SECURING THE AUTONOMOUS AUTOMOBILE

SRIDHAR IYENGAR

Vice President, Intel Labs
Intel Corporation

CROSSING CONFERENCE MAY 15-17 2017

LEGAL NOTICES AND DISCLAIMERS

This presentation contains the general insights and opinions of Intel Corporation (“Intel”). The information in this presentation is provided for information only and is not to be relied upon for any other purpose than educational. Use at your own risk! Intel makes no representations or warranties regarding the accuracy or completeness of the information in this presentation. Intel accepts no duty to update this presentation based on more current information. Intel is not liable for any damages, direct or indirect, consequential or otherwise, that may arise, directly or indirectly, from the use or misuse of the information in this presentation.

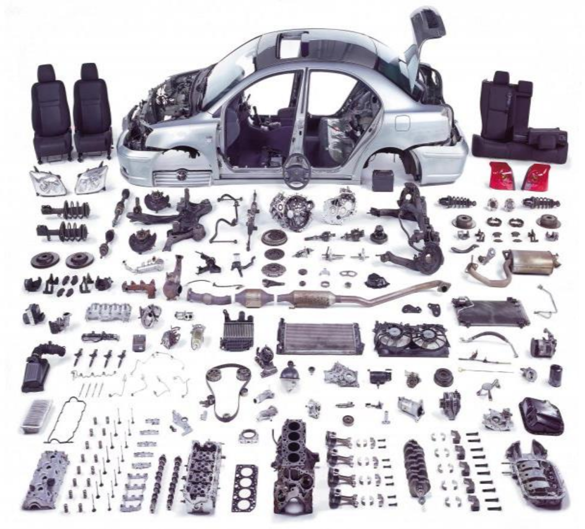
Intel technologies’ features and benefits depend on system configuration and may require enabled hardware, software or service activation. Learn more at intel.com, or from the OEM or retailer.

No computer system can be absolutely secure.

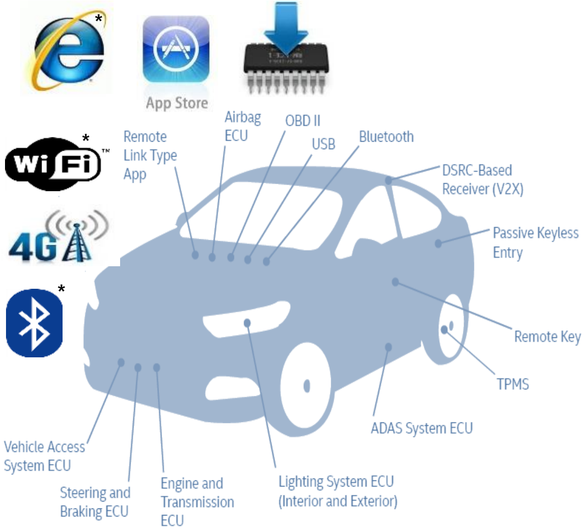
No license (express or implied, by estoppel or otherwise) to any intellectual property rights is granted by this document.

