Reverse Engineering for Thwarting Digital Supply Chain Attacks in Critical Infrastructures: Ethical Considerations

Arne Roar Nygård, Arvind Sharma and Sokratis Katsikas[a]
Department of Information Security and Communication Technology, Norwegian University of Science and Technology, Gjøvik, Norway

Keywords: Digital Supply Chain, Digital Substation, Critical Infrastructure, Cyber-attack, Cyber Risk, Ethics, Reverse Engineering, Vulnerability Disclosure, Vulnerability Research, Moral Dilemma.

Abstract: A reverse engineering process includes disassembling to analyse, test, and document the functionality of the target system. In doing so for the purpose of uncovering vulnerabilities intentionally or unintentionally introduced through the digital supply chain in components used in industrial control systems within critical infrastructures, ethical issues arise. This paper addresses such issues, by leveraging a real-life use case in the power infrastructure. A set of principles that should govern an ethical framework geared to reverse engineering for cybersecurity and recommendations on action needed to complement such a framework are proposed.

1 INTRODUCTION

The digital transformation of industrial processes, enabled by many technologies, including the Industrial Internet of Things (IIoT), is progressing worldwide at an increasing pace. The IIoT is not a standalone system obtained from a single supplier or manufacturer, having proprietary hardware and software. Instead, it is composed of various interconnected components designed, manufactured, and operated by different entities in different parts of the world (Martin, 2020). Several actors are involved in setting up the IIoT ecosystem in an IIoT technology stack, including sensing/actuating device manufacturers, firmware developers, radio access network providers, cloud service providers, and end-users. The endpoint devices are made of embedded hardware that interacts with the physical environment and is driven by firmware or operating systems software processes. This uses access points, gateways, and core IP networks to connect to cloud servers, hosting applications and services. IIoT-related vulnerabilities, if successfully exploited, can affect the device itself and the application field in which the IIoT device operates.

Using digital technologies, i.e., introducing IIoT devices and sensors coupled to electrical grid equipment, allows real-time data to facilitate efficient decision-making. IIoT devices and sensors often use wireless communication abilities such as the next-generation wireless communication standards, i.e., 5G (Tao et al., 2020). Existing industrial control systems (ICS) that are siloed and air-gapped will, in the future, possibly include numerous devices capable of wireless communication. These IIoT devices and sensors are produced at affordable prices and made in large bulks (Koelsch, 2019). Cost efficiency is essential for the manufacturer, leading to an increasingly complex equipment and solution production supply chain. The various parts, especially hardware, are produced in multiple countries and then shipped to the vendor assembly line and put together without proper investigation of the actual content in each part. This means that no proof of cybersecurity is provided as part of the supply chain, and therefore no trust can be placed on the resulting product.

Integrating multiple devices and components designed and manufactured by different entities makes the system extremely vulnerable to supply chain attacks (Farooq and Zhu, 2019). A digital supply chain attack is a combination of at least two attacks. The first attack is on a supplier that is then

[a] https://orcid.org/0000-0003-2966-9683

Nygård, A., Sharma, A. and Katsikas, S.
Reverse Engineering for Thwarting Digital Supply Chain Attacks in Critical Infrastructures: Ethical Considerations.
DOI: 10.5220/0011384300003283
In *Proceedings of the 19th International Conference on Security and Cryptography (SECRYPT 2022)*, pages 461-468
ISBN: 978-989-758-590-6; ISSN: 2184-7711

used to attack the target to gain access to its assets. The target can be the final customer or another supplier. For an attack to be classified as a supply chain one, both the supplier and the customer must be targets (ENISA, 2021).

With the emergence and rapid adoption of IIoT technologies in critical infrastructure systems, supply chain attacks become more complex and involve international entities. Since the IIoT is inherently a decentralised system, controlling the entire supply chain is challenging. However, the challenges go much beyond the regulation of the supply chain.

