RollBack

A New Time-Agnostic Replay Attack Against the Automotive Remote Keyless Entry Systems

Levente Csikor
NCS Group
Institute for Infocomm Research, A*STAR

Hoon Wei Lim
NCS Group

Joint work with **Jun Wen Wong** (NCS Group / DSBJ), **Soundarya Ramesh** (NUS), **Rohini Poolat Parameswarath** (NUS), **Mun Choon Chan** (NUS)

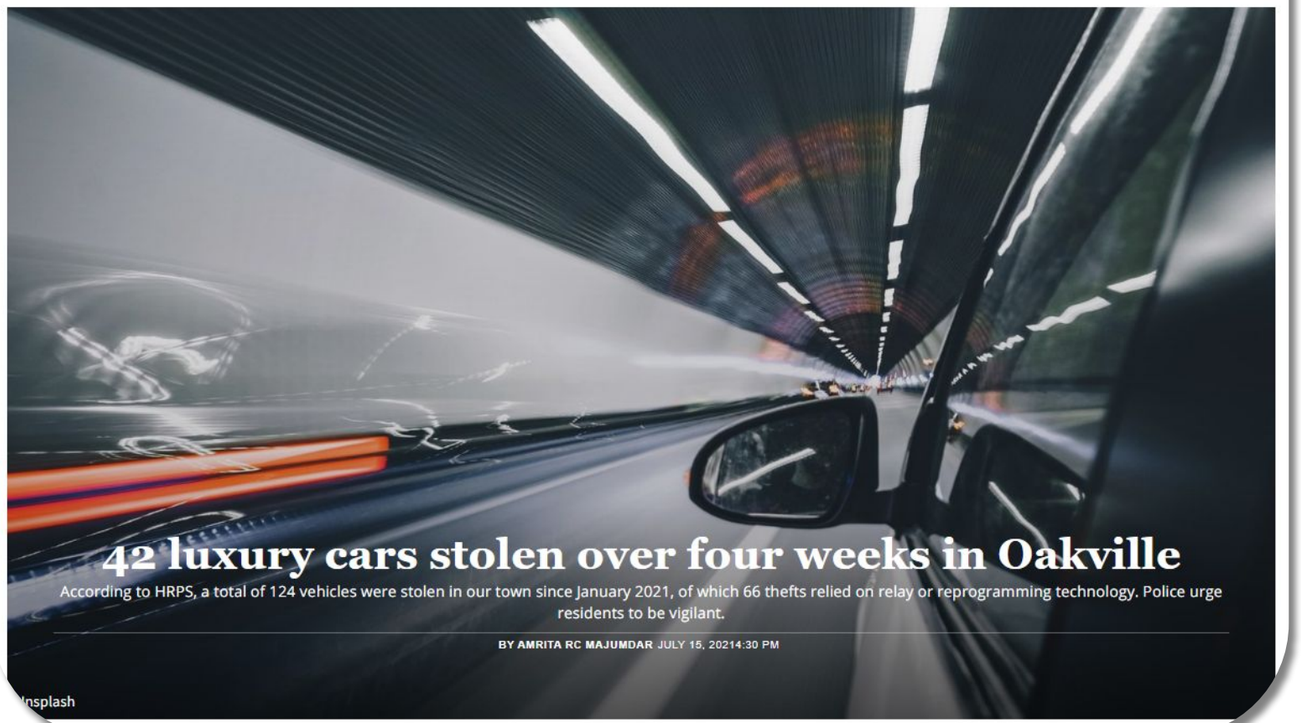
Keyless car thefts have been on the rise

Oakville News

Search...

NEWS | CULTURE & LIFESTYLE | BUSINESS | COMMUNITY | REVIEWS | OPINION | HEALTH | SPORTS

HOME / NEWS /



42 luxury cars stolen over four weeks in Oakville

According to HRPS, a total of 124 vehicles were stolen in our town since January 2021, of which 66 thefts relied on relay or reprogramming technology. Police urge residents to be vigilant.

BY AMRITA RC MAJUMDAR JULY 15, 20214:30 PM

Unsplash

News ▸ Northern Ireland ▸ Co Tyrone

Police warning after sixth keyless car theft in Mid Ulster this year

Detectives are investigating the theft of a blue Hyundai Tucson in Donaghmore

SHARE COMMENTS

By Conor Coyle Fermanagh and Tyrone reporter
10:34, 28 APR 2022

NEWS

Enter your **postcode** for **local news** and **info**

Enter your postcode Go

In YourArea

Keyless car thefts have been on the rise

- **Keyless entry car technology now accounts for nearly 50% of all vehicle thefts**
  UK Daily Mail, Jul 2021
- **The risk of technology-enabled vehicle theft will continue to increase**
  Auto-ISAC Threat Assessment Report 2021
- **Keyless entry/key fob is one of top two most common attack vectors**
  Upstream Global Automotive Cybersecurity Report 2022

Mail Online

Threats against remote keyless entry systems

- **Manipulation of key fob signals**
  - Signal jamming
  - Relay (amplification) attacks
  - **Replay attacks**
- **Attack on key management and cryptographic algorithms**
  - Key enrolment
  - Key replacement
  - Key extraction

Recent car hacks based on replay of signals

BLEEPINGCOMPUTER

Search Site

NEWS | DOWNLOADS | VIRUS REMOVAL GUIDES | TUTORIALS | DEALS

Home › News › Security › Honda bug lets a hacker unlock and start your car via replay attack

Honda bug lets a hacker unlock and start your car via replay attack

By Ax Sharma — March 25, 2022 — 03:28 AM — 3

SECURITYWEEK

CYBERSECURITY NEWS, INSIGHTS & ANALYSIS

Cloud Security | Identity & Access | Data Protection | Network Security | Application Security

Home › Vulnerabilities

Honda Admits Hackers Could Unlock Car Doors, Start Engines

By Ionut Arghire on July 13, 2022

Share | Tweet | Recommend 0 | RSS

"Rolling-PWN attack" targets Remote Keyless System on Honda vehicles

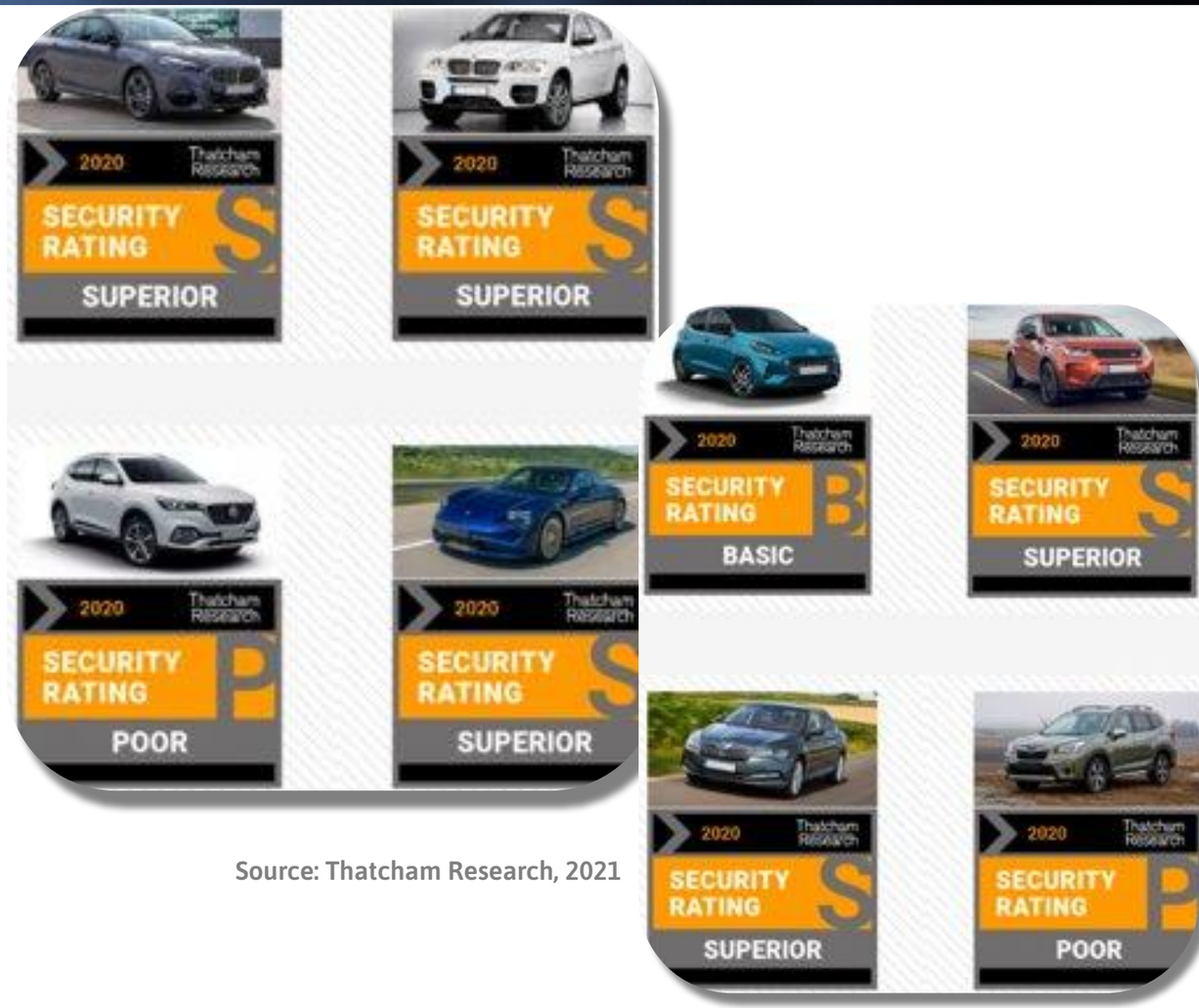
Honda has confirmed that researchers were indeed able to hack the remote keyless entry system of certain Honda vehicles to unlock the doors and start the engine.

Over the weekend, security researchers Kevin2600 and Wesley Li from Star-V Lab published information on a security bug they identified in the rolling codes mechanism of the remote keyless system of Honda vehicles, which allowed them to open car doors without the key fob present.

Our new findings in a nutshell

New replay attack - RollBack

- Revealed **highly unusual behavior** – more effective than previously known key fob replay attacks
- **Initial discovery in Aug 2021**: unlocked a car by replaying two consecutive signals within 5 seconds
- **Derived new generic attack metrics in Mar 2022** that work across different car makes & models: **no. of signals, sequence, interval, instructions in the signal**
- **Appear consistent with security assessments** by Thatcham Research – Consumer Security Ratings 2021



Source: Thatcham Research, 2021

Responsible disclosure

- Notified key fob chip manufacturers in Apr 2022
- Shared findings with Auto-ISAC in May 2022

