

首届国际数字经济安全与隐私大会综述

钱江波, 董理*, 张雪垣, 王让定

(宁波大学 信息科学与工程学院, 浙江 宁波 315211)

摘要: 对 2020 年首届国际数字经济安全与隐私大会 (SPDE 2020) 进行了综述. 出席本次线上会议的有来自中国、澳大利亚等国家的著名专家学者. 会议围绕数字经济领域中的安全和隐私问题, 就网络安全、隐私保护、异常入侵检测、信任计算和取证、攻击和对策、隐蔽通信、安全协议、匿名通信安全和社会科学中的隐私安全问题等多个主题开展交流研讨. 本次大会充分展示了数字经济信息安全领域的最新研究成果, 对于引领高水平的信息安全研究、促进学术交流与科研合作、推动信息隐私安全基础研究和实际工程应用的紧密结合起到了积极作用.

关键词: 数字经济; 信息安全; 隐私保护; 计算机网络; 国际会议

中图分类号: TP309.2

文献标志码: A

文章编号: 1001-5132 (2021) 04-0021-07

在网络数字空间中, 信息的安全与隐私问题是一个至关重要的问题, 尤其在如今蓬勃发展的数字经济活动中, 各种新技术的脆弱性和潜在威胁有待发现, 而其对应的解决方案也亟待在实践中验证和测试. 2020 年首届国际数字经济安全与隐私大会 (SPDE 2020) 着眼于数字经济中的安全和隐私问题, 就网络安全、隐私保护、异常入侵检测、可信计算和取证、攻击和对策、隐蔽通信、安全协议、匿名通信安全以及社会科学中存在的安全隐私问题等 9 项专题进行了充分的交流和讨论. 大会组委会邀请数十位国际数字经济安全领域的顶级学者作报告, 包括 4 场主旨报告以及 12 场特邀报告. 相信本次大会能够有效促进学界和业界之间的广泛合作, 进一步开启与社会学等相关学科的跨学科研究.

1 会议概况

本次国际数字经济安全与隐私大会的学术会议于 2020 年 10 月 30 日在浙江衢州市东南数字经济发展研究院召开 (受疫情影响, 本次大会开闭幕式在线对外直播, 相关主旨报告、特邀报告和分组研讨以视频会议方式进行). 会议由电气和电子工程师协会 (IEEE) 主办, 东南数字经济发展研究院和

宁波大学联合承办, 澳大利亚悉尼科技大学和迪肯大学协办. 会议主席由来自希腊塞萨洛尼基亚里士多德大学的 George Karagiannidis 教授和波音公司 Zhang Zhensheng 教授担任. 程序委员会联合主席由悉尼科技大学余水教授、IBM 研究院 (苏黎世) Peter Mueller 教授以及宁波大学信息科学与工程学院钱江波教授担任.

在大会开幕式上, 我国衢州市科学技术协会陈利民主席、宁波大学信息科学与工程学院副院长钱江波教授分别致欢迎词, 澳大利亚悉尼科技大学余水教授对大会组织情况进行了介绍. 本次会议共收到投稿论文 132 篇, 论文分别来自中国、澳大利亚、希腊和印度等国家. 大会技术委员会及其他特邀审稿人, 对所有提交的论文进行了严格的同行评审, 最终有 49 篇论文被接受发表, 接收率为 37%. 接受论文全部进行了线上口头报告交流, 每篇论文报告时间约 15 min, 之后有约 5 min 问答. 大会技术委员会根据论文审稿得分及其报告质量, 分领域遴选出 5 篇论文, 颁发论文奖.

2 研究热点

2.1 网络空间安全

网络空间是集互联网、通信网、物联网及其相

收稿日期: 2020-11-15.

宁波大学学报 (理工版) 网址: <http://journalg.nbu.edu.cn/>

第一作者: 钱江波 (1974-), 男, 浙江宁波人, 教授, 主要研究方向: 分布式计算与系统. E-mail: qianjiangbo@nbu.edu.cn

*通信作者: 董理 (1990-), 男, 浙江宁波人, 讲师, 主要研究方向: 多媒体信号安全处理. E-mail: dongli@nbu.edu.cn

关终端在内的数据链路集合. 伴随物联网设备和大型终端设备的发展和普及, 部分传统的软件定义网络(Software Defined Network, SDN)、数据传输协议和安全密钥访问协议将面临全新、强大的恶意网络攻击, 例如恶意信息流量造成网络数据传输瘫痪、恶意节点盗取用户密钥等. 如何优化现有的安全措施, 提高网络抗攻击能力和鲁棒性是维护网络空间安全的关键问题.

