Le contrôle des redirections

Si les redirections [1] sont à peu prêt aussi vieilles que le web, elles n'étaient, jusqu'à l'apparition des micro-blogs, que rarement utilisées, mises en place par les connaisseurs, lors du déménagement d'un document important.

Dans ce contexte, quand Kevin Gilbertson proposa en 2002 le premier service en-ligne de rétrécissement d'URL (TinyURL.com), permettant de créer à la demande, une redirection depuis une une adresse courte vers l'adresse de son choix, il n'eut qu'un succès modéré. L'initiative tomba presque dans l'oubli, et ce n'est qu'une demi-décennie plus tard, avec l'essor de Twitter que ce service rencontra d'un coup un large public. En effet, le principe de Twitter étant de proposer un blog dont les billets sont plus courts que des SMS, pouvoir réduire une URL devint un enjeu de taille, si j'ose dire. En effet, d'une part certaines URL sont simplement trop longues pour être gazouillées, et d'autre part, une fois l'adresse collée dans un micro-billet il ne reste plus beaucoup de place pour en expliquer l'intérêt.

TinyURL.com fut donc dans un premier temps directement proposé depuis l'interface du site de microblogage pour aider à la rédaction des messages. Puis devant le succès rencontré par cet intermédiaire, de nombreux concurrents vinrent occuper leurs parts de marché, tel que Bit.ly, qui se démarqua par les statistiques offertes sur l'utilisation des liens courts qu'il produit.

Et progressivement, chaque gros acteur du web se mit à

proposer son propre service de rétrécissement, pour faire plaisir à ses utilisateurs avec un service techniquement trivial, ne pas dépendre d'un tiers et enfin pour mettre la main, chacun, sur sa parcelle de statistiques d'usage !

Car utiliser un raccourcisseur d'URL revient en fait à ajouter une barrière de péage d'autoroute entre les personnes auxquelles vous communiquez le lien court, et le document que vous souhaitiez porter à leur attention. Bien sûr, c'est une barrière pour laquelle tout le monde est abonné (pour l'instant), et elle ne fait que ralentir un peu le trafic, mais surtout, elle identifie au passage qui l'a franchi, quand et combien de fois.

Or, si cette information était jusque là collectée par l'émetteur du document de destination seulement, elle n'était pas aussi facilement recoupable et monnayable que si c'est un acteur central qui collecte toutes les visites effectuées suivant les recommandations des millions d'utilisateurs de Twitter, de Facebook ou de Google…

Et puis, d'un point de vue pragmatique, au-delà de la seconde d'attente ajoutée après le clic, ou du respect de la vie privée, un autre problème se pose, celui de la pérennité de ces étapes intermédiaires. Aujourd'hui, TinyURL.com se vante de servir des milliards de redirections par mois, mais ce service, qui n'est pas géré par une entreprise, est voué à disparaître, car son nom (qui avait besoin d'être explicite au début) est trop long pour être efficace aujourd'hui. Or, quand les serveurs de TinyURL seront éteints, c'est plus d'un milliard d'adresses qui, d'un coup, ne mèneront plus à rien.

Alors, quand on voit avec quel empressement les entreprises se sont mises à proposer ce gadget en apparence anodin, on peut avoir envie de ne pas se laisser enfermer nous non plus par une compagnie particulière, de suivre cet exemple en s'installant chacun son raccourcisseur d'URL à soi. Après tout, ça ne sera qu'une corde de plus à mettre à l'arc de la

NoBox.

Toutefois, la question de la pérennité des redirections mises en place reste posée… En ce premier novembre, il est presque de bon ton de se demander ce qu'on fera du serveur personnel d'un défunt.

Mais pour l'heure, place au détail de l'enfer des redirections vers lequel on nous mène, et qui transforme progressivement le web en maison qui rend fou des 12 travaux d'Astérix… [2]

Le web se dirige-t-il vers un cauchemar de redirections ?

Is the Web heading toward redirect Hell?

22 septembre 2010 – Royal.Pingdom.com
(Traduction Framalang : Zitor, Barbidule, Daria, Goofy, Siltaar)

Google le fait. Facebook le fait. Yahoo le fait. Microsoft le fait. Et bientôt, Twitter le fera.

Nous parlons de la manie qu'ont tous les services web d'ajouter une étape intermédiaire pour échantillonner ce sur quoi nous cliquons avant de nous envoyer vers notre vraie destination. Ça dure déjà depuis un certain temps, et c'est progressivement en train de devenir un enfer de redirections. Cela a un coût.

Du trafic déjà en trop

Il y a déjà beaucoup de redirections en place, auxquelles vous ne songez pas forcément. Par exemple :

- Chaque fois que vous cliquez sur un résultat de recherche dans Google ou Bing, il y a un passage obligé par les serveurs du moteur de recherche pour analyse

avant d’être redirigé vers le site réellement ciblé;
- Chaque fois que vous cliquez sur un titre dans un flux RSS Feedburner, vous êtes aussi redirigé avant d’arriver à la véritable cible;
- Chaque fois que vous cliquez sur un lien sortant de Facebook, il y a une étape intermédiaire passant par un serveur de Facebook avant de vous rediriger vers où vous voulez aller.

