2023年工业控制系统安全热点回眸

程鹏[1],张镇勇[2],车欣[1],陈积明[1*]

1. 浙江大学控制科学与工程学院,工业控制技术全国重点实验室,杭州 310027
2. 贵州大学计算机科学与技术学院,省部共建公共大数据国家重点实验室,贵阳 550000

摘要 2023年,勒索病毒仍然威胁着全球工业控制系统安全,地缘政治冲突加剧导致工控系统成为敌对双方网络攻击的重要战场,供应链攻击再度成为工控系统的软肋。工控系统安全行业关注度持续提升,各国围绕工控系统安全展开大规模演习;工控系统安全政策、标准相继出台,相关行业有规可循、有法可依;软硬件漏洞仍然是工控系统"硬伤",而"离地攻击"则可绕开漏洞实施"低成本、大威胁"攻击;研究人员开发了新型攻击手段,深度横向移动攻击、PLC勒索病毒使得威胁直指工控系统控制层,模块化、功能强大的工控系统攻击工具Pipedream为攻击者指明攻击路径;工控系统安全防护技术持续迭代更新,安全厂商和研究机构相继推出安全监控平台、可信DCS、攻击取证工具、轻量级密码算法、零信任机制传感器,网络安全逐渐被考虑纳入工控系统设计环节,功能安全、信息安全一体化协同设计取得突破;在PLC运行时安全测试、协议实现正确性测试、协议逆向分析技术、攻击检测技术方面都有创新性研究成果;新兴技术如人工智能、数字孪生、大语言模型等为工控系统安全带来机遇;工控安全外溢到卫星系统,欧美等国开始为网络战的空天战场作准备。

关键词 工业控制系统;安全防护技术;数字化;智能化

2023年,地缘政治冲突引发的工控系统攻击事件再次凸显工控系统在国家安全层面的重要性。面向工控系统的大规模安全演练逐步走向常态化,以可靠性为主的传统工控系统面临漏洞多且难修复的难题,新型攻击手段能够实现攻击在异构PLC之间的深度横向移动,面向PLC的勒索病毒将直接威胁控制过程。

工控安全巨头Dragos披露的工控攻击工具Pipedream将影响使用CodeSys开发的所有工控系统。安全企业和研究机构提出了可信工控设备、轻量级密码算法、零信任机制等以保护工控系统。前沿研究在工控设备模糊测试、协议逆向、攻击检测等方面均取得创新性成果。人工智能、数字孪生、大语言模型等新兴技术有望被应用于解决工控安全问题。卫星系统安全成为继工控安全之后全球黑客关注的目标。

收稿日期:2023-12-28;修回日期:2024-01-04

作者简介:程鹏,教授,研究方向为信息物理系统安全,电子信箱:lunarheart@zju.edu.cn;陈积明(通信作者),教授,研究方向为网络系统安全,电子信箱:cjm@zju.edu.cn

引用格式:程鹏,张镇勇,车欣,等. 2023年工业控制系统安全热点回眸[J]. 科技导报, 2024, 42(1): 314-328; doi:10.3981/j.issn.1000-7857.2024.01.021

1　工控安全事件全球爆发

2023年,勒索病毒仍然是关键基础设施的主要威胁,巴以冲突、俄乌冲突开辟了面向工控系统的网络战场,供应链漏洞显现了超大规模杀伤力。

1.1　勒索病毒仍是主要威胁

勒索病毒自发现以来,仍然影响着各大关键基础设施,工控系统也不例外。2023年1月,葡萄牙市政供水公司Aguas do Porto遭到Lockbit勒索软件攻击[1],Lockbit已将Aguas do Porto添加到其Tor网站的被攻击目标列表中,并威胁要泄露被盗数据。2月,全球最大的半导体制造设备和服务供应商,美国应用材料公司表示其一家上游供应商遭到勒索软件攻击[2],由此产生的关联影响预计将给下季度造成2.5亿美元的损失。4月,意大利供水公司AltoCalore Servizi SpA被勒索软件袭击[3],导致其所有IT系统无法使用。5月,瑞士自动化巨头ABB成为网络犯罪组织Black Basta发起的勒索软件攻击受害者[4],影响了数百台设备。全球工控安全龙头企业Dragos门户网站和客户支持系统遭到勒索病毒的攻击[5],一个网络犯罪团伙试图突破Dragos的防御系统,渗透到其内部网络。7月,全球最大芯片制造商台积电遭到LockBit勒索软件团伙攻击[6],被索要7000万美元赎金。12月,美国造船公司Austal USA遭到猎人国际(Hunters International)勒索软件和数据勒索组织的攻击[7]。

1.2　地缘冲突引爆网络攻击

地缘冲突仍然持续,巴以冲突再度成为全球关注的焦点,而随着热战而起的是乌云密布的网络战争。7月,伊朗黑客组织“网络复仇者”(Cyber-Av3ngers),在Telegram频道中声称已经渗透和瘫痪了以色列最大的炼油厂运营商BAZAN集团网络[8],该组织利用CheckPoint防火墙漏洞渗透到了炼油厂的网络,并发布了BAZAN集团公司SCADA系统的屏幕截图。这一攻击造成BAZAN集团网站bazan.co.il和eng.bazan.co.il出现访问超时、HTTP 502错误、服务器拒绝服务等。CyberAv3ngers也攻击了以色列上加利利地区的灌溉系统和污水处理系统[9],导致监控这些系统的数个水位监测器失灵。被入侵的控制器显示一条消息“你被黑客入侵了,打倒以色列”(图1)。美国宾州阿里奎帕市市政供水系统也遭到该黑客组织的控制[10],攻击者关闭了一条负责从阿里奎帕市水务局处理厂向浣熊镇和波特镇输送饮用水的水泵。12月,美国网络安全和基础设施安全局分析了CyberAv3ngers发起的网络攻击事件[11],指出这些攻击的一个共同点是,均利用了以色列生产的Unitronics可编程逻辑控制器(programming logic controller,PLC)的漏洞。

图1　以色列生产的Unitronics可编程逻辑控制器遭伊朗黑客组织CyberAv3ngers控制

10月18日,以色列黑客组织Red Devil成功渗透伊朗电力网络[12],造成伊朗全国范围内多地电力供应中断。事后,该组织向伊朗发出警告:“请不要玩火,否则下一次攻击会造成更大的破坏,这并不是你们所熟知的网络攻击。”这表明地缘政治冲突会加剧网络战争,而面向民生工程的工控系统成为主要目标。另外,俄乌战争持续到了2023年,双方的网络战争也从未停歇。11月9日,美国网络安全公司Mandiant发布报告[13],俄罗斯军事情报机构的黑客组织沙虫(Sandworm)针对乌克兰一处变电站发起了新型协同攻击。Sandworm首先使用工控级“离地攻击”技术使变电站断路器跳闸,导致意外停电;同时,乌克兰各地的关键基础设施遭到大规模导弹袭击,物理设施被彻底摧毁。Sandworm通过虚拟机管理程序获得了对工控环境的访问权限,该虚拟机管理程序为目标变电站托管了SCADA服务。进一步,利用名为“a.iso”的光盘镜像执行本地MicroSCADA二进制文件,执行恶意控制命令来关闭变电站。此外,Sandworm在变电站IT环境中部署了恶意数据擦除软件CADDYWIPER的新变种,以造成进一步的破坏,并掩盖攻击的踪迹。

1.3 供应链攻击肆虐横行

2023年最流行的供应链攻击莫过于针对文件传输工具MOVEit的攻击,该攻击横行肆虐,影响了英国、加拿大、法国、以色列等20多个国家和地区,造成了400多个组织的敏感数据泄露。攻击者利用Progress Software软件公司MOVEit Transfer软件的0-Day漏洞,非法访问受害者的服务器[14]。Progress Software软件公司称该漏洞是一个未知的SQL注入漏洞,漏洞编号为CVE-2023-34362[15]。6月,三大工业控制器制造商施耐德电气、西门子能源和霍尼韦尔均遭到MOVEit攻击[16],美国国家实验室放射性废物储存设施也受到该攻击的影响[17]。为了节省产品开发时间,越来越多公司使用现成的第三方代码库或工具加速产品开发进度。而作为供应链的上游企业,如果第三方代码库或工具的研发企业安全意识薄弱导致出现安全漏洞,无疑将殃及池鱼,致使下游企业也面临严重安全威胁。

