Bulut Gözübüyük, Wes Bailey,
Douglas Everson, Zheng Dong,
Long Cheng, Mert D. Pesé

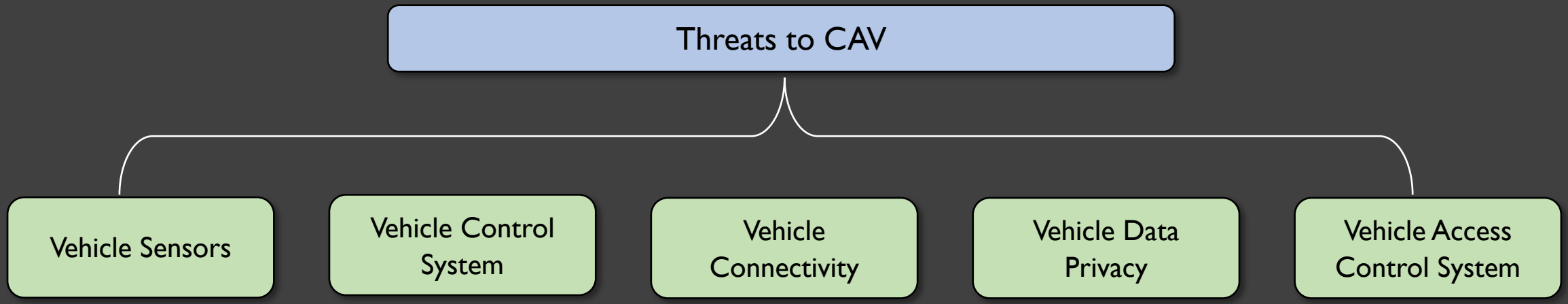
An Overview of Security in Connected and Autonomous Vehicles

AIoTSys 2023
Virtual Presentation, 10/22/23

School of COMPUTING

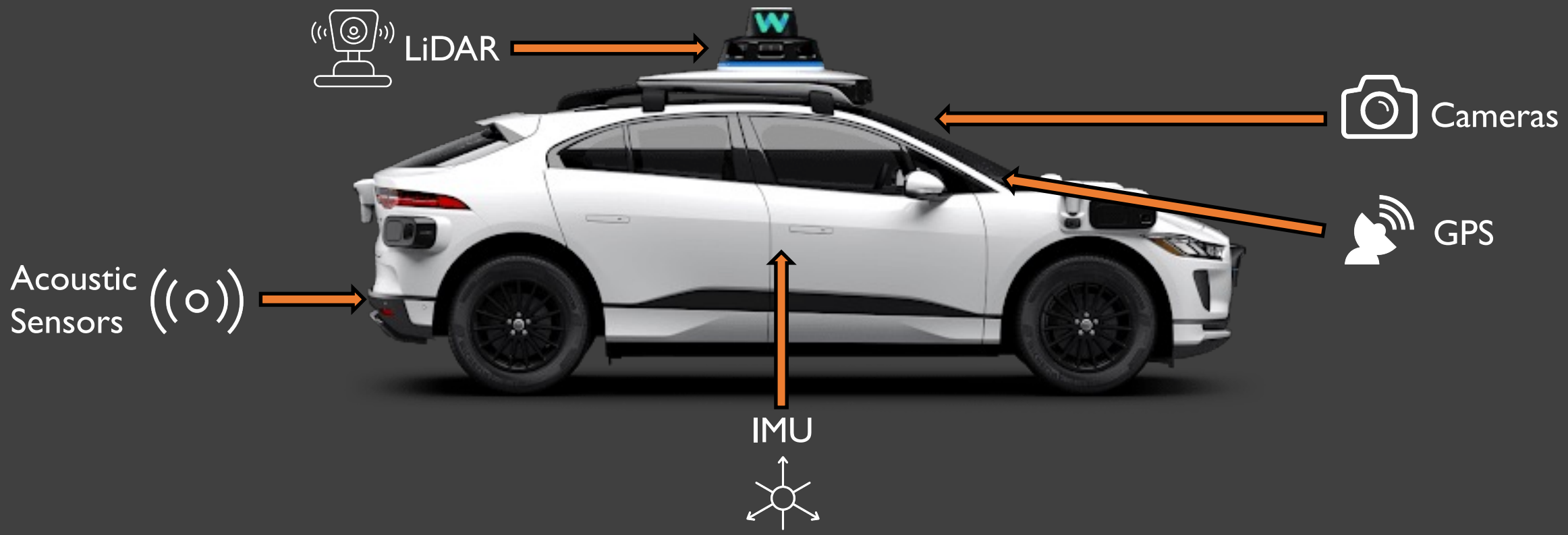
TigerSec Laboratory
@ Clemson University

