Access Your Tesla without Your Awareness

Compromising Keyless Entry System of Model 3

Kun Jiang[1], Xinyi Xie[1], Rui Dai[1], Lihui Wang[1], Jun Lu[1], Qing Li[12] and Jun Yu[12]

[1] Security Laboratory of Shanghai Fudan Microelectronics Group Co. Ltd, China

[2] State Key Laboratory of ASIC & System, Fudan University, Shanghai, China

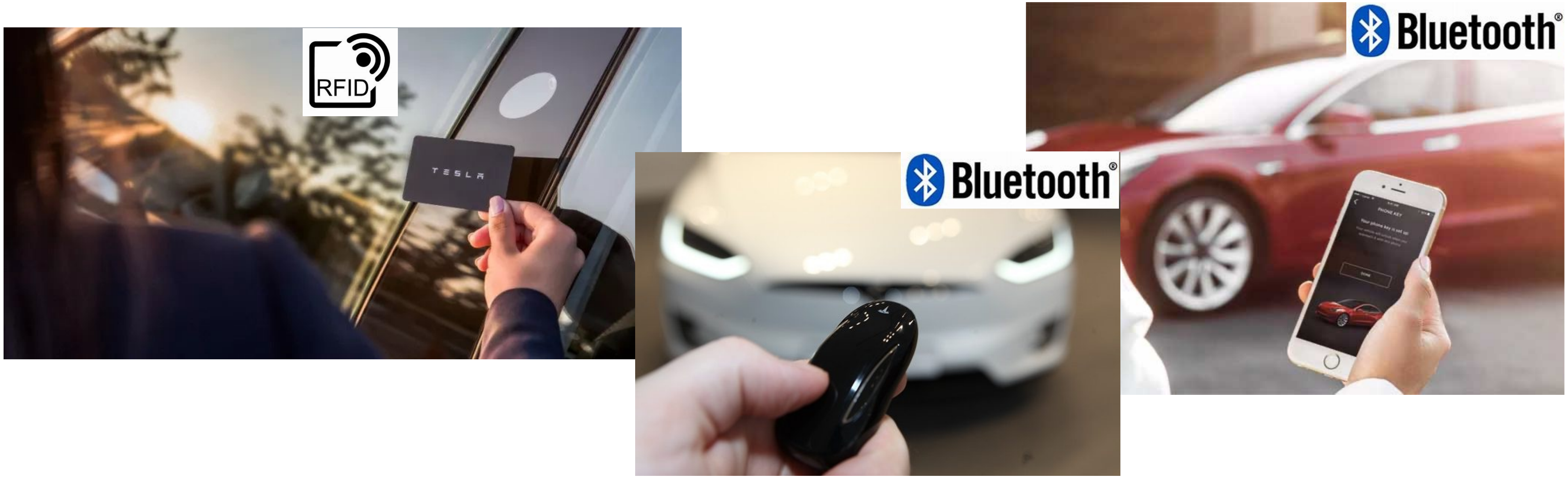
Network and Distributed System Security Symposium, NDSS 2023

March 2, 2023. | San Diego, California

Motivation & Who we are

◆ Motivation

- *My colleague bought a Model 3 for his wife (during sales promotion)* ^_^
- *Model 3 has equipped with Key Card, BLE Key Fob and Phone Key*



Motivation & Who we are

◆ Motivation

- *My colleague bought a Model 3 for his wife (during a sales promotion)* ^_^
- *Tesla introduced Key Card, BLE Key Fob and Phone Key*

◆ Familiar with

- Contactless *Smart Card*
- *RFID* (**ISO 14443**)
- *Side Channel Attack and Countermeasures*
- *Cyber-Physical Systems Security*

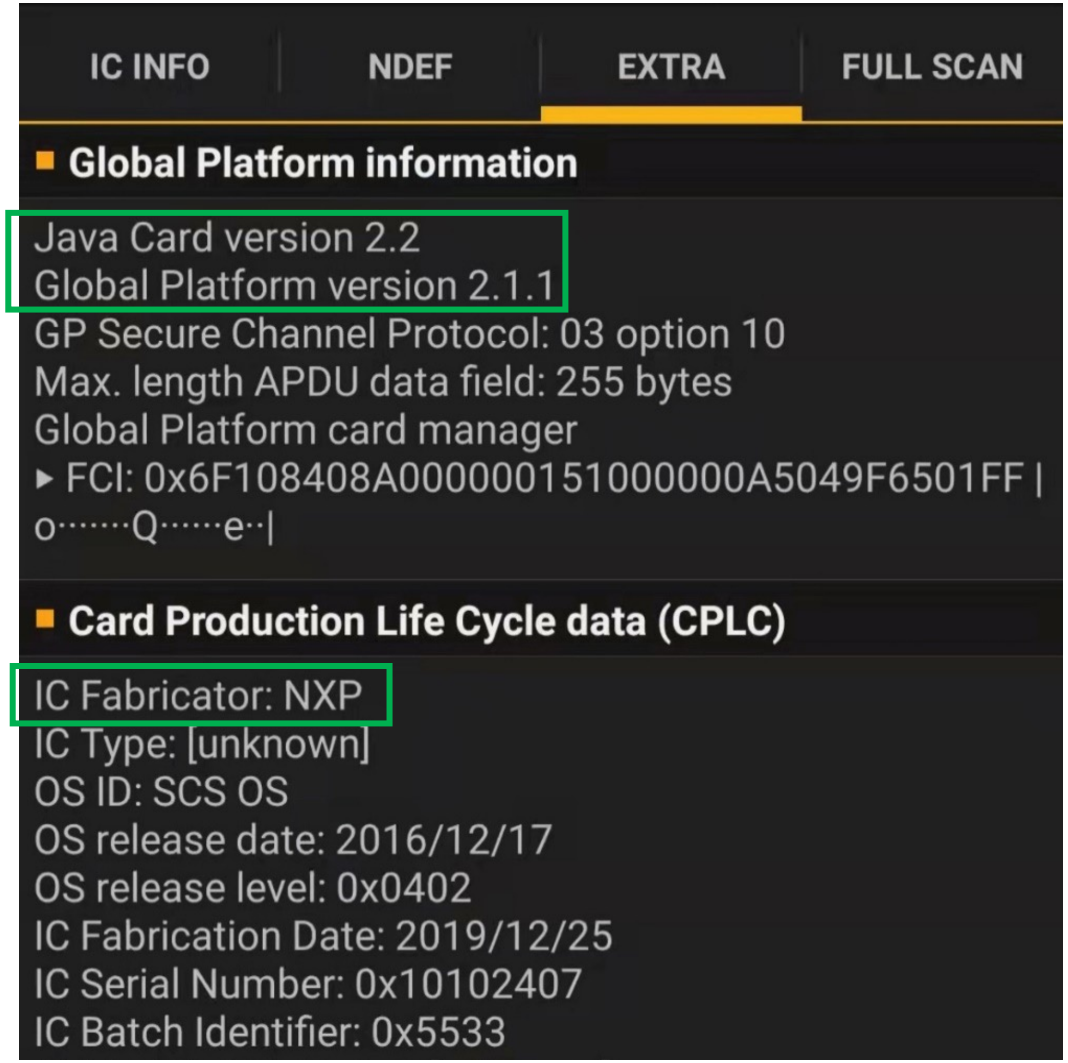
Key Card & Phone Key

Pairing and Authentication Protocols Recovery

Key Card IC Details

- **Java Card Manufactured by NXP**
  - Banking Payment
  - National ID
  - Electronic Passport

- **Common Criteria EAL 5 or 6 + Certified**
  - RSA, ECC, AES
  - Simple Power Analysis Protection
  - Differential Power Analysis Protection
  - Timing Analysis Protection
  - Fault Injection Protection



