On the Cyber-Physical Security of Connected and Autonomous Driving Systems

Alfred Chen

Assistant Professor, UC Irvine

UCIRVINE

AS^{2}Guard

Autonomous & Smart Systems Guard Research Group

A bit about myself & my group

- Assistant Professor, Computer Science, UC Irvine (2018 -)
  - Ph.D., University of Michigan
- Group: **AS^{2}Guard** (Autonomous & Smart Systems **Guard**)
- Expertise: **AI/Systems/Network Security**, mainly in **mobile/CPS/IoT**

AS^{2}Guard

Autonomous & Smart Systems
Guard Research Group

Cyber

Physical

Security
www

Our research so far in mobile/CPS/IoT security

- **CPS AI Security**
  - **Autonomous Driving (AD)** [ACM CCS'19, Usenix Security'20 (a), '20 (b), '21, IEEE S&P'21, NDSS'22, CVPR'22, ICLR'20]
  - **Intelligent transportation** [NDSS'18, TRB'18,'19,'20, ITS'21]
- **Network Security**
  - **Connected Vehicle (CV)** [Usenix Security'21]
  - **Automotive IoT** [Usenix Security'20, NDSS'20]
  - **Network protocol** [ACM CCS'15,'18, IEEE S&P'16]
- **UI (User Interface) Security**
  - **Smartphone** [Usenix Security'14, MobiSys'19]
- **Access Control / Policy Enforcement**
  - **Smartphone** [NDSS'16]
  - **Smart home** [NDSS'17]
- **Side Channel**
  - **Smartphone** [Usenix Security'14]
  - **Network** [ACM CCS'15]

Most recent focus (2018-): CPS AI security in automotive & transp. domains

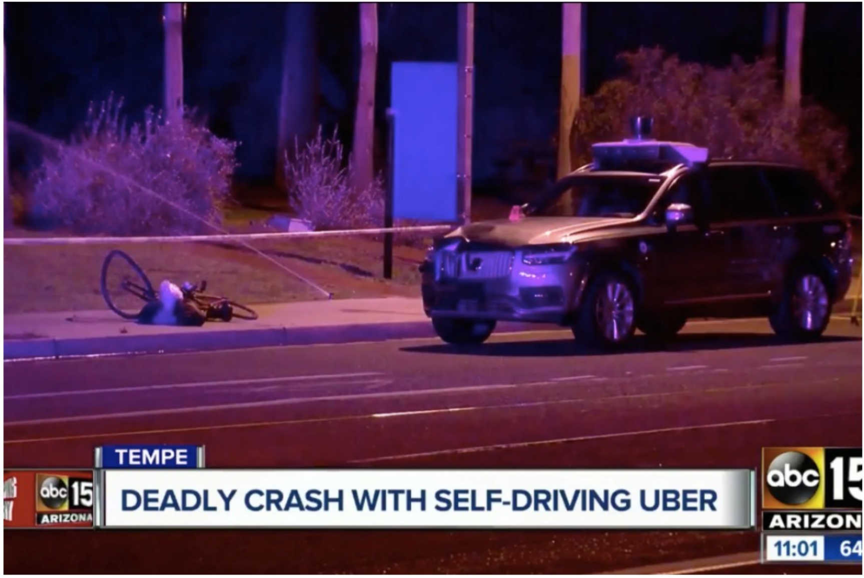
- **CPS AI Security**
  - **Autonomous Driving (AD)** [ACM CCS'19, Usenix Security'20 (a), '20 (b), '21, IEEE S&P'21, NDSS'22, CVPR'22, ICLR'20]
  - **Intelligent transportation** [NDSS'18, TRB'18,'19,'20, ITS'21]
- **Network Security**
  - **Connected Vehicle (CV)** [Usenix Security'21]
  - **Automotive IoT** [Usenix Security'20, NDSS'20]
  - **Network protocol** [ACM CCS'15,'18, IEEE S&P'16]
- **UI (User Interface) Security**
  - **Smartphone** [Usenix Security'14, MobiSys'19]
- **Access Control / Policy Enforcement**
  - **Smartphone** [NDSS'16]
  - **Smart home** [NDSS'17]
- **Side Channel**
  - **Smartphone** [Usenix Security'14]
  - **Network** [ACM CCS'15]

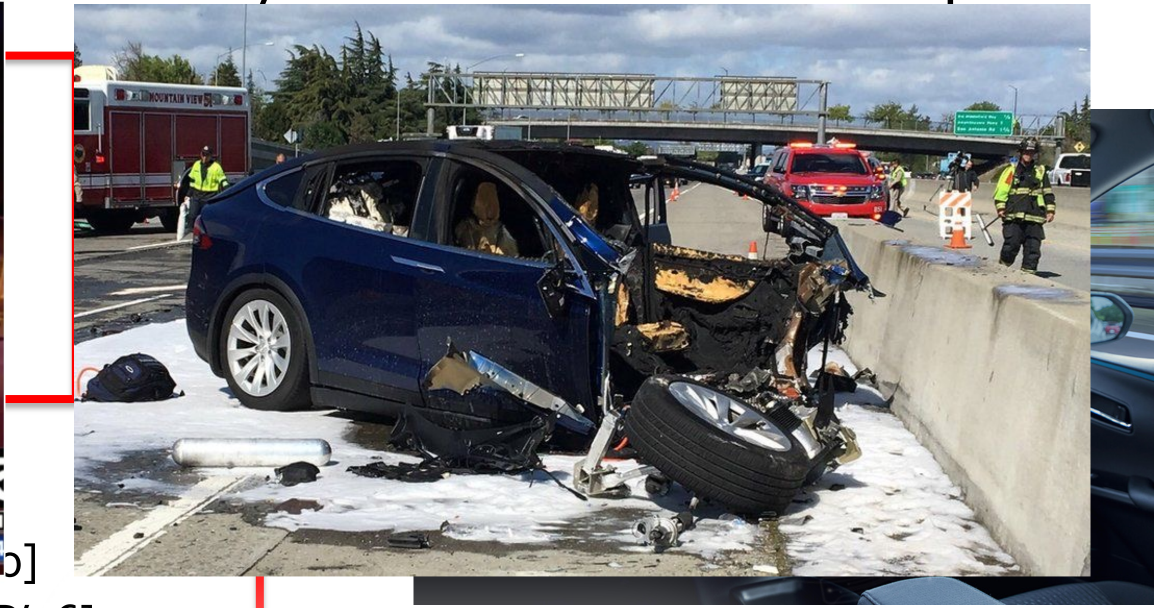
Autonomous Driving (AD)

V2X-based Intelligent Transp.

Most recent focus (2018-): CPS AI security in automotive & transp. domains

- CPS A
  - Aut
    User
    NDS
  - Inte
    TRB
- Netw
  - Con
  - Aut]
  - Network protocol [ACM CCS'15,'18, IEEE S&P'16]
- UI (User Interface) Security
  - Smartphone [Usenix Security'14, MobiSys'19]
- Access Control / Policy Enforcement
  - Smartphone [NDSS'1
  - Smart home [NDSS'
- Side Channel
  - Smartphone [Usenix Security'1
  - Network [ACM CCS'15]





V2X-based Intelligent Transp.

Most recent focus (2018-): CPS AI security in automotive & transp. domains

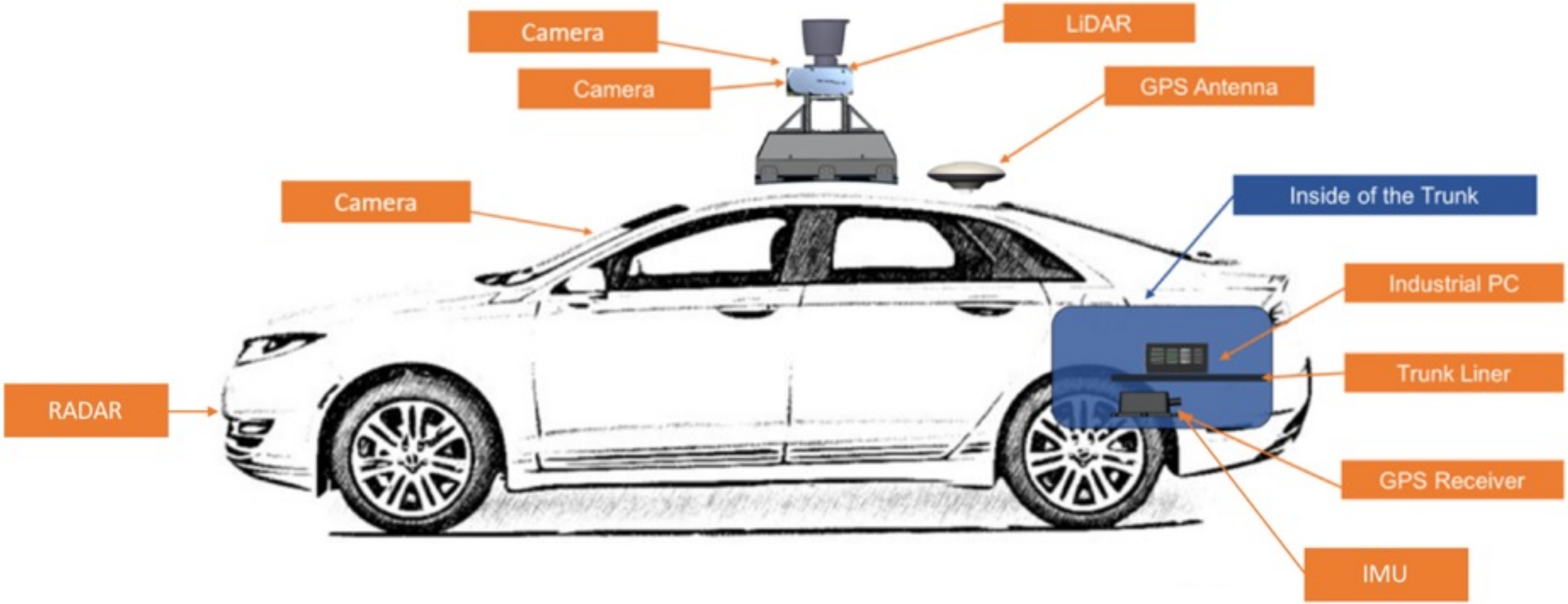
- **CPS AI Security**
  - **Autonomous Driving (AD)** [ACM CCS'19, Usenix Security'20 (a), '20 (b), '21, IEEE S&P'21, NDSS'22, CVPR'22, ICLR'20]
  - **Intelligent transportation** [NDSS'18, TRB'18,'19,'20, ITS'21]
- **Network Security**
  - **Connected Vehicle (CV)** [Usenix Security'21]
  - **Automotive IoT** [Usenix Security'20, NDSS'20]
  - **Network protocol** [ACM CCS'15,'18, IEEE S&P'16]
- **UI (User Interface) Security**
  - **Smartphone** [Usenix Security'14, MobiSys'19]
- **Access Control / Policy Enforcement**
  - **Smartphone** [NDSS'16]
  - **Smart home** [NDSS'17]
- **Side Channel**
  - **Smartphone** [Usenix Security'14]
  - **Network** [ACM CCS'15]

Autonomous Driving (AD)

V2X-based Intelligent Transp.

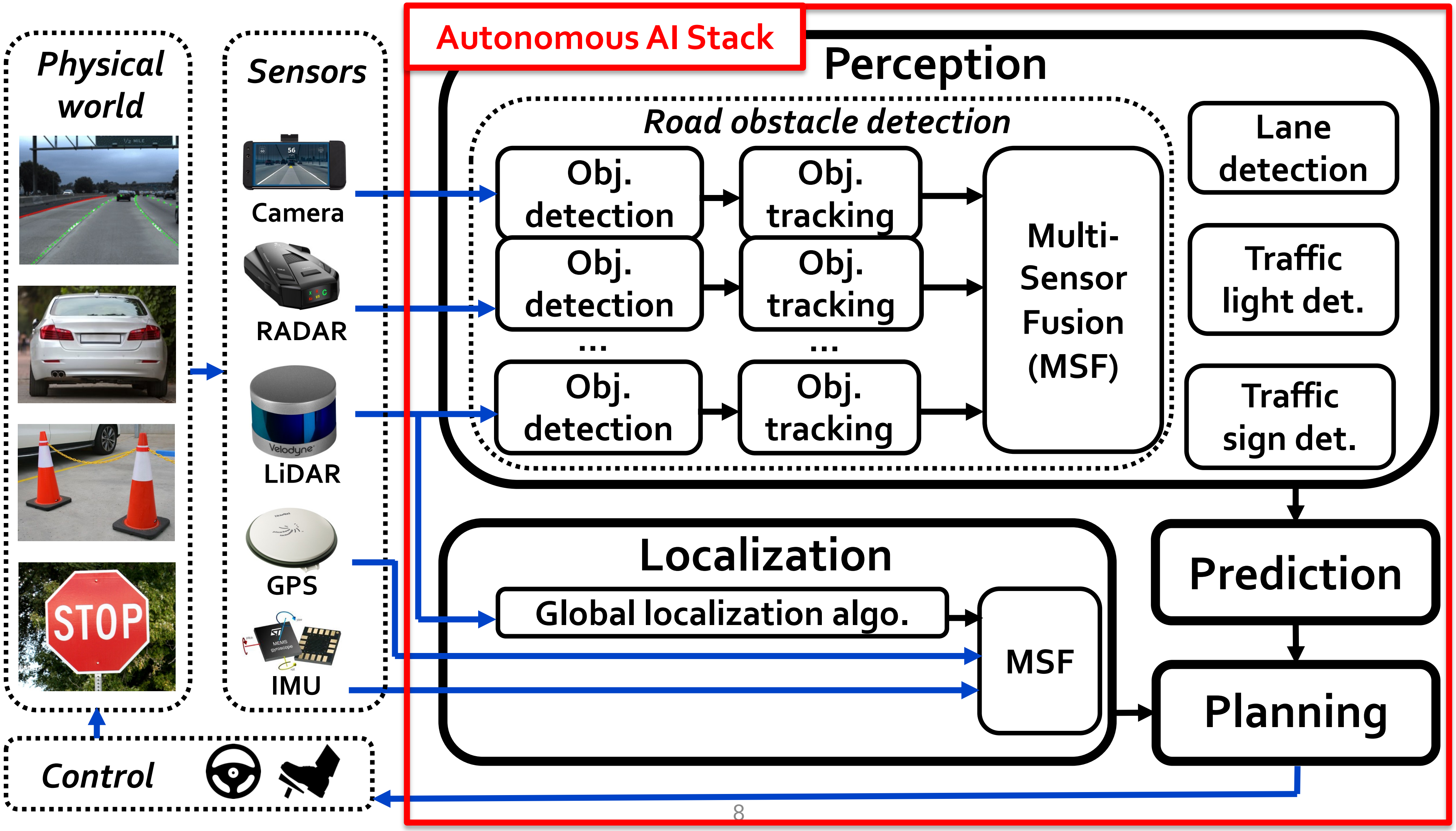
Background: Autonomous Driving (AD) technology

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

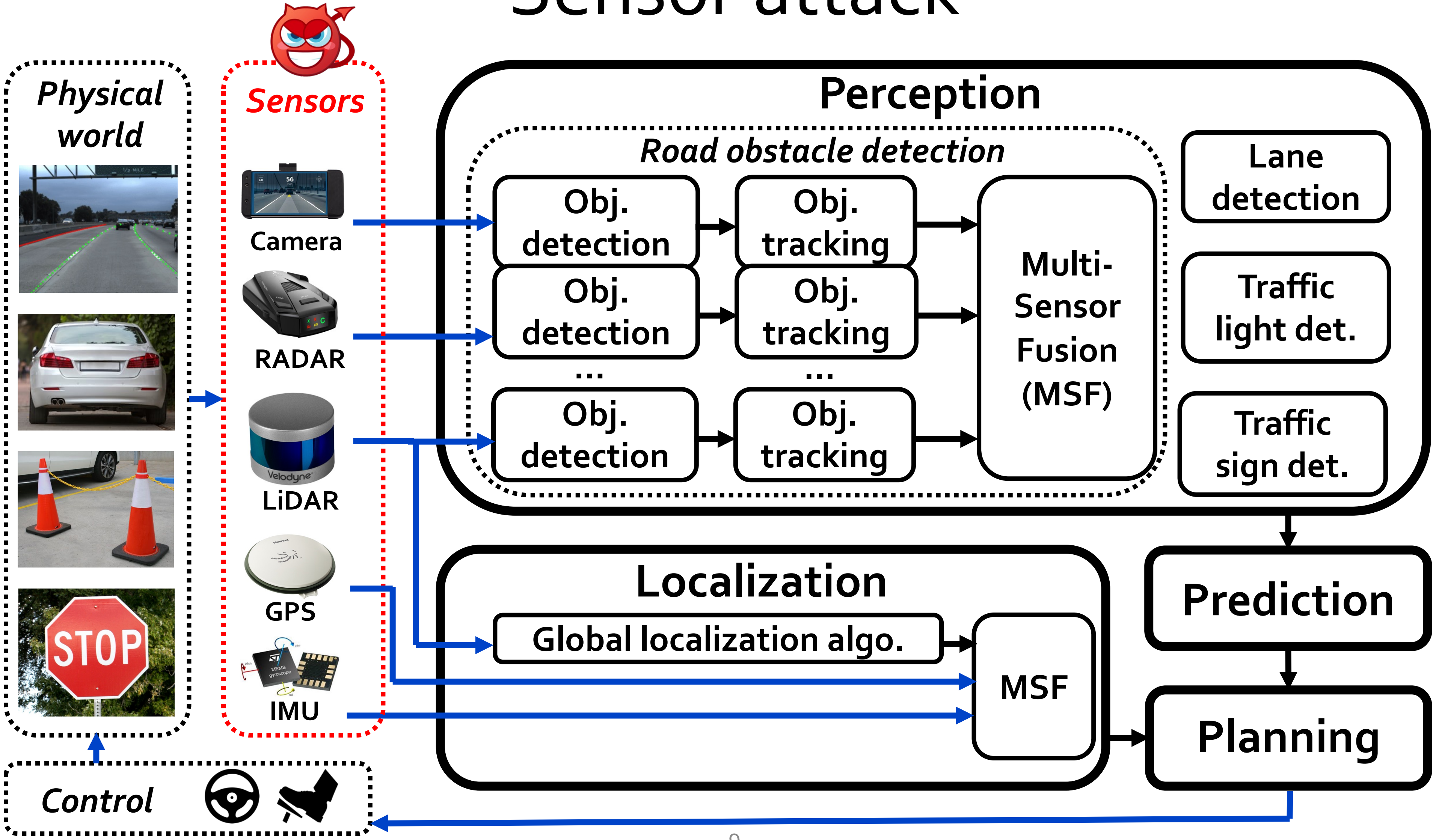


(*Image source: https://github.com/ApolloAuto/apollo)

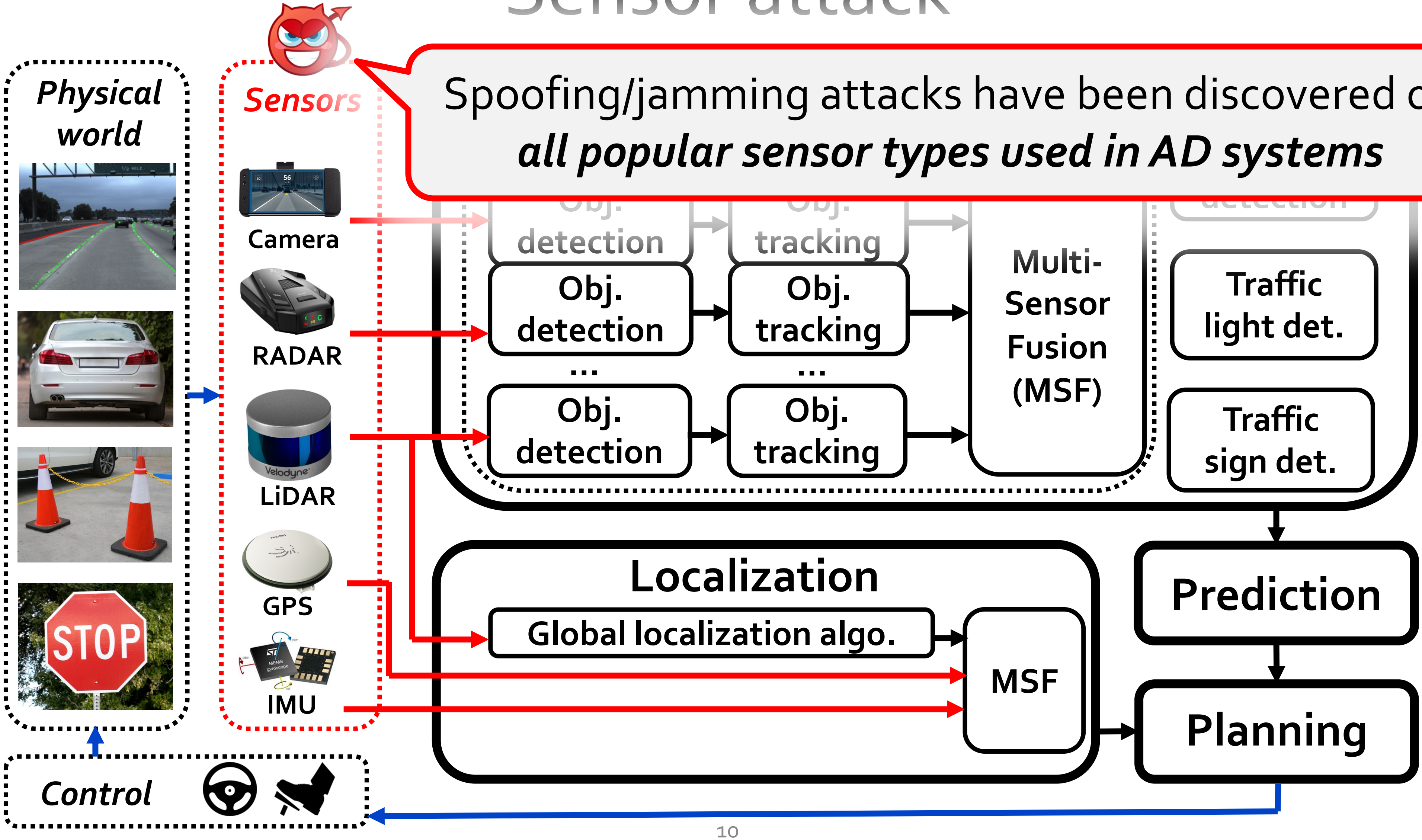
Background: System architecture of industry-grade AD



General & fundamental attack surface #1: Sensor attack

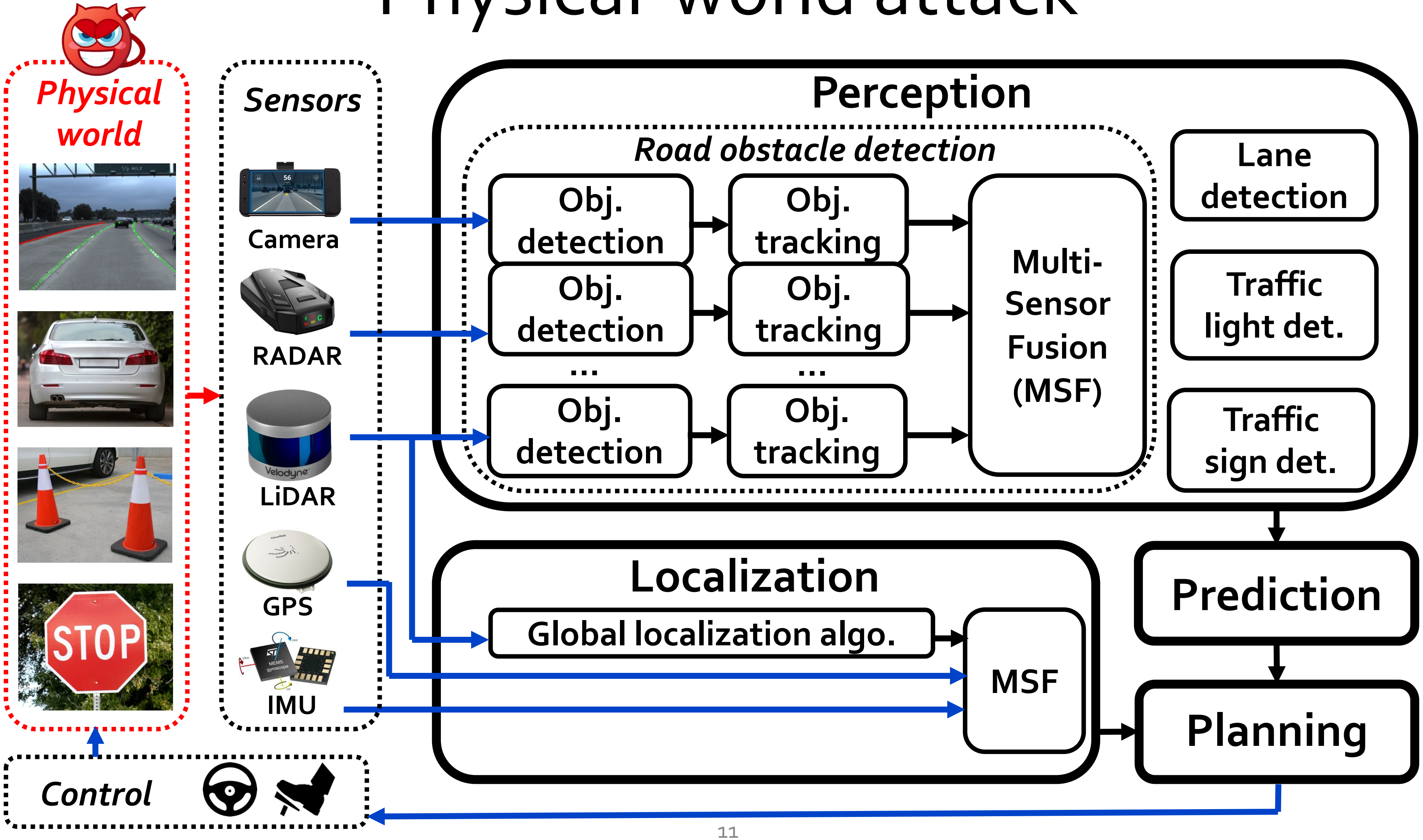


General & fundamental attack surface #1: Sensor attack

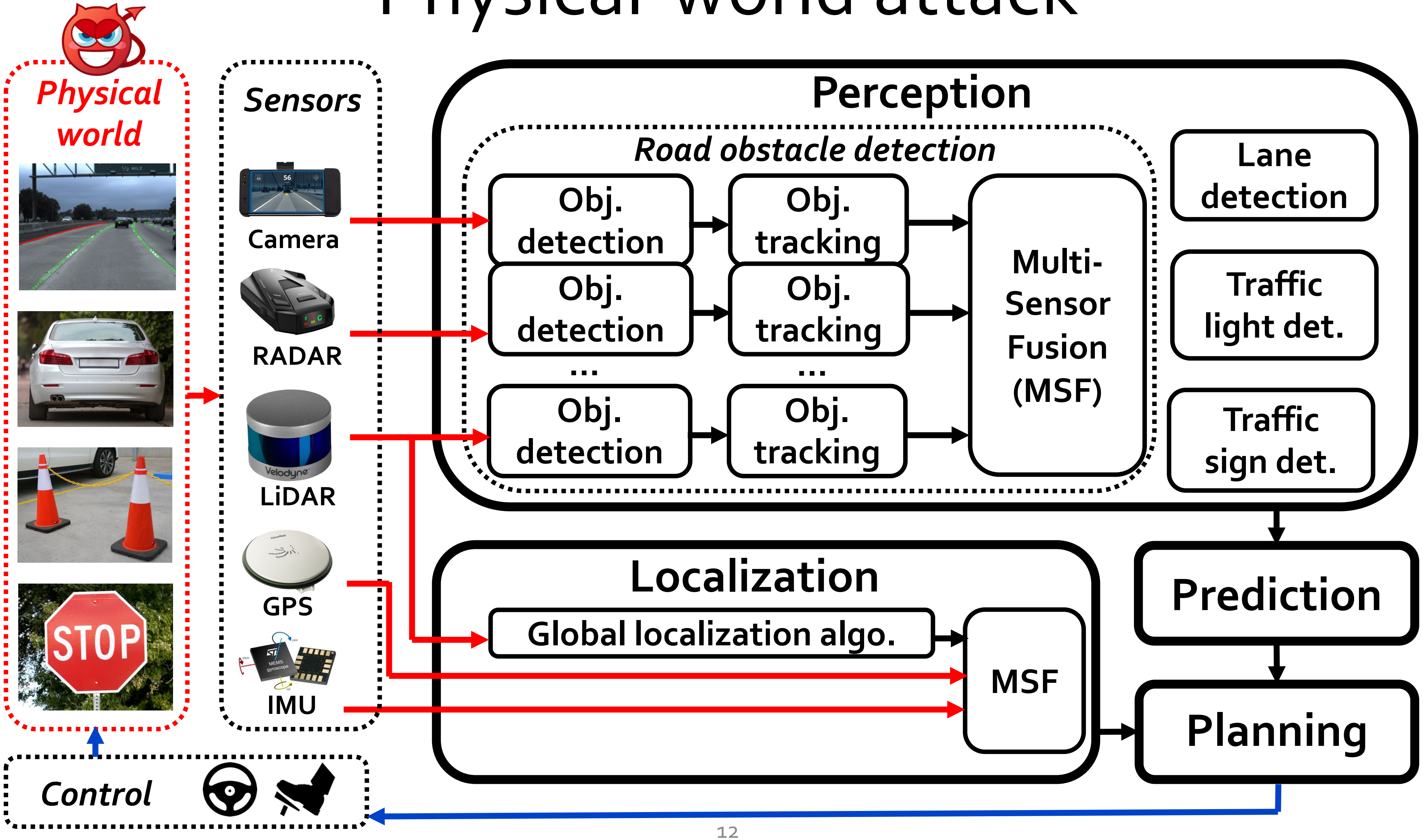


Spoofing/jamming attacks have been discovered on ***all popular sensor types used in AD systems***

