Sicherheitszertifizierung für die Digitale Transformation

Anwendung auf den Industrial Data Space

Die Digitale Transformation bedeutet für Firmen nicht nur die Erzeugung, Vernetzung und Verarbeitung von Daten in unternehmensinternen Prozessen, sondern auch eine engere datenbasierte Zusammenarbeit über Unternehmensgrenzen hinweg. Der Industrial Data Space bietet die dafür notwendige Dateninfrastruktur, indem er es ermöglicht, Daten dezentral (Punkt zu Punkt) auszutauschen, ihnen Nutzungsbedingungen anzuheften, die auch nach der Übertragung vom Empfänger respektiert werden und durch ein Zertifizierungsschema Vertrauen zwischen den Teilnehmern sicherstellt. Die effiziente (Re-)Zertifizierung der in komplexen Daten-Ökosystemen wie dem Industrial Data Space eingesetzten Software wird durch automatisierte Zertifizierungsprozesse ermöglicht und anhand des Werkzeugs CARiSMA exemplarisch gezeigt.

Mit der Digitalisierung eröffnen sich für Unternehmen jeglicher Branche neue Möglichkeiten, durch Datengewinnung und -austausch Prozesse deutlich effizienter zu gestalten oder gänzlich neue Geschäftsmodelle im Sinne datengetriebener Services oder Produkte anzubieten, wie integrierte Tracking-Information in der Supply Chain oder Predictive-Maintenance-Dienste für Maschinen und Anlagen. Diese Beispiele zeigen, dass Daten gerade dann an Wert gewinnen, wenn sie ausgetauscht und mit Daten anderer Quellen vernetzt werden. Der Agrarmaschinenhersteller Claas bietet beispielsweise Apps für seine Mähdrescher an, um während des Erntevorgangs den Ertrag und die Nährstoffzusammensetzung und so auf den Quadratmeter genau die erforderliche optimale Düngermischung für die nachfolgende Aussaat zu berechnen [1]. Dies setzt u.a. die Zusammenarbeit und den Austausch von Daten zwischen dem Anlagenhersteller, -betreiber und Düngemittelhersteller voraus.

Die Stärke deutscher Unternehmen liegt vor allem in dem Bau von Maschinen und Anlagen und somit in der Erzeugung der Daten, die die Basis für die Digitalisierung bilden. Gleichzeitig bestehen gerade bei europäischen und deutschen Unternehmen Vorbehalte gegenüber dem Prinzip „dare to share“ aus Angst vor dem unkontrollierten Abfluss von Daten. Spätestens außerhalb Europas werden viele Datenschutzregelungen als unzureichend angesehen. Die Unternehmen sehen sich folglich dem Konflikt ausgesetzt, einerseits im Sinne der Wettbewerbsfähigkeit Daten austauschen und andererseits ihre Daten schützen zu müssen.

Diese scheinbare Unvereinbarkeit lässt sich durch eine Dateninfrastruktur auflösen, die Datensouveränität gewährleistet. Der Industrial Data Space bietet eine technische Lösung, Daten Nutzungsbedingungen anzuheften, die auch nach der Datenübertragung im empfangenden Software-Gateway respektiert werden [2]. Dies setzt voraus, dass die Teilnehmer und die eingesetzte Software im Industrial Data Space vertrauenswürdig sind. Dies wird durch Zertifizierung der Organisation und der Software gemäß eines spezifischen Zertifizierungsschemas sowie gegebenenfalls entsprechend Richtlinien relevanter Verbände und gesetzlich festgelegten Standards sichergestellt. Insbesondere die Zertifizierung der Software unterliegt jedoch einem aufwändigen und fehleranfälligen Prozess, der für jede Änderung an der Komponente erneut durchgeführt werden muss.

Das an der Universität Koblenz-Landau entwickelte Sicherheitsmodellierungs- und Analysewerkzeug CARiSMA bietet Ansätze, die in einer teilautomatisierten und effizienten Erstzertifizierung angewendet werden können und auch bereits exemplarisch im Rahmen von Cloud Computing angewendet wurden. Basierend auf diesen Ansätzen werden im Folgenden die Anforderungen und Abläufe einer automatisierten Zertifizierung und Rezertifizierung von Software anhand des Beispiels Industrial Data Space erläutert.

