SCONE Confidential Computing Environment: Protecting Applications Against Powerful Adversaries

Christof Fetzer
TU Dresden, Germany

Abstract

Our objective is to protect the code, data, and keys of applications against all users with access to the computer systems. In some domains (e.g., healthcare domain), this must be guaranteed, even if the application is not entirely correct. To simplify the adoption of confidential computing, SCONE transforms cloud-native applications into confidential cloud-native applications running on vanilla Kubernetes clusters. The applications can run on Intel SGX, Intel TDX, and AMD SEV. In the near future, SCONE will also support confidential GPUs. The confidentiality, integrity, and consistency of an application's data and keys are guaranteed by always keeping the data encrypted, i.e., at rest, in transit, and in use. This enables us to add a protection layer around applications to prevent data loss caused be bugs and backdoors in the application code.

2012 ACM Subject Classification Security and privacy → Software security engineering; Security and privacy

Keywords and phrases trusted execution environments, security

Digital Object Identifier 10.4230/LIPIcs.OPODIS.2025.1

Category Invited Talk

29th International Conference on Principles of Distributed Systems (OPODIS 2025).
Editors: Andrei Arusoaie, Emanuel Onica, Michael Spear, and Sara Tucci-Piergiovanni; Article No. 1; pp. 1:1–1:1

Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany