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

SAFECode Perspective on Cybersecurity Certification

Steven B. Lipner
Executive Director, SAFECode
January 2018

Introduction

The inclusion of an EU-wide Information and Communications Technology certification framework as part of the new EU cybersecurity legislation [1] has caused renewed interest in the topic of security certification and evaluation. This paper is based on SAFECode members' experience with security certifications going back to the late 1970s. It reviews lessons learned from past security certification and evaluation initiatives and presents SAFECode's observations and recommendations regarding any new cybersecurity certification schemes.

A History of Certification Schemes

Security certification of commercial information technology (IT) products is not new. The first security certification scheme, the US Trusted Computer Systems Evaluation Criteria [2] [3] or Orange Book, was introduced in 1983. In 1990, the governments of France, Germany, the Netherlands, and the United Kingdom joined to create the international Information Technology Security Evaluation Criteria (ITSEC) [4], which was subsequently adopted by a number of other nations. The creators of the Orange Book and ITSEC joined forces in 1999 to create the international Common Criteria (CC) [5]. The CC was adopted as an International (ISO) Standard and supplanted both the ITSEC and the Orange Book. The adoption of the CC also marked the creation of an international agreement under which CC evaluation results were mutually recognized by more than twenty member countries.

All of the certification schemes mentioned above had some key attributes in common:

- They focused on ensuring that security features of IT products – such as password management and encryption – were present and functioned correctly.
- They required developers to produce documentation and functional tests of their products and to make completed product, documentation, and test systems and results available to government or government-licensed evaluators.
- They relied on expert evaluators to assess the adequacy of the provided evidence, and thus the certifiability of the end product.
- They incorporated a hierarchy of certification levels, with higher levels intended for applications where it was necessary to protect more sensitive information against more serious threats. Certification at higher levels required with more and more formal documentation, and additional evaluator effort.

As the implementation of historic certification schemes played out, use and interconnection of IT products grew explosively, as did the discovery and exploitation of IT product security vulnerabilities. While numerous IT products have undergone

certification since 1985, there is no evidence that certified products experience fewer or less severe vulnerabilities than those that are not certified.[1,2] In addition, the classic certification model in which evaluators review the finished product and its documentation means that products are only certified months or years after they are completed and released for sale. Thus, many users rely on products that have not completed certification – a trend amplified by rapid product cycles and by the delivery of IT functions in the form of rapidly updated cloud services both of which are increasingly common today.

Making Certification Work

The members of SAFECode believe that an effective cybersecurity certification scheme can be of value both to suppliers and users of IT products and services. Such a scheme can enable users to identify products and online services that provide effective security and can incentivize suppliers to invest in effective security – and help to ensure that they are rewarded for that investment. However, realizing that value will require a certification scheme or schemes that recognize both the lessons of the past and the realities of modern IT. In particular:

- While appropriate selection, design, and implementation of security features is critical to enabling products or online services to be used securely, security vulnerabilities can occur in any part of a product or service and seldom result from errors in security features. Thus, the entire product or service must be secure, not just its security features.
- The historic approach of after-the-fact certification is very much like trying to "test quality in" to a completed product by finding errors and making the developer fix them – an approach that developers recognize as both costly and ineffective. Instead, the modern paradigm is to build security (and quality) in as the product is being built. When the product or service is complete, its security is assured to the greatest extent practicable. Understanding the process used to develop the product or service is often a more effective predictor of security than reviewing the product or service after it has been created.
- Product lifecycles, and especially online service lifecycles, are short. In the case of the software that implements online cloud services, updates occur, and updated versions are put into use weekly or even daily. Given today's technology, an after-the-fact certification scheme will either have the effect that few or no user organizations will ever be using a certified product or service or will force user organizations to rely on outdated or obsolete products or services.
- As organizations and individuals become more and more dependent on cloud services, certification of individual hardware or software products addresses less of their need for effective security. A modern certification scheme should not only consider the secure design and implementation of hardware and software but also the secure configuration and operation of services that customers rely on.
- Certification schemes that provide varying levels of certification incentivize developers to seek the highest levels of certification. Users tend not to value or seek products that are certified at lower levels, and the quest for higher levels leads to longer delays in certification – and to fewer and fewer users applying products that have actually been certified. To the extent that a certification scheme incorporates varying levels of certification, those levels should be clearly linked to classes of systems or products and the classes of risks those systems will face. Such a linkage will make the certification process more efficient for developers and more valuable to users.
- Today's market for IT products and services is an international one that extends well beyond the EU or the USA. A new certification scheme should rely on international standards and seek broad mutual recognition in order to provide maximum benefit to users and developers worldwide.

The members of SAFECode – and many other development organizations worldwide – have responded to customers' needs for secure products and services by adopting secure-by-design development processes that incorporate security as a *mandatory* consideration *during the development of all* software. Security is built into the product from the beginning of design until it is ready for release to customers. The fact that the secure development process has been followed is recorded in the development organization's workflow management system. After-the-fact testing may be used to confirm that the process has been followed, but should not be necessary if the organization has an effective secure development process in place – the security is built in as the product is built.

