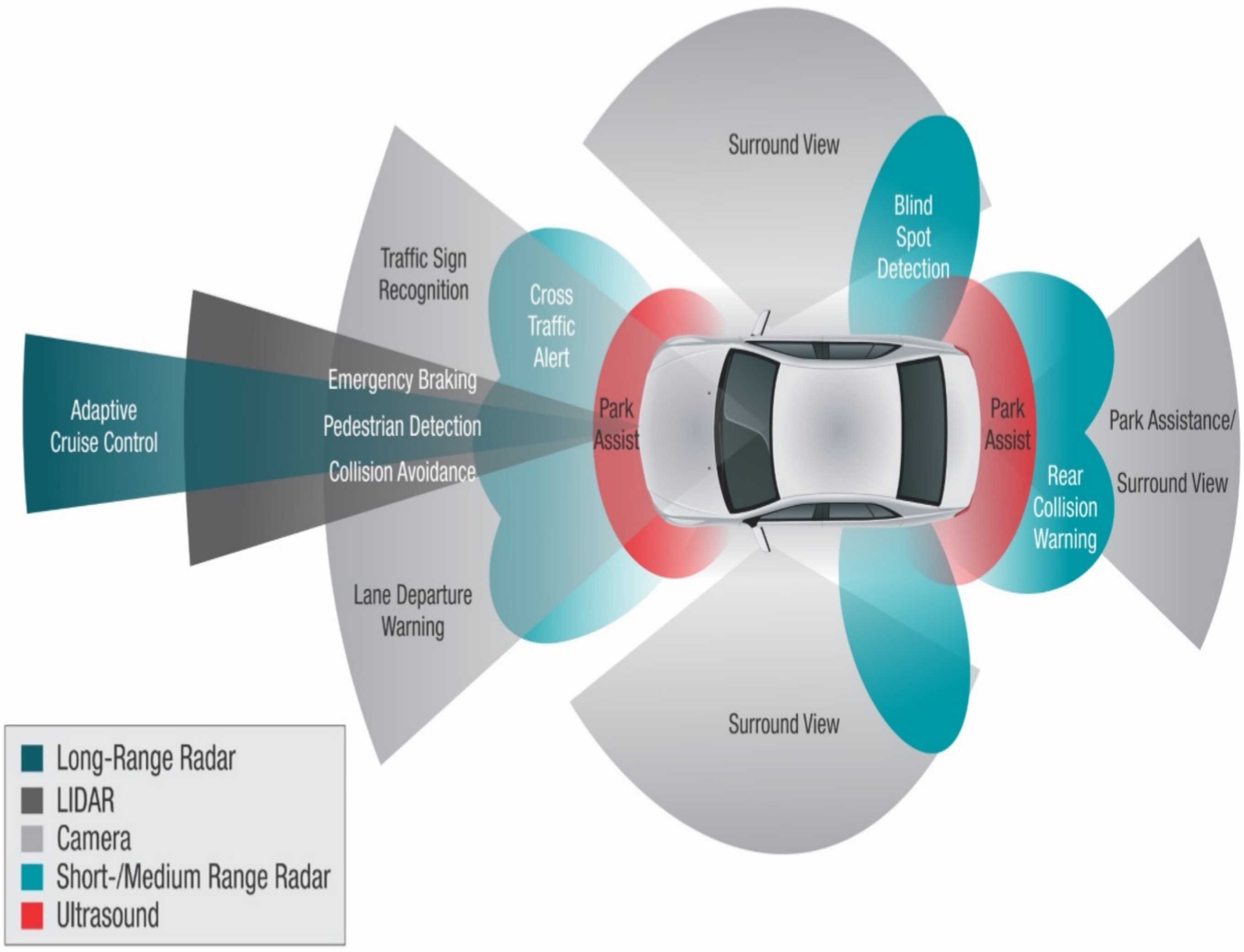
Attacking Self-driving Cars

Yongdae Kim

SysSec@KAIST

Sensors for Autonomous Vehicles



❖ Proximity (5m).
: Ultrasonic sensors
(Parking assistance)

❖ Short Range (30m).
: Cameras, Short-range radars
(Traffic sign recognition, Parking assistance)

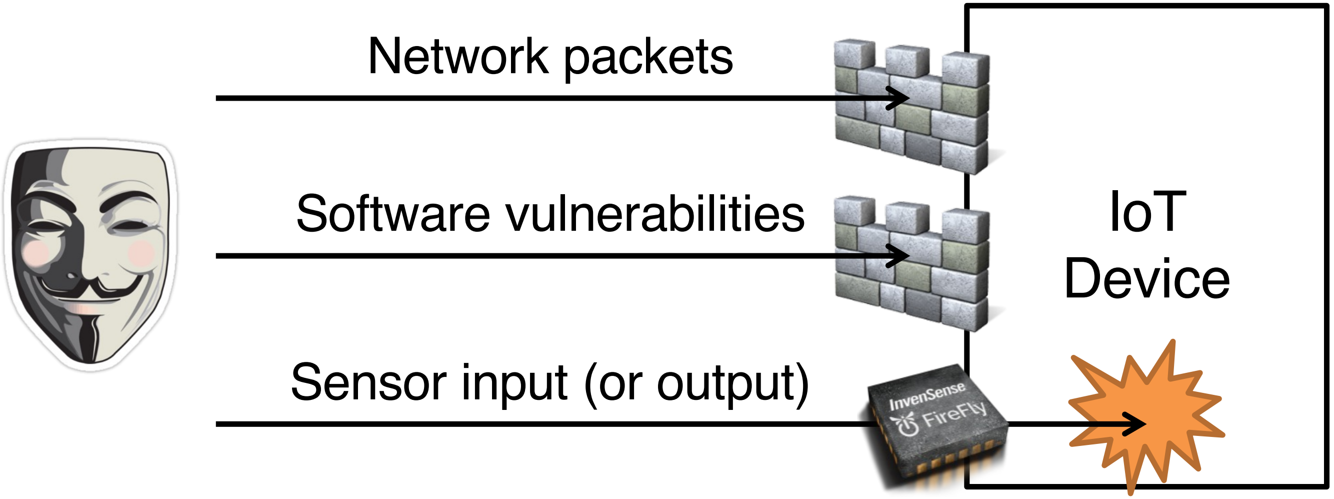
❖ Medium Range (80m)
: LiDAR and Medium range
radars (MRR)
(Collision avoidance, Pedestrian detection)

❖ Long Range (250m)
: Long-range radars (LRR)
(High speed)

