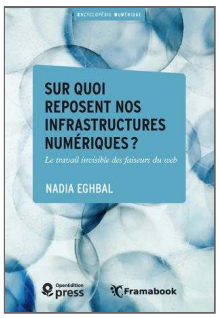

Nadia Eghbal

Sur quoi reposent nos infrastructures numériques ?
Le travail invisible des faiseurs du web

OpenEdition Press

Introduction

DOI : 10.4000/books.oep.1809
Éditeur : OpenEdition Press, Framabook
Lieu d'édition : OpenEdition Press, Framabook
Année d'édition : 2017
Collection : Encyclopédie numérique
ISBN électronique : 9782821894938

INTRODUCTION

En 1998, une équipe d'experts en sécurité se constitua au Royaume-Uni pour élaborer une panoplie d'outils de chiffrement libres destinés à Internet.

Très vite, tout le monde se mit à parler de leur projet, intitulé OpenSSL (les développeurs avaient pris comme base de départ un projet australien existant, SSLeay). Non seulement il était complet et relativement fiable, mais il était libre. Il n'est pas facile d'écrire de la cryptographie et OpenSSL avait résolu un problème épineux pour les développeurs du monde entier : en 2014, deux tiers des serveurs web utilisaient OpenSSL, et les sites pouvaient donc transmettre de façon sécurisée les codes de cartes de crédit et autres informations sensibles *via* Internet.

Pendant ce temps, le projet était toujours géré de façon informelle par un petit groupe de volontaires. Un conseiller du département de la Défense des États-Unis, Steve Marquess, avait remarqué qu'un contributeur, Stephen Henson, travaillait à temps plein sur OpenSSL. Par curiosité, Marquess lui demanda ce qu'il gagnait et il fut surpris d'apprendre que le salaire de Henson était cinq fois inférieur au sien.

Marquess s'était toujours considéré comme un bon programmeur, mais ses talents faisaient pâle figure à côté de ceux de Henson. Comme bien d'autres, Marquess imaginait à tort que quelqu'un d'aussi talentueux que Henson aurait un salaire à sa mesure.

Henson travaillait sur OpenSSL depuis 1998. Marquess avait rejoint le projet plus récemment, au début des années 2000, et avait travaillé avec Henson pendant plusieurs années avant d'apprendre sa situation financière.

Par son travail au département de la Défense, Marquess savait à quel point OpenSSL était crucial non seulement pour leur propre système, mais aussi pour d'autres industries dans le monde, de l'investissement à l'aéronautique en passant par la santé. Jusqu'alors, il avait « toujours supposé (comme le reste du

monde) que l'équipe d'OpenSSL était grande, active et bien financée »[1]. En réalité, OpenSSL ne rapportait même pas assez pour payer un seul salarié.

Marquess décida de s'impliquer dans le projet : il avait contribué au code de temps à autre, mais il se rendit compte qu'il serait plus utile en tant qu'homme d'affaires. Il commença par négocier des petits contrats de conseil par le biais d'une entreprise à but non lucratif pour maintenir à flot OpenSSL dans ses années les plus dures. Comme le volume des contrats croissait, il créa une entité légale pour collecter ces revenus, l'OpenSSL Software Foundation (OSF). Malgré le nombre de personnes et d'entreprises qui utilisaient leur logiciel, l'OSF ne reçut jamais plus de 2 000 dollars de dons par an. Les revenus bruts de l'activité de conseil et des contrats ne dépassèrent jamais un million de dollars, qui furent presque entièrement dépensés en frais d'hébergement et en tests de sécurité (qui peuvent coûter plusieurs centaines de milliers de dollars).

Il y avait juste de quoi payer le salaire d'un développeur, Stephen Henson. Cela signifie que les deux tiers du Web reposaient sur un logiciel de chiffrement maintenu par un seul employé à temps plein.

L'équipe d'OpenSSL continua de travailler de façon relativement anonyme jusqu'en avril 2014, quand un ingénieur de chez Google, Neel Mehta, découvrit une faille de sécurité majeure dans OpenSSL. Deux jours plus tard, un autre ingénieur, de l'entreprise finlandaise Codenomicon, découvrit le même problème.

