Cybersicherheit beyond 2020!

Herausforderungen für die IT-Sicherheitsforschung

Claudia Eckert

Einführung

Informations- und Kommunikationstechnologie (IKT) durchdringt alle unsere Lebens- und Arbeitsbereiche. Dies manifestiert sich in der sogenannten 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 Endprodukte, 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 Kommunikationstechnikbereichen. 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 cloudbasierten 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 cyberphysischen 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 Grenze zwischen digitaler und physikalischer Welt und damit auch ein bisher verlässlicher Schutzwall. Dies erhöht nicht nur die potenziellen 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 Cyberspionage 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

DOI 10.1007/s00287-017-1025-6

Claudia Eckert
Fakultät für Informatik, Lehrstuhl für Sicherheit in der Informatik, I20, TU München, München
Fraunhofer-Institut AISEC, München
E-Mail: Claudia.Eckert@in.tum.de

Herausforderungen, die nicht nur technologische Innovationen erfordern, sondern auch ein Umdenken bei der sicheren Entwicklung und dem Betrieb von sicheren cyberphysischen Systemen. Eine ausführliche Darstellung der Sicherheitsherausforderungen im Bereich Industrie 4.0 sowie konkrete Lösungsansätze hierzu findet man u. a. in [5, 6].

Mit dem Begriff der Cybersicherheit wird der Konvergenz von realer mit virtueller, IT-getriebener Welt und der damit einhergehenden Herausforderungen an die IT-Sicherheit Rechnung getragen. Cybersicherheit kann damit als konsequente Weiterentwicklung der IT-Sicherheit (vgl. [4]) verstanden werden. Der Forschungs- und Entwicklungsbedarf im Bereich der Cybersicherheit wurde bereits in verschiedenen Positionspapieren aus unterschiedlichen Blickwinkeln sowohl für die nationale Forschung (vgl. [3]) als auch die europäische Forschung (vgl. [2]) sowie auch die internationale Forschung und Standardisierung (vgl. [11]) 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.

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 vordefinierten Parametern 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 Softwareartefakten 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 substanziell zu erschweren, dass für Angreifer das Kosten-Nutzen-Verhältnis unattraktiv wird. Am Lehrstuhl I20 der TUM und am Fraunhofer AISEC werden in Forschungsprojekten erste entsprechende Lösungen für kognitive Sicherheitssysteme erarbeitet (u. a. [9, 20]).

Digitale Identitäten für Objekte und Transaktionen

In vernetzten cyberphysischen 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. [12]). Neue Protokolle sind zu erforschen und in die Systemarchitekturen zu integrieren, um die Potenziale smarter Materialien für zukünftige vernetzte IoT-Systeme nutzbar zu machen. Mit der PEP-Schutzfolie (vgl. u. a. [16]) 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 cyberphysischen 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 sogenannten 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 Softwarekomponenten, 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 Systemarchitekturen 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 angriffsresiliente Techniken zur kontinuierlichen, lernenden Selbstüberwachung und auch zur Threat Analytics, um mit neuen Techniken der Datenfusion, Angriffsmuster frühzeitig zu erkennen. Die Absicherung physikalischer Kommunikationsverbindungen (Physical Layer) mit möglichst geringer Latenz erfordert neue Sicherheitskonzepte, durch die beispielsweise kryptografische Schlüssel aus den individuellen, charakteristischen Eigenschaften des physikalischen Kanals abgeleitet werden. Mit solchen Ansätzen könnten, vergleichbar mit Quantenkryptografielösungen, angriffsresiliente Übertragungssysteme entwickelt werden. Es werden vertrauenswürdige Hard- und Softwarearchitekturen 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. [10, 15]) kann ein vernetztes cyberphysisches 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 Codeteile geladen und zur Ausführung gebracht werden. Kritische Systembereiche sollten von unkritischen Teilen isoliert werden, um mögliche Schadensrisiken zu begrenzen. Neue Softwarearchitekturen und Konzepte hierzu werden derzeit erforscht und erprobt (vgl. u. a. [7, 17]).

Softwaresicherheit

Vernetzte cyberphysische Systeme sind softwareintensive 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, sodass auch unsichere Komponenten von Dritten bzw. Legacy-Systeme, die nicht gehärtet werden können, sicher integriert werden können, sodass ein Zusammenspiel zwischen sicheren und unsicheren Komponenten unter nachweislicher Einhaltung von geforderten Sicherheitsniveaus möglich ist. Erforderlich sind fortgeschrittene Testumgebungen, um mit Werkzeugen die Sicherheit von Software automatisiert prüfen zu können. In aktuellen Projekten werden bereits Methoden und Werkzeugumgebungen entwickelt (vgl. [8, 13]), die eine automatische Analyse von C-Code hinsichtlich Sicherheitsschwachstellen ermöglichen oder auch die automatisierte Analyse von Apps (u. a. [19]). 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 Softwareupdates 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. [1, 18]).

