



オフエンシブ自動車セキュリティ ティ・カーハッキングケーススタ ディー

KAMEL GHALI

CAR HACKING VILLAGE



\$whoami < Mohammad Kamel Ghali

- ❖ Security Delivery Manager - Accenture
- ❖ ASRG Japan Lead
- ❖ Car Hacking Village Vice President
- ❖ Bsides Tokyo Organizer
- ❖ Car Hacking Trainer
- ❖ Hobbies: Cooking, Pokemon, Anime
- ❖ Learning: Mobile App Development



***All opinions expressed in this presentation are my own and in no way reflect the views or opinions of my employer, Car Hacking Village, or any other entity or organization**





カーハッキングビレージとは？

Hands-on Car Hacking



Car Hacking CTF



カーハッキングビレージとは？

Educational Workshops



Live Car Hacking Demos





Agenda

- ❖ 自動車サイバーセキュリティとカーハッキングの概要
 - ❖ カーハッキング一覧
 - ❖ カーハッキングの特徴
- ❖ 車って、本当にハッキングされたりする??
- ❖ 自動車サイバーセキュリティケーススタディー
 - ❖ カーハッキング犯罪
 - ❖ カーハッキング研究



自動車サイバーセキュリティとカーハッキングの概要

車がハッキング可能ですって



現代車

CASE



Conected

車両とインターネットの接続



Autonomous
Automated

自動運転技術



Shared

カーシェアリング



Electric

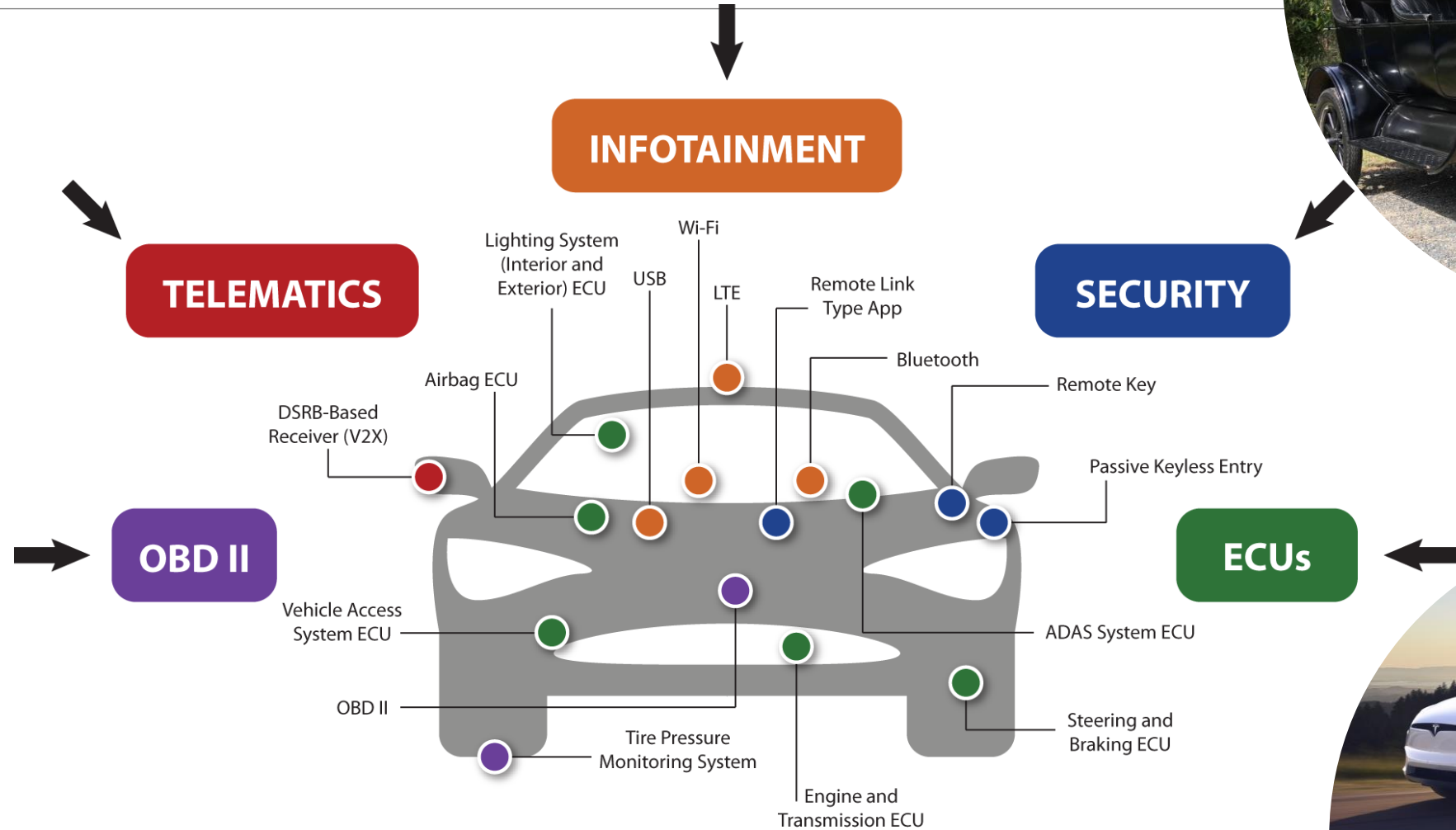
電気自動車の普及

Source: NEC Solutions





現代車





カーハッキングー覧

攻撃方法が多すぎ
学ぶことが多すぎ



カーハッキング一覧

The Car Hacking Kill Chain (Simplified)

