In Favour of Posting

THE CHINESE UNIVERSITY OF HONG KONG
Department of Information Engineering

Seminar

Next Generation Trusted Platform Modules (TPM2.0)

by

Dr. Liqun Chen
Hewlett-Packard Laboratories
United Kingdom

Date : 11 April, 2014 (Friday)
Time : 3:00pm - 4:00pm
Venue : Room 1009 William M.W. Mong Engineering Building
The Chinese University of Hong Kong

Abstract

This talk is about trusted computing, the next generation of trusted platform modules (TPM2.0) and the cryptographic algorithms that are supported by them. After briefly describing the background of trusted computing and trusted platforms, we will discuss TPM2.0 and the cryptographic algorithms that it supports. The design target for TPM2.0 was high performance in hardware and we illustrate the design process used to achieve this by considering the development of the TPM2.0 digital signature primitive. This is a simple elliptic curve signature scheme and can be used to generate different types of signatures. Two known applications of this primitive are direct anonymous attestation (DAA) and U-Prove.

Biography

Liqun Chen is a researcher at Hewlett-Packard Laboratories. She has developed several cryptographic schemes adopted by International Standards and some of them have been implemented in Trusted Platform Modules (TPM). She has an extensive publication record and holds 46 granted US patents in cryptography and information security. Liqun has served as editor, or co-editor, for six ISO/IEC standard documents. She also serves as an associate editor of IEEE Transactions on Information Forensics and Security and an editorial board member of International Journal of Information Security. Liqun obtained her BSc, MSc and PhD in Engineering from Southeast University. Prior to joining HP, she worked at Southeast University, the University of Oxford and Royal Holloway, University of London.

**** ALL ARE WELCOME ****

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