网络安全测量研究综述

朱倍江
1024041144
南京邮电大学

摘要—本报告对网络安全测量领域进行了全面的知识体系化梳理，其分析基于 2019 年至 2024 年间发表于五大顶级网络安全学术会议（IEEE S&P、USENIX Security、NDSS、CCS、IMC）的研究成果。通过对数百篇论文的分析与归类，我们提炼了该领域的发展演进、核心方法论及重要发现。我们的分析围绕五大核心主题展开：（1）保障互联网基础协议安全的持续性努力；（2）对复杂且不断演化的对抗性生态系统的特征刻画；（3）测量技术在新兴技术领域（如人工智能和去中心化系统）的拓展应用；（4）对安全与隐私中“人的因素”日益增长的关注；以及（5）测量科学本身的成熟，包括方法论和伦理方面的考量。我们识别出若干贯穿性的趋势，包括良性测量对攻击技术的再利用、人工智能作为分析对象和工具的双重角色，以及对“真实世界”大规模纵向研究的日益重视。本报告最后概述了关键的开放性挑战和未来有前景的研究方向，旨在为研究人员和实践者在现代网络安全测量领域提供一份基础性参考。

***Index Terms*—Network security measurement, cyber security measurement, security metrics, security assessment, network security evaluation**

I. 引言

测量是实证计算机科学的基石。在网络安全领域，测量将抽象的威胁转化为可量化的风险，从而指导有效防御措施的开发、评估与部署。可以明确地说，“无法测量，就无法保护”。

该领域的演进轨迹清晰可见，从早期的网络监控和入侵检测，发展到当前对复杂的、多阶段攻击和社会技术系统的特征刻画。研究焦点已从测量简单的网络现象（如丢包率）转向分析精密的攻击活动。

本报告的范围限定于 2019 年至 2024 年间，聚焦于五大顶级学术会议：IEEE S&P、USENIX Security、ACM CCS、NDSS 和 ACM IMC。选择这“五大”会议是经过深思熟虑的，因为它们代表了同行评议安全研究的最高水平，共同塑造了该领域的发展方向 [1]。其中，IMC 是纯粹测量研究的首要会议，而“四大”安全会议则展示了这些测量成果如何被应用于解决关键安全问题。本报告采用主题式结构，旨在提供一个全面的综述，不仅总结研究成果，更致力于连接不同研究分支，识别宏观趋势，并为未来工作指明方向。

II. 巩固根基：核心互联网基础设施的安全测量

本节分析致力于评估互联网基础协议安全性和韧性的研究。这些研究至关重要，因为核心基础设施的脆弱性会对建立其上的所有服务产生连锁反应。该领域的研究通常以大规模、纵向测量为特征，旨在追踪协议的部署情况、识别错误配置，并验证安全扩展在真实世界中的有效性。

A. 路由安全测量（*BGP*、*RPKI*、*MANRS*）

边界网关协议（BGP）劫持和路由泄露仍然是持续存在的威胁。此领域的研究旨在测量资源公钥基础设施（RPKI）和路由安全互认规范（MANRS）等防御机制的采纳率和有效性。

相关研究揭示了安全协议测量的清晰生命周期：首先是测量问题本身（如 BGP 劫持），随后是测量解决方案的部署情况（如 RPKI 的采纳率），接着是评估方案的有效性（如无效路由的减少），最后是测量解决方案自身的脆弱性（如 RPKI 降级攻击）。这一循环展示了路由安全测量领域的成熟度。例如，早期的工作侧重于检测劫持，随着 RPKI 的开发，焦点转向追踪其部署情况 [3]。当部署达到一定规模后，研究人员开始探究其是否真正有效 [4]。如今，随着 RPKI 成为核心基础设施的一部分，对抗性研究开始探测其弱点 [5]，从而完成一个循环并为下一代防御技术（如 ASPA [6]）开启新的循环。

具体而言，《RPKI is Coming of Age: A Longitudinal Study of RPKI Deployment and Invalid Route Origins》[3] 和《On Measuring RPKI Relying Parties》

[7] 等研究提供了关键的纵向数据，显示了 RPKI 缓慢但稳健的部署进程。它们不仅测量部署数量，还分析了其对无效路由宣告的实际影响。《Mind Your MANRS: Measuring the MANRS Ecosystem》 [9] 则超越了纯协议分析，对一个由社区驱动的倡议进行测量，评估 MANRS 参与者是否真正遵守了其安全最佳实践，这标志着研究向测量社会技术型安全解决方案的转变。同时，BGP 劫持问题的持续存在催生了对新型检测方法的研究，如《Themis: Accelerating the Detection of Route Origin Hijacking》 [10] 和《ROV-MI: Large-Scale, Accurate and Efficient Measurement of ROV》 [4] 旨在提升恶意路由事件检测的速度和准确性。然而，防御机制并非完美，《Stalloris: RPKI Downgrade Attack》 [5] 的研究表明，即使已部署的安全机制也可能存在设计缺陷，凸显了对防御措施本身进行持续测量和对抗性测试的必要性。

B. 域名与解析安全测量（DNS、DNSSEC、DoH/DoT、缓存投毒）

域名系统（DNS）是缓存投毒等攻击的常见目标，也是隐私和审查测量的关键节点。该领域的研究重点在于安全扩展（DNSSEC、DoH/DoT）的部署情况以及新旧漏洞的发现。

一个强有力的趋势是通过新的测量视角“重新发现”旧的威胁。《DNS Cache Poisoning Attack Reloaded: Revolutions With Side Channels》 [11] 是一篇里程碑式的论文，它证明了一个经典的、被认为已解决的攻击（SAD-DNS）由于旁路信道的存在而依然可行，这激发了新一轮的测量和防御研究。社区曾认为 SAD-DNS 攻击已基本被缓解，然而这篇 CCS '20 的论文表明，网络层面的旁路信道使其再度变得现实。这激发了新的研究兴趣。随后，CCS '24 的论文《Internet's Invisible Enemy: Detecting and Measuring Web Cache Poisoning in the Wild》 [12] 在此基础上更进一步，不仅关注单一漏洞，而是创建了一个系统化的框架（HCache）来发现

任何缓存投毒漏洞，并发现了全新的攻击类别。这显示了研究从测量特定已知缺陷到构建框架以测量一类缺陷的演进。该研究发现，Tranco 排名前 1000 的域名中有 17

