



百度一下

# XCON2022

## AIoT安全体系建设实践

夏良钊 百度AIoT安全研究负责人



# CONTENT 目录

A | AIoT安全的现状和趋势

B | 百度AIoT安全体系框架

C | 纵深防御方案建设

D | 行业影响力建设

文档仅限技术交流，切勿商用，违者必究

- ❑ 负责百度AIoT业务安全保障和体系建设，业务范围包括小度DuerOS生态、Apollo无人车及AI智能硬件
- ❑ 针对AIoT安全生态广泛开展安全研究，在上游内核模块、蓝牙&Wi-Fi等组件中累计获得300+ CVE，获得谷歌、高通、联发科的多次致谢，团队成员多次受邀在BlackHat上发表演讲
- ❑ 打造业界领先的AIoT+移动安全解决方案，在OTA、入侵防护、应用检测与加固等场景中持续赋能外部客户



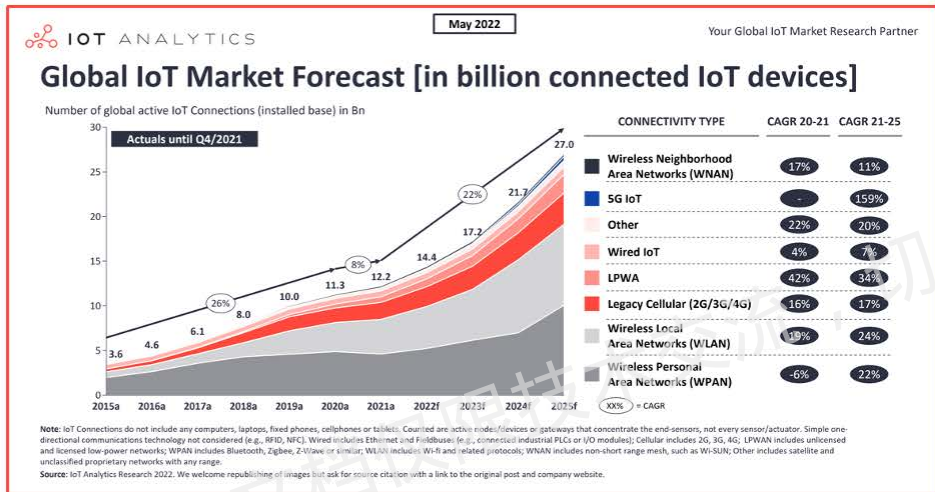
# PART A



## AIoT安全的现状和趋势

IoT安全态势

文档仅限技术交流，违者必究



■ 2022, 预计达到144亿, 增长率18%

■ 2025, 预计达到270亿, 增长率22%

## A

## IoT安全态势

## IoT Malware Destination



■ IoT恶意软件增长700% --- Zscaler

## A timeline of notable IoT attacks in 2021

AUG

Dark targets devices with firmware built by Arcadyan only two days after the vulnerabilities are published.

SEP

Meris malware uses compromised MikroTik devices to launch the largest ever DDoS attack on Russian internet and index.

DEC

Dark variant targets TP-Link routers.

FEB

The emergence of Dark, a Mirai variant, targeting multiple routers, firewalls, and IoT devices.

Dark targets devices with SDK by Realtek only two days after the vulnerabilities are published.

Mozi malware evolves to achieve persistence on network gateways manufactured by Netgear, Huawei, and ZTE.

Moobot, another Mirai variant, starts targeting Hikvision cameras using a vulnerability published in September.

Mirai botnet starts to use the Log4j vulnerability. Researchers witness Log4j used to create Muhstik and Mirai botnets that attacked Linux devices.

