Arndt Bode
Manfred Broy
Hans-Joachim Bungartz
Florian Matthes

Hrsg.

50 Jahre Universitäts-Informatik in München

Springer Vieweg

50 Jahre Universitäts-Informatik in München

Arndt Bode · Manfred Broy ·
Hans-Joachim Bungartz · Florian Matthes
(Hrsg.)

50 Jahre Universitäts-Informatik in München

Springer Vieweg

Herausgeber

Arndt Bode
Inst. f. Informatik, LS Rechnertechnik
Technische Universität München
Garching, Deutschland

Hans-Joachim Bungartz
Inst. f. Informatik
Technische Universität München
Garching, Deutschland

Manfred Broy
Zentrum Digitalisierung Bayern
Garching, Deutschland

Florian Matthes
Inst. f. Informatik
Technische Universität München
Garching, Deutschland

ISBN 978-3-662-54711-3 ISBN 978-3-662-54712-0 (eBook)
DOI 10.1007/978-3-662-54712-0

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Springer Vieweg

Gedruckt auf säurefreiem und chlorfrei gebleichtem Papier

Springer Vieweg ist Teil von Springer Nature
Die eingetragene Gesellschaft ist Springer-Verlag GmbH Deutschland
Die Anschrift der Gesellschaft ist: Heidelberger Platz 3, 14197 Berlin, Germany

50 Jahre Informatik an den Universitäten in München

Mit der Feier zu „50 Jahre Universitäts-Informatik in München“ wird des Ereignisses gedacht, dass im Jahre 1967 F.L. Bauer an der Technischen Universität München erstmalig eine Lehrveranstaltung durchführte, die den Begriff „Informatik“ verwendete.

Das Entstehen der Informatik in München war stark geprägt durch die Rechenanlage PERM. Neben den riesigen Herausforderungen bei ihrer Konstruktion wurde den Beteiligten schnell deutlich, dass die Programmierung ganz besondere Fragestellungen mit sich brachte. F.L. Bauer und K. Samuelson waren dadurch frühzeitig auf dieses Thema aufmerksam geworden. Im Zentrum stand zunächst die Suche nach einer algorithmischen Sprache, insbesondere für numerische Anwendungen. ALGOL war die Antwort aus München und wurde 1960 die erste durch ein internationales Komitee festgelegte Programmiersprache. Schnell zeigte sich, dass nicht nur die Sprache von Bedeutung ist, sondern dass auch die methodische Beherrschung der Programmierung eine große Herausforderung darstellt. Mit der „NATO Software Engineering Conference“ 1968 in Garmisch, organisiert von F.L. Bauer, wurde der Begriff des Software Engineerings eingeführt und nachhaltig geprägt. Zur gleichen Zeit waren erste Vorlesungen zum Thema Informatik entstanden.

Schnell wuchs das Fach heran. Die hohe Bedeutung des Themas „Informatik“ für die Wirtschaft ging Hand in Hand mit dem Auf- und Ausbau des Faches. So entstand ein Institut für Informatik an der Technischen Universität München. Schritt für Schritt wurden weitere Lehrstühle eingerichtet. Die Fakultät für Mathematik wurde umbenannt in eine Fakultät für Mathematik und Informatik. Anfang der 90er-Jahre zeigte sich, dass das Fach Informatik so viel Eigenständigkeit entwickelt hatte, dass es eine eigene Fakultät rechtfertigte.

Schon in den 80er-Jahren hatte die Universität der Bundeswehr das Fach Informatik mit starker Unterstützung der Technischen Universität München eingerichtet. An der Ludwig-Maximilians-Universität entstand das Fach der Informatik Anfang der 90er-Jahre, nachdem bereits 1974 das Institut für Informatik gegründet worden war. An der Technischen Universität München zeigte sich Ende der 90er-Jahre, dass eine Erweiterung des Faches von der Kerninformatik auf relevante, aufstrebende Anwendungsfächer notwendig war. So entstanden die Wirtschaftsinformatik und zusätzliche Lehrstühle in einzelnen Anwendungsgebieten. Die ersten zwei Jahrzehnte des 21sten Jahrhunderts waren dann geprägt durch die schnelle Ausweitung des Faches auf die unterschiedlichsten Anwendungsgebiete in praktisch allen Wissensbereichen und insbesondere durch die Nutzung

von Informatik, nicht zuletzt durch eingebettete Systeme, Smartphones, World Wide Web, im täglichen Leben nahezu aller Menschen.

Parallel zum schnellen Ausbau des Faches an den Universitäten entstanden in München eine Fülle von Instituten zu Fragen der Informatik in der Fraunhofer Gesellschaft, aber auch unabhängigen Forschungsinstituten wie fortiss. Bereits 1962 entstand mit dem Leibniz-Rechenzentrum der Bayerischen Akademie der Wissenschaften ein hoch effizienter IT-Dienstleister für die Münchner Universitäten, der heute auch Querschnittsaufgaben, wie den Betrieb eines Supercomputers der weltweit höchsten Leistungsklasse, sicherstellt. Heute ist die Münchner Informatik die wohl stärkste Informatik in Deutschland, nicht zuletzt auch geprägt durch den Umstand, dass München einer der führenden Digital Hubs in Europa ist.