加密 DNS 协议的部署和性能是另一个主要焦点。《An End-to-End, Large-Scale Measurement of

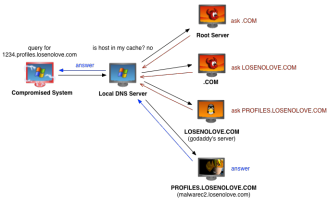

图 1. DNS 流量测量示意图

DNS-over-Encryption》 [3] 和《DNS Privacy with Speed? Evaluating DNS over QUIC and its Impact on Web Performance》 [9] 等研究测量了 DoH/DoT/DoQ 在隐私增益与潜在性能成本之间的权衡。此外，对 DNS 生态系统复杂性的研究，如《TsuNAME: exploiting misconfiguration and vulnerability to DDoS DNS》 [15]，揭示了错误配置如何导致强大的放大攻击。而《Roll, Roll, Roll Your Root: A Comprehensive Analysis of the First Ever DNSSEC Root KSK Rollover》 [3] 等纵向研究为维护全球安全基础设施的运营挑战提供了宝贵的见解。

C. 传输层与应用协议安全测量（TLS、QUIC、Web 缓存、邮件认证）

这一领域涵盖了直接承载用户数据的协议的安全性。测量工作主要关注密码学的正确实现、证书生态系统的健康状况，以及安全头部和策略的采纳情况。

在邮件安全方面，《A Large-scale and Longitudinal Measurement Study of DKIM Deployment》 [16] 是一个深度、多维度的测量研究典范。它结合了被动 DNS 数据、邮件头和主动扫描，发现尽管 DKIM 的采纳率可观（Alexa 前 100 万域名中占 28.1

在 TLS 和证书生态系统方面，《Does Certificate Transparency Break the Web? Measuring Adoption and Error Rate》 [21] 和《Certificate Transparency in the Wild: Exploring the Reliability of Monitors》 [22] 评估了证书透明度（CT）生态系统的健康状况，这是检测恶意证书的关键组成部分。一个反复出现的主题是，尽管多年来不断有警告，但应用程序仍然未能正确实现 TLS [20]。

对于新兴协议，QUIC 的兴起推动了如《QUICsand: Quantifying QUIC Reconnaissance Scans and DoS Flooding Events》 [23] 和《It's over 9000: analyzing early QUIC deployments》 [15] 等测量研究，刻画了其早期部署模式和安全挑战。

贯穿这些研究的一个共同主题是安全部署的“最后一公里”问题。无论是 DKIM、TLS 还是其他协议，初步部署只是成功的一半。真正的安全效益常常因持续的错误配置、糟糕的密钥管理以及未能采纳最佳实践（如 DKIM 中的过签名 [19]）而受到损害。这表明，未来的研究不仅要关注协议

是否被使用，更要关注它如何被使用，这需要更细致的度量标准来捕捉部署的质量，而不仅仅是其存在。

III. 描绘阴影：对抗性生态系统特征刻画

本节探讨利用测量来理解和量化攻击者及其基础设施行为的研究。这些研究对于制定有效的威胁情报、检测系统和缓解策略至关重要。它们通常涉及从敌对环境（如僵尸网络、暗网市场和诈骗活动）中进行创新的数据收集。

A. 恶意软件、僵尸网络与非法服务

理解恶意软件和僵尸网络的生命周期、基础设施及经济模式是安全研究的基石。测量研究追踪了从 Mirai 等物联网僵尸网络到安卓恶意软件分发的各种威胁。

研究趋势已从测量单一威胁转向测量整个威胁生态系统。早期的恶意软件研究可能集中于分类一个二进制文件或分析单个僵尸网络的 C2 协议。而近期的论文展现了更宏观、系统化的视角。例如，《Cleaning Up the Internet of Evil Things: Real-World Evidence on ISP and Consumer Efforts to Remove Mirai》 [28] 和《Measurement and Analysis of Hajime, a Peer-to-peer IoT Botnet》 [28] 深入剖析了特定的大规模物联网僵尸网络，刻画了它们的传播方式以及清除工作的有效性，这延续了早期对僵尸网络测量的传统 [29]。更进一步，《A Large-scale Temporal Measurement of Android Malicious Apps》 [30] 进行了纵向分析，揭示了恶意活动如何随时间持续存在并在不同应用商店间迁移。而《Resident Evil: Understanding Residential IP Proxy as a Dark Service》 [21] 则测量了一个完整的非法

服务，展示了被攻陷的家庭 IP 如何被货币化，用于进一步的恶意活动。这种演进表明，研究人员正在从分析单个实体转向分析支撑网络犯罪的经济和后勤系统。

B. 网络欺诈、诈骗与滥用

该领域关注网络犯罪中面向用户的一面，测量依赖社会工程学的钓鱼、网络诈骗和其他滥用行为的普遍性与机制。

刻画这类复杂的滥用行为需要超越单一的网络追踪。最具影响力的研究现在整合了多种方法论。《Like, Comment, Get Scammed: Characterizing Comment Scams on Media Platforms》 [26] 是现代生态系统特征研究的典范。它首先通过自定义基础设施收集了包含 880 万条评论的大规模数据集；然后开发了基于文本、图像和时间特征的多维度过滤器来识别诈骗；接着通过 IRB 批准的用户研究，主动与 50 名诈骗者互动以了解其后端操作；最后利用区块链分析来量化其财务影响。这篇在 NDSS 2024 上获得杰出论文奖的成果，全面揭示了诈骗活动的运作模式、规避策略（如使用视觉相似字符 [32]）以及高达数百万美元的经济损失。

同样，《Sunrise to Sunset: Analyzing the End-to-end Life Cycle and Effectiveness of Phishing Attacks at Scale》 [33] 提供了对钓鱼攻击的纵向视角，测量了从攻击发起至被缓解的“黄金时间”，并量化了受害者数量和经济损失。而《C-FRAME: Characterizing and measuring in-the-wild CAPTCHA attacks》 [35] 则开发了一个新颖的测量系统，实时捕获 CAPTCHA 破解请求，揭示了从 Twitter 僵尸账号创建到黄牛抢票等滥用行为的规模和性质。

人的因素是核心。《A Representative Study on Human Detection of Artificially Generated Media Across Countries》 [35] 测量了一个关键的非技术方面：人类对伪造媒体的感知能力。研究发现，人们不仅不擅长识别伪造品，甚至常常认为 AI 生成的内容比真实内容

