看雪 2017 安全开发者峰会

Kanxue 2017 Security Developer Summit

2000-2017

开启IoT设备的上帝模式

Jingle@腾讯反病毒实验室

#whoami

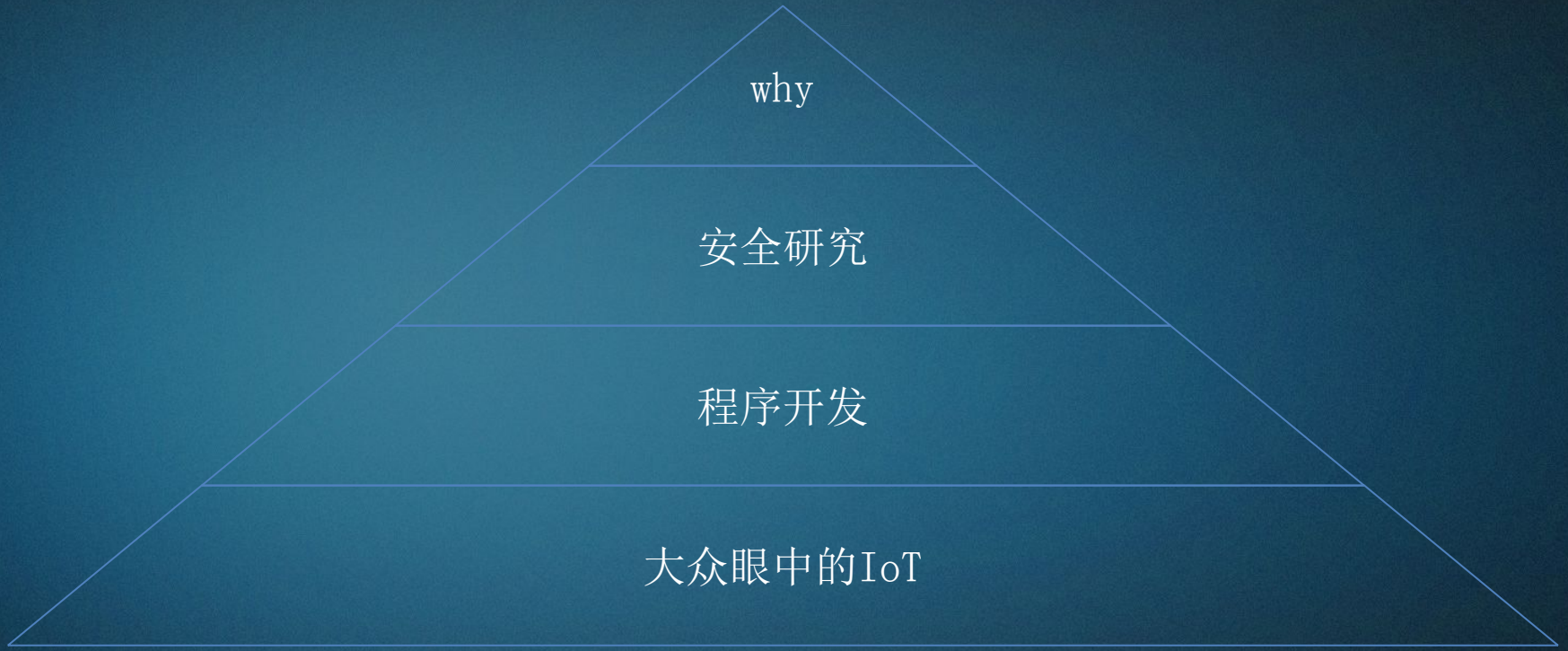
Jingle

- 腾讯反病毒实验室
- 腾讯哈勃分析系统开源版(HaboMalHunter)
- 恶意代码分析
- IoT安全研究
- 涉及的漏洞已经全部上报CNNVD

内容提要

- 背景介绍
- Root方法
- 安全威胁
- 缓解措施

背景介绍



Root 方法

攻击建模

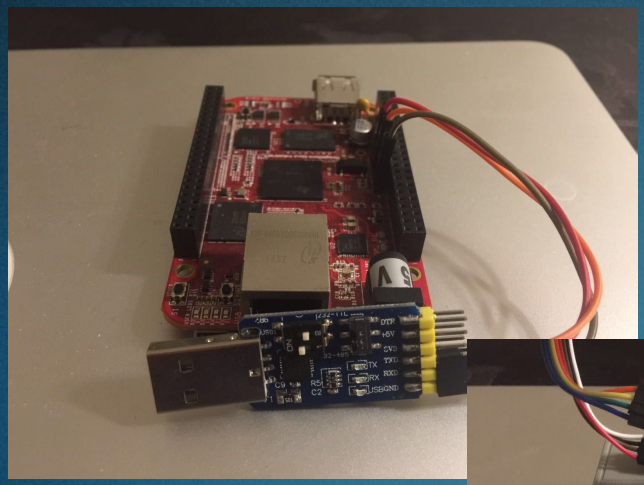
应用层

系统层

网络层

硬件层

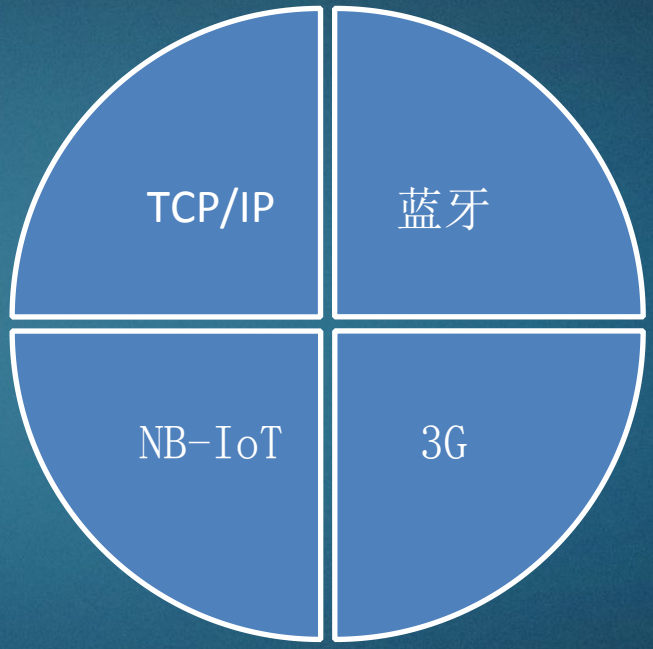
硬件层



串口调试

FLASH 编程器

网络层



系统层

CNNVD-201708-1472

Uboot校验固件

CRC32

校验值来自固件头

伪造固件

CNNVD-201708-1472

Blank