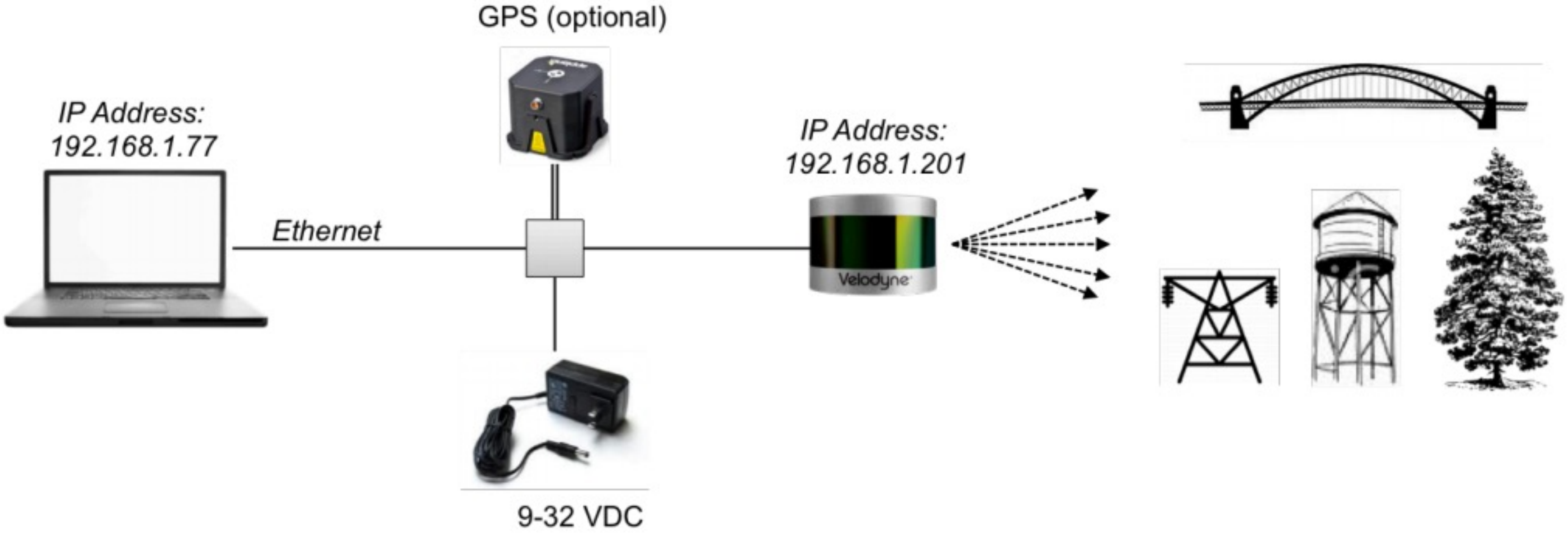
Sensor & Security

- ❑ Many prevention and detection mechanisms
  - For malicious network traffics
  - For software vulnerabilities

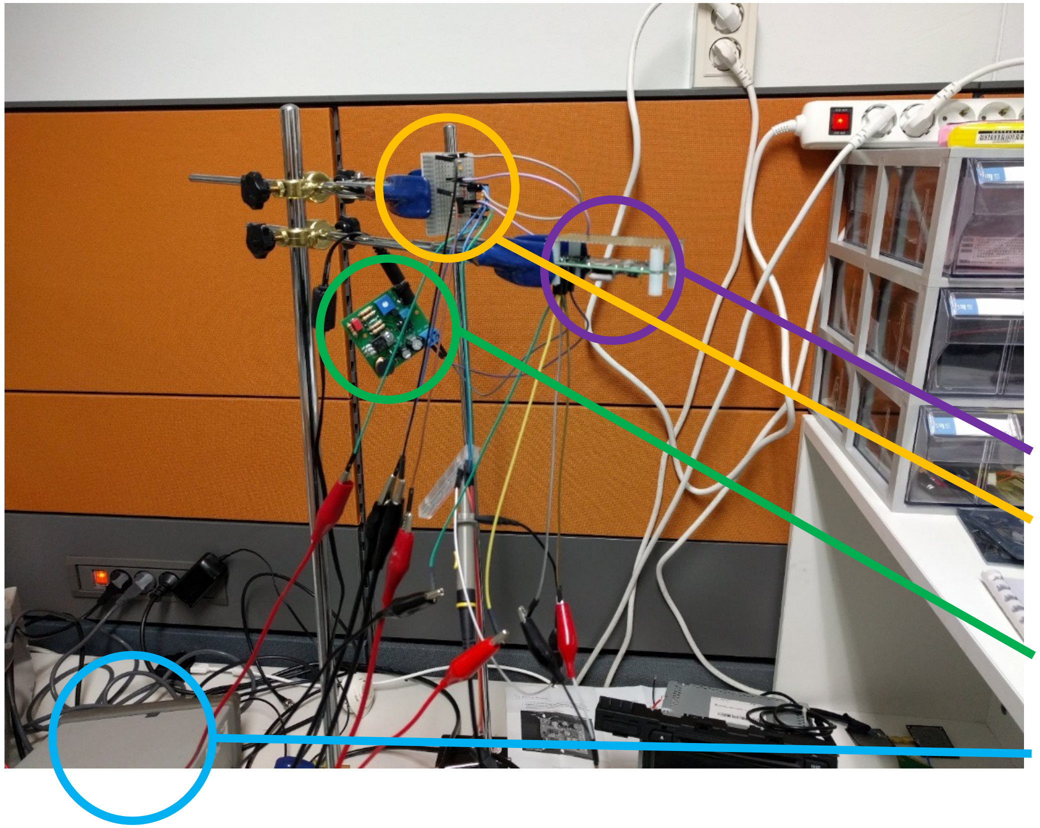
Sensor = A new attack vector



Velodyne VLP-16 [CHES'17]



