

# Comprehensive Experimental Analyses of Automotive Attack Surfaces

2018.9.27  
Hyunki kim

- **Hyunki Kim** S. Checkoway, D. McCoy, Roesner, and T. Kohno, "Comprehensive Experimental Analyses of Automotive Attack Surfaces", CCS'18
- **R1 Shuxuan Zhou** Kyong-Tak Cho and G. Roesner, "Automotive Attack Surfaces are More Vulnerable", CCS'16
- **R2 Byungkyu Lee** M. Contag and G. Roesner, "How They Did It: An Analysis of Emis...

Authors: **Stephen Checkoway**, Damon McCoy, Brian Kantor,  
Danny Anderson, Hovav Shacham, Stefan Savage, (UCSD)  
Karl Koscher, Alexei Czeskis, Franziska Roesner, and Tadayoshi Kohno (UW)

**KAIST**

Written by Sanha Park

# Intro

CAR HACKING JUST GOT REAL



# Intro

❖ Jeep Cherokee hacked in 2015



**CHARLIE MILLER**

SECURITY ENGINEER, TWITTER

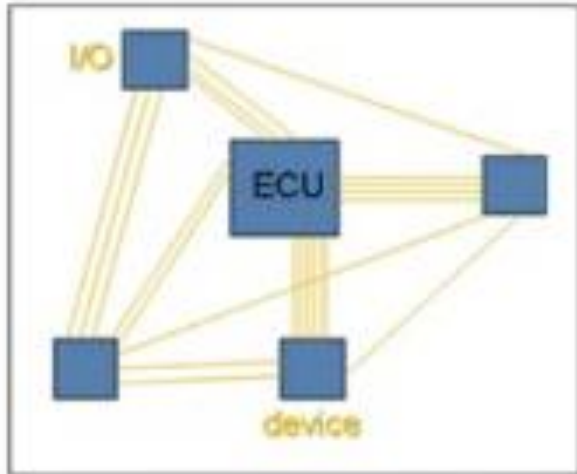
**CHRIS VALASEK**

DIRECTOR OF VEHICLE SAFETY RESEARCH, IOACTIVE

# Why can we attack?



Without CAN



1980's

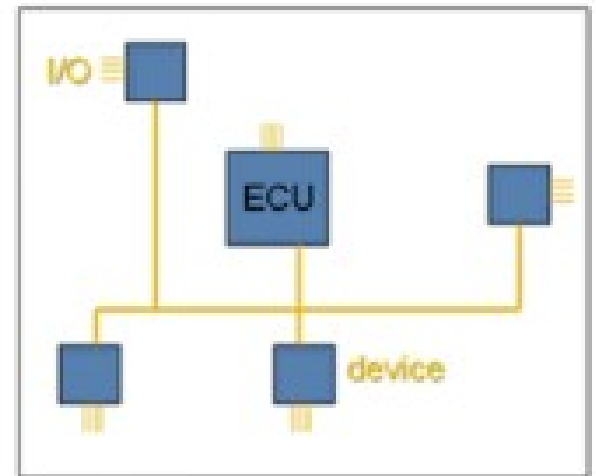


Today



©2001 HowStuffWorks

With CAN



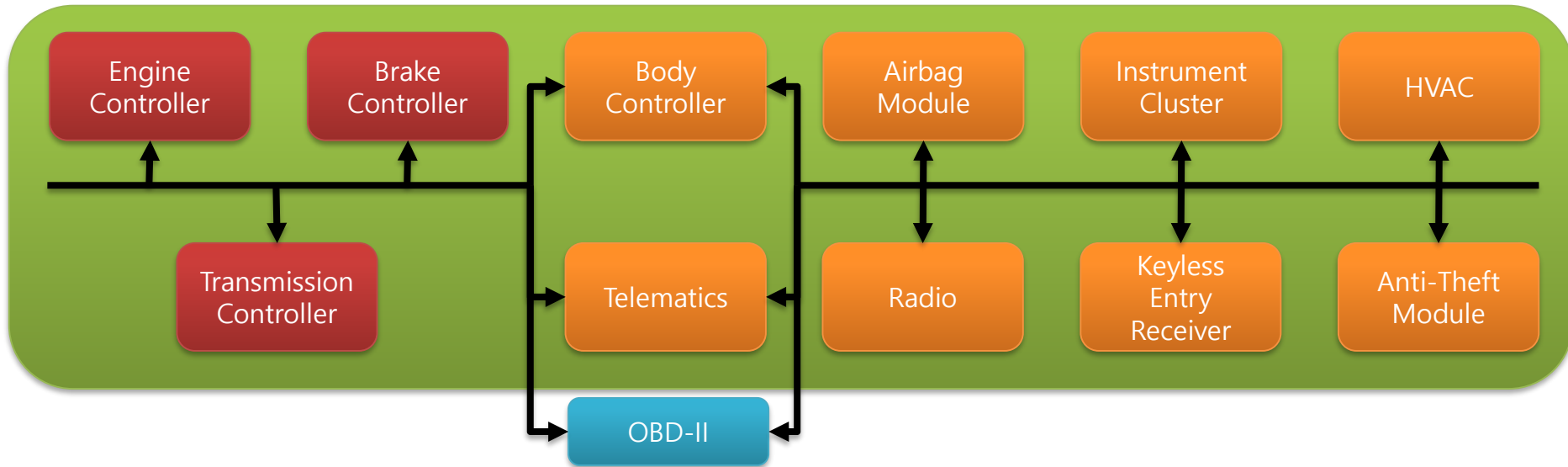
# Why can we attack?

MOTHERBOARD

PART 2

# REMOTE CONTROLLED

# Cars' system



- ❖ ECU(Electronic Control Unit) :
  - Ubiquitous computer controller
- ❖ ECU interconnection driven by safety, efficiency, and capability requirements
- ❖ But, also has some fatal shortcomings

