SAFECode
Software Assurance Forum for Excellence in Code
Driving Security and Integrity

SAFECode Comments on EU Cybersecurity Legislation

Steve Lipner

October 2018

Introduction

Early this year, SAFECode released a white paper that discussed our perspective on government programs for cybersecurity certification of information technology products and services. The release of that paper was driven by the European Union (EU) initiative to pass cybersecurity legislation that, among other things, creates new EU cybersecurity certification schemes.

Since we released our white paper, the European Commission, Parliament, and Council have made a great deal of progress in refining the proposed legislation. While the legislation has not yet been finalized, detailed language has been proposed and it is now possible for us to review the proposals under consideration and provide more specific comments and suggestions.

This paper is not a line-by-line markup of the draft legislation. Rather, it addresses issues related to security certification and secure development that are raised by the draft, often in more than one article. For each issue, we provide our perspective and suggestions, and indicate which articles of the draft legislation bear on the issue.

We hope that these comments and suggestions are helpful to the EU authorities, and to the broader community, as they consider the draft EU legislation and next steps toward an EU cybersecurity certification regime.

Vulnerabilities (Known and Unknown) and Updates

The draft EU legislation refers in several places (Articles 43 and 45) to requirements that software be free from vulnerabilities. While freedom from vulnerabilities is a critical objective for software (and in general IT product and service) developers, given the current state of the art, perfect security is not achievable for software that must provide customers with a usable level of functionality and be delivered in a realistic timeframe (months or quarters rather than decades). Thus, any requirement that delivered products be free from unknown vulnerabilities is unrealistic and unsatisfiable.

The draft also refers to requirements that delivered software be free from known vulnerabilities. This requirement is reasonable and appropriate: developers should ensure that new software releases remedy previously-discovered serious vulnerabilities as a matter of course. They should also take steps to ensure that third-party components that they incorporate are free from known vulnerabilities that could have an impact on the software they are releasing[1]. Meeting the latter requirement may involve incorporating the latest version of third-party components or even fixing vulnerabilities in third-party components before incorporating them.

The discussion of known and unknown vulnerabilities is closely tied to the issue of software updates. Any secure development process worthy of the name will include a process for remediating newly discovered (previously unknown) vulnerabilities and using a root cause analysis of such vulnerabilities to help enhance the security of future releases. The draft legislation alludes in Articles 45 and 47) to secure software updates but does not specifically address the fact that all developers should implement vulnerability response processes for the products they deliver.

[1] In some cases, a vulnerability may be present in a third-party component, the component may be used in such a way that the vulnerability cannot be triggered or exploited.

Security by Design

"Security by design" is a phrase that is widely used as a shorthand for the proposition that IT product developers should consider security early and as a fundamental tenet of the design of a product or service. Security by design goes hand in hand with "security by default" – the tenet that products should be delivered to customers in a secure configuration. Specific techniques for achieving security by design and default vary – from threat modeling to attack surface analysis to formal specification – but security by design and default are fundamental.

Only the Parliament markup of Section 45 of the draft legislation refers to "security by design" and security by default. If the legislation is to demonstrate the EU's commitment to effective security of IT products and services, it is important that a reference to security by design and default be included.

Secure Development Process

As the SAFECode white paper and other SAFECode documents make clear, secure IT products and services result from the developer's application of a secure development process. Such a process incorporates "security by design" and goes on to mandate the application of tools and techniques that help to prevent the introduction of vulnerabilities during development. Effective secure development processes incorporate root cause analysis of newly discovered vulnerabilities as a vehicle for achieving process improvement and driving out newly discovered classes of vulnerabilities. Thus, unlike after-the-fact security testing, secure development processes can eliminate entire classes of vulnerabilities before a product or service is delivered to customers.

The draft EU legislation refers to certification of secure development processes, but only in the Parliament markup of Section 47. Given the importance of secure development process to effective IT product and service security, it would be appropriate for the legislation to identify explicitly certification of secure development process as an objective of any EU certification scheme.

Schemes and Assurance Levels

The draft legislation (Article 44) anticipates the establishment of multiple certification schemes but does not elaborate on the anticipated scope of individual schemes. It may be appropriate to create separate schemes for different classes of IT products and services – perhaps one scheme for consumer IoT devices, a second for desktop IT or commercial cloud services, and a third for IT components embedded in safety critical systems or critical infrastructures. However, it is important that all schemes be based on a common set of principles – such as application of secure development process, security by design, security by default, root cause analysis and continuous improvement. Establishment and adherence to such a set of common principles will facilitate the broad adoption of secure engineering practices and the sharing of techniques, tools, and training across the EU and global developer community.

The SAFECode white paper suggested that EU certification schemes avoid the introduction of multiple "levels" of assurance. This suggestion was based on experience with the Common Criteria where developers have sought to compete on the basis of product assurance levels attained by creating additional product documentation rather than delivering better assured (more secure) products. The draft EU legislation (Article 46) refers to multiple assurance levels: basic, substantial, and high. The

establishment of multiple levels may be appropriate if different levels are required for certification of different classes of products and services. Continuing with the example above, consumer IoT devices might be required to be evaluated at the basic level, enterprise and consumer desktop IT at the substantial level, and critical infrastructure embedded systems at the high level. Today, the Common Criteria Mutual Recognition Arrangement follows such a practice by establishing an appropriate assurance level for each class of product or technology subject to evaluation.

Assuming the EU legislation does go forward with a mandate for multiple evaluation levels, it is important that higher levels incorporate requirements for practical measures that actually improve product or service security. For example, products evaluated at "substantial" or "high" might be required to undergo more exhaustive threat modeling, or application of multiple static code analysis tools. The specifics of such requirements are a detail to be left for evaluation scheme developers, but the principles that levels are associated with classes of products and services and that higher levels require more rigorous secure development processes are appropriate for inclusion in the legislation.

Self-Certification

The Parliament-introduced Article 46a introduces the notion of self-certification for products and services evaluated at the "basic" level. Self-certification has the potential to be an appropriate and cost-effective option. Self-certification also provides an incentive for certification scheme developers and certification authorities to articulate clear and unambiguous certification requirements.

Standards and Mutual Recognition

The draft legislation includes multiple references to international standards (every article with the exception of Articles 45 and 46). Given the international character of the IT industry, SAFECode can only applaud this recognition of the importance of international standards to the creation of effective EU cybersecurity certification schemes. ISO/IEC 27034 (Information technology -- Security techniques -- Application security) in particular provides a basis for standardization of the secure development processes that are fundamental to the creation of secure software products.

Expanding on the discussion of international standards, SAFECode stresses the importance of international mutual recognition of IT evaluations. The international Common Criteria Mutual Recognition Arrangement includes member countries worldwide (many European) and Common Criteria evaluations are widely sought by IT vendors. The Common Criteria are an international standard (ISO/IEC 15408) that undergoes periodic review and updating to consider issues such as those raised in earlier sections of this paper. Thus, compatibility of EU certification schemes with Common Criteria is an important objective and one that could appropriately be made explicit in the EU legislation.

Summary

The members of SAFECode are pleased to see the progress that the EU has made in drafting cybersecurity legislation, and in considering the issues related to the security evaluation of IT products and services. The comments in this paper seek to encourage the development of certification schemes that will be beneficial for IT users and vendors in Europe and worldwide.