Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD

Nationales Zentrum für Cybersicherheit NCSC
Informatiksicherheit SEC

1. Juli 2022

Technologiebetrachtung

Confidential Computing

1 Einführung

Die Sicherheit informationsverarbeitender Prozesse in IT-Systemen stellt insbesondere vor dem Hintergrund der zunehmenden Nutzung von «Cloud Computing» und entsprechenden Dienstleistungen ein grosses Problem dar. Während die Speicherung und Übertragung von Daten mit Hilfe von kryptografischen Verfahren hinreichend gut gesichert werden kann, stellt die sichere Datenverarbeitung[1] die zentrale Herausforderung dar: Wie können Daten verarbeitet werden, ohne dass man die die Verarbeitung steuernde Software (Code) und die entsprechende Ausführungsumgebung effektiv kontrollieren kann? In der Vergangenheit sind dazu verschiedene Lösungsansätze entwickelt und teilweise auch umgesetzt worden.

Im Rahmen dieser Technologiebetrachtung wird mit «Confidential Computing» einer dieser Lösungsansätze kurz vorgestellt und diskutiert, d. h. es wird aufgezeigt, worum es geht, wie der Ansatz grob funktioniert, was die Vor- und Nachteile sind und wie das Potential und die Zukunftsaussichten einzuschätzen sind.

2 Problemstellung

Wie einleitend erwähnt, stellt die sichere Verarbeitung von Daten in einem IT-System eine grosse Herausforderung dar. Dabei müssen sowohl die Integrität der Umgebung, in der die Anwendung ausgeführt wird (d. h. die Ausführungsumgebung), als auch die Vertraulichkeit der Daten während ihrer Verarbeitung gewährleistet sein. Gemäss Abbildung 1 umfasst die Ausführungsumgebung nicht nur die Anwendung selbst (inklusive Daten und Code), die in einer virtuellen Maschine (VM) ausgeführt wird, sondern auch das Gast-Betriebssystem der VM, den Hypervisor, das Host-Betriebssystem und die Hardware. All diese Komponenten müssen vor einer Kompromittierung und Exfiltration von Daten geschützt sind, damit die Sicherheit der Anwendung nicht unterwandert werden kann. Entsprechend sind die in Abbildung 1 rot eingefärbten Komponenten für die Sicherheit der Datenverarbeitung kritisch und müssen als vertrauenswürdig[2] angenommen werden.

---

[1] Man spricht in diesem Zusammenhang auch etwa von «Data in Use» (gegenüber «Data at Rest» für gespeicherte und «Data in Transit» für übertragene Daten).

[2] In der IT-Sicherheit müssen die (System-)Komponenten, deren Sicherheit man weder beweisen noch verifizieren kann, als vertrauenswürdig angenommen werden. Sie stellen in ihrer Gesamtheit die Trusted Computing Base (TCB) dar, die so klein als möglich gehalten werden muss.