Der Sammelband „50 Jahre Informatik“, kann nicht die Entwicklung der Informatik in München umfassend nachzeichnen, sondern soll durch exemplarisch ausgewählte Beiträge aus den drei universitären Münchner Informatiken die Vielfalt der Arbeitsgebiete der modernen Informatik darstellen. Damit sind bei weitem nicht alle Teilgebiete abgedeckt, auf denen in den Informatiken der Münchner Universitäten geforscht und gelehrt wird. Auch wurde bewusst darauf verzichtet, Beiträge von Informatikerinnen und Informatikern aufzunehmen, deren Arbeitsgebiete zur Angewandten Informatik in anderen Fächern zählen. Bewusst wurde auf Beiträge aus den Hochschulen für Angewandte Wissenschaften sowie auf die gesamte außeruniversitäre Forschung und Lehre in der Wirtschaft, den Kommunen und der Verwaltung verzichtet. Einschlägige Übersichten nennen eine drei- bis vierstellige Zahl von informatiknahen Unternehmen allein im Großraum München. Allein daran ist zu sehen, welche Bedeutung für Wertschöpfung und Arbeitsplätze aus den ersten Anfängen der Informatik vor 50 Jahren entstanden ist, ganz zu schweigen von der Wucht, mit der die Informatik heute unser Leben prägt.

Die Herausgeber danken an dieser Stelle den Autorinnen und Autoren, den Gutachterinnen und Gutachtern und insbesondere dem Redaktionsteam, allen voran Frau Ursula Eschbach, die die Zusammenstellung massiv unterstützt haben.

Allen Lesern wünschen wir informative Lektüre und der Informatik – nicht nur in München – die Fortsetzung ihrer Erfolgsgeschichte entlang der Entwicklungslinien, die die Beiträge dieses Bandes aufzeichnen.

Arndt Bode, Manfred Broy, Hans-Joachim Bungartz, Forian Matthes

Inhaltsverzeichnis

Über die Herausgeber

Professor Dr. Dr. h.c. Arndt Bode war von 1987 bis 2017 Inhaber des Lehrstuhls für Rechnertechnik und Rechnerarchitektur der Fakultät für Informatik an der Technischen Universität München. Von 1999 bis 2008 war er Vizepräsident und CIO der TU München, von 2008 bis 2017 war er Vorsitzender des Direktoriums des Leibniz-Rechenzentrums der Bayerischen Akademie der Wissenschaften. Nach Studium und Promotion in Karlsruhe war er wissenschaftlicher Mitarbeiter an den Universitäten Gießen und Erlangen-Nürnberg. Sein wissenschaftlicher Schwerpunkt liegt im Bereich der Rechnerarchitektur, speziell von Höchstleistungsrechnern und zugehörigen Programmiermodellen und -werkzeugen sowie im Bereich des energieeffizienten Betriebs großer Rechenzentren.

Professor Dr. Dr. h.c. Manfred Broy leitete von 1989 bis 2015 als ordentlicher Professor für Informatik am Institut für Informatik der Technischen Universität München den Lehrstuhl Software & Systems Engineering. Seine Forschung zielt auf die Beherrschung der Evolution leistungsstarker Software-Systeme durch den Einsatz wohldurchdachter Prozesse, langlebiger flexibler Softwarearchitekturen und moderner Werkzeuge auf Basis mathematisch und logisch fundierter Methoden. Er gründete das Forschungsinstitut für angewandte Forschungstechnik fortiss. Seit Januar 2016 ist der Gründungspräsident des Zentrums Digitalisierung.Bayern. Durch die unter der Leitung von Professor Broy erarbeitete acatech-Studie agenda cyber-physical systems wurden maßgebliche Initiativen auf nationaler Ebene wie Industrie 4.0 angestoßen.

Professor Dr. Hans-Joachim Bungartz ist seit 2005 Ordinarius für Informatik (Wissenschaftliches Rechnen) und seit 2013 Dekan der Fakultät für Informatik sowie Graduate Dean an der TU München. Er ist Mitglied des Direktoriums des Leibniz-Rechenzentrums und seit 2011 Vorsitzender des Vorstands des Deutschen Forschungsnetzes (DFN-Verein). Frühere Stationen – nach Studium (Mathematik und Informatik), Promotion und Habilitation an der TUM – waren die Universitäten Augsburg und Stuttgart. Seine Arbeitsgebiete liegen im Scientific Computing, High-Performance Computing sowie Computational Science and Engineering.

Professor Dr. Florian Matthes leitet den Lehrstuhl für Software Engineering betrieblicher Informationssysteme am Institut für Informatik der Technischen Universität München. Seine aktuellen Forschungsschwerpunkte sind das Enterprise Architecture Management, Software-Plattformen und -Ökosysteme sowie Soziale Software. Als Leiter der Fachgruppe für Softwarearchitektur der Gesellschaft für Informatik, Beiratsmitglied der Ernst Denert-Stiftung für Software Engineering und Organisator zahlreicher Fachveranstaltungen im Bereich Unternehmensarchitektur legt er besonderen Wert auf die interdisziplinäre Zusammenarbeit zwischen Praktikern und Wissenschaftlern (Informatik, Wirtschaft, Design, Rechtswissenschaften). Er ist Mitgründer und Aufsichtsratsvorsitzender der CoreMedia AG und infoAsset AG und Gründungsbotschafter der TU München.

Cybersicherheit Beyond 2020!

1

Herausforderungen für die IT-Sicherheitsforschung

Claudia Eckert

Zusammenfassung

Mit der Zusammenführung von physischen Systemen mit virtuellen Objekten zu Cyber-Physischen Systemen (CPS) schwinden die Grenzen zwischen digitaler und physikalischer Welt und damit auch ein bisher verlässlicher Schutzwall. Dies erhöht die potentiellen Auswirkungen von erfolgreichen Angriffen und macht ein prinzipielles Umdenken beim Umgang mit diesen Gefahren notwendig. Die Gewährleistung der Integrität, Vertraulichkeit und Verfügbarkeit sind die bekannten Schutzziele, die bereits bei der klassischen IT-Sicherheit verfolgt werden. Durch die Verbindung zwischen digitaler und physischer Welt wird jedoch die Erfüllung der Ziele zunehmend schwieriger und komplexer; die IT-Sicherheitsforschung steht vor neuen Herausforderungen. Der Beitrag diskutiert wichtige derartige Herausforderungen, wie die Erforschung proaktiver Schutzverfahren, die Entwicklung resilienter System-Architekturen oder aber auch die Erforschung neuer Ansätze für eine kontrollierbare Weitergabe und Nutzung von Informationen in vernetzten Umgebungen.

1.1 Einführung

Informations- und Kommunikationstechnologie (IKT) durchdringt alle unsere Lebens- und Arbeitsbereiche. Dies manifestiert sich in der so genannten digitalen Transformation dieser Bereiche. In der digitalen Produktion ist dieser digitale Wandel durch das Schlagwort Industrie 4.0 charakterisiert. Er betrifft sowohl die Produktionsabläufe als auch die entstehenden smarten Produkte, wie Maschinen, Werkstücke oder die Endpro-

C. Eckert (✉)
Fakultät für Informatik, Lehrstuhl für Sicherheit in der Informatik, I20, TU München,
Fraunhofer-Institut AISEC München
München, Deutschland

A. Bode et al. (Hrsg.), *50 Jahre Universitäts-Informatik in München*,
DOI 10.1007/978-3-662-54712-0_1

dukte, die durch die integrierten IKT Technologien neue Fähigkeiten erlangen. Durch die digitale Transformation und die zunehmende Vernetzung verschwinden die Grenzen zwischen den vormals getrennten Informations- und Kommunikationstechnik-Bereichen. IT-Systeme mit ganz unterschiedlichen Sicherheitsanforderungen werden miteinander verbunden. Dadurch eröffnen sich neue Verwundbarkeiten und Möglichkeiten für gezielte Angriffe, um Daten zu manipulieren, Know-how abfließen zu lassen oder aber auch die Verfügbarkeit von Anlagen und Systemen zu stören. Über smarte Sensorik und Aktorik werden kontinuierlich Daten erhoben, vorverarbeitet und für die Bereitstellung von Mehrwertdiensten, wie vorausschauende Wartung, auf Cloud-basierten Plattformen verfügbar gemacht. Die entsprechenden Daten beinhalten häufig unternehmensrelevantes Know-how, wie beispielsweise Details aus Produktionsabläufen, die nur kontrolliert weitergegeben und auch nur kontrollierbar genutzt werden dürfen.

Konsequenzen für die IT-Sicherheit

Das Beispiel der digitalen Transformation in der Industrie 4.0 verdeutlicht charakteristische Phänomene, die sich aus der Zusammenführung von physischen Systemen mit virtuellen Objekten zu Cyber-Physischen Systemen (CPS) ergeben. Analoge Herausforderungen ergeben sich beispielsweise auch bei der vernetzten Mobilität, Stichwort automatisiertes Fahren, der vernetzten Gesundheitsversorgung oder aber auch der Vernetzung von Heimumgebungen und ganz allgemein im Internet of Things (IoT). In allen diesen Zukunftsszenarien schwinden die Grenzen zwischen digitaler und physikalischer Welt und damit auch ein bisher verlässlicher Schutzwall. Dies erhöht nicht nur die potentiellen Auswirkungen von erfolgreichen Angriffen, sondern macht auch ein prinzipielles Umdenken beim Umgang mit diesen Gefahren notwendig, da sich auch die Angriffslandschaft in den letzten Jahren dramatisch verändert hat. Cyberkriminalität und Cyber-Spionage haben sich professionalisiert. Angriffe richten sich zunehmend gezielt auf bestimmte Organisationen oder einzelne Personen und entziehen sich den üblichen Schutzmechanismen wie Firewalls, Anti-Viren-Programmen und Intrusion Detection Systemen. Die finanziellen Möglichkeiten der Angreifer wachsen mit dem Anstieg des Schadenspotenzials. Die Frühwarn- und Verteidigungsstrategien von Unternehmen, Verwaltung und privaten Nutzern sind dieser Situation nicht gewachsen. Die IT-Sicherheitsforschung steht vor erheblichen Herausforderungen, die nicht nur technologische Innovationen erfordern, sondern auch ein Umdenken bei der sicheren Entwicklung und dem Betrieb von sicheren Cyber-Physischen-Systemen. Eine ausführliche Darstellung der Sicherheitsherausforderungen im Bereich Industrie 4.0 sowie konkrete Lösungsansätze hierzu findet man u. a. in [1, 2].

Mit dem Begriff der Cyber-Sicherheit wird der Konvergenz von realer mit virtueller, IT-getriebener Welt und der damit einhergehenden Herausforderungen an die IT-Sicherheit, Rechnung getragen. Cyber-Sicherheit kann damit als konsequente Weiterentwicklung der IT-Sicherheit (vgl. [3]) verstanden werden. Der Forschungs- und Entwicklungs-

bedarf im Bereich der Cybersicherheit wurde bereits in verschiedenen Positionspapieren aus unterschiedlichen Blickwinkeln sowohl für die nationale Forschung (vgl. [4]), als auch die europäische Forschung (vgl. [5]) sowie auch die internationale Forschung und Standardisierung (vgl. [6]) erarbeitet. Nachfolgend werden ausgewählte Herausforderungen diskutiert und es wird auf ausgewählte aktuelle Forschungsarbeiten in diesen Bereichen, die am Lehrstuhl I20 der TU München sowie am assoziierten Fraunhofer-Institut AISEC durchgeführt werden, verwiesen.

