Cryptage

Briefing sur les affaires publiques de l'Internet Society

03 June 2016

Introduction

Nous sommes entourés de technologies de chiffrement. Le chiffrement est utilisé pour protéger les données envoyées depuis tous types d'appareils par le biais d'une multitude de réseaux divers. En plus de protéger les porte-clés électroniques mémorisant des mots de passe pour des ordinateurs et des tableurs qui sont « strictement personnels », le chiffrement permet de protéger les informations qui sont échangées chaque fois qu'une personne utilise un distributeur de billets, réalise un achat depuis un téléphone intelligent, passe un appel depuis un téléphone mobile ou appuie sur une clé électronique pour déverrouiller une voiture. De plus en plus présente dans notre quotidien, cette technologie polyvalente est essentielle pour assurer la sécurité dans beaucoup de nos activités.

Le chiffrement électronique, c'est-à-dire le processus de brouillage ou de cryptage des données afin que seule une personne disposant des moyens de les renvoyer à leur état d'origine puisse les consulter, est couramment utilisé pour protéger les données stockées sur des systèmes informatiques ainsi que les données transmises par des réseaux informatiques, y compris l'Internet. S'agissant des données transmises sur un réseau, le chiffrement moderne brouille les données à l'aide d'une valeur ou d'une clé secrète que seuls le destinataire et l'expéditeur des données connaissent. Pour ce qui est des données stockées, la valeur secrète n'est généralement connue que par le propriétaire des données.

Le chiffrement et les techniques associées sont également utilisés pour développer une sécurité renforcée des transactions financières et pour protéger les communications privées d'utilisateurs finaux. Ces technologies permettent par exemple de déterminer si des données ont été altérées (intégrité des données) et de renforcer la confiance des utilisateurs dans le fait qu'ils communiquent avec les destinataires prévus (authentification), et elles font partie des protocoles qui apportent la preuve que les messages ont été envoyés et reçus (non-répudiation).

Les technologies de chiffrement permettent aux internautes de protéger la confidentialité de leurs données et communications contre des observations et des intrusions indésirables. Le chiffrement constitue également le fondement technique de la confiance sur Internet. Il promeut la liberté d'expression, le commerce, la confidentialité et la confiance des utilisateurs, et contribue à la protection des données contre des acteurs malveillants. C'est pour ces raisons que l'Internet Society pense que le chiffrement devrait être la norme pour le trafic sur Internet et le stockage des données.

Du fait que des acteurs malveillants peuvent utiliser le chiffrement pour masquer leurs activités ou pour détourner les données des utilisateurs (par exemple, à l'aide d'un logiciel rançonneur[1]), les membres des agences de sécurité gouvernementales et des organismes d'application de la loi se sont dits préoccupés par les répercussions négatives que le chiffrement pourrait avoir sur leur capacité à protéger les citoyens et à faire appliquer la loi.

Bien qu'elle comprenne ces préoccupations, l'Internet Society demeure fermement convaincue que le chiffrement est une solution technique importante que tous les internautes – les particuliers, les gouvernements, les entreprises et d'autres communautés – doivent utiliser pour protéger leurs communications et leurs données. Nous pensons que les tentatives juridiques et techniques visant à limiter l'utilisation du chiffrement, que celle-ci soit bien intentionnée ou non, auront des retombées négatives sur la sécurité des citoyens qui respectent la loi.

Principales considérations

Dans la pratique, les technologies de chiffrement sont réparties dans les catégories suivantes :

- **Le chiffrement symétrique** utilise une clé identique pour chiffrer et déchiffrer le message. L'expéditeur et le destinataire ont tous deux accès à la même clé. Bien que le chiffrement symétrique soit rapide et efficace pour des ordinateurs, il nécessite de s'assurer que la clé est fournie de manière fiable au destinataire et qu'elle ne tombe pas entre de mauvaises mains.

