CISPA
HELMHOLTZ CENTER FOR INFORMATION SECURITY

DP3T: Deploying decentralized, privacy-preserving contact tracing

Wouter Lueks | March 29, 2023

Some slides adapted from Carmela Troncoso

A collaborative (marathon-length) sprint

Maintenance and support

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 2020 to summer 2021 – **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

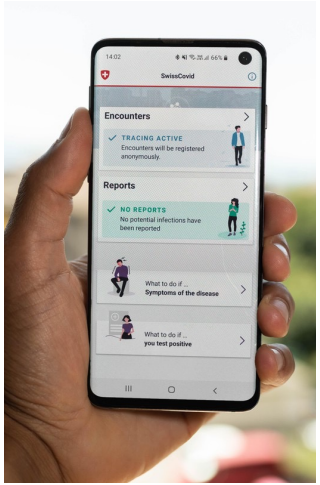
INESC TEC: Prof. Manuel Barbosa (FCUP), Prof. Rui Oliveira (UMinho), Prof. José Pereira (UMinho)

https://github.com/DP-3T/documents

The “hidden” constraint
Reality

- **Millions of users:** need scalability and reliability

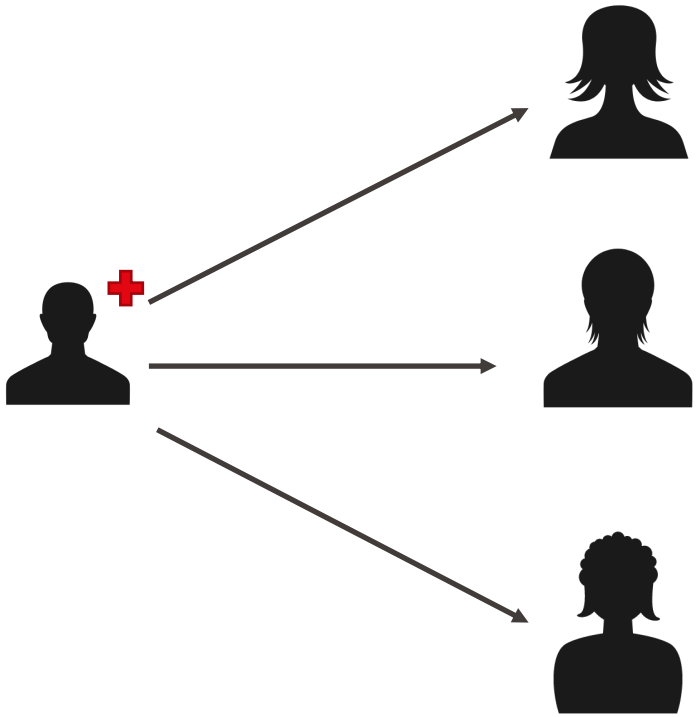
- **Deploy within weeks/months:** Design under time pressure!
  - Need fast, robust verification
  - KISS principle: Keep It Simple Stupid
  - Avoid new technologies or non-mainstream



- Use **existing infrastructure & hardware**

Wouter Lueks

Digital Contact Tracing



Contact:
close enough &
long enough

Digital Contact Tracing: **notify** people that were close enough and long enough to a contagious individual

Design Principle: purpose limitation by default, ensure system can be used **only** for notifications

Risks of Digital Contact Tracing

System must embed social contact information!

- **Privacy Risks**
  - **Leak location traces** (who was where when) of positive and non-positive individuals
  - **Reveal medical information** (positive individuals, exposures)
  - **Leak social interactions** between individuals
- **Social Risks**
  - **Control** who gets notified, and thus quarantines and who not

Europe

German police used a tracing app to scout crime witnesses. Some fear that's fuel for covid conspiracists.

By Rachel Pannett

January 13, 2022 | Updated January 13, 2022 at 8:19 a.m. EST

The New York Times

The Coronavirus Pandemic › | Covid-19 Updates | Coronavirus Map a

Living by the Code: In China, Covid-Era Controls May Outlast the Virus

The country has instituted a wide range of high-tech controls on society as part of a mostly successful effort to stop the virus. The consequences may endure.

