看雪 2017 安全开发者峰会

Kanxue 2017 Security Developer Summit

2000-2017

智能化的安全：设备&应用&ICS

王东@启明星辰ADLab@VDLab

自我介绍

- 08到16，电子科大，安全研究(kernel/rk/ark/malware/program analysis)
- 16起，启明星辰 ADLab，西南团队，安全研究(vulnerability)
- 17起，启明星辰&东方电气 VDLab，ICS安全研究(vulnerability)

1. 智能化

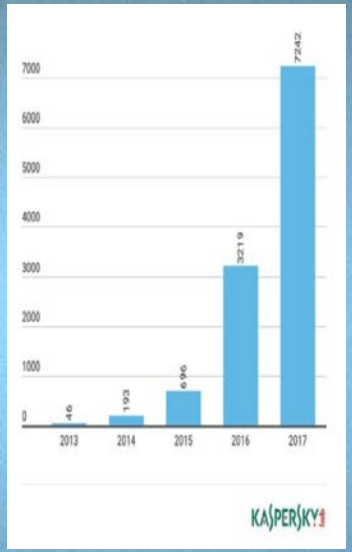
IOT（Internet Of Things）

万物互联：设备联网、系统联网

万物智能：智能设备、智能应用

万物智慧：智慧小区、智慧医疗

1. 智能化



功能的智能化 != 安全也智能化

传统Security问题，照单全收：

1）被攻击，远程控制 （特斯拉汽车）

2）发起攻击，拒绝服务 （mira）

!!!不仅仅是数量上的提升!!!

2. Security→Safety

传统Security的损失：

1）财产损失：数字资产损失，货币资产损失

2）数据损失：员工信息泄露，客户信息泄露，数据删除

传统Security的补救：

1）对内：备份和恢复，清除恶意代码，还原数据库

2）对外：鞠躬道歉，赔钱了事

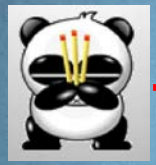
2. Security→Safety

补救的成效：

1）对于责任方：一般来说，业务系统和数据一如当初，实质上只有货币损失

2）对于受害方：一般来说，感受不到太大损失，顶多就是抽风

2. Security→Safety



逻辑量

Safety

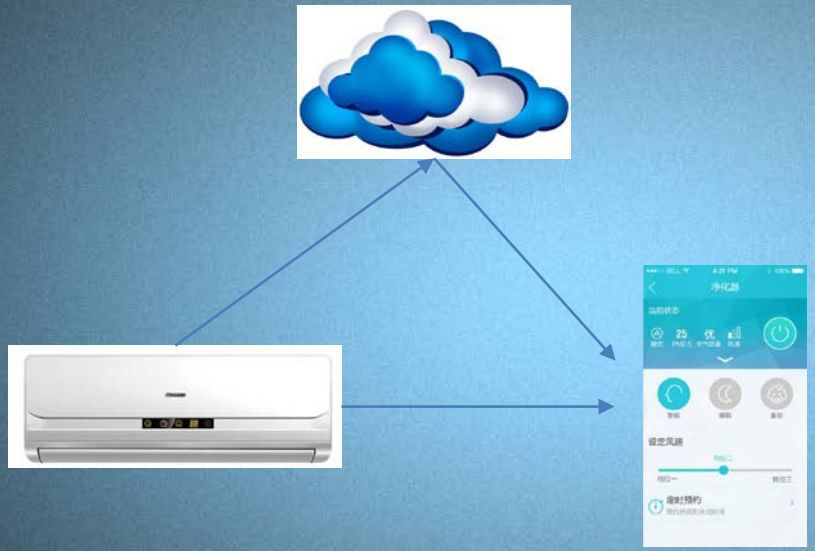
2. Security→Safety

太阳般光芒=智能化

- 智能冰箱，温度被恶意操控，食物隐形变坏，伤人
- 智能汽车，高速熄火，伤人
- 智慧医疗，精准诊断信息被利用，伤人
- 工业控制，锅炉温控异常炸锅，伤人

智能化轻易将逻辑security演变为物理safety，来看栗子

3. 智能设备



智能设备遍地开花：

1）家电类 2）穿戴类 3）安防类 4）逗比类

典型架构：

1）设备和云端，TCP/IP (WIFI)

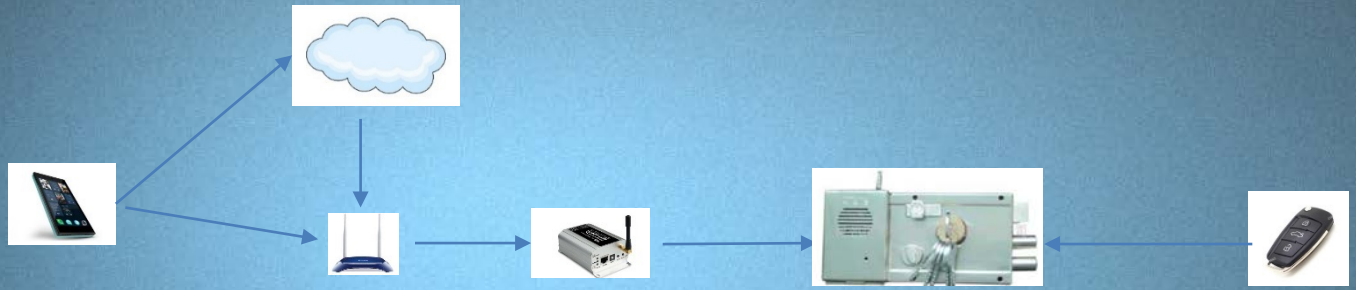
2）app和云端， TCP/IP

3）设备和app，TCP/IP 或 蓝牙(BLE)

