Le traçage anonyme, dangereux oxymore

Xavier Bonnetain, Anne Canteaut, Véronique Cortier, Pierrick Gaudry, Lucca Hirschi, Steve Kremer, Stéphanie Lacour, Matthieu Lequesne, Gaëtan Leurent, Léo Perrin, et al.

Le traçage anonyme, dangereux oxymore

Analyse de risques à destination des non-spécialistes

Version du 21 avril 2020

Par : **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**, Université Paris-Saclay, 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.
Contact : contact@risques-tracage.fr Web: https://risques-tracage.fr/

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 garderons 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-dessous, nous présentons les détournements possibles d'une telle technologie, quels que soient les détails de sa mise en œuvre.

Scénario. *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.*

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**

Introduction

Le monde fait face à l'épidémie de COVID-19. De nombreux pays, dont la France, envisagent de mettre en place un système de traçage des contacts des malades à l'aide d'une application mobile. L'idée qui guide les pouvoirs publics est que, si quelqu'un est testé positif au virus, il sera possible avec une telle application d'alerter toutes les personnes qui l'ont côtoyé les jours précédents et, ce faisant, de les inciter à se mettre en quarantaine, à consulter un médecin ou à se faire tester. Depuis le début de l'épidémie, des collègues chercheurs en sécurité informatique se sont investis dans la conception de tels systèmes, d'autres comme R. Anderson [1], S. Landau [2], B. Schneier [3] et S. Vaudenay [4], ont dénoncé leurs dangers ou se sont exprimés fermement contre leur mise en œuvre. Étant donné les risques potentiels pour la vie privée, l'usage d'une telle application fait débat.

En premier lieu, ces applications n'ont de sens que si elles permettent effectivement de détecter les contacts à risque. Cela suppose que les applications de traçage puissent évaluer précisément la distance d'une personne (plus ou moins d'un mètre?) quels que soient l'environnement et le positionnement du téléphone. En pratique, il faudra faire un compromis, mais il y aura probablement à la fois des contacts non détectés (notamment les cas de transmissions par les surfaces) et des fausses alertes (comme une détection à travers un mur). Cela suppose également une adoption massive, par la population, de ces solutions qui nécessitent en général un smartphone et souvent du Bluetooth. Par ailleurs, contrairement à la procédure existante[1], ces technologies alertent de manière systématique et indifférenciée les personnes qui ont été au contact d'un malade, ce qui implique que le patient comme les professionnels compétents sont dépossédés de la faculté de déterminer finement qui il est réellement souhaitable d'alerter. On pourrait pourtant interroger, par exemple, la nécessité de conseiller à tous les contacts de se déplacer pour un test, alors que pour des personnes très âgées ou présentant des pathologies préexistantes, cela représenterait en réalité un risque supplémentaire. Ces aspects sont souvent peu abordés dans les documentations publiques des applications proposées. Nous ne discuterons donc pas ici de l'efficacité des applications de traçage mais de leur sécurité, même s'il nous semble indispensable d'évaluer leur intérêt et de le comparer avec celui de la procédure existante ou de la détection de clusters par les épidémiologistes.

La question des risques pour les libertés publiques a, elle, déjà été soulevée, notamment par la Quadrature du Net [7]. Notre contribution se cantonnera à l'étude de plusieurs scénarios d'usage afin de mettre en lumière les dérives concrètes qu'une telle application rendrait possibles. Même si certaines de ces failles de sécurité pourraient être en partie évitées par des modifications importantes des protocoles proposés, la plupart des scénarios que nous envisageons sont inhérents aux fonctionnalités-mêmes de ces applications.

Nous commençons par présenter le fonctionnement général de ce type d'application. Les scénarios d'attaque sont discutés à partir de la section 4.

1. La procédure existante repose sur des mécanismes de déclaration des maladies et sur la prise en charge par les autorités publiques d'une enquête visant à retracer avec une personne contaminée ses contacts à risque. Les autorités publiques contactent alors ces derniers, et leur conseillent une conduite à tenir. En pensant calquer l'outil technique sur ces procédures existantes, on oublie par ailleurs que la mise en œuvre des règles de droit donne toujours lieu à de multiples arrangements [5, 6].