Sensitive business addresses among 500,000 published in COVID data breach

By **Jonathan Kearsley** and **Clair Weaver**

February 14, 2022 — 7.00pm

"including **defence sites**, a **missile maintenance unit** and **domestic violence shelters**"

NEWS WEBSITE OF THE YEAR
The Telegraph

Coronavirus News Politics Business Sport World Money Opinion Life Style Travel Cu

Family Women Columnists Men Cookbook Food & Drink Health & Fitness Education & Careers Tel M

Test and trace is being used to harass women - already

There's a deeply troubling phenomenon emerging out of handing over data in restaurants and pubs

By Marisa Bate

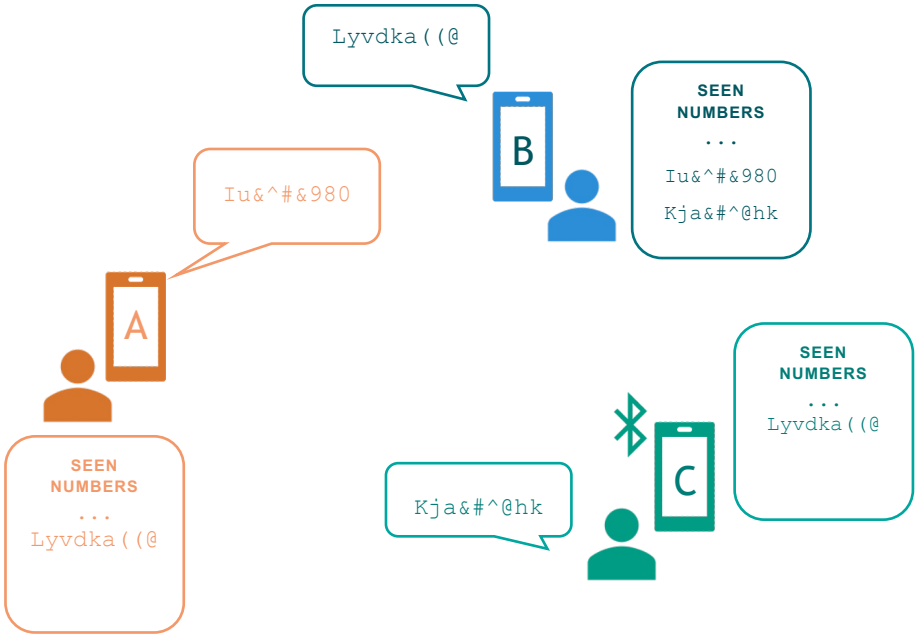
15 July 2020 • 3:32pm

Theresa Stadler, Wouter Lueks, Katharina Kohls, Carmela Troncoso: Preliminary Analysis of Potential Harms in the Luca Tracing System. CoRR abs/2103.11958 (2021)


Infrastructure Matters
(when you build a road, people will use it,
... and use it in ways you didn't expect)
Photo by Johannes Plenio on Unsplash


Purpose Limitation by Design
ensure your system can be used only for the
purpose that you initially defined
Infrastructure Matters
(when you build a road, people will use it,
... and use it in ways you didn't expect)
Photo by Johannes Plenio on Unsplash

Decentralized Architecture
Walking around

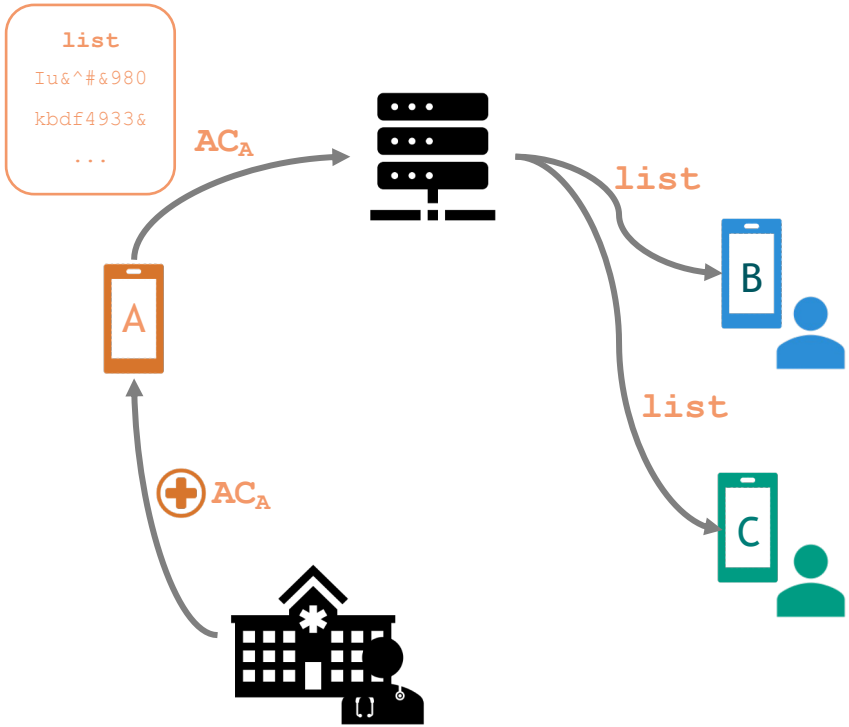


When a device hears a random identifier from a nearby device, it records having seen that number.

