Yui Kee Computing Ltd.

Newsletter

November 2011

Contents

Privacy Protection in Hong Kong Allows Identity Theft

<web-link for this article>

Allan Dyer

Regular readers will know that personal data privacy is a reoccurring theme and its importance is linked to our security both online and offline. Earlier this year, on separate occasions, I found that my Bank and my ISP were using my Hong Kong ID number (HKID) as a default password for access to their services. I view this as a very stupid and insecure practice - the HKID is not a secret, so it should not be used as a password; and I decided to report the incidents to the Personal Data Privacy Commissioner, chiefly as a violation of Data Protection Principle (DPP) 4:

> **Principle 4** -- Security of personal data This requires appropriate security measures to be applied to personal data (including data in a form in which access to or processing of the data is not practicable).

The cases have now been concluded, but I decided to follow-up with some questions about the issues. My questions and the Office of the Privacy Commissioner's replies are quoted below, with further comments and discussion. The quotes have been edited for length and to eliminate direct reference to the cases.

> *These cases raise some interesting information security issues that I would like to discuss in my company's newsletter. I would be grateful if your Office could answer the following questions:*
>
> 1. *What is the meaning of "identifier"?*
> 2. *What is the meaning of "authenticator"?*
> 3. *What do you understand by "identity theft"?*
> 4. *Do you regard "identity theft" as an issue that is strongly linked to Personal Data Privacy?*
> 5. *What do you know about the prevalence of identity theft in the USA and the link to misuse of Social Security Numbers? Do you think there is a lesson here for Hong Kong?*
>
> *Your question numbers 1 to 5*
>
> **[...]** Because we are not empowered by the Ordinance to operate outside of its DPPs and its provisions, it would serve no useful purpose if we interpret or further discuss the meanings and issues of "identifier", "authenticator" and "identity theft" as raised by you.

Although the use of Hong Kong Identity Card number as a shared secret for authentication, and the potential this creates for identity theft are outside the remit of the Ordinance, this Office is aware of the possible downfall. In fact, you would know that you are not the first IT security professional who calls for this practice to be changed. Since we are not mandated under the Ordinance to intervene in this particular issue, we could only urge data user not to do so. You may like to know that in an upcoming Guidance Note related to IT, we have put this down as a recommended best practice to data users to raise the general awareness.

I am disappointed that the Office decided not to answer the question. DPP4 clearly requires "appropriate security measures" so the Commissioner must, in relevant cases, make a decision on whether certain practices are "appropriate" and "security measures". The meanings of "identifier", "authenticator" and "identity theft" are therefore highly relevant to the DPPs and the provisions of the Ordinance.

The upcoming Guidance Note related to IT is good news.

6. *DPP1 requires that the data subject be explicitly informed of the purpose for which the data are to be used, however DPP3 allows use of the data for "a directly related purpose". "Directly related" is a very subjective term. Can the data subject require the data user to stop using the data for a purpose that was not explicitly declared at the time of collection?*

Your question number 6

You asked whether the data subject can require the data user to stop using the data for a purpose that was not explicitly declared at the time of collection. DPP3 provides that the data user shall not, without the proscribed consent of the data subject, use the personal data for any purpose other than the purpose for which the data were to be used at the time of collection of the data, or for a directly related purpose. As the law at present allows a data user to use personal data for a purpose directly related to its collection purpose, even if a data subject makes the request, the data user is not legally bound to follow.

The data user and data subject can have very different views on what is a directly related purpose. When I presented my HKID card to my Bank and ISP my purpose was to prove who I was when I entered the commercial relationship with the company. I did not consider that the company would then take the number from my HKID card, and set it as a default password for the company's services on the internet. In fact, when I opened my account at my Bank, it was before banks had websites, let alone online banking services. Personally, I see "proof of identity by comparing a face to a picture of a face on a Government issued identity document" when entering a commercial relationship with a company as a completely different and unrelated purpose to "we've got to set the default password to something, and we're too lazy to actually ask the customer" when providing ongoing services in an existing relationship.

