Quand le ciel se couvre

Ces derniers temps avec la monté en puissance du cloud computing pour le grand public nos applications tendent à disparaîtres et nos PC se transforment en petit espace de stockage (quelques gigaoctets sur un SSD) connectés. Les serveurs d'avant deviennent intelligents et ne se content plus de stocker. Ils nous fournissent applications et données. Applications propriétaires. Données trop publiques.

Un récent billet de Joanna Rutkowska me fait penser à une vieille idée. Dans ces conditions je serai partant pour utiliser quelque chose comme un Chromebook. Mon problème principal de la perte du contrôle des données est presque résolu. La solution est le chiffrement. Le chiffrement protège nos données de toute une série d'acteurs dont nous sommes forcé d'accorder notre confiance.

Le problème: est-ce que les fournisseurs de services seraient prêts à héberger toutes nos données chiffrées (donc inintelligible)? En générant nos clés de chiffrement et en chiffrant côté client les données avant de les envoyer sur le cloud toute cette polémique autour de dropbox n'aurait pas eu lieu. En même temps on pouvait s'y attendre, franchement comment un service comme dropbox ou Google pourrait héberger nos données pour ne rien en faire? Absolument rien, mis à part les stocker. Il n'y aurait donc aucune exploitation possible de ces données, quasiment plus d'intelligences dans ce cloud, juste du stockage. Un service si *gentil* serait de toute manière sous une licence type AGPL. Sinon où est l'intérêt?
Et cette intelligence sur le cloud, qu'elle est son utilité? Généralement établir notre graphe social (comme le dit Éric Schmidt de manière décomplexée), découvrir nos centres d'intérêts. Ce serait un peu plus compliqué avec un carnet d'adresses chiffré.

Je serai vraiment surpris que dans un avenir plus ou moins proche il soit possible de faire cela avec un Chromebook. Nous avons toutes les technologies et l'expérience requise pour implémenter cette idée, ce n'est *que* de la cryptographie. Il faudrait adapter un peu quelques applications clientes (pensez au potentiel d'aKonadi). Avec différents couples de clés on pourrait choisir avec qu'elle personne ou groupe(s) de personnes on partage une information Il y a des protocoles cryptographiques spécifiques pour ça. La notion d'espace partagé et surtout public de dropbox est une hérésie. Pour de nombreux types de données (agenda, localisation, numéro de téléphone, etc.) l'utilisateur a un besoin presque naturel de partager à des groupes de différents niveaux de confiance. Confiance relative. Confiance absolue pour le partage public.

Il faut donc garder nos bonnes vieilles applications clientes. Mettre plus de données chiffrées dans ce cloud qui est en train de tous nous baiser. Cela n'exclue pas de garder des applications *web-based* comme Gmail. Avec la solution de Joanna Rutkowska une application comme Gmail pourrait aussi avoir accès à nos données chiffrées.
De plus conserver les applications clientes ne peut que favoriser les standards et l'interopérabilité. J'aime savoir que Kontact, Evolution et Thunderbird puissent exploiter les mêmes données sur mon cloud, ou alors LibreOffice et KOffice. Avec des applications uniquement en ligne comme Gmail ou Google Docs on risque de perdre en interopérabilité (on sera rattaché à un service) et en qualité. Je trouve surtout ça moins élégant d'un point de vue informatique.
Certaines personnes aiment écrire des logiciels amateurs (par plaisir de comprendre comment fonctionne un ordinateur ou pour un besoin particulier) ou aiment savoir si une mise à jour d'un programme utilisé courrament a changée son comportement. La culture du Do It Yourself a besoin de ça.

Par sécurité (cf. les problèmes d'Amazon, du PSN et bien d'autres) il serait bon de synchroniser par exemple un NAS personnel avec notre petit morceau de cloud. Ce support de stockage devrait disposer (tout comme notre smartphone, tablette et PC portable) des clés appropriées pour garder les données non chiffrées (sécurité oblige, mais si souhaitable à ce niveau on peut utiliser TPM ou TXT). Le PC de bureau peut être connecté localement au NAS. Je pense que sur un PC fixe il est idiot d'utiliser un service cloud alors qu'on a un support de stockage qui peut s'occuper de synchroniser les modifications effectuées depuis ce PC. Si je veux regarder Titanic dans mon salon et qu'il est sur mon NAS non chiffré, pourquoi aller le chercher sur Internet? De même pour un simple fichier (et oui, bientôt avec Google Music vous pourrez écouter dans votre salon de la musique en ligne. La même qui se trouve sur votre disque dur). Par contre si le fichier est modifié, le support de stockage peut s'occuper de faire le chiffrement et la synchronisation. Par la suite on pourra continuer à éditer ce fichier avec un

smartphone ou appareil type Chromebook sur le cloud. Pourquoi faire confiance inutilement à toute une flopée de services et gâcher des ressources?
On peut citer la couche d'abstraction d'aKonadi qui est très intéressante pour interagir avec le cloud. aKonadi permet de synchroniser son calendrier ainsi que ces contacts (sur gmail ou serveur personnel de façon transparente). Lorsque j'édite mon calendrier en ligne avec ma tablette mon calendrier KOrganizer est mis à jour sur le PC de bureau. Connexions sécurisées et calendrier sur mon disque dur disponible en mode non connecté (malheureusement le calendrier en ligne est visible pour Google). C'est un peu ce fonctionnement qu'il faudrait généraliser à toutes nos données.

La cryptographie est une arme puissante et incontournable qui nous aidera à conserver notre vie privée.

On pourra lire également ceci.
