

Contact-Tracing / Exposure-Notification
respectueux de la vie privée
Utilité, Sécurité et un premier retour d'expérience

Benjamin NGUYEN¹

¹Laboratoire d'Informatique Fondamentale d'Orléans (LIFO)
INSA Centre Val de Loire & Université d'Orléans
GDR CNRS Sécurité Informatique – GT Protection de la Vie Privée

Séminaire LIMOS
25 Juin, 2020



Outline

Introduction et contexte

Avertissement

La volonté de développer de nouvelles approches pour lutter contre l'épidémie

Pourquoi confiner ?

Evaluation "PVP"

Utilité

Protocoles

A/G

DP3T

ROBERT

Différences

Déploiement de StopCovid

Attaques

Attaques génériques : Principe

Attaques génériques : Exemples

Attaques sur DP3T

Attaques sur StopCovid

Le modèle d'attaque : un enjeu de gouvernance

Differential privacy

Définition

Idée d'approche

Conclusion

Introduction et Contexte

Avertissement

Une tentative pour éclairer l'actualité par des considérations scientifiques

Nous sommes dans l'actualité brûlante

L'application *StopCovid* a été déployée le 2 juin en France, le gouvernement vient de faire un premier retour sur l'efficacité du dispositif

Des débats et des décisions dans d'autres pays européens

- ▶ Refus du déploiement en Belgique
- ▶ Hésitations quant au type d'app à déployer en Allemagne
- ▶ Développements de Novid19 en Autriche à base de Géoloc (Géorgie)
- ▶ App très intrusive déployée à Singapour [MoH20]
- ▶ Utilisation de bracelets électroniques de géolocalisation à Hong Kong [CNB])
- ▶ ...

Avertissement

Une tentative pour éclairer l'actualité par des considérations scientifiques

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")
- ▶ Les deux grandes familles de solutions concurrentes en cours de développement (DP3T [CT20] / Solution AppleGoogle [AG20] et ROBERT [IP20])
- ▶ Je ne présenterai pas la nouvelle solution en cours de développement par Inria (DESIRE [BBC⁺20]).

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) implémenté par une APP ?

Impact d'une APP 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).*

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, et qui va gérer D_1 (et peut être D_2 ?).

Important : D_2 est appliqué indépendamment de l'app à toute personne *diagnosed*

Contexte

Modélisation

Prédicats représentant des attributs des individus

- ▶ *contaminated* : la personne est malade et contagieuse.
- ▶ *diagnosed* : la personne a été testé positive par un test médical.
- ▶ *atRisk* : le processus de décision D_1 indique que la personne est à risque ($P(\textit{contaminated}|\textit{atRisk})$ est “grand”) et qu’il faut ensuite suivre un autre processus D_2 .

Utilisation subséquente du processus de décision D_1 / Objectifs de D_2

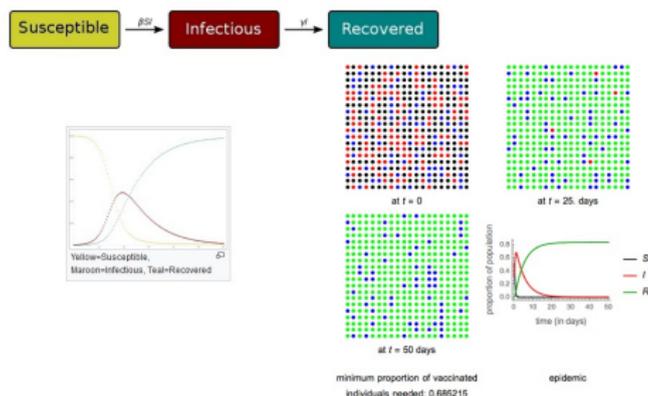
- ▶ Donner des droits aux individus *atRisk*, e.g. optimiser l’utilisation des tests en donnant priorité aux individus *atRisk*. optimise test usage by testing in priority *atRisk* individuals.
- ▶ Donner des droits aux individus $\neg\textit{atRisk}$, e.g. laisser les personnes $\neg\textit{atRisk}$ faire leurs courses, visiter des personnes âgées, etc.
- ▶ Retirer des droits aux individus *atRisk*, e.g. leur dire de rester à la maison
- ▶ ... un peu de tout ?

