Spirale
arts • lettres • sciences humaines

SPIRALE

Cache-cache : décentralisation, pair-à-pair et confidentialité. Entretien avec David McKinney, développeur et testeur d'intrusion chez Subgraph

Marie-Ève Fortin

Numéro 257, été 2016

Sous le radar

URI : https://id.erudit.org/iderudit/83626ac

Aller au sommaire du numéro

Éditeur(s)

Spirale magazine culturel inc.

ISSN

0225-9044 (imprimé)
1923-3213 (numérique)

Découvrir la revue

Citer cet article

Fortin, M.-È. (2016). Cache-cache : décentralisation, pair-à-pair et confidentialité. Entretien avec David McKinney, développeur et testeur d'intrusion chez Subgraph. *Spirale*, (257), 43–47.

CACHE-CACHE : DÉCENTRALISATION, PAIR-À-PAIR ET CONFIDENTIALITÉ

PAR MARIE-ÈVE FORTIN

Entretien avec David McKinney, développeur et testeur d'intrusion chez Subgraph

À la surface de l'océan informationnel flotte tout ce qui se reproduit et finit par s'alourdir du poids de sa propre multiplicité proliférante. Tous les objets surchargés des aléas de la surexposition, du visionnement frénétique, des commentaires, du partage, de la circulation et des couches de sens qui y sont plaquées finissent par couler à pic sous le poids de leur propre obésité sémantique. Comment nous assurer que les résidus photographiques, bribes de conversations et autres informations vétustes que nous laissons tomber, faute de temps, dans les profondeurs insondables de l'internet ne se retrouveront pas dans des filets ennemis ? Et qui sera ultimement apte à extraire du sens de la masse de plus en plus compacte de données en circulation, à l'organiser et à y tracer de nouveaux itinéraires ?

LOIN D'ÊTRE DOGMATIQUE, PARANOÏAQUE OU CATASTROPHISTE, DAVID MCKINNEY ŒUVRE À TROUVER DES SOLUTIONS DE CONNECTIVITÉ ET DE COMMUNICATION QUI PERMETTENT D'ÉVITER LES PLATEFORMES À GRAND TRAFIC DANS UN SOUCI DE CONFIDENTIALITÉ, MAIS AUSSI DE TRANSPARENCE.

Nous supposons qu'une certaine intelligibilité émergera du récit des explorateurs, soit de ceux qui effectuent des allers-retours entre les profondeurs et la surface : entre les mondes entérinés par les pouvoirs et ceux qui s'y dérobent ; entre le code indéchiffrable pour la plupart et la page qui s'affiche comme par magie, en langues et images compréhensibles ; entre les masses de données et les contenus organisés. Ces plongeurs, ce sont les codeurs, les informaticiens, les *geeks* et les spécialistes du traitement de l'information, mais aussi tous ceux qui cherchent autre chose que ce qui s'affiche *par défaut*. Parallèlement, chacun de nous peaufine ses habiletés de pêcheur virtuel pour être en mesure de trouver le plus de renseignements et d'artéfacts culturels convoités tout en évitant la noyade dans une mer informationnelle dont la taille double chaque deux ans[1].

Certains d'entre eux ont pour mission de créer des outils permettant de naviguer entre les réseaux ouverts et les « routes parallèles » cryptées ; ils le font par volonté d'explorer d'autres avenues, par idéologie et parfois pour protéger l'anonymat de personnes à risque. C'est le cas de David McKinney, développeur et testeur d'intrusion, avec qui je me suis entretenue en avril dernier. En l'écoutant parler de son travail avec passion et fierté, j'ai constaté qu'il peut être extrêmement gratifiant de jouer le rôle de guide des réseaux parallèles et de « passeur » ouvrant l'accès à des chemins peu empruntés, à être, en somme, l'éclaireur des voies d'évitement et des sorties de secours.

Loin d'être dogmatique, paranoïaque ou catastrophiste, David McKinney œuvre à trouver des solutions de connectivité et de communication qui permettent d'éviter les plateformes à grand trafic dans un souci de confidentialité, mais

aussi de transparence. Et s'il évoque l'importance des communautés virtuelles et du code en accès libre *(open source)*, ce qu'il préconise se situe de l'autre côté du miroir des utopies de la collectivité mondiale ou du citoyen du monde et repose plutôt sur les notions de microcommunautés, de décentralisation des systèmes et d'échanges entre pairs. Par ailleurs, si la luxuriance informationnelle donne la chance à qui le veut de se cacher dans la jungle numérique, elle forme aussi un territoire foisonnant, regorgeant de recoins inexplorés et de lieux de rencontre singuliers.

