Verified Value Chains, Innovation and Competition

Paper accepted for presentation at the

2023 IEEE International Conference on Cyber Security and Resilience (CSR)

Venice, July 31 – August 2

https://www.ieee-csr.org/

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

Marc Stöttinger
RheinMain University of Applied Sciences
Wiesbaden, Germany
Marc.Stoettinger@hs-rm.de

Maja Malenko
Hensoldt Cyber
Taufkirchen, Germany
Maja.Malenko@hensoldt.net

Armand Puccetti
CEA-List
Gif sur Yvette, France
armand.puccetti@cea.fr

Hagen Sankowski
LibreSilicon
Berlin, Germany
hsank@nospam.chipforge.org

Sylvain Guilley
Télécom Paris, Institut Polytechnique de Paris
and
Secure-IC S.A.S.
Paris, France
sylvain.guilley@telecom-paristech.fr

Torsten Grawunder
Swissbit Germany
Berlin, Germany
torsten.grawunder@swissbit.com

Jean-Pierre Seifert
TU Berlin
Berlin, Germany
jean-pierre.seifert@tu-berlin.de

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

René Rathfelder
IAV
Berlin, Germany
rene.rathfelder@iav.de

Christoph Lüth
DFKI
Bremen, Germany
christoph.lueth@dfki.de

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

Norbert Herfurth
IHP - Leibniz-Institut für innovative Mikroelektronik
Frankfurt/Oder, Germany
herfurth@ihp-microelectronics.com

This paper has partially been supported by the German Federal Ministry of Education and Research.

978-1-6654-9952-1/22/$31.00 ©2023 IEEE

***Abstract*— The paper addresses three issues: The first one is vulnerabilities in IT systems, the second is significant market power in hardware production, and the third is sovereignty of nations and manufacturers regarding their IT input. The paper reviews some recent developments towards open verifiable components, such as for open processors, hardware security modules, operating systems, and semiconductor production systems. These developments provide opportunities for new products. Even manufacturers in non-leading countries might be empowered to produce hard-to-attack products. Currently pending IT security regulation will not achieve such a level of security by itself. Open and better verified, ultimately provably secure components will foster more sovereignty. Technical limits and costs of the approaches are discussed. It is concluded that fighting vulnerabilities and providing space for new products and jobs justify further privately and publicly supported research.**

Keywords: cybersecurity, open-source, transparency, sovereignty, verification, supply chain, competition, regulation

Reference to this paper: For quotation with page numbers, please refer to the final version to be made available by the IEEE. For other references to the paper, please use:

Weber, Arnd; Guilley, Sylvain; Rathfelder, René; Stöttinger, Marc; Grawunder, Torsten; Lüth, Christoph; Malenko, Maja; Reith, Steffen; Puccetti, Armand; Seifert, Jean-Pierre; Herfurth, Norbert; Heiser, Gernot; Sankowski, Hagen: Verified Value Chains, Innovation and Competition. Paper to be presented at 2023 IEEE International Conference on Cyber Security and Resilience (CSR), Venice, July 31 – August 2. https://www.ieee-csr.org/

I. CHALLENGES

A. Lack of Security

Society's dependence on information technology leads to heavy demands on this technology's secure and robust operation. Contemporary IT systems do not fully meet these requirements. As a result, infrastructure may fail, company secrets may be stolen, cars may be remotely controlled by attackers, financial losses may be caused, and political institutions may be spied on (note: this subsection is partially based on [1]).

Design flaws, and vulnerabilities in hardware and software implementation are drivers of the aforementioned attacks. They may result from flaws in the application software, such as the Log4j vulnerability, or a lack of suitable security update procedures in IoT-devices (e.g., Mirai; cf. [2]). Frequent causes are weaknesses in operating systems, such as the Heartbleed OpenSSL bug, and the flaws exploited by the WannaCry ransomware – in the latter case the weaknesses were actually known to intelligence agencies, who kept them to themselves, knowingly exposing critical systems. Mainstream operating systems fail to reliably isolate non-trustworthy code, as demonstrated by attacks on security company RSA [3], and more recently on Continental [4].

New types of attacks arise from hardware Trojans [5], whose existence has already been suspected in electronic semiconductor devices, e.g., FPGA chips and military radar systems in Syria [6, 7, 8], and are examples of attacks on IT supply chains [9, 10].

