嵌入式系统联谊会
www.esbf.org

# 物联网设备的安全攻防和实践

360北极星战队　2019年10月

2019年中国上海嵌入式系统安全论坛

# CONTENTS/目录

PART/01

# 物联网行业的发展与安全

# 高速发展的物联网产业


| | 2016 | 2017 | 2018 | 2019 | 2020 | 2021 |
|---|---|---|---|---|---|---|
| 终端安全 | 240 | 302 | 373 | 459 | 541 | 631 |
| 网关安全 | 102 | 138 | 186 | 251 | 327 | 415 |
| 专业服务 | 570 | 734 | 946 | 1221 | 1589 | 2071 |
| | | | | | 2457 | 3118 |

**全球联网设备数量高速增长，“万物互联”成为全球网络未来发展的重要方向。据GSMA预测，2025年全球物联网设备（包括蜂窝及非蜂窝）联网数量将达到252亿，同时物联网市场规模将达到目前的四倍。此外，工业物联网设备联网数量在2016年至2025年间，将从24亿增加到138亿，增幅达五倍左右。**


图 1.3 全球和国内物联网相关设备暴露情况


图 1.8 全球和国内物联网服务暴露情况

# IOT安全现状堪忧

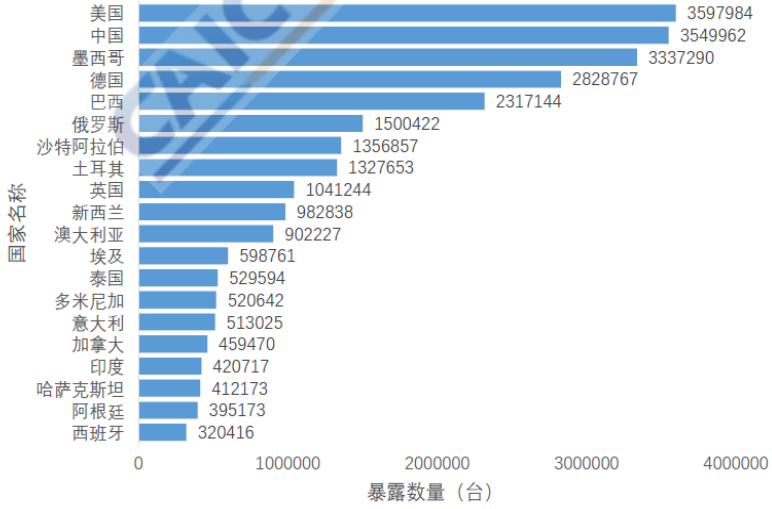



图 1.6 暴露的路由器国家分布

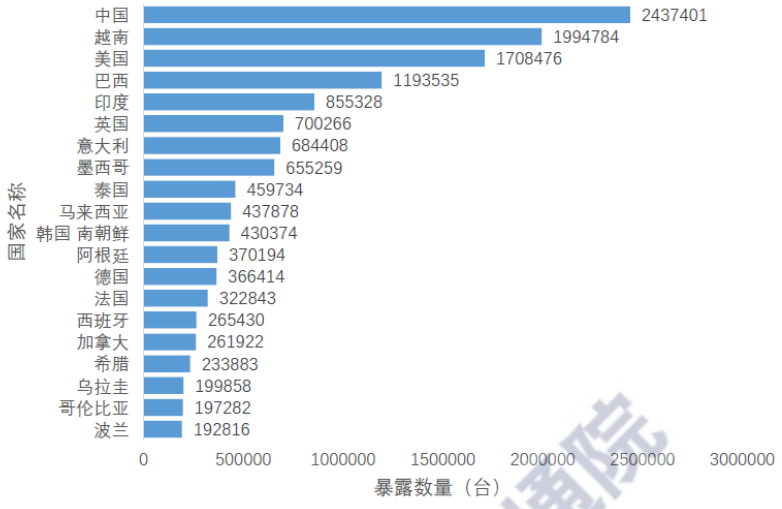
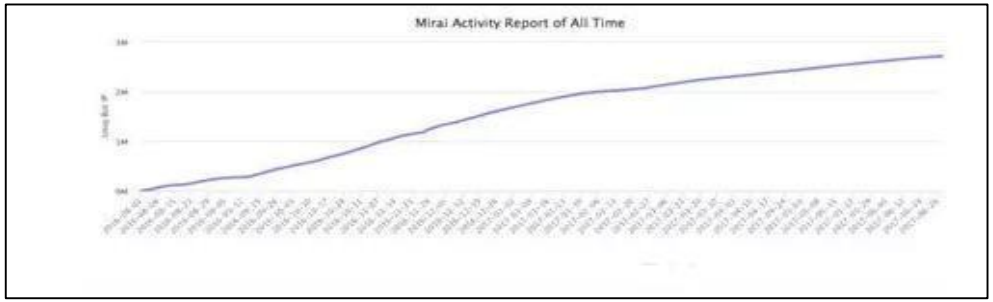
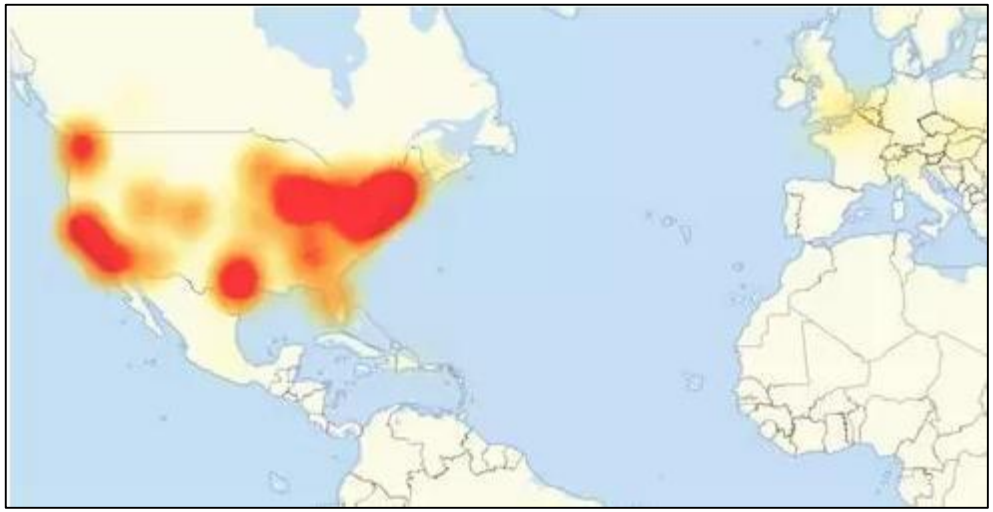



图 1.7 暴露的视频监控设备国家分布

**我国暴露于互联网的路由器及视频监控设备数量排名全球前列，路由器数量超过350万台，仅次于美国。视频监控设备数量超过240万台，位居第一；**

# IOT安全问题引发的安全事件



2016年10月21日，美国域名服务商Dyn遭受到来自Mirai僵尸网络的数十万网络摄像头、数字录像机设备组成的僵尸网络高达620G流量的DDoS攻击，导致美国东海岸大面积断网,Twitter、亚马逊、华尔街日报等数百个重要网站无法访问。同年，德国电信遭遇网络攻击，超90万台路由器无法联网，断网事故共持续数个小时，导致德国电信无法为用户提供正常网络服务。

