KEEPING UP WITH MODERN AUTOMOTIVE EXPLOITATION

SPEAKER: KAMEL GHALI

ROOTCON 15

*Disclaimer: All views represented in this presentation are my own and do not represent my employer or any other third party

SPEAKER INTRODUCTION

- "Automotive Cybersecurity Technology Architect" at White Motion
  - Subsidiary of Marelli (Big Italian Automotive Supplier)
  - Based in Tokyo
- Trilingual Car Hacking Enthusiast
  - English, Arabic, and Japanese
  - Ex-Admin of ASRG Detroit
  - Founder of ASRG Japan (haven't done much yet though)
- Jack of ~~all~~ some trades, master of none
- Recent areas of interest:
  - Bluetooth
  - USB
  - RF
  - Digital Forensics
- Hobbies include fighting games, cooking, playing the ukulele, and getting lost

OBJECTIVES OF THIS TALK

- Automotive Cybersecurity in 2021
  - We'll start with an intro
- Case Studies of Recent Significant Disclosures
  - Lexus Bluetooth Hack (2020)
  - Tesla Bluetooth Hack (2020)
  - Tesla Drone Hack (2021)
  - What do they have in common?
- IoT Security
- Product Vulnerability Management

AUTOMOTIVE SECURITY IN 2021

- Rapidly Growing Industry
  - Thanks to Chris and Charlie
- Public Safety
  - Contrast to traditional IT security
- Little Regulation
  - Governments and standardization bodies are catching up
  - ISO 21434, UN ECE WP29
- Shortage of Professionals
  - Please help
- Massive Supply Chain

AUTOMOTIVE SECURITY IN 2021

- Development Process Integration
  - OEMs and Suppliers are still incorporating security
  - Policies and best practice are widely still under development
- Industry Groups Encouraging Collaboration
  - AUTO-ISAC, J-AUTO-ISAC, ASRG

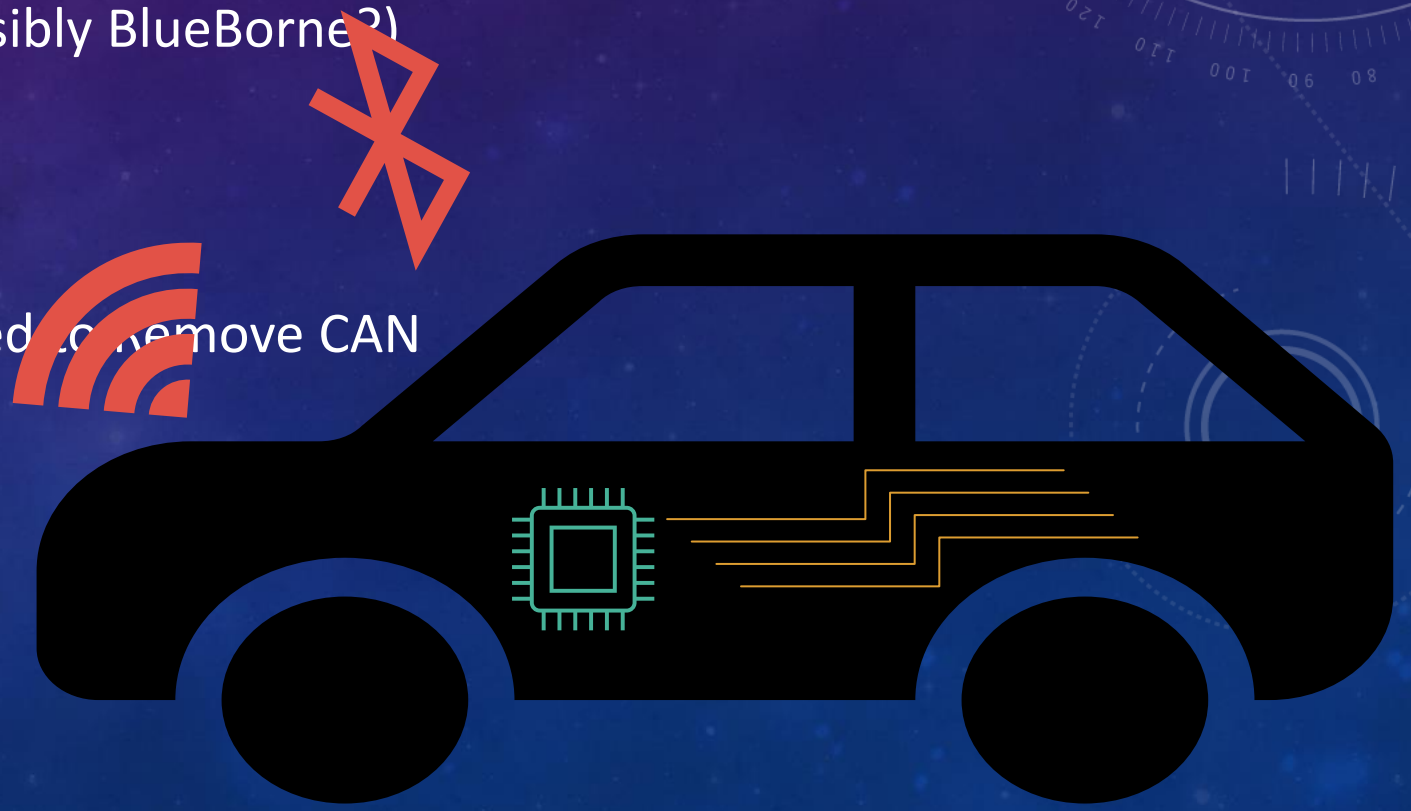
RECENT AUTOMOTIVE SECURITY CASE STUDIES

DISCLAIMER:

