Editors: Fabio Massacci, fabio.massacci@unitn.it | John Steven, john@zernorth.io

The Challenges of Software Cybersecurity Certification

José L. Hernández-Ramos | European Commission, Joint Research Centre
Sara N. Matheu and Antonio Skarmeta | University of Murcia

In 2019, the new European Union (EU) cybersecurity regulation "Cybersecurity Act" ("CSA")[1] entered into force to create a common framework for the certification of any information and communication technology (ICT) system, including products, services, and processes. The main purpose of this framework is to reduce the current fragmentation of cybersecurity certification schemes[2] as well as to increase end users' trust in a hyperconnected society[3] by fostering a mutual recognition of certified ICT components in any EU country.

Despite the expected benefits of cybersecurity certification in terms of transparency for end users and the use of best practices, software providers still consider cybersecurity certification to be a costly and complex process. Indeed, certification could cause delays in the launch of new systems, with a significant economic impact.[4] So, from the industry's perspective, why should companies invest time and money in certifying ICT components and systems? This is not an easy question to answer, as security and privacy are not yet highly demanded features, due to a lack of awareness.[5] The consequence is a vicious circle in which the lack of demand (or awareness) and the required effort cause software providers to oppose applying certification processes that, in turn, would increase user awareness.

In this context, we believe that the realization of the cybersecurity certification framework promoted by the CSA is key to fostering transparency and trust and, consequently, awareness of ICT systems' cybersecurity. However, it requires the joint effort of certification bodies, manufacturers, and software providers so that an ICT system is certified according the cybersecurity of its software components. This aspect could be addressed through the inclusion of cybersecurity requirements in the development, maintenance, and operation of software components in certification schemes, as mentioned by a recent report from the EU Agency for Cybersecurity (ENISA).[6] However, other challenges also need to be addressed. Thus, our main goal is to increase the awareness of the challenges of cybersecurity certification so that the accreditation's benefits can be leveraged by end users through a more trustworthy digital ecosystem. Based on recent reports provided by ENISA[4,6] and according to our own experience in this area,[7] some of these aspects include the following:

- Definition and certification under different assurance levels; those levels are defined by the CSA and need to be considered by certification bodies and manufacturers when certifying their systems.
- Software composability and software updates, which impact the certification of a whole system and its components during their lifecycle; these aspects are of interest to manufacturers and software providers as well as cybersecurity certification practitioners for defining the relationship between different certification schemes.
- Development of coordinated vulnerability disclosure (CVD) procedures, which must be followed by vulnerability providers (e.g., a certain company or cybersecurity researcher) to maintain software providers' control of their systems.

Cybersecurity Certification Assurance Levels

The first problem concerns what must be certified and how deeply. The evaluation of a software component should consider the system where the component will be deployed as well as the different levels of assurance for the certification process. These assurance levels are defined by the CSA regulation to indicate the rigor and depth of the certification process

Digital Object Identifier 10.1109/MSEC.2020.3037845
Date of current version: 25 January 2021

(self-assessment, basic, substantial, and high) to harmonize the different levels provided by existing certification schemes. For example, the well-known Common Criteria Scheme[8] already defines its own evaluation assurance levels, with the same purpose. This way, a software component could be evaluated according to a certain assurance level, considering the context and the domain where it will be used. However, this could be unknown when a component is created, or the same component might be deployed in systems that are certified under different assurance levels and contexts.

Should the same software component be certified several times according to different assurance levels and contexts where it might be deployed?

This could make software providers more reluctant to use certification processes if lightweight and efficient approaches are not in place. Furthermore, the fulfillment of a certain assurance level should be measured according to agreed cybersecurity standards. However, there is a lack of standardized and widely used approaches to carry out these processes.[9] This could reduce users' trust in the cybersecurity certification of software components. Indeed, end users could find it difficult to compare the cybersecurity level of various ICT systems that were certified with various schemes or based on different standards. Consequently, the use of a harmonized set of standards for different assurance levels is a key factor for the cybersecurity certification process.

Software Composability

A single ICT system could be made up of components and subsystems that have additional software modules. Therefore, the system's cybersecurity certification depends on the accreditation of each of its subsystems and software components. However, each of these components may have been certified by using different schemes and assurance levels. Therefore, the question becomes,

How should the different certifications of each component be assembled to compose a system's cybersecurity certification?

Furthermore, the development of a software component may not be linked to a specific product or system. Thus, the certification of a module in certain hardware and in a particular operating system may not be valid for the composition of a specific system. This aspect could hinder the potential reuse of previous certifications for the accreditation of a whole system. In this case, it is important to identify which information from the certification process could help to avoid (at least partially) the recertification of a component. If proper actions are not in place, a new certification process could be required, with additional effort and cost.

