

Dear Members of the Selection Committee,

I am pleased to nominate the paper "TZ-DATASHIELD: Automated Data Protection for Embedded Systems via Data-Flow-Based Compartmentalization" (NDSS 2025) for the Best Scientific Cybersecurity Paper Competition. This paper makes a significant and timely contribution to foundational cybersecurity research by addressing a critical challenge in modern embedded and trusted execution environments: enforcing strong data protection guarantees in complex, real-world systems.

Embedded systems increasingly rely on trusted execution environments (TEEs), such as ARM TrustZone, to isolate sensitive computations from potentially compromised software stacks. However, in practice, developers face substantial difficulty in correctly partitioning data and enforcing least-privilege access across secure and non-secure domains. Manual compartmentalization is error-prone, brittle, and often leads to overprivileged or incorrectly protected data flows, weakening the intended security guarantees of TEEs.

This paper directly addresses this fundamental problem by introducing TZ-DATASHIELD, an automated data protection framework based on precise data-flow analysis and systematic compartmentalization. The key insight of the work is to treat data protection not as a manual annotation problem, but as a principled data-flow enforcement problem that can be inferred and synthesized automatically from program behavior.

TZ-DATASHIELD constructs a fine-grained model of how data propagates through embedded system software and uses this model to automatically derive compartmentalization policies that enforce strict separation between secure and non-secure worlds. By grounding security decisions in observed and inferred data flows, the system significantly reduces reliance on developer expertise and minimizes the risk of misconfiguration.

A major strength of the paper is its end-to-end automation, which spans program analysis, policy synthesis, and enforcement integration. This full pipeline approach transforms a traditionally manual, error-prone security task into a systematic, repeatable process. Importantly, the authors demonstrate that their approach is practical for real embedded

systems, showing that strong security guarantees can be achieved without requiring substantial manual redesign of existing applications.

The empirical evaluation further underscores the contribution's significance. TZ-DATASHIELD is applied to realistic embedded software scenarios, where it successfully identifies sensitive data flows and enforces correct compartmentalization policies. The results demonstrate both improved security assurance and reduced developer burden, underscoring the approach's real-world applicability.

From a scientific standpoint, this work advances the foundations of embedded system security by introducing a unified, data-flow-centric framework for reasoning about trust boundaries. It bridges program analysis and systems security to enable principled enforcement of least privilege across heterogeneous execution environments. This represents a meaningful step toward automating secure system design in domains where manual reasoning has traditionally dominated.

In summary, this paper merits strong consideration for the award due to its clear conceptual innovation, rigorous technical approach, and strong practical impact. It addresses a fundamental and persistent problem in embedded system security and provides a scalable, automated solution that is likely to influence future research and practice in the design of trusted execution environments and the construction of secure systems.

Sincerely,

Doowon Kim

Assistant Professor

Computer Science

University of Tennessee, Knoxville