

MIDC·2019 | 智能新时代
小米 I o T 安全峰会

蓝牙安全之第二战场

曾颖涛 小米 AIoT 安全实验室研究员

目录

蓝牙设备联动安全

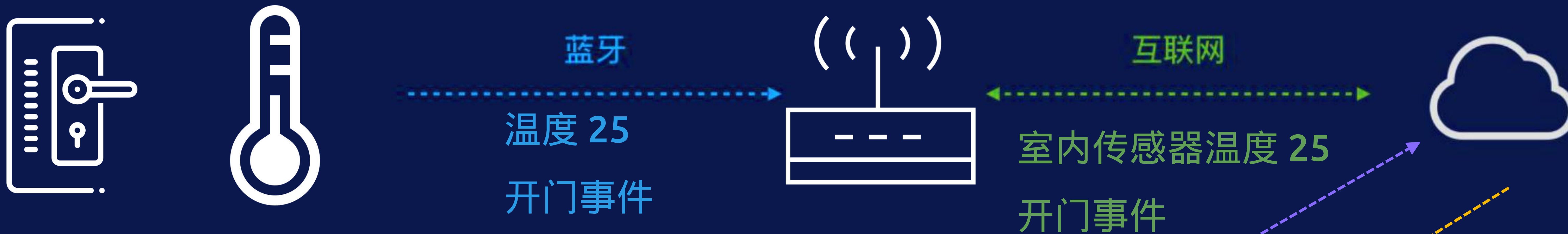
芯片厂商隐患

蓝牙硬件安全

蓝牙安全架构

蓝牙设备联动

依靠于蓝牙网关实现设备联动功能



让传感器具有访问互联网能力
通过蓝牙广播实现事件互联

获取家里传感器数据



室内温度过热打开空调
主人回家打开室内电器

蓝牙广播协议分析

5203 16.066598 0inapina 34:6a:bf Broadcast LE LL 57

Frame 5202: 57 bytes on wire (456 bits), 57 bytes captured (456 bits) on interface
Nordic BLE Sniffer
Bluetooth Low Energy Link Layer
Access Address: 0x8e89bed6
Packet Header: 0x1f00 (PDU Type: ADV_IND, ChSel: #1, TxAdd: Public)
Advertising Address: Qingping_34:6a:bf (58:2d:34:34:6a:bf)
Advertising Data
Flags
Service Data - 16 bit UUID
Length: 21
Type: Service Data - 16 bit UUID (0x16)
UUID 16:
Service Data: 5020aa0101bf6a34342d580d10043a01b801
CRC: 0x167b64

0000	f2 32 00 02 ac d9 06 0a 01 27 39 00 00 9b 0c 00	.2.....'9.....
0010	00 d6 be 89 8e 00 1f bf 6a 34 34 2d 58 02 01 06j44-X...
0020	15 16 95 fe 50 20 aa 01 01 bf 6a 34 34 2d 58 0d	...P..j44-X.
0030	10 04 3a 01 b8 01 68 de 26	...h.&

FrameCtrl 5020
PID aa01
Counter 01
Mac (bf6a34342d58)
EID 100d
Data len 04
Data 013a b801
温度 31.4
湿度 44



蓝牙广播事件

电量
温度
湿度
水壶
传感器数据
开关门事件(加密)

time	mac	name	data	parsedata
14:57:49	A7:A7:76	纹保管箱	shDecrypter(iv_index	
14:57:49	52:9D:3D	智能门锁	applicationKey(bytes.fromhex(appkey))], deviceKey(bytes.fromhex(devicekey), address], networkKey(bytes.fromhex(networkkey), iv_index))]	
14:57:49	80:58:F1	温湿度计	041002fc00	TEMP:25.2
14:57:49	00:00:31	温湿度计	0610021509	HUMIDITY:232.2
14:57:50	86:F1:2F	恒温电水壶	051002003c	BOIL
14:57:50	6F:E7:E6	金属旅行	0809534d492d4d3153	
14:57:50	E5:92:CB	电动牙刷	0610022c01	HUMIDITY:30.0
14:57:50	80:58:F1	温湿度计	0d1004fa00fd00	TEMP:25.0&HUMIDITY:25.3
14:57:51	34:6A:BF	牙温湿度	0809534d492d4d4331	
14:57:52	FD:6E:DF	声波电动	0809534d492d4d3153	
14:57:52	C4:09:43	电动牙刷	0a100132	BATTERY:50
14:57:52	5E:87:FC	显湿度计2	0610022c01	HUMIDITY:30.0
14:57:52	80:58:F1	温湿度计	0d1004f900fa00	TEMP:24.9&HUMIDITY:25.0
14:57:53	34:6A:BF	牙温湿度	0809534d492d4d3153	
14:57:54	0A:09:34	电动牙刷	0610022c01	HUMIDITY:30.0
14:57:54	80:58:F1	温湿度计	061002f800	HUMIDITY:24.8
14:57:55	34:6A:BF	牙温湿度	0809534d492d4d3153	
14:57:55	75:D5:36	电动牙刷	041002fc00	TEMP:25.2
14:57:55	80:58:F1	温湿度计		
14:57:56	A1:63:A0	显湿度计2		
14:57:56	34:B0:F6	显湿度计2		
14:57:57	52:9D:3D	智能门锁	3d9d523706de07a53eb5747375eb274c5c	ENCRYPT:3d9d523706de07a53eb5747375eb274c5c
14:57:57	92:2E:C2	电动牙刷	0809534d492d4d3153	
14:57:57	80:58:F1	温湿度计	041002fc00	TEMP:25.2
14:57:58	5E:87:FC	显湿度计2	061002fa00	HUMIDITY:25.0
14:57:58	AD:53:58	显湿度计2	0610020401	HUMIDITY:26.0
14:57:59	34:6A:BF	牙温湿度	0d1004fb00fc00	TEMP:25.1&HUMIDITY:25.2
14:57:59	80:58:F1	温湿度计	041002fc00	TEMP:25.2
14:58:00	52:9D:3D	智能门锁		
14:58:00	80:58:F1	温湿度计	0610022c01	HUMIDITY:30.0
14:58:01	34:6A:BF	牙温湿度	0d1004f900fa00	TEMP:24.9&HUMIDITY:25.0
14:58:01	80:58:F1	温湿度计	041002fc00	TEMP:25.2
14:58:02	80:58:F1	温湿度计	0610022c01	HUMIDITY:30.0
14:58:04	5E:87:FC	显湿度计2	061002fa00	HUMIDITY:25.0
14:58:04	80:58:F1	温湿度计	0610022c01	HUMIDITY:30.0

蓝牙广播协议分析

```
if (p_beacon->frame_ctrl & ENCRYPT_MASK) {  
    p_info->encrypted = 1;  
}
```

协议参数由设备端决定



蓝牙设备联动隐患



蓝牙芯片厂商隐患

芯片厂商OTA

manifest.json

```
{  
  "manifest": {  
    "application": {  
      "bin_file": "Duck.bin",  
      "dat_file": "Duck.dat",  
      "init_packet_data": {  
        "application_version": 67,  
        "device_revision": 65535,  
        "device_type": 65535,  
        "firmware_crc16": 12368,  
        "softdevice_req": [  
          100  
        ]  
      }  
    },  
    "dfu_version": 0.5  
  }  
}
```

A厂商 Legacy OTA (SDK 11.x)

```
$ ls xxac.extracted
```

```
Duck.bin # 设备固件  
Duck.dat # 设备签名文件  
manifest.json # 文件清单
```

```
Duck.dat
```

```
ff ff ff ff 43 00 00 00 01 00 64 00 50 30
```

硬件版本信息
固件版本

SoftDevices 列表以及芯片型号
固件CRC16 校验

```
$ hexdump -n 64 -C B.bin
```

```
00000000  70 51 aa ff 78 88 00 00  43 72 b3 55 31 2e 30 2e  
00000010  35 00 ff ff ff ff ff ff  ff ff ff ff 2c d0 6d 59  
00000020  00 ff ff ff ff ff ff ff  ff ff ff ff ff ff ff ff  
00000030  ff ff ff ff ff ff ff ff  ff ff ff ff ff ff ff ff
```

文件头 2byte 70 51
标识符 2byte aa ff
固件大小 4byte
CRC32 4byte
版本 16byte
编译时间 4byte
固件加密 1Byte
保留位

B厂商 OTA

芯片厂商OTA方案

OTA_UUID_SERVICE="00010203-0405-0607-0809-0a0b0c0d1912"

SPP_DATA_OTA="00010203-0405-0607-0809-0a0b0c0d2b12"

```

null@null:~/mi/code/ble/mibeacon/release$ gatttool --primary -b A4:C1:38:5E:87:FC
attr handle = 0x0001, end grp handle = 0x0007 uuid: 00001800-0000-1000-8000-00805f9b34fb
attr handle = 0x0008, end grp handle = 0x000b uuid: 00001801-0000-1000-8000-00805f9b34fb
attr handle = 0x000c, end grp handle = 0x0016 uuid: 0000180a-0000-1000-8000-00805f9b34fb
attr handle = 0x0017, end grp handle = 0x001e uuid: 00010203-0405-0607-0809-0a0b0c0d1910
attr handle = 0x001f, end grp handle = 0x0022 uuid: 00010203-0405-0607-0809-0a0b0c0d1912
attr handle = 0x0023, end grp handle = 0x0049 uuid: 0000fe95-0000-1000-8000-00805f9b34fb
attr handle = 0x004a, end grp handle = 0x006d uuid: ebe0ccb0-7a0a-4b0c-8a1a-6ff2997da3a6
    
```

Write 0x00ff

Write 0x01ff # OTA_START

0000 26800000000005d024b4e4c5470038800 b8a2

0100 ae8000000000000000c40e010000000000 bfd6

0200 0c6481a2090b1a40c006c006c006c006 610d

...