2 行业关注度持续上升

工控系统面临的攻击威胁持续加剧,警示相关行业"亡羊补牢"否则会造成不可估量的损失,工控企业的安全考量需要具有长远目光和主动意识。根据美国SANS报告[18],2019年,38%的受访者认为工控系统面临的威胁"很高",2021年增长至40%,2022年增长至41%,2023年增长至44%。自动化产业巨头罗克韦尔公司公布了《工控系统中100多起网络安全事件剖析》的调查结果[19],显示2020—2022年的工控网络安全事件已超过1991—2000年期间报告的总数,威胁行为者最关注能源行业(占攻击的39%),网络钓鱼仍然是最流行的攻击技术(34%),在超过1/2的工控安全事件中,SCADA系统是最主要目标(53%),可编程逻辑控制器是第二常见的目标(22%)。

为应对工控系统面临的攻击威胁,4月18—21日,北约组织在爱沙尼亚首都塔林举行代号为"Locked Shields 2023"的网络安全演习[20],如图2[21]所示,以应对针对电网、水处理系统和其他关键基础设施的网络攻击,提升重大危机情况下合作战术和战略决策的能力。中国工信部主办"铸网2022"[22]和"铸网"2023[23]网络安全演练,通过调动全国工信力量,围绕电信、工业互联网等核心工业产业,汇聚百余支网络安全专业队伍,通过实网攻防、远程渗透等形式,开展工业领域的网络安全实网演练,全面检验重点行业和企业的网络安全防护能力。

图2 Locked Shields网络防御演习画面

3 各国相继推出工控安全政策和标准

保障工控系统安全至关重要,是国家安全的重要一环,但仅依赖行业自觉性仍然不够,需要政府主导,做到有规可循、有法可依。2023年2月7日,美国政府问责局发布《网络安全高危系列:保护网络关键基础设施的挑战》[24],以建议联邦政府在保护工业控制系统方面发挥更强有力的作用,尤其针对电力和其他能源系统。3月2日,美国国家网络总监办公室发布拜登政府首份《国家网络安全战略》[25],该战略详细阐述了拜登政府将采取的网络安全政策措施,围绕建立"可防御、有韧性的数字生态系统"的内容,涉及5大支柱共27项举措。9月28日,美国国家标准与技术研究院(NIST)发布了NIST SP 800-82 Rev. 3[26],该标准提供了关于如何确保工控系统安全的指南,同时满足工控独特的性能、可靠性和安全要求。

中国早在2015年便开始制定相关法规政策,尤其是面向工控行业的等保2.0,为工控系统安全保驾护航。2022年年底,工信部再发布《工业和信息化领域数据安全管理办法(试行)》[27],主要内容包括界定工业和信息化领域数据和数据处理者概

念,明确监管范围和监管职责,确定数据分类分级管理、重要数据识别与备案相关要求,针对不同级别的数据,围绕数据收集、存储、加工、传输、提供、公开、销毁、出境、转移、委托处理等环节,提出相应安全管理和保护要求,自2023年1月1日起施行。3月17日,国家标准化管理委员会发布2023年第1号中华人民共和国国家标准公告,批准发布国家标准GB/T 42445—2023《工业自动化和控制系统安全IACS环境下的补丁管理》[28],该标准描述了对已经建立并正在维护的工业自动化和控制系统(IACS)补丁管理计划资产所有者和IACS产品供应商的要求。7月,中国牵头提出的国际标准ISO/IEC 24392:2023《网络安全:工业互联网平台安全参考模型》[29]正式发布,从工业互联网平台安全域、系统生命周期和业务场景3个视角构建了工业互联网平台安全参考模型。

4　工控系统面临新型威胁

工控系统软硬件漏洞不可避免,包括难以修复的漏洞、来不及修复的"永久漏洞"。"离地攻击"则绕开漏洞而利用工控系统资源攻击系统自身,大大降低了攻击成本,对工控系统构成极大威胁。另外,研究人员开发出新型攻击手段,PLC深度横向移动攻击、PLC勒索病毒使得威胁直指工控系统控制层。模块化、功能强大的工控系统攻击工具Pipedream成为黑客组织热捧的工控系统攻击手段。

4.1　漏洞威胁不可避免

4.1.1　难以修复的漏洞

由于工控系统所在生产环境的特殊性,难以平衡安全维护和生产效益之间的关系,导致工控系统很多漏洞无法修复,可以说是"顽疾"。在2010年震网事件中[30],攻击者利用Microsoft Windows中的多个0-DAY漏洞获得对西门子组态软件和PLC的访问权限,成功破坏伊朗布什尔核设施的约1000台高速离心机(图3[31])。然而,在震网事件发生十多年后,新的研究表明用户依然很少启用PLC的安全控制机制。西门子企图通过加密机制来保护私有协议的数据读写和编程操作,但这种加密机制依然存在漏洞。Claroty的Team82团队[32]在私钥未知的情况下,假冒西门子TIA Portal编程软件与PLC进行通信,成功从PLC中提取密码,从而绕过访问控制机制的保护。这说明,即使西门子采用代码混淆技术来保护自定义加密算法,仍然无法消除硬编码私钥带来的安全隐患。2023年Black Hat Europe上,来自德国ENLYZE公司的安全研究人员[33]构建了一个可用于逆向分析S7-1500软件控制器的框架,并首次对S7-1500控制器的通信协议进行了完整描述,证明了即使西门子采用定制加密机制,这样的努力还是没能提高控制器的安全性。

图3　震网病毒感染伊朗核设施

4.1.2　来不及修复的"永久漏洞"

漏洞利用是攻击者成功执行攻击的重要途径,一个简单常识便是通过修复漏洞来杜绝攻击,然而,漏洞总是出现,并且有些漏洞可能永远都不会被修复。2023年8月,美国网络安全公司Synsaber在《工控脆弱性》[34]报告中提到"永久漏洞"(forever-day vulnerability)的概念,指在即将退役或结束生命周期的设备中发现的漏洞,这些设备生产时间久远或供应商早已停止提供相应服务,因此,供应商不会修补这些易受攻击的漏洞。考虑工控系统长达10~20年的使用年限,其存在大量此类漏洞而无法找到供应商提供的补丁产品,安全防护能力被严重削弱。

那么,考虑这样一个场景,如果目标控制系统使用的数百万设备包含了已知且容易被利用的漏洞,攻击者为什么还要花费大量精力去挖掘0-Day漏洞呢?在用于炼油厂、电厂和其他关键基础设施的软件或设备中,未修补的"永久漏洞"数量正在不

断增加,成为可被攻击者轻易获取和利用的“猎物”。根据Fortinet 2017年第二季度的统计数据[35],攻击者正利用存在至少3年且未安装补丁的漏洞对90%的组织或单位进行网络攻击。如果没有及时安装补丁或没有资金更新过时设备,存在“永久漏洞”的路由器、服务器和工控设备,随时都可能被远程黑客入侵、篡改甚至关闭。例如,在ABB销售的机器人软件ABB WebWare Server中存在“永久漏洞”[36],攻击者可以远程发送命令来关闭或控制搭载该软件的工程师站。但是,ABB发布通告称:“由于这些是接近生命周期结束的传统产品,ABB并不打算修补存在该漏洞的组件。”用户无意修复的“永久漏洞”也会造成重大损失,如臭名昭著的WannaCry勒索软件,预估已造成全球超过40亿美元的损失[37]。

4.2 新型攻击手段层出不穷

4.2.1 低成本大威胁的“离地攻击”

