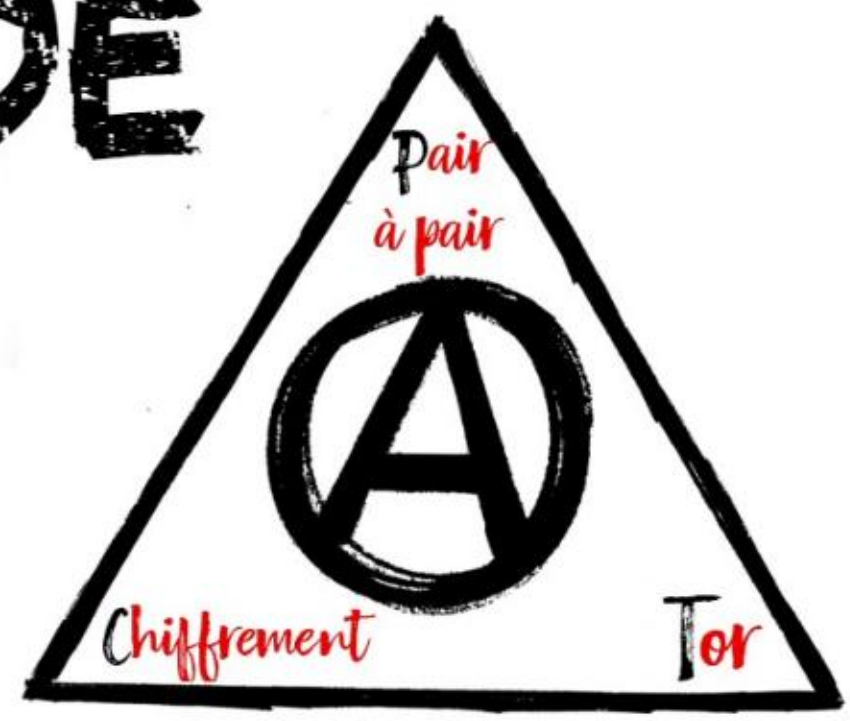
C.P.T.

LE GUIDE


Pair
à pair
Chiffrement
Tor


INFRASTRUC-
TURES
NUMÉRIQUES
DE
COMMUNICATION
POUR LES
ANARCHISTES

Infrastructures numériques de communication pour les anarchistes (et tous les autres…)

Un aperçu détaillé et un guide des diverses applications qui utilisent le pair-à-pair, le chiffrement et Tor

Source :

The Guide to Peer-to-Peer, Encryption, and Tor: New Communication Infrastructure for Anarchists, *It's Going Down*, 06 oct. 2022.

Traduction : Christophe Masutti

Révisions Framalang : ellébore, goofy, Henri-Paul, jums, Sichat, Wisi_eu

Framasoft

IT'S GOING DOWN

(Préambule)

Nous avons des adversaires, ils sont nombreux. Depuis la première diffusion de Pretty Good Privacy (PGP) en 1991 par Philip Zimmermann, nombreuses furent les autorités publiques ou organisations privées à s'inquiéter du fait que des individus puissent échanger des messages rigoureusement indéchiffrables en vertu de lois mathématiques (c'est moins vrai avec les innovations en calculateurs quantiques). Depuis lors, les craintes ne cessèrent d'alimenter l'imaginaire du bloc réactionnaire.

On a tout envisagé, surtout en se servant de la lutte contre le terrorisme et la pédopornographie, pour mieux faire le procès d'intention des réseaux militants, activistes, anarchistes. Jusqu'au jour où les révélations d'E. Snowden (et bien d'autres à la suite) montrèrent à quel point la vie privée était menacée (elle l'est depuis 50 ans de capitalisme de surveillance), d'autant plus que les outils de communication des multinationales du numérique sont largement utilisés par les populations.

Les libertariens s'enivrèrent de cette soif de protection de nos correspondances. Ils y voyaient (et c'est toujours le cas) un point d'ancrage de leur idéologie capitaliste, promouvant une «liberté» contre l'État mais de fait soumise aux logiques débridées du marché. Dès lors, ceux qu'on appelle les crypto-anarchistes, firent feu de ce bois, en connectant un goût certain pour le solutionnisme technologique (blockchain et compagnie) et un modèle individualiste de communication entièrement chiffré où les crypto-monnaies remplissent le rôle central dans ce marché prétendu libre, mais ô combien producteur d'inégalités.

Alimentant le mélange des genres, certains analystes, encore très récemment, confondent allègrement les anarchistes et les crypto-anarchistes, pour mieux dénigrer l'importance que nous accordons à la légitimité sociale, solidaire et égalitaire des protocoles de communication basés sur le chiffrement. Or, ce sont autant de moyens d'expression et de mobilisation démocratique et ils occupent une place centrale dans les conditions de mobilisation politique.

Les groupes anarchistes figurent parmi les plus concernés, surtout parce que les logiques d'action et les idées qui y sont partagées sont de plus en plus insupportables aux yeux des gouvernements, qu'il s'agisse de dictatures, d'illibéralisme, ou de néofascisme. Pour ces adversaires, le simple fait d'utiliser des communications chiffrées (sauf quand il s'agit de protéger leurs corruptions et leurs perversions) est une activité suspecte. Viennent alors les moyens de coercition, de surveillance et de contrôle, la technopolice. Dans cette lutte qui semble sans fin, il faut néanmoins faire preuve de pondération autant que d'analyse critique. Bien souvent on se précipite sur des outils apparemment sûrs mais peu résilients. Gratter la couche d'incertitude ne consiste pas à décourager l'usage de ces outils mais montrer combien leur usage ne fait pas l'économie de mises en garde.

Dans le texte qui suit, issu de la plateforme d'information et de médias It's Going Down, l'auteur prend le parti de la prévention. Par exemple, ce n'est pas parce que le créateur du protocole Signal et co-fondateur de la Signal Foundation est aussi un anarchiste (quoique assez individualiste) que l'utilisation de Signal est un moyen fiable de communication pour un groupe anarchiste ou plus simplement militant. La convivialité d'un tel outil est certes nécessaire pour son adoption, mais on doit toujours se demander ce qui a été sacrifié en termes de failles de sécurité. Le même questionnement doit être adressé à tous les autres outils de communication chiffrée.

C'est à cette lourde tâche que s'attelle l'auteur de ce texte, et il ne faudra pas lui tenir rigueur de l'absence de certains protocoles tels Matrix ou XMPP. Certes, on ne peut pas aborder tous les sujets, mais il faut aussi lire cet article d'après l'expérience personnelle de l'auteur. Si Signal et Briar sont les objets centraux de ses préoccupations, son travail cherche surtout à produire une vulgarisation de concepts difficiles d'accès. C'est aussi l'occasion d'une mise au point actuelle sur nos rapports aux outils de communication chiffrée et la manière dont ces techniques et leurs choix conditionnent nos communications. On n'oubliera pas son message conclusif, fort simple : lorsqu'on le peut, mieux vaut éteindre son téléphone et rencontrer ses amis pour de vrai…

Framatophe / Christophe Masutti

Infrastructures numériques de communication pour les anarchistes (et tous les autres…)

— *Un aperçu détaillé et un guide des diverses applications qui utilisent le pair-à-pair, le chiffrement et Tor* —

Les applications de chat sécurisées avec chiffrement constituent une infrastructure numérique essentielle pour les anarchistes. Elles doivent donc être examinées de près. Signal est un outil de chiffrement sécurisé très utilisé par les anarchistes aujourd'hui. Au-delà des rumeurs complotistes, l'architecture de base et les objectifs de développement de Signal présentent certaines implications en termes de sécurité pour les anarchistes. Signal est un service de communication centralisé. La centralisation peut avoir des conséquences sur la sécurité, en particulier lorsque elle est mise en perspective avec l'éventail des menaces. D'autres applications de chat sécurisées, comme Briar et Cwtch, sont des outils de communication pair-à-pair qui, en plus d'être chiffrés comme Signal, font transiter tout le trafic par Tor (appelé aussi CPT pour communication Chiffrée en Pair-à-pair via Tor). Cette conception de communication sécurisée offre de grands avantages en termes de sécurité, d'anonymat et de respect de la vie privée, par rapport à des services plus courants tels que Signal, malgré quelques réserves. Cependant, les anarchistes devraient sérieusement envisager d'essayer et d'utiliser Briar et/ou Cwtch, pour pouvoir former une infrastructure de communication plus résiliente et plus sûre.

Malgré tout, la meilleure façon de communiquer en toute sécurité demeure le face à face.

Chhhhuuut...

Il est ici question des outils numériques qui permettent de communiquer en toute sécurité et en toute confidentialité. Pour bien commencer, il s'agit d'insister sur le fait que le moyen le plus sûr de communiquer reste une rencontre en face à face, à l'abri des caméras et hors de portée sonore d'autres personnes et appareils. Les anarchistes se promenaient pour discuter bien avant que les textos chiffrés n'existent, et ils devraient continuer à le faire aujourd'hui, à chaque fois que c'est possible.

Ceci étant dit, il est indéniable que les outils de communication numérique sécurisés font maintenant partie de notre infrastructure anarchiste. Peut-être que nous sommes nombreux à nous appuyer sur eux plus que nous ne le devrions, mais ils sont devenus incontournables pour se coordonner, collaborer et rester en contact. Puisque ces outils constituent une infrastructure indispensable, il est vital pour nous d'examiner et réévaluer constamment leur sécurité et leur aptitude à protéger nos communications contre nos adversaires.

Au cours des dix ou vingt dernières années, les anarchistes ont été les premiers à adopter ces outils et ces techniques de communication chiffrée. Ils ont joué un rôle majeur dans la banalisation et la diffusion de leur utilisation au sein de nos propres communautés, ou auprès d'autres communautés engagées dans la résistance et la lutte. Le texte qui suit a pour but de présenter aux anarchistes les nouveaux outils de communication chiffrée et sécurisée. Il s'agit de démontrer que nous devrions les adopter afin de renforcer la résilience et l'autonomie de notre infrastructure. Nous pouvons étudier les avantages de ces nouvelles applications, voir comment elles peuvent nous aider à échapper à la surveillance et à la répression – et par la suite les utiliser efficacement dans nos mouvements et les promouvoir plus largement.

Le plus simple est de présenter les nouvelles applications de chat sécurisé en les comparant avec celle que tout le monde connaît : Signal. Signal est de facto l'infrastructure de communication sécurisée de beaucoup d'utilisatrices, du moins en Amérique du Nord. Et de plus en plus, elle devient omniprésente en dehors des cercles anarchistes. Si vous lisez ceci, vous utilisez probablement Signal, et il y a de fortes chances que votre mère ou qu'un collègue de travail l'utilise également. L'utilisation de Signal a explosé en janvier 2021 (à tel point que le service a été interrompu pendant 24 heures), atteignant 40 millions d'utilisateurs quotidiens. Signal permet aux utilisateurs d'échanger très facilement des messages chiffrés. Il est issu d'un projet antérieur appelé TextSecure, qui permettait de chiffrer les messages SMS (les textos à l'ancienne, pour les baby zoomers qui nous lisent). TextSecure, et plus tard Signal, ont très tôt bénéficié de la confiance des anarchistes, en grande partie grâce au réseau de confiance IRL entre le développeur principal, Moxie Marlinspike, et d'autres anarchistes.

Au début de l'année 2022, Moxie a quitté Signal, ce qui a déclenché une nouvelle vague de propos alarmistes à tendance complotiste. Le PDG anarchiste de Signal a démissionné. Signal est neutralisé. Un article intitulé «Signal Warning», publié sur It's Going Down, a tenté de dissiper ces inquiétudes et ces hypothèses complotistes, tout en discutant de la question de savoir si les anarchistes peuvent encore «faire confiance» à Signal (ils le peuvent, avec des mises en garde comme toujours). L'article a réitéré les raisons pour lesquelles Signal est, en fait, tout à fait sûr et digne de confiance (il est minutieusement audité et examiné par des experts en sécurité).

Cependant, l'article a laissé entendre que le départ de Moxie établissait, à tout le moins, une piqûre de rappel sur la nécessité d'un examen critique et sceptique permanent de Signal, et qu'il en va de même pour tout outil ou logiciel tiers utilisé par les anarchistes.

