Computer Security and Privacy (COM-301)

Security principles

Interactive exercises I

Carmela Troncoso
SPRING Lab
carmela.troncoso@epfl.ch

Securing Dragons

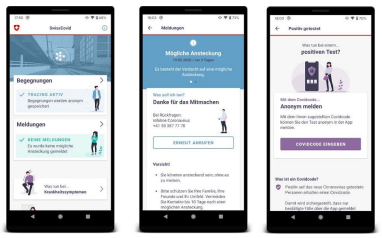
Dany and Jorah decide to hide a dragon egg inside a crypt. The crypt has two locks and can be opened only if both locks get unlocked. Dany has the key to one lock and Jorah has the key to the other.

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.

(a) Open design is orthogonal to how the mechanism is build
(b) there is no least privilege, as once you open the crypt you can do anything with the egg
(c) There is no complete mediation as only access is checked, after any egg-security operation is not validated
(d) Separation of privilege: neither Dany nor Jorah, on their own, can breach the security policy.

The protocol behind SwissCovid



Digital Proximity Tracing

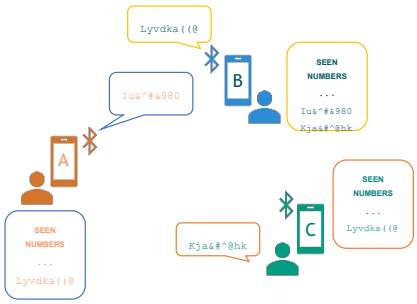
Goals

- 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

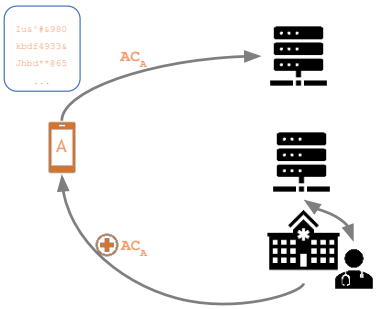
How it works
Walking around



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



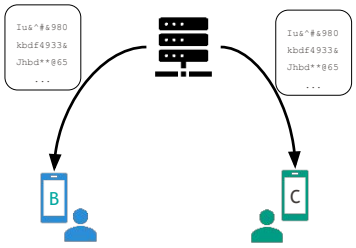
When a user is diagnosed positive, if they consent, they upload their keys (their numbers)

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

The protocol used in SwissCovid is very simple: there is no complex or new cryptography, and there is no complex composition of mechanisms

While this implies that some attacks are still possible (https://github.com/DP-3T/documents/blob/master/Security%20analysis/Privacy%20and%20Security%20Attacks%20on%20Digital%20Proximity%20Tracing%20Systems.pdf), given the speed at which the app had to be developed the design favours easy verification, as the attacks remaining have quite high cost.

Which principles does SwissCovid follow?
Fail-safe default

One of the core designs principle for the app was fail-safe for privacy. If there is any error or any information leaks, the privacy of the users is always protected.

On the authorization side it also follows the principle. If any error occur, no information can be uploaded.

Which principles does SwissCovid follow?
Complete mediation

Most security-critical operations have a check: there is a verification code to upload the keys to the server, and the Google/Apple Exposure Notification framework in the mobile OS checks that the app has permission to access the information. However, not every action in the phone is checked (ambient authority).

Which principles does SwissCovid follow?
Open design

Design and implementation are open (links in slide 10)

Which principles does SwissCovid follow? Separation of privilege

The separation of privilege principle is behind the decision that checks are done locally. This means that, with only one device, or only the server, one can learn nothing about the users.

Which principles does SwissCovid follow?
Least privilege

The design is thought with data minimization as a main goal. As explained in the lecture, data minimization is a direct implementation of the least privilege principle: devices in the system only learn the exact amount of information needed to achieve their purpose. With the information they have, they cannot do any other operation than the ones expected.

Which principles does SwissCovid follow?
Least common mechanism

16

From the point of view of privacy, the system is decentralized, which means that phones do not rely on anything else to keep privacy, there is no privacy-related mechanism common to users.

On the other hand, the system relies on a central server for availability. While this decision creates an availability single point of failure, it was needed to be able to deploy the system in such a small amount of time (https://arxiv.org/abs/1704.08065 for more info on trade-offs and why centralized components exist in deployed decentralized system)

Which principles does SwissCovid follow? Psychological acceptability

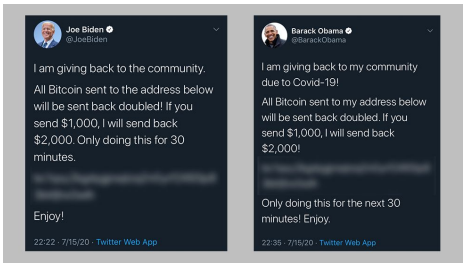
Intuition versus understanding: People understand the idea yet they still do not understand the mechanism and many believe the system traces them.
The counterintuitive properties of the system, one can do contact tracing without tracing, makes it hard to believe for users. This is a common problem with modern privacy enhancing technologies.

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

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

[Remember these are possible answers]

What could have Twitter done?

- Separation of privilege: have more than one employee needed to perform an action in the "master tool"
- Least privilege*:* have less privileges on the master tool. For instance, give employees accessing the tool capability to only change a number of accounts
- Least common mechanism: Have different master tools for different subsets of users

Of course, taking these actions would come at a price. For example, in all three actions reaction to a bad event would take more time (you need two people, you need to find the correct employee that can change the account under attack).

What principles were not followed?
See above

Are mock phishing trainings a good way to achieve this?
This is arguable.

According to the paper we linked to, no, mock phishing is not a good idea. It leads to employees wasting too much time on trying to recognize scams (time they are not working) and at the end of the day this does not eliminate clicking on phishing. Another interesting finding: the commonly used mock-phishing gives employee false impression of “I am well-trained and will not fall into the phishing email” and it actually **increases** the successful rate of phishing attacks, compared to no training.