Taxonomy


Threats to CAV
Vehicle Sensors
Vehicle Control System
Vehicle Connectivity
Vehicle Data Privacy
Vehicle Access Control System

Threats to Vehicle Sensors

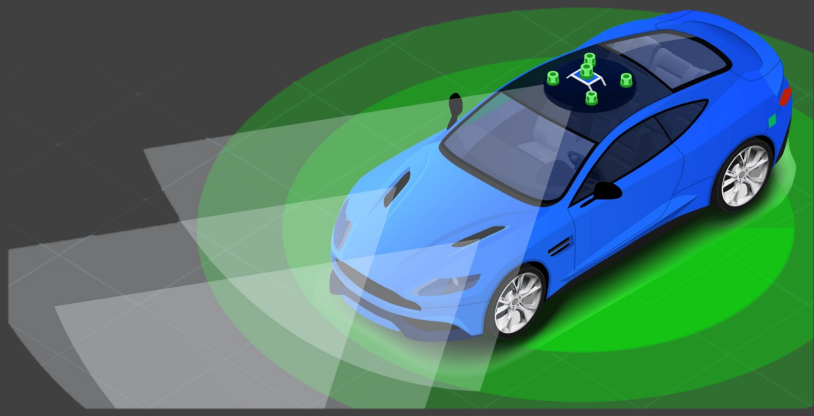
CAVs are highly complex and interconnected systems that often involve many sensors



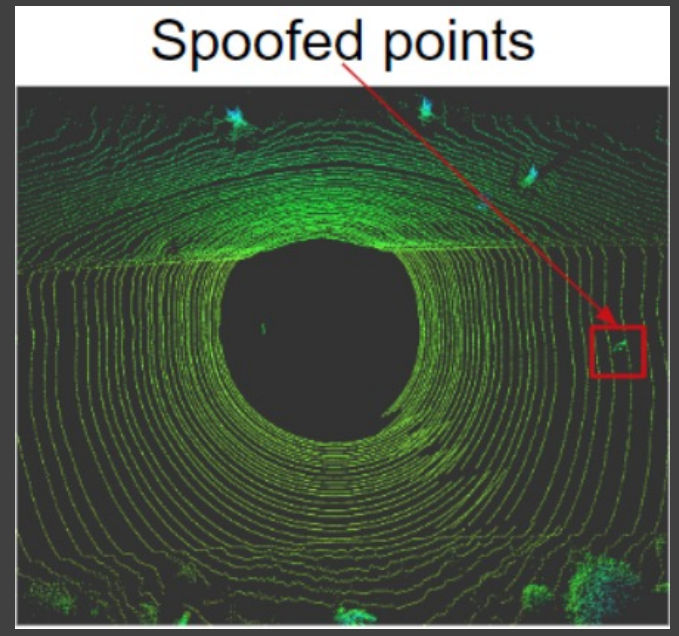
GPS Attacks

- Categorized as:
  - Jamming
  - Spoofing
- Poses a serious threat to the security and reliability of CAV's localization and can cause vehicles to drift off course and potentially lead to accidents.

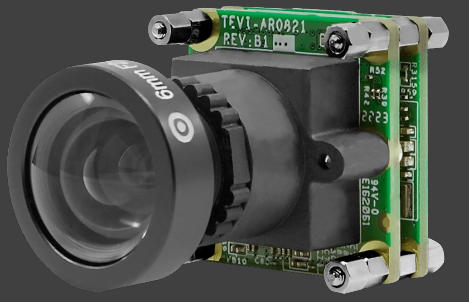
LiDAR Attacks



- Vulnerable to spoofing attacks of the device's laser pulses which can be launched from nearby devices.
- Crafting signal perturbations in LiDAR to induce false obstacle alerts [Ca19].
  - Mitigation using physical invariants to detect these anomalies.



