**感兴趣的**

**1. 钉枪：突破ARM特权隔离**

多处理器设备 使用低权限处理器调试高权限处理器，：

介绍https://compass.cs.wayne.edu/nailgun/

论文地址：[已下载]

https://www.computer.org/csdl/proceedings-article/sp/2019/666000b156/19skgcwSgsE

github项目地址：

https://github.com/ningzhenyu/nailgun

**2. 畅游EL3：终极提权之旅**

ppt地址：[已下载]

https://speakerdeck.com/hhj4ck/el3-tour-get-the-ultimate-privilege-of-android-phone

**3. 危险的文件快传应用：亿级用户量的隐私泄露漏洞的发现、利用和防御**

华为

**听的还可以的**

**4.全球卫星搜救系统的安全性分析**

**听到了一点的**

**5.模糊测试蜂窝网络(如果允许的话)**

**6.DramaQueen - Drammer和Rampage攻击之旅**

Drammer

Rampage <https://rampageattack.com/>

researcher‘s blog https://vvdveen.com/

**7.灰烬中燃烧：基带的童话故事**

**没有怎么听懂的**

**8.无处安放的shellcode**

http://blogs.360.cn/post/Binder\_Kernel\_Vul\_CH.html

**9.新一代移动网络和基带的崛起**

https://speakerdeck.com/marcograss/2pac-2furious-envisioning-an-ios-compromise-in-2019

**10.PAC研究**

ppt地址：[已下载]

https://github.com/bazad/presentations/blob/master/MOSEC-2019-A-study-in-PAC.pdf

**11.举例XNU中的引用计数问题**

天府杯2018远程越狱项目中使用的内核提权漏洞(CVE-2019-6225)

<http://blogs.360.cn/post/IPC%20Voucher%20UaF%20Remote%20Jailbreak%20Stage%202.html>

**12.一些JSC的故事**

ppt地址：[已下载]