Et ainsi de suite, et ainsi de suite, et ainsi de suite. C’est, bien sûr, parce que Google, Facebook et les autres sociétés en ligne aiment suivre les clics et le comportement de leurs utilisateurs. Vous connaître est une vraie ressource pour ces sociétés. Cela peut les aider à améliorer leur service, à le monétiser plus efficacement et dans de nombreux cas, ces données elles-mêmes valent de l’argent. Au final ce suivi de clic peut aussi être bon pour les utilisateurs finaux, en particulier s’il permet à un service d’améliorer sa qualité.

Mais…

Les choses sont en train de déraper

S’il ne s’agissait que d’une seule étape supplémentaire, cela pourrait aller. Mais si vous regardez autour, vous vous rendrez compte que ces redirections sont en train de s’empiler, chaque service interceptant des informations sur le clic lors du cheminement vers la destination finale. Vous savez, celle que l’utilisateur a vraiment demandée.

Cela peut vite devenir incontrôlable. Nous avons vu des scénarios où les liens sortants de Facebook, par exemple, vous redirigent d’abord vers un serveur Facebook, puis vers un racourcisseur d’URL (par exemple bit.ly), qui à son tour vous redirige vers une URL plus longue qui elle-même génère plusieurs redirections avant que FINALEMENT vous parveniez à la cible. Il n’est pas rare qu’il y ait plus de trois

redirections vers différents sites qui, du point de vue de l'utilisateur, sont du trafic superflu.

Le problème, c'est que ce trafic supplémentaire n'est pas gratuit. Cela rallonge le temps nécessaire pour atteindre l'objectif, et cela rajoute d'autres liens (au sens propre !) dans la chaîne, ce qui peut la briser ou la ralentir. Cela peut même faire apparaitre des sites comme indisponibles alors qu'ils ne le sont pas, simplement parce que quelque chose sur le chemin est tombé en panne.

Et il semble que cette pratique soit de plus en plus répandue sur le Web.

Un exemple récent de cette « mode de la redirection » : Twitter

Vous souvenez-vous de cette vague de raccourcisseurs d'URL qui est venue quand Twitter a commencé à devenir populaire? C'est là que commence notre histoire.

Twitter a d'abord utilisé le déjà établi TinyURL.com comme raccourcisseur d'URL par défaut. C'était un partenaire idéal pour Twitter et sa limite de 140 caractères par message.

Puis vinrent Bit.ly et une pléthore d'autres raccourcisseurs d'URL, qui voulaient eux aussi surfer sur le succès grandissant de Twitter. Bit.ly a rapidement réussi à remplacer TinyURL comme réducteur d'URL par défaut pour Twitter. Grâce à cela, Bit.ly a mis la main sur une foule de données : la liste d'une bonne partie des liens postés sur Twitter, et de leur popularité, chaque clic pouvant être tracé.

Ce n'était qu'une question de temps avant que Twitter ne veuille garder ces données pour lui seul. Pourquoi s'en priverait-il ? Cela lui permet d'avoir le contrôle total de l'infrastructure nécessaire à son fonctionnement, tout en récupérant des informations sur ce que les utilisateurs aiment

s’échanger, et ainsi de suite. Twitter a donc créé récemment son propre raccourcisseur d’URL, t.co. Dans le cas de Twitter, cela peut parfaitement se comprendre.

Cela est bel et bon, mais voici maintenant la partie la plus intéressante qui est la plus pertinente pour cet article : d’ici la fin de l’année, Twitter va rediriger TOUS les liens vers son raccourcisseur d’URL, y compris les liens déjà raccourcis par d’autres services comme Bit.ly ou Goo.gl, le raccourcisseur de Google. En canalisant tous les clics vers ses propres serveurs, Twitter va acquérir une connaissance précise de la façon dont son service est utilisé, et de ses utilisateurs. Cela lui donne le contrôle total sur la qualité de son service. C’est une bonne chose pour Twitter.

Mais qu’arrive-t-il quand tout le monde veut un morceau du gâteau ? Redirection après redirection après redirection avant d’arriver à notre destination ? Oui, c’est exactement ce qui se passe, et vous aurez à vivre avec ce trafic supplémentaire.

Voici ce à quoi le partage de liens pourrait ressembler une fois que Twitter aura commencé à soumettre tous les clics à son propre service :

1. Quelqu’un partage un lien goo.gl sur Twitter, il est alors transformé en un lien t.co.
2. En cliquant sur le lien t.co, l’utilisateur est alors redirigé vers les serveurs de Twitter pour convertir le lien t.co en lien goo.gl et se voit réorienté dessus.
3. Le lien goo.gl dirige l’utilisateur vers les serveurs de Google pour y être résolu et ré-orienter enfin l’utilisateur vers la cible qu’il souhaitais atteindre.
4. Rien n’empêche cette cible de n’être à son tour qu’une nouvelle redirection…

Vous en avez la tête qui tourne, hein ?

