New cryptographic schemes with application in network security and computer forensics

Ms Jiang Lin

Abstract:

Nowadays, the Internet facilitates daily business and activities for companies and governments. However, accompanying the convenience provided by the Internet are the increasingly serious new security problems and challenges. The thesis addresses two particular security problems by applying solutions that utilize a large number of cryptographic objects. The first problem addressed is about the delegation of digital signing power in real world situations. The first part of the seminar introduces a new provable-security ($t_{1/n_1-t_{2/n_2}}$) distributed threshold proxy threshold signature scheme, which enables the original signer group to freely designate proxy signers after the delegation task is required. In other words, there is no need to pre-define the delegation infrastructure. The proxy signature can be generated by a combination of any $t_{2}$ individual participants with their secret keys. The second problem comes from the requirement of an efficient and accurate verification scheme for hard disk integrity in computer forensics. The second part of the seminar proposes a cylinder-head-sector hashing scheme (CHS for short) to calculate hash values for the sectors in the same cylinder, head and track. Then a more general hashing scheme that does not consider the physical structure of hard disk, k-Dimension hashing scheme (k-D for short), is proposed. It assigns all sectors into k-dimension spaces logically with the same sector present in k chains. Even with bad sectors, there is still a high probability that the integrity of unaffected sectors can be verified. The experiments undertaken on our implemented k-D scheme show that both the time for computing the hash values and the storage space for the hash values are reasonable.

About the Speaker:

Lin JIANG is a PhD student of Dr. Lucas Hui. Her research interests include applied cryptography, computer forensics and network security, focusing on proxy signature and data integrity checking.

Date & Time:
April 27, 2010
Tuesday
11:00 am

Venue:
Room 313
Chow Yei Ching Building
The University of Hong Kong

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