

5G网络安全

华为无线网络产品线
无线网络研究部



01

移动网络安全演进

02

5G网络安全标准

03

5G设备安全保障体系

04

总结展望





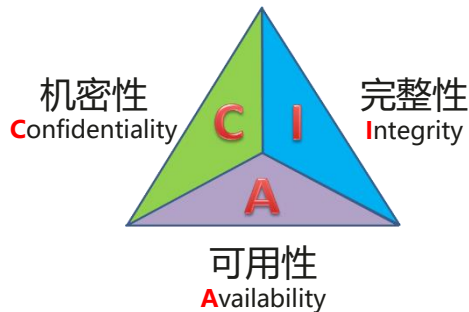
Claude E. Shannon
(April 30, 1916 – February 24, 2001)
图片来自互联网

- Shannon, 1948年创建 “**信息论**”
 - Shannon, Claude (1948). "A Mathematical Theory of Communication" . *Bell System Technical Journal* **27** (3): 379-423
- 1949年, 定义 “**信息论安全性**” 或 “**绝对安全**”
 - Shannon, Claude (1949). "Communication Theory of **Secrecy Systems**". *Bell System Technical Journal* **28** (4): 656–715
 - **Perfect Security** or **Information-theoretic Security**, 意思是说它的安全性完全是以信息论为基础的, 即使攻击者有无限的计算能力时也不能破解
- “这一发现将密码从技术(art)变成科学(science)”, 奠定了现代密码理论的基础

参考书:

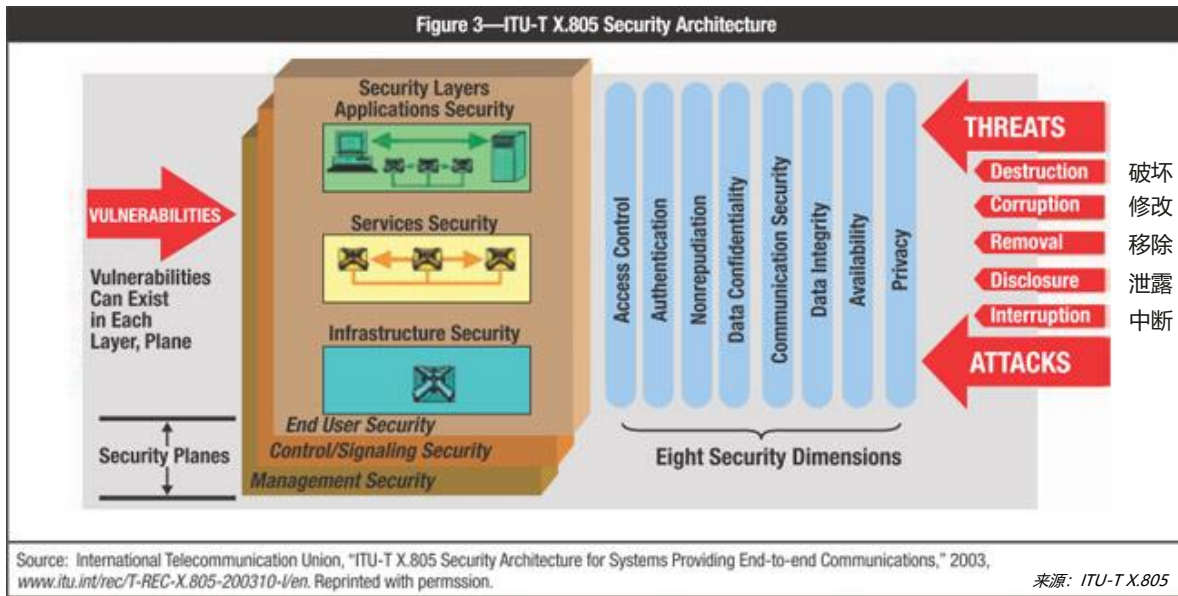
1. 中国移动研究院《5G安全技术标准》,
2. Bruce Schneier《Applied Cryptography 应用密码学》

安全的一般概念



- 真实性 Authenticity
- 可追溯性 Accountability
- 抗抵赖性 Non-repudiation
- ...