Encore plus de niveaux de redirection ?

Il y a un an, nous avons écrit un article sur les inconvénients potentiels des raccourcisseurs d'URL, et il s'applique parfaitement à ce scénario plus général avec de multiples redirections entre les sites. Les conséquences de ces redirections sur les performances, la sécurité et la confidentialité sont les mêmes.

Nous soupçonnons fortement que le chemin pris par Twitter (échantillonner et enregistrer les clics avant expédition vers la cible, avec ou sans raccourcisseurs d'URL) laisse présager des pratiques à venir chez les autres services Web qui ne le font pas déjà.

Et même quand les services principaux ne le font pas, de plus en plus d'intermédiaires et d'applications tierces, comme les raccourcisseurs d'URL, apparaissent tous les jours. L'autre jour, le fabricant d'antivirus McAfee a annoncé la version-bêta de McAf.ee, un raccourcisseur d'URL « sécurisé ». C'est peut-être super, qui sait, mais à la lumière de ce que nous vous avons dit dans cet article, il est difficile de ne pas penser : quoi, encore une autre niveau de redirection ? Est-ce vraiment vers cela que le Web évolue ? Est-ce vraiment ce que nous voulons ?

Notes

[1] Ce mécanisme du protocole HTTP permettant de faire rebondir la navigation vers une autre page au chargement d'une URL.

[2] Crédit photo : Kudumomo (Creative Commons Parternité)

Entretien avec Hackable:Devices, site de diffusion massive de matériel libre

Les dimanches pluvieux, quand le bobo va chez Ikea, le hacker surfe sur Hackable:Devices…

Si vous étiez des dernières Ubuntu Party ou RMLL, vous n'avez pu passer à côté du stand, toujours très fréquenté, de Hackable:Devices sans remarquer les étranges appareils et instruments insolites, gadgets et machines que cette dynamique équipe présente fièrement aux passants. Et je ne puis cacher mon émotion d'avoir vu pour de vrai une carte Arduino ou une imprimante 3D à l'œuvre, après en avoir d'abord entendu parler en théorie sur ce blog.

Qu'est-ce donc que **Hackable:Devices** ? Dire qu'il s'agit d'une boutique en ligne proposant du « hardware open source », ou « matériel libre » en bon français, est vrai mais c'est un peu réducteur car ce serait taire la dimension communautaire (et militante) du projet.

D'ailleurs vous êtes ainsi accueilli en première page du site : « Les logiciels libres n'ont pas amené la liberté qu'au logiciel. Chez hackable-devices nous croyons sincèrement que le matériel et l'électronique peuvent être utilisés et développés selon les mêmes processus communautaires. Nous

pensons que la culture du DIY *(ou Do It Yourself pour Faites-le vous-même)* et l'apprentissage par la pratique doivent être encouragés. Nous savons que les gens se rencontrent pour créer, améliorer et s'amuser tout à la fois. Nous sommes persuadés que les objets doivent réellement vous appartenir. »

Tout d'un coup nous voici à des années-lumière du modèle Apple. Et je me prends à rêver que les professeurs de technologies fassent de plus en plus souvent leurs courses sur ce site.

Impossible d'attendre plus longtemps avant de les rencontrer et mettre nous aussi ce passionnant projet en lumière.

Entretien avec John Lejeune et l'équipe des h:D

Réalisé le 11 août par Siltaär pour Framasoft

Bonjour John, pour commencer, pouvez-vous nous dire qui se cache derrière le smiley bleu du logo ?

Alors, l'équipe se détaille de la manière suivante :

- Cécile Montagne, qui s'occupe des aspects administratifs et comptables
- Jérôme Blondon, développeur et actuel chef de projet
- Johan Charpentier, développeur et actuel administrateur système
- John Lejeune, développeur et actuel *community manager* / « chef produit », si tant est que les communautés se *manage* et que les produits aient un chef. En charge du rédactionnel sur le site et sur les routes le reste du temps
- Louis Montagne, CEO de la SCOP Bearstech, à l'origine du projet
- Wim Vandeputte, CEO kd85.com, aussi sur les routes pour les ateliers

Sans oublier les remontées d'infos via les utilisateurs, les hackers, les hackspaces, etc..

Ainsi que d'autres personnes qui vont rejoindre la société dès qu'elle sera créée, comme Paul Coudamy.

Dans quelles circonstances s'est monté Hackable Devices ?

Le projet est né chez Bearstech, juste après le dernier Chaos Communication Camp (2007), Laurent Haond et Louis Montagne, qui y étaient, sont revenus avec beaucoup d'idées et du matériel, comme un Neo 1973.

Ca a donné lieu à pas mal de projets chez Bearstech, dont la distribution des OpenMoko, puis, suite à des discussions entre hackers lors du 25C3 à Berlin, au sujet de la diffusion du hardware libre et des hacks électroniques en tous genres, ça a bien pris forme.Il y avait déjà un embryon de stand hackable-devices lors du Hacking At Random 2009. C'est à partir de là que les choses se sont mises en place, et que les premiers développements de la plate-forme ont vu le jour.

