2023年网络空间安全科技热点回眸

冯登国,连一峰

中国科学院软件研究所,北京 100190

摘要 2023年,美国、欧洲、澳大利亚、日本、韩国、印度等国家或地区陆续发布网络空间安全国家政策和战略计划。与此同时,以APT攻击、勒索攻击、供应链攻击、新型网络攻击、移动端攻击为代表的高隐蔽性、高破坏性攻击活动频发,对全球网络空间带来严重安全威胁。零信任、机密计算、隐私计算、弹性安全技术蓬勃发展,量子密钥分发和抗量子密码技术持续取得技术创新和突破,生成式人工智能为网络安全开创了全新的发展空间,网络空间安全领域正面临前所未有的发展机遇和应用前景。

关键词 网络空间安全;数据安全;人工智能安全

2023年,网络安全在国家安全中的战略地位持续提升,网络空间技术对抗成为国家级竞争、博弈甚至军事冲突的有力武器。各类高隐蔽性、高破坏性攻击活动层出不穷,网络协议、系统架构、软硬件研发模式、应用场景成为网络攻击的新型目标。零信任、机密计算、隐私计算、弹性安全、量子计算安全,以及基于生成式人工智能技术的网络安全技术研究和应用取得了快速发展。

1 网络安全的战略地位日益显著

2023年俄乌战争、巴以冲突等地缘热点事件持续爆发,全球安全形势紧张。伴随实体战争的推进,网络空间成为激烈对抗和博弈的关键场所。为积极应对网络安全形势变化,各国纷纷加大网络安全战略部署,立足应对国家级网络攻击威胁,大力提升网络安全攻防能力。

1.1 美国网络安全战略重点

2023年3月2日,美国政府发布了《国家网络安全战略》,这是拜登政府首次发布的国家级、战略性网络安全政策,对美国今后一个时期的网络安全工作提出了顶层设计和总体部署。该战略提出:针对当前复杂的威胁环境和快速演进的新技术,美国政府决定在今后10年重新构想网络空间并将其作为实现其价值观目标的工具。美国政府拟从根本上调整其对网络空间角色、责任和资源的分配方

收稿日期:2023-12-23; 修回日期: 2024-01-03

基金项目:国家重点研发计划项目(2020YFB1806504)

作者简介:冯登国,研究员,中国科学院院士,研究方向为网络空间安全,电子信箱:fengdg@263.net

引用格式:冯登国,连一峰. 2023年网络空间安全科技热点回眸[J]. 科技导报, 2024, 42(1): 232-244; doi:10.3981/j.issn.1000-7857.2024.01.015

式,并做出两大转变:一是重新平衡网络空间安全责任,今后将更多地将责任转移到专业机构;二是重新调整激励措施,强调在解决当前紧迫威胁的同时面向未来进行战略规划和投入。该战略充斥着对华意识形态的偏见,毫不掩饰其反华制华立场,充分说明了国际网络空间博弈斗争的复杂性。

2023年7月13日,美国白宫发布《国家网络安全战略实施计划》(NCSIP),详细阐述了相关职能部门在保障美国网络安全方面的举措和要求,并设定具体时间节点,体现了美国抢占"第五空间"制高点的战略图谋。该计划的实施要点与美国《国家网络安全战略》相配套,聚焦于强化5个方面的工作:一是基础设施防护;二是威胁实体应对;三是市场力量培塑;四是网络标准把控;五是国际网络合作。

1.2　欧洲网络安全战略重点

2023年1月,《关于在欧盟全境实施高度统一网络安全措施的指令》正式生效,主要内容包括:建设协调的网络安全框架;加强欧盟和国际层面的合作;明确网络安全风险管理措施和报告义务;规定对各类网络运营主体的登记和管理要求;建立成员国的信息共享机制;完善对各类网络运行实体的监督和执法措施。为保障该指令得到落地实施,欧盟还制定了严格的时间表和路线图。

2023年2月,欧盟发布的《为实施国家网络安全战略而建立有效的治理框架》提出,各成员国应努力建设一套治理框架,以实现更好的网络安全战略实施效果。为保障战略目标的实现,欧盟将治理框架划分为政治治理、战略治理、运营治理、技术治理四大维度,其中,政治治理维度上提出鼓励网络空间建设使用公私合作关系(PPP)模式;战略治理维度上提出重视预算规划和资源分配以及设置风险识别和缓解机构;运营治理维度上提出完善突发事件应急响应机制,并重视网络安全宣传教育;技术治理维度上强调加强认证与标准化建设。另外,该框架还提出要实行配套的监测评估机制,用以评价成员国网络安全战略实施效果。

2023年4月18日,欧盟委员会通过了关于《网络团结法案》的提案。法案通过时间正值俄乌战争之际,体现了欧盟促进成员国之间合作并为重大网络危机做好准备的意愿,以更好应对因地缘政治局势紧张而产生的网络安全威胁。其目标的实现主要依托以下行动内容:一是部署泛欧安全运营中心基础设施(欧洲网络盾牌),以建立和加强共同检测与态势感知能力;二是建立网络应急机制,形成欧盟网络安全储备,以支持成员国准备、应对重大和大规模网络安全事件;三是建立欧洲网络安全事件审查机制,审查和评估重大或大规模事件。

1.3　亚洲国家网络安全战略重点

2022年12月,日本政府修订了新版《国家安全保障战略》,要求强化网络防御方针,加强网络防护能力建设,构建与美欧同等水平的网络安全能力。根据新版战略,日本将围绕3个方面发力:一是持续调整编制体制,完善充实自卫队网络作战体制与力量;二是加强立法,制定指导性文件,明确支持强化网络安全技术发展;三是建设网络防御新系统,深化对外合作以强化网络防护能力[1]。

2023年2月和6月,韩国分别发布了新版的《国防白皮书》《国家安保战略》,在上述文件指导下,韩国将实施"进攻性网络战"战略,注重加强国家网络安全能力,主动应对新型安全问题。强调在保护自身网络系统安全时,韩国网络战部队将"网络遏制"作为作战重点内容列入整体行动计划。另一方面,韩国网络作战司令部将发展核心作战能力,使其成为国家战略遏制力量组成部分[2]。

2023年1月,印度总理莫迪提出要"建立先进网络安全框架,组建专门网络安全部队"。这一倡议旨在加强印度的网络防御能力,保护信息技术网络。为有效应对针对政府机构和基础设施的新型网络攻击,印度各个地区都将考虑设立这样的部门。2023年10月,印度政府宣布将从印度各邦和中央直辖区警察部队以及中央警察组织中抽调人员,成立一支专门的"网络突击队"[3]。

1.4　其他国家网络安全战略重点

其他国家如澳大利亚,在2023年也加强了网络安全战略部署。据澳内政部官网显示,该国《2023—2030国家网络安全战略计划》于2023年底颁布,并于2030年完成。该战略计划分为两个阶段实施,第一阶段将持续到2025年,旨在"打下坚