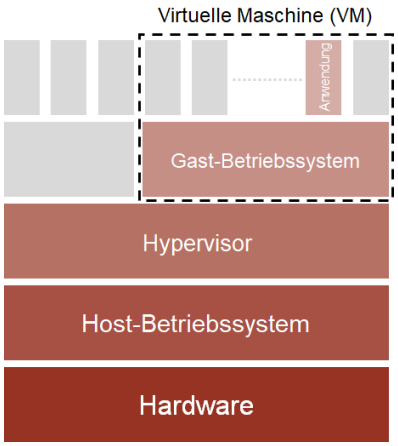

Abbildung 1: Verarbeitung von Daten in einem IT-System

Wenn eine Anwendung nicht lokal («On Premises») ausgeführt wird, sondern stattdessen die Dienstleistungen eines Cloud-Anbieters in Anspruch genommen werden, dann muss der Datenverarbeiter nicht nur auf die Vertrauenswürdigkeit seiner eigenen IT-Systeme zählen können, sondern auch auf die Vertrauenswürdigkeit dieses Anbieters und dessen IT-Systeme. Diese Situation ist in Abbildung 2 schematisch dargestellt. Der Datenverarbeiter sendet Daten und Code zum Cloud-Anbieter, der in einer von ihm bereitgestellten Ausführungsumgebung den Code auf die Daten anwendet und dem Datenverarbeiter am Schluss das Resultat (auf eine gesicherte Art und Weise) zurückgibt. Dabei hat der Datenverarbeiter in der Regel keine Möglichkeit, die Ausführungsumgebung und deren Sicherheit direkt zu kontrollieren, d. h. er ist hier auf das Versprechen des Cloud-Anbieters und entsprechende Bescheinigungen und Zertifikate angewiesen.

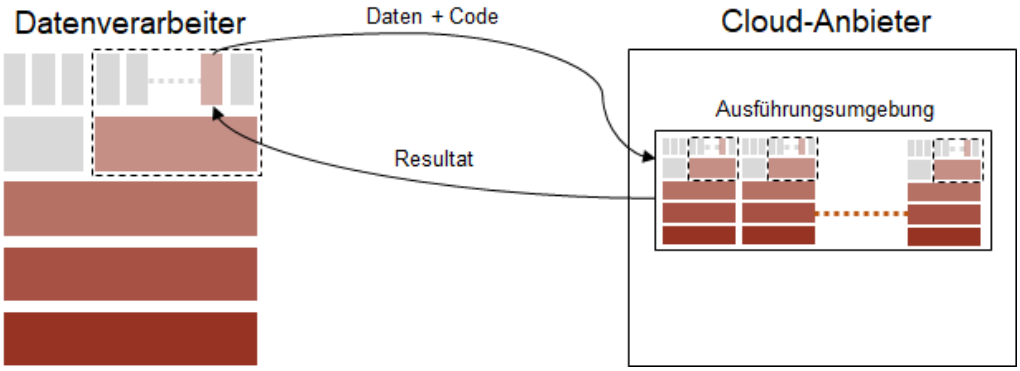

Abbildung 2: Die Ausführung einer Anwendung im Rahmen von «Cloud Computing»

Die dieser Situation zugrundeliegende Problemstellung wird in der Literatur auch etwa als «Secure Remote Computation» umschrieben: Wie kann auf einer fremdbetriebenen und nicht direkt kontrollierbaren IT-Infrastruktur eine vertrauenswürdige Ausführungsumgebung bereitgestellt und die Exfiltration von Daten wirksam verhindert werden, so dass insgesamt eine «sichere» Datenverarbeitung resultiert? Diese Frage stellt die Umkehrung der Problemstellung dar, die sich mit dem Schutz einer vertrauenswürdigen IT-Infrastruktur vor potentiell bösartigem Code (z. B. Java-Applets) befasst und mit Sandboxing wenigstens teilweise gelöst werden kann. Beim Sandboxing wird die Ausführungsumgebung minimal gehalten und soweit als möglich vom Rest der IT-Infrastruktur abgeschottet (isoliert), damit potentiell bösartiger Code diese nicht beeinflussen oder kompromittieren kann. Sandboxing ist für das «Secure Remote Computation» keine Option, weil es eben nicht die IT-Infrastruktur ist, die

geschützt werden muss, sondern die Daten und der Code. Für das «Secure Remote Computation»-Problem sind andere und meist auch komplexere Lösungsansätze erforderlich.

3 Lösungsansätze

Langfristig wird die Lösung des «Secure Remote Computation»-Problems wohl in voll homomorphen Verschlüsselungsverfahren liegen müssen. Mit solchen Verfahren kann der Datenverarbeiter dem Cloud-Anbieter seine Daten so in verschlüsselter Form zur Verfügung stellen, dass dieser die Daten verarbeiten aber nicht entschlüsseln kann, d. h. es ist dann sichergestellt, dass der Cloud-Anbieter die Daten nicht im Klartext sieht. Am Ende der Datenverarbeitung wird das Resultat in immer noch verschlüsselter Form dem Datenverarbeiter zurückgegeben, so dass dieser das Resultat entschlüsseln kann. Damit lässt sich eine Software-mässig realisierbare Lösung für das «Secure Remote Computation»-Problem konstruieren. Leider sind die heute bekannten und zur Verfügung stehenden voll homomorphen Verschlüsselungsverfahren zu wenig effizient, als dass sie für allgemeine Datenverarbeitungsaufgaben genutzt werden könnten.