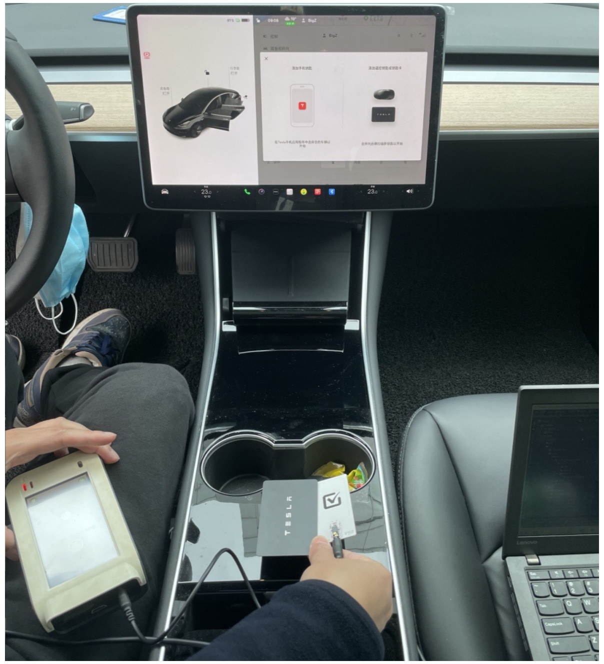
■ Global Platform information

```
Java Card version 2.2
Global Platform version 2.1.1
GP Secure Channel Protocol: 03 option 10
Max. length APDU data field: 255 bytes
Global Platform card manager
▸ FCI: 0x6F108408A000000151000000A5049F6501FF |
o·······Q·······e··|
```

■ Card Production Life Cycle data (CPLC)

```
IC Fabricator: NXP
IC Type: [unknown]
OS ID: SCS OS
OS release date: 2016/12/17
OS release level: 0x0402
IC Fabrication Date: 2019/12/25
IC Serial Number: 0x10102407
IC Batch Identifier: 0x5533
```

Key Card Sniffer Setup

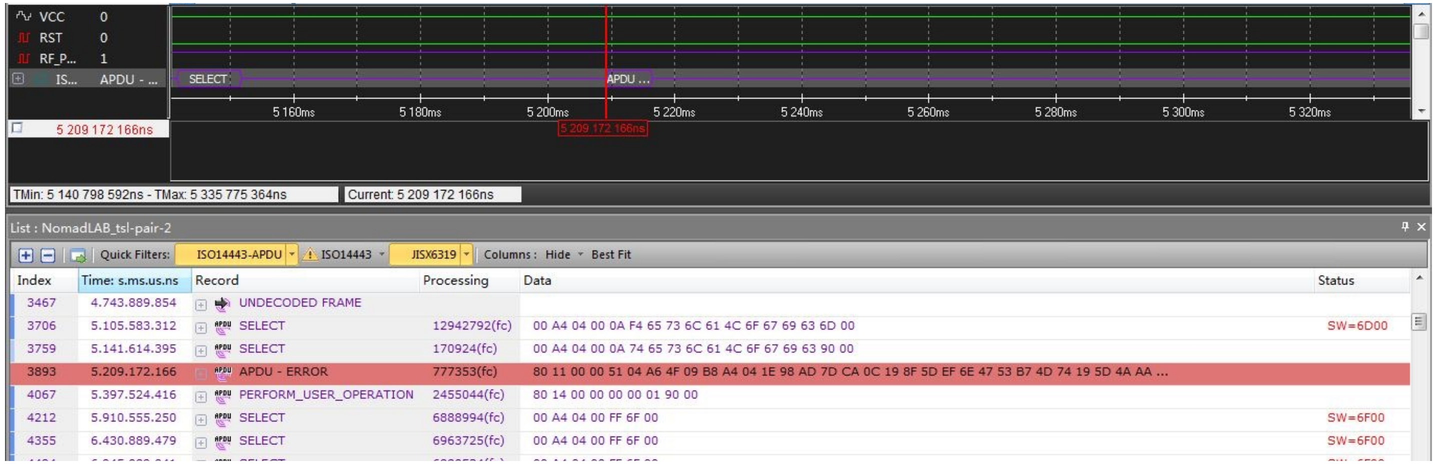


◆ ISO 14443 Spy

- ***MP300 TCL3*** or ***NomadLAB*** Contactless spy tool
- Set up as the picture ➔

◆ Powerful Protocol Analyzer

- ***MPManager*** or ***RGPA*** Software
- Use 3 Key Cards for testing
- Communication data logging ➔



TMin: 5 140 798 592ns - TMax: 5 335 775 364ns

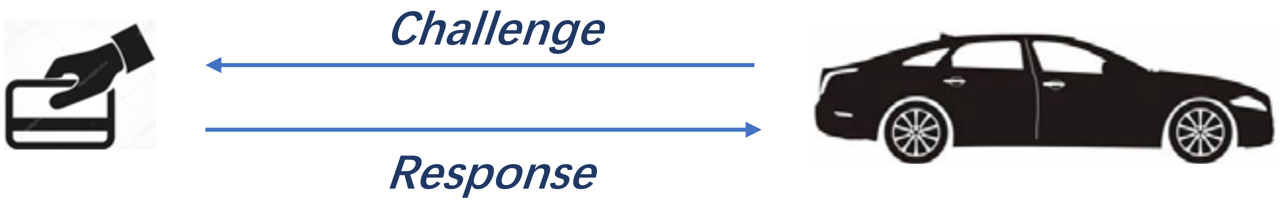
Current: 5 209 172 166ns

List : NomadLAB_tsl-pair-2

Index	Time: s.ms.us.ns	Record	Processing	Data	Status
3467	4.743.889.854	UNDECODED FRAME			
3706	5.105.583.312	SELECT	12942792(fc)	00 A4 04 00 0A F4 65 73 6C 61 4C 6F 67 69 63 6D 00	SW=6D00
3759	5.141.614.395	SELECT	170924(fc)	00 A4 04 00 0A 74 65 73 6C 61 4C 6F 67 69 63 90 00	
3893	5.209.172.166	APDU - ERROR	777353(fc)	80 11 00 00 51 04 A6 4F 09 B8 A4 04 1E 98 AD 7D CA 0C 19 8F 5D EF 6E 47 53 B7 4D 74 19 5D 4A AA ...	
4067	5.397.524.416	PERFORM_USER_OPERATION	2455044(fc)	80 14 00 00 00 00 01 90 00	
4212	5.910.555.250	SELECT	6888994(fc)	00 A4 04 00 FF 6F 00	SW=6F00
4355	6.430.889.479	SELECT	6963725(fc)	00 A4 04 00 FF 6F 00	SW=6F00

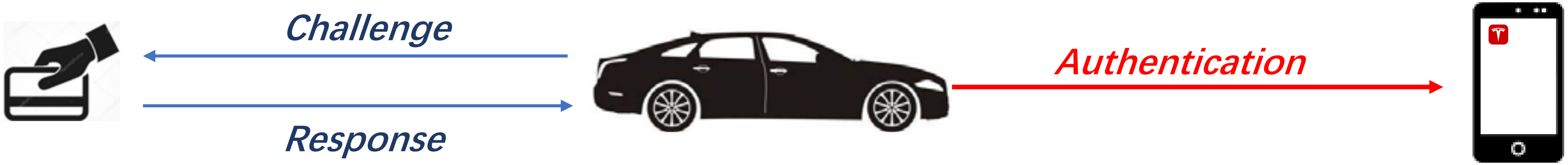
Kun Jiang et al. | "Access Your Tesla without Your Awareness: Compromising Keyless Entry System of Model 3" | NDSS 2023

Key Card



- **Challenge and Response Authentication Protocol**
  - Exchange ECC 256bit Public Key
- **Something Unknown**
  - Elliptic Curve Parameters
  - $Response$ **=** $\mathbf{g(}$ $Challenge$ $\mathbf{)}$, $\mathbf{g(*)}$ Function

