L'analyse côté client

Qu'est-ce que c'est ?

Pourquoi menace-t-elle la confidentialité et la fiabilité des communications ?

Le chiffrement est une technologie conçue pour aider les utilisateurs d'Internet à garantir la confidentialité et la sécurité de leurs informations et de leurs communications. Le processus de chiffrement brouille les informations, afin que celles-ci ne puissent être lues que par quelqu'un qui dispose de la « clé » pour déchiffrer ces informations. Le chiffrement protège les activités du quotidien telles que la gestion bancaire et les achats en ligne. Il évite également que des données soient volées en cas de piratage de données, et permet de s'assurer que les messages confidentiels le restent. Le chiffrement est également crucial pour protéger les communications des forces de l'ordre, du personnel militaire et, de plus en plus, des intervenants en cas d'urgence.

Le chiffrement de bout en bout (en anglais, end-to-end ou E2E) — dans le cadre duquel les clés nécessaires au déchiffrage d'une communication chiffrée sont uniquement stockées sur les appareils qui communiquent — assure le meilleur niveau de sécurité et de fiabilité, car sa conception ne permet qu'au destinataire visé de détenir la clé permettant de déchiffrer le message. Le chiffrement E2E est un outil crucial pour assurer la sécurité et la confidentialité des communications. L'analyse du message, même si elle a lieu « côté client », détruit le modèle de chiffrement E2E et nuit fondamentalement à la confidentialité attendue par les utilisateurs.

Qu'est-ce que l'analyse côté client ?

L'analyse côté client est un terme générique faisant référence aux systèmes qui analysent les données du message (ex. : texte, images, vidéos, fichiers) pour voir si elles existent dans une base de données de contenu répréhensible avant l'envoi du message à son destinataire. Par exemple, votre logiciel anti-virus peut y avoir recours pour trouver et désactiver des logiciels malveillants sur votre ordinateur.

Tandis que d'importants fournisseurs de plateforme mettent en œuvre un chiffrement E2E plus massif et que certaines agences de forces de l'ordre demandent à obtenir l'accès aux données de messages pour mieux identifier et empêcher le partage de données à caractère répréhensible,[1] l'analyse côté client pourrait devenir le mécanisme de prédilection pour lutter contre les données répréhensibles partagées sur des services à chiffrement E2E, sans en compromettre le chiffrement.

Cependant, l'analyse côté client compromettrait la confidentialité et la sécurité auxquels les utilisateurs s'attendent et se fient. En empêchant les données du message de rester privées entre l'émetteur et le destinataire, l'analyse côté client détruit le modèle de confiance du chiffrement E2E. La complexité que cela

1 https://www.newamerica.org/oti/press-releases/open-letter-law-enforcement-us-uk-and-australia-weak-encryption-puts-billions-internet-users-risk/

vient ajouter limite également la fiabilité du système de communication, et risque d'empêcher des messages authentiques de parvenir à leur destinataire.

L'analyse côté client pour empêcher le partage de données à caractère répréhensible

Lorsqu'elle vise à empêcher le partage de données à caractère répréhensible, l'analyse côté client fait généralement référence à une façon dont un logiciel sur les appareils des utilisateurs (souvent désignés sous le terme de « clients », notamment les smartphones, les tablettes ou les ordinateurs) crée des « empreintes » numériques uniques[2] pour les données de l'utilisateur (nommés « hachages »). Le logiciel compare ensuite ces empreintes aux empreintes numériques de données répréhensibles connues, comme des logiciels malveillants (malwares), des images, des vidéos ou des graphiques.[3] En cas de correspondance, le logiciel peut empêcher ce fichier d'être envoyé, et/ou signaler cette tentative à un tiers, souvent à l'insu de l'utilisateur.

Comment fonctionne l'analyse côté client ?

Il existe deux méthodes de base d'analyse côté client pour rechercher des données répréhensibles sur un service de communication à chiffrement E2E, l'une étant la comparaison des empreintes numériques sur l'appareil de l'utilisateur et l'autre la comparaison des empreintes numériques sur un serveur distant (les données restant sur l'appareil).

