国 际 电 信 联 盟

ITU-T X.1814

（09/2022）

国际电信联盟
电信标准化部门

X系列：数据网、开放系统通信和安全性

IMT-2020安全

IMT-2020通信系统安全导则

ITU-T X.1814建议书

ITU-T X系列建议书

数据网、开放系统通信和安全性

公用数据网	X.1–X.199
开放系统互连	X.200–X.299
网间互通	X.300–X.399
消息处理系统	X.400–X.499
号码簿	X.500–X.599
OSI组网和系统概貌	X.600–X.699
OSI管理	X.700–X.799
安全	X.800–X.849
OSI应用	X.850–X.899
开放分布式处理	X.900–X.999
信息和网络安全	
一般安全问题	X.1000–X.1029
网络安全	X.1030–X.1049
安全管理	X.1050–X.1069
生物测定	X.1080–X.1099
安全应用和服务（1）	
组播安全	X.1100–X.1109
家庭网络安全	X.1110–X.1119
移动安全	X.1120–X.1139
万维网安全（1）	X.1140–X.1149
应用安全（1）	X.1150–X.1159
对等网络安全	X.1160–X.1169
网络身份安全	X.1170–X.1179
IPTV安全	X.1180–X.1199
网络空间安全	
网络安全	X.1200–X.1229
反垃圾信息	X.1230–X.1249
身份管理	X.1250–X.1279
安全应用和服务（2）	
应急通信	X.1300–X.1309
泛在传感器网络安全	X.1310–X.1319
智能电网安全	X.1330–X.1339
验证邮件	X.1340–X.1349
物联网（IoT）安全	X.1350–X.1369
智能交通系统（ITS）安全	X.1370–X.1399
分布式账簿技术（DLT）安全	X.1400–X.1429
应用安全（2）	X.1450–X.1459
万维网安全（2）	X.1470–X.1489
网络安全信息交换	
网络安全概述	X.1500–X.1519
漏洞/状态信息交换	X.1520–X.1539
事件/事故/启发式信息交换	X.1540–X.1549
政策的交换	X.1550–X.1559
启发式和信息请求	X.1560–X.1569
标识和发现	X.1570–X.1579
确保交换	X.1580–X.1589
网络防御	X.1590–X.1599
云计算安全	
云计算安全概述	X.1600–X.1601
云计算安全设计	X.1602–X.1639
云计算安全最佳做法和指导原则	X.1640–X.1659
云计算安全实施方案	X.1660–X.1679
其他云计算安全	X.1680–X.1699
量子通信	
术语	X.1700–X.1701
量子随机数发生器	X.1702–X.1709
QKDN安全框架	X.1710–X.1711
QKDN安全设计	X.1712–X.1719
QKDN安全技术	X.1720–X.1729
数据安全	
大数据安全	X.1750–X.1759
数据保护	X.1770–X.1789
IMT-2020安全	**X.1800–X.1819**

ITU-T X.1814建议书

IMT-2020通信系统安全导则

概要

联网的物联网（IoT）设备和移动应用需要灵活、安全且能够保护个人隐私的无线网络接入。IMT-2020通信系统的设计应满足此类高级要求。需要为IMT-2020通信系统定义一个安全框架，并可将其作为就IMT-2020安全主题编撰更加详细的技术建议书的基础。

ITU-T X.1814建议书确定了与IMT-2020通信系统安全相关的所有组件，并定义了IMT-2020通信系统的安全导则。它描述了通用IMT-2020架构及其域。此外该建议书还确定了威胁，并规定了每个组件的安全能力要求，同时考虑到了独特的网络特征。本建议书基于3GPP 5G安全架构。

历史沿革

版本	建议书	批准日期	研究组	唯一识别码*
1.0	ITU-T X.1814	2022-09-02	17	11.1002/1000/14992

关键词

能力；IMT-2020通信系统；多接入边缘计算；网络切片；网络虚拟化；安全导则；威胁。

* 欲查阅建议书，请在您的网络浏览器地址域键入URL http://handle.itu.int/，随后输入建议书的唯一ID，例如，http://handle.itu.int/11.1002/1000/11830-en。

前言

国际电信联盟（ITU）是从事电信、信息和通信技术（ICT）领域工作的联合国专门机构。国际电信联盟电信标准化部门（ITU-T）是国际电信联盟的常设机构，负责研究技术、操作和资费问题，并且为在世界范围内实现电信标准化，发表有关上述研究项目的建议书。

每四年一届的世界电信标准化全会（WTSA）确定ITU-T各研究组的研究课题，再由各研究组制定有关这些课题的建议书。

WTSA第1号决议规定了批准建议书须遵循的程序。

属ITU-T研究范围的某些信息技术领域的必要标准，是与国际标准化组织（ISO）和国际电工技术委员会（IEC）合作制定的。

注

本建议书为简明扼要起见而使用的“主管部门”一词，既指电信主管部门，又指经认可的运营机构。

遵守本建议书的规定是以自愿为基础的，但建议书可能包含某些强制性条款（以确保例如互操作性或适用性等），只有满足所有强制性条款的规定，才能达到遵守建议书的目的。“应该”或“必须”等其它一些强制性用语及其否定形式被用于表达特定要求。使用此类用语不表示要求任何一方遵守本建议书。

知识产权

国际电联提请注意：本建议书的应用或实施可能涉及使用已申报的知识产权。国际电联对无论是其成员还是建议书制定程序之外的其它机构提出的有关已申报的知识产权的证据、有效性或适用性不表示意见。

至本建议书批准之日止，国际电联已收到实施本建议书可能需要的受专利保护的知识产权的通知。但需要提醒实施者注意的是，这可能并非最新信息，因此大力提倡他们通过下列网址查询电信标准化局（TSB）的专利数据库：http://www.itu.int/ITU-T/ipr/。

目录

ITU-T X.1814建议书

IMT-2020通信系统安全导则

1 范围

本建议书为IMT-2020通信系统的开发提供了安全导则，其中确定了与IMT-2020通信系统安全相关的所有组件，即用户设备、接入网和核心网。另外这一建议书还描述了通用IMT-2020架构及其域，确定了威胁，并规定了每个组件的安全能力要求，同时考虑到了独特的网络特征，例如多接入边缘计算、软件定义网络、动态网络功能虚拟化和网络切片。本建议书基于3GPP 5G安全架构。

2 参引

下列ITU-T建议书和其他参引的条款，通过在本建议书中的引用而构成本建议书的条款。在出版时，所指出的版本是有效的。所有的建议书和其他参引均会得到修订；因此本建议书的使用者应查证是否有可能使用下列建议书和其他参引的最新版本。当前有效的ITU-T建议书清单定期出版。

本建议书引用某个文件，并非意味着该文件作为单独文件出现时具备建议书的地位。

[ITU-T X.800] ITU-T X.800建议书（1991年），CCITT应用的开放系统互连（OSI）安全体系结构

[ITU-T X.1038] ITU-T X.1038建议书（2016年），软件定义网络的安全要求和参考体系结构

3 定义

3.1 他处定义的术语

3.1.1 本建议书使用[ITU-T X.800]中的以下术语：

– 接入控制（access control）；

– 认证（authentication）；

– 可用性（availability）；

– 保密性（confidentiality）；

– 数据完整性（data integrity）；

– 隐私（privacy）；

– 否认（repudiation）；

– 安全服务（security service）。

此外，本建议书使用了他处定义的以下附加术语：

3.1.2 控制（control）[b-ITU-T X.1408]：修改风险的措施。

注1 – 控制包括修改风险的任何过程、策略、设备、规程或其他行动。

注2 – 控制有可能不总是发挥预期或假定的修改效果。

3.1.3 分布式拒绝服务（DDoS）攻击[b-ITU-T Y.4807]：未经授权访问系统资源或延迟系统操作和功能，危害多个系统以淹没目标系统的带宽或资源，导致授权用户无法使用。

3.1.4 指南[b-ITU-T X.1401]：说明应该做什么和如何做，以实现策略中规定的目标。

3.1.5 网络功能[ITU-T Y.3100]：IMT-2020背景下网络中的一种处理功能。

注1 – 网络功能包括但不限于网络节点功能，例如会话管理、移动性管理和传输功能，其功能行为和接口已定义。

注2 – 网络功能可以在专用硬件上实现，也可以作为虚拟化软件功能实现。

注3 – 网络功能不是资源，而是可以使用资源进行实例化的任何网络功能。

3.1.6 网络功能虚拟化[b-ITU-T X.1811]：一种技术，支持在共享物理网络上创建逻辑隔离的网络分区，以便多个虚拟网络的异构集合可在共享网络上同时共存。

3.1.7 网络切片[b-ITU-T Y.3100]：提供特定网络能力和网络特性的逻辑网络。

注1 – 网络切片支持定制网络的创建，为不同市场场景提供灵活的解决方案，这些场景在功能、性能和资源分配方面有不同要求。

注2 – 网络切片可能具有公开其功能的能力。

注3 – 网络切片的行为是通过网络切片实例实现的。

3.1.8 编排[b-ITU-T Y.3100]：在IMT-2020的背景下，旨在通过优化标准为物理和虚拟基础设施自动安排、协调、实例化和使用网络功能和资源的过程。

3.1.9 安全能力[b-ISO 81001-1]：类别广泛的技术、行政或组织控制，用于管理数据和系统的保密性、完整性、可用性和问责制风险。

3.1.10 供应商[b-ISO 10393]：提供产品或服务的组织或个人。

3.1.11 系统[b-ISO/IEC 27000]：应用、服务、信息技术资产或其他信息处理组件。

3.1.12 威胁[b-ITU-T X.1406]：意外事件的潜在原因，可对系统或组织造成损害。

3.1.13 虚拟化网络功能[b-ITU-T Y.3150]：一种网络功能，其功能软件与硬件分离，并在虚拟机上运行。

3.2 本建议书中定义的术语

本建议书定义了以下术语：

3.2.1 域：基于与IMT-2020网络相关的物理或逻辑方面的一组网络实体。

3.2.2 IMT-2020通信系统：为IMT-2020服务管理IMT-2020通信过程的系统。

注1 – 5G指ITU-T所述IMT-2020。

注2 – IMT-2020通信系统与本建议书中的IMT-2020系统相同。

3.2.3 IMT-2020生态系统：一组利益攸关方相互作用，形成一个稳定运行的IMT-2020系统。

注 – 这主要依赖于IMT-2020通信技术，在该技术中，一个生命体社区包含生产者、消费者和供应商，他们贡献了大量的产品、技术和专业知识，以使IMT-2020系统在基础设施、网络、平台、服务和应用等不同层面上工作。

