

基于网络流量的 小众涉诈应用程序识别与应用

Identification and Application of Niche Fraud-Related Applications Based on Network Traffic

孙婧瑜,余思阳,曹京卫,刘珊珊,陆小军(中国联合网络通信集团有限公司,北京 100033)

Sun Jingyu, Yu Siyang, Cao Jingwei, Liu Shanshan, Lu Xiaojun (China United Network Communications Group Co., Ltd., Beijing 100033, China)

摘要:

小众涉诈恶意程序是涉诈恶意程序中更狡猾、更隐蔽、更具对抗性的一个子集,其隐蔽性强、变种快的特点给网络安全带来了严峻挑战。提出基于网络流量的小众涉诈应用程序智能识别方法。该方法通过实时采集并深度解析应用程序网络流量数据,采用流量还原技术提取多维特征向量;构建了动态更新的小众涉诈应用程序特征知识库,引入机器学习算法实现特征匹配与异常检测,提升对小众新型变种涉诈应用程序的识别准确率。

关键词:

网络流量;小众涉诈应用程序;动态研判;识别
doi:10.12045/j.issn.1007-3043.2026.09.013
文章编号:1007-3043(2026)09-0069-05
中图分类号:TN918
文献标识码:A
开放科学(资源服务)标识码(OSID): 

Abstract:

Niche fraud-related malware represents a more cunning, covert, and adversarial subset of fraud-related malwares. Its strong concealment and rapid variant characteristics pose severe challenges to cybersecurity. An intelligent identification method for niche fraud-related applications based on network traffic is proposed. By collecting application network traffic data in real time and performing in-depth parsing, the multi-dimensional feature vectors are extracted using traffic reconstruction technology. Furthermore, a dynamically updated feature knowledge base for niche fraud-related applications is constructed, and machine learning algorithms are introduced to achieve feature matching and anomaly detection, thereby enhancing the accuracy of identifying novel variants of niche fraud-related applications.

Keywords:

Network traffic; Niche fraud-related applications; Dynamic analysis; Identification

引用格式:孙婧瑜,余思阳,曹京卫,等. 基于网络流量的小众涉诈应用程序识别与应用[J]. 邮电设计技术, 2026(9): 69-73.

0 引言

小众涉诈 APP 是当前电信网络诈骗的主要工具之一。这类 APP 并非来自官方应用商店,而是由诈骗团伙私自开发、包装,并通过特定链接、二维码、聊天群等方式传播的恶意应用程序。当前小众涉诈应用程序呈现爆发式增长态势,对网络空间安全和用户资产安全构成严重威胁^[1]。这类恶意应用往往采用高度隐蔽的技术手段,并通过快速迭代变种逃避检测,传统防护手段难以对其形成进行有效拦截。涉诈应用

程序不仅会造成重大经济损失,更会危及个人隐私与数据安全,严重破坏数字生态信任体系^[2]。

因此,小众涉诈 APP 识别已成为网络安全领域的关键课题。然而,静态代码分析、权限检查等传统方法需人工定义规则,难以应对快速迭代的加壳、混淆技术^[3];另外,有些研究依赖用户行为数据(如短信内容、GPS 轨迹等),存在隐私泄露风险,使实际部署受到制约。本文提出了一种基于网络流量的小众涉诈 APP 识别方法,即使 APP 本身是新的、未知的,但其通信行为会暴露出固有的恶意模式或特征。该方法利用现有基础设施的优势,采集核心网络的全流量数据信息,提取 APP 源文件,使用智能算法对文件进行分析

收稿日期:2026-08-04

和识别,并动态更新文件库,提高对涉诈 APP 的识别性能,更好地维护网络安全环境。

1 网络流量分析及还原

1.1 流量分析

小众涉诈 APP 为实现诈骗目的,其网络通信行为会与正常合法 APP 存在显著差异。系统通过深度包检测(DPI)和流量元数据分析,采用 NetFlow 与实时抓包协同的流量监测架构捕捉这类异常模式。NetFlow 基于“流”的元数据记录机制,通过 IP 五元组及 TCP 标志位、数据量等传输层特征,构建网络层流量画像,支持秒级粒度的带宽异常检测,单节点可处理 40 Gbit/s 流量^[4]。实时抓包工具(如 Wireshark、tcpdump 等)通过网卡嗅探实现全栈解析,从物理层帧结构到应用层载荷深度解码,支持 TLS 握手还原与协议逆向^[5]。两者形成分层协同:NetFlow 从宏观维度完成异常流量初筛,触发定向抓包进行微观分析,定位隐蔽通信特征;抓包工具侧重于应用层的深度检测。

