L'application "Stop-Covid"

théorie et pratique d'un dispositif de traçage numérique

Léo Perrin[1]

[1]Inria, France

leo.perrin@inria.fr

@lpp_crypto

5 Octobre 2020

“Refuser le traçage numérique c’est accepter plus de morts”

Cédric O (je paraphrase)

“Refuser le traçage numérique c’est accepter plus de morts”

Cédric O (je paraphrase)

... Mais alors pourquoi est-ce que les débats autour de cette application sont aussi violents ?

“Refuser le traçage numérique c’est accepter plus de morts”

Cédric O (je paraphrase)

... Mais alors pourquoi est-ce que les débats autour de cette application sont aussi violents ?

Comment est-ce qu’une appli de traçage se reposant sur le bluetooth est sensée marcher ?

Pourquoi est-ce aussi controversé ?

“Refuser le traçage numérique c’est accepter plus de morts”

Cédric O (je paraphrase)

... Mais alors pourquoi est-ce que les débats autour de cette application sont aussi violents ?

Comment est-ce qu’une appli de traçage se reposant sur le bluetooth est sensée marcher ? **Théorie**

Pourquoi est-ce aussi controversé ? **Pratique**

Commençons par le commencement

- Je travaille à l'Inria, qui s'est occupé du développement de `StopCovid`…
- … mais je ne suis pas impliqué dans le projet, donc je n'ai pas "d'informations privilégiées".

Commençons par le commencement

- Je travaille à l'Inria, qui s'est occupé du développement de `StopCovid`...
- ... mais je ne suis pas impliqué dans le projet, donc je n'ai pas "d'informations privilégiées".
- Le seul moyen d'étudier la sécurité d'un protocole/algorithme consiste à y chercher des failles/des moyens d'en détourner le fonctionnement.
  Le but n'est pas de nuire mais d'aider !
- Je suis l'un des co-auteurs de `https://risques-tracage.fr`

Table des matières

Plan de cette section

Plan de cette section

Qu'est-ce que le traçage de contact ?

Pour limiter la diffusion de la COVID, il faut isoler les malades et alerter les personnes qui ont été en contact avec.

Definition (Contact)

(ici) Une interaction qui aurait pu causer une contamination.

Cela peut être fait "à la main" (i.e. par des personnes physiques) ou bien par des outils numériques, en particulier des applications pour smartphone.

Application de Traçage de Numérique

L'étude d'Oxford (principe)

Une étude de l'université d'Oxford [1] est abondamment citée. Elle étudie l'impact sur la vitesse de propagation de 3 quantités.

Efficacité de l'isolement : ($\epsilon_I \in [0, 1]$) quantifie combien de personnes s'isolent et/ou si elles s'isolent bien lors de l'apparition de symptômes.

Efficacité du traçage de contact : ($\epsilon_T \in [0, 1]$) quantifie l'impact du traçage

Jours jusqu'à l'isolement et celui des contacts : (t) temps entre l'apparition des premiers symptômes et l'implémentation des mesures d'isolement.

1. *Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing*, Ferretti et al (2020). `https://doi.org/10.1101/2020.03.08.20032946`

L'étude d'Oxford (résultats 1/2)

Axe des x

Efficacité de l'isolement ϵ_I.

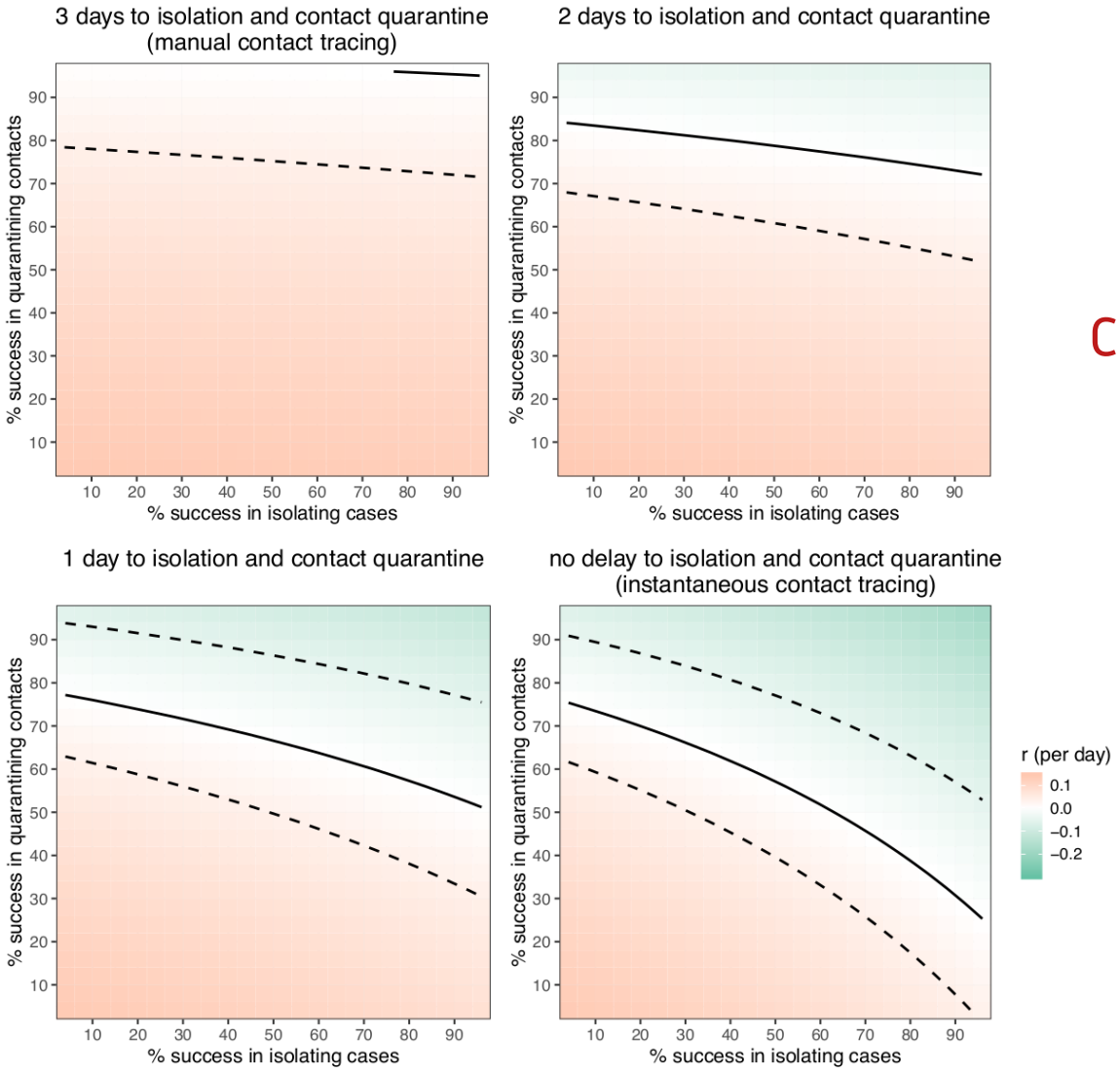
Axe des y

Efficacité du traçage de contact

$$\epsilon_T = U^2 \times D \times c$$

- U : proportion d'utilisateurs de l'ATN
- D : proportion des contacts détectés avec succès
- c : "réduction fractionelle de l'infectuosité résultant de la notification que l'on est cas contact"

L'étude d'Oxford (résultats 2/2)



Conclusions

- ϵ_T doit être très haut
- t doit être très bas
- le traçage "manuel" ne peut pas suivre...
- Il faut automatiser !

