TENCENT SECURITY CONFERENCE 2018
2018腾讯安全国际技术峰会

The Future Is Here :

IoT Devices Security

lakehu / lake2

Director of Tencent Security Platform Department

Leader of Tencent Blade Team

About Tencent Blade Team

- Founded By **Tencent Security Platform Department**.
- Focus on security research of AI, IoT & Mobile devices.
- Found 100+ security vulnerabilities (Google, Apple).
- Contact us: **https://blade.tencent.com**

BLADE Tencent Blade

Agenda

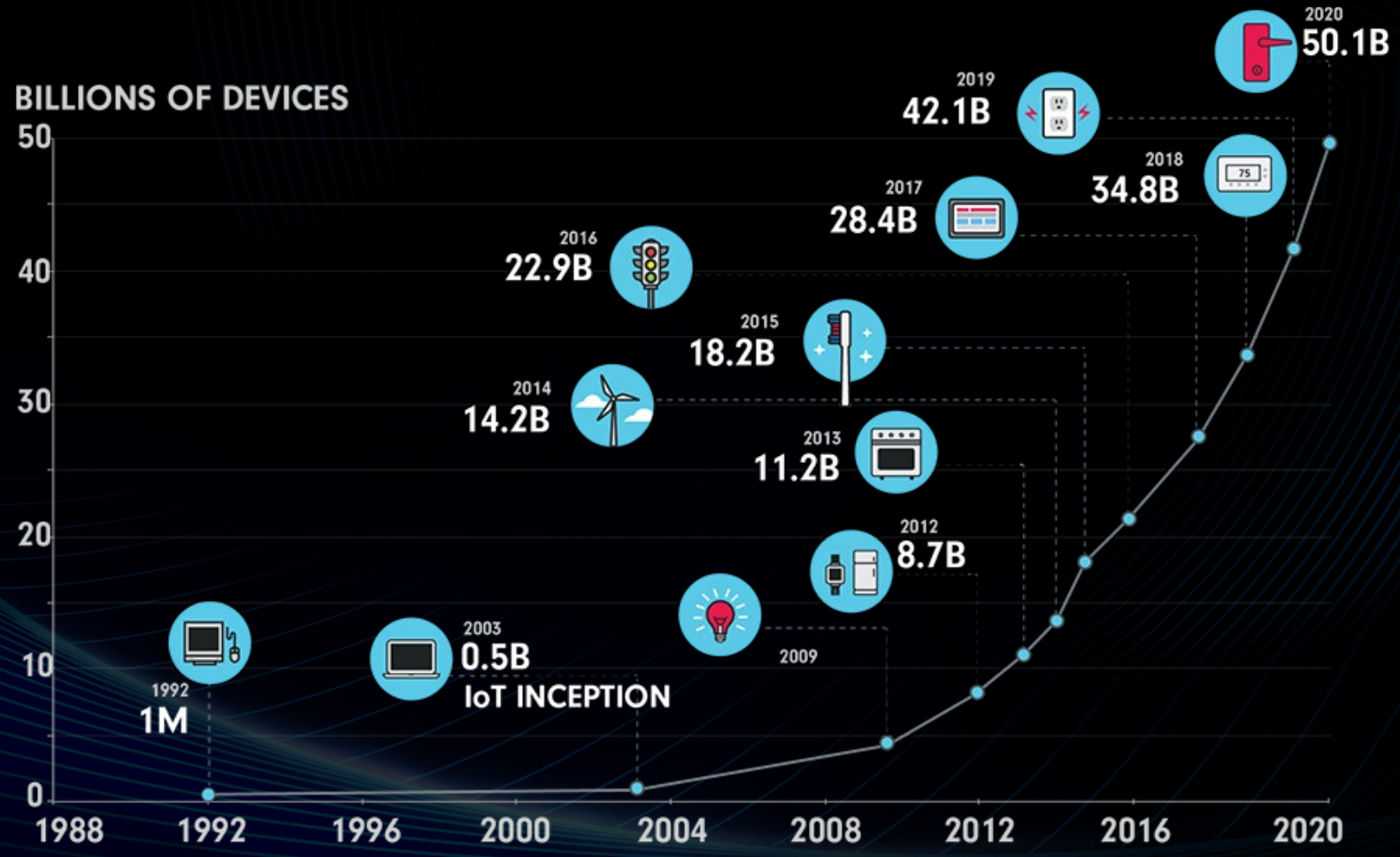
- Introduction to IoT Devices
- Our Research
- How to secure your IoT Product
- Summary

Introduction to IoT Devices

What is IoT Devices

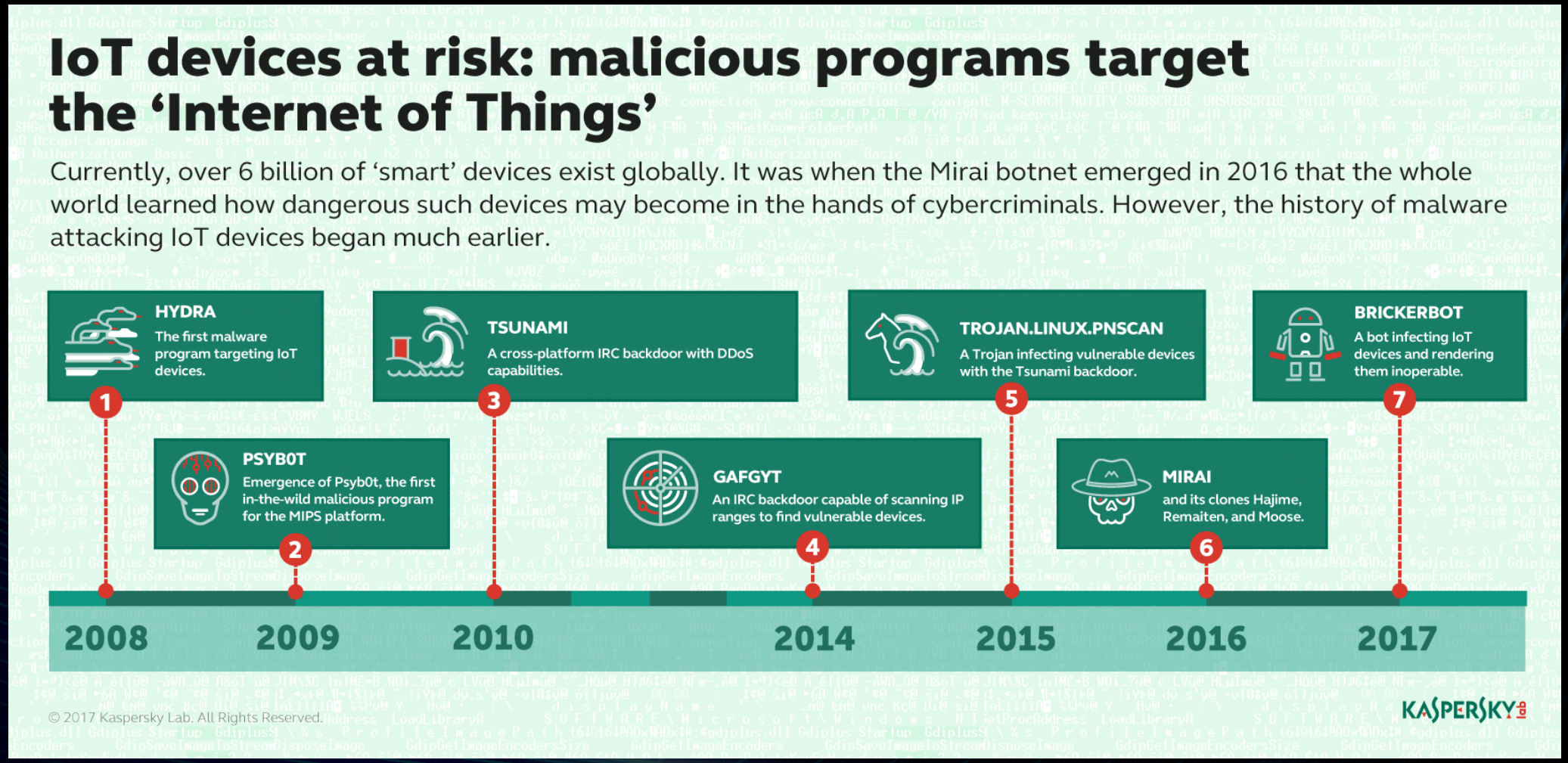
Ref: https://hackernoon.com/internet-of-everything-the-iot-market-is-projected-to-expand-12x-from-2017-2023-175f845c2bcf

