“Contact-Tracing” respecteux de la vie privée

Utilité et sécurité

Benjamin NGUYEN[1]

[1] Laboratoire d’Informatique Fondamentale d’Orléans (LIFO)
INSA Centre Val de Loire
Université d’Orléans

April 28, 2020

Outline I

Avertissement

Une tentative pour éclairer l’actualité par des considérations scientifiques

Nous sommes dans l’actualité brulante

- Un débat, et un vote (non contraignant) à l’Assemblée Nationale mardi 28/4/2020
- Des débats et des décisions dans d’autres pays européens (déploiement d’une app en Autriche, refus du déploiement en Belgique, incertitude quant au type d’app à déployer en Allemagne) et dans d’autres pays tout court (app très intrusive déployée à Singapour [MoH20])

Objectifs de cette présentation

Vous permettre de vous construire une opinion sur la question en vous présentant :

- Le contexte et le problème de vie privée liée au contact tracing (sans se positionner sur l’aspect “éthique”)
- Deux solutions concurrentes en cours de développement (DP3T [CT20] et ROBERT [IP20])
- Quelques éléments de réflexion de ma part (avec Cédric Eichler et Nicolas Anciaux) basés sur une approche de *differential privacy*.

Contexte

Impact de l’épidémie sur les droits fondamentaux

L’épidémie de Covid19

- Une situation inédite en période de paix en France.
- Le confinement, une solution “massue” et sous-optimale ?
- Peut-on savoir qui il faut confiner et qui déconfiner de manière automatique (ou plus ou moins guidée par une politique publique) ?

Impact sur les droit fondamentaux

- En faveur des droits fondamentaux : liberté de déplacement, liberté de réunion, liberté de culte, etc.
- En défaveur des droits fondamentaux : égalité de traitement (pour ceux qui ne peuvent pas installer l’app), liberté d’opinion (ne pas installer l’app), vie privée
- **Il n’y a pas de hiérarchie pour les droits fondamentaux, même si l’un peut prendre le pas sur l’autre dans certaines circonstances.**

Contexte

Peut-on améliorer la situation ?

Un problème d’optimisation ! (Maxime ANTOINE, Juriste)

- *Vu ce qui précède on observe des effets potentiellement favorables et défavorables sur les droits fondamentaux qu’il convient de mettre en balance (bénéfice/risque classique).*
- *Une fois qu’on a déterminé que le jeu en valait la chandelle, il convient de rentrer dans le moule juridique existant ou réformé (c’est pratique d’être l’Etat :p).*
- *A ce jour, il n’y a à mon sens pas que très peu de problématiques juridiques majeures puisque le RGPD permet le traitement de données de santé ou de géolocalisation sur le fondement du consentement ou de l’obligation légale. Les finalités sont bien déterminées, la minimisation et la durée de conservation est bien dans les têtes de chacun, l’information sera à n’en pas douté claire et transparente et le consentement éclairé.*

Contexte

Quels algorithmes d’aide à la décision mettre en place ?

La possibilité grâce aux technologies “informatiques” de personnalisation

- D_1 : Diagnostic automatique et personnalisé. Pourrait se mesurer par une valeur de risque ($r \in [0;1]$). Se mesure a priori par un booléen $atRisk \in \{0,1\}$
- D_2 : Aide à la décision post-diagnostic automatique et personnalisé. Peu spécifié à l’heure actuelle. (i.e. popup avec un numéro de téléphone à appeler). Des éléments (e.g. avis de la CNIL [CNI20] du 26/4) peuvent donner à penser qu’une décision de confinement automatisée pourrait être prise.

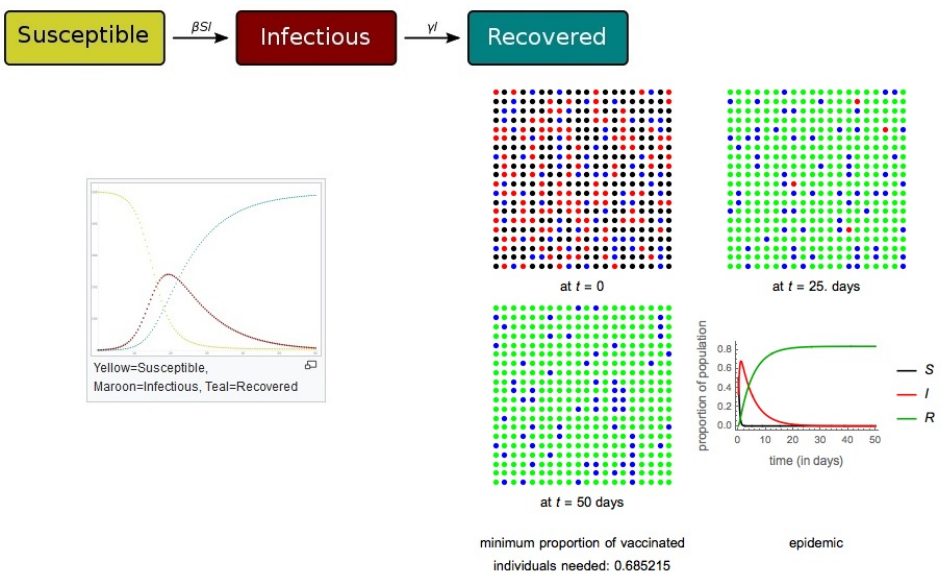
Idée : développer une application (*StopCovid*) qui sera installé sur le téléphone de chaque personne.