1.2 流量还原

原始的网络流量以二进制方式呈现,无法直接读取和应用,需要通过相关工具和技术将其转换为容易读取的数据信息^[6],这一处理过程即为流量还原。该过程需对采集到的网络流量进行解码和分析,包括识别流量中的协议、业务、提取流量中的原始文件等。流量数据包解析还原就是对二进制比特流中各个位置的字段进行提取和解析重组,具体包括端口匹配、流量特征检测、自动连接关联和行为特征分析等^[7-8]。

如图 1 所示,初始阶段系统通过端口匹配快速筛选流量类型,例如标准端口 80 指向 HTTP 网页服务,443 对应 HTTPS 加密通信。此类基于端口映射的初筛

机制效率极高,但需警惕端口伪造行为,例如木马程序利用 53 端口伪装 DNS 流量进行隐蔽隧道通信^[9-11]。因此需叠加流量特征检测技术,针对标准协议(如 HTTP),依据 RFC 规范解析 Header 结构、URL 路径与状态码等字段;对于非标或加密协议(如私有物联网协议与 SSH 加密会话),则通过逆向工程提取固定报文头、统计交互时序或分析加密元数据,构建协议特征库以实现精准识别。

在复杂网络场景中,自动连接关联技术至关重要。当协议采用动态端口协商机制时,系统需解析控制链路报文获取动态端口参数,通过五元组源 IP、目的 IP、源端口、目的端口与协议关联离散会话,跨多链路重组完整业务流^[12-13]。对于加密或高度混淆的流量(如 Tor 匿名通信),则依赖行为特征分析,通过机器学习模型对连接频率、流量突发模式与数据包长度分布进行建模,结合上下文信息识别潜在威胁。

最终的数据重组需实现比特流到业务对象的转化,通过 TCP 序号排序与分片偏移量计算还原完整文件^[14]。这一技术链条将混沌的二进制信号转化为可读的通信日志、可审计的文件实体及可追溯的行为画像,为网络安全监测、取证溯源及业务优化构筑数据基石。

2 基于网络流量的小众涉诈 APP 识别技术

2.1 基于网络流量的小众涉诈 APP 识别框架

基于网络流量的小众涉诈 APP 识别框架充分利用现有基础设施的优势,采集核心网络的全流量数据,使用基于 Netflow 的流量分析技术和抓包工具对这些原始流量信息进行分析:通过端口匹配、流量特征检测、自动连接关联和行为特征分析等对原始流量进行解码和分析。最后,本文通过随机森林算法对 APP 进行识别分类。

首先,将获取的网络流量进行分析还原,然后对还原出的 APK 文件进行研判,其中所有的样本都要被静态研判,而高风险 APP 还需要动态研判;同时,依托定期更新的小众涉诈 APP 特征库,可以提供最新的涉诈 APP 特征。最后,将研判确认的小众涉诈 APP 循环更新到涉诈 APP 资源库中,以提高模型后续识别的准确率。

