Ghost Cars and *Fake Obstacles*: Autonomy Software Security in Emerging Autonomous Driving & Smart Transportation

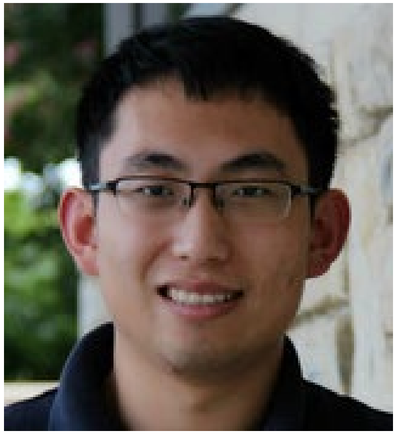
Qi Alfred Chen

Assistant Professor, Dept. of CS

UCIrvine

A bit about me

- **Qi Alfred Chen**
  - Assistant Prof. in CS@UC Irvine
  - Ph.D., U of Michigan
- Area: **Cybersecurity**



www
Cyber security
Shift

Impact: Demo & vuln. report

Usenix Sec'14

Usenix Sec'14

Euro S&P'17

NDSS'18

17,000 views a day!

which is used by the attacker to tra

Malware Infers the Timin
Legitimate Client Com

Left-turn lanes spill over and block whole roads. In this perioc travel time is > 6x higher for half of vehicles, and > 14x for 22% of vehicles.

cve.mitre.org — NDSS'16, Euro S&P'17

US-CERT
UNITED STATES COMPUTER
EMERGENCY READINESS TEAM — IEEE S&P'16

Usenix Sec'14
NDSS'16

Linux — CCS'15

comcast — CCS'17

Apple — CCS'17

Microsoft — CCS'17

NYCDOT Pilot — NDSS'18

CONNECTED VEHICLE PILOT
TAMPA — NDSS'18

Impact: Media coverage

Usenix Securiy'14

ars TECHNICA

BBC NEWS

CBS

NBC NEWS

AH AndroidHeadlines

PC PCMAG.COM

tom's guide

HOT HARDWARE

IEEE S&P'16

security affairs

SECURITYWEEK
INTERNET AND ENTERPRISE SECURITY NEWS, INSIGHTS & ANALYSIS

SC MAGAZINE

nakedsecurity
News. Opinion. Advice. Research.

HELPNETSECURITY

Euro S&P'17

WIRED

BLEEPINGCOMPUTER

M

AH AndroidHeadlines

TechRepublic®

Recent interest: Autonomy software security in smart transportation

Connected Vehicle (CV)

Autonomous Vehicle (AV)

U.S. Department of Transportation

TOYOTA

Ford

Qualcomm

lyft

Uber

TESLA

Aurora

GM

WAYMO

apollo

Recent interest: Autonomy software security in smart transportation

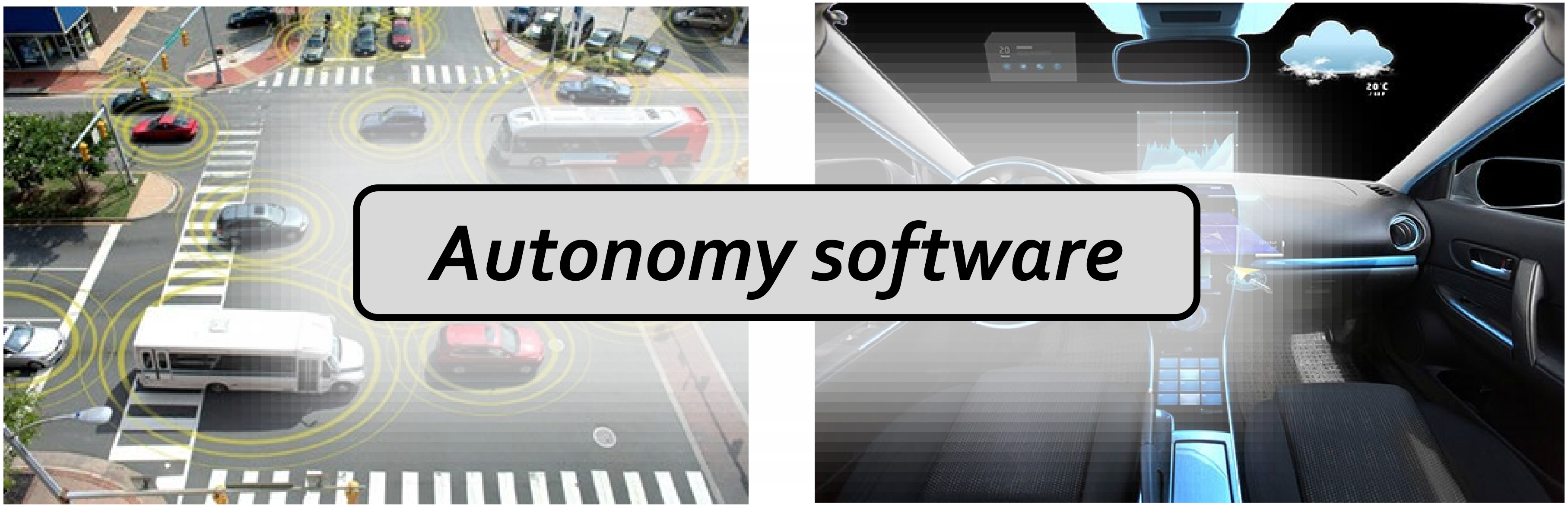
Connected Vehicle (CV)

Autonomous Vehicle (AV)

Recent interest: Autonomy software security in smart transportation

Connected Vehicle (CV)

Autonomous Vehicle (AV)



Autonomy software

Recent interest: Autonomy software security in smart transportation

Connected Vehicle (CV)

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

Autonomy software

Autonomous Vehicle (AV)

[ACM CCS’19]
First software security analysis of LiDAR-based AV perception

Recent interest: Autonomy software security in smart transportation

Connected Vehicle (CV)

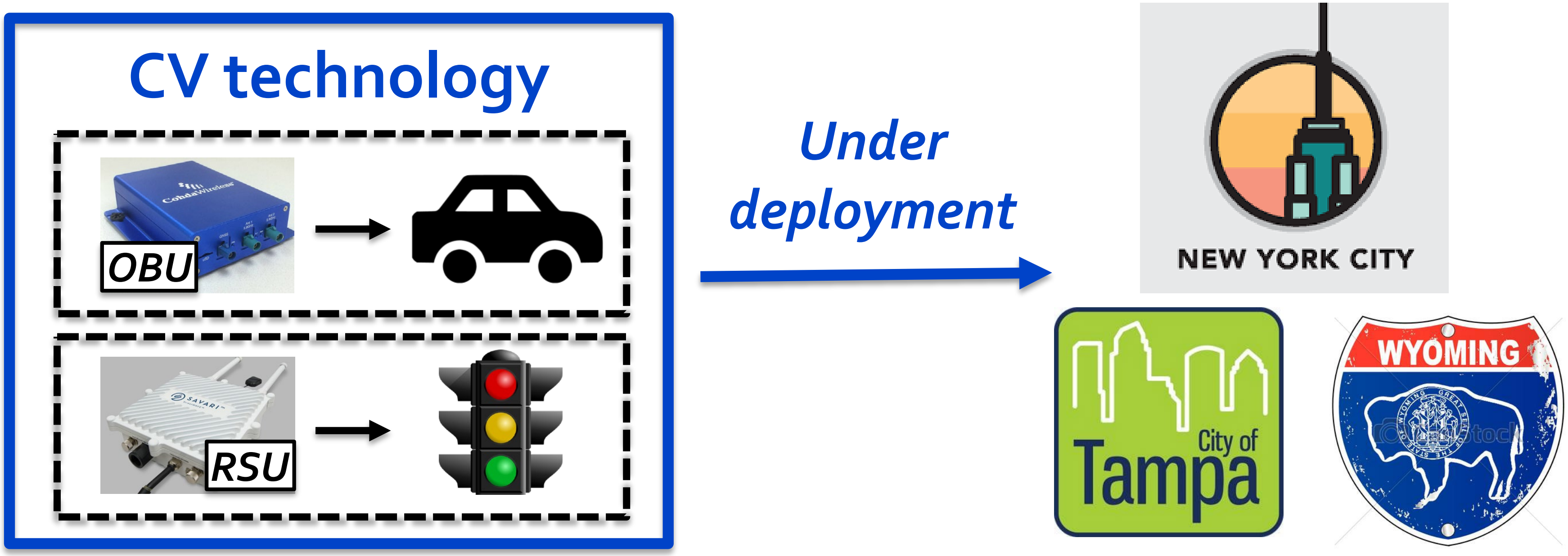
[ISOC NDSS'18]
First software security analysis of a CV-based transportation system