Contexte

Le diagnostic médical

D_1 : Diagnostic médical

Une épidémie se mesure habituellement avec un modèle SIR [WOK27] ou SIS (Susceptible, Infected-Contagious, Recovered-NonContagious / Susceptible, Infected, Susceptible) qui est un modèle de propagation classique. Il est paramétré par un taux d'infection β, et un taux de guérison γ. Permet de calculer des données “macro” comme le R_0 (nombre de reproductions)



Contexte

Le diagnostic médical

L’approche *StopCovid*

- Dans l’approche *StopCovid*, le modèle est différent : chaque individu doit avoir un diagnostic personnalisé. Ce diagnostic est calculé à partir d’un risque d’être infecté, en faisant l’hypothèse qu’on connait ses voisins, et leur état (S, I, ou R).
- Cette décision peut utiliser des données personnelles complémentaires (age, condition médicale, mesures de prévention personnelles, etc.)
- La valeur S, I ou R ne peut être connue en réalité qu’après un *test médical*

Contexte

La décision *comportementale*

D_2 : Décision comportementale

Une fois qu’on connait son risque, les autorités sanitaires qu’on appelle au téléphone (ou l’app de manière automatique) pourront indiquer un comportement à adopter : aller se faire tester (serait-on prioritaire ?), se confiner sans faire de test, se laver les poumons à l’eau de javel, etc. Cette décision peut être prise en utilisant (ou pas) des données personnelles *complémentaires* comme l’age, le métier, les antécédents médicaux, etc.

Contexte

Qui a écrit les algorithmes ?

D_1

L’algorithme de décision du risque médical est développé par les médecins ou le ministère. L’algorithme peut être très simple, cf Singapour [MoH20] : si vous avez un contact “non protégé” de plus de 30 minutes avec une personnes infectée à moins de 2m. Pour fonctionner, cet algorithme nécessite donc :

- De pouvoir mesurer une distance
- De pouvoir connaitre l’état d’infection des voisins
- De pouvoir mesurer une durée d’exposition

Paramètres mesurés

- La position ou proximité : GPS, Bluetooth ou ultrasons
- La durée : horloge interne
- L’état des voisins : problème de confidentialité des données. Divers algos ont été proposés (dont DP3T, ROBERT).

Contexte

Qui a écrit les algorithmes ?

D_2

Je n’ai pas pour le moment pu obtenir de version pour l’algorithme de décision du comportement. On peut penser que l’algorithme pourrait demander à toutes les personnes à risque de se confiner par défaut sans test, et d’aller se faire tester si on est un personne prioritaire à pouvoir sortir (e.g. personnel soignant, policier, enseignant, pilote de centrale nucléaire, etc.)

Le point de vue GDPR

Il serait très étonnant qu’il soit possible de prendre une décision automatisée de confinement en se basant uniquement sur le résultat de l’app. (cf. décisions de justice automatique, décision de prêts automatiques, etc.)

Contexte

Les tests

Les tests par jour

- On fait actuellement environ 30K test par jour en France
- Objectif le 11 mai : 100K
- Objectif en Allemagne : 1M

Pourquoi est-ce important ?