Key Card & Phone Key



◆ Something in Common

- Elliptic Curve Parameters and Key Pair Format

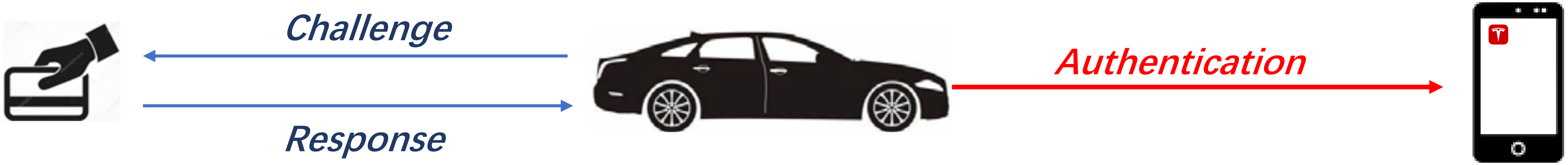
◆ Tesla Mobile App Contains More Information

- Bluetooth HCI Logs
- Cryptography Operations

◆ Widely Used Tools for Static Analysis & Dynamical Analysis

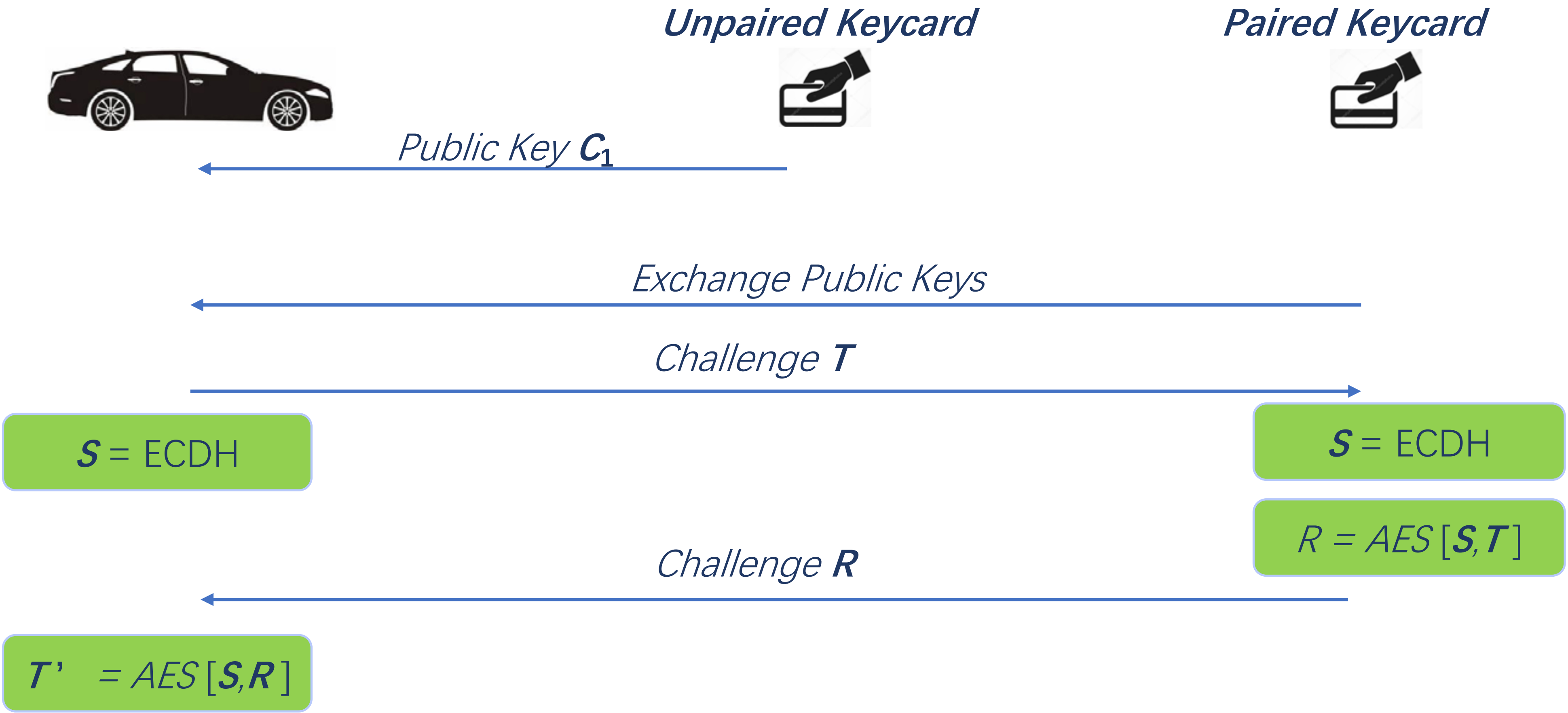
- JDAX, IDA, Frida,…

Key Card & Phone Key



- **Elliptic Curve Parameters**
  - NIST P256 Curve Parameters
- **Cryptography Operations**
  - ECDH, AES, SHA-1
- **$g(*)$ Function**
  - Related to the ECDH share secret and AES operations
  - Re-established with guessing and a programmable Java card for testing

