5G安全风险分析及标准进展

Risk Analysis and Specification Progress of 5G Security

杨红梅/YANG Hongmei[1]，赵勇/ZHAO Yong[2]

（1. 中国信息通信研究院，北京 100191；
2. 中国电信股份有限公司北京分公司，北京 100010）
(1. China Academy of Information and Communications Technology, Beijing 100191, China;
2. China Telecom Co., Ltd. Beijing Branch, Beijing 100010, China)

摘要：5G网络新技术、新特征带来了新的安全风险与挑战，主要体现在虚拟化设备安全边界模糊，数据泄露风险有所增加，海量多样化终端容易成为新的攻击目标以及新业务场景下安全责任主体划分难度加大等方面。5G安全相关标准重点研究5G安全关键技术、5G系统安全架构和流程相关要求、设备安全保障等，目前已完成第1版本（R15）的标准制定工作，预计2019年底完成第2阶段（R16）5G安全的标准制定工作。

关键词：5G；基础设施；关键技术；安全风险；供应链风险；标准

Abstract: New technologies and features of 5G network bring new security risks and challenges. It is mainly reflected in the blurred security boundary of virtualization equipment, the increased risk of data leakage, massive diversified terminals which are vulnerable to attack, and the increased difficulty in the division of security responsibility subjects in new business scenarios. The 5G security specifications focus on the key technologies of 5G security, the security architecture and process, security assurance, etc. At present, the first phase (R15) of 5G security specifications has been published, and the second phase (R16) is expected to be completed by the end of 2019.

Key words: 5G; infrastructure; key technology; security risk; supply chain security risk; specification

DOI：10.12142/ZTETJ.201904001
网络出版地址：http://kns.cnki.net/kcms/detail/34.1228.tn.20190704.1915.002.html

网络出版日期：2019-07-05
收稿日期：2019-06-13

5G时代，移动通信将大幅提升移动互联网业务的使用体验，进一步满足海量物联网应用的多样化需求，与工业、医疗、交通、金融等行业深度融合，实现“无处不在，万物互联”。5G网络与垂直行业深度融合的特点导致5G安全问题不仅影响人和人之间的通信，还将会影响到各行各业，有些场景甚至可能威胁到人们的生命财产安全乃至国家安全；因此，世界主要国家均将5G作为优先发展的战略性领域，5G安全问题成为世界各国关注的焦点。

近期，部分组织或国家（如欧盟、美国、捷克等）在5G安全领域发布了多个5G安全相关报告，这些报告所表达的观点主要涵盖2个方面：一是5G安全意义重大，5G网络的安全性对于国家安全、经济安全和其他国家利益以及全球稳定性至关重要；二是5G将面临新的安全风险，有必要开展5G安全风险评估，并倡导将供应链安全及非技术因素纳入5G安全评估范畴。中国在2016年12月发布《国家网络空间安全战略》，提出要统筹网络发展和安全2件大事，认为安全是发展的保障，发展是安全的目的。

1 5G网络的主要特点

5G是新一代信息通信技术的主要发展方向，业务应用从移动互联网扩展到移动物联网领域，服务

对象从人与人通信拓展到人与物、物与物通信，并将与经济社会各领域深度融合，引发人们生产、生活方式的深刻变革。国际电信联盟无线电通信组（ITU-R）定义了5G的3类典型业务场景：增强移动宽带（eMBB）、海量机器类通信（mMTC）、高可靠低时延通信（uRLLC），它们的应用需求以及对网络的性能要求各不相同。

与4G相比，5G网络整体架构延续4G特点，仍采用接入层、核心网层和应用层3层架构。不过，为了应对5G需求和场景对网络提出的挑战，并满足更加灵活、更加智能的发展趋势，5G网络进行了创新和变革。5G网络有以下几个主要特征：采用新型基础设施平台和新型核心网架构；比4G支持更多样化的业务场景；支持更高的性能指标并提供更强、更灵活的通信安全能力。下面我们从网络和安全2方面分别阐述。

（1）5G网络方面。基于网络功能虚拟化（NFV）和软件定义网络（SDN）技术实现基于通用硬件的新型基础设施平台。新型核心网基于统一基础设施平台进行云化部署，具有硬件平台通用化、软件功能模块化的特点：能够重构网络控制和转发机制，进一步实现控制和转发分离，改变单一管道和固化的服务模式；利用友好开放的基础设施环境，可为不同用户和垂直行业提供定制化的网络服务，构建资源全共享、功能易编排、业务紧耦合的综合信息化服务使能平台；利用服务化架构、网络切片、边缘计算、5G网络能力开放等技术满足各行业需求。

