ZTE中兴

5G 安全白皮书

安全让 5G 走得更远

中兴通讯股份有限公司

2019 年 5 月

前　言

5G 遵循网络业务融合和按需服务的核心理念，引入了丰富的接入能力、灵活的网络架构以及更高的安全性，改变了移动网络单一的管道服务模式，为传统消费互联网提供了增强的带宽和更高的性价比，同时也为产业互联网提供了高度可定制化的网络服务以及综合信息服务平台。

垂直行业业务的多元化是产业互联网的一个显著特征。不同的安全等级要求、不同的网络架构、不同的流量特征、差异化的协议类型等，决定了难以采用统一的策略和架构来构建 5G 网络的安全架构，需要面向特定的社会、经济背景与法律框架，结合具体的业务场景进行专网定制。

产业互联网的稳定与健康发展，决定了互联网的未来。随着标准与应用的推进，5G 步入了规模商用的前夜，为了确保网络安全，让 5G 走得更远，我们需要做得更多。

目 录

content

1

第 一 部 分

构建更安全灵活的 5G 网络

1.1 产业互联网优势之选

移动通信网作为商业化的电信网络，在标准设计之初，就充分考虑了网络接入的移动性、可靠性和安全性。通过 SIM/USIM 等身份标识、认证授权、信道与承载加密、访问控制等方式，提供了良好的安全通信能力。经过包括运营商、标准组织以及设备商等在内的电信产业界几十年的锤炼，移动通信网络安全架构日臻完善，成为未来产业互联网安全通信的优势之选。

5G 网络继承了 4G 的安全特性，同时对认证授权、隐私保护、数据传输安全、网络架构和互通安全等进行了优化或增强。相对 WiFi、企业专网等非 3GPP 接入机制，5G 提供了更大范围的移动性，也为用户提供了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。

5G 提供了基于统一认证框架的双向认证能力，使终端和网络都能够确认对方身份的合法性。这样不仅能避免非法用户接入网络，也能避免利用伪基站、伪热点进行诈骗或者窃取用户信息。另外，由于对终端进行认证，可以追溯终端使用者的身份和行为轨迹，增加了攻击者的法律风险，可以有效降低攻击的概率。

5G 网络为终端提供了端到端的安全通道，使终端之间能够有效地隔离，即使某一终端被攻破，恶意程序也很难在 5G 网络中横向传播，使得攻击的扩散势头以及导致的损失得到遏制。

传统消费互联网的设计初衷是开放性，这也是导致网络安全问题频发的一个根源。未来的产业互联网将会连接金融、能源、工业、交通等重要领域的高价值资产，半封闭甚至封闭性的网络将是更好的选择。5G 网络切片不但能够为不同 SLA 的业务提供网络架构的定制，还能够提供安全的网络隔离能力。

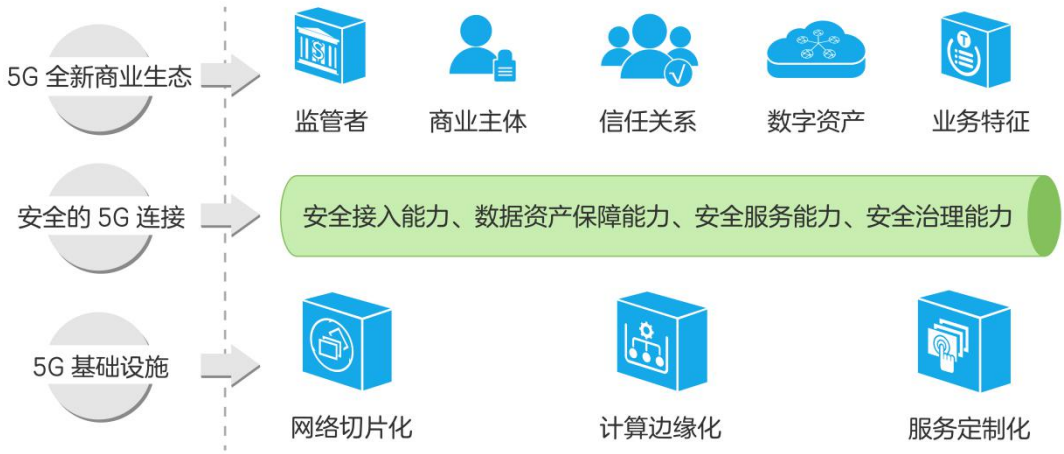
目前，3GPP 正在进一步对增强的基于服务的架构安全、固定移动融合安全、非公众网络（NPN）安全以及公众网络（PLMN）与 NPN 互通安全、增强的蜂窝物联网安全、高可靠低时延（uRLLC）业务安全、基于 3GPP 的应用的认证和密钥管理、V2X 业务安全等领域开展标准研究或者标准制订工作，以进一步增强 5G 网络在面向不同业务场景时的安全能力，为用户提供更全面、灵活的网络安全选项。

中兴通讯认为，未来的 5G 将成为整个社会的基石。如果说传统移动网络的安全性主要影响的是互联网经济的话，5G 网络的安全性将会对包括实体经济在内的所有社会、经济领域的安全带来重大影响。因此，在 3GPP 标准定义的安全框架之上，我们需要更加全面、更加系统化的分析 5G 面临的安全挑战，并作出应对。