3. 智能设备

有一种智能设备不安全会很不安全：

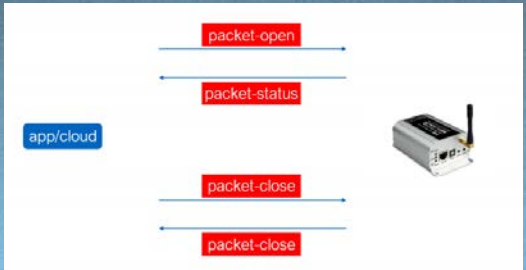
3. 智能设备

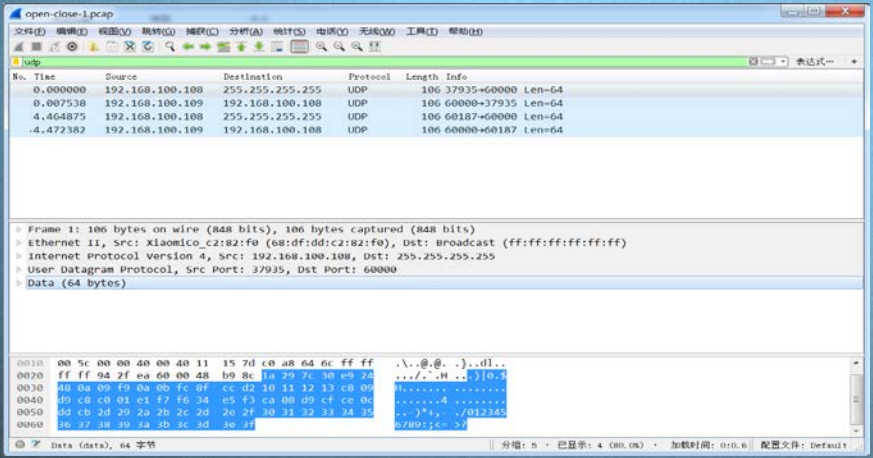


- 遥控锁
- 智能锁

3. 智能设备

开/关门1次
1）64字节
2）udp
3）广播





工欲善其事必先利其器

1）wireshark

2）tcpdump

3）路由器

3. 智能设备

```
ff ff ff ff ff ff 68 df  dd c2 82 f0 08 00 45 00   ......h. ......E.
00 5c 00 00 40 00 40 11  15 7d c0 a8 64 6c ff ff   .\..@.@. .}..dl..
ff ff d3 7d ea 60 00 48  b9 2a 1a 29 49 44 e9 24   ...}.`.H .*.)ID.$
48 0a 09 f9 0a 0b fc 8f  cc d2 10 11 12 13 c8 09   H....... ........
d9 c8 c0 01 e1 f7 f6 34  e5 f3 ca 08 d9 cf ce 0c   .......4 ........
dd cb 21 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35   ..!)*+,- ./012345
36 37 38 39 3a 3b 3c 3d  3e 3f                     6789:;<= >?
```

```
ff ff ff ff ff ff 68 df  dd c2 82 f0 08 00 45 00   ......h. ......E.
00 5c 00 00 40 00 40 11  15 7d c0 a8 64 6c ff ff   .\..@.@. .}..dl..
ff ff c2 e2 ea 60 00 48  c5 ec 1a 29 4c 1d e9 24   .....`.H ...)L..$
48 0a 09 f9 0a 0b fc 8f  cc d2 10 11 12 13 c8 09   H....... ........
d9 c8 c0 01 e1 f7 f6 34  e5 f3 ca 08 d9 cf ce 0c   .......4 ........
dd cb 22 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35   .."")*+,- ./012345
36 37 38 39 3a 3b 3c 3d  3e 3f                     6789:;<= >?
```

```
ff ff ff ff ff ff 68 df  dd c2 82 f0 08 00 45 00   ......h. ......E.
00 5c 00 00 40 00 40 11  15 7d c0 a8 64 6c ff ff   .\..@.@. .}..dl..
ff ff dd 8f ea 60 00 48  a7 32 1a 29 4f 2a e9 24   .....`.H .2.)O*.$
48 0a 09 f9 0a 0b fc 8f  cc d2 10 11 12 13 c8 09   H....... ........
d9 c8 c0 01 e1 f7 f6 34  e5 f3 ca 08 d9 cf ce 0c   .......4 ........
dd cb 23 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35   ..#)*+,- ./012345
36 37 38 39 3a 3b 3c 3d  3e 3f                     6789:;<= >?
```

3次连续开门报文

1）差异非常小

2）有差异规律

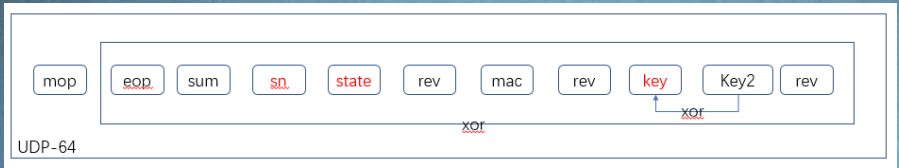
重放攻击

1）pcap抓包发送

Wifi下如何抓包

1）请求是广播报文

3. 智能设备



抓包可还原sn和密钥

1）Rsn = (sn ^ vN)

2）Rkey =(key ^ vN) ^ (key2 ^ vN)

协议简答，APP逆向难度降低：

1）简单编码：vN xox N, N=[1,len)

