移动边缘计算安全研究

边缘计算...
关注微信公众号：边缘计算社区

本文在介绍边缘计算概念、应用场景的基础上，分析移动边缘计算的安全威胁、安全防护框架、安全防护方案，并展望后续研究方向。目前 5G 研究正在业界如火如荼的开展。5G网络通过支持增强移动带宽、低时延高可靠、大规模 MTC 终端连接三大业务场景，满足用户高带宽、低时延和大连接业务的需求。移动边缘计算提供本地分流、灵活路由、高效计算和存储能力，成为满足5G支持三大业务场景的关键技术如下。

（1）增强移动带宽 (eMBB) 的高带宽，给核心网带来更大的数据流量冲击，负责用户数据转发的网关成为整个网络的瓶颈。移动边缘计算提供的本地分流、灵活路由等，能够有效减缓核心网的数据传输压力。

（2） 超低时延高可靠 (uRLLC) 的时延限制，对网络时延提出苛刻的要求。移动边缘计算提供的本地业务处理、内容加速等技术，明显减少数据流在核心网中的传输时间。

（3）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。移动边缘计算可为物联网终端近距离提供计算、存储能力。

在 5G 架构设计中，通过支持用户面数据网关的下沉部署、灵活分流等，实现对移动边缘计算的支持。同时， 移动边缘计算可将移动网络的位置服务、带宽管理等开放给上层应用，从而实现优化业务应用，开发新商业模式，进一步促进移动通信网络和业务的深度融合，提升网络的价值，如图 1所示。

