基于5G的垂直行业安全新特征与对策

New Characteristics and Countermeasures for Vertical Industries Security in 5G

汤凯/TANG Kai
（中兴通讯股份有限公司，广东 深圳 518057）
(ZTE Corporation, Shenzhen 518057, China)

摘要：分析了5G的新技术给网络安全性带来的新挑战。针对传统安全产品和技术，提出了优化与增强的要求。同时还从环境、业务、资产和运营4个角度，总结了垂直行业应用的各种新特征，并分析了这些特征给安全性带来的挑战与影响，同时提出了一些针对性的缓解措施。

关键词：5G；垂直行业；安全；物联网；网络切片；移动边缘计算；运营技术

Abstract: The new challenges brought by the new technologies of 5G on network security are analyzed, and the optimization and enhancement requirements for traditional security products and technologies are proposed in this paper. Various new application characteristics of vertical industry applications are extracted from four perspectives of environment, service, assets and operations. The challenges and effects of these characteristics on security are analyzed, and some targeted mitigation measures are put forward.

Key words: 5G; vertical industries; security; internet of things; network slice; mobile edge computing; operation technology

DOI：10.12142/ZTETJ.201904009
网络出版地址：http://kns.cnki.net/kcms/detail/34.1228.tn.20190708.1603.004.html

网络出版日期：2019-07-09
收稿日期：2019-05-28

1 安全是产业互联网的基石

如果说在消费互联网时代，“控制住了网络就控制住了世界”只是一句口号的话，那么在5G时代，这句话即将变成现实。随着越来越多的设备、基础设施、行业应用与数字化资产承载于5G网络之上，网络安全逐步上升为事关国家和社会稳定发展的重大命题。

根据越来越频繁的安全事件可以看出，针对物联网、电网、交通基础设施等非传统价值目标的攻击比例越来越高，攻击的门槛越来越低，手段也越来越丰富。随着5G网络大规模部署，无论是从黑色产业链角度，还是出于其他政治、军事、经济、社会等目的，5G所连接的重要基础设施，对攻击者的吸引力都会与日俱增。未来20年，通过网络对各类基础设施进行破坏、劫持、勒索的网络恐怖主义将会成为各国政府、各行业监管机构、基础设施提供者、企业运营者以及广大公众需要经常直面的问题。全社会需要从政策、法规、组织、技术等各个层面提前做出应对，设立多条安全防线，构建完善的网络空间安全治理框架，为未来产业互联网的可持续发展提供稳定的基石。

2 传统威胁叠加新挑战

在5G阶段，大量现有的方法论、信息技术（IT）将会继续在垂直行业中使用，传统上用于攻击的漏洞、工具与手段都能够直接作用于垂直行业应用并产生威胁。由于被攻击的目标往往还会连接物理世界的人、资产和关键基础设施，会使得

风险后果更为严重，处置起来也更为复杂。由于垂直行业应用往往会具有多种不同的特征，相互之间关联交织，从而导致威胁与攻击显得更加隐蔽和复杂。5G面向网络架构的定制化，引入了软件定义网络（SDN）/网络功能虚拟化（NFV）等，这种基础设施层面的灵活性与动态性也进一步加剧了安全挑战。因此，总体上基于5G的垂直行业应用安全呈现出攻击面扩大化、攻击方式泛在化、安全边界模糊等趋势。

传统的安全机制与防御产品、服务与技术，例如认证/加密算法、密钥管理系统、防火墙、入侵检测系统（IDS）/入侵防御系统（IPS）、各种面向主机以及云基础设施的漏洞管理以及安全加固手段，需要针对性地进行优化、增强，以适应5G时代垂直行业应用的新特征。必要时，还需要引进一些特殊的安全技术，来填补传统安全盲点。

3 新特征下的安全对策

区别于传统的消费互联网的商业模式与业务架构的单一性，产业互联网由于面向场景的多元化，具备了很多独特的新特征。我们对这些新特征进行了如下的更细维度的系统化归纳与分类。每一类新特征，都可能会对垂直行业应用安全带来消极影响。

