

第十五届CCFC计算机取证技术峰会暨展会

THE 15TH CHINA COMPUTER FORENSIC CONFERENCE & EXHIBITION

■ 电子数据取证技术最新发展与应用 ■

2019.11.5 -11.7

武汉市·荷田大酒店

智能门锁破解实战

Light & 胡一米 @ PwnMonkeyLab

胖猴实验室 (PwnMonkey Security Lab)

专注于互联网和物联网的前沿安全攻防技术研究，成立于2015年，目前研究方向主要为智能门锁、近场通信方向



CNNVD-201709-133

CNNVD-201810-1628

.....

CVE-2017-14262

CVE-2019-17627

.....

☰ E pwn@pwnmonkey.org



CONTENTS

1

智能门锁介绍

2

智能门锁通信架构

3

智能门锁攻击演示

4

总结及展望

PART ONE

智能门锁介绍

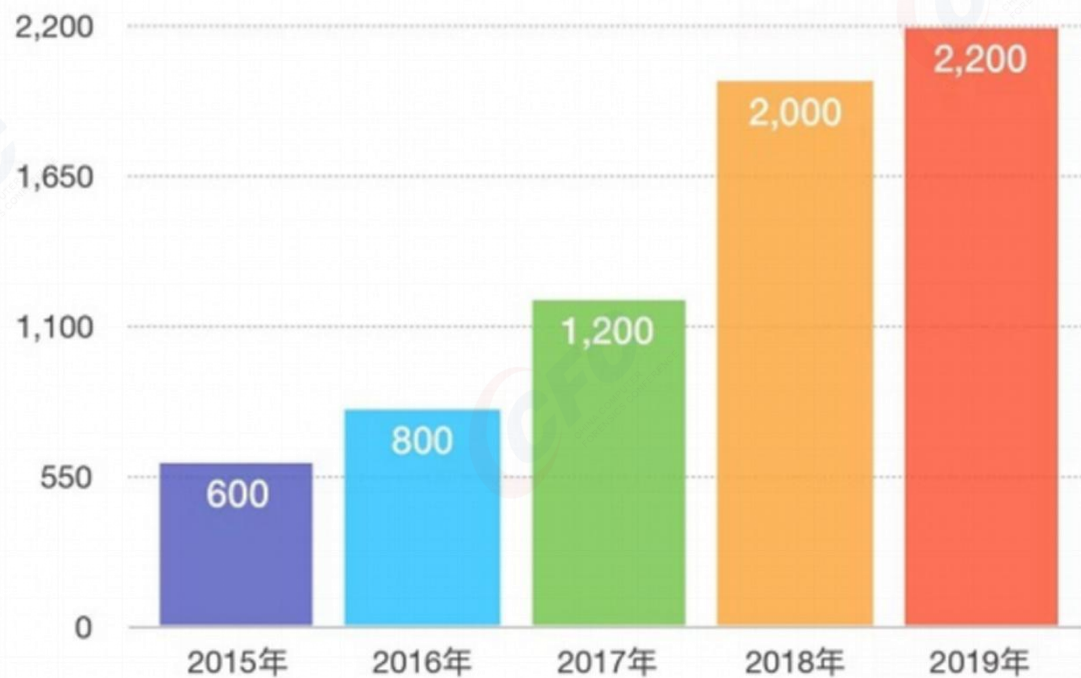


迅速发展中的智能门锁行业

中国智能锁产销量增长示意图（单位万套）



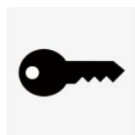
中国智能锁企业数量增长示意图（单位：个）





智能门锁介绍

与普通门锁相比，智能门锁具备了更多的开锁方式



钥匙开锁



VS



密码开锁



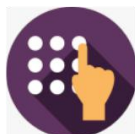
指纹开锁



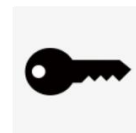
门禁卡开锁



手机开锁



密码开锁



钥匙开锁

...

