Matrix me désespère

Océane*

[2023-07-11 mar. 14:28]

Je suis un peu en retard sur mon rythme de publication, désolée ! Je continue d'écrire quand j'en ai le temps.

J'ai plusieurs soucis avec Matrix, je parlerai d'abord d'une décentralisation et d'un chiffrement insuffisants, puis de l'impact de leur client, Element, sur nos communications.

Premièrement, on me dit que Matrix est décentralisé, je crois que relativement à Matrix.org ce protocole est à peu près aussi décentralisé que les emails relativement à Gmail. Ensuite, le chiffrement a plusieurs problèmes :

1. Il est impossible de signaler un message dans un salon chiffré. Le message étant chiffré, il est censé être inaccessible, mais c'est un faux paradoxe puisqu'il est possible de prouver l'authenticité d'un message (en le signant). Il serait donc tout à fait possible de concevoir un algorithme chiffrant *et* signant les messages, comme le DIME permet théoriquement de le faire, permettant ainsi de transférer un message signé à la modération du serveur, au cas-par-cas. En bref, cela veut dire qu'il faut choisir entre le chiffrement de bout-en-bout (une préoccupation importante pour les utilisataires de logiciels libres) et le signalement des messages (une préoccupation importante pour les minorités de pouvoir). Symboliquement on doit choisir entre les enjeux des libristes et ceux des minorités de pouvoir, féministes, personnes racisées, mineures, handicapées, *etc*., comme si ces deux catégories étaient mutuellement exclusives.

2. Il est possible d'importer l'ensemble des messages d'un compte Matrix sur un appareil que l'on contrôle, irrévocablement, avec le mot de passe du compte et celui du téléphone de sa victime. Il suffit de s'authentifier sur un appareil que l'on contrôle, puis de vérifier sa session depuis un appareil légitime, pour importer l'ensemble des messages chiffrés. Peu importe que théoriquement ou dans le monde de Mon Petit Poney un mot de passe et un appareil vérifié représentent une forme d'authentification multi-facteurs : dans le monde réel, un

*oceane@disroot.org | océ.fr

prédateur domestique ou un officier de police judiciaire y ont à peu près forcément accès : vous pouvez être poursuivi·e pour refuser de transmettre vos identifiants à la police, dans le cadre d'un abus de lois antiterrorisme et d'une répression assumée, par les juges, comme politique. De même, si vous êtes sous emprise, par définition vous n'exercez pas toutes vos facultés de jugement, et vous pouvez lui transmettre votre mot de passe de téléphone pour une raison quelconque ; de manière générale, nos colocataires/conjoint·es ont des chances raisonnables de connaître notre mot de passe de téléphone, et la plupart des gens n'utilisent pas de gestionnaires de mots de passe, et ce n'est pas bien, mais ça veut dire qu'en général ces personnes ont 2 ou 3 mots de passe différents et qu'un prédateur peut très bien connaître ou déduire celui du compte Matrix. En bref, dans le monde réel, cette « authentification à deux facteurs » est extrêmement faible, et permettant de télécharger l'ensemble des messages, notamment chiffrés de bout-en-bout, de sa victime, potentiellement à son insu, cette faiblesse est très dangereuse.

3. Les messages sur Matrix n'ont pas rotation des paires de clés *via* un système de double cliquet. Cette rotation permet d'empêcher un intrus pouvant, par exemple, casser la clé de chiffrement par force brute, d'accéder à l'ensemble des messages, c'est ce que l'on appelle le PFS (*« Perfect Forward Secrecy »*). Le principe de chiffrement à double cliquet, un standard présent notamment dans OMEMO, Signal, et Cwtch, permet de changer de clé de chiffrement dès que l'on répond à un·e correspondant·e (c'est-à-dire à chaque aller-retour Alice → Bob → Alice). Avec de telles propriétés, un modèle de menace pouvant casser une clé de chiffrement par force brute (comme un serveur Matrix) ne pourrait accéder qu'à quelques messages.

4. La plupart des comptes Matrix étant hébergés sur un serveur appartenant à New Vector, l'entreprise (à but lucratif) qui pilote la Fondation Matrix et qui en développe le client principal, on peut raisonnable considérer qu'elle dispose des clés de chiffrement pour 99 % des conversations sur la norme Matrix, et donc qu'elle peut casser par force brute une clé de sécurité pour accéder à l'ensemble des messages échangés dans un salon.

Au fait, New Vector a été présent à un salon européen dédié à la police. Il ne s'agit pas de verser dans des théories du complot alors que leurs éventuelles conférences (je n'ai pas suivi cette affaire) sont sans doute enregistrées et accessibles au grand public, mais je ne vois pas de raison particulière de leur faire confiance.

Parlons maintenant de la manière dont le client Element impacte notre communication. Matrix optimise pour l'engagement de deux manières : premièrement car cet écosystème « ouvert » est fort de 4000 MSC, tandis que XMPP, par comparaison,

n'en a que 500, ce qui rend le développement de clients particulièrement complexe – à ma connaissance, seul Element en implémente toutes les fonctionnalités.

Ensuite car après une levée de 20 millions d'euros en capital-risque, New Vector a mis sur pied l'équipe « *delight* », qui a pour tâche, *grosso modo*, de récompenser les interactions avec l'interface utilisataire. Ces récompenses fournissant de la dopamine, elles sont perçues comme une forme de solidarité, et l'oubli du caractère individuel de chaque récompense dans une longue expérience de récompense donne un sentiment de solidarité inconditionnelle, et donc de sacré[1]. Émettre des jugements moraux permet justement d'« optimiser » cette illusion. Mais cette optimisation pour l'engagement a aussi évidemment pour conséquence d'imposer à leurs utilisataires les besoins de leurs investissaires et donc de les empêcher de répondre aux leurs ou à ceux de leur entourage, ce qui peut évidemment créer des tensions, donner lieu à des situations de maltraitance (notamment chez des personnes mineures), en tout cas à des addictions comportementales, *etc*.

On retrouve donc dans la plupart des salons Matrix cette manière violente et non-assumée d'impliquer que les messages de nos correspondant·es seraient malvenus, parce qu'ils nous incitent à rechercher ces récompenses et donc cette illusion de sacralité, au lieu de nous concentrer sur la construction de notre vie, par exemple sur des tâches domestiques, ou sur le fait de caresser son chat, afin d'avoir théoriquement accès à la solidarité sur laquelle est fondée notre société. L'aboutissement logique de l'optimisation pour l'engagement est la désaffiliation.

[1] Je ne veux pas réduire le sacré à la solidarité, il y a plein d'autres éléments qui me semblent importants, mais dans le cadre qui nous intéresse ici, c'en est la propriété la plus pertinente.