

无线通讯协议安全分析

VFSec—宋希峰





Part ONE

第一部分

无线安全 概述

无线 \neq 无线Wi-Fi

无线安全 \neq 移动安全

近距离通信

NFC

射频RF

蓝牙

Zigbee

Wi-Fi

远距离通信

移动数据

GPS

Radio

ADS-B

SATCOM

无线安全攻击手段



报文监听

使用频率相同的监听设备对目标无线报文进行收集分析和解密。

劫持攻击

一般通过拒绝服务或者其他干扰方式，将其劫持到一个虚假或者可控制的信号中。

监

重

劫

骗

重放攻击

对无时间戳或无随机性的无线信号进行重放操作

欺骗攻击

结合无线监听及解密，直接构造合法的可通过认证的报文进行欺骗攻击

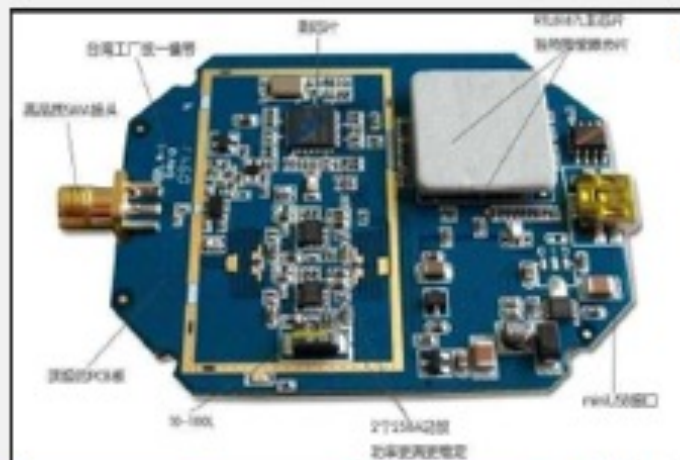


Part Two

第二部分

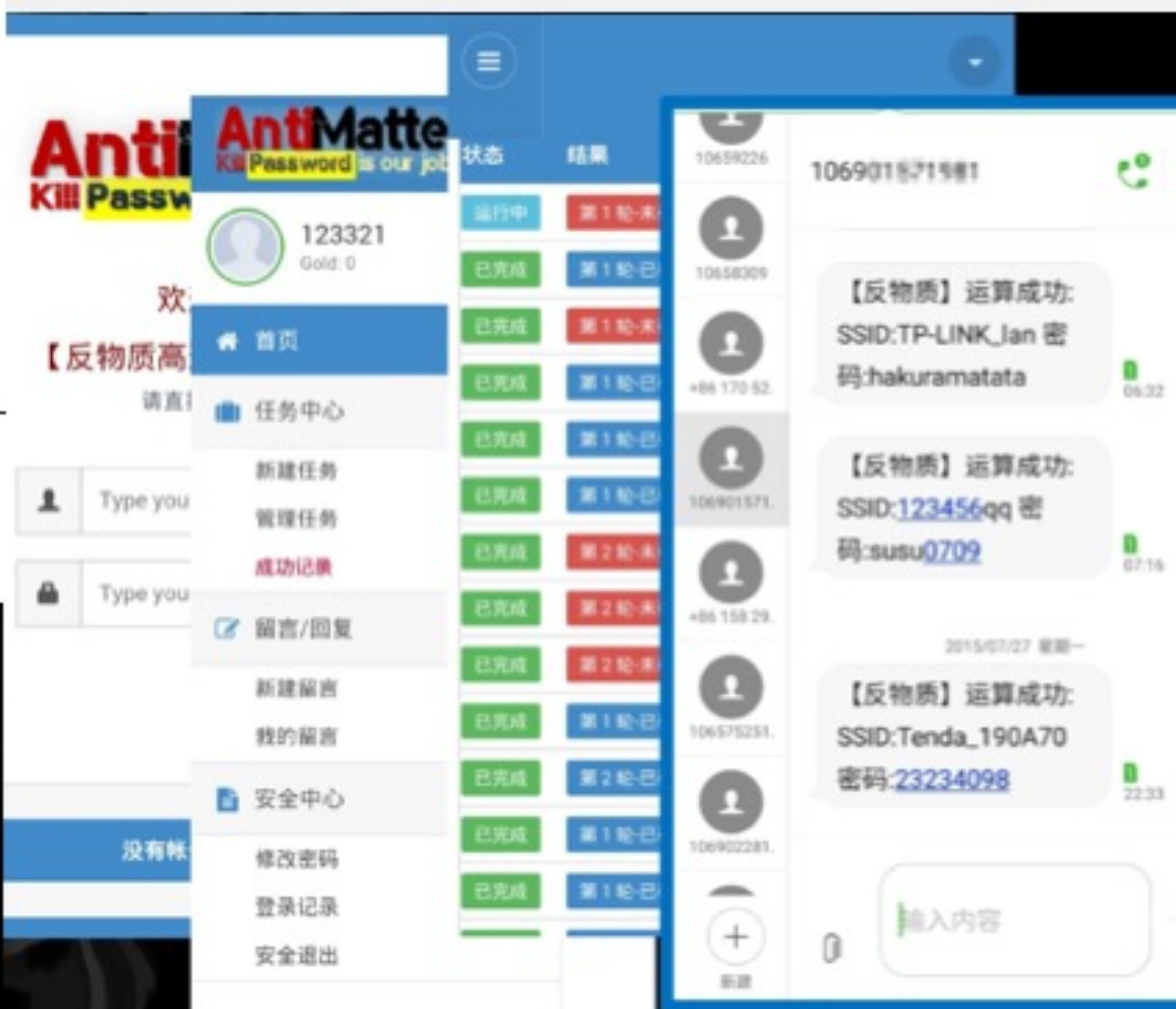
无线Wi-Fi 安全

Part Two 无线Wi-Fi安全



06-07年

08-09年



| 评估类 | 评估项 | 检测内容 |
|----------|---------------|--------------------------|
| 密码安全 | * 弱口令密码测试 | 检测wifi密码是否为弱密码可轻易猜解 |
| | * 暴力破解 | 检测wifi密码是否可被暴力破解 |
| | * 路由管理系统弱口令测试 | 检测路由管理系统是否存在默认账户 |
| 路由系统测试 | * 欺骗性攻击测试 | 检测是否可搭建相同软AP欺骗用户访问链接 |
| | * 路由安全漏洞测试 | 检测已有路由器存在的一些已知的安全风险 |
| 中间人攻击 | * 信息篡改测试 | 篡改通讯数据并重新发送 |
| | * 信息窃取测试 | 截取通讯数据获取账户、密码等敏感数据 |
| | * DNS欺骗测试 | 冒充DNS服务器，实现控制用户访问 |
| | * 会话劫持 | 介于两台机器中间实现通讯数据控制 |
| | * ARP欺骗测试 | 对局域网内交互数据进行嗅探 |
| WEB端管理测试 | * sql注入测试 | 检测参数是否可以进行sql注入攻击 |
| | * 信息泄漏测试 | 检测是否含有敏感信息的url |
| | * 跨站脚本攻击 | 检测是否可以进行xss攻击 |
| | * 用户越权操作 | 检测是否可以非法越权操作 |
| | * 登录接口绕过 | 检测是否可以绕过登录接口 |
| | * 端口开放情况 | 检测服务端各设备、服务器端口开放情况。 |
| 无线网络 | * 接入点端口开放情况 | 检测是否有任何不必要的端口打开 |
| | * DDOS攻击测试 | 检测AP能否承受模拟的802.11 DoS攻击 |
| | * AP默认账号密码测试 | 检测AP是否更改默认管理账号密码 |
| | * 身份验证测试 | 检测是否开启更强身份验证措施如：私钥 |
| | * AP加密测试 | 检测AP采用加密方式，如果为WEP测试破解时长等 |
| | * AP信道测试 | 检测AP是否使用正确的ESSID和信道 |

