5G网络的设备及其接入安全

Security of 5G Network Elements and Access Control

陆海涛/LU Haitao，李刚/LI Gang，高旭昇/GAO Xusheng
（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基站在自身的硬件和软件资源、无线空口、传输接口和管理接口等方面所面临的安全威胁，以及针对这些安全威胁的安全解决方案。认为安全对5G产品来说非常重要，也是5G技术能够切实推广应用的重要基础。5G网络的设备及其接入所面临的安全威胁随着技术的演进不断更新变化，需要人们采取相应的安全技术来应对。

关键词：安全威胁；加密；认证；授权

Abstract: The security threats faced by 5G base station in its own hardware and software resources, wireless air interface, transmission interface and management interface are analyzed in this paper, as well as the security solutions to these security threats. It is considered that security is very important for 5G products and is an important basis for the practical application of 5G technology. With the evolution of technology, security threats are constantly changing. It is necessary to adopt appropriate security technology to ensure product safety.

Key words: security threats; encryption; authentication; authorization

DOI：10.12142/ZTETJ.201904004
网络出版地址：http://kns.cnki.net/kcms/detail/34.1228.TN.20190716.1701.006.html

网络出版日期：2019-07-17
收稿日期：2019-05-25

随着物联网的大规模应用，越来越多的设备接入到5G网络，并要求提供大容量、大连接和高可靠低时延的移动通信。2018年6月13日，第3代合作伙伴（3GPP）正式发布5G新空口（NR）标准方案，完成了5G全功能的标准化工作。3GPP定义了5G的3大应用场景分别为：增强移动宽带（eMBB）、高可靠低时延通信（uRLLC）以及海量机器类通信（mMTC），支持诸如物联网、触觉互联网等更高数据速率、更低时延和更大规模的设备连接，对安全提出挑战。

5G网络的新架构如图1[1]所示，主要由用户设备（UE）、无线接入网络（RAN）、5G核心网（5GC）功能组件和数据网络（DN）组成。

其中RAN是5G基站（gNB）设备，用来连接所有终端用户；UE提供对用户服务的访问；接入及移动性管理功能（AMF）提供核心网控制面功能；用户面功能（UPF）提供核心网用户面功能；鉴权服务器功能（AUSF）提供认证服务器功能，用于归属网络的5G安全过程。

本文中，我们讨论的5G网络设备和接入安全主要是针对5G基站设备。安全的核心关注点就在gNB的外部接口和gNB的内部互联安全需求，通常安全攻击点都是在系统的外部接口发起。RAN的核心在于如何保证UE与gNB空口上传输信息的安全性、5G基站本身操作维护的网管系统的接口安全性等。

1 5G网络设备的接入安全威胁

5G基站设备，是无线通信网络

中的一部分，存在于 UE 和核心网间，实现无线接入技术。如图 1 所示，5G 基站设备的安全威胁，主要有 4 个方面：一是构成 gNB 的硬件、软件及网络的基础设施的安全威胁；二是针对连接 NG-UE 的空口上传送信息的空口安全威胁；三是针对连接到 5GC 的 N2 和 N3 参考点的传输网络安全和信息的安全威胁；四是对基站连接到网管的管理平面的安全威胁，具体如图 2 所示。

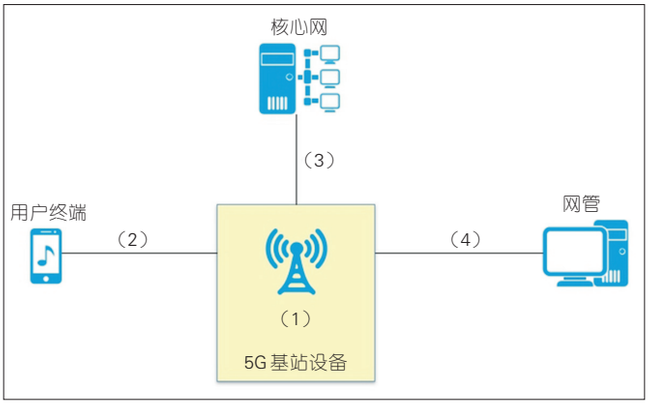


图 2▶
5G基站设备接口

(1)基础设施的安全威胁。

基站设备的基础设备包括部署环境、硬件设备以及基站内部的软件版本、数据、文件等。对于部署环境和硬件，其面临的安全威胁是损坏设备周围环境，如温度、烟雾等，或直接破坏设备的硬件。对于基站内的软件，其面临的安全威胁是非授权登录基站或普通账户登录基站后执行非授权的访问，从而破坏基站的数据、文件等，导致基站功能不可用。

