



# 5G 移动通信网络安全

· 彭 晋 ·

中国移动通信研究院安全技术研究所

2019年04月

## 1 万物互联的应用场景





--安全风险可能影响国家和社会多个领域

-  智能家居
-  车联网
-  智慧城市
-  工业物联网





## 2 多样化的终端形态与接入技术

--终端形态与多接入提出新的安全要求

-  无人值守的物联网终端
-  车载终端
-  云端机器人
-  多种接入技术并存

## 3 新技术的驱动

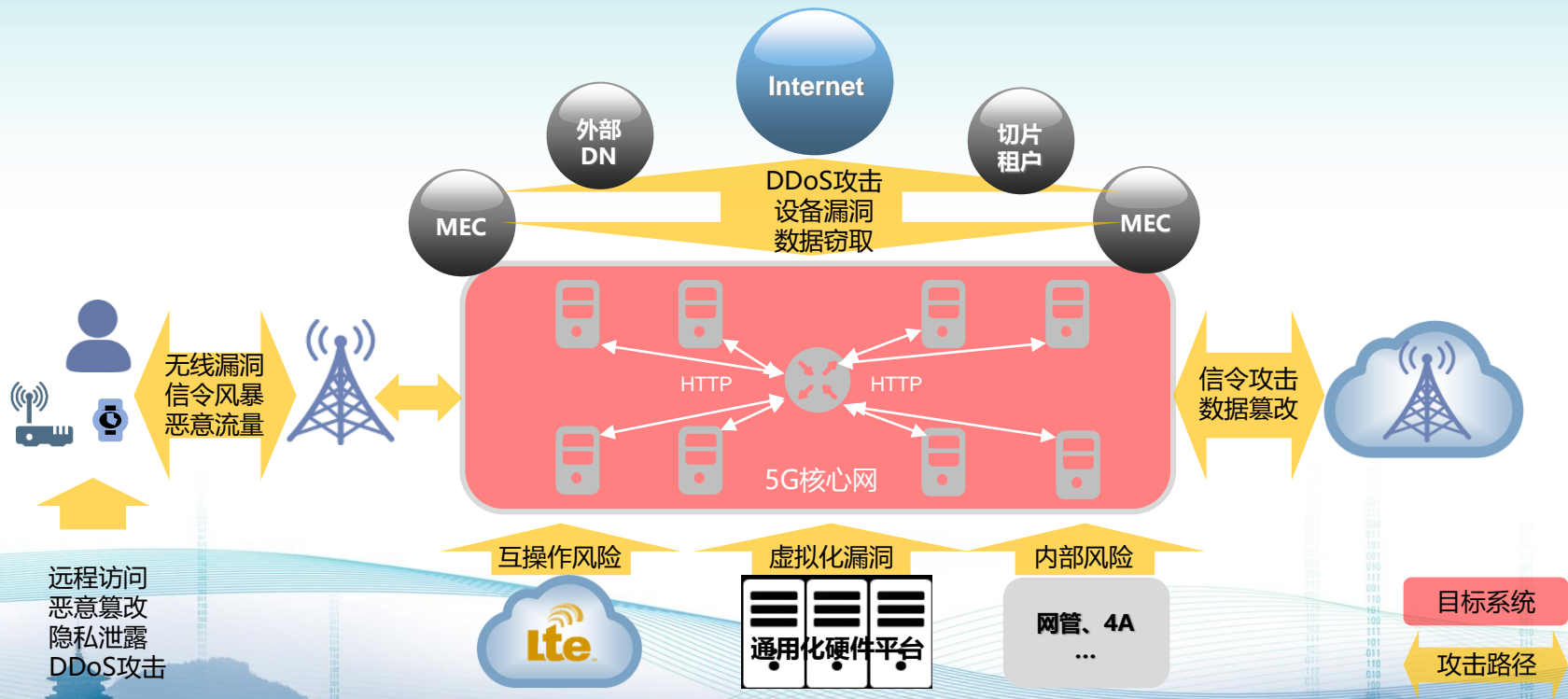
--IT技术引入移动网络，产生新问题

-  移动边缘计算技术
-  网络切片技术

# 组网结构视角下的5G安全



2019 西湖论剑·网络安全大会  
WEST LAKE CYBERSECURITY CONFERENCE



远程访问  
恶意篡改  
隐私泄露  
DDoS攻击

无线漏洞  
信令风暴  
恶意流量

DDoS攻击  
设备漏洞  
数据窃取

信令攻击  
数据篡改

互操作风险

虚拟化漏洞

内部风险

通用化硬件平台

网管、4A  
...

