PISA

Professional Information Security Association

Phone : (852) 8104-6800
Fax : (852) 2900-8338
Email : info@pisa.org.hk
URL : www.pisa.org.hk

LC Paper No. CB(2) 4/02-03(05)

Mr. Eric Lee Ka Cheung
Chairman
Bills Committee on Inland Revenue (Amendment) (No. 2) Bill 2001
Legislative Council
8, Jackson Road
Central
Hong Kong

20 September 2002

Dear Mr. Cheung,

Comment on Inland Revenue (Amendment) (No. 2) Bill 2001

Professional Information Security Association (PISA) is a not-for-profit organization for local information security professionals. Our objective is to promote security awareness to the IT industry and general public in Hong Kong, utilizing our expertise and knowledge to help bringing prosperity to the society in the Information Age. As such we find it a necessity to express our concerns on the captioned bill to amend the Inland Revenue Ordinance.

1. The Electronic Transaction Ordinance (ETO) 2000 sets the basis for the development of electronic commerce of Hong Kong. ETO recognizes digital signature as the **only one** proven technology among other known electronic signatures that satisfies the requirements of authentication, confidentiality, integrity and non-repudiation. As a matter of principle, before there is any confirmed revision to the ETO, the governmental services should not try to bypass the ETO and employ another technology option like PIN.

2. When the ETO 2000 was passed, technologies like PIN, SSL, digital signature and etc. were already mature in the market. It merely reflected that ETO had reviewed all these technologies before confirming digital signature as the only accepted technology. Such understanding had been repeatedly confirmed in the several replies of the government to the public during the consultation of the ETO in 2000. What has changed since year 2000 that can support Inland Revenue Department (IRD) to accept PIN in addition to digital signature?

Previous reply of IRD to PISA did **not** address the above two points on the principle. Some of the backgrounds that IRD's proposal quoted for supporting the proposal did exist on or before year 2000. Should it be valid the ETO should have been rewritten by then.

3. PIN is **much less secure** than digital signature. PIN is known to be easily cracked by brute force attack, social engineering or intelligent guess. The weakness of PIN not only attracts crackers, it also attracts people to delay tax return filing by submitting an incorrect filing and put the blame on unauthorized access by third party afterwards.

4. PIN **cannot** fulfil the requirement of non-repudiation. Firstly, IRD also keeps a copy of the password; secondly whoever can successfully crack the password can use it in the same way as the owner. It creates doubts when there is legal dispute. IRD's intention to enforce repudiation on tax-payer by law (to make tax-payer liable when they promised to keep the password to his/her own) is unfair.

5. It is a misconception that the tax return filing is of low risk (compared with Internet banking) because so called "there is no financial transaction". In Internet banking, the client and the bank are governed by mutual agreement on civil rights only (also quoted in IRD's reply letter) whereas tax payers indeed have very great liability (that leads to an offence!) in submitting untrue, incorrect and incomplete tax return. Furthermore, the fact that clients have choice of banks makes the balance of power totally different. The citizens are in unfavourable position in misfiled tax return cases against IRD. Lastly, the information involved in the tax return filing process is regarded as highly personal and confidential. A PIN based tax return filing system could lead to security risks like the UK IR as stated in point #6.

6. UK's IR suspended her Tax e-filing system in May 2002 due to security breach. Some people's records were modified and some people view others' information in their own file. The system was resumed in July 2002. However, the root cause leading to the breach is still not clarified till now (reference #1). It is a good example to indicate how sensitive tax filing information is and how insecure a PIN based system is.

- Quoted below is comment from spokesman of Ernest and Young LLP on the UK IR's online system (reference #2):

> *(extracted)*
> Accounting company Ernst & Young LLP conducted an internal review of the (UK) IR's online system soon after it went public about two years ago and determined that security issues kept Ernst & Young from recommending the system to its customers or using it themselves, Rayner Peett an Ernst & Young spokesman said Friday.
>
> "Our review turned up a number of concerns about the IR's online filing system, including the flexibility of the system, but one of the main concerns was over security. Such a system has to be able to guarantee the absolute security of confidential information and we didn't feel the IR's system could do that. The government has encouraged people to file online and what we hope is that this breach in security will goad the government into doing whatever is necessary to assure the security and confidentiality that taxpayers require," Peett said.