> *« Maintenant que la couche de vernis est enlevée, notre capacité à analyser Signal et à évaluer son utilisation dans nos milieux peut s'affranchir des distorsions que la confiance peut parfois engendrer. Nous devons désormais considérer l'application et son protocole sous-jacent tels qu'ils sont : un code utilisé dans un ordinateur, avec tous*

> *les avantages et les inconvénients que cela comporte. On en est encore loin, et, à ce jour, on ne va même pas dans cette direction. Mais, comme tous les systèmes techniques, nous devons les aborder de manière sceptique et rationnelle »*

Signal continue de jouir d'une grande confiance, et aucune contre-indication irréfutable n'a encore été apportée en ce qui concerne la sécurité de Signal. Ce qui suit n'est pas un appel à abandonner Signal – Signal reste un excellent outil. Mais, étant donné son rôle prépondérant dans l'infrastructure anarchiste et l'intérêt renouvelé pour la question de savoir si nous pouvons ou devons faire confiance à Signal, nous pouvons profiter de cette occasion pour examiner de près l'application, son fonctionnement, la manière dont nous l'utilisons, et explorer les alternatives. Un examen minutieux de Signal ne révèle pas de portes dérobées secrètes (backdoors), ni de vulnérabilités béantes. Mais il révèle une priorité donnée à l'expérience utilisateur et à la rationalisation du développement par rapport aux objectifs de sécurité les plus solides. Les objectifs et les caractéristiques du projet Signal ne correspondent peut-être pas exactement à notre modèle de menace. Et en raison du fonctionnement structurel de Signal, les anarchistes dépendent d'un service centralisé pour l'essentiel de leurs communications sécurisées en ligne. Cela a des conséquences sur la sécurité, la vie privée et la fiabilité.

Il existe toutefois des alternatives développées en grande partie pour répondre spécifiquement à ces problèmes. Briar et Cwtch sont deux nouvelles applications de chat sécurisé qui, comme Signal, permettent également l'échange de messages chiffrés. Elles sont en apparence très proches de Signal, mais leur fonctionnement est très différent. Alors que Signal est un service de messagerie chiffrée, Briar et Cwtch sont des applications qui permettent l'échange de messages **C**hiffrés et en **P**air-à-pair via **T**or (CPT). Ces applications CPT et leur fonctionnement seront présentés en détail. Mais la meilleure façon d'expliquer leurs avantages (et pourquoi les anarchistes devraient s'intéresser à d'autres applications de chat sécurisées alors que nous avons déjà Signal) passe par une analyse critique approfondie de Signal.

Modèle de menace et avertissements

Avant d'entrer dans le vif du sujet, il est important de replacer cette discussion dans son contexte en définissant un modèle de menace pertinent. Dans le cadre de cette discussion, nos adversaires sont les forces de l'ordre au niveau national ou bien les forces de l'ordre locales qui ont un accès aux outils des forces de l'ordre nationale. Malgré le chiffrement de bout en bout qui dissimule le contenu des messages en transit, ces adversaires disposent de nombreuses ressources qui pourraient être utilisées pour découvrir ou perturber nos activités, nos communications ou nos réseaux afin de pouvoir nous réprimer. Il s'agit des ressources suivantes :

- Ils ont un accès facile aux sites de médias sociaux et à toutes autres informations publiques.
- Dans certains cas, ils peuvent surveiller l'ensemble du trafic internet du domicile d'une personne ciblée ou de son téléphone.
- Ils peuvent accéder à des données ou à des métadonnées « anonymisées » qui proviennent d'applications, d'opérateurs de téléphonique, de fournisseurs d'accès à Internet, etc.
- Ils peuvent accéder au trafic réseau collecté en masse à partir des nombreux goulots d'étranglement de l'infrastructure internet.
- Avec plus ou moins de succès, ils peuvent combiner, analyser et corréler ces données et ce trafic réseau afin de désanonymiser les utilisateurs, de cartographier les réseaux sociaux ou de révéler d'autres informations potentiellement sensibles sur des individus ou des groupes et sur leurs communications.
- Ils peuvent compromettre l'infrastructure de l'internet (FAI, fournisseurs de services, entreprises, développeurs d'applications) par la coercition ou le piratage[1].

1 Par le biais d'un hameçonnage ou d'une ruse

Le présent guide vise à atténuer les capacités susmentionnées de ces adversaires, mais il en existe bien d'autres qui ne peuvent pas être abordées ici :

- Ils peuvent infecter à distance les appareils des personnes ciblées avec des logiciels malveillants d'enregistrement de frappe au clavier et de pistage, dans des cas extrêmes.
- Ils peuvent accéder à des communications chiffrées par l'intermédiaire d'informateurs confidentiels ou d'agents infiltrés.
- Ils peuvent exercer de fortes pressions ou recourir à la torture pour contraindre des personnes à déverrouiller leur téléphone ou leur ordinateur ou à donner leurs mots de passe.
- Bien qu'ils ne puissent pas casser un système de chiffrement robuste dans un délai raisonnable, ils peuvent, en cas de saisie, être en mesure d'obtenir des données à partir d'appareils apparemment chiffrés grâce à d'autres vulnérabilités (par exemple, dans le système d'exploitation de l'appareil) ou de défaillances de la sécurité opérationnelle.

Toute méthode de communication sécurisée dépend fortement des pratiques de sécurité de l'utilisateur. Peu importe que vous utilisiez l'*Application de Chat Sécurisée Préférée d'Edward Snowden* ™ si votre adversaire a installé un enregistreur de frappe sur votre téléphone, ou si quelqu'un partage des captures d'écran de vos messages chiffrés sur Twitter, ou encore si votre téléphone a été saisi et n'est pas correctement sécurisé.

Une explication détaillée de la sécurité opérationnelle, de la culture de la sécurité, des concepts connexes et des meilleures pratiques dépasse le cadre de ce texte – cette analyse n'est qu'une *partie* de la sécurité opérationnelle pertinente pour le modèle de menace concerné. Vous devez envisager une politique générale de sécurité pour vous protéger contre la menace des infiltrés et des informateurs. Comment utiliser en toute sécurité des appareils, comme les téléphones et les ordinateurs portables, pour qu'ils ne puissent pas servir à monter un dossier s'ils sont saisis, et comment

adopter des bonnes habitudes pour réduire au minimum les données qui se retrouvent sur les appareils électroniques (rencontrez-vous face à face et laissez votre téléphone à la maison !)

La «cybersécurité» évolue rapidement : il y a une guerre d'usure entre les menaces et les développeurs d'applications. Les informations fournies ici seront peut-être obsolètes au moment où vous lirez ces lignes. Les caractéristiques ou la mise en œuvre des applications peuvent changer, qui invalident partiellement certains des arguments avancés ici (ou qui les renforcent). Si la sécurité de vos communications électroniques est cruciale pour votre sécurité, vous ne devriez pas vous croire sur parole n'importe quelle recommandation, ici ou ailleurs.

Perte de Signal

Illustration 1: Comment cela a commencé, et ce que c'est aujourd'hui...

Vous avez probablement utilisé Signal aujourd'hui. Et Signal ne pose pas vraiment de gros problèmes. Il est important de préciser que malgré les critiques qui suivent, l'objectif n'est pas d'inciter à la panique quant à l'utilisation de Signal. Il ne s'agit pas de supprimer l'application immédiatement, de brûler votre téléphone et de vous enfuir dans les bois. Cela dit, peut-être pourriez-vous le faire pour votre santé mentale, mais en tout cas pas seulement à cause de ce guide. Vous pourriez envisager de faire une petite randonnée au préalable.

Parution Framablog, le 11/04/2023 (traduction Framalang)

Une parenthèse pour répondre à certaines idées complotistes

Une rapide recherche sur DuckDuckGo (ou peut-être une recherche sur Twitter ? Je ne saurais dire) avec les termes « Signal CIA », donnera lieu à de nombreuses désinformations et théories complotistes à propos de Signal. Compte tenu de la nature déjà critique de ce guide et de l'importance d'avoir un avis nuancé, penchons-nous un peu sur ces théories.

La plus répandue nous dit que Signal aurait été développé secrètement par la CIA et qu'il serait donc *backdoorisé*. Par conséquent, la CIA (ou parfois la NSA) aurait la possibilité d'accéder facilement à tout ce que vous dites sur Signal en passant par leur porte dérobée secrète.

> « L'étincelle de vérité qui a embrasé cette théorie complotiste est la suivante : entre 2013 et 2016, les développeurs de Signal ont reçu un peu moins de 3 millions de dollars américains de financement de la part de l'Open Technology Fund (OTF). L'OTF était à l'origine un programme de Radio Free Asia, supervisé par l'Agence américaine pour les médias mondiaux (U. S. Agency for Global Media, USAGM – depuis 2019, l'OTF est directement financé par l'USAGM). L'USAGM est une « agence indépendante du gouvernement américain », qui promeut les intérêts nationaux des États-Unis à l'échelle internationale et qui est financée et gérée directement par le gouvernement américain. Donc ce dernier gère et finance USAGM/Radio Free Asia, qui finance l'OTF, qui a financé le développement de Signal (et Hillary Clinton était secrétaire d'État à l'époque !!) : c'est *donc* la CIA qui aurait créé Signal… »

L'USAGM (et tous ses projets tels que Radio Free Asia et l'OTF) promeut les intérêts nationaux américains en sapant ou en perturbant les gouvernements avec lesquels les États-Unis sont en concurrence ou en conflit. Outre la promotion de contre-feux médiatiques (via le soutien à une « presse libre et indépendante » dans ces pays), cela implique également la production d'outils pouvant être utilisés pour contourner la censure et résister aux « régimes oppressifs ».

Les bénéficiaires de la FTO sont connus et ce n'est un secret pour personne que l'objectif affiché de la FTO consiste à créer des outils pour subvertir les

régimes qui s'appuient fortement sur la répression en ligne, sur la surveillance généralisée et sur la censure massive de l'internet pour se maintenir au pouvoir (et que ces régimes sont ceux dont le gouvernement américain n'est pas fan). Comment et pourquoi cela se produit en relation avec des projets tels que Signal est clairement rapporté par des médias grand public tels que le Wall Street Journal. Des médias comme RT rapportent également ces mêmes informations hors contexte et en les embellissant de manière sensationnelle, ce qui conduit à ces théories complotistes.

Illustration 2: Le journaliste Kit Klarenburg se plaît à produire des articles farfelus sur Signal pour des médias tels que RT.

Signal est un logiciel open source, ce qui signifie que l'ensemble de son code est vérifié et examiné par des experts. C'est l'application-phare où tout le monde cherche une porte dérobée de la CIA. Or, en ce qui concerne la surveillance de masse, il est plus facile et plus efficace pour nos adversaires de dissimuler des dispositifs de surveillance dans des applications et des infrastructures internet fermées et couramment utilisées, avec la coopération d'entreprises complices. Et en termes de surveillance ciblée, il est plus facile d'installer des logiciels malveillants sur votre téléphone.

De nombreux projets de logiciels open-source, comme Signal, ont été financés par des moyens similaires. La FTO finance ou a financé de nombreux autres projets dont vous avez peut-être entendu parler : Tor (au sujet duquel il existe des théories complotistes similaires), K-9 Mail, NoScript, F-Droid, Certbot et Tails (qui compte des anarchistes parmi ses développeurs).

Ces financements sont toujours révélés de manière transparente. Il suffit de consulter la page des sponsors de Tails, où l'on peut voir que l'OTF est un ancien sponsor (et que son principal sponsor actuel est… le département d'État des États-Unis !) Les deux applications CPT dont il est question dans ce guide sont en partie financées par des sources similaires.