Keycard Pairing and Authentication



Unpaired Keycard

Paired Keycard

Public Key $\boldsymbol{C_1}$

Exchange Public Keys

Challenge ***T***

S = ECDH

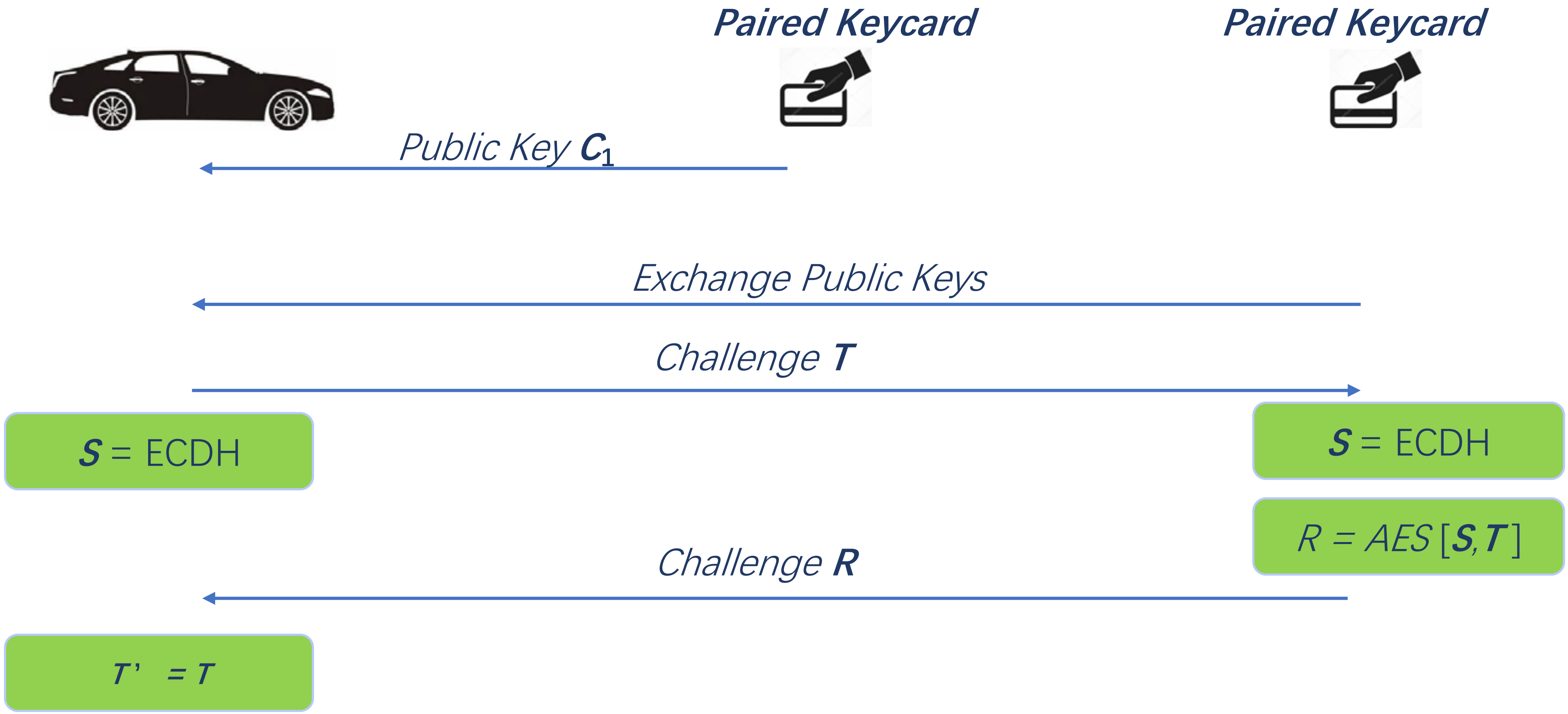
S = ECDH

$R = AES\,[\boldsymbol{S},\boldsymbol{T}]$

Challenge ***R***

$\boldsymbol{T}' = AES\,[\boldsymbol{S},\boldsymbol{R}]$

Keycard Pairing and Authentication



Paired Keycard

Paired Keycard

Public Key C_1

Exchange Public Keys

Challenge T

S = ECDH

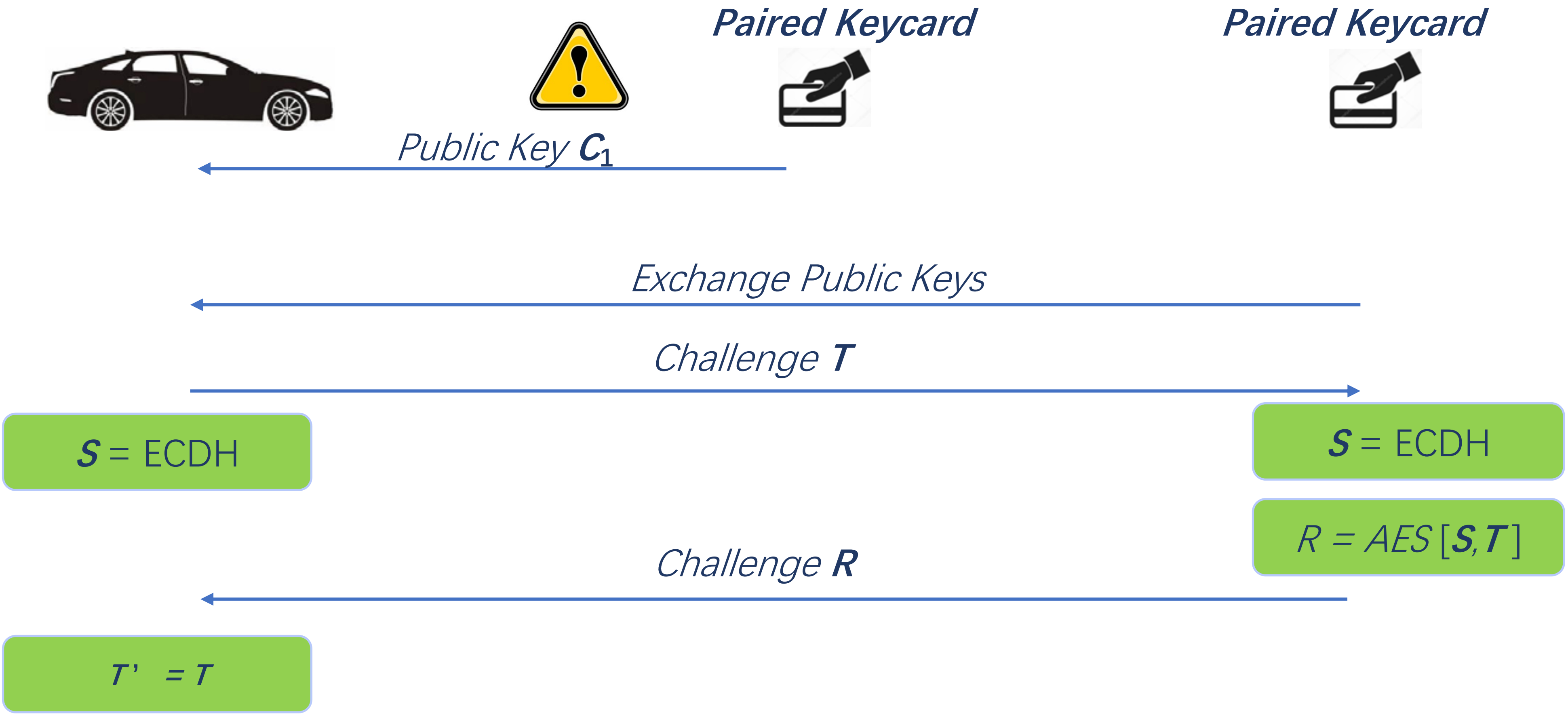
S = ECDH

$R = AES\,[S, T]$

Challenge R

$T' = T$

Keycard Pairing and Authentication



Paired Keycard

Paired Keycard

Public Key $\boldsymbol{C_1}$

Exchange Public Keys

Challenge ***T***

S = ECDH

S = ECDH

R = AES [***S***, ***T***]

Challenge ***R***

T' = T

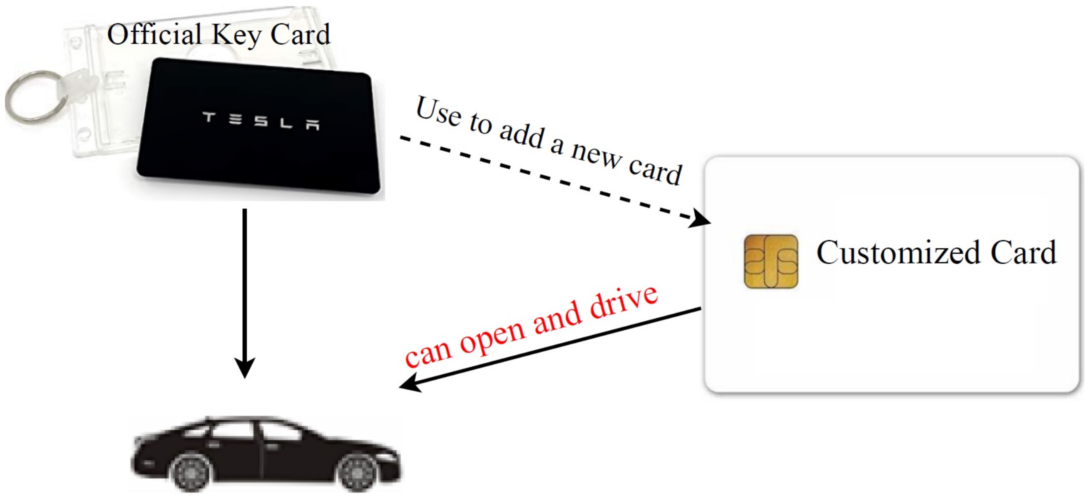
The vehicle does not verify Keycard certificates. It makes unofficial products work.