模型的结构如图 2 所示。该小众涉诈 APP 识别模型采用静态与动态分析相结合的机制,对可疑 APP 进行多维度检测。首先,系统将待检测的 APK 文件及网

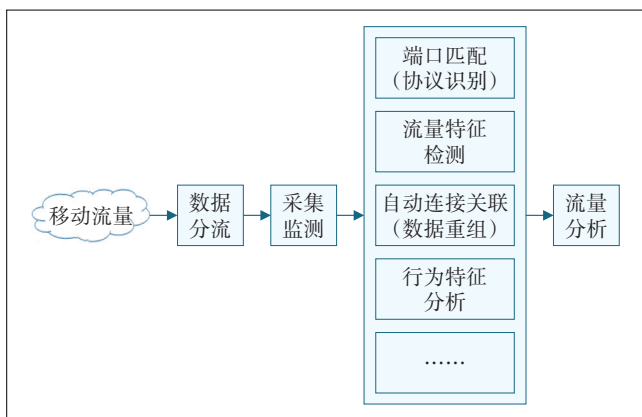


图 1 流量还原技术

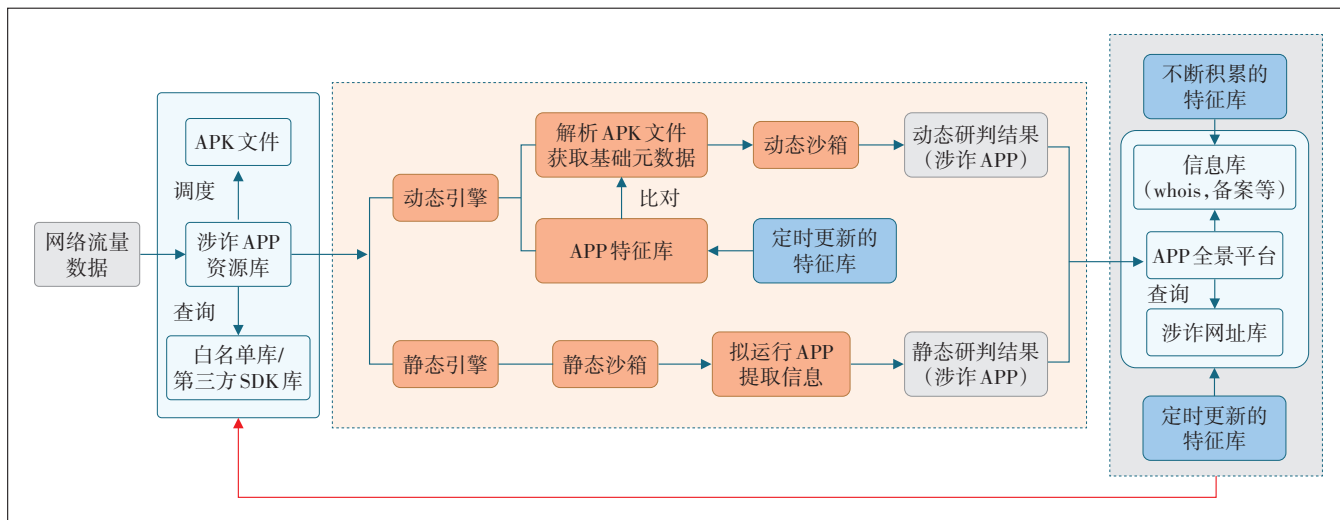


图2 基于网络流量的小众涉诈APP识别模型

络流量数据作为输入。在静态分析阶段,静态引擎通过静态沙箱解析 APK 文件,提取权限、代码特征等信息,并与 APP 特征库、涉诈网址库、备案信息库等进行比对,初步判断 APP 是否涉诈。同时,系统会查询白名单库或第三方 SDK 库,以排除合法应用的干扰;在动态分析阶段,动态引擎将 APP 置于动态沙箱中运行,实时监控其行为,并与定时更新的恶意行为特征库进行比对,进一步验证其风险。静态与动态研判的结果相互补充,最终综合判定该 APP 是否涉诈。此外,系统会将新发现的恶意特征反馈至特征库,形成闭环学习机制,持续提升检测能力。整个流程依托资源库和全景平台的数据支持,确保研判的准确性和时效性,可有效应对不断演变的涉诈威胁。

2.2 基于网络流量的小众涉诈APP识别研判流程

小众涉诈APP的研判流程如图3所示。首先对待研判样本进行分析,检查是否需要重新研判,该环节需要将研判样本与特征库进行匹配。若匹配成功,则进一步查询该样本是否已被研判。若未被研判,流程将进入选择研判引擎的关键环节。引擎类型根据评分动态调整:若评分超过90分,系统自动下发动态引擎,超过90分的样本被判定为高风险,需要更深入的动态引擎分析,本文使用动态沙箱进行动态研判;若评分未超过90分,系统仅调用静态引擎进行基础研判,静态引擎则作为必选基础组件。选定引擎后,系统执行研判分析,生成结果并进入结果处理阶段(包括结果验证、反馈或执行等相应操作)。最终,所有相关数据会被存储至数据库,同时通过动态引擎的资源

