Ghost Cars & Fake Obstacles: First Look at Control Software Stack Security in Emerging Smart Transportation

Qi Alfred Chen
Assistant Professor, Dept. of CS
Recent interest: Software security in smart transportation
Recent interest: Software security in smart transportation

Connected Vehicle (CV)  Autonomous Vehicle (AV)
Recent interest: Software security in smart transportation

Connected Vehicle (CV)  Autonomous Vehicle (AV)

Control software stack
Recent interest: Software security in smart transportation

Connected Vehicle (CV)  Autonomous Vehicle (AV)

[ISOC NDSS’18]  
*First software security analysis* of a CV-based transportation system

[ACM CCS’19]  
*First software security analysis* of LiDAR-based AV perception
Recent interest: Software security in smart transportation

**Connected Vehicle (CV)**

- **What**: CV data spoofing on USDOT’s smart traffic light control (for reducing congestion)
- **How**: Static & dynamic s/w analysis
- **Finding**: New security vuln at traffic control algorithm level
  - *One single attack vehicle can create massive traffic jams!*
  - Demo time!

[ISOC NDSS’18]

*First software security analysis* of a CV-based transportation system
Recent interest: Software security in smart transportation

- What: LiDAR spoofing on Baidu Apollo, a production-level AV
- How: Modelling & optimization
- Finding: Attacker can strategically spoof to make AV “see” fake front obstacle

[ACM CCS’19]
First software security analysis of LiDAR-based AV perception
Security implication: Emergency brake attack

• Cause AV to decrease speed from $43\text{km/h}$ to $0\text{km/h}$ within 1 sec!
Conclusion

• Initiated **the first research efforts** to perform security analysis of control software stacks in CAV systems
• Discovered **new attacks**, analyzed **root causes**, and demonstrated **security & safety implications**
• **Only the beginning** of CAV software security research
  – Inherently an inter-disciplinary direction, **always open to collaboration**!
  – Initiated the **1st ACM AutoSec workshop** to build community

**Contact:**
Qi Alfred Chen  
Computer Science, UC Irvine  
Email: alfchen@uci.edu  
Homepage: https://www.ics.uci.edu/~alfchen/