1.2 Cybersicherheit Beyond 2020

Cybersicherheit umfasst Maßnahmen, um Systeme und einzelne Komponenten vor Manipulationen zu schützen, man spricht hier vom Schutzziel der Integrität, um die Vertraulichkeit sensibler Informationen zu gewährleisten, aber auch um die Verfügbarkeit von Funktionen und Diensten zu gewährleisten. Die Gewährleistung der Integrität, Vertraulichkeit und Verfügbarkeit sind die bekannten Schutzziele, die bereits bei der klassischen IT-Sicherheit verfolgt werden. Durch die Verbindung zwischen digitaler und physischer Welt wird jedoch die Erfüllung der Ziele zunehmend schwieriger und komplexer.

Kognitive Sicherheit

Um die Schutzziele zu erfüllen, werden neue Analyse- und Erkennungsverfahren benötigt, um Schwachstellen und konkrete Angriffe oder Angriffsversuche auf vernetzte Systeme frühzeitig und mit möglichst hoher Präzision zu erkennen, damit ein möglicher Schaden begrenzt werden kann. Gefordert ist der nächste große Schritt im Bereich der IT-Sicherheitsforschung, der sich gerade unter dem Begriff **kognitive Sicherheit** etabliert. Während herkömmliche Sicherheitsdienste im Wesentlichen reaktiv entsprechend vordefinierter Parameter und Konfigurationen Analysen durchführen und Entscheidungen treffen (z. B. Zugriff ist berechtigt, Benutzer ist authentisch), agieren kognitive Sicherheitsdienste proaktiv. Basierend auf maschinellen Lernverfahren und Methoden der künstlichen Intelligenz sind sie in der Lage, Daten zu interpretieren, proaktiv Abweichungen von Normalverhalten zu detektieren, autonom nach Sicherheitslücken zu suchen und automatisiert und effizient riesige, strukturierte und unstrukturierte Datensätze aus verschiedensten Quellen zu analysieren und daraus automatisiert evidenzbasierte Rückschlüsse und Handlungsempfehlungen zu generieren. Kognitive Sicherheitstechnologie orientiert sich an bewährten menschlichen Denkstrukturen: (1) verstehen (u. a. Analyse großer Datenvolumina von Schadcode, um Gemeinsamkeiten zu identifizieren und Verhaltensweisen von bösartigen Software-Artefakten zu verstehen), (2) Schlüsse ziehen (u. a. Interpretation von Informationen) und (3) kontinuierliches Lernen (u. a. Sammeln von Daten über Sicherheitsbedrohungen und -Vorfälle und Ableiten von Erkenntnissen). Mittels solcher proaktiver Maßnahmen zur Überwachung und Kontrolle sind Manipulationsversuche und

unerwünschte Informationsabflüsse wirksam zu verhindern oder zumindest so substantiell zu erschweren, dass für Angreifer das Kosten-Nutzenverhältnis unattraktiv wird. Am Lehrstuhl I20 der TUM und am Fraunhofer AISEC werden in Forschungsprojekten erste entsprechende Lösungen für kognitive Sicherheitssysteme erarbeitet (u. a. [7, 8]).

Digitale Identitäten für Objekte und Transaktionen

In vernetzten Cyber-Physischen Systemen werden Daten unternehmensübergreifend von Maschine zu Maschine ausgetauscht, wobei zukünftig Maschinen oder Objekte direkt mit z. B. einem Lieferanten kommunizieren werden. Ein sicherer Informationsaustausch entlang des gesamten Wertschöpfungsprozesses erfordert Konzepte um Menschen, Maschinen und Prozesse eindeutig auch über Unternehmensgrenzen hinweg zu identifizieren. Kommunikationsbeziehungen müssen agil etabliert werden können, d. h. Kommunikationspartner müssen in der Lage sein, auch ad-hoc einen vertrauenswürdigen Kommunikationskanal aufzubauen. Benötigt werden neue Ansätze zur skalierenden, **fälschungssicheren Identifizierung** von Systemkomponenten, wie dies beispielsweise mit Smarten Materialien, wie Physical Unclonable Functions (PUF), in Ansätzen bereits heute möglich ist (vgl. u. a. [9]). Neue Protokolle sind zu erforschen und in die System-Architekturen zu integrieren, um die Potentiale Smarter Materialien für zukünftige vernetzte IoT-Systeme nutzbar zu machen. Mit der PEP-Schutzfolie (vgl. u. a [10]). wird eine smarte, PUF-basierte Schutzfolie entwickelt, die es ermöglicht, Objekte mit einer eindeutigen Identität zu versorgen und zudem einen Manipulationsschutz für die Objekte realisiert.