（2）5G安全方面。5G网络采用统一的认证框架来融合不同的接入认证方式，并优化现有的安全认证协议（如安全上下文的传输、密钥更新管理等）；采用差异化身份管理机制以及匿名化技术来保护用户隐私；为不同应用场景提供按需的安全保护，可满足业务多样化的时延要求、终端设备的生命周期要求；采用更加灵活的安全机制保障网络安全。总体来说，5G可提供更健壮的业务安全性、更严密的数据保护以及更强的用户隐私性，可提供比4G系统更强大的通信安全能力。

2 5G安全风险分析

相比于传统3G/4G网络，5G核心网基于NFV等新技术，在架构和功能上提供更泛在的接入支持、更灵活的控制和转发机制，以及更友好的能力开放方式，打破了传统电信网络的封闭性，同时能与云化基础设施结合，为普通消费者、应用提供商和垂直行业提供网络切片、边缘计算等新型业务能力。5G网络新技术新业务带来便利性的同时，也带来了安全风险和挑战。

2.1 5G新技术新特性带来的安全风险与挑战

5G面临的新安全风险和挑战主要包括：实体网元变为虚拟化软件，物理资源共享，设备安全边界模糊，开放端口成为数据泄露的脆弱点，多样化终端的安全能力差异大，容易成为新的攻击目标以及新业务场景下安全责任归属问题等。

（1）基础设施虚拟化云化。

基础设施虚拟化云化给网络安全带来了突出挑战，具体表现在以下几个方面：虚拟化服务化架构模糊了传统网络边界，给虚拟化软件及虚拟机间的通信安全带来风险；集中的控制点容易成为网络攻击的“重灾区”；分层解耦、多厂商集成导致安全问题快速定位和溯源困难；开源软件的脆弱性及安全漏洞，给自动化安全评估和修复带来挑战，同时新型网络架构对安全运维人员的经验、技能提出了新的挑战。

（2）边缘计算。

边缘计算是指在网络边缘、靠近用户的位置上提供信息技术（IT）的服务、环境和云计算的能力，边缘计算节点可根据应用服务的需求部署于移动网络的边缘，提供超低时延的同时也能够降低高带宽业务的数据流对核心网的压力。但是，边缘计算带来便利的同时也带来了安全风险和挑战：一方面，移动边缘计算（MEC）基础设施通常部署在网络边缘，客观缩短了攻击者与MEC物理设施之间的距离，使得攻击者更容易接触到MEC网络基础设施，被攻击后可能会造成物理设备毁坏、服务中断、用户隐私和数据泄露等严重后果；另一方面，由于性能、成本、部署灵活性要求等多种因素制约，MEC节点的安全能力不够完善，可抵御的攻击种类和抵御单个攻击的强度不够，容易被攻击，使5G网络面临风险；另外，MEC服务不仅可由网络运营商提供，也可由第三方服务商提供，当MEC服务由第三方提供时，在接入网络的时候

如果没有调用认证与鉴权接口，则面临恶意第三方接入网络提供非法服务的风险等。

（3）网络切片。

5G 网络切片是在统一基础设施上，为用户提供专用服务。网络切片为不同业务提供差异化安全服务的同时，也面临一定的安全风险：不同的网络切片承载不同的 5G 业务，但网络切片共享网络基础设施，这就对切片的安全隔离能力带来挑战。若网络切片的认证和授权能力不足，则可能造成敏感信息和/或隐私信息泄漏，并且被攻击者所利用。另外，在 5G 新业务场景下，运营商可能会以网络切片的模式向第三方企业、用户提供网络服务，对于此种服务中涉及的运营商、虚拟运营商、用户等不同层和不同域的安全责任主体划分问题面临挑战。

（4）网络能力开放。

5G 网络基于网络能力开放技术，与垂直行业深度融合，使得垂直行业可以充分利用网络能力的同时灵活开发新业务，但也带来新的风险和挑战：5G 网络能力开放架构可能会面临网络能力的非授权访问和使用、数据泄露、用户和网络敏感信息泄露等安全风险，同时攻击者还可以利用 5G 网络能力开放架构提供的应用程序编程接口（API）对网络进行拒绝服务攻击；随着跨行业应用的开展，需要开放共享相应的用户个人信息、网络数据和业务数据，这些信息和数据从运营商内部的封闭平台开放共享到垂直行业企业的开放平台上，运营商对数据的控制力减弱，数据泄露的风险增大。另外，跨行业数据共享过程中一旦发生用户数据泄露等安全事件，将面临主体间的责任划分不清的风险。