- 加：增加新的威胁与风险
- 减：降低安全架构可选择性
- 乘：叠加、放大传统的威胁与风险
- 除：影响安全架构实施效果

另外，还有一些新特征会对垂直行业应用安全带来积极影响。通过降低成本与复杂性，提升可定制性，这些特征可以从相反的方向对消极特征带来的影响起到一定的抵消作用。以上各种影响都需要在制定垂直行业安全解决方案时，基于威胁模型进行统筹分析，以被保护的垂直行业资产为中心，依据威胁的重要性以及风险后果进行技术方案的权衡与定制。

按照对应的能力层次，本文中，我们将各种垂直行业应用新特征划分为4种类型：环境型特征、业务型特征、资产型特征以及运营型特征。

3.1 环境型特征

（1）低功耗：大规模物联网（IoT）的要求。

很多负责传感、环境监测控制的设备，需要运行在无法进行持续外部供电的环境当中。由于体积或成本等因素的限制，这些设备自身很难储备太大的电能，需要设法降低功耗，以获得更长的工作时间。目前，产业界对于此类设备连续工作时间的初步共识是10 Y左右。设备的功耗来自于各个方面，优化也需要针对不同的组件分别展开，例如使用更高集成度的处理硬件、轻量级的操作系统与协议，采用窄带物联网（NB-IoT）、远距离无线（LoRa）等低功耗广域网（LPWAN）技术。从安全角度看，在此类终端中加载复杂的安全逻辑是比较困难的，因此需要考虑使用其他的辅助手段来提供增强型保护，例如在汇聚/网关设备上加载安全逻辑，对来往终端的行为与流量进行监测控制、分析与过滤；使用具有高度网络隔离性的接入措施等。通过对认证协议进行优化，尽量减少网络交互的次数。对于必须使用加密的场景，需要在安全性与功耗之间进行适当的权衡，选用合适的加密算法，并根据业务特点对其进行轻量化改造，例如减少密钥长度、降低加密计算轮次、减少密钥更新次数等。

低功耗的微控制单元（MCU）中很少配置硬件随机数发生器，这会极大地影响加密算法的安全性，因此需要研究软硬件结合的方法来提供足够的随机性。

（2）无人化：缺乏可视度。

诸如IoT设备、网关之类的边缘基础设施经常部署在远离人群与管理中心的环境中，存在大量管理盲点，难以对其进行现场维护与管理。这类设备无论是被攻击还是被劫持作为攻击发起者，往往很难立即发觉并进行快速处置。需要考虑通过5G网络对各种基础设施与设备进行资产发现与管理，以提高对于设备的可视度，并对软件无线更新（OTA）/固件无线更新（FOTA）提供安全通道。在资源允许的情况下，可以在设备版本中内置相应的安全代理软件，对设备运行的安全状态进行充分。

（3）开放性：信任边界退行至硬件内部。

大量物联网设备将会暴露在公开的环境中，这使得安全威胁从原先多发生在网络边界开始向不设防的硬件层次转移，攻击者也更容易针对设备发起拒绝服务攻击（DoS）攻击、侧信道攻击等。

从终端整体看，要考虑防拆型设计。该设计将使任何物理性的侵入都会破坏掉设备的关键部件，从而减少硬件上的侵入对设备的机密性与完整性带来的威胁。防拆型设计适用于用户对于设备本身的物理价值不太敏感的场景。

从硬件接口或电路的角度考虑，要注意防调试设计。该设计能够使得入侵者获得设备硬件的控制权后，无法从软件上对设备的操作系统、服务、应用编程接口（API）和业务软件进行窃听、调试与修改，或难以获取设备硬件或者软件的最高权限。

从操作系统的角度考虑，除了基本的安全加固手段之外，还可以参考可信计算工作组（TCG），并基于可信平台模块（TPM）芯片提供根信任并构建完整的信任链，来保护设备上系统的机密性与完整性，防护恶意代码注入。还可以对代码进行混淆或加壳处理，防止攻击者进行反向工程，对软件知识产权产生威胁。对于终端能力受限的场景，可以只引入部分加固能力，例如Secure Boot、镜像签名等。

