Department of Computer Science, The University of Hong Kong

CS Seminar

Analysis of Human Identification Protocols

Professor Josef Pieprzyk
School of Electrical Engg and Computer Science
Queensland University of Technology
Australia

Date:
December 6, 2017
Wednesday
2:30 pm

Venue:
Room 328
Chow Yei Ching Building
The University of Hong Kong

Abstract:
Human identification protocols are challenge-response protocols that rely on human computational ability to reply to random challenges from the server based on a public function of a shared secret and the challenge to authenticate the human user. One security criterion for a human identification protocol is the number of challenge-response pairs the adversary needs to observe before it can deduce the secret. In order to increase this number, protocol designers have tried to construct protocols that cannot be represented as a system of linear equations or congruences.

In the talk, we take a closer look at different ways from algebra, lattices and coding theory to obtain the secret from a system of linear congruences. We then show examples of human identification protocols from literature that can be transformed into a system of linear congruences. The resulting attack limits the number of authentication sessions these protocols can be used before secret renewal.

About the Speaker:
Josef Pieprzyk is a Professor in School of Electrical Engineering and Computer Science at Queensland University of Techology. His main research interest focus is Cryptology and Information Security and includes design and analysis of cryptographic algorithms (such as encryption, hashing and digital signatures), secure multiparty computations, cryptographic protocols, copyright protection, e-commerce, web security and cybercrime prevention. Professor Pieprzyk is a member of the editorial boards for International Journal of Information Security, Journal of Mathematical Cryptology, International Journal of Applied Cryptography, Fundamenta Informaticae, Journal of Research and Practice in Information Technology, International Journal of Security and Networks and International Journal of Information and Computer Security. Professor Pieprzyk published 5 books, edited 10 books (conference proceedings published by Springer), 6 book chapters, and more than 300 papers in refereed journals and refereed international conferences.

All are welcome!
For enquiries, please call 2859 2180 or email enquiry@cs.hku.hk
Department of Computer Science
The University of Hong Kong