iHub

Privacy Seminar

Course organisation

Jaap-Henk Hoepman

iHub
Radboud University
Karlstad University

jhh@cs.ru.nl // www.cs.ru.nl/~jhh // blog.xot.nl
@xot@someone.elses.computer // @xotoxot.bsky.social

Radboud University

Dan Perjovschi, 2007

Organisation

- **Teachers**
  - Jaap-Henk Hoepman (jhh@cs.ru.nl); Erasmus 19.20
  - Christine Utz (christine.utz@ru.nl);
- **Brightspace hardly used**
  - Website: https://www.cs.ru.nl/~jhh/secsem.html
  - Wiki: http://wiki.science.ru.nl/privacy/

Seminar

- **Seminar**
  - Student lecture
  - Student paper
- **Grade = weighted average**
  - But only if all grades at least 5.5
  - If not, lowest grade is final grade!
- **Working in groups**
  - 3 (or 2) people
- **Attendance required**
  - We start 15:30 sharp!
- **Lecture rooms (check the online roster!)**
  - EOS N 01.180 until March 12 (with some exceptions!)
  - EOS N 01.180 from April 9 onwards.

Course schedule

Date	Time	Topic	Deadline
29-1	15:30	(no lecture due to illness)	
5-2	15:30	Course organisation and Privacy: an overview, by Jaap-Henk Hoepman	
12-2	15:30	Privacy: an overview (continued)	
19-2	15:30	Writing and Speaking and Privacy by design, by Jaap-Henk Hoepman.	
26-2	15:30	Usable privacy, by Christine Utz	
5-3	15:30		
12-3	15:30		
19-3		(no lecture)	
26-3		(no lecture)	
2-4		(no lecture)	
9-4	15:30		skeleton
16-4	15:30		
23-4	15:30		
30-4		(no lecture)	
7-5	15:30		
14-5		(no lecture)	
21-5	15:30		
28-5	15:30		
4-6	15:30		final paper

Topics (first come first serve)

- **Privacy in databases**
  - How to provide (controlled) access to personal data stored in databases, without immediately threatening the privacy of the people involved, using mechanisms like differential privacy or statistical disclosure control.
- **Privacy friendly search**
  - How to hide the query (i.e. what is searched for) from the party hosting the database.
- **Searching in encrypted databases**
  - How to also hide the underlying data in the database from the party hosting the database.

- **Polymorphic encryption**
  - How to protect privacy in e.g. health care where data must be made conditionally accessible to certain care providers while staying encrypted in general.
- **Privacy friendly identity management**
  - How to use e.g. attribute based credentials or other claims based approaches to make identity management more privacy friendly.
- **Privacy friendly revocation of credentials**
  - How to (efficiently) revoke anonymous credentials. I.e. how to revoke a particular credential, even though individual credentials cannot be traced by definition

- **Revocable privacy**
  - How to guarantee privacy while also guaranteeing that all users of a system abide by some predetermined rules, i.e. how to design systems that are both privacy friendly and secure.
- **Privacy friendly location based services**
  - How to provide a service that depends on the user's current location, without revealing the actual, exact location?

- **Privacy in asynchronous messaging**
  - How to establish contact anonymously, and how to subsequently exchange messages in an unlinkable fashion that prevents the service provider to learn who is communicating with who.
- **Anonymous cryptocurrencies**
  - How to make Bitcoin like cryptocurrencies privacy friendly.
- **Secure multiparty computation**
  - How to jointly compute the output of a function (e.g. some aggregate statistic) without revealing the individual inputs.
- **Obfuscation**
  - Can obfuscation and other methods of ‘resistance’ help to protect your privacy?

Research

- **analyse a particular practical case**
  - what are the privacy issues (from a societal and legal perspective) and how are they dealt with
- **give a precise and concise problem description**
  - in technical terms: define your model; your assumptions
- **investigate possible PETs that apply**
  - summarise your analysis
- **pick one and solve the problem (involves a protocol)**
  - describe this in sufficient detail!
- **(informally) prove or argue correctness**

Student lecture

- **Goal of lecture**
  - to inform other students about your research
- **Important**
  - make lecture interactive
  - add additional material
- **Discuss draft**
  - Thursday 12:30-13:15 the week before, room Erasmus 19.20
  - mail slides etc. at least one day before.

Student lecture: grading

Content

- **Argumentation and Depth**
  - A solid basis and backing of all statements.
- **Intelligibility**
  - Quality of explanation; take audience into account.
- **Comprehensiveness**
  - Cover all important aspects (incl. legal/societal); separates important/secondary issues.
- **Structure**
  - Logical ordering; relationship between the topics.

Form and performance

- **Attractiveness**
  - Captivating audience, supporting materials.
- **Delivery**
  - Engagement and contact with the audience.
- **Interaction**
  - Level of interactivity, the way you respond to questions.

Grading

- **Possible criteria scores**
  - -: worse than average
  - 0: average (typcial score)
  - +: better than average
- **All 0 on criteria then 7 is the grade**

Student paper

- **Goal**
  - Report on research
  - Express own perspective and opinion on PETs
- **Format**
  - Roughly 12-14 pages (depending on group size, excluding references)
    - *A4, reasonable margins, 10-11 pt font*
- **Beware**
  - Collect your own literature as well
  - Use input obtained during presentation in class

Student paper: AI Tools

- **Meta goal**
  - Learn to write a scientific report
  - Develop your own style of writing
  - See writing as a tool that helps you think and understand the problem space and the possible solutions
- **Refrain from using AI tools**
  - Verbatim copies of AI generated text are considered fraudulent behaviour
  - Use sparingly to correct style: not everyone should write like a boring US marketing copywriter

Student paper

- **Typical structure**
  - Context
  - Problem description
    - *Including legal/social analysis*
  - Proposed solution
  - Technical analysis
  - Conclusions

Student paper: planning

- **Average timespan**
  - Literature study: 2 weeks
  - Perform research: 2 weeks
  - Write skeleton: 1 week
  - Write final paper: 3 weeks
- **Deadlines**
  - April 9: Skeleton
  - June 4: Final paper
- **So start as soon as you can!**

Student paper: grading

Content

- **(Technical) quality**
  - Understanding of the (technical) issues. Correctness of all (technical) statements.
- **Analysis**
  - Proper argumentation, completeness, distinguishing main and secondary points.
- **Quality of references**
  - Relevance, completeness and originality.
- **Own opinion**

Form

- **Style**
  - Clarity, objectiveness, spelling and grammar.
- **Structure**
  - Logical structure and proper flow.
- **Attractiveness**
  - Formatting of paper, including bibliography.

Working in groups

- **Everyone responsible for all output**
  - Review each others work!
- **Work together, not seperately**
- **Plan your work**
- **Equally divide work**
  - And make sure everyone delivers
  - If not: notify me before everything escalates….

Remaining points

- **Contribute to the *wiki***
  - http://wiki.privacy.cs.ru.nl/Main_Page

Questions

[Monty Python's Argument Clinic sketch]