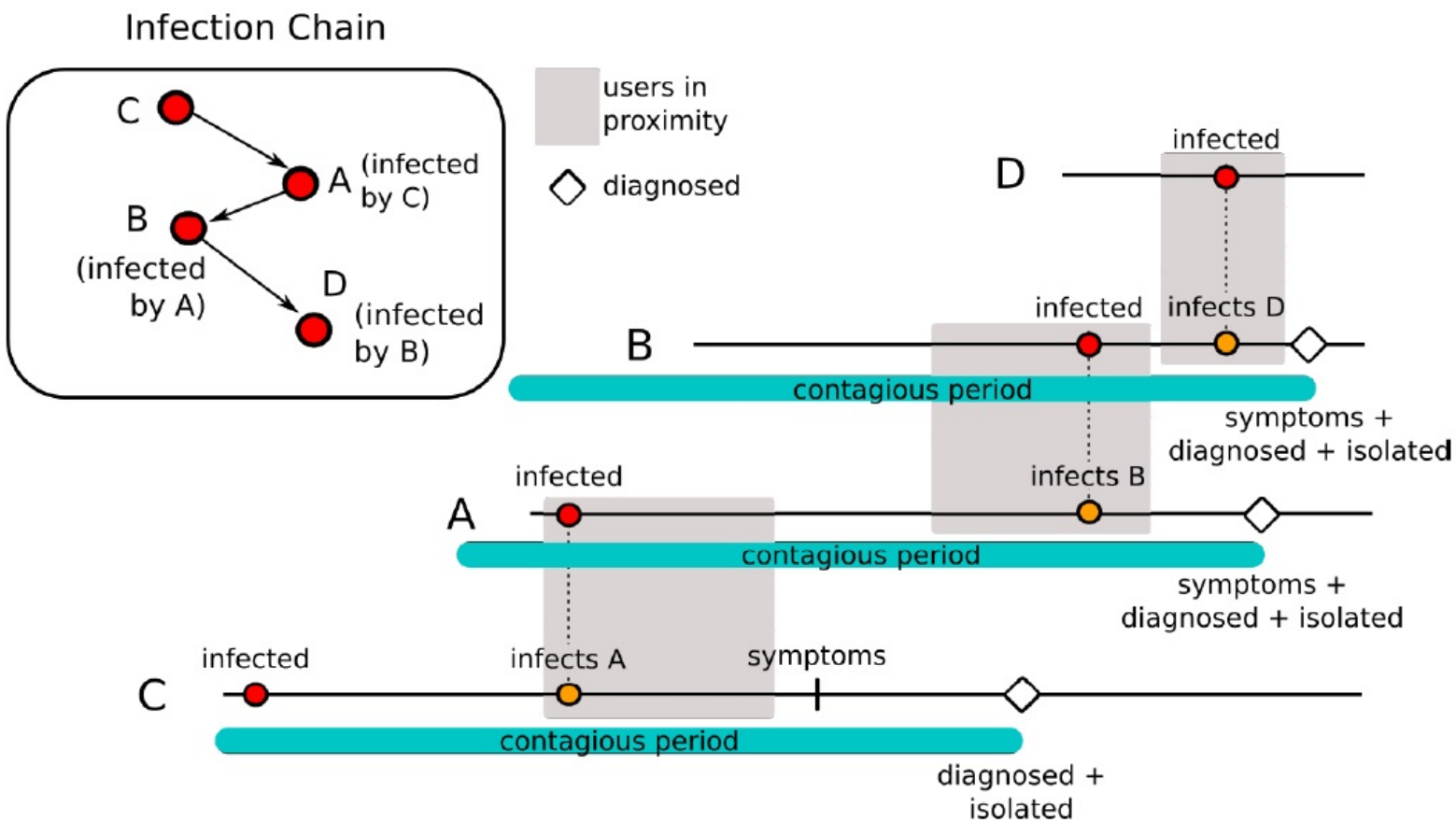
- Permet de donner une valeur “certifiée” (modulo les erreurs de chimie) à un état S, I ou R
- On peut ensuite développer une politique publique sur cette base : e.g. tester les personnes ayant un “travail indispensable” et laisser sortir les S ou R, ou tester des personnes en contact avec des I, et confiner les I, ou tout autre politique en 2 phase : i) test d’une partie spécifique (ou pas) de la population ii) application d’une règle de décision selon l’état du test

Le nombre de tests en France est faible ! Mais on ne connait pas non plus la distribution des S/I/R à la sortie du confinement (ou nous dit que $S \approx 90\%$)

Contexte

Mais au fait, pourquoi confiner avec une app ?

Quelle est l’utilité du confinement avec une app, et pourquoi serait-ce intéressant (pour ralentir l’épidémie) de confiner des personnes ayant été en contact avec des individus malades ?



Contexte

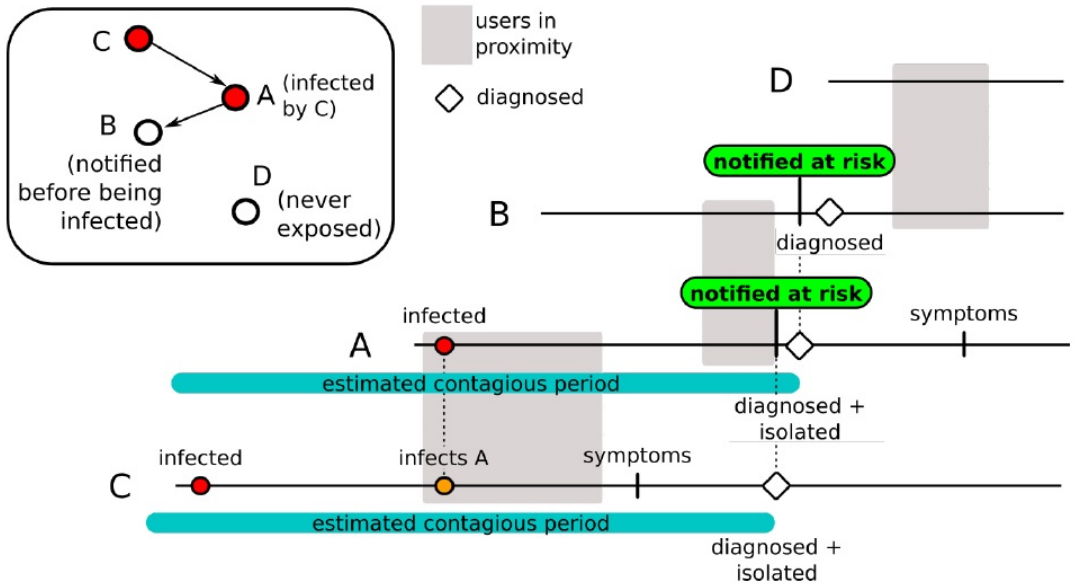


Figure 2: Example of the infection process with proximity tracing App that starts with person C being infected.