实的基础”。为此,将建立6大网络盾牌:一是教育公民和企业提高网络安全意识;二是实施安全技术计划,参与美英等多国组织的软件开发同盟;三是加强政府企业之间的网络威胁信息共享;四是保护关键基础设施的安全;五是通过网络技能增强主权能力;六是采取一致的全球行动,加强与邻国的伙伴关系,相互交流经验,提高网络安全水平。

2 高隐蔽性、高破坏性攻击持续高发

网络安全战略地位的不断提升,是各国应对新形势下国家间竞争、对抗和博弈的必然趋势,同时也预示着国际网络空间安全态势的持续紧张。2023年以来,高隐蔽性、高破坏性的网络攻击持续高发,各类新型网络、关键基础设施、应用系统和软硬件构建模式面临严重的安全威胁。

2.1 APT攻击成为网络空间制导武器

APT(advanced persistent threat,高级持续性威胁)攻击,是攻击组织针对高价值目标实施的具有针对性、持续性的攻击行为。APT攻击通常针对特定目标进行精细策划,利用目标的“零日漏洞”,使用复杂的高对抗性恶意软件进行突破,长期潜伏或监控目标,并不断获取数据信息,因此,APT攻击具有精准打击、高强度打击等特点,是网络战中的制导武器。“零日漏洞”是当前APT攻击的关键武器库资源。2023年上半年,Chrome、Safari浏览器与对应平台Windows、MacOS、iOS下的提权逃逸漏洞占所有漏洞比例近80%[4]。

全球范围内,部分地区的APT攻击随着热点地缘政治事件变得活跃,俄乌战争等传统军事冲突中也频繁看到APT攻击的现实案例,APT攻击成为一种新的作战形态。美国网络安全和基础设施安全局(CISA)持续关注APT攻击,通过发布APT活动报告和漏洞利用警告,不断建设和完善APT防御体系。在最近的报道中,美国政府通过开展漏洞披露共享服务和建设相关平台,帮助联邦机构发现并解决了1000多个可能被黑客利用的漏洞[5]。

中国也面临严重的APT攻击威胁。2023年,海莲花、蔓灵花、毒云藤、响尾蛇、Winnti、APT-Q-27、Lazarus等APT组织对中国频繁发动攻击,涉及政府、能源、科研教育、金融商贸等重点领域[4]。

为了更好地应对APT攻击,中国不断加强网络空间安全体系建设,包括出台相关法律法规、开展技术改造、推动漏洞治理等。特别是针对关键基础设施的安全问题,出台了《关键信息基础设施安全保护条例》并正式实施,制定了该领域首部国家标准《信息安全技术 关键信息基础设施安全保护要求》。网络安全监管部门、重点行业部门、安全机构和厂商也不断尝试运用人工智能、大数据等新兴技术解决APT攻击的检测和防护问题。

2.2 勒索攻击成为数据安全主要威胁

勒索攻击通常利用漏洞入侵受害者的信息设备,以非法手段控制或窃取受害者的敏感数据。在早期的勒索攻击中,攻击者通常强行加密目标数据,要求受害者支付赎金以获取解密密钥。通过定期备份数据可以避免或减少此类勒索攻击造成的损失。近年来,勒索攻击进一步升级演变为双重勒索和三重勒索,双重勒索使受害者面临敏感数据泄露的威胁,三重勒索中攻击者通过联系受害者的客户、合作者等利益相关者逼迫受害者交付赎金。

2023年勒索攻击在全球范围内持续高发,仅上半年就有48个勒索软件组织攻击并公开勒索2200多名受害者,波及众多国家的政府、金融、教育、医疗等行业。例如,勒索软件团伙Clop分别利用GoAnywhere MFT软件的“零日漏洞”(CVE-2023-0669)、MOVEit Transfer的SQL注入漏洞(CVE-2023-34362)攻击并窃取了百余家组织的数据;福特公司遭受黑客组织8base的双重勒索攻击,由于未在规定期限内支付赎金,包括客户个人档案、雇佣合同、交易发票等在内的近10 GB业务敏感信息被公布;英国曼彻斯特大学遭受三重勒索攻击,攻击者复制了校方的众多敏感数据,包含学校教职工和学生的隐私信息以及校方为研究目的收集的英国国民医疗服务体系(NHS)中超过百万患者的隐私信息,逼迫校方支付赎金。

勒索攻击的危害不只限于直接泄露敏感数据,更有可能造成被攻击组织的业务停摆。例如,2023年10月,波音公司因遭受勒索组织LockBit的攻击

(图1),大量敏感数据被窃取,导致公司的零部件和分销业务受到影响。

图1　波音公司遭受LockBit勒索攻击

2.3　新型网络成为渗透攻击重要目标

新型网络设施设备,例如,工业互联网与工业控制系统(ICS)、车联网与智能网联汽车、卫星网络与卫星定位系统等,逐渐成为网络渗透攻击的重要目标,同时,由于各类新型网络之间的相互融合,渗透攻击也呈现出跨网跨域的新趋势。

以监督控制和数据采集系统(SCADA)为代表的工业控制系统一直是网络攻击的重灾区。根据Cybernews的调查统计,自2023年10月7日以色列与哈马斯武装组织爆发冲突以来,已有58个黑客组织参与到本次网络大战中,其网络攻击的重点就是对方的SCADA和其他工业控制系统。同时,工控系统相关的网络协议如Modbus、MQTT等也成为攻击者的突破对象,研究人员已发现400起针对Modbus协议的攻击事件。

近年来,卫星互联网的发展如火如荼,由于缺乏安全标准以及防护能力,许多网络安全问题应运而生。攻击者可以对卫星信号施加干扰或进行信号欺骗,从而对供电、供水和交通运输等关键的社会基础设施造成严重影响。2023年以来,基于卫星定位的飞机导航系统已经成为网络攻击者的新目标,一种名为"GPS欺骗"的网络攻击手段近几个月来激增。攻击者向飞行管理系统发送虚假GPS信号,由于飞机无法分辨真伪,导致导航系统出现偏差,飞机偏离航线,如果飞机未经许可进入他国领空或禁飞空域,将构成较大安全风险。国际航空资讯机构飞行运营集团发布的报告显示,截至2023年11月上旬,该机构收到近50份涉及GPS欺骗的报告,其中多数发生在中东地区。