固件地址(addr_index)

设备固件内容

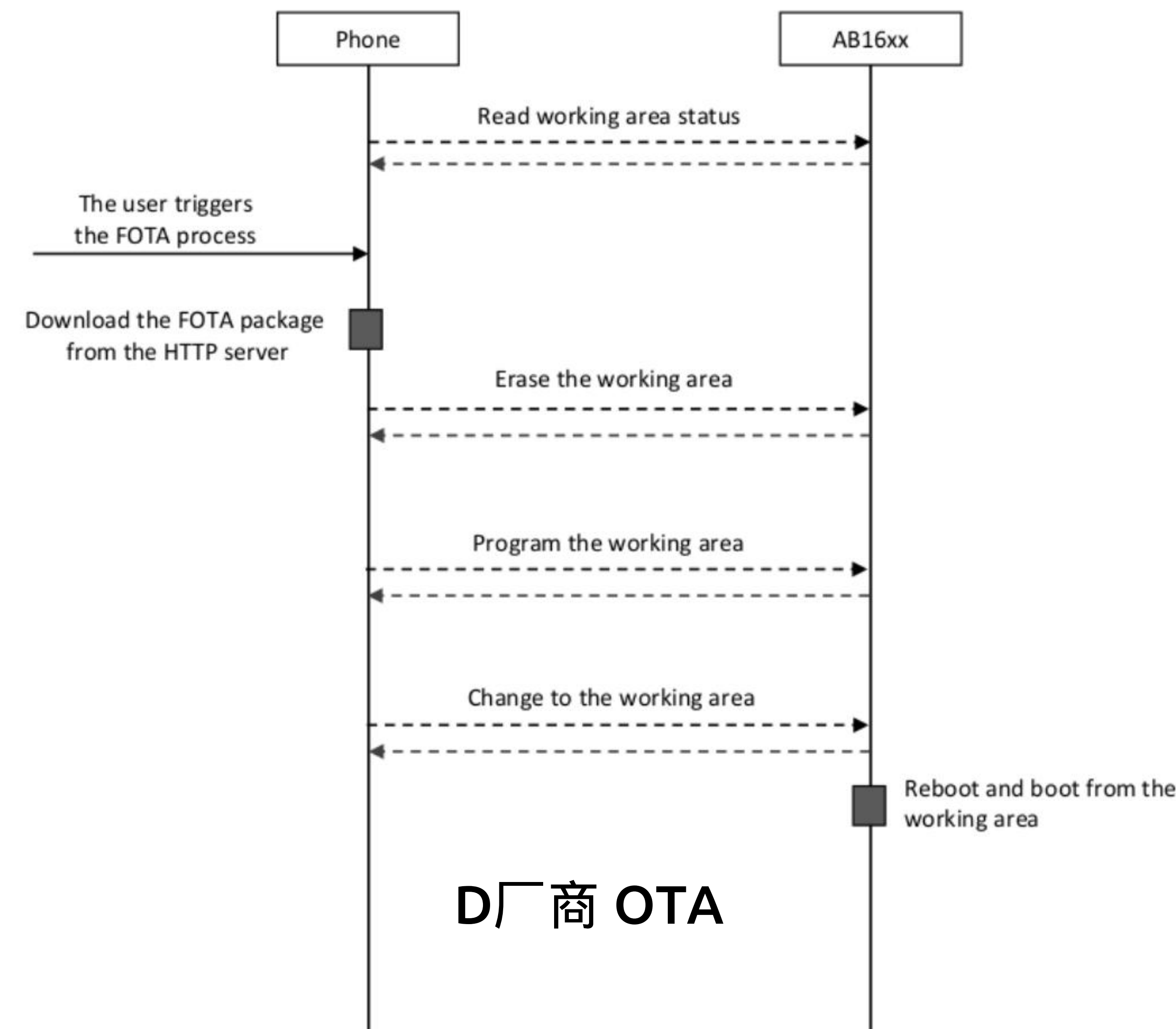
对前18byte的CRC16

C厂商 OTA



2. FOTA Application Flow

2.1. Flow chart



芯片厂商OTA方案

BLEEDINGBIT OAD RCE漏洞 (CVE-2018-7080)

BLEEDINGBIT OAD RCE漏洞只发生在Aruba Access Point Series 300中，其使用了 OAD (Over the Air firmware Download, OTA固件下载) 特征。技术上讲，这实际上是BLE芯片设计用来进行固件更新的后门。OAD特征常被用作开发工具，也被用于AP生产中。允许附近的攻击者来访问和安装全新和不同版本的固件，甚至覆写BLE芯片的操作系统。

默认情况下，OTA特征并不自动配置为解决安全更新固件的问题。OAD允许运行在BLE芯片上的固件通过GATT事务进行简单更新。在Aruba的AP中，**会加入一个硬编码的密码来预防OAD特征被攻击者滥用。**

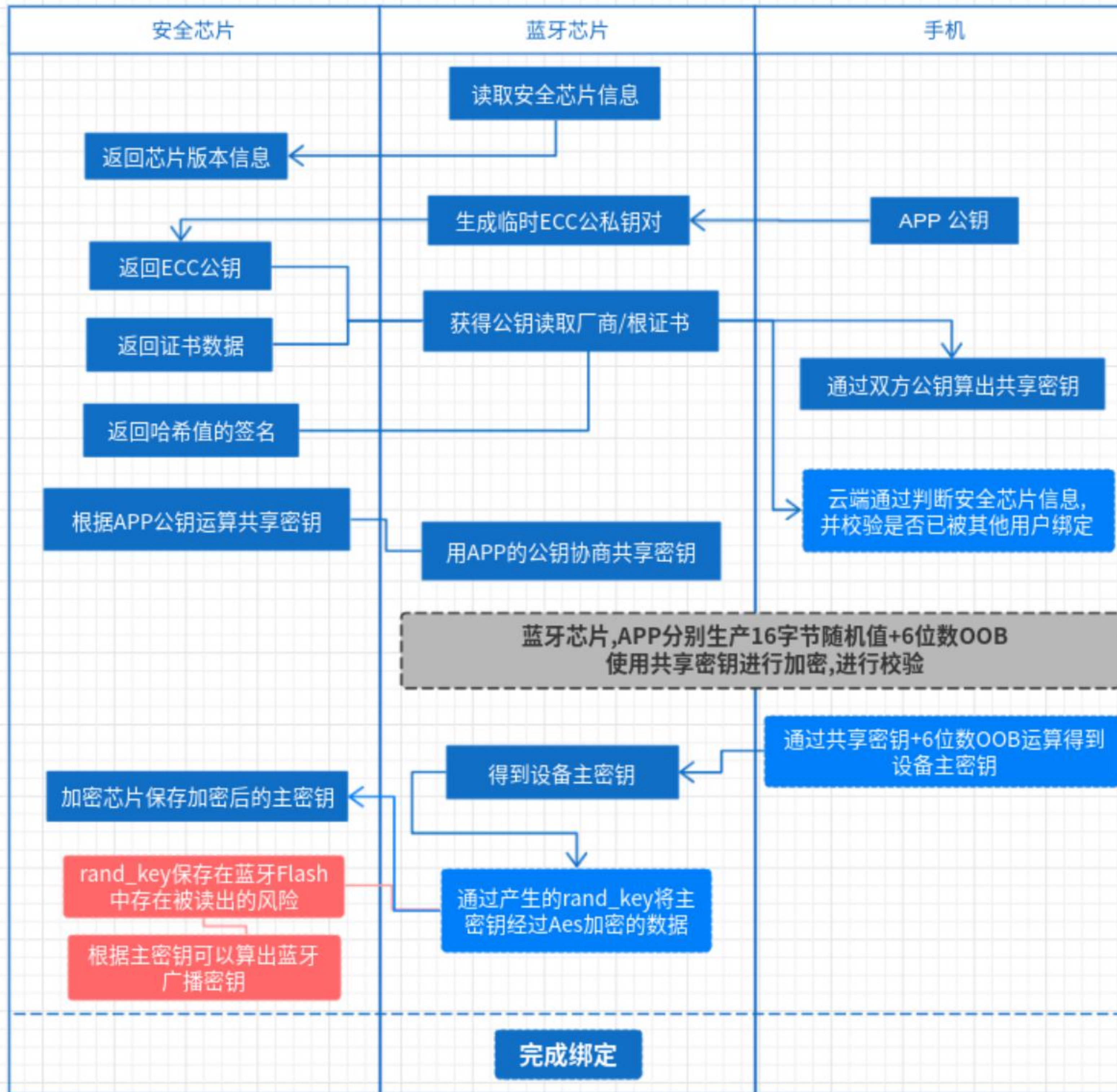
但是通过合法更新或逆向Aruba的BLE固件来获取硬编码密码的攻击者可以连接到有漏洞的AP的BLE芯片，并上传含有攻击者代码的恶意固件，达到重写操作系统、获取完全控制权的目的。