Ein zunehmend wichtiges Thema bei der Vernetzung und Kooperation von Cyber-Physischen Systemen wird die Abbildung von rechtlich relevanten Transaktionen durch direkte Maschine-zu-Maschine Interaktionen sein, wie sich dies beispielswiese in Bestellprozessen oder auch in der Logistik bereits anbahnt. Hierbei sind Fragen der Nichtabstreitbarkeit, also Zuordenbarkeit von Aktionen ebenso zu klären, wie die Frage der Rechtzeitigkeit, Vollständigkeit und Korrektheit von Aktionen oder aber auch Haftungsfragen. Das automatisierte Aushandeln von so genannten smarten, rechtssicheren Verträgen (**smart contracts**) zwischen Maschinen wird derzeit sehr intensiv erforscht. Mit der Blockchain-Technologie stehen interessante Konzepte zur Verfügung, um Transaktionen zu identifizieren und ohne zentrale Vertrauensstrukturen zu verwalten, jedoch ist es derzeit noch nicht umfassend geklärt, welche verlässlichen und nachvollziehbaren Sicherheitsgarantien eine Blockchain-basierte Anwendung tatsächlich geben kann und wie das Risiko ihres Einsatzes zu beurteilen ist. In dem Blockchain-Labor am Fraunhofer AISEC wird deshalb eine Experimentier- und Evaluationsumgebung aufgebaut, in der verschiedene Blockchain-Technologien in unterschiedlichen Szenarien aufgesetzt und hinsichtlich ihrer Sicherheit und Robustheit untersucht werden können.

Angriffs-Resilienz-by-Design

Da aufgrund der Komplexität der vernetzten Systeme, der Vielfalt der vernetzten Hard- und Software-Komponenten, aber auch der hohen Dynamik der Prozesse erfolgreiche Angriffe nicht ausgeschlossen werden können, ist es erforderlich, die Systeme durch technische Maßnahmen und organisatorische Prozesse proaktiv auf die Behandlung von Schadenssituationen vorzubereiten. Es sind neue System-Architekturen, sowie Methoden und Werkzeuge erforderlich, um vernetzte Systeme so zu entwickeln, dass sie qua Design ein hohes Maß an Sicherheit bieten. Man spricht in diesem Zusammenhang auch oft von Security by Design, wobei hierbei vordringlich Maßnahmen zum Manipulations- und Vertraulichkeitsschutz betrachtet werden. Zukünftige vernetzte Systeme erfordern darüber hinausgehende Ansätze, die das neue Paradigma der **Angriffs-Resilienz-by-Design** unterstützen. Erforderlich sind Angriffs-resiliente Techniken zur kontinuierlichen, lernenden Selbstüberwachung und auch zur Threat Analytics, um mit neuen Techniken der Datenfusion, Angriffsmuster frühzeitig zu erkennen. Die Absicherung physikalischer Kommunikations-Verbindungen (physical layer) mit möglichst geringer Latenz erfordert neue Sicherheitskonzepte, durch die beispielsweise kryptographische Schlüssel aus den individuellen, charakteristischen Eigenschaften des physikalischen Kanals abgeleitet werden. Mit solchen Ansätzen könnten, vergleichbar mit Quanten-Kryptographie-Lösungen, Angriffs-resiliente Übertragungssysteme entwickelt werden. Es werden vertrauenswürdige Hard- und Software-Architekturen benötigt, um geschützte Ausführungsumgebungen für die Verarbeitung sensitiver Daten zu ermöglichen. Durch fortgeschrittene Isolations- und Virtualisierungstechniken sowie Maßnahmen zur kontinuierlichen Integritätsmessung kombiniert mit fortgeschrittenen Techniken der Virtual Machine Introspection (VMI) (vgl. u. a [11, 12]), kann ein vernetztes Cyber-Physisches System resilient betrieben werden. Das System kann damit kontinuierlich und autonom seinen Systemzustand gegen einzuhaltende Regelwerke und Anforderungen abgleichen. Es ist zudem sicherzustellen, dass keine manipulierten Code-Teile geladen und zur Ausführung gebracht werden. Kritische Systembereiche sollten von unkritischen Teilen isoliert werden, um mögliche Schadensrisiken zu begrenzen. Neue Software-Architekturen und Konzepte hierzu werden derzeit erforscht und erprobt (vgl. u. a. [13, 14]).

Software-Sicherheit

Vernetzte Cyber-Physische Systeme sind Software-intensive Systeme, in denen Altsysteme mit Neuentwicklungen integriert betrieben werden müssen. Es werden Methoden und Werkzeuge benötigt, um Software möglichst automatisiert vor deren Inbetriebnahme hinsichtlich möglicher Schwachstellen zu analysieren und diese soweit möglich, automatisiert und semantikerhaltend zu beheben. Es müssen Kapselungstechniken, wie isolierte Container und Sandboxes, weiterentwickelt werden, so dass auch unsichere Komponenten von Dritten bzw. Legacy-Systeme, die nicht gehärtet werden können, sicher integriert wer-

den können, so dass ein Zusammenspiel zwischen sicheren und unsicheren Komponenten unter nachweislicher Einhaltung von geforderten Sicherheitsniveaus möglich ist. Erforderlich sind fortgeschrittene Test-Umgebungen, um mit Werkzeugen die Sicherheit von Software automatisiert prüfen zu können. In aktuellen Projekten werden bereits Methoden und Werkzeugumgebungen entwickelt (vgl. [15, 16]), die eine automatische Analyse von C-Code hinsichtlich Sicherheitsschwachstellen ermöglichen, oder auch die automatisierte Analyse von Apps (u. a. [17]). Darüber hinaus sind Methoden und Werkzeuge zu etablieren, um Software in einem durchgehenden Software-Lebenszyklus-Prozess sicher zu entwickeln, sicher auszurollen, sicher zu warten und aktuell zu halten. Fragen des sicheren Software-Updates nehmen hierbei eine besondere Rolle ein. Am Fraunhofer AISEC werden Methoden, Werkzeuge und Vorgehensweisen zur Entwicklung und Analyse von sicheren Softwarekomponenten erforscht, die den gesamten Lebenszyklus von Softwarelösungen abdecken. Ein Fokus der aktuellen Arbeiten liegt auf der Entwicklung konstruktiver Maßnahmen, um Sicherheit bereits im Entwurf zu planen und angemessen bei Integration und Konfiguration zu berücksichtigen (vgl. u. a. [18, 19]).

