Audience spellbound by renowned speaker

Cryptographer Vaudenay among top experts at ASIACRYPT 2007

By Samuel Aubrey

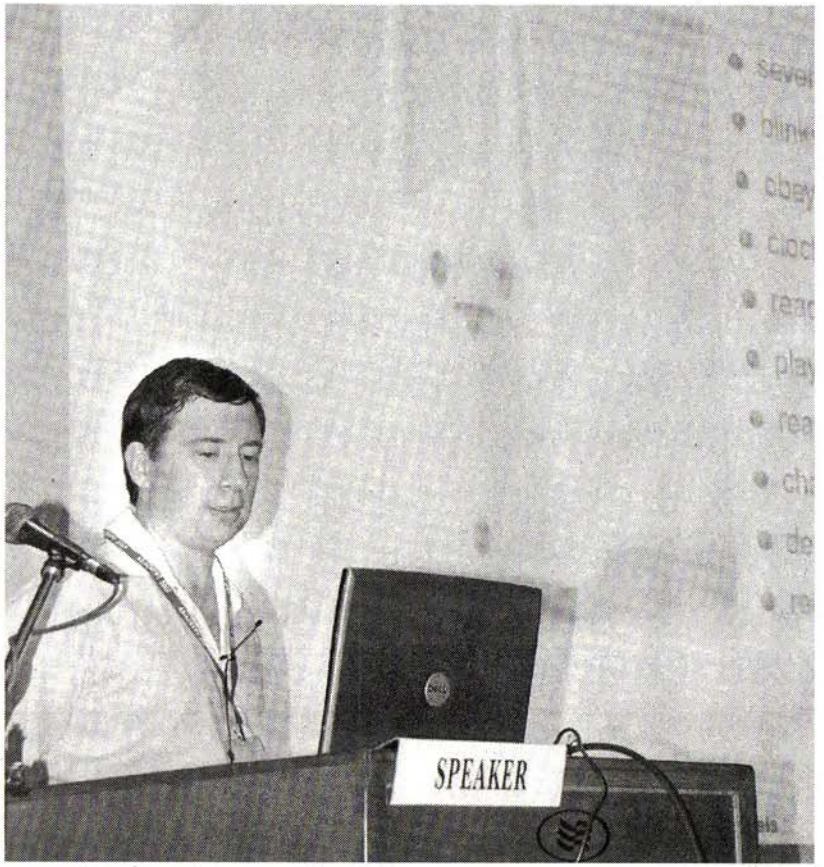
KUCHING: One of the world's renowned cryptographers Serge Vaudenay was among the renowned speakers at the International Conference on the Theory and Application of Cryptology and Information Security, ASIACRYPT 2007 in Kuching.

On Monday, which was also the first day of the conference, he chaired a session on Number Theory and Elliptic Curve, and later presented a paper on 'Privacy Models for Radio-frequency identification (RFID)'.

Vaudenay, a professor at École Polytechnique Fédérale de Lausanne (EPFL), or Swiss Federal Institute of Technology, was one of the many experts in cryptology and information security invited to Kuching.

The 39-year-old Frenchman has published several papers related to cryptanalysis and design of block ciphers and protocol. He is also one of the authors of the IDEA NXT (FOX) algorithm together with Pascal Junod.

Amongst his achievements was the discovery of a severe vulnerability in the SSL/TLS protocol, following the attack he forged, and which leads to the interception of the password.



INTERESTING PRESENTATION: Serge Vaudenay presents his paper on Privacy Models for Radio-frequency identification (RFID). — Photo by Johnathan Bullet

He also published a paper about biased statistical properties in the Blowfish cipher and is the author of the best attack on the Bluetooth cipher: E0.

In 1997 he introduced the decorrelation theory, a system for designing block ciphers to be provably secure against many cryptanalytic attacks.

He has been at the lead of the Laboratory of Security and Cryptography (LASEC) of EPFL, which is in the heart of Europe and is one of Europe's leading institutions of science and technology.

The four-day ASIACRYPT 2007 is being organised in Kuching by the Information Security Research (iSECURES) Lab of Swinburne University of Technology (Sarawak Campus) and the Sarawak Development Institute (SDI), with support from the Sarawak government.

Cryptology is the practice and study of hiding information. In modern times, cryptology is considered to be a branch of both mathematics and computer science, and is affiliated closely with information theory, computer security and engineering.

It is used in applications present in technologically advanced societies; examples include the security of ATM cards, computer passwords, and electronic commerce.

Some 170 experts from universities and industry players from 30 countries from as far as Europe and North American regions are participating in the conference.