Report from Dagstuhl Seminar 24112

EU Cyber Resilience Act: Socio-Technical and Research Challenges

Mila Dalla Preda[*1], Serge Egelman[*2], Anna Maria Mandalari[*3], Volker Stocker[†4], Juan Tapiador[†5], and Narseo Vallina-Rodriguez[*6]

1 **University of Verona, IT.** mila.dallapreda@univr.it
2 **ICSI – Berkeley, US.** egelman@cs.berkeley.edu
3 **University College London, GB.** a.mandalari@ucl.ac.uk
4 **TU-Berlin, DE.** vstocker@inet.tu-berlin.de
5 **UC3M – Madrid, ES.** jestevez@inf.uc3m.es
6 **IMDEA Networks Institute – Madrid, ES.** narseo.vallina@imdea.org

Abstract

This report documents the program and the outcomes of Dagstuhl Seminar *"EU Cyber Resilience Act: Socio-Technical and Research Challenges"* (24112). This timely seminar brought together experts in computer science, tech policy, and economics, as well as industry stakeholders, national agencies, and regulators to identify new research challenges posed by the EU Cyber Resilience Act (CRA), a new EU regulation that aims to set essential cybersecurity requirements for digital products to be permissible in the EU market.

The seminar focused on analyzing the proposed text and standards for identifying obstacles in standardization, developer practices, user awareness, and software analysis methods for easing adoption, certification, and enforcement. Seminar participants noted the complexity of designing meaningful cybersecurity regulations and of aligning regulatory requirements with technological advancements, market trends, and vendor incentives, referencing past challenges with GDPR and COPPA adoption and compliance. The seminar also emphasized the importance of regulators, marketplaces, and both mobile and IoT platforms in eliminating malicious and deceptive actors from the market, and promoting transparent security practices from vendors and their software supply chain. The seminar showed the need for multi-disciplinary and collaborative efforts to support the CRA's successful implementation and enhance cybersecurity across the EU.

Seminar March 10–13, 2024 – https://www.dagstuhl.de/24112
2012 ACM Subject Classification Security and privacy → Human and societal aspects of security and privacy
Keywords and phrases Cyber Resilience Act, Software Testing, Software Analysis, IoT, Security Regulations, Security Economics
Digital Object Identifier 10.4230/DagRep.14.3.52

[*] Editor / Organizer
[†] Editorial Assistant / Collector

EU Cyber Resilience Act: Socio-Technical and Research Challenges, *Dagstuhl Reports*, Vol. 14, Issue 3, pp. 52–74
Editors: Mila Dalla Preda, Serge Egelman, Anna Maria Mandalari, Volker Stocker, Juan Tapiador, and Narseo Vallina-Rodriguez

Dagstuhl Reports
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

1 Executive Summary

Mila Dalla Preda
Serge Egelman
Anna Maria Mandalari
Narseo Vallina-Rodriguez

Introduction and Motivation

The increasing number of cyberattacks affecting digital products has caused significant security and financial costs to societies. For example, the Mirai attack in 2016 compromised millions of Internet of Things (IoT) devices by exploiting default usernames and passwords, turning them into a botnet army that launched a massive Distributed Denial of Service (DDoS) attack. This attack significantly impacted critical Internet services, causing major outages and disruptions on platforms like Twitter and Netflix [1].

The European Commission has proposed in 2022 the EU Cyber Resilience Act (CRA) to define the legislative framework of essential cybersecurity requirements that product manufacturers must meet when placing any product with digital elements on the internal market, while empowering users to make better security-aware decisions when purchasing and deploying digital products. Following its adoption in 2024, manufacturers will have two years to comply with the new rule, with specific deadlines for different types of products.

The roadmap for CRA adoption follows a multi-phased approach, focusing on high-risk products first and progressively expanding to cover a broader range of digital products over the next few years, aiming to ensure robust cybersecurity standards across the EU. Specifically, during the first year, the focus will be on raising awareness among stakeholders and providing guidance on compliance requirements. The European Commission and national authorities will offer support and resources to help manufacturers understand the new obligations. Then, during the second year, manufacturers and developers will need to ensure that their products meet CRA requirements. This includes implementing necessary security measures, conducting risk assessments, and updating product documentation.

In this scenario, device and software analysis methods – from formal methods to black-box testing – are essential for facilitating compliance at different stages of the product life-cycle, but also for self-attestation and independent verification and certification. However, the rapid evolution and increasing complexity of new technologies and other socio-technical factors such as developers' awareness and incentives for compliance may add further challenges and barriers to adoption.

On the one hand, it is essential to understand whether regulatory requirements are realistic, unambiguous, and whether they are partially misaligned with technology trends, manufacturers' incentives and goals, and with users' privacy and security awareness. For example, research evidence has shown that many developers do not fully comply with the General Data Protection Regulation (GDPR) and the USA Children Online Privacy Protection Act (COPPA) requirements due to their dependency on obscure third-party components for development support and advertising, economic incentives, poor software engineering habits, or even a lack of awareness about the regulations' existence and scope (and hence their compliance obligations). On the other hand, we need to assess to which extent existing device and software analysis methods are fit for aiding developers and manufacturers in assessing compliance, but also for independent certification by third-parties and regulatory

enforcement. Yet, current software and device analysis techniques (e.g., black-box testing) often over-simplify the complexity of digital products and present various scalability and coverage limitations that prevent them from reliably auditing and testing whether observed software properties in digital products comply with regulatory requirements.

This Dagstuhl Seminar united a multidisciplinary group of tech and legal academics, industry actors, and policy experts to share their knowledge and experience to collaboratively explore the complex landscape of research and socio-technical challenges for the adoption and enforcement of the CRA. These challenges arise from developer practices and incentives, user awareness, and the feasibility of existing software analysis methods for certification and enforcement.

Seminar Structure

The seminar had a dynamic structure during the 3 days, combining dedicated presentations, panels, and multi-disciplinary working groups to encourage active participation and dialogue between different communities and stakeholders. Arriving on Sunday and starting with a welcome dinner at Schloss Dagstuhl. The three-day seminar activities were structured as follows:

- **Day 1.** The first morning was dedicated to participant introductions, setting common ground on seminar objectives through short elevator pitches by participants, followed by two seminar-like talks and guided discussions. This engaging round of introductions provided a comprehensive overview of the diverse knowledge and skills present in the room, setting the scene for collaborative and constructive discussions. Following these introductions, the seminar continued with an introductory talk by the organizers, a key presentation by Christin Hartung-Kümmerling and Anna Schwendicke from the BSI on the fundamentals, goals, and roadmap of the CRA, and a talk by Vicent Toubina (CNIL) on their experiences with GDPR implementation and enforcement. Following these, participants engaged in open discussions to identify sub-problems of interest. At the end of the first day, participants formed multidisciplinary discussion groups to summarize seminar outputs and a brainstorm session for identifying three key topics for further discussion: (*i*) Understanding and Aiding the Developer Ecosystem; (*ii*) Standardization Efforts; and (*iii*) Tools for Regulatory Enforcement.
- **Day 2.** The second day continued with the interactive group discussions, finalizing with a final all-hands group to consolidate the outputs of the discussions. The day ended with a social activity involving a guided visit to the Völklingen Ironworks, and a dinner in Saarbrücken.
- **Day 3.** The final day involved several all-hands sessions to identify the main outcomes of the seminar, and research challenges for easing CRA adoption and compliance, ensuring continued progress beyond the seminar.