1.2 全新的安全挑战

重新定义 5G 基础设施

5G 商业生态引入了新的监管者、商业主体，也带来了不同的信任模型。为了打造多元化、可信的 5G 生态，承载不同业务特征的数字资产，实现 ITU-T 定义的商业目标，5G 网络基础设施不再局限于纯粹的流量承载，而是在 SDN/NFV、MEC 等新技术的支撑下，进行了重新定义，提供基于切片定制的按需网络服务。



5G 能力架构及安全保障

安全可靠的 5G 专网接入

随着互联网从消费领域向产业领域不断演进，并逐步涉及能源、工业、交通等关键基础设施，其承载的商业价值与社会影响力远远高于传统的消费类业务，因此网络评价指标不再局限于带宽与流量价格，对于安全性与可靠性的充分考量成为首要的因素以及非常刚性的约束。未来，5G 将深入我们的生活方式，影响全社会的福祉，并与产业创新与经济增长直接相关，5G 网络必须能够提供不低于传统高等级专网的安全性与可靠性，才能够胜任关键基础设施中高价值资产的承载，这需要在网络切片基础之上提供进一步的安全加固能力。

在面向重要基础设施的 5G 专网中，可以按照资产价值及其 SLA 特征，将业务网络分割为不同的区域，不同的区域采用具有不同安全属性的网络切片进行承载。

融贯行业的资产保障

5G 连接了物联网和垂直行业的关键基础设施，实现了移动网络从面向人的连接向面向机器连接的演变，也使得安全威胁在 IT 域与 OT 域之间进行双向渗透变得可能。另外，由于被攻击的目标往往连接物理世界的人或资产，使得攻击导致的后果更为严重，后续的处置也更为复杂。由于各类基础设施大量分散在网络的边缘，因此边缘计算（MEC）将会是垂直行业重要的选择与屏障。运营商需要采取必要的安全措施，保护 MEC 节点自身以及 MEC 节点中客户数字资产的安全。

持续创新的安全服务

随着网络与业务融合的深入展开，一方面，5G 网络自身需要在充分考虑特定行业的业务特点与安全态势基础上，引入新型智能化检测技术与防御手段，提供持续创新的安全能力。另一方面，5G 网络可以向垂直行业应用，开放自身的安全能力，降低垂直行业的安全开发与部署成本，提升创新效率。

多元化的网络安全治理

产业互联网与 5G 网络融合，同样也会对网络安全治理带来冲击。首先是安全规范的多元化，如金融、电力、工业互联网等不同行业，对于基础设施有着与电信网络不同的安全法规和标准、数据保护规范以及安全评测标准；其次是资产主体的多元化，例如 MEC 上的设备、平台及应用，往往需要贯穿多个商业主体。5G 如何满足这种多元化的网络安全治理需求，能否构建统一的网络安全治理体系，有待探索。

第 二 部 分

可定制化的切片安全

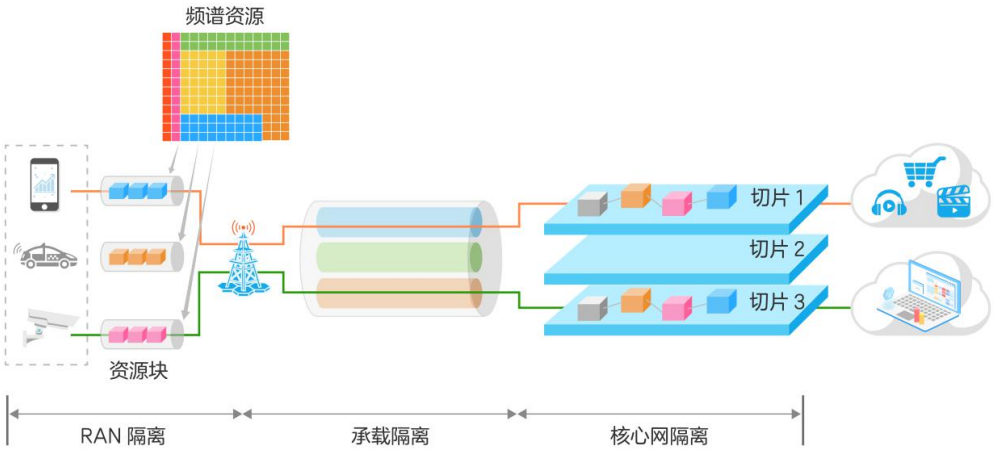
2.1 网络切片和切片安全

5G 网络切片是基于无线接入网、承载网与核心网基础设施，以及网络虚拟化技术构建的一个面向不同业务特征的逻辑网络。运营商可以为不同行业应用在共享的网络基础设施上通过能力开放、智能调度、安全隔离等技术分别构建彼此隔离的 5G 网络切片，提供差异化的网络服务。

网络切片技术有利于构建以运营商为中心的开放网络生态，充分发挥网络基础设施的潜力，拓展新的收入来源。同时，对于垂直行业而言，网络切片也有利于大大降低专网的建设和运营成本，并且可以借助网络切片灵活的性能弹缩优势，快速满足动态变化的网络需求。网络切片技术的应用是电信网络的一次重大变革，为电信网络和行业应用的深度融合奠定了坚实基础。区别于传统物理专网的私有性与封闭性，5G 网络切片是建立在共享资源之上的虚拟化专用网络，切片安全除了提供传统移动网络安全机制之外（例如接入认证、接入层和非接入层信令和数据的加密与完整性保护等），还需要提供网络切片之间端到端安全隔离机制。

2.2 网络切片的端到端隔离

为了满足不同业务的安全等级需求，网络切片结合了各种物理隔离和逻辑隔离机制，来实现网络切片间的隔离防护。5G 网络切片端到端隔离可分为 RAN 隔离、承载隔离和核心网隔离，如下图所示。



