Sachbericht der Siemens AG zum Teilvorhaben „Generische Anwendungs-Schnittstelle für Trust Anchor zur Sicherstellung der Vertrauenswürdigkeit entlang der Lieferkette“

-

Teil I: Kurzbericht

Das diesem Bericht zugrundeliegende Vorhaben wurde eingereicht durch den Verbund mit Nummer 16ME0259 im Rahmen der Ausschreibung des Bundesministeriums für Bildung und Forschung (BMBF) zur Förderung von Forschungsvorhaben für „Vertrauenswürdige Elektronik (ZEUS)“

Förderkennzeichen: 16ME0259
Vorhabenbezeichnung: VE-FIDES: Knowhow-Schutz und Identifizierbarkeit von Elektronikkomponenten für vertrauenswürdige Produktionsketten
Teilvorhaben: Generische Anwendungs-Schnittstelle für Trust Anchor zur Sicherstellung der Vertrauenswürdigkeit entlang der Lieferkette
Laufzeit des Vorhabens: 01.03.2021 – 31.12.2024

Autor und Projektleiter des Teilvorhabens:

Daniel Schneider
Siemens AG
FT RPD CST SES-DE
Otto-Hahn-Ring 6, 81739 München
Telefon: +49 152 22591409
E-Mail: schneider.ds.daniel@siemens.com

1 Ursprüngliche Aufgabenstellung und Ausgangslage

Die globale Produktion elektronischer Komponenten stellt Unternehmen vor die Herausforderung, die Vertrauenswürdigkeit ihrer Produkte entlang der gesamten Lieferkette sicherzustellen. Zu Projektbeginn existierten keine standardisierten Methoden, um Fälschungen oder Manipulationen an elektronischen Komponenten zuverlässig auf einem industriellen Gerät zu erkennen. Das Teilvorhaben adressierte diese Problemstellung durch die Entwicklung einer generischen Schnittstelle zur Integritätsprüfung der verbauten Komponenten auf einem industriellen Gerät.

2 Ablauf des Vorhabens

Die Siemens AG war als Verbundkoordinator für die Gesamtprojektkoordination verantwortlich und beteiligte sich an zwei wesentlichen Arbeitspaketen. Im Rahmen von AP1 wurden die Vertrauenswürdigkeit entlang der Lieferkette definiert, die Anwendung am Tachographen-System unterstützt und relevante Sicherheitsstandards analysiert. Der technische Schwerpunkt lag in AP4, wo eine Trust Anchor API für Secure Elements entwickelt und ein Demonstrator zur Validierung der Konzepte implementiert wurde. Die Projektdurchführung erfolgte in enger Abstimmung zwischen allen Partnern durch regelmäßige Projekttreffen. Durch kontinuierliche technische Reviews und Abstimmungen wurde die Qualität der Entwicklungen sichergestellt. Ein Highlight zum Ende des Projektes war die Organisation eines öffentlichen Workshops bei der Siemens AG in München, bei dem die Projektergebnisse einem breiten Fachpublikum vorgestellt wurden.

3 Wesentliche Ergebnisse

Im Rahmen des Projekts wurden folgende Hauptergebnisse erzielt:

- Entwicklung eines umfassenden Sicherheitskonzepts zur Verbesserung der Vertrauenswürdigkeit elektronischer Komponenten, das sowohl die Produktion als auch die gesamte Lieferkette berücksichtigt.
- Implementierung einer generischen Trust Anchor API, die die sichere Kommunikation zwischen Host-System und Secure Element ermöglicht und dabei verschiedene Sicherheitsmechanismen unterstützt. Die API wurde dabei

so gestaltet, dass sie flexibel an unterschiedliche Anwendungsszenarien angepasst werden kann.

- Realisierung eines funktionsfähigen Demonstrators, der die praktische Anwendbarkeit der entwickelten Konzepte zur Erkennung von Manipulationen und zur Sicherstellung der Hardware-Integrität validiert. Der Demonstrator basiert auf einem SIMATIC IOT2050 als Host-System und zeigt die erfolgreiche Integration aller entwickelten Komponenten.
- Erfolgreiche Publikation und Präsentation der Forschungsergebnisse auf der DATE-Konferenz 2023, was die wissenschaftliche Relevanz der entwickelten Lösungen bestätigt.
- Im Rahmen der Entwicklungsarbeiten entstanden mehrere Erfindungsmeldungen, die verschiedene innovative Aspekte der Hardware-Sicherheit adressieren und die technologische Bedeutung der Projektergebnisse unterstreichen.

4 Zusammenarbeit mit Forschungseinrichtungen

Die Entwicklung und Validierung der Konzepte erfolgte in Zusammenarbeit mit verschiedenen Projektpartnern. Mit der Technischen Universität München wurde die Integration von Secure Elements vorangetrieben, was die Basis für den entwickelten Demonstrator bildete. Durch den regelmäßigen Austausch im Projektkonsortium konnten unterschiedliche Perspektiven und Expertisen eingebracht werden, was die Qualität der Ergebnisse maßgeblich förderte. Die etablierten Kooperationsstrukturen bilden eine solide Grundlage für zukünftige Forschungsaktivitäten im Bereich der Hardware-Sicherheit und Lieferketten-Integrität.

5 Ausblick und Verwertung

Die entwickelten Konzepte und Implementierungen bilden eine solide Basis für die weitere Industrialisierung von Methoden zur Absicherung elektronischer Lieferketten. Ein öffentlicher Workshop bei der Siemens AG in München zum Projektende ermöglichte den Wissenstransfer der Projektergebnisse an ein breites Fachpublikum und unterstrich das große Interesse der Industrie und Forschung an den entwickelten Lösungen. Die erarbeiteten Schutzrechte und Standards sichern dabei die nachhaltige Nutzung und Weiterentwicklung der Projektergebnisse.