(2)空口的安全威胁。

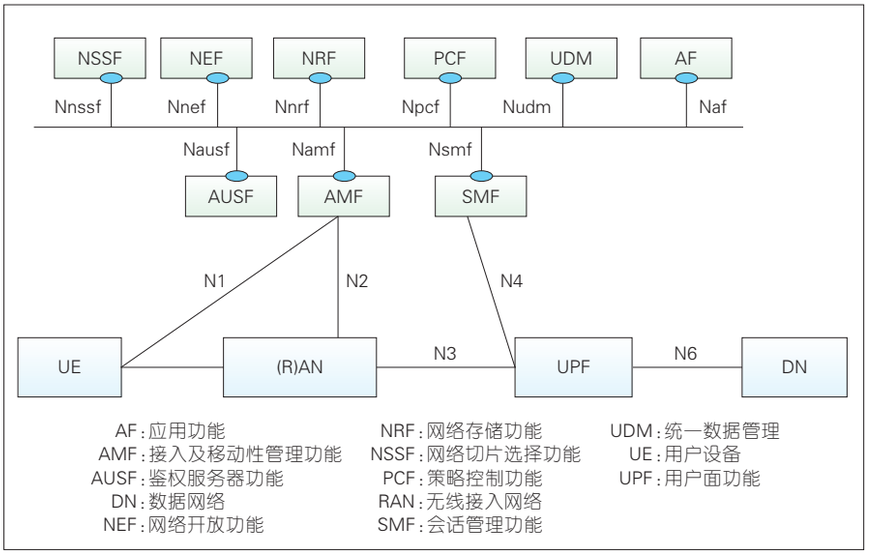
空口指用户终端和基站设备间的空中无线信号传播。空口的安全威胁主要表现为 3 方面：信息泄露，在基站发射信号的覆盖区域，非法用户也能接收，并通过侦听、嗅探、暴力破解等手段获取基站的转发数据，造成信息泄露；数据欺骗，例如伪造虚假的基站发射无线信号，骗取合法用户接入，然后盗取用户数据或实施欺诈；攻击设备发射强干扰信号，破坏正常用户和基站的无线连接，从而造成正常基站的业务中断。

(3)核心网接口的安全威胁。

基站的核心网接口包括基站与核心网、基站与基站间的用户面数据和信令面数据接口，通过以太网传输。因此也会面临与一般 IP 网络相同的安全威胁，包括不安全的网络传输协议引起的数据泄漏，针对网络可用性的攻击（例如拒绝服务（DOS）攻击、广播包攻击，缓冲区溢出等造成基站不能提供正常服务），以及对传输数据篡改破坏数据完整性。

(4)网管接口的安全威胁。

网管接口是后台网管设备与前台基站的管理面数据接口，也通过以太网传输。网管接口的安全威胁首先是网络传输协议。一些不安全的网络传输协议，例如 Telnet、文件传输协议（FTP）、超文本传输协议（HTTP）、简单网络管理协议（SNMP）v1/v2 等不进行加密处理，很容易受到嗅探攻击，导致数据泄漏；第 2 个威胁是账户和密码管理的健壮性，例如密码较弱，就很容易受到字典攻击或暴力破解，基站被非法登录攻击；第 3 个威胁是权限控制管理，如果账户的分级权限控制不好，也会造成非授权用户或授权用户的非授权访问，破坏数据的