至于CVE-2018-7080，**该制造商建议在生产环境下禁用OAD功能，因为它仅用于开发和测试用途。**

```
public class BluetoothLeService
    extends Service
{
    public static String AB_ACCESS_COOKIE = "F9CA0CA23171          89F6B340";
    public static UUID AB_CHARACTERISTIC_UNLOCK_UUID;
    public static UUID AB_SERVICE_UUID; E厂商 OTA
```


蓝牙硬件安全

硬件安全芯片分析



绕过蓝牙芯片读取保护

Jlink 读取Flash数据

RBPCONF

Flash空间读取保护

APPROTECT

禁止寄存器映射地址

>Reset halt # 复位并中断芯片程序

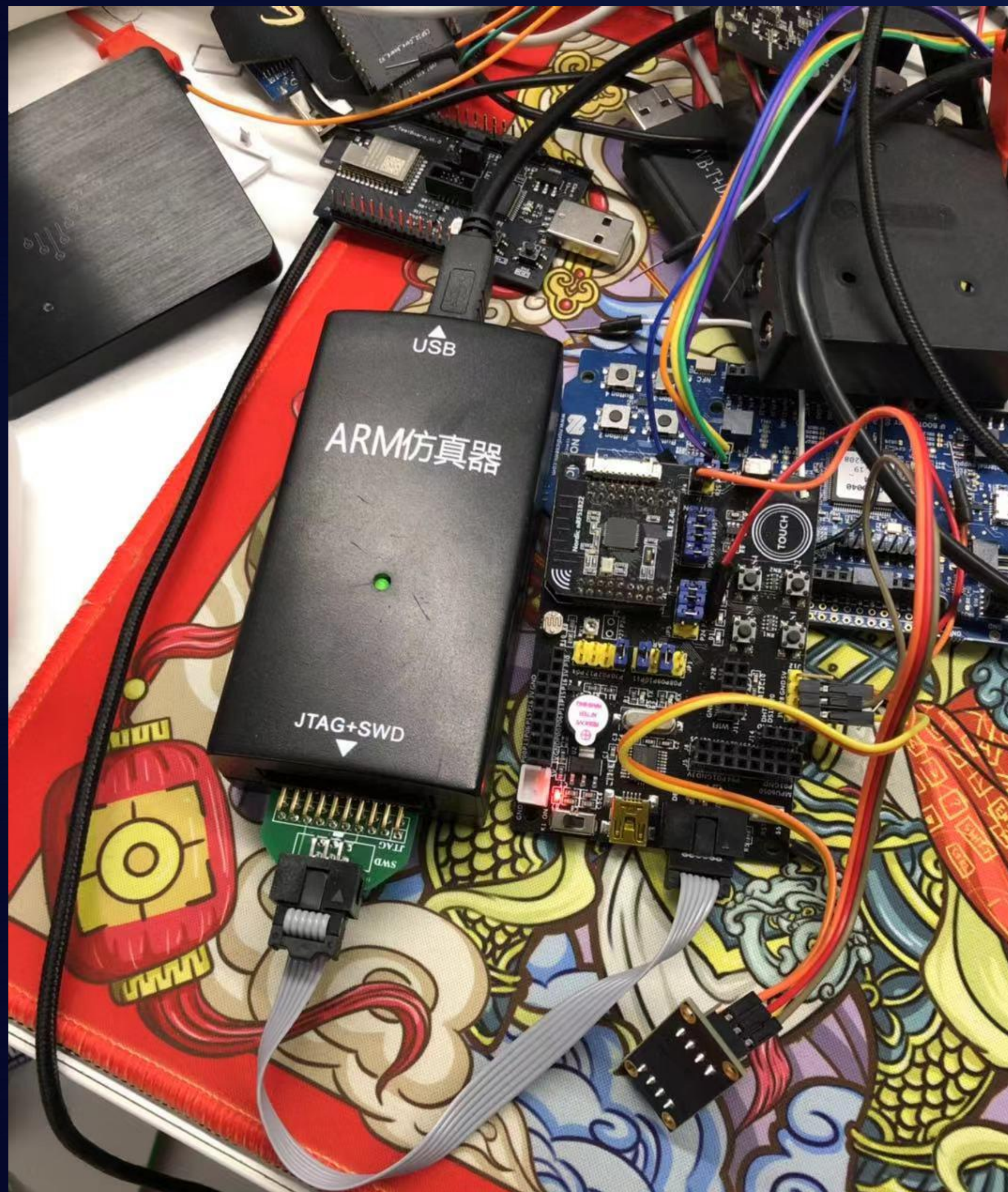
>reg # 读取寄存器

>step # 单步执行下一条指令

>reg

>step

无法通过JLink读取数据，
但是可以操作芯片寄存器找到ldr指令



绕过蓝牙芯片读取保护

```
> reg
==== arm v7m registers
(0) r0 (/32): 0x00000000
(1) r1 (/32): 0x00000000
(2) r2 (/32): 0x00000000
(3) r3 (/32): 0x0000031F
(4) r4 (/32): 0x10001000
(5) r5 (/32): 0x00000000
(6) r6 (/32): 0x00000000
(7) r7 (/32): 0x00000000
(8) r8 (/32): 0x00000000
(9) r9 (/32): 0x00000000
(10) r10 (/32): 0x00000000
(11) r11 (/32): 0x00000000
(12) r12 (/32): 0x00000000
(13) sp (/32): 0x20000400
(14) lr (/32): 0xFFFFFFFF
(15) pc (/32): 0x00000322
(16) xPSR (/32): 0x01000000
(17) msp (/32): 0x20000400
(18) psp (/32): 0x00000000
(19) primask (/1): 0x00
(20) basepri (/8): 0x00
(21) faultmask (/1): 0x00
(22) control (/2): 0x00
(23) d0 (/64): 0x0000000000000000
(24) d1 (/64): 0x0000000000000000
(25) d2 (/64): 0x0000000000000000
(26) d3 (/64): 0x0000000000000000
(27) d4 (/64): 0x0000000000000000
(28) d5 (/64): 0x0000000000000000
(29) d6 (/64): 0x0000000000000000
```

```
> step
target halted due to single-step, current mode: Thread
xPSR: 0x01000000 pc: 0x00000324 msp: 0x20000400
> reg
==== arm v7m registers
(0) r0 (/32): 0xFFFFFFFF
(1) r1 (/32): 0x00000000
(2) r2 (/32): 0x00000000
(3) r3 (/32): 0x0000031F
(4) r4 (/32): 0x10001000
(5) r5 (/32): 0x00000000
(6) r6 (/32): 0x00000000
(7) r7 (/32): 0x00000000
(8) r8 (/32): 0x00000000
(9) r9 (/32): 0x00000000
(10) r10 (/32): 0x00000000
(11) r11 (/32): 0x00000000
(12) r12 (/32): 0x00000000
(13) sp (/32): 0x20000400
(14) lr (/32): 0xFFFFFFFF
(15) pc (/32): 0x00000324
```

```
> reg r4 0x00000322
r4 (/32): 0x00000322
> reg pc 0x00000322
pc (/32): 0x00000322
> step
target halted due to single-step, current mode: Thread
xPSR: 0x01000000 pc: 0x00000324 msp: 0x20000400
> reg r0
r0 (/32): 0x68006960
>
```

