

CS 253 Cyber Security
Automotive

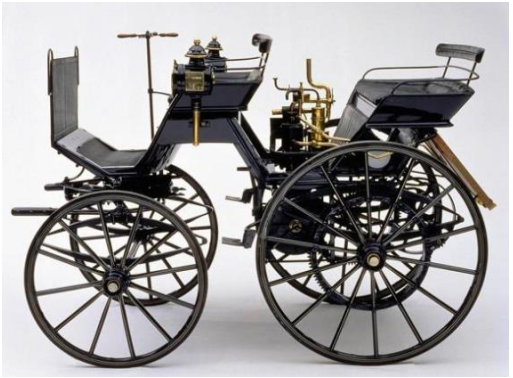
ShanghaiTech University

PART ONE

01

Automotive Security

Automobiles Security



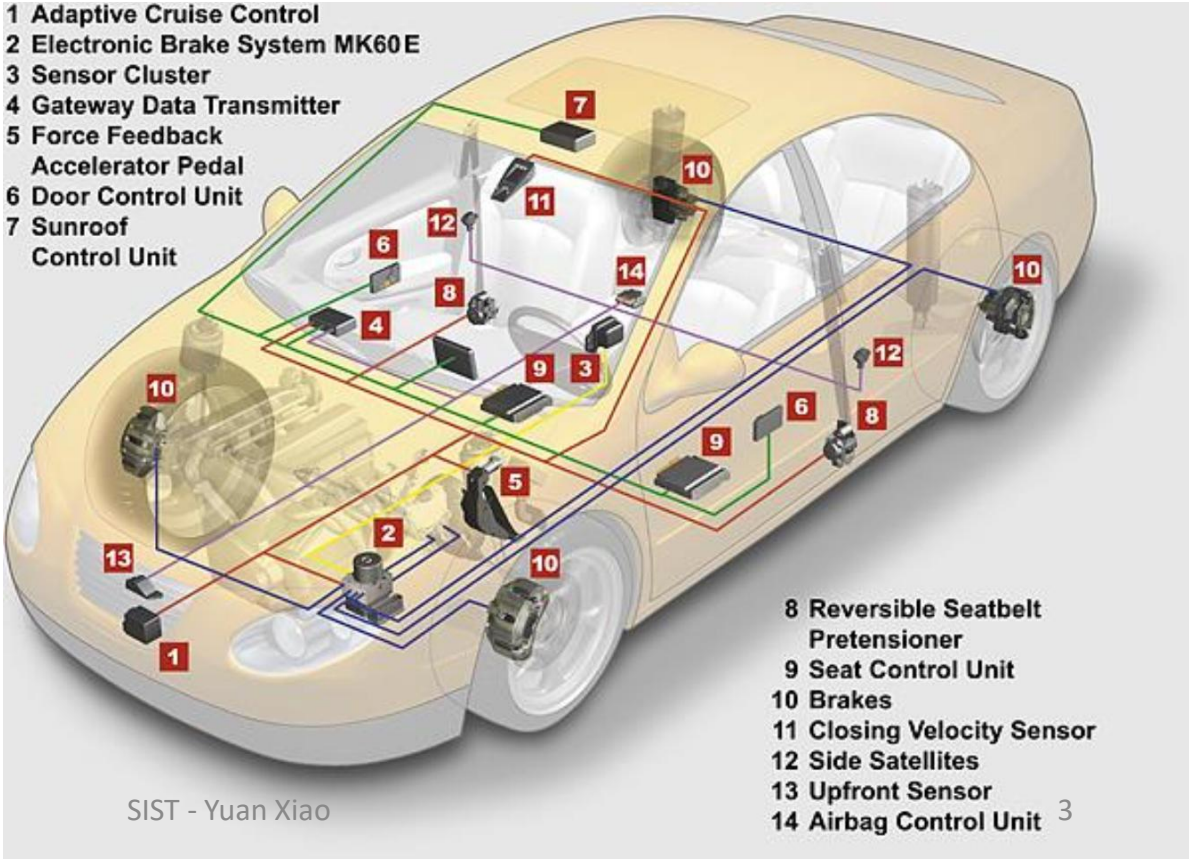
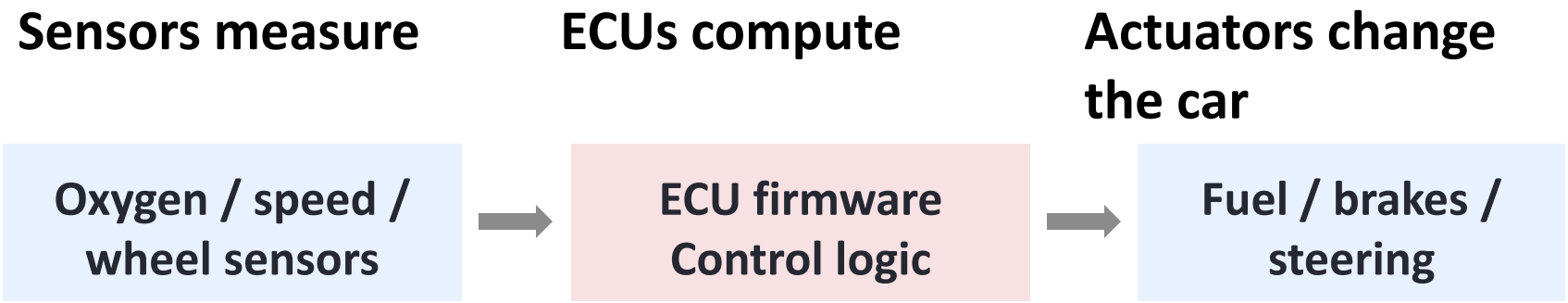