Velodyne VLP-16 Experimental Setting

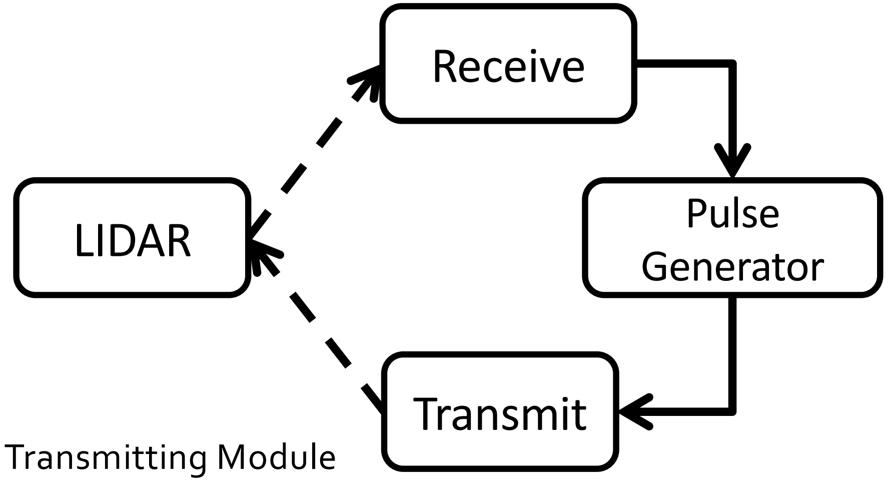


Transmitting Module

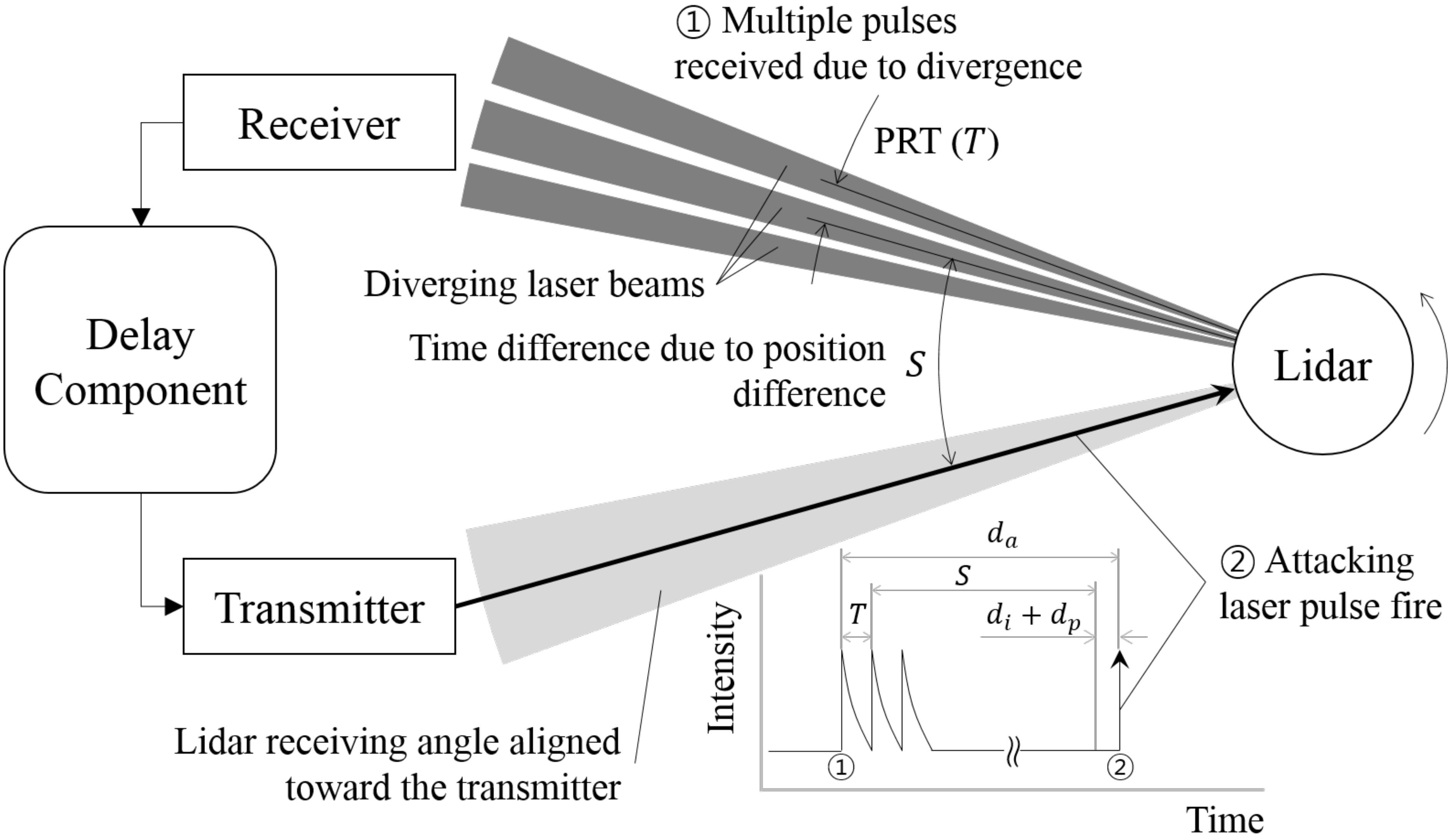
Receiving Module

DC Generator

Pulse Generator



Velodyne VLP-16: Fundamental Idea


① Multiple pulses received due to divergence
PRT (T)
Receiver
Delay Component
Diverging laser beams
Time difference due to position difference
S
Lidar
Transmitter
d_a
S
T
$d_i + d_p$
② Attacking laser pulse fire
Intensity
①
②
Time
Lidar receiving angle aligned toward the transmitter

VLP-16 Experiment

Lidar Exposure to Strong Light Source

Curved Surface

VLP-16 Experiment

Lidar Spoofing of Multiple Moving Fake Dots

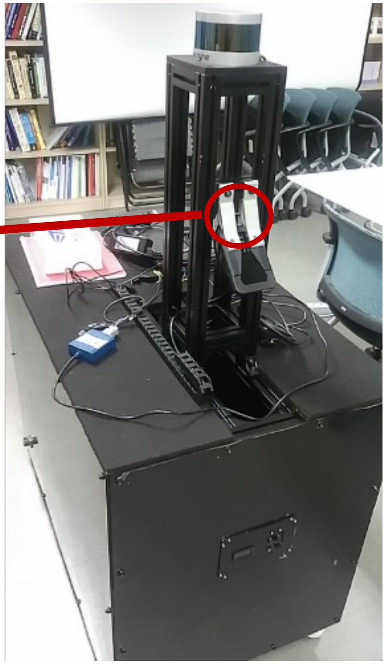
Mobileye

egoSpeed: 5.03 yawRate: 0.70 expDTime: 0.03 egoAccel: -0.26 Day gfi: 135
istance
FRANCE BOISSONS
green

- GM
- BMW
- Nissan
- Volvo
- (over 19 in total)

Mobileye-560 [Unpublished]

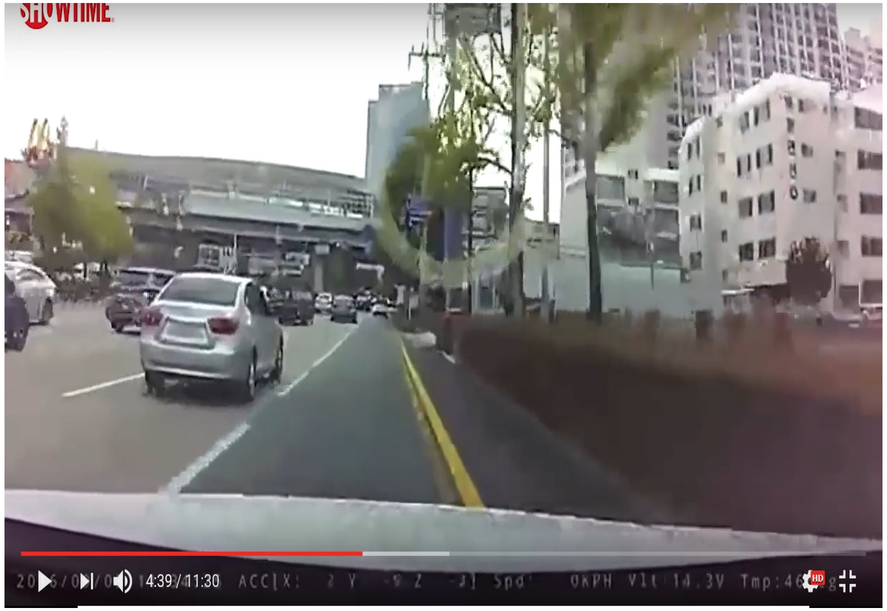
- Classify the objects
  - Vehicle, Pedestrian, Truck, Bike, Bicycle, Sign, Lane etc.
- Information about the Object
  - Distance, Velocity, State, etc.
- Recognition range : ~80m
- Black and White screen