更可信，这对信息战和虚假信息传播具有深远影响。

C. 互联网审查与信息控制

测量互联网审查是一个充满挑战但至关重要的领域。研究旨在识别哪些内容被封锁、在何处被封锁以及使用了何种技术机制，最终目标是开发有效的规避策略。

审查与反审查之间的猫鼠游戏正在加速。审查方部署了更复杂的、通常基于机器学习的封锁系统。作为

表 I
核心基础设施安全关键测量研究概览

论文标题与引用	领域	方法论	数据集/规模	关键发现
Internet's Invisible Enemy: Detecting and Measuring Web Cache Poisoning in the Wild [12]	DNS/Web 缓存	大规模主动扫描，采用新颖的 HCache 框架	Tranco Top 1000 域名及其 22,114 个子域名	[17]% 的被测域名易受 WCP 攻击；发现了 7 种新的攻击向量。
A Large-scale and Longitudinal Measurement Study of DKIM Deployment [17]	邮件认证	被动 DNS、邮件头分析、主动扫描	[5] 年的 950 万条 DKIM 记录，4.6 亿个 DKIM 签名，Alexa Top [1]M 域名	[28].1% 的域名启用了 DKIM，但其中 2.9% 存在错误配置，且普遍存在弱密钥和弱签名问题。
Your Router is My Prober: Measuring IPv6 Networks via ICMP Rate Limiting Side Channels [24]	IPv6/路由	利用 ICMP 速率限制旁路信道进行主动测量	110 万个远程路由器，覆盖 9.5k 个 AS	提出了一种仅需单个观测点即可大规模测量 IPv6 网络属性（如 ISAV 部署）的新方法。
RPKI is Coming of Age: A Longitudinal Study of RPKI Deployment and Invalid Route Origins [**?**]	路由安全	纵向被动数据分析	RPKI 仓库和 BGP 更新数据	测量了 RPKI 的部署增长情况，并量化了其在减少无效路由宣告方面的有效性。
Like, Comment, Get Scammed: Characterizing Comment Scams on Media Platforms [26]	在线欺诈	大规模数据收集、多特征检测、与攻击者互动（用户研究）、区块链分析	880 万条 YouTube 评论，与 50 名诈骗者互动	刻画了评论诈骗的活动、动态和规避技术，并量化了数百万美元的经济损失。
"Do Anything Now": Characterizing and Evaluating In-The-Wild Jailbreak Prompts on LLMs [**?**]	AI 安全	真实世界越狱提示的收集与分类，对主流 LLM 的有效性测试	[1],405 个越狱提示，针对 6 个主流 LLM 的 107,250 个测试样本	现有 LLM 安全措施对越狱提示普遍无效（部分成功率 >95%）；识别了主要攻击策略。

回应，研究社区正转向自动化发现规避策略。《Geneva: Evolving Censorship Evasion Strategies》 [36] 代表了一种范式转变。它不再手动发现规避技术，而是使用遗传算法通过操纵数据包流来

自动演化出新的策略。这是一种从 "为理解而测量" 到 "为行动而测量" 的转变。该方法将问题框架化为一个演化搜索空间，其中 "基因" 是数据包操纵原语（如丢弃、篡改、分片）。通过 "繁殖" 策略并测试其 "适应度"（即是否绕过审查），Geneva 实现了发现过程的自动化。

与此同时，基础设施的建设也在推进。《ICLab: A Global, Longitudinal Internet Censorship Measurement Platform》 [39] 和《Censored Planet: An Internet-wide, Longitudinal Censorship Observatory》 [40] 描述了进行持续、全球规模审查监控所需的基础设施，使研究人员能够追踪封锁策略随时间的变化。而对特定国家审查技术的研究，如《How China Detects and Blocks Shadowsocks》 [7] 和《Investigating Large Scale HTTPS Interception in Kazakhstan》 [7]，为设计有效的规避工具提供了必要的实证依据。这表明，该领域的未来在于能够实时动态适应不断变化的审查环境的 AI 驱动系统。

IV. 拓展前沿：新兴技术领域的测量

本节涵盖了将安全测量原理应用于新兴和快速发展的技术领域。这里的挑战通常是双重的：不仅系统是新的，而且应该测量什么以及如何测量的定义本身也常常是开放的研究问题。

A. 人工智能与机器学习的攻击面

随着人工智能/机器学习模型，特别是大型语言模型（LLM）的普及，它们引入了新颖的攻击面。该领域的测量研究旨在刻画和量化这些新的脆弱性，从数据投毒到提示注入和有害内容的生成。

一个定义现代安全研究的特征是人工智能（AI）的双重角色。一方面，AI 是新的测量对象，研究人员正在量化其对越狱攻击、数据投毒和深度伪造的脆弱性 [27]。另一方面，AI 正成为一种

测量工具，用于异常检测 [43]、日志分析 [44]，甚至演化出审查规避策略（如第二节所述）。

在 LLM 越狱方面，《"Do Anything Now": Characterizing and Evaluating In-The-Wild Jailbreak Prompts on Large Language Models》 [27] 是一项基础性的测量研究。它收集并分析了上千个真实世界的越狱提示，对其攻击策略（如权限提升）进行分类，并

表 II
对抗性生态系统测量研究分类法

威胁类别	论文标题与引用	主要数据源	测量方法	关键特征/发现
恶意软件/僵尸网络	Cleaning Up the Internet of Evil Things: Real-World Evidence on ISP and Consumer Efforts to Remove Mirai [?]	僵尸网络扫描数据、ISP 报告	纵向数据分析、生态系统参与者行为分析	刻画了 Mirai 僵尸网络的清除过程，评估了 ISP 和消费者在缓解威胁中的作用。
在线欺诈/诈骗	Like, Comment, Get Scammed: Characterizing Comment Scams on Media Platforms [26]	YouTube API、WhatsApp、公共区块链	被动数据收集、主动与对手互动（用户研究）、金融交易分析	刻画了诈骗活动、规避策略（身份伪装、文本混淆），并量化了数百万美元的经济损失。
互联网审查	Geneva: Evolving Censorship Evasion Strategies [?]	实验室和真实世界审查系统（中国、印度、哈萨克斯坦）	基于遗传算法的主动探测与策略演化	自动化发现了新的审查规避策略，揭示了审查系统中的未知行为。
恶意软件分类	TESSERACT: Eliminating Experimental Bias in Malware Classification across Space and Time [?]	安卓应用数据集(12.9 万个应用，跨越 3 年)	提出了时空约束和新的评估指标（AUT），以消除实验偏见	证实了先前研究结果存在偏差，并展示了通过适当调优可显著提升分类器性能。
漏洞利用	C-FRAME: Characterizing and measuring in-the-wild CAPTCHA attacks [?]	CAPTCHA 破解服务平台	设计并部署了首个用于收集真实世界 CAPTCHA 攻击数据的测量系统	捕获了超过 42 万次攻击，涵盖 1417 个网站，识别了 34 种攻击类别，包括僵尸账户创建和黄牛抢票。

测量了它们对主流 LLM 的有效性，发现成功率高达 95

在深度伪造检测方面，《A Representative Study on Human Detection of Artificially Generated Media》 [35] 测量了一个关键的非技术层面：人类的感知能力。研究发现，人们不仅不擅长识别伪造内容，甚至认为 AI 生成的内容