■ 每年十亿级 IoT 设备被攻击 --- Securingsam Network



# A

## 小度DuerOS助手

通过自然语言对话交互方式，可实现在不同场景下信息查询、生活服务出行路况、影音娱乐等数百项功能服务

### 中国最大的对话式人工智能操作系统

66亿

单月语音交互次数

2亿+台

IoT智能家居设备连接

### 繁荣的合作伙伴生态及开发者社区

500+家

知名企业合作伙伴

5.2万名

开发者

35万+间

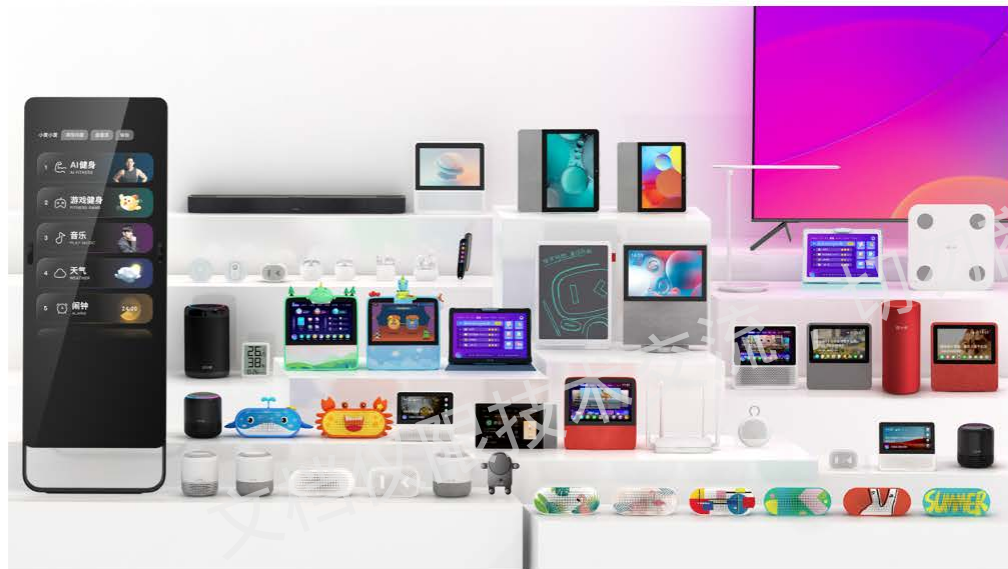
合作酒店客房

5200+项

技能支持

# A

## 种类繁多的设备



■ 不同的安全要求

■ 不同的攻击面

■ 不同的策略

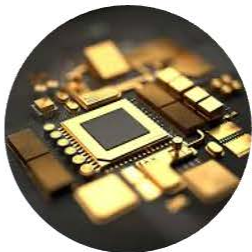






### 业务安全

账号体系攻击  
恶意调试刷机  
远程静默监控



### 供应链安全

内核驱动漏洞  
射频通讯模组漏洞  
三方技能/SDK漏洞



### 数据安全

不安全的传输  
关键数据未加密  
缺乏权限控制与审计



### AI安全

人脸识别绕过  
声纹脸纹突破  
海豚音攻击



### 监管及舆论

法律监管  
各大破解比赛  
负面新闻及报道