Zunächst werden der Industrial Data Space vorgestellt, dessen Eigenschaften charakterisiert und anschließend die Anforderungen an eine Zertifizierung erörtert. Darauf aufbauend wird gezeigt, welche dieser Anforderungen bereits von bestehenden Technologien von CARiSMA abgedeckt werden. Auf dieser Grundlage wird ein Konzept für eine Erstzertifizierung sowie anschließend eine Erweiterung um eine Rezertifizierung vorgestellt. Im letzten Abschnitt werden die Vorteile, Herausforderungen sowie unser Ansatz für eine automatisierte (Re-)Zertifizierung zusammengefasst.

Der Industrial Data Space

Der Industrial Data Space wurde federführend durch die Fraunhofer-Gesellschaft entwickelt und ermöglicht den sicheren und kontrollierbaren Austausch von Daten zwischen Unternehmen. Damit Unternehmen auf dieser Basis neue Services und Produkte anbieten können, hat

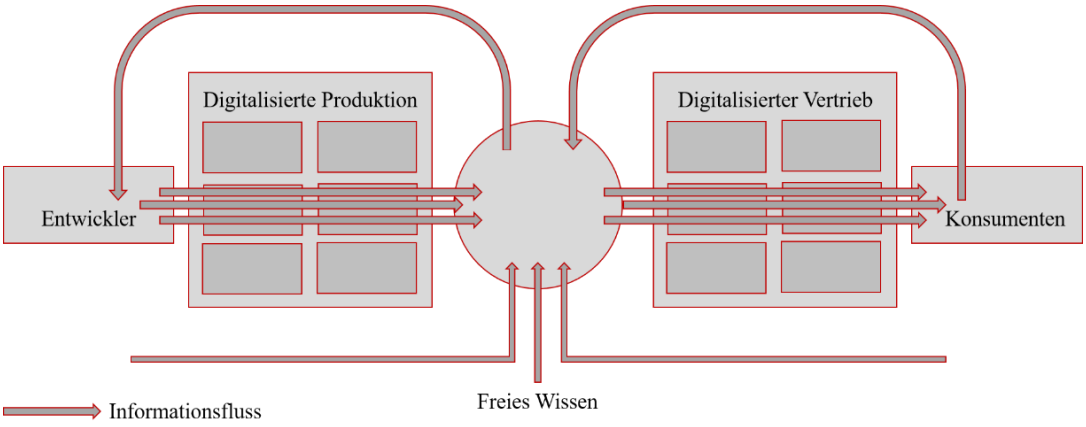

Abbildung 1: Informationsfluss im Industrial Data Space

der Industrial Data Space die Vernetzung von Daten aus heterogenen Quellen verschiedener Domänen und Funktionen zur Aufgabe (vgl. Abbildung 1). Dazu werden Daten von Seiten der Leistungserstellung (Beschaffung, Produktion) mit denen des Vertriebs verknüpft. Auch freie und öffentliche Datenquellen lassen sich in dieses „Smart Data Management“ einbinden. Das Datenangebot wird ähnlich einer Suchmaschine über einen Industrial Data Space Broker publiziert und mithilfe von Metadaten beschrieben, die u.a. Berechtigungen und ggf. einen Preis enthalten. Der Datenaustausch zwischen Anbieter und Nutzer findet Punkt zu Punkt über den Industrial Data Space Connector, ein Software-Gateway, statt. Der IDS Connecter ist insofern „smart“, als dass in ihm IT-Services („Apps“) eingehängt werden können, die etwa Legacy-Systeme anbinden oder Berechnungen (z.B. einen Planungsalgorithmus) ausführen. Der Datenbereitsteller kann über das IDS Metadatenvokabular seinen Daten Nutzungsbedingungen bezüglich Dauer der Nutzung, Anzahl der Aufrufe, Rollen und der Apps beim Empfänger anheften. Dadurch kann beispielsweise verhindert werden, dass bestimmte Daten zusammengeführt oder für einen anderen als den ursprünglichen vereinbarten Zweck verwendet werden.

Zwar bildet Dezentralität ein Kernelement des Industrial Data Space. Gleichwohl lassen sich die Connectors nicht nur als Endpunkte für einzelne Server, PCs oder Geräte des Internet of Things nutzen, sondern auch für cloudbasierte Dienste.