Autonomous Vehicle (AV)

[ACM CCS'19]
First software security analysis of LiDAR-based AV perception

Background: Connected Vehicle technology

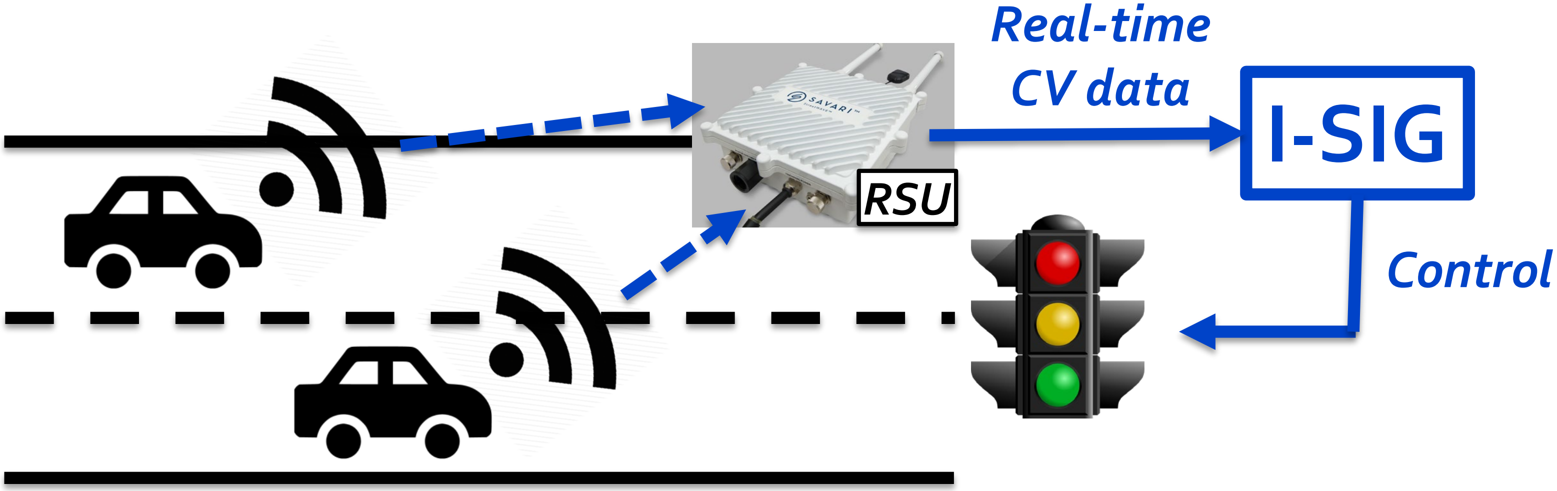
- Wirelessly connect vehicles & infrastructure to dramatically improve **mobility** & **safety**
- Will **soon** transform transportation systems today
  - 2016.9, USDOT launched ***CV Pilot Program***



CV = Connected Vehicle OBU = On-Board Unit RSU = Road-Side Unit

First security analysis of CV-based transp.

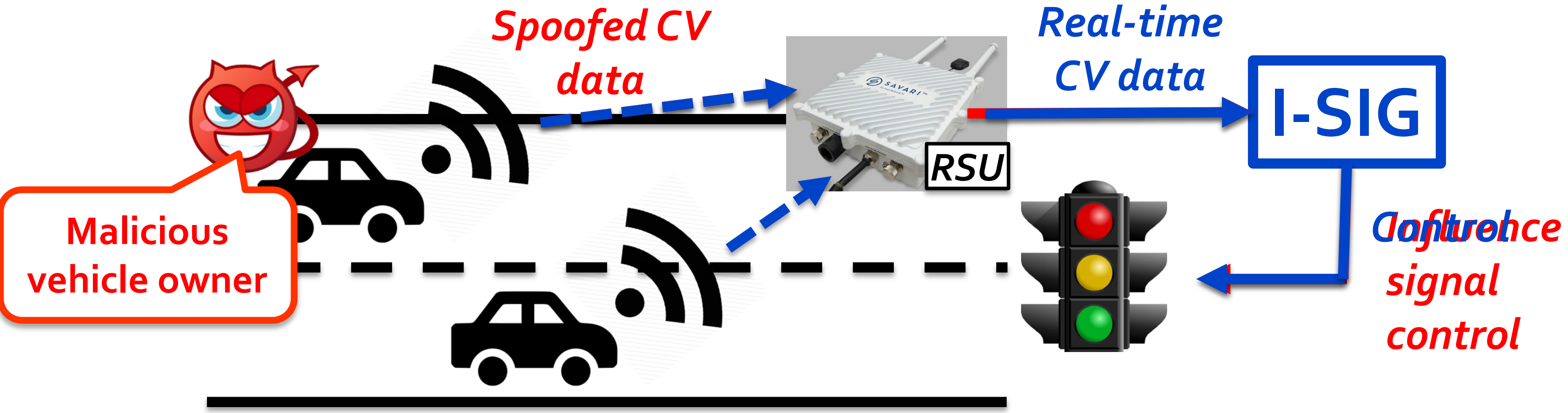
- **Target**: Intelligent Traffic Signal System (I-SIG)
  - – Use real-time CV data for intelligent signal control
  - – USDOT sponsored design & impl.
  - – Fully implemented & tested in Anthem, AZ, & Palo Alto, CA
    - ~30% reduction in total vehicle delay
  - – Under deployment in NYC and Tampa, FL



CV = Connected Vehicle OBU = On-Board Unit RSU = Road-Side Unit

Threat model

- Malicious vehicle owners deliberately control the OBU to send spoofed data
  - OBU is compromised physically[1], wirelessly[2], or by malware[3]



[1] Koscher et al.@IEEE S&P'10 [2] Checkoway et al.@Usenix Security'11 [3] Mazloom et al.@Usenix WOOT'16

Attack goals

Traffic congestion

Increase total delay of vehicles in the intersection

Personal gain

Minimize attacker's travel time (at the cost of others')