# IOT的安全获得广泛关注

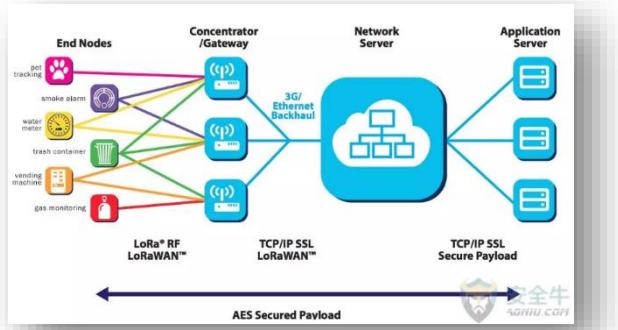



**2019RSA大会上，有关IOT安全的论坛是最火热的方向之一。IOT在工业、商业、生活、医疗等领域的安全是会议的主要方向。**

PART/02

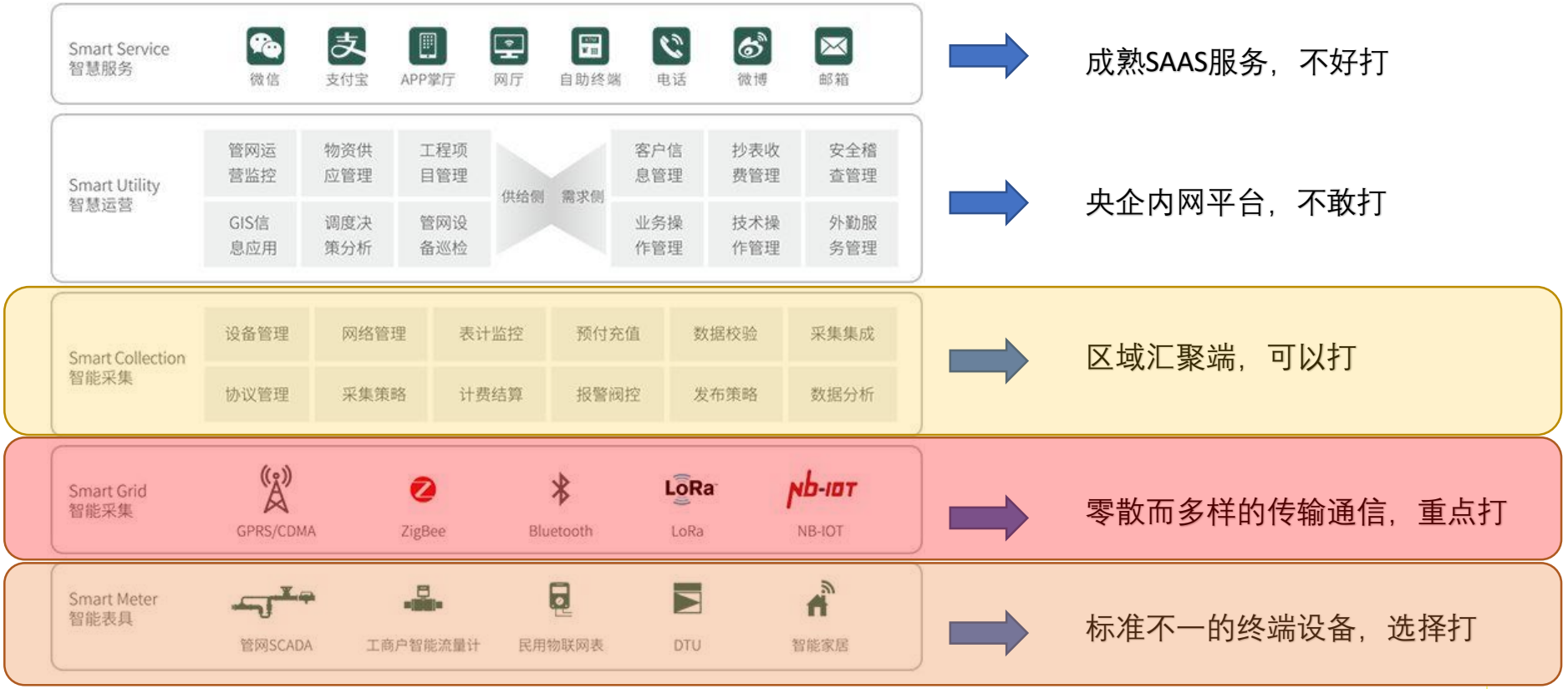
# 物联网设备的攻击思考及实践

# 如何用一个水表劫持一个城市


**《我用一个水表劫持了一座城市》中，通过对于Lora协议的不当利用分析得出了耸人听闻的结论**

# 如果我是黑客……

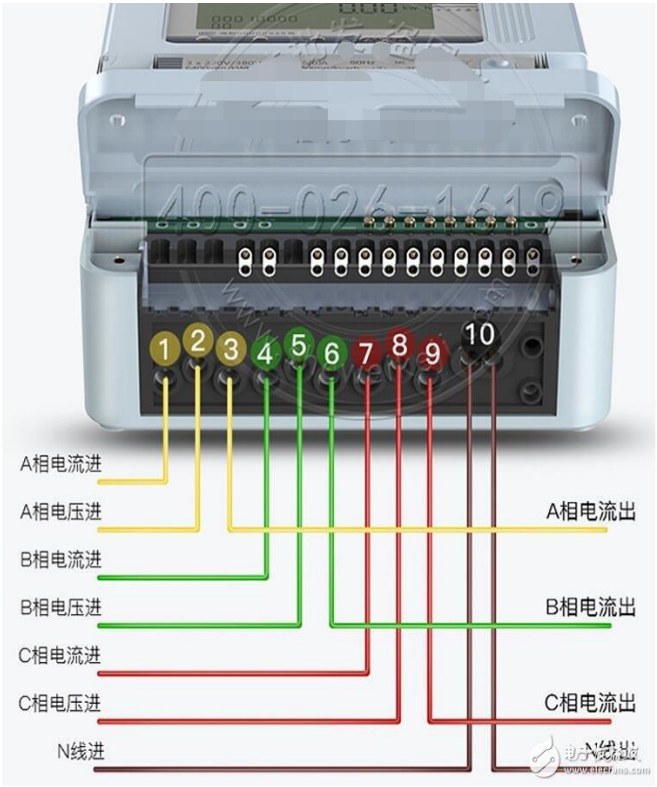

Smart Service
智慧服务
微信
支付宝
APP掌厅
网厅
自助终端
电话
微博
邮箱
成熟SAAS服务，不好打
Smart Utility
智慧运营
管网运营监控
物资供应管理
工程项目管理
GIS信息应用
调度决策分析
管网设备巡检
供给侧
需求侧
客户信息管理
抄表收费管理
安全稽查管理
业务操作管理
技术操作管理
外勤服务管理
央企内网平台，不敢打
Smart Collection
智能采集
设备管理
网络管理
表计监控
预付充值
数据校验
采集集成
协议管理
采集策略
计费结算
报警阀控
发布策略
数据分析
区域汇聚端，可以打
Smart Grid
智能采集
GPRS/CDMA
ZigBee
Bluetooth
LoRa
NB-IOT
零散而多样的传输通信，重点打
Smart Meter
智能表具
管网SCADA
工商户智能流量计
民用物联网表
DTU
智能家居
标准不一的终端设备，选择打

# 攻击实践下表计设备风险点

终端侧

通信侧

# 终端侧风险 – 物理安全风险




主板信息残留风险

物理接口暴露风险

接口调试提权风险

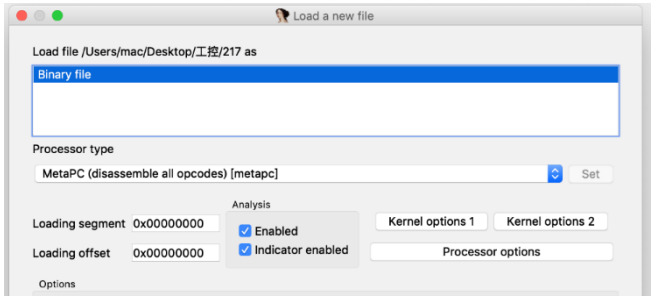
接口内容提取风险

# 终端侧风险 – 固件安全风险

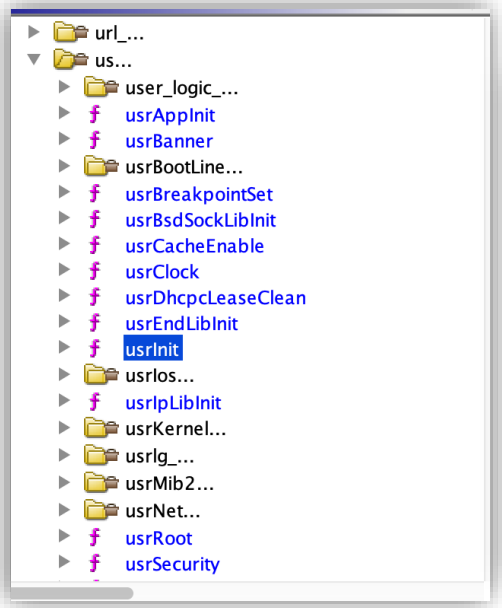
## 1.提取固件

```
~/Desktop » binwalk 6-bin.bin                                    16:12:20

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
155672        0x26018         LZMA compressed data, properties: 0x5D, dictionary
 size: 65536 bytes, uncompressed size: 300028 bytes
233464        0x38FF8         TRX firmware header, little endian, image size: 19
41504 bytes, CRC32: 0x2DAE9AF0, flags: 0x0, version: 1, header size: 28 bytes, l
oader offset: 0x1C, linux kernel offset: 0x0, rootfs offset: 0x0
233492        0x39014         LZMA compressed data, properties: 0x5D, dictionary
 size: 65536 bytes, uncompressed size: 4629600 bytes
1635467       0x18F48B        StuffIt Deluxe Segment (data): f%
2174969       0x212FF9        Squashfs filesystem, little endian, version 4.0, c
ompression:xz, size: 13061274 bytes, 2642 inodes, blocksize: 131072 bytes, creat
ed: 2018-05-19 04:25:38
```