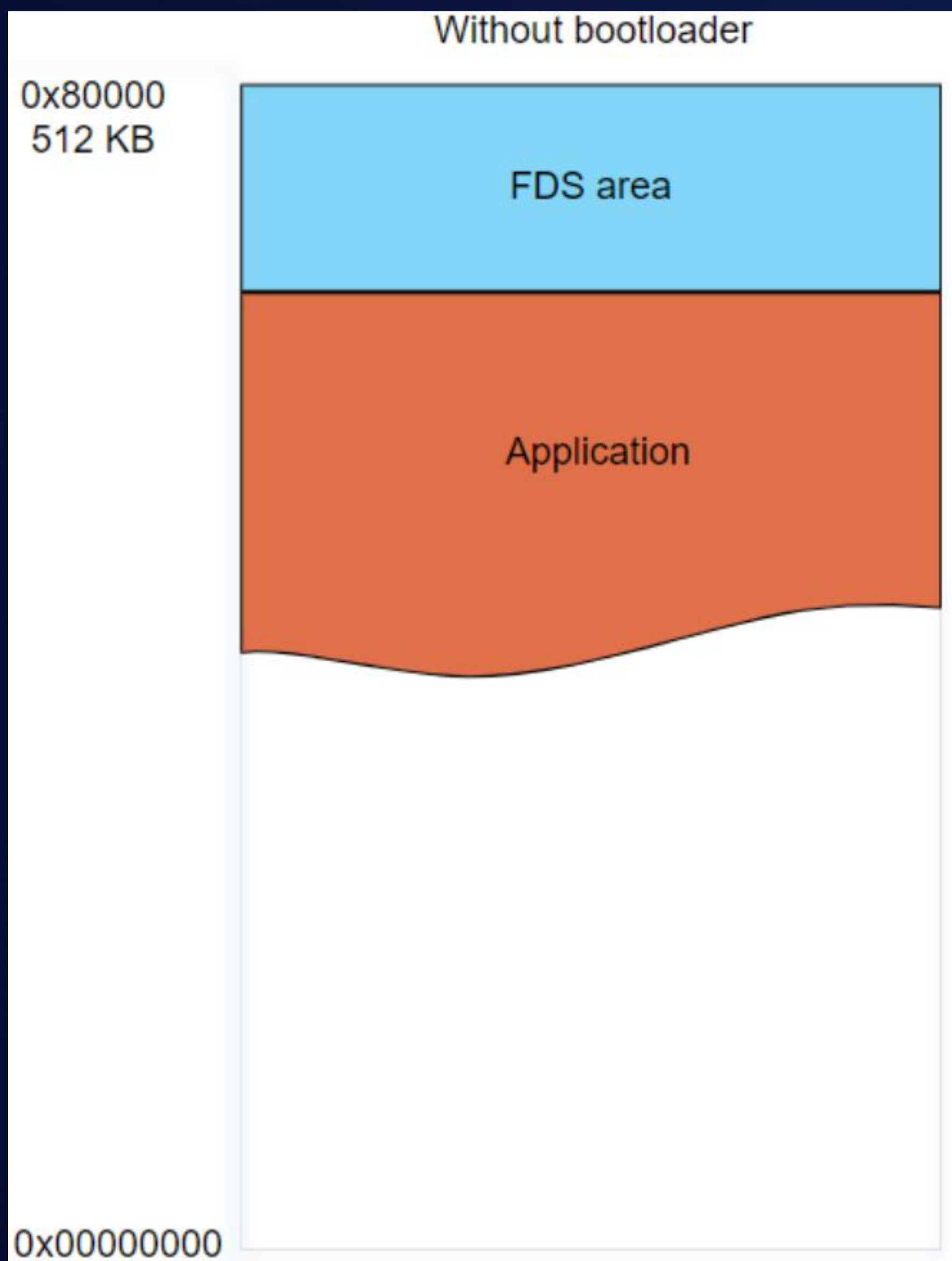
```
null@null:~$ printf "\x60\x69\x00\x68" >> binarycode
null@null:~$ hexdump -C binarycode
00000000 60 69 00 68
00000004
null@null:~$ arm-none-eabi-objdump -D --target binary -Mforce-thumb -marm binarycode
binarycode: file format binary
Disassembly of section .data:
00000000 <.data>:
0: 6960 ldr r0, [r4, #20]
e_r2: 6800 ldr r0, [r0, #0]
```

ldr r0,[r4,#20]

将寄存器r4+20字数据读入寄存器r0
可通过这种方式循环读取四字节数据

绕过蓝牙芯片读取保护

Flash Data Storage (FDS)



```
import re
import struct

# Based on https://www.pentestpartners.com/security-blog/nrf51822-c
HOST="127.0.0.1"
PORT="4444"

tn = telnetlib.Telnet(HOST, PORT)
tn.set_debuglevel(0)
tn.read_until(">")

def tncmd(cmd):
    tn.write(cmd + "\n")
    return tn.read_until(">")

tncmd("reset halt")

with open("Flash.bin", "w") as outfile:
    for addr in xrange(int("0x7dfe0", 16), int("0x80000", 16), 4):
        tncmd("reg pc 0x322")
        tncmd("reg r4 " + hex(addr))
        tncmd("step")
        resp = tncmd("reg r0")
        t = re.findall(r'0x[0-9a-fA-F]+', resp)
        if t:
            outfile.write(struct.pack("I", int(t[0], 16)))
        if (addr % int("0x400", 16)) == 0:
            print hex(addr)
```

循环读取四个字节

ldr 指令地址

要读取数据地址

找到Flash中保存的数据

Flash Data Storage (FDS)

```
int _psm_record_read(uint16_t rec_key, uint8_t *out, uint16_t out_len)
{
    uint32_t ret = 0;
    fds_flash_record_t flash_record;
    fds_record_desc_t record_desc;
    fds_find_token_t ftok = {0};

    ret = fds_record_find( RECORD_FILE_ID, rec_key, &record_desc, &ftok);

#define RECORD_FILE_ID 0x4 19 // file used to storage
#define RECORD_KEY 0xB :F
#define RECORD_KEY_INFO 0x10

```

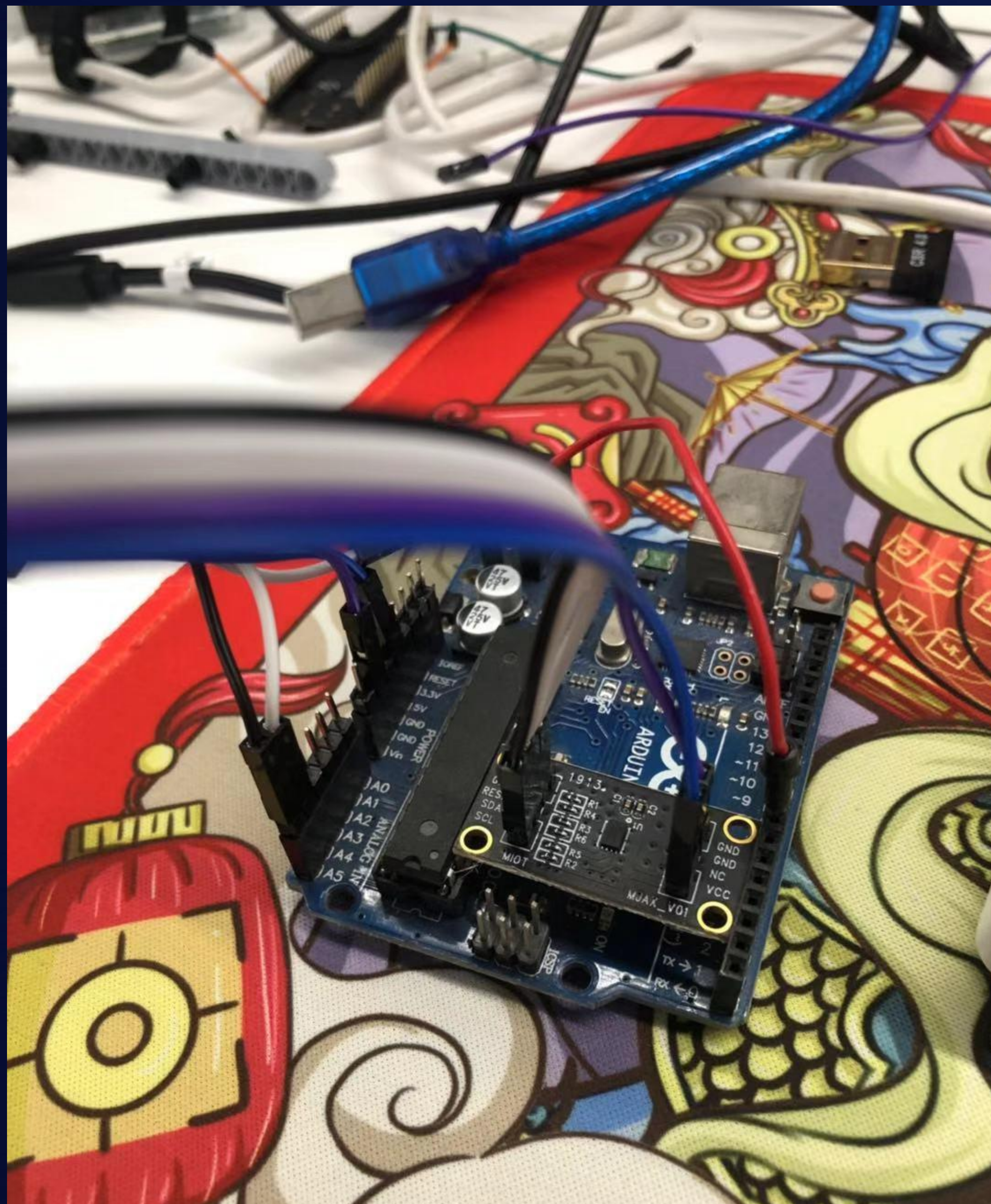
Data Page Tag : 0xDEAD CODE 0xF11E 01FE

Hex dump showing data from Flash storage. Key annotations include:

- Data Page Tag:** 0xDEAD CODE 0xF11E 01FE (highlighted in red)
- RECORD_FILE_ID:** 0x4 19 (highlighted in red)
- rand_key:** 0xB :F (indicated by a red arrow)

