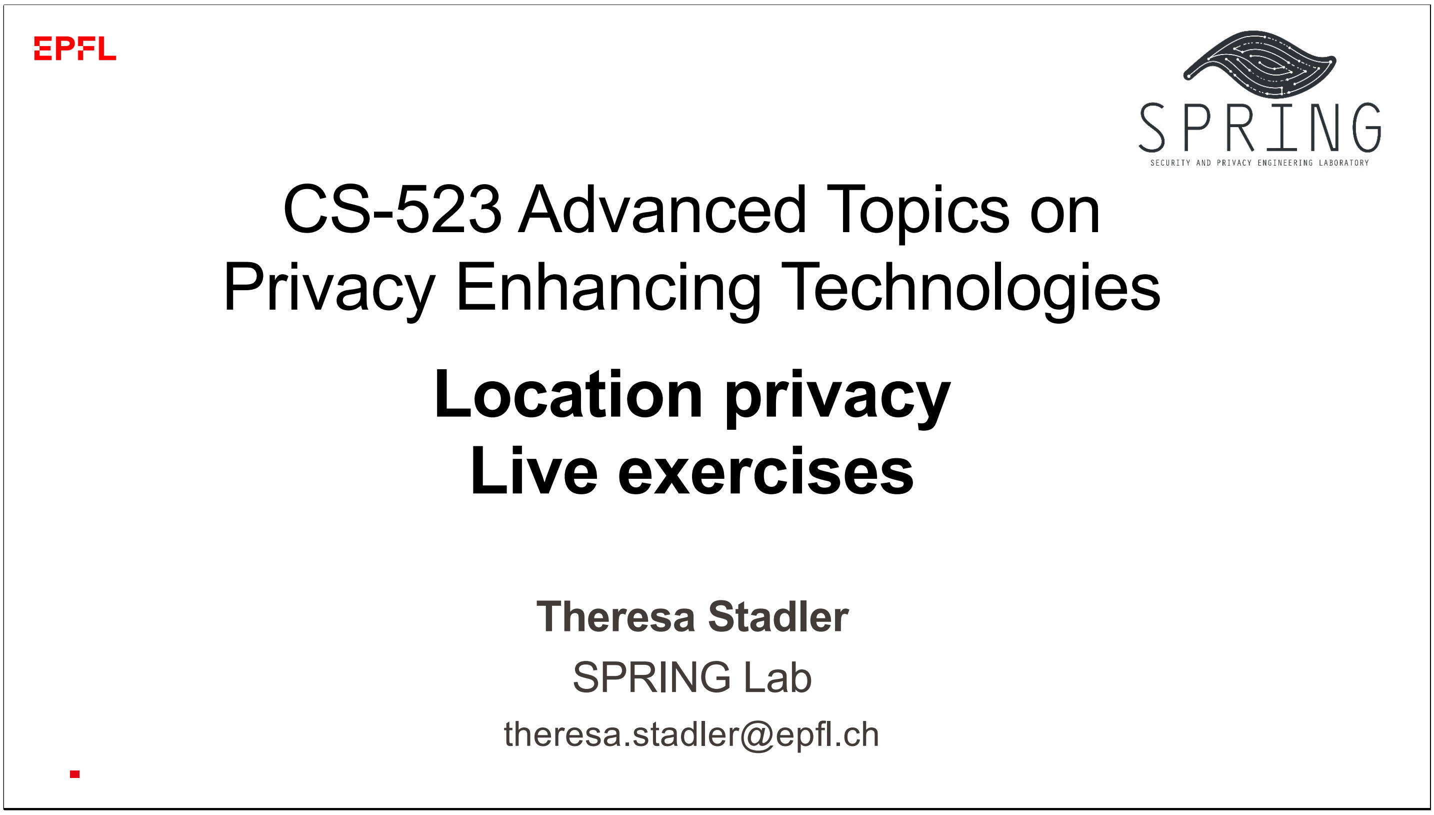


CS-523 Advanced Topics on Privacy Enhancing Technologies

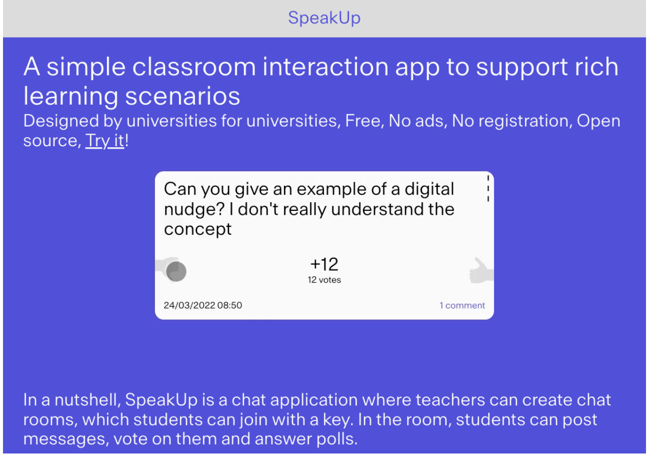
Location privacy
Live exercises

Theresa Stadler

SPRING Lab

theresa.stadler@epfl.ch

SpeakUp



SpeakUp