Bis praxistaugliche voll homomorphe Verschlüsselungsverfahren verfügbar sind, kann versucht werden, das «Secure Remote Computation»-Problem mit Hilfe von vertrauenswürdigen Hardware-Komponenten zu lösen. Damit lässt sich die Integrität einer Ausführungsumgebung bis zu einem bestimmten Punkt gewährleisten. Vertrauenswürdige Hardware-Komponenten gibt es in verschiedenen Formfaktoren, wie z. B. Smartcards, Sicherheitselemente, Hardware-Sicherheitsmodule und Trusted Platform Modules (TPMs). Letztere sind im Rahmen der «Trusted Computing»-Initiative der Trusted Computing Group (TCG[3]) spezifiziert und seither auch breit verbaut worden. Mit Hilfe eines TPM kann sichergestellt werden, dass ein IT-System in einen definierten Zustand aufstartet («bootet») und entsprechend nicht von manipulierter Software kompromittiert worden ist. Damit kann die Integrität einer Ausführungsumgebung gesichert werden - wenigstens solange, bis nicht bekannte Software in das System geladen und ausgeführt wird. Weil dies früher oder später geschehen wird, ist der der Aufwand, den die Nutzung eines TPM verursacht, gegenüber dem Nutzen relativ hoch.

Eine einfachere und breiter einsetzbare Möglichkeit zur Hardware-Unterstützung ist von einem Industriekonsortium[4] unter der Bezeichnung «Confidential Computing» vorgeschlagen worden. Dabei bietet die Hardware die Möglichkeit, eine sogenannte Trusted Execution Environment (TEE) als «sichere Enklave» zu betreiben, in der eine Datenverarbeitung in einem gesicherten Modus stattfinden kann, d. h. die Verarbeitung findet nur im Prozessor statt und keine Software ausser der die TEE betreibende Anwendung kann auf die TEE zugreifen oder Daten von dort auslesen. Zudem kann die Anwendung sowohl die TEE als auch den Code, der in der TEE ausgeführt werden soll, vor der Einspielung von Daten validieren (man spricht in diesem Zusammenhang von «Remote Attestation»). Damit Zustandsvariablen und Resultate zwischengespeichert werden können, unterstützt die TEE auch ein sogenanntes «Sealing», d. h. eine kryptografische Absicherung solcher Daten in der dafür vorgesehenen Speicherablage. Die Schlüssel, die für «Remote Attestation» und «Sealing» erforderlich sind, existieren nur in der Hardware bzw. in den entsprechenden TEEs und können von dort nicht bzw. nur mit unverhältnismässig grossem Aufwand ausgelesen werden.

Die Ausführung einer Anwendung unter Zuhilfenahme einer TEE ist in Abbildung 3 dargestellt. Man beachte, dass die einzigen vertrauenswürdigen Komponenten in diesem Szenario die Anwendung selbst und die TEE sind (beide sind in der Abbildung rot eingefärbt). Insbesondere kann in diesem Szenario der Betreiber des IT-Systems die Daten der Anwendung

[3] https://trustedcomputinggroup.org
[4] https://confidentialcomputing.io

nicht einsehen – wenigstens solange die Hardware die spezifizierten Features von «Confidential Computing» korrekt umsetzt. Konkret bedeutet das, dass dem Lieferanten der Hardware vertraut werden muss.