2）SN：锁的序列码

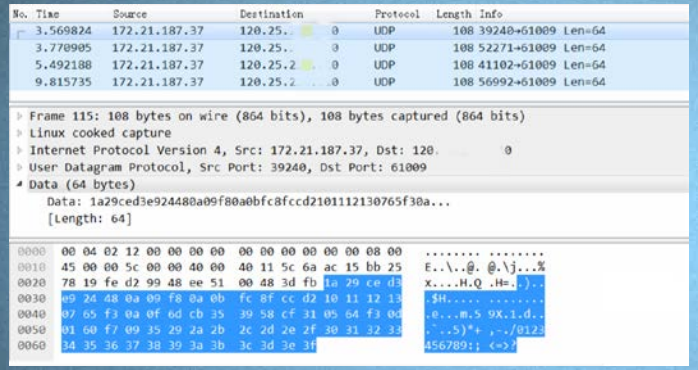
3）state：锁的开关状态

4）key：锁的密码

开/关命令，key和sn必须匹配

3. 智能设备

非局域网的报文如何



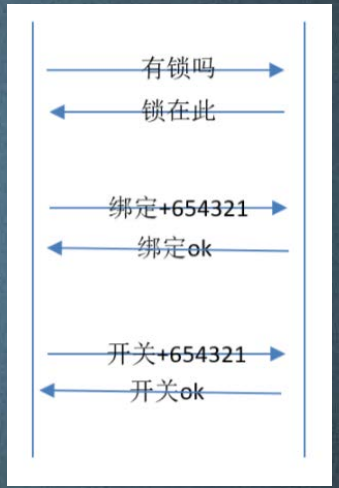
如出一辙，一次抓包，随时随地，随心所欲

如果没法抓包,且无法接入局域网

1）协议：已知

2）SN：223224301， 223224302，223224303…可预测

3）key：654321



3. 智能设备

献上惊喜(bindless)：

1）一部手机

2）下载app

3）蹭网

4）打开app

5）点击绑定

6）打完收工

简单、从容、优雅

3. 智能设备

修复方法：

0）重新设计：采用安全交互协议…nothing

1）重放攻击：本质是开关协议无状态导致的

- App端在开关命令之前加一个命令get_ramdon,从锁端获取一个random
- App端在开关命令中加入random
- 锁端在处理开关命令式检测random是否为保存的值

2）默认密钥：本质是交互设计

- App端使用逻辑中强制要求修改默认密钥

3. 智能设备

3）信息泄露：限制泄露能力

- 限制广播能力，只有搜索命令使用广播
- 限制sn预测能力，采用GUID风格
- 限制密钥泄露，用共享密钥加密get_random来认证

不仅仅是智能锁，WIFI空调、WIFI插座、WIFI摄像头…都存在这类问题

WIFI组网是没有任何安全性可言的，方便开发，也方便攻击者

3. 智能设备

早期蓝牙在IOT中翻不起浪(BR/EDR)

1）能耗无优势

2）组网麻烦,强制配对

3）开发麻烦， bsd-socket

低功耗蓝牙浪起来了(BLE)：

1） 能耗优势非常明显

2） 配对方式灵活

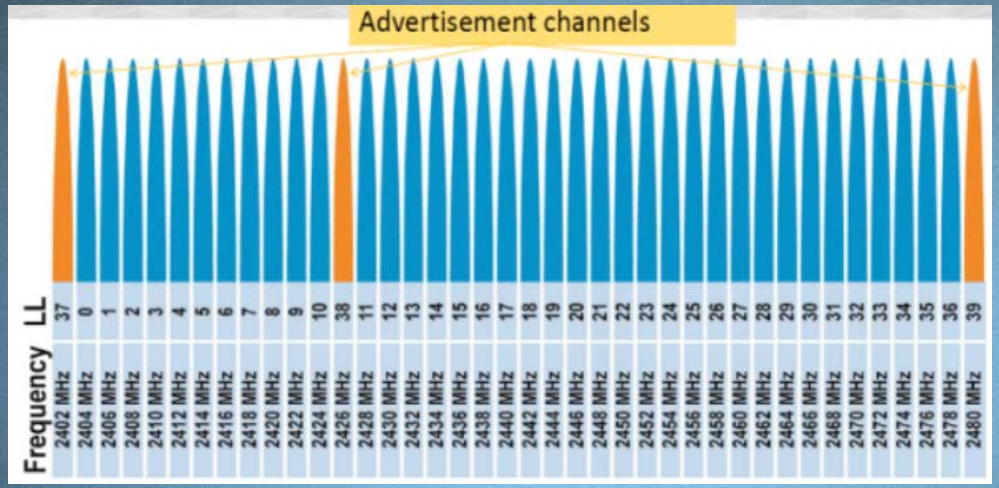
3） 基于GATT开发简单

4） 高带宽也不是总需要的

5） 互联网也不总是需要的

6） 支持WIFI手机也支持蓝牙

3. 智能设备



直接网络层搞，代价大

相比WIFI，BLE自带安全光环

1）点对点通信，不需要中间设备

2）跳频传输，信道加密

3） 抓包麻烦

3. 智能设备

```
GATT_MGR{
  GATT_Service_UUID{
    GATT_Characteristic_UUID{
      dataXXXX;
      GATT_Descriptor_UUID;
      …}
    …}
  …}
```

COM

```
private synchronized void doWrite(Object o) {
    if(o instanceof BluetoothGattCharacteristic) {
        sIsWriting = true;
        mGatt.writeCharacteristic(
            (BluetoothGattCharacteristic)o);
    } else if(o instanceof BluetoothGattDescriptor) {
        sIsWriting = true;
        mGatt.writeDescriptor((BluetoothGattDescriptor) o);
    } else {
        nextWrite();
    }
}
```

3. 智能设备

```
static {
    Config.bltServerUUID = UUID.fromString("0000fee7-0000-1000-8000-00805f9b34fb");
    Config.readDataUUID = UUID.fromString("000036f6-0000-1000-8000-00805f9b34fb");
    Config.CLIENT_CHARACTERISTIC_CONFIG = UUID.fromString("00002902-0000-1000-8000-00805f9b34fb");
    Config.writeDataUUID = UUID.fromString("000036f5-0000-1000-8000-00805f9b34fb");
    Config.OAD_SERVICE_UUID = UUID.fromString("f000ffc0-0451-4000-b000-000000000000");
    Config.OAD_READ_UUID = UUID.fromString("f000ffc1-0451-4000-b000-000000000000");
    Config.OAD_WRITE_UUID = UUID.fromString("f000ffc2-0451-4000-b000-000000000000");
    Config.key = new byte[]{32, 87, 47, 82, 54, 75, 63, 71, 48, 80, 65, 88, 17, 99, 45, 43};
    Config.yx_key = new byte[]{58, 96, 67, 42, 92, 1, 33, 31, 41, 30, 15, 78, 12, 19, 40, 37};
    Config.password = new byte[]{48, 48, 48, 48, 48, 48};
}
```

