DOI: 10.33142/ec.v2i3.233

# 5G网络终端接入安全思考

史锦斌　李 博
天元瑞信通信技术股份有限公司，陕西 西安 710075

[摘要]第五代移动通信系统（5G）三大典型应用场景分别是增强型移动宽带、高可靠低时延网络和海量连接。5G除了提供超高速的移动互联网应用外，还需要为车联网、物联网（IoT）、工业制造等垂直行业的发展提供稳定可靠的网络接入，为垂直行业的信息化发展提供网络信息基础平台。新技术产生的全新应用场景和服务方式给5G网络的安全带来新的安全需求与风险。网络安全是对整个系统的要求，涉及到终端、接入、传输、核心、应用等多个环节，本文仅就网络终端和接入对安全的要求谈一些自己的思考。
[关键词]终端；安全；

# Considerations on Access Security of 5G Network Terminal

*SHI Jinbin, LI Bo*
Tianyuan Credit Suisse Communications Technology Co., Ltd., Shanxi, Xian, China 710075

**Abstract:**The five generation mobile communication system (5G) three typical application scenarios are enhanced mobile broadband, high reliability and low delay network and mass connection. 5G not only provides ultra-high-speed mobile Internet applications, but also needs to be connected to cars. The development of vertical industry, such as Internet of things (IoT), provides stable and reliable network access, and provides the basic platform of network information for the information development of vertical industry. The new application scenario and service mode of the new technology bring new security requirements and risks to the security of 5G network. Network security is the requirement of the whole system. It involves terminal, access, transmission, core and application. Such as many links, this paper only on the network terminals and access to security requirements to talk about some of their own thinking.
**Keywords:**Terminal; Security

## 1 接入终端类型和技术多样化

5G 为万物互联而生，5G 除了满足人与人的通信，还要实现人与物、物与物的通信，为此，5G 网络需要支持采用不同接入类型和技术的不同种类终端接入。按接入类型分，5G 网络需要支持 3GPP 接入和非 3GPP 接入，可信任接入和非可信任接入；从接入技术分，5G 网络需要支持 5G 新无线技术接入，还要向下兼容 3G 接入、LTE 接入、WLAN 接入以及各种固网接入技术；从终端类型分，可以是有卡终端和无卡终端。有卡终端以 SIM/USIM 卡作为用户身份和密钥载体，具备一定的计算和存储能力；无卡终端没有内置专用载体存储身份密钥信息，通常以 IP 地址或者 MAC 作为自己的身份，用数字证书提供安全保障。因此 5G 网络是融合了多种接入类型、接入技术和多种类型的终端的异构型网络，这样导致对安全需求的要求不尽相同，不同类型终端使用不同的认证协议和密钥协商机制。5G 网络需要构建统一的认证体系来满足不同的接入机制认证，满足具有不同安全能力终端的安全接入需求。

## 2 不同应用应用场景安全要求不同

5G 网络需要支持三大类典型应用：增强移动宽带（eMBB）、海量机器类通信（mMTC）和超可靠低时延通信（uRLLC）。这三类应用场景根据各自的应用特性存在不同的接入安全需求。

eMBB 重点是提供超高带宽，用于满足诸如虚拟现实（VR）、大视频等对带宽有极高要求的业务。3GPP 制定 5G 第一阶段的标准就是为了满足 eMBB 应用。eMBB 应用的接入安全通过继承和扩展 LTE 的接入安全机制实现，主要针对 LTE 接入下用户首次接入时 IMSI 采用明文传送存在的安全风险，采取了 IMSI 加密传输的机制，另外结合 5G 网络架构，进一步增强了密钥派生机制来满足各接入层次安全传输的需要。

mMTC 应用的主要特点是接入网络的终端数量巨大，终端无卡，安全能力较弱，功耗小，资源受限，小数据传送等。按照传统的接入方式，每个终端和网络之间需要进行多次交互才能完成认证过程，实现网络接入。mMTC 应用下，如果终端仍然延用传统接入方式，海量终端并发接入网络极有可能产生信令风暴，造成网络拥塞；另外，在接入失