This is an area where the law needs amendment. If a data user uses data for a purpose that was not explicitly declared, then the data subject should have the right to require them to stop.

7. *If a data user knows or can reasonably assume that a data item is known to one or more third parties, is it appropriate for the data user to use that data item as a default password for security purposes?*

8. *Is it necessary for there to be evidence that a complainant's personal data was leaked before you would consider there to have been a contravention of DPP4? If not, what other factors would you consider?*

In discussing disclosure of account information by my ISP, you pointed out that the HKID number was not the only information required before account information was disclosed, and that my login ID and account number are not easily available to a third party.

9. *Are you aware that the login ID is also the user part of the email address, and therefore known to all email correspondents?*

10. *Following up a technical issue, my ISP called me today on my mobile, I asked them to call back on my office number. Later in the call, my ISP wanted me to login to their website, but, not being at home, I did not have the account number to hand. The ISP did not hesitate to give out my account number. Does this incident change your assessment as to the difficulty of a third party obtaining my account number?*

Your questions numbers 7 to 10

DPP4 requires a data user to take all reasonably practicable steps to ensure that personal data are protected against unauthorized or accidental access. The fact that the personal data held by the data user were leaked is one of the clear indications that the data user had breached the requirements of DPP4.

The mere facts that the data item used by a data user as a default password is known by other parties or that the service provider could give out the customer's account number or login ID do not necessarily mean that the data user or the service provider has contravened DPP4. We shall examine if the data user has already taken all reasonably practicable steps to safeguard the data security. In your case, the data user gave your account number to you only. Unless there is substantial evidence, we cannot assume that the service provider has no procedure in place to safeguard its customer's personal data security during its interaction with you when it was the service provider who initiated the call to contact you.

This is perhaps the most disappointing answer, and it comes back to the concepts of "identifier", "authenticator" and "identity theft" that the Office said, "would serve no useful purpose if we interpret or further discuss [the concepts]". I suggest that is is "reasonably practicable" to make sure a default password is secret - that it is not known by a third party. The only reasonable answer to my question 7 is "No", and I suggest that the Commissioner should consider the use of a non-secret item of personal data as a default password to be entirely inappropriate, and therefore an automatic violation of DPP4.

The second part of the answer is also flawed. The contention is that, because the ISP phoned me (on my mobile) they were justified in thinking it was me, even though I did not authenticate myself, and even though I asked them to phone another number.

In practical terms, if I pay my ISP by cheque, then my ISP, and certain staff within my ISP, have all the necessary information to register my bank account for online banking. Similarly, if I send an email to my bank, my bank, and certain staff at my bank, have all the necessary information to contact my ISP, get my account number, reset my password and gain access to my private email held at my ISP. There is a reason why my ISP and my Bank do not share their offices, however convenient it might be in terms of reduced costs and sharing of data. The fact is that this kind of sloppy handling of security and privacy is not limited to my Bank and my ISP, or even Banks and ISPs, but it is endemic to most service providers in Hong Kong. Each additional organisation with weak security and privacy controls makes an incident both more likely and more damaging. Perhaps the only "defence" saving Hong Kong from massive criminal identity theft is that the criminals have been fully occupied with the opportunities presented by the USA Social Security Number.

More Information

Views on the Review of the Personal Data (Privacy) Ordinance
Views on the PDPO Legislative Proposal
The Professional Commons holds Open Forum on Privacy
Privacy Laws to be Tightened
Privacy and Obscenity: Hong Kong's Showbiz Sex Scandal
Social Security Numbers: Identification is Not Authentication

Hong Kong Amends Strategic Commodities Import and Export Regulations

<web-link for this article>

Hong Kong's Trade and Industry Department has announced an amendment to Schedule 1 of the Import & Export (Strategic Commodities) Regulations in Strategic Trade Controls Circular No. 7/2011. The amendment includes two changes to the regulations on Information Security products:

- 5A002(b)- Add the control on certain systems, equipment, application specific electronic assemblies, modules and integrated circuits, designed or modified to enable an item to achieve or exceed the controlled performance levels for cryptographic functionality.
- 5A002, Note (j)- Remove the control on certain information security equipment in which the cryptographic function cannot be used or can only be made usable by means of cryptographic activation.