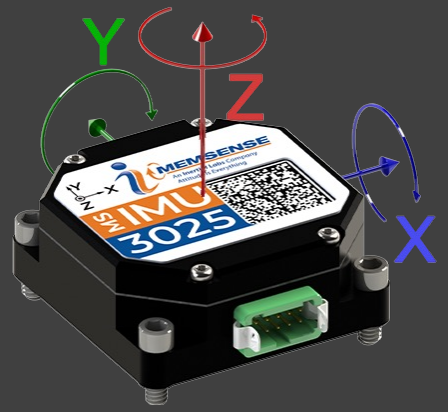
Camera Attacks



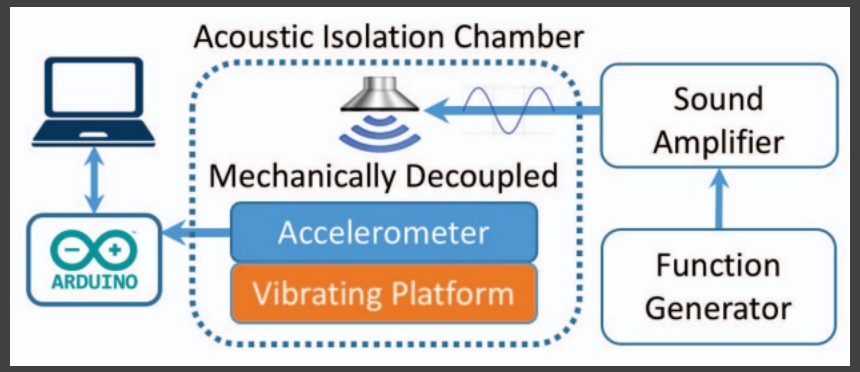
- CAV cameras gather visual data for spatial perception.
- Threats:
  - Readily available light sources can compromise camera function.
  - Risks include blinding' and rapid on-off' attacks, disrupting safe operation.
- Image Manipulation:
  - Malicious inputs can deceive CAV's DNN-based image classification.
  - Adhesive overlays trick neural networks, causing misdetection and potential crashes [Sa21].

- Acoustic Attacks:
  - Directed acoustic waves blur images, affecting object detection.

IMU Attacks



- IMUs measure vehicle dynamics using accelerometers, gyroscopes, and magnetometers in CAVs.
- Accelerometers assist Electronic Stability Control (ESC) in maintaining vehicle control.
- Vulnerability:
  - Sonic attacks on MEMS accelerometers [Tr17].
  - Potential compromised response from ESC, leading to instability.



