Risks and Limits of covid-19 tracing app

Véronique Cortier, CNRS research director
(Nancy, France)
https://members.loria.fr/VCortier/

Co-author of a document explaining tracing risks to the public together with a group of 14 researchers

Risks of tracing apps

No guaranteed privacy

All proximity tracing systems enable a motivated attacker to identify the infected people she has been in close proximity to.

acknowledged in the DP-3T security analysis

Risks of tracing apps

No guaranteed privacy

All proximity tracing systems enable a motivated attacker to identify the infected people she has been in close proximity to.

- A motivated neighbour can learn who is infected in his building
- A motivated organisation can do that too, on a larger scale
- Depending on the app : the state and/or Google and Apple have the ability to learn who is infected

acknowledged in the DP-3T security analysis

Risks of tracing apps

No guaranteed privacy

All proximity tracing systems enable a motivated attacker to identify the infected people she has been in close proximity to.

- A motivated neighbour can learn who is infected in his building
- A motivated organisation can do that too, on a larger scale
- Depending on the app : the state and/or Google and Apple have the ability to learn who is infected

False alarms

An attacker can trigger false alarms about encounters with an infected person that do not reflect real-world physical proximity.

acknowledged in the DP-3T security analysis

Risks of tracing apps

No guaranteed privacy

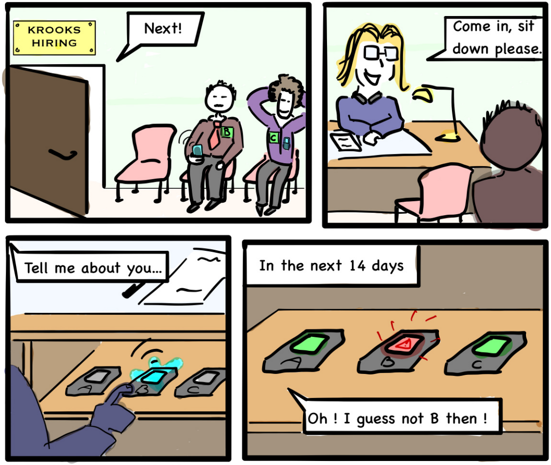
All proximity tracing systems enable a motivated attacker to identify the infected people she has been in close proximity to.

- A motivated neighbour can learn who is infected in his building
- A motivated organisation can do that too, on a larger scale
- Depending on the app : the state and/or Google and Apple have the ability to learn who is infected

For centralized applications (such as ROBERT/stopcovid)

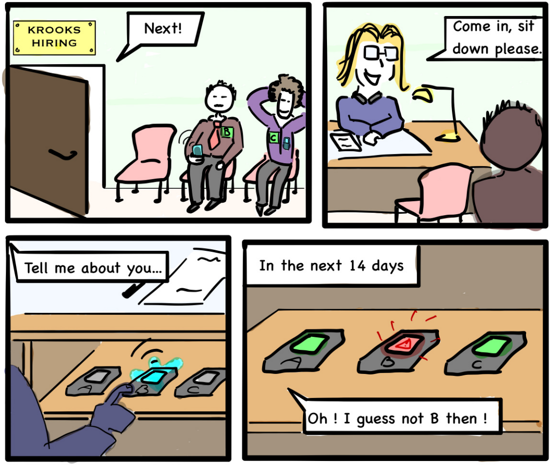
- The server may learn the social graph of infected people (it knows who these people met)
- The server may know when Alice, notified at risk, still continues to meet people like Bob (if either Bob or Alice declare themselves as positive)

The KROOKS company



Disclaimer : this attack works only if tracing apps were working (don't be too afraid for the moment).

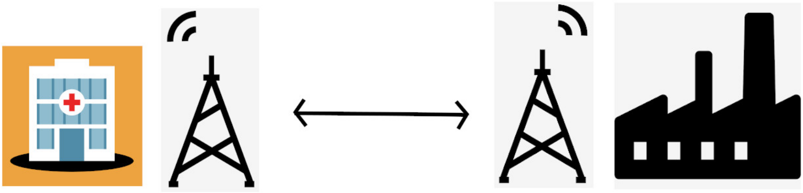
The KROOKS company



Disclaimer : this attack works only if tracing apps were working (don't be too afraid for the moment).

