Schlussbericht

Universell konfigurierbare Sicherheitslösung für Cyber-Physikalische heterogene Systeme

UNIKOPS

Förderprogramm	IKT 2020 – Forschung für Innovationen
Förderkennzeichen	16KIS0004
Projektlaufzeit	01.03.2013-29.02.2016
Stand	01.08.2016
Autoren	Stephan Kornemann Prof. Dr. Peter Langendörfer
Zuwendungsempfänger	IHP GmbH

Das diesem Bericht zugrundeliegende Vorhaben wurde durch Mittel des Bundesministeriums für Bildung und Forschung (BMBF) unter dem Förderkennzeichen 16KIS0004 gefördert. Die inhaltliche Verantwortung dieses Berichtes liegt bei den Autoren.

Inhaltsverzeichnis

Abbildungsverzeichnis

1. Kurze Darstellung

1.1.Aufgabenstellung

Das Ziel des Verbundprojektes UNIKOPS war die Entwicklung von Sicherheitsbausteinen für das Management von zukünftigen Cyber-Physical-Systems (CPS). Für dieses Projekt wurden vor allem ressourcenbeschränkte Systeme betrachtet, die in Automatisierungsanwendungen, Internet of Things (IoT) und Smart Metering-Anwendungen verwendet werden. Um die Akzeptanz für Hersteller bzw. Anwender zu erhöhen, müssen die Sicherheitskomponenten einfach und ohne große Konfiguration zu integrieren sein.

Bisherige Systeme, welche ähnliche Ziele verfolgen, decken prinzipiell einzelne Bereiche ab, allerdings sind diese Lösungen speziell auf die untersuchten Anwendungen angepasst und können nicht ohne weiteres in andere Systeme portiert werden. Daher müssen Bausteine entwickelt werden, die universell verwendet werden können, und welche an die beschränkten Ressourcen von Sensorknoten angepasst sind. Die Teilbereiche der Bausteine, die entwickelt werden, gliedern sich in eine gegenseitige inhärente Code Attestierung und ein effizientes Code-Image Update in einer Multihop-Umgebung. Neben diesen Teilbereichen werden auch Konzepte und Mechanismen zur Erkennung von Angriffen und Manipulationsversuchen sowie ein Modul für Funktionsfreischaltungen entwickelt.

1.1.Vorhabenvoraussetzungen

Das IHP ist ein Institut der Leibniz-Gemeinschaft und betreibt Forschung und Entwicklung zu siliziumbasierten Systemen, Höchstfrequenz-Schaltungen und -Technologien einschließlich neuer Materialien. Es erarbeitet innovative Lösungen für Anwendungsbereiche wie die drahtlose und Breitbandkommunikation, Luft- und Raumfahrt, Biotechnologie und Medizin, Automobilindustrie, Sicherheitstechnik und Industrieautomatisierung. Das IHP beschäftigt ca. 300 Mitarbeiterinnen und Mitarbeiter. Es verfügt über eine Pilotlinie für technologische Entwicklungen und die Präparation von Hochgeschwindigkeits-Schaltkreisen mit 0,13/0,25 µm-BiCMOS-Technologien, die sich in einem 1000 m² großen Reinraum der Klasse 1 befindet.

Das Institut ist in die vier Abteilungen Material Forschung, Technologie, Schaltungsentwurf und Systemdesign gegliedert und verfolgt erfolgreich einen vertikalen Forschungsansatz in dem die einzelnen Abteilungen durch die Nutzung von Synergien effizienter und schneller Forschungsthemen bearbeiten können.

Die Abteilung Systemdesign verfügte zu Beginn des UNIKOPS-Projektes bereits über mehrjährige Erfahrung im Bereich von Kommunikation und Sicherheit in drahtlosen Sensornetzen. So wurden im Rahmen von anderen Forschungsprojekten (TSN, TANDEM, UbiSecSens, TAMPRES, SMART) bereits erfolgreich Sicherheits- und Kommunikationskonzepte umgesetzt.

Durch eine enge Zusammenarbeit mit Universitäten und Fachhochschulen in Berlin und Brandenburg bestehen sehr gute Möglichkeiten zur wissenschaftlichen Verwertung der Ergebnisse in Forschung und Lehre.

1.2.Planung und Ablauf des Vorhabens

Gemäß den Vorgaben aus dem Vollantrags war das IHP primär für die gegenseitige inhärente Code Attestierung und für die Mechanismen zur Erkennung von Angriffen und Manipulationen

verantwortlich. Des Weiteren war eine enge Zusammenarbeit mit den Projektpartnern (RUB, HAW, ESCRYPT) vorgesehen.

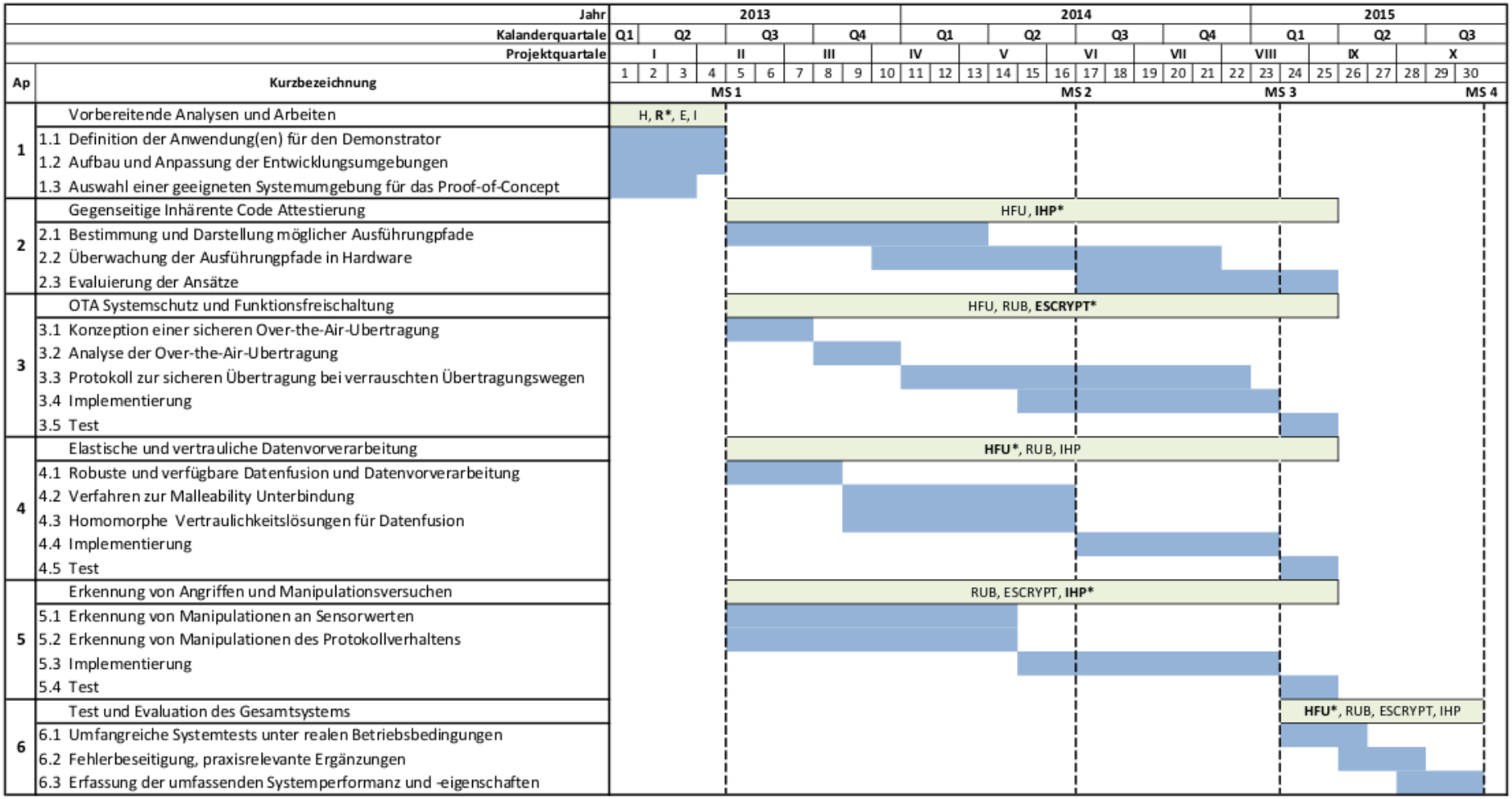
Die Aufgaben des IHP in den einzelnen Arbeitspaketen waren wie folgt:

- **Arbeitspaket 1:** Auswahl geeigneter Hardware- und Softwarekomponenten für das Proof-of-Concept
- **Arbeitspaket 2:** Hardwareunterstützte Überwachung der Ausführungspfade für eine gegenseitige inhärente Code Attestierung. Evaluierung von Hash-basierten sowie von Cipher-basierten Ansätzen
- **Arbeitspaket 3:** Unterstützung der Projektpartner bei der Softwareentwicklung.
- **Arbeitspaket 4:** Unterstützung bei der Entwicklung des Protokolls, welches für die Kommunikation zwischen den Knoten und der Basisstation verantwortlich ist.
- **Arbeitspaket 5**: Entwicklung von Mechanismen zur Erkennung von Angriffen und Manipulationsversuchen sowie deren Evaluierung.
- **Arbeitspaket 6:** Test und Evaluation des Gesamtsystems.

