Contact Tracing

Jaap-Henk Hoepman

Privacy & Identity Lab
iHub, Radboud Universiteit
Rijksuniversiteit Groningen

✉ *jhh@cs.ru.nl* // *www.cs.ru.nl/~jhh* // blog.xot.nl // @xotoxot

1

Agenda

- **Scope: contact tracing, from a technical perspective (mostly)**
- **Contact tracing basics**
- **Distributed versus centralized**
- **Privacy & security issues**
- **GACT: the Google/Apple platform**

2

Contact tracing basics

- **Goals (informed by epidimiological information)**
  - Identify "contacts" of infected patients over certain period (typically 14 days)
- **Contact?**
  - Someone in close proximity (within 1 – 2 meters)
  - For a certain amount of time (at least 5 – 10 minutes)
  - Depending on context (indoors/outside?, wall separating people?….)
- **Traditionally a labour intensive, manual process**
  - Interviewing infected patients and their potential contacts (also necessary to reassure people)

3

"Solutionalism?": Smartphones support for contact tracing

- **Using a contact tracing app**
  - For example based on location data
- **Mobile network (cell tower) data?**
  - Very imprecise: 100m – 10 km
- **GPS?**
  - Imprecise (especially indoors): 5 – 10 meters precision
- **QR!**
  - Check in/out; virtual handshake
  - Explicit consent, but therefore not automatic

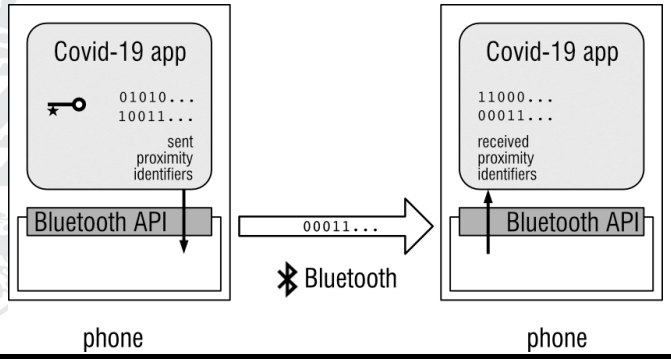
4

Bluetooth based app

- **Smartphones send Bluetooth signals regularly**
- **Use signal strenght to estimate distance**
  - Bluetooth is short range (several meters), but
  - Conditions may severely affect accuracy of estimate: bodies and buildings block signals, and signals travel far over water
- **Phones store signals received (if relevant)**
  - Contacts automatically logged
  - Provided both phones have Bluetooth switched on
- **Effective if > 60 – 70% of all people have app installed and Bluetooth switched on**
  - May be hard to meet in practice

5

Bluetooth based contact tracing (1)



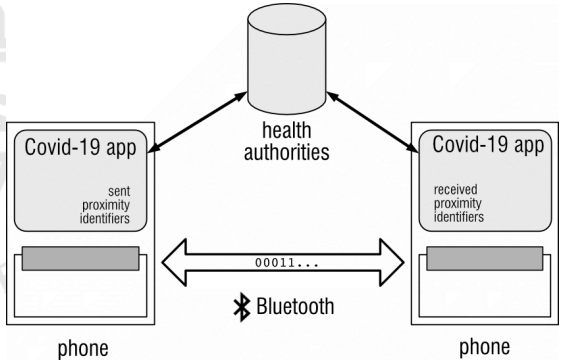
6

Bluetooth based contact tracing (2)

- **Broadcast**
  - Phone broadcasts proximity identifier (psuedonym) regularly
  - Changed regularly to avoid tracing (but not too fast to determine relevance for contact)
  - Change in sync with changing MAC address
  - Derived from daily/global key for efficiency
  - Keys/identifiers retained for fixed period (14 days)
- **Collect**
  - Phone collects any received proximity identifiers, keeping only those relevant for contact (distance + time)
  - Phone may tag these with time and location information
  - Phone automatically discards old proximity identifiers after fixed period (14 days)

7

Bluetooth based contact tracing (3)



8

Bluetooth based contact tracing (4)

Centralised (PEPP-PT/ROBERT)

- **Determining contacts is done by central server**
  - Infected patients phone is asked to upload all the proximity identifiers it collected to central server
  - These identifiers contain information that allow the server to establish the true identity of all contacts
  - Server warns these contacts

Distributed (DP3T)

- **Determining contacts is done on phone itself**
  - Infected patients phone is asked to upload all its own proximity identifiers (or the keys used to generate them) to central server
  - Other phones regularly contact this server for updates
  - Match new downloaded proximity identifiers with previously collected ones
  - Phone itself generates warning

