

Privacy Seminar Course Organisation Radboud University Jaap-Henk Hoepman Privacy & Identity Lab Radboud University University of Groningen ⊠ jhh@cs.ru.nl // ⁴ www.cs.ru.nl/~jhh // ⁴ blog.xot.nl // @xotoxot

Organisation

- Teachers
 - Jaap-Henk Hoepman (jhh@cs.ru.nl); Erasmus 19.12
 - Hanna Schraffenberger (<u>H.Schraffenberger@ru.nl</u>);
- Brightspace hardly used
 - Website: https://www.cs.ru.nl/~jhh/secsem.html
 - Wiki: http://wiki.science.ru.nl/privacy/

Jaap-Henk Hoepman // 03-02-2022 // Privacy Seminar Organisation

Seminar

Seminar

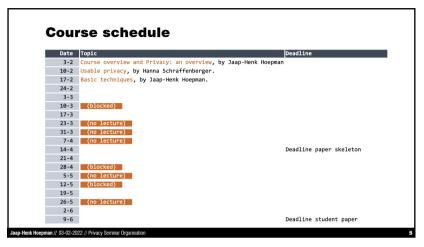
2

- 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
 - 4 or 5 people
- Attendance required
- Lecture rooms
 - HG 00.071 (until and including March 17) and Mercator 1 00.28 (from April

4

3

1



Searching in encrypted databases How to also hide the underlying data in the database from the party hosting the database.

Privacy in databases

Privacy friendly search

Jaap-Henk Hoepman // 03-02-2022 // Privacy Seminar Organisation

Privacy in machine learning
How to ensure that individual data used to train a machine learning model is not leaked when using the model.

How to hide the query (i.e. what is searched for) from the party hosting the database.

Topics (first come first serve)

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.

Anonymous cryptocurrencies

How to make Bitcoin like cryptocurrencies privacy friendly. 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. Le. how to revoke a particular credential, even though individual credentials cannot be traced by definition

Revocable privacy

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.

Secure multiparty computation
 How to jointly compute the output of a function (e.g. some aggregate statistic) without revealing the individual inputs.

Can obfuscation and other methods of 'resistance' help to protect your privacy?

5

6

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

Jaap-Henk Hoepman // 03-02-2022 // Privacy Seminar Organisation

Student lecture

- Goal of lecture
 - to inform other students about your research
- Important
 - make lecture interactive
 - add additional material
- Discuss draft
 - thursday 13:00-13:15 the week before, room TBA
 - mail slides etc. at least two day before

Jaap-Henk Hoepman // 03-02-2022 // Privacy Seminar Organisation

Student lecture: grading

Content

Argumentation and Depth

 Whether your lecture provides a solid basis and backing of all statements and claims made, and whether it covers all important topics in sufficient

Intelligibility

Whether the message comes across, whether your lecture connects to what your audience expects and understands, how well you explain certain topics.

Comprehensiveness

Whether your lecture covers all important aspects, and clearly separates important issues from secondary details. Equal attention should be paid to technical and legal/societal issues.

Form and performance

Logical ordering of your lecture, the relationship between the topics.

Whether your lecture captivates the audience, your use of supporting materials (e.g. powerpoint).

 Delivery
 Level of engagement and contact with the audience, your presence in front of the class, the liveliness and tone of your lecture

Interaction

Level of interactivity, the way you respond to questions.

Language

Pronunciation, vocabulary, grammar.

Jaap-Henk Hoepman // 03-02-2022 // Privacy Seminar Organisation

Goal

• Report on research

Student paper

• Express own perspective and opinion on PETs

Format

• Roughly 15-20 pages (depending on group size, excluding references) ★A4, reasonable margins, 10-11 pt font

- Collect your own literature as well
- Use input obtained during presentation in class

Jaap-Henk Hoepman // 03-02-2022 // Privacy Seminar Organisation

10

9

Student paper

■ Typical structure

- Context
- Problem description
 - ★ Including legal/social analysis
- Proposed solution
- Technical analysis
- Conclusions

Jaap-Henk Hoepman // 03-02-2022 // Privacy Seminar Organisation

Student paper: planning

Average timespan

- Literature study: 2 weeks
- Perform research: 2 weeks
- Write skeleton: 1 week
- Write final paper: 3 weeks

Deadlines

- April 14: Skeleton
- June 9: Final paper
- So start as soon as you can!

Jaap-Henk Hoepman // 03-02-2022 // Privacy Seminar Organisation

11 12

Student paper: grading Content Form ■ (Technical) quality Whether the paper shows an understanding of the (technical) issues involved. Correctness of all Clarity of writing, objectiveness, linguistic quality (in terms of spelling and grammar). (technical) statements and claims. Analysis Whether a proper argumentation is given, and Logical structure of the paper, helping the reader understand what he is about to read, giving the whether all main aspects of the topic are addressed, with proper regard of what are the main points and what are only secondary points. (This covers the criteria argumentation, depth and intelligibility, and paper a natural flow. Attractiveness Formatting of the paper, including precise formatting of the bibliography. comprehensiveness used for scoring the presentation.) Quality of references Whether you found and cite all relevant literature. Originality (finding relevant references yourself) is appreciated. Own opinion Whether the paper clearly expresses and argues your own opinion on the subject matter. Jaap-Henk Hoepman // 03-02-2022 // Privacy Seminar Organisation

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....

Jaap-Henk Hoepman // 03-02-2022 // Privacy Seminar Organisation

14

16

14

13

Remaining points

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

Jaap-Henk Hoepman // 03-02-2022 // Privacy Seminar Organisation

15

4