大多数一般性场景往往只需要保护关键信息，例如安全密钥、重要配置参数等。此时可以引入TEE可信执行环境，以较低成本方式实现对于关键信息与能力的保护。

（4）异构性：系统之系统。

面对多样化的环境，物联网系统会根据自身需要综合采用射频标识（RFID）、Zigbee、蓝牙、WiFi、5G等多样化的设备类型与接入方式，增加了攻击向量。同样的防御手段，必须要在不同的硬件、操作系统、协议栈上部署，加大了安全成本与防御难度。此时，点防御的概念已难以奏效，面防御以及立体化防御成为首选，各种无代理安全技术将在其中发挥更大的作用。通过对设备、流量等扫描分析，能够从设备外部及时发现与处置各种威胁。

边缘计算（MEC）[1]由于更为靠近用户的资产，可以为物联网提供第一道安全屏障。通过在其上部署相应的物联网网关或平台，在对业务流量进行收敛与处理的同时，对物联网终端及其连接的资产进行隔离保护，以降低资产的暴露性，减少网络攻击面。

（5）灵活性：动态基础设施。

网络切片技术是5G网络中一种在共享基础设施上提供私网服务能力的技术。关于连接、服务和数据在网络切片中被隔离保护的效果，需要有不低于传统企业专网的可靠性与安全性，用户才敢于将企业专网迁移到5G基础设施之中。

5G网络切片引入的NFV/SDN技术，在带来灵活性的同时，也带来租户间的东西向威胁以及安全边界的不确定性。随着NFV的自动编排与虚机位置的动态变化，基础设施的架构也需要通过SDN进行相应的动态调整。因此，一方面，基础设施内部需要通过微分段等零信任网络技术，构建更加立体化、细粒度的安全防御体系；另一方面，安全能力需要跟随计算能力进行动态编排、定制与调整，以减少基础设施的灵活新与弹性带来的威胁。

（6）区域性：降低了移动性的复杂度。

由于需要连接到实际的物理资产，很多行业应用一般会具有较强的固定性与区域性，这也给安全解决方案带来了很多的便利性，例如无需考虑复杂的漫游性场景与环境的多变性与复杂性。

3.2 业务型特征

（1）大连接：海量设备以及海量数据。

在智慧城市环境监测控制、资源计量等场景，为了追求高精度的管理，连接密度往往会非常高。大连接已经成为5G的典型特征之一，这直接导致了安全威胁从攻击源与攻击目标2个方向上的规模快速变大，并在空间上呈现广域化与分散化的特征。

一些特殊的问题需要进行一些针对性的设计来解决，例如信令风暴、海量设备密钥管理等。可以考虑引入聚合认证、层次化标识与密钥生成技术等。

传统的防御手段主要面向移动互联网，相应的产品设计参数也是参照人的行为模式以及业务模型而配置。物联网带来的大连接、小数据包会给基础设施层面带来全新的流量模型，相应的产品设计、参数配置也需要进行调整。例如，防火墙类的设备的连接数以及小报文处理能力，需要进行优化调整。防御设备上对于过滤策略的配置，也需要针对海量设备的特点，进行更加精准的匹配，例如通过设备身份信息。

（2）低时延：实时性体验。

车联网、互动娱乐、远程医疗、

工业互联网等应用，对于通信的低时延、实时性、抗抖动性有着非常高的要求。如不满足这些要求则会导致很多问题，有时会很严重，例如涉及车内/车外的人身安危的自动驾驶业务；有时则不严重，可能仅会在商业上降低用户的满意度，例如第一人称射击（FPS）类游戏等。

从安全角度考虑，除了提高设备处理能力，5G网络还通过减少层次之间、端到端之间的安全冗余的方式在安全性与低时延之间进行优化，甚至可以完全基于业务层面实现安全性，而不依赖于5G网络。

有些业务场景对接入时延比较敏感，可以简化、优化认证框架，以减少网络交互次数以及处理流程。对于加密的场景，需要对加密算法进行优化，以减少加密、解密带来的时延，减少密钥更新频率。对于基于MEC的业务，可以将认证能力下沉到边缘进行。