# Oakland 2010, they showed...

- ❖ Safety-critical systems can be compromised
  - Selectively enable/disable brakes
  - Stop engine
  - Control lights
- ❖ Owning one ECU = total compromise
- ❖ ECUs can be reprogrammed (while driving!)
  
- ❖ Limit: Need physical access

[Oakland'10] koscher et al. Experimental Security Analysis of a Modern Automobile.

# Threat model

- ❖ Technical (theoretical) Capabilities
  - Capabilities in analyzing the system
  - Focuses on making technical capabilities realistic
- ❖ Operational (real-time) capabilities
  - Show how malicious payload is delivered
  - Attack vector
    - Indirect physical access
    - short-range wireless access
    - long-range wireless access

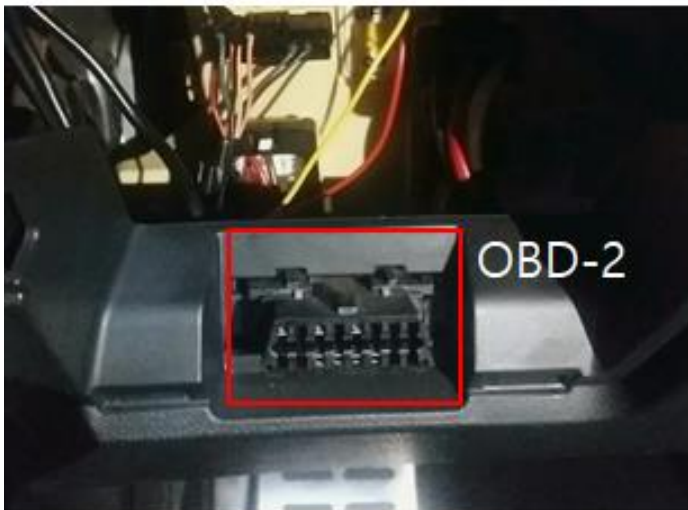


# Indirect physical

## ❖ Definition:

- Attacks over physical interfaces
- Constrained: Adversary may not **directly** access the physical interfaces herself

## ❖ OBD(stands for On Board Diagnostic)



Port



Scanner



PassThru

# Indirect physical

## ❖ Definition:

- Attacks over physical interfaces
- Constrained: Adversary may not **directly** access the physical interfaces herself

## ❖ Extends attack surface to the device



# Short-range wireless

- ❖ Definition: Attacks via short-range wireless communication (meters range or less)