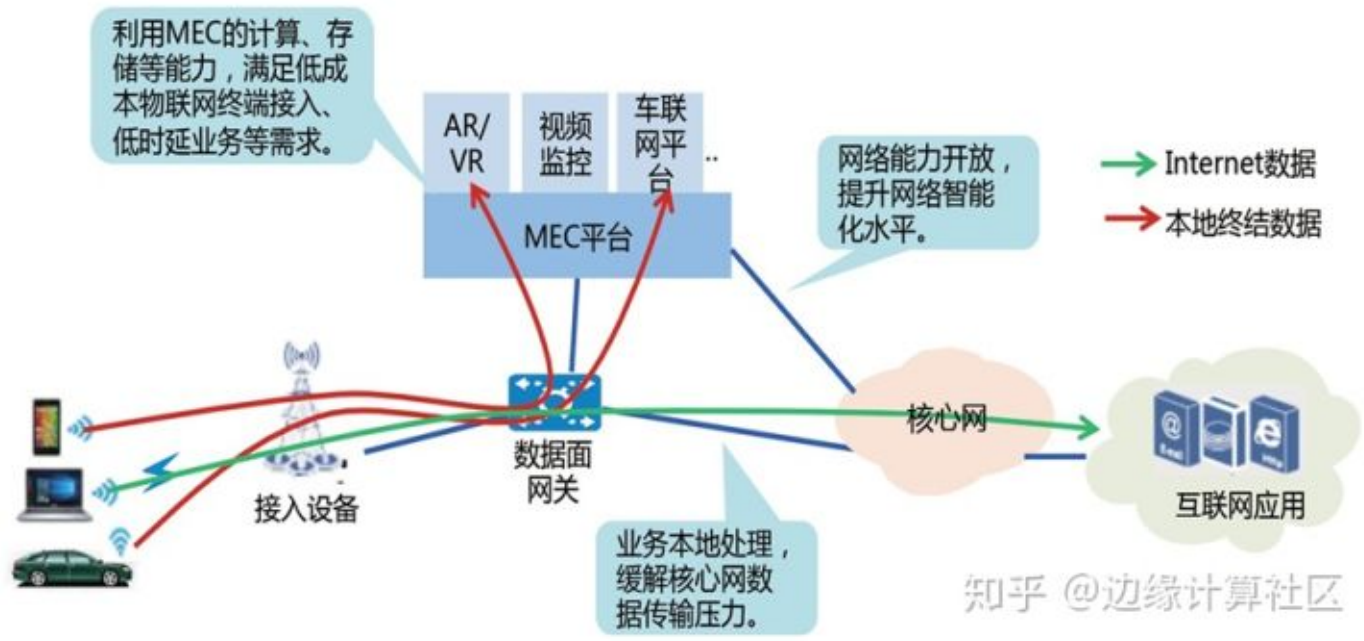

图1 边缘计算的价值

由于移动边缘计算平台和移动边缘计算应用部署在通用服务器上，并且靠近用户，处于相对不安全的物理环境、管理控制能力减弱等，导致移动边缘计算存在移动边缘计算平台和移动边缘计算应用遭受非授权访问、敏感数据泄露、(D)DoS攻击，物理设备遭受物理攻击等安全问题。因此，移动边缘计算安全成为移动边缘计算安全研究中需重点解决的问题之一。本文在介绍边缘计算概念的基础上，重点分析了移动边缘计算的安全威胁、安全防护框架及防护要求，并展望后续研究方向。

一、边缘计算概念

1.ETSIMEC 移动边缘计算

移动边缘计算由欧洲电信标准化协会（ETSI）提出，主要是指通过在靠近网络接入侧部署通用服务器，从而提供 IT 服务环境以及云计算能力，旨在进一步减少时延，提升网络运营效率、提高业务分发、传送能力，优化、改善终端用户体验。2014 年 9 月，ETSI 成立了 MEC（Mobile Edge Computing， 移动边缘计算）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（如图 2 所示）等开展深入研究。2016 年，ETSI 把此概念扩展为多接入边缘计算， 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）。