对于 SDN, Xu 等^[1]利用网络数据的时空特征来检测分布式拒绝服务攻击(Distributed Denial of Service, DDoS), 同时利用流表(Flow Table)来抵御 DDoS 攻击. 在 DARPA 数据集上的实验结果证明了该方法的有效性. Zhi 等^[2]针对恶意流条目会破坏 SDN 在数据层面的数据包转发的问题, 设计了一种基于 P4 的方案来检测和定位恶意数据流. 而搭载于无线传感器网络的 SDN (称为 SD-WSNs), 由于其连接不稳定、安全性低、内部敌手众多等缺陷使其安全维护工作更具挑战. 对此, Zhao 等^[3]在综合考虑路由效率和安全性后, 提出了一种对抗环境下 SD-WSNs 的可信链路分离多径选择方法, 相较于传统方案具备更好的性能.

在安全协议、密钥协议方面, Zhu 等^[4]针对人工智能(Artificial Intelligence, AI)用户设计了一种新的可进化密钥协调机制, 该方案可以观察共享信标, 以基于深度自动编码器进行演化; 使用交换观察到的特征作为调和基于共享密钥的表征. Zhang 等^[5]则对 Spring 安全系统的两个方面, 即身份验证和身份授权进行了深入研究; 并基于对该系统安全机制的优化, 提出了一种可信任的 RBAC(Role-based Access Control)模型.

2.2 隐私保护

加速到来的社会数字化转型, 让互联网积聚了越来越多的敏感数据. 同时, 随着人们逐渐重视隐私保护, 针对隐私的监管政策也在近些年相继落地, 例如即将于 2021 年生效的《民法典》. 隐私信息的多样化, 导致了隐私可以从各种角度以各种形式泄露, 如直接从授信第三方(Trusted Third Party, TTP)或者中央机构(Central Authority, CA)泄露、安全性能不足的移动终端泄露以及部分带有少量敏感信息的公开数据库泄露. 因此, 在数据的存储和使用环节中存在大量数据隐私泄露隐患.

针对隐私的存储安全, Fan 等^[6]提出了一种基于区块链的智能网格数据聚合方案, 该方案不依赖 TTP 或 CA, 实现了去中心化. 在该方案中, 领导者选举算法用于选择居住区中的智能电表作为挖掘节点来构建区块, 节点采用 Paillier 加密系统算法来汇总用户的用电量数据, 保证了用户数据的机密性和完整性, 同时方便计费 and 功率调节. 而对于存储于本地的数据, 例如移动终端的定位信息, Wu 等^[7]利用本地差分隐私(Local Differential Privacy, LDP)构造用于隐私数据的攻击和防御. 根据 LDP 和用户的个性化要求提供新颖的隐私定义, 为满足 LDP 的定位信息提供个性化的位置隐私保护机制, 实验证明该方案具有可靠的安保效用和隐私保障.

针对隐私数据的使用安全, 机器学习领域已涌现了许多新兴技术来保护隐私, 其中联邦学习(Federated Learning, FL)以梯度传输替代数据传输, 防止隐私泄漏. 为了进一步验证梯度传输机制的安全性, Wu^[8]提出了一种称为隐私从梯度泄漏(Privacy-leaks from Gradients, PLFG)的新方法, 以仅通过梯度来推断敏感信息. PLFG 方法用每次迭代中从受害者处获得的梯度来构建特殊模型, 然后通过该模型更新初始噪声以推断受害者的隐私数据. 实验结果表明, 即使仅利用梯度, 也可以披露用户的隐私, 且当前流行的防御措施(梯度噪声添加和梯度压缩)无法进行有效防御.

