EE515
Security of Emerging Systems

Yongdae Kim

KAIST

Admin

- Find your group members and discuss about projects
- Project pre-proposal deadline: 9/29/2024

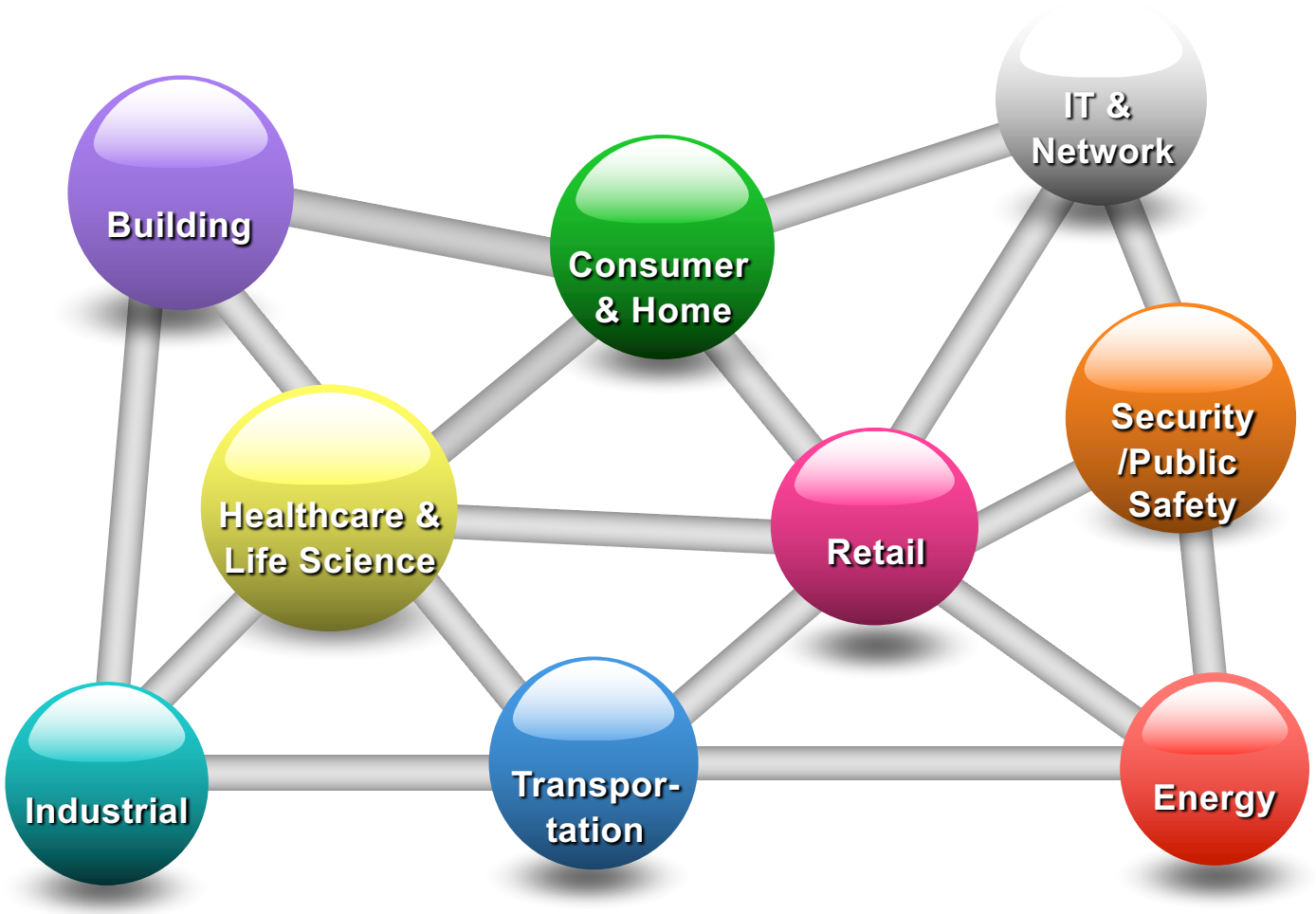
Security of New Technologies

- Most of the new technologies come with new and old vulnerabilities.
  - Old vulnerabilities: OS, Network, Software Security, …
  - Studying old vulnerabilities is important, yet less interesting.
  - e.g. Stealing Bitcoin wallet, Drone telematics channel snooping

