Can You Trust Autonomous Vehicles: Contactless Attacks against Sensors of Self-Driving Vehicles

Jianhao Liu Qihoo360 SKY-GO Team

Chen Yan USSLab, Zhejiang University

Wenyuan Xu Zhejiang University & University of South Carolina

360 WWW.360.COM

SKY-GO 360 VEHICLE CYBER SECURITY

浙江大學 ZHEJIANG UNIVERSITY

智能系统安全实验室 UBIQUITOUS SYSTEM SECURITY LAB.

Who Are We

Jianhao Liu

Director

Qihoo 360

SKY-GO Vehicle Cyber Security Team

Wenyuan Xu

Professor

Zhejiang University

University of South Carolina

Chen Yan

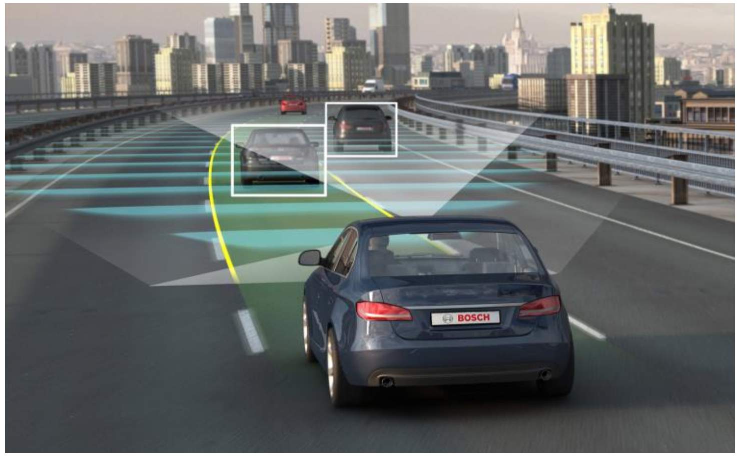
Ph.D. Student

USSLab

Zhejiang University

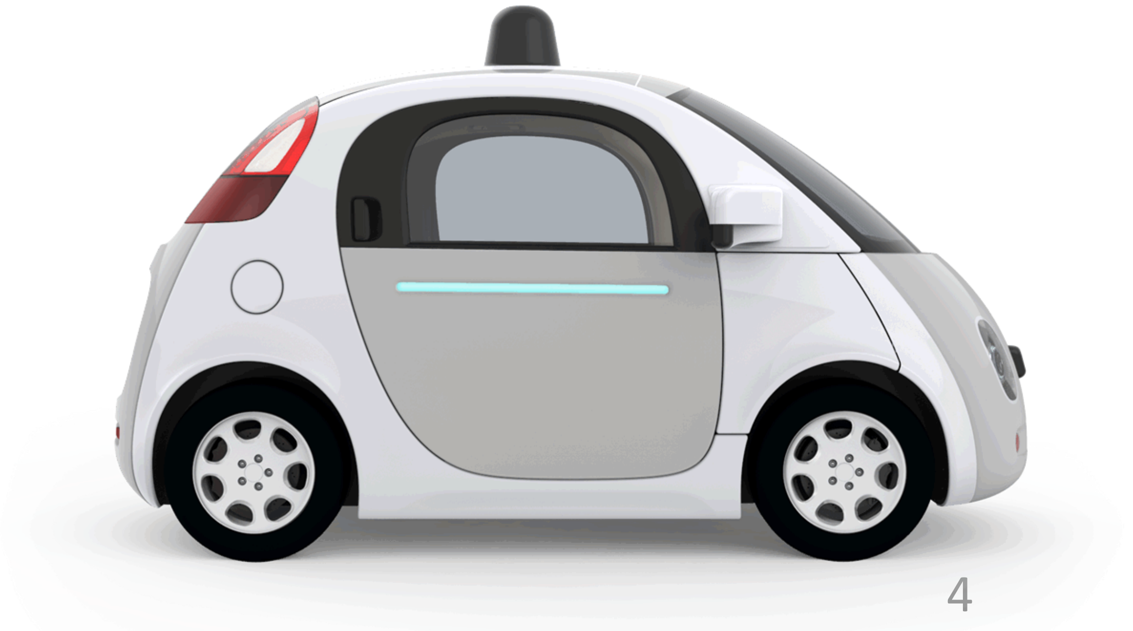
Roadmap

- **Autonomous Vehicles**
- **Hacking Sensors**
- **Our Attacks**
  - Ultrasonic sensors
  - MMW radars
  - Cameras
- **Discussion**

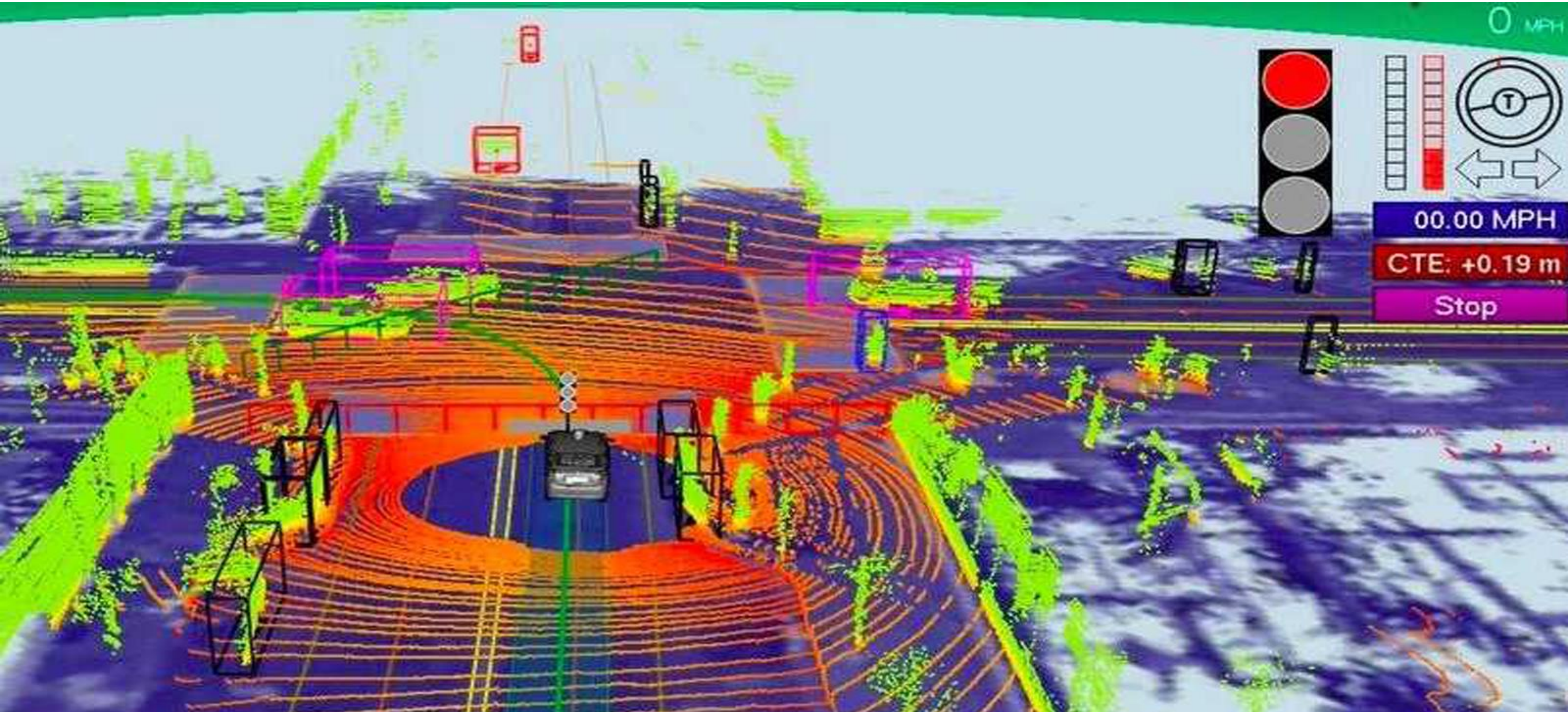


The Car Hacking History

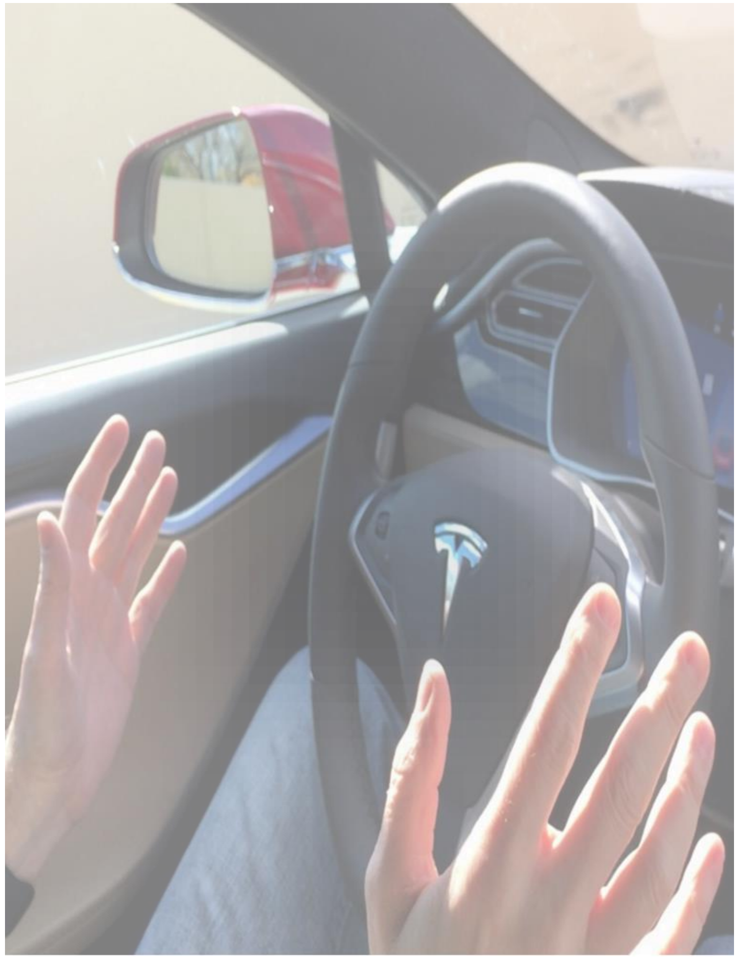
- Car ===> CAN bus hacking
- Connected car ===> Telematics hacking
- Autonomous car ===> Automatic system hacking



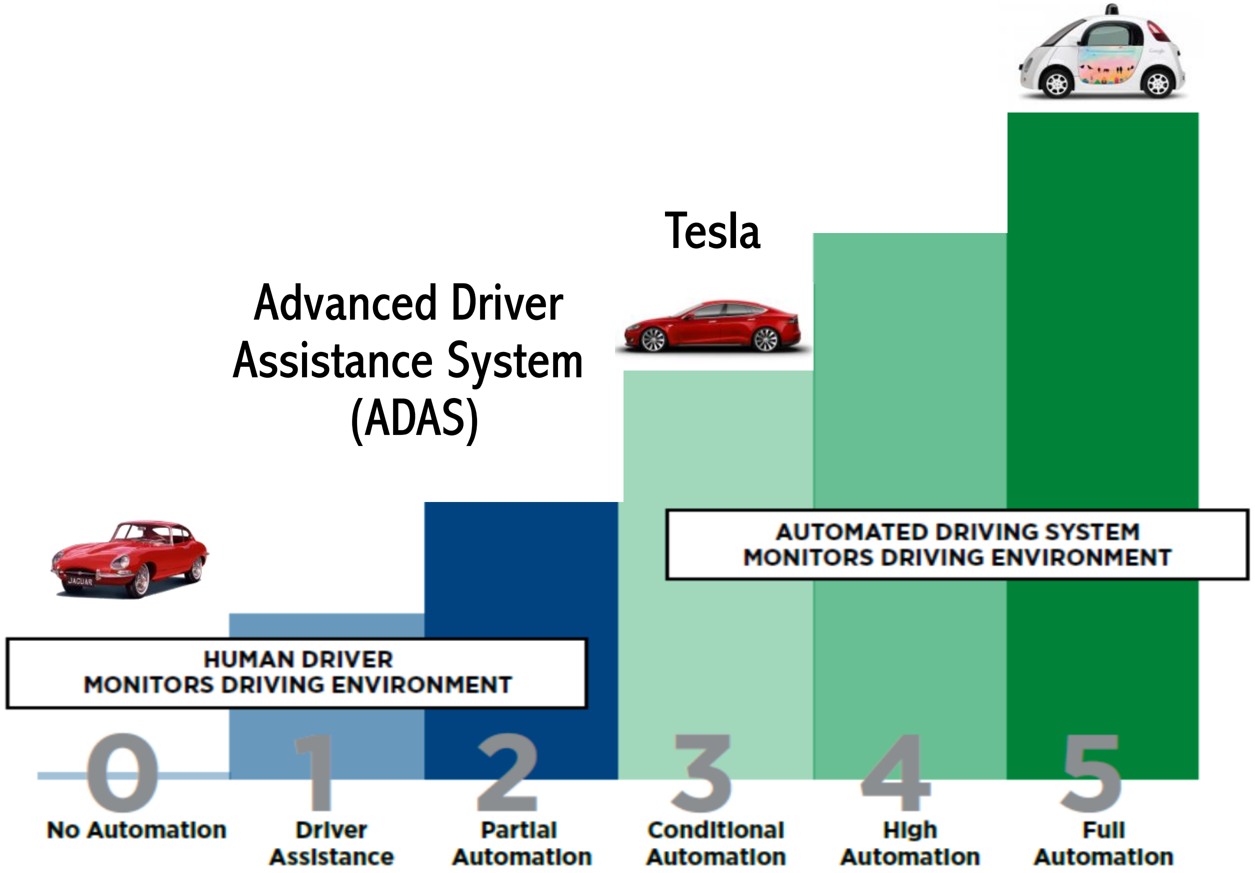
What is Autonomous Vehicle?



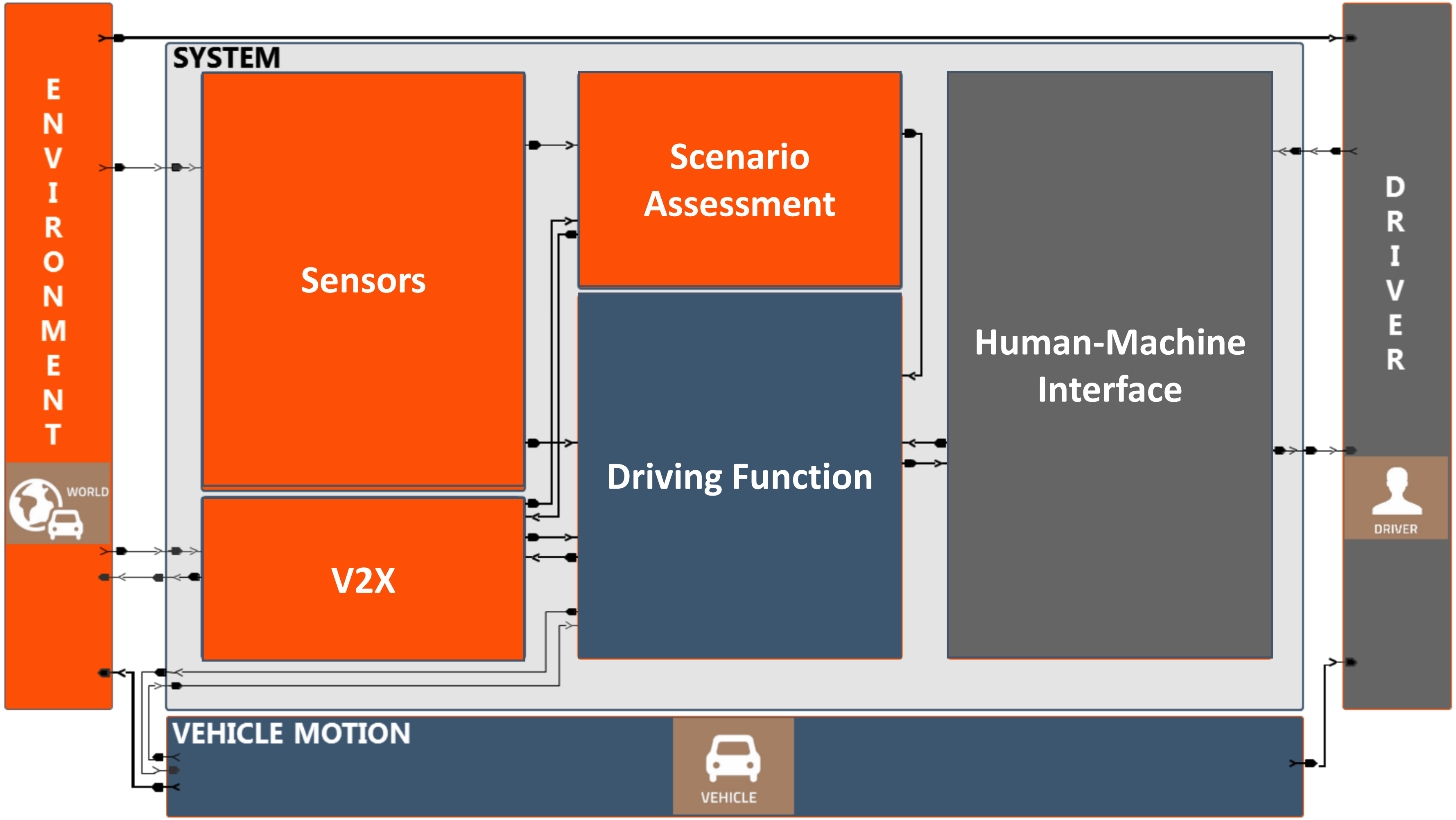
Levels of Driving Automation



SAE J3016

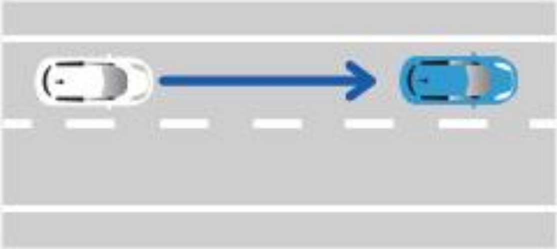


Sensors in automated driving system

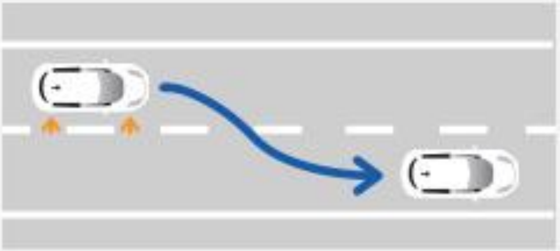


Source:Michael Aeberhard, BMW Group Research and Technology

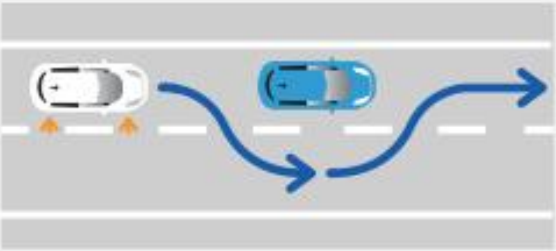
Automatic Driving Applications



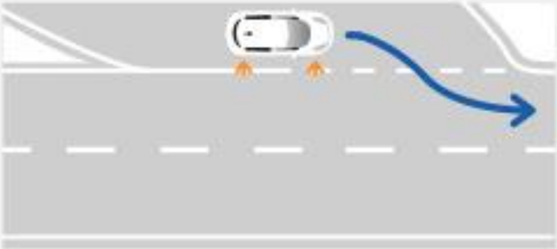
Autonomous Lane Keeping
Autonomous Distance Control



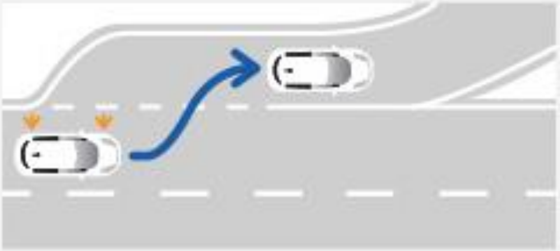
Autonomous Lane Change



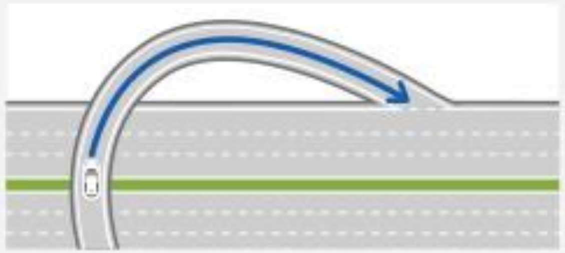
Autonomous Overtaking



Autonomous Highway Merge



Autonomous Highway Exit



Autonomous Interchange

Sensors for Self-Driving

Cameras

Senses reflected light, limited when dark. Sees colour, so can be used to read signs, signals, etc.

