Hong Kong Computer Society 香港電腦學會

Founder Member
South East Asia Regional Computer Confederation
SEARCC

Room 1915, 19/F, China Merchants Tower,
Shun Tak Centre, 168 Connaught Rd. C.,
Hong Kong.

Tel : (852) 2834 2228
Fax : (852) 2834 3003
URL : http://www.hkcs.org.hk
E-mail : hkcs@hkcs.org.hk

立法會 CB(2) 1160/02-03(01)號文件
LC Paper No. CB(2) 1160/02-03(01)

10 February 2003

The Hon Eric LI Ka-cheung, JP
Chairman
Bills Committee on Inland Revenue (Amendment) (No. 2) Bill 2001

cc: Alice Lau, JP, Commissioner, Inland Revenue Department
Secretary, Bills Committee, Legislative Council

Dear Mr. Li,

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

I am writing to express the concerns that the Hong Kong Computer Society (HKCS), and, in particular, our Information Security Specialist Group (ISSG), has about the advisability of the above Bill. Some Members of the HKCS have closely followed the development of this Bill, and the related Electronic Transactions Ordinance, and we have previously submitted opinions on both topics. Most recently, on 17 January 2003, a representative of the ISSG Executive Committee attended a meeting organised by Hon Sin Chung Kai with representatives of other Societies who also had expressed concerns about the bill. Also in attendance where: Alice Lau, Commissioner of the IRD and other officers of the IRD; ITSD; and the Finance Department.

During this meeting a number of concerns were addressed, changes to the proposals were explained, and a demonstration of the latest version of the proposed system provided. After discussing the report of this meeting we have reached the following conclusions and recommendations:

1. Summary

The modifications have considerably improved the proposed system, and addressed some of the concerns raised in earlier submissions. However, the essential purpose of the system is fundamentally flawed. The system does not match up to the requirements set forth in the "UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001" and the Bill is in direct conflict with advice provided by ITBB during its public consultation period on the Electronic Transactions Ordinance in November 1999. Passing the Bill would be detrimental to the progress of eGovernment, eCommerce in general, the progress and competitiveness of Hong Kong, and the position of Hong Kong as an IT hub.

Hong Kong Computer Society 香港電腦學會

Founder Member
South East Asia Regional Computer Confederation
SEARCC

Room 1915, 19/F, China Merchants Tower,
Shun Tak Centre, 168 Connaught Rd. C.,
Hong Kong.

Tel : (852) 2834 2228
Fax : (852) 2834 3003
URL : http://www.hkcs.org.hk
E-mail : hkcs@hkcs.org.hk

We regret that we must object to a well-planned project that a lot of effort has been put into mainly for reasons outside the scope of the project. The project could work well for the electronic submission of tax returns, but, in the wider contexts of greater IRD accessibility, promotion of eGovernment, eCommerce law, promotion of IT usage, improving the competitiveness of Hong Kong and bridging the digital divide, it would be detrimental.

2. Advice of the ITBB

On at least three occasions during the Public Comment period on the Electronic Transactions Ordinance in late 1999, the ITBB gave formal reasons why the use of Digital Signature technology and not the use of Passwords, PINs etc. was the preferred approach.

In a response to the Law Society, LC Paper No. CB(1)230/99-00(11), the ITBB laid out the purposes of a signature, advised, "digital signature-based technology is the only technically mature technology that provides the security service of ensuring integrity and non-repudiation in an open network environment" and stated, " we would require digital signature technology to be used".
(see http://www.legco.gov.hk/yr98-99/english/bc/bc19/papers/b1941111.pdf)

In a response to Cable and Wireless HKT, LC Paper No. CB(1) 343/99-00(05), the ITBB repeated the statement on technological maturity and also said, "Security breaches of any kind due to immaturity of the technology would substantially undermine the confidence of the public in participating in electronic commerce. This would impede the development of electronic commerce in Hong Kong."
(see http://www.legco.gov.hk/yr98-99/english/bc/bc19/papers/a343e05.pdf)

In a reponse to the Business Software Alliance, LC Paper No. CD(1) 409/99-00(01), the ITBB again repeated the statement on technological maturity - this was clearly an important cornerstone of ITBB thinking at that time. The statement on impeding the development of electronic commerce is also repeated.
(see http://www.legco.gov.hk/yr98-99/english/bc/bc19/papers/a409e01.pdf)

As can be seen, the ITBB very clearly stated in response to public comment questions raised that Digital Signature technology was the minimum level of security acceptable to the Government. We have not seen advice agreeing that technical advances since 1999 have overridden this initial opinion or that the original advice provided by the Government may have been incorrect.

Hong Kong Computer Society 香港電腦學會

Founder Member
South East Asia Regional Computer Confederation
SEARCC

Room 1915, 19/F, China Merchants Tower,
Shun Tak Centre, 168 Connaught Rd. C.,
Hong Kong.