The changes will take effect on a day to be appointed by the Director-General of Trade and Industry by a notice published in the Gazette.

More Information

Strategic Trade Controls Circular No. 7/2011
Highlights of the Import and Export (Strategic Commodities) Regulations

AVAR 2011 Hong Kong Report

<web-link for this article>

The fourteenth Anti-Virus Asia Researchers Annual Conference took place on the 9th - 11th November in the heart of Wan Chai, Hong Kong.

Figure 1 The stage is set

As usual, several significant industry meetings took place alongside the conference, with the Wild List Organisation and the Anti-Virus Product Developer Consortium both holding meetings on the 9th. AVAR itself held its Directors' meeting on the 9th, and the Members' Annual General Meeting at the end of the conference.

Figure 2 Coffee

The conference itself was kicked off by Roy Ko, Centre Manager of Hong Kong CERT, giving the Keynote speech on Creating a Safe, Clean and Reliable Cyberspace. The conference then split into two streams, with Andrew Lee and Pierre-Marc Bureau examining the motivations of malware authors, revealed through case-studies, while Young Jun Chang discussed targeted attacks in Korea.

Igor Muttik looked at the potential for malware in the pre-boot environment of the Extensible Firmware Interface (EFI), concluding that pre-OS malware is easy to write and unpleasant to deal with, so we need better coverage and tools. Igor earned the Best Speaker Award at the end of the conference.

Several presentations looked at malware on mobile devices. V Dhanalakshmi covered the Android security model, the threats and ways to mitigate the risks. Itshak Carmona covered Symbian, Android and iPhone malware. Cao Yang and Zou Shihong showed how malware on Symbian and Android devices can attack the most popular mobile payment systems in China.

On the defence side, Yu Guo Liu looked at providing a one-stop solution for both PC and mobile platforms.

Different countries provide different environments and opportunities for malware. Jim Wang explained how to reverse-engineer programs written in the Chinese programming language EPL (Easy Programming Language) and Kazumasa Itabashi discussed tricks used to target regional Japanese and Chinese software.

Three presenters, Lukas Hasik, Raymond Roberts and Xue Yang also described attack techniques: Google image poisoning, Obfuscation and Exploit Kits respectively.

Jianfeng Lu, Jeffrey Ma, Rajesh Nikam and Benny Czarny each took a different look at defensive techniques while Tony Lee and Richard Thomas covered cross-industry cooperation and testing methodologies.

Alfons Tanujaya, Randy Abrams, Darya Gudkova and Cameron Camp gave four presentations related to social engineering and user education.

The conference social programme included the Gala Dinner, held at the famous Jumbo Kingdom floating restaurant in Aberdeen Harbour and the islands tour on a traditional Chinese junk.

AVAR 2012 will be hosted by Tencent in Mainland China.

More Information

[Welcome to AVAR 2011 in Hong Kong]
[Anti-Virus Product Developers Consortium]
[Latest WildList]

