Security Analysis of Next-generation Connected Vehicle based Transportation

Qi Alfred Chen, Yucheng Yin, Yiheng Feng, Z. Morley Mao, Henry X. Liu
University of Michigan
ACM CCS FEAST workshop 2017
Background: Connected Vehicle (CV) technology

- Wirelessly connect vehicles & infrastructure
- **Goal**: Dramatically improve mobility, safety, environmental impact, & public agency operations
Background: Recent advances

• Will *soon* transform transportation systems today

• 2016.9, USDOT launched **CV Pilot Program**
  – National effort to deploy, test, & operationalize CV-based transportation systems
  – Launched in *3 cities*

• 2016.11, USDOT proposed to *mandate* CV tech in *all light-duty vehicles*, starting from *as soon as 2020*
Cybersecurity of CV-based transportation

• However, such dramatically increased connectivity also opens a new door for **cyber attacks**

• **Highly important** to understand potential security vulnerabilities & new security challenges
  – Need to ensure **security** & **safety** for vehicles, transportation infrastructure, drivers & pedestrians
  – Need to perform study **now** so that they can be proactively addressed before nationwide deployment
Our work

• Start by performing security analysis
• **Current focus**: Intelligent Traffic Signal System (I-SIG)
  – Use real-time CV data for intelligent signal control
  – USDOT sponsored design & impl.
Threat model

• Start by performing security analysis
• **Current focus**: Intelligent Traffic Signal System (I-SIG)
  – Use real-time CV data for intelligent signal control
  – USDOT sponsored design & impl.
• **Threat model**: Malicious vehicles send spoofed data
Preliminary results

• **Finding**: Vulnerability in the smart traffic control logic
  – Spoofed data from *one single attack vehicle* can greatly manipulate the traffic control
  – The smart control algorithm can be fooled to:
    • Add tens of *“ghost” vehicles*
    • Extend green light by spoofing to a *late arriving* vehicle
Congestion attack results

• One car to cause massive road-blocking effect!

Gas station

Left-turn lane spills over and blocks the entire approach

Only one single vehicle is attacking

The spillover starts and blocks one through lane
Open questions

• More security analysis
  – Other types of attack goals
    • **Personal gain**: Reduce attack vehicle’s travel time at the cost of others
    • **Safety attack**: Increase the safety risk of a specific or a set of vehicles
  – Other CV-based transportation systems
    • **60+ types of open sourced prototypes** developed by USDOT

• Defense solution directions
  – Data spoofing detection
    • Systematically **transform CV systems** to include detection logic
  – Hardware-assisted data spoofing prevention
    • E.g., leverage Intel SGX, ARM TrustZone
    • Need systematic mechanism to **partition protocol binaries**
• A full paper of our current findings will appear in NDSS’18
• Any comments?