***Spirale* :** Je t'ai demandé, d'entrée de jeu, en quoi consistait ton travail actuellement, et tu m'as dit plancher sur la conception d'un logiciel qui protège les utilisateurs « à haut risque ». Qui sont-ils ?

David McKinney : Tout le monde court le risque de voir sa vie privée envahie et ses communications interceptées, tout simplement parce que le fonctionnement de la société se fonde sur la collecte de données et l'analyse de celles-ci. Cela a pour conséquence que de nombreux enjeux doivent être pris en compte : nous avons, d'un côté, la surveillance, la lutte au terrorisme et la prévention des crimes et, de l'autre, ceux qui cherchent des marchés cibles pour leurs produits.

Nos clients, les utilisateurs à risque, peuvent être des journalistes, des activistes ou des blogueurs. Dans le cas des journalistes, ils auront recours à nos services pour communiquer avec leurs sources confidentielles, des lanceurs d'alerte, par exemple, ou des personnes dont l'identité doit rester secrète sous peine de nuire à leur carrière ou d'en faire des cibles.

***Spirale* :** Que penses-tu du discours des entreprises qui se défendent en disant que ceux qui n'ont rien à se reprocher n'ont aucune raison de s'opposer à la collecte de données ?

DM : Officiellement, ces données sont collectées pour proposer des produits et services qui correspondent aux intérêts des clients, mais le problème est qu'elles sont « stockées » dans d'immenses bases de données on ne sait trop où, et qu'il n'y a aucun moyen de savoir qui les utilise et à quelles fins. Ces données sont vendues à des tiers, ou des pirates s'en emparent et peuvent les revendre sur le web caché.

***Spirale* :** Ce qui est frappant, c'est que les entreprises revendiquent le droit de se prémunir contre des attaques, mais que les citoyens sont toujours incités à donner le plus de renseignements possible à leur sujet. Ça me semble injuste.

DM : En effet, et je crois que la technologie devrait être au service de la population. Les gens devraient avoir le droit de se protéger contre ces risques, et il devrait être facile pour eux de le faire. Ils ne devraient pas avoir à être des spécialistes de l'informatique pour utiliser des logiciels leur permettant de communiquer avec leurs amis, pour organiser des événements ou pour acheter des choses en ligne.

Combattre la cryptographie d'une main et la financer de l'autre : la bipolarité américaine

***Spirale* :** Tu reviens d'un voyage en Europe, où tu es allé rencontrer plusieurs clients qui pourraient être intéressés par votre technologie. Comment cela s'est-il déroulé ?

DM : Nous avons rencontré des utilisateurs potentiels, des défenseurs des droits de l'homme, un de nos concurrents qui offre un logiciel similaire et certaines personnes qui nous financent.

***Spirale* :** Et quelles sont vos sources de financement ?

DM : C'est principalement le gouvernement des États-Unis. Ils ont un fonds, appelé l'*Open Technology Fund,* destiné aux projets qui tentent de régler les problèmes de censure dans les pays où la population est réduite au silence par des gouvernements oppressifs. Notre technologie aide les gens à communiquer entre eux ou simplement à publier sur Twitter, ou à utiliser Google ou Wikipédia pour chercher de l'information. Nous sommes financés par le même groupe qui commandite le projet Tor.

***Spirale* :** On entend surtout parler de Tor comme d'un moyen d'accéder au web caché…

DM : Oui, c'est une épée à double tranchant, mais ça doit l'être. Cette technologie est bien faite ; ce sont les gens qui décident s'ils l'utilisent pour faire de bonnes ou de mauvaises choses. En gros, Tor décentralise la navigation web. La connexion passe par plusieurs canaux situés dans divers pays qui ne connaissent pas la source des informations qu'ils reçoivent. Ça permet de *surfer* sur l'internet en tout anonymat puisque les communications sont cryptées du début à la fin du processus.