Supply chain attacks can be executed when adversaries use hidden backdoors that have been inserted through the manipulation of hardware and firmware components or software elements. At the beginning of 2019, a report by Andrew Huang of the Supply Chain Security entitled “If I were a Nation-State ...” (Huang, 2019) was presented at the Blue Hat IL Conference. the Report Describes Supply Chains’ Insecurity in Introducing Backdoors into the Hardware Component of Many Electronic Devices. This Insecurity Is Even More Accentuated When Such Devices Are Used in ICS Employed in Critical Infrastructures.

to Increase Security and Resilience at the Hardware Level, One Must Know How These Devices Are Vulnerable and Identify Relevant Attack Vectors. a Robust Method to Do This Is Reverse Engineering, Which Retrieves Information from Anything Artificial to Understand Its Inner Structures and Workings (Fyrbiak Et Al., 2017). Thus, Reverse Engineering Can Be Very Supportive in Securing Digital Supply Chains.

but Is Reverse Engineering Legal and Ethical? the Legal Debate around Reverse Engineering Has Been Going on for Years. It Usually Revolves around the Question of What Social and Economic Impact Reverse Engineering Has on the Society as a Whole. of Course, Calculating This Impact Largely Depends on What Reverse Engineering Is Used for (Eilam, 2005). However, Ethical Aspects of Reverse Engineering Have Not Been so Extensively Debated or Researched, Even Less so in the Context of Critical Infrastructure.

This Paper Addresses Ethical Considerations concerning the Use of Reverse Engineering Practices to Analyse Devices Used in ICS Operating in Critical Infrastructure, including the Sharing of the Knowledge Derived through the Process, with the Intention of Thwarting Digital Supply Chain Attacks.

with the Aid of a Use Case in the Power Infrastructure, Embedding Communication and Information Exchange Functionality More than Ever before, Nationally and Internationally, This Paper Contributes Ethical Principles That Should Be Observed When Reverse Engineering Is Used in the Critical Infrastructure Sector, towards an Ethical Framework for Researchers and Practitioners in the Field, and Recommendations on Action Needed to Supplement Such a Framework.

the Remaining of the Paper Is Structured as Follows: Section 2 Presents the Background Necessary for the Paper to Be Self-Sustained and Reviews Relevant Work. Section 3 Discusses the Use Case. Section 4 Addresses Ethical Considerations and, Finally, Section 5 Summarizes Our Conclusions and Proposes Topics for Further Research.

2 BACKGROUND AND RELEVANT WORK

2.1 Digital Supply Chain Attacks

Despite the growing concern and acknowledging that addressing cybersecurity risks in the digital supply chain is a complex problem, few research works (ENISA, 2021; Martin, 2020; Farooq and Zhu, 2019; Lysne, 2018; Ghadge et al., 2020) have addressed it. This is even more challenging when managing supply chain cyber-security risks in digitally transformed industrial settings, particularly critical infrastructures. As discussed in (Lysne, 2018), four aspects of industrial espionage make this type of attack far more difficult to handle than the scenarios addressed in mainstream security research:

1. When malware is already in the system at the purchase, stopping it from entering is futile.
2. When there is no golden sample, it is impossible to detect tampering by comparing a system to a known healthy system.
3. Built-in security mechanisms in system chips, operating systems, or compilers are in the hands of vendors we may not trust.
4. The malicious actions of the system can be performed anywhere in the technology stack, from low-level hardware to software controlling the user interface.

A variety of techniques can be used to implement supply chain attacks. Table 1 (ENISA, 2021) lists these techniques and examples of how each attack method can be realised. Each method in the table identifies how the attack happened, not what was attacked, and several techniques may be applied in the same attack.

Table 1: Supply chain attack techniques.

