# Sichere IT ohne Schwachstellen und Hintertüren

Weber, Arnd; Heiser, Gernot; Kuhlmann, Dirk; Schallbruch, Martin; Chattopadhyay, Anupam; Guilley, Sylvain; Kasper, Michael; Krauß, Christoph; Krüger, Philipp S.; Reith, Steffen; Seifert, Jean-Pierre

Veröffentlichungsversion / Published Version
Zeitschriftenartikel / journal article

**Empfohlene Zitierung / Suggested Citation:**
Weber, A., Heiser, G., Kuhlmann, D., Schallbruch, M., Chattopadhyay, A., Guilley, S., ... Seifert, J.-P. (2020). Sichere IT ohne Schwachstellen und Hintertüren. *TATuP - Zeitschrift für Technikfolgenabschätzung in Theorie und Praxis / Journal for Technology Assessment in Theory and Practice*, *29*(1), 30-36. https://doi.org/10.14512/tatup.29.1.30

# Sichere IT ohne Schwachstellen und Hintertüren

**Arnd Weber**, *Hexentalstr. 31, 79283 Bollschweil (arnd.weber@alumni.kit.edu)*
**Gernot Heiser**, *UNSW Sydney (gernot@unsw.edu.au)*
**Dirk Kuhlmann**, *Fraunhofer-Institut für System- und Innovationsforschung (dirk.kuhlmann@alumni.tu-berlin.de)*
**Martin Schallbruch**, *Digital Society Institute, European School of Management and Technology (ESMT) (martin.schallbruch@esmt.org)*
**Anupam Chattopadhyay**, *Nanyang Technical University (anupam@ntu.edu.sg)*
**Sylvain Guilley**, *Télécom ParisTech (sylvain.guilley@telecom-paristech.fr)*
**Michael Kasper**, *Fraunhofer Singapore (michael.kasper@fraunhofer.sg)*
**Christoph Krauß**, *Fraunhofer-Institut für sichere Informationstechnologie (christoph.krauss@sit.fraunhofer.de)*
**Philipp S. Krüger**, *Digital Hub Cybersecurity (philipp.krueger@alumni.digitalhub-cybersecurity.com)*
**Steffen Reith**, *Hochschule RheinMain (Steffen.Reith@hs-rm.de)*
**Jean-Pierre Seifert**, *Technische Universität Berlin (jpseifert@sect.tu-berlin.de)*



Unsere zunehmende Abhängigkeit von Informationstechnik erhöht kontinuierlich die Safety- und Security-Anforderungen bei deren Einsatz. Ein zentrales Problem hierbei sind Schwachstellen von Hard- und Software. Marktkräfte konnten diese Situation bislang nicht grundsätzlich beheben. Eine Gegenstrategie sollte deshalb folgende Optionen erwägen: (1) private und staatliche Förderung offener und sicherer IT-Produktion, (2) Verbesserung der souveränen Kontrolle bei der Produktion aller kritischen IT-Komponenten innerhalb eines Wirtschaftsraumes sowie (3) verbesserte und durchgesetzte Regulierung. Dieser Beitrag 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.

***Secure IT without vulnerabilities and back doors***

*Increasing dependence on information technology calls for strengthening the requirements on their safety and security. Vulnerabilities that result from flaws in hardware and software are a core problem which market mechanisms have failed to eliminate. A strategy for resolving this issue should consider the following options: (1) private- and public-sector funding for open and secure production, (2) strengthening the sovereign control over the production of critical IT components within an economic zone, and (3) improving and enforcing regulation. This paper analyses the strengths and weaknesses of these options and proposes a globally distributed, secure supply chain based on open and mathematically proved components. The approach supports the integration of legacy and new proprietary components.*


https://doi.org/10.14512/tatup.29.1.30
Submitted: 22. 09. 2019. Peer reviewed. Accepted: 08. 01. 2020

**Keywords:** *cybersecurity, sovereignty, open source, verification, supply chain risks*

## 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 im Sinne von Vertrauenswürdigkeit, Integrität, Verfügbarkeit (*confidentiality*, *integrity*, *availability*, CIA). Beide 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 (Weber et al. 2018 a, 2018 b).

Wesentliche Ursache für die Angriffsmöglichkeiten sind vielfältige 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 World Wide Web 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 (Becker et al. 2014), deren Existenz in elektronischen Halbleiterbauelementen, z. B. FPGA-Chips, und militärischen Radaranlagen in Syrien bereits behauptet wurde. Von zunehmender Bedeutung ist auch die Möglichkeit von Angriffen auf IT-Lieferketten (Huang 2019).