针对IT系统的攻击往往需要攻击者具备丰富的漏洞知识,然而,由于工控系统操作的对象是物理系统,设计成功的攻击无需挖掘大量漏洞,利用工控系统自身的控制逻辑便可实现对物理系统的破坏。2023年,在美国SANS的一份报告中首次提出“离地攻击”(living-off-the-land attack)的概念[38]。“离地攻击”是利用目标系统已有的资源或工具向目标系统发起攻击的一种低成本攻击方式,可被利用的系统资源包括:(1)有效凭据。攻击者可以利用有效凭据从信息网横向移动到控制网,然后利用合法账户在整个控制网络中任意“游走”。(2)工控协议。攻击者利用控制系统中已部署的工控协议向目标设备发送恶意攻击流量,控制目标包括HMI、PLC、RTU等。(3)运行脚本。攻击者可利用系统中预装的PowerShell运行恶意软件,而无需额外引入攻击工具或恶意载荷,这有助于躲避检测。(4)组态软件。组态软件能够监视、控制和修改生产过程,也会被攻击者利用来非法操控控制系统。(5)可信的网络路径。攻击者利用防火墙允许的网络端口或协议访问目标设备,从而避免被防火墙阻断。

常规网络攻击需要攻击者事先完成攻击载荷构造,并将攻击载荷传输进系统内网,最后再投送到指定目标设备。另外,还需对攻击载荷进行加密处理以实现隐蔽性。因为缺乏对目标系统的了解,难以做到定向攻击。相比之下,采用“离地攻击”,攻击者只利用目标系统已有资源或工具,存在以下优点:(1)攻击者不需要额外构造攻击载荷,攻击成本更少;(2)攻击行为混淆在正常操作中,没有明显特征,难以被防御机制检测,潜伏时间更长;(3)由于攻击者使用系统中的合法工具,攻击手段灵活性和适应性更强。典型案例,如,攻击者渗透进入佛罗里达州奥尔德斯马市的水处理设施控制系统中[39],利用HMI上调了水中氢氧化钠碱液的含量,使其达到有毒水平;Trisis/Triton病毒利用工程师站与PLC的通信协议篡改了PLC的控制逻辑[40]。

4.2.2 控制器深度横向移动攻击

根据工控系统的普渡模型(Purdue model),控制层的控制器一直是攻击者劫持的终极目标,伊朗震网、沙特海渊、美国风鲨等攻击,最后都聚焦于如何利用控制器实现物理破坏,而控制器的安全问题远不止“由外至内”被非法利用,也能“由内向外”产生更大规模的攻击影响。2023年,安全公司Forescout公布了一份在PLC之间进行深度横向移动攻击的研究报告[41],这是对“深度横向移动”攻击的首次系统研究。科研人员在搭建的可移动桥梁实验环境中,利用2个被披露的安全漏洞CVE-2022-45788和CVE-2022-45789,对控制桥梁移动的PLC进行攻击,实现了以最大速度关闭桥梁,同时将安全系统禁用,最终物理损坏桥梁的攻击目标。

如图4所示,在所设计的可移动升降桥控制系统实验环境中,桥梁系统的执行器由施耐德M340 PLC控制,SCADA系统通过耦合器Wago 750与施

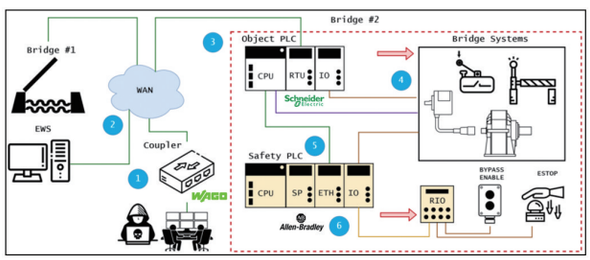

图4 PLC深度横向移动攻击路径

耐德 M340进行通信交互,实现对桥梁的开启和关闭控制。桥梁系统的物理安全由 Allen-Bradley GuardLogix生产的安全PLC负责,该安全PLC与施耐德M340通过以太网接口进行交互。在进行攻击时,执行如下操作:(1) 攻击者利用 CVE-2021-31886漏洞获取耦合器 Wago 750远程代码执行权限,以便与 M340 进行自由通信;(2) 利用 CVE-2022-45789漏洞实现认证绕过并能自由登录访问 M340;(3) 利用 CVE-2022-45788 漏洞获取 M340 的远程代码执行权限,以便与GuardLogix安全PLC进行自由通信;(4) 利用CVE-2019-12256漏洞获取GuardLogix安全PLC以太网模块的远程代码执行权限;(5) 禁用GuardLogix安全PLC。科研人员渗透进入桥梁系统控制网络后,综合利用上述漏洞获取不同PLC的控制权限,完成了在不同PLC间的深度横向移动攻击,最终实现了对桥梁系统的物理破坏。

4.2.3　基于PLC实现的勒索病毒

虽然勒索病毒在全球范围内广泛传播,但其主要针对IT系统的主机和服务器。工控系统最核心的设备是控制器,其掌握着生产流程的"命脉",工控厂商长期以来一直担忧控制器可能会受到勒索病毒攻击,如今这种担忧已变成现实。2023年,来自法国网络安全公司 Orange Cyberdefense 的科研人员提出了一种名为 Dead Man's PLC(DM-PLC)的新型网络敲诈勒索方法[42],旨在对工控设备进行勒索攻击,同时规避现有的网络安全防御和恢复策略。DM-PLC在实施工控系统网络勒索攻击时分为3个阶段。在准备阶段,攻击者通过工程师站识别并验证当前PLC项目,识别PLC之间的通信关系,并深入了解核心代码块。这一阶段是为了深入了解生产过程,为后续的攻击做准备。在部署阶段,通过建立不同PLC之间、工程师站与PLC之间的通信,完成定时轮询并检测工程师站和PLC的设备状态,确保勒索行为未被篡改,通过引入支持操作过程中断的控制代码,使得攻击者在攻击时能够禁用核心代码块的运行,从而破坏生产过程。此外,还采取措施防止受害者响应并恢复。在攻击阶段,攻击者将攻击控制参数由OFF(0)状态切换至ON(1)状态,DM-PLC接收指令后离开网络潜伏状态,开始执行攻击函数。当受害者支付赎金后,通过输入解锁密钥,可将攻击参数再次切换为OFF(0)状态,从而停止运行DM-PLC。

与传统网络攻击方法不同,DM-PLC方法强调利用合法的、由供应商提供的PLC功能,无需开发复杂的攻击代码。其关键特征在于绕过当前系统的网络安全响应和恢复机制,使得很难直接移除被感染的PLC。借助特定的攻击触发机制,例如,勒索定时器超时机制或攻击行为篡改检测机制,确保攻击只有在特定条件下才会被触发,并以最大程度影响工控系统的运行。这种灵活而定制的方法使得DM-PLC成为一种具有极强破坏能力的网络攻击手段。

4.2.4　新型工控攻击工具诞生

随着攻击技术和手段不断进化,新型攻击工具成为最大威胁。2023年,科研人员开始大量关注针对工控系统的Pipedream攻击工具[43],该工具由一套和工控系统攻击相关的定制工具组成,利用MITRE ATT&CK for ICS矩阵量化其攻击能力,Pipedream覆盖了38%的已知攻击技术和83%的已知攻击策略。即使其针对的对象是特定的Omron和Schneider PLC,但由于Pipedream利用的缺陷实体被大范围地应用,例如CodeSys作为数百种工业设备的供应商使用的控制系统开发平台,在市场上具有高达35%的占有率。因此,该工具实际上具有极其广阔的火力覆盖面积。在攻击方法上,其首先利用模块扫描目标设备,对设备详细信息进行侦察,再利用设备安全缺陷将恶意代码上传至目标设备,对设备参数进行修改。针对施耐德PLC产品,Pipedream通过目标端口为27127的UDP组播识别本地网络上所有的施耐德PLC。由于UDP 27127是工作站用于发现PLC的标准端口,因此,这种扫描方式具有极高隐蔽性。然后,利用CODESYS和其他可用设备协议安全性上的不足对PLC的密码进行暴力破解。进而执行拒绝服务攻击、死包攻击、发送自定义Modbus命令等多种恶意攻击。针对欧姆龙PLC产品,Pipedream使用FINS协议扫描欧姆龙设备,通过轮询连接到PLC,然后将任意文件备份或恢复到PLC,或在PLC上加载恶意代理,