Rapid Growth of IoT



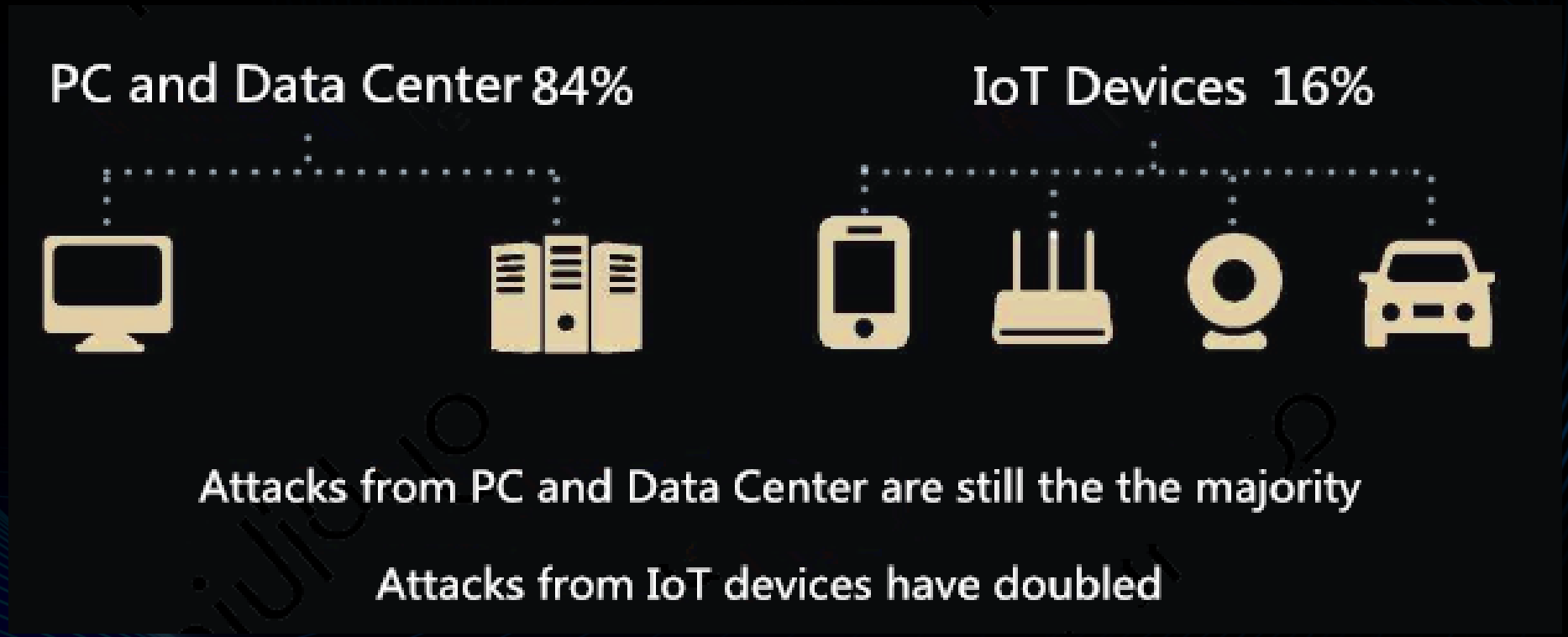
Ref: https://hackernoon.com/internet-of-everything-the-iot-market-is-projected-to-expand-12x-from-2017-2023-175f845c2bcf

Increased Attacks on IoT



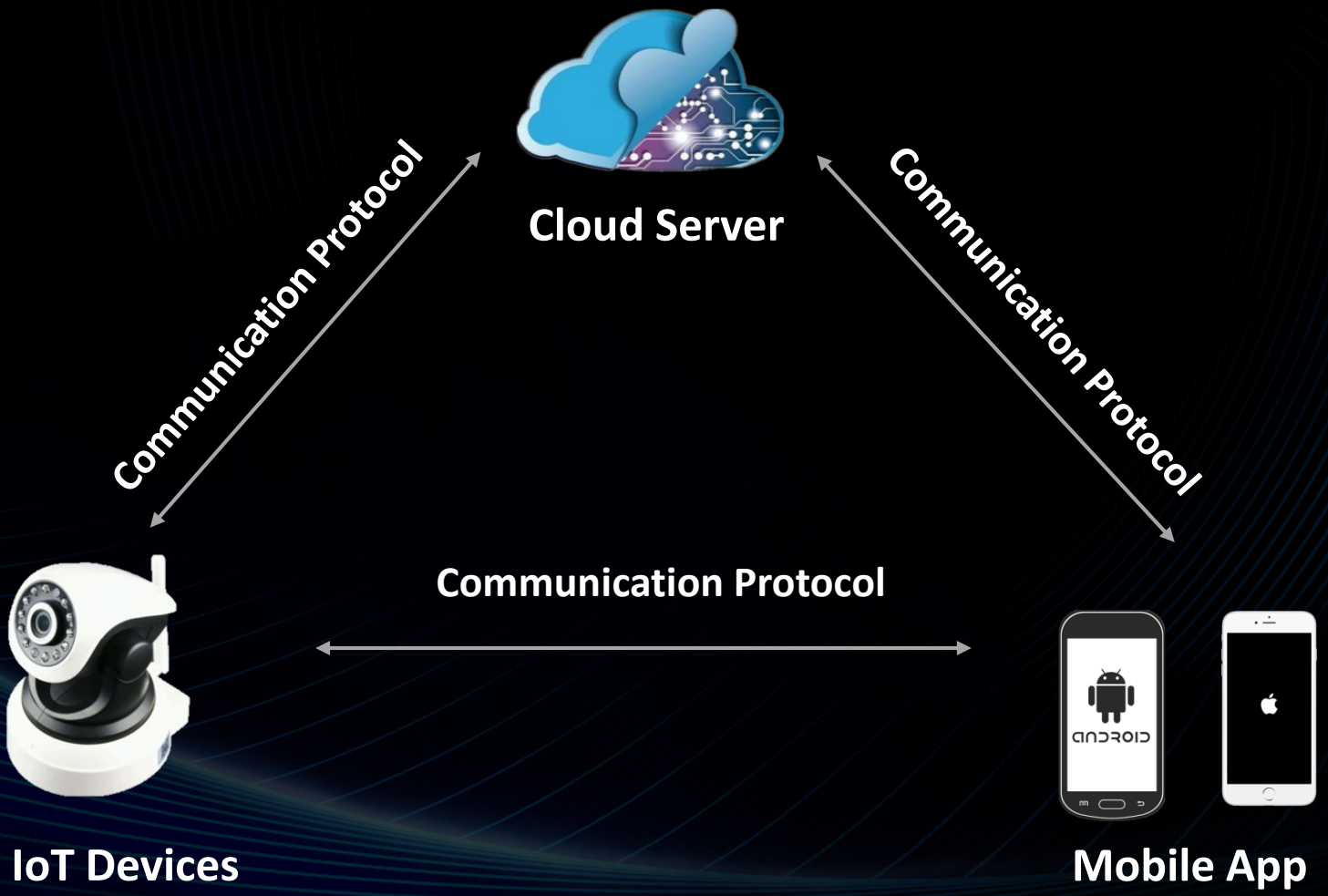
Ref: https://twitter.com/appknox/status/1031443217605124096

Increased Attacks on IoT



Our Research

Attack Surface of IoT Devices



Hack IoT Devices for Fun




Pwning Smart Socket （ GeekPwn 2014 ）

Insecure Authentication

Pwning Smart Oven (GeekPwn 2015)

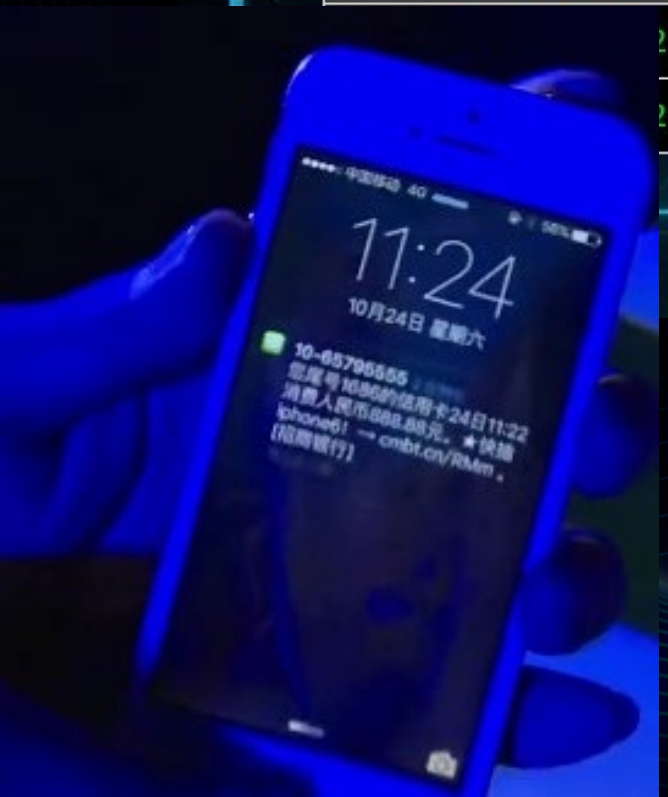
Pwning Smart Oven (GeekPwn 2015)