Spirale **:** Donc Tor est financé par le gouvernement américain, alors que c'est aux États-Unis que le scandale de la collecte massive des données téléphoniques a éclaté à la suite des révélations d'Edward Snowden en 2013. N'est-ce pas paradoxal ?

DM : En fait, aux États-Unis, une frange du pouvoir gouvernemental est favorable à une certaine forme de censure et souhaite accroître la surveillance des citoyens. Je pense, par exemple, aux « agences à trois lettres » comme la CIA, le FBI et la NSA. Mais il existe aussi une faction du gouvernement américain qui souhaite aider les résidents des pays non démocratiques à avoir une presse libre et à pouvoir communiquer en toute confidentialité ; ces deux volets sont donc financés parallèlement.

Spirale **:** As-tu déjà fait affaire avec des clients qui souhaitaient avoir recours à vos services et dont les besoins étaient étranges ou suspects ?

DM : Pas vraiment suspects, mais une personne rencontrée en Europe nous a demandé conseil. Elle souhaitait utiliser notre logiciel, mais la police confisquait systématiquement ses ordinateurs portables parce qu'elle employait des logiciels de cryptage. Elle voulait savoir s'il y avait un moyen de faire en sorte que l'ordinateur semble anodin. Nous lui avons suggéré d'avoir un ordinateur d'apparence générique, dont le bureau ne comporterait aucun logiciel ou document compromettant et qui pourrait ne contenir, disons, que quelques applications de base et le jeu de cartes Solitaire. Pour accéder au contenu de son vrai ordinateur, cette personne pourrait se connecter à un portail d'accès à distance protégé par un mot de passe. Cette opération prend tout son sens lorsqu'on sait que la police confisque de l'équipement en le faisant par surprise, pour arriver à mettre la main sur un ordinateur alors qu'une session est ouverte et que l'information n'y est plus cryptée. Il ne faut pas oublier, du reste, que le cryptage est illégal dans de nombreux pays.

Spirale **:** Est-ce que le cryptage des appareils est l'un des services que vous offrez ?

DM : Oui. Notre système d'exploitation est crypté par défaut. Il faut entrer un long mot de passe pour y avoir accès. Nous recommandons à nos clients d'éteindre l'appareil dans lequel il est installé lorsqu'ils se déplacent, de ne pas se contenter de le mettre en veille, afin que le cryptage soit actif.

Spirale **:** Crois-tu qu'il y ait plus de tentatives d'encadrer ou d'interdire le cryptage avec la montée du terrorisme ? As-tu constaté une différence ?

DM : Dans les années 1990, il y a eu les *crypto wars* aux États-Unis, un débat public à propos du chiffrement des données. Le gouvernement a mis certains pays sur une liste noire en raison de leur recours à la cryptographie, et souhaitait aussi avoir accès à des portes dérobées (*backdoors*) en se munissant de passe-partout qui lui auraient permis de tout décrypter. Le projet de loi n'a finalement pas été adopté, ce qui a été une victoire pour la population, mais nous assistons à un retour des pressions contre le cryptage, comme dans l'affaire récente opposant le FBI et Apple. C'est plutôt extraordinaire qu'Apple ait décidé de s'opposer au gouvernement, puisque rien ne l'y obligeait. La société aurait très bien pu s'incliner, mais ses dirigeants ont calculé que cela était préférable pour éviter que ses clients perdent confiance en ses produits. Et, de fait, si le gouvernement pouvait imposer l'ajout de portes dérobées aux technologies vendues sur son territoire, la sécurité serait automatiquement compromise, puisque si le gouvernement a accès à une porte arrière, il est évidemment possible que d'autres gouvernements, des pirates ou des terroristes y aient accès aussi.

Enjeux de la décentralisation et recours au pair-à-pair

Spirale **:** Crois-tu qu'il soit possible de se servir des technologies sans être exposé à la collecte de données ou à la géolocalisation, ou est-ce une idée utopique ?

