28.07.2023 – 08:00 Uhr

Sécurité d'un backup, test réussi ou presque

Bern (ots) -

Le nouveau protocole de sauvegarde de Whatsapp a été soumis à une analyse de sécurité exhaustive. Une faille a été identifiée, qui peut être résolue avec un mot de passe fort.

Chaque jour, plus de cent milliards de messages sont échangés sur Whatsapp. Le chiffrement de bout en bout assure leur confidentialité. Toutefois, jusqu'à récemment encore, la sauvegarde automatique des conversations n'offrait pas le même niveau de sécurité, car l'entreprise connaissait la clé personnelle des données stockées dans le cloud. " Le backup était totalement sécurisé, sauf vis-à-vis de Whatsapp ", indique la cryptographe Julia Hesse, qui est soutenue par le FNS et travaille à l'Institut de recherche IBM Research à Zurich.

C'est peut-être aussi pour cette raison que le service de messagerie a introduit fin 2021 un nouveau protocole de sauvegarde que Julia Hesse a maintenant examiné de près avec des collègues de l'ETH Zurich et de l'Université de Wuppertal. Selon cette étude, l'entreprise ne peut désormais plus accéder aux sauvegardes.

L'entreprise n'a pas accès à son propre coffre-fort

Pour l'analyse, l'équipe a créé un modèle formel décrivant toutes les exigences que doit satisfaire un système de sauvegarde sûr, telle qu'une longueur de clé suffisante. Elle a ensuite comparé ce modèle idéal avec le protocole effectivement utilisé. À cette fin, elle est allée chercher ses informations auprès de différentes sources, notamment dans les documents officiels publiés par Whatsapp et en discutant avec des membres de l'entreprise qui ont développé ce nouveau protocole. " Nous avons dû faire confiance aux indications données par l'entreprise, indique la chercheuse. Cependant, je ne vois aucun intérêt de leur part à ne pas dire la vérité. " Après tout, une analyse de sécurité externe supplémentaire est à l'avantage de l'entreprise.

Dans le nouveau système, la copie de la clé n'est plus conservée par l'entreprise comme auparavant, mais dans un ordinateur indépendant particulièrement sûr auquel l'entreprise n'a pas accès et dont le code ne peut plus être changé. Quiconque perd son smartphone devra utiliser un mot de passe pour accéder à cette clé et restaurer les conversations. " La clé est en quelque sorte déposée dans un coffre qui ne peut être ouvert qu'avec ce mot de passe ", explique Julia Hesse.

Les bienfaits de l'examen par les pairs

En outre, le protocole protège les sauvegardes contre ce qu'on appelle les attaques par force brute qui consistent à essayer autant de mots de passe qu'il faut jusqu'à trouver le bon. " Même lors d'une attaque puissante qui prendrait le contrôle des serveurs de Whatsapp, le système ne permet que dix essais - ensuite la clé est détruite. " Les données seraient alors aussi perdues pour l'utilisatrice ou l'utilisateur.

L'équipe a cependant découvert une faille potentielle dans cette fonction : en principe, le système supprime les anciennes versions du backup lorsqu'une nouvelle sauvegarde est réalisée, notamment lors d'un changement de mot de passe. " Une attaque de Whatsapp ou de l'extérieur pourrait assurer la conservation des anciennes versions, ce qui rendrait possibles dix essais supplémentaires pour chaque version encore existante ", explique la chercheuse. Mais le choix d'un mot de passe fort permet de réduire à néant cette faille. " Que l'agresseur ait dix ou deux cents essais revient au même si on utilise au moins huit caractères avec des caractères spéciaux et non pas son code postal. "

Le risque d'attaques potentielles n'augmente-t-il pas si le protocole de sécurité, y compris les failles potentielles, est publié en détail, comme cela a été fait dans cette étude ? " Dans la recherche, nous sommes désormais convaincus qu'une description formelle et accessible au public du protocole accroît la sécurité ", explique Julia Hesse. Cela permet à d'autres spécialistes de tout réexaminer ou de se pencher sur de nouveaux aspects. " C'est en quelque sorte un processus d'examen par les pairs gratuit bien plus précieux que si l'entreprise gardait le protocole secret. "

G. T. Davies et al.: Security Analysis of the WhatsApp End-to-End Encrypted Backup Protocol. Crypto IACR (2023)

Le texte de cet actu et de plus amples informations sont disponibles sur le site Internet du Fonds national suisse.

Contact:

Julia Hesse;
IBM Research Zurich;
Säumerstrasse 4;
8803 Rüschlikon;
Tél.: +41 43 538 72 79;
E-mail: juliahesse2@gmail.com