車聯網的攻擊手法策略與威脅現況分享

Paul Fan

關於講者

Paul Fan (范紀鍠)

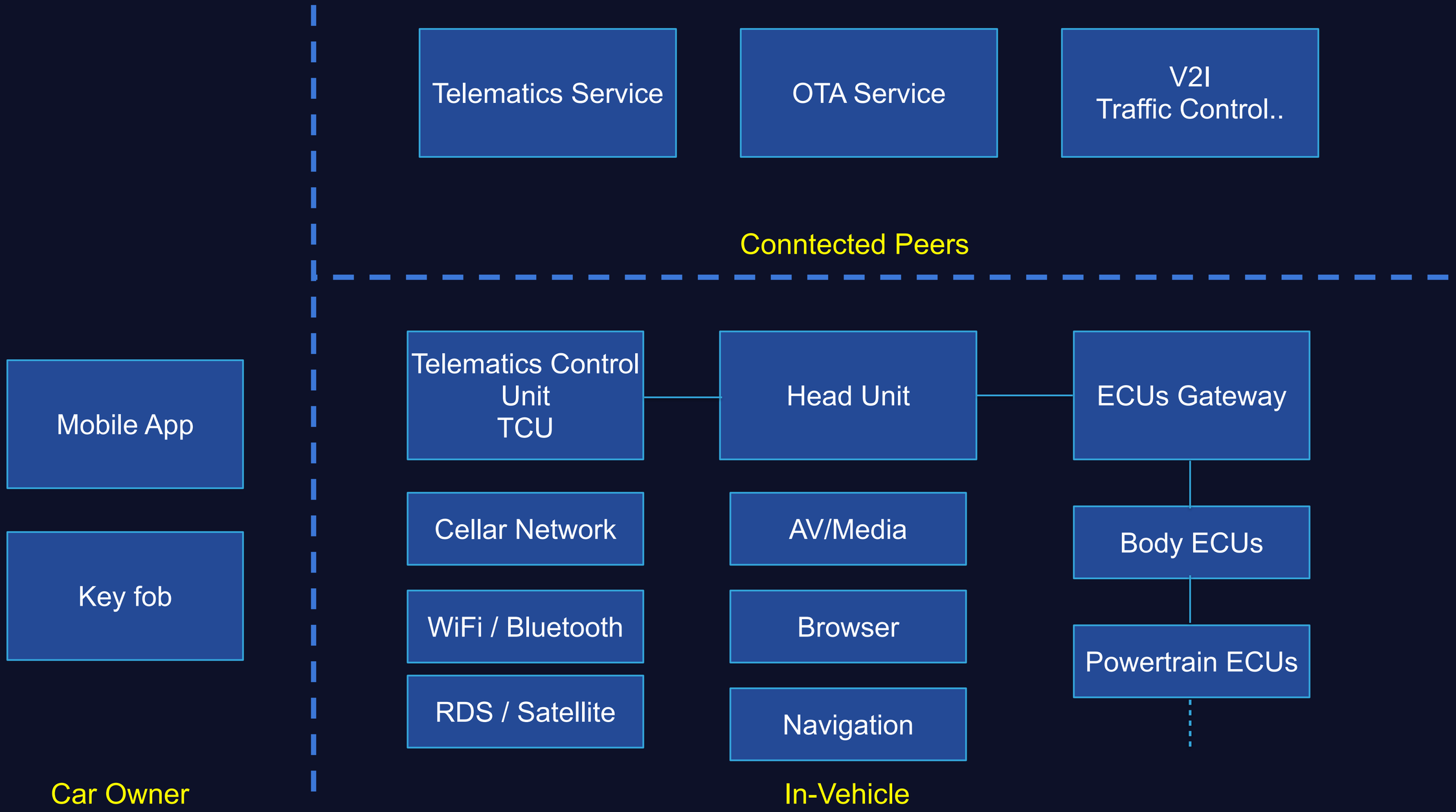
CYBAVO 共同創辦人暨執行長

曾任奇虎360安全衛士和國際化產品集團總經理

曾任趨勢科技核心技術部門 資深研發經理

從事安全產業18年擅長將安全解決方案產品化，具有大規模數億用戶安全營運能力，對於Windows Malware / APT攻擊 / 區塊鏈安全 / 車聯網安全都有涉入研究