Die im Rahmen eines Cloud-Computing-Angebots angemieteten Ressourcen, unterteilen sich in drei Ebenen. Zunächst bietet Infrastructure-as-a-Service (IaaS) das Anmieten von Hardware und einer minimalen Infrastruktur. Platform-as-a-Service (PaaS) stellt ein Betriebssystem zur Verfügung, auf dem Software eingespielt werden kann, während Software-as-a-Service (SaaS) nur die Verarbeitung oder Lagerung von Daten anbietet. Die Risiken hängen stark von der verwendeten Ebene sowie dem verwendeten Verteilungsmodell ab (z.B. öffentlich, privat, intern, extern). Im Industrial Data Space können neben selbst betriebenen Rechenzentren alle drei Ebenen zum Einsatz kommen und müssen in entsprechenden Arbeiten berücksichtigt werden.

Die am Industrial Data Space beteiligten Unternehmen und Forschungseinrichtungen konzentrieren ihre Arbeit hauptsächlich auf die Erstellung von Anforderungskatalogen, Richtlinien und Verträgen, wobei die Umsetzung dieser den jeweiligen Zertifizierungsstellen und Dienstanbietern überlassen wird. Trotz der hohen Komplexität und der Notwendigkeit zur Berücksichtigung unterschiedlichster Anforderungen sowie Anhängigkeiten wird mangels ausreichender Werkzeugunterstützung vor allem in der Zertifizierung auf eine rein manuelle Kontrolle der zu zertifizierenden Artefakte gesetzt.

Weiterhin liegen für den Industrial Data Space als neue Idee bisher nur wenige Forschungsergebnisse vor. Es lassen sich jedoch einige der auf den Ansatz des Cloud Computing bezogenen Forschungsergebnisse auf den Industrial Data Space übertragen. Zu berücksichtigen ist dabei, dass es sich beim Cloud-Computing im Vergleich zum Industrial Data Space vielmehr um einen offenen Ansatz handelt, der teils mit geringeren, vor allem aber anderen, Sicherheitsanforderungen verbundenen ist.

Vom Cloud Computing auf den Industrial Data Space lassen sich vor allem Arbeiten zur Kommunikationssicherheit und Identifizierung der an der Kommunikation beteiligten Parteien übertragen. Ein zusätzlicher Fokus im Industrial Data Space liegt auf Nutzungsbestimmungen der zwischen Unternehmen ausgetauschten Daten.

Sicherheitszertifizierung im Industrial Data Space

Bei unternehmensübergreifenden Geschäftsprozessen im Industrial Data Space und dem damit verbundenen Austausch von Daten sind verschiedene Compliance-Auflagen zu berücksichtigen. Es muss geprüft werden, welche Daten und in welcher Form das Unternehmen verlassen dürfen sowie zu welchen Zwecken diese Daten verwendet werden dürfen. Dürfen die jeweiligen Daten das Unternehmen verlassen, so kann z.B. abhängig vom Verwendungszweck eine Anonymisierung notwendig sein. Sämtliche in diesem Prozess beteiligten Komponenten von der Entscheidungsfindung über die Anonymisierung und Übertragung bis zur Datenverarbeitung müssen per Zertifikat belegen, dass diese die jeweils gültigen Richtlinien und Normen einhalten [3, 4, 5].