On peut débattre sans fin sur les sources de financement des projets open source qui renforcent la protection de la vie privée ou la résistance à la surveillance : conflits d'intérêts, éthique, crédibilité, développement de tels outils dans un contexte de géopolitique néolibérale… Il est bon de faire preuve de scepticisme et de critiquer la manière dont les projets sont financés, mais cela ne doit pas nous conduire à des théories complotistes qui obscurcissent les discussions sur leur sécurité dans la pratique. Signal a été financé par de nombreuses sources « douteuses » : le développement initial de Signal a été financé par la vente du projet précurseur (TextSecure) à Twitter, pour un montant inconnu. Plus récemment, Signal a bénéficié d'un prêt de 50 millions de dollars à taux zéro de la part du fondateur de WhatsApp, qui est aujourd'hui directeur général de la Signal Foundation. Il existe de nombreuses preuves valables qui expliquent pourquoi et comment Signal a été financé par une initiative des États-Unis visant à dominer le monde, mais elles ne suggèrent ni n'impliquent d'aucune façon l'existence d'une porte dérobée, impossible à dissimuler, conçue par la CIA pour cibler les utilisatrices de Signal.

– Alors, Signal c'est bien, en fait ?

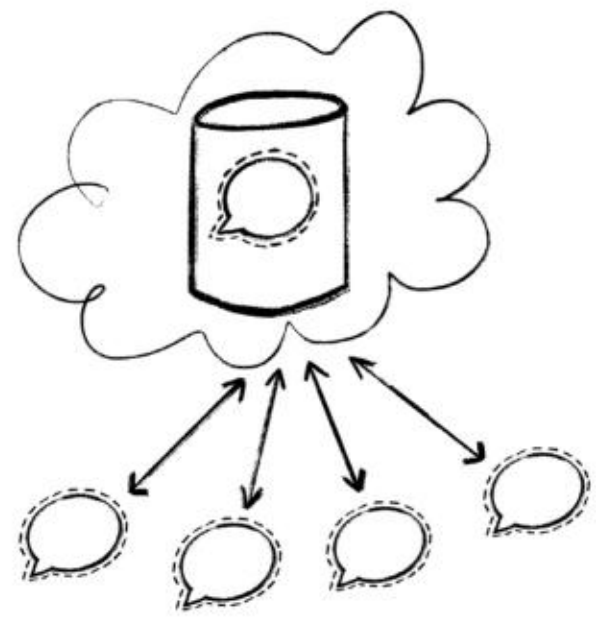
Si Signal n'est pas une opération secrète de la CIA, alors tout va bien, non ? Les protocoles de chiffrement de Signal sont communément considérés comme sûrs. En outre, Signal a l'habitude d'améliorer ses fonctionnalités et de remédier aux vulnérabilités en temps voulu, de manière transparente. Signal a réussi à rendre les discussions chiffrées de bout en bout suffisamment faciles pour devenir populaires. L'adoption généralisée de Signal est très certainement une bonne chose.

Thèses complotistes mises à part, les anarchistes ont toutefois de bonnes raisons d'être sceptiques à l'égard de Signal. Pendant le développement de Signal, Moxie a adopté une approche quelque peu dogmatique à l'égard de nombreux choix structurels et d'ingénierie logicielle. Ces décisions ont été prises intentionnellement (comme expliqué dans des articles de blog, lors de conférences ou dans divers fils de discussion sur GitHub) afin de faciliter l'adoption généralisée de Signal Messenger parmi les utilisateurs les moins

avertis, mais aussi pour préparer la croissance du projet à long terme, et ainsi permettre une évolution rationalisée tout en ajoutant de nouvelles fonctionnalités.

Les adeptes de la cybersécurité en ligne ont longtemps critiqué ces décisions comme étant des compromis qui sacrifient la sécurité, la vie privée ou l'anonymat de l'utilisateur au profit des propres objectifs de Moxie pour Signal. S'aventurer trop loin risquerait de nous entraîner sur le terrain des débats dominés par les mâles prétentieux du logiciel libre (si ce n'est pas déjà le cas). Pour être bref, les justifications de Moxie se résument à maintenir la compétitivité de Signal dans l'écosystème capitaliste de la Silicon Valley, axé sur le profit. Mise à part les stratégies de développement logiciel dans le cadre du capitalisme moderne, les caractéristiques concrètes de Signal les plus souvent critiquées sont les suivantes :

1. Signal s'appuie sur une infrastructure de serveurs centralisée.
2. Signal exige que chaque compte soit lié à un numéro de téléphone.
3. Signal dispose d'un système de paiement en crypto-monnaie intégré.



Peut-être que Moxie a eu raison et que ses compromis en valaient la peine : aujourd'hui, Signal est extrêmement populaire, l'application s'est massivement développée avec un minimum de problèmes de croissance, de nombreuses nouvelles fonctionnalités (à la fois pour la convivialité et la sécurité) ont été facilement introduites, et elle semble être durable dans un avenir prévisible[2]. Mais l'omniprésence de Signal en tant qu'infrastructure anarchiste exige un examen minutieux de ces critiques, en particulier lorsqu'elles s'appliquent à nos cas d'utilisation et à notre modèle de menace dans un monde en mutation. Cet examen permettra d'expliquer comment

2 Cependant, Signal semble vraiment vouloir obtenir davantage de dons de la part des utilisateurs, malgré le prêt de 50 millions de dollars contracté par l'entreprise. ¯_(ツ)_/¯

les applications CPT comme Briar et Cwtch, qui utilisent une approche complètement différente de la communication sécurisée, nous apportent potentiellement plus de résilience et de sécurité.

Signal en tant que service centralisé

Signal est moins une application qu'un service. Signal (Open Whisper Systems/The Signal Foundation) fournit l'application Signal (que vous pouvez télécharger et exécuter sur votre téléphone ou votre ordinateur) et gère un serveur Signal[3]. L'application Signal ne peut rien faire en soi. Le serveur Signal fournit la couche de service en traitant et en relayant tous les messages envoyés et reçus via l'application Signal. C'est ainsi que fonctionnent la plupart des applications de chat. Discord, WhatsApp, iMessage, Instagram/Facebook Messenger et Twitter dms sont tous des services de communication centralisés, où vous exécutez une application sur votre appareil et où un serveur centralisé, exploité par un tiers, relaie les messages entre les individus. Une telle centralisation présente de nombreux avantages pour l'utilisateur : vous pouvez synchroniser vos messages et votre profil sur le serveur pour y accéder sur différents appareils ; vous pouvez envoyer un message à votre ami même s'il n'est pas en ligne et le serveur stockera le message jusqu'à ce que votre ami se connecte et le récupère ; les discussions de groupe entre plusieurs utilisateurs fonctionnent parfaitement, même si les utilisateurs sont en ligne ou hors ligne à des moments différents.

Signal utilise le chiffrement de bout en bout, ce qui signifie que le serveur Signal ne peut lire aucun de vos messages. Mais qu'il soit un service de communication centralisé a de nombreuses implications importantes en termes de sécurité et de fiabilité.

3 Au lieu d'un serveur physique unique, il s'agit en fait d'un énorme réseau de serveurs loués dans les datacenters d'Amazon un peu partout aux États-Unis – ce qui peut être résumé à un serveur Signal unique pour les besoins de notre discussion.

Le bureau de poste de Signal

Signal-en-tant-que-service est comparable à un service postal. Il s'agit d'un très bon service postal, comme il en existe peut-être quelque part en Europe. Dans cet exemple, le serveur Signal est un bureau de poste. Vous écrivez une lettre à votre ami et la scellez dans une enveloppe avec une adresse (disons que personne d'autre que votre ami ne peut ouvrir l'enveloppe – c'est le chiffrement). À votre convenance, vous déposez toutes les lettres que vous envoyez au bureau de poste Signal, où elles sont triées et envoyées aux différents amis auxquels elles sont destinées. Si un ami n'est pas là, pas de problème ! Le bureau de poste Signal conservera la lettre jusqu'à ce qu'il trouve votre ami à la maison, ou votre ami peut simplement la récupérer au bureau de poste le plus proche. Le bureau de poste Signal est vraiment bien (c'est l'Europe, hein !) et vous permet même de faire suivre votre courrier partout où vous souhaitez le recevoir.

Peut-être aurez-vous remarqué qu'un problème de sécurité potentiel se pose sur le fait de confier tout son courrier au bureau de poste Signal. Les enveloppes scellées signifient qu'aucun facteur ou employé ne peut lire vos lettres (le chiffrement les empêche d'ouvrir les enveloppes). Mais celles et ceux qui côtoient régulièrement leur facteur savent qu'il peut en apprendre beaucoup sur vous, simplement en traitant votre courrier : il sait de qui vous recevez des lettres, il connaît tous vos abonnements à des magazines, mais aussi quand vous êtes à la maison ou non, tous les différents endroits où vous faites suivre votre courrier et toutes les choses embarrassantes que vous commandez en ligne. C'est le problème d'un service centralisé qui s'occupe de tout votre courrier – je veux dire de vos messages !

Parution Framablog, le 11/04/2023 (traduction Framalang)

Les métadonnées, c'est pour toujours

Les informations que tous les employés du bureau de poste Signal connaissent sur vous et votre courrier sont des métadonnées. Les métadonnées sont des données… sur les données. Elles peuvent inclure des éléments tels que l'expéditeur et le destinataire d'un message, l'heure à laquelle il a été envoyé et le lieu où il a été distribué. Tout le trafic sur Internet génère intrinsèquement ce type de métadonnées. Les serveurs centralisés constituent un point d'entrée facile pour observer ou collecter toutes ces métadonnées, puisque tous les messages passent par un point unique. Il convient de souligner que l'exemple ci-dessus du bureau de poste Signal n'est qu'une métaphore pour illustrer ce que sont les métadonnées et pourquoi elles constituent une préoccupation importante pour les services de communication centralisés. Signal est en fait *extrêmement doué* pour minimiser ou masquer les métadonnées. Grâce à la magie noire du chiffrement et à une conception intelligente du logiciel, il y a très peu de métadonnées auxquelles le serveur Signal peut facilement accéder. Selon les propres termes de Signal :

> *« Les éléments que nous ne stockons pas comprennent tout ce qui concerne les contacts d'un utilisateur (tels que les contacts eux-mêmes, un hachage des contacts, ou toute autre information dérivée sur les contacts), tout ce qui concerne les groupes d'un utilisateur (les groupes auxquels il appartient, leur nombre, les listes de membres des groupes, etc.), ou tout enregistrement des personnes avec lesquelles un utilisateur a communiqué. »*

Il n'existe que deux parties de métadonnées connues pour être stockées de manière persistante, et qui permettent de savoir :

- si un numéro de téléphone est enregistré auprès d'un compte Signal
- la dernière fois qu'un compte Signal a été connecté au serveur.

C'est une bonne chose ! En théorie, c'est tout ce qu'un employé curieux du bureau de poste Signal peut savoir sur vous. Mais cela est dû, en partie, à l'approche « Moi, je ne le vois pas » du serveur lui-même. Dans une certaine

mesure, nous devons croire sur parole ce que le serveur Signal prétend faire…

Bien obligés de faire confiance

Tout comme l'application Signal sur votre téléphone ou votre ordinateur, le serveur Signal est également basé sur du code principalement[4] open source. Il est donc soumis à des contrôles similaires par des experts en sécurité. Cependant, il y a une réalité importante et inévitable à prendre en compte : nous sommes obligés de croire que le serveur de Signal exécute effectivement le même code open source que celui qui est partagé avec nous. Il s'agit là d'un problème fondamental lorsque l'on se fie à un serveur centralisé géré par une tierce partie.

« Nous ne collectons ni ne stockons aucune information sensible sur nos utilisateurs, et cela ne changera jamais. » (blog de Signal)

En tant que grande association à but non lucratif, Signal ne peut pas systématiquement se soustraire aux ordonnances ou aux citations à comparaître qui concerne les données d'utilisateurs. Signal dispose même d'une page sur son site web qui énumère plusieurs citations à comparaître et les réponses qu'elle y a apportées. Mais rappelons-nous des deux types de métadonnées stockées par le serveur Signal qui peuvent être divulguées :

4 Récemment, Signal a choisi de fermer une partie du code de son serveur, soi-disant pour lui permettre de lutter contre le spam sur la plateforme. Cela signifie que désormais, une petite partie du code du serveur Signal n'est pas partagée publiquement. Ce changement dénote également une augmentation, bien qu'extrêmement minime, de la collecte de métadonnées côté serveur, puisqu'elle est nécessaire pour faciliter la lutte efficace contre le spam, même de manière basique. Il n'y a aucune raison de suspecter une manœuvre malveillante, mais il est important de noter qu'il s'agit là encore d'une décision stratégique qui sacrifie les questions de sécurité dans l'intérêt de l'expérience de l'utilisateur.