Image from https://www.aa1car.com/library/2004/bf110412.htm

Digital controls and software



Timing, integrity and safe operating limits matter as much as confidentiality.

Digital control connects software decisions to physical motion

The car is a software platform



Infotainment and phone integration



Connectivity, apps and updates

CarPlay / Android Auto images retained from the course deck

CAN Bus and ECUs

- ECUs exchange small messages on a shared bus
- Identifier selects message type and arbitration priority
- Classic CAN has no built-in cryptographic sender authentication

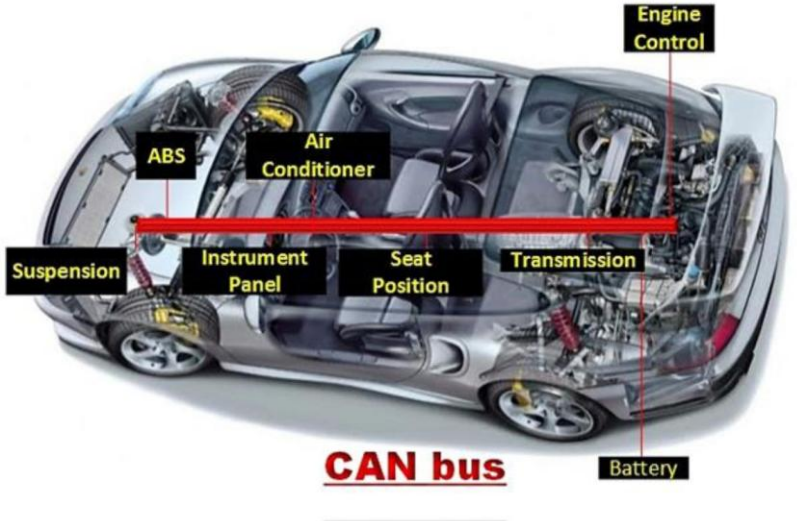
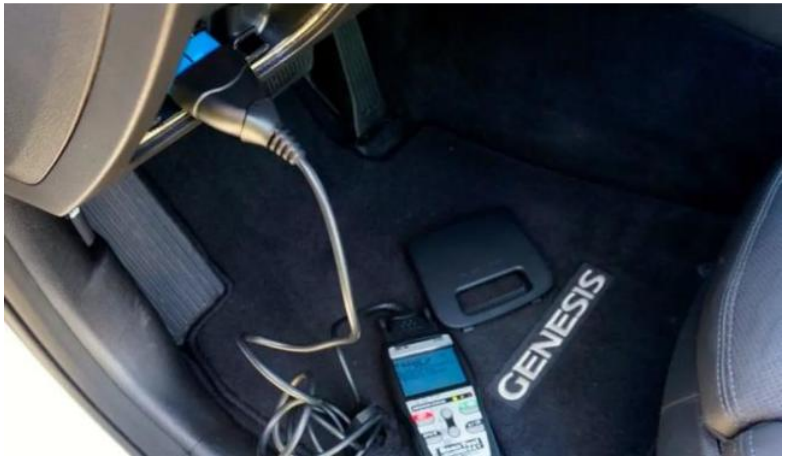


Illustration retained from the course deck / Infosec Institute

OBD-II: a legitimate diagnostic boundary



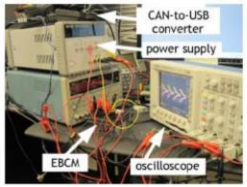
A physical socket for diagnostics

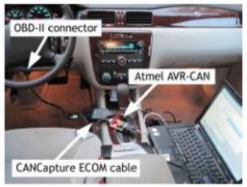


Service tools add another trust boundary

Images retained from the course deck

Case study 1: CAN takeover (2010)







