最新の自動車盗難方法を防ぐ技術
-リレーアタックから自動車を守るには-

車載システムセキュリティ部、車載コアテクノロジー開発統括部、オートモーティブソリューション事業本部
ルネサス エレクトロニクス株式会社

森山　大輔

背景

自動車の盗難はドライバーにとって非常に重要なことである。EU 圏内では 2020 年に 447,700 件の盗難があったと報告されている [1]。また、アメリカの FBI は 2020 年に USA 全体で起こった自動車盗難事件は 810,400 であり、2019 年に比べて 11.8%上昇したと発表している [2][3]。全米保険犯罪局 NICB は 2018 年にオーナーの手に戻ることができた盗難車は約 60%であったことを報じている [3]。盗難車は犯罪の追跡を逃れるために部品に解体され、国外に輸出されているといったことが時々起きている。昔は自動車ドアのロック・ロック解除は物理的な鍵を用いており、オプションとして別の方法を提供するといった形式であった。しかし、近年の自動車では多くの会社がリモートキーレスエントリーシステムやパッシブキーレスエントリーシステム(PKES: passive keyless entry with start)を導入している。これらの方式は現代では自動車にアクセスする一般的な方法となっている。パッシブキーレスエントリーでは所有者が自動車に物理的にアクセスする必要がなく、所有している車と PKES キーフォブの距離が一定以内 (1-2 メートル)になると自動的にエンジン動作などの仕組みが働く。この手法によって所有者にとっては利便性が向上した一方で、ワイヤレス通信起因の攻撃が犯罪に利用されるようになっていった。

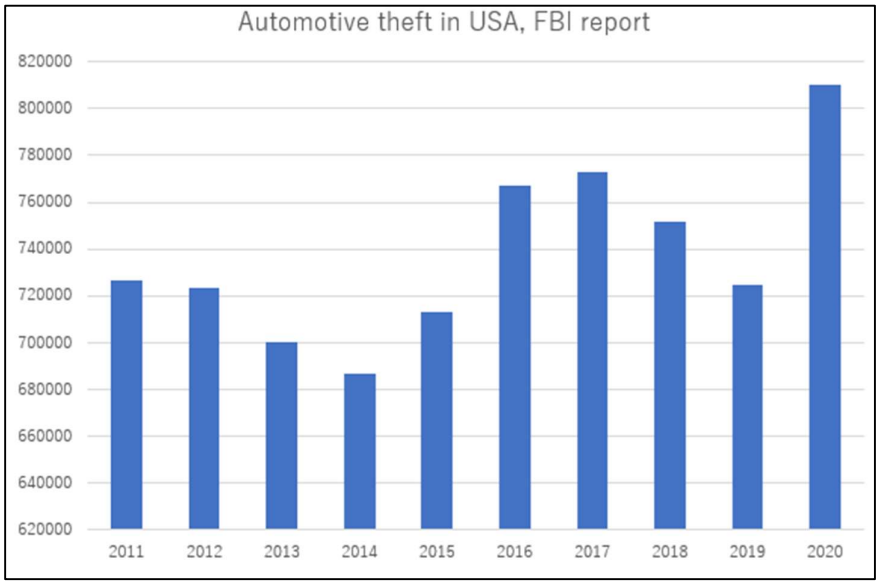

図 1. USA における自動車盗難件数 [2][3]

PKES キーフォブの安全性

PKES キーフォブ自身には一定の組み込まれた認証メカニズムが備わっている。1 つの PKES キーフォブは対応する 1 つの車しかドアを開けることはなく、他の車はロックされたままである。つまりある特定の無線周波数を用いた双方向のやり取りがキーフォブと対象の車とで行われている。キーフォブには小さなマイクロコントローラが格納されており、自動車側から受け取った要求に対して一定のアルゴリズムにより算出した結果を返送する。

正当性を確かめる非常に簡単な方法は、自動車とキーフォブ間でユニークな値を共有しておくことである。もし所有者がパーキングに近づくなどして、キーフォブが自動車から起動のためのメッセージを受け取ると、そのユニークな値を返答し、対象の車は受け取った値が自動車内に保持されている値と一致しているときに限りドアをアンロックすればよい。ユニークな値を複数用意しておき、いずれかを使う・順に使うなどのアイデアなどもあり得るであろう。しかしながら、このような簡単な方式は現実世界では脆弱で安全性が低いものとされる。正規のキーフォブから送られたメッセージを何らかの形で記録されてしまうと、後日キーフォブの代わりにそのメッセージを再送することで、自動車はドアをアンロックしてしまう。OEM の中には再送攻撃を防ぐため、2000 年前後にローリングコードという方式を導入しているものもある。ローリングコードでは過去のコードを無効化し、送信者と受信者の双方が次の正しい通信のための値を計算する仕組みを持っている。

