A JOB WELL DONE: Phan (seated seventh right) with the organisers, speakers and delegates of ASIACRYPT 2007 pose for a group photograph at the end of the conference.

Raphael traces his career in cryptology

Samuel Aubrey
someoftest_team@yahoo.com

THE film 'Hackers' starring a young Angelina Jolie had a famous line that goes "Mess with the best, die like the rest".

Portraying hackers as cool and hip, the film showed how disorderly and unstable the society could become when vital information kept on online computer systems and databases were breached — and tampered with.

But where there is problem there is an answer; enter cryptology, which is the practice and study of hiding information from hackers. 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.

Studies on encoding and decoding information and messages in order to secure them are becoming vital these days, due to higher dependence on online systems to manage information and even to do business and banking transactions.

Sarawakian Dr Raphael Phan is one of the very few Malaysians making their names in the field of cryptology worldwide.

He is one of the pioneers behind the setting up of Information Security Research (iSECURES) laboratory at Swinburne University of Technology Sarawak Campus, and was its director from 2004 to 2006.

His big move came this year when he moved to Switzerland, to join the École Polytechnique Fédérale de Lausanne (EPFL), which is one of Europe's leading institutions of science and technology.

There, he is a researcher of Laboratory of Security and Cryptography (LASEC), working under well-known French cryptographer Serge Vaudenay.

This month, Kuching became the first Malaysian city to host the Annual International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT), one of the top three cryptologic conferences in the world.

Phan returned to Kuching as the General Chair of ASIACRYPT 2007, in a way finished something he began for he led the team that won the bid for Kuching to host the conference three years ago.

In this interview with thesundaypost, Phan shared his views on the level of cryptology in Malaysia, and his new designation in Switzerland.

... with DR RAPHAEL PHAN

Q: You're a specialist in a field which not many people know or even heard of. What sparked your interest in this field?

A: When I was doing my undergraduate studies, there was a course, subject in this area. I found the ideas and techniques very intriguing. And I also realise that not many Malaysians work in this field. Basically if you want to excel in something, you have to be above the rest, and find your own niche.

Q: Was it when you were studying in Multimedia University (MMU)?

A: I was studying in MMU, where I graduated with B. Eng (Hons) degree in Electronics majoring in Computer Engineering. This was when I grew interested in cryptology. I then completed my M. EngSc. (Research) on "Cryptanalysis of the Advanced Encryption Standard (AES) and Skipjack" also in MMU. And then Ph.D (Eng) on "Cryptanalysis of Block Ciphers: Generalization, Extensions & Integrations", also in MMU.

Q: You were one of those who pioneered the formation of iSECURES in Swinburne Sarawak. How did that come about?

A: As I said, because there are not many researchers doing cryptology in Malaysia. After discussion with colleagues, we decided a formal set-up where we can work among ourselves and external parties in an effort to bring the security level of homegrown information security techniques on par with international standards.

Q: On what par are we, in terms of information security techniques?

A: I think not many people realise the importance of cryptology. A lot people just want to know how to use the latest technology in cryptology, rather than wanting to find out how it really works. So, one of the things that we want to achieve when we formed iSECURES was to be at the early part of the process, to be generators of those techniques rather than end users.

Q: Why is there a need to have higher level of cryptology understanding in Malaysia?

A: Just like any military technology, you just don't want to be buyers of technology of other people. You want to able to generate the technology yourself so that you can use it and get money from selling it to somebody else. I think Malaysia is still at an early stage in terms of generating this kind of technology but we in iSECURES are making the first step.

Q: So do you agree with Chief Minister Pehin Sri Abdul Taib Mahmud who said that research and development of information security is the next niche for Sarawak?

A: Yes, Sarawakians can be generators of knowledge and initiators of homegrown cryptologic techniques, rather than just developers and implementers. I believe this is a niche we can participate in. The State government too had shown its commitment by becoming the major financial supporter behind ASIACRYPT 2007, where we managed to attract more than 170 cryptologists from 30 countries to Kuching.

Q: Finally, tell us about your new designation in Switzerland.

A: It's cool there (laughing). It's a nice feeling to feel cool all the time. Cool, fresh air not coming from air conditioning. Other than that, the rest is basically the same. You can buy ingredients from the supermarket, and cook traditional Malaysian Chinese food.

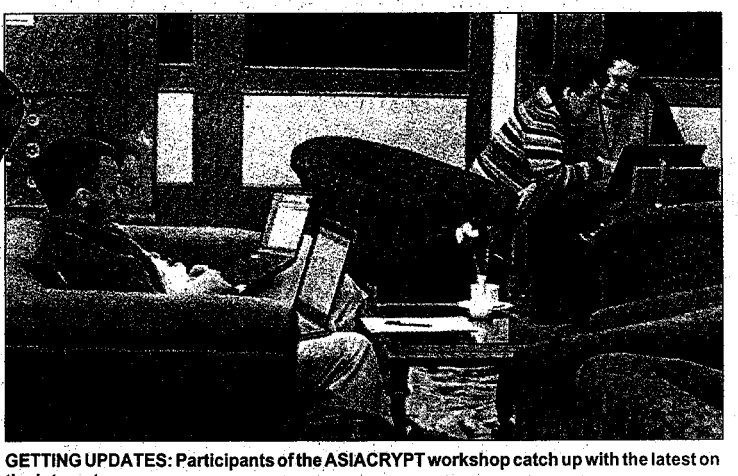
Q: So, you're basically still a home-boy at heart?

A: Still, of course-lah. In the first few months, we had to ask friends to buy stuff for us, then package them and send over to us. My family still very much likes Malaysian food. And we try to retain that identity of ours there.

HARDWORKING TEAM: Phan (right) with members of the ASIACRYPT 2007 organising committee, which also includes Swinburne senior lecturer Dr Dennis Wong (left).

DR RAPHAEL PHAN: Not many people realise the importance of cryptology.

MEETING OF MINDS: Cryptologists from different countries sharing ideas and knowledge at the ASIACRYPT 2007.



GETTING UPDATES: Participants of the ASIACRYPT workshop catch up with the latest on the Internet.