工业控制系统（ICS）网络安全漏洞挖掘与防护技术

孟　震[1]　韩伟华[2]　张宝宝[3]
1.沈阳市和平区汉口街18号　辽宁沈阳　110001
2.石家庄市长安区跃进路193号　河北石家庄　050032
3.山西省大同市平城区凯德世家　山西大同　037008

摘　要：随着工业控制系统（ICS）在能源、电力、制造和交通等关键基础设施中的广泛应用，其网络安全问题日益突出。ICS系统长期依赖专有协议、传统控制设备以及低延迟通信特性，这使得其面临特有的网络攻击风险。本文以ICS系统为研究对象，分析网络安全漏洞的产生机理，探讨漏洞挖掘技术与防护技术的研究现状及应用方法。文章对漏洞扫描、模糊测试、协议逆向、行为分析等挖掘技术进行了系统总结，并结合入侵检测、防火墙、访问控制及工业网络隔离等防护措施提出优化策略。研究表明，漏洞挖掘与防护技术的协同应用能够有效提升ICS网络安全防御能力，同时在保障生产连续性、降低攻击风险及提高系统韧性方面具有重要作用。

关键词：工业控制系统；网络安全；漏洞挖掘；防护技术；入侵检测

引言

工业控制系统（Industrial Control System，ICS）是现代工业生产的核心技术平台，涵盖了分布式控制系统（DCS）、可编程逻辑控制器（PLC）、监控与数据采集系统（SCADA）及智能传感器等组成部分。随着信息化和自动化技术的发展，ICS系统逐渐与企业网络、云平台及远程监控系统互联，网络攻击面显著增加。ICS系统的特殊性在于其对实时性和安全性的高要求，同时其设备和协议长期缺乏安全设计，使得系统容易受到恶意攻击。近年来，包括Stuxnet、Industroyer和Triton在内的针对ICS系统的攻击事件显示，工业控制系统面临的威胁已经从理论层面转向实际破坏层面，对国家基础设施及工业生产安全构成严重威胁。因此，研究ICS系统网络安全漏洞的挖掘与防护技术具有重要学术价值和实践意义。本文结合现有ICS安全研究，系统分析漏洞挖掘技术与防护技术，提出具有可操作性的策略和方法，为提高ICS系统韧性提供理论参考。

一、工业控制系统网络安全漏洞分析

（一）漏洞产生的内部因素

ICS系统的网络安全漏洞多由系统设计缺陷和实现问题引起。控制设备长期依赖专用硬件和嵌入式软件，存在协议简化、认证机制缺失及默认配置不安全的问题。此外，许多工业设备采用过时的操作系统和通信协议，安全更新周期长或缺乏更新支持，导致已知漏洞长期存在。系统功能实现过程中，为保证生产连续性而牺牲安全性，例如开放远程控制接口、允许无验证通信等，都增加了系统被攻击的风险。

（二）外部攻击环境及威胁因素

ICS系统在工业互联网环境下运行，其网络拓扑复杂、通信协议多样，攻击者能够通过网络渗透、恶意软件植入及社工手段获取系统访问权限。攻击者可能利用零日漏洞、已知缺陷或配置错误实施攻击，破坏控制逻辑或篡改数据。同时，ICS系统对安全事件响应机制不完善，攻击发现延迟严重，使威胁放大效应明显。

（三）典型漏洞类型分析

ICS系统漏洞类型主要包括协议漏洞、设备固件漏洞、配置缺陷及权限管理漏洞等。协议漏洞通常表现为未加密通信、数据包验证缺失及缓冲区溢出等问题。设备固件漏洞可能被攻击者通过远程上传恶意程序触发，破坏系统控制逻辑。配置缺陷包括默认密码、开放端口和弱访问控制等问题，而权限管理漏洞则导致非授权用户能够访问关键控制模块。这些漏洞的存在使ICS系统在面对高级持续性威胁（APT）时缺乏有效防御手段。

二、ICS网络安全漏洞挖掘技术

（一）漏洞扫描技术

漏洞扫描是工业控制系统（ICS）安全评估的重要手段，通过自动化扫描器检测网络设备、操作系统及应用

程序中存在的已知漏洞，为风险管理提供基础数据。针对ICS系统，漏洞扫描不仅要涵盖传统IT网络中的通用漏洞，还需要结合工业协议特性，如Modbus、DNP3、PROFINET及OPC等，以识别设备端口开放状态、默认配置、弱口令及协议实现缺陷。扫描器能够快速覆盖大规模网络设备，对批量化检测具有明显优势，并能生成可量化的安全报告，便于管理人员进行风险评估和优先级排序。然而，漏洞扫描也存在局限性，对零日漏洞（未知漏洞）、复杂逻辑缺陷和定制化攻击手段的识别能力有限。此外，ICS环境对可用性要求较高，频繁扫描可能对生产设备造成干扰，因此在实际应用中需结合扫描策略、频率控制及风险隔离机制。通常，漏洞扫描应与模糊测试、协议逆向和行为分析等方法结合使用，形成多层次、多维度的漏洞发现体系，以提高ICS网络的整体安全性。

