Schlussbericht des Verbundprojekts

ALESSIO für die Siemens AG

Das diesem Bericht zugrundeliegende Vorhaben wurde mit Nummer 16KIS0631 im Forschungsrahmenprogramm der Bundesregierung zur IT-Sicherheit „Selbstbestimmt und sicher in der digitalen Welt“ auf die Ausschreibung des Bundesministeriums für Bildung und Forschung (BMBF) zur Förderung von Forschungsinitiativen auf dem Gebiet der „Hightech für IT-Sicherheit“ im Rahmen des Förderprogramms „IKT 2020 – Forschung für Innovationen“ eingereicht.

ALESSIO

Architektur für **l**angfristig**e** **S**icherheit durch **S**ecure Elements mit Update-Funkt**io**n

Förderkennzeichen: 16KIS0631

Vorhabenbezeichnung: ALESSIO

Laufzeit des Vorhabens: 01.01.2017 – 31.12.2019

Autor: Dr. Fabrizio De Santis

Kurzdarstellung des Vorhabens

In vielen Industrieanwendungen wie Industriesteuerungen, Antriebsteuerungen oder in der Fertigungsautomatisierung und allgemein bei kritischen Infrastrukturen ist die Sicherheit von Lösungen und Komponenten ein hohes Schutzziel und solllangfristig über viele Jahren garantiert werden. Aufgrund der hohen und zunehmenden Komplexität von eingebetteten Systemen ist es oft ratsam, die notwendige kryptografischen Funktionen zur Gewährleistung der Informationssicherheit in sogenannte Hardware Secure Elements (HSEs) zu kapseln. Ein HSE ist ein hochsicheres, nicht unbedingt Update-fähiges, kryptografisches Modul, das in verschiedenen Technologieausprägungen implementiert werden kann und dem sicheren Speichern von Schlüsselmaterialen und Zertifikaten sowie der sicheren Ausführung von kryptographischen Algorithmen dient. So gelingt es, ein eingebettetes System auf Basis eines mit hoher Sorgfalt gehärteten HSE abzusichern und die Angriffsfläche des Systems möglichst gering zu halten. Trotzdem zeigt die Erfahrung, dass die Sicherheit eines Systems über die Dauer aufgrund der Entstehung neuer Angriffsmethoden abnimmt. Bei Industrieanwendungen ist es besonders oft der Fall, dass die Sicherheit von Produkten mit einem Zeithorizont von mehreren Jahrzehnten garantiert werden muss. Aufgrund dessen und weil sich selbst die erforderlichen kryptografischen Funktionen eines Sicherheitselements über die Zeit ändern können, war es das Ziel des zugrundeliegenden Vorhabens, zu untersuchen, wie eine langfristige Sicherheit von eingebetteten Systemen für Industrieanwendungen in kritischen Infrastrukturen erreicht werden kann, indem ein Secure Element mit einem integrierten sicheren Update-Mechanismus ausgestattet wird.

Aufgabenstellung

Im Rahmen des ALESSIO-Projekts wurden zwei Ansätze zur Aktualisierung eines SEs erforscht:

1. Sicheres Element als dedizierter ASIC-Chip mit aktualisierbarer Firmware (ASIC-SE);
2. Sicheres Element als rekonfigurierbarer FPGA-Chip mit aktualisierbaren Hardware-Komponenten (FPGA-SE).

Das Ziel des Gesamtvorhabens war, eine lange Laufzeit der Geräte im Feld und sich ändernde Umstände, wie beispielsweise die Notwendigkeit von zusätzlichen Sicherheitsfunktionen, zu berücksichtigen.

Der Fokus der Siemens Arbeit lag speziell auf der Konzepterarbeitung, Integration und Analyse eines Secure Elements mit sicherer Update-Funktion auf Basis einer FPGA-basierten System-On-a-Chip-Plattform (FPGA-SoC), die eine Aktualisierung des FPGA-basierten Secure Elements zur Laufzeit ermöglicht.

Zuerst wurden die Anforderungen an ein Secure Element im industriellen Kontext erarbeitet. Anschließend wurde die Sicherheitsarchitektur eines Secure Elements mit sicherem Update-Mechanismus konzipiert und das Basis-System protypisch im FPGA implementiert. Das daraus resultierende Update-fähige FPGA-basierte Secure Element wurde über das vorhandene Bussystem an die Haupt-CPU des FPGA-SoCs angeschlossen und in ein Linux-basiertes System auf der Software-Seite integriert. Des Weiteren wurden sowohl Software-Angriffe als auch physische nicht invasive Fehlerangriffe auf das FPGA-basierte Secure Element durchgeführt, die dazu dienten, zusätzliche Kontrollmechanismen zu konzipieren, die zum Schutz vor Laufzeitmanipulationsangriffe beitragen. Anschließend wurden die von den Partnern entwickelten kryptografischen Komponenten zur gerätespezifischen Schlüsselgenerierung und zur seitenkanalsicheren Entschlüsselung in das FPGA-basierte Secure Element integriert und in einem industriellen Szenario mit einem Demonstrator veranschaulicht.