Eine substanzielle Verbesserung der Situation im Bereich IT-Sicherheit konnte in den letzten Jahren nicht erreicht werden, wie die Statistik der *Computer Vulnerabilities and Expo-*

*sures* zeigt (MITRE 2019). Spätestens seit den Snowden-Veröffentlichungen im Jahr 2013 muss davon ausgegangen werden, dass nationale Nachrichtendienste Schwachstellen gezielt herstellen oder ankaufen (Abb. 1). Offenkundig betrifft dies nicht nur die Dienste der USA: Auch 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 aus strategischer Motivation geheim gehaltenen Hintertüren können unter Umständen von Kriminellen ausgenutzt werden, wie das Beispiel *WannaCry* belegt.

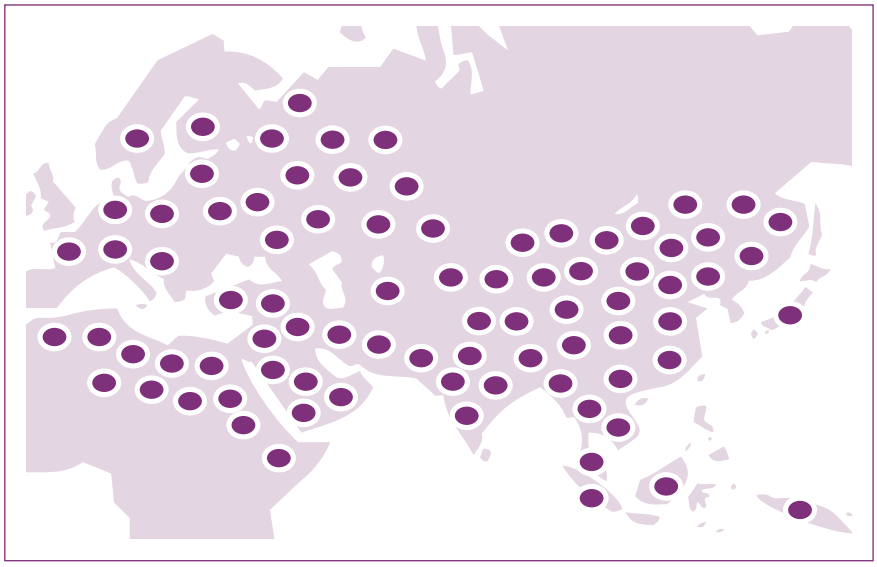


**Abb. 1:** Von der US-amerikanischen National Security Agency (NSA) kompromittierte Computer. Jeder Punkt repräsentiert > 500 Geräte. Der Whistleblower Edward Snowden veröffentlichte, dass z. B. Maschinen von HP, Dell und Cisco unterminiert und die Firmen Belgacom und Gemalto gehackt wurden.
*Quelle: Angepasster Ausschnitt aus Snowden 2013*

Nahezu täglich werden neue Schwachstellen entdeckt, die von Fehlern in der Programmierung bis zu ausnutzbaren Seiteneffekten spekulativer Programmausführung in der Hardware reichen (*Spectre* und *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 Softwaremodule und Chips, werden inzwischen in einer komplexen weltweiten Arbeitsteilung erstellt. Dabei sind viele Details der Implementierungen selbst für große industrielle Kunden intransparent. Dies gilt für integrierte komplexe Softwaremodule ebenso wie für einzelne Hardwarekomponenten. Daraus ergeben sich vielfältige Angriffsmöglichkeiten (Weber et al. 2018 a).

*Zertifizierungen haben bislang lediglich begrenzte Aussagekraft für die IT-Sicherheit.*

Angesichts der Abhängigkeit von digitalen Systemen und den Auseinandersetzungen im Cyberraum erscheint es unzureichend, das Risiko von schwerwiegenden Sicherheitsverletzungen ausschließlich mit Methoden des Risikomanagements und inkrementellen Updates anzugehen (Odlyzko 2019). In Ergänzung hierzu ist es erforderlich, einen grundlegenden 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 (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 infrage zu stellen und nach realisierbaren Ansätzen zu suchen.

Herkömmliche Ansätze wie umfangreicheres Testen und *Patching* haben sich bisher als nicht ausreichend erwiesen (Weber et al. 2018 a). 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 selbst mit unterminierten Werkzeugen entwickelt worden sein könnten.

