 DOI: https://doi.org/10.12349/iser.v6i3.5206

Network security technology and industrial network solutions

Guo Li

Tongling Nonferrous Metals Group Co., Ltd. Jinxin Copper Branch, Tongling, Anhui, 244000, China

Abstract

With the rapid development of industrial automation and information technology, the industrial network is increasingly complex, and the network security problem is increasingly prominent, and has become a key factor restricting the development of industrial automation and intelligent manufacturing. In order to cope with this challenge, this paper analyzes the application of network security technology in the industrial network, according to the characteristics of the industrial network, summarizes the security challenges facing the industrial network, and puts forward the corresponding solutions, including network isolation, access control, data encryption, security audit and so on. This scheme can effectively deal with all kinds of security threats faced by the industrial network, and provide a strong guarantee for the development of industrial automation and intelligent manufacturing in China.

Keywords

network security technology; industrial network; solution

网络安全技术与工业网络解决方案

李国

铜陵有色金属集团股份有限公司金新铜业分公司，中国 · 安徽 铜陵 244000

摘　要

随着工业自动化和信息化的高速发展，工业网络日益复杂，网络安全问题日益凸显，成为制约工业自动化和智能制造发展的关键因素。为应对这一挑战，本文分析了网络安全技术在工业网络中的应用，针对工业网络特点，总结了工业网络面临的安全挑战，提出了相应的解决方案，包括网络隔离、访问控制、数据加密、安全审计等。该方案能够有效应对工业网络面临的各类安全威胁，为我国工业自动化和智能制造的发展提供有力保障。

关键词

网络安全技术；工业网络；解决方案

1 引言

随着信息化、智能化技术的快速发展，网络安全问题日益凸显，特别是在工业网络领域。工业网络是工业自动化和智能制造的基础，其安全稳定运行对于保障国家经济安全和社会稳定具有重要意义。然而，近年来，工业网络攻击事件频发，对工业生产、国家安全和人民生命财产安全造成了严重威胁。因此，研究网络安全技术与工业网络解决方案，提高工业网络安全防护能力，已成为当前亟待解决的问题。

2 网络安全技术在工业网络中的应用

2.1 防火墙技术

防火墙是一种网络安全设备，它通过监控和控制网络流量，防止未经授权的访问和攻击，确保网络的安全。防火墙的原理基于访问控制策略，对进出网络的数据包进行审查和过滤。防火墙根据预设的安全策略，允许或拒绝特定 IP 地址、端口号、协议等的数据包通过 [1]。记录网络流量，便于分析安全事件和追踪攻击源。将内部网络与外部网络进行隔离，降低安全风险。实时监控网络流量，发现异常行为并及时报警。识别并阻止恶意攻击，保护网络免受侵害。

工业网络具有实时性、稳定性、可靠性等特点，对网络安全要求较高。防火墙技术在工业网络中的应用主要体现在以下几个方面：（1）边界防护：在工业网络的边界部署防火墙，防止外部攻击者入侵内部网络。（2）内网隔离：在工业内部网络中，根据业务需求和安全等级，将网络划分为多个安全区域，通过防火墙实现区域间的隔离。（3）数据加密：对敏感数据进行加密传输，确保数据在传输过程中的安全性。（4）安全审计：对工业网络进行安全审计，及时发现并处理安全漏洞。（5）应急响应：在发生安全事件时，防火墙可以迅速响应，切断攻击源，降低损失。

【作者简介】李国（1984–），男，中国安徽合肥人，本科，工程师，从事工业物联网、工业互联网、工业大数据与计算研究。

2.2 入侵检测与防御系统（IDS/IPS）

入侵检测与防御系统（IDS/IPS）是一种用于检测和防御网络攻击的安全技术。IDS/IPS 通过部署在网络中的传感器，实时采集网络流量、系统日志、用户行为等数据。将采集到的数据与预先定义的攻击特征库进行匹配，判断是否存在攻击行为。通过分析数据间的关联性，发现异常行为，如恶意代码、非法访问等。当检测到攻击行为时，IDS/IPS 会发出警报，并采取相应的防御措施，如阻断攻击源、隔离受感染设备等。IDS/IPS 通过规则库对攻击行为进行识别，具有较强的可扩展性和针对性。除了规则匹配，IDS/IPS 还可以通过分析用户行为和系统行为，发现异常行为。IDS/IPS 可以不断学习网络环境，优化检测规则，提高检测效果。

IDS/IPS 可以实时监测工业网络的流量和设备状态，及时发现异常行为。IDS/IPS 可以记录网络设备的操作日志，便于事后分析和追溯。通过分析检测到的攻击行为，评估工业网络的安全态势。IDS/IPS 可以及时阻断攻击行为，保护工业网络的安全。当检测到设备受到攻击时，IDS/IPS 可以隔离该设备，防止攻击扩散。在遭受攻击时，IDS/IPS 可以为应急响应提供数据支持，提高应对效率。

