船舶电子信息系统安全防护与数据加密技术

何逸泽
邯郸市交通运输综合行政执法支队　河北　邯郸　056004

摘　要：船舶电子信息系统作为现代航运的核心支撑，其安全性直接关系到船舶航行安全与运营效率。随着网络攻击手段的多样化，系统面临数据泄露、非法访问及通信中断等风险。本文聚焦安全防护与数据加密技术，系统分析通信加密、存储加密及身份认证加密等关键技术，探讨防火墙、入侵检测、安全审计等防护机制的应用，结合船舶特殊环境提出分层防御策略，旨在为船舶电子信息系统安全设计提供理论参考与实践指导，助力航运业应对数字化安全挑战。

关键词：船舶电子信息系统；安全防护实践；数据加密技术应用

引言

船舶电子信息系统集成了导航、通信、动力控制等关键功能，是现代船舶的“神经中枢”。然而，随着船舶与岸基、卫星及其他船舶间通信的数字化程度提升，系统暴露于开放网络环境中的风险显著增加。黑客可能通过截获通信数据、篡改控制指令或攻击存储设备，导致航行事故或数据泄露等严重后果。传统安全防护手段已难以应对复杂威胁，数据加密技术因其能提供端到端的安全保障，成为保障系统安全的核心手段。

1 船舶电子信息系统安全防护实践

1.1 安全架构设计

（1）分层安全架构是其中的核心设计理念之一，它将整个系统划分为不同功能层级，每个层级承担特定安全职责并实施针对性防护措施。这种架构设计遵循从上至下或从外至内的防护逻辑，确保攻击者在突破某一层级后仍需面对后续层级的严格审查，从而大幅增加攻击难度与成本[1]。各层级间通过明确定义的接口进行交互，既保证功能完整性，又限制攻击面扩散。（2）安全区域划分是另一关键设计要素，它基于系统功能关联性与安全需求差异，将物理或逻辑空间划分为不同安全等级的区域。这些区域通过访问控制策略与边界防护设备实现隔离，核心业务区域通常部署最严格的安全措施，仅允许必要通信通过，并记录所有访问行为。不同区域间的数据交换需经过严格审查与转换，防止敏感信息泄露或恶意代码传播，这种划分方式有效限制了攻击范围，即使某一区域被攻破，攻击者也难以横向移动至其他关键区域。（3）安全通信协议选择直接关系到数据传输过程中的安全性，船舶电子信息系统需根据通信场景特点选择适配协议。对于内部网络通信，可采用具备加密与认证功能的专用协议，确保数据在可控环境中安全传输；对于与岸基或其他船舶的远程通信，则需选用国际通用的安全协议。这些协议通常融合对称与非对称加密技术，既保证传输效率，又确保数据机密性，并支持完整性校验与身份认证功能，防止数据被篡改或伪造。

1.2 防火墙与入侵检测系统/入侵防御系统

防火墙与入侵检测系统（IDS）/入侵防御系统（IPS）是船舶电子信息系统安全防护体系中的关键组件，它们通过不同的技术手段协同工作，为系统提供多层次的安全保障。一方面，防火墙作为网络边界的第一道防线，通过预设的访问控制策略对进出网络的流量进行筛选，仅允许符合规则的通信通过，从而阻止未经授权的访问尝试。其配置与管理需根据船舶电子信息系统实际业务需求和网络拓扑结构进行精细化设计，既要确保关键业务应用的正常通信，又要严格限制不必要的网络连接。管理员需定期审查防火墙规则库，及时更新策略以应对新出现的安全威胁，同时开启日志记录功能以便追踪异常流量来源。另一方面，入侵检测系统（IDS）则侧重于对网络流量的深度分析，通过模式匹配、异常检测等技术手段识别潜在的攻击行为。IDS通常部署在关键网络节点，持续监控通过的流量，一旦检测到可疑活动立即生成警报通知安全团队。与防火墙的被动防御不同，IDS具备主动分析能力，能够发现已知和未知的攻击模式，为安全防护提供更全面的视角。此外，入侵防御系统（IPS）在功能上与IDS类似，但具备更强的主动响应能力。当检测到攻击行为时，IPS不仅能发出警报，还能自动阻断恶意流量，防止攻击进一步扩散。这种实时拦截机制显著提升了系统的安全防护效率，尤其适用于对实时性要求较高的船舶电子信息系统。

