Yui Kee Computing Ltd.

# Newsletter

April 2009

## Contents



## Security Humour

*<web-link for this article>*

xkcd reveals the secret of security questions.

**More Information**

Security Question

## Legco Panel Discusses .hk Administration

*<web-link for this article>*

*Allan Dyer*

On the 7th April 2009 I attended the Legco Panel on Information Techniology and Broadcasting, to present the Hong Kong Computer Society's views on the Review of the Administration of internet domain names in Hong Kong.

There were fourteen delegations, including Sir John Strickland, representing the HKIRC, who said he was there to listen.

Major themes in the views were transparency, accountability and the Regsitry- Registrar model. Other delegations that mentioned the Registry-Registrar issue were wholly in favour, and concerned with the delay in introducing it, in contrast to the view I put that there needs to be more consideration of whether it actually benefits Hong Kong.

Some views were contradictory: one organisation thought the current arrangements for becoming an HKIRC member were too difficult and wanted to make membership of HKIRC automatic for domain name holders. Tiglion, an ISP, said they did not want to be forced to become an HKIRC member, and considered it a direct contravention of Article 27 of the Basic Law of HKSAR that guarantees freedom of association.

The Legislators, including Hon Ronny TONG Ka-wah, Hon Cyd HO Sau-lan, and Hon Emily LAU Wai-hing, were particularly interested in the status of the draft MOU, the confidential

parts of the Consultant's Report, and the submission from the Hong Kong Human Rights Monitor (who did not attend the meeting) and freedom of speech.

On the effects on free speech, Sir John Strickland pointed out that HKIRC was just a small company with the sole purpose of associating names with numbers: once you have a domain name, they have no control over the content. He did not discuss how HKIRC de-registered over 8000 domain names that were being used for spam-related activities. This directly relates to the HKCS view that .hk domains should be subject to Hong Kong law, and the Human Rights Monitor's call for open procedures on refusals and disqualifications.

The Legislators didn't get all the answers they wanted, and asked for the topic to be included on the agenda of the next meeting in May.

**More Information**

Views on the "Review on Administration of Internet domain names in Hong Kong"
Background brief on the review on administration of Internet domain names in Hong Kong
Agenda of the Legislative Council Panel on IT and Broadcasting Meeting on Tuesday, 7 April 2009, at 4:30 pm in the Chamber of the Legislative Council Building

# ICAC Claims it doesn't use Foxy

*<web-link for this article>*

Following the leak of a letter sent to them, Hong Kong's ICAC (Independent Commission Against Corruption) has reviewed their internal IT system and confirmed that they have not installed the Foxy file-sharing software. Foxy is popular in Hong Kong, probably because of its Chinese-language interface, and has become notorious since it was used to widely distribute Edison Chen's private photos and it's involvement in the leakage of Police documents. The default Foxy installation options are probably more permissive about sharing than many users realize.

In the latest case, a Foxy user downloaded a letter dated Sep 2005 from a bank to the ICAC and three companies under ICAC investigation and their bank account numbers were also leaked on the Internet. In a statement, the ICAC said, "Following internal inquiries, it is established that the Commission doesn't possess any soft copy of the document concerned. In 2005, we only received a signed letter from the bank in the form of a hard copy, which was apparently different from the document reportedly leaked on the internet".

**More Information**

ICAC: We are not the source of data leakage
Data Leak Disease Spreads to Police?
Privacy and Obscenity: Hong Kong's Showbiz Sex Scandal
Data Leak Disease

# Trail of Exposure

*<web-link for this article>*

The trial of a computer technician in Hong Kong's highest profile data-leakage case, the Edison Chen sex photos scandal, is proceeding with witnesses describing the chain of sharing that led to the photos being splashed across the internet. Sze Ho-chun is accused of three counts of obtaining access to a computer with a view to dishonest gain for himself or others. The prosecution alleges that Sze copied the photos and uploaded them to a server on the internet while Edison's laptop was being repaired at the shop where he worked. Witnesses Fanny Choi and Janet Leung say that Sze mentioned the photos when he was repairing a computer at their office, and showed them the photos online. He then downloaded them to a CD, which he gave to Ms Leung. She later lent the CD to a Ms Mak for one or two days.

