Cybersecurity Certification for Agile and Dynamic Software Systems – a Process-Based Approach

Volkmar Lotz
SAP Security Research
SAP Labs France
Mougins, France
volkmar.lotz@sap.com

***Abstract*— In this extended abstract, we outline an approach for security certification of products or services for modern commercial systems that are characterized by agile development, the integration of development and operations, and high dynamics of system features and structures. The proposed scheme rather evaluates the processes applied in development and operations than investigates into the validity of the product properties itself. We argue that the resulting claims are still suitable to increase the confidence in the security of products and services resulting from such processes.**

Keywords—security, certification, agile development, software

I. INTRODUCTION

The continued digital transformation of business, government, society and private life increases both the dependency on ICT infrastructures and systems and the speed in which new digital solutions are made available on the market. Infrastructure technologies like cloud computing or 5G mobile communication allow the fast processing of vast amounts of data, scaling resources and features to the actual demand of customers. This leads to highly dynamic and flexible systems that can immediately respond to changed requirements and contexts.

The characteristics of the new technologies have dramatically changed the way how software systems are built today. Agile methods with extremely short release cycles dominate commercial software development for the cloud and lead to seamless integration of development activities and system operations ("DevOps") and a continuous stream of new releases of systems and services through automated build processes ("Continuous Deployment / Continuous Integration – CD/CI") [1]. Software vendors and cloud providers focus their own development investments on core functionalities, while consuming the remaining software from 3rd party vendors including open source software. The price to pay for the required agility and flexibility is an increasingly complex supply chain with rich dependencies as well as an increased difficulty to analyze and assess the properties of such systems.

The digital transformation can only show its full potential, if cybersecurity risks can be managed, and if customers, consumers and users can place trust in the underlying technology. Certification is a well-established traditional means to define and formalize desired properties and behaviors or best practices to achieve them – by establishing criteria – and to gain confidence about the validity of such properties and behaviors – by evaluation of a system or service against the criteria. This role of certification for cybersecurity has been exemplified by the long history of certification schemes – ranging back to the US Orange Book of 1983 [2] --, by the many certification schemes that have been established since then – a report by ECSO [3] counts almost 100 of them –, and by its prominent role in the cybersecurity strategy of the European Commission [4]. The European Cybersecurity Act [5] became effective in June 2019 and establishes the European Cybersecurity Certification Framework, targeting the security of products, services and processes and under which the European Cybersecurity Agency (ENISA) is expected to propose several harmonized schemes in the coming years, including a scheme for cloud services which is currently under preparation.

In this paper, we focus on cybersecurity certification of commercial products and services that drive the digital transformation of economy and society and exhibit the characteristics described above: highly dynamic, short release cycles and relying on a complex supply chain. We call such products or services "modern commercial" for short. With a focus on the criteria, we motivate that schemes targeting the evaluation of single products and services with the aim of understanding and demonstrating how the security mechanisms of the particular product or service meet their security requirements do not scale to modern commercial systems, and propose an alternative approach based on evaluating how a product or service has been developed and is operated rather than what has actually been developed and deployed. We are convinced that certification is a powerful instrument in the cybersecurity arsenal and that the security of commercial systems (distinguished from critical infrastructures and mission-critical systems) can highly benefit from certification.

II. REQUIREMENTS FOR CYBERSECURITY CERTIFICATION

Certification is defined by Wikipedia [6] as the "formal attestation of the confirmation of certain characteristics of an object, person, or organization, often based on some form of external review, education, assessment, or audit". In practice, certification schemes are typically based on standards, allowing either self-declaration or 3rd party evaluation, and are driven by government or industry. Accreditation based certification is an established means to make substantiated statements about properties and functionalities of IT systems, products or services. Such statements can assist buyers in making informed decisions about the security level of software and help them to compare different solutions. While certification statements are neither able nor meant to provide any guarantee about a product's security, they increase transparency and give additional trust, based on the evidence provided and determined by the rigor of the evaluation that leads to a certificate and demonstrating that security best practices and state-of-the-art security technologies have been diligently applied. Hence, security certification plays an important role in improving cybersecurity, complementing other preventive elements of a cybersecurity strategy.