Edward Snowden revealed that thousands of computers were compromised by the U.S. National Security Agency, including machines from HP, Dell, and Cisco, and even telcos and security companies, such as Belgacom and Gemalto were hacked [11, 12, 13]. Ever since these disclosures it must be assumed that national intelligence services are deliberately creating or hoarding vulnerabilities. Moreover, they may insert back doors in cryptographic implementations [14]. This does not only apply to U.S. intelligence services; Russia is also highly active in cyberspace as is China and others. More than two decades ago, officers of the Chinese People's Liberation Army proposed implementing "logic bombs" for computer networks ([15], cf. zero-days used with Aurora [16]). 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 exploitation of side effects of speculative program execution in hardware (the Spectre and Meltdown exploits). Furthermore, development tools may contain Trojans that inject vulnerabilities [17]. The production of most computer components is currently conducted in a complex worldwide division of labor, which eases injection of Trojans. In general, hardware and software implementations are too complex to analyze even for large industrial customers, resulting in a huge attack surface.

Despite much research, practical computer security has not significantly improved in recent years, as indicated by the statistics of known computer vulnerabilities and exposures, which topped 25,000 in 2022 [18]. Google alone puts out hundreds of security updates every week [19].

Why is IT security in such a precarious state? One reason is that security has a social as well as a technical dimension. Security is a process [20], and without involvement of the user no system can be secure. However, even technical security is a hard problem. Firstly, absolute security is not achievable, it can only be analyzed with respect to assumed capabilities of a potential attacker, the *threat model*; this may be incomplete. Secondly, security is not what is called *compositional*; if we combine two secure systems, the resulting system may be insecure. This means that it is not sufficient to establish security of every part, we have to analyze the whole system. But even security analysis of components is not possible if their implementation details are inaccessible, so open development and open-source help to increase technical security.

B. Supply-Chain Security

Threats to supply chains have recently received mainstream attention, for instance disruptions due to the COVID-19 pandemic, and export regulations blocking the export of ASML machines or the import of Huawei devices. Political tensions affecting countries with large production capabilities, such as Taiwan, create further threats. Supply chains consisting of single providers of closed components thus do not provide sovereignty over system designs. The problems result in encouragement of local production, which reduces economies of scale.

C. Innovation and competency

The third threat arises from market concentration in IT production. While efficient markets reward superior competitors with increased market share, we now have oligopolies or even near-monopolies with Google, Apple etc. or the Big Three in EDA (Cadence, Synopsys, Mentor/Siemens). As a result, countries outside the oligopoly will strive to regain transparency of what they purchase and rebuild competency to compete. Countries/regions suffering from oligopolistic pricing (e.g., Europe in mobile communications [21]) could try to counter-act. Other players, e.g., India and China, simply want a share of the value and

jobs, so are developing competency in hard- and software design, in particular ASICs. The Indian government, for example, has launched the Digital India RISC-V (DIR-V) program for the development of next generation RISC-V based silicon.

II. Potential Solutions

Markets and public policies have failed to solve security threats. The European Commission, based on a study by Bitcom [22], estimates that EU-wide damages resulting from security violations amount to at least €180 billion annually [23].

As there are no easy solutions, we need to examine approaches aimed at limiting damage and improving security in the long term. Given the market failure, they must include policy actions. Examples of current proposals are:

1. Legislation, as in Singapore [24], in Europe with the draft Cyber Resilience Act [25] and the draft Product Liability Directive [26] or in the U.S. the National Cybersecurity Strategy [27].
2. Suitable publicly funded research, e.g., as with the U.S. Open Technology Fund [28].
3. Public support of openness and security education.
4. Increasing requirements on software and hardware security in government procurement [29, 30].

Technical steps, whether taken voluntarily or required by regulation, include:

1. Openness as a prerequisite to check the security of a component, as explained above.
2. Verification of components, e.g., better scrutiny [31], use of automatic static and dynamic program analysis [32], or formal proofs of correctness (as done by Intel, Airbus, Microsoft etc. [30, 1].

We examine these steps in the rest of this section.

A. Free and Open Components and Tools

After the success of open-source software ecosystems, such as Linux and Apache, there have been attempts to create open hardware designs and processes, e.g., RISC-V processors and open process design kits (PDKs) for ASIC production. Some of these developments have been supported by DARPA.

One more example is the CHIPS Alliance, an open and collaborative environment hosted by the Linux Foundation. It comprises several working groups and is supported by major industry and academic partners (e.g., Google, Intel, Microsoft, Alibaba, etc.). The Alliance promotes the development, adoption, and standardization of open-source hardware ecosystems.

Several open-source RISC-V projects for building secure and trustworthy systems have emerged. Sanctum is an open Root of Trust that offers security properties similar to Intel SGX. Keystone is an open framework for creating customizable trusted execution environments (TEEs) on RISC-V; other examples are MultiZone, SiFive's WorldGuard, and the academic TIMBER-V and HECTOR-V [33].