更可信，这对虚假信息的影响发出了严峻警告。技术性检测论文如《ProFake: Detecting Deepfakes in the Wild...》 [43] 则对此进行了补充。

在模型安全方面，《BadMerging: Backdoor Attacks Against Model Merging》 [45] 和《Membership Inference Attacks...》 [5] 等论文测量了机器学习流程本身的安全问题，展示了投毒模型或窃取敏感训练数据的新方法。这种从将 ML 应用于安全问题（如恶意软件检测 [47]）到测量 ML 模型自身安全性的演进，展示了测量社区如何将其方法论适应于一个全新的、以语义失效为特征而非传统缓冲区溢出的漏洞类别。

B. 去中心化系统的安全性与经济学

区块链、加密货币和去中心化金融（DeFi）创建了一个新颖的社会经济系统，带来了独特的安全和隐私挑战。测量研究对于理解市场动态、矿工行为、智能合约漏洞以及隐私技术的有效性至关重要。

区块链的透明性悖论为安全测量提供了独特的机遇。区块链常因其透明性而备受赞誉，而正是这种透明性使其成为安全测量的沃土。研究人员可以分析一个完整的、不可变的、公开的交易历史。这催生了强大的新测量方法，例如精确量化诈骗的经济影响 [26] 或分析像矿工可提取价值（MEV）这样的市场级现象 [48]。然而，同样的透明性也是主要隐私问题的根源，这反过来又推动了对隐私保护测量技术的研究。

《BlockSci: Design and applications of a blockchain analysis platform》 [49] 是一个关键的基础设施项目，它提供了一个高性能工具来解析和分析区块链数据，极大地推动了后续研究。利用这类平台，研究人员得以深入分析加密货币生态中的欺诈行为。例如，《Like, Comment, Get Scammed》 [26] 利用区块链分析来追踪和量化诈骗的资金流，而《TxPhishScope: Towards Detecting and Understanding Transaction-based Phishing on Ethereum》 [46] 则专门研究了以太坊生态系统内的钓鱼活动。

在市场动态方面，《Flash Boys [2].0: Frontrunning in Decentralized Exchanges, Miner Extractable Value, and Consensus Instability》 [48] 测量了由 MEV 引起的经济激励及其带来的安全风险（如共识不稳定性），而《Demystifying DeFi MEV Activities in Flashbots

Bundle》 [46] 则对这些活动进行了更深入的刻画。

在智能合约漏洞方面，《Smart Contract Vulnerabilities: Vulnerable Does Not Imply Exploited》 [20] 提供了一个重要的、基于测量的现实检验，分析了理论上存在漏洞的合约与在野外被实际利用的合约之间的差距。

C. 物联网与网络物理系统的威胁

联网设备在家庭、工业和车辆中的普及，创建了一个巨大且异构的攻击面。由于设备多样性、专有协议以及大规模数据收集的困难，该领域的测量充满挑战。

面对不透明的嵌入式设备，一个强大且反复出现的测量技术是分析用于控制该设备的移动伴侣应用 [46]。研究人员发现，他们无需直接分析嵌入式设备的固件，而是可以通过分析其配套的安卓或 iOS 应用来获取关键信息。这些应用中包含了 API 端点、协议细节和硬编码的凭证，为理解设备的后端基础设施和潜在漏洞提供了路线图。这是一个巧妙的思路转变，将一个限制（不透明的设备）转化为了一个机遇。

利用这种方法，《Information Exposure From Consumer IoT Devices: A Multidimensional, Network-Informed Measurement Approach》 [3] 和《Deep Dive into the IoT Backend Ecosystem》 [9] 通过网络流量分析，描绘出物联网设备数据流向，揭示了制造商和第三方进行的大量数据收集活动。《OVRseen: Auditing Network Traffic and Privacy Policies in Oculus VR》 [54] 将此方法应用于 VR 生态系统，发现了隐私政策与实际数据流之间的显著差异。

在漏洞发现方面，《SoK: Security Evaluation of Home-Based IoT Deployment》 [21] 对家庭物联网威胁进行了知识系统化梳理。而《FirmWire: Transparent Dynamic Analysis for Cellular Baseband Firmware》 [4] 等研究开发了新的工具，用于自动发现这些不透明设备固件中的漏洞。对于网络物理系统和汽车安全，《A Comprehensive Analysis of Security Vulnerabilities and Attacks in Satellite Modems》 [43] 和《Automated Cross-Platform Reverse Engineering of CAN Bus Commands》 [57] 展示了测量和逆向工程在关键基础设施和车辆安全分析中的应用。

V. 人的因素：面向用户的安全与隐私测量

本节聚焦于将人作为被测系统核心组成部分的研究。通过研究用户的行为、理解和感知，评估安全机制在真实世界中的有效性，并量化直接影响个体的隐私危害。

A. 安全系统中的可用性、感知与行为

一个技术上安全但用户无法使用或理解的系统，在实践中并不安全。该研究领域运用人机交互（HCI）的方法来测量安全的“面向人”的方面。

该领域一个重要的研究线索是测量安全系统设计工作方式与用户感知工作方式之间的差距。这种“心智模型失配”是许多安全失败的根源。研究正从简单地宣称“可用性很重要”转向定量地测量这些失配及其安全影响。例如，一个开发者创建了一个密码管理器，认为其价值主张显而易见。而像《”I don’ t see why I would ever want to use it”: Analyzing the Usability of Popular Smartphone Password Managers》 [22] 这样的用户研究论文则通过测量用户感知发现，用户认为“太麻烦”、“不信任它存储所有密码”或“不理解其工作原理”。这不是密码管理器的技术失败，而是其设计未能与用户关于信任和便利性的心智模型对齐。

具体来说，《Is FIDO2 the Kingslayer of User Authentication? A Comparative Usability Study...》 [39] 和上述密码管理器研究 [22] 通过用户研究，测量了现代认证技术的可用性和采纳障碍，揭示了即使技术上更优越的解决方案在用户接受度和理解方面也面临重大挑战。同时，《”If HTTPS Were Secure, I Wouldn’t Need [2]FA” - End User and Administrator Mental Models of HTTPS》 [21] 测量了人们对 HTTPS 等安全技术的心智模型，常常发现关键且危险的误解。《A Comprehensive Quality Evaluation of Security and Privacy Advice on the Web》 [33] 则测量了普通用户能接触到的网络安全建议的质量，发现它们往往不一致、不完整或不切实际。这些测量为设计者提供了纯技术分析无法提供的具体、可操作的反馈。