LiDAR

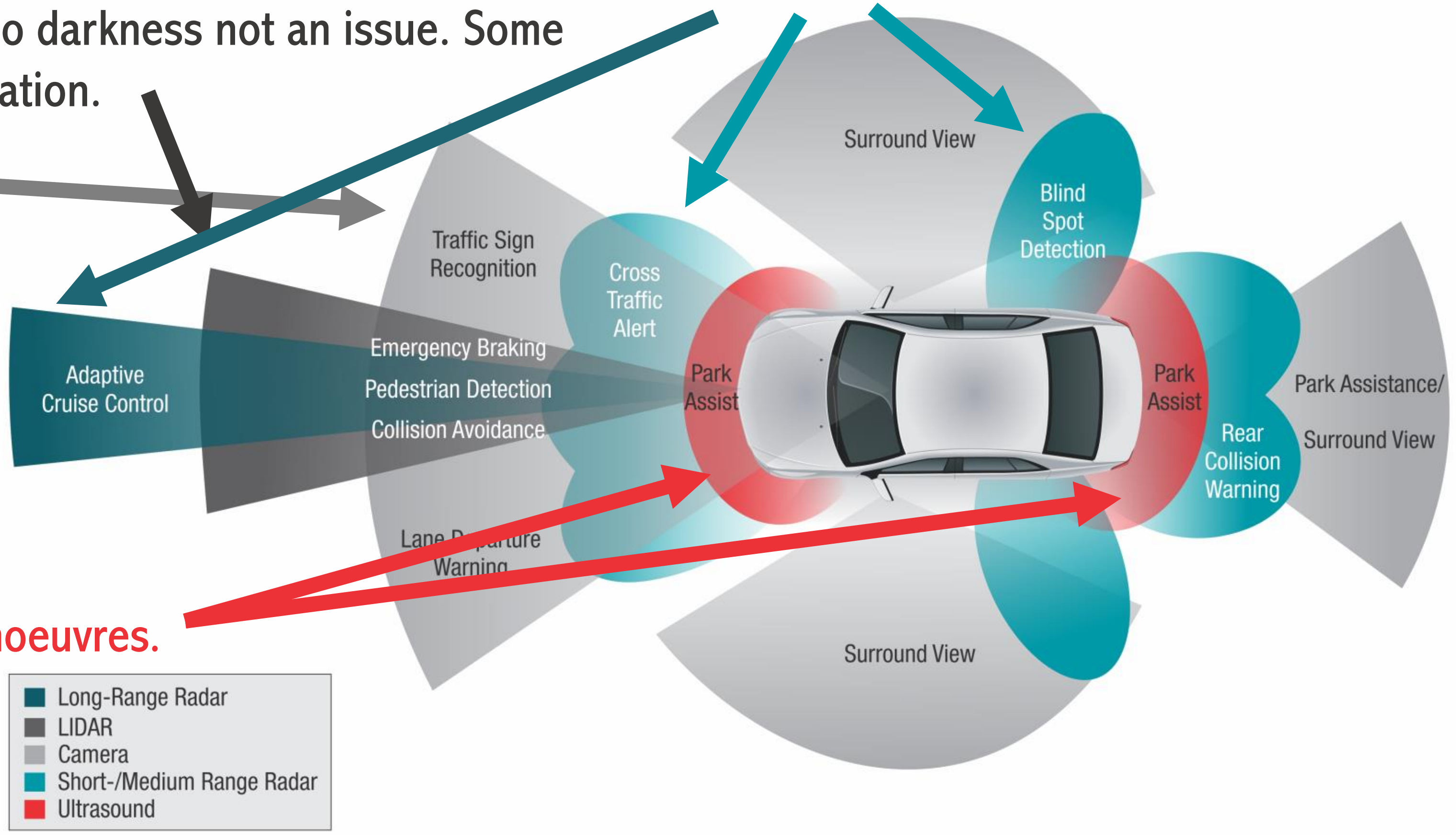
Emits light, so darkness not an issue. Some weather limitation.

Radar

Works in low light & poor weather, but lower resolution.

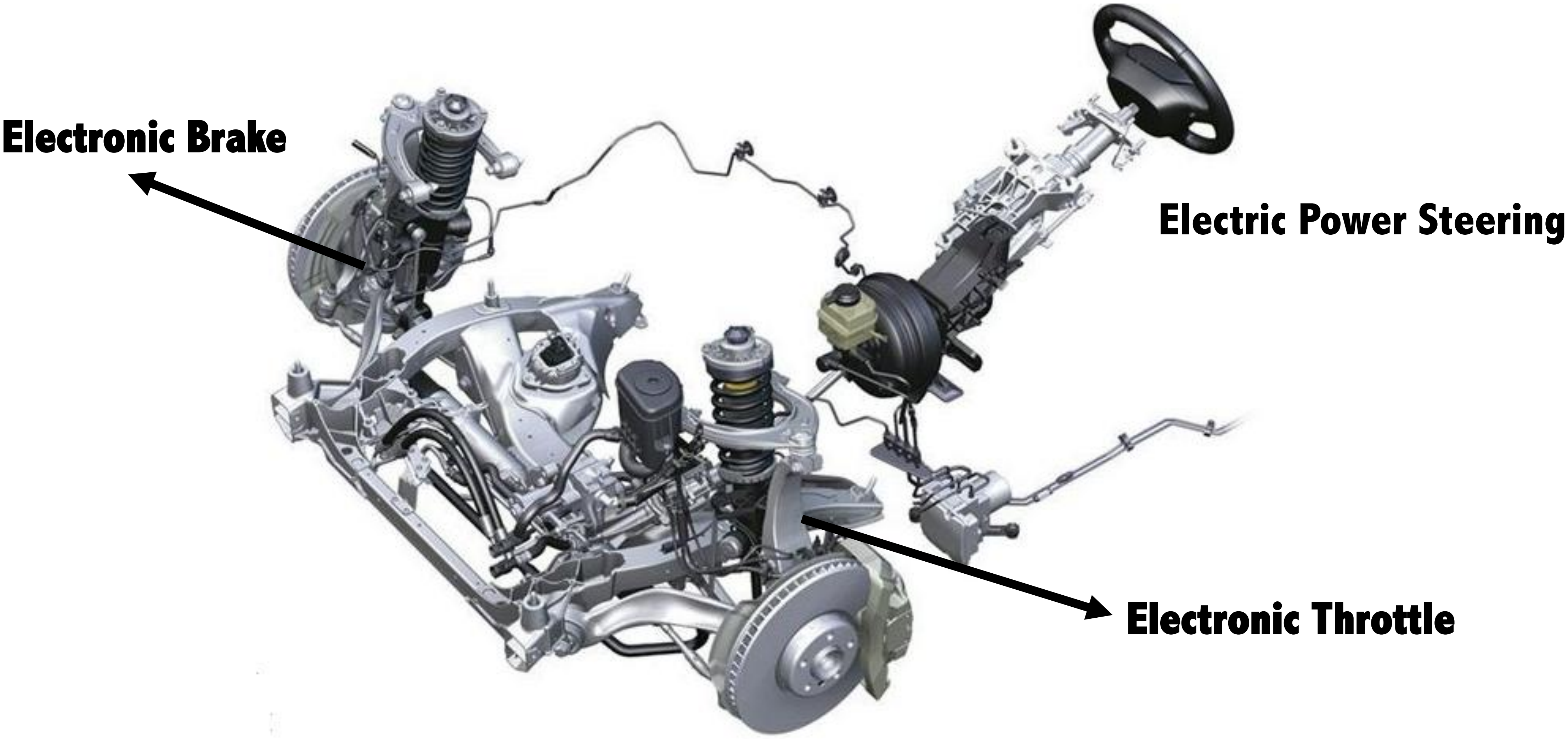
Ultrasonic Sensors

Limited to proximity, low speed manoeuvres.



Source: Texas Instruments

Vehicle Controllers



Electronic Brake

Electric Power Steering

Electronic Throttle

How to Hack Sensors?

Sensors

Ultrasonic Sensors

Jamming

Spoofing

MMW Radars

Jamming

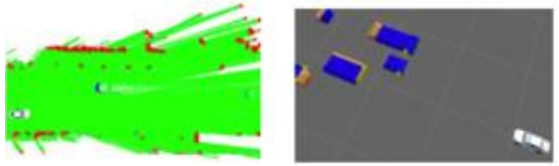
Spoofing

Cameras

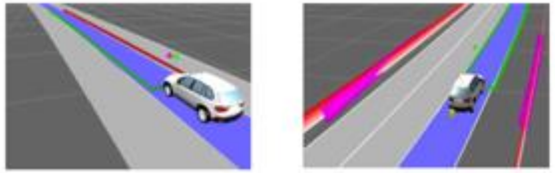
Blinding

Automated System

Representations and Fusion



Road Model and Localization



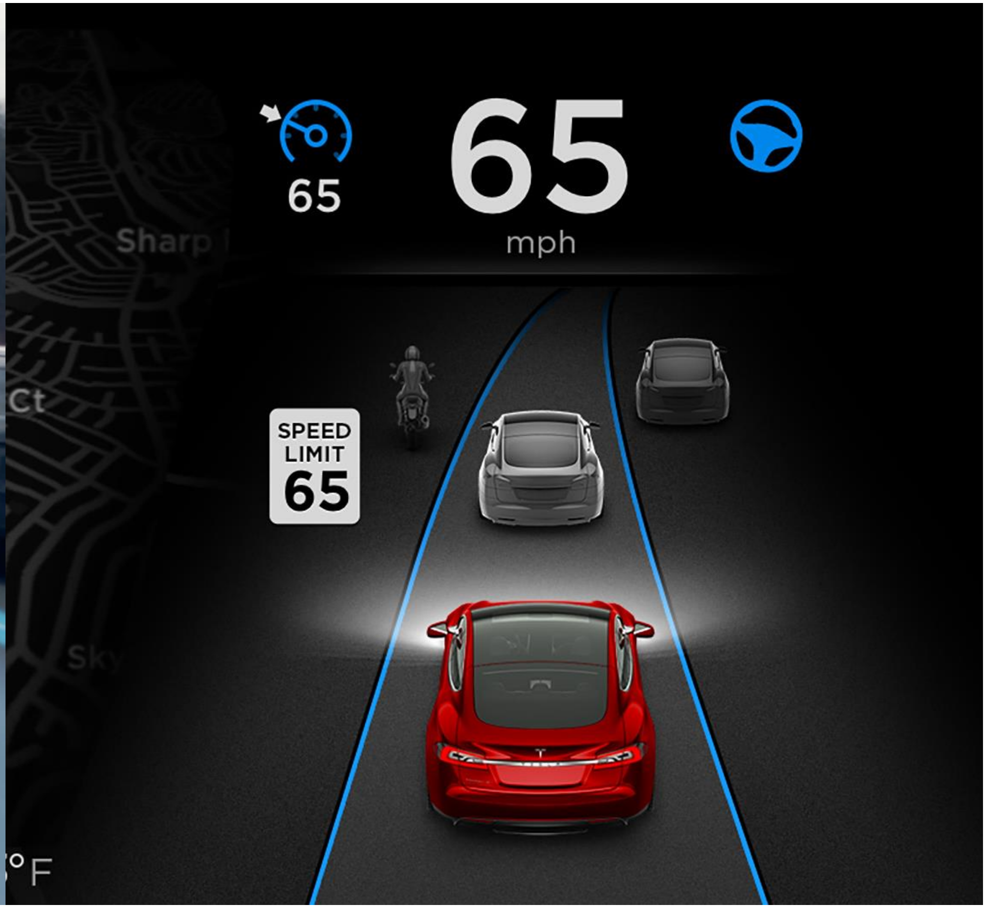
Situation Interpretation

Control

HMI Display

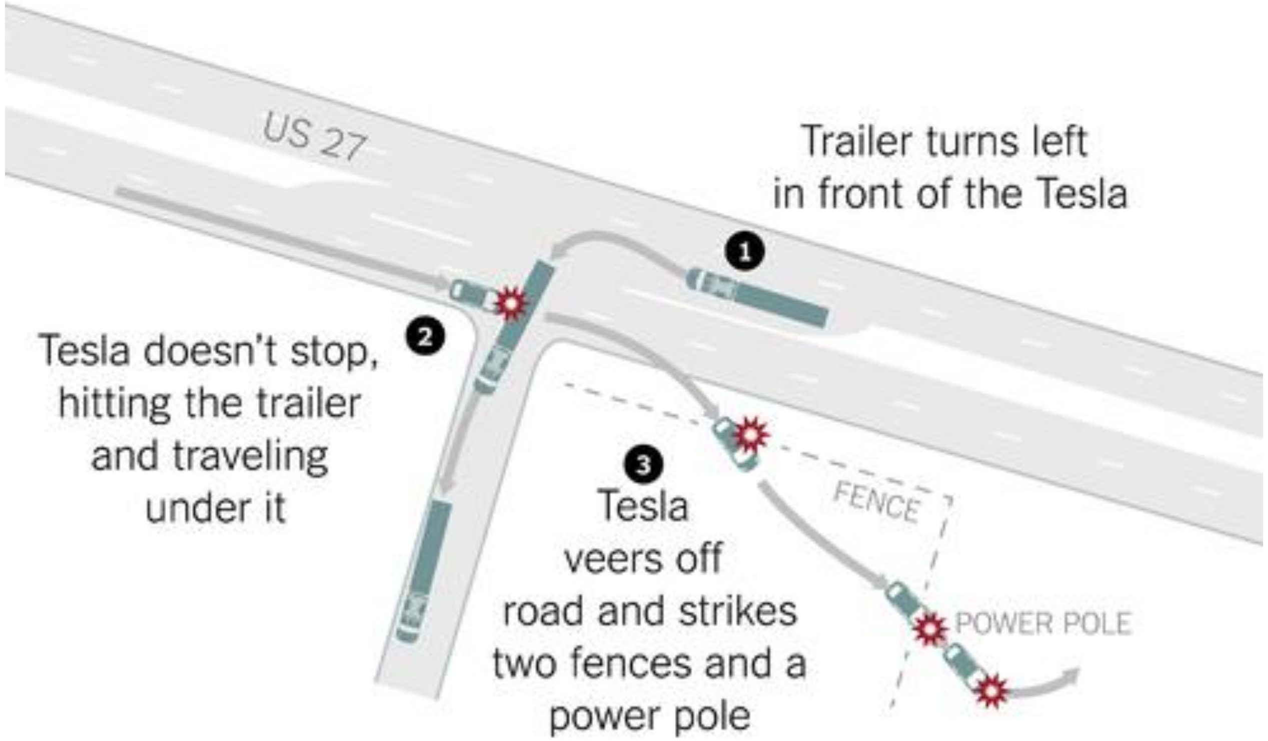
Tesla Autopilot

Autosteer
Autopark
Summon
Auto Lane Change
Traffic-Aware Cruise Control



Tesla: A Tragic Loss

- **First fatal crash while using Autopilot on May 7, 2016.**
- **Reliability of sensors.**

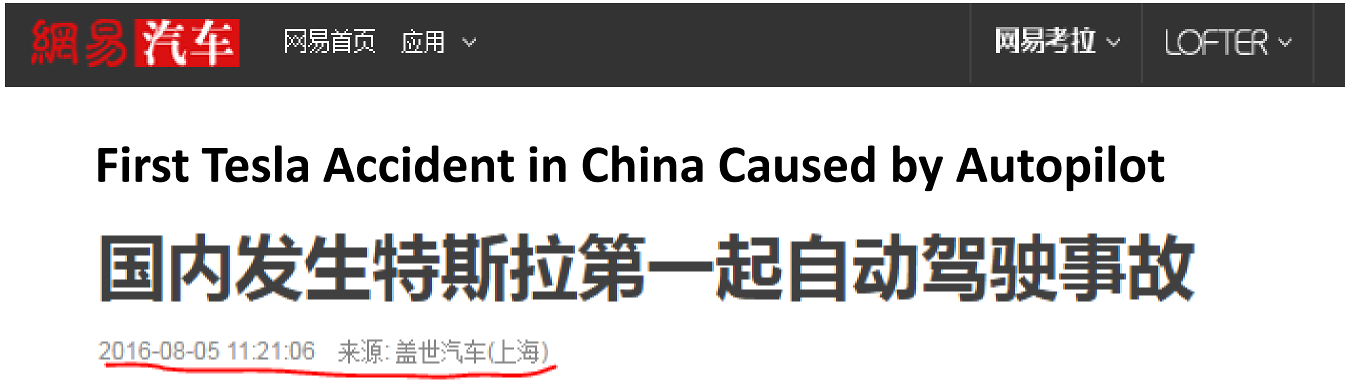


1 Trailer turns left in front of the Tesla

2 Tesla doesn't stop, hitting the trailer and traveling under it

3 Tesla veers off road and strikes two fences and a power pole

Source: The New York Times



First Tesla Accident in China Caused by Autopilot

国内发生特斯拉第一起自动驾驶事故

2016-08-05 11:21:06 来源: 盖世汽车(上海)

Existing Sensors on Tesla Model S

One MMW Radar

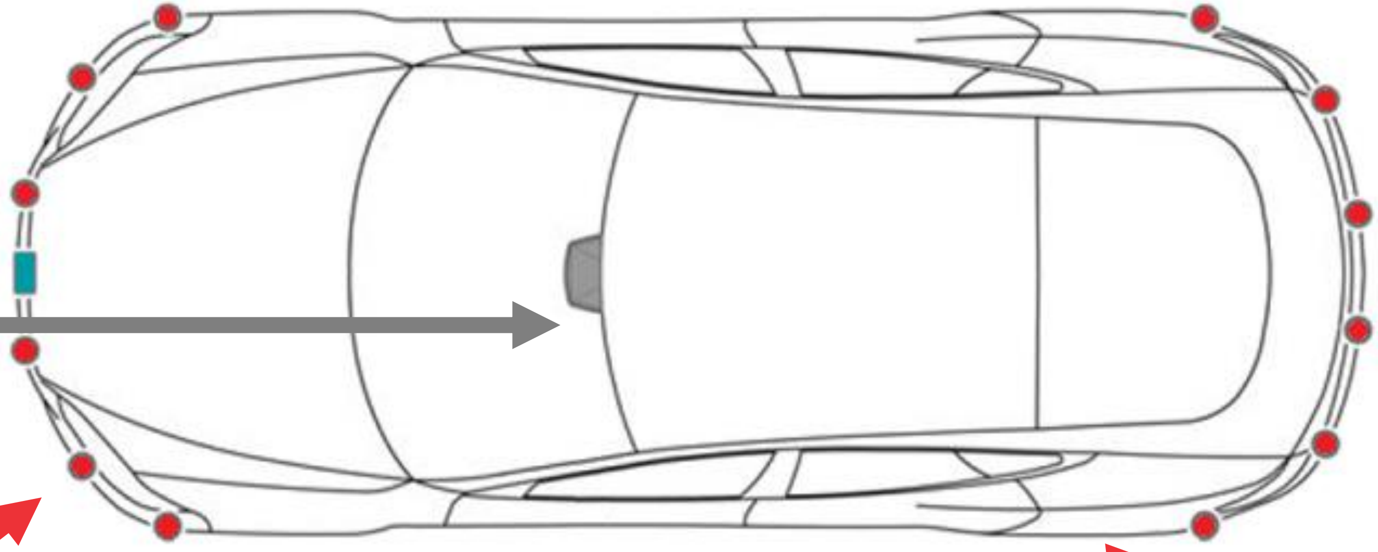
A Medium range Radar is mounted in the front grill.