Hard Coded & HTTP Plaintext Transmission

Pwning Mobile POS (GeekPwn 2015)

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
2:19	622588******8809	磁条卡	¥ 0	A6F769******026174	开始劫持 删除
2:19	622588******8809	磁条卡	¥ 0	5C04E8******9C0102	开始劫持 删除

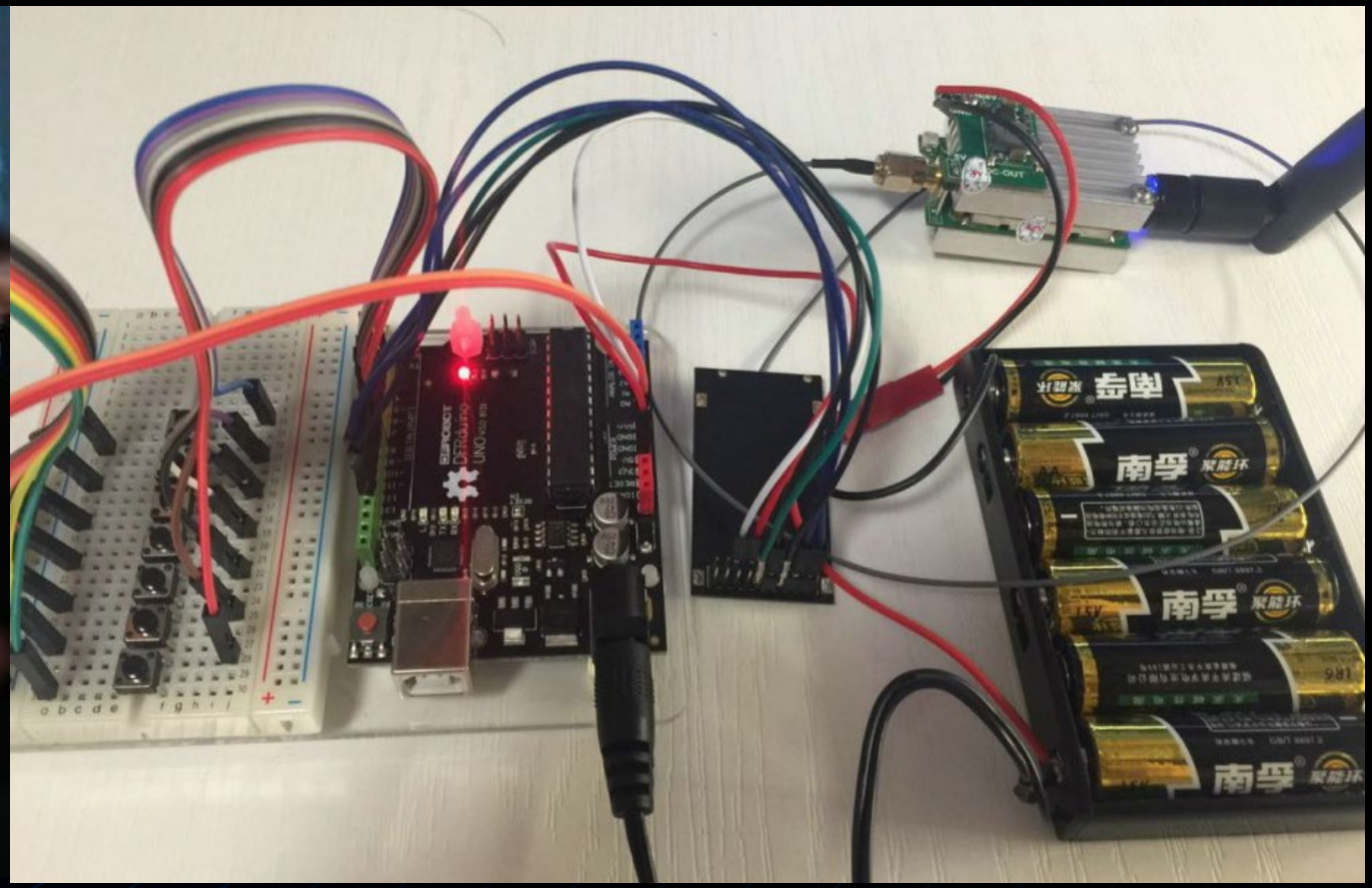


Replay Attack

Pwning Smart Camera（GeekPwn 2014）

Traffic Hijacking

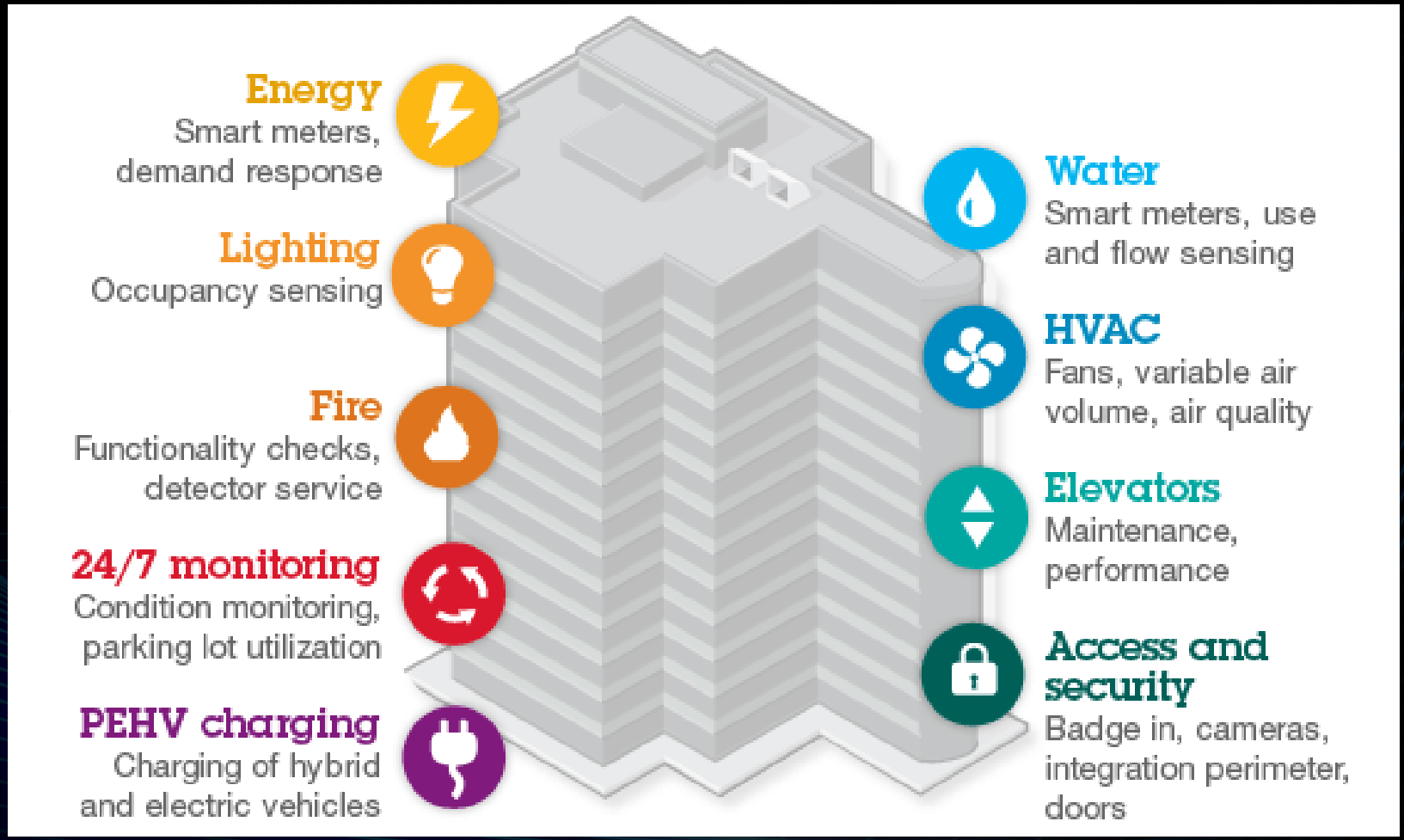
Pwning DJI Drone (GeekPwn 2015)