针对第1款不联网的BLE锁：

1）GATT通信的UUID

2）GATT通信的数据加密方式

3）没有MAC绑定机制

```
public static byte[] Encrypt(byte[] arg5, byte[] arg6) {
    byte[] v1;
    try {
        SecretKeySpec v3 = new SecretKeySpec(arg6, "AES");
        Cipher v0 = Cipher.getInstance("AES/ECB/NoPadding");
        v0.init(1, ((Key)v3));
        v1 = v0.doFinal(arg5);
    }
    catch(Exception v2) {
        v1 = null;
    }

    return v1;
}
```

```
static {
    TYPE.GET_TOKEN = new TYPE("GET_TOKEN", 0, 1537);
    TYPE.OPEN_LOCK = new TYPE("OPEN_LOCK", 1, 1281);
    TYPE.GET_BATTERY = new TYPE("GET_BATTERY", 2, 513);
    TYPE.LOCK_STATUS = new TYPE("LOCK_STATUS", 3, 1294);
    TYPE.RESET_LOCK = new TYPE("RESET_LOCK", 4, 1292);
    TYPE.RESET_PASSWORD = new TYPE("RESET_PASSWORD", 5, 1283);
    TYPE.RESET_PASSWORD2 = new TYPE("RESET_PASSWORD2", 6, 1284);
    TYPE.RESET_AQ = new TYPE("RESET_AQ", 7, 2561);
    TYPE.UPDATE_VERSION = new TYPE("UPDATE_VERSION", 8, 769);
    TYPE.GET_MODE = new TYPE("GET_MODE", 9, 1312);
    TYPE.SET_MODE = new TYPE("SET_MODE", 10, 1313);
    TYPE.GET_LOCK_STATUS = new TYPE("GET_LOCK_STATUS", 11, 1314);
    TYPE.GET_GSM_ID = new TYPE("GET_GSM_ID", 12, 1315);
    TYPE.GET_GSM_VERSION = new TYPE("GET_GSM_VERSION", 13, 1316);
    TYPE.$VALUES = new TYPE[]{TYPE.GET_TOKEN, TYPE.OPEN_LOCK, TYPE.
}
```

伪造App发起请求即可…开锁

3. 智能设备

云端之巅，上帝之力

有很多消费型BLE设备是严重依赖云端，

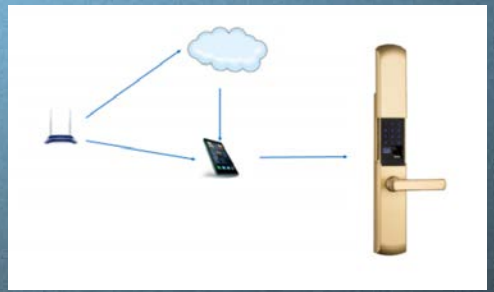
比如下面的这款锁：

1）App必须联网用手机号注册账号

2）App必须联网才能绑定设备

3）App必须联网才能开关门

4）App必须联网才能动态授权其他人开锁



3. 智能设备

```
public void baseListener(View paramView, String paramString)
{
  paramView = new AlertDialog.Builder(this.val$context).setTitle("  服务器");
  paramString = new ServerUrl.1.1(this, new String[] { "http://      com:8080", "http://192.168.1.1      ", "http://192.16
  paramView = paramView.setItems(new String[] {  服务器",  服务器",  服务器",  服务器",  服务器",  服务器",
  paramView.setCanceledOnTouchOutside(true);
  paramView.setOnDismissListener(new ServerUrl.1.2(this));
}
```

域名 .com 的信息　委托购买　访问详情

域名基本信息　网站基本信息　以下信息获取时间：2017-08-10 17:13:52 点击更新

所有者：　. China　& Electronics Co.,Ltd.

Registrant Name：

所有者联系邮箱：　-@163.com

```
public final class BuildConfig
{
  public static final String APPLICATION_ID = "com.       lock";
  public static final String BUILD_TYPE = "release";
  public static final boolean DEBUG = false;
  public static final String FLAVOR = "";
  public static final String OEM_ID =  ";
  public static final int VERSION_CODE = 1;
  public static final String VERSION_NAME = "1.0";
  public static final String xi    HtmlServerUrl = "http://    com:8080";
  public static final String xi    ServerUrl = "https://    .90:4437";
```