Attack goals

This work

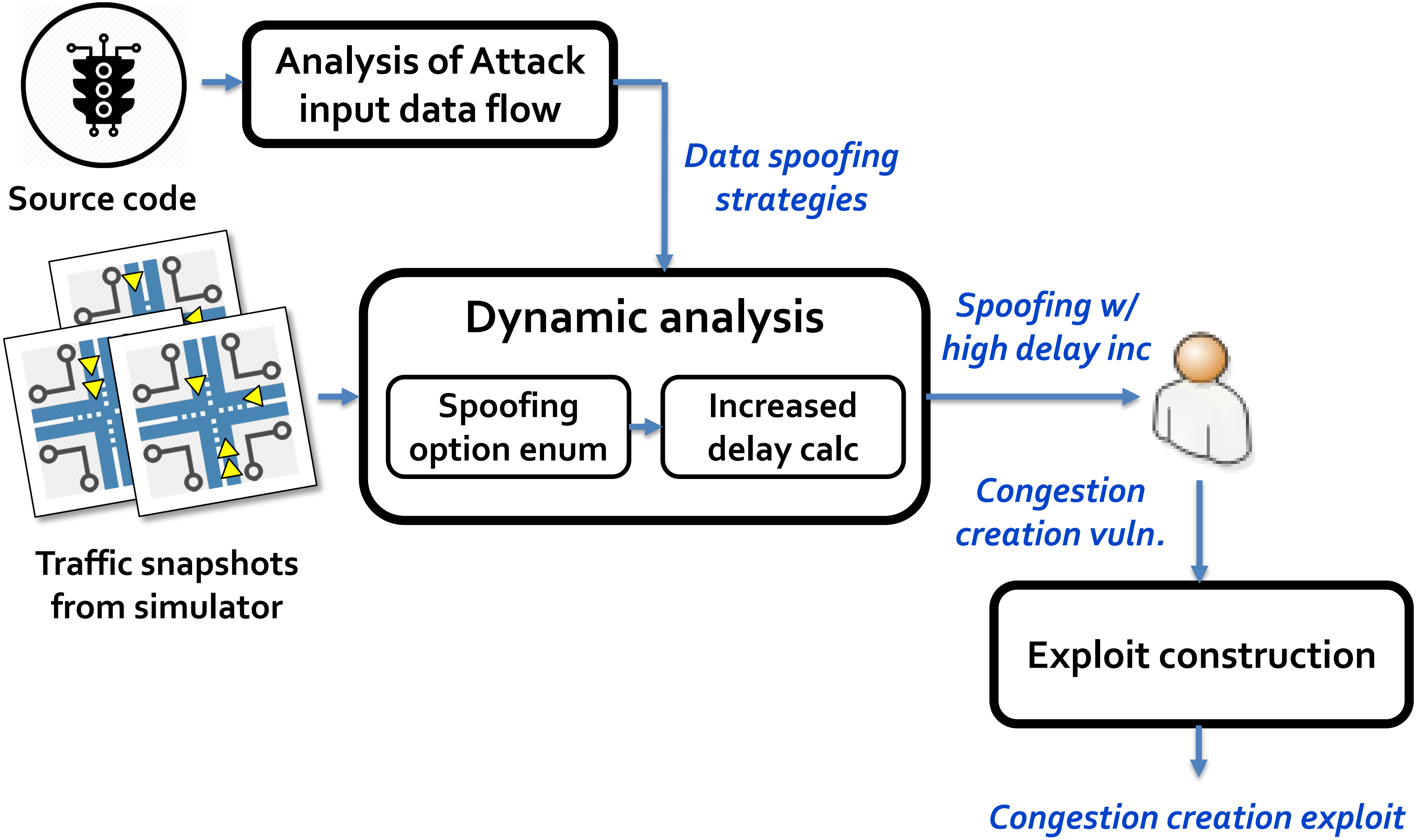
Traffic congestion

Increase total delay of vehicles in the intersection

Personal gain

Minimize attacker's travel time (at the cost of others')

Analysis methodology



Source code

Analysis of Attack input data flow

Data spoofing strategies

Traffic snapshots from simulator

Dynamic analysis

Spoofing option enum

Increased delay calc

Spoofing w/ high delay inc

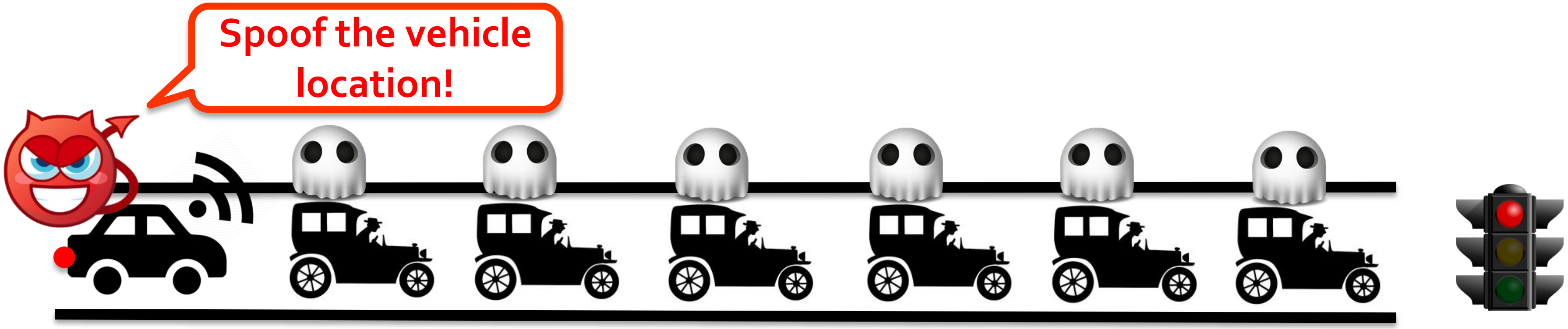
Congestion creation vuln.

Exploit construction

Congestion creation exploit

Software vulnerability discovery

- **Finding**: Traffic control algorithm level vulnerabilities
  - 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*** to waste green light
    - Extend green light by spoofing as a ***late arriving*** vehicle



Attack video demo

- Demo time!
  - https://www.youtube.com/watch?v=3iV1sAxPuLo

Recent interest: Autonomy software security in smart transportation

Connected Vehicle (CV)

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

Autonomous Vehicle (AV)

[ACM CCS'19]
First software security analysis of LiDAR-based AV perception

Recent interest: Autonomy software security in smart transportation

Connected Vehicle (CV)

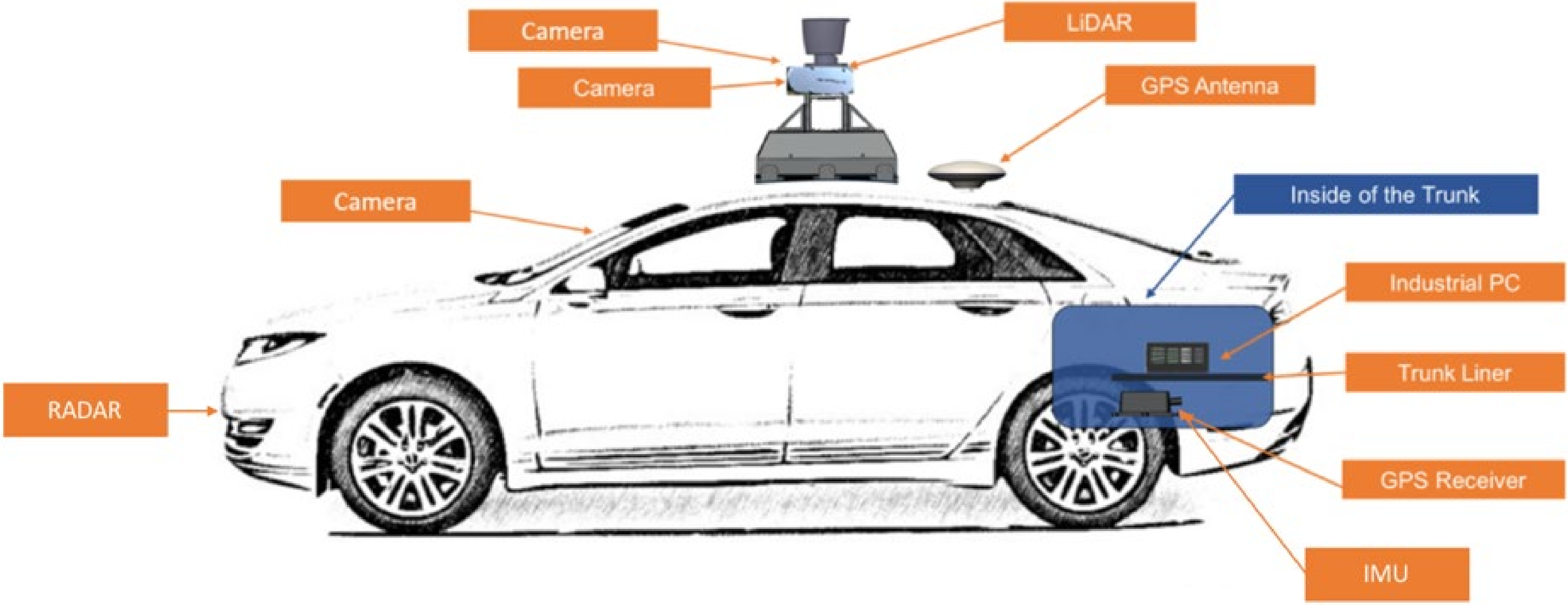
[ISOC NDSS’18]
First software security analysis of a CV-based transportation system