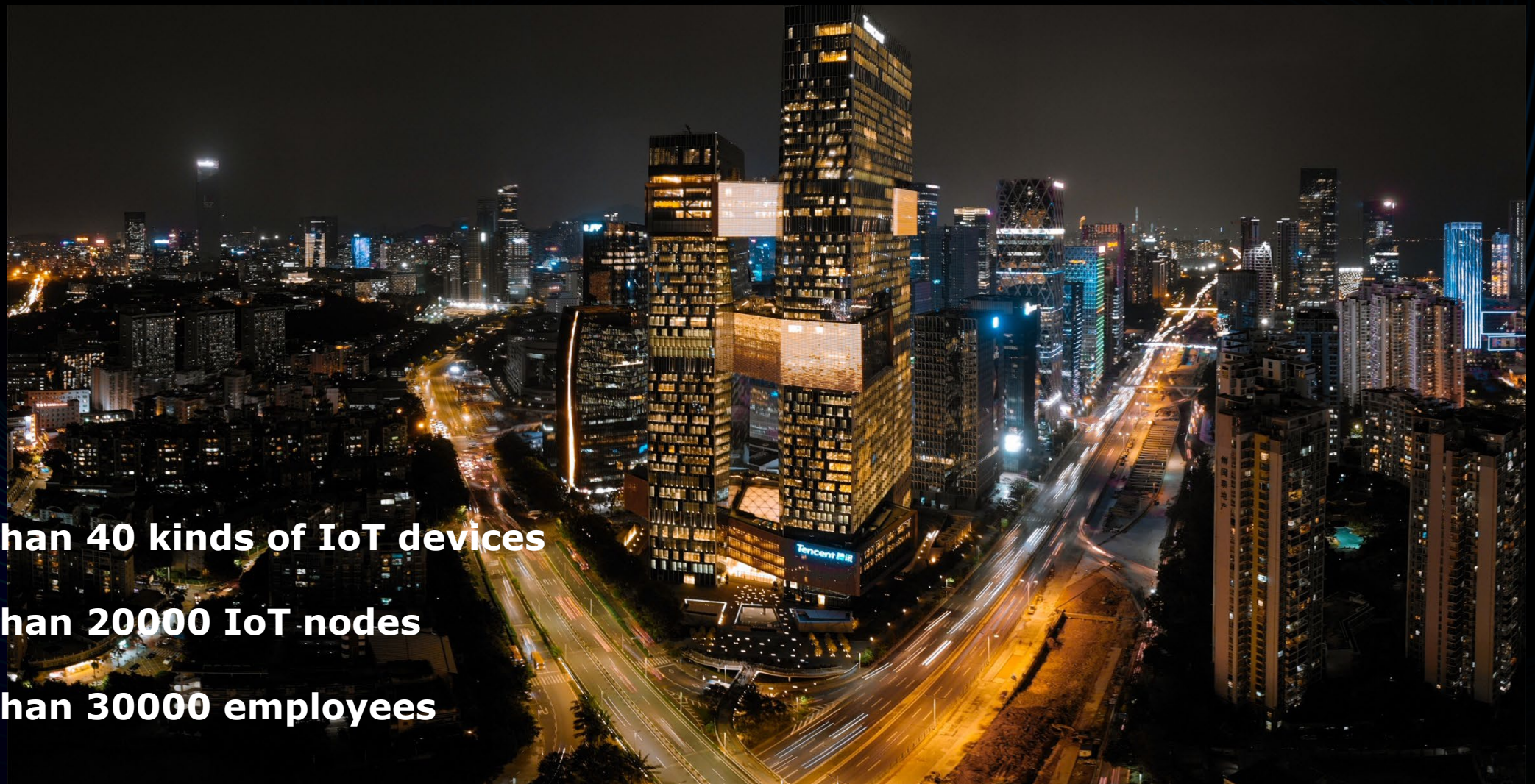
Radio Frequency Signal Hijacking

Remote Attack Intelligent Building

What is Intelligent Building



Tencent Binhai Building（HITB 2018 AMS）



More than 40 kinds of IoT devices

More than 20000 IoT nodes

More than 30000 employees

Security Risk in ZigBee Devices

	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: A New ZigBee Pentest tools

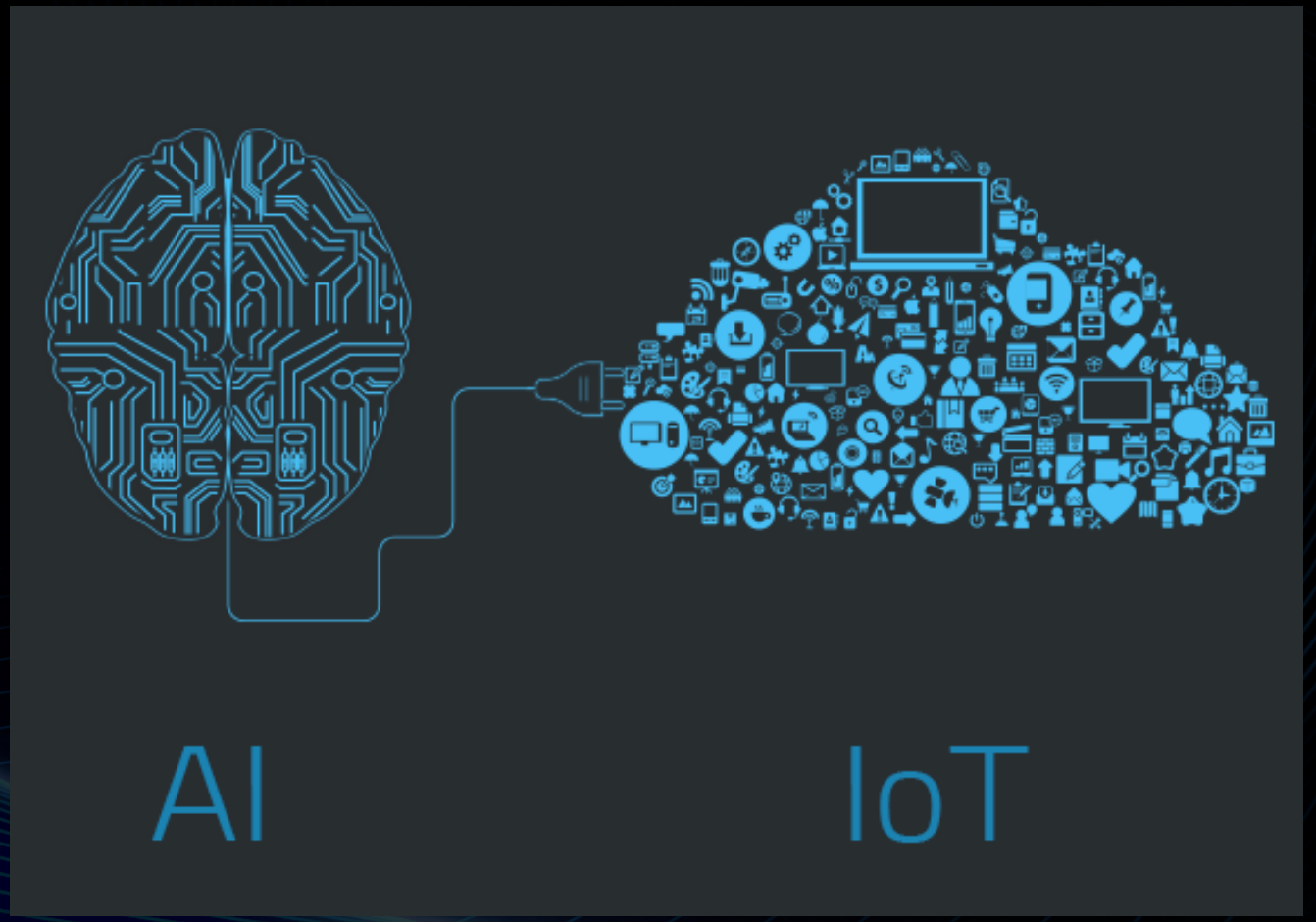
	Sniff Packet	Network Scan	Replay Packet	Insecure Rejoin	Auto Update NwkSeq / Frame Counter	Command Inject	Capture NWK Key	Batch Attack
KillerBee	YES	YES	YES					
SecBee	YES	YES		YES			YES	
Z3sec	YES	YES			YES	YES	YES	
ZomBee	YES	YES	YES	YES	YES	YES	YES	YES

