ISC 2019 第七届互联网安全大会

5G安全-让子弹再飞一会

黄琳

360集团高级技术经理

黄琳

360集团 高级技术经理

ISC 第七届互联网安全大会

360互联网安全中心

5G安全 – 让子弹再飞一会

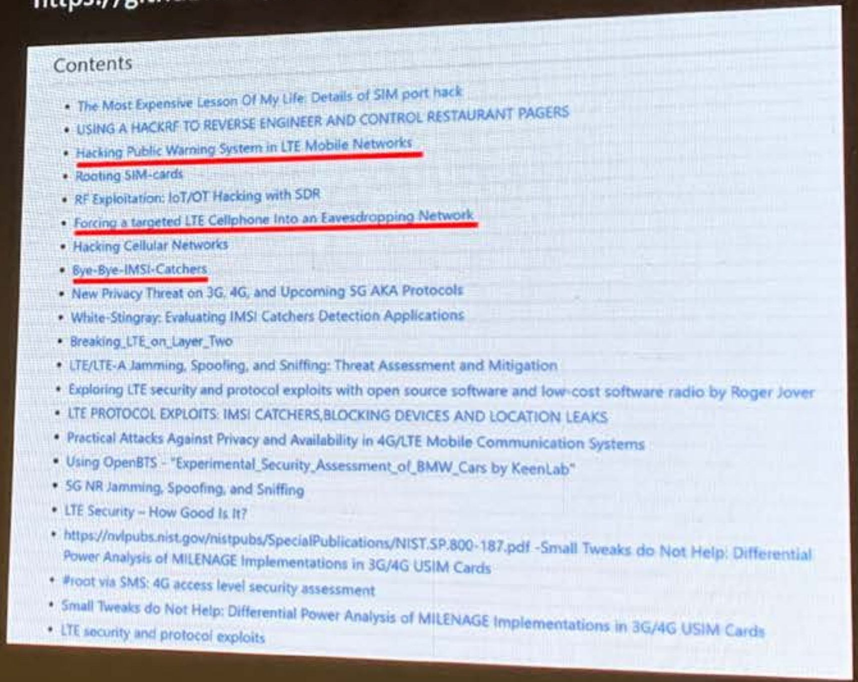
360安全研究院 黄琳

基础通信设施的安全问题

通信网络相关的安全问题是一个长期存在的话题，并不是因为5G新引入的。

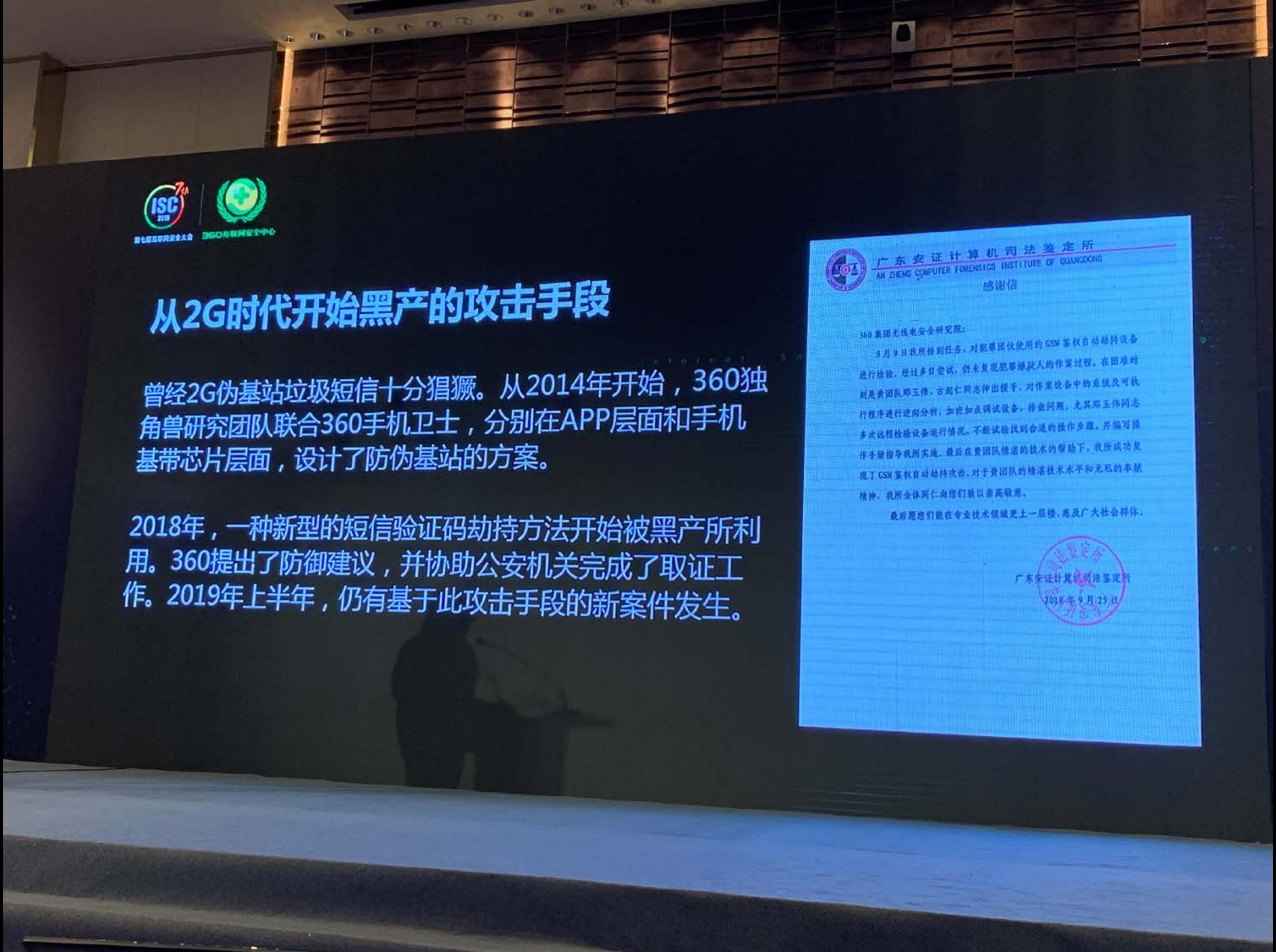
关键基础设施连接无线网络的风险，过去就存在，现在也存在，将来依然存在

https://github.com/W00t3k/Awesome-Cellular-Hacking



Contents

- The Most Expensive Lesson Of My Life: Details of SIM port hack
- USING A HACKRF TO REVERSE ENGINEER AND CONTROL RESTAURANT PAGERS
- Hacking Public Warning System in LTE Mobile Networks
- Rooting SIM-cards
- RF Exploitation: IoT/OT Hacking with SDR
- Forcing a targeted LTE Cellphone Into an Eavesdropping Network
- Hacking Cellular Networks
- Bye-Bye-IMSI-Catchers
- New Privacy Threat on 3G, 4G, and Upcoming 5G AKA Protocols
- White-Stingray: Evaluating IMSI Catchers Detection Applications
- Breaking_LTE_on_Layer_Two
- LTE/LTE-A Jamming, Spoofing, and Sniffing: Threat Assessment and Mitigation
- Exploring LTE security and protocol exploits with open source software and low-cost software radio by Roger Jover
- LTE PROTOCOL EXPLOITS: IMSI CATCHERS,BLOCKING DEVICES AND LOCATION LEAKS
- Practical Attacks Against Privacy and Availability in 4G/LTE Mobile Communication Systems
- Using OpenBTS - "Experimental_Security_Assessment_of_BMW_Cars by KeenLab"
- 5G NR Jamming, Spoofing, and Sniffing
- LTE Security – How Good Is It?
- https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-187.pdf -Small Tweaks do Not Help: Differential Power Analysis of MILENAGE Implementations in 3G/4G USIM Cards
- #root via SMS: 4G access level security assessment
- Small Tweaks do Not Help: Differential Power Analysis of MILENAGE Implementations in 3G/4G USIM Cards
- LTE security and protocol exploits



