La certification de produits fonctionne-t-elle ?

Par **Renaud LABELLE**
et **Sylvain LEROY**
Agence nationale de la sécurité des systèmes d'information (ANSSI)

Les services numériques que nous utilisons au quotidien reposent sur de nombreux mécanismes de sécurité (contrôle d'accès, chiffrement, intégrité, etc.) qui sont pour la plupart installés dans des produits disponibles sur le marché (pare-feu, VPN, composants de sécurité).

Or, si les descriptifs se ressemblent souvent, tous les produits ne se valent pas, et il est très difficile de reconnaître ceux qui apportent un réel niveau de sécurité. Pour se faire un avis sur un produit, il n'existe pas d'autre solution que de vérifier en profondeur que les fonctions de sécurité qu'il prétend apporter sont bien présentes et remplissent leur rôle. Cette vérification nécessite, compte tenu de la complexité des technologies en jeu, des experts de haut niveau dans de nombreux domaines (cryptographie, architecture matérielle, systèmes d'exploitation, développement logiciel sécurisé, etc.) qui doivent en permanence se tenir à jour des nouvelles méthodes utilisées par les attaquants et des mécanismes qui permettent de s'en protéger.

La certification de sécurité est une réponse à cette problématique : effectuée par un tiers indépendant du fabricant, c'est une méthode normalisée d'évaluation de la sécurité des produits, qui permet d'attester qu'ils exécutent correctement les fonctions de sécurité qu'ils prétendent offrir.

L'évaluation de sécurité s'est développée en même temps qu'Internet

L'évaluation des produits de sécurité est née aux États-Unis à la fin des années 1960 dans le monde de la défense, pour maîtriser l'accès distant aux informations militaires classifiées dans les réseaux ancêtres d'Internet. Elle aboutit en 1986 à la publication des "Trusted Computer System Evaluation Criteria" (TCSEC), qui eurent un impact considérable dans le monde naissant de la sécurité informatique, mais qui se révélèrent inapplicables, tant les évaluations préconisées étaient longues et coûteuses.

Rapidement, la communauté économique européenne décida de se doter de ses propres critères : quatre pays avancés dans le domaine, le Royaume-Uni, l'Allemagne, les Pays-Bas et la France, publièrent conjointement en 1990 les "Information Technology Security Evaluation Criteria" (ITSEC), plus orientés vers les produits commerciaux civils. Les autres pays européens, moins avancés, reconnaissaient les évaluations effectuées par ces quatre pays, dans le cadre d'un accord appelé SOG-IS.

En parallèle, d'autres pays non européens développèrent leurs propres critères. Rapidement, il devint nécessaire d'unifier toutes ces initiatives, notamment pour permettre une reconnaissance mutuelle des évaluations. Ainsi émergèrent les « critères communs », initiés par l'ISO en 1999, qui furent reconnus par 17 pays dans le cadre de l'accord international CCRA. Toujours en vigueur aujourd'hui, ils sont utilisés dans le cadre des « certifications critères communs ».

Dans la foulée, la DCSSI (ancêtre de l'ANSSI) fit publier le décret 2002-535 du 18 avril 2002 qui instaura le schéma de certification français actuel, conforme aux « critères communs ». En 2008,

elle créa un autre type de certification, dite « certification de sécurité de premier niveau » (CSPN), plus simple et mieux adaptée aux produits logiciels.

La certification de sécurité en détail

La certification de sécurité est l'attestation de la robustesse d'un produit, basée sur une analyse de conformité et des tests de pénétration. Elle est réalisée sous l'autorité de l'ANSSI par des entreprises privées que celle-ci agrée, les « centres d'évaluation de la sécurité des technologies de l'information » (CESTI).

L'industriel souhaitant faire certifier un produit doit d'abord avoir établi une « cible de sécurité », c'est-à-dire la liste des propriétés de sécurité que son produit prétend satisfaire. La cible de sécurité trace en particulier la frontière entre ce qui est de la responsabilité du produit et ce qui est supposé acquis dans son environnement. Après vérification de la cohérence de cette cible de sécurité par l'ANSSI, l'évaluation est effectuée aux frais de l'industriel par un CESTI de son choix.

À la suite de cette évaluation, un rapport est rédigé par le CESTI et envoyé à l'ANSSI qui, au vu de son contenu, décide la certification ou non du produit, éventuellement en y ajoutant des conditions particulières d'emploi.

Dans le cas d'une certification effectuée selon les critères communs, le CESTI réalise deux grands types de travaux :

- d'une part, il vérifie la conformité des fonctions de sécurité du produit avec celles décrites dans la cible de sécurité, ainsi que sa conformité aux référentiels et critères d'évaluation (qui définissent, en fonction du niveau de certification souhaité, un niveau d'exigence et la puissance de l'attaquant considéré) ;
- d'autre part, il réalise une analyse de vulnérabilités pour s'assurer qu'il n'est pas possible pour un attaquant de contourner les fonctions de sécurité, en regardant le code source du produit, son architecture, la manière dont il doit être mis en œuvre, et en réalisant des tests de pénétration ciblés. En fonction des types de produits et des niveaux visés, ce type de certification peut durer entre 6 et 18 mois et est très coûteux. Il est particulièrement adapté aux composants de sécurité et aux puces des cartes bancaires.

