Defend Your Vehicle against Relay Attack
-Defense Technology against Latest Automotive Theft Technique-

Daisuke Moriyama, Automotive System Security Department, Automotive Core Technology Development Division, Automotive Solution Business Unit, Renesas Electronics Corporation

Background

Automotive car theft is a critical issue for drivers. EU law enforcement recorded 447,700 cars theft in 2020 [1]. The FBI reported 810,400 vehicles were stolen across the US in 2020; this is increased by 11.8% from 2019 [2][3]. NICB (National Insurance Crime Bureau) reported in 2018 that around 60% of stolen cars could not recovered [4]. These cars are sometimes disassembled and exported to another country to avoid the tracking of criminal activity. Historically, physical keys controlled the lock/unlock mechanism is performed with a physical key and most vehicles still have physical key options as a secondary entry option. However, many automotive companies provide a passive keyless entry with start (PKES) system, in addition to the remote keyless entry (RKE) systems. PKES and RKE are now the primary way individuals access their vehicle today. With a PKES system, not only can you gain access to the vehicle but this technology enables you start the engine if the PKES key fob is in close proximity (1-2 meters) to the vehicle. Now you can access your vehicle and start the car without any physical connection to the vehicle. While PKES and RKE offer a layer of convenience for vehicle users, they introduce an additional wireless attack vector for criminals.

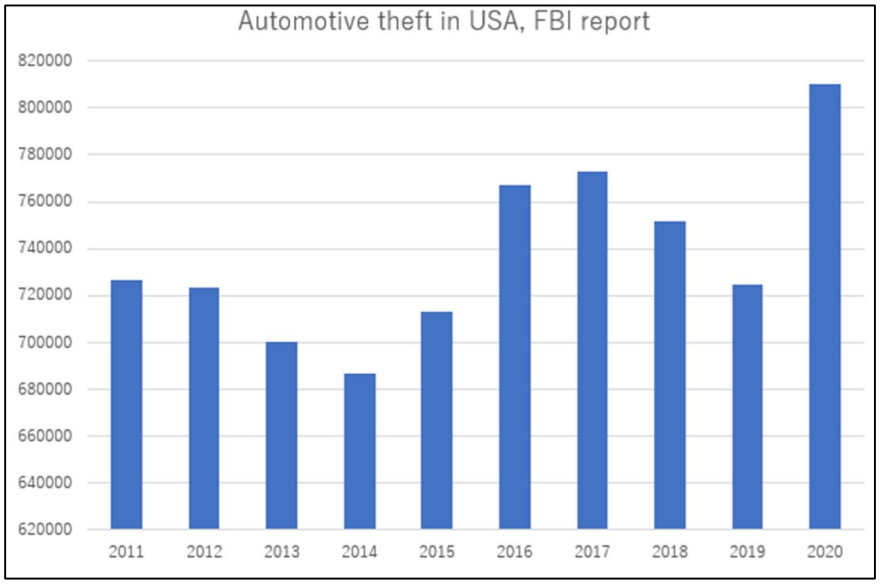

Figure 1. Statistics of automotive theft in USA [2][3]

© 2022 Renesas Electronics

On the PKES Key Fob Security

Each PKES key fob has a built-in authentication mechanism. One PKES key fob can open only one unique vehicle A specific handshake interaction between the key fob and a target car is performed using radio frequencies and advanced communication protocols. A small microcontroller contained in the key fob utilizes a cryptographic algorithm to perform an authentication and transmits a valid response against the challenge message given from the vehicle.

One very naive approach to check the validity is to store a unique number in both automotive and key fob. If the key fob receives a wake-up message from the vehicle as the owner goes to the vehicle parking space, it sends the unique number. The target vehicle unlocks the door only if the receiving number is equivalent to the stored number. One optional idea is to store the multiple of unique numbers and use one of them. However, this mechanism is vulnerable in the real world. It is easy for an adversary to mount a replay attack by recording messages transmitted from a legitimate PKES key fob. When the adversary resends them on behalf of the key fob later, the target vehicle unlocks the door. Several OEMs had introduced rolling code schemes to prevent replay attacks around the year 2000; rolling code schemes disallow older codes and both the transmitter and receiver using the rolling code algorithm will compute the next valid transmissions.