从2G时代开始黑产的攻击手段

曾经2G伪基站垃圾短信十分猖獗。从2014年开始，360独角兽研究团队联合360手机卫士，分别在APP层面和手机基带芯片层面，设计了防伪基站的方案。

2018年，一种新型的短信验证码劫持方法开始被黑产所利用。360提出了防御建议，并协助公安机关完成了取证工作。2019年上半年，仍有基于此攻击手段的新案件发生。

广东安证计算机司法鉴定所
AN ZHENG COMPUTER FORENSICS INSTITUTE OF GUANGDONG

感谢信

360集团无线电安全研究院：

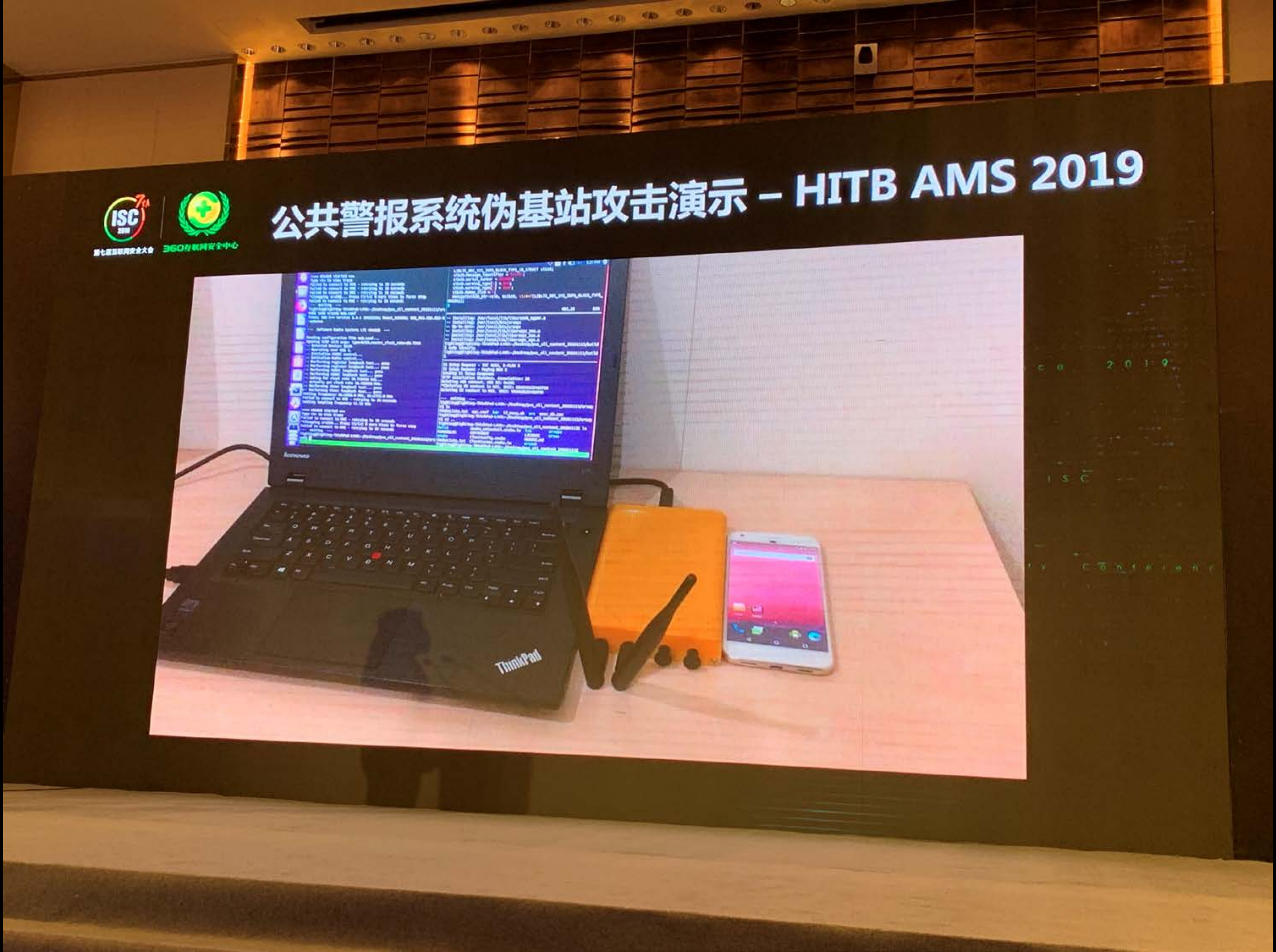
9月9日我所接到任务，对犯罪团伙使用的GSM鉴权自动劫持设备进行检验，经过多日尝试，仍未复现犯罪嫌疑人的作案过程。在困难时刻是贵团队郑玉伟、古起仁同志伸出援手，对作案设备中的系统及可执行程序进行逆向分析，加班加点调试设备，排查问题，尤其郑玉伟同志多次远程检验设备运行情况，不断试验找到合适的操作步骤，并编写操作手册指导我所实施。最后在贵团队精湛的技术的帮助下，我所成功复现了GSM鉴权自动劫持攻击。对于贵团队的精湛技术水平和无私的奉献精神，我所全体同仁向您们致以崇高敬意。