車聯網架構


Telematics Service
OTA Service
V2I
Traffic Control..
Conntected Peers
Mobile App
Key fob
Telematics Control Unit
TCU
Head Unit
ECUs Gateway
Cellar Network
AV/Media
Body ECUs
WiFi / Bluetooth
Browser
Powertrain ECUs
RDS / Satellite
Navigation
Car Owner
In-Vehicle

車聯網攻擊案例 1

車款: Tesla Model S

公布時間: 2014

漏洞發現者: 360

攻擊效果: 遠端開啟車門，控制燈光，雨刷

車聯網攻擊案例 1

攻擊方式：

- Mobile App 與 Telematic Cloud認證機制有缺失，可以進行MitM中間人攻擊
- 取得車主Mobile App assess token 並可以複製到任何一台laptop進行操作

修復方式：

Mobile App 升級 與 Telematic Cloud 修改

-

車聯網攻擊案例 2

車款: Jeep Cherokee 自由光 2014年份

公布時間: 2015

漏洞發現者: Dr. Charlie Miller / Chris Valasek

攻擊效果: 遠端控制車輛 油門, 方向盘, 煞車等

車聯網攻擊案例 2

攻擊方式：

- Uconnect同時連接到汽車的兩根總線CAN-C和CAN IHS上
- Sprint網絡允許不同的設備（包括汽車) 自由連線通信
- 開放埠6667 D-Bus
- 修改V850韌體，並透過OMAP刷新
- 逆向工程破譯CAN通訊協定

修復方式：

召回140萬台受影響車輛，進行韌體更新

-

車聯網攻擊案例 3

車款: Tesla Model S

公布時間: 2016

漏洞發現者: Keen Security Lab of Tencent

攻擊效果: 遠端控制車輛 油門, 方向盘, 煞車等

車聯網攻擊案例 3

攻擊方式：

- 偽造固定的SSID Tesla Guest，等待車輛連接
- 利用已知的Webkit 漏洞攻擊車機Browser，執行shell code
- 利用已知舊版Linux Kernel含有漏洞CVE-2013-6282，可取得Root權限
- 透過SD Card修改OTA韌體更新
- 透過UDP傳送偽造的CAN訊息

修復方式：

OTA進行韌體更新

-

車聯網攻擊案例 4

車款: Tesla Model S

公布時間: 2017

漏洞發現者: Keen Security Lab of Tencent

攻擊效果: 遠端控制車輛 油門, 方向盘, 煞車等

車聯網攻擊案例 4

攻擊方式：

- 偽造固定的SSID Tesla Guest，等待車輛連接
- 利用已知的Webkit 漏洞攻擊車機Browser，執行shell code
- 更新Linux後依然存在另一個漏洞，可進行提權，關閉AppArmor
- SD Card依然未保護，韌體已進行簽章驗證，但檔案系統FatFS r0.09存在漏洞，可略過簽章驗證

修復方式：

OTA進行韌體更新

車聯網攻擊案例 5

車款: BMW

公布時間: 2017

漏洞發現者: Keen Security Lab of Tencent

攻擊效果: 遠端控制車輛解鎖，取得車輛內相關個人資訊

車聯網攻擊案例 5

第一種攻擊方式：

- ConnectedDrive Service透過2G或3G使用HTTP連上後台，駭客架設偽基站攔截所有訊息
- 透過仿造的設定檔使ConnectedDrive Service連到假的新聞URL
- 因使用有漏洞的WebKit使駭客可透過TOCTOU提權
- 透過Qnet登入沒有認證設定的Head Unit - Jacinto

第二種攻擊方式：

- NGTP允許透過SMS喚醒汽車進行更新設定檔
- 透過偽基站傳送假設定檔，並造成校驗簽章時的緩存溢位漏洞
- 經由TCB傳送假的UDS訊息

修復方式：

OTA升級行動網路的設定檔，軟體更新部分則由車廠維修體系執行

車聯網攻擊案例 6

車款: Mercedes-Benz E Class

公布時間: 2020 (2019 security fixed)