Demonstration based on the paper



扫一扫，直接在手机上打开



Part Three

第三部分

RFID安全

RFID与NFC
的关系

频段

频段差异：

NFC仅限于13.56MHz高频段，不像RFID有较多频段可选

距离

通讯距离差异：

NFC大多在10厘米以内，而RFID可能扩展到几十米；

模式

工作模式差异：

NFC可被当作射频卡、阅读器或者点对点模式来使用，RFID需要阅读器和标签组成

场景

应用场景差异：

RFID往往运用于生产、物流、资产管理等企业场景，而NFC则更多运用在公交、门禁、手机支付上，更适合普通用户

| | 低頻(LF) | 高頻(HF) | 超高頻(UHF) | 微波(Microwave) | |
|------------|------------------|-------------------------------|-------------------------------|-----------------------------------|------------------------------------|
| 頻率 | 100~500KHz | 10~15MHz | 433~950MHz | 1GHz以上 | |
| 常見頻段 | 125KHz 135KHz | | | | |
| 系統型態 | 被動式 | | | | |
| 全球接受頻率 | 是 | | | | |
| 通訊距離 | 50cm以內 | | | | |
| 傳輸功率 | 72dB μ A/m | | | | |
| 成熟度 | 成熟 | | | | |
| 讀取方式 | 電磁感應 | | | | |
| | | 低頻(LF) | 高頻(HF) | 超高頻(UHF) | 微波(Microwave) |
| 價格 | | 低 | 中 | 高 | 高 |
| 環境影響 | | X | 金屬 | 潮濕 | 潮濕 |
| 資料傳輸率 | | 低 | 高 | 較高 | 最高 |
| 記憶體(Bytes) | | 64~1K | 256~512K | 64~512 | 16~64 |
| ISO對應標準 | | ISO18000-2 Two Type 被動式 | ISO18000-3 Two Mode 被動式 | ISO18000-6 Two Type 被動/半主動式 | ISO18000-4 Two Mode 被動式/半主動式 |
| 應用 | | 門禁系統 動物識別 存貨控制 晶片防盜鎖 | 智慧卡 圖書館管理 商品管理 | 鐵路車廂監控 倉存管理 | 道路收費系統 |

目前RFID攻击方法主要表现在对ID、IC卡本身的攻击。

测试工具：ACR122U、Proxmark3等

对RFID攻击方法总结分为以下5种：

- 1、卡数据窃取
- 2、卡校验绕过(模拟卡)
- 3、卡复制
- 4、卡数据破解与篡改
- 5、终端攻击



IC卡

1)

2)

3)

4)

5)

Proxmark3连接状态: **已连接** ☒ 自动识别串口号 ☐ 手动设置串口号 COM1 关于

低频卡操作区

读ID/MID卡

类型:

卡号:

克隆ID卡

克隆MID卡

读T5xx卡

写T5xx卡

特殊功能

一键自动解析

字典密钥扫描

知一密求全密

默认密码扫描

现场有卡嗅探

读卡类型

天线电压

固件版本

PRNG破解

模拟VID卡

无卡嗅探

修改VID号

修复VID卡

读VID卡全卡到编辑区

清空信息区

清空编辑区

进度:

KEYA: ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐

KEYB: ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐

读取

清除

数据编辑区

新建数据

保存

另存为

对比数据

选择文件

| 扇区 | 块 | 数据 |
|----|----|---------------------------------------|
| 0 | 0 | A273659125080400012D39E108AB051D |
| 0 | 1 | 00000000000000000000000000000000 |
| 0 | 2 | 00000000000000000000000000000000 |
| 0 | 3 | FFFFFFFFFFFFFFFFF078069FFFFFFFFFFFFFF |
| 1 | 4 | 03000100112030201703120101000034 |
| 1 | 5 | B9C8C8B0000000000000004646464646 |
| 1 | 6 | 32020419820806132900201603120023 |
| 1 | 7 | A4896A928F5FFF078069E0AE560FA419 |
| 2 | 8 | 00000000000000000000000000000000 |
| 2 | 9 | 00000000000000000000000000000000 |
| 2 | 10 | 00000000000000000000000000000000 |
| 2 | 11 | A4896A928F5FFF078069E0AE560FA419 |
| 3 | 12 | 03010100000000160312160312170312 |
| 3 | 13 | 00000000FFFFFFFFF000000000F20B2 |
| 3 | 14 | 00000000000000000000000000000000 |
| 3 | 15 | A4896A928F5FFF078069E0AE560FA419 |

显示信息

```

2016/11/28 22:33:13 正在测试该卡是否含有默认密码
2016/11/28 22:33:23 正在进行“知一密求全密”操作
Nested操作结束
0块读取成功
1块读取成功
2块读取成功
3块读取成功
4块读取成功
5块读取成功
6块读取成功

```

原始返回

```

data : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
data : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
trailer: 00 00 00 00 00 00 ff 07 80 69 e0 ae 56 0f a4 19
proxmark3> hf mf rdsc 15 A A4896A928F5F
--sector no:15 key type:A key:a4 89 6a 92 bf 5f

#4# READ SECTOR FINISHED
is0k:01
data : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
data : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
data : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
trailer: 00 00 00 00 00 00 ff 07 80 69 e0 ae 56 0f a4 19

```

高频卡操作

还原有密SSO卡

克隆到有密SSO卡

克隆到空白SSO卡

克隆到VID卡

克隆到

块区操作

块区号: 类型:

密匙:

数据:

读取 ☐ 写入 ☐

块区操作

小工具

转换

☐ 16转10 ☐ 中文转16 ☐ eml转dump

3)