Remote Attack Intelligent Building

Remote Attack Intelligent Building

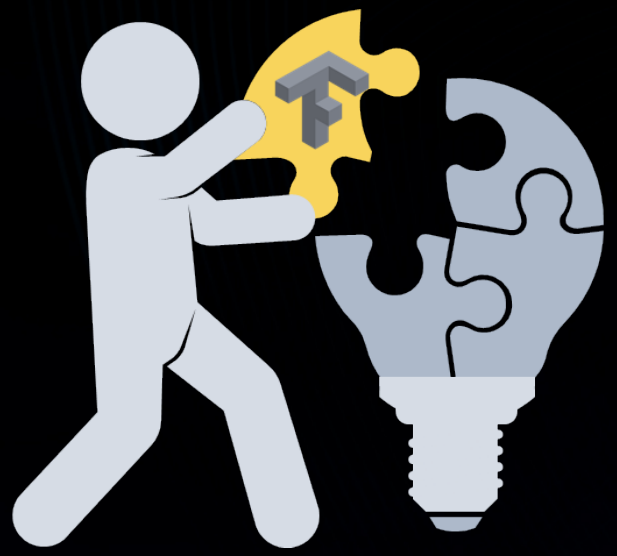
Attack AI + IoT

New Attack Surface in IoT Devices



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

First Vulnerability in Google TensorFlow



security@tensorflow.org

TensorFlow Security Advisories

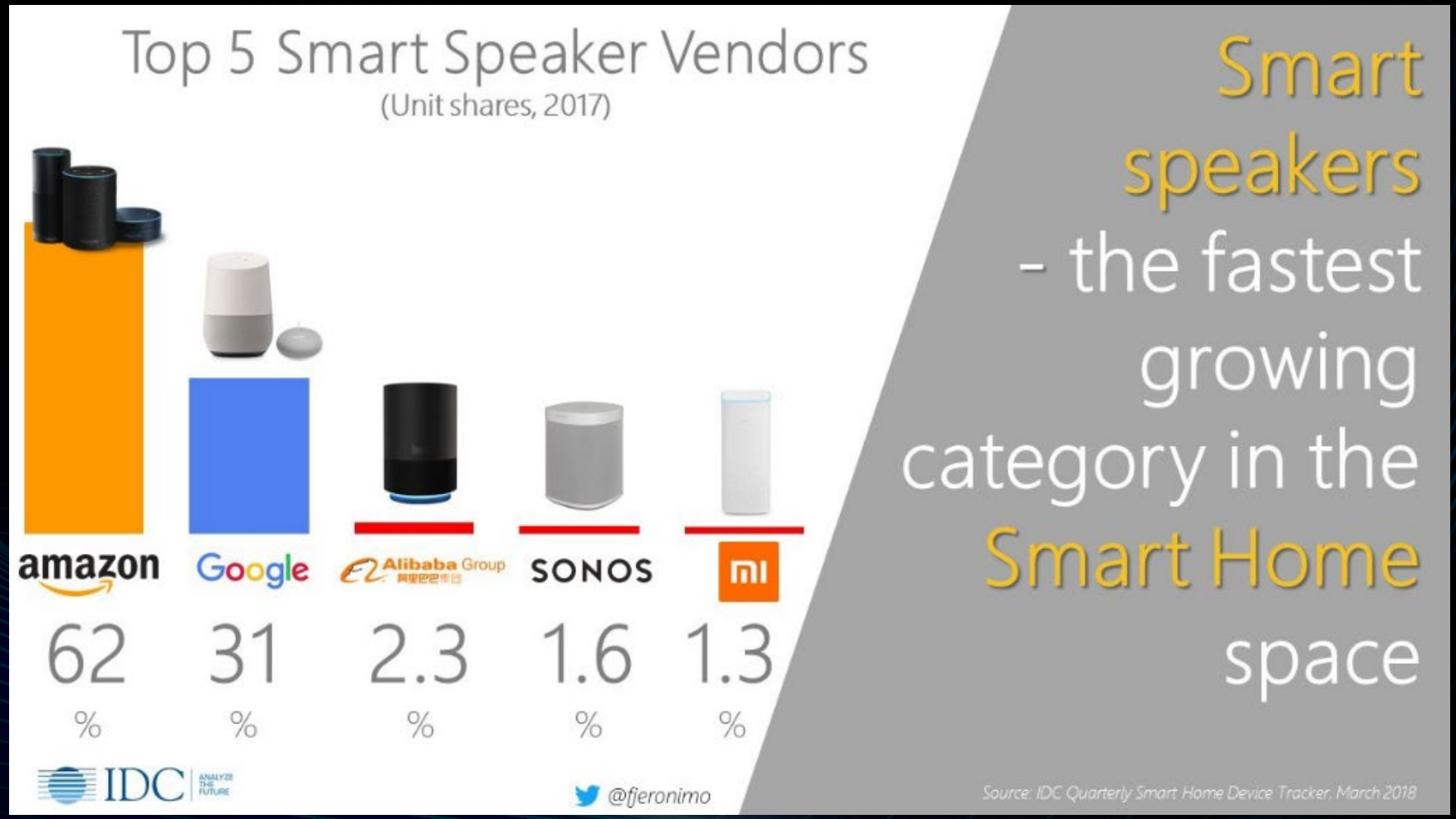
We regularly publish security advisories about using TensorFlow.

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.

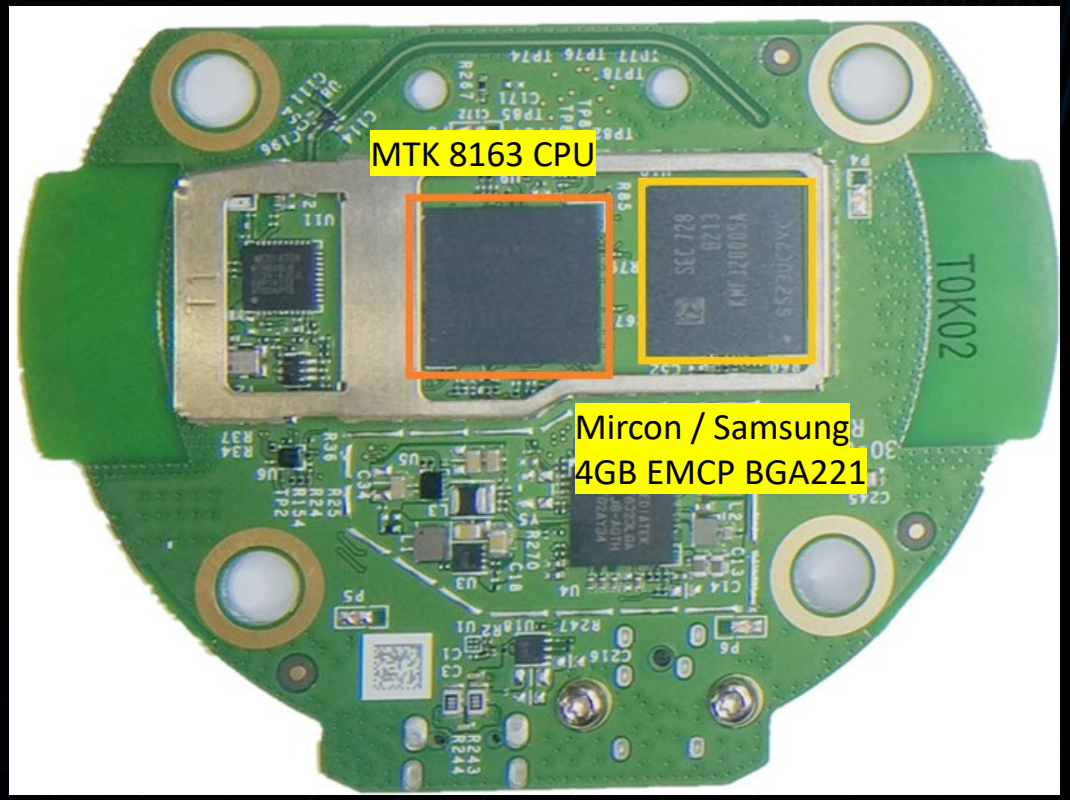
Advisory Number	Type	Versions affected	Reported by	Additional Information
TFSA-2018-006	Crafted Configuration File results in Invalid Memory Access	<= 1.7	Blade Team of Tencent	
TFSA-2018-005	Old Snappy Library Usage Resulting in Memcpy Parameter Overlap	<= 1.7	Blade Team of Tencent	
TFSA-2018-004	Checkpoint 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

