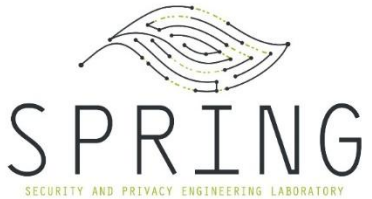


Computer Security and Privacy (COM-301)

Security principles

Interactive exercises I

Carmela Troncoso

SPRING Lab

carmela.troncoso@epfl.ch

Securing Dragons

Dany and Jorah decide to hide a dragon egg inside a crypt. The crypt has two locks and can be opened only if both locks get unlocked. Dany has the key to one lock and Jorah has the key to the other.

What security principle did Dany and Jorah follow to decide on this mechanism?

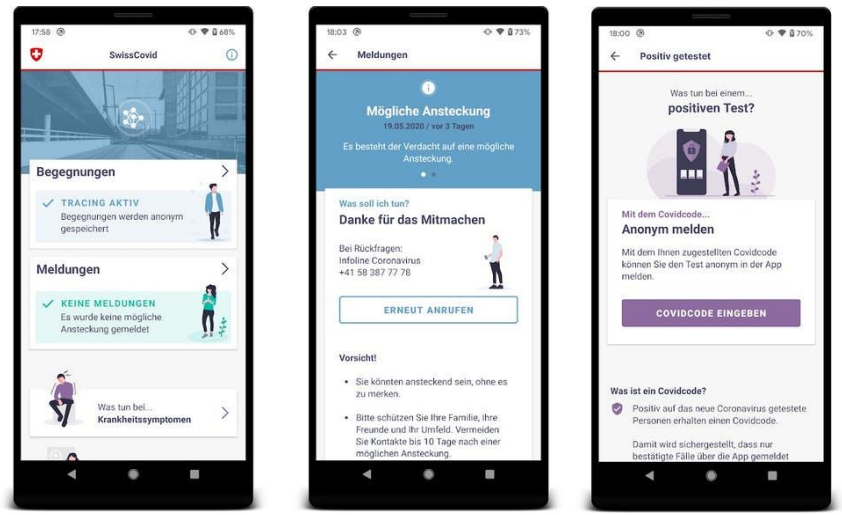
(a) Open design.

(b) Least privilege.

(c) Complete mediation.

(d) Separation of privilege.

The protocol behind SwissCovid

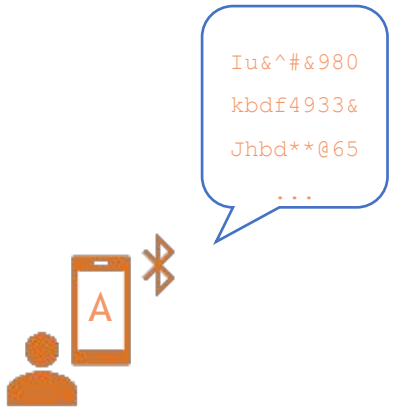


Digital Proximity Tracing

Goals

- Notify users that they have been in contact with a COVID+ user.
- Cover more people than those COVID+ patients can remember
- Notify them faster than the manual system could do
- Increase the scalability of manual notifications