Voraussetzungen unter denen das Vorhaben durchgeführt wurde

Das Technologiefeld „Cybersecurity Technology“ war bzw. ist in Forschungsprojekten beteiligt, in denen Sicherheitsarchitekturen und Lösungen in unterschiedlichen industriellen Anwendungsgebieten mit Bezug zu eingebetteten Systemen untersucht werden. Erfahrungen und Erkenntnisse aus diesen Projekten unterstützen die Arbeiten des Verbundvorhabens ALESSIO. Zum Beispiel wurden im EU Projekt IoT@Work (IoT@Work, 2010-2013) Sicherheitsarchitekturen für IoT-basierte Plug&Work

Szenarien in der industriellen Automatisierung konzeptioniert (Fischer, Gessner, & Fries, 2012) (Fischer & Gessner, Security architecture elements for IoT enabled automation networks, 2012). Im EU-Projekt RERUM (RERUM, 2013-2016) wurden Konzepte zum Schutz der Sicherheit und Privacy von IoT-basierten Sensoren und Systemen im Kontext von Smart Cities erforscht (Pöhls, et al., 2014). Im BMBF Projekt SIBASE wurden Security-Anforderungen, -Bausteine und -Architekturen für sichere eingebettete Systeme der nächsten Generation entwickelt (Fischer, Mucha, Hess, & Reiss, 2017). Im BMBF Projekt IUNO wurde das Entwurfsprinzip „Security by Design“ für Industrie 4.0 Geräte umgesetzt, von der Security-Analyse, über die Definition von Anforderungen, bis hin zur Erarbeitung einer Sicherheitsarchitektur und der letztendlichen prototypischen Erprobung in Demonstratoren (IUNO, 2015-2018).

Planung und Ablauf des Vorhabens

Das ALESSIO Projekt war in sieben Arbeitspakete gegliedert:

- AP1: Koordination und Steuerung
- AP2: Anforderungen und Spezifikation
- AP3: Hardware-Architektur für integre, Update-fähige Systeme
- AP4: Hardwarebasierte Softwaresicherheit
- AP5: Sicherheitsanalysen, Angriffsmethoden, und Vergleich der unterschiedlichen Architekturen
- AP6: Demonstrator Implementierungen
- AP7: Verbreitung und Standardisierung der Ergebnisse

Siemens beteiligte sich an folgenden (Teil-)Arbeitspakten:

- AP2: Anforderungen und Spezifikation
- AP3: Hardware-Architektur für integre, Update-fähige Systeme
    - AP3.1: Entwicklung neuer Generation von Sicherheitsarchitekturen
    - AP3.4: Entwicklung des Basis-Systems für ein FPGA-SE
    - AP3.6: Integration von Basis-System, Funktionsblöcken und Software
- AP4: Hardwarebasierte Softwaresicherheit
    - AP4.4: Sicheres FW/SW Update

    - AP4.6: Verzahnte Sicherheitslösungen durch HW/SW Co-Design
- AP5: Sicherheitsanalysen, Angriffsmethoden, und Vergleich der unterschiedlichen Architekturen
    - AP5.1: Methodik und Werkzeuge für Software-Sicherheitsanalysen
    - AP5.2: Fehlerangriffe auf Sichere Elemente
    - AP5.5: Vergleichende Untersuchung der Lösungen
- AP6: Demonstrator Implementierungen
    - AP6.1.1: Aufbau der Demonstrator-Umgebung
    - AP6.1.2: Integration der Projektergebnisse

Die Arbeiten im Teilvorhaben lieferten Ergebnisbeiträge zu folgenden Meilensteinen:

M12

- Anforderungsspezifikation für Secure Elements im industriellen Umfeld

M24

- Hardware-Architektur für FPGA-basiertes Secure Element
- Konzept zur Integration eines FPGA-basierten Secure Elements in Software

M36

- Lauffähige Hardware-Konfiguration des FPGA-basierten SE
- Treiber und Software API für FPGA-SE
- Sicherheitsanalyse eines Systems mit FPGA-basiertem Secure Element
- Demonstrator für FPGA-basiertes Secure Element in industriellem Szenario

Wissenschaftlicher und technischer Stand zu Beginn des Vorhabens

Seit wenigen Jahren sind FPGA-basierte System-on-Chip-Plattformen (FPGA-SoC) auf dem Markt verfügbar[1,2], die sich besonders gut für bestimmte eingebettete

[1] http://www.xilinx.com/products/silicon-devices/soc/zynq-7000.html
[2] https://www.altera.com/products/soc/portfolio/cyclone-v-soc/overview.html

Anwendungen eignen, weil sie auf der einen Seite eine reguläre moderne CPU zur einfachen Umsetzung eines eingebetteten Systems (z.B. ARM Cortex-A Prozessor), auf der anderen Seite ein FPGA für die Unterstützung bei besonders rechenintensiven, zeit- oder sicherheitskritischen Aufgaben, zur Verfügung stellen.

Die Umsetzung eines im FPGA-Teil isolierten und gleichzeitig zur Laufzeit aktualisierbaren Secure Elements unter Anwendung eines Soft-CPU Prozessors (Wikipedia, 2020) auf einer FPGA-SoC-Plattform war bis zum Start des Projekts neu. Die Herausforderung lag hier in der sicheren Implementierung der Schaltungen im FPGA, die Absicherung der Nachladbarkeit des FPGA-Bitstromes und die HW/SW-Partitionierung bzw. Isolierung zwischen dem FPGA-SE und der anderen Software und Hardware-Komponenten.

Zusammenarbeit mit anderen Stellen

Im Projekt ALESSIO gab es über die gesamte Laufzeit einen kontinuierlichen Austausch und eine enge Zusammenarbeit mit den Partnern. Im Speziellen erfolgte eine Konsortium übergreifende Zusammenarbeit in AP2 für die Spezifikation der Anforderungen und der zu erforschenden Lösungen für die Aktualisierbarkeit eines Secure Elements im industriellen Umfeld. In AP3 und AP6 erfolgte eine Zusammenarbeit mit den Partnern Fraunhofer AISEC und TU München während der Entwicklung und Integration der unterliegenden kryptografischen Komponenten des FPGA-basierten Secure Elements und während des Aufbaus des FPGA-Demonstrators. Außerdem erfolgte über die gesamte Laufzeit des Projekts ein regelmäßiger Austausch mit allen Partnern remote, sowie vor Ort auf AP-spezifischen und AP-übergreifenden Workshops.