Breaking Amazon Echo Speaker

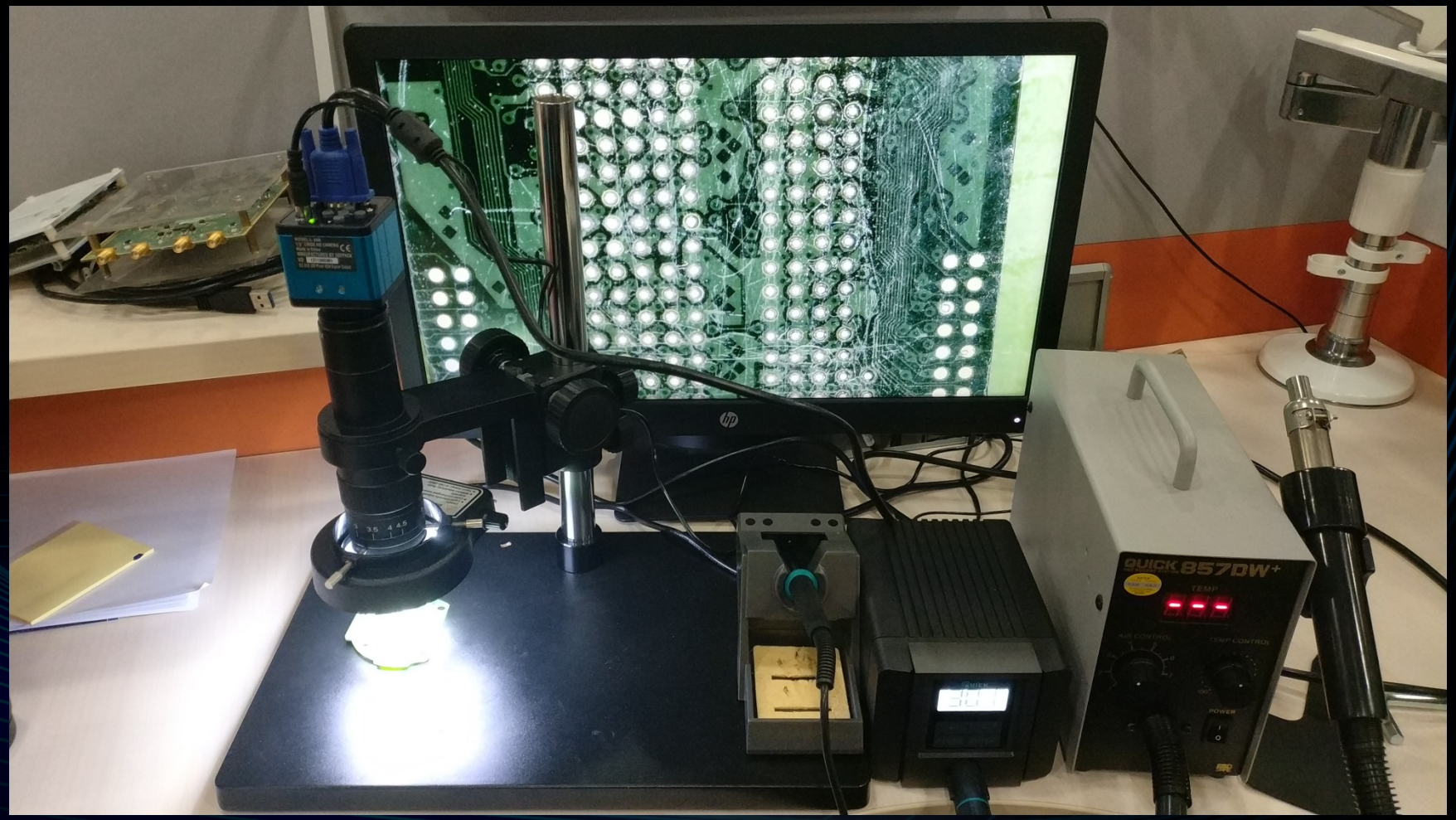
Amazon Echo Market Share



A Brief Look at Amazon Echo



Firmware Extraction and Modification



Building ROOT Debugging Environment

```
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
```