蓝牙芯片FDS存储数据

安全芯片硬件交互

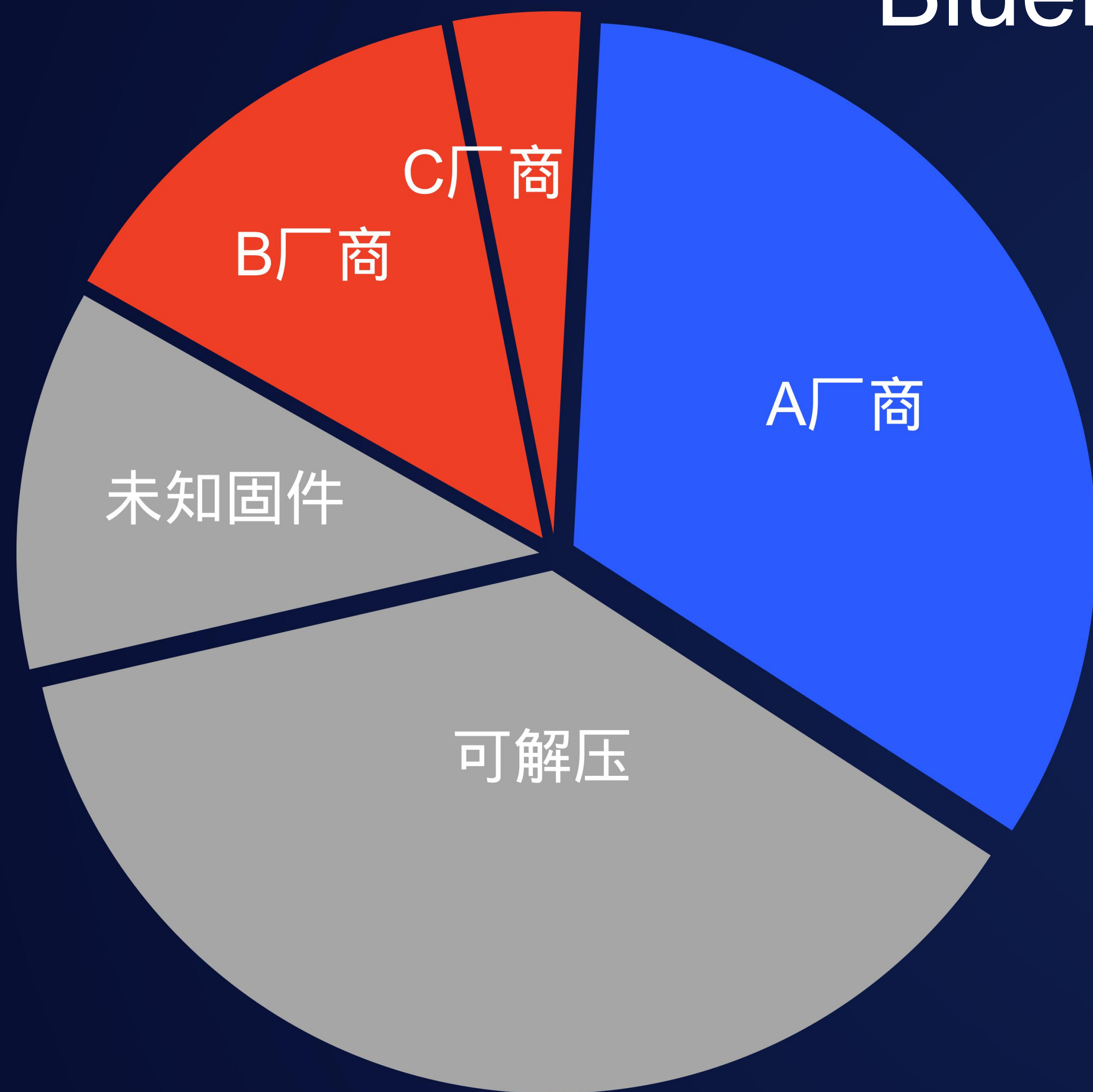


```

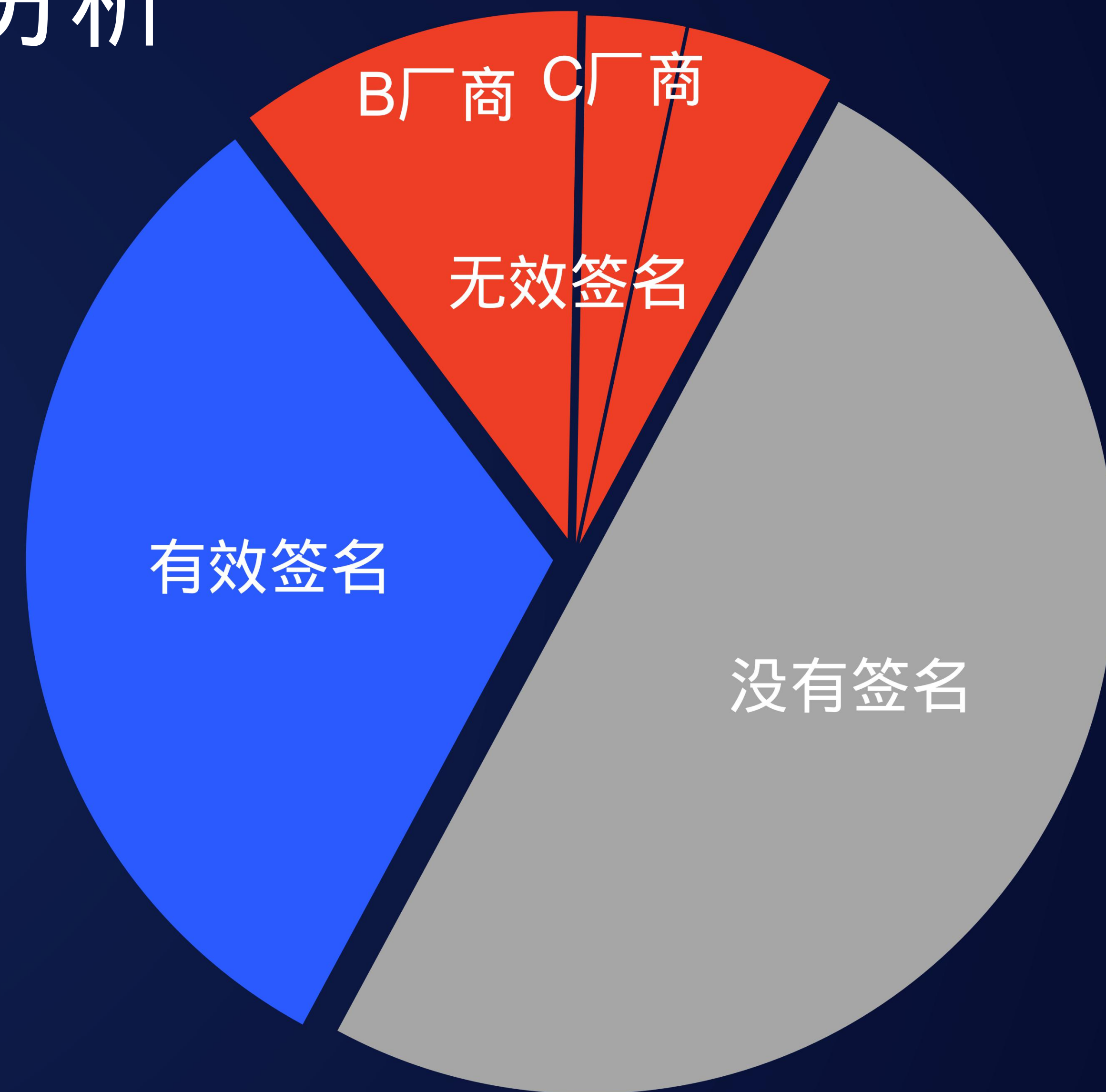
securityChip
0x18c1, 0x0948, 0x3bd3, 0x2a5a, 0x5ee5, 0x4f6c, 0x7df7, 0x6c7e,
0xa50a, 0xb483, 0x8618, 0x9791, 0xe32e, 0xf2a7, 0xc03c, 0xd1b5,
0x2942, 0x38cb, 0x0a50, 0x1bd9, 0x6f66, 0x7eef, 0x4c74, 0x5dfd,
0xb58b, 0xa402, 0x9699, 0x8710, 0xf3af, 0xe226, 0xd0bd, 0xc134,
0x39c3, 0x284a, 0x1ad1, 0x0b58, 0x7fe7, 0x6e6e, 0x5cf5, 0x4d7c,
0xc60c, 0xd785, 0xe51e, 0xf497, 0x8028, 0x91a1, 0xa33a, 0xb2b3,
0x4a44, 0x5bcd, 0x6956, 0x78df, 0x0c60, 0x1de0, 0x2f72, 0x3cfa,
0xd68d, 0xc704, 0xf59f, 0xe416, 0x90a9, 0x8110, 0x7221, 0x6332,
0x5ac5, 0x4b4c, 0x79d7, 0x685e, 0x1ce1, 0x0d00, 0xfef1, 0xede2,
0xe70e, 0xf687, 0xc41c, 0xd595, 0xa12a, 0xb03b, 0xc14c, 0xd25d,
0x6b46, 0x7acf, 0x4854, 0x59dd, 0x2d62, 0x3e73, 0x4f84, 0x5095,
0xf78f, 0xe606, 0xd49d, 0xc514, 0xb1ab, 0xa0bc, 0x91cd, 0x82de,
0x7bc7, 0x6a4e, 0x58d5, 0x495c, 0x3de3, 0x2ef4, 0x1f05, 0x0e16, 0x1727, 0x0838, 0x1949, 0x0a5a, 0x1b6b, 0x0c7c, 0x1d8d, 0x0e9e, 0x1fa, 0x00b1, 0x01c2, 0x02d3, 0x03e4, 0x04f5, 0x0606, 0x0717, 0x0828, 0x0939, 0x0a4a, 0x0b5b, 0x0c6c, 0x0d7d, 0x0e8e, 0x0f9f, 0x1010, 0x1121, 0x1232, 0x1343, 0x1454, 0x1565, 0x1676, 0x1787, 0x1898, 0x19a9, 0x1ab, 0x1bc, 0x1cd, 0x1de, 0x1ef, 0x1ff, 0x200, 0x201, 0x202, 0x203, 0x204, 0x205, 0x206, 0x207, 0x208, 0x209, 0x20a, 0x20b, 0x20c, 0x20d, 0x20e, 0x20f, 0x210, 0x211, 0x212, 0x213, 0x214, 0x215, 0x216, 0x217, 0x218, 0x219, 0x21a, 0x21b, 0x21c, 0x21d, 0x21e, 0x21f, 0x220, 0x221, 0x222, 0x223, 0x224, 0x225, 0x226, 0x227, 0x228, 0x229, 0x22a, 0x22b, 0x22c, 0x22d, 0x22e, 0x22f, 0x230, 0x231, 0x232, 0x233, 0x234, 0x235, 0x236, 0x237, 0x238, 0x239, 0x23a, 0x23b, 0x23c, 0x23d, 0x23e, 0x23f, 0x240, 0x241, 0x242, 0x243, 0x244, 0x245, 0x246, 0x247, 0x248, 0x249, 0x24a, 0x24b, 0x24c, 0x24d, 0x24e, 0x24f, 0x250, 0x251, 0x252, 0x253, 0x254, 0x255, 0x256, 0x257, 0x258, 0x259, 0x25a, 0x25b, 0x25c, 0x25d, 0x25e, 0x25f, 0x260, 0x261, 0x262, 0x263, 0x264, 0x265, 0x266, 0x267, 0x268, 0x269, 0x26a, 0x26b, 0x26c, 0x26d, 0x26e, 0x26f, 0x270, 0x271, 0x272, 0x273, 0x274, 0x275, 0x276, 0x277, 0x278, 0x279, 0x27a, 0x27b, 0x27c, 0x27d, 0x27e, 0x27f, 0x280, 0x281, 0x282, 0x283, 0x284, 0x285, 0x286, 0x287, 0x288, 0x289, 0x28a, 0x28b, 0x28c, 0x28d, 0x28e, 0x28f, 0x290, 0x291, 0x292, 0x293, 0x294, 0x295, 0x296, 0x297, 0x298, 0x299, 0x29a, 0x29b, 0x29c, 0x29d, 0x29e, 0x29f, 0x2a0, 0x2a1, 0x2a2, 0x2a3, 0x2a4, 0x2a5, 0x2a6, 0x2a7, 0x2a8, 0x2a9, 0x2aa, 0x2ab, 0x2ac, 0x2ad, 0x2ae, 0x2af, 0x2b0, 0x2b1, 0x2b2, 0x2b3, 0x2b4, 0x2b5, 0x2b6, 0x2b7, 0x2b8, 0x2b9, 0x2ba, 0x2bb, 0x2bc, 0x2bd, 0x2be, 0x2bf, 0x2c0, 0x2c1, 0x2c2, 0x2c3, 0x2c4, 0x2c5, 0x2c6, 0x2c7, 0x2c8, 0x2c9, 0x2ca, 0x2cb, 0x2cc, 0x2cd, 0x2ce, 0x2cf, 0x2d0, 0x2d1, 0x2d2, 0x2d3, 0x2d4, 0x2d5, 0x2d6, 0x2d7, 0x2d8, 0x2d9, 0x2da, 0x2db, 0x2dc, 0x2dd, 0x2de, 0x2df, 0x2e0, 0x2e1, 0x2e2, 0x2e3, 0x2e4, 0x2e5, 0x2e6, 0x2e7, 0x2e8, 0x2e9, 0x2ea, 0x2eb, 0x2ec, 0x2ed, 0x2ee, 0x2ef, 0x2f0, 0x2f1, 0x2f2, 0x2f3, 0x2f4, 0x2f5, 0x2f6, 0x2f7, 0x2f8, 0x2f9, 0x2fa, 0x2fb, 0x2fc, 0x2fd, 0x2fe, 0x2ff, 0x300, 0x301, 0x302, 0x303, 0x304, 0x305, 0x306, 0x307, 0x308, 0x309, 0x30a, 0x30b, 0x30c, 0x30d, 0x30e, 0x30f, 0x310, 0x311, 0x312, 0x313, 0x314, 0x315, 0x316, 0x317, 0x318, 0x319, 0x31a, 0x31b, 0x31c, 0x31d, 0x31e, 0x31f, 0x320, 0x321, 0x322, 0x323, 0x324, 0x325, 0x326, 0x327, 0x328, 0x329, 0x32a, 0x32b, 0x32c, 0x32d, 0x32e, 0x32f, 0x330, 0x331, 0x332, 0x333, 0x334, 0x335, 0x336, 0x337, 0x338, 0x339, 0x33a, 0x33b, 0x33c, 0x33d, 0x33e, 0x33f, 0x340, 0x341, 0x342, 0x343, 0x344, 0x345, 0x346, 0x347, 0x348, 0x349, 0x34a, 0x34b, 0x34c, 0x34d, 0x34e, 0x34f, 0x350, 0x351, 0x352, 0x353, 0x354, 0x355, 0x356, 0x357, 0x358, 0x359, 0x35a, 0x35b, 0x35c, 0x35d, 0x35e, 0x35f, 0x360, 0x361, 0x362, 0x363, 0x364, 0x365, 0x366, 0x367, 0x368, 0x369, 0x36a, 0x36b, 0x36c, 0x36d, 0x36e, 0x36f, 0x370, 0x371, 0x372, 0x373, 0x374, 0x375, 0x376, 0x377, 0x378, 0x379, 0x37a, 0x37b, 0x37c, 0x37d, 0x37e, 0x37f, 0x380, 0x381, 0x382, 0x383, 0x384, 0x385, 0x386, 0x387, 0x388, 0x389, 0x38a, 0x38b, 0x38c, 0x38d, 0x38e, 0x38f, 0x390, 0x391, 0x392, 0x393, 0x394, 0x395, 0x396, 0x397, 0x398, 0x399, 0x39a, 0x39b, 0x39c, 0x39d, 0x39e, 0x39f, 0x3a0, 