从保密性与完整性角度探讨网络安全的实现困境

叶焕发

摘 要：

本文分析了网络安全难以实现的原因，尤其是从信息系统的保密性与完整性两个核心方面展开讨论。随着信息技术的不断发展，网络安全问题日益复杂化，保密性和完整性作为信息系统安全的基础，面临着巨大的挑战。保密性保障信息不被未经授权的访问，但复杂的加密技术和密钥管理容易导致操作上的困难和系统性能下降；完整性则确保数据的准确性和一致性，但在面对复杂的攻击手段时，现有的技术手段有时只能检测篡改，无法彻底防止数据的损坏。两者的局限性使得网络安全体系的构建充满了挑战。此外，随着网络威胁的不断演变，传统的安全防护机制难以应对新型攻击，企业和组织需要综合考虑多层次的防护策略。本文通过分析信息系统中保密性与完整性机制的不足，探讨了当前网络安全难以实现的根本原因，并为未来可能的解决方案提供参考。

关键词：网络安全；信息系统；保密性与完整性；

引言

在当今数字化和信息化迅速发展的时代，网络安全已成为全球范围内的重要议题。随着互联网和信息技术的广泛应用，信息系统在各类组织的管理、决策和运营中扮演着核心角色。然而，网络安全威胁也随之增加，且日益复杂和多样化，对信息系统的保密性和完整性构成了严重的挑战[1]。保密性与完整性是信息系统安全的两个基本维度，确保了系统中的数据在传输、存储和处理过程中不被未经授权的访问或篡改。然而，尽管技术不断进步，实现网络安全依然充满了困难和挑战。首先，保密性是指信息系统中敏感数据不被未经授权的人员或系统访问。为了确保保密性，通常采用加密技术、访问控制和身份验证等手段。然而，随着攻击技术的不断演化，即使使用了高级加密技术，密钥管理依然存在巨大挑战。密钥的丢失、泄露或管理不当都会使加密系统失效，进而导致敏感数据的泄露。此外，随着数据流量的增加和网络复杂性的提升，加密操作可能会对系统性能带来显著影响，降低用户体验和处理效率。因此，尽管保密性对于保障网络安全至关重要，但其实际实施中面临着技术和操作层面的诸多困境。

其次，完整性则是指确保信息在传输、存储和处理的整个过程中保持其原始状态，防止被篡改或损坏。完整性机制通过哈希函数、数字签名和数据校验等手段来验证数据是否发生改变。然而，尽管这些技术能够有效检测到数据被篡改的行为，它们在应对复杂的攻击时却显得力不从心。现有的完整性保护技术主要是被动的，即只能在数据遭到篡改后进行检测，而无法在攻击发生时主动阻止篡改行为。因此，信息系统的完整性保护在面对恶意攻击和数据篡改时具有一定的局限性。

综合来看，信息系统的保密性与完整性是确保网络安全的基础，但这两个方面各自的局限性，以及面对不断演变的网络威胁，使得网络安全的实现依然充满了困难和挑战。如何在保障保密性和完整性的前提下应对复杂的攻击，构建更加稳健的安全体系，已成为当前网络安全研究的关键问题[2]。本文将从保密性与完整性保护机制的角度出发，分析当前网络安全难以实现的根本原因，探讨未来可能的防护策略。

1 保密性与完整性面临的挑战

1.1 信息系统保密性的概念与挑战

信息系统的保密性是指确保系统内的敏感数据不会被未经授权的用户或系统访问、读取或泄露。保密性是信息安全的核心原则之一，旨在通过加密、访问控制、身份验证等手段保护数据的隐私性和机密性。然而，随着信息系统复杂性的增加和网络威胁的多样化，保密性面临着诸多挑战[3]。首先，密钥管理是一个常见的问题，密钥的泄露、丢失或管理不当会使加密技术失效，导致敏感数据暴露于风险之中。其次，随着网络流量的增加和系统规模的扩展，加密

操作可能会对系统性能产生负面影响，增加处理时间和资源消耗。此外，内部人员的安全隐患也是保密性面临的挑战之一，内部威胁往往难以通过常规的外部安全机制进行防范。因此，尽管保密性技术在不断进步，保障信息系统中的数据机密性仍然是一项复杂且具有挑战性的任务。