The full seminar agenda is available at: `https://www.dagstuhl.de/24112/schedule.pdf`.

References

1 Manos Antonakakis, Tim April, Michael Bailey, Matt Bernhard, Elie Bursztein, Jaime Cochran, Zakir Durumeric, J Alex Halderman, Luca Invernizzi, Michalis Kallitsis, et al. Understanding the mirai botnet. In *26th USENIX security symposium (USENIX Security 17)*, pages 1093–1110, 2017.

2 Jukka Ruohonen and Kalle Hjerppe. The gdpr enforcement fines at glance. *Information Systems*, 106:101876, 2022.

3 Célestin Matte, Nataliia Bielova, and Cristiana Santos. Do cookie banners respect my choice?: Measuring legal compliance of banners from iab europe's transparency and consent framework. In *2020 IEEE Symposium on Security and Privacy (SP)*, pages 791–809. IEEE, 2020.

4 Irwin Reyes, Primal Wijesekera, Joel Reardon, Amit Elazari Bar On, Abbas Razaghpanah, Narseo Vallina-Rodriguez, Serge Egelman, et al. "won't somebody think of the children?" examining coppa compliance at scale. In *The 18th Privacy Enhancing Technologies Symposium (PETS 2018)*, 2018.

5 Christoph Bösch, Benjamin Erb, Frank Kargl, Henning Kopp, and Stefan Pfattheicher. Tales from the dark side: Privacy dark strategies and privacy dark patterns. *Proceedings on Privacy Enhancing Technologies*, 2016.

6 Noura Alomar and Serge Egelman. Developers say the darnedest things: Privacy compliance processes followed by developers of child-directed apps. *Proceedings on Privacy Enhancing Technologies*, 2022.

7 Michael Backes, Sven Bugiel, and Erik Derr. Reliable third-party library detection in android and its security applications. In *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*, pages 356–367, 2016.

8 Andrei Costin, Jonas Zaddach, Aurélien Francillon, and Davide Balzarotti. A {Large-scale} analysis of the security of embedded firmwares. In *23rd USENIX security symposium (USENIX Security 14)*, pages 95–110, 2014.

9 Gianluca Anselmi, Anna Maria Mandalari, Sara Lazzaro, and Vincenzo De Angelis. *COPSEC: Compliance-Oriented IoT Security and Privacy Evaluation Framework*. Association for Computing Machinery, New York, NY, USA, 2023.

10 Aniketh Girish, Tianrui Hu, Vijay Prakash, Daniel J Dubois, Srdjan Matic, Danny Yuxing Huang, Serge Egelman, Joel Reardon, Juan Tapiador, David Choffnes, et al. In the room where it happens: Characterizing local communication and threats in smart homes. In *Proceedings of the 2023 ACM on Internet Measurement Conference*, pages 437–456, 2023.

2 Table of Contents

3 Expected Objectives

Mila Dalla Preda, Serge Egelman, Anna Maria Mandalari, Narseo Vallina-Rodriguez

The goal of this multi-disciplinary seminar on the CRA was to foster comprehensive understanding, collaboration, and strategic planning among stakeholders and research disciplines to aid effective implementation and compliance with the upcoming cybersecurity regulations. Specifically:

1. **Bridging the gap between policy, users and developers.** New tech regulations are often perceived as too late and too difficult to enforce. Regulations can be ambiguous and difficult to interpret and implement by non-legal experts like software developers, even for large companies with legal support [2, 3]. We also note that legal experts may not be able to appropriately capture technical challenges and concepts in the law. Evidence and experience show that even core aspects of the GDPR such as informed consent were interpreted differently by national Data Protection Agencies, thus leading to confusion across developers and facilitating abuse. The EU single market should foster harmonized enforcement across all member states. We wanted to review the legal framework conditions and the research literature to identify shortcomings of existing tech policies and regulations at the compliance and enforcement level. Specifically, we wanted to cover the EU GDPR and EU CRA, but also related international efforts like COPPA and NIST's Cybersecurity Framework in the USA and industry certification frameworks like the IoXT Alliance. This analysis allowed us to assess regulation's aptness and effectiveness at achieving their core objectives, as well as potential barriers for (1) compliance; and (2) both self- and independent certification schemes like certification authorities and regulatory bodies. In fact, one particular discussion of interest was about the effectiveness and shortcomings of self-certification schemes and the processes followed by certification authorities in order to identify procedures and protocols to avoid malicious and deceptive actors from cheating or giving a false sense of compliance [4, 5]. Discussing the legal context from a socio-technical perspective is key to (1) identifying barriers to adoption due to regulations' misalignment with developers' expectations and incentives, and users' preferences (Topic 2), and (2) mapping the requirements and scope of certification frameworks to testing methods for compliance and enforcement (Topic 3).

2. **Understanding development and consumption habits.** Software development practices, industry incentives, and the lack of strict enforcement actions are known barriers to the adoption of the regulation. Additionally, user awareness is key not only to pressure industry actors to comply with regulations but also to pressure policymakers in the development of stricter policies and demanding enforcement actions. Unfortunately, regulatory requirements are often misaligned with developer's development paradigms and incentives [4]. Some developers may not be fully aware of how to comply with the rule or may not be familiar with the principles of privacy- and security-by-default engineering when creating new products [6]. In some cases, developers may introduce harmful components in their programs and products due to their dependency on third-party service providers and libraries (i.e., the supply chain) [7, 8], or they may need to cause privacy harm to enhance the security of their programs (e.g., anti-fraud measures). In this

topic, we presented and discussed developer- and user-studies, metrics and methodologies to understand whether existing software development practices are aligned with regulatory requirements, and if users are aware of their digital rights and the potential threats inherent to the use of connected devices and software.

3. **Technology for compliance, certification, and enforcement.** This block aimed to explore the gap between legal requirements and software analysis. Software analysis and verification methods can play a fundamental role in aiding developers to make their products compliant with regulation, but also in enabling certification and enforcement actions by validating program and device security and privacy properties without any access to device code and specifications using black-box testing methods. We wanted to first evaluate to which extent regulatory requirements can be automatically verified without human involvement, and which ones are ambiguous and open to interpretation. A fundamental concern is about the fitness of current testing methods – proposed by academia as well as by industry – to automatically verify and certify all the properties and security requirements of regulatory frameworks, at scale [9]. This is a complex and hard problem to solve, as there are open research and technical challenges to enable fully automated software testing, even more if it must be done from a regulatory perspective. In fact, most prior work neglects the highly interconnected and complex nature of modern programs, which often interact with neighbouring devices and with their environment [10]. In this seminar, we wanted to integrate the perspective of regulators and cybersecurity agencies, cybersecurity researchers, software engineering researchers, and industry to gather their opinions about how software testing can enable compliance, certification, and enforcement. We wanted to put a special focus on efforts targeting privacy and security analysis of consumer-oriented mobile applications and IoT products, and discuss the applicability, limitations, and strengths of both white- and black-box testing methods for pre- and post-release analysis. We wanted to discuss a research agenda to develop new methodologies that can effectively aid developers at the design, development, and release stages (white- and gray-box testing), and both regulators and certification authorities (black-box testing).