In order to maximize the uptake of cybersecurity certification, especially in the domain of modern commercial systems including cloud services, certification criteria and schemes need to be designed in a way that lead to meaningful

DOI 10.1109/EuroS&PW51379.2020.00020

security statements about products and services while simultaneously maintain economic viability. The latter is of particular importance in the commercial setting: conducting a certification should not introduce inadequate additional costs in terms of investments and resources needed, nor should it lead to major delays of release cycles or the go-to-market time for new products or services.

For agile and dynamic software systems, economic viability of a certification scheme means

- Being integrated in a formal framework that guarantees that different certifiers operate on an equivalent, comparable and competitive basis and that end users can be assured that the certification is valid and comparable regardless of any specific certifying body. This includes formal approval of certification and evaluation bodies by accreditation bodies that ensure that certifiers and evaluators operate in accordance with standard common methodologies to comparable levels of rigor and scrutiny.
- Being of global scale, spanning nations, verticals and organizations. If schemes are instantiated under the auspices of individual nations or organizations, mutual recognition agreements, like they exist, for instance, to a limited extent for the Common Criteria, are essential. Otherwise, the need for multiple efforts – either to support different schemes or to repeat certifications under different (national) regimes for the same scheme – would increase the costs of certification for globally operating vendors to a level that will not be rewarded by the market. Such recognition agreements should be strictly implemented in order to avoid their circumvention and to provide planning reliability to the vendors.
- Having a scope covering a variety of products, services and contexts, so that organizations can establish routines to support certification across their product portfolio. This means that the security objectives and functional requirements for a target of evaluation cannot be uniformly stated and should be following a risk assessment taking its specific context into account.
- Allowing for continuous assessments matching the release cycles of modern commercial software systems. Given the criticality of fast release cycles (weekly, daily or even hourly) and the automated build technologies supporting such a tight schedule, continuous assessment including the maintenance of the certificate needs to show a high degree of automation as well. Changes of the behavior of systems, e.g., caused by using higher-order programming concepts like Java reflection, need to be included in the assessment.
- Supporting the usage of claims or certificates about components of the system or infrastructure the system is relying on, as well as the validation of assumptions on those components. The support of compositional reasoning about security is essential when systems resulting from complex supply chains should be in the scope of a security. certification.

In the remainder of the paper, we focus on the latter three requirements which are those that relate to the certification criteria (in contrast to the certification scheme, which includes entities, their relations, and the process to govern the certifications).

III. Common Criteria

Since the mid 1990s, the Common Criteria (CC) [7], standardized as ISO 15408, serve as a reference point for security certification of ICT components and systems across sectors. The CC target the security of products and systems based on the analysis of required development documentation and independent vulnerability analysis at graded levels of depth and rigor ("Evaluation Assurance Levels").

The scope of the certification is individually defined following a risk analysis and described in a so-called Security Target. Security Targets can be schematized for given product categories (Protection Profiles). The CC are implemented as a national government scheme, with the Security Target evaluation and the product evaluation being conducted by accredited 3rd party evaluation laboratories. Mutual recognition agreements between governments exist, but are limited to certain product categories and lower assurance levels.

While the CC have been applied successfully in focused business domains like smart cards and firewalls, their adoption in general has been limited. In particular, this is the case for modern commercial software systems, where CC certifications only follow customer demand, typically in the Public Sector. This is mainly due to their focus on single products and systems which does not allow them to scale well to modern software development and miss the key requirements on economic viability including automation, the support of continuous assessment at manageable costs and compositionality. Each CC certificate applies to one specific version of a software and is, in general, invalidated with the next version. The certification process is lengthy and does not match the speed of product development, especially not for cloud-based software-as-a-service offers developed and deployed in a DevOps model with their extremely short release cycles. Software built on a platform with contributions from many different vendors including open source software can only be certified on a per-component base with limited value for the overall system security. While the latest CC versions include elements to address these challenges, the obstacles in practice remain: delta certifications are not supported by the criteria themselves, and the composition class is constrained by requiring access to the design information of the implemented components. To meet these challenges, the CC and the related evaluation methodology (CEM) would need to be reformed towards the support of delta certifications and taking the dependencies of systems built and operated on a (cloud) platform as well as such platforms themselves into account.