1 Fonctionnement du dispositif

Notre analyse porte sur les propositions récentes de système de traçage à l'aide de Bluetooth. Ces systèmes ont été proposés comme une solution plus satisfaisante au regard du respect de la vie privée que les systèmes reposant sur la géolocalisation précise de tous les habitants, à l'instar de ce qui s'est fait en Chine, et au sujet desquels la plupart des pays européens, ainsi que la Commission européenne[2], se sont montrés réticents. Plusieurs systèmes de traçage alternatifs[3] ont ainsi été proposés ces dernières semaines par des spécialistes de sécurité informatique, chercheurs et industriels. Sont en particulier concernés par notre étude (liste non-exhaustive) : le protocole DP3T[4] (sous diverses variantes), sa déclinaison par l'alliance Apple/Google[5], le protocole PACT-Est[6], le protocole PACT-Ouest[7], le protocole TCN[8], le protocole ROBERT[9]. **Les acronymes de la plupart des systèmes mentionnés précédemment promettent de « respecter la vie privée des utilisateurs ». Mais il est important d'expliciter ce que signifie (et ne signifie pas) ce slogan.**

Nous en profitons pour rappeler un principe fondamental en sécurité informatique : il est indispensable que la description et le code d'un système soient publiés puis expertisés pour qu'il soit envisageable de lui accorder la moindre confiance.

1.1 Principe général

Les diverses variantes publiées des systèmes de traçage « respectueux de la vie privée » suivent toutes un schéma relativement proche de celui illustré dans la bande dessinée page 4. Le téléphone portable de chaque utilisateur génère très régulièrement (par exemple toutes les 5 minutes) un code aléatoire (une suite de lettres et de chiffres), qu'on appellera un *pseudonyme*. À chaque fois que deux téléphones sont en contact proche, ils s'échangent par liaison Bluetooth[10] leurs pseudonymes de l'instant, et notent le jour et l'heure de l'échange. Ces informations sont stockées dans le téléphone de chaque utilisateur pendant deux semaines. Lorsqu'un utilisateur (appelons-le Alice) est testé positif, l'application alerte toutes les personnes avec qui il a échangé des pseudonymes au cours des 14 jours précédents, par exemple l'utilisateur Bob. Ces derniers reçoivent une notification (assortie de recommandations en fonction de la durée passée au contact du malade). La procédure permettant à l'application d'utiliser les pseudonymes enregistrés pour prévenir les contacts dépend des protocoles et sera détaillée à la section suivante.

2. https://ec.europa.eu/commission/presscorner/detail/en/ip_20_670, consulté le 18 avril 2020.

3. Ces systèmes ne permettent pas d'identifier des « clusters » puisqu'ils n'utilisent aucune information de géolocalisation.

4. DP3T = *Decentralized Privacy-Preserving Proximity Tracing* https://github.com/DP-3T/documents/ consulté le 18 avril 2020.

5. https://www.apple.com/covid19/contacttracing/ consulté le 18 avril 2020.

6. PACT = *Private Automated Contact Tracing*, https://pact.mit.edu/ consulté le 18 avril 2020.

7. https://covidsafe.cs.washington.edu/ consulté le 20 avril 2020.

8. https://tcn-coalition.org/ consulté le 20 avril 2020.

9. ROBERT = ROBust and privacy-presERving proximity Tracing, https://github.com/ROBERT-proximity-tracing/documents/ consulté le 18 avril 2020.

10. Notons que le Bluetooth n'est pas conçu pour tester une proximité physique et, de fait, va considérer que deux personnes situées de différents côtés d'un mur ont été « en contact ». Mais son utilisation évite l'emploi de moyens de géolocalisation qui révèlent la position précise de chacun à chaque instant.

FIG. 1 – *Illustration du fonctionnement de l'application dans le modèle dit décentralisé, comme utilisé par D3PT et Apple/Google. Les protocoles centralisés comme ROBERT ne suivent pas la même procédure pour prévenir Bob quand Alice tombe malade. À partir d'un dessin de Nicky Case (ncase.me, consulté le jeudi 18 avril), traduction en français par Meï (@MeiVongola).*

1.2 Qui certifie qu'Alice est malade ?

Lorsqu'Alice tombe malade, elle doit déclencher l'application pour que les personnes avec qui elle a été en contact soient prévenues. Mais qui certifie qu'Alice est malade et que les informations doivent êtres transmises ? Deux possibilités sont envisageables.

