Bitmessage, le courrier enfin sécurisé ?

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 8 juillet 2013

https://www.bortzmeyer.org/bitmessage.html

Le système de messagerie Bitmessage est publié depuis plusieurs mois mais il a acquis une soudaine célébrité avec les révélations sur le programme PRISM. Il y a déjà eu beaucoup d'articles (y compris en français) sur Bitmessage donc je vais ici plutôt me concentrer sur des détails qui n'ont pas toujours été mentionnés.

Un rappel d'abord : Bitmessage est prévu pour faire de la messagerie sécurisée, notamment protégée contre l'espionnage de la NSA ou de la DGSE. Il opère en utilisant des adresses qui sont un condensat d'une clé publique (la mienne est BM-2D8rwZkR1KvUMCnBhH7MGzTwVRXnDvhMC9, vous pouvez m'écrire mais vous pouvez aussi essayer l'auto-répondeur BM-orkCbppXWSqPpAxnz6jnfTZ2djb5pJKDb). Les messages sont transmis au monde entier (Bitmessage n'a pas de préoccupations écologiques et fait travailler toutes les machines du réseau) mais seul le récepteur pourra le lire. Au bout d'une heure trente de fonctionnement de mon logiciel, j'ai traité :

```
2791 messages person-to-person
700 broadcast
6072 public keys
```

Autre point pas écologique : Bitmessage dépend de « preuves de travail » (résolution de problèmes nécessitant la force brute comme de trouver une collision dans une fonction de condensation) pour limiter le spam et les attaques Sybil.

Bitmessage est documenté dans un (très court et très elliptique) "*whitepaper*" <https://bitmessage.org/bitmessage.pdf> et a une mise en œuvre de référence <https://github.com/Bitmessage/PyBitmessage> en Python.

Comme tous les systèmes à preuve de travail, il est très difficile à régler. Si le problème à résoudre est trop difficile, on ne pourra pas envoyer de Bitmessage depuis son "*smartphone*". Et s'il est trop facile, un botnet pourra envoyer autant de spam que ça lui chante.

Les adresses Bitmessage sont une bonne illustration de ma conjecture <https://www.bortzmeyer.org/no-free-lunch.html> comme quoi on ne peut pas avoir tout à la fois dans un identificateur. Ici, les concepteurs de Bitmessage ont sacrifié l'utilisabilité à la sécurité.

Notez qu'il existe une autre catégorie d'adresses, dérivée d'une phrase de passe et pas d'une clé publique (la mienne est BM-2DBbqaL9CSi7pVhzfHahy9vPD2hY3aTt5c). Le "*whitepaper*" n'en parle pas et je ne trouve pas de documentation sur leur principe. C'est en problème courant avec Bitmessage : la documentation est courte, et en retard sur le code.

Le lien avec Bitcoin, souvent cité, n'est pas clair non plus, à part quelques vagues analogies.

Bitmessage ne semble pas non plus très bien sécurisé contre les attaques par déni de service. Les nœuds de "*bootstrap*", et les relais, sont publics et connus (ils sont même dans le code, en src/defaultKnownNodes.p Ils peuvent être attaqués.

Attention aussi à la sécurité du poste local. Dans la version actuelle (0.3) du client de référence, la base de données SQLite contenant les messages, le carnet d'adresses, etc, est en clair. Même si on a effacé les messages, ils sont juste marqués détruits mais ils restent dans la boîte. Attention donc en cas de vol ou de perquisition. Il est recommandé d'avoir un disque local chiffré.

Enfin, attention, l'adresse de l'émetteur est vue par tout le réseau (où tout le monde peut s'inscrire). Cela ne donne pas accès au contenu des messages mais cela permet de savoir qui parle avec qui. La solution est de changer d'adresse souvent (ce que permet le client actuel facilement) au prix d'une perte de continuité dans sa réputation.

Je n'ai pas encore vu de comparaison systématique avec des systèmes concurrents comme TorChat, Freemail <https://freenetproject.org/freemail.html> ou Cryptocat <https://crypto.cat/>.

Bref, Bitmessage est intéressant et prometteur mais loin d'être fini.

Quelques articles utiles :

— Une bonne documentation de départ <http://cryptojunky.com/blog/2013/03/09/setting-up-and> (en anglais).
— Un bon article d'introduction <http://www.coindesk.com/bitmessage-is-the-bitcoin-of-onlin> (en anglais).
— Plutôt drôle : comment envoyer une image <http://tedjonesweb.blogspot.fr/2013/06/how-to-send-files-like-e-mail.html> avec le protocole et le client actuels. Cela rappellera des bons souvenirs aux utilisateurs d'UUCP et d'Usenet.
— Une bonne analyse de sécurité <https://bitmessage.org/forum/index.php?topic=1666.0>, très critique (et très technique, attention).
— Une expérience (réussie) d'd'attaque contre la sécurité de Bitmessage <http://secupost.net/>,
— Trois bons articles en français : chez Korben <http://korben.info/bitmessage.html>, chez Turblog <http://blog.spyou.org/wordpress-mu/2013/06/17/bitmessage-le-bitcoin-de> et sur PCinpact <http://www.pcinpact.com/news/80282-bitmessage-lorsque-protocole-bit htm>. Et une discussion (plutôt confuse) sur LinuxFr <http://linuxfr.org/users/julmx/journaux/bitmessage-envoi-de-messages-chiffres-en-p2p>.

Je voulais remercier nominativement les personnes qui m'ont aidé à explorer Bitmessage mais la plupart d'entre elles étaient anonymes... Donc, remerciements aux anonymes et à Changaco <http://changaco.net/>.