（5）海量多样化终端。

5G 支持多种接入技术，终端类型复杂多样，终端的安全能力差异巨大，终端设备分散不便统一管理，应用需求复杂难以部署强有力安全防护。因此，5G 时代海量多样化终端会给 5G 网络带来安全风险。

巨量化、泛在化的智能终端易被利用成为新攻击源。一方面在 mMTC 场景下，未来将有数以百亿计的终端接入物联网，一旦这些终端被入侵利用，形成规模化的设备僵尸网络，将成为新型高容量分布式拒绝服务（DDoS）攻击源，进而对用户应用、后台系统等发起攻击；另一方面，物联网终端提供的数据信息量巨大，分类众多，应用场景多元化，但缺乏统一的安全标识和认证管理机制，这也增加了网络管理的难度。

另外，终端上日趋开放的用户应用生态环境将加大安全管理挑战。在 5G 的泛在连接场景下，生产类、生活类应用可能同时安装在一台用户终端上，开放的应用生态环境在带来生产和生活便利的同时，也加剧了恶意应用威胁其他应用安全、终端安全以及后台生产系统安全的风险。

2.2 5G 融合应用面临的安全风险与挑战

5G 融合应用基于 5G 网络开展业务，因此也面临 5G 新技术、新特性带来的安全风险与挑战，并具有各自业务本身的特点。同时，5G 新应用迭代速度快，5G 规模商用对经济社会带来的影响有待持续评估，安全风险呈现动态演进、持续变化的特点。具体表现为：（1）eMBB 场景下个人信息泄漏风险加大；（2）uRLLC 场景下数据保护风险加大；（3）mMTC 场景下多种终端形态导致海量终端被攻击的风险增大。

另外，5G 融合应用业务发展模式尚不明朗，其面临的风险可能在相当长一段时间之后才会逐步显现，有待持续跟踪研究。

2.3 应对举措

针对 5G 网络和业务面临的安全风险，可以从以下几个方面来应对：完善 5G 安全相关政策和管理制度，确保 5G 安全能力建设和业务发展同步推进；加大 5G 安全研发投入，在 5G 网络建设过程中，将安全需求纳入到业务设计、网络和网元动态部署的各个环节中，形成针对 5G 网络特点的主动防御体系；构建 5G 安全标准体系，加强 5G 网络安全新技术研究，制定完善 5G 安全技术标准，提升国际标准话语权。

3 5G 安全标准进展

3.1 国际标准

5G 相关国际标准主要由第 3 代合作伙伴计划（3GPP）研究制定，分为 R15 和 R16 2 个版本来满足 ITU IMT-2020 的全部需求：R15 为 5G 基础版本，重点支持 eMBB 业务和基础的 uRLLC 业务；R16 为 5G 增

强版本，将支持更多类型的业务。目前，3GPP已完成了R15独立组网5G标准，并将于2019年底发布R16标准。R16标准在R15的基础上，进一步增强网络支持eMBB的能力和效率，重点提升对垂直行业应用的支持，特别是对uRLLC类业务以及mMTC类业务的支持。

5G安全研究及标准制定与5G总体架构相关工作保持同步。3GPP于2018年6月完成了第1阶段（R15）5G安全标准，重点研究5G系统安全架构和流程相关要求，包括安全框架、接入安全、用户数据的机密性和完整性保护、移动性和会话管理安全、用户身份的隐私保护以及与演进的分组系统（EPS）的互通等相关内容。预计2019年底将可以完成第2阶段（R16）5G安全标准的工作，将重点推进uRLLC安全、切片安全、5G蜂窝物联网（CIoT）安全、增强的服务化架构（eSBA）安全、位置业务安全增强等工作。

5G安全相关的主要国际标准如下：

- 5G系统安全架构和流程（3GPP TS 33.501）[1]；
- 3GPP系统架构演进（SAE）安全架构（3GPP TS 33.401）[2]；
- 安全保障通用要求（3GPP TS 33.117）[3]；
- 5G安全保障规范NR Node B（gNB）（3GPP TS 33.511）[4]；
- 5G安全保障规范接入与移动管理功能（AMF）、用户平面功能（UPF）、统一数据管理（UDM）、会话管理功能（SMF）、认证服务器功能（AUSF）、安全边界保护代理（SEPP）、网络存储功能（NRF）、网络开放功能（NEF）（3GPP TS 33.512~519）[5]-[12]。

