Kurzfassung zum Sachbericht

Vorhabenbezeichnung: 16KIS1441, CRYPTECS (Verbundnummer KIS6DFR008)

Verbundprojekt: Cloud-Ready Privacy-Preserving Technologies - CRYPTECS

Teilvorhaben: Die Verbindung von Privatsphäre wahrenden Datenanalysemethoden und Trusted-Execution-Environments

Projektlaufzeit: 01.07.2021 bis 30.06.2024

Aufgabenstellung und Ausgangssituation

Das Projekt CRYPTECS hatte das Ziel, Privacy-Preserving-Computing (PPC)-Technologien für den industriellen Einsatz bereitzustellen. Ziel war die Entwicklung einer Cloud-Plattform, die die Nutzung von Trusted-Execution-Environments (TEEs) ermöglicht, um sensitive Daten sicher und unter Wahrung der Privatsphäre zu verarbeiten.

Die zentrale Fragestellung bestand darin, wie sich vertrauenswürdige und skalierbare Systeme zur Verarbeitung sensibler Daten realisieren lassen. Dabei ging es um sowohl personenbezogene Daten, die durch Regulierungen wie die DSGVO geschützt sind, als auch industrielle Daten, bei denen Bedenken hinsichtlich des Verlusts von Wettbewerbsvorteilen und Betriebsgeheimnissen bestehen.

Trusted-Execution-Environments wie Intel SGX und AMD SEV bieten die Möglichkeit, Daten sicher in nicht-vertrauenswürdigen Umgebungen zu verarbeiten. Dabei bleiben Programmcodes und Daten in einer TEE zur gesamten Laufzeit im Arbeitsspeicher verschlüsselt. Diese Technologie ermöglicht eine vertrauenswürdige Datenverarbeitung und bildete die Grundlage der von Edgeless Systems im Verbundprojekt durchgeführten Arbeiten.

Ablauf und Zusammenarbeit

Die Projektarbeit begann aufgrund begrenzter Kapazitäten mit Verzögerungen. Der Rückstand konnte aber im Verlauf des Jahres 2022 schnell aufgeholt werden.

Früh im Laufe des Projekts schied die Firma Aircloak aus dem Konsortium aus. Dies erforderte eine Anpassung des Arbeitsplans. Insbesondere musste der eigentlich von Aircloak kommende Proxy für Privacy-Preserving-Computing-Verfahren wieder aus den Planungen entfernt und die Architektur der geplanten Plattform angepasst werden. Infolgedessen wurde auf Seiten von Edgeless Systems der ursprüngliche Fokus weg von TEE-basierten Datenbanken hin zu TEE-basierten Kubernetes-Umgebungen[1] geändert. Dies hatte Einfluss auf die Ausgestaltung sämtlicher technischer Arbeitspakete auf Seiten von Edgeless Systems.

Als Basis für die Arbeiten diente fortan die von Edgeless Systems entwickelte Open-Source-Software Constellation, die es zum Ziel hat, ganze Kubernetes-Umgebungen mittels TEEs abzuschirmen. Im Laufe des Projekts wurde Constellation schrittweise erweitert und optimiert. Dabei wurde insbesondere eng mit dem Verbundpartner Bosch zusammengearbeitet, um die PPC-Plattform CarbyneStack mit Constellation zu integrieren.

[1] Bei Kubernetes handelt es sich um den de-facto Standard zur skalierbaren Ausführung von Anwendungen in Cloud-Umgebungen.

Wesentliche Ergebnisse

Wie geplant, wurde der Großteil der Zeit auf die Arbeitspakte 3, 4 und 5 verwendet, die Teile der großen Arbeitspakete „Individuelle Verbesserung der PPC Verfahren“, „Integration der PPC Verfahren“ und „Konzeptionierung und Umsetzung der Plattform” des Verbundprojekts waren. Details sind im Folgenden aufgeführt.

Erhöhung des Durchsatzes für TEE-basierte Software (AP3)

Die Plattform Constellation wurde so ausgebaut, dass eine quasi unbegrenzte Skalierung in Cloud-Umgebungen möglich wird. Zudem wurden die folgenden zentralen Verbesserungen an Constellation durchgeführt:

- Unterstützung für die TEE-Technologie Intel TDX
- Unterstützung für die TEE-Technologie der Nvidia H100; hierdurch können auch aktuelle KI-Anwendungen auf Constellation geschützt ausgeführt werden.
- Bereitstellung eines Proxys zur automatischen Ver- und Entschlüsselung von Cloud-Speichern wie S3
- Ende-zu-Ende-Absicherung der Software-Supply-Chain mit Hilfe des Projekts Sigstore[2]: Alle Softwarekomponenten von Constellation werden kryptographisch signiert und die entsprechenden Signaturen in einem global einsehbaren, verteilten und fälschungssicheren Log abgelegt. Dies stellte einen Meilenstein in der Abwehr von Supply-Chain-Angriffen dar.

