Karlsruher Institut für Technologie

Intelligent IISAS Sensor-Actuator-Systems

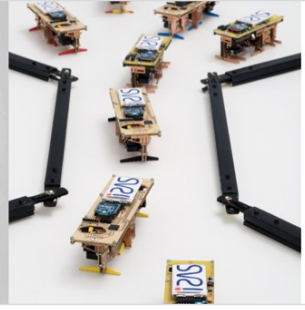
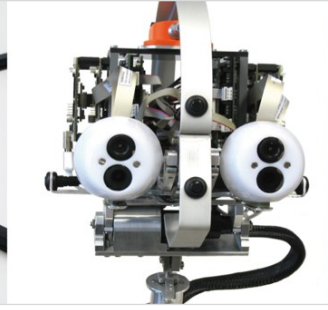
Interaktive Echtzeitsysteme IES

Fraunhofer IOSB

AMD Secure Encrypted Virtualization

Pascal Siekiera | 27. Januar 2023

Betreuer: Paul Wagner


Inhaltsverzeichnis

1. Einleitung
- Cloud-Computing
- Stand der Technik

2. AMD
- AMD Secure Memory Encryption
- AMD Secure Encrypted Virtualization

3. Vergleich mit Intel SGX
- Intel SGX
- Funktion & Anwendungsfälle | Sicherheit | Performance | Remote Attestation

4. Schluss
- Zusammenfassung
- Ausblick

Cloud-Computing

- Bereitstellung IT-Ressourcen
- Modelle
  - Infrastructure as a Service
  - Platform as a Service
  - Software as a Service
- Sicherheit wichtig → **Trusted** Cloud-Computing

{Bechtold 2005; IBM Zugriff: 12/2022; Ruediger Weis und Andreas Bogk 2004}

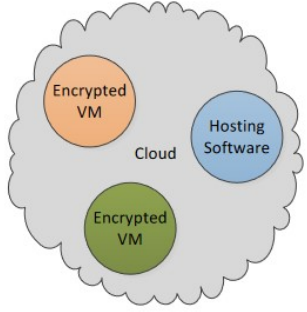


Abbildung: Verschlüsselte VMs in der Cloud *{David Kaplan und Tom Woller 2021}*.

Stand der Technik

1961	Cloud-Computing Konzept (John McCarthy)
Ende 1990er	Kundenbeziehungsmanagement-Webseite (Firma Salesforce) | SaaS
2006	Amazon Web Services (Amazon) | IaaS
2015	Veröffentlichung Intel Software Guard eXtensions
Mai 2016	Ankündigung AMD Secure Encrypted Virtualization
2018	Veröffentlichung AMD Secure Encrypted Virtualization

{Surbiryala und Rong 2019; Intel Corporation 2022, Zugriff: 11/2022; Advanced Micro Devices, Inc. 2020, Zugriff: 11/2022}

AMD Secure Memory Encryption

- Allzweckmechanismus zur Hauptspeicher-Verschlüsselung
- Hardware-Bauteile in CPU-Architektur
- Advanced Encryption Standard (AES) Modul
- AMD Secure Prozessor → Schlüssel
- Zwei Verschlüsselungsmodelle
  - Full Memory Encryption
  - Partial Memory Encryption

{David Kaplan und Tom Woller 2021}

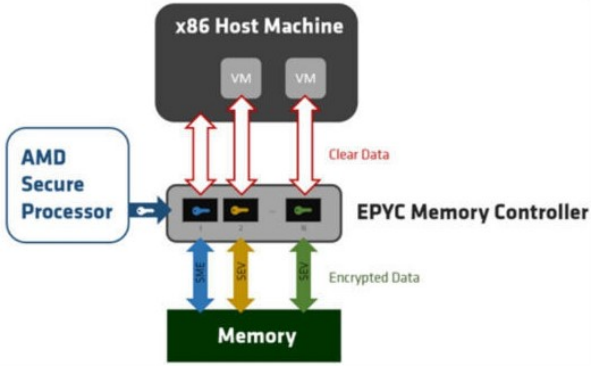
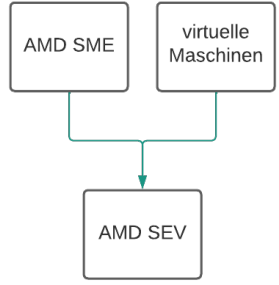


Abbildung: Speicher-Verschlüsselung durch AMD Secure Prozessor bei AMD SME *{Advanced Micro Devices, Inc. 2020, Zugriff: 11/2022}*.

AMD Secure Encrypted Virtualization I

- Kombiniert AMD SME & virtuelle Maschinen
- AMD-V Architektur
- Ziel: virtuelle Maschinen schützen
  - Physische Angriffe
  - Hypervisor-Angriffe
  - Angriffe anderer virtuellen Maschinen
- Keine Software-Modifikationen



{David Kaplan und Tom Woller 2021; Buhren, Werling und Seifert 2019}

Abbildung: AMD SEV Kombination aus AMD SME & virtuellen Maschinen.