The search for answers to the above technical questions was also intended to help to generally illuminate other orthogonal questions that relate more to the future research agenda in this field and to future policy-making and regulatory enforcement actions.

4 Seminar Participants

Mila Dalla Preda, Serge Egelman, Anna Maria Mandalari, Narseo Vallina-Rodriguez

We designed our seminar structure (discussed in Section 2.5) and the list of invited participants with different backgrounds and expertise to create the right environment for discussing these three intertwined socio-technical topics.

The diverse set of participants covers a broad range of research areas and stakeholders like industry and regulators which are relevant for CRA implementation and enforcement: (i) black-box testing, formal methods, and runtime compliance to help address technical

aspects of the EU Cyber Resilience Act; (ii) supply chain analysis, vulnerability detection, and attribution to provide insights into securing complex, multi-component systems; and (iii) human factors, patching, and automatic updates to discuss practical implications for end-users.

Thanks to this multidisciplinary set of participants, the seminar has benefited from a balanced perspective, fostering discussions that bridge technical solutions and policy requirements with research efforts for the adoption and enforcement of the Cyber Resilience Act.

5 Overview of the Talks

This section describes the three talks of day 1.

5.1 Seminar Introduction

On the first day, seminar organizers delivered a talk to introduce the seminar motivation and goals, highlighting the critical importance of the CRA and the research challenges it opens. This talk emphasized the seminar's goal of fostering collaboration and generating a constructive and multi-disciplinary analysis of the EU Cyber Resilience Act and its challenges, leveraging the experience gained with previous regulations such as the EU GDPR and COPPA.

5.2 The EU Cyber Resilience Act

Christin Hartung-Kümmerling (BSI – Freital, DE) and Anna Schwendicke, (BSI – Freital, DE)

In today's world, many products with digital elements are affected by cyberattacks as they lack cybersecurity. The provision of security updates is often inconsistent and insufficient. Additionally, users often do not have the needed access to information that would enable them to choose products that are more cyber-secure. The upcoming Cyber Resilience Act (CRA) therefore addresses these problems as it regulates the market access in form of horizontal European cybersecurity requirements for a broad range of digital products and services. Cybersecurity will be addressed throughout a product's lifecycle – from development until the end of the support period. CRA is part of the New Legislative Framework, a framework meant to improve the internal market by setting up rules for market surveillance and conformity assessment. The CRA extends said framework from safety to security for the first time on a broad basis. It is demanding compliance to security requirements relating to the properties of products with digital elements, extensive information for users, as well as vulnerability management throughout a defined support phase. As security is not a stable state, continuous monitoring is necessary in order to ensure that a product's vulnerabilities are handled in time before they can be used as gateways for cyberattacks. Without knowing a product's contents it is, however, impossible to make any statement regarding its security. As a means to have more clarity about the software components of products, the CRA requires manufacturers

to draw up a software bill of materials (SBOM) in order to facilitate their vulnerability handling. The SBOM does not have to be published, but market surveillance authorities can request them. The German Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik) has published technical guidance on SBOM by defining formal and technical requirements, which will help manufacturers to draft one. Once the CRA is adopted, there will be an implementation period in order to set up the necessary infrastructure and to give manufacturers time to prepare. Manufacturers have to report actively exploited vulnerabilities and severe security incidents starting 21 months after the CRA has entered into force and fulfill all other CRA requirements 36 months after the date of entry into force. As certain products require a third-party conformity assessment Member States have to ensure that there are enough notified bodies available to carry out this task. Therefore, each Member State has to have established the required notification infrastructure 18 months after the regulation has entered into force and ought to have enough notified bodies available 24 months after the CRA has come into effect.

5.3 Experiences from GDPR adoption and enforcement

Vincent Toubiana, CNIL – Paris, FR)

The GDPR, implemented in May 2018, will soon turn six years old. In this talk, Vincent Toubiana – Head of LINC (CNIL's Digital Innovation Lab – gave a quick introduction to GPRD enforcement process at CNIL: describing the enforcement chain (complaint, audit/-controls, sanctions) and discussing the challenges that emerged, how they were handled and the success in enforcement. The talk identified key lessons from 6 years of GDPR enforcement that could be applied to the EU Cyber Resilience Act. Several topics, in fact, were discussed: (i) the need and challenges to synchronize and foster collaboration with other DPAs and other authorities that get new responsibilities and competences, (ii) the adaptation to a changing jurisprudence (on concepts such as personal data and what happens when certain cases are elevated to the European Court of Justice), (iii) the estimation of economical impact, which can be intertwined with data protection and market competition challenges, and (iv) technical challenges for easing enforcement and regulatory control in cases such as dark patterns or guidelines for the correct use of web cookies.

6 Breakout Sessions

The identified topics for the three working groups were:

1. Analyzing the developer ecosystem and their incentives for compliance, including communication channels for responsible disclosures and developer obligations towards them and supply chain concerns.
2. The status of existing standardization efforts relevant for CRA compliance.
3. Regulatory compliance and enforcement, including independent assessment and product life-cycle management.

Seminar participants rotated between these breakout groups to better capture their different perspectives and experiences in these three aspects, particularly with regards to

the implementation and enforcement of prior tech policies. After each breakout session, we organized a plenary meeting to present the conclusions of the different groups and identify (i) synergies between them, (ii) research challenges and (iii) potential areas for discussion.

6.1 Working Group 1: Developer Ecosystem

The objective of this session was to delve into the intricacies of the developer ecosystem concerning the EU Cyber Resilience Act (CRA). The discussions aimed to identify and address the challenges developers may face in complying with the Act, particularly in areas such as software development practices, vulnerability disclosure, lifecycle management, and secure-by-default standards.

Developer Awareness

During the first year after its implementation, CRA's primary goal is to promote developer awareness. This campaign must be performed at a global scale, as CRA will impact on any manufacturer or software developer targeting the EU market. Although the provisions of CRA might appear vague and high-level (as we will discuss in the context of current standards), their consequences are broad and global. In fact, it is important to first understand whether developers will perceive CRA as a challenge or a barrier that may impact their processes and business. Since the CRA makes a distinction in compliance obligations based on the risk-category/type of product/service and not the size of the firm that offers those, the CRA is asymmetric but only with regards to product type, not in terms of compliance obligations and resulting cost. This could lead to a crowding out of small firms in some contexts (e.g., limited resources and mechanisms to comply). These aspects highlight the need for agencies to start awareness campaigns promptly, drawing from lessons learned from previous regulations like GDPR by CNIL and other EU Data Protection Agencies.

