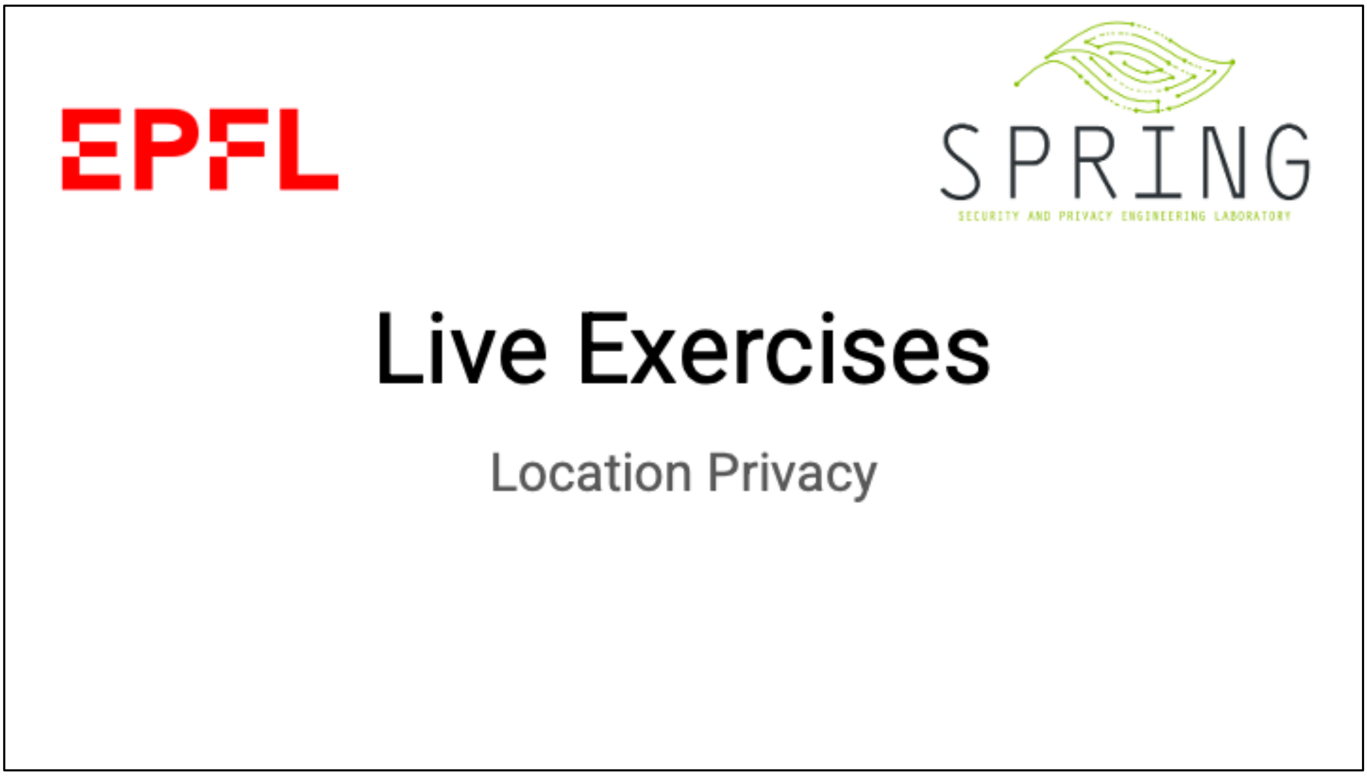


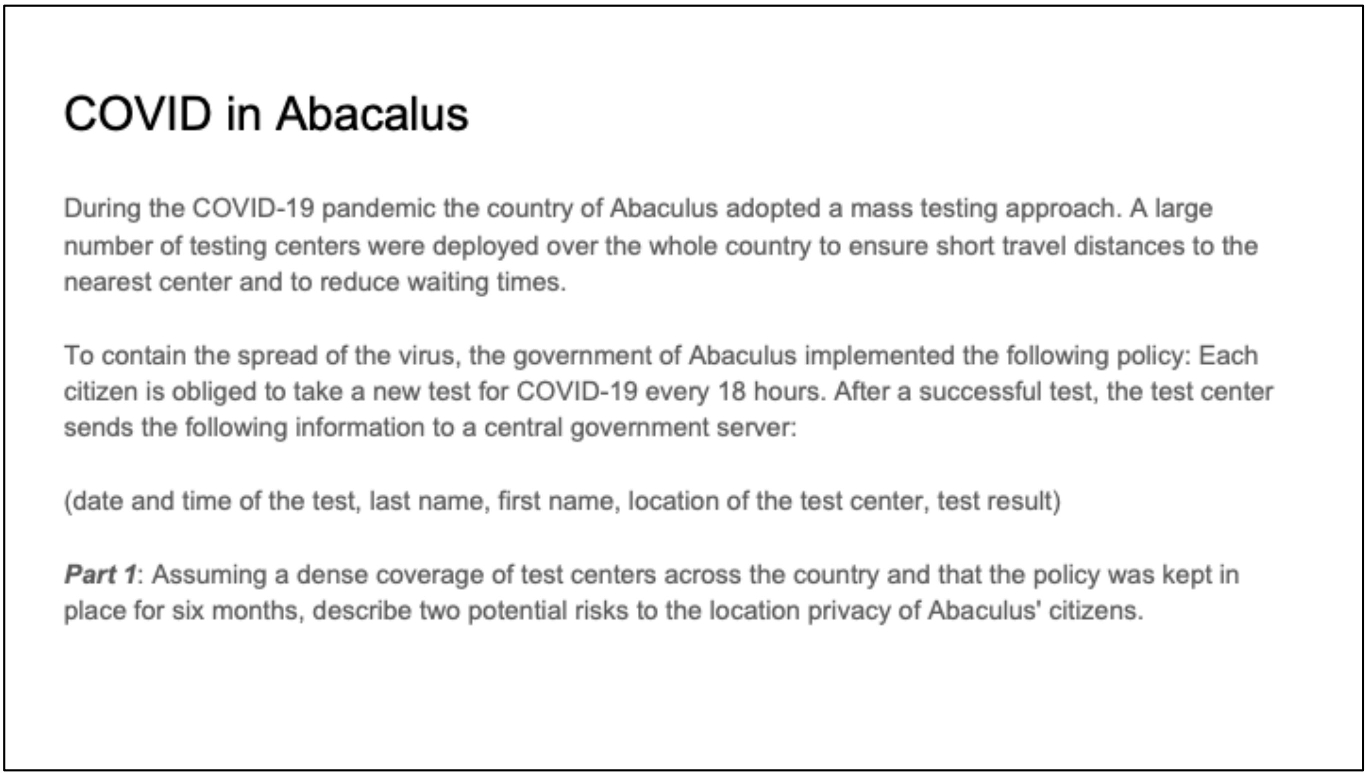
EPFL

SPRING

SECURITY AND PRIVACY ENGINEERING LABORATORY

Live Exercises

Location Privacy



COVID in Abacalus

During the COVID-19 pandemic the country of Abaculus adopted a mass testing approach. A large number of testing centers were deployed over the whole country to ensure short travel distances to the nearest center and to reduce waiting times.