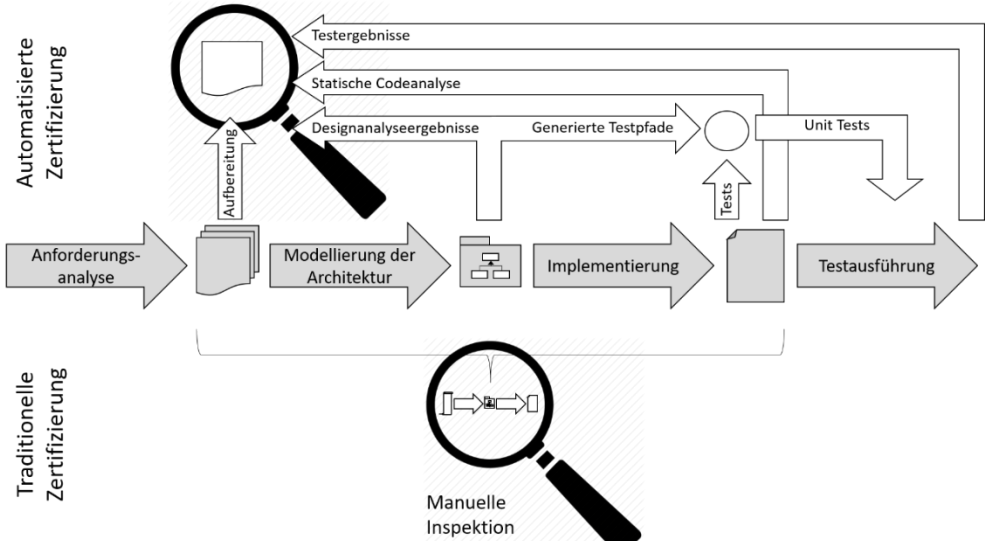

Abbildung 2: Manueller und automatisierter Zertifizierungsprozess

Allgemein werden solche Zertifizierungen in der Industrie nach manueller Analyse unter Zuhilfenahme von normalsprachlichen Leitfäden oder Prüfkatalogen erstellt. Speziell zur Zertifizierung von Software-as-a-Service-Lösungen hat der Verband der Cloud-Services-Industrie in Deutschland (EuroCloud Deutschland eco) ein Gütesiegel und einen zugehörigen Prüfkatalog entwickelt. Vergleichbare Zertifizierungen werden vom Industrial Data Space e.V. für einen Datenaustausch zwischen Unternehmen angestrebt und zurzeit entwickelt [6].

Relevante allgemeinere Sicherheitsstandards für Cloud-Computing, den Industrial Data Space und andere IT-Anwendungen sind das „Statement on Auditing Standards (SAS) Nummer 70 Typ II“ und das ISO-Zertifikat 27001. Medizinische Produkte müssen z.B. neben diesen Standards auch nach der EU Richtlinie 93/42/EWG bzw. deren nationalen Umsetzungen zertifiziert werden.

Aus diesen Vorbildern und gesetzlichen Standards ergibt sich die Notwendigkeit einer Sicherheitszertifizierung der verwendeten Komponenten als wichtiger Bestandteil des Industrial Data Space, um eine sichere Kommunikation sowie Datenaustausch zu ermöglichen.

Für solch eine Sicherheitszertifizierung im Industrial Data Space wurden von der Fraunhofer-Gesellschaft sechs Hauptaspekte identifiziert [6]:

- Verbindungssicherheit gegen Manipulation und Abhören der übertragenen Daten.
- Identitätsnachweis zwischen den jeweiligen Kommunikationspartnern.
- Datennutzungskontrolle zur Einhaltung von Standards zur sicheren Speicherung und Verarbeitung sowie Richtlinien zur Nutzungsdauer und Weitergabe von bereitgestellten Daten
- Sichere Ausführungsumgebung zur Einhaltung von Sicherheitslevels auf unterschiedlichen Plattformen
- Remote Attestation der Einhaltung von Löschungsfristen und der Feststellung eines vertrauenswürdigen Zustandes des Gegenübers
- Applikation-Layer-Virtualisierung für die Auslagerung von Teilsystemen in die Cloud

Zur Zertifizierung einer Komponente unter Berücksichtigung dieser Aspekte müssen vielfältige Eigenschaften berücksichtigt werden. Wird solch eine Zertifizierung ohne eine Werkzeugunterstützung durchgeführt, ergibt sich daraus ein langwieriger und fehleranfälliger Prozess.

Modellbasiertes Sicherheitstesten

Die moderne Gesellschaft und die Wirtschaft setzen auf Infrastrukturen für Kommunikation, Finanzen, Energieverteilung und Transport. Diese Infrastrukturen hängen zunehmend von vernetzten Informationssystemen ab. Dies führt zu Schwachstellen, für deren Ausnutzung in jüngster Zeit eine Reihe von weithin bekannt gewordenen Beispielen gefunden wurden. Der korrekte Entwurf und die Implementierung von sicherheitskritischen Systemen, die Teil eines Netzwerks sind, ist eine schwierige Aufgabe. In der Praxis treten die meisten Schwachstellen bei Fehlern in Implementierungen auf. Daher ist es von hoher Bedeutung, Vertrauen beim Schutz implementierter sicherheitskritischer Systeme gegen Angriffe zu gewinnen.