It is interesting to see that Google is developing a large, secured chain of free and open components, with the potential to achieve a high level of process control, security and cost savings. This chain consists of the following:

- KataOS [34], an operating system for IoT systems based on the provably secure seL4 kernel;
- the OpenTitan hardware root of trust system, which delivers hardware IP blocks focused on security, verification, and reuse as well as software that supports the development of secure hardware (although OpenTitan requires the use of several languages, making its code hard to read and reuse);
- the Caliptra initiative aiming at designing a hardware security module (HSM) with an open register transfer level (RTL) design, in cooperation with Microsoft, AMD and others [35]. In early 2023, only draft specifications are available.
- the Skywater fab using Openlane EDA tools to create open GDS II-files (graphical data system);
- the LibreSilicon initiative to produce a cell generator, in co-operation with Google [36].

The latter would increase competition with the current EDA-oligopoly, and ultimately ease changing fabs when using the same mask set. It would also ease later analysis of produced silicon because cell identification will become easier. It would thus improve approaches as developed by degate.org for reverse-engineering of chips, using microscopes.

Also noteworthy is YosysHQ, a company that develops an open-source EDA ecosystem which includes the Yosys synthesis tool, nextpnr place and route tool, SymbiYosys formal verification flow, riscv-formal framework, etc.

There are more initiatives elsewhere. Some with involvement from our partners include:

- Devices running seL4 operating system kernel are in use in multiple defence forces and apparently planned to be used with Boeing Chinooks, too (Collins Aerospace, cf. [37, 38]).
- In the automotive sector, Horizon Robotics and Xcalibyte explore the use of seL4 [39].
- More open PDKs are emerging, as from Global Foundries and IHP (Germany) [40].
- The functional correctness of the award-winning VexRiscv RV32I [41, 42] processor design is currently being formally verified within the German HEP project (*H*ardening the value chain through open-source *E*DA tools and *P*rocessors; cf. http://hep-alliance.org/ and [43, 44]).
- An open tool for masking AES-keys against side-channel attacks has been produced by partners of project HEP. With suitable tools, e.g., with a modification of SpinalHDL providing annotations, it can be checked that synthesis will not eliminate masking [45]. It is planned to formally verify the correctness of the masking scheme. Github addresses of the results of project HEP will be made available at http://hep-alliance.org/.
- The RISC-V design CV32E40S from the *Open Hardware Group* enables complete PMP and IOPMP (physical memory protection) support, along with more advanced security features (such as sensitive CSR register protection).
- MiG-V is HENSOLDT Cyber's logic-encrypted processor targeting high-security applications. It is

based on a CVA6 RISC-V (previously called Ariane) implementation enhanced in performance and security and logically locked against supply chain attacks.

- TIMBER-V is an academic TEE that enhances RISC-V with tagged memory concept for isolated execution of multiple enclaves on embedded platforms.
- In project "Progenitor", a demonstrator of an open VPN-router is being developed, using open tools and components such as VexRiscv, WireGuard and KiCad [46].

B. *Verification and Formal Proof*

Verification is the process of showing that an implementation (hardware or software) satisfies its requirements. It can be in the form of code review, testing, static code analysis, model-checking or formal (mathematical) proof.

Of these, a formal proof offers the best guarantee of correctness, and *in extensio* security, but requires most effort. For realistic systems, complete formal proof of the full system is still out of reach, but formally proved components, such as RISC-V cores [47, 48] or operating system kernels (e.g., seL4) are feasible, publicly available, and offer a substantial increase in confidence.

For example, an operating system with a formally proved compartmentalization property provides a significant increase in security, as attacks against one compartment will not affect others, and hence not compromise the overall security. Of course, this does nothing to secure the software running inside the compartment (e.g., an email client, browser or an insecure operating system), and the system is still susceptible to hardware-based attacks such as transient execution attacks or Trojans. Note also that formal proof generally requires access to the source code.

However, even if complete formal proof is not possible due to the high effort involved, other methods of verification can be applied, such as abstract interpretation analyses [49]. These can detect run-time errors automatically by executing the source code after abstracting away the code's data and control flow.

At the CRE workshop in 2018 we suggested, regarding the production of open components: "When producing new components… reserve a sufficient share of resources for two or even three teams independently conducting validations." ([29], cf. [50]). While similar efforts are meanwhile happening [28], attackers may still place Trojans or find vulnerabilities, so the objective of formally proving components will remain on the agenda.

In an effort to strengthen Germany's digital sovereignty, the German Cyber Agency ("Agentur für Innovation in der Cybersicherheit") conducted studies on the ecosystems of trustworthy IT. By applying formal verification methods for software, hardware, and supply chains, and by creating a cross-sector community for their use, these studies should provide a basis to further research and development of safety-critical systems that must be formally analyzed and verified.

C. *Dynamics of Change*

What are some key causes why all these open and more secure things took place?