TEEs im Zusammenhang mit PPC-Verfahren (AP 4)

Die vom Projektpartner Bosch entwickelte Plattform CarbyneStack wurde erfolgreich auf Constellation zum Laufen gebracht und getestet. Die Kombination lieferte herausragende Eigenschaften für PPC-Anwendungen.

Prüfung, Implementierung und erste Auswertung der TEE-Technologie innerhalb der PPC-Plattform (AP 5)

Umfangreiche Benchmarks wurden mit Constellation durchgeführt. Das Ergebnis ist, dass Anwendungen wie HashiCorp Vault auf Constellation nahezu die gleiche Leistung wie auf ungeschützten Kubernetes-Plattformen erzielen können.

Bewertung

Die Entwicklungen im Rahmen von CRYPTECS zeigten klare Fortschritte bei der Nutzung von TEE-gestützten Technologien für sichere und skalierbare Anwendungen in der Cloud. Die Ergebnisse bieten eine vielversprechende Basis für industrielle Anwendungen mit höchsten Sicherheitsanforderungen.

[2] https://www.sigstore.dev/

Abschließender Sachbericht

Vorhabenbezeichnung: 16KIS1441, CRYPTECS (Verbundnummer KIS6DFR008)

Verbundprojekt: Cloud-Ready Privacy-Preserving Technologies - CRYPTECS

Teilvorhaben: Die Verbindung von Privatsphäre wahrenden Datenanalysemethoden und Trusted-Execution-Environments

Projektlaufzeit: 01.07.2021 bis 30.06.2024

1 Übersicht

Das Projekt CRYPTECS hatte das Ziel, Privacy-Preserving-Computing (PPC)-Technologien für den industriellen Einsatz bereitzustellen. Ziel war die Entwicklung einer Cloud-Plattform, die die Nutzung von Trusted-Execution-Environments (TEEs) ermöglicht, um sensitive Daten sicher und unter Wahrung der Privatsphäre zu verarbeiten.

Die zentrale Fragestellung bestand darin, wie sich vertrauenswürdige und skalierbare Systeme zur Verarbeitung sensibler Daten realisieren lassen. Dabei ging es um sowohl personenbezogene Daten, die durch Regulierungen wie die DSGVO geschützt sind, als auch industrielle Daten, bei denen Bedenken hinsichtlich des Verlusts von Wettbewerbsvorteilen und Betriebsgeheimnissen bestehen.

Trusted-Execution-Environments wie Intel SGX und AMD SEV bieten die Möglichkeit, Daten sicher in nicht-vertrauenswürdigen Umgebungen zu verarbeiten. Dabei bleiben Programmcodes und Daten in einer TEE zur gesamten Laufzeit im Arbeitsspeicher verschlüsselt. Diese Technologie ermöglicht eine vertrauenswürdige Datenverarbeitung und bildete die Grundlage der von Edgeless Systems im Verbundprojekt durchgeführten Arbeiten.

2 Verwendung der Zuwendungen

2.1 Wichtigste Positionen des zahlenmäßigen Nachweises

Den mit Abstand größten Anteil an den ursprünglich geplanten Projektkosten von 240.836€ nehmen die Personalkosten (0831) mit einem ursprünglich geplanten Gesamtvolumen von 168.750€ ein. Dahinter folgen die „sonstigen unmittelbaren Vorhabenkosten“ (0850) mit einem ursprünglich geplanten Gesamtvolumen von 64.286€. Diese sonstigen Kosten setzen sich aus zwei Unterposten zusammen: Löhne für Werkstudenten in der Entwicklung (55.476€) und Miete für TEE-fähige Cloud-Ressourcen zur Entwicklung (8.810€). Daneben sah der ursprüngliche Projektplan noch 5.000€ für Abschreibungen auf die Anschaffung eigener Entwicklungshardware (0847) und 2.800€ (0838) für projektbezogene Reisen vor.