最后愿您们能在专业技术领域更上一层楼，惠及广大社会群体。

广东安证计算机司法鉴定所
2018年9月25日

4G网络的安全风险举例 – 公共警报系统

尽管4G网络存在少量
安全风险，但利用难度大
4G网络的黑产攻击鲜有发现
一种潜在的安全风险是
公共警报系统

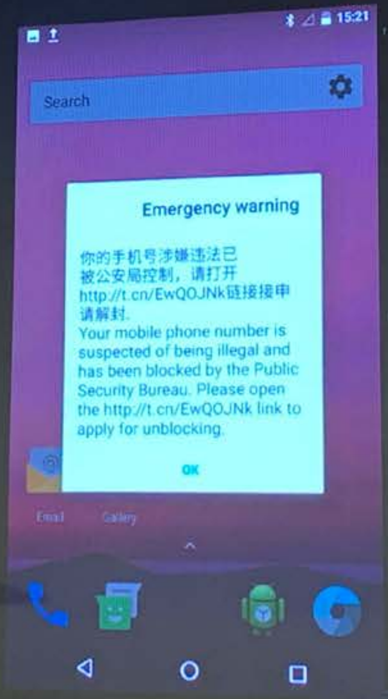


公共警报系统伪基站攻击演示 – HITB AMS 2019

公共警报系统伪基站攻击 – 用于定向攻击

由于警报短信作为一种特殊的短信，可以直接在手机应用层展现。所以是一种可以穿透多层协议，从空口直达操作系统层面的特殊通道

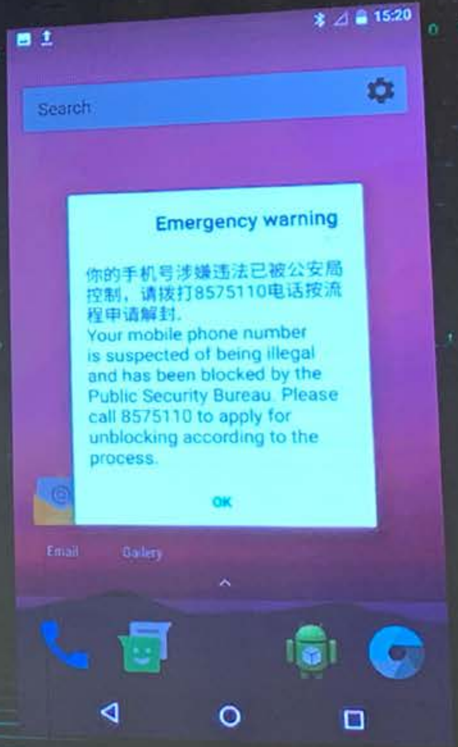
若某一款手机在OS层面有警报短信的某种漏洞，那么该攻击手段有可能被用于高级目标的定向攻击



Emergency warning

你的手机号涉嫌违法已被公安局控制，请打开http://t.cn/EwQOJNk链接接申请解封.
Your mobile phone number is suspected of being illegal and has been blocked by the Public Security Bureau. Please open the http://t.cn/EwQOJNk link to apply for unblocking.