自動車セキュリティは 10 年前には重要なトピックとは捉えられていなかったため、いくつかの自動車は PKES キーフォブとの通信にこのような基本的な検証方法しか載せていなかった。そのため、転送されたメッセージが再送された場合、これらの車はドアを開けてしまう。ローリングコードであってもリプレイ攻撃に対しての脆弱性が指摘されており、多くの自動車 OEM にかつて用いられていた KEELOQ® (*1)はリプレイ攻撃や暗号解析に対して安全ではないことが研究者によって指摘されている [5][6][7]。実際、『コードグラバー』と呼ばれるデバイスが存在し、キーフォブが正規の通信を行うために信号を発信している間に転送データを記憶する装置がある。この機器はその後、いつでも正規キーフォブの代わりに記録していたメッセージを転送することでドアのロックを解除することができる。どのように窃盗犯が自動車を盗み出したかを確かめることは非常に難しいが、コードグラバーを用いた自動車盗難は現実的に起こりうるもので、多くのウェブサイトではコードグラバーに対してケアするように注意喚起を現在も促している。この攻撃は技術的な側面からすると、キーフォブからの返答が通信前に確定しておらず、返答される値の候補が指数的に大きい（例えばランダムに選んだ 128-bit 値に見えるなど）のであれば最小限の被害に食い止めることができる。そのため、このようなリプレイ攻撃に対しては共通鍵暗号を用いた典型的なチャレンジレスポンス認証によって対策をとることが可能である。もし暗号学的なアルゴリズムが用いられており、秘密鍵管理が正しく行われているのであれば、出力されたデータからの機密情報漏洩は起こらない。また、キーフォブと自動車の間の認証プロトコルが十分に安全であることが示されているものを採用している限りにおいては、攻撃者によって挿入された偽造メッセージが受理されることはなく、非正規の人物によって自動車のドアが開けられることはない。

(*1) KEELOQ は Microchip Technology Inc. の登録商標です。

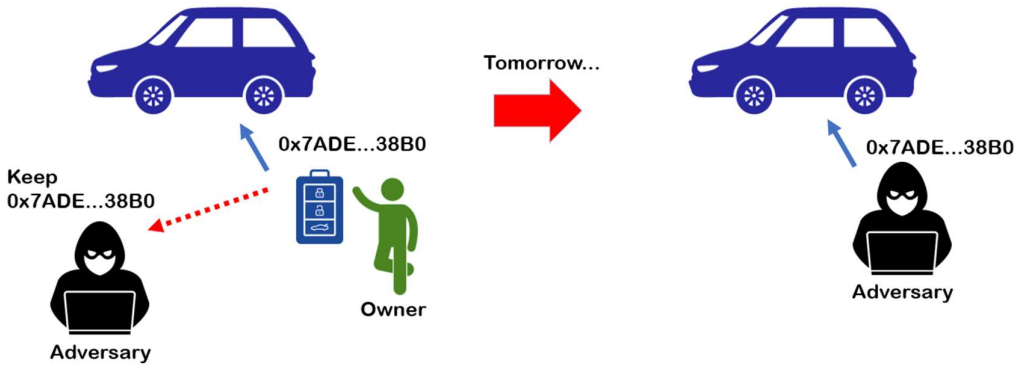

図 2. コードグラバーを利用した盗難

リレーアタックとは？

PKES システムが広く導入されるにつれて自動車盗難の方向性は大きく変わっており、近年ではリレーアタックによる自動車盗難が問題視されるようになってきた。リプレイ攻撃を防ぐ目的でキーフォブ端末に安全なチャレンジレスポンス認証が実装されている場合であっても、リレーアタックは通信におけるデータを変更しないためこのようなセキュリティ機構の影響を受けないためである。

リレーアタックは 2 人の共謀した攻撃者によって実行される。片方の攻撃者は対象の自動車に近い位置におり、もう片方の攻撃者はキーフォブの近くにいるようにする（対象となるキーフォブが家の中の棚に置かれている、あるいは本来の所有者のポケットに入っている等）。2 人が特殊な装置をそれぞれ起動すると、この装置は自動車とキーフォブの通信を中継する形でデータを転送する。元々のキーフォブから出される信号の伝達可能距離が高々2 から 5 メートル程度であったとしても、特殊な装置同士が本来のワイヤレス通信に変わって通信を行うために、中継デバイスの性能や外部環境によって左右されるものの、通信距離が飛躍的に（例えば 300m 程度まで）伸ばされる。