5G 网络切片端到端隔离模型

RAN 隔离

网络切片在 RAN 侧的隔离主要面向无线频谱资源以及基站处理资源。5G OFDMA 系统中，无线频谱从时域、频域、空域维度被划分为不同的资源块，用于承载终端和基站之间数据传输。频谱资源的隔离可以分为物理隔离和逻辑隔离。物理隔离是给网络切片分配专用频谱带宽，这时分配给切片的资源块是连续的。逻辑隔离是资源块按照不同切片的要求按需分配，分配给每个切片的资源块是不连续的，多个切片共享总的频谱资源。

无论是物理隔离还是逻辑隔离，由于资源块的正交性，两者的隔离能力基本相当。但是专用频谱的覆盖范围和覆盖效果通常不如共享频谱，当数据文件较大，或者用户处于小区边缘时，由于无法使用更宽的频谱传输，使用物理隔离的切片往往无法达到更高的传输速率。另外由于物理隔离方式实现成本较高，资源分配不够灵活，因此频谱租赁代价高昂。逻辑隔离可以实现基站调度器根据不同切片的传输要求，对资源块动态调配，提高了频谱资源利用率，因此，行业应用在无特殊要求的情况下，应首选逻辑隔离方案。

DU 和 CU 是对传统 RAN 功能的进一步重构，DU 用于处理 L1(PHY)和 L2(MAC)层功能，例如资源块调度、调制编码、功控等功能，CU 用于处理 L2 层以上的功能，例如分组数据汇聚、切换等功能。基站处理资源的隔离可以从 DU 和 CU 两个方面考虑，DU 软件目前依赖于专用硬件实现，CU 软件则既可以在专用硬件运行，也可以虚拟化在通用服务器上运行。网络切片在 DU 的处理资源隔离可通过物理隔离的方式，为不同的切片分配不同的 DU 单板或处理核，也可以通过逻辑隔离的方式共享处理资源。从专用硬件成本和处理效率的角度，DU 更多采用共享处理资源的方式。当 CU 软件运行在专用硬件上时，策略可以类似于 DU，更倾向于共享处理资源。当 CU 软件运行在通用服务器上时，网络切片在 CU 的隔离可基于 NFV 隔离技术实现，通过虚机/容器隔离实现 CU 隔离。根据切片的安全隔离要求，在 DU、CU 上的隔离机制可单独或组合使用。

承载隔离

5G 网络依托数据中心部署，跨越数据中心的物理通信链路需要承载多个切片的业务数据。网络切片在承载侧的隔离可通过软隔离和硬隔离两种方案实现。

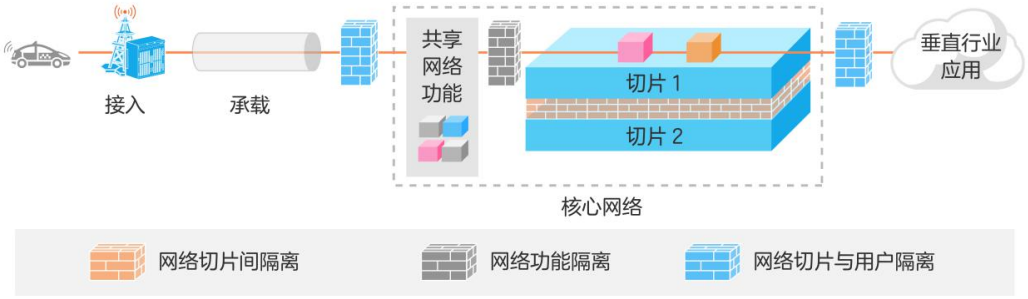
软隔离方案基于现有网络机制，通过 VLAN 标签与网络切片标识的映射实现。网络切片具备唯一的切片标识，根据切片标识为不同的切片数据映射封装不同的 VLAN 标签，通过 VLAN 隔离实现切片的承载隔离。

软隔离方案虽然将不同切片的数据进行了 VLAN 区分，但是标记有 VLAN 标签的所有切片数据仍然混杂在一起进行调度转发。硬隔离方案则引入 FlexE 技术，基于以太网协议，在 L1(PHY)和 L2(MAC)层之间创造另一“垫层”，实现 FlexE 分片。FlexE 分片是基于时隙调度将一个物理以太网端口划分为多个以太网弹性管道，使得承载网络既具备类似于 TDM(时分复用)独占时隙、隔离性好的特性，又具备以太网统计复用、网络效率高的特点。

网络切片的承载隔离可以同时使用软隔离和硬隔离的方案，在对网络切片使用 VLAN 实现逻辑隔离的情况下，进一步利用 FlexE 分片技术，实现在时隙层面的物理隔离。

核心网隔离

5G 核心网基于虚拟化基础设施构建，并且由很多种不同的网络功能构成，有些网络功能为切片专用，有些则在多个切片之间共享，因此在核心网侧的隔离需要采用多重隔离机制，如下图所示。



核心网隔离模型

网络切片间隔离

由于网络切片共享统一的核心网基础设施，为了确保一个切片的异常不会影响到其他切片，一方面，核心网可以采用物理隔离的方案，为安全性要求较高的切片分配相对独立的物理资源，另一方面，还可以采用逻辑隔离方案，借助成熟的虚拟化技术，在网络层通过划分 VLAN/VXLAN 子网进行隔离，在管理层通过分权分域实现切片管理和编排的隔离。相对于物理隔离方案，逻辑隔离对资源分配更加灵活，更为经济。