Kun Jiang et al. | “Access Your Tesla without Your Awareness: Compromising Keyless Entry System of Model 3” | NDSS 2023

Unofficial Products may lead to threats

◆ A Customized Key Card for POC

- Generate a key pair based on NIST p-256
- Support related cryptography operations
- Back door command to read the ECC private key



◆ Other Unofficial products leakage example

UNCATEGORIZED · TESLA

Teen hacker says he's found way to remotely control 25 Tesla EVs around the world

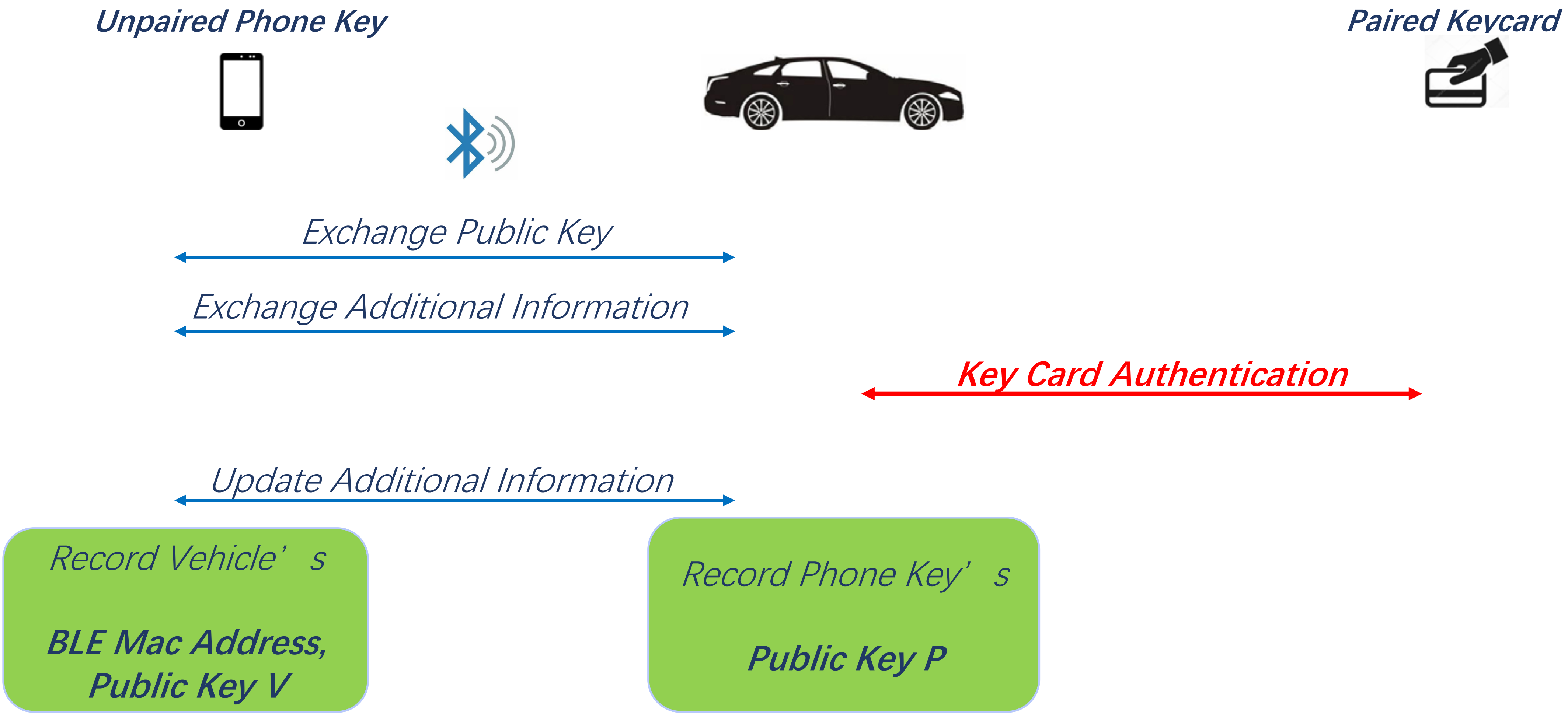
BY KATRINA NICHOLAS, JORDAN ROBERTSON AND BLOOMBERG

January 12, 2022 at 4:53 PM GMT+8

Updated January 13, 2022 at 5:27 PM GMT+8

Kun Jiang et al. | "Access Your Tesla without Your Awareness: Compromising Keyless Entry System of Model 3" | NDSS 2023

Phone Key Pairing



Unpaired Phone Key

Paired Keycard

Exchange Public Key

Exchange Additional Information

Key Card Authentication

Update Additional Information

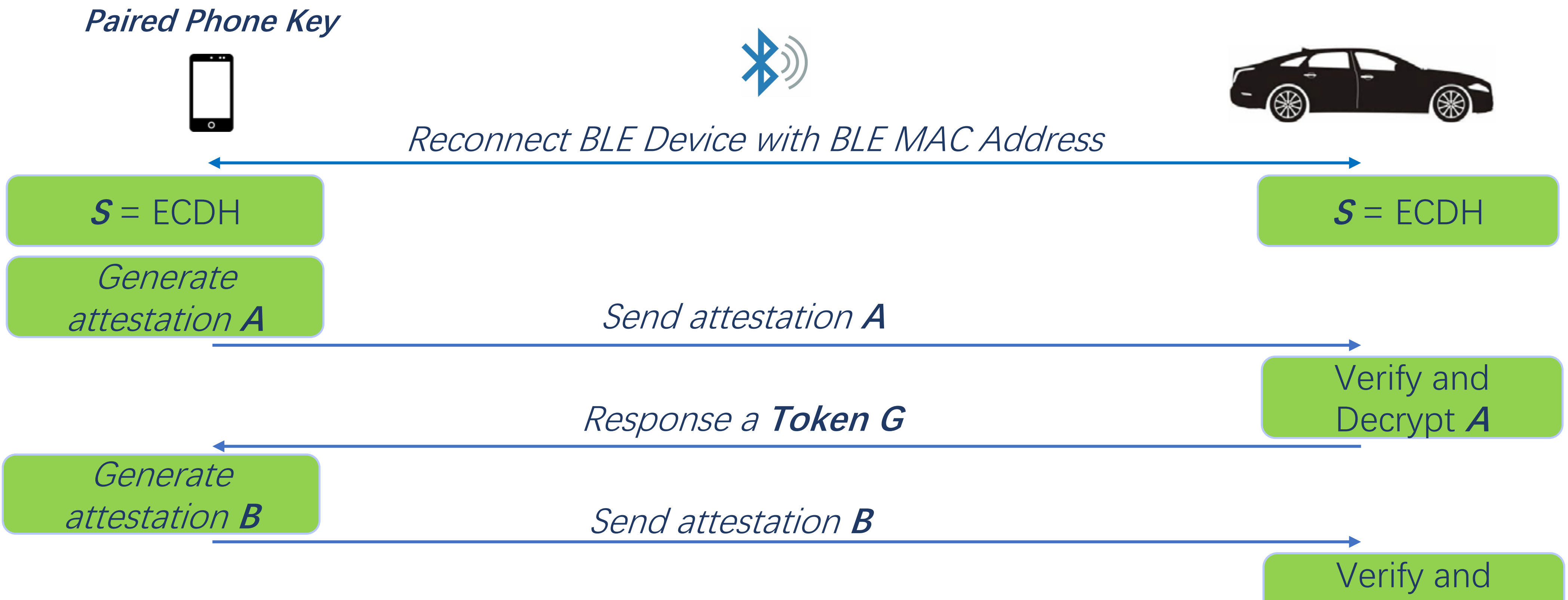
Record Vehicle’ s

BLE Mac Address, Public Key V

Record Phone Key’ s

Public Key P

Phone Key Keyless Entry Authentication


Paired Phone Key
Reconnect BLE Device with BLE MAC Address
S = ECDH
S = ECDH
*Generate attestation **A***
*Send attestation **A***
Verify and Decrypt ***A***
*Response a **Token G***
*Generate attestation **B***
*Send attestation **B***
Verify and Decrypt ***B***
Unlock

Format of an attestation

0x00	payload length	0x0a	counter	keyID	ciphertext	GCM tag

Ciphertext encrypted by AES-GCM mode

For Attestation ***B***, the token ***G*** will be the GCM additional authenticated data

Kun Jiang et al. | "Access Your Tesla without Your Awareness: Compromising Keyless Entry System of Model 3" | NDSS 2023

Security Analysis

◆ Private Key Protection

- **Key Card and Vehicle**: Private keys are both securely stored in a **Secure Element** (SE)
- **Phone Key**: Protected by **KeyStore** (Android)