败情况下终端不断尝试重新接入网络发起认证，这对于低功耗无人值守的 MTC 终端将加速其电池消耗。因此需要研究包括简化认证机制，优化认证协议在内的满足 MTC 设备高效快速接入的轻量化安全接入方式。针对物联网传输的是小数据且是零星传送的数据特征，需要为小数据传送建立通道。如果小数据传送的无线网络缺少安全保护机制，攻击者就有可能通过访问小数据接口入侵网络，因此还需要研究针对小数据的空口传输安全保证机制 [1]。

uRLLC 应用对通信可靠性，低时延有极高的要求，例如车联网、远程医疗等应用。网络安全通常与网络性能效率是互为矛盾的，增强网络安全防护机制，必然以牺牲网络性能，降低网络效率为代价，uRLLC 应用也不例外，如果引入安全机制，就必然会影响业务时延。但是安全对于 uRLLC 应用又是不可或缺的，如果车联网业务缺乏安全机制保护，就会存在交通信息被窃取或篡改进而影响到行车安全甚至威胁到生命安全。因此在保证可靠性和低时延等业务性能的同时，需要研究 uRLLC 的接入安全，研究车联网通信时的身份认证、车辆身份信息的保护、数据传输安全等接入安全解决方案。

## 3 5G 移动终端共性安全需求

（1）可信执行环境

伴随着 5G 技术的发展，移动终端正在成为互联网和物联网业务的关键入口，网络攻击面的大幅扩大，敏感信息的指数增加，使得 5G 终端将面临更加艰难的安全环境。为 5G 终端建立可信任执行环境，是 5G 时代的必然要求。

移动终端的运行环境面临来自硬件和软件的威胁，移动终端硬件安全威胁主要来源于终端芯片设计安全漏洞或硬件体系安全防护不足，可导致平台安全权限被获取、存储的隐私数据被窃取等安全风险，需要从硬件角度设计使终端核心器件具有抗物理攻击的能力，为移动终端的安全起到基础作用；移动终端软件系统是移动终端的灵魂，对软件系统的攻击包括：利用操作系统漏洞等获取终端控制权、修改安全策略，利用信息保护缺失、内存监管漏洞、应用程序漏洞等窃取用户信息、篡改信息和信令、植入恶意代码、扰乱系统的正常工作，利用 WIFI、蓝牙等外设配置漏洞吸引终端接入，窃取敏感信息等。利用上述攻击手段，可以轻易地收集用户数据，控制和更改终端软件，甚至在极端情况下，可以遥控瘫痪所有入网的终端，威胁国家网络安全。因此需对移动终端从硬件和软件层面采取有效措施，建立可信执行环境，保证终端平台的安全。

（2）安全体系完备性与可裁剪性

3G/4 G 时代，终端安全技术的主要驱动力是解决普通民众移动支付等安全问题，终端厂家的安全方案基本是专用和封闭的。但是进入 5G 时代，行业用户成为重要利益相关方以及万物互联成为新生态的趋势，将使行业安全和物联网安全成为 5G 终端安全技术新的强大动力。

终端安全能力包括终端防护、用户认证、入网认证、信息加密、安全存储、应用管理等，涉及平台安全、信息安全、使用安全、安全管理等多方面安全要求。不同行业对终端安全能力有着不同的需求，如果终端业界为不同行业分别设计安全架构，既不经济也不现实。为了高效率地适应差异化安全需求，应该建立统一的终端安全技术体系，该技术体系能够以组件化方式提供完备的的安全能力，同时又能够根据行业需求，方便地进行组件的组合和裁剪，提供高、中、低不同等级的安全能力，满足差异化安全要求。

从国家对信息领域的发展要求来看，在新兴信息领域实施军民战略已上升到国家战略层面。国防行业以及政府、公安等涉及国家安全和社会稳定的特殊行业，对移动通信的需求非常旺盛，安全性有着更高的要求。终端安全体系应该着眼安全能力要求更全面的特殊行业，提供完备的安全功能集。在面向普通垂直行业和普通公众用户时，安全架构能够进行有针对性地功能裁剪，为普通行业和普通公众用户提供在成本范围内的安全功能。以最小的代价实现通用终端与高安全行业终端安全防护体系的构建，满足国家对信息领域安全建设的要求 [2]。