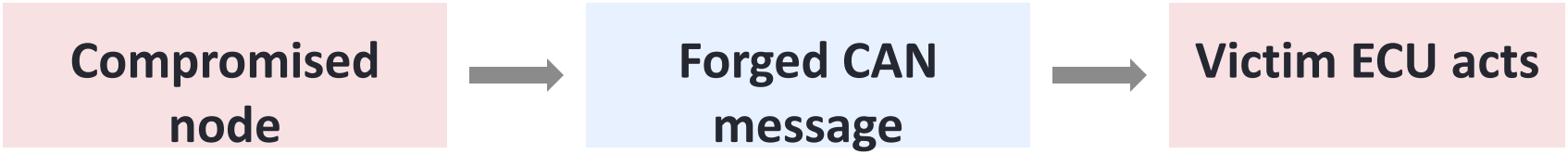
Access: connect equipment inside the car



Evidence: bench and controlled vehicle tests

Koscher et al., IEEE S&P 2010 / original experimental photos

CAN takeover: the trust assumption



- Message ID indicates meaning, not authenticated origin
- Injection changes signals or commands
- Flooding can deny timely communication

Threat model: attacker already has access to the relevant vehicle network

CAN takeover: impact and limits

- The test car accepted unauthorized control messages
- The displayed speed and driver message could be falsified
- Physical access and the tested architecture limited the claim



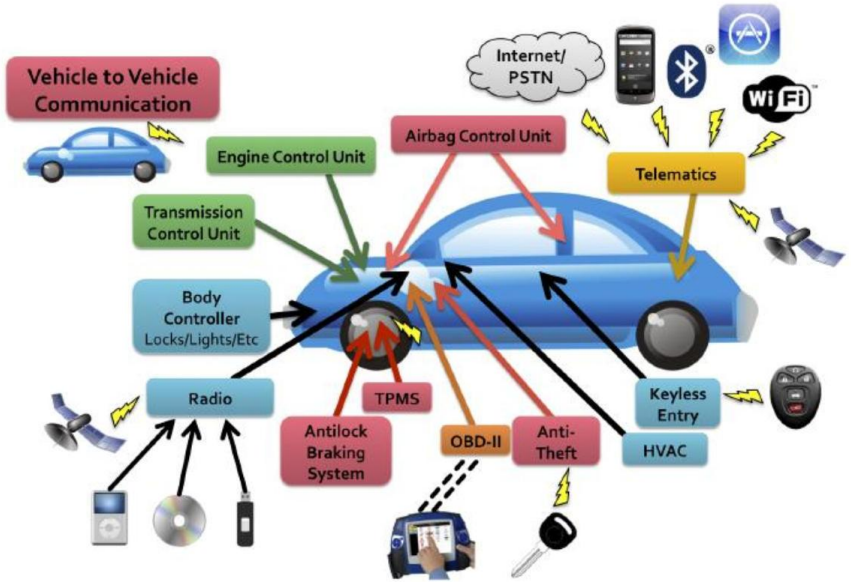
Koscher et al., 2010. The photographed vehicle is in Park

PART TWO

02

Remote Attack Vectors

Remote attack surfaces



- Indirect physical: media and service tools
- Nearby: Bluetooth, Wi-Fi and wireless accessories
- Wide area: cellular services and cloud APIs

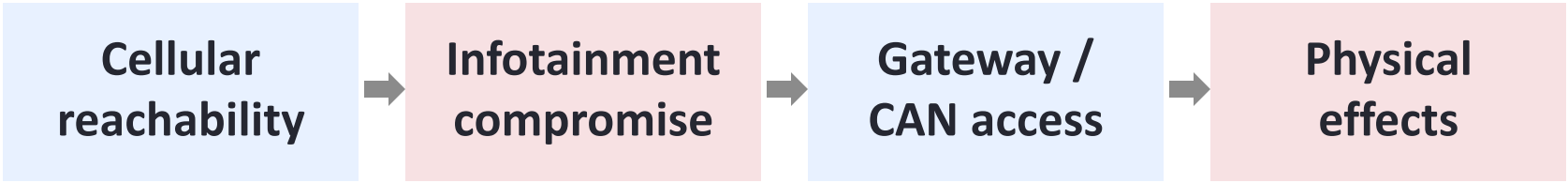
Attack-surface illustration retained from the course deck

Connectivity changes the attacker’s reach

OBD-II / service tools	Physical or workshop access Tool compromise can bridge to the car
Bluetooth	Nearby wireless access Pairing and implementation flaws matter
Cellular / cloud	Remote reach, potentially a fleet Authorization and isolation limit impact