The case clearly illustrates the difficulty of keeping interesting information secret, and also dispels the myth that only men share erotic images.

**10th April 2009**

Police Officer Ho Ming-yin has given evidence at the trial that, on 28th January 2008, the day the photos were first circulated on the internet, Sze searched for a secure delete program, downloaded it at 18:08, used it up to 18:23 and uninstalled it at 18:28. Only 11 fragments of the pictures were found on his machine, five with hash values that matched those on the CD he gave to Ms Leung. Ms Ho said that she could not be certain what types of files were deleted by the Secure Delete program.

**15th April 2009**

Acting Superintendent Paul Jackson has given evidence that a CD marked "X", containing 1321 files, 660 of them non-duplicated photos was burned at 1.20pm on June 8, 2006 - the day, according to prosecutors, when Sze gave a disc marked "X" to Ms Leung. The first directory on the disc was created the previous day at either 13.54 or 21.54pm, depending on the time zone setting of the computer. Jackson said there was "99.9%" compatibility between fragments of deleted files retrieved from Sze's home computer and the pictures on the CD.

Sze has chosen not to give evidence, and the prosecution and defence will give their final submissions on 21st April 2009.

**30th April 2009**

Kowloon City chief magistrate Tong Man found Sze Ho-chun guilty of three counts of obtaining access to a computer for dishonest gain for himself or another. In his two-hour ruling, Tong said that the offences Sze committed were very serious because he took advantage of his profession. He breached not only the trust his employer had in him but also the trust a client had in his employer. Sze will be sentenced on 13th May, the maximum sentence for the offences is 5 years, but a magistrate's court is limited to 3 years.

The magistrate said that most of the prosecution witnesses were credible and honest, but cast doubt on some parts of the evidence of Edison Chen, questioning why Chen would suddenly change his usual practice by permanently deleting the pictures from the notebook he sent for repair. He suggested that Chen might be playing down his own responsibility for negligence in securing the photos.

Privacy Commissioner Roderick Woo Bun spoke for a review of the Personal Data Privacy Ordinance (PDPO) to provide a deterrent to prevent leaks of sensitive data. At the moment, the Commissioner has very limited powers: he can issue an enforcement notice, in essence saying, "don't do it again", and on a repeat offence refer the case to law enforcement.

Yui Kee's Chief Consultant commented, "Some people might dismiss this case as a celebrity sex scandal, but it highlights important, but generally boring, issues for everyone. Computer technicians are reminded that they have a duty of trust to their employer and clients when handling data. Users are reminded that they must plan in advance how they protect their sensitive data (whether that is personal photos, financial information, or anything else). It is too late to think you should have encrypted certain files when your laptop has broken down, and you are handing it to a technician you hope is honest and trustworthy. The Government must consider how to improve the PDPO to address the fact that disclosure is one-way: no-one can un-disclose Edison's photos, they can still be found easily on the internet. Damage inflicted by disclosing sensitive personal data cannot be undone. An enforcement notice is sometimes an appropriate way of improving the handling of personal data, before an incident. Something stronger is required after an incident."

**More Information**

Edison driver tells of 3-hour laptop lapse
Privacy and Obscenity: Hong Kong's Showbiz Sex Scandal
Jail looms for Edison sex-pics copier
Guilty verdict in HK sex scandal

# Security Reports from Microsoft and F-Secure

*<web-link for this article>*

Microsoft has released their "Security Intelligence Report", covering the period July to December 2008, and F-Secure has released their "IT threat summary" for the first quarter of 2009.

Microsoft highlights the rise of rogue security software that uses fear and annoyance tactics to convince victims to pay for “full versions” of the software in order to remove and protect themselves from malware, to stop the continual alerts and warnings, or both. Microsoft also provides various statistics relating to vulnerabilities and disclosures, noting that operating system vulnerabilities are declining as more are found in browsers and other applications.