Die zeitliche Planung der Arbeitspakete ist in Abbildung 1 dargestellt. Allerdings konnte diese Planung nicht eingehalten werden. Dadurch wurde eine kostenneutrale Verlängerung von 6 Monaten beantragt. Gründe für die Verlängerung lagen in der Verzögerung bei der Bearbeitung des Arbeitspaketes 2 und in der Anpassung der Arbeitsziele im Arbeitspaket 5.

Die Entwicklung der gegenseitigen inhärenten Code Attestierung (AP2) ist wesentlicher Bestandteil der universellen Sicherheitslösung für Cyber Physical Systems. Bisher existierte keine Lösung, die einen vergleichbaren Ansatz verfolgt und ein entsprechend hohes Maß an Sicherheit bieten kann. Aufgrund der Komplexität war eine ausreichende Bearbeitung in der vorgesehenen Projektlaufzeit nicht möglich. Des Weiteren führten nicht eingeplante Arbeiten im AP4 zu weiteren Verzögerungen. Im AP4 wurde seitens des IHPs ein Routing Protokoll für Sensornetze entwickelt, dass von den Projektpartnern im Folgenden verwendet wird. Aufgrund dieser Abhängigkeit wurde das Arbeitspaket entsprechend priorisiert.

Bei der Bearbeitung des AP5 hat sich im Laufe des Projektes eine sinnvolle Anpassung der Ziele ergeben. So ist es sinnvoll nicht nur die Mechanismen selbst sondern auch die Laufzeitumgebung zur Ausführung der Mechanismen der Angriffserkennung zu untersuchen und geeignete Lösungen zu entwickeln. So wurde nach der Untersuchung von zwei neuen Mechanismen eine Lösung für eine Laufzeitumgebung entwickelt, die universell auf verschiedenen Geräteklassen eingesetzt werden kann.



- **Abbildung 1: Zeitliche Planung des Vorhabens (Gant-Chart)**

1.3.Wissenschaftlicher und technischer Stand

Zum Zeitpunkt der Beantragung des Projektes UNIKOPS existierten bereits Ansätze, die eine Manipulation der Firmware von leistungsschwächeren Geräten erkennen konnten. Solche Ansätze basieren zum einen auf Zeitbeschränkungen hinsichtlich der Bearbeitungszeit bei zugrunde gelegten Challenge-Response Verfahren oder aber sie versuchen auszunutzen, dass der verfügbare Platz zum Ablegen von Schadcode nicht vorhanden ist. Allerdings ist auch ein Angriff bekannt, welcher diese Verfahren umgeht. Um sicherzustellen, dass Geräte mit begrenzten Ressourcen nicht kompromittiert werden können bzw. ausschließlich autorisierten Code ausführen, soll ein Ansatz untersucht werden, den wir als Intrinsic Code Attestation (ICA) bezeichnen. Das Ziel der Untersuchungen ist die Entwicklung einer Hardwareeinheit, die bei der Ausführung des Programmtextes von innen heraus sicherstellt, dass nur authentifizierter Programmcode ausgeführt wird bzw. ausgeführt werden kann.

Neben der Sicherstellung, dass Schadcode nicht auf den Sensorknoten ausgeführt werden kann, muss auch ein korrektes Systemverhaltens sichergestellt werden. Abweichungen vom normalen Systemverhalten kann durch direkte Manipulation der Sensorknoten, des Netzwerkverhaltens, aber auch durch die Manipulation von Messwerte hervorgerufen werden. Zum Zeitpunkt der Beantragung gab es keinen ganzheitlichen Ansatz solche Abweichungen zu erkennen. Es gibt einige Arbeiten zur Erkennung von Angriffen auf Routing-Protokolle für diese Ansätze muss allerdings festgestellt werden, dass sie vom verwendeten Protokoll abhängig sind. Auch ein zentralistischer Ansatz für eine Firewall in Sensornetzen wird in der Literatur beschrieben. Dieser Ansatz erscheint, wegen der Notwendigkeit die Rohdaten an eine zentrale Stelle zu senden, ungeeignet. In anderen Ansätzen wird vorgeschlagen, Abweichungen im Protokollverhalten als Indikation für Angriffe zu nutzen. Keiner der hier zitierten Ansätze analysiert die in den Protokollpaketen enthaltenen Daten.

Deswegen untersuchen wir einen neuen Ansatz, der Mechanismen zur Erkennung von Abweichungen im Protokollverhalten aber auch zur Erkennung von Abweichungen in den Paketinhalten kombiniert. Um dieses in drahtlosen Sensornetzen realisierbar zu machen, müssen alle Mechanismen extrem leichtgewichtig sein. Um Abweichungen von normalem Protokollverhalten erkennen zu können, muss das System wissen, was das normale Systemverhalten ist. Der Ansatz von Piotrowski[1] et al. kann nicht genutzt werden, da z. B. in AAL-Anwendungen eine eindeutige zeitliche Kommunikationsreihenfolge nicht vorabdefiniert werden kann. In UNIKOPS sollen Mechanismen entwickelt werden, mit denen für unterschiedliche Anwendungsszenarien die korrekten Protokollabläufe gelernt werden können, um anschließend als Basis für die Erkennung von Angriffen verwendet werden zu können. Darüber hinaus sollen Mechanismen zur Analyse der Paketinhalte entwickelt werden. Den Ausgangspunkt bildet die RANBAR[2] Idee. Allerdings sollen nicht nur direkte Abweichungen von den Sensordaten erkannt werden, sondern es sollen auch Änderungen in den Sensordaten erkannt werden, die zwar noch im erlaubten Bereich liegen, aber trotzdem beeinflusst sind. Ziel der Untersuchung ist festzustellen, wie die Verteilung der Daten sein muss, um solche Analysen zu ermöglichen ohne die Sensorknoten zu überlasten. Ähnliches gilt für die Analyse der Sensordaten.

---

[1] Piotrowski, Krzysztof, et al. "Specification of an IDS Scheme and Secure Code Attestation Protocol for WSAN." (2011).

[2] Buttyan, L., P. Schaffer, and I. Vajda. "RANBAR: RANSAC-Based Resilient Data Aggregation in Sensor Networks." *4th ACM Workshop on Security of Ad Hoc and Sensor Networks, ACM SASN*. 2006.

1.4.Zusammenarbeit mit anderen Stellen

Das UNIKOPS-Konsortium setzt sich aus vier Partnern zusammen. In der ersten Phase des Projektes wurden Anwendungen für den Demonstrator definiert und eine geeignete Hardwareplattform definiert. Anschließend erfolgte die Umsetzung der einzelnen Komponenten. Dieses erfolgte je nach Arbeitspaket bei den Projektpartnern oder in enger Kooperation einzelner Partner.

Bei der Bearbeitung der Arbeitspakete unterstützte das IHP die anderen Projektpartner bei der Lösung von Problemen und bei der Implementierung der Module. Da der verwendete Sensorknoten bereits in vielen Projekten vom IHP verwendet wurde, konnten die Erfahrungen mit der Plattform bei der Lösung von Problemen helfen.

Die enge Kooperation mit der RUB bei der Umsetzung des ICA-Verfahrens, führte zu sehr guten Ergebnissen und konnte zu einem erfolgreichen Abschluss des Arbeitspaketes beitragen. Auch die Zusammenarbeit mit den anderen Partnern führte zu interessanten Ideen, welche für die erfolgreiche Bearbeitung der Arbeitspakete 4 und 5 beitrugen.

In der letzten Phase des Projektes erfolgte die Integration und Realisierung der Demonstratoren. In dieser Phase konnten zusätzliche Treffen aller Projektpartner zu einem erfolgreichen Abschluss des Projektes beitragen.

1.5.Erzielte Ergebnisse aus den einzelnen Arbeitspaketen

1.5.1. Arbeitspaket 1 – Vorbereitende Arbeiten und Analysen

Aufgabe 1.1 (Definition der Anwendungen für den Demonstrator):

Das Arbeitspaket befasste sich mit der Spezifikation des Demonstrators. Es wurden Anforderungen für diesen definiert, so dass die Spezifikation in die Bearbeitung der anderen Arbeitspakete eingehen konnte.

Aufgabe 1.2 (Aufbau und Anpassung der Entwicklungsumgebung):

Als Entwicklungsumgebung der Softwaremodule wurde das Code Composer Studio (CCS) von Texas Instruments ausgewählt. Dieses umfasst für die Entwicklung alle notwendigen Features, welches eine schnelle und effiziente Arbeit zulässt. Als Ausgangsbasis für die Softwaremodule stellte das IHP für den Sensorknoten ein Betriebssystem (langOS) bereit. Dieses konnte dann genutzt werden, um weitere Softwaremodule zu entwickeln. Damit alle Projektpartner einen schnellen Einstieg in die Arbeit mit CCS, langOS und dem IHPnode finden konnten, wurde ein Workshop vom IHP veranstaltet.

Aufgabe 1.3 (Auswahl einer geeigneten Systemumgebung für das Proof-of-Concept):

Das IHP hatte den anderen Projektpartnern verschiedene Plattformen für die Umsetzung der Arbeitspakete, als auch des Demonstrators vorgestellt. Daraufhin wurde gemeinschaftlich der IHPnode für den Aufbau eines Sensornetzes und der Raspberry PI als Gateway ausgewählt. Der IHPnode, welcher bereits für viele erfolgreiche Projekte vom IHP verwendet wurde, eignete sich sehr gut um die Aufgabenbereiche aus den Arbeitspaketen abzudecken. Zusätzlich konnte das Knowhow des IHP über die verwendete Plattform in die Arbeit der Arbeitspakete miteingehen. Die Entscheidung den Raspberry Pi als Gateway zu verwenden, wurde auf Grundlage des Gerätepreises und der Verbreitung des Systems in der Community getroffen.