其中，《5G系统安全架构和流程》和《3GPP系统架构演进（SAE）安全架构》主要规定独立组网（SA）架构和非独立组网（NSA）架构下的5G网络架构及安全机制相关内容；安全保障系列规范主要规定5G网元的基线要求（数据和信息保护、可用性和完整性保护、认证和授权、会话保护、日志等）、抗攻击能力、端口扫描、漏洞扫描等的技术要求和测试方法等。

3.2 中国标准

中国5G安全标准分为行业标准和国家标准2大类，主要研究5G安全关键技术、架构和流程、虚拟化安全技术、设备安全保障等。行业标准在中国通信标准化协会（CCSA）研究制定，预计在2020年完成大部分标准；国家标准在国家标准化管理委员会制定，正在陆续立项。

目前正在研究制定的中国标准如下：

- 5G移动通信网安全技术要求（2018-2367T-YD）；
- NFV安全技术要求（H-2019009066）；
- 移动通信网络设备安全保障要求5G基站（gNB）（H-2019008972）；
- 5G移动通信网络设备安全保障要求核心网网络功能（H-2018008666）；
- NFV环境下移动通信核心网安全需求研究（B-2018008682）；
- 5G网络切片安全技术要求（B-2017006541）；
- 5G边缘计算安全技术研究（B-2019008981）。

目前正立项的国家标准如下：

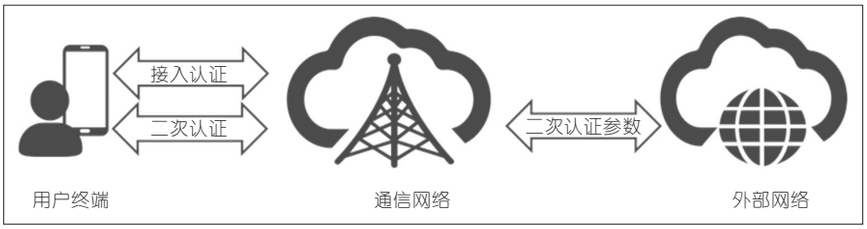
- 5G移动通信网通信安全技术要求（G-2019009101）；
- 5G移动通信网络设备安全保障要求核心网网络功能（G-2019009031）；
- 5G移动通信网络设备安全保障要求5G基站（G-2019009031）。

以上行业和国家标准的主要内容基本与对应的国际标准一致，旨在指导5G移动通信网络设备的研发，并为运营商和监管机构在5G安全方面开展工作提供技术参考。

4 结束语

在当前5G发展的关键时期，中国应进一步加快5G技术创新，提升产业竞争优势，打造5G精品网络，构建新型基础设施，坚持5G产品全球化路线，继续推动5G产业快速发展。同时，为了应对5G面临的安全风险和挑战，应进一步加强国际交流合作，提升中国在5G安全领域的话语权；加大5G安全研发投入，突破5G安全关键技术研究，提升中国5G网络和设备的安全性可靠性；加强5G与垂直行业的融合创新研究，构建支撑行业发展的具有灵活高效安全属性的5G网络，并积极推动5G安全的全球标准以及后续产业

➡下转第18页



▲图 9 二次认证的示意图

一、对不同接入场景的统一，以及对认证框架的统一。正是有了这些不同角度和层面的统一，使得 5G 网络可以为各种不同类型的终端提供安全的认证机制和流程，并为后续安全保护打下了坚实的基础。

但同时我们也要看到，5G 的认证仍然面临着诸多挑战，例如学术界通过形式化分析方法对 5G 认证机制进行评估[4-5]，发现了一些潜在的风险点并促使网络协议改进。在通信网络的演进过程中，考虑网络的后向兼容性，无线通信系统始终坚持以对称密钥作为认证的基础，并因此衍生出一系列的安全参数。因此，基于对称密钥的信任状是整个网络认证和后续安全保障的基础。但对于 5G 及后续的网络，需要考虑更多的应用场景，并需要与垂直行业做更深入的结合。这些条件下，可能产生新形态的信任状需求。因此，如何做到不同形态的信任状的统一，将会是后续认证演进的考虑方向。此外，对于轻量级的物联网应用，如何充分发挥无线通信网络已有的安全优势，实现通信网络和业务之间认证的统一，降低物联网终端的能耗，提升安全保障效率，也是目前 5G 标准正在研究制定的内容之一。