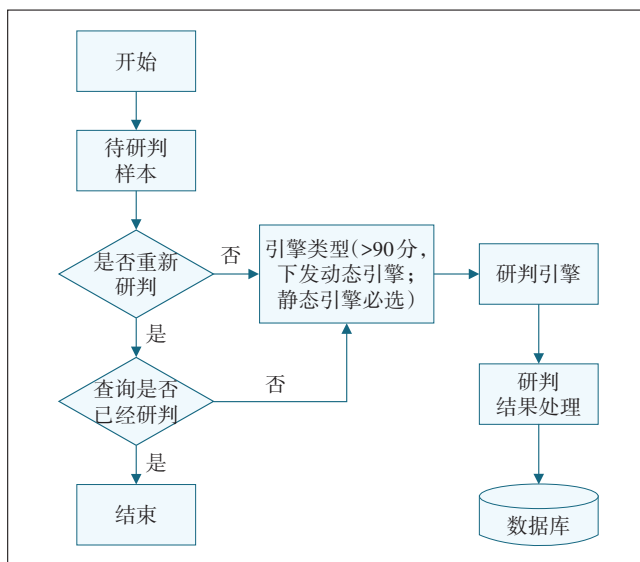


图3 小众涉诈APP研判流程

分配优化,提升系统响应能力。该机制采用“静态+动态”双引擎分析,整个过程注重自动化与逻辑判断,确保研判的准确性,结合多维度特征库和沙箱环境,实现高效、精准的小众涉诈APP识别。同时,系统具备自学习能力,随着新特征不断入库,可动态适配不断变化的恶意APP。

3 应用示例

3.1 涉诈贷款APP识别

基于网络流量的研判体系是当前最主要的现网涉诈研判体系。在该体系下,网络流量通过分光器接

入 NTA 研判引擎, NTA 研判引擎加载最新的涉诈 APP 识别策略, 并基于识别策略对流量进行分析研判, 现网涉诈研判流程如图 4 所示。系统实时输出与策略相匹配的涉诈事件话单, 提供打击线索, 预警、劝阻信息和封堵处置指令。

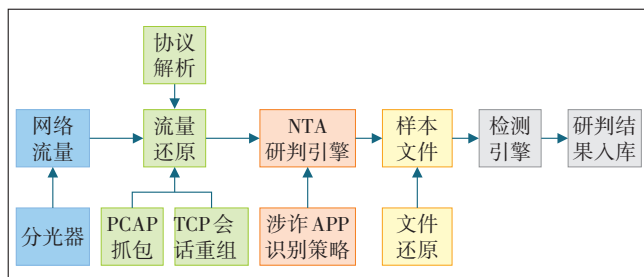


图 4 现网涉诈研判

图 5 所示为涉诈贷款 APP 的识别框架。小众涉诈 APP 像通过私人渠道实施“杀猪盘”的骗子一样, 目标精准, 隐蔽性强, 危害更大。本示例主要基于中文名称相似度比来判断待测 APP 是否属于贷款类涉诈程序。

3.2 模型识别策略

在基于网络流量的涉诈研判体系中, 通过收集各地涉案情报域名和互联网情报域名, 对 APP 源码、结构等特征进行解析提取, 依据 16 类互联网诈骗分类生成模版策略。通过不断分析积累的识别模版策略库, NTA 研判引擎和分布式研判引擎可以及时发现最新出现的各类涉诈 APP。

a) 网络请求基本信息策略。请求中也包含着能够代表 APP 内容的很多关键参数。通过分析这些关

键参数, 找出能够代表某类涉诈 APP 的模版策略, 形成网络请求基本信息模版策略。

b) 恶意程序关键源码模版策略。源代码是 APP 功能的底层体现, 在访问程序时, 通过加载、渲染和执行相应的代码, 在设备中加载相应功能。贷款类诈骗 APP 中往往会带有各类贷款相关的信息, 因此可以通过源码进行分析, 并基于这一关系进行检测。

c) 策略的更新和优化。从实时性和准确性两方面入手, 在实时性方面, 将每天新检出的模板特征及时更新至统一特征库平台, 校验通过后下发全国, 提升引擎检测信息能力, 进而提高劝阻成功率。在准确性方面, 首先对识别策略进行自检测, 其次是类型库比对检测, 若命中多种类型的样本则需要更新策略。最后进行现网抽检, 若出现检出误报情况, 则需查找原因重新设定策略。