1.5.2. Arbeitspaket 2 – Gegenseitige Inhärente Code Attestierung

Aufgabe 2.1 (Bestimmung und Darstellung möglicher Ausführungspfade):

Das IHP untersuchte mögliche Angriffe auf die Ausführungspfade von Programmen. Die Untersuchung zeigte, dass vor allem Return-Oriented-Programming (ROP)-Angriffe genutzt werden können, um Schadsoftware auf den Sensorknoten auszuführen. ROP-Angriffe manipulieren den Aufrufstack so, dass beim Rücksprung indirekt vorhandener Maschinencode ausgeführt wird. Durch eine gezielte Auswahl von Maschinencodeteilen kann nicht authentifizierter Code ausgeführt werden.

Aufgabe 2.2 (Überwachung der Ausführungspfade in Hardware):

Das IHP hat einen neuen Ansatz für eine lokale Code Attestierung, namens Intrinsic Code Attestation, entwickelt. Das Verfahren erlaubt mit Hilfe einer Speicherdecodierungseinheit nur authentifizierten Programmcode auszuführen. Bei der Verschlüsselung des Programmtextes wird sichergestellt, dass Abhängigkeiten zwischen den Anweisungen in Form eines Chiper Block Chainings (CBC) entstehen. Diese Abhängigkeiten stellen sicher, dass einzelne Anweisungen nicht für Return Oriented Programming (ROP) – Angriffe missbräuchlich genutzt werden können. Das ICA-Verfahren wurde als Patent (PCT/EP2016/051756) angemeldet.

Aufgabe 2.3 (Evaluierung der Ansätze):

Die Evaluierung der ICA wurde durch das IHP durchgeführt. Hierzu wurde eine geeignete Werkzeugkette entwickelt, welche die Übersetzung von Quellcode zur modifizierten Architektur ermöglicht. Zusätzlich erfolgte eine Implementierung des ICA Verfahren in einer Hardwarebeschreibungssprache (HDL) auf dem tinyVLIW8 Soft-Core. Bei der Auswahl des Verschlüsselungsverfahrens unterstütze der Projektpartner RUB die Arbeiten. Die Ergebnisse wurden im Paper „Intrinsic Code Attestation by Instruction Chaining for Embedded Devices“ veröffentlicht.

1.5.3. Arbeitspaket 3 – OTA Systemschutz und Funktionsfreischaltung

Das IHP war in diesem Arbeitspaket nicht direkt involviert. Allerdings konnten die Projektpartner bei technischen Fragen und Implementierungsdetails zum verwendeten Sensorknoten und des Betriebssystems unterstützt werden.

1.5.4. Arbeitspaket 4 – Elastische und vertrauliche Datenvorverarbeitung

Aufgabe 4.3 (Homomorphe Vertraulichkeitslösungen für Datenfusion)

Das Arbeitspaket wurde gemeinsam mit HSO und RUB durchgeführt. Für die Übertragung der Daten innerhalb des Sensornetzes sollte die Routing-Protokoll Implementierung FET-MHR erweitert und verwendet werden. Allerdings funktionierte die Implementierung ausschließlich auf der Simulationsumgebung. Aus diesem Grund musste das Protokoll auf den IHPnode portiert werden. Dazu wurde im Rahmen von UNIKOPS eine Masterarbeit ausgeschrieben, welches die Portierung sowie neue Konzepte für das Sensornetzbetriebssystem bearbeiten sollte. Neben dem Routing-Protokoll wurde auch ein CSMA/CA Verfahren entwickelt.

Die neuen Konzepte für das Betriebssystem langOS wurden im Rahmen der 13. Fachgespräche „Drahtlose Sensornetze“ der deutschsprachigen Sensornetz-Forschergemeinde präsentiert. Die neuen Konzepte erleichterten auch die Integration der Sicherheitsmodule aus Arbeitspaket 5.

Das vorgestellte Betriebssystem langOS wurde als Open Source Projekt registriert und auf SourceForge unter https://sourceforge.net/projects/langos/ veröffentlicht.

Neben der eigentlichen Implementierung wurde ein Sensornetz-Testbed im IHP entwickelt und aufgebaut. Dieses konnte für den Funktionstest und die Fehlersuche genutzt werden.

1.5.5. Arbeitspaket 5 – Mechanismen zur Erkennung von Angriffen und Manipulationen

Für die **Arbeitspakete 5.1 – Erkennung von Manipulationen an Sensorwerten** und **5.2 – Erkennung von Manipulationen des Protokollverhaltens** wurden zwei universelle Algorithmen entworfen, welche das Detektieren von zeitlich signifikanten Änderungen ermöglicht. Diese erzielten gute Ergebnisse, allerdings waren diese nicht aussagekräftig mit anderen Algorithmen zu vergleichen. Des Weiteren wurde festgestellt, dass ein fixer Algorithmus für die Erkennung der verschiedenen Angriffe nicht sinnvoll ist. Da sich die Methoden der Angreifer sehr schnell anpassen, muss sich auch das Sicherheitssystem schnell und leicht anpassen lassen. Dazu wurde ein Konzept entwickelt, dass die Flexibilität des Systems unterstützt. Dieses Konzept beinhaltet ein speziell für Sicherheitsanalysen entwickelten Interpreter, welcher leicht in bestehende Betriebssysteme integriert werden kann.

Aufgabe 5.3 (Implementierung):

Dieses Arbeitspaket teilte sich in zwei Bereiche. Zum einem wurde als Proof-of-Concept das Konzept des universellen Sicherheitssystems in das langOS Betriebssystem integriert und die Funktion auf dem IHPnode validiert. Der andere Bereich konzentrierte sich auf die Entwicklung eines Frameworks, welches eine leichte Nutzung des Systems sicherstellen soll.

Zur Implementierung von Sicherheitsalgorithmen wurde für die Evaluierung ein Assembler implementiert, welcher es ermöglicht die entsprechenden Algorithmen zu implementieren.

Aufgabe 5.4 (Test):

Das IHP hat einen Funktionstest mit den entwickelten Sicherheitskomponenten durchgeführt. Für den Test wurde das Testbed, welches im Arbeitspaket 4 entwickelt wurde genutzt. Der Funktionstest zeigte, dass die zusätzlichen Sicherheitskomponenten, welche für das langOS Betriebssystem entwickelt wurden, sich perfekt ins Gesamtsystem integrieren lassen.

1.5.6. Arbeitspaket 6 – Test und Evaluation des Gesamtsystems

Aufgabe 6.1 (Umfangreiche Systemtests unter realen Betriebsbedingungen):

Das IHP konnte mit Hilfe des Testbeds einen Dauertest des IDS durchführen. Hierzu wurde ein Sensornetz aufgebaut, welches auch als Demonstrator diente. Der Dauertest zeigte, dass Verbesserungen in der Stabilität des Systems gemacht werden müssen.

Aufgabe 6.2 (Fehlerbeseitigung, praxisrelevante Ergänzungen):

Das IHP unterstütze die Arbeiten der HSO bei der Fehlerbeseitigung der Übertragung der Fountain-Codes. Um eine verbesserte Darstellung der Ergebnisse zu ermöglichen, erstellte das IHP eine grafische Visualisierung der Ausgaben.

Aufgabe 6.3 (Erfassung der umfassenden Systemperformanz und –eigenschaften):

Die Performance des IDS wurde durch statische und dynamische Analysen durchgeführt. Da das IDS eine Art Virtuelle Maschine darstellt, konnte es mit anderen Virtualisierungsansätzen, wie Maté[3], verglichen werden. Die Performance in Geschwindigkeit sowie genutztem Speicherbereich war deutlich besser.

1.6.Technische Beschreibung der Ergebnisse

Das IHP war vor allem bei der Umsetzung der Intrinsic Code Attestierung und des universellen Intrustion Detection Systems beteiligt. Dieser Abschnitt enthält die technischen Beschreibungen dieser Arbeiten.

1.6.1. Intrinsic Code Attestation (ICA)

Das IHP hat sich zum Ziel gesetzt im Rahmen des UNIKOPS-Projektes Mechanismen zur lokalen Code Attestierung zu untersuchen bzw. einen neuen Ansatz zu entwickeln. Im Projektzeitraum wurde das Konzept der Intrinsic Code Attestation (ICA) entwickelt und bzgl. der Eignung in Low Power Microcontrollern untersucht. Die ICA basiert auf einer kryptographischen Verkettung von Instruktionen, so dass der Programmcode von Dritten nicht ausgelesen und Code Injection Angriffe verhindert werden können. Die Abbildung 2 zeigt diese Verkettung. Hierzu wird jede Instruktion mit einer Nonce erweitert, welches für die kryptographische Verarbeitung der Nachfolgeinstruktion verwendet wird. Die Nonce wird mit der Instruktion zusammen verschlüsselt, so dass eine Instruktion nur dann entschlüsselt werden kann, wenn die vorangegangene Instruktion zuvor entschlüsselt wurde. Damit kann verhindert werden, dass ohne Kenntnis des Schlüssels neuer Programmcode eingebracht bzw. der vorhandene Programmcode in veränderter Reihenfolge verwendet werden kann. Die Entschlüsselung der Instruktionen wird in den Datenpfad des Microcontroller integriert, so dass sie nicht umgangen werden kann. Dadurch kann sichergestellt werden, dass der Prozessorkern nur verschlüsselte Instruktionen ausführt und der Nutzer Kenntnis über den Programmschlüssel haben muss, um neuen Programmtext einzuspielen. Darüber hinaus verhindert die Verschlüsselung des Programmtextes dessen Auslesen und schützt somit die Intellectual Property des Programmcodeherstellers. Das Konzept der ICA wurde zum Patent (PCT/EP2016/051756) angemeldet.