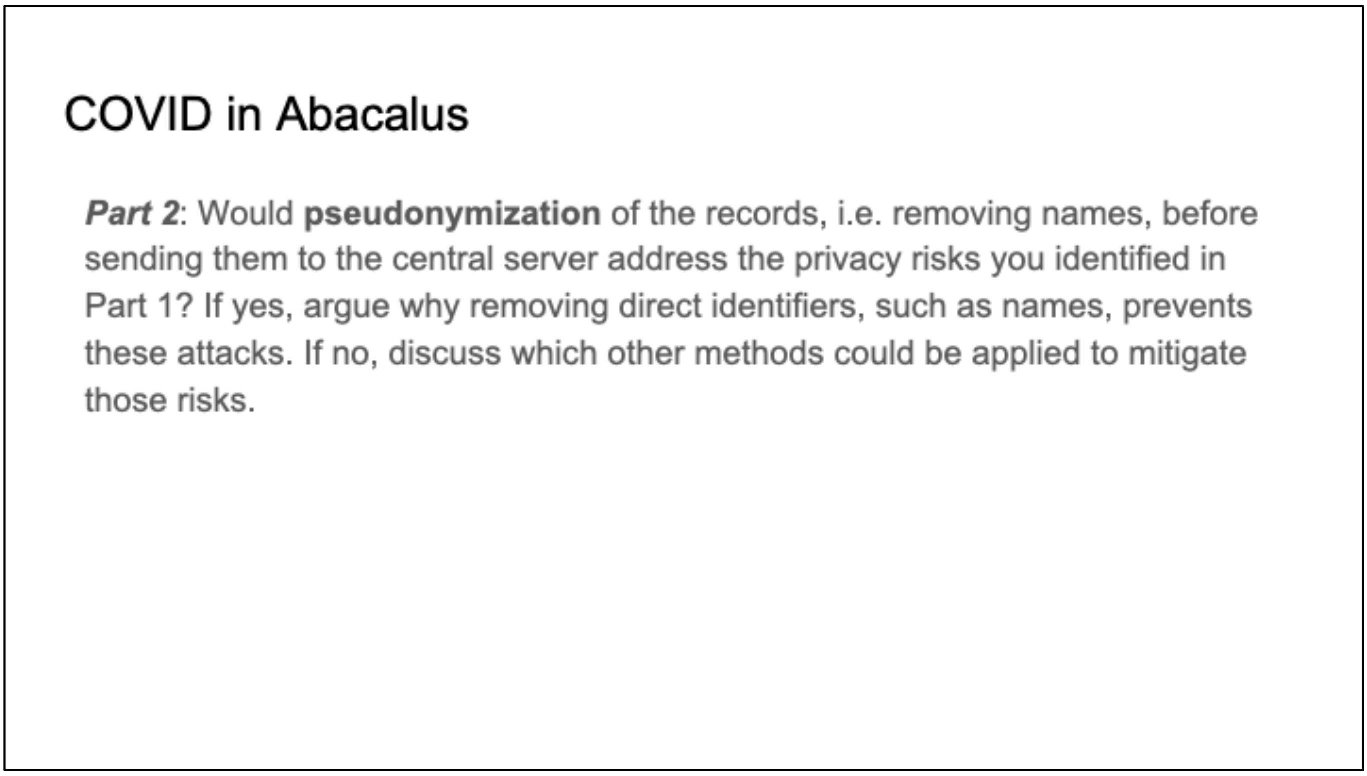
To contain the spread of the virus, the government of Abaculus implemented the following policy: Each citizen is obliged to take a new test for COVID-19 every 18 hours. After a successful test, the test center sends the following information to a central government server:

(date and time of the test, last name, first name, location of the test center, test result)

Part 1: Assuming a dense coverage of test centers across the country and that the policy was kept in place for six months, describe two potential risks to the location privacy of Abaculus' citizens.

Example threat: It is likely that most people will always select the test center closest to either their work or to their home location. The dense coverage implies that this should allow the government, or anyone who obtains access to the data stored at the gov server think about law enforcement) to obtain a good guess about where people live and work.

Note: The government also learns who test positives. However, this is not a threat to citizen's location privacy and the intended function of the system.