Bluetooth



TPMS



Remote key



Immobilizer

# Long-range wireless

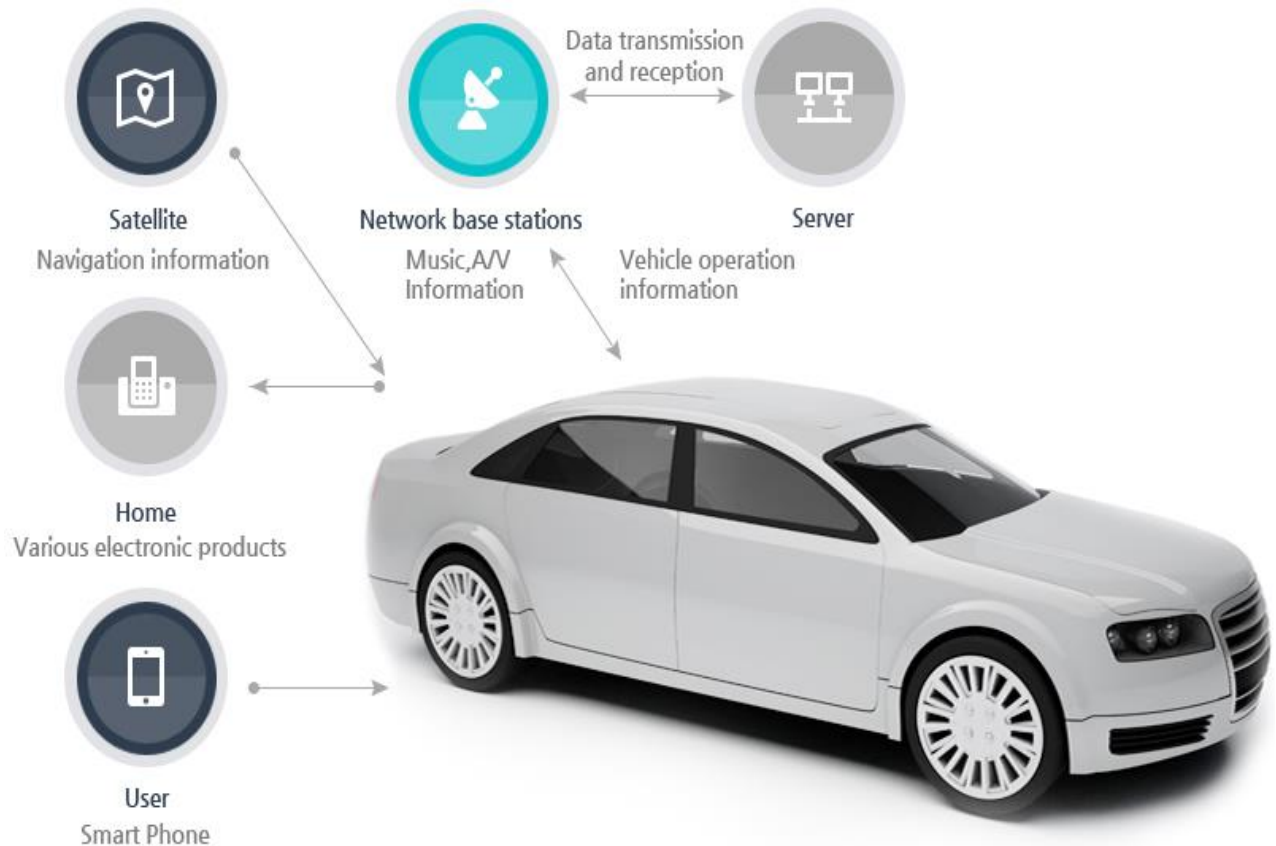
- ❖ Definition: Attacks via long-range wireless communication (miles, global-scale)
- ❖ Broadcast channel
  - Satellite Radio, GPS, RDS



Satellite Radio

# Long-range wireless

- ❖ Definition: Attacks via long-range wireless communication (miles, global-scale)
- ❖ Addressable channel
  - Telematics



