Keyoxide est à la cryptographie ce que des Lego en mercure seraient à l'aérospatial

Océane*

[2024-02-29 jeu. 18:49]

Dans le premier Iron Man, qui est incidemment le dernier film Marvel où l'on voit une journaliste faire son travail, Tony Stark se fait construire un premier cœur, expérimental, dans une caverne où il est retenu en otage, en Afghanistan. Puis comme c'est un prototype conçu avec les moyens du bord pour lui sauver la vie, il se fait construire un second cœur, plus durable, plus puissant. Il demande à sa secrétaire, Pepper Potts, de l'incinérer, et elle le lui rend sous la forme d'une décoration de bureau, cadeau sentimental où il est écrit « Preuve que Tony Stark a un cœur ».

C'est ainsi que je vois OpenPGP : un prototype expérimental, un objet sentimental pour linuxien·ne, destiné à prouver son identité sur Keyoxide par exemple, quelque part sur une étagère entre une figurine Toad et un Tardis en Lego. J'appellerais bien à abandonner cette norme de toute urgence, à ne pas donner à ses utilisataires un faux sentiment de sécurité, alors qu'elle est difficile à implémenter (à travers des bibliothèques comme GnuPG ou OpenPGPjs) et à utiliser de manière sécurisée (du point de vue par exemple de la rotation de clé).

Ces dernières années, des entreprises réputées ont connu des failles de sécurité critiques autour d'OpenPGP, comme :

- Yubico a sorti des clés de sécurité FIPS (certifiées par le gouvernement états-unien pour l'usage en entreprise) dont l'envoi de trois emails signés permettait de déduire la clé privée,
- la faille de sécurité Efail permettait de lire l'ensemble des emails, ProtonMail a publié un communiqué notamment signé par le créateur de PGP, disant que c'était un problème d'implémentation et non de standard (ce qui est plus ou moins un mensonge), et qu'il fallait utiliser des implémentations sécurisées, comme ProtonMail ou GnuPG, et envoyer ses emails en texte brut,

*océane.fr

- ProtonMail, qui implémente OpenPGP en Javascript, a été victime d'un bug d'injection XSS inter-sites, et, de mémoire, me semble l'avoir nié dans un premier temps, ce qui est exactement ce que l'on attend d'une entreprise de sécurité informatique, et

- une autre faille de sécurité, que je ne cherche pas dans l'immédiat par manque de connexion internet, et car cette liste n'est qu'un exemple, concernant de nombreuses implémentations.

Plus vos conversations chiffrées avec OpenPGP intègrent de collaborataires, plus le risque d'une implémentation vulnérable à une faille de sécurité, ou d'un serveur d'emails transmettant le contenu chiffré à une agence de renseignement, ou encore que l'un de vos contacts fasse une erreur et réponde en clair, s'accroît. Une mitigation possible et très insuffisante peut être de converser en texte brut et de pratiquer le *bottom posting*, c'est-à-dire de ne citer que les extraits auxquels vous répondez et de supprimer le reste, ce qui limiterait le risque d'envoyer l'ensemble du fil en cas de mauvaise manipulation. Cette norme reste un bingo de mauvaises pratiques de sécurité informatique, ce qui en exclut tout usage militant.

Quelle différence donc entre un profil Keyoxide et un vaisseau spatial de Kylo Ren en Lego ? À part bien sûr le risque de se doxxer soi-même, ce que des expert·es en cryptographie ont déjà fait, ou alors d'inscrire son morinom dans une base de données inaltérable (la page d'accueil du serveur OpenPGP du MIT a un bouton « Oui, supprimer ma clé ! » redirigeant vers une entrée de FAQ disant que non, on ne peut pas supprimer sa clé) ? Quel danger pour moi, qui ne suis simplement pas sûre de vouloir garder mon prénom actuel, et qui ai failli téléverser une clé quelques années avant ma transition ? Quel risque, alors que le développeur principal de Keyoxide est en bons termes avec des admins d'instance plus ou moins incompétents, mais pleins d'aplomb, et ayant par le passé mobilisé leurs audiences contre des personnes racisées ? Pourvu que notre clé publique et nos certifications ne permettent pas de remonter jusqu'à notre identité réelle, par exemple en certifiant notre profil LinkedIn, pas grand-chose ; mais ça ne sort pas pour autant l'usage d'OpenPGP des pratiques à risque. Est-ce un exemple à donner à des personnes mineures ?