敏感的设备

上游供应链冗长



敏感的用户

时刻关心个人隐私



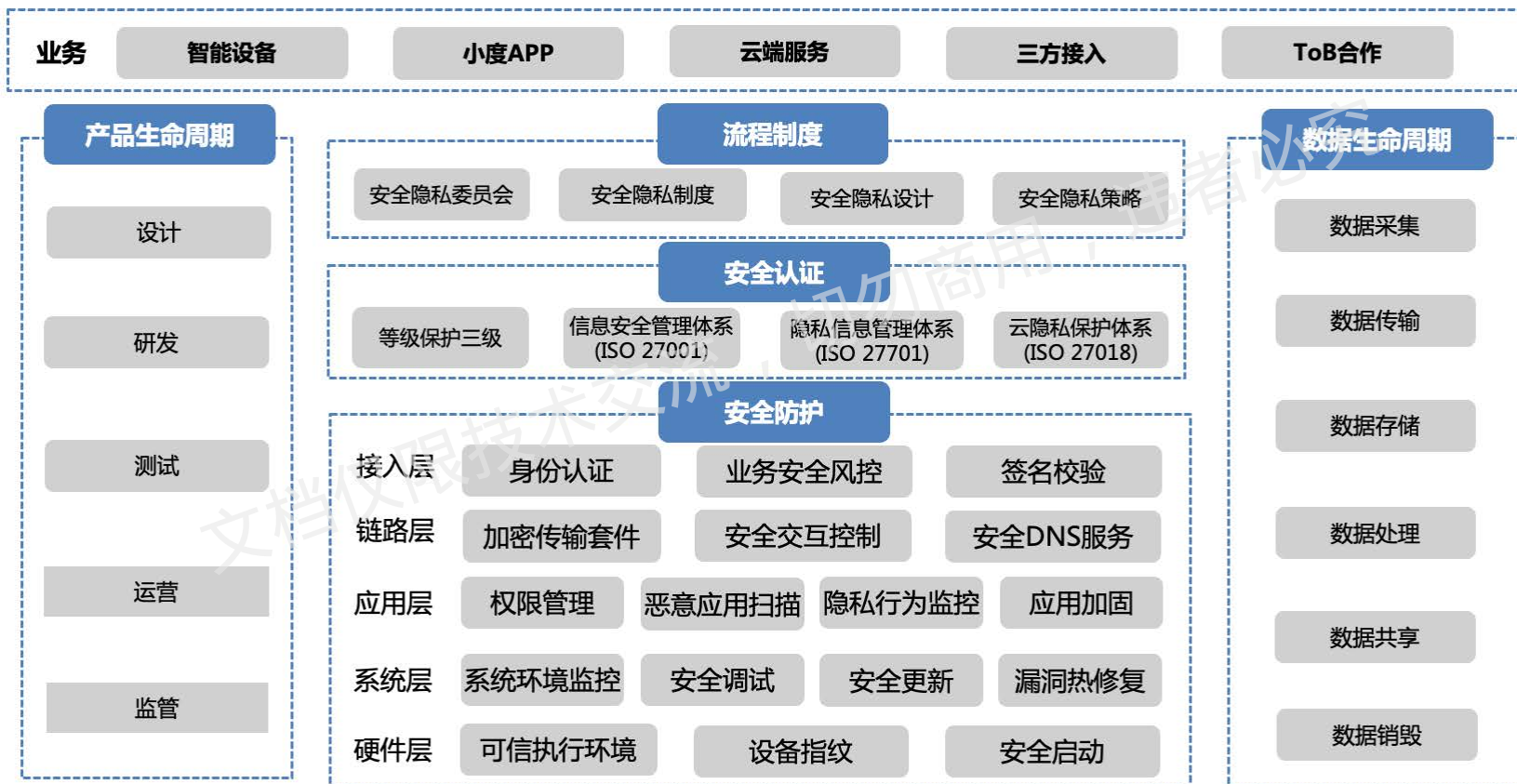
敏感的业务

处理大量个人数据

# PART B

## 百度 AIoT 安全体系框架

全生命周期主动安全体系



## 设计阶段

产品安全基线

安全编码规范

业务安全培训

安全方案评审

## 研发阶段

安全基础组件

SDK安全准入

三方应用集成

代码安全扫描

## 测试阶段

应用安全扫描

固件安全扫描

数据安全扫描

设备渗透测试

## 运营阶段

安全应急响应

安全补丁管理

系统安全防护

业务安全风险

## 监管阶段

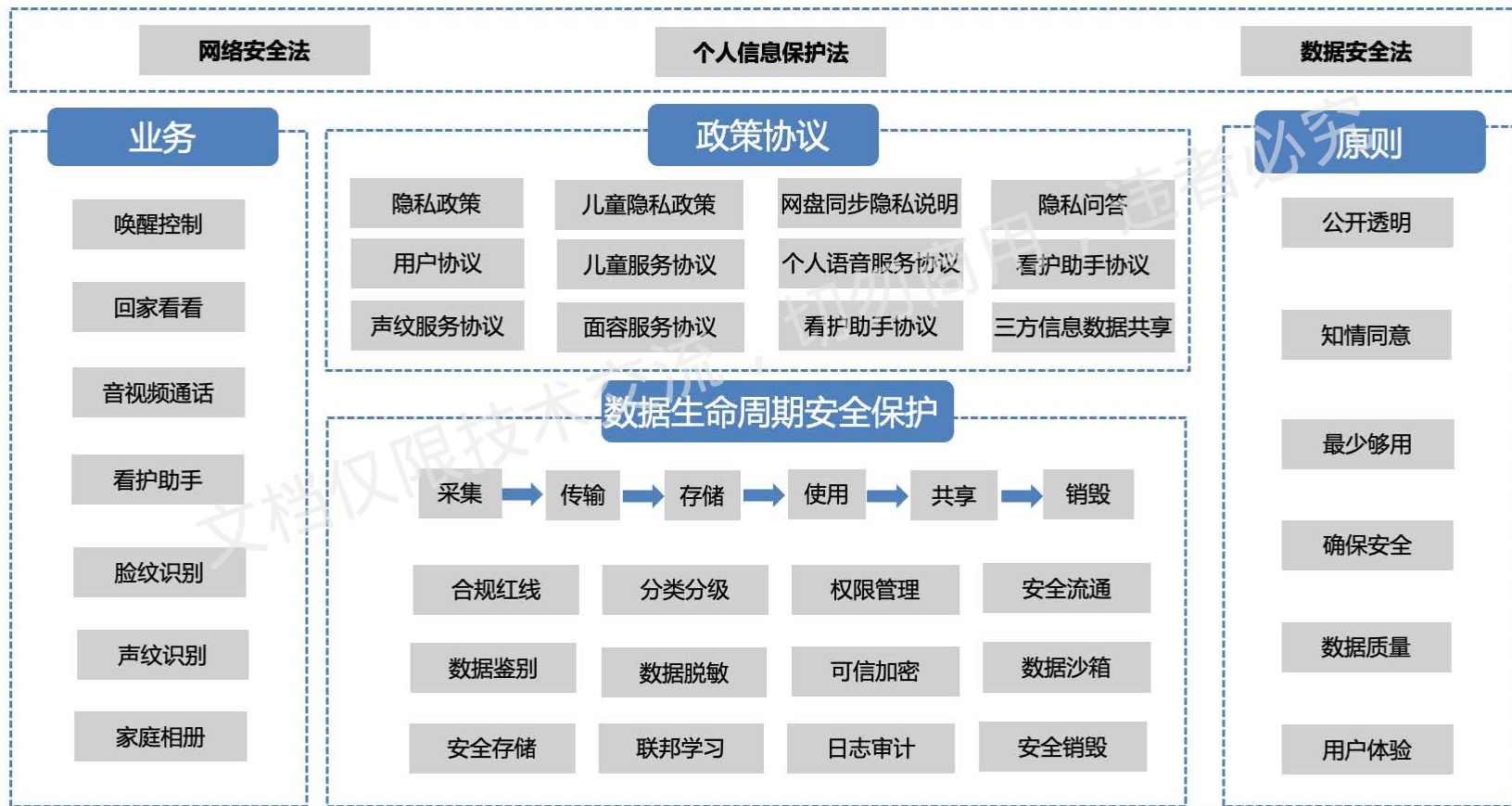
产品口径库

安全标准参与

安全隐私认证

企业安全白皮书







# PART C



## 纵深防御方案建设

安全合规技术

文档仅限技术交流，切勿商用，违者必究



# 供应链漏洞管理与运营

## 发现

审计 + 逆向 + Fuzzing

应用

三方应用

三方SDK

三方技能

系统



硬件



Qualcomm

UNISOC

Rockchip

@mlogic

## 管理

流程 + 方案

三方应用准入规范

三方SDK准入规范