▲图 1 5G的网络架构

机密性和完整性；还有就是会话管理控制，例如缺乏最大会话连接数限制，就容易遭受 DOS 攻击，导致系统资源耗尽等。

2 5G 网络设备及接入的安全方案

相比于 2G/3G/4G 在网络上存在的安全弱点，5G 在网络定义和标准还建立过程中，安全性是一个核心问题。5G 的应用场景和网络架构要复杂许多，包括 eMBB 场景下的大容量用户通信保证、uRLLC 场景下的大量物联网设备接入、云化的集中单元（CU）部署、虚拟化的网络架构等，对安全性都有着很大的挑战。

3GPP 33.501[2] 提出 5G 网络安全整体架构，具体如图 3 所示。

图 3 中，（I）是网络访问安全，表示一组安全功能，使 UE 能够安全地通过网络验证和访问服务，包括 3GPP 访问和非 3GPP 访问；（II）是网络域安全，表示一组安全功能，使网络节点能够安全地交换信令数据和用户平面数据；（III）是用户域安全，表示保护用户访问移动设备的一组安全功能；（IV）是应用域安全，表示一组安全性功能，使用户和供应商中的应用程序能够安全地交换消息。

5G 协议引入了用户永久标识符（SUPI）和用户隐藏标识符（SUCI）的概念。更重要的是，5G 规范中引入了基于公钥基础设施（PKI）的安全体系结构，允许验证和鉴别源自 5GC 的控制面消息（CPM）。

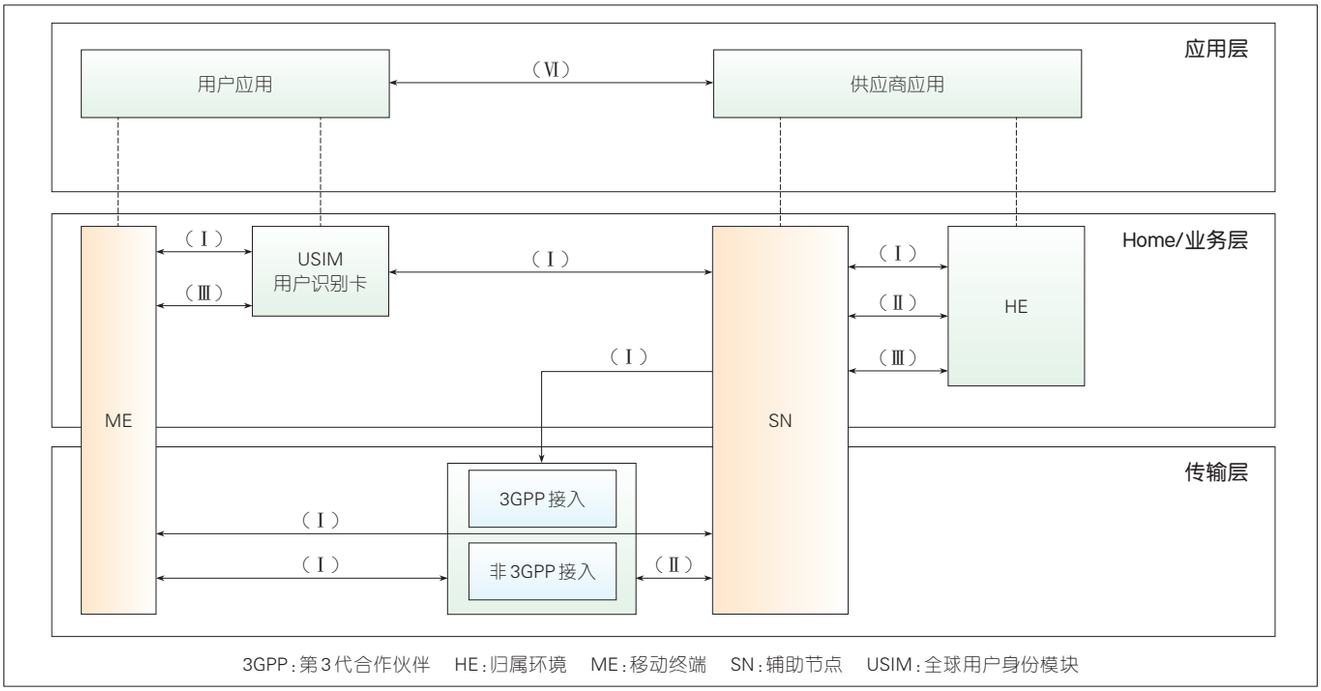
这是 3GPP 协议在 5G 体系架构上的安全考虑。具体地，针对 5G 基站设备及其接入，并根据图 2 所示的 4 个方面的安全威胁，我们分别采用了不同的安全解决方案。

