Securing Self-Driving Cars (one company at a time)

Dr. Charlie Miller, Chris Valasek

Colton Asnes

TABLE OF CONTENTS

Goal of the paper

Establish fundamental details of autonomous cars, their threat level, and security mechanisms for members of the *public* and other fields

Self-Driving Cars

01

Current State

Self-Driving Car Levels

Level 0: No automation: driver in full control; even with cruise control

Level 1: Driver assistance:ex. lane keep assistance

Level 2: Partial automation: car controls steering, acceleration, and braking; driver must keep hands on the wheel

Level 3: Conditional automation: car *can* control all elements of driving and monitors environment

Level 4: High automation: can operate without a human; ex. Self-driving fleets from uber, cruise

Level 5: Full automation: needs no human interaction at all

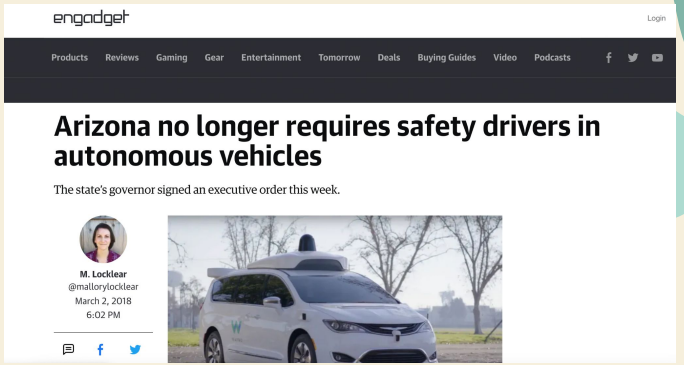
USE CASES

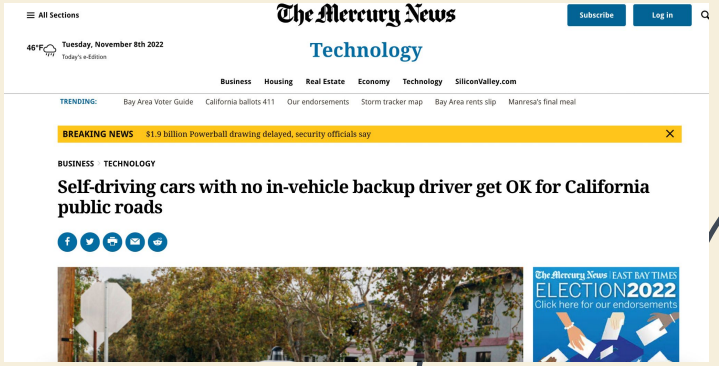
Production Vehicles

Ride-Sharing

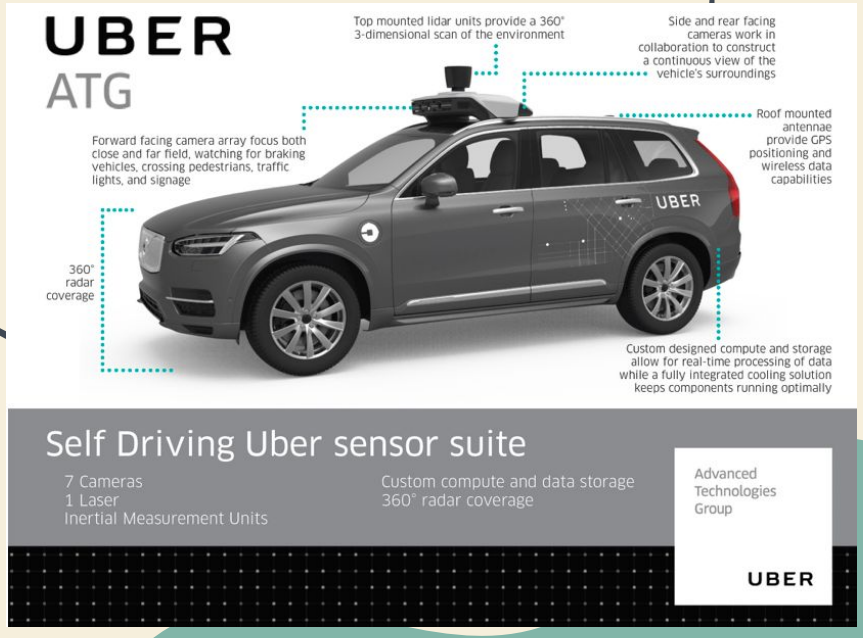
Regulations

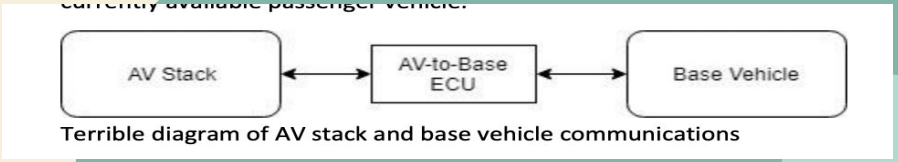
- Many places have no regulations on self-driving cars
- 2014: California required human inside self-driving cars
- Arizona (2018): no longer required safety drivers
- California followed; required ways for the vehicle to communicate with law enforcement
- Self-driving programs drive *a lot*