The relationship between the security level provided by each software component will also depend on how these modules are interconnected. Indeed, a certain vulnerability in a software library could be more or less exploited depending on the use of the library by the system. Additionally, in an increasingly interconnected world, the security of a certain software component could be influenced by the security level of a system with which the component is communicating. In fact, a system's security level may be reduced if it needs to communicate with a vulnerable system for its intended operation. Therefore, software composability aspects go beyond the usual intrasystem vision.

To address such issues, a key factor is to identify the relationship between software components and certification schemes. For this purpose, there is an additional need to establish a common set of requirements and guidelines that foster an effective and efficient composability process, taking into account the context of use and CSA assurance levels. These aspects are crucial to deal with the cybersecurity certification of emerging scenarios, such as the ongoing development of contact tracing frameworks and mobile apps to restrain the spread of COVID-19. Indeed, such systems will be composed by several components, including mobile apps and back-end servers, which could be certified according to different schemes and varying requirements, depending on the country.

Software Updates

According to the CSA, cybersecurity certification schemes must provide support throughout the lifecycle of an ICT system. This means that the cybersecurity level of a certain system could change during its lifecycle, and, consequently, the system could need to be recertified. In particular, during an ICT system's lifecycle, its software components will be updated to extend functionality or cope with a security issue. These updates could modify the interactions and communication with other components within the system and even with other systems. Beyond updating a component itself, a software module's operating environment can also be revised. Furthermore, the certification of systems' components could expire throughout their lifecycle.

How could software updates affect the cybersecurity certification of software components and the whole system?

Depending on the type of software update, the cybersecurity recertification of a component

could be required, which, in turn, might necessitate the recertification of the system where the component is deployed. During the process, the software component (and even the whole system) may not be operational, and it may become vulnerable to attacks and threats. Therefore, the system should be put in a secure state based on stable software versions. This aspect could require a system to manage and track the different software versions associated with software components and their relationships. Furthermore, due to the potential cost of the recertification process, manufacturers and software providers may be reluctant to produce regular updates for their systems, or they might update the systems without using a recertification process. To address this aspect, the use of lightweight, efficient, and automated testing techniques is paramount for the recertification process so that software providers can be encouraged to recertify their updated systems.

CVD

The current trend toward the interconnection of physical devices implies an increase of the attack surface that can be ubiquitously exploited. While mitigating such attacks and vulnerabilities requires suitable security mechanisms and protocols, efficient vulnerability disclosure and sharing is a key factor for cybersecurity certification. In fact, the CSA explicitly mentions the use of repositories that list vulnerabilities as a source of supplementary cybersecurity information for certified ICT systems. The main reason is that a repository of vulnerabilities could foster increasing trust in ICT systems and a growing awareness of cybersecurity risks, and it could help with the tracking of an ICT system's cybersecurity level throughout the system's lifecycle.

However, as described in a recent report by the Center for European Policy Studies,[10] the realization of a CVD framework requires the cooperation and collaboration of different stakeholders at the EU level, including manufacturers and vulnerability finders. The CVD process embraces the discovery, reporting, publication, and remediation of vulnerabilities to minimize the associated risks as well as to increase transparency for end users. Therefore, CVD can help to bridge cybersecurity certification and the software industry. But

> *will software providers be willing to share information about their components' vulnerabilities?*

To cope with this aspect, the vulnerability disclosure process should be also responsible in such a way that manufacturers and software providers are given a certain period of time to prepare patches and notify users in a timely and reliable manner before a vulnerability is disclosed. Toward this end, we believe that the development of an EU platform for the vulnerability disclosure process must be fostered. As suggested by a recent ENISA report,[6] this platform could be used to share additional cybersecurity information from an ICT system, including threat models, testing processes, software versions, and information about certification schemes. For the realization of such a program, the use of emerging technologies, such as blockchain, could be considered for building a transparent EU platform on which manufacturers, software providers, and end users share cybersecurity information about ICT systems.[11] This platform would serve to foster the alignment of software development activities with the cybersecurity certification process.

Quo Vadis?

Continuous technological advances will enable the development of new ICT systems, shaping innovative digital ecosystems for the benefit of society. As recognized by the CSA, this requires that certification schemes provide a high level of flexibility to adapt to a changing technological environment to avoid the risk of becoming outdated. Furthermore, the CSA regulation contemplates the publication of the Union Rolling Work Program (Article 47) that will be periodically updated to identify strategic priorities for future certification schemes based on criteria such as market demand.

One of the main current advances is the development of 5G technologies and systems that are intended to transform the next digital age. These systems will be enriched by software components whose cybersecurity will affect the deployment of 5G technology. So,

> *how can cybersecurity certification help to promote the deployment of 5G?*

As described in the "Cybersecurity of 5G networks" recommendation,[12] the realization of a cybersecurity certification framework should promote consistent security levels and the creation of certification schemes adapted to 5G-related equipment and software. The use of cybersecurity certification schemes would foster a common understanding of the threats, assets, attacks, and risks of 5G systems, and it would help to recognize the cybersecurity level of a certain 5G system across all EU member states.