- **Le chiffrement asymétrique**, également appelé « chiffrement à clé publique », est une forme de chiffrement unidirectionnelle. Les clés sont fournies par paire, et il n'est possible de déchiffrer les informations qui ont été chiffrées avec la clé publique qu'à l'aide de la clé privée correspondante. Le destinataire publie une clé publique afin que l'expéditeur puisse chiffrer ses données. Le destinataire utilise ensuite une clé privée pour déchiffrer les données. Le processus est similaire à celui d'une boîte à lettres verrouillée équipée d'une fente où insérer le courrier, lequel ne peut être ensuite récupéré par son propriétaire qu'à l'aide d'une clé. Le chiffrement à clé publique est plus sûr que le chiffrement symétrique, car il n'est pas nécessaire de transférer la clé.

- **Le chiffrement de bout en bout désigne** toute forme de chiffrement par laquelle seuls l'expéditeur et le destinataire prévu peuvent lire le message. L'aspect le plus important du chiffrement de bout en bout est qu'aucun tiers, même la partie qui fournit le service de communication, n'a connaissance de la clé de chiffrement. Le chiffrement de bout en bout comprend par exemple les protocoles Pretty Good Privacy (PGP) et Off-the-Record Messaging (OTR). Il existe plusieurs services de communication par chiffrement de bout en bout, comme iMessage d'Apple, Telegram et Threema. L'Electronic Frontier Foundation a publié un tableau de bord des messageries sécurisées[1] qui présente des informations sur les caractéristiques des divers services.

- **Le chiffrement de données statiques** désigne toute forme de chiffrement protégeant les données qui sont physiquement stockées dans un format numérique (par exemple, sur des ordinateurs, des disques de stockage, des appareils mobiles ou l'Internet des objets).

Dans la pratique, le chiffrement s'applique dans le cadre d'une approche à plusieurs niveaux. Par exemple, un utilisateur chiffre son courriel à l'aide d'un protocole PGP ou d'extensions multifonctions/sécurisées du courrier Internet (S/MIME), et le fournisseur de service de messagerie électronique (par exemple, Gmail) chiffre la transmission du courriel à l'aide du protocole HTTPS.

Il est important de noter qu'avec le chiffrement, toutes les données de communications ne sont pas nécessairement illisibles. Par exemple, il est possible que les métadonnées de communication – y compris les identifiants des expéditeurs et des destinataires, la longueur des messages, le lieu, la date et l'heure, ainsi que les données utilisées afin de faire respecter la loi – soient exposées en texte clair.

1 Consulter https://www.eff.org/secure-messaging-scorecard.

Difficultés

La disponibilité généralisée du chiffrement, ainsi que sa nature polyvalente et son utilisation par différents acteurs, présente un certain nombre de difficultés.

- **Liberté d'expression, anonymat et abus.** Les technologies de chiffrement facilitent les communications anonymes, ce qui représente un lien vital potentiel pour les citoyens et les militants qui vivent sous des régimes et des individus oppressifs dans des communautés vulnérables, comme les victimes de violence familiale, ceux qui participent à des programmes de protection de témoins, et des agents de police banalisés. La même technologie peut toutefois également aider des acteurs malveillants à masquer leurs activités et leurs communications grâce à des outils d'anonymat à des fins de cyberintimidation et d'autres formes d'abus en ligne.

  L'Internet Society reconnaît le bien-fondé de l'objectif des États nations visant à protéger leurs citoyens, mais elle met en garde contre les tentatives de réglementation des technologies qui ont pour but d'empêcher les criminels de communiquer en toute confidentialité. Cette approche risque vraisemblablement d'entraver la protection de la confidentialité des données et des communications des citoyens qui respectent la loi et de compromettre leurs droits à la confidentialité et à jouir de la liberté d'expression et de la liberté d'opinion. Comme nous l'avons présenté en détail dans notre rapport intitulé Collaborative Security (sécurité collaborative)[2], l'objectif global de la sécurité devrait consister à promouvoir la confiance dans l'Internet et à assurer la poursuite de l'essor de l'Internet en tant que moteur de l'innovation économique et sociale.

