Contact tracing applications

A brief summary of the 2020 gt-c2/gt-pvp reading group on contact tracing

Alain Passelègue - June 30, 2021 - Journées Nationales 2021 du GDR Sécurité Informatique

A bit of context

March 2020 - Europe

- Covid-19 strikes Europe, shutdowns in most European countries

- (Asian) countries start to use technology to track individuals as a tool to reduce the spread of Covid-19:
  - Track GPS position, credit card payments, public transport, … (South Korea, Singapour)
  - Electronic tags to restrict and surveil movements of potentially infected individuals (Hong-Kong)
  - Video surveillance and facial recognition (China, South Korea, Singapour, Russia, …)

- In the West: Bluetooth contact tracing as a sensible solution?
  - Bluetooth can be used to detect nearby devices without tracking location

Bluetooth contact tracing in the West

- Two main approaches: **“centralized”** (France, UK, Norway) vs **“decentralized”** (Switzerland, USA, Austria, Italy, Ireland, …)

- Heated debates, warnings about the risks of such apps, decentralized approach favoured by many experts https://www.esat.kuleuven.be/cosic/sites/contact-tracing-joint-statement/

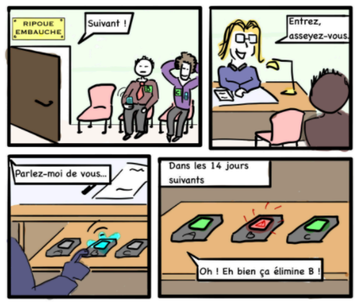
Joint Statement on Contact Tracing: Date 19th April 2020

The undersigned represent scientists and researchers from across the globe. The current COVID-19 crisis is unprecedented and we need innovative ways of coming out of the current lockdowns. However, we are concerned that some “solutions” to the crisis may, via mission creep, result in systems which would allow unprecedented surveillance of society at large.

- Contact tracing **cannot be secure** https://www.risques-tracage.fr/

Le traçage anonyme, dangereux oxymore

Analyse de risques à destination des non-spécialistes



Seminars on contact tracing apps

- Seminars for French researchers in the underlying areas (limited audience for various reasons…)

  Co-organized with Geoffroy Couteau, with the help of Benjamin Nguyen and after discussions with Brice Minaud, David Pointcheval, Damien Vergnaud, …

- **Objectives:**
  - Understand the different paradigms: designs, specifications, bluetooth usage, risk scoring, …
  - Attacks and choices made (or not) to mitigate them
  - Security/efficiency trade-offs
  - Compare what is supposed to be implemented and what is actually deployed
  - Inform the population

Mise en garde contre les applications de traçage

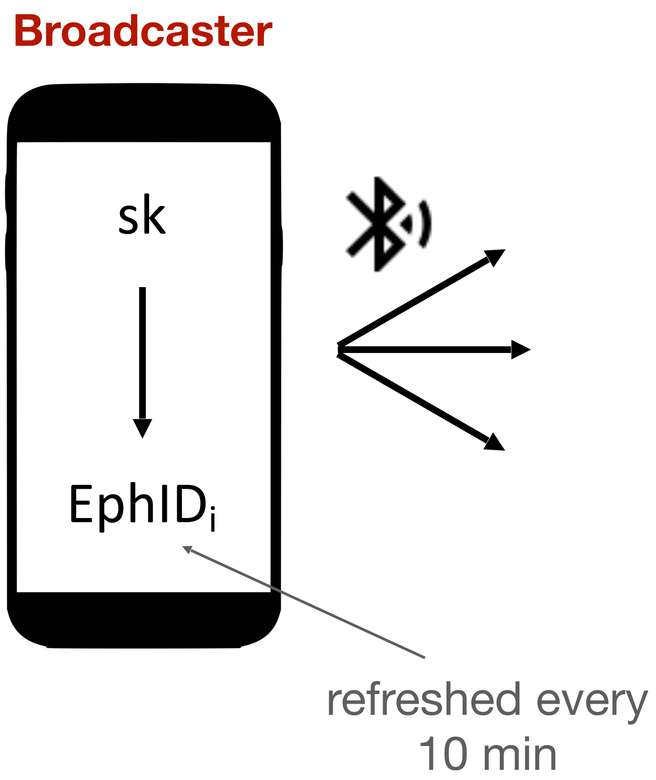
Ce document comprend deux parties, avec, pour chacune d'entre elles, sa liste de signataires. La première partie est un texte écrit et signé par des spécialistes du domaine. La seconde partie est un texte court qui mentionne le soutien apporté à ce texte par des informaticiennes et informaticiens qui ont de l'intérêt pour les domaines de la cryptologie et de la sécurité informatique, sans s'en sentir spécialistes. Il est suivi par la liste de ses signataires.