2.3 异常入侵检测

伴随车联网的兴起, 无人驾驶技术、车辆联合通信网络、智能交通系统等技术正在快速发展. 由于交通的即时性, 一旦出现黑客入侵干扰的情况, 将造成不堪设想的严重事故. 因此, 探索该领域的潜在漏洞和优化信息安全保证显得尤为重要.

Han 等^[9]探讨了隐藏入侵检测系统(Intrusion Detection System, IDS)功能, 并在对车联网(Internet of Vehicle, IoV)进行攻击时获得了高精度的方法. 为保护有关异常检测的隐藏层的隐私功能, 提出了基于复值神经网络的入侵检测系统(Complex Valued Neural Network-based Intrusion Detection System, CVNNs-IDS), 该方法用编码器将数据实时转换为图像, 然后将其映射到复杂域, 同时旋转数据以重建真实特征, 实现系统保护的目. 同时,

针对自动驾驶汽车网络,恶意的节点(汽车)可能会伪造信息,并以灾难性后果威胁乘客和其他车辆的安全.对此,Zhai等^[10]提出了一种新的基于信誉的入侵检测方案,可以通过动态信用和信誉评估来检测恶意的自动驾驶车辆.同时,为了进一步鼓励用户参与,还为入侵检测系统中的自动驾驶车辆建立了激励机制.

此外,在深度学习领域,对于异常数据入侵的检测仍是一大挑战,例如数据缺失问题、超参数优化困难问题等.在会议中,有学者提出了基于联合学习和转移学习的网络异常检测方法来解决数据短缺的问题;也有学者提出可以通过对自适应布谷鸟和网格搜索算法进行改进,以改善参数的优化效率.

2.4 信任计算和取证

在当今时代,网络技术和云计算功能正逐渐普及,并开始得到大规模应用.如何确保数据使用过程中的安全,是此类应用场景的核心之一.例如,数据所有者将其数据外包给云并享受便捷服务的同时,如何有效解决数据的降维问题、高通信开销问题;在外包计算中,又如何有效抵御计算器之间合谋的威胁;在基于声誉投票的共识算法中,由马太效应引起的信用价值积累,如何优化系统集中化的风险.

Badar等^[11]使用机器学习技术开发了多所有者加密排名关键字搜索算法,该算法利用主成分分析实现了低开销的系统维护,利用 K 均值聚类方法解决了多所有者模型的不同文档的质量问题,并设计搜索平衡索引树来实现快速查询和高效搜索.Li等^[12]提出了一种基于多用户动态对称可搜索加密(Multi-user Dynamic Symmetric Searchable Encryption, M-DSSE)的盲存储属性值类型数据库的多用户DSSE方案,即授权用户可通过关键字或属性搜索文件,同时确保文件的机密性.Zhu等^[13]提出了一种基于PBFT(Practical Byzantine Fault Tolerance)机制的新的区块链共识方案,将节点分为生产节点、上层节点和公共节点3类,前2类通过节点选择算法生成并定期替换.在节点选择算法中,引入了随机参数以使信誉值不再作为唯一标准.另外,为了解决PBFT中消息复杂度高、可扩展性差问题,还使用ISODATA算法对系统中的

节点进行分割,简化了现有PBFT算法的共识过程,极大地降低了PBFT算法的消息传递复杂度.

2.5 攻击和对策

在现实场景中,利用神经网络处理语音、图像数据是达到特定目的如分类、识别等的常用手段.但同时得益于神经网络的强大学习能力,不法分子可利用特殊神经网络,如对抗生成网络、对抗样本技术等,生成虚假数据,严重威胁了现有信息数据安全^[14].对抗样本的出现对当下神经网络技术的安全性、鲁棒性带来了巨大挑战.研究基于神经网络的攻击手段以及防御手段是近年来信息攻防领域一大研究热点.

在语音领域,语音伪造篡改技术与取证检测技术一直在博弈中互相促进、发展.Wang等^[15]设计了一个基于卷积神经网络(Convolutional Neural Network, CNN)的端到端框架,该框架由编码器和解码器组成,实现了将秘密信息编码到音频载体中,以尽可能小的失真代价完成密信传输,且保证不被检测.同时,Yan等^[16]提出了一种基于递归神经网络(Recurrent Neural Network, RNN)和线性频率倒谱系数(Linear Frequency Cepstral Coefficients, LFCC)的取证算法来检测4种常见的伪造操作.

