



President's Message



AISP is now one year old. With half the EXCO retired under the constitution, we have new blood being introduced to the team. We warmly welcome Martin Khoo (IDA), Cecil Su (Grant Thornton) and Jimmy Sng (PricewaterhouseCoopers) to the team! We also sincerely thank those who served last year for their invaluable contributions to AISP.

A key milestone was reached in April when we successful co-organised our first flagship conference with IDA. We had a record attendance of nearly 400 participants for the seminar and over 135 participants for the second day's workshop session. Many thanks to Andrew Sansom who chaired the seminar organising committee and his very hardworking and dedicated team members from AISP and IDA (led by Grace Chew) Special thanks to Christina Gan, Senior Director, IDA who has provided tremendous support, resources and guidance to the committee.

This year, a lot of effort will be focused on developing and launching the Body of Knowledge ('BoK'), Infocomm Security Professional Roadmap ('ISPR') and the AISP certification examinations and related training courses. The BoK and ISPR projects are well underway. Planning has also begun for the certification examinations and related courses. As the Institutes of Higher Learning ('IHL') have been actively creating AISP student Chapters in the campuses, AISP will be developing special programmes for them this coming year. Last but not least, we will continue to develop the popular Academic series of seminars and balance this with lighter evening networking events.

I end this short note with a request to all our members to actively promote AISP and reach out to other information security professionals to get them to know us better and to strongly encourage them to join us. We need a strong membership base to achieve our aspirations to be a strong and credible professional body. We need your help to build the foundation stones of success.

Know Your Enemy:

The Singapore HoneyNet Project



The Singapore HoneyNet Chapter was formed back in 2003 in support of the HoneyNet Project alliance based out of Chicago. Its members are volunteers from diverse professional backgrounds coming together in the spirit of information security sharing and collaboration. We have no products, services or employees, and our research is done on a volunteer basis. It is our goal to learn the tools, tactics, and motives of the blackhat community and share these lessons learned. It is hoped that our research will benefit both its members and the security community. Similar to many of the sister chapters, the main goals of the local chapter are to raise awareness, educate members with research and collaborate with other sister chapters.

The Singapore HoneyNet testbed is currently located at a lab space courtesy of one of the local tertiary institution which provided us with physical space and IP space. From here, we have managed to capture various malware and observe different attack vectors spanning from malware to web-based phishing and spam traffic. During the initial phase, some of the team members have also taken to task to document the attack vectors and behavioral aspects of the sequence of activities, which is used to contribute to the country-specific statistics in support of the HoneyNet Project alliance.

Top attacks of Q4 2008

Generally, short of mostly hydra-flux plus fast flux networks (bots), the prevalence of malware strikes and the ever-increasing strain of phishing sites, we have observed the following attack trends hammering away in our local Singapore sensors in the last quarter:

1. Conficker/Downadup worm spread
2. Asprox botnet SQL injection attacks
3. Waledac worm spreads to email attachments and e-postcards
4. Web infections and redirections to malware hosted sites
5. Malicious Flash and PDF used in Adobe plug-ins
6. MS08-067 exploit in the wild attempts

Moving forward

Currently, there are a few activities which the local chapter have been getting involved in with various organizations in the honeynet world. Some of the upcoming activities that the team will be undertaking include but not limited to the following:

1. engaging in the GDH (Global Distributed HoneyNet) Phase 2
2. identifying malicious web pages that launch drive-by-download attacks by inspecting static heuristics on the page denoted by the URL
3. analyzing MMORPG vulnerabilities - trojans targetting account information
4. collaboration with a Japanese security think-tank organization
5. malware analysis

For more information on the Singapore HoneyNet Project, please visit <http://www.honeynet.sg/>. A new KYE (Know Your Enemy) paper detailing the analysis and containment of the Conficker worm has just been released by one of the chapters, and this can be downloaded from our link or the main site.

For e-mail queries and feedback: cecil.su@honeynet.sg

Privacy & Security in Singapore's Healthcare Sector



On 17th February 2009, Singapore General Hospital (SGH) the oldest (established in 1821) and largest acute tertiary hospital and national referral centre in Singapore, together with Singapore Telecommunications Limited (SingTel), and HSAGlobal announced their successful pilot of the Community Care Management Solution (CCMS), an electronic health record and management system that makes patient data available to health care providers across the island state. The use of technology is not new.