Several comparisons are made between XP and Vista that show a much lower level of vulnerability exploits and malware infections in the newer OS. Whether this is because Vista is inherently more secure, or just less targeted by attackers because it is unpopular, cannot be deduced from the statistics. The data from Microsoft's Malicious Software Removal Tool (MSRT) shows that, even in the heaviest infected countries, such as Russia, Brazil and Turkey, MSRT discovers malware less than 3% of the times it is run. Whether this is because malware prevalence is low, or that MSRT is not good at discovering malware, or because the self-reporting introduces sampling bias (e.g. people who use MSRT and discover malware on their computer remove the infection and then keep running MSRT regularly, while other computers never have MSRT run, and remain infected and uncounted) is unknown.

Microsoft's report finds that 97% of email is unwanted, being spam, or carrying malicious software or phishing attacks.

F-Secure describes the story of January to March as "Worms, worms and more worms".

F-Secure highlights Conficker (Downadup) as the biggest malware story of 2009 so far, it is a classic worm exploiting vulnerabilities in Microsoft Windows, of the type that has not been seen in the past few years. However, Conficker has advanced features such as heavy encryption, a peer-to-peer functionality meaning that infected computers can communicate with each other without the need for a server, and the ability to convert and update itself.

Mikko Hyppönen, F-Secure's Chief Research Officer says: "The authors behind Conficker are professionals. They have infected millions of computers, and could do anything they wanted with them. The mystery is why they haven't done that. Not yet, anyway."

Conficker changed operation modes on April 1st, gaining front page media coverage world-wide. However, the gang behind the worm took no immediate action with their botnet. The mystery continues.

Worms have also started using social networking. The latest variant of the Koobface worm spreading on Facebook steals your logon credentials for Facebook. It logs in, steals your picture and friends' e-mail addresses, creates a fake YouTube page with your Facebook photo and then sends an e-mail to your friends saying they've been tagged in a video on YouTube.

"When you get a message in Facebook from a friend, you tend to trust the message to be real. And when people follow a "funny link" to a video and are prompted to "update" their player, they easily fall for these attacks," Hyppönen explains.

The first quarter was also historical as it saw the birth of the first SMS worm, Sexy View, designed for smartphones. Sexy View, like Koobface, is a social engineering worm which uses the contacts stored on your smartphone to spread. It sends a text message to your contacts telling them to check out some hot pictures and offers a link to a website.

Your contacts follow the URL because it came from you. They are asked to install an application, which now sends the worm to all their contacts. The worm sends the information about the phone to its makers who then use this information to send SMS spam.

"Sexy View is important in many ways, " Hyppönen continues."It is the first text message worm ever. It's also the first mobile phone worm that circumvents the signature checks that are meant to secure the latest smartphones. And the motive behind it seems to be to collect information for mobile phone spamming purposes. Mobile phone spam is already a big problem in some parts of the world - eventually it will be an issue everywhere."

**More Information**

Q1 2009 Security Threat Summary
The Latest Microsoft Security Intelligence Report

# Diamonds are a Cryptographer's Best Friend

*<web-link for this article>*

The University of Melbourne has developed the world's first commercially-available Single Photon Source. The product has been announced by Quantum Communications Victoria (QCV), the premier facility for Quantum Communication technology in Australia, located in the School of Physics at the University of Melbourne.

The system works by growing microscopic crystals of diamond directly onto the tips of optical fibres, so that single photons emitted from the diamond crystals are channelled directly into the fibre. The device, called SPS 1.01, is designed for simple operation and it utilises an FC fibre-optic port for single photon output. It is housed in a convenient 19 inch rack-mount box. The possible applications include quantum communications, quantum optics, quantum computing, quantum metrology, optical calibration, microscopy and optical sensing.

OCV CEO Dr. Shane Huntington explained, "As an initial application the Single Photon Source will be integrated into existing commercial Quantum Cryptosystems, drastically improving their performance and providing one hundred percent secure telecommunications." Quantum entanglement potentially allows secure transmission of encryption keys. Also, quantum computing could render existing mathematical encryption systems obsolete.

However, strong encryption has been likened to a mile-high stake by Bruce Schneier: it is very difficult to get over, but an attacker will find it easy to go around. xkcd has also made the same point.

