Secure IT without Vulnerabilities and Backdoors

Arnd Weber
Bollschweil, Germany
arnd.weber@alumni.kit.edu

Gernot Heiser
UNSW
Sydney, Australia
gernot@unsw.edu.au

Dirk Kuhlmann†
formerly Fraunhofer ISI
Karlsruhe, Germany

Martin Schallbruch
Digital Society Institute, ESMT
Berlin, Germany
martin.schallbruch@esmt.org

Anupam Chattopadhyay
Nanyang Technical University
Singapore
anupam@ntu.edu.sg

Sylvain Guilley
Télécom ParisTech
Paris, France
sylvain.guilley@telecom-paristech.fr

Michael Kasper
Fraunhofer Singapore
Singapore
michael.kasper@fraunhofer.sg

Christoph Krauß
Darmstadt University of Applied Sciences
Darmstadt, Germany
christoph.krauss@h-da.de

Philipp S. Krüger
Digital Hub Cybersecurity
Darmstadt, Germany
philipp.krueger@alumni.digitalhub-cybersecurity.com

Steffen Reith
RheinMain University of Applied Sciences
Wiesbaden, Germany
Steffen.Reith@hs-rm.de

Jean-Pierre Seifert
TU Berlin
Berlin, Germany
jpseifert@sect.tu-berlin.de

***Abstract*—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.**

Keywords—cybersecurity, sovereignty, open source, verification, supply chain risks

Problems

The dependence of the industrial society on information technology leads to heavy demands on this technology's secure operation – both in terms of functional reliability (safety) and IT security (confidentiality, integrity, and availability). Currently produced IT systems do not fully meet these requirements. As a result, infrastructure can fail, company secrets can be stolen, cars can be controlled by remote attackers, financial losses can be caused, and political institutions can be spied on (Weber et al. 2018a, 2018b).[1]

The underlying enablers of such attacks are weaknesses in hard- and software. They start with simple errors in the application software, such as the *Heartbleed* bug within a component used for encryption on the World Wide Web. They continue with attacks such as by the *WannaCry* ransomware, which exploited weaknesses in operating systems known to intelligence agencies, but not fixed. More recent are hardware Trojans (Becker et al. 2014), whose existence has already been suspected in electronic semiconductor devices, e.g., FPGA chips and military radar systems in Syria (Adee 2008, Haaretz 2018). Also of increasing importance is the possibility of attacks on IT supply chains (Bunnie 2019, cf. Fig. 1; Bloomberg 2021).

IT security has not substantially improved in recent years, as the statistics of *computer vulnerabilities and exposures* show (Mitre 2019). Ever since the Snowden disclosures, it must be assumed that national intelligence services are deliberately creating or purchasing vulnerabilities (Fig. 2, 3). This does not only apply to U.S. intelligence services, Russia is also highly active in cyberspace, as is China. More than two decades ago, officers of the Chinese People's Liberation Army proposed implementing "logic bombs" for computer networks (Liang and Wang 1999). Such backdoors, when kept secret for strategic purposes, can be exploited by criminals, as the *WannaCry* example has demonstrated.

New vulnerabilities are discovered almost daily, ranging from programming errors to exploiting side effects of speculative program execution in hardware, for example, the *Spectre*

[1] This article was originally published in German in the journal *TATuP– Journal for Technology Assessment in Theory and Practice,* in 2020, a journal issued by KIT-ITAS, Karlsruhe, Germany ("Sichere IT ohne Schwachstellen und Hintertüren", TATuP 1/2020, pp. 30-36, https://tatup.de/index.php/tatup/article/view/6792/11459, https://doi.org/10.14512/tatup.29.1.30. Original submission: Sept. 22., 2019. Peer reviewed. Accepted: Jan. 8., 2020. Distributed under the terms of the Creative Commons Attribution License CCBY 4.0 (https://creativecommons.org/licenses/by/4.0/).
The paper originates from the Quattro-S initiative (Security, Safety, Sovereignty, Social Product) set up by the authors in 2016. The version at hand has been improved slightly, and some illustrations and references were added.