TRANSITION IN COMPLEXITY

Mechanical → Electronic Control Units → Networks → System of Systems

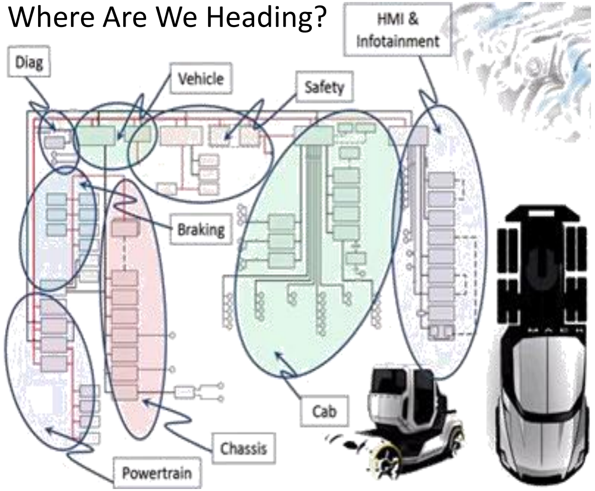


Source: MechanicalEngineering.com



Source: Intel Security

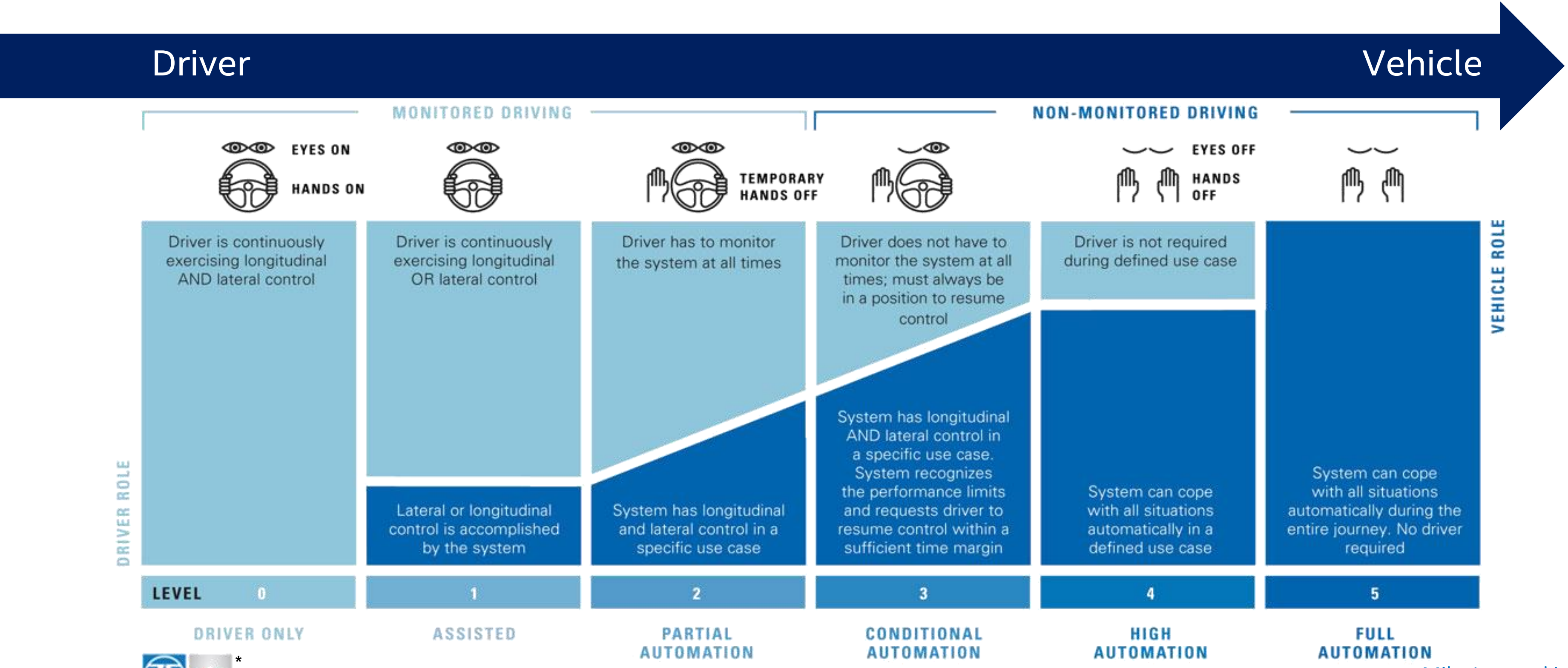
Where Are We Heading?



Source: Volvo

*Other names and brands may be claimed as the property of others

TRANSITION IN RESPONSIBILITY



LEVEL	0	1	2	3	4	5
	MONITORED DRIVING			NON-MONITORED DRIVING		
	EYES ON HANDS ON		TEMPORARY HANDS OFF		EYES OFF HANDS OFF	
DRIVER ROLE	Driver is continuously exercising longitudinal AND lateral control	Driver is continuously exercising longitudinal OR lateral control	Driver has to monitor the system at all times	Driver does not have to monitor the system at all times; must always be in a position to resume control	Driver is not required during defined use case	
VEHICLE ROLE		Lateral or longitudinal control is accomplished by the system	System has longitudinal and lateral control in a specific use case	System has longitudinal AND lateral control in a specific use case. System recognizes the performance limits and requests driver to resume control within a sufficient time margin	System can cope with all situations automatically in a defined use case	System can cope with all situations automatically during the entire journey. No driver required
	DRIVER ONLY	ASSISTED	PARTIAL AUTOMATION	CONDITIONAL AUTOMATION	HIGH AUTOMATION	FULL AUTOMATION

ZF TRW *

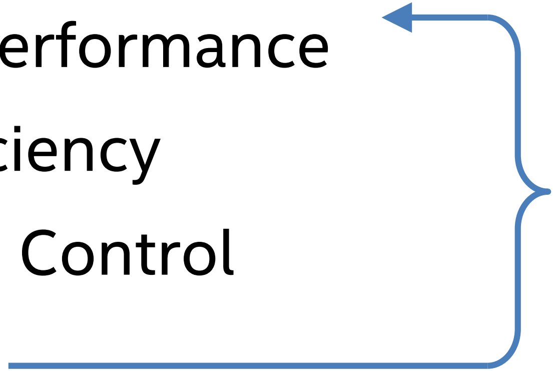
*Other names and brands may be claimed as the property of others