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 (ou notification d'exposition)

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 connaît 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 connaît 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'âge, le métier, les antécédents médicaux, etc.

Note : Importance de bien analyser D_2 afin de comprendre l'impact des attaques (e.g. création de faux positifs)

Contexte

Conception de D_1

Exemples pour D_1

- ▶ Singapour [MoH20] : contact “non protégé” de plus de 30 minutes avec une personne infectée à moins de 2m.
- ▶ France : contact de plus de 15 minutes avec une personne infectée à moins de 1m.

Contexte

Conception de D_1

Données nécessaires

Pour fonctionner, cet algorithme nécessite donc :

- ▶ De pouvoir mesurer une distance
- ▶ De pouvoir connaître l'état d'infection des voisins
- ▶ De pouvoir mesurer une durée d'exposition

Paramètres mesurés

- ▶ La position ou proximité : GPS, Bluetooth [GEG20] ou ultrasons
- ▶ La durée : horloge interne (synchronisée) mais problème pour relier les identifiants temporaires
- ▶ L'état des voisins

Contexte

Conception de D_1

Problème de confidentialité des données

C'est surtout l'état des voisins qui a été étudiée sous cet angle, mais aussi la difficulté de calculer l'exposition (centralisée vs décentralisée).

Divers algos ont été proposés pour sécuriser cet aspect (DP3T, ROBERT, ...).

Contexte

Conception de D_2

D_2

Je n'ai pas pour le moment pu obtenir de version pour d'un algorithme "automatique" de décision du comportement à adopter. 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.)

Simulation

L'imprécision de D_2 est également préjudiciable pour réaliser des simulations.

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

Supposition : On veut optimiser l'utilisation de tests

Les tests par jour

On fait actuellement environ 35K test par jour en France (début juin), on était à 30K précédemment (70K en Allemagne)

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 (“optimiser”) : 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 phases : 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 connaît 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 ?

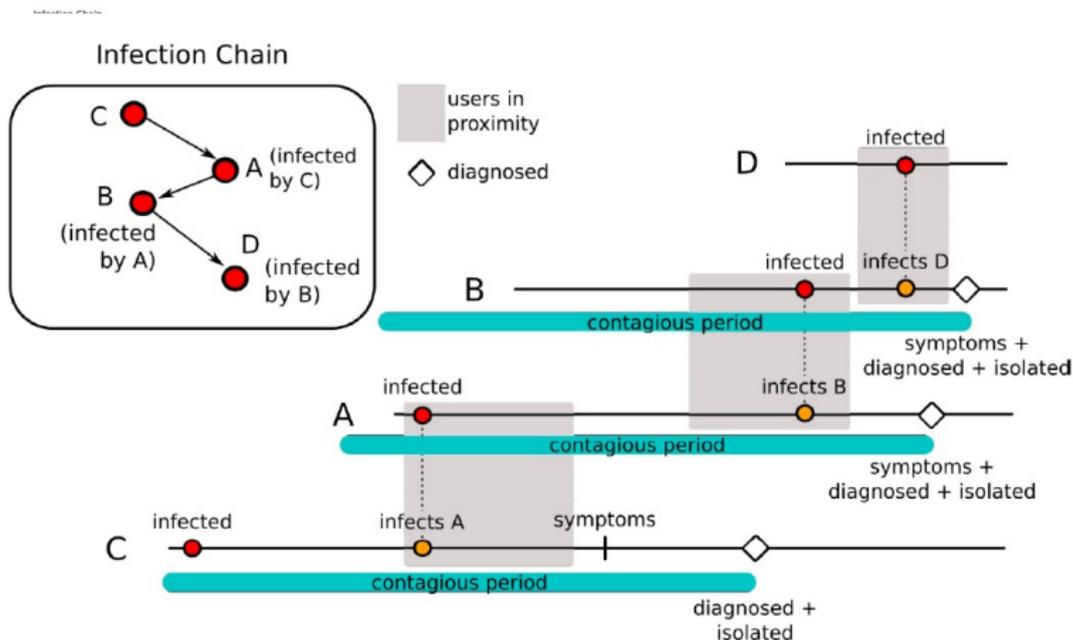


Figure 1: Example of the infection process without proximity tracing App.