(1) Open-source development has frequently been driven by highly trained enthusiasts, professionals, and students. (2) It can reduce efforts for individual participants by sharing development costs ([51], cf. [52]). (3) Support by government organizations was crucial to the development of some core components, such as RISC-V and seL4, e.g., by DARPA and Australia's NICTA. (4) The open-source space is less dominated by U.S. players than that of proprietary solutions, see Yosys and RISC-V processors such ETH's Ariane, Alibaba's C910 or VexRiscv.

Such factors could influence the creation of even more open and secure components, contributing to more sovereignty for less powerful players. Free-loading of some existing components, such as RISC-V designs, is understandable, but will not contribute significantly to more security or innovation.

III. Challenges and Options

A. *Physics of Hardware*

A secure software stack does not help if compromised hardware allows bypassing its protections. However, creating trustworthy hardware is a formidable challenge. Firstly, formal verification of hardware designs is similarly hard as software designs. Secondly, the tools that convert the design into a mask for chip production are confidential and may contain Trojan horses, and insiders may manipulate designs. For ASICs, to our knowledge, no open tools for formally verifying the correctness of GDS or mask data exist. Thirdly, correct (digital) functionality of hardware is based on several levels of abstractions on top of analog features, which can hide Trojans. Furthermore, these abstractions may be leaky, enabling attacks such as Rowhammer, Spectre, Meltdown, and Hertzbleed as discussed above [5, 53, 54, 55]. Competing tools or open tools and fabs could provide choice to industrial customers to vary processes and fabs, as long as both are not formally provable. While on one hand this gives attackers more targets, it makes it harder for them to target specific products. Prices might increase, but removing the EDA oligopoly could counterbalance this.

Another issue is the economics of advanced silicon technologies (e.g., with extreme ultraviolet lithography as used by ASML and TSCM, cf. [56]. While shrinking feature sizes and increased energy efficiency are a result of competition, the increasing cost of fabs able to produce them increase the barrier for new competitors or nation states trying to produce competitive products. However, feature sizes of 16 to 45 nm are still profitable for IoT devices, automobiles etc. [57]. There might be market niches even for 130nm technologies for transparent, verifiable ASICs. Large structures would enable a maker scene to develop innovative products that become economical over time. This may sound overly optimistic, but remember that originally other inventions were also thought to be non-competitive or insignificant, such as the personal computer, Linux, or Internet-enabled mobile phones. A challenge is to use the verification approach for smaller, more energy-efficient and cheaper technologies. To investigate ("degate") smaller cells with microscopes might work for smaller structures as well. The reason for this is that the cells are much larger than the structures, so the former can be identified. Such optical inspection may not be effective if an attacker invents something new. Imagine dopant-level Trojans not being conceived yet [58]. Other means to protect chips designs obfuscate these or prove their correct working [59, 60], but a fab could try to hide small Trojans somewhere around such a protected design, which may or may not be identifiable with a microscope. Therefore, a comprehensive control of the delivered chip would help, if needed on the legal level.

Inherent randomness of low-level hardware characteristics, while making analysis more difficult, enables new security features, e.g., unique chip identity (physically unclonable functions; cf. ISO/IEC 20897 [61]). Such features can protect against physical attacks (the unclonability property implies that the chip key is sensitive to invasive probing) and against malware (the key cannot be modified as it is a physical property of the chip).

B. Public Policies such as Legislation

Legislation is being implemented to reduce the societal costs of attacks. While it may be optimistic to expect a 33 percent reduction due to certification according to the pending European Computer Resilience Act [23], compared to a situation without it, this would be only a little more than the growth of vulnerabilities of up to 20 percent p.a. [18], and leave a large fraction unaddressed. It will therefore not stop criminals from finding new vulnerabilities, nor prevent nation states from injecting Trojans. The European Commission appears to be aware of this, see Fig. 1.

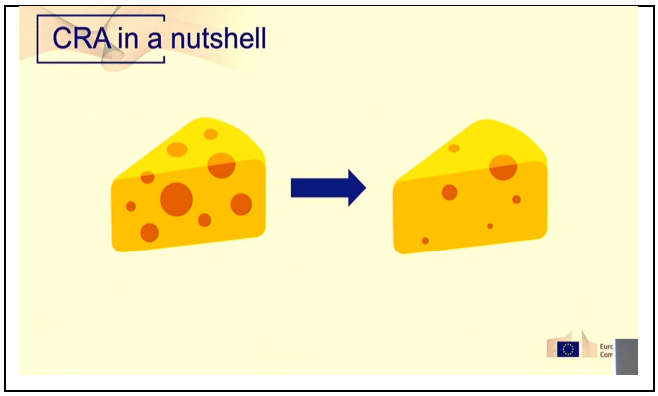

Fig. 1. : The EU draft Cyber Resilience Act, as visualized by an EU Commission representative in a presentation [63]. According to the speaker, the objective of the regulation is to reduce the number of security holes.