## 2.导入IDA



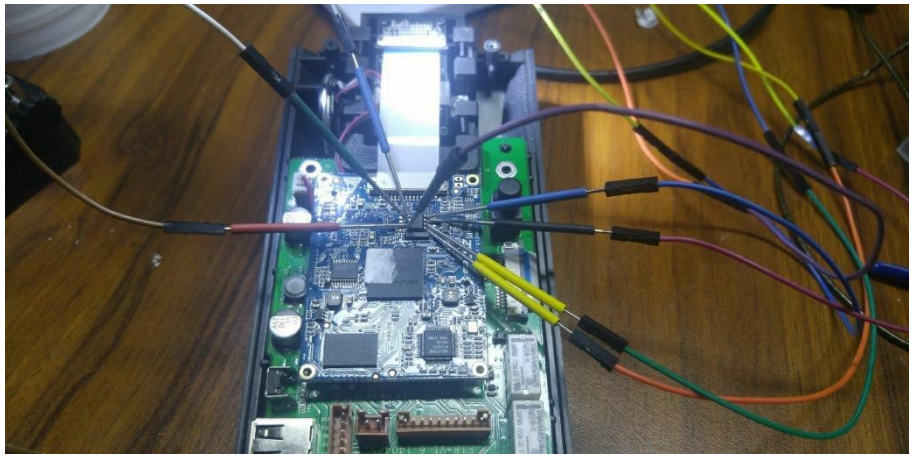

## 3.解析代码结构




## 4.分析&修改函数指向

```
                        DAT_00326ff0
00326ff0 00 00 01 00     undefined4  00000100h

                        PTR_excConnect_00326ff4
00326ff4 00 14 bb b0     addr        excConnect

                        PTR_excExcHandle_00326ff8
00326ff8 00 14 be 68     addr        excExcHandle

                        DAT_00326ffc
00326ffc 00 00 02 00     undefined4  00000200h

                        PTR_excConnect_00327000
00327000 00 14 bb b0     addr        excConnect

                        PTR_excExcHandle_00327004
00327004 00 14 be 68     addr        excExcHandle
```