1.3 安全审计与日志管理

安全审计与日志管理是船舶电子信息系统安全防护

中不可或缺的环节，它通过系统化记录、分析安全事件与系统活动，为安全策略优化与风险处置提供关键依据。其中，安全事件记录需覆盖系统各层级的关键操作，包括用户登录、权限变更、数据访问、配置修改等行为，确保所有可能影响系统安全的活动均被完整捕获。记录内容应包含时间戳、操作主体、操作对象及具体动作等核心要素，以便后续追溯与分析[2]。分析环节则侧重于从海量日志中提取有价值信息，通过关联不同事件的时间顺序与逻辑关系，识别潜在攻击模式或异常行为。另外，日志集中管理通过将分散在各设备与系统中的日志汇聚至统一平台，解决日志孤岛问题，提升分析效率与准确性。集中管理需考虑日志传输的安全性，采用加密通道防止数据在传输过程中被篡改或窃取，同时确保日志的完整性，避免因设备故障或人为干预导致记录缺失。日志分析工具是挖掘日志价值的核心，其功能涵盖日志清洗、格式标准化、事件关联分析及可视化展示等。清洗与标准化处理可消除不同设备日志的格式差异，为后续分析奠定基础；事件关联分析通过建立时间、空间、逻辑等多维度关联模型，将零散日志转化为有意义的攻击链或操作流程；可视化展示则以图表、仪表盘等形式直观呈现安全态势，帮助管理员快速定位关键问题。

1.4 应急响应与灾难恢复

（1）应急响应计划制定需基于全面的风险评估，明确可能影响系统的各类威胁场景，如网络攻击、设备故障或自然灾害等，并针对不同场景设计详细的响应流程。计划应涵盖事件检测、初步分析、影响范围评估、处置措施选择及后续恢复等环节，确保每一步都有明确的责任人与操作指引。同时，需建立跨部门协作机制，整合安全、运维、业务等团队资源，形成统一指挥的应急响应体系，避免因职责不清导致响应延误。（2）数据备份与恢复策略是保障业务连续性的关键，需根据数据重要性与更新频率制定差异化备份方案。核心业务数据应采用实时或准实时备份，确保数据丢失窗口最小化；非关键数据可适当降低备份频率以平衡存储成本[3]。备份介质需选择安全可靠的存储方式，如异地容灾中心或加密云存储，防止因单一地点故障导致数据永久丢失。（3）恢复策略需明确数据还原流程与优先级，优先恢复支撑关键业务运行的数据，确保系统在故障后能快速恢复核心功能。灾难恢复演练与评估是验证应急响应能力的重要手段，需定期模拟真实故障场景，检验应急响应计划的有效性。（4）演练应覆盖从事件触发到系统完全恢复的全流程，重点测试团队协作效率、处置措施执行情况及恢复时间目标是否达标。演练结束后需开展全面评估，分析响应过程中的薄弱环节，如信息传递延迟、资源调配不足或技术操作失误等，并据此优化应急响应计划与恢复策略。

2 船舶电子信息系统中的数据加密应用

2.1 通信加密

（1）船舶与岸基通信加密需满足高安全性与高可靠性的双重需求，通常采用混合加密机制，结合对称加密与非对称加密的优势。在通信建立阶段，使用非对称加密算法（如RSA或ECC）交换会话密钥，确保密钥传输的安全性；在数据传输阶段，则利用对称加密算法（如AES）对实际业务数据进行加密，提升加密效率。同时，需引入数字签名技术，对传输数据进行完整性校验，防止数据在传输过程中被篡改，确保岸基接收到的信息与船舶发送的内容完全一致。（2）船舶间通信加密面临动态网络环境与设备异构性挑战，需采用轻量级加密协议以适应带宽有限与计算资源受限的场景。部分方案通过预共享密钥机制简化密钥管理流程，船舶在出厂或入网时预先配置加密密钥，通信时直接调用密钥进行加密，减少密钥协商过程的开销[4]。针对船舶间频繁的短时通信需求，还可采用会话密钥动态更新策略，每次通信生成新的临时密钥，即使某一密钥泄露，也不会影响其他通信的安全性。（3）卫星通信加密技术需应对长距离传输与信号衰减带来的安全风险，通常采用分层加密架构，在物理层对信号进行调制加密，防止信号被截获后直接解析。在网络层与应用层则通过IPSec或TLS等协议实现端到端加密，确保数据在卫星链路与地面网络中的全程保护。为应对卫星通信的高延迟特性，加密算法需优化计算效率，减少加密解密过程对通信时延的影响。此外，卫星通信加密还需考虑抗干扰能力，通过扩频技术或跳频技术分散信号能量，降低被恶意干扰的风险，确保在复杂电磁环境下仍能维持安全通信。