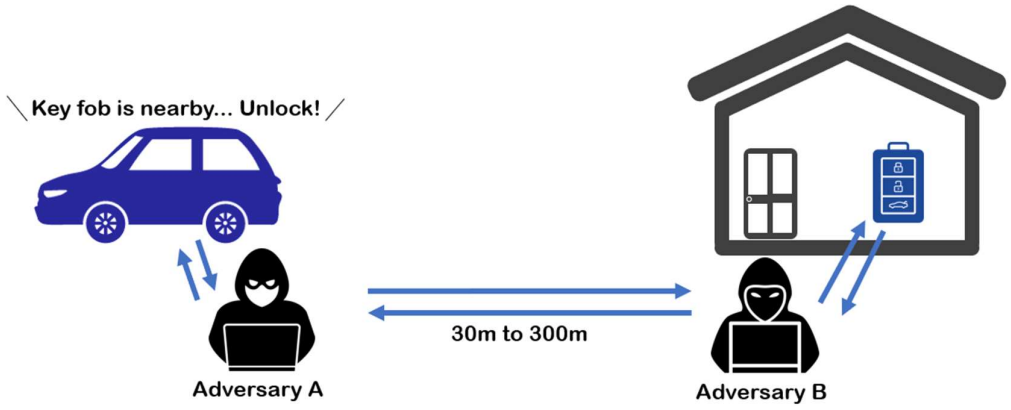

図 3. リレーアタックを利用した盗難

実際に、アメリカではリレーアタックによって窃盗犯が高級な自動車を盗む様子を監視カメラが捉えた映像が公開されている [8]。日本では 2019 年に自動車の窃盗犯を捕まえた際、同時に警察によってリレーアタックに用いた端末が押収されたとの報道があった [9]。また、実際の自動車盗難とは独立に、研究分野においても本ホ

ワイトペーパー執筆時点においてリレーアタックは注目を集めており、多くの研究者が特定の車種の自動車がリレーアタックに対して安全であるか脆弱であるかの調査結果を発表している [10]。それでは、現在のリレーアタック問題に対してどのように立ち向かうべきであろうか？

既存の PKES キーフォブは一般的に、Low Frequency (LF)あるいは Ultra High Frequency (UHF)が用いられていることが多い。近年は一部の自動車会社から、最新車種の一部においてユーザのスマートフォンをキーフォブとして利用することができるようになるサービスを提供していることがある。この場合、Bluetooth Low Energy (BLE)が自動車との通信の役割を担うことで、自動車のロック・アンロックのための認証が実行される。さらに BLE は通信距離を制限するための測距認証機能もサポートされている。しかしながら、2022 年にサイバーセキュリティ研究グループによると、既存の BLE による測距認証はリレーアタックを防ぐには不十分であることを報告している。そのため、リレーアタックを防ぐためには別の技術的なアプローチが必要になる。

Ultra Wide Band (UWB)による距離測定

リレーアタックを用いた自動車盗難が多くのウェブサイトに掲載され認知され、多くの開発者はこの問題を解決するためにどのワイヤレス通信を採用するべきかを再考した。その中でも、Ultra Wide Band (UWB) 技術に着目が集まっている。UWB は多くの距離測定の方法を提供しており、正確性は 10cm 以下になるものも可能である。特に UWB は Round Trip Time (RTT) による測距方法をサポートしているため、本ホワイトペーパーでも基本概念を説明する。RTT は以下の計算を行うことで導かれるものである。

検証者は高精度のタイマーを持っており、証明者にメッセージを送った時刻 t_s にカウントを開始するとしよう。証明者はメッセージ（ワイヤレス信号）を受け取ると、特定のプログラムを実行して返答する値を計算する。証明者が検証者に対して返答を送るまでに必要とする計算時間全体を t_p とする。検証者が証明者から返答を受け取ると、検証者はカウンタを止める。この時刻が t_e であったとしよう。この状況では、この 1 回の双方向の通信全体にかかった時間は $t_e - t_s$ である。この時間のうち、ワイヤレス信号の通信のみに使われた時間は $(t_e - t_s) - t_p$ である。この時間を 1/2 したものは Time of Flight (ToF) と呼ばれる。ToF は 2 者の単方向における通信時間を示すものである。ワイヤレス通信には周波数によって一意に定まる伝達速度 ps があることを想定すると、検証者と証明者の距離 $dist$ は結果的に $dist = ps \times ((t_e - t_s) - t_p)/2$ として求めることができる。