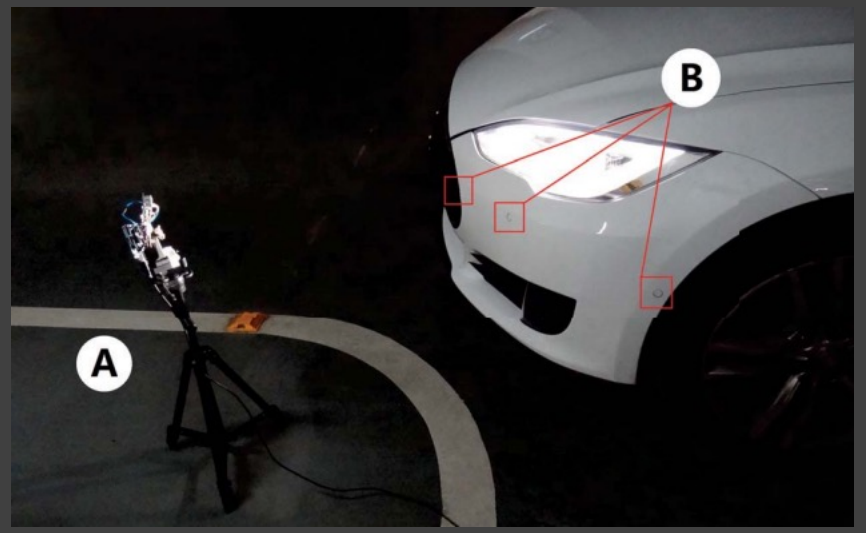
Maneuver Attacks

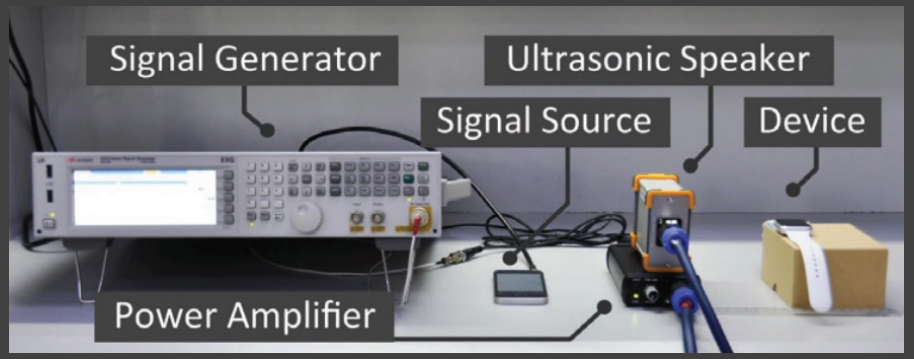
- Shift in Focus from Sensor Manipulation to Systemic Vulnerabilities.
- Introduction of Methodology to Detect Adversarial Driving Maneuvers [So23].

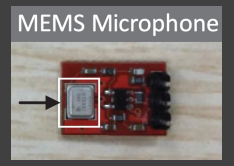
- Uncovering Inherent Weaknesses in Data Interpretation by the System.

Acoustic Sensor Attacks

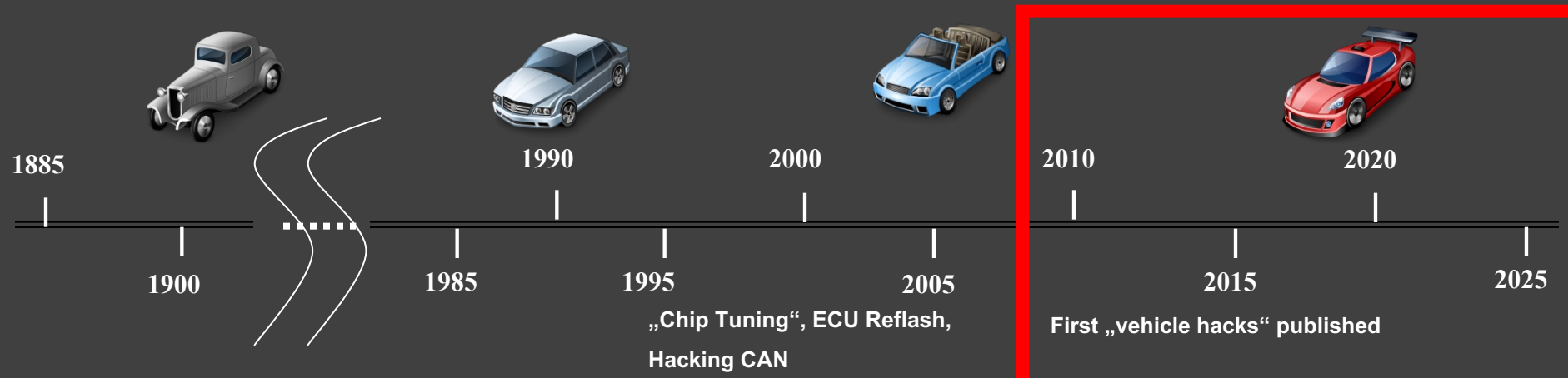
- Ultrasonic Sensors Susceptible to Jamming & Spoofing [Xu18]
- Voice Assistants Vulnerable to Hidden Commands [Zh17].