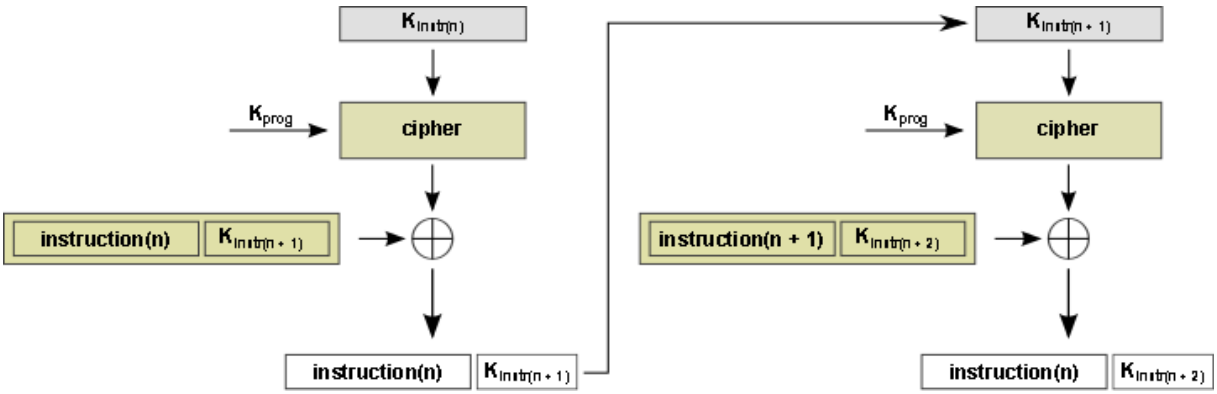


Abbildung 2: Intrinsic Code Attestation durch eine kryptographische Verkettung von Instruktionen

Aufgrund der Verschlüsselung von Instruktionen, ist die Umsetzung bzw. die Integration der ICA stark an die Instruction Set Architecture (ISA) des Prozessorkerns gebunden. Im Rahmen des Projektes wurden zwei verschiedene Prozessorkerne hinsichtlich ihrer Eignung für die ICA untersucht. Zunächst

[3] Levis, Philip, and David Culler. "Maté: A tiny virtual machine for sensor networks." *ACM Sigplan Notices* 37.10 (2002): 85-95.

wurde der MSP430 betrachtet. Hierbei handelt es sich um einen RISC-Prozessor mit einer Von-Neumann-Architektur. Bei der Von-Neumann-Architektur werden Programmtext und dynamische Daten im gleichen Speicher abgelegt. Aus diesem Grund ist diese Architektur besonders anfällig für Code Injection-Angriffe. Der MSP430 verwendet darüber hinaus eine ISA mit unterschiedlich langen Instruktionen. Die Instruktionen werden jeweils Wort-weise (16-bit) vom Decoder eingelesen und dekodiert. Erst nach der Dekodierung steht fest, ob ein zusätzliches Wort eingelesen werden muss oder ob der Nonce im Programmtext folgt. Zur Unterstützung eines variablen Befehlsatzformates, wie das des MSP430, nutzt die ICA einen Block Cipher im Counter Mode (CTR). Mittels des CTR wird ein Schlüsselstrom erzeugt, der mittels einer XOR-Operation Bit-weise über den Klartext gelegt wird. Damit können Klartexte beliebiger länge verschlüsselt werden. Die Verwendung des CTR hat zudem den Vorteil, dass die Entschlüsselung keinen direkten Einfluss auf die Ausführung der Instruktionen hat. Die aufwendige Block-Operation wird im Anschluss an die Verarbeitung des Befehls durchgeführt. Für die hierfür notwendigen Taktzyklen, kann der Prozessorkern kurzzeitig unterbrochen werden. Als zweite untersuchte Architektur wurde der tinyVLIW8[4] untersucht[1]. Der tinyVLIW8 verwendet im Gegensatz zum MSP430 ein festes Befehlsformat. Darüber hinaus wird jeder Befehl mit einer dedizierten Adresse adressiert. Beides vereinfacht die Integration der ICA wesentlich. Hierzu muss lediglich das Befehlswort im Speicher um die Länge des Nonce erweitert werden. Die Untersuchungen haben zu dem Ergebnis geführt, dass die ICA für beide Architekturen verwendet werden kann. Beim MSP430 entsteht jedoch ein wesentlicher größerer Aufwand bei der Integration. Darüber hinaus hat die ICA beim MSP430 Einfluss auf die maximale Programmgröße.

Evaluierung

Zur Evaluierung wurde das Konzept in den MSPsim integriert. Der MSPsim ist ein Cycle Accurate Simulator (CAS) der vom Swedish Institute of Computer Science (SICS) entwickelt wurde. Der Simulator ist vollständig in Java geschrieben und erlaubt die Simulation von verschiedenen MSP430-basierten Sensornetzplattformen. So kann z. B. Programmcode, der für den bekannten Berkley Mote TmoteSky entwickelt wurde, unverändert simuliert werden. In der neusten Version des MSPsim wird auch die MSP430X Architektur unterstützt, so dass auch Programmcode des IHPnode simuliert werden kann. Der Block Cipher wird aktuell über Standard Bibliotheken in den MSPsim integriert.

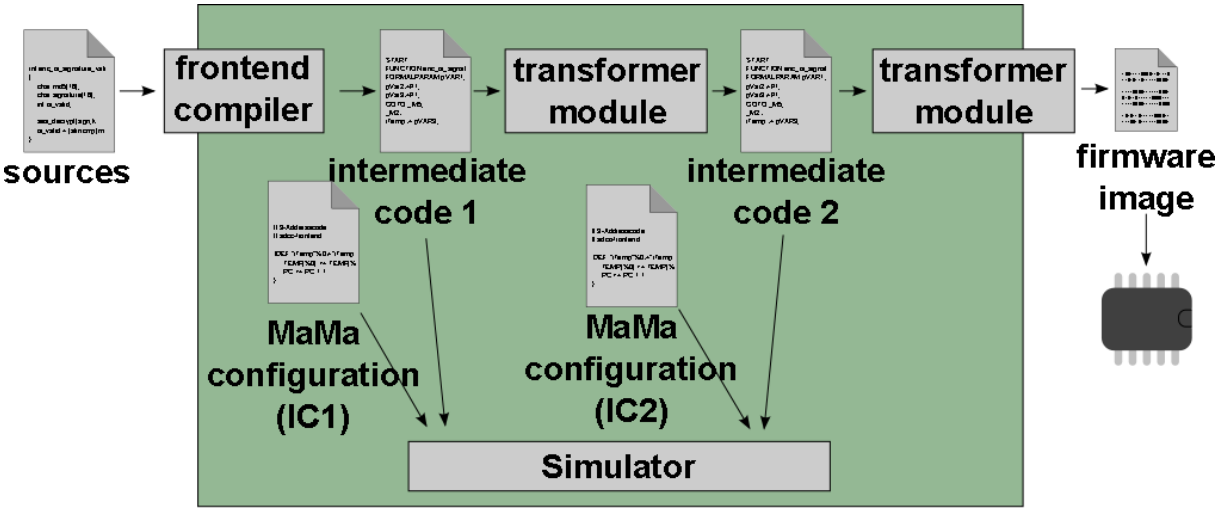


Abbildung 3: Werkzeugkette für die Erzeugung von verschlüsselter Firmware

[4] **A Tiny Scale VLIW Processor for Real-time Constrained Embedded Control Tasks;** *Oliver Stecklina, Michael Methfessel;* 27.-29. August 2014: DSD 2014 17th Euromicro Conference on Digital Systems Design (Verona, Italy)

Nach Abschluss der Integration der ICA in den MSPsim wurde mit der Entwicklung der Werkzeugkette begonnen. Als Basis wurden hierfür das LLVM[5] Framework von Chris Lattner und das CoMet[6] Framework der BTU Cottbus verwendet. LLVM ist ein modularer Compiler der verschiedene Frontends bereitstellt. Somit können direkt C basierte Compiler, wie der Clang Compiler verwendet werden, um Quellcode für unterschiedliche Zielarchitekturen zu übersetzen. LLVM hat den Vorteil, dass viele Optimierungen in jeder Zeitphase des Übersetzungsvorgangs verwendet werden können und es um beliebige Module erweitert werden kann. Allerdings ist es ein sehr komplexes System, welches bei Eigenentwicklungen ein tiefes Verständnis der internen Strukturen fordert. Das CoMet Framework hingegen lässt eine sehr einfache Struktur zu und es ist möglich die Zielarchitekturen zu simulieren. CoMet, stellt aber keinen Compiler einer Hochsprache bereit. Somit wurde eine Möglichkeit erarbeitet, welche beide Vorteile miteinander verknüpft. Dazu wurde eine recht einfache Instruction Set Architectur (ISA) spezifiziert. Die ISA kann mit Hilfe einer MaMa Spezifikation für das CoMet-Framework beschrieben werden. Diese wurde als Referenz für die Ausgaben des LLVM Framework und als Eingabe des CoMet Framework definiert. Um die Ausgaben durch LLVM zu generieren, musste eine neue Zielarchitektur (Target) implementiert werden. Parallel dazu wurden die benötigten Transformationsmodule für das CoMet-Framework entworfen. Eine studentische Hilfskraft konnte die Arbeiten unterstützen, so dass gute Fortschritte erzielt werden konnten.