2.1 基础设施的安全方案

基站基础设施的安全，首先要确保对基站设备本身及周围组网设施的物理安全，如设置门禁、监测控制、配备烟雾、温度传感器等，有异常及时通知管理员。

同时，还要做好防火墙配置。基站设备在系统组网中通过 IP 协议连接核心网、网管服务器等网络设备，很容易遭受 IP 网络的攻击，如 DoS、广播包、缓冲区溢出攻击等。通过配置防火墙过滤规则，只提供对外开放的端口/协议列表，不使用的端口缺省拒绝。另外，还可以配置入侵检测系统（IDS），对网络攻击行为及时检测并警报，以尽快采取响应措施。

除了基站硬件和组网环境，基站软件资源具体包括操作系统、软



▲图 3　5G 安全体系结构

件版本、数据存储文件也是重要的基础设施。攻击者会利用操作系统和数据库等漏洞攻击设备，因此需要定期对设备软硬件进行安全威胁分析和评估。每发布一个软件版本，都需要经过第三方软件的安全扫描和评估，以将发现的漏洞和风险及时解决。通过对版本的数字签名来检验版本的合法性，防止被篡改。数据存储文件的安全是通过设置安全存储区，对数据分类（不同分类的数据存储在不同的存储区），并进行严格的访问控制，以确保机密性。例如，基站的机密信息要加密存储，存放在安全存储区，只有管理员权限才能访问。

2.2 空口的安全方案

（1）支持双向认证。

在2G时代，移动终端使用普通用户身份识别卡（SIM），只支持可扩展身份认证协议（EAP）-SIM单向鉴权，即网络对SIM卡进行身份合法性认证，而没有用户终端对网络的认证，这就造成“伪基站”。长期演进（LTE）使用了全新的双向认证方式，使用配置用户识别模块（UIM）的USIM卡，只有都完成网络对终端认证和终端对网络认证后才接入网络。

5G的双向认证流程和LTE变化不大，可以不换卡，不换号，并且使用EAP-认证与密钥协商协议（AKA），支持统一框架下的双向认证。EAP-AKA的认证流程[2]如图4。增加5G-AKA认证，是通过向归