Contexte

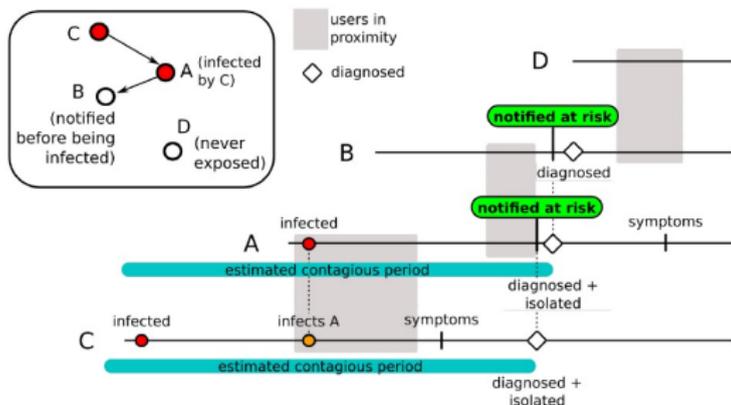


Figure 2: Example of the infection process with proximity tracing App that starts with person C being infected.

Figure 2: D'après [IP20]

Evaluation “PVP”

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'âge (moins de 44% des plus de 65 ans).

Evaluation "PVP" : une mise en balance utilité vs. risque

Comment quantifier D_2 ?

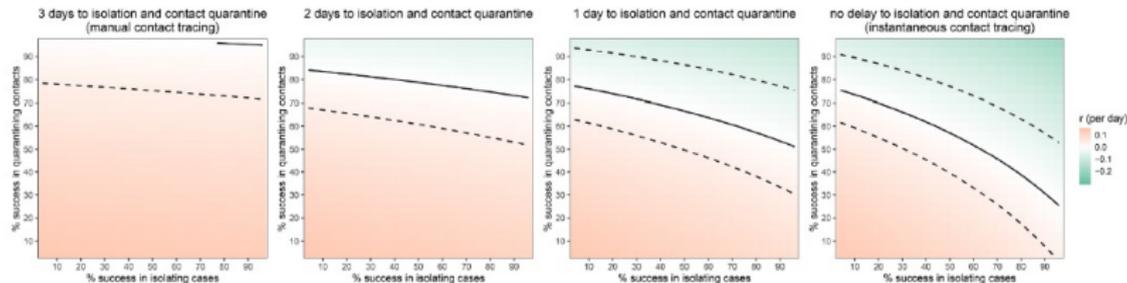


Fig. 3. Quantifying intervention success. Heat map plot showing the exponential growth rate of the epidemic r as a function of the success rate of instant isolation of symptomatic cases (x axis) and the success rate of instant contact tracing (y axis). Positive values of r (red) imply a growing epidemic; 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 3: D'après [FWK⁺20]

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

Comment quantifier D_2 ?

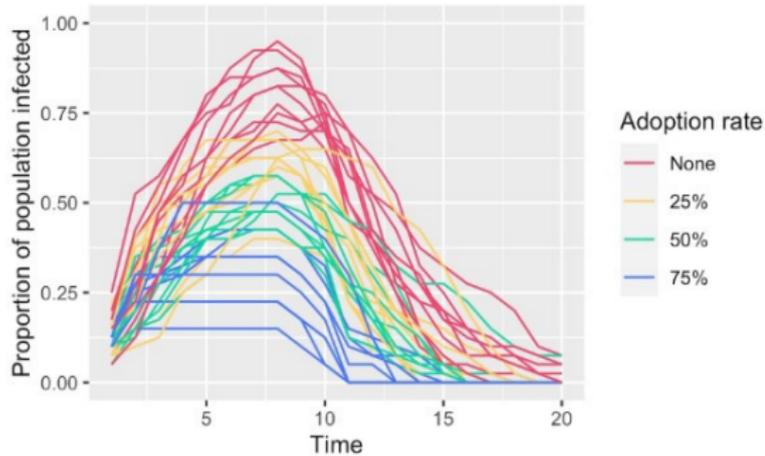


Figure 4: D’après [YLS20]