针对其他主体(图像、网站、应用等)的白盒攻击或黑盒攻击以及相关的抵御技术也在本次会议中引起广泛讨论.例如,Liu等^[17]提出了2种新的提高可传递性方法,称翻转不变攻击方法和亮度不变攻击方法,可以自然地与其他基于梯度的方法结合,并得到更高的攻击成功率和更好的可传递性.Li等^[18]提出了一种基于联合学习的边缘计算系统中的新型检测系统,以检测各种高级持续性威胁(Advanced Persistent Threat, APT),该系统能够以较高的检测精度和较低的误报率检测包括现实生活中APT在内的多数攻击.

2.6 隐蔽通信

隐写技术作为先进的隐蔽通信手段,不同于单纯使用密码来维护信息的完整性和不可读取性,其利用载体冗余隐藏密信,提高信息的隐蔽性,从而实现秘密通信的目的.隐写分析技术则是与之相对抗的分析技术,旨在分析、识别、隔离可疑的含密载体,甚至提取推断出密信内容.

Qian等^[19]提出了一种在隐蔽域中进行数据计

算的思想,即利用信息隐藏可以在图像、音频、随机数据等隐蔽的背景下执行一些数据计算任务。在提出的框架中,发送方可以隐藏其源数据,将其分为两部分,然后将其上传到服务器。服务器在隐秘的内部执行计算,并将隐蔽的计算结果返回给接收器。利用隐蔽结果,接收方可以提取源数据的计算结果。在此过程中,服务器和对手很难获得源数据,因为它们隐藏在载体中,且可以通过公共渠道进行传输。同时,由于计算是在隐蔽域中实现,因此云服务器无法获取计算结果。不同于传统的隐写术方法主要关注嵌密前载体密信的匹配或者嵌入时失真代价最小化,Zhang 等^[20]提出了一种新的音频后处理隐写术模型,该模型在完成一般隐写嵌入后,可一定程度上进一步优化隐写痕迹,提高隐蔽性,且不影响嵌入信息的提取。

2.7 安全协议

网络安全协议是营造网络安全环境的基础,是构建安全网络的关键技术。设计并保证协议的安全性和正确性能够从基础上保证网络安全,避免因安全等级不足而导致数据信息丢失或损坏等问题。例如,传统的网络服务程序:FTP、POP 和 Telnet 在本质上用明文传送口令和数据,非常容易被“中间人”截获这些口令和数据。因此,设计更安全的协议保护算法及数据十分必要。

针对时空数据,Fu 等^[21]提出了一种基于区块链技术的协议,该协议包括位置信息证明(Proof of Location, PoL)创建、共识和块排序,以及一种 PoL 共识算法来验证 PoL,交易并创建区块。方案采用并行无回路有向图(Directed Acyclic Graph, DAG)架构生成区块存储用的区块链拓扑,并进一步对协议进行了威胁分析,以评估该协议的吞吐量、可伸缩性和容错能力。Zhu 等^[22]通过自动分析策略,攻击了一种量子后的密钥交换协议(NewHope-Key-Exchange),并分析其安全性。分析方法主要集中在数论变换(Number Theoretic Transforms, NTT)以及 NewHope 中应用的利用环上错误进行学习的假设上。安全性和效率对 NewHope 的影响通过基于特别设计的攻击模型(使用 Oracle 软件)进行分析。在完全安全不可区分模型和部分泄漏安全不可区分模型的假设下,通过分别配置密钥交换协议,并在不同情况下评估了不同的安全强度和

效率,验证了 NTT 结构对安全协议的影响。

2.8 匿名通信安全

重视隐私的用户在进行部分网络活动中,会尝试增强自身的匿名性使自己的真实身份或隐私信息不被泄露。其中,匿名属性包括不可辨识性(Unidentifiability)和不可联系性(Unlinkability)。不可辨识性是指对手无法识别用户的身份和行为;不可联系性是指对手无法通过观察系统将消息、行为和用户进行关联。

