit (lower diagram) and receiver circuit in the vehicle (upper diagram). [11]

On a wireless communication system, we usually have three components: transmitter, receiver, and antenna [12].

Transmitter gets a data stream, generates the corresponding radio signal based on data, and forwards it to the antenna. The antenna is responsible for transmitting the electromagnetic signal over the air or receiving from it. This signal is carried to the receiver which should transform this weak signal captured by the antenna into a signal which contains all the original data sent by the transmitter. Also, another job of the receiver is to filter unnecessary signals over the air which were not intended for the system where the receiver belongs

IV. DATA FRAME

What data are being transmitted between key fob and vehicle? Every time that the key fob is pressed, we transmit a signal which contains an address field that is used for identification, the data for the action required to perform, and a rolling code for security reasons.

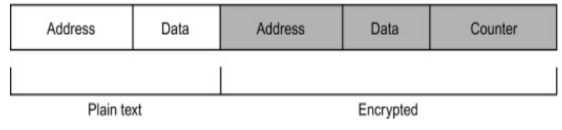

Fig. 2. Key fob signal frame template [13]

On [14] we have two real model frames generated from reverse-engineering the vehicles' signal. Although they are different from each other and contain some unique fields they contain all the elements described above.

With each command that we push on our key fobs, we transmit a signal on-air that contains two parts. As we can see on [13]. We have a part of the signal which contains data in plain text form and encrypted data. The receiver in our cars gets the signals on the air, filters them, and accepts them based on plain data address fields. After a signal is determined that it was intended for our system the signal should be decrypted. Then we have a comparison if the decrypted data matches the plain data.

For security reasons, each signal contains a counter which is called rolling code. This value is a 40bit (depends on model) number [15] which increments with every new command. For a car to accept a command as legit, the signal that it receives should be one of the next 256 counters of the last saved counter on the vehicle. This security measurement has been implemented to avoid the danger of accessing a car with a signal that a legit key fob has generated by simply replaying the same signal. For example, if the signal did not contain the rolling code someone with a radio device can capture and save a signal which unlocks the car, created by the key fob. Later the thief can launch this signal and the car is going to be unlocked. The presence of the rolling code prevents this situation from happening, by telling the car controller to accept only commands with a rolling code which should be one of 256 next ones.

V. SECURITY RISKS

The introduction of keyless systems was a security standard meant for convenience. Even though it's a technology easy to use it also added new vulnerabilities to overall car security. In this section, we will describe the methods that are used to exploit those vulnerabilities to steal the car or the valuables inside it.

Types of attack that thieves use to steal vehicles with a keyless security system:

- Jamming attack,
- Replay attack,
- Cryptographic attacks [14]
- Relay attack
- RollJam attack
- Key programming

Jamming attacks - consists of using a jamming device that transmits signals on a range of frequencies which are intended to decrease the signal-to-noise ratio of legit signals (we call legit signals – signals released from the fob). This noise can transform the original signal by changing its characteristics and make the receiver drop this signal. So, the car is not going to execute any signal. If the user tried to lock the car and didn't check the flashing lights of the car, he has left the car open.

Replay attack – this type of attack was more common before the introduction of rolling codes. The signal which key-fob transmitted contained only the fob id and the command type. Someone can record this signal and then retransmit it to access the vehicle. To evade this kind of attack is necessary that each signal transmitted to be different from the previous ones. This has been achieved by the introduction of rolling codes on RKE systems and a pseudo-random-generated value for immobilizer systems. But this kind of attack still can happen even with the presence of rolling codes. A situation when this can happen is when an adversary has the fob for few seconds, pushes the button, and records the signal. The car must be out of reach from the fob. Later he can use this signal to open the vehicle.

About the cryptographic attack, they usually consist of using computation power to receive the cryptographic key. The adversary collects some valid signal from a legit key fob to the car (we can call these traces) and uses these traces to reverse engineer the frame and calculate the key. On [16] [14] just 4 to 8 traces and few minutes are enough to enter and start the car. The main vulnerability is the fact that most of the cryptographic schemas are outdated and provide little security for nowadays risks. The most common cryptographic mechanisms that we can find on fobs are [14] Hitag2, Hitag3, Megamos, DST40, Keeloq, AES. Fobs use symmetric encryption instead of the more secure asymmetric version. This happens because like the case with IoT devices we must deal we limited resources which constrains the fob's design. It should be noted that asymmetric encryption can consume 100 times more CPU cycles than symmetric encryption [17]. Mostly of cryptographic schemas use a key with a size of 40 to 80 bits which is not enough to provide safety for the current computation power of our computers. Hitag2 schema which is found both on REK and immobilizer systems can be easily broken with method on [14].

