浅谈电子商务网络信息安全技术的优化

温 娜　高 亮　王淑敏

（中国标准化研究院）

摘　要：随着社会经济的发展，电子商务得到快速发展，但信息窃取、信息篡改与网络攻击也接踵而至，对我国电子商务产业的健康、迅速发展造成了威胁。我国的计算机网络技术体系也在与这些安全威胁的斗争中不断健全，实现了网络信息安全技术模块各个环节的标准化。本文分析了电子商务对信息的安全要求，介绍了几种主要安全威胁，阐述了防火墙、数据加密技术等信息安全技术的具体内容并分析了几种未来的技术优化方向。

关键词：电子商务，网络技术安全，标准化，技术方案

DOI编码：10.3969/j.issn.1674–5698.2024.07.010

Discussion on the Optimization of E-commerce Network Information Security Technology

WEN Na　GAO Liang　WANG Shu-min

（China National Institute of Standardization）

Abstract: With the development of social economy, e-commerce has experienced rapid growth. However, along with it comes the threat of information theft, tampering, and cyber attacks, which pose a threat to the healthy and rapid development of China's e-commerce industry. China's computer network technology system has been continuously improved in its conflict against these threats, achieving standardization in various aspects of network information security technology. This paper analyzes the security requirements of information in e-commerce, introduces several main security threats, elaborates on the specific content of information security technologies such as firewalls and data encryption, and analyzes several future directions for technological optimization.

Keywords: e-commerce, network technology security, standardization, technical proposal

0 引言

计算机网络技术的发展促进了商业和经济模式的变革，电子商务作为一种崭新的商务活动模式，受到全世界、全社会的广泛关注和吸纳[1]。电子商务基于信息资源与实体经济相互结合产生效益的理念，具有普遍性、方便性、安全性以及整体性等特点，可实现广告宣传、网上支付、电子账户

基金项目：本文是国家市场监管总局科研条件专项资金项目“面向多边贸易合作的技贸措施研究能力建设”（一期）（项目编号：[2060503]150019000000210006）研究成果。

作者简介：温娜，高级工程师，博士，研究方向为数据与知识工程相关技术标准化。

高亮，工程师，硕士研究生，研究方向为数据与知识工程相关技术标准化。

王淑敏，助理研究员，硕士研究生，研究领域为知识管理与知识产权标准化。

等功能，甫一出现就为互联网经济的发展注入了强大动力[2]。但同时，电子商务网络信息安全问题也日益凸显，黑客攻击、隐私数据泄露、电信诈骗等网络安全风险带来的威胁不断增加，电子商务的可靠性和安全性正受到威胁[3,4]。要推动当代社会电子商务的可持续发展，保障互联网经济的稳步增长，必须以保障计算机网络安全为基础和前提[5]。

1 电子商务信息安全现状

随着电子商务的发展，构建大型、便捷的电子商务信息安全环境已成为保证我国电子商务产业健康可持续发展的基础要素。明确电子商务信息安全现状有助于帮助研究者们采取更有效的措施解决网络信息安全问题，更高效、更严密地维护电子商务信息安全环境[6]。

1.1 电子商务信息安全主要要求

对电子商务信息安全的保护包括对信息的有效性、机密性、完整性与真实性的要求[5]。

1.1.1 有效性

有效性是电子商务的基础。电子商务是涉及现实的贸易，因此合约、订单的效力直接影响着交易的正常进行，参与经济交易的双方主体未经对方同意都不能违反约定。

1.1.2 机密性

机密性是电子商务的前提。电子商务过程中，应严格保证交易各方在交易中提供的相关信息保密，即便经济交易的双方在履约过程中出现任何纠纷，也能够得到有效的解决和合理的仲裁。

1.1.3 完整性

完整性是电子商务正常进行的保障。在电子商务双方确认贸易内容后，需要确保订单、合约等信息的完整性，保证交易双方基本信息无误及交易的正常进行。

1.1.4 真实性

真实性是电子商务与现实的关键连接点。电子商务贸易双方通过互联网以电子订单的方式达成交易，但交易货物往往具备现实实体，交易资金也具备现实购买力。因此，电子商务更需要对交易双方的现实身份进行确认，保证交易对象真实存在且具备完成交易的现实能力。

1.2 电子商务面临的主要安全问题

电子商务的信息安全面临着诸多安全问题，主要包括信息的窃取、信息的篡改、假冒与恶意破坏[7]。

1.2.1 信息的窃取

电子商务主要通过互联网平台进行信息的传递，各种交易活动也是在互联网的平台上完成，交易信息对用户来说属于商业机密，但当企业的信息数据安全工作准备不足时，很容易在信息传递、信息存储等路径上遭遇不法分子的非法信息窃取[8]。

