Does product certification really work?

Renaud Labelle & **Sylvain Leroy**,
Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)

Abstract:
Faced with the wide variety of security products (firewalls, VPNs, etc.), users sometimes feel helpless. How to know which are the best? The security certifications made in France under ANSSI's supervision are based on an objective, duplicable assessment. They are one answer to this question, at least for products (such as debit/credit cards) with highly standardized features. Although this process offers a widely recognized, serious warrant of security, it relies on procedures worked out about twenty years ago and is not really adapted for products to offer a higher level of security. The European certification process now being rolled out will eventually replace national assessment procedures. It seeks to broaden the scope of certification so as to allow for assessments of everyday devices and take into account a product's whole life cycle.

The digital services we use, day in day out, rely on several measures of security (controlled access, encryption, integrity protocols, etc.) that are usually installed in products available on the market (firewalls, VPN, antivirus programs).[1]

Although technical specifications often look alike, not all products are on par. It is very hard to know which measures actually raise the level of security. To form an opinion about a product, there is no other solution than an in-depth assessment of whether the security features are indeed installed and work as claimed. Given the complexity of digital technology, this verification requires high-level experts from several fields (cryptography, hardware architecture, operating systems, software security development, etc.) who must constantly keep up to date on the new methods used by attacking forces and on the ways to protect against them.

Security certification is one response to this situation. Conducted by a third party independent from the manufacturer, it is a standardized method for evaluating the security of digital products in order to attest whether security features are correctly executed.

Security assessments have come along with the Internet

The assessment of security products started in the United States at the end of the 1960s in the defense sector, the aim being to control access from a distance to classified military information on the network that preceded the Internet. In 1986, the publication of the Trusted Computer System Evaluation Criteria (TCSEC) had a considerable impact on the still young field of computer security. However these criteria turned out to be inapplicable given the duration and cost of assessments.

[1] This article has been translated from French by Noal Mellott (Omaha Beach, France). The translation into English has, with the editor's approval, completed a few bibliographical references. All websites were consulted in June 2021.

The European Economic Community soon decided to adopt its own criteria. In 1990, the four countries in advance on this question — the United Kingdom, Netherlands, Germany and France — jointly published the Information Technology Security Evaluation Criteria (ITSEC), which were more oriented toward the civilian products that were coming to the market. Under the so-called SOGIS agreement, the other, less advanced countries in Europe recognized the assessments made by these four.

In parallel, non-European countries were designing their own criteria. It soon became necessary to harmonize all these initiatives so as to allow for the mutual recognition of the assessments made. Thus arose in 1999 a set of "joint criteria" at the initiative of the ISO, which seventeen countries would recognize under the international Common Criteria Recognition Arrangement (CCRA). These criteria, still in force, are used for "common criteria certifications".

Subsequently, the DCSSI (the predecessor of ANSSI, the National Cybersecurity Agency of France) published Decree n°2002-535 on 18 April 2002, which made the current procedure for French certification compliant with the "common criteria". In 2008, it designed another type of certification called a "certification of security at the first level" (CSPN), a fast-track approach that is simpler and better adapted to software.

Security certification in detail

Security certification attests to a product's robustness by analyzing the results of penetration tests and the product's compliance with specifications. It is delivered under the authority of ANSSI by any private firm certified as a "center of evaluation of the security of information technology" (CESTI).

The manufacturer who wants to have a product certified must first declare its "security target" (*i.e.*, the list of security properties claimed for the product). This target sets the bounds between security properties in the product itself and those presumably in the product's environment. After ANSSI checks the security target's coherence, a CESTI chosen by the manufacturer makes the assessment, the manufacturer bearing the cost. Following the evaluation, the CESTI writes a report and sends it to ANSSI which, taking cognizance of its contents, will decide whether or not to certify the product. ANSII may eventually add specific conditions for using the product.

In the case of a COMMON CRITERIA CERTIFICATION, CESTIs undertake two major types of investigation:

- On the one hand, they will verify whether a product's security features comply with those described in the "security target" and with the criteria and specifications used for the assessment. Depending on the level of certification requested, these criteria define the level of requirements for tests and the power to be used by the attacking force.
- On the other hand, they analyze a product's points of vulnerability, by examining the product's source code, architecture or method of implementation, to make sure that an attacking force cannot dodge its security features. This analysis entails conducting targeted penetration tests. As a function of the type of products and the sought-for level of security, this certification takes from six to eighteen months. This very expensive procedure is best suited for security components and banking card chips.

In contrast, France's FAST TRACK CERTIFICATION (level 1) is carried out within 25 days if the product does not have functions using encryption (otherwise 35 days) and in a black box (*i.e.*, without examining the source code). It amounts to an "expert opinion" about the product's security features in relation to an attack of moderate intensity. Since this certification is not conducted in line with the common criteria methodology, it does not enjoy international recognition.

Pros and cons of certification

Certification offers manufacturers a unique possibility for having their products assessed in depth at a given time by a third party who launches high-level attacks under an internationally recognized arrangement.