Note : even easier for decentralized applications like DP3T (no need of dedicated phones)

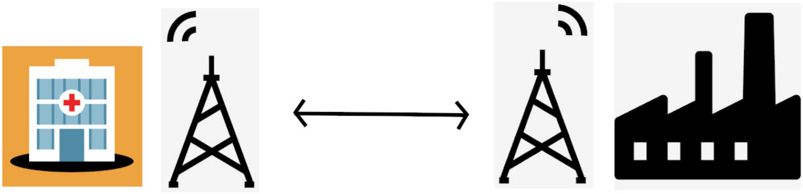
An attack scenario



Scenario (RansomWorkers)

Mr. EconomySpy uses two high range bluetooth antennas and relays messages from phones around a medical lab to a competing company. At the end of the day, the factory is paralyzed.

An attack scenario



Scenario (RansomWorkers)

Mr. EconomySpy uses two high range bluetooth antennas and relays messages from phones around a medical lab to a competing company. At the end of the day, the factory is paralyzed.

- Another use case : a student wishes her university to get close in order to cancel her exam.
- More scenarios in our document

Risks : contact tracing apps have bugs

- Number of privacy, security, functionality and usability issues in the COVIDSafe app (Australia)
- The French National Commission on Informatics and Liberty (CNIL) confirmed several security and privacy issues in the StopCovid app (France), and publicly summoned the Health department to address them.
- Cocoa app (Japan) suspended at least two times as a consequence of bugs.
- False notifications in Switzerland on iOS 13.7

Limits : A contact tracing application - really ?

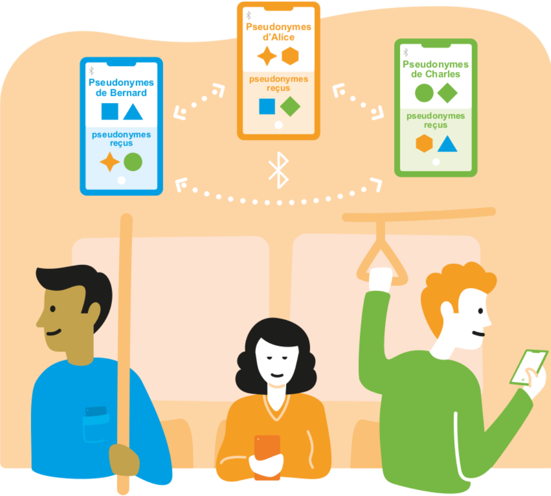
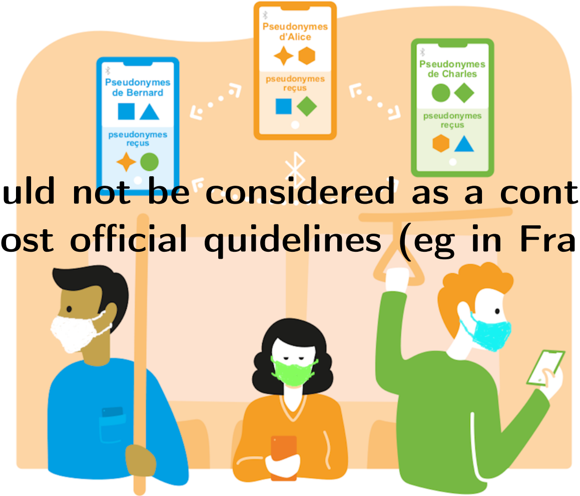


Illustration of the Robert (French) covid-19 tracing app

Limits : A contact tracing application - really ?