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 Dateneigentümer 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. [14, 17]). 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 Architekturansatz (vgl. Abb. 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 (s. Abb. 1), der den kontrollierten Austausch von Daten zwischen den Teilnehmern am Industrial Data Space ermöglicht.

Die Architektur aus Abb. 1 enthält zudem einen Broker, der die Veröffentlichung von Diensten ermöglicht. Im ebenfalls aufgeführten App-Store 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 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 Sicherheitsarchitektur 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-

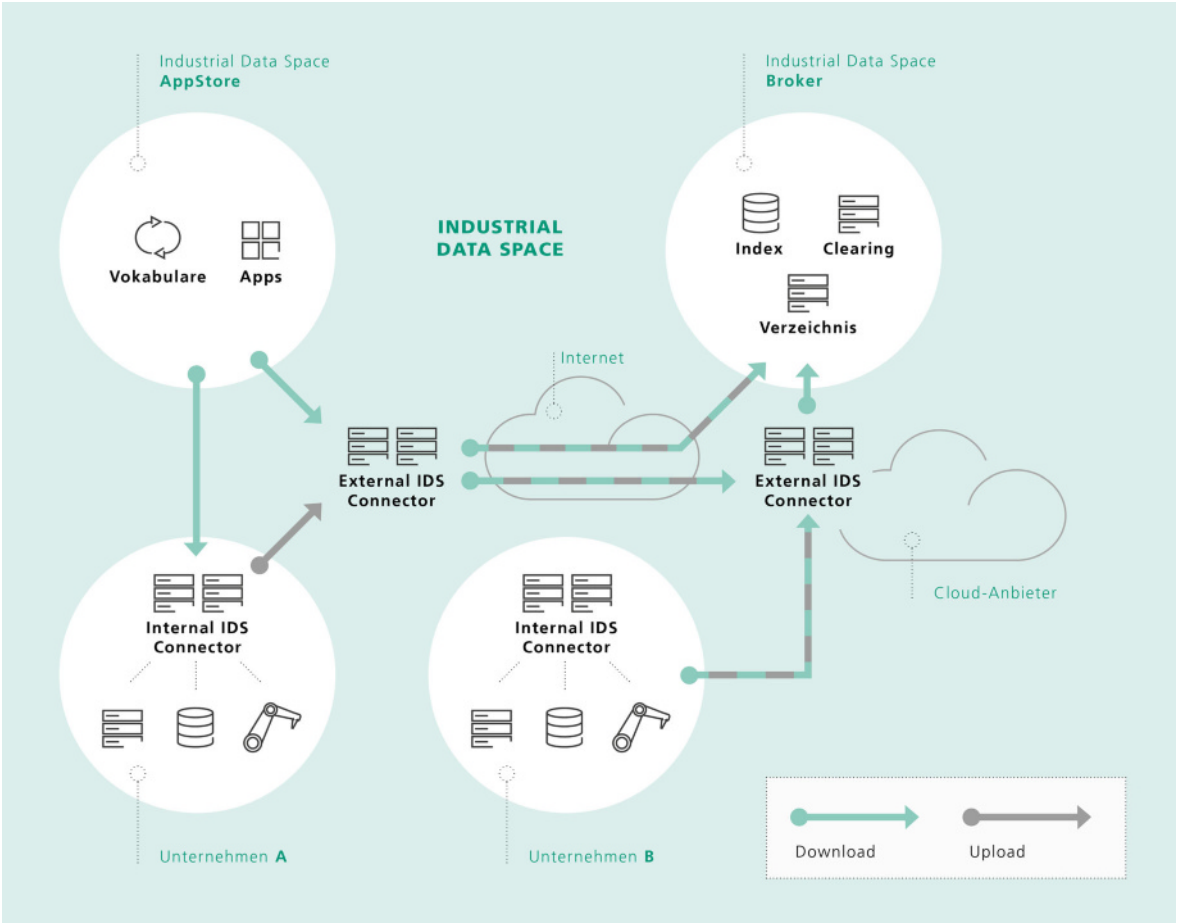

Abb. 1 Softwarearchitektur des Industrial Data Space

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 Containerkonzept 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 Konnektorsicherheitsarchitektur 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 Analysealgorithmen in einen solchen Container des Quellkonnektors laden und direkt vor Ort ausführen. Der Konnektor garantiert zum einen, dass die Analyseverfahren nur auf die dafür erforderlichen Daten zugreifen können, und zum anderen dem Zulieferer, dass der Code seines Analyseverfahrens geschützt ist. Dadurch erfolgen alle aufwendigen und 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.

