从架构看边缘计算安全

2019-03-28 09:04

目前5G研究正在业界如火如荼的开展。5G网络通过对增强移动带宽、低时延高可靠、大规模MTC终端连接三大场景的支持，来满足用户的高带宽、低时延和大连接业务的需求。边缘计算的靠近用户、业务本地处理、灵活路由等特点，成为满足5G业务需求的重要技术，所以5G架构在设计时就支持边缘计算。随着5G技术的研究，边缘技术受到业界的高度重视。本文在介绍边缘计算概念的基础上，重点分析了边缘计算的安全威胁、安全防护框架，并给出了后续工作重点。

1

边缘计算的概念

边缘计算技术主要是指通过在靠近网络接入侧部署通用服务器，从而为网络提供IT和云计算的能力，强调靠近用户。5G的三大关键场景[1]促进了边缘计算的发展：

增强移动带宽(eMBB)的高带宽，给核心网带来更大数据流量的冲击，负责用户数据转发的网关成为网络吞吐率的瓶颈，需要边缘计算提供的本地分流、灵活路由等，有效减缓核心网的数据传输压力。
低时延高可靠(uRLLC)的时延限制，需要边缘计算提供的本地业务处理、内容加速等技术。

大规模MTC终端连接(mMTC)存在很多资源受限的物联网终端，无法实现高能耗的计算、存储等，需要边缘计算为物联网终端近距离提供计算、存储能力。在5G架构设计[2]中，通过支持用户面数据网关的下沉部署、灵活分流等，实现对边缘计算的支持。同时，网络的位置服务、带宽管理等可以包装成能力，通过能力开放提供给边缘计算的应用，从而优化业务应用，开发新商业模式，进一步促进网络和业务的深度融合。

边缘计算的价值包括：

利用靠近用户的便于计算环境，为低成本物联网终端以及边缘计算应用提供就近计算、存储等能力，满足低时延业务需求；

基于MEC平台，将网络能力以可管可控的方式开放给MEC应用，促进业务发展，提升网络价值和智能化水平；

通过将业务卸载到MEC平台本地处理，大大缓解了核心网数据传输和处理压力。

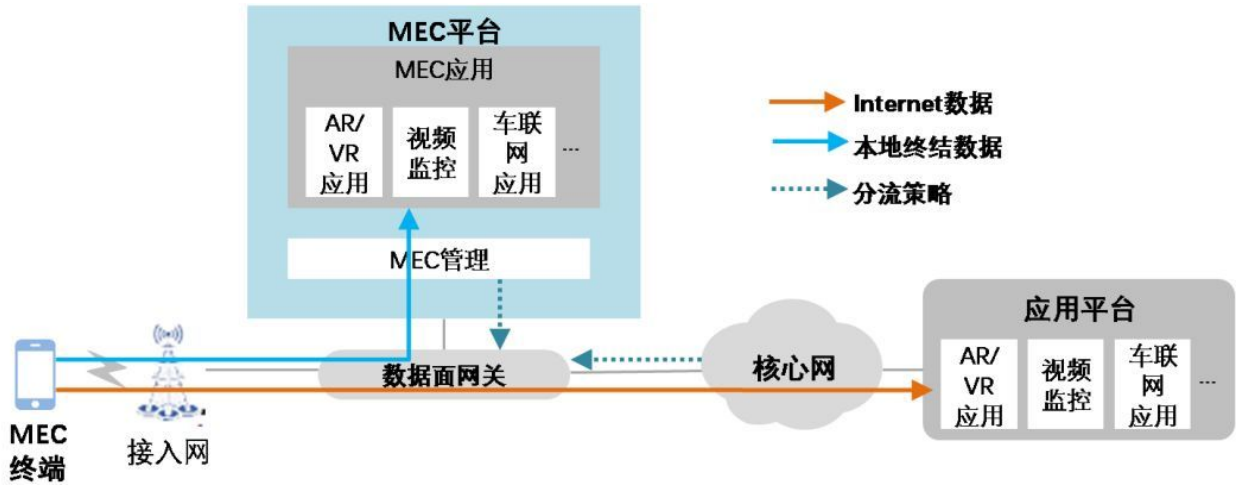

图1 部署MEC后的数据流

欧洲电信标准化协会（European Telecommunication Standard Institute, ETSI）已于2014年9月成立了MEC（Mobile Edge Computing, MEC）工作组，针对MEC技术的服务场景、技术要求、框架以及参考架构（如下图2）[3]等开展深入研究。2016年，ETSI把此概念扩展为多接入边缘计算(Multi-Access Edge Computing)，将边缘计算能力从电信蜂窝网络进一步延伸至其它无线接入网络（如Wi-Fi）。

