AVVISO DI SEMINARIO

Riccardo Lazzeretti

Signal Processing in the Encrypted Domain for Privacy Preserving Applications

Giovedì 2 Febbraio 2017, h 11:00 in Aula Magna

Abstract:
Recent advance in Secure Multi-Party Computation (SMPC) and Homomorphic Encryption (HE) opened the way for several privacy preserving applications. However such techniques have high complexity and needs to be used in a clever way. In this seminar an introduction to the topic and some possible applications are provided, focusing principally in privacy preserving biometric authentication and privacy preserving consensus algorithm for decentralized information fusion.
The first application aims to solve privacy issues related to the use of user's biometric in remote authentication protocols. Biometric data are inherent parts of a person's body and cannot be replaced if they are compromised. Even worse, compromised biometric data can be used to have access to sensitive information and to impersonate the victim for malicious purposes. Processing biometric signals in the encrypted domain provides a secure and elegant way to overcome the aforementioned problems. Thanks to SMPC techniques, it is possible to carry out the match between any two biometric templates by working only on encrypted data, but the high complexity prevents their use in practical applications, hence a it is necessary that the underlying biometric processing algorithms and the STPC protocol are designed jointly by taking into account both the cryptographic and the signal processing facets of the problem.
The second application focuses on the protection of sensor privacy in distributed environments, where a central coordination node is missing. In the area of Internet of Thing (IoT), to deal with a large amount of information, and provide accurate measurements, service providers adopt information fusion, which can be performed by means of consensus algorithms. These algorithms allow distributed agents to (iteratively) compute linear functions on the exchanged data, and take decisions based on the outcome, without the need for the support of a central entity. However, data fusion raises several security concerns, especially when private or security critical information are involved in the computation. ODIN is a novel algorithm based on the popular consensus gossip algorithm that allows information fusion over encrypted data and prevents distributed agents have direct access neither to the data while they iteratively reach consensus, nor the final consensus value, but they can only retrieve partial information, e.g., a binary decision.

Short bio:
Riccardo Lazzeretti graduated with a degree in computer science engineering from the University of Siena, Italy, in 2007, where he continued his studies as a Ph.D. student under the supervision of Prof. Mauro Barni in the Information Engineering Department. From November 2009 to May 2010, he was with Philips Lab in Eindhoven, The Netherlands. In 2012, he received a research grant and continued his research in the Information Engineering and Mathematics Department of the University of Siena. From September

2016 he is continuing his research activities in the Mathematical Department of the University of Padua together with Prof. Conti. His research activity is mainly focused on privacy-preserving applications based on secure two-party computation tools. He authored several scientific papers, appeared in the proceedings of top-level international conferences and journals, and is regularly invited as a TPC member to the top-level conferences in his areas of interest. He is associate editor of "Elsevier Journal of Information Security and Applications", Program Co-Chair of "51th IEEE International Carnahan Conference on Security Technologies (ICCST 2017)" and ˆ Workshop chair of "IEEE International Conference on Advanced and Trusted Computing (ATC 2017)". He has been assistant in various courses at academic level.