# 终端侧风险 – 存储安全风险

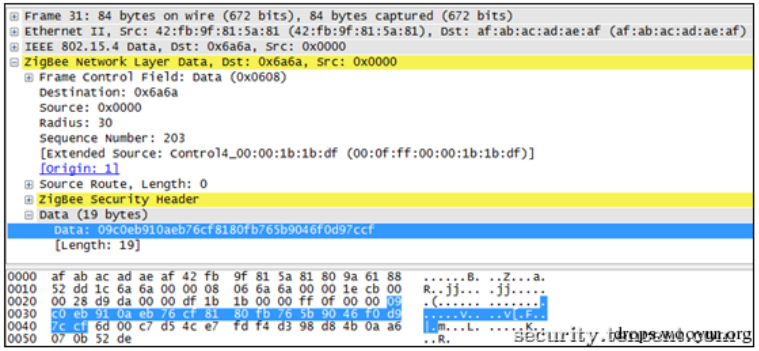


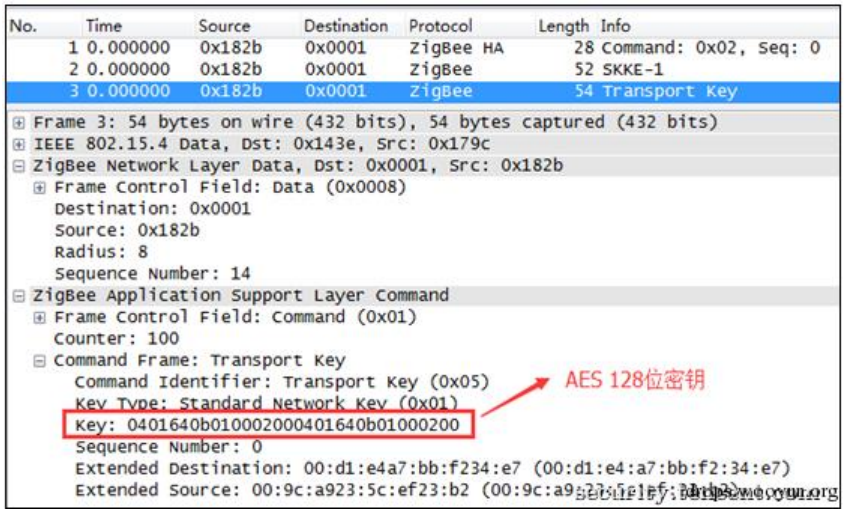
敏感信息提取

密钥提取

固件提取

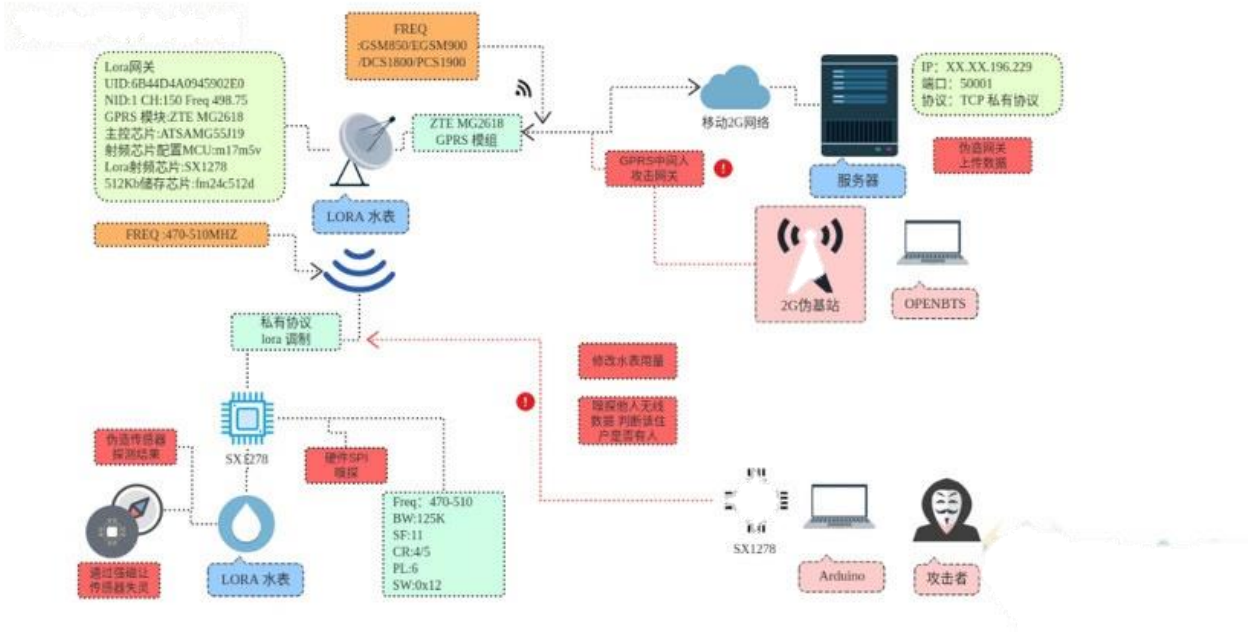
# 通信侧风险 – 内容劫持




**针对Zigbee传输协议中非安全模式下对于通信内容和密钥的劫持破解**

# 通信侧风险 – 中间人攻击




**以2G伪基站为攻击节点的，针对水表信息汇聚侧的劫持攻击场景**

PART/03

# 物联网设备的防御思考及实践

# 知攻然后知防

## 攻击

物理攻击

固件攻击

存储攻击

通信攻击

身份攻击

## 防御

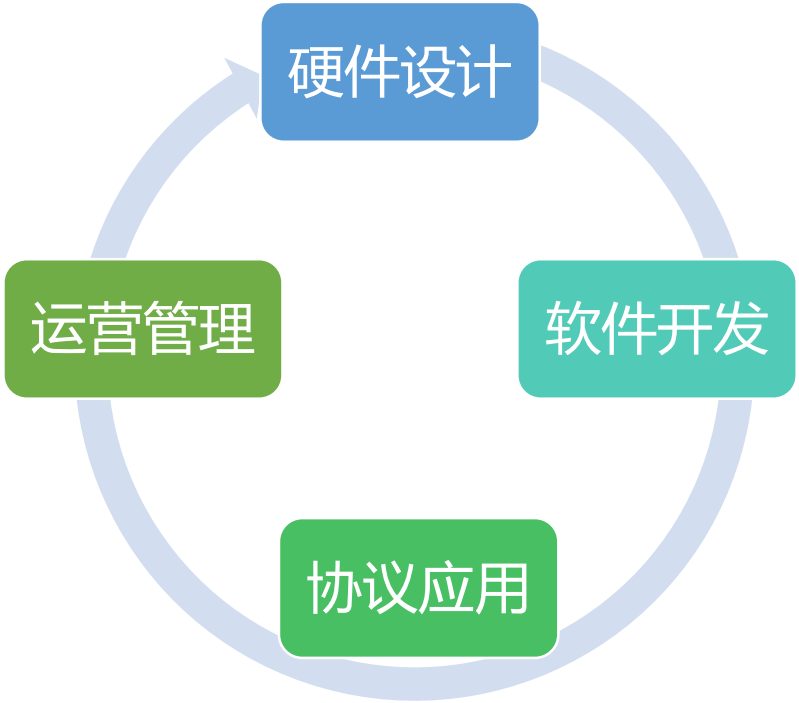
合规建设

固件加固

密钥安全

通信安全

# 合规建设 – 表计安全基线




设计开发符合对应行业规范

软件编码不存在安全漏洞