Fazit

Neue Ansätze und Methoden sind erforderlich, um vernetzte komplexe cyberphysische 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. Angermeier D, Eichler J (2016) Risk-driven security engineering in the automotive domain. Embedded Security in Cars (escar USA)
2. Backes M, Buxmann P, Eckert C, Holz T, Müller-Quade J, Raabe O, Waidner M (2016) Key Challenges in IT Security Research, Discussion Paper for the Dialogue on IT Security 2016. SecUnity. https://it-security-map.eu
3. Beyerer J, Eckert C, Martini P, Waidner M (2014) Strategie- und Positionspapier Cyber-Sicherheit 2020, Herausforderungen für die IT-Sicherheitsforschung. Fraunhofer-Gesellschaft. https://www.aisec.fraunhofer.de/content/dam/aisec/Dokumente/Publikationen/Studien_TechReports/Fraunhofer-Strategie-und_Positionspapier_Cyber-Sicherheit2020.pdf
4. Eckert C (2014) IT-Sicherheit: Konzepte – Verfahren – Protokolle, 9. Aufl. De Gruyter
5. Eckert C (2017) Cyber-Sicherheit in der Industrie 4.0. In: Reinhart G (Hrsg) Handbuch Industrie 4.0: Geschäftsmodelle, Prozesse, Technik. Carl-Hanser Verlag (im Druck)
6. Eckert C, Fallenbeck N (2015) Industrie 4.0 meets IT-Sicherheit: eine Herausforderung! Informatik-Spektrum
7. Huber M, Horsch J, Velten M, Weiß M, Wessel S (2015) A Secure Architecture for Operating System-Level Virtualization on Mobile Devices. In: 11th International Conference on Information Security and Cryptology Inscrypt 2015.
8. Ibing A (2016) Dynamic Symbolic Execution with Interpolation Based Path Merging. In: Int Conf Advances and Trends in Software Engineering.
9. Kolosnjaji B, Zarras A, Lengyel T, Webster G, Eckert C (2016) Adaptive Semantics-Aware Malware Classification. In: 13th Conference on Detection of Intrusions and Malware & Vulnerability Assessment.
10. Lengyel T, Kittel T, Eckert C (2015) Virtual Machine Introspection with Xen on ARM. In: 2nd Workshop on Security in Highly Connected IT Systems (SHCIS).
11. Leukert B, Kubach T, Eckert C et al. IoT 2020: Smart and Secure IoT Platform. http://www.iec.ch/whitepaper/pdf/iecWP-IoT2020-LR.pdf
12. Merli D, Sigl G, Eckert C (2013) Identities for embedded systems enabled by physical unclonable functions. Number Theory Cryptogr 8260:125–138
13. Muntean P, Adnan R, Ibing A, Eckert C (2015) 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). IEEE Computer Society, Vancouver, Canada
14. Otto B et al. Industrial Data Space. Whitepaper. https://www.fraunhofer.de/de/forschung/fraunhofer-initiativen/industrial-data-space.htm
15. Pfoh J (2013) Leveraging Derivative Virtual Machine Introspection Methods for Security Applications. Doctoral Thesis, Technische Universität München
16. Schimmel O, Hennig M (2014) Kopier- und Manipulationsschutz für eingebettete Systeme. Datenschutz Datensicherheit – DuD 38(11):742–746
17. Schütte J, Brost G (2016) A Data Usage Control System Using Dynamic Taint Tracking. In: Proceedings of the International Conference on Advanced Information Network and Applications (AINA).
18. Teichmann C, Renatus S, Eichler J (2016) Agile threat assessment and mitigation: an approach for method selection and tailoring. Int J Sec Software Eng (IJSSE) 7(1)
19. Titze D, Stephanow P, Schütte J (2014) App-Ray: User-Driven and Fully Automated Android App Security Assessment. Fraunhofer AISEC TechReport
20. Xiao H, Eckert C (2013) Indicative Support Vector Clustering with Its Application on Anomaly Detection. In: IEEE 12th International Conference on Machine Learning and Applications.