15TH

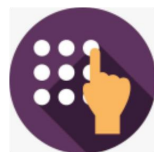
CHINA COMPUTER
FORENSICS CONFERENCE

CFC
CHINA COMPUTER
FORENSICS CONFERENCE



智能门锁介绍

在更加实用和便捷的同时
是否也更加安全了呢？



密码开锁

密码泄露



指纹开锁

指纹膜



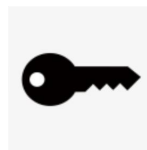
手机开锁

通信监听



门禁卡开锁

卡片复制



钥匙开锁

开锁工具

PART TWO

智能门锁通信架构



目前，智能门锁主要有两种使用方式

1

通过**手机蓝牙**

实现门锁与用户的直接交互



2

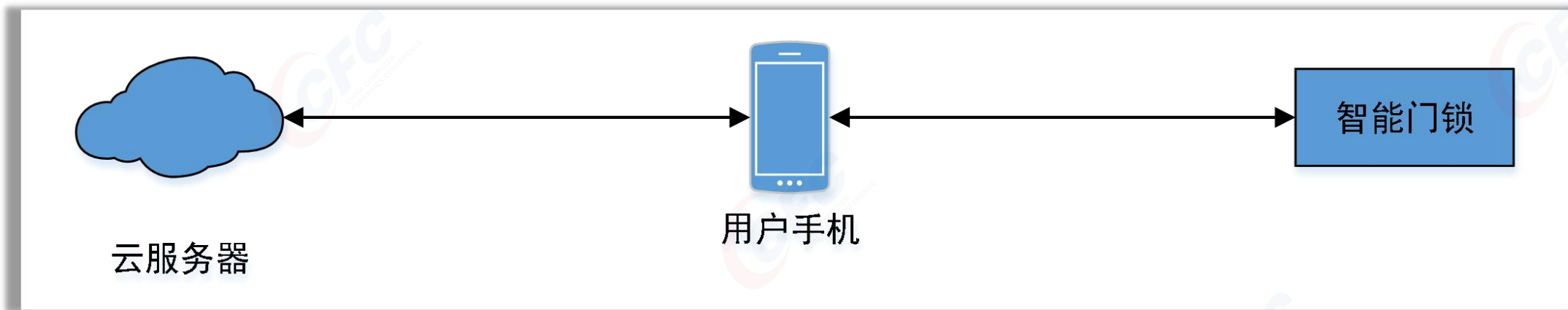
通过**门锁网关**

实现门锁与用户的间接交互



智能门锁通信架构

1 在使用手机蓝牙的通信方式中



手机会直接控制门锁，也会帮助门锁转发信息给云服务器