下面是某食堂餐卡被破解后获取到的数据，只有第1扇区存在数据。通过多次充值、消费等数据的对比，得到以下结果：

60块餐卡. dump

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F | 01 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F | | | |
|--------|----|----|----|----|-------|----|----|----|----|----|--------|----|----|----|----|----|----|----|-------------------|---|---|---|---|---|---|---|---|---|---|---|---|--|--|--|
| 0000h: | | | | | 充值前余额 | | | | 62 | 63 | 上次消费日期 | | | | 66 | 67 | 68 | 69 | ž,bâ2...bcdefghi | | | | | | | | | | | | | | | |
| 0010h: | 00 | 00 | 00 | 00 | | | | | 00 | 00 | | | | | 00 | 00 | 00 | 00 | | | | | | | | | | | | | | | | |
| 0020h: | 00 | 00 | 00 | 00 | | | | | 00 | 00 | | | | | 00 | 00 | 00 | 00 | | | | | | | | | | | | | | | | |
| 0030h: | FF | FF | FF | FF | FF | FF | FF | 07 | 80 | 69 | FF | FF | FF | FF | FF | FF | FF | FF | ÿÿÿÿÿÿÿ.€iÿÿÿÿÿÿÿ | | | | | | | | | | | | | | | |
| 0040h: | 1A | 5A | 80 | 99 | 01 | 64 | 00 | 03 | 23 | AE | 01 | FF | FF | 03 | FF | 00 | | | .Z€™.d..#@.ÿÿ.ÿ. | | | | | | | | | | | | | | | |
| 0050h: | 1A | 5A | 80 | 99 | 01 | 58 | 02 | 03 | 23 | AE | 01 | FF | FF | 03 | FF | 00 | | | .Z€™.X..#@.ÿÿ.ÿ. | | | | | | | | | | | | | | | |
| 0060h: | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | | | | | | | | | | | | | | | | |
| 0070h: | | | | | | | | | FF | 07 | 80 | 69 | FF | FF | FF | FF | | | .€iÿÿÿÿÿÿÿ | | | | | | | | | | | | | | | |
| 0080h: | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | | | | | | | | | | | | | | | | | | |

Annotations:

- 充值后余额，当消费后，该值与充值前余额均会变成消费后的余额 (points to 0040h-0050h)
- 检验值 (points to 0040h-0050h)
- 当天消费次数 (points to 0040h-0050h)

1、余
算单位
充值后

2、检
充值后
下方余
省去分

比如我
将上面



其计
10元;

发现在
修改
日期,

以直接

| | | | | | | | | | | | | | |
|--------|----|----|----|----|----|----|----|----|----|----|----|----|---|
| 0040h: | 1A | 5A | 80 | 99 | 01 | 64 | 00 | 03 | 23 | AE | 01 | FF | : |
| 0050h: | 1A | 5A | 80 | 99 | 01 | 00 | 0A | 03 | 23 | AE | 01 | FF | : |



Part Four

第四部分

蓝牙安全

BLE(Bluetooth Low Energy)协议栈



硬件

CSR4.0蓝牙适配器(接收器)

NRF51822开发板 (适合开发 价格适中)

CC2540 USB Dongle (仅支持BLE 价格便宜)

Ubertooth (价格贵)

工具

bluez bluez-utils

lightblue、ble scanner

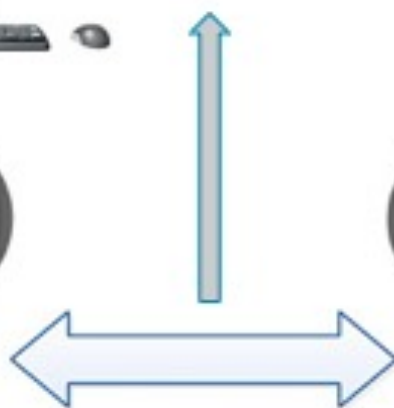
pygatt



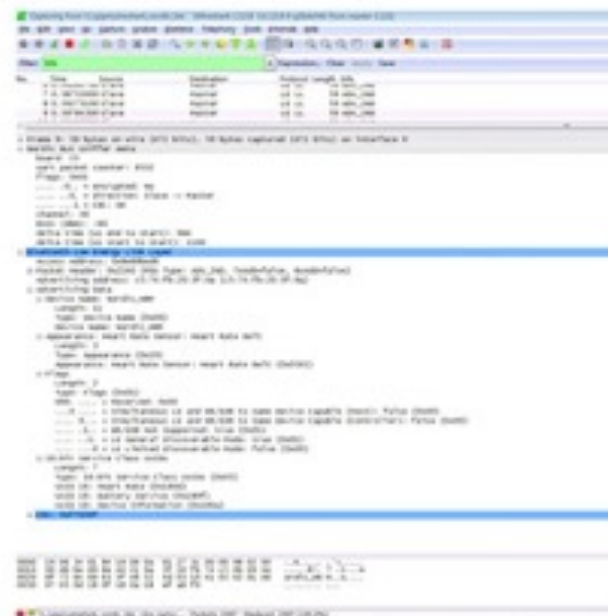
将Dongle连接到计算机的USB接口上
打开Sniffer软件进行抓包和协议分析



Central



Peripheral



Part Four 蓝牙安全

命

设

Wireshark 1.12.8 (x112.8-0-g5b6e541) from master-1.12.7

Filter: **ble** Expression... Clear Apply Save

包列表

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|------------|--------|-------------|----------|--------|---------|
| 6 | 0.000000 | Slave | Master | LE LL | 59 | ADV_IND |
| 7 | 0.38753000 | Slave | Master | LE LL | 59 | ADV_IND |
| 8 | 0.39273100 | Slave | Master | LE LL | 59 | ADV_IND |
| 9 | 0.39764300 | Slave | Master | LE LL | 59 | ADV_IND |

包信息

Frame 9: 59 bytes on wire (472 bits), 59 bytes captured (472 bits) on interface 0

Nordic BLE Sniffer meta

- board: 25
- uart packet counter: 6532
- flags: 0x01
 - ...0... = encrypted: no
 - ...0... = direction: Slave -> Master
 - ...1... = CRC: ok
- channel: 39
- RSSI (dBm): -60
- delta time (us end to start): 664
- delta time (us start to start): 1160

包解析

Bluetooth Low Energy Link Layer

- Access Address: 0x8e89bed6
- Packet Header: 0x2140 (PDU Type: ADV_IND, TxAdd=false, RxAdd=false)
- Advertising Address: c5:74:fb:20:3f:9a (c5:74:fb:20:3f:9a)
- Advertising Data
 - Device Name: Nordic_HRM
 - Length: 11
 - Type: Device Name (0x09)
 - Device Name: Nordic_HRM
 - Appearance: Heart Rate Sensor: Heart Rate Belt
 - Length: 3
 - Type: Appearance (0x19)
 - Appearance: Heart Rate Sensor: Heart Rate Belt (0x0341)
 - Flags
 - Length: 2
 - Type: Flags (0x01)
 - 000... = Reserved: 0x00
 - ...0... = Simultaneous LE and BR/EDR to Same Device Capable (Host): false (0x00)
 - ...0... = Simultaneous LE and BR/EDR to Same Device Capable (Controller): false (0x00)
 - ...1... = BR/EDR not Supported: true (0x01)
 - ...1... = LE General Discoverable Mode: true (0x01)
 - ...0... = LE Limited Discoverable Mode: false (0x00)
 - 16-bit Service Class UUIDs
 - Length: 7
 - Type: 16-bit Service Class UUIDs (0x03)
 - UUID 16: Heart Rate (0x180d)
 - UUID 16: Battery Service (0x180f)
 - UUID 16: Device Information (0x180a)
- CRC: 0xf7650f