Figure 3 Gala dinner at Jumbo Kingdom

Figure 4 Presentation of the WildList Reporters Award

Figure 5 Conference delegates leave the floating restaurant

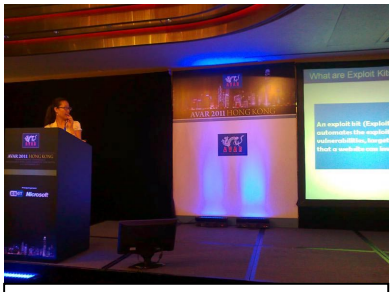


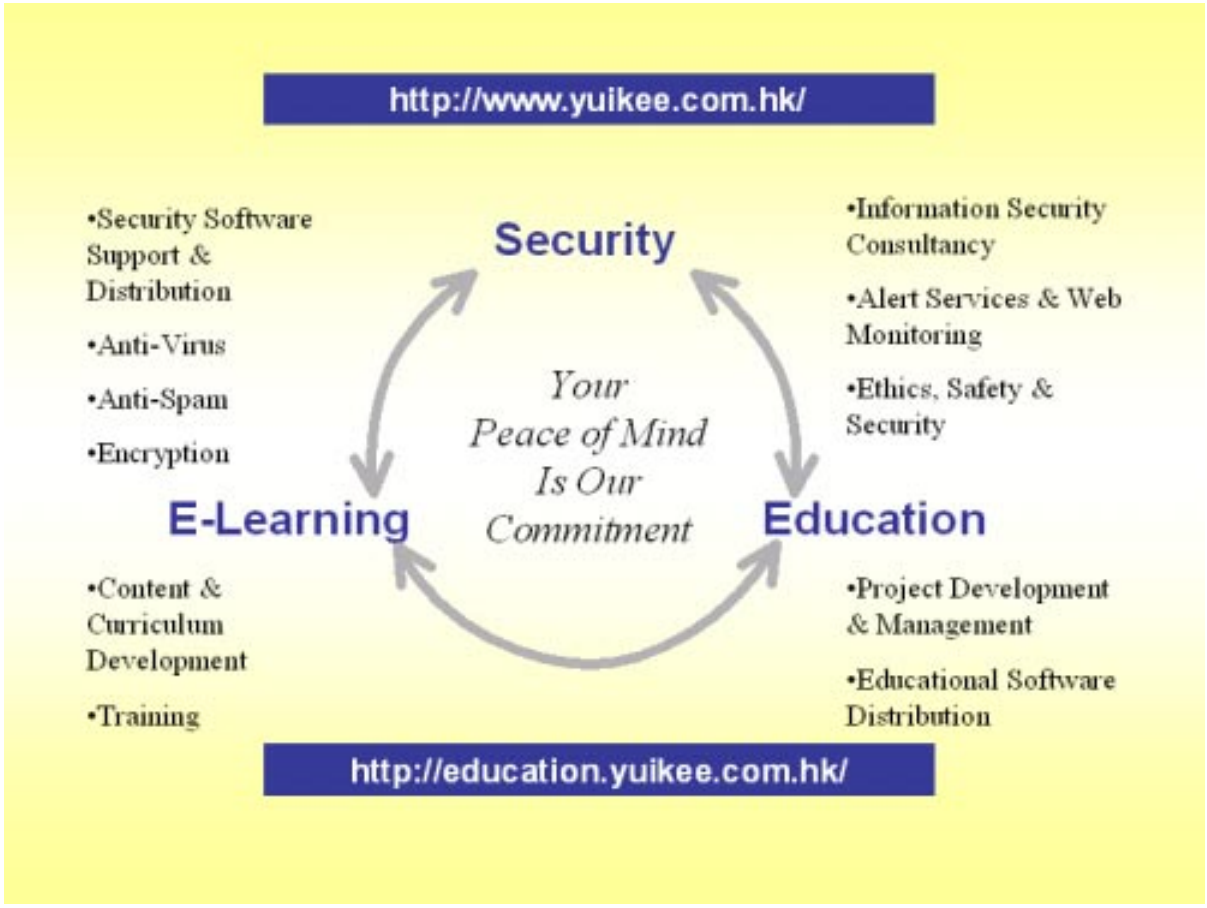
Figure 7 Xue Yang dissects an exploit kit

Figure 8 The AVAR junk arrives

Figure 6 Some suspicious characters

YUI KEE
銳基電腦顧問有限公司
Anti-Virus, Network Security & Education

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/