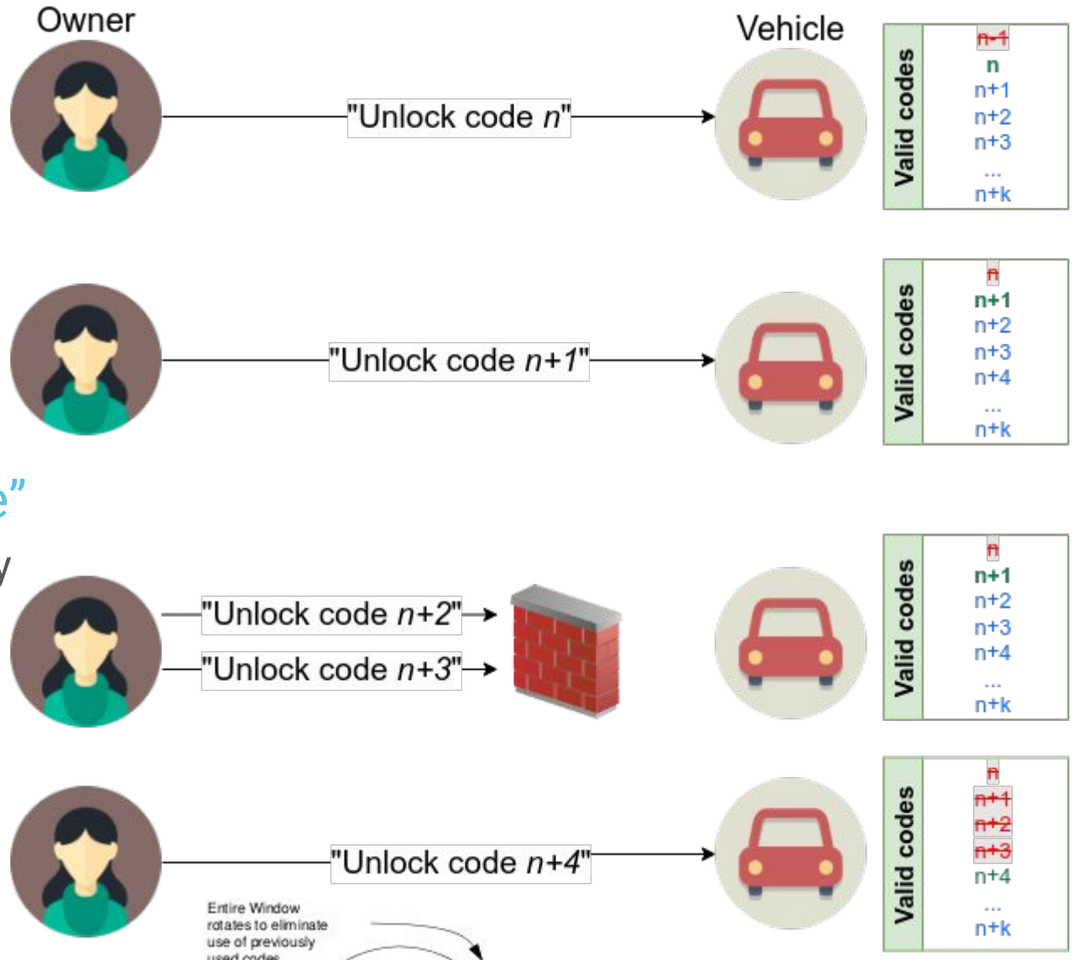
background

Rolling codes

Brief overview of the operation

Rolling codes in a nutshell

- **Every key fob signal transmission is unique**
  - "There are NO two unlock signals that are the same"
    - Every time a button is pressed and a signal is received by the vehicle, both increase a counter for the next use
    - If counters are in sync upon reception → vehicle acts as instructed/expected



- Note: provision is made if key fob's counter is "in the future"
  - Buttons accidentally pressed but far outside of the vehicle's vicinity

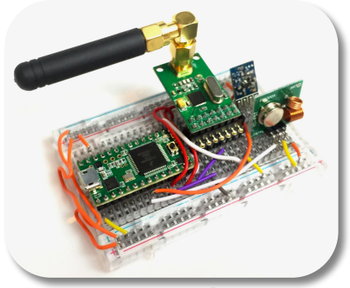
  - Upon successful reception, counters become re-synchronized again

[1] Microchip, "KeeLoq™ Code Hopping Encoder," Microchip HCS200, https://bit.ly/3GqCl5c, 2011 [Accessed: Jul 2022].

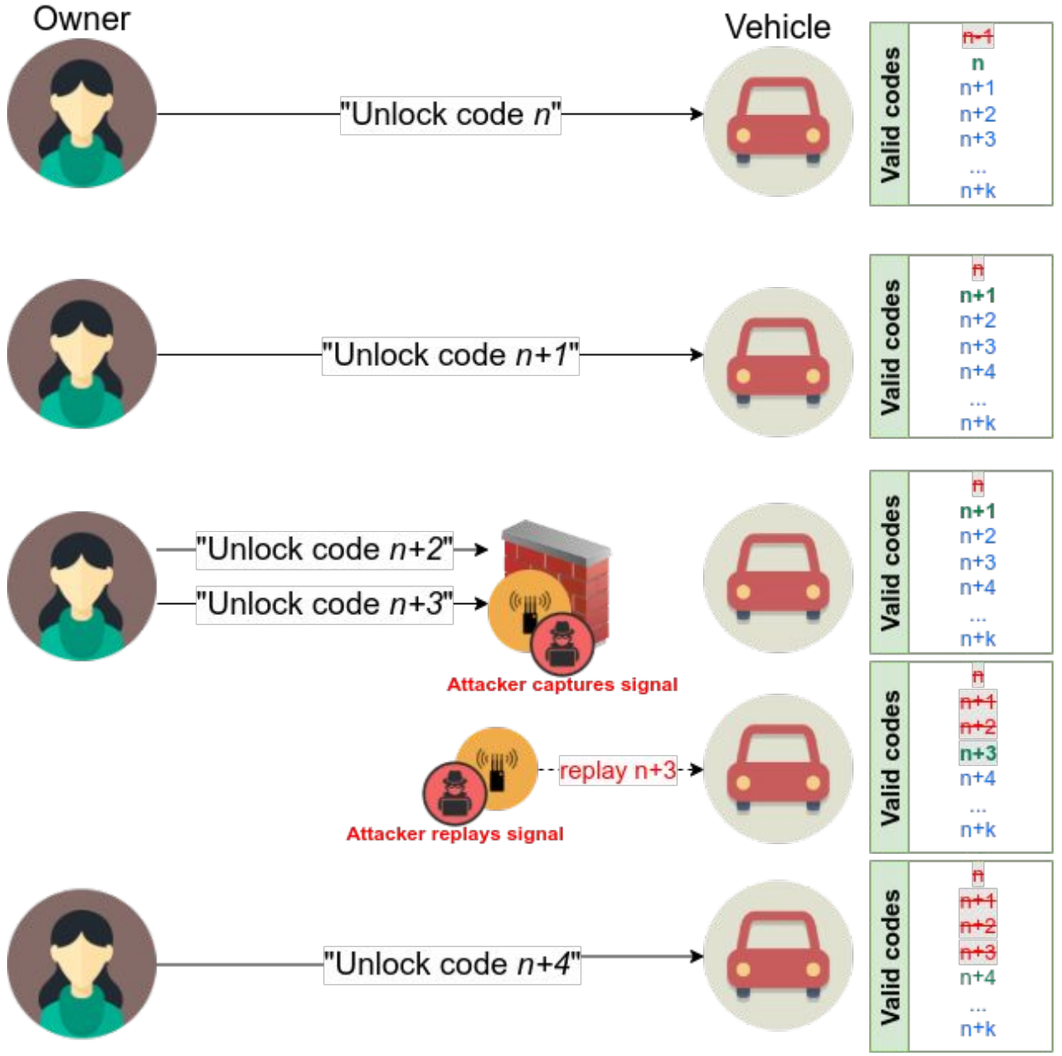
Rolling codes - Straightforward “exploit”

- **If an attacker can capture the signals of the accidental button presses outside of the vicinity of the vehicle**
  - We have the “future codes” → Straightforward “exploit”
- **BUT: Obtaining valid “future code” in reality is extremely difficult**

- **RollJam attack**
  - Signal Jamming + Capturing + Replaying
  - Lure the owner into a situation where “future codes” can be obtained easily



- **RollJam is/was not a “new hack”**
  - it converts the safety provisioning feature into an exploit



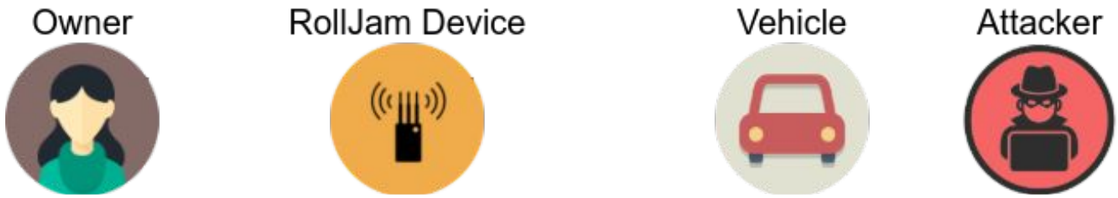
related work

RollJam

Infamous attack against all rolling code-based systems

RollJam in a nutshell

- **Good-guy hacker, Samy Kamkar, proposed it in 2015**
- **Special-purpose small device (< 30 USD)**
  - Close to the vehicle (suffixed at a hidden spot)
  - It can
    - Capture
    - Jam
    - Replay signals
  - Acts as Man-in-the-Middle proxy between the key fob and the vehicle

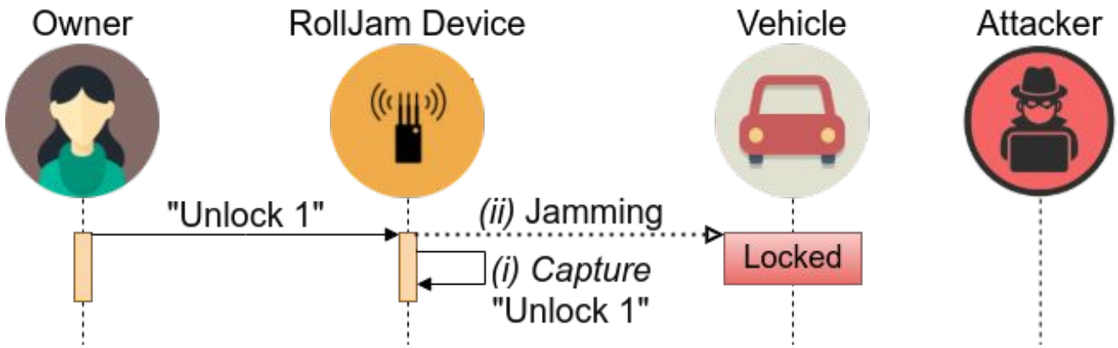


RollJam in the news: https://www.wired.com/2015/08/hackers-tiny-device-unlocks-cars-opens-garages/

RollJam in a nutshell

- **Good-guy hacker, Samy Kamkar, proposed it in 2015**
- **Special-purpose small device (< 30 USD)**
  - Close to the vehicle (suffixed at a hidden spot)
  - It can
    - Capture
    - Jam
    - Replay signals
  - Acts as Man-in-the-Middle proxy between the key fob and the vehicle

- **First “unlock” signal sent**
  - Captured and jammed to hinder the car to receive it

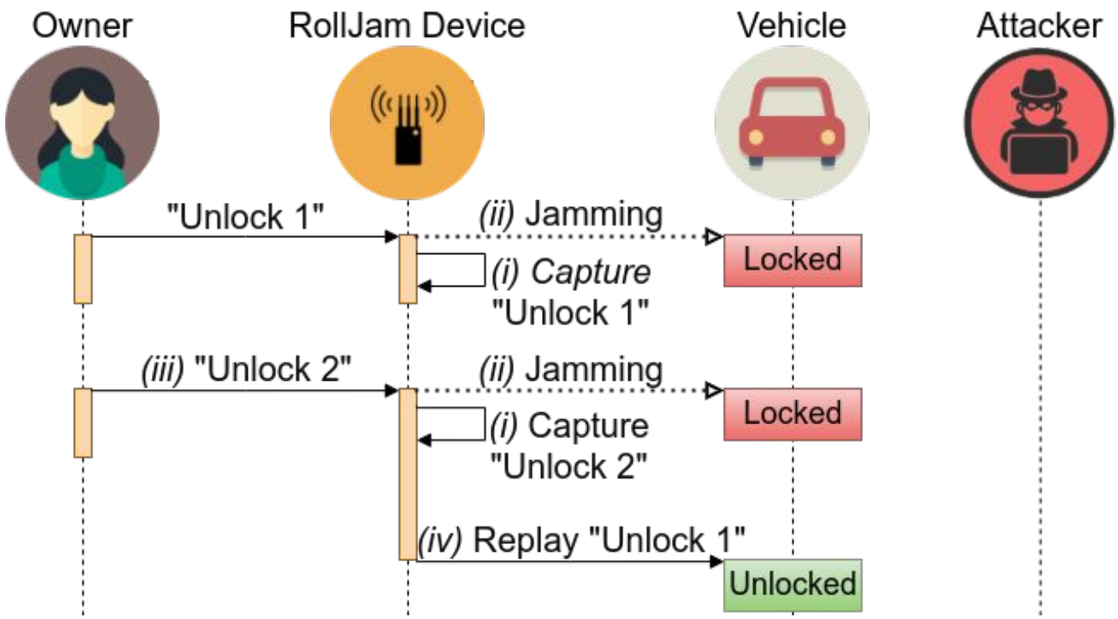


RollJam in the news: https://www.wired.com/2015/08/hackers-tiny-device-unlocks-cars-opens-garages/