Autonomous Vehicle (AV)

[ACM CCS’19]
First software security analysis of LiDAR-based AV perception

Background: Autonomous Vehicle technology

- Equip vehicles with various types of sensors to enable self driving

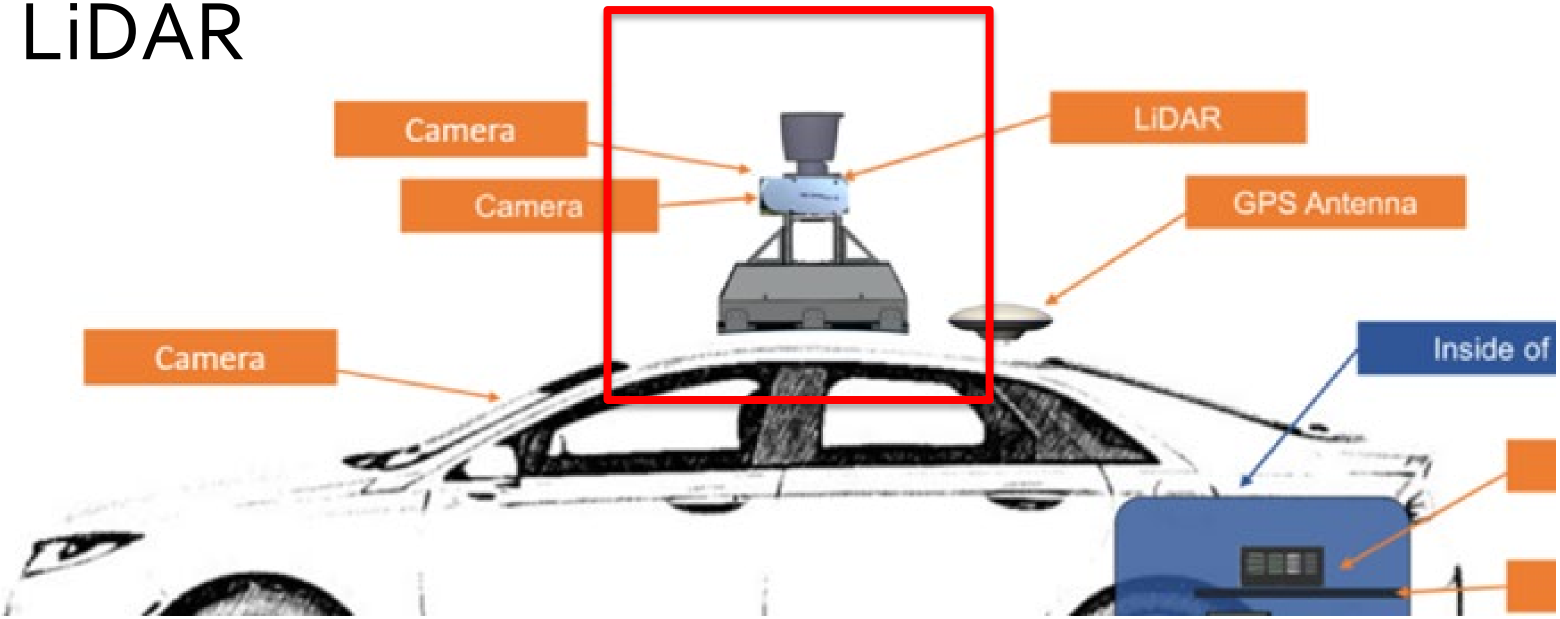


Background: Autonomous Vehicle technology

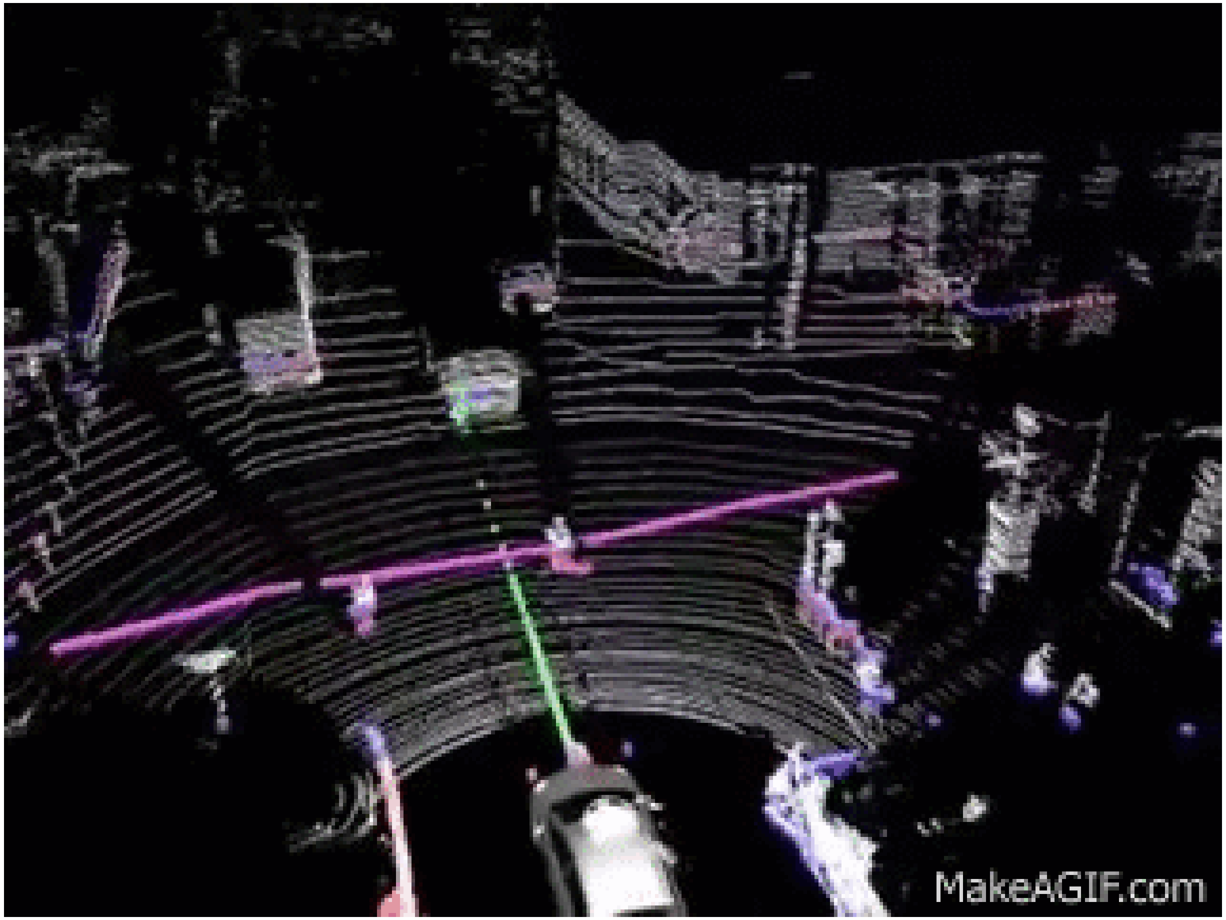
- Under active development in huge number of companies, some already made into production

Goal: First security analysis of AV software

- New attack surface: Sensors
  - Key input channel for critical control decisions
  - Public channel shared with potential adversaries
    - *Fundamentally unavoidable attack surface!*
- LiDAR