Figure: D’après [IP20]

Evaluation “PVP” : une mise en balance utilité vs. risque

Approche générale

Etude d’impact

Pour pouvoir déployer une application d’aide à la décision automatisée, et de mesurer son impact sur la vie privée, il convient tout d’abord de montrer que l’application est *utile*.

Définition : Utilité

L’utilité d’un algorithme de prise de décision est mesuré par la qualité de ses résultats sur un jeu de microdonnées exactes. On qualifiera cet algorithme avec les métriques habituelles : Précision, rappel, taux de FP, taux de FN, F-mesure, ROC, etc.

Cette définition peut être utilisée pour quantifier D_1.

Evaluation “PVP” : une mise en balance utilité vs. risque

Comment quantifier D_2 ?

Utilité de D_2

L’utilité de D_2 peut être mesurée par rapport à un (ou plusieurs) critère(s) à optimiser : par exemple par le nombre maximal de personnes infectée à un instant donnée, ou le nombre total de morts, la durée du confinement multipliée par le nombre de personnes confinées, etc.

Utilité de *StopCovid*

Ferretti *et al.* [FWK+20] ont montré que l’efficacité de l’application dépend quadratiquement de son taux d’adoption, sous l’hypothèse qu’une personne se confine dès qu’elle reçoit l’information qu’elle est *à risque* (par opposition à un modèle où on ne confine que les personnes symptomatiques).

Par ailleurs, on pourra noter que le taux de possession d’un smartphone dépend beaucoup de l’age (moins de 44% des plus de 65 ans).

Evaluation “PVP” : une mise en balance utilité vs. risque

Comment quantifier D_2 ?

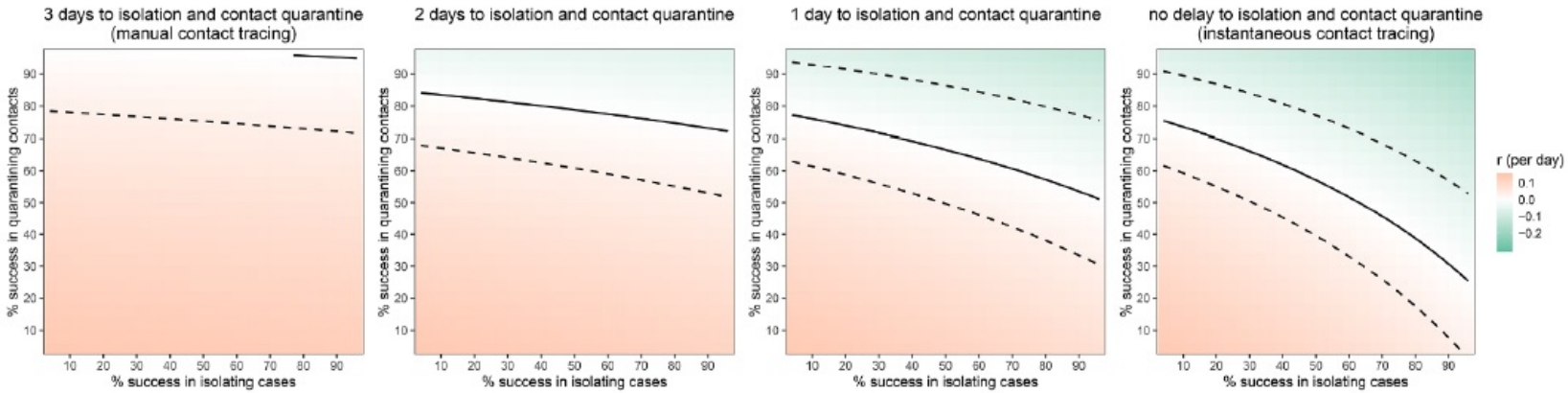


Fig. 3. Quantifying intervention success. Heat map plot showing the exponential growth rate of the epidemic r as a function of the success rate of instant isolation of symptomatic cases (x axis) and the success rate of instant contact tracing (y axis). Positive values of r (red) imply a growing epidemic; negative values of r (green) imply a declining epidemic, with greater negative values implying faster decline. The solid black line shows r=0, i.e., the threshold for epidemic control. The dashed lines show uncertainty in the threshold due to uncertainty in R_0 (see figs. S15 to S17). The different panels show variation in the delay associated with the intervention - from initiating symptoms to case isolation and quarantine of contacts.

Figure: D’après [FWK+20]

Evaluation “PVP” : une mise en balance utilité vs. risque

Comment quantifier D_2 ?

