Le traçage anonyme, dangereux oxymore

Analyse de risques à destination des non-spécialistes

Le traçage automatisé des contacts à l'aide d'une application sur smartphone- comporte de nombreux risques, indépendamment des détails de fonctionnement de cette application. Nous sommes spécialistes en cryptographie, sécurité ou droit des technologies. Notre expertise réside notamment dans notre capacité à anticiper les multiples abus, détournements et autres comportements malveillants qui pourraient émerger. Nous proposons une analyse des risques d'une telle application, fondée sur l'étude de scénarios concrets, à destination de non-spécialistes.

Dans le but affiché de ralentir la progression de l'épidémie COVID-19, la France envisage de mettre en place un système de traçage des contacts des malades à l'aide d'une application mobile. Les concepteurs de ce type d'applications assurent qu'elles sont respectueuses de la vie privée. Cependant cette notion reste vague. Nous souhaitons donc contribuer au débat public en apportant un éclairage sur ce que pourrait et ne pourrait pas garantir une application de traçage, afin que chacun puisse se forger une opinion sur l'opportunité de son déploiement.

L'intérêt d'une telle application réside dans sa capacité effective à détecter les contacts à risque et à utiliser cette information de manière pertinente dans les mesures de lutte contre l'épidémie comme l'accès à des tests de dépistage ou la mise en quarantaine. N'ayant pas de compétence en épidémiologie, nous nous gardons de juger de l'impact de ces applications de traçage sur la propagation de l'épidémie. Mais cette évaluation nous semble indispensable pour mettre en balance leurs possibles bénéfices avec leurs risques.

Notre expertise en tant que spécialistes en cryptographie, sécurité ou droit des technologies réside notamment dans notre capacité à anticiper les multiples abus, détournements et autres comportements malveillants qui pourraient émerger. À l'heure actuelle, un vif débat a lieu entre les spécialistes du domaine sur la sécurité des applications proposées, opposant souvent les applications dites «centralisées » à celles dites « décentralisées ». Indépendamment de ces considérations techniques, nous voulons alerter sur les dangers intrinsèques d'une application de traçage. À l'aide de différents scénarios concrets comme celui ci-dessus, nous présentons les détournements possibles d'une telle technologie, quels que soient les détails de sa mise en œuvre.

EXEMPLE

L'entreprise RIPOUE souhaite recruter une personne pour un CDD. Elle veut s'assurer que le candidat ne tombe pas malade entre l'entretien d'embauche et la signature du contrat. Elle utilise donc un téléphone dédié qui est allumé seulement pendant l'entretien, et qui recevra une alerte si le candidat est testé positif plus tard.

Résumé :

Il n'y a pas de base de données nominative des malades
VRAI

Les données sont anonymes
FAUX

Il est impossible de retrouver qui a contaminé qui
FAUX

Il est impossible de savoir si une personne précise est malade ou non

FAUX

Il est impossible de déclencher une fausse alerte
FAUX

L'utilisation du Bluetooth ne pose pas de problème de sécurité
FAUX

Ce dispositif rend impossible un fichage à grande échelle
FAUX

Si vous ne l'avez vu : _« Tous surveillés : 7 milliards de suspects ?», un documentaire de Sylvain Louvet (CAPA, France, 2019), 95 min. sur arte.tv du 14 avril au 19 juin [1]

DOCUMENT COMPLET À TÉLÉCHARGER SUR :

HTTPS://RISQUES-TRACAGE.FR/ Contact : contact@risques-tracage.fr

QUI SOMMES-NOUS ?

* Xavier Bonnetain [2], University of Waterloo, Canada ;
* Anne Canteaut [3], Inria ;
* Véronique Cortier [4], CNRS, Loria ;
* Pierrick Gaudry [5], CNRS, Loria ;
* Lucca Hirschi [6], Inria ;
* Steve Kremer [7], Inria ;
* Stéphanie Lacour [8], CNRS ;
* Matthieu Lequesne [9], Sorbonne Université et Inria ;
* Gaëtan Leurent [10], Inria ;
* Léo Perrin [11], Inria ;
* André Schrottenloher [12], Inria ;
* Emmanuel Thomé [13], Inria ;
* Serge Vaudenay [14], EPFL, Suisse ;
* Christophe Vuillot [15], Inria.

https://www.arte.tv/fr/videos/083310-000-A/tous-surveilles-7-milliards-de-suspects/
[2] https://www.bonneta.in/
[3] http://www.paris.inria.fr/secret/Anne.Canteaut/
[4] https://members.loria.fr/VCortier/
[5] https://members.loria.fr/PGaudry/
[6] https://members.loria.fr/LHirschi/
[7] https://members.loria.fr/SKremer/
[8] https://isp.cnrs.fr/?project=lacour-stephanie
[9] https://who.paris.inria.fr/Matthieu.Lequesne/index.php
[10] https://who.paris.inria.fr/Gaetan.Leurent/
[11] https://who.paris.inria.fr/Leo.Perrin/
[12] https://who.paris.inria.fr/Andre.Schrottenloher/pages/home.html
[13] https://members.loria.fr/EThome/
[14] https://people.epfl.ch/serge.vaudenay
[15] https://www.vuillot.info/
—