Mike Lemanski

CROSSING CONFERENCE 2017

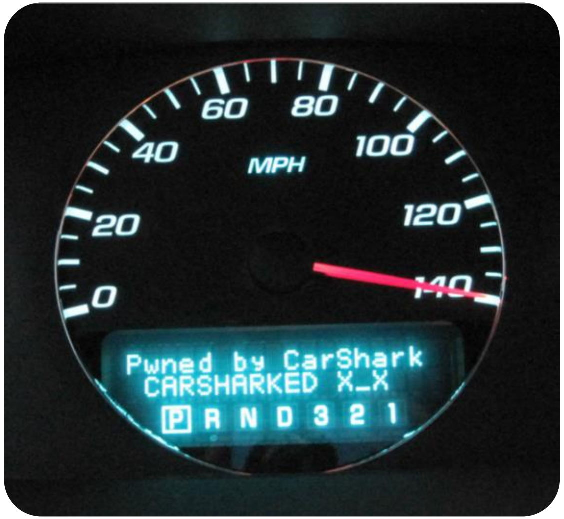
WHAT IS DRIVING THESE TRANSITIONS?

1. Safety
2. Engine Performance
3. Fuel Efficiency
4. Emission Control
5. Security

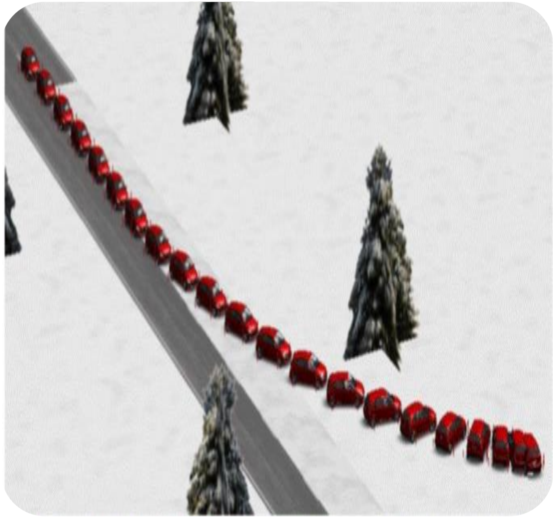


Is it time for a transition in priority?

AUTOMOBILES MAKE ATTRACTIVE TARGETS



Oakland 2010



CHES 2013

BlackHat 2015, 2016

Experimental Security Analysis of a Modern Automobile, Kosher et al, 2010
Non-invasive Spoofing Attacks for anti-lock braking systems, Shoukry at al, 2013

WHAT MAKES AUTOMOBILES SO VULNERABLE?

The Number of ECUs Have Increased Over Time

Infiniti*	**11** in 2006	**34** in 2014
Jeep*	**7** in 2010	**17** in 2014
Ranger Rover*	**41** in 2010	**98** in 2014
Toyota Prius*	**23** in 2006	**40** in 2014

Source: A Survey of Remote Automotive Attack surfaces, by Miller & Valasek

*Other names and brands may be claimed as the property of others

Large Threat Surface

- ~100 M lines of code

Physical Access

- OBD-II ports, USB, disc, iPod with access to internal networks

Short and Long-Range Wireless Access

- Bluetooth, Remote keyless entry, Tire Pressure Monitor, GPS, Cellular all exploitable

Open Internal Networks, Open Protocols

- CAN bus is unencrypted, easy to spoof, lack of authentication

Not Designed With A Malicious Adversary In Mind

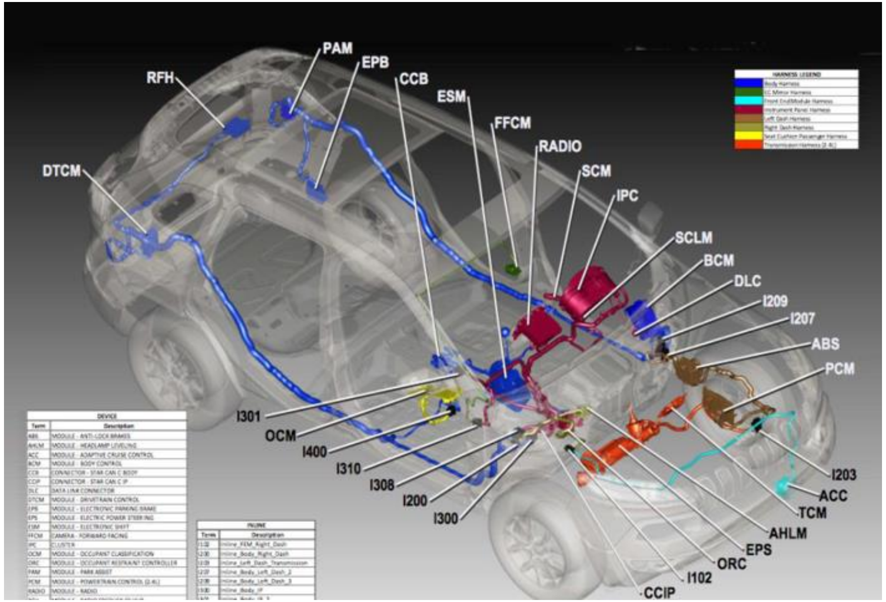
HOW TO SECURE THE AUTONOMOUS AUTOMOBILE?