B. 隐私泄露与网络追踪的普遍性

这类研究量化了用户数据在网络上被收集、共享和暴露的程度，这些行为通常对用户不透明或出乎意

表 III
新兴领域测量方法总结

领域	论文标题与引用	测量对象	新颖方法论/挑战	关键发现
AI/ML	”Do Anything Now”: Characterizing and Evaluating In-The-Wild Jailbreak Prompts on Large Language Models [?]	真实世界的 LLM 越狱提示	收集和分类自然语言对抗性输入；测量针对闭源商业 API 的成功率。	现有防护措施普遍无效（部分提示成功率 >95%）；识别了常见的攻击模式，如权限提升。
去中心化系统	Flash Boys [2].0: Frontrunning in Decentralized Exchanges, Miner Extractable Value, and Consensus Instability [?]	去中心化交易所中的矿工可提取价值（MEV）	分析公共区块链数据以量化经济激励和系统性风险。	MEV 导致了抢先交易，并可能引发共识层面的不稳定性。
物联网/CPS	OVRseen: Auditing Network Traffic and Privacy Policies in Oculus VR [?]	Oculus VR 应用和平台的数据收集与共享行为	结合网络流量解密、数据流提取和基于 NLP 的隐私政策分析，以检查“言行是否一致”。	约 70% 的数据流未在隐私政策中得到妥善披露；数据主要流向追踪和分析服务。
物联网/CPS	IoTFlow: Inferring IoT Device Behavior at Scale through Static Mobile Companion App Analysis [?]	物联网设备的后端通信行为	通过静态分析移动伴侣应用来推断不透明设备的网络行为，绕过了直接分析设备固件的困难。	能够大规模、自动化地识别物联网设备的云后端和通信协议，揭示潜在的安全和隐私风险。

料。它为推动隐私增强技术（PETs）和制定法规提供了实证依据。

一个强有力且反复出现的发现是，公司在其隐私政策中声称的数据处理方式（“言”）与它们通过网络流量分析测量到的实际数据处理方式（“行”）之间存在巨大且可测量的差距。这种“言行不一”是一个核心主题。这里的研究不仅仅是发现追踪器，更是通过实证证明这种差异来追究平台的责任。

例如，《Watching You Watch: The Tracking Ecosystem of Over-the-Top TV Streaming Devices》[22] 和《OVRseen: Auditing Network Traffic and Privacy Policies in Oculus VR》[54] 是测量新兴生态系统隐私问题的绝佳案例。它们通过监控设备、捕获流量，并绘制数据流向第三方追踪器和分析服务的地图，揭示了一个复杂且通常未披露的数据共享网络。《OVRseen》发现约 70

一些研究揭示了具体的隐私危害。《Leaky Forms: A Study of Email and Password Exfiltration Before Form Submission》[5] 发现了一个惊人的现象：追踪器会在用户输入表单时捕获数据，即使用户从未点击“提交”按钮。《Log: It’s Big, It’s Heavy, It’s Filled with Personal Data! Measuring the Logging of Sensitive Information in the Android Ecosystem》[44] 则发现安卓应用普遍存在记录个人身份信息（PII）的行为。

研究还持续发现隐私政策与实际行为的脱节。除了《OVRseen》的发现，像《POLICYCOMP: Counterpart Comparison of Privacy Policies...》[44] 这样的研究开发了自动化方法，以大规模分析这些法律文件并发现其中的不一致之处。这些工作为监管机构（如 FTC，曾主办关于 OVRseen 的演讲 [59]）和隐私倡导者提供了具体的、无可否认的证据。

VI. 测量科学：方法论、工具与伦理

本节从元层面审视了专注于改进安全测量技术本身的研究。这包括发明新的数据收集技术、构建可重用的分析平台，以及对该领域方法论和伦理基础的批判性反思。

A. 测量技术与观测点的创新

互联网的规模、多样性以及日益增长的加密使用，使得测量成为一项持续的挑战。该领域的研究开发了新颖的方法来观测网络上发生的事情。

面对加密和缺乏合作观测点，研究人员日益采用一种“对抗性思维”来服务于良性目的。他们积极寻找并利用协议和系统中的旁路信道、设计缺陷和经济漏洞，将其作为测量工具。这是一个从传统的被动监控或主动探测向更具对抗性和机会主义的测量方式的重大转变。

《Your Router is My Prober: Measuring IPv6 Networks via ICMP Rate Limiting Side Channels》[24] 是一篇具有范式转换意义的论文。它将一个旨在防止 DoS 攻击的协议特性（ICMP 速率限制）转变为一个旁路信道，用于从单一观测点测量广阔 IPv6 地址空间中的网络可达性和安全策略（ISAV）部署情况。

这种方法巧妙地利用了路由器自身的防御机制来进行测量，是解决测量基础设施缺乏问题的极具创新性的方案。

同样，《C-FRAME: Characterizing and measuring in-the-wild CAPTCHA attacks》 [35] 在 CAPTCHA 破解服务生态系统中识别出一个独特的观测点，从而能够大规模被动收集关于真实世界攻击的数据。而《Geneva: Evolving Censorship Evasion Strategies》 [37] 则利用遗传算法，不仅进行测量，还主动发现与网络中间设备交互并绕过它们的新方法。

B. 分析框架与平台的开发

一次性的测量脚本很有用，但可重用、开源的平台能为整个社区的研究加速。该领域致力于构建网络安全领域的 “科学仪器”。

BlockSci 和 TESSERACT 等平台的开发标志着一个科学学科的成熟。社区不再是每个研究小组都构建自己的临时工具，而是投资于共享、可重用和开源的基础设施。这提高了效率，增强了可复现性，并使研究人员能够更有效地在彼此工作的基础上进行构建。

例如，在区块链分析领域，《BlockSci: Design and applications of a blockchain analysis platform》 [49] 创建了一个高性能的内存数据库，专门用于分析区块链数据，使得大规模分析变得可行，从而催生了一波关于加密货币经济和安全的研究。

在恶意软件分类评估方面，《TESSERACT: Eliminating Experimental Bias in Malware Classification across Space and Time》 [41] 不仅是一项批判，更是一个建设性的解决方案。它提供了一个开源框架，使研究人员能够对基于机器学习的恶意软件分类器进行公平的、时间感知的评估，解决了可复现性和结果虚高这一关键问题。

在审查测量方面，《ICLab》 [39] 和《Censored Planet》 [40] 是大规模、可操作平台的例子，它们为更广泛的研究社区提供了数据和基础设施来研究审查制度。

C. 应对偏见、可复现性与伦理挑战

随着测量研究变得越来越强大并处理更多敏感数据，社区开始对其工作的严谨性和伦理进行批判性自我反思。

在方法论严谨性方面，《TESSERACT》 [41] 是一个典型例子，它指出许多 “机器学习用于恶意软件检测” 的论文因实验设计中的时空偏见而报告了虚高的结果，并提出了更公平评估的具体约束。《Dos and Don’ts of Machine Learning in Computer Security》 [30] 则对这一主题进行了更广泛的知识系统化梳理。