包字节

```
0000 19 06 34 01 84 19 06 0a 01 27 3c 00 00 98 02 00  ..4.....'.....
0010 00 06 8e 89 8e 40 21 9a 3f 20 fb 74 c5 0b 09 4e  ....@!..T..E...N
0020 ef 72 64 69 63 5f 48 32 4d 03 19 41 03 02 01 06  ....ordic_HRM.A....
0030 07 03 0d 18 0f 18 0a 18 ef a6 f0  .....
```



```
root@ZerOne: ~ - Shell No. 2 - Konsole <2>
Session Edit View Bookmarks Settings Help

root@ZerOne:~# l2ping -s 40000 00:12:D2:91:34:C8
Ping: 00:12:D2:91:34:C8 from 00:11:67:BE:EB:00 (data size 40000) ...
98 bytes from 00:12:D2:91:34:C8 id 0 time 7489.55ms
98 bytes from 00:12:D2:91:34:C8 id 1 time 7317.64ms
98 bytes from 00:12:D2:91:34:C8 id 2 time 7525.42ms

root@0xroot:~/mousejack/tools# ./nrf24-network-mapper.py -a C6:4A:78:A2:02
2016-03-17 14:33:57.951] Trying address C6:4A:78:A2:00
2016-03-17 14:33:58.572] Trying address C6:4A:78:A2:01
2016-03-17 14:33:58.680] Successful ping of C6:4A:78:A2:01 on channel 15
2016-03-17 14:33:59.197] Trying address C6:4A:78:A2:02
2016-03-17 14:33:59.523] Successful ping of C6:4A:78:A2:02 on channel 44
2016-03-17 14:33:59.819] Trying address C6:4A:78:A2:03
2016-03-17 14:33:59.829] Successful ping of C6:4A:78:A2:03 on channel 2
2016-03-17 14:34:00.432] Trying address C6:4A:78:A2:04
2016-03-17 14:34:01.042] Trying address C6:4A:78:A2:05
2016-03-17 14:34:01.648] Trying address C6:4A:78:A2:06
2016-03-17 14:34:02.256] Trying address C6:4A:78:A2:07
2016-03-17 14:34:02.861] Trying address C6:4A:78:A2:08
2016-03-17 14:34:03.467] Trying address C6:4A:78:A2:09
2016-03-17 14:34:04.076] Trying address C6:4A:78:A2:0A
```



Part Five

第五部分

其他无线 协议

| | 频段 | 制式 |
|-------|--|-----|
| 调频广播 | 87MHz—108MHz | WFM |
| 中波广播 | 526.5kHz—1606.5kHz | AM |
| 短波广播 | 3MHz—30MHz | AM |
| 机场塔台 | 118MHz—135.975MHz | AM |
| 民用对讲机 | VHF: 136MHz—174MHz UHF: 400MHz—470MHz | NFM |
| 超短波电台 | 50—54MHz, 144—148MHz, 430—440MHz | NFM |



Part Five

其他无线协议



启明星辰

搭建ADS-B

硬件

RTL2832U R820T (电视棒)

RTL.SDR全波段接收器(100KHz-1766MHz)

工具

Dump1090 (Linux)