# Attack surfaces explored in depth

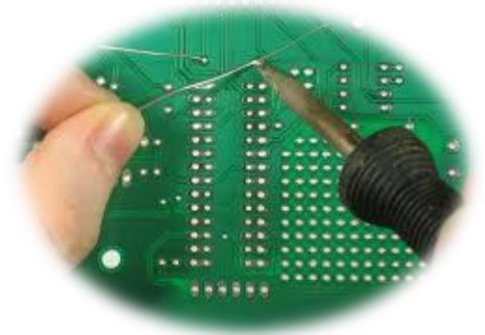
- ❖ Components we compromised
  - Indirect physical: Media player, OBDII
  - Short-range wireless: Bluetooth
  - Long-range wireless: Cellular
- ❖ Every attack vector leads to complete car compromise

# Premise

- ❖ No direct physical access
- ❖ Already know how to deal with CAN signal
- ❖ Recent made sedan, 2 same model

# Overall methodology

- ❖ Extract device's firmware
  - Read memory out over the CAN bus (CarShark)
  - Desolder flash memory chips in ECUs
- ❖ Reverse engineering firmware
  - IDA Pro
  - Custom tools
- ❖ Identify and test vulnerable code paths





# Indirect physical: Media player attack

- ❖ Code for ISO-9660 leads to
  - Vulnerable : in a module that uploads firmware.

```
./usr/share/scripts/update/installer/system_module_check.lua

91     local fname= string.format("%s/swdl.iso", os.getenv("USB_STICK")
or "/fs/usb0")
92     local FLAGPOS=128
93
94     local f = io.open(fname, "rb")
95     if f then
96         local r, e = f:seek("set", FLAGPOS)
97         if r and (r == FLAGPOS) then
98             local x = f:read(1)
99             if x then
100                 if x == "S" then
101                     print("system_module_check: skip ISO integrity
check")
```

# Indirect physical: Media player attack

- ❖ Code for ISO-9660 leads to
  - Vulnerable : in a module that uploads firmware