DM : Je crois fermement à la décentralisation, qui permettrait d'éviter d'utiliser de gros fournisseurs de services comme Facebook et Google. Il existe déjà certains projets en ce sens, notamment un équivalent de Facebook décentralisé nommé Diaspora, où chacun reste propriétaire de ses données. Il y a aussi Twister, un site similaire à Twitter qui utilise BitTorrent par l'entremise de Tor pour partager Twitter entre les ordinateurs de tous les utilisateurs, de sorte que la source ne peut être identifiée. Ces technologies sont viables, mais il faut que des gens les utilisent, et, très souvent, elles en sont à un stade expérimental qui demande d'avoir quelques connaissances techniques pour pouvoir les utiliser de façon réellement sécuritaire. L'avantage de taille des sites comme Facebook, c'est qu'ils sont très faciles à utiliser.

Spirale **:** J'ai l'impression qu'une certaine inquiétude plane au-dessus de tout ce qui concerne la collecte de données ; nous sommes conscients d'être vulnérables, mais ne savons pas vraiment comment éviter de l'être.

DM : Il n'y a pas vraiment d'option grand public en ce moment. Facebook offre des services gratuits en contrepartie du profilage de ses clients et de la revente des renseignements à leur sujet. Et pourtant, de nombreuses personnes sont d'accord avec ce modèle, plusieurs souhaitent recevoir de la publicité ciblée, et non des annonces choisies aléatoirement, sans lien avec leurs préférences.

Spirale **:** Il me semble que, depuis le tout début des réseaux sociaux, la publicité équivaut à un compromis punitif que l'utilisateur doit tolérer pour avoir accès à des systèmes gratuitement. Certains sites offrent d'ailleurs l'option de payer pour avoir *le privilège* de ne plus voir de publicités.

DM : Oui, et c'est d'ailleurs un très bon plan pour ces entreprises qui vont retirer les pubs et accepter votre argent tout en continuant de faire du profilage et d'utiliser vos renseignements personnels. Pourtant, il existe divers modèles d'infrastructures de sites qui permettent aux fournisseurs de services de ne pas savoir ce que leurs utilisateurs font ou pensent. Que ces systèmes soient payants ou non, ils peuvent être mis en place et nous savons comment le faire. Il est parfaitement possible aujourd'hui de fournir un service ou de donner accès à un réseau social sans obtenir de renseignements sur les utilisateurs, mais quelqu'un doit développer une telle technologie à grande échelle, que les gens auront envie d'utiliser. Disons qu'à ce chapitre, la partie n'est pas gagnée.

Spirale **:** Crois-tu que le modèle des échanges pair-à-pair pourrait être efficace en ce sens, et viable à long terme ?

DM : Le pair-à-pair repose sur une répartition du poids entre tous. La partition et le partage des fichiers permettent de mettre sur pied des sites qui peuvent être exploités à faible coût puisque les frais de bande passante sont répartis entre les utilisateurs. Plutôt que de passer par un serveur central, il est possible d'avoir de plus petits réseaux fondés sur des intérêts communs, par exemple, plutôt que de gros sites mondiaux comme Facebook, qui accumulent les données de milliards d'utilisateurs dans une gigantesque base de données centrale. Ce mode de fonctionnement centralisé demande énormément de ressources. Je crois que les gens se tourneront éventuellement vers le pair-à-pair si nous développons des technologies qui seront faciles à utiliser.

Fantasme de vie privée et pouvoir des lois

Spirale **:** Certaines personnes ont le fantasme de vivre complètement « sous le radar » pour échapper à la surveillance et pouvoir vivre sans être suivies ou cataloguées. Crois-tu que cela est possible de nos jours ?

DM : Certaines personnes souhaitent effectivement échapper aux technologies ou rêvent de revenir à une époque prétechnologique par dégoût de l'interconnexion permanente et de la possibilité d'être localisé ou suivi en tout temps par divers moyens, mais ce n'est pas mon cas (rire). Je fais affaire avec des gens qui veulent utiliser la technologie pour avoir plus de pouvoir et qui souhaitent se servir du réseau de communication mondial, mais qui s'opposent à la surveillance de leurs activités et de leurs interactions sociales. Nous devrions tous ultimement avoir le droit de communiquer avec d'autres personnes sans que des gouvernements ou des sociétés prennent forcément part à la communication !

Spirale **:** Effectivement. Dans ce cas, quelle devrait être, à ton avis, la portée des lois qui tentent de régir le droit à la vie privée ?