- **A** is nearby **B**: records **B**'s number
- **B** is nearby **A** and **C**: records **A**,**C**'s number
- **C** is nearby **B**: records **B**'s number

Beacons **rotate** every ~10 minutes to prevent tracking

Decentralized Architecture
Exposure notification



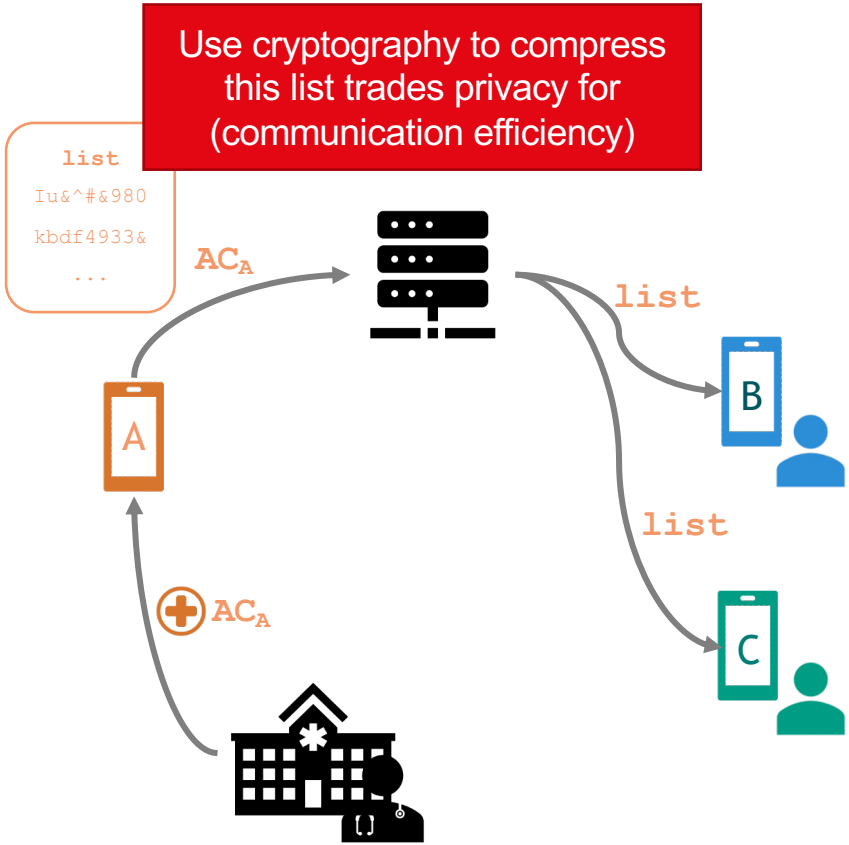
A user with a **positive diagnosis**:

- Uploads their own list

Other devices:

- Download uploaded lists with **positive** identifiers
- And use these to compute their user's **exposure**
- **Notify** user if exposure high enough

Decentralized Architecture
Exposure notification



A user with a **positive diagnosis**:

- Uploads their own list

Other devices:

- Download uploaded lists with **positive** identifiers
- And use these to compute their user's **exposure**
- **Notify** user if exposure high enough

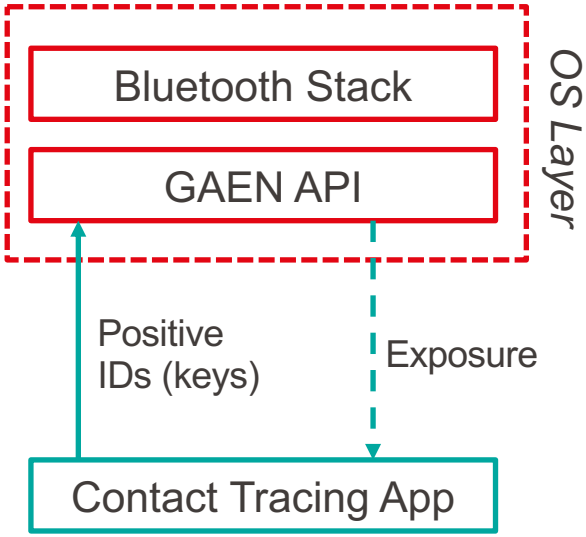
Integrating with Hardware
Phones + Bluetooth Low Energy