This first awareness stage opens interesting research opportunities to measure the effectiveness of these campaigns to raise developer awareness. It is still unclear which channels and mechanisms regulators will use to effectively raise global awareness. We propose utilizing platforms like mobile and IoT platform app stores and technical development forums (e.g., StackOverflow) for raising awareness and facilitating communication between regulators and developers. Seminar participants emphasized that these efforts must be accompanied by well-grounded and pragmatic standardization processes – still an ongoing process – , to provide comprehensive technical documentation that can facilitate compliance and understanding of current regulatory requirements. By addressing these key areas and questions, regulators and developers can work together to ensure effective compliance with CRA, fostering a more secure and resilient software development ecosystem.

Facilitating Self-Attestation and Testability

The CRA requires vendors to perform self-attestation on certain security properties (e.g., use of cryptographic functions),[1] meaning they must internally assess and document their compliance with the Act's security requirements throughout its life-cycle; i.e., from the designing to the post-release stages of the product. However, these requirements vary depending on the criticality of the product, and they do not seem well-specified. Consequently,

[1] https://www.enisa.europa.eu/publications/cyber-resilience-act-requirements-standards-mapping

clear definitions of the responsibilities and liabilities of developers and vendors are essential to avoid uncertainty and ensure compliance but rule requirements are still too high level. One discussion revolved around whether these points may become more concrete as standards get developed. This clarity could be enhanced through collaboration with platforms like GitHub, developer forums and events, and other development repositories, and involving more actively the research community in this process.

The base of secure-by-default assessments raises questions: *Will it be done via checklists or based on a set of standards?* This approach has proven ineffective in prior regulatory contexts such as the USA COPPA rule, even when assisted by organizations forming part of certification schemes [7]. We suggest that we need more process-oriented approaches, focusing on a methodology rather than a simple checklist, similar to the SSDF NIST SP800-218 framework.[2] Creating guidelines and clear procedures is vital for enabling seamless compliance and fostering a secure software development environment. These frameworks, tools, and processes – currently non-existent – could be integrated into Integrated Development Environment (IDE) tools, which would indeed open exciting research and market opportunities. For instance, formal verification tools or tools for automatic Software Bill of Material (SBOM) generation and management could be developed and integrated into IDEs, providing centralized repositories of libraries to help developers manage dependencies effectively. Yet, while self-attestation encourages vendors to proactively identify and fix security issues and comply with regulatory requirements, it is possible that certain vendors may have incentives to avoid compliance and elude external controls. Consequently, this opens an interesting research problem that involves developer studies and empirical approaches to understand developer incentives and the effectiveness of various self-attestation approaches to reduce the number of vulnerable devices in the EU market. st." SSDF NIST SP800-218 (`https://csrc.nist.gov/projects/ssdf`).

Software Supply Chain (SBOM)

A significant amount of seminar time and effort focused on **Software Bill of Materials (SBOMs)**[3] extraction and generation. SBOMs are a key concept in the CRA because they provide a comprehensive inventory of all components and dependencies in a digital product, which is crucial for identifying and managing vulnerabilities. SBOMs enhance transparency and security by allowing regulators and developers to trace, verify, and address potential risks throughout the software supply chain. Therefore, ensuring the accuracy and trustworthiness of SBOMs is essential but, *can SBOMs released by developers and vendors be entirely accurate? Should developers' self-disclosed SBOMs be trusted?*

While the German Federal Office for Information Security (BSI) and other EU national agencies have released guidelines for SBOM generation and management,[4] it is known that vendors and developers face challenges in keeping track of all dependencies when integrating open-source tools and third-party code, as many of their dependencies can be proprietary black-boxes outside their control [5, 3, 6, 8]. Additionally, as several research studies show, developers also struggle at maintaining effectively their dependencies: prior work results show that app developers only slowly adapt new library versions, exposing their end-users to large windows of vulnerability [1].

---

[2] `https://csrc.nist.gov/pubs/sp/800/218/final`
[3] `https://www.cisa.gov/sbom`
[4] `https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03183/TR-03183_node.html`

This complex scenario is compounded by the high number of supply-chain attacks that can negatively impact the security guarantees of a digital product. However, one discussion point was about the level of information expected to be disclosed by developers about their dependencies, and whether this will be effective at tackling issues such as those described by Backes *et al.* [1]. This opened a discussion about the need for proper labeling [3], and how to include versioning (and customization, as for example in open-source libraries) of dependencies in the SBOMs throughout the whole lifecycle of the product, as libraries and dependencies can experience multiple changes and releases along the supply chain. This may have direct consequences on users' security. For example, *will all developers using open-source tools maintain and send upstream patches to their products to fix vulnerabilities they have found in their products? Will they have the right mechanisms to ensure that all their customers get the patches?*

Establishing a reliable method to gain control over the supply chain and verify the correctness of SBOMs using both black- [5] and gray-box [6] testing techniques is essential, especially when considering the potential lack of developer awareness or in cases of potentially deceptive developers. Microsoft has developed open-source tools for SBOM generation.[7] [8] These tools could be integrated into IDEs to raise awareness and would benefit from a community-built repository of third-party library fingerprints for detection. However, we note that creating such repository is a daunting effort (particularly in terms of maintaining it due to versioning and – in the case of commercial libraries offering analytics and advertising SDKs – due to company merges and acquisitions). Moreover, it is also known that fingerprint-based methods with static analysis methods can easily introduce false positives (e.g., identifying libraries that may not be actually integrated in the code), and false negatives (e.g., not identifying libraries in obfuscated programs), as the research literature in the mobile domain has shown [9, 5]. One challenge would be how to extract SBOMs from software running in the cloud, either partially or entirely as in the case of Amazon Skills [4]. In these scenarios, the platform could do the dependency checks, however there are lambda functions that can be used by deceptive developers to avoid scrutiny.

Shadow libraries and dependencies, i.e., where developers (partially) copy-paste someone's code to take responsibility, might make it difficult to fix critical code as these developers may be using under-resourced/homebrew code without investing in its testing/development/-maintenance.

In fact, many vulnerabilities manifest across connections between chunks of code. Therefore, it is necessary to manage the exposure to responsibilities for these problems. For instance, an incorrect use of methods provided by a cryptographic library can have devastating consequences for software security. Unfortunately, the concept of SBOM may only reveal that a particular library is used but not such development errors.

Participants pointed out that most scenarios will require SBOM extraction and generation from binary files since developers may introduce libraries during compilation time or even compiled products with incomplete SBOMs [2]. There is a risk of an entity not knowing what chain of dependencies are in their software, and automation could reveal unexpected hidden

[5] Black-box testing or closed-box testing is a form of software testing that is performed with no knowledge of a system's internals, and it can be carried out to evaluate the functionality, security, performance, and other aspects of an application.

[6] Gray-box testing is a method you can use to debug software and evaluate vulnerabilities with some but limited knowledge of the workings of the component being tested.

[7] `https://github.com/microsoft/component-detection`

[8] `https://github.com/microsoft/sbom-tool`

risks. Yet, it is an open research challenge to check the correctness of SBOMs from binaries, especially for regulators needing to verify vendors' and developers claims. This may have legal consequences given EU laws prohibiting reverse engineering as we will discuss in §6.1.

