> électroniques, et l'offuscation de liens internet.

Pour qu'un ordinateur exécute un programme, il doit en disposer d'une copie, et donc le programme ne peut pas être secret. C'est ennuyeux si les auteurs de ce programme souhaitent protéger les idées, algorithmes, codages des données, etc., qu'ils ont utilisés et peut-être inventés à cette fin. Il en va de même pour les circuits électroniques qui, d'une certaine façon, sont des programmes transformés en objets : en vendant un circuit, il semble que vous rendez accessible à l'acheteur les idées qui ont permis de le concevoir, qu'il peut alors voler et réutiliser à votre insu. L'offuscation des programmes et des circuits est devenue une question grave.

En informatique, on distingue le programme source écrit en langage de haut niveau, assez facile à lire par un humain, et le programme compilé, résultat de la transformation du programme source en instructions directement exécutables par l'ordinateur (ou en circuit électronique si l'on considère la version matérielle d'un programme). Cette transformation rend en général assez incompréhensible la logique utilisée pour concevoir le programme, donc ses idées. Cependant, des techniques dites de désassemblage ou de décompilation permettent de retrouver un certain nombre d'informations du programme source, voire de rendre parfaitement clairs les traitements qu'opère le programme compilé (ou le circuit).

RENDRE ININTELLIGIBLE SANS EMPÊCHER DE FONCTIONNER

Pour éviter cette rétro-ingénierie, des techniques d'offuscation empêchent la compréhension et donc la réutilisation des idées des programmes et circuits, cela sans compromettre leur fonctionnement.

3 OFFUSCATION MILITAIRE

Les militaires utilisent diverses méthodes d'offuscation, par exemple pour se fondre eux-mêmes dans les paysages ou, à l'inverse, pour exhiber des armes en grand nombre… mais factices. En voici deux exemples.

L'opération Fortitude

La désinformation a joué un rôle important dans l'organisation et la mise en œuvre du débarquement allié en Normandie, en 1944. L'opération Fortitude, destinée à masquer le lieu exact du débarquement, a été un succès, et son rôle a sans doute été décisif dans l'issue de la guerre contre les nazis. Les Alliés ont utilisé dans le cadre de cette opération divers stratagèmes :

– de faux chars gonflables et de faux bateaux ;
– des unités fantômes menant une intense activité radio ;
– des fuites délibérées de fausses informations vers les diplomates des États neutres, qui ensuite parvenaient aux Allemands ;
– des agents doubles intoxiquant les services secrets allemands ;
– des reconnaissances aériennes et maritimes intenses sur toute la longueur de la côte pour que l'ennemi ne dispose d'aucun indice sur le lieu réel du débarquement ;
– des bombardements sur le nord de la France laissant croire que la priorité était le Pas-de-Calais.

Les généraux allemands furent persuadés que le débarquement en Normandie était une diversion. Ils choisirent de maintenir en alerte les 150 000 hommes de leur XV[e] armée dans le Pas-de-Calais et ne prirent que tardivement la décision d'envoyer ces troupes combattre en Normandie.

Après le débarquement, ces opérations massives d'offuscation se sont poursuivies avec une armée fantôme, la « Ghost Army » composée de 1 000 hommes qui en simulaient 30 000. Elle suivait l'armée réelle et utilisait toutes les techniques possibles de désinformation pour perturber les décisions allemandes et disperser leurs efforts.

Les bateaux et avions furtifs

Les avions militaires sont aujourd'hui conçus pour avoir des signatures radar et infrarouge aussi faibles que possible. La furtivité radar d'un avion est caractérisée par sa « surface équivalente radar », ou SER, qui est la superficie plane qui renverrait la même énergie que l'avion. On sait obtenir des valeurs de SER de l'ordre du mètre carré pour les avions. Le Lockheed Martin F-22 Raptor de l'armée de l'air des États-Unis *(photo ci-dessus)* aurait même une SER équivalente à celle d'un oiseau.

Voici des procédés élémentaires pour brouiller la lecture d'un programme, même quand il est écrit en langage de haut niveau :

– Supprimer les commentaires du programme. C'est la première et la plus simple des opérations d'offuscation envisageables.

– Changer le nom des variables pour qu'elles n'évoquent rien, par exemple en les nommant v1, v2, v3, v4, ..., et utiliser plusieurs fois les mêmes noms de variable quand il est possible de le faire sans perturber le fonctionnement.

– Compresser le programme au maximum. Certains langages comme le Fortran ont la propriété qu'en supprimant tous les blancs d'un programme, rien ne change dans son fonctionnement ; mais ce n'est pas le seul type de compression envisageable. Des raccourcis de syntaxe sont souvent prévus et les utiliser systématiquement obscurcira un programme.

– Compliquer sans véritable raison. À l'inverse de la compression, l'introduction d'instructions inutiles qui ne seront jamais exécutées produira aussi des difficultés de compréhension. Par exemple on peut ajouter des « si-alors_sinon » allant toujours vers la même alternative et qui ne serviront donc à rien.

