5G网安全部署探讨

Study on 5G Network Security Deployment

高　枫，马　铮，张曼君，张小梅，丁　攀（中国联通网络技术研究院，北京，100048）
Gao Feng，Ma Zheng，Zhang Manjun，Zhang Xiaomei，Ding Pan（China Unicom Network Technology Research Institute，Beijing 100048，China）

摘　要：
多样化的场景、接入方式以及新型网络架构，给5G网络安全带来了新的需求和挑战。从5G网络的安全威胁分析入手，分析了NFV、SDN、云计算、网络切片、异构接入的安全需求，提出了接入安全域、核心安全域、业务安全域与管理安全域的安全部署策略，对5G网络安全部署架构进行了探讨。

关键词：
5G网络；部署；安全
doi：10.12045/j.issn.1007-3043.2019.04.010
中图分类号：TN915.08
文献标识码：A
文章编号：1007-3043（2019）04-0045-04

Abstract：
Diversified scenarios，diversified access modes and new network architecture bring new demands and challenges to 5G network security. Starting from the security threat analysis for 5G network，the security requirements of NFV，SDN，cloud computing，network slicing and heterogeneous access are analyzed. The security deployment strategies of access security domain，core security domain，business security domain and management security domain are proposed. The security deployment architecture of 5G network is discussed.

Keywords：
5G network；Deployment；Security

引用格式：高枫，马铮，张曼君，等. 5G网安全部署探讨[J]. 邮电设计技术，2019(4)：45-48.

0 前言

当前，全球5G网络部署的步伐不断加速，国内运营商积极开展5G内外场功能验证和规模组网试验。5G技术发展演进，5G移动技术与IT技术不断融合，带来了网络架构的变革，使得网络能够灵活地支撑多种应用场景。网络架构的演进及业务的创新，为5G网络安全带来了新的需求和挑战。

从5G网络的安全威胁分析入手，分析5G网络安全需求，在此基础上对5G网络安全部署进行探讨。

收稿日期：2019-03-20

1 5G网络安全威胁分析

1.1 5G网络基础设施

1.1.1 NFV

NFV的引入使5G网络具有网元功能软件化、资源共享、部署集中化的特点，这些特点导致传统网络安全发生了变化。网元功能软件化使传统硬件网元设备物理边界消失，软件安全问题突出；计算、存储及网络资源共享化，把虚拟机安全、虚拟化软件安全和数据安全等问题引入移动网络；部署集中化使病毒传播速度加快，此外，攻击者可能利用通用硬件漏洞发起攻击。

1.1.2 SDN

SDN使设备的控制面和数据面解耦，控制面实现集中控制，开放可编程接口供应用层使用，实现了灵活的定义网络。

集中控制使安全威胁由转发面转移到控制面，控制器安全风险增大，一旦控制器受到攻击，整个SDN网络都会受到影响，甚至瘫痪。采用标准化的接口和统一的协议，更容易被攻击者利用进而发起攻击；应用层开放可编程的特性加大了攻击者通过软件进行攻击的风险。