1. Alice s'auto-diagnostique et déclenche elle-même le signalement.
2. Il est nécessaire que la maladie d'Alice soit confirmée par un test ou un professionnel de santé, pour que les informations soient diffusées (par exemple en donnant à Alice un code à usage unique qui déclenchera le signalement).

Nous n'envisagerons que la seconde possibilité qui semble être l'option choisie par les protocoles proposés en Europe[11]. En effet, si les personnes peuvent se déclarer malades sans contrôle d'une autorité médicale, n'importe quel utilisateur malveillant peut faire de fausses déclarations de maladie, comme dans le scénario suivant. La multiplication de telles fausses déclarations va rapidement rendre le système inopérant.

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

Nous n'avons pas encore expliqué comment il était possible de prévenir Bob qu'il a été en contact avec une personne malade. Une idée simple, mais risquée en termes de confidentialité des données médicales, consisterait à établir une liste des personnes malades. Cette idée est écartée par les applications qualifiées de « respectueuses de la vie privée » qui lui préfèrent deux solutions alternatives, qui correspondent à deux modèles différents de diffusion des données.

1. **Le modèle dit « décentralisé ».** Lorsqu'elle est diagnostiquée, Alice envoie à tout le monde la liste des pseudonymes qu'elle a émis ces derniers jours. Techniquement cela peut se faire en pair-à-pair, ou en passant par un intermédiaire comme une agence de santé, symbolisée par un hôpital[12] dans la bande dessinée. Bob peut interroger cette base de données pour savoir si l'un des pseudonymes qu'il a reçus et enregistrés dernièrement s'y trouve. S'il y a une correspondance, l'application lui envoie une alerte. Les protocoles DP3T, PACT et Apple/Google suivent ce modèle.
2. **Le modèle dit « centralisé ».** Lorsqu'elle est diagnostiquée, Alice envoie à l'autorité centrale la liste des pseudonymes qu'elle a enregistrés ces derniers jours. Cette liste des contacts à risque n'est pas diffusée et n'est connue que de l'autorité centrale. Dans ce modèle, Bob, à l'instar de chaque utilisateur, contacte chaque jour l'autorité centrale, et lui fournit la liste des pseudonymes qu'il a émis[13] pour savoir si l'un d'entre eux figure dans la base de données des contacts à risque. Le cas échéant, il reçoit une notification.

11. Il paraît indispensable, pour que le système soit efficient, que ces déclarations reposent sur des tests eux-mêmes fiables.
12. C'est le choix fait dans les protocoles DP3T, PACT et Apple/Google.
13. Dans le cas particulier de ROBERT, l'autorité centrale calcule l'ensemble des pseudonymes de Bob, bien qu'elle ne connaisse pas a priori son identité.

Ces deux modèles comportent des avantages et des inconvénients. Le modèle centralisé nécessite de faire confiance à une autorité centrale. Par exemple, l'autorité peut exploiter la liste des contacts reçus par les «nouveaux» malades, et y détecter des individus qui ont été précédemment déclarés exposés au virus, constatant ainsi que ces derniers méprisent leur consigne de quarantaine. Le modèle décentralisé ne pose *a priori* pas ce problème, mais ouvre la porte à certaines attaques. Ces deux modèles seront étudiés par la suite. Leurs différences sont importantes, même si la plupart des scénarios discutés fonctionnent indépendamment du modèle.

3 Les données ne sont pas anonymes

Les protocoles de traçage décentralisés nécessitent la constitution d'un fichier des malades du COVID-19, au même titre que pour certaines maladies à déclaration obligatoire définies par la loi. Les modèles centralisés, eux, possèdent un fichier de personnes susceptibles de contracter la maladie puisqu'elles ont été en contact avec un malade. Dans tous les cas, ces fichiers sont *pseudonymisés*, ce qui signifie que les malades ne sont pas identifiés par leur nom ou leur numéro Insee mais par un code ou un numéro qui est indépendant de leur identité réelle. Dans les systèmes proposés, le fichier des malades du COVID-19 est pseudonymisé avec des mécanismes cryptographiques[14] au même titre par exemple que le fichier des déclarations du VIH-Sida. Cependant, ce numéro pourrait être désanonymisé en le combinant avec d'autres informations dans la base de données (les identifiants de personnes ayant été en contact), ou extérieures à la base de données (par exemple collectées avec une antenne Bluetooth), ou encore par adresse IP. **Il ne s'agit donc pas d'une base de données anonyme** telle que définie par exemple par le RGPD.