Während des Projekts stellte sich heraus, dass die Anschaffung eigener Hardware nicht notwendig war und dass weniger Reisen als ursprünglich geplant für die Koordination des Projekts notwendig waren. Deshalb wurden diese Posten in verringertem Umfang, respektive gar nicht abgerufen. Im Gegenzug stellten sich einige technische Arbeiten als komplexer dar, als ursprünglich angenommen. Dementsprechend wurde eine Umwidmung von Mitteln von dem Posten 0850 hin zu 0831 vorgenommen, wie in folgender Tabelle dargestellt:

Posten	Ursprünglich geplante Kosten	Geänderte Gesamtkalkulation	Veränderung
Personalkosten (0831)	168.750,00	198.851,22	+30.101,22
Sonstige unmittelbare Vorhabenskosten (0850)	64.286,20	34.184,98	-30.101,22

Die Förderquote des Teilprojekt betrug 60%.

2.2 Notwendigkeit und Angemessenheit der geleisteten Projektarbeiten

Die im Projekt verwendeten Mittel dienten der Bearbeitung der in der Vorhabenbeschreibung definierten Arbeitspakete. Die Ziele des Projekts und der einzelnen Arbeitspakete wurden aus Forschungs- und Entwicklungssicht ambitioniert gesetzt und konnten trotz des unerwarteten Ausscheidens des Verbundpartners Aircloak und den damit verbundenen notwendigen kurzfristigen Anpassungen in großen Teilen erfolgreich abgeschlossen werden. Es konnten wichtige wissenschaftliche und technische Erkenntnisse im Bereich der PPC-Verfahren und TEE-Technologie gewonnen werden. Zudem konnten diese Erkenntnisse nahe der Marktreife gebracht werden. Aus Sicht von Edgeless Systems stellt dies insgesamt einen guten bis sehr guten Erfolg dar. Der Einsatz der Mittel erscheint vor diesem Hintergrund angemessen.

2.3 Zeitlicher Rahmen

Von Seiten Edgeless Systems wurde die ursprüngliche Projektlaufzeit von Juli 2021 bis Juni 2024 eingehalten. Andere Verbundpartner haben basierend auf einer kostenneutralen Verlängerung auch noch nach Juni 2024 Arbeiten durchgeführt. Aufgrund von Personalmangel konnten auf Seiten Edgeless Systems die Arbeiten jedoch erst im Januar 2022 beginnen. Der entstandene Verzug konnte aber durch vorübergehende Mehrarbeit aufgeholt werden.

3 Ergebnisse

Das Ziel des CRYPTECS-Verbundprojekts bestand darin, „Technologien zum Schutz der Privatsphäre weiterzuentwickeln und in Form einer Cloud-Plattform für die industrielle Nutzung in den Bereichen IoT und Automotive verfügbar zu machen.“ Dabei sollten innerhalb der Plattform unterschiedliche Technologien zum Schutz von Daten zum Einsatz kommen. Zu diesen Technologien gehörten Multiparty Computation (MPC), Homomorphe Verschlüsselung (HE), Differential Privacy (SDC) und Trusted Execution Environments (TEEs).

Die folgende Abbildung 1 stammt aus der ursprünglichen Gesamtvorhabenbeschreibung.

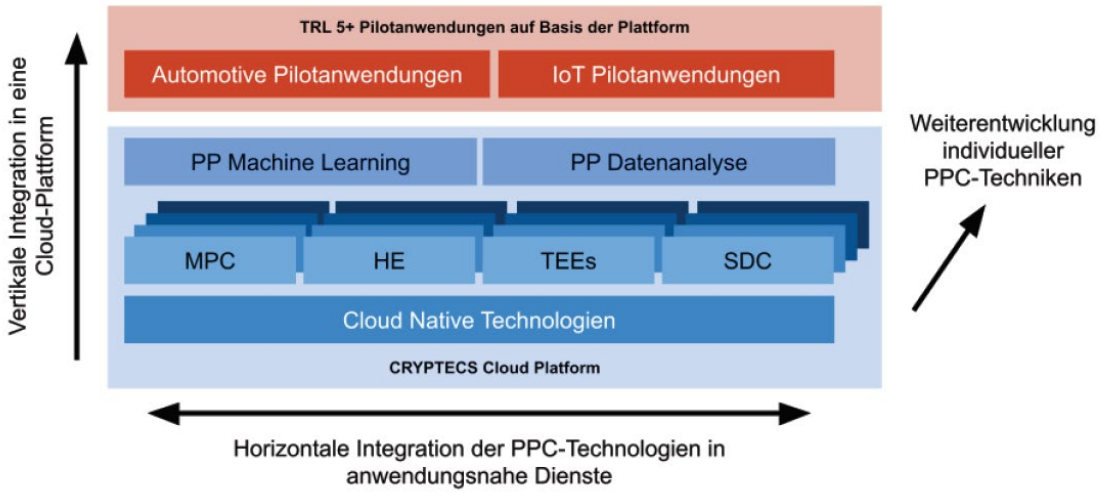

Abbildung 1: Skizze der ursprünglich geplanten Plattform aus der Gesamtvorhabenbeschreibung des CRYPTECS Projekts