泛在社交网络(Pervasive Social Networking, PSN)中最重要的问题之一是其安全性和隐私性的保障,因此信任关系在 PSN 系统中起着至关重要的作用。Wang 等^[23]提出了一种匿名信任认证(Anony Trust)方案,该方案可以在保护隐私的同时认证用户的身份和信任级别,还可以使用受信任的服务器来实现条件性追溯,并且可以用多个授权的访问点切换在线和离线状态。基于该理念设计的轻量级秘密聊天应用(AnonyChat)在安卓手机系统平台上具有良好的表现,其安全性、匿名性、计算复杂度和通信成本等均有良好性能。

比特币是一种基于区块链的去中心化和匿名化的数字货币支付系统。研究其去匿名化技术,有助于更好地优化改进匿名化系统。Shen 等^[24]提出了一种通过分析传播信息来获取原始交易的方法,通过结合传播模式提取和节点权重分配来计算模式匹配分数。在显示比特币系统实验中表明,该方案可以将原始交易与目标节点进行有效匹配,其精确度最高可达 81.3%。

2.9 社会科学隐私安全

随着用户在移动社交网络内的共享行为激增,大量的包含用户敏感信息的数据被公司获取。出于研究、学术、企业发展等客观现实因素的需求,部分非核心的用户数据会在脱敏后向部分社会开放,用于数据研究和算法开发。其中,初期的用户信息如何合法收集、匿名处理问题,后期的用户数据如何有效脱敏、删除隐私信息问题,已成为社会科学隐私数据安全的关注重点。

基于现有的用户隐私保护机制,Wu 等^[25]构建了一种相互依赖的安全博弈模型,以期为用户做出最佳的隐私保护决策。该方法首先根据用户的相互依赖关系计算影响矩阵,然后构建相互依赖

的安全博弈模型,最后求取该博弈的纳什均衡,得出最佳投资决策.同时,还证明了纳什均衡的存在性和唯一性,且可用迭代方法来计算均衡值.相反,利用先验背景知识来重新识别用户或可实现去匿名化攻击.对此,Zhang等^[26]提出了一种针对匿名社交网络的新型攻击模型,称为边缘邻域图攻击(Edge Neighborhood Graph Attack, ENGA),在该模型中,假定对手具有关于目标及其两跳邻居的背景知识,在合成数据集和真实数据集上进行的实验,证明了ENGA的有效性.

另外,大量用户在移动人群感知中将数据信息上传到平台,可能导致感测平台成为攻击者的目标,而且大大增加了时间延迟和带宽成本.为此,Yang等^[27]提出了一种基于边缘服务器的用户聚类隐私保护方案.其中,边缘服务器利用聚类方法隐藏用户的相关信息,在对用户进行打标签后将其上传到感测平台;然后平台随机匹配用户和用户集.该机制可以有效验证用户上传数据的有效性和安全性,同时还具备保护用户身份的功能.

3 会议亮点

3.1 特邀报告

大会邀请到4位国际专家进行前沿主旨演讲,8位国内外安全领域知名专家作了特邀报告.此外,应广大青年学子的要求,大会还举办了小组会议,就如何在顶级会议/期刊上发表论文进行了交流和解答.美国奥本大学毛世文教授、中国武汉大学王志波教授以及澳大利亚悉尼科技大学余水教授,分享了个人研究经历、顶级期刊发表论文过程以及审稿流程等方面内容.本次会议提供了高质量的“线上+线下”的学术互动交流活动,使在校学生及各类研究人员等可以与著名学者直接对话,以视频会议的方式面对面交流、解惑与探讨.

3.2 论文奖项

根据审稿人评审分数,并经过大会技术委员会对录取论文的严格评估,最终选取如下5项论文奖:“最佳学生论文”“隐私方向最佳论文”“加密方向最佳论文”“数字经济最佳论文”“行业应用最佳论文”,详见表1.

通过设置各类奖项,鼓励青年学者积极参与学术活动,支持学者在各自研究领域进行深入的

探索.

