Applis de traçage : scénarios pour les non-spécialistes

Un document de plus sur les dangers de l'application de traçage ? Nous n'allons pas reproduire ici les 13 pages documentées et augmentées de notes de référence d'une équipe de 14 spécialistes en cryptographie :

Xavier Bonnetain, University of Waterloo, Canada ; Anne Canteaut, Inria ; Véronique Cortier, CNRS, Loria ; Pierrick Gaudry, CNRS, Loria ; Lucca Hirschi, Inria ; Steve Kremer, Inria ; Stéphanie Lacour, CNRS ; Matthieu Lequesne, Sorbonne Université et Inria ; Gaëtan Leurent, Inria ; Léo Perrin, Inria ; André Schrottenloher, Inria ; Emmanuel Thomé, Inria ; Serge Vaudenay, EPFL, Suisse ; Christophe Vuillot, Inria.

… mais ils ont fait un effort tout à fait louable de pédagogie pour qu'au-delà des problèmes techniques réels, nous comprenions tous. Le document s'intitule : **Le traçage anonyme, dangereux oxymore, Analyse de risques à destination des non-spécialistes**

Nous vous invitons évidemment à en découvrir l'intégralité, mais voici simplement les cas fictifs (hélas réalistes), les scénarios que les spécialistes nous proposent.

Au moment où va peut-être se déclencher une offensive médiatique *en faveur* d'une application de surveillance de la part du gouvernement ou de Google+Apple, il n'est probablement pas inutile d'avoir *des exemples simples et faciles à comprendre* pour expliquer notre opposition.

Nous avons ajouté en complément la conclusion de l'ensemble du document qui précise clairement les limites de toute solution technique et les valeurs que doit respecter l'informatique. Que les auteurs soient vivement remerciés de cet exercice d'éducation de tous qu'ils ont eu l'excellente idée de placer sous licence CC-BY 4.0 .

⇒ Accéder aux articles déjà publiés dans notre dossier StopCovid

1. Fausse déclaration

Le joueur de foot Gronaldo doit disputer le prochain match de Ligue des champions. Pour l'empêcher de jouer, il suffit pour un adversaire de laisser son téléphone à côté de celui de Gronaldo à son insu, puis de se déclarer malade. Gronaldo recevra une alerte, car il aurait été en contact avec une personne infectée, et devra rester 14 jours éloigné des terrains

2. Le suspect unique

M. Lambda qui, pour éviter la contamination, ne sort de chez lui que pour faire ses courses à l'épicerie du quartier, reçoit une notification de son téléphone. Il en déduit que le responsable n'est autre que l'épicier.

3. Croisement d'informations

Mme Toutlemonde qui, elle, croise beaucoup de gens dans la journée, reçoit une notification. Il lui suffit de discuter quelques instants avec son voisin de palier et un collègue de bureau, pour savoir que le malade ne fait pas partie de son entourage professionnel, mais qu'il habite l'immeuble. Grâce à ces indices, elle suspecte fortement (peut-être à tort) M. Harisk du 3^{e} étage, qui est ambulancier, d'avoir contaminé tous ses voisins. Elle s'empresse de prévenir le reste des habitants de l'immeuble via les réseaux sociaux.

4. Mes voisins sont-ils malades ?

M. Ipokondriac voudrait savoir si ses voisins sont malades. Il récupère son vieux téléphone dans un placard, y installe l'application TraceVIRUS, et le laisse dans sa boîte aux lettres en bas de l'immeuble. Tous les voisins passent à côté à chaque fois qu'ils rentrent chez eux, et le téléphone recevra une notification si l'un d'entre eux est malade.

5. Candidat à l'embauche

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 uniquement pendant l'entretien, et qui recevra une alerte si le candidat est testé positif plus tard.

6. Les paparazzi

M. Paparazzo cherche des informations sur la vie privée de Mme Star. Il soudoie Mme Rimelle, la maquilleuse qui intervient sur le tournage de son dernier film pour qu'elle allume un téléphone dédié et qu'elle le place à proximité de celui de Mme Star. M. Paparazzo récupère ensuite le téléphone. Il recevra une notification si Mme Star est infectée par le virus.