End-to-End 通信安全：ITU-T X.805 安全体系架构



安全框架：三面三层、八个安全维度、五类常见威胁与攻击

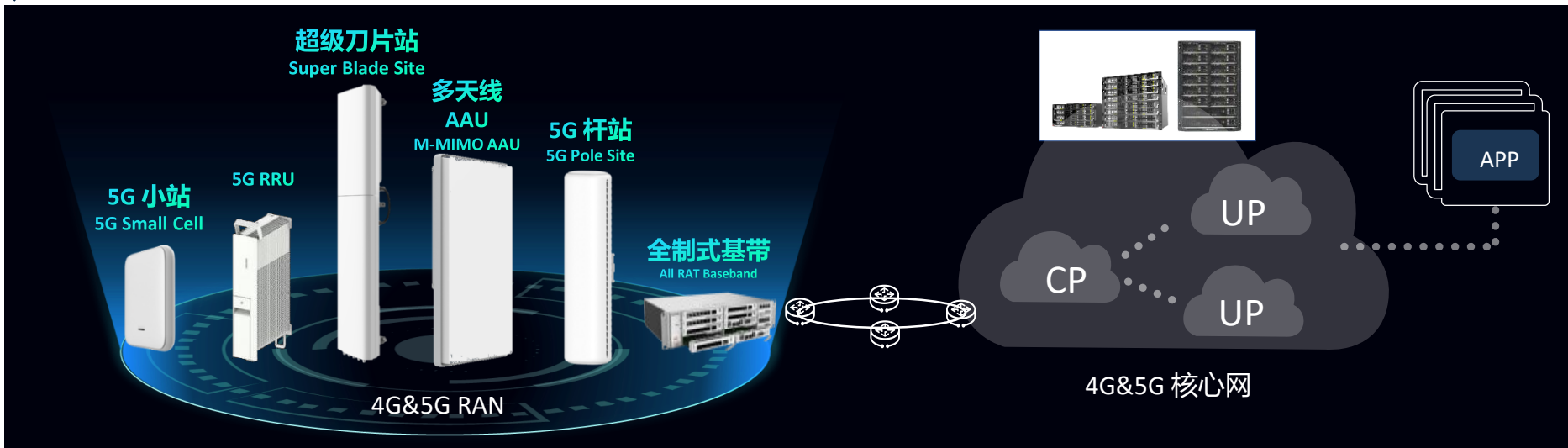
安全防护：定义和计划阶段、执行阶段、运维阶段

安全三同步：同步规划、同步建设、同步运维



移动网络安全演进

5G网络使能百行千业，并持续演进



媒体直播



智能操控



智慧工业



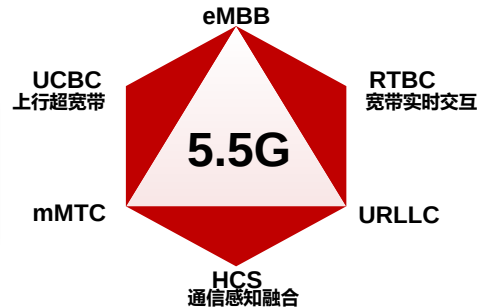
智能电网



智慧医疗

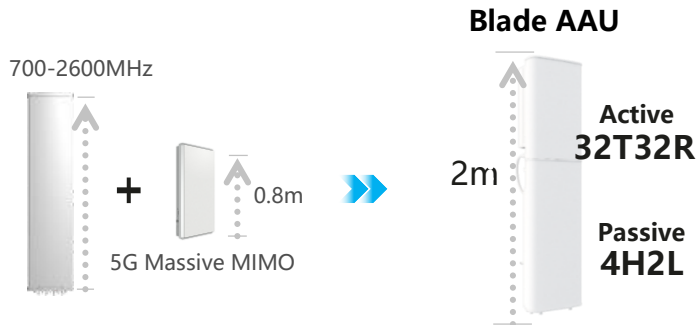


智能驾驶

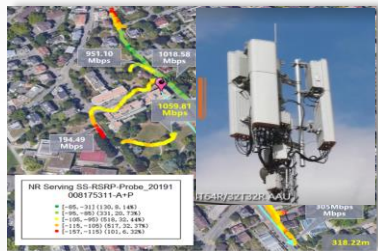


5G基站的部署形态演进：集成化、简约化

AAU和基站天线的集成化



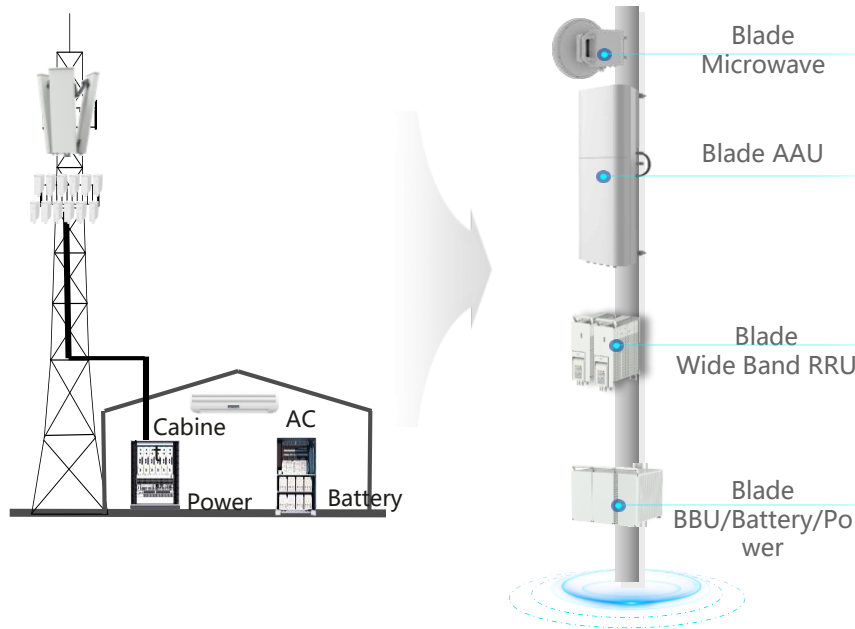
Single-Mast M-MIMO Deployment



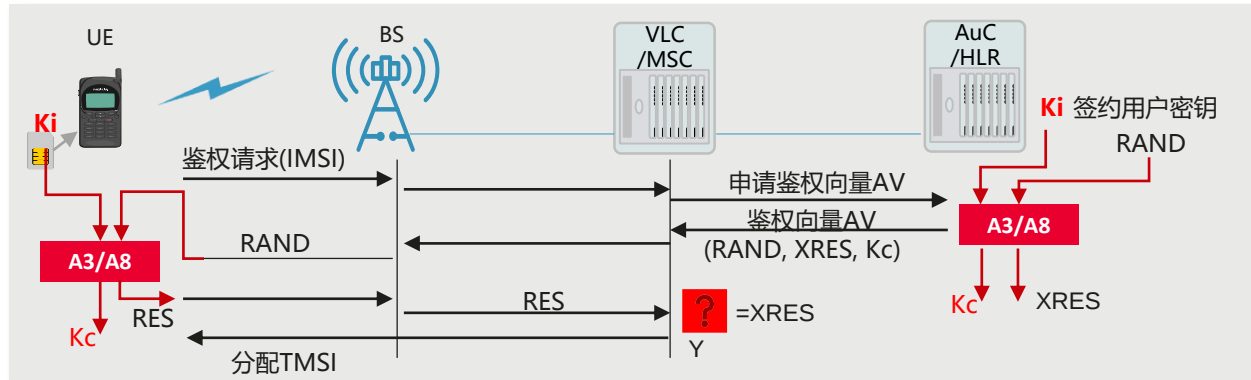
BladeAAU
支持更方便的部署
更低的站点条件要求

Sunrise
@Zurich

Zero Footprint 基站站点的简化



安全需求概述：以2G标准（GSM）为例



安全需求

- 双向认证
- 加密算法增强
- 安全起始与终结点
- 完整性保护
- 隐私保护

用户认证

- UE是谁: IMSI
- 证明UE是自己: 接入认证 (基于Challenge-Response)
- 认证及密钥建立: AKA (Authentication & Key Agreement)
- 单向认证: 仅对UE认证

机密性保护

- USIM和HLR共享 K_i
- A_3/A_8 算法 (COMP128) 生成会话密钥 K_c (64 bit)
- COMP128-1算法初期保密, 但公开后即发现漏洞
- 加密密钥 K_c , 加密算法 $A_5(1/2/3/4)$, $1/2$ 被破解

完整性保护

- 无
- 2G通信以语音为主, 完整性保护效果不明显
- 2G时代重视机密性, 最初未设计完整性保护

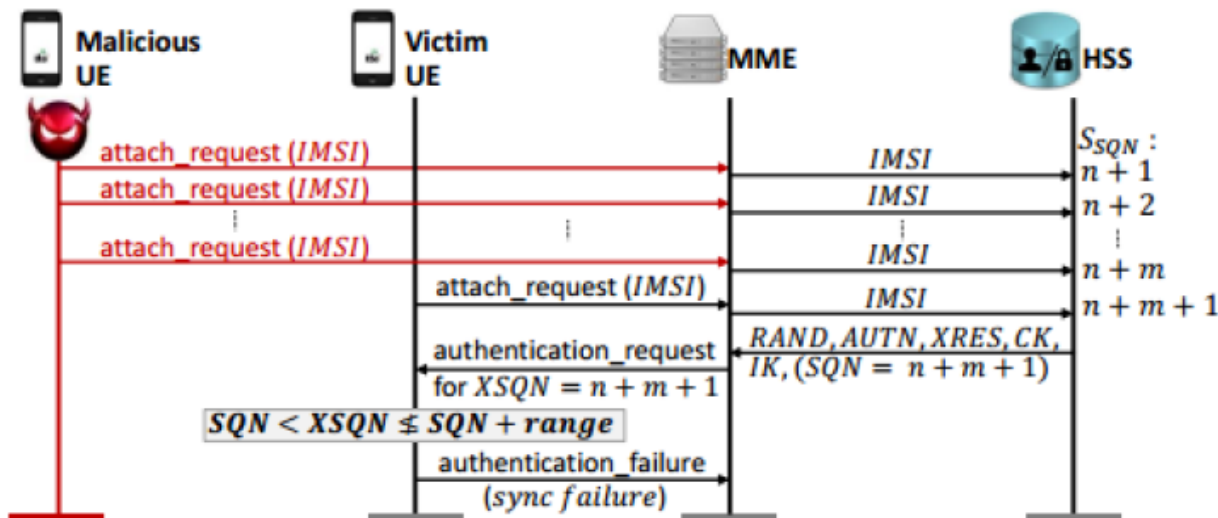
隐私保护

- UE认证通过后, 使用临时身份TMSI, 且定时更新, 体现了隐私保护的考虑
- 但首次请求中, IMSI依然明文发送, 无法防止IMSI catcher的跟踪或无意泄露

4G安全标准协议分析: LTEInspector

NDSS 2018论文

1. 提出一种LTEInspector的测试方法（基于模型的系统性对抗测试方法）
2. 使用该方法在美国四大运营商网络中确认了先前9种攻击漏洞，并发现了10种新的攻击漏洞
3. 针对新发现的攻击（10种中的8种），通过实验证明使用较低的花费（USRP等，约\$4000）便可实现，



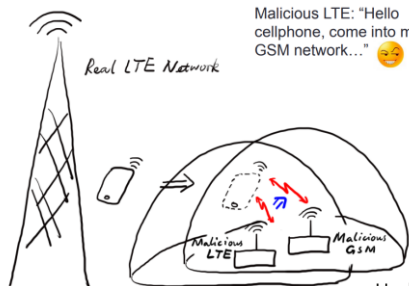
引自 NDSS 2018论文

- 前提：攻击者建立恶意UE，并知道目标UE的IMSI
- 攻击步骤：
 - A. 恶意UE使用目标UE的IMSI向核心网源源不断发送attach request（并保证每次的attach request消息中至少有一个IE与上一个不同，目的在于HSS只会处理与已收到的请求消息不同的请求）
 - B. 上述attach request导致HSS侧的SQN不断增加，于是目标UE即使后续入网时通过AUTS纠正了SQN，攻击者仍可以使用A的步骤重新组织其入网
- 效果：扰乱目标UE的入网请求