目标系统

攻击路径

# 攻防能力视角下的5G安全



2019 西湖论剑·网络安全大会  
WEST LAKE CYBERSECURITY CONFERENCE

计算  
能力



信任  
关系



攻击  
手段

对已有算法的破解  
能力在提升

开放互联降低了整  
体信任程度

网络日益复杂带来  
新的漏洞



# 5G: 更安全的安全算法



2019 西湖论剑·网络安全大会  
WEST LAKE CYBERSECURITY CONFERENCE



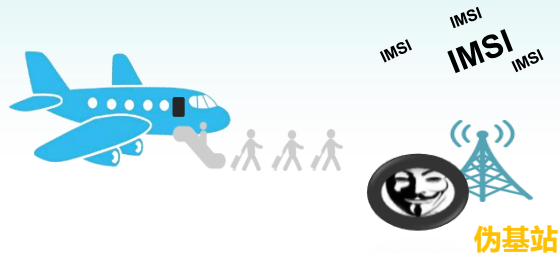
# 5G: 更严密的隐私保护



2019 西湖论剑·网络安全大会  
WEST LAKE CYBERSECURITY CONFERENCE

## 2/3/4G网络

面临空口用户  
隐私被伪基站窃  
取的威胁



## 2/3/4G网络



5G网络  
通过用户身份  
SUPI加密, 提升  
隐私保护



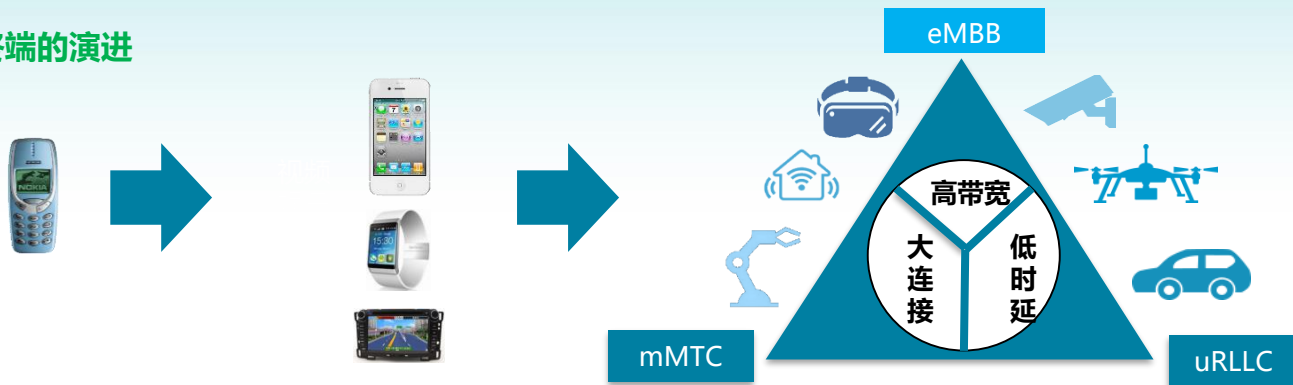
## 5G网络



# 挑战：更复杂的终端安全态势



## ● 5G终端的演进



## ● 智能设备较安全性较低

- 硬件无安全环境（SE或TEE）
- 可远程访问
- 无人值守
- 发展迅速但缺乏安全保障

## ● 新型安全事件频发



*Securityweek: Over 500,000 IoT Devices Vulnerable to Mirai Botnet*



*News.softpedia: Hackers Breach Sauna Camera, leak of nude videos*



*Scmagazine: Hackers use Mirai botnet to slowly mine bitcoins with IoT devices*

## ● 应对措施

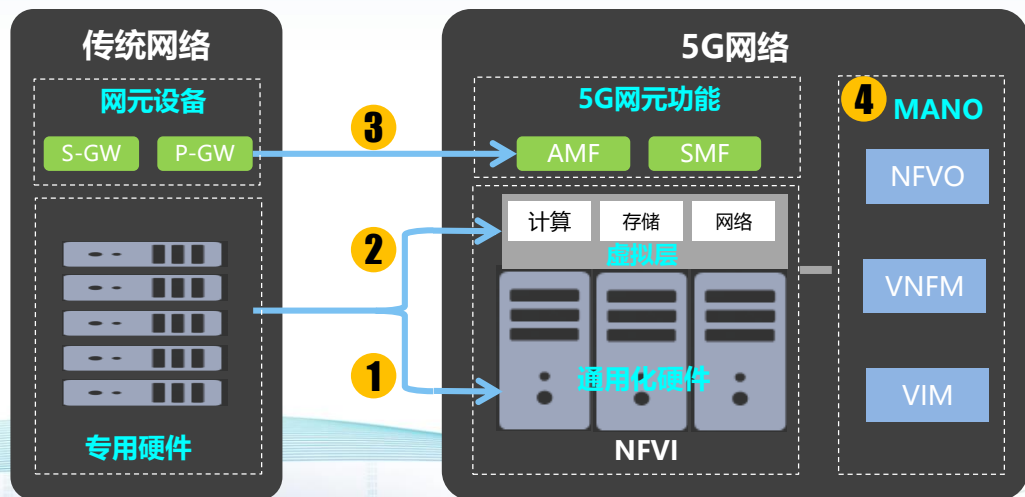
- 事前：标准、评测、认证等
- 事中：预警、监测、分析、升级等
- 事后：召回、反馈、改进等

