

> 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. ■

L'AUTEUR



LOÏC MANGIN
rédacteur en chef adjoint
à *Pour la Science*

UN PEU PLUS PRÈS DES ÉTOILES

Invitée de la «Résidence 1+2», qui associe photographes et scientifiques, Manon Lanjouère explore le rêve d'Icare et les études balistiques qu'il impose... pour les prolonger.

Le 16 juillet 1969, 13 h 32, Cap Canaveral, en Floride. C'était il y a tout juste cinquante ans. Près d'un million de spectateurs sont là, les yeux rivés vers le ciel, les mains en visière pour éviter l'éblouissement. Ils ont tous fait le déplacement pour assister au décollage, historique, de la fusée *Saturn V* emmenant à son bord les hommes qui, les premiers, poseront le pied sur la Lune cinq jours plus tard.

Manon Lanjouère n'était pas née, mais elle a tout autant que le public du

centre spatial Kennedy les yeux tournés vers le ciel, la Lune et, plus encore, vers l'espace. Diplômée en 2017 de l'école des Gobelins, elle est l'une des trois photographes de la quatrième «Résidence 1+2». Cette manifestation organisée à Toulouse associe le monde de la photographie d'auteur à l'univers scientifique particulièrement dense dans la région Occitanie. Pendant deux mois, les photographes, d'horizons différents, côtoient le monde de la recherche.

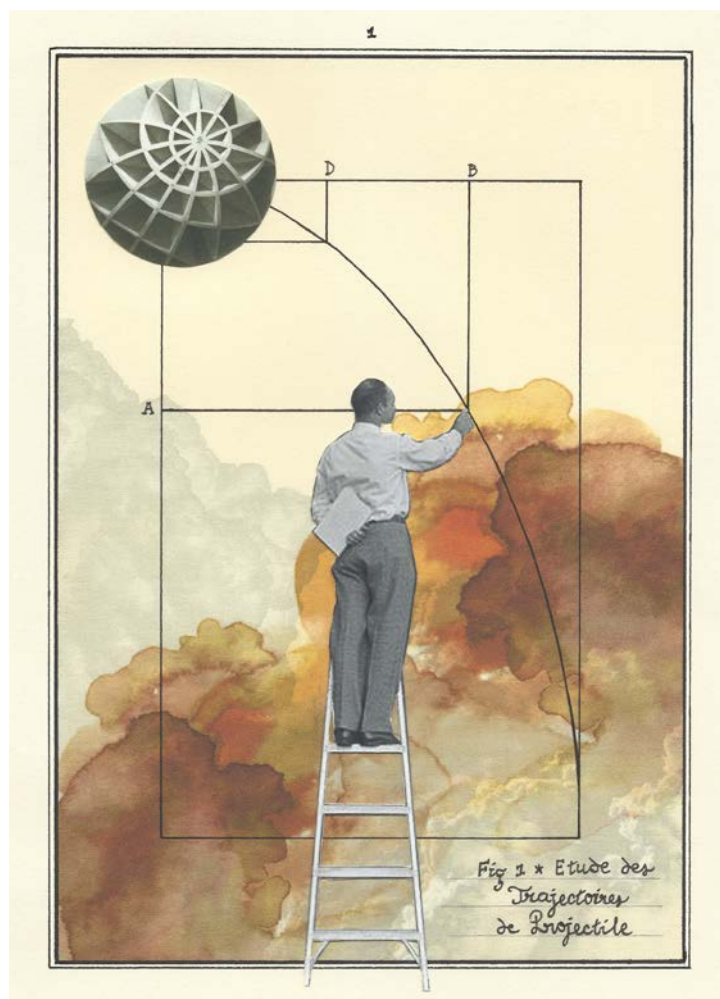
Les échanges ont été très fertiles: «Nous, les scientifiques, nous sommes très accrochés à la réalité», avoue Sylvestre Maurice, astrophysicien à l'Institut de recherche en astrophysique et planétologie, à Toulouse, et parrain de l'édition 2019. «Nous sommes des explorateurs à vrai dire assez peu rêveurs. Avec eux [les photographes], j'ai retrouvé cette part de rêve.»

Manon Lanjouère a pris ses quartiers auprès de Serge Gracieux, muséographe à la Cité de l'espace, et de Laurent Joly, chef du département d'aérodynamique, énergétique et propulsion et professeur à l'Institut supérieur de l'aéronautique et de l'espace (Isae-Supaero).

