Cryptage

De quelle manière il peut protéger les journalistes et la liberté de la presse

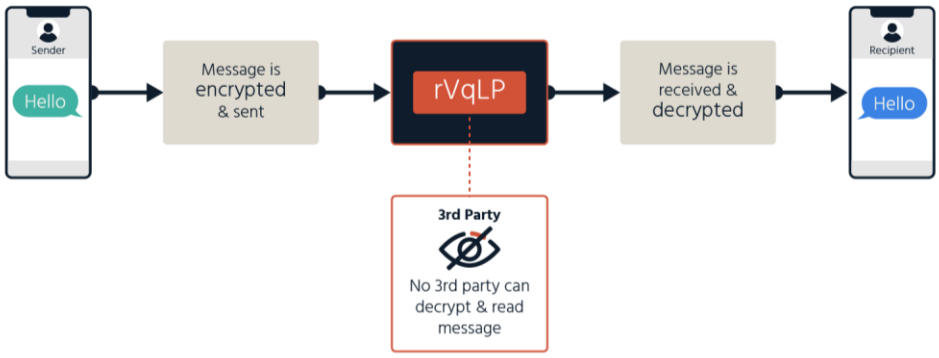
Août 2022

Le cryptage est un outil conçu pour aider les utilisateurs d'Internet à garantir la confidentialité et la sécurité de leurs données et de leurs communications sur Internet. Il joue un rôle crucial dans la protection des activités numériques au quotidien, telles que la gestion bancaire et les achats en ligne, en empêchant le vol de données sensibles en cas de piratage et en assurant la confidentialité des messages confidentiels.

Le cryptage est essentiel à la protection de la liberté d'expression et de la confidentialité.

Qu'est-ce que le cryptage?

Le cryptage est le processus visant à brouiller les informations afin que celles-ci soient uniquement lisibles par une personne disposant de la clé pour les ouvrir et les restituer à leur état initial. Le cryptage de bout en bout (E2E) assure le meilleur niveau de sécurité et de confiance, car, grâce à sa conception, seul le destinataire prévu détient la clé permettant de décrypter le message. Aucun tiers ne devrait disposer de cette clé.



Le cryptage est tout particulièrement important pour certains groupes, notamment pour les journalistes, à qui il permet d'assurer la sécurité des individus et de protéger la liberté de la presse.

Le cryptage et la sécurité des journalistes

Le cryptage est un outil essentiel pour les journalistes. Si les journalistes ne peuvent pas communiquer en toute confiance avec leurs collègues et leurs sources, ils ne peuvent pas exercer leur travail sans

danger. De même, s'ils ne sont pas en mesure d'assurer l'anonymat de leurs sources, ces sources risquent de ne pas leur révéler leurs informations, et le public en subira les conséquences.

Contacter les sources en toute sécurité: les sources des journalistes acceptent parfois de partager des informations incriminant une institution ou des informations personnelles à la condition expresse que les journalistes protègent leur identité. Le cryptage de bout en bout permet aux journalistes d'établir une relation de confiance avec ces sources.

Garantir l'intégrité des informations: les journalistes ont besoin de pouvoir signaler aux lecteurs qu'ils ont créé des contenus fiables, et de s'assurer que cela correspond à ce que les publics ciblés voient effectivement sur Internet.

Les protocoles tels que HTTPS contribuent à la protection des données lorsqu'elles transitent entre un site Internet d'actualité et le lecteur. Cela protège également les journalistes contre la censure: il est plus difficile pour les censeurs de bloquer les messages ou l'accès aux informations s'ils ne sont pas en mesure d'intercepter les données.

Protection contre les attaquants: il est arrivé à de nombreuses reprises que les plateformes en ligne et les terminaux de journalistes et de médias soient piratés et surveillés par des acteurs gouvernementaux ou privés. La National Security Agency (NSA) américaine aurait ainsi piraté le système de communication en interne d'Al-Jazeera. Les journalistes sont également confrontés à des menaces telles que les violences en ligne, le doxing (collecte et divulgation sur Internet d'informations personnelles) et le cyberharcèlement. Le cryptage de bout en bout contribue à la protection des communications contre la surveillance et l'interception par des tiers.

Demander des comptes aux gouvernements et aux institutions: un aspect primordial du journalisme est sa capacité à demander des comptes aux personnes et aux institutions au pouvoir vis-à-vis de leurs décisions et de leurs actes. Pour ce faire, il est crucial que les journalistes aient accès à des outils de sécurité numériques permettant d'empêcher de puissantes entités (nationales ou étrangères) de consulter ou de modifier leurs recherches, leurs conversations et leurs sources.

Une politique robuste sur le cryptage protège les journalistes partout: lorsque des pays soutiennent le cryptage de bout en bout, ils aident les journalistes de leur propre État, mais aussi dans le monde entier, en définissant une norme de protection du cryptage mondial.

Le cryptaget a permis à des journalistes de révéler une affaire de corruption mondiale

La fuite des documents panaméens (Panama Papers) a commencé fin 2014, lorsqu'une source non identifiée a contacté Bastian Obermayer, un journaliste travaillant pour le quotidien allemand Suddeutsche Zeitung. M. Obermayer a déclaré que sa source l'avait contacté par un chat crypté, et lui avait proposé des données visant à « rendre ces crimes publics ». Mais la source l'a averti que sa « vie était en danger », souhaitait communiquer uniquement par des canaux cryptés, et a refusé toute rencontre en personne. La fuite des Panama Papers a révélé le système d'évasion fiscale au niveau mondial mis en place pour ses clients par un cabinet d'avocats du Panama. Elle rassemblait 2,6 téraoctets de données (11,5 millions de documents) et a impliqué près de 400 journalistes de plus de 100 organisations de presse réparties dans plus de 80 pays, qui ont collaboré pour présenter les affaires qui la composaient.

Le cryptage a aidé des lanceurs d'alerte à contacter des journalistes

En 2015, The Intercept a reçu des fichiers envoyés par un individu par le biais de SecureDrop, un logiciel conçu pour aider les lanceurs d'alerte à transmettre de manière anonyme des informations aux médias. L'affaire a permis de constater que Securus, une entreprise offrant des services téléphoniques dans plus de 2 200 prisons aux États-Unis, conservait des enregistrements pour chaque appel passé par plus de 1,2 million de détenus qui utilisaient ce service dans 37 États, notamment l'heure, le numéro appelé, le nom du détenu, et même des enregistrements sonores de chaque appel. Ces enregistrements étaient fréquemment vendus à leurs clients des forces de l'ordre, notamment des conversations des détenus avec leurs avocats supposées être protégées par le secret professionnel. Ces révélations choquantes ont uniquement pu être rendues publiques, car un individu qui a eu accès aux fichiers les a partagés avec The Intercept en utilisant SecureDrop.

Pourquoi « l'accès exceptionnel » n'est pas la bonne réponse

Les termes « accès exceptionnel » font généralement référence au fait de donner aux forces de l'ordre et aux agences de renseignement la possibilité d'intercepter et d'accéder à des communications cryptées, ou d'ordonner à des entreprises de faire cela en leur nom. Non seulement cela nuit à la sécurité sur Internet, mais cela met également les journalistes en danger, à la fois sur Internet et dans le monde réel. Voici comment:

- **Les faiblesses imposées nous affaiblissent tous**: toute porte d'accès à un service sécurisé est une faiblesse. L'accès exceptionnel met en danger les informations et conversations privées, car il permet aux gouvernements d'accéder à vos informations privées, et car il crée dans le même temps une porte dérobée pour les malfaiteurs. Il n'existe pas de verrou numérique que seuls les « gentils » pourraient ouvrir.
- **L'absence de cryptage peut inciter des journalistes à ne pas publier de contenus risqués**: si les journalistes ne disposent pas des moyens de travailler en sécurité, ils pourraient décider de ne pas enquêter sur des sujets sensibles par peur des représailles, de la surveillance et du harcèlement auxquels ils pourraient être exposés. Une démocratie saine a besoin qu'une presse libre, puissante et indépendante informe le public sur ce que font les gouvernements, les institutions et les entreprises auxquels il accorde sa confiance.

Recommandation

Protéger la liberté de la presse en défendant le cryptage robuste de bout en bout et en veillant à ce que les journalistes et le grand public puissent l'utiliser en toute liberté. Les journalistes doivent être

en sécurité sur Internet pour pouvoir demander des comptes aux gouvernements et aux institutions, révéler des affaires importantes et susceptibles d'entraîner des conséquences, protéger leurs sources et renforcer la santé des démocraties.

Découvrez plus d'informations sur l'importance du cryptage pour les journalistes

Pour en savoir davantage, rendez-vous sur www.cpj.org et @pressfreedom sur Twitter.

Formation et ressources sur le cryptage de l'Internet Society

https://www.internetsociety.org/fr/issues/encryption/resources/

https://www.internetsociety.org/fr/learning/encryption/