A simple classroom interaction app to support rich learning scenarios

Designed by universities for universities, Free, No ads, No registration, Open source, Try it!

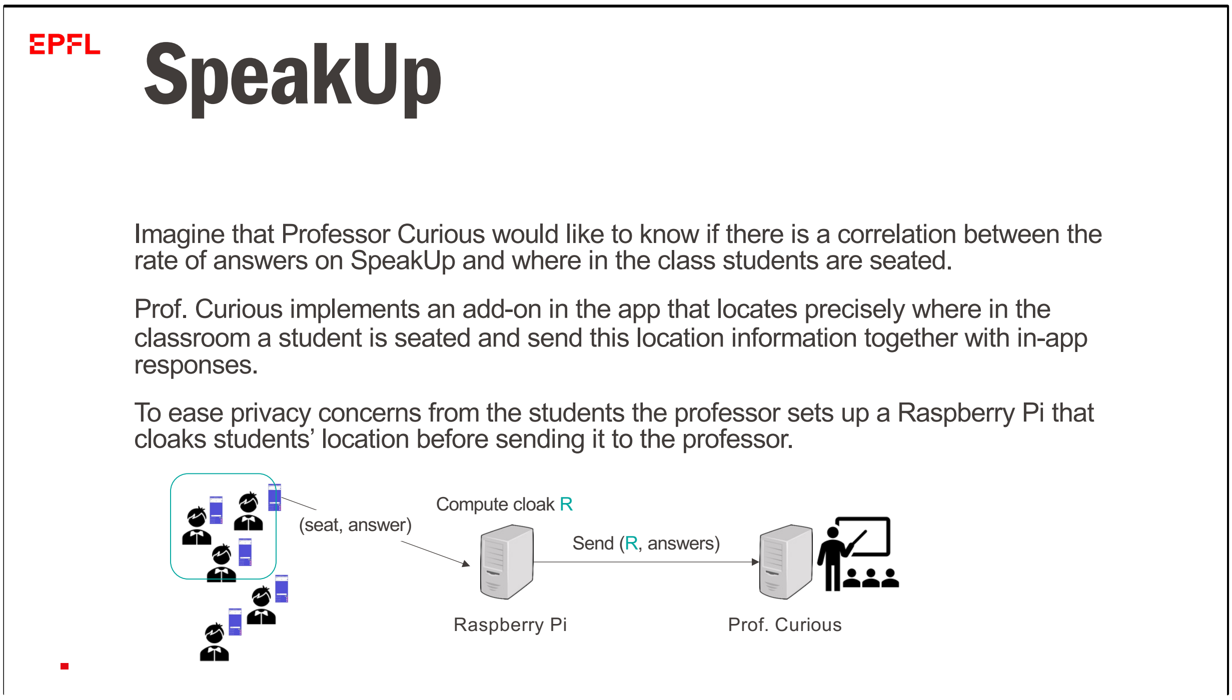
Can you give an example of a digital nudge? I don't really understand the concept

