



Dear Members of the Selection Committee,

I am writing to nominate the paper “TZ-DATASHIELD: Automated Data Protection for Embedded Systems via Data-Flow-Based Compartmentalization” (published and presented in the NDSS’25) for the Best Scientific Cybersecurity Paper Competition.

This work addresses a critical and increasingly urgent problem in the security of embedded systems: how to provide strong, principled protection of sensitive data in microcontroller-based environments under realistic and powerful adversary models.

Embedded systems underpin a wide range of safety- and security-critical applications, yet their constrained computational and memory resources have historically limited the deployment of robust security mechanisms. Previously, there are attempts to mitigate this issue by partitioning firmware into isolated units. However, they fundamentally suffer from a mismatch between compartment granularity and the true attack surface. Coarse-grained designs expose unnecessary resources, while fine-grained designs introduce excessive overhead and complex sharing patterns.

This paper makes the important observation that these limitations are not incidental, but rather stem from an inadequate abstraction for defining security boundaries. The core contribution of this work is the introduction of sensitive data flow based compartmentalization, an abstraction that aligns compartment boundaries directly with the flow of sensitive data. By grounding isolation decisions in data dependencies rather than structural program units, the authors provide a principled method for minimizing both attack surface and runtime overhead. This conceptual shift transforms compartmentalization from a heuristic engineering practice into a systematic, analysis-driven process.

Beyond the idea, the authors develop a comprehensive framework that integrates compiler-based analysis, automated code instrumentation, and hardware-assisted isolation via ARM TrustZone. The system addresses multiple challenges that have remained unresolved in prior work. First, it achieves fine-grained yet efficient isolation by constructing compartments that contain only the minimal code and data required for each sensitive data flow. Second, it introduces a novel intra-TEE isolation mechanism, overcoming the long-standing limitation that TrustZone provides no isolation within the secure world. Third, it enforces control-flow integrity (CFI) and data-flow integrity (DFI) for accesses to shared and peripheral resources, thereby closing critical gaps that could otherwise be exploited by advanced attacks such as code-reuse and data-only attacks.

A distinguishing strength of this work is its end-to-end design and practical realization. It is implemented as an LLVM-based toolchain that enables developers to annotate sensitive data and automatically generate secure firmware, significantly lowering the barrier to adoption. The system is evaluated on a diverse set of real-world MCU applications, including both bare-metal and RTOS-based systems. The results demonstrate substantial security improvements, such as significant

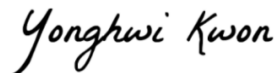
reduction in ROP gadgets. These gains are achieved with moderate overhead, highlighting the practicality of the approach in resource-constrained environments.

Equally important is the paper's rigorous treatment of adversarial capabilities. Unlike many prior works, this study explicitly considers strong adversaries capable of compromising privileged software, and demonstrates that the proposed design effectively contains such attacks within isolated compartments. This realistic threat model significantly strengthens the relevance and credibility of the contributions.

From a broader perspective, this work establishes a new paradigm for data-centric security in embedded systems. By unifying static data-flow analysis, compiler transformations, and hardware-enforced isolation, it provides a coherent framework for reasoning about and enforcing security properties at the level of data dependencies. The ideas introduced in this paper are likely to influence future research across multiple domains, including embedded system security, trusted execution environments, and compiler-assisted defenses.

In conclusion, the paper represents a substantial advancement in the science of cybersecurity. It combines conceptual innovation, technical depth, and practical impact in a manner that is rarely achieved. I strongly recommend this paper for the award, as it not only addresses a pressing problem but also provides a principled and generalizable solution that advances the state of the art.

Sincerely,



Yonghwi Kwon
Assistant Professor
University of Maryland
Electrical and Computer Engineering (ECE)
Maryland Cybersecurity Center (MC2)
University of Maryland Institute for Advanced Computer Studies (UMIACS)
Computer Science (CS), Affiliated

Short Bio

I am an assistant professor of the Department of ECE (Electrical & Computer Engineering) at the University of Maryland. Previously, I was an assistant professor of computer science at the University of Virginia, right after obtaining my PhD from Purdue University in 2018. I am broadly interested in solving system security problems. I am a recipient of the NSF CAREER and CRII Awards, two ACM Distinguished Paper Awards (OOPSLA and ASE), and two Best Paper Awards in Automated Software Engineering (ASE) and WISA. I also won the championship of the National CCDC (Collegiate Cyber Defense Competition) in 2019 and 2020 as a team coach.