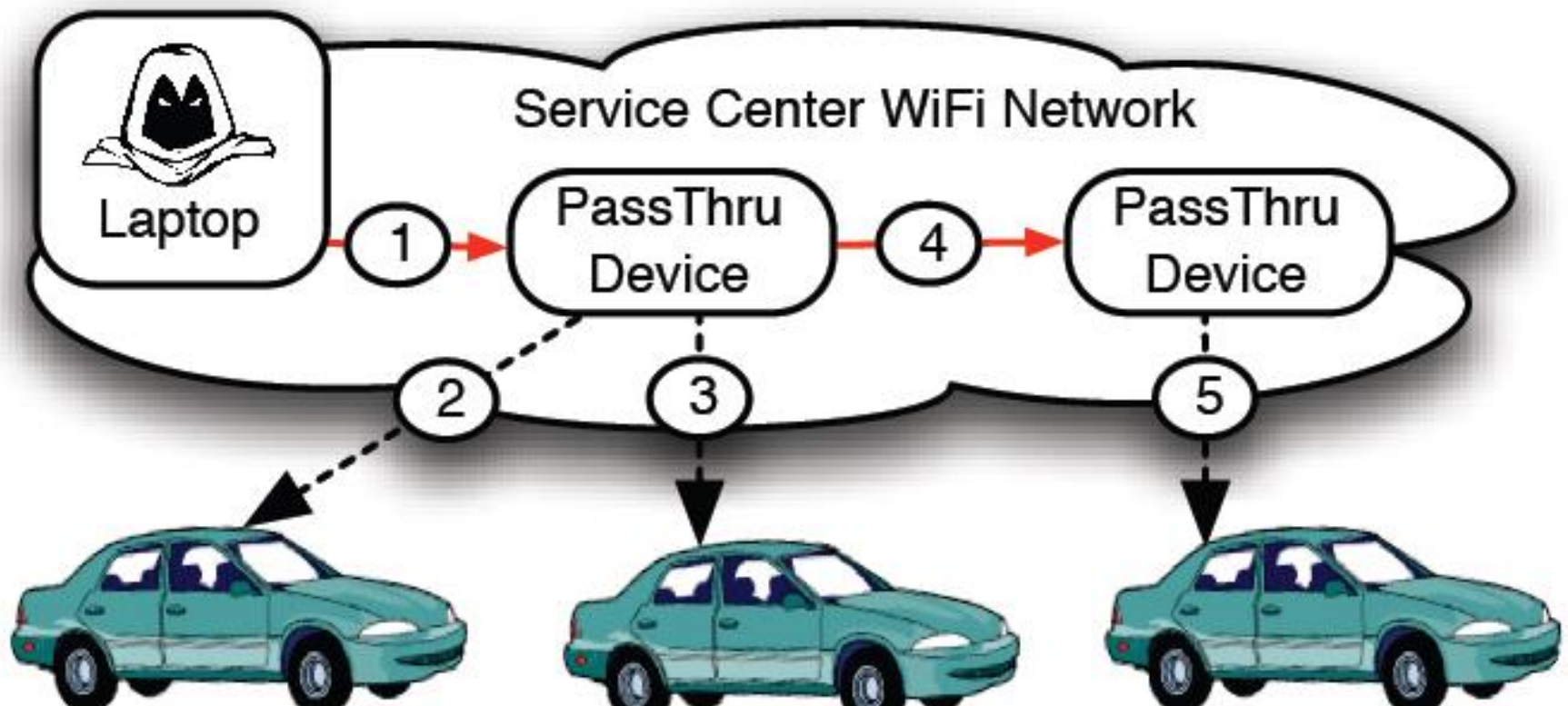
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
0000h:	DC	BC	47	9C	27	F6	2D	93	3B	EC	74	5A	8D	A5	E3	98	. "Gæ'ô-";itZ.Yã"
0010h:	B6	9F	BD	F7	C8	57	6B	89	C2	C7	6B	E7	BC	6B	21	EA	ŷŷ+žWk%Åçkç%k!è
0020h:	96	DC	0C	D8	DD	F4	B9	9B	64	CE	8F	8B	2A	D0	8A	47	-Ü.ØŸô' >dl.< *DŠG
0030h:	2F	44	F7	D2	3F	45	06	4D	48	96	9E	6E	7D	7F	23	17	/D:Ô?E.MH-žn}.#.
0040h:	49	C9	FE	D1	F1	22	A0	34	20	C6	D0	5E	DF	DD	E8	14	IÉpNñ" 4 EB^BŸè.
0050h:	A6	A6	2B	08	B1	47	41	03	79	18	F0	8C	3D	E2	6D	BC	+.iGA.y.ŠE-ām¼
0060h:	49	5D	A0	CE	EB	CE	F7	C7	8A	1E	A5	68	FB	8E	3A	98	I) ièi÷çŠ.VhúŽ:~
0070h:	78	FE	40	EA	10	4D	38	30	07	5A	BC	D4	E8	B9	1D	34	xp@è.M80.ZHôè'.4
0080h:	53	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	S.....
0090h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00A0h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00B0h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00C0h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00D0h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00E0h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00F0h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
0100h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
0110h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....



# Short-range wireless: OBDII

❖ PassThru device has no authentication method

1. Connect to same WiFi with device to get to CAN bus
2. Implant malicious code inside the device



# Short-range wireless: Bluetooth attack

- ❖ Custom-built code contains vulnerability
  - Strcpy() bug → execute arbitrary code(Bufferoverflow)
- 1. Using owner's smartphone as stepping-stone
  - Trojan Horse application
  - Check whether other party is telematics unit
    - if so it sends our attack payload
- 2. Can directly pair with Bluetooth undetectably
  - USRP software radio
  - MAC address ; 2ways to get
  - Brute force PIN ;10hrs per car

# Short-range wireless: Bluetooth attack

Frontline Test Equipment Bluetooth Protocol Analyzer - [9955.0bps]

File Edit Search System Acquisition View Window Help

Start

All Layers View

LMP L2CAP RFCOMM SDP OBEX TCS HCR PPP SPP AT HID HCRP AVDTP AVCTP Triggers

Index	Slave Master	Type	Description	Payload
8	Slave	-	Access Error	
9	Master	NALL	NALL Packet	
10	Slave	-	Access Error	
11	Master	NALL	NALL Packet	
12	Slave	DM1	LMP_version_req	4C 01 01 00 2C 02
13	Master	NALL	NALL Packet	
14	Slave	-	Access Error	
15	Master	NALL	NALL Packet	
16	Slave	-	Access Error	
17	Master	NALL	NALL Packet	
18	Slave	-	Access Error	
19	Master	DM1	LMP_features_req	4E 0F FE 0F 00 18 18 00 00
20	Slave	NALL	NALL Packet	
21	Master	NALL	NALL Packet	
22	Slave	-	Access Error	