3.2.4 IMT-2020业务：IMT-2020生态系统提供的一项益处。

3.2.5 流表溢出攻击：消耗转发和处理流的数据包的流表的攻击，导致没有空间留给其他流来安装流规则，从而导致网络拒绝服务（DoS）。

4 缩写词和首字母缩略语

本建议书使用下列缩写词和首字母缩略语：

4G 第四代移动通信技术

AMF 接入和移动性管理功能

API 应用编程接口

AUSF 认证服务器功能

C-PDU 控制协议数据单元

CU/DU 中央单元/分布式单元

DCI 数据中心互连

DDoS 分布式拒绝服务

DoS 拒绝服务

eMBB 增强型移动宽带

FAT 文件分配表

IMSI 国际移动用户标识

IMT-2020 国际移动通信-2020

IoT 物联网

LTE 长期演进

MAC 消息认证码

MEC 多接入边缘计算

MEHW 移动设备硬件

mIoT 海量物联网

mMTC 海量机器类通信

MNO 移动网络运营商

NAS 非接入层
NF 网络功能
NFV 网络功能虚拟化
NFVI 网络功能虚拟化基础设施
NRF 网络功能存储库功能
OAM 运营、行政和管理
O&M 运营和管理
PII 个人身份信息
PSK 预共享密钥
RA/CA 注册机构和认证机构
RRC 无线资源控制
SBA 基于服务的架构
SBI 基于服务的接口
SDN 软件定义网络
SMF 会话管理功能
SQL 结构化查询语言
SSL 安全套接字层
TA 信任锚
TLS 传输层安全
TMSI 临时移动用户身份
TPM 可信平台模块
UDM 统一数据管理
UE 用户设备
UICC 通用集成电路卡
URLLC 超可靠性和低延迟通信
USIM 通用用户识别模块
VM 虚拟机
VNF 虚拟网络功能
VoIP IP电话

5 惯例

在本建议书中，关键词“应该”是指一项建议的并非需绝对遵守的规范。因此，声称合规不一定使用本规范。

6 IMT-2020通信系统安全概述

6.1 简化的IMT-2020架构

本节概述IMT-2020通信系统安全问题。联网的移动设备和移动应用需要灵活、安全和可信的无线网络接入。IMT-2020通信系统的设计应满足此类高级要求。

IMT-2020通信系统由连接到IMT-2020接入网的设备组成，该接入网又连接到系统的其余部分，这被称为IMT-2020核心网。

图1显示了简化的3GPP 5G系统架构。IMT-2020接入网包括3GPP无线基站和/或非3GPP接入网。IMT-2020核心网架构在支持云实现和物联网（IoT）方面明显优于4G，在网络切片和基于服务的架构（SBA）方面有重大改进。

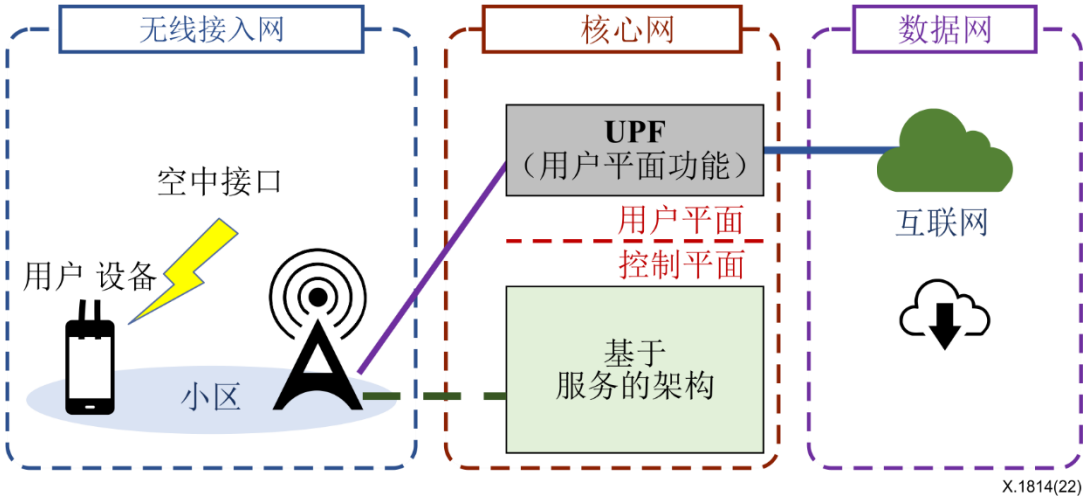


图1 – 简化的IMT-2020架构

6.2 IMT-2020系统的总体架构

IMT-2020系统旨在提供具有不同性能要求的广泛服务。根据3GPP规范，IMT-2020网络中提供的服务可以分为三类：(1) 增强型移动宽带（eMBB）支持比第四代移动通信技术/长期演进网络（4G/LTE）更高的数据速率和更高的用户移动性；(2) 海量物联网（mIoT）提供海量机器类通信；(3) 超可靠性和低延迟通信（URLLC）支持可靠性要求更高和更低延迟的任务关键型服务。IMT-2020系统将成为一个灵活的平台，支持新的业务案例，并整合汽车、制造、能源、电子卫生和娱乐等垂直行业。此外，与前几代移动网络相比，IMT-2020系统的部署和维护将更加容易。为了解决此类具有挑战性的要求，IMT-2020系统引入了许多创新技术，如网络切片、网络功能虚拟化（NFV）、软件定义网络（SDN）、基于服务的架构（SBA）和中央单元/分布式单元（CU/DU）分离。

IMT-2020系统的总体架构[b-ITU-T X.1811]如图2所示，根据所需功能其中包括传输层、网络层、服务层和管理平面。

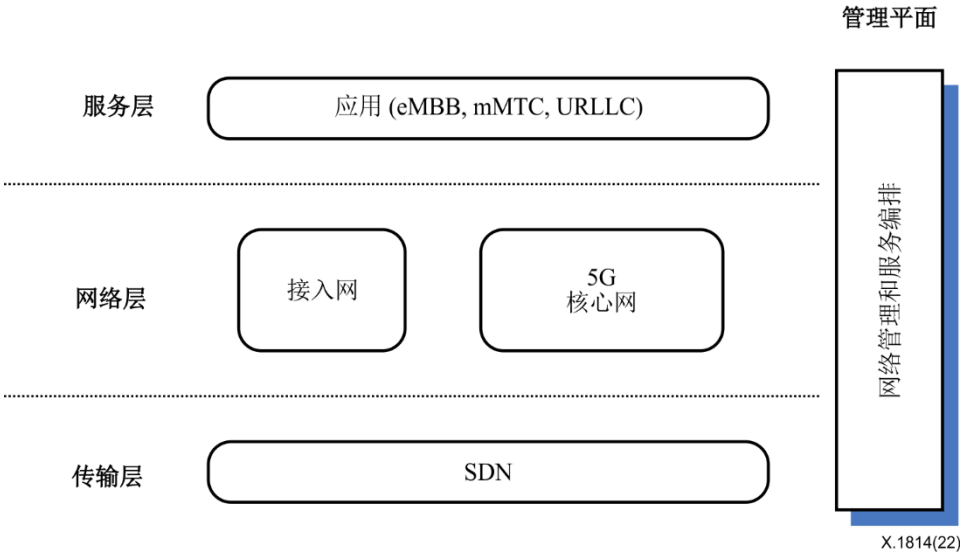


图2 – IMT-2020系统的总体架构[b-ITU-T X.1811] [b- TS 33.501]

- 传输层：用于将数据包从源传输到目的地。除了传统的传输技术（例如多协议标签交换），IMT-2020系统还引入了SDN技术，以提高传输速度并更轻松地适应服务需求。
- 网络层：由接入网和核心网组成。前者允许UE接入IMT-2020网络。后者的设计考虑到了SBA的可扩展性和简单性。它由许多支持数据连通性和业务部署的网络功能组成。网络功能的示例包括认证服务器功能（AUSF）、接入和移动性管理功能（AMF）以及会话管理功能（SMF）。
- 服务层：由运行在IMT-2020系统顶层的应用组成，可能是eMBB、mMTC或URLLC应用。
- 管理平面：负责网络管理和业务编排。

6.3 IMT-2020系统的域

IMT-2020安全应该根据域、层、安全需求和安全能力来定义。

域是基于与IMT-2020网络相关的物理或逻辑方面的一组网络实体。切片域的概念用于捕获网络切片方面。它可以代表IMT-2020网络中的不同功能、服务和参与者。图3显示了典型的IMT-2020域。

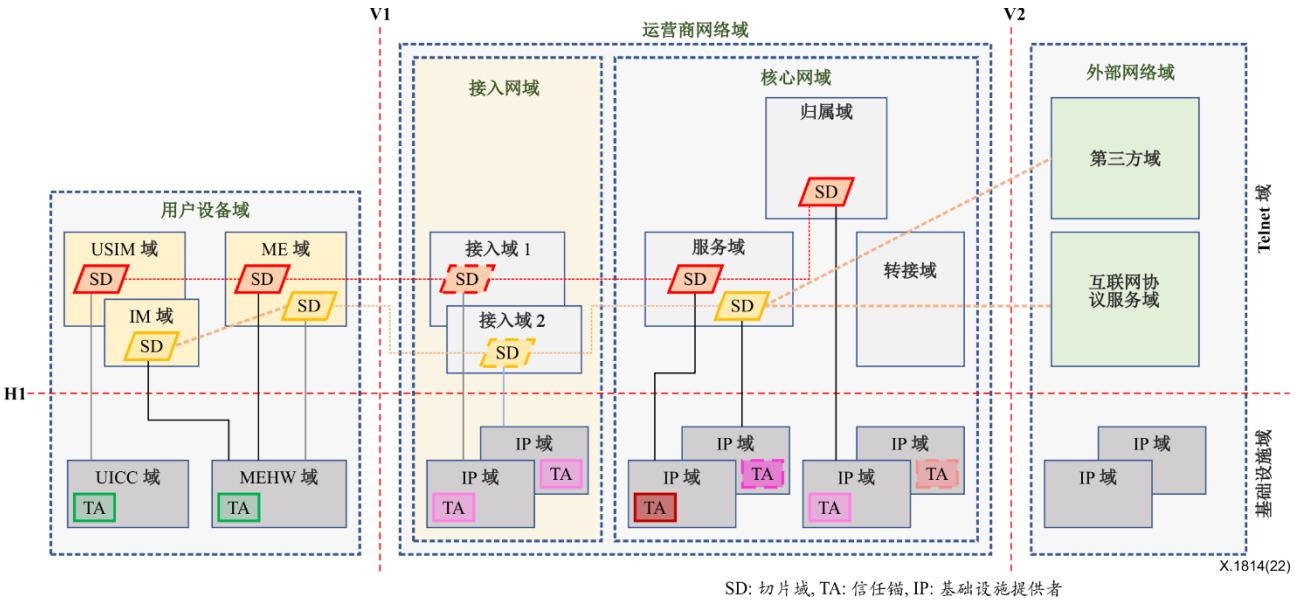


图3 – 典型的IMT-2020域

图3中位于H1线上方的网元代表逻辑网络的各个方面，称为租户域，位于H1线下方的网元代表物理网络的各个方面，称为基础设施域。V1线将用户设备（UE）域与接入网域分开，V2线进一步将核心网络域与外部网络域分开，例如运营商网络使用的互联网协议服务。