Zu diesem Zweck präsentieren wir Arbeiten zum systematischen Testen von sicherheitskritischen Systemen. Die Idee ist, das System (auf der abstrakten Designebene) mit einer formalen Spezifikationssprache zu spezifizieren und diese Spezifikation zu verwenden, um Testsequenzen zu generieren, um Sicherheitsschwächen in einer Implementierung auf systematische Weise zu finden. Konkret findet UMLsec Anwendung, um die nicht verknüpfte Last-Transaktion der Common Electronic Purse Specification (CEPS) zu spezifizieren. Wir verwenden diese Spezifikation, um Testsequenzen für Implementierungen des Protokolls zu generieren. CEPS ist ein Kandidat für einen global interoperablen elektronischen Geldbörsen-Standard, unterstützt von mehreren Organisationen (u.a. Visa International), die zusammen

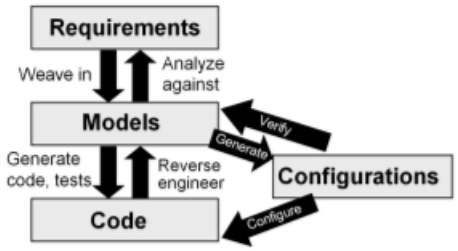

Abbildung 3: Modellbasierte Sicherheitstechnik

90 Prozent der elektronischen Geldbörsen der Welt ausmachen. Sicherheit spielt folglich in diesem Kontext eine herausragende Rolle.

Tests können bekanntermaßen nicht das Fehlen von Implementierungsfehlern beweisen. Es ist jedoch derzeit die am weitesten verbreitete Technik in der Industrie, um ein gewisses Maß an Vertrauen in der Abwesenheit größerer Fehler zu gewinnen, da das mechanisch unterstützte Beweisen der Theoreme oder die Modellüberprüfung von Code bisher in der Größe behandelbarer Systeme limitiert ist und als vergleichsweise teuer gilt.

Die Wirksamkeit des Testens hängt entscheidend von der Fähigkeit ab, geeignete Teststrategien zu identifizieren. Dies ist sehr schwierig bei der Prüfung auf Sicherheitsanforderungen, da es nicht ausreicht festzustellen, dass die meiste Zeit keine Fehler auftreten, da die verbleibenden, nicht getesteten Situationen, die zu Ausfällen führen, von motivierten Angreifern gefunden werden müssen und dann systematisch ausgebeutet werden. Vielmehr muss festgestellt werden, dass bestimmte sicherheitskritische Teile des Systems unter allen denkbaren Angriffsversuchen aus der Systemumgebung tatsächlich fehlerfrei sind. Die vorliegende Arbeit soll einige Hinweise geben, wie dies systematisch geschehen kann.

Die hier vorgestellte Arbeit ist Teil eines allgemeineren Ansatzes zur modellbasierten Sicherheitstechnik, der in Abbildung 3 dargestellt ist [7].

(Re-)Zertifizierung mittels CARiSMA

Die von uns entwickelten Techniken zur Modellierung und Verifizierung von Sicherheitsanforderungen auf UML-Modellen und konkreten Implementierungen der jeweiligen Modelle sind geeignet, um ein umfassendes Konzept zur Absicherung von digitalen Geräten und Netzwerken zu erstellen

Ein konkreter Ansatz zur Modellierung komplexer Internet-basierter Systeme, der in unserem Sicherheitsmodellierungswerkzeug CARiSMA verwendet wird, ist UMLsec [8]. Im UMLsec-Ansatz können Software-Design-Modelle, die mit der Unified Modeling Language (UML) erstellt werden, wie in Abbildung 4 mit sicherheitsrelevanten Informationen annotiert werden.

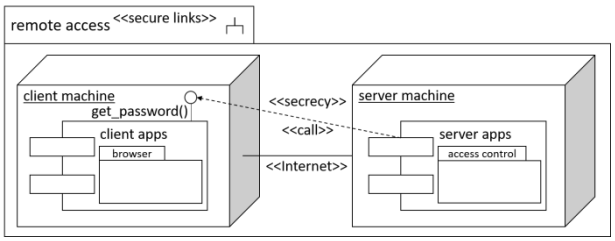

Abbildung 4: : UMLsec Beispiel Secure Links

Mittels des UMLsec-Stereotyps <<secure links>> wird in dem Beispiel aus die Anforderung spezifiziert, dass kritische Kommunikation, wie z.B. die Passwortabfrage zwischen Client und Server im Industrial Data Space, über abgesicherte Verbindungen erfolgen muss. Die kritische Kommunikation wird mittels des Stereotyps <<secrecy>> gekennzeichnet.

