

acoustique), éviter d'être repéré par les radars (discrétion radar), éviter d'engendrer trop de chaleur (discrétion thermique), éviter d'être identifié par les télémètres (discrétion laser), et éviter d'être repéré en émettant soi-même des ondes radar!

Pour obtenir cette furtivité, on joue à la fois sur les formes géométriques, sur les matériaux, sur les trajets empruntés, par exemple en favorisant le vol à très basse altitude. On utilise aussi des leurres, du brouillage ou, mieux, de la manipulation électronique des ondes en renvoyant au radar ennemi un signal de même fréquence que celui qu'il émet. On étudie aussi des techniques pour entourer les avions d'un champ de plasma qui absorbe les ondes radar.

Dans les conflits modernes, induire en erreur l'ennemi par la désinformation prend des formes cruelles dont la loyauté est parfois discutée. Pendant la guerre d'Algérie, la Bleuite fut une opération d'infiltration et d'intoxication à grande échelle, montée par les services secrets français du SDECE (Service de documentation extérieur et de contre-espionnage). Elle resta longtemps méconnue du public, malgré ses effets dévastateurs. Les agents français dressaient des listes de prétendus collaborateurs algériens de l'armée française et les faisaient parvenir aux chefs de l'Armée de libération nationale algérienne. Ces fausses informations ont provoqué de terribles purges internes qui ont fait des centaines de morts parmi les cadres combattants algériens.

FAUSSES LANGUES

Un bel exemple, lui aussi ancien, d'offuscation est celui des fausses langues telles que le verlan, le javanais ou le louchébem, des argots plus ou moins codifiés issus du français. Tout le monde connaît le verlan dont le principe consiste à changer l'ordre des syllabes ou des lettres d'un mot pour le rendre incompréhensible. La transformation est parfois assez compliquée. Exemples de mots en verlan: la reum, une meuf, un keum, la teuf, un rebeu, la zicmu, une caillera, pécho, vénère, reuf, reup, laisse béton (pour la traduction et d'autres exemples, voir www.francaisavec pierre.com/le-verlan/).

Le javanais procède d'une déformation des mots plus mécanique, où l'offuscation consiste à ajouter des lettres selon les règles suivantes (voir [https://fr.wikipedia.org/wiki/Javanais_\(argot\)](https://fr.wikipedia.org/wiki/Javanais_(argot))):

- Ajouter *av* après chaque consonne (sauf si elle est finale) ou groupe de consonnes tel que *ch*, *cl*, *ph*, *tr*, etc. (train → travain, bon → bavon, champion → chavampavion, bonjour → bavonjavour). Ne pas ajouter *av* dans le cas du *e* muet (tarte → tavarte).

- Ajouter *av* aux mots monosyllabes (*a* → *ava*, *en* → *aven*, *un* → *avun*, etc.) et aux mots commençant par une voyelle

(abricot → avabracicavot, allumettes → avallavumavettes, immeuble → avimmaveuble).

- Considérer le *y* comme une consonne s'il est suivi d'une voyelle (moyen → mavoyaven).

Le louchébem, qui fut utilisé par les bouchers, se définit en une seule phrase: substituer *l* à la consonne initiale de la première syllabe du mot ou, si le mot commence par un *l* ou une voyelle, de la syllabe suivante et rétablir, en fin de mot, la consonne initiale avec un suffixe libre. On a ainsi: bonjour → lonjourbem, boucher → louchébem, client → lienclès, lame → lalamen, café → laféquès, combien → lombienquès, comprendre → lomprenquès, en douce → en loucedé.

Le jeu des contrepèteries est aussi une forme d'offuscation pratiquée pour échanger des messages à caractère grivois. Comme pour le verlan, on permute des syllabes ou des lettres, mais cette fois le jeu s'applique non plus à des mots isolés mais à des phrases, ce qui rend parfois très délicat le déchiffrement. Voici quelques exemples: des boules antimites; cet ordi me remplit de joie; l'hirondelle ne craint pas la traque; attention aux coups de feu; les soupers russes manquent de pain; quand les athées se battent, les abbés se taisent (voir <https://lapoulequimue.fr> pour les solutions).

Parmi les méthodes d'offuscation utilisées par les malfrats, les militaires, les espions ou les écrivains, mentionnons encore le simple changement d'identité, les déguisements, la radio que l'on fait hurler pendant que l'on parle, et l'anagramme ou l'acrostiche qui permettent de signer discrètement un texte comme l'ont fait Boris Vian avec Bison Ravi et François Villon avec ce poème:

Vous portâtes, digne Vierge, princesse,

Iésus régnant qui n'a ni fin ni cesse.

Le Tout-Puissant, prenant notre faiblesse,

Laissa les cieux et nous vint secourir,

Offrit à mort sa très chère jeunesse;

Notre Seigneur tel est, tel le confesse:

En cette foi je veux vivre et mourir.

AVEC L'INFORMATIQUE, L'OFFUSCATION RENOUVELÉE

Avec l'informatique, de nouvelles formes d'offuscation sont apparues, et elles y jouent des rôles parfois centraux. J'ai déjà mentionné les méthodes consistant à brouiller les pistes pour fausser les données récoltées par ceux qui nous espionnent en cliquant sur des liens qui ne nous intéressent pas, ou en utilisant des techniques de camouflage réseau.

Je ne détaillerai pas la pratique massive des infox (*fake news*) dans les réseaux sociaux modernes qui ne sont que de la diffusion d'informations fausses. En revanche, je mentionnerai deux types d'offuscations nouvelles liées aux technologies de l'information: l'offuscation de programmes informatiques et de circuits >

OFFUSCATION OU OBFUSCATION

« Offuscation » est un mot dérivé du latin *offuscare*, qui signifie « obscurcir ». Il était notamment utilisé en astronomie (par exemple : « offuscation du soleil par les nuages »). En anglais, le terme est *obfuscation*, et cette orthographe avec un *b* est parfois utilisée en français. Le problème de la bonne orthographe a donné lieu à un âpre débat sur [wikipedia](https://fr.wikipedia.org/wiki/Discussion:Offuscation) (voir <https://fr.wikipedia.org/wiki/Discussion:Offuscation>) qui a finalement adopté, comme on le fait ici, les deux *f*. Le terme « brouillage » est parfois recommandé, mais nous lui préférons « offuscation », simple à prononcer et présent dans les dictionnaires de langue française.

> 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.

OFFUSCATION MILITAIRE

3



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.

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, **Axolotl #8 : Fake !**, vidéo sur les fausses informations : <https://youtu.be/IvMzllKrJEQ>

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'obfuscation 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'obfuscation, l'IOCCC (International Obfuscated C Code Contest, www.ioccc.org).

Il existe aussi des programmes « obfuscateurs » qui automatisent le brouillage. Partant d'un programme P, un programme obfuscateur 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'obfuscation. 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 locator*) 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'obfuscation 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'obfuscation 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. ■