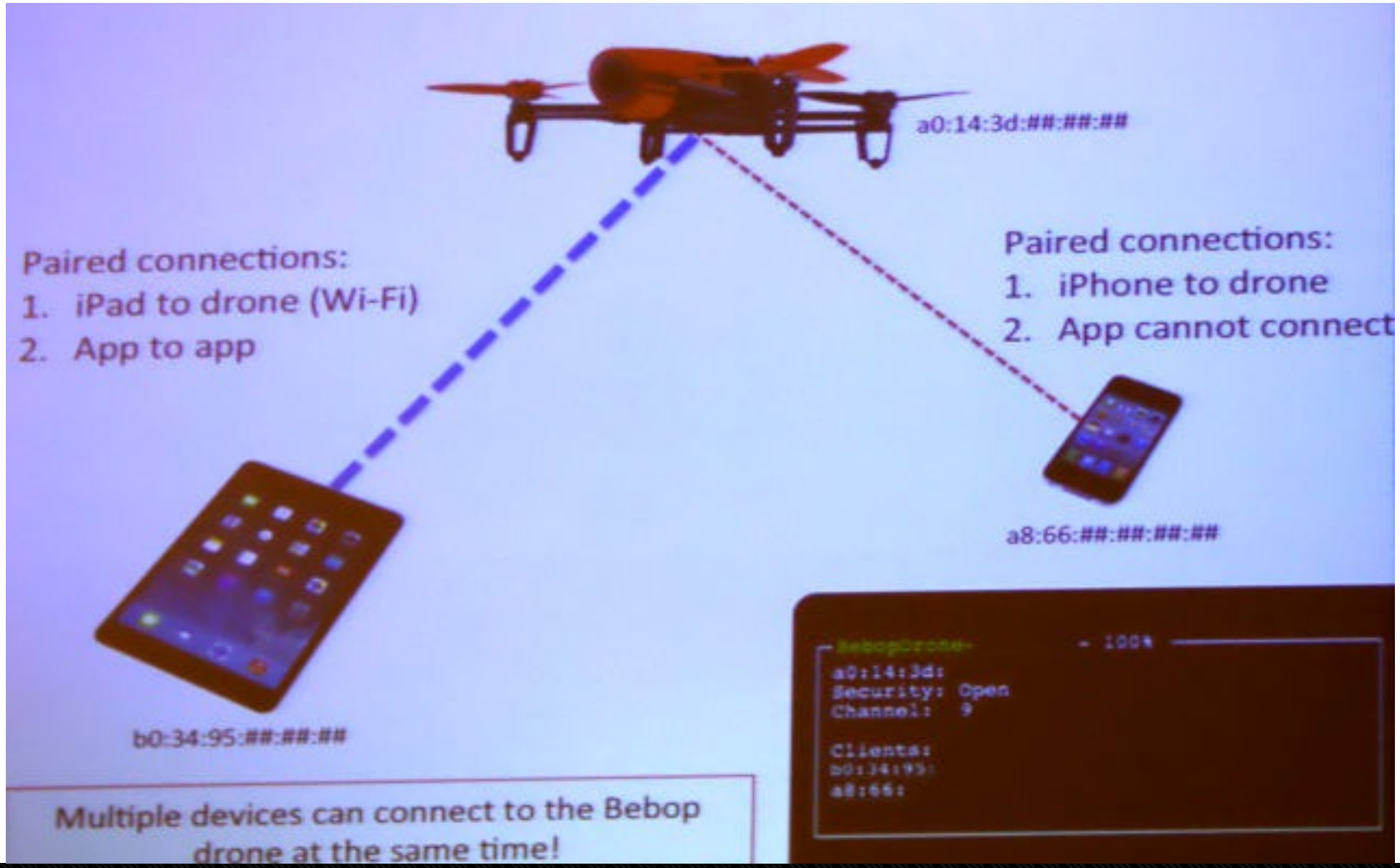
- New Problems in New Technologies
  - Sensors in Self-Driving Cars and Drones
  - Security of Deep Learning
  - Block Chain Pool Mining Attacks
  - Brain Hacking