Zur Validierung des ICA Verfahren wurde eine Implementierung des Konzepts in einer Hardwarebeschreibungssprache (HDL) umgesetzt. Hierzu wurde der tinyVLIW8 als Soft-Core ausgewählt. Dieser eignete sich sehr gut für die Validierung, da alle Instruktionen gleich breit sind. Dies vereinfachte die Integration erheblich. Für das Verschlüsselungsverfahren (Chiper) standen drei Algorithmen zur Verfügung. Zwei Versionen des AES und der leichtgewichtige PRINCE. Der Projektpartner RUB zeigte, dass die PRINCE Variante sehr gute Latenz-Eigenschaften aufweist, welche für den Einsatz in der Speicherdekodierungseinheit (MDU) gewünscht ist. Die Integration der MDU wird in Abbildung 4 dargestellt.

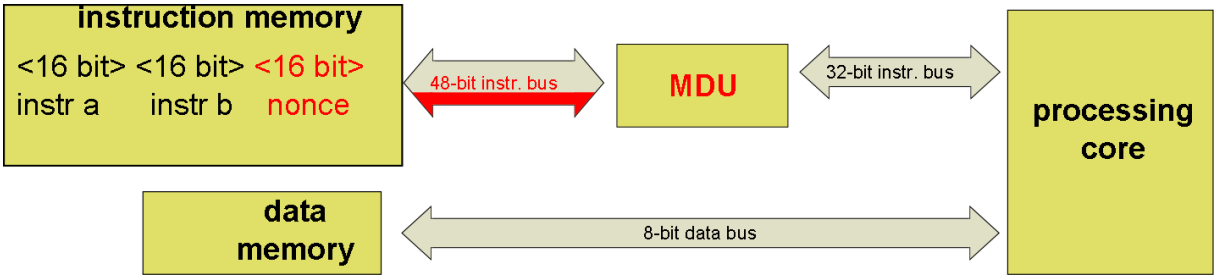


Abbildung 4: Integration der Speicherdekodierungseinheit (MDU) in den tinyVLIW8

Nach der Umsetzung des PRINCE in HDL konnten die Verfahren miteinander verglichen werden. Für die Integration des ICA-Verfahrens in die MDU des tinyVLIW8 wurde das PRINCE Verfahren ausgewählt. Dieser hatte sich gegenüber den anderen Varianten performance-technisch durchgesetzt. Genauere Information sind dem Paper „Intrinsic Code Attestation by Instruction Chaining for Embedded Devices“, welches auf der SecureComm2015 veröffentlicht wurde zu entnehmen.

---

[5] **LLVM: A Compilation Framework for Lifelong Program Analysis & Transformation;** Chris Lattner and Vikram Adve 2004; In *Proceedings of the international symposium on Code generation and optimization: feedback-directed and runtime optimization* (CGO '04). IEEE Computer Society, Washington, DC, USA, 75-

[6] **Ein konfigurierbarer Zwischencodesimulator zum compilerzentrierten Mikroprozessorentwurf**; *R. Urban, M. Schölzel, H. T. Vierhaus*; Tagungsband des Workshops Methoden und Beschreibungssprachen zur Modellierung und Verifikation von Schaltungen und Systemen (MBMV'13), 201

Tabelle 1: Design-Größen der Blockverschlüsselungsverfahren

Cipher	Cycles	Logical Cells (LCs)	Registers
AES [7]	60	2403	428
AES [8]	12	8855	792
PRINCE [9]	11	750	70
PRINCE (unrolled) [10]	0	1875	0

Tabelle 2: Design-Größen der Soft-Cores

Softcore	Logical Cells (LCs)
TinyVLIW8	1162
MDU (Skeleton)	126
MDU with PRINCE	2001

1.6.2. FET-MHR Routing –Protokoll

Für die Einbindung von Sensornetzwerken in bestehende Infrastrukturen wurde in den letzten Jahren der 6LoWPAN-Standard entwickelt. Dieser beschreibt Methoden und Verfahren zur Nutzung von IPv6 auf ressourcenbeschränkten Systemen. Die Nutzung von IPv6 bietet die Möglichkeit, einen direkten Zugriff von Geräten aus dem Internet auf die Sensorknoten zu gewähren. Damit lassen sich die Informationen wesentlich leichter in bestehende Internetdienste integrieren. Am IHP wurde mit dem FET-MHR-Protokoll ein Protokoll entwickelt, welches sich besonders für autonome batteriebetriebene Geräte eignet. Im Rahmen des UNIKOPS Vorhabens sollte dieses Protokoll um 6LoWPAN erweitert werden. Darüber hinaus sollten, die in IPv6 integrierten Mechanismen zur sicheren Datenübertragung hinsichtlich ihrer Eignung für Sensornetze untersucht werden.

Es stellte sich heraus, dass die Implementierung des FET-MHR-Protokolls, welches zu Beginn des Projekts ausschließlich für die Simulationsumgebung Castalia implementiert war, nicht auf einen realen Sensorknoten lauffähig war. Aus diesem Grund musste eine Portierung des Protokolls auf den IHPnode vom IHP durchgeführt werden.

Um den Projektpartnern die Einarbeitung in das Protokoll sowie in die Hardwareplattform zu vereinfachen, wurde im IHP ein Workshop durchgeführt. In diesem Workshop wurden das Protokoll und die Entwicklungs- und Simulationsumgebung vorgestellt und erste Ansätze zur Integration der eigenen Arbeiten geboten.

---

[7] R. Usselmann. AES (Rijndael) IP Core :: Overview, 2013

[8] F. Vater and P. Langedörfer. An Area Efficient Realisation of AES for Wireless

[9] J. Borghoff, A. Canteaut, T. Güneysu, E. B. Kavun, M. Knezevic, L. R. Knudsen, T. Yalcin. PRINCE – A low-latency block cipher for pervasive computing applications – extended abstract. *In Proceedings of the 18th International Conference on the Theory and Application of Cryptology and Information Security*

[10] J. Borghoff, A. Canteaut, T. Güneysu, E. B. Kavun, M. Knezevic, L. R. Knudsen, T. Yalcin. PRINCE – A low-latency block cipher for pervasive computing applications – extended abstract. *In Proceedings of the 18th International Conference on the Theory and Application of Cryptology and Information Security*

Um die Arbeiten im Arbeitspaket voranzutreiben, wurde eine Masterarbeit zu diesem Thema ausgeschrieben. Die Arbeit wurde im ersten Quartal 2015 abgeschlossen und es konnten gute Ergebnisse erzielt werden. Das Thema der Arbeit wurde so ausgelegt, dass neue Konfigurations-Konzepte für das Betriebssystem langOS entwickelt wurden. Somit ist es nun möglich den Protokoll-Stack zur Übersetzungszeit anzupassen, ohne dass eine Veränderung im Quelltext vorgenommen werden muss. Es wurden auch neue Features, wie z. B. Hooks, eingebaut. Diese Funktionalität vereinfachte die Einbindung des IDS-Systems (Arbeitspaket 5) erheblich. Durch die internen Anpassungen wurde auch das FET-MHR-Protokoll entsprechend weiterentwickelt. Es konnte eine saubere Trennung der MAC- und der Routing-Schicht erreicht werden. Neben den Arbeiten an der Routing-Schicht wurde auch ein CSMA/CA MAC-Protokoll implementiert und zur langOS Bibliothek hinzugefügt. Somit ist es nun möglich die bestehenden Routing-Algorithmen mit einem Medienzugriffsverfahren zu erweitern.

Abbildung 5: Lage der Sensorknoten im Testbed

Für einen Funktionstest des FET-MHR-Protokolls wurde ein Testbed im IHP aufgebaut. Es wurden 8 Knoten für die Testreihe verwendet. Die Lage der IHPnodes ist in Abbildung 5 dargestellt. Dieses wurde am Anfang des Projektes implementiert. Für eine bessere Darstellungen sowie die Möglichkeit Debug-Ausgaben vom gesamten Sensornetz zu erhalten, wurde eine graphische Benutzeroberfläche für die Schnittstelle des Testbeds entworfen. Mit dieser war es möglich viele Probleme in der Implementierung des Protokolls aufzudecken. Allerdings waren nach Abschluss der Masterarbeit nach einige Probleme im Protokoll vorhanden, welche bei längeren Laufzeiten des Systems auftraten. Damit diese Probleme nicht die Integration der Fountain-Codes beeinträchtigten, wurde ein bestehendes Routing-Protokoll verwendet. Allerdings konnte durch das CSMA/CA-Verfahren eine Verbesserung der Verbindungsqualität erzielt werden.

Im Berichtszeitraum wurde das vorgestellte Betriebssystem langOS als Open Source Projekt registriert und auf SourceForge unter https://sourceforge.net/projects/langos/ veröffentlicht.