网络功能隔离

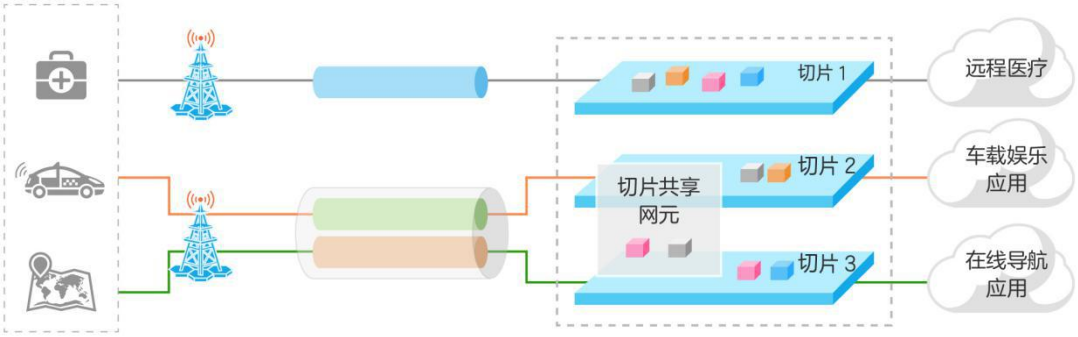
不同网络功能（NF）需要根据自身的安全级别要求与信任关系，进行安全域划分，以提供网络功能之间的相互隔离。随着 MEC 应用的普及，大量 UPF 等网络功能需要从核心网络域下沉至网络边缘，与基站或 DU/CU 共址部署，这会使得下沉的 NF 与其他核心网 NF 被进一步划分到不同的安全子域。切片共享的网络功能与切片内的网络功能互访时，需要设置安全防护机制（例如白名单）进行控制，限制非法访问。

网络切片与用户隔离

为了避免 CN 网络切片遭受来自外部的攻击进而威胁到切片安全、可靠的运行，可以在切片网络和终端用户之间、以及切片网络和行业应用之间部署安全隔离机制。切片网络和终端用户之间的隔离可采用基于切片的接入认证和访问控制等机制。切片网络和行业应用的隔离，可以通过部署虚拟或者物理防火墙，并设置访问策略来进行。

2.3 面向应用的切片定制

5G 网络切片面向不同垂直行业的业务特征提供差异化的按需服务定制能力，其中安全性是定制过程中必须考虑的关键因素之一，如下图所示。



面向垂直行业应用的切片定制

对于业务时延和安全性要求极高的应用，例如远程医疗业务，必须提供切片安全隔离等级最高、切片接入控制最严格的网络服务。因此在设计、编排、部署切片时可实施如下端到端的物理隔离方案：在无线侧分配独立的小区、专用频段；在核心网侧分配专用的处理机资源；在传输网络上使用专线进行传输。

对于普通的网络应用，例如车载娱乐、在线导航等，对安全性无严苛要求，在设计、编排和部署切片时，可采用如下隔离方案：无线侧基于共享小区、资源块隔离；核心网侧可以共享部分控制面 NF，用户面和其他控制面 NF 基于切片隔离；承载网侧共享传输资源，通过策略路由、SDN、IPSec、FlexE 等技术实现隔离。

第 三 部 分

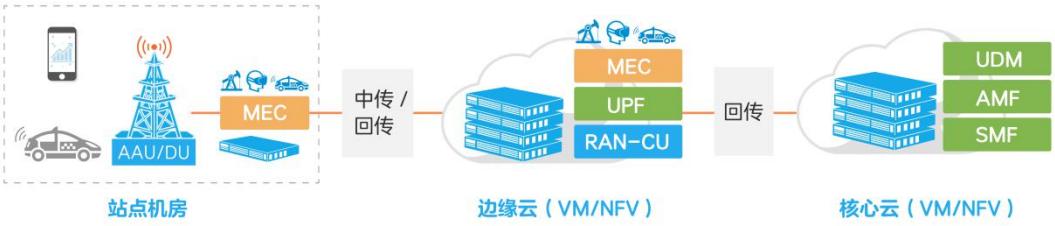
边缘计算安全

3.1 MEC 在 5G 中的应用

多接入边缘计算技术（MEC）是 5G 业务多元化的核心技术之一，采用分布式网络架构，把服务能力和应用推进到网络边缘，改变了当前网络与业务分离的状态，是 5G 的代表性能力。

在 5G 架构设计中，通过支持用户面功能（UPF）下沉部署、灵活分流等功能，实现对 MEC 的支持，同时 MEC 可将移动网络的位置服务、带宽管理等开放给上层应用，从而优化业务应用，启发新的商业模式，进一步提升网络价值。

MEC 将数据缓存能力、流量转发能力与应用服务能力进行下沉，网络位置更接近用户，能够大幅降低业务时延，满足车联网、工业互联网等低时延业务需求，减少对传输网的带宽压力，降低传输成本，支持高清视频、AR/VR 等高带宽业务的需求，并进一步提高内容分发效率，提升用户体验。