System Info

Packet Header

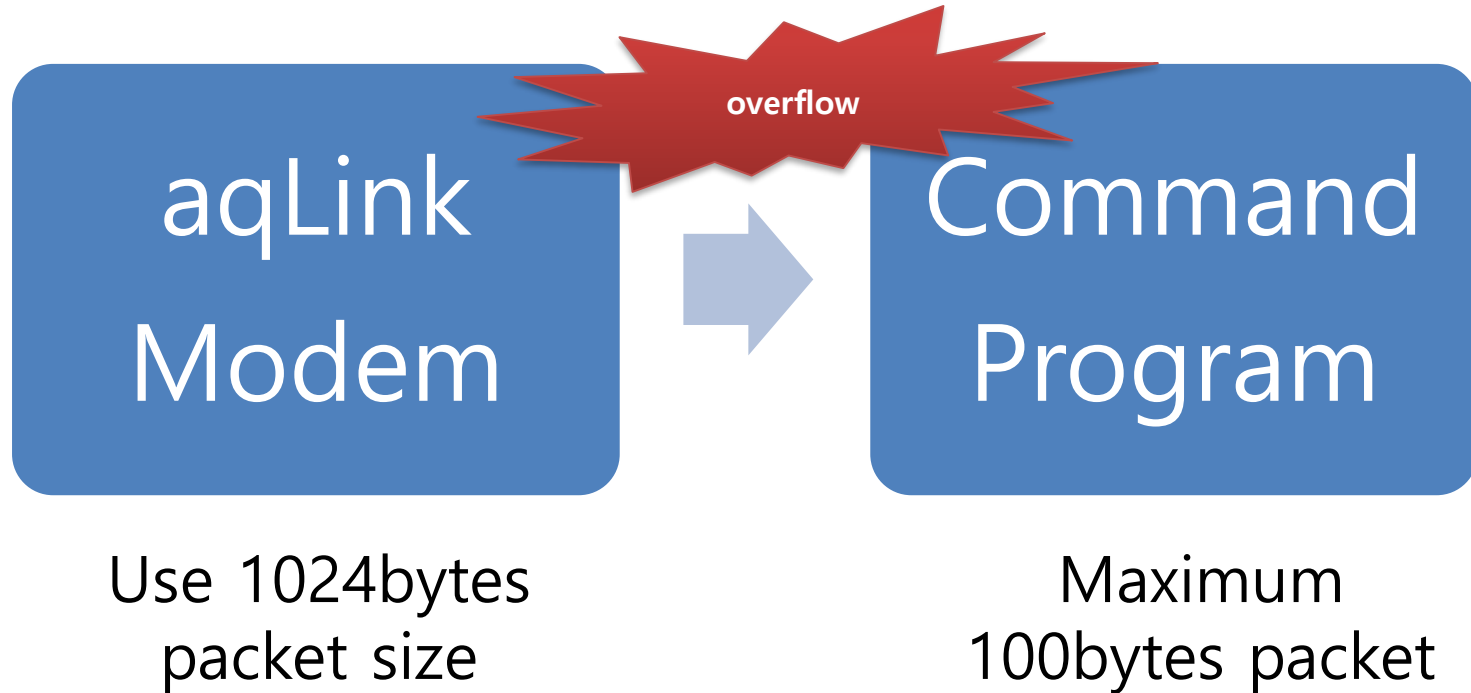
AM_ADDR	TYPE	FLOW	ADRN	SEQN	IEC
-	0010	-	-	-	-

AM\_ADDR

channel: 22718 LMP: 63 L2CAP: 10 RFCOMM: 0 SDP: 0 OBEX: 0 TCS: 0 HCR: 0 PPP: 0 SPP: 0 AT: 0 HID: 0 HCRP: 0 AVDTP: 0 AVCTP: 0