基础设施域包含由硬件和软件实现的网元，此类网元充当基础设施提供者。这其中包括管理程序（hypervisors）（创建和运行虚拟机的软件）以及信任锚，即信任被假定而非派生的权威实体[b-ITU-T X.509]。

在H1线下的UE侧，UE域由通用集成电路卡（UICC）和移动设备硬件（MEHW）域组成，前者提供防篡改模块，后者提供包括可信执行环境在内的硬件支持。

在网络侧线H1下，有一个基础设施提供者（IP）域，其中包括特定的接入（无线）硬件以及核心功能所需的计算、存储和联网的一组硬件。

信任锚（TA）用于为虚拟化系统提供信任。这包括确保租户域的完整性，以及租户域在指定的可信基础设施上执行。TA还可用于验证基础设施域的完整性，并将租户域绑定到基础设施域。

租户域包含几个使用基础设施域的逻辑域，例如执行其功能。在UE侧，租户域包括移动设备、通用用户识别模块（USIM）、驻留在硬件部分中的几个软件应用之一，称为UICC，用于存储用户相关信息，并实现与用户侧和身份管理域上的认证和加密相关的安全功能。网络侧的租户域包括接入（A）、服务（S）、归属（H）、中转（T）、第三方（3P）、互联网协议服务和管理（M）域。

6.4 总体安全要求和能力

本节款总结了[b-ITU-T X.805]描述的一般安全方面（要求）。本节的目的是为IMT-2020系统的安全能力提供基础。附录I提供了用于提供端到端网络安全的通用网络安全体系结构。

安全层是指网络设备和设施分组的层次结构[b-ITU-T X.805]。

安全层由与一个或几个域所提供服务的一个方面相关的一组协议、数据和功能组成。IMT-2020安全架构层提供了协议、数据和功能的高级视图，此类协议、数据和功能在某种意义上是相关的，它们暴露于共同的威胁环境中，并表现出相似的安全要求。对用户设备和无线接入网之间的通信而言，常见的威胁包括无线电干扰、伪基站攻击、空中用户平面数据注入和欺骗性无线资源控制（RRC）消息。另一方面，对UE和核心网之间的通信而言，常见的威胁则包括对订阅标识符的跟踪、欺骗性控制平面消息以及对安全能力的篡改等。IMT-2020网络中管理服务的常见威胁示例包括未经授权的配置更改、网络密钥和证书的泄露以及恶意网络功能的动态添加等。管理层包括与传统网络管理相关的方面（配置、软件升级、系统用户账户管理、日志收集/分析等）以及尤其值得关注的安全管理方面（安全监控审计、密钥和证书管理等）。此外，涉及虚拟化管理和服务创建/组合（编排、网络切片管理、隔离和虚拟机（VM）管理等）的方面亦属于这一层。

安全区域扩展了安全域且一个安全区域需要遵守一个或多个层或域的安全要求。

安全能力通常被定义为类别广泛的技术、行政或组织控制，以管理数据和系统的保密性、完整性、可用性和问责制风险[b-ISO 81001-1]。它指的是针对一个安全方面（如完整性）的安全功能和机制（包括安全措施和对策）的集合，其中包含安全功能和机制，以避免、检测、阻止、抵消和最小化IMT-2020网络的安全风险，特别是网络的物理和逻辑基础设施、其服务、UE、信令和数据的风险。表1提供了各安全域的安全要求。

表1 – 各安全区域的安全要求

安全区域	安全要求
接入网	确定与接入层和域相关的安全要求，以应对与该域相关的威胁。此类要求的示例包括用户计划和控制层数据的保密性和完整性保护以及安全移动性。
应用或服务	确定提供最终用户应用和服务（例如VoIP、VoLTE）的应用层的安全要求，以应对与该域相关的威胁。此类要求的示例包括用户使用应用和安全服务发现的认证和授权。
管理	确定管理层和管理域的安全要求，以应对与该域相关的威胁，包括安全管理（如安全升级、安全编排）和安保管理（即监控、密钥和接入管理）。
用户设备	确定与UE域相关的安全要求，包括设备的接入控制，以处理与该域相关的威胁。此类要求的示例包括与网络之间的相互认证以及安全环境的安全存储。
网络	确定与核心网以及运营商网络和外部网络之间的通信相关的安全要求，包括与运营商和外部网络域中的节点之间安全地交换信令和最终用户数据相关的方面。例如网络安全、用户隐私和订户认证。
基础设施和虚拟化	确定IP域的安全要求，例如，用于租户域之间以及租户域和基础设施域之间的证明、安全切片/隔离和信任问题。

表2描述了各安全维度的安全能力[b-ITU-T X.805]。其中七项（即身份和接入管理、认证、不可否认性、保密性、完整性、可用性和隐私性）均来自[b-ITU-T X.805]，其他三项（即审计[b-ITU-T X.800]、信任和保证以及合规性）则是IMT-2020安全架构中的安全维度。

表2 – 安全能力

安全维度	安全能力
身份和接入管理	安全能力是指用于接入控制和凭证及角色管理的安全功能和机制（包括安全措施和对策）的集合。
认证	安全能力是指用于认证的安全功能和机制（包括安全措施和对策）的集合，用于验证用户的认证属性的有效性，例如所声明的身份。
不可否认性	安全能力是指用于不可否认服务的安全功能和机制（包括安全措施和对策）的集合，该服务防止对参与特定行动的错误否认。
保密性	安全能力是指安全功能和机制（包括安全措施和对策）的集合，用于保护数据免受未经授权的披露。
完整性	安全能力是指完整性服务的安全功能和机制（包括安全措施和对策）的集合，用于保护数据不被创建或修改。
可用性	安全能力是指用于资源可用性的安全功能和机制（包括安全措施和对策）的集合，即使在存在攻击的情况下也是如此。备灾机制包括在分类中。
隐私性	安全能力是指用于隐私服务的安全功能和机制（包括安全措施和对策）的集合，隐私服务用于向实体提供确定其将交互和共享其个人身份信息的程度的权利。
审计	安全能力是指审计服务的安全功能和机制（包括安全措施和对策）的集合，审计服务提供对系统记录和活动的审查和检查，以确定系统能力的充分性，并检测系统安全和能力方面的漏洞。此外，亦包括对收集数据的审计。
信任和保证	安全能力是指用于信任和保证服务的安全功能和机制（包括安全措施和对策）的集合，信任和保证服务用于传达有关系统可信度的信息。
合规性	安全能力是指用于合规性服务的安全功能和机制（包括安全措施和对策）的集合，其允许实体或系统履行合同或法律义务。

7 IMT-2020通信系统的组件和可信度

7.1 IMT-2020组件

联网的IoT设备和移动应用需要灵活、安全且能够保护个人隐私的无线网络接入。设计IMT-2020通信系统应满足[b-ITU-T Y.3101]子条款7.8和7.9中描述的要求。IMT-2020网络包括四个组件：UE、无线接入网、传输网和核心网，如图4所示。

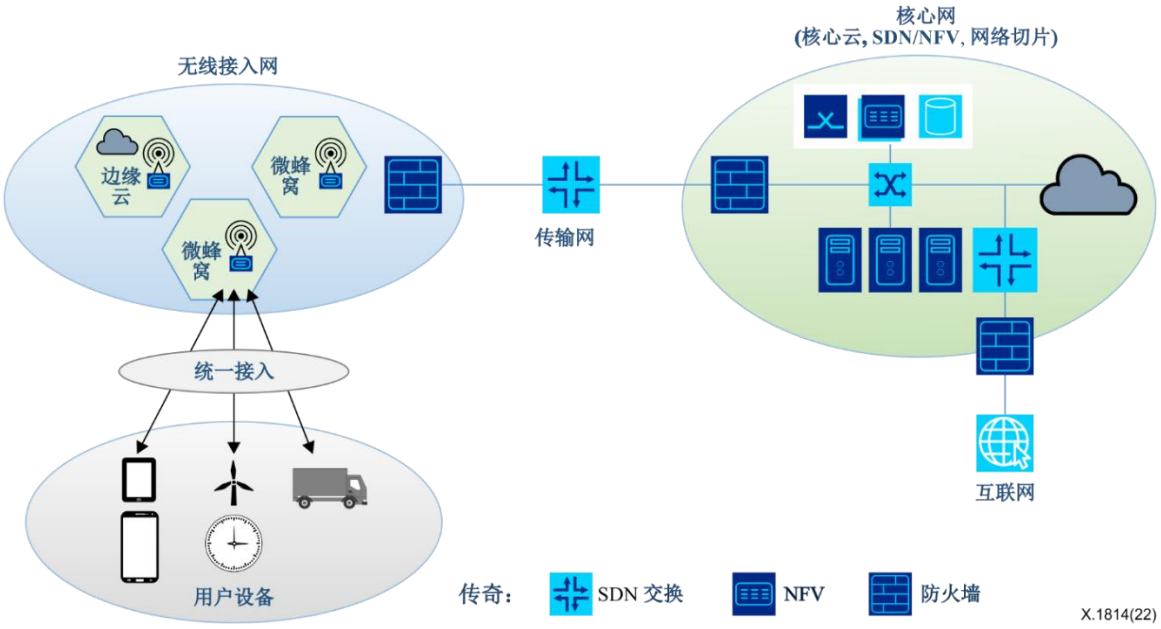


图4 – IMT-2020通信网络（源自[b-ITU讲习班]）

IMT-2020系统将建立在移动云、SDN、NFV和网络切片之上，以应对大规模连接、灵活性和成本最小化的挑战。因此，需要为NFV、网络切片和边缘云计算确定安全措施。

NFV将网络功能从专有硬件设备中分离出来，作为软件在虚拟机中运行

虚拟网络功能（VNF）是NFV的逻辑结果，它是一种网络功能，其功能软件与硬件分离，并在VM上运行[b- ITU-T Y.3100]。VNFs执行特定的网络功能，例如防火墙、交换、入侵检测系统和入侵保护系统。

网络切片是虚拟网络架构的一种形式，利用固定网络中SDN和NFV背后的原理。IMT-2020网络又被分为虚拟网络，每个虚拟网络针对一个业务案例进行了优化，故称为网络切片。它们可以跨越多个网络域，包括接入、核心和传输，并在多个运营商中部署，如图5所示

