La proposition du fantôme

De quoi s'agit-il, quels sont ses impacts, et peut-elle atteindre ses objectifs ?

Qu'est-ce que la proposition dite « du fantôme », et pourquoi devrions-nous nous en préoccuper ?

Au moins un gouvernement a récemment proposé, afin de faciliter l'accès à des messages chiffrés de bout en bout, une modification des technologies, afin qu'un tiers puisse écouter des conversations chiffrées, sans être repéré. Les partisans de cette mesure affirment qu'elle peut répondre à des besoins policiers ou de sécurité nationale sans affaiblir le chiffrement utilisé pour les messages. Cependant, cette proposition du fantôme créerait des vulnérabilités de sécurité systémiques dans les services de communication confidentielle, et altérerait fondamentalement la relation de confiance entre les utilisateurs et les fournisseurs de services.

Qu'est-ce que la « proposition du fantôme », et quel est son impact sur la sécurité et la confidentialité ?

Le terme de « proposition du fantôme » fait référence à une proposition dans laquelle les fournisseurs d'applications de messagerie à chiffrement de bout en bout disposent d'un moyen d'ajouter un tiers dans des échanges chiffrés à l'insu des autres parties. Cela requiert la coopération du fournisseur du service de communication. En tirant parti des fonctionnalités de messagerie de groupe de nombreux services, un utilisateur serait ajouté « silencieusement » à une conversation, en supprimant la notification habituelle en cas d'ajout d'un nouvel utilisateur à un groupe.

La sécurité d'un service de communication chiffrée est basée sur la gestion efficace et transparente des clés de chiffrement (qui garantit que seuls les destinataires souhaités détiennent les clés permettant de déchiffrer les messages). Pour que le chiffrement assure le niveau de confidentialité attendu par les utilisateurs, la totalité du système doit veiller à ce que seuls les destinataires souhaités aient accès aux clés nécessaires (qui permettent le déchiffrement des données).

Les partisans de la proposition du fantôme soutiennent que le fait d'inclure un tiers à une conversation de façon dissimulée est préférable aux autres moyens permettant d'obtenir un accès exceptionnel, car cette méthode ne remet pas en cause les mécanismes de chiffrement. Cependant, même si la cryptographie utilisée pour chiffrer les données des messages n'est pas affectée, cela introduirait une faille de sécurité dans l'application de messagerie utilisée par tous les utilisateurs, à savoir, la compromission de la gestion des clés de chiffrement qui permettrait à des utilisateurs non-autorisés d'accéder aux données de communications chiffrées.

CC BY-NC-SA 4.0

De plus, en ce qui concerne la fiabilité d'un service, si un système de messagerie ne tient pas ses promesses en matière de confidentialité, l'aspect spécifique des services qui a été modifié n'a pas d'importance. Le système n'assure simplement pas la protection qu'en attend l'utilisateur.

La proposition du fantôme dans les faits : des participants silencieux dans les discussions de groupe

Dans un système de messagerie de groupe à chiffrement de bout en bout (E2E), le fournisseur de services gère la distribution des clés aux utilisateurs. Ce service est dissimulé aux utilisateurs finaux dans une vaste mesure, afin de simplifier l'expérience utilisateur ; toutefois, si quelqu'un est ajouté dans une discussion de groupe, les utilisateurs en sont informés. La messagerie de groupe en E2E se base sur ce service pour veiller à ce que les utilisateurs souhaités soient ajoutés dans un message de groupe, et qu'aucun utilisateur non souhaité ou inconnu, pas même le fournisseur de services lui-même, ne soit en mesure de déchiffrer les communications.

La distribution des clés est complexe. Par exemple, un service de discussion chiffré doit également mettre à jour de manière sécurisée les clés d'un utilisateur lorsque celui-ci réinstalle l'application ou change d'appareil, s'il souhaite rester dans les mêmes groupes.

La proposition du fantôme modifie le processus de distribution des clés en distribuant secrètement des clés à des personnes ne faisant pas partie de la discussion de groupe, permettant ainsi à des membres du groupe non-autorisés de suivre la conversation. La proposition du fantôme nécessiterait également que les fournisseurs de service suppriment les notifications aux utilisateurs signalant que de nouvelles parties non-autorisées ont accès à leurs communications.