To quote the Prime Minister of Estonia [62]:

Question by Alexander Martin, The Record: Do you think that cyber-attacks will lessen, with increased resilience? Answer by Kaja Kallas: I don't think they will. They have been increasing because this is the way where you can hurt the society.

Therefore, legislation may need to be sharpened, by, e.g.:

- Require addressing entire value chains, for example, for critical infrastructures or armed forces, in order to have more resilient products permanently available, and "entire value chain" includes any sort of tools (for building hard- and software), fabs, knowledge of semiconductor physics, etc., with explicit containment of scope for attacks by nation states.
- Improve dealing with untrustworthy code (e.g., make it mandatory to run only in separate compartments, possibly with a common user interface).
- Require openness of designs. If certification is required, as planned in the EU, there are concerns among open-source proponents that the increased compliance burden may have the unintended effect of discouraging open-source development [25, 64, 65, 66]. It has been suggested to allow open-source components to be certified by peers (cf. [67]); peers might be able to judge formal proofs. In contrast, the U.S. National Cybersecurity Strategy [27] aims at limiting liability for programmers, while providing support for improving the security of hundreds of open components [28].
- Support of validation of code by independent groups.
- Support of formal proofs or other improved forms of verification, for selected components and for entire value chains. This would foster IT components that are secure in a strong sense, instead of traditional, reactive approaches to "IT security".
- Increase liability for components, including for unknown vulnerabilities and Trojans. This would go further than the emerging EU draft liability directive. While it will be difficult and costly to implement, and take time, it would contribute to achieving more secure IT.

Several countries or regions could implement complete verified, relatively vulnerability-free value chain components including trustworthy fabs; to finance this:

- Nations could create a suitable steering group to develop schemes for cost-sharing.
- The use of certification procedures should be coordinated. If, e.g., Common Criteria evalutions are to be applied, Protection Profiles [68] should be applicable across borders. More simple forms might be more efficient, such as from ISO 27,000 or CENELEC EN 17640 FiT CEM [69].

C. Securing Value Chains without Government Intervention

Industry may move by its own motivations, as with RISC-V, Caliptra and the projects supported by Google and others; this could be the beginning of a new trend. Especially for defense and critical infrastructure, open implementations and stronger verification are advantageous. Following initiatives by DARPA and Google, the emergence of thoroughly verified, free-to-use open hard- and software components is conceivable. Realizing this vision will require other nations and companies to participate by contributing designs and verified components. Open specifications will help by reducing dependency on individual suppliers. Attractive next steps, could be:

- Open HSMs, complying with an open specification, including specific random-number generator, core algorithms, methods for tamper resistance, open RTL- or GDS II-files, open non-volatile memory, etc.
- Cell libraries for feature sizes smaller than 180/130nm that can be handled by multiple fabs.
- Open process flows for mask generation. A tape-out-ready GDS layout file requires significant processing to obtain single-layer GDS files that can be handed to the mask shop, especially for multi-project wafer (MPW) runs. While these processes are mostly automated or at least semi-automated, and open-source tools like Klayout can go a long way, they are not yet powerful enough for a complete mask generation process. Furthermore, the fab-specific mask generation scripts as well as optical proximity correction (OPC) rules are mostly proprietary and confidential.
- A complete, formally verified operating system.
- Automatic generation of proofs for operating system components.

- Redesign office suites to force unknown code to run in a confined environment, analyzable by administrators [70, 71].

Applying such steps to entire value chains, one by one, would foster security and sovereignty, and could be performed with global distribution of work and costs. It would increase related education and encourage innovation.

IV. Conclusions

Certification is a hotly discussed topic. While more widespread use may mitigate some security problems, on its own it will not solve the security problem. The massive economic and strategic interests of advanced persistent treats (organized crime and state actors) imply that large resources will continue to be committed to finding and exploiting vulnerabilities. As only formal verification of components has a chance to categorically rule out vulnerabilities, comprehensive verification must remain a priority, across research, education, regulation, and procurement.

However, attackers may then aim at attacking steps of the value chain which cannot be formally verified, such as parts of chips outside the protected part, imagine dopant-level Trojans had not yet been thought of. The verification process might be attacked, too, think of compromising the tools used for it through a malicious update or of bribing the verifiers. Crypto algorithms could be compromised [14]. So, we cannot promise 100 percent security. But we outlined a path which has the potential to reduce attacks by orders of magnitudes.

At the same time, the path, due to the transparency, would allow for the participation of many more designers, companies and countries than a market migrating towards oligopolies.

Towards that vision remain some important steps: Independent validation of security remains important for components or products that have not been formally verified.