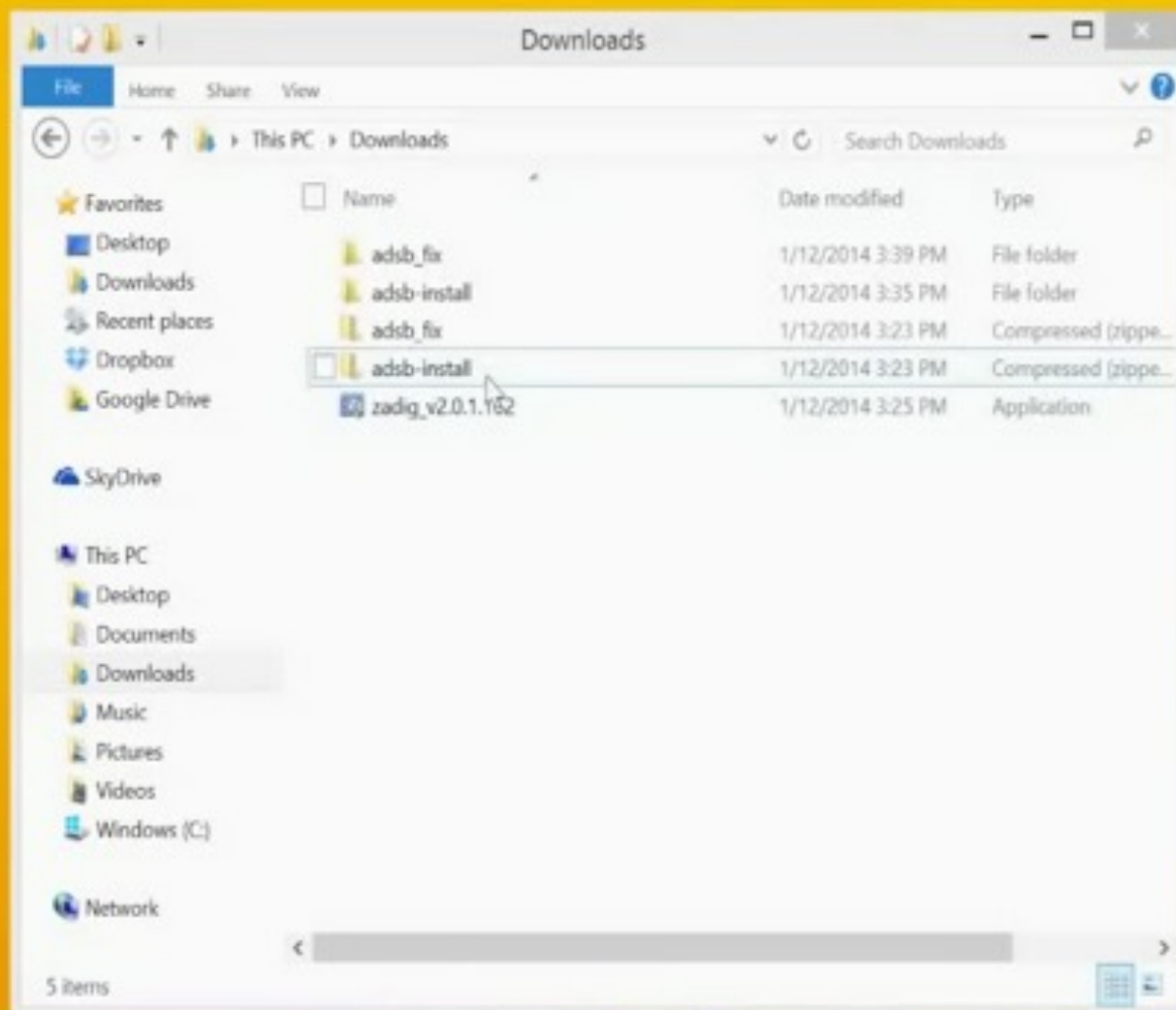
Zadig 驱动

SDRSharp

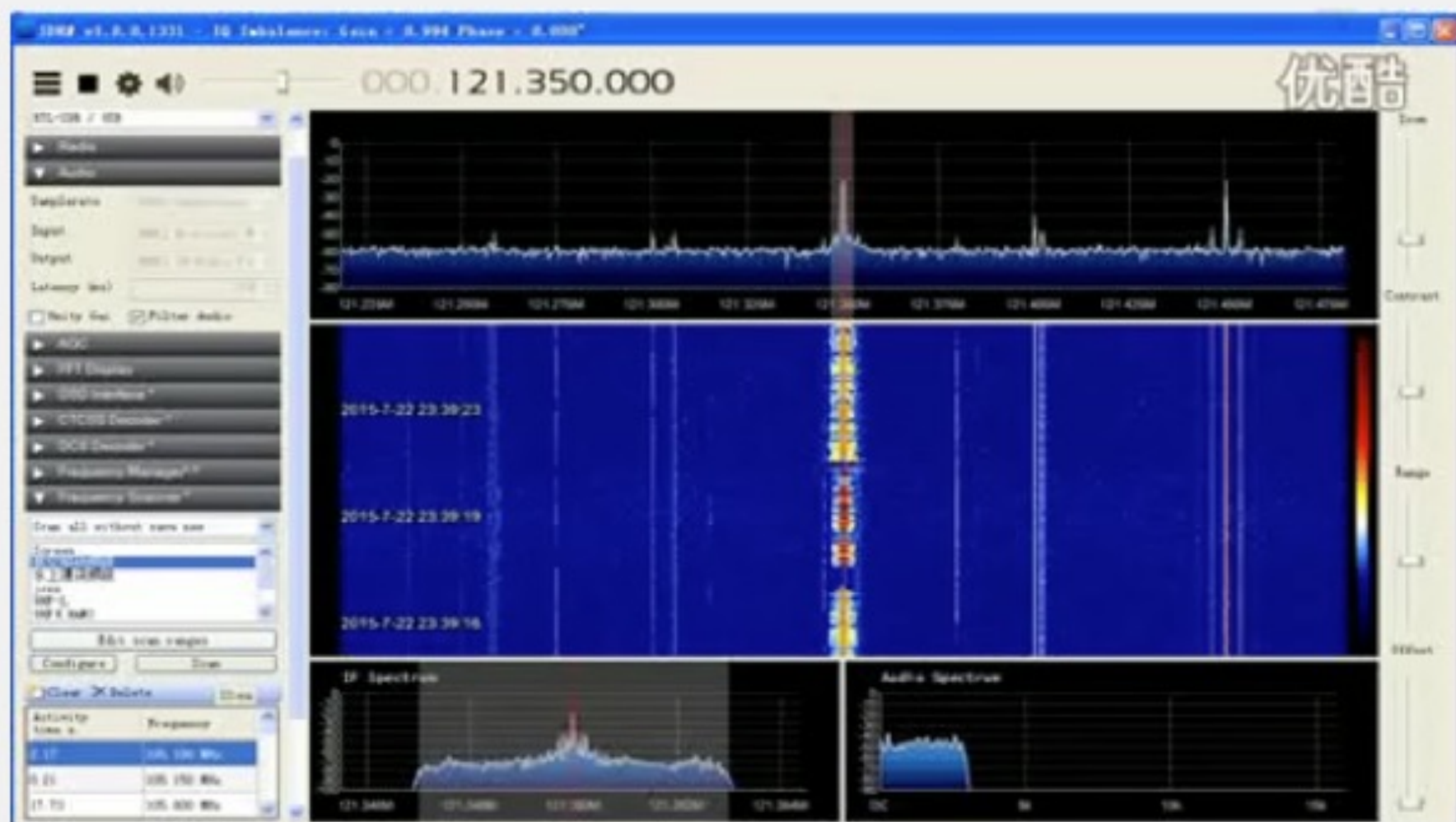
RTL1090

VirtualRadar





Part Five 其他无线协议





Part Five

其他无线协议



启明星辰

ZigBee安全

ZigBee(紫蜂协议)基于IEEE802.15.4标准,作为一种低成本、低功耗、近距离的无线组网通讯技术。

Zigbee是一个比较安全无线协议,它采用AES加密

抓包硬件设备: CC2530或CC2531 USB Dongle

协议分析软件:

Ubiquia Protocol Analyzer、Perytons Protocol Analyzer

TI Packet Sniffer等

Part Five 其他无线协议



Untitled - Ubiquiti Protocol Analyzer

File Tools Device View Window Help

| Traffic View | | | | | | | | | |
|--------------|-----------|-----------------|----------|-------|--------|--------------------|------------------------------|--------|----------|
| No Filters | | | | | | | | | |
| Ln. | Timestamp | Time Delta | Ch. | Stack | Layer | Packet Information | MAC S. | MAC D. | MAC Seq. |
| 558 | 5 | 10:35:41.483335 | 0.000760 | 11 | ZigBee | MAC | Acknowledgement | | |
| 559 | 12 | 10:35:42.486159 | 1.002824 | 11 | ZigBee | MAC | Data Request | 0xDAD3 | 0x00... |
| 560 | 5 | 10:35:42.486927 | 0.000768 | 11 | ZigBee | MAC | Acknowledgement | | |
| 561 | 12 | 10:35:43.490991 | 1.004064 | 11 | ZigBee | MAC | Data Request | 0xDAD3 | 0x00... |
| 562 | 5 | 10:35:43.491759 | 0.000768 | 11 | ZigBee | MAC | Acknowledgement | | |
| 563 | 12 | 10:35:44.496047 | 1.004288 | 11 | ZigBee | MAC | Data Request | 0xDAD3 | 0x00... |
| 564 | 5 | 10:35:44.496815 | 0.000768 | 11 | ZigBee | MAC | Acknowledgement | | |
| 565 | 126 | 10:35:44.674742 | 0.177920 | 11 | ZigBee | APS | Power Configuration | 0xDAD3 | 0x00... |
| 566 | 5 | 10:35:44.679158 | 0.004416 | 11 | ZigBee | MAC | Acknowledgement | | |
| 567 | 12 | 10:35:44.782511 | 0.103352 | 11 | ZigBee | MAC | Data Request | 0xDAD3 | 0x00... |
| 568 | 5 | 10:35:44.783278 | 0.000768 | 11 | ZigBee | MAC | Acknowledgement | | |
