SÉCURISER NOS COMMUNICATIONS : DE L'EMAIL À WHATSAPP, ET AU-DELÀ (PAR THOMAS BAIGNÈRES ET MATTHIEU FINIASZ, OLVID)

Lorsque Ray Tomlinson envoie "QWERTYUIOP" sur le réseau ARPANET en juillet 1971, il ne se doute probablement pas être à l'origine d'un système de communication qui sera utilisé par des milliards de personnes pendant plus de 40 ans. Aujourd'hui, 6 milliards d'adresses échangent plus de 150 millions d'emails chaque minute (dont ⅔ de propositions douteuses), en reposant sur des standards de communication dont l'origine précède la séparation des Beatles et l'invention de la cryptographie moderne.

En 1977, au MIT, Rivest, Shamir et Adleman (RSA) inventent le premier chiffrement à clé publique et la première signature numérique. Ils suggèrent alors d'utiliser leurs algorithmes pour sécuriser le « mail électronique » et les virements bancaires. Mais ce n'est qu'avec la démocratisation d'Internet dans les années 90 que les communications électroniques deviennent un outil business incontournable. La question du chiffrement des emails se pose alors réellement.

Deux standards émergent, PGP et S/MIME, dont la préoccupation principale est l'authentification de l'échange initial des clés cryptographiques permettant de chiffrer le contenu des emails et de garantir l'identité de l'envoyeur. Ces deux standards sont contraints de respecter le vieillissant protocole SMTP qui impose l'échange de méta-données en clair dans les entêtes de l'email. Par ailleurs, l'usage attendu de l'email (comme la conservation des messages sur le serveur) impose de pouvoir re-déchiffrer ses messages à tout moment dans le futur. Autrement dit, l'utilisateur qui aura consciencieusement pris le temps d'acheter un certificat S/MIME, de l'échanger avec ses contacts et de l'installer dans tous ses

clients mail, n'aura pourtant pas la garantie que ses communications ne seront pas déchiffrées un jour. Le chiffrement du mail étant condamné à utiliser des techniques précédant la carrière solo de Michael Jackson, c'est ailleurs qu'il faut chercher des solutions.

L'avènement du mobile a ouvert la voie à de nouveaux modes de communication et en particulier des messageries instantanées comme WhatsApp et Telegram. C'est l'occasion de s'affranchir des protocoles existants et de tirer profit de 40 ans d'innovation en cryptographie. Le chiffrement « statique » imposé par le mail est remplacé par la notion de « canal sécurisé », un support vivant qui évolue au fur et à mesure des échanges.

L'intégration de la technologie de Signal par WhatsApp met « gratuitement » à la portée de chacun une technologie dont la promesse de protéger tous les échanges va bien au-delà de ce qu'il est envisageable pour le mail. « Double ratchetting », « forward-secrecy », « backward-secrecy » : derrière chacun de ces termes techniques se cache une avancée en matière de protection de la vie privée, une réponse à une menace bien réelle.

La technologie WhatsApp est-elle donc supérieure en tout point à ce qui se faisait avant ? Malheureusement non. En se focalisant exclusivement sur les propriétés de ce « canal sécurisé », WhatsApp a oublié un élément essentiel : garantir la sécurité de la création même de ce canal, autrement dit, de la bonne authentification de l'échange initial des clés cryptographiques si chère à S/MIME et PGP.

Ainsi, souvent sans le savoir, les utilisateurs de WhatsApp font confiance à un serveur central tout puissant pour récupérer les clés cryptographiques de leurs interlocuteurs. À chaque instant, ce serveur peut les cibler et décider de déchiffrer les messages de son choix, sans que ces utilisateurs ne s'en rendent compte. Ce « tiers de confiance » imposé est la pierre angulaire de l'intégralité de l'architecture de sécurité. Ce n'est pas seulement un risque si Facebook (ou l'État américain) décide « d'espionner » les conversations, c'est aussi un « single point of failure » en

cas de compromission de ce serveur. Un tel modèle de sécurité est sans doute suffisant pour échanger des photos de vacances, certainement pas pour protéger les intérêts d'une belle entreprise ou le destin de la France.

L'environnement de travail a changé ces dernières années. WhatsApp et Slack offrent de nouvelles façons de collaborer en ligne. Si le mail reste encore incontournable aujourd'hui, ses jours sont comptés. Se pose aujourd'hui la question de la sécurisation de ces nouveaux outils, comme se posait dans les années 90 la question de la sécurisation du mail. Nous devons apprendre des erreurs passées : la sécurité doit être pensée dès la conception, en intégrant des mesures cryptographiques modernes au cœur des échanges. Cela passera nécessairement par le chiffrement de bout-en-bout des échanges, rendu possible par deux étapes fondamentales : une distribution sécurisée des clés cryptographiques et des identités numériques, couplée à une utilisation adéquate de ces clés pour établir des canaux dynamiques de communication sécurisée.

Les géants américains de la communication comme Google et Facebook vivent essentiellement de l'exploitation des données personnelles qu'ils font transiter. Il ne faut pas s'attendre à ce qu'ils deviennent les nouveaux pionniers du chiffrement. Forte de son savoir-faire, la France a sans aucun doute une belle carte à jouer.