1. **Les comparaisons effectuées sur l'appareil de l'utilisateur (correspondance avec des empreintes numériques locales)**
   L'application sur l'appareil d'un utilisateur (téléphone, tablette ou ordinateur) comprend une base de données complète des empreintes numériques fonctionnellement uniques à identifier. Les données que l'utilisateur est sur le point de chiffrer et d'envoyer dans un message sont converties en une empreinte numérique avec les mêmes techniques que celles utilisées pour les empreintes numériques de la base de données complète. En cas de correspondance, le message ne pourra pas être envoyé, et un tiers désigné (par exemple, les forces de l'ordre, une agence de sécurité nationale ou le fournisseur des services de filtre) pourra en être informé.

2. **Les comparaisons effectuées sur un serveur**
   La tenue à jour d'une base de données complète et la réalisation de l'analyse en temps réel peut s'avérer complexe sur l'appareil de l'utilisateur. L'autre solution est donc de transférer les empreintes numériques des données d'un utilisateur vers un serveur où sera effectuée la comparaison avec une base de données centrale.

Les problèmes posés par l'analyse côté client des données à caractère répréhensible

Lorsque la comparaison des empreintes numériques est effectuée sur un serveur distant, cela peut permettre au fournisseur d'accès, ainsi qu'à toute personne avec qui le fournisseur accepte de partager ces informations, de surveiller et de filtrer les données que souhaite envoyer l'utilisateur. Lorsque la comparaison est effectuée sur l'appareil de l'utilisateur, si des tiers sont informés en cas de découverte de données inappropriées, le problème est le même. Cela va fondamentalement à l'encontre de la raison d'être du chiffrement E2E. Les communications à chiffrement E2E privées et sécurisées entre deux parties, ou au sein d'un groupe, ont vocation à rester privées. Si des personnes suspectent que leurs données sont analysées, elles peuvent s'auto-censurer, passer à un autre service sans analyse côté client ou utiliser un autre moyen de communication.

2 Il serait possible de développer un système où les empreintes numériques ne seraient pas aussi uniques, ce qui engendrerait l'utilisation de la même empreinte numérique par différents contenus. Cependant, dans les cas où de faux positifs risquent d'entraîner l'utilisation de ressources importantes (notamment une intervention policière), les concepteurs des systèmes d'analyse côté client chercheront à rendre les empreintes aussi uniques que possible.

3 L'analyse côté client n'est que l'une des manières proposées par les forces de l'ordre ou les agences de sécurité pour obtenir l'accès aux communications chiffrées des utilisateurs. Pour plus d'informations, consultez : https://www.internetsociety.org/resources/doc/2018/encryption-brief/

Cela crée des vulnérabilités que peuvent exploiter des criminels : L'ajout d'une fonctionnalité d'analyse côté client augmente la surface d'attaque avec la création de moyens supplémentaires d'interférer dans les communications en manipulant la base contenant les données à caractère répréhensible. Des personnes mal intentionnées ayant la possibilité d'ajouter des empreintes numériques dans la base de données et de recevoir des notifications en cas de correspondance avec ces empreintes auraient la possibilité de surveiller les données d'un utilisateur spécifique avant qu'elles ne soient chiffrées et envoyées. Cela leur permettrait de surveiller à qui, quand et où certaines données ont été transmises. Ces empreintes pourraient inclure les mots de passe fréquemment utilisés ou d'autres informations, permettant ainsi des attaques telles que le piratage psychologique, l'extorsion ou le chantage. En utilisant les fonctionnalités de blocage d'un système, des criminels pourraient également décider d'empêcher des utilisateurs d'envoyer des données spécifiques. Cela pourrait servir à cibler des utilisations légitimes, notamment en nuisant aux communications des forces de l'ordre, des intervenants en cas d'urgence ou du personnel de la sécurité nationale.