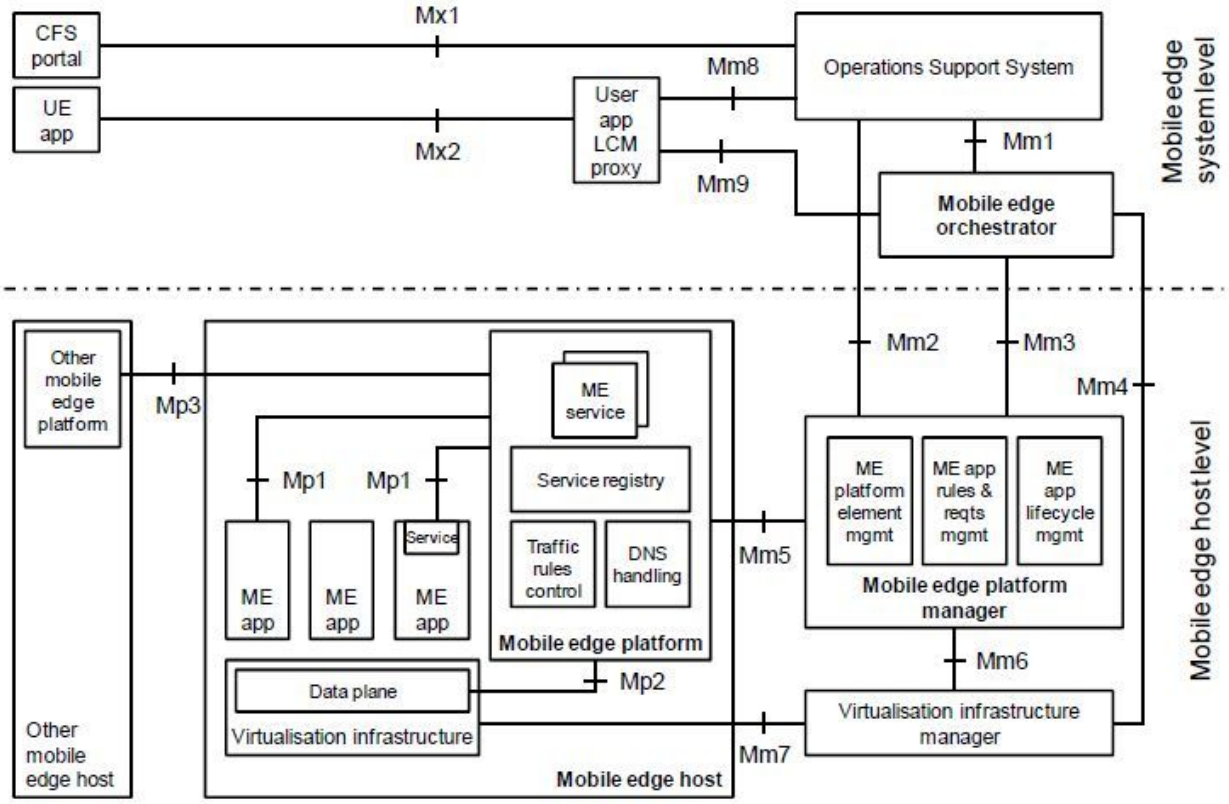

图2 ETSI MEC参考架构

MEC参考架构与ETSI的NFV(Network Function Virtualization)架构[4]很类似。由物理基础设施（Mobile edge host）和虚拟化基础设施(Virtualization infrastructure)为ME app和MEC平台(Mobile edge platform)提供计算、存储和网络资源，由MEC平台实现ME app的发现、通知以及为ME app提供路由选择等管理，由虚拟化基础设施管理提供对虚拟化基础设施的管理，由移动边缘计算平台管理(Mobile edge platform manager)提供对移动边缘计算平台的管理，由移动边缘编排器(Mobile edge orchestrator)提供对ME app的编排。ETSI在2017年2月发布了在NFV环境中如何部署MEC架构[5]，使得MEC在移动网络中的落地变得更加容易。此部署场景中，ME App和移动边缘计算平台MEP均为VNF部署在NFV基础设施上。