Attack technique	Example
Malware infection	Spyware is used to steal credentials from employees.
Social engineering	Phishing, fake applications, typo-squatting, Wi-Fi impersonation, convincing the supplier to do something
Brute-force attack	Guessing a Secure Shell Protocol (SSH) password, guessing a web login
Exploiting software vulnerability	SQL injection or buffer overflow exploit in an application
Exploiting configuration vulnerability	Taking advantage of a configuration problem
Physical attack or modification	Modify hardware, physical intrusion
Open-source intelligence (OSINT)	Search online for credentials, API keys, usernames
Counterfeiting	Imitation of USB with malicious purposes

The threats may include backdoor channels in devices, injected viruses, provided faulty chips, or loading with malicious software. Such malicious modifications can target the firmware that controls and operates the device. Recent real-world incidents such as Zombie Zero and NotPetya demonstrate the feasibility of such firmware trojan attacks. An alarming characteristic of firmware trojans is that they are highly stealthy and persistent, exploiting the essential software in an embedded device. In their simplest form, firmware trojans can realise Denial of Service (DoS) attacks and attack the availability of an ICS, as was the case in the attacks against the Ukraine's power grid in 2015 and 2016. Beyond DoS, advanced and stealthy firmware trojans can target the confidentiality of information by exposing sensitive information and thus enabling more sophisticated attacks. For ICS deployed in critical industries, leaked information can compromise operations. For example, extracting the water pressure values in a water treatment facility using a firmware trojan can enable sensor spoofing attacks and compromise the functionality of the plant (Martin, 2020).

In addition to firmware, hardware is also susceptible to supply chain attacks. RE is illuminated as a tool for revealing malware and malicious manipulations.

2.2 Reverse Engineering

Formally, reverse engineering is “the process of analysing a subject system to identify the system's components and their interrelationships and to create representations of the system in another form or at a higher level of abstraction” (Eilam, 2005). Reverse engineering is employed to understand the physical and functional details to replicate or redesign the original (Hariharan, 2018). Traditionally reverse engineering has been about taking shrink-wrapped products and physically dissecting them to uncover their design secrets. Such secrets were then typically used to make similar or better products. In many industries, reverse engineering involves examining the effect under a microscope or taking it apart and figuring out what each piece does (Eilam, 2005). It has been described as “fundamentally directed to discovery and learning”. Reverse engineering has evolved to enable understanding increasingly complex systems.

Underlying hardware components form the basis of trust in virtually any computing system (Wiesen et al., 2019a). Those security failures in hardware pose a devastating threat to our daily lives. As a result, security engineers commonly employ hardware reverse engineering to identify security vulnerabilities, detect IP violations, or conduct very-large-scale integration (VLSI) failure analysis.

In the software world, reverse engineering boils down to taking an existing program for which source code or proper documentation is not available and attempting to recover details regarding its design and implementation (Eilam, 2005). Reverse Engineering of software is undertaken “to learn about the structure and organisation of the product or to learn its algorithm”.

To detect fabrication faults, copyright infringements, counterfeit products, or malicious manipulations, Hardware Reverse Engineering is usually the tool of choice. While hardware reverse engineering is a highly complex and universal tool for legitimate purposes, it can also be employed with illegitimate intentions, undermining the integrity of Integrated Circuits via piracy, subsequent weakening of security functions, or insertion of Hardware Trojans (Wiesen et al., 2019b).

2.3 Ethics in Reverse Engineering

There is currently no single ethical framework that guides the conduct of cybersecurity research in general, far less in cybersecurity vulnerability research and cybersecurity reverse engineering. In view of this shortage, the closest applicable frameworks are the codes of ethics that guide the behavior of the members of organizations such as the Association for Computing Machinery (ACM), the Institute of Electrical and Electronics Engineers (IEEE), and the Information Systems Security Association, Inc. (ISSA) in carrying out their professional duties (Gotterbarn et al., 2018; Gotterbarn et al., 1997; IEEE, 2014; ISSA, 2020).

As noted in (Nweke and Wolthusen, 2020) these generic ethical frameworks have some drawbacks in that they fail to offer a clear decision-making process when confronted with an ethical issue: absence of shared community values, lack of consensus on enforcement, and limited individual expertise (Carle, 2003).