Because automotive security was not a trend topic 10 years ago, several vehicles only equip such a naive verification method with the PKES key fob interaction. Therefore, if the transmitted message is replayed, these cars has opened the door. Even rolling code algorithms are still subject to replay attacks. For example, several security researchers reported that KEELOQ® (*1) previously used in many OEMs as a Rolling code algorithm was insecure against the replay attack or cryptoanalysis [5][6][7]. In fact, a device called “code grabber” memorizes the transferred data emitted from the key fob during the legitimate interaction and it sends the recorded message on behalf of the original key fob later. While it is hard to determine how automotives are stolen by the criminals, vehicle theft with the code grabber is practical and many websites still provide a reminder to care against the code grabber. This attack can be minimized when the response from the key fob is not pre-determined and its variation is exponentially large (e.g., it looks like randomly chosen 128-bit sequence) from the technical viewpoint. Therefore, a typical symmetric key based challenge response authentication can be a countermeasure against the replay attack. If the cryptographic algorithm itself is secure and its corresponding key is securely managed, there is no leakage from the generated output. Moreover, if an authentication protocol implemented in the key fob and automotive is secure, then no malicious message injected by the attacker can be accepted and the target vehicle does not open the door nor start the car for the illegitimate person.

(*1) KEELOQ is a trademark or registered trademark of Microchip Technology Inc.

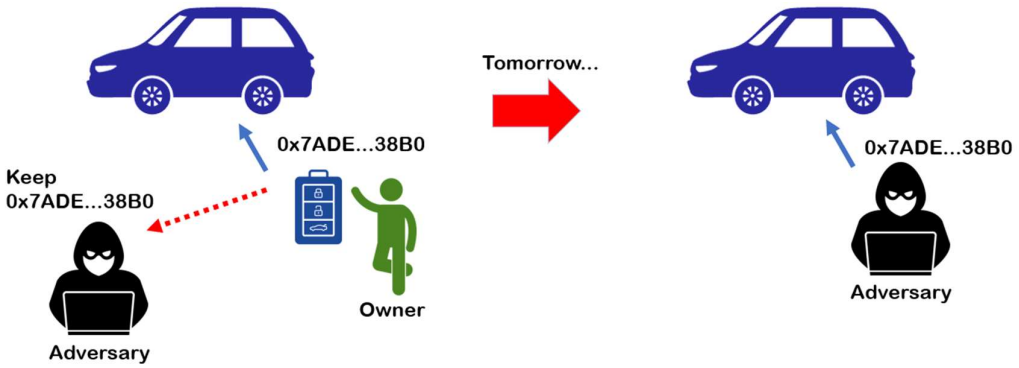

Figure 2. Automotive Theft with Code Grabber

What is a Relay Attack?

With the large adoption of PKES systems the automotive car theft landscape has change and the relay attack has become popular in recent years. Even if a secure challenge-response authentication is implemented in the key fob device, the relay attack bypasses the security mechanism because the relay attack targets the physical layer in the communication.

The relay attack is mounted by two colluded attackers. One attacker is close to the target vehicle and another adversary gets near to the key fob (put on the shelf in a house or kept in an original driver's pocket). When two people activate the special devices, these devices intermediate the communication between the automotive and key fob. While the signal source emitted by the original key fob is at most 2 to 5 meters long, the two special devices relay the communication and drastically lengthen the communication range (e.g., up to 300 meter) depending on the device customization and environment.