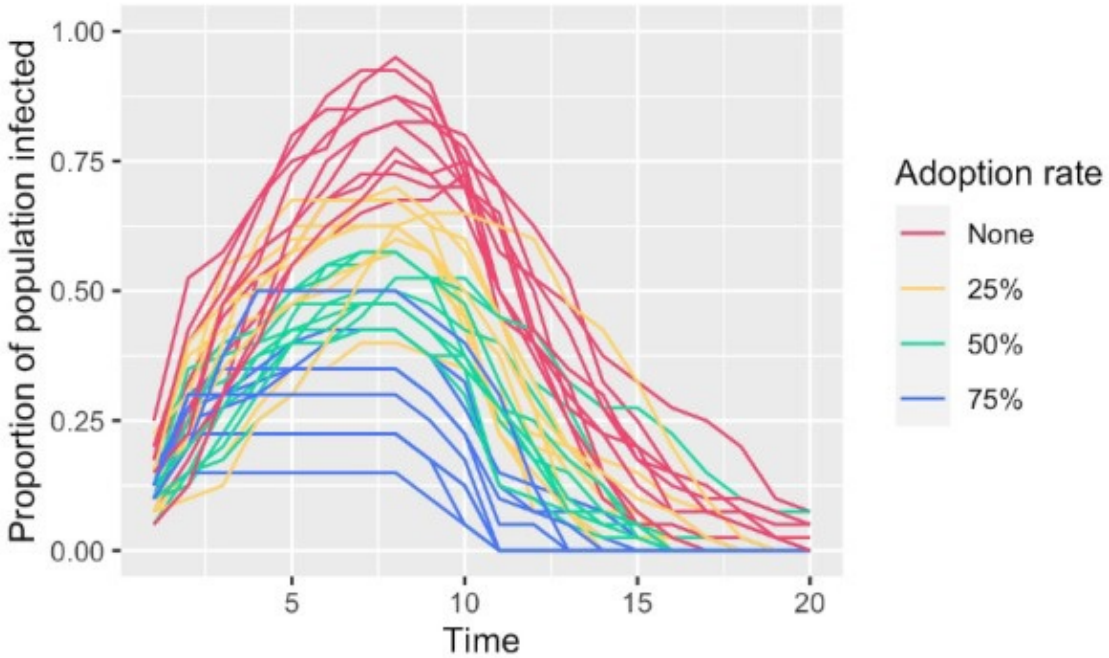


Figure: D’après [YLS20]

Comparison of infection curves from simulations at varying rates of peer-to-peer contact tracing application adoption. The proportion of the population with active infection is plotted across time for multiple adoption rates. Time is an arbitrary unit that represents the sequence of events in the simulation. The results of 10 random simulations per adoption rate are given.

Evaluation “PVP” : une mise en balance utilité vs. risque

Est-ce que D_1 marche ?

L’application mobile est-elle performante pour lutter contre l’épidémie ?

- Adoptabilité de l’application (ce qui poser la question qu’elle soit obligatoire)
- Problème de catégories d’age n’ayant pas de mobile
- Faux positifs

Exist-t-il une technique tout aussi efficace et moins invasive pour atteindre le même objectif ?

Continuer avec les interview papier ?

Evaluation “PVP” : une mise en balance utilité vs. risque

Est-ce que D_2 marche ?

Est-ce que la décision algorithmique est légale ? Souhaitable ? Ethique ? L’avis de la CNIL rendu le 26/4 est plutôt en faveur de la mise en place d’une app [CNI20].

Les risques

Quantifier le risque de fuite de données

Qu’est ce qui peut fuiter ?

- Une donnée personnelle : le statut infecté ou non
- Des données personnelles : le cercle et l’horaire de rencontres
- D’autres données nécessaires pour faire le calcul de D_1 : age, localisation, . . .

Est-ce que ça va fuiter ?

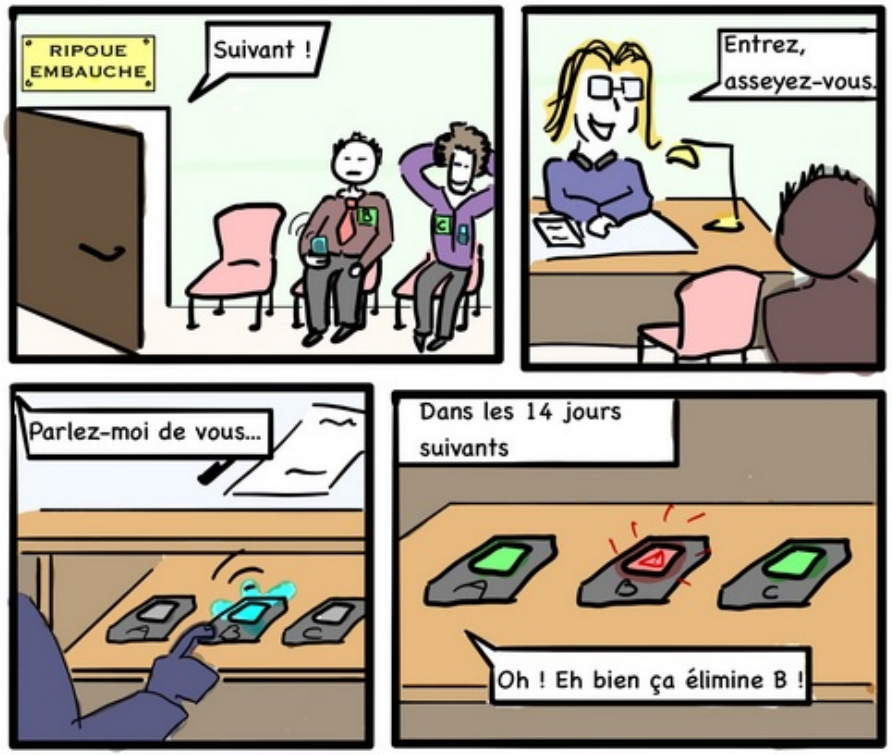
- Il faut monter une attaque (pas forcément simple selon le modèle d’attaque)
- Il faut faire croire au modèle d’attaque (on va en discuter par la suite)