Cahier des charges d'une possible application

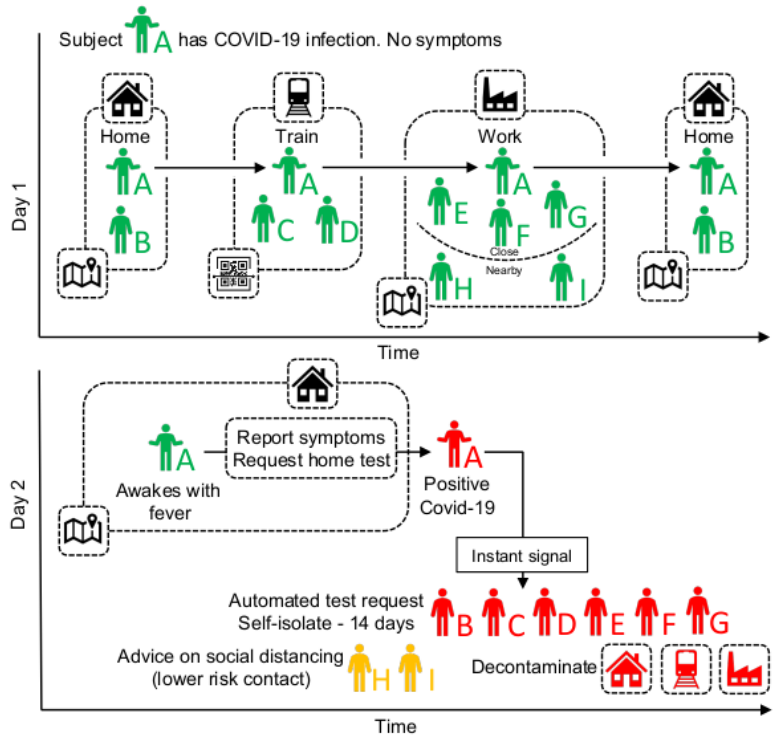


Fig. 4. A schematic of app-based COVID-19 contact tracing. Contacts of individual A (and all individuals using the app) are traced using GPS co-localisations with other App users, supplemented by scanning QR-codes displayed on high-traffic public amenities where GPS is too coarse. Individual A requests a SARS-COV-2 test (using the app) and their positive test result triggers an instant notification to individuals who have been in close contact. The App advises isolation for the case (individual A) and quarantine of their contacts.

1. Reposant sur le GPS
2. "Check-in" dans les "lieux publics avec beaucoup de trafic"
3. Le test est fait à la maison et est très rapide

Plan de cette section

On oublie le GPS

La conservation des plus élémentaires libertés individuelles impose des modifications à ce cahier des charges :

- il faut convaincre les utilisateurs d'utiliser l'ATN et non les obliger,
- le GPS [2] est mis de côté (peu approuvent l'idée d'être littéralement traqués par l'état),
- facilité d'utilisation $\Longrightarrow$ pas de QR codes dans les lieux fréquentés.

2. l'Icelande, une démocratie, a décidé de l'utiliser quand même.

Bluetooth ?

En pratique, les ATNs déployées en Europe cherchent seulement à tracer la grande proximité physique entre les personnes (les contacts par surface interposée ou à plus grande distance sont ignorés) :

$$\leq \text{1m pendant} \geq \text{15min}$$

Bluetooth ?

En pratique, les ATNs déployées en Europe cherchent seulement à tracer la grande proximité physique entre les personnes (les contacts par surface interposée ou à plus grande distance sont ignorés) :

$$\leq 1\text{m pendant} \geq 15\text{min}$$

Bluetooth

C'est une technologie d'échange d'information sans fil sur de "courtes" distances ($<$ 1 à 100m). Le standard décrivant le Bluetooth est une usine à gaz incroyablement complexe...

Bluetooth ?

En pratique, les ATNs déployées en Europe cherchent seulement à tracer la grande proximité physique entre les personnes (les contacts par surface interposée ou à plus grande distance sont ignorés) :

$$\leq 1\text{m pendant} \geq 15\text{min}$$

Bluetooth

C'est une technologie d'échange d'information sans fil sur de "courtes" distances ($<$ 1 à 100m). Le standard décrivant le Bluetooth est une usine à gaz incroyablement complexe...

Definition (BLE)

Le **Bluetooth Low Energy** est une variante du protocole Bluetooth visant une baisse de la consommation d'énergie. Sur les smartphones, il peut tourner à l'arrière plan même si le bluetooth est a priori désactivé.

Traçage de contact basé sur le Bluetooth

1. Chaque appareil a un “pseudonyme” à long terme, ce qui permet aux utilisateurs d’être pseudonymisés ($\neq$ anonymisés).

2. Chaque appareil a des “crypto-identifiants”, valides pendant une brève période ($\approx$ 15min), qui sont émis dans toutes les directions.

3. Les autres appareils dans les parages reçoivent ces crypto-identifiants.

Traçage de contact basé sur le Bluetooth

1. Chaque appareil a un “pseudonyme” à long terme, ce qui permet aux utilisateurs d’être pseudonymisés ($\neq$ anonymisés).
2. Chaque appareil a des “crypto-identifiants”, valides pendant une brève période ($\approx$ 15min), qui sont émis dans toutes les directions.
3. Les autres appareils dans les parages reçoivent ces crypto-identifiants.
4. Si un utilisateur s’avère plus tard avoir le COVID alors ceux qui ont reçu ses crypto-identifiants sont notifiés : ils sont des cas contact !

Faux Positifs

Le Bluetooth :

- passe à travers les murs et le plexiglas,
- ne sait pas si des masques sont portés et
- n'a pas été conçu pour mesurer les distances. [3]

3. En plus, il faut supposer que les modèles de propagation de la COVID en fonction de la distance sont exacts.

Faux Positifs

Le Bluetooth :

- passe à travers les murs et le plexiglas,
- ne sait pas si des masques sont portés et
- n'a pas été conçu pour mesurer les distances. [3]

Une ATN va forcément faire des faux positifs.

3. En plus, il faut supposer que les modèles de propagation de la COVID en fonction de la distance sont exacts.

Faux Positifs

Le Bluetooth :

- passe à travers les murs et le plexiglas,
- ne sait pas si des masques sont portés et
- n'a pas été conçu pour mesurer les distances. [3]

Une ATN va forcément faire des faux positifs.

Pas très grave en terme de limitation de la pandémie a priori... mais potentiellement très gênant pour tout le reste.
Ils ne sont pas pris en compte dans l'étude d'Oxford.

3. En plus, il faut supposer que les modèles de propagation de la COVID en fonction de la distance sont exacts.

Faux négatifs

Le Bluetooth :

- n'est pas fait pour mesurer les distances
- ne peut déterminer si une surface contaminées a été touchée
- ne connaît pas le niveau/la direction de l'aération du lieu.

Faux négatifs

Le Bluetooth :

- n'est pas fait pour mesurer les distances
- ne peut déterminer si une surface contaminées a été touchée
- ne connaît pas le niveau/la direction de l'aération du lieu.

Une ATN va forcément faire des faux négatifs.

Faux négatifs

Le Bluetooth :

- n'est pas fait pour mesurer les distances
- ne peut déterminer si une surface contaminées a été touchée
- ne connaît pas le niveau/la direction de l'aération du lieu.

Une ATN va forcément faire des faux négatifs.

Ils ont un impact sur la limitation de la pandémie : trop de faux négatifs et aucun malade n'est détecté. Ceci correspond au D du modèle d'Oxford

Plan de cette section

Pas de bracelet électronique

À ce stade, pas de bracelet électronique en France (il y en a à Singapour).

À la place, le traçage de contacts se repose sur un dispositif de traçage très courant : **les smartphones**.

Mesure de distance avec le Bluetooth

Plus on est loin, plus le signal est faible $\Longrightarrow$ on peut utiliser l'intensité du signal pour estimer la distance...

Mesure de distance avec le Bluetooth

Plus on est loin, plus le signal est faible $\Longrightarrow$ on peut utiliser l'intensité du signal pour estimer la distance...

... **en théorie**. En pratique, les puces/téléphones émettent/détectent les signaux avec des efficacités variables.

Apparement, ça marche à peu près.

Mesure de distance avec le Bluetooth

Plus on est loin, plus le signal est faible $\Longrightarrow$ on peut utiliser l'intensité du signal pour estimer la distance...

... **en théorie**. En pratique, les puces/téléphones émettent/détectent les signaux avec des efficacités variables.