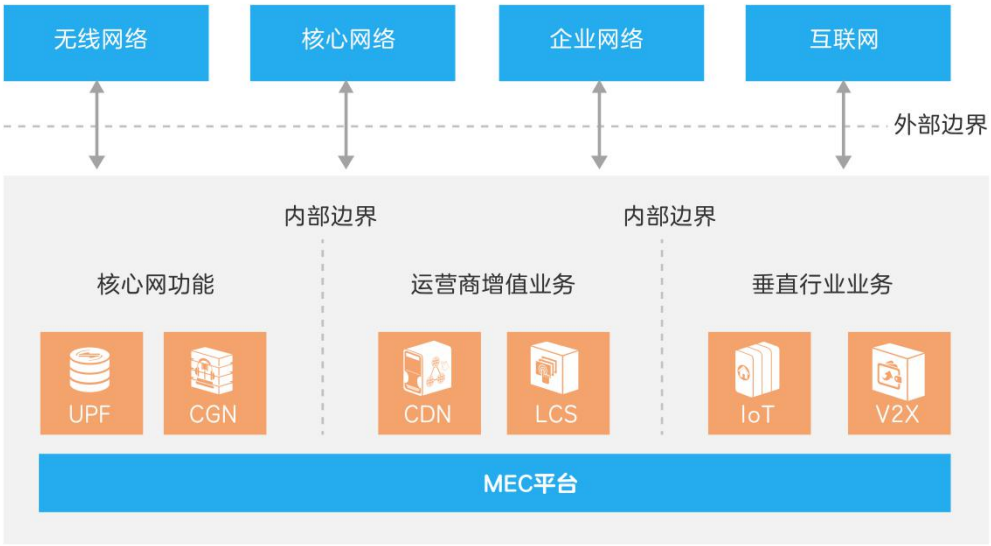


5G 网络中的 MEC

随着 5G 网络即将步入商用，未来各种超高带宽类、低时延类的新兴业务将逐步涌现，因此，一方面，对 5G 网络中部署 MEC 面临的安全问题的研究需要加强；另一方面，还需要研究将 MEC 部署在企业园区或指定的安全区域所带来的新的安全挑战。

3.2 安全是 MEC 部署的关键要素

典型的 MEC 承载了部分核心网功能、运营商增值业务以及垂直行业业务等，并与无线接入网络、核心网、企业网络、互联网等多个外部网络互联。从总体上看，MEC 是中心计算的延伸，既继承了中心计算的优势，也面临和中心计算相似的威胁；具体来看，由于在物理位置、网络边界、客户主体、业务类型等多方面发生了变化，导致 MEC 在组网架构与运营模式上与传统电信网存在较大差异，因此在安全性方面也面临新的挑战。



MEC 架构

网络架构

由于 MEC 节点靠近网络的边缘，外部环境可信度降低，管理控制能力减弱，使得 MEC 平台和 MEC 应用处于相对不安全的物理环境，更容易遭受非授权访问、敏感数据泄露、(D)DoS 攻击、设备物理攻击等威胁。另外，运营商网络功能与不可信任的第三方应用共平台部署，进一步导致网络边界模糊、虚拟机逃逸、镜像篡改、数据窃取与篡改等诸多安全问题，使得内部威胁滋生蔓延的风险加大，增大了运营商资产和行业资产的风险。

网络功能

部分核心网功能跟随 MEC 下沉到边缘数据中心，增大了核心网面临的攻击面。传统电信网络由核心网网关，例如 GGSN，PGW，收集用户计费信息上报给计费系统实施计费。如果以上网关跟随 MEC 部署在接入站点，例如赛事场馆、购物中心等公共场所，由于流量不经过核心区域，可能存在非法窃听、欺骗性计费等威胁。另外，由于 MEC 节点的业务覆盖范围有限，一旦用户发生跨节点切换，例如高铁数据服务，也会面临站点间相互信任、网络连接上下文如何安全传递等安全问题。

网络运维

MEC 是一个多元化系统，包括了移动通信网络、MEC 能力开放服务以及行业应用等多个系统，因此需要构建有效的信任模型，为多个系统的安全共存提供信任基础。除了需要建立用户、行业应用及 MEC 服务（如定位服务）之间的信任模型，还需要考虑建立移动终端、网络切片与 MEC 平台之间的信任模型。MEC 架构与 5G 网络由两个不同的标准体系定义，如何将两者有机融合，满足运营商及行业用户不同的运维需求，是 MEC 需要重点研究的问题之一。

3.3 MEC 安全防护

MEC 的安全防护继承了电信云数据中心的安全防护手段，包括云化的基础设施加固，以及虚拟化的网络安全服务等。同时，针对 MEC 面临的全新安全挑战，还需要从多个方面进行针对性的加固。

基础设施加固

物理安全：根据不同业务场景，MEC 节点可部署在边缘数据中心、无人值守的站点机房，甚至靠近用户的现场。由于处于相对开放的环境中，MEC 设备更易遭受物理性破坏，需要与场所的提供方一起，共同评估和保障基础设施的物理安全，引入门禁、环境监控等安全措施；对于 MEC 设备，还需要加强自身防盗、防破坏方面的结构设计，对设备的 I/O 接口、调试接口进行控制。此外 MEC 节点还必须具备在严苛、恶劣物理环境下的持续工作能力。

平台安全：针对部署在运营商控制较弱区域的 MEC 节点，需要引入安全加固措施，加强平台管理安全、数据存储和传输安全，在需要时引入可信计算等技术，从系统启动到上层应用，逐级验证，构建可信的 MEC 平台。为保证更高的可用性，同质化的 MEC 之间可以建立起“MEC 资源池”，相互之间提供异地灾备能力，当遇到不可抗的外部事件时，可以快速切换到其他 MEC，保证业务的连续性。