STEP 1. 侵入

Wireless Networks

Physical Access

STEP 2. コントロール

Reflash ECUs

Exploit Vulnerabilities

STEP 3. 車の操作

Ransomware

Impact Operation



カーハッキングー覧

STEP 1.
侵入

INFOTAINMENT

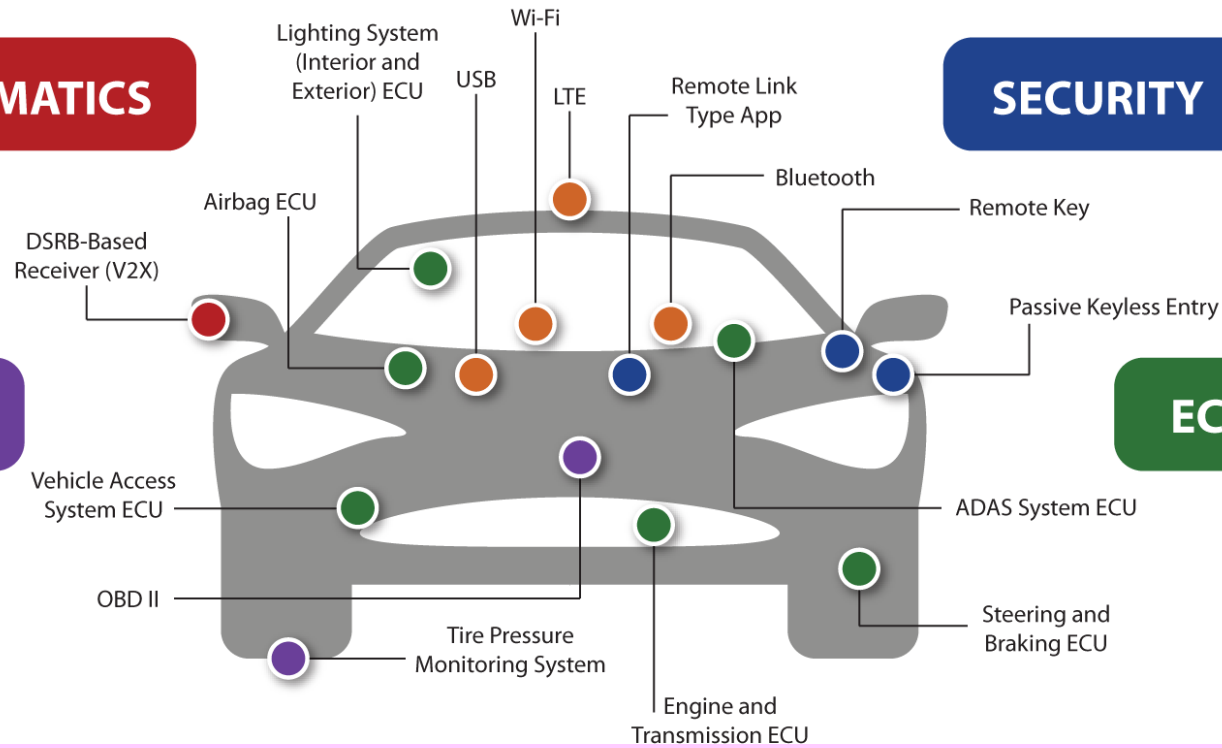
TELEMATICS

SECURITY

OBD II

ECUs

STEP 2.
コントロール



カーハッキングー覧

**2014
Jeep Hack**