典型攻击案例：安全性妥协可导致严重后果

原因：基站发出重定向指令在认证之前

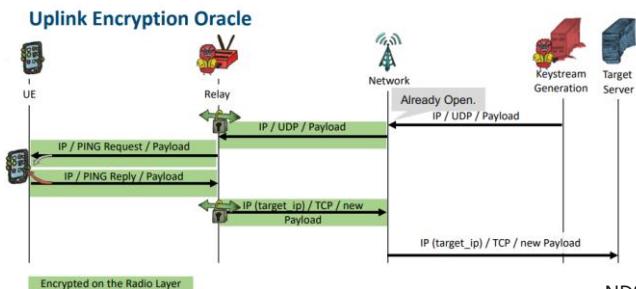
Redirection Attack



Hack In The Box 2016

2016, 奇虎360, 4G重定向攻击

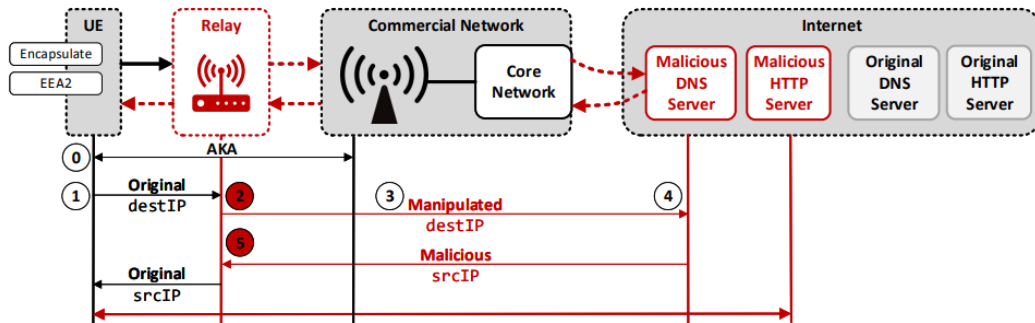
原因：用户面信息无完整性保护



NDSS 2020

2020, 德国波鸿鲁尔大学等, 4G IMP4GT 中间人攻击, 绕过双向认证冒充身份

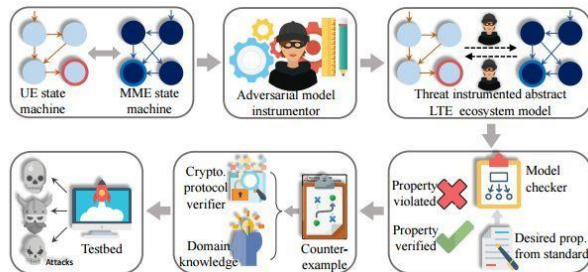
原因：用户面信息无完整性保护



IEEE S&P 2019

2019, 德国波鸿鲁尔大学, 4G aLTEr 中间人攻击, 实现DNS欺骗

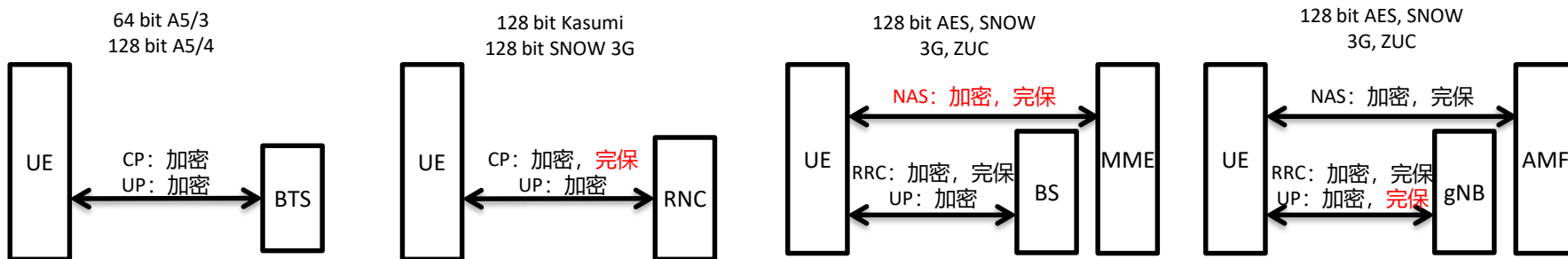
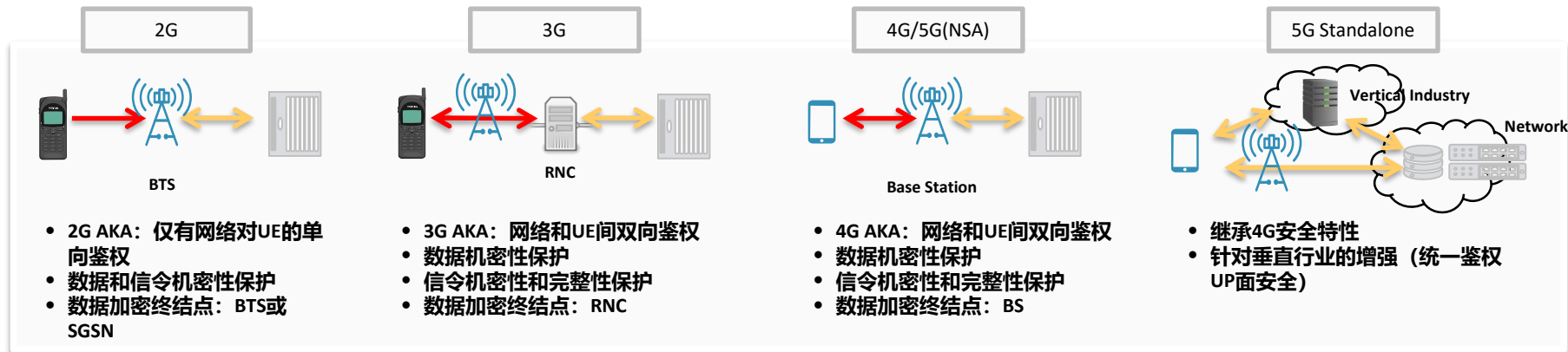
原因：协议交互中的潜在风险



NDSS 2018

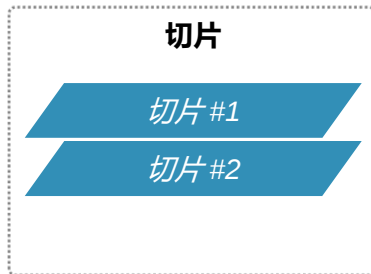
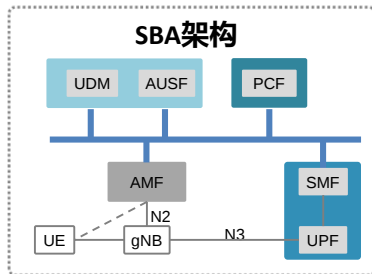
2017, 普度大学等LTEInspector, 4G漏洞（附着、去附着、寻呼）的系统分析

2/3/4/5G的安全标准演进



5G网络软件和部署架构变化，引入新的接口和边界

SBA和切片软件新架构需适配新安全



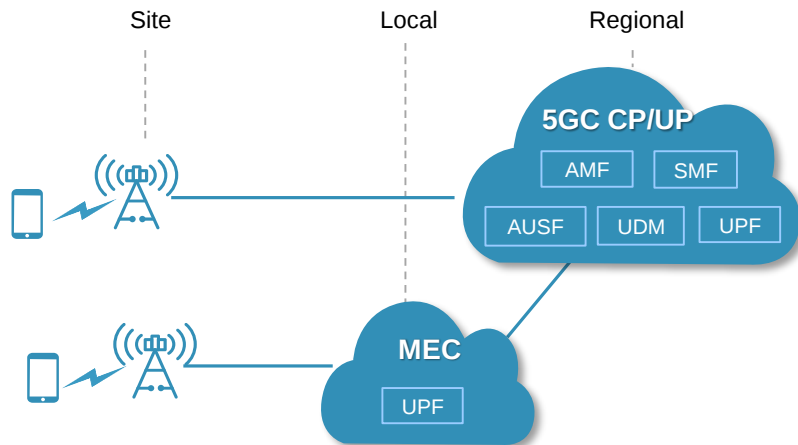
软件架构变化

- 5GC内部模块进行服务化（SBA）重构，支持业务按需部署
- 5G切片实现业务快速部署和扩容，成本更低

安全挑战

- 5GC网元基于SBA的身份认证、消息通信需加强防护
- 切片之间的边界需做好隔离，防止切片间的攻击

5GC UP支持下沉部署，需构筑MEC安全能力



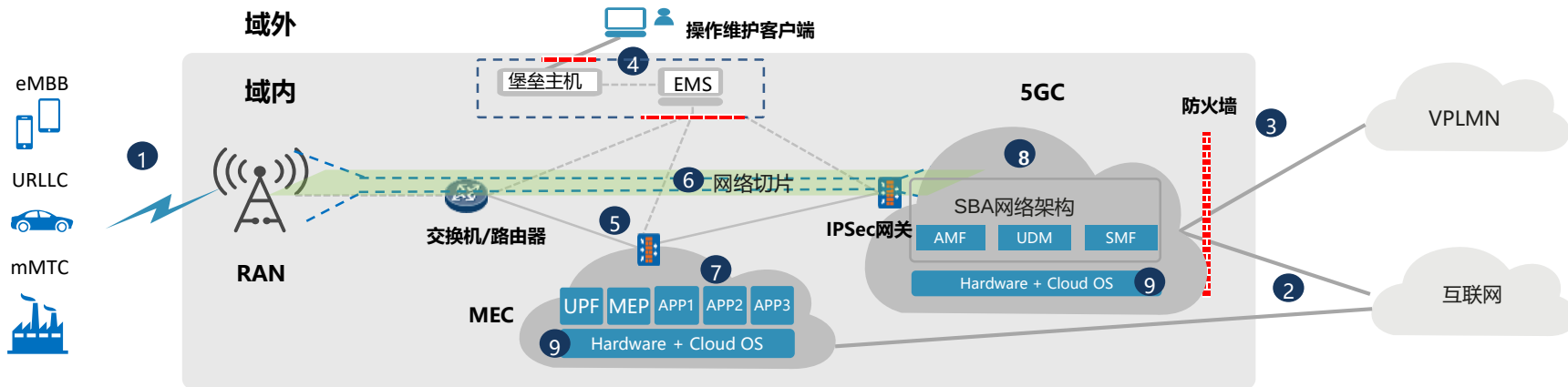
UPF部署位置变化

- UPF下沉部署（MEC），支撑本地分流，降低业务时延

安全挑战

- UPF从中心机房到边缘机房或企业园区，需加强边界防护

5G网络关键安全威胁



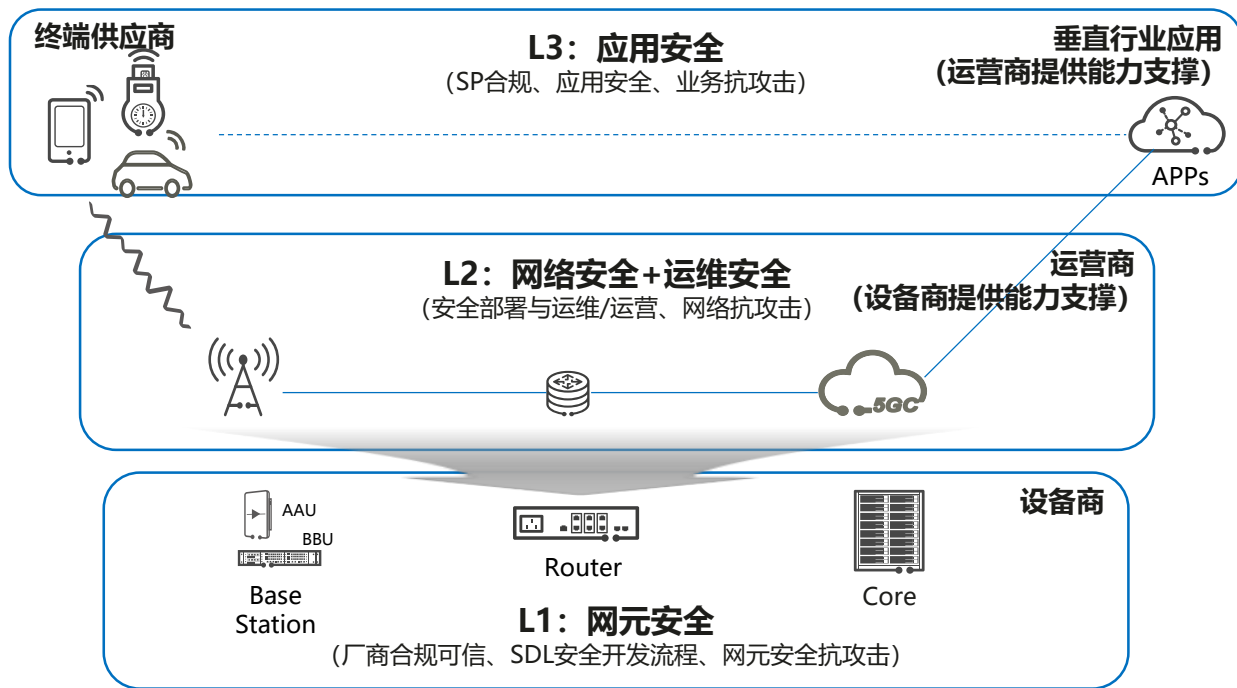
域外威胁

- 1 空口安全威胁**
 - 窃取/篡改用户数据
 - Dos攻击拒绝访问
 - 伪基站攻击
 - 空口信号干扰
- 2 互联网安全威胁**
 - 数据传输中被泄露或篡改
 - Internet上DDoS攻击而拒绝数据服务。
 - 能力开放API非授权访问 (NEF)
- 3 漫游安全威胁**
 - 数据传输中被泄露或篡改
 - 伪造漫游伙伴和拒绝服务
- 4 外部访问EMS安全威胁**
 - 数据传输中被泄露或篡改
 - 未经授权用户擅自操作
 - 授权用户恶意操作