表1 2020年SPDE会议获奖论文

论文奖项	论文题目
隐私方向最佳论文	A personalized preservation mechanism satisfying local differential privacy in location-based services
加密方向最佳论文	Revocable attribute-based encryption scheme with arithmetic span program for cloud-assisted IoT
数字经济最佳论文	A PoL protocol for spatiotemporal blockchain
行业应用最佳论文	Intrusion detection scheme for autonomous driving vehicles
最佳学生论文	Robust, imperceptible and end-to-end audio steganography based on CNN

3.3 推荐专刊

会议技术委员会根据论文评审结果得分,共选取12篇大会接收论文推荐至相关的SCI期刊,期刊包括人工智能物联网应用安全与隐私专刊《Digital Communications and Networks》、物理无线通信的人工智能专刊《Physical Communication》、IEEE Access物联网攻防专刊《进展与挑战》以及移动边缘计算中的安全人工智能专刊《Computer Communications》.按照计算机领域国际学术会议惯例,每篇推荐文章要求至少有约30%新增加内容(技术或者实验部分).通过推荐专刊这一渠道,参会者可进一步提升其学术成果的影响力.

4 结语

随着数字经济互联网产业蓬勃发展,数据安全与隐私问题变得越发突出.在大数据时代,切实保障网络信息安全、隐私数据安全是国家发展信息产业的基石,同时也是国家发展战略层面的重大决策.探索各种环境条件下可靠的安全数据处理方法与技术,对保障数字经济中的安全和隐私至关重要.本次会议的召开为网络安全、隐私保护等课题提供了诸多具有重要参考价值的研究成果,并搭建了学术界与产业界交流的平台.

本次会议得到了我国衢州市东南数字经济发展研究院和宁波大学信息科学与工程学院、澳大利亚悉尼科技大学和迪肯大学以及德国施普林格(Springer)出版社和我国宁波大学学报编辑部的大

力支持.

参考文献:

- [1] Xu Y, Ma J X, Zhong S. Detection and defense against DDoS attack on SDN controller based on spatiotemporal feature[C]//Proceeding of International Conference on Security and Privacy in Digital Economy, 2020.
- [2] Zhi Y F, Yang L, Yang G L, et al. Protecting the data plane of SDN from malicious flow entries based on P4[C]//Proceeding of International Conference on Security and Privacy in Digital Economy, 2020.
- [3] Zhao P, Zhao W T, Liu Q, et al. Trusted link-separation multipath selection for software-defined wireless sensor networks in adversarial environments[C]//Proceeding of International Conference on Security and Privacy in Digital Economy, 2020.
- [4] Zhu S S, Han Y L, Yang X Y, et al. Efficient and evolvable key reconciliation mechanism in multi-party networks based on automatic learning structure[C]//Proceeding of International Conference on Security and Privacy in Digital Economy, 2020.
- [5] Zhang G X, Zhang M Y, Fan X Y. Improvements based on JWT and RBAC for spring security framework[C]//Proceeding of International Conference on Security and Privacy in Digital Economy, 2020.
- [6] Fan H B, Liu Y N, Zeng Z X. Decentralizing privacy-preserving data aggregation scheme using blockchain in smart grid[C]//Proceeding of International Conference on Security and Privacy in Digital Economy, 2020.
- [7] Wu D T, Wu X T, Gao J Q, et al. A personalized preservation mechanism satisfying local differential privacy in location-based services[C]//Proceeding of International Conference on Security and Privacy in Digital Economy, 2020.
- [8] Wu F. PLFG: A privacy attack method based on gradients for federated learning[C]//Proceeding of International Conference on Security and Privacy in Digital Economy, 2020.
- [9] Han M, Cheng P Z, Ma S D. CVNNs-IDS: Complex-valued neural network based in-vehicle intrusion detection system[C]//Proceeding of International Conference on Security and Privacy in Digital Economy, 2020.
- [10] Zhai W D, Su Z. Intrusion detection scheme for autonomous driving vehicles[C]//Proceeding of International Conference on Security and Privacy in Digital Economy, 2020.
- [11] Badar L T, Xu C G, Zakir A. Multi-owner encrypted ranked keyword search using machine learning techniques[C]//Proceeding of International Conference on Security and Privacy in Digital Economy, 2020.
- [12] Li S S, Xu C X, Zhang Y, et al. Multi-user dynamic symmetric searchable encryption for attribute-value type database in cloud storage[C]//Proceeding of International Conference on Security and Privacy in Digital Economy, 2020.
- [13] Zhu S C, Zhang Z Y, Chen L Q, et al. A PBFT consensus scheme with reputation value voting based on dynamic clustering[C]//Proceeding of International Conference on Security and Privacy in Digital Economy, 2020.
- [14] Wang D H, Wang R D, Dong L, et al. Adversarial examples attack and countermeasure for speech recognition system: A survey[C]//Proceeding of International Conference on Security and Privacy in Digital Economy, 2020.
- [15] Wang J, Wang R D, Dong L, et al. Robust, imperceptible and end-to-end audio steganography based on CNN[C]//Proceeding of International Conference on Security and Privacy in Digital Economy, 2020.
- [16] Yan D Q, Wu T T. Detection of various speech forgery operations based on recurrent neural network[C]//Proceeding of International Conference on Security and Privacy in Digital Economy, 2020.
- [17] Liu W P, Li Z P. Enhancing adversarial examples with flip-invariance and brightness-invariance[C]//Proceeding of International Conference on Security and Privacy in Digital Economy, 2020.
- [18] Li Z T, Chen J L, Zhang J L, et al. Detecting advanced persistent threat in edge computing via federated learning[C]//Proceeding of International Conference on Security and Privacy in Digital Economy, 2020.
- [19] Qian Z X, Wang Z C, Zhang X P. Data computing in covert domain[C]//Proceeding of International Conference on Security and Privacy in Digital Economy, 2020.
- [20] Zhang X Y, Wang R D, Dong L, et al. Post-processing for enhancing audio steganographic undetectability[C]//Proceeding of International Conference on Security and Privacy in Digital Economy, 2020.
- [21] Fu Y, Chen H H, Qian J B, et al. A PoL protocol for spatiotemporal blockchain[C]//Proceeding of International Conference on Security and Privacy in Digital Economy, 2020.
- [22] Zhu S S, Han Y L. Analysis toward RLWE-based key

