L'analyse côté client : cas de l'UE

Qu'est-ce que c'est et pourquoi menace-t-elle la confidentialité et la fiabilité des communications ?

Décembre 2023

Résumé et recommandations

Le Parlement européen examine la « proposition de règlement établissant des règles en vue de prévenir et de combattre les abus sexuels sur enfants » (proposition CSA). Certaines discussions ont porté sur le cryptage de bout en bout ainsi que sur l'utilisation de technologies d'analyse côté client. L'Internet Society cherche à contribuer à ce débat, car le recours à l'analyse côté client ne permettrait plus au cryptage de bout en bout d'offrir le même niveau de confiance, ce qui mettrait en danger la sécurité et la vie privée des internautes européens.

Recommandations

L'Internet Society formule les recommandations suivantes sur la base de la proposition de la Commission européenne :

1. Que le Comité européen mette en place des garanties pour le cryptage de bout en bout.
2. Que le Comité européen interdise l'utilisation de technologies d'analyse pour une surveillance généralisée, y compris l'analyse côté client.

L'analyse côté client met à mal la confiance offerte par le cryptage de bout en bout

Une idée fausse très répandue est que l'on peut disposer d'un cryptage de bout en bout (E2EE) robuste tout en recourant simultanément à une analyse côté client. Cette théorie erronée repose sur l'idée que l'analyse a lieu *avant* le début du processus de cryptage. Même si cela est vrai d'un point de vue formel, la réalité est que l'analyse rend inutile le cryptage, crée de nouveaux risques de sécurité et met en danger la vie privée des Européens.

Si nous sommes tous d'accord sur le fait que le cryptage est une technologie qui nous protège, nous devons comprendre que l'analyse côté client invalide son objectif.

Qu'est-ce que l'analyse côté client ?

L'analyse côté client ou CSS (de l'anglais Client-Side Scanning) est un terme générique qui désigne les systèmes qui analysent les données du message (ex. : texte, images, vidéos, fichiers) afin de rechercher des correspondances ou des similitudes avec une base de données de contenus répréhensibles avant l'envoi du message à son destinataire.

Quels sont les risques liés à l'analyse côté client ?

Les principaux fournisseurs de plateformes mettent de plus en plus souvent en œuvre un cryptage de bout en bout pour leurs utilisateurs afin d'améliorer la sécurité, la confidentialité et la confiance. En même temps, les forces de l'ordre cherchent de plus en plus souvent à accéder au contenu des messages pour empêcher le partage de contenus répréhensibles.

Les entreprises qui proposent des technologies de CSS les présentent comme étant une solution. Elles prétendent offrir une technologie qui ne brise pas le cryptage, et ne le compromet nullement. Cependant,

> Briser le cryptage, revient à trafiquer une enveloppe pendant qu'elle transite par un bureau de poste. L'analyse côté client revient à lire la lettre au fur et à mesure qu'elle est rédigée. Avec l'analyse côté client, l'enveloppe n'est pas trafiquée, mais le résultat est le même : l'accord de confidentialité est enfreint.

En outre, comme l'explique l'avis conjoint de l'EDPB et du CEPD[1], la CSS « peut être facilement contournée en cryptant le contenu à l'aide d'une application distincte ». Cela signifie que ces techniques ouvrent la porte à une mesure disproportionnée, qui met en danger chaque citoyen, sans apporter de véritable solution au problème.

Le cryptage de bout en bout est un outil essentiel pour assurer la sécurité et la confidentialité des communications. La CSS va à l'encontre de l'objectif du cryptage de bout en bout et enfreint fondamentalement la confidentialité à laquelle les utilisateurs s'attendent lorsqu'ils utilisent des outils de communication à E2EE. Cet abus de confiance :

[1] « Avis conjoint 04/2022 de l'EDPB et du CEPD sur la proposition de règlement du Parlement européen et du Conseil établissant des règles en vue de prévenir et de combattre les abus sexuels sur les enfants », 28 juillet 2022, https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-042022-proposal_en

- **Présente un risque sérieux pour les droits fondamentaux,** comme indiqué dans l'avis conjoint de l'EDPB et du CEPD.
- **Réduit la confiance dans l'écosystème Internet.** La perte de confiance est préjudiciable à l'économie numérique et pourrait mettre à mal les ambitions de l'UE pour la décennie numérique.
- **Porte atteinte à la sécurité des communications et des services en ligne**, comme l'a remarqué la commission mixte de la justice du Parlement irlandais.[2]

Conclusion

Les partisans de l'analyse côté client considèrent cette technologie comme une solution pour identifier les contenus répréhensibles dans les environnements E2EE. Cependant, ce document a expliqué comment la CSS enfreint l'accord de confiance du cryptage de bout en bout et les dangers qu'elle présente. Pour plus d'informations sur le fonctionnement de la CSS et ses défauts inhérents, la fiche d'information de l'Internet Society sur l'analyse côté client peut servir de ressource pour des discussions politiques détaillées.[3] Nos informations[4] sur ce qu'est le cryptage et sur la manière dont il contribue à la sécurité et à la confidentialité peuvent également constituer une ressource précieuse.

À propos de l'Internet Society

L'Internet Society est une organisation caritative mondiale fondée en 1992 par certains des pionniers d'Internet. Nous pensons qu'Internet est une force bénéfique et nous œuvrons pour un Internet ouvert, connecté à l'échelle mondiale, sécurisé et digne de confiance qui profite à tous. Avec 110 chapitres actifs sur six continents, dont 28 en Europe, et plus de 100 000 utilisateurs individuels soutenant nos activités, l'Internet Society est une partie prenante importante et un interlocuteur fiable et techniquement informé de la société civile pour les questions relatives à la gouvernance de l'Internet.

[2] "Political Contribution on Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL laying down rules to prevent and combat child sexual abuse", Houses of the Oireachtas, Joint Committee on Justice, March 2023, https://opac.oireachtas.ie/Data/Library3/Documents%20Laid/2023/pdf/MTQzZG9jc2xhaWQzMDAzMjAyM18qMzAwMzIzXzEyMjEzMA==.pdf

[3] « Fiche d'information : L'analyse côté client » Internet Society, 26 septembre 2022, https://www.internetsociety.org/fr/resources/doc/2020/lanalyse-cote-client/

[4] « Qu'est-ce que le cryptage ? » Internet Society, 14 juillet 2022, https://www.internetsociety.org/issues/encryption/what-is/