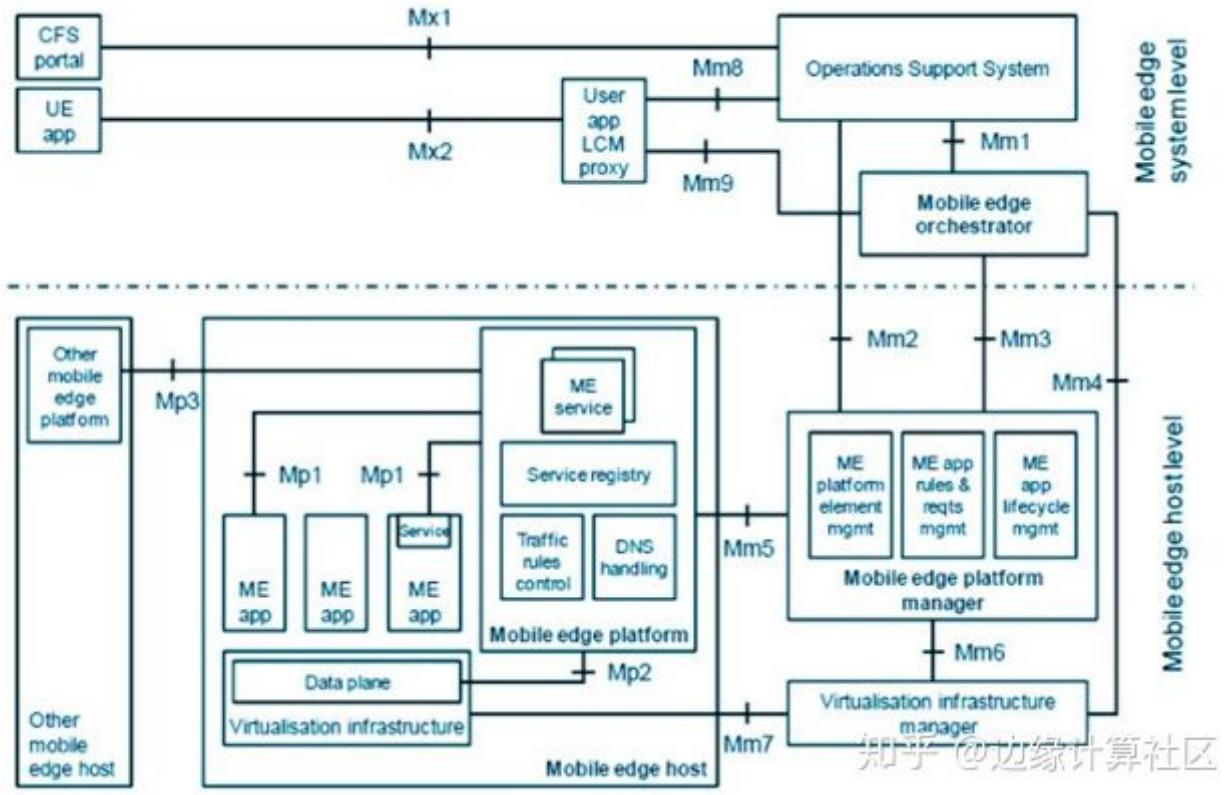

图2 MEC参考架构

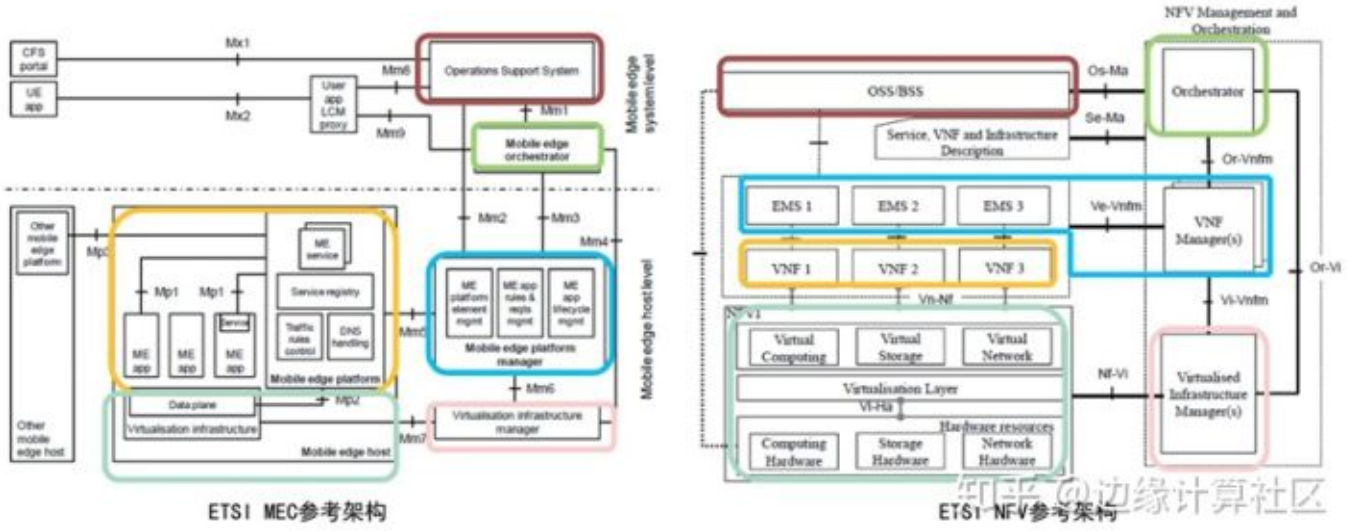

图3 MEC参考架构和NFV参考架构对比

MEC 参考架构与 ETSI 的NFV 架构很类似（如图3 所示）。由物理基础（MobileEdgeHost）和虚拟化基础设施为 ME app 和 MEC 平台提供计算、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提供对移动边缘计算平台的管理，由移动边缘编排器提供对 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，为 MEC 在移动网络中的落地提供了实施指南。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。

2.其它边缘计算

随着 5G 以及移动互联网、物联网的发展，边缘计算目前已成为一个业界高度关注的技术之一，产业界根据各自需求和现状提出了多种边缘计算的定义。如ECC(Edge ComputingConsortium) 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，并提出了边缘计算参考架构 2.0； 2011 年，思科针对物联网场景提出了雾计算的概念，将数据、处理和应用程序集中在网络边缘的设备中，而不是几乎全部保存在云中，是云计算的延伸概念。2015 年 11 月， 由 ARM、思科、戴尔、英特尔以及微软等成立了 OpenFog Consortium（ 开放雾联盟）。雾计算技术将计算、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。2017 年 2 月OpenFog Consortium 宣布发布 OpenFog 参考架构。该架构是一个旨在支持物联网、5G 和人工智能应用的数据密集型需求的通用技术框架。OpenFog 参考架构描述了 OpenFog 的八大支柱和描述架构。

