Enhancing security on MAC and multiparty computation

KUCHING: Ways and methods to enhance cryptographic message authentication code (MAC) and security on multiparty computation were hot topics discussed on Day 2 of ASIACRYPT 2007 here yesterday.

Experts from big corporations such as 3G provider Nippon Telegraph and Telephone Corporation (NTT) and computer processor giant Advanced Micro Devices, Inc (AMD) were joined by academicians in exploring new ideas to secure encrypted data in computers and networking.

Yesterday's sessions only started in the afternoon as speakers and attendees took the morning off to visit Semenggok Wildlife Rehabilitation Centre and Kampung Annah Rais.

NTT Japan's Kan Yasuda kicked off the session on MAC and Implementation by presenting a paper on Boosting Merkle-Damgard Hashing for Message Authentication.

Two researchers G Jakimoski and KP Subbalakshmi from Stevens Institute of Technology then presented their paper entitled 'On Efficient Message Authentication via Block Cipher Design Techniques'.

This was followed by Symmetric Key Cryptography on Modern Graphics Hardware by AMD's software engineer Jason Yang. The session was chaired by Thomas Johanssen from University of Lund, Sweden

Seoul National University's Jung Hee Cheon then chaired a session on Multiparty Computation after a short break.

Matthew Green from John Hopkins University talked about Blind Identity-Based Encryption

and Simulatable Oblivious Transfer and this was followed by another academician Payman Mohassel (Department of Computer Science, University of California) talking on Multi-Party Indirect Indexing and Applications.

Researchers from Computer Science Department, Columbia University and RSA Laboratories, also based in United States, were the final presenters with their paper, Two-Party Computing with Encrypted Data.

The day was rounded up with a rump session, which is basically informal discussions and demonstration of computer skills.

Today, there will be sessions on block-cipher multiparty computation II, foundation and a keynote talk on Authenticated Key Exchange and Key Encapsulation in the Standard Model.

Chief Minister Pehin Sri Abdul Taib Mahmud is expected to deliver his official remarks at a dinner banquet hosted by the State at a leading hotel here today.