5G 网络攻击技术研究及防护建议

邵晓萌　韩文婷

（中国信息通信研究院安全研究所，北京 100191）

摘要：为挖掘 5G 网络潜在的脆弱性及安全威胁，提升网络安全评测能力，分析了 5G 网络的安全风险、梳理了 5G 网络安全攻击技术，研究并提出了应对 5G 网络安全攻击的防护建议。

关键词：5G；空口攻击；信令风暴；协议攻击

中图分类号：TN929.5　　**文献标志码：**A

引用格式：邵晓萌，韩文婷．5G 网络攻击技术研究及防护建议[J]．信息通信技术与政策，2022，48(12)：79-81.

DOI：10.12267/j.issn.2096-5931.2022.12.013

0　引言

随着我国 5G 商用进程加速以及 5G 网络与垂直行业的深度融合，各类终端设备接入 5G 网络，打破了传统电信网络的封闭性，带来了新的漏洞类型和攻击方式。同时，5G 网络引入软件定义网络（Software Defined Network，SDN）、网络功能虚拟化（Network Functions Virtualization，NFV）、多接入边缘计算（Multi-access Edge Computing，MEC）等一系列新技术，进一步增加了攻击暴露面，从而导致网络安全问题变得错综复杂。针对 5G 网络的攻击，可能造成网络服务中断，并对公众基本服务产生重大影响，从而摧毁公众对移动技术和服务提供商的信任。因此，需全面分析 5G 网络安全攻击技术，挖掘 5G 网络潜在的安全风险，增强 5G 网络的抗攻击能力，提升 5G 网络安全。

1　5G 网络安全攻击风险

5G 网络安全[1]攻击风险可分为终端、接入网、核心网 3 个方面。5G 时代海量物联网终端，其中大量功耗低、计算和存储资源有限的终端难以部署复杂的安全策略，一旦被攻击容易形成僵尸网络，将会成为攻击源，进而引发对用户应用和后台系统等的网络攻击，带来网络中断、系统瘫痪等安全风险。5G 接入网主要存在空口的用户数据窃听篡改、空口 DDOS 攻击、伪基站或者其它攻击源对空口的恶意干扰、基站数据传输未加密完保等安全隐患，可能造成终端用户的隐私数据或者行业应用的关键数据泄漏、通信数据流量被窃听篡改等安全风险。5G 核心网引入了网络功能虚拟化、网络切片、边缘计算、服务化架构、网络能力开放等新技术，网络架构有了重大变化，带来了新的安全挑战。攻击者可以利用 5G 终端、5G 接入网、5G 核心网的安全风险发起攻击。

2　5G 网络安全攻击技术

2.1　5G 终端安全攻击技术

5G 终端大致分为消费类终端和行业类终端。消费类终端包括 5G 智能手机、AR/VR 终端、Pad、移动路由器等。行业类终端包括 5G 通用模组、行业 CPE、车载终端等。这两类终端面临的安全攻击[2]主要包括：中间人攻击、终端劫持攻击和分布式拒绝服务（DDoS）攻击。

（1）终端监听或中间人攻击：攻击者可以发起中间人攻击，进行监听窃取和篡改通信信息，影响终端业务

正常运作，严重时会直接导致网络瘫痪，造成通信事故。

(2) 终端劫持攻击：攻击者通过劫持终端，监听用户信息，伪装为合法用户向网关或者基站发送恶意请求，尝试非法接入网络或者嗅探网络中的有效信息。

(3) 分布式拒绝服务攻击：攻击者控制终端在同一时刻发送大量数据，形成大规模僵尸网络，从而导致网络拥塞，造成数据丢包，引起服务瘫痪。

2.2 5G 无线接入网安全攻击技术

5G 无线接入网安全攻击主要是获取用户信息或者中断用户服务，用户终端接入 5G 网络时，一方面，由于空口信道的开放性，无线信号容易受到干扰，无线链路也容易受到非法接收机信号监听；另一方面，非法基站可以利用 5G 空口协议的漏洞，尝试伪基站接入，从而将用户接入至伪基站，获取用户的信息，或中断用户通信服务。无线接入网面临的安全攻击[5]主要包括空口协议攻击和空口信道攻击，空口协议攻击包括伪基站攻击、会话劫持攻击、位置信息捕获攻击等。空口信道攻击包括射频和无线干扰、频谱资源滥用等。

(1) 伪基站攻击：攻击者通过非法使用运营商的频率，利用通信网络及协议的缺陷和漏洞，假冒运营商网络，伪装成运营商基站，通过增加发射信号功率等手段，导致以其为中心、特定半径范围内的移动终端从运营商合法基站切换至伪基站，从而收集终端信息。同时，伪基站可伪造任意发送号码强行向覆盖区域内的终端发送短消息。

(2) 会话劫持：攻击者可以利用 open-air 接口的脆弱性，窃取合法的经过身份验证的会话 ID，并对会话流的流量进行控制，实现会话流重定向，或者修改会话的资源映射关系，导致正常会话无法占用空口无线资源，导致会话中断。

(3) 位置信息捕获攻击：攻击者通过监听设备嗅探寻呼消息，验证目标蜂窝用户是否在拦截范围内，从而获取用户的位置信息

(4) 射频和无线干扰：攻击者故意破坏/干扰网络射频，导致相关用户不可访问核心网络(及相关服务)。

(5) 频谱资源滥用：攻击者通过模仿合法许可用户的信号特征、干扰射频以占用特定的空闲频谱，导致授权频段被占用，导致空闲资源缺乏，可能导致基站拒绝其他正常用户所请求的频谱资源。