Eingehende Darstellung

Verwendung der Zuwendung und erzielte Ergebnisse im Einzelnen mit Gegenüberstellung der vorgegebenen Ziele

Ziel der Siemens AG war die Erarbeitung von FPGA-basierten Secure Elements von der Definition der Anforderungen, über das Konzept der Sicherheitsarchitektur und die Implementierung eines Basis-Systems, die Integration der von den Partnern

gelieferten Teil-Komponenten, die Evaluierung von logischen und physischen Angriffsmethoden, bis hin zur prototypischen Erprobung in einem Demonstrator.

Zu Beginn des Projekts wurden Anforderungen definiert, die ein Secure Element im industriellen Umfeld, z.B. für IEC62443, erfüllen muss (AP2). Anschließend wurde eine Sicherheitsarchitektur mit der Möglichkeit einer sicheren Aktualisierung der SE-Komponenten entworfen, die sowohl die nötigen FPGA Module als auch das Gesamtsystem aus Hardware und Software betrachtet (AP3). Des Weiteren wurde ausgearbeitet, wie sich ein FPGA Secure Element in ein eingebettetes System mit Linux Betriebssystem integrieren lässt, welche Schutzmöglichkeiten sich dadurch für Betriebssystem und Applikationen ergeben und welchen Einfluss die Update-Fähigkeit auf das Gesamtsystem hat (AP4). Um Angriffsmöglichkeiten besser abzuschätzen und mögliche Gegenmaßnahmen erarbeiten zu können, wurden zusätzlich sowohl logische Software-Manipulationsangriffe als auch physische nicht invasive Fehlerangriffe auf dem FPGA-SE untersucht. Des Weiteren wurden Integritätsschutzmechanismen der FPGA-Konfiguration vor Manipulations- und Fehlerangriffe während des normalen FPGA-Betriebes erarbeitet (AP5). Die gewonnen Erkenntnisse flossen in eine Demonstrator-Implementierung ein (AP6).

Im Folgenden wird auf die Arbeiten in den einzelnen Unterarbeitspaketen detaillierter eingegangen.

AP2: Anforderungen und Spezifikation

In diesem Arbeitspaket wurden die Anforderungen für den Einsatz von Secure Elements im industriellen Umfeld erarbeitet. Ein besonderes Augenmerk wurde auf die langfristige Sicherheit und den Bedarf an Aktualisierungen der Sicherheitsfunktionen bzw. der kryptografischen Funktionen des Secure Elements gelegt. Insbesondere wurden Use Cases für den langfristigen Einsatz von Secure Elements und deren Aktualisierung im Feld erarbeitet und das damit verbundene Produktlebenszyklus-Management, wie z.B. die notwendigen Abläufe zur Aktualisierung des Secure Elements in industriellen Automatisierungsanlagen, berücksichtig. Der Fokus lag speziell auf der Notwendigkeit von Sicherheitsupdates und deren Anwendung auf Secure Elements unter verschiedenen Randbedingungen. Des Weiteren wurden die Vorgaben der einzelnen Standards von (ISA/IEC 62443: Security for Industrial

Automation and Control Systems, 2007-2018) durchgearbeitet, um Anforderungen von Sicherheitsupdates in der industriellen Produktion aus der Sicht von ISA/IEC 62443 zu identifizieren. Die resultierenden Ergebnisse der Anforderungsanalyse dienten als Basis für die Arbeiten in den darauffolgenden Arbeitspaketen.

Ergebnisbeitrag:

- M12: Anforderungsspezifikation für Secure Elements im industriellen Umfeld

AP3.1: Entwicklung neuer Generation von Sicherheitsarchitekturen

Ziel dieses Arbeitspakets war die Erarbeitung einer Sicherheitsarchitektur für die Implementierung eines FPGA-basierten Secure Elements (FPGA-SE) in der konfigurierbaren FPGA-Logik einer FPGA-basierten System-on-Chip-Plattform (FPGA-SoC) mit integrierter Haupt-CPU (z.B. ARM Cortex-A basierter Prozessor). Diese Architektur wurde auf Basis einer Soft-CPU zur flexiblen Gestaltung von im Secure Element gekapselten kryptographischen Komponenten entworfen. Ein wichtiger Punkt dabei war die Aufteilung der Sicherheitsfunktion zwischen der Haupt-CPU und dem FPGA-SE inklusive der Aufteilung von kryptografischen Modulen, der Soft-CPU, deren Firmware und dem sicheren Update-Mechanismus. Dafür wurde eine Soft-CPU als Kern des Secure-Elements genommen, mit dem Ziel, zum einen die Steuerungsaufgaben der kryptografischen Funktionalität des Secure Elements zu übernehmen, zum anderen eine Isolation zwischen der Haupt-CPU und der kryptografischen Module zum Schutz vor Angriffe auf die kryptografische Module zu realisieren. Insbesondere war die Aufgabe der Soft-CPU die Orchestrierung der kryptografischen Module innerhalb des FPGA-SEs (z.B. um ein sicheres Update des FPGA-SEs durchzuführen) und die Realisierung von Schutz- und Kontrollmechanismen zum Schutz vor Manipulationsangriffe auf die kryptografischen Module des FPGA-SEs, die sonst aufwändig und fehleranfällig in Hardware zu implementieren wären. Für die Auswahl der Soft-CPU wurden zunächst Kriterien wie u.a. Aktualisierbarkeit, Lizenz, Programmiersprache, Tools und Community-Unterstützung identifiziert. Danach wurden verschiedene Soft-CPU Implementierungen nach den identifizierten Kriterien bewertet und daraus wurde die Zylin Processing Unit (ZPU) Soft-CPU (Harboe, 2020) als Kandidat ausgewählt. Über

die Soft-CPU erfolgt eine Trennung zwischen der Haupt-CPU und den sicherheitskritischen Komponenten, die an der ZPU angeschlossen sind. Diese Trennung bietet einen Schutz vor Angriffen, die über die Haupt-CPU durchgeführt werden können. Außerdem unterstützt die Sicherheitsarchitektur des FPGA-SEs einen sicheren Mechanismus zur Aktualisierung von Hardware- und Firmware-Komponenten auf dem FPGA über eine sichere partielle Rekonfiguration der FPGA-Logik (Lie & Feng-yan, 2009). Zwei besondere Vorteile dieses Aktualisierungsverfahrens sind:

1. Die Aktualisierung des FPGA-SEs kann zur Laufzeit durchgeführt werden, ohne Unterbrechung des Betriebs einer industriellen FPGA-basierten Steuerung, (auf English: „Live Patching“);
2. Die Aktualisierung des FPGA-SEs kann zur Laufzeit durchgeführt werden, ohne auf die vom FPGA-Hersteller zur Verfügung gestellten – nicht aktualisierbaren - kryptografischen Mechanismen zurückzuzugreifen, wobei diese eventuell zusätzlich in Kombination dazu verwendet werden können.