> *« Les données à caractère personnel qui ont fait l'objet d'une pseudonymisation et qui pourraient être attribuées à une personne physique par le recours à des informations supplémentaires devraient être considérées comme des informations concernant une personne physique identifiable. »*
>
> — Règlement Général sur la Protection des Données

Cette base contient donc des données à caractère personnel au sens du RGPD et de la loi française[15]. Elle contient, en outre, des données qualifiées de sensibles (données de santé) auxquelles notre droit confère des propriétés particulières, en limitant notamment les possibilités de les traiter[16].

Anonyme ou pseudonyme ?

– M. Dupont est malade	⊘ **NOMINATIF**
– Le pseudonyme `439Hxs` est malade	⊘ **PSEUDONYME**
– Il y a 50 437 malades en Île-de-France	☑ **ANONYME**

14. Par exemple, les protocoles DP3T et Apple/Google utilisent HMAC−SHA256 qui est considéré comme sûr à l'heure actuelle.

15. En ce sens que ces données permettent, fût-ce indirectement, d'identifier les personnes concernées.

16. Article 6 de la loi n. 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée pour la dernière fois en 2019 et article 9 du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).

4 Comment retrouver qui vous a contaminé ?

Bien que les pseudonymes des malades ne divulguent pas leur identité, les utilisateurs du système peuvent eux facilement déduire des informations sur les autres utilisateurs dès qu'ils apprennent qu'une personne qu'ils ont rencontrée au cours des deux dernières semaines vient de tomber malade.

Scénario 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*[17] *que le responsable n'est autre que l'épicier.*

Scénario 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 3e 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.*

Ces scénarios crédibles sont totalement indépendants des détails de l'application. Ils ne nécessitent aucune compétence particulière en informatique. Ils illustrent les limitations inhérentes à ce type de mécanisme. S'il n'est effectivement *a priori* pas possible pour l'autorité centrale de contourner la pseudonymisation des usagers, il n'est en revanche pas difficile de le faire pour un simple utilisateur.

Ces technologies de traçage ont la particularité d'avertir de manière systématique et sans discernement toutes les personnes rencontrées par un malade, ce qui ne peut s'apparenter pour les malades à une notification volontaire et réfléchie des personnes de leur entourage proche. Dans les modèles décentralisés, c'est même l'ensemble de la population qui est destinataire des données de santé récoltées par le système, ce qui est radicalement différent de tous les dispositifs existants.

Dans la mesure où le traçage agirait comme un système de dénonciation des malades à grande échelle, les informations qu'il apporte provoqueraient la suspicion, transformeraient la possible contamination en une faute morale[18] et exacerberaient la stigmatisation des personnes à risque dans un contexte déjà sensible.

De tels effets sont déjà rapportés en Corée par exemple[19], provoquant de véritables « chasses aux sorcières ». Ce risque de stigmatisation a d'ailleurs été jugé préoccupant il y a vingt ans, au moment de la constitution du fichier des personnes séropositives, et cette inquiétude semble encore plus légitime à l'heure des réseaux sociaux.

17. Nous remarquons que M. Lambda a pu se tromper : sa notification pourrait être due par exemple à un autre voisin, effectivement malade, dont le smartphone a été détecté par celui de M. Lambda à travers le mur.

18. Le traçage est en effet une solution de gestion individualisante de la problématique complexe du déconfinement. Cette interprétation peut s'appuyer sur les travaux des chercheurs en sciences sociales, par exemple [8], qui montrent que l'évolution de notre système de santé durant les dernières décennies a mené à une valorisation de la figure de l'individu rationnel et informé, responsable et capable de faire des choix avisés à partir des informations et des incitations économiques des pouvoirs publics. La réponse envisagée au travers du recours à ce type d'application va dans le même sens.