2.2 数据存储加密

数据存储加密是船舶电子信息系统数据安全防护的核心环节，通过技术手段对存储介质中的数据进行加密处理，确保数据在静态存储状态下的机密性与完整性。（1）本地存储加密方案需兼顾安全性与设备性能，通常采用全盘加密或文件级加密技术。全盘加密通过硬件加密芯片或软件加密驱动对存储设备进行整体加密，所有写入设备的数据均自动加密，读取时需通过合法认证解密，这种方式实现简单且对上层应用透明，但需确保加密密钥的安全存储，避免因密钥泄露导致数据暴露。文件级加密则针对特定敏感文件或目录实施加密，灵活性更高，可针对不同安全等级的数据采用差异化加密策略，

减少加密对系统性能的影响，但需应用层配合实现加密逻辑，可能增加开发复杂度。（2）云存储加密策略需应对数据脱离本地控制的安全风险，通常采用客户端加密与服务端加密相结合的方式。客户端加密在数据上传至云端前完成加密处理，确保云服务提供商无法直接访问明文数据，密钥由用户独立管理，这种方式安全性最高，但需用户自行承担密钥管理责任，且加密后的数据无法直接利用云服务的搜索或分析功能。服务端加密则由云服务提供商在存储阶段对数据进行加密，用户通过访问控制权限管理数据访问，这种方式使用便捷，但需信任云服务提供商的密钥管理能力。（3）数据库加密技术需解决数据加密与查询效率的矛盾，通常采用字段级加密或透明数据加密（TDE）方案。字段级加密针对数据库中的敏感字段实施加密，加密后的数据以密文形式存储，查询时需通过解密函数实时解密，这种方式安全性高但可能影响查询性能，需优化加密算法与解密逻辑以减少延迟。透明数据加密则在数据库文件层面实施加密，对上层应用完全透明，无需修改应用程序即可实现数据加密，但加密粒度较粗，无法针对特定字段实施差异化保护，且需确保数据库服务进程能够安全访问加密密钥，避免密钥泄露导致全库数据暴露。

2.3 身份认证加密

一方面，在身份认证环节，加密技术主要用于保护认证凭证的传输与存储安全，防止攻击者窃取或篡改用户身份信息。传统基于用户名和密码的认证方式易受暴力破解或中间人攻击，因此常结合加密哈希函数对密码进行单向加密存储，即使数据库泄露，攻击者也无法直接获取明文密码[5]。动态口令技术则通过时间同步或事件触发生成一次性密码，结合加密算法确保每次认证的随机性，有效抵御重放攻击。更高级的认证方式如基于公钥基础设施（PKI）的数字证书认证，通过非对称加密技术验证用户身份，私钥由用户独占持有，公钥绑定用户身份信息并由可信机构签发，认证过程中双方通过加密通道交换证书并验证签名，确保身份的真实性与不可抵赖性。另一方面，加密令牌与数字证书是身份认证加密的典型实现形式，加密令牌通常采用硬件或软件形式生成动态认证码，其内部集成加密芯片或算法，确保令牌生成过程的不可预测性。令牌与认证服务器之间通过加密协议同步状态，用户输入令牌码与静态凭证（如密码）完成多因素认证，提升认证安全性。数字证书则作为用户或设备的电子身份证，包含公钥、身份信息及可信机构的数字签名，通过加密技术确保证书的完整性与真实性。在船舶电子系统中，数字证书可用于船舶设备、岸基系统及用户终端的身份认证，建立端到端的信任链，确保通信双方的身份可信。

结语

综上所述，船舶电子信息系统安全防护是动态演进的过程，需持续跟踪技术发展与威胁态势，优化加密算法与防护策略。未来，随着量子计算、人工智能等技术的突破，传统加密体系可能面临挑战，需提前布局抗量子加密等前沿技术。航运企业应建立“技术-管理-人员”三位一体的安全体系，强化全员安全意识，定期开展攻防演练与漏洞修复。

参考文献：

[1]郎方.大数据背景下电子信息系统安全防护技术研究[J].中国新技术新产品,2025,(20):130-132.

[2]王文强.电子信息系统中的数据加密技术及安全性提升措施[J].消费电子,2025,(4):221-223.

[3]卜骁男.电子信息数据加密技术在计算机网络安全中的应用[J].中国自动识别技术,2025,(4):67-69.

[4]袁海锋.大数据背景下电子信息数据的安全防护机制研究[J].计算机应用文摘,2025,41(13):219-221.

[5]陈跃辉.互联网环境下计算机网络数据安全加密技术研究[J].网络安全和信息化,2021,(6):32-34.