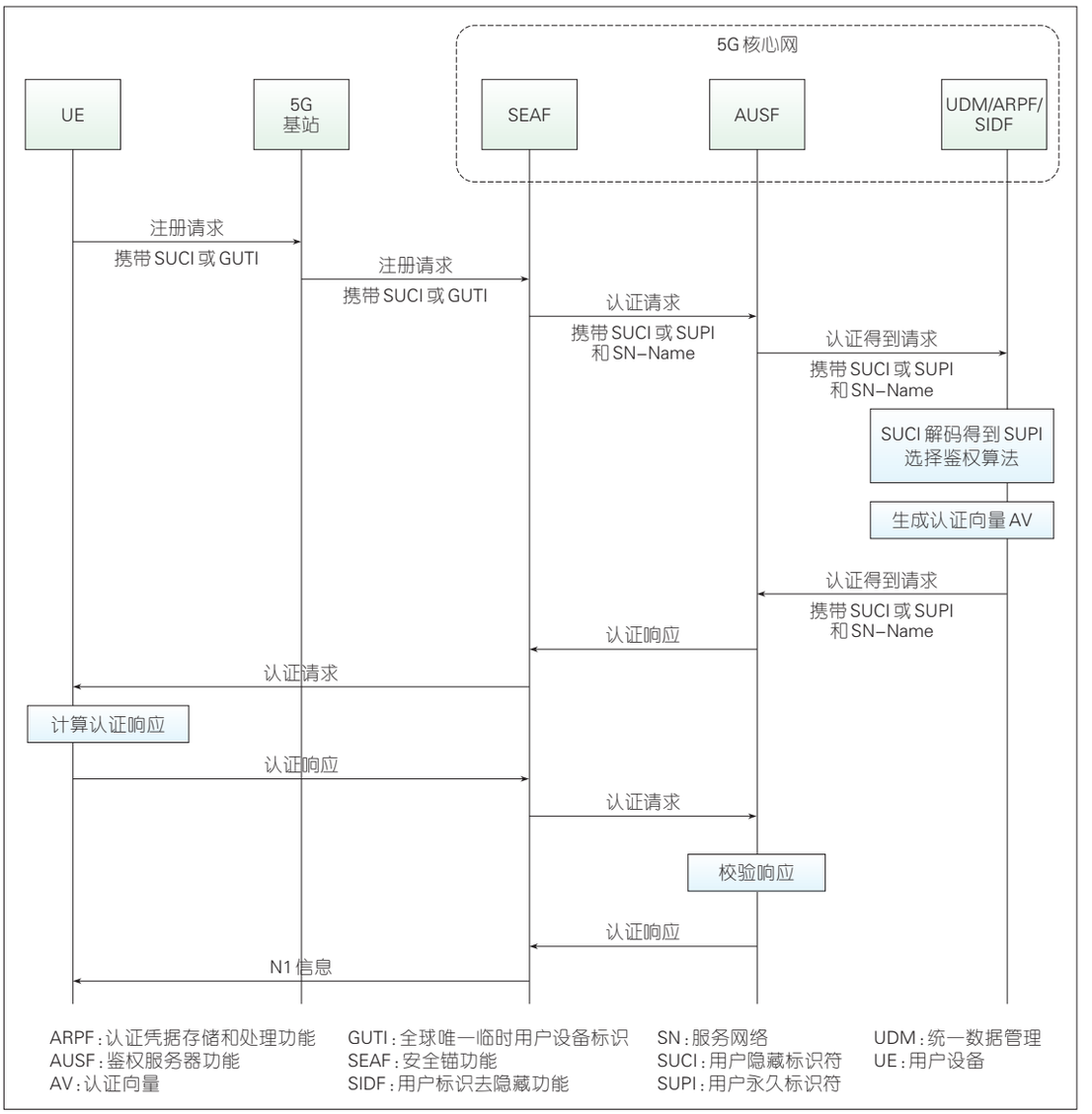


图4▶ 可扩展身份认证-认证与密钥协商协议认证流程

属网络提供UE从访客网络成功认证的证明，来进一步增强EPS-AKA的安全性。

(2)支持数据机密性。

数据加密指发送方通过加密算法将明文数据转换为密文数据，保证数据不被泄露。5G基站根据SMF发送的安全策略激活用户数据的加密，支持NEA0、128-NEA1、128-NEA2、128-NEA3等加密算法，加密算法再由5G基站通过安全模式信令(RRC)指示给UE。加密密钥由UE和5G基站分别生成。

(3)支持数据完整性。

支持数据完整性指发送方通过完整性算法计算出完整性消息认证码(MAC-I)，接收方通过完整性算法进行计算(X-MAC)，再比较MAC-I和X-MAC是否一致，以保证数据不被篡改。

5G基站根据SMF发送的安全策略激活用户数据的完整性保护。完保算法由5G基站通过RRC信令指示给UE。5G基站支持NEA0、128-NEA1、128-NEA2、128-NEA3等完整性算法，发送方采用协商确定的某一完整性保护算法。完保密钥由UE和5G基站分别生成。