- The British Computer Society highlights lessons from UK Inland Revenue security problems in their e-bulletin (reference #3)

> *(extracted)*
> 'Taxpayers expect confidentiality from the Revenue, and that applies to electronic services as well,' says BCS chief executive David Clarke. 'Although this incident is reported to be accidental from the limited facts available, it does pose the question of whether it could happen again or whether the Revenue's system would remain impervious to deliberate attack.'
> …
> He adds, 'We would expect that the lessons learned from this occurrence will be applied to other government online developments.'

7. IRD cited a number of countries as examples of PIN-based Tax Return Filing adoption without figures and study to prove their success in cost-effectiveness and security.
   - The example of UK is even a counter-example itself! UK's system failed in both security (as indicated in point #6) and cost-effectiveness (up to now only 1% adoption rate instead of 50% claimed before implementation, see reference #4).
   - The example of Australia is irrelevant. Australian e-tax return filing in fact uses a kind of digital certificate technology and use digital signature to encrypt and sign the tax return

filing (reference #5). If it is a success, credit should be given to the digital signature based system. Australian system can give a hint to Hong Kong that alternative exists in digital signature technology implementation. Australia uses a different e-tax return filing application each year and the digital certificate pairs are generated each year.

8. We have some other concerns on the details of implementation of the e-Filing system as provided by IRD's reply to PISA. They merely made us even more worried than before. We are not to dig into the detail so just list some of them for your consideration.
   - IRD adopted RC4 encryption algorithm which is known to be vulnerable towards some attacks
   - The planned PIN implementation uses 6-digit PIN which is extraordinarily weak.
   - The intended tax return e-filing system provides function to review submitted data and status of payment at a later day. It bears even higher risks by attracting third party to break in to collect the information of financial position of tax payers.
   - PIN based system requires password storage that poses severe security and management problem. These problems are simply avoided if IRD sticks to using digital signature.

9. IRD's proposal to Telephone Filing is not realistic
   - IRD said that there is "Instruction Notes for Telefiling" to guide the tax-payer and a "Telefiling Record Sheet" to help entry of the record on paper before telephone filing. If an average tax-payer will read the note and fill in the record sheet, they will have instead filled in the tax filing form and mailed it out. No one will choose a further step to dial a telephone number and do the entry again.

PISA has the following proposals:

1. A lot of the issues the IRD is trying to deal with in her proposed bill should fall in the scope of the ETO review. IRD should therefore suspend or pull out the current proposal until the review of ETO set out a clear direction. Otherwise IRD will set a very bad example to the public and to the business that, firstly, IRD is bypassing the policy laid down by ETO; secondly, IRD is confusing the public in mixing up PIN and digital signature – two technologies with largely different level of security.

2. PISA proposes to establish an authority to develop and adopt security assessment for governmental services should the ETO review approves PIN as an accepted technology. This authority is essential if HKSARG maintains two drastically different technologies (PIN and digital signature) in application to the government services. The governmental services should be assessed and labelled to different categories according to the risk associated. To every category in the security risk labelling of governmental services, the security requirement should be developed. It is under such framework that the risk assessment of IRD's proposal system be sound and logical.

3. PISA consider PIN based system is **not** suitable for IRD Tax Return Filing system. IRD should continue to use digital signature to sign the filing.

We appreciate our opinions be considered by the Bills Committee and look forward to your reply. PISA would attend the public meeting in October as well. Please contact me at telephone 8104-6800 or email: sc.leung@pisa.org.hk.

Yours faithfully,

Mr. LEUNG Siu Cheong
Chairperson
Professional Information Security Association

Cc:

Bills Committee on Inland Revenue (Amendment) (No. 2) Bill 2001,
Legislative Councillors, and
Commissioner of Inland Revenue

References

1. Revenue security flaw taxes government (VNE.NET Online News July 4, 2002)
   http://www.computeractive.co.uk/News/1133243

2. Security breach on UK tax site halts online filing (IDG report May 31, 2002)
   http://www.idg.net/ic_869764_5055_1-2793.html

3. British Computer Society highlighted lessons from UK Inland Revenue Security Problems (BCS e-Bulletin Archive Issue 26: June 26th 2002)
   http://www.bcs.org/ebulletin/020626/security

4. Online Tax Return doomed - The Guardian (Thursday August 29, 2002)
   http://politics.guardian.co.uk/news/story/0,9174,782193,00.html

5. Five easy steps to use e-tax (Australian Taxation Office web site)
   http://www.etax.ato.gov.au/webpages/fivesteps.asp