以上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高带宽、低时延和大规模 MTC 终端连接业务。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技术验证阶段。本文后续将基于ETSI MEC 架构展开分析。

二、移动边缘计算应用场景

MEC 典型的应用场景可以分成本地分流、数据服务和业务优化 3 个大类。

（1）本地分流是利用 MEC 进行内容本地分流业务，提升运营商用户体验、并节省运营商传输带宽，主要包括本地视频监控、VR/AR、本地视频直播、工业控制以及边缘 CDN 等。

（2）数据服务是 MEC 应用利用通过MEC 平台提供的移动运营商网络的位置信息等进行其它业务开发，提供高价值智能服务，主要包括室内定位、车联网等。

（3）业务优化是 MEC 应用根据网络的QoS 来调整应用的发送机制，提升用户的业务体验，包括视频直播和游戏加速等。

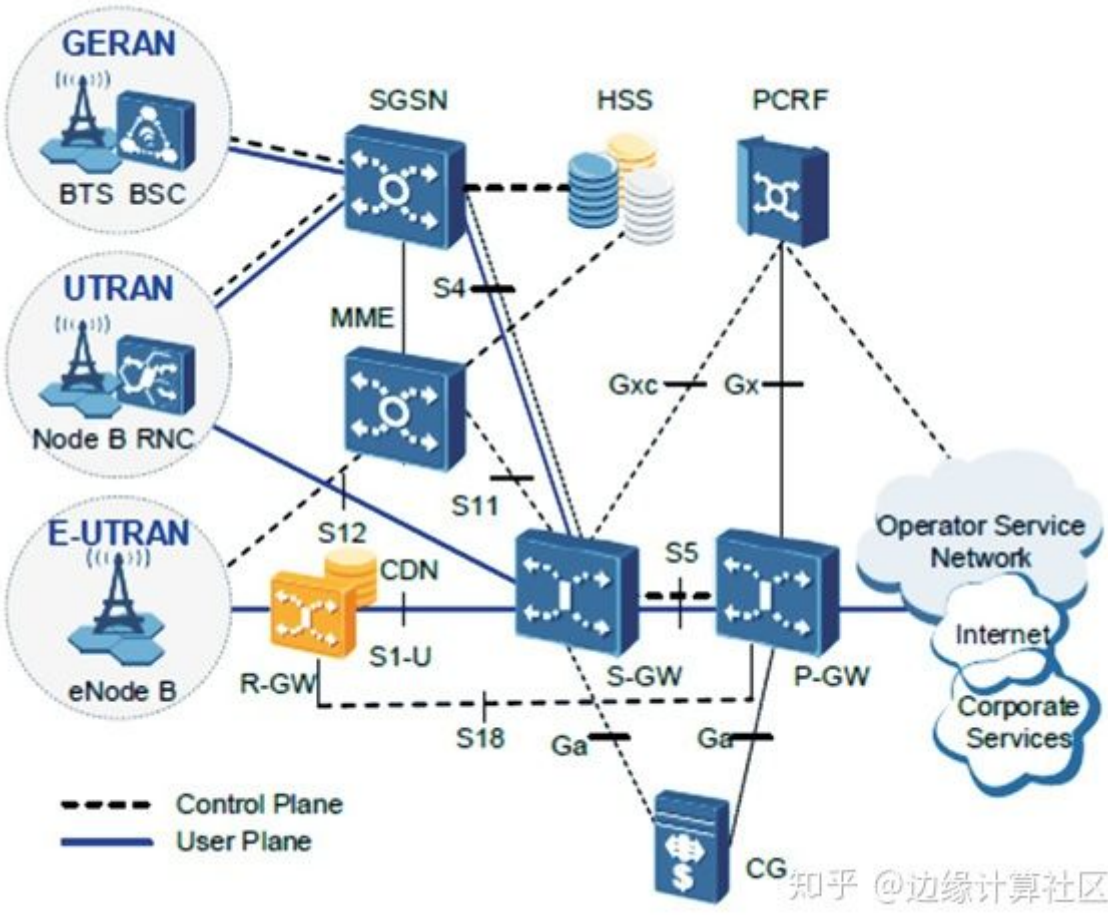

图4 网关+CDN下沉方案

图 4 描述了某运营商基于 MEC 的 CDN 下沉方案。该方案中，R-GW 充当分流网关，其分流策略可以通过手工或自动的方式进行配置。R-GW 将用户流量分流到 MEC 平台上的 CDN 应用，实现 CDN 下沉， 提供加速内容业务，从而给用户提供更好的业务体验。