边缘计算目前已成为一个业界关注的技术，除了MEC，在产业界不同组织，也提出了不同的边缘计算定义。如ECC (Edge Computing Consortium)定义边缘计算是在靠近物或数据源头的网络边缘侧，融合网络、计算、存储、应用核心能力的开放平台。雾计算将计算、通信、控制和存储资源与服务分布给用户或靠近用户的设备与系统，是云计算概念的自然延伸和扩展[6]，可以认为是另外一种形式的MEC。可见，标准和产业界的边缘计算概念均具备靠近网络边缘、业务本地化处理等特点，从而更好的为用户提供移动视频QoS优化、移动CDN下沉、VR直播、增强现实(AR)、视频监控与智能分析、V2X应用、工业控制等业务。目前业界边缘计算标准还在制定中，边缘计算平台以及业务的部署处于试点阶段。

2

边缘计算的安全威胁

对于运营商的网络，一般认为核心网机房处于相对封闭的环境，受运营商控制，安全性有一定保证。而接入网相对更易被用户接触，处于不安全的环境。边缘计算的本地业务处理特性，使得数据在核心网之外终结，运营商的控制力减弱，攻击者可能通过边缘计算平台或的应用攻击核心网，造成敏感数据泄露、(D)DOS攻击等。所以，边缘计算安全成为边缘计算建设必须要重点考虑的关键问题。根据ETSI的MEC架构，边缘计算的安全威胁重点应考虑：

基础设施的物理安全威胁，虚拟化软件及操作系统的漏洞被攻击者利用等。
MEC平台存在木马、病毒攻击，恶意ME app对MEC平台的非授权访问、(D)DoS攻击，以及MEC平台与ME app等之间传输的数据被篡改、拦截和重放等。

ME app存在木马、病毒攻击；恶意用户或恶意ME app可非法访问ME app，导致敏感数据泄露、(D)DoS攻击等； ME app与MEC平台等之间传输的数据被篡改、拦截和重放等。

MEC编排和管理系统：其网元存在木马、病毒攻击；编排和管理网元的相关接口上传输的数据被篡改、拦截和重放等；大量恶意终端通过终端上的UE app不断发起UE应用加载请求，可能对编排网元造成(D)DoS攻击。

数据面网关存在的木马、病毒攻击；攻击者可近距离接触数据面网关，发起物理攻击；数据面网关与MEC平台等之间传输的数据被篡改、拦截和重放等。

3

边缘计算的安全防护

边缘计算安全除了考虑基础设施的安全以及管理、组网安全之外，还应考虑MEC平台安全、ME app安全、数据面网关安全以及MEC编排和管理的安全，其安全防护框架如下图。