One camera

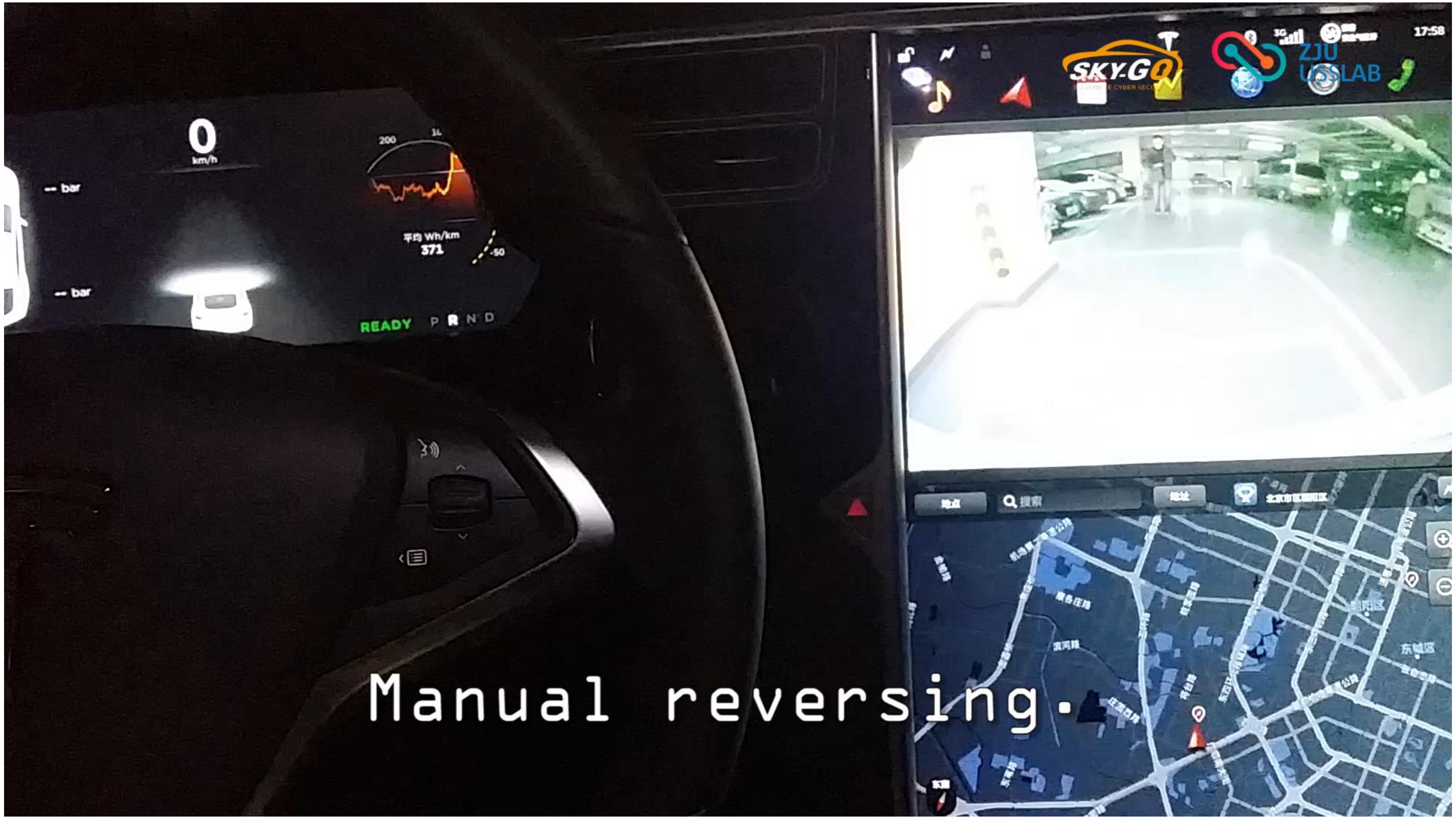
A forward looking camera is mounted on the windshield under the rear view mirror.

12 ultrasonic sensors

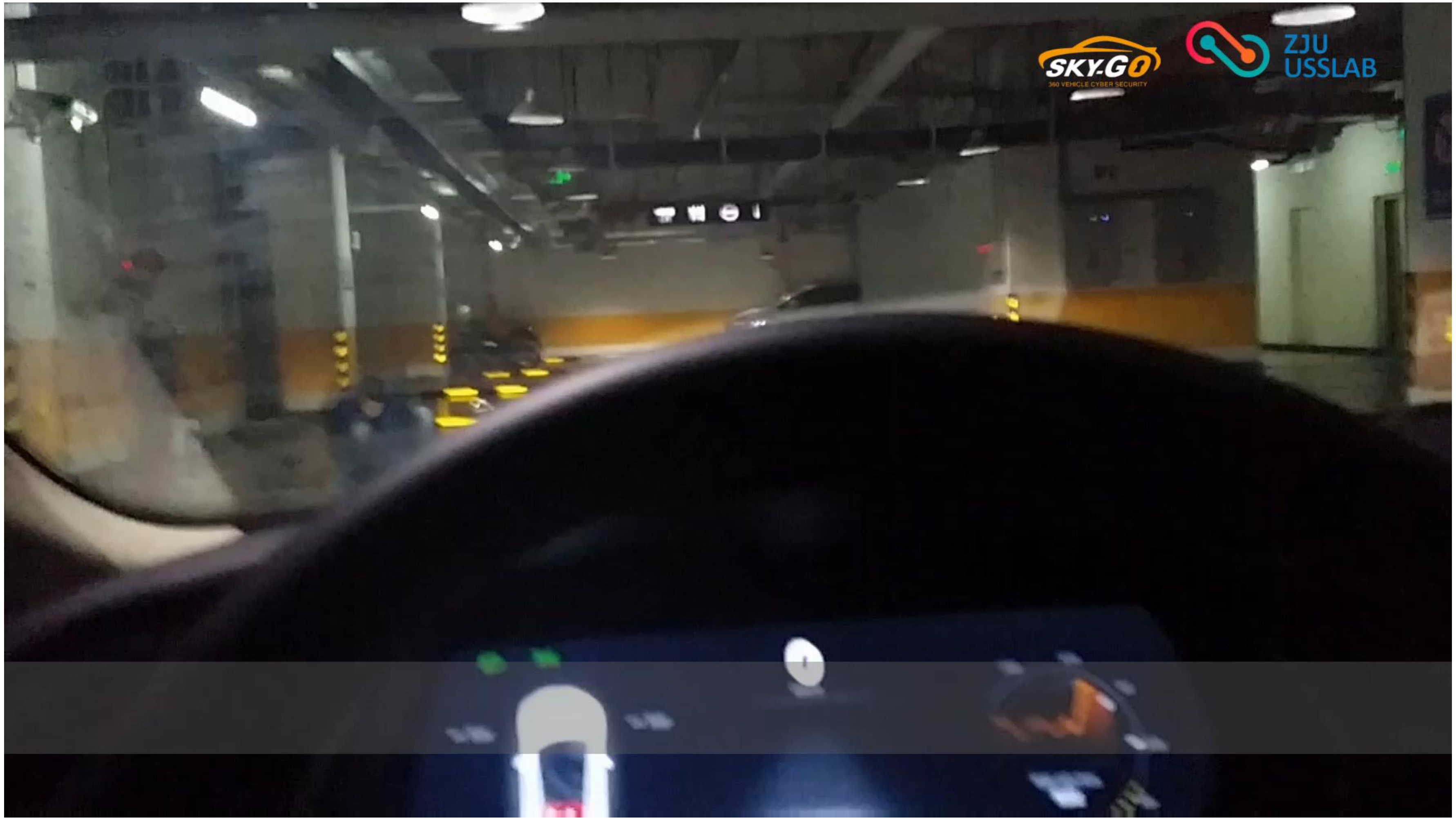
Ultrasonic sensors are located near the front and rear bumpers.



HMI Display Mistakes – Demo on Tesla



Control Mistakes – Demo on Tesla



Attacking Ultrasonic Sensors

On Tesla, Audi, Volkswagen, and Ford

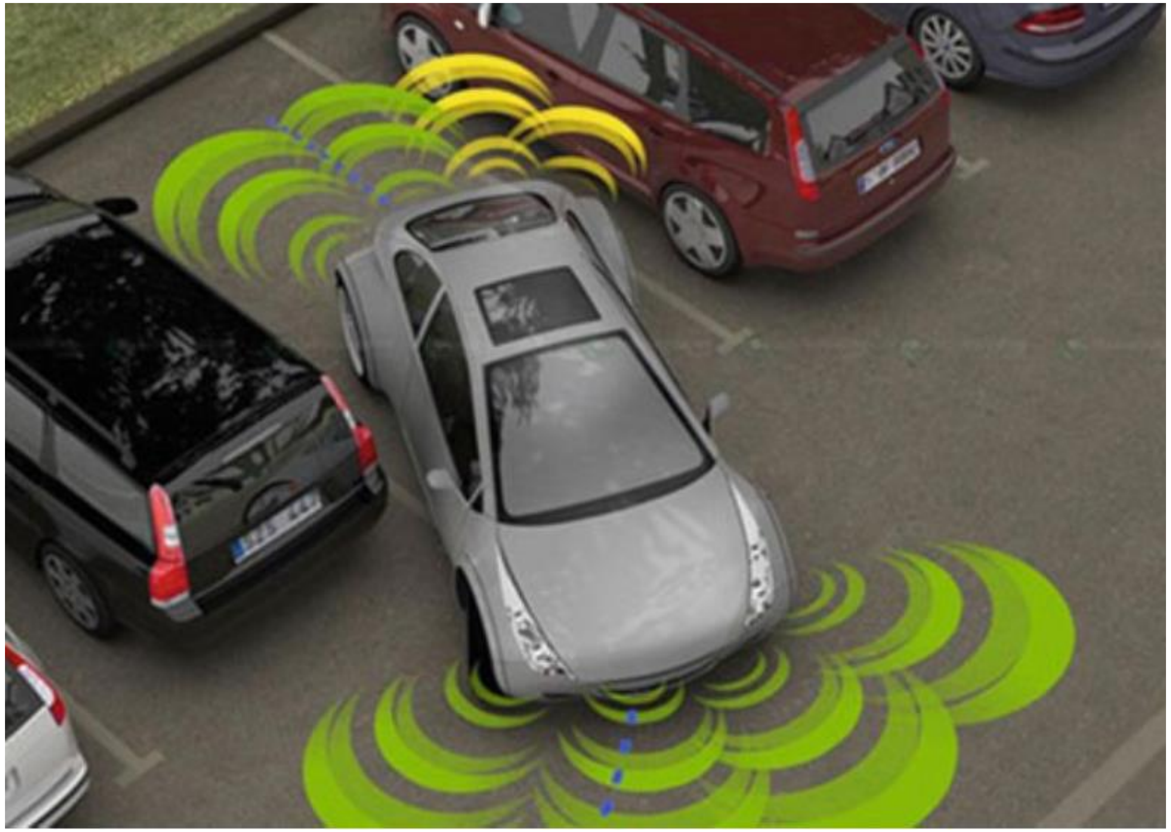
Ultrasonic Sensor

What is ultrasonic sensor?

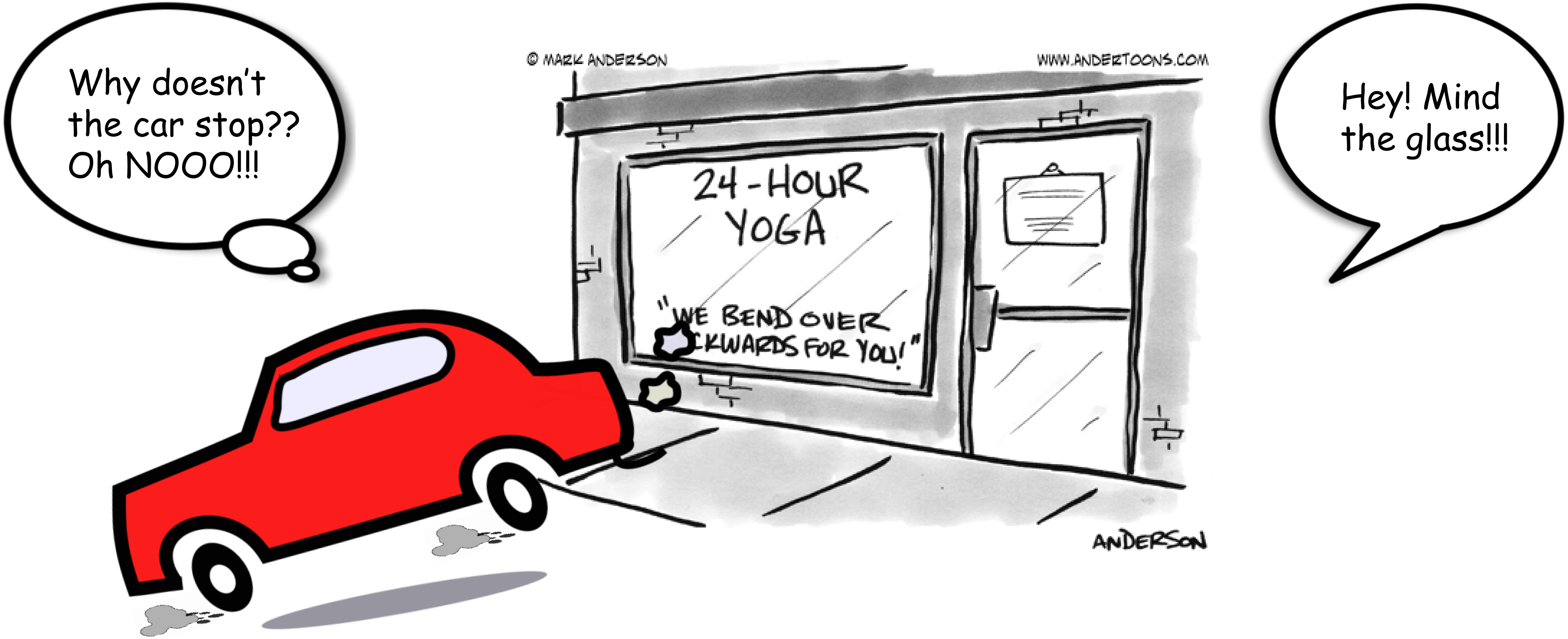
- **Measures distance**
- **Proximity sensor (< 2m)**

- **Applications**
  - Parking assistance
  - Parking space detection
  - Self parking
  - Tesla's summon

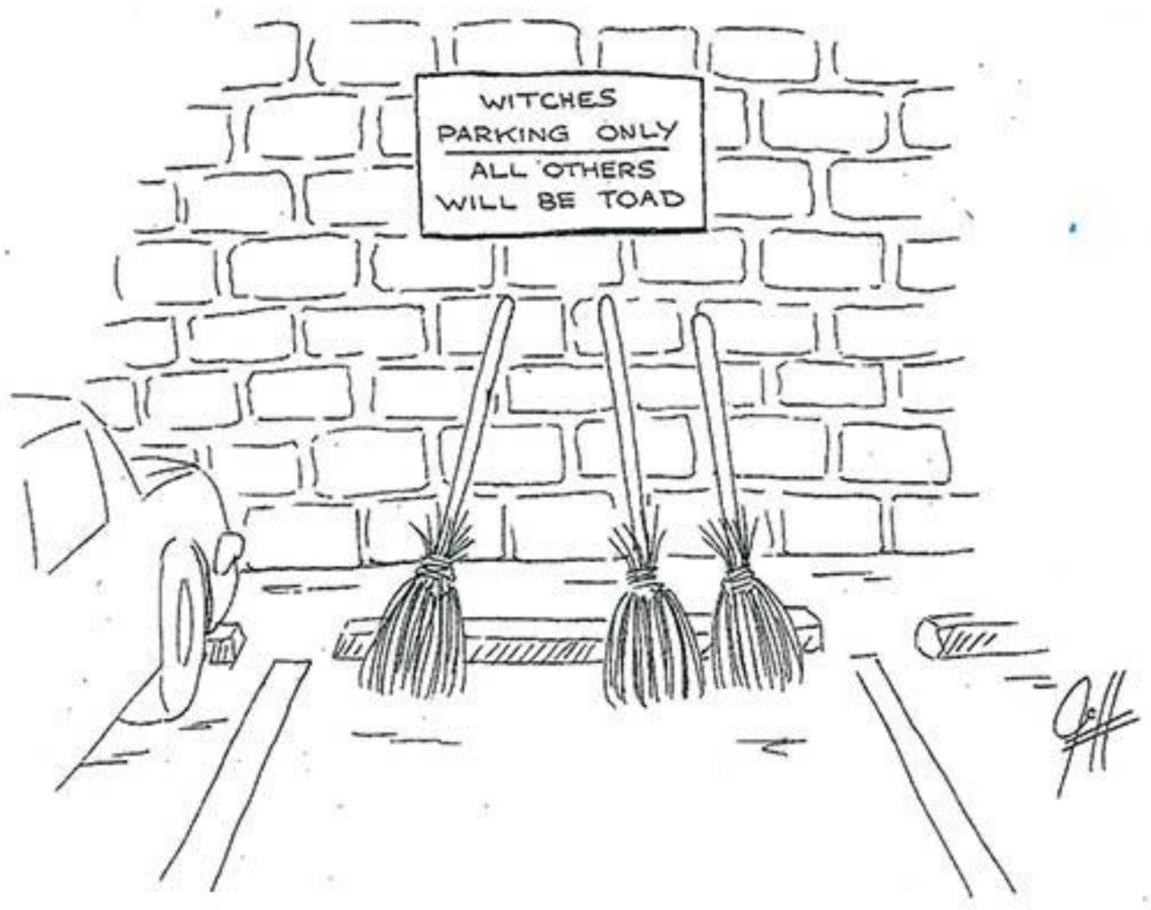
Parking assistance & Distance display



Misuse 1: The car doesn’t stop while it should.



Misuse 2: The car stops while it shouldn’t.

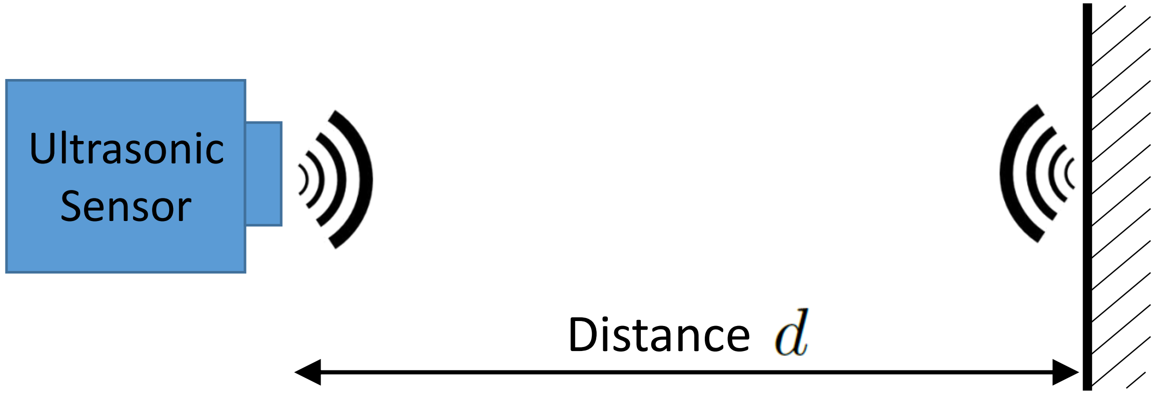


How do ultrasonic sensors work?