La certification de sécurité de premier niveau française est réalisée en temps limité (25 jours si le produit ne contient pas de fonctions cryptographiques, 35 jours s'il en contient), en boîte noire (sans examen du code source) et est essentiellement un « avis d'expert » sur les fonctions de sécurité apportées par un produit, en prenant en compte un attaquant de niveau modéré. Cette certification n'est pas réalisée selon la méthodologie des critères communs et n'est donc pas reconnue au niveau international.

Les forces et les faiblesses de la certification

La certification offre à un industriel la possibilité unique de faire évaluer son produit en profondeur à un instant donné par un tiers réalisant des attaques de niveau élevé, selon un cadre reconnu internationalement.

Des évaluations coûteuses

Pour atteindre ce niveau d'exigence, des moyens importants sont mobilisés : les CESTI sont régulièrement audités par les meilleurs experts de l'ANSSI afin de s'assurer qu'ils sont bien en mesure de mettre en œuvre le niveau d'attaque attendu. Chaque évaluation est vérifiée par un certificateur de l'ANSSI, qui s'assure que tous les chemins d'attaque possibles ont été effectivement

testés ; en cas de doute, les experts de l'ANSSI et du CESTI engagent un dialogue de pair à pair. Tout ceci permet de garantir que les produits ont été évalués de manière très sérieuse, et que ceux qui obtiennent la certification sont de qualité. Mais, en contrepartie, les évaluations sont coûteuses, et elles ne restent compétitives que parce que l'État accepte d'entretenir à ses frais un centre de certification et des experts de haut niveau à l'ANSSI.

De plus, réaliser des attaques de niveau élevé nécessite des investissements conséquents en équipements et en ressources humaines, qui reflètent les moyens de plus en plus importants mobilisés par les attaquants (entre autres, des groupes criminels). À titre d'exemple, le niveau usuel de certification des cartes à puce requiert de mettre en œuvre des lasers ou des logiciels complexes d'analyse de code.

Une reconnaissance mutuelle difficile à atteindre en pratique

Si les critères communs fournissent une définition commune du niveau de l'attaquant, leur interprétation est difficile, et les évaluations opérées par les différents pays ne sont pas toujours équivalentes. Ainsi, pour les cartes à puce et les composants, des travaux sont menés en permanence par l'ensemble des parties prenantes européennes (industriels, centres de certification, CESTI) pour atteindre une interprétation uniforme de ces critères. Malgré ces travaux, des différences subsistent entre les pays, et l'assurance que chaque évaluation sera effectuée de la même façon dans chaque laboratoire reste illusoire.

Forts de ce constat, les États-Unis aujourd'hui ne réalisent plus que des tests de conformité pour les produits commerciaux. De même, au niveau mondial, seules les évaluations de simple conformité sont reconnues.

Un processus qui n'est pas adapté aux produits complexes ou aux systèmes

Pour être exhaustive, l'évaluation d'un produit selon les critères communs nécessite l'étude de sa documentation, de ses processus de développement, l'audit de ses sites de développement et de production, de ses processus de gestion de vulnérabilité, l'analyse de son code, la réalisation d'attaques physiques, et ce sur l'intégralité du périmètre du produit. Pour les produits complexes, les coûts deviennent rapidement prohibitifs.

De plus, cette certification n'est pas du tout adaptée aux produits modernes, qui sont souvent très connectés et composés d'applications fonctionnant sur des terminaux mobiles et des serveurs distants.

En limitant le nombre de jours utilisables par l'évaluation, la CSPN limite les coûts. Cependant, en temps limité, elle ne peut prétendre à l'exhaustivité, et elle n'est, par conséquent, adaptée qu'aux produits simples.

C'est aussi parce que la certification n'est pas adaptée à tous les cas qu'apparaissent de nouveaux modèles d'évaluation, comme les *bugs bounties*, qui promettent d'être plus agiles, ou les *pentests* mis en œuvre par des prestataires d'audits qui, bénéficiant d'un cadre moins strict, peuvent évaluer des systèmes complexes, voire des systèmes d'information dans leur intégralité (et se révèlent très utiles pour les applications modernes).

Une gestion des vulnérabilités perfectible

Si la certification permet de se faire une bonne idée de la sécurité apportée par un produit, il est fort probable que des vulnérabilités soient découvertes pendant sa durée de vie, remettant potentiellement en cause la valeur du certificat délivré. Pour en tenir compte, certains produits sont réexaminés périodiquement, et les certificats sont depuis peu archivés au bout de cinq ans (ce qui indique qu'un produit ne peut plus être considéré de confiance au-delà de cette durée sans réévaluation).