Comment s'est fait le rapprochement entre Bearstech, Kd85 et faberNovel ?

Bearstech a déjà créé une société avec faberNovel, en 2006 : af83, c'est un partenaire de choix pour réussir le lancement d'une entreprise. Pour Kd85, le plus naturellement du monde, puisque nous nous retrouvions sur les mêmes évènements (FOSDEM, HAR, CCC, RMLL, etc.). Wim a pas mal promu OpenBSD ces dix dernières années.

On discute aussi aujourd'hui avec d'autres partenaires, comme NodA par exemple.

Pourquoi avoir choisi un nom anglais ?

Parce que « Matériels Bidouillables » ça garde une connotation péjorative que « Hackable » n'a pas, et que ça ne *sonne* plus juste (tout comme Framasoft a pris le pas sur

« FramaLogiciel », je suppose)

Parce que nous voulions d'emblée avoir une couverture Européenne, mondiale (par la nature même des projets et des fournisseurs), et que l'Anglais reste l'Esperanto *de facto*.

D'autre part, avec tous ces joyeux lurons qui forment l'équipe, nous pouvons répondre aux demandes en anglais, allemand, espagnol, flamand et bien sûr, français. C'est l'anglais qui nous permet de communiquer entre nous.

Enfin, parce qu'on avait besoin d'un nouveau nom, quelque chose qui soit facilement identifiable et qui soit juste à la limite, toujours un peu ambigu, … On voit le hacking comme l'augmentation, l'amélioration ou la compréhension, et c'est ce message que l'on veut faire passer.

Quels sont les objectifs du site ?

Le site n'est qu'une des 3 activités de la future société Hackable:Devices, mais on ne va pas en dire trop tout de suite

Ses objectifs :

- Faciliter et promouvoir la distribution du matériel modifiable, en privilégiant celui qui offre des licences libres (en construisant un site rentable permettant de fédérer les distributeurs de ces matériels, de trouver les nouveaux matériels et de les mettre en avant) ;
- Fédérer et accompagner ceux qui font des prototypes, des petites séries, des projets, afin d'avoir une plate-forme commune et de produire les meilleurs ;
- Promouvoir l'initiation, l'éducation et le fun à travers certains produits/kits, et bien sur promouvoir le Libre en général ;
- Être un support pour les évènements et autres salons lorsque les utilisateurs souhaitent « mettre les mains dedans » ;

- Servir de base à la création d’objets design, libres et numériques.

D’où est venue l’idée de vendre du matériel ?

C’était un besoin à la base. Pour avoir constaté qu’il n’était pas toujours simple de trouver l’info, d’importer des choses sans surprises, puis de gérer les frais divers (port, douanes, etc..), nous nous sommes dis que nous n’étions pas les seuls à avoir ce genre de problématique. L’expérience du Freerunner a été le déclencheur. On voulait pouvoir avoir accès à un LinuxDevices.com, mais sur lequel on pourrait acheter.

Et avec quelles infrastructures ?

Pour l’instant, grâce à celles de kd85 et de Bearstech. Ce sont ces deux sociétés qui soutiennent et développent le projet en attendant la création d’une entité juridique autonome. Le premier pour la logistique, à savoir tout ce qui concerne la réception du stock, les expéditions. Le second pour gérer le reste, à savoir les développements et l’hébergement du site, les fiches produits, le suivi et la facturation, les plaisirs douaniers et administratifs en tous genres.

En ce qui concerne les évènements et les ateliers, nous nous partageons la tâche selon les disponibilités de chacun, les proximités géographiques, et nous nous retrouvons parfois au complet sur d’autres, comme les RMLL ou les Chaos Computer Congress.

Comment s’est montée la communauté ?

Par le bouche à oreille principalement, et parce que nous sommes nous même issus de cette communauté.

Ensuite, c’est un travail quotidien de mail, de publication, de déplacements pour des démonstrations, d’ateliers d’initiation…

Et aujourd'hui, combien compte-elle de personnes (hackers, créateurs, fabricants, investisseurs) ?

h:D c'est aujourd'hui plus de 500 utilisateurs actifs, un peu plus de 7000 visiteurs mensuels, pour une quarantaine de produits. Beaucoup de nos membres sont des hackers, même si cela tend à se diffuser, au profit d'un public plus large. Les artistes, designers, plasticiens, musiciens, sont de plus en plus nombreux à nous rejoindre et c'est tant mieux.

Les investisseurs, pour l'instant, point. Nous supportons seuls les coûts, mais ça ne saurait tarder

Pour combien de projets ?

Près d'une dizaine. Tous ne sont pas nécessairement liés à Hackable:Devices et tous ne sont pas encore publiés, il y a pas mal de *work in progress*.

C'est un des problèmes à surmonter. On a beau dire release early, release often, concrètement, il faut toujours lutter contre la tendance « oui, mais c'est pas encore prêt, j'ai encore quelques trucs à terminer avant publication ».