域内威胁

- 5 域内传输威胁**
 - 数据传输中被泄露或篡改 (5GC/ME C/gNB之间)
- 6 切片威胁**
 - 越权进行切片运维管理
 - 切片间资源抢占
 - 切片间数据泄露
- 7 MEC内部的威胁**
 - 边界入侵威胁
 - 恶意APP攻击 MEC/UPF网元
- 8 5GC威胁**
 - 边界入侵威胁
 - DDoS攻击威胁
 - SBA通信威胁
- 9 云化威胁**
 - 虚拟化威胁
 - MANO威胁
 - 虚拟机/容器威胁

5G E2E网络安全：分层模型已成为业界共识



业界规范和方法论

IEC62443 IACS,
ISO/IEC 27034

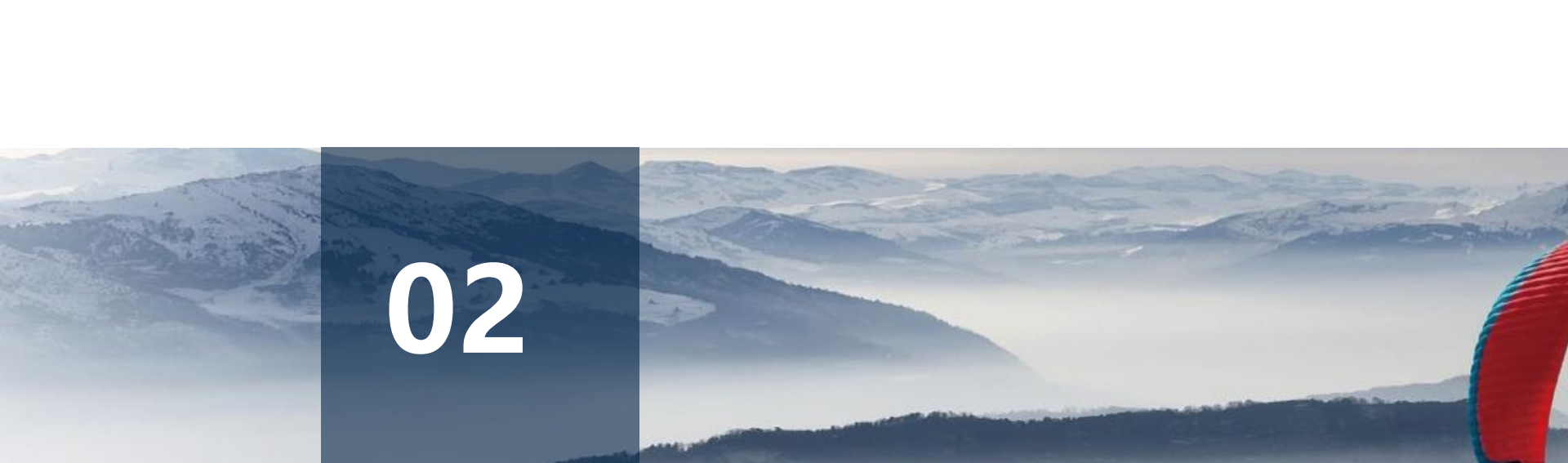
NIST CSF,
NCSC CAF,
3GPP

ISO19600, NIST SSDF,
NIST SP800-160, **3GPP**,
GSMA NESAS/SCAS

Inspired by 3GPP 33.501 security architecture

5G网络可以按通信业界的安全模型分为3个层级

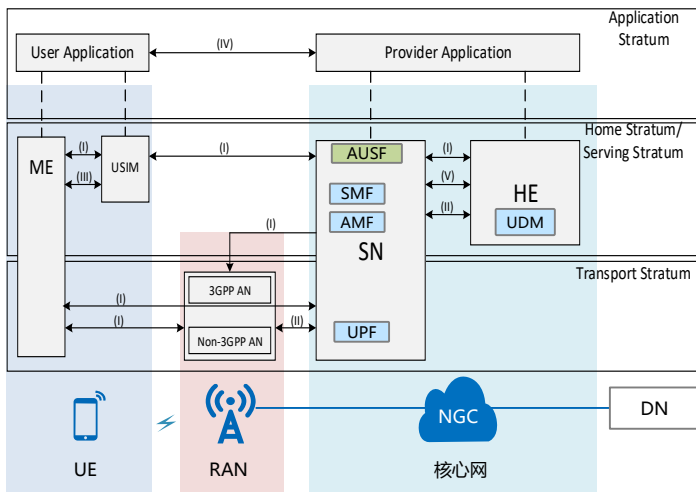
5G安全需要设备商、运营商、应用服务提供商等多方分层协作，共建5G安全体系



02

5G网络安全标准

3GPP标准定义的安全架构



(I)网络访问安全、(II)网络域安全、(III)用户域安全、(IV)应用域安全、(V)服务域安全

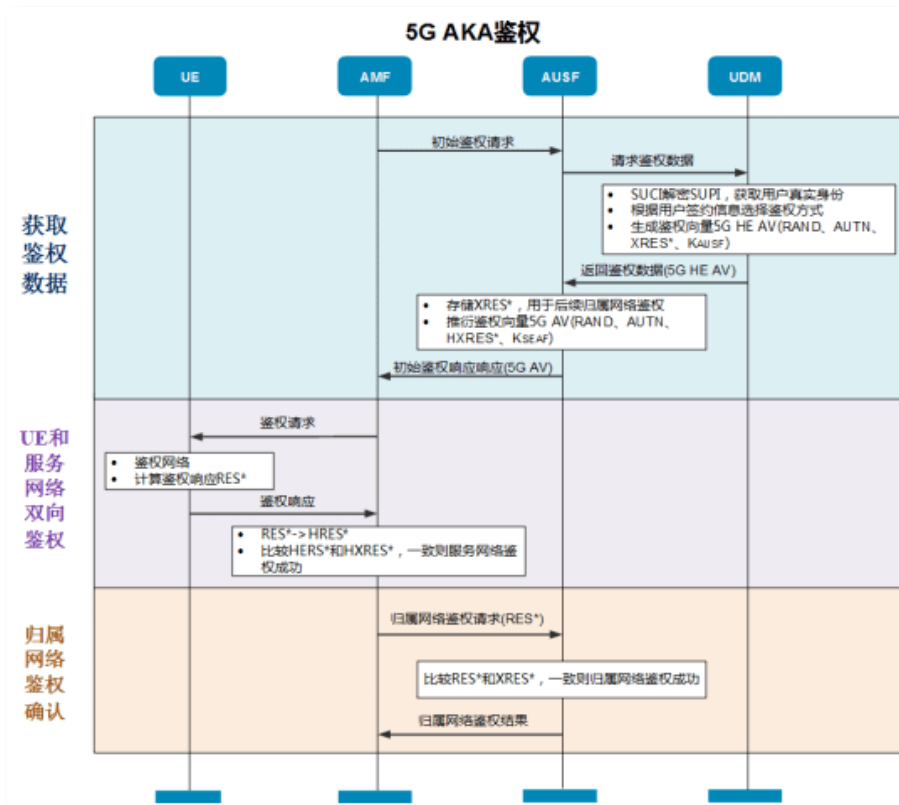
来源: 3GPP TS 33.501

- 核心网负责用户身份认证, 保护用户签约信息
- RAN通过空口加密、IPSec保证传输安全

3GPP标准安全目标

- 确保**合法认证**方可接入网络:
 - ✓ UE与网络间进行双向认证, 防范伪基站
 - ✓ UE由高制式网络回落到低制式, 防范降维攻击
- 保障空口的**机密性、完整性**:
 - ✓ 加密算法密钥使用256bit密钥
 - ✓ 新增IMSI加密保护用户隐私
 - ✓ 用户面新增完整性保护
- 确保3GPP网元间**连接安全**:
 - ✓ 3GPP各网元间使用IPSec保护传递信息安全
 - ✓ 5GC归属域与漫游域之间通过SEPP保证安全
 - ✓ 5GC服务功能间使用HTTPS

02 5G安全认证：UE接入认证5G-AKA



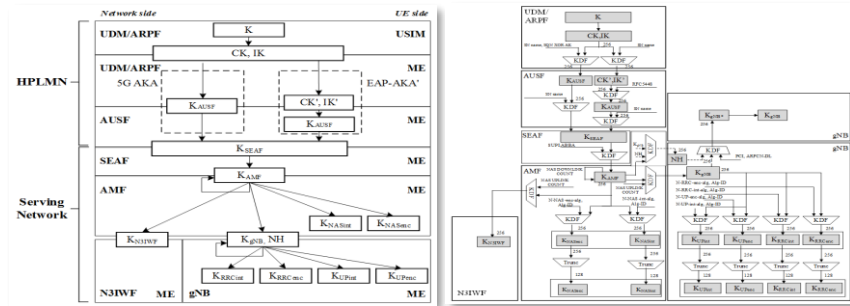
5G-AKA流程可分为，获取鉴权数据、UE和服务网络双向鉴权、归属网络鉴权确认三个子流程：

