

PROTEGER DES VIES & LA LIBERTE

ou comment des
applications de
traçage de
contacts
peuvent
déjouer et
le COVID-19
et Big Brother



Un des problèmes avec le COVID-19, c'est que deux jours avant que la maladie ne soit détectable, on est déjà contagieux.



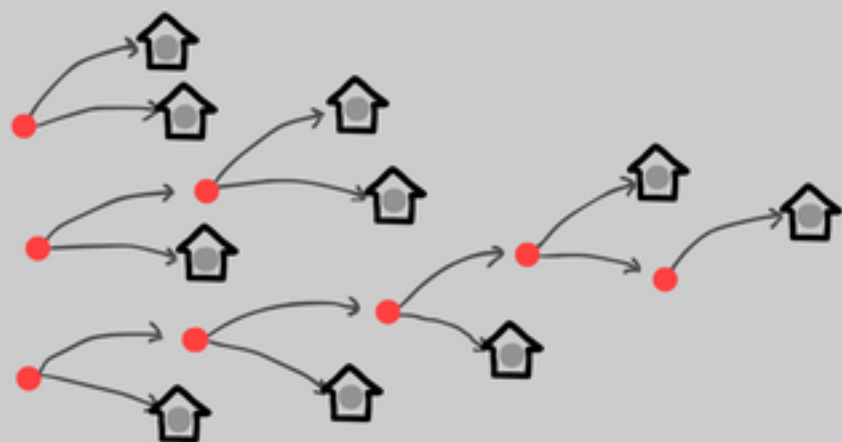
néanmoins on ne devient contagieux que trois jours *après* avoir été infecté ! Donc si une personne avec qui vous avez été en contact se place en quarantaine le jour où elle apprend que vous êtes vous-même infecté...



On stoppe le virus, en étant toujours en avance d'un jour sur lui !

* et quid des personnes asymptomatiques me direz-vous ? Ben en fait il s'avère qu'il.elles jouent un rôle mineur dans la propagation du COVID19. jetez donc un coup d'oeil aux références à la fin de la BD !

Ça s'appelle le "traçage des contacts"
et c'est une des techniques-clés
qui a permis à la Corée du Sud et
à Taiwan de maîtriser l'épidémie.
Nous ferions bien de faire de même.



Et on n'a même pas besoin de tracer
tous les contacts entre les gens !
60% serait déjà suffisant.

* comment ça 60% ? voir les références à la fin de la BD.

Néanmoins, ce traçage doit quasiment être fait en temps réel pour être efficace. La méthode traditionnelle pour obtenir ces informations (par interrogatoire) est trop lente.

C'est là où les applications de traçage entrent en jeu !

Devrons-nous sacrifier notre vie privée pour autant ?



OH QUE



NON



Il est tout à fait possible de
sauver des vies tout en protégeant
nos libertés, à l'aide
d'un procédé simplissime !

pour nous l'expliquer voici
Alice & Bob ...



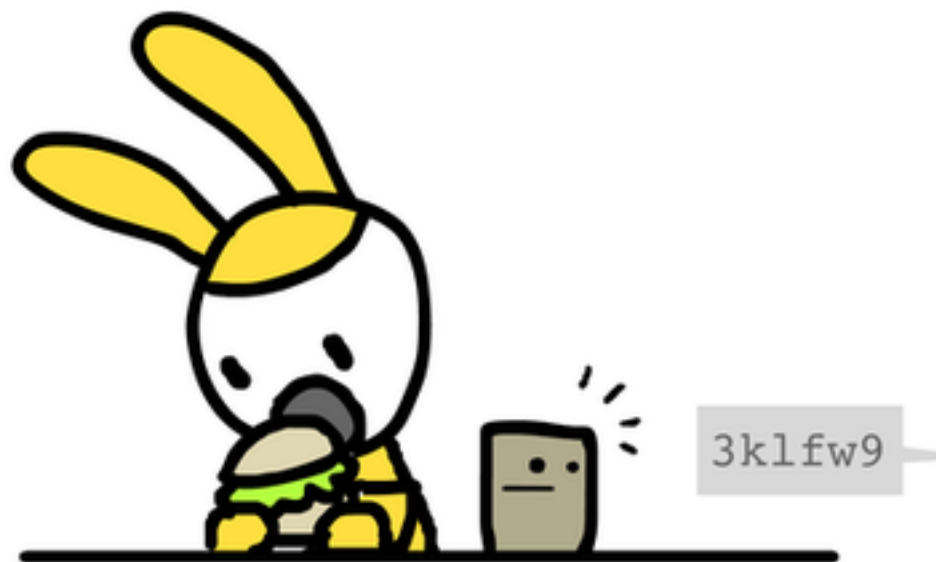
Alice télécharge une application de traçage (dont le code est public, ce qui fait qu'on peut vérifier que l'application fonctionne bien comme ceci :)



toutes les 5 minutes, son téléphone envoie un charabia aléatoire et unique à tous les autres téléphones à proximité, par Bluetooth.

* 5 minutes plus ou moins, c'est un exemple ! par ailleurs techniquement ce sont des messages pseudo-aléatoires mais ça ne change rien à notre affaire.