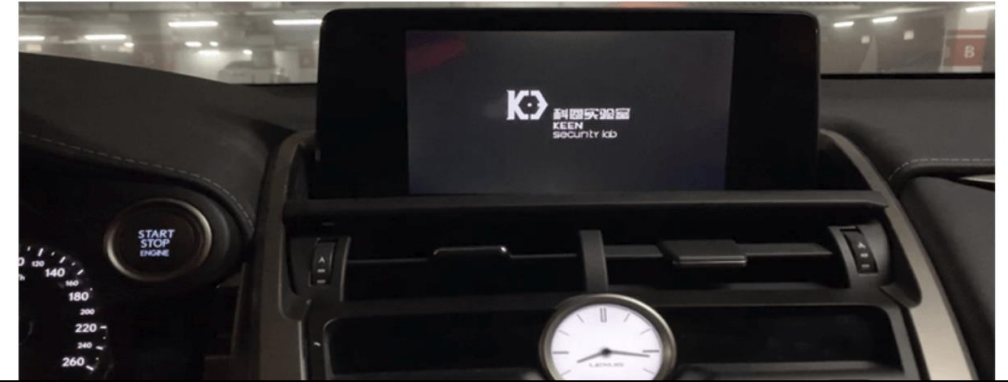
**STEP 3.
車の操作**

**2020
Lexus Hack**



Tencent Keen Security Lab: Experimental Security Assessment on Lexus Cars

by Tencent Keen Security Lab



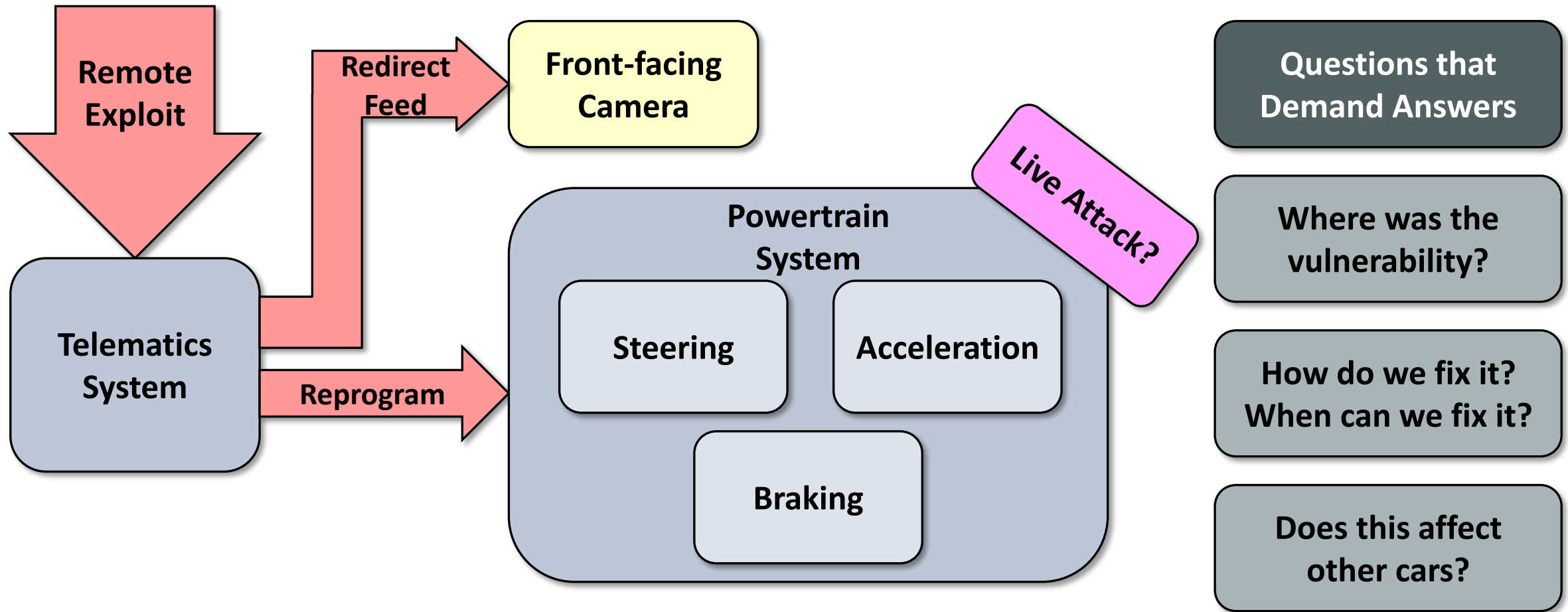


フェイク事例

- ❖ メディアでは「カーハッキング」はどんな感じだろう？
- ❖ Credit: Designated Survivor



フェイク事例





車って、本当にハッキング ングされたりする??

YES!