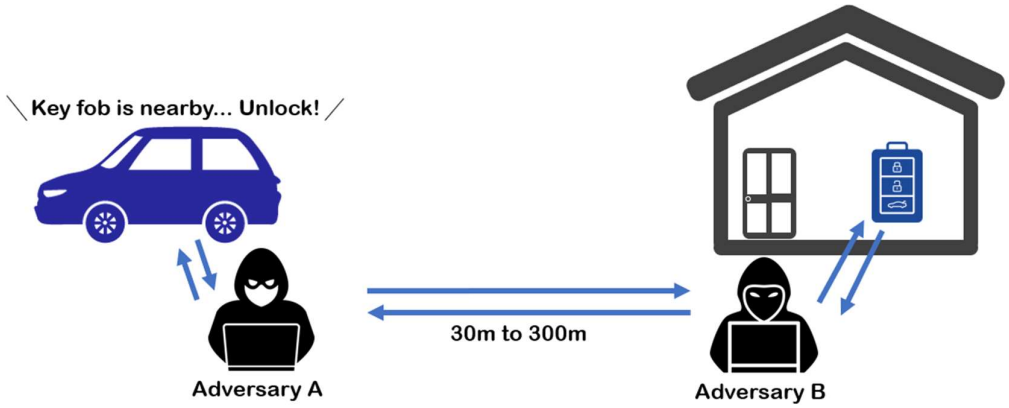

Figure 3. Automotive Theft with Relay Attack

Actually, US law enforcement sometimes discloses the crime scene captured by surveillance cameras showing thieves conducting a relay attack to steal a luxury car [8]. Japanese police arrested a person who stole a vehicle and they confiscated the device to mount the relay attack in 2019 [9].

The traditional PKES key fob uses Low Frequency (LF) or Ultra High Frequency (UHF) transmitter. Several automotive companies provide an optional service for latest series of vehicle so that the user's smartphone can be worked as a key fob. In this case, Bluetooth Low Energy (BLE) communication is performed between the smartphone and automotive for authentication to lock/unlock the door. Moreover, BLE has a function of proximity authentication to limit the communication range. However, a cyber security research group identified in 2022 that the current BLE proximity authentication is not enough to defend the relay attack [10]. Therefore, more technical approach is required to prevent the relay attack.

Ranging Measurement with Ultra Wide Band (UWB)

As the automotive theft with the relay attack is cited in many web pages, many developers rethink which wireless interface can tackle this problem, Especially, they focus on the Ultra Wide Band (UWB) technology because it provides various distance measurement methods and its accuracy can be smaller than 10cm. Especially, UWB supports the evaluation of the Round Trip Time (RTT). One RTT can be calculated with the following equations.

A verifier has a high precision timer and starts the count when it sends a message to the prover at time $\boldsymbol{t_s}$. When a prover receives the message (wireless signal), it runs a specific program to derive a response. Assume $\boldsymbol{t_p}$ is the total computation time until the prover sends the response to the verifier. Upon receiving a message from the prover, the verifier stops the count at time $\boldsymbol{t_e}$. In this situation, the total communication period is calculated as $\boldsymbol{t_e - t_s}$. The wireless signal transmission over the air among this duration is computed as $\boldsymbol{(t_e - t_s) - t_p}$. The half of this duration is typically called Time of Flight (ToF). ToF shows the consumed time to transmit a one-way signal between two devices. When the propagation speed which is uniquely determined by the radio frequency is denoted by $\boldsymbol{ps}$, the distance $\boldsymbol{dist}$ between the prover and verifier is computed as $\boldsymbol{dist = ps \times ((t_e - t_s) - t_p)/2}$.

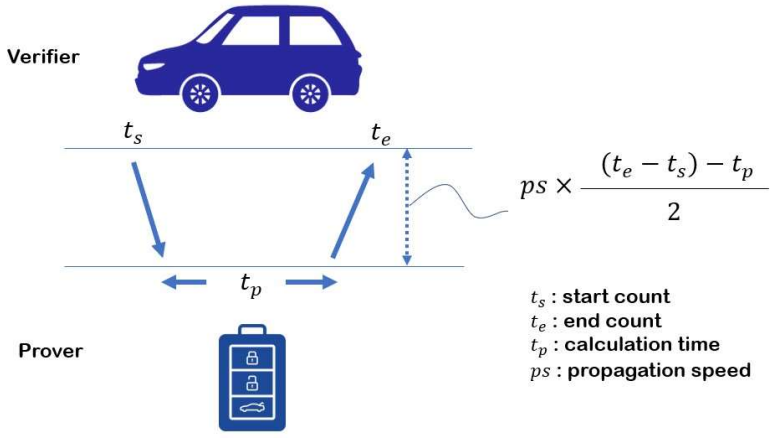

Figure 4. Distance Estimation from Communication Time

If $\boldsymbol{t_p}$ consumed by the prover is predetermined, the variance caused in this estimation is only caused by the physical environment. When the maximum distance to be supported (quality assurance) in this authentication is settled, there exists a reference time duration $\boldsymbol{t_{max}}$ which

is the borderline of acceptance or rejection. If $(t_e - t_s) - t_p > t_{max}$, it is suspectable that the communication may be relayed. This observation and statistical analysis from the Proof of Concept design will provide a reliable constant t_{max} in the commercial product.