RollJam in a nutshell

- Good-guy hacker, Samy Kamkar, proposed it in 2015
- Special-purpose small device (< 30 USD)
  - Close to the vehicle (suffixed at a hidden spot)
  - It can
    - Capture
    - Jam
    - Replay signals
  - Acts as Man-in-the-Middle proxy between the key fob and the vehicle

- First “unlock” signal sent
  - Captured and jammed to hinder the car to receive it
- Second “unlock” signal sent (as a retry)
  - Captured and jammed + first signal replayed
- Vehicle acts as intended

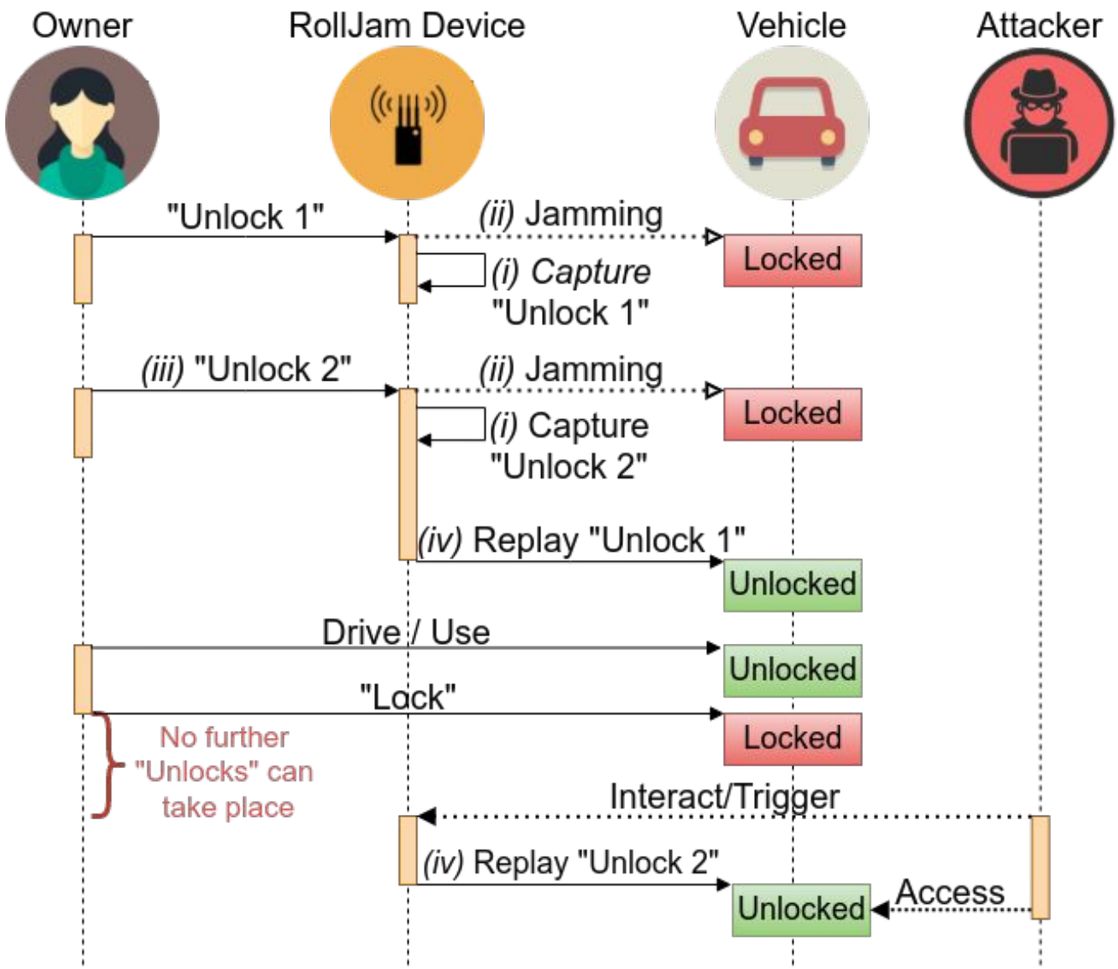


RollJam in the news: https://www.wired.com/2015/08/hackers-tiny-device-unlocks-cars-opens-garages/

RollJam in a nutshell

- Good-guy hacker, Samy Kamkar, proposed it in 2015
- Special-purpose small device (< 30 USD)
  - Close to the vehicle (suffixed at a hidden spot)
  - It can
    - Capture
    - Jam
    - Replay signals
  - Acts as Man-in-the-Middle proxy between the key fob and the vehicle

- First “unlock” signal sent
  - Captured and jammed to hinder the car to receive it
- Second “unlock” signal sent (as a retry)
  - Captured and jammed + first signal replayed
- Vehicle acts as intended
- Attacker has the next valid yet unused “unlock” signal



*Assuming that lock and unlock signals do not use the same counter

RollJam in the news: https://www.wired.com/2015/08/hackers-tiny-device-unlocks-cars-opens-garages/

this is what you came for

RollBack

Time-Agnostic Re-Synchronization Attacks

CVE-2022-36945
CVE-2022-37305
CVE-2022-37418

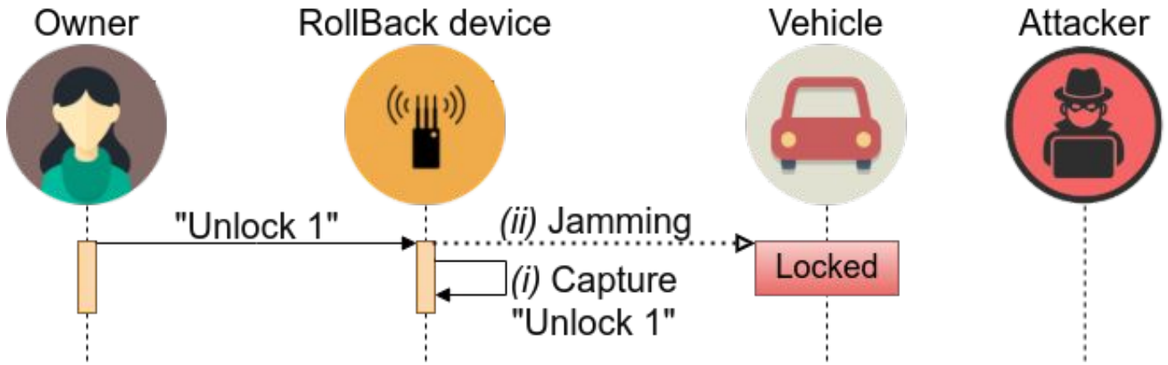
RollBack - two captured signals

- **Setup is similar to RollJam**
  - Capture + Jam* + Replay
- **HOWEVER: RollBack is different**

*RollBack does not necessitate jamming but it can ease/fasten the signal capturing process

RollBack - two captured signals

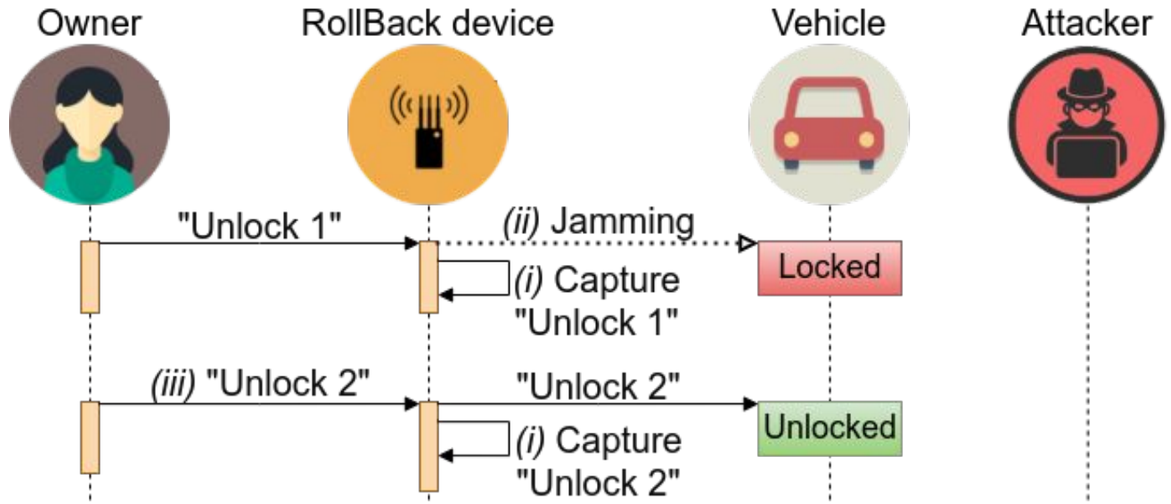
- **Setup is similar to RollJam**
  - Capture + Jam* + Replay
- **HOWEVER: RollBack is different**
- **First “unlock” signal sent**
  - Captured and jammed to hinder the car to receive it



*RollBack does not necessitate jamming but it can ease/fasten the signal capturing process

RollBack - two captured signals

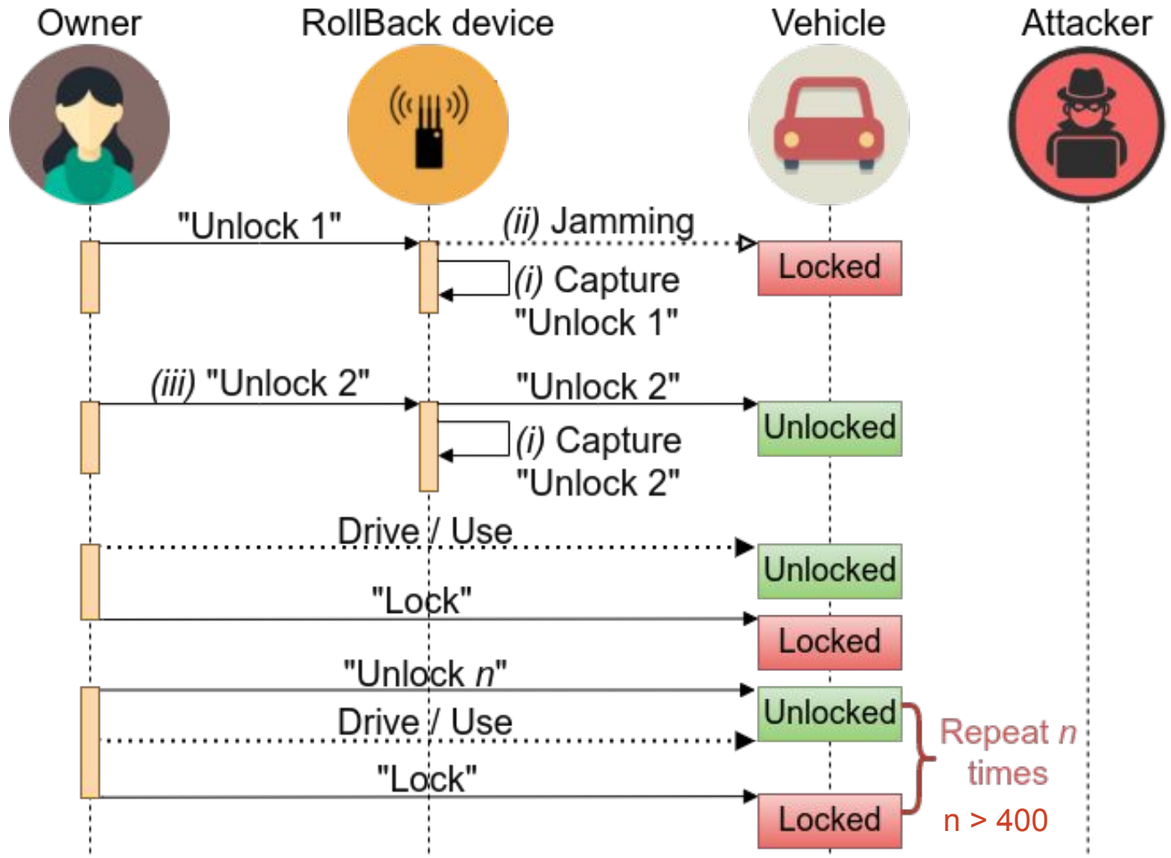
- Setup is similar to RollJam
  - Capture + Jam* + Replay
- HOWEVER: RollBack is different
- First “unlock” signal sent
  - Captured and jammed to hinder the car to receive it
- Second “unlock” signal sent (as a retry)
  - Captured only and let the vehicle receive it
- Vehicle acts as intended