9

Hidden assumption

App/phone of user in distributed setting is somehow trusted to behave honestly

10

Main privacy/security risks

Centralised

- **False alerts; denial of service**
- **Know who infected you**
- **Learn social graph (of infected people, and those in close contact)**

Distributed

- **False alerts; denial of service**
- **Know who infected you**
- **Trace movements of infected people (using released daily keys/proximity identifiers)**

11

Privacy & Identity Lab

iHub

Radboud Universiteit

rijksuniversiteit groningen

12

Privacy & Identity Lab

iHub

Radboud Universiteit

rijksuniversiteit groningen

GACT: Google Apple Contact Tracing platform

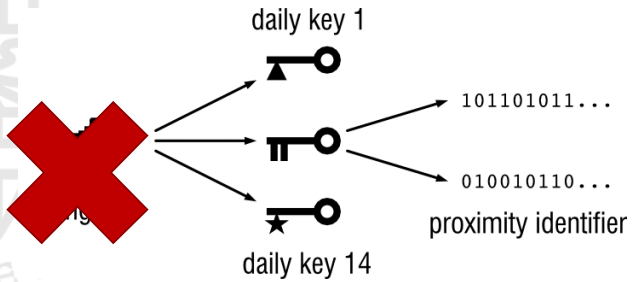
13

GACT principles

- Distributed
- First to be released as an API in May
- Later to be embedded in OS
- Specifications in flux
  - https://www.apple.com/covid19/contacttracing/
  - First called Contact Tracing, now called Exposure Notification
- Only way for apps to use Bluetooth
- Once enabled works, even if user has no app installed

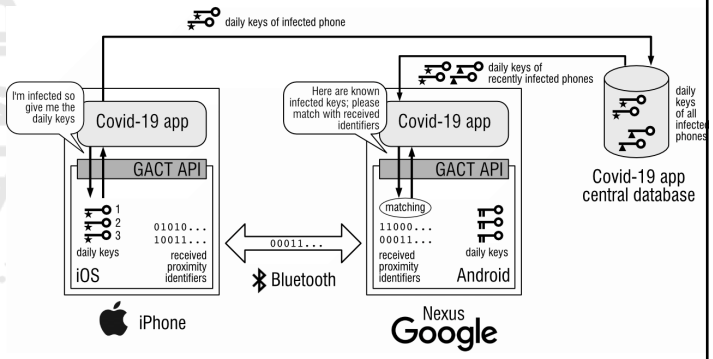
14

GACT: keys



15

GACT: API



16

Analysis (1)

- **Consent based**
  - Accroding to FAQ: opt-in; but how “off” is “off”?
- **Contact tracing moves from the app layer down to the OS layer**
  - Available all the time → no longer limited in time
  - For all kinds of apps → no longer limited in use
  - Loss of control → you can uninstall an app, but not an OS
- **GACT monopoly**
  - Because any contract tracing app is required to use it; otherwise no access to Bluetooth (which is a problem especially under iOS)
  - Microdata solely under Apple/Google control
- **Enormous amount of trust put in Google and Apple**

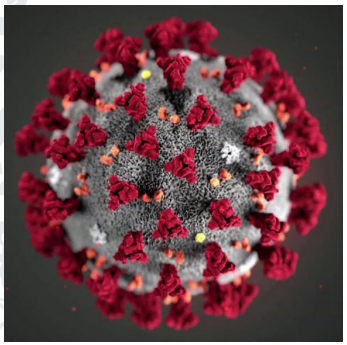
17

Analysis (2)

- **Distributed can be made centralised**
  - Any app can report the locally computed result back to the central server
  - And can learn important metadata when cleverly using API
- **Function creep**
  - China: monitor Uyghurs. Israel: monitor Palestinians.
  - Monitor the visitors of abortion clinics, coffee shops, gay bars, ….
  - Contact tracing also has tremendous commercial value.
- **This (technically) creates a dormant functionality for mass surveillance**
  - Interoperable between Google and Android
  - Interoperable globally

18

It’s a bit like…. Having a virus in your house



- **We have removed the spikes**
- **We will only release with your explicit consent**
- **We will remove it as soon as it is no longer necessary**
- **…**
- **It all depends on how afraid you are of virusses…**

19

Questions / discussion

[Monty Python’s Argument Clinic sketch]

jhh@cs.ru.nl www.cs.ru.nl/~jhh blog.xot.nl twitter: @xotoxot
Jaap-Henk Hoepman //

20