Title: Identification and information leakage on the Web

Abstract:
In the last decade, social media have become a mass phenomenon, which refers to the social Web and mobile social apps. The use of quantified self devices has made this phenomenon even more significant. This entails a huge amount of user data that is shared, collected and exchanged among users and applications. Data sharing has the drawback of privacy risks. Authorization protocols and cryptographic systems may not be enough to ensure that user data are not used for non-legitimate purposes.

One of the risks concerns the aggregation and mining of public and authorized user data to discover unlinked identities of the user and to infer information that the user may not want to share.

What people often typically ignore is that combining data gathered from different sources makes it possible to obtain a very precise picture of their personal information, preferences and tendencies. This issue concerns public data but also data shared among third party applications.

This raises some important questions. How can users defend their privacy and what are the main risk factors? Does the average user really care? If they do, how can they defend themselves? And if they do not, is it possible to raise their awareness by showing them the possibilities and risks?

This speech will present some studies and approaches that my work has addressed in the last years with different research groups, concerning inference risks in social networks and mobile social apps. The aim of these works is to provide users with supporting tools to make them more aware of privacy risks and make the process of information sharing more informative.