One of the earliest and most influential works related to ethics in security vulnerability research is presented in (Leiwo and Heikkuri, 1998). In this paper, ethics as a foundation of secure interconnection of systems is critically analysed and several problems of the ethical layer are identified to suggest a new group and social contract layer, on top of the ethical layer.

A common ethical framework for security researchers was proposed in (Carle, 2003), where different ethical frameworks were presented and applied to case studies with scenarios of security research.

An ethical guideline for security researchers was proposed in (Sassaman, 2010), where case studies of ethical failings were analysed to demonstrate the problems that could arise when the right or wrong course of action is not perfectly clear. The same approach with use case analysis was followed in (Dittrich et al., 2010) to recommend appropriate responses to difficult issues of privacy and responsible disclosure of vulnerability information.

According to (Matwyshyn et. al, 2010), security vulnerability researchers perform an essential social function as they provide an information gap between the creators, or exploiters of vulnerable systems and the third parties who will likely be harmed because of them. Use case analysis was also used in this paper to recommend best practices in security vulnerability research.

Hypothetical and actual examples to illustrate the reasons for increasing the availability of proprietary operational data for legitimate research purposes were provided in (Shou, 2011). Reasons, such as privacy and competition, to limit data sharing were also discussed. The capabilities and limitations of several existing models of data sharing were analysed, to propose an infrastructure specifically designed for making proprietary operational data available for cyber security research and experimentation.

The ethical implications of security vulnerability research for critical infrastructure protection were examined in (Nweke and Wolthusen, 2020), by using three normative ethical theories, namely deontological, consequentialist and virtue ethics. A hypothetical scenario relating to security vulnerability in a critical infrastructure was analysed in the light of these theories to provide guidance for security researchers involved in security vulnerability research, and the issue of how a security researcher would make an ethical decision when confronted with an ethical dilemma was discussed.

Ethics in hardware reverse engineering apparently has not received research attention. As noted in (Center for Cybersecurity policy and law, 2019), the disclosure of hardware vulnerabilities differs from software ones in that hardware mitigations may require action at multiple system layers; the larger number of participants often required to develop, test and deploy mitigations addressing hardware vulnerabilities; and the potential for reliance on third parties for distribution of mitigations addressing hardware vulnerabilities. These differences can be addressed by improving the coordinated vulnerability disclosure process as recommended in (Center for Cybersecurity policy and law, 2019).

As can be noted, real life or hypothetical case study analysis is a common approach deployed in most of the works related to ethics in security vulnerability research; we present a real-life use case to approach ethical considerations and challenges in reverse engineering in the power infrastructure.

3 THE USE CASE

Digital substations provide industrial power operations, real-time functionalities and information access. Digital substations based on the IEC 61850 standard is a new concept that involves replacing most of hardwired copper connections in the substation with process bus technology over fibre cabling (Khodabakhsh et al., 2020). The development of digital substations provides real-time functionality

and access to information valuable to the power infrastructure's efficient operation.

A digital substation consists of several physical and cyber infrastructures in switchyard and substation buildings. One of the main challenges with a digital substation is to ensure the security, availability, and reliability of power systems as in conventional methods and interoperability capability for different vendors.

Physical infrastructure components of a digital substation at the process level are current transformers (CT), voltage transformers (VT), merging units (MU), breakers, sensors, etc., and the cyber infrastructure includes a communication network, Intelligent Electronic Devices (IEDs), switches, software and hardware at the station level. A Human Machine Interface (HMI) is the graphical interface between the human operator and the controller (all the physical devices) of an industrial system for interaction and communication between them. SCADA is a centralised system used for monitoring and controlling a plant. IED is a microprocessor-based device used by the electric power industry to maintain power system switching devices. Current and voltage transformers are devices that constantly interact with the physical electric power environment and communicate with the controller via a shared process bus. MU is a device that enables the implementation of an IEC61850 process bus by converting the analog signals from the conventional CT/VT into IEC61850 for metering, protection, and control purposes.