Dimanche 26 avril 2020
Contact: contact@attention-stopcovid.fr

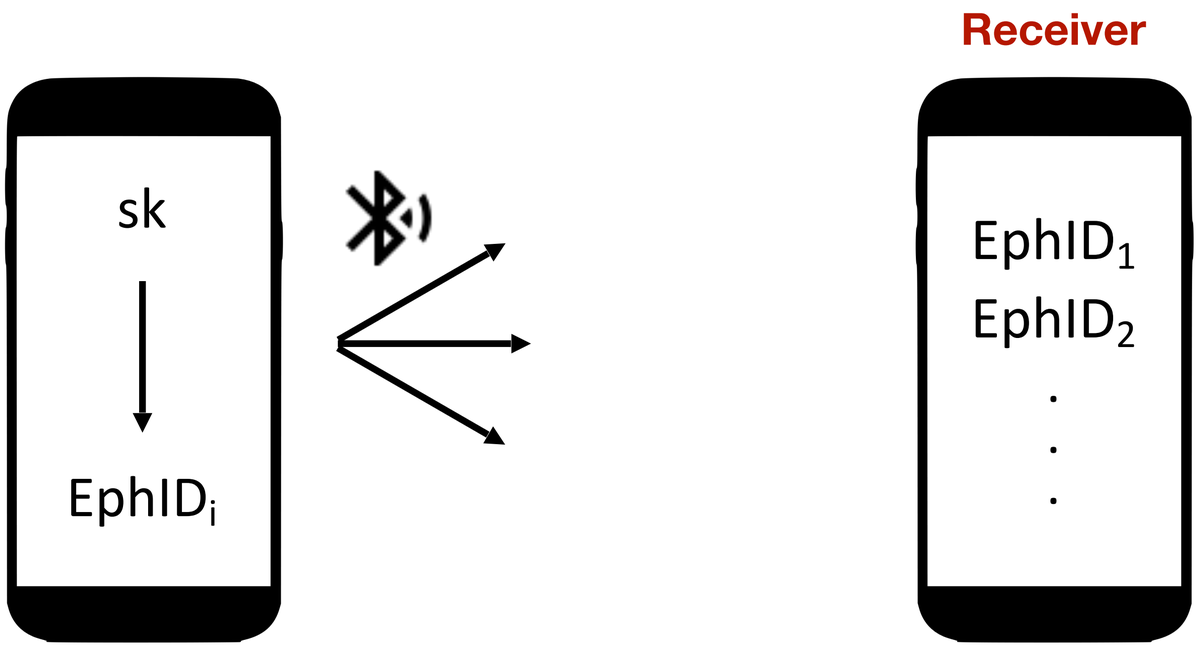
List of seminars

1. Blue and Robert, *by Cédric Lauradoux (Citi, Privatics), May 27*
2. DP3T, *by Geoffroy Couteau (IRIF) and Alain Passelègue, May 29*
3. Bluetooth Low Energy (BLE) in contact tracing, *by Mathieu Cunche (Citi, Privatics), June 3*
4. Differential privacy in contact tracing, *by Benjamin Nguyen (LIFO), June 6*
5. Evaluation of risk of exposure from RSSI measures, *by Jean-Marie Gorce (Citi, Socrate), June 26*
6. Contact tracing in Canada, *by Sébastien Gambs (UQAM), September 15*