1.2 信息系统完整性的概念与局限性

信息系统的完整性是指确保数据在传输、存储和处理的过程中保持准确、一致且未经篡改。它的核心目标是防止数据的损坏、丢失或被未经授权的修改，从而保证系统能够依赖这些数据做出正确的决策[4]。常见的完整性保护手段包括哈希函数、数字签名和数据校验等技术，通过这些机制可以检测出数据是否发生了异常变化。然而，信息系统的完整性也存在局限性。首先，完整性保护通常是被动的，虽然能够检测到数据被篡改，但无法主动阻止攻击行为的发生。其次，完整性保护手段在面对高级持续性威胁和零日攻击等复杂攻击时可能显得力不从心。此外，维护数据的一致性和完整性通常伴随着较高的计算成本，尤其在处理大量数据时，系统的资源消耗和性能下降也是不得不面对的难题。因此，虽然完整性在信息系统中至关重要，但其局限性使得实现全面的数据保护仍面临许多挑战。

1.3 网络威胁演变对保密性与完整性的影响

随着网络威胁的不断演变，信息系统的保密性和完整性面临的挑战也日益加剧。首先，在保密性方面，传统的加密技术虽然能有效防止数据泄露，但随着量子计算和更高级攻击方法的出现，现有的加密算法面临被破解的风险，密钥管理的复杂性也进一步加大。其次，随着信息系统的开放性和复杂性增加，内部威胁和人为失误也成为保密性难以控制的因素[5]。完整性方面，新型网络攻击能够在不被立即检测的情况下篡改数据，现有的检测机制通常只能事后发现篡改行为，而无法提前预防。此外，物联网和云计算的广泛应用，导致系统的边界模糊化，增加了确保数据完整性的一致性和管理复杂度。因此，网络威胁的演变给信息系统的保密性和完整性带来了前所未有的挑战，使得这些领域的防护机制亟需升级和创新。

2 保密性与完整性保护机制的现状与不足

2.1 常见的保护机制及其优缺点

常见的保密性和完整性保护机制包括加密技术、访问控制、身份验证、哈希函数和数字签名等。这些机制在信息系统安全中起到了关键作用，但也各有优缺点。加密技术是最常见的保密性保护手段，通过将数据转化为不可读的格式，防止未经授权的访问。其优点在于能够有效保护数据机密性，特别是在传输过程中，但缺点是密钥管理复杂，且加密过程会影响系统性能。访问控制和身份验证则通过限制和确认用户身份，确保只有合法用户能够访问系统资源，它们的优点是提供了精细的权限管理，但在实施和管理上较为复杂，且面对内部人员威胁时难以完全防护。哈希函数和数字签名用于完整性保护，确保数据在传输和存储过程中未被篡改，它们的优点是计算简单、效率高，能快速检测到数据异常，缺点是只能在事后检测，无法预防篡改行为。此外，这些机制在应对新型高级持续性威胁时往往显得不足，现有的技术手段难以完全阻挡复杂的攻击。因此，虽然这些保护机制在保密性和完整性保障中起到重要作用，但也面临性能、管理和应对新威胁的局限性。

2.2 保密性与完整性协同保护的必要性

保密性与完整性协同保护在信息系统安全中具有极其重要的必要性，因为单一的保密性或完整性保护无法充分应对复杂的安全威胁。保密性侧重于防止未经授权的人员或系统访问敏感数据，确保数据的私密性；而完整性则确保数据在传输、存储和处理过程中保持准确和未被篡改。这两者在信息安全中相辅相成，缺一不可。如果只注重保密性而忽视完整性，即使数据未被泄露，也可能因篡改导致数据失真，影响系统的决策与操作[6]。反之，如果只保护完整性而忽视保密性，虽然数据准确，但仍可能被未经授权的人读取，导致信息泄露。因此，协同保护能够更全面地抵御内部和外部的安全威胁。现代信息系统面临的攻击手段日趋复杂化，攻击者不仅试图窃取数据，还可能篡改或破坏系统中的数据，以达到更隐蔽或严重的目的。因此，通过保密性与完整性的协同保护，可以同时防止数据被未经授权的访问和篡改，确保系统的安全性、可靠性与可信度。这种多层次的保护机制不仅能够提高系统的整体安全性，还能够为组织在应对不断演变的威胁时提供更为稳固的防线。