Since 2021, co-authors Steffen Reith, Jean-Pierre Seifert and Arnd Weber have been working in a research project aiming at producing an open hardware security module, using an open, partially formally verified processor, as well as open means against side-channel attacks and an open EDA tool chain (project HEP, funded by the German Federal Ministry of Education and Research, http://hep-alliance.org/). The editorial work for producing the paper at hand has partially been supported by HEP and by the University of New South Wales.

† Deceased in 2022

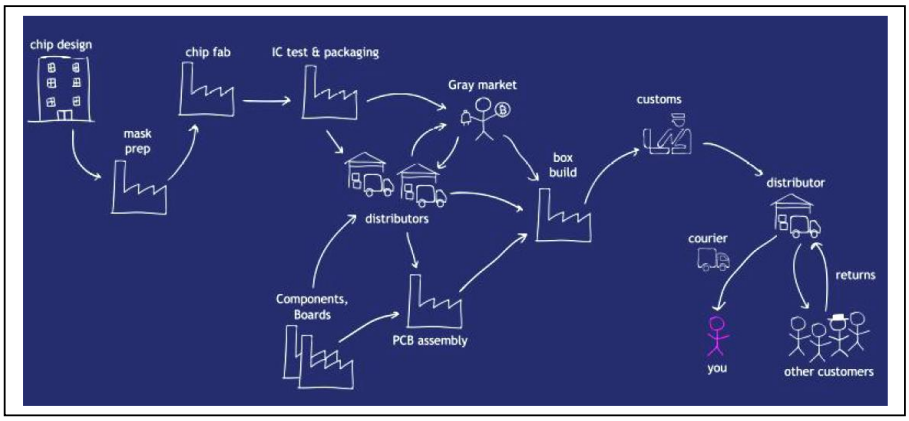

Fig. 1. Attack surface. *Source: Bunnie (2019).*

and *Meltdown* weaknesses. Development tools may contain Trojans that inject vulnerabilities (Thompson 1984). The production of most computer components is currently conducted in a complex worldwide division of labor. Many implementation details are impenetrable even to large industrial customers. This applies to integrated complex software modules as well as to individual hardware components resulting in a wide range of attack possibilities (Weber et al., 2018a).

Given our dependence on digital systems and established presence of malicious actors in cyberspace, risk-management methods and incremental updates (Odlyzko 2019) seem highly inadequate for addressing severe security breaches. Information technology needs a more fundamental transformation to significantly improve security, while taking into account the increasing concentration of competencies and value creation worldwide (Müller-Quade et al., 2017).

Addendum of October, 2022: Since publication of this article the COVID-19 pandemic happened, which has triggered supply-chain issues and that encouraged local sourcing. An increased use of open specifications would reduce dependency on individual suppliers.

DEVELOPMENT OPTIONS

The complete prevention of vulnerabilities in hardware and software is generally regarded as infeasible. It is argued that software and hardware are too complicated, formally verified solutions are expensive and inflexible, and that 100% security is not achievable. While there is support for such assessments from an empirical and historical perspective, it remains a research task to assess the premises of these arguments, to challenge them, and to search for feasible approaches. Conventional approaches, such as more extensive testing and patching have proven insufficient (Weber et al. 2018a). Gradual improvements, such as updates or additional system layers, can only gradually vulnerabilities and are a poor match to attacks by well-financed actors. Introducing additional monitoring components also offers limited protection as these can themselves be exploited for attacks, especially if they have been developed with compromised tools.

There is a current debate in the European Union on whether IT security can be improved by regulating hardware and software, for example, by requiring certification in accordance with the *Common Criteria* or the 2019 EU *Cybersecurity Act.* In practice, such certifications provide very limited protection, as they focus on development processes and testing and are thus unable to establish security.

Fig. 2. Computers compromised by the U.S. National Security Agency (NSA), by 2013. Each dot represents >500 devices. Whistleblower Edward Snowden published that machines from HP, Dell, and Cisco were compromised, and the companies Belgacom and Gemalto were hacked (Appelbaum 2013). *Source of image: Adapted from Snowden (2013).*

Fig. 3. NSA employees opening a Cisco parcel (above) and a load-station for implanting a beacon (below). *Source: Snowden-documents, Leaksource 2013.*

Even if all certified software components were proved secure, the remains the risk of hardware weaknesses, for example, by compromising the design or production process. Verification of hardware is difficult, as manufacturers keep design secret to hide potential weaknesses, or due to process requirements. This lack of transparency tends to reduce security because critical components cannot be independently verified (Saltzer and Schroeder 1975; Eurosmart 2014). In particular, customers cannot evaluate the security of a product themselves. On top, demanding higher certification levels is very costly.

