智能设备安全

cradmin
Tencent Blade Team

关于我

- 张博(cradminzhang)
- Tencent Blade Team技术负责人
- 移动互联网/IoT/AI安全
- 曾经的防黑反黑老兵

关于团队-Tencent Blade Team

- 隶属于腾讯安全平台部
- 聚焦移动互联网/IoT/AI等领域的安全研究
- 发现Google/Amazon等厂商70+安全漏洞
- 联系我们： https://blade.tencent.com

轻用其芒，动即有伤，是为凶器；
深藏若拙，临机取决，是为利器。

智能设备介绍

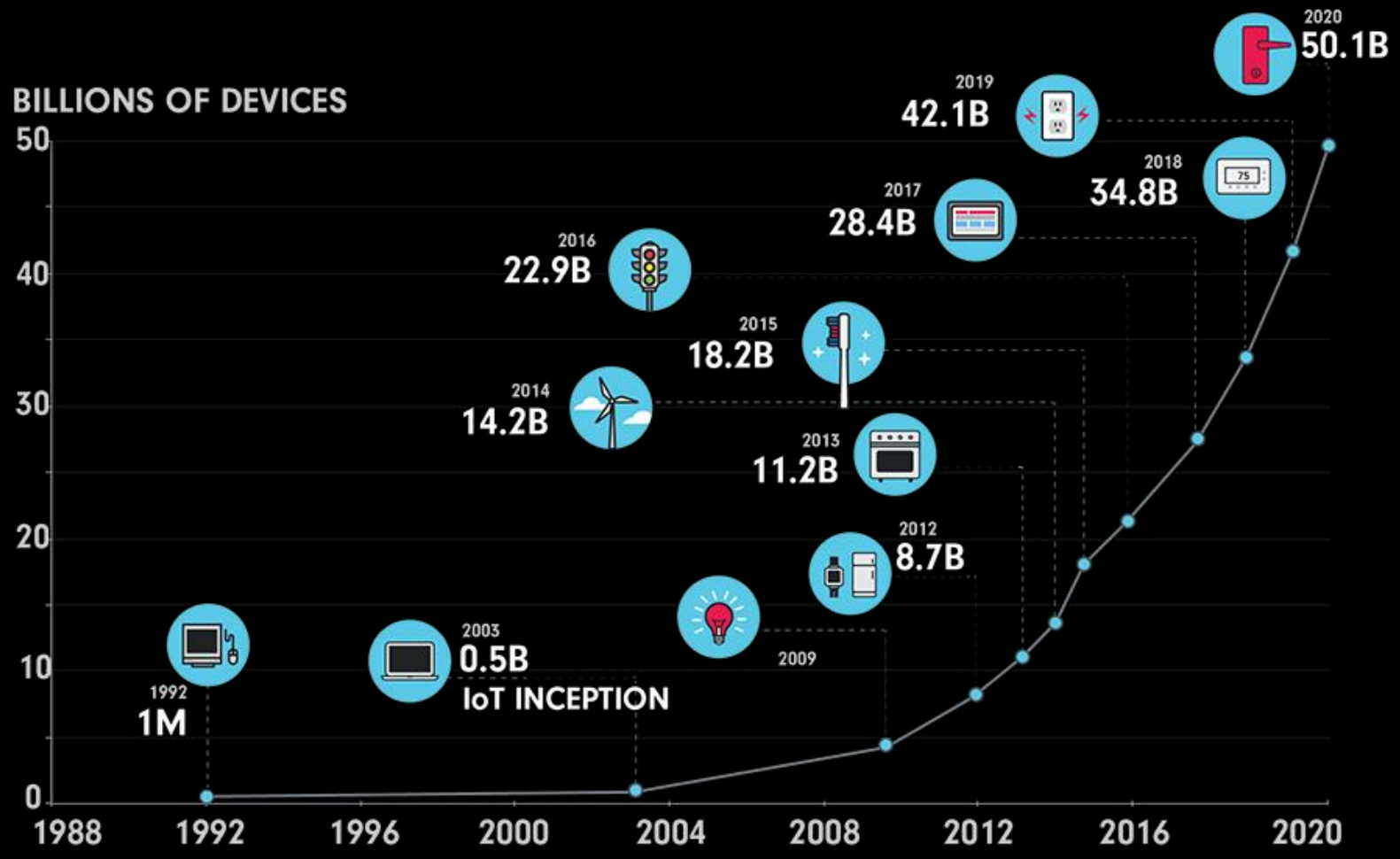
CONTENTS

什么是智能设备

- IoT /smart device: Connected => Smart

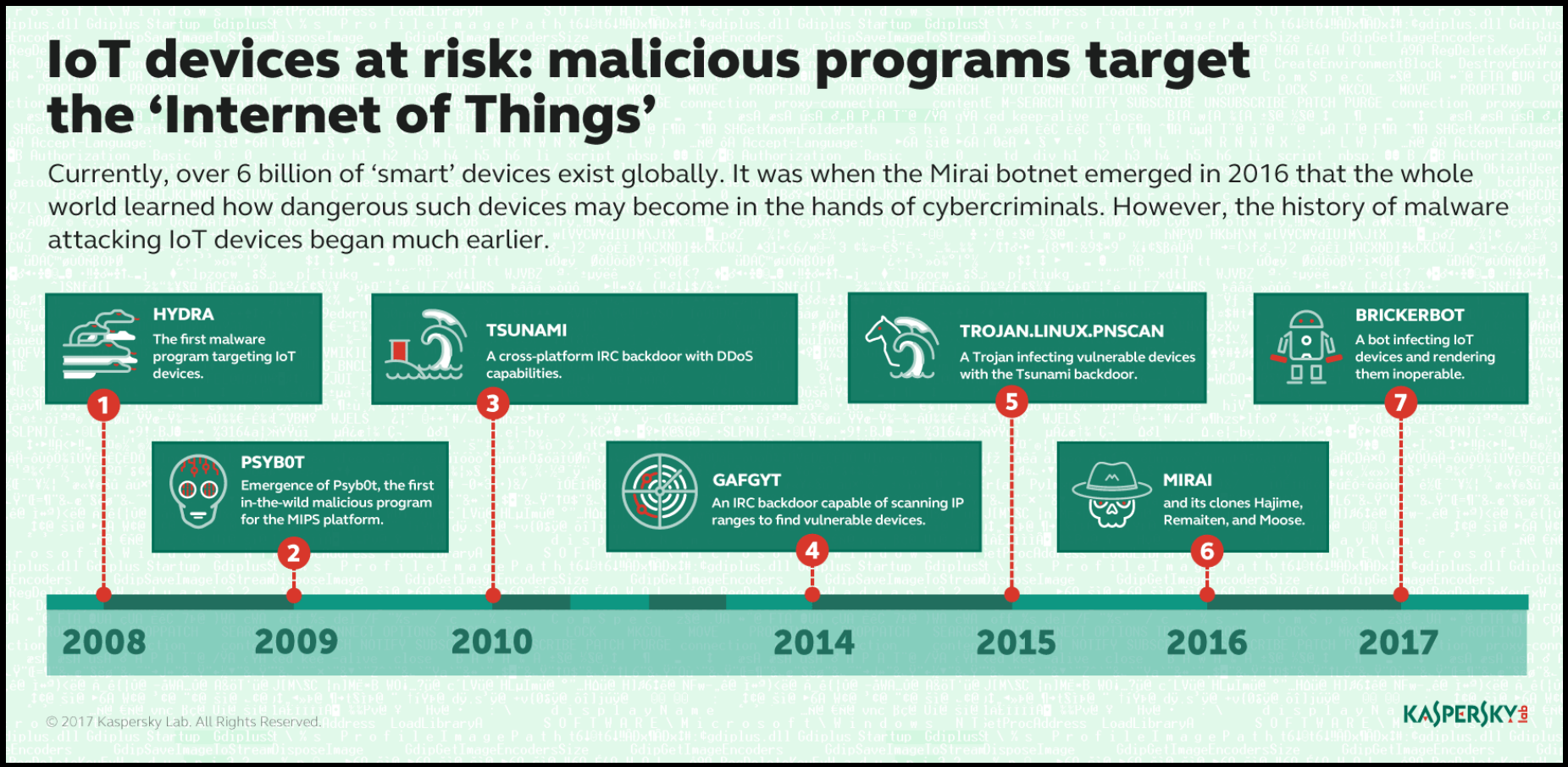
Ref: https://hackernoon.com/internet-of-everything-the-iot-market-is-projected-to-expand-12x-from-2017-2023-175f845c2bcf