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 pose la question qu'elle soit obligatoire)
- ▶ Problème de catégories d'âge n'ayant pas de mobile (faux négatifs)
- ▶ Multiples soucis de mesures et calibration [ope] : Faux positifs, faux négatifs
- ▶ Balance utilité vs. sucollecte de données dans la remontée de contacts trop courts ou trop distants

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].

Protocoles

Protocoles

Approche AppleGoogle

What Apple and Google have proposed



Figure 5: D'après Apple/Google

Protocoles

Algorithme Decentralized Privacy Preserving Proximity Tracing (DP3T)

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) (une clé aléatoire par jour pour Apple/Google)
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 : $EphID_1 || \dots || EphID_n = PRG(PRF(SK_t, "public_string"))$
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 .

Protocoles

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 pour observer les dispositifs présents), croiser ces données avec d'autres (e.g. géoloc). 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.

Protocoles

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 envoyés 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~~) !/ Attention à l'implément ;))
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 *pendant une certaine durée (2j avant déclaration des symptômes ou 14j si pas de symptômes)*
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 (algorithme D_2).

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 **honnête-mais-curieux voire trusted**. Le modèle d'attaque de l'OS / constructeur est moins clair (covert ?).

DP3T/AG vs ROBERT

Similitudes et différences

Similarités

Broadcast de pseudonymes temporaires changeants, et récupération des pseudonymes observés, stockage de ces pseudonymes en local.

Différences : Lors d'un diagnostic médical

- ▶ DP3T publie vers un serveur centralisé une (ou plusieurs) clé permettant de reconstruire ses propres identifiants temporaires sur une durée de 14j. Ce serveur envoie ces clés à tous les autres utilisateurs, qui peuvent calculer localement D_1 .
- ▶ ROBERT publie vers un serveur centralisé la liste des identifiant temporaires avec qui on a été en contact. Ce serveur dispose de la capacité à déchiffrer qui est qui (table de correspondance ID/TID), et se charge de calculer D_1 puis d'avertir les utilisateurs identifiés.

Déploiement de StopCovid

L'App StopCovid en chiffres

Quelques éléments sur le déploiement de l'app au 23 juin 2020

- ▶ Déployée depuis le 2 juin 2020 sur l'infrastructure labellisée ANSSI "SecNum Cloud" OutScale (Dassault Systèmes)
- ▶ Environ 2.000.000 de téléchargements et d'activations pour 500.000 déinstallations
- ▶ 68 personnes ont déclaré leur test positif via QRCode
- ▶ 250 contacts remontés pour 14 *atRisk* activés.
- ▶ Coûts de développements gratuits, environ 100K par mois depuis juin 2020 (Dassault Systèmes, Lunabee Studio, puis à partir de septembre Cap Gemini), à comparer avec 20M€ au total en Allemagne et 1M par mois, et 4M£ au total au Royaume Uni.

Attaques

Les risques

Quantifier le risque de fuite de données

Qu'est ce qui peut fuiter ?

- ▶ Une donnée personnelle : le statut *diagnosed*
- ▶ Une donnée personnelle : le statut *atRisk*
- ▶ Des données personnelles : le cercle et l'horaire de rencontres
- ▶ Des données agrégées : des endroits "contaminants"
- ▶ D'autres données nécessaires pour faire le calcul de D_1 : age, localisation, ...

Est-ce que ça va fuiter ?