从而获得更强的攻击定向能力。

由于Pipedream滥用多种工控协议且涉及海量的工控产品,美国联邦调查局认为Pipedream的研究者至少拥有国家级高级持续威胁攻击开发的能力。由此可见,针对工控系统的攻击态势愈演愈烈,攻击者的手段趋向于复杂化,潜在的攻击目标逐步扩大化,攻击工具的威胁能力和威胁强度日益增高。

5 工控安全防护技术更新换代

面对工控系统风云变幻的攻击手段,卓有成效的安全防护迫在眉睫,各大企业纷纷推出新产品,以应对日益严峻的工控系统安全威胁。

5.1 美国开发下一代工控安全平台

2023年6月,美国Network Perception公司推出下一代NP-View平台[44],用于实现工控网络的轻量级、非侵入性可视化,其特点在于其能够为安全团队提供快速、直观的网络漏洞识别和风险评估能力。NP-View利用改进算法创建更加直观的拓扑图,为技术和非技术用户提供一个易于理解的风险定位系统,拓扑图不仅能够展示网络结构,还能揭示潜在的安全漏洞和风险点。NP-View优化了其路径分析算法,利用先进的拓扑推理技术,显著提升了对网络安全风险的分析效率。NP-View平台还提供一系列网络安全解决方案,包括网络可见性、防火墙审计等。在网络可见性方面,为了在复杂的网络环境中确保网络的安全性和可管理性,该平台作为网络架构的中枢信息汇聚点,采纳网络子网及安全区标签化的最佳实践,对网络拓扑进行独立的文档验证。在防火墙审计方面,NP-View允许生成、排序、自定义和导出支持设备的所有规则的报告,以确保网络设备的持续合规性和安全性。此外,NP-View采用路径分析技术,展示了资产在网络中可能到达的潜在路径,为资产被渗透的情况提供了预见性分析。

5.2 中国推出首台可信DCS

2023年11月,中国首台国产可信DCS在华能威海电厂辅助控制系统成功投运[45],在电力安全领域再次取得重大突破,为电站提供了更加安全可信的运行环境。该系统采用100%国产化设计,首次实现了控制系统核心上、下位机CPU芯片、操作系统、中间件和控制应用的软硬件全面可信,可有效阻止从多种路径发起的恶意渗透、操纵和篡改攻击。系统已通过可信权威认证,是中国首个、唯一通过全栈可信功能测试和验证的工业控制系统。

5.3 微软发布工控系统取证工具

在2023年黑客大会上,来自Microsoft Defender的研究人员[46]发布了用于分析PLC元数据和项目文件的开源取证工具包。工控系统取证工具使调查人员能够识别工控环境中的可疑攻击,以便在事件响应或手动检查期间检测受损设备。该工控取证工具已经开源,允许调查人员验证工具的操作或根据特定需求进行定制。

5.4 NIST公布轻量级加密算法

2023年2月,美国NIST宣布轻量级密码学标准算法Ascon为遴选计划的优胜者[47],该计划旨在选出最佳算法来保护硬件资源有限的设备。Ascon算法基于Sponge操作模式的SPN置换实现轻量级哈希和加密,在功耗、计算速度、消息开销等方面优势明显,可用于微型传感器和执行器,例如植入式医疗设备、道路和桥梁内的压力检测器等,工控场景下的诸多设备可以采用该加密方法来保证数据传输的安全性。

5.5 Cynalytica推出基于“零信任机制”的传感器

零信任机制是基于“永远不信任,总是验证”的原则,对网络的访问者身份进行双向认证。在传统的访问控制手段,一旦用户通过初始验证,系统通常会信任用户或设备,而零信任模型要求对于每次访问行为进行持续验证,将关键网络划分为更小的、可管理的单元,限制攻击者在内部网络中横向移动的能力。零信任机制也可通过边缘安全访问服务提供零信任访问支持,或者通过云平台整合传统网络安全服务(如防火墙、VPN、零信任网络访问),为用户提供远程、统一且可扩展的安全访问服务,并且能够实现对网络流量的高效管理和控制。

2023年4月,美国网络安全公司Cynalytica推出工控系统监控传感器OTNetGuard[48],如图5所示,OTNetGuard可为工控系统提供安全的、带外数

图5　Cynalytica推出零信任机制传感器OTNetGuard

据监控。OTNetGuard特点如下:(1) 全新的模块化数据捕获平台,支持广泛的工控网络通信,如模拟信号、串行通信和TCP/IP网络流量;(2) 与Cynalytica的AnalytICS引擎兼容,提供加密通信传输、深度数据包解析(DPI)功能,深度分析报文并对异常进行警报,可集成到现有的SIEM/SOAR解决方案中;(3) 支持无线通信,如SFP、Wi-Fi、蜂窝网络;(4) 支持本地存储和边缘离线分析;(5) 可通过更换不同的物理层模块实现对不同协议深度数据包解析,物理层模块包括RS-232、RS-485/422、高速Profibus-DP、CAN总线等。作为零信任网络架构的重要组成部分,OTNetGuard能够实现对潜在物理威胁和操作异常的带外态势感知。

5.6　逐步推行"安全融于设计"

国际制造业咨询机构ARC权威专家Cosman在2019年便提出工控系统需要实现"安全融于设计"(Secure by design)[49],这种设计理念非常重要,但仍然只是一种安全保障的思路。2023年5月,北美电力可靠性公司NERC发布了《基于网络的传输计划》(Cyber-Informed Transmission Planning)白皮书[50],强调日益复杂的网络攻击要求电力系统加强韧性,抵御潜在攻击对系统的影响。NERC将优先制定以网络安全为基础的输电规划方案,将网络安全风险纳入输电规划活动中,以减轻网络攻击导致的可靠性问题。设计者需要深入研究安全威胁相关的突发事件对电网的影响,并为传统输电网络升级提供新视角。通过在未设立安全措施的系统中加入安全设计,将会降低电力系统可靠性和安全性风险。

5.7　强调工控一体化安全防护

国际标准组织IEC/ISO/IEEE以及区域性组织均强调了工控系统功能安全和信息安全的重要性。随着智能化元素增多,工控系统硬件故障包括组件失效、供电不足、过热失效、界面失效、通信中断等,以及网络攻击如远程访问、信息窃取、物理破坏、设备跳板等,均呈现出高涌现、多并发、信物协同等特点,难以分析和辨识。功能安全与信息安全共存会产生整体安全冲突,为功能需要而开放的端口和远程访问平台均会带来网络安全风险,而网络攻击具有强隐蔽性和高级持久性,信息物理攻击路径难预测,矛盾存在的功能安全和信息安全措施难以协调。中国机械工业仪器仪表综合技术经济研究所的研究者指出,可将工控系统的普渡模型分成信息域、耦合域和物理域,在构建新型智能工厂时,需要将功能安全与信息安全协同设计,形成工控系统一体化安全建设方案[51]。

6　前沿防护技术推陈出新

工控系统安全研究持续向更深更难问题发起挑战,在PLC运行时安全测试、协议实现正确性测试、协议逆向分析技术、攻击检测技术方面均取得较大进展,应用计算机安全协会主办的国际顶级会议ACSAC连续两年将杰出论文奖颁给了工控安全方向的文章。

6.1　PLC运行时安全测试工具

如何在运行时环境中测试PLC的安全性一直是一大挑战。来自新加坡(新加坡科技设计大学)、美国(NYU Tandon School of Engineering, New York University Abu Dhabi)和德国(CISPA Helmholtz Center for Information Security)的研究者解决了这一问题,并提出测试工具FieldFuzz[52]来实现任意PLC的运行时安全测试。由于PLC运行在闭源代码之上,需要以黑盒方式或通过逆向工程进行模糊测试。FieldFuzz框架运用基于网络的模糊测试方法,对Codesys运行时(被80多家工业PLC厂商的400多种设备所使用)进行安全风险分析。FieldFuzz的主要贡献包括:(1) 通过逆向工程实现应用程序和运行时组件的远程控制;(2) 通过网络流量自动发现控制命令和提取状态码;(3) 开发测试监控系统以实现系统跟踪和覆盖率计算。研究者使