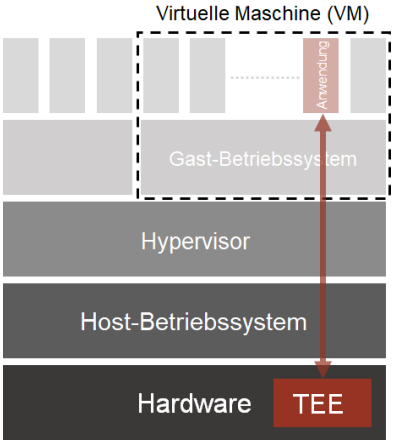

Abbildung 3: Die Ausführung einer Anwendung unter Zuhilfenahme einer TEE

Besonders interessant und erfolgversprechend erscheint nun der Einsatz von «Confidential Computing» in einer Cloud-Umgebung. Die Abbildung 2 entsprechende Situation ist in Abbildung 4 schematisch dargestellt. Demnach werden Daten und Code vom Datenverarbeiter so in die TEE des Cloud-Anbieters eingespiesen, dass sie End-zu-End verschlüsselt sind und erst in der TEE entschlüsselt werden. Weil sie auch erst in der TEE ausgeführt werden, hat der Cloud-Anbieter als Betreiber der Ausführungsumgebung bzw. TEE keine Möglichkeit, die Daten einzusehen oder den Code und damit die Datenverarbeitung zu kompromittieren. Die TEE stellt damit eine gesicherte Ausführungsumgebung zur Verfügung, deren Integrität die Anwendung selbst validieren kann. Mit Hilfe von «Remote Attestation» kann sichergestellt werden, dass sowohl die TEE als auch der dort ausgeführte Code authentisch sind und die Datenverarbeitung korrekt und im Sinne des Datenverarbeiters verläuft. Das Resultat wird der Anwendung direkt von der die Datenverarbeitung leistenden TEE zugestellt. Natürlich bleibt die Sicherheit der Datenverarbeitung auf der Seite des Datenverarbeiters abhängig von allen Komponenten. Auf der Seite des Cloud-Anbieters können aber die Abhängigkeiten und erforderliche Vertrauenswürdigkeit stark reduziert werden. Damit kann sich auch der Cloud-Anbieter aus der Verantwortung nehmen, weil er keine Möglichkeit hat, Daten einzusehen oder Code zu kompromittieren.

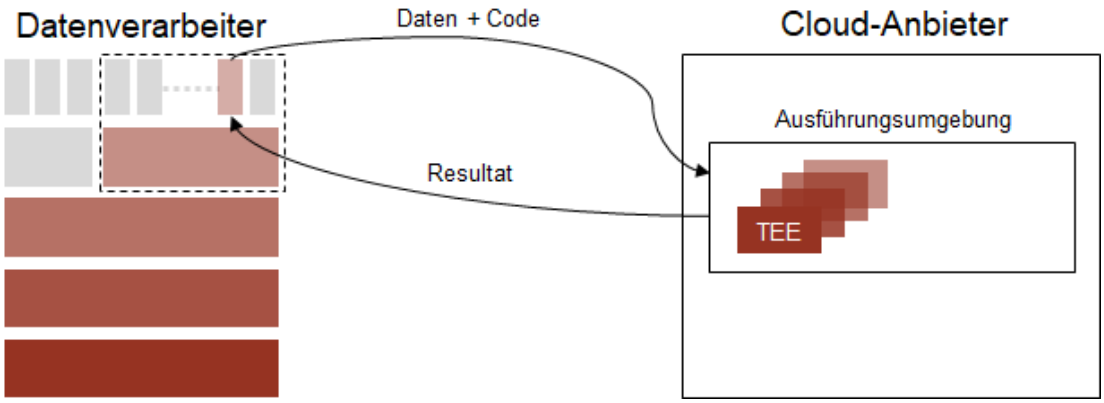

Abbildung 4: Die Ausführung einer Anwendung unter Zuhilfenahme einer TEE in einer Cloud-Umgebung

Der Begriff «Confidential Computing» bezeichnet den skizzierten Technologieansatz, der von unterschiedlichen Hardwarelieferanten auch unterschiedlich umgesetzt und implementiert werden kann und wird. Beispiele sind die Software Guard Extensions (SGX) von Intel [CD16], TrustZone von ARM und Secure Encrypted Virtualization (SEV[5]) von AMD.