漏洞發現者: 360

攻擊效果: 遠端解鎖車門, 燈光控制, 天窗控制

車聯網攻擊案例 6

攻擊方式：

- HERMES (TCU) Jailbreak
  - Dump NAND file，進行逆向工程
  - No Secure Boot，放入後門與透過Debug shell修改系統服務
- 憑證管理服務不當儲存PKCS#12客戶端憑證、加密的密碼、CA憑證
  - libimp_broadband_common.so 有加解密函式
  - 固定的 (hardcode) AES256 Key
- Head Unit的browser有SSRF漏洞

修復方式：

修復雲端憑證管理服務，軟體更新部分則由車廠維修體系執行

車聯網攻擊案例 7

車款: Tesla Model X

公布時間: 2020/12

漏洞發現者: COSIC

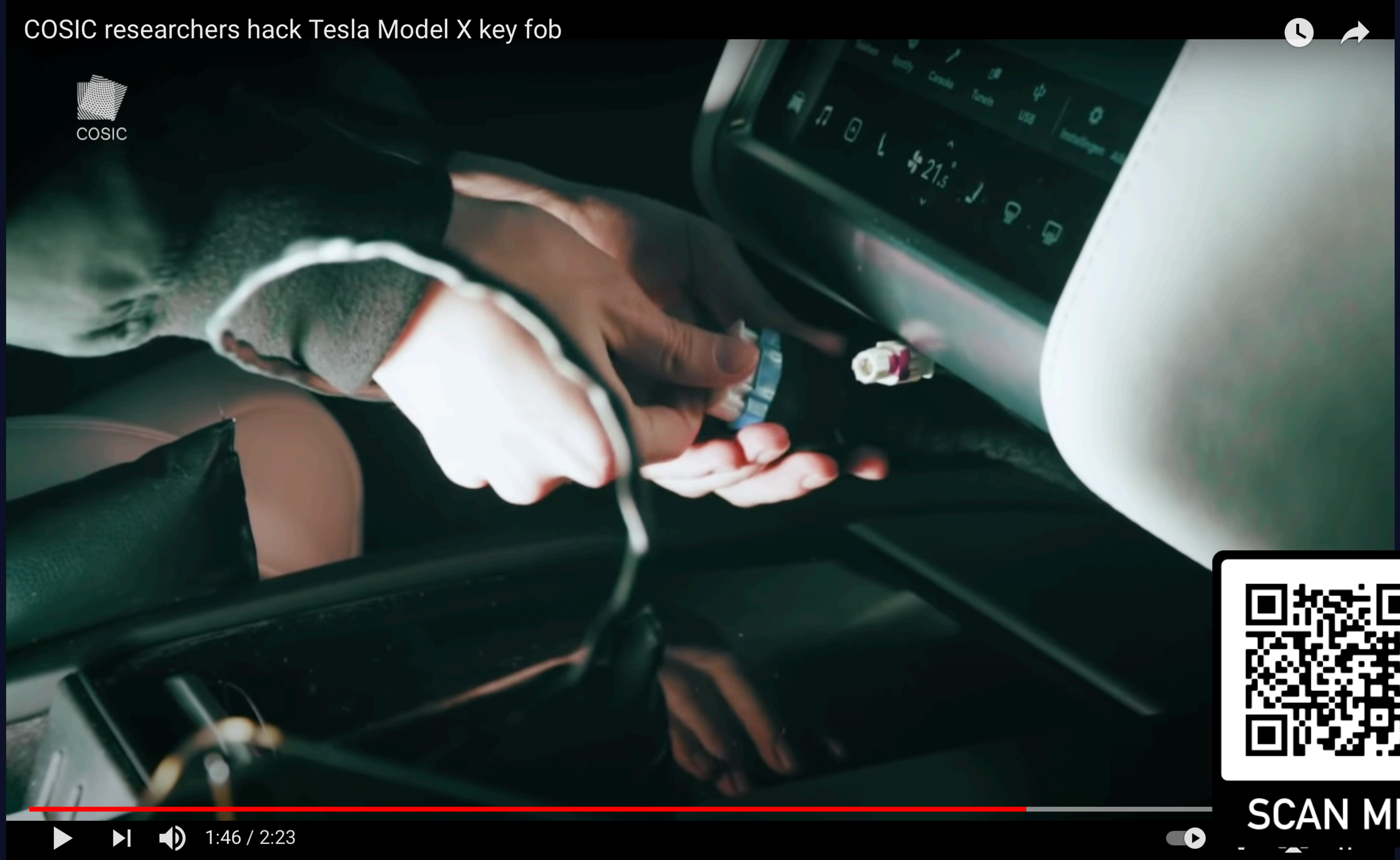
攻擊效果: 近距離非接觸式 keyless 複製取的車輛完整操作

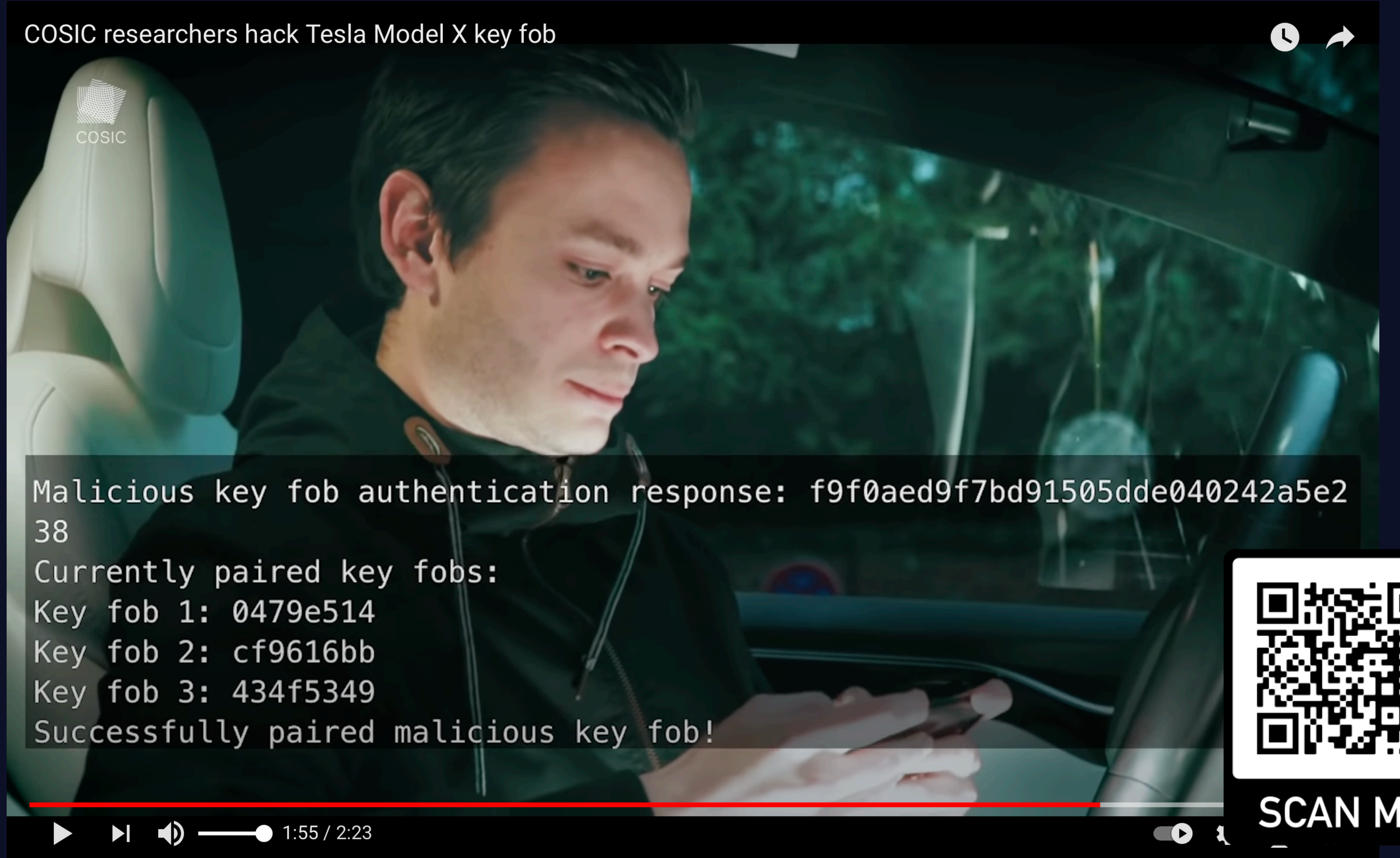
- Video: https://youtu.be/watch?v=clrNuBb3myE


