



5G零信任安全技术研究

IMT-2020 (5G) 推进组

2022年4月

目 次

前 言	III
1. 范围	1
2. 缩略语	1
3. 概述	2
4. 零信任架构及关键技术	3
4.1. 零信任安全架构	3
4.1.1. 总体框架	3
4.1.2. 功能组件和逻辑组成	4
4.2. 零信任关键技术及实现	5
4.2.1. 精确的身份管理	5
4.2.2. 网络与业务隐藏与保护	5
4.2.3. 持续信任评估	6
4.2.4. 动态访问控制	6
4.2.5. 终端安全防护	6
5. 5G 零信任应用场景分析	6
5.1. 网络服务能力开放	6
5.2. 服务化架构	7
5.3. 网络切片	8
5.4. 移动边缘计算	9
5.5. 网络运维	10
5.6. 物联网安全	12
6. 5G 零信任应用解决方案	14
6.1. 网络服务能力开放	14
6.2. 移动边缘计算	15
6.3. 网络运维	17
7. 展望及建议	18
7.1. 展望	18
7.2. 建议	19

前 言

5G 泛在连接、低时延响应、动态切片特性在扩展网络时空边际、重构垂直行业信息生态的同时，带来安全边界模糊、复杂隐蔽攻击快速传播、终端信任建立困难的新型威胁态势，提升新一代移动通信系统的安全性已经上升为各国的战略需求。当前国际上 5G 安全关键理论技术和标准研究仍处于发展阶段，现有 5G 安全防护体系依然依赖物理边界，形成防护边界与攻击链路错位分布格局，安全体系缺乏安全边界的动态调整能力；同时，传统安全防护方法认证、授权机制僵化，缺乏时间演化特性，难以应对 5G 新型威胁态势。因此，亟需在当前 5G 安全体系的基础上进一步发展 5G 安全新范式，提出物理安全边界与软件定义安全界限的协同防护机制、构建传统认证授权模型与动态信任评估的主动互馈模型，增强现有 5G 安全体系的威胁消解能力。零信任模型具有“永不信任，持续认证，最小特权”特性，通过持续信任评估、动态访问授权和灵活微隔离技术，零信任可有效识别非可信终端、最小化攻击影响范围，并结合网络和业务的隐藏来减少攻击暴露面，降低安全风险。因此，零信任模型可应用于 5G 安全领域，扩展现有 5G 安全体系的防护能力，有效提升 5G 安全性。

本报告深入分析了零信任技术在 5G 网络的服务能力开放、服务化架构、网络切片、互联互通、边缘计算、网络运维等各种场景下的应用需求，给出了零信任在网络服务能力开放、移动边缘计算、网络运维等场景中的应用案例，针对零信任技术在 5G 网络中的应用进行了积极探索。

本报告由 IMT-2020 (5G) 推进组提出并归口。

本报告起草单位：中国信息通信研究院、华为技术有限公司、中国移动通信有限公司研究院、亚信科技（成都）有限公司、奇安信科技集团股份有限公司、杭州安恒信息技术股份有限公司、恒安嘉新（北京）科技股份有限公司、网宿科技股份有限公司、北京神州绿盟科技有限公司、中国移动通信有限公司信息安全管理与运行中心、中兴通讯股份有限公司、北京小米移动软件有限公司、中国电信集团有限公司

本报告主要起草人：邵晓萌、焦杨、杨红梅、栗栗、杜海涛、吴荣、李科、韩科科、崔洋、胡华东、孙玲玲、庞勇、乔思远、罗海龙、陈三强、赵宁、梁伟、徐昕白、赵亮、潘文欣、

王立超、于乐、游世林、梁浩然、薄明霞

5G 零信任安全技术研究

1. 范围

本报告描述了零信任架构和关键技术、零信任在5G网络中的应用场景以及部分场景下的零信任应用解决方案。

本报告可以为5G移动通信网的安全手段建设及安全防护提供技术参考。

2. 缩略语

下列缩略语适用于本报告。

缩略语	英文	中文
3GPP	3rd Generation Partnership Project	第三代合作伙伴计划
AD	Active Directory	活动目录
AF	Application Function	应用功能
API	Application Programming Interface	应用程序接口
BSS	Business support system	业务支撑系统
DDoS	Distributed Deny Of Service	分布式拒绝服务
DIB	The Defense Innovation Board	美国国防创新委员会
DoD	United States Department of Defense	美国国防部
ETSI	European Telecommunication Standard Institute	欧洲电信标准化组织
IAM	Identity and Access Management	身份识别与访问管理
IDS	Intrusion Detection System	入侵检测系统
IoT	Internet of Things	物联网
IPS	Intrusion Prevention System	入侵防御系统
LDAP	Light weight Directory Access Protocol	轻量目录访问协议
MEC	Multi-Access Edge Computing	多接入边缘计算

NEF	Network Exposure Function	网络开放功能
NCCoE	National Cybersecurity Center of Excellence	国家网络安全卓越中心
NFV	Network Function Virtualization	网络功能虚拟化
NIST	National Institute of Standards and Technology	美国国家标准技术研究院
NRF	NF Respository Function	网络存储功能
NSA	National Security Agency	美国国家安全局
NSS	National Security System	美国国家安全系统
NSSAA	Network Slice-Specific Authentication and Authorization	网络切片身份验证和鉴权
NWDAF	Network Data Analytics Function	网络数据分析功能

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。
如要下载或阅读全文，请访问：

<https://d.book118.com/986101005024010113>