这一过程中，信息的机密性将遭受破坏，交易双方也会因此遭受财产损失，可能造成社会对电子商务的信任危机。同时，被窃取盗取的信息数据可能被用于施行威胁度更高的其他信息安全破坏行为，对用户财产安全与信用造成更严重的破坏。

1.2.2 信息的篡改

信息的篡改是在信息窃取基础上更加恶劣的信息安全破坏行为。入侵者通过信息窃取等行为掌握信息传递规律后，可能从3个方面对数据信息进行篡改。

（1）利用某些技术手段改变数据流的次序，实现对信息的篡改；

（2）将某些数据直接删除，破坏信息的完整性；

（3）在数据流中根据破解获得的规律增加某些信息，导致交易内容或形式发生变化。

信息篡改在信息窃取的基础上，进一步破坏了信息的有效性与完整性，可能对交易双方均造成财产与信用损失，对电子商务参与者间的信任网络造成损害[9]。

1.2.3 假冒

假冒也是一种以信息窃取为基础的信息安全破坏行为，其危害尤甚于窃取和篡改信息。假冒是指入侵者通过窃取掌握信息数据及其格式、规律，冒名合法用户传输伪造信息或截取重要信息，容易造成交易对方出现错误判断和经济损失[10]。

不法分子会利用漏洞、木马病毒、间谍软件等

手段篡取合法用户的注册地址等关键安全信息，并假托他人信息注册或盗取账号进行互联网交易，借此牟利，主要表现在：冒充注册、冒充他人账号消费、栽赃或超前消费；冒充注册域名原主机、原用户账号进行信息欺诈等恶劣的非法行为。

假冒行为不仅造成了受害者的经济损失、破坏了电子商务发展所必需的真实可靠的贸易环境，更破坏了整个互联网的信任环境，对电子商务的发展乃至互联网的发展进程都将造成极其恶劣的影响。

1.2.4 恶意破坏

电子商务在计算机网络技术环境下进行贸易交流时，部分不法分子能够通过网络中的安全漏洞入侵私人计算机，窃取重要的用户信息或有针对性地对计算机进行攻击，让计算机陷入瘫痪等无法使用的状态，实施一系列的破坏行动[10]。

此外，不法分子也会对规模较大的电子商务平台进行针对性的攻击，让平台陷入瘫痪状态，趁机实施进一步的各种破坏行为，例如：分布式拒绝服务攻击、SQL注入攻击、跨站脚本攻击等。也有不法分子使用这种攻击手段劫持平台并敲诈勒索平台运营方，扰乱平台运营秩序和电子商务贸易秩序。

这两种恶意破坏行为均利用了计算机网络技术环境自身的潜在问题或不足，对电子商务的参与者和运营者造成了经济损失与信用损害。

2 电子商务信息安全技术与优化

安全性是保障电子商务长期发展的关键问题，也是利用互联网进行交易的根本，为了保证有效性等主要信息安全得到充分保护，防火墙、信息加密、数字签名等信息安全技术相继出现，承担起从纷繁复杂的安全威胁中保障电子商务信息安全的使命[7,11]。

2.1 防火墙技术

防火墙是两个信任程度不同的网络之间的软件或硬件设备的组合，对网络之间的通信进行控制。防火墙的主要工作是对网络与外界交换的流量进行监控，主要任务是抵御不被信任的网络数据可能的威胁，隔离网络内可能具有威胁的异常数据，准入安全可信任的数据信息。防火墙会根据是否具备授权资格决定是否允许该用户或信息在本网络中进行流通和共享，可以阻止不法分子的非法访问行为，将病毒和木马排除在网络外，防止网络内部重要的信息数据被篡改、破坏或窃取[12]。

防火墙技术的应用应注意两点，（1）防火墙也存在一定的弊端，若防火墙的数据更新出现太大的延迟，防火墙的实时服务请求就会难以实现，可能影响网络的正常工作。（2）由于工作站是病毒入侵网络的一个主要途径，所以要将防火墙装置安装在工作站上，做到信息数据的安全防护工作[8]。

目前，对防火墙的优化方向一方面是网络通信与访问控制模块的优化，以实现对合法用户与非法入侵者更准确更迅速的辨别为目标；另一方面是针对当前防火墙技术无法对数据驱动型攻击做出有效应对，因此需要在局域网内部架设新型防火墙，克服目前的安全缺陷。

2.2 信息加密技术

加密技术主要对电子商务信息的传递过程进行保护。在信息传递前后，分别通过加密解密算法对信息明文和密文处理，防止不法分子窃取传输中的信息数据，实现数据传输过程中的信息安全保护。