SDN安全威胁主要来源于应用层、控制层、数据层以及南向和北向接口，如图1所示。

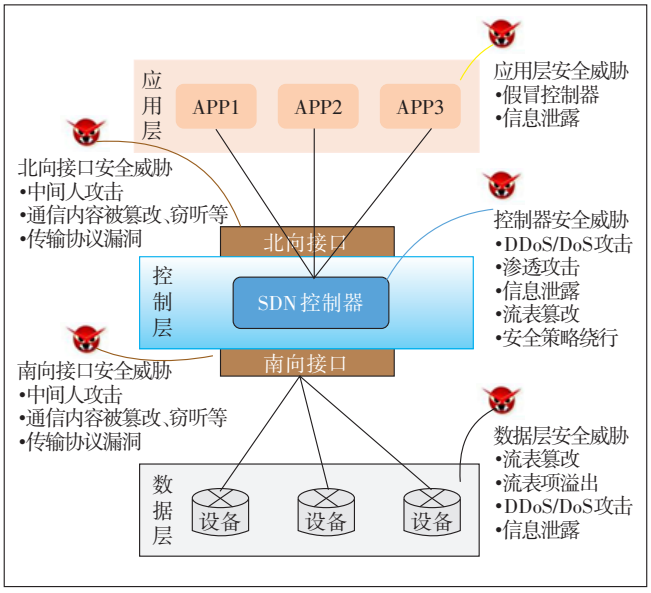

图1　SDN安全威胁

1.1.3 云计算

5G网络应用云计算技术，面临的安全威胁包括：

a）传统安全问题。虚拟化软件同样面临传统网络安全问题，如访问控制、安全隔离、操作系统/应用程序的漏洞攻击、防病毒/恶意代码等。

b）虚拟化引入新的安全问题。虚拟化技术的引入带来了新的攻击面，如虚拟化软件VM、虚拟化管理软件VMM等；由于传统安全设备对虚拟化网络流量不可见，虚拟化网络流量安全问题可能存在；用户对其本身的数据控制能力减弱，数据及隐私安全保护要求提高。

1.2 网络切片

在5G网络中引入网络切片技术，可实现灵活的资源编排和调度，为不同业务类型提供差异化的服务能力。网络切片面临的安全威胁主要包括：

a）UE访问未经授权的网络切片。

b）网络切片密码泄漏，导致攻击者获取其他网络切片的数据。

c）越权进行网络切片运维。

d）非法占用资源影响其他网络切片，导致资源过度消耗的DDoS攻击。

e）当1个终端同时用2个切片时，攻击者从1个切片获取另1个切片信息等。

1.3 异构接入网络

5G网络兼容多种异构接入方式，包括3GPP接入和非3GPP接入，异构接入网络带来的安全威胁包括：

a）接入性能问题。不同的接入技术可能使用不同的认证机制，如WLAN、蜂窝、D2D的认证机制各不相同。使用不同认证机制的终端接入网络后，核心网需对不同认证机制采取不同的安全信息管理（如认证信息），由此产生的资源开销，将影响终端接入网络的性能。

b）不同接入网络间切换时的安全性问题。终端在不同的接入网之间进行切换，不同网络的认证机制、安全等级可能不同。攻击者如从较低安全等级的网络接入后，切换至较高安全等级的网络，则可能获取到不应获得的敏感信息。

2 5G网络安全需求分析

2.1 网络基础设施安全

2.1.1 NFV

NFV的安全需求主要包括：

a）VNF安全。VNF软件包安全管理；访问控制，敏感数据保护。

b）NFVI安全。保障虚拟机及其管理器安全。

c）NFV网络安全需求。通信双方相互认证，对通信内容进行保护；边界防护、安全域划分及流量隔离等。

d）MANO安全需求。MANO实体安全加固，防止敏感信息泄露；安装防病毒软件；实体间双向认证，保护通信内容；严格配置MANO系统账号与管理权限。

2.1.2 SDN

SDN的安全需求主要包括：

a）应用层的安全需求。APP对控制器身份进行认证；APP和控制器之间的通信保护；APP自身安全加固。

b）控制器的安全需求。具备DDoS/DoS防护能力；服务器安全加固，满足安全服务最小化原则；执行策略冲突检测和防止机制；对接入的APP进行身份认证和权限检查。

c）转发层的安全需求。满足安全服务最小化原则；具备限速功能。

d）南北向接口的安全需求。双向认证；对通信内容进行机密性、完整性和防重放保护；对协议强壮性进行分析和测试，并修复漏洞。

2.1.3 云计算

a）虚拟机安全需求。病毒/恶意软件入侵防护；虚拟机之间隔离；虚拟机之间通信安全，迁移安全，镜像存储安全；虚拟机访问控制等。

b）虚拟机管理器（VMM）安全需求。代码可靠性；病毒入侵防护，防止非法访问；安全配置和管理等。

c）虚拟化网络安全。结合虚拟化后的网络拓扑，重建网络安全域；判断虚机之间的流量通信是否符合安全策略，判断是否存在网络攻击；虚拟机网络始化时实现网络安全策略的自动部署，虚拟机迁移时，保证迁移前后网络安全配置环境一致。