2.3 核心网接口的安全方案

5G基站设备的传输安全主要包括N2、N3口的传输安全，并按照开放式系统互联(OSI)七层协议，在不同的协议层都有各自的安全解决方案。

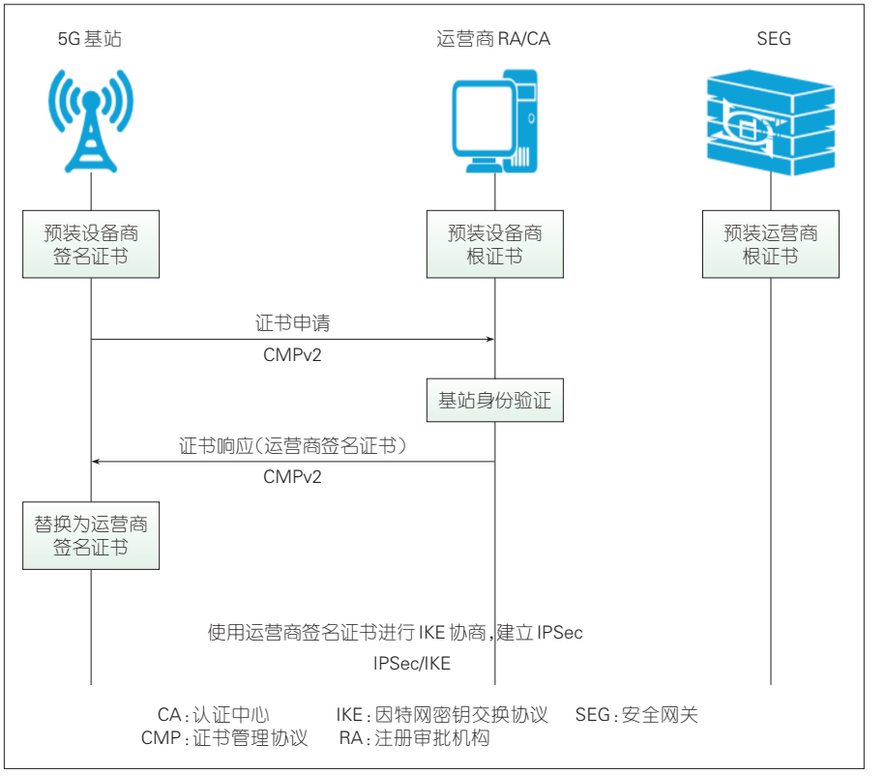
(1)物理层安全。物理层通过线缆屏蔽传输信号，防止外部监测和干扰，同时支持多物理链路和多物理端口冗余备份，提供系统的可用性。

(2)链路层安全。对不同数据平面，链路层使用虚拟局域网(VLAN)隔离，防止DoS攻击和数据嗅探；支持MACSec加密，为用户提供安全的MAC层数据发送和接收服务，包括用户数据加密、数据帧完整性检查及数据源真实性校验；支持802.1x访问控制和认证协议，只有通过有效认证，基站才能接入运营商网络，网络物理端口才对基站开放，以限制未经授权的用户/设备通过接入端口访问局域网(LAN)/无线局域网(WLAN)。

(3)网络层安全。网络层支持IPSec安全隧道协议，提供端到端的加密和认证功能，保证数据的完整性和机密性。通信时和通信对象的密钥交换方式使用Internet密钥交换协议(IKE)、RFC5996、数据传输使用封装安全载荷(ESP)报文格式、RFC4303。

5G规范中引入了基于PKI的安全体系结构，3GPP 33.310协议定义了基站数字证书的注册机制，以及应用数字证书与核心网安全网关(SEG)建立安全通信链路的过程[3]，具体如图5所示。

首先是准备阶段，基站由设备商预先提供出厂生成的公私钥对，并预装由设备商签名的数字证书、运营商的登记授权(RA)/证书授权(CA)服务器预装设备商的根证书、核心网SEG预装运营商根证书。然后基站向核心网注册使用CMPv2协议向RA/CA发起证书申请，RA/CA则使用设备商根证书和



▲图5 5G公钥基础设施安全结构

设备商签名证书来对基站进行身份验证，验证通过后给基站签发运营商证书并返回证书响应，基站证书替换为运营商签名证书，完成基站注册。随后基站就使用运营商签名证书和核心网安全网关建立 IPSec 连接。