Diese mittels UMLsec um Sicherheitsanforderungen erweiterten UML-Modelle können nachfolgend mit automatischen Werkzeugen wie CARiSMA auf Einhaltung der mittels UMLsec spezifizierten Sicherheitsanforderungen überprüft [9] und ggf. vorhandene Schwachstellen automatisch korrigiert werden [10].

In dem Beispiel aus Abbildung 4 ist eine <<Internet>>-Verbindung nicht ausreichend, um die <<secrecy>>-Anforderung des Passwortabrufes durch einen Server aus der digitalen Produktion des Industrial Data Spaces an einen Client aus dem digitalen Vertrieb zu erfüllen.

Weiterhin kann durch die Generierung von Sicherheitsmonitoren aus den in UMLsec spezifizierten Sicherheitsanforderungen die Sicherheit auch zur Laufzeit überwacht werden [11, 7]. Ebenfalls ist eine Generierung von Testpfaden zur Überprüfung der Sicherheitsanforderungen mittels desselben Mechanismus‘ möglich.

Erstzertifizierung: Während bei einer traditionellen manuellen Zertifizierung entsprechend Abbildung 2 alle Entwicklungsschritte ganzheitlich von einem Menschen betrachtet werden, werden in CARiSMA die Ergebnisse einzelner Entwicklungsschritte automatisiert ausgewertet und aufbereitet. Dabei werden z.B. natürlich sprachliche Fragen zu Privatsphärenpräferenzen der Anwender der jeweiligen Plattform generiert.

Zukünftig können in diesen aufbereiteten Daten sowohl die existierenden Ergebnisse der Anforderungsanalyse, wie z.B. für diese Zertifizierung relevante Standards und Sicherheitsanforderungen, die Berücksichtigung und Einhaltung der Sicherheitsanforderungen in Softwaredesign bzw. Softwarearchitektur und in dessen Implementierung als auch letztendlich die Auswertung von Nutzertests und aus den Sicherheitsspezifikationen generierter Tests zusammengeführt werden.

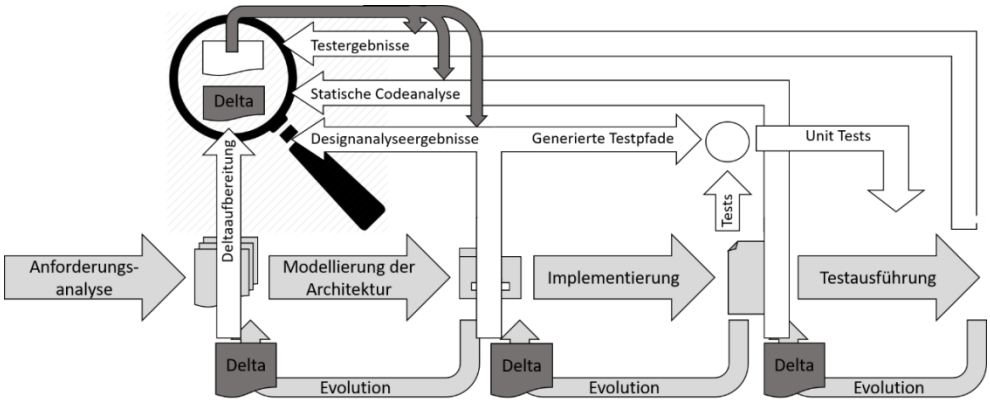

Abbildung 5: Rezertifizierung mittels CARiSMA

Dabei bilden die mittels UMLsec modellierbaren Sicherheitsanforderungen einen großen Teil der für die Sicherheitszertifizierung im Industrial Data Space benötigten Kriterien ab. Durch eine Anwendung der mit UMLsec verbundenen Werkzeuge auf die Herausforderung der Sicherheitszertifizierung im Industrial Data Space kann auch die geforderte Automatisierung des Zertifizierungsprozesses erreicht werden.

Sowohl mittels der Spezifikation und Analyse von Sicherheitsanforderungen in UMLsec werden die Architekturebene als auch durch die Generierung von Sicherheitsmonitoren und Testpfaden große Teile der Implementierungsebne abgedeckt.