1.6.3. Universelles Intrusion Detection System (IDS)

Bei der Erkennung von Manipulationen an Sensorwerten ist eine kontinuierliche Überwachung der Messwerte notwendig. Dazu wurde basierend auf der Signifikanzanalyse[11] ein Verfahren entwickelt, welches es ermöglicht eine kontinuierliche Überwachung von Messdaten durchzuführen. Die *Timeslot-based Significance Analysis (TSSA)* wurde für die geringen Ressourcen der Zielplattform optimiert, so dass nur eine geringe Belastung des Prozessors und des Speichers entsteht. Dazu wird der eingehende Datenstrom in Zeitschlitze eingeteilt (siehe Abbildung 6) und die dazugehörigen Daten mittels eines geeigneten Mittelwertverfahrens reduziert. Diese Vorgehensweise minimiert zum einen die Menge der zu betrachtenden Daten und zum anderen können kleine natürliche Abweichungen gefiltert werden. Die Mittelwerte der einzelnen Zeitschlitze werden dann mittels Signifikanzanalyse untersucht. Wenn signifikante Änderungen im Verlauf der Daten auftreten, zeigen sich diese in einem Ausschlag der Ergebnisse. Durch eine einfache Peak-Detektion können nun aus den vorhandenen Daten verdächtige Sensorwerte ermittelt werden.

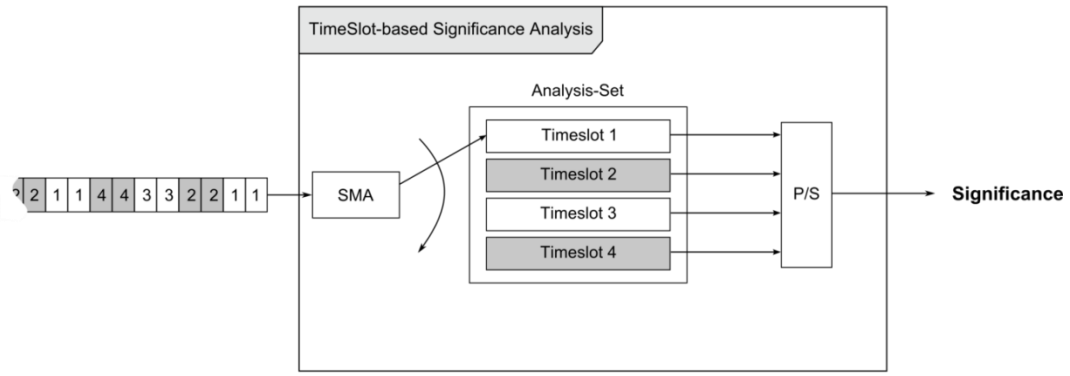


Abbildung 6: Konzept der TimeSlot-based Significance Analysis (TSSA)

Die Erkennung von Manipulationen des Protokollverhaltens zeigt sich ähnlich der Sensordaten. Allerdings stehen hier verschiedene Daten in Relation zueinander. Des Weiteren darf die Analyse die Applikation und den dazugehörigen Netzwerkstack nicht negativ beeinflussen. Für diesen Zweck wurde ein Verfahren entwickelt, welches sich gut in den Netzwerkstack integrieren lässt und die Sensorapplikation nicht negativ beeinflusst. Dieses wird im nächsten Abschnitt näher erläutert. Für die Analyse der Paketstatistiken sowie der Meta-Informationen (z. B. RSSI-Werte) wird dann das in AP5.1 verwendete TSSA-Verfahren angewandt. Für die Analyse der Header-Informationen kommt ein zusätzliches Verfahren, die *Data-Set Significance Analysis (DSSA)* zum Einsatz, welches ähnlich der TSSA funktioniert. Allerdings wurde es nicht für kontinuierliche, sondern für paketspezifische Daten entwickelt. Die Evaluierung der Algorithmen wurde anhand von gesammelten Messdaten und Paketinformationen durchgeführt. Allerdings war ein direkter Vergleich mit anderen Algorithmen nicht möglich, weil es keine standardisierte Ausführungsplattform und Vergleichsverfahren gibt.

Das IHP hat ein Konzept entwickelt, welches es ermöglicht beliebige Algorithmen unabhängig vom Betriebssystem und der verwendeten Architektur auszuführen. Außerdem wurde im Laufe des

[11] Kornemann, S., Ortmann, S., Langendörfer, P., & Fragkiadakis, A. Enabling Wireless Sensor Nodes for Self-Contained Jamming Detection. *Journal of Cyber Security*, *3*(2), 133-158.

Projektes festgestellt, dass ein fixer Algorithmus für die Erkennung der verschiedenen Angriffe nicht sinnvoll ist. Da sich die Methoden der Angreifer sehr schnell anpassen, muss sich auch das Sicherheitssystem schnell und leicht anpassen lassen. Das Konzept unterstützt diese Flexibilität.

Universal Intrusion Detection System (IDS)

Dazu wurde ein Interpreter entworfen, welcher IDS-Algorithmen ausführen kann und es ermöglicht diese leicht in bestehende Betriebssysteme zu integrieren. Dazu müssen die Sicherheitsalgorithmen zunächst in einen spezifischen Bytecode kompiliert und dann in den Interpreter geladen werden. Die Architektur des Interpreter wird in Abbildung 7 dargestellt. Die Integration ins Betriebssystem wird durch Dienstzugangspunkte (SAPs) realisiert. Diese sind zwischen den Schichten des Protokollstapels lokalisiert. Die SAPs generieren bei eingehenden Daten/Paketen ein Event, welches dem Interpreter veranlasst einen spezifischen Bytecode auszuführen. Zur Validierung wurde das Konzept in das langOS Betriebssystem integriert. Die Erweiterungen des Betriebssystem, welche im Arbeitspaket 4 entwickelt wurden, konnten zu einer einfachen Implementierung beitragen. Für die Entwicklung von Sicherheitsalgorithmen für dieses System, wurde ein Assembler entwickelt.

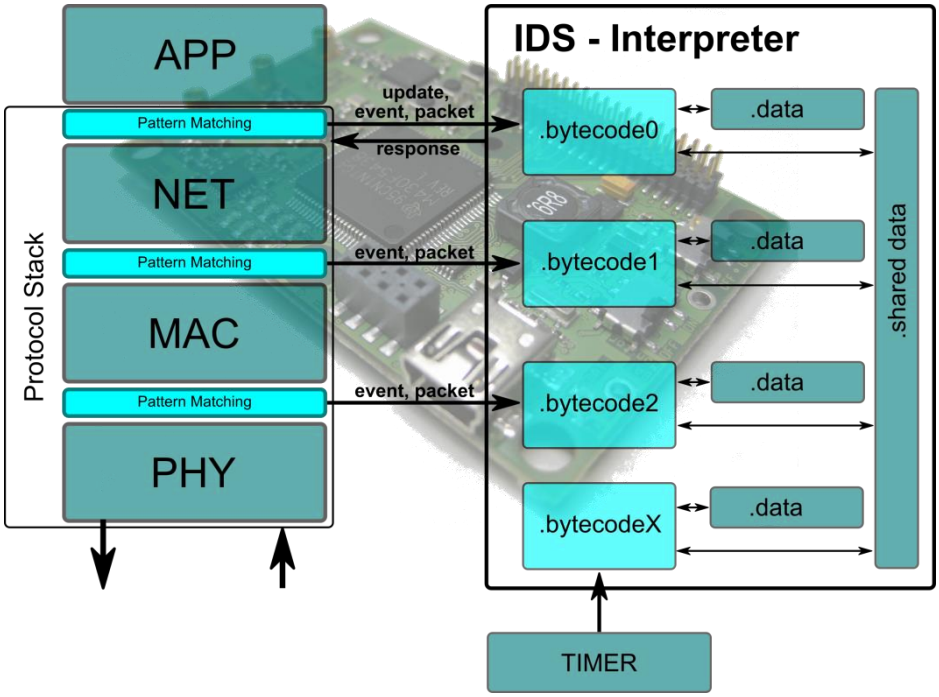


Abbildung 7: Architektur des IDS Interpreter

Damit auch Hochsprachen für die Entwicklung der Sicherheitsalgorithmen verwendet werden können wurde an einer Compiler-Pipeline gearbeitet. Das erste Konzept der Pipeline (Abbildung 8) beinhaltete den Entwurf des IDS-Algorithmus in der funktionalen Hochsprache Haskell. Diese Sprache eignete sich zwar gut für die Beschreibung der Sicherheitsalgorithmen, allerdings zeigten sich nach der Übersetzung des Quelltextes in die Zwischensprache LLVM einige Probleme. Die Ausgabe des Compilers war sehr komplex, da die gesamte Laufzeitumgebung von Haskell mit übersetzt wurde. Da der zeitliche Aufwand sehr hoch gewesen wäre, wurde beschlossen den IDS Algorithmus in einer imperativen Sprache bereitzustellen. Somit konnte mit Hilfe des Clang-Compilers der C-Code in entsprechenden LLVM Code übersetzt werden. Die Teilschritte für die Werkzeugkette wurden so ausgelegt, dass Synergien mit dem Arbeitspacket 2 genutzt werden konnten. Somit mussten nur

architekturspezifische Anpassungen an den Transformationsmodulen des CoMet-Frameworks für dieses Arbeitspacket implementiert werden.