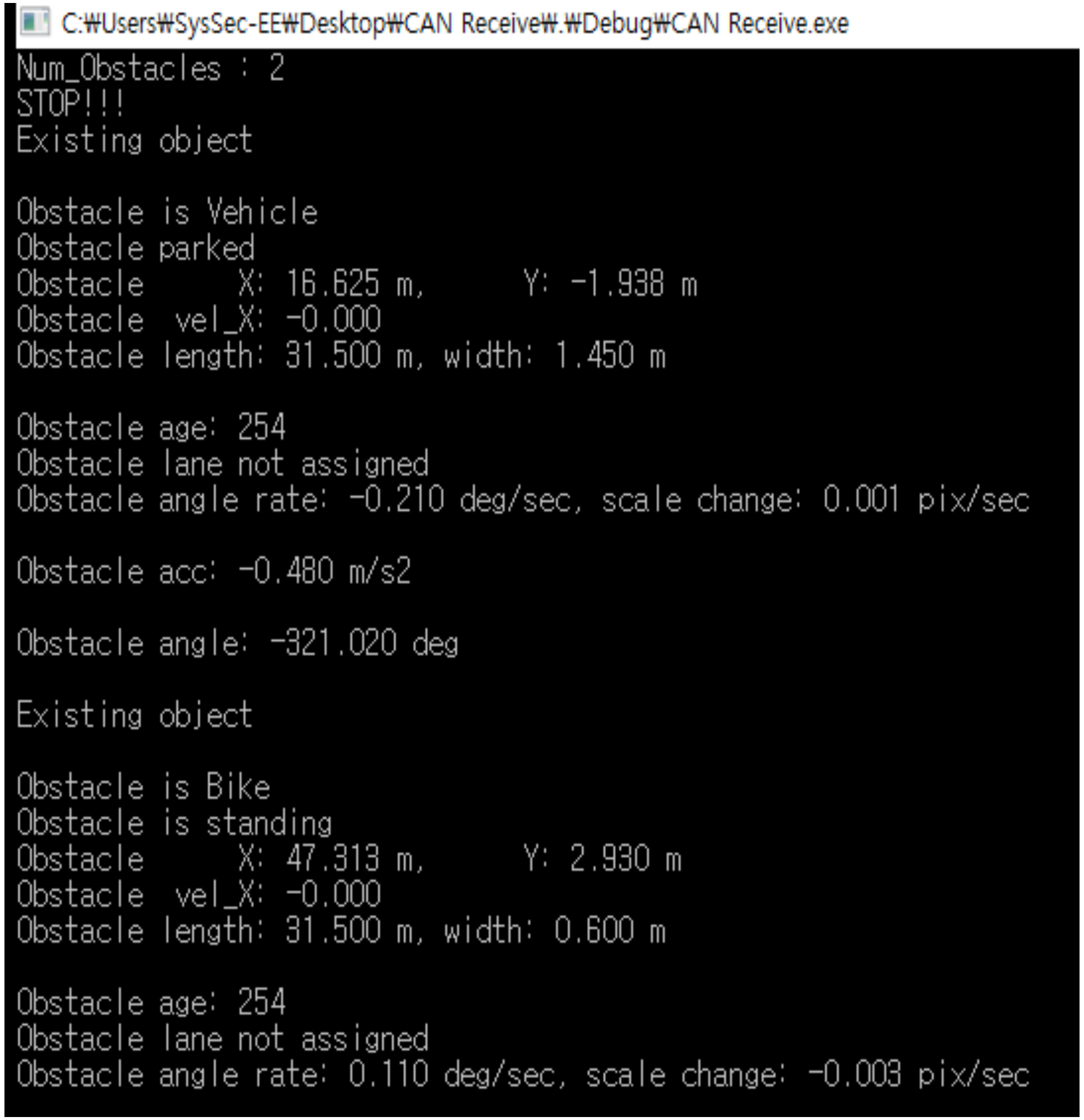


Parser

Parser prints the results for black box video.

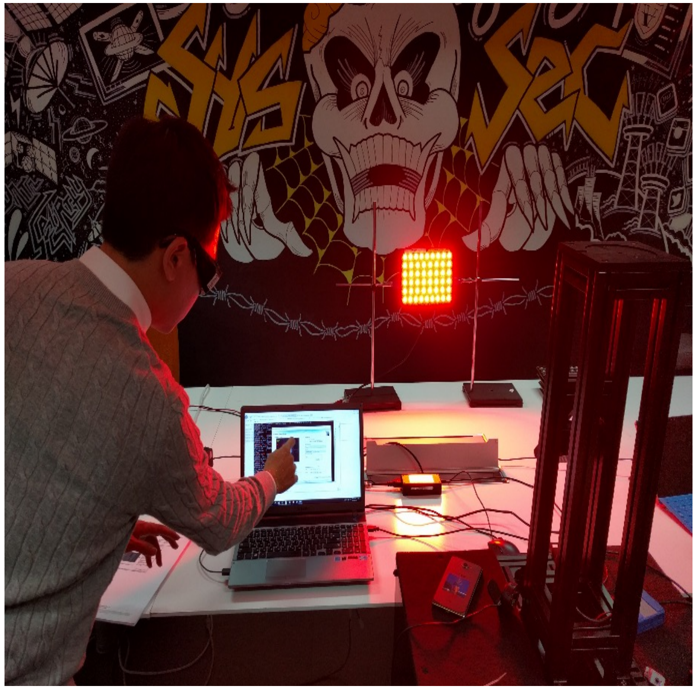
(Object classification, velocity, accelerometer …)