车联网云、管、端架构中的各个重要环节都面临着网络攻击威胁,近年来车联网服务平台及智能网联汽车安全事件频发。2023年2月,来自以色列SaiFlow的调查结果证实了电动汽车充电基础设施面临的潜在风险,多个电动汽车充电系统中发现的新型漏洞可被利用并远程关闭充电站,甚至遭受数据和能源窃取。7月,CISA联合BitSight公司发布公告称,MICODUS公司提供的全球定位系统(GPS)存在多个安全漏洞并可波及全球超百万辆汽车(图2)。8月,研究人员发现影响本田汽车的重放攻击漏洞,附近攻击者可通过拦截车钥匙发送到汽车的射频信号,解锁Acura等车型的本田汽车。

图2　MICODUS GPS软件漏洞波及范围

UpstreamSecurity发布的《2023年全球汽车行业网络安全报告》显示,在过去5年中,全球汽车行业由于网络攻击造成的经济损失超过5000亿美元。

2.4　供应链安全成为网络安全防护关键短板

信息系统的复杂功能需求和快速开发需求促使软硬件开发过程呈现出模块化协同开发、组件代码复用等特征。软硬件模块间的关联关系,以及全生命周期中涉及的开发者、供应商、用户等角色,共同构成了复杂的供应链网络。在软件供应链场景中,系统的开发、分发等各个环节均有可能引发安全问题,供应链安全问题不再局限于系统或模块自身,而是可能直接影响整个生态。

软件开发工具包(SDK)是一些被软件工程师用于为特定的软件包、软件框架、硬件平台、操作系统等创建应用软件的开发工具集合,是软件供应链中的关键环节。利用SDK的漏洞甚至故意在SDK设置恶意代码或逻辑后门,从而攻击使用了该SDK的所有应用软件,已经成为典型的供应链攻击手段。2023年10月30日,国家安全部微信公众号专门发布文章"警惕!一些境外SDK背后的'数据间

谍'窃密",指出境外一些别有用心的组织和人员,正在通过SDK搜集我用户数据和个人信息(图3)[6]。

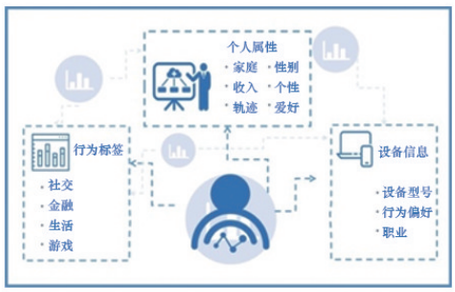

图3 SDK搜集用户数据和个人信息

欧美国家很早就开始关注软件供应链安全,并制定了大量软件供应链相关的政策。美国2000年就发布了《国家信息安全保障采购政策》,规定了信息技术和相关产品的审查机制;2008年在《国家网络安全综合计划》中强调了建立全方位措施以进行全球供应链风险管理,将供应链安全问题上升到了国家威胁和国家对抗层面;2021年发布的《关于改善国家网络安全的行政命令》进一步明确了加强软件供应链安全的要求[7]。ISO等国际标准化组织发布了ISO 28000系列标准、ISO/IEC 27036《供应商关系的信息安全》、ISO/IEC 27034《应用安全》、ISO/IEC 15288《系统生命周期过程》、ISO/IEC 20243《开放可信技术供应商标准——减少被恶意污染和伪冒的产品》等软件供应链安全相关标准。

中国也高度重视供应链安全问题,工业和信息化部发布的《"十四五"软件和信息技术服务业发展规划》提出,建设国家和行业级别的开源社区安全审查体系,保证各个行业广泛使用重要开源产品和技术服务的安全性[8]。华为等企业也积极投入开源社区建设,如OpenEuler开源社区已经汇聚了数千款上游组件,助力软件供应链安全。

由于供应链安全问题自身的复杂性和历史原因,中国当前供应链安全形势仍很严峻,包括开源生态建设较为落后,标准制定和技术实践不足,尚未形成完整的供应链安全保障技术体系等。

2.5 云系统安全和移动端安全成为关注重点

2023年,以ChatGPT为代表的大模型进一步推动了云服务的普及应用。与此同时,智能手机、平板电脑、可穿戴设备等移动端设备也得到了普及,成为整个互联网中数据采集、存储、计算的重要节点。云系统安全和移动端安全成为网络空间安全的重要环节,得到了越来越多的关注。

云系统涉及多种安全风险,包括数据泄露、数据丢失、云服务滥用、拒绝服务攻击、账号劫持/服务流量劫持等。移动端安全主要涉及移动设备的安全性,包括数据安全、应用程序安全、网络安全等多方面。2023年7月,Android签名漏洞爆发,木马程序可以利用该漏洞寄生在正常APK中,受影响的APK包括天翼宽带等大量知名应用。与传统终端或服务器相比,移动端具有更多接触个人敏感信息或个人资产的机会,其中可穿戴设备最具代表性。互联网数据中心(IDC)发布的《中国可穿戴设备市场季度跟踪报告》显示,2023年第二季度中国可穿戴设备市场出货量为3350万台,同比增长17.3%。这些设备能够采集、存储诸如用户心跳、血压、地理位置等敏感信息,进一步提高了移动端的攻击价值,加剧了其面临的安全威胁。

3 零信任、机密计算、隐私计算与弹性安全技术蓬勃发展

为了更好应对日益严峻的网络安全形势,提高关键信息基础设施、重要信息系统和整体网络空间的安全保障能力。2023年以来,以零信任、机密计算、隐私计算、弹性安全为代表的网络安全技术也在蓬勃发展并不断取得突破。

3.1 零信任技术

零信任坚持"永不信任,持续验证"的理念,打破了传统网络安全防护模式的限制,对网络边界安全进行全新审视。零信任已从一个新兴安全理念逐步发展成为全球网络安全的关键方法和技术。

2023年1月,美国陆军成立了零信任架构能力管理办公室,加速推进零信任架构实施,其目标是确保信息系统的安全性,防止任何形式未经授权的访问和数据泄露,到2027年形成由零信任架构提供全面安全保护的统一网络。2月,美国国防信息系统局(DISA)宣布完成零信任项目"雷霆穹顶

(Thunderdome)”企业级网络安全样机(图4)[9]。该样机标志着美国军方零信任建设工作由理论研究转向实践。4月,CISA发布第2版《零信任成熟度模型》[10],旨在降低美国机构实施零信任的壁垒。7月,Fortinet发布《2023年全球零信任发展报告》,揭示了零信任安全当前的部署实施现状以及最新进展,指出零信任相关部署占比正稳步提升[11]。8月,中国信息通信研究院发布了《零信任发展研究报告(2023)》,阐述了过去2年多零信任产业的发展和变化,指出目前中国正在从政策、行业实践、产业发展等多方面对零信任进行积极探索,前期以推动零信任理论研究和技术创新为主,后期加强零信任技术应用和工程落地[12]。