Tous deux contactèrent immédiatement l'équipe d'OpenSSL.

Ce bug, surnommé Heartbleed[2], s'était glissé dans une mise à jour de 2011. Il était passé inaperçu pendant des années. Heartbleed pouvait permettre à n'importe quel pirate suffisamment doué de détourner des informations sécurisées en transit vers des serveurs vulnérables, y compris des mots de passe, des identifiants de cartes de crédit et autres données sensibles.

1. Les propos de Steve Marquess ont été recueillis par l'auteure lors d'interviews par téléphone et par courriel.
2. Pour en savoir plus sur Heartbleed, voir l'article « Heartbleed », sur Wikipédia.

Joseph Steinberg, un éditorialiste spécialisé en cybersécurité, écrivit : « On pourrait dire que Heartbleed est la pire vulnérabilité découverte… depuis qu'Internet a commencé à être utilisé pour des opérations commerciales. »

Grâce à un large écho médiatique, le grand public entendit parler de ce bug informatique, au moins de nom. Des plateformes majeures, comme Instagram, Gmail ou Netflix, furent affectées par Heartbleed.

Certains journalistes attirèrent l'attention sur l'OpenSSL lui-même, et la manière dont l'équipe de développement avait lutté pendant des années pour pouvoir continuer ses travaux. Les experts en sécurité connaissaient les limites d'OpenSSL, mais l'équipe ne parvenait pas à capter les ressources ou l'attention adéquates pour résoudre les problèmes.

Marquess écrivit à propos de Heartbleed : « Ce qui est mystérieux, ce n'est pas qu'une poignée de bénévoles surchargés de travail ait raté ce bug, mais plutôt qu'il n'y ait pas eu davantage de bugs de ce genre. »

Des personnes envoyèrent des dons pour soutenir la fondation, et Marquess les remercia pour leur enthousiasme, mais le premier cycle de dons ne totalisa qu'environ 9 000 dollars : largement en-deçà du nécessaire pour soutenir une équipe dédiée.

Marquess adressa alors à Internet un vibrant plaidoyer pour une levée de fonds :

> Les gars qui travaillent sur OpenSSL ne sont là ni pour l'argent ni pour la gloire (qui, en dehors des cercles geeks, a entendu parler d'eux ou d'OpenSSL avant que les médias ne s'emparent d'Heartbleed ?). Ils travaillent pour la fierté de créer et parce qu'ils se sentent responsables de ce en quoi ils croient.
>
> Il faut des nerfs d'acier pour travailler pendant des années sur des centaines de milliers de lignes d'un code très complexe, où tout le monde peut voir chacune des lignes que vous manipulez, en sachant que ce code est utilisé par des banques, des pare-feux, des systèmes d'armement, des sites web, des smartphones, l'industrie, le Gouvernement, partout. Et tout cela en

> acceptant de ne pas être apprécié à votre juste valeur et d'être ignoré jusqu'à ce que quelque chose tourne mal.
>
> Il devrait y avoir au moins une demi-douzaine de membres à temps plein dans l'équipe au lieu d'un seul pour se consacrer au soin et à la maintenance que demande OpenSSL, sans devoir gérer en même temps l'aspect commercial.
>
> Si vous êtes un décideur dans une multinationale ou un Gouvernement, pensez-y. Je vous en prie. Je me fais vieux, je fatigue et j'aimerais un jour prendre ma retraite.

Après Heartbleed, OpenSSL a obtenu enfin le financement nécessaire – en tout cas jusqu'à présent. L'équipe dispose à l'heure actuelle d'assez d'argent pour payer quatre employés à temps plein pendant trois ans. Mais au bout d'un an et demi de ce financement, Marquess n'est malgré tout pas certain de l'avenir.

Il a admis que Heartbleed a été une bénédiction pour eux, mais trouve « légèrement ironique » que ce soit une faille de cette ampleur qui ait donné plus de visibilité à leur cause. Et quand les fonds seront épuisés et que le monde sera passé à autre chose, Marquess craint qu'ils ne se retrouvent dans la même situation qu'avant Heartbleed, voire pire : la clientèle que Marquess a mis des années à se constituer a disparu, puisque l'équipe se consacre désormais exclusivement à OpenSSL et n'a plus le temps d'honorer d'autres contrats.