用FieldFuzz对Codesys不同版本的runtime进行了模糊测试,根据实验结果,FieldFuzz的漏洞发现速率提高了约8.3倍,并在测试arm32和x64架构的runtime时,崩溃发现数量提高了约291倍和262倍。

6.2 协议实现正确性测试工具

协议实现是网络基础设施的重要组成部分,协议实现中隐藏的漏洞很容易被敌手利用以发起攻击。因此,保证协议实现的正确性非常重要。然而,由于缺乏有效的反馈机制和足够的协议状态空间探索技术,常用的漏洞检测技术(如模糊测试)在测试协议实现时面临很大挑战。中国和新加坡联合研究团队(清华大学、电子科技大学和新加坡国立大学)解决了这一问题,并在2023年四大安全顶会之一的Usenix Security上发布了工具Bleem[53]。Bleem是一种面向数据包序列的黑盒模糊测试器,用于协议实现的漏洞检测。Bleem并不关注单个数据包的生成,而是在序列级别上生成数据包。其通过非侵入式分析系统输出序列来提供有效的反馈机制,通过及时跟踪各方的状态空间来支持引导式模糊测试,并利用交互式流量信息来生成协议逻辑感知的数据包序列。通过实验验证,Bleem在一天的时间内可以将分支覆盖率提高174.93%。

6.3 面向语义信息的协议逆向分析技术

可编程逻辑控制器是工控系统的重要组成部分,在关键基础设施(如电力、石化、冶金)中发挥着核心作用。近年来,Stuxnet、Triton等一系列攻击事件表明攻击者对PLC的控制器变量(如设备状态和内部程序逻辑)具有浓厚兴趣。从网络流量中监测控制器变量是抵御该攻击的有效方法,这依赖于对PLC使用的工业控制协议(ICP)进行语义解析。然而,ICP的私有性使得解析控制器变量语义变得困难。ACSAC杰出论文奖授予了解决这一难题的论文,科研人员提出了一个名为SePanner[54]的语义解析框架,可以自动从私有ICP的网络流量中解析控制器变量的语义。SePanner能够自动采集不同状态下的PLC与上位机软件的网络交互流量,利用ICP协议"起始对齐"的特点,对网络流量进行多状态对比。SePanner克服了传统语义解析工具在解析语义时依赖协议先验知识和时间戳定位的特点,能够从流量中直接定位代表目标控制器变量的语义字段,进而找到包含目标语义信息的工控协议报文及"语义—字段"对应关系。同时,SePanner通过一系列过滤机制来克服乱序字段和动态字段的干扰。实验表明,SePanner可以从PLC的网络流量中精确提取PLC控制器的变量语义,并能在部分流量缺失时依旧保持识别准确率。SePanner解析出的控制器变量语义有效支持了PLC实时状态监测和异常流量识别,同时对其他私有二进制协议具有良好的扩展性。

从防护者角度,协议逆向技术是分析工控网络安全的重要手段,在安全四大顶会NDSS 2023上,来自美国的研究者提出了一款协议逆向工具BinaryInferno[55]。这是一款用于自动化逆向二进制协议格式的工具,其以一组具有相同格式的消息作为输入,从字段语义的角度出发,利用不同语义内生的统计学特征作为检测手段,归纳了IEEE浮点数字段、时间戳字段、长度字段等常见字段的特性,并且通过搜索常见序列化习语来发现可变长度序列,因而能够推广到逆向不可见数据类型的协议。相较于逆向工程领域中较为传统的多序列比对方法,BinaryInferno既能对字段的语义作出解释,又具有较低的误判率。在对10个二进制协议数据包集进行逆向的实验中,其识别字段边界的平均精确度为0.69,平均召回率为0.73,平均误报率为0.04,明显优于其他5种最先进的协议逆向工程工具:Awre(0.18, 0.03, 0.04)、FieldHunter(0.68, 0.37, 0.01)、Nemesys(0.31, 0.44, 0.11)、Netplier(0.29, 0.75, 0.22)和Netzob(0.57, 0.42, 0.03)。作为最新的研究成果,BinaryInferno有效弥补了原有语义识别方法无法将数据类型从已知推广到未知的缺陷,而其模块化的设计也为功能的进一步拓展提供了可行性。虽然该工具仍依赖于输入报文集合的聚类质量,以及逆向工程师对于模块的选择和应用能力,但其仍是现有二进制协议逆向分析较好的工具之一。

6.4 新型工控系统攻击检测技术

攻击者在对工控系统进行攻击时,会将攻击行为伪装成正常的SCADA操作,从而躲避现有安全工具的检查。美国国家实验室的研究人员提出了

一款新型攻击检测工具SCAPHY[56],通过利用SCADA独特的执行阶段来识别出合法的行为,从而区分出正常和恶意操作。例如,SCADA系统会在初始化阶段设置工控设备,但不会在生产过程中再对工控设备进行其他设置。为了提取SCADA系统执行期间的独特行为,SCAPHY首先利用公开的工控系统约定,生成一个新的物理过程依赖和影响图(PDIG),用以识别异常的物理状态。然后,SCAPHY会使用PDIG进行物理过程感知,通过引导SCADA过程控制执行的代码路径,揭示合法过程控制阶段独有的API调用序列。基于合法的API调用序列,SCAPHY会监控不合法的过程控制行为。研究人员在美国国家实验室的工控系统实验床中进行了实验,在4个工业场景下,SCAPHY的攻击检测准确率达到了95%(平均值),误报率为3.5%(平均值),图6给出了佛罗里达州水厂中毒攻击事件还原及使用SCAPHY检测的效果。

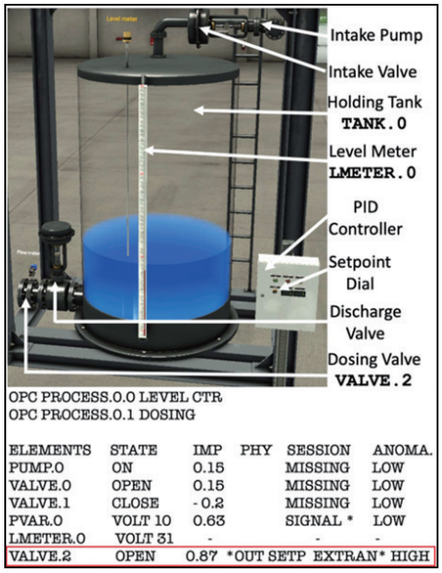

图6　佛罗里达州水厂中毒攻击事件还原及使用SCAPHY检测的效果

7　新兴技术给工控系统安全带来机遇

随着人工智能和大数据的发展,人工智能、数字孪生、大语言模型等新兴技术也逐渐被应用于工控系统安全。

7.1　基于人工智能的补丁技术

2023年2月,美国网络安全公司Trackd启动了自动修复软件漏洞技术的项目[57],以构建一个不断更新的修补漏洞经验的数据库,并将其与机器学习技术相结合,以帮助修复团队了解哪些补丁可能具有破坏性,以及哪些补丁可以在无需人工干预的情况下安全地自动部署。人工智能技术能够提升威胁检测、风险预测等性能,增强网络和设备安全评估能力,彻底改变工控系统安全"敌多我寡""敌强我弱"的局面。然而,人工智能在工控系统安全领域的应用也具有挑战,存在误报率高、缺乏透明度、数据质量低和对抗性攻击威胁等问题。重要的是,安全团队要仔细考虑在工控系统安全中使用人工智能的好处和挑战,并实施最佳实践,以确保人工智能的有效使用。这些最佳实践可能包括选择正确的人工智能算法、确保高质量的数据、纳入人类监督范围、定期测试人工智能算法性能,以评估其有效性并识别潜在漏洞。