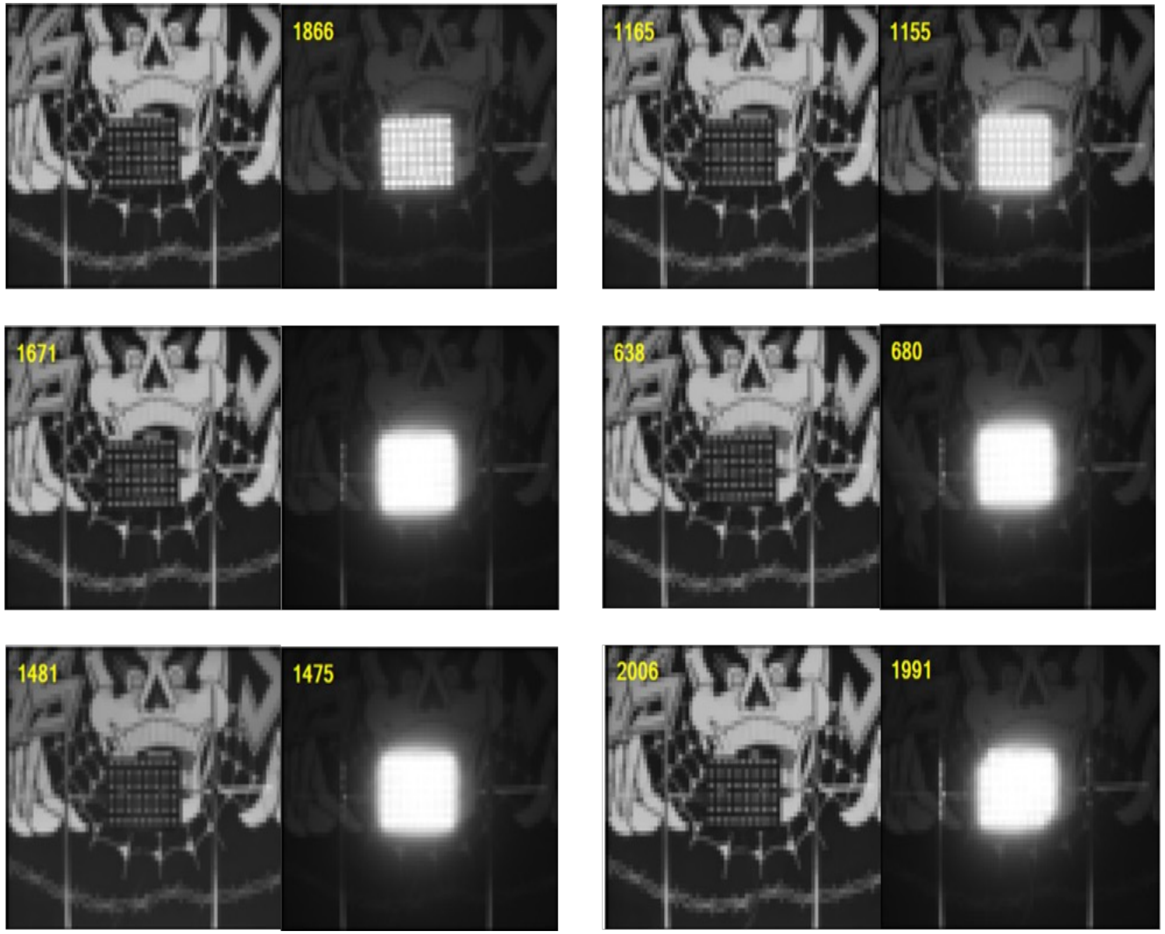

C:₩Users₩SysSec-EE₩Desktop₩CAN Receive₩.₩Debug₩CAN Receive.exe

```
Num_Obstacles : 2
STOP!!!
Existing object

Obstacle is Vehicle
Obstacle parked
Obstacle      X: 16.625 m,      Y: -1.938 m
Obstacle  vel_X: -0.000
Obstacle length: 31.500 m, width: 1.450 m

Obstacle age: 254
Obstacle lane not assigned
Obstacle angle rate: -0.210 deg/sec, scale change: 0.001 pix/sec

Obstacle acc: -0.480 m/s2

Obstacle angle: -321.020 deg

Existing object

Obstacle is Bike
Obstacle is standing
Obstacle      X: 47.313 m,      Y: 2.930 m
Obstacle  vel_X: -0.000
Obstacle length: 31.500 m, width: 0.600 m

Obstacle age: 254
Obstacle lane not assigned
Obstacle angle rate: 0.110 deg/sec, scale change: -0.003 pix/sec
```

Blinding Attack (Visible Light)

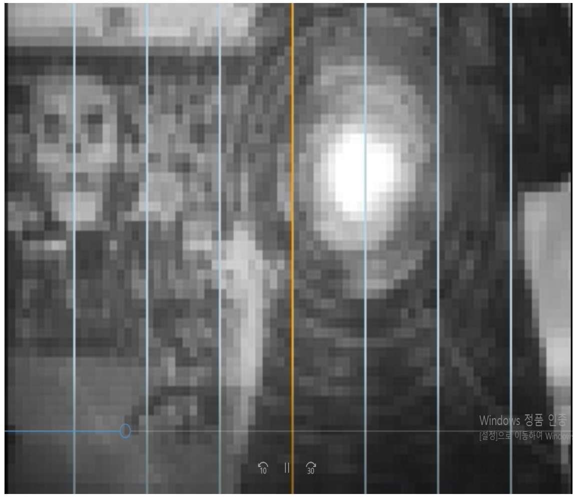


Experiment setup



980nm, 385nm, 460nm, 520nm, 585nm, 620nm

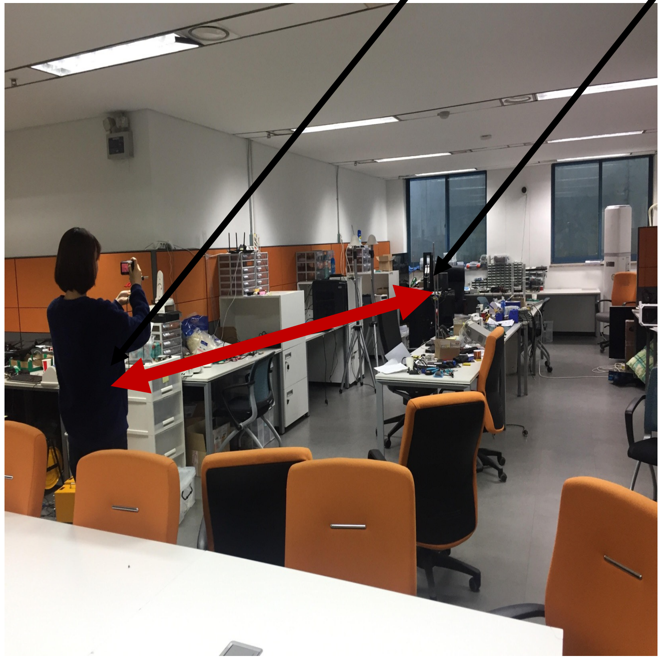
Invisible Light (IR)