智能设备快速增长



Ref: https://hackernoon.com/internet-of-everything-the-iot-market-is-projected-to-expand-12x-from-2017-2023-175f845c2bcf

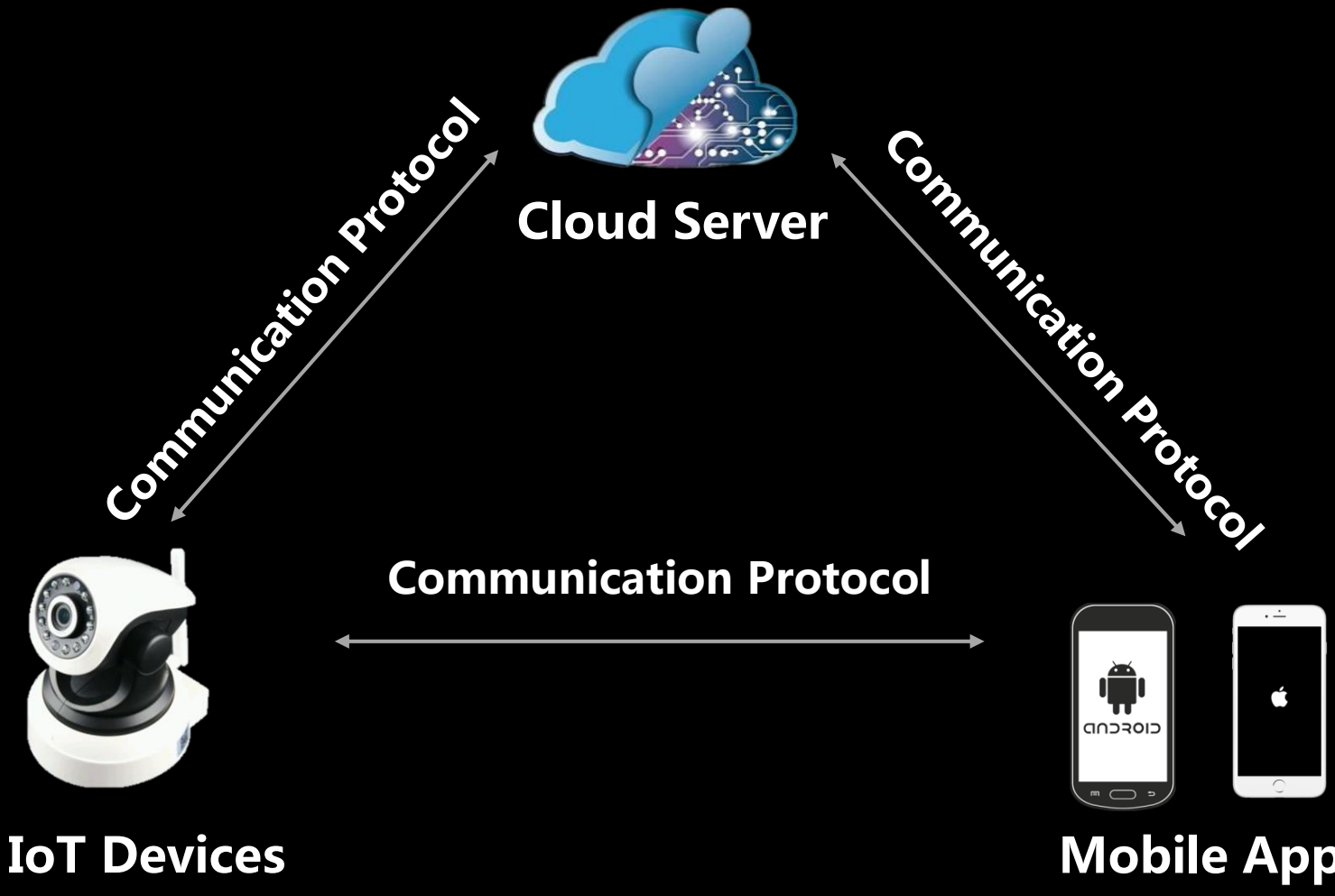
针对智能设备的攻击在增加



团队研究成果

CONTENTS

智能设备攻击面


Cloud Server
Communication Protocol
Communication Protocol
Communication Protocol
IoT Devices
Mobile App

攻击智能插座


腾讯安全应急响应中心
Tencent Security Response Center
[*] 准备开启插座
[*] 加密指令
[*] 发送攻击指令
[*] 解密指令
[*] 攻击成功!

攻击智能烤箱

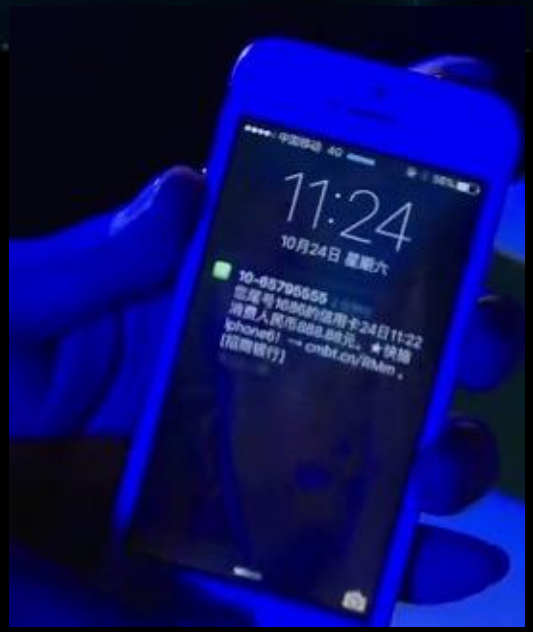
攻击智能烤箱


编号 设备名 设备ID MAC编号 产品编号 AccessT
oken
1 长帝烤箱 143978966640726527 b4430da2a348 IFGTGA dabf88be502a765
e24968d13fff23af9
2 公牛远程控制插座 144038760000809239 AC-CF-23-21-C7-9D MWE786
b8a4c4066d3fbff6baf0dd20b02492937
3 测试设备 143938340273949718 b4430da298b8 EPIQJ4 e5662458175c2ee
8253a3bad11976d1e
监听完毕,是否进入攻击模式(Y/N)? y
请输入要攻击的设备ID: 1
编号 简介
1 开启高温加热模式
2 开启低温冷却模式
3 开启烤叉加热模式
4 终止运行
5 自毁模式
6 窃取烤箱控制权限