19. En Corée du Sud, les habitants peuvent recevoir des alertes indiquant qu'une personne habitant le même quartier a été testée positive au virus. Ces alertes donnent son sexe, son âge et la liste de ses déplacements récents. Bien qu'*a priori* anonymes, ces informations ont pu conduire à des identifications par le public, suivies de campagnes de dénigrement en ligne (on reproche à un contaminé d'avoir potentiellement propagé le virus). https://www.bbc.com/news/world-asia-51733145

Scénario 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 Comment savoir si une personne précise est malade ? L'espionnage à la portée de tous

Par essence, tous les systèmes de traçage qui notifient les contacts des malades peuvent être détournés pour savoir si une personne ciblée tombe malade. Pour avoir des informations fiables sur une personne précise, il suffit d'utiliser un téléphone dédié, sur lequel on installe l'application [20], et qu'on ne met au contact que de cette personne. Les deux téléphones enregistreront le contact, et si la cible est testée positive le téléphone dédié recevra une alerte.

Scénario 5 (L'entretien d'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. (Voir Figure 2.)*

Beaucoup de scénarios similaires sont envisageables, par exemple un banquier qui hésiterait à accorder un prêt à un client. Tous ces scénarios sont très simples à mettre en place.

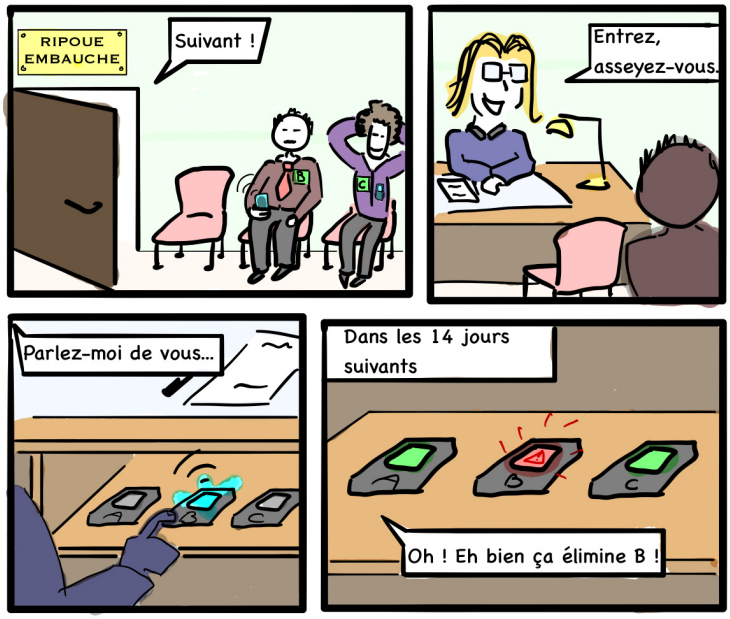

FIG. 2 – *Possible détournement de l'application lors d'un entretien d'embauche.*

20. Des techniques simples permettent également d'installer de multiples fois la même application sur le même téléphone, ce qui facilite encore une telle approche.

Scénario 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.*

En fonction des détails techniques du protocole, il pourrait être possible de créer de fausses identités dans l'application pour tracer un grand nombre de personnes sans avoir à acheter un téléphone pour chaque cible. On peut aussi capter les messages Bluetooth à grande distance (plus d'un kilomètre [9]) avec une antenne dédiée. Dans le modèle décentralisé, on capture ainsi le pseudonyme de la cible, et on peut vérifier s'il fait partie de ceux identifiés comme malades dans les deux semaines qui suivent. Les scénarios d'attaque précédents sont possibles pour tous les protocoles de traçage envisagés, mais plus simples à mettre en œuvre dans le modèle décentralisé.