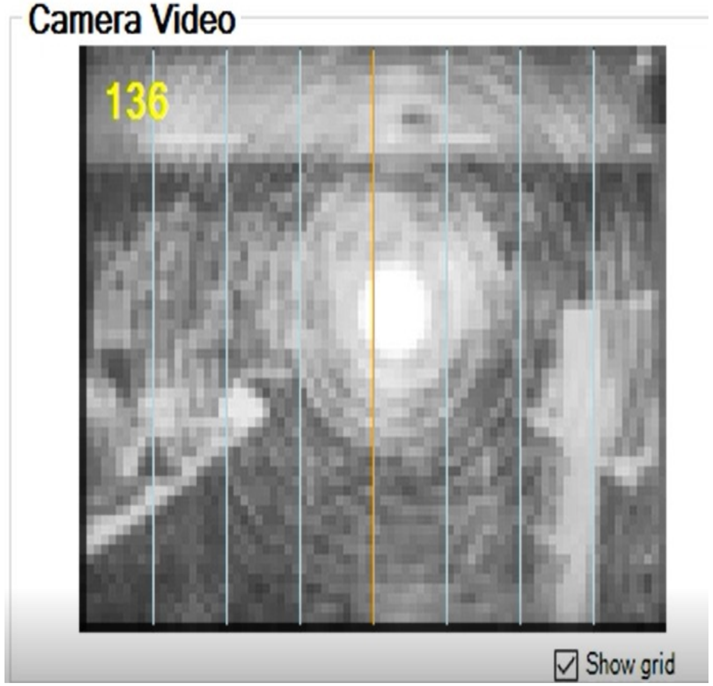
780nm 3mW Laser module: **Blinding!**

780nm 100mW Laser module

Camera

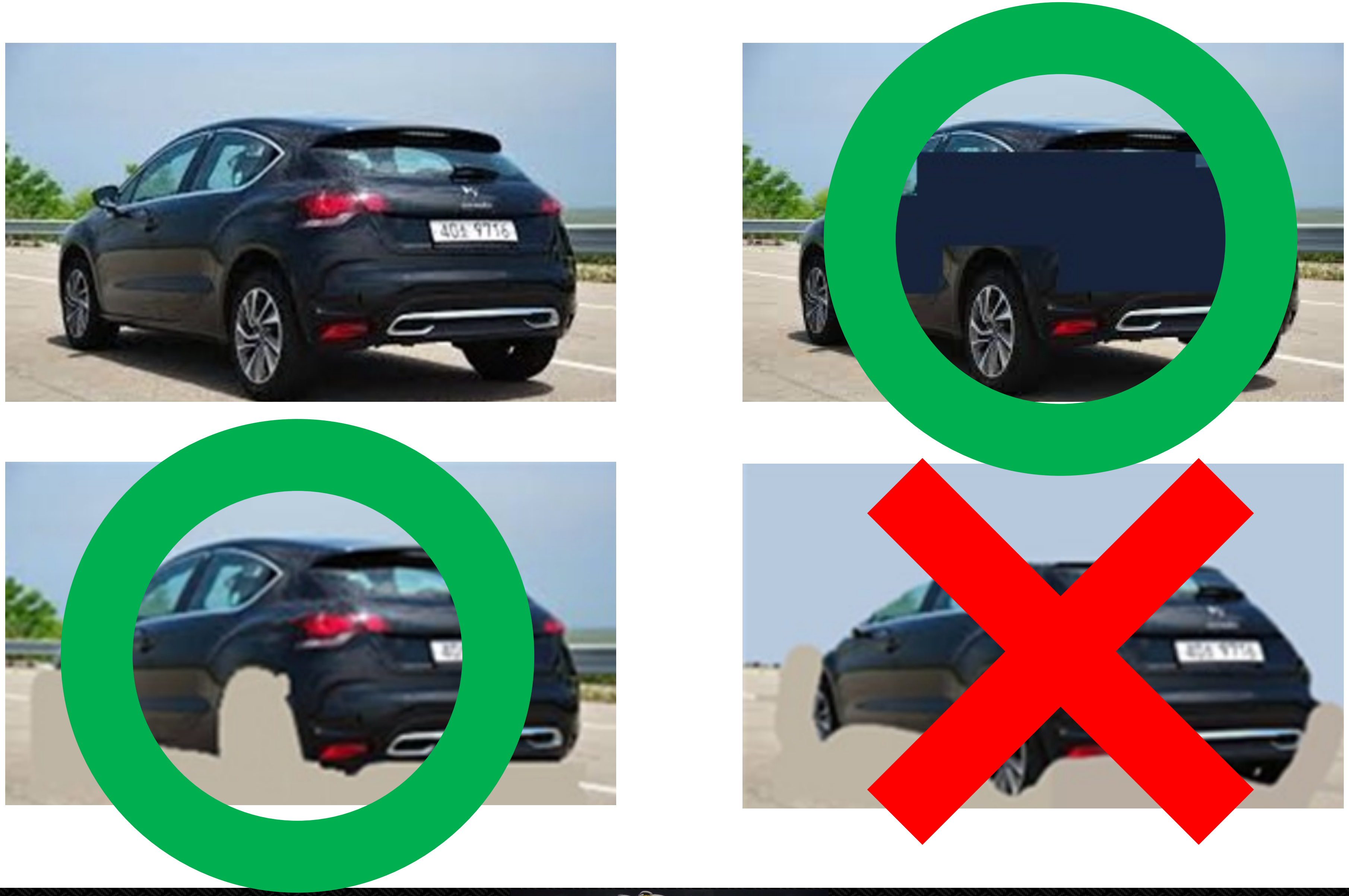


Blinding!



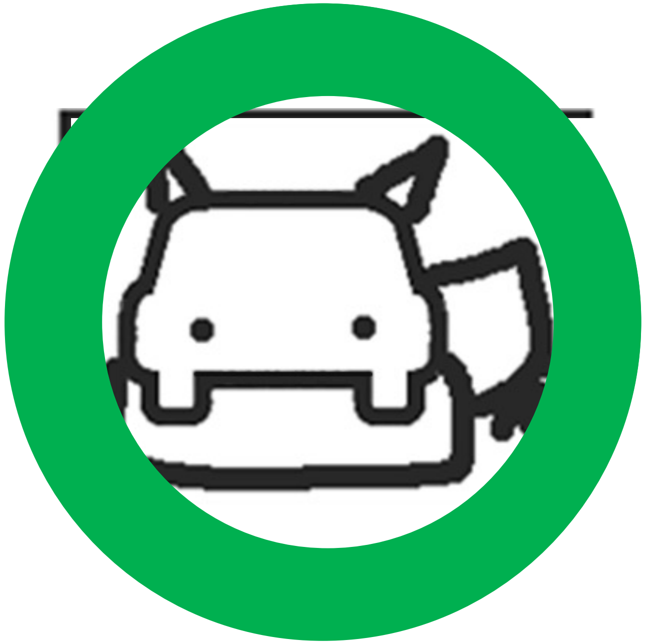
3. Camera module blinded by laser injection