WHILE I AM NOT DIRECTLY RELATED TO THE FOLLOWING PIECES OF RESEARCH, I BELIEVE THEY ARE VALUABLE SOURCES OF INFORMATION FOR ANYONE LEARNING MORE ON THIS TOPIC. CREDITS IN THE END.

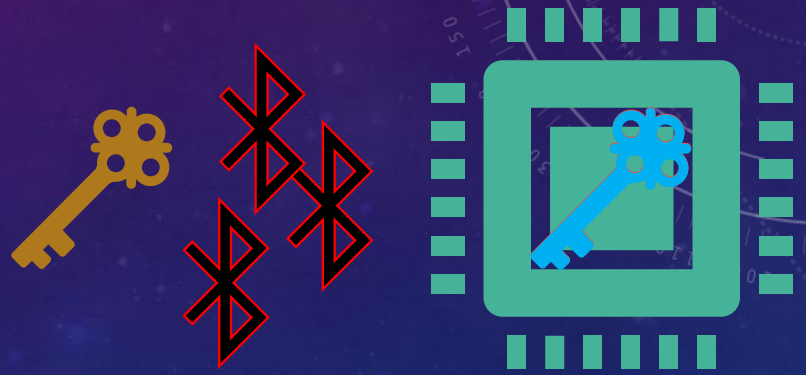
SHORT CASE STUDY 1: LEXUS BLUETOOTH HACK – MARCH 2020

- Disclosed by Tencent Keen Labs in March of 2020
- Undisclosed Bluetooth Vulnerability (Possibly BlueBorne?) Granted RCE
- High Privilege RCE on Main IVI Board
- Wi-Fi Based Backdoor Established
- Lack of Firmware Signature Checks Abused to Remove CAN Messaging Filters
- Arbitrary CAN Bus Transmission Granted

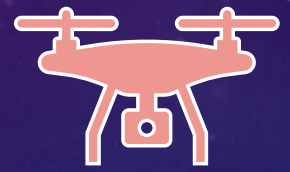


SHORT CASE STUDY 2: TESLA KEY FOB HACK – NOVEMBER 2020

- Disclosed by Lennert Wouters of KU Leuvan University in Belgium
- Unsigned Key Fob Updates Delivered via Bluetooth from BCM
- VIN Only Input Needed to Authenticate
- Car Unlock Signal Retrieved From Newly Flashed Key Fob
- Lack of Certificate Check Between Vehicle BCM and Forged Key Fob Enabled Full Pairing
- Vehicle Controls Unlocked
- Vroom Vroom



SHORT CASE STUDY 3: TESLA DRONE HACK (T-BONE) - 2021



- Research by Ralf-Phillip Weinmann and Benedikt Schmotzle
- Default SSID All Teslas Connect To: Tesla Service
  - At least in Europe
- ConnMan Vuln.
  - Common, Lightweight Network Manager for IoT
  - DNS, DHCP, IPv4/6
  - CVE-2021-26675
    - Network-Adjacent RCE
  - CVE-2021-26676
    - Stack Information Leakage
    - Enabled bypass of ASLR and DEP
  - Privilege Escalation on Infotainment Unit

WHAT DO THEY ALL HAVE IN COMMON?

- Close-Range Wireless Technologies
  - Bluetooth, Wi-Fi
- Lack of Signature Checks
  - Allowed re-flashing
- IoT-Centric Vulnerabilities
  - Bluetooth and ConnMan are common attack surfaces in IoT security
- Performed on Modern Vehicles
  - Especially considering Teslas and their frequent OTA updates
- Post-Production Vehicles

HOW DO WE DEAL WITH THIS IN THE FUTURE?

- Implementation of New Standards
  - Security should be implemented into the entire development process
  - Training for Engineers and Development Managers
- Comprehensive Product Vulnerability Management
  - Every OEM needs to be ready to act on new vulnerability information
  - Intake, Processing, Action

REFERENCES USED

- ISO/SAE 21434 Road Vehicles – Cybersecurity Engineering Standard
  - https://www.iso.org/standard/70918.html
- Tesla Drone Hack Paper
  - https://kunnamon.io/tbone/
- Keen Labs Lexus Research
  - https://keenlab.tencent.com/en/2020/03/30/Tencent-Keen-Security-Lab-Experimental-Security-Assessment-on-Lexus-Cars/
- Article About Tesla Fob Hack
  - https://www.wired.com/story/tesla-model-x-hack-bluetooth/

THANK YOU!

KAMEL.GHALI@WHITE-MOTION.COM