在伦理框架方面，一篇 NDSS 的伦理学论文 [64] 精辟地指出了挑战：“网络数据测量……产生了无数的洞见……然而社区却不存在一个统一的伦理规范来证明这些研究的合理性。” 该论文分析了过往的研究和会议指南，描绘了利益、危害和利益相关者的空间，并呼吁建立一个更结构化的伦理框架。许多测量研究在没有用户同意的情况下收集敏感数据，这带来了伦理困境，并迫使社区就何为合乎伦理的研究展开艰难对话，最终在论文征稿中形成更明确的指南 [65]。

在可复现性方面，像 IMC 等会议设立“复现”分会场 [66]，显示出对可复现性的日益重视。《Replication: ”When to Use and When not to Use BBR”》 [66] 等论文对于验证和建立在先前发现之上的研究至关重要。整个过程是一个科学自我修正和专业化的过程。

VII. 综合与未来方向

本节将综合前述各节的线索，描绘该领域的全貌，并确定未来 5 到 10 年最紧迫的挑战和机遇。

A. 贯穿性趋势综合

- 测量与攻击的双向性：技术在两个方向上流动。旁路信道攻击被重新用于良性测量 [24]，而测量平台则被用于自动化攻击发现 [37]。
- 纵向与 “真实世界” 研究的兴起：研究正从基于实验室的静态数据集转向对真实世界系统进行持续、大规模的监控 [17]。这提供了更现实、更有影响力的结果，但也带来了重大的伦理和数据管理挑战。
- 人工智能的双刃剑效应：AI 既是需要测量的新型复杂攻击面 [27]，也是用于大规模自动化分析和检测的强大工具 [43]。
- 社会技术与经济视角的重要性日益凸显：越来越多的研究将用户行为 [21]、经济激励 [48] 和政策合规性 [5] 作为首要测量对象，认识到技术机制并非存在于真空中。

表 IV
安全测量的方法论进展

方法/平台与引用	解决的问题	核心创新	影响/应用
iVantage / ICMP 旁路信道探测 [24]	缺乏用于测量广阔且稀疏的 IPv6 空间的观测点。	将 ICMP 速率限制视为旁路信道而非障碍。通过观察错误消息速率的变化，从单个探测点推断远程网络属性（可达性、过滤策略）。	实现了迄今为止最大规模的 IPv6 源地址验证（ISAV）测量。提供了一种无需控制端点即可进行远程网络测量的通用技术。
Geneva / 遗传算法 [?]	手动发现审查规避策略速度慢且难以扩展。	将策略发现框架化为演化搜索问题。通过组合、变异和评估数据包操纵原语来自动演化出有效的规避策略。	自动化了审查规避策略的发现过程，找到了多种已知和全新的策略，揭示了审查系统的新行为。
TESSERACT / 消除偏见框架 [?]	基于 ML 的恶意软件分类研究中普遍存在时空偏见，导致结果虚高且缺乏可比性。	提出了用于公平实验设计的具体时空约束，并引入了新的评估指标（AUT）来衡量分类器在真实世界中的鲁棒性。	为社区提供了一个评估 ML 恶意软件分类器的标准框架，提高了研究的可复现性和现实意义。
BlockSci / 高性能分析平台 [?]	分析整个区块链数据的计算成本高昂，阻碍了大规模研究。	设计并实现了一个专门用于区块链分析的、高性能的内存列式数据库，速度远超传统工具。	极大地降低了区块链分析的门槛，催生了大量关于加密货币安全、隐私和经济学的后续研究。

B. 未来研究方向与开放性挑战

- 测量下一代网络（5G/6G 及未来网络）：未来网络架构的安全性是即将举行的研讨会的核心议题 [67]。迫切需要新的测量方法来评估网络切片、卫星通信（NTN）和去中心化无线等特性的安全性。如何测量一个高度虚拟化、动态且由地面和非地面组件构成的网络的安全，是一个核心问题。
- 软件供应链的自动化与持续测量：尽管已有一些工作 [68]，但现代软件供应链的复杂性带来了巨大的测量挑战。未来的工作需要开发可扩展的技术，以持续测量开源依赖、CI/CD 管道和容器镜像仓库中漏洞的引入和传播。
- 开发鲁棒且公平的安全度量标准：正如一篇主题演讲的反思所指出的 [1]，该领域常常缺乏衡量安全成果的鲁棒指标，类似于汽车安全领域的“每百万英里死亡人数”。未来的研究应专注于开发和验证能够衡量实际用户伤害、攻击经济影响以及已部署防御措施真实效益的指标，超越简单的漏洞计数或检测率。
- 主动与对抗性测量的伦理问题：随着像 iVantage [24] 和 Geneva [37] 这样的技术变得越来越普遍，社区需要一个更健全的伦理框架。在何种情况下，“测量”会越界成为“未经授权的访问”或“网络破坏”？我们如何平衡理解对抗性系统的需求与造成伤害的风险？未来的工作必须超越临时的 IRB 批准，建立明确的社区规范和最佳实践 [64]。
- 测量 AI 集成系统的安全性：目前的焦点是模型本身 [27]。下一个前沿是测量一个集成了 AI 的完整系统的安全性。一个与外部 API 和用户数据交互的 LLM 代理如何产生新的、涌现性的安全漏洞？这需要一类新的测量研究，将 AI 模型分析与传统的系统和网络安全技术相结合。

参考文献

[1] NDSS 2022: one of the top four security conference... - SAP Community, [Online]. Available: https://community.sap.com/t5/application-development-and-automation-blog-posts/ndss-2022-one-of-the-top-four-security-conferences/ba-p/13528365, Accessed: June [17], 2025.

[2] A Data-Driven Reflection on [36] Years of Security and Privacy Research - USENIX, [Online]. Available: https://www.usenix.org/system/files/cset19-paper_baset.pdf, Accessed: June [17], 2025.

[3] ACM IMC 2019 - Accepted Papers, [Online]. Available: https://conferences.sigcomm.org/imc/2019/accepted/, Accessed: June [17], 2025.

[4] NDSS Symposium 2022: Accepted Papers, [Online]. Available: https://www.ndss-symposium.org/ndss2022/accepted-papers/, Accessed: June [17], 2025.

[5] USENIX Security '22 Fall Accepted Papers | USENIX, [Online]. Available: https://www.usenix.org/conference/usenixsecurity22/fall-accepted-papers, Accessed: June [17], 2025.