- 获取鉴权数据：**AMF首先向AUSF发起初始鉴权请求，AUSF向UDM请求鉴权数据。UDM完成SUCI->SUPI解密，根据用户签约信息选择鉴权方式并生成对应的鉴权向量。5G AKA鉴权中一次只能获取一个鉴权向量，且AUSF会做一次推衍转换。将推衍鉴权向量发给AMF。
- UE和服务网络双向鉴权 (AMF)：**
 - UE根据AUTN鉴权网络，验证通过后计算鉴权响应发送给核心网。
 - 服务网络鉴权UE，AMF验证UE返回的鉴权响应，与AUSF发来的鉴权向量作对比，如果一致，则服务网络鉴权成功。
- 归属网络鉴权确认(AUSF)：**5G新增流程，AMF将UE的鉴权响应发给AUSF，AUSF验证UE的鉴权响应，与UDM发来的鉴权向量作对比，如果一致，则归属网络鉴权成功。

移动网络采用单向分层密钥架构

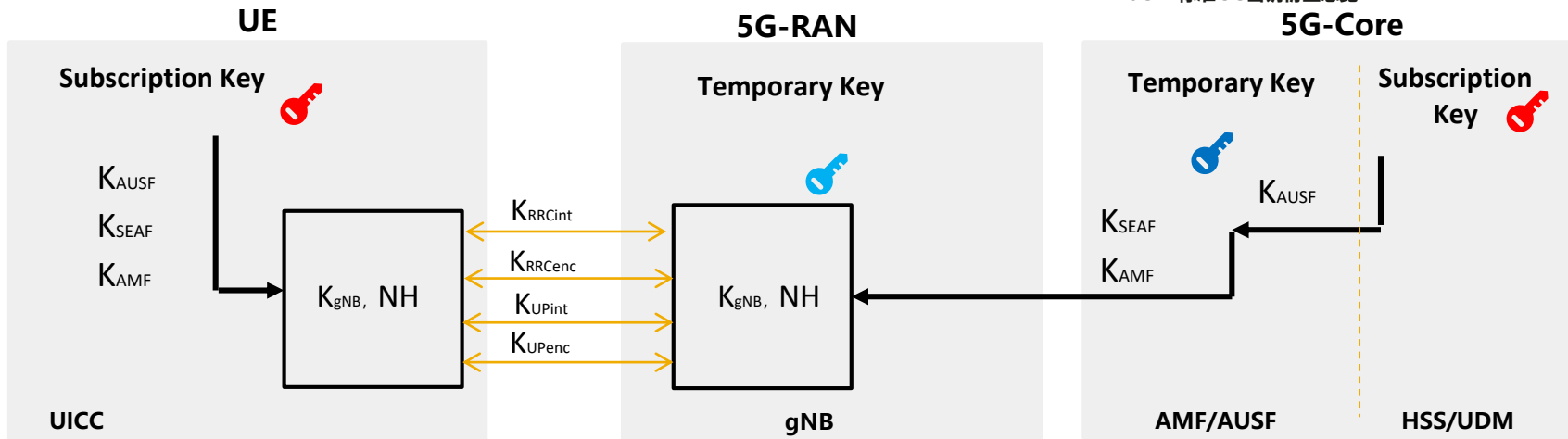
- 根密钥 (Subscription Key) 用来生成其他下层密钥 (eg. K_{AUSF})
- 根密钥无法直接生成基站密钥, 需要逐层推演
- 下层密钥无法推演出上层密钥

根密钥存储在UICC(eg. 终端USIM卡)和运营商网络的HSS/UDM中
 基站只能获得临时通信密钥, 无法推演出根密钥



3GPP标准 5G密钥衍生总览

来源: 3GPP TS 33.501



5G安全标准主要特点：继承4G的安全能力，持续增强

- 4G网络基于一系列安全方案，在过去10年运行未出现大范围攻击。
- 在4G网络有较强安全的共识下，5G重用4G安全架构，并对部分已知的风险，做进一步安全增强。

4G

用户面数据无完保

用户ID明文传输

网络级业务安全策略

漫游用户数据
明文传输

不同接入采用不同
鉴权方式

用户数据128位加密



5G

用户面完整性保护



更好的
空口安全

用户隐私保护



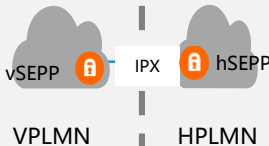
更完善的
用户隐私保护

用户级安全策略



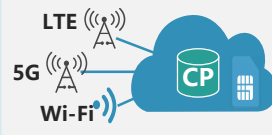
更灵活的
安全策略

漫游安全



增强的
漫游安全

统一鉴权



更高的
用户鉴权体验

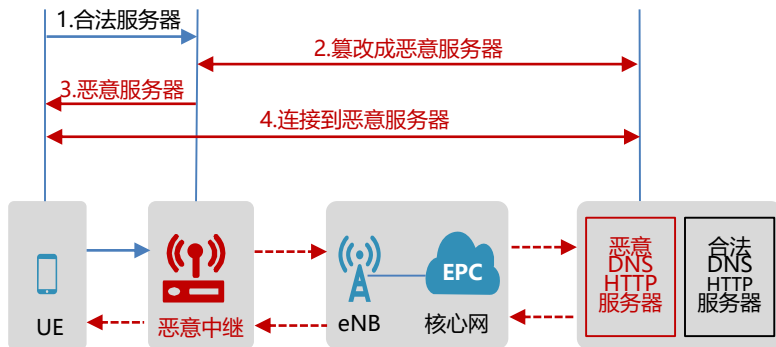
256位加密算法
(R19~)