本案例对获取的网络流量进行分析还原, 提取涉诈 APP 源码, 构建涉诈贷款类 APP 的策略和模型。流量还原技术将这些碎片化的数据包重新“拼接”成完整的会话和文件。通过还原 HTTP/HTTPS、DNS、TLS/SSL 等协议, 系统能够精准地识别出 APP 连接的域名和 IP 地址, 特别是那些使用短生命周期域名、DGA 域名或指向境外小众数据中心的服务器, 这些是涉诈应用的典型基础设施特征。此外, 系统还可分析出异常的通信模式: 在用户提交贷款申请后, 立即高频联系多个不同的第三方支付或短信接口, 该行为暗示其正在同步实施信息窃取或发送诈骗短信。

使用时, 输入待测的 APP 中文名称, 例如“急速贷”“信用钱包”等。接下来, 将输入的待测 APP 名称

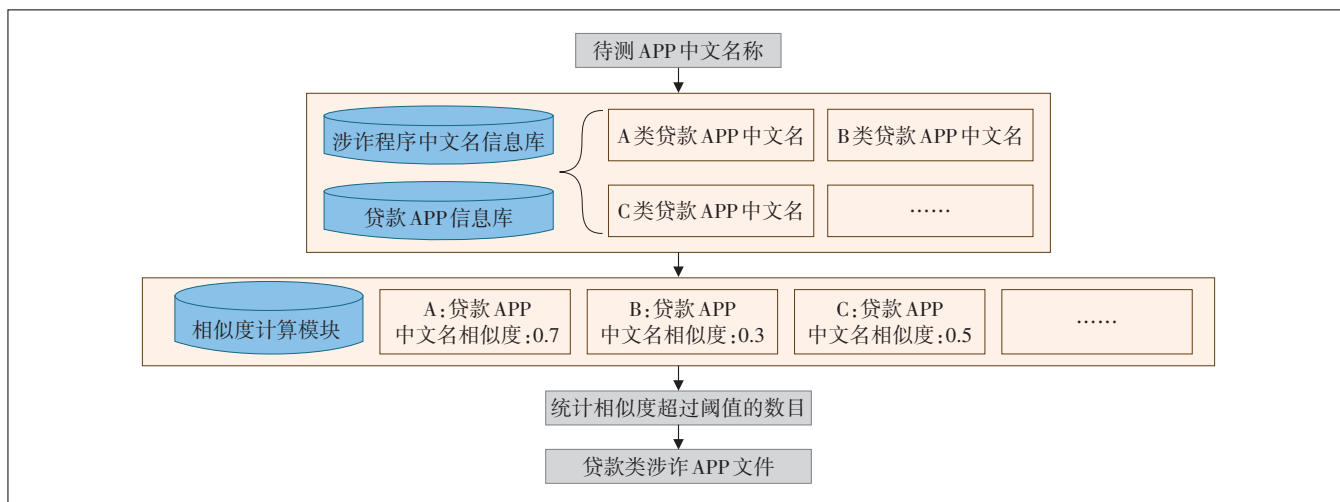


图 5 涉诈贷款 APP 的识别

与贷款信息库进行匹配。系统中保存了已知涉诈贷款APP名称库和正常的贷款APP名称库,系统可通过“贷”“钱包”等关键词进行模糊匹配,识别潜在的涉诈APP。其次,进行相似度计算:将待测APP名称与信息库中的名称逐一比对,计算待测名称与库中每个样本的相似度分值,这些分值设定在0~1区间。最后,进行阈值判断并输出报告:预设一个相似度阈值为0.6,统计超过该阈值的匹配数量,若超过阈值的匹配数达到判定标准,则判定待测APP为涉诈贷款APP,并输出涉诈APP文档。

该方案主要利用文本相似度算法进行快速筛查,适用于识别仿冒知名贷款APP或包含特定敏感词的恶意应用,作为涉诈APP检测系统中的初级过滤模块,需要配合后续的动态行为检测来提升研判准确性。流程中信息库需持续更新维护,以应对不断变化的诈骗APP命名策略。