Tel : (852) 2834 2228
Fax : (852) 2834 3003
URL : http://www.hkcs.org.hk
E-mail : hkcs@hkcs.org.hk

3. Electronic Submission of Tax Returns

There is no such thing as a perfect security system or of a system with perfect security. Each system needs to be evaluated in terms of the risks involved. The worst-case scenario is that, after a fair amount of effort, an attacker could submit an invalid tax return for a victim. The incident would be discovered when the victim submitted their real return, and, after a certain amount of inconvenience, the situation would be resolved. There would be no benefit to the attacker, except maybe to have knowingly caused inconvenience to both the authorised user and to the IRD. Therefore, minimal security is required, and the proposed system provides that.

4. Greater IRD Accessibility

The features of a form pre-filled with personal information and saving of data from partially filled forms have been put on hold pending the independent security review. Likewise, online tax enquiry will not be initially available. It is likely that the review will result in these features being put on permanent hold: a six digit PIN does not provide sufficient security to protect the highly detailed personal information in a tax return (which includes details of family relationships and details capable of permitting identity theft on many other systems). A well-organised attacker could make apparently legitimate access attempts from a large number of compromised machines (see the details of many recent email worms, or Code Red zombies) at minimal cost.

For example, (in a recent test case) a 166MHz Pentium computer was used to execute one million access attempts to a "secure" system in 6 days. A non-targeted attack (i.e., not directed at a particular person) trying random PINs could expect success one in a million attempts (remember that five attempts are allowed for each user before an account is locked-out in the proposed IRD system). More sensibly, the attacker could concentrate on trying the most commonly used 6 digit numbers, and get a much higher success rate. A targeted attack would probably use other methods to try to establish the most likely PIN for that victim, with a pretty good chance of success.

If the review concludes that a 6 digit PIN is not sufficiently secure to protect such personal information, the users who have embraced the system to file their tax return this year will find themselves at a dead-end next year. In order to get easier access to their IRD stored data, they will need to abandon the PIN scheme they have learnt and try to understand something else. Alternatively, they will become disillusioned and give up on eGovernment altogether.

5. Promotion of eGovernment

As Alice Lau suggested, the tax-filing scheme will be seen as a pioneer and other departments will follow suit. PIN authentication will be seen as an easy way to achieve

HONG KONG COMPUTER SOCIETY

Room 1915, 19/F, China Merchants Tower,
Shun Tak Centre, 168 Connaught Rd. C.,
Hong Kong.

Tel : (852) 2834 2228
Fax : (852) 2834 3003
URL : http://www.hkcs.org.hk
E-mail : hkcs@hkcs.org.hk

results in eGovernment provision. Each department will evaluate the security requirements for their own system and decide on their own password requirements. Users will face a confusing mixture: different lengths, numeric or alphanumeric, case-sensitive or not, is punctuation allowed etc...

Users will also face a choice between two evils: choosing the same password for every service would be insecure (and should be discouraged in the guidance notes), but remembering multiple passwords is difficult, and writing them down is insecure too. The more eGovernment applications the users choose to use, the harder it becomes for each user to effectively and securely use such multiple systems. Additionally the respective Government Departments may be required to undertake a greater level of administrative overhead e.g. users continuously applying a wrong password (i.e. that used for satisfying the needs of another Department's system) due to the disparate mix of user identifiers and verification techniques employed.

As demonstrated by the previous simple example, using passwords will make individual eGovernment applications more accessible, but they will be damaging to the progress of eGovernment overall.

6. eCommerce Law

The Government is a leader in electronic provision of services, and the commercial sector will, to some extent, follow the Government lead. This re-writes and escalates the password overload problem further.

However, the IRD Amendment also sets the precedent that a "shared secret"[1] can be used for non-repudiation. Logically, this makes no sense: a number that is known to both the taxpayer and the IRD when attached to a tax return cannot "prove" that the taxpayer intended to make that tax return. In the context of a tax return, it does not matter much - if someone later claims that they did not make the return, then they are guilty of not making a tax return instead (while this is probably a lesser offence than making a fraudulent return, the tax still gets paid in the end). In the context of the wider society, the precedent is dangerous: lazy system designers can use it to justify bad designs and judges could be persuaded by arguments based on it.

Article 6 paragraph 3 of the "UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001" sets out requirements for an electronic signature to be regarded as reliable:

---

1 A "shared secret" is a code known by both the authorised user and any other third party.

Hong Kong Computer Society 香港電腦學會

Founder Member

South East Asia Regional Computer Confederation

SEARCC

HONG KONG COMPUTER SOCIETY

Room 1915, 19/F, China Merchants Tower,
Shun Tak Centre, 168 Connaught Rd. C.,
Hong Kong.

Tel : (852) 2834 2228
Fax : (852) 2834 3003
URL : http://www.hkcs.org.hk
E-mail : hkcs@hkcs.org.hk

a. The signature creation data are, within the context in which they are used, linked to the signatory and to no other person;

b. The signature creation data were, at the time of signing, under the control of the signatory and of no other person;

c. Any alteration to the electronic signature, made after the time of signing, is detectable; and

d. Where the purpose of the legal requirement for a signature is to provide assurance as to the integrity of the information to which it relates, any alteration made to that information after the time of signing is detectable.