L'autre souci souvent rencontré c'est, « ben, ça vaut pas le coup, c'est trop simple, je vais pas publier ça !?! ». Typiquement, tout ce qui tourne autour d'Arduino est souvent dans ce cas.

Et puis il y a des projets qui demandent pas mal de coordination avant de voir le jour, par exemple en ce moment autour de la surveillance de la consommation énergétique, avec une collaboration entre Snootlab, Nod-A et OpenEnergyMonitor.org, ou encore autour de la fabrication d'un notebook communautaire, avec blogARM.

Quels sont les projets les plus actifs ?

Aujourd'hui, en terme de réalisations, je dirais NanoNote, Milkymist, Mutable Instruments, Proxmark (site officiel)

aussi.

Quels sont vos projets préférés ?

Difficile comme question. Au sein de l'équipe, chacun a ses préférences, ce qui fait qu'au final, il n'y a pas un projet qui attire toutes les attentions.

À titre personnel, j'aime bien ce qui est lié au son, à la radio, donc je dirais Tryphon (site officiel), Sonodrome (site officiel), Mutable Instruments (site officiel). Mais j'aime aussi Milkymist (site officiel) et NanoNote (site ooficiel), pour l'aspect Copyleft qu'ils illustrent à merveille.

Parlez-moi du projet NoBox/Soxyd référencé sur Hackable-Devices.org. De quoi s'agit-il ?

Il s'agit de permettre aux utilisateurs de se réapproprier les données, au travers d'une « box » à installer chez soi. La problématique est connue de Framasoft, je me souviens avoir lu récemment la traduction de l'interview d'Eben Moglen, par Glyn Moody.

Comment vous y êtes vous intéressés ?

En ce qui me concerne, j'ai découvert cette problématique avec certains membres de FDN il y a quelques temps déjà. Elle commence à se diffuser grâce à l'émergence de matériel adéquat, mais aussi en réponse au cloud et aux questionnements qu'il apporte.

Sur la plate-forme à proprement parler, elle est apparue sur l'initiative spontanée de Gordontesos, après une discussion sur IRC.

Et où en est-il chez vous ?

Gordontesos a commençé les développements sur un Sheevaplug il y a quelques semaines. La coopération est ouverte.

J’ai eu l’occasion à Bordeaux de discuter du sujet avec Benjamin Bayard lors des RMLL 2010, qui me confirmait l’importance de l’expérience utilisateur au niveau de l’interface graphique. C’est à mon sens le point sur lequel se concentrer.

Et le Freerunner, on est en route pour une v2 ?

J’aimerais bien, mais j’en doute. Avec la prolifération des smartphones, l’apparition d’Android et consort, je doute qu’OpenMoko se relance dans l’aventure, au profit du Wiki Reader. À mon sens, cela restera une plate-forme de tests / prototypage / amusement sans jamais atteindre le grand public.

Une petite baisse de régime sur le flux Identica depuis un mois ? Tout le monde est en vacances ?

Oui.

Enfin, plus maintenant si vous suivez ce lien

Cherchez-vous de nouveaux contributeurs ?

Toujours.

Qu’il s’agisse d’info à remonter, d’évènements auxquels participer, de produits susceptibles d’intégrer h:D, de traductions, vous êtes les bienvenus.

Pour finir, la traditionnelle question de clôture des entretiens : « Quelle est la question que je n’ai pas posée mais à laquelle vous auriez voulu répondre ? »

Celle-ci justement.

Blague à part : « Où en est le hardware Libre ? » peut-être.

Réponse : Ça bouge pas mal ces temps-ci, avec des initiatives telles que Ohanda ou encore le Open Hardware Summit de New-York en septembre. Ce sera peut-être l’occasion de voir émerger une définition commune, en cours sur Freedomdefined.

La liberté contre les traces dans le nuage – Une interview d'Eben Moglen

Il y a un peu plus d'une semaine Tristan Nitot évoquait sur son blog une « magnifique interview » du juriste Eben Moglen par le journaliste Glyn Moody (que nous connaissons bien sûr le Framablog, preuve en est qu'ils ont l'honneur de tags dédiés : Moglen et Moody).

C'est la traduction de l'intégralité de cette interview que nous vous proposons ci-dessous.

Pourquoi Nitot était-il si enthousiaste ? Parce qu'il est légitime de s'inquiéter chaque jour davantage du devenir de nos données personnelles captées par des Facebook et des Google. Mais la critique récurrente sans possibilités d'alternatives pousse au découragement.

Or, poursuit-il, cette interview propose « une ébauche de solution technique qui pourrait bien signer la fin du Minitel 2.0 ». Eben Moglen y explique « comment des petits ordinateurs comme le Sheevaplug (cf photo ci-contre) ou le Linutop 2 pourraient bien changer la donne en permettant la construction d'un réseau social distribué (ou a-centré) dont chacun pourrait contrôler un bout et surtout contrôler son niveau de participation ».