1 Smartcards and other limited-function encryption devices are generally agreed to be an exception. Such devices are evaluated under a highly tailored variant of Common Criteria that was created jointly by device vendors and evaluators. Even in the case of smartcards, there has been some cause for concern. See https://www.internetsociety.org/blog/2017/11/roca-encryption-vulnerability/

2 For example, during the period between 2000 and 2013, Microsoft released one security update in response to an issue discovered by a Common Criteria security evaluation. The issue was viewed as low-impact and there is no evidence that it was ever exploited.

The international standards community has recognized the importance of secure development processes, and an emerging ISO Standard 27034 [6] provides a guide for implementing a secure development process. This standard can provide a basis for security certification of a developer's process. Adoption of an international standard would have the benefits of international recognition (potentially beyond the EU), continuous improvement as new security engineering techniques were devised, and broad acceptability.

Secure development processes are the only practical approach to implementing products and services that protect users' information, and thus have been widely adopted by commercial development organizations worldwide. SAFECode has taken the lead in meeting such organizations' needs by developing and releasing free process guidance and developer training that can be downloaded and applied by any organization that seeks to create more secure products. However, adoption by small and mid-sized development organizations has been less common and there is still a need for additional resources to aid small and mid-sized development organizations. SAFECode is committed to working with the community to meet that need.

Summary

SAFECode believes that a new EU security certification scheme can help encourage the development of more secure IT products and services and provide meaningful assurance to IT users – *provided* the scheme is consistent with the current state of IT security and with current development practices for IT products and services, and that it is flexible enough to accommodate new best practices in development. In summary, SAFECode recommends:

- The EU security certification schemes should focus on evaluating developers' processes that build security into products and services, and on efficiently gaining confidence that those processes have been followed.
- The EU security certification schemes should be aligned with appropriate international standards for secure development, and in particular with the ISO/IEC 27034 series of standards and allow for mutual recognition.
- If the EU adopts certification schemes that provide multiple levels or grades of security certifications, those levels should be clearly tied to classes of applications and anticipated risks so that both developers and users will have clear guidance on what level of certification is required and appropriate.
- That the EU commit to ensuring that small and medium development organizations have access to resources that enable them to adopt processes that conform with international standards for effective secure development.
- The EU security certification should be kept independent from certifications in the areas of safety or privacy. However, security standards may specify safety-related or privacy-related protection goals, e.g. that security must not impair or weaken safety functionality.

SAFECode and its members are ready to serve as a resource in the development of standards and guidance that help organizations of all sizes adopt and implement effective secure development processes. SAFECode is also committed to working with EU organizations as appropriate to support the creation of effective security certification schemes.

About The Author

Steven B. Lipner is the executive director of SAFECode, a non-profit organization dedicated to increasing trust in information and communications technology products and services through the advancement of effective software assurance methods. He is also an adjunct professor of computer science in the Institute for Software Research at Carnegie Mellon University. He retired in 2015 as partner director of program management at Microsoft Corporation. At Microsoft, he was responsible for the Security Development Lifecycle (SDL), including the development of software assurance requirements, processes and tools, and oversight of the application of the SDL by development teams. Mr. Lipner has been an active contributor to IT product security evaluation processes since the late 1970s and was responsible for government security evaluations of Microsoft products. He has more than 40 years' experience as a researcher, development manager, and general manager in information technology security, and is named as inventor on twelve U.S. patents in the field of computer and network security. He was elected to the United States National Academy of Engineering in 2017.

References

1 European Commission, "JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL - Resilience, Deterrence and Defence: Building strong cybersecurity for the EU," Euopean Commission, Brussels, 2017, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017JC0450&from=EN

2 United States Department of Defense, "Trusted Computer Systems Evaluation Criteria," United States Department of Defense, Washington DC, 1983, 1985, https://csrc.nist.gov/csrc/media/publications/conference-paper/1998/10/08/proceedings-of-the-21st-nissc-1998/documents/early-cs-papers/dod85.pdf

3 S. B. Lipner, "The Birth and Death of the Orange Book," IEEE Annals of the History of Computing, vol. 37, no. 2, pp. 19-31, April - June 2015

4 Governments of France, Germany, the Netherlands, the United Kingdom, "Information Security Technology Evaluation Criteria," Department of Trade and Industry, London, 1991, http://iwar.org.uk/comsec/resources/standards/itsec.htm

5 Common Criteria Management Board, "Common Criteria for Information Technology Security Evaluation," Common Criteria Mutual Recognition Arrangement, 1999 - 2017, http://www.commoncriteriaportal.org/cc/

6 International Organization for Standardization, "Information technology -- Security techniques -- Application security -- Part 1: Overview and concepts," International Organization for Standardization, 2011, https://www.iso.org/standard/44378.html