Sichere IT

ohne Schwachstellen und Hintertüren

Working Paper[1]

Entwurf vom 3.1.2020

Arnd Weber, *ehemals Institut für Technikfolgenabschätzung, KIT, Deutschland (arnd.weber@alumni.kit.edu)*

Gernot Heiser, *UNSW Sydney; Data61, CSIRO, Australien; Hensoldt Cyber, Deutschland (gernot@unsw.edu.au)*

Dirk Kuhlmann, *Fraunhofer ISI, Deutschland (dirk.kuhlmann@alumni.tu-berlin.de)*

Martin Schallbruch, *Digital Society Institute, ESMT Berlin*, Deutschland *(martin.schallbruch@esmt.org)*

Anupam Chattopadhyay, *School of Computer Science and Engineering, Nanyang Technical University, Singapur (anupam@ntu.edu.sg)*

Sylvain Guilley, *Télécom ParisTech, Secure-IC, Frankreich (sylvain.guilley@telecom-paristech.fr)*

Michael Kasper, *Fraunhofer Singapur (michael.kasper@fraunhofer.sg)*

Christoph Krauß, *Fraunhofer-Institut für sichere Informationstechnologie, Deutschland (christoph.krauss@sit.fraunhofer.de)*

Philipp S. Krüger, *Digital Hub Cybersecurity, Deutschland (philipp.krueger@alumni.digitalhub-cybersecurity.com)*

Steffen Reith, *Hochschule RheinMain, Deutschland (Steffen.Reith@hs-rm.de)*

Jean-Pierre Seifert, *Institut für Softwaretechnik und Theoretische Informatik, TU Berlin, Deutschland (jpseifert@sect.tu-berlin.de)*

Abstract

Unsere zunehmende Abhängigkeit von Informationstechnik erhöht kontinuierlich die *Safety- und Security-Anforderungen* beim Einsatz dieser Technik. Ein zentrales Problem hierbei sind Schwachstellen von Hard- und Software. Marktkräfte konnten diese Situation bislang nicht grundsätzlich beheben. Eine Gegenstrategie hätte deshalb folgende Optionen zu erwägen: (1) private und staatliche Förderung offener und sicherer IT Produktion, (2) Verbesserung der souveränen Kontrolle bei der Produktion aller IT-Komponenten innerhalb eines Wirtschaftsraumes sowie (3) verbesserte und durchgesetzte Regulierung. Dieses Papier analysiert Vor- und Nachteile dieser Optionen. Es wird vorgeschlagen, die Sicherheit der Schlüsselkomponenten einer Lieferkette durch weltweit verteilte, offene und ggf. mathematisch bewiesene Komponenten zu gewährleisten. Der beschriebene Ansatz erlaubt die Nutzung existierender und neuer proprietärer Komponenten.

[1] Vorbehaltlich endgültiger Akzeptanz zur Veröffentlichung in „TATuP – Zeitschrift für Technikfolgenabschätzung in Theorie und Praxis“ 1/2020 vorgesehen (KIT, vgl. https://www.tatup.de). Kommentare willkommen! Bitte möglichst die endgültige, gedruckte Fassung zitieren.

Probleme

Die Abhängigkeit der Industriegesellschaft von Informationstechnik führt zu hohen Anforderungen an den sicheren Betrieb dieser Technik – sowohl im Sinne der funktionellen Verlässlichkeit (Safety) als auch der IT-Sicherheit (Security im Sinne von *CIA*: *c*onfidentiality, *i*ntegrity, *a*vailability). Diese Anforderungen können, insbesondere in Kombination, durch derzeit produzierte IT-Systeme nur bedingt sichergestellt werden. Infolgedessen können Infrastrukturen ausfallen, Betriebsgeheimnisse entwendet, Autos ferngesteuert, Vermögensschäden verursacht und politische Institutionen ausgespäht werden (Details und Quellen in Weber et al. 2018a, 2018b).

Wesentliche Ursache für die Angriffsmöglichkeiten sind zugrundeliegende Schwächen in Hard- und Software. Sie beginnen bei einfachen Fehlern in der Anwendungssoftware wie etwa dem *Heartbleed-Bug* innerhalb einer Komponente, die zur Verschlüsselung im WWW genutzt wurde. Sie setzen sich fort in Angriffen wie durch die Erpressersoftware *WannaCry*, die den Geheimdiensten bekannte, aber nicht beseitigte Schwächen in Betriebssystemen ausnutzte. Neueren Datums sind Hardware-Trojaner (s. z.B. Becker et al. 2014), wie sie für FPGA-Chips (Actel) und militärische Radaranlagen bereits vermutet wurden (Syrien). Von zunehmender Bedeutung ist auch die Möglichkeit von Angriffen auf IT-Lieferketten (vgl. Bunnie 2019).

