Cryptage

Briefing sur la politique publique de l'Internet Society

11 août 2022

Introduction

Nous sommes entourés de technologies de cryptage. Le cryptage 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 cryptage 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 cryptage, c'est-à-dire le processus de brouillage ou de chiffrement 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 cryptage 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 les données stockées, la clé est généralement cryptée à l'aide d'un code PIN ou d'un mot de passe connu uniquement du propriétaire de l'appareil.

Le cryptage et les techniques associées sont également utilisés pour développer une sécurité renforcée des transactions financières et pour protéger les communications privées des 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). Elles font partie des protocoles qui apportent la preuve que les messages ont été envoyés et reçus (non-répudiation).

Considérations clés

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

- **Le cryptage symétrique** utilise une clé identique pour crypter et décrypter le message. L'expéditeur et le destinataire ont tous deux accès à la même clé. Bien que le cryptage 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 cryptage asymétrique**, également appelé « cryptage à clé publique », est une forme de cryptage unidirectionnelle. Les clés sont fournies par paires, et il n'est possible de décrypter les informations qui ont été cryptées avec la clé publique qu'à l'aide de la clé privée correspondante. Le destinataire publie une clé publique afin que l'expéditeur puisse crypter ses données. Le destinataire utilise ensuite une clé privée pour décrypter 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 cryptage à clé publique est plus sûr que le cryptage symétrique, car il n'est pas nécessaire de transférer la clé.

- **Le cryptage de bout en bout (E2E)** désigne toute forme de cryptage par laquelle seuls l'expéditeur et le destinataire prévu peuvent lire le message. L'aspect le plus important du cryptage de bout en bout est qu'aucun tiers, même la partie qui fournit le service de communication, n'a connaissance de la clé de cryptage. Le cryptage de bout en bout comprend par exemple les protocoles Pretty Good Privacy (PGP) et Off-the-Record Messaging (OTR). Les services de communication à cryptage de bout en bout comprennent par exemple iMessage d'Apple, Signal, ProtonMail, WhatsApp et Threema. L'Electronic Frontier Foundation a publié un guide « Surveillance Self Defense »[1] qui fournit des informations et des kits d'outils sur les fonctionnalités de divers services et appareils.

- **Le cryptage de données statiques** désigne toute forme de cryptage 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 cryptage s'applique dans le cadre d'une approche à plusieurs niveaux. Par exemple, un utilisateur crypte 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.

1 https://ssd.eff.org/fr

Il est important de noter qu'avec le cryptage, 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 – soient exposées en texte clair.

Défis

La disponibilité généralisée du cryptage, 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 cryptage 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 cyberharcèlement 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 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 leur liberté d'expression et de leur 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 sur Internet et à assurer la poursuite de l'essor d'Internet en tant que moteur de l'innovation technique et des avantages économiques et sociaux.

- **Le dilemme entre la sécurité et la confidentialité.** Les débats politiques sur le cryptage 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

2 https://www.internetsociety.org/fr/collaborativesecurity/

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.

- **Les portes dérobées du cryptage.** Cette expression désigne l'idée selon laquelle un outil peut aider un tiers autorisé à accéder à des données cryptées et à les décrypter sans avoir besoin 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 les 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.** Dans le contexte du cryptage, les technologies inviolables sont conçues afin que des attaquants ne puissent pas facilement modifier les appareils, les applications ou les données, et que toute altération soit évidente. Utilisées en conjonction avec le cryptage, 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 cryptage, 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

3 Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications, IAB Statement on Internet Confidentiality, W3C TAG Finding: End-to-End Encryption and the Web, W3C TAG Finding: Securing the Web, https://www.m3aawg.org/news/keys-under-doormats-authors-receive-m3aawg-jd-falk-award-for-clarifying-insecurity-of.

également présenter des difficultés pour les forces de l'ordre qui tentent d'accéder aux communications et aux données des suspects.[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 et leurs activités en ligne. Nous encourageons le développement ouvert et la grande disponibilité des technologies de sécurité des 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 au respect à la vie privée.

- **Cryptage.** Le cryptage devrait être la norme pour tout le trafic Internet. 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, soient cryptées par défaut. Dans la mesure du possible, le cryptage de bout en bout devrait être disponible.

- **Technologies inviolables.** En soutien au cryptage, les technologies inviolables doivent continuer à être développées et mises en œuvre. Les gouvernements ne doivent pas exiger la conception de vulnérabilités dans les outils, 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 d'accéder au contenu de données cryptées.

4 https://www.cnbc.com/2016/03/29/apple-vs-fbi-all-you-need-to-know.html

- **Divulgation responsable des vulnérabilités.** Les gouvernements doivent soutenir le travail des chercheurs et d'autres acteurs dans le domaine de la sécurité afin d'identifier et de divulguer de manière responsable les vulnérabilités de sécurité et de confidentialité. Ils doivent éviter de créer ou de stimuler un marché pour les vulnérabilités « zero-day ».

- **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. L'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.

Rassembler les parties prenantes mondiales

En 2020, l'Internet Society a rejoint avec fierté Global Partners Digital et le Center for Democracy and Technology en tant que membre fondateur de la Global Encryption Coalition, qui compte désormais plus de 300 membres organisationnels et individuels, et qui a accueilli la première Journée mondiale du cryptage le 21 octobre 2021.

L'Internet Society a signé la pétition « Secure the Internet » (sécuriser Internet)[5] pour montrer son soutien aux principes de la pétition, à savoir 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.

5 https://www.securetheinternet.org/

- 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.

L'Internet Society continue de prêter sa voix aux lettres ouvertes et aux coalitions de parties prenantes en faveur d'un cryptage fort et fiable. Vous trouverez ici une archive actualisée de ces déclarations: https://www.internetsociety.org/open-letters/

Ressources supplémentaires

Les fiches et documents d'information de l'Internet Society liés à ce problème sont disponibles gratuitement sur le site Web de l'Internet Society, et vous en trouverez un bon nombre sur notre page de ressources de cryptage: https://www.internetsociety.org/fr/issues/encryption/resources/

Les communiqués de presse et la couverture médiatique liés au cryptage de l'Internet Society sont disponibles sur notre page de centre média: https://www.internetsociety.org/fr/newsroom/?tx_category=cryptage

Vous trouverez les articles de l'Internet Society sur le cryptage sur notre page d'articles de blog: https://www.internetsociety.org/fr/blog/?tx_category=cryptage