Account	Responsive Information in Signal's Possession
[redacted]	Last connection date: 1634169600000 (unix millis) Account created: 1606866784432 (unix millis)

Illustration 3: Les réponses de Signal indiquent la date de la dernière connexion, la date de création du compte et le numéro de téléphone (caviardé)

À l'heure où nous écrivons ces lignes, il n'y a aucune raison de douter de ce qui a été divulgué, mais il faut noter que Signal se conforme également à des procédures-bâillon qui l'empêchent de révéler qu'elle a reçu une citation à comparaître ou un mandat. Historiquement, Signal se bat contre ces injonctions, mais nous ne pouvons savoir ce qui nous est inconnu, notamment car Signal n'emploie pas de *warrant canary*, ces alertes en creux qui annoncent aux utilisateurs qu'aucun mandat spécifique n'a été émis pour le moment [une manière détournée d'annoncer des mandats dans le cas où cette annonce disparaisse, NDLR]. Il n'y a aucune raison sérieuse de penser que Signal a coopéré avec les autorités plus fréquemment qu'elle ne le prétend, mais il y a trois scénarios à envisager :

1. Des modifications de la loi pourraient contraindre Signal, sur demande, à collecter et à divulguer davantage d'informations sur ses utilisateurs et ce, à l'insu du public.
2. Signal pourrait être convaincu par des arguments éthiques, moraux, politiques ou patriotiques de coopérer secrètement avec des adversaires.
3. Signal pourrait être infiltré ou piraté par ces adversaires afin de collecter secrètement davantage de données sur les utilisateurs ou afin que le peu de métadonnées disponibles puissent leur être plus facilement transmis.

Tous ces scénarios sont concevables, ils ont des précédents historiques ailleurs, mais ils ne sont pas forcément probables ni vraisemblables. En raison de la

«magie noire du chiffrement» susmentionnée et de la complexité des protocoles des réseaux, même si le serveur Signal se retrouvait altéré pour devenir malveillant, il y aurait toujours une limite à la quantité de métadonnées qui peuvent être collectées sans que les utilisatrices ou les observateurs ne s'en aperçoivent. Cela n'équivaudrait pas, par exemple, à ce que le bureau de poste Signal laisse entrer un espion (par une véritable « porte dérobée installée par la CIA ») qui viendrait lire et enregistrer toutes les métadonnées de chaque message qui passe par ce bureau. Des changements dans les procédures et le code pourraient avoir pour conséquence que des quantités faibles, mais toujours plus importantes de métadonnées (ou autres informations), deviennent facilement disponibles pour des adversaires, et cela pourrait se produire sans que nous en soyons conscients. Il n'y a pas de raison particulière de se méfier du serveur Signal à ce stade, mais les anarchistes doivent évaluer la confiance qu'ils accordent à un tiers, même s'il est historiquement digne de confiance comme Signal.

Illustration 4: Intelligence Community Comprehensive National Initiative Data Center (Utah)

Mégadonnées

De nombreux et puissants ennemis sont capables d'intercepter et de stocker des quantités massives de trafic sur Internet. Il peut s'agir du contenu de messages non chiffré, mais avec l'utilisation généralisée du

chiffrement, ce sont surtout des métadonnées et l'activité internet de chacun qui sont ainsi capturées et stockées.

Nous pouvons choisir de croire que Signal n'aide pas activement nos adversaires à collecter des métadonnées sur les communications des utilisateurs et utilisatrices, mais nos adversaires disposent de nombreux autres moyens pour collecter ces données : la coopération avec des entreprises comme Amazon ou Google (Signal est actuellement hébergé par Amazon Web Services), ou bien en ciblant ces hébergeurs sans leur accord, ou tout simplement en surveillant le trafic internet à grande échelle.

Les métadonnées relatives aux activités en ligne sont également de plus en plus accessibles à des adversaires moins puissants, ceux qui peuvent les acheter, sous forme brute ou déjà analysées, à des courtiers de données, qui à leur tour les achètent ou les acquièrent via des sociétés spécialisées dans le développement d'applications ou les fournisseurs de téléphones portables.

Les métadonnées ainsi collectées donnent lieu à des jeux de données volumineux et peu maniables qui étaient auparavant difficiles à analyser. Mais de plus en plus, nos adversaires (et même des organisations ou des journalistes) peuvent s'emparer de ces énormes jeux de données, les combiner et leur appliquer de puissants outils d'analyse algorithmique pour obtenir des corrélations utiles sur des personnes ou des groupes de personnes (c'est ce que l'on appelle souvent le « Big Data »). Même l'accès à de petites quantités de ces données et à des techniques d'analyse rudimentaires permet de désanonymiser des personnes et de produire des résultats utiles.

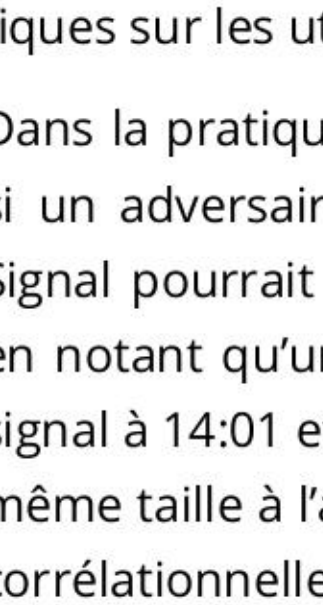
Histoire des messages de Jean-Michel

Voici un scénario fictif qui montre comment l'analyse du trafic et la corrélation des métadonnées peuvent désanonymiser un utilisateur de Signal.

Imaginez un cinéphile assidu, mais mal élevé, disons Jean-Michel, qui passe son temps à envoyer des messages via Signal pendant la projection. Les reflets de l'écran de son téléphone (Jean-Michel n'utilise pas le mode sombre) gênent tout le monde dans la salle. Mais la salle est suffisamment sombre pour que Lucie, la gérante qui s'occupe de tout, ne puisse pas savoir exactement qui envoie des messages en permanence. Lucie commence alors à collecter toutes les données qui transitent par le réseau Wi-Fi du cinéma, à la recherche de connexions au serveur Signal. Les connexions fréquentes de Jean-Michel à ce serveur apparaissent immédiatement. Lucie est en mesure d'enregistrer l'adresse MAC (un identifiant unique associé à chaque téléphone) et peut confirmer que c'est le même appareil qui utilise fréquemment Signal sur le réseau Wi-Fi du cinéma pendant les heures de projection. Lucie est ensuite en mesure d'établir une corrélation avec les relevés de transactions par carte bancaire de la billetterie et d'identifier une carte qui achète toujours des billets de cinéma à l'heure où l'appareil utilise fréquemment Signal (le nom du détenteur de la carte est également révélé : Jean-Michel). Avec l'adresse MAC de son téléphone, son nom et sa carte de crédit, Lucie peut fournir ces informations à un détective privé véreux, qui achètera l'accès à de vastes jeux de données collectées par des courtiers de données (auprès des fournisseurs de téléphones portables et des applica-

tions mobiles), et déterminera un lieu où le même téléphone portable est le plus fréquemment utilisé. Outre le cinéma, il s'agit du domicile de Jean-Michel. Lucie se rend chez Jean-Michel de nuit et fait exploser sa voiture (car la salle de cinéma était en fait une couverture pour les Hell's Angels du coin).

Des métadonnées militarisées



> « Nous tuons des gens en nous appuyant sur des métadonnées… mais ce n'est pas avec les métadonnées que nous les tuons ! » (dit avec un sourire en coin, les rires fusent dans l'assistance) – Général Michael Hayden, *ancien Directeur de la NSA (1999-2005) et Directeur de la CIA (2006-2009).*

Sur un Internet où les adversaires ont les moyens de collecter et d'analyser d'énormes volumes de métadonnées et de données de trafic, l'utilisation de serveurs centralisés peut s'avérer dangereuse. Ils peuvent facilement cibler les appareils qui communiquent avec le serveur Signal en surveillant le trafic internet en général, au niveau des fournisseurs d'accès, ou éventuellement aux points de connexion avec le serveur lui-même. Ils peuvent ensuite essayer d'utiliser des techniques d'analyse pour révéler des éléments spécifiques sur les utilisatrices individuelles ou leurs communications via Signal.

Dans la pratique, cela peut s'avérer difficile. Vous pourriez vous demander si un adversaire qui observe tout le trafic entrant et sortant du serveur Signal pourrait déterminer que vous et votre ami échangez des messages en notant qu'un message a été envoyé de votre adresse IP au serveur de signal à 14:01 et que le serveur de Signal a ensuite envoyé un message de la même taille à l'adresse IP de votre ami à 14:02. Heureusement, une analyse corrélationnelle très simple comme celle-ci n'est pas possible en raison de l'importance du trafic entrant et sortant en permanence du serveur de Signal et de la manière dont ce trafic est traité à ce niveau. C'est moins vrai pour les appels vidéo/voix où les protocoles internet utilisés rendent plus plausible l'analyse corrélationnelle du trafic pour déterminer qui a appelé qui. Il n'en reste pas moins que la tâche reste très difficile pour qui observe

l'ensemble du trafic entrant et sortant du serveur de Signal afin d'essayer de déterminer qui parle à qui. Peut-être même que cette tâche est impossible à ce jour.

Pourtant, les techniques de collecte de données et les outils d'analyse algorithmique communément appelés « Big Data » deviennent chaque jour plus puissants. Nos adversaires sont à la pointe de cette évolution. L'utilisation généralisée du chiffrement dans toutes les télécommunications a rendu l'espionnage illicite traditionnel beaucoup moins efficace et, par conséquent, nos adversaires sont fortement incités à accroître leurs capacités de collecte et d'analyse des métadonnées. Ils le disent clairement : « Si vous avez suffisamment de métadonnées, vous n'avez pas vraiment besoin du contenu »[5]. Ils tuent des gens sur la base de métadonnées.

Ainsi, bien qu'il ne soit peut-être pas possible de déterminer avec certitude une information aussi fine que « qui a parlé à qui à un moment précis », nos adversaires continuent d'améliorer à un rythme soutenu leur aptitude à extraire, à partir des métadonnées, toutes les informations sensibles qu'ils peuvent. Certaines fuites nous apprennent régulièrement qu'ils étaient en possession de dispositifs de surveillance plus puissants ou plus invasifs qu'on ne le pensait jusqu'à présent. Il n'est pas absurde d'en déduire que leurs possibilités sont bien étendues que ce que nous en savons déjà.

Signal est plus vulnérable à ce type de surveillance et d'analyse parce qu'il s'agit d'un service centralisé. Le trafic de Signal sur Internet n'est pas difficile à repérer et le serveur Signal est un élément central facile à observer ou qui permet de collecter des métadonnées sur les utilisateurs et leurs activités. D'éventuelles compromissions de Signal, des modifications dans les conditions d'utilisation ou encore des évolutions législatives pourraient faciliter les analyses de trafic et la collecte des métadonnées de Signal, pour que nos adversaires puissent les analyser.

Les utilisateurs individuels peuvent mettre en œuvre certaines mesures de protection, comme faire transiter leur trafic Signal par Tor ou un VPN, mais cela peut s'avérer techniquement difficile à mettre en œuvre et propice aux

5 Stewart Baker, Conseiller Général de la NSA.

erreurs. Tout effort visant à rendre plus difficile la liaison d'une utilisatrice de Signal à une personne donnée est également rendu complexe par le fait que Signal exige de chaque compte qu'il soit lié à un numéro de téléphone (nous y reviendrons plus tard).

Dépendances et points faibles

Un service centralisé signifie non seulement qu'il existe un point de contrôle central, mais aussi un point faible unique : Signal ne fonctionne pas si le serveur Signal est en panne. Il est facile de l'oublier jusqu'au jour où cela se produit. Signal peut faire une erreur de configuration ou faire face à un afflux de nouveaux utilisateurs à cause d'un tweet viral et tout à coup Signal ne fonctionne carrément plus.