应用层

Blank

应用层

Blank

安全威胁

威胁种类

- 传统威胁
- DDoS
- 内网穿透
- 挖矿

安全威胁

Blank

总结

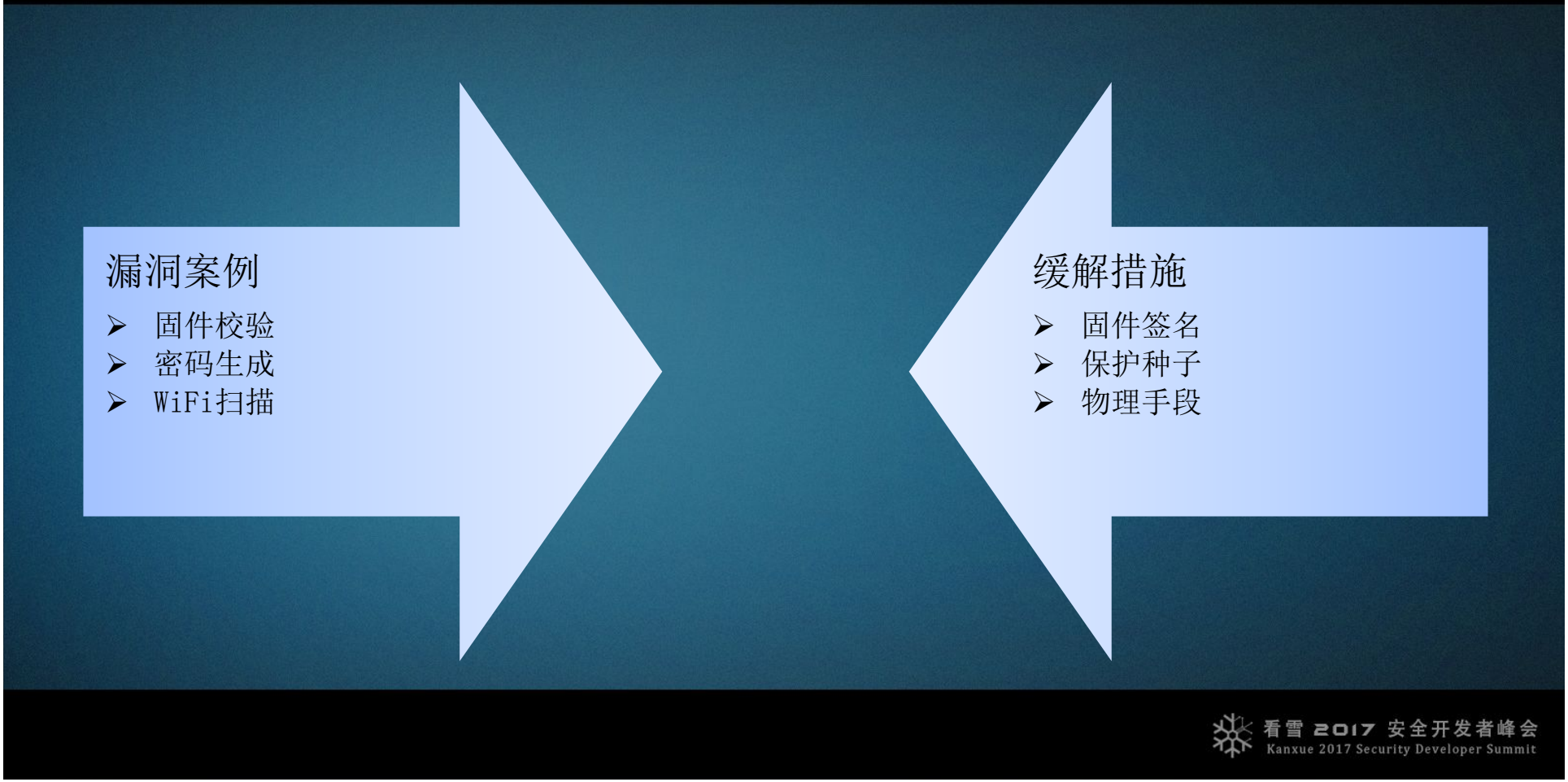
IoT安全发展会符合一种自然规律

攻强守弱

相互焦灼

守强攻弱

缓解措施



参考资料

1. https://www.armis.com/blueborne/
2. https://wikidevi.com/wiki/Ralink_RT5350
3. "Basic Secure Boot for OMAP-L138 C6748," http://processors.wiki.ti.com/index.php/Basic_Secure_Boot_for_OMAP-L138_C6748
4. http://www.cnnvd.org.cn/web/xxk/ldxqById.tag?CNNVD=CNNVD-201708-1472
5. https://github.com/tencent/habomalhunter

Thank you very much