Information Rights Management

Mit der zunehmenden Vernetzung und Digitalisierung entstehen große Datenmengen. Diese Daten werden zu einem wichtigen Bestandteil sowohl der Wertschöpfung durch die Entwicklung datenbasierter Mehrwertdienste, als auch zur Qualitätsverbesserung durch datenbasierte Steuerungen und Planungen. Daten und die datenzentrischen Anwendungen werden damit zu einem werthaltigen und schützenswerten Gut. Dies erfordert Konzepte für ein **Information-Rights-Management**, das sicherstellt, dass der Daten-Eigentümer nachvollziehbar bestimmen kann, wer seine Daten besitzen und weiterverarbeiten darf. Abschließend gehen wir etwas ausführlicher auf das aktuelle Forschungsprojekt des Industrial Data Space (IDS) der Fraunhofer-Gesellschaft ein, dessen Ziel es ist, hierfür Referenzarchitekturen und -Implementierungen zu erforschen und zusammen mit industriellen Partnern zu erproben (vgl. [13, 20]). Der IDS hat das Ziel, eine Referenzarchitektur für einen sicheren Datenraum zu schaffen, der Unternehmen verschiedener Branchen die souveräne Bewirtschaftung ihrer Datengüter ermöglicht. Der Datenraum basiert auf einem dezentralen Architektur-Ansatz (vgl. Abb. 1.1), bei dem die Dateneigner ihre Datenhoheit und Datensouveränität nicht aufgeben müssen. Der Industrial Data Space ist im Kern eine serviceorientierte Architektur. Eine zentrale Komponente der Architektur ist der Industrial Data Space Konnektor (siehe Abb. 1.1), der den kontrollierten Austausch von Daten zwischen den Teilnehmern am Industrial Data Space ermöglicht.

Die Architektur aus Abb. 1.1 enthält zudem einen Broker, der die Veröffentlichung von Diensten ermöglicht. Im ebenfalls aufgeführten AppStore werden Vokabulare, Systemadapter und Daten- und Service-Apps vorgehalten. Diese Komponenten können auf einen IDS-Konnektor geladen und dort ausgeführt werden. Systemadapter dienen dabei der Anbindung von Systemen, die nicht Bestandteil des Data Space sind. Daten- und

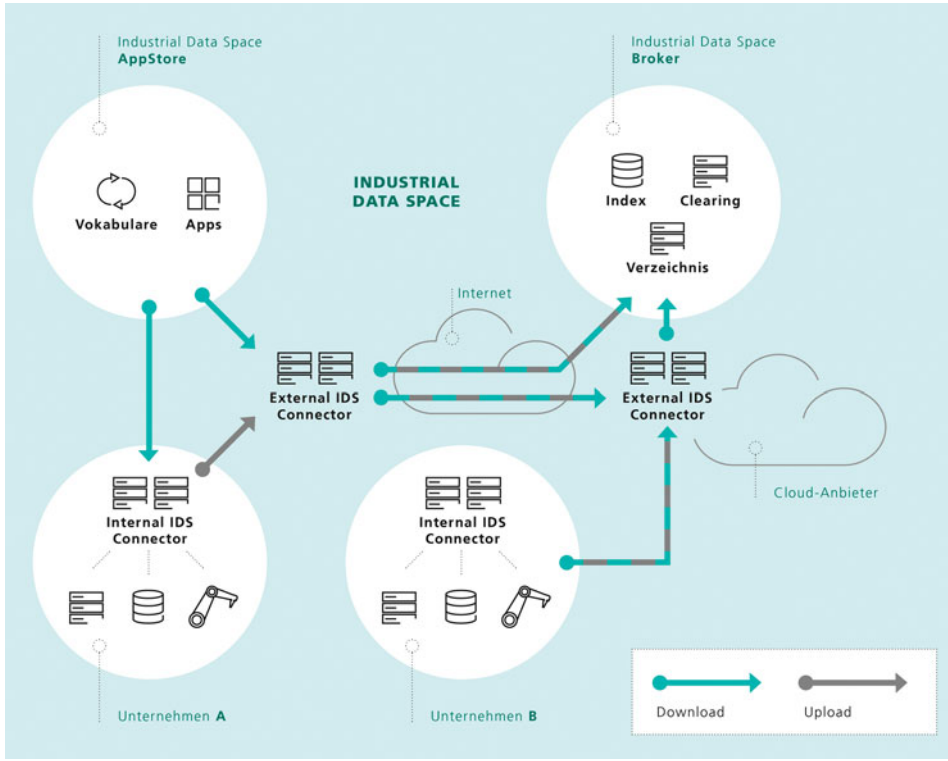

Abb. 1.1 Software-Architektur des Industrial Data Space

Service-Apps können einfach sein und lediglich der Filterung oder Anonymisierung von Daten dienen. Sie können aber auch Daten aus mehreren Quellen verdichten und komplexe Operationen ausführen. Einzelne Datendienste können miteinander verknüpft werden und ermöglichen so die Kombination zu komplexen Diensten mit hohem Mehrwert.