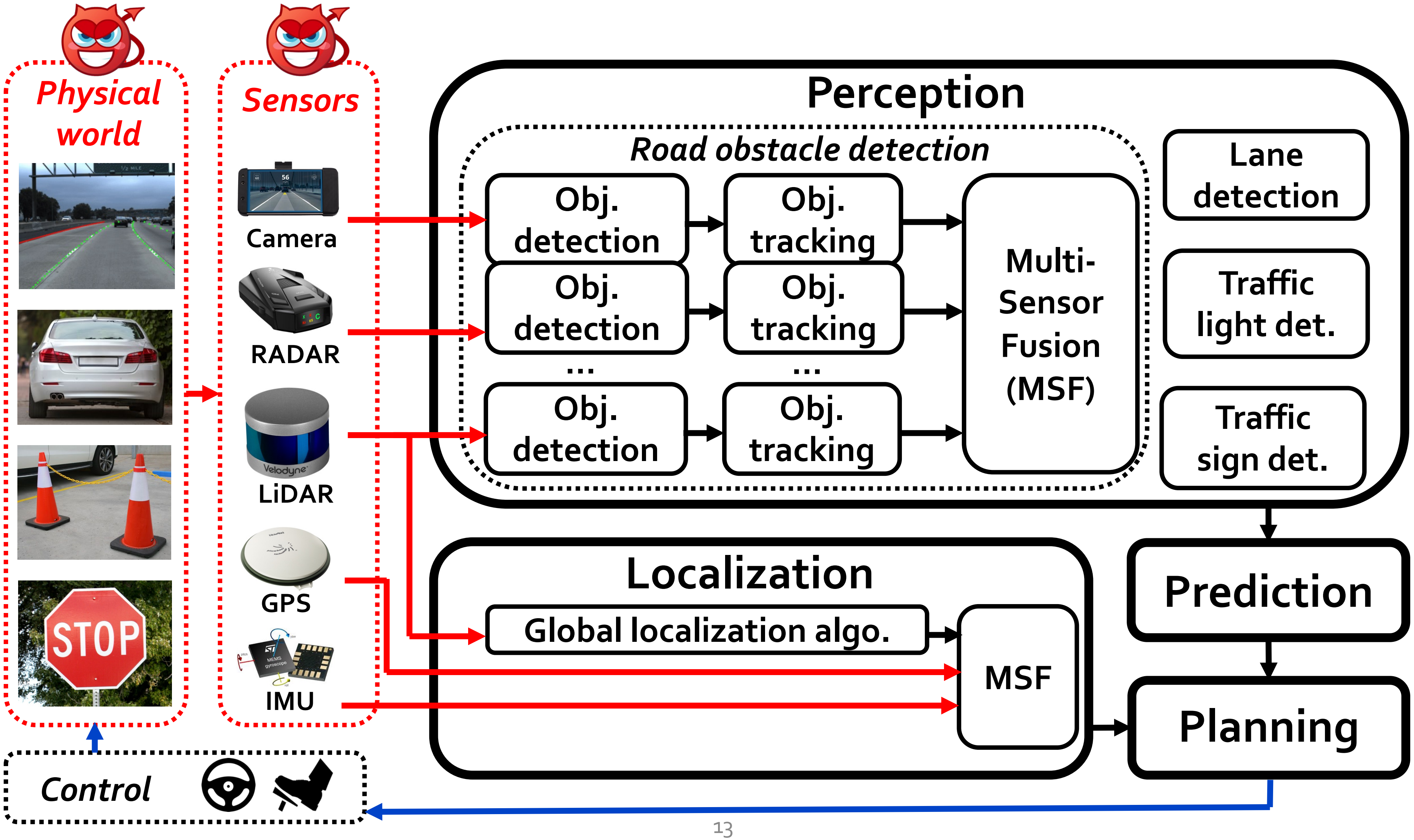
General & fundamental attack surface #2: Physical-world attack

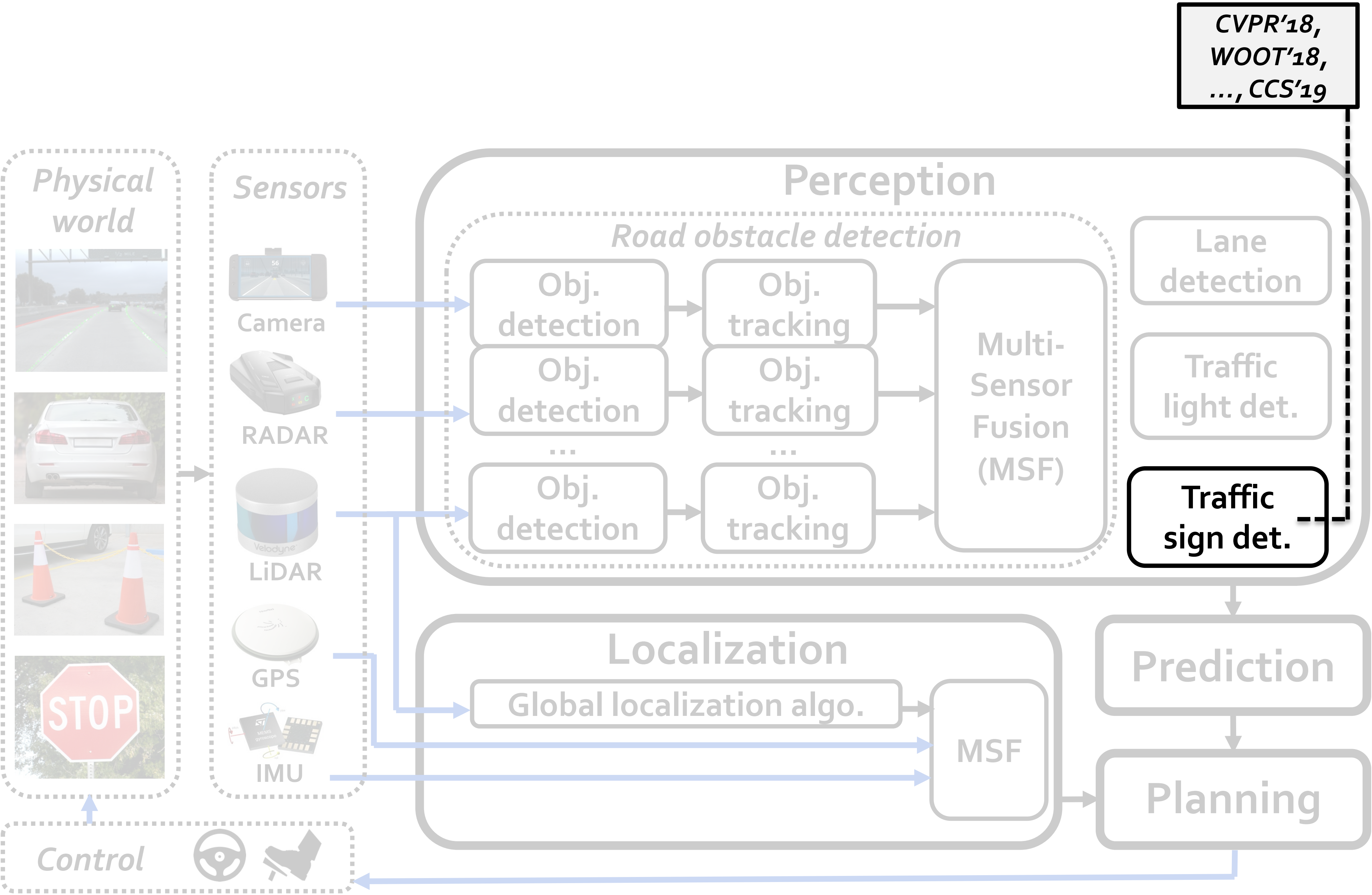


General & fundamental attack surface #2: Physical-world attack

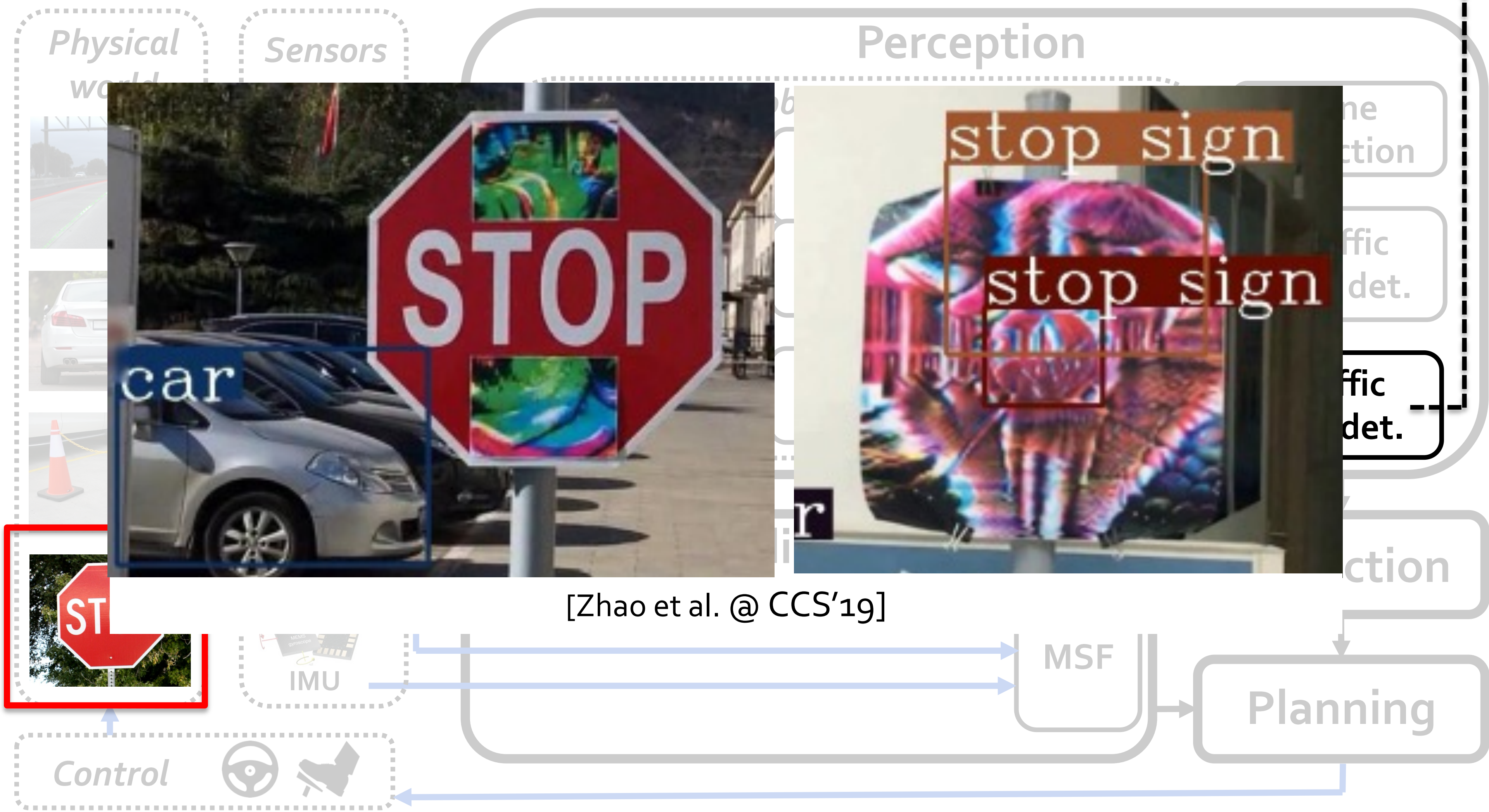


Both are considered in my research

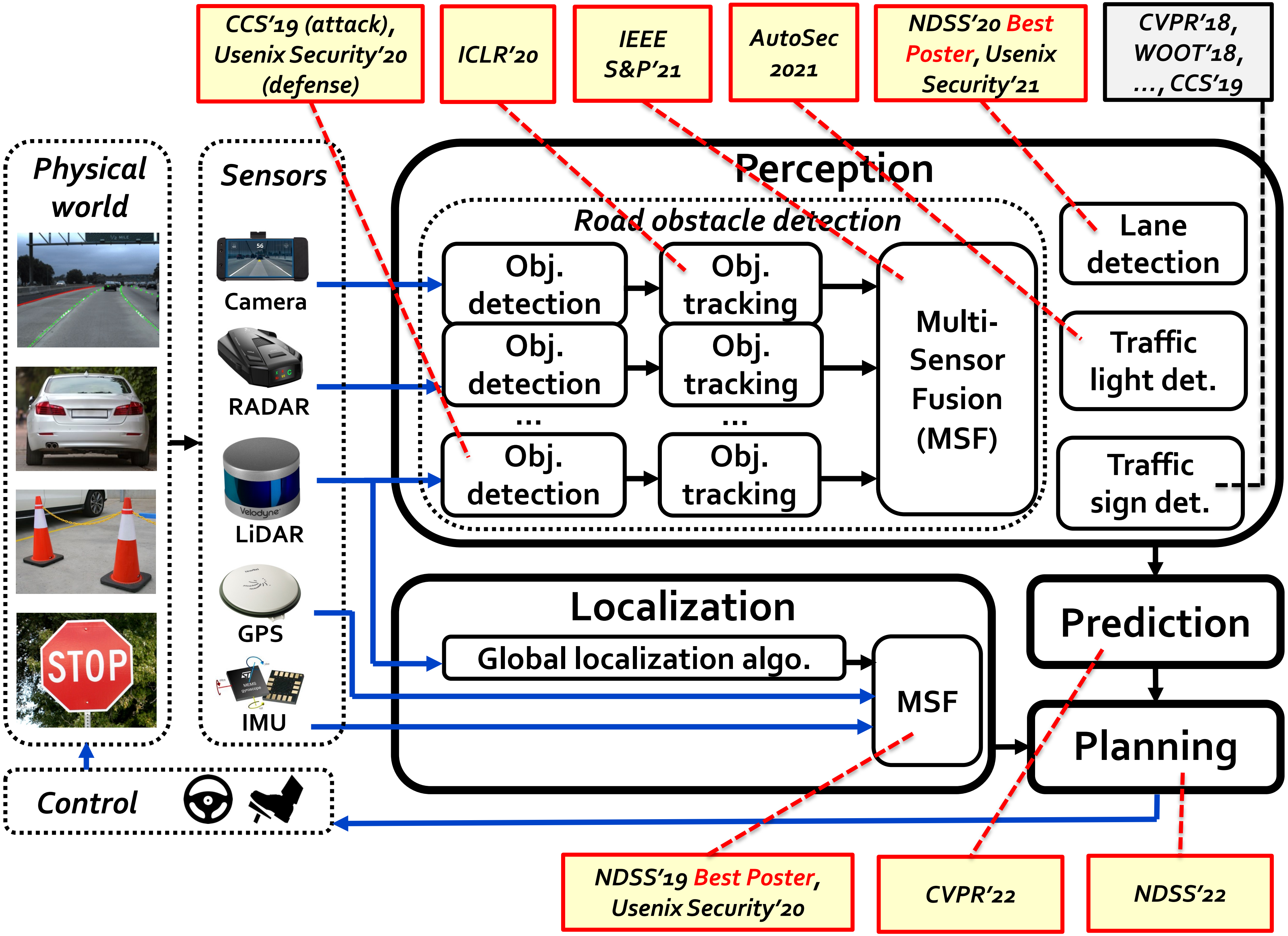



CVPR'18,
WOOT'18,
…, CCS'19
Physical world
STOP
Sensors
Camera
RADAR
LiDAR
Velodyne
GPS
IMU
Control
Perception
Road obstacle detection
Obj. detection
Obj. tracking
Obj. detection
Obj. tracking
…
…
Obj. detection
Obj. tracking
Multi-Sensor Fusion (MSF)
Lane detection
Traffic light det.
Traffic sign det.
Localization
Global localization algo.
MSF
Prediction
Planning

CVPR'18, WOOT'18, …, CCS'19



[Zhao et al. @ CCS'19]



CCS'19 (attack), Usenix Security'20 (defense)

ICLR'20

IEEE S&P'21

AutoSec 2021

NDSS'20 Best Poster, Usenix Security'21

CVPR'18, WOOT'18, …, CCS'19

Physical world

Sensors

Camera

RADAR

LiDAR

GPS

IMU

Perception

Road obstacle detection

Obj. detection

Obj. tracking

Obj. detection

Obj. tracking

…

…

Obj. detection

Obj. tracking

Multi-Sensor Fusion (MSF)

Lane detection

Traffic light det.

Traffic sign det.

Localization

Global localization algo.

MSF

Prediction

Planning

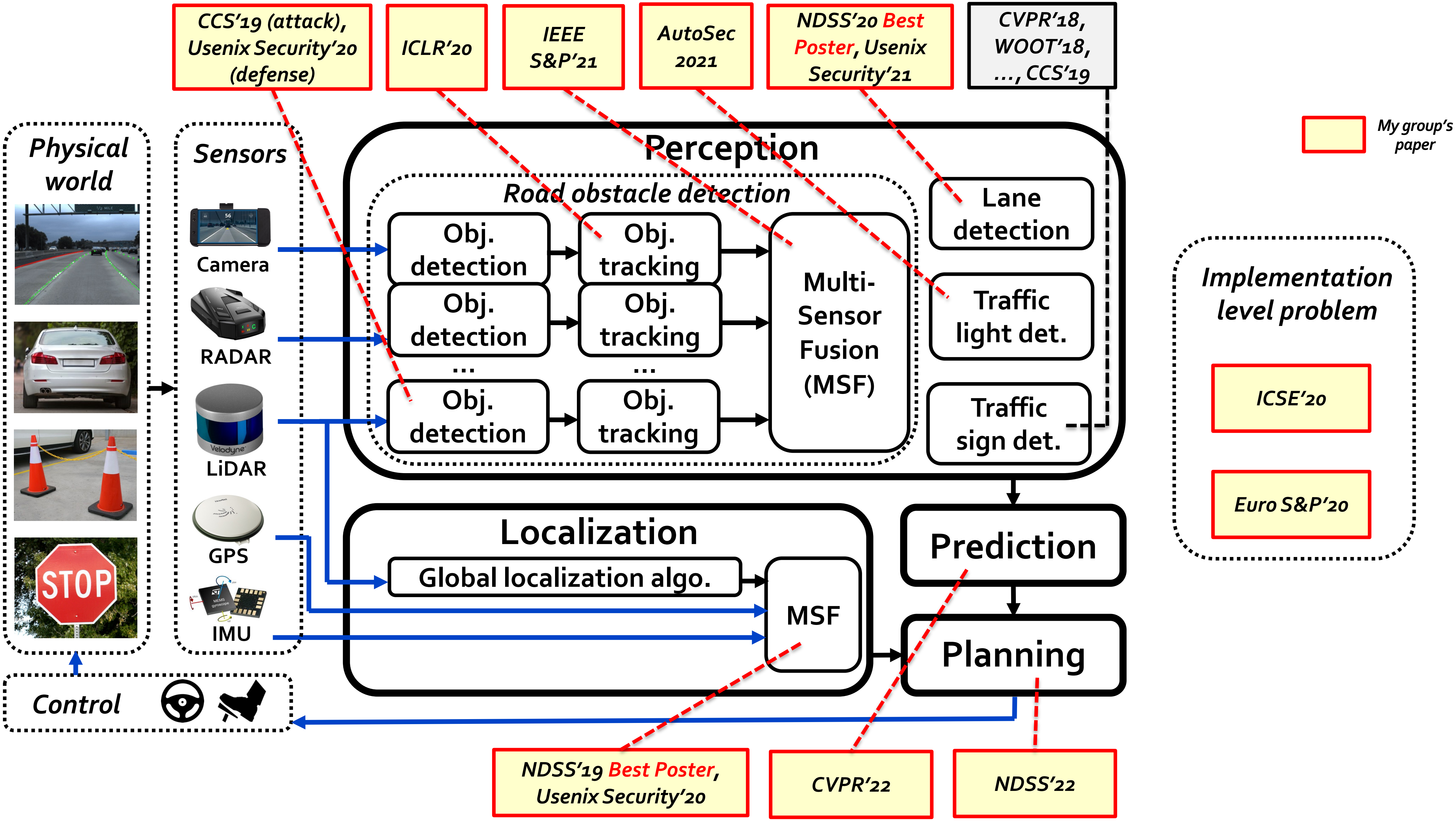
Control

NDSS'19 Best Poster, Usenix Security'20

CVPR'22

NDSS'22

🟨 *My group's paper*



CCS'19 (attack), Usenix Security'20 (defense)

ICLR'20

IEEE S&P'21

AutoSec 2021

NDSS'20 Best Poster, Usenix Security'21

CVPR'18, WOOT'18, …, CCS'19

🟨 My group's paper

Physical world

Sensors

Camera

RADAR

LiDAR

GPS

IMU

Control

Perception

Road obstacle detection

Obj. detection → Obj. tracking

Obj. detection → Obj. tracking

…

Obj. detection → Obj. tracking

Multi-Sensor Fusion (MSF)

Lane detection

Traffic light det.

Traffic sign det.

Localization

Global localization algo.

MSF

Prediction

Planning

Implementation level problem

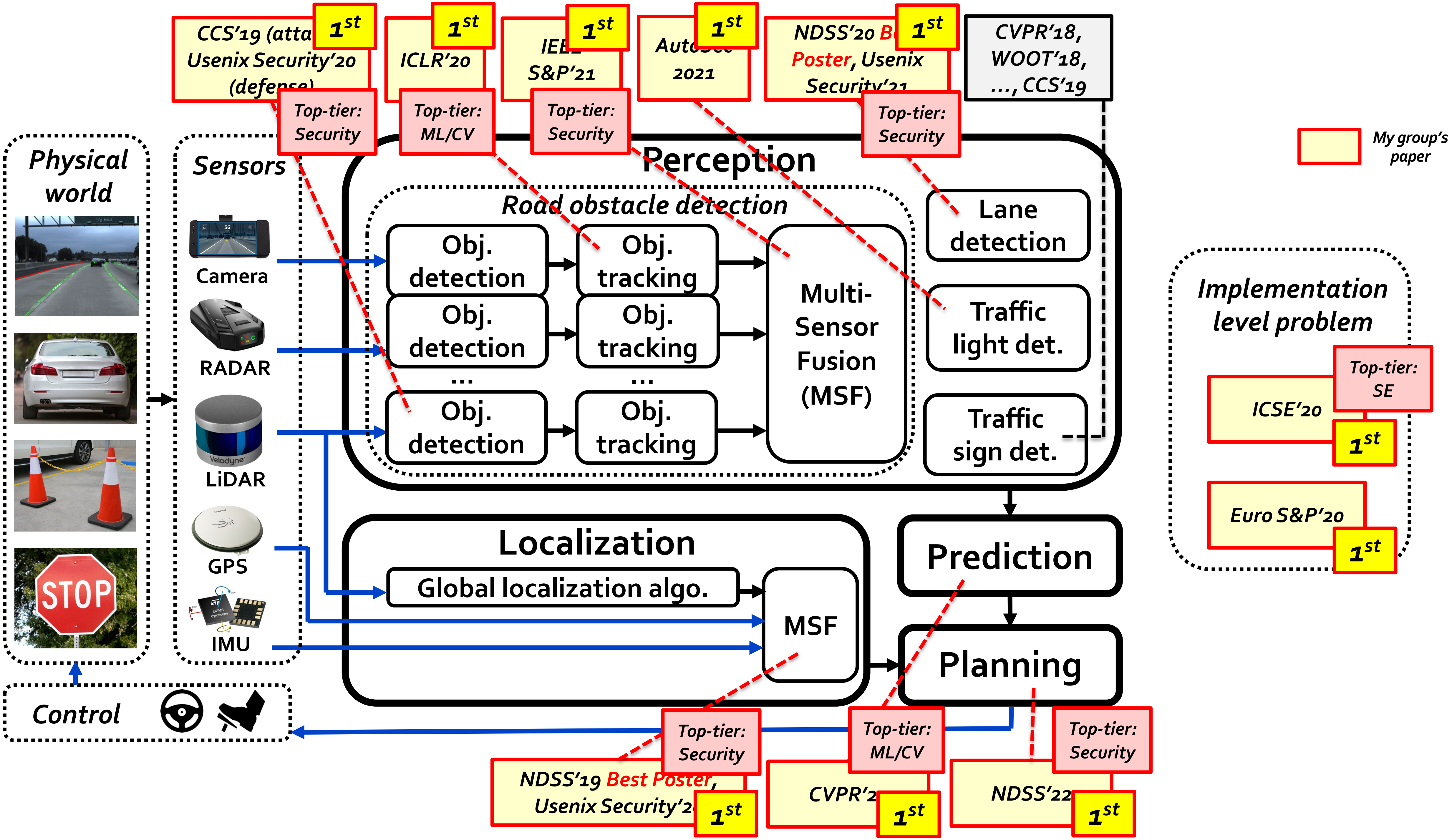
ICSE'20

Euro S&P'20

NDSS'19 Best Poster, Usenix Security'20

CVPR'22

NDSS'22



CCS'19 (atta
Usenix Security'20
(defense)
1st
Top-tier: Security

ICLR'20
1st
Top-tier: ML/CV

IEE
S&P'21
1st
Top-tier: Security

Auto
2021
1st

NDSS'20 B
Poster, Usenix
Security'21
1st
Top-tier: Security

CVPR'18,
WOOT'18,
…, CCS'19

🟨 My group's paper

Physical world

Sensors

Camera

RADAR

LiDAR

GPS

IMU

Perception

Road obstacle detection

Obj. detection → Obj. tracking

Obj. detection → Obj. tracking

…

Obj. detection → Obj. tracking

Multi-Sensor Fusion (MSF)

Lane detection

Traffic light det.

Traffic sign det.

Localization

Global localization algo.

MSF

Prediction

Planning

Control

Implementation level problem

ICSE'20
Top-tier: SE
1st

Euro S&P'20
1st

Top-tier: Security
NDSS'19 Best Poster,
Usenix Security'2
1st

Top-tier: ML/CV
CVPR'2
1st

Top-tier: Security
NDSS'22
1st

CCS'19 (atta 1st
Usenix Security'20
(defense)

1st ICLR'20

1st IEEE S&P'21

1st AutoSec 2021

NDSS'20 Be 1st Poster, Usenix Security'21

CVPR'18, WOOT'18, …, CCS'19

My group's paper

- ***First*** security analysis for **3D object detection**
- Attack vector: LiDAR spoofing

Physical world

RADAR

LiDAR

GPS

IMU

Control

Obj. detection

Obj. tracking

Localization

Global localization algo.