Et Tristan de conclure de manière cinglante : « l'identité en ligne, la liste de nos relations, les archives de nos messages échangés sont bien trop précieuses pour être confiées à quelconque organisation privée, quelle qu'elle soit ».

La décennie « Microsoft » qui s'achève nous aura vu essayer, avec plus ou moins de succès, d'empêcher le contrôle de nos ordinateurs personnels, en y substituant du logiciel propriétaire par du logiciel libre.

La décennie « Google » qui s'annonce risque fort d'être celle des tentatives pour empêcher le contrôle d'Internet, en ne laissant plus nos données personnelles sur des serveurs privés mais sur nos propres serveurs personnels.

Remarque : à propos d'Eben Moglen, nous vous rappelons l'existence d'une conférence que nous considérons parmi les plus importantes jamais présentées par la communauté du Libre.

Une interview d'Eben Moglen – La liberté contre les données dans le nuage

Interview: Eben Moglen – Freedom vs. The Cloud Log

Eben Moglen interviewé par Glyn Moody – 17 mars 2010 – The H (Traduction Framalang : Goofy, Simon Descarpentries et Barbidule)

Le logiciel libre a gagné : presque tous les poids lourds du Web les plus en vue comme Google, Facebook et Twitter, fonctionnent grâce à lui. Mais celui-ci risque aussi de perdre la partie, car ces mêmes services représentent aujourd'hui une sérieuse menace pour notre liberté, en raison de l'énorme masse d'informations qu'ils détiennent sur nous, et de la surveillance approfondie que cela implique.

Eben Moglen est sûrement mieux placé que quiconque pour savoir quels sont les enjeux. Il a été le principal conseiller juridique de la Free Software Foundation pendant 13 ans, et il

a contribué à plusieurs versions préparatoires de la licence GNU GPL. Tout en étant professeur de droit à l'école de droit de Columbia, il a été le directeur fondateur du Software Freedom Law Center (Centre Juridique du Logiciel Libre). Le voici aujourd'hui avec un projet ambitieux pour nous préserver des entreprises de services en ligne qui, bien que séduisantes, menacent nos libertés. Il a expliqué ce problème à Glyn Moody, et comment nous pouvons y remédier.

Glyn Moody : Quelle est donc cette menace à laquelle vous faites face ?

Eben Moglen : Nous sommes face à une sorte de dilemme social qui vient d'une dérive dans la conception de fond. Nous avions un Internet conçu autour de la notion de parité – des machines sans relation hiérarchique entre elles, et sans garanties quant à leur architectures internes et leur comportements, mises en communication par une série de règles qui permettaient à des réseaux hétérogènes d'être interconnectés sur le principe admis de l'égalité de tous.

Sur le Web, les problèmes de société engendrés par le modèle client-serveur viennent de ce que les serveurs conservent dans leur journaux de connexion (logs) les traces de toute activité humaine sur le Web, et que ces journaux peuvent être centralisés sur des serveurs sous contrôle hiérarchisé. Ces traces deviennent le pouvoir. À l'exception des moteurs de recherche, que personne ne sait encore décentraliser efficacement, quasiment aucun autre service ne repose vraiment sur un modèle hiérarchisé. Ils reposent en fait sur le Web – c'est-à-dire le modèle de pair-à-pair non hiérarchisé créé par Tim Berners-Lee, et qui est aujourd'hui la structure de données dominante dans notre monde.

Les services sont centralisés dans un but commercial. Le pouvoir des traces est monnayable, parce qu'elles fournissent un moyen de surveillance qui est intéressant autant pour le commerce que pour le contrôle social exercé par les

gouvernements. Si bien que le Web, avec des services fournis suivant une architecture de base client-serveur, devient un outil de surveillance autant qu'un prestataire de services supplémentaires. Et la surveillance devient le service masqué, caché au cœur de tous les services gratuits.

Le nuage est le nom vernaculaire que nous donnons à une amélioration importante du Web côté serveur – le serveur, décentralisé. Au lieu d'être une petite boîte d'acier, c'est un périphérique digital qui peut être en train de fonctionner n'importe où. Ce qui signifie que dans tous les cas, les serveurs cessent d'être soumis à un contrôle légal significatif. Ils n'opèrent plus d'une manière politiquement orientée, car ils ne sont plus en métal, sujets aux orientations localisées des lois. Dans un monde de prestation de services virtuels, le serveur qui assure le service, et donc le journal qui provient du service de surveillance induit, peut être transporté sur n'importe quel domaine à n'importe quel moment, et débarrassé de toute obligation légale presque aussi librement.

C'est la pire des conséquences.

GM : Est-ce qu'un autre facteur déclenchant de ce phénomène n'a pas été la monétisation d'Internet, qui a transféré le pouvoir à une entreprise fournissant des services aux consommateurs ?