◆ Replay Attack Protection

- Phone Key involves the **counter** by AES-GCM Mode

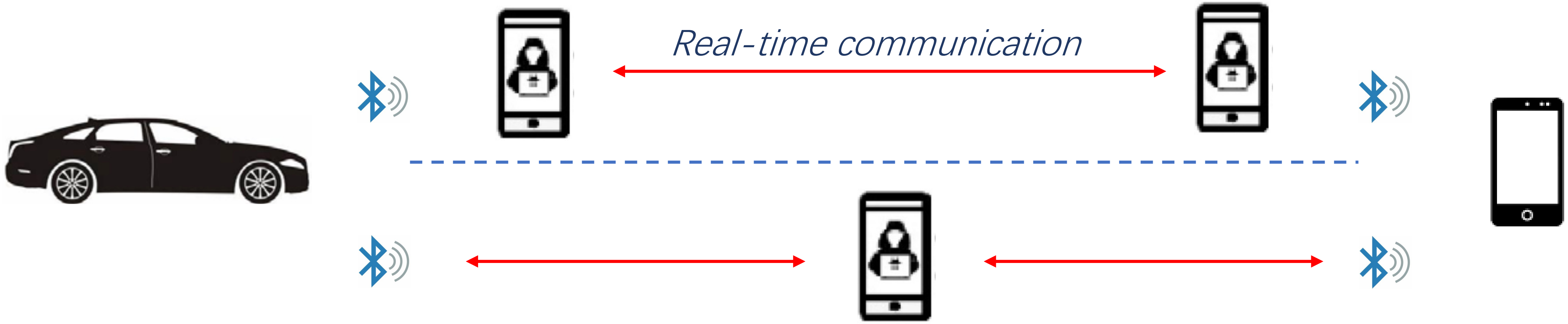
◆ Potential Issues

- Dose not enable the **BLE link layer encryption**
- Vehicles use **Static BLE MAC Address**
- The **update of token *G*** does not depend on the change of connection states. It fixed over a couple of hours

Susceptible to Relay or MitM attacks

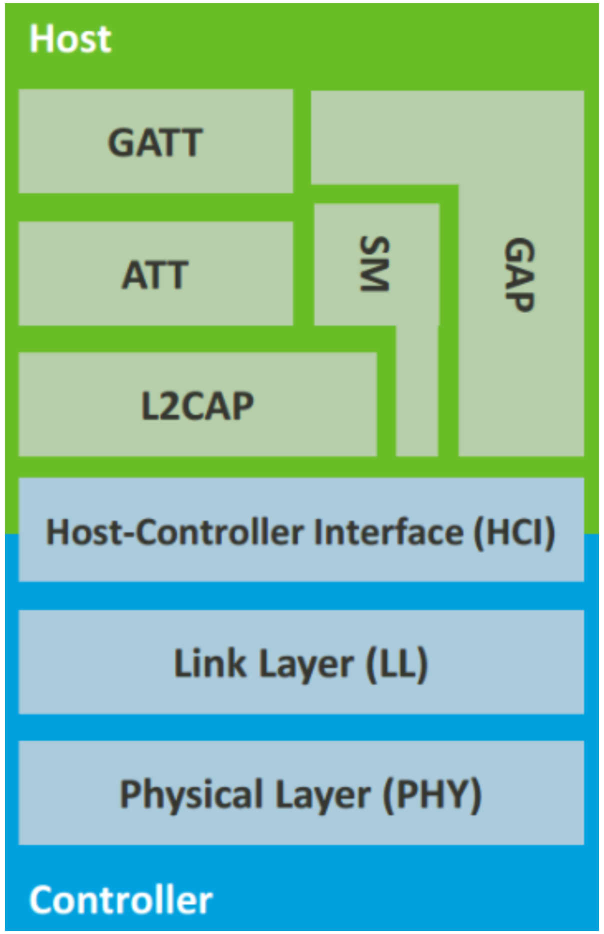
- **Two Attack devices**
  - One fake as the Vehicle, One fake as the Phone Key
  - Real-time message relay

- **One Attack device**
  - Round-trip message relay



Kun Jiang et al. | "Access Your Tesla without Your Awareness: Compromising Keyless Entry System of Model 3" | NDSS 2023

BLE Relay Attack



GATT Layer Relay: Gattacker (S J.), Btlejuice (D C.)

- Not support for link layer encryption
- Detectable added latency

Link layer relay: Sniffle Relay (NCC Group). 2022.

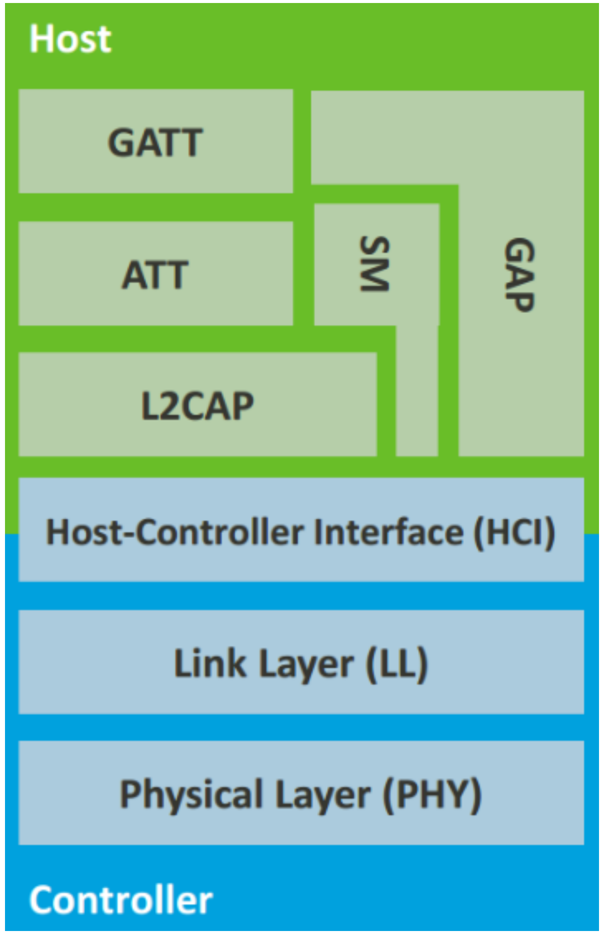
- Can circumvent link layer encryption.
- Need customize link layer stack

Analog Relay: Staat et al. 2022

- Simple hardware, low latency
- Limited relay distance

Kun Jiang et al. | "Access Your Tesla without Your Awareness: Compromising Keyless Entry System of Model 3" | NDSS 2023

BLE Relay Attack



GATT Layer Relay: Gattacker (S J.), Btlejuice (D C.)

- Not support for link layer encryption
- Detectable added latency

Link layer relay: Sniffle Relay (NCC Group). 2022.