Attempts to produce critical systems domestically and thus ensure the control of a national IT production are more ambitious. China, for example, has the political power to control the entire value chain. Complete autonomy is difficult to achieve in IT systems though. As soon as manufacturers produce for the global market and source components from other suppliers, design flaws or deliberately inserted backdoors can impact IT systems.

OPEN, VERIFIED SUPPLY CHAINS

We propose an approach that combines open production, verified hard- and software, and secure supply chains. Specifically, we suggest implementing open production practices across the entire supply chain, encompassing inputs and tools as well as the products themselves. To do this, we first need to answer a critical question: How can weaknesses and backdoors be eliminated? We furthermore need to ask how the approach could be financed and reconciled with private-sector amortization of development expenses for new products.

A. Openness

From a security perspective, open systems have some fundamental advantages over confidential systems. For example, the U.S. Department of Defense states, in a call for proposals for cybersecurity projects: "Current commodity computer hardware and software are proprietary. A thorough security review cannot be performed on systems with undisclosed components." (SBIR 2018) Two open system examples are the Linux OS and the Linux-based Android. Both have successfully established themselves on the market. The hardware sector seems to develop similarly: the *RISC-V* processor design is an open processor architecture, developed at UC Berkeley with funding from the Defense Advanced Research Projects Agency (DARPA) and in cooperation with industry partners. It makes the development of open implementations and supply chains easier.

Note that open source on its own does not ensure absence of errors, as evidenced by the previously mentioned *Heartbleed* bug. It was rooted in an implementation error in open-source code that remained undiscovered for years. However, openness enables independent inspection and analysis.

B. Formal Verification

While more intensive and independent testing would significantly improve the security of open-source components, testing alone, however, can never rule out the possibility of undetected errors. However, specifications and designs can be improved, for example, by more thorough use of automatic static and dynamic program analysis (Kiss et al., 2015).

The only approach that can completely rule out faults is mathematical proof. For operating systems this was pioneered by *seL4*, a member of the *L4* family of operating system microkernels (Klein et al. 2014, cf. Fig. 4).

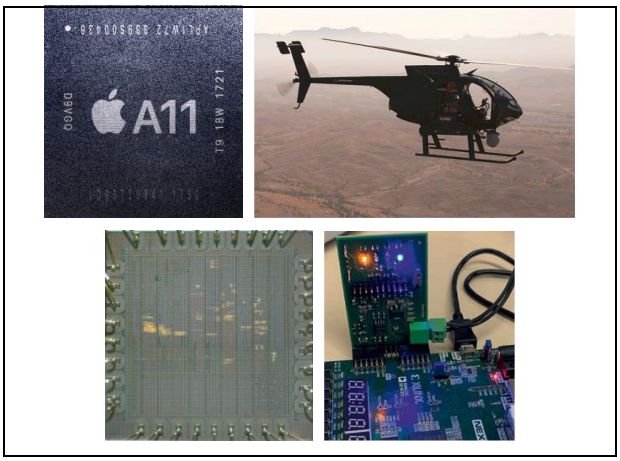

Fig. 4. Examples of new approaches applied in research, prototypes, and products. Clockwise: 1) Apple A11 chip with Secure Element, using the L4 operating system kernel; 2) Unmanned Boeing helicopter using the open and proved-correct seL4; 3) Security module using the open LEON SPARC v8 processor; 4) Prototype of an open security module using the open VexRiscv processor, with a hardware accelerator for ChaCha stream encryption, created exclusively with open design tools (running on an FPGA chip). *Sources: Wikipedia 2020, Data61 2020, Secure-IC 2020, Schultz/Reith 2020.*

Triggered by the floating-point division error in Intel Pentium processors in 1994, formal verification of parts of CPU designs has been standard for decades. Corresponding efforts exist to verify complete *RISC-V* processors (Chlipala 2017, Erbsen et al. 2021). However, the underlying formal specifications and proofs are laborious and usually lose their validity as soon as even minor changes are made to the verified object.

