In Favour of Posting

THE CHINESE UNIVERSITY OF HONG KONG

Department of Information Engineering

Seminar

Secure Multiparty Computation versus Secure Outsourcing

By

Prof. Yvo Desmedt

University of Texas at Dallas, USA

Date : 26th April, 2019 (Fri)
Time : 15:30pm – 16:30pm
Venue : Room 801, Ho Sin Hang Engineering Building
The Chinese University of Hong Kong

Abstract

The lecture starts with explaining Secure Multi-Party Computation (MPC). Then we explain the rise of cloud storage, cloud computing and social networks. We regard it as a consequence of a failure in the design of adequate OS (operating systems). We survey some of the solutions proposed to address security problems on the cloud.

This presentation is focused on analyzing whether MPC is the correct technique for this problem. Moreover, besides issues as speed, we show that other problems pop up that are irrelevant in a typical MPC setting.

Biography

Yvo Desmedt is the Jonsson Distinguished Professor at the University of Texas at Dallas, a Honorary Professor at University College London, a Fellow of the International Association of Cryptologic Research (IACR) and a Member of the Belgium Royal Academy of Science. He received his Ph.D. (1984, Summa cum Laude) from the University of Leuven, Belgium. He held positions at: Universite de Montreal, University of Wisconsin - Milwaukee (founding director of the Center for Cryptography, Computer and Network Security), and Florida State University (Director of the Laboratory of Security and Assurance in Information Technology, one of the first 14 NSA Centers of Excellence). He was BT Chair and Chair of Information Communication Technology at University College London. He has held numerous visiting appointments. He is the Editor-in-Chief of IET Information Security and Chair of the Steering Committee of CANS. He was Program Chair of e.g., Crypto 1994, the ACM Workshop on Scientific Aspects of Cyber Terrorism 2002, and ISC 2013. He has authored over 200 refereed papers, primarily on cryptography, computer security, and network security. He has made important predictions, such as his 1983 technical description how cyber could be used to attack control systems (realized by Stuxnet), and his 1996 prediction hackers will target Certifying Authorities (DigiNotar was targeted in 2011).

**** ALL ARE WELCOME ****

Host: Sherman S. M. Chow (Tel: 3943-8376, Email: sherman@ie.cuhk.edu.hk)
Enquiries: Information Engineering Dept., CUHK (Tel.: 3943-8385)