Contact
Tracing Apps: Engineering Privacy in Quicksand

Prof. Carmela Troncoso
@carmelatroncoso
https://spring.epfl.ch/

3.2.2021
A collaborative (continued) sprint

March 2020 - Start

April 2020 – GAEN is announced

May 2020 – Final version DP3T

June 2020 – Pilot SwissCovid (& other EU apps)

July 2020 – SwissCovid launch

August/September 2020 – Towards international interoperability

September/November 2020 – Presence tracing

Decentralized Privacy-Preserving Proximity Tracing

Contact the first author for the latest version.

EPFL: Prof. Carmela Troncoso, Prof. Mathias Payer, Prof. Jean-Pierre Hubaux, Prof. Marcel Salathé, Prof. James Larus, Prof. Edouard Bugnion, Dr. Wouter Lueks, Theresa Stadler, Dr. Apostolos Pyrgelis, Dr. Daniele Antonioli, Ludovic Barman, Sylvain Chatel

ETHZ: Prof. Kenneth Paterson, Prof. Srdjan Ćapkun, Prof. David Basin, Dr. Jan Beutel, Dr. Dennis Jackson, Dr. Marc Roeschlin, Patrick Leu

KU Leuven: Prof. Bart Preneel, Prof. Nigel Smart, Dr. Aysajan Abidin

TU Delft: Prof. Seda Gürses

University College London: Dr. Michael Veale

CISPA: Prof. Cas Cremers, Prof. Michael Backes, Dr. Nils Ole Tippenhauer

University of Oxford: Dr. Reuben Binns

University of Torino / ISI Foundation: Prof. Ciro Cattuto

Aix Marseille Univ, Université de Toulon, CNRS, CPT: Dr. Alain Barrat

IMDEA Software Institute: Prof. Dario Fiore

INESC TEC: Prof. Manuel Barbosa (FCUP), Prof. Rui Oliveira (UMinho), Prof. José Pereira (UMinho)
A collaborative (continued) sprint Marathon

March 2020 - Start

April 2020 – GAEN is announced

May 2020 – Final version DP3T

June 2020 – Pilot SwissCovid (& other EU apps)

July 2020 – SwissCovid launch

August/September 2020 – Towards international interoperability

September/November 2020 – Presence tracing

Decentralized Privacy-Preserving Proximity Tracing

Contact the first author for the latest version.

EPFL: Prof. Carmela Troncoso, Prof. Mathias Payer, Prof. Jean-Pierre Hubaux, Prof. Marcel Salathé, Prof. James Larus, Prof. Edouard Bugnion, Dr. Wouter Luks, Theresa Stadler, Dr. Apostolos Pyrgelis, Dr. Daniele Antonioli, Ludovic Barman, Sylvain Chatel

ETHZ: Prof. Kenneth Paterson, Prof. Srdjan Čapkun, Prof. David Basin, Dr. Jan Beutel, Dr. Dennis Jackson, Dr. Marc Roeschlin, Patrick Leu

KU Leuven: Prof. Bart Preneel, Prof. Nigel Smart, Dr. Aysajan Abidin

TU Delft: Prof. Seda Gürses

University College London: Dr. Michael Veale

CISPA: Prof. Cas Cremers, Prof. Michael Backes, Dr. Nils Ole Tilippenhauer

University of Oxford: Dr. Reuben Binns

University of Torino / ISI Foundation: Prof. Ciro Cattuto

Aix Marseille Univ, Université de Toulon, CNRS, CPT: Dr. Alain Barrat

IMDEA Software Institute: Prof. Dario Fiore

INESC TEC: Prof. Manuel Barbosa (FCUP), Prof. Rui Oliveira (UMinho), Prof. José Pereira (UMinho)
A collaborative (continued) sprint Marathon Ironman

March 2020 - **Start**

April 2020 – **GAEN is announced**

May 2020 – **Final version DP3T**

June 2020 – **Pilot SwissCovid**
(& other EU apps)

July 2020 – **SwissCovid launch**

August/September 2020 – **Towards international interoperability**

September/November 2020 – **Presence tracing**

---

**Decentralized Privacy-Preserving Proximity Tracing**

**Version:** 25 May 2020.
Contact the first author for the latest version.

**EPFL:** Prof. Carmela Troncoso, Prof. Mathias Payer, Prof. Jean-Pierre Hubaux, Prof. Marcel Salathé, Prof. James Larus, Prof. Edouard Bugnion, Dr. Wouter Lueks, Theresa Stadler, Dr. Apostolos Pyrgelis, Dr. Daniele Antonioli, Ludovic Barman, Sylvain Chatel

