Privacy-Enhancing Technologies HT21

Sonja Buchegger, buc@kth.se

KTH Computer Science and Communication

Overview of this lecture

- How the course works
  - Goals
  - Setup
  - Everyone's tasks
  - Deadlines
  - Time investment
  - Topics
  - Criteria, policies
- Capture state/preferences
- How to do well and get the most out of the course
- Get a notion of what PET means

KTH Computer Science and Communication

How the course works

- Exploring privacy topics through research papers

KTH Computer Science and Communication

After completion of the course, the student should be able to:

- **identify threats against privacy** in an IT system,
- explain and use basic **terminology** in the area correctly,
- **find and use documentation** of privacy-related problems and technologies,
- demonstrate an **overview of privacy enhancing technologies** (PET),
- **analyse descriptions of PET** systems with regard to their protection of privacy and function,
- identify vulnerabilities from PET system descriptions, predict their equivalent threat, and choose **countermeasures** against identified threats and show their efficiency,
- compare countermeasures and **evaluate their side effects**,
- **present and explain their reasoning to others**,

in order to

- as citizen and expert be able to discuss privacy in general and PET in particular,
- in professional life and/or research projects be able to use existing privacy enhancing technologies and develop their own.

KTH Computer Science and Communication

Setup

- Some lectures and several seminars
- At each seminar, some participants **present a topic** relevant to privacy-enhancing technologies, followed by a discussion. The presentation is complemented by a **written report**. Before each presentation (incl. lectures), there will be a **short quiz on the related reading.**
- Course responsible teacher: Sonja Buchegger
- Teaching assistant: Md Sakib Nizam Khan

KTH Computer Science and Communication

Schedule

- Today: intro, topics
- Next few days: pick topic/group
- Next few weeks:
  - Lectures
  - Seminars with student presentations
- Throughout: reading research papers, writing report

KTH Computer Science and Communication

Tasks

- Form group and pick topic
- Read papers, select papers on your topic for the others to read
- Answer quizzes, design quiz with solutions
- Participate in discussions, prepare discussion
- Present your topic
- Write a report on your topic
- Peer-review
- Revise your report

KTH Computer Science and Communication

Deadlines (within 1 week)

- Form group and pick draft topic (by Monday)
- Read required general papers (before class)
- Read papers/presentation topic (before class)
- Answer quizzes (during class)
- Participate in discussions (during class)
- Select papers on your topic for the others to read (by Monday the week before the presentation)
- Design quiz with solutions (by Monday before your presentation)
- Prepare discussion (design, facilitate, document) (by Monday before your presentation)
- Draft slides

KTH Computer Science and Communication

Deadlines, ctd.

- Get approval from course responsible for selected papers, quiz questions, discussion prompts according to the deadlines listed with these tasks
- Present your topic (during your seminar)
- Write a report on your topic (deadline depending on your presentation seminar (PS) day: PS1 (Sep 15) PS2 (Sep 22) PS3 (Sep 29) PS4 (Oct 07)
- Peer-review 1 report (Monday after reception)
- Revise your report given feedback (week 7 after topic)

KTH Computer Science and Communication

Week 35: lecture	Monday deadlines	class	weeks after topic			
Week 36:: lecture	groups/topics		pres.	report	between	revision
Week 37: lecture						
PS1 week 38	PS1, PS2 slides PS3, PS4 report	PS1 presentation	2	4	2	7
PS2 week 39	PS1 on PS3 feedback, PS2 on PS4	PS2 presentation	2	4	2	7
PS3 week 40	PS3, PS4 slides, PS1, PS2 report	PS3 presentation	4	2	-2	7
PS4 week 41	PS3 on PS1 feedback, PS4 on PS2	PS4 presentation	4	2	-2	7
week 43	all final reports					

KTH Computer Science and Communication

Sample time allocation for 7.5 ECTS (assumption: 8 groups)

- 20 h attendance (8h teacher-led, 12h seminars)
- 40 h research on own topic and presentation preparation
- 40 h research on own topic and report writing, revision
- 5 h discussion design and documentation
- 5 h quiz preparation
- 69 h reading (~23 papers, 3 h/paper - 8x2 seminars, 2x1 lectures, 5 general)
- 1 h course evaluation
- 6 h peer review
- 2 h planning
- 12 h buffer, independent reading, reflection

KTH Computer Science and Communication

Attendance policy

- Default: attend every lecture/seminar, pass quizzes
- Deviations and compensation:
  - Fail or miss a quiz -> summarize required reading
  - Miss a lecture -> in addition to quiz compensation, summarize lecture content (if slides available) or read and summarize a paper listed as optional reading
  - Miss a seminar -> in addition to quiz compensation, provide extra reviews for reports on the missed topics
  - Miss a deadline -> DON'T! Others depend on you. Seek help within the group if you struggle, seek help from me if the whole group struggles.