Auf europäischer Ebene wird derzeit diskutiert, ob IT-Sicherheit durch Regulierung der Hard- und Software 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 meist nur mit Tests prüfen. Selbst wenn alle zertifizierten Software-Komponenten bewiesenermaßen sicher wären, besteht die Frage nach möglichen Hard-

ware-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, die Kontrolle der IT Produktion auf nationaler Ebene sicherzustellen und kritische Systeme ausschließlich im Inland zu produzieren. 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.

*Eine Herausforderung für die Forschung besteht darin, Verfahren zu entwickeln, die komplexere Systeme kostengünstig verifizieren können.*

## 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 ist zunächst die Schlüsselfrage zu beantworten: Wie können Schwächen und Hintertüren tatsächlich eliminiert werden? Danach ist zu fragen, wie der Ansatz zu finanzieren und mit der privatwirtschaftlichen Amortisation von Entwicklungsaufwänden für neue Produkte vereinbaren wäre.

### Offenheit

Aus Sicherheitsperspektive haben offene Systeme einige grundsätzliche Vorteile gegenüber vertraulichen Systemen. So konstatiert das US Department of Defence im Rahmen einer Ausschreibung für Projekte zur Cybersicherheit: „Current commodity computer hardware and software are proprietary. A thorough security review cannot be performed on systems with undisclosed components." (SBIR 2018) Beispiele für offene Systeme sind 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 an der Universität Berkeley unter Förderung durch die Defense Advanced Research Projects Agency (DARPA) und in Kooperation mit der Industrie entwickelt wurde, ermöglicht freie Inspektion und lizenzkostenfreie Weiterentwicklung.

*Open source* ist per se nicht mit Fehlerfreiheit gleichzusetzen. Dies belegt z. B. der bereits angesprochene *Heartbleed-Bug,* der auf einem jahrelang unentdeckten Implementierungsfehler beruhte. Hier sind 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 (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.

### Formale Verifikation

Gegen unentdeckte Schwächen 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, die komplexere Systeme kostengünstig verifizieren können. 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.


**Abb. 2:** Diese Entwicklungen zeigen beispielhaft, dass die neuen Ansätze in der Forschung, in Prototypen und in Produkten angewendet werden. *(V. l. n. r.:)* [1] Apples A11-Chip mit Secure Element, in dem der L4 Betriebssystemkern verwendet wird; [2] Unbemannter Boeing Hubschrauber kontrolliert durch das offene, bewiesene seL4; [3] Sicherheitsmodul mit dem offenen LEON-SPARC-v8-Prozessor; [4] 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: [1] Wikipedia (2020); [2] Data61 (2020); [3] Sylvain Guilley, Secure-IC; [4] Steffen Reith*



## 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 Betriebssysteme 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 *Fabs* genannten Produktionsanlagen. Diese erfordern Milliardeninvestitionen und sind, neben den USA und Israel, auf wenige fernöstliche Länder konzentriert. Eine 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, wie durch das *Libre Silicon*-Projekt angestrebt (Libre Silicon 2020).

Die genannten Optionen müssen teils erst noch entwickelt und 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 hier:

- 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 selten Instrumente zur formalen Spezifikation oder Verifikation 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 auf die Forschungsetats mehrerer Länder und Unternehmen verteilt, dem Beispiel der Kooperation von US-Firmen mit der DARPA folgend, 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, S. 9). Inzwischen hat auch die Industrie in den USA, Asien und Europa begonnen, sich intensiver mit dieser Thematik auseinanderzusetzen und bspw. hochleistungsfähige Multicore-CPUs auf RISC-V Basis zu entwickeln oder auf Softwareseite auf das verifizierte Mikrokernel-Betriebssystem seL4 zurückzugreifen (Sauter 2019; Hettinga 2019; hartpunkt.de 2018).

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 Implementierung offener Verifizierung

Im Sinne eines *constructive technology assessment* lassen sich Risiken für den deutschen, europäischen und letztlich globalen Raum nur dann substanziell 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 Pilotprojekten 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 geografisch 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 geografisch 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 Regierungsinstitutionen gefördert werden: die Agentur für Innovation in der Cybersicherheit und die Agentur zur Förderung von Sprunginnovationen.