*RollBack does not necessitate jamming but it can ease/fasten the signal capturing process

RollBack - two captured signals

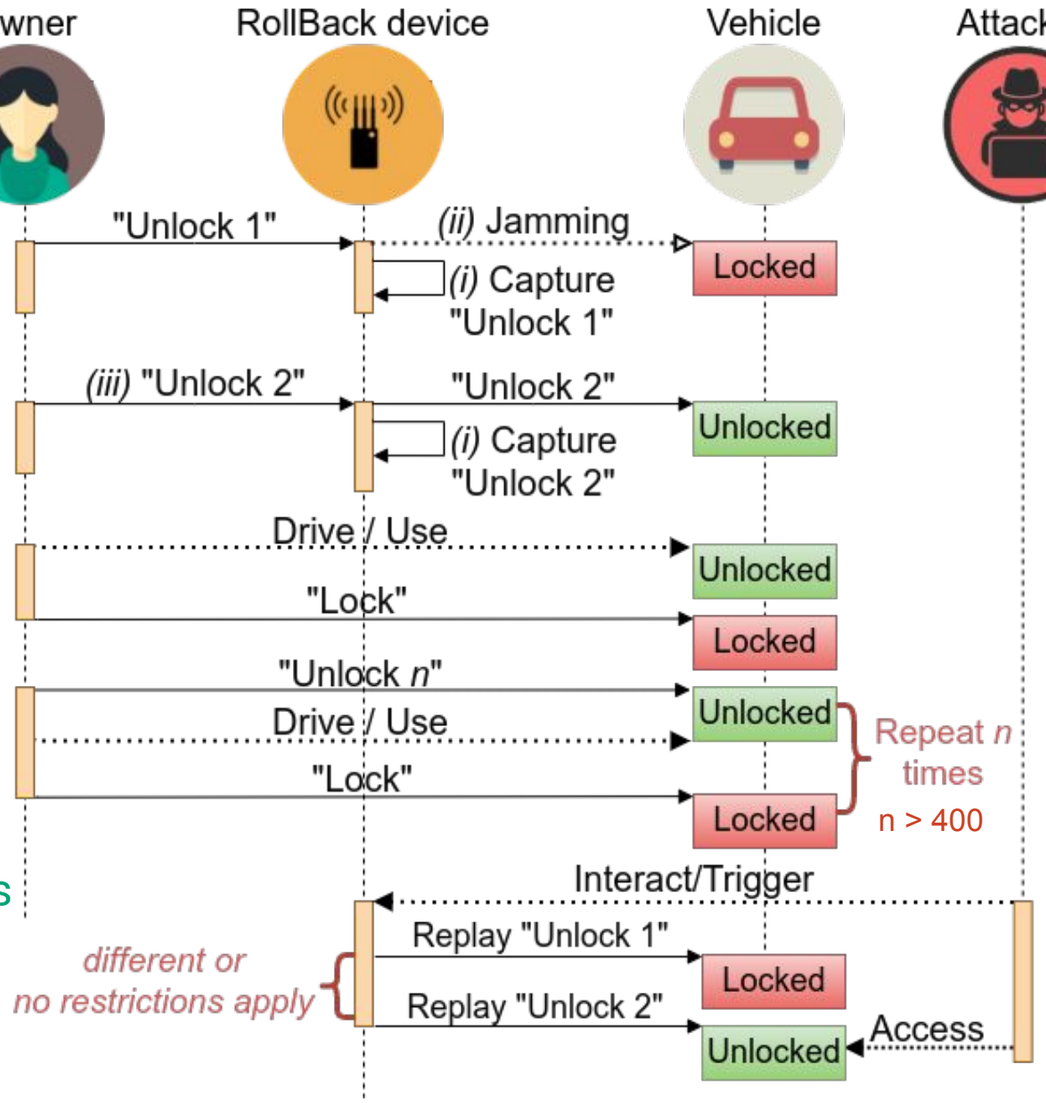
- **Setup is similar to RollJam**
  - Capture + Jam* + Replay
- **HOWEVER: RollBack is different**
- **First “unlock” signal sent**
  - Captured and jammed to hinder the car to receive it
- **Second “unlock” signal sent (as a retry)**
  - Captured only and let the vehicle receive it
- **Vehicle acts as intended**
- **Owner uses the vehicle/key fob as usual**
  - as many times s/he wants



*RollBack does not necessitate jamming but it can ease/fasten the signal capturing process

RollBack - two captured signals

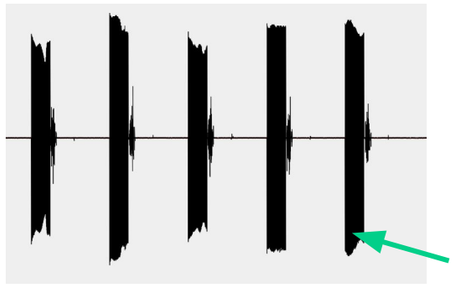
- **Setup is similar to RollJam**
  - Capture + Jam* + Replay
- **HOWEVER: RollBack is different**
- **First “unlock” signal sent**
  - Captured and jammed to hinder the car to receive it
- **Second “unlock” signal sent (as a retry)**
  - Captured only and let the vehicle receive it
- **Vehicle acts as intended**
- **Owner uses the vehicle/key fob as usual**
  - as many times s/he wants
- **Attacker can replay the two consecutive “unlock” signals**
  - note: some system has more restrictions on the replayed signals (see later)



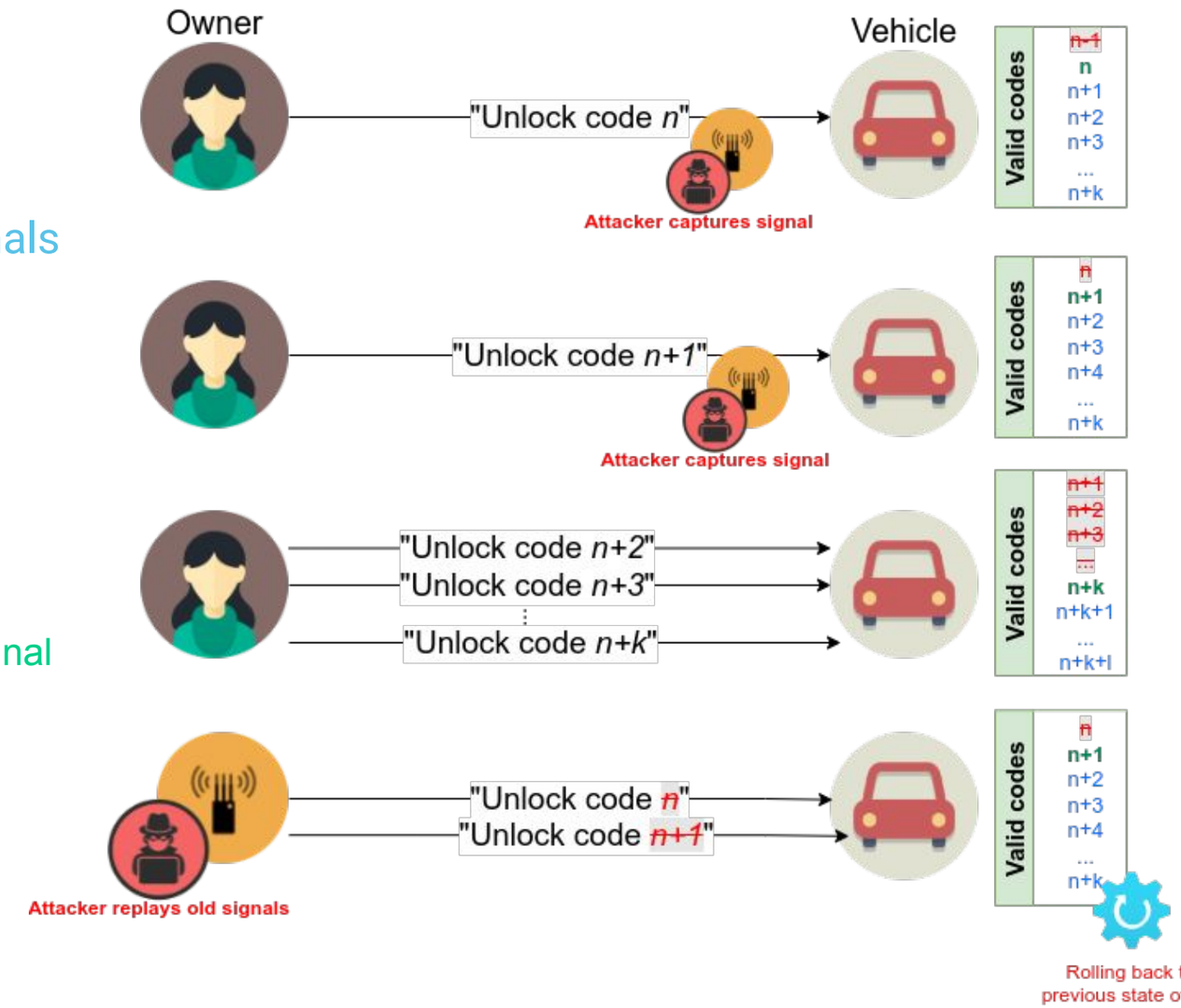
*RollBack does not necessitate jamming but it can ease/fasten the signal capturing process

Why RollBack? Advantages?

- **Rolling back to a previous code/state**
  - The captured consecutive signals are replayed
  - The vehicle re-synchronize to a previous code
    - To the old counters in the last replayed signal
  - Vehicle acts according to the instruction in the signals
    - i.e., unlocks

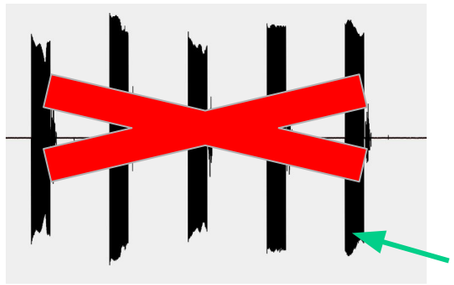


1. last unlock signal received

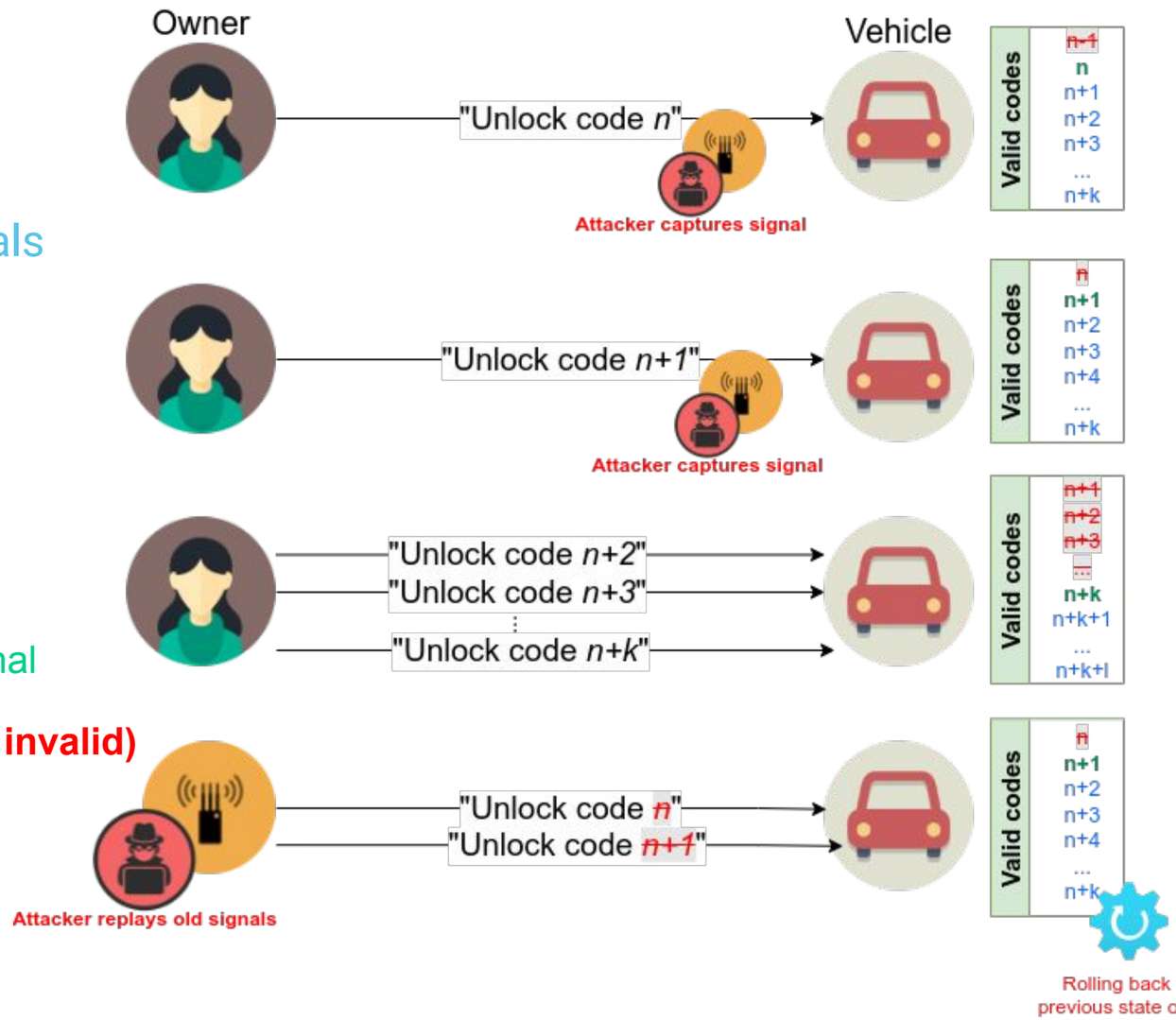


Why RollBack? Advantages?

- **Rolling back to a previous code/state**
  - The captured consecutive signals are replayed
  - The vehicle re-synchronize to a previous code
    - To the old counters in the last replayed signals
  - Vehicle acts according to the instruction in the signals
    - i.e., unlocks

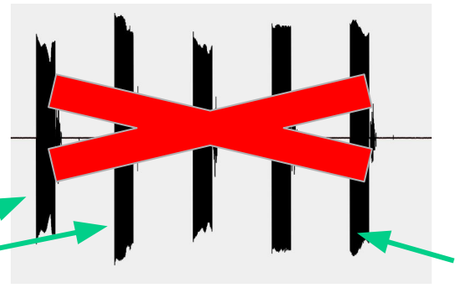


1. last unlock signal received
(all signals are invalid)



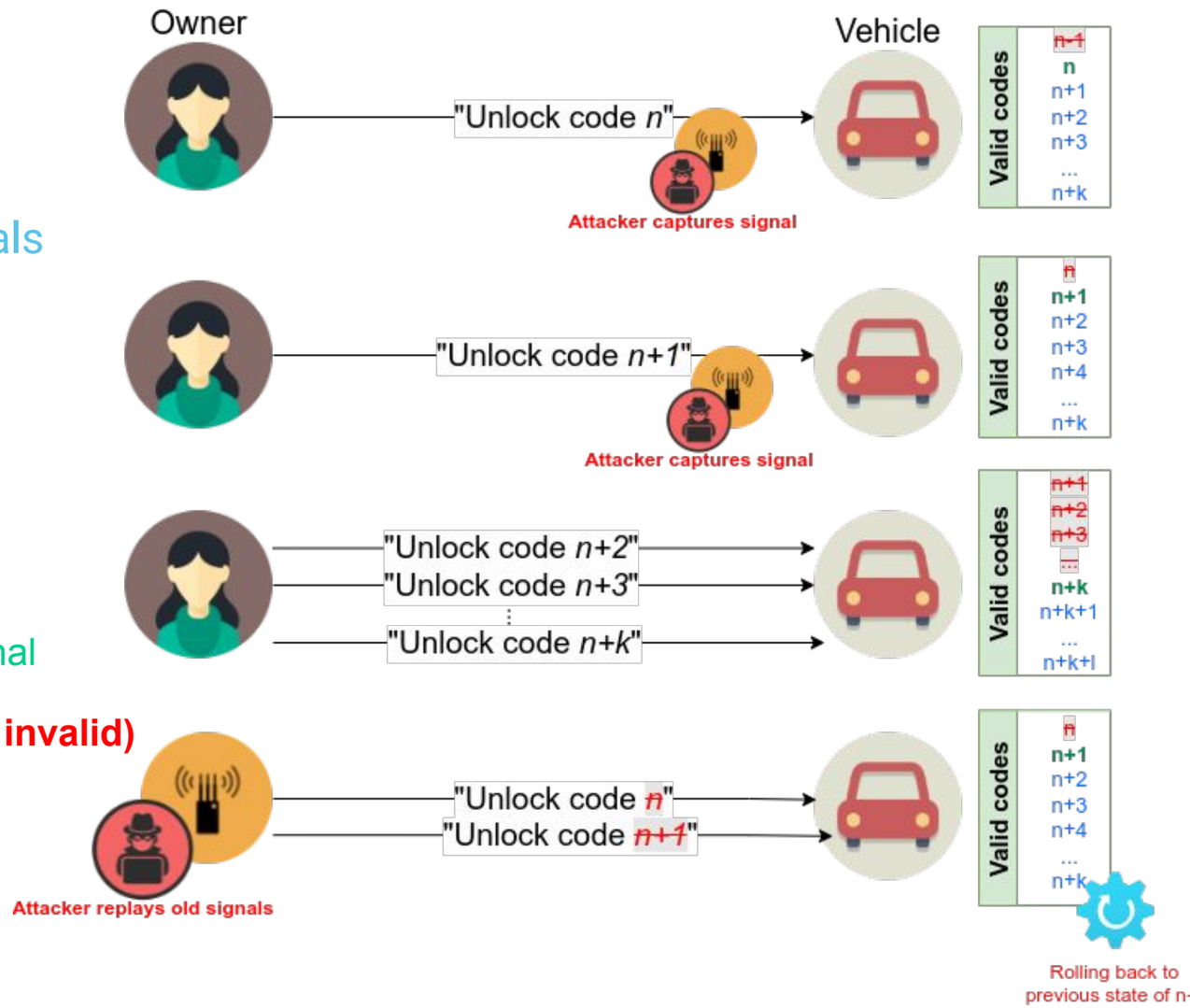
Why RollBack? Advantages?

- **Rolling back to a previous code/state**
  - The captured consecutive signals are replayed
  - The vehicle re-synchronize to a previous code
    - To the old counters in the last replayed signals
  - Vehicle acts according to the instruction in the signals
    - i.e., unlocks



2. replay first two unlock signals

1. last unlock signal received
(all signals are invalid)

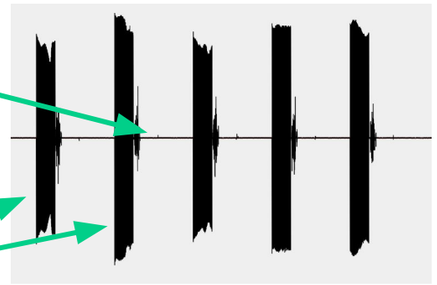


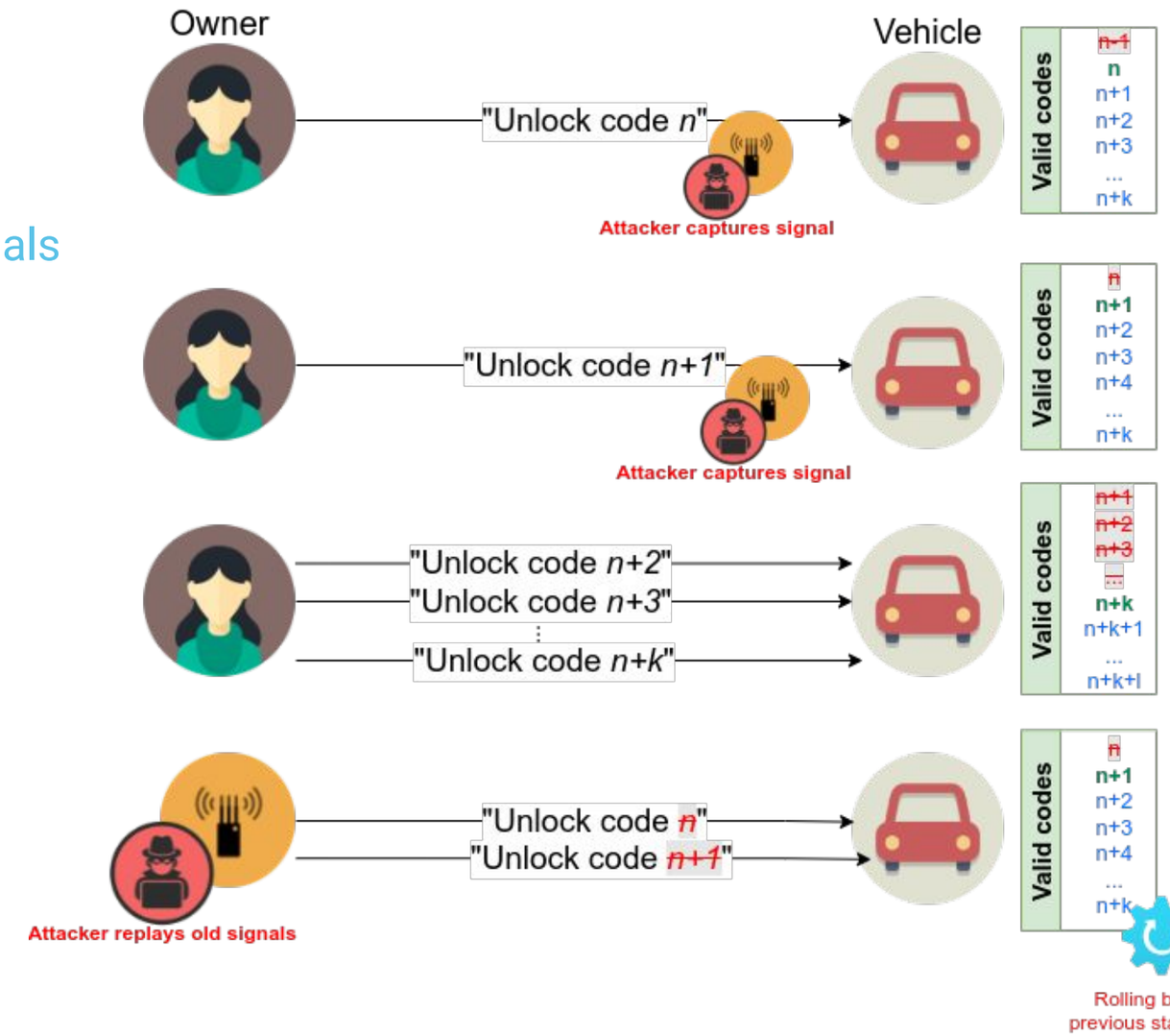
Why RollBack? Advantages?