攻击移动POS机

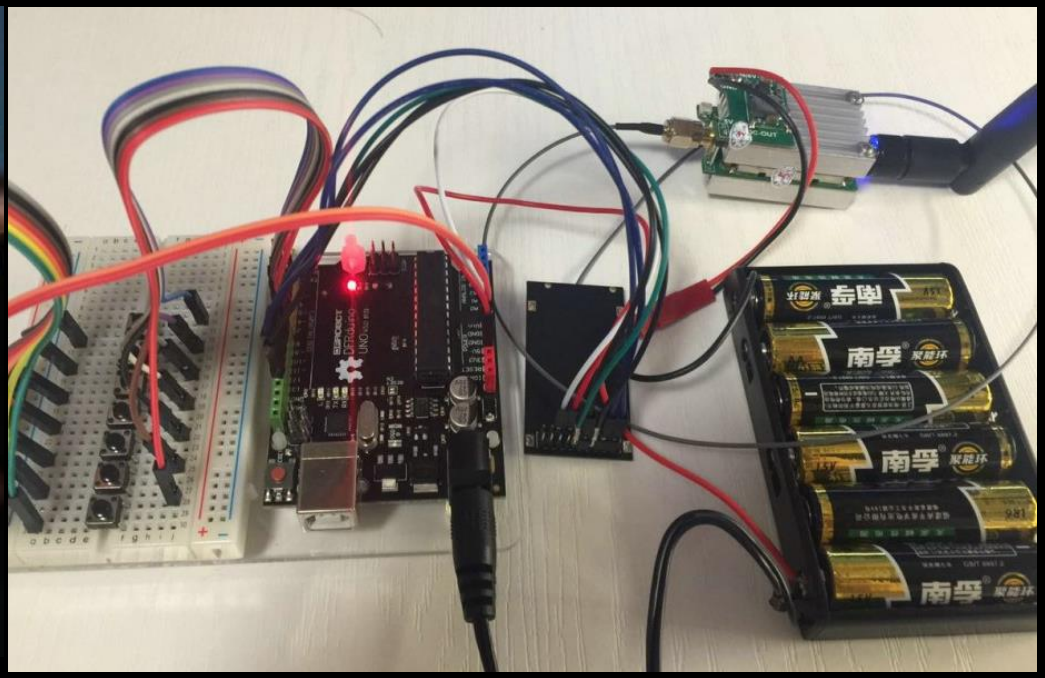
移动POS机劫持系统

时间	卡号	卡类型	消费金额	加密口令	操作
2015-08-04 18:12:19	622588******8809	磁条卡	￥0	A6F769******026174	开始劫持 删除
2015-08-03 18:02:19	622588******8809	磁条卡	￥0	5C04E8******9C0102	开始劫持 删除



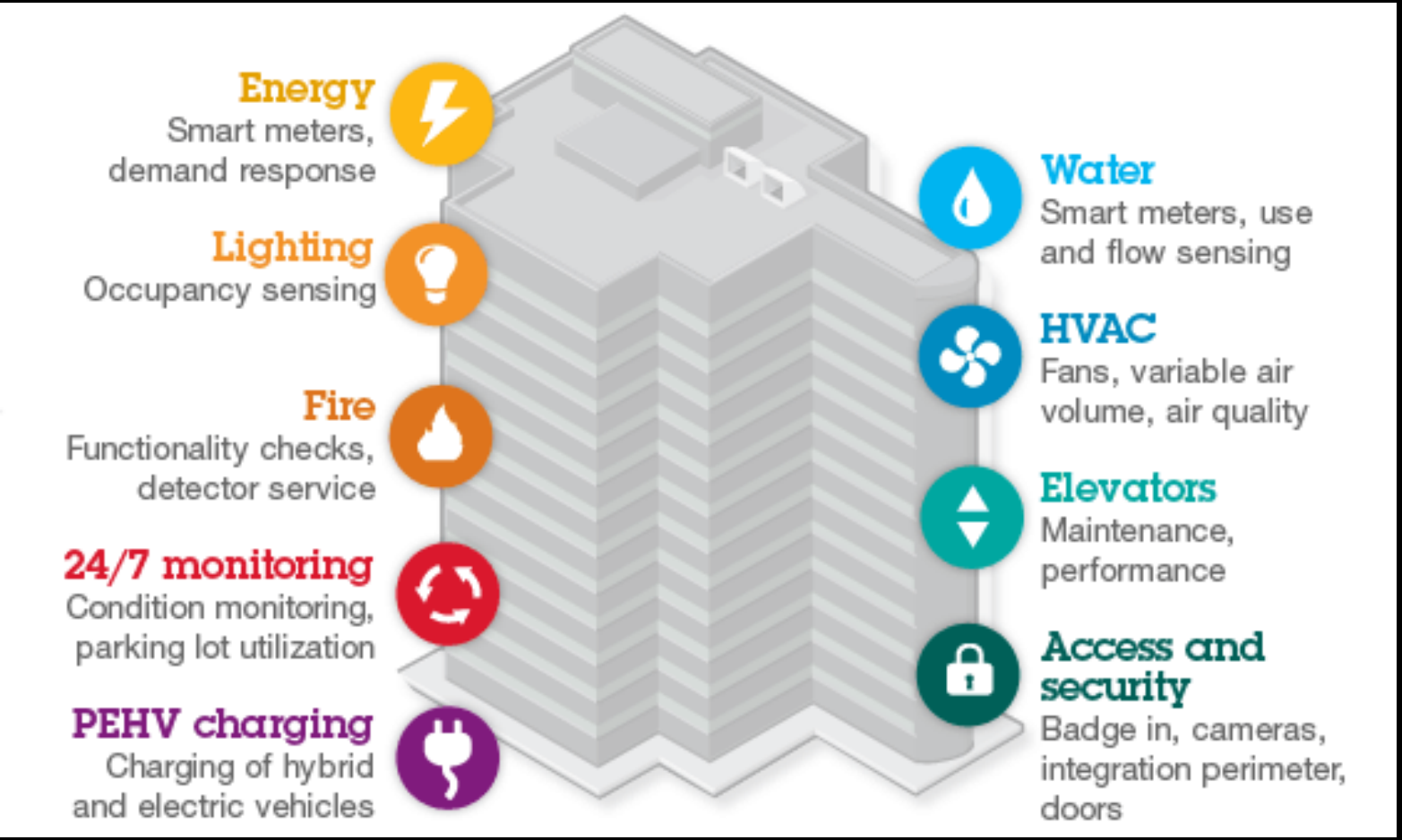
攻击智能摄像头

攻击DJI无人机



攻击智能楼宇

- 什么是智能楼宇



腾讯滨海大厦


More than 40 kinds of IoT devices
More than 20000 IoT nodes
More than 30000 employees

ZigBee设备的安全问题

	Info Leak	Insecure Encryption	Insecure Rejoin	Old ZigBee Protocol
Samsung	Y		Y	Y
ABB	Y	Y	Y	Y
XiaoMi	Y			Y
Others	Y	Y	Y	Y