AMD Secure Encrypted Virtualization II

- Sicherheitsmodell
  - Isolierte Bereiche anstatt Ring-basiert
  - Streng kontrollierte Kommunikationspfade zwischen Hypervisor & Gast
- Schwachstellen
  - SEV-Plattform vortäuschen
  - Migrations- & Debug-Override-Angriffe

{David Kaplan und Tom Woller 2021; Buhren, Werling und Seifert 2019}

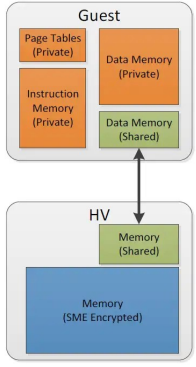


Abbildung: AMD SEV Sicherheitsmodell *{David Kaplan und Tom Woller 2021}*.

Intel SGX

- x86 Prozessorarchitektur Erweiterung
- Hardware-unterstützte Trusted Execution Environments (TEE) / Enklaven
- Schutz vor physikalische Speicherzugriffe o.Ä. Zugriffskontrollmechanismus
- Hardware-basierte Memory Encryption Engine (MEE)
- Datentransport zwischen Enklaven-Seiten-Cache (EPC) & System-Speicher

{Costan und Devadas 2016; Knauth u. a. 2018; Mofrad u. a. 2018; Swami 2017}

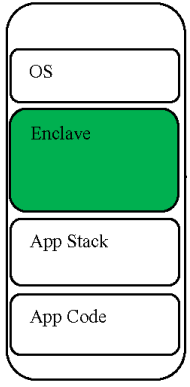


Abbildung: Intel SGX Enklaven Layout *{Xing, Shanahan und Leslie-Hurd 2016}*.

Funktion & Anwendungsfälle

AMD SEV	Intel SGX
Server-Prozessor (AMD EPYC)	Desktop- / Server-Prozessor
Anspruchsvolle Anwendungen	Mikro-Services / kleinere Apps
Viele Daten, kein höheres Maß an Sicherheit	Kleine Menge an sicherheits-sensitiven Daten

{Mofrad u. a. 2018}

Sicherheit

- Intel SGX
  - Advanced Encryption Standard (AES) → Speicherintegritätsschutz
  - Denial of Service Angriffe
  - Cache-Zugriffsmessungen → Enklaven-Geheimnisse
  - Seitenkanalangriffe
- AMD SEV
  - Memory Encryption Engine nutzt AES im Electronic Codebook (ECB) Modus
    → Kein Speicherintegritätsschutz
  - Manipulation von Speicherseiten / DOS-Angriffe durch höher privilegierten Hypervisor
    → VM-spezifischen AMD Secure Prozessor Schlüssel

{Mofrad u. a. 2018}

Performance

- Verschlüsselter Speicher, großer Pufferspeicher $\rightarrow$ AMD schneller
- Einsatz AMD SEV $\rightarrow$ Leistungseinbuße $\sim$1,9x
- Einsatz Intel SGX $\rightarrow$ Leistungseinbuße $\sim$8,2x

Komplexer Workload mit großem Pufferspeicher $\rightarrow$ **AMD übertrifft Intel**

{Mofrad u. a. 2018}

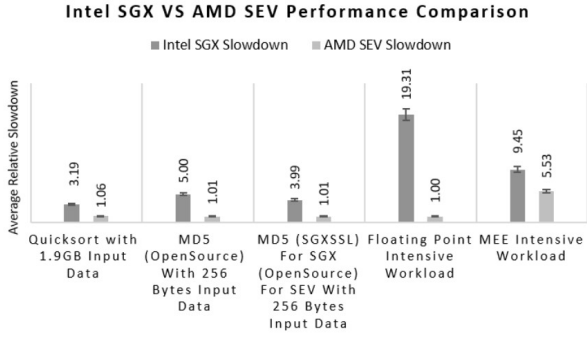


Abbildung: Vergleich Leistungssenkung: AMD SEV vs Intel SGX *{Mofrad u. a. 2018}*.

Remote Attestation

Sicherheitsmechanismus → Vertrauenswürdigkeit, Verifikation der Geräte-Integrität

- Intel SGX
  - Gegen Vortäuschen von SGX
  - Sichere Kommunikationskanäle zu externen Stellen
  - Intel signierte Enklaven
    - Quoting Enclave
- AMD SEV
  - Gegen Vortäuschen SEV & Modifikation von virtuellen Maschinen
  - Einsatz oder Migration eines Gastes
  - Sicherer Übertragungskanal
    → Authentizität, Integrität & Vertraulichkeit der Kommunikation

{Knauth u. a. 2018; Swami 2017; Buhren, Werling und Seifert 2019}

Schlussfolgerung

- Intel SGX
  - Starker Speicherintegritätsschutz

  → Kleine aber streng sicherheitskritische Applikationen
- AMD SEV
  - Kein Speicherintegritätsschutz
  - Bereitstellung großer Mengen an Ressourcen für Applikationen
  - Bessere Performance als Intel SGX