- **Rolling back to a previous code/state**
  - The captured consecutive signals are replayed
  - The vehicle re-synchronize to a previous code
    - To the old counters in the last replayed signals
  - Vehicle acts according to the instruction in the signals
    - i.e., unlocks

3. Vehicle unlocks, counters rolled back to this state

2. replay first two unlock signals

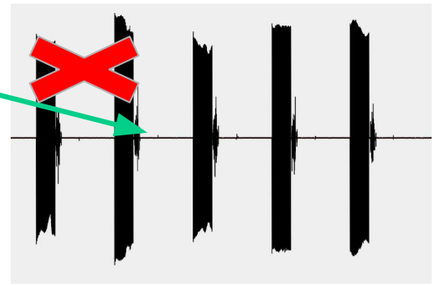


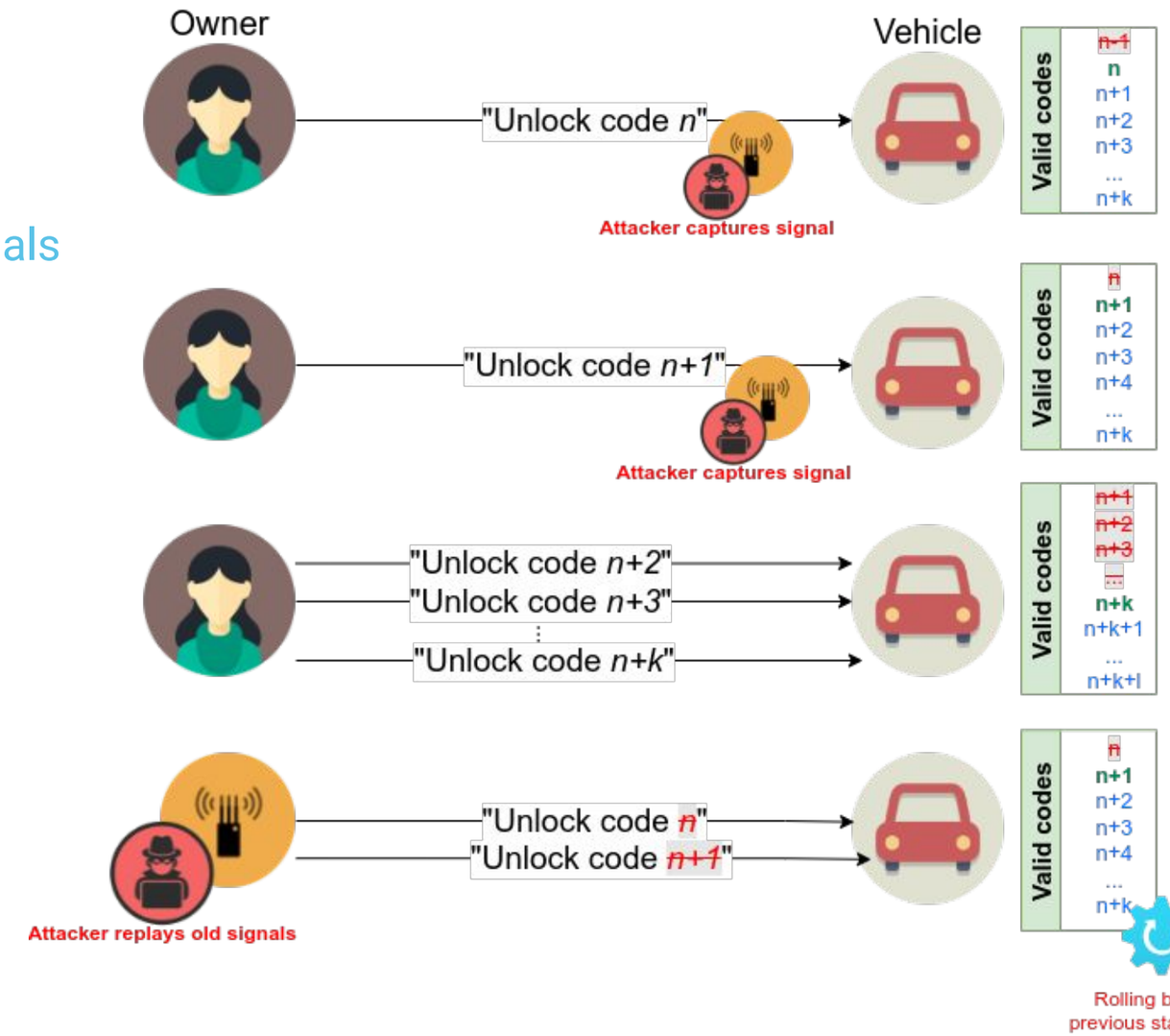


Why RollBack? Advantages?

- **Rolling back to a previous code/state**
  - The captured consecutive signals are replayed
  - The vehicle re-synchronize to a previous code
    - To the old counters in the last replayed signals
  - Vehicle acts according to the instruction in the signals
    - i.e., unlocks

3. Vehicle unlocks, counters rolled back to this state **(first two signals become invalid)**

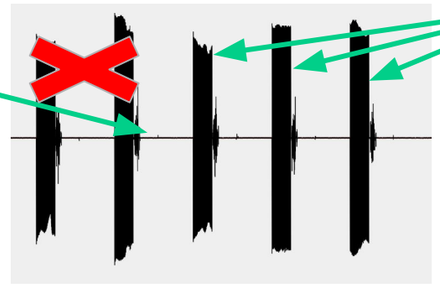




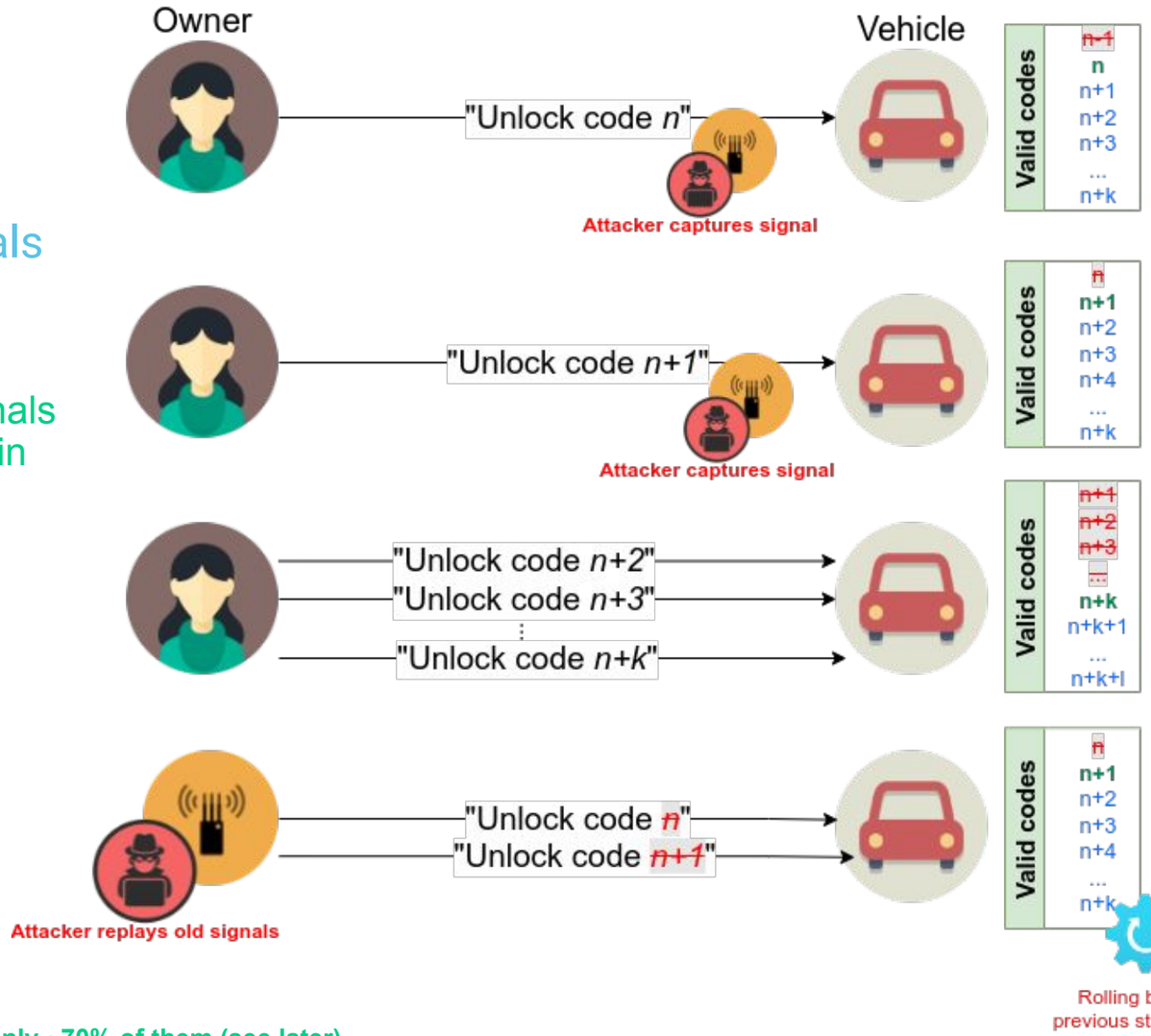
Why RollBack? Advantages?

- **Rolling back to a previous code/state**
  - The captured consecutive signals are replayed
  - The vehicle re-synchronize to a previous code
    - To the old counters in the last replayed signals
  - Vehicle acts according to the instruction in the signals
    - i.e., unlocks

3. Vehicle unlocks, counters rolled back to this state **(first two signals become invalid)**



4. These signals are valid again



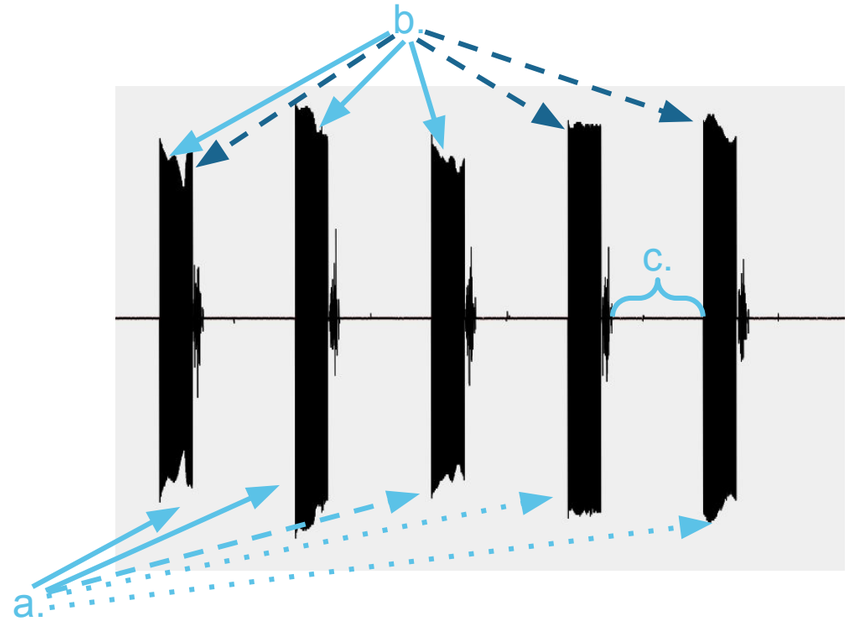
- **Time-agnostic – attacker can rollback the system**
  - At any time
  - As many times as desired

} **More effective* than RollJam**

*More effective '`iff`' vulnerable: RollJam "breaks" all rolling code-based systems, while RollBack only ~70% of them (see later)

RollBack - Variants

- **Different vulnerable RKE systems impose different requirements**
- **Properties:**
  - a. Number of signals
    - how many signals do we need to capture?
  - b. Sequence / consecutiveness
    - capture signal in order only OR strictly sequentially?
      - *capture and replay (1, 2, 3) vs. (1, 4, 5)*
  - c. Time frame
    - How fast do we need to replay the captured signals?