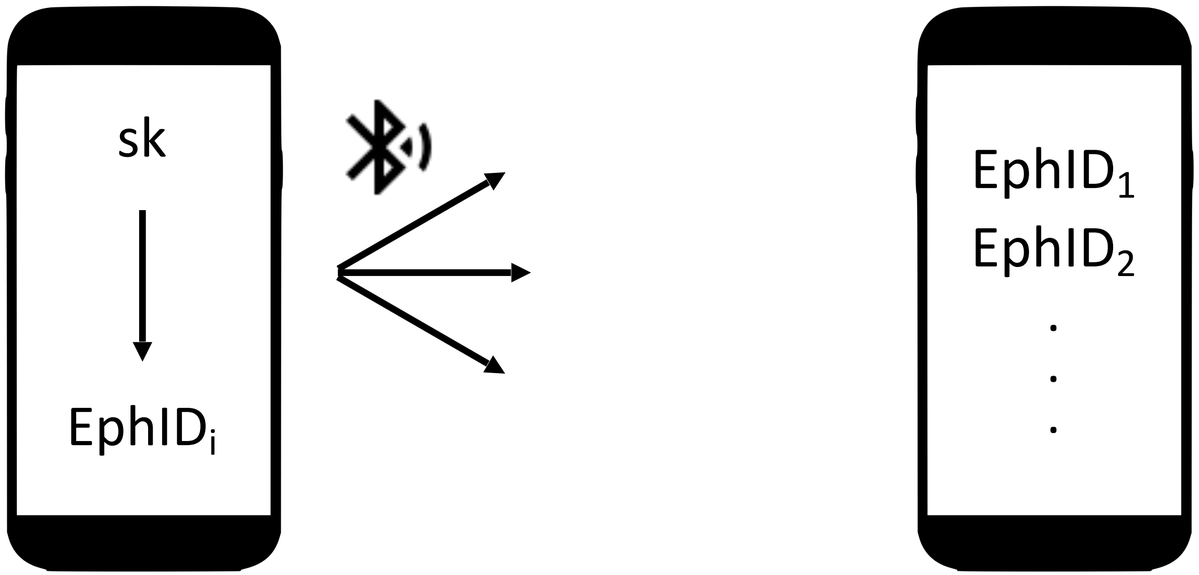
Bluetooth contact tracing: the theory



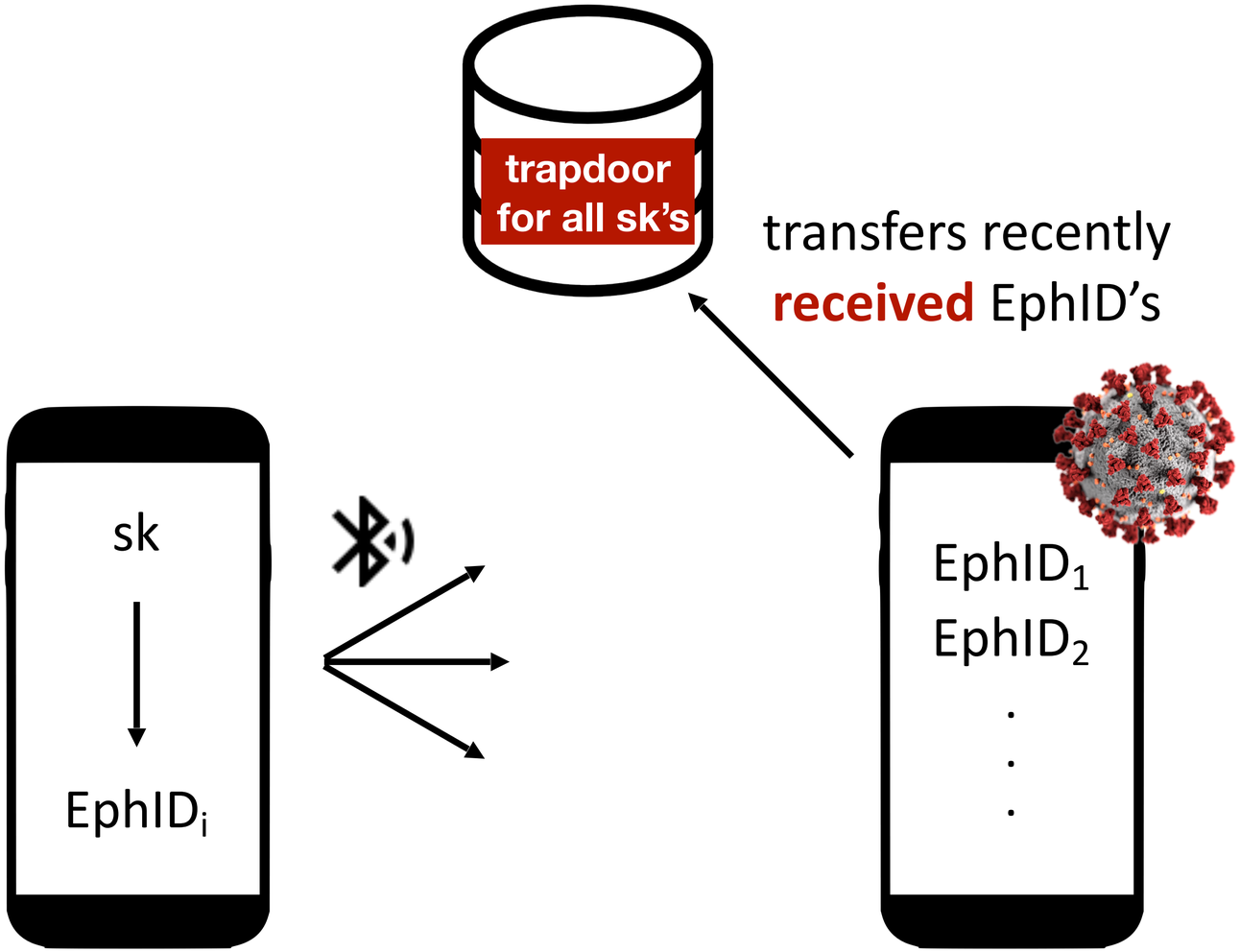
Bluetooth contact tracing: the theory



Bluetooth contact tracing: the theory



Bluetooth contact tracing: the theory

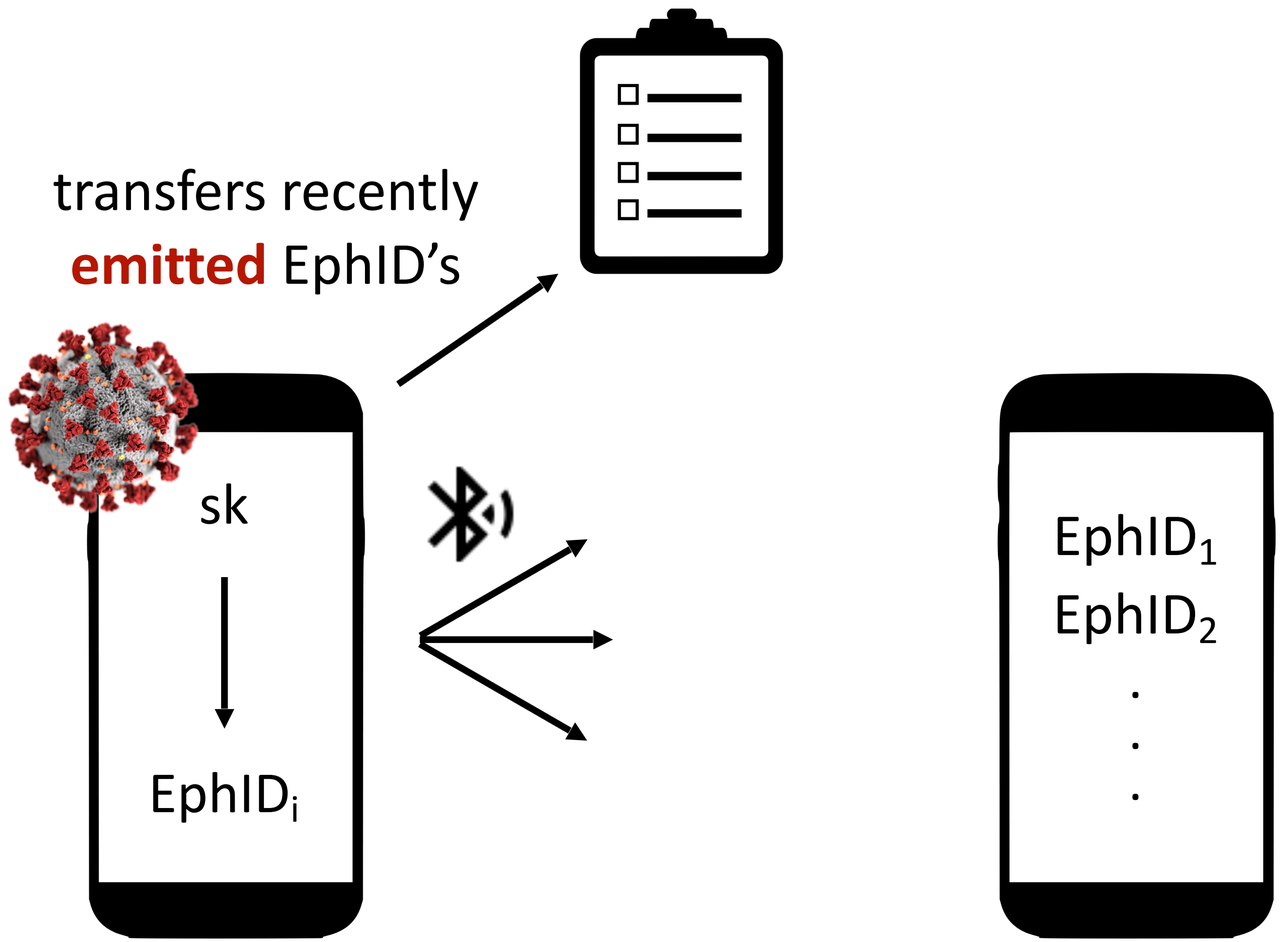


Centralized (Robert)

1. Infected user sends to the central server **all the EphID it received**
2. Server **recovers the corresponding contacts** and **computes a risk of exposure**
3. Server **alerts** contacts at risk

Server knows all users who have been in contact with infected users

Bluetooth contact tracing: the theory



Centralized (Robert)

1. Infected user sends to the central server **all the EphID it received**
2. Server **recovers the corresponding contacts** and **computes a risk of exposure**
3. Server **alerts** contacts at risk

Server knows all users who have been in contact with infected users

Decentralized (DP3T)

1. Infected user sends to the central server **all the EphID it emitted**
2. Server is just a **public bulletin board** of all recently **infected EphID's**
3. After each update of the list of infected EphID's, each individual looks for match with its **received EphID's**

Server knows (basically) nothing, exposure is checked locally by every user

Insecure by definition

Some inherent attacks