6 Comment déclencher une fausse alerte et faire croire à quelqu'un qu'il risque d'être malade ?

Scénario 7 (Le militant anti-système)**.** *M. Hanty, qui présente des symptômes du COVID-19, est un militant anti-système. 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 est testé positif ; tous les promeneurs reçoivent une notification.*

Scénario 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.*

Le même scénario peut être utilisé pour cibler des personnes précises (adversaire lors d'une compétition sportive, concurrent pour un entretien d'embauche, personne-clef lors d'une négociation, ...) ou de manière collective à grande échelle pour rendre l'ensemble du système inopérant. La possibilité de déclencher de fausses alertes pourrait aussi être exploitée dans des scénarios dans lesquels un utilisateur fait croire qu'il a croisé un malade pour être testé en priorité, bénéficier d'un arrêt de travail, ou encore échapper à une échéance qu'il redoute, comme dans le scénario suivant.

Scénario 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 !*

7 Activer le Bluetooth pose des problèmes de sécurité

Le simple fait d'activer le Bluetooth sur son téléphone pose des problèmes de sécurité et de respect de la vie privée, c'est d'ailleurs pourquoi il est généralement recommandé de le désactiver le plus souvent possible.

Son utilisation peut en effet ouvrir des failles de sécurité qui exploiteraient des bugs dans le système Bluetooth du téléphone. Concrètement, l'attaque Blueborne [10] publiée en 2017 permettait justement de prendre le contrôle de nombreux équipements (ordinateurs, téléphone, ...) en exploitant ce type de bug. Si certains téléphones n'ont pas été mis à jour depuis 2017, activer le Bluetooth pourrait être très dangereux !

Le signal Bluetooth peut aussi être utilisé pour tracer les utilisateurs. Chacun d'entre nous a déjà pu observer à quel point il était facile d'identifier les appareils connectés en Bluetooth chez ses voisins ou utilisés par les voyageurs dans un train. Généraliser son utilisation ouvre de multiples possibilités.

Scénario 10 (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.*

Scénario 11 (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.*

Plusieurs chaînes de grands magasins utilisent déjà un traçage Bluetooth pour suivre leurs clients dans le magasin, et mieux cibler la publicité [11]. Si l'usage du Bluetooth se généralise, on peut imaginer de nombreuses façons de l'exploiter pour bien d'autres sortes de traçage.

8 Vers un système parallèle de fichage à grande échelle ?

Même si l'application envisagée ne procédera pas elle-même à un traçage des malades, il est possible d'utiliser les signaux échangés par l'application pour mettre en place un fichage à grande échelle. La difficulté de mise en œuvre d'un tel fichage varie avec les détails techniques du protocole utilisé. C'est particulièrement facile avec un système décentralisé, car la liste des pseudonymes des malades est publique, et il suffit donc de les ré-identifier. Avec un système centralisé, il faut pouvoir créer une fausse identité ou utiliser un nouveau téléphone puis entrer en contact avec la personne à tracer. Mais dans tous les cas, il sera difficile de définir un protocole qui évite complètement ce type d'attaque.

Par les utilisateurs. Le traçage peut être fait par les utilisateurs eux-mêmes, dans le but de mieux se protéger. Les informations échangées pour le traçage sont à l'échelle locale. Mais si les utilisateurs unissent leurs forces, ils peuvent reconstruire une information globale, comme dans les applications de détection de radars routiers. Par exemple, on ne peut empêcher l'apparition d'une application « améliorée » (appelons-la

GeoTraceVIRUS) qui enregistrerait les endroits où se trouvent des malades, en plus de tracer les contacts directs avec des malades.

Dans un système décentralisé, il suffit que GeoTraceVIRUS enregistre les coordonnées GPS en même temps que les messages Bluetooth qu'il reçoit. Quand un pseudonyme est déclaré malade, GeoTraceVIRUS permet de savoir exactement où il se trouvait lorsqu'il l'a reçu, et partage cette information avec les autres utilisateurs. Dans un système centralisé, GeoTraceVIRUS peut enregistrer les déplacements des utilisateurs, et procéder par recoupement quand certains utilisateurs reçoivent une notification TraceVIRUS. Avec suffisamment d'utilisateurs de GeoTraceVIRUS, cela permet au moins de localiser dans quel quartier habitent les malades.

Scénario 12 (L'application GeoTraceVIRUS)**.** *Peu après avoir installé l'application TraceVIRUS, 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.

Une autre application « améliorée », que des utilisateurs pourraient être tentés d'installer, proposerait de booster le signal Bluetooth pour être prévenu en cas de contact moins proche avec des malades. Certaines de ces applications alternatives pourraient être malveillantes, et aspirer les données privées des utilisateurs.