Variant	#SIGNALS	SEQUENCE	TIMEFRAME
$RollBack_{\otimes}^{\text{Loose}}(2)$	2	Loose	$\otimes$
$RollBack_{N}^{\text{Strict}}(2)$	2	Strict	N sec
$RollBack_{\otimes}^{\text{Strict}}(3)$	3	Strict	$\otimes$
$RollBack_{\otimes}^{\text{Strict}}(5)$	5	Strict	$\otimes$

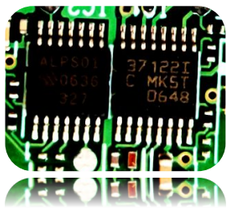
Yes, so far no variant in between, i.e., no variant found yet like
- (2, Strict, X)
- (2, Loose, *y* sec)

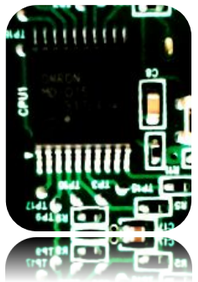
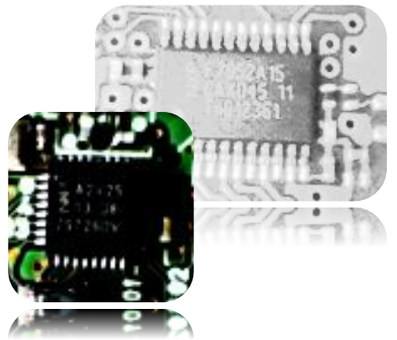
Disclaimer

- No REAL attempts made in the wild
- All recorded signals were permanently deleted after the tests
  - except for two vehicles for testing the time-agnostic feature of RollBack
  - afterward, those signals were permanently deleted
- *RollBack attack (or any replay attack) does not make any harm to the vehicle*
  - key fob might be temporarily blocked
  - the physical key has to be used once to access the vehicle

RollBack “in the wild”

- Evaluation on a limited set of vehicles so far
- “Blurry” conclusion
  - Age **DOES NOT** matter
  - Petrol vs. hybrid **DOES NOT** matter
  - Most of the popular Asian cars tested **ARE** affected
    - All tested **Mazda, Honda, Kia ARE** vulnerable
    - All tested **Toyota cars ARE** safe
  - **All** Mfr. 2 **and** Mfr. 3 **ARE affected***
    - They both need **2 signals only**
  - **Most** Mfr. 1 **RKE ARE affected***
    - Mazda needs 3 signals
    - Honda needs 5 signals
  - **Vehicles using** Mfr. 4**’s RKE ARE NOT affected***



Car Make	Model	Mfg. date	RKE manufacturer	RollBack (variant)
Honda	Model 1 (hybrid)	2016	Mfr. 1 - chip 1	$RollBack_{\otimes}^{\text{Strict}}(5)$
	Model 1	2018	Mfr. 1 - chip 2	$RollBack_{\otimes}^{\text{Strict}}(5)$
	Model 2	2017	Mfr. 1 - chip 1	$RollBack_{\otimes}^{\text{Strict}}(5)$
	Model 3	2017	Mrf. 1 - chip 1	$RollBack_{\otimes}^{\text{Strict}}(5)$
Hyundai	Model 1	2015	Mfr. 2 - chip 1	$RollBack_{\otimes}^{\text{Loose}}(2)$
	Model 1	2012	Mfr. 1 - chip 3	NO
	Model 2	2020		NO
Kia	Model 1	2017	Mfr. 2 - chip 2	$RollBack_{\otimes}^{\text{Loose}}(2)$
	Model 1	2015	Mfr. 2 - chip 2	$RollBack_{\otimes}^{\text{Loose}}(2)$
Mazda	Model 1	2018	Mfr. 1 - chip 4	$RollBack_{\otimes}^{\text{Strict}}(3)$
	Model 2	2018	Mfr. 1 - chip 5	$RollBack_{\otimes}^{\text{Strict}}(3)$
	Model 3	2020	Mfr. 1 - chip 4	$RollBack_{\otimes}^{\text{Strict}}(3)$
	Model 4	2019	Mfr. 1 - chip 4	$RollBack_{\otimes}^{\text{Strict}}(3)$
	Model 5	2018	Mfr. 1 - chip 5	$RollBack_{\otimes}^{\text{Strict}}(3)$
Nissan	Model 1	2014	Mfr. 1 - chip 6	NO
	Model 2	2009	Mfr. 3 - chip 1	$RollBack_{5}^{\text{Strict}}(2)$
	Model 3		Mfr. 1 - chip 7	$RollBack_{8}^{\text{Strict}}(2)$
Toyota	Model 1			NO
	Model 2		Mfr. 4 - chip 1	NO
	Model 3		Mfr. 4 - chip 2	NO

*Although not the key fobs have the flaw but probably the receiving unit (typically manufactured by other OEMs), we observe a correlation (so far)

this might be of interest too

DEMO

RollBack in action

RollBack in General

https://youtu.be/auPtxnbly4s
https://youtu.be/ltY11yo95R8
https://youtu.be/sdsfDKSfGhU
https://youtu.be/nyVqsaSCKks
and maybe more

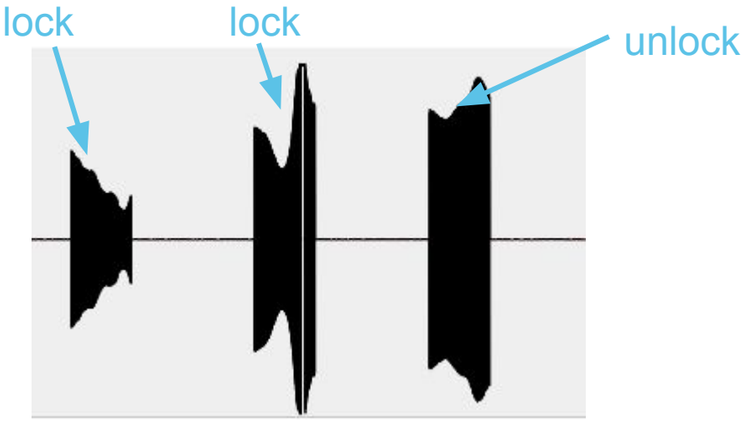
something new

RollBack

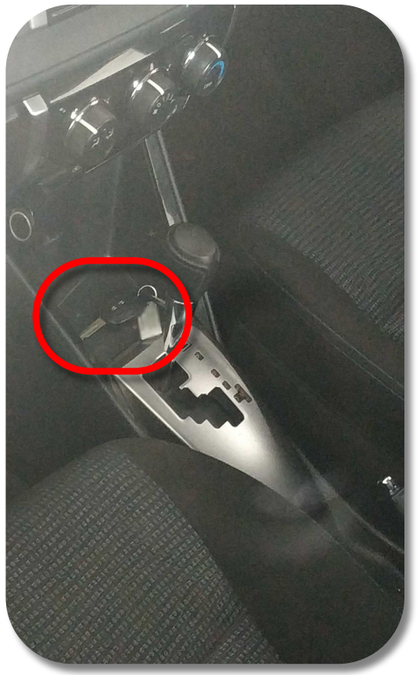
is instruction-agnostic

RollBack - Instruction-agnostic

- **Instruction encoded in the signal DOES NOT matter**
  - confirmed for Mazda
    - we only need 3 consecutive signals
  - confirmed for Kia (see demo later)
    - any two sequential but NOT STRICTLY CONSECUTIVE signals work



- **Attackers have even fewer things to do**
  1. Victim goes to a parking lot (e.g., to do the groceries)
  2. Presses the lock button (twice)
     a. most of us press the lock button twice (to confirm)
  3. Wait for the victim to come back and capture the "unlock" signal
  4. PROFIT



Car-sharing scenario

- **NOTE:**
  - *Car-sharing* / Car-renting use cases are the simplest
  - In *car-sharing*, the original key is usually inside → vehicle is at risk

RollBack: instruction-agnostic

https://youtu.be/auPtxnbly4s
https://youtu.be/ltY11yo95R8
https://youtu.be/sdsfDKSfGhU
https://youtu.be/nyVqsaSCKks
and maybe more

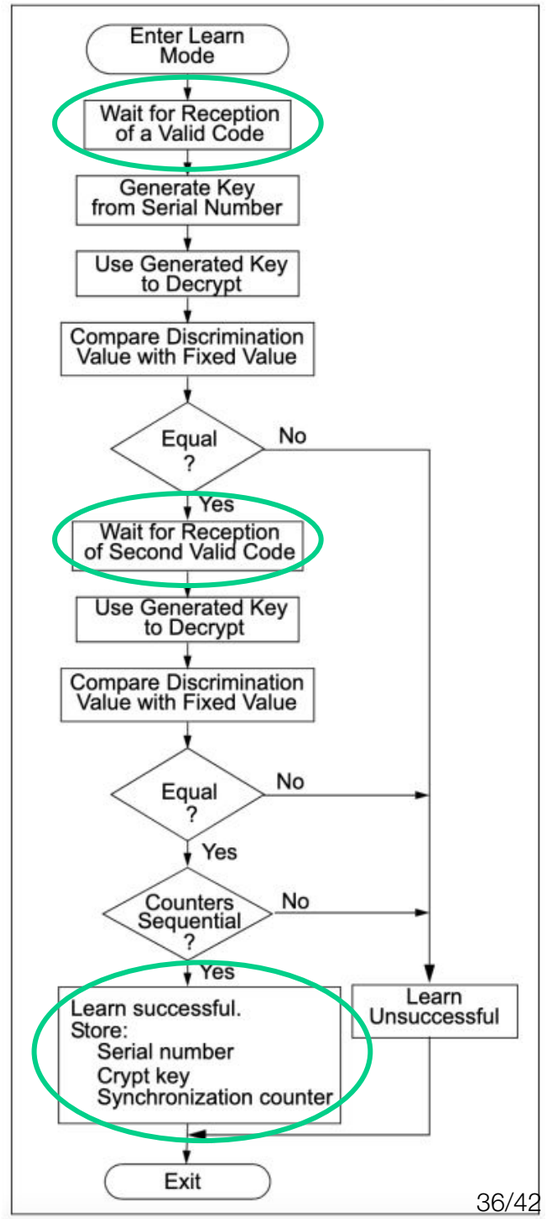
Root Cause & Mitigation

The missing pieces of the puzzle

Root Cause & Mitigation

- **Root cause:** still unknown
- **Possible candidate: key fob learning process**
  - Microchip has publicly available documentation [1]

https://i.ytimg.com/vi/8ARxmFVPJ3o/maxresdefault.jpg

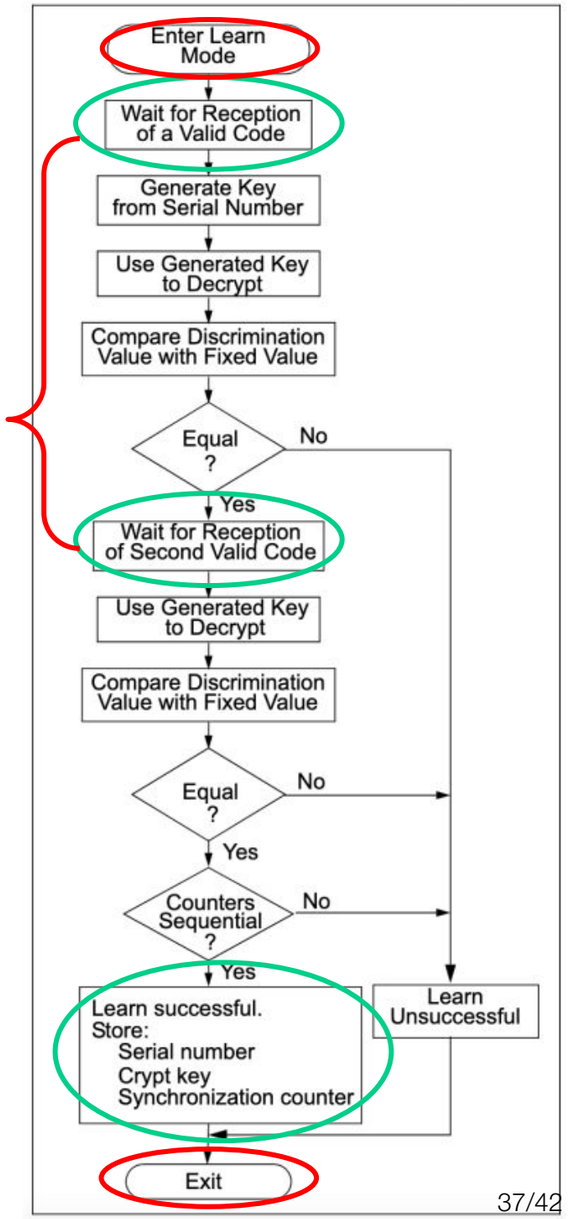


[1] Microchip, “KeeLoq™ Code Hopping Encoder,” Microchip HCS200, https://bit.ly/3GqCl5c, 2011 [Accessed: Jul 2022].