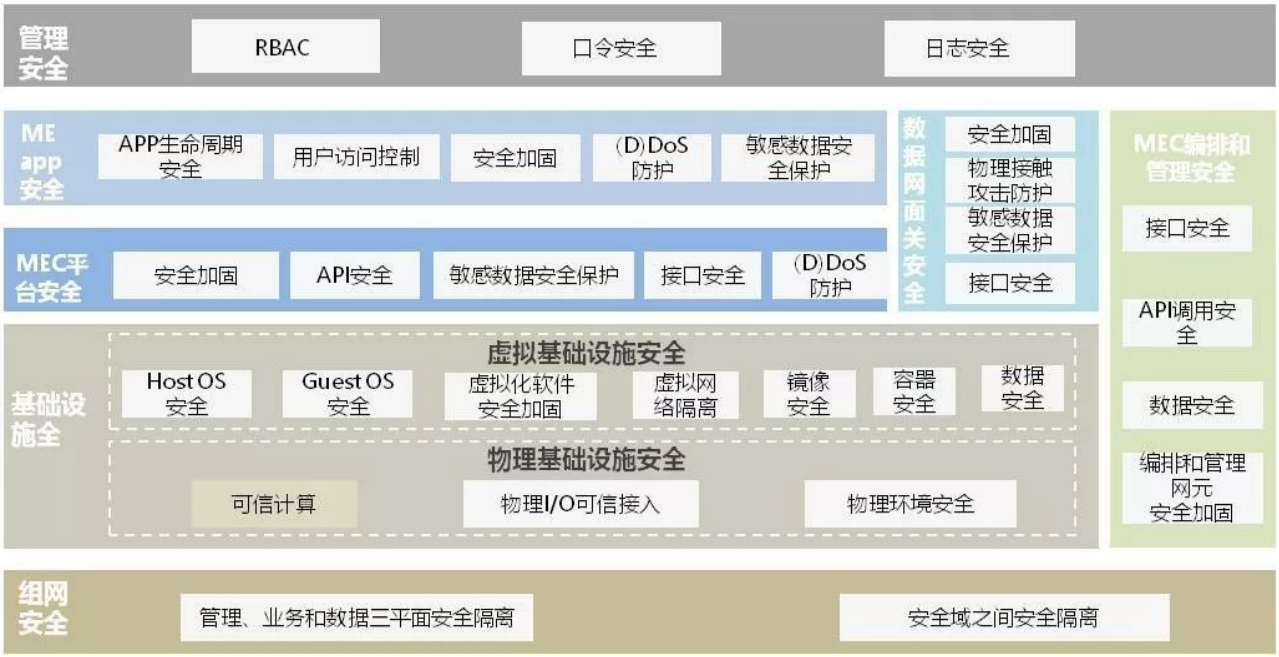

图3 边缘计算安全防护框架

边缘计算的安全防护，应该包含以下要求：

基础设施安全：在物理基础设施安全方面，应通过加锁、人员管理等保证物理环境安全，并对服务器的I/O进行访问控制。在条件允许时，可使用可信计算保证物理服务器的可信；在虚拟基础设施安全方面，应对Host OS、虚拟化软件、Guest OS进行安全加

固，防止镜像被篡改，并提供虚拟网络隔离和数据安全机制。当虚拟机中部署容器时，还应考虑容器的安全，包括容器之间的隔离，容器使用root权限的限制等。

MEC平台安全：包含接口安全、API调用安全、MEC平台自身的安全加固以及敏感数据的安全保护、(D)DoS防护，实现MEC平台与其他网元（如ME a）间的通信数据的机密性、完整性、防重放，以及MEC平台的网络信息等敏感数据的安全保护、防(D)DoS攻击等。

ME app安全：包含MEC app生命周期安全、用户访问控制、安全加固、(D)DoS防护和敏感数据安全保护，实现只有合法的ME app才能够上线，合法的用户才能够访问ME app。

数据面网关安全：包含数据面网关的安全加固、接口安全、敏感数据保护以及物理接触攻击防护，实现用户数据能够按照分流策略进行正确的转发。

MEC编排和管理安全：包含接口安全、API调用安全、数据安全和MEC编排和管理网元安全加固,实现对资源的安全编排和管理。

管理安全：与传统网络的安全管理一样，包含账号和口令的安全、授权、日志的安全等，保证只有授权的用户才能执行操作，所有操作记录日志。

组网安全：与传统的组网安全原则相同，包含三平面的安全隔离、安全域的划分和安全隔离，保证安全风险不在业务、数据和管理面之间、安全域之间扩散。

4

边缘计算安全的后续工作

目前，边缘计算还处于研究和试验阶段，对于ME app的类型、应用场景等，运营商和厂商均还在探索和试点中。本文中主要针对边缘计算架构层面进行了安全分析，并提出架构层面的安全防框架。对于具体的边缘计算应用场景的安全，还需根据应用的需求进行深入分析，包括边缘计算应用的业务安全、数据安全以及安全监控等。另外，对于有高安全要求的边缘计算应用，还应考虑如何通过能力开放，将网络的安全能力以安全服务的方式提供给边缘计算app。

参考文献

[1]3GPP TS 22.261: Service requirements for the 5G system;Stage 1

[2] 3GPP TS 23.501 V0.3.0 (2017-02) System Architecture for the 5G System; Stage 2 (Release 15)

[3] ETSI GS MEC 003 V1.1.1 (2016-03) Mobile Edge Computing (MEC); Framework and Reference Architecture

[4] ETSI GS MEC 017 V1.1.1 (2018-02) Mobile Edge Computing (MEC); Deployment of Mobile Edge Computing in an NFV environment

[5] ETSI GS NFV 002: Network Functions Virtualisation (NFV); Architectural Framework

[6] OpenFog Reference Architecture for Fog Computing, Openfog Consotium, 2017