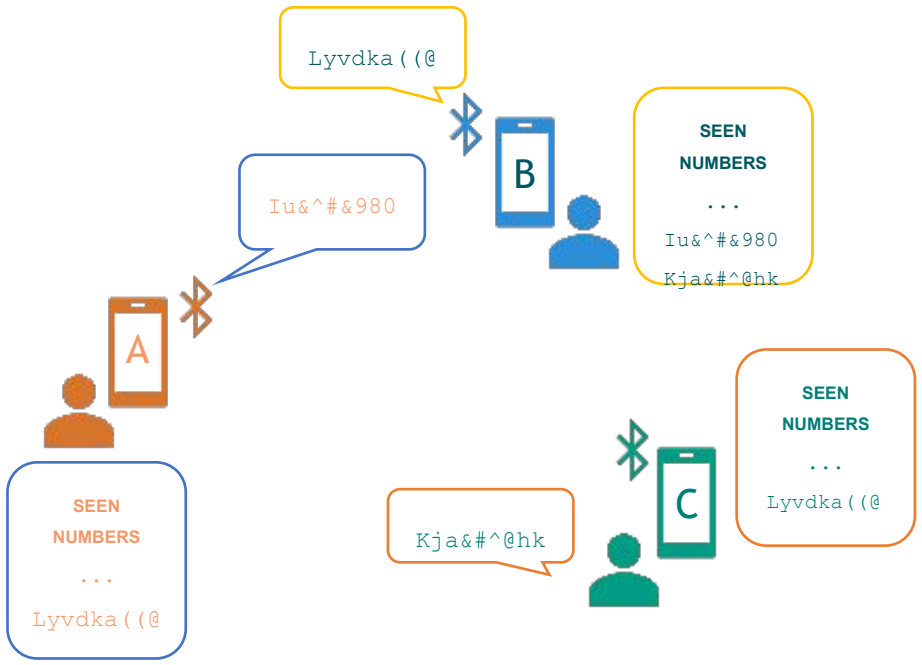
How it works
Installation



- **The App creates** a secret every day and from this key it derives **random identifiers** 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

How it works

Walking around

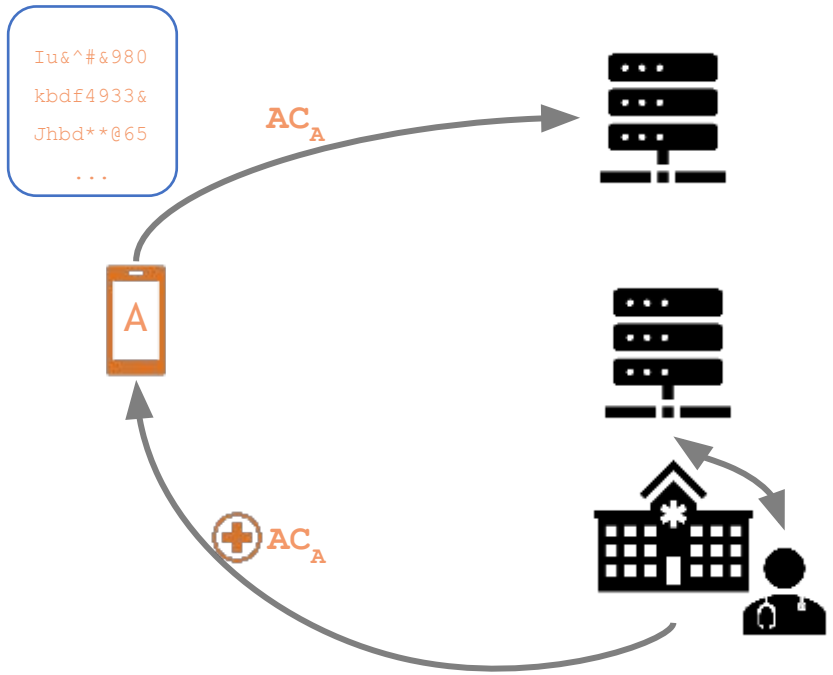


When a phone with the app hears a random identifier from a nearby app, it records having seen that number.

- **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

How it works

Upon diagnosis



When a user is diagnosed positive, if they consent, they upload their keys (their numbers)