- If you met just 1 person and you receive an alert, this person has to be infected…
  Easy to generalize (compare alerts with co-workers, use n phones, …)

- ***Differential privacy could help:*** add false alerts? Depends on consequences

- ***More attacks:*** deploy multiple devices to gather information, force an alert on a target, replay/relay attacks…
  —see talk by Véronique Cortier?

Design-related attacks

1. Tracking users and their social interaction

Centralized

- **Server can link any EphID** to a **unique** user **(including non-infected users)**
- Infected user sends **all its contacts** to server
- **Mixnets** to prevent it to receive all contacts at once but **are NOT implemented**
- **Corrupting the server is devastating**

Decentralized

- Link EphID's emitted by **1 infected user** within the same day… Up to **14 days** with auxiliary info
- Users could be willing to share when and where they met a **target infected user**
- Reconstruct a partial social graph of a **target infected user**
- **Easy to mount but does not scale well**

Design-related attacks

2. Identifying an infected user

Centralized

- **Upload is supposed to be anonymous**
- **Mostly inherent attacks** (but server has tons of data to mount them… Still costly)

Decentralized

- **Data pooling** is very easy since **EphID's of infected users are public and linkable** on each 1-day period
- **Quite easy to identify an infected user**

Bluetooth contact tracing: the practice

Bluetooth as a measuring tape…

- To estimate risk of exposure: at least distance and duration of encounter
- Measures are **sensitive to environment**

Manufacturer	Device Name	Model	Distance (m)	Orientation	Average (dBm)
APPLE	iPhone X	iPhone X	2	Top	-53.84
SAMSUNG	Galaxy Note 9	SM-N960F	2	Top	-59.64
SAMSUNG	Galaxy S8	SM-G950F	2	Top	-69.13
SAMSUNG	Galaxy S10+	SM-G975F	2	Top	-57.87
SAMSUNG	Galaxy Note 10+	SM-N975F	2	Top	-49.9
APPLE	iPhone 6	iPhone 6	2	Top	-59.06
HUAWEI	Mate 20 Pro	LYA-L29	2	Top	-70.56

Figure: RSSI measures depending of phone model

Bluetooth contact tracing: the practice

Bluetooth as a measuring tape…

- To estimate risk of exposure: at least distance and duration of encounter
- Measures are **sensitive to environment**
- **Metadata are broadcasted** together with EphID's to correct measures (e.g., phone model, …)
- All these metadata are **easy to collect** and **drastically help attacking privacy** (e.g., DP-3T++ app available freely on Android store handles this automatically)
- StopCovid **stored all encounters** and not just those with risk (long and close enough), as pointed out by Gaëtan Leurent… Later patched.

Thanks!