Several tooling systems are available to aid this process, such as OWASP CycloneDX[9] and SPDX[10] by the Linux Foundation. It is important to ensure developers do not run scared if there is too little information available, making the compliance process too daunting. CRA may result in more awareness of what elements the code is linking to. A kind of 'dependency amnesty' could encourage those down the chain to provide an SBOM. Otherwise, each developer needs to know all the code they use, even if it's in a library made by someone else. ol and the high number of supply chain attacks that can negatively impact on the security guarantees of a digital product. It is essential establishing a reliable method to gain control over the supply chain and verify the correctness of SBOMs using both gray- and black-box testing techniques as questions arise about when to trust an SBOM disclosed by the developer due to lack of developer awareness or in the case of potentially deceptive developers. Another discussion point was regarding how to do labeling and versioning of SBOMs throughout the whole lifecycle of the product as libraries and dependencies can experience multiple releases.

Effective and Transparent Vulnerability Disclosure Processes

Vulnerability disclosures are critical in the context of the CRA as they ensure that all identified security weaknesses are promptly reported and addressed to the software developer/vendor when identified, thereby reducing the risk of exploitation. By mandating transparent and timely disclosure of vulnerabilities, the CRA aims to foster a culture of accountability and continuous improvement in software security, thus enhancing the resilience of digital products and protecting consumers and businesses from cyber threats.

The research community, including organizations like OWASP,[11] has established several best practices for responsible disclosures to ensure that security vulnerabilities are addressed effectively and ethically. Generally, these practices involve a coordinated process where researchers privately notify the affected vendors about the discovered vulnerabilities, providing them with detailed information and a reasonable time frame to develop and deploy fixes. The standard time frame for fixing a security issue is around 90 days, although this can vary depending on the severity of the vulnerability and the complexity of the fix required and the challenges to demonstrate evidence of in-the-wild exploitation. Researchers are encouraged to maintain confidentiality and offer assistance during this period. In practice, there are many challenges and hidden incentives that often impede proceeding according to these best practices. As discussed in the seminar, vendors and software developers are not always proactive in releasing patches for their products, and researchers often struggle at finding the right communication channel or contact point at a particular vendor. Additionally, defining what constitutes a vulnerability is complex, with debates on whether all vulnerabilities require a CVE [12] and how to handle vendors that do not acknowledge some vulnerabilities (i.e., *"won't fix"*). In fact, the CVE format, while widely used by the security community, is not always the best option. Examples are attacks related to personal data access or privacy concerns.

---

[9] `https://cyclonedx.org/`

[10] `https://spdx.dev/`

[11] `https://cheatsheetseries.owasp.org/cheatsheets/Vulnerability_Disclosure_Cheat_Sheet.html`

[12] CVE stands for Common Vulnerabilities and Exposures. CVE is a glossary that classifies vulnerabilities. The glossary analyzes vulnerabilities and then uses the Common Vulnerability Scoring System (CVSS) to evaluate the threat level of a vulnerability.

When a developer claims that a reported vulnerability is actually a feature and decides not to fix it, it presents a significant challenge in the responsible disclosure process. This situation requires careful handling to ensure security concerns are addressed without dismissing valid reports. Researchers should document their findings thoroughly and provide a clear explanation of why the identified issue constitutes a vulnerability, including potential risks and impact on users. They can escalate the matter by seeking a second opinion from independent security experts and even openly disclose the vulnerability to raise broader awareness (e.g., through interactions with the press or academic publications). In some cases, involving regulatory bodies or industry standards organizations may be necessary to resolve the dispute and ensure that security vulnerabilities are not overlooked under the guise of being a feature. This approach helps maintain a balance between legitimate security concerns and the developer's design choices, ensuring that user safety remains a priority. CRA articles 32-34 and ENISA's "Good Practices for Vulnerability Disclosure"[13] set minimum requirements for vulnerability disclosures and offer detailed guidance on handling and disclosing vulnerabilities, including scenarios where there might be disagreements on whether an issue is a vulnerability. In the USA, CISA has also defined a new framework for documenting vulnerabilities. It will be important to monitor if CRA will have a positive impact on the responsible disclosure process to ensure that vendors effectively take measures.

Yet, regulators face the challenge of ensuring that every vulnerability is disclosed, clearly defined, and ultimately patched in the products. Moreover, the risk of criminalizing researchers who find vulnerabilities exists: while reverse engineering is usually allowed for achieving interoperability, research, and security analysis, companies can decide to take legal action against security researchers. Additionally, there is the potential exploitation of identified vulnerabilities by authorities as part of this process that could be used for cyberwarfare, such as zero-day exploits. It would be necessary to facilitate mechanisms to increase the transparency of these processes and the interactions between researchers and vendors, hence increasing public awareness on patched and unpatched vulnerabilities.

CRA opens multiple interesting research and industrial opportunities in the context of vulnerability disclosure and product lifecycle management. For example, better defining what a vulnerability constitutes (would privacy threats fall in this context?), finding effective means for balancing intellectual property protection and security – a challenging socio-technical problem in the context of the CRA – , or conducting empirical measurements to see whether CRA has indeed contributed to fix vulnerabilities in digital products. Performing such empirical analysis would be similar in objectives to those measurements showing whether GDPR has contributed to protect users' privacy on the web. Consequently, measuring the impact of regulations in-the-wild is inherently hard to measure as there is a diffusion process of impacts across digital ecosystems and jurisdictions.

Product Life Cycle Management

Product life cycle management is essential to ensure that security measures are maintained throughout the entire lifespan of a product, from development to end-of-life. This continuous oversight helps in (promptly) addressing and patching emerging vulnerabilities and maintaining compliance with security standards and requirements over time. However, product life cycle support may vary significantly depending on manufacturer/developer incentives

[13] https://www.enisa.europa.eu/publications/vulnerability-disclosure

and security standards, the product type (e.g., a smart bulb vs. a smartphone), so the CRA should include clear and specific vendor requirements tailored to different product categories and their inherent threats.[14]

Seminar participants did not observe strict requirements on how vendors should acknowledge vulnerabilities, the confidentiality clauses (as it can be abused by vendors to avoid fixing issues), and the time required for fixing the vulnerability (Annex I states "without delay"), as well as usability requirements to inform users about the security properties of a product and means to reduce threats or patch products. Based on GDPR experience, it is unclear whether vendors will diligently and clearly inform users, and what will be the temporal support of vendors over their products as, for example in the case of smartphone manufacturers, they will have to dedicate engineering teams to support various product lines with specific hardware requirements. This has been identified as another problem that could be better studied through developer studies and large-scale empirical measurements.

6.2 Working Group 2: Standardization Efforts

Standardization efforts are crucial for facilitating the adoption of the CRA provisions. To ensure compliance, seminar participants consider CRA requirements need to be carefully translated into harmonized (yet realistic and clear) standards that manufacturers can adhere to. Yet, this is still an ongoing effort, so drawing conclusions at this stage is hard and potentially premature.

During the first day, the group began discussing the differences between the existing CE standard (safety-oriented) [15] and the requirements necessary for CRA certification (security-oriented). Specifically, the CRA falls under the New Legislative Framework (NLF),[16] which governs market access and surveillance. This framework comprises several modules that vendors can choose from, such as one that checks the product type and another that documents the development process. Insights from the existing CE marking process tell us that documentation must be held and shown to an authority upon request.