供应链安全扫描（应用+SDK+技能+固件）

补丁筛选

系统补丁计划

补丁验证

芯片补丁计划

补丁维护

## 运营

热修复

+

OTA

热补丁制作



热补丁下发

官方补丁包



官方补丁下发





## 供应链漏洞管理与运营

**300+**

供应链漏洞

**50+**

热修复补丁

**500+**

官方补丁合入

**2000w+**

热修复能力覆盖

文档仅限技术交流，切勿商用，违者必究





# 设备风险感知与响应



总览设备问题-设备维度

sn	存在恶意app (病毒app)	root	magisk
9505	否	是	否
9505	否	是	否
9505	否	是	否
9505	否	是	是
9505	否	是	否
9505	否	是	否
9504	否	是	否
9504	否	是	否

总览app维度-app访问隐私权限行为

隐私权限调用应用名称	隐私权限调用总次数	隐私权限调用总设备量	摄像头调用次数	摄像头调用设备量	麦克风调用次数	麦克风调用设备量	地理位置调用次数	地理位置调用设备量
com.1	2	2	2	2	0	0	0	
com.1	2	1	0	0	0	0	2	
com.1	2	1	0	0	0	0	2	
com.1	0	0	0	0	0	0	0	
com.1	0	0	0	0	0	0	0	

