Communiqué de presse
21 septembre 2021

Application e-santé : l'Institut Mines-Télécom conçoit un protocole sécurisé, respectueux de la vie privée et infalsifiable

Les enseignants-chercheurs de la Chaire Valeurs et Politiques des Informations Personnelles ont imaginé un protocole pour les applications e-santé

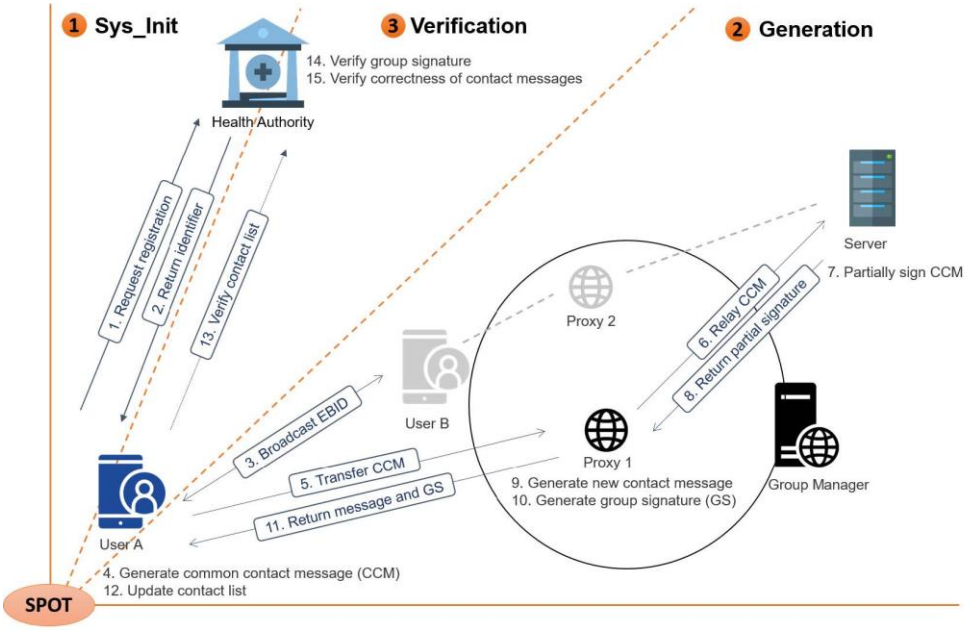
La Chaire Valeurs et Politiques des Informations Personnelles (VP-IP) de l'Institut Mines-Télécom explore de manière pluridisciplinaire depuis sa création en 2013, les problématiques liées à l'utilisation et à la protection des données personnelles. Dans la lignée de ses travaux, ses équipes ont conçu le protocole SPOT qui s'applique aux applications sanitaires de contact tracing qui ont été développées pendant la pandémie. Ce protocole permet de garantir des niveaux élevés de sécurité, de confidentialité des données tout en étant évolutif (scalable). Il prévient également les fraudes en empêchant les utilisateurs malveillants de pouvoir créer de fausses alertes de cas contact positifs, une avancée majeure dans la cybersécurité de ce type d'application.

En réponse à la pandémie, puissances étatiques et géants du numérique ont développé des applications de contacts tracing permettant d'informer une personne qu'elle a été au contact d'une personne infectée. Pour ce type d'application critique, le choix du protocole d'échange d'information est capital car il détermine les niveaux de sécurité des utilisateurs et de la protection de leurs données. Il va définir quelles sont les données transmises, les organisations qui hébergent les informations et qui opèrent les systèmes de transmission. Maryline Laurent, co-fondatrice de la Chaire Valeurs et Politiques des Informations Personnelles de l'Institut Mines-Télécom a co-encadré les travaux de recherche de Souha Masmoudi avec Nesrine Kaâniche sur le protocole de proximité SPOT - Secure and Privacy-preserving prOximiTy. Celui-ci met les standards techniques au plus haut. Il offre ainsi aux citoyens un outil numérique digne de confiance qui préserve leur vie privée dans l'esprit des lois européennes.

SPOT, une conception agile

SPOT repose sur une double architecture centralisée/décentralisée. Le front-end est décentralisé avec différents groupes de proxys, le back-end est centralisé sur le serveur. Comme la majeure partie des applications de ce type, le protocole SPOT s'appuie sur le Bluetooth des smartphones des utilisateurs et un système d'identités éphémères (EBID).

La proximité entre utilisateurs génère un message de contact commun (CCM). Celui-ci est envoyé via le groupe de proxys sur un serveur central de confiance qui le signe partiellement. La signature partielle est ensuite renvoyée aux proxys. Chaque proxy étend la signature partielle avec l'identité de l'utilisateur correspondant, le signe au nom du groupe de proxys (le proxy génère une signature de groupe sur ce message) et renvoie la signature qui a été générée, à l'utilisateur. Tous les messages sont stockés localement sur le terminal de l'utilisateur dans une liste de contacts. S'il est infecté, l'utilisateur envoie sa liste de contacts à l'autorité sanitaire qui vérifie l'exactitude des messages pour les authentifier. Une fois confirmés, l'autorité sanitaire les signe avant de les partager avec tous les utilisateurs de l'application SPOT qui peuvent en toute discrétion calculer s'ils sont cas contacts et le risque de contamination.



