Frontiers of Information Technology & Electronic Engineering
www.jzus.zju.edu.cn; engineering.cae.cn; www.springerlink.com
ISSN 2095-9184 (print); ISSN 2095-9230 (online)
E-mail: jzus@zju.edu.cn

社论:

网络空间安全：挑战与机遇

邬江兴[1]，李建华[†‡2]，季新生[1]
[1]国家数字交换系统工程技术研究中心，中国郑州市，450002
[2]上海交通大学网络空间安全学院，中国上海市，200240
[†]E-mail: lijh888@sjtu.edu.cn

本文译自 Wu JX, Li JH, Ji XS, 2018. Security for cyberspace: challenges and opportunities. *Front Inform Technol Electron Eng*, 19(12):1459-1461. https://doi.org/10.1631/FITEE.1840000

目前，网络空间已成为继陆、海、空、天之后的“第五疆域”。网络空间安全也面临日益突出的重大挑战。

首先，基于已知攻击特征封堵的传统防御技术已无法有效抵御新型网络攻击，例如 0-day 攻击和高级持续威胁（APT）等。攻击者常利用隐蔽复杂手段，通过持久渗透发动针对性攻击，表现出强烈隐蔽性、潜伏性和长期纠缠性，使防御方面临“未知漏洞引发未知攻击”的防御困境。进一步，对基于预置后门的攻击，现有主被动防御和密码技术也显得力不从心。

其次，随着网络可编程和网络功能虚拟化的快速发展，在为网络应用提供丰富编程接口的同时，也可能为黑客攻击提供新途径，从而为网络安全带来更复杂的风险。

最后，因为难以完整采集网络流量、网络状态和网络语义，网络脆弱性分析较为困难，更缺乏较为全面的多层次、多角度和多功能的网络安全威胁评估方法和手段。

针对上述挑战，探讨发展新型网络空间安全理论和技术势在必行。首先，应将安全性作为信息系统架构设计的首要考虑因素，以避免或减少因各种软硬件设计漏洞或后门引发的攻击威胁，从而使信息网络具备内生安全免疫能力；其次，应考虑为网络空间提供自适应的安全保护措施；此外，应研究和使用先进的安全技术，如新型密码技术；最后，新型网络、计算和人工智能等也可能为网络空间带来新的安全增量。

在此背景下，中国工程院院刊《信息与电子工程前沿（英文）》组织了本期“网络空间安全”专刊，邀请并开放征集国内外学者投稿，旨在推动网络空间安全先进理论、技术和产业的发展。本期专题特刊共收集 7 篇论文，包括 3 篇综述论文和 4 篇研究论文。

1 专刊内容概述

邬江兴院士提出的拟态防御是一种基于架构设计的内生安全防御技术，具有抵御未知新型威胁的能力和广义鲁棒控制功能，是一种前景广阔的网络空间使能技术。拟态云工作流一文探讨了基于多种物理服务器、虚拟机管理程序和虚拟机操作系统，构建动态异构冗余并行任务执行子空间的方法；设计了对并行任务执行结果的综合判决机制，提供对疑似未知攻击的感知发现能力；基于判决结果或预定策略，研究了基于反馈控制的并行任务执行子空间动态重构方案，通过有效阻断攻击链条，抵御基于未知漏洞/后门的攻击。

李建华教授讨论了人工智能（AI）与网络安全相交叉的研究内容，主要集中在两个方面：一方面，深度学习等人工智能技术，可以用来构建

‡ 通讯作者

网络安全中的智能模型，以实现恶意软件分类、入侵检测和攻击智能感知。另一方面，AI 模型需要特定的网络安全防御和保护技术，以对抗敌对的机器学习，同时保护机器学习中的隐私、保障联合学习的安全等。

柴洪峰院士团队针对移动交易中的银行卡注册安全问题，在分析几种传统机器学习算法基础上，设计了改进的梯度增强决策树（GBDT）算法——XGBoost，并应用于实际系统，基于对绑卡行为的分析进一步扩展了多个特征。其研究结果和框架已被全球支付处理商的移动支付欺诈侦测系统的新设计方案采纳。

CAESAR 是由美国国家标准与技术研究院（NIST）资助的认证加密算法征集竞赛。任奎教授团队介绍了 CAESAR 竞赛候选算法的设计要求和筛选进展；根据设计结构和加密模式对最后一轮候选认证加密方案进行分类；对候选方案的性能和安全作了全面评估，并讨论了未来研究趋势。

Shen Wang 团队对可编程软件定义网络（SDN）的最新研究进展进行了全面综述，重点介绍了架构和安全等方面现有的研究内容以及需解决的问题，总结了 SDN 网络技术在架构和安全上面临的许多挑战。

Kaoru OTA 和 Mian-xiong DONG 教授的团队针对物联网雾计算提出一种拜占庭容错联网方法和两种资源分配策略，其目的是建立一个名为“SIoTFog”的安全雾网络，以抵御拜占庭错误，提高传输和处理物联网大数据的效率。研究涉及单个拜占庭错误和多个拜占庭错误两种情况，对它们在面临不同程度风险时的性能进行了比较。

随着雾计算的发展，出现了将外包隐私集合交集（PSI）计算委托给雾的需求。然而，现有 PSI 方案主要基于全同态加密（FHE）或配对计算。周福才团队提出一种“具有完整性保护的更快的雾辅助隐私集合交集”新方案，在没有解密能力的情况下，雾被委托对加密数据进行交集操作。

2 工作展望

网络空间安全面临许多挑战和机遇，一些新专题也受到越来越广泛的关注。例如，人因安全作为一个跨学科专题，近年发展很快；另外，容侵加密是未来 5G、6G 等网络中的一个重要课题。与此同时，网络空间安全技术的应用也正扩展到更多新领域。

邬江兴教授，中国工程院院士，国家数字交换系统工程技术研究中心主任，教授，博导，信息与通信系统、计算机与网络、网络空间安全领域著名专家。中国首套万门程控交换系统总设计师，拟态计算和拟态防御发明人。

李建华教授，上海交通大学网络空间安全学院院长，教授，博导。信息内容分析技术国家工程实验室主任，中国网络空间安全协会副理事长，教育部网络空间安全专业教学指导委员会副主任委员。主要研究领域为网络空间安全理论与技术。

季新生教授，国家数字交换系统工程技术研究中心总工程师