Auf Grundlage der generierten Testpfade können zukünftig weiterhin die vorhandenen Nutzertests auf Abdeckung der Testpfade geprüft sowie bei Bedarf zusätzliche Tests generiert werden. Die gegebenenfalls generierten Testfälle erweitern die vorhandenen Nutzertests um sicherheitsspezifische Testfälle und werden gemeinsam mit den Nutzertest ausgeführt. Die Testergebnisse werden dann für die Zertifizierung aufbereitet.

Die Aufbereitung der Testausführung kann dabei mehr als eine Statistik über erfolgreich ausgeführte Testfälle enthalten. Durch die explizit unter dem Gesichtspunkt der Sicherheit generierten Testfälle, können in der Aufbereitung der Testergebnisse explizite Aussagen über die Eigenschaften der Implementierung bezüglich bestimmter Sicherheitsanforderungen getroffen werden.

Für die Identifizierung relevanter Regulierungen bei der Auswertung der Anforderungsanalyse werden diese als Ontologie dargestellt. Diese Ontologie kann genutzt werden, um ein gegebenes System bezüglich der Einhaltung von Compliance-Anforderungen zu untersuchen. Zusätzlich können mittels einer erweiterten Werkzeugunterstützung Systemmodelle auf bestimmte, als relevant identifizierte Eigenschaften geprüft werden [12].

Rezertifizierung: Die separate Aufbereitung einzelner Entwicklungsschritte im vorgeschlagenen Zertifizierungsprozess ermöglicht die in Abbildung 5 in dunkelgrau dargestellte Erweiterung des Zertifizierungsansatzes um eine Rezertifizierung eines zuvor mittels dieses Zertifizierungsprozesses zertifizierten Programms, in der von einem menschlichen Gutachter nur noch die aufbereiteten Änderungen begutachtet werden müssen.

Für jeden einzelnen Schritt des Entwicklungsablaufes wird in diesem Rezertifizierungsansatz ein Delta generiert, welches die vorgenommenen Änderungen beinhaltet. Anhand dieses Deltas wird der jeweils vorangehende Schritt neu bewertet und ggf. z.B. neue einzuhaltende Normen, Sicherheitsanforderungen, Testpfade oder Sicherheitsmonitore generiert und an den nachfolgenden Schritt übergeben.

Bei der Präsentation der Ergebnisse können diese Deltas und die Ergebnisse der erweiterten Analysen in einer Form separat aufbereitet werden, die es ermöglicht, nicht erneut alle Bestandteile des Programms und Entwicklungsprozesses für die Rezertifizierung manuell betrachten zu müssen. Dazu werden die Ergebnisse vorheriger Zertifizierungen mit den Ergebnissen der Rezertifizierung kombiniert und wiederum ein Delta berechnet, welches für eine manuelle Begutachtung ausgegeben wird.

Zusammenfassung

Durch eine starke Automatisierung des Zertifizierungs- und vor allem des Rezertifizierungsprozesses kann nicht nur die Effizienz der Zertifizierung gesteigert und eine Zertifizierung dadurch für deutlich mehr Produkte verfügbar gemacht werden. Durch eine zielgerichtete Aufbereitung der Daten sowie eine verbesserte Berücksichtigung aller Abhängigkeiten kann auch die Effektivität der Zertifizierung gesteigert werden.

In großen System wie dem Industrial Data Space ist es für einen Menschen nahezu unmöglich, alle Abhängigkeiten sowie deren Auswirkungen zu erkennen und zu beurteilen. Zu viele Implementierungen, Instanzen und Versionen kommen hierbei zum Einsatz. Eine Werkzeugunterstützung ist an dieser Stelle daher zwingend notwendig. Der von uns vorgestellte Ansatz erfüllt die Anforderungen zur Berücksichtigung von Abhängigkeiten und Auswirkungen, die an solch eine Werkzeugunterstützung gestellt werden.

Die Strukturierung des vorgestellten Zertifizierungsablaufes ermöglicht zum einen die Berücksichtigung von Abhängigkeiten innerhalb der zu zertifizierenden Plattform, zum anderen insbesondere auch solche zwischen den einzelnen Schritten des Entwicklungsprozesses.