**More Information**

Quantum Communications Victoria
SPS 1.01 product brochure
World's first commercial source of individual photons

# Ireland Scraps e-Voting

*<web-link for this article>*

Irish Minister for the Environment, Heritage and Local Government, John Gormley has announced that it will be disposing of its e-voting machines, ending a scheme to introduce e-voting that was started in 2004. The equipment is a Dutch-designed Nedap/PowerVote system, which was criticised on the grounds of security, reliability and the lack of an audit trail.

Gormley affirmed Ireland's preference for older technology, "the public in broad terms appear to be satisfied with the present paper-based system and we must recognise this in deciding on the future steps to be taken with the electronic voting system."

In 2004, the then-Taoseach Bertie Ahern strongly supported the modernisation scheme, "otherwise, this country will move into the 21st century being a laughing stock with our stupid old pencils." However, pencils have now won.

In general e-voting systems are introduced because politicians want to "improve" and "modernise" the process. Richard Kay pointed out the fallacy, "Attempts to reduce the cost and time of voting tend to be based upon the assumption that speed and cost reduction are more important than transparency - which couldn't be further from the reality."

Information Security experts generally point out many advantages of traditional technology for voting, Bruce Schneier has often discussed the difficulties involved in e-voting. Richard Kay commented on Ireland's U-turn, "Frankly I've never met anyone I respect with knowledge of my subject who would want to touch any e-voting system that doesn't involve a paper trail which can be confirmed manually at every stage of the process."

**More Information**

Ireland scraps evoting in favour of 'stupid old pencils'
When Voting Machine Audit Logs Don't Help
Can You Count on Voting Machines?
Voting Machines (cartoon)
Comparing the Security of Electronic Slot Machines and Electronic Voting Machines
The Problem with Electronic Voting Machines

# Kaspersky Lab releases analytical article on in-the-cloud security

*<web-link for this article>*

*Yuliya Yudina, Kaspersky Lab*

Kaspersky Lab, a leading developer of secure content management systems, presents its latest analytical article "Clear skies ahead: cloud computing and in-the-cloud security" by Magnus Kalkuhl, the company's senior regional researcher in Germany. The article aims to clarify the concept of cloud computing and the related concept of in-the-cloud security.

Cloud computing is based on a combination of powerful servers and fast Internet connections. This concept had a forerunner in the shape of the mainframe - terminal model (which later transformed into the server - thin client model). In general terms, cloud computing is about renting IT capacity of any kind to anyone who needs it.

With cloud computing, portability can be combined with performance: you can buy a cheap laptop and use it as a thin client. Then all you need to do is connect to your in-the-cloud-provider and enjoy as much performance and memory as you need. A significant risk associated with the technology is that the user has to keep all the data, some of which may be confidential, on the service provider's servers, making it a potential target for cybercriminals. It will be a couple of years before cloud computing really takes off as companies will have to get used to the idea of sharing all of their data with service providers.

In-the-cloud security is the use of outsourced security services that are offered in the cloud, while the operating system is still running locally on the desktop PC. In-the-cloud security comes in different flavors: for instance, Kaspersky Lab offers Kaspersky Hosted Security Services, which provide anti-spam and anti-malware services by filtering traffic for harmful

content before it reaches the end user. The company's personal products also offer in-the-cloud security in the form of the Kaspersky Security Network.

