Never Trust, Verify Every Transfer: A Zero Trust Perspective on CDS*

Yujin Kim[1] and Jungsoo Park[1]

Kangnam University, Yongin, Republic of Korea
darly@kangnam.ac.kr, jspark@kangnam.ac.kr

Abstract

Network separation protects sensitive data, but efficiency needs have driven the use of Transfer Cross Domain Solutions (CDS). The existing CDS depend on static rules and implicit trust, leaving them exposed to insider and malware threats. This paper proposes a Zero Trust-based Transfer CDS using a Device Agent/Gateway model that verifies users and devices and enforces dynamic boundary policies for secure, auditable data exchange.

Keywords: Cross Domain Solution, Transfer CDS, Zero Trust, Secure Information Exchange

1 Introduction

Network separation has been vital in national cybersecurity, isolating internal systems from external networks to block threats such as malware and data leakage. Its main goal is to protect sensitive data by physically or logically preventing illegal access from the internet. However, with growing demands for both efficiency and security, network interconnection technologies have enabled limited but secure data exchange between networks, highlighting the need for Cross Domain Solutions (CDS) to ensure safe information transfer across domains.

2 Background

CDS enable secure information exchange across distinct security domains and are categorized into Access, Transfer, and Multi-Level CDS. This study focuses on Transfer CDS[1], which controls data transmission between domains and ensures secure transfer in network-separated environments. Existing Transfer CDS, particularly Guard systems, mainly rely on static rule-based filtering and implicit trust, which are inadequate against insider threats and polymorphic malware. To overcome these limitations, we propose the integration of the Zero Trust model, which emphasizes continuous verification of users, devices, and data, along with the principle of least privilege.

The Zero Trust model follows the principle of "Never Trust, Always Verify." Unlike perimeter-based security, it continuously verifies all entities and enforces dynamic policies based on location, device posture, and data sensitivity.

3 Proposed Architecture

This study proposes a Device Agent/Gateway-based model[2] to implement Zero Trust principles within the Transfer CDS. In this model, a Device Agent on user endpoints verifies user

[*] Proceedings of the 9th International Conference on Mobile Internet Security (MobiSec'25), Article No. P-36, December 16-18, 2025, Sapporo, Japan.

and device identities and collaborates with the Policy Decision Point (PDP) to assess transfer requests. Data transmission is performed through a Gateway (Policy Enforcement Point, PEP) located at the security boundary. The Transfer CDS connects two distinct security domains with a single data transmission path. The Gateway communicates in real time with the Policy Administrator (PA) to allow only approved communication paths, serving as the control point for access and transfer requests. The PDP integrates results from Content Disarm and Reconstruction (CDR) and Data Loss Prevention (DLP) modules with user and device attributes to make policy decisions. This architecture ensures consistent policies, centralized control, and real-time enforcement throughout data transmission.

The proposed model operates as follows. When a user initiates a transfer, the Device Agent and PDP verify identity and device security through MFA and posture checks, blocking untrusted requests. The file is inspected using CDR and DLP. CDR removes malicious elements, and DLP detects sensitive data leakage. Based on these results, the PDP decides to allow or deny the transfer and sends its decision to the PEP. The Gateway allows only authorized paths and blocks abnormal sessions. All results are logged, and approved data is encrypted and signed to ensure integrity and confidentiality. Continuous monitoring and audit logging maintain post-transfer security and data trustworthiness.

4 Conclusion

Consequently, this architecture achieves comprehensive security beyond the simple allowance of information transfer with the Device Agent/Gateway-based model. It is expected that this will compensate for the limitations of static rule-based mechanisms in existing Transfer CDS and, by integrating with the Zero Trust security model, enable secure and flexible information transfer.

Acknowledgement

This work was supported by the IITP (Institute of Information & Communications Technology Planning & Evaluation) - ITRC (Information Technology Research Center) grant funded by the Korea government (Ministry of Science and ICT) (IITP-2025-RS-2020-II201602).

References

[1] V. Sundaravarathan et al., *"Cross-Domain Solutions (CDS): A Comprehensive Survey,"* IEEE Access, vol. 12, pp. 163551–163620, 2024. doi: 10.1109/ACCESS.2024.3483659.

[2] S. Rose et al., *Zero Trust Architecture,* NIST Special Publication 800-207, National Institute of Standards and Technology, Gaithersburg, MD, USA, Aug. 2020. Available: https://doi.org/10.6028/NIST.SP.800-207