Dans la mesure où les messages sont aléatoires et ne contiennent aucune donnée de géolocalisation, ils ne contiennent AUCUNE information sur l'identité d'Alice ni sur les endroits où elle est allée.



En plus d'envoyer ses messages aléatoires, le téléphone d'Alice reçoit également les messages des autres téléphones à proximité.

Par exemple, celui de Bob.

Bob a installé la même application de traçage sur son téléphone (ou une autre application de traçage respectueuse de sa vie privée et compatible avec celle d'Alice).



Si Bob et Alice restent à proximité plus de 5 minutes, leurs téléphones vont échanger un message aléatoire et unique.

Leurs téléphones se souviennent de tous les messages dits et entendus ces derniers 14 jours.

CE QUE J'AI DIT

aSt5yv 1lwda6

8jUIL4 5lPomk

rtxnbk 33trGb

49djv7 ryteq8

12poLV VB490s

CE QUE J'AI ENTENDU

89ckxj 3klfw9

g83kxS wWjcd6

1789xI 439Hxs

59f7y5 zpw7UU

FFyc67 xlc902



Rappel: Les messages aléatoires ne contiennent AUCUNE INFO, l'intimité d'Alice est protégée de Bob, et vice versa!

* 14 jours est aussi juste un exemple! Les épidémiologistes pourraient apprendre que la "période infectieuse" est en fait plus courte ou plus longue que cela.

Le lendemain, Alice développe une toux sèche et de la fièvre.

Alice se fait tester.



Alice a le COVID-19.

Ce n'est pas un bon jour pour Alice.

Mais elle peut maintenant se venger du virus ! Alice envoie la liste des messages qu'elle a envoyés ces 14 derniers jours à un hopital, en utilisant un code qui lui a été fourni à cet effet par son médecin (c'est pour éviter le spam).



Alice peut également cacher les messages qu'elle veut garder pour elle, comme ceux que l'application a envoyés quand elle était à la maison.

L'Hôpital range les messages aléatoires d'Alice dans sa base de données.



TOUT CE QUE LES
COVID19 ONT DIT :



J'insiste encore : ces messages ne contiennent aucune information sur les endroits où elle est allée, sur son identité, *ni même sur le nombre de personnes avec qui elle a été en contact* ! Ces informations ne sont d'aucun usage à l'hôpital.

* Différents hôpitaux peuvent mettre ces bases de données en commun, mais dans la mesure où aucune information personnelle n'y est stockée ça ne présente pas de danger.

...mais pas pour Bob !



Le téléphone de Bob vérifie régulièrement la liste de messages de cas du COVID-19 de l'hôpital, et voit s'il a "entendu" n'importe lequel de téléphones proches ces derniers 14 jours.

(Le charabia ne donne à Bob
AUCUNE AUTRE INFO PERSONNELLE.)

* Le vrai protocole DP-3T est encore PLUS sécurisé ! il utilise une méthode appelée "cuckoo filter" pour que les téléphones ne connaissent QUE les messages covid-19 qu'ils ont entendus, sans révéler TOUS les messages covid-19.

S'il a reçu, mettons, 6 messages envoyés par le téléphone de personnes atteintes de COVID19 (6 * 5 minutes : 30 minutes d'exposition au virus), le téléphone va suggérer à Bob de se placer en quarantaine.



Et ainsi Bob stoppe la propagation du virus, en étant un jour en avance sur lui !

* à nouveau, ces nombres ne sont que des exemples !

Et voilà !

C'est comme ça que le traçage numérique des contacts peut proactivement prévenir la transmission du COVID-19 *tout en* protégeant nos droits.



Merci, Alice & Bob !
Prenez soin de vous.

RÉFÉRENCES :

Cette BD vise à vulgariser le protocole **DP-3T**, tel qu'il fonctionnait en date du 9 avril 2020. En réalité, c'est un truc assez complexe et *très* sécurisé ! pour en savoir plus :

github.com/DP-3T/documents

Il existe un autre protocole similaire, garantissant également la protection de la vie privée, le protocole **TCN** :

github.com/TCNCoalition/TCN

Enfin, vous trouverez ici l'étude de l'université d'Oxford qui montre que les applications de traçage pourraient à elles seules permettre de contenir l'épidémie (*sans* quarantaine généralisée).

Ferretti & Wymant et al. "Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing." *Science* (2020).

Cette BD est dans le

DOMAINE PUBLIC

Ce qui veut dire que vous avez automatiquement le droit de la republier sur votre propre site. Et même, nous serions très heureux que vous l'utilisiez pour illustrer le fonctionnement de votre propre application de traçage! (du moment qu'elle respecte la vie privée des gens tel que cela est décrit dans la BD).

Cela veut aussi dire que vous avez le droit de traduire ce texte! (les polices utilisées sont : "Patrick Hand" et "Open Sans").



by **Nicky Case**

ncase.me + patreon.com/ncase

avec l'aide précieuse de

Prof. Carmela Troncoso (security)
& **Prof. Marcel Salathé** (epidemiology)