三、移动边缘计算安全

1. 移动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， 其安全威胁如图 5 所示。

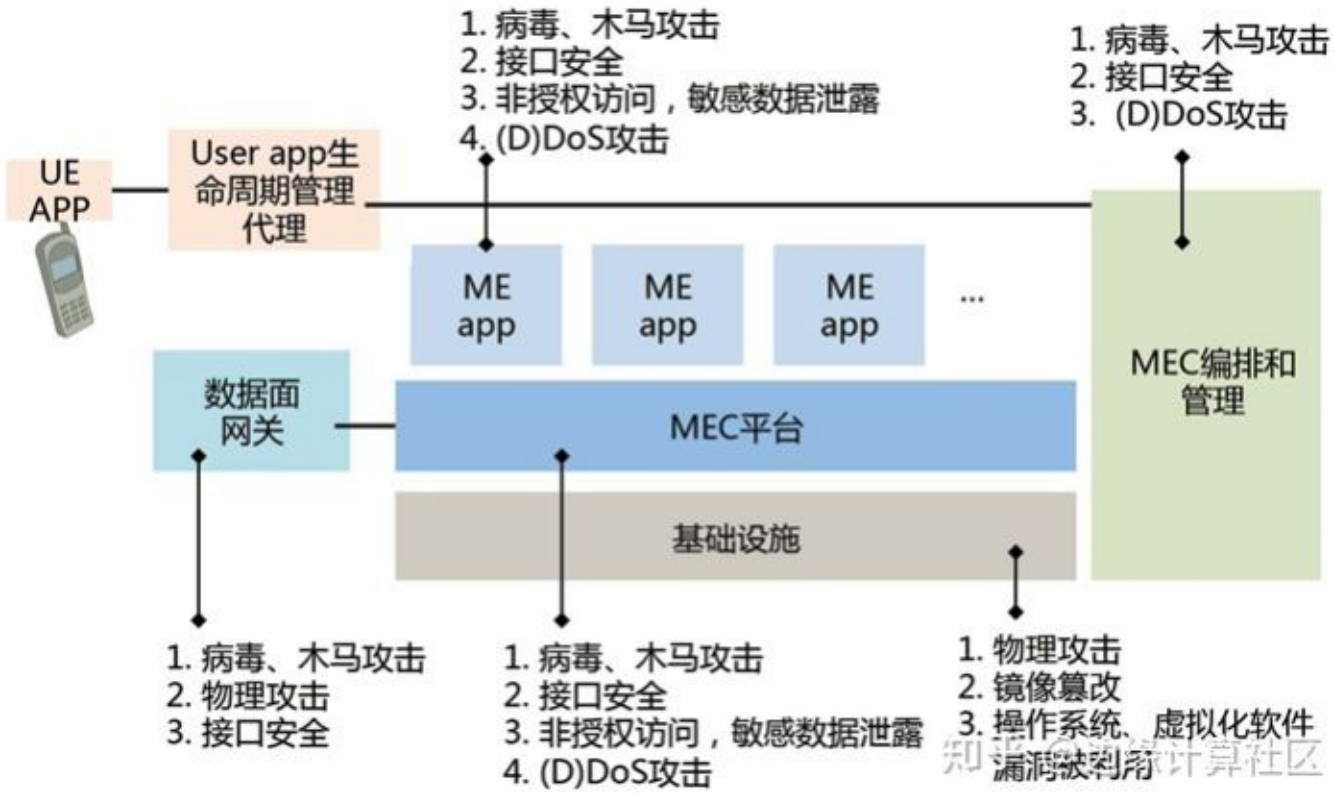

图5 边缘计算安全威胁

边缘计算的安全威胁重点应考虑如下。

（1）基础设施安全：与云计算基础设施的安全威胁类似，包括攻击者可通过近距离接触硬件基础设施，对其进行物理攻击； 攻击者可非法访问物理服务器的I/O 接口，获得敏感信息； 攻击者可篡改镜像，利用 Host OS 或虚拟化软件漏洞攻击 Host OS 或利用 Guest