COSIC researchers hack Tesla Model X key fob
COSIC
pi@raspberrypi:~/poc/src $ sudo python3 stage1.py
0:25 / 2:23
SCAN ME


COSIC researchers hack Tesla Model X key fob
COSIC
Connected to target key fob!
APPGITHASH 3e6a8d57a904a9e9
BLGITHASH 11278d0ba0ff3690
LFVERSION 0102000301020000
HARDWAREID CC2541_TESLA_REVD
Pushing malicious firmware to the target key fob...
18%| | 1399/7954 [00:18<01:29, 73.
0:45 / 2:23
SCAN ME


COSIC researchers hack Tesla Model X key fob
COSIC
Open Trunk: 6d1290edc24d2ba49edd51001fbd566f
Lock all: 0a442a25759aabd38590d57d37b60312
Ready to unlock the target car...
Unlocking doors
Opening left falcon
1:26 / 2:23
SCAN ME

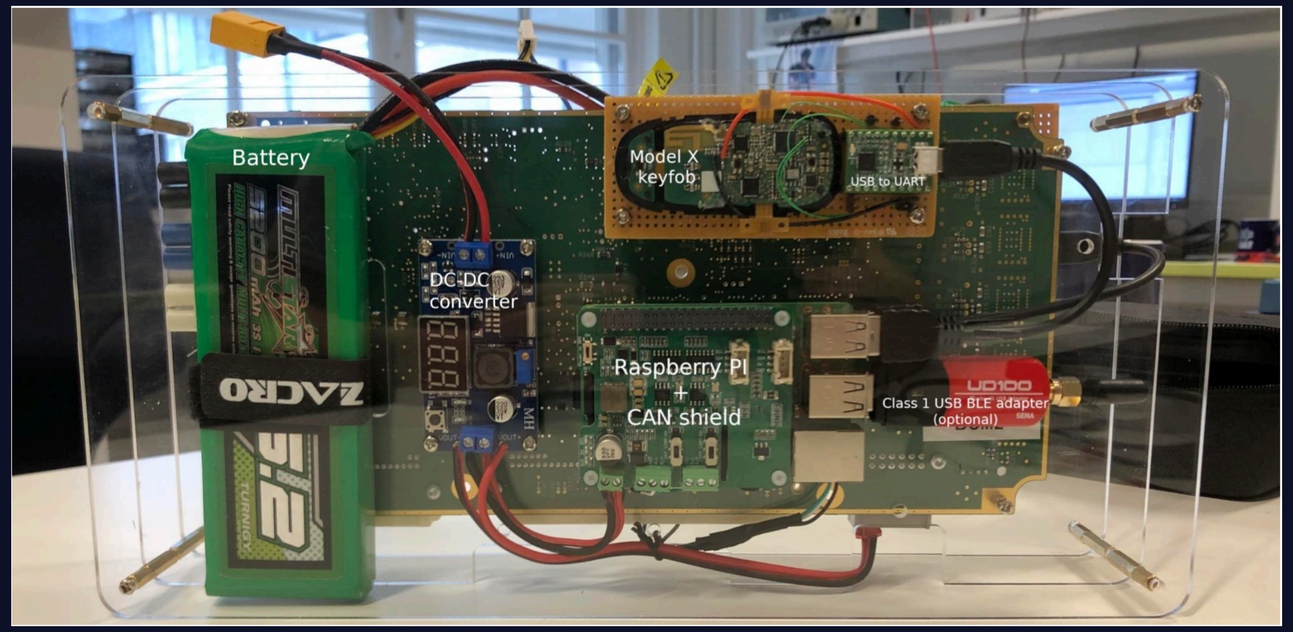