2.2 网络切片安全

网络切片安全需求主要包括：

a）网络资源隔离，不同切片采用不同密钥。

b）切片ID验证，避免未经授权的切片访问。

c）不同切片使用不同Key加密传输，防止Key泄露引发的切片攻击。

d）BSS/OSS系统和切片管理系统分离，切片运维权限受控。

e）运维审计，操作可追溯。

f）对合法用户异常行为进行抑制，限制接入，强制下线。

2.3 异构接入安全

a）统一认证机制。5G网络兼容多种异构接入方式，包括3GPP接入和非3GPP接入，因此，5G网络需构建兼容多种认证机制的统一认证框架。

b）安全互操作。终端可能在异构网络间进行切换，需保证异构网络间切换的安全互操作，如安全上下文的传递、密钥的更新、安全上下文的隔离等。

3 5G网络安全目标及部署

3.1 总体目标

5G网络安全总体目标包括：

a）保障通信及数据安全。提供机密性及完整性保护；提供增强的隐私保护，保护用户隐私。

b）保障异构接入安全。提供统一认证框架，支持多种接入方式和接入凭证，保障终端设备安全接入网络。

c）保障新型网络架构安全。提供SDN/NFV安全机制；提供网络切片安全机制。

d）支持差异化安全。提供按需的安全保护，满足多种应用场景的差异化安全需求。

e）开放安全能力，保障能力开放安全。支持数字身份管理、认证能力等的安全能力开放；提供全面的安全机制。

3.2 安全部署架构

如图2所示，5G网络安全部署架构划分为接入安全域、核心安全域、业务安全域与管理安全域。

3.2.1 接入安全域

由于该域处于用户侧网络环境之中，为保障网络和业务的安全性，应重点保证用户鉴权功能的可用性，对用户数据和信令进行保护。

3.2.2 核心安全域

该域需要与内外部业务平台对接，因此要做好入侵检测、攻击防御、数据保护等工作，同时针对该域的云化、软件化特性也需要对集中控制器、南北向接口等进行重点防护。

考虑非安全区域小基站通过安全网关接入核心网域，安全网关在核心网域进行部署，与基站之间通过双向认证后建立并管理IPSec隧道，通过该安全隧道，为无线侧与核心网之间控制面信令、用户面数据提供完整性和机密性保障，从而实现安全接入。