Cela crée de nouveaux défis techniques et procéduraux : si les comparaisons sont effectuées sur l'appareil de l'utilisateur, tenir à jour la base de données de références complète sur chaque appareil représente déjà de nombreux défis. Parmi ces défis figurent des contraintes procédurales potentielles (ex. : le processus permettant d'ajouter ou de supprimer des empreintes de données dans la base de données ; qui contrôle la base de données ou peut y accéder), la bande passante nécessaire pour transmettre les versions mises à jour de la base de données et la puissance de traitement sur les appareils nécessaire pour effectuer la comparaison en temps réel. Il existe également d'autres considérations à prendre en compte, notamment l'exposition potentielle de la base de données de référence lors de son installation sur l'appareil client, susceptible d'offrir aux criminels des informations sur le système d'analyse. Si les comparaisons sont effectuées sur un serveur central, l'empreinte numérique des données que l'utilisateur cherche à envoyer sera accessible à toute personne contrôlant le serveur central, que ces données soient « répréhensibles » ou non aux yeux de la partie chargée de la surveillance. Cela engendre un nouvel ensemble de problèmes relatifs à la sécurité et à la confidentialité des utilisateurs, avec le risque d'exposer des informations sur leur activité à toute personne ayant accès au serveur.

Risques de dérives et d'utilisation à d'autres fins : une fois mises en œuvre, les techniques d'analyse côté client pourraient ne pas être restreintes à l'identification des pires données, notamment à caractère pédopornographique ou terroriste (les deux exemples les plus souvent mis en avant pour justifier leur utilisation). Elles pourraient par exemple permettre d'obtenir des informations à des fins publicitaires, d'empêcher le partage de données légitimes, voire de bloquer les communications entre des utilisateurs (comme les opposants politiques). Il est difficile de restreindre la base de données uniquement aux empreintes d'images, de vidéos ou d'URL relatives à des activités illégales, comme certains le proposent. En créant des empreintes numériques pour davantage de données afin de pouvoir établir des comparaisons avec les empreintes numériques des données de l'utilisateur, toute personne responsable de la base de données peut surveiller n'importe quel type de contenu. De plus, un système d'analyse côté client pourrait être développé pour surveiller les données textuelles des messages envoyés, ce qui engendrerait encore plus de risques pour notre sécurité et notre vie privée.

Les criminels utiliseront un autre service : il existe des systèmes de communications à chiffrement E2E en dehors de la juridiction de tout gouvernement. Un criminel réellement déterminé pourrait se passer des services dont il sait qu'ils ont recours à une analyse côté client pour éviter d'être repéré. Les criminels pourraient également modifier les données à caractère répréhensibles, notamment en changeant l'empreinte numérique, et éviter ainsi la détection par le système d'analyse côté client.

Conclusion

La lutte contre le partage de données à caractère terroriste ou pédopornographique est une cause importante, mais cela ne peut pas être effectué d'une manière qui affaiblirait la sécurité de tous les utilisateurs en modifiant l'infrastructure de communication pour potentiellement surveiller les échanges de tout un chacun. Le chiffrement E2E permet à des milliards d'utilisateurs dans le monde entier de communiquer en

toute sécurité et de façon confidentielle,[4] et des plateformes majeures continuent d'avancer dans cette direction afin de soutenir la fiabilité de leurs plateformes et services.[5] L'analyse côté client des services de communications à chiffrement E2E ne constitue pas une solution appropriée pour le filtrage des données à caractère répréhensibles, et cela s'applique également à toute méthode qui nuirait à la base du caractère confidentiel et fiable des communications desquelles nous dépendons.

Références pour en savoir plus

Internet Society. Juin 2018. *Encryption Brief.* https://www.internetsociety.org/resources/doc/2018/encryption-brief/

Matthew Green. Décembre 2019. *Can end-to-end encrypted systems detect child sexual abuse imagery?* https://blog.cryptographyengineering.com/2019/12/08/on-client-side-media-scanning/

Electronic Frontier Foundation. Novembre 2019. *Why Adding Client-Side Scanning Breaks End-To-End Encryption.* https://www.eff.org/deeplinks/2019/11/why-adding-client-side-scanning-breaks-end-end-encryption

4 https://telegram.org/blog/200-million ; https://www.newsweek.com/whatsapp-facebook-passes-two-billion-users-pledges-encryption-support-1486993

5 https://www.facebook.com/notes/mark-zuckerberg/a-privacy-focused-vision-for-social-networking/10156700570096634/