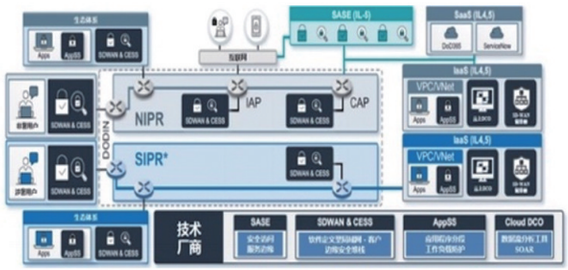

图4　“雷霆穹顶”企业级网络安全样机

3.2　隐私计算与机密计算技术

数据隐私性问题持续引起全球关注。IBM在一项研究报告中指出,2023年全球数据泄漏的平均成本达到445万美元,比3年前增加了15%[13]。以安全多方计算、联邦学习等技术为基础的隐私计算技术,作为数据隐私保护的重要技术受到了各行业的重视。2023年1月,Omniscient的CEO Jon Jacobson在世界经济论坛中分享了隐私计算的价值与重要性[14],进一步加深了人们对隐私计算的理解与认识,推动了隐私计算的标准化进程。2023年1月,美国国家标准技术研究所(NIST)开展新一轮多方面方案征集活动,截至2023年4月共收到12份相关建议。2月,NIST提出了一种基于可信执行环境(TEE)的隐私计算方案,该方案旨在高效创建、管理并保护系统运行时需要的敏感数据[15]。

2022年,国家工业和信息化部等16部门发布的《关于促进数据安全产业发展的指导意见》[16]指出,加强隐私计算技术攻关和产品研发,推进安全多方计算、联邦学习、全同态加密等技术应用。6月,中国信息通信研究院发布的《隐私计算应用研究报告(2023年)》[17]分析并总结了国内隐私计算所面临的机遇与挑战,展望了隐私计算应用的未来发展趋势。

除国家政策及产业界的大力推动外,2023年各类学术会议上,研究人员也针对隐私计算提出了多种高效的新方案。其中,具有鲁棒性和可安全聚合的联邦学习方案、安全模型更为精确的安全多方计算、更高效简洁而无需初始化的全同态加密方案等隐私保护技术的提出,进一步推动了隐私计算技术的全面发展。

机密计算是涉及硬件安全、系统安全、数据安全等在内的一种新型安全计算模式,通过在基于硬件的可信执行环境(TEE)中执行计算来保护使用中的数据,其最终安全目标是在未来的网络数字空间内,所有的高安全应用程序都是基于硬件TEE的机密计算程序。

2023年7月,VMware、AMD、三星及RISC-V共同推进机密计算标准的建立,加大机密计算认证框架的构建,以实现实用的机密计算技术[18]。围绕GPU、ARM、RISC-V等硬件环境的机密计算技术2023年取得了快速发展:提出了以机密GPU为代表的异构TEE,可在不依赖CPU TEE的前提下确保异构计算安全,为人工智能、大模型提供安全可信的异构算力,如NVIDIA H100/H800系列GPU[19]在Hopper架构中引入了基于GPU的机密计算安全功能。在基于ARM CCA扩展架构方面,利用CCA的Monitor固件创建用户进程级安全飞地,从而实现基于ARM CCA的TEE安全架构扩展,在ARM设备上提供类似x86的通用TEE环境[20]。在基于RISC-V开放性软硬件TEE架构方面,利用硬件的可编程性从底层解决TEE的侧信道安全问题,提出了能够抵御瞬态执行攻击和微架构侧信道攻击的内存共享机制,并通过改进的动态缓存分区方案以提高性能[21]。在机密容器技术和证明服务框架方面,提出了基于TEE和TPM的多信任根证明服务框架方案[22],针对机密容器的静态及动态完整性证明和监控方法与代表性方案keylime相比,其完整性监控性能提升了71.4%。微软Azure平台的Par-

ma[23]方案利用SEV-SNP提供的VM级隔离,设计并实现了新的机密容器架构,可以直接运行未经修改的容器,实现容器环境的远程证明与安全策略实施。另外,新一代机密计算通信框架(Confidential 6G)可为6G等新型通信技术提供机密计算能力,如欧盟于2023年立项的Confidential 6G项目[24]。

3.3 弹性安全技术

由于在各类不可信环境中进行数据处理、多方共享与数据分析的需求日渐提升,弹性安全技术已成为网络安全领域的新潮流,其目标是提升系统或网络的带菌生存和入侵容忍能力。

2023年3月美国发布的《国家网络安全战略》提出以"通向富有弹性的网络空间之路"为目标,建立一个"可防御、富有弹性"的数字生态体系。

网络安全是数字中国建设的重要基础,《数字中国建设整体布局规划》[25]明确提出要"筑牢可信可控的数字安全屏障"。面对技术发展带来的新安全威胁、新攻击手段、新应用需求,必须积极推动构建富有弹性的网络空间安全保障体系[26],提出实现弹性安全的新理念、新思想、新方法,综合运用并创新发展弹性公钥基础设施(PKI)、定制可信空间、移动目标防御、棘轮安全机制、拟态防御、可信计算、机密计算等技术。

就拟态防御技术进展而言,2023年主要分为2方面:一是将拟态防御技术与网络弹性、6G通信、系统安全等方向进行结合,强化内生安全能力,典型代表包括使用内生安全构造在网络弹性整个生命周期的赋能方法[27]、针对6G安全问题提出的内生安全在6G空口和天地一体化场景中的应用解决方案[28]、针对控制流劫持攻击提出的进程异构冗余执行系统[29]等。二是对拟态防御技术进行形式化分析,典型代表包括使用Verifast定理证明器分别对拟态路由器的TCP协议代理[30]和边界网关协议BGP代理[31]的形式化验证。

4 量子计算技术蓄势待发

4.1 量子计算对密码学和信息安全的挑战

量子计算是结合量子力学和计算机科学的一种新型计算方式。量子计算机突破了传统计算机的计算限制,可高效解决一些在经典计算模式下"指数"级困难的问题。

2023年谷歌在量子计算纠错、含噪处理等方面取得了多项突破[32-34],在其最新的70个量子比特的Sycamore量子处理器上,通过随机电路采样的模拟计算成本估计,评估出Sycamore量子处理器能够在几秒内完成目前世界排名第一的Frontier超级计算机需要47.2年才能完成的计算任务(图5)。6月,PsiQuantum借助新型容错量子计算架构,提出了破解椭圆曲线密码(ECC)的新方案,所需的计算资源较之前减少了700倍[35]。