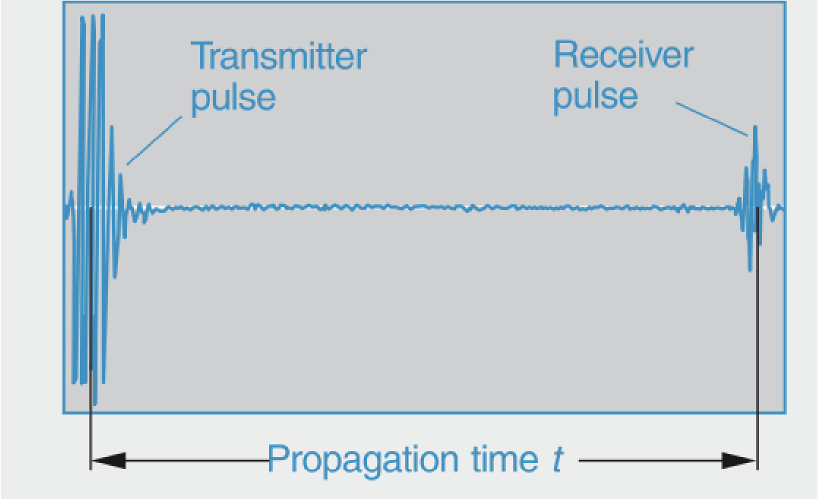
- **Emit ultrasound and receive echoes**
- **Piezoelectric Effect**
- **Measure the propagation time (Time of Flight)**
- **Calculate the distance** $d = 0.5 \cdot t_e \cdot c$

t_e : propagation time of echoes

c : velocity of sound in air



Electrical signal



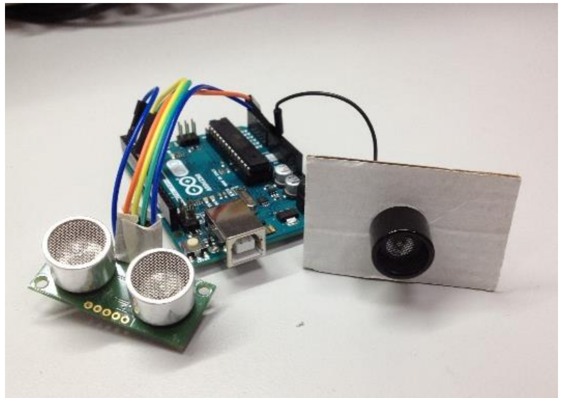
Attacking ultrasonic sensors

Attacks:

- **Jamming – generates ultrasonic noises – denial of service**
- **Spoofing – crafts fake ultrasonic echo pulses – alters distance**
- **Quieting – diminishes original ultrasonic echoes – hides obstacles**

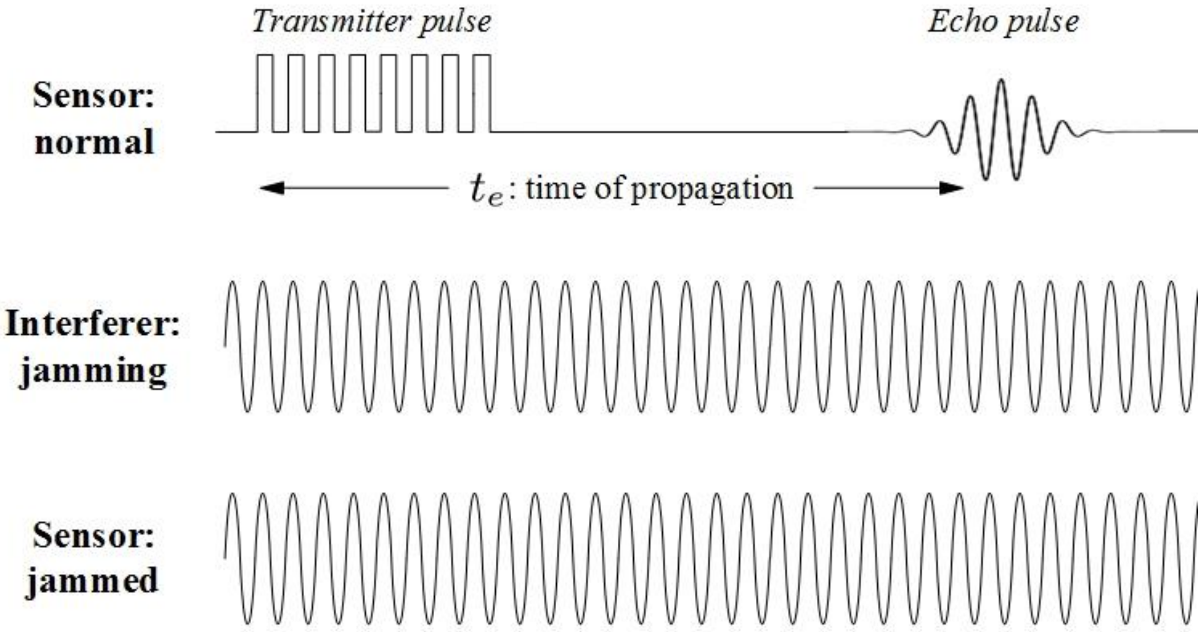
Equipment:

- **Ultrasonic transducers ($0.4) – emit ultrasound**
- **Signal suppliers – generate excitation signals**
  - Arduino ($24.95)
  - Signal generator (~$20)



Jamming Attack

- **Basic Idea:**
  - – Injecting ultrasonic noises
  - – At resonant frequency (40 – 50 kHz)
  - – Causing Denial of Service

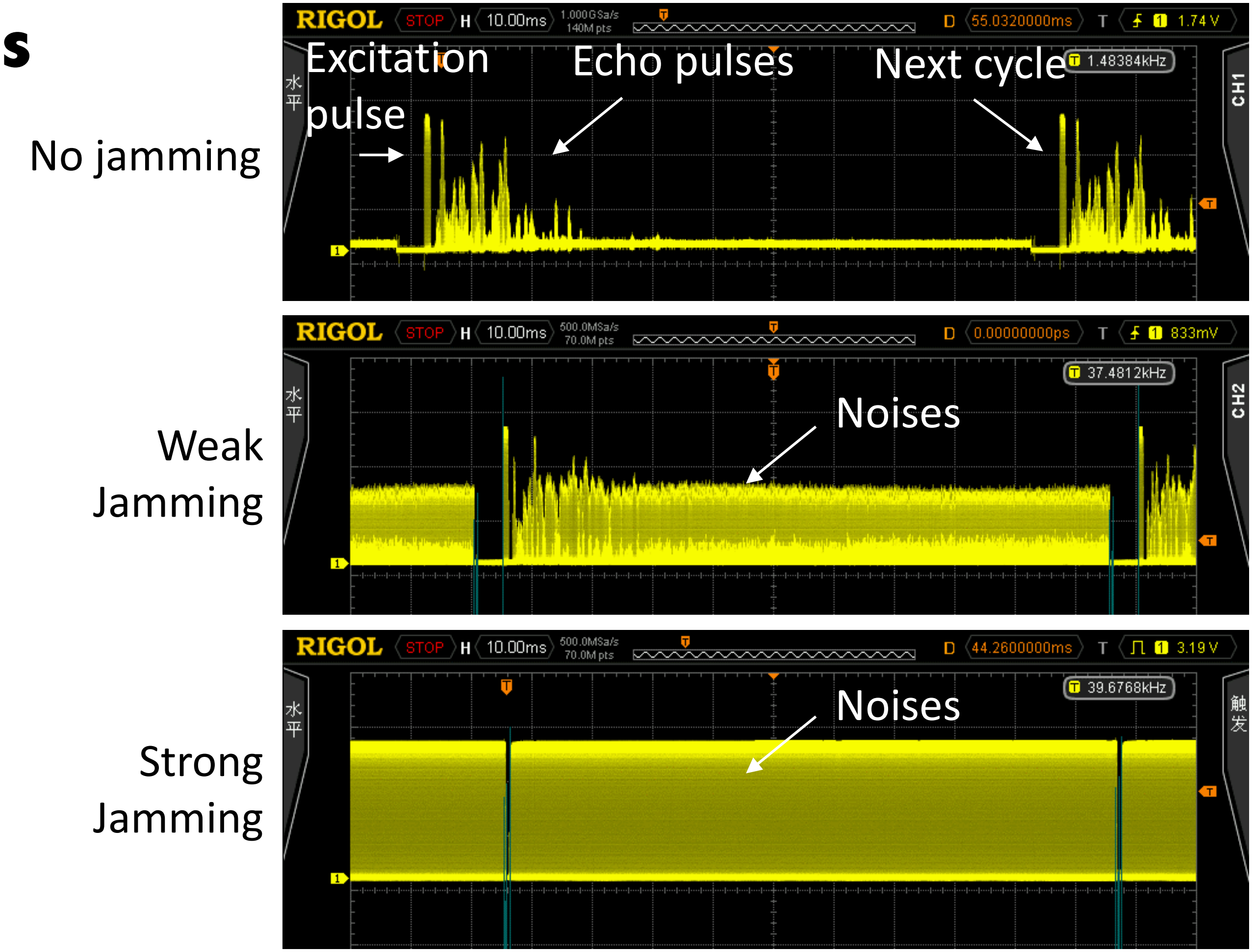


- **Tested ultrasonic sensors:**
  - – In laboratories: 8 models of stand-alone ultrasonic sensors
  - – Outdoors: Tesla, Audi, Volkswagen, Ford

Jamming Attack – in lab

- **8 models of ultrasonic sensors**
  - HC-SR04
  - SRF01
  - SRF05
  - MaxSonar MB1200
  - JSN-SR04T
  - FreeCars V4
  - Grove ultrasonic ranger
  - Audi Q3 sensors
- **Sensor reading**
  - **Zero** distance
  - **Maximum** distance

Received electrical signals at the sensor



How should cars behave to jamming?

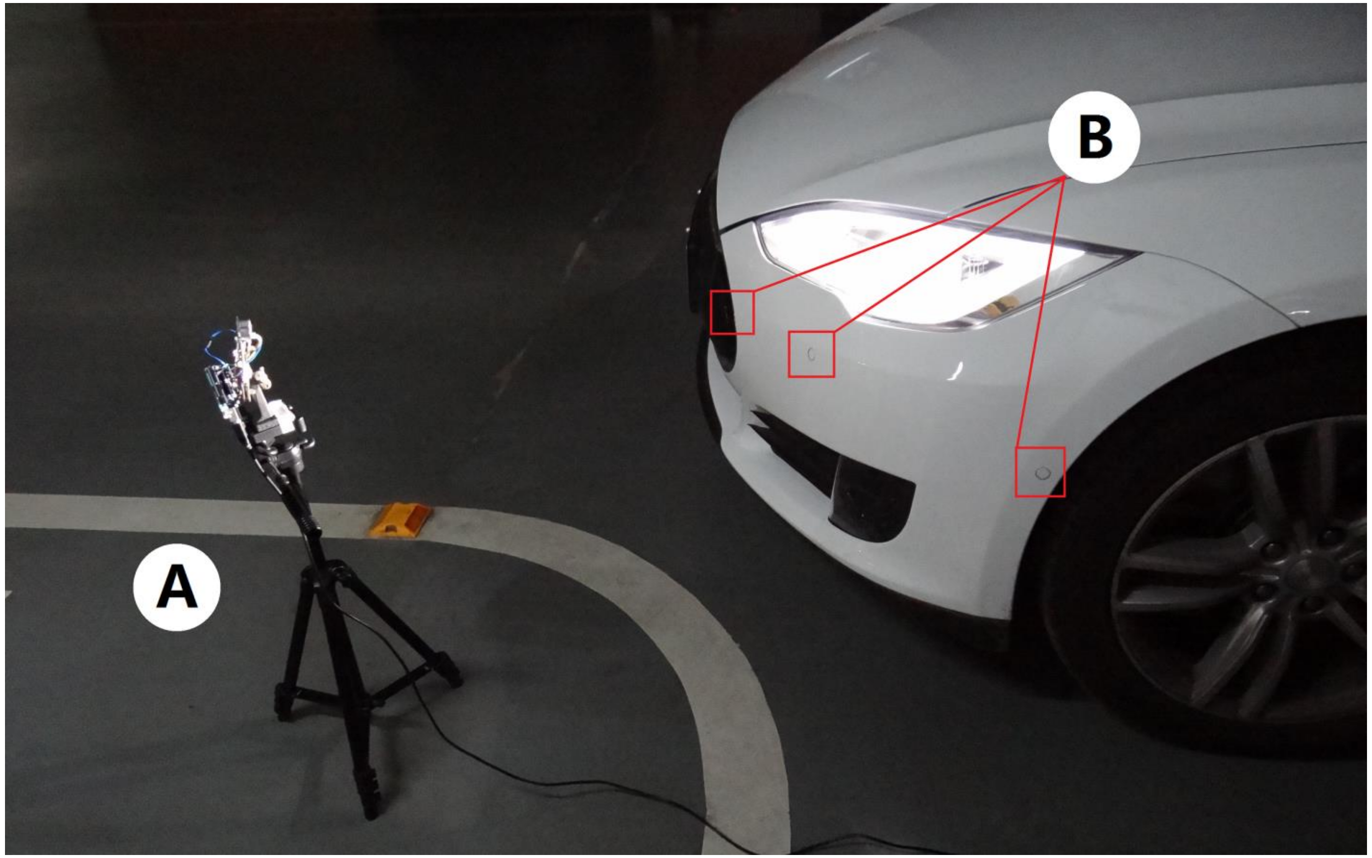
Zero distance?

or

Maximum distance?

Jamming Attack – on vehicles

- **4 different vehicles**
  - Audi Q3
  - Volkswagen Tiguan
  - Ford Fiesta
  - Tesla Model S
    - Self parking
    - Summon
- **Results**
  - **Maximum** distance



Experiment setup on Tesla Model S

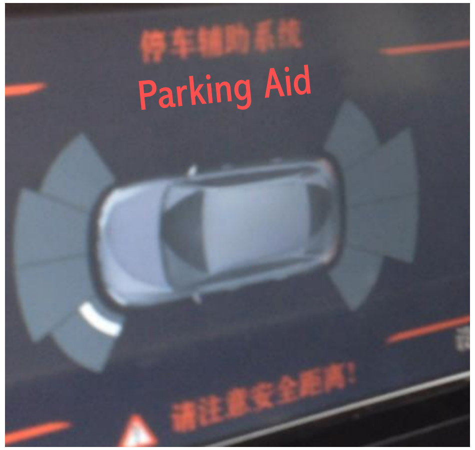
Jamming Attack – Demo on Audi

Jamming hides obstacles.

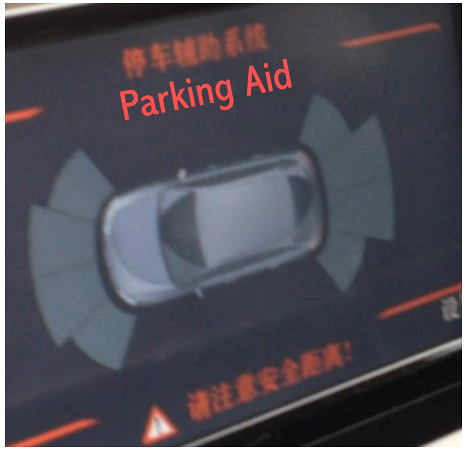
Jamming Attack – Results

- **On ultrasonic sensors**
  - Zero or maximum distance
- **On vehicles with parking assistance**
  - Maximum distance
- **On self-parking and summon?**

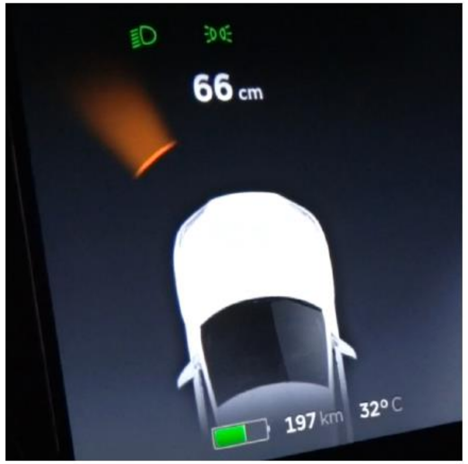
Note: If a sensor is unable to provide feedback, the instrument panel displays an alert message.



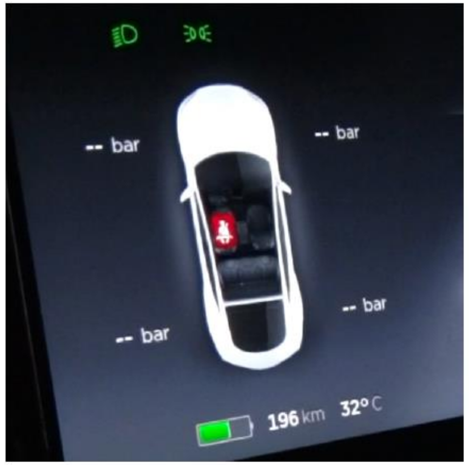
Audi Normal



Audi Jammed

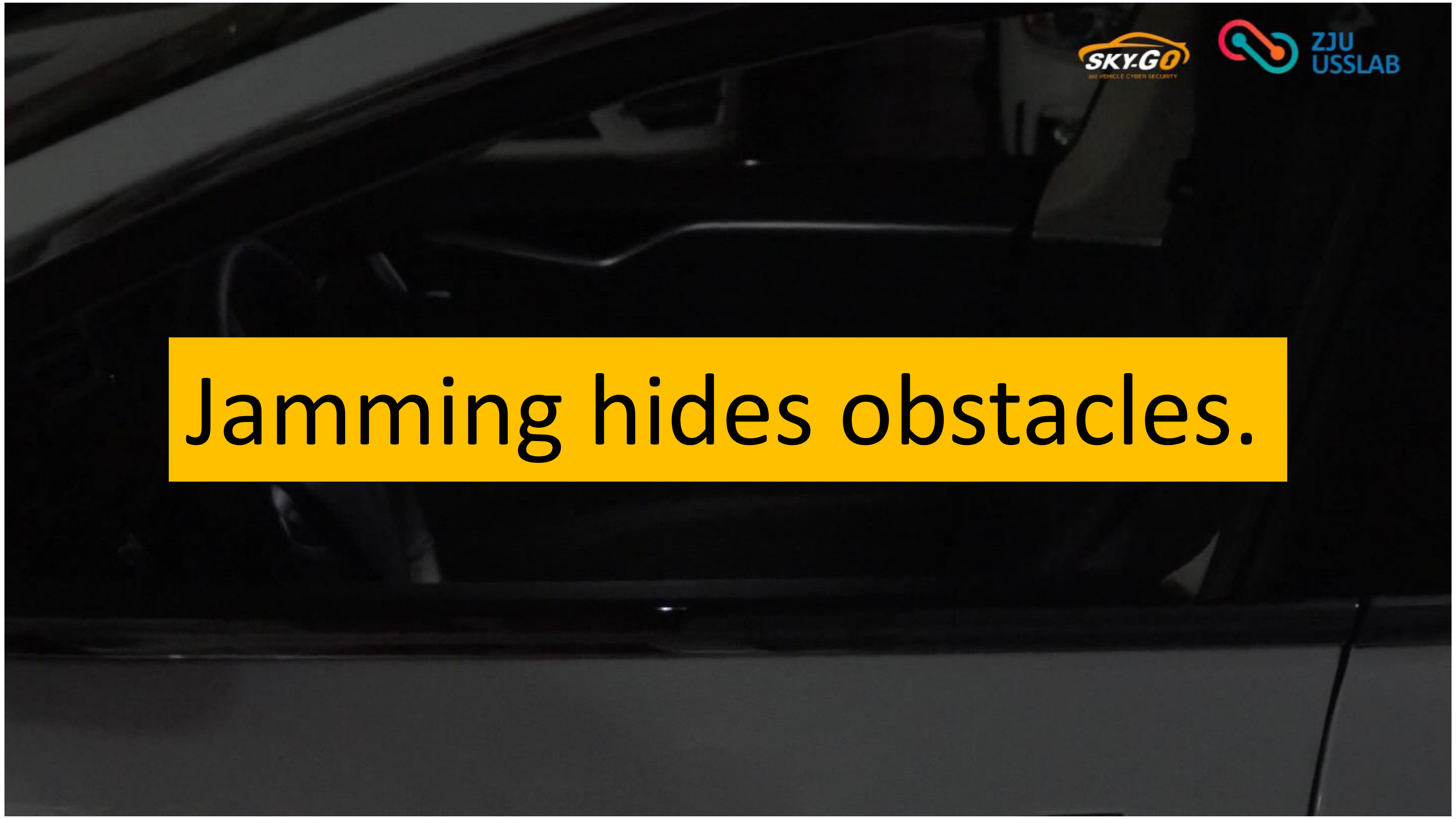


Tesla Normal



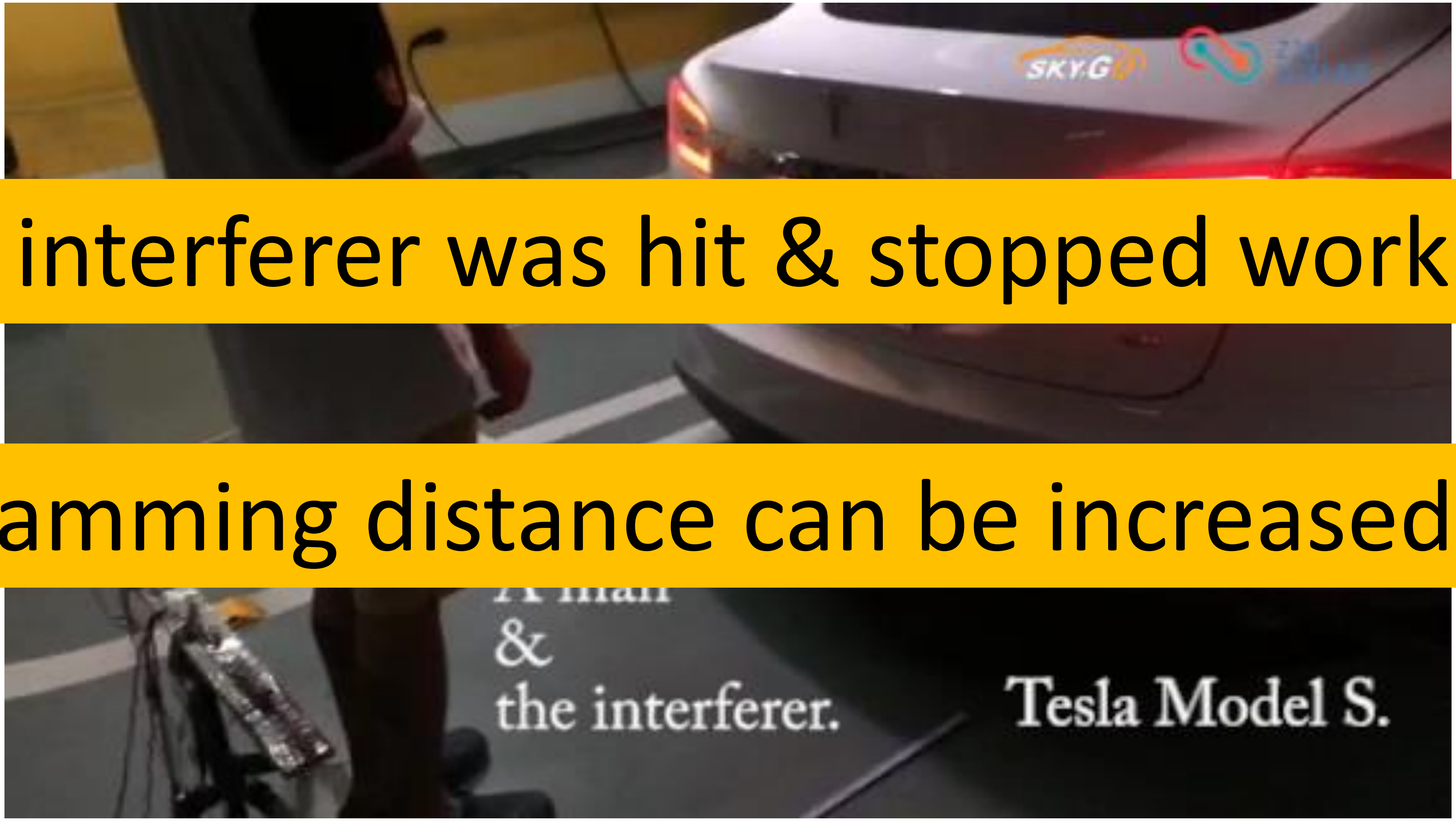
Tesla Jammed

Jamming Attack – Demo on Tesla Summon



Jamming hides obstacles.