Eine substantielle Verbesserung der Situation im Bereich IT-Sicherheit konnte in den letzten Jahren nicht erreicht werden, wie die Statistik der *Computer Vulnerabilities and Exposures* zeigt (Mitre 2019). Spätestens seit den Snowden-Veröffentlichungen muss davon ausgegangen werden, dass nationale Nachrichtendienste Schwachstellen gezielt herstellen oder ankaufen (Abb. 1). Offenkundig betrifft dies nicht nur die Dienste der USA: Russland ist stark im „Cyberspace“ aktiv, gleiches gilt für China. Offiziere der chinesischen Volksbefreiungsarmee haben bereits vor zwei Jahrzehnten die Herstellung „logischer Bomben“ für Computernetzwerke vorgeschlagen (Liang und Wang 1999). Die geheim gehaltenen Hintertüren können unter Umständen von Kriminellen ausgenutzt werden, wie das Beispiel *WannaCry* belegt.

Nahezu täglich werden neue Schwachstellen entdeckt, die von Fehlern in der Programmierung bis zur Ausbeutung von Seiteneffekten spekulativer Programmausführung in der Hardware reichen (*Spectre, Meltdown*). Inzwischen muss selbst die Möglichkeit einer aktiven Einschleusung von Schwachstellen durch die verwendeten Entwicklungswerkzeuge in Erwägung gezogen werden. Die meisten Komponenten für Computer, einschließlich Softwaremodulen und Chips, werden inzwischen in einer komplexen weltweiten Arbeitsteilung erstellt, da dies Skalenerträge ermöglicht. Dabei sind viele Details der Implementierungen selbst für große industrielle Kunden intransparent. Dies gilt für integrierte komplexe Softwaremodule ebenso wie für einzelne Chips und die Frage, wie dieser schaltet. Daraus ergeben sich vielfältige Angriffsmöglichkeiten (Weber et al. 2018a).

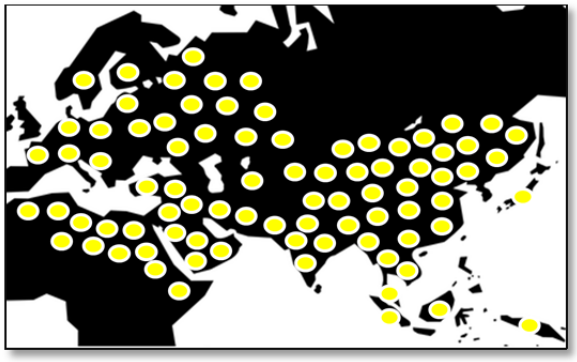

Abb. 1: Von der NSA kompromittierte Computer. Jeder Punkt repräsentiert >500 Geräte. Snowden veröffentlichte, dass z.B. Maschinen von HP, Dell und Cisco unterminiert und die Firmen Belgacom und Gemalto gehackt wurden. Die Abbildung stellt einen neu gezeichneten Ausschnitt der Snowden-Folie „Worldwide SIGINT“ dar (Snowden 2013). *Quelle: Autoren*

Angesichts der Abhängigkeit von digitalen Systemen und den Auseinandersetzungen im Cyberraum erscheint es unzureichend, das Risiko von „giant security breaches“ ausschließlich mit Methoden des „risk management“ und inkrementellen Updates anzugehen (wie z.B. Odlyzko 2019). In Ergänzung hierzu ist es erforderlich, einen grundlegenderen Wandel in die Wege zu leiten, der informationstechnische Sicherheit mittels ökonomisch vertretbarer Verfahren fundamental verbessert und zwar unter Berücksichtigung der weltweit steigenden Konzentration von Kompetenzen und Wertschöpfung (vgl. z.B. Müller-Quade et al. 2017).

Entwicklungsoptionen

Die grundsätzliche Vermeidung von Schwachstellen in Hardware und Software wird im Allgemeinen als nahezu unlösbares Problem angesehen. So wird geltend gemacht, Soft- und Hardware seien zu kompliziert, verifizierte Lösungen teuer und unflexibel und hundertprozentige Sicherheit ohnehin nicht erreichbar. Obwohl aus empirischer und historischer Sicht einiges für diese Einschätzungen spricht, bleibt es Aufgabe der Forschung, die Prämissen dieser Argumente zu ermitteln, sie in Frage zu stellen und nach realisierbaren Ansätzen zu suchen.