- Can circumvent link layer encryption.
- Need customize link layer stack

Analog Relay: Staat et al. 2022

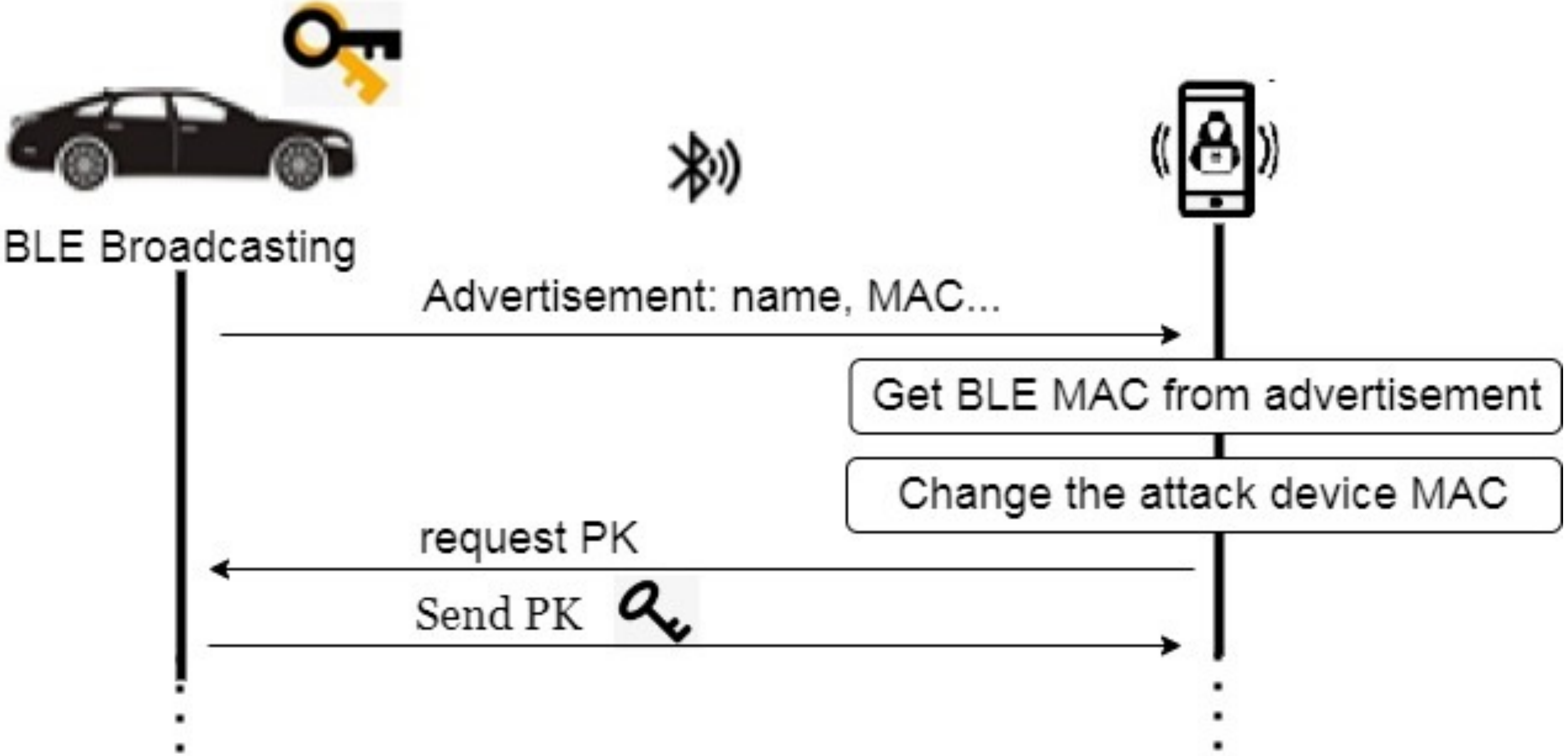
- Simple hardware, low latency
- Limited relay distance

Kun Jiang et al. | “Access Your Tesla without Your Awareness: Compromising Keyless Entry System of Model 3” | NDSS 2023

Attack Phases

◆ BLE MAC Spoof

- Get the **MAC** address and **Public key** of model 3 according to the BLE advertisement
- Change the **MAC** address of a attack device same as Model 3

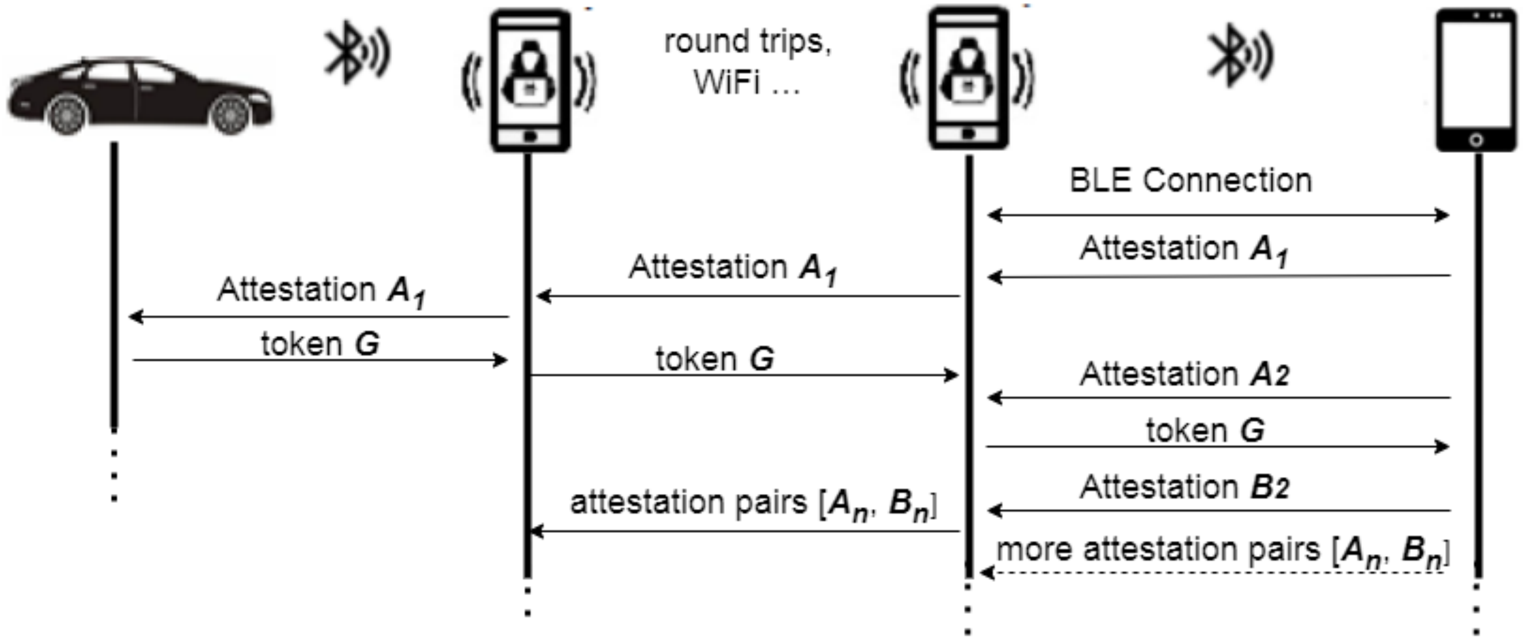

BLE Broadcasting
Advertisement: name, MAC...
Get BLE MAC from advertisement
Change the attack device MAC
request PK
Send PK

Kun Jiang et al. | "Access Your Tesla without Your Awareness: Compromising Keyless Entry System of Model 3" | NDSS 2023

Attack Phases

◆ Attestations Capture

- approaches the Phone Key to get attestation ***A*** and relay it
- Vehicle side attack device gets the token ***G*** and relay it
- The attacker will get attestation [***A***, ***B***] as a pair