Mobileye Classification

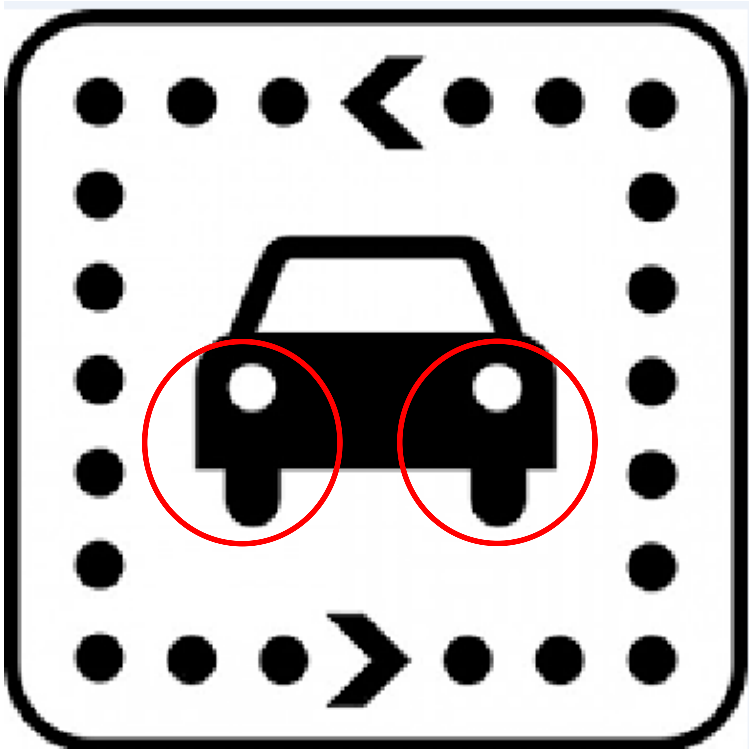


Are You Serious?