Marquess lui-même a bientôt l'âge de la retraite. Il est le seul qui accepte de s'occuper des affaires commerciales et du rôle exécutif associés à OpenSSL comme les impôts, la recherche de clients, et la gestion des donateurs. Le reste de son équipe préfère se concentrer sur l'écriture et la maintenance du code. Il ne peut embaucher personne pour le remplacer quand il prendra sa retraite, parce qu'il ne perçoit actuellement aucun salaire. « Je ne crois pas qu'on puisse tenir comme ça plus d'un an ou deux », a-t-il fait remarquer.

L'histoire d'OpenSSL n'est pas unique, et par bien des aspects, Marquess trouve que lui et son équipe font partie des mieux lotis. Bien d'autres projets sont toujours en manque de reconnaissance et de financement, alors qu'ils constituent l'infrastructure numérique, infrastructure absolument cruciale puisque tous les logiciels d'aujourd'hui, et par conséquent tous les aspects de notre vie quotidienne, en dépendent.

Relever ses courriels, lire les actualités, vérifier le prix des actions, faire des achats en ligne, aller chez le médecin, appeler le service client – qu'on le réalise ou non, tout ce que nous faisons est rendu possible par des projets comme OpenSSL. Sans eux, la technologie sur laquelle repose la société moderne ne pourrait tout simplement pas fonctionner.

Beaucoup de ces projets sont créés et maintenus par des volontaires et offerts au public gratuitement. Tous ceux qui le veulent, de Facebook au programmeur amateur, peuvent utiliser ce code pour créer leurs propres applications. Et ils le font.

S'il est difficile de croire, comme le dit Marquess, « qu'un groupe hétéroclite d'amateurs puisse faire mieux que de gigantesques sociétés avec leur argent et leurs ressources », considérez plutôt que c'est lié à la montée en puissance du travail collaboratif pair à pair dans le monde.

Des *startups* jusqu'ici impensables comme Uber ou Airbnb se sont transformées en l'espace de quelques années en poids lourds du monde des affaires et remettent en question des industries phares comme le transport ou l'hôtellerie. Des musiciens se font un nom sur YouTube ou SoundCloud plutôt qu'en passant par les majors. Créateurs et artistes concrétisent leurs idées *via* des plateformes de financement participatif telles que Kickstarter ou Patreon.

Les autres projets de l'infrastructure sont également issus de la passion et de la créativité de développeurs qui se sont dit : « je pourrais faire ça mieux », et qui collaborent pour développer et livrer du code au monde entier. La différence, c'est que des millions de personnes ont besoin de ce code dans leur vie quotidienne.

Comme le code n'est pas aussi sexy qu'une vidéo virale sur YouTube ou une campagne Kickstarter, le grand public

est très loin de pouvoir l'apprécier à sa juste valeur, si bien que le code qui a révolutionné les technologies de l'information manque très largement du soutien des institutions.

Mais nous ne pourrons ignorer cela plus longtemps.

Ces cinq dernières années, notre dépendance aux logiciels ainsi qu'au code libre et public qui les fait fonctionner s'est accélérée. Les technologies se sont fait une place dans tous les aspects de notre quotidien, et plus nous utilisons de logiciels, plus nous en créons, et plus cela demande de travail de maintenance.

Toutes les *startups* qui réussissent ont besoin d'une infrastructure publique pour assurer leur succès. Pourtant, aucune entreprise n'est assez motivée pour agir seule. Pendant que le monde progresse à toute vitesse vers l'ère moderne des *startups*, du code et des technologies, l'infrastructure reste à la traîne. Les fissures des fondations ne sont pas encore très visibles, mais elles s'élargissent. Après des années de croissance sans précédent qui nous ont propulsés dans une époque de prospérité, nous devons maintenant agir pour nous assurer que le monde que nous avons bâti en si peu de temps ne va pas s'effondrer brutalement sans crier gare.

Pour comprendre comment nous pouvons préserver l'avenir, nous devons d'abord comprendre ce qu'est le logiciel lui-même.