EM : C'est tout à fait exact. Le capitalisme a aussi son plan d'architecte, qu'il rechigne à abandonner. En fait, ce que le réseau impose surtout au capitalisme, c'est de l'obliger à reconsidérer son architecture par un processus social que nous baptisons bien maladroitement dés-intermédiation. Ce qui correspond vraiment à la description d'un réseau qui contraint le capitalisme à changer son mode de fonctionnement. Mais les résistances à ce mouvement sont nombreuses, et ce qui nous intéresse tous énormément, je suppose, quand nous voyons l'ascension de Google vers une position prééminente, c'est la

façon dont Google se comporte ou non (les deux à la fois d'ailleurs) à la manière de Microsoft dans sa phase de croissance. Ce sont ces sortes de tentations qui s'imposent à vous lorsque vous croissez au point de devenir le plus grand organisme d'un écosystème.

GM : Pensez-vous que le logiciel libre a réagi un peu lentement face au problème que vous soulevez ?

EM : Oui, je crois que c'est vrai. Je pense que c'est difficile conceptuellement, et dans une large mesure cette difficulté vient de ce que nous vivons un changement de génération. À la suite d'une conférence que j'ai donnée récemment, une jeune femme s'est approchée et m'a dit : « j'ai 23 ans, et aucun de mes amis ne s'inquiète de la protection de sa vie privée ». Eh bien voilà un autre paramètre important, n'est-ce pas ? – parce que nous faisons des logiciels aujourd'hui en utilisant toute l'énergie et les neurones de gens qui ont grandi dans un monde qui a déjà été touché par tout cela. Richard et moi pouvons avoir l'air un peu vieux jeu.

GM : Et donc quelle est la solution que vous proposez ?

EM : Si nous avions une classification des services qui soit véritablement défendable intellectuellement, nous nous rendrions compte qu'un grand nombre d'entre eux qui sont aujourd'hui hautement centralisés, et qui représentent une part importante de la surveillance contenue dans la société vers laquelle nous nous dirigeons, sont en fait des services qui n'exigent pas une centralisation pour être technologiquement viables. En réalité ils proposent juste le Web dans un nouvel emballage.

Les applications de réseaux sociaux en sont l'exemple le plus flagrant. Elles s'appuient, dans leurs métaphores élémentaires de fonctionnement, sur une relation bilatérale appelée amitié, et sur ses conséquences multilatérales. Et elles sont

complètement façonnées autour de structures du Web déjà existantes. Facebook c'est un hébergement Web gratuit avec des gadgets en php et des APIs, et un espionnage permanent – pas vraiment une offre imbattable.

Voici donc ce que je propose : si nous pouvions désagréger les journaux de connexion, tout en procurant aux gens les mêmes fonctionnalités, nous atteindrions une situation Pareto-supérieure. Tout le monde – sauf M. Zuckerberg peut-être – s'en porterait mieux, et personne n'en serait victime. Et nous pouvons le faire en utilisant ce qui existe déjà.

Le meilleur matériel est la SheevaPlug, un serveur ultra-léger, à base de processeur ARM (basse consommation), à brancher sur une prise murale. Un appareil qui peut être vendu à tous, une fois pour toutes et pour un prix modique ; les gens le ramènent à la maison, le branchent sur une prise électrique, puis sur une prise réseau, et c'est parti. Il s'installe, se configure via votre navigateur Web, ou n'importe quelle machine disponible au logis, et puis il va chercher toutes les données de vos réseaux sociaux en ligne, et peut fermer vos comptes. Il fait de lui-même une sauvegarde chiffrée vers les prises de vos amis, si bien que chacun est sécurisé de façon optimale, disposant d'une version protégée de ses données chez ses amis.

Et il se met à faire toutes les opérations que nous estimons nécessaires avec une application de réseau social. Il lit les flux, il s'occupe du mur sur lequel écrivent vos amis – il rend toutes les fonctionnalités compatibles avec ce dont vous avez l'habitude.

Mais le journal de connexion est chez vous, et dans la société à laquelle j'appartiens au moins, nous avons encore quelques vestiges de règles qui encadrent l'accès au domicile privé : si des gens veulent accéder au journal de connexion ils doivent avoir une commission rogatoire. En fait, dans chaque société, le domicile privé de quelqu'un est presque aussi

sacré qu'il peut l'être.

Et donc, ce que je propose basiquement, c'est que nous construisions un environnement de réseau social reposant sur les logiciels libres dont nous disposons, qui sont d'ailleurs déjà les logiciels utilisés dans la partie serveur des réseaux sociaux; et que nous nous équipions d'un appareil qui inclura une distribution libre dont chacun pourra faire tout ce qu'il veut, et du matériel bon marché qui conquerra le monde entier que nous l'utilisions pour ça ou non, parce qu'il a un aspect et des fonctions tout à fait séduisantes pour son prix.