SDN是一种旨在使网络变得敏捷和灵活的架构。SDN的目的是通过支持公司和网络服务提供商快速响应不断变化的业务需求来改善网络控制。

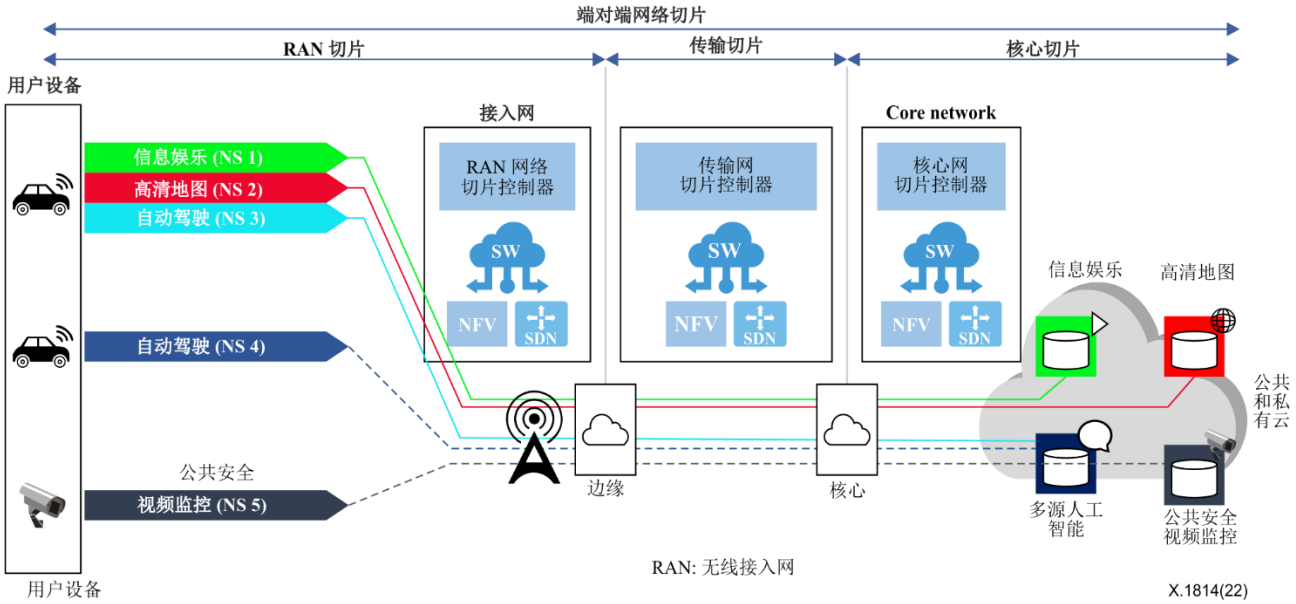


图5 – IMT-2020网络切片

IMT-2020传输网络是提供移动IMT-2020的IP传输基础设施。

边缘计算将云计算的能力推到IMT-2020网络的边缘。边缘计算是一种分布式计算模式，其中计算主要或完全在被称为智能设备或边缘设备的分布式设备节点上执行，而不是以集中式云环境执行为主。边缘计算使数据的处理和存储更接近设备。这使得物联网设备能够低延迟地提供服务

7.2 IMT-2020通信系统的可信度

IMT-2020通信系统的可信度有五个属性，即复原力、通信安全、身份管理、隐私和安全保证：

- 快速恢复能力：指某组织抵御网络中断所产生影响的能力。IMT-2020中各种互补和部分重叠的功能，有助于实现IMT-2020通信系统对网络攻击和非恶意事件的快速恢复能力。
- 通信安全：适用于IMT-2020中的数据通信。在IMT-2020系统中，设备及其自身基础设施的安全通信至关重要。
- 身份管理：指管理IMT-2020域内中已知身份属性的生命周期、值、类型和可选元数据的过程及策略。无论是否漫游，均应为识别和验证用户提供安全的身份管理，确保只有真正的用户才能获取网络服务。它应建立在强大的加密原语和安全特性之上。
- 隐私：在[b-ISO/TS 21719-2]中，数据隐私被定义为个人和组织在收集、使用、保留、披露和处置个人信息方面的权利和义务。隐私要保护个人可识别信息（PII）以防被未经授权方用于识别用户。
- 安全保证：安全保证是相信已经或将满足安全目标的理由的依据。安全保证是确保网络设备满足安全要求的一种手段，是在安全开发和产品生命周期流程后执行的。

8 对组件和功能的威胁

图6所示为IMT-2020系统中的典型威胁。这些威胁分为三类：众所周知的来自软件漏洞、配置错误和泛洪攻击的威胁；来自基础设施共享的威胁；以及来自网络层面的威胁，如与SDN、NFV、网络切片、云计算相关的威胁。

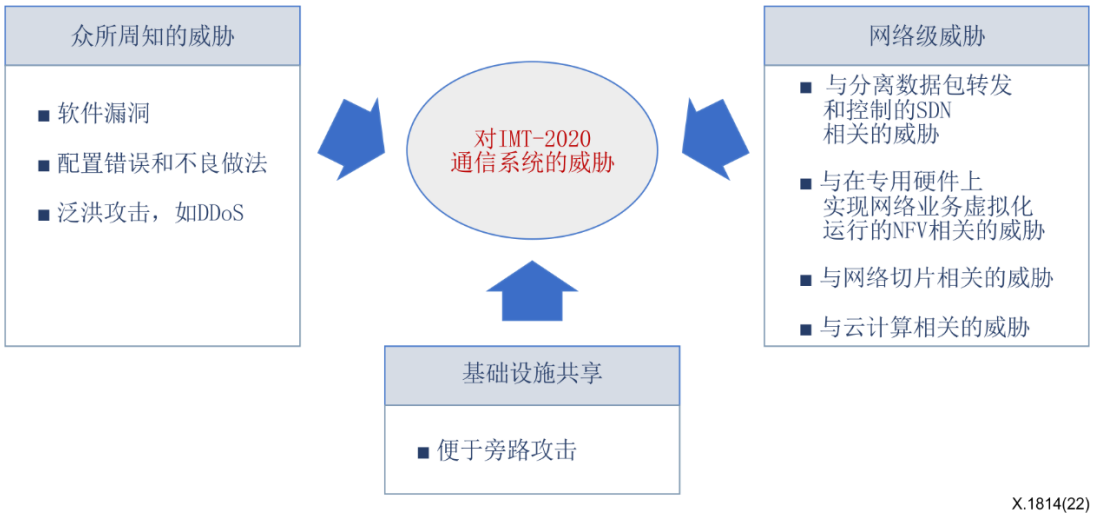


图6 – IMT-2020中的典型威胁[b-ITU讲习班]

8.1 一般威胁

下列为[b-ENISA]中确定的一般威胁：

- **拒绝服务（DoS）**[b-ENISA]：这种攻击企图通过用大量请求淹没网络服务来暂时或无限期地干扰或破坏网络服务，从而使目标用户无法使用网络资源。这类威胁花样繁多，如泛滥、放大、信号风暴和饱和攻击等，可能会导致DoS。常见的DoS攻击包括：(1)缓冲溢出攻击 – 最常见的DoS攻击。其概念是向一个网络地址发送的流量超出程序员设计系统的处理能力。它包括下面列出的攻击，以及其他旨在利用特定应用程序或网络漏洞的攻击。(2)ICMP flood – 通过发送欺骗数据包来利用错误配置的网络设备，这些数据包会敲击目标网络上的每台计算机，而不仅仅是一台特定的计算机。网络被触发后放大流量。这种攻击也称为smurf攻击或死亡ping。(3)SYN flood – 发送连接到服务器的请求，但从不完成握手。一直持续到所有打开的端口都被请求塞满，没有端口可供合法用户用来进行连接。
- **分布式拒绝服务（DDoS）**[b-ENISA]：DDoS攻击是指多个系统针对单个系统进行DoS攻击，对单个目标进行同步DoS攻击。本质区别是，不是从一个位置攻击，而是从多个位置同时攻击目标。
- **数据破坏、泄露、窃取、破坏和操纵信息**[b-ENISA]：这包括通过未经授权访问系统和/或网络窃取PII，未经授权获取和可能发布私人数据/生物识别/医疗数据、组织机密信息或政府/国家相关信息。诸如用户凭证、加密密钥、网络安全日志、软件配置等其他类型数据的窃取、破坏或泄露也可能会帮助攻击者进行各种类型的攻击。
- **窃听**[b-ENISA]：窃听是一个术语，指未经授权拦截信息。在这种威胁中，入侵者企图篡改各种IMT-2020网络元素（SDN控制器、网络功能、边缘节点、虚拟化协调器）的应用层和通信层。它包括窃听用户数据、机密信息、系统时间、用户位置、

电子消息和网络上转发的数据信号。威胁者监视、偷窥和/或窃听组织，以跟踪位置或访问敏感信息。

- **利用软件和硬件漏洞**[b-ENISA]：这种类型的威胁使恶意攻击者能够利用未知的（卖家和用户）软件或硬件漏洞或已知但未修补的漏洞发起攻击。例如，利用已知的硬件和软件缺陷，如崩溃和缓冲溢出。还包括利用与前几代移动通信相关的其他已知漏洞。

- **恶意代码或软件**[b-ENISA]：恶意代码是一个术语，是指软件系统或脚本的任何部分中旨在对系统造成不良影响、安全漏洞或损害的任何代码。威胁包括安装和分发恶意软件，或者在产品或更新中植入特定代码或软件。恶意的软件包括恶意软件、勒索软件、病毒、蠕虫、特洛伊木马、SQL（结构化查询语言）注入[b-SQL]、流氓安全软件、流氓软件和爱心软件。例如，IMT-2020环境中，使用未授权的VNF可以随意安装并将其自身注册到核心网络中以揭露恶意API，也是一种恶意软件。

- **被损害的供应链、供应商和服务提供商**[b-ENISA]：如果供应链、供应商和服务提供商受损害，这使得供应商能够在产品中插入隐藏的硬件、恶意软件和软件缺陷。它还使他们能够实现不受控制的软件更新，操纵功能，包括逃避审计机制的功能和后门。

  如果在产品测试、维护、配置和操作期间涉及第三方的不可信人员，为执行维护活动和提供技术支持，他们能够访问网络管理设施（本地和通过远程接口）。这种网络操作、管理和运行（OAM）的访问特权为这些人员提供了访问各种类型数据的机会，例如用户、系统和网络配置数据以及遥测数据。

- **定向威胁**[b-ENISA]：定向威胁来自针对特定组织或行业的恶意软件。这是一种令人十分担忧的犯罪软件，因为它的意图是获取敏感信息。这种攻击手段十分老道或持久性很强的威胁可能针对敏感信息或敏感和关键服务的可用性。

- **利用安全、管理和操作程序中的缺陷**[b-ENISA]：虽然这与IMT-2020没有直接关系，但当涉及复杂的技术和需要在管理网络时使用操作程序时，这种威胁会变得十分重要。这种威胁包括但不限于利用网络的运行和安全管理、软件的配置、更新和补丁管理中的缺陷。运行和安全程序的缺乏或设计不当所导致的错误可能会影响网络的完整性和可用性。

- **滥用认证**[b-ENISA]：这种威胁可能会影响多个网络入口点，如UE（移动设备和物联网）、运营和管理接口、漫游和垂直服务。这种威胁涉及窃取用户凭据、暴力破解用户帐户、破解密码、掩盖用户身份和损害物联网分组认证，这些都是威胁者滥用IMT-2020认证系统所使用的技术。