A relay attack is two people attack. Each person has a relay box. One adversity should stay with the device close to the car's door and the other one should try to capture the key fob signal by being in proximity of it. If the second relay box captures the signal, it gets amplified and delivered to the first relay box. The first relay box transmits the signal to the door and the PREK system unlocks the door. If the car has a push to start system, the key fob should be placed close to the ignition button to start the car. To prevent this type of attack the key fob should be kept inside a Faraday box or electro equipment like fridge, microwave, etc. Also, some key fobs have a button to turn them off when not needed.

RollJam attack was created to bypass a REK that has implemented rolling code as a security measurement. As mentioned before: a car with rolling code on its signal frame does not accept as valid, signals with a rolling code smaller or equal to that of the last executed command by the car. So, what a RollJam device does is: when a car owner presses a button on its fob the RollJam is using an antenna to jam the signal and another one to save the signal. In this way, the car is not going to receive a valid signal. So, it's not going to execute the command. If the user did not detect that the car didn't react, the car could be left open. If the user detects the issue, he is going to repeat the command, the RollJam device is going to save and jam this signal too. After jamming it's going to transmit the first saved signal. The user is going to see that the car executed the command. The adversity now has a signal with a greater rolling code (second signal) than the last executed (first signal). He can broadcast the signal to access the car. More on RollJam attack can be seen at [18].

Key programming [19] is a technique when an adversary after entering a car with a start push button, can program a new fob using the diagnostic port under the steering wheel which can be used to start the car.

VI. ESCAPING FROM THE CURRENT FOB LIMITATIONS

A key fob is a small and limited device that always deals with the hardships of having limited resources. They are two solutions to escape from this situation:

- Implementation of better technology on building key fobs to provide more computing power and better battery life
- Integrate the key fob capabilities to a more powerful device possessed by any car owner
- Key fobs have low computing power because their power capacity is small. They have a small 3V battery on their body which should power on the device for an average of three to four years. This lifespan is an important aspect of RKE systems in terms of commodity because the fob doesn't have any led signal to inform the user about the remaining charge. If the battery needs to be replaced too quickly, it's not going to be a likable feature. There are some solutions for this:
- Increasing the battery size to allow more computation power for the same lifespan
- Designing the fob with a chargeable battery. The fob should have a power indicator and for convenience can allow wireless changing as we

find in smartwatches. The charging dock could be incorporated on the vehicle panel.

- Removing the need for batteries as providers of electricity by generating electricity from heat and light [20]. If this technology can be developed further to allow running more powerful devices with just the heat generated from hands it could be a perfect application for fobs technology. The solution of energy harvesting is not limited to light and heat but also includes wind, sound waves, RF radiation, etc.

VII. PROPOSED SOLUTION

Bensky proposes a time-based solution [13] for RollJam attacks. Adding a time field on the signal's frame is going to make replayed signal invalid because the difference between signal creating and the time that signal was received should be bigger than the allowed difference. The time field should be encrypted to prevent tampering with the value. A prototype of this solution can be found on [21]. Because of the vulnerability that RKE systems have from relay attacks the industry has reacted and implemented some changes to its security protocols [22]:

- Adding features like video monitoring, location tracker, fuel-consuming, system hacking notification to allow a user to track the vehicle even if it got stolen.
- Designing the key fob to transmit the signal on such a broad range that conventional relay boxes cannot transmit the whole signal.
- Incorporating motion sensor on key fob which stops the fob from transmitting data when fob has been stationary for some time.
- Some brands are creating smart keys with a button that can turn them off, so no signal is going to be transmitted and no signal can be eavesdropped.

Most key fobs use a loop antenna [23]. The radiation pattern of this antenna is shown in the image below. From what we can see from the pattern if we reduce the human body influence the wave should propagate the same distance for the same amount of time (a spherical wave). This is convenient, ideally, the car's owner just needs an air distance of 100 meters and neither the direction of the key fob nor our direction is going to influence the propagation of signal over the air. In real life factors like the human body should be taken into consideration and the wave shape tends to be less than a perfect sphere.