Root Cause & Mitigation

- **Root cause:** still unknown
- **Possible candidate: key fob learning process**
  - Microchip has publicly available documentation [1]
  - HOWEVER: there are several unusual steps
    - entering/exiting from the learning mode? *Forever learning mode?*
    - time frame between signals
    - vehicle reaction
    - old key fob re-added?

https://i.ytimg.com/vi/8ARxmFVPJ3o/maxresdefault.jpg

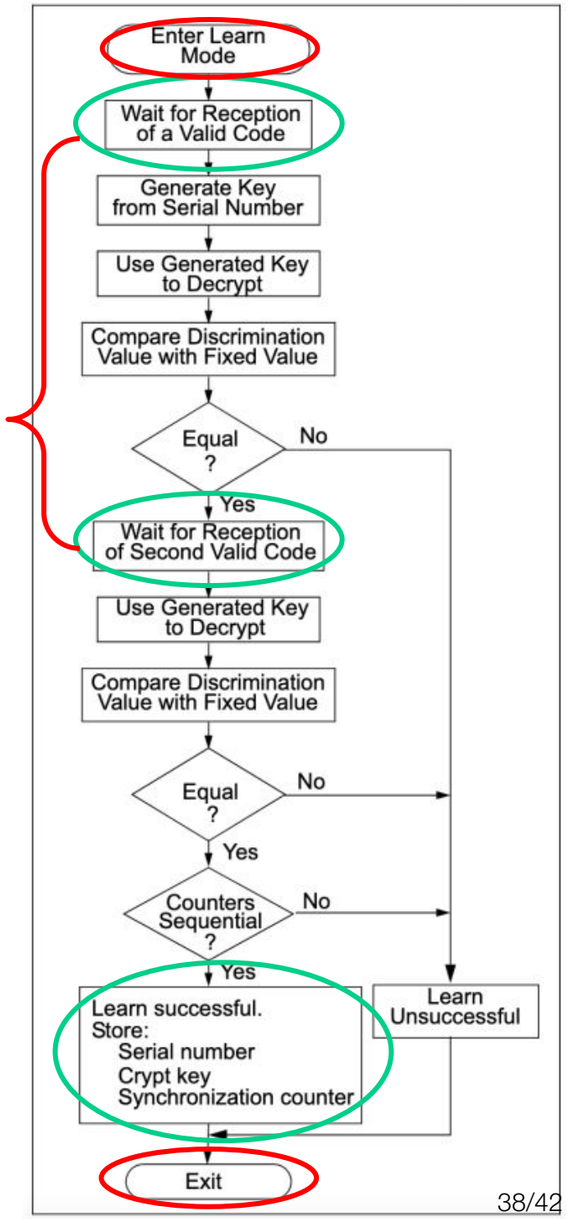


[1] Microchip, “KeeLoq™ Code Hopping Encoder,” Microchip HCS200, https://bit.ly/3GqCl5c, 2011 [Accessed: Jul 2022].

Root Cause & Mitigation

- **Root cause:** still unknown
- **Possible candidate: key fob learning process**
  - Microchip has publicly available documentation [1]
  - HOWEVER: there are several unusual steps
    - entering/exiting from the learning mode? *Forever learning mode?*
    - time frame between signals
    - vehicle reaction
    - old key fob re-added?
- **Mitigation**
  - General advice: most jamming-based attacks can be avoided by precautionary measures
    - e.g., first signal received but second was not in the case of RollJam

https://i.ytimg.com/vi/8ARxmFVPJ3o/maxresdefault.jpg

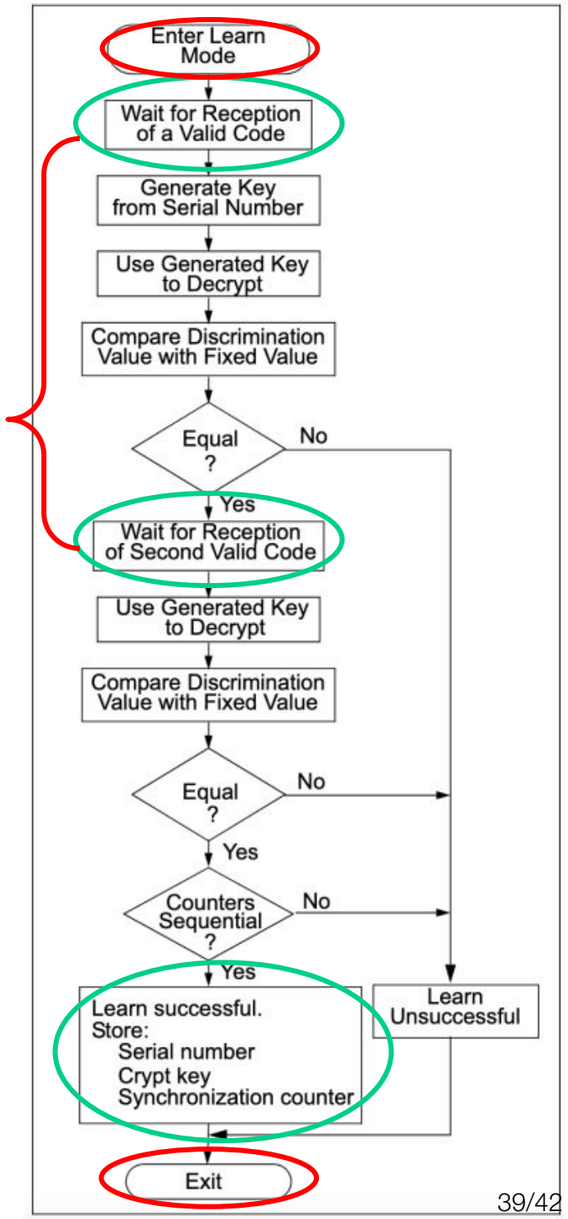


[1] Microchip, “KeeLoq™ Code Hopping Encoder,” Microchip HCS200, https://bit.ly/3GqCl5c, 2011 [Accessed: Jul 2022].

Root Cause & Mitigation

- **Root cause:** still unknown
- **Possible candidate: key fob learning process**
  - Microchip has publicly available documentation [1]
  - HOWEVER: there are several unusual steps
    - entering/exiting from the learning mode? *Forever learning mode?*
    - time frame between signals
    - vehicle reaction
    - old key fob re-added?
- **Mitigation**
  - General advice: most jamming-based attacks can be avoided by precautionary measures
    - e.g., first signal received but second was not in the case of RollJam
  - **RollBack does not necessitates jamming**
  - **Being time-agnostic, no precautionary measure applies**

https://i.ytimg.com/vi/8ARxmFVPJ3o/maxresdefault.jpg

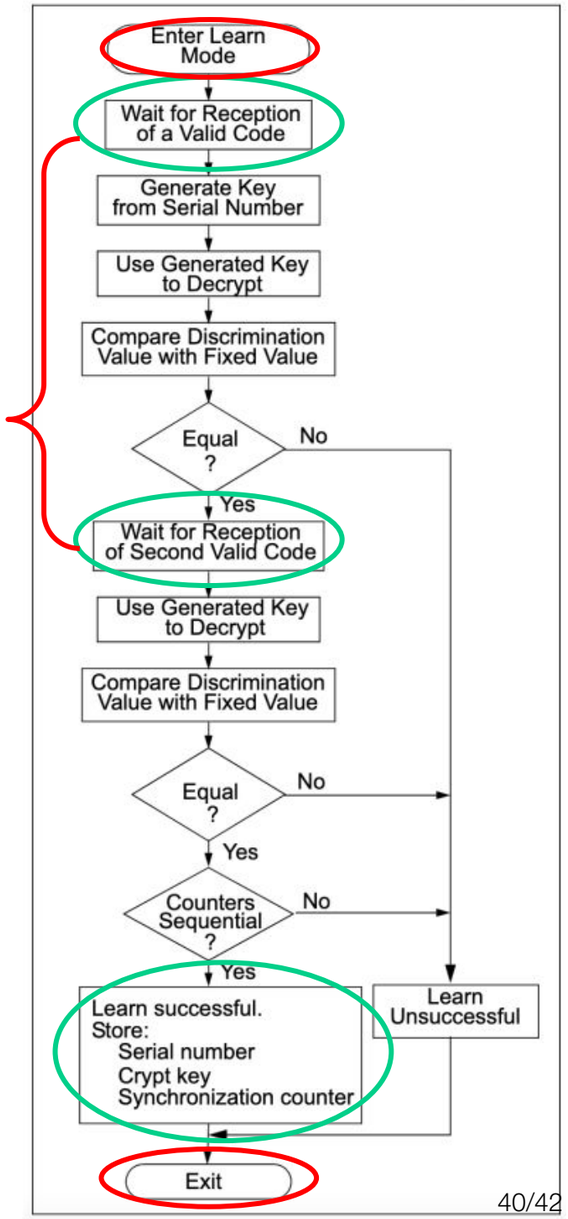


[1] Microchip, “KeeLoq™ Code Hopping Encoder,” Microchip HCS200, https://bit.ly/3GqCl5c, 2011 [Accessed: Jul 2022].

Root Cause & Mitigation

- **Root cause:** still unknown
- **Possible candidate: key fob learning process**
  - Microchip has publicly available documentation [1]
  - HOWEVER: there are several unusual steps
    - entering/exiting from the learning mode? *Forever learning mode?*
    - time frame between signals
    - vehicle reaction
    - old key fob re-added?
- **Mitigation**
  - General advice: most jamming-based attacks can be avoided by precautionary measures
    - e.g., first signal received but second was not in the case of RollJam
  - **RollBack does not necessitates jamming**
  - **Being time-agnostic, no precautionary measure applies**
- **Use timestamps along with the rolling codes (and check!)**

https://i.ytimg.com/vi/8ARxmFVPJ3o/maxresdefault.jpg



[1] Microchip, "KeeLoq™ Code Hopping Encoder," Microchip HCS200, https://bit.ly/3GqCl5c, 2011 [Accessed: Jul 2022].

black hat USA 2022

Sound bytes a.k.a.
3 KEY TAKEAWAYS

1) **RollBack** - Capturing and replaying *a couple* of signals re-synchronizes the rolling codes and unlocks most of today's modern (Asian) vehicles tested
   a) RollBack is *instruction-agnostic*

2) Unlike RollJam, **RollBack**
   a) *does not require signal jamming*, only signal capturing *once*
   b) captured signals can be replayed *at any time* and *as many times* as desired

3) So far, the root cause is not confirmed and no explicit mitigation exists
   a) adding timestamps to the signals (and checking them) might help

black hat USA 2022

Q&A

Levente Csikor
NCS Group
Institute for Infocomm Research, A*STAR
levente.csikor@gmail.com
csikor_levente@i2r.a-star.edu.sg

Agency for Science, Technology and Research
SINGAPORE

Hoon Wei Lim
NCS Group
hoonwei.lim@ncs.com.sg

ncs

Reach out to us for any further enquiry

Thanks to our co-authors:
Jun Wen Wong (NCS Group / DSBJ),
Soundarya Ramesh (NUS),
Rohini Poolat Parameswarath (NUS),
Mun Choon Chan (NUS)
for their support (e.g., their cars :D) and inputs

Whitepaper will be released soon on the Black Hat site with more information.
Don't forget to get back ;)

Photo by Kelly Sikkema on Unsplash