Heap Buffer Overflow in Amazon Echo Whad

```
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

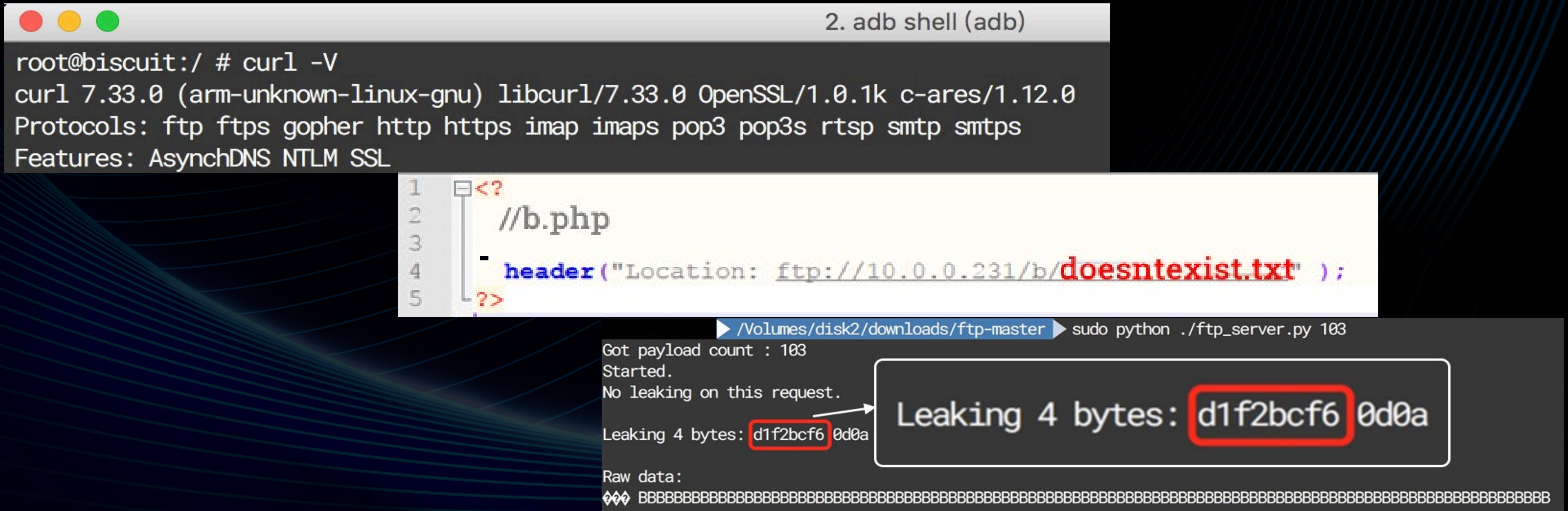
→ **out-of-bounds write** here, postData[-1]=0

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

https://github.com/civetweb/civetweb

Information Leak via Network

- CVE-2017-1000254 of libcurl in FTP connection is exploitable.
- To reproduce the vulnerability, we can control Echo to send a FTP request.

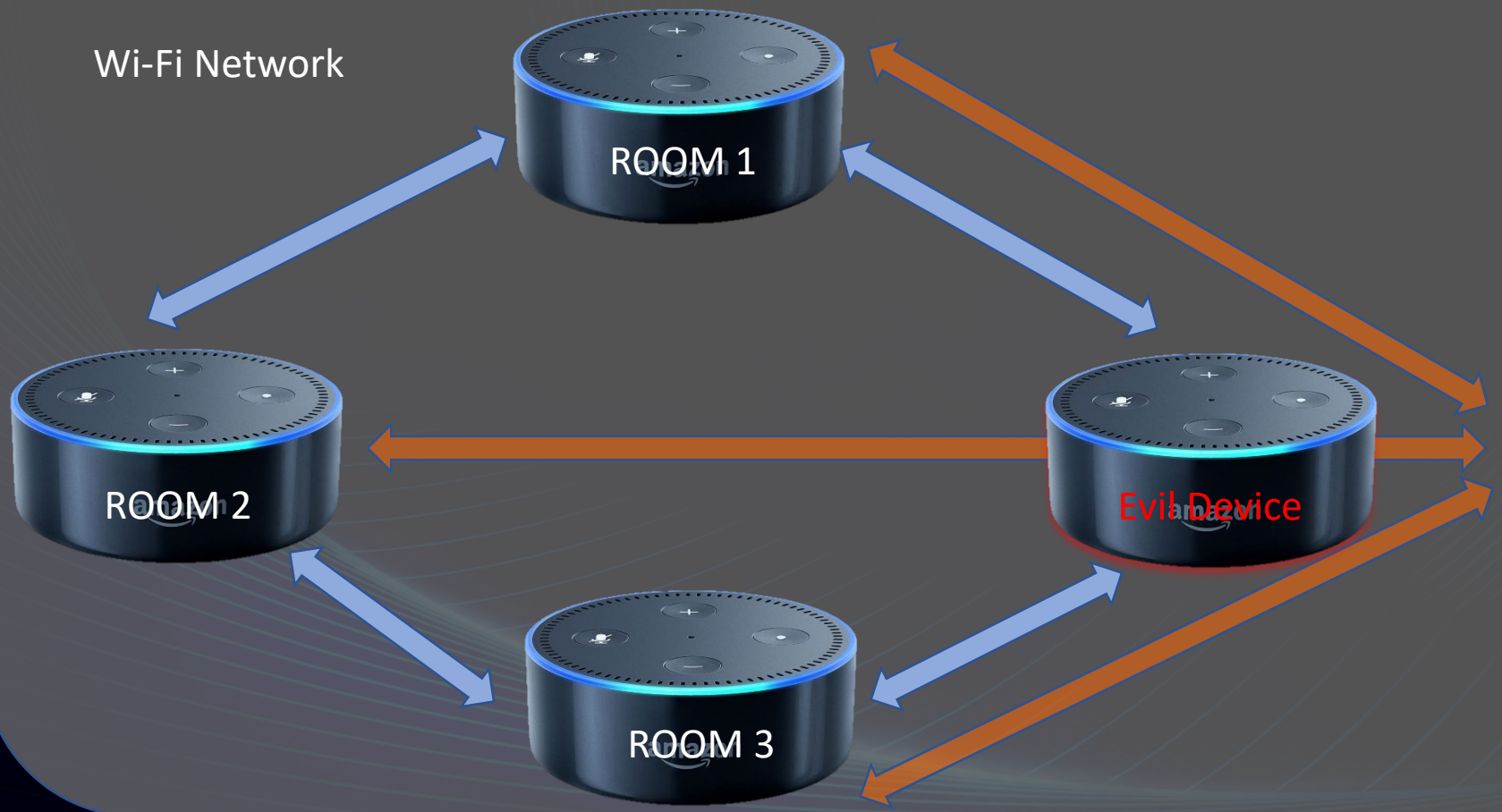


Attack Chain

Step 1: Use a physical hacked device to get all echo device's certs & private keys.

Attack Chain

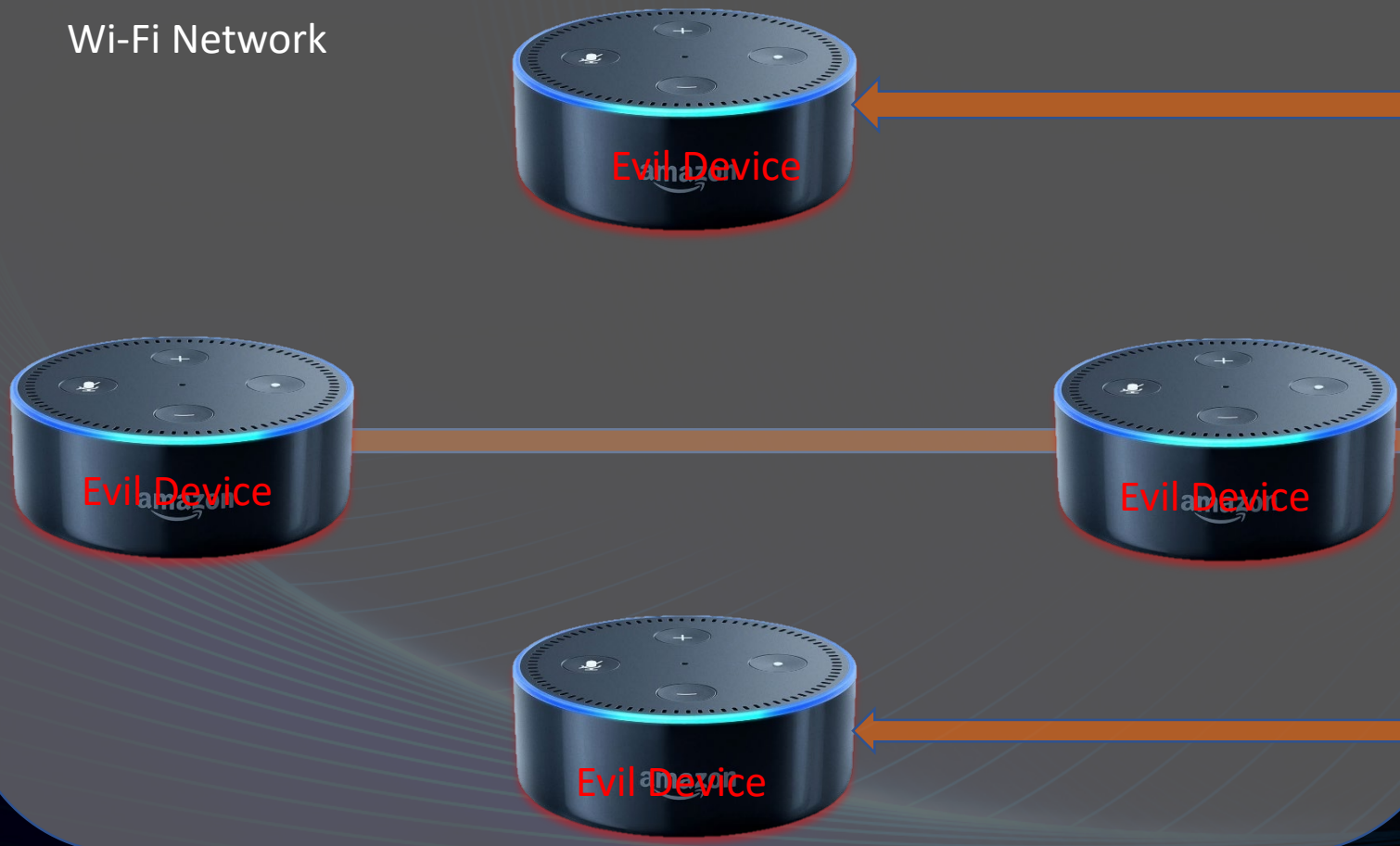
Step 2: Start attacking all devices in the LAN.



Attack Chain

Step 3: All Amazon Echo enter remote silent eavesdropping mode.

Wi-Fi Network



Remote Server

Acknowledgement

- Reported to Amazon in May, fixed in July.

> "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."

Acknowledgement

How to secure your IoT Products

SDL

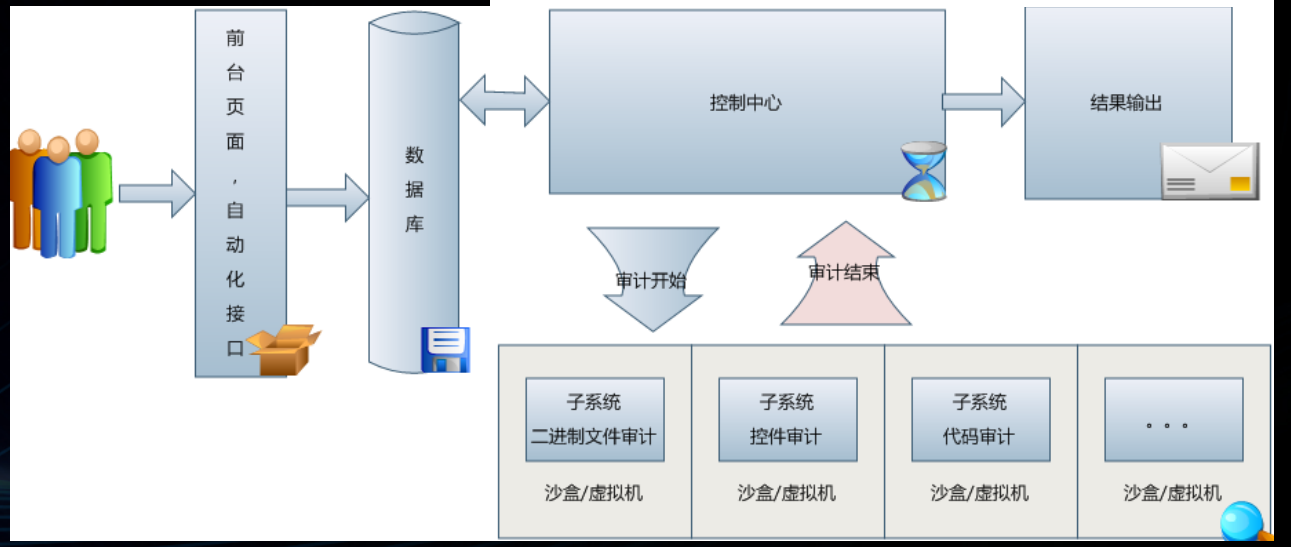

Training
Requirements
Design
Implementation
Verification
Release
Response
安全技术培训
安全意识培训
安全规范
安全需求建立
质量标准建立
风险识别
安全设计
攻击面分析
威胁建模
提供安全开发工具
安全开发规范和最佳实践
安全API
代码审计
渗透测试
应急响应方案
上线前集成环境安全检查
安全运维规范
应急响应执行
人工巡查
漏洞扫描系统
安全情报系统

IoT Security Specification

- **APP Security**
  - iOS / Android / Windows / ……