COSIC researchers hack Tesla Model X key fob
COSIC
SCAN ME
1:46 / 2:23


COSIC researchers hack Tesla Model X key fob
COSIC
Malicious key fob authentication response: f9f0aed9f7bd91505dde040242a5e2
38
Currently paired key fobs:
Key fob 1: 0479e514
Key fob 2: cf9616bb
Key fob 3: 434f5349
Successfully paired malicious key fob!
1:55 / 2:23
SCAN ME

車聯網攻擊案例 7

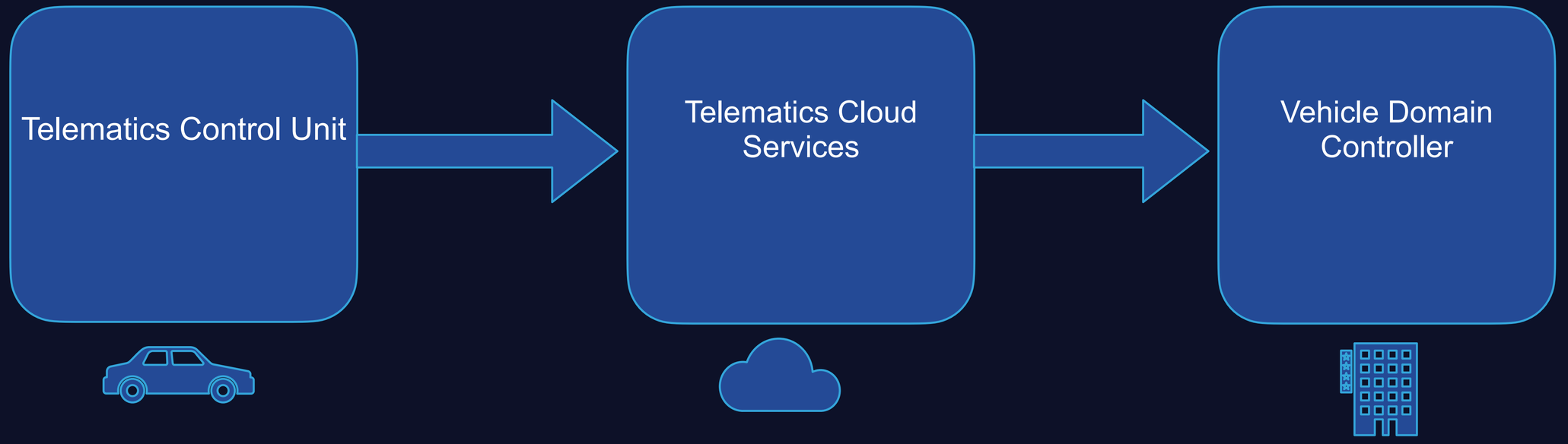
攻擊方式：

- 駭客透過eBay購買的BCM，並設定目標車輛的識別碼(VIN)
- 喚醒key fob更新惡意的韌體，取得一次性unlock assess code
- 透過一次性的unlock access code解鎖車子
- 進入車內，連接上OBD，利用洩漏的Toolbox工具將偽造的key fob與車配對



從TCU拿下整個車廠Domain Admin

- TCU內的eSIM APN/VPN 配置不當
- 黑客模擬TCU 與VPN access token 連接上車廠Telematics服務
- 對外上線服務網路與公司網路互通