4 Potential und Zukunftsaussichten

Mit Hilfe von «Confidential Computing» und entsprechenden TEEs kann die Verarbeitung von Daten sicherer und im Umfeld von Cloud Computing auch weniger abhängig von der Vertrauenswürdigkeit des oder der Cloud-Anbieter gestaltet werden. Insofern ist der Ansatz für das «Secure Remote Computation»-Problem interessant und stellt einen wichtigen Beitrag zur Verbesserung der digitalen Souveränität in einer sich zunehmend auf Cloud Computing ausrichtenden Welt dar. Man kann davon ausgehen, dass noch mehr Implementierungen (als SGX, TrustZone und SEV) auf dem Markt erscheinen und von den Cloud-Anbietern in ihren Rechenzentren auch verbaut werden. Sinnvollerweise eingesetzt werden sie in Anwendungen, bei denen Daten auch gegenüber den Cloud-Anbieter geschützt werden müssen, wie z.B. bei der Verwaltung kryptografischer Schlüssel oder dem Abgleich von datenschutzrelevanten Daten (z. B. Abgleich von persönlichen Kontaktdaten im End-zu-End verschlüsselnden Messenger Signal). Mittlerweile gibt es für «Confidential Computing» und entsprechende TEEs auch Schweizer Anbieter, wie z. B. Decentriq[6], CYSEC[7] oder Securosys[8].

Trotz seiner Vorzüge stellt «Confidential Computing» kein Allheilmittel für die IT-Sicherheit dar. Auch wenn damit die Abhängigkeit von der Vertrauenswürdigkeit der Cloud-Anbieter sinkt, kommt eine neue Abhängigkeit hinzu: Die Vertrauenswürdigkeit der Lieferanten der TEEs muss sichergestellt sein. Ein Cloud-Anbieter könnte mit einem Lieferanten kooperieren, um gemeinsam eine Datenverarbeitung in einer TEE zu kompromittieren. Allerdings ist eine solche Kooperation in der Realität wohl nur schwer zu etablieren und noch schwerer geheim zu halten. Letztlich können auch Implementierungen von «Confidential Computing» und entsprechende TEEs (z. B. über Seitenkanäle) angegriffen werden[9]. Ein für die IT-Sicherheit übliches Katz-und-Maus-Spiel wird sich auch in diesem Bereich einstellen.

Abkürzungen

IT	Informationstechnologie
SEV	Secure Encrypted Virtualization
SEV-ES	SEV Encrypted State
SEV-SNP	SEV Secure Nested Paging
SGX	Software Guard Extensions
TCB	Trusted Computing Base
TCG	Trusted Computing Group
TEE	Trusted Execution Environment
TPM	Trusted Platform Module
VM	Virtuelle Maschine

[5] SEV gibt es in verschiedenen Ausprägungen, wie z.B. SEV-ES (SEV Encrypted State) und SEV-SNP (SEV Secure Nested Paging).

[6] https://www.decentriq.com

[7] https://www.cysec.com

[8] https://www.securosys.com

[9] Eine Zusammenstellung aller publizierten Angriffe gegen Intel SGX findet sich z.B. in [NBB20].

Referenzen

[CD16] V. Costan und S. Devadas, Intel SGX Explained, IACR Cryptology ePrint Archive, Vol. 2016, No. 086, https://eprint.iacr.org/2016/086.pdf

[NBB20] A. Nilsson, P. Nikbakht Bideh und J. Brorsson, A Survey of Published Attacks on Intel SGX, arXiv: 2006.13598, https://arxiv.org/abs/2006.13598