7. Le militant antisystème

M. Hanty, qui présente des symptômes du COVID-19, est un militant antisystème. Pour dénoncer la mise en place de l'application TraceVIRUS, il attache son téléphone à son chien, et le laisse courir dans le parc toute la journée. Le lendemain il va voir le médecin et il est testé positif ; tous les promeneurs reçoivent une notification.

8. L'ingérence étrangère

Le sous-marin Le Terrifiant doit appareiller dans quelques jours, mais Jean Bond est un agent étranger qui veut empêcher son départ. Il recrute Mata-Hatchoum qui présente des symptômes, et lui demande de faire le tour des bars de marins. Mata-Hatchoum va ensuite se faire tester, et 5 marins reçoivent une notification de l'application. Le Terrifiant est obligé de rester à quai.

9. L'élève Ducovid

L'élève Ducovid a un contrôle de français la semaine prochaine, mais il n'a pas lu l'œuvre au programme. Grâce à une petite annonce, il trouve M. Enrumais qui présente des symptômes et accepte de lui prêter son téléphone. Il fait passer le téléphone de M. Enrumais dans toute la classe, puis le laisse traîner en salle des profs. Il le rend ensuite à M. Enrumais, qui va voir un médecin. Le médecin constate que M. Enrumais est malade du COVID et le déclare dans l'application du téléphone. Ceci déclenche une alerte pour toute la classe et pour tous les professeurs, le lycée est fermé !

10. Le cambriolage

M. Rafletou veut cambrioler la maison de l'oncle canard. Avant d'entrer, il utilise une antenne pour détecter les signaux Bluetooth. Il sait que l'oncle canard utilise TraceVIRUS, et s'il n'y a pas de signal c'est que la maison est vide.

11. Le centre commercial

Le centre commercial La Fayote veut protéger ses clients, et refuser ceux qui n'utilisent pas l'application TraceVIRUS. Comme l'application diffuse régulièrement des messages, il suffit que le vigile à l'entrée utilise une antenne Bluetooth pour détecter les clients qui utilisent l'application, et ceux qui ne l'utilisent pas.

12. L'application GeoTraceVIRUS

Peu après avoir installé l'applicationTraceVIRUS, Mme Toutlemonde entend parler de l'application GeoTraceVIRUS qui réutilise les informations TraceVIRUS pour localiser les malades. Mme Toutlemonde apprend ainsi qu'un malade s'est rendu samedi dernier au supermarché PetitPrix. Par crainte (peut-être infondée) d'attraper le virus, elle ne fera pas ses courses chez PetitPrix cette semaine.

13. L'assurance

La chaîne de supermarché SansScrupule utilise des traceurs Bluetooth pour suivre les clients dans ses magasins. Ils relient l'identifiant Bluetooth à l'identité réelle à partir de l'application MySansScrupule, ou avec les cartes bancaires lors du passage en caisse. Pendant que M. Lambda fait ses courses, ils peuvent simuler un contact avec son téléphone, et ils seront donc prévenus si M. Lambda est malade. Cette information sera transmise au service assurance du groupe.