Die Umsetzung des Backend hatte sehr viel Zeit in Anspruch genommen und es mussten aufgrund der Komplexität, Einschränkungen in der Funktionalität vorgenommen werden. Somit werden in der aktuellen Version nicht alle Instruktionen unterstützt. Auch eine Optimierung des MaMa-spezifischen Zwischencode konnte somit nicht realisiert werden. Für die Weiterverarbeitung des Codes wurden verschiedene Transformations-Module für das CoMet-Framework entwickelt. Da die Ausgangssprache sehr allgemein gehalten wurde, mussten zunächst die zur Verfügung stehenden Instruktionen in die Instruktionen der Zielarchitektur überführt werden. Des Weiteren mussten noch Transformationen für spezifische Optimierung erstellt werden. Damit die virtuellen Register der Ausgangsarchitektur auf die der Zielarchitektur abgebildet werden konnten, wurden Module zur Registerallokation implementiert. Für die Generierung des Bytecode wurde ebenfalls ein Modul geschrieben.

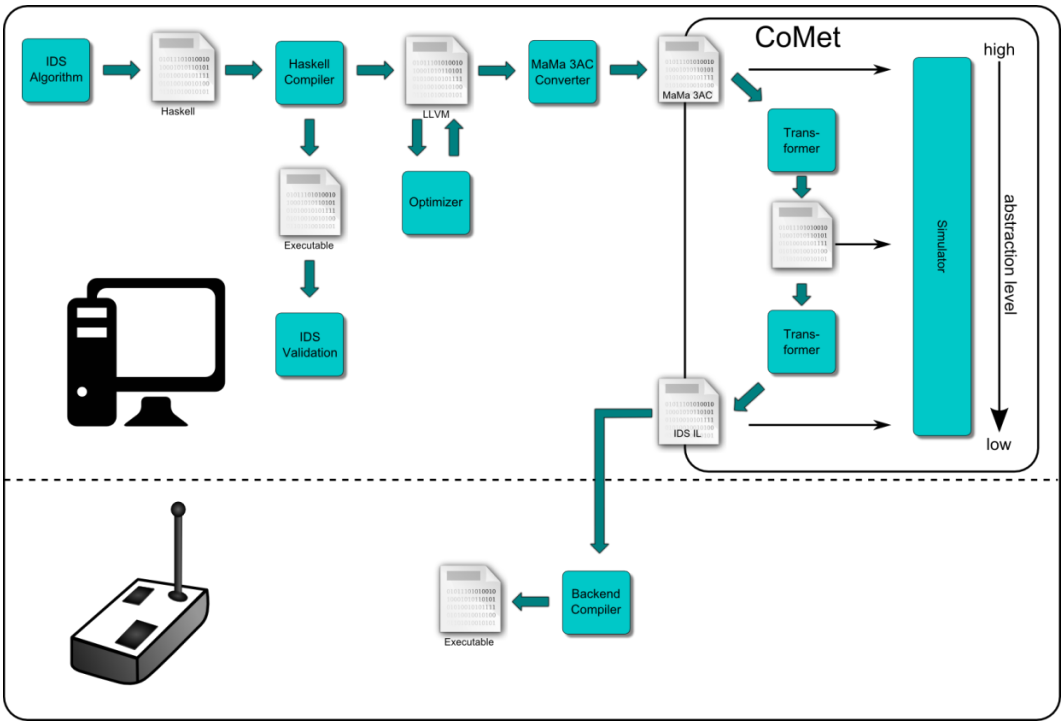


Abbildung 8: Gesamtüberblick der Compiler-Pipeline

Im Laufe des Projektes zeigte sich, dass sich das CoMet-Framework prinzipiell für Simulationen der Zielarchitektur eignet. Allerdings konnten aufgrund interner Strukturen diese nicht ideal genutzt werden. Somit war es nur bedingt möglich die Simulation für Laufzeitmessungen zu nutzen.

Demonstrator

Der vorgestellte Interpreter wurde in das langOS Betriebssystem integriert und auf dem IHPnode wurde die Funktionalität validiert.

Im Projektzeitraum wurde auch ein Demonstrator des IDS-Systems umgesetzt. Dieser setzt ein SmartHome-Szenario um. Für den Demonstrator wurde eine einfache Sensorapplikation entworfen, welche periodisch die aktuelle Temperatur sowie Luftfeuchte über ein angeschlossenes Sensorboard misst. Diese Werte werden dann zu einer Senke über das CC1101-Funkmodul gesendet. Die Senke verarbeitet die empfangenen Werte und bereitet diese grafisch in einer Webseite auf (Abbildung 9).

Die Senke ist ein Raspberry Pi, welcher als Gateway-Knoten dient. Auf diesem läuft ein Apache Webserver und ermöglicht über ein WLAN-Modul den Zugriff von mobilen Endgeräten.

Nachdem die Sensor-Applikation ein Paket mit den Messdaten versendet, wird ein Event ausgelöst. Dieses triggert den Interpreter, welcher den registrierten Bytecode ausführt. Der Bytecode überprüft die oberen und unteren Grenzwerte der beiden Messwerte und fügt an das Paket ein Status-Byte an. Dieses Status-Byte wird ebenfalls in der Webseite dargestellt. Die Webseite ermöglicht auch die Änderung des Bytecode. Die Änderung wird erreicht, indem ein neuer Bytecode an die Sensorknoten versandt wird. Diese überschreiben ihren aktuellen Bytecode.

Abbildung 9: Grafische Oberfläche des Smart Meters

1.7.Abschlusspräsentation

Als Abschluss des Projektes wurde am 23. Februar 2016 in Offenburg eine Präsentation der Ergebnisse durchgeführt. An der Präsentation nahmen alle Projektpartner teil.

Das IHP präsentierte in Kooperation mit der RUB das ICA-Verfahren. Hierfür wurden von der RUB die generellen Prinzipien des Verfahrens und die Realisierung auf den tinyVLIW8 in einem Vortrag präsentiert.

Außerdem wurde das universelle IDS in einem Demonstrator vorgeführt. Dazu wurde ein Sensornetz im Präsentationsraum aufgebaut, welches mit einem Gateway kommunizierte. Im Vortrag wurde dann auf das Konzept und dessen Integration auf Sensorknoten eingegangen. Die direkte Umsetzung konnte mit Hilfe des Demonstrators interaktiv gezeigt werden.

2. Zahlenmäßiger Nachweis

Dem IHP sind im Rahmen des UNIKOPS Projektes, die folgenden Kostenposition gefördert worden.

Position	Beschreibung
0812	Beschäftigungsentgelt E12-E15
0817	Beschäftigungsentgelt E1-E11
0822	Sonstige Beschäftigungsentgelte
0835	Vergabe von Aufträgen
0843	Sonstige allgemeine Verwaltungsausgaben
0846	Dienstreisen

Tabelle 3: Kostenposition des IHP

Durch die Beschäftigungsentgelte konnten über die Projektlaufzeit zwei wissenschaftliche Mitarbeiter Vollzeit beschäftigt werden. Darüber hinaus konnten zwei studentische Hilfskräfte finanziert werden, die die Programmierung von einzelnen Modulen unterstützten.

Zur Deckung der mit dem Zuwendungszweck zusammenhängenden Ausgaben für Infrastrukturleistungen wurde ein Zuschlag von 10 % auf die gesamten für das Vorhaben angesetzten Personalausgaben angewandt.

Die Reisemittel wurden für die Reisen zu den Projekttreffen und zur Teilnahme an Fachkonferenzen genutzt.

3. Notwendigkeit und Angemessenheit der geleisteten Arbeiten

Die Entwicklungen in den Bereichen Industrie 4.0, Home Automation und Ambient Assisted Living sowie Medical Life Care. Aktuelle Marktprognosen zeigen, dass der Bedarf in den nächsten Jahren überproportional steigen wird. Hiermit verbunden ist aber auch der Bedarf nach Sicherheitslösungen für die Klasse von Geräten. Insbesondere die eingeschränkten Ressourcen und die Besonderheiten bei den Ad-Hoc-Netzwerken führen dazu, dass bestehende Sicherheitslösungen, wie sie im Bereich der Bürogeräte/PCs seit langen zu finden sind, nur eingeschränkt wiederverwendet werden können.

Dazu wurden im UNIKOPS-Projekt mit dem ICA-Verfahren und dem universellen IDS zwei essentielle Konzepte erarbeitet, welche auf die beschränkten Ressourcen angepasst sind und eine optimale Sicherheitslösung darstellen. Dieses war nur möglich durch den Einsatz von zwei Wissenschaftlern, welche im Bereich von Software- und Hardware-Sicherheitslösungen spezialisiert sind. Durch die Unterstützung der Arbeiten durch die studentischen Hilfskräfte konnte die Umsetzung der Konzepte in der Projektlaufzeit realisiert werden. Ebenso die Unterstützung der Arbeiten in der Testphase war essentiell für die Fertigstellung der Demonstratoren.

4. Nutzen und Verwendbarkeit der Ergebnisse

4.1.1. Verwendung in weiteren Forschungsprojekten

Das IHP und dessen Abteilung Systeme sind stetig aktiv an verschiedenen Forschungsprojekten beteiligt. Ein Schwerpunkt liegt hierbei beim Entwurf und der Entwicklung von Sensorknoten im sicherheitskritischen Umfeld. Die gewonnen Erkenntnisse aus dem UNIKOPS-Projekt können direkt und indirekt wiederverwendet werden. Zusätzlich ermöglichen Gemeinsamkeiten zwischen den

Projekten die Nutzung von Synergien. So wird insbesondere das ICA-Verfahren, das Betriebssystem langOS sowie die Arbeiten an einem universellen IDS in auch in anderen Projekten verwendet.

4.1.2. KOMKAB – Kommunizierende Kabine

Das Projekt KOMKAB beschäftigt sich mit der drahtlosen Kommunikation von Sensoren mit einem Kabinenmanagementsystem. Die Arbeiten am Intrusion Detection System werden in diesem Projekt weitergeführt und erweitert, um ein sicheres Gesamtsystem zu gewährleisten.