MSF

Prediction

Planning

mplementation level problem

Top-tier: SE

ICSE'20

1st

Top-tier: Security

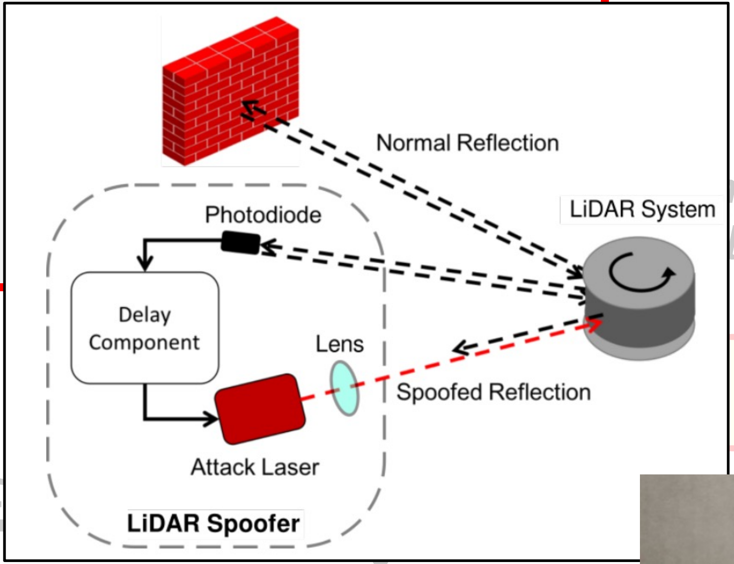
NDSS'19 Best Poster, Usenix Security'2 1st

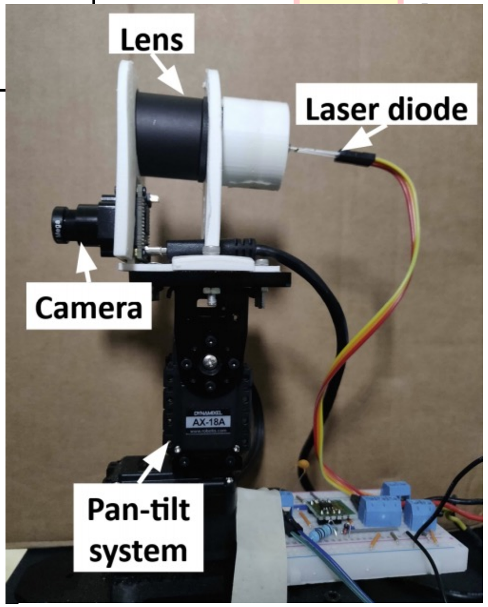
Top-tier: ML/CV

CVPR'2 1st

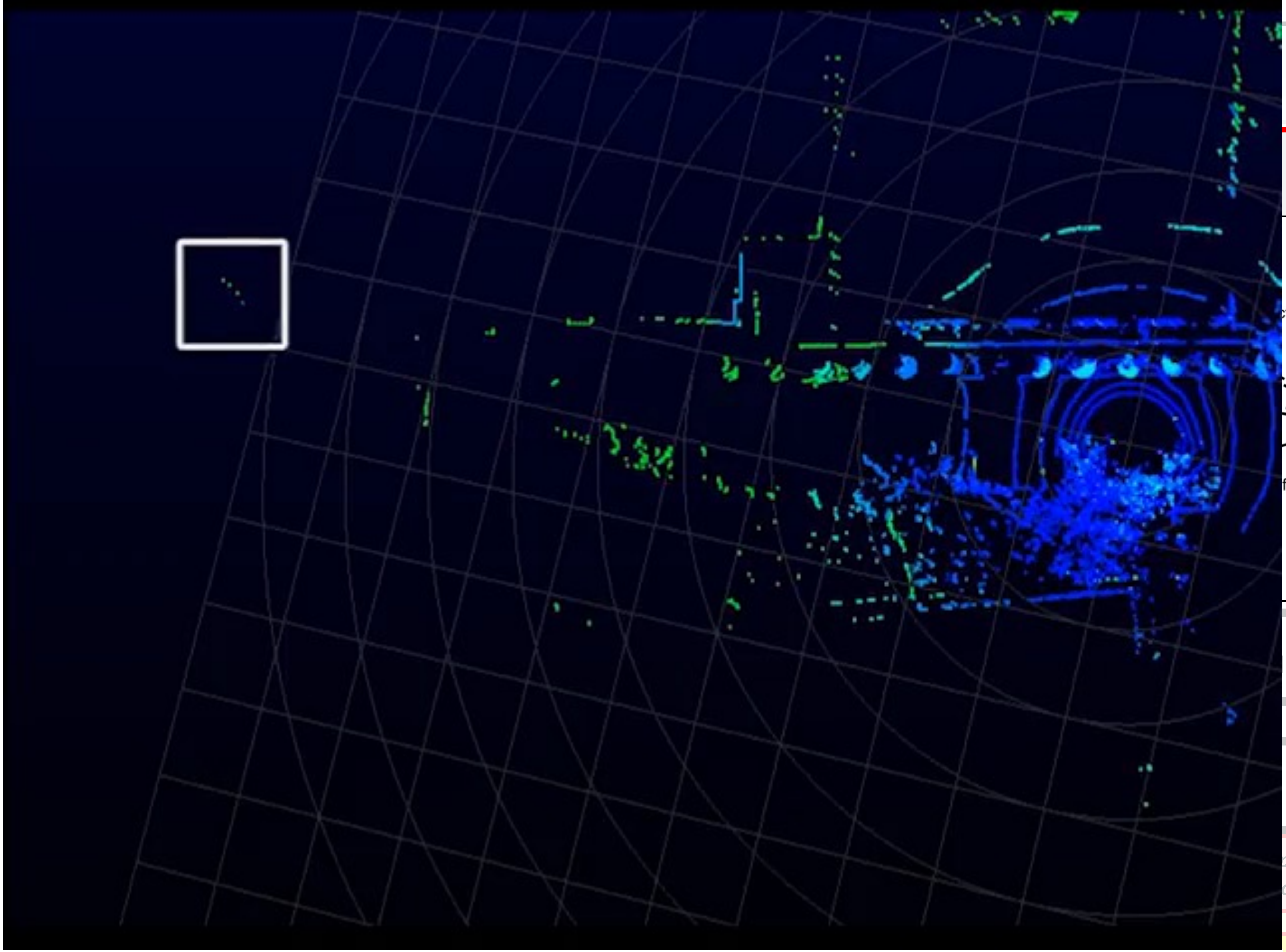
Top-tier: Security

NDSS'22 1st

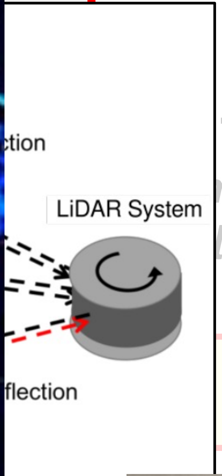




[Cao et al. @ AutoSec'21]



[Shin et al. @ CHES'17]



My group's paper

nplementation level problem

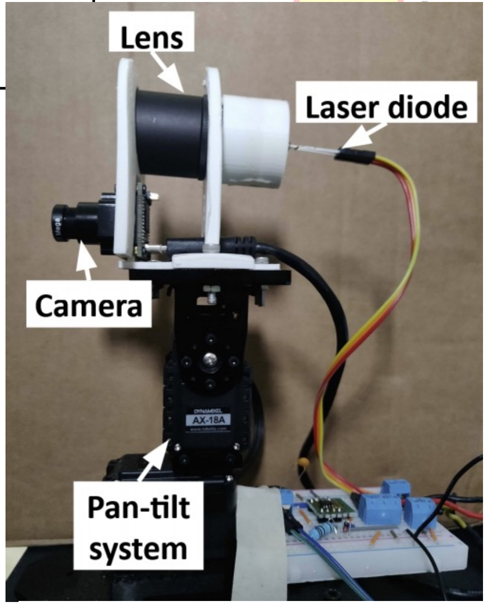
Top-tier: SE

ICSE'20

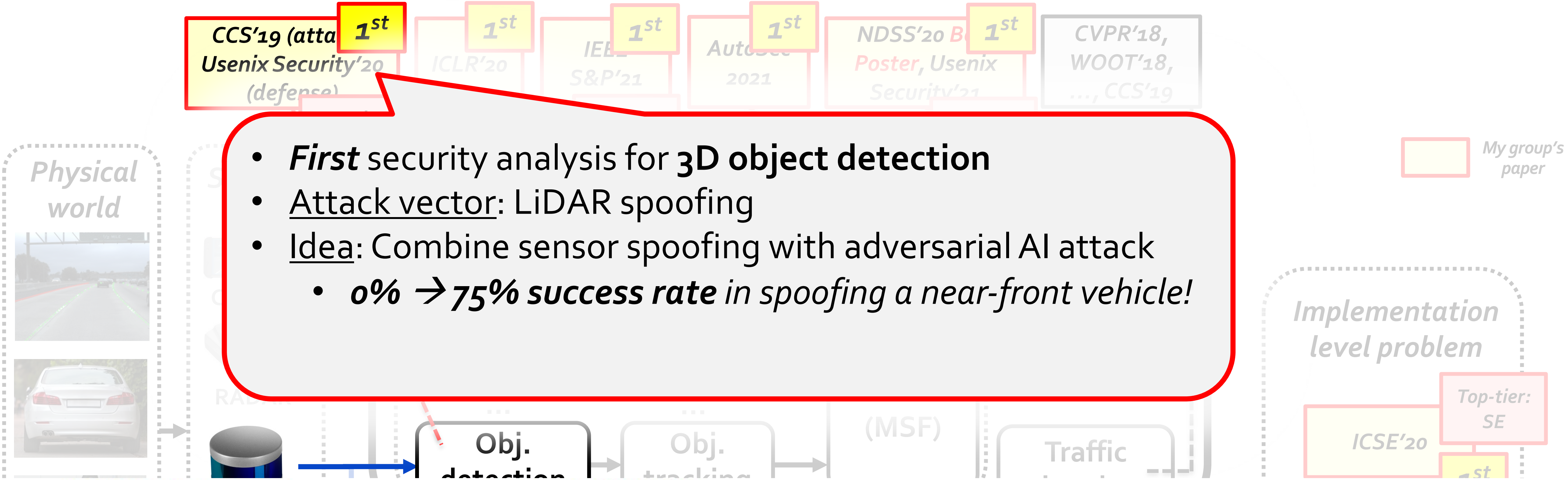
1st

-tier: curity

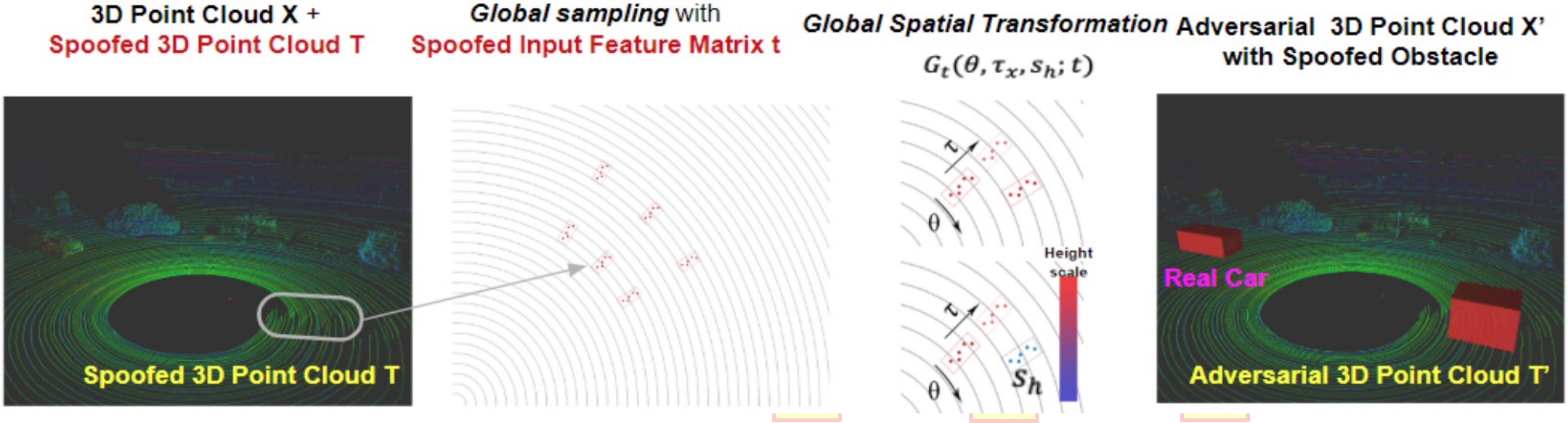
1st



[Cao et al. @ AutoSec'21]



- ***First*** security analysis for **3D object detection**
- <u>Attack vector</u>: LiDAR spoofing
- <u>Idea</u>: Combine sensor spoofing with adversarial AI attack
  - ***0% → 75% success rate*** *in spoofing a near-front vehicle!*


3D Point Cloud X +
Spoofed 3D Point Cloud T
Global sampling with
Spoofed Input Feature Matrix t
Global Spatial Transformation
$G_t(\theta, \tau_x, s_h; t)$
Adversarial 3D Point Cloud X'
with Spoofed Obstacle
Spoofed 3D Point Cloud T
τ
θ
Height
scale
s_h
Real Car
Adversarial 3D Point Cloud T'

CCS'19 (atta... 1st
Usenix Security'20
(defense)

ICLR'20 1st

IEEE S&P'21 1st

AutoSec 2021 1st

NDSS'20 B... Poster, Usenix Security'21 1st

CVPR'18, WOOT'18, ..., CCS'19

- ***First*** security analysis for **3D object detection**
- Attack vector: LiDAR spoofing
- Idea: Combine sensor spoofing with adversarial AI attack
  - ***0% → 75% success rate*** *in spoofing a near-front vehicle!*
- Impact: Causing emergency brake or permanent stop

My group's paper

Physical world

LiDAR

Obj. detection

Obj. tracking

(MSF)

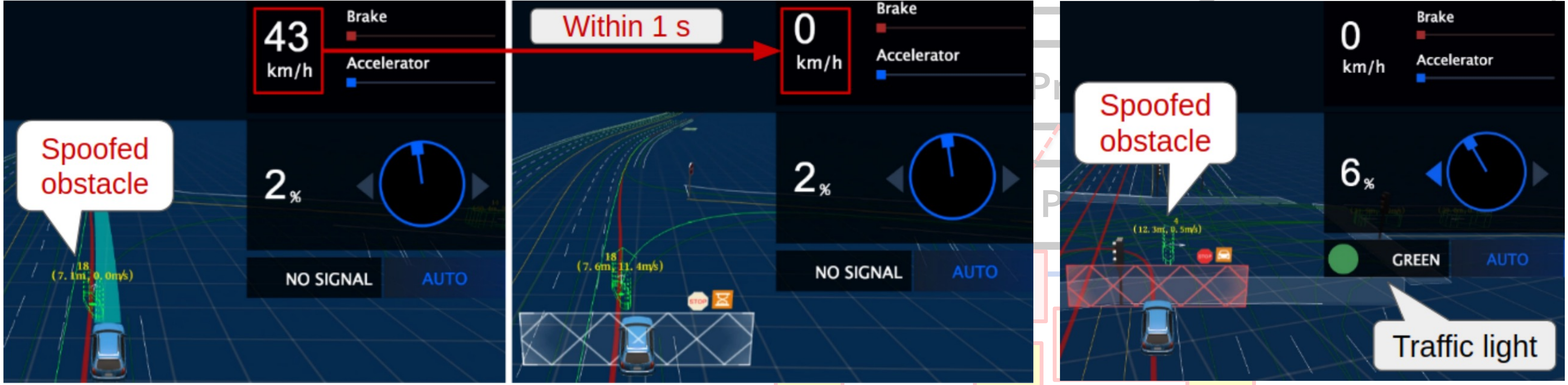
Traffic sign det.

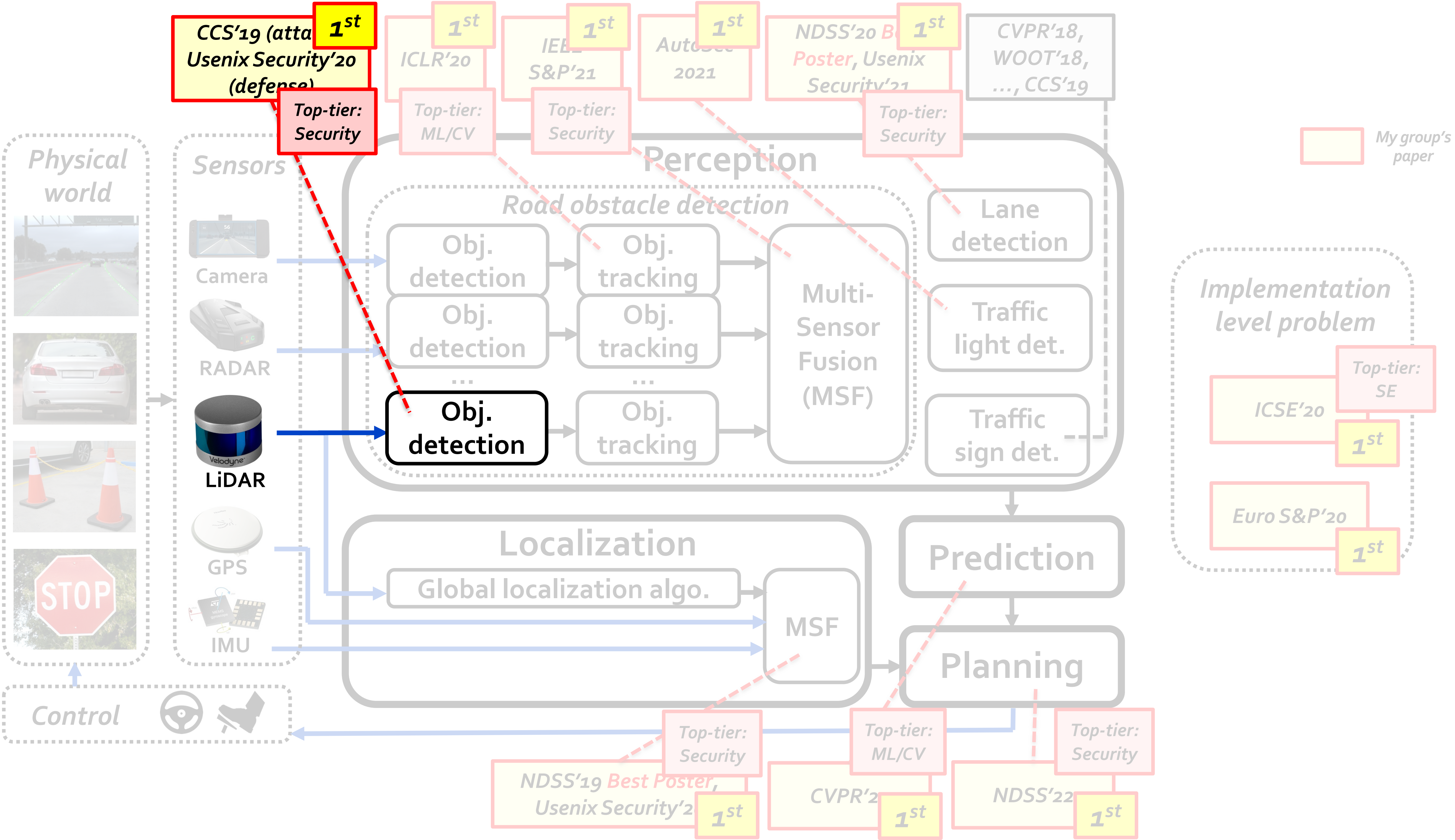
Implementation level problem

ICSE'20

Top-tier: SE

1st





CCS'19 (atta
Usenix Security'20
(defense)

1st

Top-tier: Security

ICLR'20

1st

Top-tier: ML/CV

IEE
S&P'21

1st

Top-tier: Security

Auto
2021

1st

NDSS'20 B
Poster, Usenix
Security'21

1st

Top-tier: Security

CVPR'18,
WOOT'18,
…, CCS'19

My group's paper

Physical world

Sensors

Camera

RADAR

LiDAR

GPS

IMU

Perception

Road obstacle detection

Obj. detection

Obj. tracking

Obj. detection

Obj. tracking

…

…

Obj. detection

Obj. tracking

Multi-Sensor Fusion (MSF)

Lane detection

Traffic light det.

Traffic sign det.

Implementation level problem

Top-tier: SE

ICSE'20

1st

Euro S&P'20

1st

Localization

Global localization algo.

MSF

Prediction

Planning

Control

Top-tier: Security

NDSS'19 Best Poster,
Usenix Security'2

1st

Top-tier: ML/CV

CVPR'2

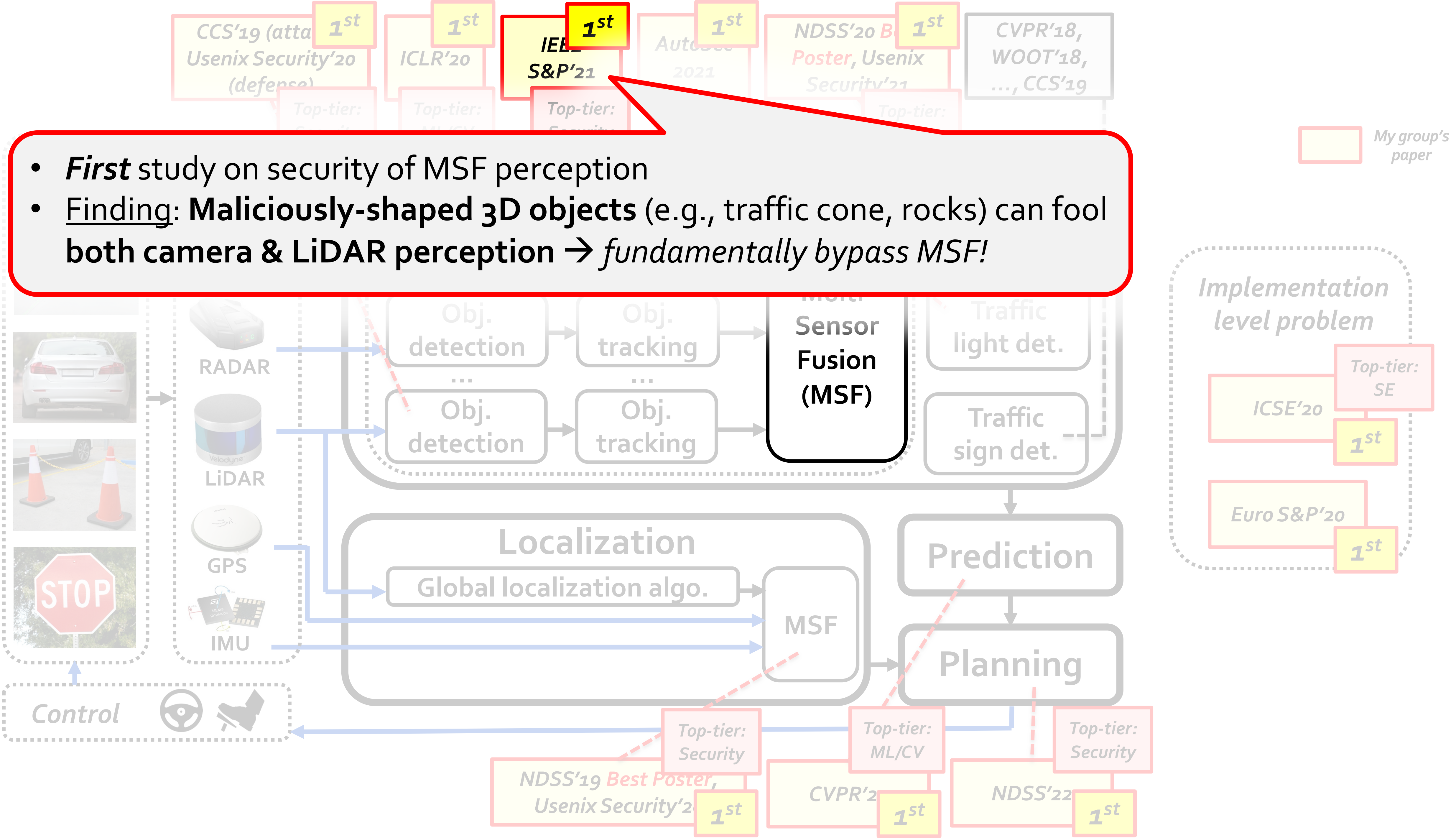
1st

Top-tier: Security

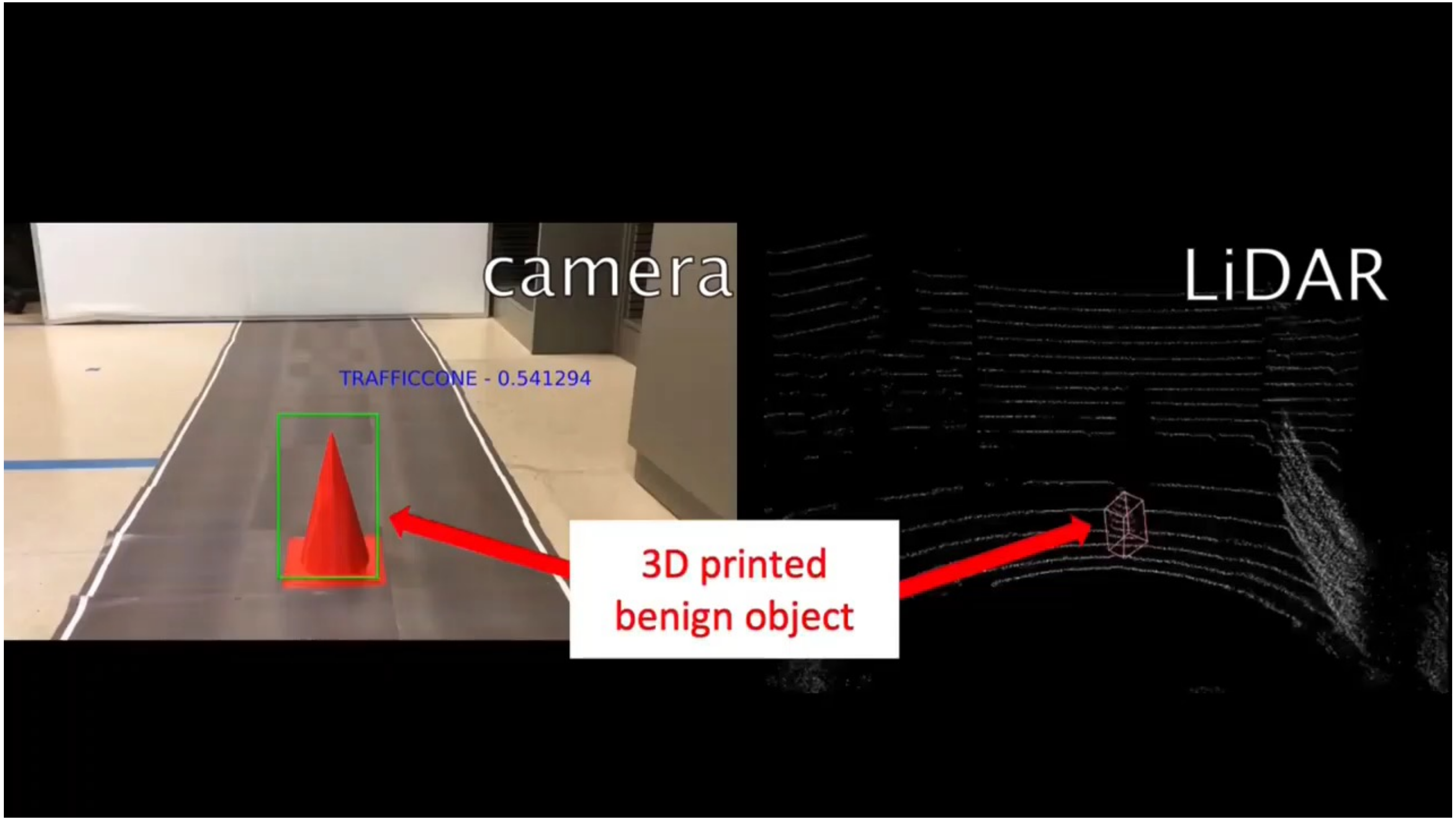
NDSS'22

1st

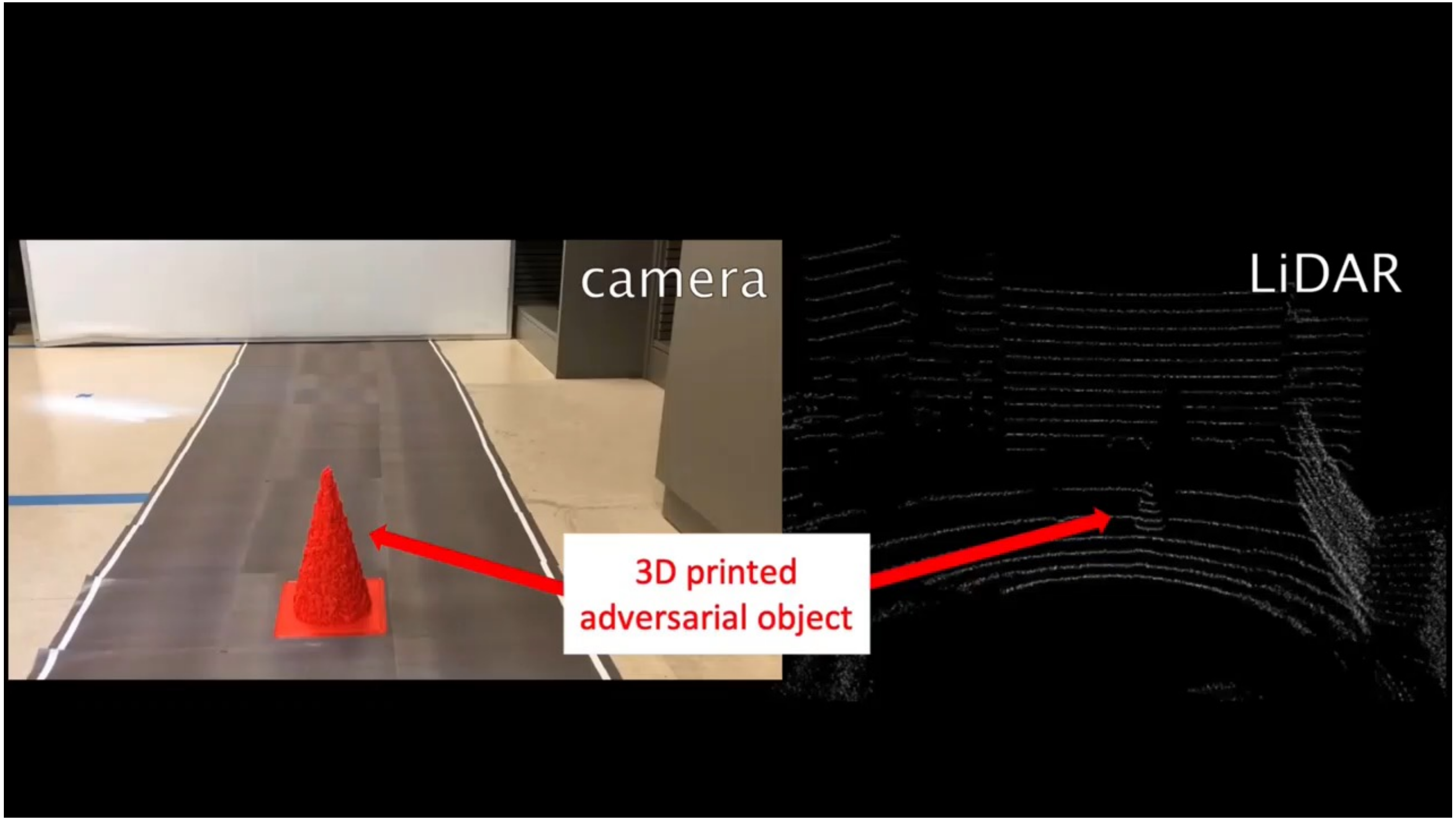
- ***First*** study on security of MSF perception
- Finding: **Maliciously-shaped 3D objects** (e.g., traffic cone, rocks) can fool **both camera & LiDAR perception** → *fundamentally bypass MSF!*