SECURE THE PLATFORM

SECURE THE COMMUNICATION

SECURE THE ANALYTICS

CONTROLLER AREA NETWORK (CAN) BASICS


PAM
EPB
RFH
CCB
ESM
FFCM
RADIO
SCM
IPC
DTCM
SCLM
BCM
DLC
I209
I207
ABS
PCM
I301
OCM
I400
I310
I308
I200
I300
I203
ACC
TCM
AHLM
EPS
ORC
I102
CCIP
HARNESS LEGEND
Body Harness
IC Mirror Harness
Front End Module Harness
Instrument Panel Harness
Left Dash Harness
Right Dash Harness
Seat Cushion Passenger Harness
Transmission Harness (2.4L)
DEVICE
Term
Description
ABS MODULE - ANTI-LOCK BRAKES
AHLM MODULE - HEADLAMP LEVELING
ACC MODULE - ADAPTIVE CRUISE CONTROL
BCM MODULE - BODY CONTROL
CCB CONNECTOR - STAR CAN C BODY
CCIP CONNECTOR - STAR CAN C IP
DLC DATA LINK CONNECTOR
DTCM MODULE - DRIVETRAIN CONTROL
EPB MODULE - ELECTRONIC PARKING BRAKE
EPS MODULE - ELECTRIC POWER STEERING
ESM MODULE - ELECTRONIC SHIFT
FFCM CAMERA - FORWARD FACING
IPC CLUSTER
OCM MODULE - OCCUPANT CLASSIFICATION
ORC MODULE - OCCUPANT RESTRAINT CONTROLLER
PAM MODULE - PARK ASSIST
PCM MODULE - POWERTRAIN CONTROL (2.4L)
RADIO MODULE - RADIO
INLINE
Term
Description
I102 Inline_FEM_Right_Dash
I200 Inline_Body_Right_Dash
I209 Inline_Left_Dash_Transmission
I207 Inline_Body_Left_Dash_2
I208 Inline_Body_Left_Dash_3
I300 Inline_Body_IP

CAN-C Network 2014 Jeep Cherokee

Source: A Survey of Remote Automotive Attack surfaces, by Miller & Valasek

In-car Fabric That Connects The ECUs

Simple Packet Format

Broadcast To All ECUs

Simple Priority Based Arbitration

Gateways Route Data Between Buses

WHAT CAN POSSIBLY GO WRONG?

Easy to Spoof an ECU

- No Authentication Field

Easy to Snoop

Easy to Inject & Send Packets to Any ECU

Trivial Denial-of-Service Attacks

Weak Access Controls

- ECU Firmware Upgrade and Diagnostic Service Easily Exploitable

Identifier (ID) 11 bits 0x0 -0X7FF 29 bits (0x0v-0x1FFFFFFF)	Data Length Code (DLC) 4 bits	Data Up to 8 bytes Length Specified by DLC

Simple CAN message format

```
While (1) {
 send_message_with_id_0():
}
```

DoS attack with message ID = 0

Source: Hopping on the CAN bus, BlackHat Asia 2015, Eric Evenchick

THE INDUSTRY RESPONDS

SAE J3061 – Cybersecurity Guidebook For Cyber-physical Vehicle Systems

a) Enumerate All Attack Surfaces And Conduct Threat Analysis
b) Reduce Attack Surface
c) Harden Hardware And Software
d) Security Testing (Penetration, Fuzzing, Etc.)

SAE J3101 – Hardware-protected Security For Ground Vehicle Applications

a) Secure Boot
b) Secure Storage
c) Secure Execution Environment
d) Secure Debug, Many Other Hardware Capabilities…
e) OTA Software Authentication, Detection, And Recovery Mechanisms

Apply the Lessons of the PC Ecosystem!

HOW TO SECURE THE AUTONOMOUS AUTOMOBILE?