ZomBee: ZigBee渗透测试工具

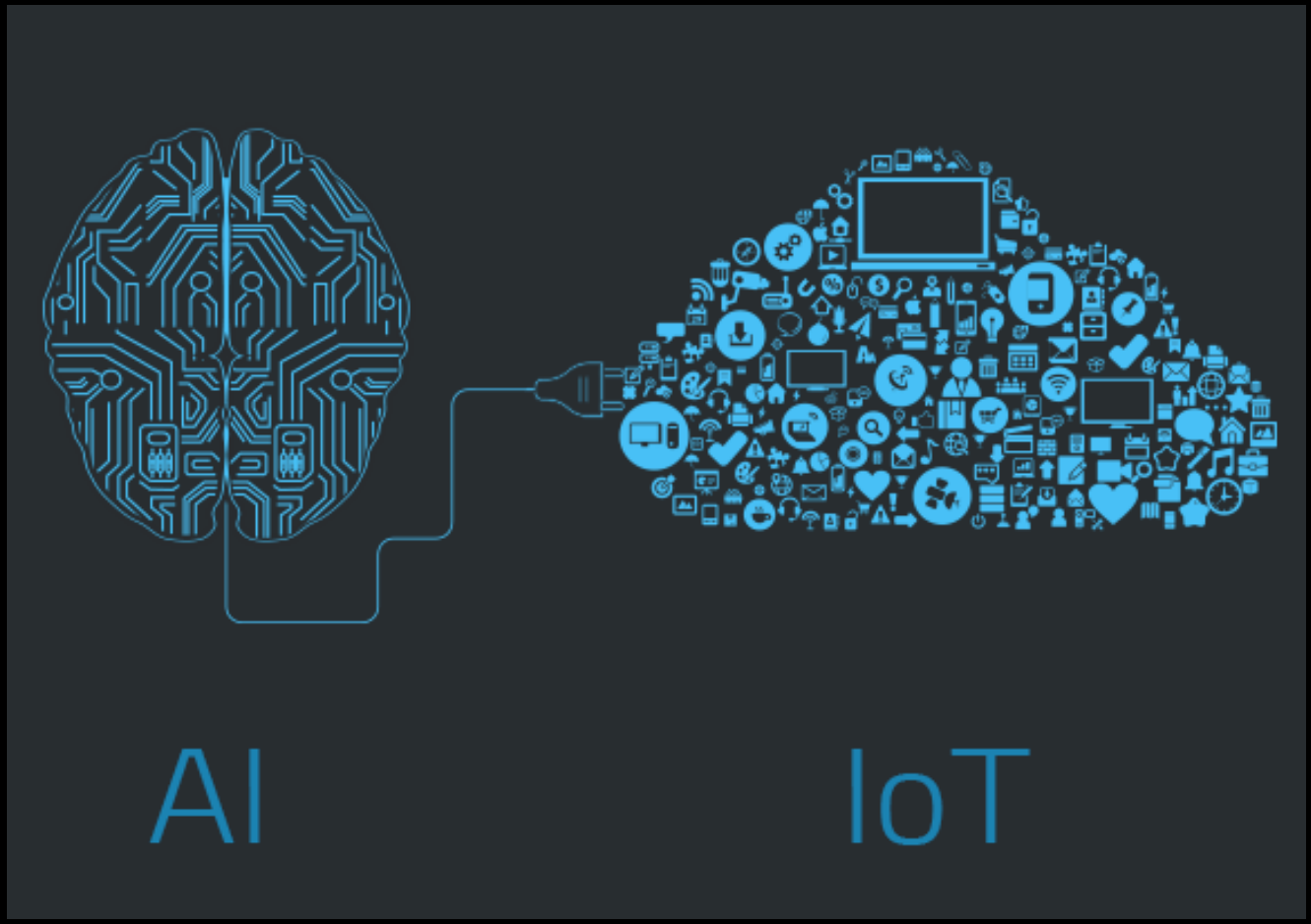
	Sniff Packet	Network Scan	Replay Packet	Insecure Rejoin	Auto Update NwkSeq / Frame Counter	Command Inject	Capture NWK Key	Batch Attack
KillerBee	YES	YES	YES					
SecBee	YES	YES		YES			YES	
Z3sec	YES	YES			YES	YES	YES	
ZomBee	YES	YES	YES	YES	YES	YES	YES	YES

远程攻击智能楼宇

BLADE Tencent Blade

远程攻击智能楼宇

AI时代-新的攻击面？



https://www.iotevents.org/event/artificial-intelligence-meets-internet-things/

TensorFlow第一个高危安全风险

TensorFlow恶意模型导致代码执行

腾讯报告TensorFlow首个安全风险 谷歌确认并致谢

腾讯科技 2017-12-15 19:59

日前，腾讯发现谷歌人工智能学习系统TensorFlow存在严重安全风险，可被黑客利用带来安全威胁。据悉，该风险是TensorFlow首个自身安全风险，腾讯安全平台部预研团队已向谷歌报告这一风险并获得致谢。

TensorFlow其他内存破坏漏洞

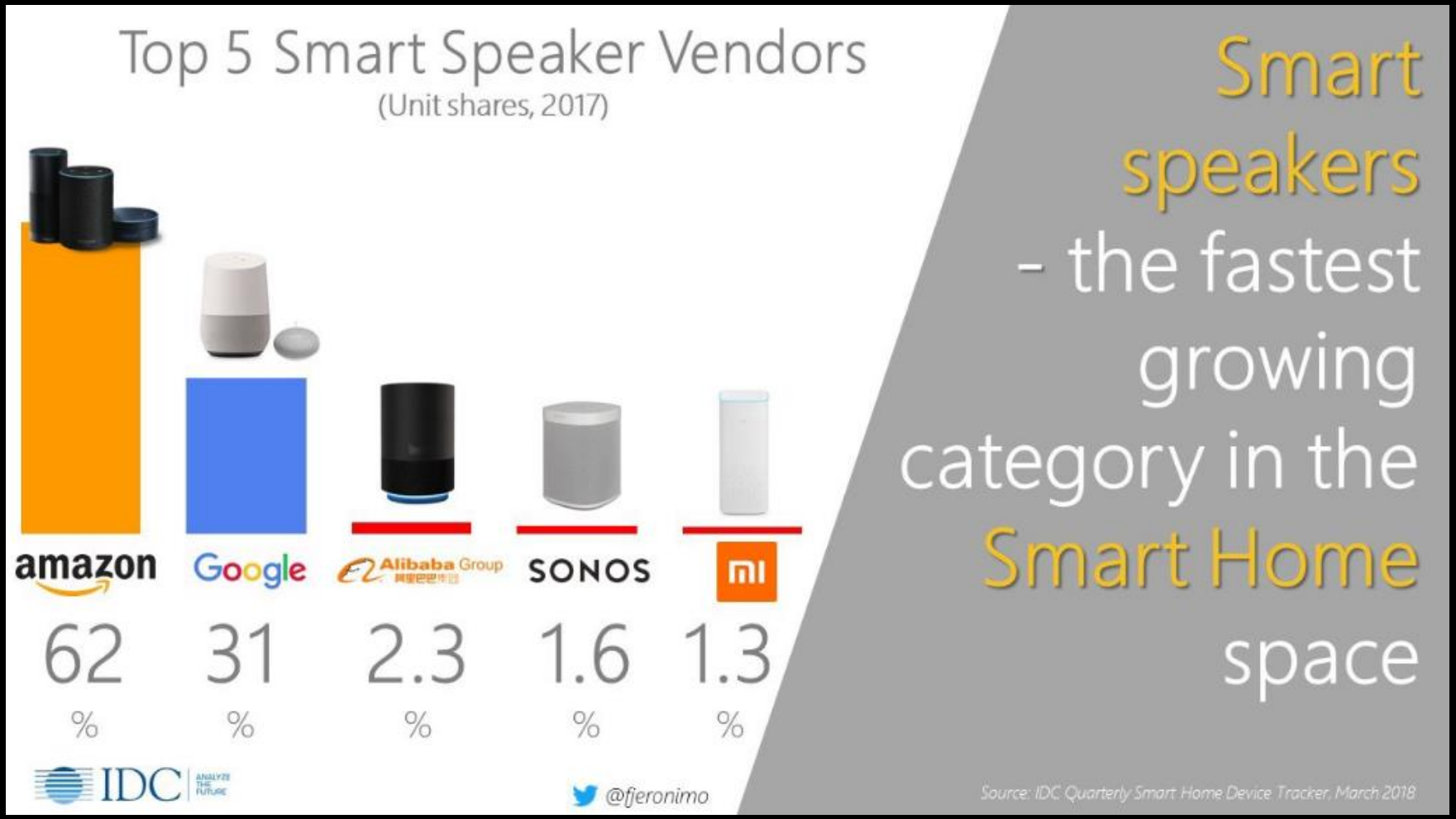
TensorFlow Security Advisories

We regularly publish security advisories about using TensorFlow.