Est-ce un problème vu l’utilité qu’on va tirer de cette application ?

Je vous laisse vous faire votre propre opinion.

Attaques génériques sur *StopCovid*

Pour les nuls



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.

Figure: D’après [XB20]

Attaques génériques sur *StopCovid*

Principe

Un certain nombre d’attaques génériques ont été proposées dans [XB20]. Certaines concernent la vie privée (obtenir la valeur d’une donnée sensible), d’autres pas.

Attaques génériques sur *StopCovid*

Quelques exemples

PVP : Suspect unique

On utilise spécifiquement un téléphone qu’on allume une seule fois, juste lorsqu’on est à côté de la personne qui nous intéresse, puis on isole le téléphone. Si jamais on obtient une notification qu’on est “à risque” c’est que la personne a été testée positive. **Applications :** entretien d’embauche, paparrazzi.

Contremesure

Utilisation de faux positifs et de faux négatifs.

Attaques génériques sur *StopCovid*

Quelques exemples

Coercition

Une supermarché (ou une milice) vous oblige à utiliser l’application alors qu’elle est optionnelle.

Contremesure

Tout comme dans le vote électronique, on doit pouvoir passer l’app dans un mode “mensonge” qui ne dévoile pas la donnée personnelle, e.g. en tapant un pin code qui ne passe dans le mode véritable que s’il est correct.

Attaques génériques sur *StopCovid*

Quelques exemples

Déni de service (militant anti-système ou agent secret)

- En attachant un téléphone infecté à son chien qu’on laisse courir dans un parc, on réussit à infecter de nombreuses personnes.
- En infectant le téléphone d’individus spécifiques (par exemple des militaires) on peut réussir à empêcher un bâtiment de guerre d’appareiller.

Contremesure

Détection d’outliers ou résolution hors technologie (la protection se fait au niveau de D_2).

Le protocole Decentralized Privacy Preserving Proximity Tracking

Algorithme

1. Au départ, l’app est installée sur le téléphone et se crée un clé secrète SK_0 (chaque utilisateur dispose donc de sa clé)
2. Chaque jour, l’app calcule une nouvelle clé $SK_{n+1} = H(SK_n)$ à l’aide d’une fonction de hachage publique.
3. Chaque jour, l’app calcule une liste de 24×60 identifiant temporaires ($EphID_i$) à l’aide d’une fonction pseudo aléatoire et un algorithme de chiffrement : $EphID_1||...||EphID_n = PRG(PRF(SK_t, ``public\_string''))$
4. L’app émet en continu son $EphID_i$ actuel, et stocke les $EphID$ des autres appareils à proximité (et d’autres données comme t, i, la force du signal), sans jamais les transmettre. C’est pour cette raison que l’approche est dite “decentralized”.
5. Lorsqu’un utilisateur est testé positif, il publie auprès du serveur backend la SK_t correspondant à sa première époque infectieuse, ainsi que t. En faisant ça, l’app doit également choisir une nouvelle clé SK_{new}
6. Tous les jours, le serveur backend transmet la liste des SK_t, t.
7. Tous les jours, chaque app peut donc voir si elle a été en contact à un moment donné avec une personne infectée en testant ses $EphID$ stockés par rapport à ceux qu’elle peut recalculer. Elle peut ensuite exécuter l’algorithme D_1, et éventuellement D_2.

Le protocole Decentralized Privacy Preserving Proximity Tracking

Modèle d’attaque

Utilisateur lambda

Honnête mais curieux. Il n’a que les informations données par l’app le concernant, mais peut essayer en utilisant cette connaissance d’inférer des données sur les autres utilisateurs.

Utilisateur technophile

Peut observer les données qui transitent sur le téléphone, au niveau du BT (avec une antenne). Peut modifier le code de sa propre application. Peut vouloir effectuer une attaque DoS.

Espionnage par l’infrastructure

ISP, sysadmin, etc. Ces attaques sont clairement en violation des lois.