Ergebnisbeitrag:

- M24: Hardware-Architektur für ein FPGA-basiertes Secure Element
- M24: Konzept zur Integration eines FPGA-basierten Secure Elements in Software

AP3.4: Entwicklung des Basis-Systems für ein FPGA-SE

In dem Arbeitspaket wurde die im AP3.1 erarbeitete Sicherheitsarchitektur des FPGA-basierten Secure Elements (FPGA-SE) umgesetzt und das Basis-System prototypisch auf einem Xilinx Zynq-7020 FPGA-SoC-Plattform (Xilinx, 2020) implementiert und getestet. Zunächst wurde die ZPU Soft-CPU zum Laufen gebracht und soweit angepasst, dass auf der einen Seite die Konnektivität zu der Haupt-CPU über ein Bus-/Interconnect-System (AXI-Bus) hergestellt wird und auf der anderen Seite der Anschluss der kryptografischen Module über ein zweites Bus-System (Wishbone-Bus) des FPGA-SEs ermöglicht wird. Des Weiteren wurde eine Firmware für die Soft-CPU entwickelt, um die Nachrichten von der Haupt-CPU über das Bus-/Interconnect-System entgegenzunehmen, zu validieren und verarbeiten und die Steuerung der gesamten FPGA-SE-Funktionalität zu orchestrieren. Zu Testzwecken wurde dazu ein

physikalischer Zufallszahlengenerator (auf English: True Random Number Generator, TRNG) implementiert (Dichtl & Golić, 2007) und die Qualität der gelieferten Output-Zufallszahlen erfolgreich getestet. Ein Prototyp dieser Implementierung wurde an die Projektpartner im Laufe des Projekts übermittelt. Anhand des von den Partnern gelieferten Feedbacks zur besseren Integration deren kryptografischer Module wurden weitere Verbesserungen an der Busarchitektur vorgenommen. Dadurch wurde die Performance des FPGA-SEs deutlich verbessert.

Ergebnisbeitrag:

- M24: Hardware-Architektur für ein FPGA-basiertes Secure Element
- M24: Konzept zur Integration eines FPGA-basierten Secure Elements in Software
- M36: Implementierung der Basiskomponenten eines FPGA-basierten Secure Elements

AP3.6: Integration von Basis-System, Funktionsblöcken und Software

In diesem Arbeitspaket wurden die von den Partnern gelieferten kryptografischen Module zur gerätespezifischen Schlüsselgenerierung unter Verwendung einer Physical Unclonable Function (PUF) (Suh & Devadas, 2007), (Meng-Day, 2010) und zur seitenkanalsicheren authentifizierten Entschlüsselung unter Verwendung einer Leakage-Resilient Pseudo-Random Function (LRPRF) (Medwed, Standaert, & Joux, 2012), (Unterstein, Heyszl, De Santis, Specht, & Sigl, 2018) in das in AP3.4 entwickelte FPGA-SE integriert. Insbesondere wurden die kryptografischen Module per Bus-System an die Soft-CPU des FPGA-SEs angebunden. Weiterhin wurde das FPGA-SE per Bus-System an die fest verankerte Haupt-CPU des FPGA-SoCs angeschlossen, um ein Kommunikationskanal zwischen dem auf dem Haupt-CPU laufenden Linux Betriebssystem und dem FPGA-SE herzustellen. Anschließend wurde die Firmware der Soft-CPU erweitert, um anhand der von den Partnern gelieferten kryptografischen Komponenten ein sicheres Update des FPGA-SEs durchzuführen und das FPGA-SE von der Linux-Seite zu bedienen. Zum Schluss wurde das resultierende FPGA-SE mit Update-Funktion unter verschiedenen Randbedienungen, wie z.B.

Temperaturveränderungen und CPU-Auslastung, mit speziellem Fokus auf der Stabilität des PUF- und TRNG-Verhaltens mit Erfolg getestet.

Ergebnisbeitrag:

- M24: Hardware-Architektur für ein FPGA-basiertes Secure Element
- M24: Konzept zur Integration eines FPGA-basierten Secure Elements in Software
- M36: Lauffähige Hardware-Konfiguration des FPGA-basierten SE