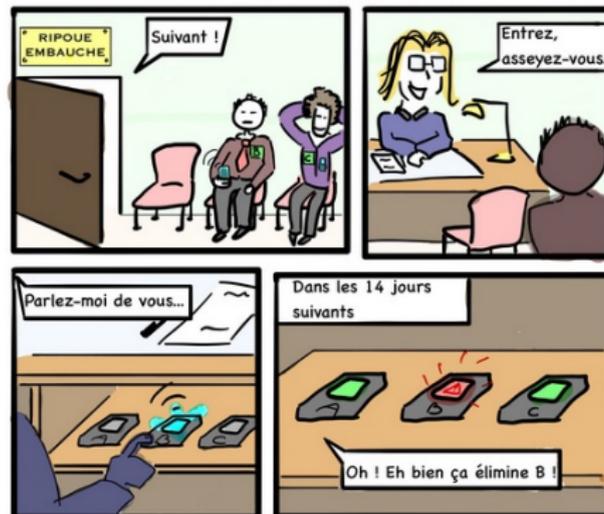
- ▶ Il faut monter une attaque (pas forcément simple selon le modèle d'attaque)
- ▶ Il faut faire croire au modèle d'attaque (on va en discuter par la suite)
- ▶ Certaines données non prévues fuient actuellement dans StopCovid, et les "patches" sont en cours (voir interventions de Sportisse dans la presse du 23/6 [OPC⁺20] sur la v1.1) – captcha google, pas de mixnets, et autres joyusetés.

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 6: D'après [BCC⁺20]

Attaques génériques sur *StopCovid*

Principe

Un certain nombre d'attaques génériques ont été proposées dans [BCC⁺20]. 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, paparazzi.

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).

Quelques attaques sur DP3T [Vau20]

Impersonnification du serveur central

Un attaquant envoie à un utilisateur honnête de l'app un *EphID* généré à partir d'une SK_x . L'attaquant intercepte ensuite la communication avec le serveur et l'individu et envoie SK_x à cet individu pour lui faire croire qu'il est contaminé.

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 dispose a priori d'un jour pour le faire).

Curiosité

En plaçant des antennes BT on peut récolter l'ensemble des identifiants d'une zone, et savoir s'ils sont contaminés. On peut corréler cette info avec des données de géoloc de l'antenne "indiscreète".

Attaques / Faiblesses de StopCovid

Colocalisation des individus infectés

Comme les mixnets ne sont pas utilisés (contrairement à ce qui est spécifié dans le protocole), il est possible pour le serveur de savoir toutes les personnes (sauf la personne *diagnosed*) qui étaient présentes au même endroit.

Collecte excessive de données

Les téléphones ne filtrent pas les contacts basés sur la distance et la durée.

Payload non chiffré

Le RSSI et la correction (dépendant du modèle du téléphone) sont envoyés en clairs.

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.

Réalisme du modèle d'attaque ?

Est-ce que le modèle d'attaque du serveur centralisé HbC est correct compte tenu du nombres d'attaques (internes et externe) qu'il risque de subir ?

DP3T/AG 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 connaît les ID et est capable de déidentifier un individu, en connaissant son $EBID_t$ et t . Dans DP3T le serveur n'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 connaît déjà tout un tas d'informations sur vous ? Dans la presse : Bras de fer actuel [O20] ...

La *Differential Privacy*, un modèle
intrinsèquement respectueux de la
vie privée ?

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 $\epsilon \in \mathbb{R}^{+*}$, $\delta \in \mathbb{R}^+$ et \mathcal{A} un algorithme aléatoire prenant en entrée un jeu de données D . On note $\text{im } \mathcal{A}$ l'image de \mathcal{A} . L'algorithme \mathcal{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 $S \in \text{im } \mathcal{A}$ on a :

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

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 brouter. 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.

Mise en place (work in progress)

- ▶ Générer des faux positifs et des faux négatifs dans le processus de décision D_1
- ▶ Vérifier (comparer) la qualité de la décision, en faisant des *simulations*

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.