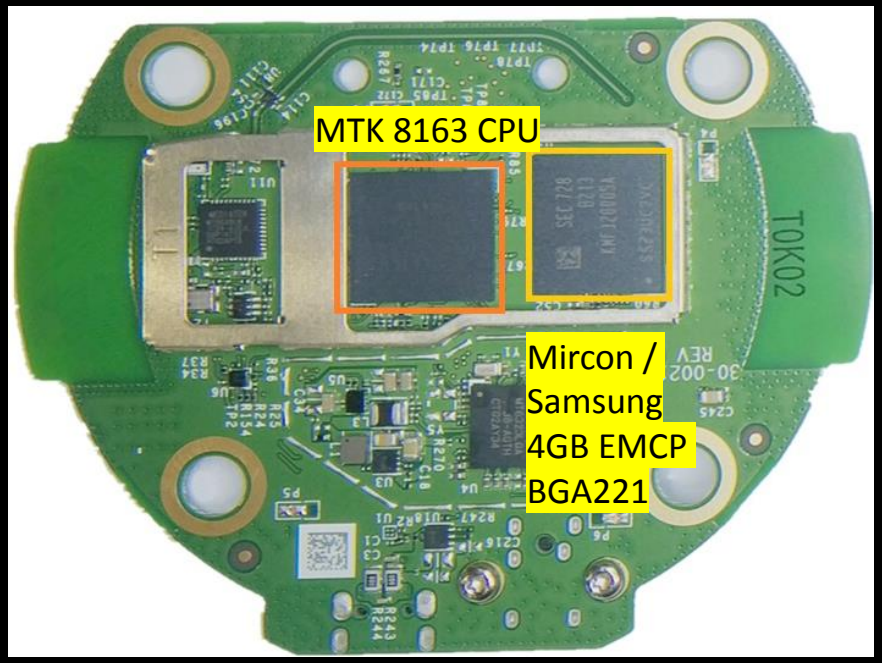
Note: In conjunction with these security advisories, we strongly encourage TensorFlow users to read and understand TensorFlow's security model as outlined in SECURITY.md.

Advisory Number	Type	Versions affected	Reported by	Additional Information
TFSA-2018-006	Crafted Configuration File results in Invalid Memory Access	<= 1.7	Blade Team of Tencent	
TFSA-2018-005	Old Snappy Library Usage Resulting in Memcpy Parameter Overlap	<= 1.7	Blade Team of Tencent	
TFSA-2018-004	Checkpoint Meta File Out-of-Bounds Read	<= 1.7	Blade Team of Tencent	
TFSA-2018-003	TensorFlow Lite TOCO FlatBuffer Parsing Vulnerability	<= 1.7	Blade Team of Tencent	
TFSA-2018-002	GIF File Parsing Null Pointer Dereference Error	<= 1.5	Blade Team of Tencent	
TFSA-2018-001	BMP File Parser Out-of-bounds Read	<= 1.6	Blade Team of Tencent	
-	Out Of Bounds Read	<= 1.4	Blade Team of Tencent	issue report

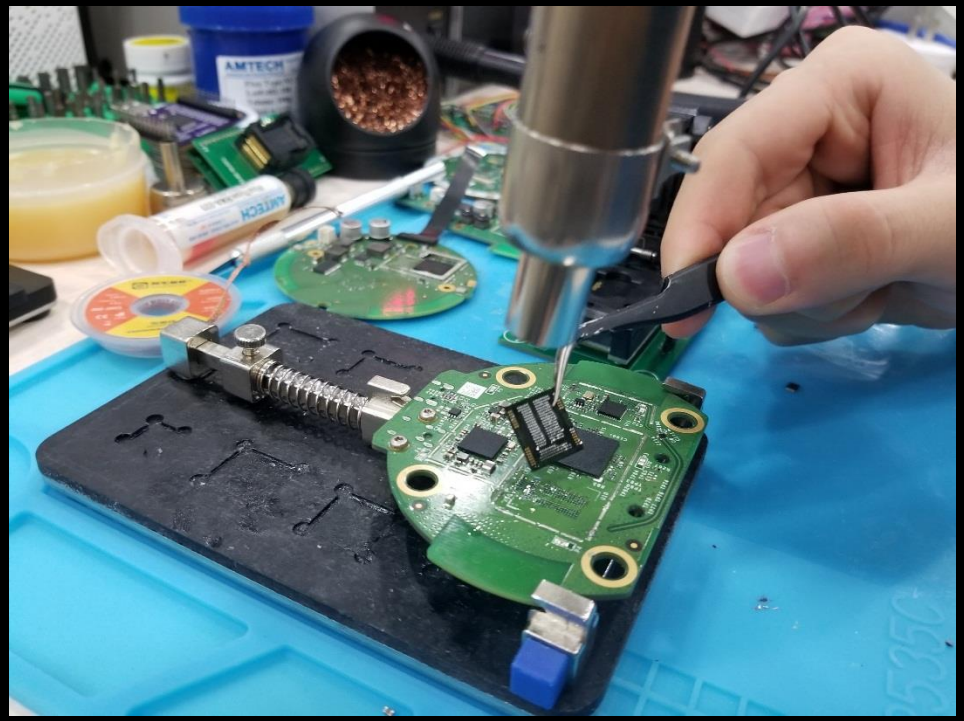
攻击Amazon Echo智能音箱



Amazon Echo介绍



固件提取和修改



焊下FLASH芯片

焊接设备

搭建Root调试环境

```
root@kali:~# adb devices
List of devices attached
G090LF1180950M8C        device

root@kali:~# adb shell su
root@biscuit:/data/data # id
id
uid=0(root) gid=0(root) context=u:r:su:s0
root@biscuit:/data/data # cat /system/build.prop
cat /system/build.prop

# begin build properties
# autogenerated by buildinfo.sh
ro.build.id=LVY48F
ro.build.display.id=LVY48F
ro.build.version.incremental=272.6.0.8_user_608490720
ro.build.version.number=608490720
ro.build.mktg.fireos=Fire OS vNext
ro.build.version.name=Fire OS 5.5.2.2 (608490720)
ro.build.version.fireos=5.5.2.2
ro.build.version.fireos.sdk=4
ro.build.version.fireos=5.5.2.2
ro.build.version.fireos.sdk=4
ro.build.version.sdk=22
ro.build.version.codename=REL
ro.build.version.all_codenames=REL
ro.build.version.release=5.1.1
ro.build.version.security_patch=2017-12-01
```

代码执行：Whad中的缓冲区溢出

```
const char *con_len_str = mg_get_header(conn, "Content-Length");
if (con_len_str) {
    unsigned long con_len = atoi(con_len_str);
    if (con_len > 0) {
        conobj.postData = (char *)malloc(con_len + 1);
        if (conobj.postData != NULL) {
            // malloc may fail for huge requests
            mg_read(conn, conobj.postData, con_len);
            conobj.postData[con_len] = 0;
            formParams = conobj.postData;
            conobj.postDataLen = con_len;
        }
    }
}
```

user supplied value

atoi("-1"), returns a signed int
then **forced typecast** to unsigned int **0xffffffff**