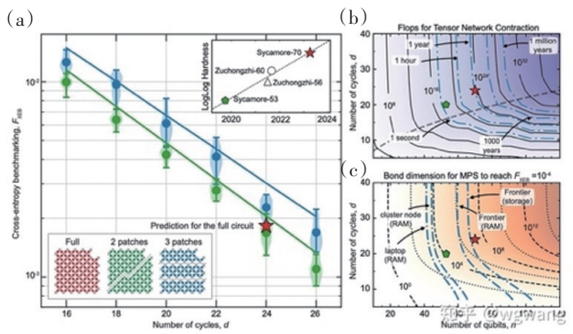

图5 Sycamore量子处理器计算能力评估

2023年10月,由中国科学技术大学、中国科学院上海微系统与信息技术研究所和国家并行计算机工程技术研究中心合作,完成了255个光子的"九章三号"量子计算原型机[36]。在处理高斯玻色取样中,"九章三号"从相同分布中生成单个理想样本仅需1.27 μs,而Frontier超级计算机需要大约600年(图6)。

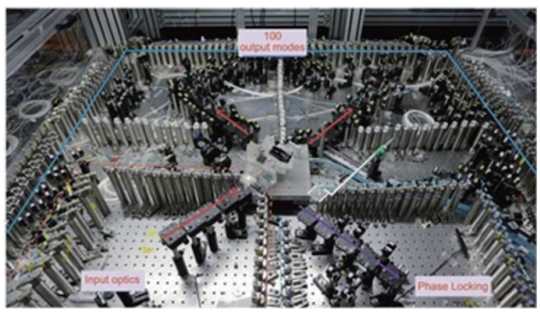

图6 "九章三号"光量子计算原型机实验装置

这些进展推动着向量子计算时代的逼近,强大且稳健的算力突破带来的最终结果是威胁基于传统困难性问题的密码学部件以及信息安全体系。因为安全性是依赖于经典计算机无法计算的困难问题,而随着量子计算的高速发展,在多项式时间内解决这些困难问题有望成为可能。甚至有研究人员认为,可以通过13436量子比特位的量子计算机在177 d内完成RSA 2048的破解[37],256比特的椭圆曲线算法可以在9 h内使用126133猫态量子比特位的量子计算机完成破解[38],创造出更高量子比特的量子计算机与更低量子比特需求的量子攻击算法来彻底攻破它们只剩下时间问题了。当然,这个时间可能很长。

为了应对量子计算对传统密码学与信息安全技术体系带来的威胁,应尽早部署后量子密码(也称为抗量子密码)技术。一方面,以量子密钥分发为代表的量子密码技术相关工作取得阶段性进展,2023年1月,中国科学技术大学与清华大学提出模式匹配量子密钥分发(MP-QKD)协议,研究结果表明该协议在不需激光器锁频锁相的条件下,可以实现远距离安全成码且在城域距离有较高的成码率,有效降低了协议实现难度,对未来量子通信网络构建具有重要意义[39]。5月,中国科学技术大学发现了量子密钥分发发送端调制器件的一种安全漏洞,并利用该漏洞完成了量子黑客攻击[40]。另一方面,后量子密码技术仍然可以使用经典方式处理信息,但其安全性基于与RSA和椭圆曲线密码不同的数学困难问题。

2023年3月,美国发布的《国家网络安全战略》提出联邦政府优先考虑并逐步将公共网络和系统向抗量子密码环境过渡;加拿大国防部和武装部(DND/CAF)发布量子科学和技术战略实施计划《Quantum 2030》,提出为应对量子计算威胁,正在制定新型后量子密码(PQC)标准[41]。在量子计算快速发展的背景下,后量子密码技术的研发与迁移需提前布局,要求包括密码算法、协议、组件和基础设施等均更新为量子安全的密码技术,在此过程中需积极应对密码算法设计、实现以及兼容性等方面的挑战。

4.2　量子计算在网络安全领域的应用前景

量子计算具有更高的计算速度和更强的安全性,为网络安全领域的发展提供了新的机遇和可能性。2023年8月,NIST发布了抗量子加密标准草案,其中公钥封装机制是CRYSTALS-KYBER,3种数字签名方案为CRYSTALS-Dilithium、FALCON和SPHINCS+,预计于2024年投入使用[42](图7)。

图7　NIST发布抗量子加密标准草案

2023年3月,量子安全供应商QuSecure表示完成了首个实时端到端量子弹性加密通信卫星链路,这标志着美国卫星数据传输首次使用抗量子加密,这一进展是美国在后量子密码技术应用方面的里程碑[43]。6月,IBM宣布首次证明量子计算机可在100多个量子位规模下得到准确结果,超越了经典方法,这一结果标志着我们正在步入量子计算实用的新时代[44]。8月,谷歌部署混合椭圆曲线X25519和后量子Kyber算法的TLS协议,其安全性与目前使用的传统TLS加密一样,但在延迟和吞吐量等性能方面存在一定差异。11月,研究人员提出量子密钥分发通过其独特的反窃听机制,可成为增强网络通信安全的核心解决方案[45]。

量子计算的快速发展揭示了解决各种现实挑战的巨大潜力,在网络安全领域推动了后量子密码学的蓬勃发展,进一步加强了网络与信息安全体系的安全性。

5　生成式人工智能技术拓展应用

近年来,生成式人工智能技术获得了快速发展。2023年4月,谷歌公司将生成式人工智能引入网络安全领域,发布名为云安全人工智能工作台(Cloud Security AI Workbench)的网络安全套件,

结合了对软件漏洞、恶意软件、威胁指标和威胁行为者概况的综合感知能力,用于高效查找、总结和应对安全威胁。

5.1 生成式人工智能带来的挑战和机遇

随着训练数据以及参数量的增加,生成式模型的性能不断提升,涵盖了文本(如OpenAI的GPT-4)、图像(如Stability AI的SD-XL)、语音(如OpenAI的Whisper)和视频(如Runway的Gen-2)等多个领域。这些进展不仅拓宽了生成式人工智能的应用范围,也为各个行业带来了更多的创新机遇。大模型正在朝着多模态的方向发展,OpenAI的GPT-4V能够处理图像和文本的组合输入,谷歌的Gemini可以理解文本、代码、图像、语音和视频等多种类型的数据。

国内的生成式人工智能领域也在高速发展。2023年8月,第一批大模型如百度的文心一言以及科大讯飞的星火等已获国家批准正式为公众提供服务;11月,昆仑万维的天工以及面壁智能的露卡等大模型也已通过备案即将上线。

生成式人工智能在快速发展的同时,也带来了诸多挑战。首先,幻觉问题普遍存在于开源和闭源大模型之中。由于训练数据中包含的虚假信息以及预训练和对齐阶段可能引入的错误知识,大模型会生成不符合源内容或者不符合常识的输出[46]。其次,大模型也可以被用来生成不安全的内容,例如,越狱攻击会绕过模型供应商对于输入指令施加的安全限制,从而引导大模型生成有害的内容。南洋理工大学研究人员通过收集大量越狱数据并对大语言模型进行微调,实现了自动化的越狱指令生成[47]。德国亥姆霍兹信息中心(CISPA)研究人员揭示了文本生成图像模型同样可以用来生成不安全的图片,并使用图片编辑方法制造出了有害的表情包[48]。最后,生成式人工智能还存在隐私泄露的风险。谷歌研究人员发现记忆现象广泛存在于大语言模型[49]和扩散模型[50]中,特别是训练集中重复次数较高的数据,可以通过查询恢复出来。