AP4.4: Sicheres FW/SW Update

Ziel der Arbeiten in diesem Arbeitspaket war die Klärung von praktischen Fragen bzgl. des Aktualisierungsprozesses eines FPGA-SEs. Ist immer ein Neustart des kompletten Systems erforderlich, um das aktualisierte FPGA-SE verwenden zu können? Im Rahmen des Arbeitspakets wurde die Frage negativ beantwortet, in dem geklärt wurde, dass die vom FPGA-Hersteller vorhandenen Mechanismen zur partiellen Re-Konfigurationen der FPGA-Logik zur Aktualisierung des FPGA-SEs während des normalen Betriebes des FPGA-SEs, also zur Laufzeit, angestoßen und vom FPGA-SE selbst orchestriert werden können. Somit ist kein Neustart des kompletten Systems notwendig. Wer kann eine Aktualisierung starten? Im Rahmen des Arbeitspakets wurden Zugriffe auf das FPGA-SE zum Starten einer Aktualisierung bzw. Benutzung des FPGA-SEs sowohl über die herkömmlichen schon vorhandenen Berechtigungsmechanismen des Linux-Systems als auch mit einer dedizierten Authentifizierungsmechanismus über das FPGA-SE selbst beschränkt. Wie sollten Sicherheitsanwendungen reagieren während das FPGA-SE nicht zur Verfügung steht? Im Allgemeinen sind Secure Elements eine beschränkte Ressource, auf die nur sequenziell zugegriffen werden kann. Um dies zu abstrahieren wurde ein primitiver Ressourcemanager benutzt, der ein Scheduling der Zugriffe vornimmt. Zusätzlich teilte das FPGA-SE über dessen Treiber einer Applikation durch unterschiedliche Fehlercodes mit, ob ein Zugriff nur temporär nicht funktioniert oder ob ein genereller Fehler aufgetreten ist (z.B. EBUSY, EAGAIN). Müssen Maßnahmen getroffen werden, die im Fall einer fehlgeschlagenen Aktualisierung das System in einen sicheren Zustand versetzen? Im Rahmen des Arbeitspaket wurden Fallback-Mechanismen

eingesetzt um bei einem fehlgeschlagenen Update, den vorherigen Zustand wiederherzustellen.

Ergebnisbeitrag:

- M24: Hardware-Architektur für ein FPGA-basiertes Secure Element
- M24: Konzept zur Integration eines FPGA-basierten Secure Elements in Software

AP4.6: Verzahnte Sicherheitslösungen durch HW/SW Co-Design

In diesem Arbeitspaket wurden Konzepte und Linux-Software entwickelt, um das FPGA-SE von Linux-Programmen auf der Haupt-CPU verwendbar zu machen. Insbesondere wurden ein Linux Kernel Treiber und eine Linux User Space API für die Verwendung des FPGA-SEs unter Linux konzipiert und umgesetzt, um die im AP3 integrierten kryptografischen Module des FPGA-SE auf einem Linux-System unter verschiedenen Randbedienungen zu testen. Im Rahmen des Arbeitspakets wurden verschiedene Aufteilungsmöglichkeiten für HW/SW Co-Design und deren Vor- und Nachteile gegenübergestellt. Daraus stellte sich klar, dass die Orchestrierung der kryptografischen Module und des Update-Mechanismus durch eine Soft-CPU der beste Kompromiss zwischen Sicherheit und Performance war, um zum einen das FPGA-SE von der Linux-Seite verfügbar zu machen, und zum anderen um die Benutzerkomplexität weg zu abstrahieren, in dem nur hohe Abstraktionsbefehle von der Linux-Seite benötigt werden. Dieser HW/SW-Aufteilungsansatz half die Angriffsfläche des FPGA-SEs sehr gering zu halten, da nur wenige sehr primitive Befehlen an das FPGA-SE übermittelt werden, die von der Soft-CPU zusätzlich validiert werden. Um die Kommunikation zwischen dem FPGA-SE und dem Linux-System möglichst performant und einfach zu realisieren, wurden FIFO Input/Output Mechanismen dazu gebaut, um den Input/Output Dataverkehren zu regeln.

Ergebnisbeitrag:

- M24: Hardware-Architektur für ein FPGA-basiertes Secure Element
- M24: Konzept zur Integration eines FPGA-basierten Secure Elements in Software

- M36: Treiber und Software API für FPGA-SE

AP5.1: Methodik und Werkzeuge für Software-Sicherheitsanalysen

In diesem Arbeitspaket wurde untersucht, welche logischen Software-Angriffe das entwickelte FPGA-SE aushebeln können. Im Rahmen dieses Arbeitspakets wurde eine Bedrohungsanalyse des FPGA-SEs durchgeführt, die dazu diente, die im AP3 und AP4 entwickelte Firmware der Soft-CPU und den Linux-Kernel Treiber der Haupt-CPU mit zusätzlichen Sicherheits- und Kontrollschutzmechanismen zu erweitern. Insbesondere wurden HW/SW-Integritätsschutzmechanismen zur Sicherstellung der Integrität des FPGA-SEs zur Laufzeit erarbeitet, um die FPGA-Konfiguration auch während des Betriebes vor Manipulationsangriffe zu schützen.

Ergebnisbeitrag:

- M36: Sicherheitsanalyse eines Systems mit FPGA-basiertem Secure Element

AP5.2: Fehlerangriffe auf Sichere Elemente

In diesem Arbeitspaket wurde untersucht, welches Angriffspotential sich hinter nicht-invasiven Angriffsmethoden verbirgt und wie man ein FPGA-SE ggf. besser davor schützen könnte. Dieses Szenario war speziell interessant, da Angreifer mit diesen Methoden einfach und ohne chemische oder mechanische Manipulation des FPGAs Angriffe durchführen könnten. Zunächst wurde anhand der Literatur ein Überblick über die aktuellen Bedrohungen durch Fehlerangriffe gewonnen. Danach wurden erfolgreich Fehlerangriffe mit einem billigen Elektromagnetischen-Pulsgerät auf die SRAM-Speicherzellen durchgeführt, die die Konfiguration eines FPGAs zur Laufzeit definieren. Es gelang, die durch Lookup-Tables repräsentierte Funktion logischer Gatter durch elektromagnetische Impulse zu verändern. Da bei diesem Angriff die Lookup-Table verändert wird, bleibt die Veränderung bis zu einem Neustart des Systems erhalten. Es wurde auch ein Verfahren entwickelt, das es ermöglicht, derartige Angriffe zu erkennen. Außerdem wurde ein Test-Framework zur Simulation von Fehlerangriffen für FPGA-Systeme prototypisch entwickelt.