（二）模糊测试与协议逆向

模糊测试（Fuzzing）是一种通过向目标系统发送大量异常或随机输入数据，观察系统异常响应以发现潜在漏洞的技术。针对ICS系统，模糊测试需要结合工业协议的特性进行定制化，例如针对Modbus或DNP3协议生成异常命令、超限数据或不规则帧，以揭示设备缓冲区溢出、异常命令处理错误、协议解析漏洞及状态机异常。模糊测试能够发现传统扫描手段难以检测的隐蔽缺陷，尤其在设备固件和协议解析层面表现出独特优势。协议逆向则通过分析未知或闭源协议的通信模式、数据结构及状态转换逻辑，识别潜在安全风险。这在工业设备广泛使用私有协议、文档缺失或未公开的情况下尤为重要。通过协议逆向，安全研究人员能够模拟异常操作、构建漏洞触发条件，补充漏洞扫描和模糊测试的不足。二者互为补充，共同为发现零日漏洞、协议缺陷及潜在安全风险提供了有效途径，为ICS系统的防护和加固提供技术支撑。

（三）行为分析与异常检测

行为分析技术通过建立ICS系统正常操作和通信模式的模型，对偏离正常模式的异常行为进行检测，从而识别潜在威胁。异常检测方法涵盖统计分析、机器学习和深度学习等技术手段，可针对网络流量异常、操作指令异常、设备状态异常及内部威胁进行监测。例如，通过分析控制命令序列的频率、时序及逻辑关系，可以及时发现异常操作或未经授权的控制行为。行为分析在零日攻击、内部威胁和复杂持续性攻击（APT）防御中具有重要作用，能够弥补漏洞扫描和模糊测试在未知攻击识别方面的不足。然而，行为分析依赖大量历史数据用于模型训练，模型的准确性直接影响误报率和漏报率。在实际应用中，需结合安全专家经验、规则库及其他防护手段进行协同部署，以保证检测效果和生产环境安全。行为分析的实时性、可扩展性及与其他安全技术的协作能力，是其在ICS网络安全防护体系中能否发挥核心作用的关键。

三、ICS网络安全防护技术

（一）访问控制与网络隔离

访问控制是保障工业控制系统（ICS）安全的基础措施，通过身份认证、权限管理和策略配置，有效限制未授权用户对系统资源的访问。身份认证不仅包括传统的用户名与密码，还可结合多因素认证、生物识别技术或智能卡，实现对操作人员身份的严格验证。权限管理则基于“最小权限原则”，确保每个用户仅能访问其工作所需的功能和数据，避免权限滥用造成的风险。此外，结合安全策略配置，可以对关键操作设置审批机制和操作审计，实时记录和追踪系统操作行为，为事后分析和追责提供依据。

在网络层面，通过网络分区与隔离技术，将关键控制网络与企业办公网络、互联网或其他非关键网络进行物理或逻辑隔离，显著减少潜在攻击面。常见的隔离方式包括物理隔离、防火墙策略隔离、虚拟局域网（VLAN）划分和访问控制列表（ACL）等。这种隔离不仅降低了外部攻击风险，还能在内部出现安全事件时，将影响范围限制在单一网络分区内，防止攻击在不同网络间横向传播。同时，合理的网络分区与隔离可以优化系统性能，使关键控制流程的通信更加高效和安全。

（二）入侵检测与防御系统

针对ICS网络特点，专用的入侵检测与防御系统（IDS/IPS）在保障生产连续性的同时，实现对异常行为和攻击行为的实时监控。ICS网络与传统IT网络不同，其通信协议、数据传输模式和实时性要求较高，因此入侵检测系统必须兼顾安全性和实时性，避免因误报或处理延迟对生产控制产生负面影响。

具体技术包括签名检测、异常行为分析和深度数据包检测。签名检测通过匹配已知攻击特征，实现对恶意流量的快速识别；异常行为分析则通过对正常网络行为建模，发现异常操作或潜在威胁，能够检测未知攻击；深度数据包检测可解析工业协议和报文内容，对命令合