0xffffffff (uint -1) will pass the check

integer overflow here, malloc(0)

dlmalloc, same as malloc(8), pass this check

heap buffer overflow here

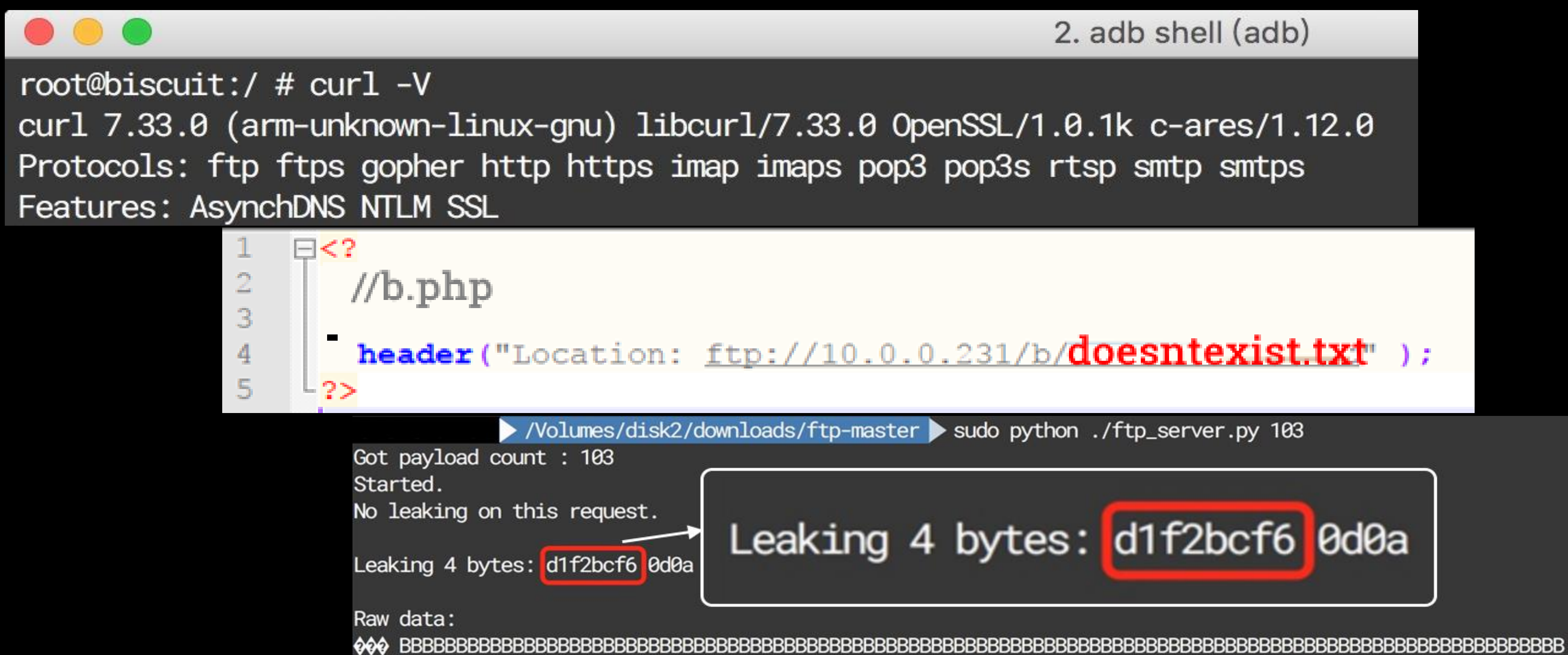
out-of-bounds write here, postData[-1]=0

potential **information leak** here, string not zero terminated, and return to the caller