Die bestehenden Modellierungs- und Analysefähigkeiten von CARiSMA decken bereits große Teile der benötigten Eigenschaften und Fähigkeiten ab und können mit kleinen Erweiterungen den vorgestellten (Re-)Zertifizierungsansatz unterstützen.

Dabei ist von Vorteil, dass von CARiSMA in der Softwareentwicklung weit verbreitete und standardisierte Artefakte wie z.B. UML-Modelle verwendet werden. Dies ermöglicht es, CARiSMA ohne große Anpassungen in bestehende Entwicklungsabläufe zu integrieren.

Um Software-Tests als Teil des Zertifizierungsprozesses zukünftig in einem realitätsnahen Prüfumfeld zur ermöglichen, wird ergänzend zur teilautomatisierten werkzeugbasierten Zertifizierung ein „Industrial Data Space Lab“ am Fraunhofer ISST aufgebaut. Das Lab ermöglicht es Unternehmen, ihre Implementierungen von Bausteinen des Industrial Data Space gegen andere Komponenten von verschiedenen Anbietern und auf unterschiedlichen Sicherheitslevels zu testen.

Literaturverzeichnis

[1] AgrarHeute, „Farming 4.0 bei der Getreideernte,“ [Online]. Available: https://www.agrarheute.com/news/farming-40-getreideernte. [Zugriff am 26.09.2017].

[2] Industrial Data Space e. V., [Online]. Available: http://www.industrialdataspace.org.

[3] S. Ahmadian, F. Coerschulte und J. Jürjens, „Supporting the Security Certification of Cloud-Computing-Infrastructures,“ in *International Symposium on Buisness Modeling and Software Design*, 2015.

[4] J. Jürjens, „Geschäftsprozesse in der Cloud - aber sicher ! (… und compliant),“ in *Software Engineering + Architectures*, 2014.

[5] S. Wenzel, C. Wessel, T. Humberg und J. Jürjens, „Securing Processes for Outsourcing into the Cloud,“ in *International Conference on Cloud Computing and Services Science*, 2012.

[6] B. Otto, J. Jürjens, J. Schon, S. Auer, N. Menz, S. Wenzel und J. Circllies, „Industrial Data Space -- Digitale Souveränität über Daten,“ Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e.V., München, 2016.

[7] J. Jürjens, „Model-based Security Testing using UMLsec,“ *Electronic Notes in Theoretical Computer Science*, Bd. 1, Nr. 220, pp. 93-104, 2008.

[8] J. Jürjens, Secure Systems Development with UML, Heidelberg: Springer, 2005.

[9] J. Jürjens, „Sound Methods and Effective Tools for Model-based Security Engineering with UML,“ in *International Conference on Software Engineering*, 2005.

[10] J. Jürjens, „Automated Security Hardening for Evolving UML Models,“ in *International Conference on Software Engineering*, 2011.

[11] A. Bauer, J. Jürjens und Y. Yijun, „Run-Time Security Traceability for Evolving Systems,“ *The Computer Journal*, Bd. 54, Nr. 1, pp. 58--87, 2011.

[12] T. Humberg, C. Wessel, D. Poggenpohl, S. Wenzel, T. Ruroth und J. Jürjens, „Using Ontologies to Analyze Compliance Requirements of Cloud-Based Processes,“ in *Cloud Computing and Services Science (selected best papers)*, 2014.

Autoren

Sven Peldszus

Sven Peldszus ist wissenschaftlicher Mitarbeiter in der Arbeitsgruppe Software-Engineering von Prof. Dr. Jan Jürjens an der Universität Koblenz-Landau. Sein Fokus liegt auf der statischen Softwareanalyse.

speldszus@uni-koblenz.de

Dr.-Ing. Jan Cirullies

Jan Cirullies ist Leiter der Abteilung Digitization in Logistics am Fraunhofer-Institut für Software- und Systemtechnik ISST in Dortmund. Seit 2015 unterstützt er die Initiative Industrial Data Space durch Projektmanagement, Architekturentwicklung und mit Use Cases.

jan.cirullies@isst.fraunhofer.de

Prof. Dr. Jan Jürjens

Jan Jürjens ist Professor für Software-Engineering an der Universität Koblenz-Landau sowie Director Research Projects am Fraunhofer ISST in Dortmund. Er ist Autor des Buches "Secure Systems Development with UML" (Springer-Verlag 2005, chinesische Übersetzung 2009).

http://jan.jurjens.de