- **身份盗窃或欺骗**[b-ENISA]：身份盗窃是指故意使用另一个实体的身份。当恶意攻击者成功确定合法实体的身份，然后伪装成合法实体发动进一步攻击时，这就会成为一种威胁。身份欺骗是指冒充其他实体的身份，然后使用该身份来实现目标的行为。身份欺骗是一种可以影响任何软件组件或人工代理的威胁。在这种攻击中，攻击者假冒合法控制器的身份，并与合法控制器控制的网络功能（即数据平面的元素）进行互动，以触发若干其他类型的攻击（发动网络流、转移流量等）。社会工程和暴力破解用户帐户/密码也可能被用作欺骗或窃取用户凭证的技术。例如，国际移动用户身份（IMSI）捕获攻击可用于通过捕获用户UE的IMSI来揭示用户的身份。这种攻击也可以通过设置伪基站进行实施，对已失去访问移动用户临时身份

（TMSI）的UE来说，伪基站被认为是优选基站。用户将使用他们的IMSI进行响应。此外，IMT-2020网络有不同的参与者，如虚拟移动网络运营商（VMNOs）、通信服务提供商（CSP）和网络基础设施提供商。

8.2 对用户设备的威胁

现已查明UE面临以下安全威胁：

- **恶意软件感染**[b-ENISA]：如果在UE上安装了恶意软件，攻击者可能会利用被感染的UE发起某种攻击，例如窃取UE内部的个人数据、启动DDoS或试图感染其他UE。恶意的软件包括恶意软件、勒索软件、病毒、蠕虫、特洛伊木马和流氓安全软件。一旦恶意软件感染了UE，移动端点就作为僵尸网络被纳入进来。
- **来自僵尸网络的威胁**[b-Khan]：僵尸网络是一种恶意软件，可以控制一组联网设备。移动僵尸网络可以针对许多移动端点自动对IMT-2020系统发起各种攻击（例如DoS）。随着IMT-2020将高算力移动电话互联，这些威胁正在增加。此外，物联网设备的连接开辟了新的威胁类型。因此，物联网设备容易受到物联网僵尸网络的攻击。例如，Mirai未来组合僵尸网络，它在2016年影响了数百万台IP摄像机。
- **来自移动恶意软件的威胁**[b-Khan]：移动恶意软件可以允许攻击者窃取存储在移动设备上的PII数据，甚至发起针对其他实体（如其他UE、移动接入网和移动运营商核心网络）的攻击（如DoS攻击）。
- **未经授权访问和破坏、公开或修改用户和信令数据**：攻击者可以获得UE和下一代节点B之间传送的用户和信令数据的未授权访问，或者对其进行破坏、公开或修改。
- **篡改订阅凭证**：攻击者可以篡改用于身份验证和机密性的订阅凭证。

8.3 对接入网的威胁

现已发现接入网面临以下安全威胁：

- **恶意或意外高流量**[b-NGMN]：随着网络容量和UE项目数量的增加，因大型事件导致的意外或恶意网络流量模式发生巨大变化的风险很高。在这种规模下，无法辨别网络激增的意图，因此防止恶意事件就成了主要目标，但包括这两种情况。
- **运营商链路之间的密钥泄漏**[b-NGMN]：空中接口加密（有时是完整性）密钥是从主核心网络计算出来的，然后通过信令链路，如SS7（7号信令系统）[b-ITU-T Q.700]或Diameter [b-RFC 3588]发送到受访无线网络。这是一个明显的暴露点，显示了密钥是如何泄漏的。
- **用户平面完整性的损害**[b-NGMN]：有一种风险，整个会话将被截取并用于将坏数据插入移动连接（或者通过将数据传递到服务端点而浪费数据）。
- **可选安全性实现**[b-Khan]，[b-NGMN]：这个威胁来自可选安全性实现。有许多不影响互操作性（主要是与UE的互操作性）的安全规定，并且这些选项以往被视为部署选项。这种选择可能导致操作者不可避免地受到没有过错的其他操作者的行为的影响的风险。它还会损害系统级安全假设。如果没有这一认证步骤，密钥层就无法实现其设计目标，即保护用户免受故障基站的影响。

- **基于虚假缓冲状态报告的威胁**[b-Khan]：攻击者可以利用基站等接入网组件的缓冲状态报告获取数据包调度、负载平衡和准入控制算法等信息，以实现其恶意目的。然后，攻击者可以通过伪装成合法的UE发送虚假的缓冲状态报告，从而危及操作。
- **消息插入威胁**[b-Khan]：消息注入可以对IMT-2020网络发起DoS攻击。例如，流表更新不正确的SDN设备可能会过载。攻击者还可以在唤醒期间将控制协议数据单元（C-PDU）注入系统，对新来的UE开展DoS攻击。
- **来自微蜂窝的威胁**[b-Khan]：基站的物理尺寸大幅缩小，被放置在商场、公共场所、体育场和医院等室内位置。此外，毫米波频率的新频率使用也将促进这些微型基站的使用。然而，它们在物理上不如IMT-2020之前的网络中使用的宏基站安全。此外，基站数量的增多将增加IMT-2020网络的潜在漏洞。
- **会话劫持**[b-ENISA]：会话劫持与空中接口有关，是一种用户会话被攻击者接管的攻击。如果一个合法的身份验证会话被接管，攻击者就可以控制特定流量的整个会话，进行另一种类型的攻击。
- **假冒接入网的威胁**[b-ENISA]：如果基站遭到破坏，攻击者可以冒充合法基站，进行中间人攻击或修改网络流量。这种威胁导致篡改移动UE和网络之间的通信，以发起另一个动作。
- **操纵接入网配置数据**[b-ENISA]：如果基站等接入网元素受损，攻击者可以伪造配置数据并发起其他攻击（例如DoS）。
- **来自身份的威胁（IMSI）捕捉**[b-ENISA]：攻击者如果利用蜂窝寻呼协议，可将受害者的软身份与寻呼时机相关联。恶意攻击者可以核实受害者的位置信息，注入伪造的寻呼消息，并发起拒绝服务攻击。
- **被操纵的RRC连接请求造成的服务中断**：如果攻击者操纵以明文形式传输的RRC连接请求消息，那么受害者的临时身份信息可用于阻止受害者的后续网络连接。附录II详细介绍攻击场景。

8.4 软件定义网络面临的威胁

[ITU-T X.1038]号建议书中描述了SDN面临的威胁。

8.5 核心网面临的威胁

核心网面临的安全威胁如下所示：

- **DDoS** [b-Khan]：可以通过利用控制多个受感染UE的僵尸网络，以信令放大和AUSF及UDM饱和的形式发起DDoS攻击。
- **与传输层安全（TLS）/安全套接字层（SSL）有关的威胁**[b-Khan]：在基于SDN的核心网中使用的基于TLS/SSL的通信易受攻击，如TCP/SYN（同步）DDoS、TLS中的RC4偏差、针对SSL/TLS的浏览器漏洞利用（BEAST）攻击、压缩比信息泄漏一点通（CRIME）攻击、LUCKY 13攻击[b-Goodin]和在降级旧版加密上填充Oracle（POODLE）攻击[b-Möller]。
- **SDN扫描器**[b-Khan]：攻击者可以分析SDN流量并手动收集网络信息，如基础设施协议和SDN控制器关键网元。收集到的信息可用于实施各种攻击，如DoS、TCP重置、重放和欺骗攻击。

- **恶意流量分流**[b-ENISA]：破坏一个网元，使攻击者可以分流业务流量并窃听网络流量。流量分流是一种与数据平面网元有关的威胁。虚拟化网络中流量分流的典型例子是非法侵入网络切片。当任何一个活跃节点中切片之间的隔离遭受破坏，或者当对边缘设备中的切片的强制性访问被绕过或配置错误时，都可能出现这种威胁。
- **滥用审计工具**[b-ENISA]：网络运营商使用审计工具来监控网络活动并获取可用于优化、安全或商业目的等多种目的的信息。通过这种类型的软件工具，恶意攻击者能够为攻击开展侦察活动。恶意攻击者通常利用移动网络运营商（MNO）内拥有这些工具特别访问权限的内部人员来提取敏感信息。
- **泄露用户验证/授权数据的长期密钥**[b-ENISA]：这种威胁与泄露用于身份验证和安全控制的长期密钥有关，泄露由在核心网中操作的内部人员或恶意或不值得信任的人员导致。
- **利用配置错误或配置不当的系统/网络**[b-ENISA]：如果系统和网络配置不当或配置错误，攻击者就能访问关键资产。利用一个无意中配置错误的系统，为攻击者创造了接触网络中重要资产的机会。配置错误可能发生在解决方案实施生命周期的各个阶段，如产品安装和维护阶段。
- **流量嗅探**[b-ENISA]：攻击者使用的嗅探器是一种软件或硬件工具，用于拦截、记录和分析网络流量和数据。通过嗅探，攻击者还能够窃听网元的数据，或链接窃取敏感信息。嗅探可能发生在任何有持续流量的地方。
- **恶意网络功能注册**[b-ENISA]：这种威胁是指在IMT-2020网络中部署恶意网络功能。未经授权的网络功能或嵌入木马的功能，由内部人员（移动网络运营商）或供应商/服务提供商引入网络，可能被滥用安装在SBA中，并通过网络功能存储库（NRF）功能在核心网中注册，以暴露其他恶意的API。通过安装或激活未经授权的网络功能（NF），攻击者可以访问网络中的敏感资产以实施其他类型的攻击，如DoS、分发恶意软件或窃取敏感信息。
- **不安全的网络功能开放给第三方应用功能**[b-Ta-Hao Ting]：内部和外部网络之间的网络功能开放实现IMT-2020的动态和灵活部署。如消息被欺骗或篡改，将对整个核心网造成伤害。
- **不安全的基于服务的接口**[b-TS 33.501]：网元之间通过基于服务的接口（SBI）的消息被欺骗或篡改，并且可能被修改和泄露。

8.6 网络切片面临的威胁

网络切片面临的威胁如下所示：

- **网络间切片通信面临的威胁**[b-Khan]：攻击者可以破坏切片之间的通信，以阻止切片的正常生命周期管理。
- **冒充攻击**[b-Khan]：攻击者可以冒充物理主机平台分配不可用资源。此外，攻击者可以冒充网络切片管理员，窃取网络切片创建参数。
- **安全策略不匹配**[b-Khan]：不同切片的安全策略和安全协议的差异，使得攻击者可以通过较不安全的切片访问网络切片系统和控制实体。
- **DoS** [b-Khan]：攻击者对虚拟化网络或物理资源进行DoS攻击，以耗尽其他切片的可用网络资源。