200+  
异常应用

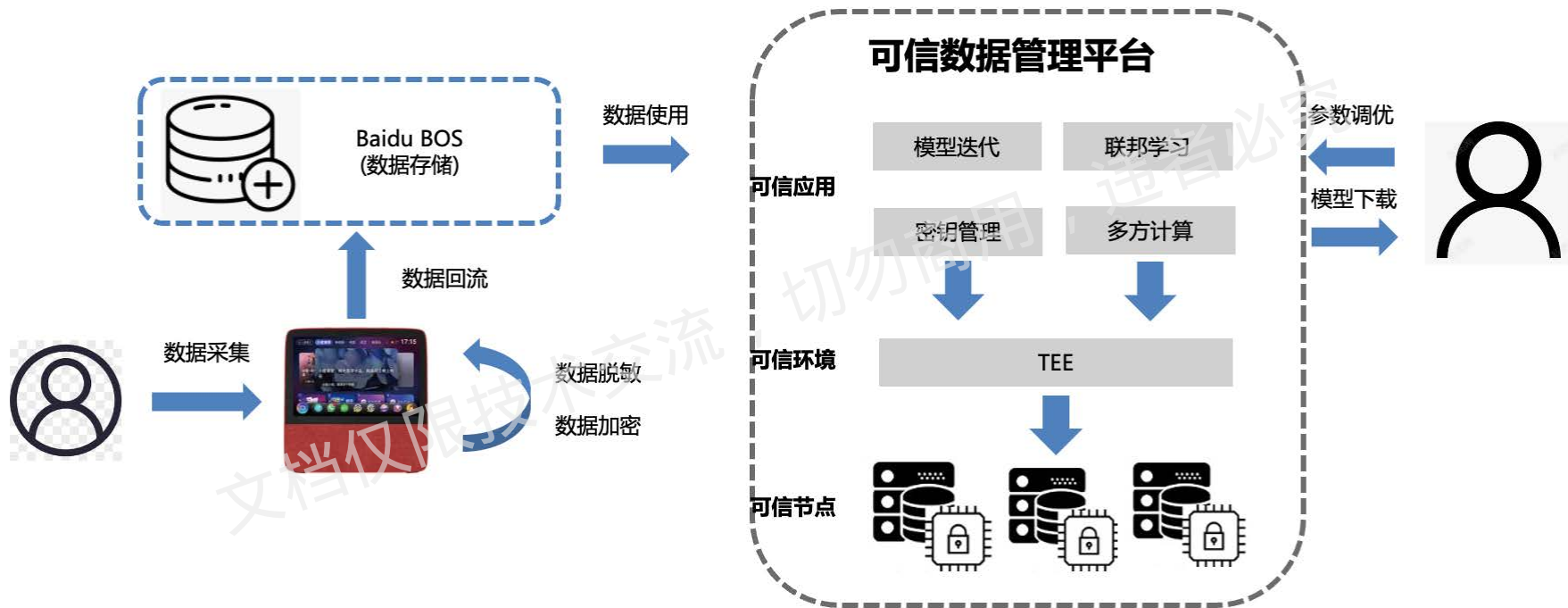
160+  
异常设备

100w+  
能力覆盖





# 基于可信环境的数据保护





# PART D



## 行业影响力建设

共建行业安全生态





# 漏洞挖掘

## February

Researchers	CVEs
Lewei Qu(曲乐炜) and Dong xiang Ke(柯懂湘) of Baidu AIoT Security Team	CVE-2021-39616,CVE-2021-39635,CVE-2021-39658

## January

Researchers	CVEs
Lewei Qu(曲乐炜) of Baidu AIoT Security Team	CVE-2021-1049

### MediaTek components

These vulnerabilities affect MediaTek components and further details are available directly from MediaTek. The severity assessment of these issues is provided directly by MediaTek.

CVE	References	Severity	Component
CVE-2022-20024	A-2019705228 M-ALPS06219064*	High	System service
CVE-2022-20025	A-209700749 M-ALPS06126832*	High	Bluetooth
CVE-2022-20026	A-209705229 M-ALPS06126827*	High	Bluetooth
CVE-2022-20027	A-209702508 M-ALPS06126826*	High	Bluetooth
CVE-2022-20028	A-209702509 M-ALPS06198663*	High	Bluetooth

## MIUI 某系统服务存在指针重复释放漏洞

内部标识	CVE编号	CVSS分数	发布时间
MiSVD-2022-134	<u>CVE-2020-14123</u>	4.2 中危	2022-04-22

### 漏洞描述及影响

MIUI 某系统服务存在指针重复释放漏洞。在函数调用时，内存指针拷贝给两个功能模块，攻击者受影响模块崩溃，影响正常功能，如果成功利用该漏洞可造成权限提升。

## CVE-2020-11836 MTK AEE module is in debug mode

2021-02-04

OPPO security team sincerely appreciates these security researchers' efforts to help us improve our security. We will continue to work with more security researchers to apply for CVE IDs.

### Acknowledgements

Vulnerabilities Submitted by: Qu Lewei, Baidu AIoT security team