Autorité de santé

Ne doit apprendre l’état de santé d’un utilisateur que si celui-ci décide de le partager avec l’autorité.

Le protocole Decentralized Privacy Preserving Proximity Tracking

Modèle d’attaque

Epidémiologistes

Dans le cadre de DP3T une fonctionnalité est le partage d’informations dans le cadre d’études épidémiologiques, sur la base du volontariat.

Serveur backend

Covert. Observe ce qu’il voit, peut tout stocker, peut modifier du code tant qu’il ne se fait pas détecter.

Services de l’état

Covert. Souhaite retrouver les informations des individus, et possède des moyens techniques illimités.

Attaquant à budget illimité (un autre état)

Attaquant malicieux.

ROBust and privacy-presERving proximity Tracing

Algorithme

1. Lors de l’installation, l’app génère un *ID* unique, qui est ensuite transmis au serveur backend.
2. Le serveur utilise *ID* pour générer une liste d’identifiants temporaires $EBID_t$ qui sont envoyé régulièrement à l’app (d’où le fait que cette approche est considérée comme “centralized”)
3. L’app émet en continu la valeur de son $EBID_t$, en la changeant toutes les x minutes
4. L’app stocke la liste des *EBID* qu’elle capte à proximité (et a priori pas d’autre info)
5. Si un individu utilisant l’app est infecté, il envoie via un *mixnet* la liste des *EBID* avec qui il a été en contact
6. Le serveur backend déchiffre les *EBID* pour retrouver les *ID* des individus en contact, et lance l’algorithme D_1.
7. Chaque individu peut demander son statut au serveur. Si le statut est “à risque”, l’app passe en mode limité, et se bloque. Seule l’autorité de santé pourra débloquer l’app suite à un test covid négatif.

ROBust and privacy-presERving proximity Tracing

Modèle d’attaque

Le modèle d’attaque de ROBERT est similaire à celui de DP3T, à ceci près que le serveur backend est **trusted**. Le modèle d’attaque de l’OS / constructeur est moins clair (covert ?).

Quelques attaques sur DP3T [Vau20]

Impersonnification du serveur central

Un individu contamine un utilisateur honnête de l'app via un *EphID* généré à partir d'une SK_x. Il intercepte ensuite la communication avec le serveur et l'individu et envoie SK_x à l'individu honnête.

Replay attack

Un individu malhonnête décide de dériver un *EphID* à partir d'un SK_x contaminé publié par le serveur. Il émet ensuite ce *EphID* afin de contaminer d'autres personnes (il dispo a priori d'un jour pour le faire).

Une “attaque” sur ROBERT

Impossibilité d’audit à posteriori

Pour des raisons de minimisation, les données sur l’état Covid+ des individus est effacé au bout d’un certain temps (15j). Comment est-il possible d’auditer la décision de l’algorithme qui aura i.e. décidé du confinement d’une personne ? Il serait donc possible de bloquer des individus chez eux, sans donner de justification.

DP3T vs ROBERT

Décentralisé vs centralisé ? Ou enjeu de gouvernance des données ?

Indépendamment des attaques sur les protocoles qui peuvent exister, les modèles d’attaque eux-mêmes posent problème.

Serveur central

ROBERT fait confiance au serveur central (opéré par l’état), le serveur connait les *ID* et est capable de déidentifier un individu, en connaissant son $EBID_t$ et t. Dans DP3T le serveur d’obtient jamais cette information (qui reste dans le téléphone – même si des attaques d’impersonnification sont possibles)

Google/Apple

Dans DP3T, l’utilisateur fait confiance au constructeur de son téléphone, puisqu’il y stocke sa clé SK_0 ce qui permet de calculer les *EphID*. Ce n’est pas le cas de ROBERT où seuls les *EBID* du passé transitent par le téléphone.

En qui avez vous confiance ?

Google/Apple ? L’état français ? Et si vous étiez russe ? Chinois ? Américain ? Qui connait déjà tout un tas d’informations sur vous ?

Peut-on proposer une application plus respectueuse de la vie privée ?

Une approche basée sur la *differential privacy*

Differential Privacy

La *differential privacy* (confidentialité différentielle) peut apporter des garanties probabilistes d'anonymat pour un algorithme. Cette contrainte quantifie la probabilité de pouvoir désanonymiser (i.e. déduire des informations au sujet d'un individu) un individu en observant le résultat de l'exécution d'un algorithme.

Définition

Soit $\varepsilon \in \mathbb{R}^{+*}$, $\delta \in \mathbb{R}^{+}$ et $\mathscr{A}$ un algorithme aléatoire prenant en entrée un jeu de données D. On note $\mathrm{im}\ \mathscr{A}$ l'image de $\mathscr{A}$. L'algorithme $\mathscr{A}$ est dit respecter la contrainte de ε, δ-differential privacy si, pour tous les jeux de données D_1 et D_2 tels qu'ils ne diffèrent que sur un seul élément (i.e. les données d'une personne) alors quel que soit $S \in \mathrm{im}\ \mathscr{A}$ on a :

$$\Pr[S|\mathscr{A}(D_1)] \leq \exp(\varepsilon) \cdot \Pr[S|\mathscr{A}(D_2)] + \delta$$

Peut-on proposer une application plus respectueuse de la vie privée ?