网络安全：MEC 连接了多重外部网络，传统的边界防御、内外部认证、隔离与加密等防护技术，需要继续在 MEC 中使用。从 MEC 平台内部来看，MEC 被划为不同的功能域，如管理域、核心网域、基础服务域（位置业务/CDN 等）、第三方应用域等，彼此之间需要划分到不同安全域，引入各种虚拟安全能力，实现隔离和访问控制。同时需要部署入侵检测技术、异常流量分析、反 APT 等系统，对恶意软件、恶意攻击等行为进行检测，防止威胁横向扩展。此外，基于边缘分布式的特点，可以在多个 MEC 节点部署检测点，相互协作实现对恶意攻击的检测。

运维管理安全增强

MEC 上运行和存储着运营商和行业客户的各种数据资产，同时，5G 核心网用户面的下沉也带来了非法窃听、欺骗性计费等威胁。为了确保 MEC 节点中资产与数据的安全，需要对使用 MEC 的各方的行为执行认证（Authentication）、授权（Authorization）、审计（Audit），此外，还需要在平台层面、网络层面、业务层面等多个维度，对数据资产的所有权、使用权和运维权进行分权分域的管理。当边缘域与核心域之间涉及到管理、计费等关键性通讯时，需要充分利用 PKI 以及 TLS/IPSec 等协议，实施认证授权与传输加密。

为了确保运行版本的安全，防止带毒运行，MEC 需要支持针对 VNF 版本包在不同交付环节之间的签名（发布方）与 验签（接收方），同时需要对发布的版本包做签名校验。

为了避免安全漏洞影响到 MEC 节点上其它功能域的安全，在第三方应用引入之前，需要执行严格的管控流程，对其进行全面的安全评估和检测。同时通过应用注册过程对应用权限进行控制，通过审计手段对应用行为进行问责，以规范第三方应用的运行。

数据资产保护

MEC 节点位于网络边缘，处于运营商控制较弱的开放网络环境中，数据窃取、泄露的风险相对较高。部分垂直行业，对数据管控有更严格的要求，要求企业数据不出园区。这对 MEC 中数据存储、传输、处理的安全性提出了较高的要求。

在 MEC 部署、业务运行过程中，必须对 MEC 应用可能涉及的数据进行识别，包括用户的标识、接入位置等。对安全要求高的数据需要采用加密方式存储；对行业高价值资产数据，应尽量使用 IPSec/TLS 等安全传输方式，避免传输过程中数据泄露或被篡改。对数据处理、分析和使用，需要服从当地的数据隐私法律法规，结合数据操作对象的认证、授权等方式规范数据的处理使用，并对操作过程进行记录。如果涉及数据隐私，在使用之前需要对数据进行脱敏处理。

第 四 部 分

安全能力开放

4.1 安全能力开放模型

5G 网络能够通过能力开放接口将网络能力对外开放，以便垂直行业按照各自的需求编排定制化的网络服务。为了满足不同垂直行业的安全需求，5G 网络通过将安全能力进行抽象、封装，与其他网络能力一起开放给行业应用，配合资源动态部署与按需组合，为垂直行业提供灵活、可定制的差异化安全能力。

5G 安全能力开放模型如下图所示。

5G 安全能力开放模型

5G 安全能力开放模型可分为资源层、能力层和应用层三个层面。

资源层提供各种基础资源的抽象与封装。资源可以是各种类型和形态，以资源池的形式提供，包括安全功能资源池、安全算法资源池、安全信息资源池和可信计算资源池等。安全功能资源池包括虚拟防火墙、虚拟安全网关等虚拟化安全设施；安全算法资源池包括一系列加密算法、完整性算法、AI 算法等；安全信息资源池包括各种漏洞库、病毒库、威胁情报等安全相关的信息资源；可信计算资源池包括支持可信计算的硬件模块与软件平台。

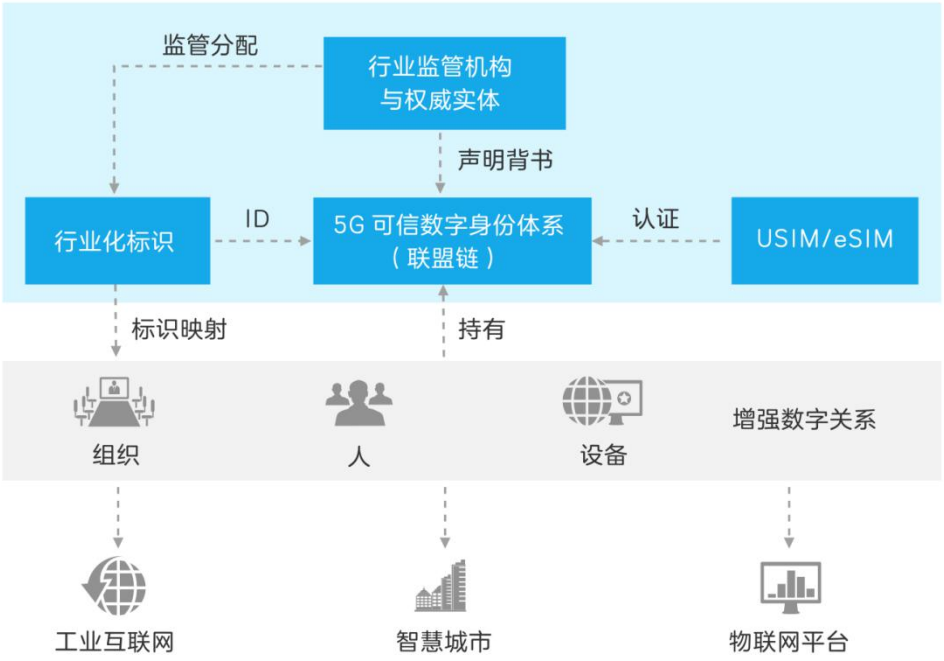
能力层提供了各种可供应用层调用的安全能力集，例如数字身份体系、可信计算体系、通道加密体系等。这些能力集由网络运营商整合和维护，结合 5G 网络的优势，对应用提供具备高度可用性与灵活性的能力调用接口。