  → Komplexe & oder ältere Anwendungen / Dienstleistungen

Zusammenfassung

- Trusted Cloud-Computing wird seit 1990er immer wichtiger
- AMD Secure Encrypted Virtualization (SEV)
  - Release 2018 | AMD EPYC Server-Prozessor
  - Komplexe & oder ältere Anwendungen / Dienstleistungen
    → Cloud-Computing mit virtuellen Maschinen
- Intel Software Guard eXtensions (SGX)
  - Release 2015 | Skylake Desktop-Prozessor
  - Kleine aber streng sicherheitskritische Applikationen
    → Desktop- & Server-Applikationen

Ausblick

- Trusted Cloud-Computing nimmt an Popularität zu
- AMD SEV für Sicherheit nötig
  $\rightarrow$ In Zukunft weiterhin verwendet
- AMD SEV aktuelles Problem
  - Speicherintegritätsschutz
  - Seitenkanalangriffe

{Computerbase 08/2021, Zugriff: 01/2023}

Literatur I

[1] Advanced Micro Devices, Inc. *Secure Encrypted Virtualization API Version 0.24 — Technical Preview*. Techn. Ber. Advanced Micro Devices, Inc., 2020, Zugriff: 11/2022.

[2] Stefan Bechtold. *Trusted Computing: rechtliche Probleme einer entstehenden Technologie*. ger. Preprints of the Max Planck Institute for Research on Collective Goods 2005,20. Bonn, 2005. URL: http://hdl.handle.net/10419/26879.

[3] Robert Buhren, Christian Werling und Jean-Pierre Seifert. „Insecure Until Proven Updated: Analyzing AMD SEV's Remote Attestation“. In: *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*. CCS '19. London, United Kingdom: Association for Computing Machinery, 2019, S. 1087–1099. ISBN: 9781450367479. DOI: 10.1145/3319535.3354216. URL: https://doi.org/10.1145/3319535.3354216.

Literatur

Literatur II

[4] Computerbase. *AMD SEV Manipulation der Spannung ermöglicht Angriff auf EPYC*. Techn. Ber. Computerbase, 8/2021, Zugriff: 01/2023. URL: https://www.computerbase.de/2021-08/amd-sev-manipulation-der-spannung-ermoeglicht-angriff-auf-epyc/.

[5] Victor Costan und Srinivas Devadas. *Intel SGX Explained*. Cryptology ePrint Archive, Paper 2016/086. https://eprint.iacr.org/2016/086. 2016. URL: https://eprint.iacr.org/2016/086.

[6] Jeremy Powell David Kaplan und Tom Woller. *AMD MEMORY ENCRYPTION*. Techn. Ber. Advanced Micro Devices, 2021.

[7] IBM. *Was ist Cloud-Computing? - Deutschland - IBM*. Techn. Ber. IBM, Zugriff: 12/2022.

[8] Intel Corporation. *Intel® Software Guard Extensions (Intel SGX), Protect and Isolate Confidential Data — Even While You Share and Process It*. Techn. Ber. Intel Corporation, 2022, Zugriff: 11/2022.

[9] Thomas Knauth u. a. *Integrating Remote Attestation with Transport Layer Security*. 2018. DOI: 10.48550/ARXIV.1801.05863. URL: https://arxiv.org/abs/1801.05863.

Literatur

Literatur III

[10] Saeid Mofrad u. a. „A Comparison Study of Intel SGX and AMD Memory Encryption Technology“. In: *Proceedings of the 7th International Workshop on Hardware and Architectural Support for Security and Privacy*. HASP '18. Los Angeles, California: Association for Computing Machinery, 2018. ISBN: 9781450365000. DOI: 10.1145/3214292.3214301. URL: https://doi.org/10.1145/3214292.3214301.

[11] Ruediger Weis und Andreas Bogk. *Trusted Computing - eine unendliche Geschichte*. Techn. Ber. cryptolabs Amsterdam, Chaos Computer Club Berlin, 2004.

[12] Jayachander Surbiryala und Chunming Rong. „Cloud Computing: History and Overview“. In: *2019 IEEE Cloud Summit*. 2019, S. 1–7. DOI: 10.1109/CloudSummit47114.2019.00007.

[13] Yogesh Swami. *SGX Remote Attestation is not Sufficient*. Cryptology ePrint Archive, Paper 2017/736. https://eprint.iacr.org/2017/736. 2017. URL: https://eprint.iacr.org/2017/736.

Literatur

Literatur IV

[14] Bin Cedric Xing, Mark Shanahan und Rebekah Leslie-Hurd. „Intel® Software Guard Extensions (Intel® SGX) Software Support for Dynamic Memory Allocation inside an Enclave“. In: *Proceedings of the Hardware and Architectural Support for Security and Privacy 2016*. HASP 2016. Seoul, Republic of Korea: Association for Computing Machinery, 2016. ISBN: 9781450347693. DOI: 10.1145/2948618.2954330. URL: https://doi.org/10.1145/2948618.2954330.

Literatur