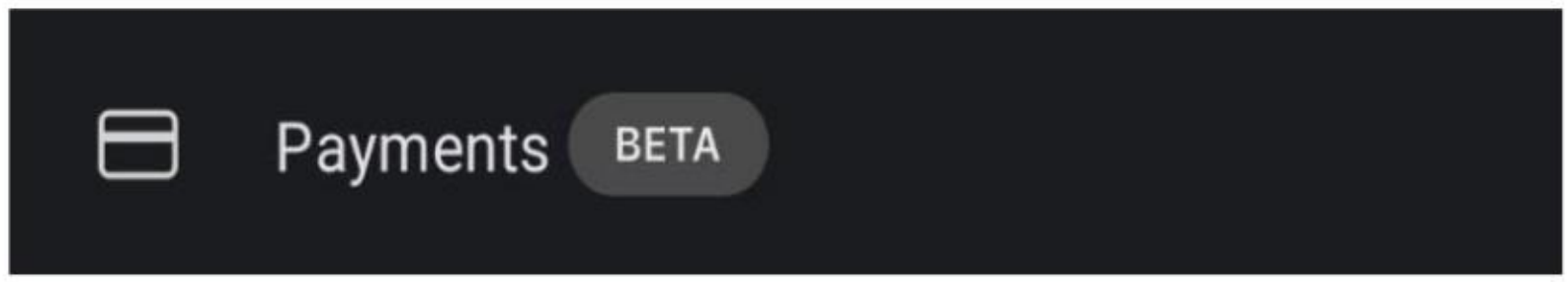
Signal pourrait également tomber en panne à la suite d'actions intentées par un adversaire. Imaginons une attaque par déni de service (ou tout autre cyberattaque) qui viserait à perturber le fonctionnement de Signal lors d'une rébellion massive. Les fournisseurs de services qui hébergent le serveur Signal pourraient également décider de le mettre hors service sans avertissement pour diverses raisons : sous la pression d'un adversaire, sous une pression politique, sous la pression de l'opinion publique ou pour des raisons financières.

Des adversaires qui contrôlent directement l'infrastructure Internet locale peuvent tout aussi bien perturber un service centralisé. Lorsque cela se produit dans certains endroits, Signal réagit en général rapidement en mettant en œuvre des solutions de contournement ou des modifications créatives, ce qui donne lieu à un jeu du chat et de la souris entre Signal et

l'État qui tente de bloquer Signal dans la zone qu'il contrôle. Une fois encore, il s'agit de rester confiant dans le fait que les intérêts de Signal s'alignent toujours sur les nôtres lorsqu'un adversaire tente de perturber Signal de cette manière dans une région donnée.

Cryptocontroverse

En 2021, Signal a entrepris d'intégrer un nouveau système de paiement dans l'application en utilisant la crypto-monnaie MobileCoin. Si vous ne le saviez pas, vous n'êtes probablement pas le seul, mais c'est juste là, sur la page de vos paramètres.



MobileCoin est une crypto-monnaie peu connue, qui privilégie la protection de la vie privée, et que Moxie a également contribué à développer. Au-delà des débats sur les systèmes pyramidaux de crypto-monnaies, le problème est qu'en incluant ce type de paiements dans l'application, Signal s'expose à des vérifications de légalité beaucoup plus approfondies de la part des autorités. En effet, les crypto-monnaies étant propices à la criminalité et aux escroqueries, le gouvernement américain se préoccupe de plus en plus d'encadrer leur utilisation. Signal n'est pas une bande de pirates, c'est une organisation à but non lucratif très connue. Elle ne peut pas résister long-temps aux nouvelles lois que le gouvernement américain pourrait adopter pour réglementer les crypto-monnaies.

Si les millions d'utilisateurs de Signal utilisaient effectivement MobileCoin pour leurs transactions quotidiennes, il ne serait pas difficile d'imaginer que Signal fasse l'objet d'un plus grand contrôle de la part de l'organisme fédéral américain de réglementation (la Securities and Exchange Commis-sion) ou autres autorités. Le gouvernement n'aime pas les systèmes de chiffrement, mais il aime encore moins les gens ordinaires qui paient pour de la drogue ou échappent à l'impôt. Imaginez un scénario dans lequel les

cybercriminels s'appuieraient sur Signal et MobileCoin pour accepter les paiements des victimes de rançongiciels. Cela pourrait vraiment mettre le feu aux poudres et dégrader considérablement l'image de Signal en tant qu'outil de communication fiable et sécurisé.

Un mouchard en coulisses

Cette frustration devrait déjà être familière aux anarchistes qui utilisent Signal. En effet, les comptes Signal nécessitent un numéro de téléphone. Quel que soit le numéro de téléphone auquel un compte est lié, il est également divulgué à toute personne avec laquelle vous vous connectez sur Signal. En outre, il est très facile de déterminer si un numéro de téléphone donné est lié à un compte Signal actif.

Il existe des solutions pour contourner ce problème, mais elles impliquent toutes d'obtenir un numéro de téléphone qui n'est pas lié à votre identité afin de pouvoir l'utiliser pour ouvrir un compte Signal. En fonction de l'endroit où vous vous trouvez, des ressources dont vous disposez et de votre niveau de compétence technique, cette démarche peut s'avérer peu pratique, voire bien trop contraignante. Signal ne permet pas non plus d'utiliser facilement plusieurs comptes à partir du même téléphone ou ordinateur. Configurer plusieurs comptes Signal pour différentes identités, ou pour les associer à différents projets, devient une tâche énorme, d'autant plus que vous avez besoin d'un numéro de téléphone distinct pour chacun d'entre eux.

Pour des adversaires qui disposent de ressources limitées, il est toujours assez facile d'identifier une personne sur la base de son numéro de téléphone. En outre, s'ils se procurent un téléphone qui n'est pas correctement éteint ou chiffré, ils ont accès aux numéros de téléphone des contacts et des membres du groupe. Il s'agit évidemment d'un problème de sécurité opérationnelle qui dépasse le cadre de Signal, mais le fait que Signal exige que chaque compte soit lié à un numéro de téléphone accroît considérablement la possibilité de pouvoir cartographier le réseau, ce qui entraîne des conséquences dommageables.

On ignore si Signal permettra un jour l'existence de comptes sans qu'ils soient liés à un numéro de téléphone ou à un autre identifiant de la vie réelle. On a pu dire qu'ils ne le feront jamais, ou que le projet est en cours mais perdu dans les limbes[6]. Quoi qu'il en soit, il s'agit d'un problème majeur pour de nombreux cas d'utilisation par des anarchistes.

6 Pardonnez ce pavé sur les numéros de téléphone. Bien que, dans les fils de questions-réponses sur Github, Signal ait mentionné être ouvert à l'idée de ne plus exiger de numéro de téléphone, il n'y a pas eu d'annonce officielle indiquant qu'il s'agissait d'une fonctionnalité à venir et en cours de développement. Il semblerait que l'un des problèmes liés à l'abandon des numéros de téléphone pour l'enregistrement soit la rupture de la compatibilité avec les anciens comptes Signal, en raison de la manière dont les choses étaient mises en œuvre à l'époque de TextSecure. C'est paradoxal, étant donné que le principal argument de Moxie contre les modèles décentralisés est qu'il serait trop difficile d'aller vite – il y a trop de travail à faire avant de pouvoir mettre en œuvre de nouvelles fonctionnalités. Et pourtant, Signal est bloqué par un problème très embarrassant à cause d'un ancien code concernant l'enregistrement des comptes auprès d'un serveur central. Moxie a également expliqué que les numéros de téléphone sont utilisés comme point de référence de votre identité dans Signal pour faciliter la préservation de votre « graphe social ». Au lieu que Signal ait à maintenir une sorte de réseau social en votre nom, tous vos contacts sont identifiés par leur numéro de téléphone dans le carnet d'adresses de votre téléphone, ce qui facilite le maintien et la conservation de votre liste de contacts lorsque vous passez d'autres applications à Signal, ou si vous avez un nouveau téléphone, ou que sais-je encore. Pour Moxie, il semble qu'avoir à « redécouvrir » ses contacts régulièrement et en tout lieu soit un horrible inconvénient. Pour les anarchistes, cela devrait être considéré comme un avantage d'avoir à maintenir intentionnellement notre « graphe social » basé sur nos affinités, nos désirs et notre confiance. Nous devrions constamment réévaluer et réexaminer qui fait partie de notre « graphe social » pour des raisons de sécurité (est-ce que je fais encore confiance à tous ceux qui ont mon numéro de téléphone d'il y a 10 ans ?) et pour encourager des relations sociales intentionnelles (suis-je toujours ami avec tous ceux qui ont mon numéro de téléphone d'il y a 10 ans ?). Dernière anecdote sur l'utilisation des numéros de téléphone par Signal : Signal dépense plus d'argent pour la vérification des numéros de téléphone que pour l'hébergement du reste du service : 1 017 990 dollars pour Twillio, le service de vérification des numéros de téléphone, contre 887 069 dollars pour le service d'hébergement web d'Amazon.

Parution Framablog, le 11/04/2023 (traduction Framalang)

Vers une pratique plus stricte

Après avoir longuement discuté de Signal, il est temps de présenter quelques alternatives qui répondent à certains de ces problèmes : Briar et Cwtch. Briar et Cwtch sont, par leur conception même, extrêmement résistants aux métadonnées et offrent un meilleur anonymat. Ils sont également plus résilients, car ils ne disposent pas de serveur central ou de risque de défaillance en un point unique. Mais ces avantages ont un coût : une plus grande sécurité s'accompagne de quelques bizarreries d'utilisation auxquelles il faut s'habituer.

Rappelons que Cwtch et Briar sont des applications CPT :

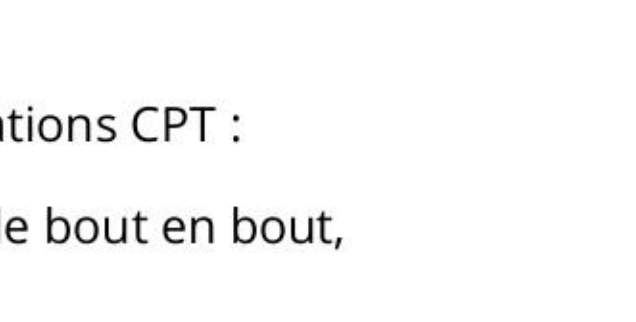
C : comme Signal, les messages sont chiffrés de bout en bout,

P : pour la transmission en pair-à-pair,

T : les identités et les activités des utilisatrices sont anonymisées par l'envoi de tous messages via Tor.

Parce qu'elles partagent une architecture de base, elles ont de nombreuses fonctionnalités et caractéristiques communes.

Pair-à-pair



Signal est un service de communication centralisé, qui utilise un serveur pour relayer et transmettre chaque message que vous envoyez à vos amis. Les problèmes liés à ce modèle ont été longuement discutés ! Vous êtes probablement lassés d'en entendre parler maintenant. Le P de CPT signifie pair-à-pair. Dans un tel modèle, vous échangez des messages directement avec vos amis. Il n'y a pas de serveur central intermédiaire géré par un tiers. Chaque connexion directe s'appuie uniquement sur l'infrastructure plus large d'Internet.

Vous vous souvenez du bureau de poste Signal ? Avec un modèle pair-à-pair, vous ne passez pas par un service postal pour traiter votre courrier. Vous remettez vous-même chaque lettre directement à votre ami. Vous l'écrivez, vous la scellez dans une enveloppe (chiffrement de bout en bout), vous la mettez dans votre sac et vous traversez la ville à vélo pour la remettre en main propre.

La communication pair-à-pair offre une grande résistance aux métadonnées. Il n'y a pas de serveur central qui traite chaque message auquel des métadonnées peuvent être associées. Il est ainsi plus difficile pour les adversaires de collecter en masse des métadonnées sur les communications que de surveiller le trafic entrant et sortant de quelques serveurs centraux connus. Il n'y a pas non plus de point de défaillance unique. Tant qu'il existe une route sur Internet pour que vous et votre amie puissiez vous connecter, vous pouvez discuter.