# 挑战：NFV安全



2019 西湖论剑·网络安全大会  
WEST LAKE CYBERSECURITY CONFERENCE

NFV的云基础设施、新管理编排系统及解耦架构，给5G引入**新**安全挑战



## 引入云计算基础设施带来的安全问题

- 1 通用硬件的安全漏洞更易被利用
- 2 虚拟机/容器逃逸、数据泄露、DoS攻击等
- 3 网元镜像被非法访问、篡改等

## 新增管理编排系统的安全问题

- 4 MANO安全漏洞被利用，接口数据被篡改、API被非法调用等

软硬件解耦、应用与基础软件解耦，形成多组件、多设备、多厂商产业环境，组网结构和管理运维更复杂，对软件及设备质量控制、系统集成及安全运维能力提出了更高要求。

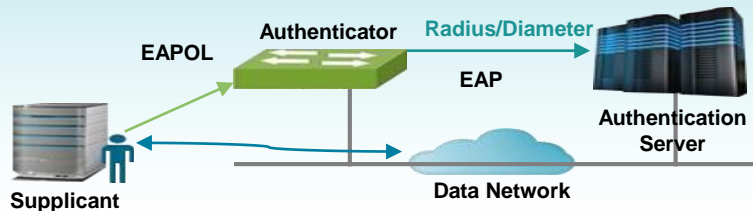


# 挑战：对垂直行业的支撑



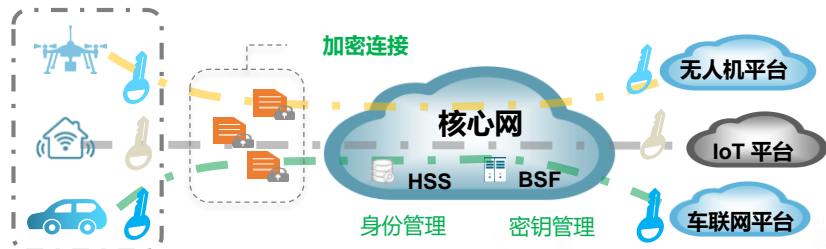
## EAP：统一认证框架

- 支持EAP框架，从而可以适配多种安全凭证和认证方式



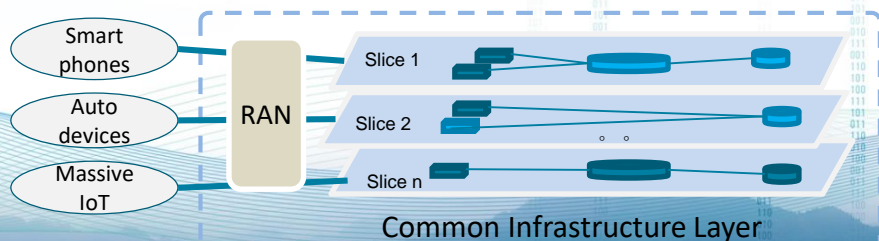
## AKMA：安全认证能力开放

- 基于用户卡和网络的身份认证体系，为第三方提供认证服务和安全通道



## 切片：提供差异化安全能力

- 提供差异化切片安全保证，提供灵活、开放的切片安全能力，满足服务及行业安全需求



# 5G安全标准与5G安全后续方向



2019 西湖论剑·网络安全大会  
WEST LAKE CYBERSECURITY CONFERENCE



5G安全保障

密钥派生安全

量子安全算法应用指南

5G能力开放安全

e2e安全

语音连续性

伪基站预防

5G生态系统信任模型

F1接口安全

V2X安全

uRLLC安全

mlIoT安全

V2X安全

... ..

MEC安全

... ..

网络切片安全

位置服务安全

... ..



- 5G首次提出“通信改变社会”的愿景，强调电信运营商与垂直行业的互信、协作，是产业融合、跨界拓展和生态重构的新机遇



- 5G安全需要考虑计算力的提升、信任模型的变化、网络架构的演进，在技术标准、网络建设等方面都需要整个产业的紧密配合



- 5G生命期还很长，可能出现新的安全风险，给5G产业带来新的机遇与挑战

# 谢谢