增强的
密码算法

(1) 5G用户面完整性保护

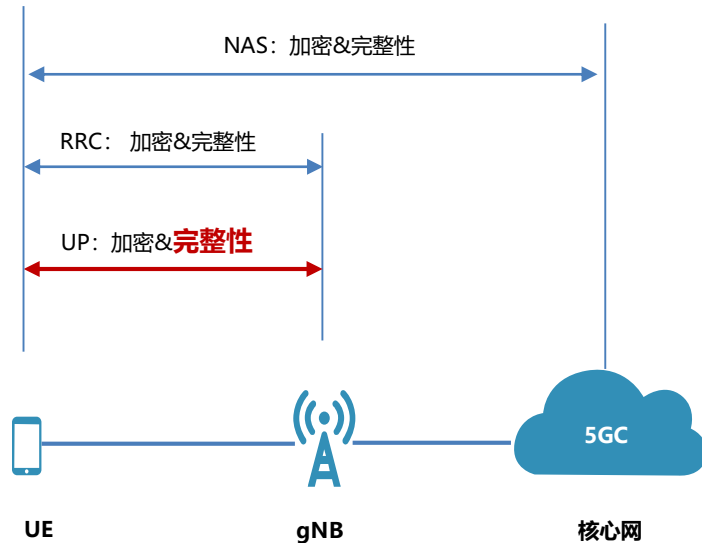
实验室场景可篡改4G用户数据进行DNS欺骗



- GSMA 2018.6.27发布该漏洞，风险源于LTE标准用户面数据缺少完整性保护
- 漏洞攻击仅实验室特定场景可实现，商用4G网络仍可抵御该攻击

来源: <https://alter-attack.net/>

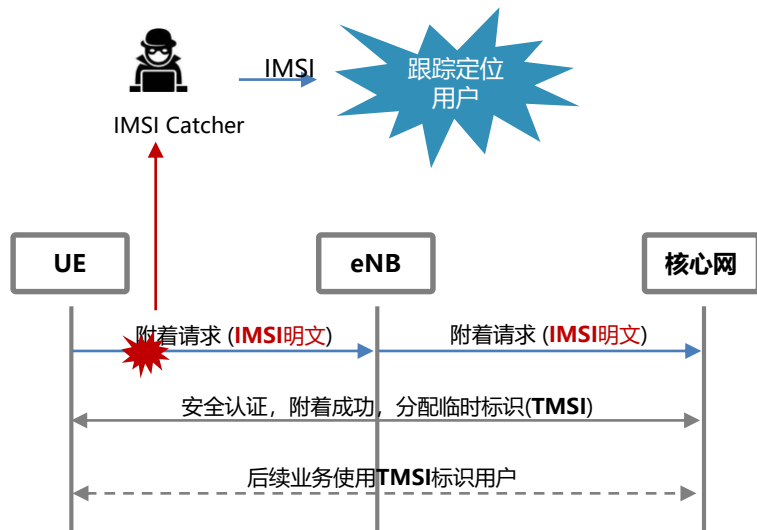
5G增加用户面完整性保护，防止篡改



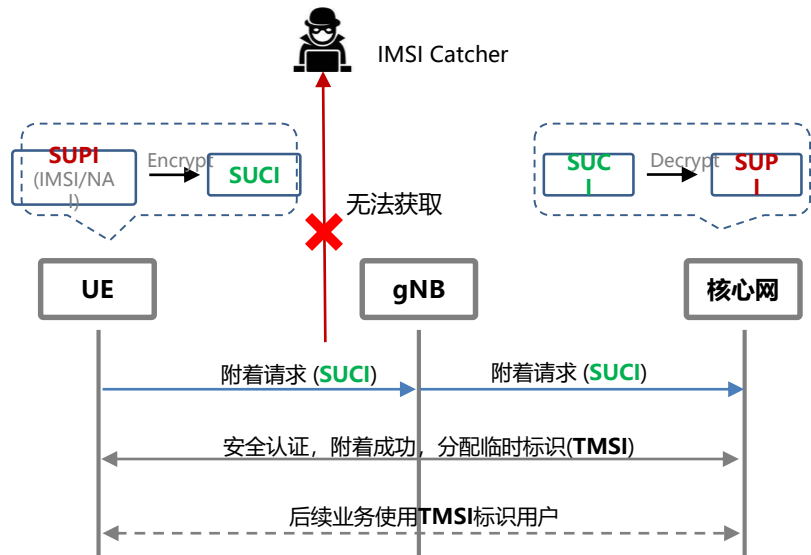
用户面数据流量高，开启完保功能对性能要求变高

(2) 5G用户身份标示隐私保护 –SUPI和SUCI

4G: 注册认证前IMSI明文传输, 存泄露可能



5G: SUPI加密传输, 避免IMSI传输泄露



(3) 5G用户面 (UP) 安全机制：细粒度的安全策略控制

价值：根据不同应用提供灵活的空口安全保护

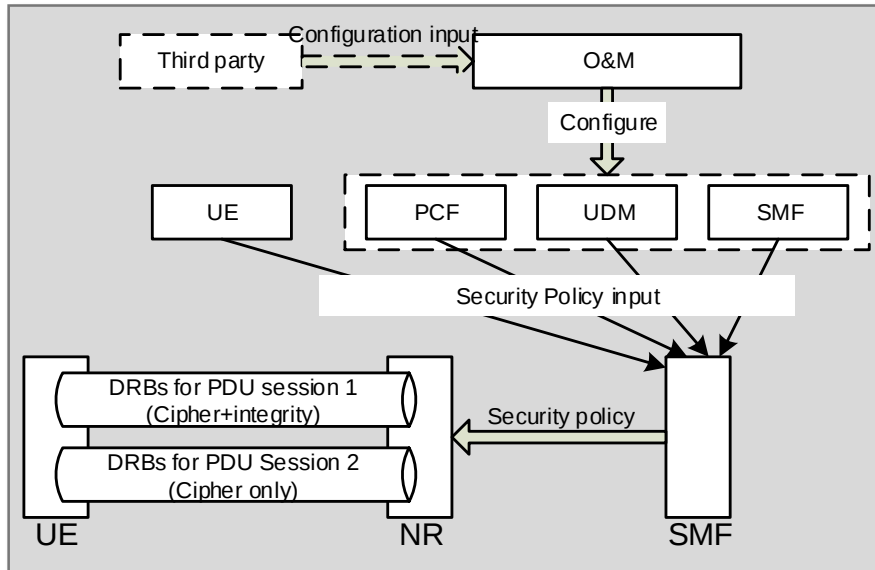
- 应用层提供安全：空口不加密，节省资源，减少处理时延
- 空口管道提供安全：空口启动加密/完保，满足高安全业务需求；
- 传统eMBB业务：只提供加密统一的加解密开关

标准结论：

- 支持根据**PDU session粒度**开启/关闭空口DRB的加密/完整性保护
- SMF下发安全策略，携带一个加密指示和一个完保指示。指示类型为“Required”、“Not Needed”和“Preferred”
- RAN2/RAN3/SA2/SA3的相关规范中已经写入相关机制

技术方案：

- SMF下发安全策略，指示gNB是否开启空口用户面加密/完保。
- gNB根据策略激活空口用户面安全保护。



(4) 5G漫游安全由SEPP或安全网关保证

2G/3G/4G 漫游边界存安全风险



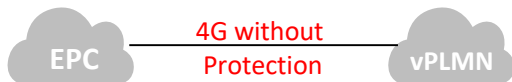
EU Black hat会议:

可以通过Diameter和SS7来攻击运营商网络



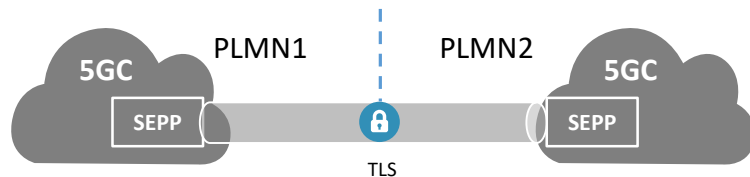
2016 Orange统计:

检测到大量来自Africa和ME的非法SS7请求

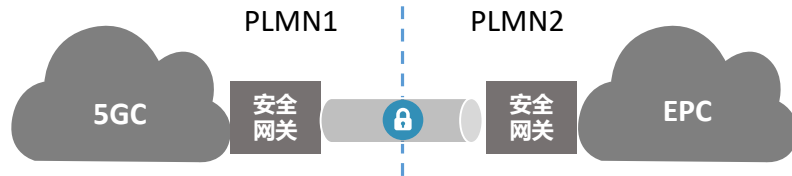


- 无过滤器来阻止无效消息
- 无端到端的信令保护
- 不受信任或不安全的服务合作伙伴

5G漫游安全增强



- 通过TLS安全协议对传输数据进行加密、完整性保护
- 引入SEPP, 实现消息过滤、拓扑隐藏



- 部署安全网关保证5GC与2/3/4G核心网漫游安全

(5) 5G安全统一鉴权框架

4G: 3GPP和non-3GPP终端鉴权 使用**不同方式(及网元)**



LTE:

- UE通过3GPP接入和non-3GPP接入使用**不同**的鉴权方法。
- 鉴权使用的网元不同, 密钥架构不同

问题:

- EPS AKA是3GPP系统特有的鉴权方法, 不被“业界”广泛使用, 变成了扩展3GPP技术的门槛

5G: 3GPP和non-3GPP终端鉴权 使用**3GPP网元**



5G:

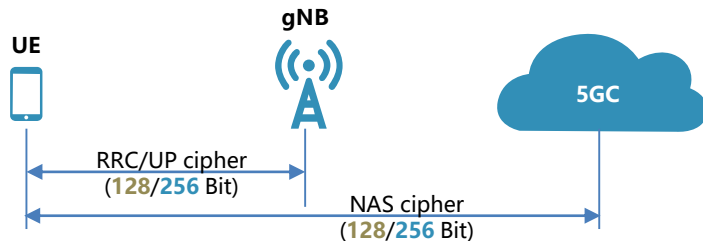
- UE通过3GPP接入和non-3GPP接入使用**相同**的鉴权方法。
- 鉴权使用的网元相同, 密钥架构相同

支持EAP鉴权框架:

- EAP是普遍使用的鉴权框架, 支持EAP鉴权可使能ToB应用。
- 现有: EAP-AKA', EAP-TLS

(6) 5G加密安全性增强：密钥长度128bit→256bit（讨论中）

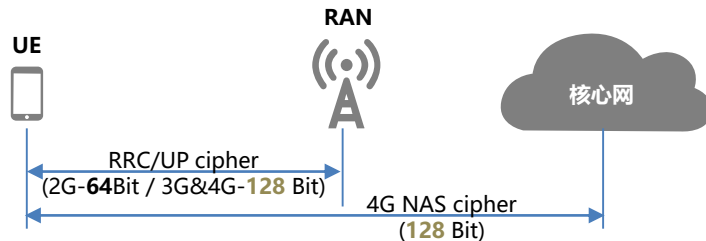
5G密钥可提升到256 Bit，防御未来量子计算风险



未来量子计算机解密

* 量子计算机的概念1980年代提出，研发迄今还没有一台真正走出实验室，世界上还没有真正意义上的量子计算机。

2/3/4G密钥为64/128 Bit，当前足够安全



Summit (巅峰) 超级计算机解密

- Summit是当前最先进超级计算机，在美国橡树岭国家实验室运行。
- 超算仅少量国家的国家级实验室拥有，网络即便降维为2/3/4G，也足够安全。

3GPP密码算法标准

算法	私有	私有	KASUMI	 KASUMI	KASUMI	 SNOW 3G	SNOW 3G	 AES	AES	 ZUC	ZUC
密钥长度 bit	64	64	64	128	128	128	128	128	128	128	128
模式	加密	加密	加密	加密	完保	加密	完保	加密	完保	加密	完保
2G GSM	A5/1	A5/2	A5/3	A5/4							
2G GPRS	GEA1	GEA2	GEA3	GEA4	GIA4	GEA5	GIA5				
3G UMTS				UEA1	UIA1	UEA2	UIA2				
4G LTE						128-EEA1	128-EIA1	128-EEA2	128-EIA2	128-EEA3	128-EIA3
5G NR						128-NEA1	128-NIA1	128-NEA2	128-NIA2	128-NEA3	128-NIA3

ZUC算法的标准化情况

3GPP标准	TS 35.221	Specification of the 3GPP Confidentiality and Integrity Algorithms EEA3 & EIA3; Document 1: EEA3 and EIA3 specifications
	TS 35.222	Specification of the 3GPP Confidentiality and Integrity Algorithms EEA3 & EIA3; Document 2: ZUC specification
	TS 35.223	Specification of the 3GPP Confidentiality and Integrity Algorithms EEA3 & EIA3; Document 3: Implementors' test data
中国国家密码标准	GB/T 33133-2016	信息安全技术祖冲之序列密码算法
国际标准	ISO/IEC 18033-4	Information technology — Security techniques — Encryption algorithms — Part 4: Stream ciphers