For example Short Messaging Service (SMS) are widely used to remind patients of upcoming hospital appointments and even your queue status if you are within the hospital's grounds. Essentially, the solution has the following features:

1. The patient's complete health information as in the case notes and not just the discharge summary can be shared across the continuum of care providers including step down providers such as polyclinics and those in community care settings;
2. Health care providers similarly can access the information through their personal computers or PDAs to view and to update a patient's records as well as to share them with similar providers; and
3. The solution is offered as a Software as a Service (SaaS) model, for health care providers to use the service by paying a monthly subscription fee.

Looking to the future, patients can access, view, receive timely update and test results through an online portal. If the patient uses a monitoring device, then information such as blood glucose and weight from the device can also be uploaded to the portal, allowing healthcare providers to provide timely medical advice so as to prevent serious problems from developing.

What is unique here is that the solution is available in Singapore where there is no specific legislation governing the privacy of personal information per se, such as the Personal Data Ordinance (Hong Kong) or one pertaining to personal health information such as HIPAA (US).

Currently personal information is protected on an industry or sector specific level (the banking sector for example); although there is a general code on protecting personal information, The Model Data Protection Code, based on the OECD Guidelines. Meanwhile the Government has reportedly formed an inter-ministry committee to review the issue and to find a way that can protect an individual's personal data and addresses at the same time issues relating to privacy concerns, commercial requirements and other national interests.

The efforts by SGH and her partners are laudable in terms of providing better health care service for the patients and health providers as well. The solution as it stands raised a number of legal, security and privacy related issues:

a) Is the patient's consent given to the hospital on a blanket one time basis, therefore allowing the information to be subsequently released to a third party (a step down health care provider for example) or do we need to consult the patient each time before the information is released to a potential health care provider? What happens when the patient changes his or her health care provider and what is the requirement in relation to protecting the information held by the previous health care provider?

b) In the event of any mistake entered by the patient and or in conjunction with a third party health care provider on the online portal and a treatment is given by an innocent third party doctor based on the information, who then will be responsible for the adverse medical treatment of the patient?

c) How is security ensured across the whole continuum of those who possess the health information of the patients? For example, if a physician chooses to download a patient's information on his or her PDA and the device was subsequently stolen?

Perhaps a Singapore version of HIPAA or sometime akin to it to address the many inter-related legal, security and privacy issues may be needed as the next logical step to undergird these laudable efforts by the hospital and her providers.

KK Lim is a Senior Lecturer at School of Information Technology, Nanyang Polytechnic, Singapore. He also serves on the Association of Information Security Professionals in Singapore (AISP) and the editorial review board of The Journal of Information Privacy and Security. This article is written in his personal capacity and the author can be reached at kklim@live.com.sg.

This article was originally published in the International Association of Privacy Professionals monthly newsletter, the Privacy Advisor.

AISP 1ST Annual General Meeting 25 March 2009

AISP held the 1st Annual General Meeting on 25 March 2009 at SCS Resource Centre. AISP President, Mr Gerard Tan, presented the activities organized during work year 2008/2009, before paving way for the election of the Executive Committee for 2009/2010.

A big thank you to the Committee Members and the outgoing Committee Members for your commitment, passion, and personal dedication in running AISP, activities, programmes and our events throughout your appointment!



Backrow: Andrew Sansom(Committee Member), Tan Wei Chong(Committee Member), Paul Ng(Committee Member), John Tan(Committee Member), Jimmy Sng(Committee Member), Cecil Su(Committee Member)
Frontrow: Josephine Tan(Treasurer), Martin Khoo(Vice President), Gerard Tan(President), Freddy Tan(Vice President), Douglas Tang(Secretary)
Absent: George Wang(Vice President)

Take a look at our happenings at AGM!



AISP-IDA Information Security Seminar 2009

AISP and IDA jointly organized the 1st Information Security Seminar 2009 on 2nd April. The event "Managing Information Security Threats in a Changing World" received overwhelming response with nearly 400 participants attended the seminar, held at Suntec Singapore International Convention & Exhibition centre. We put together a panel of eminent overseas and local speakers and shared their insights in combating Information Security threats.



The workshop held on 3rd April at Nanyang Polytechnic, was well attended over 135 participants. Dr Eugene Schultz, Chief Technology Officer and Chief Information Security officer high tower Software, USA, gave a very comprehensive yet humorous course on "Incident Response and Forensics".



Calendar of Events

Event	Date	Venue
Career Talk by Andrew Sansom	6 May 2009	Singapore Computer Society
Career Talk by WDA	14 May 2009	Singapore Computer Society