（3）标准化的安全接口

在建立统一的安全体系同时，5G 终端还应该提供开放的安全服务环境，提供标准化的安全接口。通过标准接口，支持第三方安全服务和安全模块的引入，便于行业客户的二次开发，允许行业用户通过标准接口快速地实现行业定制，支持不同行业终端的快速部署与专用化服务，提升终端产品的服务水平和竞争力。

## 4 5G 移动终端个性安全需求

（1）eMBB 终端安全需求

eMBB 终端覆盖了增强移动宽带应用场景，是人与人、人与网、人与物间信息链接的主要载体，也是行业用户开展移动办公等处理行业敏感信息的主要工具。eMBB 终端传输速率高、涉及普通用户隐私 / 行业用户敏感信息多、支持异构网络连接，因此，它的典型安全需求主要有三个方面，一是要具备与 5G 网络速率相适配的高速率加密能

力，同时还具备较低的功耗要求；二是对普通用户具备对个人信息或标识以及地址信息等等隐私信息的保护能力，对行业用户具高等级的认证、端到端加密、信息完整性保护等能力；三是具备异构接入的统一认证和安全上下文管理能力，提高异构接入安全上下文切换效率。

（2）mMTC 终端安全需求

mMTC 覆盖对于联接密度要求较高的物联网应用场景，例如智慧城市、智能电网、智慧家居等，满足人们对于数字化社会的需求。由于物联网设备数量庞大，行业对物联终端的成本比较敏感。但是由于物联终端深入到城市基础设施及民众生活等涉及国计民生的重要部位，其安全性建设也不容忽视[3]。

mMTC 终端的典型安全需求包括：一是轻量级的密码算法和协议，满足 mMTC 终端的低功耗、低带宽要求；二是安全可靠的网络接入模式，如 5G 网络提供为物联终端提供去中心化的身份管理和接入认证模式，包括缩短认证链条、快速安全接入、网络与业务融合分层身份管理等，降低管理复杂度；三是低成本的设备认证和身份管理实现，满足物联终端低成本要求。

（3）uRLLC 终端安全需求

uRLLC 聚焦对时延极其敏感的行业，例如车联网、智慧工业等，满足人们对于数字化工业的需求。因这些行业的信息涉及自动驾驶、路况识别、工业控制等高风险环节，如果被假冒或篡改，将引发很大的安全事件，因此，uRLLC 比普通物联终端有着更高的安全性要求。

uRLLC 终端的典型安全需求包括：一是高安全等级的保护强度，具备高等级的认证、端到端加密、信息完整性保护等能力；二是超高可靠和超低时延的能力，在不降低安全保护强度的前提下，支持认证节点下移，简化认证框架与协议，提高移动性安全上下文迁移和密钥重建机制效率，采用高效密码算法，减少加解密处理时间[4]。

## 5 结束语

终端安全是 5G 安全体系中不可缺少的一环。安全架构在终端中引入终端安全面，在终端安全面中通过构建受信存储、计算环境和标准化安全接口，分别从终端自身和外部两方面为终端安全提供保障。终端自身安全保障可以通过构建可信存储和计算环境，提升终端自身的安全防护能力；终端外部安全保障通过引入标准化的安全接口，支持第三方安全服务和安全模块的引入，并支持基于云的安全增强机制，为终端提供安全监测、安全分析、安全管控等辅助安全功能。

[参考文献]

[1] 杨磊. 4G网络终端接入性能测量系统的设计与实现[D]. 华中科技大学, 2017.
[2] 邓勇. 基于演化博弈的D2D网络终端合作行为研究[D]. 浙江工商大学, 2016.
[3] 李广达, 孙晨华, 刘刚. 卫星网络与地面网络融合的5G网络架构[J]. 无线电工程, 2016, 46(03): 5-8.
[4] 攀延英. 5G网络技术特点分析及无线网络的规划研究[J]. 数字通信世界, 2019(02): 59.

作者简介: 史锦斌(1980年10月), 职称: 高级工程师。