A significant challenge with the CRA is that compliance is much more difficult to measure compared to existing CE rules, which cover safety and measurable aspects like voltage and electromagnetic emissions. Participants discussed whether all CRA requirements can indeed be testable and measurable. The same concerns hold for vendors' compliance.

Some interesting research questions arise from this discussion:

- How can all standardization requirements be operationalized and implemented, and then measured and tested? What are the expectations?
- How does a standard get approved as *"CRA compliant"*? This process involves three recognized European standards organizations – CEN,[17] CENELEC,[18] and ETSI[19] – which write and approve standards according to rules where member states are represented.

[14] CRA article 6 states: *"When placing a product with digital elements on the market, and for the expected product lifetime or for a period of five years from the placing of the product on the market, whichever is shorter, manufacturers shall ensure that vulnerabilities of that product are handled effectively and in accordance with the essential requirements set out in Section 2 of Annex I."*

[15] The CE marking stands for Conformité Européene, or European Conformity marking for a range of product regulations.

[16] `https://single-market-economy.ec.europa.eu/single-market/goods/new-legislative-framework_en`

[17] European Committee for Standardization

[18] European Committee for Electrotechnical Standardization

[19] European Telecommunications Standards Institute

- How do we combine different standards? Looking ahead, we can imagine that we will have a set of established standards, with at least one per sector, possibly leading to competition between standards. These will be complemented by horizontal standards that span multiple sectors.
- How can we re-evaluate standards at regular intervals based on empirical research?
- How do standards adapt to the constant evolution of technology, innovation, threat models and new applications?
- How can we write standards so that compliance is easy, affordable, and automatically verifiable?

ENISA standard

The second day, the group discussed the latest[20] ENISA's standardization guidelines. These aim at identifying relevant existing cybersecurity standards for each CRA requirement, analyzing their scope, and highlighting potential gaps to be addressed. The guidelines help in integrating standards into development processes, ensuring that developers follow secure-by-default principles throughout the product lifecycle.[21]. The file containing the updated version (April 4th 2024, released after the seminar) of the standardization guidelines is available **here**. During the seminar we had access to the previous version of these guidelines and the general observations that we made about the scope and coverage of these standards apply also to the updated version.

As regarding the security guidelines relating to the properties of products with digital elements the group wonders whether there will be tools available to help lower-resourced entities to meet these standards due to asymmetric approaches that may increase the burden to small-size organizations based on the type of product. Moreover, the group collected several observations on the proposed guidelines. For example, the document refers to *"product with digital element"*, this definition should be better specified as in its current form it, for example, also applies to a 1970s radio alarm clock with a digital display. The group also discussed the high level scope and description of requirements, which could be potentially abused by vendors to avoid scrutiny and may not apply to specific types of products and sectors.

The general consensus among participants is that, although the guidelines offer some direction for developing security standards, they still leave several aspects open to interpretation and their scope must be extended to the broad range of digital products, while being flexible enough to catch up any technical development, use-case, and innovation.

Standards and Software Developers

In the latest discussion, the group examined existing standards, including the ETSI *Cyber Security for Consumer Internet of Things: Baseline Requirements* from 2020.[22] Participants noted some outdated recommendations and problematic choices, such as entrusting the threat model to the manufacturer. For example, Provision 5.5-5 states *"device functionality that allows security-relevant changes in configuration via a network interface shall only be accessible after authentication. The exception is for network service protocols that are relied*

[20] As of March 2024
[21] https://www.cyberresilienceact.eu/the-cyber-resilience-act-annex-eu/
[22] https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf

upon by the device and where the manufacturer cannot guarantee what configuration will be required for the device to operate. NOTE 3: Protocols that are an exception include ARP, DHCP, DNS, ICMP, and NTP." In this particular example, this standard leaves fundamental network security improvements by ignoring encrypted versions of some of these protocols such as DNS-over-HTTPS (DoH) and the encrypted version of NTP, known as NTPS.

This approach could allow vendors to avoid liability for certain vulnerabilities or claim that patching is difficult due to the device's nature. The group emphasized that standardization efforts must consider developers' software development approaches, needs, and the complexities of the supply chain. They should also be updated more frequently to incorporate newer security measures and protocols, and unknown exploits.

The group also discussed the need for standards for SBOM (Software Bill of Materials) management and clear definitions of what constitutes a vulnerability and guidelines for the disclosure process that may protect security researchers and consumers from potential enterprise interests. In conclusion, the general opinion is that the definition of appropriate standards may be a challenging task due to the complexity of existing technologies and the constantly evolving threat landscape: standards can quickly become obsolete and give final consumers a wrong sense of security.

6.3 Working Group 3: Regulatory Enforcement

This working group focuses on the discussions and insights related to regulatory enforcement within the context of privacy, compliance, and standardization. Prior research experience from seminar participants in relevant projects and research efforts focused on developing technologies for regulatory compliance and testing, and from their daily activities as software developers, regulators and policymakers were essential for informing this discussion.

This working group discussions are divided into three key subsections: (*i*) Security-by-design and Security-by-default, (*ii*) Measuring and Assessing Compliance, and (*iii*) Enforcement and Standardization. Each subsection delves into critical aspects of regulatory enforcement, exploring the challenges, potential solutions, and strategic approaches necessary for effective implementation.

Security-by-design and Security-by-default

The principles of security-by-design and security-by-default are essential in the CRA, which should be effectively captured in upcoming standards. Specific sectoral security requirements must be clearly defined to establish a comprehensive catalogue for certification and also for a complete catalogue of threat models. Participants consider that reference threat models and Key Performance Indicators (KPIs) are critical for facilitating and measuring CRA adoption. Additionally, understanding the costs of regulatory enforcement and vendors' compliance in relation to their available technical, engineering and human resources is vital.

Mandatory technical documentation for compliance verification, along with third-party assessments or endorsements by trusted Certificate Authorities can help to enhance compliance. However, self-certification can be exploited by deceptive actors, particularly if this process does not involve code reviews or software testing as occurred in the case of organizations participating in the U.S. Federal Trade Commission COPPA Safe Harbor program.[23]

[23] `https://www.ftc.gov/enforcement/coppa-safe-harbor-program`

While attestation at the level of Member States is essential, incentives for data sharing across jurisdictions could improve enforcement and control, particularly benefiting those Member States with less human and technical resources, also reducing the arbitrary decisions that have been observed in enforcing GDPR in certain countries. There are questions about the feasibility and scalability of general auditing tools for devices and whether the Cyber Resilience Act (CRA) provides new tools for enforcement. The duration of attestation and the time required to remove potentially vulnerable devices from the EU market also needs consideration.

The intersection of Intellectual Property (IP) protection laws and the CRA also raises concerns, which may require changes to current intellectual property laws to facilitate reverse engineering for compliance and independent testing. Vendor liability and certification authority accountability, especially if cheating occurs, need examination and consideration. The distribution of responsibilities among supply chain actors for a given service or product, and the exclusion of cloud services from the CRA's scope, focusing solely on device software and hardware, are points for consideration from a research perspective.