Herkömmliche Ansätze wie umfangreicheres Testen und Patching haben sich bisher als nicht ausreichend erwiesen (vgl. Weber et al. 2018a für weitere Informationen). So helfen gegen mögliche Systemschwächen und durch finanzstarke Akteure gesponserte Angriffe graduelle Verbesserungen, wie Updates oder neue Systemschichten, bestenfalls graduell. Auch zusätzliche eingeführte Kontrollkomponenten bieten nur begrenzte Möglichkeiten, weil sie ihrerseits für Angriffe ausgenutzt oder umgangen werden können und zudem auch selbst mit unterminierten Werkzeugen entwickelt worden sein könnten.

Auf europäischer Ebene wird derzeit diskutiert, ob IT-Sicherheit durch Regulierung verbessert werden kann, etwa indem Zertifizierungen nach den *Common Criteria* oder dem *EU Cybersecurity Act* von 2019 vorgeschrieben werden. Derartige Zertifizierungen haben bislang lediglich begrenzte Aussagekraft, zumal bestehende Verfahren die Korrektheit der Implementierung oft nur mit Tests prüfen. Selbst wenn alle zertifizierten Software-Komponenten bewiesenermaßen sicher wären, besteht die Frage nach möglichen Hardware-Schwächen fort, etwa wenn das Design oder der Produktionsprozess geändert wird. Überprüfungen werden z.B. dort kompliziert, wo Hardware Hersteller Teile des Designs geheim halten, um Angriffe zu erschweren oder sie durch Prozessfestlegungen dazu verpflichtet sind. Hierdurch wird die Sicherheit tendenziell reduziert, da diese Komponenten nicht unabhängig nachprüfbar sind (Saltzer und Schroeder 1975; Eurosmart 2014). Ein Kunde kann ein solches Produkt nicht selbst beurteilen. Hinzu kommt, dass die Durchführung der anspruchsvolleren Zertifizierungsstufen sehr kostenintensiv ist.

Ehrgeiziger sind Versuche, kritische Systeme ausschließlich im jeweiligen Staat zu produzieren und so die Kontrolle der IT Produktion auf nationaler Ebene sicherzustellen. So verfügt z.B. China über Durchgriffsmöglichkeiten, mit denen im Prinzip die gesamte Wertschöpfungskette kontrolliert werden kann. Vollständige Autonomie ist bei IT-Systemen allerdings schwer zu erreichen, sobald Hersteller für den Weltmarkt produzieren und Komponenten anderer Anbieter beziehen, deren Designfehler oder absichtlich eingefügte Hintertüren jedes IT-System beeinflussen können, in das sie verbaut sind.

Option offene, verifizierte Lieferketten

Der im Folgenden vorgestellte Ansatz kombiniert offene Produktion, verifizierte Hard- und Software und sichere Lieferketten. Wir schlagen vor, offene Produktionsverfahren über die gesamte Lieferkette einzuführen, die Inputs und Werkzeuge ebenso wie die Produkte selbst umfasst. Hierzu sind zunächst drei Schlüsselfragen zu beantworten: Wie können Schwächen und Hintertüren tatsächlich eliminiert werden? Wie lässt sich dieser Ansatz mit der privatwirtschaftlichen Amortisation von Entwicklungsaufwänden für neue Produkte vereinbaren? Und wie sollten die Kosten offener Produktion umgelegt werden?

Offenheit

Aus Sicherheitsperspektive haben offene Systeme einige grundsätzliche Vorteile: „Current commodity computer hardware and software are proprietary. A thorough security review cannot be performed on systems with undisclosed components." (US-DARPA, vgl. SBIR 2019). Beispiele für offene Systeme sind z.B. das Betriebssystem Linux und das davon abgeleitete Android, die sich erfolgreich am Markt etabliert haben. Eine ähnliche Entwicklung könnte sich im Hardware-Bereich hinsichtlich des RISC-V Prozessor-Designs anbahnen. Diese offene Prozessorarchitektur, die ursprünglich an der Universität Berkeley unter Förderung durch die DARPA entwickelt wurde, ermöglicht freie Inspektion und lizenzkostenfreie Weiterentwicklung.

„Open source" ist per se nicht mit Fehlerfreiheit gleichzusetzen. Dies belegt z.B. der bereits ange-

sprochene *Heartbleed-Bug,* der auf einem jahrelang unentdeckten Implementierungsfehler beruhte. Hier wären Verbesserungen bei der Kontrolle von Spezifikationen und Designs etwa durch Intensivierung automatischer statischer und dynamischer Analyse von Programmen und Testen durch unabhängig arbeitende Gruppen denkbar (vgl. Kiss et al. 2015). Durch diesen Mehraufwand könnte die Sicherheit von Open Source-Komponenten erheblich verbessert werden, doch intensiveres Testen allein kann nie ausschließen, dass unentdeckte Fehler verbleiben.