7.2　数字孪生与风险评估

传统的风险评估方法面临系统复杂性和有限可视性的挑战,导致企业难以全面理解面临的攻击风险。为了应对这一挑战,以色列工控安全公司OTORIO推出集成高级攻击图分析功能的安全风险评估技术,将攻击图分析与网络数字孪生模型(Cyber Digital Twin, CDT)[58]相结合,为用户提供动态可视化网络拓扑和高级风险评判,从而能够发现工控系统中的漏洞。该安全风险评估技术,首先利用数字孪生技术建立系统实体间的复杂关系,生成工控网络的数字副本;其次,基于CDT模型生成详细的攻击图,揭示网络资产和漏洞之间的连接关系,包括描绘出网络分段间隙和针对关键资产和流程的潜在攻击向量。这种全面的风险可视化手段使企业能够及早发现工控威胁、实现主动风险管理,也能够利用这些动态生成的攻击图来精确识别潜在的攻击向量和风险点,从而采取有效措施保护工控系统的关键设备。该技术不仅彰显了数字孪生技术在网络安全领域的巨大应用潜力,更为该领域的未来发展奠定了坚实基础。

7.3　数字孪生与事件响应

在工控安全领域,事件响应是一项涉及网络和

物理设备两个维度的复杂任务。为提升事件响应的质量和效率,来自奥地利和英国的研究人员提出利用数字孪生来增强信息物理系统对网络攻击事件的响应能力[59],其提出3种模式的数字孪生:数据分析模式的数字孪生通过机器学习、大数据挖掘等技术分析历史数据,用于评估攻击范围和严重性;模拟模式的数字孪生基于物理系统运行规律搭建动态模型,用于自动评估事件的严重性,并预测可能的未来事件;复制模式的数字孪生根据真实系统运行数据复制系统,提供系统的实时数据副本来帮助调查和干预,并确保系统在根除威胁后能正确运行。

7.4 虚拟PLC提供更灵活的安全解决方案

2023年4月,汉诺威工博会上西门子展示了其首款虚拟工业控制器SIMATIC S7-1500V[60],这是一款完全虚拟的PLC。其基于SIMATIC S7-1500 PLC的功能和操作,可以像应用程序一样下载并直接集成到IT环境中。S7-1500V的特性在于其硬件的独立性,用户可以从任何地方灵活地访问控制器和SIMATIC S7-1500 PLC的所有功能。虚拟PLC超脱于传统PLC的软硬件强制绑定束缚,实现了PLC的数字孪生。虚拟PLC可以通过云端完成部署和管理,数据可以转发到边缘系统中的应用程序进行进一步处理。更为重要的是,虚拟PLC可为在役PLC运行状态安全监控和分析提供平台。

7.5 大语言模型与工控安全

2023年,掀起了通用大语言模型的竞赛浪潮,大语言模型在控制领域的应用也受到广泛关注。来自微软亚研院的研究者[61]考虑在通用大语言模型的基础上,利用少量样本和技术陷阱来重新训练决策模型,并基于该模型对HVDC系统进行控制,结果证明GPT-4比传统强化学习、模型预测方法在应对系统不确定性时的控制性能都好。来自西门子公司的研究者[62]则通过理论分析了大语言模型用于生成工业自动化模型的安全弹性,并提供方法来分析生成控制方法和自动化策略的可靠性和有效性。但不容忽视的是,大语言模型的脆弱性也会成为使用它所开发的控制环境的安全威胁。

8 工控系统安全外溢到其他领域

2023年,随着俄乌战争的恶化,战争焦点从地面转向了太空,由于卫星通信和定位对于战场环境尤为重要,卫星系统安全引起了广泛关注。

8.1 地空系统安全事件成为热点

卫星系统的地面部分成为热点攻击目标。2023年3月,黑客组织GhostSec[63]发布了一条推文,声称劫持了全球导航卫星系统GNSS的接收器,并分享了GNSS接收器的多张图像,作为其成功访问的证据。4月,隶属于GhostSec的用户在Twitter上发布了更多声明,声称摧毁了大量与俄罗斯、以色列基础设施相关的GNSS接收器。如果GhostSec的说法属实,那么这些攻击的影响可能会产生毁灭性的后果,因为卫星依赖复杂的地面网络系统来接收命令和下行信息。该事件也凸显了卫星网络存在不容忽视的漏洞,特别是提供远程通信访问的访问网关、RTU和控制器。

8.2 攻入卫星成为黑客的新目标

为测试和评估卫星系统的安全性,欧洲和美国均开展了攻击卫星的“夺旗赛”。2023年4月26—27日,法国巴黎举办首次全球航天网络安全挑战赛[64],欧洲航天局建立了一个卫星测试台来模拟夺取卫星OPS-SAT的控制权,这是该机构出于演示目的运营的一颗纳米卫星。攻击者需要对全球定位系统、姿态控制系统和机载摄像头系统等展开攻击。泰雷兹的网络安全团队成功访问了卫星的机载系统,并利用多个漏洞将恶意代码植入卫星,破坏发送回地球的数据,例如,修改卫星相机拍摄的图像,掩盖卫星图像中选定的地理区域,同时隐藏其活动以躲避检测。

2023年6月5日,在佛罗里达州肯尼迪航天中心,SpaceX和NASA有史以来第一次将一颗卫星(“月光者”号)送入近地轨道[65],以供研究人员测试在轨卫星的安全性。8月,在美国DEF CON大会上首次举办了太空夺旗赛,参赛队伍的任务是入侵“月光者”号,以突破限制控制卫星观察指定的地面目标并拍摄目标的照片,然后将该图像下载到地面

站。5支队伍参加了比赛,最终意大利黑客团队mHACKeroni成功入侵“月光者”号卫星[66],并成功传回了拍摄地球的照片(图7)。

图7　“月光者”号发射和黑客组织mHACKeroni劫持卫星后拍摄的地球照片

8.3　类似工控安全的太空安全分析技术

2022年12月30日,美国国家标准与技术研究院(NIST)发布了地空操控系统“太空运营-地面部分”的网络安全指南[67],重点关注地面部分对卫星的指挥和控制安全,指南从识别、保护、检测、响应、恢复5个方面给出安全防护的系统性功能需求,识别功能需要具备资产、数据、工具等方面的风险评估能力,保护功能需要保证在潜在网络安全事件下能够限制影响扩大,检测功能需要能够及时发现网络攻击,响应功能需要遏制攻击的传播和进一步破坏,恢复功能需要具有及时修复、降低影响、提供取证等方面的能力。这是NIST首次针对地空操控系统发布安全指南,说明地空操控系统正在面临网络攻击的威胁。

9　结论

数字化、智能化是人类社会发展的必然趋势,相伴而生的信息安全问题是难以避免的“副作用”。保障工控系统安全至关重要,但百分百保证工控系统安全是无法做到的。回眸2023年,工控系统安全依然面临严峻挑战,但新技术、新方法为解决工控系统安全防护难题提供了重要思路。现实场景中,安全产品的功能性往往被弱化以满足工控系统运行的可靠性要求,因此如何寻求折中、合理的安全方案是重中之重。随着传统产业的转型升级,工控系统未来面对的必然是跨系统协同的安全威胁。多系统(如IT系统、物联网系统、工控系统、智能系统)融合造成的工程复杂性会带来更多的安全漏洞,如何在规划、设计、建设、运行、维护等全流程考虑安全是未来要解决的重要问题。

参考文献(References)

[1] Montreal electricity organization latest victim in LockBit ransomware spree[EB/OL]. (2023-08-31) [2023-12-23]. https://therecord. media/montreal-electricity-organization-lockbit-victim.

[2] Semiconductor industry giant says ransomware attack on supplier will cost it $250 million[EB/OL]. (2023-02-17) [2023-12-23]. https://therecord. media/applied-materials-supply-chain-mks-ransomware-attack.

[3] Italy's Alto Calore Servizi SpA confirms a ransomware attack[EB/OL]. (2023-05-11)[2023-12-23]. https://izoologic.com/region/europe/italys-alto-calore-servizi-spa-confirms-a-ransomware-attack.

[4] ABB confirms data stolen in Black Basta ransomware attack[EB/OL]. (2023-05-30)[2023-12-23]. https://www.scmagazine.com/news/abb-basta-ransomware-attack.

[5] Deconstructing a Cybersecurity event[EB/OL]. (2023-05-10)[2023-12-23]. https://www.dragos.com/blog/deconstructing-a-cybersecurity-event.