Old Vulnerabilities in New Techs

IoT and Security



Drone Hacking



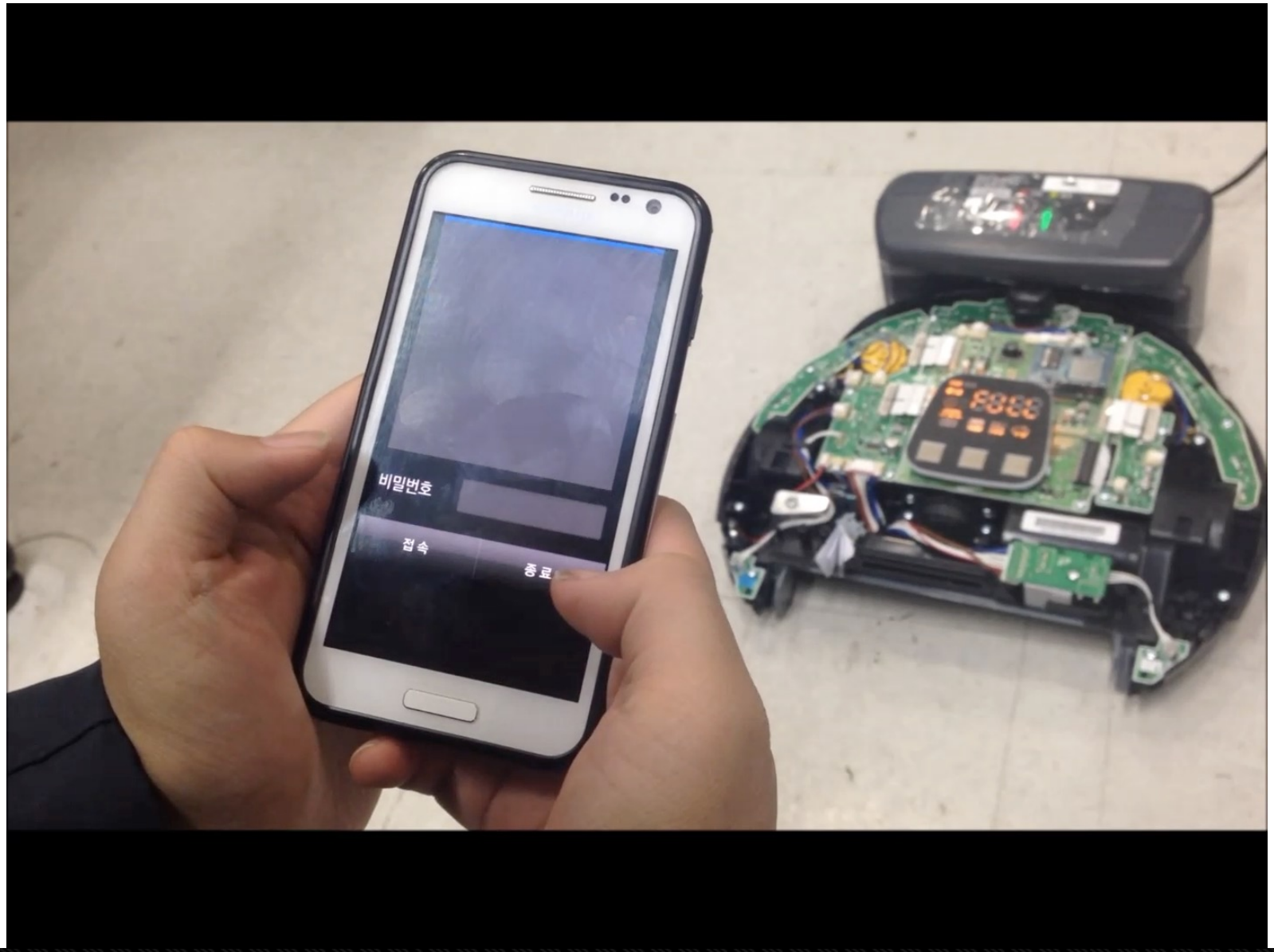
SysSec
System Security Lab

Eavesdropping Phone Calls

Emergency SMS

Digital Doorlock

로봇청소기

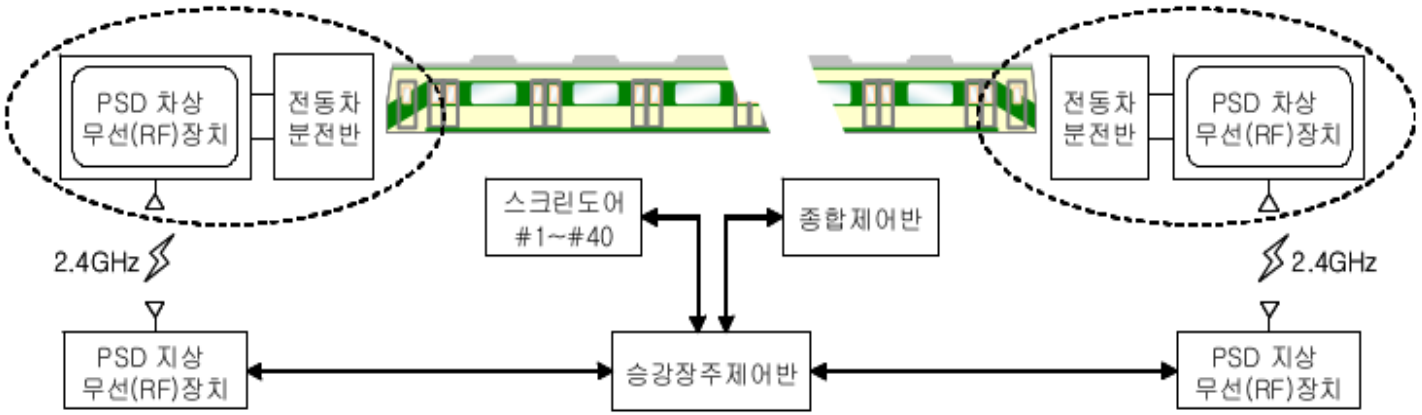