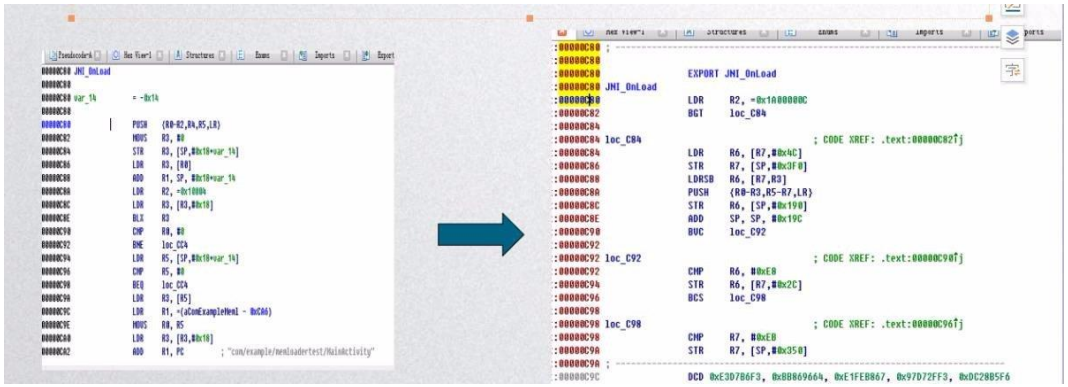
协议应用规范合理

运营管理正常合规

# 固件加固 – 核心资产的保险柜

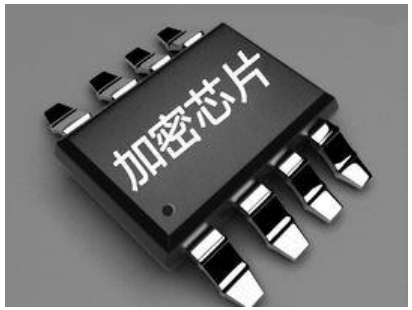
SO

Bin



针对表计固件的安全加固，通过对核心文件的代码、逻辑结构等的混淆，防止黑客的反编译攻击。保护核心代码和核心函数的运行逻辑不被发现，降低后续高级攻击风险。

# 密钥安全 – 数据和身份安全的保障




基于白盒原理保护密钥的软件SE

密钥的安全是整个表计设备数据存储加密、通信传输以及身份认证校验的技术。需采用专业的SE进行存储。包括专业的加密芯片或基于白盒原理的软SE。

# 通信安全 – 表计系统运行安全的保障


表计的通信协议多种多样，同一行业，针对不同客户种类、不同区域、不同环境所采用的通信标准也有较大的不同，这也是困扰表计行业安全的一个难题。可以考虑在不同协议之上，通过应用层的身份认证和加密，提供适配多种协议，多种场景的统一化通信安全方法。