**ETHZ:** Prof. Kenneth Paterson, Prof. Srdjan Čapkun, Prof. David Basin, Dr. Jan Beutel, Dr. Dennis Jackson, Dr. Marc Roeschlin, Patrick Leu

**KU Leuven:** Prof. Bart Preneel, Prof. Nigel Smart, Dr. Aysajan Abidin

**TU Delft:** Prof. Seda Gürses

**University College London:** Dr. Michael Veale

**CISPA:** Prof. Cas Cremers, Prof. Michael Backes, Dr. Nils Ole Tippenhauer

**University of Oxford:** Dr. Reuben Binns

**University of Torino / ISI Foundation:** Prof. Ciro Cattuto

**Aix Marseille Univ, Université de Toulon, CNRS, CPT:** Dr. Alain Barrat

**IMDEA Software Institute:** Prof. Dario Fiore

**INESC TEC:** Prof. Manuel Barbosa (FCUP), Prof. Rui Oliveira (UMinho), Prof. José Pereira (UMinho)
Technology to help with pandemic contention

- Manual tracing overwhelmed

- The need
  - A complement to notify users that have been exposed to COVID19 and they are at risk of infection
  - In a timely, efficient, and scalable manner
The constraints: Security and Privacy

- Protect from misuse (surveillance, manipulation, etc)
  - Purpose limitation by default

The constraints: Security and Privacy

German restaurants object after police use COVID data for crime-fighting

COVID contact tracing sheet leaves 'creepy' barman to text model

Australia's spy agencies caught collecting COVID-19 app data

Covid 19 coronavirus: Subway worker 'harassed' woman customer after getting details for contact tracing

Singapore reveals Covid privacy data available to police
The constraints: Security and Privacy

- Protect health-related data
- Protect from misuse (surveillance, manipulation, etc)
  - Purpose limitation by default
  - hide users identity, location, and behavior (social graph)
The constraints: Security and Privacy

- Protect health-related data
- Protect from misuse (surveillance, manipulation, etc)
  - Purpose limitation by default
  - hide users identity, location, and behavior (social graph)

- Preserve system integrity
  - Prevent false alarms & Denial of Service
The “hidden” constraint Reality

- High scalability and reliability

- Design under time pressure!
  - Need fast, robust verification
    - KISS principle: Keep It Simple Stupid
    - Avoid new technologies or non-mainstream
  - Use existing infrastructure
    - BLE beacons

- Dependencies, dependencies, dependencies
The system design
Our first idea

- The App creates a secret key (SK) and from this key it derives random identifiers (EphIDs) that it broadcasts via Bluetooth

- Secret keys are rotated every day
  \[ SK_{t+1} = H(SK_t) \]

- EphID₁ || ... || EphIDₙ = \text{PRG(PRFT}(SK_t,\text{“broadcast key”})

- A random identifier is used for a limited amount of time

- Without the key, no-one can link two identifiers
The system design
First quicksand pond...

- The App creates a secret key (SK) and from this key it derives random identifiers (EphIDs) that it broadcasts via Bluetooth.
- Secret keys are rotated every day: $SK_{t+1} = H(SK_t)$.
- EphID_1 || ... || EphID_n = PRG(PRF(SK_t, "broadcast key")).
- A random identifier is used for a limited amount of time.
- Without the key, no-one can link two identifiers.
Battery and CPU usage
- Limited round trips
- Google and Apple **must** be involved

Run in the background
- Apple **must** be involved

Compatibility Android - iOS
- Google and Apple **must** be involved

Google and Apple implement the protocol **and the API**
- Implications on privacy engineering
- Implications for epidemiology and exposure estimation (no time in this talk…)
- Implications for privacy when internationalizing (no time in this talk…)
The system design
Platform decides
Exposure Notification

- The App creates a secret every day (TEK) and from this key it derives random identifiers (RPIs) that it broadcasts via Bluetooth.
The system design
Platform decides
Exposure Notification

- The App creates a secret every day (TEK) and from this key it derives random identifiers (RPIs) that it broadcasts via Bluetooth

- A random identifier is used for a limited amount of time

- Without the key, no-one can link two identifiers
The system design
The system design
The system design
The system design
The system design
The system design

Keys
(from all positive users)
The system design

**Keys**
(from all positive users)

**A**

**B**

**C**

**SEEN NUMBERS**

- Lyvdka (@)
  - ...
The system design

Keys
(from all positive users)

SEEN NUMBERS
... 
Iu^#&980
Kja#^@hk
...