Vulnerability submission time: November, 2020

**black hat**  
EUROPE 2021

REGISTER NOW

NOVEMBER 8-11, 2021  
EXCEL LONDON / UNITED KINGDOM

ATTEND \* TRAININGS BRIEFINGS \* ARSENAL \* FEATURES \* SCHEDULE BUSINESS HALL \* SPONSORS \* PROPOSALS \*

All times are Greenwich Mean Time (UTC +0)

**BadMesher: New Attack Surfaces of Wi-Fi Mesh Network**

Lewis Qi | Security Researcher, Baidu  
Dongxiang Ke | Security Researcher, Baidu  
Yu Zhang | Security Researcher, Baidu  
Xing Wang | Security Researcher, Baidu  
Date: Thursday, November 11 | 10:25am-11:00am (Virtual)  
Format: 40-Minute Briefings  
Tracks: Network Security, Hardware / Embedded

With the increasing number of internet access devices, the application and research of the Internet of Things (IoT) have become popular day by day. As an IoT infrastructure, Wi-Fi networks play a significant role in providing quick and easy communication services for IoT devices. Furthermore, Wi-Fi Mesh has advantages in self-organization, self-management, and self-healing as a new networking technology, improving flexibility and reliability compared to the traditional network.

In this session, we will start with the keyMesh designed and certified by Wi-Fi Alliance. Then, we will pay attention to the security issues in the implementation of Wi-Fi Mesh. In detail, we will focus on the attack surfaces in network build and network control and share attack ideas for different Wi-Fi Mesh roles.