Les problèmes posés par la proposition du fantôme

Cette proposition compromet la mission du chiffrement E2E : les systèmes de communication « sécurisés » sont composés de nombreux éléments interdépendants, dont le chiffrement, qui est un élément essentiel mais qui n'est pas le seul élément important. La gestion des clés de chiffrement et la fiabilité globale du système sont des aspects cruciaux d'un système de communication E2E. Bien que la proposition du fantôme ne modifierait pas les algorithmes utilisés par les applications de messagerie à chiffrement de bout en bout pour chiffrer et déchiffrer les messages, elle introduirait une vulnérabilité de sécurité systémique dans ces services, qui aurait des conséquences négatives pour tous les utilisateurs, y compris les utilisateurs commerciaux et gouvernementaux. Cette proposition nuit à la gestion des clés et à la fiabilité du système ; par conséquent, les communications supposées être confidentielles entre l'émetteur et le destinataire peuvent ne plus l'être, et sont moins sécurisées.

Cette proposition crée une vulnérabilité que peuvent exploiter des criminels : pour que des tiers puissent être ajoutés secrètement à des communications, même s'il ne s'agissait d'atteindre qu'une seule cible, un fournisseur de services devrait modifier l'intégralité du service pour tous les utilisateurs afin de pouvoir activer cette fonctionnalité. Cela introduit une vulnérabilité intentionnelle dans le système qui, si elle est découverte, exploitée ou copiée, peut être utilisée par des tiers auxquels elle n'est pas destinée (notamment des criminels, des employés mal intentionnés ou des gouvernements hostiles) dans le but d'espionner des conversations.[1] Les communications à chiffrement E2E étant essentielles à tous les aspects de notre société, notamment pour la sécurité nationale, les forces de l'ordre et l'activité économique, le risque créé est inacceptable et inutile.

Cette proposition crée de nouveaux défis techniques et procéduraux : l'ajout d'une complexité technique supplémentaire au processus déjà complexe de gestion des clés de sécurité risque d'engendrer des vulnérabilités non souhaitées, qui pourraient être exploitées par des acteurs malveillants. La gestion efficace et sécurisée d'un accès dissimulé aux communications est une tâche très compliquée et potentiellement problématique. Des organisations, notamment des gouvernements, ont eu des difficultés à s'assurer que des données sensibles restaient sécurisées et confidentielles. Ces capacités devraient être sécurisées, non

1 « L'affaire d'Athènes » en est un exemple. https://spectrum.ieee.org/telecom/security/the-athens-affair

CC BY-NC-SA 4.0

seulement contre des criminels qui chercheraient à les exploiter, mais aussi contre des employés malveillants ou des puissances étrangères.

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 que l'on suspecte d'appliquer la proposition du fantôme pour éviter d'être repéré.

Risques de dérives et d'utilisation à d'autres fins : le concept derrière la proposition du fantôme n'est pas sélectif. Il introduit des vulnérabilités dans les protocoles d'échanges de clés et de notifications, et pourrait être utilisé de manières que ces partisans n'ont pas prévues (ex. : pour surveiller les journalistes, les partis politiques, etc.).

Conclusions

La proposition du fantôme requiert la création de failles systémiques dans des protocoles destinés au marché de masse et utilisés par les particuliers, les entreprises et les gouvernements. Elle augmente la vulnérabilité et la complexité des systèmes concernés, et augmente ainsi le risque que des développeurs introduisent accidentellement davantage de failles. Les gouvernements devraient abandonner la proposition du fantôme visant à accéder aux communications chiffrées, car le risque est trop important.

Références pour en savoir plus :

- Sharon Bradford Franklin, Andi Wilson Thompson. Mai 2018. *Open Letter to GCHQ on the Threats Posed by the Ghost Proposal.* https://www.lawfareblog.com/open-letter-gchq-threats-posed-ghost-proposal
- Matthew Green. Décembre 2018. *On Ghost Users and Messaging Backdoors* https://blog.cryptographyengineering.com/2018/12/17/on-ghost-users-and-messaging-backdoors/

CC BY-NC-SA 4.0