Jamming Attack – Demo on Tesla Summon

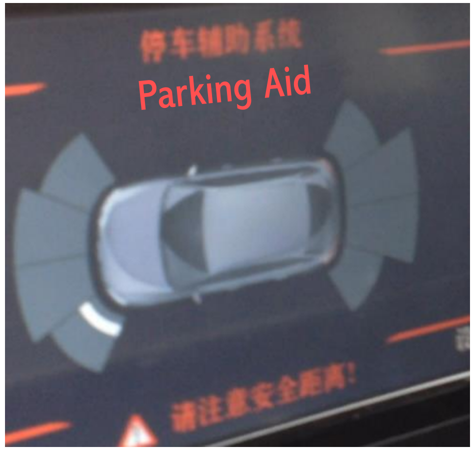


The interferer was hit & stopped working.

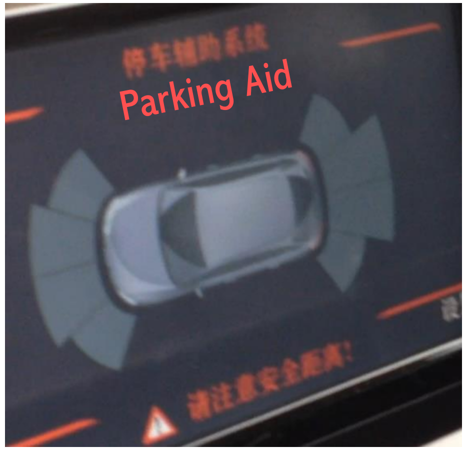
Jamming distance can be increased.

Jamming Attack – Results

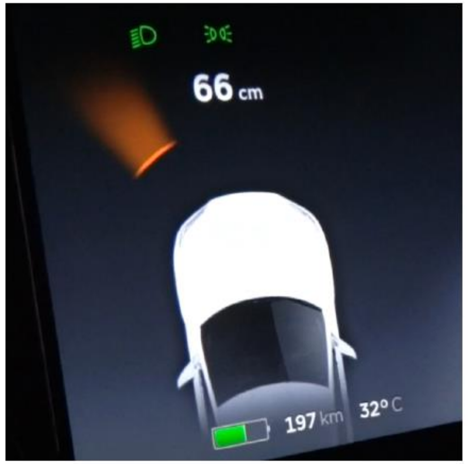
- On ultrasonic sensors
  - Zero or maximum distance
- On vehicles with parking assistance
  - Maximum distance
- **On self-parking and summon**
  - Car does not stop under strong jamming!



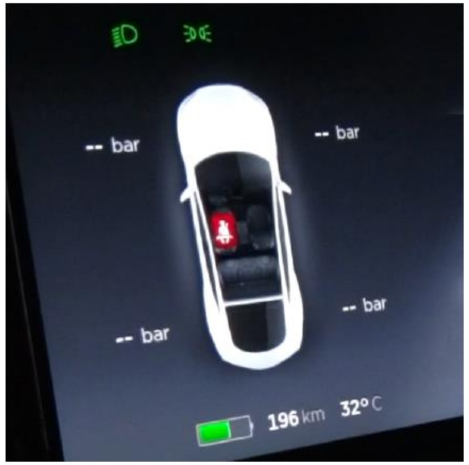
Audi Normal



Audi Jammed



Tesla Normal



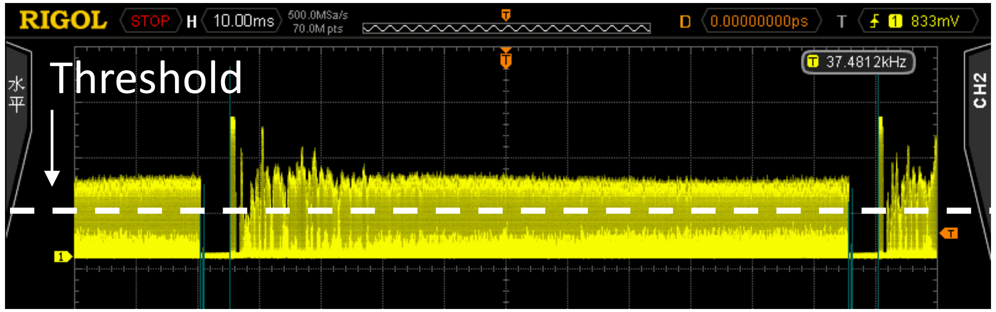
Tesla Jammed

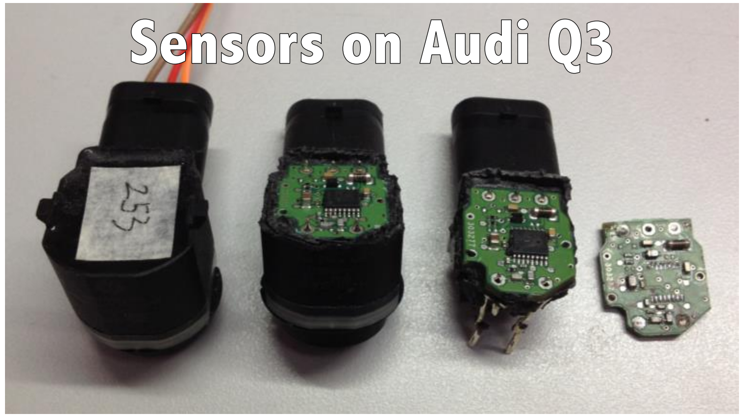
Why Zero or Max distance?

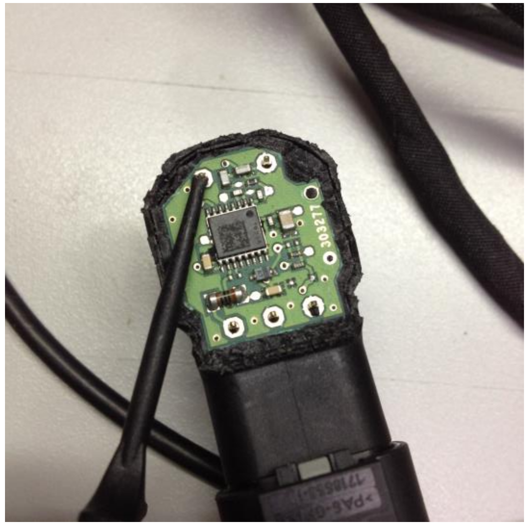
Different sensor designs

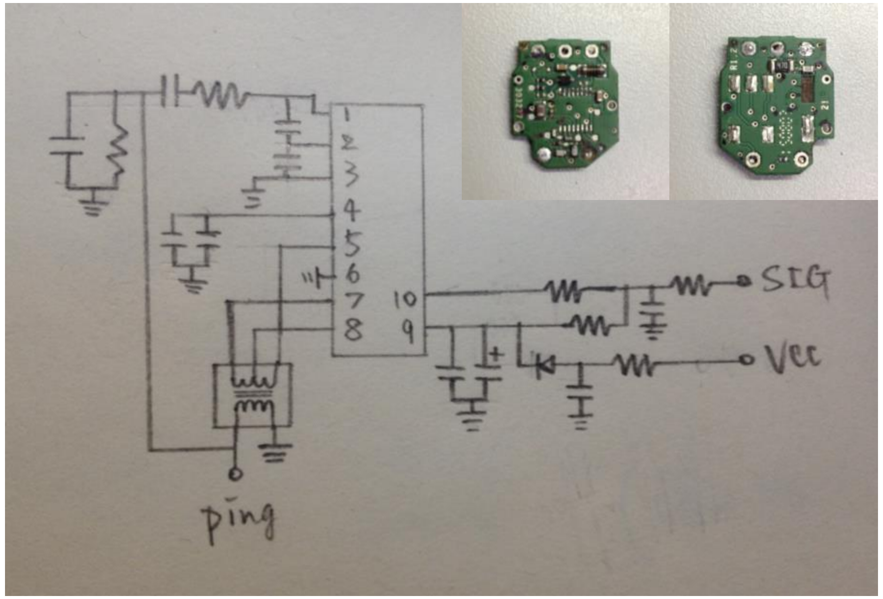
- **Zero distance**
  - Compare with a fixed threshold
- **Maximum distance**

  Application Specific IC!





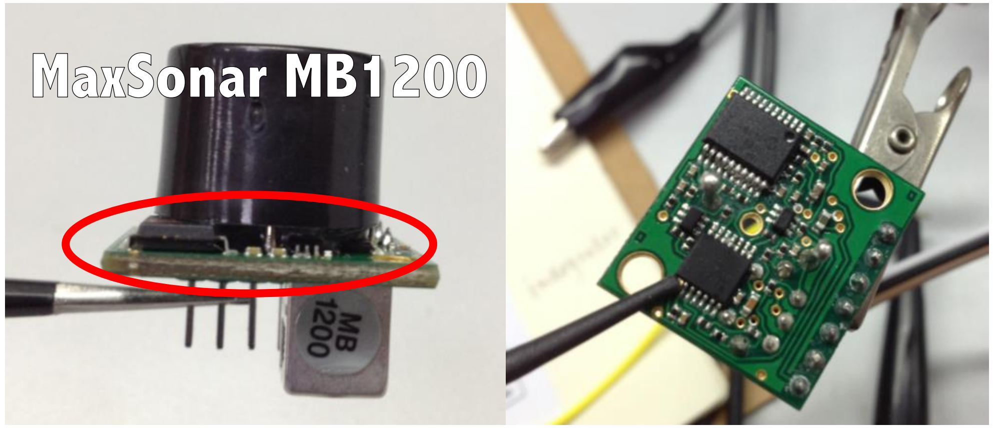


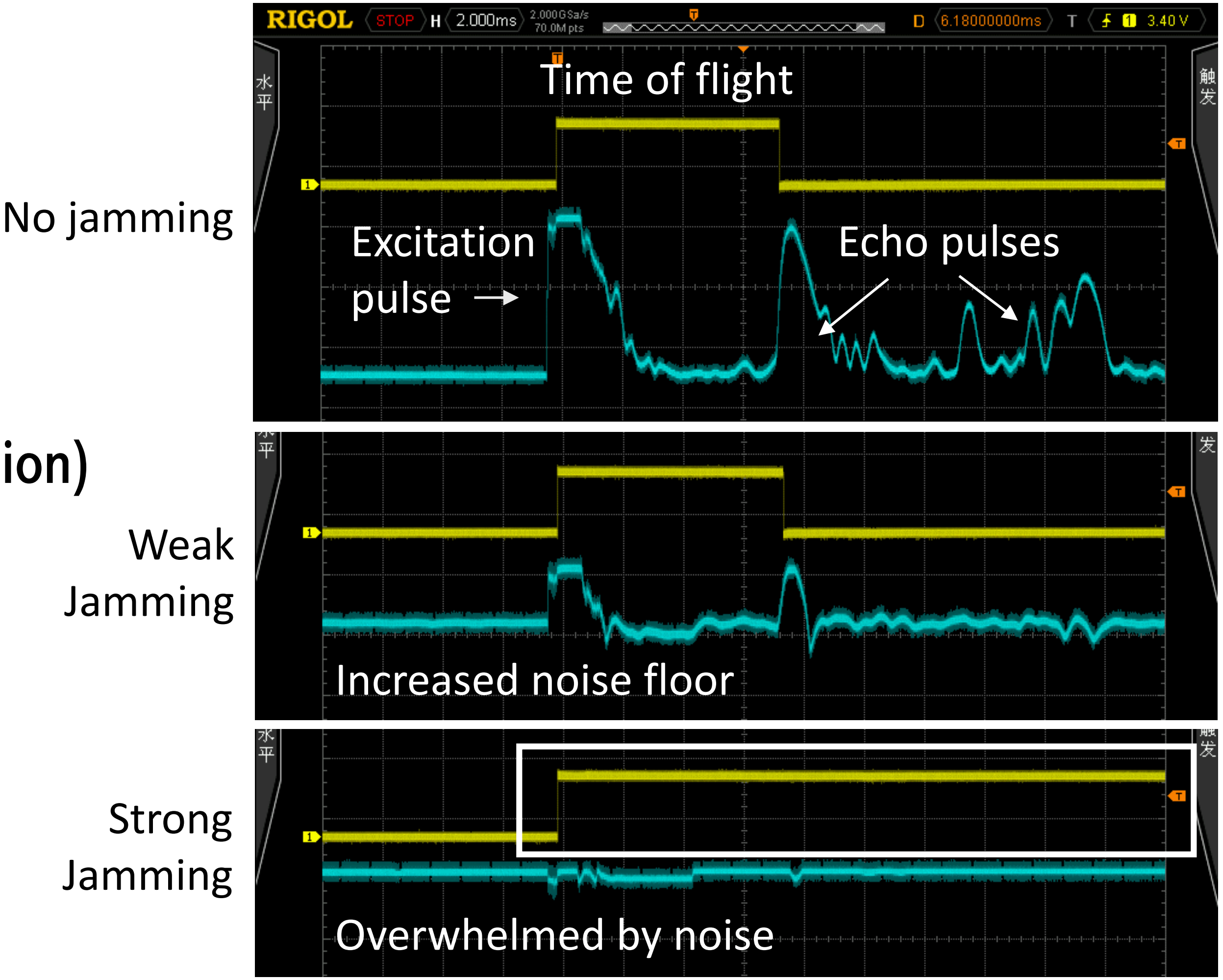


Why Zero or Max distance?

Different sensor designs

- **Zero distance**
  - Compare with a fixed threshold
- **Maximum distance**
  - Adaptive threshold (Noise Suppression)





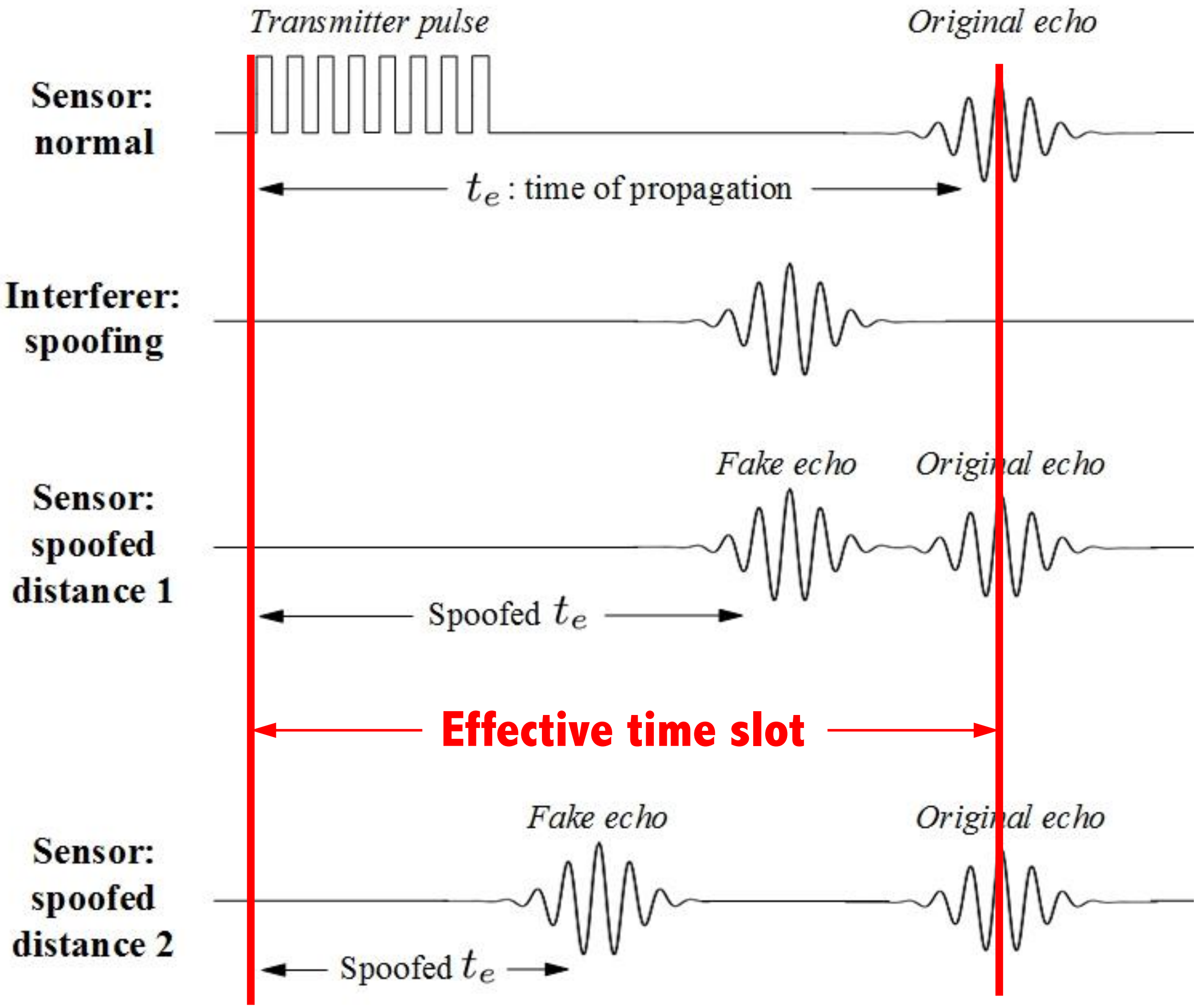
Spoofing Attack

Basic Idea

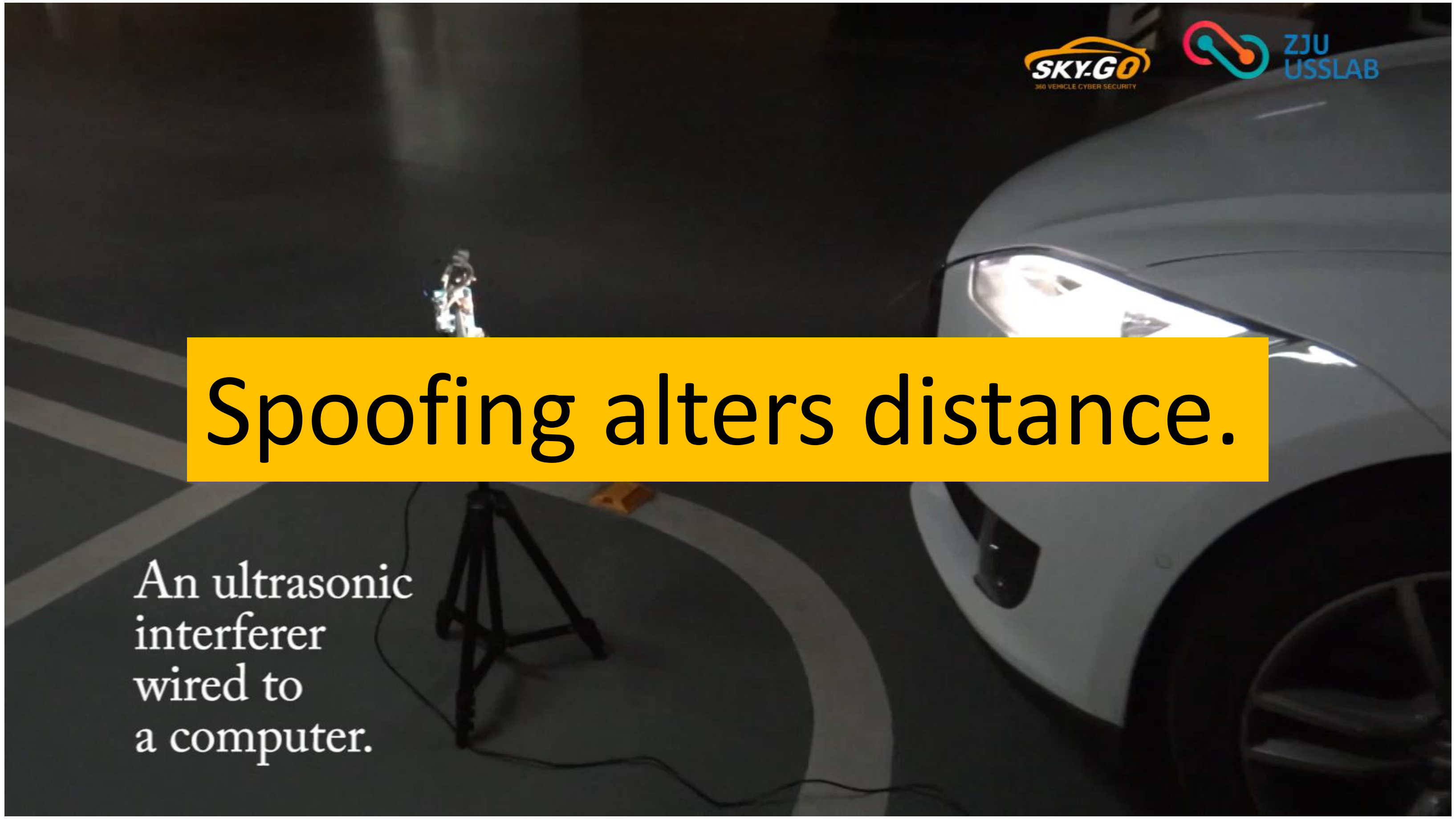
- Injecting ultrasonic pulses
- At certain time

Non-trivial

- Only the first justifiable echo will be processed
- **Effective time slot**



Spoofing Attack – Demo on Tesla



Spoofing alters distance.

