

Privacy-Enhancing Technologies

Lecture series Summer Term 2022

Thorsten Strufe

25.04.2022 – hybrid KIT and TU Dresden



*Disclaimer: This lecture was prepared in cooperation with
Patricia Arias-Cabarcos and Javier Parra-Arnau*

KASTEL Security Research Labs



Outline of Today's Lecture

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

- A brief introduction

Who's Who

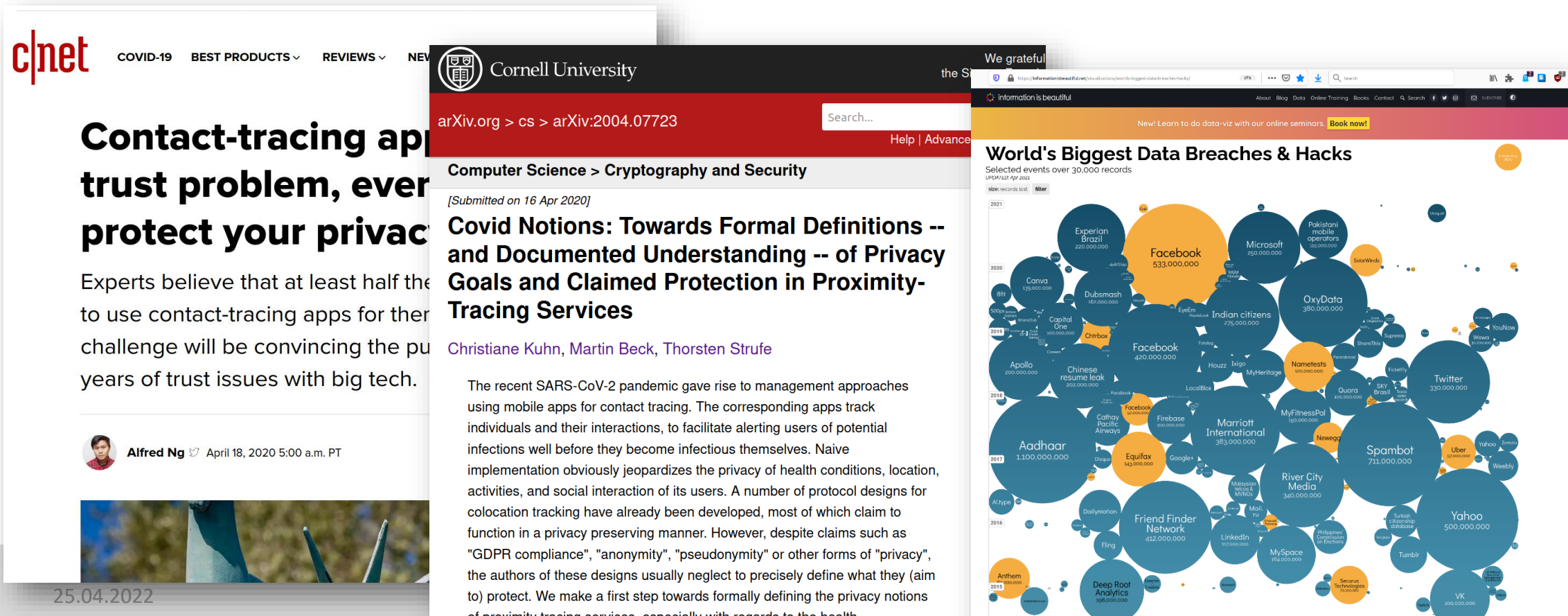
- Chair of Privacy and Security (PS)
- For the Lecture:
 - Thorsten Strufe
 - Chair professor
 - [thorsten.strufe\[at\]kit.edu](mailto:thorsten.strufe@kit.edu)
- Teaching Assistants/Exercise courses:
 - Patricia Guerra-Balboa
- Consultation
 - Send us an email or pass by, doors are open
- https://ps.tm.kit.edu/139_501.php
- <https://lists.ira.uni-karlsruhe.de/mailman/listinfo/pets>



- Course language is English (you have a choice of Eng/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 :-)

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.



The collage consists of three overlapping screenshots:

- Left Screenshot:** A c|net article titled "Contact-tracing app trust problem, ever protect your privacy". The text below the title reads: "Experts believe that at least half the... to use contact-tracing apps for their... challenge will be convincing the pu... years of trust issues with big tech." It includes a post by Alfred Ng on April 18, 2020, and a partial image of a person wearing a face mask.
- Middle Screenshot:** An arXiv.org preprint page for "Covid Notions: Towards Formal Definitions -- and Documented Understanding -- of Privacy Goals and Claimed Protection in Proximity-Tracing Services" by Christiane Kuhn, Martin Beck, and Thorsten Strufe. The submission date is 16 Apr 2020. The abstract begins: "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."
- Right Screenshot:** A bubble chart titled "World's Biggest Data Breaches & Hacks" showing selected events over 30,000 records. The chart is a bubble plot where the size of each bubble represents the number of records affected, and the color indicates the year (2015-2021). Major breaches include Aadhaar (1,100,000,000), Facebook (533,000,000), and Spambot (711,000,000).

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, 15:45h)

- Background and motivations for privacy
- Privacy metrics and adversary models
- Data-perturbative privacy-enhancing technologies
- Anonymization algorithms for databases
- The special case of location and trajectory privacy
- Anonymous communications
- Selective disclosure for identity management
- 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...
 - Two papers 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 :-)**) (also: <https://pads.ccc.de/QQS6CCpTDI>)
- In case of interest, we can organize a coding task (introduced in week 3-4, solved in groups of 2-3 students, to present in last reading group)

More organization

■ Exam:

- Oral, make an appointment early (email Ms. Sauer/Ms. Gersonde)
- Participation in the reading group is beneficial

■ Literature:

- „The little blue book“ and „Privacy is hard“ (both: Jaap-Henk Hoepman)
- Anonymous communication literature: <https://www.freehaven.net/anonbib/>
- Papers at „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?