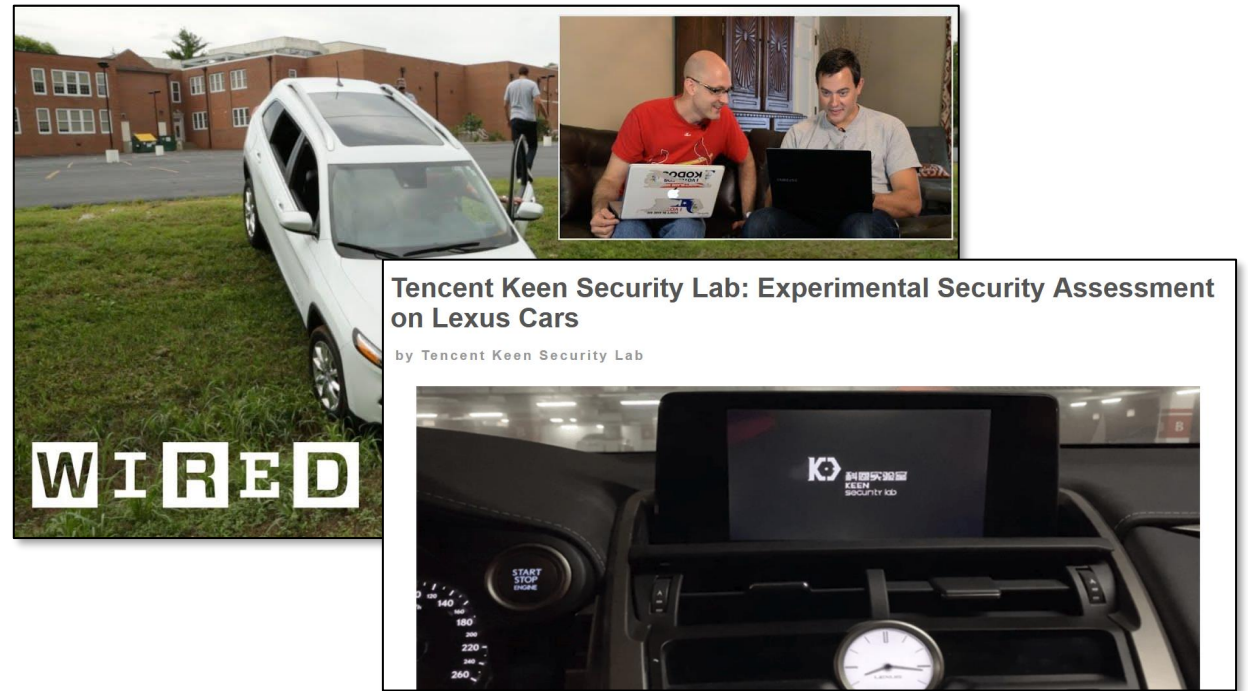


実際のカーハッキング

犯罪者



研究者



犯罪者のモチベーション

カーハッキングでどうやって簡単にお金稼ぐ、、？

犯罪者

車の Ransomwareはむずかしそう、、

やっぱり盗難だね、、



研究者のモチベーション

研究者

この車のソフト、なんか古くない？脆弱性あるのかな、、

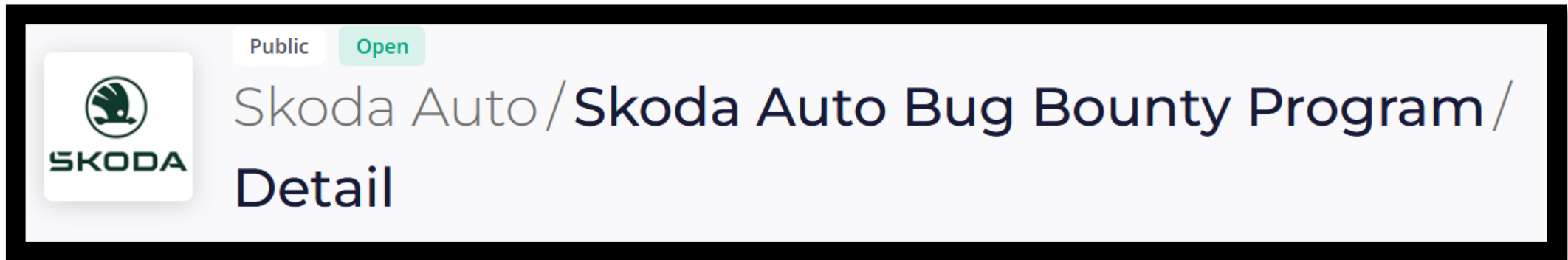


Tencent Keen
on Lexus Ca
by Tencent Keen S

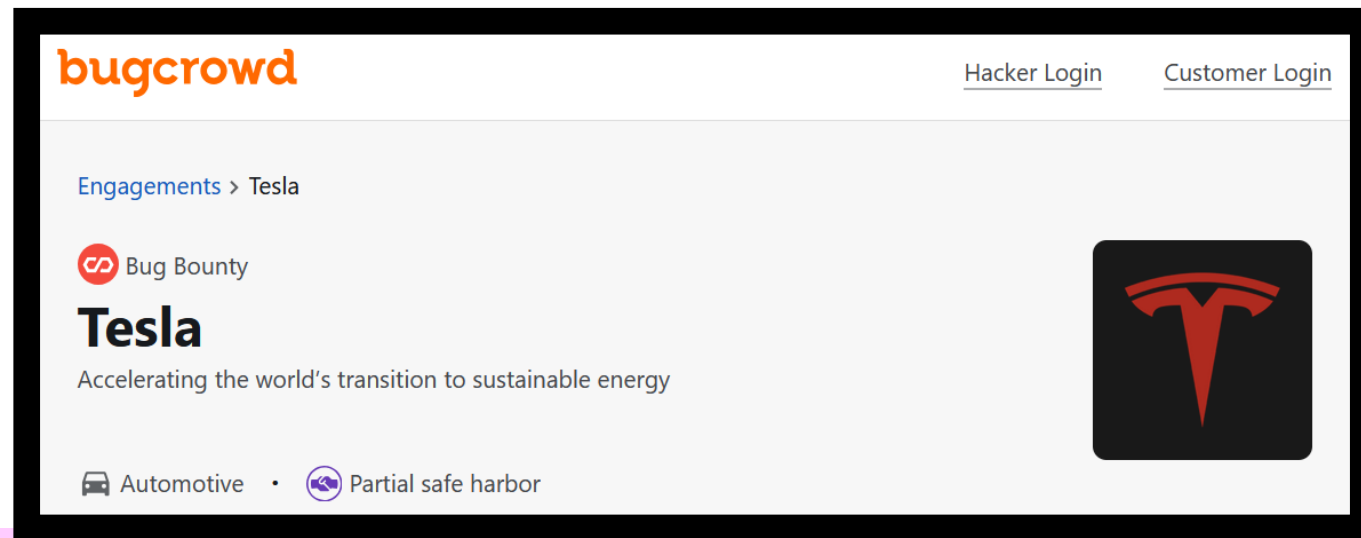