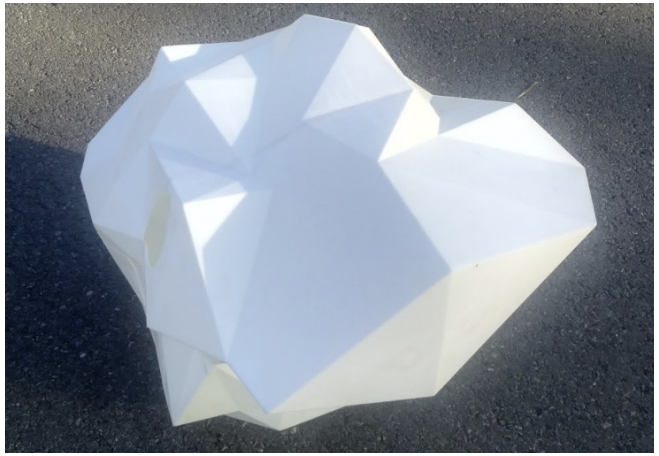
Attack demos: Benign case

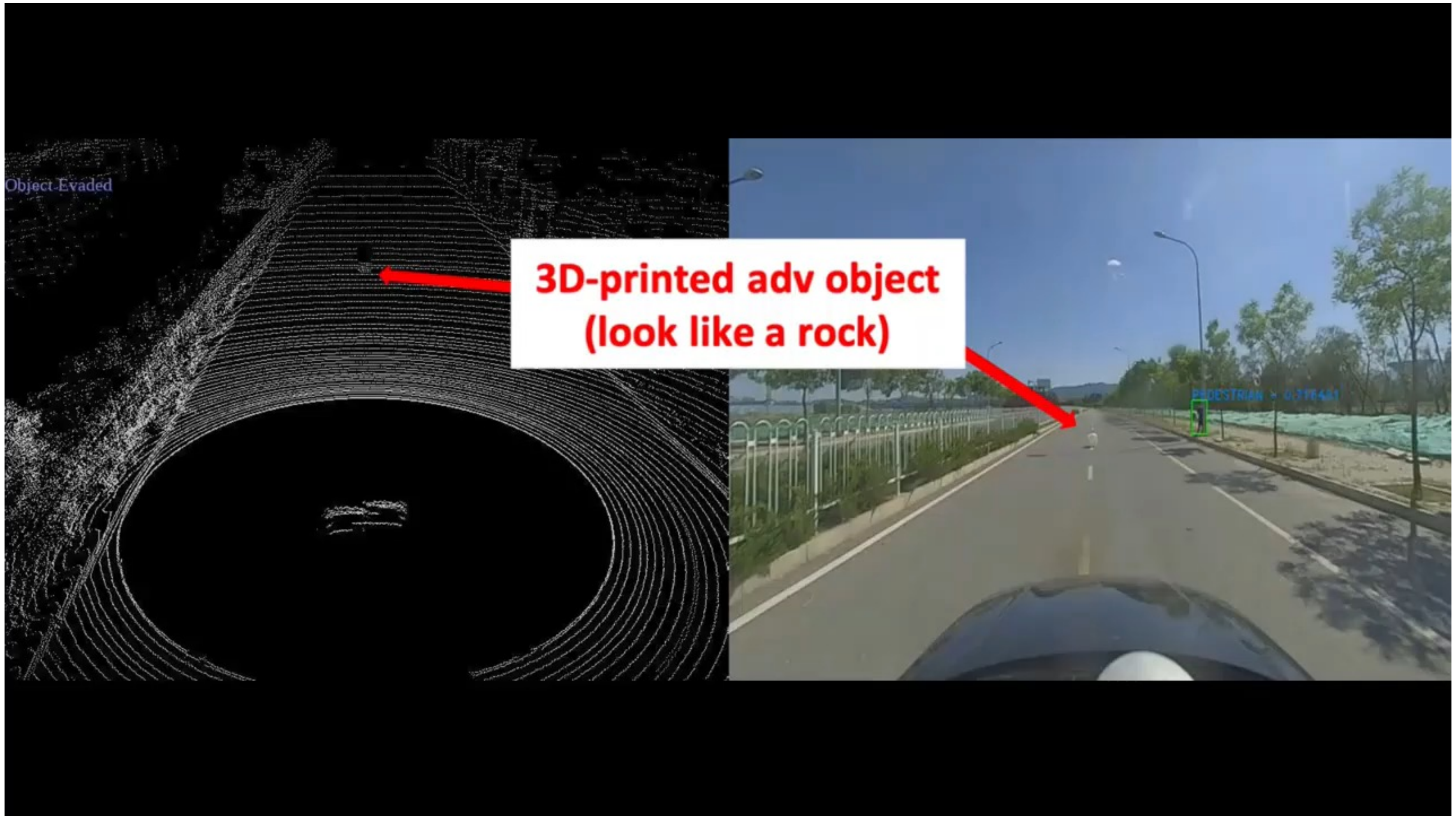


Attack demos: Adversarial case



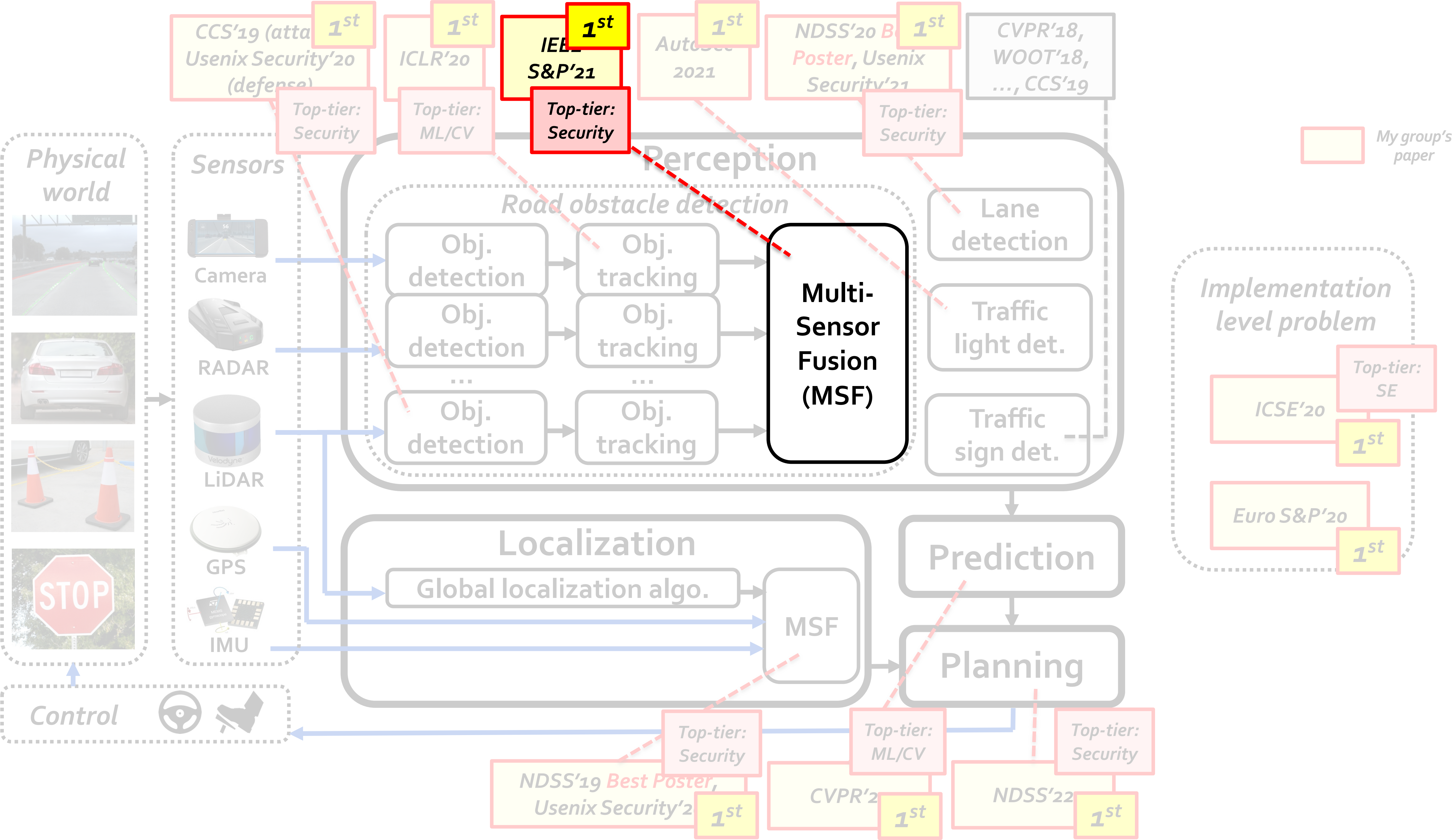
Attack demos





3D-printed adv object (look like a rock)

Demo website: https://sites.google.com/view/cav-sec/msf-adv



CCS'19 (atta
Usenix Security'20
(defense)
1st
Top-tier:
Security

ICLR'20
1st
Top-tier:
ML/CV

IEEE
S&P'21
1st
Top-tier:
Security

AutoSec
2021
1st

NDSS'20 Best
Poster, Usenix
Security'21
1st
Top-tier:
Security

CVPR'18,
WOOT'18,
…, CCS'19

My group's
paper

Physical
world

Sensors

Camera

RADAR

LiDAR

GPS

IMU

Perception

Road obstacle detection

Obj.
detection

Obj.
tracking

Obj.
detection

Obj.
tracking

…

…

Obj.
detection

Obj.
tracking

Multi-
Sensor
Fusion
(MSF)

Lane
detection

Traffic
light det.

Traffic
sign det.

Implementation
level problem

ICSE'20
Top-tier:
SE
1st

Euro S&P'20
1st

Localization

Global localization algo.

MSF

Prediction

Planning

Control

NDSS'19 Best Poster,
Usenix Security'2
Top-tier:
Security
1st

CVPR'2
Top-tier:
ML/CV
1st

NDSS'22
Top-tier:
Security
1st

CCS'19 (atta Usenix Security'20 (defense) 1st

Top-tier: Security

ICLR'20 1st

Top-tier: ML/CV

IEE S&P'21 1st

Top-tier: Security

Auto 2021 1st

NDSS'20 B **1st**

Poster, Usenix Security'21

Top-tier: Security

CVPR'18, WOOT'18, ..., CCS'19

My group's paper

- **First** to study production lane detection DNN
- Finding: Seemingly-benign **dirty road patterns** can be used to fool automatic lane centering

Ph w

e ion

Obj. detection

Obj. tracking

Sensor

Traffic light det

Implementation level problem

ICSE'20

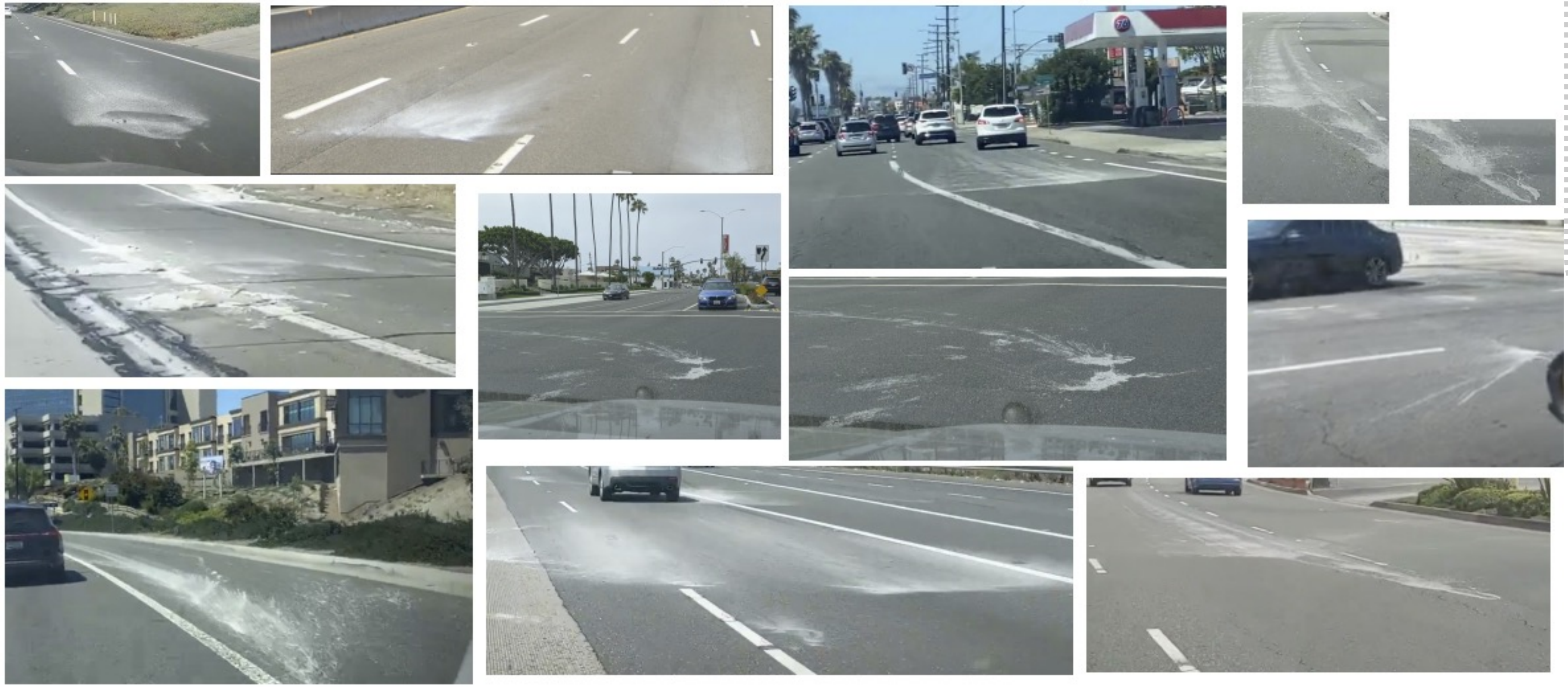
Top-tier: SE

1st

Euro S&P'20

1st

Contr



CCS'19 (atta... Usenix Security'20 (defense) 1st

ICLR'20 1st

IEEE S&P'21 1st

AutoSec 2021 1st

NDSS'20 B... Poster, Usenix Security'21 1st

CVPR'18, WOOT'18, ..., CCS'19

Top-tier: Security

Top-tier: ML/CV

Top-tier: Security

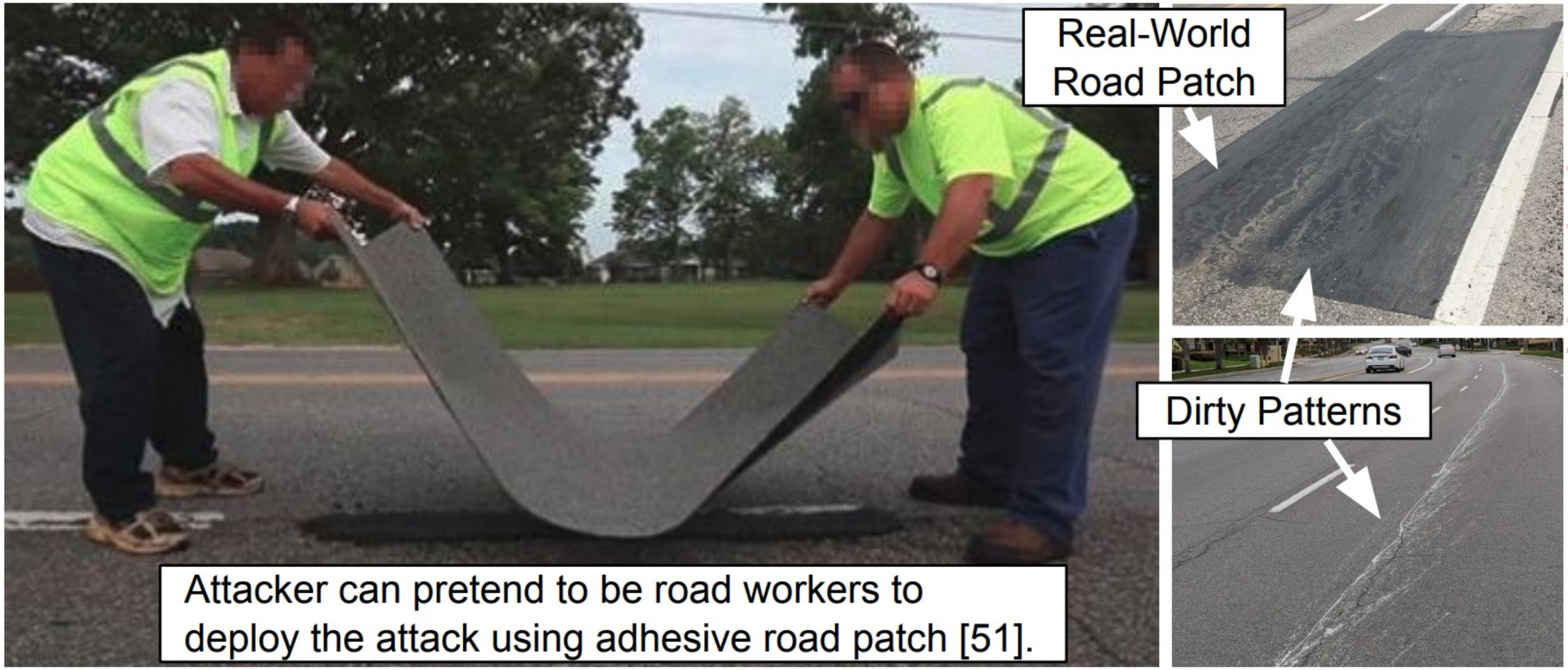
Top-tier: Security

My group's paper

- **First** to study production lane detection DNN
- Finding: Seemingly-benign **dirty road patterns** can be used to fool automatic lane centering

Obj. Obj. Traffic

Control



Attacker can pretend to be road workers to deploy the attack using adhesive road patch [51].

Implementation level problem

ICSE'20 Top-tier: SE 1st

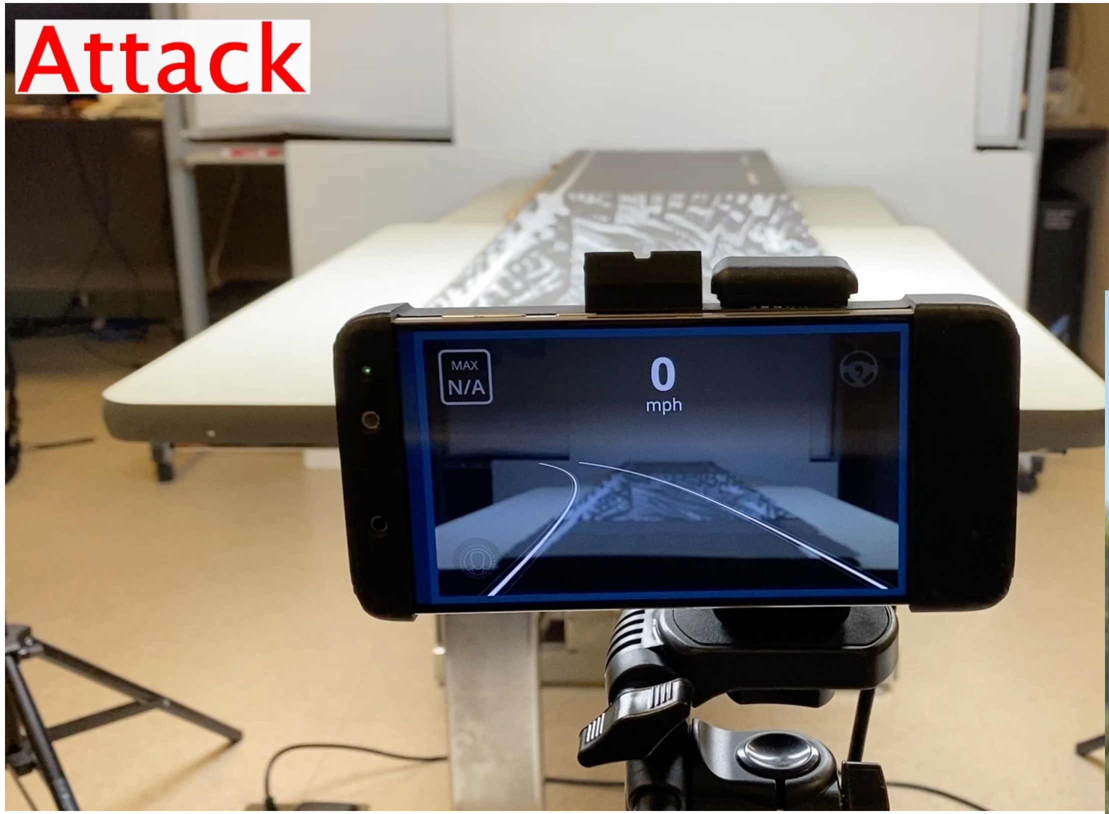
Euro S&P'20 1st

Usenix Security'2... 1st

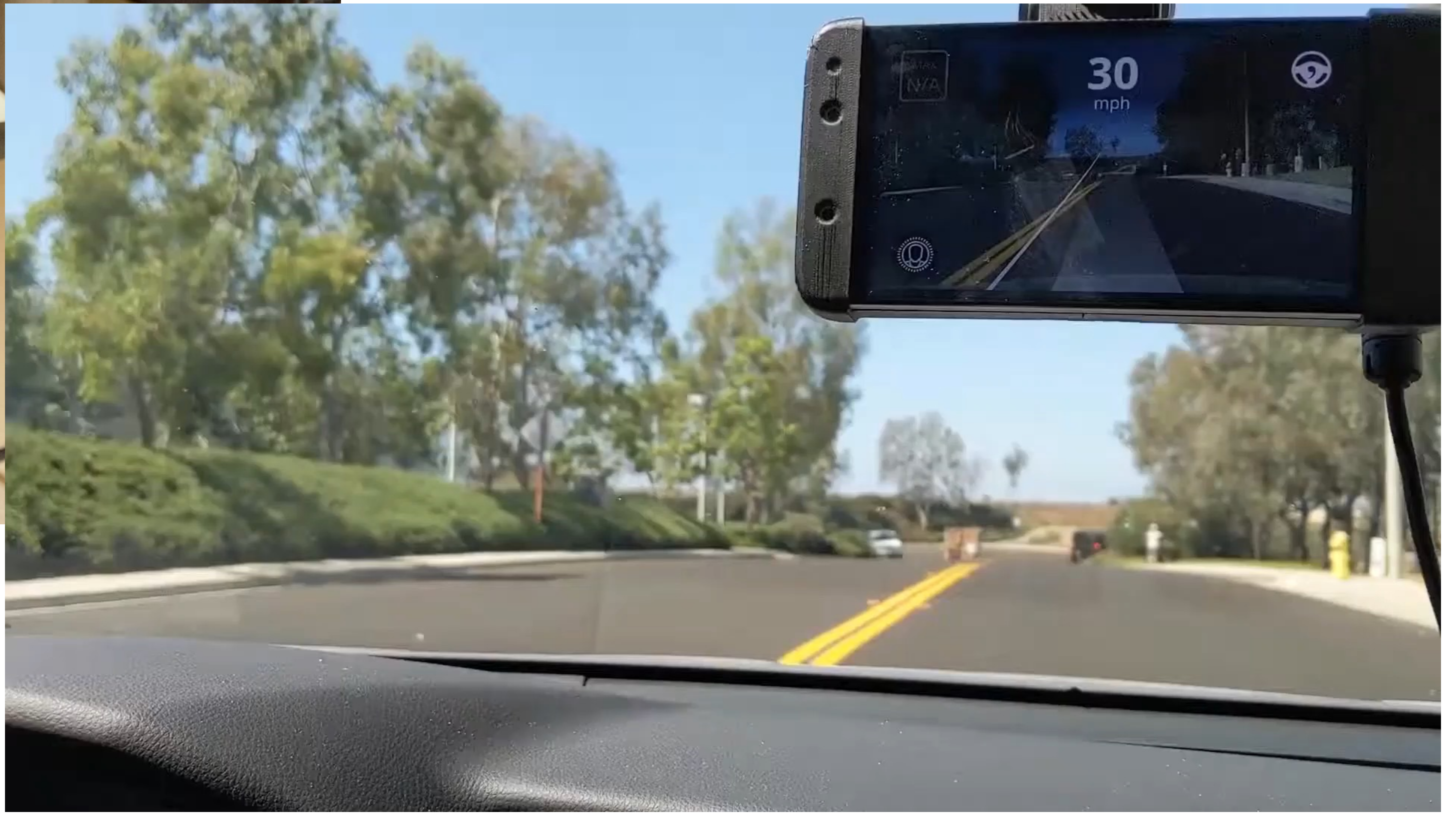
CVPR'2... 1st

NDSS'22 1st

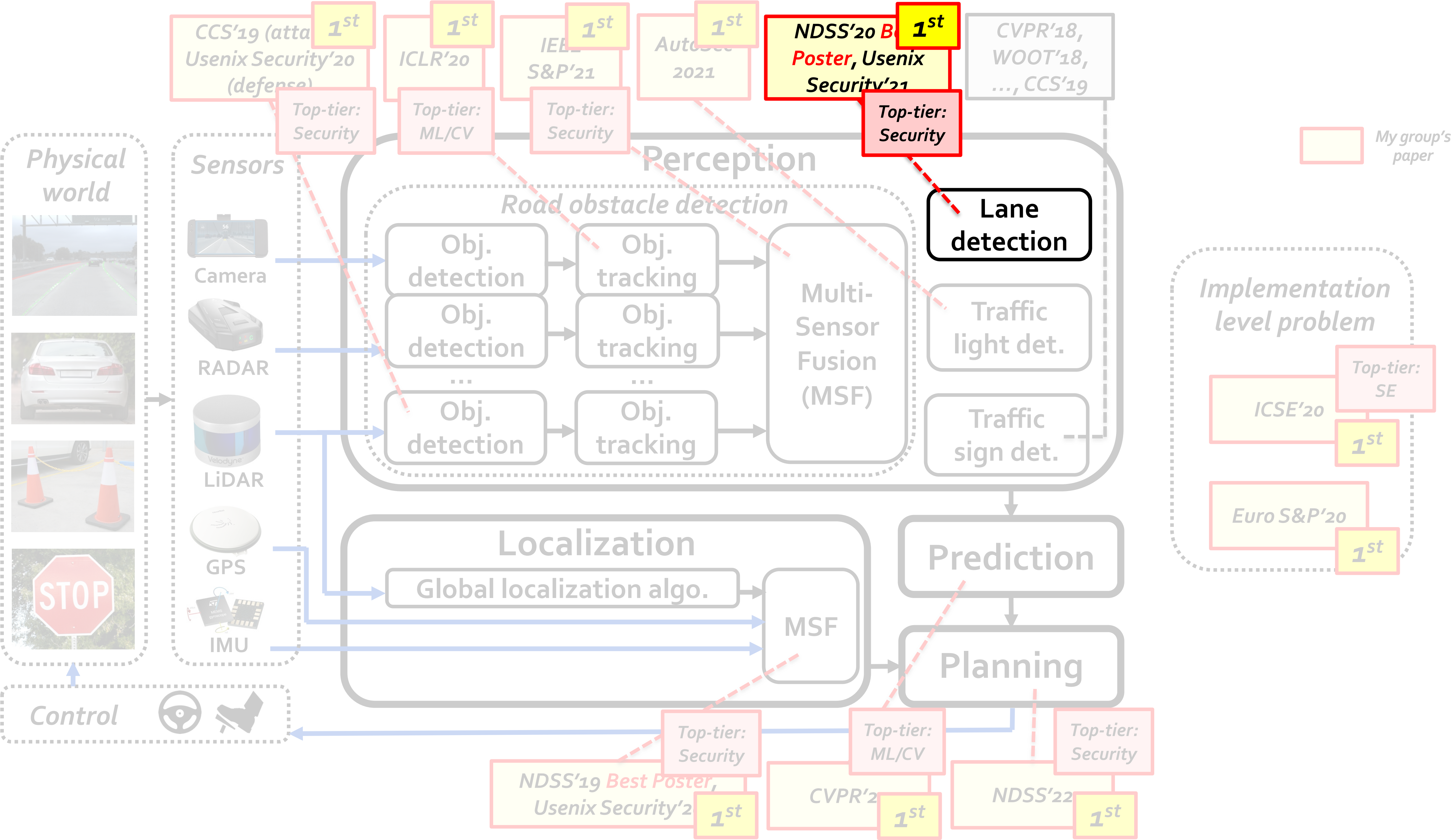
Demo: Dirty road patch attack on lane detection



100% (10/10) crash rate for real vehicle w/ AEB



Demo website: https://sites.google.com/view/cav-sec/drp-attack/


CCS'19 (atta
Usenix Security'20
(defense)
1st
Top-tier: Security

ICLR'20
1st
Top-tier: ML/CV

IEE
S&P'21
1st
Top-tier: Security

Auto
2021
1st

NDSS'20 B
Poster, Usenix
Security'21
1st
Top-tier: Security

CVPR'18,
WOOT'18,
…, CCS'19

My group's paper

Physical world

Sensors

Camera

RADAR

LiDAR

GPS

IMU

Control

Perception

Road obstacle detection

Obj. detection

Obj. tracking

Obj. detection

Obj. tracking

…

Obj. detection

Obj. tracking

Multi-Sensor Fusion (MSF)

Lane detection

Traffic light det.

Traffic sign det.

Localization

Global localization algo.