Ergebnisbeitrag:

- M36: Sicherheitsanalyse eines Systems mit FPGA-basiertem Secure Element

AP5.5: Vergleichende Untersuchung der Lösungen

In diesem Arbeitspaket wurden unterschiedliche Architekturen für Update-fähige Secure Elements (dedizierte Sicherheitschips und FPGA-basierte SEs) gegenübergestellt. Im Speziellen wurde darauf eingegangen und dargestellt, welche Formen von Updates – beispielsweise Hardware-Teile eines FPGA-basierten SE, oder hauptsächlich die Firmware des SEs – für die langfristige Sicherheit in den Anwendungen jeweils am zweckmäßigsten ist. Der Fokus wurde speziell auf die Sicherheitsfeatures hochmoderner FPGA-SoC-Plattformen gelegt, und Produkte von verschiedenen Anbietern verglichen. Neben Sicherheitseigenschaften wurden auch Zertifizierbarkeit, Kosten, Tools und Community-Unterstützung in den Vergleich mit einbezogen.

Ergebnisbeitrag:

- M36: Sicherheitsanalyse eines Systems mit FPGA-basiertem Secure Element

TAP6.1.1: Aufbau der Demonstrator-Umgebung

In diesem Teilarbeitspaket wurde eine Demonstrator-Umgebung aufgebaut, die modellhaft ein industrielles Anwendungsszenario darstellt und dazu dient, die Notwendigkeit eines sicheren Update-Mechanismus eines SEs im industriellen Kontext zu motivieren. Dies wird am Beispiel eines Zufallszahlengenerators (auf English: True Random Number Generator, TRNG) gezeigt, der nur innerhalb eines sehr begrenzten Temperaturbereichs stabil funktioniert und bei Überschreiten einer Grenztemperatur einen systematischen Fehler in den gelieferten Werten aufzeigt. Ein Hauptaugenmerk wird daraufgelegt, dass die erzielten Projektergebnisse möglichst ohne weitreichendes technisches Verständnis klar werden. Dafür werden die vom TRNG produzierten Output-Werte grafisch anschaulich dargestellt, sodass auch für Laien erkennbar ist, dass dies ein Sicherheitsproblem darstellt, welches behoben werden muss. Die Temperaturerhöhung im Demonstrator kann auf unterschiedliche

Wege ausgelöst werden, womit unterschiedliche Angriffsszenarien berücksichtigt werden. Zur Behebung des Sicherheitsproblems kann ein sicheres Update des Zufallszahlengenerators im FPGA-SE mit dem entwickelten sicheren Update-Mechanismus durchgeführt werden. Nach dem Update kann durch erneutes Anwenden der unterschiedlichen Angriffsszenarien veranschaulicht werden, dass das Update erfolgreich war und die neue Version des Zufallszahlengenerators durch Temperaturerhöhungen nicht beeinflusst werden kann. Es wurde darauf geachtet, dass der Sicherheitsbezug anschaulich in die Beispiel-Anwendung einfließt. Diese Vorarbeiten waren die Grundlage der Integration der Projektergebnisse (TAP6.1.2). Der Demonstrator wurde bei dem öffentlichen Teil der Abschlusspräsentation des ALESSIO-Projekts bei Fraunhofer AISEC in Garching vor Teilnehmern des Münchner Sicherheitsnetzwerks erfolgreich vorgeführt[3].

Ergebnisbeitrag:

- M36: Demonstrator für FPGA-basiertes Secure Element in industriellem Szenario

TAP6.1.2: Integration der Projektergebnisse

Dieses abschließende Teilarbeitspaket integriert das im AP3 erarbeitete FPGA-basierte Secure Element in die im TAP6.1.1 aufgebaute Demonstrator-Umgebung eines industriellen Szenarios. Dafür wurde der in AP3.4 entwickelte Zufallszahlgenerator angepasst, damit die Output-Zufallswerte außerhalb eines begrenzten Temperaturbereichs einen systematischen Fehler aufweisen. Dieses Modul wurde in das, im AP3 entwickelte, FPGA-SE integriertet und der originale funktionsfähige Zufallszahlgenerator als Hardware-Update für das FPGA-SE verpackt. Zum Schluss wurde der Demonstrator auf Reproduzierbarkeit von Ergebnissen unter verschiedenen Randbedienungen (Temperatur, Auslastung, …) erfolgreich getestet.

Ergebnisbeitrag:

- M36: Demonstrator für FPGA-basiertes Secure Element in industriellem Szenario

[3] https://it-security-munich.net/event/projekt-alessio-abschlussveranstaltung/

Wichtigste Positionen des zahlenmäßigen Nachweises

Der zahlenmäßige Nachweis wurde separat übermittelt.

Notwendigkeit und Angemessenheit der geleisteten Arbeiten

Wir betrachten die Durchführung des Projekts als Erfolg und die Ausgaben für angemessen. Es wurden wichtige Ergebnisse erzielt, die einen hohen konkreten Bedarf nach langfristiger Sicherheit von eingebetteten Systemen in der Wirtschaft am Standort Deutschland treffen. Die Förderung dieser Arbeiten war notwendig, um den Mangel an entsprechenden Sicherheits-Konzepten und -Lösungen zu adressieren. Die Ergebnisse konnten nur sinnvoll unter der Beteiligung von Anwendern, Chipherstellern, Herstellern von Sicherheitskomponenten und Forschungsinstitutionen erarbeitet werden, um so die Komplexität langfristig sicherer eingebetteten Systeme aus unterschiedlichen Blickwinkeln zu adressieren.

Voraussichtlicher Nutzen

Der voraussichtliche Nutzen der Projektergebnisse ist im separaten Erfolgskontrollbericht beschrieben.