ありました！！メーカーのバグバウンティプログラムに提出しよう！

バグバウンティプログラムなんかないですよ、、DEFCONで発表しようっか？

カーハッキング/バグ/バウンティ



<https://app.intigriti.com/programs/skodaauto/skodaautopivatebugbountyprogram>



<https://bugcrowd.com/engagements/tesla>



カーハッキング/バグ/バウンティ



Pwn2Own Automotive 2025: January 22-24 2025 – Tokyo, Japan

<https://vicone.com/jp/pwn2own-automotive>





カーハッキングケース スタディ

本当のカーハッキング事件をいくつか分析しよう



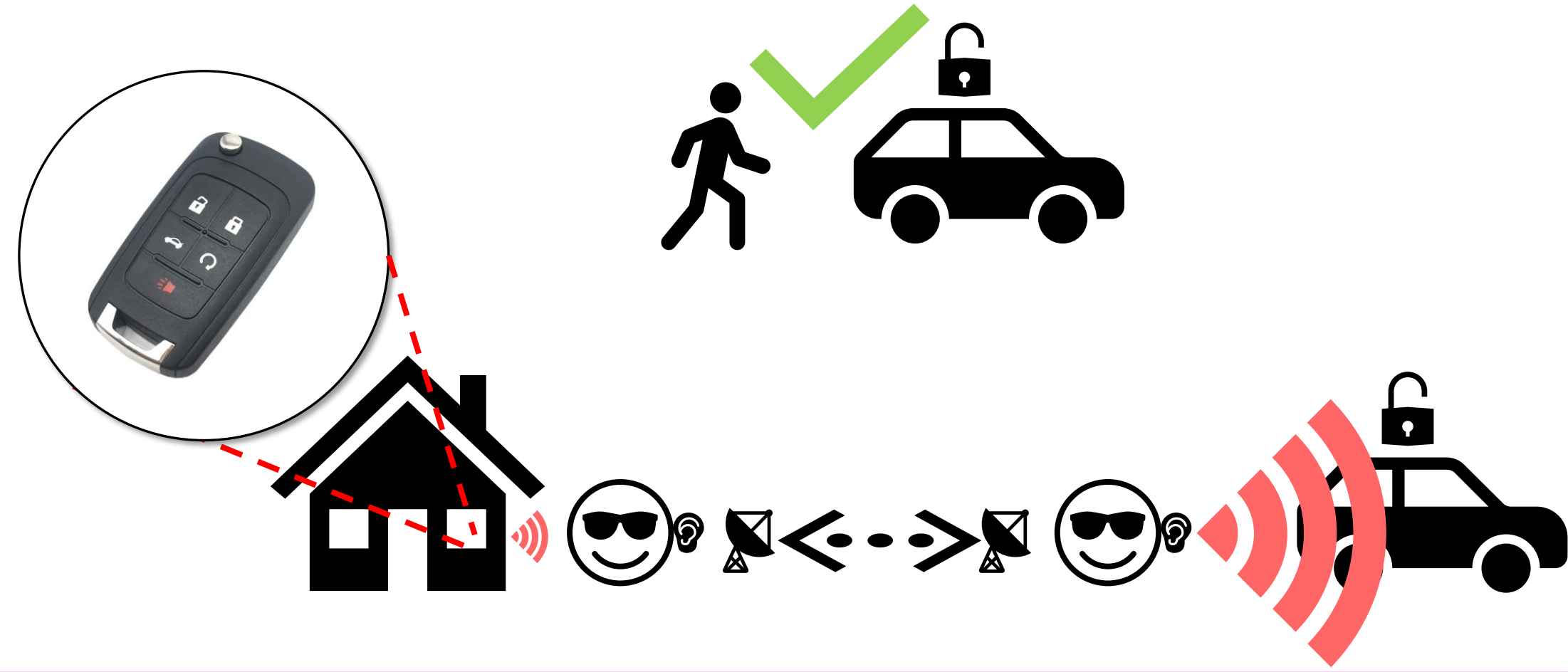


ケーススタディー:リレーアタック





ケーススタディー:リレーアタック



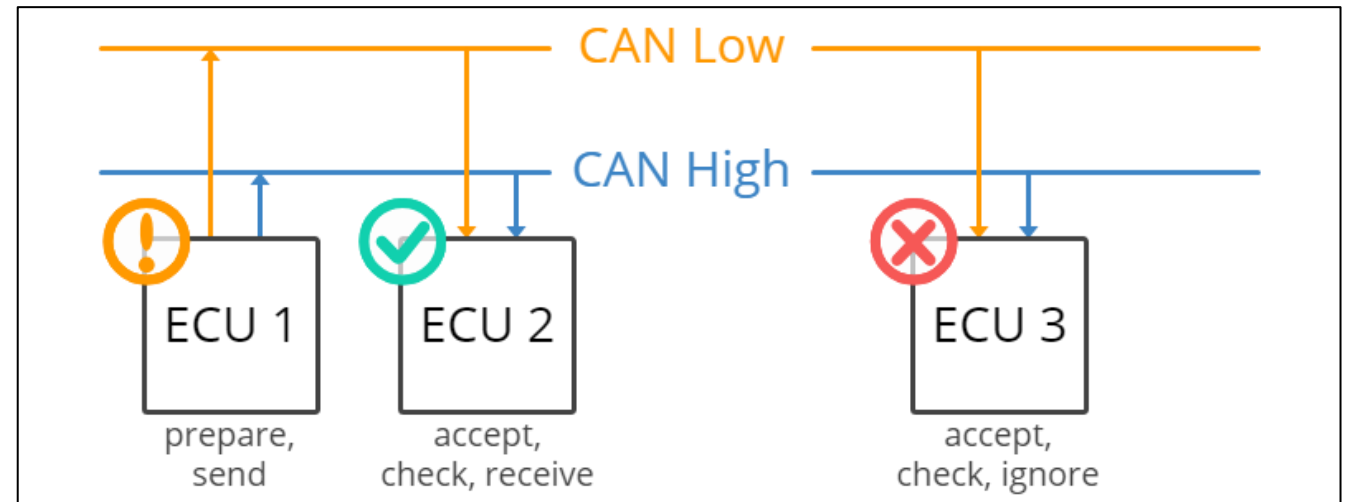


ケーススタディー: CAN インベーター

❖ Credit: Tokyo MX

ケーススタディ：CAN インベーター

- ❖ CAN Bus
 - ❖ In-vehicle Network
 - ❖ Safety-critical Applications
 - ❖ Diagnostics/Reprogramming