MSF

Prediction

Planning

Implementation level problem

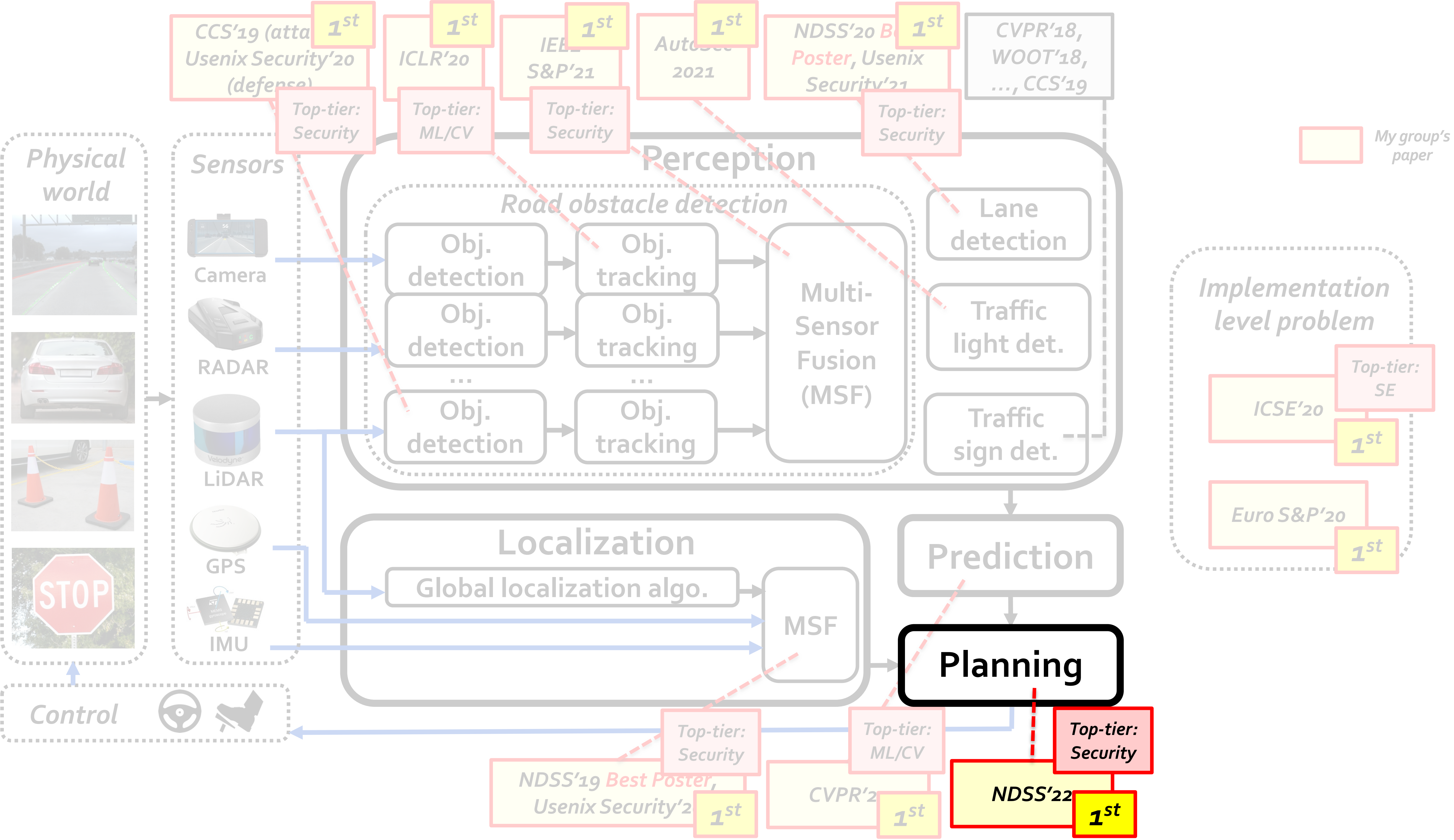
ICSE'20
Top-tier: SE
1st

Euro S&P'20
1st

NDSS'19 Best Poster,
Usenix Security'2
1st
Top-tier: Security

CVPR'2
1st
Top-tier: ML/CV

NDSS'22
1st
Top-tier: Security



CCS'19 (atta
Usenix Security'20
(defense)
1st
Top-tier: Security

ICLR'20
1st
Top-tier: ML/CV

IEE
S&P'21
1st
Top-tier: Security

Auto
2021
1st

NDSS'20 B
Poster, Usenix
Security'21
1st
Top-tier: Security

CVPR'18,
WOOT'18,
…, CCS'19

My group's paper

Physical world

Sensors

Camera

RADAR

LiDAR

GPS

IMU

Perception

Road obstacle detection

Obj. detection

Obj. tracking

Obj. detection

Obj. tracking

…

…

Obj. detection

Obj. tracking

Multi-Sensor Fusion (MSF)

Lane detection

Traffic light det.

Traffic sign det.

Localization

Global localization algo.

MSF

Prediction

Planning

Control

Implementation level problem

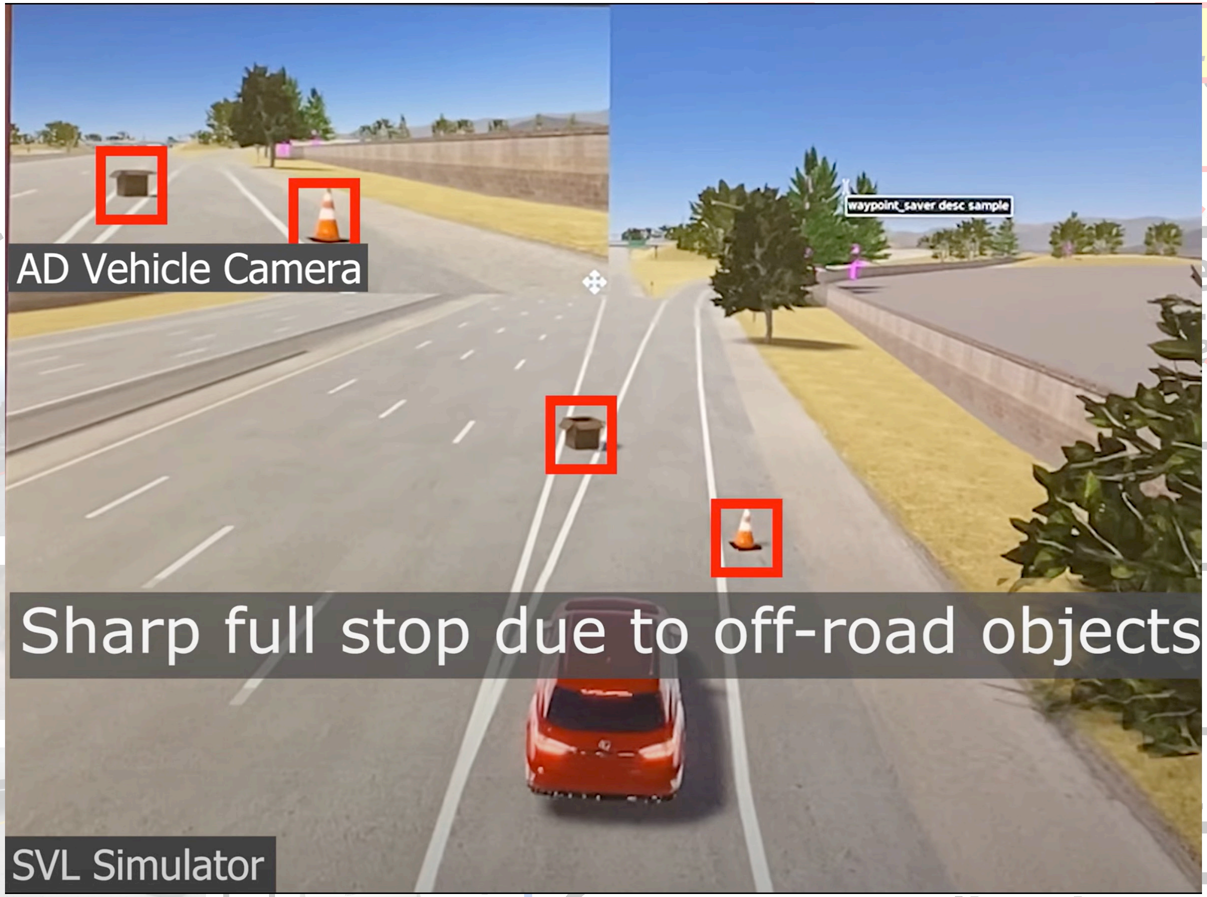
ICSE'20
Top-tier: SE
1st

Euro S&P'20
1st

Top-tier: Security
NDSS'19 Best Poster,
Usenix Security'2
1st

Top-tier: ML/CV
CVPR'2
1st

Top-tier: Security
NDSS'22
1st



Sharp full stop due to off-road objects

NDSS'20 B 1st

Poster, Usenix

CVPR'18, WOOT'18,

My group's paper

entation roblem

Top-tier: SE

E'20 1st

Euro S&P'20 1st

GPS

Localization

Global localization algo.

MSF

Prediction

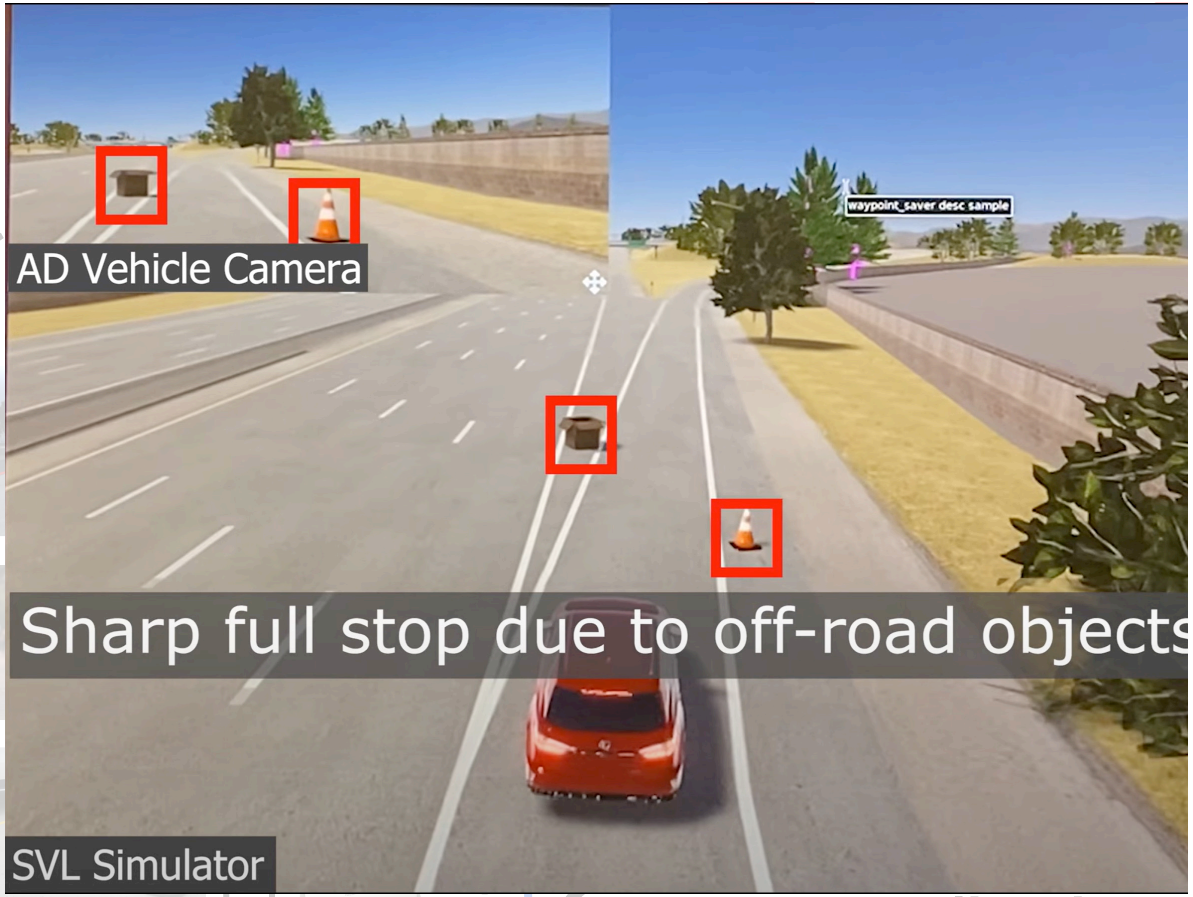
Planning

Top-tier: Security

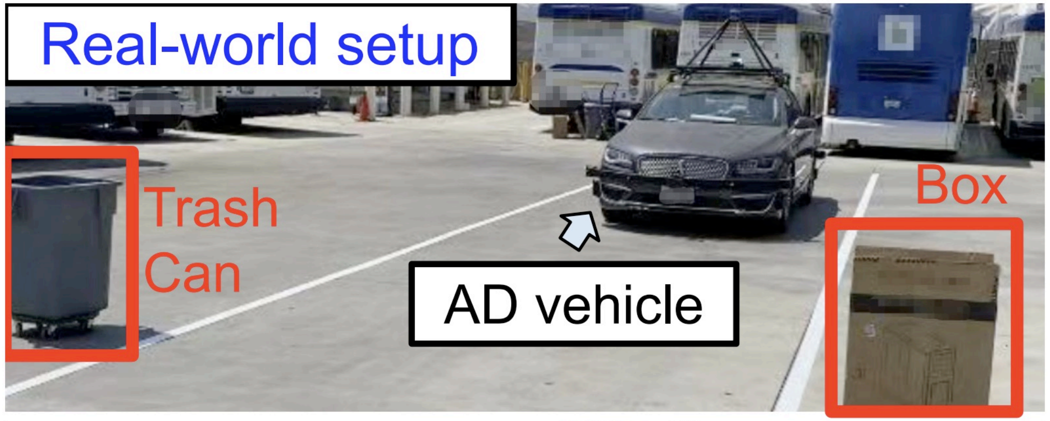
NDSS'22 1st

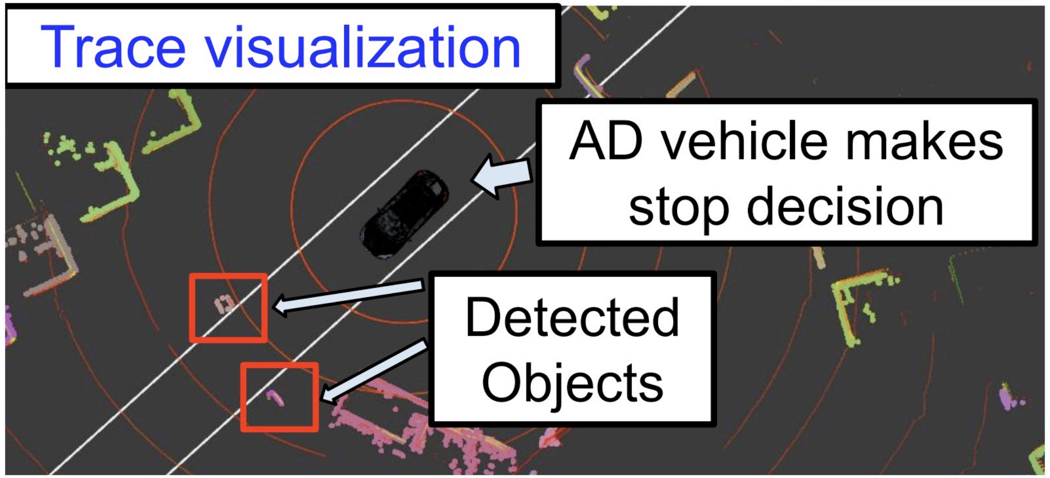
First security analysis of AD behavior planning (*program-based*)

- Finding: Common road objects (e.g., road-side cardboard boxes, parked bikes, etc.) can be used to attack AD



AD Vehicle Camera
waypoint_saver desc sample
Sharp full stop due to off-road objects
SVL Simulator





My group's paper

Top-tier: SE

1st

GPS

Localization

Global localization algo.

MSF

Demo website: *https://sites.google.com/view/cav-sec/planfuzz*

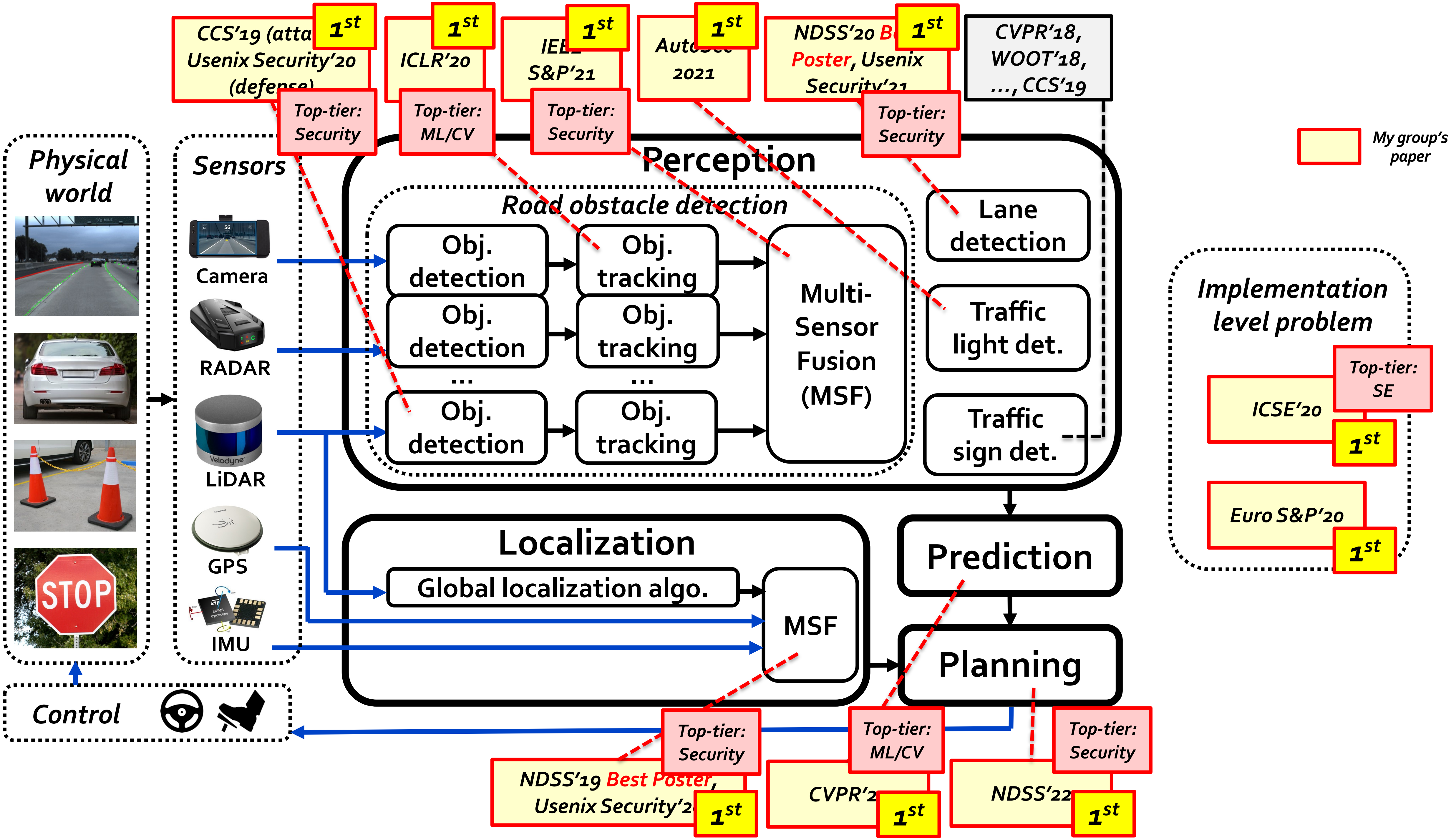
First security analysis of AD behavior planning (*program-based*)

- Finding: Common road objects (e.g., road-side cardboard boxes, parked bikes, etc.) can be used to attack AD

Planning

Top-tier: Security

NDSS'22 ***1st***



CCS'19 (atta
Usenix Security'20
(defense)
1st
Top-tier: Security

ICLR'20
1st
Top-tier: ML/CV

IEE
S&P'21
1st
Top-tier: Security

Auto
2021
1st

NDSS'20 B
Poster, Usenix
Security'21
1st
Top-tier: Security

CVPR'18,
WOOT'18,
…, CCS'19

My group's paper

Physical world

Sensors

Camera

RADAR

LiDAR

GPS

IMU

Perception

Road obstacle detection

Obj. detection

Obj. tracking

Obj. detection

Obj. tracking

…

…

Obj. detection

Obj. tracking

Multi-Sensor Fusion (MSF)

Lane detection

Traffic light det.

Traffic sign det.

Implementation level problem

ICSE'20
1st
Top-tier: SE

Euro S&P'20
1st

Localization

Global localization algo.

MSF

Prediction

Planning

Control

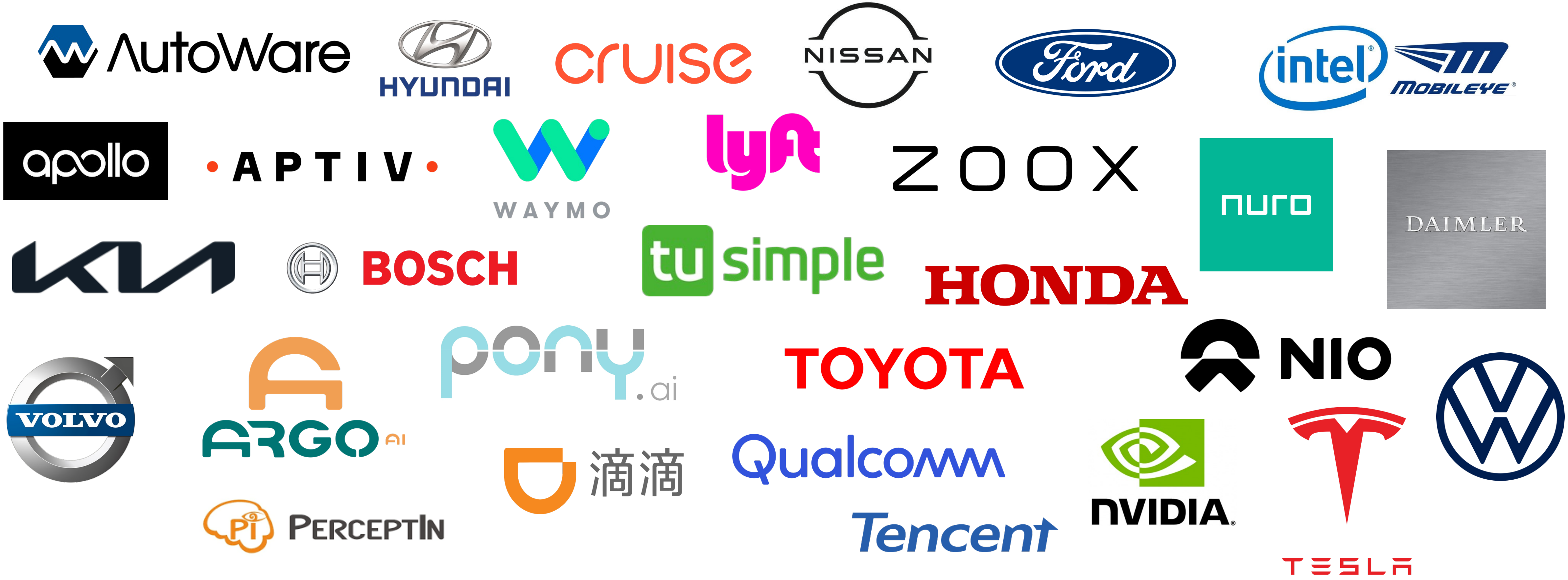
NDSS'19 *Best Poster*,
Usenix Security'2
1st
Top-tier: Security

CVPR'2
1st
Top-tier: ML/CV

NDSS'22
1st
Top-tier: Security

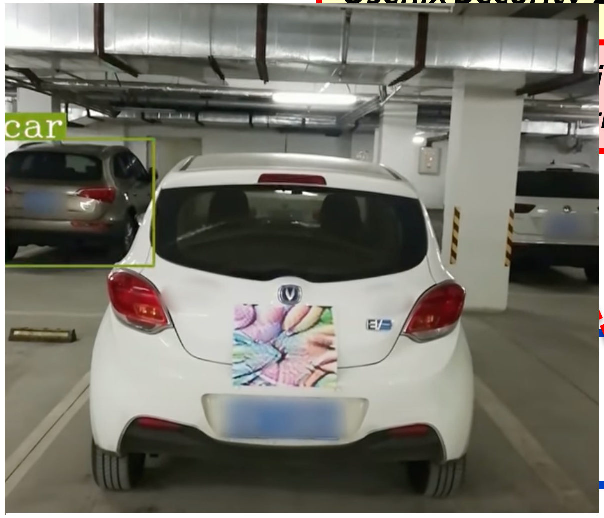
Responsible vulnerability disclosure

- Triggered **>30 AD companies** to start vuln investigation

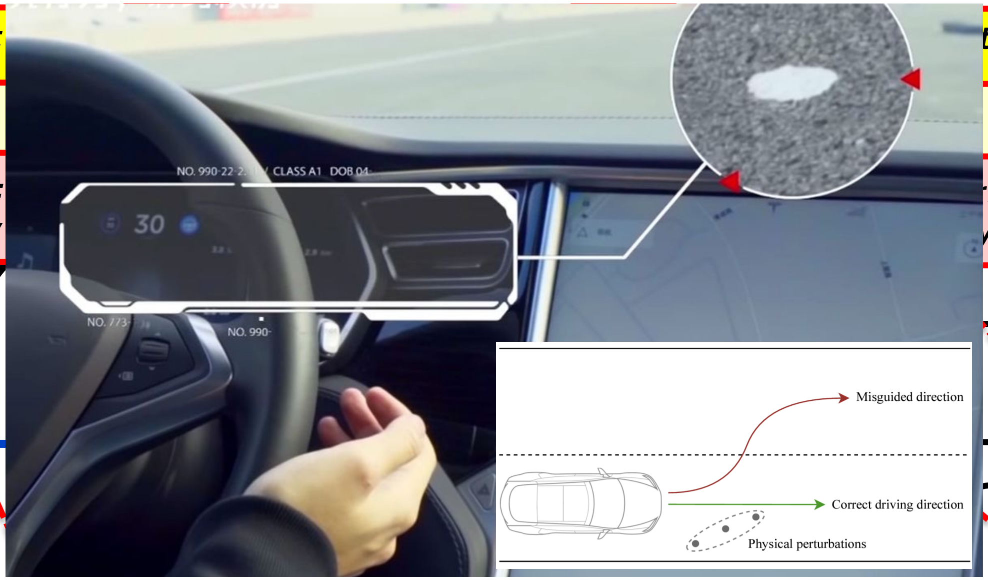


CCS'19 (atta **1st**
Usenix Security'20

ier:
ity



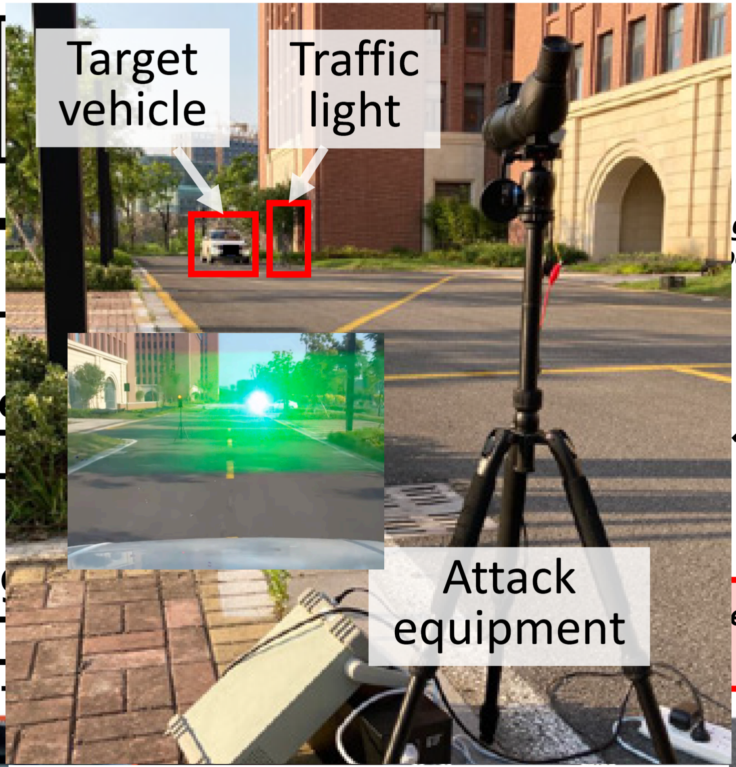
[Zhao et al. @ CCS'19]



[Jing et al. @ Usenix Security'21]

de

li



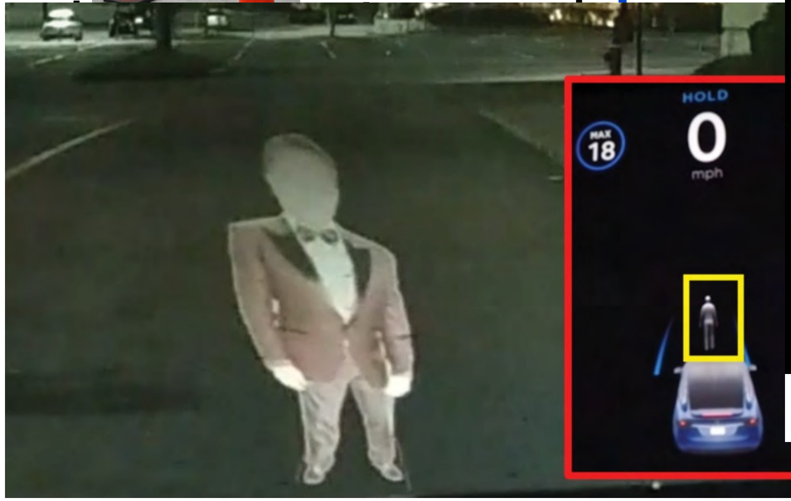
[Yan et al. @ Usenix Security'22]

group's paper

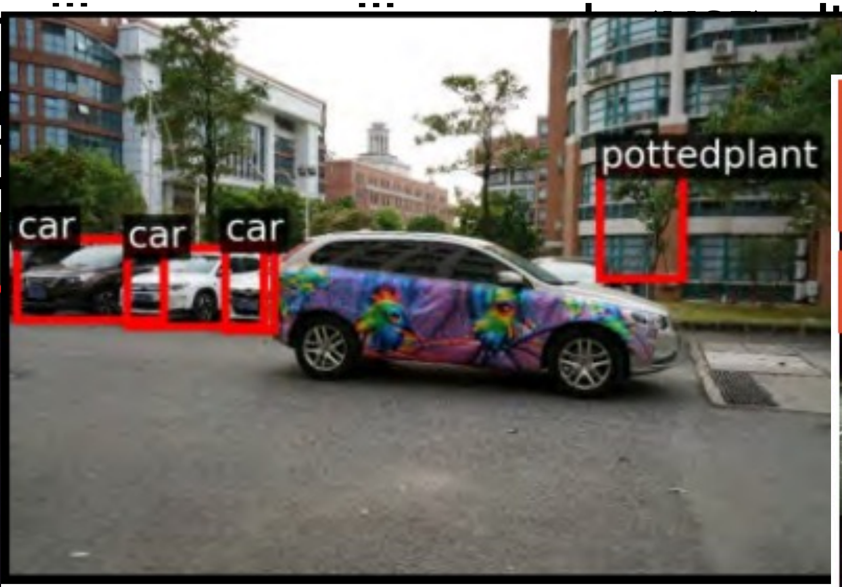
er:

LiDAR

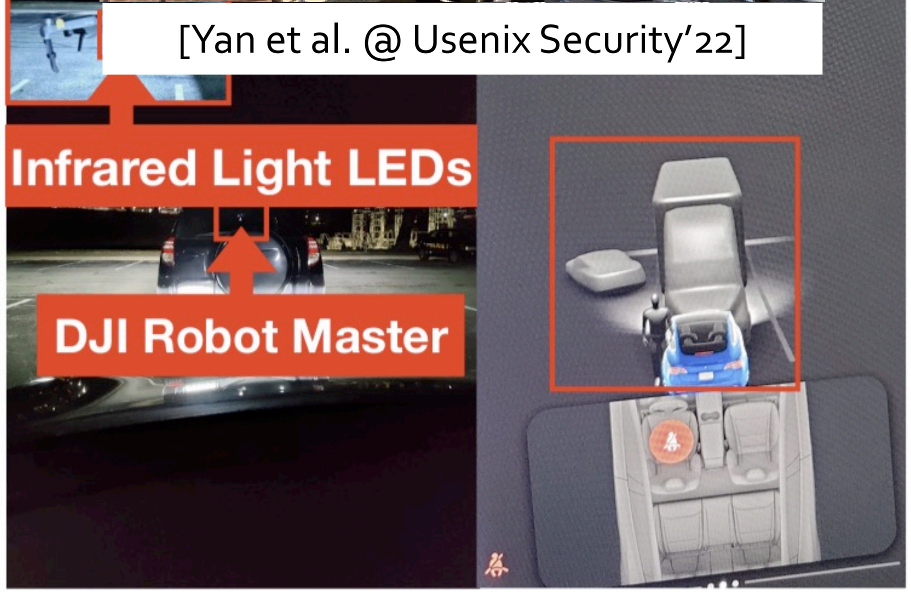
d



[Nassi et al. @ CCS'20]



[Huang et al. @ CVPR'20]



[Wang et al. @ CCS'21]

NDSS'19 ***Best Poster,***
Usenix Security'2 **1st**

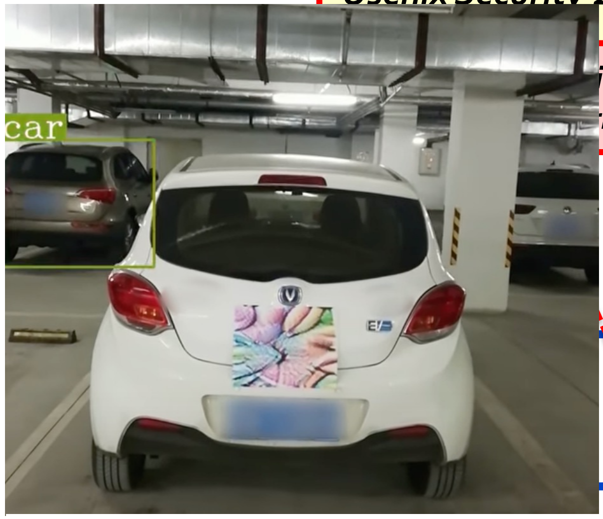
CVPR'2 **1s**

CCS'19 (atta 1st

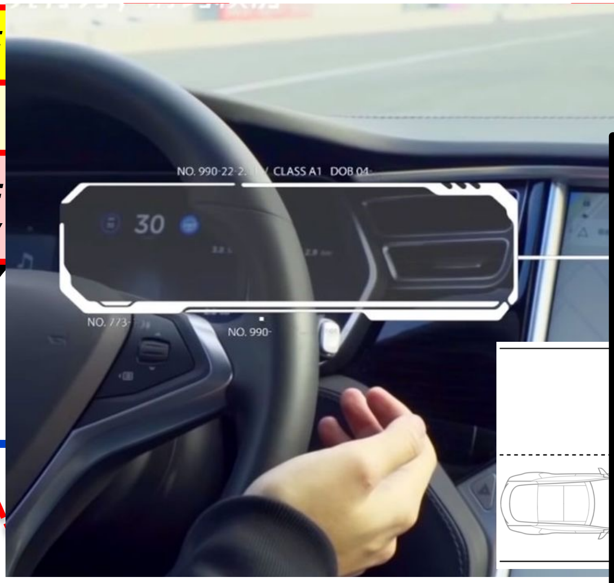
Usenix Security'20

ier:

ity

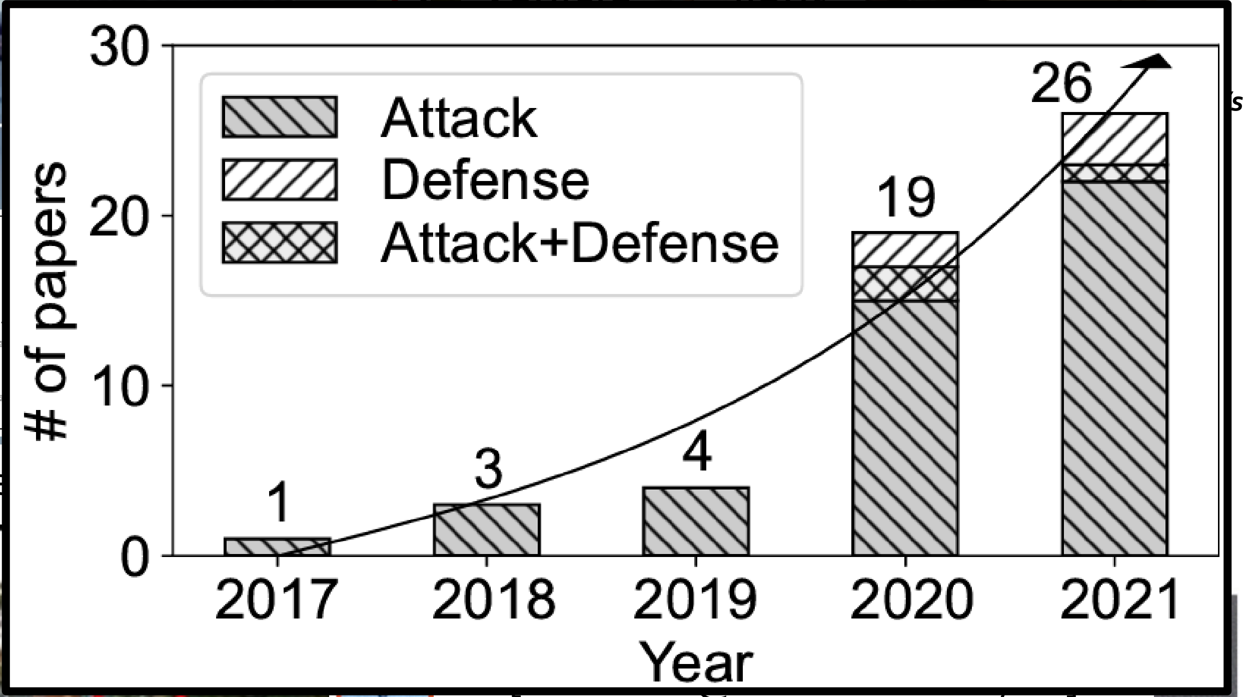


[Zhao et al. @ CCS'19]



[Jing et al. @ Usenix Se

AD AI security papers



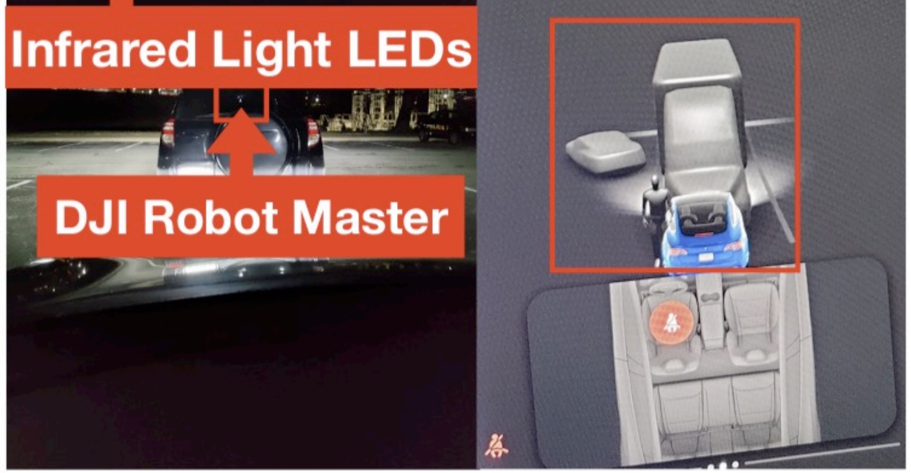
(*Systematization of Knowledge (SoK) effort from my group)

[Nassi et al. @ CCS'20]

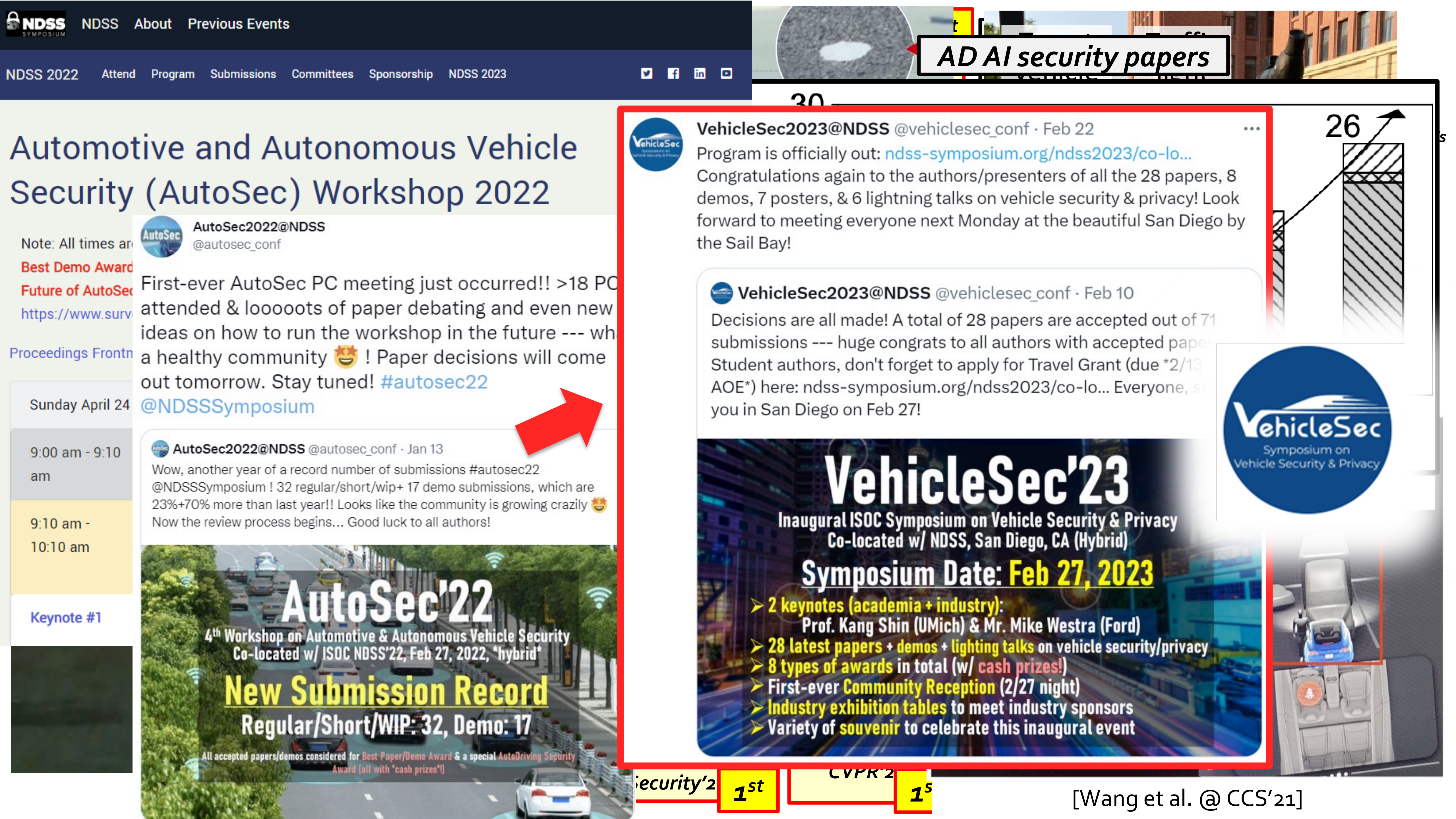
[Huang et al. @ CVPR'20]

NDSS'19 *Best Poster*, Usenix Security'2 1st

CVPR'2 1s



[Wang et al. @ CCS'21]



NDSS SYMPOSIUM | NDSS | About | Previous Events

NDSS 2022 | Attend | Program | Submissions | Committees | Sponsorship | NDSS 2023

Automotive and Autonomous Vehicle Security (AutoSec) Workshop 2022

Note: All times ar

Best Demo Award

Future of AutoSec

https://www.surv

Proceedings Frontn

Sunday April 24

9:00 am - 9:10 am

9:10 am - 10:10 am

Keynote #1

AutoSec2022@NDSS @autosec_conf

First-ever AutoSec PC meeting just occurred!! >18 PC attended & loooooots of paper debating and even new ideas on how to run the workshop in the future --- wh a healthy community 🤩 ! Paper decisions will come out tomorrow. Stay tuned! #autosec22 @NDSSSymposium

AutoSec2022@NDSS @autosec_conf · Jan 13

Wow, another year of a record number of submissions #autosec22 @NDSSSymposium ! 32 regular/short/wip+ 17 demo submissions, which are 23%+70% more than last year!! Looks like the community is growing crazily 🤩 Now the review process begins... Good luck to all authors!

AutoSec'22

4th Workshop on Automotive & Autonomous Vehicle Security

Co-located w/ ISOC NDSS'22, Feb 27, 2022, *hybrid*

New Submission Record

Regular/Short/WIP: 32, Demo: 17

All accepted papers/demos considered for Best Paper/Demo Award & a special AutoDriving Security Award (all with *cash prizes*!)

VehicleSec2023@NDSS @vehiclesec_conf · Feb 22

Program is officially out: ndss-symposium.org/ndss2023/co-lo... Congratulations again to the authors/presenters of all the 28 papers, 8 demos, 7 posters, & 6 lightning talks on vehicle security & privacy! Look forward to meeting everyone next Monday at the beautiful San Diego by the Sail Bay!

VehicleSec2023@NDSS @vehiclesec_conf · Feb 10

Decisions are all made! A total of 28 papers are accepted out of 71 submissions --- huge congrats to all authors with accepted pape Student authors, don't forget to apply for Travel Grant (due *2/13 AOE*) here: ndss-symposium.org/ndss2023/co-lo... Everyone, s you in San Diego on Feb 27!

VehicleSec'23

Inaugural ISOC Symposium on Vehicle Security & Privacy

Co-located w/ NDSS, San Diego, CA (Hybrid)

Symposium Date: Feb 27, 2023

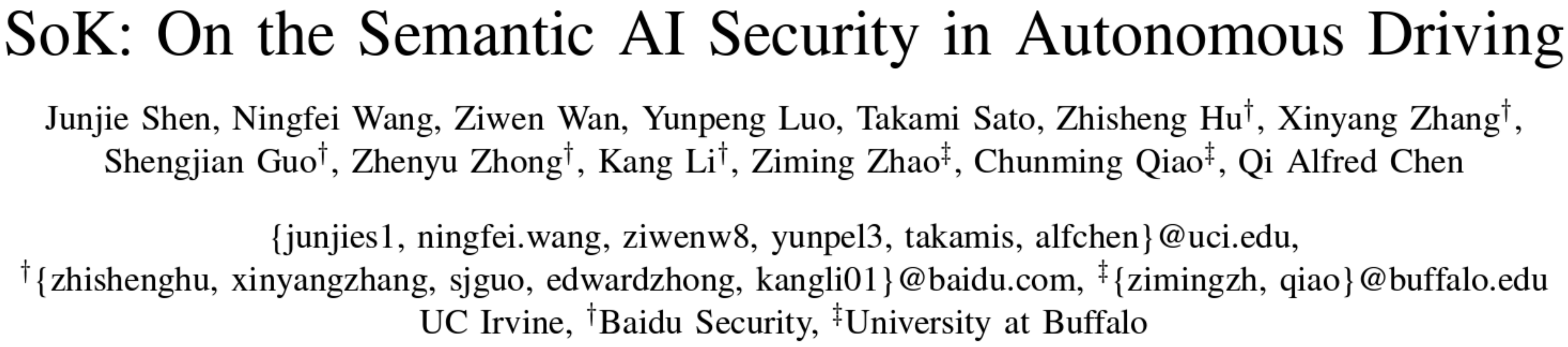
- 2 keynotes (academia + industry): Prof. Kang Shin (UMich) & Mr. Mike Westra (Ford)
- 28 latest papers + demos + lighting talks on vehicle security/privacy
- 8 types of awards in total (w/ cash prizes!)
- First-ever Community Reception (2/27 night)
- Industry exhibition tables to meet industry sponsors
- Variety of souvenir to celebrate this inaugural event

VehicleSec Symposium on Vehicle Security & Privacy

[Wang et al. @ CCS'21]

A reflection of the 5+ years of AD AI security research

- Conduct the **first Systemization of Knowledge (SoK) effort** on **semantic AI security** research in AD
  - Collect & analyze ***53 papers in past 5 years***, mainly from ***top-tier venues in security, CV (Computer Vision), ML (Machine Learning), AI, and robotics***



SoK: On the Semantic AI Security in Autonomous Driving

Junjie Shen, Ningfei Wang, Ziwen Wan, Yunpeng Luo, Takami Sato, Zhisheng Hu[†], Xinyang Zhang[†],
Shengjian Guo[†], Zhenyu Zhong[†], Kang Li[†], Ziming Zhao[‡], Chunming Qiao[‡], Qi Alfred Chen

{junjies1, ningfei.wang, ziwenw8, yunpel3, takamis, alfchen}@uci.edu,
[†]{zhishenghu, xinyangzhang, sjguo, edwardzhong, kangli01}@baidu.com, [‡]{zimingzh, qiao}@buffalo.edu
UC Irvine, [†]Baidu Security, [‡]University at Buffalo

Link: https://arxiv.org/abs/2203.05314

Our SoK effort

- **Taxonomization, status & trend analysis,** based on critical research aspects for security
  - E.g., attack/defense goal, attack vector, defense deployability, evaluation methodologies, etc.

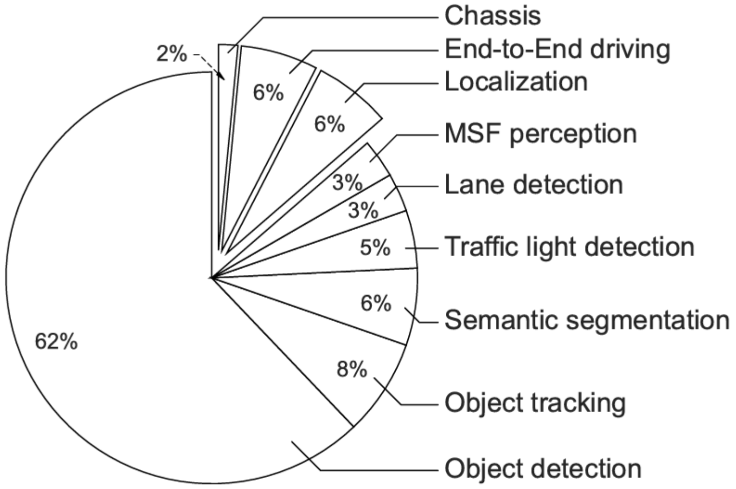
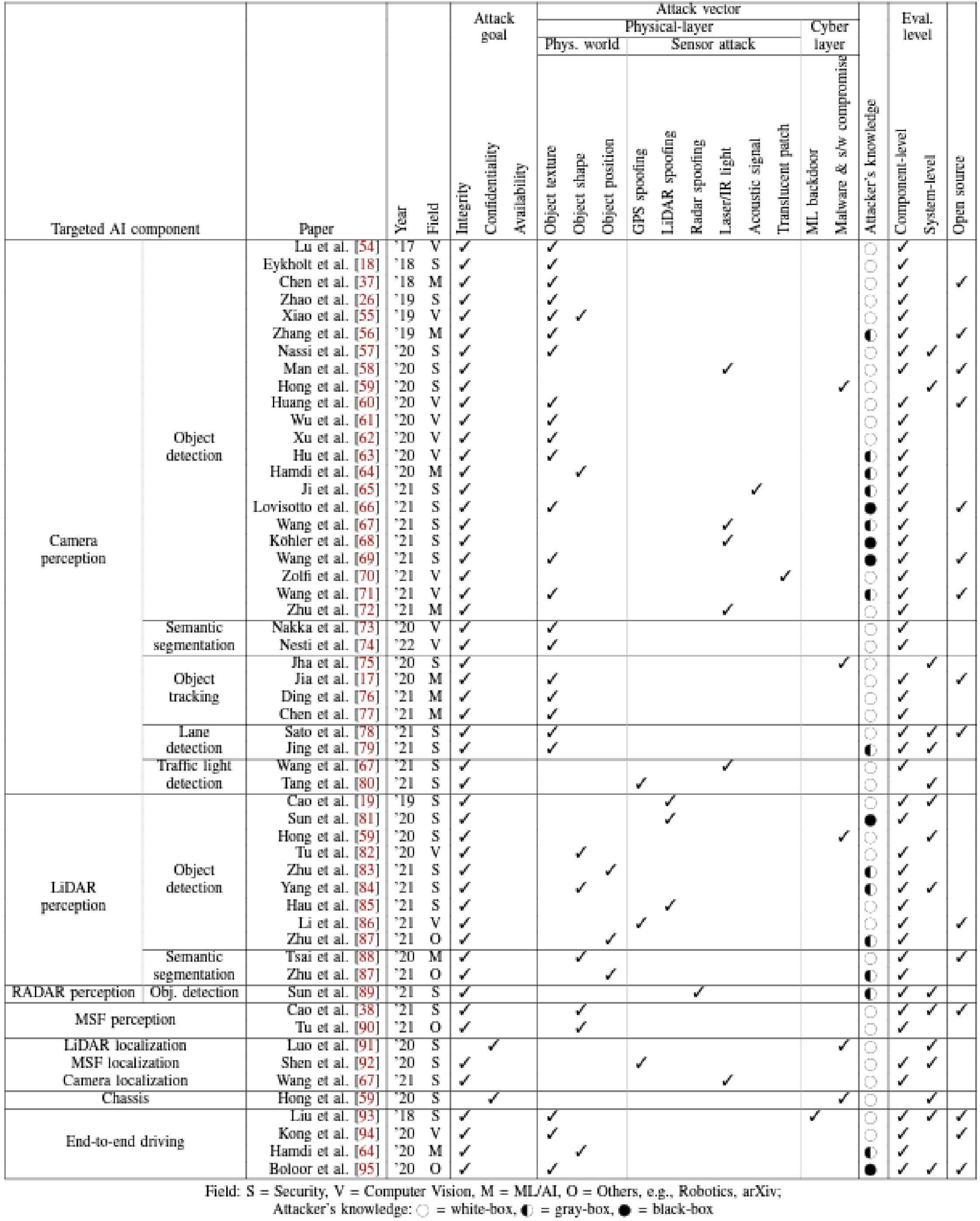


Figure 6: Distribution of (attack/defense) targeted AI components in semantic AD AI security papers.



					Attack goal			Attack vector												Eval. level		
								Physical-layer									Cyber layer					
								Phys. world			Sensor attack											
Targeted AI component		Paper	Year	Field	Integrity	Confidentiality	Availability	Object texture	Object shape	Object position	GPS spoofing	LiDAR spoofing	Radar spoofing	Laser/IR light	Acoustic signal	Translucent patch	ML backdoor	Malware & s/w compromise	Attacker's knowledge	Component-level	System-level	Open source
Camera perception	Object detection	Lu et al. [54]	'17	V	✓			✓											○	✓		
		Eykholt et al. [18]	'18	S	✓			✓											○	✓		
		Chen et al. [37]	'18	M	✓			✓											○	✓		✓
		Zhao et al. [26]	'19	S	✓			✓											○	✓		
		Xiao et al. [55]	'19	V	✓			✓	✓										○	✓		
		Zhang et al. [56]	'19	M	✓			✓											◐	✓		✓
		Nassi et al. [57]	'20	S	✓			✓											○	✓	✓	
		Man et al. [58]	'20	S	✓									✓					○	✓		✓
		Hong et al. [59]	'20	S	✓													✓	○		✓	
		Huang et al. [60]	'20	V	✓			✓											○	✓		✓
		Wu et al. [61]	'20	V	✓			✓											○	✓		
		Xu et al. [62]	'20	V	✓			✓											○	✓		
		Hu et al. [63]	'20	V	✓			✓											◐	✓		
		Hamdi et al. [64]	'20	M	✓				✓										◐	✓		
		Ji et al. [65]	'21	S	✓										✓				◐	✓		
		Lovisotto et al. [66]	'21	S	✓			✓											●	✓		✓
		Wang et al. [67]	'21	S	✓									✓					◐	✓		
		Köhler et al. [68]	'21	S	✓									✓					●	✓		
		Wang et al. [69]	'21	S	✓			✓											●	✓		✓
		Zolfi et al. [70]	'21	V	✓											✓			○	✓		
		Wang et al. [71]	'21	V	✓			✓											◐	✓		✓
		Zhu et al. [72]	'21	M	✓									✓					○	✓		
	Semantic segmentation	Nakka et al. [73]	'20	V	✓			✓											○	✓		
		Nesti et al. [74]	'22	V	✓			✓											○	✓		
	Object tracking	Jha et al. [75]	'20	S	✓													✓	○		✓	
		Jia et al. [17]	'20	M	✓			✓											○	✓		✓
		Ding et al. [76]	'21	M	✓			✓											○	✓		
		Chen et al. [77]	'21	M	✓			✓											○	✓		
	Lane detection	Sato et al. [78]	'21	S	✓			✓											○	✓	✓	✓
		Jing et al. [79]	'21	S	✓			✓											◐	✓	✓	
	Traffic light detection	Wang et al. [67]	'21	S	✓									✓					○	✓		
		Tang et al. [80]	'21	S	✓						✓								○		✓	
LiDAR perception	Object detection	Cao et al. [19]	'19	S	✓							✓							○	✓	✓	
		Sun et al. [81]	'20	S	✓							✓							●	✓		
		Hong et al. [59]	'20	S	✓													✓	○		✓	
		Tu et al. [82]	'20	V	✓				✓										○	✓		
		Zhu et al. [83]	'21	S	✓					✓									◐	✓		
		Yang et al. [84]	'21	S	✓				✓										◐	✓	✓	
		Hau et al. [85]	'21	S	✓							✓							○	✓		
		Li et al. [86]	'21	V	✓						✓								○	✓		✓
		Zhu et al. [87]	'21	O	✓					✓									◐	✓		
	Semantic segmentation	Tsai et al. [88]	'20	M	✓				✓										○	✓		✓
		Zhu et al. [87]	'21	O	✓					✓									◐	✓		
RADAR perception	Obj. detection	Sun et al. [89]	'21	S	✓								✓						◐	✓	✓	
MSF perception		Cao et al. [38]	'21	S	✓				✓										○	✓	✓	✓
		Tu et al. [90]	'21	O	✓				✓										○	✓		
LiDAR localization		Luo et al. [91]	'20	S		✓												✓	○		✓	
MSF localization		Shen et al. [92]	'20	S	✓						✓								○	✓	✓	
Camera localization		Wang et al. [67]	'21	S	✓									✓					○	✓		
Chassis		Hong et al. [59]	'20	S		✓												✓	○		✓	
End-to-end driving		Liu et al. [93]	'18	S	✓			✓									✓		○	✓	✓	✓
		Kong et al. [94]	'20	V	✓			✓											○	✓		✓
		Hamdi et al. [64]	'20	M	✓				✓										◐	✓		
		Boloor et al. [95]	'20	O	✓			✓											●	✓	✓	✓

Field: S = Security, V = Computer Vision, M = ML/AI, O = Others, e.g., Robotics, arXiv;
Attacker's knowledge: ○ = white-box, ◐ = gray-box, ● = black-box

Table I. Overview of existing semantic AD AI attacks in our SoK scope (§II-C). (s/w = software)