These components are vulnerable to cyber threats and must be secured to prevent, mitigate, and handle cyber-attacks to ensure the power system's availability and preserve reliability (Khodabakhsh et al., 2020).

The complexity of modern computer systems is so great that it is difficult to have a complete overview of the functionality, even for those who develop them. We know that building flawless systems is almost impossible. This is accepted to the extent that no one will purchase complex equipment without a support agreement that the supplier will provide software updates to correct programming errors as they are identified. Thus, complexity is not restricted to software code but includes hardware devices and social engineering to exploit business processes.

Verifying the security of components of a digital substation, consisting of techniques, methods, tools, procedures, and a methodology for systematically applying them, will support the power industry and operators of critical infrastructure, as well as authorities to verify the security of products currently being used, without us knowing their possible vulnerabilities, but if the buyers of equipment are no longer expected even to understand the equipment they buy, this has profound cost implications (Lysne, 2018). It means that the equipment vendor has the power to make the gear do things that are not in the interest of its owner. For example, the vendor could turn the equipment against its owner without the owner ever finding out.

There are many hardware components within the power infrastructure from different vendors, ranging from IT products to industry-specific tailored details. According to (Lysne, 2018), this increases what a dishonest vendor in the supply chain could do. The exact answer will vary depending on the motivation of the illegal vendor, but the actions need to be concerned the same as those we fear from third-party cyberattacks. We fear that attackers carry out espionage and surveillance to hold confidential information from companies, private per-sons, or nation-states. We fear sabotage of equipment, either permanently or temporarily.

4 ETHICAL CONSIDERATIONS

4.1 Ethical Challenges

Using reverse engineering methodology to verify the absence of unwanted content within hardware components must be interpreted with ethical caution, and several limitations should be borne in mind. First, the vast complexity of hardware trojans hiding and operating makes it difficult to generalise findings.

According to ethics, honesty, objectivity, integrity, carefulness, openness, respect for intellectual property, confidentiality, responsible publication, respect for colleagues, social responsibility, competence, and legality must be observed and respected throughout the research project. Furthermore, the confidentiality of information and of the collaborating individuals and institutions provided during and for the research must be respected. Current methods of oversight and guidance regarding cybersecurity ethics are inadequate (Macnish et al., 2020). In the latter, a lack of adequate guidance or accountability forms a barrier to consistent ethical practice. The ethical issues are complicated, although hardly new to the cybersecurity community. Despite this, there is relatively little guidance on how practitioners should proceed in many cases. There is a clear need to develop an active dialogue regarding ethics in the research and practice of cybersecurity. This, too, is

lacking, partly due to the relative lack of ethics teaching provided to computer scientists in higher education, especially when it comes to teaching cybersecurity ethics.

4.2 Ethical Principles

Resnik in (Resnik, 2020) lists 18 ethical principles for research based on what is included in various codes of ethics for analysis. In this use case, the most relevant principles seem to be:

Openness: There are various hardware components from different vendors within the power infrastructure, ranging from COTS IT products to industry-specific tailored details. The use of hardware reverse engineering to verify unwanted content within hardware components brings considerations according to openness. However, the results must be interpreted with caution, and several limitations should be considered.

Accountability: A research project aiming at verifying the security of technological components will entail human, organisational, and social kinds of problem-solving and artefact (tools, methods, techniques, procedures) development. According to ethics, honesty, objectivity, integrity, carefulness, openness, respect for intellectual property, confidentiality, responsible publication, respect for colleagues, social responsibility, competence, and legality must be observed and respected throughout the research project.

Confidentiality: The confidentiality of information the collaborating individuals and institutions provided during and for the research must be respected. Data collected throughout the study will be used concerning academic and research integrity principles. Information defined as "sensitive" must be shielded from the public and kept in an appropriate trusted group.

Social Responsibility: Appropriate credit will be given to knowledge and prior work used in publications, avoiding plagiarism. Sharing of information as far as legal and sometimes in closed groups.

