Des Routes et des Ponts (2), une introduction

Voici l'introduction du livre Des routes et des ponts *de* ***Nadia Eghbal*** *(si vous avez raté le début…) que le groupe Framalang vous traduit au fil des semaines.*

Dans cette partie, après avoir exposé la pression croissante de la demande de maintenance, elle retrace un épisode tout à fait emblématique, celui d'Heartbleed, quand il y a quelques années le monde de l'informatique prenait conscience qu'un protocole sensible et universel de sécurité n'était maintenu que par une poignée de développeurs sous-payés.

Vous souhaitez participer à la traduction hebdomadaire ? Rejoignez Framalang ou rendez-vous sur un pad dont l'adresse sera donnée sur Framasphère chaque mardi à 19h… mais si vous passez après vous êtes les bienvenu.e.s aussi !

Introduction

Traduction Framalang : Piup, xi, jums, goofy, Ced, mika, Luc, Laure, Lumibd, goofy, alienspoon, Julien / Sphinx

Tout, dans notre société moderne, des hôpitaux à la bourse en passant par les journaux et les réseaux sociaux, fonctionne grâce à des logiciels. Mais à y regarder de plus près, vous verrez que les fondations de cette infrastructure logicielle menacent de céder sous la demande. Aujourd'hui, presque tous les logiciels sont tributaires de code dit *open source* : public et gratuit, ce code est créé et maintenu par des communautés de développeurs ou disposant d'autres compétences. Comme les routes ou les ponts que tout le monde peut emprunter à pied ou dans un véhicule, le code *open source* peut être repris et utilisé par n'importe qui, entreprise ou

particulier, pour créer des logiciels. Ce code constitue l'infrastructure numérique de la société d'aujourd'hui, et tout comme l'infrastructure matérielle, elle nécessite une maintenance et un entretien réguliers. Aux États-Unis par exemple, plus de la moitié des dépenses de l'état pour les réseaux routiers et ceux de distribution d'eau est consacrée à leur seule maintenance.

Mais les ressources financières nécessaires pour soutenir cette infrastructure numérique sont bien plus difficiles à obtenir. La maintenance de code *open source* était relativement abordable à ses débuts, mais de nos jours les financements ne viennent en général que d'entreprises de logiciels, sous forme de mécénat direct ou indirect. Dans la foulée de la révolution de l'ordinateur personnel, au début des années 1980, la plupart des logiciels du commerce étaient propriétaires, et non partagés. Les outils logiciels étaient conçus et utilisés en interne dans chaque entreprise, qui vendait aux clients une licence d'utilisation de ses produits. Beaucoup d'entreprises trouvaient que l'*open source* était un domaine émergent trop peu fiable pour un usage commercial. Selon elles, les logiciels devaient être vendus, pas donnés gratuitement.

En fait, partager du code s'est révélé plus facile, plus économique et plus efficace que d'écrire du code propriétaire, et de nos jours tout le monde utilise du code *open source* : les entreprises du Fortune 500, le gouvernement, les grandes entreprises du logiciel, les startups… Cependant, cette demande supplémentaire a augmenté la charge de travail de ceux qui produisent et entretiennent cette infrastructure partagée, mais comme ces communautés sont assez discrètes, le reste du monde a mis longtemps à s'en rendre compte. Parmi nous, beaucoup considèrent qu'ouvrir un logiciel est aussi normal que pousser un bouton pour allumer la lumière, mais nous ne pensons pas au capital humain qui a rendu cela possible.

Face à cette demande sans précédent, si nous ne soutenons pas notre infrastructure numérique les conséquences seront

nombreuses. Du côté des risques, il y a les failles de sécurité et les interruptions de service causées par l'impossibilité pour les mainteneurs de fournir une assistance suffisante. Du côté des possibilités, les améliorations de ces outils logiciels sont nécessaires pour accompagner la renaissance actuelle des *startups*, qui dépendent étroitement de l'infrastructure numérique. De plus, le travail effectué dans l'*open source* est un atout dans le portfolio des développeurs et facilite leur recrutement, mais ce réservoir de talents est beaucoup moins diversifié que celui de l'industrie informatique dans son ensemble. Une augmentation du nombre de contributeurs serait donc profitable au domaine des technologies de l'information au sens large.

Aucune entreprise ou organisation n'a de raison de s'attaquer seule à ce problème, car le code *open source* est un bien public. C'est pourquoi nous devons réussir à travailler ensemble pour entretenir notre infrastructure numérique. Il existe par exemple la *Core Infrastructure Initiative* (CII) de la fondation Linux et le programme *Open Source Support* de Mozilla, ainsi que des initiatives de nombre d'entreprises de logiciel à différents niveaux.
L'entretien de notre infrastructure numérique est une idée nouvelle pour beaucoup, et les défis que cela pose ne sont pas bien cernés. De plus, l'initiative de cette infrastructure est distribuée entre beaucoup de personnes et d'organisations, ce qui met à mal les modèles classiques de gouvernance. Beaucoup de ces projets qui contribuent à l'infrastructure n'ont même pas de statut juridique. Toute stratégie de maintenance devra donc accepter et exploiter ces aspects décentralisés et communautaires du code *open source*.

Enfin, pour construire un écosystème sain et durable, il sera crucial d'éduquer les gens à ce problème, de faciliter les contributions financières et humaines des institutions, de multiplier le nombre de contributeurs *open source* et de définir les bonnes pratiques et stratégies au sein des projets

qui participent de cette infrastructure.

Le logo d’Heartbleed (licence CC 0)

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 apprit avec surprise que le salaire de Henson était cinq fois plus faible que le 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.

Comme il avait travaillé avec le Département de la Défense, Marquess savait à quel point OpenSSL était crucial, non seulement pour leur propre système, mais 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. »
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 existante pour maintenir OpenSSL à flot 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 assez pour 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 à 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, 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.

