Interdisciplinary Workshop on Data Privacy 2014 Abstracts

Data Anonymization: A Tutorial

Josep Domingo-Ferrer, Universitat Rovira i Virgili

We survey the challenges and methods related to protecting the privacy of data subjects/respondents by anonymizing their answers before release. We consider the various data formats that need anonymization (tables, on-line databases, microdata) and we sketch the main anonymization approaches. Finally, we discuss how to evaluate the utility and the protection offered by the anonymized data, including a description of the main privacy models in use.

Software engineering for mobile privacy

Bashar Nuseibeh, The Open University (UK) and Lero (Ireland)

The talk will primarily focus on our empirical studies of mobile users and the privacy issues that they may encounter.

On information theoretic metrics for security and privacy

Flávio du Pin Calmon, MIT

There is a natural duality between inference and security (privacy). By using results from information theory, statistics, inference and estimation theory, we explore this relationship and investigate what would be the optimal strategy an adversary would use to learn (infer) some secret information from the output of a system and, simultaneously, measure the worst-case information leakage. We then introduce a few security schemes that are designed to minimize the maximum amount of information that an adversary can gain.

Going Beyond Access Control in Social Networks

Barbara Carminati, University of Insubria

With the increasing popularity of On-line Social Networks (OSNs), protection of personal data has earned attention in the research community. This has resulted in many proposals, ranging from access control models to tools for privacy settings suggestion. However, the social web vision requires deeply rethinking access control and privacy enhancing technologies, both in terms of models and architectural solutions for their enforcement. In this talk, after an introduction to the problem of data protection in OSNs, we will discuss the most challenging research questions and issues.

Four years a SPY - Lessons learned in the interdisciplinary project SPION (Security and Privacy in Online Social Networks)

Bettina Berendt, KU Leuven, Belgium

The research project SPION (funded till the end of 2014) set out to advance the state of the art in security and privacy protection in online social

networks by means of technological, legal, educational, sociological, and behavioural economics approaches. In addition, its aim was to reach out to societal actors. Three computer-science partners represented a wide spectrum of technological approaches, including cryptography, traffic analysis and access control. Our subgroup's aim was to design and build "privacy feedback and awareness tools" based on data mining users' own data with a view to raising their awareness of privacy issues. The project brought together many people with a long research history into privacy issues with others for whom this topic was very new.
In this talk, I give a - necessarily - subjective account of some important developments in this project and the discussions and insights that went along with it, developments that I hope can be an inspiration to others setting out on a journey into the topic of privacy. The topics of my talk include (1) our tool FreeBu, which employs community detection algorithms and graphical interactivity towards facilitating audience management, and lessons learned from our choices regarding empirical evaluation; (2) the widening of the scope of our research from privacy to anti-discrimination, exploring discrimination-aware data mining and its opportunities and limitations; and (3) a turn to (especially school) privacy education in which we explore how to combine "informatics" with "civic education" in a way that takes both areas seriously. I look forward to your comments, questions, doubts, and more!

Privacy Vulnerability Detection
Aris Gkoulalas Divanis and Stefano Braghin, IBM Research
We will present our work in the area of automatic privacy vulnerabilities' identification. He will discuss motivation for the research, the state-of-the-art in this area, explain our proposed approach and provide experiments that demonstrate improvement.

Differential Privacy in Metric Spaces
Ollie Mason, Maynooth University
We will begin by describing a general framework for differential privacy, making only minimal assumptions on the data. This framework includes mechanisms that operate by first sanitising the data and then answering queries (so-called sanitisation mechanisms) as well as mechanisms that respond to individual queries by suitably perturbing the output. We will illustrate by example how numerical, categorical and functional data can be handled in this framework. Time permitting, linear algebraic aspects of privacy for contingency tables and smart metering will also be discussed.