Die Sicherheits-Architektur des Industrial Data Space gewährleistet eine sichere Kommunikation zwischen seinen Teilnehmern. Auch der Nutzung von Daten können Beschränkungen auferlegt werden. So ist es z. B. möglich, die Nutzungsdauer festzulegen, die Weitergabe von Daten per Richtlinie zu unterbinden oder nur bestimmte Abfragen und Aggregationslevel zuzulassen, während die Roh- und die nicht benötigten Daten unzugänglich bleiben. Der Industrial Data Space wird verschiedene Sicherheitsstufen unterstützen. Die niedrigste Stufe erlaubt es, Industrial Data Space Konnektoren auf unsicheren Plattformen auszuführen. Ein höheres Sicherheitsniveau wird durch die Bereitstellung einer sicheren Ausführungsumgebung basierend auf einem Container-Konzept gewährleistet. Dadurch können Dienste in einzelnen Containern abgeschottet werden, die über einen privilegierten, eigens gehärteten Core-Container gesteuert werden. Dieser hat auch die Möglichkeit, Kommunikationsvorgänge freizugeben oder zu unterbinden.

So haben Dienste unterschiedlicher Anbieter keine Möglichkeit, sich gegenseitig zu beeinflussen. Die Container sind standardmäßig vollständig isoliert und werden bei Bedarf explizit miteinander verkoppelt. Eine Umsetzung der Konnektor-Sicherheitsarchitektur wird derzeit am Fraunhofer AISEC schrittweise erarbeitet. Zur Umsetzung der höchsten Sicherheitsstufe wird eine auf Linux-Containern basierende hoch-sichere Lösung Trust-X entwickelt, die den TPM2.0 als Sicherheitsmodul einbindet.

Abschließend wird der Nutzen der Industrial Data Space Konzepte anhand eines Predictive Maintenance Anwendungsszenarios erläutert. Damit ein Zulieferer einer Maschine einen solchen Wartungsdienst anbieten kann, benötigt er die Produktionsdaten seines Kunden. Eine vollständige Preisgabe aller dieser Daten liegt jedoch nicht in dessen Interesse, da diese Daten Aufschluss über Produktionsdetails wie Arbeitsabläufe, Rezepturen oder Personaleinsatz liefern könnten. Weiterhin würden erhebliche Datenmengen anfallen, wenn alle Sensordaten direkt übermittelt werden müssten. In dem Szenario kann die Vorverarbeitung der Daten im Quellkonnektor erfolgen. Dabei werden sensitive Daten herausgefiltert und die Daten vorverdichtet. Die Analysealgorithmen des Zulieferers können dann im Zielkonnektor ausgeführt werden. Erfordert die Erbringung des Mehrwertdienstes die Bereitstellung unternehmenskritischer Daten aus der Produktion und verfügt der Datenanbieter über einen Konnektor auf höchstem Sicherheitsniveau, so können Garantien über den Schutz der Daten und des Codes gegeben werden, der in einem der Container auf diesem Konnektor ausgeführt wird. Der Zulieferer kann seine Analyse-Algorithmen in einen solchen Container des Quellkonnektors laden und direkt Vorort ausführen. Der Konnektor garantiert zum einen, dass die Analyse-Verfahren nur auf die dafür erforderlichen Daten zugreifen können und garantiert zudem dem Zulieferer, dass der Code seines Analyse-Verfahrens geschützt ist. Dadurch erfolgen alle aufwendigen uns sensitiven Berechnungen nahe an den Quelldaten. Alternativ können sensitive Daten aus der Quelle zum Zulieferer übermittelt werden, wenn der Zielkonnektor auf höchster Sicherheitsstufe umgesetzt ist. Die Daten können zusätzlich mit Nutzungsbedingungen und einer definierten Löschfrist ausgeliefert werden. Diese Anforderungen an die vertrauenswürdige Datenverarbeitung werden durch den Zielkonnektor nachprüfbar erfüllt.

1.3 Fazit

Neue Ansätze und Methoden sind erforderlich, um vernetzte komplexe Cyber-Physische Systeme abzusichern und über deren Lebenszeit sicher in unterschiedlichen Umgebungen zu betreiben. Ergänzend zu den herkömmlichen Ansätzen der reaktiven IT-Sicherheitsforschung sind proaktive Maßnahmen erforderlich, wie sie im neuen Forschungsfeld der kognitiven Sicherheit zu erarbeiten sind. Maschinellen Lernverfahren und Methoden der künstlichen Intelligenz zur Erhöhung der Sicherheit und auch smarte Materialien eröffnen neue Wege und Möglichkeiten im Bereich Cybersicherheit.