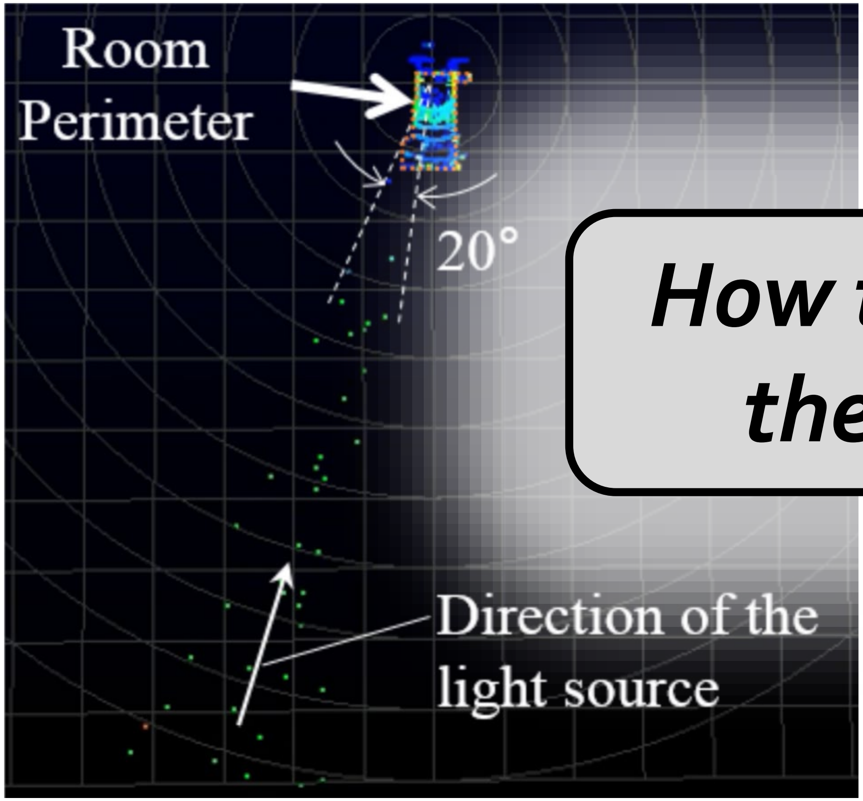


Background: LiDAR basics



Background: LiDAR attacks

- Known attack: LiDAR spoofing[1]
  - Shoot laser to LiDAR to inject points

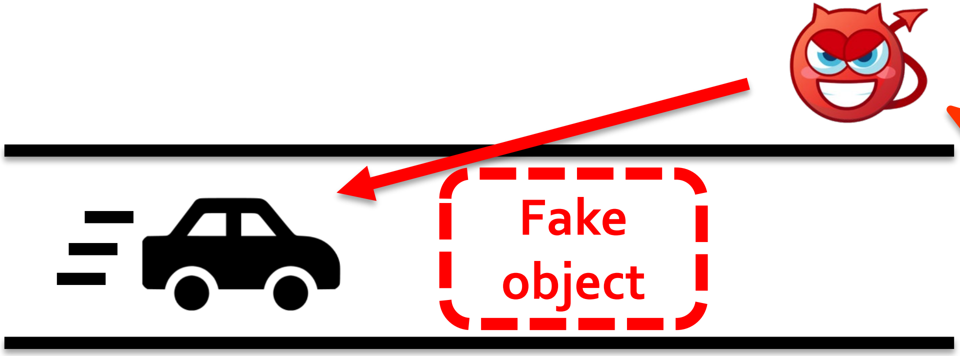


How to use this to attack the autonomy logic?

[1] Shin et al.@CHES'17

First security analysis of LiDAR-based perception in AV

- **Target**: Baidu Apollo AV software system
  - Production-grade system, drive some buses in China already
  - Open sourced ("Android in AV ecosystem")
  - Partner with 100+ car companies, including BMW, Ford, etc.
- **Attack**: LiDAR spoofing attack from road-side laser shooting devices to create fake objects
  - Trigger undesired control operations, e.g., emergency brake



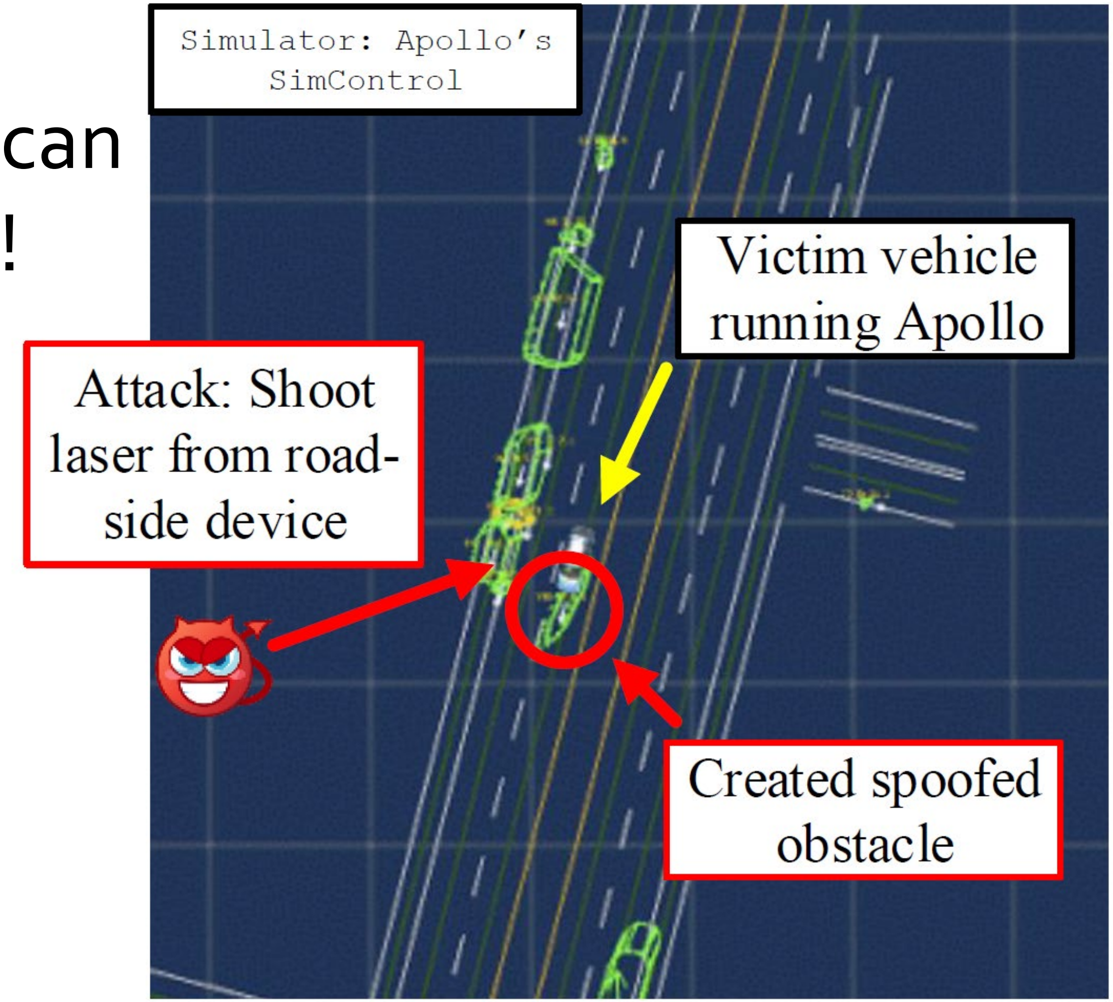
Set up road-side device to shoot laser

Analysis methodology overview

- Attack input perturbation modelling
  - Model *LiDAR spoofing attack* and *pre-processing step* into analytical functions
- Machine learning model security analysis
  - Formulate and solve an optimization problem over a DNN model
- Security implication analysis
  - Understand attack impact on AV driving behaviors & road safety