Legality: Appropriate focus on relevant laws and governmental policies must be taken.

4.3 Way Forward

Developing a code of conduct for cybersecurity research is recommended to overcome ethical dilemmas (Macnish et al., 2020). Such a code may protect researchers against legal claims and assist them in acting against ethical barriers in their research field.

When confronted with a moral dilemma, security researchers rely on the following process to make an ethical decision: “Recognize an ethical issue - Consider the parties involved – Gather all the relevant information – Formulate actions and consider alternatives – Act – Reflect on the outcome” (Nweke and Wolthusen, 2020).

According to the normative ethics approach, one principle that distinguishes morally good conduct from bad is normative. When analysing a specific situation to determine if it is ethical, it is customary to apply multiple normative principles to get a fuller understanding. A normative principle is not a branch of normative ethics or an analysis tool but a belief principle one strives to achieve, e.g., the golden rule. Before conducting reverse engineering research there are four questions relevant to ethical principles to answer:

- Why should you conduct reverse engineering research in a specific project? For example, one can evaluate if time, money, and resources are better spent elsewhere.
- For whom are you conducting the research?
- How can you conduct responsible reverse engineering research?
- How, when, and for whom should you disclose the findings?

The primary objective of a reverse engineering project is to systematically use tools, techniques, methods, and procedures to secure the digital value chain from supply and throughout the component's lifetime in the power infrastructure. This breaks down into identifying security gaps, vulnerabilities, and attack vectors in the digital value chain and components in the power system that are vulnerable and critical for its operation.

A coordinated vulnerability disclosure process, along the lines laid out in (Center for Cybersecurity policy and law, 2019), specifically targeting critical infrastructure sectors, aiming at reducing end user risk and enhancing end user security can facilitate and regulate information sharing. This goal is best accomplished when stakeholders work together, as suggested in (Korte, 2017), to mitigate vulnerabilities in a responsible and coordinated manner.

5 CONCLUSIONS

This paper discussed ethical issues and challenges and provided recommendations for ethical reverse engineering with the purpose of securing hardware

components used in industrial control systems in critical infrastructures. A use case scenario in the power sector where hardware devices connected with the network are considered trustworthy has been used to place the discussion in context. If the security researcher is aware of the ethical aspects reverse engineering is neither unethical nor illegal if it is performed honourably, according to a framework still to be developed and appropriately endorsed. Collaboration with vendors and suppliers at an industry-wide level is not only a critically essential element of defence; it is also imperative.

Future research will focus on developing a proposal for an ethical framework for cybersecurity reverse engineering and on how this can be endorsed and implemented by industry involved in critical infrastructure sectors.

ACKNOWLEDGEMENTS

This work was supported in part by the Research Council of Norway under project 310105 (Norwegian Centre for Cybersecurity in Critical Sectors - NORCICS).

REFERENCES

Carle, S. (2003). Crossing the line: Ethics for the security professional. https://www.sans.org/reading-room/whitepapers/hackers/crossing-line-ethicssecurity-professional-890

Center for cybersecurity policy and law (2019). Improving Hardware Component Vulnerability Disclosure. https://centerforcybersecuritypolicy.org/s/The-Center-for-Cybersecurity-Policy-and-Law_Improving-Hardware-Component-Vulnerability-Disclosure_Ap.pdf

Dittrich, D. et al. (2010). Building an active computer security ethics community. *IEEE Security & Privacy 9(4), 32–40*.

Eilam, E. (2005). *Reversing: Secrets of Reverse Engineering*, Wiley Publishing.

ENISA (2021). Threat Landscape for Supply Chain Attacks. https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks/@@download/fullReport

Farooq, M. and Zhu, Q. (2019). IoT Supply Chain Security: Overview, Challenges, and the Road Ahead. arXiv:1908.07828.

Fyrbiak, M. et al. (2017). Hardware reverse engineering: Overview and open challenges. *In IEEE 2nd International Verification and Security Workshop (IVSW)*.