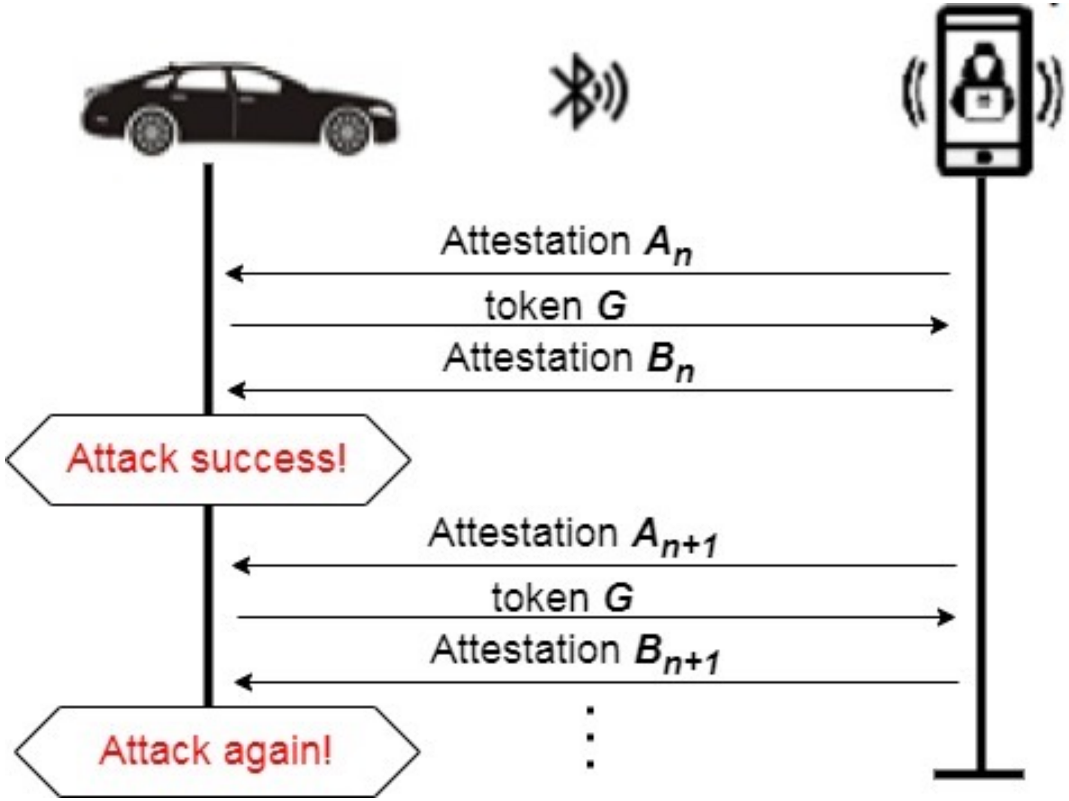


Kun Jiang et al. | “Access Your Tesla without Your Awareness: Compromising Keyless Entry System of Model 3” | NDSS 2023

Attack Phases

◆ Unlock and Access

- Attack will use Attestation pairs to unlock and access the Model 3
- Token G fixed for hours will lead to multiple access

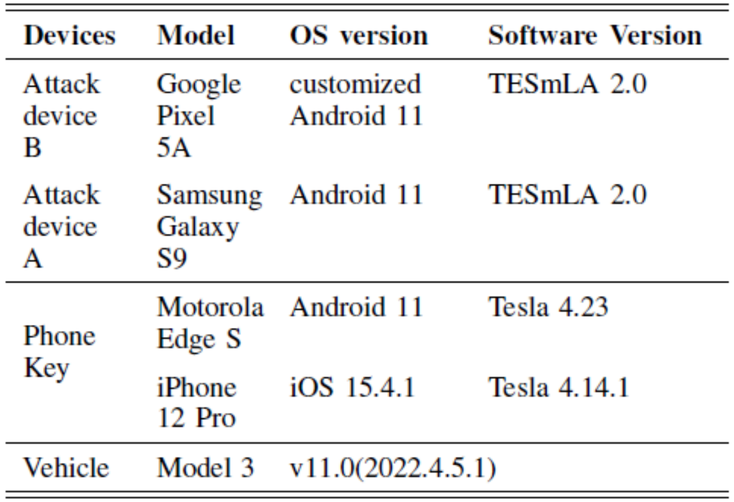


Kun Jiang et al. | “Access Your Tesla without Your Awareness: Compromising Keyless Entry System of Model 3” | NDSS 2023

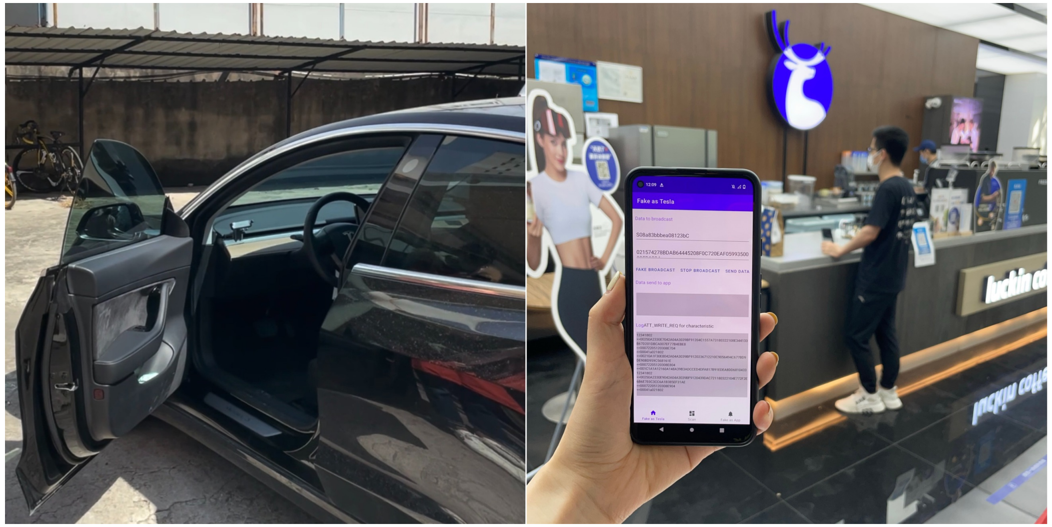
Proof of Concept

◆ Customized Android Device

- Customized the BLE firmware and disabled MAC address rotation during advertising
- Customized the android framework and enable arbitrary modify the BLE MAC address.
- **TESmLA** application performs BLE GATT relay attack



Devices	Model	OS version	Software Version
Attack device B	Google Pixel 5A	customized Android 11	TESmLA 2.0
Attack device A	Samsung Galaxy S9	Android 11	TESmLA 2.0
Phone Key	Motorola Edge S	Android 11	Tesla 4.23
	iPhone 12 Pro	iOS 15.4.1	Tesla 4.14.1
Vehicle	Model 3	v11.0(2022.4.5.1)	



```
12341802
>>00250A2330E7042A04A3039BF91204C1557A73180322108E344133
B67D201DBCA007EF77B4EBE8
<<00072205120308E704
<<00041a021802
>>00210A1F30E8042A04A3039BF9120236712210C9056494C677BD9
DE90BD959C568161E
<<00072205120308E804
<<001C1A1A12160A148A39B3ADCCED4DFA817B91EDEA8DD6810433
12341802
>>00250A2330E9042A04A3039BF9120439DAC721180322104E772F2E
6B6E7E0C3CC6A1B385EF31AE
<<00072205120308E904
<<00041a021802
```

- It happens silently in the background and out of awareness of the car owner.

Kun Jiang et al. | “Access Your Tesla without Your Awareness: Compromising Keyless Entry System of Model 3” | NDSS 2023

Countermeasures

◆ PIN to Drive

- It is worth noting that this feature disobeys the intention of PKES
- It is not the default setting of Model 3

◆ Refresh the Token *G* Frequently

- To a certain degree, refreshing the token fast enough will reduce the attack window

◆ Enable BLE link layer encryption

- Enabling BLE encryption will improve the difficulty of analysis and device spoofing
- However, it is circumvented by NCC Group, as mentioned in previous related works

◆ TOF based secure ranging（UWB）

- The PKES system can employ the Time of Flight (TOF) to avoid MitM or Relay attacks

Disclosure

◆ Dec. 2021	Begin the Project.
◆ Mar. 2022	Inform Vulnerabilities To Tesla
◆ Aug. 2022	CVE-2022-37709
◆ Other disclosure	https://github.com/fmsh-seclab/TesMla

Thanks

We thank the anonymous reviewers for their constructive and helpful comments and feedback

Thank Sultan Qasim Khan from the NCC Group for sharing their contributions to BLE Sniffle Relay

Contacts

Jiang Kun jiangkun@fmsh.com.cn Xie Xinyi xiexinyi@fmsg.com.cn

Questions?