Cependant, il n'existe pas de moyen simple de réévaluer un produit déjà évalué lorsque celui-ci a été modifié (par exemple en cas de correction d'un *bug* ou d'une vulnérabilité). Selon la procédure, sauf pour quelques cas très simples, il faudrait effectuer à nouveau la plupart des tâches.

De ce fait, ces mécanismes n'incitent pas les industriels à corriger leurs produits certifiés, et on peut encore aujourd'hui trouver des produits certifiés vulnérables, alors que des produits non certifiés sont à jour.

La certification ne vaut pas recommandation

Lorsque l'ANSSI certifie un produit, elle vérifie qu'il offre bien les fonctionnalités de sécurité qu'il prétend apporter, mais elle ne donne pas d'avis sur l'utilité ou la pertinence du produit. Ceci est une source de grande confusion chez les acquéreurs, qui pensent qu'une certification vaut recommandation.

Par contre, lorsque l'agence souhaite recommander l'utilisation d'un produit, notamment par les administrations et les opérateurs d'importance vitale (les entreprises les plus critiques de la nation), elle utilise un autre processus nommé « qualification », qui est basé sur une ou plusieurs certifications, dont les cibles de sécurité jugées pertinentes, mais aussi sur d'autres éléments comme les processus de gestion des vulnérabilités.

Cependant, la qualification est critiquée par ses utilisateurs, car elle recommande parfois des produits dont la sécurité a été évaluée en profondeur, mais qui sont bien moins performants que leurs concurrents. Prenant cette problématique très au sérieux, l'ANSSI réfléchit à l'inclusion dans ce processus de tests fonctionnels et ergonomiques, réalisés en partenariat avec les utilisateurs.

L'avenir : la certification européenne

Faisant le constat que plusieurs schémas de certification existaient, ou étaient en cours de création, dans divers pays de l'Union européenne, créant de ce fait des barrières au sein du marché intérieur et un manque de lisibilité pour les clients, la Commission européenne a proposé la mise en place d'un cadre de certification européen pour les produits, services et processus numériques, qui s'est concrétisé par la publication du "Cybersecurity Act" en juin 2019 (et qui doit entrer en vigueur en juin 2021).

La certification européenne définit trois niveaux de certification : « élevé », « substantiel » et « élémentaire » :

- Dans le cadre d'une évaluation de niveau élevé, des tests de pénétration sont menés par un tiers de confiance comme pour la majorité des évaluations critères communs effectuées en France. La certification est dans ce cas opérée préférentiellement par un organisme public.
- Le niveau substantiel repose lui sur des tests de conformité, dans un esprit similaire à l'approche américaine, qui incluent la prise en compte des vulnérabilités connues. Dans ce cas, la certification est réalisée par un tiers de confiance privé accrédité.
- Enfin, le niveau élémentaire laisse ouvert la voie à l'auto-évaluation du produit par son développeur, se rapprochant ainsi du marquage CE.

L'existence d'un niveau plus faible avec des tests plus simples, donc plus rapides, ouvre ainsi la voie à la certification d'un nombre bien plus important de produits, par exemple les objets connectés.

Cette nouvelle certification européenne va, assez naturellement, donner un cadre européen officiel au SOG-IS, mais aussi chercher à certifier de nouveaux objets, tels que les services d'informatique « nuagique » (*cloud computing*), l'IoT (*Internet of Things*), les équipements 5G ou des processus comme la certification ISO 27001 qui concerne le management de la sécurité des systèmes

d'information. Dans un second temps, des schémas dits sectoriels, adaptés spécifiquement à un secteur de l'industrie comme l'automobile ou la santé, pourraient être étudiés.

Cette certification introduit aussi des améliorations méthodologiques, comme la possibilité d'utiliser des processus analogues à la CSPN pour le niveau élevé. Enfin, elle imposera une meilleure gestion des vulnérabilités : un produit vulnérable perdra certes sa certification, mais la version corrigée pourra la récupérer plus rapidement par l'application d'une méthode sûre et rapide reposant, notamment, sur un processus audité de gestion des correctifs.

Conclusion

La certification est un processus complexe et potentiellement coûteux, qui est perfectible, mais qui reste néanmoins une manière objective et largement reconnue d'évaluer un produit de sécurité : c'est pour l'ANSSI la manière standard de se faire un avis sur un produit. La certification française, globalement de très haut niveau, est reconnue internationalement comme étant de qualité.

La certification européenne, qui est toujours en cours de négociation, est porteuse d'un grand nombre d'améliorations visant à rendre les processus plus performants. Mais au travers de l'élargissement de son champ d'action à de nouveaux types d'objets et à des niveaux plus faibles, elle devrait surtout contribuer à renforcer, pour les entreprises, mais aussi, et c'est une nouveauté, pour les citoyens, la confiance dans le numérique.