有些场景对接入时延并不敏感，仅对用户面或业务执行过程中的时延敏感；因此可以将时延敏感业务下沉到MEC执行，以减少到远程数据中心的数据及逻辑依赖。

（3）高可用：保证业务连续性。

高可用性一般是成本问题。对于5G网络而言，一般会分配专门的网络切片进行隔离保护。垂直行业可以根据各自业务的可靠性等级要求，订购相应等级的网络切片，获得相应安全等级的隔离保护能力。

对于工业互联网等场景，可以在企业网络与工业网络之间建立相应隔离区（DMZ）。

对于连接的可用性，在有些特殊场景下，可以考虑引入低轨卫星等备份连接通道，保持节点网络连接的高可用性[2]。

（4）机械性：行为基线稳定。

相比于传统消费互联网中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，人工智能（AI）技术可以更加准确地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，抵御各类高级持续性威胁（APT）攻击。

另外，垂直行业关键业务的网络拓扑与业务关系相对固定。该特性结合5G的融合身份认证能力，有助于构建零信任的垂直行业网络。

3.3 资产型特征

（1）长寿命：一个不连续的生命周期。

某些物联网设备（例如低功耗类）将会长期服役，其设备生命周期超过设备制造厂家的自身存续时间。这在未来将会是较大概率事件，会给系统的长期可用性与安全性带来挑战。

由于技术的不断演进，市场会优先选择具有更低成本、更高效能的新型设备。这会导致传统型号设备的市场窗口不断缩小，其可维护性（备件供应、硬件升级、固件/软件补丁支持等）也会随着时间推进而不断降低。

对于很多行业系统而言，设备、系统的定期维护与升级是业务健康与持续发展的必要保证。为了保证业务的连续性，降低对运营层面的冲击，垂直行业应用在设计系统方案时需要考虑以下问题：

- 物理资产与设备解耦（通过标准接口连接）；
- 多设备供应商策略，以提升设备可替代性；
- 硬件标准化，优先采用通用性强的硬件设计；
- 软件开发与硬件独立（尽量采用开源平台与技术）；
- 系统可平滑升级能力（支持新、旧设备的共存与过渡）；
- 不依赖于制造厂商的补丁更新与漏洞维护；
- 不依赖于制造厂商的安全密钥与证书管理；
- 设备终身问责机制。

另外，大量的、未经过较好的安全设计的传统物联网终端仍将长期运行，并有平滑迁移到5G基础设施中的需求。安全方案需要对这一类终端建立隔离区，并设计专门的保护措施，避免降级攻击。

（2）关键性：攻击性价比提升。

针对垂直行业的攻击，更多的将会有针对性地选择高价值的目标进行。传统的黑色产业主要利用一些通用的技术漏洞，而5G时代将会面向特定的目标进行针对性地漏洞挖掘与渗透，从而进行精准式攻击。从性价比的角度考虑，越是重要的基础设施和价值目标，越是能吸引APT攻击。

安全架构师需要像罪犯而非黑客与工程师一样来思考，他们不但

要理解业务，还需要理解业务的价值、关键处理逻辑、重要数据位置。另外，垂直行业的安全不再仅仅是IT系统的职责，更需要IT与运营技术（OT）在组织架构层面、业务流程层面结合，协同完成维护职责。

5G网络切片提供了一种多等级的网络隔离机制，因此我们可以基于各种专用资源构建关键业务网络切片。例如，垂直行业可以与运营商共建5G基站并提供排他性的网络接入，基于MEC直接提供边缘接入与认证功能，同时将流量本地转发至垂直行业自有的基础设施，而不经过外部的公共网络。基础设施可以更多地采用安全专网、内联网等特殊定制的基础设施架构，来对安全性进行加固；使用类似网闸这样的设备来将关键目标与外界网络进行高度隔离，并通过封闭性与内部的隐蔽性、动态性，来增强内生防御能力。

高价值对象的保护需要保证底层基础设施的安全与可信。路由器、交换机等容易被忽略的基础设施，很容易成为一个安全漏洞，需要提升安全性要求。可以基于5G网络切片以及固定移动融合的接入能力，构建安全专网，提供一揽子的全程设备安全能力，并且支持回溯与行为轨迹跟踪，通过审计与问责降低内部攻击风险。