https://github.com/civetweb/civetweb

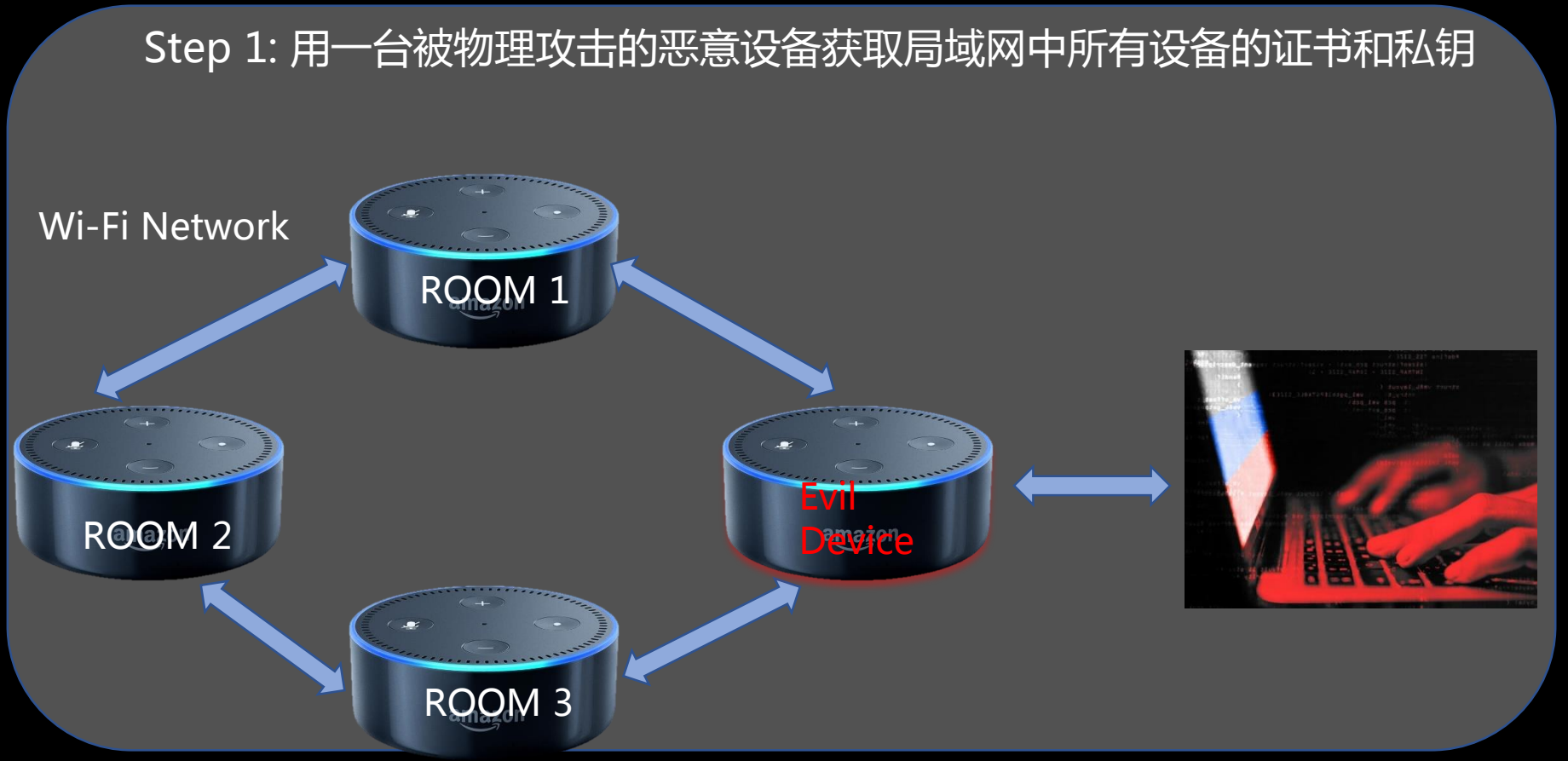
绕过ASLR：libcurl信息泄漏

- CVE-2017-1000254：libcurl在处理FTP连接时存在越界读，可被利用
- 可以控制Echo发送FTP请求，触发漏洞

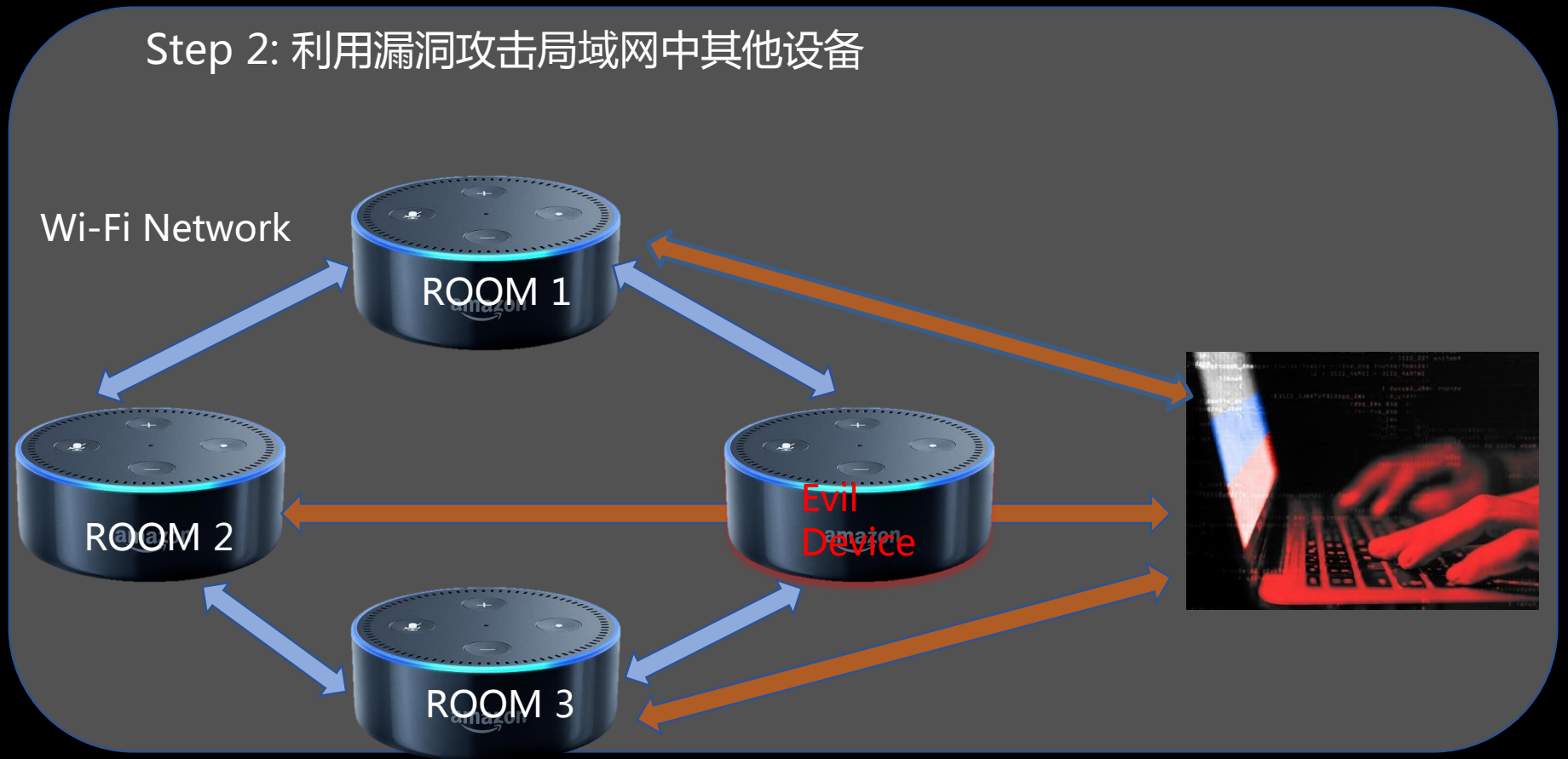


攻击过程-Step1

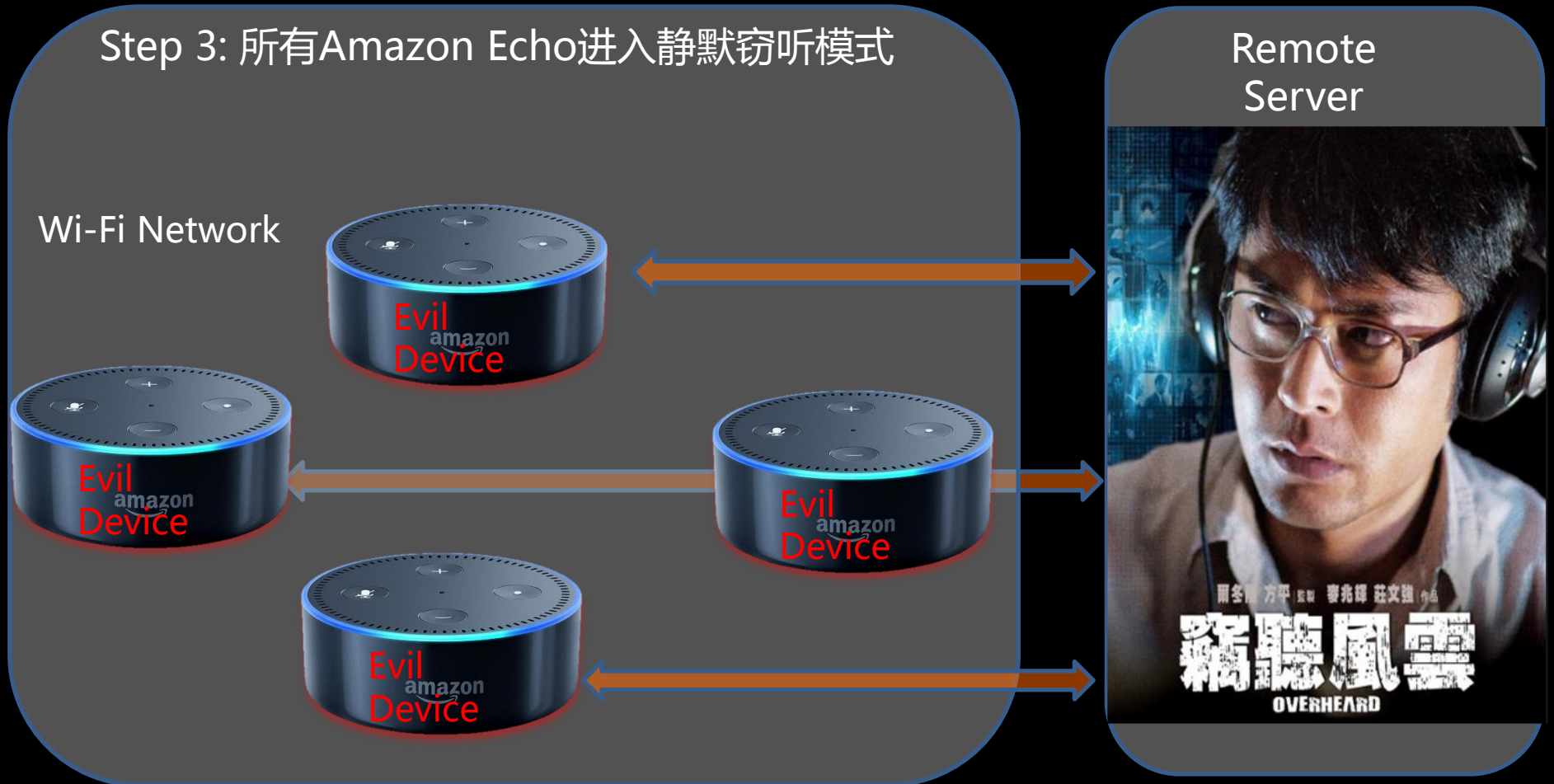
Step 1: 用一台被物理攻击的恶意设备获取局域网中所有设备的证书和私钥



攻击过程-Step2


Step 2: 利用漏洞攻击局域网中其他设备
Wi-Fi Network
ROOM 1
ROOM 2
ROOM 3
Evil Device

攻击过程-Step 3


Step 3: 所有Amazon Echo进入静默窃听模式
Wi-Fi Network
Evil Device
Evil Device
Evil Device
Evil Device
Remote Server
竊聽風雲
OVERHEARD