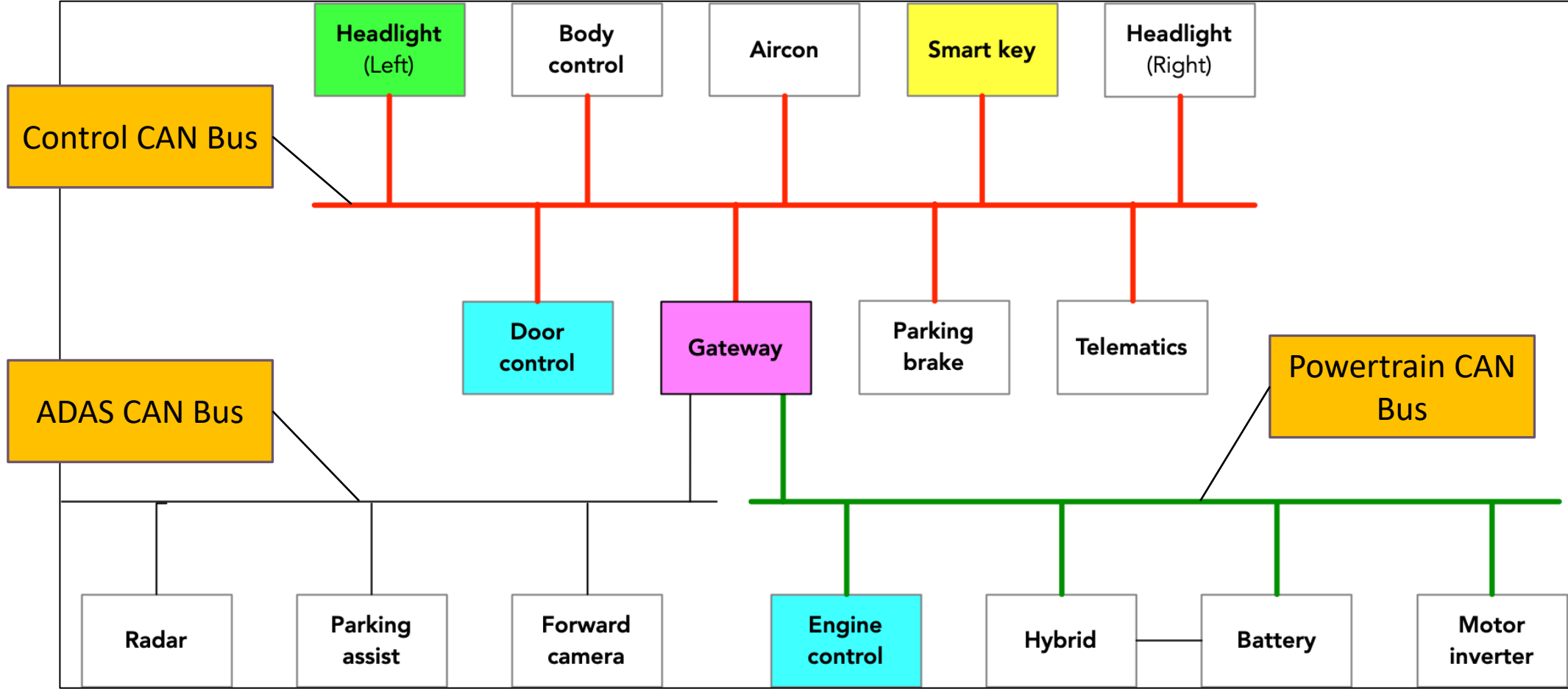
ケーススタディ: CAN インベダー

- ❖ CAN Injection
 - ❖ (AKA CAN Invader)
 - ❖ 被害者は世界中にいる
 - ❖ Ian Tabor (CHVボランティア、僕のともだち)
- ❖ 車へのダメージ、、
 - ❖ Front Bumper
 - ❖ Headlights
 - ❖ ...Gone!