An ultrasonic
interferer
wired to
a computer.

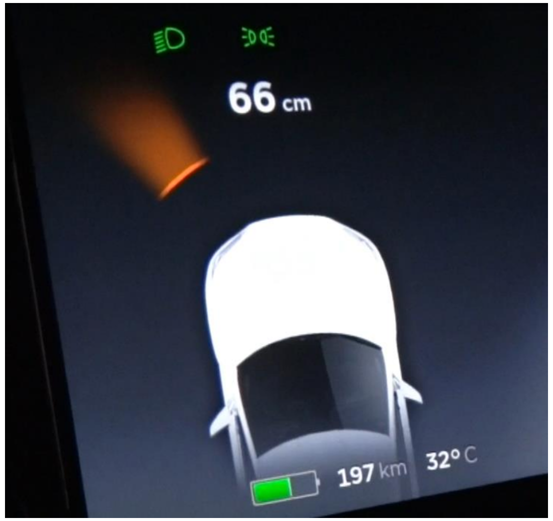
Spoofing Attack – Demo on Audi

Spoofing alters distance.

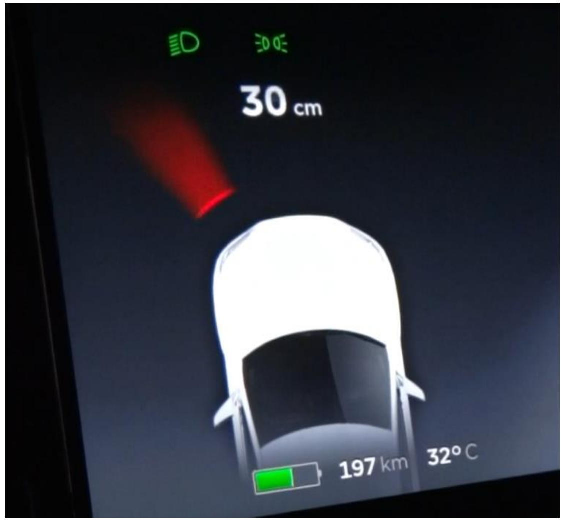
Nothing is in front of the car.

Spoofing Attack – Results

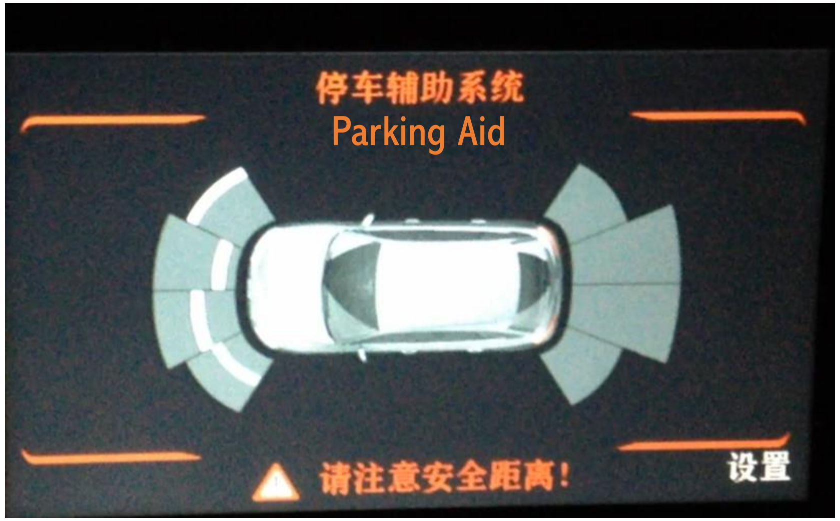
- **Manipulate sensor readings**
  - On stand-alone ultrasonic sensors
  - On cars



Tesla Normal



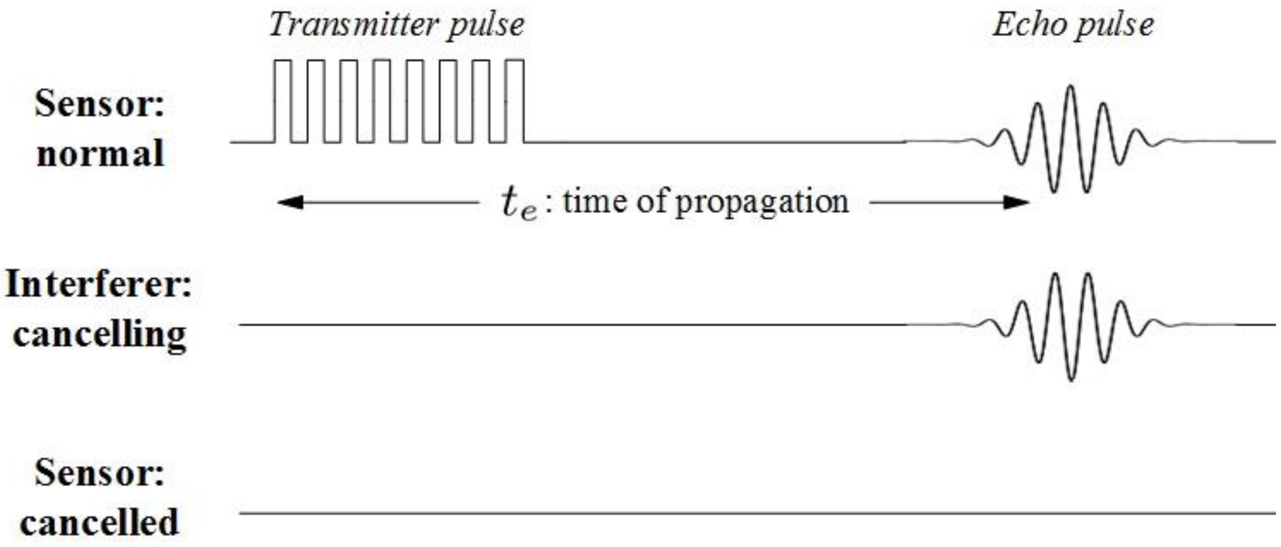
Tesla Spoofed

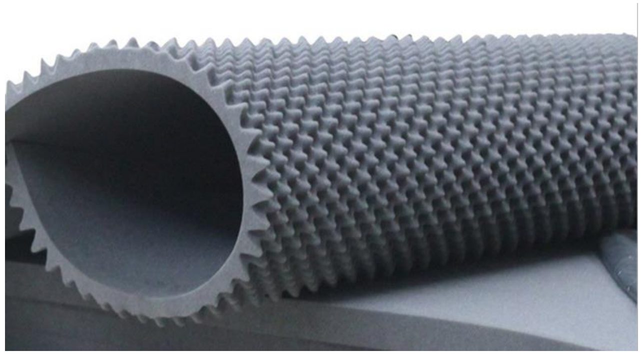


Audi Spoofed

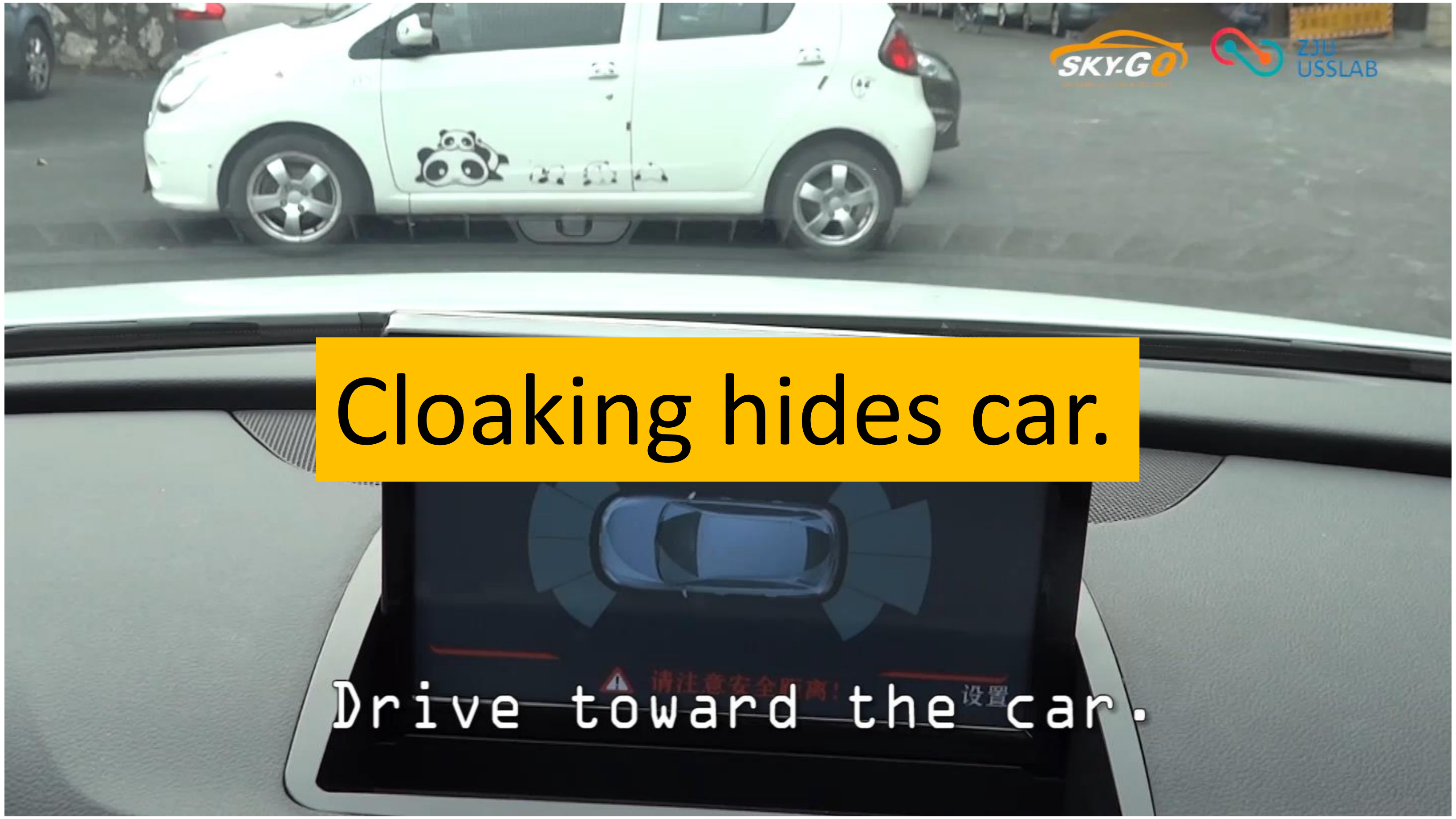
Acoustic Quieting

- **Acoustic Cancellation**
  - Cancel original sound with ones of reversed phase
  - Minor phase and amplitude adjustment
- **Cloaking**
  - Sound absorbing materials (e.g., damping foams ($3/m^2))
  - Same effect as jamming!



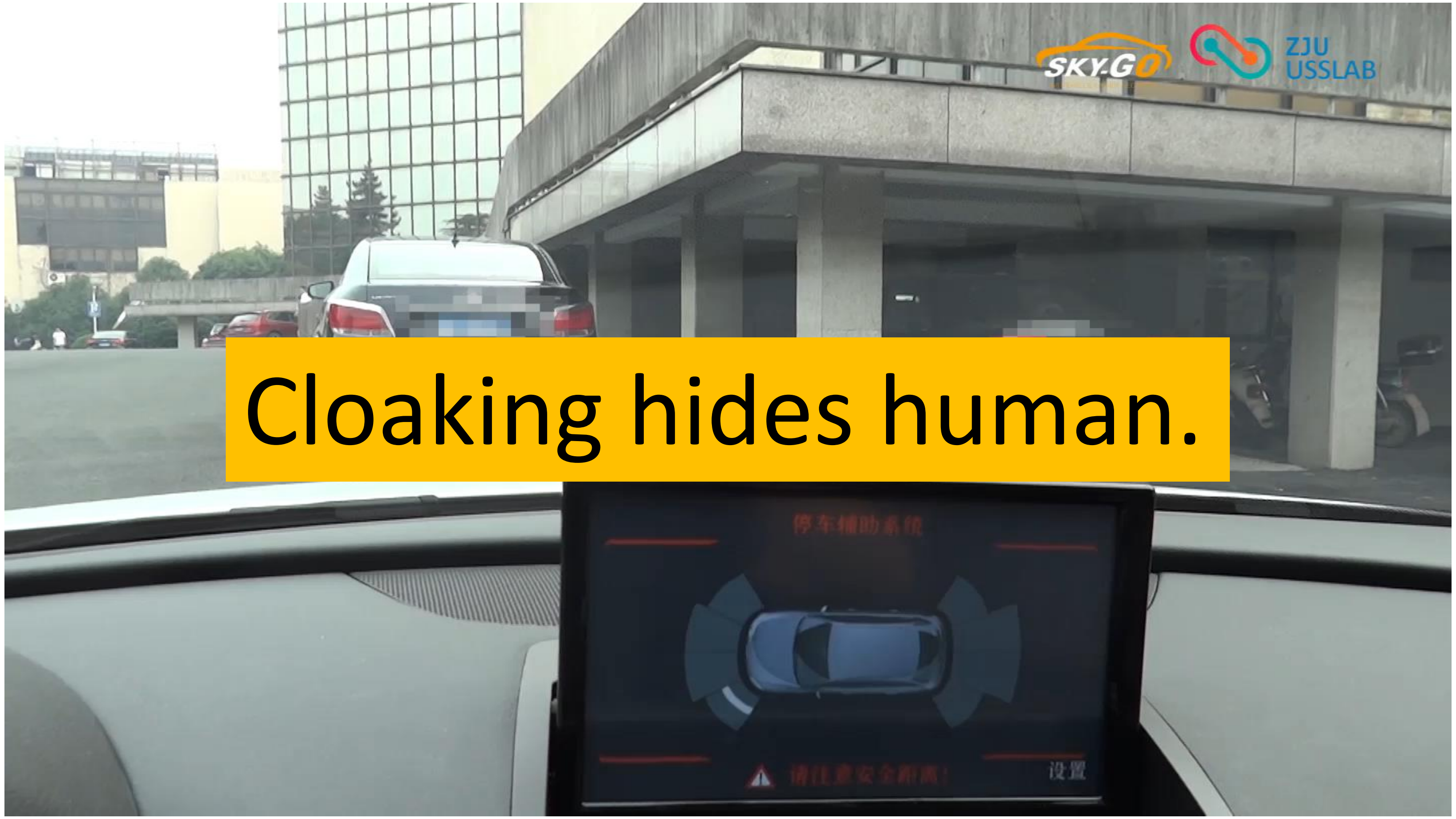


Cloaking Car – Demo



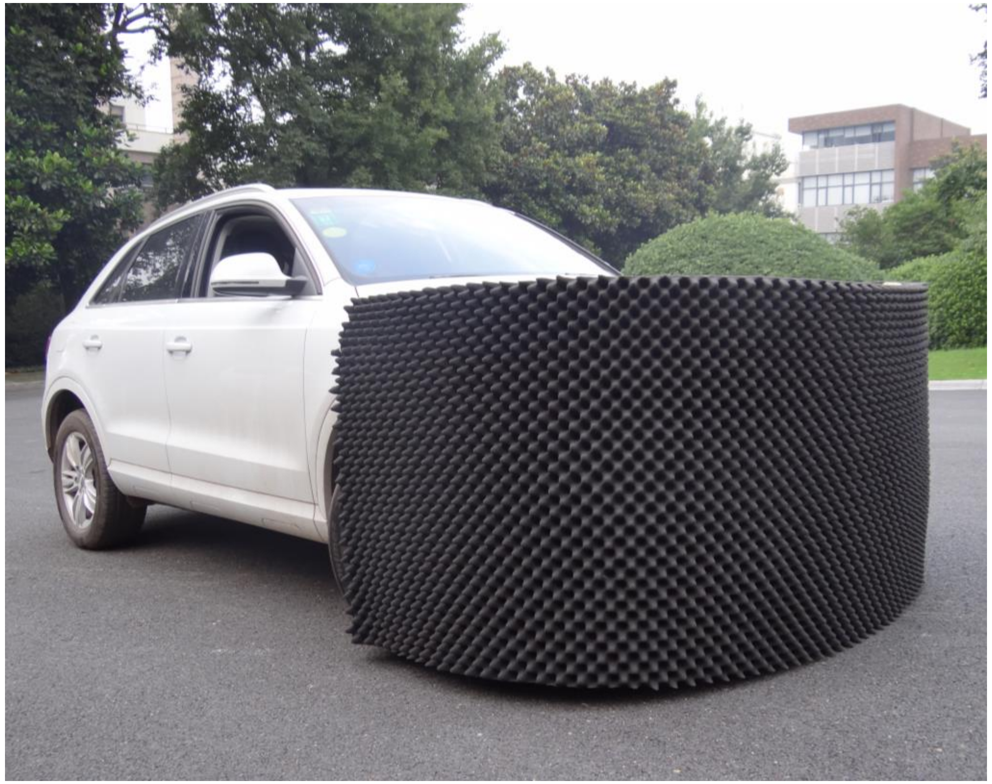
Cloaking hides car.

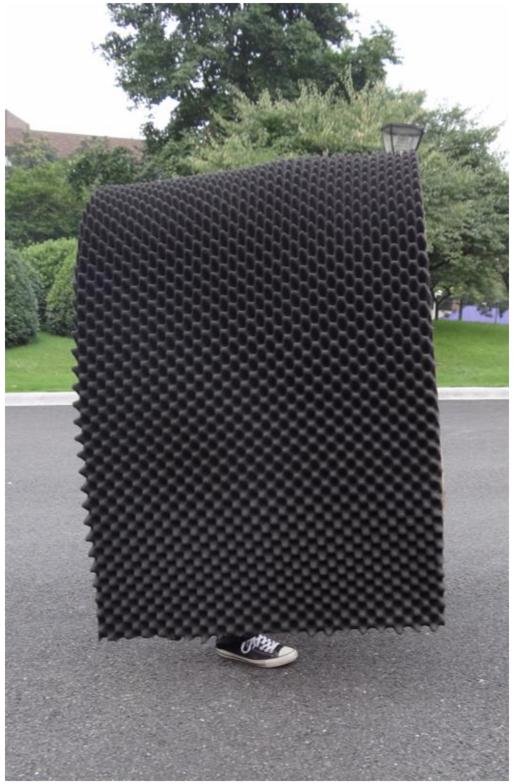
Cloaking Human – Demo



Cloaking hides human.

Invisible car! Invisible man! Invisible glass! Whee!





Attacking Millimeter Wave Radars

On Tesla Model S

Millimeter Wave Radar

What is MMW Radar?

- Measures distance, angle, speed, shape
- Short to long range sensing (30-250m)

- Applications
  - Adaptive Cruise Control (ACC)
  - Collision Avoidance
  - Blind Spot Detection

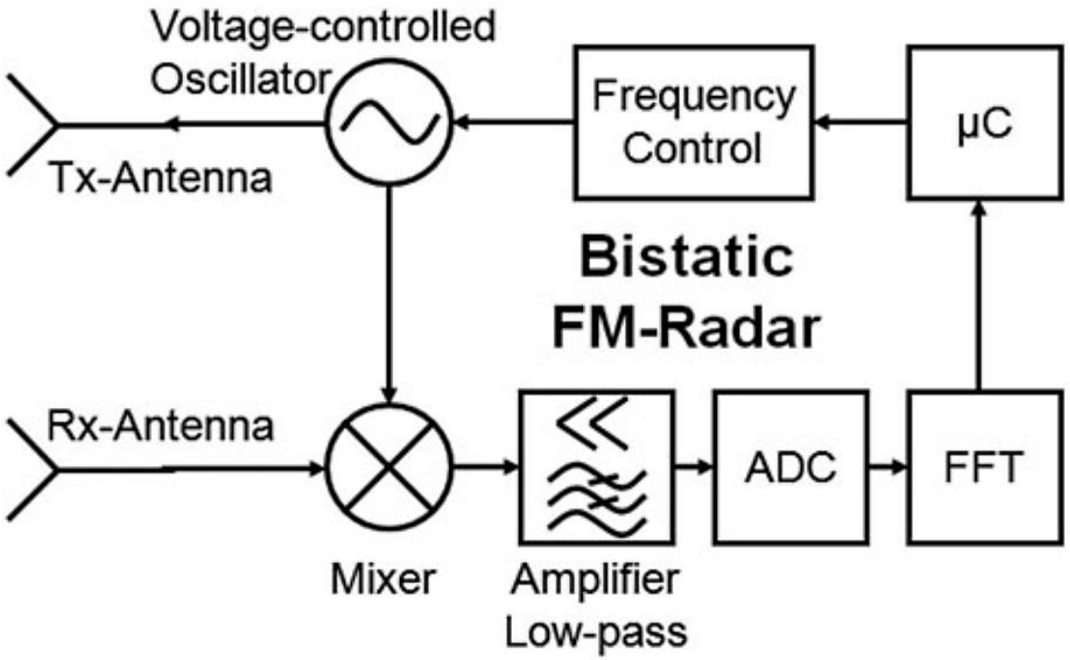
Construction of the Bosch RADAR sensors MRR and LRR3 (Source: Bosch)

Misuse 1: The car doesn’t stop while it should.