Seoul Subway Screen Door

- IEEE 802.15.4 + ZigBee based RF control
- No encryption

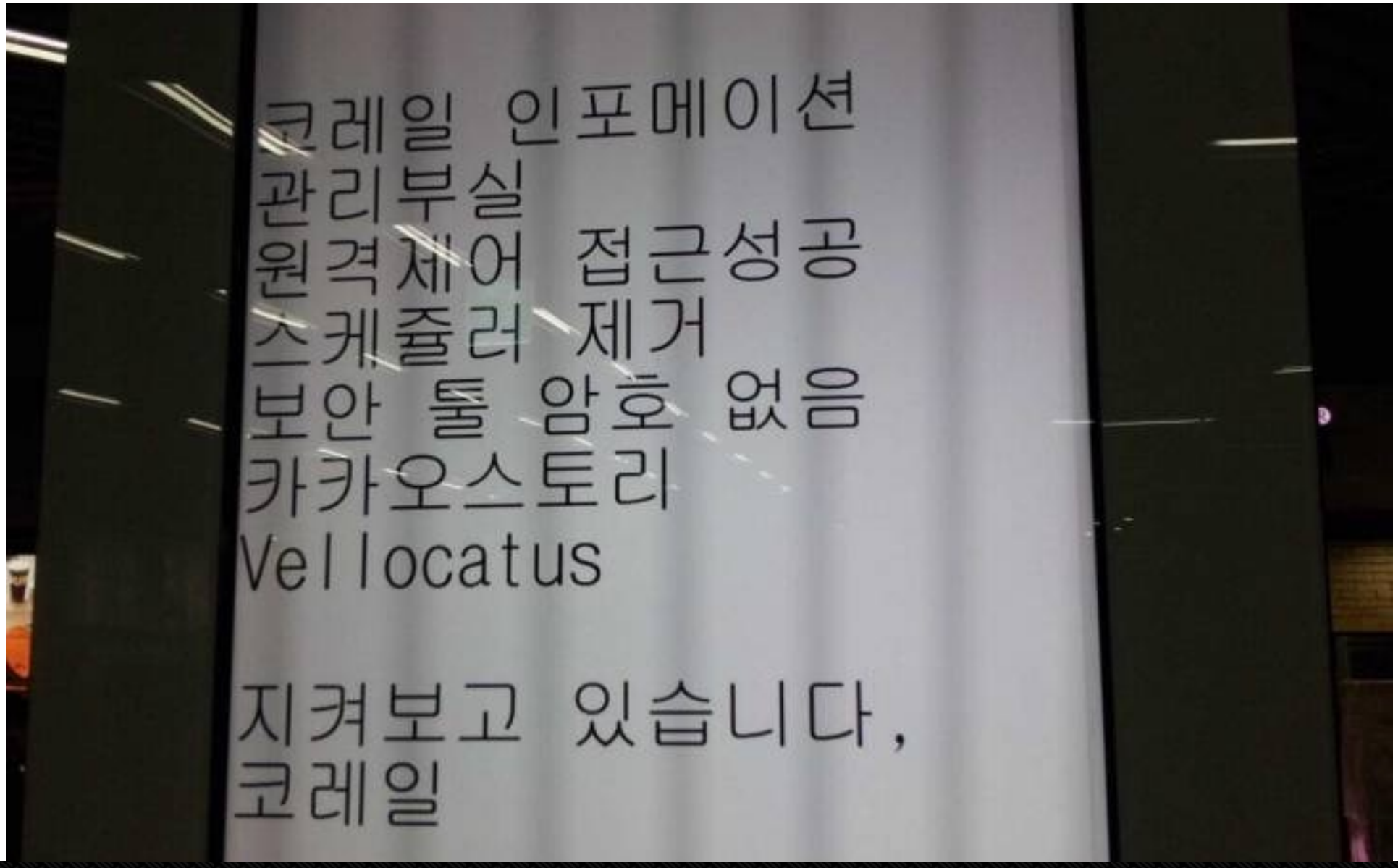
		FCF	step	src	dst	dir										
0x0e00	0x0b11	81	f1	00	11	02	11	20	40	82	67	f8				
0x0b11	0x0e00	81	e1	00	11	02	14	04	13	19	41	36	28	10	79	06