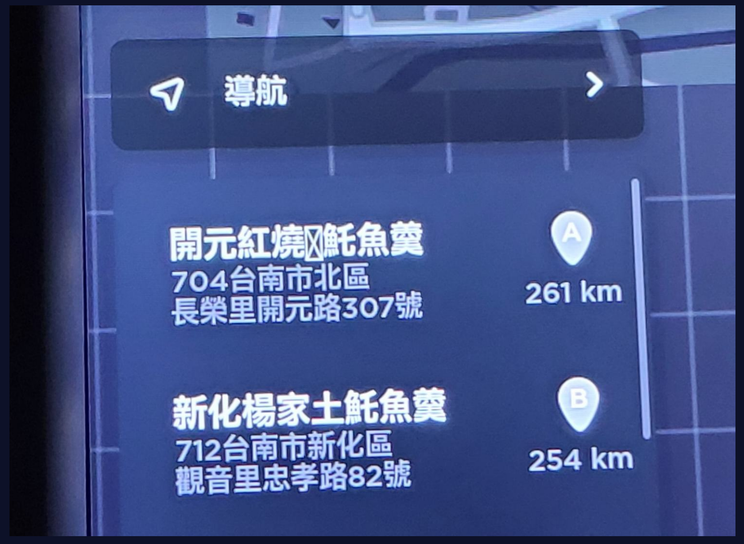
安全問題? 開元路魡魤魚羹

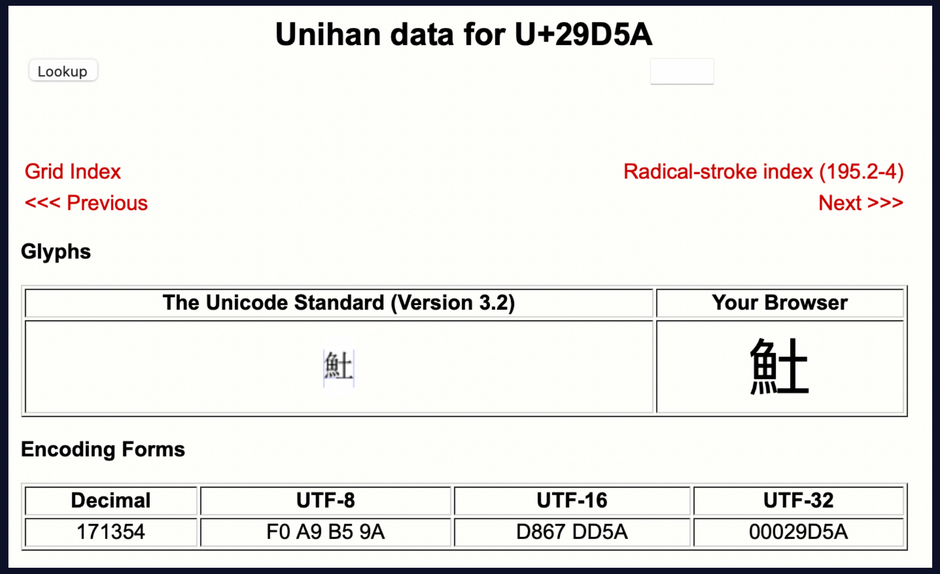
車款: Tesla Model S / X / 3 全車系

發現時間: 2021/02

問題: 中控導航地圖顯示有關"魡魤魚羹"，則黑屏系統重啟。不影響行車/動力系統。

-





Unihan data for U+29D5A

Lookup

Grid Index
<<< Previous

Radical-stroke index (195.2-4)
Next >>>

Glyphs

The Unicode Standard (Version 3.2)	Your Browser
魡	魡

Encoding Forms

Decimal	UTF-8	UTF-16	UTF-32
171354	F0 A9 B5 9A	D867 DD5A	00029D5A

安全設計盲點

Identifier (VIN / IMEI..) != Credential != Access Token

固定(hardcore)對稱式密鑰 (DES, AES128/256…) 等於 沒有密鑰

Integrity Check (完整性效驗) 比你想像中的難

Linux Kernel 版本過舊，關鍵3rd party library版本過舊

-

車廠的安全建議

開放心態，透明負責任態度處理安全危機事件

單一安全通報窗口與內部協作機制 (決策者 / 研發部門 / 營運部門 / 公關部門)

漏洞提報獎勵機制 (Security Bug Bounty Program)

內外部對產品與服務定期的測透測試 / Red-team 紅隊攻防演練

供應鏈的產品安全評估/安全響應能力要求

-

Q & A

謝謝聆聽

paul@cybavo.com