*Das Ziel „Secure IT" statt „IT security" lässt sich nur erreichen, wenn die Anzahl von Schwachstellen, Fehlern und Hintertüren idealerweise auf null reduziert wird.*

Der vorgeschlagene Ansatz hat die Absicherung der gesamten Produktions- und Lieferkette zum Ziel und erfordert deshalb abgestimmte Anstrengungen über eine 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 zwischen 10 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 für fünf Jahre ca. US-$ 1,5 Mrd. eingeplant). Die Umsetzung würde ein umfangreiches Public-Private-Partnership-Programm mit vielen Akteuren oder auch 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 durch etablierte IT-Unternehmen.

## Danksagung

Die Autoren danken G. Müller-Datz und A. Saffari für die Begutachtung sowie Vertretern US-amerikanischer und deutscher Unternehmen für Anregungen.

## Literatur

Becker, Georg; Regazzoni, Francesco; Paar, Christof; Burleson, Wayne (2014): Stealthy dopant-level hardware Trojans. Extended version. In: Journal of Cryptographic Engineering 1 (4), S. 19–31.

Bruneau, Nicolas et al. (2019): Development of the unified security requirements of PUFs during the standardization process. In: Jean-Louis Lanet und Cristian Toma (Hg.): Innovative Security Solutions for Information Technology and Communications. Cham: Springer, S. 314–330.

Chlipala, Adam (2017): Coming soon. Machine-checked mathematical proofs in everyday software and hardware development. Chaos Communication Congress. Leipzig, Deutschland, 27.–30. 12. 2017. Online verfügbar unter https://events.ccc.de/congress/2017/Fahrplan/events/9105.html, zuletzt geprüft am 06. 11. 2019.

Data61 (2020): The HACMS project @ Data61. Online verfügbar unter https://ts.data61.csiro.au/projects/TS/SMACCM/, zuletzt geprüft am 08. 01. 2020.

Eurosmart – European Smart Card Association (2014): Security IC platform protection profile with augmentation packages. Version 1.0. Online verfügbar unter https://www.commoncriteriaportal.org/files/ppfiles/pp0084b_pdf.pdf, zuletzt geprüft am 06. 11. 2019.

hartpunkt.de (2018): Hensoldt kooperiert mit CSIROs Data61. Online verfügbar unter https://www.hartpunkt.de/hensoldt-kooperiert-mit-csiros-data61/, zuletzt geprüft am 08. 01. 2020

Hettinga, Wisse (2019): Sixteen core RISC-V processor Xuan Tie 910. Alibaba. In: EENewsEurope, 25. 07. 2019. Online verfügbar unter https://www.eenewseurope.com/news/sixteen-core-risc-v-processor-xuan-tie-910-alibaba, zuletzt geprüft am 06. 11. 2019.

Huang, Andrew (2019): Supply chain security. „If I were a Nation State". BlueHat IL 2019. Israel, Tel Aviv, 06.–07. 02. 2019. Online verfügbar unter https://www.youtube.com/watch?v=RqQhWitJ1As&list=UUp892CjX6wps88JivisRMtA&index=6&t=0s, zuletzt geprüft am 21. 01. 2020.

Kiss, Balázs; Kosmatov, Nikolai; Pariente, Dillon; Puccetti, Armand (2015): Combining static and dynamic analyses for vulnerability detection. Illustration on Heartbleed. In: Nir, Piterman (Hg.): Hardware and software. Verification and testing. Cham: Springer, S. 39–50.

Klein, Gerwin et al. (2014): Comprehensive formal verification of an OS microkernel. In: ACM Transactions on Computer Systems 32 (1), S. 2:1–2:70.

Liang, Qiao; Wang, Xiangsui (1999): Unrestricted warfare. Beijing: PLA Literature and Arts Publishing House. Online verfügbar unter https://www.oodaloop.com/documents/unrestricted.pdf, zuletzt geprüft am 06. 11. 2019.

Libre Silicon (2020): Libre Silicon. Free semiconductors for everyone. Online verfügbar unter https://libresilicon.com/, zuletzt geprüft am 08. 01. 2020.

MITRE (2019): CVE Details. Online verfügbar unter https://www.cvedetails.com/browse-by-date.php, zuletzt geprüft am 06. 11. 2019.

Müller-Quade, Jörn; Reussner, Ralf; Beyerer, Jürgen (2017): Karlsruher Thesen zur Digitalen Souveränität Europas. Online verfügbar unter https://www.fzi.de/fileadmin/user_upload/PDF/2017-10-30_KA-Thesen-Digitale-Souveraenitaet-Europas_Web.pdf, zuletzt geprüft am 21. 01. 2020.