[6] NDSS Symposium 2025 Program, [Online]. Available: https://www.ndss-symposium.org/ndss-program/symposium-2025/, Accessed: June [17], 2025.

[7] ACM IMC 2020 - Accepted Papers, [Online]. Available: https://conferences.sigcomm.org/imc/2020/accepted/, Accessed: June [17], 2025.

[8] ACM IMC 2020 - Freie Universität Berlin, [Online]. Available: https://www.mi.fu-berlin.de/en/inf/groups/ilab/events/ACM-IMC-2020.html, Accessed: June [17], 2025.

[9] ACM IMC 2022 - Accepted Papers, [Online]. Available: https://conferences.sigcomm.org/imc/2022/accepted/, Accessed: June [17], 2025.

[10] USENIX Security '22 Winter Accepted Papers | USENIX, [Online]. Available: https://www.usenix.org/conference/usenixsecurity22/winter-accepted-papers, Accessed: June [17], 2025.

[11] ACM CCS 2020 - November [9]-13, 2020, [Online]. Available: https://www.sigsac.org/ccs/CCS2020/, Accessed: June [17], 2025.

[12] Internet's Invisible Enemy: Detecting and Measuring Web Cache Poisoning in the Wild - Jianjun Chen, [Online]. Available: https://www.jianjunchen.com/p/web-cache-posioning.CCS24.pdf, Accessed: June [17], 2025.

[13] Accepted Papers - ACM CCS 2024, [Online]. Available: https://www.sigsac.org/ccs/CCS2024/program/accepted-papers.html, Accessed: June [17], 2025.

[14] Hui Jiang (disambiguation) - dblp, [Online]. Available: https://dblp.org/pid/64/3246, Accessed: June [17], 2025.

[15] IMC 2021 - dblp, [Online]. Available: https://dblp.org/db/conf/imc/imc2021.html, Accessed: June [17], 2025.

[16] Qingfeng Pan's research works - ResearchGate, [Online]. Available: https://www.researchgate.net/scientific-contributions/Qingfeng-Pan-2183419070, Accessed: June [17], 2025.

[17] A Large-scale and Longitudinal Measurement Study of DKIM Deployment - USENIX, [Online]. Available: https://www.usenix.org/system/files/sec22fall_wang-chuhan.pdf, Accessed: June [17], 2025.

[18] A Large-scale and Longitudinal Measurement Study of DKIM Deployment | Kaiwen Shen, [Online]. Available: https://shenkaiwen.com/publication/2022-dkim/, Accessed: June [17], 2025.

[19] A Large-scale and Longitudinal Measurement Study of DKIM Deployment - USENIX, [Online]. Available: https://www.usenix.org/system/files/sec22_slides-wang_chuhan.pdf, Accessed: June [17], 2025.

[20] USENIX Security '21 Summer Accepted Papers | USENIX, [Online]. Available: https://www.usenix.org/conference/usenixsecurity21/summer-accepted-papers, Accessed: June [17], 2025.

[21] IEEE Symposium on Security and Privacy 2019, [Online]. Available: https://www.ieee-security.org/TC/SP2019/program-papers.html, Accessed: June [17], 2025.

[22] Conference Proceedings –ACM CCS 2019 - ACM SIGSAC, [Online]. Available: https://sigsac.org/ccs/CCS2019/index.php/proceedings/, Accessed: June [17], 2025.

[23] ACM IMC 2021 • Internet Technologies - Freie Universität Berlin, [Online]. Available: https://www.mi.fu-berlin.de/en/inf/groups/ilab/events/ACM-IMC-2021.html, Accessed: June [17], 2025.

[24] Your Router is My Prober: Measuring IPv6 Networks via ICMP Rate Limiting Side Channels, [Online]. Available: https://dev.ndss-symposium.org/wp-content/uploads/2023-49-paper.pdf, Accessed: June [17], 2025.

[25] [2210.13088] Your Router is My Prober: Measuring IPv6 Networks via ICMP Rate Limiting Side Channels - arXiv, [Online]. Available: https://arxiv.org/abs/2210.13088, Accessed: June [17], 2025.

[26] Like, Comment, Get Scammed: Characterizing Comment Scams on Media Platforms, [Online]. Available: https://like-comment-get-scammed.github.io/, Accessed: June [17], 2025.

[27] [20] CISPA Papers at CCS 2024., [Online]. Available: https://cispa.de/en/research/conferences/2024/ccs-2024, Accessed: June [17], 2025.

[28] dblp: NDSS 2019, [Online]. Available: https://dblp.org/db/conf/ndss/ndss2019, Accessed: June [17], 2025.

[29] Understanding the Mirai Botnet - USENIX, [Online]. Available: https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/antonakakis, Accessed: June [17], 2025.

[30] USENIX Security '22 Summer Accepted Papers | USENIX, [Online]. Available: https://www.usenix.org/conference/usenixsecurity22/summer-accepted-papers, Accessed: June [17], 2025.

[31] Network and Distributed System Security (NDSS) Symposium 2024, [Online]. Available: https://www.ndss-symposium.org/ndss2024/, Accessed: June [17], 2025.

[32] Like, Comment, Get Scammed: Characterizing Comment Scams on Media Platforms - Network and Distributed System Security (NDSS) Symposium, [Online]. Available: https://www.ndss-symposium.org/wp-content/uploads/2024-60-paper.pdf, Accessed: June [17], 2025.

[33] [29]th USENIX Security Symposium, USENIX Security 2020, August ..., [Online]. Available: https://researchr.org/publication/uss-2020, Accessed: June [17], 2025.

[34] Sunrise to Sunset: Analyzing the End-to-end Life Cycle and Effectiveness of Phishing Attacks at Scale - USENIX, [Online]. Available: https://www.usenix.org/system/files/sec20-oest-sunrise.pdf, Accessed: June [17], 2025.

[35] [19] CISPA Papers at S&P 2024. The IEEE Symposium on Security and Privacy is the premier forum for presenting developments in computer security and electronic privacy, and for bringing together researchers and practitioners in the field., [Online]. Available: https://cispa.de/en/research/conferences/2024/sandp-2024, Accessed: June [17], 2025.

[36] Geneva: Evolving Censorship Evasion Strategies - ResearchGate, [Online]. Available: https://www.researchgate.net/publication/337096636_Geneva_Evolving_Censorship_Evasion_Strategies, Accessed: June [17], 2025.

[37] Publications | Kevin Bock, [Online]. Available: https://kevinbock.phd/publication/, Accessed: June [17], 2025.

[38] Kevin Bock's research works | Loyola University Maryland and other places - ResearchGate, [Online]. Available: https://www.researchgate.net/scientific-contributions/Kevin-Bock-2166285163, Accessed: June [17], 2025.