法性和异常操作进行审查。IDS/IPS还可以与报警系统、日志管理平台及安全信息事件管理（SIEM）系统联动，实现多层次防护，并为应急响应提供决策支持。通过这些手段，可以有效阻断恶意访问、恶意软件传播及未授权操作，提升工业控制网络的整体安全防御能力。

（三）固件与系统安全加固

工业设备和控制系统的固件与软件是潜在攻击目标，因此系统安全加固至关重要。固件安全管理包括固件更新和补丁及时部署，确保设备运行最新版本，修补已知漏洞，防止攻击者利用旧版本漏洞进行入侵。同时，系统最小化配置策略要求关闭不必要的服务、禁用默认账号，并限制系统功能范围，以降低被攻击面。

安全配置审计可以定期检查系统设置与安全策略执行情况，确保安全措施得到落实。通信加密和日志审计也是关键措施，通过加密通信保护数据传输的完整性与机密性，通过日志审计追踪操作历史，帮助发现潜在安全隐患。

此外，引入冗余控制和异常处理机制，可提升系统的容错能力和韧性。在出现攻击或异常操作时，冗余控制可保持关键功能的连续运行，异常处理机制可自动隔离受影响模块，防止故障扩散。这种设计不仅降低了攻击成功率，也增强了系统在面对复杂威胁时的自我恢复能力，保证工业控制网络在高安全要求的环境下稳定可靠运行。

四、ICS漏洞挖掘与防护技术的综合应用

（一）协同防御策略

在工业控制系统（ICS）网络中，单一的防护手段往往难以应对日益复杂的网络威胁。因此，将漏洞挖掘与防护技术相结合，构建协同防御体系显得尤为重要。协同防御通过定期进行漏洞扫描、模糊测试和协议分析，主动发现系统潜在的安全风险。同时，将入侵检测系统（IDS）、访问控制策略、系统加固和补丁管理等被动防御手段与漏洞挖掘结果相结合，实现风险的动态缓解与闭环管理。这种方法不仅可以及时修复已知漏洞，还能提前预测潜在威胁，从而降低攻击成功率。协同防御的优势在于能够实现主动与被动防御的有效协作，使ICS网络能够动态适应新型攻击手段和不断变化的威胁环境，提升整体安全性和可靠性。

（二）智能化安全管理

随着ICS系统规模和复杂度的增加，传统人工安全管理模式存在响应慢、效率低和易出错等问题。引入大数据分析与人工智能（AI）技术，能够实现ICS安全管理的智能化和自动化。通过对历史安全事件、通信流量、设备日志及操作记录进行数据挖掘和建模，构建威胁预测模型，可以实现对潜在异常行为的提前预警，并支持实时入侵响应与风险处置。同时，AI算法能够动态分析网络流量模式，识别异常操作或攻击行为，减少人工干预成本，提高决策的速度与准确性。此外，智能化管理还支持安全态势感知和可视化展示，帮助安全运维人员全面掌握系统运行状态和潜在威胁，实现从被动防御向主动防护的转变。这种融合数据驱动与智能决策的安全管理模式，为ICS网络提供了更高水平的防护能力和可持续安全保障。

结语

随着ICS系统在关键基础设施和工业生产中的应用日益广泛，网络安全问题对国家安全和社会经济发展构成重大挑战。针对ICS的安全特点，漏洞挖掘技术与防护技术必须协同发展，以实现主动防御与被动防护的有机结合。本文系统分析了ICS漏洞产生机制、挖掘方法和防护技术，提出了综合应用和智能化管理策略，为提高ICS网络安全能力提供理论和实践参考。未来，ICS网络安全研究应进一步关注零日漏洞识别、工业协议安全强化、跨系统协同防护以及智能化安全管理体系建设，推动工业控制系统网络安全向高效、可持续和智能化方向发展。

参考文献

[1]姬五胜，李国良.工控系统信息安全[M].电子工业出版社：202501：206.

[2]姚羽，张建新，杨巍，等.工业控制网络安全技术[M].机械工业出版社：202309：391.

[3]周磊，姜双林，饶志波.工业控制系统漏洞补丁应用策略研究[J].信息技术与网络安全，2021，40（09）：58-65.

[4]刘蔚棣，郭乔进，产院东，等.工业控制系统安全发展综述[J].信息化研究，2021，47（01）：1-9+24.

[5]尹丽波.工业信息安全发展报告[M].电子工业出版社：202007：284.

[6]肖建荣.工业控制系统信息安全[M].电子工业出版社：201910：251.