SEEN NUMBERS
... 
Lyvdka{(0
...

SEEN NUMBERS
... 
Lyvdka{(0
...

A

B

C
The system design

You’ve been exposed to COVID-positive people. Take action
The system design

Only information that ever leaves the phone are the TEKs broadcasted during the contagious period.

No identity, no location, no information about others

No information available for abuse

System sunsets-by-design
The system design
The system design

AC, Keys

Health system

Societal impact

Law

App

Epidemiology

Mobile OS

Protocol (crypto)
The system design

AC, Keys

App

Health system

Societal impact

Law

Epidemiology

Mobile OS

Protocol (crypto)
Authorization mechanism
Our first design

- Crucial for security: only true positives can upload
  - Desired properties:
    - Privacy
    - Hard to delegate

- Crypto FTW! Commit to content in authorization token!

Authorization mechanism

- Crucial for security: only true positives can upload
  - Desired properties:
    - Privacy
    - Hard to delegate
  - Crypto FTW! Commit to content in authorization token!

- Health systems/staff are not digitalized everywhere
  - Simple activation codes sent via phone/mail/sms
  - Different level of automatization
  - Belgium went for (light) commitments!

Privacy engineering
Are we done?

AC, Keys

AC
Privacy engineering
Are we done?

Existence of upload
the user is COVID+
Privacy of uploads
Our first idea

Existence of upload
the user is COVID+

DP3T design paper

The pattern associated with the upload of identifiers to the server would reveal the COVID-19 positive status of users to network eavesdroppers (ISP or curious WiFi provider) and tech-savvy adversaries. If these adversaries can bind the observed IP address to a more stable identifier such as an ISP subscription number, then they can de-anonymize the confirmed positive cases. This can be mitigated by using dummy uploads.

Privacy of uploads
Practice

- Unknown environment
  - What is users’ behavior?

Privacy of uploads
Practice

- Unknown environment
  - What is users’ behavior?

- Constraints associated to the platform
  - Bandwidth
  - Server capacity
  - Battery

Privacy of uploads
Practice

- Unknown environment
  - What is users’ behavior?

- Constraints associated to the platform
  - Bandwidth
  - Server capacity
  - Battery

- Anonymity and delays not possible

Privacy of uploads
Practice

- Unknown environment
  - What is users’ behavior?

- Constraints associated to the platform
  - Bandwidth
  - Server capacity
  - Battery

- Anonymity and delays not possible

Plausible deniability
(constant time & size)

Privacy of uploads
Practice – there is authentication!
Privacy of uploads
Practice – there is authentication!

Privacy of uploads
Practice – there is authentication!

- Dummies also must realize the authentication step
  - Servers must consider dummies
  - Ensure equal timing and volume

Exposure Notification API (<v1.5) had one security mechanism:
- Only reveal key after it expires
- (Not needed, it is an implementation decision)

Implications on authorization and dummy strategy
- Cannot delay all keys!
Privacy of uploads
Practice –

- Exposure Notification API (<v1.5) had one security mechanism:
  - Only reveal key after it expires
  - (Not needed, it is an implementation decision)

- Implications on authorization and dummy strategy
  - Cannot delay all keys!
  - Dummies must mimic second upload
Privacy of uploads
Practice – servers don’t exist in the vacuum
Privacy of uploads
Practice – servers don’t exist in the vacuum

Privacy of uploads
Practice – servers don’t exist in the vacuum

Privacy of uploads
Practice – servers don’t exist in the vacuum

- Load Balancer, Firewall
  - More information than expected!
  - Off the shelf cloud managing tools

- Careful design of logging to avoid forensics
  - Coarse logging at key server
  - Only counts logged for statistics
    - e.g, active users based on dummy traffic

- Logging strategy re-designed N times

Where is this deployed?

1.87 Million active users (~22% population)

~18000 COVID-positive users uploaded their keys in December (15% of PCR in Switzerland)

Field experiment in Zurich October 2020

- 80% COVID-positive app users upload their codes
- 22% sent quarantine
- 1 in 10 tested positive after notification
- 5% of positives with respect to Manual Contact Tracing in Zurich
- Speed: ~1 day faster notification for non-household exposures (70% of the cases)
Key lessons

- Data is not a must!

- Privacy engineering goes well beyond crypto

- Privacy engineering in an agile/service world is exhausting
  - Platforms and requirements continuously change

- Good socio-technical integration is key to success and it is **hard**
  - Purpose limitation and abuse prevention is a must