4 总结和展望

随着移动互联网的发展,小众涉诈APP已成为网络犯罪分子实施诈骗的重要工具,不仅会侵害用户的财产安全,还会威胁公众数据安全和隐私。建立高效的涉诈APP识别机制,能够有效阻断诈骗链条,保护公众利益,维护网络生态安全^[15]。本文提出的动态研判与静态研判相结合的检测体系,充分发挥二者的协同优势。静态研判通过代码特征、权限分析等手段快速筛查出可疑应用,而动态研判借助沙箱环境监控APP的实时行为,识别其隐藏的恶意逻辑。二者共存既保证了模型的检测效率,又提高了研判准确性,对采用混淆、对抗技术的涉诈APP具有更强的识别能力。

未来,小众涉诈APP检测技术将朝着更智能、更全面的方向发展。一方面,可结合深度学习与大数据分析技术,提升特征提取的精度和行为建模的能力;另一方面,需加强多方协作,建立跨平台、跨行业的信息共享机制,实现涉诈情报的实时同步。此外,随着诈骗手段不断升级,检测系统也需持续优化动态与静态研判的协同机制,形成闭环防护体系,以应对日益复杂的网络安全挑战。

参考文献:

- [1] 翟福龙. 一种涉诈APP分析方法[J]. 网络安全技术与应用, 2022(4):135-138.

- [2] 夏艺丹,李乔宇,施俊帆. 混合特征的涉诈类APP分析模型的构建与研究[J]. 计算机时代, 2023(12):81-84.
- [3] 陈德兴,曾茂晰. 涉诈虚假APP的识别研究与应对措施探讨[J]. 广东公安科技, 2021, 29(3):5-7.
- [4] Kumar P P, Kasiviswanath N, Babu A S. Detecting Mobile App Fraud Review and Fake Ranking [C]//International Conference on Advanced Materials, Manufacturing and Sustainable Development (ICAMMSD 2024). Atlantis Press, 2025:313-318.
- [5] Anand A, Shivam, Manhas T, et al. Smali Code-Based Fake Application Detection [C]//International Conference on Computational Intelligence in Communications and Business Analytics. Cham: Springer Nature Switzerland, 2024: 145-160.
- [6] Rahman M, Hernandez N, Recabarren R, et al. The Art and Craft of Fraudulent App Promotion in Google Play [C]//the 2019 ACM SIGSAC Conference. ACM, 2019.
- [7] Thao L Q, Kien D T, Thuy D T T, et al. Designing a deep learning-based application for detecting fake online reviews [J]. Engineering Applications of Artificial Intelligence, 2024, 134(000): 14.
- [8] 周宇飞,马洪晓,胡铁,等. 一种涉诈APP检测系统和方法: 202211692329[P]. 2025-04-23.
- [9] 陆文红,刘剑. 基于大数据+AI机器学习的反诈模型研究[J]. 邮电设计技术, 2022(9):59-64.
- [10] 李玲玲,牛军生,蔡政. 涉虚假App的电信网络诈骗犯罪侦查难点与对策研究[J]. 中国人民公安大学学报(自然科学版), 2021, 27(2):56-61.
- [11] Dodman D. Fighting back against APP fraud [J]. Property Week, 2021(4):88.
- [12] Rahangdale G, Craig J, Gopikrishnan P, et al. Fraud App Detection using Sentimental Analysis [J]. Journal of Applied Information Science, 2023, 11(2):29-34.
- [13] Khan A, Gurav T. Integrated Approach for Mobile App Ranking Fraud Detection [J]. Imperial journal of interdisciplinary research, 2016, 2(6):1712-1716.
- [14] Javier G, Sébastien, Marcel, Julian F. Image Quality Assessment for Fake Biometric Detection: Application to Iris, Fingerprint, and Face Recognition [J]. IEEE transactions on image processing: a publication of the IEEE Signal Processing Society, 2015, 23(2):710-24.
- [15] Shibu H M, Datta S, Miah M S, et al. From Scarcity to Capability: Empowering Fake News Detection in Low-Resource Languages with LLMs [EB/OL]. [2026-02-16]. <https://arxiv.org/pdf/2501.09604>.

作者简介:

孙婧瑜,博士,主要从事网络安全产品和人工智能研究工作;余思阳,高级工程师,硕士,主要从事网络安全体系规划及产品应用工作;曹京卫,高级工程师,主要从事运营商网络信息安全的规划、建设与运营,网络安全产品、网络安全数据服务产品开发工作;刘珊珊,硕士,主要从事网络安全产品研究及应用实践等工作;陆小军,学士,主要从事网络安全产品及应用实践等工作。