3.2.3 业务安全域

该域包括能力开放平台、自营及第三方业务平台等，因此既要防护网络侧对业务的攻击和滥用，也要防止利用平台和应用对网络发起的攻击。

在该域各类平台中部署病毒防护、漏洞扫描等软硬件，并对相关业务操作进行认证、授权及审计。同时，通过核心网域的防火墙与核心网域实现对接，有效进行安全隔离和访问控制。

3.2.4 管理安全域

管理安全域主要包括运营系统，其防护策略与平台类防护类似，在该域各类平台中部署病毒防护、漏洞扫描等软硬件，并对相关操作进行认证、授权及审计。

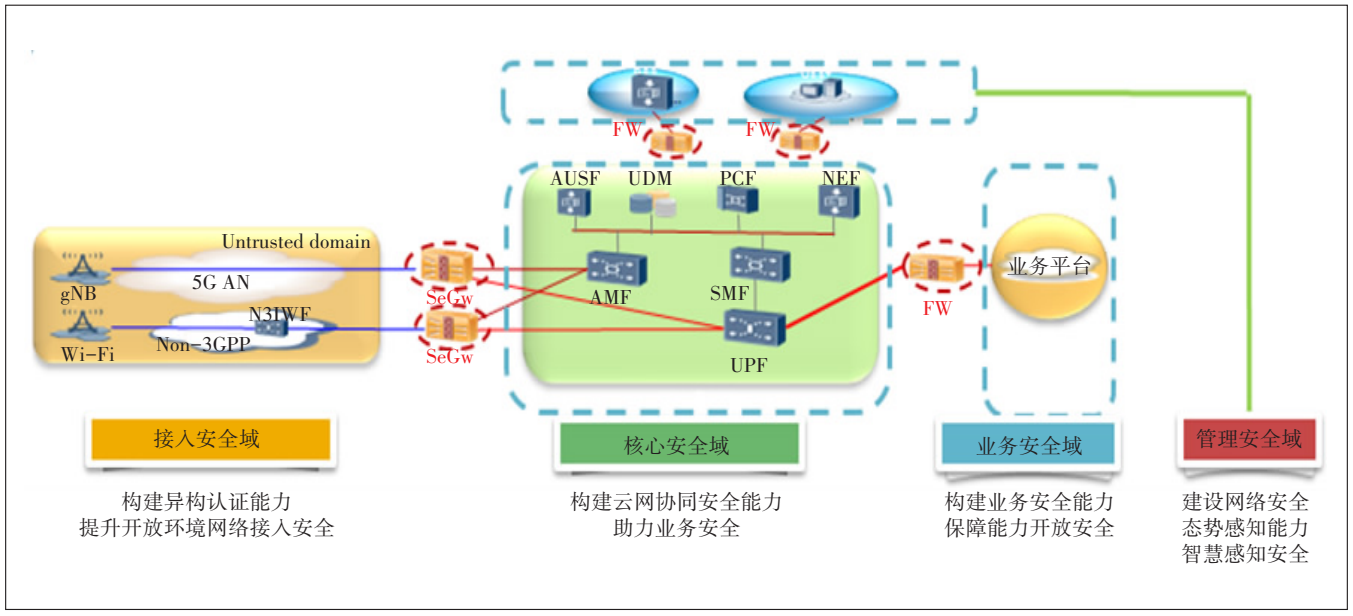

图2　5G网络安全部署架构

4 结束语

多样化的场景、接入方式以及新型网络架构，使5G网络除满足基本通信安全外，也能为不同业务场景提供差异化安全服务，适应新型网络架构及创新业务模式。本文研究分析了5G网络面临的主要安全威胁，分析了NFV、SDN、云计算、网络切片、异构接入的安全需求，在此基础上，提出了接入安全域、核心安全域、业务安全域与管理安全域的安全部署策略，对5G网络安全部署架构进行了探讨。

参考文献：

[1] IMT-2020. 5G网络安全需求与架构(白皮书)[R/OL].[2019-01-13]. http://www. txrjy. com / forum. php? mod=viewthread&tid=966155&highlight=.

[2] Overview of 5G security technology[J]. Science China(Information Sciences),2018,61(8):107-131.

[3] 王全方，琰崴. 5G电信云网络安全解决方案[J]. 邮电设计技术. 2018(11).

[4] 李宏佳，王利明，徐震，等. 5G安全：通信与计算融合演进中的需求分析与架构设计[J]. 信息安全学报，2018(9).

[5] 杜滢，朱浩，杨红梅，等. 5G移动通信技术标准综述[J]. 电信科学，2018(8):2-9.

[6] 尤肖虎，潘志文，高西奇，等. 5G移动通信发展趋势与若干关键技术[J]. 中国科学：信息科学，2014，44(5):551-563.

[7] 3GPP. Study on Architecture for Next Generation System: 3GPP TR 23.799[S/OL]. [2019-01-13]. https://portal.3gpp.org.

[8] 3GPP. System architecture for the 5G System; Stage 2: 3GPP TS 23.501[S/OL]. [2019-01-13]. https://portal.3gpp.org.

[9] 3GPP. Study on the security aspects of the next generation system: 3GPP TR 33.899[S/OL]. [2019-01-13]. https://portal.3gpp.org.

[10] 3GPP. Security architecture and procedures for 5G system: 3GPP TS 33.501[S/OL]. [2019-01-13]. https://portal.3gpp.org.

[11] 3GPP. Study on Enhancement of Network Slicing: 3GPP TR 23.740 [S/OL]. [2019-01-13]. https://portal.3gpp.org.

[12] 3GPP. Study on security aspects of 5G network slicing management: 3GPP TR 33.811[S/OL]. [2019-01-13]. https://portal.3gpp.org.

[13] 3GPP. Study on security aspects of network slicing enhancement: 3GPP TR 33.813[S/OL]. [2019-01-13]. https://portal.3gpp.org.

[14] 3GPP. Architecture enhancements for service capability exposure: 3GPP TR 23.708[S/OL]. [2019-01-13]. https://portal.3gpp.org.

[15] 3GPP. Study on evolution of cellular IoT security for the 5G System: 3GPP TR 33.861TR 33.861 [S / OL]. [2019-01-13]. https://portal.3gpp.org.

[16] 3GPP. Study on security aspects of the 5G Service Based Architecture: 3GPP TR 23.742[S/OL]. https://portal.3gpp.org.

[17] 黄开枝，金梁，赵华. 5G安全威胁及防护技术研究[J]. 邮电设计技术. 2015(6).

[18] GUAN J, WEI Z, YOU I . GRBC-based Network Security Functions placement scheme in SDS for 5G security[J]. Journal of Network and Computer Applications, 2018.

作者简介：
高枫，高级工程师，主要研究方向为移动通信网安全；马铮，高级工程师，主要研究方向为移动通信网安全、移动互联网安全相关领域；张曼君，高级工程师，博士，主要从事网络安全技术相关研究工作；张小梅，工程师，主要从事网络安全技术相关研究工作；丁攀，助理工程师，主要从事网络安全技术相关研究工作。