The RTT-based ranging method provides a precise distance measurement, but unfortunately this single method does not ensure the absolute security. The original UWB specification standardized in 2007 as IEEE 802.15.4a defines a RTT-based ranging mechanism. However, several research results insist that the current method is insufficient and more enhanced security is needed [11]. As a result, UWB specification was amended in 2020 as 802.15.4z to improve the security aspect.

UWB standardized as IEEE 802.15.4z defines the two types of physical transmission method: Low Rate Pulse (RPT) and High Rate Pulse (HRP). LRP transmits one bit pulse with a wide interval at a high power. The receiver can easily detect the individual signal. LRP is applicable when one or few data is frequently exchanged in an upper layer protocol. UWB LRP supports cryptographic distance bounding protocols that typically perform the challenge-response authentication protocol with a limited time slot.

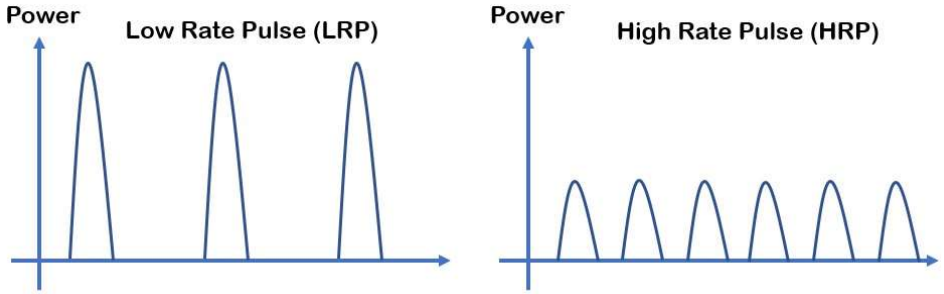

Figure 5. Difference of LRP and HRP defined in UWB

In the case of HRP, data sequence is transmitted with a short interval at a low power. While the throughput of HRP is higher than LRP, the transmitted signal may be delayed or overlapped with physical interferences as fence, hedge, building, etc. The receiver finds out an appropriate peak signal and signal order to recover the original message by checking the received signal pulse and the characteristics.

The ranging measurement defined in UWB HRP is performed with Scrambled Timestamp Sequence (STS) which is generated by a sender and verified by a receiver. This value is derived from symmetric key encryption algorithm AES with input a shared secret key and 32-bit counter. Therefore, the transaction message corresponding with STS cannot be predicted in advance from the third party. Currently, Car Connectivity Consortium provides the Digital Key 3.0 specification so that UWB HRP is mainly used for the ranging measurement, and it specifies that 4,096-bit (4,096 pulses) STS is generated from AES in total and transmitted for the distance measurement. By checking the consistency of the received STS from the expected value, a verifier estimates the prover is in a certain proximity. As a consequence, UWB HRP can prevent the typical relay attacks currently mounted to the non-UWB wireless technology.