Abb. 2 a-d: Einige Entwicklungen, die zeigen, dass die neuen Ansätze in der Forschung, in Prototypen und in Produkten angewendet werden. Von links nach rechts:

a) Apple A11-Chip mit Secure Element, in dem der L4 Betriebssystemkern verwendet wird.
b) Unbemannter Boeing Hubschrauber kontrolliert durch das offene, bewiesene seL4.
c) Sicherheitsmodul mit dem offenen LEON SPARC v8 Prozessor.
d) Prototyp eines offenen Sicherheitsmoduls mit dem offenen VexRiscv Prozessor, mit einem Hardwarebeschleuniger für die ChaCha Stromverschlüsselung, ausschließlich mit offenen Entwurfswerkzeugen erstellt (auf einem FPGA-Chip laufend).

Quellen: Wikipedia, Data 61, Secure IC, Schultz/Reith

Formale Verifikation

Hier können offene Systeme Abhilfe schaffen, deren korrektes Funktionieren in Bezug auf Vertraulichkeit und Integrität der verarbeiteten Nutzerdaten mathematisch bewiesen ist („formal verifiziert“). Ein Vorreiter bei der praktischen Realisierung solcher Systeme ist *seL4,* ein Mitglied der L4-Familie von Betriebssystem-Mikrokernen (Klein et al. 2014, vgl. Abb. 2).

Ausgelöst vom Gleitkomma-Divisions-Fehler in Intel-Prozessoren im Jahr 1994 wird seit Jahrzehnten eine formale Verifikation von Teilen der CPU-Designs durchgeführt. Entsprechende Bestrebungen existieren zur Überprüfung kompletter RISC-V Prozessoren (Chlipala 2017). Die zugrundeliegenden formalen Spezifikationen und Beweise sind jedoch aufwändig und verlieren i.d.R. ihre Gültigkeit, sobald am verifizierten Objekt auch nur geringfügige Änderungen vorgenommen werden.

Eine Herausforderung für die Forschung besteht deshalb darin, Verfahren zu entwickeln, mit denen komplexere Systeme kostengünstig zu verifizieren sind. Die Schwierigkeiten für Korrektheitsbeweise komplexer Prozessoren steigen mit der Anzahl der Transistoren, Prozessorkerne, etc. jedoch stark an. Bislang ist unklar, ob man angesichts der wachsenden Integrationsdichte und Transistoranzahl der neuesten Prozessorgenerationen deren Design je zu vertretbaren Kosten beweisen können wird oder ob der Beweisaufwand durch grundsätzliche Änderungen des CPU- und Rechnerdesigns radikal gesenkt werden kann.

Sicherung der Lieferkette

Die Lieferkette für IT kann an nahezu jedem Punkt erfolgreich angegriffen werden – Modifikation des Designs und Beeinflussung des Produktionsprozesses sind ebenso möglich wie die Subversion von Test- und Validierungsverfahren oder Austausch von Systemelementen während der Auslieferung. Es ist damit zu rechnen, dass die Sicherung einiger Komponenten, wie etwa Betriebssystemen oder Prozessoren, dazu führt, dass andere Komponenten angegriffen werden, z.B. Kommunikationschips oder verwendete Softwarewerkzeuge. Ein umfassender Ansatz hätte demzufolge möglichst große Teile dieser Kette zu sichern.

Dort, wo auf geschlossene, nicht verifizierte Anwendungen, z.B. traditionelle Betriebssysteme, zurückgegriffen werden muss, sollten diese durch Mechanismen gekapselt werden, die sie vom vertrauenswürdigen Teil des Systems trennen.

Eine zentrale Herausforderung betrifft die Sicherung der Produktion der Halbleiter in den sog. „Fabs“. Moderne Produktionsanlagen erfordern Milliardeninvestitionen und sind, neben den USA und Israel, in wenigen fernöstlichen Ländern konzentriert. Einer Strategie zur besseren Absicherung der Chip-Produktion kann sich unter anderem folgender Optionen bedienen:

- Lokale Fertigung durch als vertrauenswürdig betrachtete Betreiber und Mitarbeiter („Trusted Fab“), eventuell auf eine Reihe kritischer Schritte am Schluss der Fertigung beschränkt (Sengupta et al. 2019).
- Kontrolle der Chips durch mathematische Verfahren, wie Verschlüsselung (Šišejković et al. 2019) oder zusätzliche Leiterbahnen (Seifert und Bayer 2015).
- Stichprobenartige Inspektion von Chips durch optische Prüfung. Aus praktischer Sicht funktioniert dies am besten bei einfachen Chips mit vergleichsweise großen Strukturen, deren Herstellung für Enthusiasten aus dem open source-Umfeld machbar ist („*libre silicon*“).