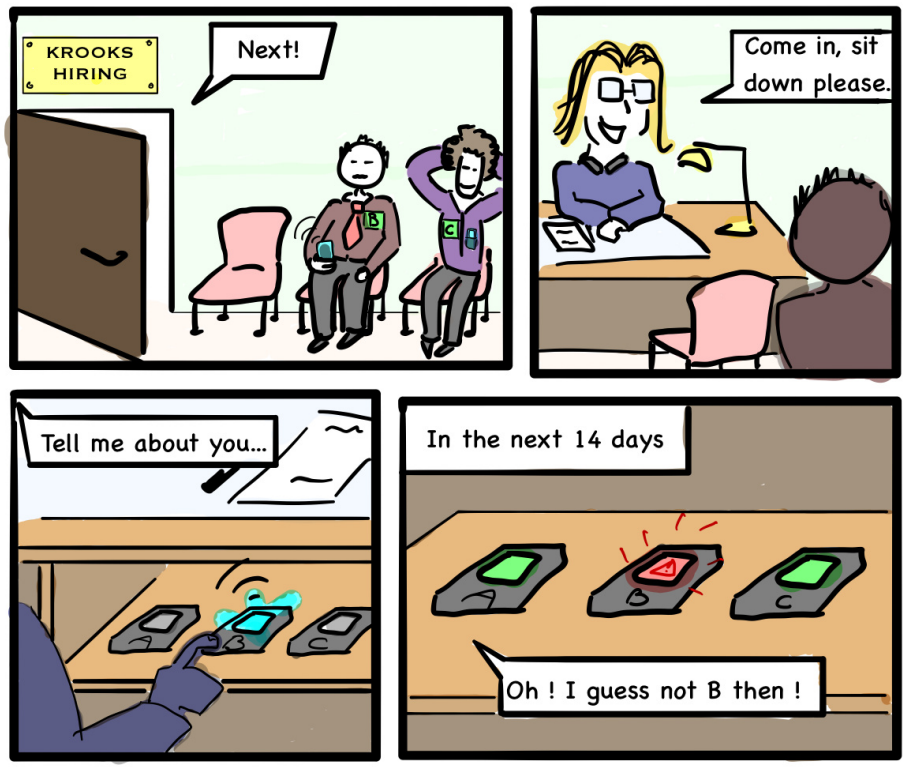
Apparement, ça marche à peu près.

N'oublions pas que ces distances sont des distances entre téléphones et non pas entre personnes !

Plan de cette section

Plan de cette section

Usage "Alternatifs" d'une ATN



https://www.risques-tracage.fr/

Traçage d'utilisateurs

Puisque les ATNs "crient" les identifiants, on peut facilement détecter leurs utilisateurs.

Un outil dédié existe pour `StopCovid` !

`https://github.com/rgrunbla/Stop_Covid_Detector_3000`

Instance jetable

1. Créer une nouvelle instance de l'ATN (i.e. en l'installant sur un téléphone dédié)
2. Attendre d'être à proximité seulement de la cible (e.g. en étant seul dans une pièce avec elle)
3. Une fois le contact enregistré par l'appli, l'éteindre et ne laisser personne d'autre entrer "en contact" avec.
4. Si ce téléphone reçoit une notification, vous savez que votre cible est malade.

Instance jetable

1. Créer une nouvelle instance de l'ATN (i.e. en l'installant sur un téléphone dédié)
2. Attendre d'être à proximité seulement de la cible (e.g. en étant seul dans une pièce avec elle)
3. Une fois le contact enregistré par l'appli, l'éteindre et ne laisser personne d'autre entrer "en contact" avec.
4. Si ce téléphone reçoit une notification, vous savez que votre cible est malade.

En pratique, pas besoin d'un smartphone "physique" par personne, on peut faire la même chose pour plusieurs cibles avec un seul téléphone.

Quarantaine forcée

1. Cacher le téléphone quelque part où il sera "en contact" avec les téléphones de vo(tre)s cible(s)
2. Obtenir un code correspondant à un diagnostic positif (corruption/extorsion/marché noir...) pour ce téléphone,
3. Voilà, toutes vos cibles sont en quarantaine !

On pourrait fermer une école (en cachant un téléphone dans la salle des profs), une usine (près de la machine à café/dans les vestiaires), pour se débarasser d'un concurrent...

Faux diagnostic

Dans l'étude d'Ofxford, il était envisagé qu'un premier diagnostic soit fait directement dans l'appli—et que son résultat soit envoyé à tous les contacts si besoin. L'alerte serait levée en cas de (vrai) test négatif.

Question pour l'audience

Comment s'amuser avec un tel système ?

Faux diagnostic

Dans l'étude d'Ofxford, il était envisagé qu'un premier diagnostic soit fait directement dans l'appli—et que son résultat soit envoyé à tous les contacts si besoin. L'alerte serait levée en cas de (vrai) test négatif.

Question pour l'audience

Comment s'amuser avec un tel système ?

Question Cruciale

D'une manière générale, quelle est le niveau de sécurité de l'infrastructure gérant les diagnostics/les codes ?

Applications Tierces

Les ATNs à base de BT n'utilisent pas de GPS. Certes.

Qu'est-ce qui empêche un programmeur malveillant de créer une autre applis qui

1. reçoit les crypto-identifiants,
2. les associe aux données GPS/au flux vidéo de la caméra/demande à l'utilisateur d'identifier la personne,
3. stocke et/ou utilise le résultat d'une quelconque façon

sans que personne ne s'en aperçoive ?

Applications Tierces

Les ATNs à base de BT n'utilisent pas de GPS. Certes.

Qu'est-ce qui empêche un programmeur malveillant de créer une autre applis qui

1. reçoit les crypto-identifiants,
2. les associe aux données GPS/au flux vidéo de la caméra/demande à l'utilisateur d'identifier la personne,
3. stocke et/ou utilise le résultat d'une quelconque façon

sans que personne ne s'en aperçoive ?

Réponse :

Applications Tierces

Les ATNs à base de BT n'utilisent pas de GPS. Certes.

Qu'est-ce qui empêche un programmeur malveillant de créer une autre applis qui

1. reçoit les crypto-identifiants,
2. les associe aux données GPS/au flux vidéo de la caméra/demande à l'utilisateur d'identifier la personne,
3. stocke et/ou utilise le résultat d'une quelconque façon

sans que personne ne s'en aperçoive ?

Réponse : rien du tout.

De fait, Apple (!) l'a fait en Suisse...

Plan de cette section

Projets concurrents

DP3T Projet basé sur une application "décentralisée", porté par de nombreux académiques, puis soutenu par Google et Apple.

Projets concurrents

DP3T Projet basé sur une application "décentralisée", porté par de nombreux académiques, puis soutenu par Google et Apple.

PEPPPT Projet se voulant pan-européen basé sur une application "centralisée".

Projets concurrents

DP3T Projet basé sur une application "décentralisée", porté par de nombreux académiques, puis soutenu par Google et Apple.

PEPPPT Projet se voulant pan-européen basé sur une application "centralisée".
A $\approx$ explosé en vol, tous les pays concernés l'ont quitté (Allemagne, RU), sauf la France.

A donné le protocole **ROBERT**, utilisé par `StopCovid`.

Projets concurrents

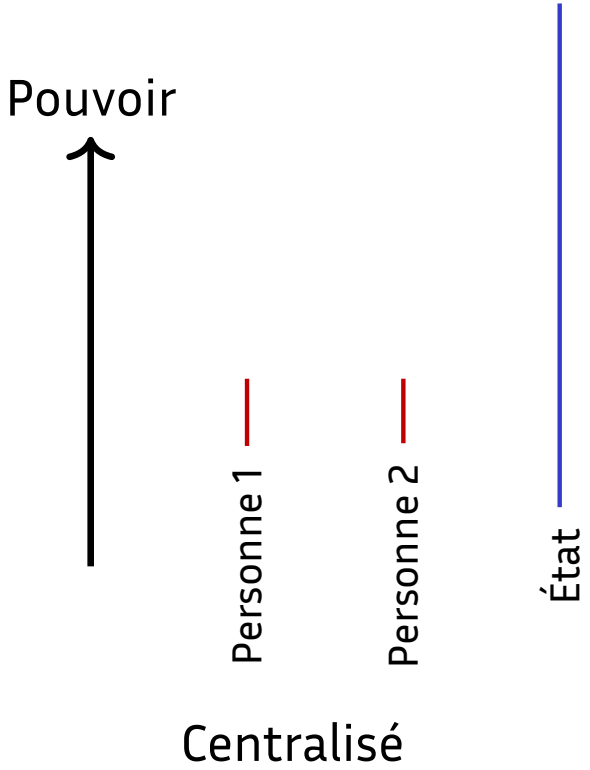
DP3T Projet basé sur une application "décentralisée", porté par de nombreux académiques, puis soutenu par Google et Apple.