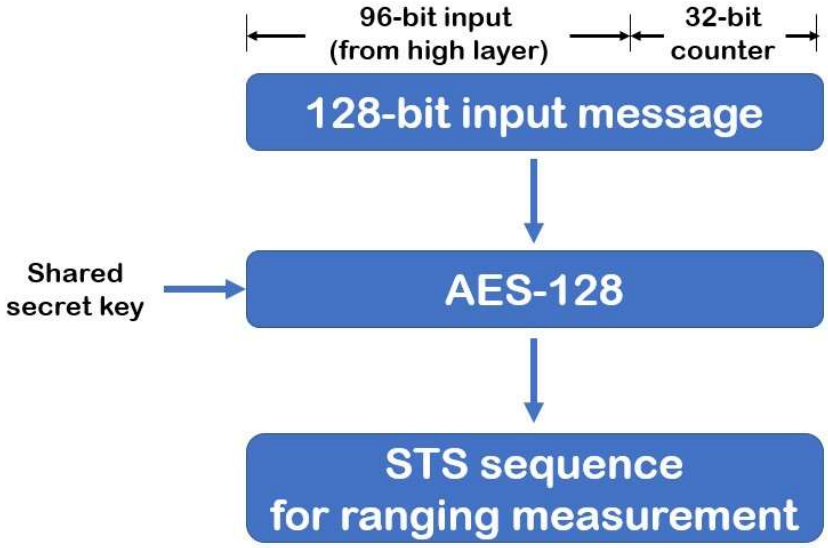

Figure 6. STS Generation used for Distance Measurement in UWB HRP

Conclusion

The automotive car theft with relay attack became a critical issue around 2020. In this white paper, we briefly reviewed a historical transition about PKES key fob security. While the relay attack is a new threat from the car owners, UWB can be a reasonable solution to minimize the relay attack using the STS method in the previous section. Digital Key 3.0 adopts the UWB system architecture as a ranging method; then STS will be widely used in the near future as a security countermeasure for the relay attack.

[References]

[1] https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Crime_statistics&oldid=568499#vehicle_thefts_in_the_EU_in_2020.2C_a_further_11.25_decrease_in_2020
[2] https://ucr.fbi.gov/crime-in-the-u.s/2019/crime-in-the-u.s.-2019/topic-pages/motor-vehicle-theft
[3] https://www.iii.org/fact-statistic/facts-statistics-auto-theft
[4] https://www.nicb.org/news/blog/nicb-west-region-task-forces-vehicle-recovery-work
[5] https://www.defcon.org/html/defcon-23/dc-23-speakers.html#Kamkar
[6] https://www.iacr.org/archive/eurocrypt2008/49650001/49650001.pdf
[7] http://eprint.iacr.org/2008/058.pdf
[8] https://www.youtube.com/watch?v=8pffcngJJq0
[9] https://www.asahi.com/articles/ASM715KJWM71OIPE01Y.html (in Japanese)
[10] https://research.nccgroup.com/2022/05/15/technical-advisory-ble-proximity-authentication-vulnerable-to-relay-attacks/
[11] https://ieeexplore.ieee.org/document/5714149

IMPORTANT NOTICE AND DISCLAIMER

RENESAS ELECTRONICS CORPORATION AND ITS SUBSIDIARIES (“RENESAS”) PROVIDES TECHNICAL SPECIFICATIONS AND RELIABILITY DATA (INCLUDING DATASHEETS), DESIGN RESOURCES (INCLUDING REFERENCE DESIGNS), APPLICATION OR OTHER DESIGN ADVICE, WEB TOOLS, SAFETY INFORMATION, AND OTHER RESOURCES “AS IS” AND WITH ALL FAULTS, AND DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT OF THIRD PARTY INTELLECTUAL PROPERTY RIGHTS.

These resources are intended for developers skilled in the art designing with Renesas products. You are solely responsible for (1) selecting the appropriate products for your application, (2) designing, validating, and testing your application, and (3) ensuring your application meets applicable standards, and any other safety, security, or other requirements. These resources are subject to change without notice. Renesas grants you permission to use these resources only for development of an application that uses Renesas products. Other reproduction or use of these resources is strictly prohibited. No license is granted to any other Renesas intellectual property or to any third party intellectual property. Renesas disclaims responsibility for, and you will fully indemnify Renesas and its representatives against, any claims, damages, costs, losses, or liabilities arising out of your use of these resources. Renesas' products are provided only subject to Renesas' Terms and Conditions of Sale or other applicable terms agreed to in writing. No use of any Renesas resources expands or otherwise alters any applicable warranties or warranty disclaimers for these products.

(Rev.1.0 Mar 2020)

Corporate Headquarters

TOYOSU FORESIA, 3-2-24 Toyosu, Koto-ku, Tokyo 135-0061, Japan
https://www.renesas.com

Contact Information

For further information on a product, technology, the most up-to-date version of a document, or your nearest sales office, please visit:
https://www.renesas.com/contact-us

Trademarks

Renesas and the Renesas logo are trademarks of Renesas Electronics Corporation. All trademarks and registered trademarks are the property of their respective owners.

© 2022 Renesas Electronics Corporation. All rights reserved.