Innerhalb des Projekts übernahm Edgeless Systems sämtliche Aufgaben im Bereich TEEs. Der ursprüngliche Plan war, dass Edgeless Systems eine TEE-basierte skalierbare relationale Datenbank entwickeln sollte, die dann zusammen mit SDC-Technologie von Aircloak eine Privatsphäre wahrende Live-Analyse von sensiblen Daten ermöglichen sollte. Als Beispielanwendungsfälle dienten unterschiedliche Szenarien, die von den Projektpartnern Bosch und Orange skizziert wurden. Dazu gehörten Datenanalysen im Personalwesen und die Auswertung von Telemetriedaten von Endverbraucher-Routern.

Aufgrund des Ausscheidens von Aircloak waren hier Anpassungen nötig. So wurde schlussendlich von Edgeless Systems eine TEE-basierte Kubernetes-Plattform namens Constellation weiterentwickelt. Diese wurde dann mit der vom Projektpartner Bosch entwickelten MPC-Plattform CarbyneStack integriert. Die Kombination aus CarbyneStack und Constellation lieferte eine vorteilhafte Kombination von Datensicherheit, Ausführungsgeschwindigkeit und Praktikabilität.

Sämtliche Projektergebnisse von Edgeless Systems stehen mit der Plattform Constellation in Verbindung. Constellation nutzt TEE-Technologie, um ganze Kubernetes-Cluster[1] von der Infrastruktur abzuschirmen. Mit diesem Ansatz ermöglicht es Constellation, sensible Daten auf Standardinfrastruktur in der Cloud zu verarbeiten. Dabei sorgt Constellation ausschließlich für die Abschirmung gegenüber der Infrastruktur. Der Anwendungsbetreiber selbst wird nicht ausgeschlossen. Diese Lücke schließt in dem oben skizzierten Ansatz CarbyneStack.

Die Grundlagen von Constellation wurden bereits vor Beginn des Projekts intern bei Edgeless Systems entwickelt. Im Rahmen von CRYPTECS wurden wesentliche Verbesserungen vorgenommen und wertvolle Erkenntnisse erzielt. Constellation ist im Kern als Open-Source-Software verfügbar[2]. Dies beinhaltet die im Rahmen des Projekts vorgenommenen

[1] Bei Kubernetes handelt es sich um den de-facto Standard für die skalierbare Ausführung von Anwendungen auf Containerbasis in Cloud-Umgebungen. Man kann sich Kubernetes als eine Art Betriebssystem für Cloud-Anwendungen vorstellen.
[2] https://github.com/edgelesssys/constellation

Erweiterungen. Die Ergebnisse der Arbeiten von Edgeless Systems werden im Folgenden nach Arbeitspaketen gegliedert dargestellt.

3.1 Erhöhung des Durchsatzes für TEE-basierte Software (AP 3)

Im Rahmen des Projekts wurde so ausgebaut, dass eine quasi unbegrenzte Skalierung in Cloud-Umgebungen wie Azure und AWS möglich wird. Dies verlangte die Entwicklung und Implementierung von komplexen kryptographischen Protokollen und die Entwicklung von unterschiedlichen Diensten und Erweiterungen für Kubernetes. Zudem wurden die folgenden zentralen Verbesserungen an Constellation durchgeführt:

- Unterstützung für die aktuelle TEE-Technologie Intel TDX; hierdurch können mehr Cloud-Infrastrukturen unterstützt werden.
- Unterstützung für die TEE-Technologie der Nvidia H100; hierdurch können auch aktuelle KI-Anwendungen auf Constellation geschützt ausgeführt werden.
- Bereitstellung eines Proxys zur automatischen Ver- und Entschlüsselung von Cloud-Speichern wie S3; hierdurch wird es möglich, von der Kosteneffizienz und den Skalierungsmöglichkeiten von Cloud-Speicher zu profitieren.
- Ende-zu-Ende-Absicherung der Software-Supply-Chain mit Hilfe des Projekts Sigstore[3]: Alle Softwarekomponenten von Constellation werden kryptographisch signiert und die entsprechenden Signaturen in einem einsehbaren, verteilten und fälschungssicheren Log namens „Rekor“ abgelegt. Konzeptuell spricht hier auch von einem „Transparency Log“. Rekor wird von verschiedenen reputablen Parteien wie der Linux Foundation betrieben. Constellation kombiniert diesen Transparency Log mit der sog. „Remote Attestation“[4] der TEEs. Dadurch kann automatisiert sichergestellt werden, dass immer nur genau die gewünschte und erwartete Softwarekomponenten von Constellation verwendet werden. Diese Kombination ist ein neuartiger Ansatz und stellt einen Meilenstein in der Abwehr von Supply-Chain-Angriffen dar.

3.2 TEEs im Zusammenhang mit PPC-Verfahren (AP 4)

Ursprünglich sollte hier eine Integration der SDC-Lösung von Aircloak stattfinden. Stattdessen wurde die vom Projektpartner Bosch entwickelte Plattform CarbyneStack erfolgreich auf Constellation in herkömmlichen Cloud-Umgebungen zum Laufen gebracht und getestet. Die Kombination lieferte herausragende Eigenschaften für PPC-Anwendungen, welche näher von Bosch evaluiert und dokumentiert wurden.

3.3 Prüfung, Implementierung und erste Auswertung der TEE-Technologie innerhalb der PPC-Plattform (AP 5)

Es wurden umfangreiche Benchmarks mit Constellation von Edgeless Systems durchgeführt. Das Ergebnis ist, dass Anwendungen wie HashiCorp Vault auf Constellation nahezu die gleiche Leistung wie auf ungeschützten Kubernetes-Plattformen erzielen können. In üblichen Szenarien wird die Latenz von Anwendungen durch Constellation um weniger als 5% negativ beeinflusst[5].

[3] https://www.sigstore.dev/
[4] https://www.edgeless.systems/wiki/what-is-confidential-computing/remote-attestation
[5] https://docs.edgeless.systems/constellation/overview/performance/application

3.4 Umsetzung und Validierung der Pilotanwendungen (AP 6)

Es wurden unterschiedliche Pilotanwendungen mit den Projektpartnern Bosch und Orange diskutiert. Schlussendlich wurden von Seiten Edgeless Systems hier keine weiteren technischen Arbeiten neben den bereits unter 3.2 beschriebenen durchgeführt.

4 Verwertbarkeit der Ergebnisse

Die Ergebnisse sind sehr gut wirtschaftlich verwertbar. Edgeless Systems vertreibt bereits erfolgreich eine „Enterprise"-Version von Constellation, die in unterschiedlichen Szenarien produktiv zum Einsatz kommt. Dazu gehört u.a. die Bereitstellung einer sicheren Cloud-Umgebung für ein großes deutsches Krankenhaus[6].

5 Bekanntgewordene Ergebnisse Dritter

Während der Projektlaufzeit wurden vereinzelt relevante Ergebnisse von Dritten bekannt. Dies betraf im Wesentlichen das Projekt „Confidential Containers"[7] der Cloud Native Computing Foundation (CNCF), welches einen ähnlichen Ansatz und ähnliche Ziele wie Constellation verfolgt. Jedoch gibt es wichtige Unterschiede: Nur mit Constellation können ganze Kubernetes-Cluster abgeschirmt und Anwendungen per „Lift & Shift" ohne Anpassungen migriert werden. Zudem ist das Projekt Confidential Containers auch Ende 2024 weiterhin nicht für den Produktiveinsatz geeignet.

6 Geplante und erfolgte Veröffentlichungen der Ergebnisse

Alle entwickelten Komponenten wurden zusammen mit ihrer Dokumentation als Open-Source unter https://github.com/edgelesssys/constellation bereitgestellt. Zudem wurden die Ergebnisse auf den folgenden Konferenzen präsentiert:

- KubeCon North America 2023, Salt Lake City: From Threats to Trust: Safeguarding Sensitive Data in K8s
- Open Confidential Computing Conference 2023, online: Always-encrypted, confidential Kubernetes with Constellation
- Open Source Summit Europe 2023, Bilbao: Kubernetes Meets Confidential Computing – The Different Ways of Scaling Sensitive Workloads

[6] https://www.edgeless.systems/resource-library/uniklinik-freiburg
[7] https://github.com/confidential-containers