

Privacy-Enhancing Technologies

Lecture series Summer Term 2021

Dr. Patricia Arias-Cabarcos, Thorsten Strufe

12.04.2021 – KIT and TU Dresden – still in pandemic times



*Disclaimer: This lecture was prepared in cooperation with
Javier Parra-Arnau*

Competence Center for Applied Security Technology



Outline of Today's Lecture

- Who are we?
- Organizational matters (preliminaries)
- Course outline

- A brief introduction

Who's Who

- Chair of Privacy and Security (PS)
- For the Lecture:
 - Dr. Patricia Arias-Cabarcos
 - KASTEL corridor
 - patricia.cabarcos[at]kit.edu
 - Thorsten Strufe
 - Chair professor
 - thorsten.strufe[at]kit.edu
- Teaching Assistants/Exercise courses:
 - None
- Consultation
 - Send us an email or pass by, doors are open
- https://ps.tm.kit.edu/139_257.php



- Course language is English (you have a choice of Eng/Spa/Ger during the exam)
- There will be some ex-cathedra parts, but please ask and discuss as much as possible!
- This course is new, so the slides and content are subject of adaptation :-)

- c|net COVID-19 BEST PRODUCTS ▾ REVIEWS ▾ NEW

Experts believe that at least half the population will be using contact-tracing apps for their own protection. The biggest challenge will be convincing the public to use them, given years of trust issues with big tech.

Alfred Ng  April 18, 2020 5:00 a.m. PT



arXiv.org > cs > arXiv:2004.07723

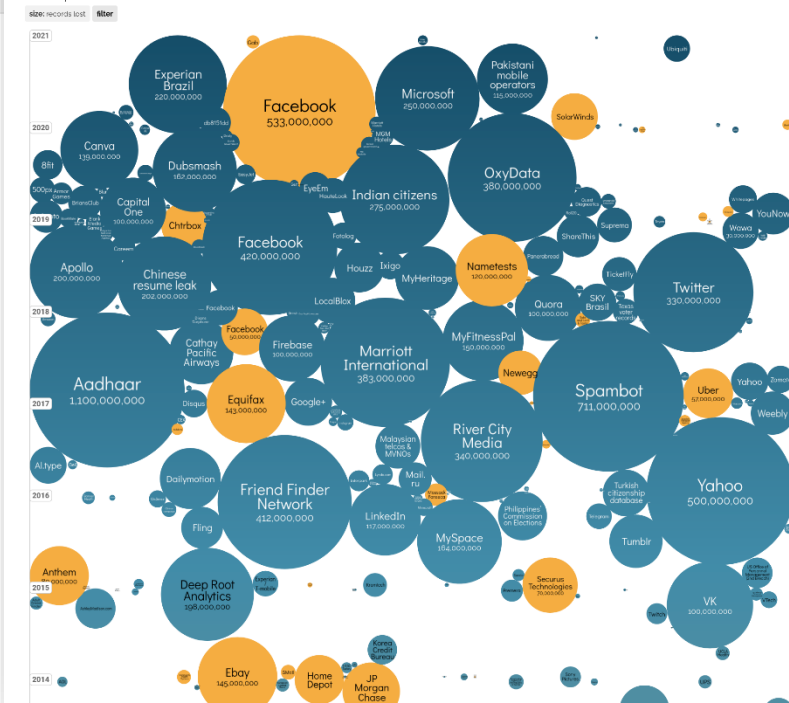
[Help](#) | [Advanc](#)

[Submitted on 16 Apr 2020]

Christiane Kuhn, Martin Beck, Thorsten Strufe

The recent SARS-CoV-2 pandemic gave rise to management approaches using mobile apps for contact tracing. The corresponding apps track individuals and their interactions, to facilitate alerting users of potential infections well before they become infectious themselves. Naive implementation obviously jeopardizes the privacy of health conditions, location, activities, and social interaction of its users. A number of protocol designs for colocation tracking have already been developed, most of which claim to function in a privacy preserving manner. However, despite claims such as "GDPR compliance", "anonymity", "pseudonymity" or other forms of "privacy", the authors of these designs usually neglect to precisely define what they (aim to) protect. We make a first step towards formally defining the privacy notions of proximity tracing services, especially with regards to the health, (co-)location, and social interaction of their users. We also give a high-level intuition of which protection the most prominent proposals can and cannot

Selected events over 30,000 records



Some Words regarding this Course

- Main topic of this course is ***the privacy of individuals*** that are using (or surrendering their data to) IT, and ***how they can be protected*** from disadvantages, failures, or abuse.
- We will analyze the adversary models and evaluation metrics underlying the design of privacy-enhancing technologies for that purpose.
- Learning outcomes
 - Critical reasoning about privacy
 - Gaining knowledge in the evaluation of privacy risks
 - Understanding of the design aspects of privacy-enhancing technologies
 - Familiarity with the latest research in the field
 - Ability to analyze and discuss the space of solutions to a given privacy problem

Preliminary Course Overview

Lecture (Mondays, 16:00h)

- Background and motivations for privacy
- Privacy metrics and adversary models
- Anonymous communications
- Data-perturbative privacy-enhancing technologies
- Anonymization algorithms for databases
- Homomorphic encryption and zero knowledge proofs
- Selective disclosure for identity management
- Usable privacy
- Applying privacy principles and case studies

The Reading Group (Exercise Course)

- Exercise course will be organized as a reading group
 - Papers (links) available on the webpage (soon, depending on |participants|)
 - Read papers early...
 - One paper with relation to lecture topics will be presented (by a random **one** of **you!**) and discussed (by **you!**) each week (please take note of the emphasize on **YOU :-)**)
- This year there won't be a coding task (usually introduced in week 3-4, solved in groups of 2-3 students with help from us, to present last Thursday of the term, we're waiting for the pandemic to end)

More organization

- Exam:
 - Oral, make an appointment early (email Ms. Sauer/Ms. Gersonde)
 - Participation in the reading group is beneficial
- Literature (there isn't much...):
 - „The little blue book“ and „Privacy is hard“ (both: Jaap-Henk Hoepman)
 - Anonymous communication literature: <https://www.freehaven.net/anonbib/>
 - Check the „Privacy Enhancing Technologies Symposium (<https://petsymposium.org>)
 - „The age of surveillance capitalism“ (Zuboff), „Privacy is Power“ (Veliz), „The unsinkable aircraft carrier“ (Campbell)
 - „1984“ (George Orwell), or, simpler, „The Circle“ (Dave Eggers)
 - Cory Doctorow, etc.

Questions?