Les avantages multiples de SPOT

- Premièrement, l'utilisateur transfère anonymement ses coordonnées vers le serveur qui ne peut pas relier les transactions des utilisateurs.
- Deuxièmement, SPOT permet à l'autorité sanitaire de vérifier l'exactitude et la validité des informations des utilisateurs grâce au travail du serveur et des proxys.
- Troisièmement, en s'appuyant sur les systèmes d'identités électroniques aléatoires du Bluetooth (EBID), qui ne peuvent être ni liés entre eux ni à leurs émetteurs, SPOT garantit que les transactions des utilisateurs ne peuvent pas être reliées entre elles. L'anonymat des utilisateurs enregistrés dans une liste de contacts est également protégé.
- Quatrièmement, chaque utilisateur peut vérifier de façon confidentielle s'il est cas contact.
- Enfin, un effort a été fourni pour minimiser les coûts énergétiques de SPOT.

Impossibilité de créer de fausses alertes

Ce nouveau protocole permet aux systèmes de santé de faire face aux pandémies en automatisant le processus de recherche des contacts tout en répondant aux exigences de sécurité et de vie privée inhérentes à ce type d'application : infalsifiable, impossibilité de déduire le réseau social d'un individu, respect des personnes dans leur choix de bénéficier du service SPOT de façon anonyme et responsable.

Grâce à l'architecture sous-jacente du réseau qui s'appuie sur un serveur centralisé et des proxys décentralisés, SPOT permet aux utilisateurs de déterminer s'ils se trouvaient à proximité de personnes infectées, sans risque de fausses alertes positives ou l'enregistrement de faux contacts.

L'objectif, avec cette contribution, est de permettre à la société de bénéficier d'une solution entièrement distribuée. Celle-ci s'appuie sur des ressources de calculs administrées par une autorité sur un territoire, tout en limitant la diffusion des informations exploitables qu'aux citoyens contributeurs, comptant alors sur le collectif et la responsabilité des individus pour œuvrer à un service efficace de contact tracing.

Maryline Laurent, co-fondatrice de la Chaire a piloté les travaux autour de SPOT : « *Ce protocole répond à un ensemble d'exigences : sécurité, protection de la vie privée et performance. A mon sens, SPOT est l'unique dispositif pouvant empêcher les utilisateurs malveillants de s'attaquer au système en créant des faux positifs. Au sein de la Chaire Valeurs et Politiques et Informations Personnelles de l'Institut Mines-Télécom, nous nous attachons à partager le meilleur de l'état de l'art et innover dans toutes les disciplines pour répondre aux nouveaux enjeux du numérique qui sont à la fois technologiques et*

éthiques. Avec SPOT, nous démontrons que les valeurs européennes sont compatibles avec les exigences techniques et économiques. »

À propos de la Chaire Valeurs et Politiques des Informations Personnelles https://cvpip.wp.imt.fr/accueil/
La Chaire se propose d'aider les entreprises, les citoyens et les pouvoirs publics dans leurs réflexions sur la collecte, l'utilisation et le partage des informations personnelles, à savoir les informations concernant les individus (leur vie privée, leurs activités professionnelles, leurs identités numériques, leurs contributions sur les réseaux sociaux, etc.) incluant celles collectées par les objets communicants qui les entourent (*smartphones*, compteurs intelligents, etc.).

À propos de l'Institut Mines-Télécom www.imt.fr
Placé sous la tutelle du Ministère en charge de l'économie, de l'industrie et du numérique, l'Institut Mines-Télécom est un établissement public d'enseignement supérieur et de recherche regroupant 8 grandes écoles : IMT Atlantique, IMT Mines Albi, IMT Mines Alès, IMT Nord Europe, Institut Mines-Télécom Business School, Mines Saint Etienne, Télécom Paris et Télécom SudParis, 2 écoles filiales : EURECOM et Insic et un réseau de partenaires stratégiques et affiliés. Ses activités menées dans les domaines des sciences de l'ingénieur et du numérique sont mises au service de la formation d'ingénieurs et de managers, de la recherche partenariale, de l'innovation et du soutien au développement économique. A l'écoute permanente du monde économique, l'IMT conjugue une forte légitimité académique et scientifique, une proximité avec les entreprises et un positionnement stratégique sur les transformations majeures du XXIe siècle : numériques, industrielles, énergétiques, écologiques et éducatives. L'IMT est membre fondateur de l'Alliance Industrie du Futur, et créateur avec la TUM de l'académie franco-allemande pour l'industrie du futur, il est doublement labellisé Carnot pour la qualité de sa recherche partenariale. L'IMT forme chaque année plus de 13000 étudiants, réalise près de 70 millions de contrats de recherche et ses incubateurs accueillent une centaine de start-ups.

@IMTFrance

propos de la Fondation Mines-Télécom www.fondation-mines-telecom.org
La Fondation Mines-Télécom, fondation reconnue d'utilité publique, soutient le développement de IMT et de ses huit écoles dans leurs missions de formation, de recherche et d'innovation. Elle rassemble plus de 90 entreprises mécènes et 2000 donateurs particuliers qui s'engagent à soutenir des projets concrets à forts impacts technologiques, industriels et sociétaux, autour du numérique, de l'énergie et de l'Industrie du futur ainsi que des actions de solidarité en faveur des étudiants. La Fondation Mines-Télécom finance ainsi, grâce au soutien des entreprises dont les partenaires fondateurs (BNP Paribas, Nokia et Orange) et des diplômés et parents d'élèves, une dizaine de programmes dans les domaines de la formation (bourses, programme d'open-innovation pour les élèves, MOOC), de la recherche (thèses, prix d'excellence, Académie franco-allemande et chaires d'enseignement-recherche), de l'innovation (prêts d'honneur aux start-up et soutien à l'incubation) et de la prospective (Cahiers de veille) ainsi que des actions en faveur du développement des écoles de l'IMT (bourses, ouverture sociale, équipements de pointe, aide à la mobilité internationale).

Contact presse :
Institut Mines-Télécom
Séverine Picault
+33 (0) 6 27 66 05 09 / +33 (0) 1 75 31 40 97
severine.picault@imt.fr