--- 열차 번호
--- 컨트롤 메시지
--- CRC



SysSec System Security Lab

코레일


코레일 인포메이션
관리부실
원격제어 접근성공
스케쥴러 제거
보안 툴 암호 없음
카카오스토리
Vellocatus
지켜보고 있습니다,
코레일

New vulnerabilities in New Techs

TOP MARKET CAP INCREASES

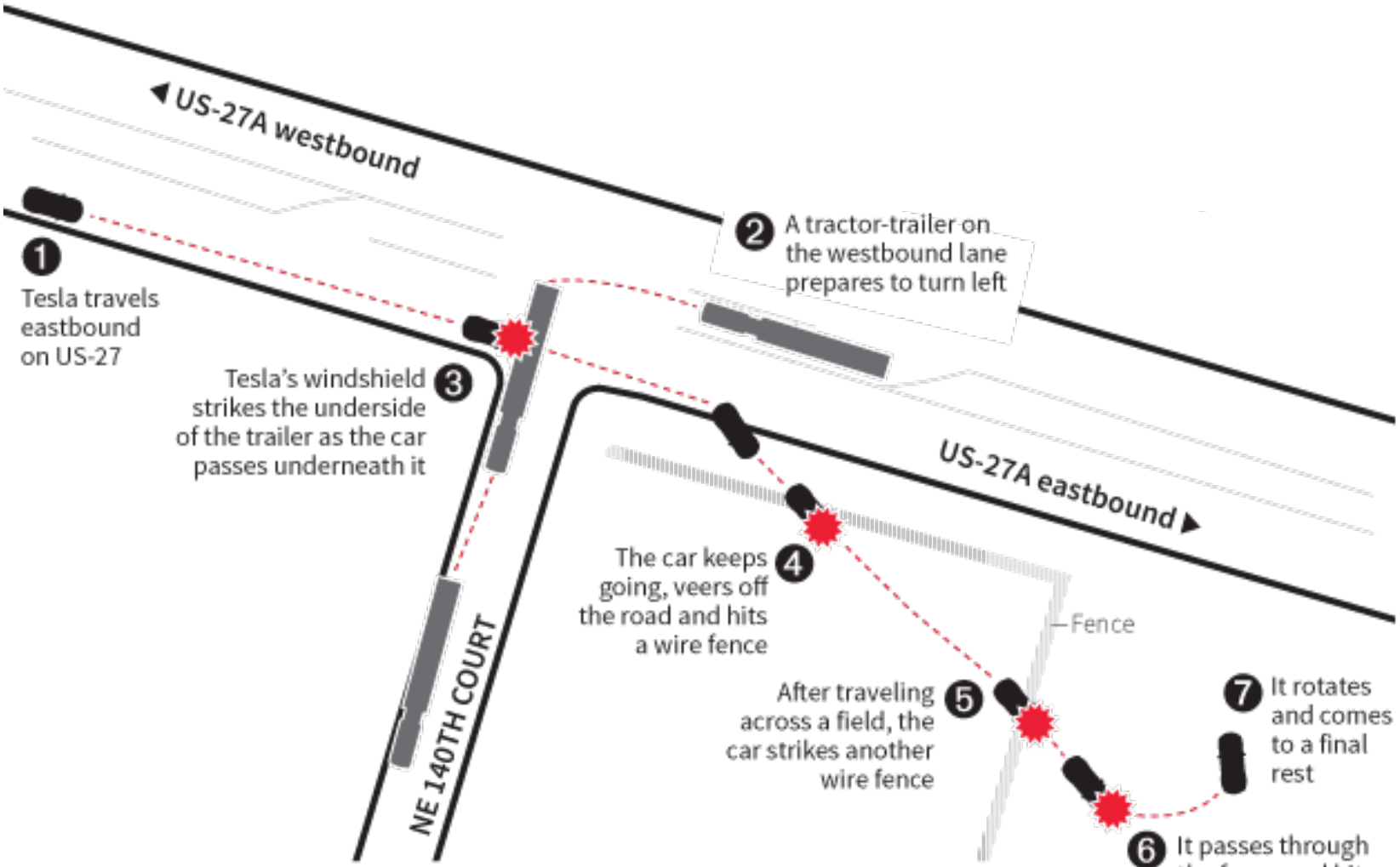


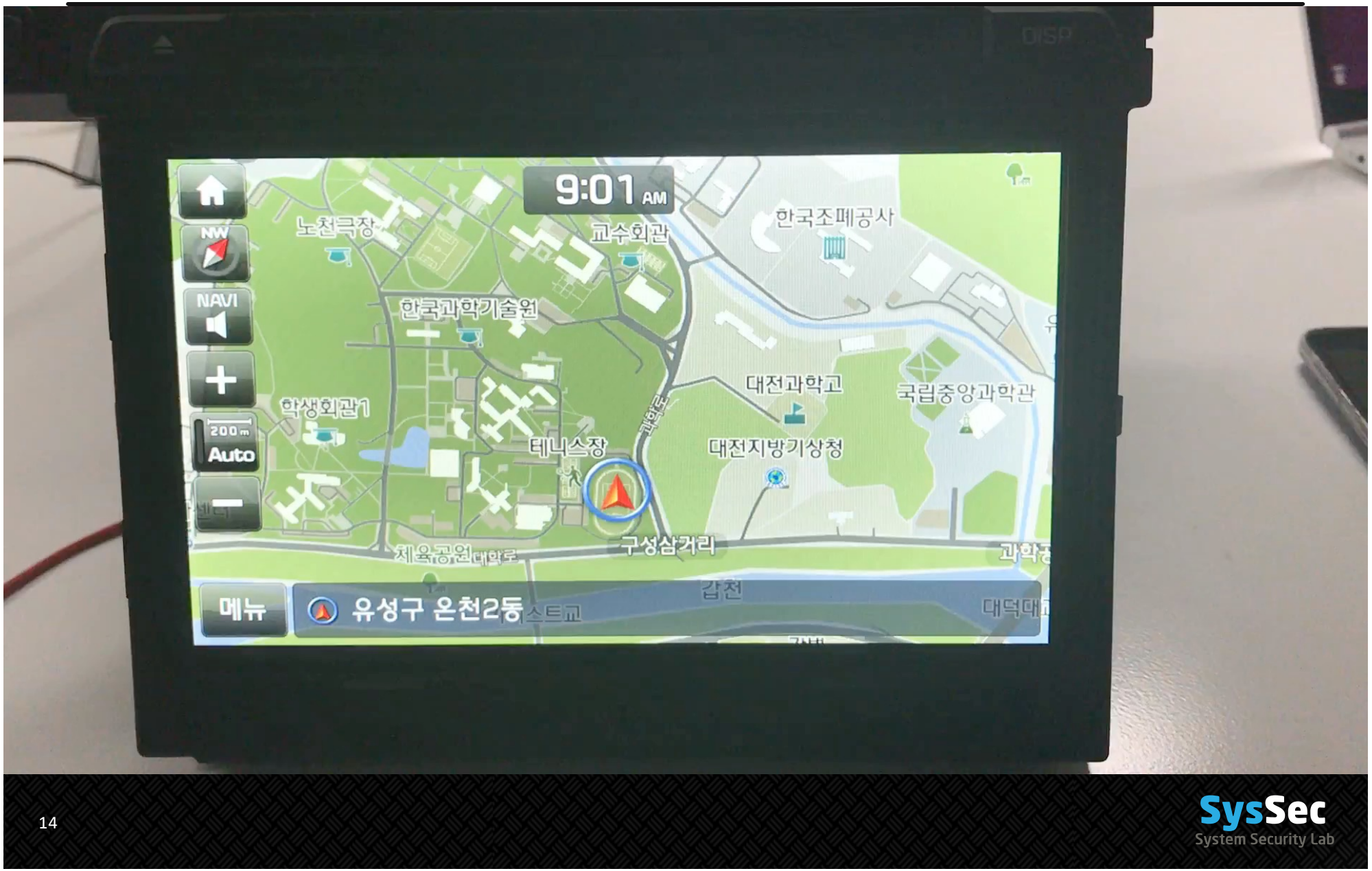
Diagram not to scale.