Would not be considered as a contact in most official quidelines (eg in France)

Limits : Adoption

Politics : “the app is efficient from the first download”

Theory : Roughly, 30% of adoption $\Rightarrow$ about 10% found contacts (for perfectly working apps)

Limits : Adoption

Politics : “the app is efficient from the first download”

Theory : Roughly, 30% of adoption ⇒ about 10% found contacts (for perfectly working apps)

Practice :

- Australia :
  - 6 weeks after deployment : 6 millions downloads, no single otherwise unidentified contact
  - 3 months after : 2 people identified by the app were tested positive
- France :
  - 10 weeks of deployment : 2.3 millions downloads, 72 exposure notifications
  - French’s prime minister Jean Castex : “StopCovid did not deliver the results that were hoped for”.

Benefits : how are they evaluated ?

It is very hard to get information on the efficiency on the apps.

We need regular and reliable figures :

- number of downloads to measure adoption
  → better : number of effectively active apps (pulling data every day)
- number of notifications to measure efficiency
  → better :
  - number of people that would not have been notified otherwise (can be asked when testing or through investigation)
  - number of notified people that are tested positive

Benefits : how are they evaluated ?

It is very hard to get information on the efficiency on the apps.

We need regular and reliable figures :

- number of downloads to measure adoption
  → better : number of effectively active apps (pulling data every day)
- number of notifications to measure efficiency
  → better :
  - number of people that would not have been notified otherwise (can be asked when testing or through investigation)
  - number of notified people that are tested positive

We need evaluation !

- requested by numerous agencies as a requirement to approve the apps
- risks (privacy loss, false alarm, attacks due to bugs) are acceptable only w.r.t. <u>actual</u> benefits

Lessons learned

Our community needs guidelines to work under such pressure

- Tracing apps seen as a gold opportunity "to do something"
  → anyone questioning apps was not willing to help...
  → in a few weeks, our community was split between the "good ones" and the "bad ones"
- Any criticism was badly perceived by the app designers
  → were working day and night, sacrificing their personal life.

Lessons learned

Our community needs guidelines to work under such pressure

- Tracing apps seen as a gold opportunity "to do something"
  → anyone questioning apps was not willing to help...
  → in a few weeks, our community was split between the "good ones" and the "bad ones"
- Any criticism was badly perceived by the app designers
  → were working day and night, sacrificing their personal life.
- Worse : politics rather than science
  - Governments were urged to do something
  - Private companies have a lot of interest in dealing with medical data
  - Research Institutes (e.g. Inria) wished to gain visibility
    → criticising stopcovid considered as treacherous

Lessons learned

Our community needs guidelines to work under such pressure

- Tracing apps seen as a gold opportunity "to do something"
  → anyone questioning apps was not willing to help...
  → in a few weeks, our community was split between the "good ones" and the "bad ones"
- Any criticism was badly perceived by the app designers
  → were working day and night, sacrificing their personal life.
- Worse : politics rather than science
  - Governments were urged to do something
  - Private companies have a lot of interest in dealing with medical data
  - Research Institutes (e.g. Inria) wished to gain visibility
    → criticising stopcovid considered as treacherous

Pressure on app designers to deliver something fast,
without peer evaluation
Pressure on opponents to not talk to the press (at least in France)

To conclude

- We need to do better, as a community.
- How the benefits of the app are currently evaluated ?
- On the long term, do we want to encourage tracing apps, for health purposes ?

Want to learn more ?

Our document on the risks of tracing apps is available online :

- (in French) `https://risques-tracage.fr/`
- (in English) `https://tracing-risks.com`

A recent and well documented discussion by Olivier Pereira.

- some slides are borrowed from this document
- `https://dial.uclouvain.be/pr/boreal/object/boreal:232991`

Statement from the Europe TPC of the ACM

Technology Policy Committee of the Association for Computing Machinery

- "at this time known contact tracing apps cannot fully preserve individual privacy and anonymity"
- lists best practices
  → we'll need a lot of time to do things right

`https://www.acm.org/binaries/content/assets/public-policy/europe-tpc-contact-tracing-statement.pdf`

Credits and licence

Image credits :

- page 4 : image made from images licensed under CC0 1.0
- pages 6, 7 : Illustration of the Robert application from https://github.com/ROBERT-proximity-tracing/documents licensed under CC BY-NC-SA 3.0 (Design : Nicolas Steff)