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 a pas eu davantage de bugs de ce genre. »

Les gens 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 la sortie de heartbleed[sic] dans les médias ?). Ils travaillent pour la fierté de créer et parce qu'ils se sentent responsables de à 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 prendre ma retraite un jour.*

Après Heartbleed, OpenSSL obtint enfin le financement nécessaire – en tous 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 pas certain de l'avenir.

Il a admis que Heartbleed a été une bénédiction pour eux, mais qu'il est « légèrement ironique » que ce soit une faille de cette ampleur qui ait donné plus de visibilité à leur cause. Et quand l'argent sera épuisé 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 travaille maintenant à plein temps sur OpenSSL et n'a plus le temps d'exécuter des 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 en ce moment aucun salaire. « Je ne crois pas qu'on puisse tenir comme ça plus d'un an ou deux » a-t-il remarqué.

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 », voyez plutôt comme 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 nos vies, et plus les gens utilisent de logiciels, plus on en crée, et plus cela demande de travail de maintenance.

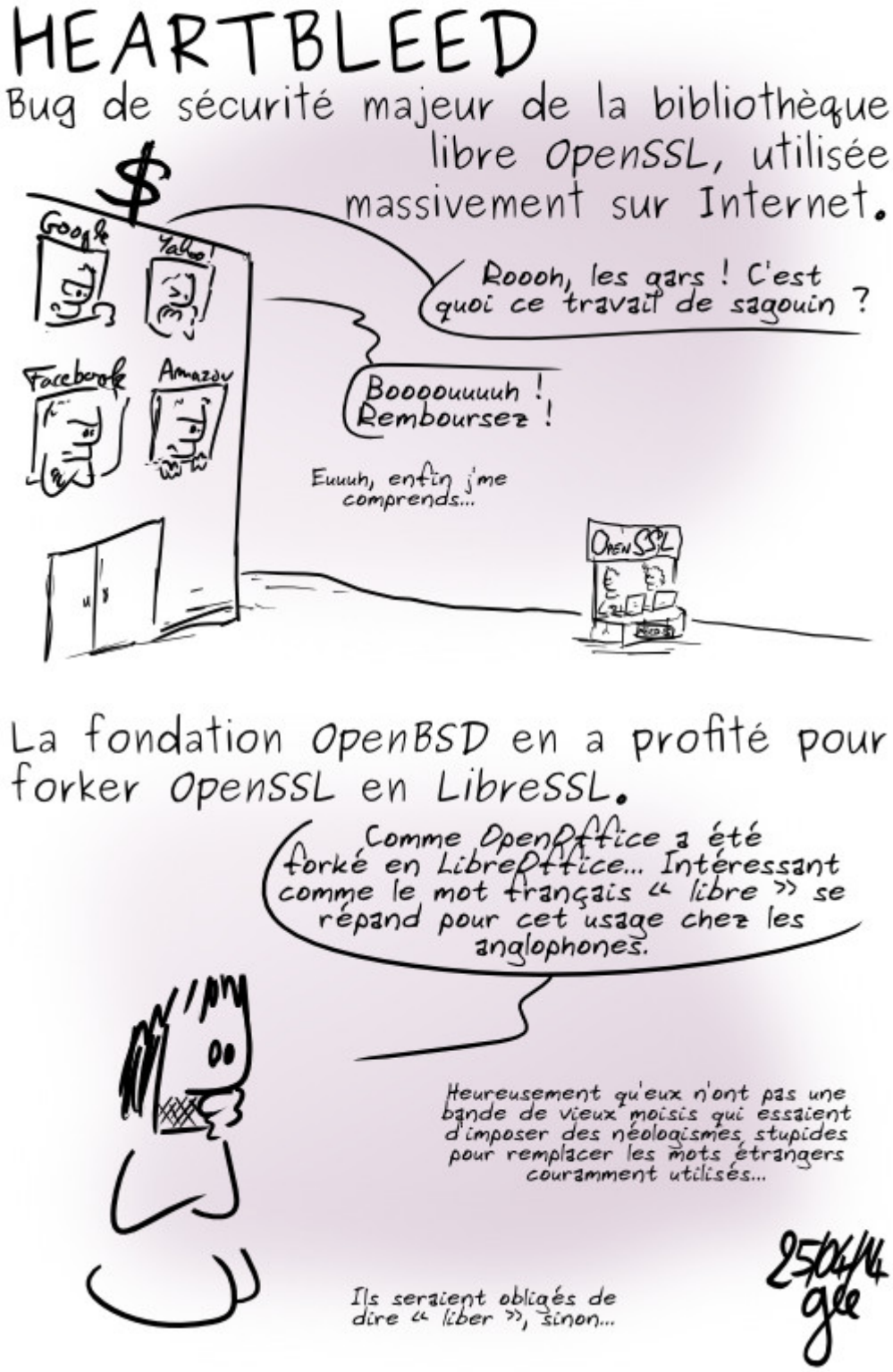
Toutes les *startups* qui réussissent ont besoin d'une infrastructure publique pour assurer leur succès, pourtant aucune entreprise n'est assez motivée pour agir seule. Pendant que le monde progresse à toute vitesse vers l'ère moderne des *startups*, du code et des technologies, l'infrastructure reste 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 croissance et 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.

(À suivre…)

La semaine prochaine : comment on fabrique des logiciels…

Geektionnerd : Heartbleed



Sources :

- [Toute l'actualité sur Heartbleed](#) sur Numerama
- [OpenSSL est mort, vive (le futur) LibreSSL](#) sur LinuxFr
- [Explication du bug](#) sur XKCD *(en)*

Crédit : [Simon Gee Giraudot](#) (Creative Commons By-Sa)