Our SoK effort: Scientific gaps identification

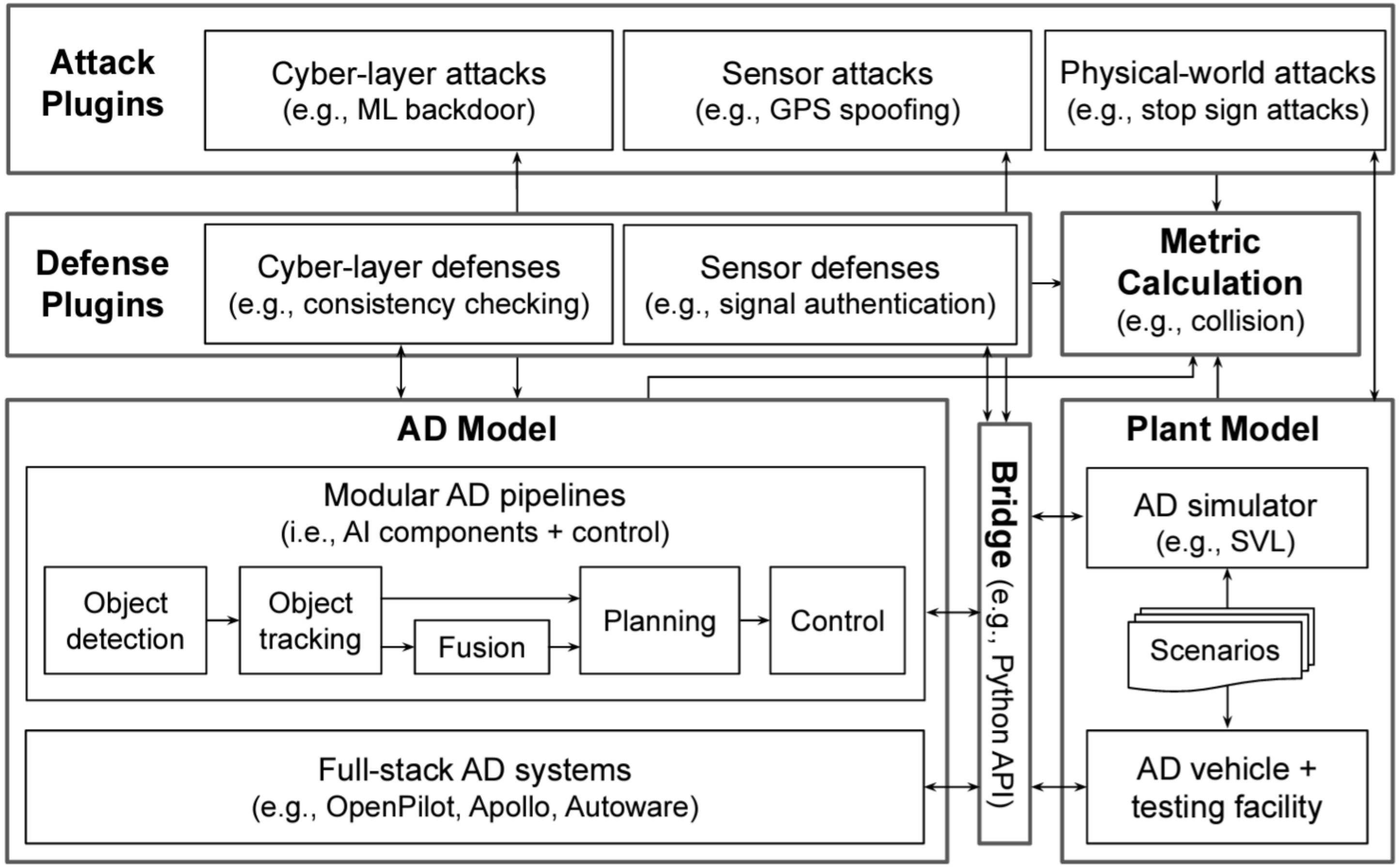
- Most importantly, identify **6 most substantial scientific gaps**
  - Observed based on quantitative comparisons both ***vertically*** among existing AD AI security works and ***horizontally*** with security works from closely-related domains
  - Scientific Gap 1: **Evaluation**: General lack of system-level evaluation
    - Only 25.4% of existing works perform system-level evaluation
  - Scientific Gap 2: **Research goal**: General lack of defense solutions
    - Only 14.3% propose defenses
    - In comparison, much more balanced in drone security area (49% on defense)
  - Scientific Gap 3: **Attack vector**: Cyber-layer attack vectors under-explored
    - Only 11.1% assume cyber-layer attack vectors, e.g., malware, ML backdoors
  - Scientific Gap 4: **Attack target**: Downstream AI components under-explored
    - Limited study on prediction & planning
  - Scientific Gap 5: **Attack goal**: Attack goals other than "integrity" under-explored
    - Limited study on confidentiality & availability
  - Scientific Gap 6: **Community**: Substantial Lack of Open Sourcing
    - <20.6% (7/34) papers from security conferences release source code

Our SoK effort

(https://arxiv.org/abs/2203.05314)

Our proposal: PASS (Platform for Autonomous driving Security and Safety)

- ***Open***, ***uniform*** & ***extensible*** system-driven evaluation platform



Attack Plugins
Cyber-layer attacks (e.g., ML backdoor)
Sensor attacks (e.g., GPS spoofing)
Physical-world attacks (e.g., stop sign attacks)
Defense Plugins
Cyber-layer defenses (e.g., consistency checking)
Sensor defenses (e.g., signal authentication)
Metric Calculation (e.g., collision)
AD Model
Modular AD pipelines (i.e., AI components + control)
Object detection
Object tracking
Fusion
Planning
Control
Full-stack AD systems (e.g., OpenPilot, Apollo, Autoware)
Bridge (e.g., Python API)
Plant Model
AD simulator (e.g., SVL)
Scenarios
AD vehicle + testing facility

Most recent focus (2018-): CPS AI security in automotive & transp. domains

- **CPS AI Security**
  - **Autonomous Driving (AD)** [ACM CCS'19, Usenix Security'20 (a), '20 (b), '21, IEEE S&P'21, NDSS'22, CVPR'22, ICLR'20]
  - **Intelligent transportation** [NDSS'18, TRB'18,'19,'20, ITS'21]
- **Network Security**
  - **Connected Vehicle (CV)** [Usenix Security'21]
  - **Automotive IoT** [Usenix Security'20, NDSS'20]
  - **Network protocol** [ACM CCS'15,'18, IEEE S&P'16]
- **UI (User Interface) Security**
  - **Smartphone** [Usenix Security'14, MobiSys'19]
- **Access Control / Policy Enforcement**
  - **Smartphone** [NDSS'16]
  - **Smart home** [NDSS'17]
- **Side Channel**
  - **Smartphone** [Usenix Security'14]
  - **Network** [ACM CCS'15]

Autonomous Driving (AD)

V2X-based Intelligent Transp.

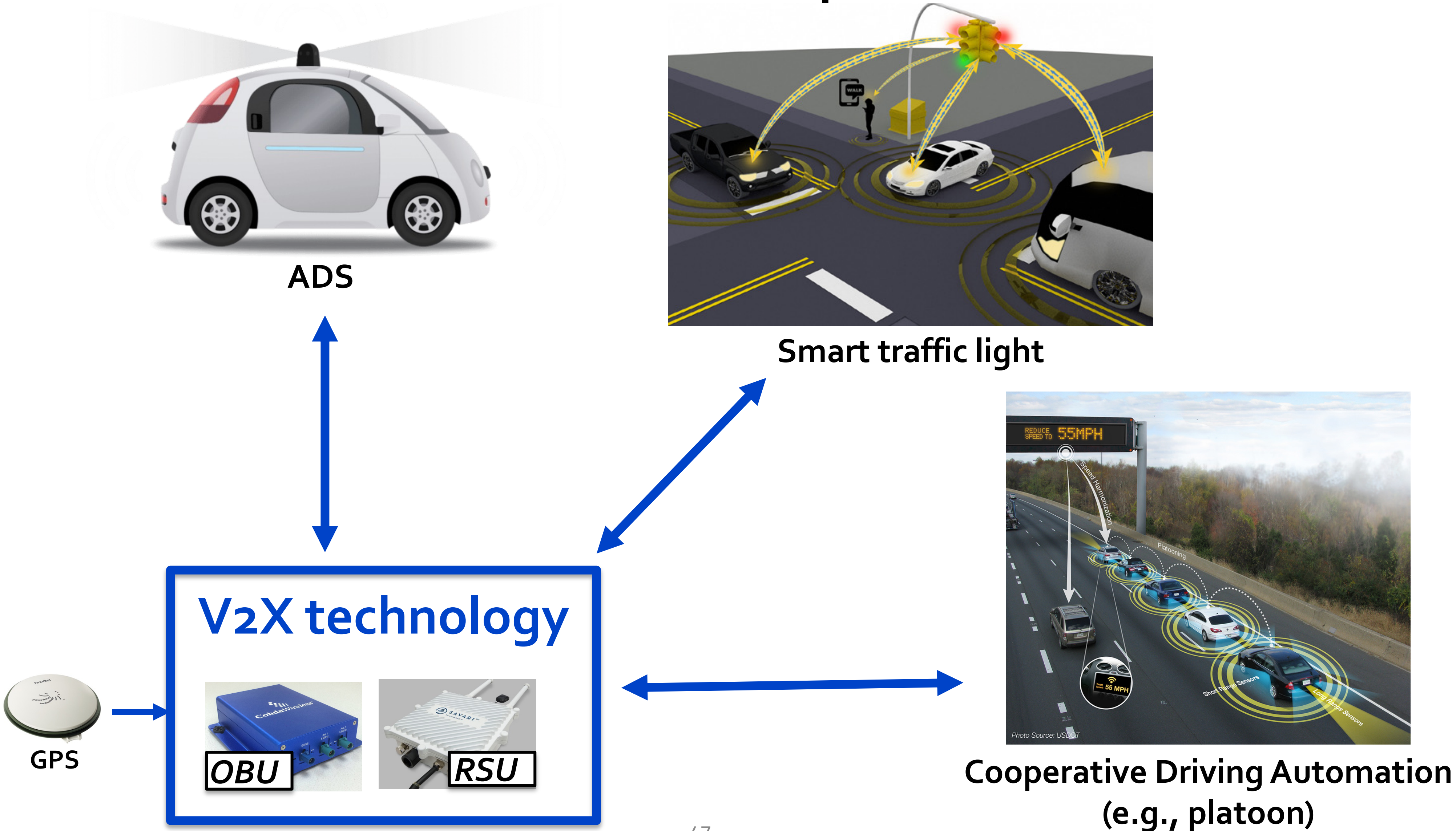
Most recent focus (2018-): CPS AI security in automotive & transp. domains

- **CPS AI Security**
  - **Autonomous Driving (AD)** [ACM CCS'19, Usenix Security'20 (a), '20 (b), '21, IEEE S&P'21, NDSS'22, CVPR'22, ICLR'20]
  - **Intelligent transportation** [NDSS'18, TRB'18,'19,'20, ITS'21]
- **Network Security**
  - **Connected Vehicle (CV)** [Usenix Security'21]
  - **Automotive IoT** [Usenix Security'20, NDSS'20]
  - **Network protocol** [ACM CCS'15,'18, IEEE S&P'16]
- **UI (User Interface) Security**
  - **Smartphone** [Usenix Security'14, MobiSys'19]
- **Access Control / Policy Enforcement**
  - **Smartphone** [NDSS'16]
  - **Smart home** [NDSS'17]
- **Side Channel**
  - **Smartphone** [Usenix Security'14]
  - **Network** [ACM CCS'15]

Autonomous Driving (AD)

V2X-based Intelligent Transp.

V2X-enabled transportation AI



ADS

Smart traffic light

Cooperative Driving Automation (e.g., platoon)

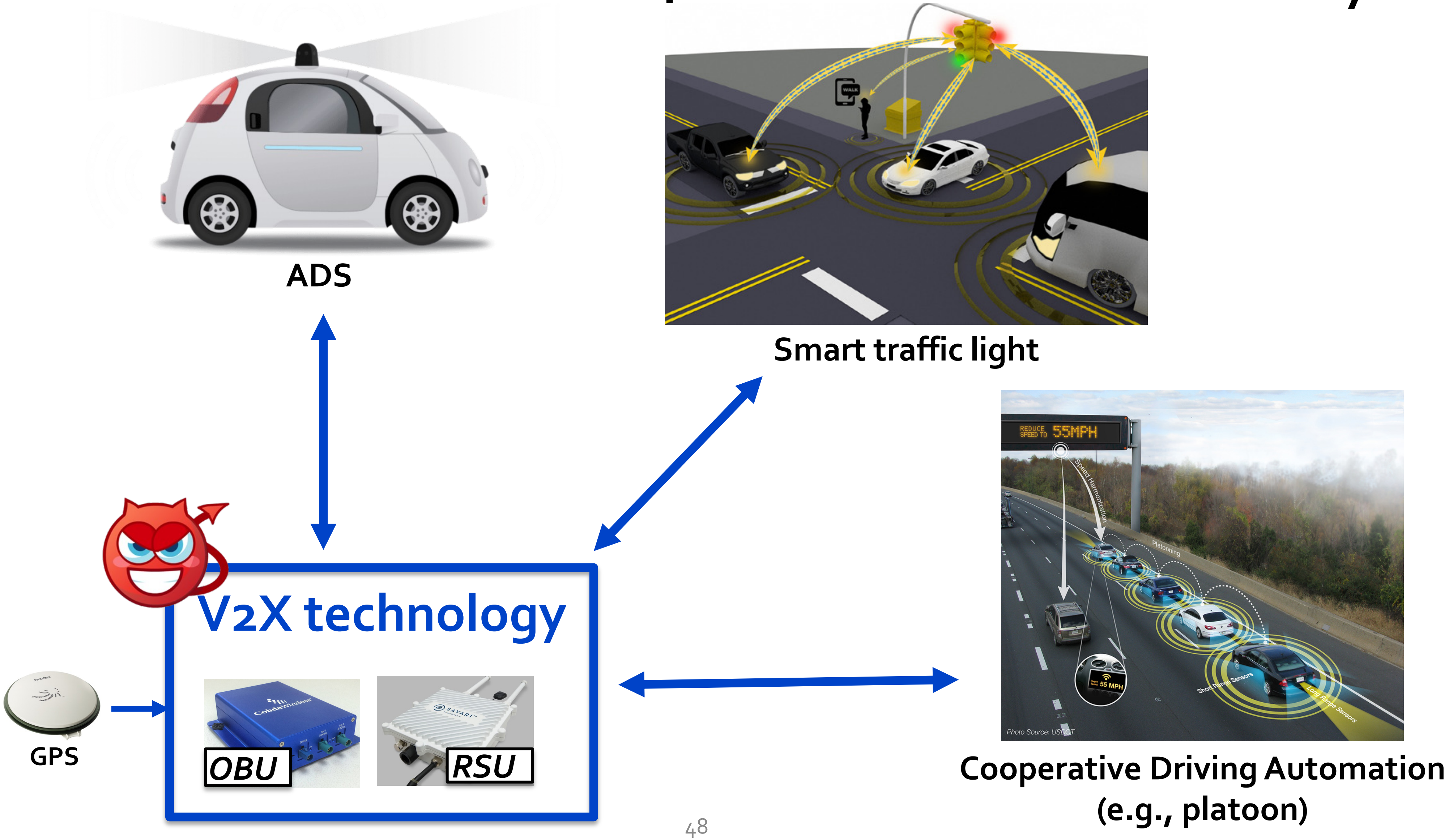
V2X technology

OBU

RSU

GPS

V2X-enabled transportation AI Security



ADS

Smart traffic light

Cooperative Driving Automation (e.g., platoon)

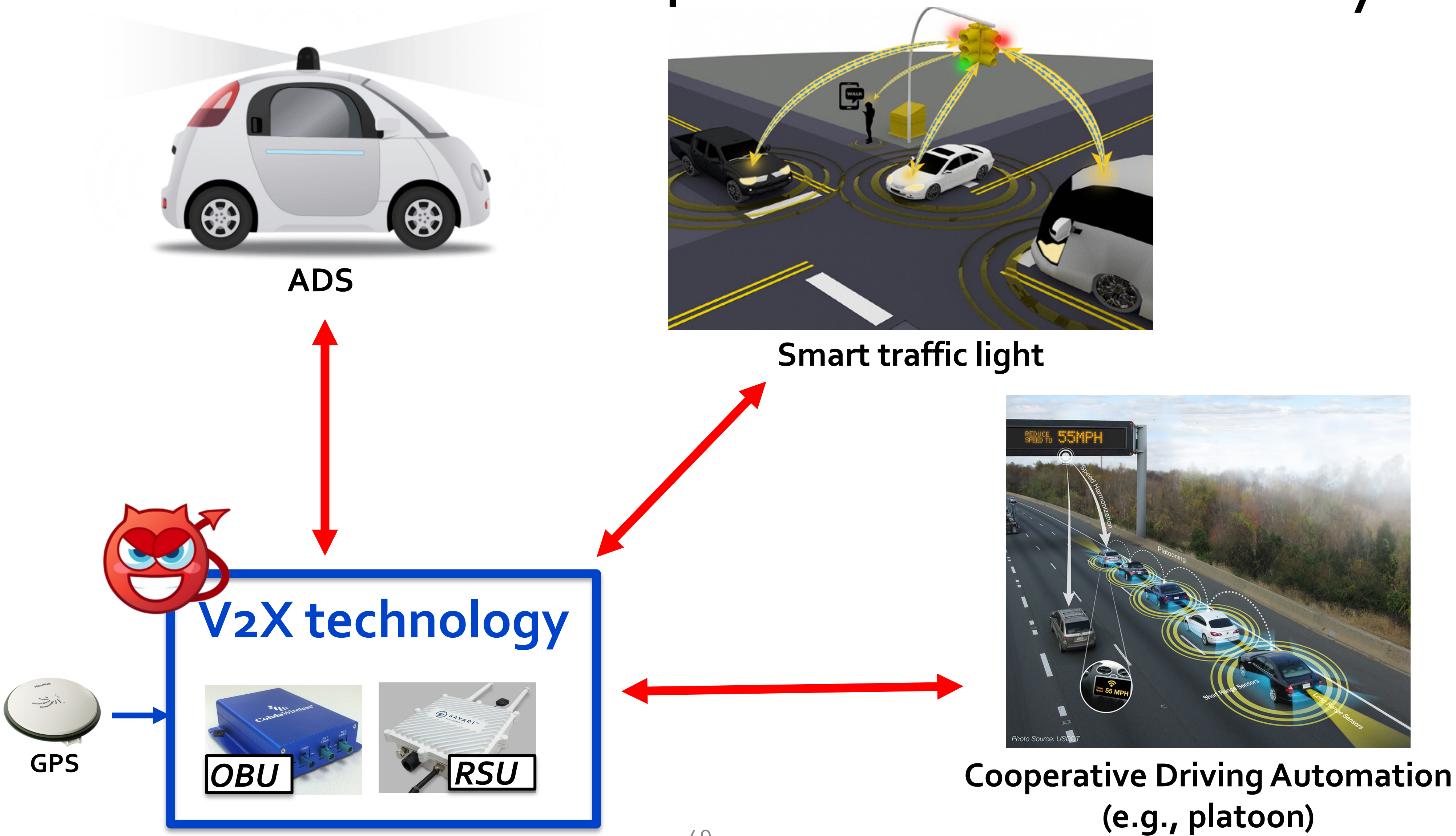
V2X technology

OBU

RSU

GPS

V2X-enabled transportation AI Security



ADS

Smart traffic light

V2X technology

OBU

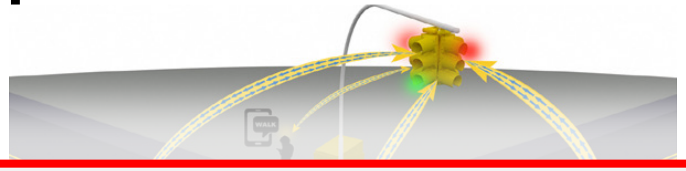
RSU

GPS

Photo Source: USDOT

Cooperative Driving Automation (e.g., platoon)

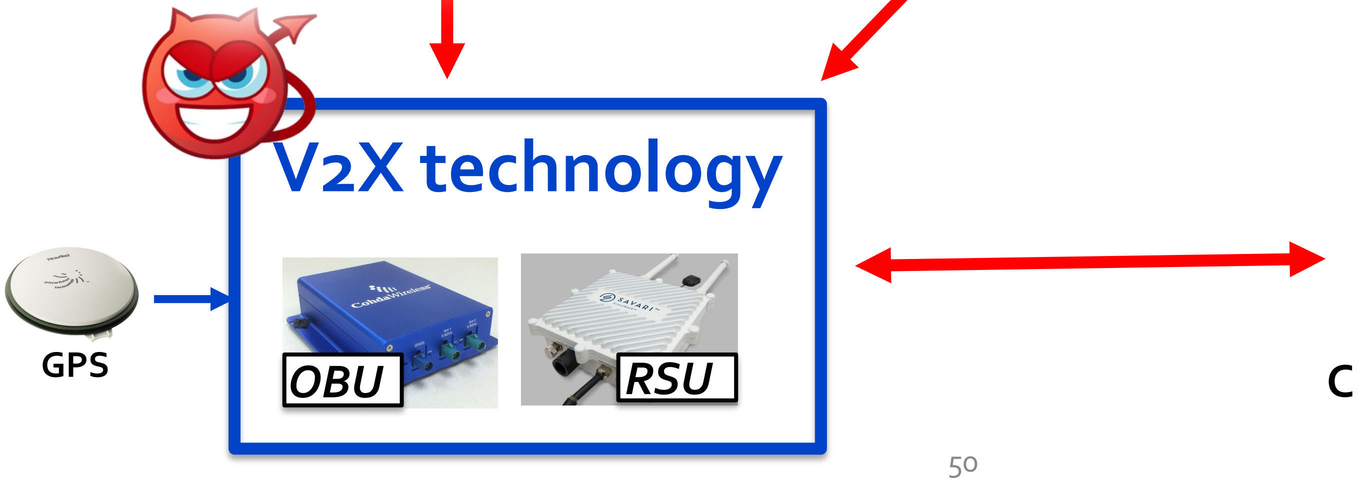
V2X-enabled transportation AI Security

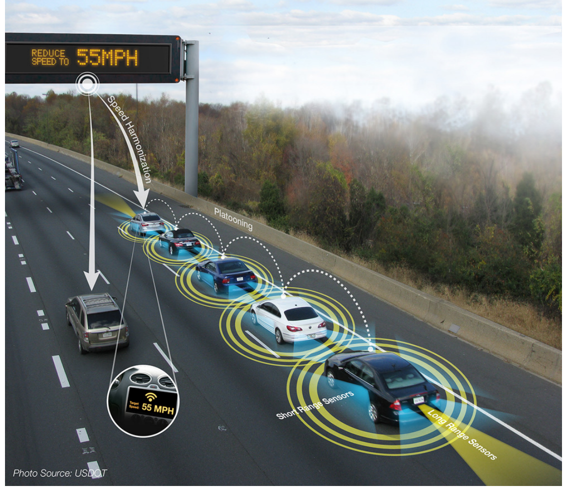


Malicious vehicle owners deliberately control OBU to broadcast spoofed V2X data

- OBU itself is compromised physically[1], wirelessly[2], or by malware[3]
- Compromise OBU input using sensor attacks

Smart traffic light

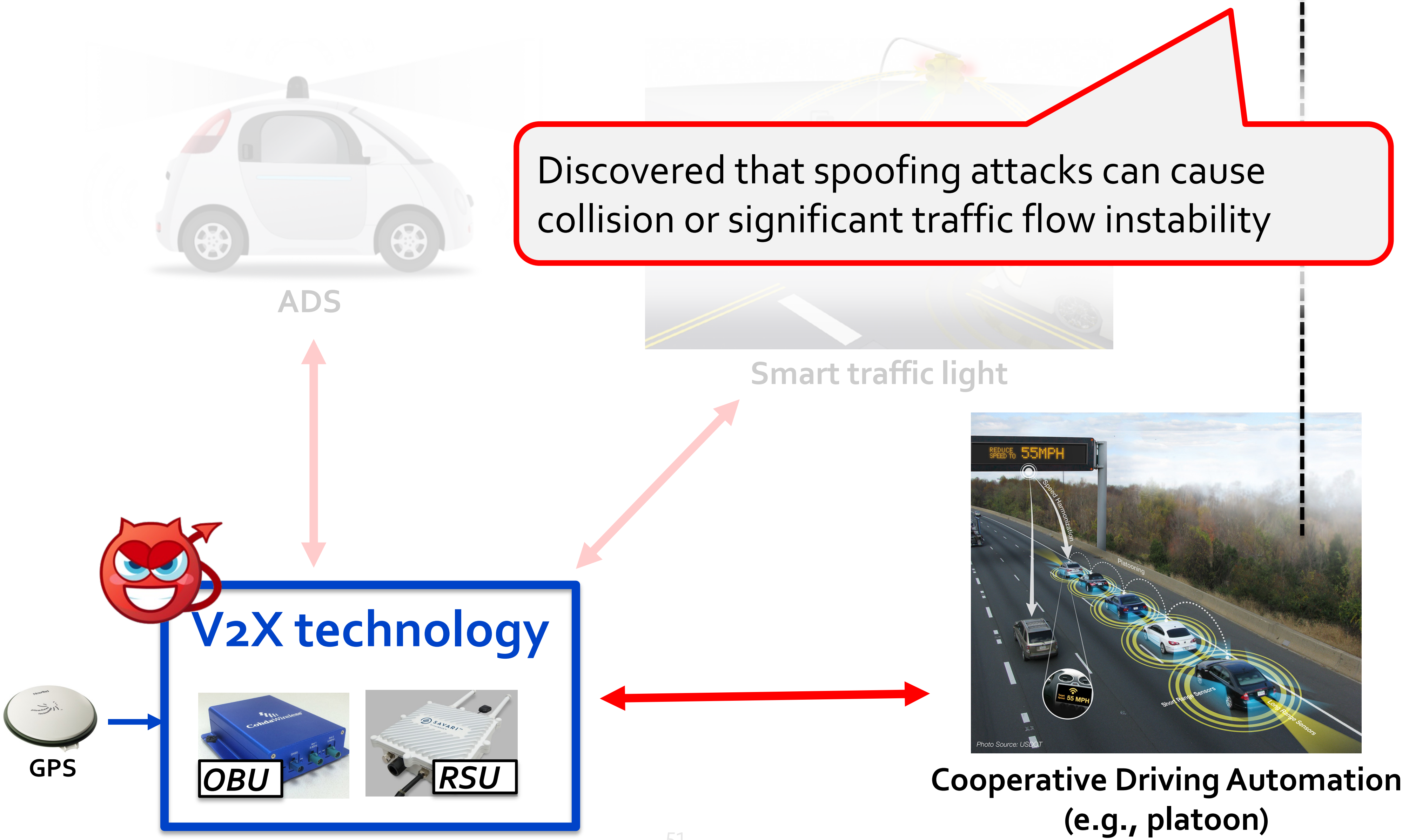




Cooperative Driving Automation (e.g., platoon)

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

IEEE Comm. Mag.'15, …, RAID'19



Discovered that spoofing attacks can cause collision or significant traffic flow instability

Usenix Security'21

IEEE Comm. Mag.'15, …, RAID'19

First to design automatic vuln discovery method using ***model checking*** *(a formal method)*

- Impact: **Automatically** discover ***14 new design flaws*** that can cause DoS or decrease flow stability

Smart traffic light

GPS

V2X technology

OBU

RSU

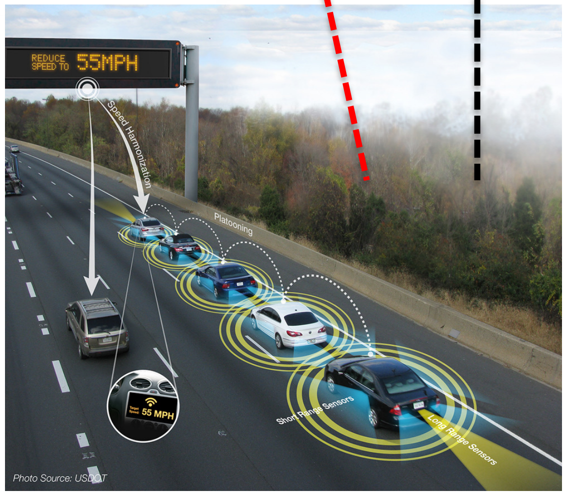


Photo Source: USDOT

Cooperative Driving Automation (e.g., platoon)

Results highlights [Usenix Security'21]

- **19 discovered vuln (*18 new* *compared to manual discovery in prior works!*)**
  - ***4 (all new)*** from P2PCD (Peer-to-Peer Certificate Distribution) protocol in IEEE 1609
  - ***15 (14 new)*** from 2 popular platoon protocols (VENTOS, PLEXE)

ID	**Name**	**Implications**
N1	Response Mute	Stop the CV device from sending learning responses
N2, N3	Request Mute	Stop the CV device from sending learning requests
N4	Numb	Stop the CV device from recording unknown certificates
A1, A2	(Prerequisites)	Cause traffic collision [1], lead to A3-15
A3, A4	Split Trigger	Interfere the traffic flow stability, decrease efficiency and safety
A5-14	PMP Block	Prevent platoon members from performing any maneuvers
A15	Inconsistency	Lead to failures of the split maneuver and the leader/follower leave maneuver

N*: CV network protocol, P2PCD A*: CV application, PMP

[1] Abdo et al. Application level attacks on connected vehicle protocols. RAID 2019

Results highlights [Usenix Security'21]

- **19 discovered vuln (*18 new* *compared to manual discovery in prior works!*)**
  - ***4 (all new)*** from P2PCD (Peer-to-Peer Certificate Distribution) protocol in IEEE 1609
  - ***15 (14 new)*** from 2 popular platoon protocols (VENTOS, PLEXE)

ID	**Name**	**Implications**
N1	Response Mute	Stop the CV device from sending learning responses
N2, N3	Request Mute	Stop the CV device from sending learning requests
N4	Numb	Stop the CV device from recording unknown certificates
A1, A2	(Prerequisites)	Cause traffic collision [1], lead to A3-15
A3, A4	Split Trigger	Interfere the traffic flow stability, decrease efficiency and safety
A5-14	PMP Block	Prevent platoon members from performing any maneuvers
A15	Inconsistency	Lead to failures of the split maneuver and the leader/follower leave maneuver

N*: CV network protocol, P2PCD A*: CV application, PMP

[1] Abdo et al. Application level attacks on connected vehicle protocols. RAID 2019

Results highlights [Usenix Security’21]

- **19 discovered vuln** (*18*
  - ***4 (all new)*** from P2PCD
  - ***15 (14 new)*** from 2 popu

ID	**Name**	**Im**
N1	Response Mute	Sto
N2, N3	Request Mute	Sto
N4	Numb	Stop
A1, A2	(Prerequisites)	Cau
A3, A4	Split Trigger	Int
A5-14	PMP Block	Pre
A15	Inconsistency	Lead to failures of the split maneuver and the leader/follower leave maneuver

<u>Representative design-level causes</u>:

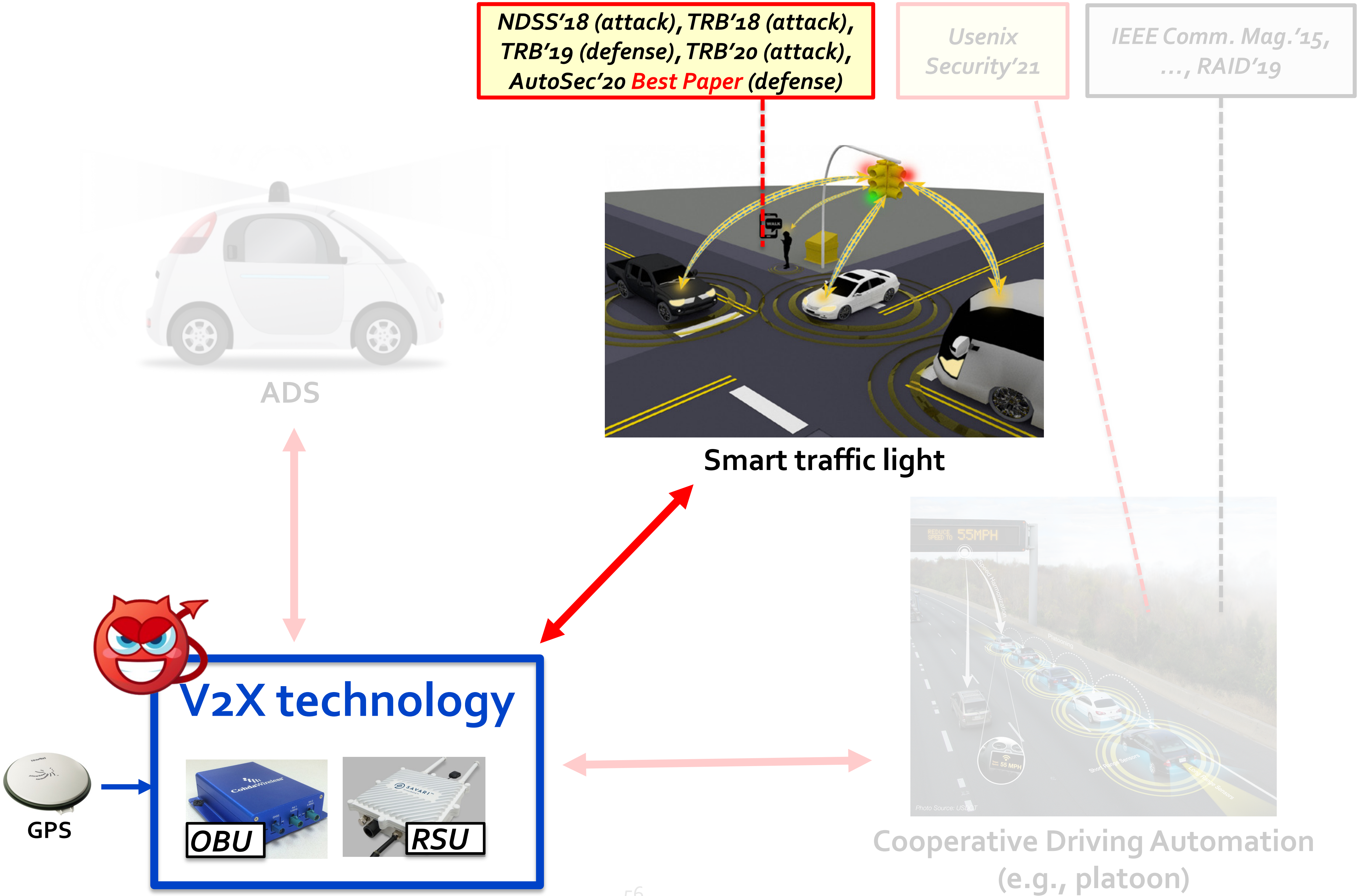
- Use **short hash** size for certificate matching
  - E.g., ***3 bytes*** in P2PCD for performance purposes → only ***10k* offline** certificate generation to find a collision due to the birthday paradox!
- Allow **unicast** message when the design **assumes broadcast** messages (e.g., message volume throttling)
- Lack of handling for **non-responding receiver**
- Lack of consistency-checking for **global states** (e.g., whether a platoon member lies about its position)

Reported to & **received vuln acknowledgements** for *all 4 newly-discovered P2PCD vulns* from **IEEE 1609 Working Group**

- Discussed **mitigation solutions**, planned to be integrated into the next version of IEEE 1609.2

N*: CV network protocol, P2PCD A*: CV application, PMP

[1] Abdo et al. Application level attacks on connected vehicle protocols. RAID 2019



NDSS'18 (attack), TRB'18 (attack), TRB'19 (defense), TRB'20 (attack), AutoSec'20 Best Paper (defense)

Usenix Security'21

IEEE Comm. Mag.'15, …, RAID'19

ADS

Smart traffic light

V2X technology

OBU

RSU

GPS

Cooperative Driving Automation (e.g., platoon)

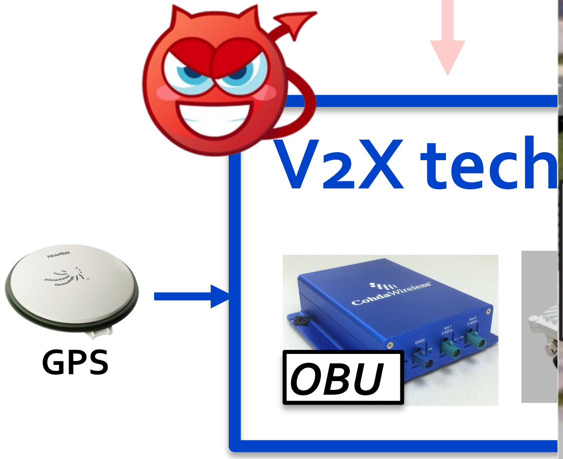
NDSS'18 (attack), TRB'18 (attack), TRB'19 (defense), TRB'20 (attack), AutoSec'20 Best Paper (defense)

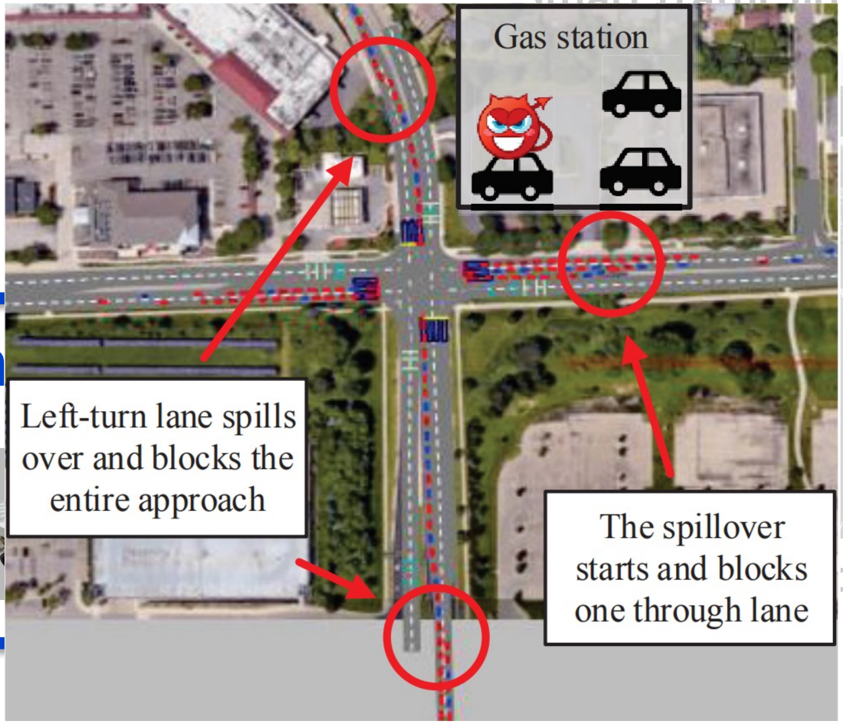
Usenix Security'21

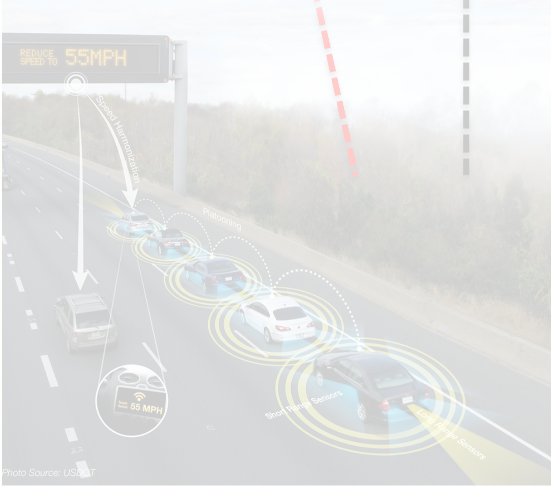
IEEE Comm. Mag.'15, …, RAID'19

First to study security of infrastructure-side V2X systems

- Target: USDOT Intelligent Traffic Signal (I-SIG) system
- Attack vector: V2X data spoofing
- Impact: ***One single attack vehicle can create massive traffic jams!***
  - Root cause: New security vuln at ***traffic control algorithm*** level
  - Demo: https://sites.google.com/view/cav-sec/congestion-attack




Gas station
Left-turn lane spills over and blocks the entire approach
The spillover starts and blocks one through lane



operative Driving Automation (e.g., platoon)

NDSS'18 (attack), TRB'18 (attack), TRB'19 (defense), TRB'20 (attack), AutoSec'20 Best Paper (defense)

Usenix Security'21

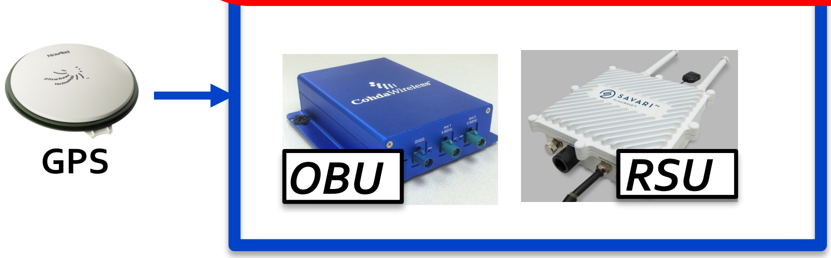
IEEE Comm. Mag.'15, …, RAID'19

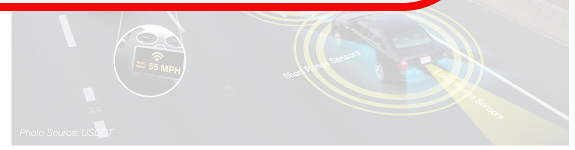
First to study security of infrastructure-side V2X systems

- Target: USDOT Intelligent Traffic Signal (I-SIG) system
- Attack vector: V2X data spoofing
- Impact: ***One single attack vehicle can create massive traffic jams!***
  - Root cause: New security vuln at ***traffic control algorithm*** level
  - Demo: https://sites.google.com/view/cav-sec/congestion-attack

Defenses:

- [TRB'19] Trajectory-based attack detection at ***transportation infrastructure*** side
- [AutoSec'20 ***Best Paper Award***] Hardware-based spoofing prevention at ***vehicle*** side





Cooperative Driving Automation (e.g., platoon)

Conclusion

- **My group: AI/systems/network security** in **mobile/IoT/CPS,** most recently actively working on **CPS AI security**, especially autonomous driving & intelligent transportation
  - Collection of our efforts: **https://sites.google.com/view/cav-sec**
- ***Only the beginning*** of this research problem space
  - Now mostly on attack side, need more on ***defense*** side
  - To facilitate community building:
    - Co-found ***ISOC Symposium on Vehicle Security & Privacy (VehicleSec) in 2023***
      - *Co-locate w/* ***NDSS at San Diego****, build upon* ***4 years*** *of* ***AutoSec Workshop*** *(also* ***co-found by me****)*

VehicleSec2023@NDSS

@vehiclesec_conf

Follow our Twitter for latest news: @vehiclesec_conf

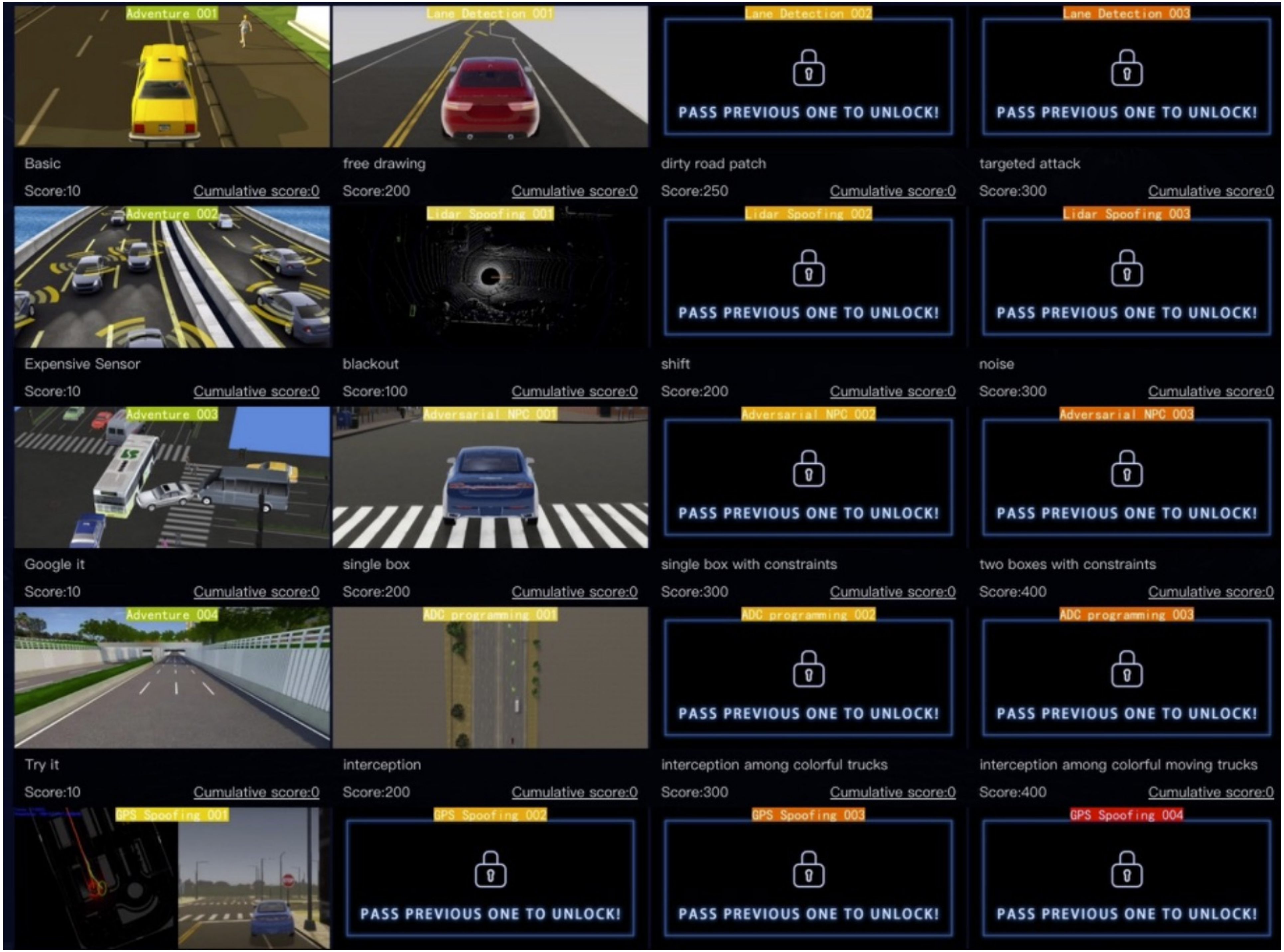
Conclusion

- **My group: AI/systems/network security** in **mobile/IoT/CPS,** most recently actively working on **CPS AI security**, especially autonomous driving & intelligent transportation
  - Collection of our efforts: **https://sites.google.com/view/cav-sec**
- ***Only the beginning*** of this research problem space
  - Now mostly on attack side, need more on ***defense*** side
  - To facilitate community building:
    - Co-found ***ISOC Symposium on Vehicle Security & Privacy (VehicleSec) in 2023***
      - *Co-locate w/* ***NDSS at San Diego****, build upon* ***4 years*** *of* ***AutoSec Workshop*** *(also* ***co-found by me****)*
    - Co-created ***DEF CON's first AutoDriving-themed hacking competition*** in 2021 (one of world's most famous hacker convention)

VehicleSec
Symposium on
Vehicle Security & Privacy

AutoDriving CTF

DEF CON 29



Adventure 001

Basic

Score:10 Cumulative score:0

Lane Detection 001

free drawing

Score:200 Cumulative score:0

Lane Detection 002

PASS PREVIOUS ONE TO UNLOCK!

dirty road patch

Score:250 Cumulative score:0

Lane Detection 003

PASS PREVIOUS ONE TO UNLOCK!

targeted attack

Score:300 Cumulative score:0

Adventure 002

Expensive Sensor

Score:10 Cumulative score:0

Lidar Spoofing 001

blackout

Score:100 Cumulative score:0

Lidar Spoofing 002

PASS PREVIOUS ONE TO UNLOCK!

shift

Score:200 Cumulative score:0

Lidar Spoofing 003

PASS PREVIOUS ONE TO UNLOCK!

noise

Score:300 Cumulative score:0

Adventure 003

Google it

Score:10 Cumulative score:0

Adversarial NPC 001

single box

Score:200 Cumulative score:0

Adversarial NPC 002

PASS PREVIOUS ONE TO UNLOCK!

single box with constraints

Score:300 Cumulative score:0

Adversarial NPC 003

PASS PREVIOUS ONE TO UNLOCK!

two boxes with constraints

Score:400 Cumulative score:0

Adventure 004

Try it

Score:10 Cumulative score:0

ADC programming 001

interception

Score:200 Cumulative score:0

ADC programming 002

PASS PREVIOUS ONE TO UNLOCK!

interception among colorful trucks

Score:300 Cumulative score:0

ADC programming 003

PASS PREVIOUS ONE TO UNLOCK!

interception among colorful moving trucks

Score:400 Cumulative score:0

GPS Spoofing 001

GPS Spoofing 002

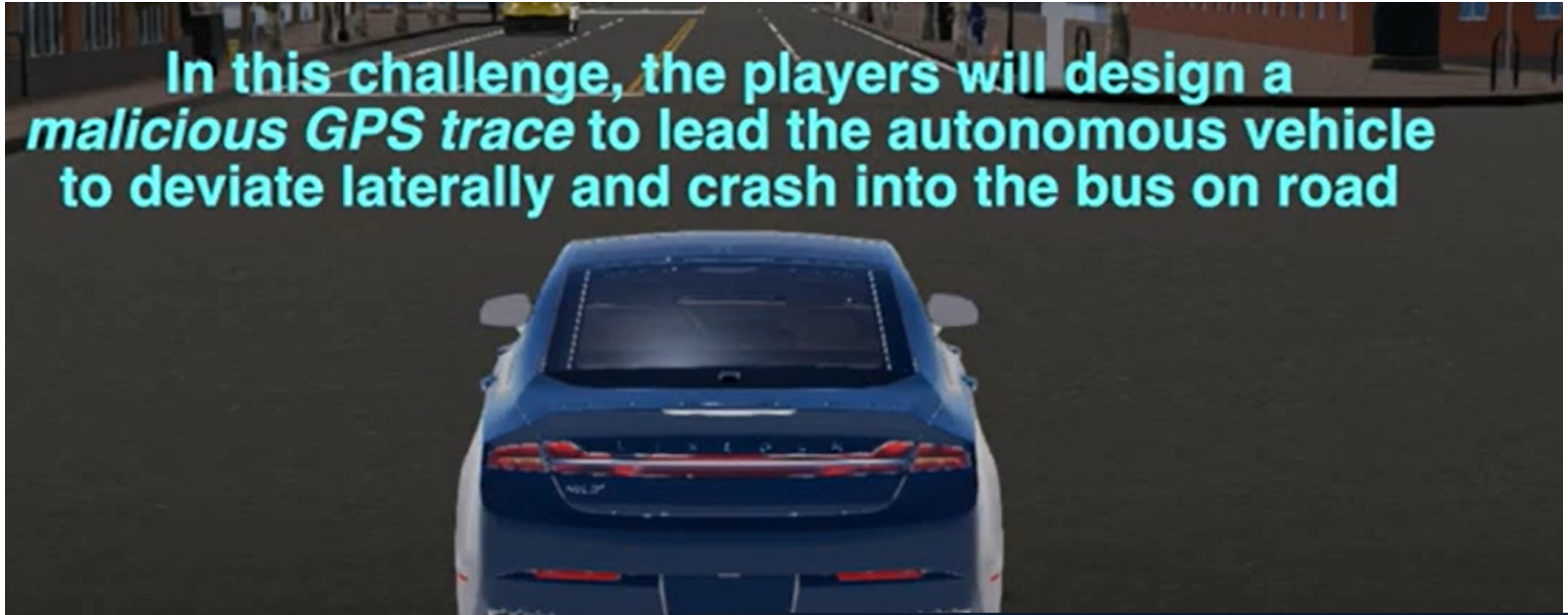
PASS PREVIOUS ONE TO UNLOCK!

GPS Spoofing 003

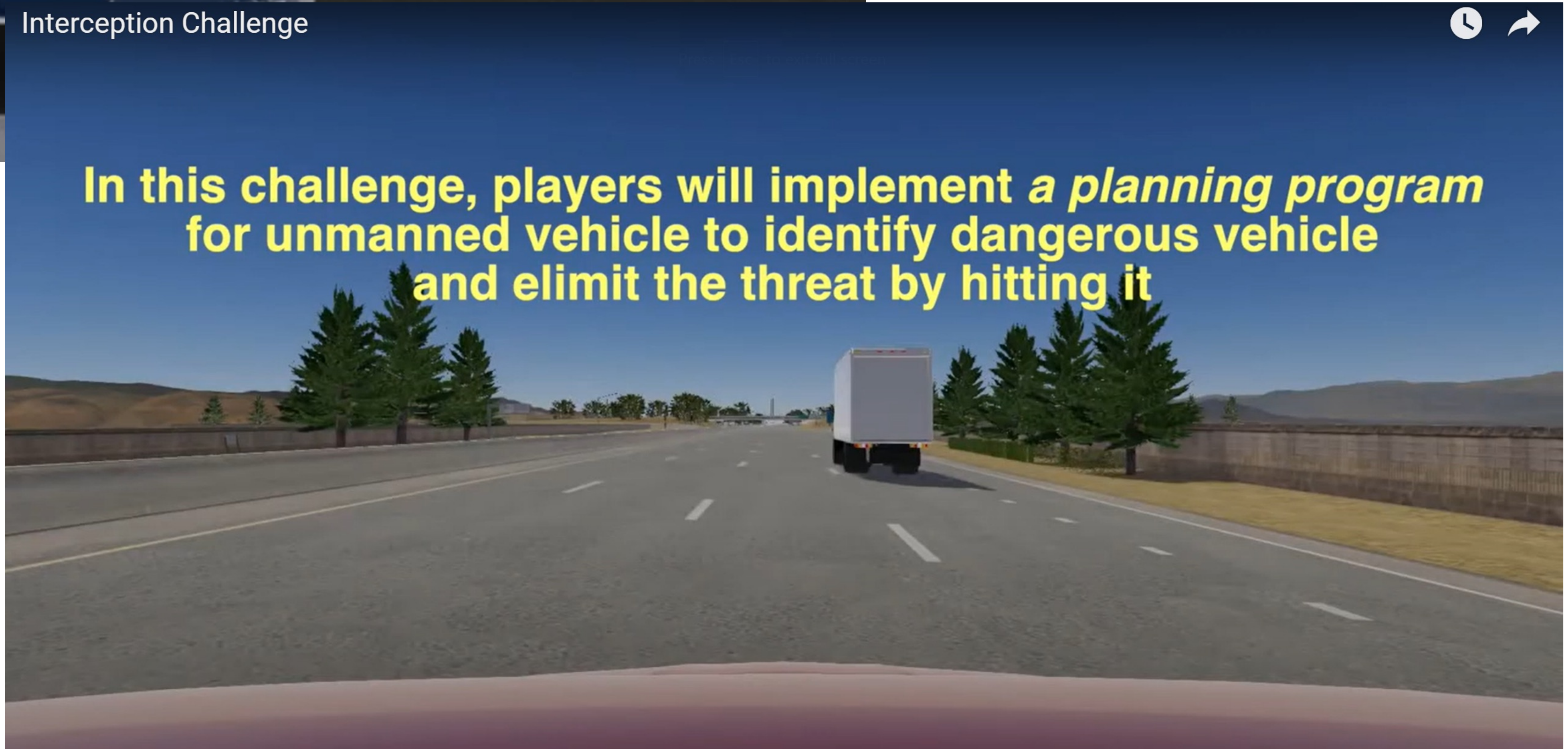
PASS PREVIOUS ONE TO UNLOCK!

GPS Spoofing 004

PASS PREVIOUS ONE TO UNLOCK!



In this challenge, the players will design a *malicious GPS trace* to lead the autonomous vehicle to deviate laterally and crash into the bus on road

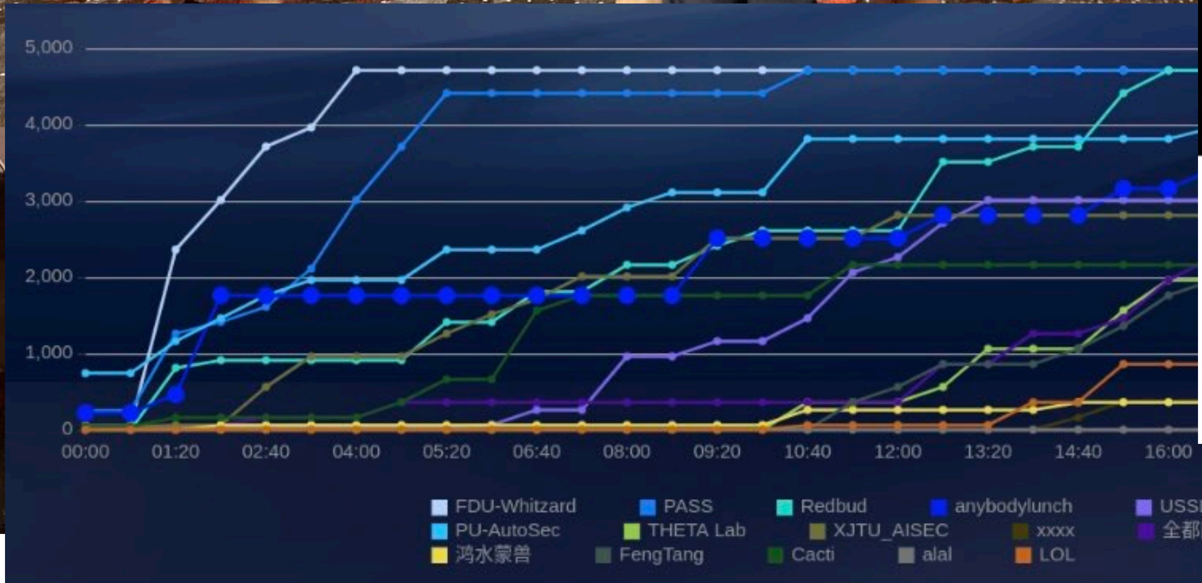


Interception Challenge

In this challenge, players will implement *a planning program* for unmanned vehicle to identify dangerous vehicle and elimit the threat by hitting it

Last year, 2nd AutoDriving CTF at DEF CON, Vegas!

Stay tuned for our 2023 event to win a DEF CON title!
(Twitter @autodrivingctf)



AutoDriving CTF
@autodrivingctf Follows you

Conclusion

- **My group: AI/systems/network security** in **mobile/IoT/CPS,** most recently actively working on **CPS AI security**, especially autonomous driving & intelligent transportation
  - Collection of our efforts: https://sites.google.com/view/cav-sec
- ***Only the beginning*** of this research problem space
  - Now mostly on attack side, need more on ***defense*** side
  - To facilitate community building:
    - Co-found ***ISOC Symposium on Vehicle Security & Privacy (VehicleSec) in 2023***
      - *Co-locate w/* ***NDSS at San Diego****, build upon* ***4 years*** *of* ***AutoSec Workshop*** *(also* ***co-found by me****)*
    - Co-created ***DEF CON's first AutoDriving-themed hacking competition*** in 2021 (one of world's most famous hacker convention)
    - Served on **NIST focused group & panel on *AD AI test standards & metrics***

Sponsors:

NSF

DEPARTMENT OF TRANSPORTATION UNITED STATES OF AMERICA

gm

TOYOTA

Qualcomm

VehicleSec
Symposium on
Vehicle Security & Privacy

AutoDriving CTF

DEF CON 29

NIST
National Institute
of Standards
and Technology

Conclusion

- **My group: AI/systems/network security** in **mobile/IoT/CPS,** most recently actively working on **CPS AI security**, especially autonomous driving & intelligent transportation
  - Collection of our efforts: **https://sites.google.com/view/cav-sec**
- ***Only the beginning*** of this research problem space
  - Now mostly on attack side, need more on ***defense*** side
  - To facilitate community building:
    - Co-found ***ISOC Symposium on Vehicle Security & Privacy (VehicleSec) in 2023***
      - *Co-locate w/ **NDSS at San Diego**, build upon **4 years** of **AutoSec Workshop** (also **co-found by me**)*
    - Co-created ***DEF CON's first AutoDriving-themed hacking competition*** in 2021 (one of world's most famous hacker convention)
    - Served on **NIST focused group & panel on *AD AI test standards & metrics***
- **Happy to chat more & seek collaboration with AUTOSAR!**
  - *E.g., standards/interfaces for **data-plane attacks** (sensor data tampering, V2X data spoofing)?*

Sponsors:

NSF

DEPARTMENT OF TRANSPORTATION UNITED STATES OF AMERICA

gm

TOYOTA

Qualcomm

Contact

Alfred Chen (alfchen@uci.edu)

Homepage:https://www.ics.uci.edu/~alfchen/

AS²Guard Autonomous & Smart Systems Guard Research Group

VehicleSec Symposium on Vehicle Security & Privacy

AutoDriving CTF

DEF CON 29