0x3a1, 0x3a2, 0x3a3, 0x3a4, 0x3a5, 0x3a6, 0x3a7, 0x3a8, 0x3a9, 0x3aa, 0x3ab, 0x3ac, 0x3ad, 0x3ae, 0x3af, 0x3b0, 0x3b1, 0x3b2, 0x3b3, 0x3b4, 0x3b5, 0x3b6, 0x3b7, 0x3b8, 0x3b9, 0x3ba, 0x3bb, 0x3bc, 0x3bd, 0x3be, 0x3bf, 0x3c0, 0x3c1, 0x3c2, 0x3c3, 0x3c4, 0x3c5, 0x3c6, 0x3c7, 0x3c8, 0x3c9, 0x3ca, 0x3cb, 0x3cc, 0x3cd, 0x3ce, 0x3cf, 0x3d0, 0x3d1, 0x3d2, 0x3d3, 0x3d4, 0x3d5, 0x3d6, 0x3d7, 0x3d8, 0x3d9, 0x3da, 0x3db, 0x3dc, 0x3dd, 0x3de, 0x3df, 0x3e0, 0x3e1, 0x3e2, 0x3e3, 0x3e4, 0x3e5, 0x3e6, 0x3e7, 0x3e8, 0x3e9, 0x3ea, 0x3eb, 0x3ec, 0x3ed, 0x3ee, 0x3ef, 0x3f0, 0x3f1, 0x3f2, 0x3f3, 0x3f4, 0x3f5, 0x3f6, 0x3f7, 0x3f8, 0x3f9, 0x3fa, 0x3fb, 0x3fc, 0x3fd, 0x3fe, 0x3ff, 0x400, 0x401, 0x402, 0x403, 0x404, 0x405, 0x406, 0x407, 0x408, 0x409, 0x40a, 0x40b, 0x40c, 0x40d, 0x40e, 0x40f, 0x410, 0x411, 0x412, 0x413, 0x414, 0x415, 0x416, 0x417, 0x418, 0x419, 0x41a, 0x41b, 0x41c, 0x41d, 0x41e, 0x41f, 0x420, 0x421, 0x422, 0x423, 0x424, 0x425, 0x426, 0x427, 0x428, 0x429, 0x42a, 0x42b, 0x42c, 0x42d, 0x42e, 0x42f, 0x430, 0x431, 0x432, 0x433, 0x434, 0x435, 0x436, 0x437, 0x438, 0x439, 0x43a, 0x43b, 0x43c, 0x43d, 0x43e, 0x43f, 0x440, 0x441, 0x442, 0x443, 0x444, 0x445, 0x446, 0x447, 0x448, 0x449, 0x44a, 0x44b, 0x44c, 0x44d, 0x44e, 0x44f, 0x450, 0x451, 0x452, 0x453, 0x454, 0x455, 0x456, 0x457, 0x458, 0x459, 0x45a, 0x45b, 0x45c, 0x45d, 0x45e, 0x45f, 0x460, 0x461, 0x462, 0x463, 0x464, 0x465, 0x466, 0x467, 0x468, 0x469, 0x46a, 0x46b, 0x46c, 0x46d, 0x46e, 0x46f, 0x470, 0x471, 0x472, 0x473, 0x474, 0x475, 0x476, 0x477, 0x478, 0x479, 0x47a, 0x47b, 0x47c, 0x47d, 0x47e, 0x47f, 0x480, 0x481, 0x482, 0x483, 0x484, 0x485, 0x486, 0x487, 0x488, 0x489, 0x48a, 0x48b, 0x48c, 0x48d, 0x48e, 0x48f, 0x490, 0x491, 0x492, 0x493, 0x494, 0x495, 0x496, 0x497, 0x498, 0x499, 0x49a, 0x49b, 0x49c, 0x49d, 0x49e, 0x49f, 0x4a0, 0x4a1, 0x4a2, 0x4a3, 0x4a4, 0x4a5, 0x4a6, 0x4a7, 0x4a8, 0x4a9, 0x4aa, 0x4ab, 0x4ac, 0x4ad, 0x4ae, 0x4af, 0x4b0, 0x4b1, 0x4b2, 0x4b3, 0x4b4, 0x4b5, 0x4b6, 0x4b7, 0x4b8, 0x4b9, 0x4ba, 0x4bb, 0x4bc, 0x4bd, 0x4be, 0x4bf, 0x4c0, 0x4c1, 0x4c2, 0x4c3, 0x4c4, 0x4c5, 0x4c6, 0x4c7, 0x4c8, 0x4c9, 0x4ca, 0x4cb, 0x4cc, 0x4cd, 0x4ce, 0x4cf, 0x4d0, 0x4d1, 0x4d2, 0x4d3, 0x4d4, 0x4d5, 0x4d6, 0x4d7, 0x4d8, 0x4d9, 0x4da, 0x4db, 0x4dc, 0x4dd, 0x4de, 0x4df, 0x4e0, 0x4e1, 0x4e2, 0x4e3, 0x4e4, 0x4e5, 0x4e6, 0x4e7, 0x4e8, 0x4e9, 0x4ea, 0x4eb, 0x4ec, 0x4ed, 0x4ee, 0x4ef, 0x4f0, 0x4f1, 0x4f2, 0x4f3, 0x4f4, 0x4f5, 0x4f6, 0x4f7, 0x4f8, 0x4f9, 0x4fa, 0x4fb, 0x4fc, 0x4fd, 0x4fe, 0x4ff, 0x500, 0x501, 0x502, 0x503, 0x504, 0x505, 0x506, 0x507, 0x508, 0x509, 0x50a, 0x50b, 0x50c, 0x50d, 0x50e, 0x50f, 0x510, 0x511, 0x512, 0x513, 0x514, 0x515, 0x516, 0x517, 0x518, 0x519, 0x51a, 0x51b, 0x51c, 0x51d, 0x51e, 0x51f, 0x520, 0x521, 0x522, 0x523, 0x524, 0x525, 0x526, 0x527, 0x528, 0x529, 0x52a, 0x52b, 0x52c, 0x52d, 0x52e, 0x52f, 0x530, 0x531, 0x532, 0x533, 0x534, 0x535, 0x536, 0x537, 0x538, 0x539, 0x53a, 0x53b, 0x53c, 0x53d, 0x53e, 0x53f, 0x540, 0x541, 0x542, 0x543, 0x544, 0x545, 0x546, 0x547, 0x548, 0x549, 0x54a, 0x54b, 0x54c, 0x54d, 0x54e, 0x54f, 0x550, 0x551, 0x552, 0x553, 0x554, 0x555, 0x556, 0x557, 0x558, 0x559, 0x55a, 0x55b, 0x55c, 0x55d, 0x55e, 0x55f, 0x560, 0x561, 0x562, 0x563, 0x564, 0x565, 0x566, 0x567, 0x568, 0x569, 0x56a, 0x56b, 0x56c, 0x56d, 0x56e, 0x56f, 0x570, 0x571, 0x572, 0x573, 0x574, 0x575, 0x576, 0x577, 0x578, 0x579, 0x57a, 0x57b, 0x57c, 0x57d, 0x57e, 0x57f, 0x580, 0x581, 0x582, 0x583, 0x584, 0x585, 0x586, 0x587, 0x588, 0x589, 0x58a, 0x58b, 0x58c, 0x58d, 0x58e, 0x58f, 0x590, 0x591, 0x592, 0x593, 0x594, 0x595, 0x596, 0x597, 0x598, 0x599, 0x59a, 0x59b, 0x59c, 0x59d, 0x59e, 0x59f, 0x5a0, 0x5a1, 0x5a2, 0x5a3, 0x5a4, 0x5a5, 0x5a6, 0x5a7, 0x5a8, 0x5a9, 0x5aa, 0x5ab, 0x5ac, 0x5ad, 0x5ae, 0x5af, 0x5b0, 0x5b1, 0x5b2, 0x5b3, 0x5b4, 0x5b5, 0x5b6, 0x5b7, 0x5b8, 0x5b9, 0x5ba, 0x5bb, 0x5bc, 0x5bd, 0x5be, 0x5bf, 0x5c0, 0x5c1, 0x5c2, 0x5c3, 0x5c4, 0x5c5, 0x5c6, 0x5c7, 0x5c8, 0x5c9, 0x5ca, 0x5cb, 0x5cc, 0x5cd, 0x5ce, 0x5cf, 0x5d0, 0x5d1, 0x5d2, 0x5d3, 0x5d4, 0x5d5, 0x5d6, 0x5d7, 0x5d8, 0x5d9, 0x5da, 0x5db, 0x5dc, 0x5dd, 0x5de, 0x5df, 0x5e0, 0x5e1, 0x5e2, 0x5e3, 0x5e4, 0x5e5, 0x5e6, 0x5e7, 0x5e8, 0x5e9, 0x5ea, 0x5eb, 0x5ec, 0x5ed, 0x5ee, 0x5ef, 0x5f0, 0x5f1, 0x5f2, 0x5f3, 0x5f4, 0x5f5, 0x5f6, 0x5f7, 