| 569 | 48 | 10:35:44.790287 | 0.007000 | 11 | ZigBee | APS | Acknowledgement | 0x0000 | 0xDA... |
| 570 | 5 | 10:35:44.792207 | 0.001920 | 11 | ZigBee | MAC | Acknowledgement | | |
| 571 | 126 | 10:35:44.852222 | 0.060016 | 11 | ZigBee | APS | Power Configuration | 0xDAD3 | 0x00... |
| 572 | 5 | 10:35:44.856638 | 0.004416 | 11 | ZigBee | MAC | Acknowledgement | | |
| 573 | 12 | 10:35:44.959743 | 0.103104 | 11 | ZigBee | MAC | Data Request | 0xDAD3 | 0x00... |
| 574 | 5 | 10:35:44.960511 | 0.000768 | 11 | ZigBee | MAC | Acknowledgement | | |
| 575 | 48 | 10:35:44.967175 | 0.006664 | 11 | ZigBee | APS | Acknowledgement | 0x0000 | 0xDA... |
| 576 | 5 | 10:35:44.969095 | 0.001920 | 11 | ZigBee | MAC | Acknowledgement | | |
| 577 | 126 | 10:35:45.029519 | 0.060424 | 11 | ZigBee | APS | Power Configuration | 0xDAD3 | 0x00... |
| 578 | 5 | 10:35:45.033935 | 0.004416 | 11 | ZigBee | MAC | Acknowledgement | | |
| 579 | 12 | 10:35:45.136966 | 0.103032 | 11 | ZigBee | MAC | Data Request | 0xDAD3 | 0x00... |
| 580 | 5 | 10:35:45.137734 | 0.000768 | 11 | ZigBee | MAC | Acknowledgement | | |
| 581 | 48 | 10:35:45.144383 | 0.006648 | 11 | ZigBee | APS | Acknowledgement | 0x0000 | 0xDA... |
| 582 | 5 | 10:35:45.146302 | 0.001920 | 11 | ZigBee | MAC | Acknowledgement | | |
| 583 | 67 | 10:35:45.203887 | 0.057504 | 11 | ZigBee | APS | Power Configuration | 0xDAD3 | 0x00... |
| 584 | 285 | 10:35:45.203887 | 0.000000 | 11 | ZigBee | ZCL | Power Configuration: Writ... | 0xDAD3 | 0x00... |
| 585 | 5 | 10:35:45.206414 | 0.002528 | 11 | ZigBee | MAC | Acknowledgement | | |
| 586 | 12 | 10:35:45.309150 | 0.102736 | 11 | ZigBee | MAC | Data Request | 0xDAD3 | 0x00... |
| 587 | 6 | 10:35:45.309150 | 0.000768 | 11 | ZigBee | MAC | Acknowledgement | | |