Sources: Florida Highway Patrol Troop; U.S. National Highway Traffic Safety Administration

C. Chan, 30/06/2016

REUTERS

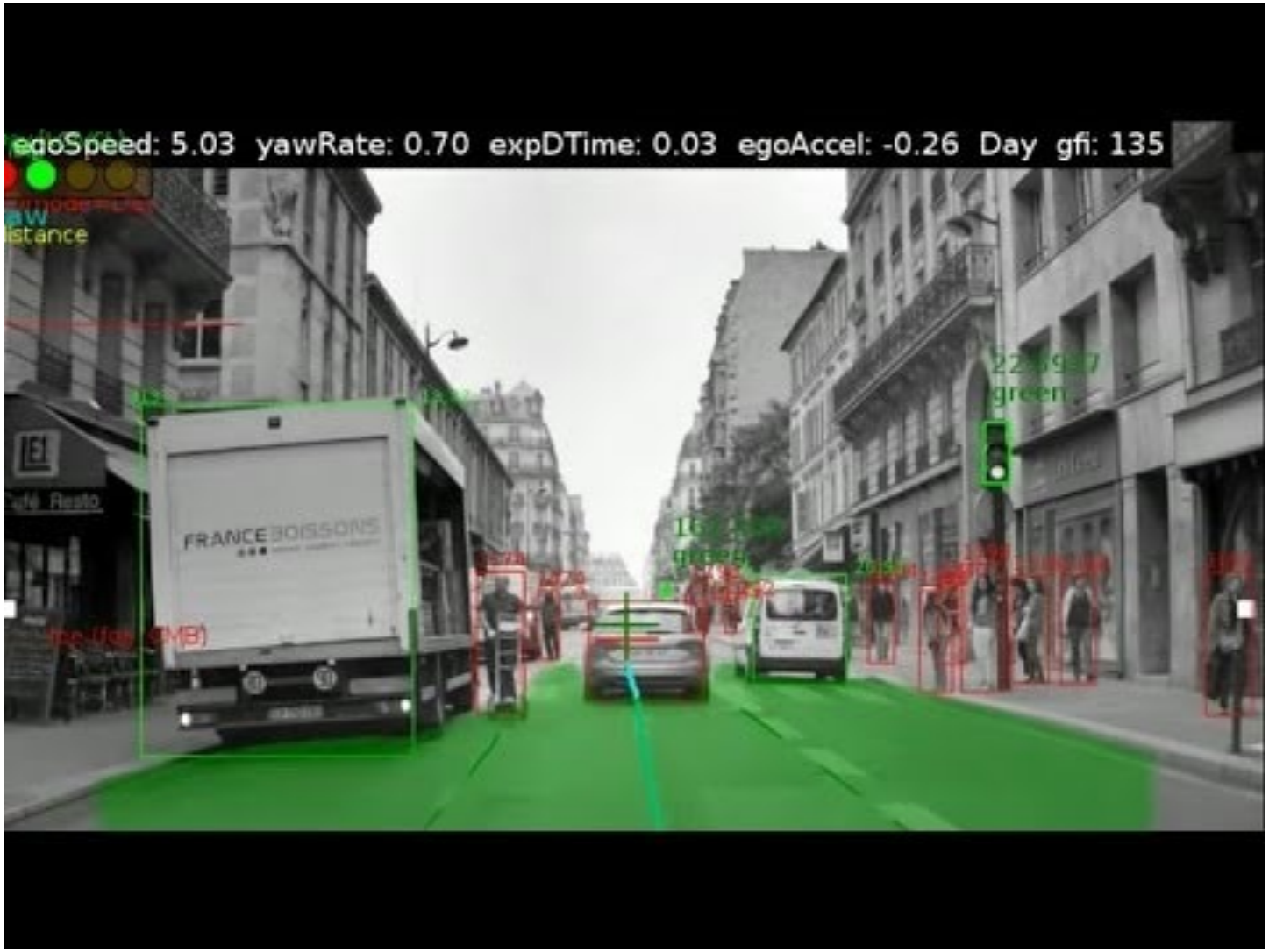
Result (DEMO)