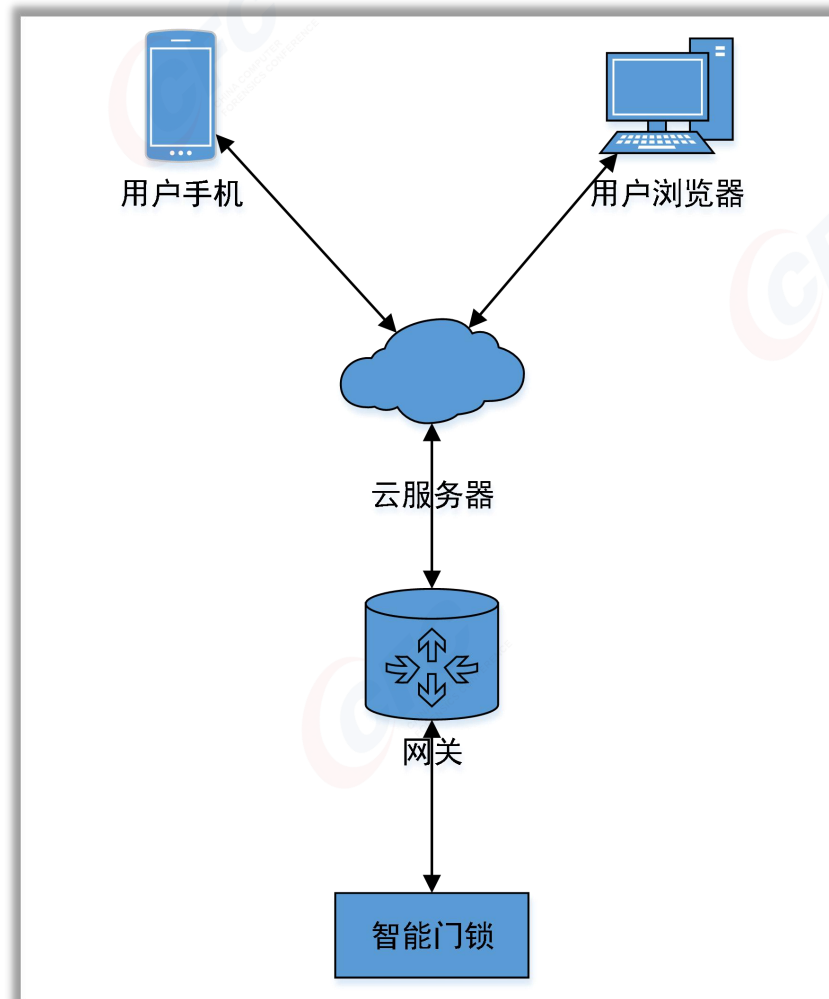


智能门锁通信架构

2

在使用网关的通信方式中

**用户通过手机等，经由云服务器、网关，
间接控制智能门锁**



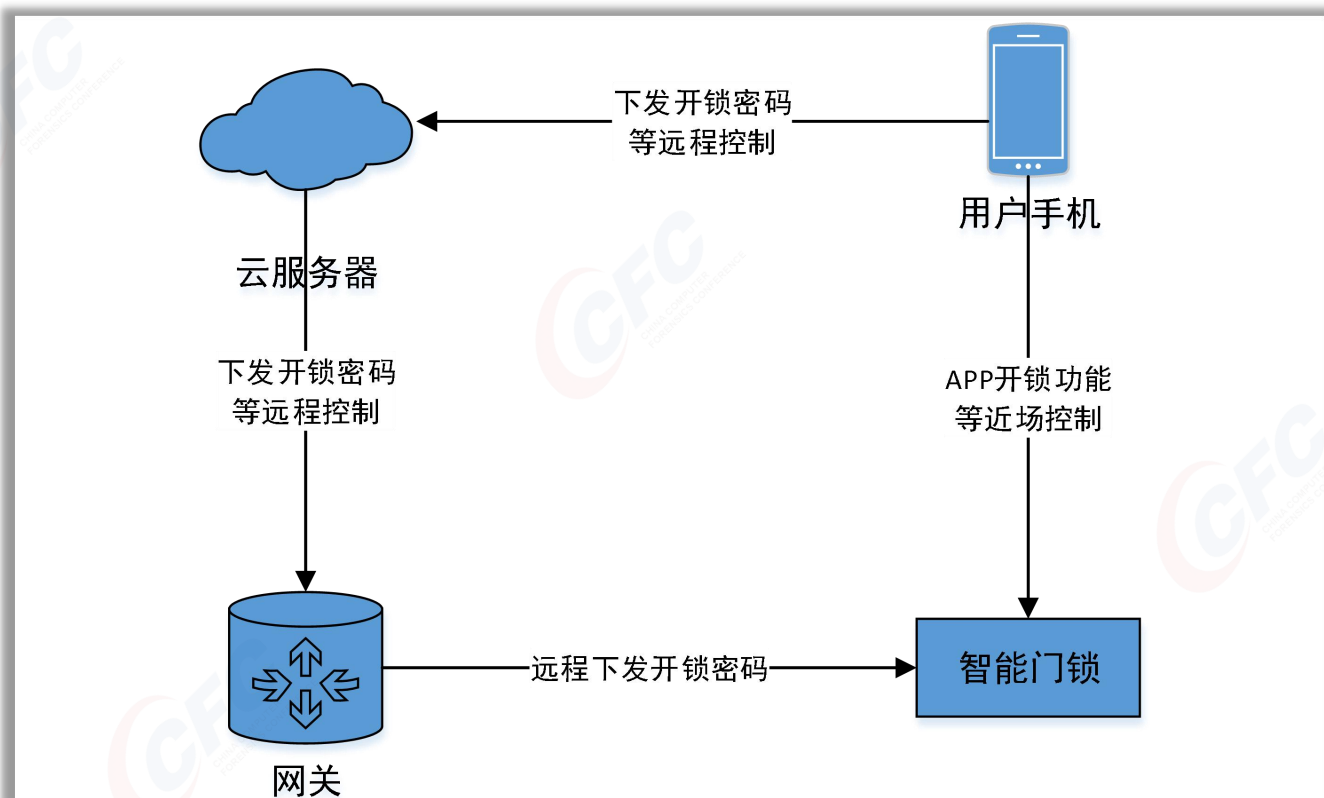
15TH

CHINA COMPUTER
FORENSIC CONFERENCE

CFC
CHINA COMPUTER
FORENSIC CONFERENCE



两种通信架构可能单独使用，也可以结合使用



PART THREE

智能门锁攻击演示



将对如下两种攻击方式进行视频讲解

攻击
演示

1

嗅探手机蓝牙通信
实现非授权开门

攻击
演示

2

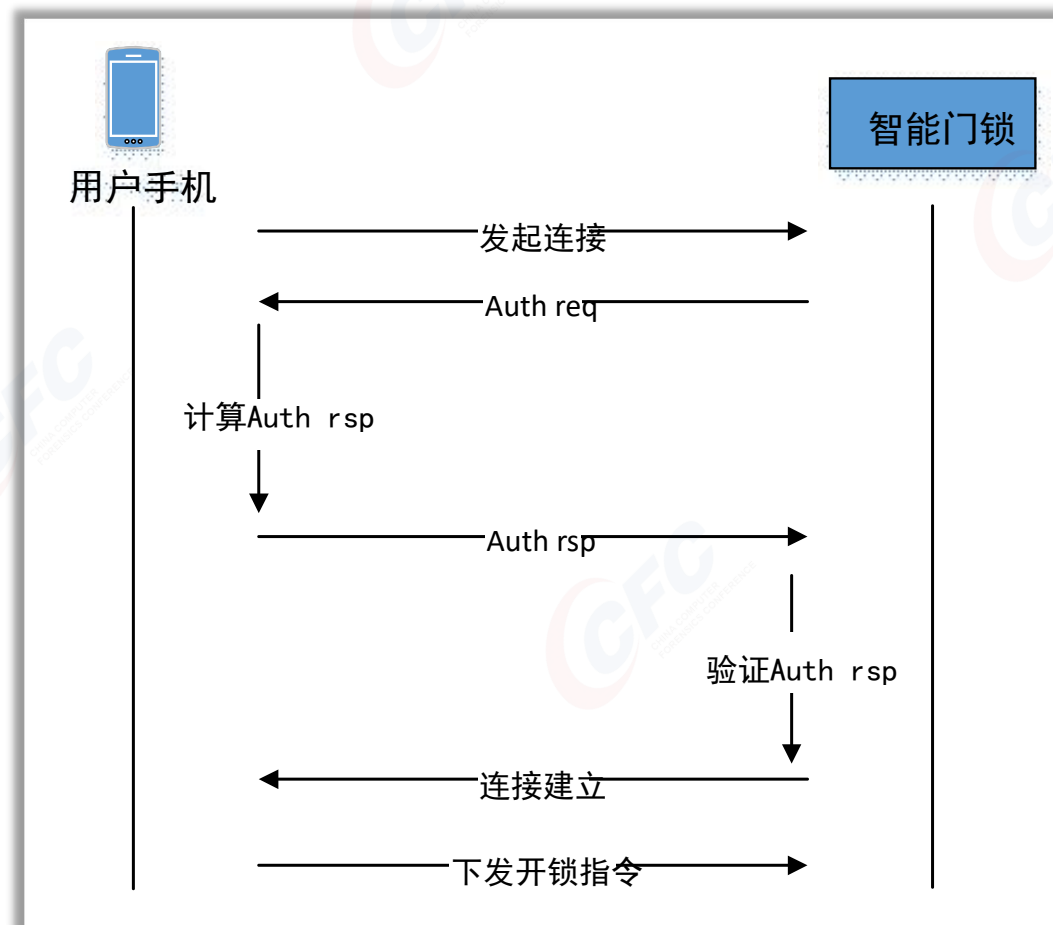
利用网关控制门锁
实现非授权开门



智能门锁攻击演示

1 嗅探手机蓝牙通信实现非授权开门

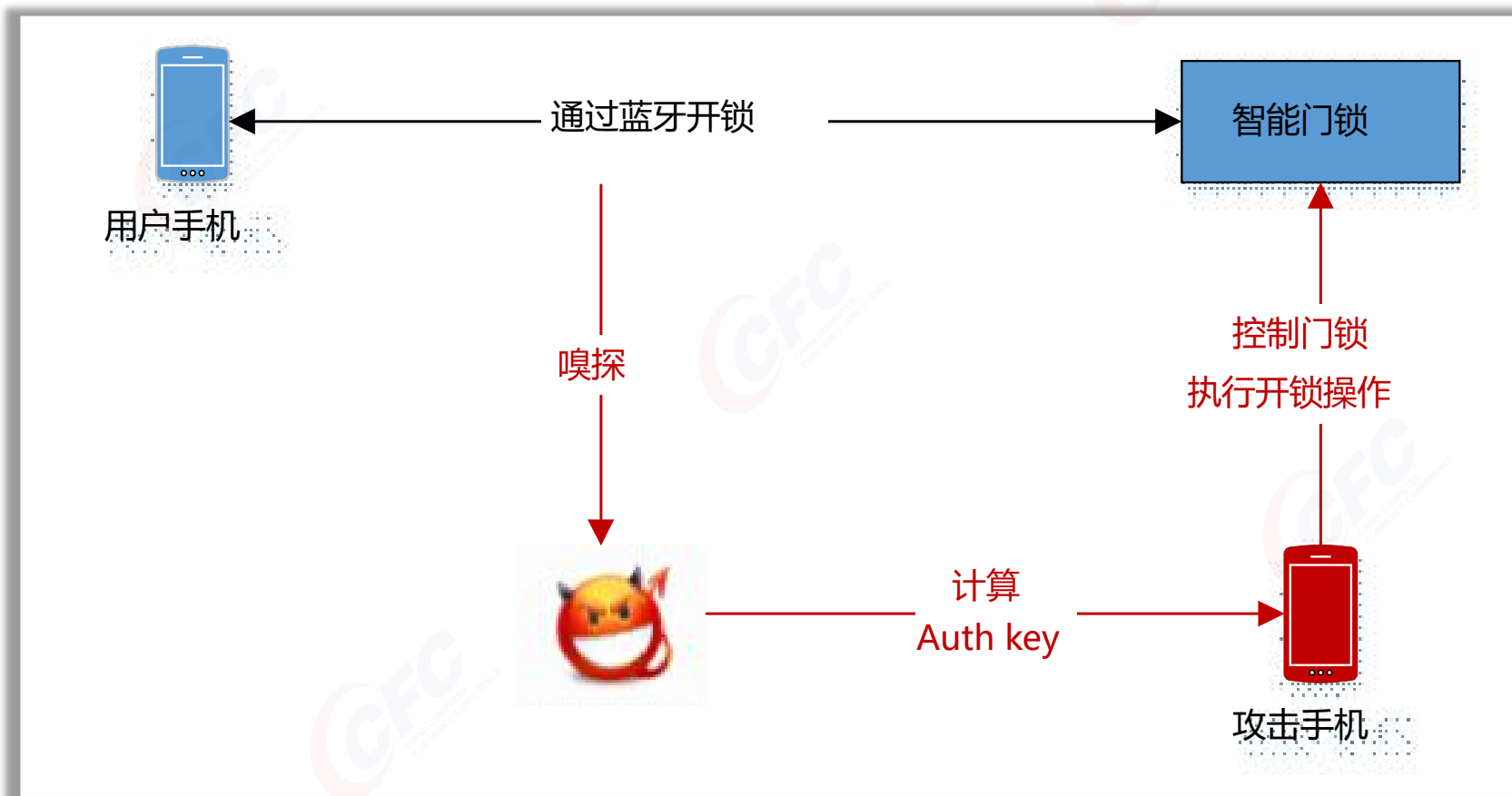
▶ 正常开锁流程