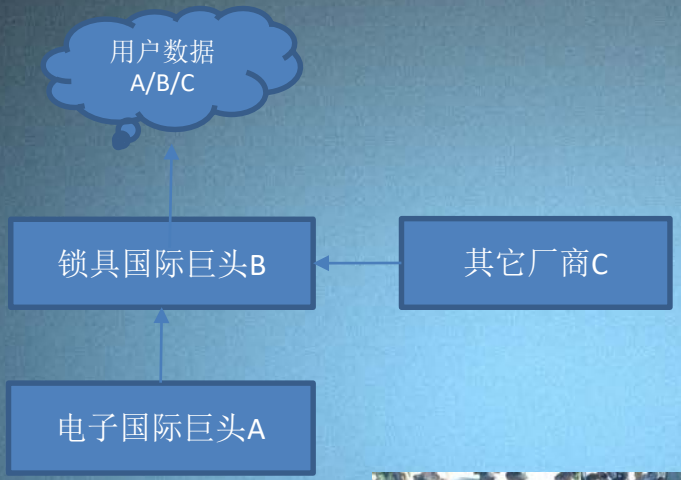
很快发现云端缺陷，获得云端的账号和开门密码：

1）登陆app，一键开门

2）编写代码调用GATT接口发送开门密码

我们继续挖了挖…

3. 智能设备



突然意识到这是一个很普遍的事情

1）硬件代工

2）软件代工

3）用户数据和运营也都代工

数据为王的时代,用户数据都不要了

3. 智能设备

修复方法：

1）加固App：必须要做，BLE的数据收发很容易被定位分析

2）密钥交换：BLE通常用JUST WORK，可设计一种物理交互在进初始绑定时交换一个数据密钥

3）绑定MAC：能做就做

4）云端安全：账号安全、信息泄露、授权指派

4. 智能应用

!!!难以拒绝!!!的智能应用增多：

1）强身健体，大街小巷都不怕

2）不限行，提前自驾，停车免费

3）夏天提前冷车，冬天提前热车

4）上门收发取件，完全不用操心

5）不用夜间排队，不用排队缴费

两类经典问题：账号安全和数据泄露

4. 智能应用

手机登陆,账号找回

!!!猫腻!!!

1）账号登录无限制，任意尝试-爆破/弱口令/撞库

2）账号找回无限制

3）短信验证码，主流4位数字,或6位数字

4. 智能应用

```
POST /v1/user/resetpwd.gz HTTP/1.1
Content-Length: 50
Content-Type: application/x-www-form-urlencoded
Host: tw[redacted]
Connection: close
User-Agent: Mozilla/5.0 (Linux; U; Android 6.0.1; zh-cn; ONEPLUS A3010 Bu
Accept-Encoding: gzip

phone=13438[redacted]&code=1234&password=133456&token=
```

账号找回的背后：

1）4位数字，解空间10**4=1万次，100个/秒，100秒

2）6位数字，解空间10**6=100万次，100个/秒，3小时

4位数字的成本几乎可以忽略

4. 智能应用

```
POST /user/register HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Content-Length: 169
Host: api.[redacted].com
Connection: Keep-Alive
Accept-Encoding: gzip
User-Agent: okhttp/3.2.0

app_version=1.0.0&channel=001&code=1111&device_id=ccd48e3e3024675c&model=GT-N7100&network=5&os=2&os_version=4.4.4&phone=13888888888&sign=5e31016d86adc3b1f1242702154ffc8d
```

```
POST /shjjappapi/service/getUser HTTP/1.1
Content-Type: application/json; charset=UTF-8
Content-Length: 174
Host: sh.[redacted]n
Connection: close
Accept-Encoding: gzip
User-Agent: okhttp/3.2.0

"lArRtakf1gXrfJxgqeoXxTk1k7mFNSUif4KSHl4t/KfaoOGffmjjkqD8rMzCjzPn8hjeqd7J3OgJ/JQv0clLz5tQ2PMn+5zsXH\VjZjA2\VaP8c6pAHQpOhE1AYyo9iKcKrMKHDEKRbXA2we5Eoi49OGKP6+/XgDYRpmL2J2Kxk1g="
```

有时候找回会复杂一点：

1）有签名，绝大部分签名都是APP固化的

2）数据加密，绝大部分加密也都是APP固化的

3）使用了HTTPS

- 不做证书校验（直接开走某合资汽车）

4. 智能应用

```
HTTP/1.1 200 OK
Server: nginx/1.10.2
Date: Sun, 19 Feb 2017 11:27:27 GMT
Content-Type: application/json; charset=utf-8
Content-Length: 34
Connection: keep-alive

{"verifycode":"3526","result":200}
```

```
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/8.0
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Tue, 18 Apr 2017 07:22:06 GMT
Content-Length: 11

true$887132
```

```
{"msg":".....................","data":"7907","status":1}
```

再来送惊喜

!!!投怀送抱的验证码!!!

1）直白告诉你是验证码

2）让你猜I

3）让你猜II

!!!一定是程序员忘记关调试LOG!!!

前面的联网BLE门锁就是如此

4. 智能应用

```
POST /ubx/relation/findRobot HTTP/1.1
Content-Type: application/json;charset=UTF-8
accept: */*
Connection: close
user-agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1;SV1)
Host: services.[redacted].com
Accept-Encoding: gzip
Content-Length: 209

{"appType":"2","relationStatus":1,"requestKey":"28BCBFD855BA06CF1714F5B1A159B76B","requestTime":"20170216104209","serviceVersion":"V1.0","systemLanguage":"CN","token":"SFWH8631EQ5N7LRGY9C02AMJ","userId":"416"}
```

```
HTTP/1.1 200 OK
Server: nginx/1.8.1
Date: Thu, 16 Feb 2017 02:47:02 GMT
Content-Type: application/json;charset=UTF-8
Connection: close
Content-Length: 1981

{"status":true,"info":"0000","models":[{"token":null,"appType":null,"serviceVersion":null,"requestKey":null,"requestTime":null,"systemLanguage":null,"countryCode":null,"loginUserId":0,"relationId":476,"equipmentId":"A1000394D094","userImage":null,"activeArea":null,"status":"1","controlUserName":"App","upUserName":"App","bindPhone":null,"bindEmail":null,"macAddress":null,"userName":"A1000394D094","userOtherName":"A1000394D094","equipmentUserId":4266,"isExitUser":1,"userEmail":null,"relationStatus":1,"relationDate":1452248909000,"relationDateNew":null,"userPhone":null,"userId":416,"upUserId":0,tTime":null,"systemLanguage":null,"countryCode":null,"loginUserId":0,"relationId":1682,"equipmentId":"A20007f4F1E6","userImage":null,"activeArea":null,"status":"1","controlUserName":"App","upUserName":"App","bindPhone":null,"bindEmail":null,"macAddress":null,"userName":"A20007f4F1E6","userOtherName":"A20007f4F1E6","equipmentUserId":5621,"isExitUser":1,"userEmail":null,"relationStatus":1,"relationDate":1456904614000,"relationDateNew":null,"userPhone":null,"userId":416,"upUserId":0,"systemTypeull,"systemLanguage":null,"countryCode":null,"loginUserId":0,"relationId":2521,"equipmentId":"T20160309135019E473","userImage":null,"activeArea":null,"status":"0","controlUserName":"App","upUserName":"App","bindPhone":null,"bindEmail":null,"macAddress":null,"userName":"T20160309135019E473","userOtherName":"T20160309135019E473","equipmentUserId":60941,"isExitUser":1,"userEmail":null,"rentrolUserImage":null,"controlUserId":0}],"macAddress":null,"openfirelp":"domesticopenfire.ubtrobot.com"}
```