Die genannten Optionen müssen teils erst noch erprobt werden.

Gleiches gilt für Ansätze zur Absicherung von Softwarewerkzeugen, die in der Herstellung von Hard- oder Software verwendet werden. Die drei zu untersuchenden Hauptoptionen sind,

- entweder ein offenes System von Werkzeugen zu schaffen und durch intensive Überprüfung die Gefahr von Schwachstellen oder Hintertüren zu minimieren,
- oder den Output eines offenen Werkzeugs formal zu verifizieren
- oder den Output mit jenen proprietärer Werkzeuge auf funktionale Äquivalenz zu vergleichen.

Natürlich muss in allen Fällen die Integrität der Prüfumgebung sichergestellt werden, was evtl. nur langfristig geschehen kann.

Der Vollständigkeit halber sei noch darauf hingewiesen, dass die Mathematik dabei helfen kann, die Authentizität von Chips sicherzustellen, z.B. durch Verwendung von „physically unclonable functions“, die physikalische Implementierungscharakteristika nutzen (Bruneau et al. 2019).

Kosten

Ein wichtiger Faktor für die Realisierung eines offenen Ansatzes ist die Finanzierbarkeit. Derzeit kommen die vorgeschlagenen formalen Verfahren aus Aufwandsgründen zumeist nicht in Betracht. Die Open-Source-Community beispielsweise setzt derzeit i.d.R. keine Instrumente zur formalen Spezifikation ein. Einerseits wird dies als zu aufwändig angesehen, andererseits schränkt eine formal orientierte Vorgehensweise die Flexibilität bei der Weiterentwicklung erheblich ein. Es besteht also Forschungs- und Handlungsbedarf, um formale Beweise leichter und kostengünstiger durchführen zu können.

Die Stückkosten für formal verifizierte, offene Komponenten könnten verringert werden, wenn man höhere Losgrößen erreicht, die Entwicklungskosten global teilt und geringere Lizenzkosten als für proprietäre Tools einbezieht. Durch formal verifizierte Systeme entstehen zudem niedrigere Kosten für Sicherheitsmaßnahmen und für Schadensbehebung. Zudem könnten solche Komponenten wegen der hohen Qualität einen Vorteil im Wettbewerb darstellen und regulatorischen Anforderungen leichter gerecht werden. Eine belastbare Schätzung der Kosten ist wegen der Vielzahl von Variablen derzeit schwer möglich.

Stand des Übergangs zu offenen, bewiesenen Systemen

Eine strategische Initiative für offene, formal bewiesene Komponenten und Systeme könnte auf einer Reihe von Vorarbeiten aufbauen, die seit längerem u.a. von der DARPA gefördert werden. Angesichts der wachsenden Abhängigkeit der US-amerikanischen IT-Wirtschaft von internationalen IT-Zulieferern folgerte die Agentur bereits 2017: “The Open-Source community needs to develop a complete infrastructure” (Salmon 2017).

Inzwischen hat auch die Industrie begonnen, sich intensiver mit dieser Thematik auseinanderzusetzen. Die offene RISC-V-Prozessorarchitektur ist ins Blickfeld von Unternehmen wie Nvidia und Western Digital geraten. Investoren im Umfeld des Alibaba-Konzerns sind dabei, hochleistungsfähige Multicore-CPUs auf RISC-V Basis zu entwickeln (EENewsEurope 2019). Auf der Softwareseite hat z .B. das validierte Mikrokernel-Betriebssystem seL4 das Interesse etwa des deutschen Unternehmens Hensoldt Cyber geweckt.

Durch diese Initiativen werden bereits heute öffentliche und private Gelder in Beweis-basierte, offene Architekturen investiert, die etwa im Bereich von Grafikkarten, Speichermedien oder eingebetteten Systemen zur Anwendung kommen sollen. Wie im

Falle von Linux/Android in der Vergangenheit bereits beobachtbar, kann eine solche Entwicklung bewirken, dass sich der Einsatz derartiger Systeme von ihren ursprünglichen Einsatzfeldern (hochsichere Anwendungen, wie Luftfahrt, Verteidigung und IT-Sicherheitsmodule) auf andere Geräteklassen ausweitet.

Fazit zur globalen Implementation offener Verifizierung

Im Sinne eines „constructive technology assessment“ lassen sich Risiken für den deutschen und europäischen Raum nur dann substantiell verringern, wenn Mechanismen entwickelt werden, die die Anzahl von Schwachstellen, Fehlern und Hintertüren nachweislich reduzieren, idealerweise auf null: „Secure IT“ statt „IT security“.