+12

12 votes

24/03/2022 08:50

In a nutshell, SpeakUp is a chat application where teachers can create chat rooms, which students can join with a key. In the room, students can post messages, vote on them and answer polls.



SpeakUp

Imagine that Professor Curious would like to know if there is a correlation between the rate of answers on SpeakUp and where in the class students are seated.

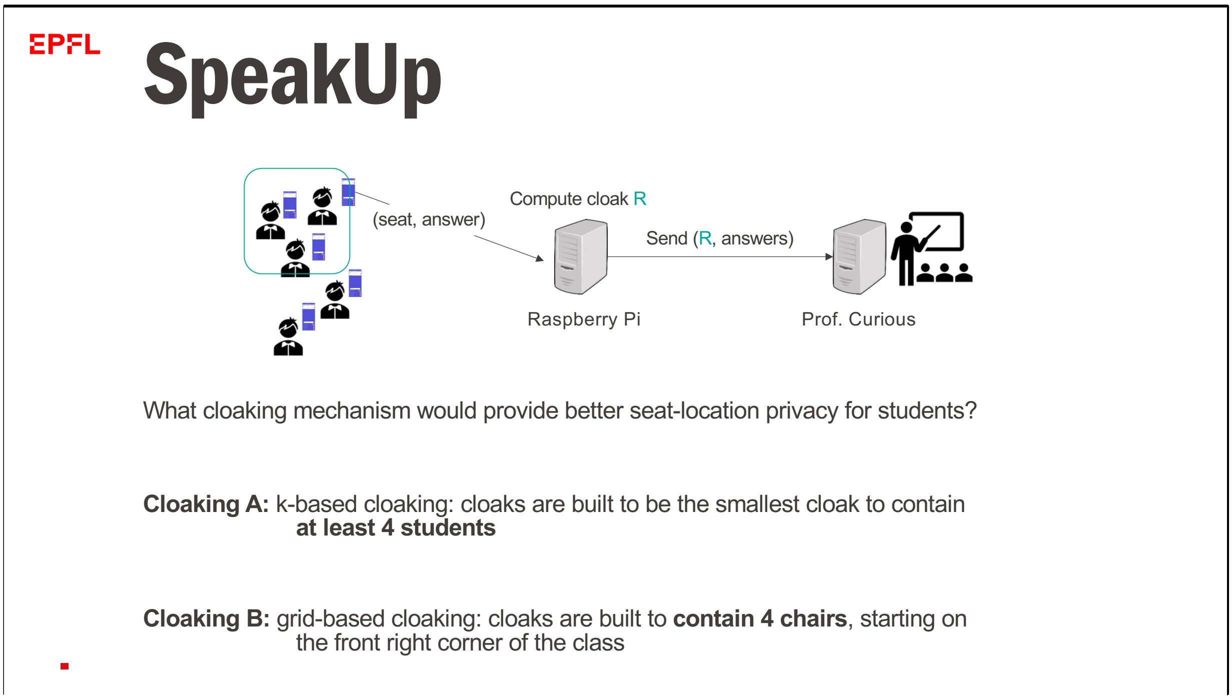
Prof. Curious implements an add-on in the app that locates precisely where in the classroom a student is seated and send this location information together with in-app responses.

To ease privacy concerns from the students the professor sets up a Raspberry Pi that cloaks students' location before sending it to the professor.

