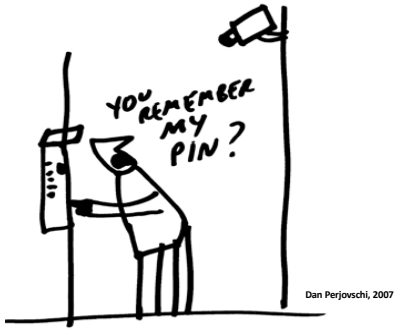
Dan Perjovschi



1

Privacy & Identity Lab

Radboud University

university of groningen

Privacy Seminar

Course Organisation

Jaap-Henk Hoepman

Privacy & Identity Lab
Radboud University
University of Groningen

✉ *jhh@cs.ru.nl* // *www.cs.ru.nl/~jhh* // blog.xot.nl // @xotoxot

2

Organisation

- **Teachers**
  - Jaap-Henk Hoepman (jhh@cs.ru.nl); Erasmus 19.29
  - Oğuzhan Ersoy
- **Brightspace hardly used**
  - Website: https://www.cs.ru.nl/~jhh/secsem.html
  - Wiki: http://wiki.science.ru.nl/privacy/

3

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**
- **Lecture rooms**
  - MERC I 00.28 (except tentative extra slots)

4

Course schedule

Date	Time	Topic	Deadline
2-2	10:30	Course organisation and Privacy: an overview, by Jaap-Henk Hoepman	
9-2	10:30	Basic techniques, by Jaap-Henk Hoepman.	
16-2	10:30	(no lecture)	
23-2	10:30		
2-3	10:30		
9-3	10:30		
16-3	10:30		
23-3		(no lecture)	
30-3		(no lecture)	
6-4		(no lecture)	
13-4	10:30		
20-4	10:30		paper skeleton
27-4		(no lecture)	
4-5		(no lecture)	
11-5	10:30		
18-5		(no lecture)	
25-5	10:30		
1-6	10:30		
	13:30	(tentative extra slot)	
8-6	10:30		final paper
	13:30	(tentative extra slot)	

5

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

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**

7

Student lecture

- **Goal of lecture**
  - to inform other students about your research
- **Important**
  - make lecture interactive
  - add additional material
- **Discuss draft**
  - Thursday 9:45-10:15 the week before, room Erasmus 19.29
  - mail slides etc. at least one day before

8

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 detail.
- **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

- **Structure**
  - Logical ordering of your lecture, the relationship between the topics.
- **Attractiveness**
  - 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.

9

Grading

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

10

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

11

Student paper

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

12

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!**

Student paper: grading

Content

- **(Technical) quality**
  - Whether the paper shows an understanding of the (technical) issues involved. Correctness of all (technical) statements and claims.
- **Analysis**
  - Whether a proper argumentation is given, and 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 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.

Form

- **Style**
  - Clarity of writing, objectiveness, linguistic quality (in terms of spelling and grammar).
- **Structure**
  - Logical structure of the paper, helping the reader understand what he is about to read, giving the paper a natural flow.
- **Attractiveness**
  - Formatting of the paper, including precise formatting of the 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]

jhh@cs.ru.nl www.cs.ru.nl/~jhh blog.xot.nl twitter: @xotoxot

17