- **边信道**[b-Khan]：攻击者获取一个切片的访问权限，对一组共享相同硬件的切片实施攻击。
- **隐私泄漏**[b-Khan]：基础设施供应商或VNF供应商窃取跨片的用户信息。
- **与管理程序（Hypervisor）有关的威胁**[b-Khan]：对管理程序实施攻击，危害资源的虚拟化。这些攻击包括管理程序的软件错误、通过托管操作系统的后门进入、DoS攻击和硬件资源攻击。

8.7 多接入边缘计算面临的威胁

边缘计算面临的威胁如下所示：

- **虚假或恶意MEC网关**[b-ENISA]：边缘网关的开放性可能会形成一种攻击场景，攻击者可以部署自己的网关设备。这种威胁会产生与中间人攻击相同的效果。
- **边缘节点过载**[b-ENISA]：如果具体的移动应用程序或物联网设备通过指向边缘节点的请求或流量发起对该组件的淹没攻击，在本地或服务层面就可能发生边缘节点过载。这种攻击来自于由物联网设备组成的边缘网络，这些设备会破坏受影响网络的相邻节点。
- **滥用边缘开放API**[b-ENISA]：如果MEC类型的应用程序的漏洞被利用，MEC节点中的开放API可能会被滥用。MEC对开放API的需求主要是为联邦服务和与不同供应商和内容创建者的交互提供支持。这种威胁可能与DoS、中间人、隐私泄露和虚拟机操纵有关。
- **设备的物理篡改**：由于边缘计算架构中的计算资源更靠近攻击者，因此更有可能对设备进行物理篡改。攻击者可能会破坏边缘节点，进而损害整个网络的效能。

8.8 网络功能虚拟化面临的威胁

网络功能虚拟化面临的威胁如下所示：

- **滥用数据中心互连（DCI）协议**[b-ENISA]：如果DCI协议的漏洞被利用，攻击者可以创造欺骗性的流量。如果在数据中心内部署虚拟化系统，可能会对数据中心产生安全威胁，需要加以考虑。
- **滥用云计算资源**[b-ENISA]：如果攻击者使用云计算服务提供商的简单注册程序，强大的计算基础设施，包括软件和硬件组件，都可能被滥用。攻击者利用云计算网络的普遍计算能力，可以在很短的时间内发起攻击。例如，攻击者可以通过滥用云计算的力量发起蛮力攻击和DoS攻击。
- **绕过网络虚拟化**[b-ENISA]：与网络切片实施和配置不当或隔离不当相关的问题可能导致数据保密性/隐私丢失（数据/流量被其他切片的实体截获）。不同租户使用的网络需要确保只有合法的流量进入或离开网络切片，而且任何交换元件都要通过安装防止切片侵入的合法流量规则来检查和执行流量隔离。在核心网层面，恶意攻击者会利用管理程序的漏洞和流量规则的配置，非法侵入切片隔离，泄露属于其他租户的数据。

- **滥用虚拟化主机**[b-ENISA]：如果应用程序在虚拟化主机上运行，这可能会引起对虚拟化环境中共享资源的滥用。在虚拟环境中，物理资源在租户之间共享，可能存在一系列导致敏感信息泄露的行为。例如，在虚拟化环境中通过搜寻（scavenging）导致的泄露甚至比在物理系统中更严重。虽然拦截是物理系统（如网络环境）中常见的威胁，但它的影响在虚拟环境中进一步加剧，因为它允许交叉检查各租户的数据流以及拓扑推断，这可能有助于建立DoS攻击。
- **基础设施完整性威胁**[b-Alwakeel]：攻击者冒充服务提供商出现在NFV的真实服务中，以获取对用户数据的访问权限。
- **滥用资源**[b-Alwakeel]：攻击者释放了一些资源，并利用它们为自己谋利。
- **更改NFV功能定义**[b-Alwakeel]：攻击者修改NFV功能的一些操作以及定义，甚至制造DoS。这通常是通过流量注入（injection）完成的。
- **权限修改**[b-Alwakeel]：攻击者在非控制数据攻击中更改用户的权限，以未经授权的方式升级或降级他们对系统实体的访问权限。
- **基于共享资源的保密性攻击**[b-Alwakeel]：使用边信道攻击，攻击者能以未经授权的方式拉取有关使用共享服务的其他用户的一些隐私信息。
- **恶意内部人员**[b-Alwakeel]：来自组织内部的受信任成员利用他们的权限，以未经授权的方式访问用户的隐私数据。

8.9 管理面临的威胁

管理面临的威胁如下所示：

- **不安全的管理接口**[b-TR 33.811]：接口不安全就是一种威胁。它使攻击者能够在未经授权的情况下获得网络管理的能力，并创建需要大量网络资源的网络切片实例或大量的网络切片实例。
- **泄露与管理功能相关的监督和报告数据**[b-TR 33.811]：监督和报告数据未得到适当的保护就是一种威胁。这将导致攻击者篡改监督/报告的结果，窃听监督和报告数据的传输，并提取敏感信息，用于对正在运行的网络切片实例实施攻击。
- **未经授权访问管理开放接口**[b-Ta-Hao Ting]：如果接口由于未经授权的访问遭受破坏，SDN、NFV和网络切片等网络功能就会出现不当故障，如未经授权更改网络功能、创建不当网络配置和修改网络功能。

9 与组件和功能相关的安全能力要求

9.1 与用户设备相关的安全能力

应支持以下UE安全能力：

- **反恶意软件能力以保护UE**：反恶意软件是一种用于在UE上防止、检测和删除恶意软件（malware）的软件程序。有三种方法可以保护UE免于感染恶意软件：基于签名的恶意软件检测、基于行为的恶意软件检测和沙箱。

- **IMSI安全能力以通过加密保护用户身份（IMSI）**：IMSI应使用对称加密算法。前提是UE有自己的IMSI和家庭网络的公共非对称密钥，且每家移动运营商（此处被称为“家庭网络”）均有一对公共/私有非对称密钥。人们假定家庭网络的私有非对称密钥由家庭网络进行保密，而家庭网络的公共非对称密钥则与具体用户的IMSI一起在移动设备中预先提供。
- **身份验证能力**：为漫游和云服务验证用户身份。
- **密钥管理能力**：支持用户身份验证和UE与网元之间的相互认证。
- **位置安全能力**：确保用户位置的安全。
- **服务网络认证**：UE应通过隐式密钥认证来认证服务网络标识符，隐式密钥认证即，在后续过程中成功使用认证和密钥协商产生的密钥来提供认证。
- **用户数据和信令数据的保密性和完整性**[b-ITU-T X.1811]：UE能够通过密码加密算法支持数据的保密性，并支持UE和网络节点之间用户数据的完整性保护和重放保护。
- **安全存储和处理订阅凭据的能力**[b-Craven]：UE能够通过防篡改硬件为凭据及其长期密钥提供完整性保护。长期密钥不应在防篡改硬件之外以未加密形式提供。应使用认证算法和订阅凭据在防篡改硬件中运行该程序。

9.2 与接入网相关的安全能力

应支持以下接入网安全能力：

- **链路安全能力**：为控制信道和用户业务信道与UE之间的通信提供保密性和完整性。
- **UE认证能力**：服务网络应在UE与网络之间的认证和密钥协商过程中认证订阅永久标识符。
- **UE授权能力**[b-Craven]：服务网络应使用从家庭网络获得的订阅配置文件来授权UE。
- **家庭网络的服务网络授权能力**[b-Craven]：应确保UE与由家庭网络授权的服务网络相连接。
- **接入网授权能力**[b-Craven]：接入网应由服务网络授权，以向UE提供服务。
- **对用户和信令数据进行保密的能力**[b-Craven]：接入网应支持对传输中的用户数据加密和对RRC信令加密。
- **保持用户和信令数据完整性的能力**[b-Craven]：UE等节点应支持在UE和下一节点B之间传输的用户数据的完整性保护和重放保护。
- **设置和配置能力**[b-Craven]：在设置和配置运营和管理（O&M）系统时，下一节点B应由注册机构和认证机构（RA/CA）进行认证和授权，如此，攻击者将无法修改下一节点B的设置和软件配置。
- **下一节点B中的密钥管理能力**[b-Craven]：需要保护IMT-2020网络核心向下一节点B提供的加密密钥的不同元素。
- **用户平面和控制平面数据处理能力**[b-Craven]：密钥管理能力类似于为下一节点B处理用户平面和控制平面数据的能力。

- **安全环境的能力**[b-Craven]：运行所有这些未加密数据的安全环境也需遵守相关要求。它应支持安全存储，例如，通过长期加密秘密和重要的配置数据。
- **解决来自RRC连接请求的服务中断威胁的能力**：为了防止被操纵的RRC连接请求威胁，基站需要与现有用户保持更长时间的RRC连接。这导致基站保持连接的时间长于现有RRC连接的等待计时器。此外，应对基站使用“限制时间”和“限制计数”参数，并应添加检查是否发生此攻击的监视进程。附录二描述了详细的攻击场景。

9.3 与软件定义网络相关的安全能力

应支持以下SDN安全能力[ITU-T X.1038]：

- SDN应用的**认证能力**，认证SDN控制器/用户/管理员；
- SDN应用的**授权能力**，授权用户/管理员获取系统信息；
- SDN应用的**数据保密能力**，对存储在应用平台中的系统信息提供保密保护，并对通过应用-控制接口传输的数据进行保密保护；
- SDN应用的**密钥/证书管理能力**，支持密钥/证书管理；
- SDN应用的**安全管理能力**，支持日志记录和审计；
- SDN应用的**应用保护能力**，支持防御应用漏洞；
- SDN应用的**数据完整性能力**，支持对通过应用-控制接口传输的数据进行完整性保护；
- SDN控制器的**认证能力**，认证管理员/SDN应用/SDN交换机；
- SDN控制器的**授权能力**，授权管理员/SDN应用管理SDN控制器；
- SDN控制器的**认证和安全管理能力**，支持防DoS保护；
- **SDN控制器的数据完整性能力**，对存储在SDN控制器中的配置数据进行完整性保护，对存储在SDN控制器中的用户数据进行完整性保护，对通过应用-控制接口传输的数据进行完整性保护，以及对通过资源-控制接口传输的数据进行完整性保护；
- SDN控制器的**密钥/证书管理能力**，进行密钥/证书管理；
- **SDN控制器的数据保密能力**，对存储在SDN控制器中的配置数据进行保密保护，对存储在SDN控制器中的用户数据进行保密保护，对通过应用-控制接口传输的数据进行保密保护，以及对通过资源-控制接口传输的数据进行保密保护；
- **SDN控制器的操作系统强化能力**，支持操作系统的强化功能；
- **SDN资源层的认证能力**，认证管理员/SDN控制器；
- **SDN资源层的授权能力**，授权管理员管理SDN交换机；
- **SDN资源层的安全管理能力**，支持日志记录和审计；
- **SDN资源层的数据完整性能力**，对存储在SDN交换机中的配置数据进行完整性保护，以及对在SDN交换机之间传输的数据进行完整性保护/对通过资源-控制接口传输的数据进行完整性保护；
- **SDN资源层的密钥/证书管理能力**，进行密钥/证书管理；