Synchronisation

Il y a un point important à noter à propos de la communication pair-à-pair : comme il n'y a pas de serveur central pour stocker et relayer les messages, vous et votre ami devez tous deux avoir l'application en cours d'exécution et avoir une connexion en ligne pour échanger des messages. C'est pourquoi ces applications CPT privilégient la communication synchrone. Que se passe-t-il si vous traversez la ville à vélo pour remettre une lettre à vos amis et… qu'ils ne sont pas chez eux ? Si vous voulez vraiment faire du pair-à-pair, vous devez remettre la lettre en main propre. Vous ne pouvez pas simplement la déposer quelque part (il n'y a pas d'endroit assez sûr !). Vous devez être en mesure de joindre directement vos amis pour leur transmettre le message – c'est l'aspect synchrone de la communication de pair à pair.

Un appel téléphonique est un bon exemple de communication synchrone. Vous ne pouvez pas avoir de conversation téléphonique si vous n'êtes pas

tous les deux au téléphone en même temps. Mais qui passe encore des appels téléphoniques ? De nos jours, nous sommes beaucoup plus habitués à un mélange de messagerie synchrone et asynchrone, et les services de communication centralisés comme Signal sont parfaits pour cela. Il arrive que vous et votre ami soyez tous deux en ligne et échangiez des messages en temps réel, mais le plus souvent, il y a un long décalage entre les messages envoyés et reçus. Au moins pour certaines personnes… Vous avez peut-être, en ce moment, votre téléphone allumé, à portée de main à tout moment. Vous répondez immédiatement à tous les messages que vous recevez, à toute heure de la journée. Donc toute communication est et doit être synchrone… si vous êtes dans ce cas, vous vous reconnaîtrez certainement.

Le passage à la communication textuelle synchrone peut être une vraie difficulté au début. Certaines lectrices et lecteurs se souviendront peut-être de ce que c'était lorsque on utilisait AIM, ICQ ou MSN Messenger (si vous vous en souvenez, vous avez mal au dos). Vous devez savoir si la personne est réellement en ligne ou non. Si la personne n'est pas en ligne, vous ne pouvez pas envoyer de messages pour plus tard. Si l'une d'entre vous ne laisse pas l'application en ligne en permanence, vous devez prendre l'habitude de prévoir des horaires pour discuter. Cela peut s'avérer très agréable. Paradoxalement, la normalisation de la communication asynchrone a entraîné le besoin d'être toujours en ligne et réactif. La communication synchrone encourage l'intentionnalité de nos communications, en les limitant aux moments où nous sommes réellement en ligne, au lieu de s'attendre à être en permanence plus ou moins disponibles.

Une autre conséquence importante de la synchronisation des connexions pair-à-pair est qu'elle peut rendre les discussions de groupe un peu bizarres. Que se passe-t-il si tous les membres du groupe ne sont pas en ligne au même moment ? Briar et Cwtch gèrent ce problème différemment, un sujet abordé plus bas, dans les sections relatives à chacune de ces applications.

Tor

Bien que la communication pair-à-pair soit très résistante aux métadonnées et évite d'autres écueils liés à l'utilisation d'un serveur central, elle ne protège pas à elle seule contre la collecte de métadonnées et l'analyse du trafic dans le cadre du « Big Data ». Tor est un très bon moyen de limiter ce problème, et les applications CPT font transiter tout le trafic par Tor.

Si vous êtes un·e anarchiste et que vous lisez ces lignes, vous devriez déjà connaître Tor et la façon dont il peut être utilisé pour assurer l'anonymat (ou plutôt la non-associativité). Les applications CPT permettent d'établir des connexions directes pair-à-pair pour échanger des messages par l'intermédiaire de Tor. Il est donc beaucoup plus difficile de vous observer de manière ciblée ou de vous pister et de corréler vos activités sur Internet, de savoir qui parle à qui ou de faire d'autres analyses utiles. Il est ainsi bien plus difficile de relier un utilisateur donné d'une application CPT à une identité réelle. Tout ce qu'un observateur peut voir, c'est que vous utilisez Tor.

Tor n'est pas un bouclier à toute épreuve et des failles potentielles ou des attaques sur le réseau Tor sont possibles. Entrer dans les détails du fonctionnement de Tor prendrait trop de temps ici, et il existe de nombreuses ressources en ligne pour vous informer. Il est également important de comprendre les mises en garde générales en ce qui concerne l'utilisation de Tor. Comme Signal, le trafic Tor peut également être altéré par des interférences au niveau de l'infrastructure Internet, ou par des attaques par déni de service qui ciblent l'ensemble du réseau Tor. Toutefois, il reste beaucoup plus difficile pour un adversaire de bloquer ou de perturber Tor que de mettre hors service ou de bloquer le serveur central de Signal.

Il faut souligner que dans certaines situations, l'utilisation de Tor peut vous singulariser. Si vous êtes la seule à utiliser Tor dans une région donnée ou à un moment donné, vous pouvez vous faire remarquer. Mais il en va de même pour toute application peu courante. Le fait d'avoir Signal sur votre téléphone vous permet également de vous démarquer. Plus il y a de gens qui utilisent Tor, mieux c'est, et s'il est utilisé correctement, Tor offre une meilleure protection contre les tentatives d'identification des utilisateurs que s'il n'était pas utilisé. Les applications CPT utilisent Tor pour tout, par défaut, de manière presque infaillible.

Pas de téléphone, pas de problème

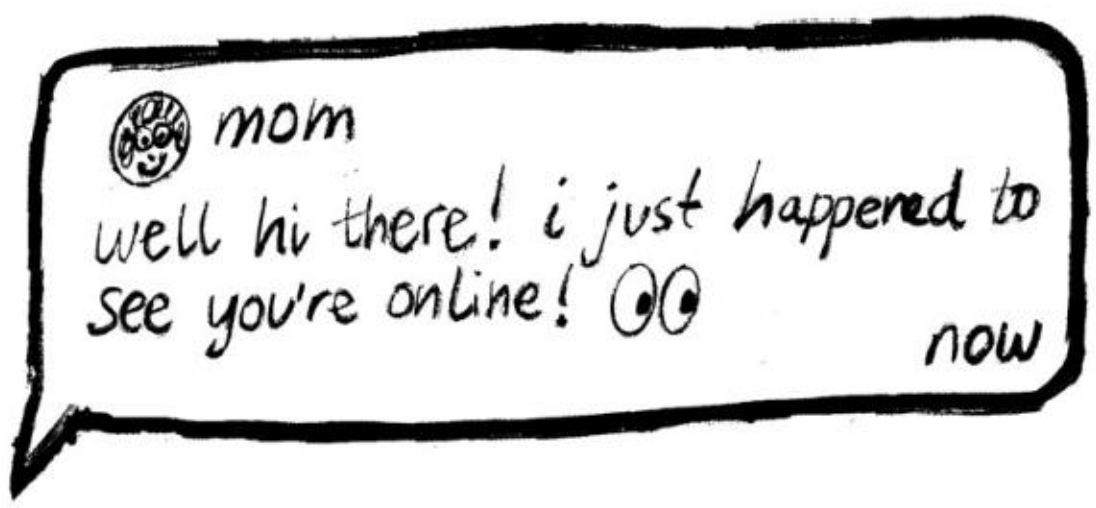
Un point facilement gagné pour les deux applications CPT présentées ici : elles ne réclament pas de numéro de téléphone pour l'enregistrement d'un compte. Votre compte est créé localement sur votre appareil et l'identifiant du compte est une très longue chaîne de caractères aléatoires que vous partagez avec vos amis pour qu'ils deviennent des contacts. Vous pouvez facilement utiliser ces applications sur un ordinateur, sur un téléphone sans carte SIM ou sur un téléphone mais sans lien direct avec votre numéro de téléphone.

Mises en garde générales concernant les applications CPT

La fuite de statut

Les communications pair-à-pair laissent inévitablement filtrer un élément particulier de métadonnées : le statut en ligne ou hors ligne d'un utilisateur. Toute personne que vous avez ajoutée en tant que contact ou à qui vous avez confié votre identifiant (ou tout adversaire ayant réussi à l'obtenir) peut savoir si vous êtes en ligne ou hors ligne à un moment donné. Cela ne s'applique pas vraiment à notre modèle de menace, sauf si vous êtes particulièrement négligent avec les personnes que vous ajoutez en tant que

contact, ou pour des événements publics qui affichent les identifiants d'utilisateurs. Mais cela vaut la peine d'être noté, parce qu'il peut parfois arriver que vous ne vouliez pas que tel ami sache que vous êtes en ligne !



Un compte par appareil

Lorsque vous ouvrez ces applications pour la première fois, vous créez un mot de passe qui sera utilisé pour chiffrer votre profil, vos contacts et l'historique de vos messages (si vous choisissez de le sauvegarder). Ces données restent chiffrées sur votre appareil lorsque vous n'utilisez pas l'application.

Comme il n'y a pas de serveur central, vous ne pouvez pas synchroniser votre compte sur plusieurs appareils. Vous pouvez migrer manuellement votre compte d'un appareil à l'autre, par exemple d'un ancien téléphone à un nouveau, mais il n'y a pas de synchronisation magique dans le cloud. Le fait d'avoir un compte distinct sur chaque appareil est une solution de contournement facile, qui encourage la compartimentation. Le fait de ne pas avoir à se soucier d'une version synchronisée sur un serveur central (même s'il est chiffré) ou sur un autre appareil est également un avantage. Cela oblige à considérer plus attentivement où se trouvent vos données et comment vous y accédez plutôt que de tout garder « dans le nuage » (c'est-à-dire sur l'ordinateur de quelqu'un d'autre). Il n'existe pas non plus de copie de vos données utilisateur qui serait sauvegardée sur un serveur tiers

afin de restaurer votre compte en cas d'oubli de votre mot de passe ou de perte de votre appareil. Si c'est perdu… c'est perdu !.

Les seuls moyens de contourner ce problème sont : soit de confier à un serveur central une copie de vos contacts et de votre compte de média social, soit de faire confiance à un autre média social, de la même manière que Signal utilise votre liste de contacts composée de numéros de téléphone. Nous ne devrions pas faire confiance à un serveur central pour stocker ces informations (même sous forme chiffrée), ni utiliser quelque chose comme des numéros de téléphone. La possibilité de devoir reconstruire vos comptes de médias sociaux à partir de zéro est le prix à payer pour éviter ces problèmes de sécurité, et encourage la pratique qui consiste à maintenir et à rétablir des liens de confiance avec nos amis.

Durée de la batterie

Exécuter des connexions pair-à-pair avec Tor signifie que l'application doit être connectée et à l'écoute en permanence au cas où l'un de vos amis vous enverrait un message. Cela peut s'avérer très gourmand en batterie sur des téléphones anciens. Le problème se pose de moins en moins, car il y a une amélioration générale de l'utilisation des batteries et ces dernières sont de meilleure qualité.

Rien pour les utilisateurs d'iOS

Aucune de ces applications ne fonctionne sur iOS, principalement en raison de l'hostilité d'Apple à l'égard de toute application qui permet d'établir des connexions pair-à-pair avec Tor. Il est peu probable que cela change à l'avenir (mais ce n'est pas impossible).

Le bestiaire CPT

Il est temps de faire connaissance avec ces applications CPT. Elles disposent toutes les deux d'excellents manuels d'utilisation qui fournissent des infor-

mations complètes, mais voici un bref aperçu de leur fonctionnement, de leurs fonctionnalités et de la manière dont on les peut les utiliser.

Briar

Site officiel de Briar — Manuel de Briar

Histoire et philosophie de l'application

Briar est développé par le Briar Project, un collectif de développeurs, de hackers et de partisans du logiciel libre, principalement basé en Europe. En plus de résister à la surveillance et à la censure, la vision globale du projet consiste à construire une infrastructure de communication et d'outils à utiliser en cas de catastrophe ou de panne d'Internet. Cette vision est évidemment intéressante pour les anarchistes qui se trouvent dans des régions où il y a un risque élevé de coupure partielle ou totale d'Internet lors d'une rébellion, ou bien là où l'infrastructure générale peut s'effondrer (c.-à-d. partout). Si les connexions à Internet sont coupées, Briar peut synchroniser les messages par Wi-Fi ou Bluetooth. Briar permet également de partager l'application elle-même directement avec un ami. Elle peut même former un réseau maillé rudimentaire entre pairs, de sorte que certains types de messages peuvent passer d'un utilisateur à l'autre.