To conclude the following questions and observations need to be addressed:

- What are the (broader) economic impacts of CRA enforcement? Which metrics can be used or need to be developed to measure this impact?
- How will the CRA change developers' incentives (e.g., with regard to their R&D efforts)? How will developers perceive the CRA and how will they respond to it? Will they view it as a burden or a beneficial regulation, and will they try to avoid regulatory scrutiny as seen with GDPR?
- Implementation of security-by-design principles in complex devices like IoT.
- Consideration of manufacturer disclaimers to avoid scrutiny and limit liability.
- Development of device and software verification standards and guidelines, both for device manufacturers and for independent certification authorities (and labs) or regulatory bodies. [24]
- Concerns that developers might perceive the CRA as a burden, similar to GDPR, potentially leading to non-cooperation with regulatory investigations, to avoid regulatory scrutiny (e.g., anti-testing) or barriers for small firms to enter the market and innovate, thus potentially stifling innovation by such firms.

Measuring Compliance and Enforcement

In this discussion, group members examined the methods and challenges associated with measuring CRA compliance and standard adoption. The discussion covered various approaches and tools for verification, as well as the potential benefits and drawbacks of different strategies.

Effective measurement of compliance with standard adoption requires the development of testable guidelines for technologies that ease the integration of Continuous Integration (CI) tools for standard verification. Software-based compliance verification is proposed as a potentially more effective alternative to traditional certification authorities, based on check-lists. Additionally, the potential for IoT Industry alliances (e.g., IoxT[25]) and their certifications to satisfy CRA requirements needs careful consideration. Establishing clear guidelines by device categories and addressing the gap between certification, adoption guidelines, and enforcement is crucial for compliance.

[24] https://owasp.org/www-project-iot-security-verification-standard/
[25] https://www.ioxtalliance.org/

Enforcement and standardization are closely intertwined, particularly within the framework of the CRA and its voluntary certification program. Effective regulatory enforcement necessitates the alignment of these efforts with standardization processes, while also addressing the challenges posed by Intellectual Property laws. The complexity of identifying trustworthy certification programs is compounded by varying national accreditation systems and the emerging market for certification schemes. Yet, the creation of standards discussed earlier, also necessitates sufficient resources and authoritative bodies, with the current reliance on industry proposals posing a limitation. The US system, such as NIST's Cybersecurity CMMC[26] could serve as a viable model.

While the tools for CRA enforcement are yet to be determined, they are anticipated to be clarified with the law's approval. However, these regulatory efforts must be aware of the limitations of current software testing methodologies, particularly in terms of scope and scale (not to mention the testability of specific regulatory requirements). Proposals include self-assessment for low-risk products and a EU-wide certification framework for high-risk products, with the European Commission expected to publish a list of high-risk categories. This requires observing these developments and analyzing their alignment with current white- and black-box testing capabilities for device and software security analysis.

The evolving interplay between regulatory enforcement, standardization, and economic impacts underscores the need for precise definitions of enforceable properties, robust evaluation and compliance tools, and comprehensive certification processes. Moving forward, participants believe that the success of the Cyber Resilience Act (CRA) will depend on aligning these efforts with existing software engineering and analysis frameworks, and adapting intellectual property laws like the EU Copyright Act. These are necessary measures to ensure thorough and effective regulatory enforcement.

- How can we measure the compliance of standard adoption and regulatory compliance in various sectors, particularly complex consumer IoT products integrated in multi-party and multi-agent environments?
- What are the differences between the scope of existing guidelines and CRA ultimate goals, and how can guidelines be tailored by device categories (e.g., IoT) or sectors?
- (How) Can the efforts started by IoT industrial alliances (e.g., IoxT), including standardization and certification processes, be leveraged for CRA compliance?
- Can standard and CRA requirements be integrated into CI tools to automate verification prior release?
- How can the balance between intellectual property protection and CRA compliance be managed? Are changes to intellectual property laws necessary to facilitate CRA enforcement and independent verification?
- What are the liability implications for vendors and certification authorities (and labs) if they are found to be non-compliant?
- What role will gatekeeping intermediaries and stakeholders, such as platform operators, e-commerce platforms and software distribution channels, play in removing non-compliant software/products from their platforms?
- What tools or frameworks can complement certification authorities with software-based test cases (black-box) for automated and independent compliance verification?
- What white-box and black-box tools can aid self-assessment for compliance based on risk, particularly for low-risk and high-risk products and the supply chain?
- What principles and methodologies of current certification processes from other regulated markets, such as food safety regulations or aerospace, be adapted to CRA?

[26] https://www.nist.gov/mep/successstories/2020/leading-way-cmmc-compliance

7 Conclusions

In the final plenary meeting, all seminar participants gathered to focus on the main challenges related to standardization, the developer ecosystem, and enforcement of the CRA. Through this discussion, participants collectively identified the research challenges and opportunities described in § 7.1.

We note that addressing these challenges requires collaboration across various disciplines and stakeholders. In fact, a few weeks after this Dagstuhl seminar, the European Commission has updated the CRA requirements, partially addressing some of the concerns raised by the participants.[27]

7.1 Opportunities

Developing and Monitoring the Development of CRA Standards:

Standardization bodies must establish and refine comprehensive standards and guidelines for CRA quickly. These should offer guidance on the scope of the regulation and consider sector-specific or device-specific requirements. The research community must evaluate whether these requirements align with threats and risks identified by the community on consumer-oriented products to effectively protect consumers and identify vendors with deceptive and insecure practices. It is also fundamental to investigate how digital platforms and software distribution platforms can help mitigate the impact of malicious actors through guidelines and publication policies as in the case of the COPPA and GDPR regulations (e.g., collection of unique identifiers and other data types in children-oriented apps).

Informing the Development of Standardization Efforts and Guidelines:

The development of standards and guidelines is fundamental for CRA adoption and compliance. We must have a multi-disciplinary debate to develop these standards and guidelines, and to analyze and discuss the scope of new standards, including the necessity for sector-specific standards. Regulators should actively promote these standards and provide clear, specific guidance on compliance, learning from the adoption and enforcement pitfalls of GDPR: standardization efforts should go hand in hand with tools for assessing compliance by vendors. The research community could inform these efforts and assess their scope and effectiveness, drawing on their research experience with consumer IoT devices and cybersecurity.

Understanding Developer Awareness and Compliance:

It is essential to conduct longitudinal developer-oriented studies (e.g., surveys) to gauge developer awareness, readiness, and incentives for compliance with CRA requirements. To maximize success, these efforts could be done in collaboration with regulatory bodies and digital platforms and marketplaces. We also consider important to encourage contributions to open-source projects by providing incentives, and addressing legal and IP issues to balance security and independent certification, with innovation. In fact, transparency regarding security guarantees (e.g., vulnerability patching) and obligations from vendors to users is crucial. Considerations of usability and incentives are also important (for instance, if someone

[27] https://www.europarl.europa.eu/doceo/document/TA-9-2024-0130_EN.pdf

buys an expensive smart refrigerator that is later found to be vulnerable, do users have incentives to isolate it as it will become just a regular fridge?). What legal expectations are there for such situations? It is important to consider the impact of CRA on the economy, including consumer expectations, market adoption, and international implications.