Indépendamment de la qualité de l'application officielle, les signaux Bluetooth sur lesquels elle repose pourront être réutilisés par d'autres applications dont la prolifération paraît difficilement gérable.

Par les entreprises d'analyse de données. Suite au scandale Cambridge Analytica [12], on sait que certaines entreprises n'hésitent pas à collecter des données de façon illégale dans le but de les monnayer. Des compagnies d'assurance ou des employeurs peu scrupuleux pourraient être intéressés par une liste de malades du COVID-19, par exemple si le fait d'avoir contracté la maladie augmente les risques de séquelles. Même si l'État ne possède pas de telle liste, l'utilisation d'une application de traçage rend possible la création d'un tel fichier par des acteurs privés.

Scénario 13 (L'assurance)**.** *La chaîne de supermarché SansScrupule utilise des traceurs Bluetooth pour suivre les clients dans ses magasins [11]. 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.*

Par des cyber-criminels. La multiplication des attaques informatiques organisées au cours des dernières années suffit à se convaincre que le cyber-crime organisé pourrait aussi essayer de récupérer ces informations.

Scénario 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, en 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.

Scénario 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 !

Une application malveillante de ce type fonctionnerait grâce à des émetteurs ou récepteurs proches de personnes susceptibles d'être infectées (à proximité d'un laboratoire d'analyses médicales par exemple). Il suffirait ensuite de relayer les messages entre les personnes potentiellement infectées et la personne qu'on souhaite déclarer à risque. Cela peut être mis en œuvre dans plusieurs des systèmes de traçage proposés (par exemple: très facilement pour DP3T, avec un peu plus de technologie pour ROBERT).

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.*

Références

[1] Ross Anderson. Contact tracing in the real world. Publié et consulté le 12 avril 2020 : https://www.lightbluetouchpaper.org/2020/04/12/contact-tracing-in-the-real-world/.

[2] Susan Landau. Looking beyond contact tracing to stop the spread. Publié le 10 avril 2020, consulté le 14 avril 2020 : https://www.lawfareblog.com/looking-beyond-contact-tracing-stop-spread.

[3] Bruce Schneier. Contact tracing COVID-19 infections via smartphone apps. Publié et consulté le 13 avril 2020 : https://www.schneier.com/blog/archives/2020/04/contact_tracing.html.

[4] Serge Vaudenay. Analysis of DP3T. Cryptology ePrint Archive, Report 2020/399, 2020. https://eprint.iacr.org/2020/399.

[5] Pascale Fombeur. Un décret d'application ne peut renvoyer à un arrêté ultérieur la mise en œuvre des principes de la loi. *AJDA*, page 831, 2000.

[6] Alan Hunt. *Explorations in Law and Society. Toward a Constitutive Theory of Law*. New York, Routledge, 1993.

[7] La Quadrature du Net. Nos arguments pour rejeter StopCOVID. Publié et consulté le 14 avril 2020 : https://www.laquadrature.net/2020/04/14/nos-arguments-pour-rejeter-stopcovid/.

[8] Frédéric Pierru. Les recompositions paradoxales de l'Etat sanitaire français. Transnationalisation, étatisation et individualisation des politiques de santé. *Education et Sociétés*, 2012/2(30):107–129, 2012.

[9] John Hering, James Burgess, Kevin Mahaffey, Mike Outmesguine, and Martin Herfurt. Long Distance Snarf, August 2004. https://trifinite.org/trifinite_stuff_lds.html, consulté le 18 avril 2020.

[10] Ben Seri and Gregory Vishnepolsky. The dangers of Bluetooth implementations: unveiling zero day vulnerabilities and security flaws in modern Bluetooth stacks.

[11] Michael Kwet. In stores, secret surveillance tracks your every move, June 2019. https://www.nytimes.com/interactive/2019/06/14/opinion/bluetooth-wireless-tracking-privacy.html, consulté le 18 avril 2020.

[12] Wikipédia. Scandale Facebook-Cambridge Analytica, 2020. http://fr.wikipedia.org/w/index.php?title=Scandale_Facebook-Cambridge_Analytica, consulté le 18 avril 2020.