La photographe s'est intéressée aux méthodes pour atteindre les altitudes extrêmes, au désir de voler, aussi ancien que l'humanité. Cette quête s'est longtemps heurtée à la physique dont les lois comme celle de la gravitation s'opposent à l'envol. Comment résoudre ce problème? Comment s'affranchir de tels



Les yeux tournés vers le ciel pour rejoindre le ciel, la Lune et l'espace tout entier. Un rêve devenu réalité grâce à la balistique.



obstacles? La résidence fut pour Manon Lanjouère l'occasion de faire un grand voyage dans l'histoire de la mécanique de la propulsion et vers le vide spatial.

Elle s'est notamment approprié la balistique (la mère de l'astronautique), cette science des trajectoires de tout projectile, de la balle lancée dans une cour de récréation aux plus grosses fusées. Ses clichés (*voir deux d'entre eux ci-dessus*) se nourrissent des travaux de Tartaglia et de Galilée aux ^{xvi}^e et ^{xvii}^e siècles sur les courbes dessinées par les boulets de canon jusqu'aux succès de la mission *Apollo 11* et de Neil Armstrong.

Elle pousse encore plus loin le rêve d'Icare en s'interrogeant sur des futurs voyages emportant des humains en impesanteur plus loin encore que la Lune, seulement «premier jalon sur la route de l'infini» selon elle, «vers un territoire noir, un continent qui n'a plus l'horizon pour limite.»

Les deux autres photographes invités de la «Résidence 1+2» sont Matthieu Gafsou et Matilda Holloway. Le premier s'est penché sur les sciences de l'environnement et les sciences humaines, la seconde sur les sciences de la représentation et les sciences naturelles. L'ensemble

des photographies sont exposées à la Chapelle des Cordeliers, à Toulouse. Elles sont également au cœur d'un coffret de trois ouvrages, publié chez Filigranes. Enfin, le vidéaste Citizen JiF a eu «carte blanche» pour réaliser un film mettant en perspective les trajectoires des résidents. Encore une histoire de trajectoire... ■

Le site de la Résidence : www.1plus2.fr



L'auteur a publié :
Pollock, Turner, Van Gogh, Vermeer et la science...
(Belin, 2018)

LES AUTEURS



JEAN-MICHEL COURTY et ÉDOUARD KIERLIK
professeurs de physique à Sorbonne Université, à Paris

QUAND LE PONT BALANCE, LES PIÉTONS DANSENT

**On croyait tout savoir sur la conception des ponts.
En fait, on avait oublié l'effet de leurs vibrations
sur la marche des piétons qui les franchissent.**

Le 10 juin 2000, le Millennium Bridge (la « passerelle du millénaire »), à Londres, était inauguré. Alors qu'une foule compacte le traversait, le pont s'est mis à osciller d'un côté à l'autre. L'amplitude du mouvement a atteint plusieurs centimètres, au point que les personnes étaient obligées de se tenir aux balustrades pour ne pas tomber. Les autorités fermeront la passerelle au public deux jours plus tard. Et il faudra 18 mois et 5 millions de livres de travaux sur la structure pour empêcher que la situation se reproduise.

Pourquoi les ingénieurs n'avaient-ils pas prévu une oscillation aussi forte ? En fait, un mécanisme original avait échappé à toutes les modélisations antérieures : lorsque les piétons sont assez nombreux, leur marche se synchronise spontanément avec les oscillations de la passerelle.

Pour comprendre les oscillations du Millennium Bridge, deux catastrophes datant du XIX^e siècle sont riches d'enseignements. La première s'est produite en 1831 avec le pont de Broughton, au Royaume-Uni : il s'est effondré lorsqu'une troupe de 60 militaires marchant au pas le franchissait. Pourquoi ? À cause d'un effet de résonance bien connu, dû à la coïncidence entre la fréquence du pas des soldats avec l'une des fréquences naturelles de vibration du pont.

RÉSONANCE SUR PONT OU SUR BALANÇOIRE

Le phénomène est le même que celui à l'œuvre lorsqu'on pousse un enfant sur une balançoire à chaque fois qu'il revient vers nous. Il n'est pas nécessaire que l'énergie fournie à chaque poussée soit importante pour que l'amplitude de l'oscillation augmente. Il suffit qu'elle soit

supérieure aux pertes subies par la balançoire lors d'une oscillation.

Dans le cas du pont de Broughton, l'effet d'un seul piéton marchant normalement était insuffisant pour le faire vibrer, car la dissipation l'emportait. Tel n'était plus le cas lorsque l'énergie était apportée par 60 gaillards marchant au pas ; d'autant plus que, amusés par les oscillations naissantes, ils se sont mis à marcher au rythme exact des mouvements du pont. Ainsi, à chaque pas, l'effet de l'impulsion verticale des pieds s'ajoutait à celui des pas précédents. L'amplitude des vibrations – ici verticales – s'est alors amplifiée jusqu'à ce que le pont cède.