- **Le dilemme entre la sécurité et la confidentialité.** Les débats politiques sur le chiffrement abordent fréquemment la question en opposant la sécurité à la confidentialité, en vue de trouver un équilibre entre la responsabilité qu'ont les gouvernements de protéger leurs citoyens et les droits des citoyens à protéger leur confidentialité contre les intrusions du gouvernement, des entreprises ou des criminels. L'Internet Society estime que la sécurité et la confidentialité ne sont pas nécessairement des concepts incompatibles. Au contraire, elles peuvent se renforcer mutuellement : la confiance des utilisateurs tient au sentiment que leurs communications sont à la fois confidentielles et sécurisées. Par exemple, l'assurance qu'un message est sûr (qu'il ne sera lu que par son destinataire prévu) permet à une variété de services Internet, en particulier le commerce électronique, de prospérer.

[2] Consulter http://www.internetsociety.org/collaborativesecurity.

- **Les portes dérobées du chiffrement.** Cette expression désigne l'idée selon laquelle un outil peut aider un tiers autorisé à accéder à des données chiffrées et à les déchiffrer sans accéder à des clés. Mais de telles portes dérobées permettraient également des accès furtifs au contenu. Le consensus technique[3] est que l'introduction de portes dérobées par l'une quelconque des techniques actuellement disponibles expose les utilisateurs légitimes à des risques et qu'elle n'empêchera probablement pas des criminels de communiquer de manière clandestine. Les acteurs malveillants seront susceptibles de trouver d'autres moyens de communiquer, alors que les utilisateurs standard ne disposent peut-être pas des mêmes outils. De ce fait, les communications criminelles pourraient être transmises sans être surveillées, alors que les communications des utilisateurs seraient exposées aux processus de surveillance et d'interception des gouvernements ou d'acteurs malveillants, qui ont découvert comment exploiter les portes dérobées.

- **Technologies inviolables.** Les technologies inviolables, qui sont associées au chiffrement, sont conçues afin que des attaquants ne puissent pas facilement les modifier, et que toute altération soit évidente. Utilisées en conjonction avec le chiffrement, les mesures contre les altérations peuvent aider à empêcher (1) l'accès à un appareil après plusieurs tentatives de connexion ; et (2) l'installation de portes dérobées de chiffrement, de programmes malveillants furtifs (code malveillant visant à accéder à différentes
zones d'un ordinateur sans autorisation), et d'autres logiciels malveillants. Ces dernières années, nous avons observé une évolution vers une utilisation accrue des technologies inviolables ainsi que de mécanismes qui effacent automatiquement les données dans certaines conditions (par exemple, au bout de 10 échecs de tentatives de saisie d'un mot de passe correct). Bien que les technologies inviolables aident à protéger l'intégrité des technologies, elles peuvent également poser des difficultés pour les organismes d'application de la loi qui tentent d'accéder aux communications et aux données d'acteurs malveillants dans le cadre d'une ordonnance judiciaire[4].

Principes directeurs

L'Internet Society offre les principes de politique d'orientation suivants :

- **Confidentialité et anonymat.** Pour soutenir la libre expression des droits de l'homme, y compris la confidentialité et la liberté d'expression, les individus doivent pouvoir communiquer par Internet de façon confidentielle et anonyme.

- **Sécurité des données.** Tout comme les individus ont le droit de protéger leurs actifs et leurs biens hors ligne, ils devraient avoir le droit d'utiliser le cryptage et d'autres outils pour protéger leurs données, leurs biens numériques

3 Consulter Keys Under Doormats : rendant obligatoire l'insécurité en obligeant l'accès du gouvernement à toutes les données et communications, IAB (Internet Architecture Board) Statement on Internet Confidentiality (Déclaration sur la confidentialité d'Internet) , Conclusions W3C TAG : cryptage de bout en bout et le Web, Conclusions W3C TAG : Sécuriser le Web, M3Blog AAWG : approuve le cryptage de bout en bout « Keys Under Doormats R ecommandations, et communiqué de presse WITSA : l'industrie de l'ICT (Information and Communication Technology) (Technologie de l'Information et de la Communication) s'oppose au décryptage des portes dérobées.

4 La question est au cœur d'un cas récent dans une Cour fédérale des É-U pour le district central de Californie impliquant le FBI et Apple.

et leurs activités en ligne. Nous encourageons le développement ouvert et la grande disponibilité des technologies de sécurité de données.

- **Confiance.** La confiance des utilisateurs est essentielle à la croissance et à l'évolution continues d'Internet, et un nombre croissant d'utilisateurs réalisent la valeur de l'utilisation d'applications et services sécurisés et qui respectent la confidentialité. Nous encourageons la fourniture de mécanismes fiables pour l'authentification, la confidentialité et l'intégrité des données comme composantes techniques essentielles pour des produits et services fiables. Nous pensons aussi que des cadres réglementaires doivent soutenir les droits des individus, y compris le droit du respect à la vie privée.

- **Cryptage.** Le cryptage devrait être la norme pour tout le trafic Internet. Œuvrer à cet objectif est un complément important aux efforts continus de la communauté technique pour s'attaquer à la surveillance de plus en plus envahissante. Les concepteurs et développeurs de produits et services numériques sont vivement encouragés à s'assurer que les données des utilisateurs, qu'elles soient stockées ou communiquées, sont cryptées par défaut. Dans la mesure du possible, les solutions de cryptage de bout en bout devraient être disponibles. De plus, les opérateurs de réseaux et de services sont encouragés à déployer le cryptage là où il n'est pas encore déployé, et il est instamment demandé aux administrateurs de politique de pare-feu de permettre le trafic crypté.

- **Technologies inviolables.** En soutien au cryptage, la « Tamper-resistant technology » (Technologie inviolable) doit continuer à être développée et à être mise en œuvre. Les gouvernements ne doivent pas exiger la conception de vulnérabilités dans les outils de technologies ou services. De même, les gouvernements ne doivent pas exiger que les outils, technologies ou services soient conçus ou développés pour permettre à des tiers l'accès au contenu de données cryptées. Les gouvernements doivent aussi soutenir le travail des chercheurs et d'autres acteurs dans le domaine de la sécurité à identifier et divulguer de manière responsable les vulnérabilités de sécurité et de confidentialité de la technologie.

- **Déploiement.** Le renforcement du déploiement de mécanismes de sécurité, tels que le cryptage, entraînera des défis dans la conception, le développement, la gestion et l'exploitabilité de gestion de réseau. La gestion de réseau, la détection des intrusions et la prévention contre les spams seront confrontées à de nouvelles obligations fonctionnelles, et de nouveaux enjeux économiques et de politique sont à prévoir.

- **Solutions multipartites.** Les criminels peuvent communiquer confidentiellement et anonymement. Résoudre les répercussions exige des actions concertées de multiples parties prenantes. Internet Society réaffirme son engagement à faciliter l'implication de toutes les parties prenantes et à jouer un rôle actif et techniquement informé dans le développement de solutions.

De plus, Internet Society a signé la pétition « Secure the Internet » (sécuriser Internet)[5] pour montrer son soutien aux principes de la pétition, c.à.d. que les gouvernements ne doivent pas :

- Interdire ou limiter l'accès de l'utilisateur au cryptage sous quelque forme que ce soit ou interdire sa mise en œuvre ou l'utilisation du cryptage par catégorie ou type.
- Exiger la conception ou mise en place de portes dérobées ou vulnérabilités dans les outils, les technologies ou les services.
- Exiger que les outils, les technologies ou les services soient conçus ou développés pour permettre à des tiers l'accès aux données non cryptées ou aux clés de cryptage.
- Rechercher à affaiblir ou détruire les standards de cryptage ou intentionnellement influencer la création de normes de cryptage, sauf pour promouvoir un plus haut niveau de sécurité des informations.
- Exiger des outils, normes, technologies ou algorithmes de cryptage non sécurisés.
- Par des accords publics ou privés, contraindre ou faire pression sur une entité à s'engager dans une activité incompatible avec les principes ci-dessus énoncés.

Ressources supplémentaires

L'Internet Society a publié plusieurs articles et du contenu supplémentaire en rapport avec cette question. Ces documents sont disponibles en libre accès sur le site web d'Internet Society et beaucoup sont disponibles sur notre page principale de cryptage à https://www.internetsociety.org/encryption

Communiqués d'Internet Society

- Internet Society répond aux rapports du gouvernement américain sur le contournement de la technologie de cryptage, https://www.internetsociety.org/news/internet-society-responds-reports-us-government's-circumvention-encryption-technology
- L'Internet Society félicite l'Internet Architecture Board pour leur recommandation sur le cryptage par défaut pour Internet, https://www.internetsociety.org/news/internet-society-commends-internet-architecture-board-recommendation-encryption-default
- La soumission d'Internet Society au Rapporteur Spécial des Nations Unies sur la Protection et la Promotion du Droit à la liberté d'expression et d'opinion en matière d'utilisation de cryptage et d'anonymat des communications numériques, http://www.internetsociety.org/doc/internet-society-submission-un-special-rapporteur-protection-and-promotion-right-freedom

5 Consulter https://www.securetheinternet.org/.

Blog

- Liberté de parole : repenser le rôle du cryptage, https://www.internetsociety.org/blog/2013/05/freedom-speech-rethinking-role-encryption

- Les portes dérobées du cryptage diminuent la confiance dans Internet, https://www.internetsociety.org/blog/tech-matters/2015/05/encryption-backdoors-decrease-trust-internet

- Solide appui de David Kaye, Rapporteur Spécial des Nations Unies pour l'anonymat et le cryptage, http://www.internetsociety.org/blog/public-policy/2015/06/strong-support-un-special-rapporteur-david-kaye-anonymity-and-encryption

- « No keys under the doormat please » (pas de clés sous le paillasson SVP), https://www.internetsociety.org/blog/public-policy-tech-matters/2015/08/no-keys-under-doormat-please

- Le conflit fondamental entre la sécurité et la vie privée (et la proposition par le Royaume-Uni d'interdire le cryptage « UK Encryption Ban ») , https://www.internetsociety.org/blog/public-policy/2015/01/fundamental-tension-between-safety-and-privacy-and-uks-proposed

- Internet Society soutient l'initiative « Let's Encrypt » (Cryptons) pour augmenter le cryptage de bout en bout, https://www.internetsociety.org/blog/tech-matters/2015/10/isoc-supports-lets-encrypt-initiative-increase-end-end-encryption

- Imaginez un monde crypté ! Un atelier à IGF (Internet Governance Forum), https://www.internetsociety.org/blog/tech-matters-public-policy/2015/11/imagine-encrypted-world-workshop-igf-2015

- Le cryptage et le respect des lois : objectif confiance, https://www.internetsociety.org/blog/tech-matters-public-policy/2015/12/encryption-and-law-enforcement-aiming-trust

- Let's Encrypt participe au service public bêta pour augmenter le cryptage sur Internet, https://www.internetsociety.org/blog/tech-matters/2015/12/lets-encrypt-enters-public-beta-increase-encryption-internet

- Internet Society signe la pétition en ligne « Secure the Internet » (Sécuriser Internet), http://www.internetsociety.org/blog/tech-matters/2016/02/internet-society-signs-secure-internet-online-petition

- Les portes dérobées du cryptage se présentent sous toutes sortes de formes – En réaction à la lettre d'Apple à ses clients, https://www.internetsociety.org/blog/public-policy/2016/02/encryption-backdoors-come-all-guises-reacting-apples-customer-letter

Documents et rapports de l'atelier

- Entraves au déploiement : scruter les potentielles différences entre l'infrastructure développée et le développement, https://www.iab.org/wp-content/IAB-uploads/2015/08/MaRNEW_1_paper_27.pdf