Data Privacy & Information Security

Fall 2016

Course outline

Instructor: Periklis A. Papakonstantinou, e-mail: periklis.research@gmail.com, 1WP-1072

Lectures: Monday 1–3.50pm at 1WP-418; office hours: 10.30–11.30am

Emailing: Make sure that your emails have in their subject "data privacy" or "information security"

Textbooks and readings: Introductory course to Information Security and Data Privacy. The material is a selection of basic topics presented in class. The main reading source is the notes you scribed during lectures. In each lecture you will be given the section numbers from the following textbooks.

1. *Introduction to Modern Cryptography*, by Katz and Lindell.
2. *Algorithmic Foundations of Differential Privacy*, by Dwork and Roth.

Web-page: we use the Rutgers Blackboard platform

The course is formally listed as "Data Privacy"

Course description, objectives & prerequisites

This class is a modern introduction to Information Security and to Data Privacy. The goal is students to obtain strong technical competence in various electronic security and privacy situations that arise in all modern IT systems. This is indispensable knowledge for everyone working in Information Systems, Data Management and Analysis, and at any level (from conducting research to building or managing systems).

Think of the following problem: consider two parties A and B communicating over the Internet, and a third malicious party (the adversary). You can think of A as an individual and B as a credit card company. We wish to provide means for A and B to *communicate securely*. What does it mean "communicate securely"? Conceptualizing, i.e. *defining*, what is the security requirement is a necessary task before deploying any secure system. For example, "communicate securely" could mean that the adversary: knows exactly how A and B encrypt messages and she can hear everything A and B say to each other but still she can make no sense of what the actual (unencrypted) messages are. Making precise what does it mean "not to be able to make any sense" is non-trivial and doesn't have a unique answer. Every approach to security involves: definitions of security – i.e. accurately specifying what do we require – and constructions that meet the requirements. This is a Secure Communication problem.

Here is a second, different problem: an insurance company wants to make a financial decision based on some statistics regarding the income and the age of all individuals in the NYC area. Is it possible (1) to store the information of the individuals such that the company can make use of the database and at the same time (2) make it impossible for the company to find out who are the individuals whose information is recorded? In other words, we wish to make possible the use of *statistical databases* and at the same time preserve the *privacy* of individuals. This is different than secure communication. Here the database is not encrypted and we wish to make its entries *anonymous*. This second problem is a Privacy problem.

This class gives a rigorous introduction both to Information Security and to Privacy. It puts forth both the basics and the state-of-the-art in the field, and is designed for a diverse audience. The content is mathematically rigorous, but there are no prerequisites other than basic mathematical background. Basic mathematics background means a course in Statistics, Probability, or Combinatorics. We will begin covering these prerequisites before proceeding with the actual topics.

Topics

- What is Security, what is Privacy, and how do they differ?
- Basic statistics and probability: prerequisites to the class
- Perfectly secure communication: security keys, their lengths, and security requirements
- Pseudo-random number generators and their role in cryptography
- Private-key encryption, one-way functions, and their variants
- Formalizing and different levels of security
- Block and stream ciphers: Encryption in the real world
- How to become an IT security consultant
- Privacy: what can never be achieved
- Privacy: making friends with reality and how to compromise what to ask for
- Differentially private databases: constructions and mechanisms
- Weaker notions of privacy: k-anonymity, ℓ-diversity, and their shortcomings
- The legal framework for Privacy and Information Security in the USA

Grading

Here is the breakdown of the final grade.

- **2 Quizzes : 20% (10% each)**
- **3 Assignments : 45% (15 points each)**

- **Term project : 20%**
- **Final exam : 15%**

* **Bonus points:** adds up to 5 points to the final percentage grade

Quizzes are mostly multiple-choice questions and test very elementary understanding of the material. The final exam is a thorough exam with regular format, where you report your answers on a provided notebook. The term project can be either an literature-review based (and comprehensive) or implementation-based.

Preparing the reports, collaboration, missed assignments/tests & remarking requests

- The assignments should be done individually by each student. You are not only allowed but also encouraged to form study groups. Your assignment report must be prepared solely by you (avoid plagiarism).
  What type of collaboration is not considered plagiarism: during your meetings to collaborate for an assignment (i) no electronic collaboration is allowed (you can only meet in person), (ii) you should not discuss the very details of the solutions, and (iii) you are not allowed to take any transcript out of your meeting; i.e. you cannot take with you any notes or any form of electronic record. Then, you let at least one hour pass in between this meeting and you starting preparing your report.
- No late assignments accepted. If there is an acceptable and well-documented reason the instructor will arrange for redistribution of marks.

Attendance and class preparation

According to Rutgers regulations any absence should be reported `https://sims.rutgers.edu/ssra/`. For weather emergencies, consult the campus home page. If the campus is open, class will be held. As typical, you are expected to prepare all assigned readings and do the assigned exercises before each class. The minimum time for preparation for a 3-hour class is *at least* twice as many hours.

Academic integrity

See above what we define as plagiarism. Any deviation from the above is a violation and *all* violations will be pursued. Students are responsible for understanding the RU Academic Integrity Policy `http://academicintegrity.rutgers.edu/files/documents/AI_Policy_2013.pdf`. On all examinations and assignments that you want to be graded, students must sign the RU Honor Pledge, which states, "On my honor, I have neither received nor given any unauthorized assistance on this examination or assignment." You can still give in assignments and exams without this statement, these will be returned corrected, but they will not be graded (default grade: zero).

Support services

If you need accommodation for a disability, obtain a Letter of Accommodation from the Office of Disability Services. The Office of Disability Services at Rutgers, The State University of New Jersey, provides student-centered and student-inclusive programming in compliance with the Americans with Disabilities Act of 1990, the Americans with Disabilities Act Amendments of 2008, Section 504 of the Rehabilitation Act of 1973, Section 508 of the Rehabilitation Act of 1998, and the New Jersey Law Against Discrimination. `https://ods.rutgers.edu`

If you are a military veteran or are on active military duty, you can obtain support through the Office of Veteran and Military Programs and Services. `http://veterans.rutgers.edu/`

If you are in need of mental health services, please use our readily available services. (Rutgers University - Newark Counseling Center: `http://counseling.newark.rutgers.edu/`)

If you are in need of physical health services, please use our readily available services. (Rutgers Health Services - Newark: `http://health.newark.rutgers.edu/`)

If you are in need of legal services, please use our readily available services: `http://rusls.rutgers.edu/`