Research is thus facing the challenge of developing methods that can verify highly complex systems at low cost. The difficulty of creating correctness proofs for complex processors increases super-linearly with number of transistors and processor cores. It is still unclear whether, given the growing integration density and transistor count of the latest processor generations, it will ever be possible to prove their design at reasonable cost, or whether proof efforts can be radically reduced by fundamental changes in CPU and computer design.

C. Securing the Supply Chain

IT supply chains can be successfully attacked at almost any point – modifying the design and influencing the production process is just as possible as subverting test and validation procedures or replacing system elements during delivery (Fig. 1). It is likely that securing some components, such as operating systems or processors, will lead to other components being attacked, e.g., communication chips or software tools. Consequently, a comprehensive approach would have to secure as much of the supply chain as possible. When it is necessary to use closed, unverified applications, such as traditional operating systems, they should be encapsulated by mechanisms that separate them from the system's trusted parts (Fig. 5). This way a trusted application, even if it is not formally verified, can provably be isolated from potentially malicious applications, unless the hardware is compromised.

A central challenge is securing the production of semiconductors in the production facilities known as *fabs*. These plants require billions of euros in investment and, apart from the USA and Israel, are concentrated in a few Far Eastern countries. A strategy to better secure chip production can make use of the following options:

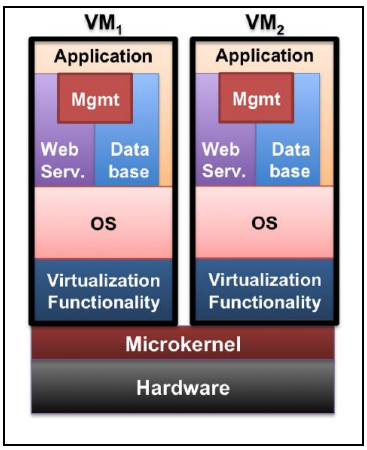

Fig. 5. Splitting virtualization functionality into a microkernel and per-VM component reduces the attack surface. *Source: Heiser (2013)*

- Local manufacturing by operators and employees that are considered trustworthy (*trusted fab*), possibly limited to a set of critical steps at the end of manufacturing (Sengupta et al., 2019).
- Chip control using mathematical methods, such as obfuscation (Šišejković et al. 2019) or additional circuitry (Seifert and Bayer 2015).
- Random chip inspections through optical inspection. From a practical point of view, this works best for simple chips with comparatively large structures that can be produced by enthusiasts from the open-source environment, as envisaged by the *Libre Silicon* project (Libre Silicon 2020).

Some of the options mentioned have yet to be developed and tested. The same applies to approaches for securing software tools used to manufacture hardware or software. The three main options to be investigated are:

- create an open system of tools and minimize the risk of vulnerabilities or backdoors through comprehensive auditing;
- formally verify the output of an open tool;
- compare the output of proprietary tools with open ones for functional equivalence.

Of course, the test environment's integrity must be ensured in all cases, which may only be possible in the long run. For the sake of completeness, it should be noted that mathematics can help to ensure the authenticity of chips, for example, by using physically unclonable functions that exploit physical implementation characteristics (Bruneau et al., 2019).

D. Costs

An essential factor in adopting an open approach is affordability. At present, the proposed formal procedures are often not considered due to their cost. For example, the open-source community is rarely using tools for formal specification or verification, because the tools are considered too expensive, and formal methods limit flexibility in further development. Thus, there is a need for research and action to make formal proofs easier and less costly to perform.

Unit costs for formally verified, open components could be reduced by achieving larger lot sizes, spreading development costs globally across several countries and corporate research budgets – following the example of U.S. companies' cooperation with DARPA – and by having lower licensing costs than for proprietary tools. Formally verified systems also result in lower costs for security measures and damage repair. Besides, such components could provide a competitive advantage and meet regulatory requirements more easily because of their high quality (although at present, certification schemes lag the state of the art and generally do not accept superior mathematical proofs as an alternative to inherently incomplete testing and process requirements). Due to the large number of variables, it is presently difficult to provide a reliable cost estimate for such transition processes.