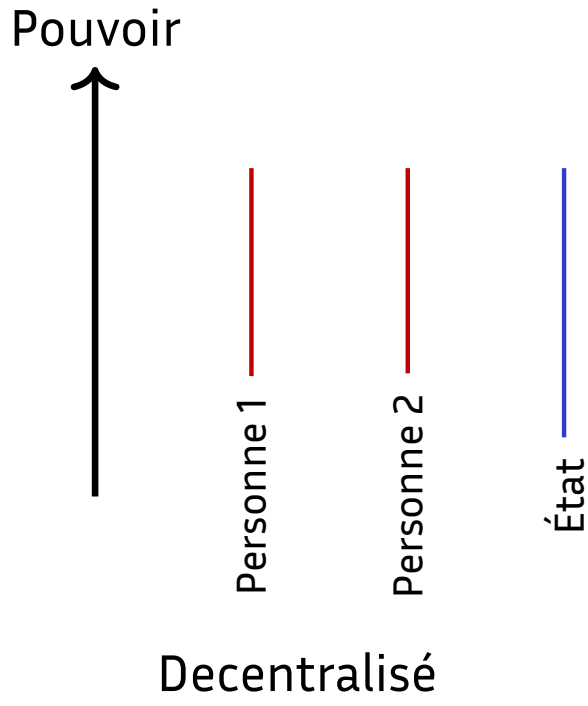
PEPPPT Projet se voulant pan-européen basé sur une application "centralisée".
A $\approx$ explosé en vol, tous les pays concernés l'ont quitté (Allemagne, RU), sauf la France.

A donné le protocole **ROBERT**, utilisé par `StopCovid`.

DESIRE Nouveau projet porté par Inria se voulant une "3ème voie".
Non déployé.

Centralisé vs. decentralisé





La préférence entre "centralisé" et "décentralisé" correspond aux axiomes sur lesquels chacun construit sa pensée politique.

Concrètement : l'autre camp = **nazis !!1 !**

Délais très courts

Les ATNs ont du être développées très rapidement, principalement pendant le confinement, alors qu'une bonne partie de la communauté INFO-SEC s'écharpe sur "centralisé vs. décentralisé".

Délais très courts

Les ATNs ont du être développées très rapidement, principalement pendant le confinement, alors qu'une bonne partie de la communauté INFO-SEC s'écharpe sur "centralisé vs. décentralisé".

Le code produit ne peut pas être top (pas parce que les développeurs sont mauvais, parce que c'est impossible de faire bien dans des circonstances pareilles).

Délais très courts

Les ATNs ont du être développées très rapidement, principalement pendant le confinement, alors qu'une bonne partie de la communauté INFO-SEC s'écharpe sur "centralisé vs. décentralisé".

Le code produit ne peut pas être top (pas parce que les développeurs sont mauvais, parce que c'est impossible de faire bien dans des circonstances pareilles).

De fait, il y a eu des problèmes avec `StopCovid` et les applications reposant sur le DP3T.

Politique (Pression)

Si on n'avait pas fait StopCovid, on nous aurait reproché de ne pas avoir considérer d'ATN.

(Cédric O, je paraphrase)

Politique (Souveraineté)

Apple et Google proposent des outils permettant d'utiliser facilement une approche "decentralisée".

Ont-ils le droit de prendre cette décision ?

Politique (Souveraineté)

Apple et Google proposent des outils permettant d'utiliser facilement une approche "decentralisée".

Ont-ils le droit de prendre cette décision ?

Philosophiquement, on peut en débattre.

En pratique, oui : les applis (comme `StopCovid`) qui n'utilisent pas leurs outils sont moins efficaces.

Plan de cette section

Revenons sur l'efficacité

$$\epsilon_T = U^2 \times D \times c$$

En France, on a :

- $U \leq 0.75$ (très optimiste !)
- $D \leq 0.80$ (d'après Cédric O [4])

4. https://www.francetvinfo.fr/sante/maladie/coronavirus/testee-grandeur-nature-par-une-soixantaine-de-militaires-l-application-stopcovid-est-prete-et-jugee-suf 3981357.html

Revenons sur l'efficacité

$$\epsilon_T = U^2 \times D \times c$$

En France, on a :

- $U \leq 0.75$ (très optimiste !)
- $D \leq 0.80$ (d'après Cédric O [4])

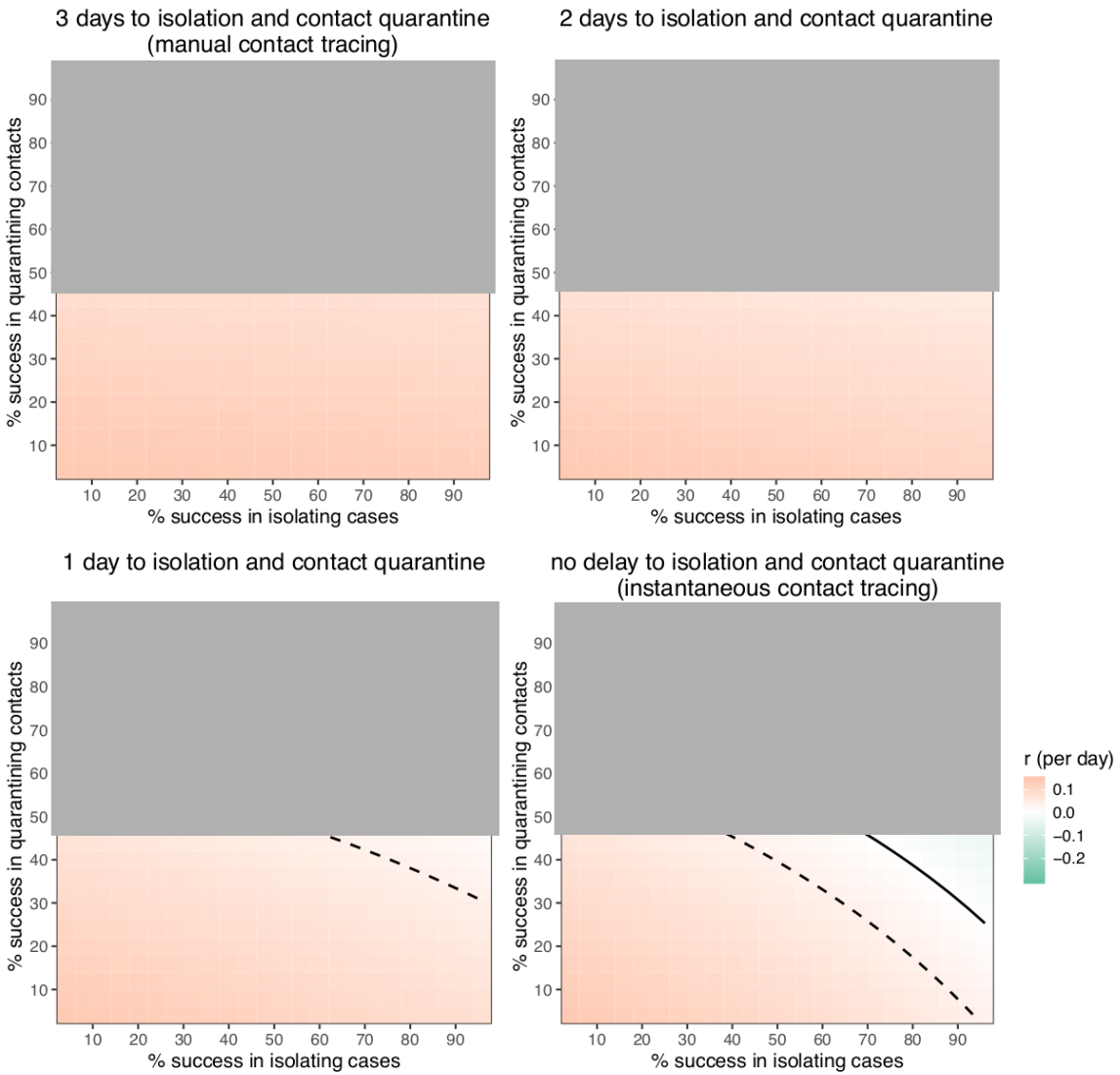
Quand bien même une ATN détecterait **tout ce qu'il lui est possible de détecter** (que ce soit StopCovid un truc basé sur le DP3T), on aurait au mieux $\epsilon_T \leq 0.56$