Literatur

1. C. Eckert: Cyber-Sicherheit in der Industrie 4.0: in Handbuch Industrie 4.0: Geschäftsmodelle, Prozesse, Technik, Carl-Hanser Verlag, erscheint April 2017, Hrsg Gunther Reinhart
2. C. Eckert, N. Fallenbeck: Industrie 4.0 meets IT-Sicherheit: eine Herausforderung! In Informatik-Spektrum, Springer, March 2015.
3. Claudia Eckert: IT-Sicherheit: Konzepte – Verfahren – Protokolle, 9th Edition, De Gruyter, 2014
4. J. Beyerer, C. Eckert, P. Martini, Michael Waidner: Strategie- und Positionspapier Cyber-Sicherheit 2020, Herausforderungen für die IT-Sicherheitsforschung, Fraunhofer-Gesellschaft 2014, https://www.aisec.fraunhofer.de/content/dam/aisec/Dokumente/Publikationen/Studien_TechReports/Fraunhofer-Strategie-und_Positionspapier_Cyber-Sicherheit2020.pdf
5. M. Backes, P. Buxmann, C. Eckert, T. Holz, J. Müller-Quade, O. Raabe, M. Waidner: Key Challenges in IT Security Research, Discussion Paper for the Dialogue on IT Security 2016, SecUnity, https://it-security-map.eu
6. B. Leukert, T. Kubach, C. Eckert et al.: IoT 2020: Smart and secure IoT platform. http://www.iec.ch/whitepaper/pdf/iecWP-loT2020-LR.pdf
7. H. Xiao and C. Eckert. Indicative Support Vector Clustering with its Application on Anomaly Detection. In IEEE 12th International Conference on Machine Learning and Applications, December 2013.
8. B. Kolosnjaji, A. Zarras, T. Lengyel, G. Webster, C. Eckert: Adaptive Semantics-Aware Malware Classification. In 13th Conference on Detection of Intrusions and Malware & Vulnerability Assessment, July 2016.
9. D. Merli, G. Sigl, C. Eckert: Identities for Embedded Systems Enabled by Physical Unclonable Functions. Number Theory and Cryptography (Lecture Notes in Computer Science), 8260:125–138, 2013.
10. O. Schimmel, M. Hennig: Kopier- und Manipulationsschutz für eingebettete Systeme. In: Datenschutz und Datensicherheit – DuD, Volume 38, Issue 11, pp 742–746, November 2014.
11. T. Lengyel, T. Kittel, C. Eckert: Virtual Machine Introspection with Xen on ARM. In 2nd Workshop on Security in highly connected IT systems (SHCIS), September 2015
12. J. Pfoh: Leveraging Derivative Virtual Machine Introspection Methods for Security Applications. Technische Universität München, 2013. Doctoral Thesis.
13. J. Schütte and G. Brost. „A Data Usage Control System using Dynamic Taint Tracking“. In: Proceedings of the International Conference on Advanced Information Network and Applications (AINA), March 2016.
14. M. Huber, J. Horsch, M. Velten, M. Weiß and S. Wessel. „A Secure Architecture for Operating System-Level Virtualization on Mobile Devices“. In: 11th International Conference on Information Security and Cryptology Inscrypt 2015. 2015.
15. A. Ibing: Dynamic Symbolic Execution with Interpolation Based Path Merging. In Int. Conf. Advances and Trends in Software Engineering, February 2016.
16. P. Muntean, R. Adnan, A. Ibing, C. Eckert: Automated Detection of Information Flow Vulnerabilities in UML State Charts and C Code. In International Conference on Software Quality, Reliability and Security Companion (QRS-C), Vancouver, Canada, August 2015. IEEE Computer Society.
17. D. Titze, P. Stephanow and J. Schütte: App-Ray: User-driven and fully automated Android app security assessment. Fraunhofer AISEC TechReport May 2014.
18. C. Teichmann, S. Renatus and J. Eichler. „Agile Threat Assessment and Mitigation: An Approach for Method Selection and Tailoring“. International Journal of Secure Software Engineering (IJSSE), 7 (1), 2016.

19. D. Angermeier and J. Eichler. „Risk-driven Security Engineering in the Automotive Domain“. Embedded Security in Cars (escar USA), 2016.
20. B. Otto et. al: Industrial Data Space, Whitepaper, https://www.fraunhofer.de/de/forschung/fraunhofer-initiativen/industrial-data-space.htm

Allgegenwärtige Mensch-Computer-Interaktion

2

Beispiele aus der Interaktion in öffentlichen und halb-öffentlichen Raum und von benutzbarer Sicherheit

Michael Koch und Florian Alt

Zusammenfassung

Computer durchdringen unseren Alltag. Dabei sind diese derart in unsere Umgebung eingebettet, dass diese von uns nicht mehr als solche wahrgenommen werden. Hierdurch entsteht die Notwendigkeit zur Schaffung unmittelbar verständlicher Benutzerschnittstellen – sowohl für Individuen als auch für Gruppen von Benutzern. Mit diesem Teilbereich der Informatik beschäftigt sich die Mensch-Computer-Interaktion. Dieser Beitrag bietet zunächst eine kurze Einführung in die Forschungsmethodik der MCI und gibt einen Einblick in die Forschungsaktivitäten zu diesem Thema an den Münchner Universitäten. Im Fokus stehen hierbei Arbeiten zu öffentlichen Bildschirmen, Blickinteraktion im öffentlichen Raum, sowie die Entwicklung sicherer und gleichzeitig benutzbarer Authentifizierungsverfahren.

2.1 Motivation

Die erfolgreiche und wirkungsvolle Nutzung von technikgestützten Kommunikations- und Informationsangeboten wird zunehmend für Menschen aller gesellschaftlicher Schichten und Funktionen relevant. Gleichzeitig werden technische Systeme, ihre Struktur, Funktionalitäten und Interaktionsformen komplexer, obwohl oder gerade weil die Systeme durch Miniaturisierung, Vernetzung und Einbettung immer weniger sichtbar und damit auch immer weniger (be)greifbar werden [1–3]. Die zukünftige Nutzung von Kommunikations-

M. Koch (✉)
Fakultät für Informatik, Universität der Bundeswehr München
München, Deutschland

F. Alt
Fakultät für Mathematik, Informatik und Statistik, Ludwig-Maximilians-Universität München
München, Deutschland

A. Bode et al. (Hrsg.), *50 Jahre Universitäts-Informatik in München*,
DOI 10.1007/978-3-662-54712-0_2