对于高价值目标的保护，还需要建立人机协同防御机制，以避免对机器的过度依赖与盲目信任。区块链技术对于类似工业互联网这样的高安全场景，同样具有优势，管理者在实施重要的控制之前，通过多方主体的共识认可后才予以执行。

（3）隐私性：设备即身份。

5G把网络的触角延伸到了各行各业之中，包括健康、智能家居、公共服务等场景，会产生大量更为精确、更为敏感的个人数据。而这些数据一旦泄露，对于用户的影响将非常严重。另外，由于设备的暴露性，以及各种边缘能力的使用，非法获取用户隐私可从任何地点发起，例如个人可穿戴设备，以及驾驶数据等。

由于设备与个人存在的对应关系，对于设备的标识以及其他相关的隐私性数据，也需要参考隐私保护相关的法规进行保护。为了防止对设备身份的识别与关联，必要时应当采用临时设备标识的方式对设备的永久标识进行替代。例如，介质访问控制（MAC）地址、IPv6地址等等。

3.4 运营型特征

（1）权属性：管理关系明确。

不同于安全边界的模糊化，大多数行业应用的解决方案涉及到的设备、资产、基础设施以及软件服务等，都是处于同一个产权边界中，因此，安全需求可以在同一个产权边界之内进行端到端一体化设计和实施。对于5G网络及基础设施而言，具有明确产权边界的行业应用系统，对于定制一揽子增强的端到端的安全服务能力非常有利。

（2）低信任：万物互联互通的空中楼阁。

开放与安全永远是一对矛盾。互联网业务通过人的自治与认知能力建立起通信对象之间的信任关系，并由业务提供者进行背书。5G生态带来了更多的参与者与商业模式，各种创新型的业务需要跨越多商业主体的产权边界与系统边界进行协同。然而，除了传统的法律手段，各商业主体之间的信任关系难以找到可信第三方进行背书。这导致大量的物联网能力实际上处于封闭状态，数据本身的价值流转仍然缺乏行之有效的手段与平台，所谓的万物互联仍然是空中楼阁。基于用户身份识别卡（SIM）/嵌入式用户身份识别卡（eSIM）的实名制、端到端可信连接能力以及产业链中的位置，运营商成为5G生态中商业化信任网络的核心。通过运营商特有的各种安全认证通道、强大的基础设施地位，可以采用去中心化标识（DID）技术[4]通过区块链聚合商业生态中多方权威与信任主体，建立跨越多监管主体、多运营商网络、多垂直行业平台之间的可信数字身份体系，消除5G信任鸿沟，支持跨垂直行业的商业模式的创新。

在诸如车联网（V2V）等设备到设备（D2D）的通信场景下，随机、动态的设备之间天然缺乏信任，并且也没有建立长期信任关系的需求。在这种场景下，如何对身份进行验证并建立安全的通道是5G车联网需要重点考虑的一个安全问题。诸如基于标识的加密（IBE）、匿名认证等技术将在此发挥更大的作用。

（3）文化差异：IT与OT的碰撞。

由于文化与经验各不相同，IT安全专家与OT专家之间在组织、方法、流程与策略等方面存在很大的

差异性。IT安全专家缺乏OT方面的专业知识，优先考虑的是安全性、合规性和审计性等要求；而OT专家缺乏安全专业知识，优先考虑的是设备或者资产的可用性。

垂直行业应用的安全需要兼顾IT与OT 2个领域、2种文化，其中领导者的支持尤为重要，需要将IT与OT的融合安全，作为企业的重要风险进行评估与跟踪。

4 结束语

为了使垂直行业用户对5G网络有足够的信心，相信5G网络能够提供与传统企业专网同样甚至更高等级的可靠性与安全性，并愿意将关键业务迁移到5G网络之上，运营商还需要做更多的工作：一方面需要提供专业化的5G安全专网的定制能力；另一方面，还需从法律层面为用户的服务质量与安全性做出承诺与保证，并能够根据相应的服务等级协议（SLA）对5G安全专网进行全生命周期端到端的安全治理。