Open-source is an important enabler for independent validation, and can help to share verification cost; it is important that emerging regulation does not undermine open-source development. Legislation in regions important for open source developments, such as the US and the EU, should treat them with essentially the same rules. Reducing the cost of certification regimes is of critical importance, options include certification by peers and streamlining certification of formally proved components.

Finally, it is important to broaden understanding of verification and security challenges at the hardware (down to semiconductor physics) as well as the software level, among experts, university students and the interested, and concerned public.

Acknowledgments

The authors are grateful to the following persons: Fabian Buschkowski, Milan Funck, Arnaud Saffari, an anonymous reader and the reviewers.

References

[1] Weber, Arnd; Heiser, Gernot; Kuhlmann, Dirk; Schallbruch, Martin; Chattopadhyay, Anupam; Guilley, Sylvain; Kasper, Michael; Krauß, Christoph; Krüger, Philipp S.; Reith, Steffen; Seifert, Jean-Pierre: Secure IT without Vulnerabilities and Backdoors. Karlsruhe: Karlsruhe Institute of Technology, 2022. https://publikationen.bibliothek.kit.edu/1000153445 DOI: 10.5445/IR/1000153445; English version of: Sichere IT ohne Schwachstellen und Hintertüren. TATuP – Zeitschrift für Technikfolgenabschätzung in Theorie und Praxis 1/2020, 30-36. https://tatup.de/index.php/tatup/article/view/6792/11459

[2] Arbor Networks: Mirai IoT Botnet Description and DDoS Attack Mitigation. Oct. 26, 2016. https://www.netscout.com/blog/asert/mirai-iot-botnet-description-and-ddos-attack-mitigation

[3] Wired, May 28, 2021: https://www.wired.com/story/the-full-story-of-the-stunning-rsa-hack-can-finally-be-told/

[4] Continental, Dec. 12, 2022: https://www.continental.com/de/presse/studien-publikationen/sonstige-publikationen/cyber-angriff-fragen-und-antworten/

[5] 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.

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

[7] 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

[8] Skorobogatov, S.; Woods, Ch.: Breakthrough Silicon Scanning Discovers Back-door in Military Chip, CHES 2012. https://www.cl.cam.ac.uk/~sps32/ches2012-backdoor.pdf

[9] 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

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

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

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

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

[14] Shumow, Dan; Ferguson, Niels: On the Possibility of a Back Door in the NIST SP800-90 Dual Ec Prng. http://rump2007.cr.yp.to/15-shumow.pdf

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

[16] Google: A new approach to China. January 12, 2010. https://googleblog.blogspot.com/2010/01/new-approach-to-china.html

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

[18] CVE Details: Access Feb. 1, 2023, https://www.cvedetails.com/browse-by-date.php

[19] Venables, Phil: Presentation at: Munich Cyber Security Conference 2022. https://it-security-munich.net/mcsc-2022/

[20] Schneier, B.: The Process of Security. 2000. https://www.schneier.com/essays/archives/2000/04/the_process_of_secur.html

[21] Weber, Arnd; Scuka, Daniel: Comment: Operators at crossroads: market protection or innovation? In: "Telecommunications Policy", Volume 40, Issue 4, April 2016, Pages 368–377, doi:10.1016/j.telpol.2015.11.009

[22] Bitcom: Wirtschaftsschutz 2021. https://www.bitkom.org/Presse/Presseinformation/Angriffsziel-deutsche-Wirtschaft-mehr-als-220-Milliarden-Euro-Schaden-pro-Jahr#_

[23] European Commission 2022: Commission Staff Working Document. Impact Assessment Report. https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act-impact-assessment

[24] Cyber Security Agency of Singapore: Cybersecurity Certification Guide, 2021. https://www.csa.gov.sg/Programmes/certification-and-labelling-schemes/cybersecurity-labelling-scheme/about-cls

[25] European Commission 2022: Draft Cyber Resilience Act COM(2022) 454 final. https://ec.europa.eu/transparency/documents-register/detail?ref=COM(2022)454&lang=en

[26] European Commission 2022: COM(2022) 495 - Proposal for a directive of the European Parliament and of the Council on liability for defective products. https://single-market-economy.ec.europa.eu/document/3193da9a-cecb-44ad-9a9c-7b6b23220bcd_en

[27] White House (2023): Biden-Harris Administration Announces National Cybersecurity Strategy. March 2, 2023. https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/

[28] Open Technology Fund 2023: https://www.opentech.fund/

[29] Weber, A.; Reith, S.; Kuhlmann, D.; Kasper, M.; Seifert, J.-P.; Krauß, C.: Open Source Value Chains for Addressing Security Issues Efficiently. IEEE Workshop on Cyber Resilience Technologies (CRS-C), Lisbon 2018. 16-20 July 2018. https://ieeexplore.ieee.org/document/8432033/