PART/04

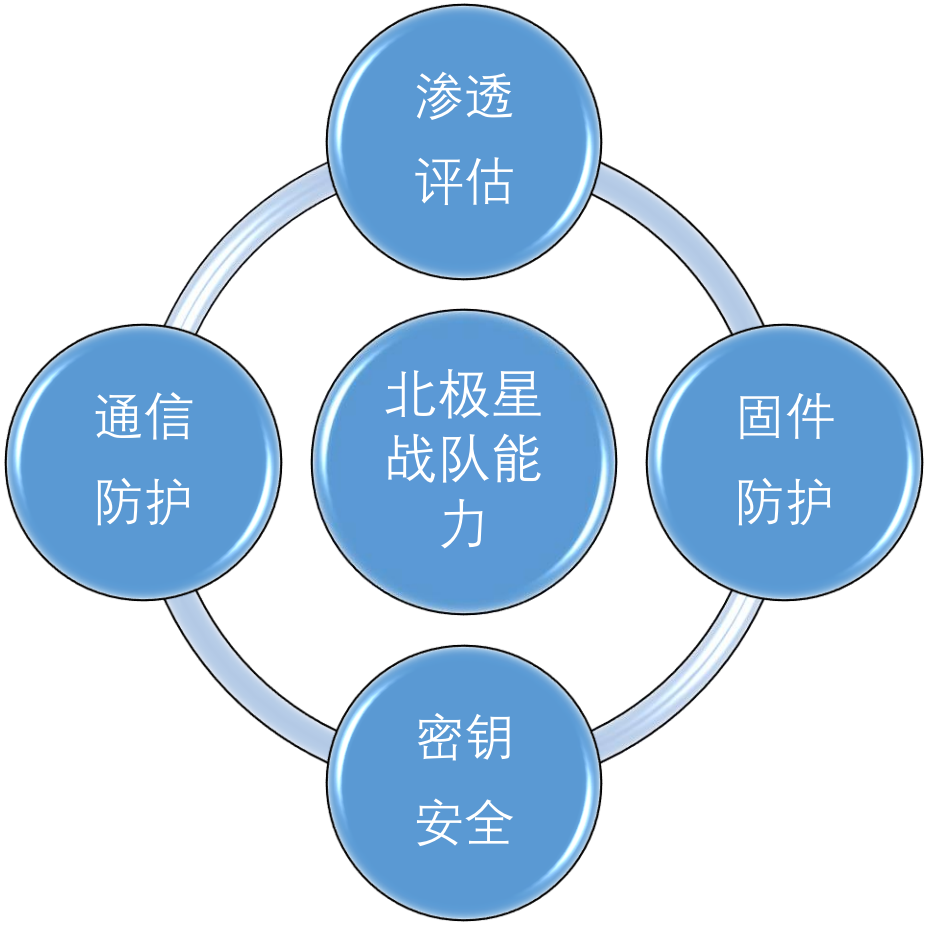
# 360北极星战队

# 360北极星战队简介

北极星战队是360物联网（IOT）领域的顶尖攻防战队，拥有针对车联网、智能家居、智能穿戴、智慧城市、智慧医疗、智慧安控等众多IOT领域的攻防积累。

- 团队愿景：万物互联，指引未来
- 团队组成
  - 勾陈一组：由从事多年IoT系统安全渗透工作的专家组成，覆盖车辆网、智能家居、安控、医疗等领域。
  - 勾陈四组：由360天御团队致力于移动端安全防护的专家组成，将能力和技术移至物联网领域，建立了完整的防御产品体系。

# 360北极星战队能力



互联万物，指引未来

# Thanks

三六零北极星