Conclusion

Travaux en cours

Par l'équipe StopCovid

- ▶ L'utilisation d'IoT pour remplacer les smartphones (prévision : juillet 2020)
- ▶ Interopérabilité au niveau Européen
- ▶ Le développement d'un nouveau protocole (DESIRE [BBC⁺20])

Au LIFO

Plateforme de simulation épidémiologique intégrant comportements et applications de notification pour permettre l'évaluation d'algorithmes respectant la *differential privacy*.

Qu'avons nous appris ?

- ▶ Le problème du traçage de contacts respectueux de la vie privée s'est développé en quelques mois comme un sujet de recherches passionnant
- ▶ La durée du transfert technologique est impressionnante
- ▶ Les enjeux politiques peuvent guider la philosophie de conception d'algorithmes (voir conception éthique d'algorithmes [KR19])
- ▶ Dû à ces enjeux politiques, il est difficile de faire accepter les limites de certaines approches
- ▶ Rester vigilants sur le fait que l'application soit réellement non obligatoire, et son utilisation libre, consentie et éclairée.
- ▶ Que penser du taux d'adoption d'environ 2% à l'heure actuelle ? A comparer avec près de 10% en Allemagne ? Différence culturelle ?

Pour en savoir plus

Le lieu pour en débattre en France

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/>

Les divers GitHubs

▶ **DP3T :**

<https://github.com/DP-3T/documents/issues>

▶ **ROBERT :** <https://github.com/>

[ROBERT-proximity-tracing/documents/issues](https://github.com/ROBERT-proximity-tracing/documents/issues)

▶ **StopCovid :** <https://gitlab.inria.fr/groups/stopcovid19/-/issues>

<https://gdr-securite.irisa.fr/actualite/liste-de-diffusion-covid-19/>

References I

-  Apple and Google, *Apple google privacy-preserving contact tracing*, 2020, <https://www.apple.com/covid19/contacttracing>.
-  Nataliia Bielova, Antoine Boutet, Claude Castelluccia, Mathieu Cunche, Cédric Lauradoux, Daniel Le Métayer, and Vincent Roca, *Desire: A third way for a european exposure notification system : Leveraging the best of centralized and decentralized systems*, Tech. report, Inria, 2020.
-  Xavier Bonnetai, Anne Canteaut, Véronique Cortier, Pierrick Gaudry, Lucca Hirschi, Steve Kremer, Stéphanie Lacour, Matthieu Lequesne, Gaëtan Leurent, Léo Perrin, André Schrottenloher, Emmanuel Thomé, Serge Vaudenay, and Christophe Vuillot, *Le traçage anonyme, dangereux oxymore. analyse de risques à destination des non-spécialistes*, 2020, <https://risques-tracage.fr/docs/risques-tracage.pdf>.

References II



CNBC, *Hong kong is putting electronic wristbands on arriving passengers to enforce coronavirus quarantine*,

<https://www.cnbc.com/2020/03/18/hong-kong-uses-electronic-wristbands-to-enforce.html>.



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.

References III



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, <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).

References IV

-  Jean-Marie Gorce, Malcolm Egan, and Rémi Gribonval, *An efficient algorithm to estimate Covid-19 infectiousness risk from BLE-RSSI measurements*, Research Report RR-9345, Inria Grenoble Rhône-Alpes, May 2020.
-  Fraunhofer 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.
-  Michael Kearns and Aaron Roth, *The ethical algorithm: The science of socially aware algorithm design*, Oxford University Press, 2019.
-  Singapore Ministry of Health, *Tracetogether*, 2020,
<https://www.tracetogether.gov.sg/>.

References V

-  Cedric O, *Stopcovid ou encore ?*, 2020, <https://medium.com/@cedric.o/stopcovid-ou-encore-b5794d99bb12>.
-  Cédric O, Maurice-Michel Planel, Simon Cauchemez, Vittoria Colizza, Bruon Sportisse, and Guillaume Poupard, *Conférence de presse sur stopcovid*, 2020.
-  *Opentrace calibration*, <https://github.com/opentrace-community/opentrace-calibration/blob/master/Trial%20Methodologies.md>.
-  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.

References VI



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/>.