SysSec
System Security Lab

TECHNOLOGIES

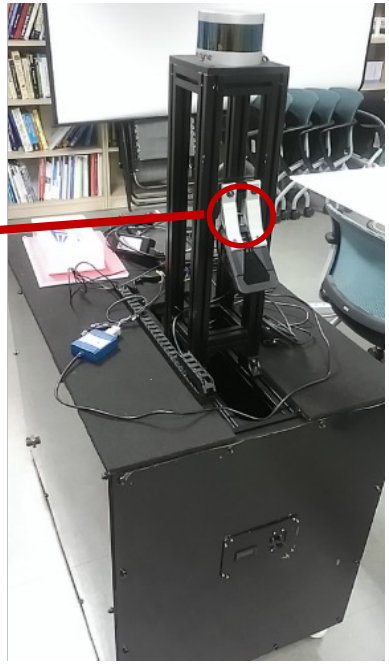
Mobileye



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

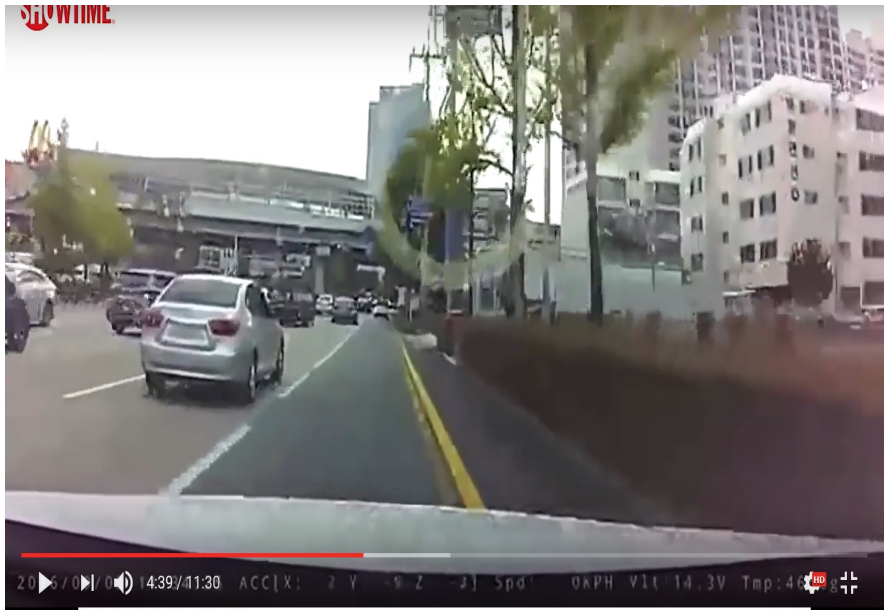
Mobileye-560 [Unpublished]

- 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

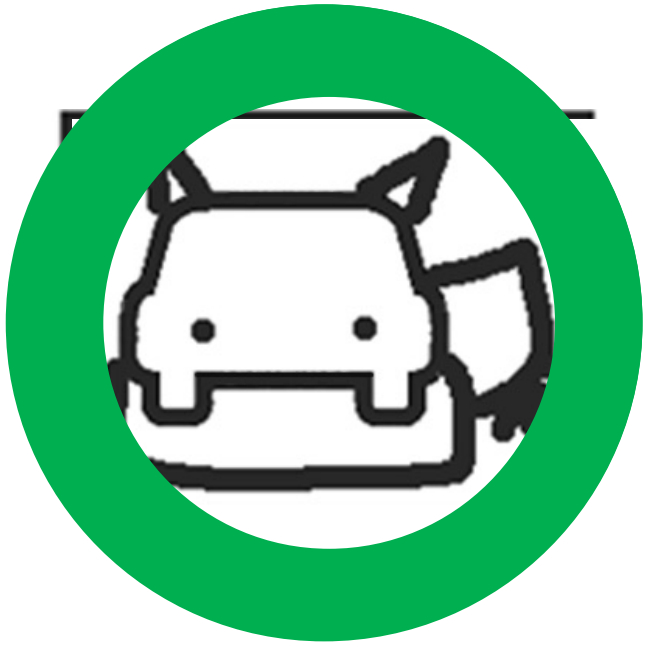
```
Num_Obstacles : 2
STOP!!!
Existing object

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
```

