



Article de Hugo Fortier
Conseiller en sécurité
ESI Technologies

La sécurité par l'obscurité : un concept dangereux

La sécurité par l'obscurité est un principe controversé par lequel la dissimulation est utilisée pour assurer la sécurité d'un produit. Autrement dit, des informations d'importance concernant la sécurité de celui-ci ne sont pas rendues publiques. Les concepteurs d'un système dont la protection repose sur cette philosophie font le raisonnement suivant : puisque les vulnérabilités du produit – théoriques ou réelles – demeurent inconnues, les probabilités sont minces que d'éventuels pirates puissent les exploiter.

De nombreuses voix s'élèvent contre cette croyance : si la sécurité d'un produit ou d'un système dépend seulement ou principalement du secret entourant ses vulnérabilités, il est manifeste qu'elle sera facilement compromise le jour où ces faiblesses seront connues. Il existe des exemples qui en font foi : Microsoft, Diebold et Cisco, entre autres organisations, ont été victimes de cette pratique.

Théorie mal fondée

L'exemple classique évoqué pour illustrer le concept de sécurité par l'obscurité (selon l'expression anglaise *security by obscurity*) est la clef que l'on dissimule sous le paillason, en supposant que personne ne pourra la trouver. À juste titre, on peut arguer que le stratagème étant passablement connu, il est fort possible qu'un cambrioleur vérifie si une clef ne se trouve pas à cet endroit précisément.

Considérons l'histoire suivante : un programmeur ayant percé le secret de la fonction de chiffrement d'un tableur communique avec son fabricant afin qu'il diffuse les correctifs nécessaires pour éviter aux utilisateurs les problèmes pouvant découler de cette faille. Le fabricant répond en sommant le programmeur de ne pas révéler la méthode permettant de percer le code, ni même de divulguer qu'il existe une possibilité de le faire, sous peine de poursuites judiciaires.

En agissant de la sorte, le fabricant estime que personne d'autre que ce programmeur ne pourra déjouer la fonction de chiffrement du produit, et que, par conséquent, personne d'autre avant lui n'a réussi à faire la même chose sans l'ébruiter. Autre facteur à ne pas perdre de vue, la divulgation des failles d'un système peut aussi se faire accidentellement.

Peu d'avantages...

De nombreux fabricants préfèrent garder secret les bogues qu'ils découvrent dans les fonctions de sécurité de leurs logiciels, sans même savoir si un tiers n'a pas déjà trouvé ces lacunes et commencé à les exploiter. Il est vrai qu'il peut être tentant de choisir cette méthode, car le fournisseur n'en paye pas le prix directement. Ce sont plutôt les utilisateurs qui, les premiers, ont à réparer les dégâts qu'elle peut causer. À long terme, toutefois, le choix n'est pas viable, ne serait-ce qu'en raison de l'atteinte à la réputation de l'entreprise.

Il existe peu d'avantages à adopter la sécurité par l'obscurité : le seul que l'on puisse dégager serait que cette forme de protection peut retarder l'ennemi dans ses tentatives de déjouer la sécurité d'un produit ou de faire une copie de celui-ci. En ce sens, la dissimulation des bogues peut agir en tant que couche supplémentaire au sein d'un système de sécurité multicouche; en cas de découverte des failles dissimulées, les autres couches continuent à assurer la protection.

...et beaucoup de risques

Toutefois, la sécurité par l'obscurité ne constitue pas à elle seule un rempart contre les menaces. Outre sa faiblesse évidente, la méthode comporte aussi un inconvénient important : puisque les informations techniques associées aux brèches affectant la sécurité sont gardées secrètes, un nombre très limité de spécialistes sont en mesure de faire les analyses qui permettraient éventuellement de les colmater. De plus, ces experts mettront généralement plus de temps à compléter le travail.

Dans le cas de produits à code source libre, de nombreux programmeurs ont accès aux informations pertinentes, ce qui accroît les probabilités de détection et de correction des faiblesses conceptuelles. Il est donc permis de croire que la publication du code source améliorerait la sécurité d'un produit, ce qui constitue une idée diamétralement opposée à la philosophie de l'« obscurantisme ».

Diffusion de rustines

Il est communément admis que la mesure la plus sûre qui puisse être adoptée par un fabricant de logiciel consiste à diffuser une rustine, le plus tôt possible après qu'une faille ait été découverte dans la sécurité de son produit, et d'informer l'ensemble des utilisateurs qu'ils doivent l'installer. Beaucoup de fabricants procèdent de cette façon, mais il faut faire attention car certaines rustines, n'ayant rien à voir avec la sécurité du produit, contiennent en fait un correctif destiné à régler une faille gardée secrète. En ne révélant pas que leur produit comporte un trou de sécurité, les concepteurs tiennent à

préservent leur réputation. Cependant, dans la réalité, ils rendent un bien mauvais service à leurs clients qui, pourraient très bien juger que la rustine n'est pas primordiale et choisir de ne pas l'installer...

C'est d'ailleurs grâce à la diffusion de rustines, que le sujet de la sécurité par l'obscurité est demeuré d'actualité malgré une baisse d'intérêt au cours des dernières années. En raison des pratiques de certains fabricants, les rustines sont maintenant analysées minutieusement par des spécialistes qui utilisent des outils évolués d'ingénierie inverse pour déceler les informations qu'elles pourraient cacher.

Un exemple d'un tel outil est le logiciel BinDiff, développé en Allemagne. En raison de la prolifération de programmes semblables, le concept de sécurité par l'obscurité est de moins en moins applicable : les logiciels d'ingénierie inverse étant accessibles à un plus grand nombre de personnes, ils font en sorte que les trous de sécurité cachés sont décelés plus rapidement.

Il semble également que le mot se soit répandu au sein de l'industrie, quant aux dangers que recèle la sécurité par l'obscurité. Il est donc à espérer que le mouvement de dénonciation s'accélère afin que cette pratique soit universellement abandonnée.