**black hat**  
ASIA 2022

REGISTER NOW

MAY 10-13, 2022  
MARINA BAY SANDS / SINGAPORE + VIRTUAL

ATTEND \* TRAININGS BRIEFINGS \* ARSENAL \* FEATURES \* SCHEDULE BUSINESS HALL \* SPONSORS \* PROPOSALS \*

All times are Singapore Time (GMT+UTC+8)

**Unix Domain Socket: A Hidden Door Leading to Privilege Escalation in the Android Ecosystem**

Dongxiang Ke | Security Researcher, Baidu Security  
Lewei Qi | Security Researcher, Baidu Security  
Han Yan | Security Researcher, Baidu Security  
Format: 40-Minute Briefings  
Tracks: Mobile, Cloud & Platform Security

Unix domain socket (UDS) is an important inter-process communication mechanism in the Android ecosystem. It can transfer IPC data safely with its access control, logical, functional, third-party applications cannot directly communicate with UDS services because of the restriction of SELinux. This, however, requires the security of UDS services. Worse still, they may introduce additional vulnerabilities into UDS from implementation, implementation misconfiguration. As a result, UDS becomes a hidden attack surface that can cause privilege escalation in the Android ecosystem.

To investigate the security of the attack surface, we investigated the UDS services in multiple Android devices and summarized the implementation scenarios of UDS in the Android ecosystem. Based on the risk analysis for each scenario, we found several vulnerabilities in the UDS services of different vendors and obtained 3 CVEs. An attacker can exploit these vulnerabilities to obtain root or system privileges.

In this presentation, we will first introduce the common scenarios of UDS by real-world examples. Then, we will explain how vendor scenarios fit together through UDS in some complex functional modules, such as the GPS. Next, we will demonstrate typical vulnerabilities in these scenarios and our exploits that can bypass all access restrictions to illustrate the security problems. Finally, we will introduce an automated analysis method for UDS services and provide certain security suggestions.

**black hat**  
USA 2022

REGISTER NOW

AUGUST 6-11, 2022  
MGM MAYS BAY / LAS VEGAS + VIRTUAL

ATTEND \* TRAININGS BRIEFINGS \* ARSENAL \* FEATURES \* SCHEDULE BUSINESS HALL \* SPONSORS \* PROPOSALS \*

All times are Pacific Time (GMT+UTC-7)

**BrokenMesh: New Attack Surfaces of Bluetooth Mesh**

Han Yan | Security Researcher, Baidu, Inc.  
Lewei Qi | Security Researcher, Baidu, Inc.  
Dongxiang Ke | Security Researcher, Baidu, Inc.  
Date: Wednesday, August 10 | 3:20pm-4:00pm (Jasmine Level 3)  
Format: 40-Minute Briefings  
Tracks: Network Security, Hardware / Embedded

Bluetooth Mesh is a mesh networking standard based on Bluetooth Low Energy. It was made public by Bluetooth Special Interest Group (Bluetooth SIG) in 2017. Bluetooth Mesh enables many-to-many device communications, and is optimized for creating large-scale device networks. It is typically suited for smart home, industrial deployments and other scenarios. At present, Bluetooth Mesh specifications have been widely supported by major chip manufacturers. But in general, security of its implementation has not been paid enough attention.

In this topic, we divided into the Bluetooth Mesh protocol, divided the mesh process into two key stages: network build and network control. We focused on the security of implementation in these two stages. Based on the protocol analysis, an automatic fuzzing tool "BLE Mesh Fuzzer" is proposed. It can cover both network build and network control stages. We evaluated our tools on 8 well-known vendors and open source projects. BLE Mesh Fuzzer has found 17 memory corruption vulnerabilities and obtained 9 CVEs. Some of the vulnerabilities can cause remote code execution without user interaction. Even, they can cause the destruction of the whole mesh network and affect tens of millions of IoT devices. Also, we studied the security of protocol wrapper application. We found 19 vulnerabilities in a well-known vendor and obtained 10 CVEs. The vulnerabilities can lead to serious consequences such as privilege escalation.