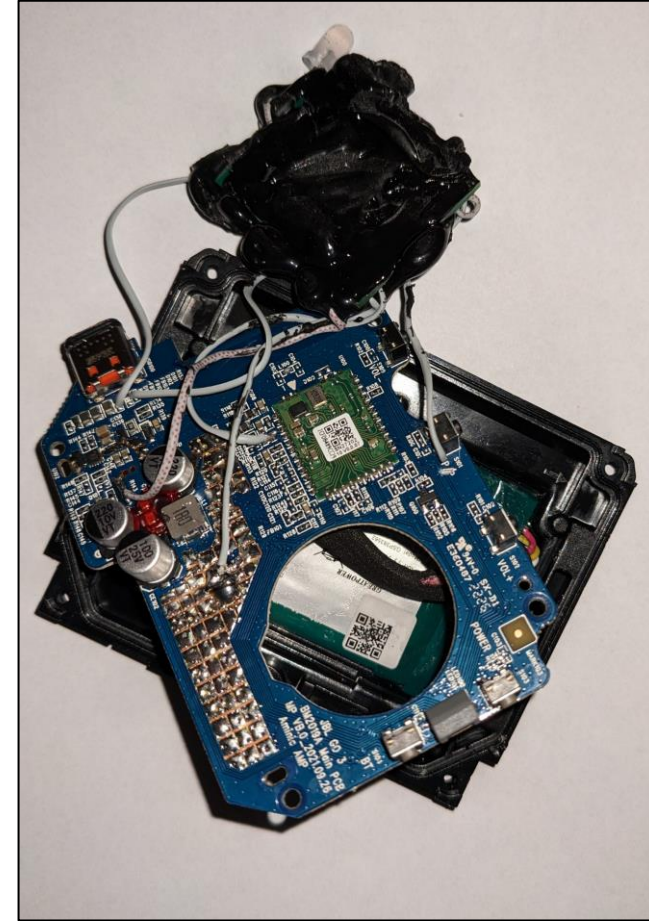


ケーススタディ：CAN インベーター





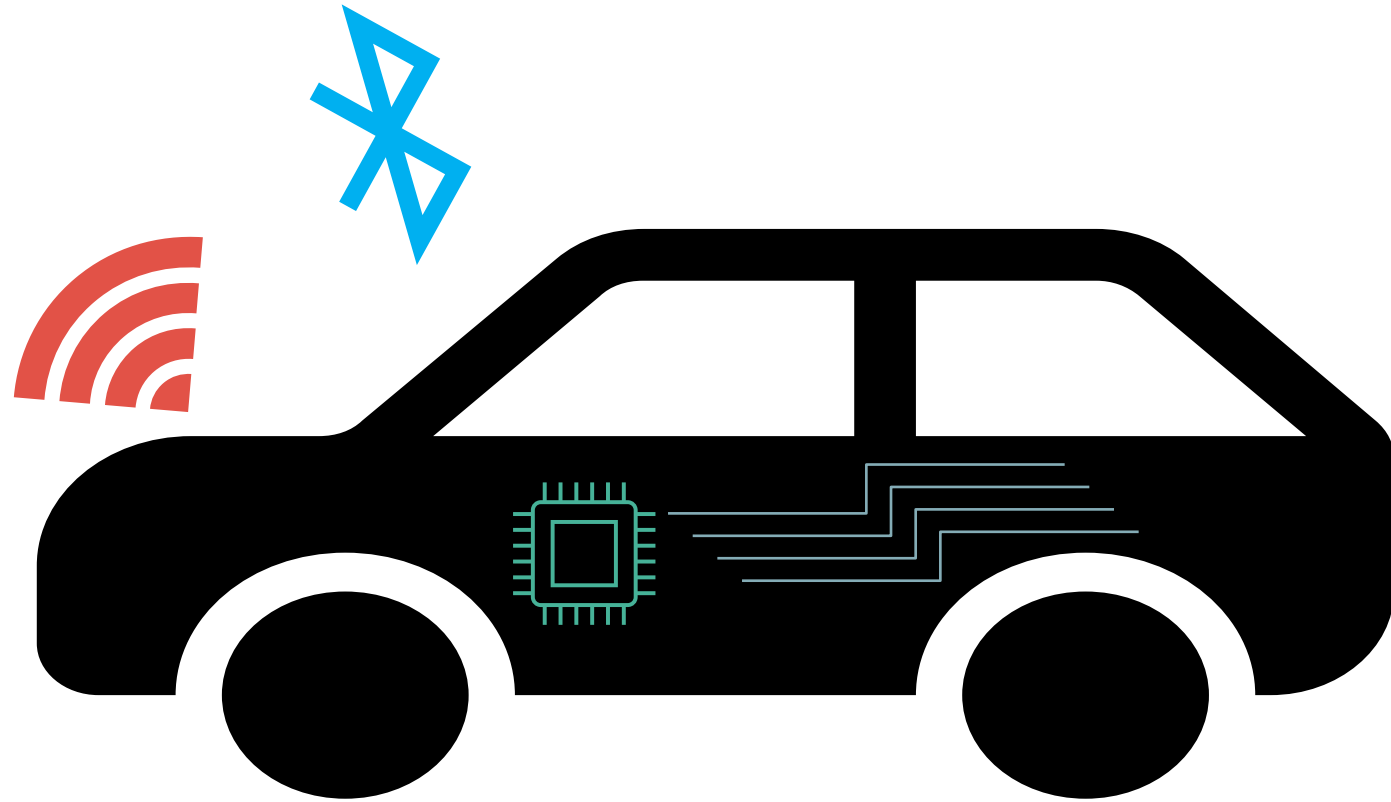
ケーススタディー: CAN インベーター





ケーススタディー: 2020 Lexus Hack

- ❖ Keen Labsによる発見
- ❖ BlueBorne という Bluetooth 脆弱性
 - High Privilege RCE on Main IVI Board
- ❖ Wi-Fi によるバックドア構築
- ❖ ファームウェア認証なし
- ❖ CAN Bus通信ゲット





Thank You! Questions?



**Want to Volunteer? Join the Car
Hacking Village Mailing List!**



Kamel Ghali

Learner | Car Hacker | Chef | Speaker