OS 漏洞攻击 MEC 平台或者 ME app 所在的虚拟机或容器，从而实现对 MEC 平台和 / 或者 ME app 的攻击。

（2）MEC 平台安全： 平台存在木马、病毒攻击； MEC 平台和 ME app 等通信时， 传输数据被篡改、拦截、重放； 攻击者可通过恶意 ME app 对 MEC 平台发起非授权访问，导致敏感数据泄露或(D)DoS 攻击等； 当 MEC 平台以 VNF 或容器方式部署时，VNF 或容器的安全威胁（如 VNF 分组被篡改、镜像被篡改等）也会影响 ME app。

（3）MEapp 安全： MEapp 存在木马、 病毒攻击； MEapp 和 MEC 平台等通信时，传输数据被篡改、拦截、重放； 恶意用户或恶意 MEapp 可非法访问 ME app，导致敏感数据泄露、(D)DoS 攻击等； 当ME app 以 VNF 或容器方式部署时，VNF或容器的安全威胁（如VNF 分组被篡改、镜像被篡改等）也会影响 MEapp。另外，在 ME app 的生命周期中，ME app 可能被非法创建、删除、更新等。

（4）MEC编排和管理系统： MEC 编排和管理系统的网元（如移动边缘编排器）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； 攻击者可通过大量恶意终端上的 UE app，不断的向 User app 生命周期管理代理发送请求，实现MEC 平台上的属于该终端的 ME app 的加载加载、实例化、终止等，对 MEC 编排网元造成 (D)DoS 攻击。

（5）数据面网关安全： 存在的木马、病毒攻击； 攻击者近距离接触数据网关，获取敏感数据或篡改数据网管配置，进一步攻击核心网；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。

2.移动边缘计算的安全防护框架

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、MEapp 安全、数据面网关安全以及 MEC 编排和管理的安全，其安全防护框架如图 6 所示。移动边缘计算的安全防护，应该包含以下要求。