Eine beträchtliche Zahl technischer Grundlagen für die Entwicklung offener, verifizierter Systeme ist bereits gelegt. Um diesen Ansatz jedoch systematisch auszubauen, bedarf es erheblicher Investitionsmittel. Nötig wären hier forschungs- und industriepolitische Programme zur Frage, wie komplette Wertschöpfungsketten von IT-Systemen offen und sicher gestaltet und verbreitet werden können. In den USA hat die DARPA hierzu einen Investitions- und Forschungsplan entwickelt (*Electronic Resurgence Initiative)*, der die lokale, sichere Produktion von IT-Komponenten zum Ziel hat. Dieser ist jedoch stark auf den militärischen Bereich fokussiert und bezieht US-Hersteller mit vertraulichen Produkten und Prozessen ein. Für den zivilen Bereich, gerade auch außerhalb der USA, sind folgende Programmelemente vonnöten:

1. Initiierung von Piloten und Prototypen, die die gesamte Wertschöpfungskette umfassen,
2. Weiterentwicklung und Tooling von Methoden der formalen Verifikation mit dem Ziel leichterer Anwendbarkeit sowie Ausweitung der Forschung zur formalen Analyse auf komplexere Systeme,
3. Techniken zur redundanten formalen Verifizierung durch geographisch verteilte, unabhängig arbeitende Teams, insbesondere zur Aufgabenverteilung und Zusammenführung der Ergebnisse,
4. Untersuchung von Techniken zur Zertifizierung, die nicht auf der Vertraulichkeit der Produktion und der Verifizierungstechniken beruhen,
5. Training einer ausreichenden Anzahl von fachlich qualifiziertem Personal, sowie
6. Entwicklung und Erprobung von Methoden zur Kontrolle geographisch entfernter Fabs und weltweiter Lieferwege.

Parallel hierzu müssten Geschäftsmodelle mit dem Ziel erarbeitet werden, die anfänglichen Kosten möglichst global zu verteilen. Ähnlich der Förderung von RISC-V wäre hier eine Kostenteilung zwischen privaten und öffentlichen Trägern naheliegend. Preiswerte, verifizierte Werkzeuge und Komponenten könnten Innovationen in vielen Branchen erleichtern und für viele Länder die „Souveränität“ im IT-Bereich stärken.

Ferner sollte untersucht werden, ob und wie eine derartige Zielstellung effizient durch politische oder durch regulatorische Maßnahmen flankiert werden sollte. Die Koordination des beschriebenen Vorhabens könnte dabei in Deutschland z.B. durch zwei in neuerer Zeit gegründete Institutionen gefördert werden, der „Agentur für Innovation in der Cybersicherheit“ (Verteidigungs- und Innenministerium) und der „Agentur zur Förderung von Sprunginnovationen“ (Forschungsministerium).

Der vorgeschlagene Ansatz hat die Absicherung der gesamten Produktions- und Lieferkette zum Ziel und erfordert deshalb abgestimmte Anstrengungen einer Vielzahl von Arbeitsgebieten. Die Komplexität eines solchen Vorhabens dürfte jener der derzeitigen Pilot-Initiativen zur Etablierung europäischer *Cyber Competence Networks* nicht nachstehen. Deren Finanzierungsrahmen liegt zwischen10 und 20 Millionen Euro und ein entsprechender Aufwand sollte auch für die Entwicklung eines technischen und organisatorischen Rahmens veranschlagt werden. Echte Produktentwicklung für den zivilen Bereich würden allerdings deutlich höhere Aufwendungen erfordern (die DARPA hat hierfür derzeit ca. U$ 1,5 Mrd. eingeplant). Die Umsetzung würde ein umfangreiches Public-Private-Partnership Programm oder den Aufbau eines nationalen oder europäischen „Champions“ unter Mobilisierung von Risikokapital erfordern, ggf. in Kooperation mit Akteuren aus anderen Ländern.

Aus politischer und ökonomischer Perspektive sollten parallele und alternative Entwicklungen auf globaler Ebene beobachtet und deren Ansätze und Risiken weiter analysiert werden. Hierzu gehören etwa Versuche, Lieferketten auf rein nationaler Ebene zu etablieren (USA, China, Indien) oder die Entwicklung und der Einsatz offener, aber bislang unbewiesener Hardware-Komponenten (Google, Alibaba, Nvidia etc.).

Die Autoren haben zur Umsetzung die Quattro S Initiative gegründet (*Security, Safety, Sovereignty, Social Product*).

Die Autoren danken den Gutachtern, Gabriele Müller-Datz, Arnaud Saffari sowie Vertretern US-amerikanischer und deutscher Unternehmen für Anregungen.