Same endpoint, different access assumptions

Jeep 2015: a boundary-crossing chain



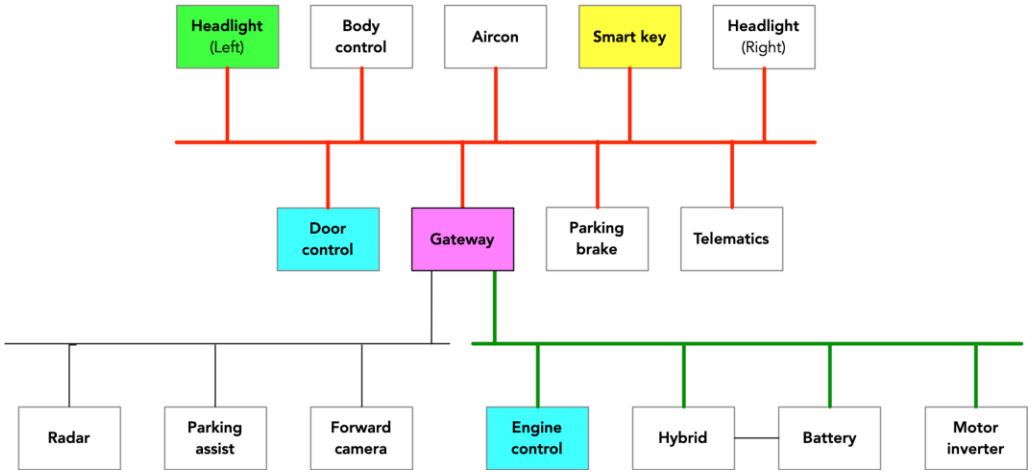
Research demonstration

About 1.4 million vehicles recalled

Miller & Valasek, 2015 / NHTSA recall investigation

2023: CAN injection becomes a theft route

- Attacker reaches wiring outside the cabin
- Injected messages bypass the intended key-authentication boundary
- A real theft technique exploits downstream trust



Ken Tindell / Canis Automotive Labs, April 2023

2024: the cloud becomes part of the car

- Researchers found Kia backend authorization flaws
- They could link an attacker account and invoke supported remote functions
- Firmware exploitation was unnecessary



Sam Curry et al., Sept. 2024. Blog illustration. Vulnerabilities fixed

2026: an anti-theft add-on adds risk

- BLE Theft Auto studied aftermarket systems
- Shared credentials and pairing flaws affected KARR / SWDS devices
- Researchers estimated at least 2.2 million equipped vehicles



David Baillot / UCSD Jacobs School of Engineering. July 2026

Modern vehicle security spans the lifecycle

Cloud identity
Owner / dealer

Gateways
Segment + authorize

Software updates
Verify + recover

Design

Least privilege
Safe-state restrictions

Operate

Monitor anomalies
Manage vulnerabilities

Respond

Revoke access
Patch the fleet

NHTSA Cybersecurity Best Practices, 2022 / recent case-study synthesis

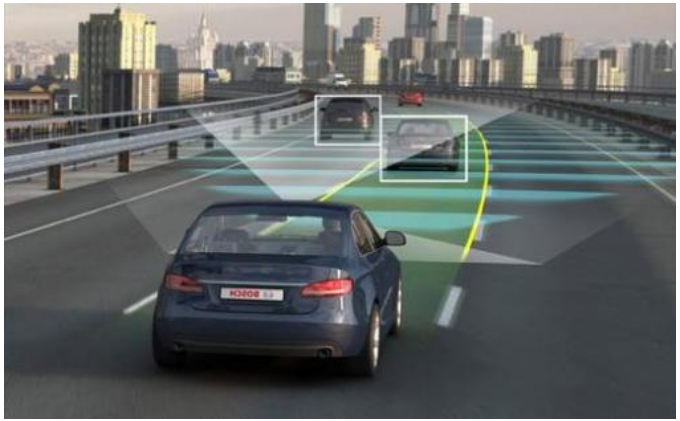
Self-driving vehicles: who does the driving?

Driver assistance Levels 0–2	Automated driving Levels 3–5
The human supervises and remains responsible for driving	The system performs the driving task within its specified conditions

Operational conditions and fallback duties define the safety claim

NHTSA automation levels. Level 3 includes a fallback-ready user

Self-driving: learning enters the control loop



Sensors → **Perception** → **Prediction** → **Planning** → **Control**

Driving image retained from the AI course deck

Discussion: from connected cars to AI

One physical outcome, several causes

- Forged CAN command: which trust boundary failed?
- Manipulated sensor input: must the attacker compromise code?
- Unexpected road situation: can harm occur without an attacker?

Next: adversarial learning, AI security and AI safety