oppo

6G 安全架构：构建基于零信任的智能安全

OPPO 6G 安全白皮书

目录

前言

01

前言

6G 时代以工业互联网、泛在的人工智能（Artificial Intelligence，AI）、零功耗通信、通感一体化（Integrated Sensing and Communication，ISAC）为代表的新业务、新终端、新连接、新架构的发展趋势会对当前的通信模式带来巨大改变，越来越多的数据开始从终端侧收集，再传输到网络侧，成为人工智能必不可少的数字资源，6G 系统将针对这些高价值数据资产进行管理。**因此，6G 安全的最大变化趋势是保护的重点从传输逐渐演变为数据与隐私。**在使用高价值数据资产的同时，需要高效的数据授权，防止归属于不同利益相关方的数据资产价值被滥用。考虑到 6G 系统业务和数据来源的多样性，需要考虑多方信任模式，针对多源的、分布式的数据，进行分布式的数据授权，同时针对个人相关数据，做好隐私保护。

随着新终端、新连接技术的发展，数据传输不仅仅局限于传统高层协议，数据安全保护的能力也需要从传统的高层保护向底层保护迁移，从而匹配 6G 新终端、新空口技术的安全需求。

根据“极简多能”的 6G 系统概念设计，对于不同子系统的数据资产，安全保护机制也需多元化，需要对 6G 系统安全功能进行动态的安全编排，用智能安全架构满足不同场景的安全需求。

本文将通过分析 6G 新业务、新终端、新连接、新架构的发展趋势和安全需求，在传统蜂窝安全机制的基础上，探索区块链、物理层安全、AI 安全、后量子安全等技术，提出基于零信任的 6G 智能安全架构。

- 5G 安全双向信任模型
- 5G 安全架构
- 5G 传输安全机制

5G 安全小结

02