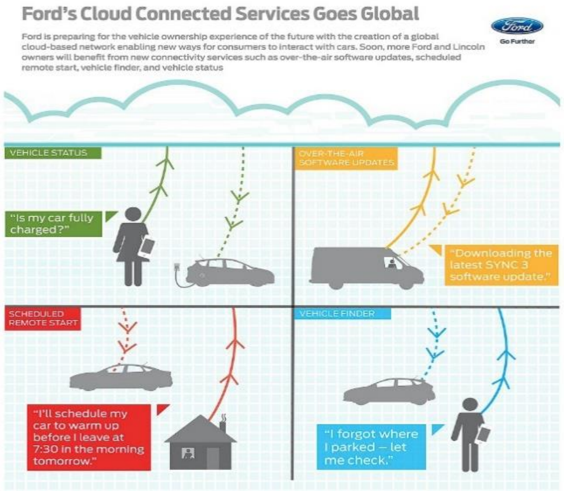
SECURE
THE
PLATFORM

SECURE
THE
COMMUNICATION

SECURE
THE
ANALYTICS

WIRELESS COMMUNICATION ENABLES NEW USAGES

Vehicle to Cloud



Ford's Cloud Connected Services Goes Global

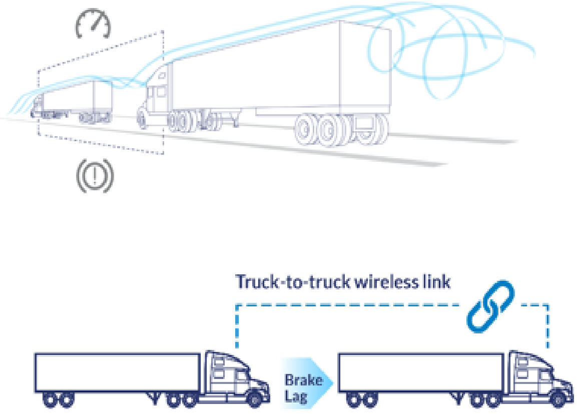
Ford is preparing for the vehicle ownership experience of the future with the creation of a global cloud-based network enabling new ways for consumers to interact with cars. Soon, more Ford and Lincoln owners will benefit from new connectivity services such as over-the-air software updates, scheduled remote start, vehicle finder, and vehicle status

Ford
Go Further
VEHICLE STATUS
"Is my car fully charged?"
OVER-THE-AIR SOFTWARE UPDATES
"Downloading the latest SYNC 3 software update."
SCHEDULED REMOTE START
"I'll schedule my car to warm up before I leave at 7:30 in the morning tomorrow."
VEHICLE FINDER
"I forgot where I parked – let me check."