2.3 加密技术

数据加密是保障工业网络信息安全的重要手段，通过将明文数据转换为只有特定接收者才能解密的密文，从而防止数据被未授权访问或篡改。对称加密算法是指加密和解密使用相同的密钥，如 DES（数据加密标准）、AES（高级加密标准）等。这些算法具有加密速度快、密钥长度短等优点，但在实际应用中，密钥的生成、分发和管理存在一定的困难 [2]。非对称加密算法是指加密和解密使用不同的密钥，如 RSA、ECC（椭圆曲线密码）等。这种算法具有较好的安全性，但加密和解密速度较慢。在实际应用中，通常将非对称加密算法用于密钥交换，而使用对称加密算法进行数据加密。哈希算法用于生成数据的摘要，如 MD5、SHA-1 等。哈希算法具有单向性，即无法从摘要中恢复原始数据。在实际应用中，哈希算法可用于验证数据的完整性和一致性。

在工业网络中，数据传输加密可以保证数据在传输过程中不被窃取、篡改。例如，使用 SSL/TLS 协议进行工业控制系统（ICS）的数据传输加密。存储加密可以保护工业网络中的数据存储安全，防止数据泄露。例如，使用 AES 加密算法对工业设备中的数据进行加密存储。通过非对称加密算法实现身份认证，确保只有授权用户才能访问工业网络中的资源。如：使用 RSA 算法进行数字签名，验证用户身份。加密技术可以用于实现访问控制，确保只有授权用户才能访问特定资源。例如，使用对称加密算法对用户密码进行加密存储，并进行加密验证。

2.4 身份认证与访问控制

在工业网络中，身份认证是确保数据安全和系统稳定运行的重要环节。用户通过输入预设的用户名和密码来证明自己的身份。这种方式简单易用，但安全性较低，易被破解。用户使用数字证书来证明自己的身份，数字证书由可信的第三方颁发。这种方式具有较高的安全性，但需要用户事先拥有数字证书 [3]。用户需要同时提供两种不同的身份验证方式，如用户名和密码、短信验证码、指纹识别等。这种方式可以有效提高安全性。通过人脸识别、指纹识别、虹膜识别等生物特征来验证用户身份。这种方式具有较高的安全性，但成本较高。基于角色的访问控制（RBAC）根据用户在组织中的角色，为其分配相应的权限。

访问控制策略是确保工业网络安全的关键，用户只能访问完成其工作所需的最低权限资源。根据用户职责和任务，为用户分配最小权限。访问控制列表（ACL）对网络资源进行访问控制，限制用户对资源的访问。通过隔离不同安全级别的网络，防止攻击者横向移动。定期对网络进行安全审计，确保访问控制策略得到有效执行。

3 工业网络面临的安全挑战

3.1 工业网络的开放性和互联性带来的风险

工业网络开放性使得数据传输更加便捷，但同时也增加了数据泄露的风险。一旦数据泄露，可能导致企业信息、商业机密泄露，甚至引发产业链的连锁反应。工业网络的互联性使得攻击者更容易通过网络入侵控制系统，对工业生产造成破坏。此外，攻击者还可能通过入侵工业网络，控制关键设备，引发安全事故 [4]。工业网络与互联网的互联互通，使得攻击者可以轻松跨越不同领域进行攻击，如针对政府、金融等关键基础设施的攻击。

3.2 工业控制系统的漏洞和脆弱性

工业控制系统普遍存在软件漏洞，攻击者可以利用这些漏洞进行攻击，如缓冲区溢出、SQL 注入等。部分工业控制系统硬件存在设计缺陷，如 CPU、内存等硬件组件可能存在安全风险。随着工业控制系统使用年限的增长，系统逐渐老化，安全防护能力下降，容易成为攻击目标。

3.3 针对工业网络的攻击手段和趋势

攻击者通过恶意软件入侵工业网络，实现对关键设备的控制。如勒索软件、木马等。攻击者通过发送钓鱼邮件，诱导工业网络用户泄露账号密码，进而入侵控制系统。攻击者利用恶意代码对工业控制系统进行攻击，如 SQL 注入、缓冲区溢出等。攻击者利用尚未公开的漏洞进行攻击，对工业网络造成严重威胁。随着工业物联网的普及，攻击者可能针对 IIoT 设备进行攻击，如入侵摄像头、传感器等。