Threats to In-Vehicle Networks



First-Generation Attacks (~2010-2015)	Second-Generation Attacks (~2015-2020)	Third-Generation Attacks (~2020-?)
CAN injection attacks requiring physical interface (OBD-II connector)	Remote attacks leveraging vulnerabilities in IVI and TCU	Remote attacks leveraging third-party apps on IVIs

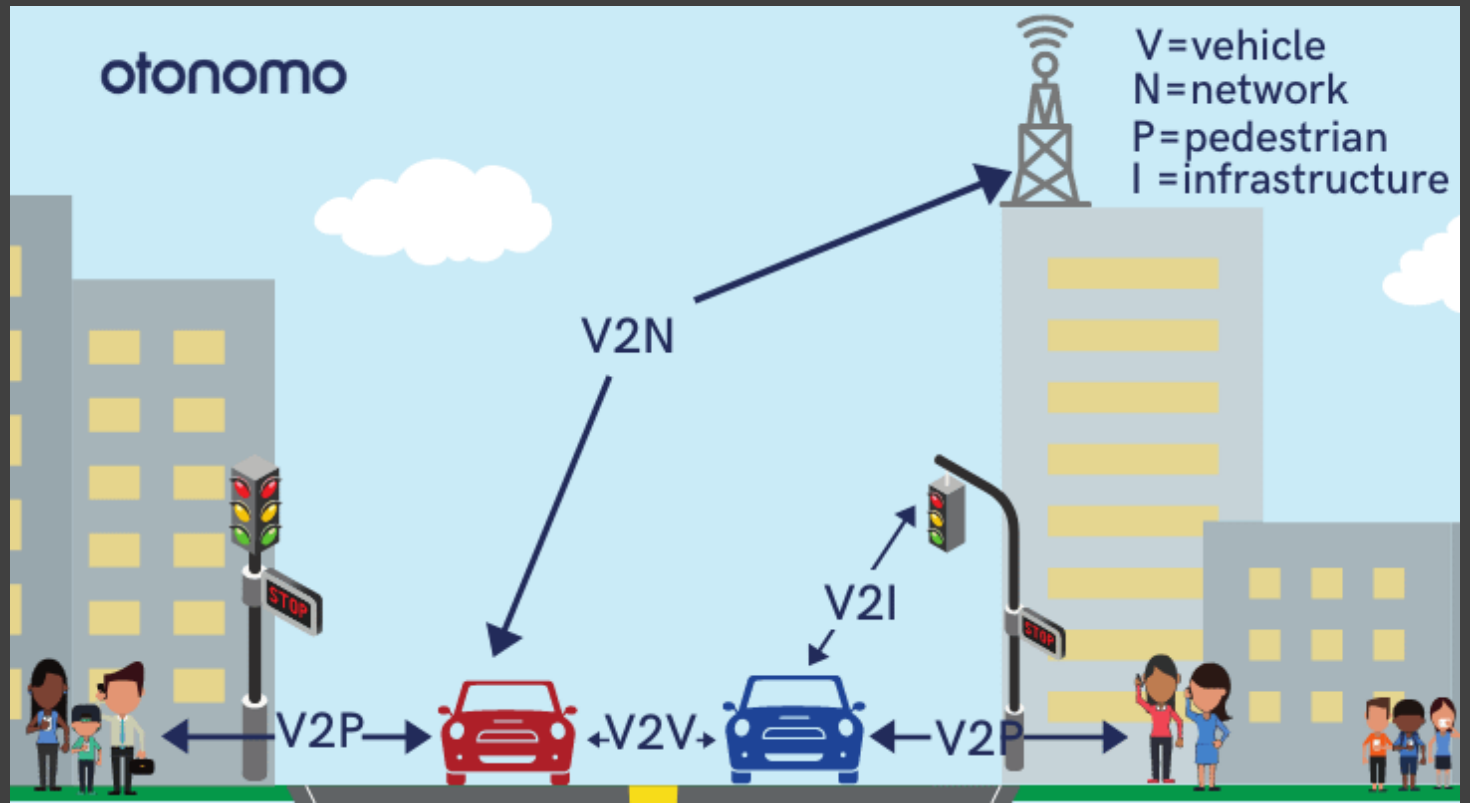
Risk / Damage Potential

Limited Attacks

Large-Scale Attacks

V2X: Vehicle-to-Everything Communication

- V2X enables communication between vehicles, infrastructure, and pedestrians.
- Cellular or short-range networks support this communication.
- Goal: Improve road safety via shared info (location, speed, etc.).