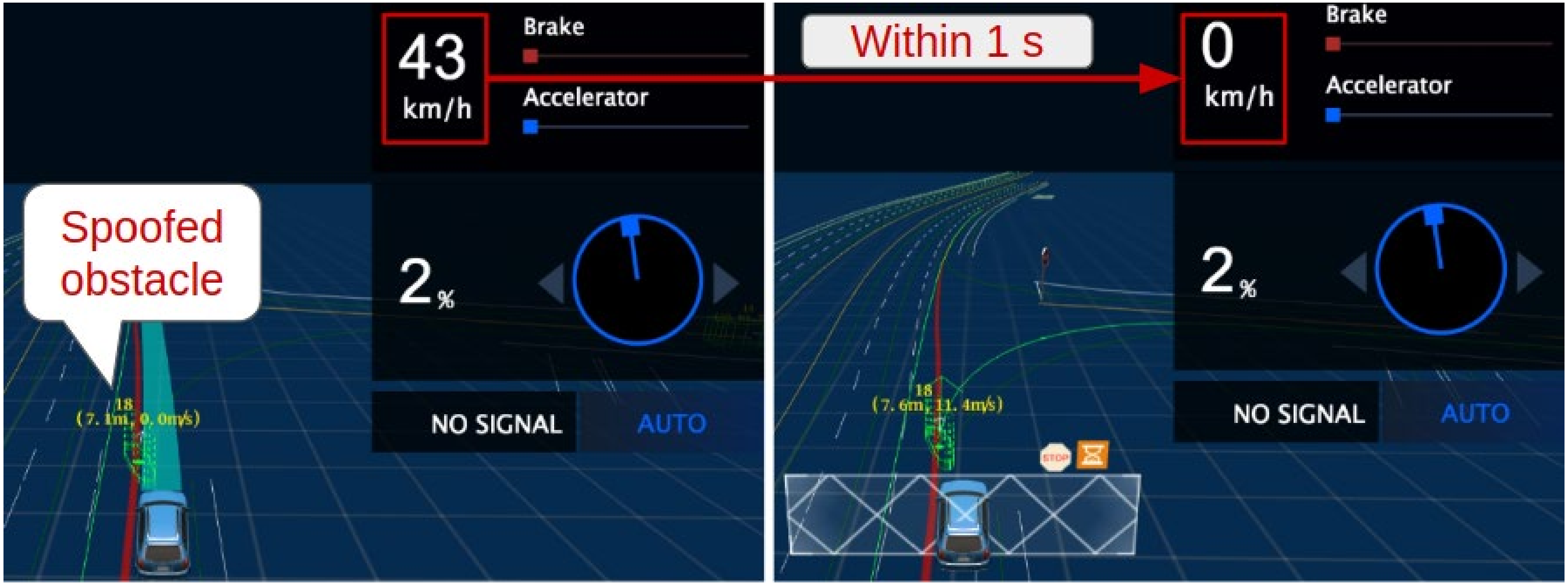
Analysis results

- Successfully find attack input that can inject fake object!


Simulator: Apollo's SimControl
Victim vehicle running Apollo
Attack: Shoot laser from road-side device
Created spoofed obstacle

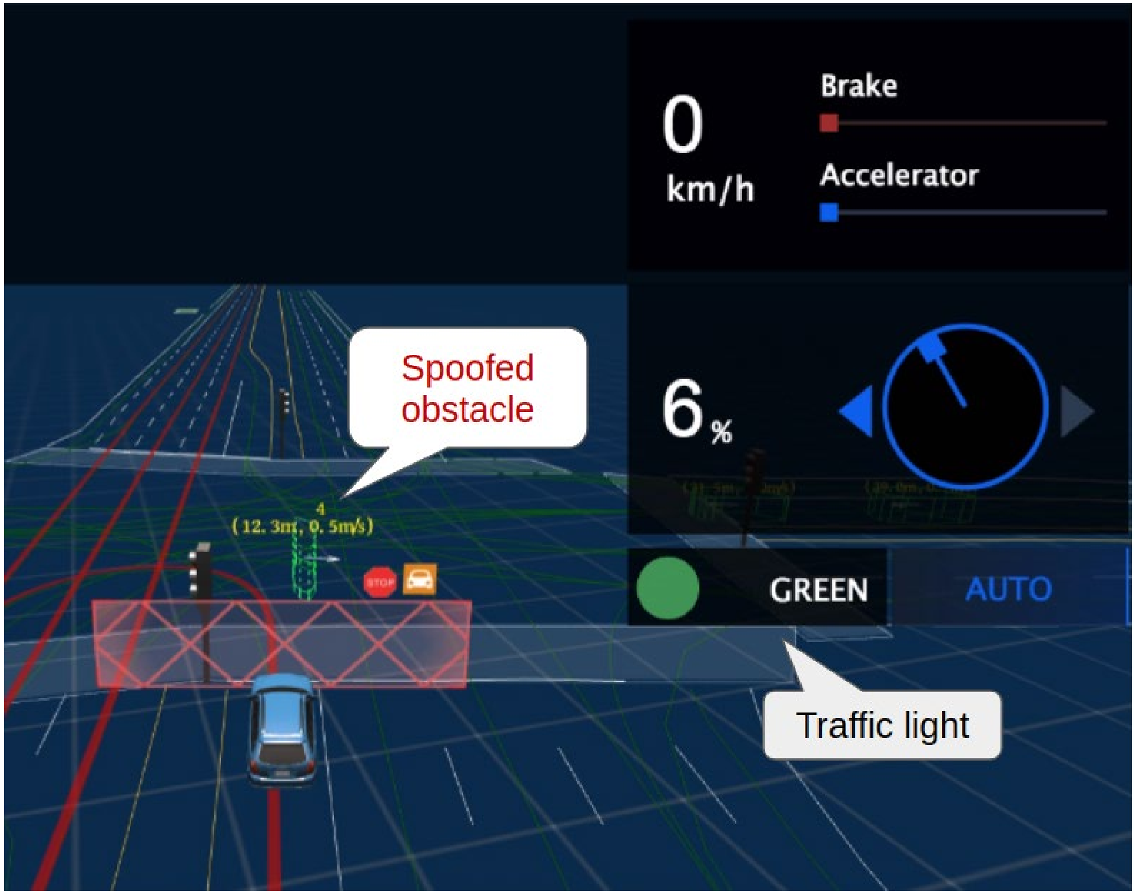
Security implication: Emergency brake attack

- Cause AV to decrease speed from ***43km/h*** **to** ***0 km/h*** within ***1 sec!***



Security implication: Car "freezing" attack

- **"Freeze" an AV** at an intersection ***forever***!

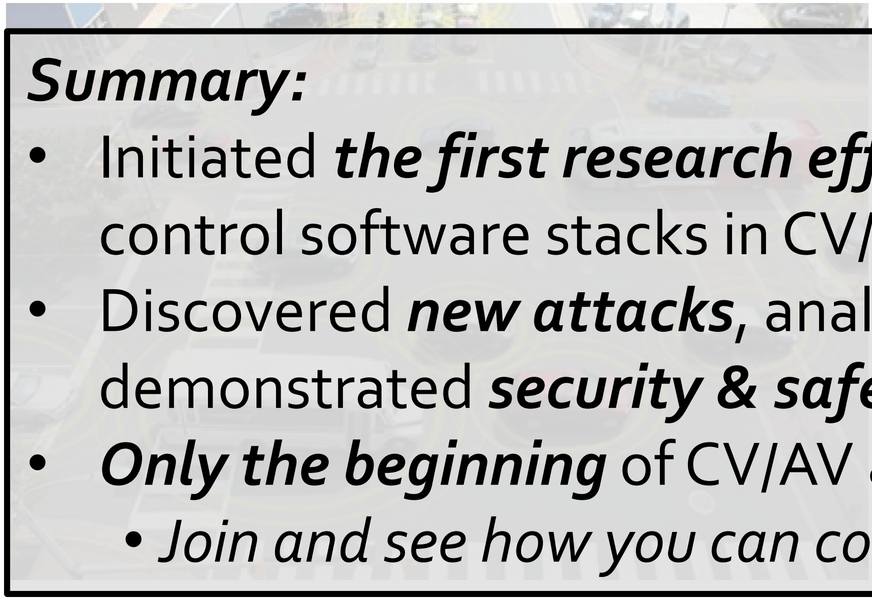


Spoofed obstacle

Traffic light

Recent interest: Autonomy software security in smart transportation

Connected Vehicle (CV)



Autonomous Vehicle (AV)

Summary:

- Initiated ***the first research efforts*** to perform security analysis of control software stacks in CV/AV systems
- Discovered ***new attacks***, analyzed ***root causes***, and demonstrated ***security & safety implications***
- ***Only the beginning*** of CV/AV autonomy s/w security research
  - *Join and see how you can contribute!*

[ISOC NDSS'18]