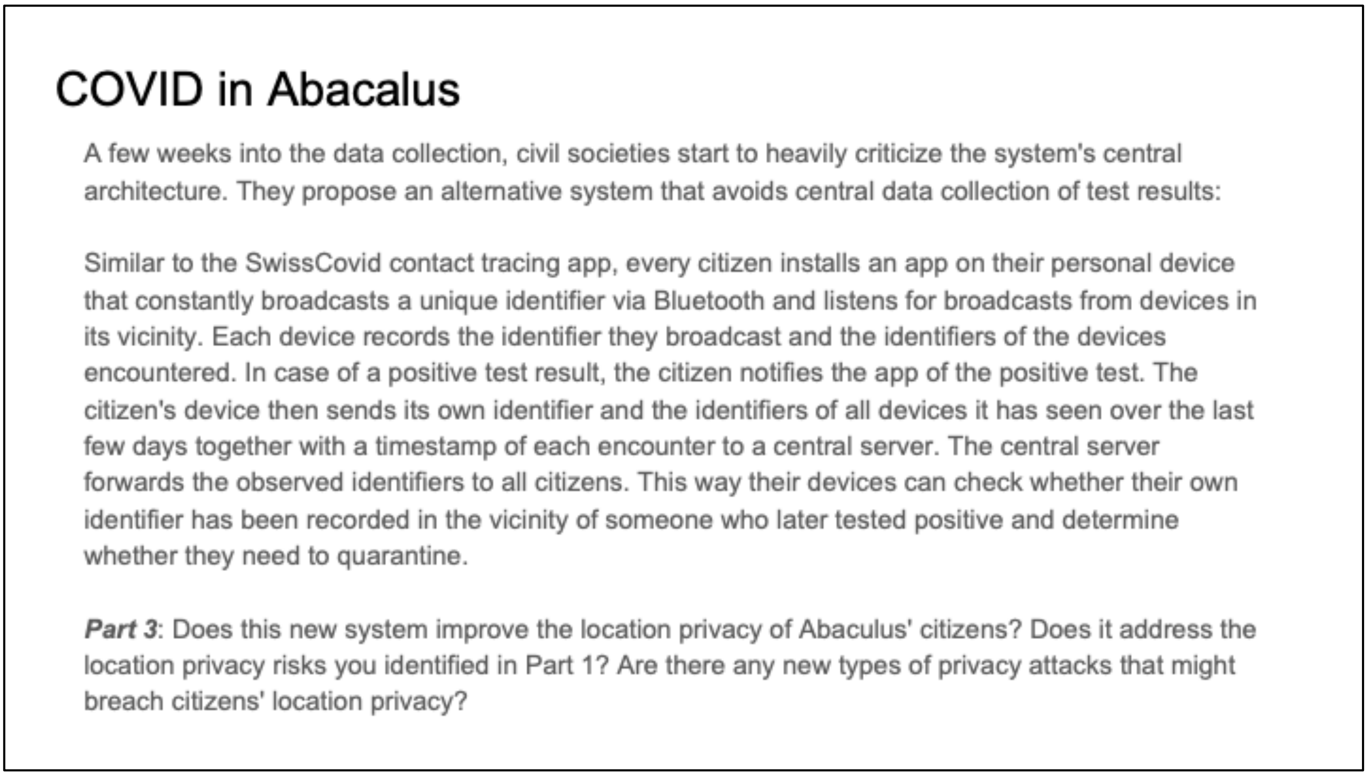


COVID in Abacalus

Part 2: Would **pseudonymization** of the records, i.e. removing names, before sending them to the central server address the privacy risks you identified in Part 1? If yes, argue why removing direct identifiers, such as names, prevents these attacks. If no, discuss which other methods could be applied to mitigate those risks.

Pseudonymisation does not address the risk of an adversary that infers the home and work location of an individual. As these two locations can act as an identifier, it would still allow the adversary to link this information back to some auxiliary information and de-anonymise the data.

A better solution would be spatial obfuscation, generalization, cloaking. (Discuss details of how these techniques apply to the concrete scenario)



COVID in Abacalus

A few weeks into the data collection, civil societies start to heavily criticize the system's central architecture. They propose an alternative system that avoids central data collection of test results:

Similar to the SwissCovid contact tracing app, every citizen installs an app on their personal device that constantly broadcasts a unique identifier via Bluetooth and listens for broadcasts from devices in its vicinity. Each device records the identifier they broadcast and the identifiers of the devices encountered. In case of a positive test result, the citizen notifies the app of the positive test. The citizen's device then sends its own identifier and the identifiers of all devices it has seen over the last few days together with a timestamp of each encounter to a central server. The central server forwards the observed identifiers to all citizens. This way their devices can check whether their own identifier has been recorded in the vicinity of someone who later tested positive and determine whether they need to quarantine.

Part 3: Does this new system improve the location privacy of Abaculus' citizens? Does it address the location privacy risks you identified in Part 1? Are there any new types of privacy attacks that might breach citizens' location privacy?

Compared to location privacy risks in part 1, without any additional information, the central adversary cannot learn home/work locations of individuals.

Still some risks:

View from central server: The central server sees timestamped, pseudonymous identifiers observed by a single device. The observation times can be used to infer co-location of devices: If device A and device B both have seen device C at the same time and later test positive, the central server can infer that devices A, B and C all met at a specific time.

View from a local adversary with the infrastructure to record BT in POIs: The adversary can track which device visited specific POIs and when. As the data is linkable this might allow adversary to re-identify the device owner (home and work location can be identifiers). This would then allow to track device over time.