面对模型自身存在的幻觉问题以及不法分子对其潜在的恶意使用风险,对生成内容和真实内容的有效鉴别有着重要意义。斯坦福大学研究人员发现,大模型生成的文本通常集中在模型对数概率函数的负曲率区域,并基于此实现了零样本场景下的生成文本检测[51];CISPA研究人员训练了机器学习分类器,用于区分真实图片和文本生成图像模型生成的虚假图片[52]。针对大模型的隐私泄露风险,由于重新训练或微调大模型具有较高的成本,如何高效准确地使模型遗忘记忆的知识也成为一个重要问题[53-54]。

5.2 基于人工智能的网络空间技术对抗

网络空间技术的迅猛发展与其带来的安全挑战相伴而生。利用人工智能技术辅助开展网络空间的攻防对抗,已经成为网络安全领域的研究热点。以生成代码为例,基于生成式人工智能的代码生成工具方兴未艾。例如,GitHub的Copilot工具提供订阅制的付费方式供用户使用。但是,人工智能自动生成的代码可能并不安全,一些生成的代码片段出现了严重的漏洞。因此,生成式人工智能的内容安全问题广受重视。

纽约大学研究人员对Copilot的安全问题进行了系统评测,在89个编程场景下使Copilot产生了1689段程序,结果显示有40%的代码是包含漏洞的[55]。这一结果引起了人们对基于生成式人工智能的代码安全性的关注。研究人员对真实场景下人工智能模型生成的代码也进行了研究,与之前工作的区别在于并非完全由人工智能模型生成代码,而是将其作为编程人员的辅助生成工具。结果显示,使用生成式人工智能模型辅助产出的代码与没有使用模型的编程人员相比,并没有显著增加安全风险[56]。生成式人工智能同样可以应用于漏洞自动化发现与修复工作。伊利诺伊大学香槟分校的研究人员使用微调后的生成式模型来生成种子,对深度学习库进行模糊测试[57]。

实验结果表明,与TensorFlow和PyTorch上最先进的模糊测试器相比,在代码覆盖率上可以分别实现30.38%和50.84%的提升。此外,研究人员还检测到65个程序缺陷,其中44个为之前未知的缺陷。纽约大学的研究人员对生成式人工智能能否修复编程人员所造成的程序缺陷进行了研究[58],结果显示,针对作者构造的有限场景,当给出一个精

心构建的提示时,生成式人工智能模型可以生成正确的修复程序。这项成果虽然距离实用化还有较大差距,但仍然为我们揭示了生成式人工智能在这一领域的发展前景。

5.3 人工智能的安全监管

由于人工智能技术在数据处理、计算推理、输出结果等方面与传统领域存在的巨大差别,其自身的安全性问题也不断引起人们的关注和担忧。特别是随着大模型在世界范围内的广泛应用,各国政府都开始建立针对这一领域的系统性监管机制。

从2022年3月1日颁布首部全国范围的人工智能专门法规《互联网信息服务算法推荐管理规定》[59]起,中国就在持续完善对于人工智能技术的监管体系。中央网信办、工信部、公安部于2022年11月25日联合发布了《互联网信息服务深度合成管理规定》[60]。该规定明确了深度合成服务提供商和技术供应商的全方位责任,涵盖数据安全、个人信息保护、透明度等方面。生成式人工智能服务提供商需要根据该规定在生成内容(图片、视频等)上添加标记,并需要按照规定向网信办提交相关算法。2023年6月23日,网信办公布了第一批备案的深度合成算法,即《人工智能算法备案清单》,进一步明确了服务商的算法备案义务。

2023年7月13日,国家互联网办公室、发改委、教育部、科技部、工信部、公安部、广电总局联合发布了《生成式人工智能服务管理暂行办法》[61]。该办法于2023年8月15日生效,旨在进一步规范生成式人工智能技术,规定生成式人工智能服务提供者须承担多项重要义务,包括监控其服务生成的各类内容。该办法还强调了中国现有的网络安全和个人隐私规则,规定了对用户个人信息的保护,禁止非法收集和共享数据等。

中国针对人工智能的监管工作正在有条不紊地推进,世界各国也将注意力和资源投入到人工智能安全合规的立法流程中。美国总统拜登在2023年10月30日签署了一项关于人工智能的行政命令,内容涵盖了国家安全、消费者隐私保护等多个议题。该政令的主要要求包括人工智能系统研发人员需与政府分享其安全测试结果;完善相关标准,设计测试工具,确保其人工智能系统的安全性、可靠性;同时还包含在未来制定一系列新标准,建立网络安全计划,规划《国家安全备忘录》等内容,从而指导人工智能安全监管的逐步完善。

欧盟也在稳步推进人工智能相关的法律制定工作。2023年12月,欧盟各方就人工智能监管的全面规则基本达成一致,有望推动《人工智能法案》正式生效。该法案对人工智能的应用按照风险等级进行了分类,根据分类对具有不同风险性的人工智能应用实施不同严格程度的监控和披露要求,并直接禁止了人工智能的部分应用。

总的来说,全球人工智能治理的战略趋于多样化。不同的国家和地区虽然选择了不同的方向和策略,但都在持续大力推动人工智能安全监管机制的落实和完善。

6 结论

网络空间安全是典型的交叉型学科,既需要在基础理论、体系架构、算法、模型等方面大力推进基础研究工作,又需要充分面向各行业领域需求,构建实战化的安全防护能力,研究范围与通信、电子、计算机、自动控制等领域密切融合,在某些方面与管理学、经济学、社会学等学科领域也形成了交叉。

随着各国政府对网络安全战略地位的日益重视,网络空间安全科技的发展也日新月异。一方面,各类新型、高隐蔽性、高破坏性、跨域跨空间的攻击模式和攻击渠道持续刷新人们的认知。另一方面,零信任、机密计算、隐私计算、弹性安全、量子计算、生成式人工智能等新兴技术也不断为我们提升和扩充安全防护能力。网络空间安全已经进入百花齐放、百家争鸣的蓬勃发展阶段,挑战与机遇并存,亟需我们从国家监管、理论突破、技术攻关、体系建设、行业应用等各个层面协调行动,共同发力,围绕供应链安全、弹性安全、网络生态安全、智能安全、人机协同安全等核心维度,加强中国整体网络空间安全的防护能力和保障能力,形成为国家安全、经济发展和社会进步保驾护航的有力屏障。

致谢:左晓栋教授、徐静研究员、苏璞睿研究员、张敏研究员、陈恺研究员、秦宇研究员等提供的相关素材,以及中国科学院学部战略咨询项目《网络空间安全学科发展战略研究》的支持。

参考文献(References)

[1] 2023年以来日自卫队加速网络作战力量建设主要动向[EB/OL]. (2023-07-11) [2023-12-09]. https://www.sohu.com/a/696748160_100040985.