# Long-range wireless: Cellular attack

## 1. Attack @ Lowest level of protocol stack



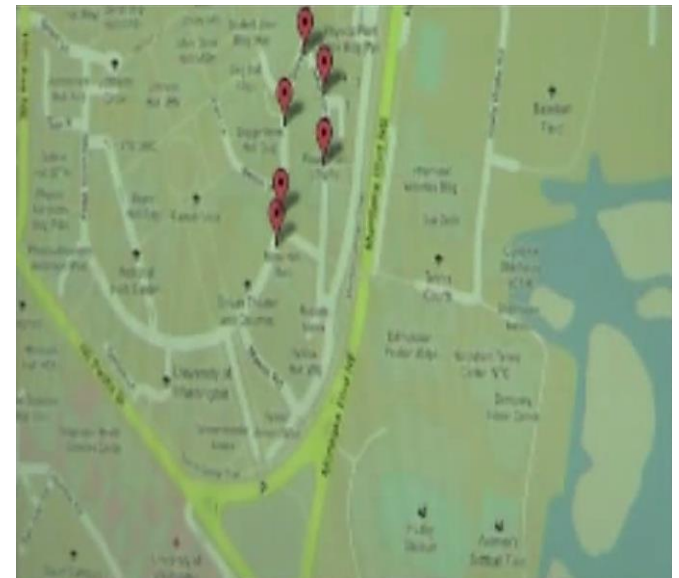
# Car theft

1. Compromise car
2. Get Car's INFO (GPS...)
3. Unlock doors
4. Start engine
5. Bypass anti-theft



# Surveillance

- ❖ Compromised car
  - ❖ Continuously report GPS coordinates
  - ❖ Stream audio recorded from the in-cabin mic
    - Detect voice (VAD)
    - Compress audio
    - Stream to remote computer
- E.g.) Professor Yongdae Kim

