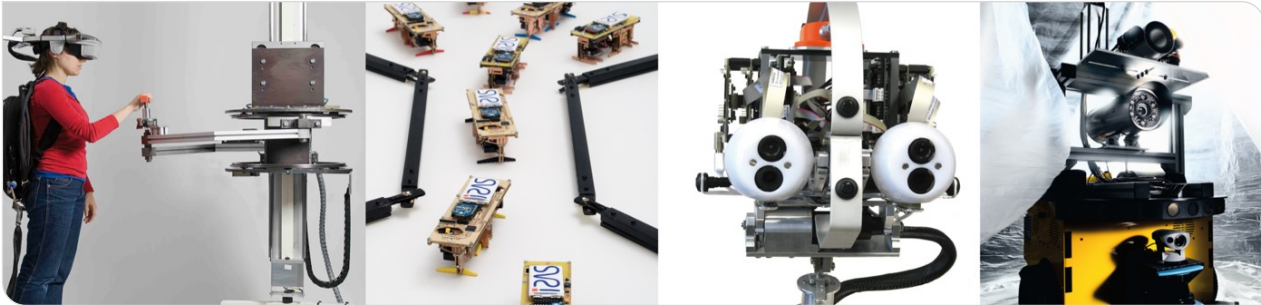


AMD Secure Encrypted Virtualization

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

Einleitung
○○

AMD
○○○

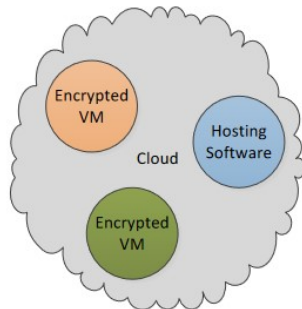
Vergleich mit Intel SGX
○○○○○○

Schluss
○

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}



{David Kaplan und Tom Woller 2021}

Stand der Technik

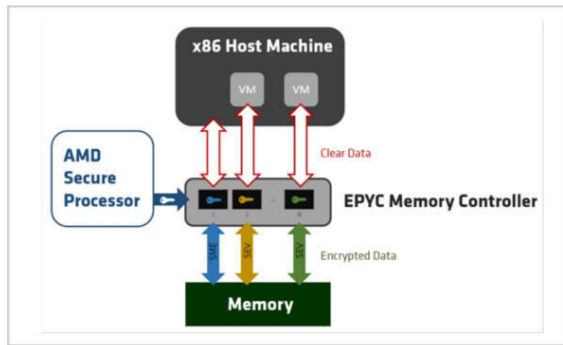
1961	●	Cloud-Computing Konzept (John McCarthy)
Ende 1990er	●	Kundenbeziehungsmanagement-Webseite (Firma Salesforce) SaaS
2006	●	Amazon Web Services (Amazon) IaaS
2015	●	Veröffentlichung Intel Software Guard eXtensions
Mai 2016	●	Ankündigung AMD Secure Encrypted Virtualization
2018	●	Veröffentlichung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



{Advanced Micro Devices, Inc. 2020, Zugriff: 11/2022}

AMD Secure Encrypted Virtualization I

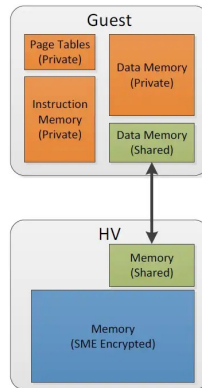
- kombiniert AMD SME & virtuelle Maschinen
- AMD-V Architektur
- Ziel: virtuelle Maschinen schützen
 - physische Angriffe
 - Hypervisor-Angriffe
 - Angriffe anderer virtuellen Maschinen
- keine Software-Modifikationen

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

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}



{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}

Funktion & Anwendungsfälle

AMD SEV	Intel SGX
Server-Prozessor (AMD EPYC) anspruchsvolle Anwendungen viele Daten, kein höheres Maß an Sicherheit	Desktop- / Mobile-Prozessor Mikro-Services / kleinere Apps kleine Menge an sicherheits-sensitiven Daten

{Mofrad u. a. 2018}

Sicherheit

■ Intel SGX

- Advanced Encryption Standard → Speicherintegritätsschutz
- Betriebssystem (OS) übernimmt System Calls → Denial of Service Attacke möglich (Enklaven-Prozesse von OS verweigert oder eliminiert)
- Leistungssteigerung durch Multi-Threading → Kontrollfluss Verlust möglich
- Cache-Zugriffsmessungen → Enklaven-Geheimnisse
- Seitenkanalangriffe

■ AMD SEV

- Memory Encryption Engine im Electronic Codebook (ECB) Modus
- Data-Leaks durch ECB → AMD Algorithmus
- kein Speicherintegritätsschutz
- Manipulation von Speicherseiten / DOS-Angriffe durch höher privilegierten Hypervisor → VM-spezifischen AMD Secure Prozessor Schlüssel

{Mofrad u. a. 2018}

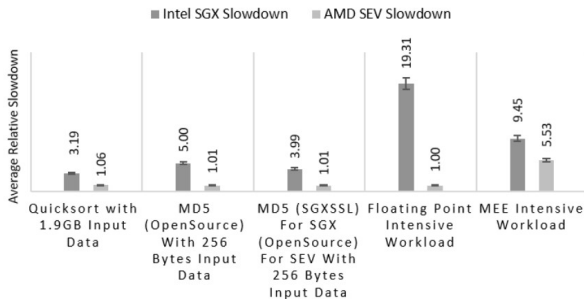
Performance

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

komplexer Workload mit großem Pufferspeicher
→ **AMD übertrifft Intel**

{Mofrad u. a. 2018}

Intel SGX VS AMD SEV Performance Comparison



{Mofrad u. a. 2018}

Remote Attestation

Sicherheitsmechanismus → Vertrauenswürdigkeit, Verifikation der Geräte-Integrität

■ Intel SGX

- gegen Vortäuschen von SGX
- bei Enklaven-Instanziierung nötig
- Intel signierte Enklaven
 - Provisioning Enclave
 - Provisioning Certification Enclave
 - Quoting Enclave

■ AMD SEV

- gegen Vortäuschen SEV & Modifikation von virtuellen Maschinen
- bei Einsatz oder Migration eines Gastes nötig
- 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-Applikationen

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>.
- [4] 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>.

Literatur II

- [5] Jeremy Powell David Kaplan und Tom Woller. *AMD MEMORY ENCRYPTION*. Techn. Ber. Advanced Micro Devices, 2021.
- [6] IBM. *Was ist Cloud-Computing? - Deutschland - IBM*. Techn. Ber. IBM, Zugriff: 12/2022.
- [7] 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.
- [8] 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>.
- [9] 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>.

Literatur III

- [10] Ruediger Weis und Andreas Bogk. *Trusted Computing - eine unendliche Geschichte*. Techn. Ber. cryptolabs Amsterdam, Chaos Computer Club Berlin, 2004.
- [11] 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.
- [12] 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>.