目前的密钥加密技术主要分为对称密钥加密技术与非对称密钥加密技术，前者又称私钥加密，在加密阶段与解密阶段使用相同密钥，例如：DES加密算法等，具有时空复杂度低，运行效率高等优势，但密钥传递困难；后者也被称为公钥加密，在加密与解密阶段使用不同的密钥，这两种不同的密钥需要同时使用，并明确二者之间的配对关系，例如：RSA加密算法，传递保密功能更优但时空复杂度较高且对大容量信息加载速度较慢[13]。实际应用中常将两种加密手段混合使用并根据数据保密等级决定加密方式。

2.3 信息识别技术

信息识别技术是指身份认证技术与数字签名技术的交叉使用。数字签名是数字文档上附加的一段特殊数据，用于确保文档的来源安全、内容完整有效、未遭篡改。数字签名需要传输前后双方均

使用摘要算法提取特征摘要，传输方特征摘要使用公钥加密后传输，接收方特征摘要将被用于与接收、解密后的传输方摘要对比，若一致则说明传输过程安全。身份认证是通过验证用户提供的身份信息与其所宣称的身份的一致性确保用户身份真实。身份认证需要用户在注册、身份验证阶段提供姓名、手机号码、身份证号等真实身份信息和相关证明材料，以便在必要情况下通过社会身份信息与生物身份信息对用户身份进行验真，防止假冒等信息安全破坏行为[3,8]。

上述两种技术可以有效保护数据的有效性、私密性与完整性，但现阶段这两种技术都对数据中心依赖度较高，这导致数据中心可能成为不法分子的重点攻击对象，反而不利于信息安全的保护。目前，很多研究都侧重于探索基于区块链、去中心化标识等技术的信息识别技术，以期实现建立去中心化的信任模式。

2.4 入侵检测系统技术

入侵检测系统与防火墙相同，是一种防护性技术，通过采集和分析用户的网络行为数据以及关键节点信息来监测异常数据与入侵行为并及时采取措施，发出警报或直接采取措施阻止不法分子的入侵活动。

如今入侵检测系统技术存在漏报与误报、无法识别新型攻击模式、难以处理数据量过大的复杂网络信息等问题。目前，针对入侵检测系统上述问题，研究者们提出了很多优化方向，例如：引入人工智能技术与机械学习算法，通过训练模型尽可能地规避漏报与误报；引入行为分析技术和上下文感知技术，对流量与用户行为进行深度分析，以期提高检测的精准度与效率；综合多种入侵检测系统，全方面多层次地进行分析与检测；引入实时响应和自动化技术，减轻管理员工作负担等研究方向[14]。

3 结语

电子商务极大地提高了交易的简便性与效率，为我国互联网经济的发展注入了强大动力，是我国迈入大数据时代后不可或缺的强力经济增长点之一。正因此，积极改进和优化防火墙技术、数据加密技术等信息安全技术对于维护电子商务贸易的安全，保护用户对电子商务行为的信任，维持稳定的电子商务贸易秩序具有不可或缺的重要意义，应当得到相关领域研究者的关注与重视。

参考文献

[1] 陆元婷. 大数据时代电子商务安全问题研究[J]. 现代国企研究, 2017(14):97+99.

[2] 胡晓超. 电子商务网络信息安全技术的研究[J]. 计算机光盘软件与应用, 2014, 17(13):180+182.

[3] 陈鸣钟. 电子商务中网络安全问题的探讨[J]. 内江科技, 2020, 41(01):98–99.

[4] 李悦,卢彪. 网络安全技术在电子商务中的应用[J]. 无线互联科技, 2016(18):134–136.

[5] 吴文杰. 电子商务中网络安全问题的探讨[J]. 科技风, 2022(21):53–55.

[6] 吴蕾蕾. 电子商务信息安全现状分析与对策[J]. 经济师, 2022(06):234–236.

[7] 尚荣斌. 电子商务网络信息安全技术应用浅析[J]. 科技信息, 2011(12):618.

[8] 杨巍. 谈电子商务中的网络安全管理问题[J]. 网络安全技术与应用, 2015(07):37–38.

[9] 徐卫红,刘婷. 网络安全对电子商务发展的影响和策略[J]. 成功(教育), 2010(03):274.

[10] 段敬周. 计算机网络安全技术在电子商务中的应用[J]. 中外企业家, 2019(01):53.

[11] 杨颖. 电子商务安全问题分析[J]. 中国科技信息, 2005(20):53.

[12] 郝玉洁,常征. 网络安全与防火墙技术[J]. 电子科技大学学报(社科版), 2002(01):5–7.

[13] 王玲. 网络信息安全的数据加密技术[J]. 信息安全与通信保密, 2007(04):64–65+68.

[14] 胡华平, 陈海涛, 黄辰林, 等. 入侵检测系统研究现状及发展趋势[J]. 计算机工程与科学, 2001(02):20–25.