UNIVERSITÄT ZU LÜBECK

Evaluating RISC-V Enclaves: Performance Benchmarks and Configuration Best Practices

Bewertung von RISC-V-Enklaven: Leistungsbenchmarks und bewährte Konfigurationspraktiken

Masterarbeit

verfasst am
Institut für Technische Informatik

im Rahmen des Studiengangs
IT Security
der Universität zu Lübeck

vorgelegt von
Basil Ugbomoiko

ausgegeben und betreut von
Dr.-Ing. Saleh Mulhem

mit Unterstützung von
Henry Strunck

Lübeck, den 31. August 2025

Eidesstattliche Erklärung

Ich erkläre hiermit an Eides statt, dass ich diese Arbeit selbständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe.

_____

Basil Ugbomoiko

Zusammenfassung

Diese Arbeit bewertet die Leistung von Keystone-Enklaven, einer Open-Source Trusted Execution Environment (TEE) für RISC-V-Plattformen. Keystone ermöglicht sichere Berechnungen, indem sensible Workloads vom restlichen System isoliert werden. Zur Leistungsbewertung werden zentrale Systemparameter wie die Anzahl der CPU-Kerne, die Cache-Größe, die Speicherzuweisung und die Konfiguration der Enklave untersucht. Mithilfe standardisierter Benchmarking-Tools wie lmbench und CoreMark werden Ausführungszeit, Kontextwechsel-Overhead, Speicherlatenz und CPU-Auslastung unter verschiedenen Hardware- und Softwarekonfigurationen gemessen. Die experimentelle Analyse identifiziert wichtige Leistungsengpässe, die die Effizienz der Enklaven beeinträchtigen. Auf Basis dieser Erkenntnisse werden Konfigurationsrichtlinien und Optimierungsempfehlungen vorgestellt, die auf unterschiedliche Workload-Profile zugeschnitten sind, z. B. rechenintensive, speicherintensive und gemischte Anwendungen. Die gewonnenen Erkenntnisse tragen dazu bei, den Einsatz von Keystone-Enklaven zu optimieren und ihre praktische Anwendbarkeit in sicherheitskritischen Bereichen auf RISC-V-Architekturen zu verbessern.

Abstract

This thesis evaluates the performance of Keystone enclaves, an open-source Trusted Execution Environment (TEE) designed for RISC-V platforms. Keystone enables secure computation by isolating sensitive workloads from the rest of the system. To assess its performance, the study benchmarks critical system parameters, including the number of CPU cores, cache size, memory allocation, and enclave configuration. Using industry-standard benchmarking tools such as lmbench and CoreMark, the research measures execution time, context switch overhead, memory latency, and CPU utilization across a range of hardware and software configurations. The experimental analysis identifies key performance bottlenecks that impact the efficiency of enclave execution. Based on these findings, the study presents configuration best practices and tuning recommendations tailored to various workload profiles, such as compute-bound, memory-intensive, and mixed applications. The insights gained from this evaluation contribute to optimizing the deployment of Keystone enclaves, making them more viable for real-world use cases that demand secure and efficient execution on RISC-V architectures.

Contents

1

Introduction

2

Background and System Architecture

2.1 Trusted Execution Environments

2.2 Keystone architecture overview

2.3 Comparison with other TEEs

2.4 Performance considerations in TEEs

3

Methodology

3.1 Experimental setup

3.2 Benchmarking tools and metrics

3.3 Parameter Variation Strategy

3.4 Data Collection and Analysis Procedures

4

Results and discussion

5

System Configuration Recommendations

5.1 General Configuration Guidelines

5.2 Recommendations for Compute-intensive Workloads

5.3 Recommendations for Memory-intensive Workloads

5.4 Limitations and Bottlenecks

5.5 Implications for Future TEE Design

6

Conclusion and Future Work

6.1 Summary of Contributions

6.2 Limitations of the Current Study

6.3 Directions for Future Research