Briar est un logiciel open source et a également fait l'objet d'un audit de sécurité indépendant en 2013.

- À l'heure où nous écrivons ces lignes, Briar est disponible pour Android et la version actuelle est la 1.4.9.
- Une version desktop bêta est disponible pour Linux (version actuelle 0.2.1.), bien qu'il lui manque de nombreuses fonctionnalités.
- Des versions Windows et macOS du client desktop sont prévues.

Utiliser Briar

Conversation basique

Le clavardage de base fonctionne très bien. Les amis doivent s'ajouter mutuellement pour pouvoir se connecter. Briar dispose d'une petite interface agréable pour effectuer cette opération en présentiel en scannant les codes QR de l'autre. Mais il est également possible de le faire à distance en partageant les identifiants (sous la forme d'un « lien briar://"), ou bien un utilisateur peut en « présenter » d'autres dans l'application, ce qui permet à deux utilisatrices de devenir des contacts l'une pour l'autre par l'intermédiaire de leur amie commune. Cette petite contrainte dans la manière d'ajouter des contacts peut sembler gênante, mais pensez à la façon dont ce modèle encourage des meilleures pratiques, notamment sur la confiance que l'on s'accorde en ajoutant des contacts. Briar a même un petit indicateur à côté de chaque nom d'utilisateur pour vous rappeler comment vous le « connaissez » (en personne, via des liens de partage, ou via un intermédiaire).

Actuellement, dans les discussions directes, vous pouvez envoyer des fichiers, utiliser des émojis, supprimer des messages ou les faire disparaître automatiquement au bout de sept jours. Si votre ami n'est pas en ligne, vous pouvez lui écrire un message qui sera envoyé automatiquement la prochaine fois que vous le verrez en ligne.

Groupes privés

Les groupes privés de Briar sont des groupes de discussion de base. Seul le créateur du groupe peut inviter d'autres membres. La création de groupes privés est donc très pensée en amont et destinée à un usage spécifique. Ils prennent en charge un affichage par fil de discussion (vous pouvez répondre directement à un message spécifique, même s'il ne s'agit pas du message le plus récent de la discussion), mais il s'agit d'un système assez rudimentaire. Il n'est pas possible d'envoyer des images dans un groupe privé, ni de supprimer des messages.

Avec Briar, les discussions de groupe étant véritablement sans serveur, les choses peuvent être un peu bizarres lorsque tous les membres du groupe ne sont pas en ligne en même temps. Vous vous souvenez de la synchronicité ? Tout message de groupe sera envoyé à tous les membres du groupe qui sont en ligne à ce moment-là. Briar s'appuie sur tous les membres d'un groupe pour relayer les messages aux autres membres qui ne sont pas en ligne. Si vous avez manqué certains messages dans une discussion de groupe, n'importe quel autre membre qui a reçu ces messages peut vous les transmettre lorsque vous êtes tous les deux en ligne.

Forums

Briar dispose également d'une fonction appelée Forums. Les forums fonctionnent de la même manière que les groupes privés, sauf que tout membre peut inviter d'autres membres.

Blog

La fonction de blog de Briar est plutôt sympa ! Chaque utilisateur dispose par défaut d'un flux de blog. Les articles de blog publiés par vos contacts s'affichent dans votre propre flux. Vous pouvez également commenter un billet, ou « rebloguer » le billet d'un contact pour qu'il soit partagé avec tous vos contacts (avec votre commentaire). En bref, c'est un réseau social rudimentaire qui fonctionne uniquement sur Briar.

Lecteur de flux RSS

Briar dispose également d'un lecteur de flux rss intégré qui récupère les nouveaux messages des sites d'information via Tor. Cela peut être un excellent moyen de lire le dernier communiqué de votre site de contre-information anarchiste préféré (qui fournit sûrement un flux rss, si vous ne le saviez pas déjà !). Les nouveaux messages qui proviennent des flux rss que vous avez ajoutés apparaissent dans le flux Blog, et vous pouvez les « rebloguer » pour les partager avec tous vos contacts.

Devenez un maillon

Briar propose de nombreux outils pour faire circuler des messages entre contacts, sans avoir recours à des serveurs centraux. Les forums et les blogs sont relayés d'un contact à l'autre, à l'instar des groupes privés qui synchronisent les messages entre les membres sans serveur. Tous vos contacts peuvent recevoir une copie d'un billet de blog ou de forum même si vous n'êtes pas en ligne en même temps – les contacts partagés transmettent le message pour vous. Briar ne crée pas de réseau maillé où les messages sont transmis via d'autres utilisateurs (ce qui pourrait permettre à un adversaire d'exploiter plusieurs comptes malveillants et de collecter des métadonnées). Briar ne confie aucun de vos messages à des utilisateurs auxquels ils ne sont pas destinés. Au contraire, chaque utilisatrice censée recevoir un message participe également à la transmission de ce message, et uniquement grâce à ses propres contacts. Cela peut s'avérer particulièrement utile pour créer un réseau de communication fiable qui fonctionne même si Internet est indisponible. Les utilisatrices de Briar peuvent synchroniser leurs messages par Wi-Fi ou Bluetooth. Vous pouvez vous rendre au café internet local, voir quelques amis et synchroniser divers messages de blogs et de forums. Puis une fois rentré, vos colocataires peuvent se synchroniser avec vous pour obtenir les mêmes mises à jour de tous vos contacts mutuels partagés.

Mises en garde pour Briar

Chaque instance de l'application ne prend en charge qu'un seul compte. Il n'est donc pas possible d'avoir plusieurs comptes sur le même appareil. Ce n'est pas un problème si vous utilisez Briar uniquement pour parler avec un groupe d'amis proches, mais cela rend difficile l'utilisation de Briar avec des groupes différents que vous voudriez compartimenter. Briar fournit pour cela plusieurs arguments basés sur la sécurité, dont l'un est simple : si le même appareil utilise plusieurs comptes, il pourrait théoriquement être plus facile pour un adversaire de déterminer que ces comptes sont liés, malgré l'utilisation de Tor. Si deux comptes ne sont jamais en ligne en même temps, il y a de fortes chances qu'ils utilisent le même téléphone

portable pour leurs comptes Briar individuels. Il existe d'autres raisons, et aussi des solutions de contournement, toujours est-il qu'il n'est pas possible, pour le moment, d'avoir plusieurs profils sur le même appareil.

Le protocole Briar exige également que deux utilisatrices s'ajoutent mutuellement en tant que contacts, ou qu'ils soient parrainés par un ami commun, avant de pouvoir interagir. Cela empêche de publier une adresse Briar pour recevoir des messages anonymes. Par exemple, vous voudriez publier votre identifiant Briar pour recevoir des commentaires honnêtes sur un article qui compare différentes applications de chat sécurisées.

Briar et la communication asynchrone

De manière générale, les utilisateurs et utilisatrices apprécient beaucoup la communication asynchrone. Le projet Briar travaille sur une autre application : une boîte aux lettres (Briar Mailbox) qui pourrait être utilisée facilement sur un vieux téléphone Android ou tout autre machine bon marché. Cette boîte aux lettres resterait en ligne principalement pour recevoir des messages pour vous, puis se synchroniserait avec votre appareil principal via Tor lorsque vous êtes connecté. C'est une idée intéressante. Une seule boîte aux lettres Briar pourrait potentiellement être utilisée par plusieurs utilisateurs qui se font confiance, comme des colocataires dans une maison collective, ou les clients réguliers d'un magasin d'information local. Plutôt que de s'appuyer sur un serveur central pour faciliter les échanges asynchrones, un petit serveur facile à configurer et contrôlé par vous-même serait utilisé pour stocker les messages entrants pour vous et vos amis lorsque vous n'êtes pas en ligne. Ce système étant encore en cours de développement, son degré de sécurité (par exemple, savoir si les messages stockés ou d'autres métadonnées seraient suffisamment sûrs si un adversaire accédait à la boîte aux lettres) n'est pas connu et devra faire l'objet d'une évaluation.

Cwtch

Site officiel de Cwtch — Manuel de Cwtch

Historique et philosophie de l'application

Alors oui ce nom pas facile à prononcer… ça rime avec « butch ». Apparemment, il s'agit d'un mot gallois qui signifie une étreinte offrant comme un refuge dans les bras de quelqu'un.

Cwtch est développé par l'Open Privacy Research Society, une organisation à but non lucratif basée à Vancouver. Dans l'esprit, Cwtch pourrait être décrit comme un « Signal queer ». Open Privacy s'investit beaucoup dans la création d'outils destinés à « servir les communautés marginalisées » et à résister à l'oppression. Elle a également travaillé sur d'autres projets intéressants, comme la conception d'un outil appelé « Shatter Secrets », destiné à protéger les secrets contre les scénarios dans lesquels les individus peuvent être contraints de révéler un mot de passe (comme lors d'un passage de frontière).

Cwtch est également un logiciel open source et son protocole repose en partie sur le projet CPT antérieur nommé Ricochet. Cwtch est un projet plus récent que Briar, mais son développement est rapide et de nouvelles versions sortent fréquemment.

- À l'heure où nous écrivons ces lignes, la version actuelle est la 1.8.0.
- Cwtch est disponible pour Android, Windows, Linux et macOS.

Utiliser Cwtch

Lorsque vous ouvrez Cwtch pour la première fois, vous créez votre profil, protégé par un mot de passe. Votre nouveau profil se voit attribuer un mignon petit avatar et une adresse Cwtch. Contrairement à Briar, Cwtch peut prendre en charge plusieurs profils sur le même appareil, et vous pouvez en avoir plusieurs déverrouillés en même temps. C'est idéal si vous voulez avoir des identités séparées pour différents projets ou réseaux sans

avoir à passer d'un appareil à l'autre (mais dans ce cas attention aux possibles risques de sécurité !).

Pour ajouter un ami, il suffit de lui donner votre adresse Cwtch. Il n'est pas nécessaire que vous et votre ami échangiez d'abord vos adresses pour discuter. Cela signifie qu'avec Cwtch, vous pouvez publier une adresse Cwtch publiquement et vos ami·e·s'ou non peuvent vous contacter de manière anonyme. Vous pouvez également configurer Cwtch pour qu'il bloque automatiquement les messages entrants provenant d'inconnus. Voici une adresse Cwtch pour contacter l'auteur de cet article si vous avez des commentaires ou envie d'écrire un quelconque message haineux : `g6px2uyn5tdg2gxpqqktnv7qi2i5frr5kf2dgnyielvq4o4emry4qzid`

En mode conversation directe, Cwtch propose un formatage de texte riche, des emojis et des réponses. Chaque conversation peut être configurée pour «enregistrer l'historique» ou «supprimer l'historique» à la fermeture de Cwtch.

C'est le strict minimum et cela fonctionne très bien. Pour l'instant, toutes les autres fonctionnalités de Cwtch sont «expérimentales» et vous pouvez les choisir en y accédant par les paramètres. Cela comprend les discussions de groupe, le partage de fichiers, l'envoi de photos, les photos de profil, les aperçus d'images et les liens cliquables avec leurs aperçus. Le développement de Cwtch a progressé assez rapidement, donc au moment où vous lirez ces lignes, toutes ces fonctionnalités seront peut-être entièrement développées et disponibles par défaut.

Discussions de groupe

Cwtch propose également des discussions de groupe en tant que «fonction expérimentale». Pour organiser cela, Cwtch utilise actuellement des serveurs gérés par les utilisateurs, ce qui est très différent de l'approche de Briar. Open Privacy considère que la résistance aux métadonnées des discussions de groupe est un problème ouvert, et j'espère qu'en lisant ce qui précède, vous comprendrez pourquoi. Tout comme le serveur Signal, les serveurs Cwtch sont conçus de telle sorte qu'ils soient toujours considérés comme «non fiables» et qu'ils puissent en apprendre le moins possible sur

le contenu des messages ou les métadonnées. Mais bien entendu, ces serveurs sont gérés par des utilisateurs individuels et non par une tierce partie centrale.