智能应用在云端集中存储全部用户的数据：

1）用户数据实际上只是逻辑隔离

2）传统的平行越权分分钟突出重围

4. 智能应用

有时候泄露不是这么直白：

```
POST /shjjappapi/service/getUser HTTP/1.1
Content-Type: application/json; charset=UTF-8
Content-Length: 174
Host: sh[redacted]cn
Connection: close
Accept-Encoding: gzip
User-Agent: okhttp/3.2.0

"lArRtakf1gXrfJxgqeoXxTk1k7mFNSUif4KSHl4t/KfaoOGffmjjkqD8rMzCjzPn8hjeqd7J3OgJ/JQv0dLz5tQ2PMn+5zsXH\VjZjA2\VaP8c6pAHQpOhE1AYyo9iKcKrMKHDEKRbXA2we5Eoi49OGKP6+/XgDYRpmL2J2Kxk1g="
```

加解密代码就在APP内

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Length: 1138
Date: Mon, 31 Jul 2017 02:18:09 GMT

RDzvu7x+56NdQeebakHuyBktf/jsa3TqMaO2kpnAcXUFipEoeEleB9hMrK2M
xXKdPaaOvEJ/IDG/R6qMuUkNww2KaJQXZwlw0hAjo/fjt8\VKR+KRFfnhLQ+q
IEMteVy0cN3\VwA11K/L9xI8k0qu\VI\V9\Vq+hlg2K/YmIz2EwRh5F0SM+tRvMc
i6z5U66bybiU/H6geCxUoXH+6oPhS6n25wg2Z3N0e0k5e\Viuo\VyVUa5b6hS9
0qzCKaBYIbEnlwGCN+/afdQQv8dG5cJF03fo7OIbMsCdkQsNOtSsjRVu14KC
rL8u0QusfvzmiPJAosly5gAM5l8F/bJFeoeU/Peo80t7RY\VxMCQXs\VNOiyMr
ac6EyBSTdBCv2CdJbob2jrUV3+Z1ZLRy0CmBiMARhM9Cs\VnRpMwBPV08euNx
vBkYgZAhrOQPd9sJ4+VjHmMxdpL41uFdVZv6pgg\V0UTHN9tsnLeG7k5NtbO5
eLTTNjKq\V/FN/c77ZUV+LEmZj\V3k0shufRCAz5mtJDe5O7w+38gK4Aa2XV36
EtdxwRSUmITPU8vPxZXgb5FR6FshYtnk\VUYB7OP21f+aPfki64M/MTG5Zg9R
TgsH6lvHfrnFnlP/uNnhziIlsGSRyJ9K0w2UTgiPt8p0+x85d6xEJh8HTGx2
mckOZQIExKwDbfGMrVVJI2cNSHbIAt7A09893wtPZsILTGZ4fwz097cQdk6c
1Z25UtwttUrePX9yER8nEcuvlQyt5Nb\VZ8fM0kHU2fOv6MH4F01nQhChUK9G
mX+xS2BRD/mLSsPdn+OAigv/OAiDfs9JNU8nR1vhu3VDQsrY+yiONgZAiEy9
r\V4xQBS\VMNbNHqL2zjPChNFu\V8t80aOcSuux++iM0EMptS+j336GsvzqX+QB
q8XQbMkETN9IDhd/jV+8ycxAdkVADLJ/tL1XEIHyJORxsu0p5I0HsU4zr4Ho
9lFy7evkXcRUOk893fGhNGfMSwHV\VniRw7sSq2IXCPwXkt2ZLY7DcHkYx4z+
zu5jOdmY8XNt2fRmCBLcuhB1k2HsHKvyQvRpwfJus68bN6Nr5NqnpBQ3bRKO
lqPDyZHQUDUM15CQwaB\VcM9ldi1Pt\VS+O7Heqcxg
```

4. 智能应用

这两类安全非常普遍，我们发现了很多：

1）绝大部分共享单车

2）多家共享汽车

3）合资汽车/国产汽车