Packet View

● APS - Power Configuration

▲ NWK AUX Header: (14 bytes)

▲ Network Security Control: 0x28

.... 0000 = Network Security Level: [0x0]

...0 1... = Key NWK ID: [0x1] Network Key

..1. = Extended Nonce: [0x1] Yes

00.. = Reserved: 0x0

NWK Frame Counter: 6

Source Address: 00:12:4B:00:01:9C:2E:D0

NWK Key Sequence Number: 0

▲ NWK Payload: (89 bytes)

▲ APS Header: (10 bytes)

▷ Frame Control: 0xC0

Destination Endpoint: 0x00

Profile ID: [0x0F04] Private

Cluster ID: [0x0001] General: Power Configuration

Source Endpoint: 0x0A

APS Counter: 2

▲ Extended Header: 0x0001

▲ Extended Frame Control: 0x01

.... ..01 = Fragmentation: [0x1] Fragmentation

0000 00... = Reserved: 0x0

Block Number: 4

▲ APS Payload: (79 bytes)

Fragmented Payload: [1/4-partial] (79 bytes)

NWK MIC: 0xAC28E777

▷ MAC Footer: 0xFFFF

0x0000 61 88 5C AF 15 00 00 D3 DA 48 02 00 00 D3 DA

0x0012 06 00 00 00 D8 2E 9C 01 00 4B 12 00 00 C0 00

0x0024 0F 0A 02 01 04 00 01 02 03 04 05 06 07 08 09

0x0036 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B

0x0048 1F 20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D

0x005A 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F

0x006C 43 44 45 46 47 48 49 4A 4B 4C 4D 4E 4F 50

0x007E 51 52 53 54 55 56 57 58 59 5A 5B 5C 5D 5E 5F

0x0090 60 61 62 63 64 65 66 67 68 69 6A 6B 6C 6D 6E

0x00A2 6F 70 71 72 73 74 75 76 77 78 79 7A 7B 7C 7D

0x00B4 7E 7F 80 81 82 83 84 85 86 87 88 89 8A 8B 8C

0x00C6 8D 8E 8F 90 91 92 93 94 95 96 97 98 99 9A 9B

0x00D8 9C 9D 9E 9F 00 01 02 03 04 05 06 07 08 09 0A

0x00EA 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19

0x00FC 1A 1B 1C 1D 1E 1F 20 21 22 23 24 25 26 27 28 29

0x0106 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39

0x0118 3A 3B 3C 3D 3E 3F 40 41 42 43 44 45 46 47 48 49

0x012A 4A 4B 4C 4D 4E 4F 50 51 52 53 54 55 56 57 58 59

0x013C 5A 5B 5C 5D 5E 5F 60 61 62 63 64 65 66 67 68 69

0x014E 6A 6B 6C 6D 6E 6F 70 71 72 73 74 75 76 77 78 79

0x0160 7A 7B 7C 7D 7E 7F 80 81 82 83 84 85 86 87 88 89

0x0172 8A 8B 8C 8D 8E 8F 90 91 92 93 94 95 96 97 98 99

0x0184 9A 9B 9C 9D 9E 9F 00 01 02 03 04 05 06 07 08 09

0x0196 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19

0x01A8 1A 1B 1C 1D 1E 1F 20 21 22 23 24 25 26 27 28 29

0x01BA 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39

0x01CC 3A 3B 3C 3D 3E 3F 40 41 42 43 44 45 46 47 48 49

0x01DE 4A 4B 4C 4D 4E 4F 50 51 52 53 54 55 56 57 58 59

0x01E8 5A 5B 5C 5D 5E 5F 60 61 62 63 64 65 66 67 68 69

0x01FA 6A 6B 6C 6D 6E 6F 70 71 72 73 74 75 76 77 78 79

0x020C 7A 7B 7C 7D 7E 7F 80 81 82 83 84 85 86 87 88 89

0x021E 8A 8B 8C 8D 8E 8F 90 91 92 93 94 95 96 97 98 99

0x0230 9A 9B 9C 9D 9E 9F 00 01 02 03 04 05 06 07 08 09

0x0242 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19

0x0254 1A 1B 1C 1D 1E 1F 20 21 22 23 24 25 26 27 28 29

0x0266 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39

0x0278 3A 3B 3C 3D 3E 3F 40 41 42 43 44 45 46 47 48 49

0x028A 4A 4B 4C 4D 4E 4F 50 51 52 53 54 55 56 57 58 59

0x029C 5A 5B 5C 5D 5E 5F 60 61 62 63 64 65 66 67 68 69

0x02AE 6A 6B 6C 6D 6E 6F 70 71 72 73 74 75 76 77 78 79

0x02C0 7A 7B 7C 7D 7E 7F 80 81 82 83 84 85 86 87 88 89

0x02D2 8A 8B 8C 8D 8E 8F 90 91 92 93 94 95 96 97 98 99

0x02E4 9A 9B 9C 9D 9E 9F 00 01 02 03 04 05 06 07 08 09

0x02F6 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19

0x0308 1A 1B 1C 1D 1E 1F 20 21 22 23 24 25 26 27 28 29

0x031A 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39

0x032C 3A 3B 3C 3D 3E 3F 40 41 42 43 44 45 46 47 48 49

0x033E 4A 4B 4C 4D 4E 4F 50 51 52 53 54 55 56 57 58 59

0x0350 5A 5B 5C 5D 5E 5F 60 61 62 63 64 65 66 67 68 69

0x0362 6A 6B 6C 6D 6E 6F 70 71 72 73 74 75 76 77 78 79

0x0374 7A 7B 7C 7D 7E 7F 80 81 82 83 84 85 86 87 88 89

0x0386 8A 8B 8C 8D 8E 8F 90 91 92 93 94 95 96 97 98 99

0x0398 9A 9B 9C 9D 9E 9F 00 01 02 03 04 05 06 07 08 09

0x03AA 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19

0x03BC 1A 1B 1C 1D 1E 1F 20 21 22 23 24 25 26 27 28 29

0x03CE 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39

0x03D0 3A 3B 3C 3D 3E 3F 40 41 42 43 44 45 46 47 48 49

0x03E2 4A 4B 4C 4D 4E 4F 50 51 52 53 54 55 56 57 58 59

0x03F4 5A 5B 5C 5D 5E 5F 60 61 62 63 64 65 66 67 68 69

0x0406 6A 6B 6C 6D 6E 6F 70 71 72 73 74 75 76 77 78 79

0x0418 7A 7B 7C 7D 7E 7F 80 81 82 83 84 85 86 87 88 89

0x042A 8A 8B 8C 8D 8E 8F 90 91 92 93 94 95 96 97 98 99

0x043C 9A 9B 9C 9D 9E 9F 00 01 02 03 04 05 06 07 08 09

0x044E 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19

0x0460 1A 1B 1C 1D 1E 1F 20 21 22 23 24 25 26 27 28 29

0x0472 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39

0x0484 3A 3B 3C 3D 3E 3F 40 41 42 43 44 45 46 47 48 49

0x0496 4A 4B 4C 4D 4E 4F 50 51 52 53 54 55 56 57 58 59

0x04A8 5A 5B 5C 5D 5E 5F 60 61 62 63 64 65 66 67 68 69

0x04BA 6A 6B 6C 6D 6E 6F 70 71 72 73 74 75 76 77 78 79

0x04CC 7A 7B 7C 7D 7E 7F 80 81 82 83 84 85 86 87 88 89

0x04DE 8A 8B 8C 8D 8E 8F 90 91 92 93 94 95 96 97 98 99

0x04E8 9A 9B 9C 9D 9E 9F 00 01 02 03 04 05 06 07 08 09

0x04FA 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19

0x050C 1A 1B 1C 1D 1E 1F 20 21 22 23 24 25 26 27 28 29

0x051E 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39

0x0530 3A 3B 3C 3D 3E 3F 40 41 42 43 44 45 46 47 48 49

0x0542 4A 4B 4C 4D 4E 4F 50 51 52 53 54 55 56 57 58 59

0x0554 5A 5B 5C 5D 5E 5F 60 61 62 63 64 65 66 67 68 69

0x0566 6A 6B 6C 6D 6E 6F 70 71 72 73 74 75 76 77 78 79

0x0578 7A 7B 7C 7D 7E 7F 80 81 82 83 84 85 86 87 88 89

0x058A 8A 8B 8C 8D 8E 8F 90 91 92 93 94 95 96 97 98 99

0x059C 9A 9B 9C 9D 9E 9F 00 01 02 03 04 05 06 07 08 09

0x05AE 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19

0x05C0 1A 1B 1C 1D 1E 1F 20 21 22 23 24 25 26 27 28 29

0x05D2 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39

0x05E4 3A 3B 3C 3D 3E 3F 40 41 42 43 44 45 46 47 48 49

0x05F6 4A 4B 4C 4D 4E 4F 50 51 52 53 54 55 56 57 58 59

0x0608 5A 5B 5C 5D 5E 5F 60 61 62 63 64 65 66 67 68 69

0x061A 6A 6B 6C 6D 6E 6F 70 71 72 73 74 75 76 77 78 79

0x062C 7A 7B 7C 7D 7E 7F 80 81 82 83 84 85 86 87 88 89

0x063E 8A 8B 8C 8D 8E 8F 90 91 92 93 94 95 96 97 98 99

0x0650 9A 9B 9C 9D 9E 9F 00 01 02 03 04 05 06 07 08 09

0x0662 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19

0x0674 1A 1B 1C 1D 1E 1F 20 21 22 23 24 25 26 27 28 29