2.3 5G 核心网安全攻击技术

5G 核心网在继承 4G 的安全架构的基础上，在核心网层引入网络功能虚拟化、网络切片、边缘计算、服务化架构、网络能力开放等新技术[6]，网络架构有了重大变化，从而导致 5G 网络除面临信令风暴攻击、协议攻击等传统攻击手段外，还面临一些新技术相关的攻击。

(1) 信令风暴攻击：攻击者可以利用大量信令并发攻击基站及核心网，导致基站及核心网资源不可用。

(2) 协议攻击：攻击者可以利用协议漏洞发起攻击，比如利用加密完保算法为空的配置，可以直接窃取明文或发起篡改攻击。

(3) MEC 攻击：攻击者可以发起身份认证与授权绕过攻击、边缘基础设施安全攻击、边缘数据安全攻击及 MEC 应用安全攻击，非法访问或篡改 MEC 资源、破获 MEC 基础设施、窃取用户数据、非法访问 MEC 应用等。

(4) 虚拟化攻击：攻击者可以发起 Hypervisor 安全攻击、虚拟机逃逸攻击、虚拟机滥用攻击、镜像篡改攻击、数据泄露、盗窃破坏和信息操纵攻击等，破获虚拟网络功能、导致整个系统无法安全稳定运行。

(5) 网络切片攻击：攻击者可以发起切片旁路攻击、切片通信安全攻击、切片配置安全攻击、切片开放接口安全攻击等，非法获取切片的数据信息或者影响切片的正常通信功能。

(6) 服务化架构攻击：攻击者可以发起中间人攻击、隐私数据窃取、拒绝服务攻击等，窃取服务化接口信令消息，获取用户隐私信息，耗尽网元资源等。

3 5G 网络安全防护建议

3.1 终端防护

针对终端测防护，建议重点加强终端的认证和加密完保，具体如下。

(1) 接入 5G 的终端支持 5G-AKA 或 EAP-AKA' 认证[5]，网络侧可实现对终端的双向鉴权认证，保证接入网络终端的合法性。

(2) 终端支持二次认证，通过二次认证可实现外部数据网络的 AAA 服务器对与其有签约关系的终端进行认证，然后根据认证是否成功来决定该终端是否被允许接入业务系统。

(3) 终端支持信令面及用户面的加密完保，网络侧开启控制面及数据面的加密及完整性保护，保障终

端接入网络信令及终端传输数据的机密性及完整性。

3.2 接入网防护

针对接入网侧的防护，建议重点加强认证、访问控制，具体如下。

(1) 5G 基站加强机密性和完整性保护，通过对空口数据(包括信令和用户数据)开启加密保护，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 基站通过完整性算法能够检测信令消息和用户面数据是否被篡改。

(2) 5G 基站通过终端接入访问控制防止非法终端接入和终端恶意攻击行为。

(3) 通过在基站所在位置安装防盗报警探测器等产品，实现应入侵报警、防拆报警、故障报警等功能。

3.3 核心网防护

针对核心网侧的防护，建议重点加强边界防护、流量分析，并引入零信任技术[6]，进行持续信任评估、动态访问控制、网络与业务隐藏，具体如下。

(1) 部署信令防火墙、业务防火墙、日志审计、堡垒机、漏洞扫描、数据库审计等网络安全产品进行边界防护。

(2) 部署流量检测分析产品，对 5G 核心网全流量的安全检测分析，实现终端的恶意接入检测、资产识别、漏洞和威胁利用行为检测、信令攻击检测、业务渗透入侵检测，以及流量追溯取证等。

(3) 引入零信任技术，保障 5G 网络的服务能力开放安全、服务化架构信令安全、边缘计算安全、切片安全等。

4 结束语

本文介绍了 5G 终端、5G 接入网及 5G 核心网安全攻击技术，研究并提出了 5G 终端、5G 接入网及 5G 核心网的安全防护建议。5G 网络作为“新基建”的重要组成部分，在我国新时代的建设进程中，发挥着极为重要的作用，应全面深入分析 5G 设备面临的安全风险及威胁，提升 5G 网络安全能力。

参考文献

[1] 冯泽冰，司培培. 面向 5G 资产的统一安全评测模型与体系构建[J]. 信息安全研究，2021，7(5)：436-442.

[2] 余滢鑫，余晓光，翟亚红，等. 5G 终端安全技术分析[J]. 信息安全研究，2021，7(8)：704-714.

[3] 阳陈锦剑，余晓光，余滢鑫，等. 5G 无线接入网安全研究[J]. 信息安全研究，2021，7(5)：457-465.

[4] 邱勤，张滨，吕欣. 5G 安全需求与标准体系研究[J]. 信息安全研究，2020，6(8)：673-679.

[5] 3GPP. TS 33.501: Security architecture and procedures for 5G system[S]，2020.

[6] IMT-2020(5G)推进组. 5G 零信任安全技术研究报告[R]，2020.

作者简介：

邵晓萌　中国信息通信研究院安全研究所高级工程师，长期从事 5G 安全及安全测评相关工作

韩文婷　中国信息通信研究院安全研究所助理工程师，长期从事 5G 安全相关工作

Research and protection suggestions of 5G network attack technology

SHAO Xiaomeng，HAN Wenting

(Security Research Institute，China Academy of Information and Communications Technology，Beijing 100191，China)

Abstract: In order to explore the potential vulnerabilities and security threats of 5G network and improve the network security evaluation ability，the security risks of 5G network is analyzed in this paper，the security attack technology of 5G network is sorted out，and the protection suggestions against 5G network security attack are proposed.

Keywords: 5G；air attack；signaling storm；protocol attacks

(收稿日期:2022-07-07)