[30] Peisert, Sean: Unsafe at Any Clock Speed: The Insecurity of Computer System Design, Implementation, and Operation. Security &Privacy 2022. https://ieeexplore.ieee.org/document/9693402

[31] OpenSSF: OSS Mobilization Plank 2022. https://openssf.org/oss-security-mobilization-plan/

[32] 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

[33] Weiser, Samuel; Werner, Mario; Brasser, Ferdinand; Malenko, Maja; Mangard, Stefan; Sadeghi, Ahmad-Reza: TIMBER-V: Tag-Isolated Memory Bringing Fine-grained Enclaves to RISC-V. Network and Distributed System Security Symposium (NDSS). 2019.

[34] Google: KataOS. https://opensource.googleblog.com/2022/10/announcing-kataos-and-sparrow.html

[35] Kelly, Brian et al.: Caliptra A Datacenter System on a Chip (SOC) Root of Trust (RoT). https://www.opencompute.org/documents/caliptra-silicon-rot-services-09012022-pdf

[36] Sankowski, Hagen: LibreSilicon (2022): https://github.com/chipforge/LibreSilicon-Slide-Desk/blob/master/LSA-20221207.pdf

[37] D. Cofer *et al*., "Cyberassured Systems Engineering at Scale," in *IEEE Security & Privacy*, vol. 20, no. 3, pp. 52-64, May-June 2022.

[38] seL4 Summit 2022, https://sel4.systems/Foundation/Summit/home.pml

[39] CnNVPost: Horizon Robotics launches Journey 5 chip with 128 TOPS of AI computing power. July 30, 2021. https://cnevpost.com/2021/07/30/horizon-robotics-launches-journey-5-chip-with-128-tops-of-ai-computing-power/

[40] Vater, Frank: OpenSource PDK - A key enabler to unlock the potential of an open source design flow. FSiC 2022. https://wiki.f-si.org/index.php/FSiC2022

[41] Kalnoskas, Aimee: RISC-V SoftCPU contest winners announced. 2018: https://www.microcontrollertips.com/risc-v-softcpu-contest-winners-announced/

[42] Verbeure, Tom: The VexRiscV CPU - A New Way to Design. Dec 6, 2018. https://tomverbeure.github.io/rtl/2018/12/06/The-VexRiscV-CPU-A-New-Way-To-Design.html

[43] Henkes, Tim; Herfurth, Norbert; Lüth, Christoph; Reith, Steffen: VE-HEP. Trustworthy Open-Source Hardware. Presentation at RISC-V Workshop Berlin Nov. 11, 2022

[44] Böhner, Martin; Buschkowski, Fabian; Funck, Milan; Henkes, Tim; Herdt, Vladimir; Herfurth, Norbert; Kiyan, Tuba; Lahr, Norman; Lüth, Christoph; Rathfelder, René; Reith, Steffen; Sasdrich, Pascal; Ulbricht, Markus; Wälde, Julian; Weber, Arnd: Requirements Analysis for an HSM, EDA Tools and a Demonstrator Setup. Project HEP, 2021, http://hep-alliance.org/

[45] Buschkowski, Fabian; Sasdrich, Pascal; Güneysu, Tim: Easimask – Towards Efficient, Automated, and Secure Implementation of Masking

in Hardware. Date 2023, April 19, 2023. https://www.date-conference.com/programme

[46] HSRM: Progenitor. 2023: https://www.hs-rm.de/de/fachbereiche/design-informatik-medien/forschung/progenitor

[47] Choi, Joonwon, Muralidaran Vijayaraghavan, Benjamin Sherman, Adam Chlipala, and Arvind. 'Kami: A Platform for High-Level Parametric Hardware Specification and Its Modular Verification'. Proceedings of the ACM on Programming Languages 1, no. ICFP (29 August 2017): 24:1-24:30. https://doi.org/10.1145/3110268.

[48] Gao, Dapeng, and Tom Melham. 'End-to-End Formal Verification of a RISC-V Processor Extended with Capability Pointers', 24–33. TU Wien Academic Press., 2021. https://doi.org/10.34727/2021/isbn.978-3-85448-046-4_10.

[49] Cousot P., Cousot R.: Abstract Interpretation: a unified lattice model for static analysis of programs by construction or approximation of fixpoints. Conference records of the Fourth Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages, 238-252, LA, California, 1977. ACM Press New York, USA.