Literatur

Becker, Georg T.; Regazzoni, Francesco; Paar, Christof; Burleson, Wayne P. (2014): Stealthy dopant-level hardware Trojans: extended version. J Cryptogr Eng 4:19–31.

Bruneau, Nicolas; Danger, Jean-Luc; Facon, Adrien; Guilley, Sylvain; Hamaguchi, Soshi; Hori, Yohei; Kang, Yousung; Schaub, Alexander (2019): Development of the Unified Security Requirements of PUFs During the Standardization Process. SecITC 2018. LNCS 11359.

Bunnie (Andrew Huang; 2019): Supply Chain Security - If I were a Nation State... BlueHatIL. Tel Aviv. https://msrnd-cdn-stor.azureedge.net /bluehat/bluehatil/2019/assets/doc/Supply%20Chain%20Security%20-%20If%20I%20were%20a%20Nation%20State....pdf.

Chlipala, Adam (2017): Coming Soon: Machine-Checked Mathematical Proofs in Everyday Software and Hardware Development. CCC 2017. https://events.ccc.de/congress/2017/ Fahrplan /events/9105.html.

EENewsEurope (2019): Sixteen core RISC-V processor Xuan Tie 910 | Alibaba. 25.7.2019. https://www.eenewseurope.com/news/sixteen-core-risc-v-processor-xuan-tie-910-alibaba.

Eurosmart (2014): Security IC Platform Protection Profile with Augmentation Packages. https://www.commoncriteriaportal.org/files/ppfiles/pp0084b _pdf.pdf.

Kiss, Balázs; Kosmatov, Nikolai; Pariente, Dillon; Puccetti, Armand: Combining Static and Dynamic Analyses for Vulnerability Detection. Illustration on Heartbleed (2015): Haifa Verification Conference. http://nikolai.kosmatov.free.fr/ publications/ kiss_kpp_hvc_2015.pdf.

Klein, Gerwin; Andronick, June; Elphinstone, Kevin; Murray, Toby; Sewell, Thomas; Kolanski, Rafal; Heiser, Gernot (2014): Comprehensive formal verification of an OS microkernel, ACM Transactions on Computer Systems, Volume 32, Number 1, 2:1-2:70, February 2014.

Liang, Qiao; Wang, Xiangsui (1999): Unrestricted Warfare. Beijing, PLA Literature and Arts Publishing House. https://www.oodaloop.com/ documents/ unrestricted.pdf.

Mitre (2019): CVE Details. https://www.cvedetails.com/browse-by-date.php.

Müller-Quade, Jörn; Reussner, Ralf; Beyerer, Jürgen (2017): Karlsruher Thesen zur Digitalen Souveränität Europas. https://www.fzi.de/ fileadmin/ user_upload/PDF/2017-10-30_KA-Thesen-Digitale-Souveraenitaet-Europas_ Web.pdf.

Odlyzko, Andrew (2019): Cybersecurity is not very important. ACM Ubiquity, June 2019, 1-23.

Salmon, Linton (2017): A Perspective on the Role of Open-Source IP in Government Electronic Systems. RISC-V Workshop 2017. https:// content .riscv.org/wp-content/uploads/2017/12/ Wed-1042-RISCV-Open-Source-LintonSalmon .pdf.

Saltzer, Jerome; Schroeder, Michael (1975): The protection of information in computer systems. Proceedings of the IEEE, 63(19): 1278-1308.

SBIR (2019): Open Source High Assurance System. https://www.sbir.gov/sbirsearch/detail/ 1508741.

Seifert, Jean-Pierre; Bayer, Christoph (2015): Trojan-Resilient Circuits. In: Pathan, Al-Sakib Khan (Hrsg.): Securing Cyber-Physical Systems, Boca Raton, 349-370.

Sengupta, Abhrajit; Nabeel, Mohammed; Knechtel, Johann; Sinanoglu, Ozgur (2019): A New Paradigm

in Split Manufacturing: Lock the FEOL, Unlock at the BEOL. https://ieeexplore.ieee.org/document/8715281.

Šišejković, Dominik; Merchant, Farhad; Leupers, Rainer; Ascheid, Gerd; Kegreiss, Sascha (2019): Control-Lock: Securing Processor Cores Against Software-Controlled Hardware Trojans. ACM Great Lakes Symposium on VLSI: 27-32.

Snowden, Edward (2013): Worldwide SIGINT. https://edwardsnowden.com/wp-content /uploads/2013/11/nsa1024.jpg.

Weber, Arnd; Reith, Steffen; Kasper, Michael; Kuhlmann, Dirk; Seifert, Jean-Pierre; Krauß, Christoph (2018a): Sovereignty in information technology. Security, safety and fair market access by openness and control of the supply chain. Karlsruhe, Wiesbaden, Singapur, Darmstadt, Berlin: KIT-ITAS, HS RheinMain, Fraunhofer Singapur/SIT, TU Berlin. https://www.itas.kit.edu/projekte_ webe17_quattros.php.