参考文献
[1] 胡鑫鑫,刘彩霞,刘树新,等. 移动通信网鉴权认证综述[J]. 网络与信息安全学报, 2018, 4(12): 1–15
[2] 3GPP. 3G Security; Security Architecture: 3GPP TS33.102[S]. 2013
[3] 栗栗,彭晋,齐晏鹏,等.移动通信网中的密码算法演进之三——认证篇[EB/OL].[2019–05–20]. https://mp.weixin.qq.com/s/SoA1bY4AZtbGbUKmU_X17Q
[4] BASIN D, DREIER J, HIRSCHI L, et al. A Formal Analysis of 5G Authentication[J].2018, (2):22–25.DOI:10.1145/3243734.3243846
[5] BASIN D, DREIER, HIRSCHI J, RADOMIROVIC L, S, et al. A Formal Analysis of 5G Authentication[C] //25th ACM Conference on Computer and Communications Security. USA: ACM, 2018: 1383–1396. DOI: 10.1145/3243734.3243846

作 者 简 介

齐晏鹏，中国移动通信研究院安全所项目经理、中国移动 3GPP 安全与隐私小组代表等；长期从事 LTE、5G 等基础网络通信安全研究，并参与物联网、车联网等系统安全设计工作，目前主要负责 5G 系统安全架构与协议研究；申请并获得授权专利 10 余项，发表 10 余篇论文。

彭晋，中国移动通信研究院安全所所长，曾担任 ITU–T SG13 报告人、3GPP SA1 UDC 子组主席等；研究方向为电信核心网、电信网安全、云计算安全、大数据安全等；曾负责多项国家科研项目，并参与 ITU–T、3GPP、GSMA 等国际标准工作。

⬅上接第 5 页

发展，实现 5G 技术发展与技术安全相统一。

参考文献
[1] 3GPP. Security architecture and Procedures for 5G System (Release 15): 3GPP TS 33.501 [S]. 2019
[2] 3GPP. 3GPP System Architecture Evolution (SAE); Security Architecture: 3GPP TS 33.401 [S]. 2012
[3] 3GPP. Catalogue of General Security Assurance Requirements: 3GPP TS 33.117[S]. 2017
[4] 3GPP. 5G Security Assurance Specification (SCAS); NR Node B (gNB): 3GPP TS 33.511[S]. 2019
[5] 3GPP. 5G Security Assurance Specification (SCAS); Access and Mobility Management Function (AMF): 3GPP TS 33.512[S]. 2018
[6] 3GPP. 5G Security Assurance Specification (SCAS); User Plane Function (UPF): 3GPP TS 33.513[S]. 2018
[7] 3GPP. 5G Security Assurance Specification (SCAS) for the Unified Data Management (UDM) Network Product Class: 3GPP TS 33.514[S]. 2018
[8] 3GPP. 5G Security Assurance Specification (SCAS); Session Management Function (SMF): 3GPP TS 33.515[S]. 2018
[9] 3GPP. 5G Security Assurance Specification (SCAS); Authentication Server Function (AUSF): 3GPP TS 33.516[S]. 2017
[10] 3GPP. 5G Security Assurance Specification (SCAS) for the Security Edge Protection Proxy (SEPP) Network Product Class: 3GPP TS 33.517[S]. 2018
[11] 3GPP. 5G Security Assurance Specification (SCAS) for the Network Repository Function (NRF) network product class: 3GPP TS 33.518 [S]. 2018
[12] 3GPP. 5G Security Assurance Specification (SCAS) for the Network Exposure Function (NEF) Network Product Class: 3GPP TS 33.519[S]. 2018

作 者 简 介

杨红梅，中国信息通信研究院主任工程师、CCSA TC5 WG12 副组长；主要研究领域为移动通信 3G、4G、5G 核心网及安全；负责并完成 4 项国家重大专项课题，牵头制定了移动通信核心网和安全领域多项行业标准，多次获得 CCSA 科学技术奖；发表文章 30 余篇，主编专著《演进分组系统（EPS）业务应用技术》。

赵勇，中国电信股份有限公司北京分公司高级工程师；研究领域为移动通信核心网及业务；牵头负责并完成了多个业务平台的云化工作；发表文章 10 余篇。