DM : Je ne crois pas vraiment que les lois puissent régler les problèmes de confidentialité que présentent certaines technologies. Je crois plutôt que ce sont les créateurs de ces technologies qui ont le pouvoir de le faire et qu'il est impératif qu'ils adoptent une approche mondiale. Dans un monde idéal, il devrait être possible d'implanter une nouvelle technologie sans qu'elle soit rattachée à un territoire donné et à la législation de celui-ci. Je crois fermement qu'un outil technologique qui est bien fait et qui est facilement accessible par le grand public peut combler les lacunes et les aberrations de certaines lois qui enfreignent les libertés individuelles ou qui sont simplement vétustes ou inadaptées aux réalités modernes.

Spirale **:** Encore faut-il que les créateurs de ces outils aient une vision plus humaniste de la technologie, comme celle que tu défends, et non une approche simplement commerciale…

Je te remercie de nous avoir accordé cet entretien et de nous avoir présenté l'autre pendant du discours qui se plaît à ne montrer que le

côté sombre du web caché. Il est essentiel de rappeler que votre travail, s'il est méconnu, demeure vital pour bon nombre de personnes vulnérables.

Profilage commercial et surveillance étatique : deux enjeux foncièrement distincts

Au début de la présente année, le directeur de la *National Security Agency* (NSA), Michael Rogers, a déclaré que les attentats de Paris de novembre 2015 ne seraient pas survenus sans le recours à des techniques de cryptage. Cette affirmation visait à revendiquer une fois de plus le droit à des accès privilégiés afin que l'agence soit en mesure de protéger la population.

« JE CROIS FERMEMENT QU'UN OUTIL TECHNOLOGIQUE QUI EST BIEN FAIT ET QUI EST FACILEMENT ACCESSIBLE PAR LE GRAND PUBLIC PEUT COMBLER LES LACUNES ET LES ABERRATIONS DE CERTAINES LOIS QUI ENFREIGNENT LES LIBERTÉS INDIVIDUELLES [...] »

Dans un article du rédacteur en chef de la revue *The Walrus,* Jonathan Kay, paru en juin 2016 et intitulé, avec un brin de provocation, *No One Is Watching You,* l'auteur souligne les efforts colossaux que les entreprises privées ont déployés pour donner aux utilisateurs des moteurs de recherche et des réseaux sociaux principaux un plus important contrôle des paramètres de confidentialité de ceux-ci. Selon lui, les entreprises ne se sont jamais autant soucié des questions de confidentialité et seraient désormais enclines à proposer des technologies moins intrusives. La conclusion de cet article semble d'ailleurs rejoindre la position de David McKinney, qui a souligné à plusieurs reprises lors de notre entretien que, si les entreprises souhaitent avant tout recueillir des données sur les utilisateurs à des fins de commercialisation, plusieurs gouvernements de pays démocratiques réclament le droit de surveiller davantage les citoyens à des fins de sécurité nationale, ce qui est beaucoup plus préoccupant.

On peut se réjouir de l'expiration du *Patriot Act* aux États-Unis, qui a été remplacé par le *Freedom Act,* lequel interdit la collecte de données en vrac par la NSA, mais ce sont ultimement les entreprises qui proposent des technologies et les utilisateurs de celles-ci qui doivent travailler de concert pour que la convivialité et la confidentialité aillent nécessairement de pair.

Puisque les technologies et le partage d'informations ne sont plus évitables, il est impératif que les gouvernements en suivent l'évolution de très près pour se doter d'un cadre législatif à la fois réaliste et respectueux des droits fondamentaux de la personne, dont celui du respect de la vie privée. S'il est difficile de le faire en Amérique du Nord et que les législateurs peinent à suivre la cadence effrénée des progrès, on imagine facilement comment les régimes dictatoriaux ou oppressifs peuvent retourner les avancées technologiques contre leurs propres populations. Le travail de David McKinney et de ses collègues reste, à cet égard, essentiel. ■

Liens :
https://www.torproject.org/press/press.html.en
https://diasporafoundation.org/
http://twister.net.co/
https://subgraph.com/about-us/index.en.html

1 Voir la section « Infographic » de *The Hague Declaration* au http://thehaguedeclaration.com/big-data-can-reshape-the-world-and-save-lives-infographic/.