4）知名医院的医疗应用

5）儿童手表

…

影响Safety的威胁：

1）花你的钱，骑别人的车

2）花你的钱，用你的驾照，开别人的车，撞无辜的人，让你来背锅

3）开你的车，随意所欲，你背锅

4）泄露极其隐私的个人医疗记录

5）泄露小孩子的行踪或者诱骗

…

4. 智能应用

修复方法：

1）账号安全：多次错误后需要验证码/锁定账号/短信预警，异地登录检测

2）信息泄露：渗透测试，代码审计，正确的HTTPS姿势

5. 工业控制系统

VDLab:东方电气启明星辰工业控制信息安全联合实验室

1）2017年5月，DEC中央研究院

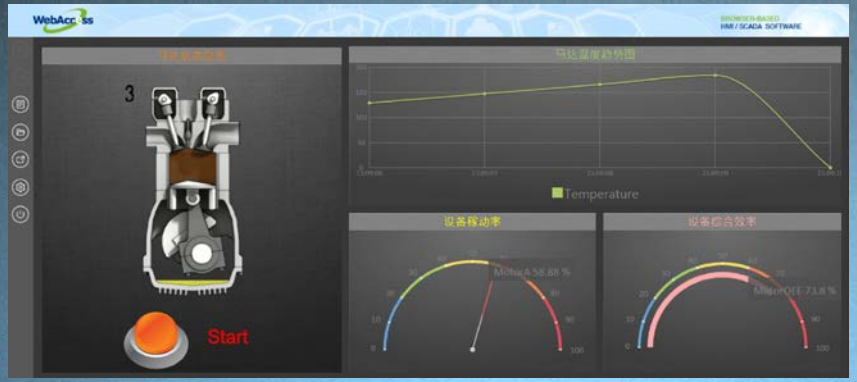
2）工业控制系统漏洞研究

- 上位机
- 协议
- 设备

3）电力行业

- 火电/水电/核电/气电/风电/光伏
- 输电/变电/配电

5. 工业控制系统ICS



依据对专业知识的需求,ICS安全分为两类：

1）ICS信息侧

2）ICS设备侧

已披露的ICS问题大多是信息侧：

1）信息管理系统

2）WEB HMI/SCADA

3）Windows/Linux上位机软件

4）安卓应用

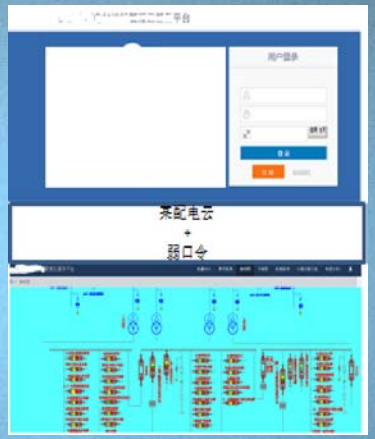
有成熟便捷的研究工具

5. 工业控制系统ICS

disableUAC
+
untrustedPath

某光伏APP
+
SQL注入

某光伏APP
+
账号安全



某配电云
+
弱口令

ICS信息侧的安全问题非常多：

1）弱口令司空见惯(NP)

2）数据泄露家常饭

3）…

强密码的问题：

1）人生有三急，紧急处理

2）争分夺秒，不容有失

3）贴墙上的强密码

5. 工业控制系统ICS

ICS的设备侧更好玩，直接控制物理事件：

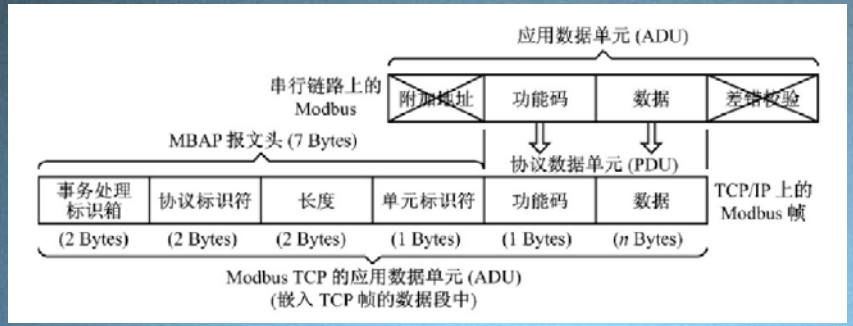
1）PLC

2）DPU

设备分析的梗

- 非安全协议，明文/无认证/无授权
- 设备性能太低
- 设备调试支持无

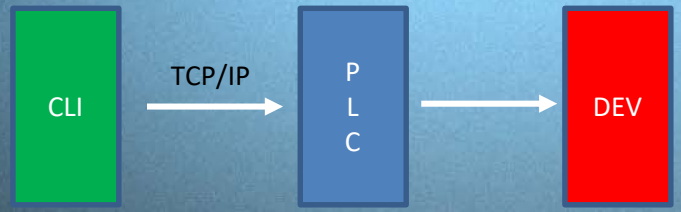
5. 工业控制系统ICS



非安全协议梗：

1）明文传输/无认证/无授权

2）一个不安全的协议，有什么安全问题呢



核心是理解PLC中线圈和寄存器的物理含义，即可任意控制设备做物理型事件。

工控通信协议几乎都是如此

5. 工业控制系统ICS

实时性要求极高：

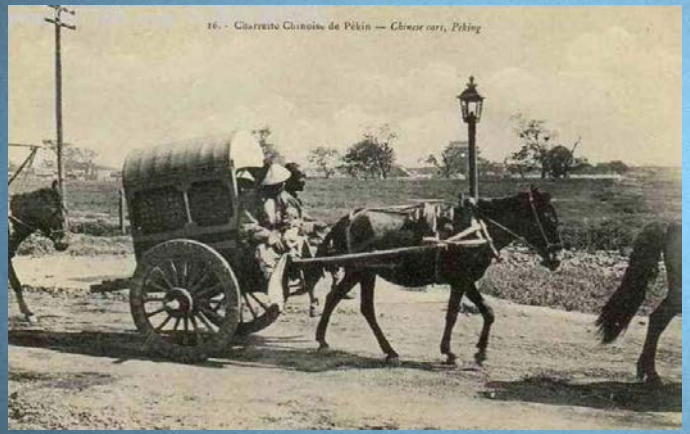
1）IT设施，最小延迟时间，平均延迟时间

2）ICS设施，最大延迟时间（PLC的cycle）

3）以某电力协议来说，报文最大周期为4ms。

- 超过4ms，认为丢包发生；
- 超过8ms，认为会话断开；
- 为了效率，TCP和IP封装都不要，直接用以太帧封装

5. 工业控制系统ICS



性能梗：

- IT设备，单机发包到单机，白搭
- ICS设备，发包分分钟搞死对方
- 更简单，多建立一点连接，对方就罢工
- ICS设备很多资源都有限
  - CPU，好一点的差不多赛扬，差一点单片机
  - 内存，256M都是冗余很高了，几十K的都有
  - 网络，socket的数量一般就支持几十个
- 给模糊测试带来很大挑战

5. 工业控制系统ICS

调试梗：

- 上位机软件容易分析
  - 可以在工程师或操作员站，甚至本机上安装进行各种调试分析
- ICS设备就疼了，没有键盘没有显示器：
  - 我要看操作系统/内存/CPU/网络/磁盘：没门
  - 设备中发生了啥，不知道
- ICS设备资料少，都是配套上位机软件资料
  - 从国内代理商买，外国厂商出货
  - 代理商很多时候也搞不清楚，直接问厂商也懒得理你
- IOS设备的OS是RTOS，即使dump出来拿PC上也无法调试分析

5. 工业控制系统ICS

1）连接抢占拒绝服务

控制连接互斥，只允许一个控制连接，所以提前抢占会话即可。

2）控制会话后门

官方手册账户外，后台还有一个隐藏的高权限账户。一开始，技术支持都不认，后来开发背锅。

3）任意内存消耗