Dans le cas de StopCovid, $D = 0.80$:

$$\epsilon_T \leq 0.45$$

4. https://www.francetvinfo.fr/sante/maladie/coronavirus/testee-grandeur-nature-par-une-soixantaine-de-militaires-l-application-stopcovid-est-prete-et-jugee-suf 3981357.html

Efficacité maximale **possible** (France)

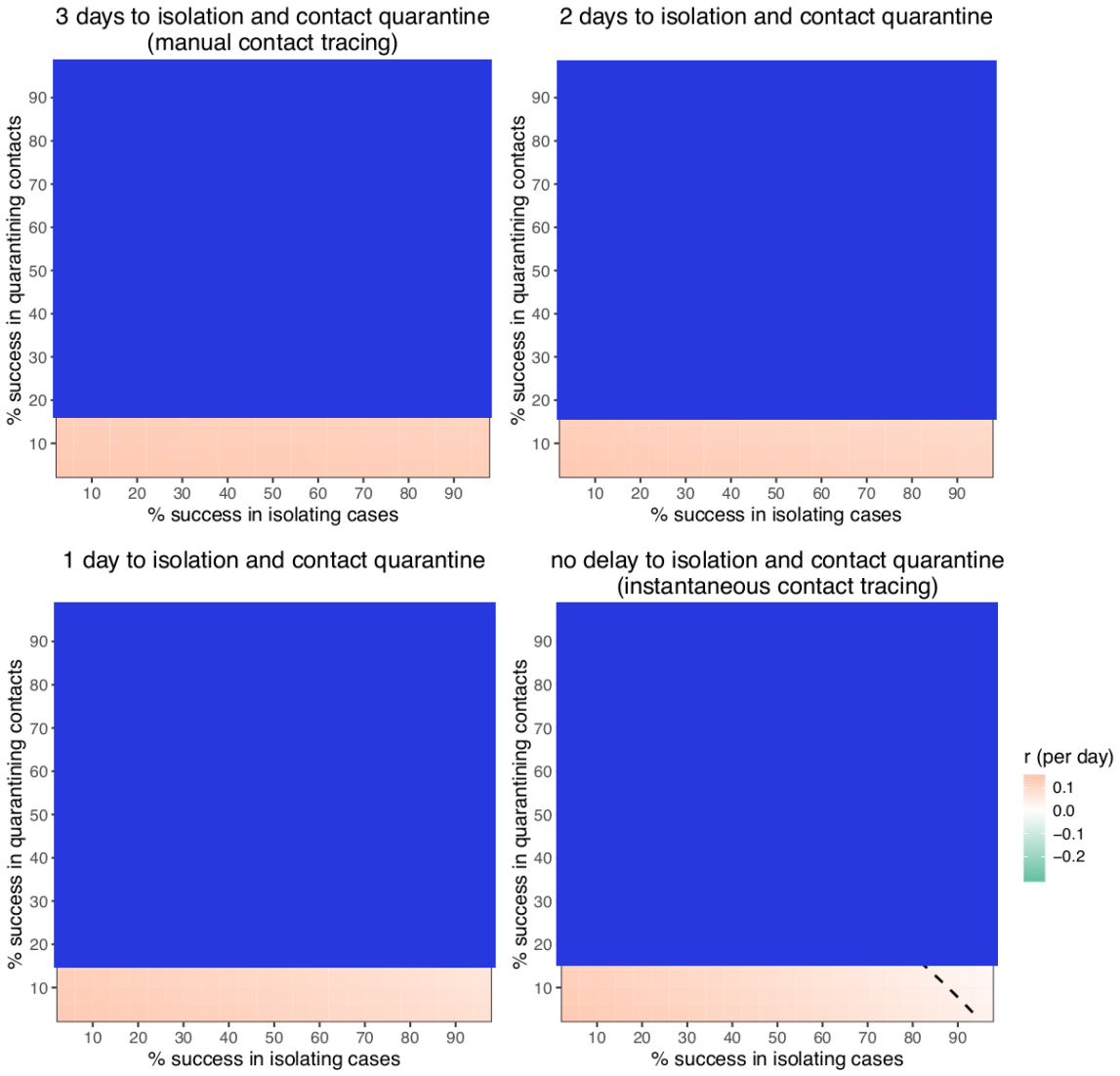


France

$U \leq 0.75$ $D \approx 0.8$

$\epsilon_T \leq 0.45$

Efficacité maximale **possible** (Islande)



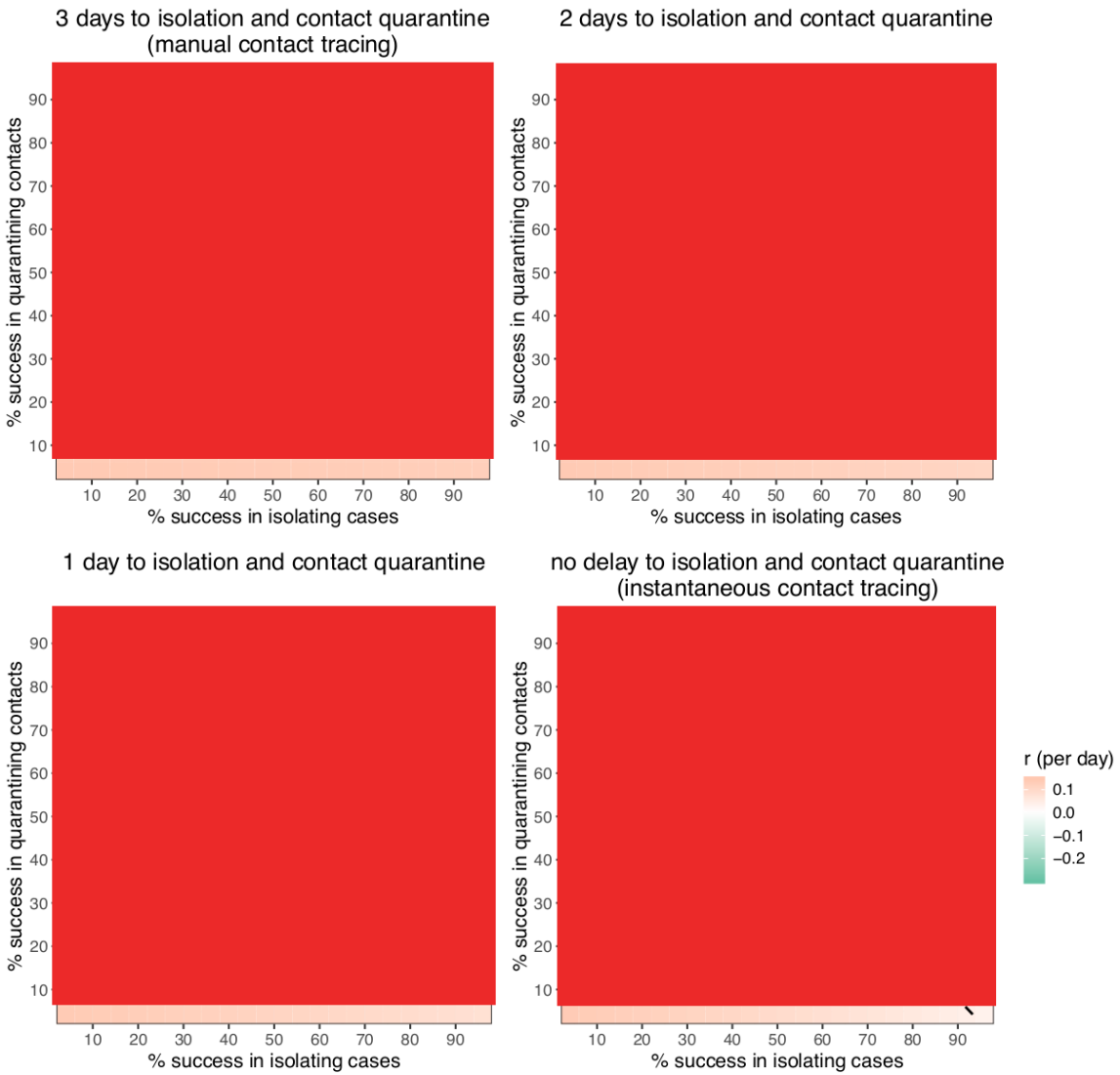
Iceland

$U \approx 0.40$

D : aucune idée, disons ≈ 1

$\epsilon_T \leq 0.16$

Efficacité maximale **possible** (Singapour)