应用层根据需要将多种安全能力进行编排，提供符合自身特点的安全防御体系。由于资源层具备很强的伸缩能力，因此应用层也能够获得很强大的弹性安全能力。

4.2 可信数字身份

5G 生态带来众多不同类型新参与者与新商业模式，例如：新监管机构、新垂直行业主体、新业务类型以及新机器连接等），这也使得 5G 生态中的监管关系、权属与管理关系、契约关系、信任关系、背书与验证关系等更为复杂化与多元化，其影响波及网络层与应用层。

随着 5G 大规模部署以及物联网能力的逐渐普及，各主体（运营商、监管者、垂直行业、OTT、第三方服务、消费者、IoT 设备等）之间需要一种能够表达新生态下相互之间更加丰富与多元化的新型数字关系的身份体系，以更好的支持 5G 业务的创新与商业模式的演进。



5G 可信数字身份体系

传统互联网数字身份体系（例如：DNS、PKI 等）基于个体自治原则、独立第三方 CA 信任模型，以一种业务无关的管理方式运作，数字关系表达能力有限，这在消费互联网背景下是合适的。5G 面向的垂直行业场景，有更合适的信任主体，更紧密的背书关系，以及更直接的权属与管理关系，具备更丰富的数字关系表达能力。另外，由于传统互联网数字身份体系的信任根大多位于主权控制之外，对于特定国家或者地区而言存在很大的安全隐患。

目前存在很多与数字身份相关的分散的研究，包括各种垂直行业标识体系、面向物联网的数字证书体系、5G 融合身份认证、跨运营商的协同等，都可以融合在统一的可信数字身份框架下。5G 生态可以以 USIM/eSIM 认证为基础，通过引入区块链、DID 等新技术，

重建面向 5G 网络与产业互联网的新型数字信任体系，使得更多不同行业的权威与可信主体（例如运营商、监管部门、互联网产业等）能够参与到 5G 数字身份生态之中，为 5G 产业互联网的创新与发展保驾护航。

4.3 智能网络防御

5G 不同的业务场景在架构、组网、软硬件组成方面都存在差别，因此面临着多种不同类型、不同手段网络攻击的风险，很难有完备的安全方案一劳永逸地杜绝网络攻击。

5G 智能网络防御能力

5G 网络支持面向机器的连接，相比于传统消费互联网人的行为的复杂性与不确定性，机器的行为模式相对简单，流量模型可预测，同时由于网络切片的使用，隔离了各种不同业务特征的网络流量，因此，通过快速的学习和训练，AI 技术可以更加准确的对垂直行业的流量与行为的异常进行检测、回溯与根因分析，为垂直行业用户提供实用化的安全分析与告警，抵御各类 APT 攻击。

AI 技术的发展为 5G 网络提供了智能化的攻击检测机制。首先，对网络中的流量和各种日志信息进行持续地收集分析，在大量的数据中提取高价值的安全事件，这些安全事件反映了网络中存在的各种行为。通过预先建立的模型对这些安全事件进行分析，分辨出其中与网络攻击相关的异常行为，就能够判断出网络攻击事件的存在和发生的位置。

仅仅检测到单个网络攻击事件是不够的，网络攻击的传播过程、发起的源头和扩散的范围都是我们需要知道的重要信息。因此，需要对安全事件进行关联分析，即在大量的安全事件中寻找事件之间的因果关系，形成整个攻击事件的攻击链条，清晰地展现攻击事件的整个过程和扩散范围。基于对网络攻击事件的深度挖掘，结合网络的基础设施情况和运行状态，就能够对网络安全态势做出评估，对未来可能遭受的网络攻击进行预测，提供针对性的预防建议和措施。

第 五 部 分

5G 安全治理与评估

5G 网络安全不仅仅是一个技术问题。诸如工业制造、能源、交通等垂直行业与 5G 的融合，打破了基础设施的天然隔离屏障，增加了基础设施面临的风险，会对 5G 网络的监管与安全提出更多的要求，例如：新的法律框架与监管模式、额外的安全评估与认证要求等。运营商作为 5G 生态的核心，需要与政府以及监管部门一起，协商、制定并实施合适的安全法规与监管流程。同时，垂直行业的业务特点也决定了面向传统消费互联网的安全治理框架与支持体系将会失效，运营商需要面向产业互联网，重构 5G 网络的安全治理体系、运维体系、客服体系，为用户提供可持续、可信、安全的网络服务；另一方面，为了建立多条安全防线，还需要将客户（尤其是垂直行业）引入到 5G 网络的治理工作中来，为客户提供面向 5G 专网的深层次治理能力。

5G 设备供应商是 5G 供应链重要的组成部分，其安全治理的水平决定了 5G 网络的安全基础。中兴通讯作为领先的 5G 解决方案与产品提供商，深刻理解消费者、客户以及各国政府、相关组织对网络安全方面的关切与重视，通过建设一流的产品安全治理体系，为客户提供安全、可信的 5G 解决方案与产品。

