Frenchman wins Best Paper Award

KUCHING: Papers presented at the ASIACRYPT 2007 here could very well have a bigger impact towards enhancing cryptographic hash functions of various information security applications worldwide.

One of them entitled Cryptanalysis of Grindahl by a young PhD student from France Thomas Peyrin (pictured right) which was also adjudged the winner of the Best Paper Award.

Peyrin, currently with France Telecom Research and Development and Japan's National Institute of Advanced Industrial Science and Technology, said the present hash functions have been broken and thus exposed to attacks.

This is following successful collision attacks recently demonstrated by a team from Shandong University, China which proves its vulnerability and thus increased the need for better and enhanced hash functions.

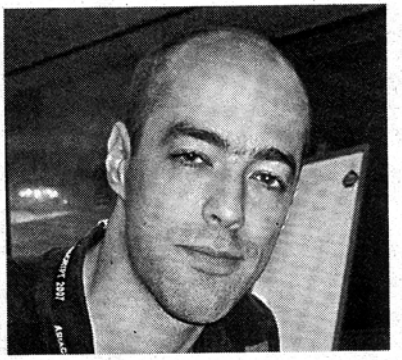
"Nowadays, hash function is a very hot topic among cryptographers worldwide and everybody is trying to build better ones. It is important to have very good hash function to better protect information security applications," said the 25-year-old, who will return to France in the next three months to complete his PhD at University of Versailles.

According to Peyrin, hash functions are used to do digital signature in various information security applications, such as authentication and message integrity, and password database.

On peer-to-peer filesharing networks, hashes are also used to identify files, providing sufficient information for locating file sources, downloading the file and verifying its content.

Peyrin said his research was based on the Grindahl hash functions, which were collection of highly parameterizable hash functions of which two specific instances had been proposed earlier this year.

This morning, his paper will be among the last three to be presented before the conference is adjourned.



The other two final papers are Cryptanalysis of the Tiger Hash by Florian Mendel (Institute for Applied Information Processing and Communications (IAIK) and Vincent Rijmen (Graz University of Technology, Austria) and A Key Recovery Attack on Edon80 by Martin Hell and Thomas Johansson from Lund University, Sweden.

The next conference, ASIACRYPT 2008, will be held in Melbourne, Australia in December next year.