```
//httpd.c
do_post(....)
        bodyLen = headers["content-length"]
        mem = malloc(bodyLen)
        if mem:
                recvAll(mem, bodyLen)
                ...
        ...
```

```
//att.c
post(...)
        headers = init(...)
        headers["content-length"] = 200MB
        send(headers)
        wait(-1)
        ...
```

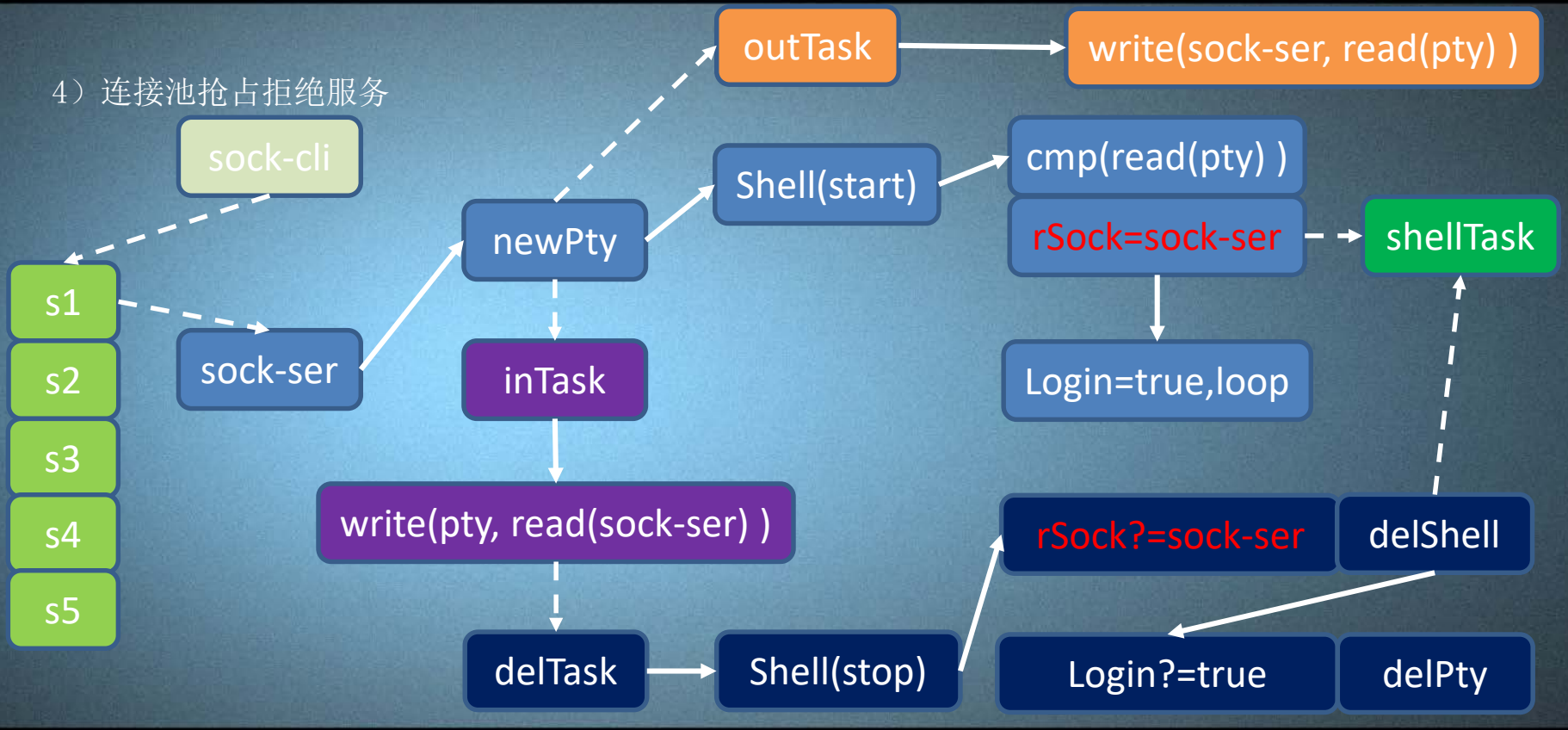
固件静态分析：

➢实时性确实挺好

➢安全性堪忧，几乎假定了其他人都是良民，我们看第一款研究的电力行业某控制器

5. 工业控制系统ICS

4）连接池抢占拒绝服务



5. 工业控制系统ICS

修复：

1）信息侧，怎么补是个问题

- 软件漏洞，协议漏洞，操作系统漏洞（交织在一起）
- 要不要中断业务（复杂系统）

2）设备侧，多方协调

- 现场/研发/主管部门/设备厂商
- 协作厂商出补丁（被拒绝）
- 硬件的更新

谢谢大家！