Creating Methodologies and Tools:

Once standards are in place, it is key to develop methodologies and tools to assist developers with compliance, including tools for SBOM generation and vulnerability management. We also advocate for and support research in formal verification methods to ensure the accuracy and reliability of SBOMs and other compliance measures that developers can use during the design and development of their products. This is especially important for resource-constrained organizations with limited financial resources. Yet, these tools must be complemented with others for independent testers (e.g., regulators, certification authorities, researchers) to facilitate external certification and assessment, recognizing that self-attestation and check-list based approaches may not always be effective. These efforts must investigate the feasibility and scalability of developing a general tool for auditing devices under CRA, and assessing the testeability of certain regulatory requirements. We must not ignore usability considerations and developer incentives for using these tools and maintaining product security throughout their life cycle. While there are companies and research efforts already offering tools for managing SBOMs, the experts expressed concerns regarding the technical challenges of SBOM generation and the aptness of regulatory requirements, which only require developers to disclose high-level dependencies. We consider essential creating effective black-box analysis tools for library version detection as it is critical for pin-pointing specific program vulnerabilities.

Public Outreach and Transparency:

Increase public outreach efforts to enhance transparency regarding security guarantees and mitigations offered by vendors, considering usability and incentives for users. Furthermore, regulators need to actively inform and guide vendors on CRA compliance requirements to avoid the pitfalls experienced with GDPR.

Multi-Disciplinary Longitudinal Analysis:

We consider key to study the overall economic impact of CRA enforcement and develop metrics to evaluate this impact. This will allow us to assess developer perceptions of CRA to understand to which extent it is seen as a burden and in which respects it is seen as a necessary and appropriate regulation by vendors. We recommend performing active scans of the EU's Internet Protocol (IP) address space to monitor the deployment of legacy non-compliant devices with public IP addresses and assess CRA's impact on replacing or isolating them.

Several participants urged for a Systematization of Knowledge (SoK) on CRA, focusing on informing the research community about this new regulation and the identified cross-disciplinary research challenges. Additionally, we considered the need to establish an EU MSCA-ITN (Marie Skłodowska-Curie Actions Innovative Training Network) to train future CRA experts with the necessary multidisciplinary background and skills.

Acknowledgements

We would like to thank and acknowledge the support that the staff of Schloss Dagstuhl has provided us before and after the seminar, as well as for their hospitality. We would also like to mention the active contribution of all the seminar participants, who have helped to ground the implications of a broad regulation with significant and global impact on software development, markets, and cybersecurity, in a scientific research agenda that will need to be addressed in the coming years. The contributions by Narseo Vallina-Rodriguez and Juan Tapiador were possible thanks to the EU H2020 TRUST aWARE project (GA 101021377). The work of Anna Maria Mandalari was supported by the EPSRC PETRAS (EP/S035362/1). The contributions of Simon Parkin were supported by the INTERSCT project, Grant No. NWA.1160.18.301, and RAPID project (Grant No. CS.007), both funded by Netherlands Organisation for Scientific Research (NWO). The contributions by Guillermo Suarez-Tangil were possible thanks to TED2021-132900A-I00 funded by MICIU/AEI /10.13039/501100011033 and the EU NextGenerationEU/ PRTR. The contribution by Volker Stocker was possible thanks to funding from the Federal Ministry of Education and Research of Germany (BMBF) under grant no. 16DII131 (Weizenbaum-Institut für die vernetzte Gesellschaft – Das Deutsche Internet-Institut).

References

1. Michael Backes, Sven Bugiel, and Erik Derr. Reliable third-party library detection in android and its security applications. In *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*, pages 356–367, 2016.
2. Tingting Bi, Boming Xia, Zhenchang Xing, Qinghua Lu, and Liming Zhu. On the way to sboms: Investigating design issues and solutions in practice. *ACM Transactions on Software Engineering and Methodology*, 2023.
3. Peter Caven and L Jean Camp. Towards a more secure ecosystem: Implications for cybersecurity labels and sboms. *Available at SSRN 4527526*, 2023.
4. Jide S Edu, Xavier Ferrer-Aran, Jose Such, and Guillermo Suarez-Tangil. Skillvet: automated traceability analysis of amazon alexa skills. *IEEE Transactions on Dependable and Secure Computing*, 20(1):161–175, 2021.
5. Álvaro Feal, Julien Gamba, Juan Tapiador, Primal Wijesekera, Joel Reardon, Serge Egelman, and Narseo Vallina-Rodriguez. Don't accept candy from strangers: An analysis of third-party mobile sdks. *Data Protection and Privacy: Data Protection and Artificial Intelligence*, 13:1, 2021.
6. Julien Gamba, Mohammed Rashed, Abbas Razaghpanah, Juan Tapiador, and Narseo Vallina-Rodriguez. An analysis of pre-installed android software. In *2020 IEEE symposium on security and privacy (SP)*, pages 1039–1055. IEEE, 2020.
7. Irwin Reyes, Primal Wijesekera, Joel Reardon, Amit Elazari Bar On, Abbas Razaghpanah, Narseo Vallina-Rodriguez, Serge Egelman, et al. "won't somebody think of the children?" examining coppa compliance at scale. In *The 18th Privacy Enhancing Technologies Symposium (PETS 2018)*, 2018.
8. Trevor Stalnaker, Nathan Wintersgill, Oscar Chaparro, Massimiliano Di Penta, Daniel M German, and Denys Poshyvanyk. Boms away! inside the minds of stakeholders: A comprehensive study of bills of materials for software systems. In *Proceedings of the 46th IEEE/ACM International Conference on Software Engineering*, pages 1–13, 2024.
9. Yafei Wu, Cong Sun, Dongrui Zeng, Gang Tan, Siqi Ma, and Peicheng Wang. {LibScan}: Towards more precise {Third-Party} library identification for android applications. In *32nd USENIX Security Symposium (USENIX Security 23)*, pages 3385–3402, 2023.

Participants

- Rainer Böhme
Universität Innsbruck, AT
- Mila Dalla Preda
University of Verona, IT
- Daniel J. Dubois
Northeastern University – Boston, US
- Carolyn Egelman
Google – Mountain View, US
- Serge Egelman
ICSI – Berkeley, US
- Hamed Haddadi
Imperial College London, GB
- Christin Hartung-Kümmerling
BSI – Freital, DE
- François Hublet
ETH Zürich, CH
- Martina Lindorfer
TU Wien, AT
- Anna Maria Mandalari
University College London, GB
- Federica Maria Francesca Paci
University of Verona, IT
- Simon Parkin
Delft University of Technology, NL
- Sergio Pastrana
Carlos III University of Madrid, ES
- Joel Reardon
University of Calgary, CA
- Anna Schwendicke
BSI – Freital, DE
- Ben Stock
CISPA – Saarbrücken, DE
- Volker Stocker
Weizenbaum Institut – Berlin, DE
- Guillermo Suárez-Tangil
IMDEA Networks Institute – Madrid, ES
- Juan Tapiador
Carlos III University of Madrid, ES
- Vincent Toubiana
CNIL – Paris, FR
- Narseo Vallina-Rodriguez
IMDEA Networks Institute – Madrid, ES