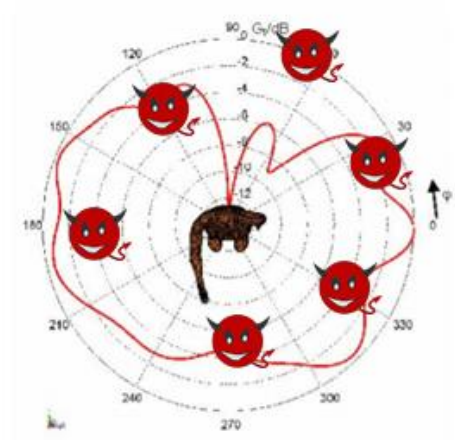

Figure 3. Key fob loop antenna radiation pattern [23]

The wireless communication problem is that signal is open for everyone to eavesdrop. Even though methods like encryption are employed the speed of evolution of IT computing power is much bigger than that of the development of vehicles security systems which also tend to be used for a long time. So, if an adversary can capture the signal, save it, and then can work on cracking the cryptography mechanism. Broadcasting the message on 360 degrees, to potential malicious antennas in every direction when you are sure in which direction your car is parked seems like overkill.

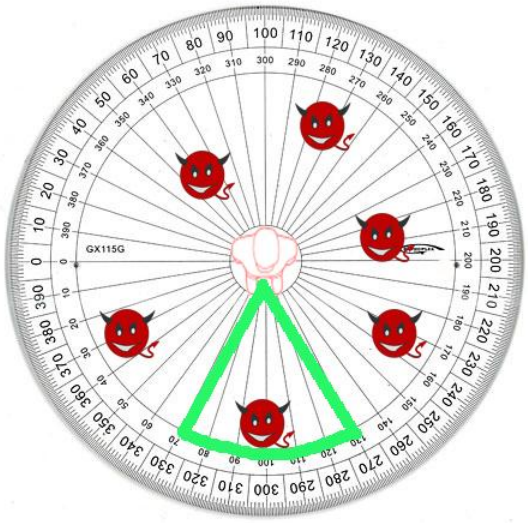

Fig. 4. New key fob antenna to limit the spread of signal

The cases when you don't know when your car is parked are too little. It's not difficult just to take the key fob from your pocket, direct it toward the car and press the button. Even if it feels unintuitive at first, it's going to become a muscle reflex soon. It may be uncomfortable, but this is how security works even in everyday life. For example, it

is recommended to have a different password for each website account, even though it can be hard to remember too many passwords it is necessary if we are concerned about our virtual life security.

VIII. CONLCUSIONS

After reviewing many possible attacks against Remote Keyless Systems, we can say that this system can offer convenience, but not necessarily security. Because components communicate wirelessly data can be eavesdropped. The best method to protect the data is by reducing the accessibility. This was the reason why we proposed a new antenna type for the RKE system. On simple RKE systems, by getting the communication data, adversaries could open the vehicles, steal anything inside but not the car itself. By incorporating the immobilizer system into the fob for the PRKES systems, security becomes worst. Relay boxes can be purchased online or if someone is skilled enough, he can make them. Through them, even the engine can be started**.** These attacks require good knowledge of technology and cannot be implemented by anyone. RKS is fine for non-critical operations like turning on the heater but for your car security, you should pray to not be eyed by a professional thief. In the end if you can lock your car with a physical key and not trust 100% the RKE system, because of the security issues that we presented, it is strongly recommended to do it.

REFERENCES

[1]. Andrew Chesterton, "How many cars are there in the world?,", CarsGuide, 6 August 2018. [Online]. Available: https://www.carsguide.com.au/car-advice/how-many-cars-are-there-in-the-world-70629. [Accessed 6 August 2021].

[2]. "Insurance Information Institute," 2020. [Online]. Available: https://www.iii.org/fact-statistic/facts-statistics-auto-theft. [Accessed 9 August 2021].

[3]. E. Kovacs, "https://www.securityweek.com/," Security Week, 03 05 2021. [Online]. Available: https://www.securityweek.com/tesla-car-hacked-remotely-drone-zero-click-exploit. [Accessed 07 September 2021].

[4]. Tencent Keen Security Lab, "https://keenlab.tencent.com," 22 03 2018. [Online]. Available: https://keenlab.tencent.com/en/whitepapers/Experimental_Security_Assessment_of_BMW_Cars_by_KeenLab.pdf. [Accessed 08 September 2021].

[5]. Y. K. K. G. S. Kyong-Tak Cho, "Who Killed My Parked Car?," University of Michigan, Ann Arbor, 23 January 2018. [Online]. Available: https://arxiv.org/pdf/1801.07741.pdf. [Accessed 5 September 2021].

[6]. "Evolution of Car Door Lock System," Das European Autohaus, [Online]. Available: https://daseuropeanautohaus.com/evolution-of-car-door-lock-system/. [Accessed 10 August 2021].

[7]. "Top 3 Ways Thieves Steal Cars," Ratchets And Wrenches, 25 November 2018. [Online]. Available: https://www.youtube.com/watch?v=j6Wntha7ft8. [Accessed 26 August 2021].