In addition to 5G systems, the development of artificial intelligence systems and quantum computing techniques could be considered for cybersecurity certification in the next future. To be successful, cybersecurity certification must go hand in hand with the software development process to promote more secure ICT systems. ■

Acknowledgment

This work has been partially funded by the European Commission, through the H2020-830929 CyberSec4Europe and H2020-952702 BIECO projects.

References

1. European Parliament, "Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on Information and Communications Technology Cybersecurity Certification (Cybersecurity Act)," 2019. Accessed: Oct. 23, 2020. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2019/881/oj
2. "State of the art syllabus: Overview of existing cybersecurity standards and certification schemes v2," European Cyber Security Organisation, Brussels, Belgium, 2017. [Online]. Available: https://ecs-org.eu/documents/publications/5a31129ea8e97.pdf
3. J. L. Hernandez-Ramos, D. Geneiatakis, I. Kounelis, G. Steri, and I. Nai Fovino, "Toward a data-driven society: A technological perspective on the development of cybersecurity and data-protection policies," *IEEE Security Privacy*, vol. 18, no. 1, pp. 28–38, Jan. 2020. doi: 10.1109/MSEC.2019.2939728.
4. "Considerations on ICT security certification in EU - Survey report," European Network and Information Security Agency, Athens, Greece, 2017. [Online]. Available: https://www.enisa.europa.eu/publications/certification_survey
5. K. Busse, J. Schäfer, and M. Smith, "Replication: No one can hack my mind revisiting a study on expert and non-expert security practices and advice," in *Proc. 15th Symp. Usable Privacy Security (SOUPS)*, 2019, pp. 117–136.
6. "Advancing software security in the EU. The role of the EU cybersecurity certification framework," European Network and Information Security Agency, Athens, Greece, 2019. [Online]. Available: https://www.enisa.europa.eu/publications/advancing-software-security-through-the-eu-certification-framework/at_download/fullReport
7. S. N. Matheu, J. L. Hernandez-Ramos, and A. F. Skarmeta, "Toward a cybersecurity certification framework for the Internet of Things," *IEEE Security Privacy*, vol. 17, no. 3, pp. 66–76, May 2019. doi: 10.1109/MSEC.2019.2904475.
8. D. S. Herrmann, *Using the Common Criteria for IT Security Evaluation*. Boca Raton, FL: CRC Press, 2002.
9. "Support of the cybersecurity certification - Recommendations for European standardisation in relation to the Cybersecurity Act," European Network and Information Security Agency, Athens, Greece, 2019. [Online]. Available: https://www.enisa.europa.eu/publications/recommendations-for-european-standardisation-in-relation-to-csa-i/at_download/fullReport
10. L. Pupillo, A. Ferreira, and G. Varisco, *Software Vulnerability Disclosure in Europe: Technology, Policies and Legal Challenges: Report of a CEPS Task Force*, CEPS Task Force Reports, Brussels, Belgium: Centre for European Policy Studies, June 28, 2018. [Online]. Available: https://www.ceps.eu/download/publication/?id=10636&pdf=CEPS%20TFRonSVD%20with%20cover_0.pdf
11. R. Neisse et al., "An interledger blockchain platform for cross-border management of cybersecurity information," *IEEE Internet Comput.*, vol. 24, no. 3, pp. 19–29, June 2020. doi: 10.1109/MIC.2020.3002423.
12. European Commission, "Commission recommendation of 26.3.2019: Cybersecurity of 5G networks," 2019. Accessed: Oct. 23, 2020. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019H0534&from=GA

José L. Hernández-Ramos is a scientific project officer at the European Commission, Joint Research Centre, Ispra, Varese, 21027, Italy. His research interests include the application of security and privacy mechanisms to the Internet of Things and transport systems. Hernández-Ramos received a Ph.D. in computer science from the University of Murcia, Spain. He has served as a technical program committee member and chair for different international conferences. Contact him at jose-luis.hernandez-ramos@ec.europa.eu.

Sara N. Matheu is a postdoctoral researcher at the University of Murcia, Murcia, 30100, Spain. Her research interests are related to security certification for the Internet of Things. Matheu received a Ph.D. in computer science from the University of Murcia in 2020. She has participated in several projects, including ARMOUR, CyberSec4Europe, and BIECO. Contact her at sara.nieves.matheu@um.es.

Antonio Skarmeta is a full professor in the Department of Information and Communications Engineering, University of Murcia, Murcia, 30100, Spain. His research interests include the integration of security services, identity, the Internet of Things, and smart cities. Skarmeta received a Ph.D. in computer science from the University of Murcia. He has published more than 200 international papers and been a member of several program committees. Contact him at skarmeta@um.es.