Tout utilisateur de Cwtch peut devenir le « serveur » d'une discussion de groupe. C'est idéal pour les groupes à usage unique, où un utilisateur peut devenir l'« hôte » d'une réunion ou d'une discussion rapide. Les serveurs de discussion de groupe de Cwtch permettent également la transmission asynchrone des messages, de sorte qu'un groupe ou une communauté peut exploiter son propre serveur en permanence pour rendre service à ses membres. La façon dont Cwtch aborde les discussions de groupe est encore en cours de développement et pourrait changer à l'avenir, mais il s'agit pour l'instant d'une solution très prometteuse et sympathique.

Correspondance asynchrone avec Cwtch

Les discussions de groupe dans Cwtch permettent la correspondance asynchrone (tant que le serveur/hôte est en ligne), mais comme Briar, Cwtch exige que les deux contacts soient en ligne pour l'envoi de messages directs. Contrairement à Briar, Cwtch ne permet pas de mettre en file d'attente les messages à envoyer à un contact une fois qu'il est en ligne.

Cwtch et la question des crypto-monnaies

Fin 2019, Open Privacy, qui développe Cwtch, a reçu un don sans conditions de 40000 dollars canadiens de la part de la fondation Zcash. Zcash est une autre crypto-monnaie centrée sur la vie privée, similaire mais nettement

inférieure à Monero[7]. En 2019, Cwtch en était au tout début de son développement, et Open Privacy a mené quelques expériences exploratoires sur l'utilisation de Zcash ou de crypto-monnaies blockchain similaires comme des solutions créatives à divers défis relatifs au chiffrement, avec l'idée qu'elles pourraient être incorporées dans Cwtch à un moment ou à un autre. Depuis lors, aucun autre travail de développement avec Zcash ou d'autres crypto-monnaies n'a été associé à Cwtch, et il semble que ce ne soit pas une priorité ou un domaine de recherche pour Open Privacy. Toutefois, il convient de mentionner ce point comme un signal d'alarme potentiel pour les personnes qui se méfient fortement des systèmes de crypto-monnaies. Rappelons que Signal dispose déjà d'une crypto-monnaie entièrement fonctionnelle intégrée à l'application, qui permet aux utilisateurs d'envoyer et de recevoir des MobileCoin.

Conclusions

(… « X a quitté le groupe »)

De nombreux lecteurs se disent peut-être : « Les applications CPT ne semblent pas très bien prendre en charge les discussions de groupe… et j'adore les discussions de groupe ! »… Premièrement, qui aime vraiment les discussions de groupe ? Deuxièmement, c'est l'occasion de soulever des critiques sur la façon dont les anarchistes finissent par utiliser les discussions de groupe dans Signal, pour faire valoir que la façon dont elles sont mises en œuvre dans Briar et Cwtch ne devrait pas être un obstacle.

Signal, Cwtch et Briar vous permettent tous les trois d'organiser facilement un groupe en temps réel (synchrone !) pour une réunion ou une discussion collective rapide qui ne pourrait pas avoir lieu en présentiel. Mais lorsque les gens parlent de « discussion de groupe » (en particulier dans le contexte de Signal), ce n'est pas vraiment ce qu'ils veulent dire. Les discussions de groupe dans Signal deviennent souvent d'énormes flux continus de mises à jour semi-publiques, de « *shitposts* », de liens repartagés, etc. qui s'appa-

7 Le créateur de Zcash, un cypherpunk du nom de Zooko Wilcox-O'Hearn, semble prétendre que Zcash est privé mais ne peut pas être utilisé dans un but criminel…

rentent davantage à des pratiques de médias sociaux. Il y a plus de membres qu'il n'est possible d'en avoir pour une conversation vraiment fonctionnelle, sans parler de la prise de décision. La diminution de l'utilité et de la sécurité selon l'augmentation de la taille, de la portée et de la persistance des groupes Signal a été bien décrite dans l'excellent article Signal Fails. Plus un groupe de discussion s'éloigne de la petite taille, du court terme, de l'intention et de l'objectif principal, plus il est difficile à mettre en œuvre avec Briar et Cwtch — et ce n'est pas une mauvaise chose. Briar et Cwtch favorisent des habitudes plus saines et plus sûres, sans les « fonctionnalités » de Signal qui encouragent la dynamique des discussions de groupe critiquées dans des articles tels que « Signal Fails ».

Proposition

Briar et Cwtch sont deux initiatives encore jeunes. Certains anarchistes en ont déjà entendu parler et essaient d'utiliser l'un ou l'autre pour des projets ou des cas d'utilisation spécifiques. Les versions actuelles peuvent sembler plus lourdes à utiliser que Signal, et elles souffrent de l'effet de réseau – tout le monde utilise Signal, donc personne ne veut utiliser autre chose [8]. Il est intéressant de souligner que les obstacles apparents à l'utilisation de Cwtch et Briar (encore en version bêta, effet de réseau, différent de ce à quoi vous êtes habitué, sans version iOS) sont exactement les mêmes que ceux qui ont découragé les premiers utilisateurs de Signal (alias TextSecure !).

Il est difficile d'amener les gens à se familiariser avec un nouvel outil et à commencer à l'utiliser. Surtout lorsque l'outil auquel ils sont habitués semble fonctionner à merveille ! Le défi est indéniable. Ce guide a pris des pages et des pages pour tenter de convaincre les anarchistes, qui sont peut-être ceux qui se préoccupent le plus de ces questions, qu'ils ont intérêt à utiliser ces applications.

---

8 Avez-vous un moment pour parler d'interopérabilité et de fédération ? Peut-être plus tard…

Les anarchistes ont déjà réussi à adopter de nouveaux outils électroniques prometteurs, à les diffuser et à les utiliser efficacement lors des actions de lutte et de résistance. La normalisation de l'utilisation des applications CPT en plus ou à la place de Signal pour la communication électronique renforcera la résilience de nos communautés et de ceux que nous pouvons convaincre d'utiliser ces outils. Ils nous aideront à nous protéger de la collecte et de l'analyse de métadonnées de plus en plus puissantes, à ne pas dépendre d'un service centralisé et à rendre plus facile l'accès à l'anonymat.

Voici donc la proposition. Après avoir lu ce guide, mettez-le en pratique et partagez-le. Vous ne pouvez pas essayer Cwtch ou Briar seul, vous avez besoin d'au moins un ami pour cela. Installez-ces applications avec votre équipe et essayez d'utiliser l'une ou l'autre pour un projet spécifique qui vous convient. Organisez une réunion hebdomadaire avec les personnes qui ne peuvent pas se rencontrer en personne pour échanger des nouvelles qui, autrement, auraient été partagées dans un groupe de discussion aggluTiné sur Signal. Gardez le contact avec quelques amis éloignés ou avec une équipe dont les membres sont distants. Vous n'êtes pas obligé de supprimer Signal (et vous ne le devriez probablement pas), mais vous contribuerez au minimum à renforcer la résilience en établissant des connexions de secours avec vos réseaux. Alors que la situation s'échauffe, la probabilité d'une répression intensive ou de fractures sociétales telles que celles qui perturbent Signal dans d'autres pays est de plus en plus grande partout, et nous aurons tout intérêt à mettre en place nos moyens de communication alternatifs le plus tôt possible !

Briar et Cwtch sont tous deux en développement actif, par des anarchistes et des sympathisants à nos causes. En les utilisant, que ce soit sérieusement ou pour le plaisir, nous pouvons contribuer à leur développement en signalant les bogues et les vulnérabilités, et en incitant leurs développeurs à continuer, sachant que leur projet est utilisé. Peut-être même que les plus férus d'informatique d'entre nous peuvent contribuer directement, en vérifiant le code et les protocoles ou même en participant à leur développement.

Outre la lecture de ce guide, essayer d'utiliser ces applications en tant que groupe d'utilisateurs curieux est le meilleur moyen d'apprécier en quoi elles sont structurellement différentes de Signal. Même si vous ne pouvez pas vous résoudre à utiliser ces applications régulièrement, le fait d'essayer différents outils de communication sécurisés et de *comprendre* comment, pourquoi et en quoi ils sont différents de ceux qui vous sont familiers améliorera vos connaissances en matière de sécurité numérique. Il n'est pas nécessaire de maîtriser les mathématiques complexes qui sous-tendent l'algorithme de chiffrement à double cliquet de Signal, mais une meilleure connaissance et une meilleure compréhension du fonctionnement théorique et pratique de ces outils permettent d'améliorer la sécurité opérationnelle dans son ensemble. Tant que nous dépendons d'une infrastructure pour communiquer, nous devrions essayer de comprendre comment cette infrastructure fonctionne, comment elle nous protège ou nous rend vulnérables, et explorer activement les moyens de la renforcer.

Le mot de la fin

Toute cette discussion a porté sur les applications de communication sécurisées qui fonctionnent sur nos téléphones et nos ordinateurs. Le mot de la fin doit rappeler que même si l'utilisation d'outils de chiffrement et d'anonymisation des communications en ligne peut vous protéger contre vos adversaires, vous ne devez jamais saisir ou dire quoi que ce soit sur une application ou un appareil sans savoir que cela pourrait être interprété devant un tribunal. Rencontrer vos amis, face à face, en plein air et loin des caméras et autres appareils électroniques est de loin le moyen le plus sûr d'avoir une conversation qui doit être sécurisée et privée. Éteignez votre téléphone, posez-le et sortez !

Appendice : d'autres applications dont vous n'avez pas forcément entendu parler

Ricochet Refresh

Ricochet était une toute première application CPT de bureau financée par le Blueprint for Free Speech, basé en Europe. Ricochet Refresh est la version actuelle. Fondamentalement, elle est très similaire à Cwtch et Briar, mais assez rudimentaire – elle dispose d'un système basique de conversation directe et de transfert de fichiers, et ne fonctionne que sur MacOS, Linux et Windows. Cette application est fonctionnelle, mais dépouillée, et n'a pas de version pour mobiles.

OnionShare

OnionShare est un projet fantastique qui fonctionne sur n'importe quel ordinateur de bureau et qui est fourni avec Tails et d'autres systèmes d'exploitation. Il permet d'envoyer et de recevoir facilement des fichiers ou d'avoir un salon de discussion éphémère rudimentaire via Tor. Il est également CPT !

Telegram

Telegram est en fait comme Twitter. Il peut s'avérer utile d'y être présent dans certains scénarios, mais il ne devrait pas être utilisé pour des communications sécurisées car il y a des fuites de métadonnées partout. Il n'est probablement pas utile de passer plus de temps à critiquer Telegram ici, mais il ne devrait pas être utilisé là où la vie privée ou la sécurité sont exigées.

Tox

Tox est un projet similaire à Briar et Cwtch, mais il n'utilise pas Tor – c'est juste CP. Tox peut être routé manuellement à travers Tor. Aucune des applications développées pour Tox n'est particulièrement conviviale.

Session

Session mérite qu'on s'y attarde un peu. L'ambiance y est très libertarienne, et activiste façon « free-speech movement ». Session utilise le protocole de chiffrement robuste de Signal, est en pair-à-pair pour les messages directs et utilise également le routage Onion pour l'anonymat (le même principe que celui qui est à la base de Tor). Cependant, au lieu de Tor, Session utilise son propre réseau de routage Onion pour lequel une « participation financière » est nécessaire afin de faire fonctionner un nœud de service qui constitue le réseau Onion. Point essentiel, cette participation financière prend la forme d'une crypto-monnaie administrée par la fondation qui développe Session. Le projet est intéressant d'un point de vue technologique, astucieux même, mais il s'agit d'une solution très « web3 » drapée dans une culture cryptobro. Malgré tout ce qu'ils prétendent, leurs discussions de groupe ne sont pas conçues pour être particulièrement résistantes à la collecte de métadonnées, et les grandes discussions de groupe semi-publiques sont simplement hébergées sur des serveurs centralisés (et apparemment envahis par des cryptobros d'extrême-droite). Peut-être que si la blockchain finit par s'imposer, ce sera une bonne option, mais pour l'instant, on ne peut pas la recommander en toute bonne conscience.

Molly

Molly est un fork du client Signal pour Android. Il utilise toujours le serveur Signal mais propose un peu plus de sécurité et de fonctionnalités sur l'appareil.

Contact

Cet article a été écrit originellement en août 2022. Courriel de l'auteur : pettingzoo riseup net ou via Cwtch : g6px2uyn5tdg2gxpqqktnv7qi2i5-frr5kf2dgnyielvq4o4emry4qzid