智能门锁攻击演示

► CVE-2019-17627



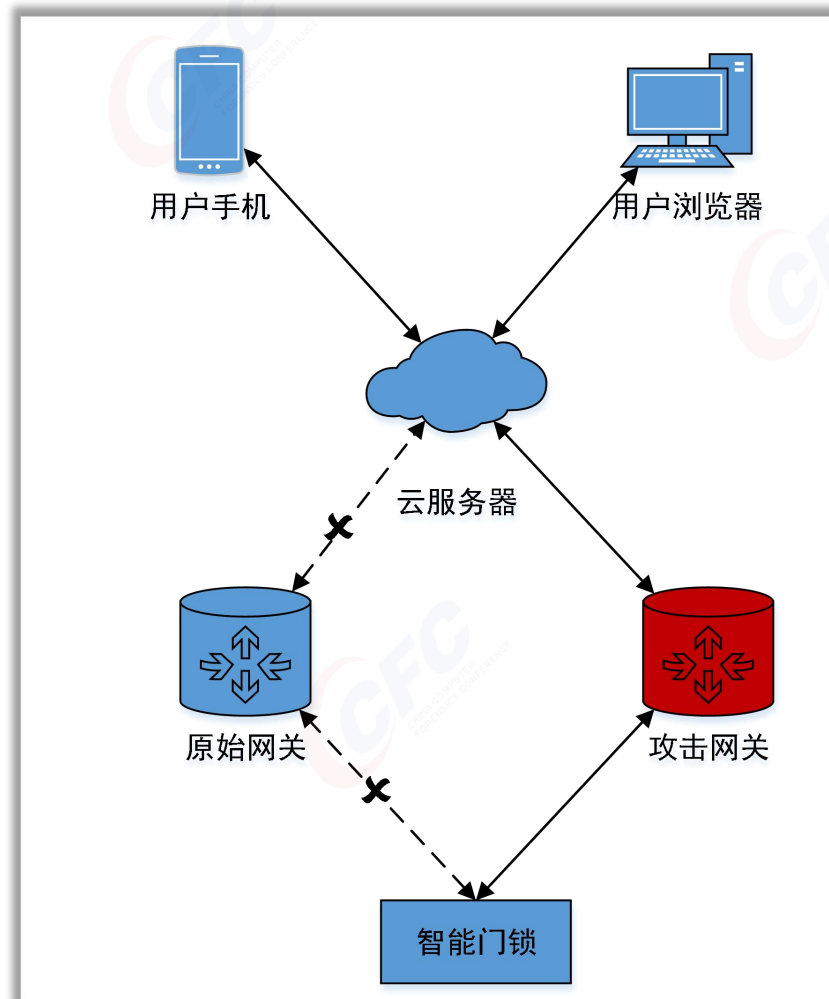


智能门锁攻击演示

2

利用网关控制门锁实现非授权开门

国内某款知名智能门锁，
门锁并未对网关进行认证，
我们可以利用恶意网关发起攻击。

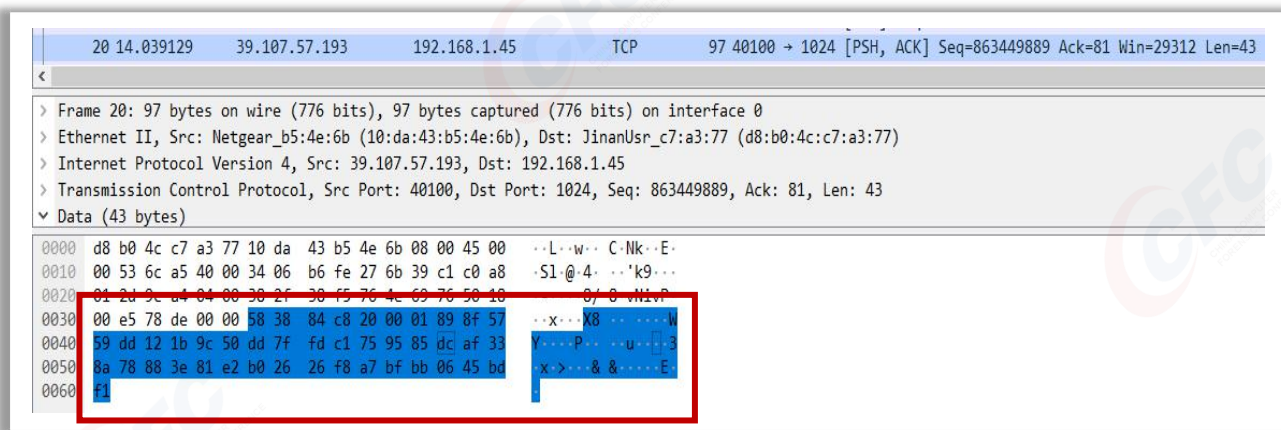




智能门锁攻击演示

分析网关与云服务器的通信

加密密钥：可以直接读取单片机内存获取



数据传输经过了加密

```
1 signed int __fastcall EncryptTxt(int msg, _DWORD secret_key, int msg_len, _WORD *cipher_len)
2 {
3     int v4; // r4
4     signed int v5; // r5
5     unsigned int *v7; // r6
6     signed int i; // r7