0x0686 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39

0x0698 3A 3B 3C 3D 3E 3F 40 41 42 43 44 45 46 47 48 49

0x06AA 4A 4B 4C 4D 4E 4F 50 51 52 53 54 55 56 57 58 59

0x06BC 5A 5B 5C 5D 5E 5F 60 61 62 63 64 65 66 67 68 69

0x06CE 6A 6B 6C 6D 6E 6F 70 71 72 73 74 75 76 77 78 79

0x06E0 7A 7B 7C 7D 7E 7F 80 81 82 83 84 85 86 87 88 89

0x06F2 8A 8B 8C 8D 8E 8F 90 91 92 93 94 95 96 97 98 99

0x0704 9A 9B 9C 9D 9E 9F 00 01 02 03 04 05 06 07 08 09

0x0716 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19

0x0728 1A 1B 1C 1D 1E 1F 20 21 22 23 24 25 26 27 28 29

0x073A 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39

0x074C 3A 3B 3C 3D 3E 3F 40 41 42 43 44 45 46 47 48 49

0x075E 4A 4B 4C 4D 4E 4F 50 51 52 53 54 55 56 57 58 59

0x0770 5A 5B 5C 5D 5E 5F 60 61 62 63 64 65 66 67 68 69

0x0782 6A 6B 6C 6D 6E 6F 70 71 72 73 74 75 76 77 78 79

0x0794 7A 7B 7C 7D 7E 7F 80 81 82 83 84 85 86 87 88 89

0x07AE 8A 8B 8C 8D 8E 8F 90 91 92 93 94 95 96 97 98 99

0x07C0 9A 9B 9C 9D 9E 9F 00 01 02 03 04 05 06 07 08 09

0x07D2 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19

0x07E4 1A 1B 1C 1D 1E 1F 20 21 22 23 24 25 26 27 28 29

0x07F6 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39

0x0808 3A 3B 3C 3D 3E 3F 40 41 42 43 44 45 46 47 48 49

0x081A 4A 4B 4C 4D 4E 4F 50 51 52 53 54 55 56 57 58 59

0x082C 5A 5B 5C 5D 5E 5F 60 61 62 63 64 65 66 67 68 69

0x083E 6A 6B 6C 6D 6E 6F 70 71 72 73 74 75 76 77 78 79

0x0850 7A 7B 7C 7D 7E 7F 80 81 82 83 84 85 86 87 88 89

0x0862 8A 8B 8C 8D 8E 8F 90 91 92 93 94 95 96 97 98 99

0x0874 9A 9B 9C 9D 9E 9F 00 01 02 03 04 05 06 07 08 09

0x0886 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19

0x0898 1A 1B 1C 1D 1E 1F 20 21 22 23 24 25 26 27 28 29

0x08AA 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39

0x08BC 3A 3B 3C 3D 3E 3F 40 41 42 43 44 45 46 47 48 49

0x08CE 4A 4B 4C 4D 4E 4F 50 51 52 53 54 55 56 57 58 59

0x08E0 5A 5B 5C 5D 5E 5F 60 61 62 63 64 65 66 67 68 69

0x08F2 6A 6B 6C 6D 6E 6F 70 71 72 73 74 75 76 77 78 79

0x0904 7A 7B 7C 7D 7E 7F 80 81 82 83 84 85 86 87 88 89

0x0916 8A 8B 8C 8D 8E 8F 90 91 92 93 94 95 96 97 98 99

0x0928 9A 9B 9C 9D 9E 9F 00 01 02 03 04 05 06 07 08 09

0x093A 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19

0x094C 1A 1B 1C 1D 1E 1F 20 21 22 23 24 25 26 27 28 29

0x095E 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39

0x0970 3A 3B 3C 3D 3E 3F 40 41 42 43 44 45 46 47 48 49

0x0982 4A 4B 4C 4D 4E 4F 50 51 52 53 54 55 56 57 58 59

0x0994 5A 5B 5C 5D 5E 5F 60 61 62 63 64 65 66 67 68 69

0x09AE 6A 6B 6C 6D 6E 6F 70 71 72 73 74 75 76 77 78 79

0x09C0 7A 7B 7C 7D 7E 7F 80 81 82 83 84 85 86 87 88 89

0x09D2 8A 8B 8C 8D 8E 8F 90 91 92 93 94 95 96 97 98 99

0x09E4 9A 9B 9C 9D 9E 9F 00 01 02 03 04 05 06 07 08 09

0x09F6 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19

0x0A08 1A 1B 1C 1D 1E 1F 20 21 22 23 24 25 26 27 28 29

0x0A1A 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39

0x0A2C 3A 3B 3C 3D 3E 3F 40 41 42 43 44 45 46 47 48 49

0x0A3E 4A 4B 4C 4D 4E 4F 50 51 52 53 54 55 56 57 58 59

0x0A50 5A 5B 5C 5D 5E 5F 60 61 62 63 64 65 66 67 68 69

0x0A62 6A 6B 6C 6D 6E 6F 70 71 72 73 74 75 76 77 78 79

0x0A74 7A 7B 7C 7D 7E 7F 80 81 82 83 84 85 86 87 88 89

0x0A86 8A 8B 8C 8D 8E 8F 90 91 92 93 94 95 96 97 98 99

0x0A98 9A 9B 9C 9D 9E 9F 00 01 02 03 04 05 06 07 08 09

0x0AAE 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19

0x0AC0 1A 1B 1C 1D 1E 1F 20 21 22 23 24 25 26 27 28 29

0x0AD2 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39

0x0AE4 3A 3B 3C 3D 3E 3F 40 41 42 43 44 45 46 47 48 49

0x0AF6 4A 4B 4C 4D 4E 4F 50 51 52 53 54 55 56 57 58 59

0x0B08 5A 5B 5C 5D 5E 5F 60 61 62 63 64 65 66 67 68 69

0x0B1A 6A 6B 6C 6D 6E 6F 70 71 72 73 74 75 76 77 78 79

0x0B2C 7A 7B 7C 7D 7E 7F 80 81 82 83 84 85 86 87 88 89

0x0B3E 8A 8B 8C 8D 8E 8F 90 91 92 93 94 95 96 97 98 99

0x0B50 9A 9B 9C 9D 9E 9F 00 01 02 03 04 05 06 07 08 09

0x0B62 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19

0x0B74 1A 1B 1C 1D 1E 1F 20 21 22 23 24 25 26 27 28 29

0x0B86 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39

0x0B98 3A 3B 3C 3D 3E 3F 40 41 42 43 44 45 46 47 48 49

0x0BAE 4A 4B 4C 4D 4E 4F 50 51 52 53 54 55 56 57 58 59

0x0BC0 5A 5B 5C 5D 5E 5F 60 61 62 63 64 65 66 67 68 69

0x0BD2 6A 6B 6C 6D 6E 6F 70 71 72 73 74 75 76 77 78 79

0x0BE4 7A 7B 7C 7D 7E 7F 80 81 82 83 84 85 86 87 88 89

0x0BF6 8A 8B 8C 8D 8E 8F 90 91 92 93 94 95 96 97 98 99

0x0C08 9A 9B 9C 9D 9E 9F 00 01 02 03 04 05 06 07 08 09

0x0C1A 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19

0x0C2C 1A 1B 1C 1D 1E 1F 20 21 22 23 24 25 26 27 28 29

0x0C3E 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39

0x0C50 3A 3B 3C 3D 3E 3F 40 41 42 43 44 45 46 47 48 49

0x0C62 4A 4B 4C 4D 4E 4F 50 51 52 53 54 55 56 57 58 59

0x0C74 5A 5B 5C 5D 5E 5F 60 61 62 63 64 65 66 67 68 69

0x0C86 6A 6B 6C 6D 6E 6F 70 71 72 73 74 75 76 77 78 79

0x0C98 7A 7B 7C 7D 7E 7F 80 81 82 83 84 85 86 87 88 89

0x0CAE 8A 8B 8C 8D 8E 8F 90 91 92 93 94 95 96 97 98 99

0x0CC0 9A 9B 9C 9D 9E 9F 00 01 02 03 04 05 06 07 08 09

0x0CD2 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19

0x0CE4 1A 1B 1C 1D 1E 1F 20 21 22 23 24 25 26 27 28 29

0x0CF6 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39

0x0D08 3A 3B 3C 3D 3E 3F 40 41 42 43 44 45 46 47 48 49

0x0D1A 4A 4B 4C 4D 4E 4F 50 51 52 53 54 55 56 57 58 59

0x0D2C 5A 5B 5C 5D 5E 5F 60 61 62 63 64 65 66 67 68 69

0x0D3E 6A 6B 6C 6D 6E 6F 70 71 72 73 74 75 76 77 78 79

0x0D50 7A 7B 7C 7D 7E 7F 80 81 82 83 84 85 86 87 88 89

0x0D62 8A 8B 8C 8D 8E 8F 90 91 92 93 94 95 96 97 98 99

0x0D74 9A 9B 9C 9D 9E 9F 00 01 02 03 04 05 06 07 08 09

0x0D86 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19

0x0D98 1A 1B 1C 1D 1E 1F 20 21 22 23 24 25 26 27 28 29

0x0DAE 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39

0x0DC0 3A 3B 3C 3D 3E 3F 40 41 42 43 44 45 46 47 48 49

0x0DD2 4A 4B 4C 4D 4E 4F 50 51 52 53 54 55 56 57 58 59

0x0DE4 5A 5B 5C 5D 5E 5F 60 61 62 63 64 65 66 67 68 69

0x0DF6 6A 6B 6C 6D 6E 6F 70 71 72 73 74 75 76 77 78 79

0x0E08 7A 7B 7C 7D 7E 7F 80 81 82 83 84 85 86 87 88 89

0x0E1A 8A 8B 8C 8D 8E 8F 90 91 92 93 94 95 96 97 98 99

0x0E2C 9A 9B 9C 9D 9E 9F 00 01 02 03 04 05 06 07 08 09

0x0E3E 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19

0x0E50 1





Venustech

THANKS!

—— 谢 谢 观 看 ——

金融 - VFSEC - 阿峰