The PIN scheme meets NONE of these requirements. It has been pointed out that the Model Law does specifically mention PINs and even clicking an "OK-box" as possible electronic signatures (in paragraphs 33 and 82), but this is taking the reference out of context: Paragraph 33 says "which may be currently used, or considered for future use, with a view to fulfilling one or more of the above-mentioned functions of handwritten signatures", therefore the mention of a particular technology does not imply that it is suitable for all the functions of a signature, for example, clicking an "OK-box" might be an acceptable method for a user to indicate they agree to be bound by a license agreement, but it provides no information about the identity of the user. Paragraph 82 starts "Given the pace of technological innovation" and ends "The various techniques listed could be used in combination to reduce systemic risk", so it is saying the techniques might be useful at some point in the future, after unknown technological innovation, and, even then, a combination of techniques might be used. In the same paragraph, "the Model Law provides criteria for the legal recognition of electronic signatures irrespective of the technology used" - it is meeting the criteria in Article 6 paragraph 3 that is important.

However, Article 6, paragraph 1 states, "Where the law requires a signature of a person, that requirement is met in relation to a data message if an electronic signature is used that is reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement." Along with the phrase "within the context" in Article 6, paragraph 3, a, this appears to allow justification of the IRD's PIN scheme - the actual risks of forged tax returns are very low, and, although the IRD as a whole "knows" the PIN, the procedural controls and separation of duties within the IRD ensures that it cannot be used.

Unfortunately, this approach would mean that the IRD would have to prove its' system was working correctly in any and every case where the validity of the PIN signature was contested - that is, it would need to conduct a full (independent?) audit and present all its' controls for protecting the relevant systems with the audit results in public court. If

Room 1915, 19/F, China Merchants Tower,
Shun Tak Centre, 168 Connaught Rd. C.,
Hong Kong.

Tel : (852) 2834 2228
Fax : (852) 2834 3003
URL : http://www.hkcs.org.hk
E-mail : hkcs@hkcs.org.hk

they did not, it would create a legal precedent, "if an organisation claims its' internal security is good and working, then that is true, and no evidence is required".

The same problem does not apply to a digital signature (using asymmetric cryptography). The ultimate trusted party in a PKI scheme is the root CA, and the root CA's private key is the most valuable secret. However, even if the worst-case scenario happens, and the root CA's private key is compromised, the digital signatures relying on it are not automatically unreliable because knowledge of the signer's private key was still needed to create them. All that has been lost is the proof of connection between a particular private key and a particular user (demonstrated by the certificate signed by the now-untrusted root CA private key). If the link between a private key and a user can be re-established (perhaps a re-registration exercise, based on a new root CA key), the signatures are still just as secure. Conversely, the validity of the PIN signatures cannot be re-established, if the security of the central system and its' procedural controls fails; all the dependant electronic signatures are permanently invalidated, the house of cards falls down.

7. Promotion of IT Usage / Bridging the Digital Divide

It is easy to forget that promotion of IT Usage is not an end in itself. If it was, we could simply set up many more video game centres - the customers are certainly IT users. The intention, surely, is to leverage IT to achieve improvements in productivity, society and competitiveness. The efforts to promote IT must therefore be directed. Thus, when recycling second-hand PC's to be used by disadvantaged individuals, the donation request specified a minimum system requirement - it was recognised that providing people with DOS or Windows 3.1 and teaching them to use it would not help them in today's technology environment.

By the same token, we should not be leading IT users into the dead-end of password overload. There is discussion of a technology-neutral stance to electronic signatures. We agree that we should not rigidly define digital signatures as the only acceptable electronic signature. The evaluation must be made on the merits of the technology in question, and we should promote the best available technology. Today, this is digital signatures.

8. Improving the Competitiveness of Hong Kong

The claims that digital signatures, in particular eCert, are difficult to understand and difficult to start using are true. The benefits are seen as more parties are dealt with. A marketplace does not exist until everyone can freely trade with everyone else, so PKI enables an electronic marketplace by enabling trading between parties with no pre-existing relationship. A territory that has a significant population that understands and

Hong Kong Computer Society 香 港 電 腦 學 會

Founder Member
South East Asia Regional Computer Confederation

Room 1915, 19/F, China Merchants Tower,
Shun Tak Centre, 168 Connaught Rd. C.,
Hong Kong.

Tel : (852) 2834 2228
Fax : (852) 2834 3003
URL : http://www.hkcs.org.hk
E-mail : hkcs@hkcs.org.hk

can use digital signatures for business, because they already use them in their private lives, will be able to enter the global electronic marketplace quicker and more smoothly.

I trust that your Committee will consider these arguments carefully, and that you will reconsider the passage of Inland Revenue (Amendment) (No. 2) Bill 2001. We would be prepared to present and elaborate our comments in person if necessary.

Yours sincerely,

Daniel Lai, JP
President