Depends on assumptions of class fullness

If the class is not full A provides worst location privacy than B, because A reveals exactly where students are located (the 4 corners of the cloak)

If the class is full, then A and B would provide the same privacy, both cloaking schemes would reveal the exact location of students.

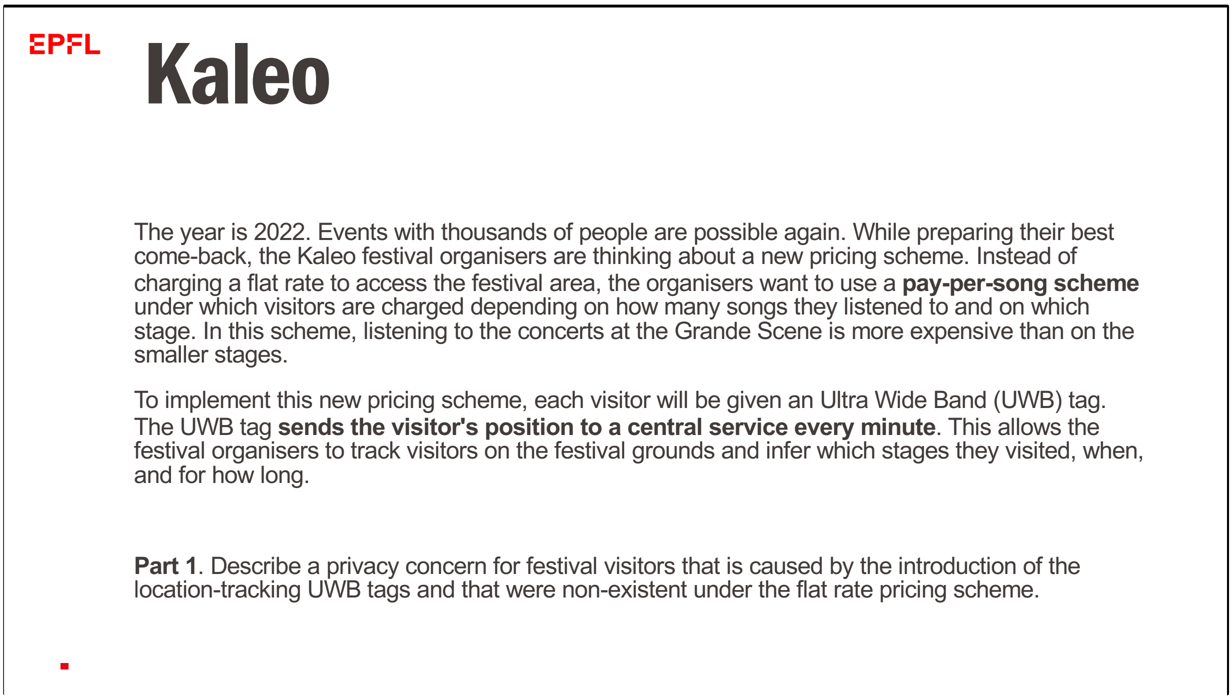


SpeakUp

What cloaking mechanism would provide better seat-location privacy for students?

Cloaking A: k-based cloaking: cloaks are built to be the smallest cloak to contain **at least 4 students**

Cloaking B: grid-based cloaking: cloaks are built to **contain 4 chairs**, starting on the front right corner of the class