KTH Computer Science and Communication

Grading criteria, rough outline

- Combination of all tasks, building on the goals.
- E: passed all quizzes, completed tasks "adequately" (presentation, report, review, seminar prep: quiz, discussion, papers)
- D: E plus "relevant" active class participation
- C: D plus tasks completed "well" on average
- B: D plus tasks completed "very well" on average
- A: D plus participation and tasks completed "excellently" for most, at least "very well" for some.

KTH Computer Science and Communication

More concretely, what does it mean?

- Will post rubrics on canvas.

KTH Computer Science and Communication

Group v. individual assessment

- Group: report, revision, quiz design, presentation organization, choice of reading, discussion setup
- Individual: quiz response, discussion participation/facilitation, presentation part, peer review

KTH Computer Science and Communication

Privacy applied to this course, expected value of visibility (concluded from mentimeter)

- video on in breakout room for almost everyone,
- video on for most, profile pic up for some, none for some in unrecorded zoom
- everyone according to comfort in recorded zoom (only course participants have access), breakout rooms are never recorded
- recording of presentations shared with course participants for most (Sonja will check with each group before posting anything)

KTH Computer Science and Communication

Topics (preliminary selection)

Suggest others if you like!

- Communications:
  - Anonymous routing (e.g.Tor)
  - Mixnets
  - Censorship resistance
  - Traffic analysis
  - Location privacy
- Data protection
  - Differential privacy
  - Anonymity/de-anonymization
  - Usage control
  - Machine learning/AI privacy
  - Privacy by Design
- Private computation
  - Secure multi-party computation
  - Homomorphic encryption
- Private information retrieval
  - PIR
  - ORAM
- Zero-knowledge proofs (e.g. anonymous attribute-based credentials)
- Transparency-enhancing tools (TETs)
- PETs and usability

KTH Computer Science and Communication

Topics (preliminary selection)

- Some application domains:
  - IoT privacy
  - Healthcare privacy
  - Big data privacy
  - Cryptocurrencies
  - Electronic voting
  - Democracy

KTH Computer Science and Communication

Context for the topic

- Frame your report/presentation by a research question to help you
  - focus your literature search
  - get a perspective to narrow down the topic

KTH Computer Science and Communication

Relative importance for allocation (concluded from mentimeter)

- 1 presentation slot
- 2 group members
- 3 topics

- Will post a structured page on Canvas that you can edit to state your constraints and preferences, structured according to the ranking above.

KTH Computer Science and Communication

Getting started:

- Get some idea of what the topics mean
- Suggest own if not listed
- Use discussion space on Canvas, can still add to today's mentimeter for almost 2 days
- Fill in Canvas page at the latest on Monday (link will be announced once set up)

KTH Computer Science and Communication

Getting started, ctd.

Reading for next week (there will be a quiz on both):

- I've got nothing to hide and other misunderstandings of privacy. Daniel Solove
- Course information (upcoming on canvas)

KTH Computer Science and Communication

Course board members

- 2 students to discuss course with, during and after evaluation
- Volunteers?

KTH Computer Science and Communication

How to do well and get the most out of the course

KTH Computer Science and Communication

First, the obvious

- Be thorough
  - Follow instructions
  - Make a plan, start early, build in buffers
  - Engage with the material
  - Seek out additional information
  - Cooperate, discuss
  - Pay attention to the news, reflect
  - Pull your weight and make sure others do
  - Actively participate

KTH Computer Science and Communication

Each group is in charge

Of the quality of their own seminar

- Quiz questions
- Selected papers
- Presentation
- Discussion questions
- Liveliness and relevance of discussion
- Enabling many voices, perspectives

- Written output quality: Report, feedback, discussion documentation, revision

KTH Computer Science and Communication

Discussion rules

- Do contribute
- Do not monopolize
- Seek balance for critical responses (somewhere between uncritical harmony and relentless critique and questioning)

KTH Computer Science and Communication

Instructions to follow (in assignments)

- Timing
- Specifications for
  - Report
  - Presentation
  - Review
  - Quiz
  - Discussion
  - Revision
- Logistics
- Literature