

COMPUTER SCIENCE SEMINAR SERIES

Department of Computer Science
City University of Hong Kong
(Departmental Seminar Seminar 2007/2008 - No 4)

BR-model extended to password setting --Authenticated Key Exchange Secure Against Dictionary Attacks

Mr JIN Haimin
PhD Student
Department of Computer Science
City University of Hong Kong

Date :

25 September 2007 (Tuesday)

Time :

12:00noon - 1:00pm

Venue :

CS Seminar Room, Rm Y6405, 6th Floor Yellow Zone, Academic Building, City University of Hong Kong, Tat Chee Avenue, Kowloon Tong.

Abstract

Password Authenticated Key Exchange (PAKE) allows users to use low-entropy passwords to establish mutually authenticated secure channel without being compromised by online/offline dictionary attacks. In this talk, we review a formal adversarial model for PAKE proposed by Bellare et al. in Eurocrypt 2000. The model can be considered as an extension to the Bellare-Rogaway model (BR-model) for cryptographically-strong key establishment and authentication protocols. In particular, we go through the model details and illustrate how the model can be used to facilitate security proofs for PAKE schemes.

Supervisor : Dr Duncan Wong (CS)

Research Interests : Applied Cryptography, Cryptographic Algorithms and Protocols, Information Security, Network Security, Wireless Security, E-Commerce Technology

All are welcome!

* * * * *

In case of questions, please contact Dr Duncan Wong at Tel: 2788 8020, E-mail: duncan@cityu.edu.hk, or visit the CS Departmental Seminar Web at <http://www.cs.cityu.edu.hk/>.