In Favour of Posting

香港中文大學
The Chinese University of Hong Kong

Institute of Theoretical Computer Science and Communications

ITCSC-CSE Joint Seminar

Authentication in Constrained Settings

By
Prof. Katerina Mitrokotsa
Assistant Professor, Department of Computer Science and Engineering,
Chalmers University of Technology

June 20, 2014, Friday
11:00 am – 12:00 noon
Room 1009, William M. W. Mong Engineering Building, CUHK

Abstract:
Access to restricted services and/or places requires authentication. However, authentication is sometimes performed in: i) noisy conditions, ii) hostile environments and iii) constrained settings. By noisy conditions, we refer to noise in the communication channel that may lead to modification of the transmitted information. By hostile environments we mainly refer to environments where attackers may attempt to impersonate legitimate users, while by constrained settings we refer to environments that may include communication among wireless devices with limited resources.

Authentication is a decision making problem where we need to decide whether or not to accept the credentials of an identity-carrying entity. In the context of cryptographic authentication, we have extensively investigated the family of distance bounding protocols. These can be used as the main countermeasure against relay attacks. We analyse the security of such protocols. These authentication problems will also be briefly connected to the problem of privacy-preservation.

Biography:
Prof. Katerina Mitrokotsa is an assistant professor at the department of Computer Science and Engineering at Chalmers University of Technology. Her main research interests lie in information and network security, privacy-preservation, machine learning for security and applied cryptography. Formerly, she held positions as a Marie Curie fellow at EPFL, as professor at the University of Applied Sciences of Western Switzerland (HES-SO), as a postdoctoral researcher in TU Delft and as a visitor assistant professor at the department of Computer Science at Vrije Universiteit in Amsterdam. She has been awarded the Rubicon Research Grant by the Netherlands Organization for Scientific Research (NWO) and a Marie Curie Intra European Fellowship.

Currently, among others she serves as associate editor for the IEEE Communications Letters and the Computers & Security Journal (Elsevier). She has served on the PCs of INFOCOM, ACNS, Africacrypt, Indocrypt and multiple other well-known conferences in the area on communications and information security.

******* ALL ARE WELCOME *******

Hosted & Enquiries : Institute of Theoretical Computer Science and Communications Tel: 3943 1257