- **SDN资源层的数据保密能力**，对存储在SDN交换机中的配置数据进行保密保护，对在SDN交换机之间传输的数据进行保密保护，以及对通过资源-控制接口传输的数据进行保密保护；
- **SDN资源层的流表防溢出能力**。SDN控制器需要通过插入和删除流条目对流表进行动态维护。

9.4 与核心网相关的安全能力

应支持以下安全能力：

- **DoS和DDoS检测和保护能力**，保护SDN中的集中控制点；
- **配置验证能力**，验证SDN网元中的流规则；
- **接入控制能力**，限制对SDN和核心网元的接入。

应支持网络开放功能和基于服务的接口的以下安全能力：

- **安全网络功能开放能力**[b-TS 33.501]：应在网络开放功能和IMT-2020运营商域之外的第三方应用功能之间执行基于客户端和服务器证书的相互认证，由TLS等安全隧道提供。网络开放功能（NEF）和应用功能之间的通信应用于提供完整性保护、重放保护和保密性保护。
- **通过基于服务的接口实现保密性、数据完整性和网元认证**[b-TS 33.501]：通过SBI进行的网元之间的通信，应通过TLS等安全隧道提供数据的完整性保护、重放保护和保密性保护以及网元认证。

9.5 与网络切片相关的安全能力

应支持以下与切片生命周期相关的安全能力[b-Olimid]：

- **切片生命周期安全能力**：应在全部四个阶段执行安全性，因为一个阶段的漏洞可能会在其他阶段引入漏洞。
- **恰当的日志记录和审计能力**：应根据规章、消费服务的目标安全级别、客户设备的专用类型（如人类使用vs机器使用）等各类因素，在不同的网络切片中实施不同级别的日志记录。应保护日志和报告的结果，因为它们的暴露会泄露敏感信息。
- **网络切片模板安全能力**：这应在传输和存储过程中受到保密性和完整性保护，且应对模板源进行认证。
- **安全编排能力**：应根据不同垂直行业的安全要求，编排和部署定制化的安全服务[b-ITU-T X.1047]。
- **切片隔离能力**：应在创造切片时保证隔离，在运行期间监控隔离，甚至如有必要进行更新[b-ITU-T X.1047]。
- **API安全能力**：API在访问和操作权限方面应具有安全性，且不得暴露流量数据；API应仅允许双方通过法律手段商定的能力和数据访问。
- **停止使用能力**：停止使用时，应销毁敏感数据（或根据情况进行安全存储），并释放资源和网络功能。

应支持以下与切片内安全相关的安全能力：

- **端到端安全能力**：切片是端到端的逻辑网络，因此应考虑端到端安全[b-ITU-T X.1047]。
- **安全机制的充分使用能力**：所有通信（如，切片和资源层、切片和切片管理器、切片的子切片、客户设备和网络中的接入点之间）均应使用适当的机制来确保达到目标安全级别；最低要求应包括数据的保密性、完整性、真实性和对等方之间的相互认证。
- **UE认证能力**：IMT-2020客户设备应有力地通过初级和更好的二级认证。
- **安全的资源功能消耗能力**：切片消耗的所有资源和网络功能均应得到安全保护。
- **租户安全能力**：租户引入的新设施（如，网络功能、配置、服务）及其集成应得到充分保护，以防止可被进一步利用的弱点。
- **身份安全能力**：应保护敏感标识符，且不得泄露标识符之间的任何关联。
- **合法拦截**：切片层和业务层应均可访问。
- **租户访问、权限和配置能力**：应符合双方之间的法律协议。

应支持以下与切片间通信相关的安全能力：

- 应对每个切片设置最低安全级别。
- **切片隔离能力**：切片之间的隔离应足够强健，以防止通过安全性较低的切片进行攻击[b-ITU-T X.1047]。
- **最低通信安全能力**：切片之间的通信应降到最低限度，由严格的规则定义，并通过安全的通道实施。
- **密钥管理能力**：不得在切片之间共享加密密钥（和其它敏感参数）。
- **最低资源分配能力**：资源分配应保证每个切片的最低可用性水平；尤其是，无论资源消耗情况如何，安全机制均应能够运行。
- 安全级别存在显著差异的切片不应共享资源或网络功能；尤其是，不得同时运行测试模式下的切片和运行阶段的切片。
- **独立安全能力**：每个切片的不同认证、授权和接入控制机制应相互独立。

9.6 与多接入边缘计算相关的安全能力

应支持以下安全能力：

- **DDoS缓解能力**，保护web云服务；
- **接入控制能力**，限制访问多接入边缘计算网元；
- **完整性验证能力**，在云计算中保护数据和存储系统；
- **服务接入控制能力**，限制基于服务的云计算元素；
- **物理安全能力**：应向未放在高度安全的边缘数据中心里的边缘节点提供物理安全，如，在制造过程中额外采用物理保护技术，或在现场实施锁定机制和其它物理保护措施。

9.7 与网络功能虚拟化相关的安全能力

应支持以下安全能力：

- **流量隔离能力**：此能力旨在确保虚拟切片和虚拟网络功能。
- **DoS攻击防御能力**[b-Alwakeel]：应使用防火墙和负载均衡器等网元缓解DoS/DDoS攻击。
- **基础设施完整性能力**[b-Alwakeel]：应使用信任链和可信平台模块（TPM）来确保不同的VNF服务提供商的安全。
- **缓解资源滥用的能力**[b-Alwakeel]：应提供高级虚拟化管理程序调度器，在进程之间提供公平的共享分配，限制每个虚拟服务允许的最大数量。
- **NFV功能定义变更保护能力**[b-Alwakeel]：应单独存储用户虚拟服务的副本，以防止恶意软件注入攻击。使用文件分配表（FAT），其中包含有关用户正在执行的服务和软件的信息。
- **禁止权限修改能力**[b-Alwakeel]：应提供通过添加资源访问的限制性策略来保护虚拟化实体免受未经授权的访问。
- **减少共享资源的能力**[b-Alwakeel]：应使用缓解边信道攻击的能力来限制对VM映像和网络功能虚拟化基础设施（NFVI）组件的访问，并控制资源的使用。这可以通过使用虚拟防火墙来防止未经授权访问系统来实现。
- **缓解恶意内部人员的能力**[b-Alwakeel]：可以使用多种能力来缓解内部攻击，其中之一是在NFV环境中记录访问情况，然后可以将其用于内部审计以检测可疑活动。另一种机制是为具有访问权限的用户设置严格的认证和授权策略。

9.8 与管理功能相关的安全能力

应支持以下安全能力[b-TR 33.811]：

- 管理服务消费者和管理服务生产者之间使用TLS等安全隧道，基于1) 客户端和服务器证书，或2) TLS-PSK预共享密钥（PSK），而实现的**相互认证能力**；
- 3GPP运营商信任域TLS之外的管理服务生产者和管理服务消费者之间接口的**完整性保护、重放保护和保密性保护能力**；
- **面向管理接口的PI安全能力**：API在访问和操作权限方面应是安全的，不得暴露流量数据；面向管理接口的API应仅允许双方通过法律手段达成一致的能力和数据访问。

附件A

IMT-2020通信系统的安全架构

（本附件是此建议书的组成部分）

[b-TS 33.501]的图4-1概述了IMT-2020通信系统的安全架构。

[b-TS 33.501]的图4-1展示了以下安全域：

– 网络接入安全(I)：使UE能够通过网络（包括通过3GPP接入网和非3GPP接入网）安全地认证和访问服务的一组安全特性，尤其是防止对（无线）接口的攻击。此外，它还包括从服务网络（SN）到接入网（AN）的安全环境交付，以实现接入安全。

– 网络域安全(II)：使网络节点能够安全地交换信令数据和用户平面数据的一组安全特性。

– 用户域安全(III)：使用户安全接入移动设备的一组安全特性。

– 应用域安全(IV)：使用户域和提供者域中的应用能够安全地交换消息的一组安全特性。应用域安全不在本建议书的范围之内。

– SBA域安全(V)：使SBA架构的NF能够在SN域之内以及与其他网络域实现安全通信的一组安全特性。包括网络功能注册、发现和授权安全问题，以及保护基于服务的接口。与[b-TS 33.401]相比，SBA域安全是一种新的安全特性。

– 安全的可见性和可配置性(VI)：使用户了解某一安全特性是否正在运行的一组特性。

附录一

提供端到端网络安全的通用网络安全架构

（本附录不构成本建议书的组成部分。）

本附录描述了提供端到端网络安全的通用网络安全架构，在[b-ITU-T X.805]中有介绍，是本建议书的基础。

[b-ITU-T X.805]定义了提供端到端网络安全的网络安全架构。该架构可应用于各种网络，其中端到端安全是一个受到关注的问题，且其功能与网络的底层技术无关。[b-ITU-T X.805]定义了提供端到端安全所需的与安全相关的一般架构元素。[b-ITU-T X.805]的目标是为制定详细的端到端网络安全建议奠定基础。