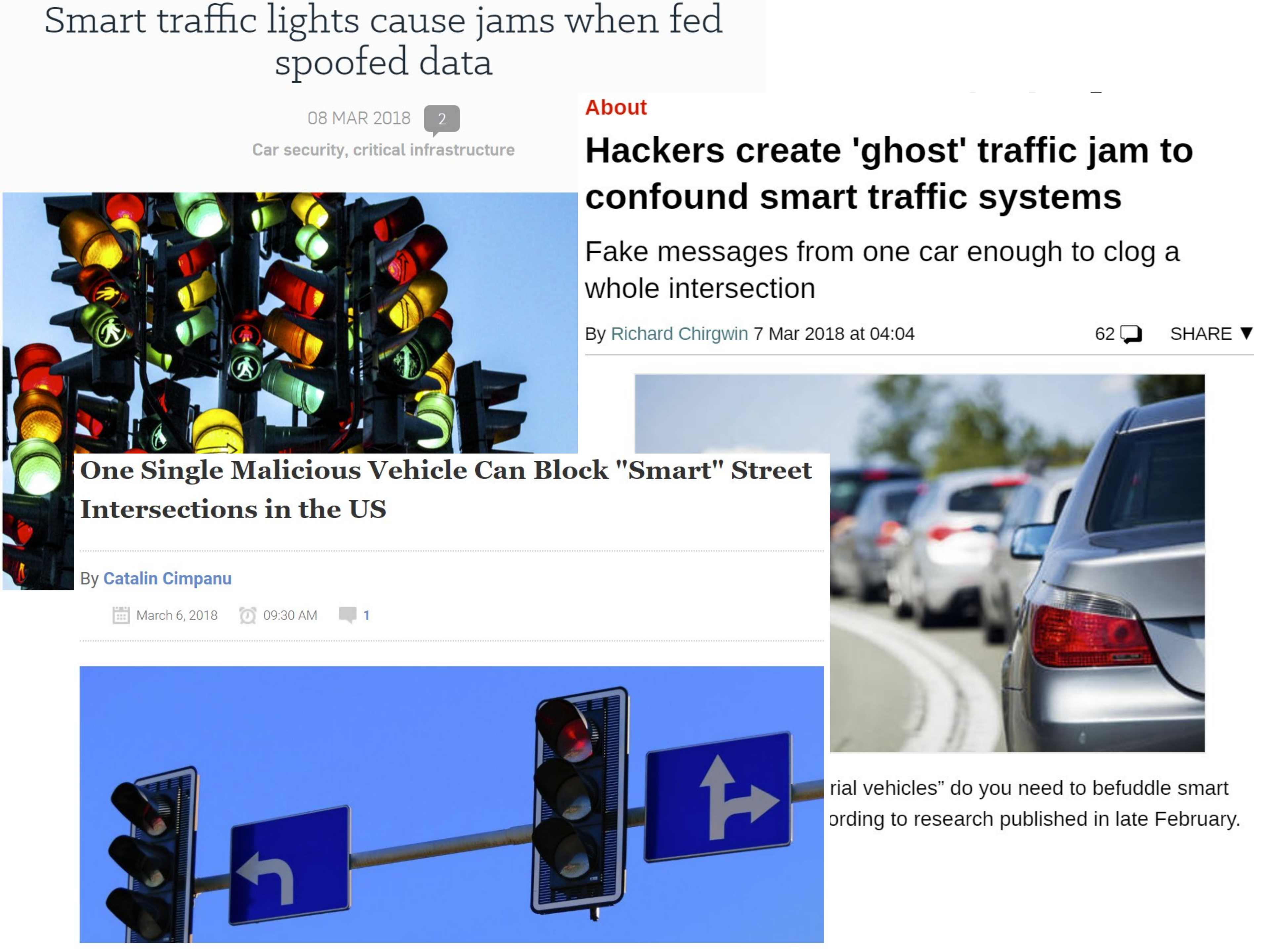
First software security analysis of a CV-based transportation system

[ACM CCS'19]

First software security analysis of LiDAR-based AV perception

Why of interest to you to join?

- For ***enthusiasts*** about self driving & smart transp.
  - Learn technology detail, & how to hack it



Smart traffic lights cause jams when fed spoofed data

08 MAR 2018 2

Car security, critical infrastructure

About

Hackers create 'ghost' traffic jam to confound smart traffic systems

Fake messages from one car enough to clog a whole intersection

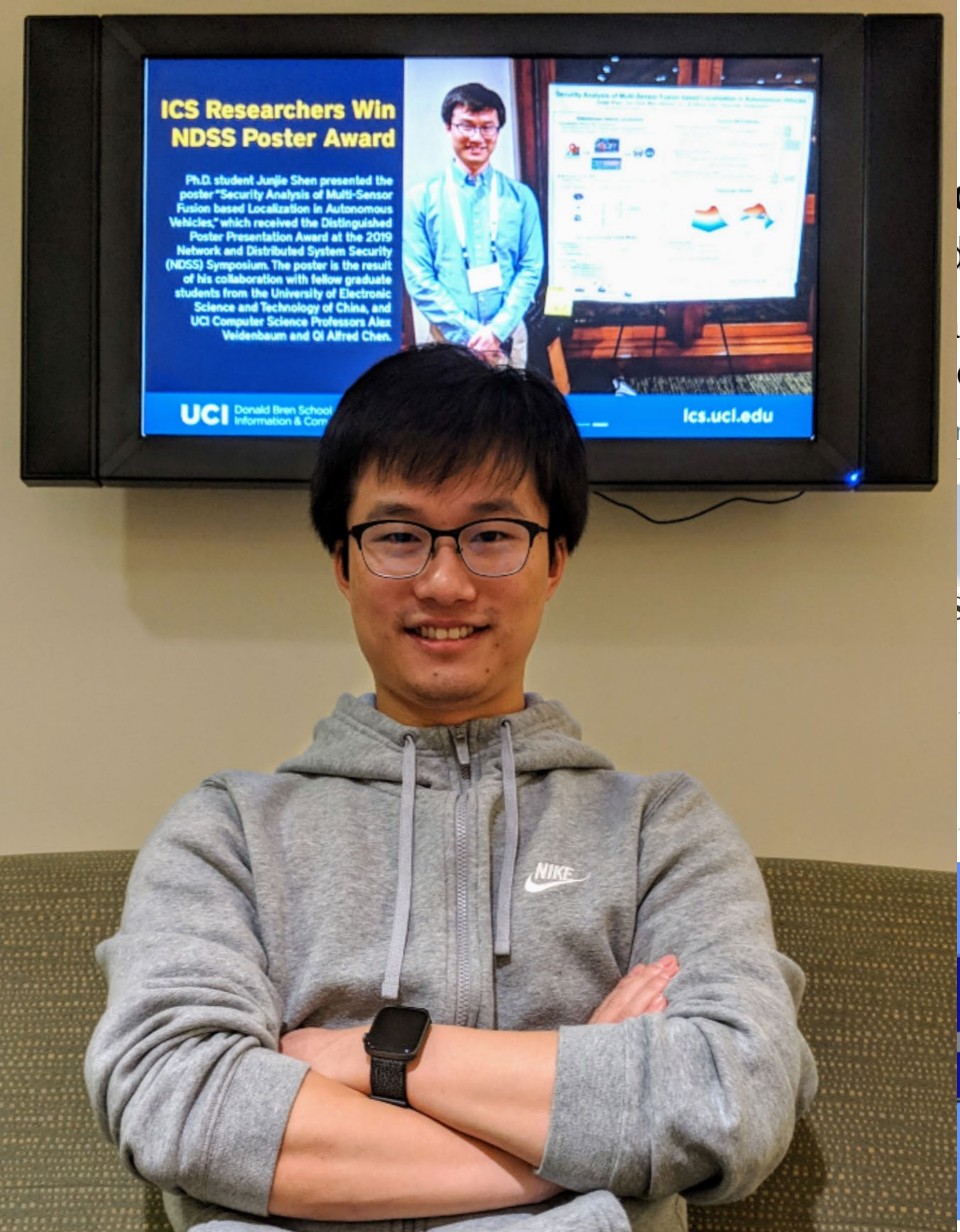
By Richard Chirgwin 7 Mar 2018 at 04:04 62 SHARE ▼

rial vehicles” do you need to befuddle smart
ording to research published in late February.