支持资源受限的物联网终端



适配5G 新组网

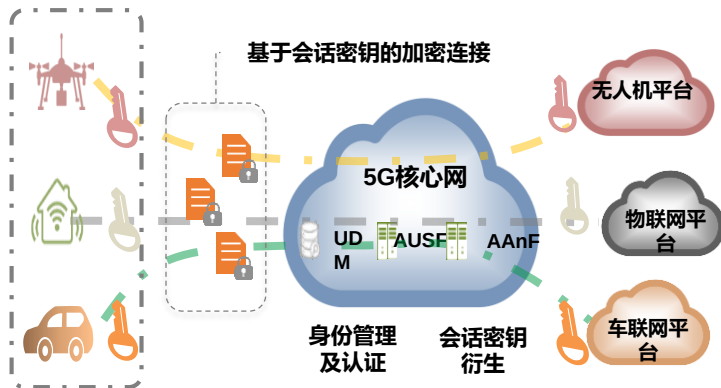


解决GBA的局限性

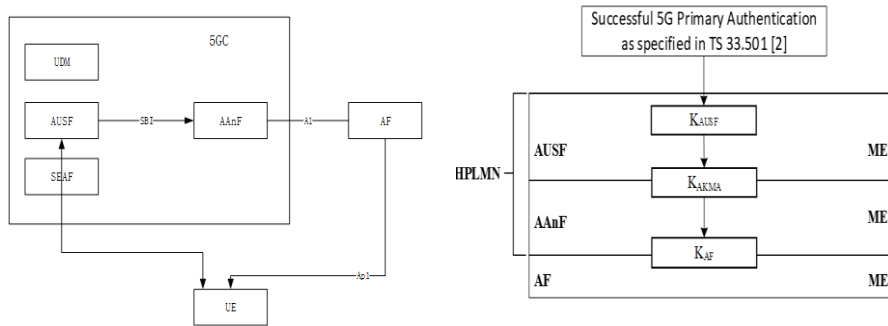


AKMA

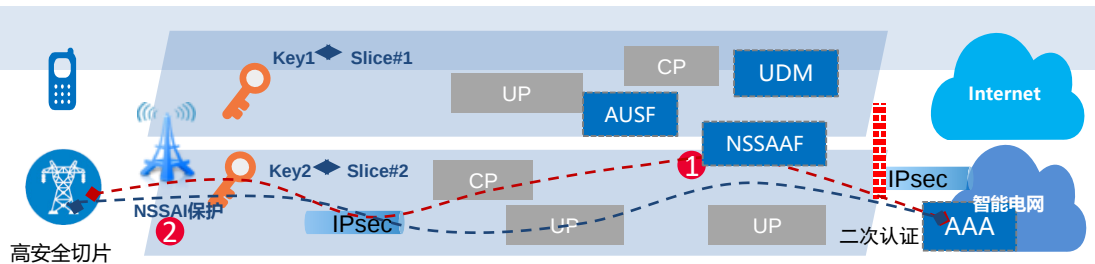
- Authentication and Key Management for Applications
- 基于用户卡和运营商网络的身份认证体系，为第三方应用提供认证服务和安全传输通道



5G网络以业务为核心，支持业务提供商为用户设置和管理密钥



- **关键技术：**AKMA密钥分发以及存储；UE和AF获得密钥K_{af}的流程
- **商业诉求：**UE和第三方的业务模块Application Function需要交互时
- **价值：**使能第三方利用3GPP预置信任状建立安全，探索开放5G安全认证能力



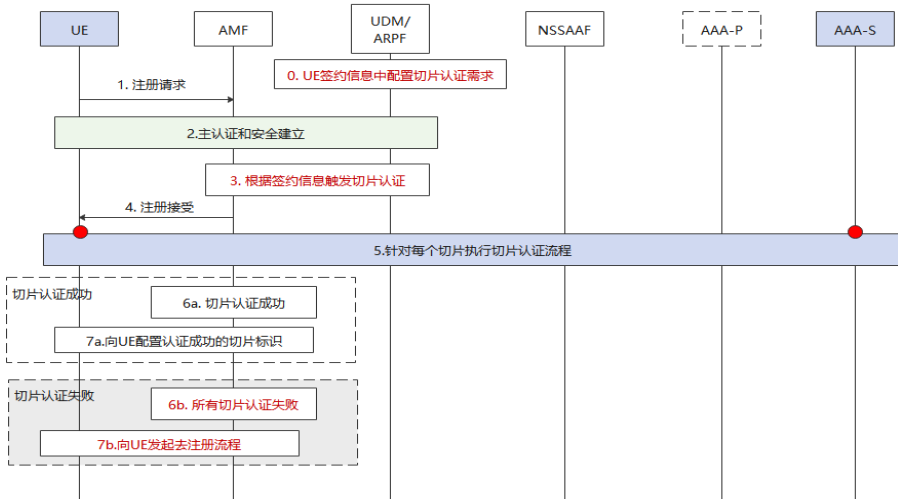
切片安全认证

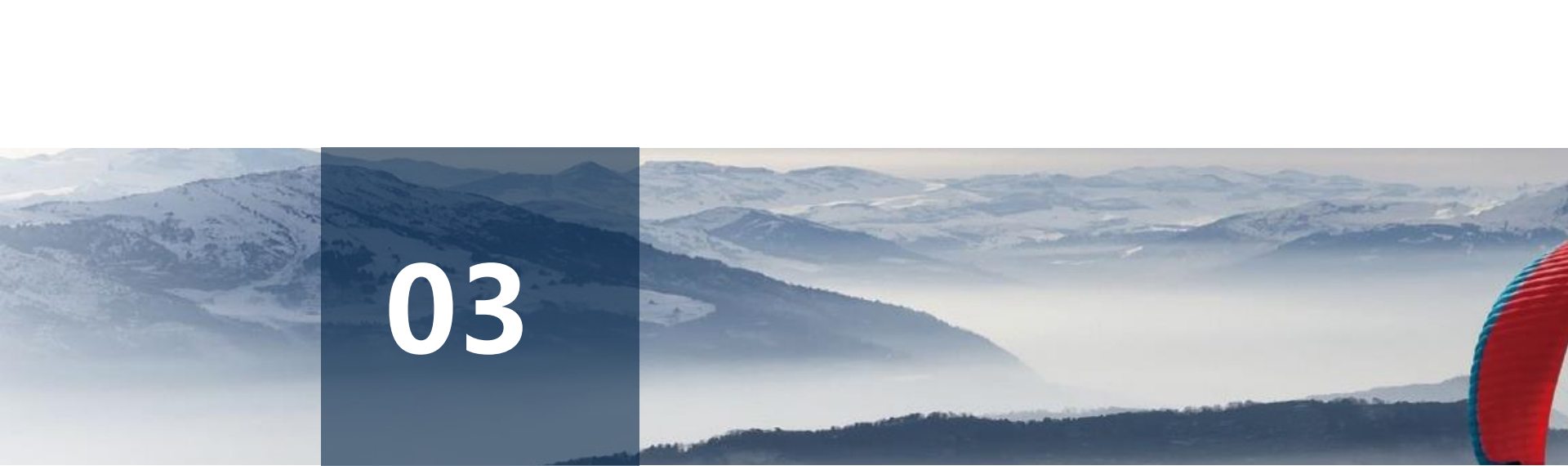
1. 5G-AKA基础上，提供切片认证；
2. 空口NSSAI加密，保护敏感用户隐私（安全开启之后）

注册过程中执行切片认证：

- 0. UDM的UE签约信息中配置切片认证需求；
- 1~2. UE接入网络执行主认证；
- 3. 主认证通过，AMF根据签约信息确定允许的切片需要切片认证；
- 4~5. AMF向UE发送注册接受消息，消息中允许的切片列表中为空。进一步的，针对每一个切片，AMF分别通过NSSAAF和AAA-P向AAA-S发起切片认证流程。
 - 6a~7a. AMF确定任意一个切片认证成功，则向UE发送认证成功的切片标识。以便UE发起后续的PDU会话建立流程进行业务。
 - 6b~7b. AMF确定所有切片认证失败，则向UE发起去注册流程。

注：UE与AAA之间使用基于EAP的认证方法。





03

5G设备安全保障体系

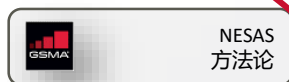
演进



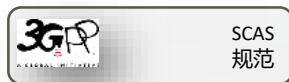
NESAS: Network Equipment Security Assurance Scheme
SCAS: Security Assurance Specification

NESAS介绍

- ✓ 标准化的网络安全评估机制
- ✓ 由GSMA和3GPP共同定义
- ✓ 移动通信行业定制
- ✓ 运营商、设备商、监管机构、行业合作伙伴共同参与



+



1. 审计

NESAS是产品开发和生命周期流程的安全审计。

审计报告



2. 测试

SCAS提供网络设备安全评估测试用例。

测试报告



NESAS价值

✓ 避免碎片化:

通过统一的安全评估标准，避免因不同国家法规和MNO不同安全需求带来的碎片化和额外开销。

✓ 技术化:

基于业界权威流程和产品评估规范，为监管机构提供技术基线。

✓ 持续演进:

根据行业需求持续演进，保障电信设备安全。

03 5G网络设备安全认证 NESAS/SCAS概述

NESAS是由GSMA和3GPP联合定义的、针对移动网络设备及其供应商流程的安全评估和审计机制。通过NESAS评估，可以证明网络设备满足一系列安全要求，以及证明网络设备是按照开发和产品生命周期流程标准而开发的。NESAS包括以下两部分：

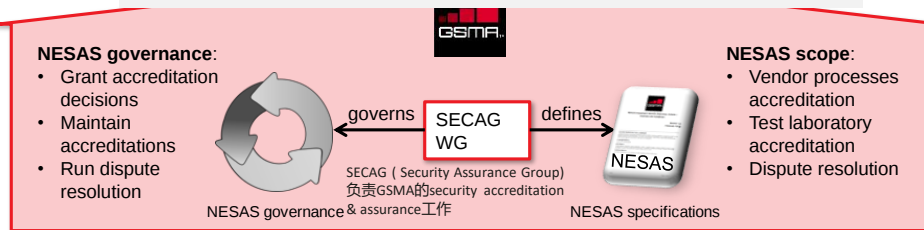
- 1、产品开发和产品生命周期流程审计：**GSMA认可的审计团队审计设备厂商，输出审计报告。GMSA NESAS Accreditation Board根据审计报告和审计团队的建议书，决策是否向设备厂商授予认可（Accreditation）。
- 2、产品安全测试：**通过GSMA认证的测试实验室，依据3GPP SCAS标准测试网络产品，并基于审计报告验证已认可的供应商开发流程应用到了被测网络产品上，输出评估报告。