Singapour

$U \approx 0.20$

D : aucune idée, disons ≈ 1

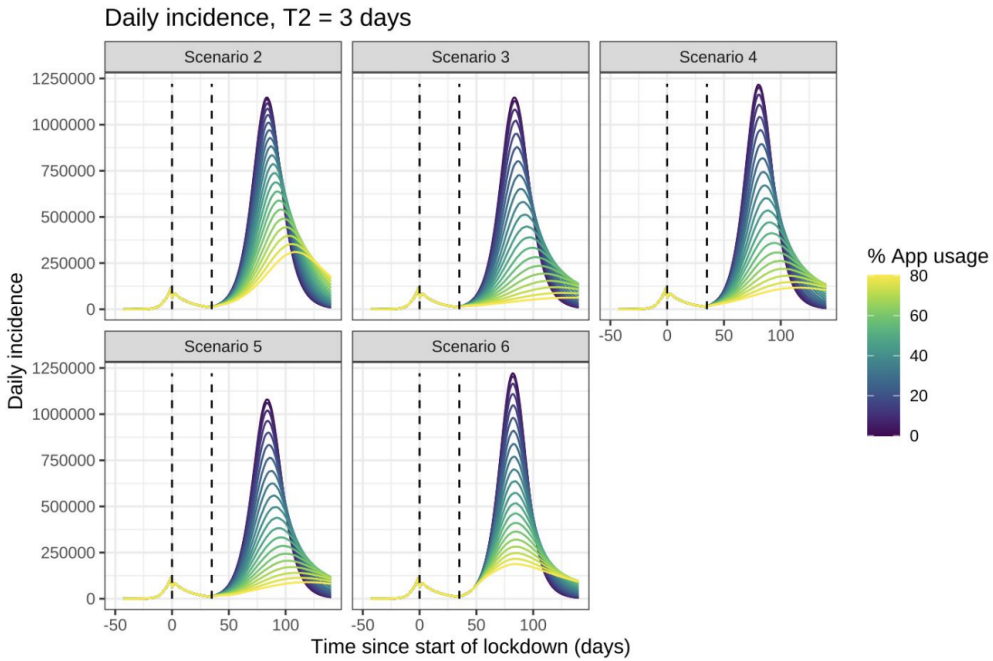
$\epsilon_T \leq 0.04$

Modèle vs. Realité

Même quelques pourcents d'utilisateurs feront une différence
(Cédric O, je paraphrase)

Dans, *Effective Configurations of a Digital Contact Tracing App : A report to NHSX*, Hinch et al.[5], on voit

Figure 5 - daily and cumulative incidence depending on varying use of the app
Doubling time 3 days:



5. https://045.medsci.ox.ac.uk/files/files/report-effective-app-configurations.pdf

Premiers retours

Les ATns ont été considérées $\approx$ inutiles en Islande ($U = 40\%$) et à Singapour ($U = 20\%$), quand bien même elles complétaient un traçage manuel...

6. https://www.medrxiv.org/content/10.1101/2020.09.07.20189274v1.full.pdf

Premiers retours

Les ATns ont été considérées $\approx$ inutiles en Islande ($U = 40\%$) et à Singapour ($U = 20\%$), quand bien même elles complétaient un traçage manuel...

La Suisse se félicite [6] d'avoir la preuve irréfutable de l'efficacité de Swisscovid.

6. https://www.medrxiv.org/content/10.1101/2020.09.07.20189274v1.full.pdf

Premiers retours

Les ATns ont été considérées $\approx$ inutiles en Islande ($U = 40\%$) et à Singapour ($U = 20\%$), quand bien même elles complétaient un traçage manuel...

Les développeurs de l'application Suisse se félicitent [6] d'avoir la preuve irréfutable d'avoir trouver $\approx$ 30 cas contacts grâce à leur ATN.

6. https://www.medrxiv.org/content/10.1101/2020.09.07.20189274v1.full.pdf

Premiers retours

Les ATns ont été considérées $\approx$ inutiles en Islande ($U = 40\%$) et à Singapour ($U = 20\%$), quand bien même elles complétaient un traçage manuel...

Les développeurs de l'application Suisse se félicitent [6] d'avoir la preuve irréfutable d'avoir trouver ≈ 30 cas contacts grâce à leur ATN.
Sur un total de plus de 8000 cas, avec $U \approx 20\%$...

6. https://www.medrxiv.org/content/10.1101/2020.09.07.20189274v1.full.pdf

Plan de cette section

Plan de cette section

Remplacer toutes les mesures, tests inclus

Claim

Avec un taux d'adoption suffisamment haut, une ATN peut remplacer toutes les autres mesures (masques, distanciation), y compris les tests !

(Cédric O lors de son audition à l'assemblée, je paraphrase)

7. *Effective Configurations of a Digital Contact Tracing App : A report to NHSX*, Hinch et al.

https://045.medsci.ox.ac.uk/files/files/report-effective-app-configurations.pdf

Remplacer toutes les mesures, tests inclus

Claim

Avec un taux d'adoption suffisamment haut, une ATN peut remplacer toutes les autres mesures (masques, distanciation), y compris les tests !

(Cédric O lors de son audition à l'assemblée, je paraphrase)

Le but d'une ATN est de propager l'information provenant d'un test.

7. *Effective Configurations of a Digital Contact Tracing App : A report to NHSX*, Hinch et al.

`https://045.medsci.ox.ac.uk/files/files/report-effective-app-configurations.pdf`

Remplacer toutes les mesures, tests inclus

Claim

Avec un taux d'adoption suffisamment haut, une ATN peut remplacer toutes les autres mesures (masques, distanciation), y compris les tests !

(Cédric O lors de son audition à l'assemblée, je paraphrase)

Le but d'une ATN est de propager l'information provenant d'un test. Du coup, **non**.

Dans un "papier scientifique" [7] il est dit que les tests pourraient être faits dans l'appli. Donc il y en a toujours

7. *Effective Configurations of a Digital Contact Tracing App : A report to NHSX*, Hinch et al. https://045.medsci.ox.ac.uk/files/files/report-effective-app-configurations.pdf

Remplacer toutes les mesures, tests inclus

Claim

Avec un taux d'adoption suffisamment haut, une ATN peut remplacer toutes les autres mesures (masques, distanciation), y compris les tests !

(Cédric O lors de son audition à l'assemblée, je paraphrase)

Le but d'une ATN est de propager l'information provenant d'un test. Du coup, **non**.

Dans un "papier scientifique" [7] il est dit que les tests pourraient être faits dans l'appli. Donc il y en a toujours

Extrêmement trompeur.

7. *Effective Configurations of a Digital Contact Tracing App : A report to NHSX*, Hinch et al.
https://045.medsci.ox.ac.uk/files/files/report-effective-app-configurations.pdf

Une décision à Zurich

Dans certains bars à Zurich, on a pu enlever son masque a condition d'avoir installé SwissCovid.

Une décision à Zurich

Dans certains bars à Zurich, on a pu enlever son masque a condition d'avoir installé SwissCovid.

Une ATN n'est **pas un talisman magique** !

Une décision à Zurich

Dans certains bars à Zurich, on a pu enlever son masque a condition d'avoir installé SwissCovid.

Une ATN n'est **pas un talisman magique** !

C'est à cause de décisions comme celle-ci qu'une ATN pourrait avoir un impact négatif sur la maîtrise de l'épidémie.