0x5f8, 0x5f9, 0x5fa, 0x5fb, 0x5fc, 0x5fd, 0x5fe, 0x5ff, 0x600, 0x601, 0x602, 0x603, 0x604, 0x605, 0x606, 0x607, 0x608, 0x609, 0x60a, 0x60b, 0x60c, 0x60d, 0x60e, 0x60f, 0x610, 0x611, 0x612, 0x613, 0x614, 0x615, 0x616, 0x617, 0x618, 0x619, 0x61a, 0x61b, 0x61c, 0x61d, 0x61e, 0x61f, 0x620, 0x621, 0x622, 0x623, 0x624, 0x625, 0x626, 0x627, 0x628, 0x629, 0x62a, 0x62b, 0x62c, 0x62d, 0x62e, 0x62f, 0x630, 0x631, 0x632, 0x633, 0x634, 0x635, 0x636, 0x637, 0x638, 0x639, 0x63a, 0x63b, 0x63c, 0x63d, 0x63e, 0x63f, 0x640, 0x641, 0x642, 0x643, 0x644, 0x645, 0x646, 0x647, 0x648, 0x649, 0x64a, 0x64b, 0x64c, 0x64d, 0x64e, 0x64f, 0x650, 0x651, 0x652, 0x653, 0x654, 0x655, 0x656, 0x657, 0x658, 0x659, 0x65a, 0x65b, 0x65c, 0x65d, 0x65e, 0x65f, 0x660, 0x661, 0x662, 0x663, 0x664, 0x665, 0x666, 0x667, 0x668, 0x669, 0x66a, 0x66b, 0x66c, 0x66d, 0x66e, 0x66f, 0x670, 0x671, 0x672, 0x673, 0x674, 0x675, 0x676, 0x677, 0x678, 0x679, 0x67a, 0x67b, 0x67c, 0x67d, 0x67e, 0x67f, 0x680, 0x681, 0x682, 0x683, 0x684, 0x685, 0x686, 0x687, 0x688, 0x689, 0x68a, 0x68b, 0x68c, 0x68d, 0x68e, 0x68f, 0x690, 0x691, 0x692, 0x693, 0x694, 0x695, 0x696, 0x697, 0x698, 0x699, 0x69a, 0x69b, 0x69c, 0x69d, 0x69e, 0x69f, 0x6a0, 0x6a1, 0x6a2, 0x6a3, 0x6a4, 0x6a5, 0x6a6, 0x6a7, 0x6a8, 0x6a9, 0x6aa, 0x6ab, 0x6ac, 0x6ad, 0x6ae, 0x6af, 0x6b0, 0x6b1, 0x6b2, 0x6b3, 0x6b4, 0x6b5, 0x6b6, 0x6b7, 0x6b8, 0x6b9, 0x6ba, 0x6bb, 0x6bc, 0x6bd, 0x6be, 0x6bf, 0x6c0, 0x6c1, 0x6c2, 0x6c3, 0x6c4, 0x6c5, 0x6c6, 0x6c7, 0x6c8, 0x6c9, 0x6ca, 0x6cb, 0x6cc, 0x6cd, 0x6ce, 0x6cf, 0x6d0, 0x6d1, 0x6d2, 0x6d3, 0x6d4, 0x6d5, 0x6d6, 0x6d7, 0x6d8, 0x6d9, 0x6da, 0x6db, 0x6dc, 0x6dd, 0x6de, 0x6df, 0x6e0, 0x6e1, 0x6e2, 0x6e3, 0x6e4, 0x6e5, 0x6e6, 0x6e7, 0x6e8, 0x6e9, 0x6ea, 0x6eb, 0x6ec, 0x6ed, 0x6ee, 0x6ef, 0x6f0, 0x6f1, 0x6f2, 0x6f3, 0x6f4, 0x6f5, 0x6f6, 0x6f7, 0x6f8, 0x6f9, 0x6fa, 0x6fb, 0x6fc, 0x6fd, 0x6fe, 0x6ff, 0x700, 0x701, 0x702, 0x703, 0x704, 0x705, 0x706, 0x707, 0x708, 0x709, 0x70a, 0x70b, 0x70c, 0x70d, 0x70e, 0x70f, 0x710, 0x711, 0x712, 0x713, 0x714, 0x715, 0x716, 0x717, 0x718, 0x719, 0x71a, 0x71b, 0x71c, 0x71d, 0x71e, 0x71f, 0x720, 0x721, 0x722, 0x723, 0x724, 0x725, 0x726, 0x727, 0x728, 0x729, 0x72a, 0x72b, 0x72c, 0x72d, 0x72e, 0x72f, 0x730, 0x731, 0x732, 0x733, 0x734, 0x735, 0x736, 0x737, 0x738, 0x739, 0x73a, 0x73b, 0x73c, 0x73d, 0x73e, 0x73f, 0x740, 0x741, 0x742, 0x743, 0x744, 0x745, 0x746, 0x747, 0x748, 0x749, 0x74a, 0x74b, 0x74c, 0x74d, 0x74e, 0x74f, 0x750, 0x751, 0x752, 0x753, 0x754, 0x755, 0x756, 0x757, 0x758, 0x759, 0x75a, 0x75b, 0x75c, 0x75d, 0x75e, 0x75f, 0x760, 0x761, 0x762, 0x763, 0x764, 0x765, 0x766, 0x767, 0x768, 0x769, 0x76a, 0x76b, 0x76c, 0x76d, 0x76e, 0x76f, 0x770, 0x771, 0x772, 0x773, 0x774, 0x775, 0x776, 0x777, 0x778, 0x779, 0x77a, 0x77b, 0x77c, 0x77d, 0x77e, 0x77f, 0x780, 0x781, 0x782, 0x783, 0x784, 0x785, 0x786, 0x787, 0x788, 0x789, 0x78a, 0x78b, 0x78c, 0x78d, 0x78e, 0x78f, 0x790, 0x791, 0x792, 0x793, 0x794, 0x795, 0x796, 0x797, 0x798, 0x799, 0x79a, 0x79b, 0x79c, 0x79d, 0x79e, 0x79f, 0x7a0, 0x7a1, 0x7a2, 0x7a3, 0x7a4, 0x7a5, 0x7a6, 0x7a7, 0x7a8, 0x7a9, 0x7aa, 0x7ab, 0x7ac, 0x7ad, 0x7ae, 0x7af, 0x7b0, 0x7b1, 0x7b2, 0x7b3, 0x7b4, 0x7b5, 0x7b6, 0x7b7, 0x7b8, 0x7b9, 0x7ba, 0x7bb, 0x7bc, 0x7bd, 0x7be, 0x7bf, 0x7c0, 0x7c1, 0x7c2, 0x7c3, 0x7c4, 0x7c5, 0x7c6, 0x7c7, 0x7c8, 0x7c9, 0x7ca, 0x7cb, 0x7cc, 0x7cd, 0x7ce, 0x7cf, 0x7d0, 0x7d1, 0x7d2, 0x7d3, 0x7d4, 0x7d5, 0x7d6, 0x7d7, 0x7d8, 0x7d9, 0x7da, 0x7db, 0x7dc, 0x7dd, 0x7de, 0x7df, 0x7e0, 0x7e1, 0x7e2, 0x7e3, 0x7e4, 0x7e5, 0x7e6, 0x7e7, 0x7e8, 0x7e9, 0x7ea, 0x7eb, 0x7ec, 0x7ed, 0x7ee, 0x7ef, 0x7f0, 0x7f1, 0x7f2, 0x7f3, 0x7f4, 0x7f5, 0x7f6, 0x7f7, 0x7f8, 0x7f9, 0x7fa, 0x7fb, 0x7fc, 0x7fd, 0x7fe, 0x7ff, 0x800, 0x801, 0x802, 0x803, 0x804, 0x805, 0x806, 0x807, 0x808, 0x809, 0x80a, 0x80b, 0x80c, 0x80d, 0x80e, 0x80f, 0x810, 0x811, 0x812, 0x813, 0x814, 0x815, 0x816, 0x817, 0x818, 0x819, 0x81a, 0x81b, 0x81c, 0x81d, 0x81e, 0x81f, 0x820, 0x821, 0x822, 0x823, 0x824, 0x825, 0x826, 0x827, 0x828, 0x829, 0x82a, 0x82b, 0x82c, 0x82d, 0x82e, 0x82f, 0x830, 0x831, 0x832, 0x833, 0x834, 0x835, 0x836, 0x837, 0x838, 0x839, 0x83a, 0x83b, 0x83c, 0x83d, 0x83e, 0x83f, 0x840, 0x841, 0x842, 0x843, 0x844, 0x845, 0x846, 0x847, 0x848, 0x849, 0x84a, 0x84b, 0x84c, 0x8
```