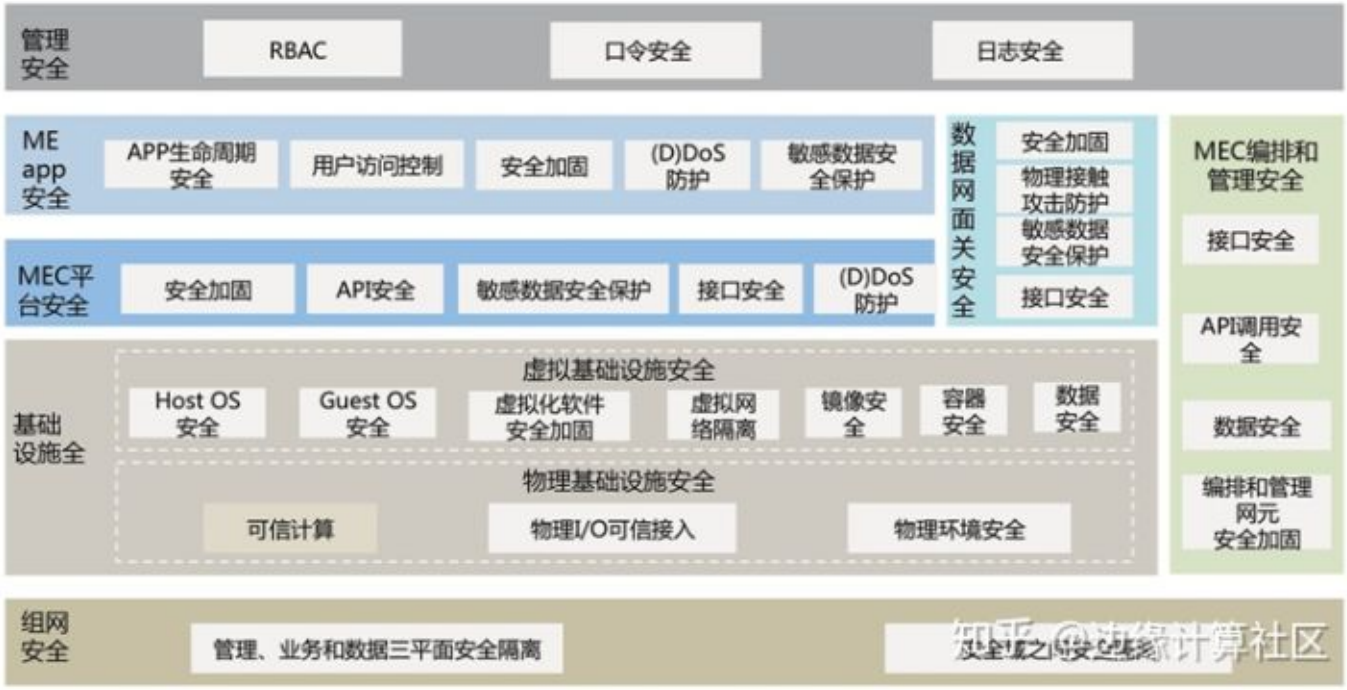

图6 边缘计算安全防护框架

（1）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。

（2） MEC 平台安全： MEC 平台与其它实体之间通信应进行相互认证，并对传输的数据进行机密性和完整性、防重放保护； 调用 MEC 平台的 API 应进行认证和授权； MEC 平台应进行安全击鼓，实现最小化原则，关闭所有不必要的端口和服务； MEC 平台的敏感数据（如用户中的位置信息、无线网络的信息等）应进行安全存储，禁止非授权访问。MEC平台还应具备 (D)DoS 防护功能等。

（3） MEapp 安全： 包含生命周期安全、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 MEapp 才能够上线，合法的用户才能够访问 MEapp。具体包括MEapp 加载、实例化以及更新、删除等生命周期管理操作应被授权后执行； 应对用户的访问进行认证和授权；MEapp 应进行安全加固； 应对 MEapp 的敏感数据进行安全的存储，防止非授权访问； MEapp 占用的虚拟资源应有限制，防止恶意移动边缘应用故意占用其它应用的虚拟化资源； MEapp 释放资源后，应对所释放的资源进行清零处理。

（4）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。具体包括数据面与 MEP 之间，数据面与交互的核心网网元之间应进行相互认证； 应对数据面与MEP 之间的接口，数据面与交互的核心网网元之间的接口上的通信内容进行机密性、完整性和防重放的保护；应对数据面上的敏感信息（如分流策略）进行安全保护； 数据面是核心网的数据转发功能网元，从核心网下沉到接入网，应防止攻击者篡改数据面网元的篡改配置数据、读取敏感信息等。

（5）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。具体包括编排和管理网元的操作系统和数据库应支持安全加固；应防止网元上的敏感数据泄漏，确保数据内容无法被未经授权的实体或个人获取 ； 编排和管理系统网元之间的通信、与其它系统之间的通信应进行相互认证，并建立安全通道；如果需远程登录移动边缘编排和管理系统网元，应使用SSHv2 等安全协议登陆进行操作维护。

（6）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。

（7）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。具体包括应该实现管理、业务和存储三平面的流量安全隔离； 在网络部署时，应通过划分不同的 VLAN 网段等实现不同安全域之间的逻辑隔离或者使用物理隔离方式实现不同安全级别的安全域之间的安全隔离，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。

四、移动边缘计算安全展望

目前，移动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，运营商以及产业界均还在探索和试点中。本文主要针对移动边缘计算概念、可能的应用场景、以及架构层面的安全威胁进行了分析，并提出架构层面的安全防护框架和安全防护要求。对于针对具体的移动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，包括移动边缘计算应用的业务安全、数据安全以及安全监控等。另外，当对于有高安全级别需求的移动边缘计算应用，运营商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移动边缘计算应用，实现在满足安全需求的同时，开发更多的商业模式，创造更多的网络价值。

作者：庄小君，杨波，王旭，彭晋

中国移动通信有限公司研究院

首发于《电信工程技术与标准化》