While the risk based approach supports their wide applicability, the Common Criteria emphasize the challenges of product and service certification in modern software development for the cloud by not meeting the agility needs, caused by their focus on individual product properties in contrast to the practices applied in development and operation to enforce those properties.

IV. A Process-based View

In order to reflect the current paradigms in the software industry, we argue that a cyber security certification scheme should, in general, be process-based, with certification

evaluating the outcomes of the processes for the individual product or system only required for high risk environments like critical infrastructures with a long lifetime for the installed technology components. In the following, we discuss some methodological concepts and elements of evaluation criteria of a process-based approach, which would help to meet the requirements stated above.

For the software and (cloud based) services industry, we promote a certification scheme that focuses on the effectiveness of the processes that are applied to the development, deployment and operation of secure software and that is based on international standards. Effectiveness of a process includes process definition, enforcement of the process application, automation of the process, and means for validating the process application. With process certification, one can provide the required insights in the security best practices applied in the development activities that each product undergoes, acknowledge different protection needs and risk exposure, as well as scale to fast release cycles and cloud operation models. It is possible to extend the scope of certification to all lifecycle phases of a software product, including deployment and operation (with elements such as, for instance, regular updates or patch management). Process oriented schemes are also better prepared for technology evolution, both for business functionality and security functionality, in that they do not require complete re-evaluation when new product versions embody the latest technology, provided these are controlled by the best-practice methodologies that were the target of the process certification.

A process-oriented security certification scheme for software products and services targets product, system and service security by investigating into how they are developed in an organization. It focuses around the establishment of a secure development life cycle (SDLC) [8] and secure operations of cloud services. Based on the assumption that well-defined and rigorously applied process elements that match the state-of-the-art in security-by-design, security testing, secure operations and more lead to a predictable security quality of the outcomes of such processes, processes that are certified once lead to security claims about many products provided there is evidence that the processes are indeed applied. Important process elements include:

- Threat modelling: The analysis of the system architecture with respect to potential attack surfaces and attack vectors
- Risk analysis: The assessment of the identified attack vectors in terms of their impact and probability
- Secure-by-design processes: The application of software engineering artefacts and best-practices to achieve secure systems, including reference architectures, programming guidelines, test strategies etc. and their enforcement
- Security APIs and libraries: reference interfaces and implementations for security functions as well as the enforcement of their usage
- Security testing and tools: security test plans, application of complementary test methods (e.g., static and dynamic analysis), penetration testing, independent validation
- Analysis and approval procedures for 3rd party and open source software including those aiming at identifying known vulnerabilities
- Processes for vulnerability disclosure and system patching
- etc.

International standards like ISO/IEC 27034 “Information technology – Security techniques – Application security” [9] take a similar approach, and a new certification scheme could refer to them. Key elements of the concept of ISO/IEC 27034 are the definition of an organizational normative framework including an organization Application Security Control Library (ASC Library), and an application security risk assessment. Following the application-specific risk assessment, controls from the ASC Library are selected to be applied during the development and operation of the respective application. Since ASC controls include both specification and validation aspects, the demonstration of process effectiveness is supported. The selected controls may include technical controls, but also any or all of the above-mentioned process controls. An organization that is compliant with ISO/IEC 27034 and chooses the process controls required by the process-based certification scheme should then straightforwardly receive certificates for the applications built in this framework. The certification effort would focus on the process controls of the ASC Library themselves – a one-off effort for the organization –, the enforcement mechanisms for the application of the controls and the risk assessment for the application at hand.

Process certifications can be conducted by external evaluators as well as being the result of vendor declarations, depending on the level of rigor that is required. Such certification schemes currently do not exist for application software development and maintenance although they can clearly be based on the model of ISO/IEC 27034. Organizations with a high level of software process capabilities and maturity, e.g., following CMMI or SPICES (ISO/IEC 15504) [11], or even security process maturity, e.g., following BSIMM [12], are expected to have an advantage when certifying their products and services under a process-based scheme, since many of the required process elements would already be in place.