2.3 现有技术如何应对新型威胁

现有的保密性与完整性技术在应对新型威胁方面，虽具备一定的防护能力，但面临诸多挑战。传统的加密技术、访问控制、身份验证和哈希函数等在防范已知的攻击模式上表现良好，能够有效地保护数据的保密性和完整性。对于保密性而言，现有的加密算法如 RSA 和 AES 在面对量子计算时，存在被破解的风险，密钥管理也变得更加复杂。此外，随着数据流量的增长和网络规模的扩大，加密操作可能带来更高的性能开销，影响系统的响应速度和处理效率。完整性保护方面，现有的哈希函数和数字签名技术虽然能够检测到数据篡改，但通常属于事后检测，无法提前预防攻击。新型攻击往往具备极强的隐蔽性和持久性，使得传统的防护技术难以及时发现和应对[7]。此外，物联网和云计算的普及使得信息系统的边界愈加模糊，数据流动性增加，给现有的保护机制带来了额外的复杂性。为应对这些新型威胁，现有技术正在逐步升级，例如引入量子加密、区块链技术和人工智能驱动的威胁检测机制。这些新兴技术能够提高保密性与完整性保护的效果，帮助系统更好地适应不断变化的攻击态势。然而，技术的迅速发展与威胁的复杂性相伴而生，现有技术仍需不断创新与优化，以应对日益严峻的网络安全挑战。

3 网络安全难以实现的根本原因分析

3.1 保密性与完整性技术的局限性

保密性与完整性技术在信息系统安全中的应用至关重要，但它们也存在明显的局限性。首先，保密性技术主要依赖于加密、访问控制和身份验证等手段来防止未经授权的访问，但这些技术面临多方面的挑战。加密技术虽然可以保护数据的机密性，但在面对复杂攻击如量子计算时可能会被轻易破解。此外，密钥管理是保密性技术的一个薄弱环节，密钥的丢失、泄露或管理不当都会导致整个系统的安全性失效。加密技术还会对系统性能产生显著影响，尤其是在大数据和高流量的环境中，可能会导致数据处理速度下降，增加处理延迟。这些技术主要是被动防御，即只能在数据被篡改后进行检测，无法主动阻止攻击行为。此外，完整性保护还依赖于多层次的系统管理和维护，任何一环节的疏漏都可能导致数据一致性被破坏，影响系统的正常运行。总体而言，虽然保密性与完整性技术在信息系统安全中起到关键作用，但它们各自的局限性限制了其在应对日益复杂的网络安全威胁中的有效性。因此，需要结合多种技术手段，并不断创新与优化这些保护机制，才能更好地提升信息系统的整体安全性。

3.2 网络环境的复杂性

随着互联网和信息技术的迅速发展，网络环境的复杂性不断增加，对信息系统的保密性与完整性带来了巨大的挑战。首先，现代网络架构日益复杂，尤其是云计算、物联网、大数据等技术的广泛应用，导致信息系统的边界变得模糊，数据流动性增加。这种复杂性使得传统的安全防护机制难以适应，例如在分布式网络和多云环境中，数据的存储和传输路径更加分散，网络节点增多，增加了数据泄露和篡改的风险。其次，网络环境中参与者的多样性进一步加剧了安全问题，不同的用户、设备和应用程序之间的互动频繁，内部人员或系统设备的失误、违规操作也可能导致严重的安全事件，难以通过单一的保密性或完整性机制来完全防护。随着攻击手段的不断演化，攻击者利用复杂的网络架构和跨境的数据传输来发起多层次、多步骤的攻击，使得信息系统很难及时识别和应对这些隐蔽而复杂的攻击[8]。此外，网络的全球化进一步加剧了网络环境的复杂性，跨国界的数据流动使得法律和法规的实施变得困难，各国在网络安全方面的政策和标准不尽相同，这给保密性与完整性保护带来了更多的挑战。总体而言，网络环境的复杂性不仅增加了信息系统管理的难度，还要求安全防护技术在灵活性、适应性和跨领域合作方面进行提升，以有效应对不断变化的安全威胁。