4 工业网络安全解决方案

4.1 网络隔离

网络隔离是指在工业控制系统中，将内部网络与外部网络进行物理或逻辑上的隔离，以防止外部网络对内部网络的非法访问和攻击，确保工业控制系统安全稳定运行。物理隔离通过物理手段将内部网络与外部网络进行分离，例如使

用独立的交换机、路由器等设备，实现物理隔离。逻辑隔离通过配置防火墙、安全策略等手段，在逻辑上对内外网进行隔离，例如设置访问控制列表（ACL）、端口过滤等[5]。隔离设备使用专门的隔离设备，如安全网关、安全隔离网闸等，实现内外网的物理和逻辑隔离。安全协议采用安全的通信协议，如 SSL/TLS 等，确保数据传输过程中的安全。

根据企业实际情况，确定网络隔离的具体需求和目标。据需求，设计合理的网络隔离方案，包括物理隔离、逻辑隔离、隔离设备等。按照设计方案，实施网络隔离，包括配置防火墙、安全策略、隔离设备等。对网络隔离效果进行监控，确保隔离效果达到预期目标。同时，定期对隔离设备进行维护和升级，以应对新的安全威胁。

4.2 访问控制

用户身份验证通过用户名、密码、指纹、RFID 卡等手段，确保用户身份的真实性。访问权限管理根据用户角色、岗位和职责，设定不同级别的访问权限。终端设备管理对终端设备进行安全配置，确保其符合安全标准。部署防火墙，限制内外部网络流量，防止恶意攻击。VPN 技术为远程用户建立安全的连接通道，确保数据传输安全。建立完善的用户管理体系，包括用户注册、权限分配、角色管理等。根据企业实际情况，制定针对性的访问控制策略。通过技术手段，如防火墙、入侵检测系统、访问控制列表等，实现访问控制。根据企业业务发展和安全需求，定期审查和更新访问控制策略。提高员工对访问控制重要性的认识，确保访问控制措施得到有效执行。

4.3 数据加密

数据加密是指利用特定的算法和密钥，将原始数据转换成无法直接识别的密文，只有具备相应解密密钥的用户才能还原出原始数据。数据加密可以有效防止数据在传输和存储过程中被非法访问、窃取或篡改，保障工业信息安全。在工控系统中，数据加密可以确保控制指令、传感器数据等在传输过程中的安全性，防止恶意攻击者篡改或窃取数据。在工业互联网平台中，数据加密可以保护用户数据、设备数据等在存储过程中的安全性，防止数据泄露。数据加密可以确保远程访问和数据共享过程中的安全性，防止数据在传输过程中被非法访问。根据实际需求选择合适的加密算法，确保加密效果和性能。建立健全的密钥管理系统，确保密钥的安全生成、存储、分发和更新。制定合理的加密策略，确保数据在传输和存储过程中的安全性。定期进行安全审计，检查加密系统的有效性和安全性。

4.4 安全审计

日志审计通过分析系统日志，记录用户行为、设备行为、网络流量等，实现对系统安全状况的实时监控。事件审计记录系统中发生的安全事件，如登录失败、非法访问等，分析事件原因，采取相应措施。数据库审计对数据库进行安全审计，包括数据访问权限、数据修改、数据删除等操作，确保数据安全。工具审计利用安全审计工具，对系统、应用、数据进行自动化审计，提高审计效率。分析审计结果，识别异常行为，如非法访问、数据泄露等，及时采取措施，防范安全风险。对安全事件进行溯源，查找安全漏洞，完善安全防护措施。根据审计结果，分析安全趋势，预测潜在安全风险，提前做好防范措施。

5 结论

研究网络安全技术与工业网络解决方案具有重要的现实意义。工业网络面临着来自外部和内部的多种网络安全威胁，如网络攻击、数据泄露、恶意软件等。现有的网络安全技术和工业网络解决方案在应对这些威胁方面存在一定的局限性。基于人工智能的工业网络安全防护体系具有较高的防护能力，能够有效应对各种网络安全威胁。在今后的工作中，应继续加强相关技术的研究和开发，为我国工业网络安全保障提供有力支持。

参考文献

[1] 胡震,曹航,于艳.基于流量分析的工控网络安全审计技术研究[J].电子产品世界,2024,31(11):4-7.

[2] 王奇,孙宏,李杜.工业网络安全防护与态势感知技术研究及应用[J].互联网周刊,2024,(15):58-60.

[3] 赵申,陈魏魏,刘振.工业互联网环境下的网络安全技术与挑战分析[J].信息系统工程,2024,(06):133-136.

[4] 童杰,丰存旭.工业控制系统网络安全靶场建设关键技术及解决方案探讨[J].工业信息安全,2023,(06):29-37.

[5] 吴涛,黄健,郭钰璐,等.工业互联网网络安全技术浅析[J].邮电设计技术,2022,(09):9-12.