Misuse 2: The car stops while it shouldn’t.

How do MMW Radars work?

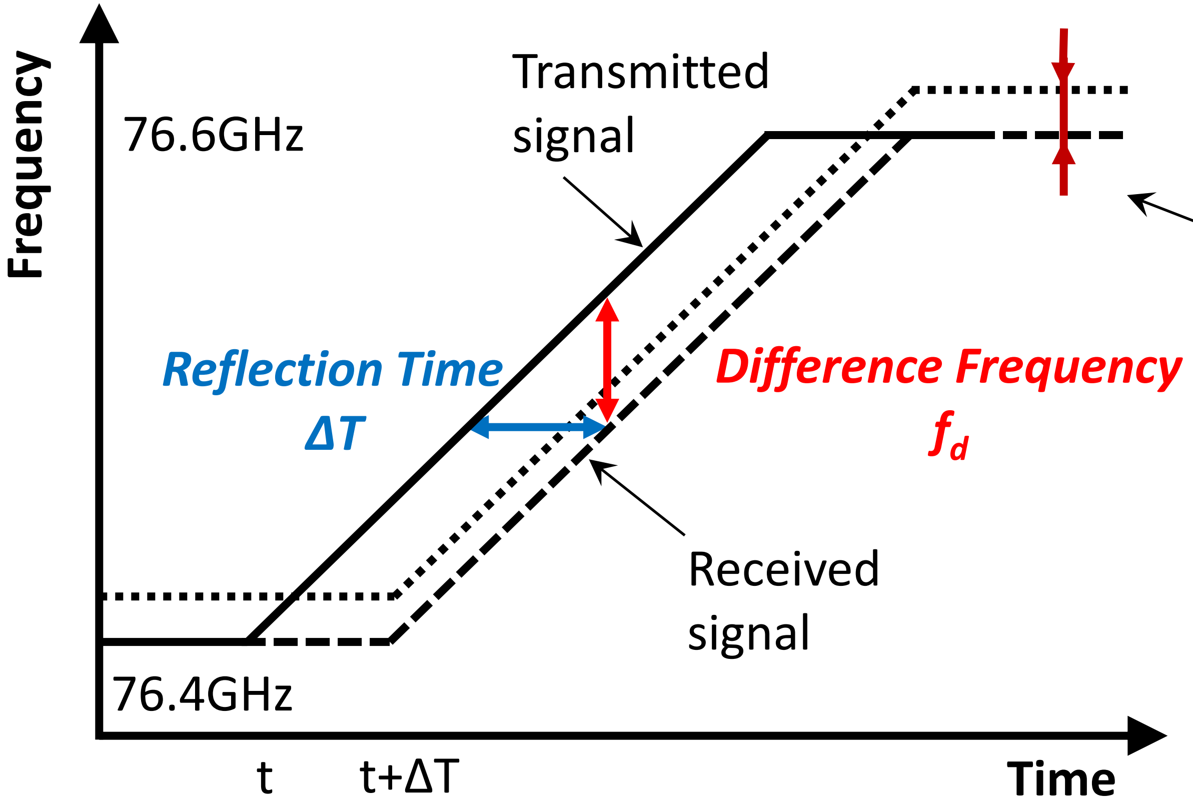
- **Transmit and receive millimeter electromagnetic waves**
- **Measure the propagation time**
- **Modulation**
  - Amplitude
  - Frequency (FMCW)
  - Phase
- **Doppler Effect**
- **Frequency Bands:**
  - 24 GHz
  - 76-77 GHz



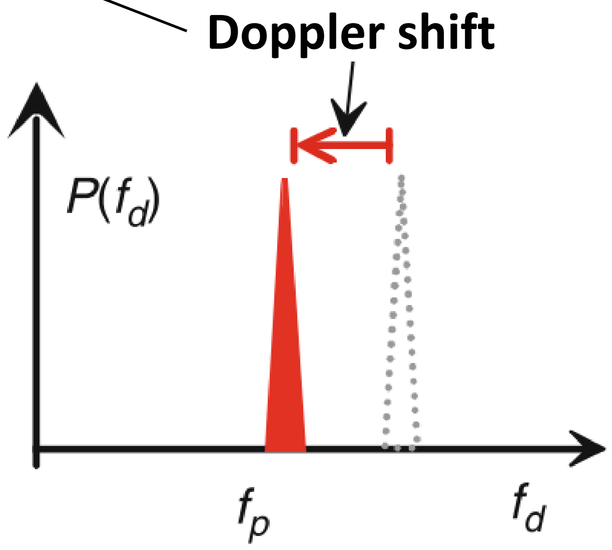
Block diagram of a bistatic Radar with frequency modulation

(Source: H. Winner, Handbook of Driver Assistance Systems)

Frequency Modulated Continuous Wave（FMCW)



$$\Delta T = \frac{f_d}{slope}$$



MMW Radar – To be discovered

#1. Understand Radar signal – Signal Analysis

- Frequency range
- Modulation process
- Ramp height (bandwidth)
- Ramps (number, duration)
- Cycle time

#2. Jamming Attack

- Feasible?
- What jamming signal?

#3. Spoofing Attack

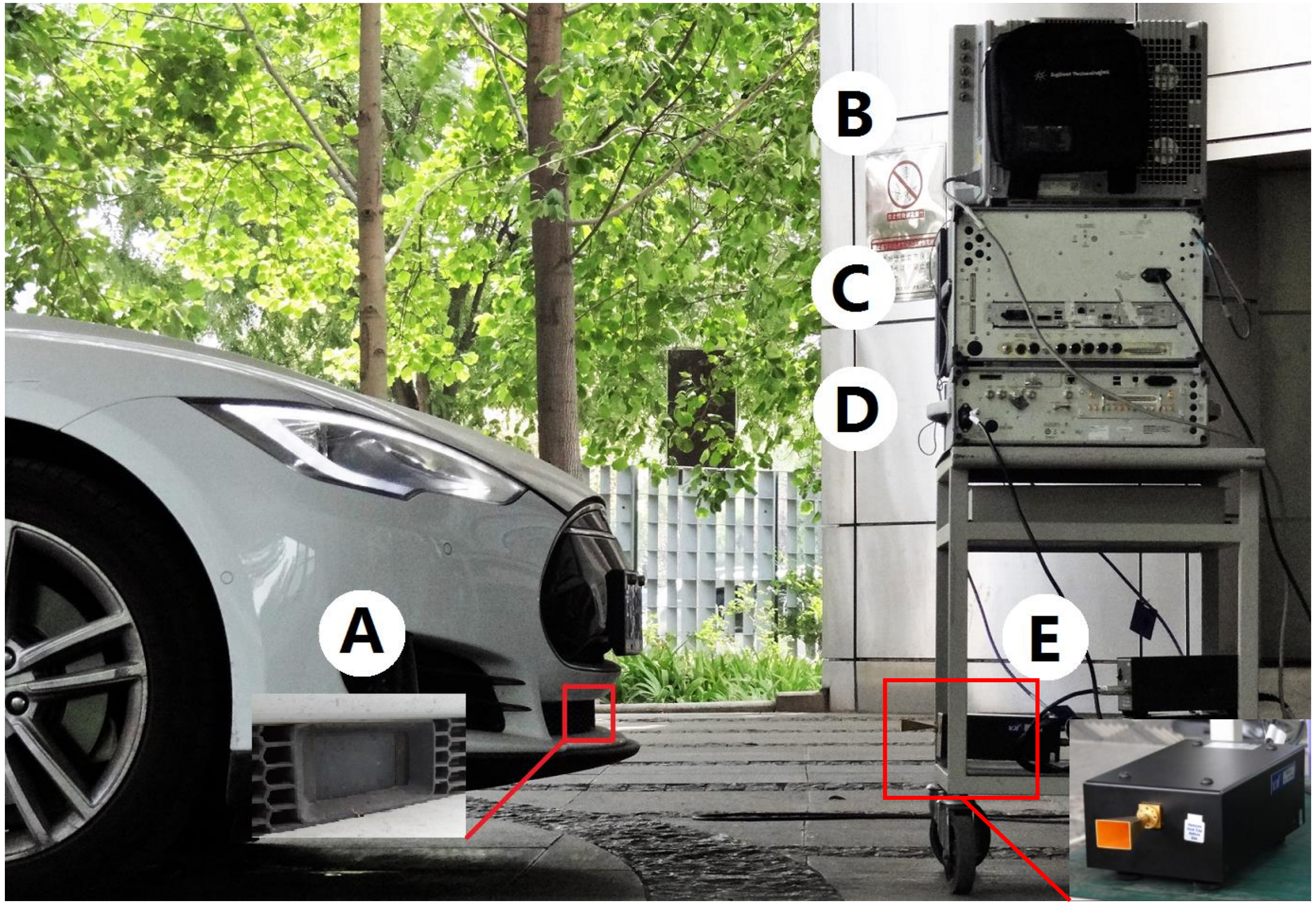
- Feasible?

The MMW Radar on Tesla Model S

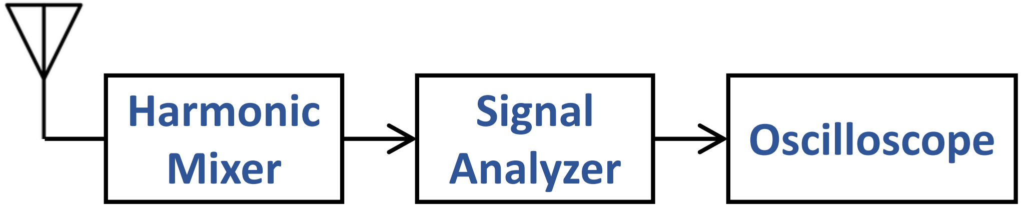
Attacking MMW Radar – Setup

- **Signal Analysis**
- **Jamming Attack**
- **Spoofing Attack**

- **Equipment:** KEYSIGHT TECHNOLOGIES
  - Tesla Model S Radar (A)
  - Signal analyzer (C)
  - Harmonic mixer (E)
  - Oscilloscope (B)
  - Signal generator (D)
  - Frequency multiplier (E)



MMW Radar Signal Analysis

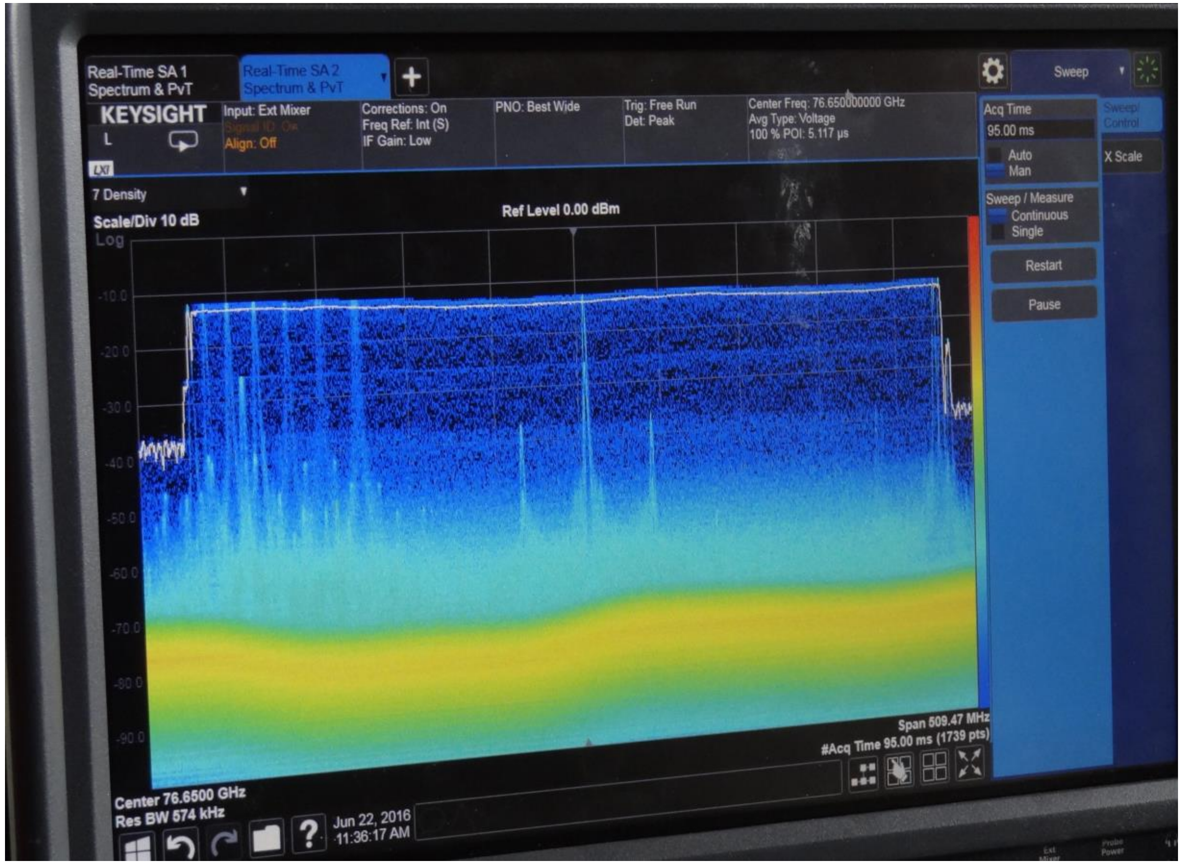


Harmonic Mixer → Signal Analyzer → Oscilloscope

Frequency domain analysis

Time domain analysis

- **Center frequency: 76.65 GHz**
- **Bandwidth: 450 MHz**
- **Modulation: FMCW**
- **Radar chirp details …**



Real-time spectrum on signal analyzer

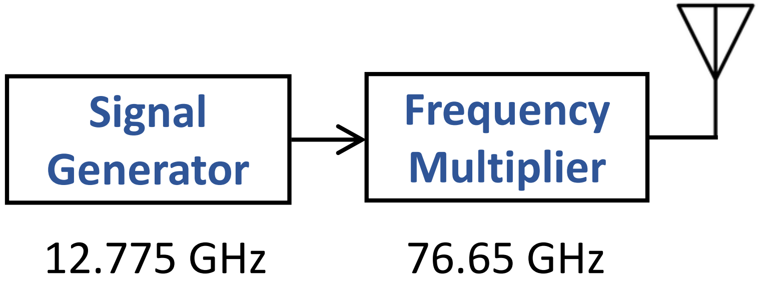
Attacks on MMW Radar

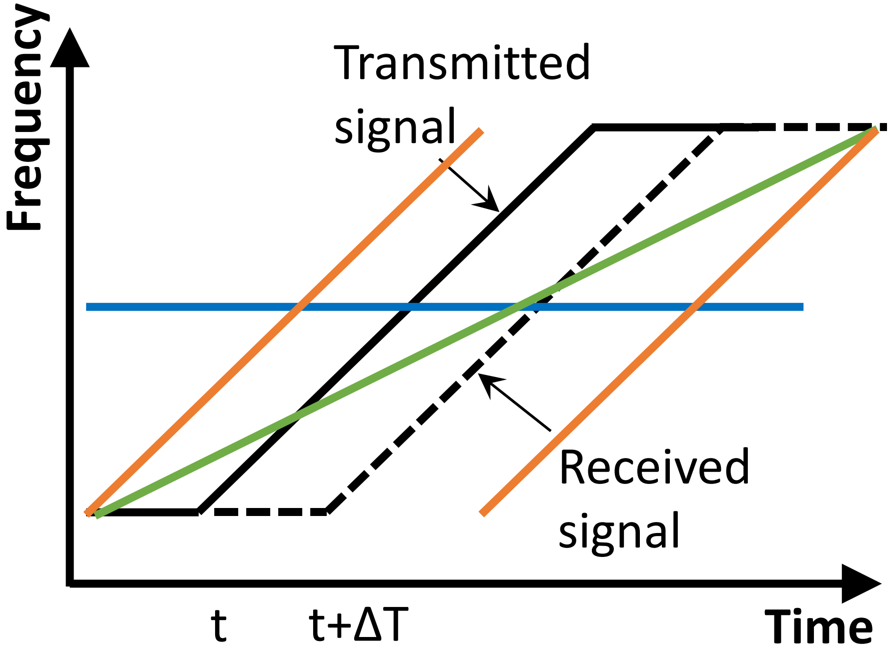
Jamming Attack

- Jam Radar within the same frequency band, i.e., 76 - 77 GHz
- At fixed frequency
- At sweeping frequency

Spoofing Attack

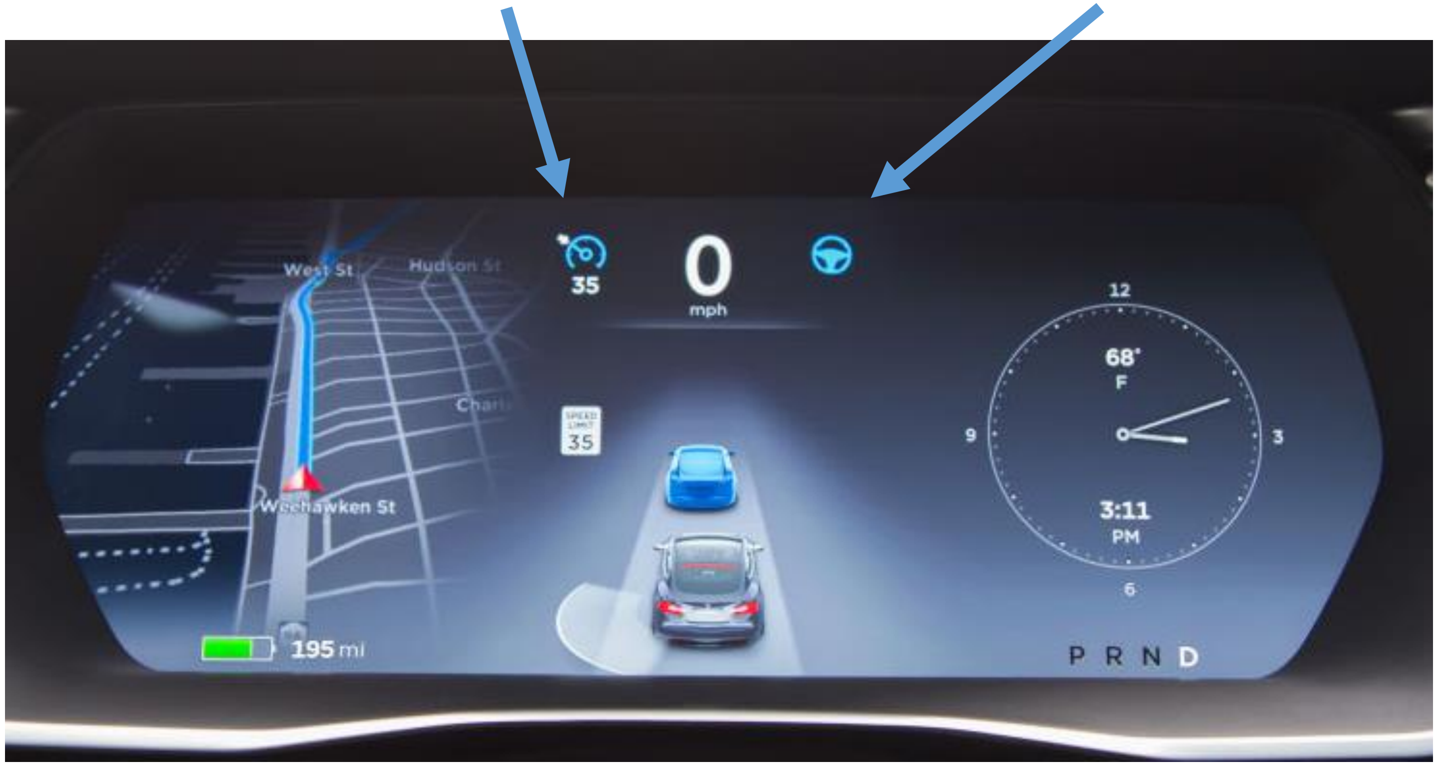
- Spoof the radar with similar RF signal





What indicates Autopilot?