Ghadge, M. et al. (2020). Managing cyber risk in supply chains: a review and research agenda. *Supply Chain Management*, vol. 25, no. 2, p. 223–240.

Gotterbarn, D. et al. (1997). Software engineering code of ethics. *Communications of the ACM 40(11), 110–118*.

Gotterbarn, D. et al. (2018). ACM code of ethics and professional conduct. ACM.

Hariharan, B. (2018). Reverse Engineering. *In Augier M., Teece D.J. (eds) The Palgrave Encyclopedia of Strategic Management. Palgrave Macmillan, London*. https://doi.org/10.1057/978-1-137-00772-8_249

Huang, A. (2019). Supply Chain Security: "If I were a Nation State...". BlueHat IL. Available: https://www.youtube.com/watch?v=RqQhWitJ1As

IEEE (2014). IEEE code of ethics. https://www.ieee.org/about/corporate/governance/p7- 8.html

ISSA (2020). ISSA code of ethics. https://www.members.issa.org/page/CodeofEthics.

Khodabakhsh, A. et al. (2020). Cyber-Security Gaps in a Digital Substation: From Sensors to SCADA. *In 9th Mediterranean Conference on Embedded Computing (MECO 2020.*

Koelsch, J.R. (2019). Battle for Cybersecurity Spreads to Sensors. url: https://www.automationworld.com/products/data/article/13320007/battle-for-cybersecurity-spreads-to-sensors.

Korte, J. (2017). Mitigating cyber risks through information sharing. *Journal of Payments Strategy & Systems*. [s. l.], v. 11, n. 3, p. 203–214.

Leiwo, J. and Heikkuri, S. (1998). An analysis of ethics as foundation of information security in distributed systems. *In Proceedings of the Thirty-First Hawaii International Conference on System Sciences*.

Lysne, O. (2018). *The Huawei and Snowden Questions: Can Electronic Equipment from Untrusted Vendors be Verified? Can an Untrusted Vendor Build Trust into Electronic Equipment?*, Cham: SpringerOpen.

Macnish, K. and van der Ham, J. (2020). Ethics in cybersecurity research and practice. *Technology in Society 2020*, 63, doi:10.1016/j.techsoc.2020.101382.

Martin, R. (2020). Assurance for Cyber Physical Systems: Addressing Supply Chain Challenges to Trustworthy Software-Enabled Things. In *2020 IEEE Systems Security Symposium (SSS)*, IEEE.

Matwyshyn, A. et al. (2010). Ethics in security vulnerability research. *IEEE Security & Privacy, vol. 8, no. 2, pp. 67-72*.

Nweke, L. and Wolthusen, S. (2020). Ethical Implications of Security Vulnerability Research for Critical Infrastructure Protection. *In 15th International Conference on Wirtschaftsinformatik*.

Resnik, D.B. (2020). What Is Ethics in Research & Why Is It Important? https://www.niehs.nih.gov/research/resources/bioethics/whatis/index.cfm.

Sassaman, L. (2010). Ethical guidelines for computer security researchers: “be reasonable”. *In Lecture Notes in Computer Science 6054, 250*.

Shou, D. (2011). Ethical considerations of sharing data for cybersecurity research. *In International Conference on Financial Cryptography and Data Security*. Springer.

Tao, J. et al. (2020). The impact of the Internet of Things supported by emerging 5G in power systems: a review. *CSEE Journal of Power and Energy Systems*. 6.2 (2020), pp. 344–352. DOI: 10.17775/CSEEJPES.2019.01850.

Wiesen, C. et al. (2019a). Promoting the Acquisition of Hardware Reverse Engineering Skills. *In 2019 IEEE Frontiers in Education Conference (FIE)*. pp. 1–9. DOI: 10.1109/FIE43999.2019.9028668.

Wiesen, C. et al. (2019b). Teaching Hardware Reverse Engineering: Educational Guidelines and Practical