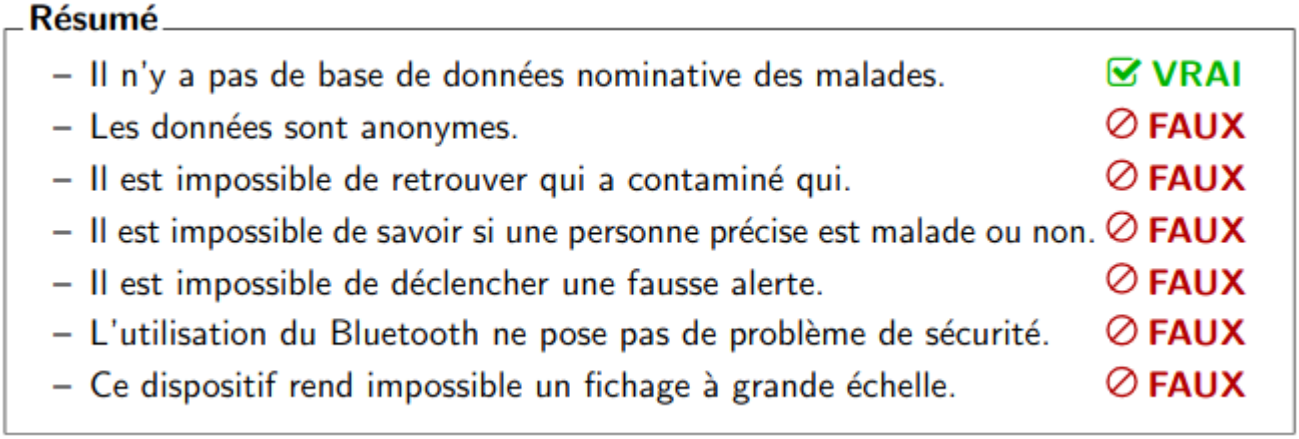
14. Le malware

Mme Toutlemonde a installé l'application chatsMignons sur son téléphone, sans savoir que c'est un logiciel espion (un « malware ») qui l'espionne. Après avoir déclaré dans TraceVIRUS qu'elle est malade, elle reçoit un message pour la faire chanter, menaçant de révéler sa maladie à son assurance et à son employeur qui risque de mettre fin à sa période d'essai. Une autre activité lucrative du crime organisé, très facile à mettre en œuvre dans certains des systèmes de traçage proposés, consisterait à garantir, moyennant finances, la mise en quatorzaine

obligatoire de personnes ciblées.

15. Vente d'alertes positives

Don Covideone vend une application InfecteTonVoisin sur Internet. Après avoir téléchargé l'application, il suffit d'approcher son téléphone d'une personne pour qu'elle reçoive une notification lui signalant qu'elle est à risque. Les attaques sont désormais possibles sans compétence technique. Ainsi, Monsieur Bouque-Maeker compte parier lors du prochain match de Ligue des champions. Par chance, il assistera à la conférence de presse de Gronaldo. Il mise alors fortement sur l'équipe adverse, pourtant donnée perdante à 10 contre 1. Il télécharge l'application InfecteTonVoisin et approche son téléphone de Gronaldo pendant l'interview. Gronaldo reçoit une alerte, il ne pourra pas disputer le match. Son équipe perd et Monsieur Bouque-Maeker remporte la mise !
[L'image ci-dessous résume l'ensemble de l'argumentaire de 13 pages, pas seulement les cas de figure plus haut mentionnés.]



Conclusion

Le traçage des contacts pose de nombreux problèmes de sécurité et de respect de la vie privée, et les quelques scénarios que nous avons présentés n'illustrent qu'un petit nombre des détournements possibles. À cet égard, la cryptographie n'apporte que des réponses très partielles.

Nombre des situations que nous avons présentées exploitent en effet les fonctionnalités de ce type de technique, plutôt que leur mise en œuvre. **Dès lors, l'arbitrage de ces risques ne pourra pas être résolu par la technique.** Il

relève de choix politiques qui mettront en balance les atteintes prévisibles aux droits et libertés fondamentaux et les bénéfices potentiels qui peuvent être espérés dans la lutte contre l'épidémie. À notre connaissance, l'estimation des bénéfices d'un éventuel traçage numérique est aujourd'hui encore très incertaine, alors même que les scénarios que nous avons développés ici sont, eux, connus et plausibles.

Un principe essentiel en sécurité informatique est que **l'innocuité d'un système ne doit en aucun cas être présumée en comptant sur l'honnêteté de certains de ses acteurs**. Ce même principe apparaît dans l'évolution de notre droit en matière de protection des données à caractère personnel. Si, avec la loi « Informatique et libertés » de 1978, c'était de la part des pouvoirs publics, et singulièrement de l'état, que des dérives étaient redoutées, les acteurs privés puis, à travers le RGPD, tous les acteurs de la société ont été associés à ces craintes. Les atteintes que les systèmes de traçage peuvent faire subir aux droits et libertés de chacun et chacune d'entre nous peuvent venir non seulement des pouvoirs publics qui en recommandent le développement et la mise en œuvre, mais aussi d'autres acteurs, collectifs ou individuels, qui sauront tirer profit des propriétés de ces systèmes comme autant de failles.

Le premier alinéa de l'article 1 de la loi de 1978 a survécu à toutes ses révisions et évolutions. L'urgence que nous ressentons collectivement face à notre situation actuelle ne doit pas nous le faire oublier : ***L'informatique doit être au service de chaque citoyen. […] elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques.***