Une approche basée sur la *differential privacy*

Approche DP classique

Une technique classique pour protéger une donnée personnelle est de la bruiter. Si c’est une donnée numérique, avec la distribution de Laplace. Si c’est une données catégorielle, avec le mécanisme exponentiel. Dans tous les cas, la donnée publiée a des chances d’être vraie mais aussi des chances d’être fausse.

On retrouve les contremesures proposées contre les attaques de vie privée.

Peut-on proposer une application plus respectueuse de la vie privée ?

La DP battue en brèche par la CNIL ?!

Problème : avis de la CNIL [CNI20]

Sur l’exactitude des données La Commission relève que, dans le protocole technique qui lui a été transmis, il est envisagé qu’on puisse introduire des faux positifs dans les notifications transmises aux personnes afin de limiter les risques de ré-identification dans certains types d’attaques. Elle considère que cette mesure ne peut ni ne doit être mise en œuvre, dès lors qu’elle aurait pour conséquence d’alerter faussement des personnes n’ayant pas eu de contact à risques, et qui seraient dès lors encouragées à se soumettre à des mesures de confinement volontaire consistant en une restriction auto-imposée de leurs libertés individuelles. Elle souligne que maintenir l’exactitude des données est une obligation légale impérieuse au titre du RGPD et de la loi « Informatique et Libertés » et qu’une telle mesure n’est pas envisageable, sous peine de remettre en cause la conformité du traitement au regard des textes applicables.

To be continued

Stop ou encore

La suite au prochain épisode

Vote de l’assemblée demain (non contraignant) pour savoir si on arrête avec le projet de l’app *StopCovid* ou si on continue, et si oui peut être qu’il y aura des éléments de décision sur le côté “centralisé” ou “décentralisé”.

Pour vous inscrire à la liste de diffusion au sujet du traçage du GDR Sécurité : `https://gdr-securite.irisa.fr/actualite/liste-de-diffusion-covid-19/`

References I

CNIL, *Délibération n 2020-046 du 24 avril 2020 portant avis sur un projet d'application mobile dénommée « stopcovid »*, 2020, https://www.cnil.fr/sites/default/files/atoms/files/deliberation_du_24_avril_2020_portant_avis_sur_un_projet_dapplication_mobile_stopcovid.pdf.

Jean-Pierre Hubaux Marcel Salathé James Larus Edouard Bugnion Wouter Lueks Theresa Stadler Apostolos Pyrgelis Daniele Antonioli Ludovic Barman Sylvain Chatel Kenneth Paterson Srdjan Čapkun David Basin Jan Beutel Dennis Jackson Bart Preneel Nigel Smart Dave Singelee Aysajan Abidin Seda Guerses Michael Veale Cas Cremers Reuben Binns Ciro Cattuto Carmela Troncoso, Mathias Payer, *Decentralized privacy preserving proximity tracing*, 2020,

References II

https://github.com/DP-3T/documents/blob/master/DP3T%20White%20Paper.pdf.


Luca Ferretti, Chris Wymant, Michelle Kendall, Lele Zhao, Anel Nurtay, Lucie Abeler-Dörner, Michael Parker, David Bonsall, and Christophe Fraser, *Quantifying sars-cov-2 transmission suggests epidemic control with digital contact tracing*, Science (2020).


Fraunhaufer AISEC Inria PRIVATICS, *Robert: Robust and privacy-preserving proximity tracing*, 2020, https://github.com/ROBERT-proximity-tracing/documents/blob/master/ROBERT-specification-EN-v1_0.pdf.


Singapore Ministry of Health, *Tracetogether*, 2020, https://www.tracetogether.gov.sg/.

References III


Serge Vaudenay, *Analysis of dp3t, between scylla and charybdis*, Tech. report, 2020, https://eprint.iacr.org/2020/399.pdf.


A.G. Mc Kendrick William Ogilvy Kermack, *A contribution to the mathematical theory of epidemics*, Proceedings of the Royal Society A **115** (1927), no. 772, 700–721.


VéroniqueCortier Pierrick Gaudry Lucca Hirschi Steve Kremer Stéphanie Lacour Matthieu Lequesne Gaëtan Leurent Léo Perrin André Schrottenloher Emmanuel Thomé Serge Vaudenay Christophe Vuillot Xavier Bonnetain, Anne Canteaut, *Le traçage anonyme, dangereux oxymore. analyse de risques à destination des non-spécialistes*, 2020, https://risques-tracage.fr/docs/risques-tracage.pdf.

References IV

T. M. Yasaka, B. M. Lehrich, and R. Sahyouni, *Peer-to-peer contact tracing: Development of a privacy-preserving smartphone app*, JMIR mHealth and uHealth **8** (2020), no. 4, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7144575/.