3.3 新兴威胁的快速发展

新兴威胁的快速发展对信息系统的保密性与完整性提出了前所未有的挑战。随着技术的进步，攻击手段变得更加复杂和难以预见，APT 攻击具有高度隐蔽性，能够长期潜伏在系统中，逐步获取敏感数据而不被察觉；零日攻击则利用尚未被发现或修复的漏洞进行入侵，使得传统的防护机制如防火墙、杀毒软件难以有效应对[9]。此外，勒索软件通过加密数据或锁定系统来勒索赎金，直接威胁系统的保密性和完整性，且这类攻击的规模和频率在全球范围内呈现上升趋势。物联网、云计算和 5G 技术的普及进一步推动了新兴威胁的发展。物联网设备数量庞大且安全标准不统一，成为黑客攻击的潜在目标；云计算环境下的数据分布式存储和共享，增加了数据泄露与篡改的风险；5G 网络带来更高的带宽和更快的连接速度，也为攻击者提供了更广泛的入侵途径。此外，量子计算的发展对现有的加密技术构成了潜在威胁，许多现行的加密算法在面对量子计算能力时可能失效，这意味着传统的保密性技术面临被彻底破解的风险。面对这些新兴威胁，现有的防护机制往往显得力不从心，难以提供足够的安全保障。因此，为了应对新型攻

击，信息系统需要不断升级和创新保密性与完整性技术，结合人工智能、区块链等新兴技术，增强系统的主动防御能力和威胁感知能力，从而提高整体的网络安全水平。

4 结语

综上所述，信息系统的保密性与完整性在保障网络安全中起到了至关重要的作用，但在面对日益复杂的网络环境和新兴威胁时，现有的技术手段存在诸多局限性。保密性保护虽然能够有效防止未经授权的访问，但密钥管理的复杂性以及加密技术在量子计算等新兴技术面前的脆弱性，给系统安全带来了巨大挑战[10]。与此同时，完整性保护机制虽然能够检测数据的篡改行为，但多为事后发现，缺乏主动防御能力。随着物联网、云计算、5G 等技术的发展，信息系统的边界愈加模糊，数据传输和存储变得更加复杂，增加了数据泄露和篡改的风险。因此，为应对这些挑战，信息系统需要更为全面的防护策略，协同应用保密性与完整性技术，同时借助人工智能、区块链等新兴技术，实现主动防御与实时监控，以有效应对未来的网络安全威胁，提升整体的安全水平。

参考文献

[1] 李选超.基于计算机信息系统的保密技术及安全管理研究[J].电子元器件与信息技术,2021,5(12):237-238.DOI:10.19772/j.cnki.2096-4455.2021.12.106.

[2] 徐金春.坚决消除政务信息系统保密管理“盲区”——浙江省开展“浙政钉”保密管理的实践与探索[J].保密工作,2024(07):39-41.DOI:10.19407/j.cnki.cn11-2785/d.2024.07.002.

[3] 瞿勇.计算机信息系统的保密技术及安全管理研究[J].数字通信世界,2021(06):161-162.

[4] 周晓辉.计算机信息系统的保密技术及安全管理阐述[J].电子技术与软件工程,2021(05):259-260.

[5] 熊宇宸.基于 DES 数据加密算法的计算机信息系统保密技术[J].信息与电脑(理论版),2021,33(17):60-62.

[6] 本刊记者.切实加强涉密信息系统运行维护委托服务管理——国家保密局有关部门负责同志答记者问[J].保密工作,2021(02):9-11.DOI:10.19407/j.cnki.cn11-2785/d.2021.02.005.

[7] 钟纪业,杨鹏.军事信息系统安全保密“四要”[J].保密科学技术,2020(06):68-69.

[8] 林海军.计算机信息系统保密技术及防范管理分析[J].数字通信世界,2020(04):140-141.

[9] 王玲玲,张倩.计算机信息系统的保密技术及安全管理研究[J].科技风,2020(06):122.DOI:10.19392/j.cnki.1671-7341.202006110.

[10] 俞虓.政府机关网络信息系统安全保密管理[J].电脑知识与技术,2019,15(11):67-68.DOI:10.14004/j.cnki.ckt.2019.1101.