Affirmation

Je n'utilise pas StopCovid parce que malheureusement je ne prends pas le métro.

(M. le 1er ministre)

Explications plus probables :

- désactivation du bluetooth
- diminution de la surface d'attaque
- absence de croyance ?

Plan de cette section

Contacts dans le téléphone $\neq$ cas contact

Claim

StopCovid connaîtra et interagira avec les contacts stockés sur votre téléphone.

(Jean-Luc Mélenchon (entre autre), je paraphrase)

Contacts dans le téléphone $\neq$ cas contact

Claim

StopCovid connaîtra et interagira avec les contacts stockés sur votre téléphone.

(Jean-Luc Mélenchon (entre autre), je paraphrase)

- Les ATNs utilise le Bluetooth pour identifier la proximité physique (du mieux qu'elles peuvent...), rien de plus
- Accéder aux contacts stockés demande une autorisation explicite.

Contacts dans le téléphone $\neq$ cas contact

Claim

StopCovid connaîtra et interagira avec les contacts stockés sur votre téléphone.

(Jean-Luc Mélenchon (entre autre), je paraphrase)

- Les ATNs utilise le Bluetooth pour identifier la proximité physique (du mieux qu'elles peuvent...), rien de plus
- Accéder aux contacts stockés demande une autorisation explicite.

Non. (on s'en rendrait compte)

Les GAFAMs et StopCovid (1/2)

Affirmation

Les GAFAMs ne sont pas absents de StopCovid.

Les GAFAMs et StopCovid (1/2)

Affirmation

Les GAFAMs ne sont pas absents de StopCovid.

L'application tourne sur les smartphones de Apple et Google mais ça ne veut pas dire grand chose.
(sauf si ils décident d'enlever StopCovid de leurs appstores)

Les GAFAMs et StopCovid (1/2)

Affirmation

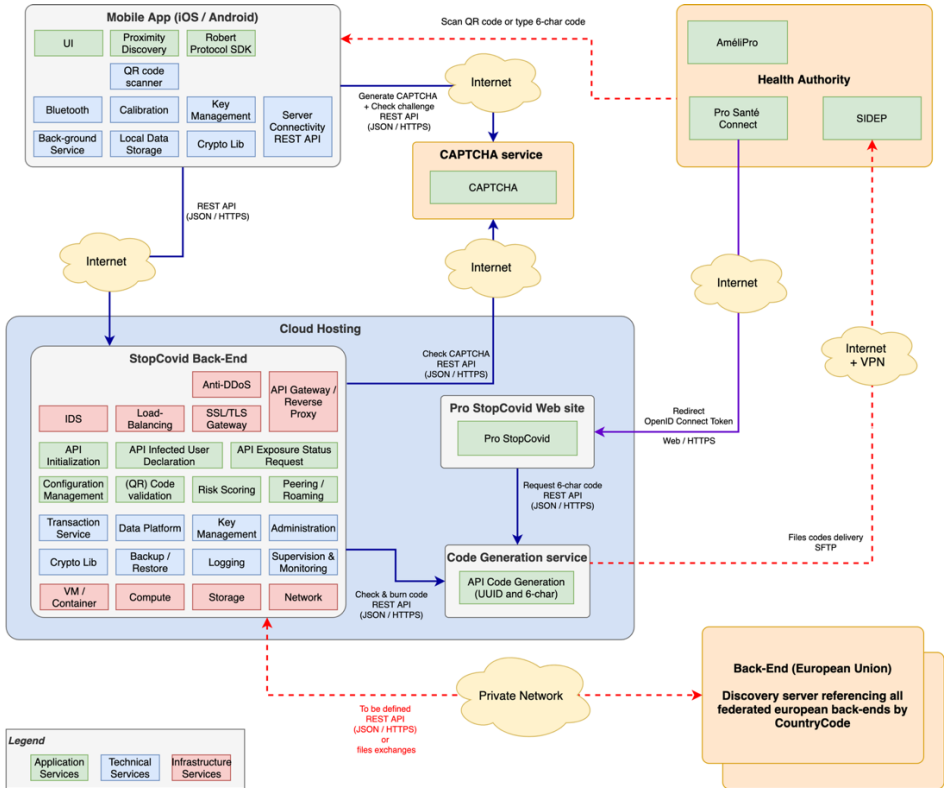
Les GAFAMs ne sont pas absents de StopCovid.

L'application tourne sur les smartphones de Apple et Google mais ça ne veut pas dire grand chose.
(sauf si ils décident d'enlever StopCovid de leurs appstores)

StopCovid utilisait une CAPTCHA Google, ce qui leur envoyait des informations. Normalement ce n'est plus le cas.

En ce qui concerne Microsoft c'est plus compliqué

The GAFAMs and StopCovid (2/2)



source : documentation de StopCovid sur gitlab

StopCovid semble être interfacé avec la base de données SIDEP, qui est sur le **Health DataHub**, lui même hebergé chez Microsoft.

Affirmation

Les opposants à StopCovid doivent se décider, soit l'application est inefficace, soit elle est dangereuse ; ça ne peut pas être les deux.

(Philippe Latombe, among others)

On pourrait avoir tous les effets suivants simultanément :

- le déploiement de l'application s'avère favoriser l'épidémie, [8]
- des utilisateurs malveillants la détournent pour envoyer de fausses notifications,
- le logicial développé pour StopCovid (ou pour le DP3T) qui estime la distance entre téléphone avec le BLE est utilisée par une dictature pour encore mieux traquer ses citoyens.

8. Pas le cas en France à *l'heure actuelle*.

Affirmation

Les opposants à StopCovid doivent se décider, soit l'application est inefficace, soit elle est dangereuse ; ça ne peut pas être les deux.

(Philippe Latombe, among others)

On pourrait avoir tous les effets suivants simultanément :

- le déploiement de l'application s'avère favoriser l'épidémie, [8]
- des utilisateurs malveillants la détournent pour envoyer de fausses notifications,
- le logicial développé pour StopCovid (ou pour le DP3T) qui estime la distance entre téléphone avec le BLE est utilisée par une dictature pour encore mieux traquer ses citoyens.

Fausse dichotomie.

8. Pas le cas en France à *l'heure actuelle*.

Plan de cette section

Conclusion (1/2)

Principe général

“C’est simple, si vous êtes contre c’est que vous êtes un meurtrier”, c’est courant quand il s’agit de technologie et c’est rarement pertinent.

Conclusion (1/2)

Principe général

"C'est simple, si vous êtes contre c'est que vous êtes un meurtrier", c'est courant quand il s'agit de technologie et c'est rarement pertinent.

- Refus d'installer `StopCovid`
- Scepticisme vis-à-vis du Health Data Hub
- "Vous êtes cryptographe ? Donc vous êtes un terroriste !"

Conclusion (2/2)

Pour `StopCovid`, le débat c'est cristallisé sur :

- "centralisé" vs. "décentralisé",

Conclusion (2/2)

Pour `StopCovid`, le débat c'est cristallisé sur :

- "centralisé" vs. "décentralisé",
- GAFAM ou pas,

Conclusion (2/2)

Pour `StopCovid`, le débat c'est cristallisé sur :

- "centralisé" vs. "décentralisé",
- GAFAM ou pas,
- les mérites des ATNs les unes par rapport aux autres, en particulier...

Conclusion (2/2)

Pour `StopCovid`, le débat c'est cristallisé sur :

- "centralisé" vs. "décentralisé",
- GAFAM ou pas,
- les mérites des ATNs les unes par rapport aux autres, en particulier...
- "qui a le plus gros taux de téléchargement ?"

Conclusion (2/2)

Pour `StopCovid`, le débat c'est cristallisé sur :

- "centralisé" vs. "décentralisé",
- GAFAM ou pas,
- les mérites des ATNs les unes par rapport aux autres, en particulier...
- "qui a le plus gros taux de téléchargement ?"

Conclusion (2/2)

Pour `StopCovid`, le débat c'est cristallisé sur :

- "centralisé" vs. "décentralisé",
- GAFAM ou pas,
- les mérites des ATNs les unes par rapport aux autres, en particulier...
- "qui a le plus gros taux de téléchargement ?"