[2] 由"被动防护"向"应对作战"转变 韩国网络战战略出现拐点[N/OL]. (2023-11-29)[2023-12-09]. http://www.81.cn/szb_223187/gfbszbxq/index.html? paperDate=2023-11-29&paperNumber=04&articleid=920370.

[3] 印度政府组建"网络突击队",加强网络安全工作[EB/OL]. [2023-12-09]. https://www.secrss.com/articles/59942.

[4] 全球高级持续性威胁(APT)2023年中报告[EB/OL]. [2023-12-12]. https://www.qianxin.com/threat/reportdetail?report_id=295.

[5] Vulnerability disclosure policy platform annual report 2022[EB/OL]. [2023-12-12]. https://www.commerce.gov/vulnerability-disclosure-policy.

[6] 警惕一些境外SDK背后的"数据间谍"窃密[EB/OL]. (2023-10-27) [2023-12-12]. https://mp.weixin.qq.com/s/xq_0nAxzuZ4t0HLXLy8BEg.

[7] CCF. 2021-2022中国计算机科学技术发展报告[M]. 北京: 机械工业出版社, 2023.

[8] 工业和信息化部关于印发"十四五"软件和信息技术服务业发展规划的通知[EB/OL]. [2023-12-12]. https://www.miit.gov.cn/cms_files/filemanager/1226211233/attach/20224/b1a5229d377c410abf08b46b096249b7.pdf.

[9] 浅析美军"雷霆穹顶"零信任项目[EB/OL]. [2023-12-11]. https://www.sohu.com/a/652865383_120319119.

[10] Zero trust maturity model[EB/OL]. [2023-12-04]. https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf.

[11] 2023零信任现状报告[EB/OL]. [2023-12-11]. https://www.fortinet.com/cn/demand/gated/report-state-of-zero-trust.

[12] 零信任发展研究报告(2023年)[EB/OL]. [2023-12-11]. http://www.caict.ac.cn/kxyj/qwfb/ztbg/202308/P020230828402611317149.pdf.

[13] Cost of a data breach 2023[EB/OL]. [2023-11-28]. https://www.ibm.com/reports/data-breach.

[14] Jacobson J. How Privacy enhancing technologies impact business, individuals and society[EB/OL]. (2023-10-25) [2023-11-28]. https://www.weforum.org/agenda/2023/10/the-impact-of-privacy-enhancing-technologies-pet-on-business-individuals-and-society.

[15] Bartock M, Souppaya M, Wheeler J, et al. NIST Interagency Report NIST IR 8320D ipd hardware enabled security: Hardware-based confidential computing initial public draft[EB/OL]. [2023-12-11]. https://nvlpubs.nist.gov/nistpubs/ir/2023/NIST.IR.8320D.ipd.pdf.

[16] 工业和信息化部等十六部门关于促进数据安全产业发展的指导意见(工信部联网安〔2022〕182号)[EB/OL]. [2023-12-11]. https://www.gov.cn/zhengce/zhengceku/2023-01/15/content_5737026.htm.

[17] 隐私计算应用研究报告(2023年)[EB/OL]. [2023-11-28]. http://www.360doc.com/content/23/0818/21/224530_1093009750.shtml.

[18] VMware与其他行业领导者共同推广机密计算[EB/OL]. [2023-06-30]. https://www.c114.com.cn/news/211/a123-6172.html.

[19] Nvidia confidential computing[EB/OL]. [2023-12-11]. https://www.nvidia.com/en-us/data-center/solutions/confidential-computing.

[20] Zhang Y M, Hu Y X, Ning Z Y, et al. Shelter: Extending arm CCA with isolation in user space[C]//32nd USENIX Security Symposium (USENIX Security 23). Berkeley: USENIX Association, 2023: 6257-6274.

[21] Drean J, Gomez-Garcia M, Bourgeat T, et al. Citadel: Side-channel-resistant enclaves with secure shared memory on a speculative out-of-order processor[EB/OL]. [2023-12-11]. https://arxiv.org/pdf/2306.14882.pdf.

[22] Shang K T, Lu F, Huang K, et al. Cluster nodes integrity attestation and monitoring scheme for confidential computing platform[C]//2023 IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom). Exeter, UK, 2023.

[23] Parma: Confidential containers via attested execution policies[EB/OL]. [2023-12-11]. https://arxiv.org/pdf/2302.03976.pdf.

[24] Confidential computing and privacy-preserving technologies for 6G[EB/OL]. [2023-12-11]. https://confidential6g.eu.

[25] 数字中国建设整体布局规划[EB/OL]. [2023-12-01]. https://www.gov.cn/govweb/zhengce/2023-02/27/content_5743484.htm.

[26] 冯登国. 打造富有弹性的网络空间安全保障体系任重道远[EB/OL]. [2023-11-12]. http://www.secrss.com/arti-

cles/60651.

[27] 邬江兴, 季新生, 贺磊, 等. 内生安全赋能网络弹性研究[J]. 信息通信技术, 2023, 17(4): 4-11.

[28] 金梁, 楼洋明, 孙小丽, 等. 6G无线内生安全理念与构想[J]. 中国科学: 信息科学, 2023, 53(2): 344-364.

[29] 马博林, 张铮, 邵昱文, 等. KMBox:基于Linux内核改造的进程异构冗余执行系统[J]. 信息安全学报, 2023, 8(1): 14-25.

[30] 金希文, 葛强, 张进, 等. 拟态路由器TCP代理设计实现与形式化验证研究[J]. 信息安全学报, 2023, 8(5): 1-13.

[31] 张进, 葛强, 徐伟海, 等. 拟态路由器BGP代理的设计实现与形式化验证[J]. 通信学报, 2023, 44(3): 33-44.

[32] Miao K C, McEwen M, Atalaya J, et al. Overcoming leakage in quantum error correction[J]. Nature Physics, 2023, 19: 1780-1786.

[33] Google Quantum AI and Collaborators. Measurement-induced entanglement and teleportation on a noisy quantum processor[J]. Nature, 2023, 622: 481-486.

[34] Google Quantum AI and Collaborators. Phase transition in random circuit sampling[EB/OL]. [2023-12-22]. https://arxiv.org/pdf/2304.11119.pdf.

[35] Litinski D. How to compute a 256-bit elliptic curve private key with only 50 million Toffoli gates[EB/OL]. [2023-06-14]. https://arxiv.org/pdf/2306.08585.pdf.