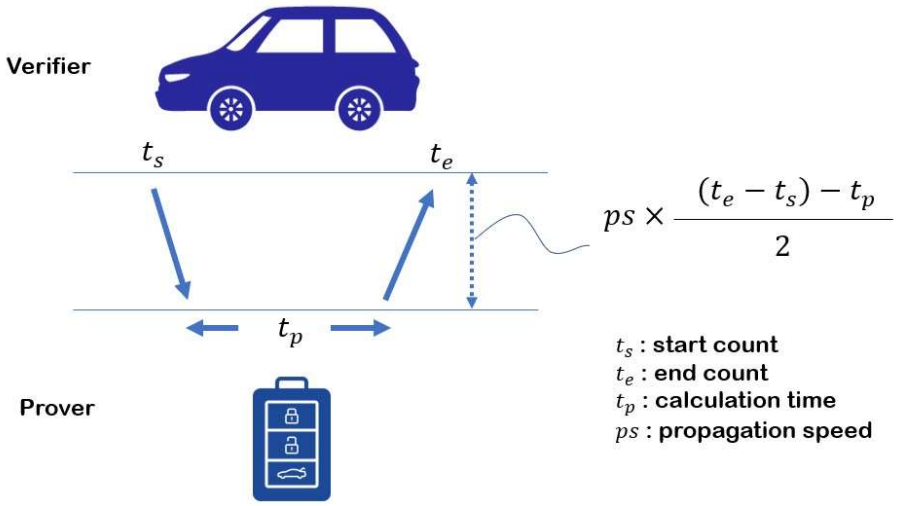

図 4. 通信時間を用いた距離測定

もし証明者によって利用される時間 t_p が事前に決められることができる場合、この測定による距離推定に対して現実においてばらつきを生じさせるのは物理現象のみである。キーフォブのようにサポートする最大距離を決めているのであれば（品質保障の観点もかねて）、認証の観点で受理するか拒否するかを判定する基準時間 t_{max} を定めることができる。もし通信を実行した際に想定された時間を超え $(t_e - t_s) - t_p > t_{max}$ となっていた場合、この通信はリレーされた疑いがあることが分かる。実際の製品においては、Proof of Concept による観測や統計解析により信頼された定数として基準時間 t_{max} を求めることが望ましい。

RTT をベースとした測距方法は非常に精密な距離測定を可能にするものの、この方式が単独で安全性を保障するものではない。IEEE 802.15.4a において 2007 年に標準化されたオリジナルの UWB において RTT を用いた測距が定義されていたものの、いくつかの研究結果により当時の方法は不十分でありセキュリティ上の改良が必要であることが指摘されていた [11]。そのため、結果的に UWB は IEEE 802.15.4z としてセキュリティを向上させるための改訂が 2020 年に行われた。

IEEE 802.15.4z にて標準化されている UWB は、物理的なデータ転送方法として Low Rate Pulse (LRP)と High Rate Pulse (HRP)の 2 種類を定義している。LRP では高い電力を用いて信号の間隔が広い 1-bit パルスが伝送される。受信する側は個別の信号を簡単に検知することができる。LRP は上位レイヤーのプロトコルにおいて 1-bit ないし数ビット程度の小さいデータが頻繁にやり取りされる状況に適している。LRP においては、RTT を利用したある限定された時間内に行うチャレンジレスポンス認証の一種である暗号学的な distance bounding protocol をサポートしている。