[50] Brewer, Eric: The Consequences of Success. OSS is Critical Infrastructure. Keynote OSSNA 2022. https://docs.google.com/presentation/d/18hkLb6CIC49tBFp2nX4prbhKaUiHj_cfXPN95zg4dS0/edit#slide=id.g11c4b3a52ba_0_315

[51] Sijstermans, F.: RISC-V at NVIDIA. 6th RISC-V Workshop, Shanghai, May 2017. https://www.youtube.com/watch?v=g6Z_5l69keI

[52] Reith, Steffen: New Directions of Hardware Based Cryptographic Modules for Modern Cars. Presentation given at IT Security for Vehicles. Düsseldorf 2016

[53] Kocher, P.; Genkin, D.; Gruss, D.; Haas, W.; Hamburg, M.; Lipp, M.; Mangard, S.; Prescher, T.; Schwarz, M.; Yarom, Y.: Spectre Attacks: Exploiting Speculative Execution. 2018. https://spectreattack.com/spectre.pdf

[54] Lipp, M.; Schwarz, M.; Gruss, D.; Prescher, T.; Haas, W.; Mangard, S.; Kocher, P.; Genkin, G.; Yarom, Y.; Hamburg, M.: Meltdown. 2018. https://meltdownattack.com/meltdown.pdf

[55] Wang, Yingchen; Riccardo Paccagnella; Elizabeth Tang He; Hovav Shacham; Christopher W. Fletcher; David Kohlbrenner: Hertzbleed: Turning Power Side-Channel Attacks Into Remote Timing Attacks on x86. 2022. https://www.usenix.org/conference/usenixsecurity22/presentation/wang-yingchen

[56] van den Brink, Martin: Technology Strategy to Drive Moore's Law into Next Decade. https://www.asml.com/-/media/asml/files/investors/investor-days/2021/asml-investor-day-2021-technology-strategy---martin-van-den-brink.pdf

[57] Heise: Verbände: EU muss Chip-Produktion jenseits von Prestigeprojekten ankurbeln. Nov. 5, 2021. https://www.heise.de/news/Verbaende-EU-muss-Chip-Produktion-jenseits-von-Prestigeprojekten-ankurbeln-6253985.html

[58] 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.

[59] Šišejković, D.; Merchant, F.; Leupers, R.; Ascheid, G.; Kegreiss, S.: Control-Lock: Securing Processor Cores Against Software-Controlled Hardware Trojans. ACM Great Lakes Symposium on VLSI 2019. https://dl.acm.org/citation.cfm?doid=3299874.3317983

[60] Seifert, J.-P.; Bayer, C.: Trojan-Resilient Circuits. In: Pathan, A. (ed.): Securing Cyber-Physical Systems, Boca Raton 2015

[61] 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.

[62] Kallas, Kaja: Feb. 19, 2023. Comments at MCSC. https://www.youtube.com/watch?v=c3ccEvrlA1k&list=PL9bgz5uwrSA20i7pK5lWYMijyC4wcXXi5&index=1

[63] Bögel, Benjamin: Cyber Resilience Act. Presentation at FOSDEM, Feb. 4, 2023. https://fosdem.org/2023/schedule/event/cyber_resilience/

[64] Aertsen, Maarten: Open-source software vs. the proposed Cyber Resilience Act. 14.11.22 https://blog.nlnetlabs.nl/open-source-software-vs-the-cyber-resilience-act/

[65] Phipps, Simon: The ultimate list of reactions to the CRA. 2023. https://blog.opensource.org/the-ultimate-list-of-reactions-to-the-cyber-resilience-act/

[66] Open Forum Europe: EU Open Source Policy Summit, Feb. 3, 2023. https://summit.openforumeurope.org/

[67] Häuer, Martin: DIN Spec 3105. Access Feb. 1, 2023. https://wiki.opensourceecology.org/wiki/DIN_SPEC_3105

[68] Common Criteria Protection Profiles (2023): https://www.commoncriteriaportal.org/pps/

[69] CENELEC: New EN 17640 'Fixed-time cybersecurity evaluation methodology for ICT products' helps evaluate the cybersecurity of ICT products. 2022. https://www.cencenelec.eu/news-and-events/news/2022/eninthespotlight/2022-10-27-new-en-17640-helps-evaluate-the-cybersecurity-of-ict-products/

[70] Kuhlmann, Dirk; Weber, Arnd: OpenTC Final Report. The Evolution of the OpenTC Architecture illustrated via its Proof-of-Concept-Prototypes. Bristol, Karlsruhe 2009, www.opentc.net, http://www.itas.kit.edu/pub/m/2009/kuua09a_contents.htm.

[71] Weber, Arnd; Weber, Dirk: Verifizierte Virtualisierung für mehr Sicherheit und Komfort. Datenschutz und Datensicherheit 1/2012, 43-47. English: Verified Virtualisation for more Security and Convenience. http://www.itas.kit.edu/pub/v/2013/wewe13b.pdf