随着国家信息安全技术网络安全等级保护基本要求2019版（等保2.0）的推出，国家对于关键信息基础设施的保护已经有了法律依据与实施准则，尤其面向物联网、云计算、大数据等新的技术环境，提出了针对性的等级保护与评测要求[5]。垂直行业需要主动对齐相应的保护等级要求，在保护自身资产的同时，承担应尽的社会责任。

参考文献
[1] ETSI. MEC Technical Requirements: ETSI GS MEC-002[S]
[2] 5G-ENSURE_D2.5 Trust Model (final) v2.2 inc History[EB/OL].[2019-05-20] http://5gensure.eu/files/5g-ensured25-trust-model-final-v22-inc-historypdf
[3] CHALLENER D, YODER K, CATHERMAN R. A Practical Guide to Trusted Computing[M].USA: IBM Press.2008
[4] Data Model and Syntaxes for Decentralized Identifiers (DIDs)[EB/OL].[2019-05-20] https://w3c-ccg.github.io/did-spec/
[5] 信息安全技术网络安全等级保护基本要求:GB/T22293-2019[S]. 2019

作者简介

汤凯，中兴通讯股份有限公司资深系统架构师；先后从事3G核心网系统与IMS系统的研究、架构设计与研发管理工作，以及物联网标识体系、区块链及安全、可信数字身份体系等方面的研究与项目孵化工作，目前主要从事5G、物联网与垂直行业等领域的解决方案与新技术研究等工作；曾参与多项国家标准的制定工作；提出10余项发明专利。

⬅上接第24页

相关的信息，做散列或者加密处理，保护数据安全。

根据通用数据保护条例（GDPR），涉及的个人数据包括：国际移动用户识别码（IMSI）、国际移动设备识别码（IMEI）、UE IP、网管用户电话号码和Email。我们采取的策略为内安全、外脱敏：欧盟内系统间数据，通过数据加密、传输通道加密、权限控制、系统加固等措施，保证个人数据的安全；欧盟外的数据转移，则使用强制脱敏的方法，要求数据使用非可逆算法脱敏处理。

（5）日志审计。

基站对于系统运行过程中的安全事件和关键信息予以记录并保存。如果发生安全入侵，可以根据日志或记录对事件进行回溯，确定事件原因，提供有效证据防止人员或实体否认执行过的活动。

3 结束语

中兴通讯5G网络设备实现了3GPP协议要求的安全功能，同时在基础设施的硬件和软件资产、操作维护的接入认证、访问控制进行了安全控制增强，在敏感数据保护、防DoS攻击方面采取了强化措施，确保5G网络设备的运营安全。

参考文献
[1] 3GPP. System Architecture for the 5G System; Stage 2(Release 15): 3GPP TS 23.501 [S]. 2019
[2] 3GPP. Security Architecture and Procedures for 5G System(Release 15):3GPP TS 33.501 [S]. 2019
[3] 3GPP. Network Domain Security (NDS); Authentication Framework (AF)(Release 15) 3GPP TS 33.310[S]. 2018
[4] RFC. Internet Key Exchange Protocol Version 2 (IKEv2): RFC 5996[S]. 2015
[5] RFC. IP Encapsulating Security Payload (ESP): RFC 4303[S]. 2005

作者简介

陆海涛，中兴通讯股份有限公司高级工程师、资深系统架构师；负责5G移动通信超密集组网关键技术研究和5G安全架构技术研究的工作，从事SDR软件平台、大规模信道仿真验证平台、FDD-Massive MIMO产品和5G产品的系统方案设计工作；获广东省科学技术二等奖以及深圳市科技创新一等奖；发表论文2篇，申请发明专利20项。

李刚，中兴通讯股份有限公司高级工程师、研发总工；从事TD-LTE、FDD-LTE、Pre5G、5G等产品的技术方案设计、架构和研发项目管理工作；发表2篇论文，申请发明专利15项。

高旭昇，中兴通讯股份有限公司高级工程师、5G产品研发总工；负责CDMA、WiMAX、LTE、5G等产品的系统方案设计、技术改进和研发管理工作；发表2篇论文，申请发明专利10项。