Amazon官方致谢

- 2018.5报告给Amazon，2018.7修复

  “Amazon would like to thank the Tencent Blade Team for working with us on resolving this issue. Customer trust is important to us and we take security seriously. Customers do not need to take any action as their devices have been automatically updated with security fixes.”

智能设备安全研究思路

CONTENTS

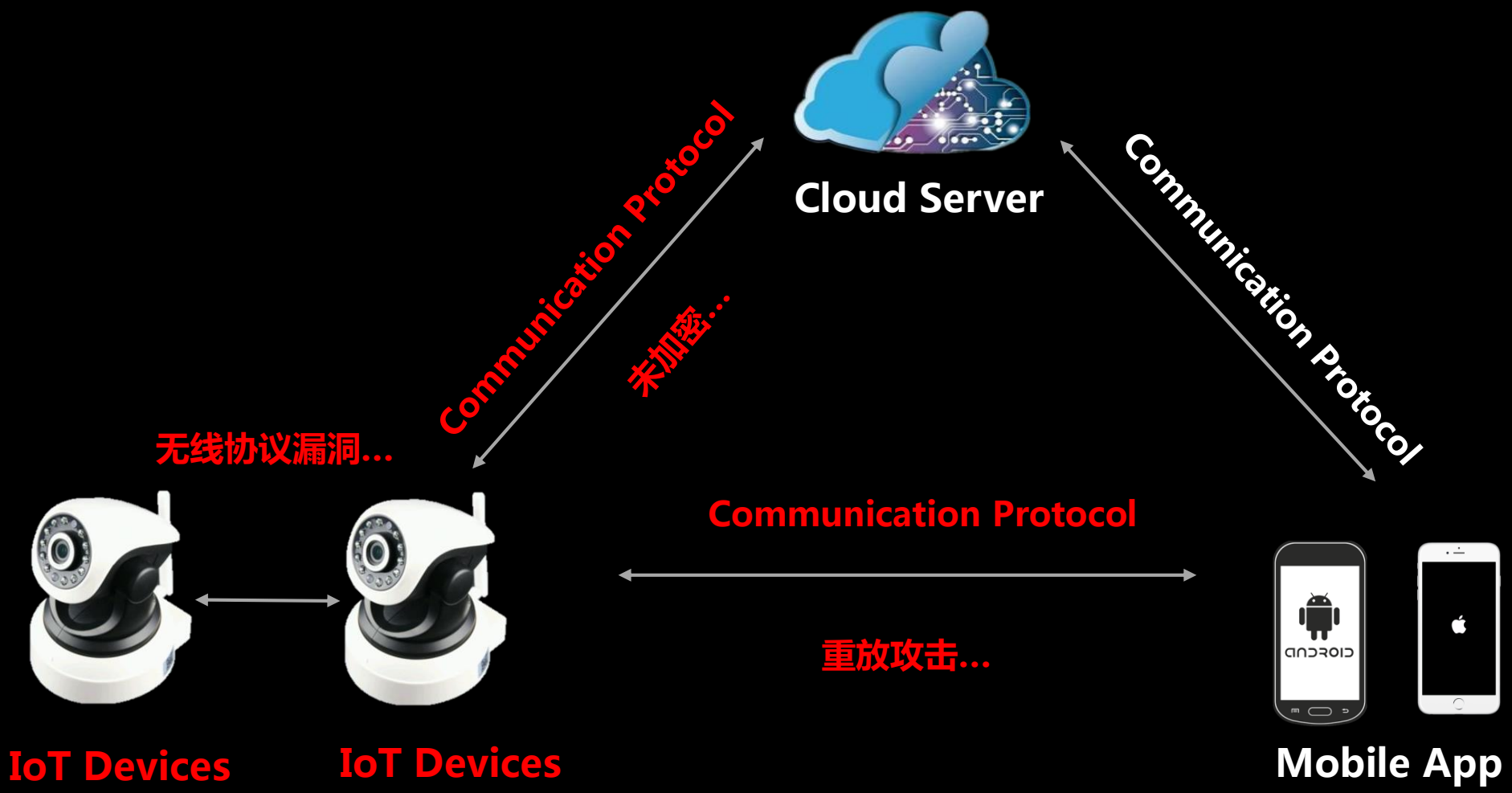
1.智能设备介绍

2.团队研究成果

3.智能设备安全研究思路

4.安全建议

智能设备攻击面-协议


Cloud Server
Communication Protocol
未加密...
Communication Protocol
无线协议漏洞...
Communication Protocol
重放攻击...
IoT Devices
IoT Devices
Mobile App

智能设备攻击面-设备

硬件：Flash提取
软件：截获OTA
…

静态：IDA
动态：模拟执行
…

开放服务
第三方库
…

硬改：重刷Flash
软改：篡改升级包
…

代码执行
绕过mitigations
…

安全建议

CONTENTS

1.智能设备介绍

2.团队研究成果

3.智能设备安全研究思路

4.安全建议

安全建议

- 现状：类比手机安全性的提升

智能手机	智能设备
标准化： 硬件：SoC，sensor 软件：Android/iOS 协议：Wi-Fi，BlueTooth	碎片化： 硬件：大厂小厂参差不齐 软件：OpenWrt，定制linux 协议：ZigBee, 私有协议等
安全意识： 普通民众普及 厂商重视	安全意识： 未全面普及 大厂开始重视(Google/Amazon)
安全社区； 白帽子积极参与	安全社区： 逐渐被主流社区认可(Pwn2Own 2018)

安全建议

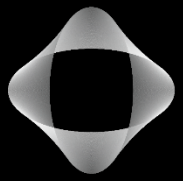
- 云端：WAF/HIDS/防DDoS...
- 移动APP：APP漏洞扫描/加固...
- 协议：
  - 加密(https)，设备端不存储密钥
  - 防重放攻击
  - 使用最新版协议标准
  - ...

安全建议

- 智能设备端：
  - 硬件/Firmware
    - 移除调试口(JTAG/UART等)
    - Secure Boot：Firmware/kernel完整性
    - DM-verity：系统镜像完整性
  - 软件
    - 安全开发规范(C/C++)，代码审计/Fuzz
    - 使用新版第三方库，定期更新
    - TEE：敏感数据及组件放在TEE中
    - 基本的Mitigations：DEP/ASLR/Stack Protection

愿景

- Tencent Blade Team愿与厂商和安全社区有更多的交流合作，共同提升智能设备的安全性



腾讯安全平台部
Tencent Security
Platform Dpt.

腾讯安全应急响应中心
Tencent Security Response Center

BLADE Tencent Blade

Thanks!