Telematics
Over The Air Update
Vehicle Finder

Source: ExtremeTech, March 2015

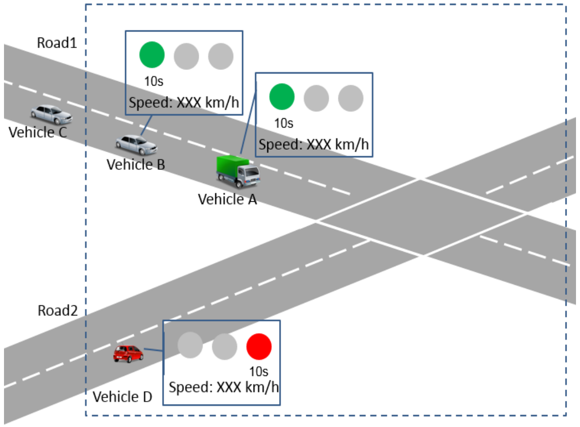
Vehicle to Vehicle



Platooning
Traffic Management
Accident Report

Source: Peloton-tech.com

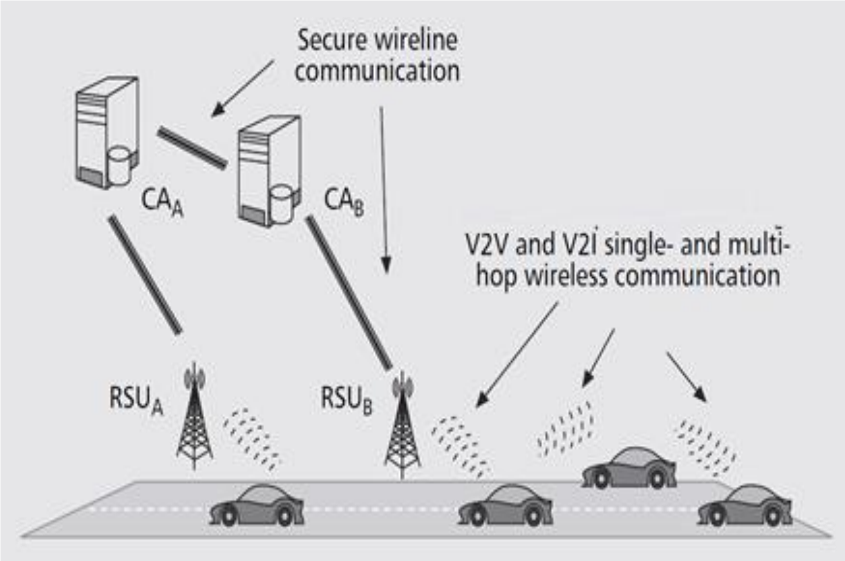
Vehicle to Infrastructure



Traffic Flow Optimization
Automatic Toll
Traffic Violations

Source: 3GPP TR22885

… BUT OPENS UP NEW ATTACKS


Secure wireline communication
CA$_A$
CA$_B$
V2V and V2I single- and multi-hop wireless communication
RSU$_A$
RSU$_B$

Abstract View Of Secure Vehicular Communication

Source: Secure Vehicular Communications Systems, by Papadimitratos et al

Forge Location by GPS Spoofing

- $300 SDR To Spoof GPS @Defcon 2015

DoS Attack By Jamming Communications

- Lose Critical Info From Platoon Leader

Forge, Inject or Replay Messages

- Masquerade as an Emergency Vehicle

Privacy Leak Via Recording Safety Beacons

- Monitor Vehicle's Locations To Infer Private Info

Collusion Attacks By Multiple Compromised Roadside Units

- Report Imaginary Events, e.g. Traffic Jam

IS DSRC THE ANSWER?

Dedicated Short Range Communications Enables Direct V2V

- Promoted By USDOT, IEEE Protocol 1609.2 in the 5.9GHz Band defines the security protocol
- Obstacles To Adoption: Cost, Interoperability, Interference, Scalability
- Biggest Obstacle: Security!
  - Public-key Crypto Is Computationally Expensive, Poorly Suited For Embedded Processor
  - Lack of Anonymity. DSRC is Inherently A Vehicle Tracking System
  - Poor Support For Revocation. No Key-rollover, Certificate Revocation List

Opens The Door for 5G!

- Many Car Companies Embedding Cellular Wireless Connectivity Anyway
- Integrate Low Latency Device-to-device And Mobile Edge Computing Capabilities For V2V
- Leverage 3GPP, ETSI Security Standards

Security is Critical for Any V2V Standard

DSRC Security Framework Analysis, by Walker, et al, Intel Labs, June 2013
Cellular vs DSRC for V2V: Why-fi in a Car? by Lanctot, Strategy Analytics, Nov 2015

HOW TO SECURE THE AUTONOMOUS AUTOMOBILE?

SECURE
THE
PLATFORM

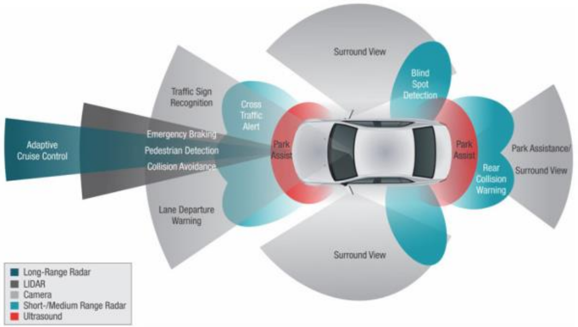
SECURE
THE
COMMUNICATION

SECURE
THE
ANALYTICS

WHAT DRIVES AUTONOMOUS DRIVING?