7     char v9; // [sp+4h] [bp-42Ch]
8     int v10; // [sp+404h] [bp-2Ch]
9     int v11; // [sp+408h] [bp-28h]
10    int v12; // [sp+40Ch] [bp-24h]
11    _DWORD *v13; // [sp+410h] [bp-20h]
12    int v14; // [sp+414h] [bp-1Ch]
13    _WORD *v15; // [sp+418h] [bp-18h]
14
15    v12 = msg;
16    v13 = secret_key;
17    v14 = msg_len;
18    v15 = cipher_len;
19    v4 = msg_len;
20    MemClr((int)&v9, 0x400);
21    v5 = (((unsigned int)(v4 >> 31) >> 29) + v4) << 13 >> 16;
22    v11 = (unsigned __int16)(v4 % 8);
23    if ( v5 > 0x80 || v5 == 0x80 && v11 )
24        return 1;
25    if ( v11 )
26        v5 = (unsigned __int16)(v5 + 1);
27    v10 = 8 * v5 & 0xFFFF;
28    copy_data((unsigned int)&v9, v12, v4);
29    v7 = (unsigned int *)&v9;
30    for ( i = 0; i < v5; i = (unsigned __int16)(i + 1) )
31    {
32        TeaEncrypt(v7, v13);
33        v7 += 2;
34    }
35    copy_data(v12, (unsigned int)&v9, v10);
36    *v15 = v10;
37    return 0;
38 }
```