EPFL

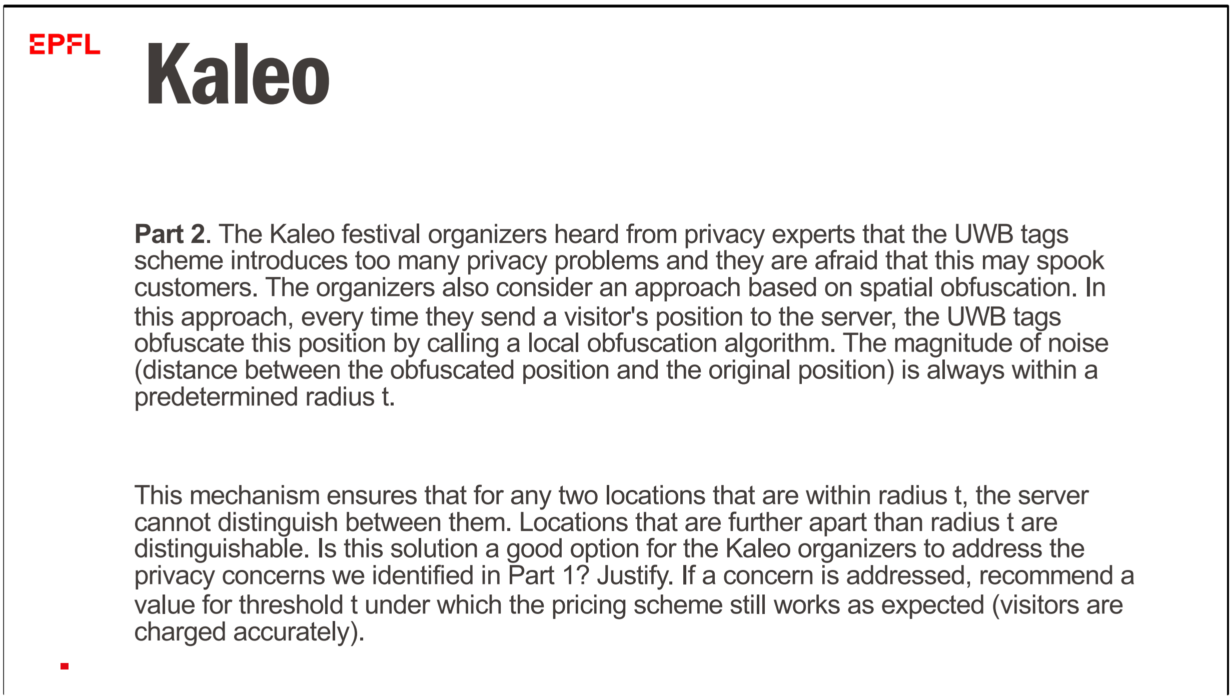
Kaleo

The year is 2022. Events with thousands of people are possible again. While preparing their best come-back, the Kaleo festival organisers are thinking about a new pricing scheme. Instead of charging a flat rate to access the festival area, the organisers want to use a **pay-per-song scheme** under which visitors are charged depending on how many songs they listened to and on which stage. In this scheme, listening to the concerts at the Grande Scene is more expensive than on the smaller stages.

To implement this new pricing scheme, each visitor will be given an Ultra Wide Band (UWB) tag. The UWB tag **sends the visitor's position to a central service every minute**. This allows the festival organisers to track visitors on the festival grounds and infer which stages they visited, when, and for how long.

Part 1. Describe a privacy concern for festival visitors that is caused by the introduction of the location-tracking UWB tags and that were non-existent under the flat rate pricing scheme.

Any concern related to tracking or to relationships (people being together at the festival) would be acceptable; but it needs to be justified why UWB allows to do tracking, or relationship discovery and why it was not possible with the previous scheme