In this talk, we will first introduce the background of Bluetooth Mesh. Then, we analyze the network build and network control protocols, illustrate the attack surfaces in their implementation and wrapper application. Next, we will share the design of BLE Mesh Fuzzer. And finally, we explain the causes of vulnerabilities through several real cases, and put forward our safety recommendations.

**black hat**  
ASIA 2022

REGISTER NOW

MAY 10-13, 2022  
MARINA BAY SANDS / SINGAPORE + VIRTUAL

ATTEND \* TRAININGS BRIEFINGS \* ARSENAL \* FEATURES \* SCHEDULE BUSINESS HALL \* SPONSORS \* PROPOSALS \*

All times are Singapore Time (GMT+UTC+8)

**Explosion: The Hidden Mines in the Android ION Driver**

Le Wu | Security Researcher, Baidu  
Xiao Li | Security Researcher, Baidu  
Luo Jia | Security Researcher, Baidu  
Date: Friday, May 13 | 3:20pm-4:00pm (Virtual & Simpor Junior Ballroom 4B10)  
Format: 40-Minute Briefings  
Tracks: Mobile, Exploit Development

The ION driver is an essential component introduced by Google into the Android kernel to facilitate allocations of device-accessible memory. It has been widely used by vendors for almost 10 years. In addition, almost all untrusted apps can access the ION driver, so any issue in ION could be exploited directly. However, only in recent years, a few ION-related vulnerabilities have been published. Due to this circumstance, it convinces us that there may be more hidden mines buried deep in the ION.

So far, we've found over 40 ION-related vulnerabilities, affecting millions of Android devices! We name the series of vulnerabilities Explosion! Different from the vulnerabilities in other Android drivers, Explosion is found to be a problem of the entire Android ecosystem due to the specialty of ION. First, ION as a base driver can be used to develop vendors' own drivers. Therefore, any flaw in ION could lead to vulnerabilities in vendors' drivers. Second, Google as upstream not only provides the design and implementation of ION's own APIs, but also provides interfaces for vendors to allow their customization to ION. Based on this, vendors could be introduced in the customization part due to poorly documented APIs from Google, misuse of ION APIs by vendors, and so on. What's more, some vendors even customize ION's core APIs, resulting in known issues of ION not properly fixed due to code conflicts.

## ■ 国家标准

《智能人体温度检测与识别系统技术要求和测试评价方法》  
《物联网 参考体系结构》修订 GB/T 33474-2016  
《汽车整车信息安全技术要求》  
《汽车数字证书应用规范》  
《汽车软件升级通用技术要求》  
《信息安全技术 关键信息基础设施安全测评要求》  
《信息安全技术 公钥基础设施 PKI 系统安全技术要求》  
《信息安全技术 边缘计算安全技术要求》  
《信息安全技术 汽车采集数据的安全要求》

## ■ 行业标准

《智能终端设备 数据安全技术要求》  
《智能显示设备适老化技术要求评测方法》  
《智能终端设备个人信息安全技术规范》  
《移动智能终端个人信息分类分级》  
《云游戏 X86 终端技术要求和测试方法》

## ■ 团体标准

《智能终端设备 数据安全技术要求》  
《智能显示设备适老化技术要求评测方法》  
《智能终端设备个人信息安全技术规范》  
《移动智能终端个人信息分类分级》  
《云游戏 X86 终端技术要求和测试方法》



## 智能终端安全生态联盟（Open AI System Security Alliance）

国内首个致力于提升智能终端生态安全的联合组织，由信通院、华为、百度联合发起成立，由安全厂商、终端厂商、高校科研机构、政府机构共同组成。联盟宗旨是希望引导一个开放、共享、合作、共建的安全生态链，促进智能终端厂商与安全厂商之间建立良性的互动与合作，共同推进智能终端安全生态的建设。





THANK YOU