E. State of the Transition to Open and Verified Systems

A strategic initiative for open, formally verified components and systems could build on a range of preliminary work that has, for quite some time, been funded by DARPA and others. Given the growing dependence of the U.S. IT economy on international IT suppliers, the agency concluded as early as 2017: "The open-source community needs to develop a complete infrastructure" (Salmon 2017, p. 9). In the meantime, industry in the United States, Asia, and Europe has also begun to engage more with this challenge; for example, by developing high-performance multicore CPUs based on *RISC-V* or, on the software side, using the verified microkernel operating system seL4 (Golem 2019, EENewsEurope 2019, Hartpunkt 2018).

Through these initiatives, public and private money is already being invested in open, sometimes even proof-based architectures, for example, for graphic cards (Nvidia; Weber et al. 2018a), storage media (Western Digital 2019), or embedded systems (Hensoldt Cyber 2020). As the Linux/Android case showed, successful open systems can broaden their application domains to other areas, leading to increased return on investment. Similarly, formally verified solutions could migrate from security-critical applications, such as aviation, defense, and IT security modules, to other areas.[2]

ENABLING THE GLOBAL IMPLEMENTATION OF OPEN VERIFICATION

In terms of constructive technology assessment (Schot 1992), risks for the German, European, and ultimately global area can only be substantially reduced if mechanisms are developed that demonstrably reduce the number of vulnerabilities, errors, and backdoors, ideally to zero: *secure IT* instead of *"IT security"*. A number of technical foundations for the development of open, verified systems have already been laid. However, considerable investment is needed to expand this approach systematically. There is a need for research and industrial policy programs on how complete value chains of IT systems can be designed and disseminated openly and securely. In the United States, DARPA has developed an investment and research plan for this purpose (*Electronic Resurgence Initiative*), which is aimed at the local and secure production of IT components. However, this work is strongly focused on the military sector and involves U.S. manufacturers with classified products and processes. The following program elements are needed for the civilian sector, especially outside the United States:

1. Initiate pilot projects and prototypes that span the entire value chain.
2. Further develop formal verification methods and tools, with the aim of more straightforward applicability, as well as an extension of research on formal analysis to more complex systems.
3. Develop techniques for integrating geographically distributed, independent formal verification teams, espe-

[2] In 2022, Google announced their open, seL4-based KataOS, aimed at securing Internet-of-Things (IoT) systems.

cially for task distribution, redundancy and merging of results.

4. Investigate techniques for certification that do not rely on the confidentiality of production and verification techniques.
5. Train a sufficient number of professionally qualified personnel.
6. Develop and test methods to control geographically distant fabs and global supply routes.

At the same time, business models must be developed that aim to globally share the initial costs. Similar to the *RISC-V* ecosystem, cost sharing between private and public sponsors would be an obvious approach. Inexpensive, verified tools and components could facilitate innovations in many industries and strengthen "sovereignty" in IT. In addition, countries should investigate whether and how political or regulatory measures could efficiently support such a goal. In Germany, for example, the coordination of the described initiative could be kicked-off by two recently established government institutions: the Agency for Innovation in Cybersecurity (Cyberagentur) and the Federal Agency for Disruptive Innovation.

The proposed approach aims to secure the entire production and supply chain and therefore requires coordinated efforts across various work areas. The complexity of such a project will exceed that of the pilot initiatives for establishing European *Cyber Competence Networks*. Their funding envelope is between €10 and €20 million, and we estimate a similar effort will be required for the development of a technical and organizational framework. However, true product development for the civilian sector would require significantly higher expenditures (DARPA budgeted about US$1.5 billion over five years for this purpose; Brown 2018). Implementation would require an extensive public-private partnership program with many players or establishing a national or European "champion" with the mobilization of venture capital, possibly in cooperation with players from other countries.

From a political and economic perspective, parallel and alternative developments at the global level should be observed, and their approaches and risks analyzed further. These include, for example, attempts to establish supply chains on a national level (U.S., China, India) or the development and use of open, but as yet unverified, hardware components by established IT companies.

Acknowledgments

The authors thank the reviewers, Anna Hudert, Gabriele Müller-Datz, Arnaud Saffari, and U.S. and German companies' representatives for suggestions.