Nous prenons ces deux éléments, nous les associons, et nous offrons aussi un certain nombre d'autres choses qui sont bonnes pour le monde entier. Par exemple, pouvoir relier automatiquement chaque petit réseau personnel par VPN depuis mon portable où que je sois, ce qui me procurera des proxies chiffrés avec lesquels mes recherches sur le Web ne pourront pas être espionnées. Cela signifie que nous aurons des masses d'ordinateurs disponibles pour ceux qui vivent en Chine ou dans d'autres endroits du monde qui subissent de mauvaises pratiques. Ainsi nous pourrons augmenter massivement l'accès à la navigation libre pour tous les autres dans le monde. Si nous voulons offrir aux gens la possibilité de profiter d'une navigation anonymisée par un routage en oignon, c'est avec ce dispositif que nous le ferons, de telle sorte qu'il y ait une possibilité crédible d'avoir de bonnes performances dans le domaine.

Bien entendu, nous fournirons également aux gens un service de courriels chiffrés – permettant de ne pas mettre leur courrier sur une machine de Google, mais dans leur propre maison, où il sera chiffré, sauvegardé chez tous les amis et ainsi de suite. D'ailleurs à très long terme nous pourrons commencer à ramener les courriels vers une situation où, sans être un moyen de communication privée, ils cesseront d'être des cartes postales quotidiennes aux services secrets.

Nous voudrions donc aussi frapper un grand coup pour faire avancer de façon significative les libertés fondamentales numériques, ce qui ne se fera pas sans un minimum de technicité.

GM : Comment allez-vous organiser et financer un tel projet, et qui va s'en occuper ?

EM : Avons-nous besoin d'argent ? Bien sûr, mais de petites sommes. Avons-nous besoin d'organisation ? Bien sûr, mais il est possible de s'auto-organiser. Vais-je aborder ce sujet au DEF CON cet été, à l'Université de Columbia ? Oui. Est-ce que M. Shuttleworth pourrait le faire s'il le voulait ? Oui encore. Ça ne va pas se faire d'un coup de baguette magique, ça se fera de la manière habituelle : quelqu'un va commencer à triturer une Debian ou une Ubuntu ou une autre distribution, et va écrire du code pour configurer tout ça, y mettre un peu de colle et deux doigts de Python pour que ça tienne ensemble. D'un point de vue quasi capitaliste, je ne pense pas que ce soit un produit invendable. En fait, c'est un produit phare, et nous devrions en tout et pour tout y consacrer juste un peu de temps pour la bonne cause jusqu'à ce que soit au point.

GM : Comment allez-vous surmonter les problèmes de masse critique qui font qu'on a du mal à convaincre les gens d'adopter un nouveau service ?

EM : C'est pour cela que la volonté constante de fournir des services de réseaux sociaux interopérables est fondamentale.

Pour le moment, j'ai l'impression que pendant que nous avancerons sur ce projet, il restera obscur un bon moment. Les gens découvriront ensuite qu'on leur propose la portabilité de leur réseau social. Les entreprises qui gèrent les réseaux sociaux laissent en friche les possibilités de leurs propres réseaux parce que tout le monde veut passer devant M. Zuckerberg avant qu'il fasse son introduction en bourse. Et c'est ainsi qu'ils nous rendront service, parce qu'ils

rendront de plus en plus facile de réaliser ce que notre boîte devra faire, c'est-à-dire se connecter pour vous, rapatrier toutes vos données personnelles, conserver votre réseau d'amis, et offrir tout ce que les services existants devraient faire.

C'est comme cela en partie que nous inciterons les gens à l'utiliser et que nous approcherons la masse critique. D'abord, c'est cool. Ensuite, il y a des gens qui ne veulent pas qu'on espionne leur vie privée. Et puis il y a ceux qui veulent faire quelque chose à propos de la grande e-muraille de Chine, et qui ne savent pas comment faire. En d'autres termes, je pense qu'il trouvera sa place dans un marché de niches, comme beaucoup d'autres produits.

GM : Alors que le marché des mobiles est en train de décoller dans les pays émergents, est-ce qu'il ne vaudrait pas mieux demander aux téléphones portables de fournir ces services ?

EM : Sur le long terme, il existe deux endroits où vous pouvez raisonnablement penser stocker votre identité numérique : l'un est l'endroit où vous vivez, l'autre est dans votre poche. Et un service qui ne serait pas disponible pour ces deux endroits à la fois n'est probablement pas un dispositif adapté.

A la question « pourquoi ne pas mettre notre serveur d'identité sur notre téléphone mobile ? », ce que je voudrais répondre c'est que nos mobiles sont très vulnérables. Dans la plupart des pays du monde, vous interpellez un type dans la rue, vous le mettez en état d'arrestation pour un motif quelconque, vous le conduisez au poste, vous copiez les données de son téléphone portable, vous lui rendez l'appareil, et vous l'avez eu.

Quand nous aurons pleinement domestiqué cette technologie pour appareils nomades, alors nous pourrons commencer à faire l'inverse de ce que font les opérateurs de réseaux. Leur activité sur la planète consiste à dévorer de d'Internet, et à

excréter du réseau propriétaire. Ils devront faire l’inverse si la technologie de la téléphonie devient libre. Nous pourrons dévorer les réseaux propriétaires et essaimer l’Internet public. Et si nous y parvenons, la lutte d’influence va devenir bien plus intéressante.