Während des Vorhabens bekanntgewordene Fortschritte auf dem Gebiet des Vorhabens bei anderer Stelle

RISC-V ist eine offene Befehlssatzarchitektur, die sich auf das Designprinzip des „Reduced Instruction Set Computer“ stütz (Wikipedia, RISC-V, 2020). Obwohl das RISC-V Projekt schon seit dem Jahr 2010 bekannt ist, werden die ersten RISC-V-basierten Soft-CPUs für FPGA-Systeme erst seit kurzem implementiert (Papon, 2018). Diese waren zum Start des Projekts, als die Auswahl der Soft-CPU getroffen wurde, leider noch nicht verfügbar. Die ZPU Soft-CPU, die als Kern des im ALESSIO-Projekt entwickelten FPGA-SEs ist, kann ohnehin mit einer moderneren RISC-V Soft-CPU ausgetauscht werden. Außerdem haben sich während der Projektlaufzeit Fortschritte auf dem Gebiet der Quantencomputern ergeben. Dies erhöht die Gefahr, dass aktuelle asymmetrische kryptografische Verfahren in absehbarer Zeit mit Quantencomputern angegriffen werden können. Obwohl quantencomputerresistente kryptografische

Verfahren nicht im Fokus des ALESSIO Projekts waren, kann das entwickelte FPGA-SE dank seines modularen Designs und seiner Update-fähigkeit mit quantencomputerresistenten Verfahren aktualisiert werden. Die Umsetzung quantencomputerresistenter Verfahren und die Verwendung von RISC-V Prozessoren als Soft-CPU werden derzeit in einem weiteren BMBF-geförderten Projekt namens AQUORYPT untersucht (Aquorypt Projekt, 2019-2022).

Erfolgte oder geplante Veröffentlichung der Ergebnisse

Im Jahr 2019 wurden die Ergebnisse des ALESSIO Projekts im Rahmen des VDMA Forum bei der „Smart Production Solutions“ (SPS) internationalen Fachmesse in Nürnberg und beim öffentlichen Teil der Abschlusspräsentation des ALESSIO Projekts mit Teilnehmern vom Münchener Sicherheitsnetzwerk bei Fraunhofer AISEC in Garching präsentiert. Ein zusammenfassendes Paper über die in AP3 erzielten Ergebnisse wurde zusammen mit dem Fraunhofer AISEC und der TU München bei dem Workshop „Trustworthy Manufacturing and Utilization of Secure Devices“ (TRUDEVICE) auf der Konferenz „Design, Automation and Test in Europe Conference“ (DATE) 2020 veröffentlicht (Unterstein, et al., 2020).

Literaturverzeichnis

Aquorypt Projekt. (2019-2022). Von https://www.forschung-it-sicherheit-kommunikationssysteme.de/projekte/aquorypt abgerufen

Dichtl, M., & Golić, J. (2007). High-Speed True Random Number Generation with Logic Gates Only. *Cryptographic Hardware and Embedded Systems*, 45-62.

Fischer, K., & Gessner, J. (2012). Security architecture elements for IoT enabled automation networks. *IEEE 17th International Conference on Emerging Technologies & Factory Automation (ETFA)*.

Fischer, K., Gessner, J., & Fries, S. (2012). Secure Identifiers and Initial Credential Bootstrapping for IoT@Work. *The Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS-2012)*.

Fischer, K., Mucha, A., Hess, E., & Reiss, F. (2017). PUF based Lightweight Hardware Trust Anchor for Secure Embedded Systems. *International Conference on Security and Management (SAM)*.

Harboe, Ø. (2020). *The Zylin ZPU*. Abgerufen am 18. 05 2020 von The Zylin ZPU: https://github.com/zylin/zpu

IoT@Work. (2010-2013). Von https://www.iot-at-work.eu/ abgerufen

ISA/IEC 62443: Security for Industrial Automation and Control Systems. (2007-2018). Von https://www.isa.org/standards-and-publications/isa-standards/ abgerufen

IUNO. (2015-2018). *https://iuno-projekt.de/*.

Lie, W., & Feng-yan, W. (2009). Dynamic Partial Reconfiguration in FPGAs. *Third International Symposium on Intelligent Information Technology Application, Shanghai*, 445-448.

Medwed, M., Standaert, F.-X., & Joux, A. (2012). Towards super-exponential side-channel security with efficient leakage-resilient PRFs. *CryptographicHardware and Embedded System (CHES)*.

Meng-Day, Y. a. (2010). Recombination of Physical Unclonable Functions. *35th Annual GOMACTech Conference*.

Papon, C. (2018). *The VexRiscV CPU - A New Way to Design*. Abgerufen am 18. 05 2020 von https://github.com/SpinalHDL/VexRiscv

Pöhls, H. C., Angelakis, V., Suppan, S., Fischer, K., Oikonomou, G., Tragos, E. Z., . . . Mouroutis, T. (2014). RERUM: Building a Reliable IoT upon Privacy- and

Security-enabled Smart Objects. *IEEE Workshop on Internet of Things Communications and Technologies (WNNC)*.

RERUM. (2013-2016). *https://ict-rerum.eu*.

Suh, E., & Devadas, S. (2007). Physical Unclonable Functions for Device Authentication and Secret Key Generation. *44th ACM/IEEE Design Automation Conference*.

Unterstein, F., Heyszl, J., De Santis, F., Specht, R., & Sigl, G. (2018). High-resolution EM attacks against leakage-resilient PRFs explained and an improved construction. *Topics in Cryptology (CT-RSA)*.