为践行开放透明的承诺，中兴通讯坚持实行持续的、全面的安全审计，采用了面向产品全生命周期的个人数据保护方法和实践，并与全球知名第三方安全评测与认证机构合作，对产品与服务的安全性进行独立测试与评估。中兴通讯正在筹建全球安全实验室，在这里，客户与独立评测机构可对中兴通讯提供的 5G 产品进行更加透明的检视与审查，以进一步提升对于中兴通讯 5G 产品与服务安全性的信心。

中兴通讯愿意与运营商、各国各地区政府、监管机构以及独立安全评估机构一起，共同研究面向 5G 网络的开放、透明治理机制，并愿意分享自身成功的安全治理理念与实践。

第 六 部 分

总结与展望

中兴通讯作为全球化的企业，始终将产品和服务安全性作为企业的基础责任之一。公司成立 30 多年以来，坚持将安全作为产品、服务和流程的一项内在属性，从公司的文化、组织、治理架构到产品研发、交付、工程服务等的每一个环节，都凝聚着对最高安全标准的追求。

随着 5G 商业化进程加速，5G 网络和垂直行业的深度结合，新型业务场景不断涌现，新技术大规模使用，都将对网络与信息安全提出新的挑战。中兴通讯将继续秉持以安全、合规为基石，不断完善产品安全治理体系，强化产品安全竞争力，同时融合业界最新、最佳实践，驱动安全能力不断创新，为全球客户提供更加安全的 5G 产品与服务。

缩略语

缩略语	英文全称	中文全称
3GPP	Third Generation Partnership Project	第三代合作伙伴计划
AAU	Active Antenna Unit	有源天线单元
AI	Artificial Intelligence	人工智能
API	Application Programming Interface	应用程序编程接口
APT	Advanced Persistent Threat	高级持续性威胁
AR	Augmented Reality	增强现实
BBU	Base Band Unit	基带处理单元
CDN	Content Delivery Network	内容分发网络
CA	Certificate Authority	证书颁发机构
CU	Centralized Unit	集中式单元
DID	Decentralized IDentifier	去中心化身份
DNS	Domain Name System	域名系统
DoS/DDoS	Denial of Service/Distributed Denial of Service	拒绝服务/分布式拒绝服务
DU	Distribute Unit	分布式单元
eSIM	embedded Subscriber Identity Module	嵌入式用户识别卡
GGSN	Gateway GPRS Support Node	网关 GPRS 支持节点
IT	Information Techonology	信息技术
ITU-T	International Technological University-Telecommunication Standardization Sector	国际电信联盟电信标准分局
MEC	Multi-access Edge Computing	多接入边缘计算

NFV	Network Function Virtualization	网络功能虚拟化
NPN	Non-Public Network	非公共网络
OT	Operation Technology	运营技术
OTT	Over The Top	互联网业务
PCF	Policy Control Function	策略控制功能
PGW	PDN Gateway	PDN 网关
PHY/MAC	Physics/Media Access Control layer	物理层/媒体接入控制层
PKI	Public Key Infrastructure	公钥基础设施
PLMN	Public Land Mobile Network	公共陆地移动网络
RAN	Radio Access Network	无线接入网络
SDN	Software Defined Network	软件定义网络
(U)SIM	(Universal) Subscriber Identity Module	(全球)用户识别卡
SLA	Service Level Agreement	服务等级协议 p
SMF	Session Management Function	会话管理功能
TDM	Time Division Multiplexing	时分复用
TLS	Transport Layer Security	传输层安全
UPF	User Plane Function	用户面功能
uRLLC	ultra Reliable & Low Latency Communication	超高可靠超低时延通信
VLAN	Virtual Local Area Network	虚拟局域网
VM	Virtual Machine	虚拟机
VR	Virtual Reality	虚拟现实
VXLAN	Virtual eXtensible LAN	可扩展虚拟局域网
V2X	Vehicle to Everything	车联网

参考文献

[1] 3GPP TS 33.501. Security Architecture and Procedures for 5G System[S], 3GPP.

[2] 5G-ENSURE_D2.7 Security Architecture[R], 5GPPP.

[3] ETSI GS MEC-002. MEC Technical Requirements[S], ETSI.

[4] IMT-2020 5G Network Security Requirement & Architecture[R], IMT-2020.

[5] GTI 5G Network Security Consideration[R], GTI

[6] ZHAO Fuchuan, WEN Jianzhong. Slicing Packet Network Infrastructure and Key Technologies for 5G Mobile Backaul[J], ZTE TECHNOLOGY,2018.8.

[7] Recommendation ITU-T X.rdmase: Requirements and Guidelines for Dynamic Malware Analysis in a Sandbox Environment[R], ITU-T.

[8] Data Model and Syntaxes for Decentralized Identifiers(DIDs). https://w3c-ccg.github.io/did-spec/

[9] Verifiable Credentials Data Model. https://w3c-github.io/vc-data-model

本文档由中兴通讯首席安全官钟宏指导

由中兴通讯安全技术专家委员会编写

感 谢

闫新成　　汤 凯　　毛玉欣　　郝振武　　马苏安

许秀莉　　李 锐　　刘建华　　周继华　　王意军

陆海涛　　林 军　　李成元　　张 灿

CHRISTOPHER MULLEY

等同事的辛勤付出

中兴通讯股份有限公司

地　址：深圳市南山区科技南路 55 号

电　话：0755-26770000

邮　编：518057

官　网：www.zte.com.cn