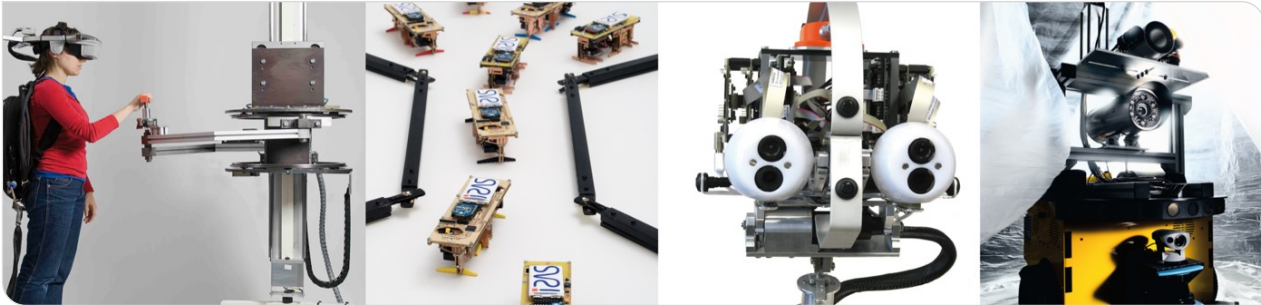


AMD Secure Encrypted Virtualization

Pascal Siekiera | 27. Januar 2023

Betreuer: Paul Wagner



Inhaltsverzeichnis

1. Einleitung

2. Stand der Technik

3. Hauptteil

- AMD Secure Memory Encryption
- AMD Secure Encrypted Virtualization
- Intel SGX

4. Evaluation

- Funktion & Anwendungsfälle
- Sicherheit
- Performance
- Remote Attestation

5. Schlussfolgerung

Einleitung
○

Stand der Technik
○

Hauptteil
○○○

Evaluation
○○○○

Schlussfolgerung
○

Einleitung

Text

- Auflistung
Umbruch
- Auflistung
 - Auflistung
 - Auflistung

Einleitung

Stand der Technik

Hauptteil

Evaluation

Schlussfolgerung

Stand der Technik

Text

- Auflistung
Umbruch
- Auflistung
 - Auflistung
 - Auflistung

Einleitung
○

Stand der Technik
●

Hauptteil
○○○

Evaluation
○○○○

Schlussfolgerung
○

AMD Secure Memory Encryption

Text

- Auflistung
Umbruch
- Auflistung
 - Auflistung
 - Auflistung

Einleitung
○

Stand der Technik
○

Hauptteil
●○○

Evaluation
○○○

Schlussfolgerung
○

AMD Secure Encrypted Virtualization

Text

- Auflistung
Umbruch
- Auflistung
 - Auflistung
 - Auflistung

Einleitung
○

Stand der Technik
○

Hauptteil
○●○

Evaluation
○○○○

Schlussfolgerung
○

Intel SGX

Text

- Auflistung
Umbruch
- Auflistung
 - Auflistung
 - Auflistung

Einleitung
○

Stand der Technik
○

Hauptteil
○○●

Evaluation
○○○○

Schlussfolgerung
○

Funktion & Anwendungsfälle

Text

- Auflistung
Umbruch
- Auflistung
 - Auflistung
 - Auflistung

Sicherheit

Text

- Auflistung
Umbruch
- Auflistung
 - Auflistung
 - Auflistung

Einleitung
○

Stand der Technik
○

Hauptteil
○○○

Evaluation
○●○○

Schlussfolgerung
○

Performance

Text

- Auflistung
Umbruch
- Auflistung
 - Auflistung
 - Auflistung

Remote Attestation

Text

- Auflistung
Umbruch
- Auflistung
 - Auflistung
 - Auflistung

Einleitung
○

Stand der Technik
○

Hauptteil
○○○

Evaluation
○○○●

Schlussfolgerung
○

Schlussfolgerung

Text

- Auflistung
Umbruch
- Auflistung
 - Auflistung
 - Auflistung

Einleitung
○

Stand der Technik
○

Hauptteil
○○○

Evaluation
○○○○

Schlussfolgerung
●

Literatur