Weber, Arnd; Reith, Steffen; Kasper, Michael; Kuhlmann, Dirk; Seifert, Jean-Pierre; Krauß, Christoph (2018b): Open Source Value Chains for Addressing Security Issues Efficiently. IEEE CRE, Lisbon. https://ieeexplore.ieee.org/ document/8432033/.

Autoren

Prof. Dr.-Ing. Anupam Chattopadhyay lehrt am SCSE, Nanyang Technical University, Singapur. An der RWTH Aachen arbeitete er an Chiparchitekturen, an EDA sowie an der Automatisierung der Spezifikation von Chips (RTL), was zu einem Spinoff führte, das von Synopsys übernommen wurde. Hierfür erhielt er die Borchers Plakette.

Prof. Dr. Sylvain Guilley ist CTO von Secure-IC, Frankreich sowie Professor an Télécom-ParisTech, Mitarbeiter der École Normale Supérieure (ENS), Außerordentlicher Professor an der Chinesischen Akademie der Wissenschaften sowie Herausgeber von Standards wie ISO/IEC 20897 (Physically Unclonable Functions).

Prof. Dr. Gernot Heiser ist leitender Forscher bei CSIRO's Data61, wo seL4 bewiesen wurde, und Scientia Professor an UNSW Sydney, wo er den John Lions Chair of Operating Systems an der UNSW Sydney innehat. Ferner ist er Gründer der Open Kernel Labs, deren L4 Kern u.a. in der Secure Enclave aller iOS-Geräte läuft. Er ist Chief Scientist (Software) bei HENSOLDT Cyber.

Michael Kasper leitet die Arbeitsgruppe "Cyber- und Information Security" bei Fraunhofer Singapore und Mitbegründer von opentrust.ai in Singapur. Er ist assoziierter Senior Researcher beim Fraunhofer Institut für Sichere Informationstechnologie (SIT).

Prof. Dr. Christoph Krauß leitet am Fraunhofer-Institut für Sichere Informationstechnologie SIT die Abteilung Cyber-Physical Systems Security und ist verantwortlich für das Geschäftsfeld Automotive Security. Weiterhin ist er Professor für das Fachgebiet Netzwerksicherheit an der Hochschule Darmstadt.

Philipp S. Krüger ist Managing Director von Accenture Security für Deutschland, Schweiz, Österreich und Russland. Er ist Mitbegründer der Digital Hub Cybersecurity, war Berater des Verteidigungsministeriums für Cyberspace und Innovation und ist Leiter der Agile Cyber Deterrence Group des Instituts für Sicherheitspolitik an der Universität Kiel.

Dirk Kuhlmann ist Senior Researcher am Fraunhofer-Institut für System- und Innovationsforschung. Von 1995 bis 2017 arbeitete er für die Hewlett Packard Laboratories in Bristol in der Forschungsgruppe für IT-Sicherheit mit Schwerpunkt Open-Source Software.

Prof. Dr. Steffen Reith ist Professor für Theoretische Informatik an der Hochschule RheinMain in Wiesbaden. Während seiner Tätigkeit bei Elektrobit Automotive hat er Produkte mit kryptografischen Funktionen entwickelt, die noch heute bei BMW, Daimler und anderen Herstellern verwendet werden.

Martin Schallbruch ist stellvertretender Direktor des Digital Society Institute (DSI) und Senior Researcher an der European School of Management and Technology (ESMT) in Berlin. Gleichzeitig ist er Lehrbeauftragter am Karlsruher Institut für Technologie. Im Bundesinnenministerium war er zuletzt Leiter der Abteilung für Informationstechnik, Digitale Gesellschaft und Cybersicherheit.

Prof. Dr. Jean-Pierre Seifert ist Einstein Professor für das Fachgebiet "Security in Telecommunications" an der TU Berlin und den Telekom Innovation Laboratories. Er hat u.a. bei Samsung geforscht. 2002 wurde er bei Infineon als "Inventor of the Year" und 2005 von Intel mit Preisen für neue CPU-Sicherheitsinstruktionen ausgezeichnet.

Dr. Arnd Weber ist Volkswirt und Soziologe. Bis zu seiner Pensionierung war er Senior Researcher beim Institut für Technikfolgenabschätzung und Systemanalyse des KIT und hat die EU und die Bundesregierung beraten. Nach einem Aufenthalt bei NTT hat er 2004 die Probleme der europäischen Mobilfunkindustrie vorausgesagt.