4.1.3. DIAMANT – Zuverlässigkeit für hochsensible langlebige komplexe verteilte Anwendung

Ziel des Vorhabens ist die Entwicklung einer Cross-Plattform für Sensorknoten. Eine Cross-Plattform stellt eine vereinheitlichte Schnittstelle zu verschiedenen Betriebssystemen für Sensorknoten bereit. Im Projekt wird auch das langOS Betriebssystem für die Untersuchungen genutzt. Außerdem wird das Testbed für das Projekt erweitert.

4.2.Nutzung in Forschung und Lehre

Das IHP verfügt über enge Kooperationen mit Hochschulen in Berlin und Brandenburg. So werden unter anderem zwei Lehrstühle der BTU Cottbus durch Mitarbeiter des IHPs geleitet. Die Forschungsinhalte des Lehrstuhls „Sicherheit in pervasiven Systemen“ stehen in direktem Zusammenhang mit den Forschungszielen des Projektes UNIKOPS. Die Entwicklung von sicheren Sensorknoten ist auch hier zentraler Schwerpunkt der Forschung. So können Erkenntnisse aus dem Projekt UNIKOPS direkt in der Lehre wiederverwendet werden.

Darüber hinaus werden für Studierende der Hochschulen Berlin/Brandenburg Praktika und Abschlussarbeiten am IHP angeboten. Die zu bearbeitenden Themen sind hierbei oftmals auf den Bereich der sicheren eingebetteten Systeme ausgelegt. Mit dem IHPnode, langOS Betriebssystem und dem entwickelten Testbed kann den Studierenden hierfür Hardware und Software zur Verfügung gestellt werden, die sie selbständig weiterentwickeln und erproben können.

5. Fortschritte bei anderen Stellen

Das Interesse an smarten Geräten wächst stetig und viele mehr drahtlose Systeme wurden während der Laufzeit des Projektes von der Industrie entwickelt. Allerdings ist die Sicherheit der Systeme und Kommunikation nicht garantiert. Jeder Hersteller verwendet seine meist proprietären Standards. Somit wird es immer wichtiger universelle Sicherheitslösungen zu entwickeln. Die von UNIKOPS adressierten Schwerpunkte Code-Update, Funktionsfreischaltung, Code-Attestierung und Intrusion Detection Systeme sind somit von zentraler Bedeutung.

Da das universelle IDS für heterogene Sensoren entwickelt wurde, ist es ideal für die die Vielzahl von unterschiedlichen Systemen geeignet. Auch die Anpassungsfähigkeit der Sicherheitsalgorithmen kann optimal an die Anwendung angepasst werden und für ein sicheres und stabiles Gesamtsystem beitragen.

Auch der Einsatz von Code-Attestierungsverfahren wird immer wichtiger, die Intellectual Property des Programmcodeherstellers zu schützen. Durch den Einsatz des ICA-Verfahrens wird dieses effizient erreicht.

6. Erfolgte und geplante Veröffentlichungen

[1] **Custom-fit security for efficient and pollution-resistant multicast OTA-programming with fountain codes.**

Stecklina, O., Kornemann, S., Grehl, F., Jung, R., Kranz, T., Leander, G., ... & Westhoff, D. (2015, July). In "*Innovations for Community Services (I4CS), 2015 15th International Conference on*"(pp. 1-8). IEEE

[2] **langOS-A Low Power Application-specific Configurable Operating System.**

Stecklina, O., Krumholz, A., & Kornemann, S. (2014, September). FGSN 2014 13. Fachgespräch „Drahtlose Sensornetze" (Potsdam, Deutschland)

[3] **Intrinsic Code Attestation by Instruction Chaining for Embedded Devices.**

Stecklina, O., Langendörfer, P., Vater, F., Kranz, T., & Leander, G. (2015, October). In "*International Conference on Security and Privacy in Communication Systems"* (pp. 97-115). Springer International Publishing.

[4] **Design of a tailor-made memory protection unit for low power microcontrollers.**

Stecklina, O., Langendörfer, P., & Menzel, H. (2013, June). In "*2013 8th IEEE International Symposium on Industrial Embedded Systems (SIES)*"(pp. 225-231). IEEE.

Berichtsblatt

1. ISBN oder ISSN	2. Berichtsart (Schlussbericht oder Veröffentlichung) Schlussbericht

3. Titel
Schlussbericht

UNIKOPS - Universell konfigurierbare Sicherheitslösung für Cyber-Physikalische heterogene Systeme

4. Autor(en) [Name(n), Vorname(n)]	5. Abschlussdatum des Vorhabens 29.02.2016
Prof. Dr. Langendörfer, Peter Kornemann , Stephan	6. Veröffentlichungsdatum
	7. Form der Publikation Bericht
8. Durchführende Institution(en) (Name, Adresse) IHP GmbH – Innovations for High Performance Microelectronics/Leibniz-Institut für innovative Mikroelektronik Im Technologiepark 25 15236 Frankfurt (Oder)	9. Ber. Nr. Durchführende Institution
	10. Förderkennzeichen 16KIS0004
	11. Seitenzahl 23
12. Fördernde Institution (Name, Adresse) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	13. Literaturangaben 11
	14. Tabellen 3
	15. Abbildungen 9

16. Zusätzliche Angaben

17. Vorgelegt bei (Titel, Ort, Datum)

18. Kurzfassung

In der Zukunft werden eingebettete Geräte und Systeme, die besonders eng mit der physikalischen Umgebung verbunden sind, immer wichtiger. Um solche Anwendungen abzusichern sind spezielle Schutzmechanismen notwendig. Diese müssen Sicherheitsfunktionen bieten, welche für Hersteller bzw. Anwender einfach einsetzbar und konfigurierbar sind sowie besonders energie-, kommunikations- und kosteneffizient sein.

UNIKOPS hat zum Ziel, universelle konfigurierbare Sicherheitslösungen für eingebettete Geräte und Systeme zu entwickeln. Dabei werden unterschiedliche Anwendungen wie Smart Metering, das Internet der Dinge (IoT) und das Ambient Assisted Living (AAL) adressiert. Die zu entwickelnden Sicherheitslösungen sollen gleichzeitig Anforderungen an Energieeffizienz und Speicherbedarf genügen. Als Teilziele des Projektes zur Sicherstellung der Systemintegrität sollen u.a. ein Systemschutz, eine bedarfsweise Funktionsfreischaltung, die vertrauliche Datenfusion überwachter und übermittelter Daten, sowei die Erkennung von Angriffen und Manipulationsversuchen entwickelt und umgesetzt werden. Zur Sicherstellung der Systemintegrität von eingebetteten Systemen wurde vom IHP das Intrinsic-Code-Attestation (ICA)-Verfahren entwickelt. Dieses erlaubt es mit Hilfe einer speziellen Hardware-Einheit nur authentifizierten Programmcode auszuführen. Das ICA-Verfahren wurde als Patent angemeldet.Damit auch Manipulationen der Kommunikationswege sowie der Daten ermittelt werden können, wurde speziell für heterogene Systeme ein neuartiges Sicherheitskonzept entwickelt, welches es ermöglicht, ein individuelles Sicherheitsniveau zu erreichen. Dieses System wurde so entworfen, dass es sich leicht in aktuelle Sensornetz-Betriebssysteme integrieren lässt.

19. Schlagwörter
ICA, IDS, WSN, Security

20. Verlag	21. Preis

Document Control Sheet

1. ISBN or ISSN	2. type of document (e.g. report, publication) report
3. title Schlussbericht UNIKOPS - Universell konfigurierbare Sicherheitslösung für Cyber-Physikalische heterogene Systeme	
4. author(s) (family name, first name(s)) Prof. Dr. Langendörfer, Peter Kornemann , Stephan	5. end of project 29.02.2016
	6. publication date
	7. form of publication Report
8. performing organization(s) (name, address)	9. originator's report no.
	10. reference no. 16KIS0004
	11. no. of pages 23
12. sponsoring agency (name, address) Bundesministerium für Bildung und Forschung (BMBF) 53170 Bonn	13. no. of references 11
	14. no. of tables 3
	15. no. of figures 9
16. supplementary notes	
17. presented at (title, place, date)	

18. abstract

Embedded devices and systems, which are closely coupled with the physical environment, will become more and more important in the near future. For the protection of these applications special security mechanisms are required. These must provide security functions which manufacturers and users can easily apply and configure. In addition, energy, communication as well as cost efficiency must also be taken into account during the design and implementation of the embedded systems.

The project UNIKOPS aims to tackle all these requirements by providing a universal configurable security solution for embedded systems. It addresses a broad variety of applications, e.g. smart metering, internet of thins (IoT) and ambient assisted living (AAL). In addition, it takes energy efficiency and constraint resources into account. To guarantee system integrity, on-demand function clearing, a trustworthy data fusion of monitored and transmitted data as well as the detection of protocol attacks and data manipulations were investigated and implemented.
IHP developed the intrinsic code attestation (ICA) method to ensure system integrity of embedded systems. A special hardware unit allows only the execution of authenticated program code. The ICA method was registered as a patent.
Manipulation of the communication channels and data has been considered and a new security concept was developed. It is especially designed for heterogeneous systems to provide individual security levels. This system has been designed for easy integration into current sensor network operating systems.

19. keywords
ICA, IDS, WSN, Security

20. publisher	21. price