OK



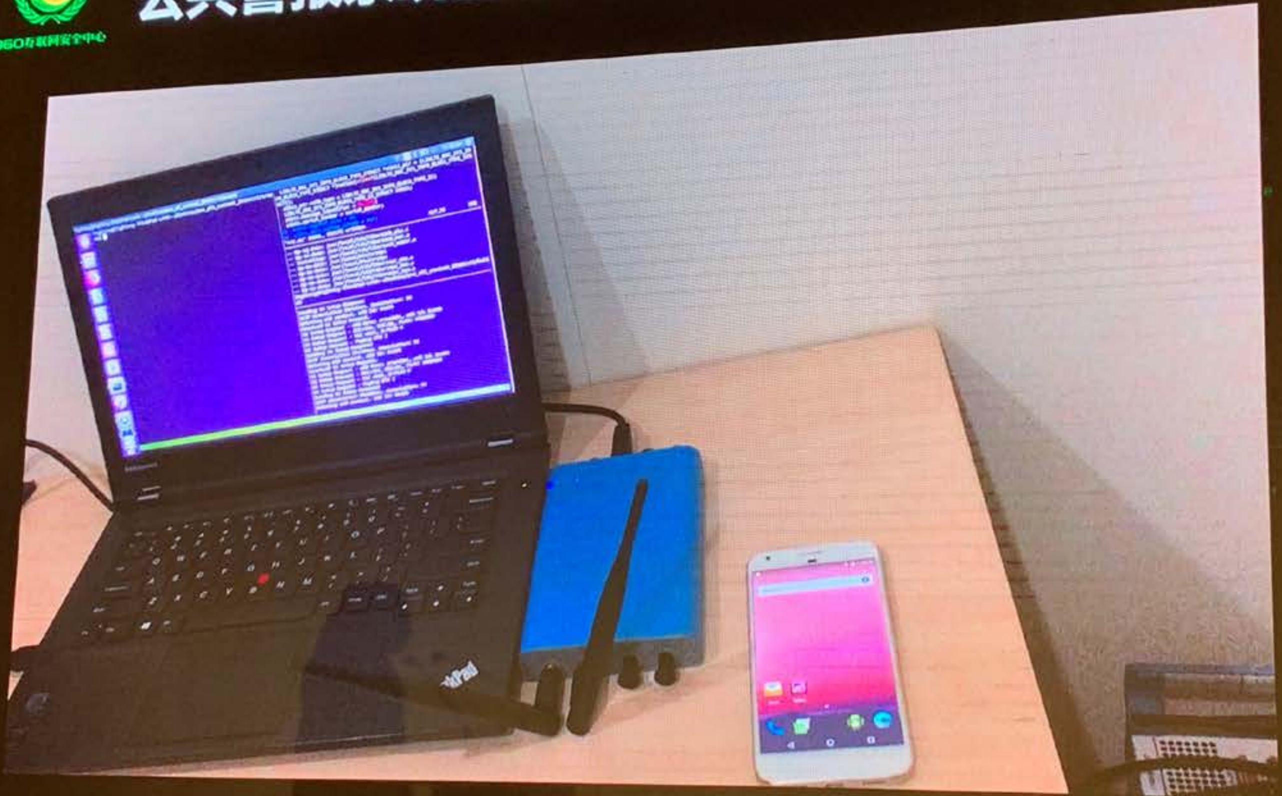
Emergency warning

你的手机号涉嫌违法已被公安局控制，请拨打8575110电话按流程申请解封.
Your mobile phone number is suspected of being illegal and has been blocked by the Public Security Bureau. Please call 8575110 to apply for unblocking according to the process.