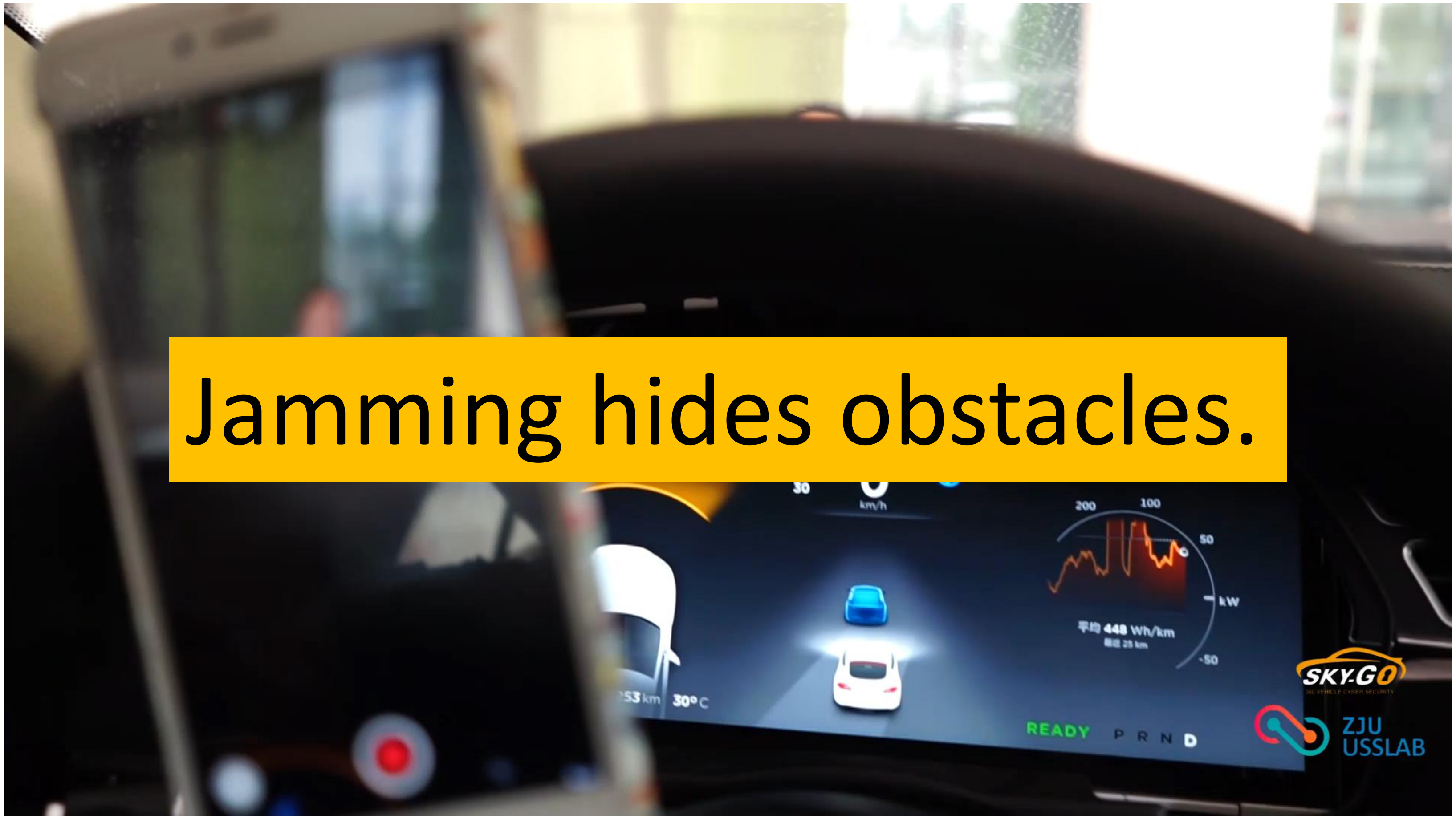
- What does blue mean?
- Why stationary?



Traffic Aware Cruise Control is on.

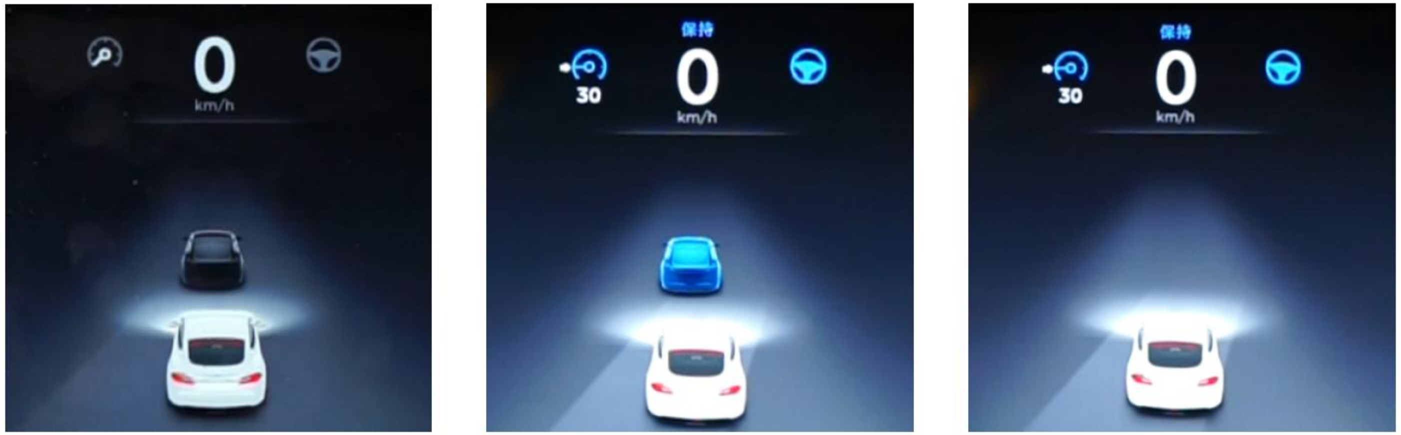
Autosteer is on.

Jamming Attack – Demo


Jamming hides obstacles.

Attacking MMW Radars – Results

- **Jamming: hides detected objects**
  - Either fixed or sweeping frequency signal worked
- **Spoofing: alters object distance**



(a) Drive gear. (b) Autopilot. (c) Jammed.

Result of jamming attack

Attacking Cameras

Mobileye & Point Grey

Tesla Model S

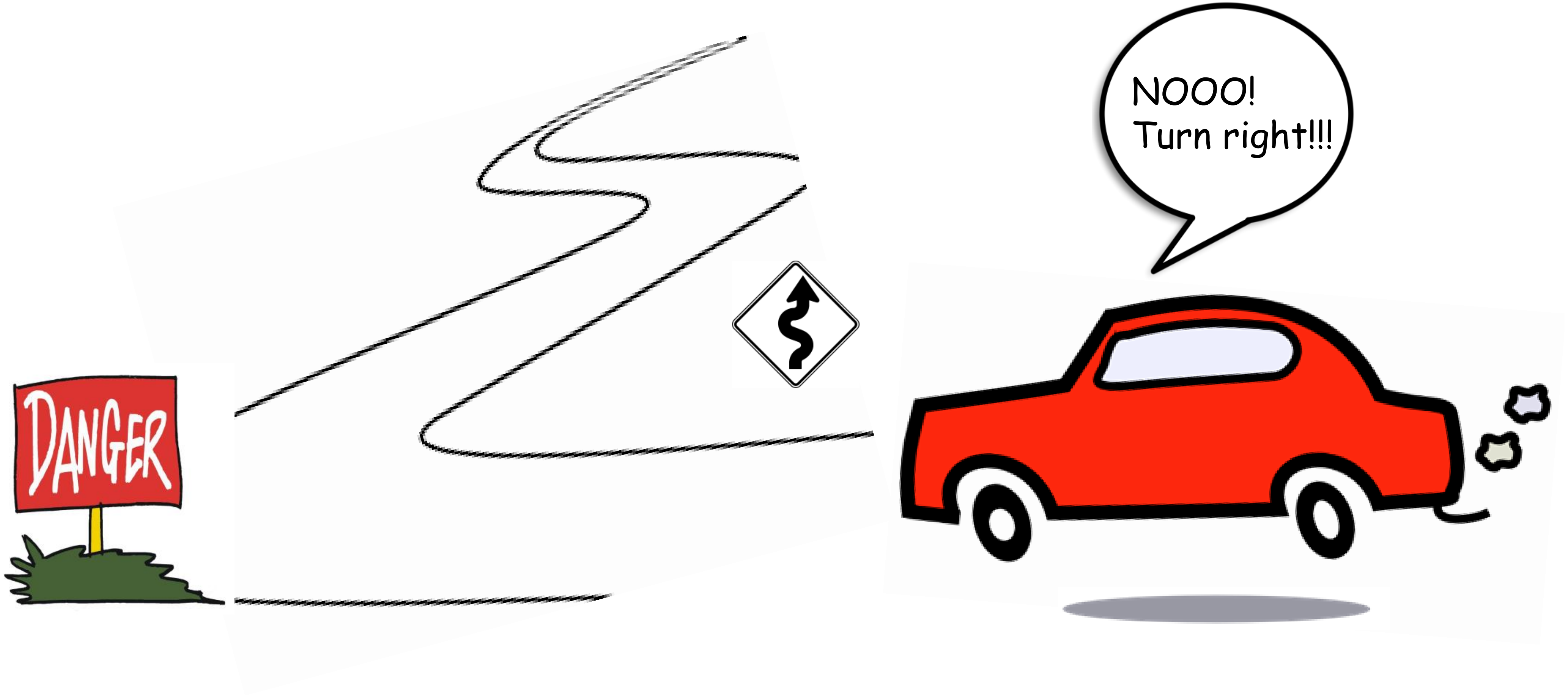
Automotive Cameras

What is automotive camera?

- **Computer vision**
- **Forward & backward**

- **Applications**
  - Lane departure warning
  - Lane keeping
  - Traffic sign recognition
  - Parking assistance

Misuse: The car doesn't steer while it should.



Attacking Cameras – Setup

Attack:

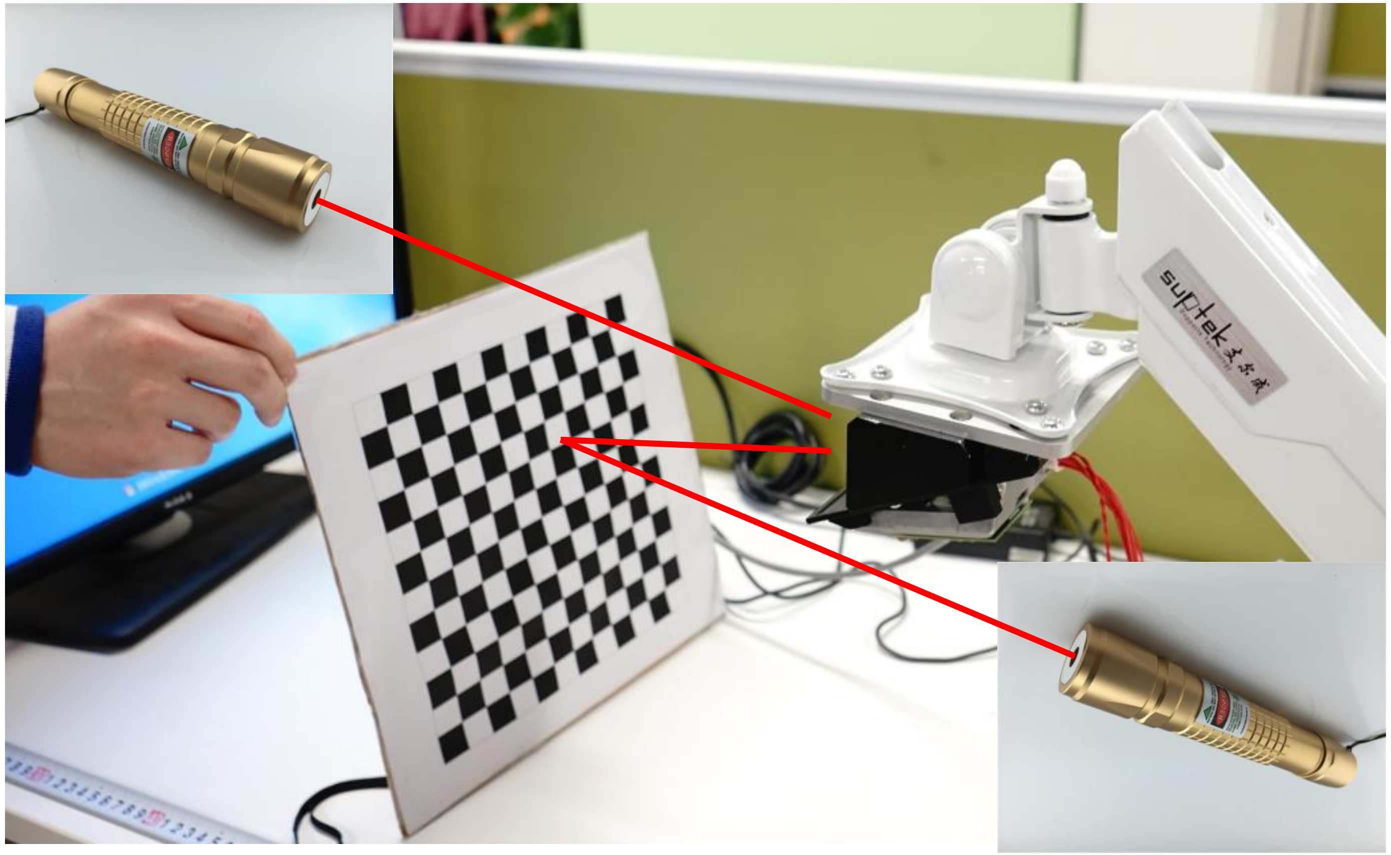
- **Blinding**

Interferers:

- LED spot ($10)
- Laser pointer ($9)
- Infrared LED spot ($11)

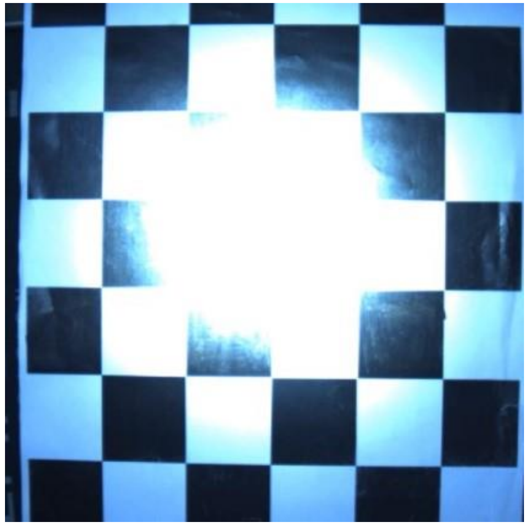
Cameras:

Mobileye, PointGrey



Blinding Cameras – Results with LED spot

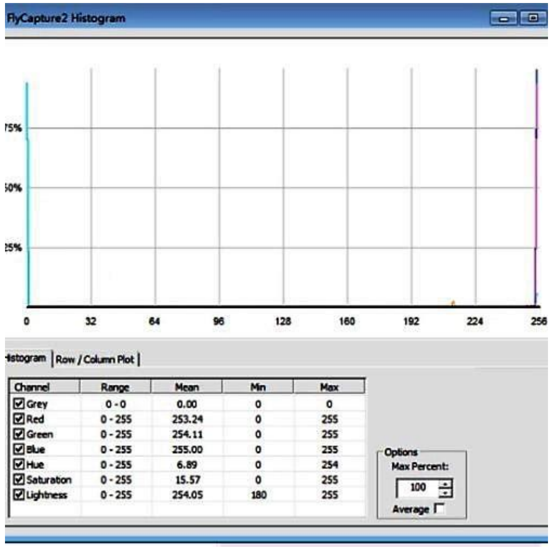
Partial blinding



LED toward the board

Total blinding

LED toward camera



Channel	Range	Mean	Min	Max
☑ Grey	0 - 0	0.00	0	0
☑ Red	0 - 255	253.24	0	255
☑ Green	0 - 255	254.11	0	255
☑ Blue	0 - 255	255.00	0	255
☑ Hue	0 - 255	6.89	0	254
☑ Saturation	0 - 255	15.57	0	255
☑ Lightness	0 - 255	254.05	180	255

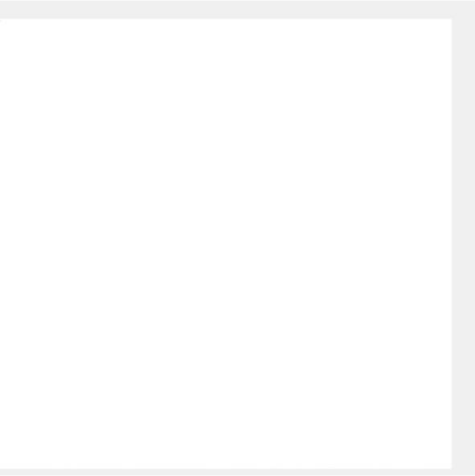
Options
Max Percent: 100
Average □

Tonal Distribution

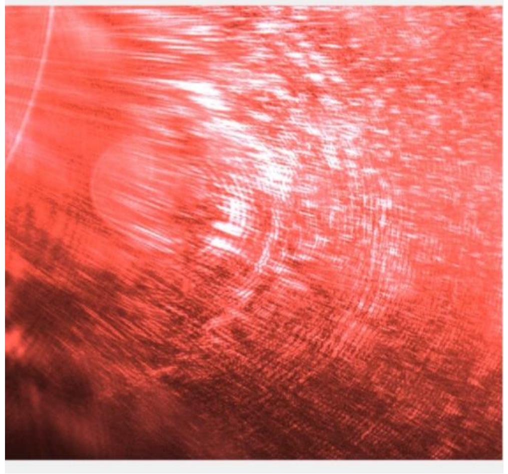
Blinding Cameras – Results with Laser beam

Total blinding

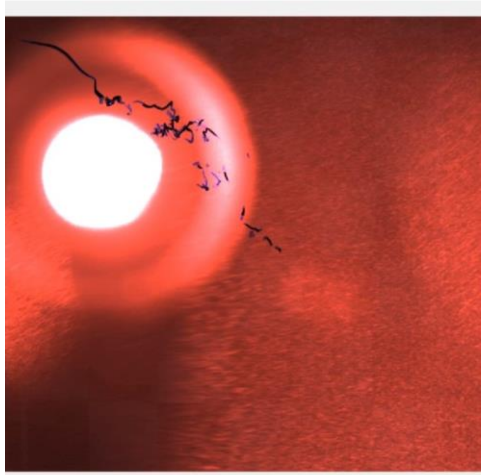
Total blinding



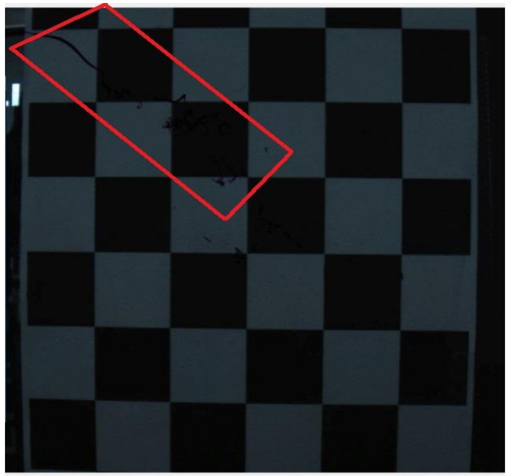
Fixed laser beam



Wobbling laser beam



Damaged



Permanently damaged

Blinding Cameras – Demo with Laser beam

Laser blinds camera.

Response from Tesla

“… We appreciate the hard work you have put into researching potential attacks on sensors used in the Autopilot system. We are currently evaluating your report and investigating the concerns your team has raised so that we can understand if any real world risks have been uncovered …”

Countermeasures

- **Sensor fail safe**
  - Zero or maximum
  - Anomaly detection
- **Sensor redundancy**
  - MIMO system
  - Different types of sensors
- **Sensor data fusion**

What’s next?

- Read more data in vehicular system
- Moving vehicle experiments
- Obtain range and angle measurement
- Increase attack range

Conclusions and Takeaway messages

- **Attacking existing sensors is feasible**
- **The sky is not falling**
- **Sensors should be designed with security in mind**
  - Think about intentional attacks
- **For customers**
  - Don’t trust semi-autonomous cars yet

Will we have fully secure autonomous cars?

Acknowledgements

- **Tongji University**
  - Dr. Xin Bi
- **Keysight Open Laboratory & Solution Center, Beijing**
- **Xpwn Team**
- **USSLab, Zhejiang University**
  - Weibin Jia, Zhou Zhuang, Guoming Zhang
- **ADLAB, AILAB, Qihoo 360**
  - Bin Guo
  - Qiang Chen

同濟大學 TONGJI UNIVERSITY

KEYSIGHT TECHNOLOGIES

XPWN 未来安全 探索盛会 EXPLORATION FOR THE UNKNOWN WORLD

Questions and Answers

Check out our whitepaper!

Jianhao Liu	liujianhao@360.cn
Chen Yan	yanchen@zju.edu.cn
Wenyuan Xu	wyxu@cse.sc.edu