In Favour of Posting

THE CHINESE UNIVERSITY OF HONG KONG
Department of Information Engineering

Seminar

Privacy-Preserving DRM

by

Dr. Radia Perlman
Fellow
Sun Microsystems

Date : 10 November, 2009 (Tue.)
Time : 2:30pm-3:30pm
Venue : Room 833, Ho Sin Hang Engineering Building
The Chinese University of Hong Kong

Abstract

This talk describes several methods for allowing a user to purchase digital content without revealing to anyone what specific item is being purchased. The talk first presents two basic schemes, one based on anonymous cash, and the other based on blind decryption, and compares them according to criteria such as efficiency and functionality. Then other features are introduced, such as having different items cost different amounts, or having additional authorization required for some items (such as "over age 21" or "citizen of US"). Then we discuss a deployment scenario in which all communication between the content provider and the user is done via a sealed box, provided by the content provider. We show that if the user can only passively monitor communications, there is no way for the user to be able to detect if the box is informing the content provider about the user's purchases. However, we demonstrate a way in which the user can interact with the box, and cooperatively construct messages to be transmitted, in such a way that the DRM concerns of the content provider cannot be circumvented, but yet there is no opportunity for covert channels between the box and the content provider.

Biography

Radia Perlman is a Fellow at Sun Microsystems. She designed the spanning tree algorithm that is the heart of bridge technology, the routing algorithm IS-IS, which will be the heart of TRILL, and did the design from which TRILL has evolved. Her research interests also include network security protocols. She is the author of two textbooks: "Interconnections" (about layer 2 and 3 technology) and (with 2 coauthors) "Network Security: Private Communication in a Public World". She has a PhD in computer science from MIT.

**** ALL ARE WELCOME ****

Host: Professor Dah-Ming Chiu (Tel: 2609-8357, Email: dmchiu@ie.cuhk.edu.hk)
Enquiries: Information Engineering Dept., CUHK (Tel.: 2609-8385)