Level 4 AV Hardware

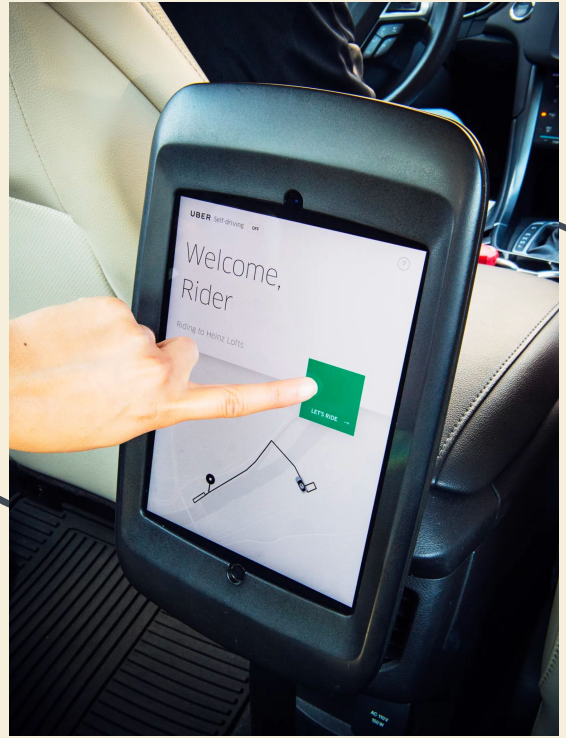




Terrible diagram of AV stack and base vehicle communications

Lidar is incredibly expensive and *not* available yet on production level vehicles

Significant computational power needed to process sensor input and actuate decisions



Level 4 AV Hardware

Using Tablets that allow passengers to interact with the vehicle

- Allow passenger to indicate a stop or destination change
- Secure module not connected to CAN

ATTACKS

2011 CHEVY MALIBU

Vulnerability in Bluetooth stack

CID old web browser

2016 Tesla Model S

2015 Jeep Cherokee

Vulnerability from Internet connection

Rogue cellular base stations

2018 BMW i3

Challenges in Securing Self-Driving Cars

01

Speed

Each company wants the biggest fleet

02

Base Vehicle

Need to secure the AV system and base vehicle

03

Ethernet

Non-standard TCP stacks

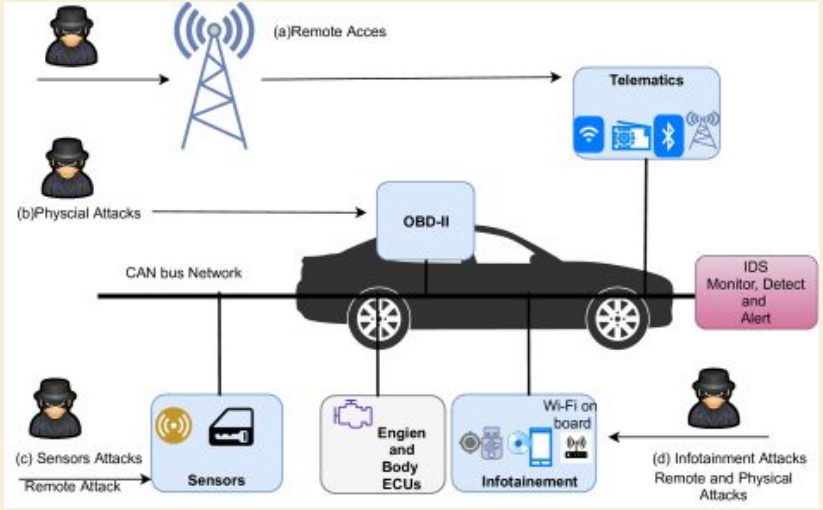
Threat Model

Long Distance (Remote Attacks):

- Can affect multiple vehicles at once
  - Listening service in the communications module
  - Remote assistance style feature (Phantom Auto)
  - Attack on base vehicle: telematics, infotainment, etc.
  -

Short Distance (Remote Attacks)

- Low-scale
  - Attack against Wi-Fi module
  - Attack against Bluetooth
  - Attack against TPMS
  - Jamming sensors



Threat Model

Physical Access Attacks:

Direct injection of CAN messages onto the CAN bus

- Implanting a device of OBD-ii dongle
- Reprogramming an ECU
- Access to CAN via Ethernet