- exchange protocol based on automatic learning structure[C]//Proceeding of International Conference on Security and Privacy in Digital Economy, 2020.
- [23] Wang P, He L M, Yan Z, et al. AnonyTrust: An anonymous trust authentication system for pervasive social networking[C]//Proceeding of International Conference on Security and Privacy in Digital Economy, 2020.
- [24] Shen M, Duan J X, Shang N, et al. Transaction deanonymization in large-scale bitcoin systems via propagation pattern analysis[C]//Proceeding of International Conference on Security and Privacy in Digital Economy, 2020.
- [25] Wu Y, Pan L, Liu F. Making privacy protection investment decisions in social networks: An interdependent security game approach[C]//Proceeding of International Conference on Security and Privacy in Digital Economy, 2020.
- [26] Zhang H Y, Xu L, Lin L M, et al. De-anonymizing social networks with edge-neighborhood graph attacks[C]//Proceeding of International Conference on Security and Privacy in Digital Economy, 2020.
- [27] Yang P, Zhang Y, Wu Q M, et al. User grouping privacy-preserving strategy based on edge computing for mobile crowdsensing[C]//Proceeding of International Conference on Security and Privacy in Digital Economy, 2020.

2020 international conference on security and privacy in digital economy

QIAN Jiangbo, DONG Li*, ZHANG Xueyuan, WANG Rangding

(Faculty of Electrical Engineering and Computer Science, Ningbo University, Ningbo 315211, China)

Abstract: This work reviews 2020 the First International Digital Economy Security and Privacy Conference (SPDE 2020). 15 renowned experts and scholars from China, Australia and other countries attended the conference online. The theme of the conference is focused on the security and privacy issues in digital economy. The conference has organized multiple sessions such as network security, privacy protection, abnormal intrusion detection, trust computing and forensics, attacks and countermeasures, covert communication, security protocols, anonymous communication security, and privacy security issues in social sciences. It provides a platform for the researchers to demonstrate their latest research achievements made in the fields concerning the security and privacy topics in the digital economy. Also addressed are the issues concerning the practical applications in the real world.

Key words: digital economy; information security; privacy protection; computer networks; international conference

(责任编辑 史小丽)