Unterstein, F., Sel, T., Zeschg, T., Jacob, N., Tempelmeier, M., Pehl, M., & De Santis, F. (2020). Secure Update of FPGA-based Secure Elements using Partial Reconfiguration. *DATE*. Von https://www.date-conference.com/workshop/w07 abgerufen

Wikipedia. (2020). *RISC-V*. Abgerufen am 18. 05 2020 von https://de.wikipedia.org/wiki/RISC-V

Wikipedia. (2020). *Soft microprocessor*. Abgerufen am 5. 3 2020 von Wikipedia, The Free Encyclopedia.: https://en.wikipedia.org/wiki/Soft_microprocessor

Xilinx, I. (2020). *Zynq-7000 SoC*. Abgerufen am 18. 05 2020 von Zynq-7000 SoC: https://www.xilinx.com/products/silicon-devices/soc/zynq-7000.html

Berichtsblatt

1. ISBN oder ISSN geplant	2. Berichtsart (Schlussbericht oder Veröffentlichung) Schlussbericht
3. Titel ALESSIO – Architektur für langfristige Sicherheit durch Secure Elements mit Update-Funktion Schlussbericht der Siemens AG	
4. Autor(en) [Name(n), Vorname(n)] Dr. Fabrizio De Santis	5. Abschlussdatum des Vorhabens 31.12.2019
	6. Veröffentlichungsdatum geplant
	7. Form der Publikation Schlussbericht
8. Durchführende Institution(en) (Name, Adresse) Siemens AG CT RDA CST SES Otto-Hahn-Ring 6 81739 München	9. Ber. Nr. Durchführende Institution
	10. Förderkennzeichen 16KIS0631
	11. Seitenzahl 19
12. Fördernde Institution (Name, Adresse) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	13. Literaturangaben 21
	14. Tabellen -
	15. Abbildungen -
16. Zusätzliche Angaben -	
17. Vorgelegt bei (Titel, Ort, Datum) -	

18. Kurzfassung

Im Forschungsvorhaben Architektur für Langfristige Sicherheit durch Secure Elements mit Update-Funktion (ALESSIO) wurde erforscht, wie langfristige Sicherheit von Lösungen und Komponenten in kritischen Infrastrukturen mit einer Lebensdauer von über 15 Jahren gewährleistet werden kann. Ziel war es, zu untersuchen, wie Hardware Secure Elements (HSE) in verschiedenen Technologieausprägungen (Smartcard und FPGA-SoC-Plattform) durch eine entsprechende Update-Fähigkeit ausgestattet werden können, um die Sicherheit von eingebetteten Systemen im industriellen Umfeld langfristig sicherzustellen. In der ALESSIO Teilvorhaben der Siemens AG wurde das Fokus speziell auf FPGA-basiertes Sicherheitselemente gelegt, von der Spezifikation der Anforderungen, über die Sicherheitsarchitektur und die Implementierung eines Basis-Systems, die Evaluierung von Angriffsmethoden, bis hin zur prototypischen Erprobung in einem Demonstrator. Zuerst wurden die Anforderungen an ein Secure Element im industriellen Umfeld erarbeitet. Anschließend wurde die Sicherheitsarchitektur eines FPGA-basierten Secure Elements (FPGA-SE) mit Update-Funktion konzipiert und das Basis-System des FPGA-SE prototypisch im FPGA implementiert. Das daraus resultierende Update-fähiges FPGA-basierte Secure Element wurde über die vorhandene Busmechanismen zur Haupt-CPU einer FPGA-SoC-Plattform angeschlossen und in ein Linux-basiertes System integriert. Des Weiteren wurden Software- und physische Angriffe auf das FPGA-basierte Secure Element durchgeführt, die dazu dienten, zusätzliche Laufzeitintegritätsmechanismen zum Schutz vor Manipulationsangriffen zu entwickeln. Anschließend wurden die von den Partnern entwickelten kryptografischen Mechanismen zur gerätspezifischen Schlüsselgenerierung und seitenkanalsicherer Entschlüsselung von Updates in das FPGA-basierte Secure Element integriert und in einem industriellen Szenario mit einem Demonstrator veranschaulicht.

19. Schlagwörter
Hardware Security, Secure Element, Industrie 4.0

20. Verlag -	21. Preis -

Document Control Sheet

1. ISBN or ISSN -	2. type of document (e.g. report, publication) Final report
3. title	
4. author(s) (family name, first name(s)) Dr. Fabrizio De Santis	5. end of project 31.12.2019
	6. publication date -
	7. form of publication Final report
8. performing organization(s) (name, address) Siemens AG CT RDA CST SES Otto-Hahn-Ring 6 81739 München	9. originator's report no. -
	10. reference no. 16KIS0631
	11. no. of pages 19
12. sponsoring agency (name, address) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	13. no. of references 21
	14. no. of tables -
	15. no. of figures -
16. supplementary notes -	
17. presented at (title, place, date) -	
18. abstract The research project „Langfristige Sicherheit durch Secure Elements mit Update-Funktion" (ALESSIO) explored how to ensure long-term security for solutions and components in critical infrastructures with a lifespan of more than 15 years. The project aimed at investigating how Hardware Secure Elements (HSE) can be equipped with an update capability in various types of technology (e.g. Smart cards and FPGA-SoC platforms) to ensure long-term security of embedded systems in industrial environments. In the ALESSIO project, the focus of Siemens AG was specifically on FPGA-based Secure Elements with the specification of the requirements, the design of a security architecture, the implementation of the underlying base system, the evaluation of attack techniques, and the prototypical realization of the FPGA-based SE in a demonstrator. More specifically, the requirements for a Secure Element in the industrial environment were initially identified. Subsequently, the security architecture of an FPGA-based Secure Element (FPGA-SE) with update function was designed and the base system of the FPGA-SE was implemented prototypically on a FPGA. The resulting update-enabled FPGA-based Secure Element was connected to the main CPU of an FPGA-SoC platform via the existing bus mechanisms and integrated into a Linux-based system. In addition, software and physical attacks were carried out on the FPGA-based Secure Element, which also helped to develop additional runtime integrity mechanisms to protect against tampering attacks. Subsequently, the cryptographic FPGA modules developed by the partners for the generation of device-specific key with a Physically Unclonable Function (PUF) and the decryption of SE-updates using a side-channel resistant cryptographic core were integrated into the FPGA-based Secure Element. Finally, a demonstrator was built to practically illustrate how to update a FPGA-based Secure Element in an industrial scenario.	
19. keywords Hardware Security, Secure Element, Industry 4.0	
20. publisher -	21. price -