Defensive Goals

Can *never* be attack proof

Primary concern is preventing passenger injury

Focus on long-distance remote attacks that are large-scale

Defenses

Trusted Execution and Bootstrapping

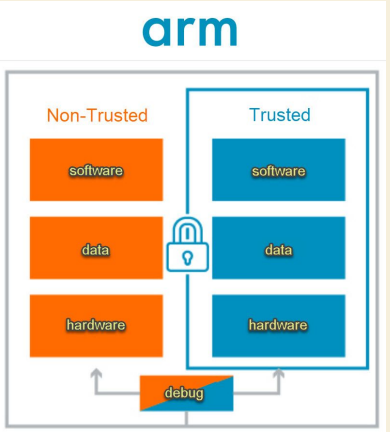
- Verify during boot up that AV code comes from manufacturer
- “Secure Boot” verifies code through trusted key in a write-protection portion of computer
- BIOS/firmware verifies bootloader -> verifies the kernel -> verifies the software image

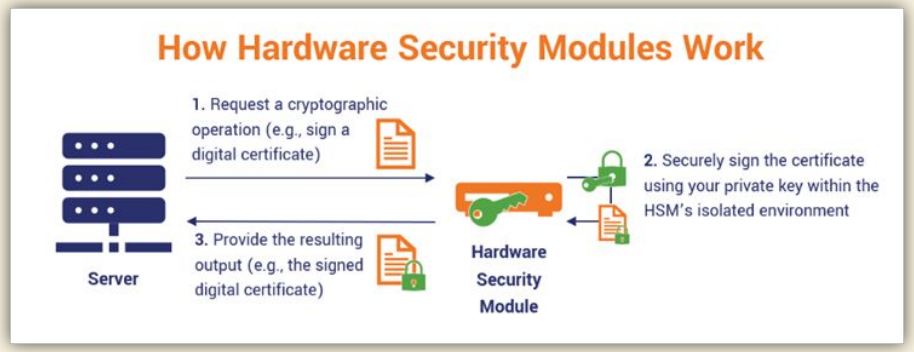
- Private key soldered into motherboard
- Force user to enter username/password to verify key from network service
- Request VIN or other identifying components from motherboard

Private Key Storage

Trusted Execution and Bootstrapping

- Keys stored in Trusted Platform Module (TMP) or stored via HSM or ARM TrustZone
- Applies for software updates as well



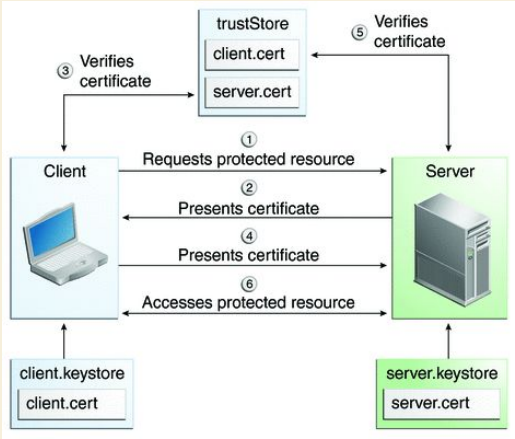


Attack Surface Reduction

- Removing Inbound Internet Connections
- Removing Bluetooth Capability
- Encryption of Data
- Separation from CAN Bus

Attack Surface Reduction

Message Signing



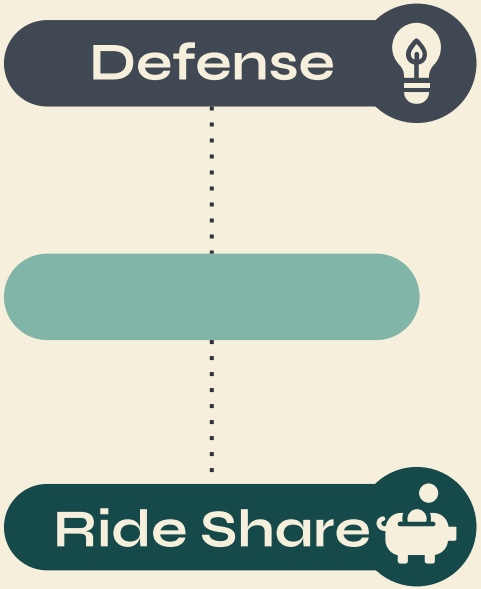
Controlling Remote Access

Threat Detection

Acceptance/Rejection

Accepted, although unprofessional process and lacked detail

Questions & Discussion



This paper focused on defending level 4 autonomous vehicles. Most consumer autonomous vehicles are level 2 or 3 and would have entertainment components. How could we defend against attacks?

Would you feel safe using level 4 autonomous ride sharing? What safety features would you be comfortable with?


slidesgo