GSMA和3GPP角色与分工

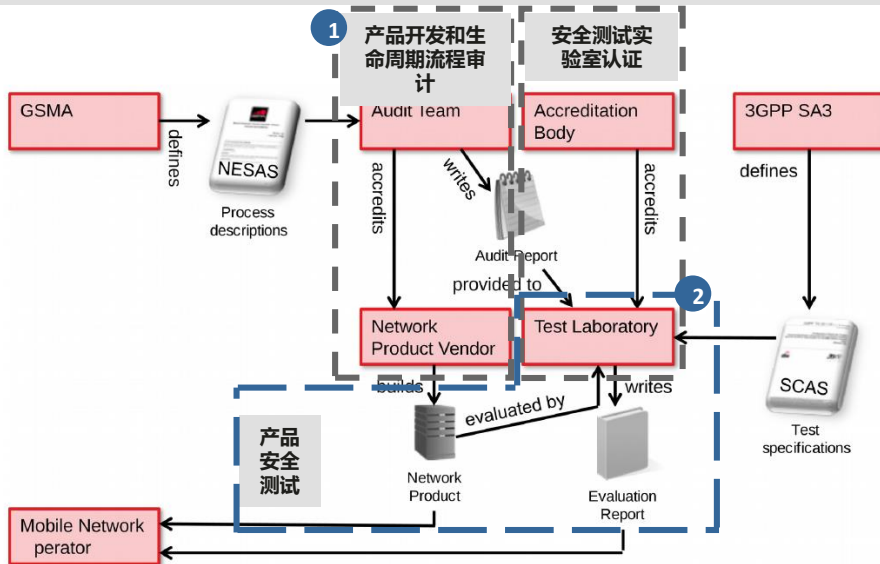
3GPP制定产品安全测试依据的SCAS标准



GSMA制定产品开发和产品生命周期流程审计的NESAS标准



NESAS High-Level 流程



NESAS/SCAS标准持续完善：覆盖更多生产要素和网元设备

NESAS 要求

设计	编码	编译	测试	发布	运维	EOX
Req.-01安全设计	Req.-04 源代码检视	Req.-10 自动化构建流程	Req.-05 安全测试	Req.-13 软件完整性保护	Req.-17 安全联络人	Req.-12 漏洞信息管理
Req.-21 第三方组件选型	Req.-18 源代码治理	Req.-11 构建环境控制		Req.-14 唯一的软件发布标识	Req.-12 漏洞信息管理	
N				Req.-16 文档准确性	Req.-07 漏洞修复流程	
				Req.-20 安全文档	Req.-08 漏洞修复独立性	
					Req.-15 安全修复沟通	

图标: N, 新要求

NESAS 2.0 增强:

1. 第三方组件选型：供应商应有流程确保第三方组件在产品生命周期的质量。供应商应选择受支持的第三方组件，并应避免使用已达到使用寿命终止的组件。
2. NESAS2.0主要针对标准质量改进和CSA合规性进行优化。.

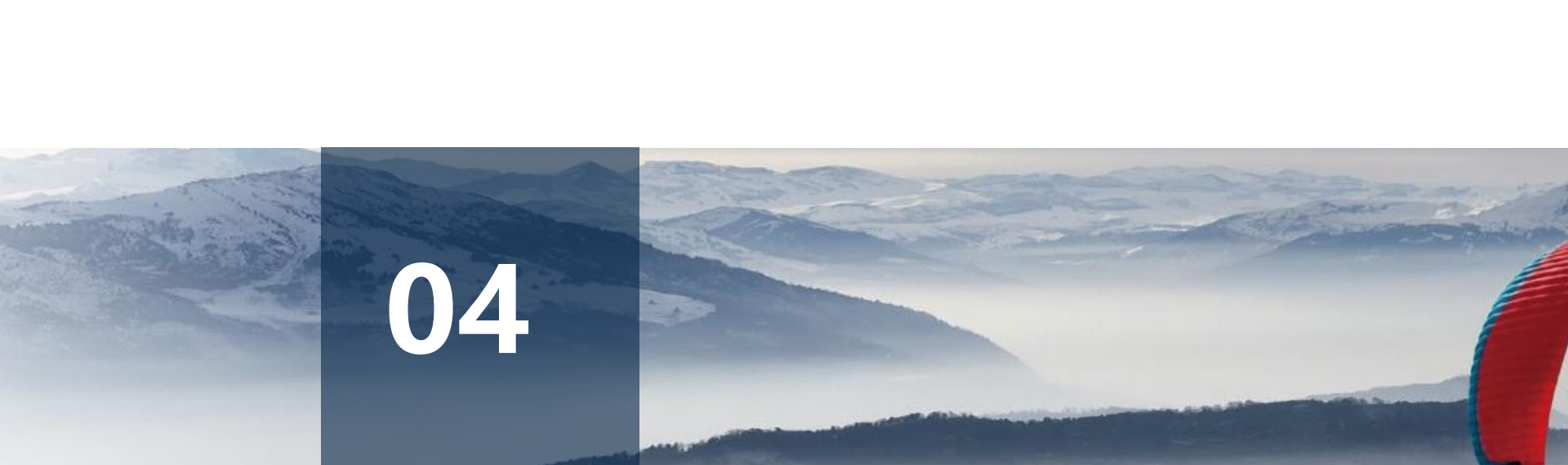
公共要求

Req.-02 版本控制, Req.-03 变更管理, Req.-06 员工教育, Req.-09 信息安全管理(ISMS), Req.-19 持续改进

SCAS 规格

通用	基站	核心网								其它
TS 33.117 通用安全保障 需求目录	TS 33.511 gNodeB	TS 33.512 AMF	TS 33.513 UPF	TS 33.514 UDM	TS 33.515 SMF	TS 33.516 AUSF	 N3IWF	 NWDAF	 NSSAAF	...
	TS 33.216 eNodeB	TS 33.517 SEPP	TS 33.518 NRF	TS 33.519 NEF	TS 33.116 MME	TS 33.250 PGW	 IPUPS	 SECOP	...	

截止2021年



04

总结及展望

- 5G安全需要设备商、运营商、应用服务提供商等多方分层协作，共建5G安全体系。
- 5G继承4G的安全能力，虽面临新的挑战，标准安全持续增强。



量子霸权



PROJECTS Post-Quantum Cryptography

2020.07.22, NIST公布后量子密码候选第三轮结果：7+8

Public-Key Encryption/KEMs

Classic McEliece
CRYSTALS-KYBER
NTRU
SABER

Digital Signatures

CRYSTALS-DILITHIUM
FALCON
Rainbow



Alternate Candidates

Public-Key Encryption/KEMs

BIKE;
FrodoKEM
HQC
NTRU Prime
SIKE

Digital Signatures

GeMSS
Picnic
SPHINCS+

安全特性	对称密码算法		非对称密码算法		量子计算机出现后对3GPP安全威胁
	加密密钥长度	完保密钥长度	加密密钥长度	完保密钥长度	
SUPI加密	128	256	128	256	SUPI加密被破解，永久身份泄露造成隐私等问题
初始认证	128	128	-	-	攻击者恢复出long term key 基于SIM卡的安全认证体系破解失效
传输安全	128	128	TLS/IPsec	TLS/IPsec	加密和完保失效造成多种中间人攻击，如数据被窃听和篡改



- ✓入侵检测和防御 Intrusion Detection and Prevention
- ✓欺诈检测 Fraud detection
- ✓信用评分和下一步最佳方案 Credit scoring and next-best offers
- ✓僵尸网络检测 Botnet Detection
- ✓(更)安全用户认证 Secure User Authentication
- ✓黑客事件预警 Hacking Incident Forecasting
- ✓垃圾邮件过滤 Spam Filter Applications
- ✓AI模型安全，防窃取，鲁棒性，隐私保护等
 - ✓闪避攻击、药饵攻击、后门攻击、模型窃取攻击等
- ✓AI治理、市场准入等风险

AI for Security vs. Security for AI

展望：5G+时代标准路线对抗加剧，安全技术备受瞩目



Improving 5G Network Security: **Open, Programmable, Secure 5G (OPS-5G) program**
New program seeks to leverage open source software and systems to address security challenges facing 5G and future wireless networks (such as 6G) , 2020.02



The program is split into four technical areas (TAs):

TA1 Standards Meet Software: Decreasing the time required for updates to OPS-5G open source software in response to new versions of the 5G standards;

TA2 Cross-scale 5G node and network security: Achieving a **usable scalable “zero-trust” security architecture** for devices ranging from **IoT sensors to servers**. The architecture should have a minimal impact on size, weight and power (SWaP), and price;

TA3 Secure slices: Mitigating new attack surfaces (such as **side-channels**) introduced by **virtualization and slicing**;

TA4 Principled programmable defenses: Changing **programmability from a threat vector to an enabler of security at scale**

三个方向安全相关

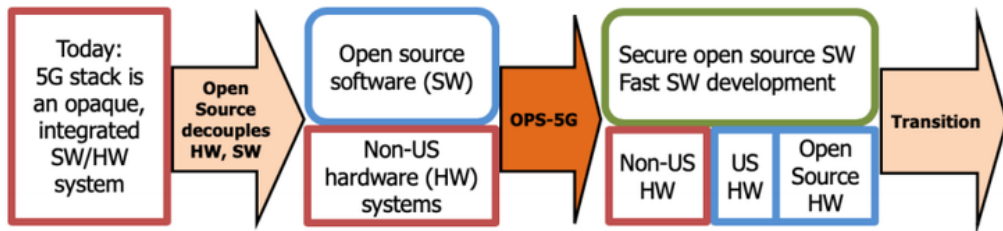
- ◆ 零信任物联网架构
- ◆ 虚拟化和切片安全
- ◆ 可编程安全防护

OPS-5G aims to lead to the development of a portable standards-compliant network stack for 5G mobile that is **open source** and **secure by design**. The "long-term objective is a **US-friendly ecosystem**" featuring a trillion networked devices

当前

专用设备
封闭环境

非美厂商
控制生态



未来

通用设备
开放环境

软硬优势
重夺霸权

Figure 1: OPS-5G augments Open Source Software to obtain a secure 5G system (red: non-US; blue: US; green: OPS-5G)

DARPA 公开材料

Thank You