We believe – and propose further research to substantiate this belief – that a process-oriented certification scheme as outlined above does not necessarily lead to weaker security assurance, provided that the methodologies and activities required are comprehensive and state-of-the-art. This can be enforced by the scheme itself requiring respective process elements as well as evidence for their application. In the context of ISO/IEC 27034 these requirements would translate into requirements on the content of the ASC Library and requirements on the selection of controls for a given application and context. A certificate then attests that best security practices are applied throughout the whole lifecycle of a product and service, including updates and security patches, which gives the desired transparency at least for lower and medium levels of assurance. We recall that certification is not meant to provide guarantees for the validity of security properties but aims at increased confidence by assuring that a thorough examination has led to a positive verdict. We think that the process-based approach provides this additional confidence even though the individual process

or service is only examined in its development and operations context.

In fact, process-based certification complements CC-like product certification in the sense of providing an effective certification scheme for highly dynamic environments like the cloud, and by paving the way for high assurance level CC certification in cases of particular security sensitivity. For instance, an organization's ASC library can contain controls that meet CC requirements (for instance, a security model, an effectiveness analysis of the security functionality or a formal verification). Following an application risk analysis (which maps to a Security Target or a Protection Profile), these ASCs can be selected for the given application task and used in a later formal CC evaluation and certification effort, where the results of the ASCs are evaluated.

Following this approach, a process certification scheme serves as the baseline for the whole industry, with a smooth transition to stronger certification requirements where they are appropriate. It would even be feasible to distinguish different assurance levels as required by the European Cybersecurity Act [5] for processes by distinguishing them (or their instances) with respect to their scope, depth and rigor, offering low entry barriers and an incremental path to certification for vendors and providers.

V. Conclusion and Further Research

In this extended abstract, we have outlined an approach for security certification of products or services for modern commercial systems that are characterized by agile development, the integration of development and operations, and high dynamics of system features and structures. These are types of systems that can clearly benefit from security certification but exhibit the weaknesses of traditional approaches to product security certification, most notably the Common Criteria: lack of flexibility, lack of scalability, high certification costs and efforts, limited mutual recognition of certificates. We propose a scheme that rather evaluates the processes applied in development and operations than investigates into the validity of the product properties itself, and we argue that the resulting claims are still suitable to increase the confidence in the security of products and services resulting from such process. The proposal is inspired by ISO/IEC 27034's concepts of application risk assessment and an application security control library and offers migration paths to Common Criteria style certification for high-risk products and environments.

Further research is planned to focus on the definition and assessment of process controls for security (here, we only mentioned some high-level examples) and the analysis of the strength of the claims that result from a process-centric approach to certification compared to a product-centric one.

Acknowledgment

This paper is supported in part by European Union's Horizon 2020 research and innovation program under grant agreement No 830892, project SPARTA.

References

[1] Christof Ebert, Gorka Gallardo, Josune Hernantes and Nicolas Serrano: "DevOps"; IEEE Software, Vol.33, No. 3, p. 94-100, 2016

[2] DOD 5200.28-STD "Department of Defense Trusted Computer System Evaluation Criteria", 1985

[3] ECSO WG1 Standardisation, certification, labelling and supply chain management: "STATE OF THE ART SYLLABUS, Overview of existing Cybersecurity standards and certification schemes"; available at https://ecs-org.eu/documents/publications/5a60b8bf83f7c.pdf, retrieved 09/03/2020

[4] European Commission: "„Resilience, Deterrence and Defence: Building strong cybersecurity for the EU"; JOIN(2017)450 final, published 13/09/2017

[5] 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 and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), PE/86/2018/REV/1

[6] https://en.wikipedia.org/wiki/Certification, retrieved 09/03/2020

[7] ISO 15408, "Common Criteria for Information Technology Security Evaluation", Version 3.1, Revision 5, 2017

[8] M. Howard: "Building more secure software with improved development processes; IEEE Security & Privacy, Volume: 2 , Issue: 6, 2004

[9] ISO/IEC 27034, "Information technology – Security techniques – Application security", 2011

[10] "CMMI for Development, Version 1.3". CMMI-DEV (Version 1.3, November 2010). Carnegie Mellon University Software Engineering Institute. 2010

[11] ISO/IEC 15504, "Information technology — Process assessment", 2004

[12] Building Security In Maturity Model (BSIMM), https://www.bsimm.com/, retrieved 24/06/2020