[8]. "The Future of Car Keys," Hyundai Motor Group, 18 June 2021. [Online]. Available: https://news.hyundaimotorgroup.com/Article/The-Future-of-Car-Keys. [Accessed 5 September 2021].

[9]. J. Clover, "Car Keys: A New Feature That Lets You Unlock a Car With Your iPhone or Apple Watch," MacRumors, 2 February 2021. [Online]. Available: https://www.macrumors.com/guide/carkey/. [Accessed 5 September 2021].

[10]. "Explaining remote keyless entry in cars," Essentra Components, 11 April 2018. [Online]. Available: https://www.essentracomponents.com/en-gb/news/product-resources/explaining-remote-keyless-entry-in-cars. [Accessed 17 August 2021].

[11]. "Requirements of remote keyless entry systems," Maxim Integrated, 16 February 2005. [Online]. Available: https://www.maximintegrated.com/en/design/technical-documents/app-notes/3/3395.html. [Accessed 18 August 2021].

[12]. L. E. FrenzelJr., "Electronics Explained Fundamentals for Engineers, Technicians, and Makers," ScienceDirect, 2018. [Online]. Available: https://www.sciencedirect.com/topics/engineering/keyless-entry-system. [Accessed 18 August 2021].

[13]. AlanBensky, "Communication protocols and modulation," Science Direct, 2019. [Online]. Available: https://www.sciencedirect.com/science/article/pii/B978012815405200004X. [Accessed 18 August 2021].

[14]. J.-s. M. S.-y. Z. Z.-j. L. a. Z.-l. L. Hai-long LIU, "Practical Contactless Attacks on Hitag2-Based Immobilizer and RKE systems," School of Optics and Electronic

Information, Huazhong University of Science and Technology, Wuhan, Hubei 430074, China, 2018. [Online]. Available: https://www.dpi-proceedings.com/index.php/dtcse/article/view/24750/24383. [Accessed 30 August 2021].

[15]. "Remote Keyless Entry Systems," The Clemson University Vehicular Electronics Laboratory, [Online]. Available: https://cecas.clemson.edu/cvel/auto/systems/remote_keyless_entry.html. [Accessed 20 August 2021].

[16]. D. O. Flavio D. Garcia, "Lock It and Still Lose It," University of Birmingham;, 10 August 2016. [Online]. Available: https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/garcia. [Accessed 27 August 2021].

[17]. Alan Grau, "Why Automotive Key Fob Encryption Hacks Are Making Headlines," Sectigo, 24 March 2020. [Online]. Available: https://sectigo.com/resource-library/why-automotive-key-fob-encryption-hacks-are-making-headlines. [Accessed 3 September 2021].

[18]. A. Yared, "Jamming Attacks," 2016. [Online]. Available: https://sites.tufts.edu/eeseniordesignhandbook/files/2016/04/EE98_TechNote_2016_OrangeTeam_Yared.pdf. [Accessed 1 September 2021].

[19]. "Keyless car theft prevention: six ways thieves can break into a car and how to prevent it," Sunday Times Driving, 18 January 2020. [Online]. Available: https://www.driving.co.uk/news/features/six-ways-thieves-can-break-into-a-car-and-how-to-prevent-it/. [Accessed 2 September 2021].

[20]. P. Woodman, "Battery-Free IoT Sensors!," everactive, 3 November 2020. [Online]. Available: https://www.youtube.com/watch?v=1vW1l7oGt5U. [Accessed 4 September 2021].

[21]. D. R. H. D. K. M. Q. N. K. A. S. Kyle Greene, "Timestamp-based Defense Mechanism Against Replay Attack in Remote Keyless Entry Systems," Electrical and Computer Engineering Department, College of Engineering and Sciences Purdue University Northwest, Hammond, IN, USA, 2020. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9043039. [Accessed 7 September 2021].

[22]. James Dolan, "14 Cars That Can't Be Stolen," hotcars, 18 September 2020. [Online]. Available: https://www.hotcars.com/19-cars-that-are-almost-impossible-to-steal/. [Accessed 6 September 2021].

[23]. M. B. A. S. M. W. A. S. A. G.-A. Chakam, "Comparison of key-fob antennas vehicle access system," Siemens VDO Automotive AG, Regensburg, Germany, 16 November 2007. [Online]. Available: https://ieeexplore.ieee.org/document/4458858. [Accessed 27 August 2021].

[24]. "Fighting vehicle crime," Interpol, 2021. [Online]. Available: https://www.interpol.int/en/Crimes/Vehicle-crime/Fighting-vehicle-crime. [Accessed 10 September 2021].