OK

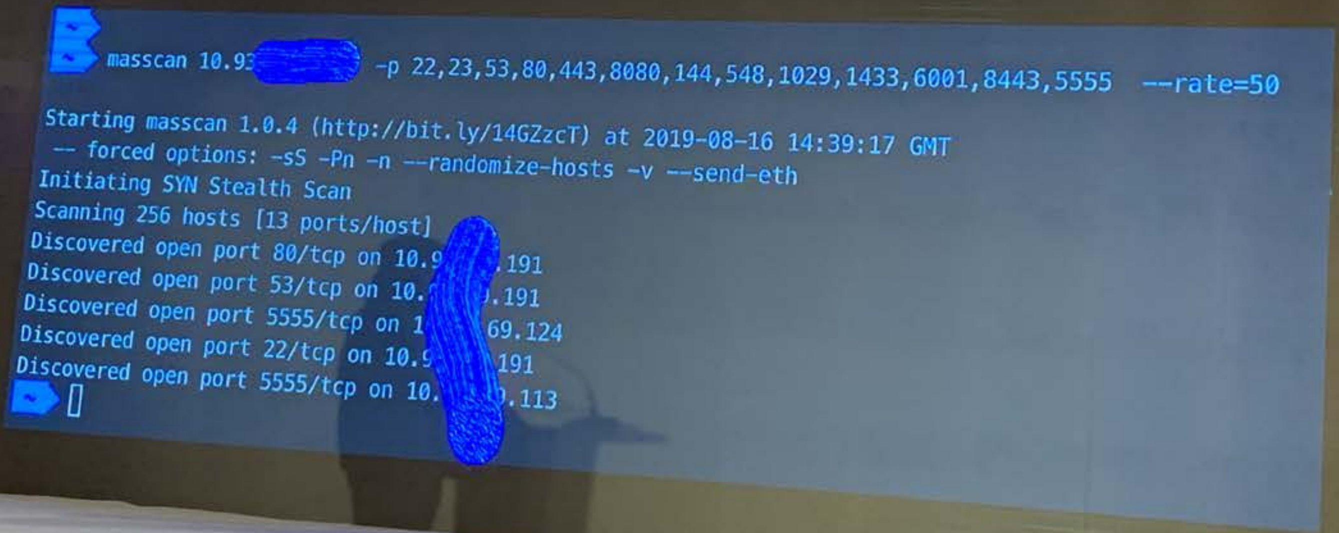
ISC 2019 第七届互联网安全大会 | 360互联网安全中心

公共警报系统伪基站攻击演示 – HITB AMS 2019



4G内网中的安全风险正在逐渐暴露

越来越多的物联网设备通过4G模块连接到互联网，有些开放端口在4G内网中暴露出来



```
~ masscan 10.9[redacted] -p 22,23,53,80,443,8080,144,548,1029,1433,6001,8443,5555  --rate=50

Starting masscan 1.0.4 (http://bit.ly/14GZzcT) at 2019-08-16 14:39:17 GMT
 -- forced options: -sS -Pn -n --randomize-hosts -v --send-eth
Initiating SYN Stealth Scan
Scanning 256 hosts [13 ports/host]
Discovered open port 80/tcp on 10.9[redacted].191
Discovered open port 53/tcp on 10.[redacted].191
Discovered open port 5555/tcp on 1[redacted]69.124
Discovered open port 22/tcp on 10.9[redacted]191
Discovered open port 5555/tcp on 10.[redacted].113
~ ▯
```

ISC 7th 2019 第七届互联网安全大会 | 360互联网安全中心

5G的安全特性主要体现在核心网5GC

从协议的角度，5G相比4G更安全

5G有NSA和SA两种组网方式

5G的安全特性主要体现在5G核心网

但目前首先落地的是NSA模式

5G有超宽带、广连接和低时延三种场景

目前只有eMBB

当前业务模式没有暴露新的攻击面

5G与垂直行业的结合

网络切片
MEC边缘计算
Vertical LAN 和自建专网
车联网，从V2X到V2X的演进

5G对垂直行业开放的接口，网络设备的部署方式等，都还需要等待5G行业应用最终落地

青岛港 基于5G连接的自动岸桥吊车 2019年1月

泛5G的物联网安全

如果考虑广义的5G安全，物联网安全不只是通信管道安全，还涉及到整个系统的信息安全。

当大量的工业设备连接到网络，还需要考虑主机安全、应用软件安全、数据安全等等。

5G+产业互联网 – 功能先行

360为产业互联网的安全保驾护航

期待4G和5G的覆盖更完善
期待5G+边缘计算得到广泛应用
期待工业专网频段得到政策支持
期待传统企业、运营商、互联网企业找到共赢的商业模式

工厂所处的位置常常得不到4G网络的良好覆盖

小鹅助理

谢谢！

扫码添加小鹅助理，与数万科技圈人士

分享重量级活动PPT、干货培训课程、高端会议免费门票