V2X Security Concerns

- **External vs. Internal Attacks:** BSM security robust against outsiders, but compromised vehicle units pose a threat.
- **5G Vulnerabilities:** Expanded attack surface, especially at network edges.
- **DoS Threats:** Jeopardizing CAV availability, potential for communication lags.
- **Forged Messages:** Misleading vehicles into harmful decisions.
- **Infrastructure Risks:** Traffic systems, like I-SIG, vulnerable to spoofing.

Threats to User-Data

- **Hyper-Connected IoT Platform**
  - Vulnerabilities and complexities of CAVs due to mobility and constant location-based service connections.
- **Data Sharing Concerns**
  - Data transferred to multiple stakeholders like car manufacturers and insurance companies.
  - Privacy concerns for CAV users.
- **Research Findings**
  - Drivers can be distinguished using pre-trip vehicle sensor data from the CAN bus [Ka17].
  - Driver re-identification using CAN messages without reverse-engineering the protocol [Re19].
  - Privacy issues in Android Automotive part of third-generation attack [Pe23].

Threats to Vehicle Access Control Systems

- **Active Key Entry Attacks:** Vulnerability to relay attacks with traditional fobs.
  - Solutions: Distance bounding protocols, rolling codes.
- **Passive Key Entry System Attacks:** Relay attacks, cryptographic flaws, and jamming.
  - Solutions: Challenge-response authentication.
- **Smartphone Digital Key Attacks:** Risks from malware, compromised communication, phishing.
  - Solutions: UWB, robust app security, encryption, 2-factor authentication.

Conclusion

- Comprehensive study of security and privacy in CAVs.
- Classification of threats based on attack surfaces.
- IoT integration heightens vulnerabilities.
- Criticality of proper authentication: Zero Trust Architecture (ZTA) as a key approach.
- Balance between technological advancement, privacy, and safety is vital for a secure transportation future.

Q & A

Bulut Gozubuyuk
bgozubu@clemson.edu

References

[Ca19] Yulong Cao, Chaowei Xiao, Benjamin Cyr, Yimeng Zhou, Won Park, Sara Rampazzi, Qi Alfred Chen, Kevin Fu, and Z. Morley Mao. Adversarial sensor attack on lidar-based perception in autonomous driving. In Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, CCS '19, page 2267–2281. Association for Computing Machinery, Nov 2019.

[Sa21] Takami Sato, Junjie Shen, Ningfei Wang, Yunhan Jia, Xue Lin, and Qi Alfred Chen. Dirty road can attack: Security of deep learning based automated lane centering under {Physical-World} attack. In 30th USENIX Security Symposium (USENIX Security 21), pages 3309–3326, 2021.

[Tr17] Timothy Trippel, Ofir Weisse, Wenyuan Xu, Peter Honeyman, and Kevin Fu. Walnut: Waging doubt on the integrity of mems accelerometers with acoustic injection attacks. In 2017 IEEE European symposium on security and privacy (EuroS&P), pages 3–18. IEEE, 2017.

[So23] Ruoyu Song, Muslum Ozgur Ozmen, Hyungsub Kim, Raymond Muller, Z Berkay Celik, and Antonio Bianchi. Discovering adversarial driving maneuvers against autonomous vehicles. In 32nd USENIX Security Symposium (USENIX Security 23), pages 2957–2974, 2023.

[Xu18] Wenyuan Xu, Chen Yan, Weibin Jia, Xiaoyu Ji, and Jianhao Liu. Analyzing and enhancing the security of ultrasonic sensors for autonomous vehicles. IEEE Internet of Things Journal, 5(6):5015–5029, Dec 2018.

[Ka17] Gorkem Kar, Shubham Jain, Marco Gruteser, Jinzhu Chen, Fan Bai, and Ramesh Govindan. Predriveid: Pre-trip driver identification from in-vehicle data. In Proceedings of the Second ACM/IEEE Symposium on Edge Computing (SEC), 2017.

[Re19]. Mina Remeli, Szilvia Lestyan, Gergely Acs, and Gergely Biczok. Automatic driver identification from in-vehicle network logs. In 2019 IEEE Intelligent Transportation Systems Conference (ITSC), page 1150–1157, 2019.

[Pe23] Mert D Pese. A first look at android automotive privacy. Technical Report, SAE Technical Paper, 2023.