Faire confiance dans le brouillard

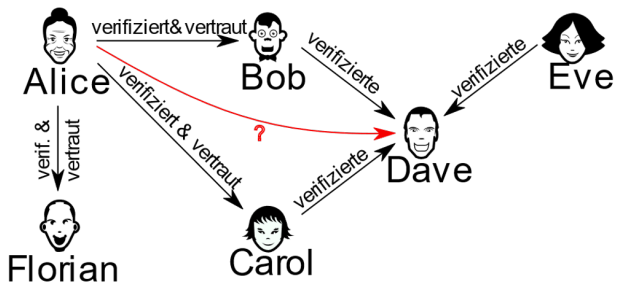
Au moins depuis les révélations d'Edward Snowden et l’entrée en vigueur de la nouvelle Loi fédérale sur la surveillance de la correspondance par poste et télécommunication (LSCPT), tout le monde sait que les communications privées n’existent pas a priori sur Internet. L'autoprotection par cryptage est donc recommandée.

Des clés publiques sont la condition nécessaire pour le cryptage, mais il est difficile de les obtenir en toute sécurité.
Non seulement les organisations publiques et privées se discréditent mutuellement par leur partenariat en matière de surveillance - ce qui les rend indignes de confiance pour la communication privée - , mais encore les exigences du milieu privé, où la communication par pseudonymes peut avoir son importance (par ex. pour séparer les identités professionnelles et sexuelles) sont aussi en conflit d’objectifs avec les systèmes d’enregistrement habituels. Ceux-ci tentent d’attribuer une identité précise à chaque personne. Dès lors, comment obtenir des clés pour protéger notre communication personnelle?

Cryptage opportuniste
Quand les deux parties sont en ligne en même temps, la méthode la plus simple est d’ajouter les clés cryptographiques au début de la communication. Cette méthode est aussi appelée cryptage opportuniste. Elle est efficace contre les agresseurs passifs qui accèdent aux données utiles uniquement par la lecture de la communication. Un agresseur actif qui peut intervenir dans un trafic de réseau pourrait toutefois modifier les données des clés lors de l’échange et remplacer les clés des participants par des clés de l’agresseur. Ainsi, l’agresseur pourra décrypter et modifier les données utiles.

Trust on First Use
Pour améliorer cela, il faut que le logiciel reconnaisse la clé. Si la clé du correspondant change, l’utilisateur en est alerté. Et même si l’agresseur n’intervient pas à chaque fois dans la communication, l’utilisateur en est au moins averti. Ce processus est aussi connu sous le nom Trust on First Use, car il faut faire confiance à la connexion au réseau lors de la première utilisation.

Trustwords
Il est évidemment aussi possible qu’un agresseur intervienne déjà lors du premier contact actif dans une connexion. On peut le découvrir en testant la clé par un autre canal de communication, par ex. en lisant les clés des e-mails sur le téléphone. Malheureusement, les clés sont des chiffres difficiles à manipuler. Pour en simplifier la lecture, la Schweizer pEp AG utilise un processus qui représente les clés par des TRUSTWORDS. Quand la voix du correspondant est reconnue au téléphone et que les bons TRUSTWORDS sont lus, on peut être sûr que la bonne clé a été échangée.



verifiziert : vérifie
vertraut : a confiance

Web of Trust
Ce qu'on appelle le Web of Trust est une alternative décentralisée traditionnelle pour vérifier les clés des personnes.
Le milieu social est intégré dans la vérification. Supposons qu'Alice ait déjà vérifié les clés de Bob, Carol et Florian et aimerait maintenant vérifier la clé de Dave. Si Bob, Carol et Eve ont déjà vérifié Dave et qu'Alice fait confiance à Bob et Carol, il suffit que Bob et Carol aient vérifié la clé de Dave. De tels certificats sont rassemblés avec Web of Trust et enregistrés sur ce qu'on appelle des serveurs de clés. Quand Alice veut contrôler une clé, son application cherche sur les serveurs de clés les certificats correspondants de personnes qu'Alice connaît et en qui elle a confiance.

Métadonnées
Pour vérifier des clés avec le Web of Trust, il faut connaître les clés que les personnes ont certifiées. Comme généralement ces certifications se font dans l'entourage d'une personne, on peut cartographier le milieu social des participants à partir de ces données de certification. Par conséquent celui qui utilise le Web of Trust pour protéger ses données de communication, exporte ses métadonnées: les données publiques du Web of Trust permettent de lire qui a (probablement) passé suffisamment de temps avec qui pour vérifier la clé.
Il est tout aussi important de protéger ces métadonnées que la communication. L'ancien directeur de la CIA et de la NASA, Michael Hayden, a admis que "We kill people based on metadata" – c'est-à-dire que les USA considèrent les métadonnées suffisamment révélatrices pour pouvoir décider d'assassiner des individus.
Malheureusement, il est techniquement beaucoup plus difficile de protéger les métadonnées que de crypter le contenu d'un flux de données.

Fog of Trust
À la Haute école spécialisée bernoise, nous travaillons avec différents partenaires européens au développement d'une procédure qui permet d'utiliser l'environnement social pour vérifier des clés sans les exporter. Comme avec le Web of Trust, les participants doivent certifier des clés, mais tous les certificats finissent sur un serveur sur le web. Avec le Fog of Trust, ils ne sont délivrés qu'aux détenteurs de clés. Si dans l'exemple ci-dessus Alice souhaite vérifier la clé de Dave, elle envoie une liste cryptée des personnes en qui elle a confiance (donc par ex. Bob, Carol et Florian). Il est important que Dave ne sache jamais à qui Alice fait confiance. Dave génère ensuite une preuve cryptographique qui montre à Alice combien de personnes de confiance ont certifié la clé de Dave (dans l'exemple, deux). Elle ne sait toutefois pas qui a certifié Dave.

Questions d'avenir
La gestion utilisable des clés représente un défi central pour la protection des données. Toute architecture de vérification des clés induit des structures de pouvoir au sein de la société, car elle règle la participation numérique. Cette problématique devrait aussi jouer un rôle dans la discussion concernant la privatisation d'une nouvelle architecture pour les documents d'identité électroniques (E-ID). La BFH soutient la discussion par sa compétence en matière de recherche et d'enseignement.

Auteur

Dr Christian Grothoff
Professeur d'informatique, BFH

Contact:
- christian.grothoff@bfh.ch

Infos:
- risis.bfh.ch

https://pixnio.com/de/landschaften/nebel/kiefer-baeume-wetter-nebel