加密算法为Tea



智能门锁攻击演示

► 解密后的固件更新命令

心跳数据包

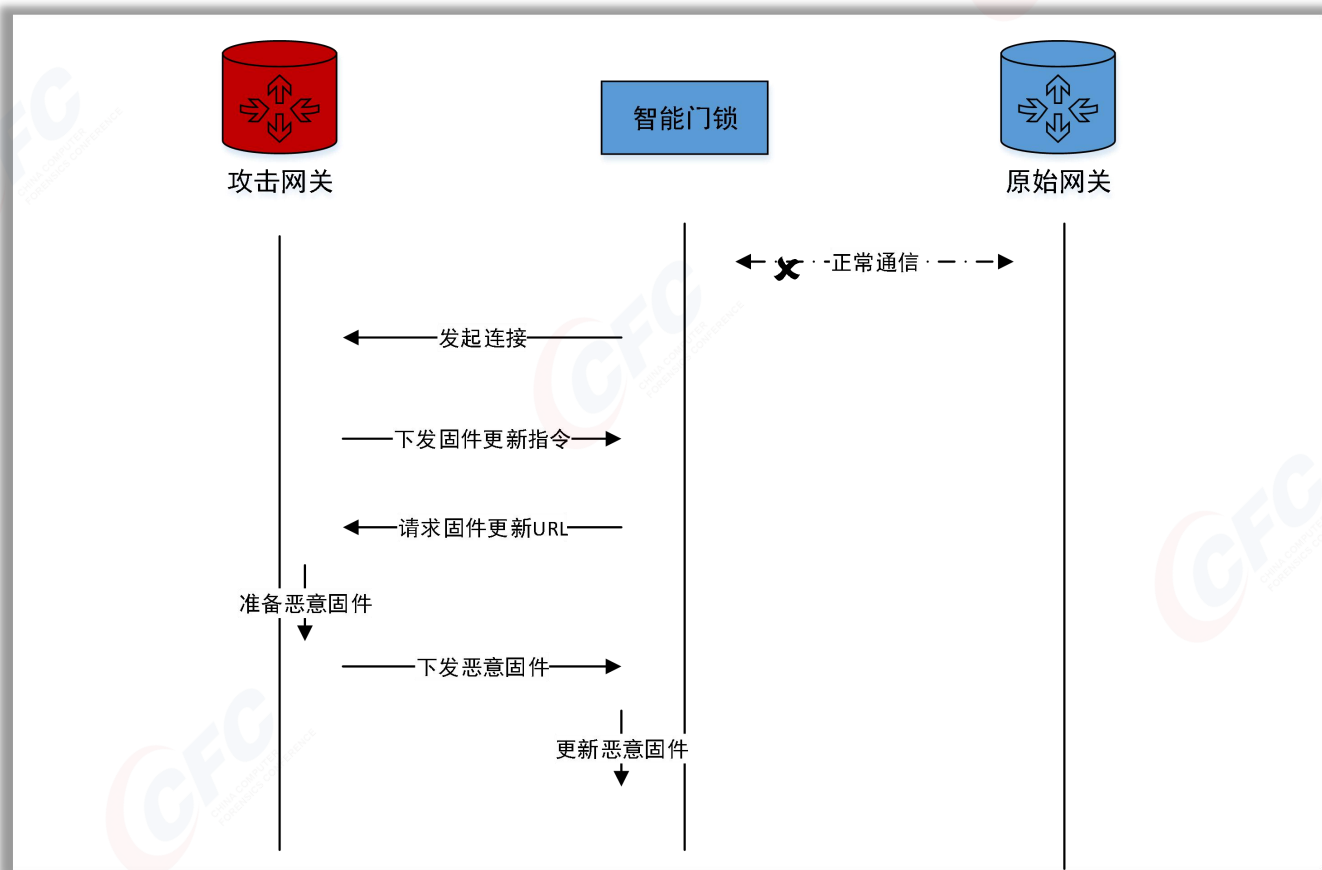
```
Lock -> Server:
58 38 84 C8 0C 00 00 52 0C 7E B6 04 00 00 10 58 00 00 00 00 00 00 00 00 00
Server -> Lock:
58 38 84 C8 0C 00 00 5B 76 2A C7 00 00 00 40 58 00 00 00 00 00 00 00 00 00
Lock -> Server:
58 38 84 C8 0C 00 00 CC 0C D4 7A 04 00 00 10 59 00 00 00 00 00 00 00 00 00
Server -> Lock:
58 38 84 C8 58 00 01 5E 38 5A 3F F3 DA 97 89 82 4F 0C 90 93 23 5D EC F8 EA 92 D6 54 BB F4 91 DE 85 DF FE 56 E0 B5 E3 51 7A 3D FB E8 F5 14 9D 7E BB F7 23 1F 21 5B B0 A7 52 C7 CA 0C A2 03 03 3B AF BD 9C 7E 26 A9 28 1F 2D 9E AC 84
8A AD 82 78 63 16 85 6B 9A 5B 08 D5 61 7B 56 90 EF E6 D9 D9 23 5C 17
Decrypt:
58 38 84 c8 45 00 09 30 81 fc 12 8d 00 33 23 30 00 e9 0f 88 0b 33 68 74 74 70 3a 2f 2f 75 70 67 72 61 64 65 2e 68 75 6f 68 65 74 65 63 68 2e 63 6f 6d 2f 41 32 33 30 2d 53 32 5f 33 5f 30 2d 48 33 5f 33 2d 44 2e 62 69 6e 69 f5 1a
24 52 31 47 d7 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
h t t p : / / u p g r a d e . h u o h e t e c h . c o m / A 2 3 0 - S 2 _ 3 _ 0 - H 3 _ 3 - D . b i n
```

固件的URL



智能门锁攻击演示

► 利用恶意网关给门锁更新恶意固件



PART FOUR

总结及展望

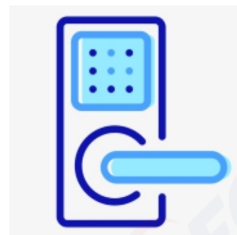
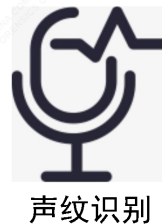


总结及展望

▶ 智能门锁方向

随着功能越来越丰富，

智能门锁面临的安全挑战也将越来越多





总结及展望

► 智能门锁方向



我们对各大厂商智能门锁都做过测评，国内如鹿客、果加、海康等；国外如三星、耶鲁等。

结果并不乐观，绝大多数智能门锁或多或少都存在一些安全问题。

智能门锁作为一类安防产品，更应该注重安全问题。

联系方式：pwn@pwnmonkey.org



THANKS FOR YOUR WATCHING