SENSE THE ENVIRONMENT

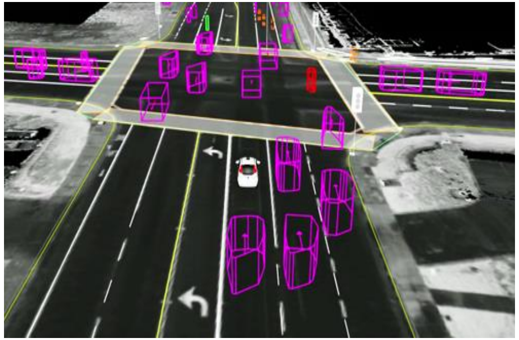
Camera, Radar, LIDAR, Ultrasound



Source: Lichaoma.com, Malcom’s Technical Blog

MAP YOUR LOCATION

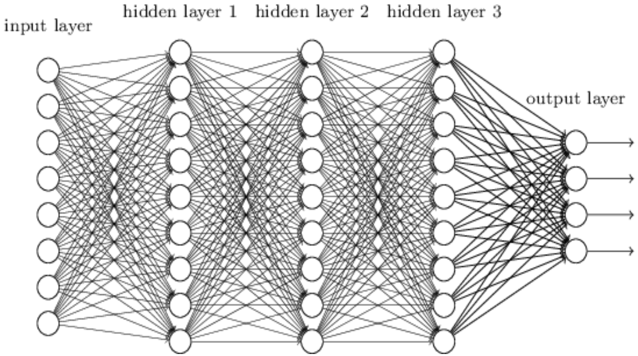
Hi-res Maps, 3D Models



Source: Chris Urmson: How a driverless car sees the road

PLAN NEXT STEPS

Deep Neural Nets



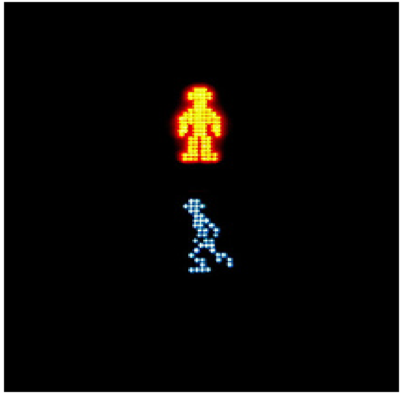
Source: Quora.com

DEEP NEURAL NETS CAN BE FOOLED

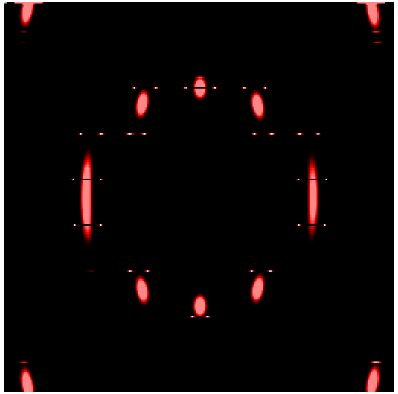
Evolution Attacks: When randomness is classified as information

DNN Recognizable, Human Unrecognizable

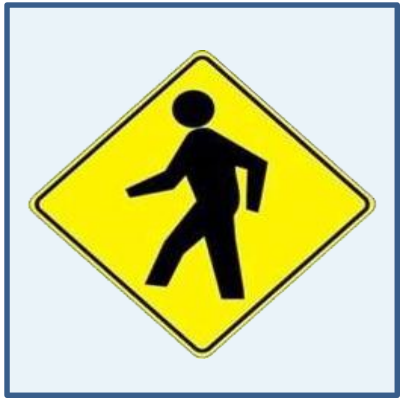
DNN:
Same as this Traffic Sign!



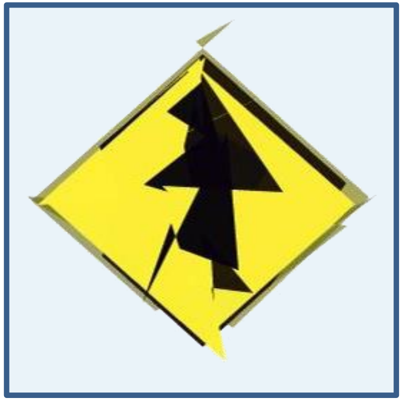
Human:
Unrecognizable



DNN:
Same as this Traffic Sign!



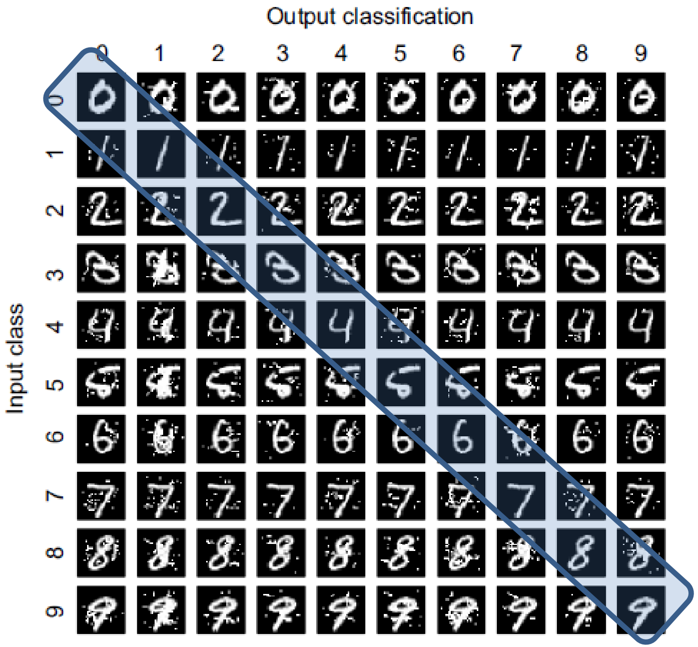
Human:
Unrecognizable



DEEP NEURAL NETS CAN BE FOOLED

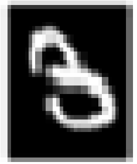
Causative Attacks: When twins are classified as different