- **Communication Protocol Security**
  - WiFi / Bluetooth / ZigBee / MQTT / WebSocket ……
- **Hardware Security Protection**
  - Debug Port / Flash Chip Encryption / System integrity Verify ……
- **Cloud Security**
  - Server / Web / Data / ……

IoT Automated Vulnerability Audit

- **Source Code Scan**
- **Firmware Analysis**
- **Wireless Protocol Security Audit**



IoT Security SDK

- Communication traffic encryption
- Firmware verification
- Exploit Mitigation

Bug Bounty Program

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

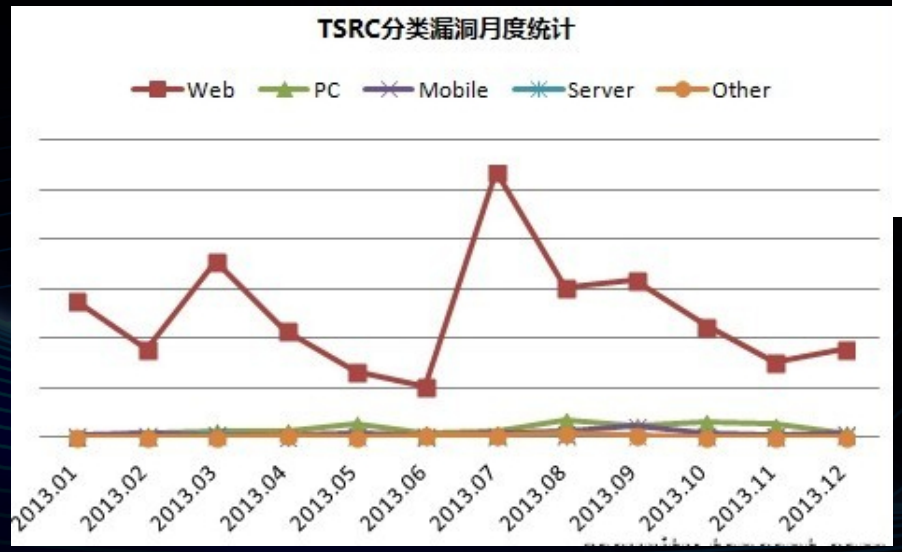
[TPSA15-20] 关于“威胁情报奖励计划（试行）”启动的安全公告

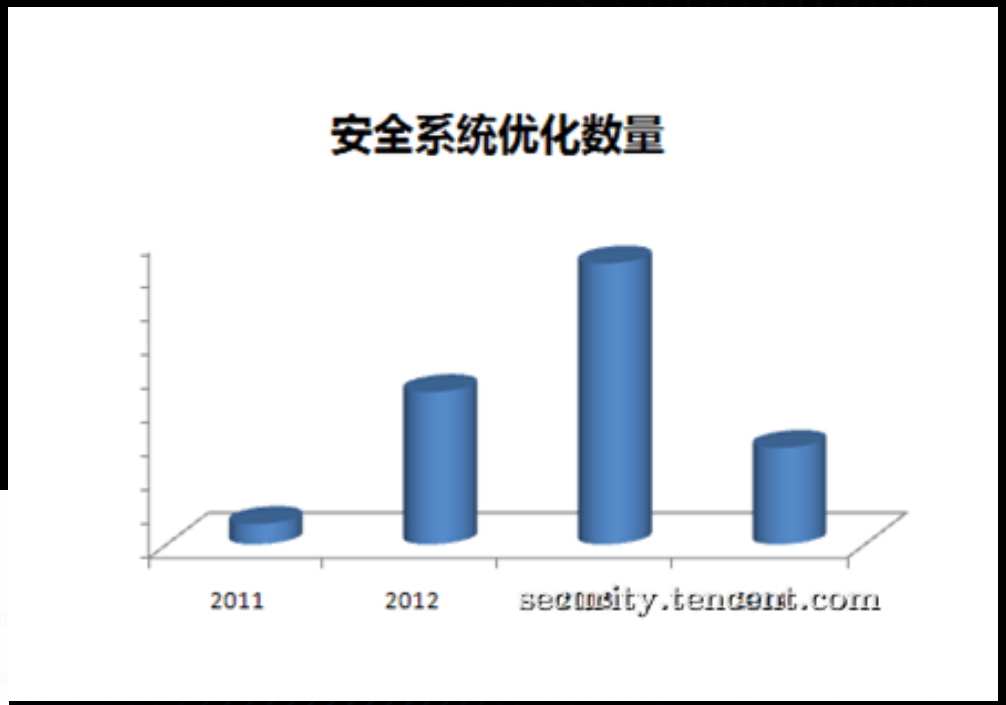
公告编号：TPSA15-20　公告来源：TSRC　发布日期：2015-10-15　分享

腾讯安全应急响应中心（简称TSRC）于2012年5月启动了，在三年多的不断试错和改进中，得到了业界广大安全专家的帮助和支持，大大提高了腾讯产品和业务的安全级别。但我们仍然觉得做得还不够，我们希望再来点改进。

自即日起，TSRC原有的“**安全漏洞奖励计划**”正式升级为“**威胁情报奖励计划**”——TSRC除原有的收集腾讯安全漏洞外，还收集与腾讯相关的任何安全威胁情报，一经确认，即按照威胁情报评分危害级别给予奖励。

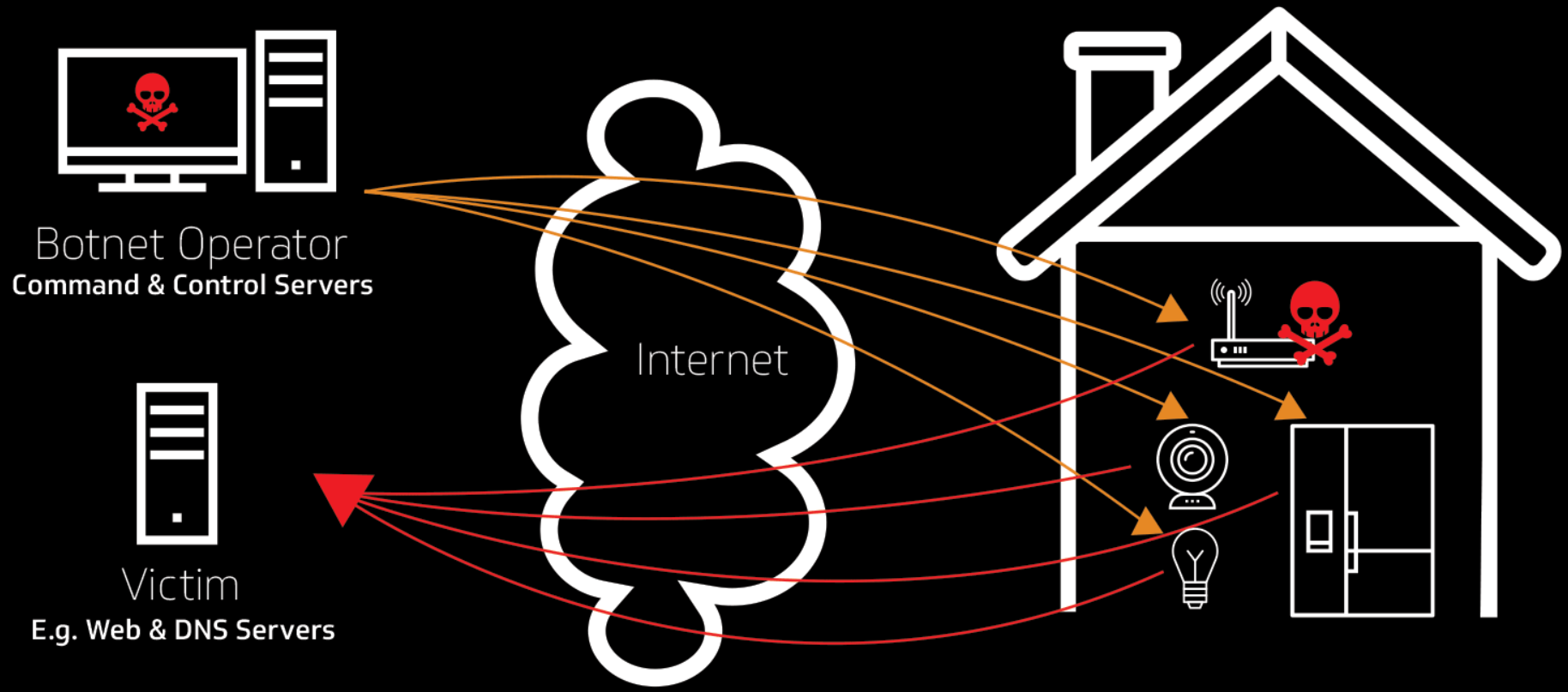
【适用条件】





Summary

Future IoT Security Battlefield：Cyber Attack



1Tb DDoS Attack By 152000 Hacked IoT Devices

Future IoT Security Battlefield：User Privacy & Safety

THANKS

Tencent Bug Bounty Program
https://en.security.tencent.com

Tencent Security Platform Dpt.

BLADE Tencent Blade

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