One Single Malicious Vehicle Can Block "Smart" Street Intersections in the US

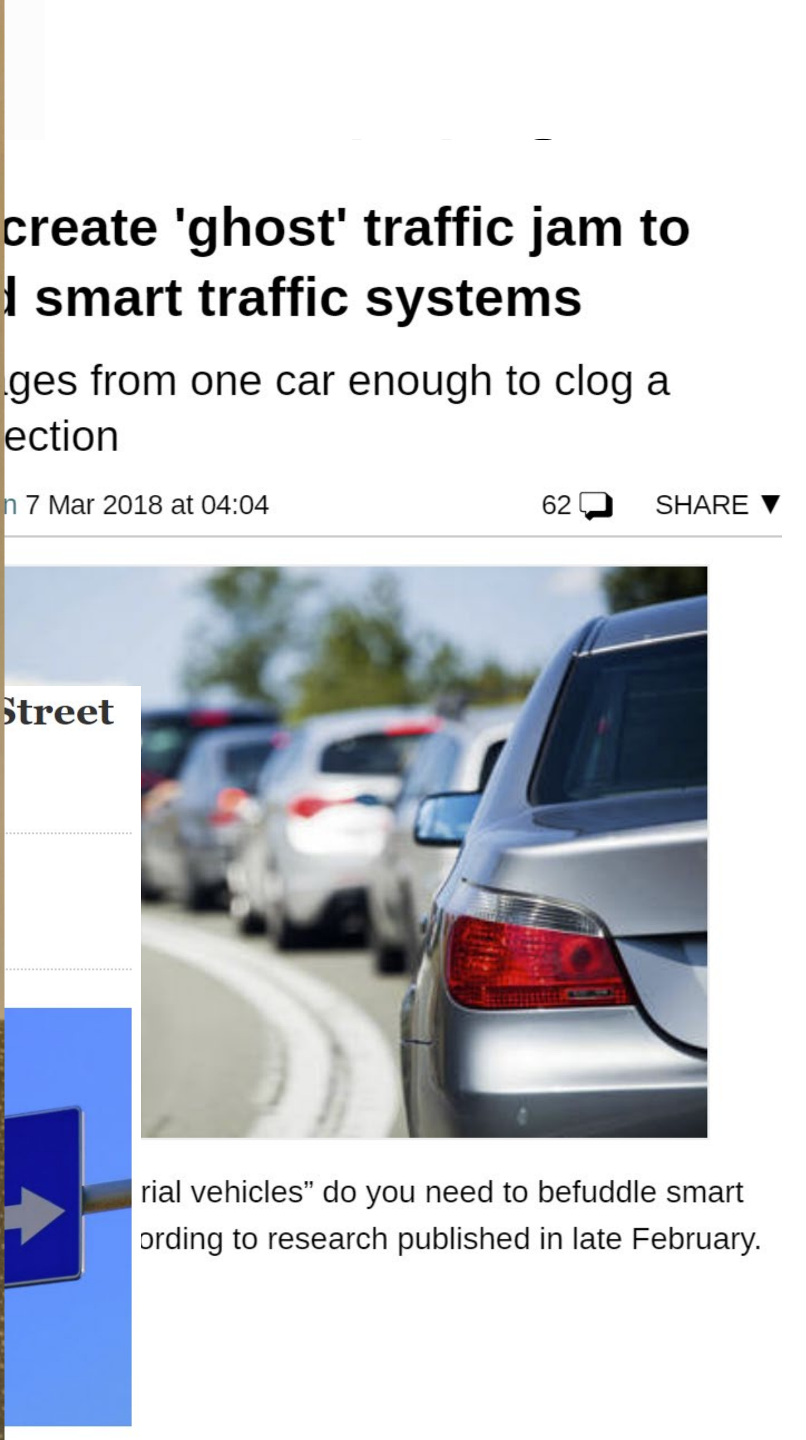
By Catalin Cimpanu

March 6, 2018 09:30 AM 1



ICS Researchers Win NDSS Poster Award

Ph.D. student Junjie Shen presented the poster “Security Analysis of Multi-Sensor Fusion based Localization in Autonomous Vehicles,” which received the Distinguished Poster Presentation Award at the 2019 Network and Distributed System Security (NDSS) Symposium. The poster is the result of his collaboration with fellow graduate students from the University of Electronic Science and Technology of China, and UCI Computer Science Professors Alex Veidenbaum and Qi Alfred Chen.

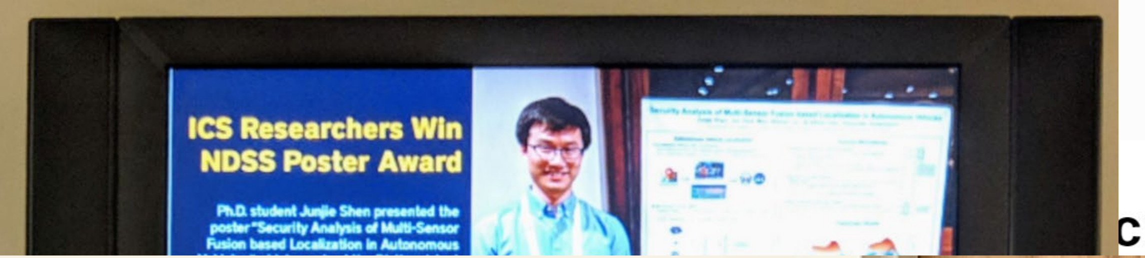


create 'ghost' traffic jam to l smart traffic systems

ges from one car enough to clog a ection

n 7 Mar 2018 at 04:04 62 SHARE ▼

rial vehicles” do you need to befuddle smart ording to research published in late February.



ICS Researchers Win NDSS Poster Award

Ph.D. student Junjie Shen presented the poster "Security Analysis of Multi-Sensor Fusion based Localization in Autonomous

create 'ghost' traffic jam to

CS Professor Qi Alfred Chen

won two out of four awards (Most Amusing Award and Most Engaging Award) for his talk

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

at the 2019 USENIX Summit on Hot Topics in Security.

Session 2
Talk 1
— Qi Alfred Chen —
Security Analysis of CV/AV Systems
Attack always possible. What is accepted
How about attestation of vehicle/infrastructure identity
Any ideas on Control Hijack Attacks to AV?
UxWorKs research needed!
Do the developing cars' are these issues fixed?
Connected Services are many. Does the Cost for Security depend on Services?
AV Level? Drivers care on Level 3. Big issue comes over Level 4
UCI Donald Bren School of Information & Computer Sciences

Why of interest to you to join?

- For ***enthusiasts*** about self driving & smart transp.
  - Learn technology detail, & how to hack it (and *gain fame* ☺)
- For ***job hunters***
  - Your relevant knowledge & hacking experience can help get internship/full-time in CV/AV companies
- For students want to do ***grad school (esp. PhD)***
  - Research experience (& maybe *papers*) in hot research topic

How can you contribute?

- Join **on-going research projects** led by my PhD students
  - *This way you can have clear guidance, not alone*
- Example projects:
  - Help build a ***simulator*** for AV security analysis/testing
  - Help develop ***new security analysis methods***
  - Help develop ***automatic AV bug discovery tools***
- Ofc if you have good research ideas, also happy to let you lead your own projects

Day-to-day experience?

- Expected workload: **at least ~16 hours/week**
  - *So that you can indeed have a **meaningful** experience in learning & research*
- Frequent discussion with my PhD students
  - Will try to assign you a desk in my lab
- Lots of coding & critical thinking
  - Language: mostly *C/C++/C#* and *python*

Conclusion

- Call for research involvement: **Autonomy software security in CV/AV systems**
  - Discover ***new attacks***, analyze ***root causes***, demo ***security/safety implications***
- Join for ***CV/AV related knowledge***, ***hacking***, ***intern/full-time***, ***research experience***, or just ***fame*** ☺
- If interest, please contact me and ***fill out this form***
  - https://forms.gle/S7QzGkVMTcLzFvcT8

Contact:

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