[39] SP 2020 - dblp, [Online]. Available: https://dblp.org/db/conf/sp/sp2020, Accessed: June [17], 2025.

[40] Accepted Papers - ACM CCS 2020 - ACM SIGSAC, [Online]. Available: https://www.sigsac.org/ccs/CCS2020/accepted-papers.html, Accessed: June [17], 2025.

[41] Top 158 papers presented at USENIX Security Symposium in 2019 - SciSpace, [Online]. Available: https://scispace.com/conferences/usenix-security-symposium-2nqvgoik/2019, Accessed: June [17], 2025.

[42] [Literature Review] TESSERACT: Eliminating Experimental Bias in Malware Classification across Space and Time (Extended Version) - Moonlight, [Online]. Available: https://www.themoonlight.io/en/review/tesseract-eliminating-experimental-bias-in-malware-classification-across-space-and-time-extended-version, Accessed: June [17], 2025.

[43] CCS 2024 - dblp, [Online]. Available: https://dblp.org/db/conf/ccs/ccs2024, Accessed: June [17], 2025.

[44] USENIX Security '23 Technical Sessions | USENIX, [Online]. Available: https://www.usenix.org/conference/usenixsecurity23/technical-sessions, Accessed: June [17], 2025.

[45] Network and Distributed System Security Symposium (NDSS) 2023, [Online]. Available: https://www.ndss-symposium.org/ndss2023/, Accessed: June [17], 2025.

[46] CCS 2023 - dblp, [Online]. Available: https://dblp.org/db/conf/ccs/ccs2023, Accessed: June [17], 2025.

[47] CCS 2022 - dblp, [Online]. Available: https://dblp.org/db/conf/ccs/ccs2022, Accessed: June [17], 2025.

[48] Accepted Papers - IEEE Symposium on Security and Privacy 2020, [Online]. Available: https://www.ieee-security.org/TC/SP2020/program-papers.html, Accessed: June [17], 2025.

[49] BlockSci: Design and applications of a blockchain analysis platform | Request PDF, [Online]. Available: https://www.researchgate.net/publication/319622440_BlockSci_Design_and_applications_of_a_blockchain_analysis_platform, Accessed: June [17], 2025.

[50] BlockSci: Design and applications of a blockchain analysis platform - arXiv, [Online]. Available: https://arxiv.org/pdf/1709.02489, Accessed: June [17], 2025.

[51] [1709.02489] BlockSci: Design and applications of a blockchain analysis platform - arXiv, [Online]. Available: https://arxiv.org/abs/1709.02489, Accessed: June [17], 2025.

[52] International Symposium on Information Processing in Sensor Networks (IPSN) - DBLP, [Online]. Available: https://dblp.org/db/conf/ipsn/index, Accessed: June [17], 2025.

[53] Accepted Papers –ACM CCS 2019, [Online]. Available: https://sigsac.org/ccs/CCS2019/index.php/program/accepted-papers/, Accessed: June [17], 2025.

[54] OVRseen: Auditing Network Traffic and Privacy Policies in Oculus VR - USENIX, [Online]. Available: https://www.usenix.org/system/files/usenixsecurity22-trimananda.pdf, Accessed: June [17], 2025.

[55] OVRSEEN: Auditing Network Traffic and Privacy Policies in Oculus VR - USENIX, [Online]. Available: https://www.usenix.org/system/files/sec22summer_trimananda.pdf, Accessed: June [17], 2025.

[56] OVRseen: Auditing Network Traffic and Privacy Policies in Oculus VR, [Online]. Available: https://athinagroup.eng.uci.edu/files/2022/09/OVRseen-AuditingNetworkTrafficAndPrivacyPoliciesInOculusVR.pdf, Accessed: June [17], 2025.

[57] NDSS 2020 Accepted Papers - NDSS Symposium, [Online]. Available: https://www.ndss-symposium.org/ndss2020/accepted-papers/, Accessed: June [17], 2025.

[58] OVRSEEN: Auditing Network Traffic and Privacy Policies in Oculus VR, [Online]. Available: https://www.ftc.gov/system/files/ftc_gov/pdf/PrivacyCon-2022-Trimananda-Markopoulou-OVRseen.pdf, Accessed: June [17], 2025.

[59] OVRseen: Auditing Network Traffic and Privacy Policies in Oculus VR, [Online]. Available: https://rtrimana.github.io/talk/ovrseen_ftc_privacycon_2022/, Accessed: June [17], 2025.

[60] Your Router is My Prober: Measuring IPv6 Networks via ICMP Rate Limiting Side Channels | Request PDF - ResearchGate, [Online]. Available: https://www.researchgate.net/publication/364690295_Your_Router_is_My_Prober_Measuring_IPv6_Networks_via_ICMP_Rate_Limiting_Side_Channels, Accessed: June [17], 2025.

[61] s2labres/tesseract-ml-release: Code library for the Tesseract framework from 'TESSERACT: Eliminating experimental bias in malware classification across space and time' - GitHub, [Online]. Available: https://github.com/s2labres/tesseract-ml-release, Accessed: June [17], 2025.

[62] TESSERACT: Eliminating Experimental Bias in Malware Classification across Space and Time (Extended Version), [Online]. Available: https://s2lab.cs.ucl.ac.uk/downloads/tesseract-extend.pdf, Accessed: June [17], 2025.

[63] TESSERACT: Eliminating Experimental Bias in Malware Classification across Space and Time - USENIX, [Online]. Available: https://www.usenix.org/system/files/sec19fall_pendlebury_prepub.pdf, Accessed: June [17], 2025.

[64] Understanding the Ethical Frameworks of Internet Measurement Studies - Network and Distributed System Security (NDSS) Symposium, [Online]. Available: https://www.ndss-symposium.org/wp-content/uploads/2023/02/ethics2023-239547-paper.pdf, Accessed: June [17], 2025.

[65] Call for Papers - ACM CCS 2021 - November, 2021, [Online]. Available: https://www.sigsac.org/ccs/CCS2021/call-for-papers.html, Accessed: June [17], 2025.

[66] ACM IMC 2023, [Online]. Available: https://conferences.sigcomm.org/imc/2023/, Accessed: June [17], 2025.

[67] Workshop on Security and Privacy of Next-Generation Networks (FutureG) 2025 Program, [Online]. Available: https://www.ndss-symposium.org/ndss-program/futureg-2025/, Accessed: June [17], 2025.

[68] SCORED'22: Proceedings of the 2022 ACM Workshop on Software Supply Chain Offensive Research and Ecosystem Defenses - ACM CCS 2022, [Online]. Available: https://www.sigsac.org/ccs/CCS2022/proceedings/scored-proceedings.html, Accessed: June [17], 2025.