[b-ITU-T X.805]建议书定义了八个安全维度：

1) 接入控制；

2) 认证；

3) 不可否认性；

4) 数据保密性；

5) 通信安全；

6) 数据完整性；

7) 可用性；以及

8) 隐私。

[b-ITU-T X.805]建议书还定义了三个安全层，它们在彼此的基础上提供基于网络的解决方案：

1) 基础设施安全层；

2) 业务安全层；和

3) 应用安全层。

此外，[b-ITU-T X.805]亦定义了三个安全平面：

1) 管理平面；

2) 控制平面；和

3) 最终用户平面。

附录二

受操纵的无线资源控制（RRC）连接请求及其能力造成的服务中断威胁

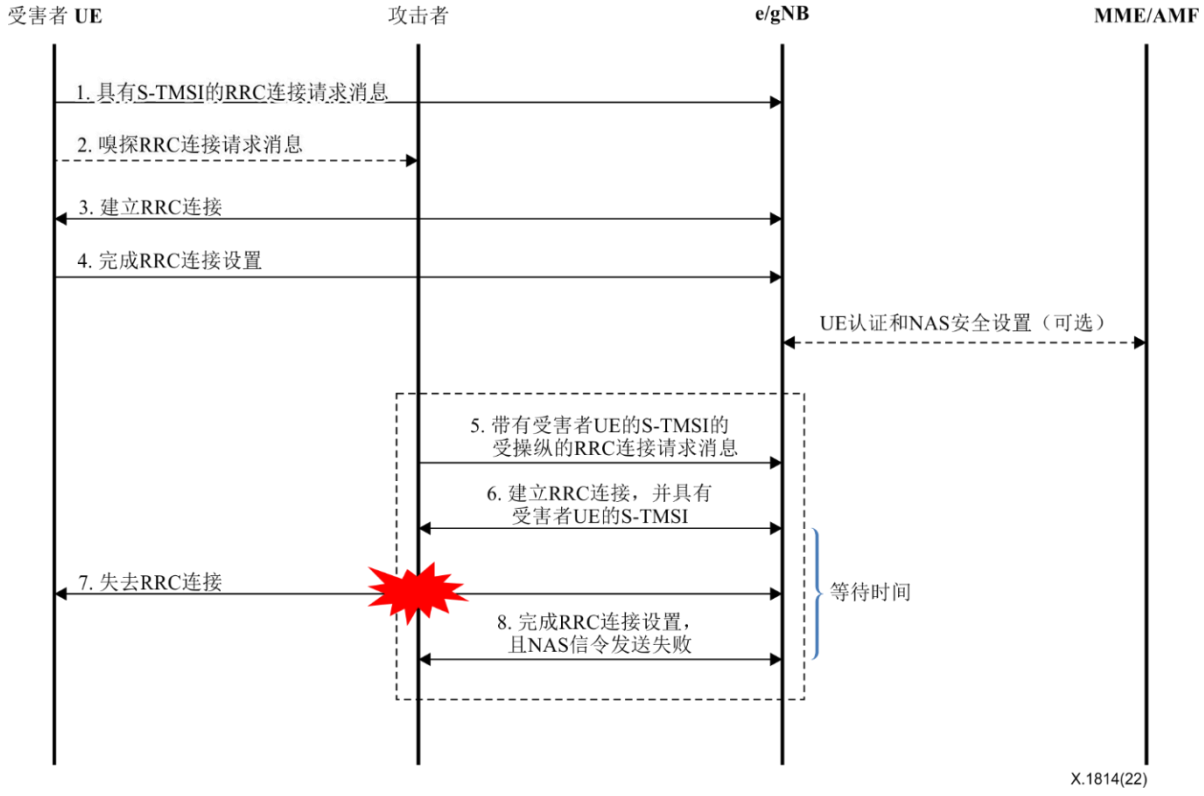
（本附录不构成本建议书的组成部分。）

II.1 概述

RRC连接请求是当UE接入网络时以明文形式发送的消息。它包括全局唯一临时标识（GUTI）或S-TMSI – UE的临时标识信息。有几种方法可以查找特定用户的临时标识信息。如果攻击者捕获此RRC连接请求并在上一步中修改以明文传输的这则消息，那么可以使用受害者的临时标识信息来持续阻止受害者的网络连接。

II.2 攻击场景

攻击者可以截获以明文传输的RRC连接请求消息，并识别临时识别信息GUTI或S-TMSI。在发送伪造的RRC连接请求消息时，攻击者会滥用临时标识信息，其消息被误认为发自受害者的UE。虽然在非接入层（NAS）信令发送期间，由于MAC（消息认证码）认证失败，攻击者的RRC连接被释放，但攻击者可以通过再次发送相同的伪造消息来持续阻止受害者的无线连接。此外，根据基于IMSI的具体规则，可定期间隔时间新创建临时标识信息。如果S-TMSI被更改，攻击者可以检测到更改并再次发送攻击消息。要阻止受害者UE的无线接入，攻击者需要发送伪造的RRC连接请求消息。这种攻击有两个先决条件：1) 攻击者需要将其移动设备放在受害者UE所在的同一个小区中，以捕获无线通信。2) 攻击者拥有可以发送伪造消息的UE。



图II.1 – 受操纵的RRC连接请求攻击场景

II.3 后果

由于此漏洞，在没有检查以确定消息是否被篡改的情况下，无线网络设备（e/gNodeB）会根据攻击者发送的消息断开与受害者UE的现有连接，并连接到攻击者的UE。受害者的UE可能仍处于无法正常接入网络的状态。

II.4 对策

最简单和最有效的对策是，基站将与现有用户的RRC连接保持一段时间。在攻击者利用盗来的受害者ID建立了RRC连接后，当NAS信令发送过程失败时，该连接将被释放。因此，如果受害者的现有连接一直保持到攻击者的RRC连接被释放，则可以保持该无线连接。通常，从攻击者尝试RRC连接到因NAS信令发送过程失败而释放RRC的时间，与基站传输RRC连接设置并等待RRC连接设置完成的时间相对应。因此，在e/gNodeB中实施了“等待计时器”[1]，以计算从它向UE发送RRC连接设置到它接收RRC连接设置完成的时间。应添加一个进程，以便基站保持连接的时间长于现有RRC连接的等待计时器时间，它现在利用复制的ID发送请求，并在对应时间内，在新连接被释放时仍保持现有连接。考虑到对通信服务和设备性能的影响，应尽量减少维护时间。

此外，攻击者可以反复向基站发送RRC连接请求，以维持受害者的服务中断状态。为了缓解这种情况，如果在时间限制内和超过计数限制的次数重复执行RRC连接和释放，则应对e/gNodeB设置“限制时间”和“限制计数”，并增添一个进程，以便基站提醒网络运营商监视攻击。

[1] 例如，3GPP TS 25.331中定义的T352。

参考文献

[b-ITU-T Q.700] Recommendation ITU-T Q.700 (1993), *Introduction to CCITT Signalling System No. 7*.

[b-ITU-T X.509] Recommendation ITU-T X.509 (2019), *Information technology – Open systems interconnection – The directory: Public-key and attribute certificate frameworks*.

[b-ITU-T X.805] Recommendation ITU-T X.805 (2003), *Security architecture for systems providing end-to-end communications*.

[b-ITU-T X.1047] Recommendation ITU-T X.1047 (2021), *Security requirements and architecture for network slice management and orchestration*.

[b-ITU-T X.1401] Recommendation ITU-T X.1401 (2019), *Security threats of distributed ledger technology*.

[b-ITU-T X.1406] Recommendation ITU-T X.1406 (2021), *Security threats to online voting systems using distributed ledger technology*.

[b-ITU-T X.1408] Recommendation ITU-T X.1408 (2021), *Security threats and requirements for data access and sharing based on the distributed ledger technology*.

[b-ITU-T X.1811] Recommendation ITU-T X.1811 (2021), *Security guidelines for applying quantum-safe algorithms in IMT-2020 systems*.

[b-ITU-T Y.3100] Recommendation ITU-T Y.3100 (2017), *Terms and definitions for IMT-2020 network*.

[b-ITU-T Y.3101] Recommendation ITU-T Y.3101 (2018), *Requirements of the IMT-2020 network*.

[b-ITU-T Y.3150] Recommendation ITU-T Y.3150 (2020) *High-level technical characteristics of network softwarization for IMT-2020*.

[b-ITU-T Y.4807] Recommendation ITU-T Y.4807 (2020) *Agility by design for telecommunication/ICT systems security used in the Internet of things*.

[b-ITU workshop] Third annual ITU IMT-2020/5G Workshop and Demo Day (July 18, 2018), *5G security activities and future plan in ITU-T SG17*.

[b-ISO 10393] ISO 10393:2013, *Consumer product recall – Guidelines for suppliers*.

[b-ISO 81001-1] ISO 81001-1:2021, *Health software and health IT systems safety, effectiveness and security – Part 1: Principles and concepts.*

[b-ISO/IEC 27000] ISO/IEC 27000:2016, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*.

[b-ISO/TS 21719-2] ISO/TS 21719-2: 2018, *Electronic fee collection – Personalization of on-board equipment (OBE) – Part 2: Using dedicated short-range communication*.

[b-RFC 3588] IETF RFC 3588 (2003), *Diameter base protocol*.

[b-TR 33.811] 3GPP TR 33.811 (2018), *Study on security aspects of 5G network slicing management*.

[b-TS 33.401] 3GPP TS 33.401 (2021), *3GPP System Architecture Evolution (SAE); Security architecture*.

[b-TS 33.501] 3GPP TS 33.501 (2022), *Security architecture and procedures for 5G System*.

[b-Alwakeel] Alwakeel, A.M., Alnaim, A., and Fernández, E.B., *A Survey of Network Function Virtualization Security*, IEEE Southeast Conf. 2018. https://www.researchgate.net/publication/328146655_A_Survey_of_Network_Function_Virtualization_Security

[b-Craven] Craven, C., *5G Security Standards: What Are They?* 10 June 2020. https://www.sdxcentral.com/5g/definitions/5g-security-standards/

[b-ENISA] European Union Agency for Cybersecurity (ENISA) (2019), *ENISA Threat Landscape for 5G Networks*.

[b-Goodin] Goodin, D. (2013), *Lucky Thirteen attack snarfs cookies protected by SSL encryption* Ars Technica. https://arstechnica.com/security/2013/02/lucky-thirteen-attack-snarfs-cookies-protected-by-ssl-encryption/

[b-Khan] Khan, R., Kumar, P., Jayakody, D.N.K, and Liyanage, M. (2019), *A Survey on Security and Privacy of 5G Technologies: Potential Solutions, Recent Advancements and Future Directions*, IEEE Communications Surveys and Tutorials, Vol. 22, No. 1, July, pp. 196-248.

[b-Möller] Möller, B, Duong, T, and Kotowicz, K. (2014), *This POODLE Bites: Exploiting The SSL 3.0 Fallback.* https://www.openssl.org/~bodo/ssl-poodle.pdf

[b-NGMN] The Next Generation Mobile Networks Alliance (NGMN Alliance) (2016), *5G security recommendations package*.

[b-Olimid] Olimid, R., and Nencioni, G. (2020) *5G Network Slicing: A Security Overview*, IEEE Access, Vol. 8, June, 99999-100009.

[b-SQL] OWASP, *SQL injection.* https://owasp.org/www-community/attacks/SQL_Injection

[b-Ta-Hao Ting] Ta-Hao Ting, Tsung-Nan Lin, Shan-Hsiang Shen, and Yu-Wei Chang (2019), *Guidelines for 5G end to end architecture and security issues*. https://arxiv.org/abs/1912.10318

ITU-T系列建议书

系列A	ITU-T工作的组织
系列D	资费及结算原则和国际电信/ICT的经济和政策问题
系列E	综合网络运行、电话业务、业务运行和人为因素
系列F	非话电信业务
系列G	传输系统和媒介、数字系统和网络
系列H	视听及多媒体系统
系列I	综合业务数字网
系列J	有线网络和电视、声音节目及其他多媒体信号的传输
系列K	干扰的防护
系列L	环境与ICT、气候变化、电子废物、节能；线缆和外部设备的其他组件的建设、安装和保护
系列M	电信管理，包括TMN和网络维护
系列N	维护：国际声音节目和电视传输电路
系列O	测量设备的技术规范
系列P	电话传输质量、电话设施及本地线路网络
系列Q	交换和信令，以及相关的测量和测试
系列R	电报传输
系列S	电报业务终端设备
系列T	远程信息处理业务的终端设备
系列U	电报交换
系列V	电话网上的数据通信
系列X	**数据网、开放系统通信和安全性**
系列Y	全球信息基础设施、互联网协议问题、下一代网络、物联网和智慧城市
系列Z	用于电信系统的语言和一般软件问题

瑞士印刷
2022年，日内瓦