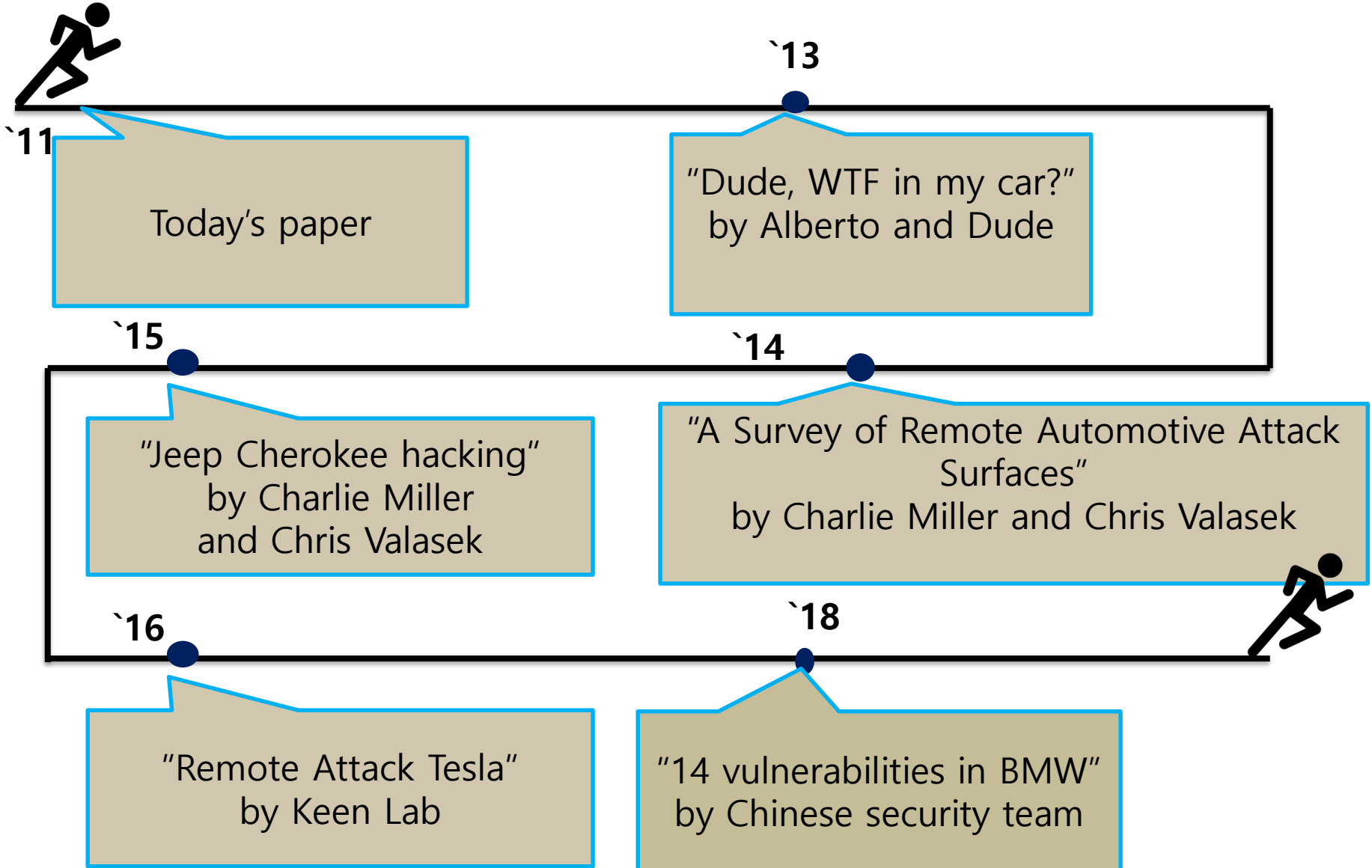




# Where to go from here?



# Where to go from here?



# Where to go from here?

- ❖ Stakeholders responding today:
  - SAE, USCAR, US DOT
- ❖ Recommendation : lessons from the PC world
  - Avoid unsafe function
  - Remove unnecessary binaries e.g.) ftp/telnet/vi
  - ASLR (Address Space Layout Randomization)
  - Stack cookies
  - Limited inbound calls

# Where to go from here?

## Achieve excellence in automotive software security

<b>Penetration testing</b>	Replicate the steps a threat agent takes to find vulnerabilities, and receive clear guidance on how to eliminate them in your server-side applications and APIs.
<b>Dynamic application security testing (DAST)</b>	Identify security vulnerabilities while web applications are running, without the need for source code.
<b>Mobile application security testing (MAST)</b>	Find vulnerabilities regardless of where they exist, including in client-side code, server-side code, third-party libraries, and underlying mobile platforms.
<b>Embedded application security testing (EAST)</b>	Verify the functional and security performance of embedded systems, and identify vulnerabilities in the embedded software stack.
<b>Software composition analysis (SCA)</b>	Detect third-party open source components in source code and binaries. Track and remediate vulnerabilities during development and in containers in production. Identify third-party licenses, and set policies to avoid noncompliance.
<b>Tools</b>	Synopsys provides industry-leading tools for software composition analysis, static code analysis, fuzz testing and protocol testing, and interactive security testing.
<b>Architecture and design</b>	Security testing and threat modeling help you find architectural, design, and system defects and flaws.
<b>Cloud security</b>	Run applications securely in the Cloud.
<b>Agile and CI/CD</b>	Build security into modern agile SDLCs.
<b>Training</b>	Synopsys creates security training courses delivered as instructor-led, eLearning, and virtual classes.
<b>Build Security In programs</b>	Synopsys offers the BSIMM, the Maturity Action Plan, security metrics, and software security initiative programs.



# Where to go from here?

## ❖ Future work

- Developing new protocol alternative to CAN bus
- Research how to encrypt CAN message
- CAN monitoring system to catch external attack

# Summary

- ❖ Current autos have broad (and increasing) external attack surface
- ❖ They demonstrated real attacks that compromised safety-critical systems
- ❖ **Industry and government are responsible**



Q&A

The image features the text "Q&A" rendered in a bold, three-dimensional, blue font. The letters are thick and have a slight shadow beneath them, giving them a 3D appearance. The ampersand is a stylized, light blue color, contrasting with the darker blue of the letters. The entire text is set against a plain white background.