[6] TSMC says supplier hacked after ransomware group claims attack on chip giant[EB/OL]. (2023-06-30)[2023-12-23]. https://www.securityweek.com/tsmc-says-supplier-hacked-after-ransomware-group-claims-attack-on-chip-giant.

[7] Ransomware attack on australian shipbuilder working for US navy[EB/OL]. (2023-12-05)[2023-12-23]. https://australiancybersecuritymagazine. com. au/ransomware-attack-on-australian-shipbuilder-working-for-us-navy.

[8] Israel's largest oil refinery website offline after DDoS attack[EB/OL]. (2023-07-30) [2023-12-23]. https://www.bleepingcomputer.com/news/security/israels-largest-oil-refinery-website-offline-after-ddos-attack.

[9] Cyber attack leaves irrigation systems in Upper Galilee dysfunctional[EB/OL]. (2023-04-09)[2023-12-23]. https://www.jpost.com/israel-news/article-738790.

[10] Iranian-linked cyber army had partial control of aliquippa water system[EB/OL]. (2023-11-25) [2023-12-23]. https://beavercountian. com/content/special-coverage/iranian-linked-cyber-army-had-partial-control-of-aliquippa-water-system.

[11] Iranian hackers exploit plcs in attack on water authority in U.S.[EB/OL]. (2023-11-29)[2023-12-03]. https://thehackernews. com/2023/11/iranian-hackers-exploit-plcs-

in-attack.html.
[12] Israeli hackers cause major disruptions in iranian electricity grid[EB/OL]. (2023-10-18)[2023-12-23]. https://www.time.news/israeli-hackers-cause-major-disruptions-in-iranian-electricity-grid.
[13] Sandworm disrupts power in ukraine using a novel attack against operational technology[EB/OL]. (2023-11-09) [2023-12-23]. https://www.mandiant.com/resources/blog/sandworm-disrupts-power-ukraine-operational-technology.
[14] MOVEit zero-day vulnerability under active exploit, data already stolen[EB/OL]. (2023-06-01) [2023-12-23]. https://www.cybersecuritydive.com/news/moveit-zero-day-vulnerability-actively-exploited/651867.
[15] MOVEit transfer and MOVEit cloud vulnerability[EB/OL]. (2023-07-05) [2023-12-23]. https://www.progress.com/security/moveit-transfer-and-moveit-cloud-vulnerability.
[16] Siemens energy, schneider electric targeted by ransomware group in MOVEit attack[EB/OL]. (2023-06-28) [2023-12-23]. https://www.securityweek.com/siemens-energy-schneider-electric-targeted-by-ransomware-group-in-moveit-attack/.
[17] Cyberattack hits US lab contractor, nuclear waste site [EB/OL]. (2023-06-16)[2023-12-23]. https://www.bloomberg.com/news/articles/2023-06-15/us-national-lab-nuclear-waste-site-hit-by-cyberattack.
[18] SANS ICS/OT cybersecurity survey: 2023′s challenges and tomorrow′s defenses[EB/OL]. (2023-09-18) [2023-12-23]. https://www.sans.org/white-papers/ics-ot-cybersecurity-survey-2023s-challenges-tomorrows-defenses.
[19] Cybersecurity incidents in industrial operations[EB/OL]. (2023-08-01) [2023-12-23]. https://www.rockwellautomation.com/en-us/campaigns/cyentiareport.html.
[20] World′s largest cyber defense exercise Locked Shields brings together ove 3000 participants[EB/OL]. (2023-04-21)[2023-12-23]. https://ccdcoe.org/news/2023/6016.
[21] NATO Allies and Partners take part in world′s largest cyber defence exercise[EB/OL]. (2023-04-11)[2023-12-23]. https://www.nato.int/cps/en/natohq/news_214144.htm?selectedLocale=en.
[22] “铸网2022”网络安全演练表现突出单位颁奖在成都举行 [EB/OL]. (2023-02-28) [2023-12-23]. https://www.wangan.com/p/11v726a96d3340fc.
[23] “铸网2023”车联网赛道网络安全实网攻防演练在临港新片区启动[EB/OL]. (2023-08-21)[2023-12-23]. https://www.sh.chinanews.com.cn/fzzx/2023-08-21/115161.shtml.
[24] Cybersecurity high-risk series: Challenges in protecting cyber critical infrastructure[EB/OL]. (2023-02-07)[2023-12-23]. https://www.gao.gov/products/gao-23-106441.
[25] National cybersecurity strategy[EB/OL]. (2023-03-01) [2023-12-23]. https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.
[26] 3 guide to operational technology security[EB/OL]. (2023-09-28) [2023-12-23]. https://csrc.nist.gov/pubs/sp/800/82/r3/final.
[27] 工业和信息化部关于印发《工业和信息化领域数据安全管理办法(试行)》的通知[EB/OL]. (2022-12-08)[2023-12-23]. https://www.gov.cn/zhengce/zhengceku/2022-12/14/content_5731918.htm.
[28] 工业自动化和控制系统安全 IACS环境下的补丁管理[EB/OL]. (2023-03-17) [2023-12-23]. https://std.samr.gov.cn/gb/search/gbDetailed?id=F789206610FAB223E05397BE0A0AE533.
[29] ISO/IEC 24392: 2023 Cybersecurity-Security reference model for industrial internet platform (SRM-IIP) [EB/OL]. (2023-07-18) [2023-12-23]. https://www.iso.org/standard/78703.html.
[30] Operation Olympic Games: The first cyberweapon[EB/OL]. (2023-11-29)[2023-12-23]. https://www.sandboxx.us/news/operation-olympic-games-the-first-cyberweapon.
[31] 美“震网”蠕虫病毒废掉伊朗1/5离心机[EB/OL]. (2012-12-03)[2023-12-23]. https://www.yazhouribao.com/view/20121203000303.
[32] The race to native code execution in PLCs: Using RCE to uncover siemens SIMATIC S7-1200/1500 hardcoded cryptographic keys[EB/OL]. (2022-10-11) [2023-12-23]. https://claroty.com/team82/research/the-race-to-native-code-execution-in-plcs-using-rce-to-uncover-siemens-simatic-s7-1200-1500-hardcoded-cryptographic-keys.
[33] A decade after stuxnet: How siemens S7 is still an attacker′s heaven[EB/OL]. (2022-12-11) [2023-12-23]. https://i.blackhat.com/EU-23/Presentations/Whitepapers/EU-23-Finck-A-Decade-After-Stuxnet-How-Siemens-S7-is-Still-an-Attackers-Heaven-wp.pdf.
[34] ICS CVE research: First half of 2023[EB/OL]. (2023-11-16) [2023-12-23]. https://synsaber.com/resources/research-reports/ics-cve-reports/ics-cve-research-first-half-2023.
[35] Report: Dissecting our Q2 threat landscape research[EB/OL]. (2017-08-21) [2023-12-23]. https://www.fortinet.com/blog/threat-research/dissecting-our-q2-threat-landscape-report.
[36] Advisory for WebWare components and related products [EB/OL]. (2012-03-23) [2023-12-23]. https://library.e.abb.com/public/35df9dc4a94ae83ac12579ca0043acc1/SI-

10231A2%20rev%200.pdf.

[37] The latest 2023 ransomware statistics[EB/OL]. (2023-01-12) [2023-12-23]. https://aag-it. com/the-latest-ransomware-statistics.

[38] Living off the land attacks and countermeasures in industrial control systems[EB/OL]. (2023-10-10) [2023-12-23]. https://www. sans. org/blog/living-off-land-attacks-countermeasures-industrial-control-systems.

[39] Hacker tries to poison water supply of Florida city[EB/OL]. (2021-02-08) [2023-12-23]. https://www. bbc. com/news/world-us-canada-55989843.

[40] Attackers deploy new ICS attack framework "TRITON" and cause operational disruption to critical infrastructure [EB/OL]. (2017-12-14) [2023-12-23]. https://www. mandiant. com/resources/blog/attackers-deploy-new-ics-attack-framework-triton.