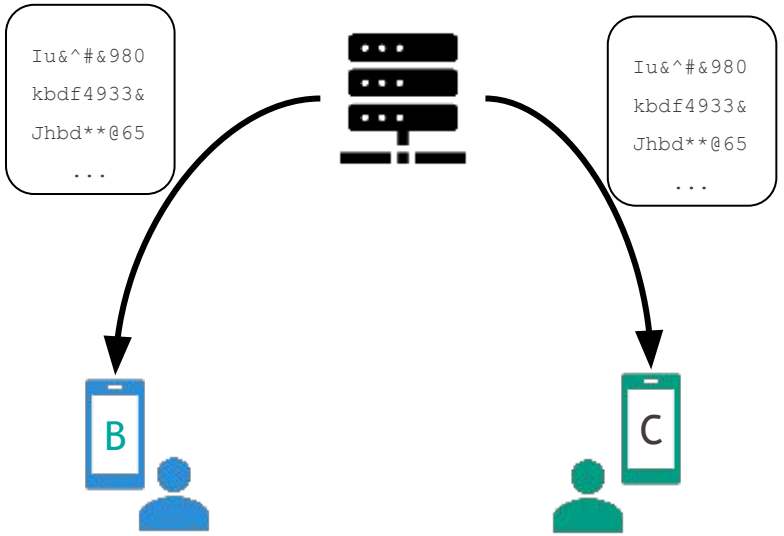
These numbers…

- Are not related to **A**'s identity
- Are not related to the locations **A** visited
- Are not related to other people **A** has interacted with or has seen

To upload their numbers, needs an authorization code. This code is requested by the doctor from an authorization server and given to the patient outside of the application

How it works

Proximity tracing



All phones download latest COVID-positive numbers and check whether they have been exposed

Each phone checks **internally**…

- Whether they have seen any of the numbers
- Whether the exposure to these numbers has been long and close enough
- If yes, show a notification for the user

More information

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

Code and documentation: https://github.com/SwissCovid/swisscovid-doc

Which principles does SwissCovid follow? How?

Principles: Cheat Sheet

1. Economy of mechanism
2. Fail-safe defaults
3. Complete mediation
4. Open Design
5. Separation of Privilege
6. Least Privilege
7. Least Common Mechanism
8. Psychological Acceptability

2 extra principles
+ Work Factor
+ Compromise Recording

Which principles does SwissCovid follow?
Economy of mechanism

Which principles does SwissCovid follow?
Fail-safe default

Which principles does SwissCovid follow?
Complete mediation

Which principles does SwissCovid follow?
Open design

Which principles does SwissCovid follow?
Separation of privilege

Which principles does SwissCovid follow?
Least privilege

Which principles does SwissCovid follow?
Least common mechanism

Which principles does SwissCovid follow?
Psychological acceptability

Twitter blames 'coordinated' attack on its systems for hack of Joe Biden, Barack Obama, Bill Gates and others

By Rishi Iyengar, CNN Business
Updated 2238 GMT (0638 HKT) July 16, 2020

On July 15, hackers took over about 130 high-profile accounts, including those of former president Barack Obama, Democratic presidential candidate Joe Biden and Tesla CEO Elon Musk. Hackers then tweeted a fake bitcoin deal from some of those accounts, reaping more than 400 bitcoin transfers worth in excess of $100,000, the Hillsborough state attorney's office said.

Twitter blames 'coordinated' attack on its systems for hack of Joe Biden, Barack Obama, Bill Gates and others

Twitter said on Thursday the hackers used a phone "spear-phishing" attack to target Twitter employees. After stealing employee credentials and getting into Twitter's systems, the hackers were able to target other employees who had access to account support tools, the company said.

Office. "The public was confused, and everyone wanted answers. We can now start answering those questions thanks to the work of IRS-CI cyber-crime experts and our law enforcement partners. Washington DC Field Office Cyber Crimes Unit analyzed the blockchain and de-anonymized bitcoin transactions allowing for the identification of two different hackers. This case serves as a great example of how following the money, international collaboration, and public-private partnerships can work to successfully take down a perceived anonymous criminal enterprise. Regardless of the illicit scheme, and whether the proceeds are virtual or tangible, IRS-CI will continue to follow the money and unravel complex financial transactions."

https://www.justice.gov/usao-ndca/pr/three-individuals-charged-alleged-roles-twitter-hack

Questions

- What could have Twitter done to avoid this problem?
- What principles were not followed and enabled the big problem?
- Training to recognize phishing is a good idea. Are mock phishing trainings a good way to achieve this?

Phishing in Organizations: Findings from a Large-Scale and Long-Term Study

https://arxiv.org/pdf/2112.07498.pdf