蓝牙安全架构

BlueEye蓝牙固件分析



蓝牙芯片方案



蓝牙OTA签名



Mac	Name	ChipType	Sign	FrameCtrl	Time
小米	电动牙刷	Nordic	有效签名	3031	10:09:53
:F7:67:1D	内69			3040	10:10:03
:EF:21:DF	空气检测			3030	10:10:03
:00:4C:F5	甲醛监测	可解压	没有签名	2050	10:10:02
:34:6A:BF	温湿度计	Nordic	无效签名	2050	10:10:03
:5E:87:FC	湿度计2	Telink	无效签名	3070	10:09:49
:80:58:F1	温湿度计	Dialog	无效签名	2070	10:10:03
:6F:E7:E6	能金属旅行	Dialog	无效签名	2031	10:10:01
:86:F1:2F	电水壶	未知固件	没有签名	2071	10:10:00
:C4:09:43	电动牙刷	Nordic	有效签名	3031	10:09:55
:88:5B:22	智能运动手	没有提供固件	没有签名	2230	10:10:03
:A7:A7:76	保管箱	Nordic	有效签名	4010	10:09:57
:AD:53:58	湿度计2	Telink	无效签名	3070	10:10:01
:34:B0:F6	湿度计2	Telink	无效签名	5830	10:10:00
:00:00:31	子温湿度计	Dialog	无效签名	2270	10:10:03
:75:D5:36	电动牙刷	Nordic	有效签名	3031	10:09:49
:A1:63:A0	湿度计2	Telink	无效签名	5830	10:09:58
:FD:6E:DF	声波电动	Nordic	有效签名	3031	10:09:51

BlueEye蓝牙审计工具
 扫描附近蓝牙产品
 分析设备芯片型号
 嗅探蓝牙广播数据
 测试芯片控制指令

Packet Log			
time	mac	data	parsedata
10:10:03	:F7:67:1D	0110020100	
10:10:03	:34:6A:BF	0d1004ef001301	TEMP:23.9&HUMIDITY:27.5
10:10:03	:80:58:F1	090610024a01	
10:10:02	:F7:67:1D	0110020100	
10:10:02	:F7:67:1D	0110020100	
10:10:01	:F7:67:1D	0110020100	
10:10:01	:AD:53:58	090610023601	
10:10:01	:00:4C:F5	0610024601	HUMIDITY:32.6
10:10:01	:F7:67:1D	0110020100	
10:10:01	:34:6A:BF	0a10015d	BATTERY:93
10:10:00	:F7:67:1D	0110020100	
10:10:00	:F7:67:1D	0110020100	
10:10:00	:00:4C:F5	1010020100	HCHO:0.01
10:10:00	:86:F1:2F	090510020054	
10:09:59	:F7:67:1D	0110020100	

OTA D4:28:1C:F7:67:1D

Select Chip 1:Nordic 2:Dialog 3:Airoha 4:Telink

BlueEye蓝牙审计框架



蓝牙认证体系





参考链接

https://github.com/hexway/apple_bleee

<https://www.armis.com/bleedingbit/>

https://e2echina.ti.com/question_answer/wireless_connectivity/bluetooth/f/103/t/164971

<https://iot.mi.com/new/guide.html?file=04-嵌入式开发指南/06-BLE产品接入/05-米家BLE MiBeacon协议>

<https://www.pentestpartners.com/security-blog/nrf51822-code-readout-protection-bypass-a-how-to>



Thanks