Odlyzko, Andrew (2019): Cybersecurity is not very important. In: Ubiquity, Issue June, S. 1–23. DOI: 10.1145/3333611.

Salmon, Linton (2017): A perspective on the role of open-source IP in government electronic systems. 7th RISC-V Workshop. Milpitas, USA, 28.–30. 11. 2017. Online verfügbar unter https://content.riscv.org/wp-content/uploads/2017/12/Wed-1042-RISCV-Open-Source-LintonSalmon.pdf, zuletzt geprüft am 21. 01. 2020.

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

Sauter, Marc (2019): Wieso RISC-V sich durchsetzen wird. In: golem.de, 17. 10. 2019. Online verfügbar unter https://www.golem.de/news/offene-prozessor-isa-wieso-risc-v-sich-durchsetzen-wird-1910-141978.html, zuletzt geprüft am 21. 01. 2020

SBIR – The Small Business Innovation Research Program (2018): Open source high assurance system. Online verfügbar unter https://www.sbir.gov/sbirsearch/detail/1508741, zuletzt geprüft am 06. 11. 2019.

Seifert, Jean-Pierre; Bayer, Christoph (2015): Trojan-resilient circuits. In: Al-Sakib Pathan (Hg.): Securing cyber-physical systems. Boca Raton: CRC Press, S. 349–370.

Sengupta, Abhrajit; Nabeel, Mohammed; Knechtel, Johann; Sinanoglu, Ozgur (2019): A new paradigm in split manufacturing. Lock the FEOL, unlock at the BEOL. In: Proceedings der Design, Automation & Test in Europe Conference & Exhibition 2019.

Šišejković, Dominik; Merchant, Farhad; Leupers, Rainer; Ascheid, Gerd; Kegreiss, Sascha (2019): Control-lock. Securing processor cores against software-controlled hardware Trojans. In: Proceedings des ACM Great Lakes Symposium on VLSI, S. 27–32.

Snowden, Edward (2013): Worldwide SIGINT. Online verfügbar unter https://edwardsnowden.com/wp-content/uploads/2013/11/nsa1024.jpg, zuletzt geprüft am 21. 01. 2020.

Weber, Arnd; Reith, Steffen; Kasper, Michael; Kuhlmann, Dirk; Seifert, Jean-Pierre; Krauß, Christoph (2018 a): Sovereignty in information technology. Security, safety and fair market access by openness and control of the supply chain. Karlsruhe: KIT-ITAS. Online verfügbar unter http://www.itas.kit.edu/pub/v/2018/weua18a.pdf, zuletzt geprüft am 21. 01. 2020.

Weber, Arnd; Reith, Steffen; Kasper, Michael; Kuhlmann, Dirk; Seifert, Jean-Pierre; Krauß, Christoph (2018 b): Open source value chains for addressing security issues efficiently. In: Proceedings der IEEE International Conference on Software Quality, Reliability and Security Companion 2018, S. 599–606.

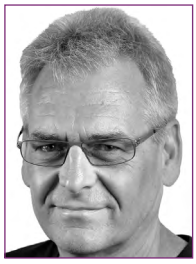
Wikipedia (2020): Apple A11 Bionic. Online verfügbar unter https://de.wikipedia.org/wiki/Apple_A11_Bionic, zuletzt geprüft am 21. 01. 2020.

### 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).

### PROF. DR.-ING. 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 und Scientia Professor an UNSW Sydney (John Lions Chair of Operating Systems). Er war 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 und Fellow der ACM, der IEEE und der australischen Akademie der Technischen Wissenschaften.

### MICHAEL KASPER

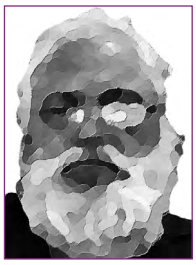
leitet die Arbeitsgruppe „Cyber- und Information Security" bei Fraunhofer Singapore und Mitbegründer von opentrust.ai in Singapur. Er ist assoziierter Senior Researcher beim Fraunhofer-Institut für Sichere Informationstechnologie (SIT).

### PROF. DR. CHRISTOPH KRAUSS

leitet am Fraunhofer-Institut für Sichere Informationstechnologie (SIT), Darmstadt, 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 (ISI), Karlsruhe. 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 für den Serieneinsatz in aktuellen Automobilen entwickelt.

### 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 Infineon, Intel und Samsung geforscht.

### 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. Er hat u. a. an der Goethe-Universität Frankfurt und bei NTT Yokosuka geforscht.