[36] Deng Y H, Gu Y C, Liu H L, et al. Gaussian boson sampling with pseudo-photon-number resolving detectors and quantum computational advantage[J]. Physical Review Letters, 2023, 131(15): 150601.

[37] Gouzien É, Sangouard N. Factoring 2048-bit RSA integers in 177 days with 13436 qubits and a multimode memory[J]. Physical Review Letters, 2021, 127(14): 140503.

[38] Gouzien É, Ruiz D, Le Régent F M, et al. Performance analysis of a repetition cat code architecture: Computing 256-bit elliptic curve logarithm in 9 hours with 126133 cat qubits[J]. Physical Review Letters, 2023, 131(4): 040602.

[39] Zhu H T, Huang Y, Liu H, et al. Experimental mode-pairing measurement-device- independent quantum key distribution without global phase locking[J]. Physical Review Letters, 2023, 130(3): 030801.

[40] Ye P, Chen W, Zhang G W, et al. Induced-photorefraction attack against quantum key distribution[J]. Physical Review Applied, 2023, 19(5): 054052.

[41] Quantum 2030: The DND/CAF quantum science & technology strategy implementation plan[EB/OL]. [2023-12-01]. https://www. canada. ca/content/dam/dnd-mdn/documents/reports/2023/dnd-caf-quantum-ststrategy-implementation-plan.pdf.

[42] NIST to standardize encryption algorithms that can resist attack by quantum computers[EB/OL]. [2023-08-24]. https://www.nist.gov/news-events/news/2023/08/nist-standardize-encryption-algorithms-can-resist-attack-quantum-computers#: ~: text=Today% 20NIST% 20released% 20draft%20standards,until%20Nov.%2022%2C%202023.

[43] QuSecure pioneers first-ever U.S. live end-to-end satellite quantum-resilient cryptographic communications link through space[EB/OL]. [2023-03-09]. https://www.qusecure.com/qusecure-pioneers-first-ever-u-s-live-end-to-end-satellite-quantum-resilient-cryptographic-communications-link-through-space/.

[44] Kim Y, Eddins A, Anand S, et al. Evidence for the utility of quantum computing before fault tolerance[J]. Nature, 2023, 618(7965): 500-505.

[45] Liang Q F. Employing quantum key distribution for enhancing network security[C]//Proceedings of the 2023 International Conference on Image, Algorithms and Artificial Intelligence (ICIAAI 2023). Setubal: Scites Press, 2023.

[46] Zhang Y, Li Y, Cui L, et al. Siren′s Song in the AI Ocean: A survey on hallucination in large language models[EB/OL]. [2023-09-24]. https://arxiv.org/pdf/2309.01219.pdf.

[47] Deng G, Liu Y, Li Y, et al. Jailbreaker: Automated jailbreak across multiple large language model chatbots[EB/OL]. [2023-10-25]. https://arxiv.org/pdf/2307.08715.pdf.

[48] Qu Y, Shen X, He X, et al. Unsafe diffusion: On the generation of unsafe images and hateful memes from text-to-image models[C]//Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security. Seattle: ACM, 2023.

[49] Carlini N, Ippolito D, Jagielski M, et al. Quantifying memorization across neural language models[C]//The Eleventh International Conference on Learning Representations. Rwanda: ICLR, 2023.

[50] Carlini N, Hayes J, Nasr M, et al. Extracting training data from diffusion models[C]//32nd USENIX Security Symposium (USENIX Security 23). Anaheim: USENIX, 2023: 5253-5270.

[51] Mitchell E, Lee Y, Khazatsky A, et al. Detectgpt: Zero-shot machine-generated text detection using probability

curvature[C]//International Conference on Machine Learning. Seattle: arXiV: 2301.11305.

[52] Sha Z, Li Z, Yu N, et al. De-fake: Detection and attribution of fake images generated by text-to-image generation models[C]//Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM, 2023: 3418-3432.

[53] Meng K, Sharma A S, Andonian A J, et al. Mass-Editing memory in a transformer[C]//The 11th International Conference on Learning Representations. Rwanda: ICLR, 2023.

[54] Gandikota R, Materzynska J, Fiotto-Kaufman J, et al. Erasing concepts from diffusion models[C]//Proceedings of the IEEE/CVF International Conference on Computer Vision. Vancouver: IEEE, 2023.

[55] Pearce H, Ahmad B, Tan B, et al. Asleep at the keyboard? Assessing the security of github copilot's code contributions[C]//2022 IEEE Symposium on Security and Privacy. OakLand: IEEE, 2022: 754-768.

[56] Sandoval G, Pearce H, Nys T, et al. Lost at C: A user study on the security implications of large language model code assistants[C]//32nd USENIX Security Symposium (USENIX Security 23). Anaheim: USENIX, 2023: 2205-2222.

[57] Deng Y, Xia C S, Peng H, et al. Large language models are zero-shot fuzzers: Fuzzing deep-learning libraries via large language models[C]//Proceedings of the 32nd ACM SIGSOFT international symposium on software testing and analysis. New York: ACM, 2023: 423-435.

[58] Pearce H, Tan B, Ahmad B, et al. Examining zero-shot vulnerability repair with large language models[C]//2023 IEEE Symposium on Security and Privacy. OakLand: IEEE, 2023: 2339-2356.

[59] 互联网信息服务算法推荐管理规定[EB/OL]. [2022-03-01]. http://www.cac.gov.cn/2022-01/04/c_1642894606364259.htm.

[60] 互联网信息服务深度合成管理规定[EB/OL]. [2022-11-25]. http://www.cac.gov.cn/2022-12/11/c_16722219493-18230.htm?utm_campaign=84.

[61] 生成式人工智能服务管理暂行办法[EB/OL]. [2023-07-13]. https://www. gov. cn/zhengce/zhengceku/202307/content_6891752.htm.

Review of 2023 cybersecurity technology hotspots

FENG Dengguo, LIAN Yifeng

Institute of Software, Chinese Academy of Sciences, Beijing 100190, China

Abstract In 2023, countries such as the United States, Europe, Australia, Japan, South Korea, and India successively released national policies and strategic plans for cybersecurity, and the strategic position of cybersecurity was becoming increasingly prominent and constantly improving. At the same time, high covert and destructive attack activities represented by APT attacks, ransomware attacks, supply chain attacks, new network attacks, and mobile attacks were frequent, posing serious security threats to the global cyberspace. Zero trust, confidential computing, privacy computing, and resilient security technologies were flourishing. Quantum key distribution and anti quantum cryptography continued to achieve technological innovation and breakthroughs. Generative artificial intelligence created a new development space for cybersecurity, and the field of cybersecurity was facing unprecedented development opportunities and application prospects.

Keywords cybersecurity; data security; artificial intelligence security

（责任编辑　卫夏雯）