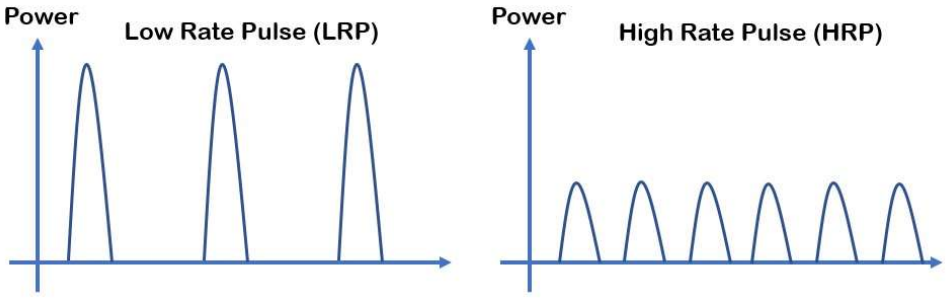

図 5. UWB に定義されている LRP と HRP の違い

HRP の場合は、連続したデータが少ない電力で短い間隔で伝送される。HRP のデータ転送効率は LRP に比べて高いが、転送される信号はフェンスや垣根、建物などの物理的な障害によって遅延や重なり合いが生じることを考慮に入れる必要がある。受信する側は適切なピークとなる波形や信号の順番を見つけ、受信した信号のパルスや特性などをチェックすることで元のメッセージを復元する必要がある。

IEEE 802.15.4z の UWB HRP 定義されている測距手法は Scrambled Timestamp Sequence (STS)と呼ばれている値を生成・検証することで行われている。この値は共通鍵暗号アルゴリズム AES に事前共有している秘密鍵と 32-bit のカウンタを入力として用いることで導かれる。そのため、STS に関わる伝送メッセージは第三者に対して予測できないものとなる。Car Connectivity Consortium は Digital Key 3.0 仕様として UWB HRP を主に距離測定に用いるものとしており、AES によって生成された合計 4,096-bit (4,096 個のパルス)の STS が距離測定のために転送されるとしている。検証者（自動車）は受け取った STS が期待している値と一致しているかを確かめることで、証明者（キーフォブ）が一定の距離範囲内であるかを判定する。結果的に、UWB HRP は UWB 以外のワイヤレス通信に対して行われている一般的なリレーアタックを防ぐことができるようになっている。

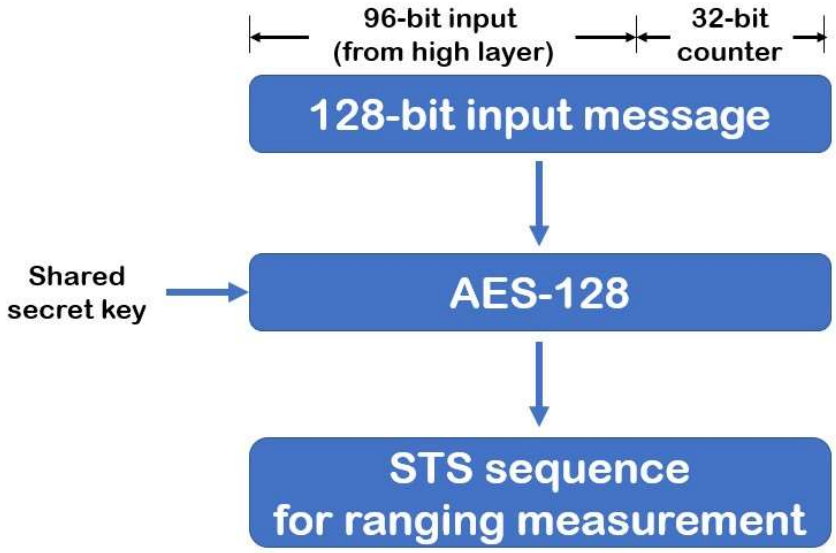

図 6. UWB HRP の距離測定に使われる STS 生成

まとめ

リレーアタックによる自動車盗難は 2020 年前後における非常に重要な課題である。このホワイトペーパーでは、PKES キーフォブのセキュリティに関係する歴史的な動向について説明した。リレーアタックは自動車オーナーにとっての新しい脅威であるが、前章で解説したように UWB に搭載されている STS の手法は、リレーアタックによる問題は最小化することができる解決法として適切なソリューションとして考えられている。Digital Key 3.0 が UWB 技術を測距方法として採用しており、その中で用いられている STS がリレーアタックに対してのセキュリティ対策として近い将来広く用いられることが期待される。

[参考資料]

[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

[10] https://research.nccgroup.com/2022/05/15/technical-advisory-ble-proximity-authentication-vulnerable-to-relay-attacks/

[11] https://ieeexplore.ieee.org/document/5714149

(Rev.1.0 Oct 2022)

本社所在地

〒 135-0061 東京都江東区豊洲 3-2-24（豊洲フォレシア）

https://www.renesas.com

お問合せ窓口

弊社の製品や技術、ドキュメントの最新情報、最寄りの営業お問合せ窓口に関する情報などは、弊社ウェブサイトをご覧ください。

http://www.renesas.com/contact/