– Brouiller la logique du programme avec des « go to » qui introduisent de la confusion en plaçant par exemple au début ce qui ne s'exécute qu'à la fin, ou inversement.

– Utiliser des particularités peu connues du langage.

Signalons à ce propos l'existence d'un concours annuel d'offuscation, l'IOCCC (International Obfuscated C Code Contest, www.ioccc.org).

Il existe aussi des programmes « offuscateurs » qui automatisent le brouillage. Partant d'un programme P, un programme offuscateur Offus le transforme en un programme P' = Offus(P) aussi peu lisible que possible, sans en changer le fonctionnement : P et P' font toujours exactement la même chose pour tout jeu de données.

Malheureusement, une série de résultats, dus en particulier à Boas Barak, des Laboratoires de Microsoft à Cambridge, montrent qu'il ne peut exister de méthodes générales et efficaces d'offuscation. Cela n'interdit pas que d'assez bons systèmes soient aujourd'hui disponibles.

OFFUSCATION DE LIENS INTERNET

Les pages internet comportent des liens (les URL, pour *uniform resource locater*) qui, lorsque le lecteur clique dessus, conduisent chacune à une autre page, pointée par le lien associé. Les robots d'indexation des moteurs de recherche parcourent aussi systématiquement que possible tout le web en exploitant ces liens et en les suivant pour visiter les pages correspondantes et compléter leurs données. Par ailleurs, les moteurs de recherche mesurent la notoriété d'une page pour déterminer sa position dans une liste de liens donnée en réponse à une requête ; pour ce faire, ils prennent en compte le nombre de liens pointant vers cette page identifiés dans les pages parcourues par leurs robots. Ce que voient ces robots doit donc être contrôlé.

Parfois les développeurs web ne veulent pas que certains liens soient suivis par les robots ou soient clairement lisibles, car ils ne souhaitent pas favoriser les notations des pages indiquées en lien, ou parce qu'ils ne veulent pas dévoiler l'URL vers laquelle ils vous envoient, ou encore parce que la mauvaise réputation de la page indiquée pourrait entraîner une pénalité de réputation pour la page qu'ils écrivent, voire son placement sur une liste de pages frauduleuses à ne jamais recommander.

Les développeurs web recherchent donc parfois, pour les pages qu'ils conçoivent, à empêcher le suivi de certains liens par les robots des moteurs de recherche, tout en faisant ce qu'il faut pour qu'un lecteur de la page puisse cliquer sur le lien et provoquer normalement le saut vers la page en question. Ce problème est celui de l'offuscation de liens : on veut indiquer un lien sans que les robots des moteurs de recherche le sachent. Il a été résolu par diverses méthodes.

Ajouter une indication « no follow » prévue pour cela dans le codage des pages web est une méthode qui devrait dissuader les robots de prendre en compte le lien concerné. Cependant, on soupçonne que les robots d'indexation ne respectent pas ce type de commande. Il faut donc trouver autre chose. Certaines techniques reviennent, en gros, à faire en sorte que le lien ne sera pas inscrit dans le texte de la page web elle-même, mais sera calculé ou lu ailleurs, puis seulement mis en action. De cette façon, un utilisateur de la page ne percevra pas de différence avec un lien usuel, alors qu'un robot ne verra pas l'URL (voir https://pxagency.fr/nofollow-obfuscation/ pour des détails techniques).

À côté du chiffrement de données, des signatures numériques et des problèmes d'authentification, l'offuscation consiste à perturber les analyses de ceux qui exploitent les données que vous ne pouvez pas faire disparaître, tels qu'un programme, un lien internet ou vos comportements sur les réseaux. Les problèmes informatiques qu'elle pose ouvrent un nouveau chapitre de la science cryptographique : les développements des ordinateurs et des réseaux obligent à repenser cet art de la dissimulation devenu essentiel à la protection de notre vie privée, ou du secret des algorithmes que l'on souhaite vendre mais pas divulguer. ■

BIBLIOGRAPHIE

H. Nissenbaum et F. Brunton, **Obfuscation - La vie privée, mode d'emploi**, C&F Éditions, 2019.

G. Di Crescenzo, **Cryptographic program obfuscation : Practical solutions and application-driven models**, dans M. Conti *et al.* (éds.), *Versatile Cybersecurity*, Springer, 2018, pp. 141-167.

H. Xu *et al.*, **On secure and usable program Obfuscation : A survey**, prépublication arXiv:1710.01139, 2017.

D. Forte *et al.*, **Hardware Protection Through Obfuscation**, Springer, 2017.

B. Barak *et al.*, **On the (im) possibility of obfuscating programs**, *Journal of the ACM*, vol. 59(2), article 6, 2012.

P. Baud, **Axolot #8 : Fake !**, vidéo sur les fausses informations : https://youtu.be/IvMzllKrJEQ