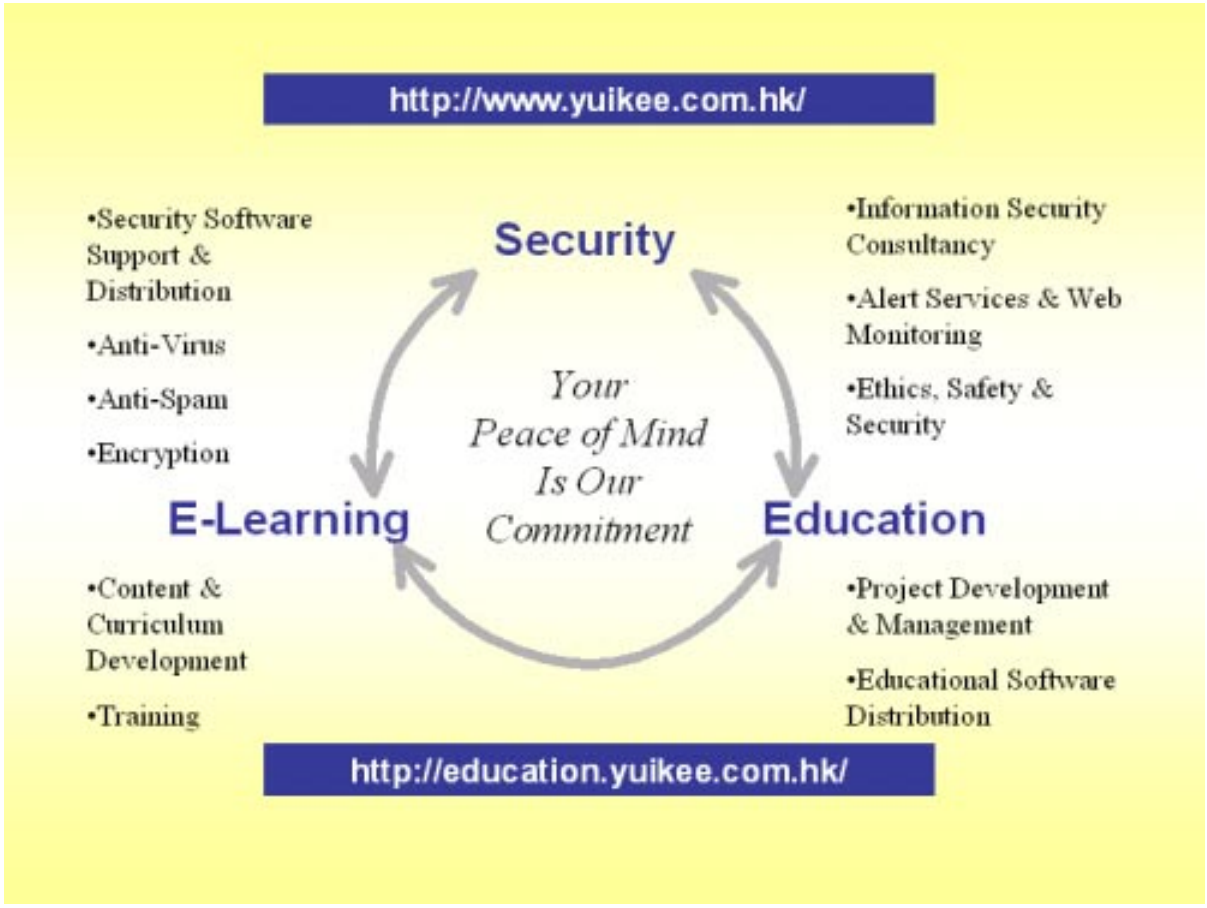
Advantages of the in-the-cloud approach to PC protection include lower memory consumption, a smaller download footprint and better response times. Its drawbacks include a dramatically increased risk of false positives.

Antivirus products which implement in-the-cloud technology have already been released and there seems little doubt that by the end of 2009, this technology will be widely accepted. As time goes on, the two approaches will merge, with individuals and organizations using cloud computers protected by in-the-cloud security services. The full version of the article is available at Viruslist.com. A summary of the article is available on Kaspersky Lab's corporate site. This material can be reproduced provided the author, company name and original source are cited. Reproduction of this material in re-written form requires the express consent of Kaspersky Lab's Public Relations department.

**More Information**

Clear skies ahead: cloud computing and in-the-cloud security
Clear skies ahead: cloud computing and in-the-cloud security (summary)


Suite C & D, 8/F, Yally Industrial Building
6 Yip Fat Street, Wong Chuk Hang, Hong Kong
Tel: 2870 8550 Fax: 2870 8563
E-mail: info@yuikee.com.hk
http://www.yuikee.com.hk/


http://www.yuikee.com.hk/
Security
•Security Software Support & Distribution
•Anti-Virus
•Anti-Spam
•Encryption
•Information Security Consultancy
•Alert Services & Web Monitoring
•Ethics, Safety & Security
Your Peace of Mind Is Our Commitment
E-Learning
Education
•Content & Curriculum Development
•Training
•Project Development & Management
•Educational Software Distribution
http://education.yuikee.com.hk/