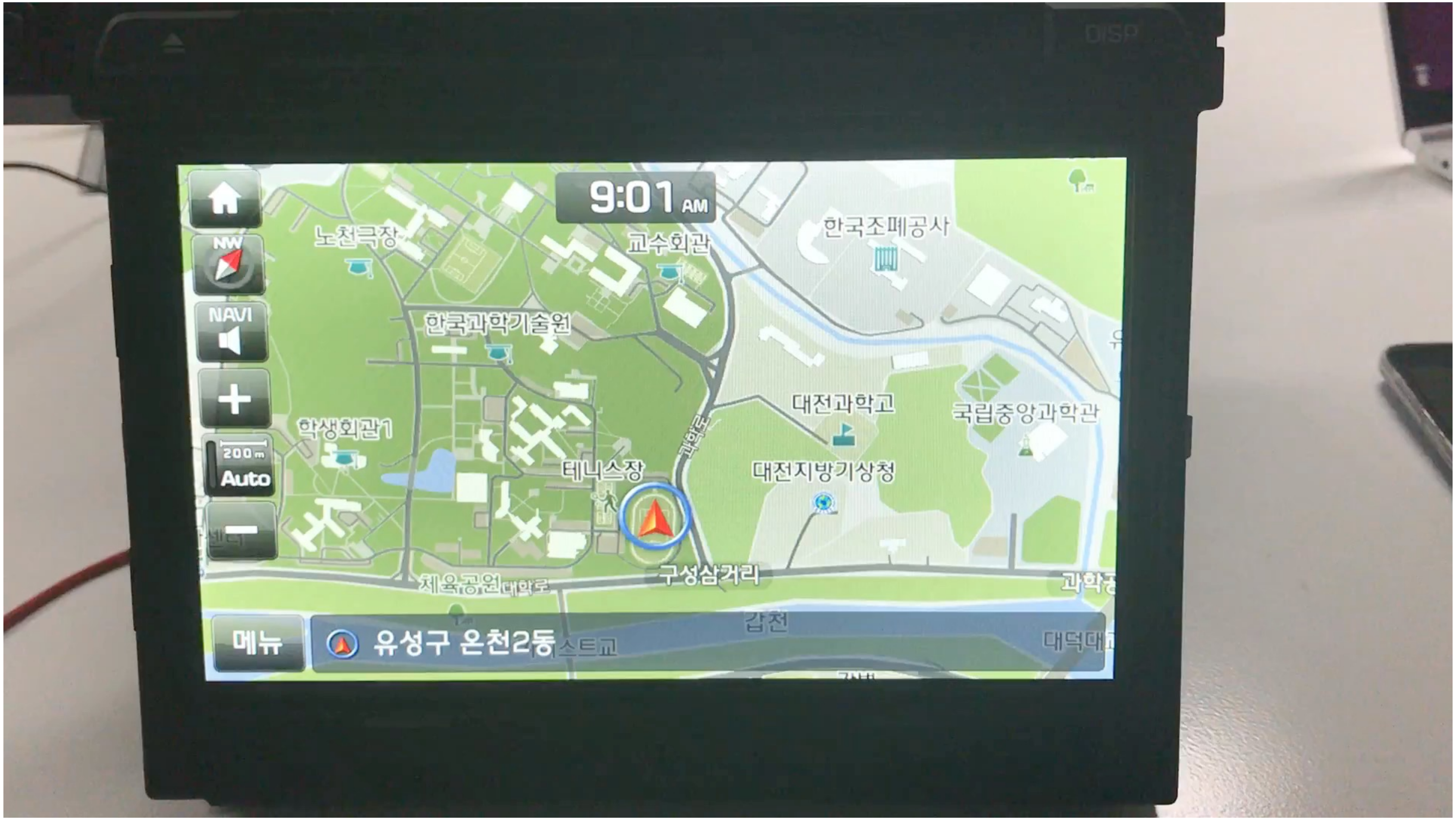
Variations



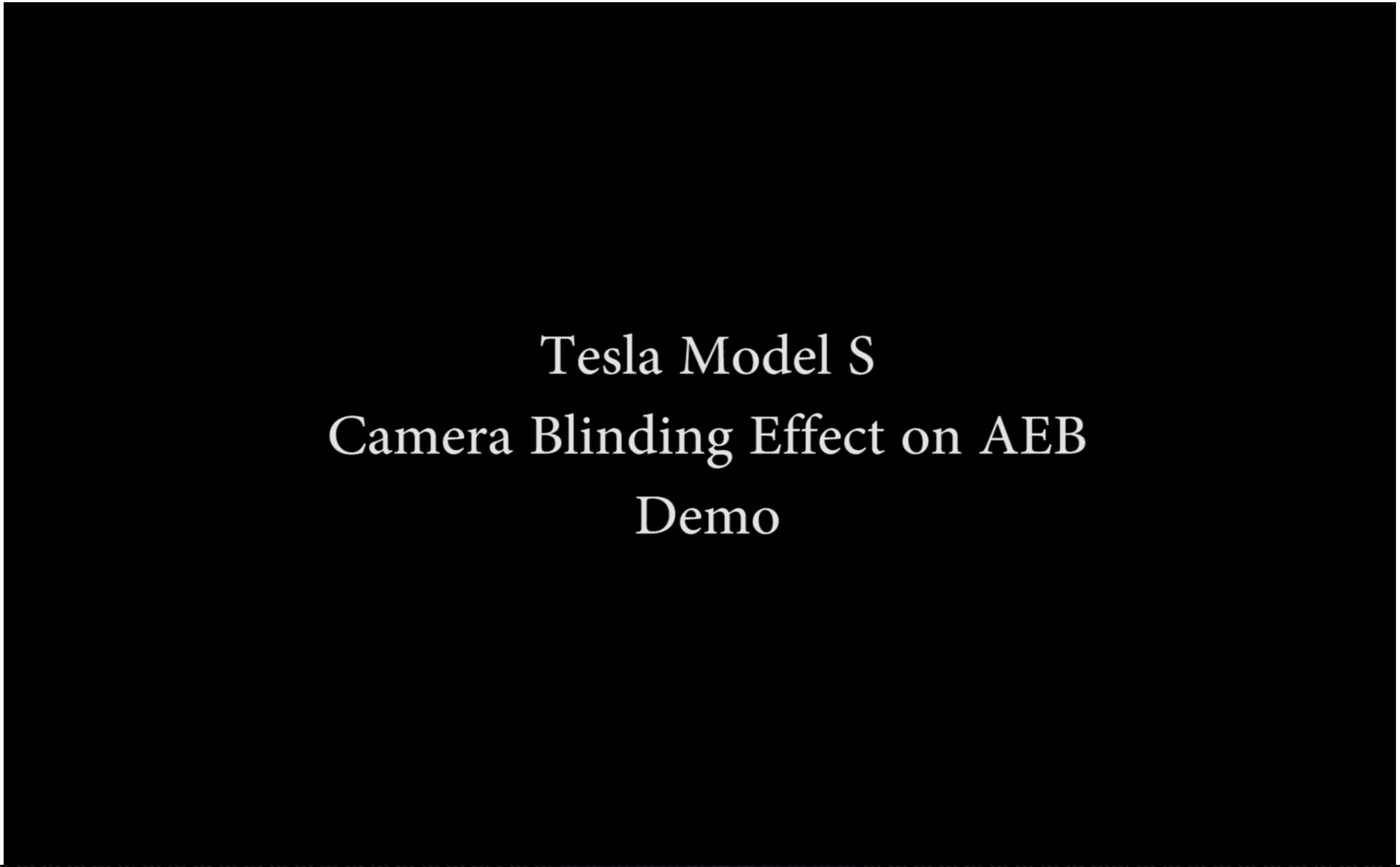
Men in the Car



GPS Spoofing



Blinding AEB



Tesla Model S

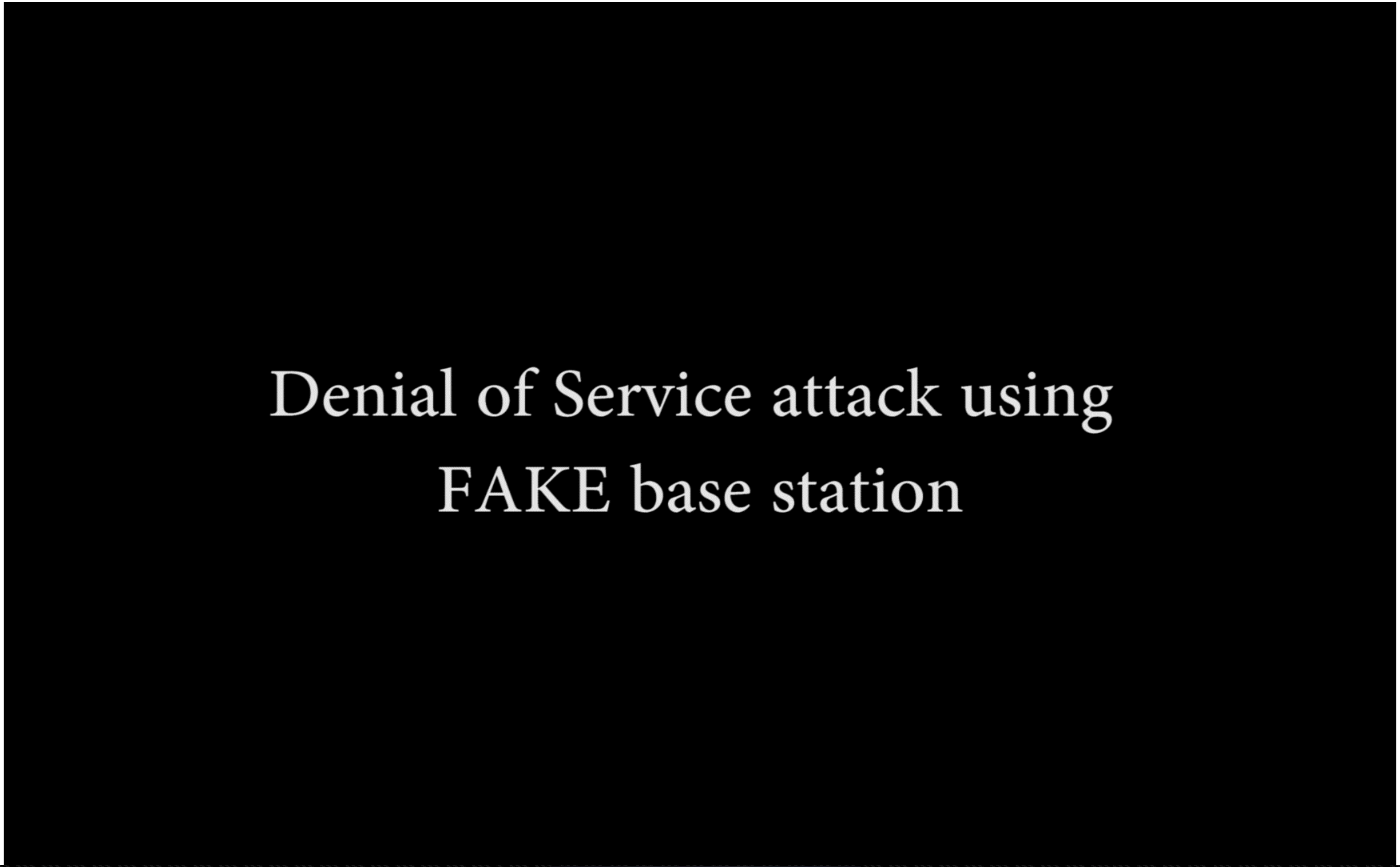
Camera Blinding Effect on AEB

Demo

GPS Spoofing and Auto-pilot

GPS Spoofing Effect on Tesla Autopilot Cruise Speed

DoS Using Fake Base Station



Denial of Service attack using
FAKE base station

Conclusion

- Sensing is one of the most important components of IoT
  - Driverless cars, Drones, Medical devices, SCADA systems, …
- For self-driving car, sensors are one of the most important components.
- But, the current sensors look insecure.
- Now it is time to look at security of sensors.

Questions?

- Yongdae Kim
  - email: yongdaek@kaist.ac.kr
  - Home: http://syssec.kaist.ac.kr/~yongdaek
  - Facebook: https://www.facebook.com/y0ngdaek
  - Twitter: https://twitter.com/yongdaek
  - Google “Yongdae Kim”