DNN Unrecognizable, Human Recognizable

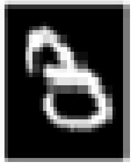


Source: The Limitations of Deep Learning in Adversarial Settings, Papenot, et al, 2016

Human: “3”



DNN: “8”



Modifying 4% of features causes the DNN to misclassify with 97% success rate

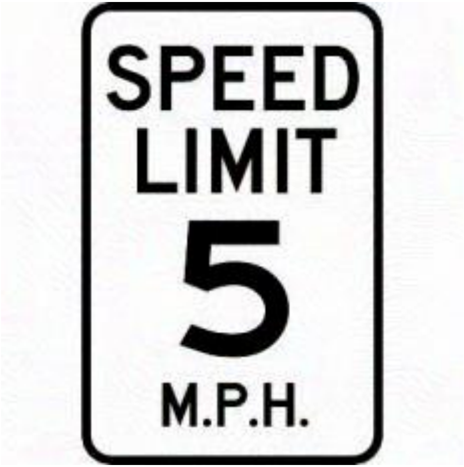
It would take minor changes to confuse these two signs!

ANOTHER VARIATION

Causative Attacks: When twins are classified as different

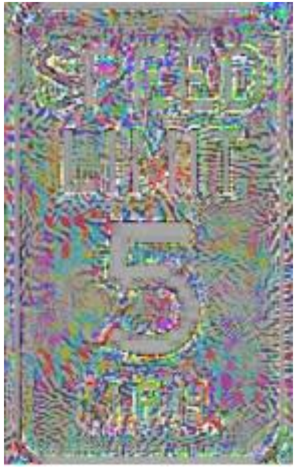
DNN Unrecognizable, Human Recognizable

Human: “Speed Limit Sign”
DNN: “Speed Limit Sign”



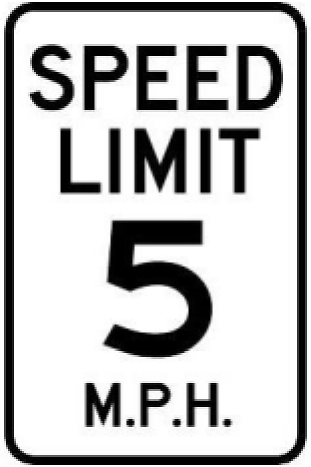
+

Error: Small
variations in intensity



=

Human: “Speed Limit Sign”
DNN: “Ruler”

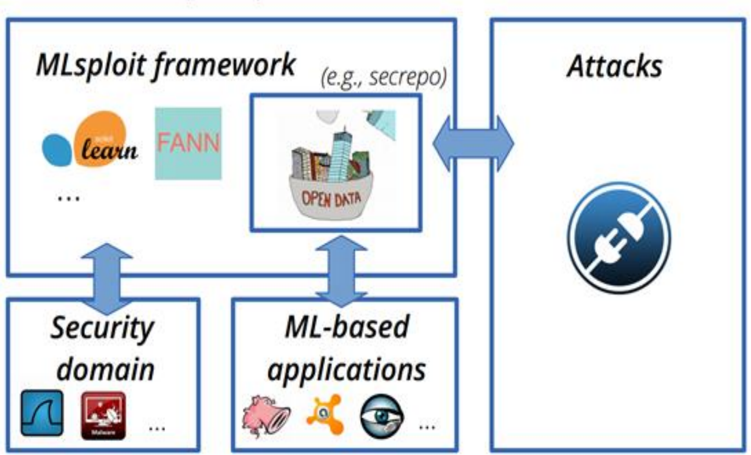


Source: Intel Labs, based on Explaining and Harnessing Adversarial Examples, by Goodfellow, et al, Google

INTEL FUNDED ACADEMIC RESEARCH

Adversary Resilient Security Analytics
Intel + Georgia Tech (ISTC-ARSA)

Mlsploit: Framework for evaluating and improving the resiliency of ML based security applications



Collaborative Autonomous Resilient Systems
Intel + EU Academia (ICRI-CARS)

RFP: Proposals in the area of security, privacy and safety of collaborative autonomous systems

- Autonomous Behavior
- Safety and Resilience
- Security and ML
- Systems Security
- Hardware Security

Need more research in Adversarial Analytics

WRAP UP

- Autonomous Driving Is In Its Early Days
- Shift In Complexity And Responsibility Makes Vehicles Vulnerable To Attacks
- Learn From The PC Ecosystem, Invest in Security Standards, Research in Adversarial Analytics
- Increased Security = Increased Safety

THANK YOU.