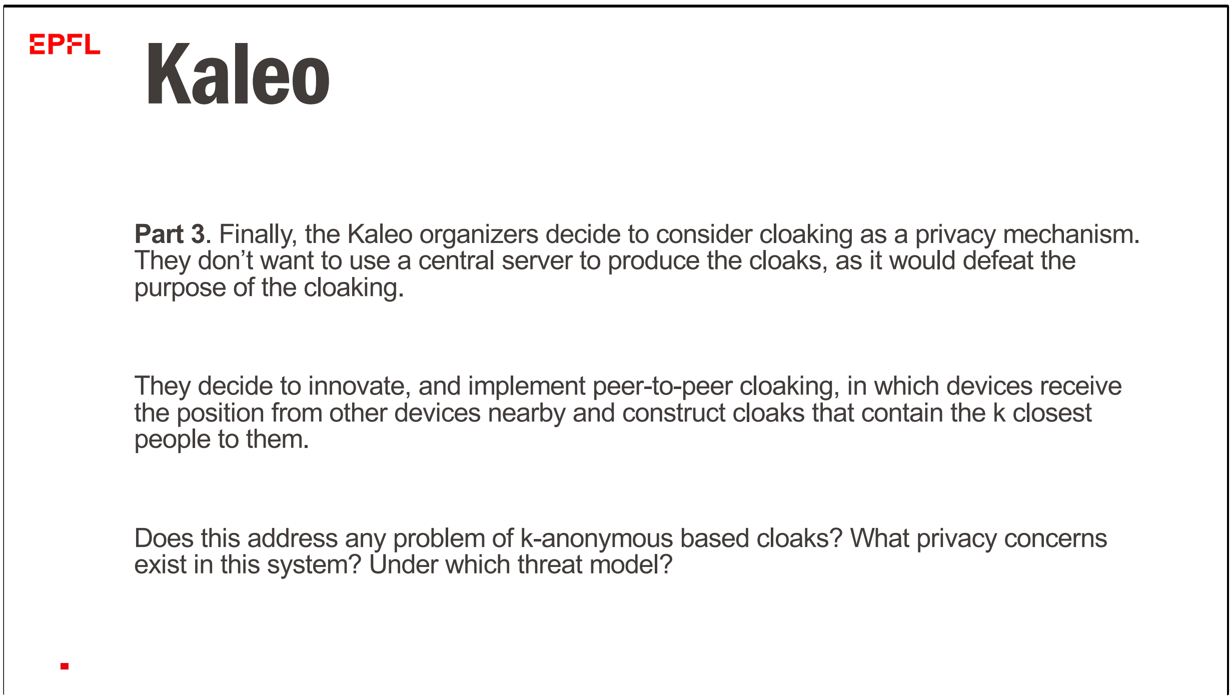


Kaleo

Part 2. The Kaleo festival organizers heard from privacy experts that the UWB tags scheme introduces too many privacy problems and they are afraid that this may spook customers. The organizers also consider an approach based on spatial obfuscation. In this approach, every time they send a visitor's position to the server, the UWB tags obfuscate this position by calling a local obfuscation algorithm. The magnitude of noise (distance between the obfuscated position and the original position) is always within a predetermined radius t.

This mechanism ensures that for any two locations that are within radius t, the server cannot distinguish between them. Locations that are further apart than radius t are distinguishable. Is this solution a good option for the Kaleo organizers to address the privacy concerns we identified in Part 1? Justify. If a concern is addressed, recommend a value for threshold t under which the pricing scheme still works as expected (visitors are charged accurately).

For the large majority of concerns the answer is along the lines of:
The value of t affects both effectiveness to address the privacy concern, and utility of the mechanism regarding fair billing of users.
If t is small, then the mechanism is ineffective in preventing finer grained tracking. If t is large then charging accurately may become very complicated (one may believe that users are in a different scenario than where they are)



Kaleo

Part 3. Finally, the Kaleo organizers decide to consider cloaking as a privacy mechanism. They don’t want to use a central server to produce the cloaks, as it would defeat the purpose of the cloaking.

They decide to innovate, and implement peer-to-peer cloaking, in which devices receive the position from other devices nearby and construct cloaks that contain the k closest people to them.

Does this address any problem of k-anonymous based cloaks? What privacy concerns exist in this system? Under which threat model?

Here the problem is that neighbouring attendees are put in an advantage position to track other attendees. Because you need to share the position with those surrounding you to find a cloack, now they can track you.

It does not address the problem of cloaks, just increases the attack surface by giving the location to more entities
The concerns are related to tracking, nothing different than before.
Threat model: adversarial Kaléo attendees.