[41] Deep lateral movement in OT networks: When is a perimeter not a perimeter? [EB/OL]. (2023-02-13) [2023-12-23]. https://www.forescout.com/blog/deep-lateral-movement-in-ot-networks-when-is-a-perimeter-not-a-perimeter.

[42] Derbyshire R, Green B, Walt C, et al. Dead man's PLC: Towards viable cyber extortion for operational technology [J/OL]. [2023-12-23]. https://arxiv.org/abs/2307.09549.

[43] Chernovite's pipedream malware targeting industrial control systems(ICS) [EB/OL]. (2022-04-13) [2023-12-23]. https://www.dragos.com/blog/industry-news/chernovite-pipedream-malware-targeting-industrial-control-systems.

[44] Unleashing the power of network visualization with NP-View's topology map[EB/OL]. (2023-06-27) [2023-12-23]. https://network-perception.com/blog-unleashing-the-power-of-network-visualization.

[45] 国内首台全国产可信DCS系统成功投运[EB/OL]. (2023-12-08) [2023-12-23]. https://www. chng. com. cn/detail_yxxw/-/article/2vMCKgtLDZqb/v/1181068.html.

[46] ICS forensics tools[EB/OL]. (2023-08-10)[2023-12-23]. https://www. blackhat. com/us-23/arsenal/schedule/index.html#ics-forensics-tools-32135.

[47] Lightweight cryptography standardization process: NIST selects ascon[EB/OL]. (2023-02-07)[2023-12-23]. https://csrc.nist.gov/news/2023/lightweight-cryptography-nist-selects-ascon.

[48] Next-Generation monitoring platform and advanced analytics for OT communications-IP, serial communications, and analog signals[EB/OL]. (2023-03-12) [2023-12-23]. https://cynalytica.com/otnetguard.

[49] Standards address the need for secure-by-design industrial control system products[EB/OL]. (2019-05-10) [2023-12-23]. https://www. arcweb. com/blog/standards-address-need-secure-design-industrial-control-system-products.

[50] Cyber-informed transmission planning[EB/OL]. (2023-05-08)[2023-12-23]. https://www.nerc.com/comm/RSTC_Reliability_Guidelines/ERO_Enterprise_Whitepaper_Cyber_Planning_2023.pdf.

[51] 制造系统功能安全与信息安全技术发展趋势及一体化解决思路[EB/OL]. (2023-07-06)[2023-12-23]. https://mp.weixin.qq.com/s/w35tP6qnqrAKCcMcpbeFQA.

[52] Bytes A, Rajput P H N, Doumanidis C, et al. FieldFuzz: In situ blackbox fuzzing of proprietary industrial automation runtimes via the network[C]//Proceedings of the 26th International Symposium on Research in Attacks, Intrusions and Defenses. New York: ACM. 2023: 499-512.

[53] Luo Z, Yu J, Zuo F, et al. Bleem: Packet sequence oriented fuzzing for protocol implementations[C]//The 32nd USENIX Security Symposium. Anaheim: USENIX Association, 2023: 4481-4498.

[54] Meng J, Yang Z, Zhang Z, et al. SePanner: Analyzing semantics of controller variables in industrial control systems based on network traffic[C]//Proceedings of the 39th Annual Computer Security Applications Conference. Austin: ACM, 2023: 310-323.

[55] Chandler J, Wick A, Fisher K. BinaryInferno: A semantic-driven approach to field inference for binary message formats[C]//The 30th Network and Distributed System Security Symposium. San Diego: CCS, 2023.

[56] Ike M, Phan K, Sadoski K, et al. Scaphy: Detecting modern ICS attacks by correlating behaviors in scada and physical[C]//In 2023 IEEE Symposium on Security and Privacy. San Francisco: CA, 2023: 20-37.

[57] Make data-driven patching decisions[EB/OL]. (2023-01-09)[2023-12-23]. https://trackd.com/learn-more.

[58] Cyber digital twin by OTORIO[EB/OL]. (2023-01-27) [2023-12-23]. https://www. otorio. com/resources/cyber-digital-twin-by-otorio.

[59] Allison D, Smith P, Mclaughlin K. Digital twin-enhanced incident response for cyber-physical systems[C]//Proceedings of the 18th International Conference on Availability, Reliability and Security. Barcelona: CCS, 2023: 1-10.

[60] SIMATIC S7-1500V familiar functionalities, completely virtual[EB/OL]. (2023-04-14) [2023-12-23]. https://www.siemens.com/global/en/products/automation/systems/industrial/plc/simatic-s7-1500/virtual-plc.html.

[61] Sparks of Artificial General Intelligence: Early experiments with GPT-4[EB/OL]. (2023-03-22) [2023-12-23]. https://www. microsoft. com/en-us/research/publication/sparks-of-artificial-general-intelligence-early-experiments-with-gpt-4.

[62] Ogundare O, Araya G Q, Akrotirianakis I, et al. Resiliency analysis of LLM generated models for Industrial Automation[J/OL]. [2023-12-23]. https://arxiv. org/abs/2308.12129.
[63] Briefing 8: Ghostsec hackers target satellite networks via GNSS receivers[EB/OL]. (2023-05-03) [2023-12-23]. https://www.kratosdefense.com/constellations/articles/ghostsec-hackers-target-satellite-networks-via-gnss-receivers.
[64] Thales seizes control of esa demonstration satellite in first cybersecurity exercise of its kind[EB/OL]. (2023-04-25) [2023-12-23]. https://www. thalesgroup. com/en/worldwide/security/press_release/thales-seizes-control-esa-demonstration-satellite-first.
[65] First in space: SpaceX and NASA launch satellite that hackers will attempt to infiltrate during DEF CON[EB/OL]. (2023-06-05) [2023-12-23]. https://cyberscoop.com/moonlighter-hack-a-sat-defcon.
[66] How a hacking crew overtook a satellite from inside a Las Vegas convention center and won $50,000[EB/OL]. (2023-08-16)[2023-12-23]. https://cyberscoop.com/mh-ackeroni-hackasat-space-def-con.
[67] Satellite Ground Segment: Applying the cybersecurity framework to satellite command and control[EB/OL]. (2022-12-30)[2023-12-23]. https://csrc.nist.gov/pubs/ir/8401/final.

Hotspots of industrial control system security in 2023

CHENG Peng[1], ZHANG Zhenyong[2], CHE Xin[1], CHEN Jiming[1*]

1. State Key Laboratory of Industrial Control Technology, College of Control Science and Engineering, Zhejiang University, Hangzhou 310027, China
2. State Key Laboratory of Public Big Data, College of Computer Science and Technology, Guizhou University, Guiyang 550000, China

Abstract In 2023 the ransomware virus still threatened the security of global industrial control systems (ICSs), intensified geopolitical conflicts made the ICS become an important battlefield for hostile cyberattacks, and the supply chain once again became the soft underbelly of ICSs. Fortunately, much more attention was paid to ICS security and large-scale exercises were carried out by countries worldwide. Besides, there were many documents launched by authorities for ICS policies and standards. For techniques, vulnerabilities were newly found and the defense approaches were evolving. Specifically, the software and hardware vulnerabilities were still the unavoidable weakness of ICSs. The "living-off-the-land attack" did not use vulnerabilities but enabled "low-cost, big threat" operations over ICSs. Besides, there were novel attacks such as deep lateral move attack on the control level, the PLC ransomware virus, and the attack toolkit Pipedream. Security vendors and research institutions launched security-specific monitoring platforms for ICSs, produced the trustful DCS, developed the forensics tools, proposed the lightweight cryptographic algorithms, and designed zero trust mechanism sensors. The idea of "secure by design" was gradually taken into the design of ICSs. There were also advanced researches on runtime PLC security testing, protocol implementation correctness testing, protocol reverse analysis, and attack detection. The emerging technologies, such as artificial intelligence, digital twin, and large language model, brought opportunities to the ICS security. Moreover, the ICS security had spillover to satellite systems, and the Europe and US began to prepare for the battlefield of cyber warfare in the space.

Keywords industrial control system; safety pretection technology; digitalize; smart

（责任编辑　卫夏雯）