- Battery and CPU usage
  - Broadcast only: no connections
  - Therefore: limited payload (<20 bytes)
  - Cannot measure often
  - **OS Level**: Google and Apple must be involved
- Run in the background
  - **OS Level:** Apple must be involved
- Compatibility Android - iOS
  - **OS Level:** Google and Apple must be involved
- Preventing Tracking
  - Must rotate BLE beacon and BT MAC simultaneously
  - **OS Level:** Google and Apple must be involved

Blagovesta Kostova, Seda Gürses, Carmela Troncoso. Privacy Engineering Meets Software Engineering. On the Challenges of Engineering Privacy By Design

Google/Apple Exposure Notification (GAEN) Framework
Integrating with Mobile Platforms

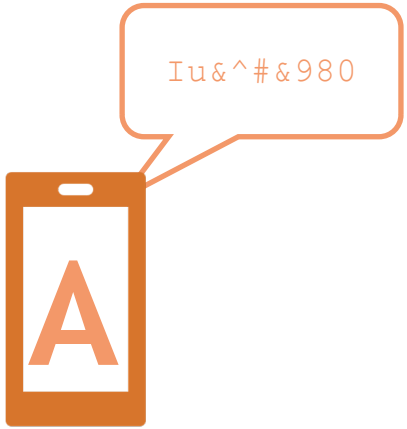
- The Google and Apple Exposure Notification API (GAEN) exposed OS level features
- But with **high level** interface only
- Google and Apple **choose security and privacy trade-offs**:
  - Yes, it made deploying (risky) centralized apps virtually impossible
  - But it also **limited** deploying more privacy-friendly designs and prevented other **design points**
- And API license terms ensure, e.g.,
  - That location data cannot be used in the app
  - That there can be only one app per state/nation
- On other words, the **deployment context gave power to** mobile OS manufacturers



James R. Larus. Whose smartphone is it? Communications of the ACM. 2021

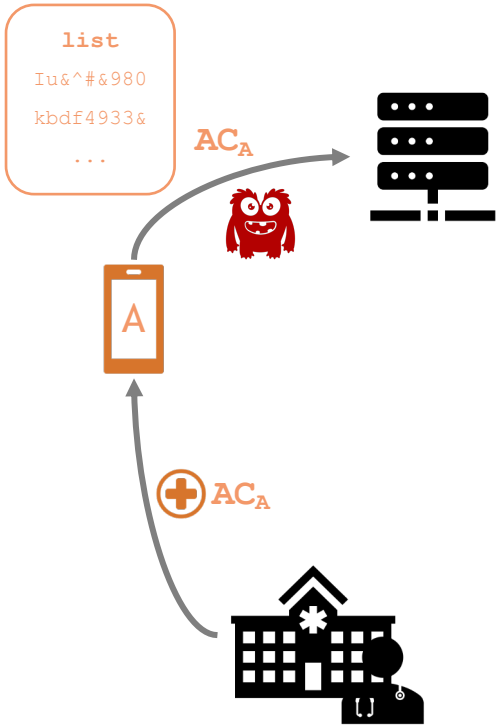
Privacy at all Layers
BT Protocol stack

- We must ensure privacy by **considering all layers** simultaneously
- Phones **transmit BLE beacons** that rotate frequently
- But they do so using the BLE stack: hence, **BT MAC address** is also **visible**
- To prevent tracking using BLE beacons: phones must **rotate both simultaneously**
- **Requires OS-level changes** (and not supported by older phones / stacks)



Privacy at all Layers
Network Layer

- Uploads by phones are very easy to detect by **network adversaries,** and **reveal that somebody has COVID-19**
- (Despite all protocol-level protections)
- Solution: app makes random **dummy uploads** (that look exactly like real uploas) to provide **plausible deniability**
- Deployed this in CH, but details are tricky
- And requires operating system to give app **background processing**



Conclusions
Lessons Learned

- **Purpose Limitation:** Technology brings risks, need to design using **purpose limitation** to ensure protection
- **Context matters:** how and where you deploy technology influences what you can achieve:
  - Contact Tracing Apps required OS level changes by Google and Apple
  - And thus gave them the **power to control** what could and could not be done
- **Privacy must be maintained at all layers:** protocol layer only is not enough, e.g.
  - Interaction between BT beacons and MACs
  - Unobservability at network layer when uploading

Carmela Troncoso, Dan Bogdanov, Edouard Bugnion, Sylvain Chatel, Cas Cremers, Seda F. Gürses, et al.: Deploying decentralized, privacy-preserving proximity tracing. Commun. ACM 65(9): 48-57 (2022)