The costs of assessments

Major means have to be used to reach the level of security required. CESTIs undergo regular audits by ANSSI's best experts, the aim being to ensure that these centers are capable of conducting attacks at the required level. A certifier from ANSSI verifies each assessment and sees to it that all possible paths of attack have actually been tested. In cases of doubt, experts from ANSSI and the CESTI discuss matters on an equal footing. This procedure guarantees that a product has undergone a serious evaluation and ensures the quality of the certificate delivered. As a consequence, assessments are expensive. They remain competitive only because the state accepts to cover the costs of CESTIs and of the top-notch experts at ANSSI. Conducting high-level attacks requires major investments in equipment and human resources, a reflection of the ever more sophisticated means used by attacking forces (including criminal groups). For instance, the usual level of certification for payment cards requires using lasers or complex software to analyze the code.

The difficulty of mutually recognizing security assessments

Even though the common criteria set the definition of the level of the attack, they are hard to interpret; and the assessments made by different countries are not always equivalent. To take payment cards as an example, European stakeholders (manufacturers, certification centers) have worked tirelessly to reach a consensus about how to interpret the common criteria. Despite this work, differences subsist between countries, and it is unrealistic to expect that every laboratory makes every assessment in the same way. With this situation in mind, the United States conducts tests for commercial products only.

Only assessments of simple conformity are recognized worldwide.

A process not adapted to complex products or systems

To be exhaustive, a common criteria assessment of a product entails poring over its documents, examining how it has been developed, auditing its sites of development and production, evaluating its vulnerability management, analyzing its code, conducting physical attacks… and all of this must be done on the product's whole attack surface. The costs soon become prohibitive for complex products. Furthermore, this certification is not at all adapted to modern products, which are often connected and use applications operating on mobile terminals and distant servers.

By limiting the number of days for an assessment, fast-track security certification (CSPN) curbs costs. Given the limited period of testing however, it cannot claim to be exhaustive. It is, therefore, suitable only for simple products.

Since certification is not adapted to all cases, new forms of evaluation are being proposed, such as bug bounties (promising in terms of agility) and penetration tests. These "pentests" are conducted by auditors who, less strictly regulated, may evaluate complex systems or even whole information systems. They have proven to be very useful for modern applications.

Vulnerability management: Room for improvement

While certification provides us with a good idea about a product's degree of security, points of vulnerability are more likely to be discovered over the course of a product's life span. So, is it worthwhile to obtain certification? One response is to have products reexamined periodically. Since security certificates are now archived after five years, a product cannot be deemed trustworthy beyond this period without undergoing a new assessment.

There is, however, no simple means for reevaluating a product that has already been assessed but has been modified in the meantime (*e.g.*, to correct bugs or close points of vulnerability). According to the rules and except for a few very simple products, it would be necessary to rerun the product through most of the processes for an assessment. For this reason, manufacturers are not motivated to correct products that have already been certified. As a consequence, we find on the market certified products that are vulnerable alongside products that have not been certified but have been kept up to date!

Certification is not recommendation

When ANSSI certifies a product, it verifies whether the product offers the security features it claims to have but does not formulate an opinion about the product's utility or pertinence. This is a major source of confusion for buyers, who think that certification amounts to recommendation.

In contrast, when ANSII wants to recommend using a product (in particular, to public administrations or operators of vital importance — the firms critical to the national economy), it resorts to another process: "qualification". Qualification is based on one or more certifications conducted with relevant security targets and, too, on other elements, such as vulnerability management processes. Users have criticized qualification, since it might lead to recommending products that have undergone an in-depth security assessment but do not work as well as competing products. Having taken this criticism seriously, ANSII is reflecting on including functional and ergonomic tests in the process of qualification. These tests would be conducted in partnership with users.

The future: European certification

Given that various certification procedures have been, or are being, adopted in EU member states, this situation erects barriers inside the single market and is, for users, wanting in clarity. The European Commission has thus proposed a framework for a European certification of digital products, services and processes. This proposal took concrete form with the publication of the *Cybersecurity Act* in June 2019, which will take effect in June 2021.[2]

This act provides for three levels of certification: basic, substantial and high:

- For the high level, a trusted third party will conduct penetration tests (as for most common criteria assessments made in France). In this case, certification is preferably delivered by a public entity.
- The substantial level of certification relies on tests of conformity (similar to the American approach), which take account of known points of vulnerability. This certification is realized by a trusted third party: a private accredited entity.

[2] 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) available via https://eur-lex.europa.eu/eli/reg/2019/881/oj.

● At the basic level, the door is open for a self-evaluation of products by developers (similar to the CE label). This low-level procedure with simpler tests provides a fast-track approach for certifying many more products (such as connected devices).

These new EU certification procedures provide an official framework for the SOGIS agreement, but they are also intended for the certification of new products, such as cloud computing services, the Internet of things (IoT), 5G equipment, or even processes (such as ISO 27001 certification, which concerns information system security management). In a second phase, an approach could be examined that would be adapted to specific sectors (like the automobile industry or health).

This certification makes methodological improvements, such as the possibility of using processes similar to the fast-track CSPN for the highest level of security. It will also require a better vulnerability management. A vulnerable product will lose its certification, but the corrected version will be able to retrieve certification faster through a method, fast and sure, based on an audited process of how patches are managed.

Conclusion

Certification is a complex, potentially expensive procedure. Although there is room for improvement, it is an objective, widely recognized method for assessing product security. For ANSSI, certification is the standard way to form an opinion about a product. The quality of French certification (globally of a very high level) has been recognized internationally.

European certification, still being negotiated, will bring many improvements for making the process of certification more effective. But by broadening the scope of action to new types of objects and to lower levels of security, it should reinforce firms and — this is something new — contribute to building up the confidence of citizens in digital technology.