About the Authors

Prof. Dr.-Ing. Anupam Chattopadhyay teaches at SCSE, Nanyang Technical University, Singapore. At RWTH Aachen, he worked on chip architectures, on EDA, and on automation of chip specification (RTL).

Prof. Dr.-Ing. Sylvain Guilley is CTO of Secure-IC, France, as well as Professor at Télécom ParisTech, Associate Professor at École Normale Supérieure (ENS), Associate Professor at the Chinese Academy of Sciences, and Editor of standards such as ISO/IEC 20897 (Physically Unclonable Functions).

Prof. Dr. Gernot Heiser is Scientia (distinguished) Professor at UNSW Sydney, where he holds the John Lions Chair of Operating Systems. He was the founder of Open Kernel Labs, whose L4 kernel runs in the Secure Enclave of all iOS devices, and led the design and verification of the seL4 microkernel. He is Chief Scientist (Software) at HENSOLDT Cyber. Heiser is a Fellow of the ACM, the IEEE, the Australian Academy of Technical Sciences (ATSE) and the Royal Society of NSW (RSN).

Michael Kasper leads the Cyber and Information Security group at Fraunhofer Singapore and co-founder of opentrust.ai in Singapore. He is an associate senior researcher at the Fraunhofer Institute for Secure Information Technology (SIT).

Prof. Dr. Christoph Krauß is professor for network security at Darmstadt University of Applied Sciences. Earlier he headed the Cyber-Physical Systems Security department at the Fraunhofer Institute for Secure Information Technology (SIT), Darmstadt.

Philipp S. Krüger is Managing Director of Accenture Security for Germany, Switzerland, Austria, and Russia. He is co-founder of the Digital Hub Cybersecurity, was an advisor to the Ministry of Defense for Cyberspace and Innovation, and is head of the Agile Cyber Deterrence Group of the Institute for Security Policy at Kiel University.

Dirk Kuhlmann was a Senior Researcher at the Fraunhofer Institute for Systems and Innovation Research (ISI), Karlsruhe. From 1995 to 2017, he worked for Hewlett Packard Laboratories in Bristol in the IT security research group, focusing on open-source software.

Prof. Dr. Steffen Reith is Professor of Theoretical Computer Science at RheinMain University of Applied Sciences in Wiesbaden. During his work at Elektrobit Automotive, he developed products with cryptographic functions for use in current automobiles.

Martin Schallbruch is Deputy Director of the Digital Society Institute (DSI) and Senior Researcher at the European School of Management and Technology (ESMT) in Berlin. At the same time, he is a lecturer at the Karlsruhe Institute of Technology. At the German Federal Ministry of the Interior, he was most recently Head of the Department for Information Technology, Digital Society, and Cybersecurity.

Prof. Dr. Jean-Pierre Seifert is Einstein Professor for "Security in Telecommunications" at the TU Berlin and the Telekom Innovation Laboratories. He has conducted research at Infineon, Intel, and Samsung, among others.

Dr. Arnd Weber is an economist and sociologist. Until his retirement, he was a senior researcher at the Institute for Technology Assessment and Systems Analysis at KIT, Karlsruhe, advising the European Commission and the German government. He has done research with Goethe University Frankfurt and NTT, Yokosuka.

References

Adee, Sally (2008): The Hunt for the Kill Switch. http://spectrum.ieee.org/semiconductors/design/the-hunt-for-the-kill-switch

Appelbaum, J. (2013): NSA ANT Catalog. https://www.eff.org/files/2014/01/06/20131230-appelbaum-nsa_ant_catalog.pdf

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

Bloomberg (2021): The Long Hack: How China Exploited a U.S. Tech Supplier https://www.bloomberg.com/features/2021-supermicro/

Brown, Eric (2018): DARPA launches POSH project for open source hardware IP blocks. https://www.linux.com/blog/2018/7/darpa-drops-35-million-posh-open-source-hardware-project

Bruneau, Nicolas; Danger, Jean-Luc; Facon, Adrien; Guilley, Sylvain; Hamaguchi, Soshi; Hori, Yohei et al. (2019): Development of the Unified

Security Requirements of PUFs During the Standardization Process. SecITC 2018, Bucharest, Romania. LNCS 11359: Springer.