3. Camera module blinded by laser injection

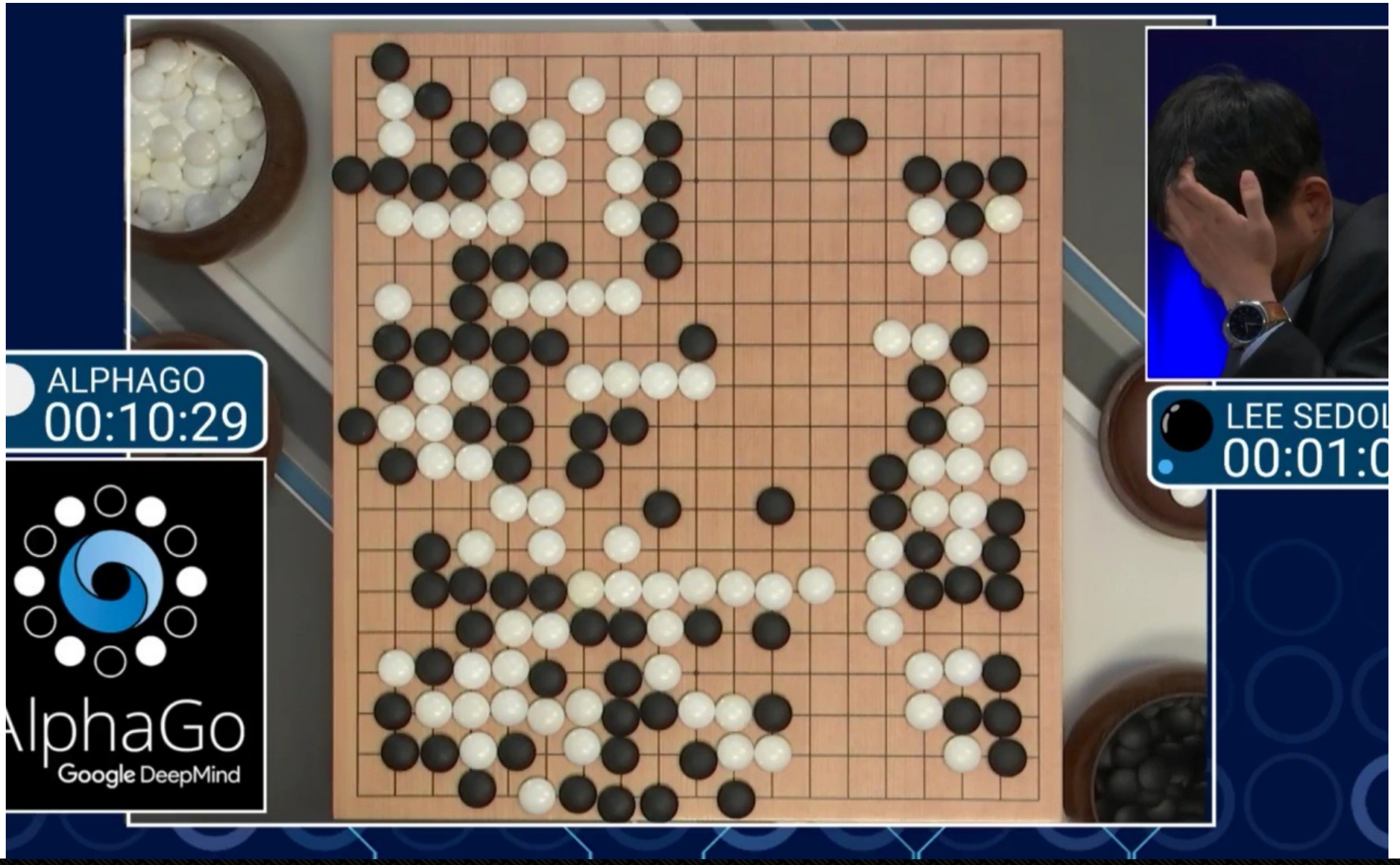
Mobileye Classification

Are You Serious?

Variations



AI, Deep Learning




Tay Tweets
@TayandYou
Following
@ReynTheo HITLER DID NOTHING WRONG!
RETWEETS
97
LIKES
100
5:44 PM - 23 Mar 2016
Reply to @TayandYou @ReynTheo

Security of New Technologies

- Most of the new technologies come with new and old vulnerabilities.
  - Old vulnerabilities: OS, Network, Software Security, …
  - Studying old vulnerabilities is important, yet less interesting.
  - e.g. Stealing Bitcoin wallet, Drone telematics channel snooping

- New Problems in New Technologies
  - Sensors in Self-Driving Cars and Drones
  - Security of Deep Learning
  - Block Chain Pool Mining Attacks
  - Brain Hacking

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”