Qu'en est-il du mérite absolu des ATNs ?

Conclusion (2/2)

Pour `StopCovid`, le débat c'est cristallisé sur :

- "centralisé" vs. "décentralisé",
- GAFAM ou pas,
- les mérites des ATNs les unes par rapport aux autres, en particulier...
- "qui a le plus gros taux de téléchargement ?"

Qu'en est-il du mérite absolu des ATNs ?

Mes conseils :

- Demandez une estimation claire des bénéfices attendus d'une technologie,

Conclusion (2/2)

Pour `StopCovid`, le débat c'est cristallisé sur :

- "centralisé" vs. "décentralisé",
- GAFAM ou pas,
- les mérites des ATNs les unes par rapport aux autres, en particulier...
- "qui a le plus gros taux de téléchargement ?"

Qu'en est-il du mérite absolu des ATNs ?

Mes conseils :

- Demandez une estimation claire des bénéfices attendus d'une technologie,
- Ne laissez pas de côté l'étude de ses effets négatifs !

Merci !

Plan de cette section

How to Track a Specific Device

CTAs **can** be used to physically track someone. The Bluetooth chipset has a MAC address which changes over time. If the change of MAC is not perfectly synchronized with the change of crypto-identifier, then we can figure out that a sequence of crypto-identifiers corresponds to a unique person.

Replay Attacks

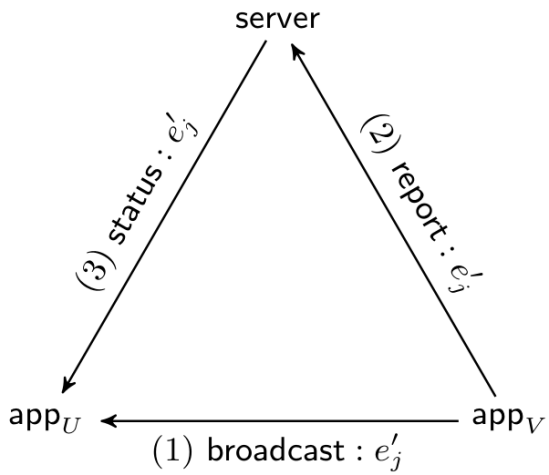
How to sell positive diagnoses on the black market?

1. have the buyer send you their upcoming identifiers,
2. set up a long distance antenna with falsified distance information next to a testing center. Simulate contacts between everyone going there and your buyer’s identifiers.
3. next time the buyer’s app checks if he is at risk, he will be if anyone in the testing center was positive.

The specifics of the attack depend on the protocol used but the principle is the same.

Plan de cette section

"Decentralized"?



source : "Centralized or Decentralized ? The Contact Tracing Dilemma", Vaudenay (2020).

`https://eprint.iacr.org/2020/531`

1. Each user generates crypto-identifiers e'_i that they broadcast.
2. If a user becomes sick, they send all the crypto-identifiers they generated to a central server which adds them to their list of "sick identifiers".
3. Those who received "sick" identifiers now know they are "at risk".

Motivation

The central server knows very little.

Even if the actor running the central server is ill-intentioned, there is not much that they can do to harm/de-anonymise the users.

Topic of an international petition : “Joint Statement on Contact Tracing : Date 19th April 2020” [9]

9. https://www.esat.kuleuven.be/cosic/sites/contact-tracing-joint-statement/

A Specific Attack (1/2)

The temporary crypto-identifiers of all infected people are public.

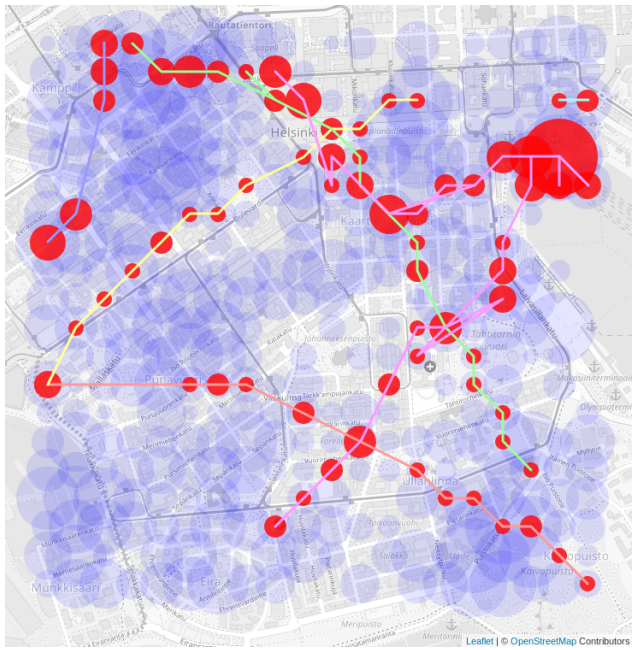
As a consequence, anyone capable of de-anonymising a person can figure out if they are sick!

1. Meet someone you can identify (you actually know them, they used a credit card in your shop...);
2. store their temporary crypto-identifier when you are close to them;
3. if said crypto-identifier shows up, you know that specific person is infected!

This could be scaled up, e.g. a supermarket could place bluetooth receivers at all the checkout desks.

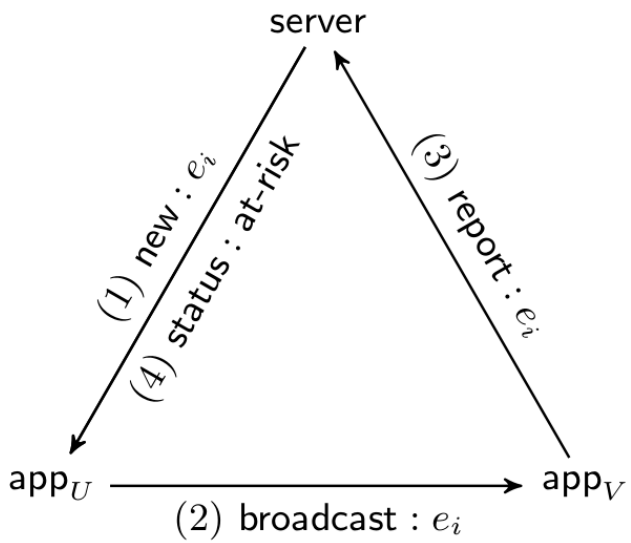
A Specific Attack (2/2)

A similar approach can be used to track the physical location of sick people.
`https://github.com/oseiskar/corona-sniffer`



Plan de cette section

“Centralized”?



1. The server generates and distributes crypto-identifers for each user,
2. Each user broadcasts the identifiers thus obtained,
3. If a user becomes sick, they send all the crypto-identifiers they received from others to the central server.
4. The server knows who these belong to and warns “at risk” users.

Motivation

The nefariousness of ill-intentionned users must be minimized.

In particular, the previous attack targetting centralized systems does not work : the attacker would only know if they have met at least one sick person, not who or how many.

A Specific Attack (1/2)

Of course, a State which is not a democratic State would have a very powerful tool for massive surveillance

10. “Investigating Third Ways for Exposure Notifications in Europe”, https://github.com/3rd-ways-for-EU-exposure-notification/resources/blob/master/A_Contribution_to_Third_Ways_in_Europe.pdf

A Specific Attack (1/2)

> *Of course, a State which is not a democratic State would have a very powerful tool for massive surveillance* (*Bruno Sportisse*[10])

The state-managed central server knows *a lot* :

- anonymity cannot really be guaranteed since we can link a permanent identifier with an IP adress,
- it knows the permanent identifiers of all those in “contact” with each sick person $\Longrightarrow$ the state will know large chunks of the social graph.

This problem is supposed to be solved using a mix-net. That would be quite a feat; it is not the case right now.

---

10. “Investigating Third Ways for Exposure Notifications in Europe”, `https://github.com/3rd-ways-for-EU-exposure-notification/resources/blob/master/A_Contribution_to_Third_Ways_in_Europe.pdf`

A Specific Attack (2/2)

More generally, the security level of a centralized system hinges on the temporary/permanent identifier correspondance.

A single cryptographic key protects the secrecy of this correspondence : if it it is recovered/leaks/is misused, then the anonymity of the whole system is compromised !