Bunnie (Andrew Huang; 2019): Supply Chain Security − If I were a Nation State... BlueHatIL. Tel Aviv, Israel. 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, Leipzig, Germany. https://events.ccc.de/congress/2017/Fahrplan/events/9105.html

Data61 (2020): The HACMS project @ Data61. https://ts.data61.csiro.au/projects/TS/SMACCM/

EENewsEurope (2019): Sixteen core RISC-V processor Xuan Tie 910 | Alibaba. July 25, 2019. https://www.eenewseurope.com/news/sixteen-core-risc-v-processor-xuan-tie-910-alibaba

Erbsen, Andres; Gruetter, Samuel; Choi, Joonwon; Wood, Clark; Chlipala, Adam (2021): Integration Verification Across Software and Hardware for a Simple Embedded System. Proceedings of the 42nd ACM SIGPLAN Conference on Programming Language Design and Implementation (PLDI'21)

Eurosmart (2014): Security IC Platform Protection Profile with Augmentation Packages. https://www.commoncriteriaportal.org/files/ppfiles/pp0084b_pdf.pdf

Golem (2019): Why RISC-V will prevail. https://www.golem.de/news/offene-prozessor-isa-wieso-risc-v-sich-durchsetzen-wird-1910-141978.html

Haaretz (2018): No longer a secret. How Israel destroyed Syria's Nuclear Reactor. https://www.haaretz.com/world-news/MAGAZINE-no-longer-a-secret-how-israel-destroyed-syria-s-nuclear-reactor-1.5914407

Heiser, Gernot (2013): Protecting eGovernment Against Attacks, Sydney (White Paper). https://www.itas.kit.edu/downloads/projekt/projekt_webe12_cosiso_heiser_paper.pdf

Hartpunkt (2018): Hensoldt partners with CSIRO's Data61. https://www.hartpunkt.de/hensoldt-kooperiert-mit-csiros-data61/

HENSOLDT Cyber (2020): HENSOLDT Cyber presents MiG-V, the first RISC-V Processor „Made in Germany" for Security Applications. May 10, 2020. https://hensoldt-cyber.com/wp-content/uploads/2020/05/20200515-HENSOLDT-Cyber-PM-MiG-V-is-ready-1.pdf

Kiss, Balázs; Kosmatov, Nikolai; Pariente, Dillon; Puccetti, Armand (2015): Combining Static and Dynamic Analyses for Vulnerability Detection. Illustration on Heartbleed: Haifa Verification Conference, Israel. 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. In: ACM Transactions on Computer Systems, 32, (1), 2:1-2:70.

Leaksource (2013): NSA TAO Supply Chain Interdiction. https://leaksource.files.wordpress.com/2013/12/nsa-tao-supply-chain-interdiction.jpg

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

Libre Silicon (2020): (website). https://libresilicon.com/

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. In: 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, Milpitas, USA. 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. In: Proceedings of the IEEE, 63 (19): 1278-1308.

SBIR - The Small Business Innovation Research Program (2018): Open Source High Assurance System. https://www.sbir.gov/sbirsearch/detail/1508741, last verified November 6, 2019.

Schot, Johan (1992): Constructive Technology Assessment and Technology Dynamics: The Case of Clean Technologies. In: Science, Technology, & Human Values. 17 (1), 36-56

Schultz/Reith (2020): Image by Steffen Reith, personal communication

Secure-IC (2020): Image by Sylvain Guilley, personal communication

Seifert, Jean-Pierre; Bayer, Christoph (2015): Trojan-Resilient Circuits. In: Pathan, Al-Sakib Khan (Hrsg.): Securing Cyber-Physical Systems. Boca Raton: CRC Press, 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. Proceedings des ACM Great Lakes Symposium on VLSI, Tysons Corner, USA: 27-32.

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

Thompson, Ken: Reflections on trusting trust. Communications of the ACM. Volume 27 Issue 8, Aug 1984. 761-763

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, Singapore, Darmstadt, Berlin: KIT-ITAS, HS RheinMain, Fraunhofer Singapore/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/

Western Digital: RISC-V SweRV Core Available to Open Source Community. April 11, 2019. https://blog.westerndigital.com/risc-v-swerv-core-open-source/

Wikipedia (2020): Apple A11 Bionic. https://de.wikipedia.org/wiki/Apple_A11_Bionic