2.4 网管接口的安全方案

网管是对基站设备的管理系统完成基本的数据配置、监测控制、性能统计等功能。基站与网管系统通过 IP 网络连接，有可能暴露在公网，因此面临非法入侵、信息泄露、服务中断、物理破坏等安全威胁。和网管接口相关的安全解决方案如下几个方面。

（1）账户管理。

基站系统支持集中账户管理和本地账户管理。集中账户是指由网管创建和管理并集中到网管进行认证的账户，本地账户是由网管创建但在基站本地进行认证的账户。账户管理支持常用的用户名密码方式认证，以及基于 PKI 的数字证书双因素认证方式。

对于使用用户密码认证方式，为避免密码易被破解，系统可以支持强制为系统配置高强度密码，如长度至少 8 位，密码必须至少包含数字、大写字母、小写字母、特殊字符中的 3 类。同时，系统支持检测密码强度是否满足要求，如果密码不满足规则，可以强制用户在登录时修改为高强度密码。

系统还可以根据不同的用户要求，为帐号设置对应的有效期，帐号到了有效期，将不允许再使用。为了避免用户密码被暴力破解，系统支持对登录密码尝试次数做限定，超出尝试次数，用户会被锁定，锁定又支持按照用户来源锁定和按照用户锁定的锁定策略。

（2）权限管理。

对接入系统的用户需要做身份认证，非授权用户不能接入系统。用户接入系统后，还需要进行权限控制，即用户能够读取/修改/执行系统文件是否在授权范围内。系统需要对用户分组，不同等级的用户分组有不同的权限。

登录用户通过身份验证后，可以对 5G 基站设备进行管理操作。基站需要根据用户的分组对用户操作进行授权控制，为用户授予相应的操作权限。系统遵循最小特权和职责分离的原则，为不同职能的用户创建出不同权限的角色。

同样，帐号信息类也有专门的权限控制，只有授予了帐号修改权限的安全管理员才能对帐号以及权限进行配置，避免帐号权限被恶意修改。

（3）传输安全。

系统通过支持安全链路传输数据，使用安全通道协议（SSH）/安全文件传送协议（SFTP）/简单网络管理协议（SNMPv3）协议，以及基于这些协议实现的加密安全通道，确保数据在网络传输过程中难以被窃取和篡改。

采用 SSH/SFTP 协议可以有效地避免远程管理信息泄露问题，及上下层网络管理系统间的数据传输链路信息泄露问题。SSH/SFTP 协议提供的功能包括所有传输数据的加密，防止域名系统（DNS）欺骗和 IP 欺骗，通过数据压缩加快数据传输，并替换 Telnet，为 FTP 提供安全通道[4]。

采用 SNMP V3 协议对数据进行完整性检测，以保证数据不会在传输时被修改或者损坏，并且可以保证传输序列不会被故意修改。数据源的鉴别保证了传输数据和数据源对的一致性。数据加密确保了数据在传输时不会被窃取或者泄露。消息时间序列指的是超出制定时间窗生成的数据不会被接受。在消息重传和消息重新排序时，生成的消息可能会超出制定时间窗。SNMPV3 识别服务用来确定一个消息是否由消息实体识别的用户来发送，是否在传输中被编辑、重传或其传输方向被修改。SNMPV3 加密服务用来对消息实体加密以保证数据不会被直接读取[5]。

（4）敏感信息保护。

依据隐私保护原则，客户的隐私信息需要保密，也就是说没有权限的人不能查看，也无权传播。在必须要传播的某些数据中，如果携带了用户数据，则需要对用户数据做匿名化处理。

个人隐私数据指可以直接或者间接关联到用户个人的信息，如已知用户号码能反查到用户姓名，那么用户号码就是个人隐私。这种关联比较直接，称为直接个人信息。某些信息需要绕几个圈才能关联到用户信息的，称为间接个人信息。

所谓的匿名化指在任何有导出文件的地方，如果涉及到用户隐私

➡下转第 55 页

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。