STATEMENT BY ISFS TO BILLS COMMITTEE ON INLAND REVENUE (AMENDMENT) (NO. 2) BILL 2001

Our Premise:

ISFS is a society for computer security and forensics professionals. From our point of view, any measures to make the job of computer crime investigation easier are welcome. However, the amendment proposed by Inland Revenue Department (IRD) accepts password and any signing tools for signing the tax return in addition to the Digital Certificate generated Digital Signature. This amendment weakens the entire IT security infrastructure established through the use of Digital Certificate for authorized and legally accepted signing tools.

There are two issues to the established IT security infrastructure in Hong Kong. First, it implies that password and any signing devices can generate authorized digital signature with the same security level as using digital certificate which is technically incorrect. Second, non-repudiation cannot be achieved by signing a message using the password, because each password used in the IRD tax return system is a shared secret between commissioner of IRD and the owner.

Therefore, ISFS is not in favour of the amendment made by IRD in the Inland Revenue (Amendment) (No. 2) Bill 2001.

Our Comments:

1. The direction and motivation of the amendment is on the right track.

2. Tax return via telefiling is a good alternative for non-computer users.

3. Password, PIN or TIN can be used for authenticating taxpayers to IRD's web application. However, they cannot be used for proving the genuineness of tax-return documents as more than one party has access to the taxpayer's password.

   Digital certification/Digital signature can serve the purposes of authentication and non-repudiation. However, password, PIN or TIN can only achieve the purpose of **identification and authentication**, but **not non-repudiation**.

…/page 2

Under IRD's proposed scheme, the holder of the cryptographic key in IRD as well as the password owner would have the capability to generate the same cryptographic hash. Therefore, the cryptographic hash cannot be used to protect IRD in a lawsuit if the password owner claims the tax return produced by IRD has been modified. This is because non-repudiation cannot be guaranteed.

As described in most of the security and cryptography text books, the password is used for achieving identification and authentication purposes. It can also be used for generating cryptographic hash and digital signature. However, unlike Public Key Cryptography, password generated digital signature and authentication schemes cannot achieve the objective of non-repudiation. Currently, the Public Key Cryptographic algorithm is the only scheme that can be used for providing non-repudiation check of an electronic document as supported by the Hong Kong Law.

4. Password, PIN or TIN in IRD's proposed tax-return system is not securely designed. According to the amendment made in the bill, "password means any combination of letters, characters, numbers or other symbols selected by a person and **approved by the Commissioner** for use in systems designated by the Commissioner for the purpose of authenticating the person's identification in communicating with the Commissioner;". Therefore, the Commissioner of IRD would have the privilege to access or review the password chosen by the taxpayer. In addition, in traditional shared password systems, the cryptographic checksum will be generated using the same secret which is known to both sender and recipient of the message. Therefore the password of the taxpayer is known to people other than the taxpayer.

   Furthermore, Itsik Mantin, Adi Shamir and Scott Fluhrer have pointed out RC4 has implicit cryptographic weakness in their article entitled "Weaknesses in the Key Scheduling Algorithm of RC4". According to their paper, RC4 is more applicable for stream data protection where keys would be re-newed each time after a message is encrypted. Therefore, IRD should be take special care in implementing encryption schemes that make use of RC4.

   Most of our members have to deal with digital evidence in security investigations. We hope that our comments would be helpful for IRD in modifying the password scheme as well as rethink the concept of password usage in authentication and identification applications.

5. The definition of in the bill proposed by IRD on the tax-return signature return process is **not clearly defined and not precisely written**. In IRD proposed bill, "...how a digital signature or password or any other signing device is to be affixed to a return furnished under this section ..." is proposed to be added to the IRD Ordinance. However, this does not clearly stated how the tax-return signature is generated and sent to IRD.

   The statement even implies that password is affixed to a return furnished under this section. ISFS believes that IRD has proposed a potentially infeasible use of password in the tax return system. We suggest modifying the wordings in the bill to avoid this ambiguity.

6. In IRD's proposed solution for tax return, it would be possible to use the password for identification and authentication purposes if it is known to the owner of the password only.

   Traditionally, passwords are kept in a hashed format in order to prevent others from obtaining the key to decrypt all the passwords. In the proposed IRD tax return system, passwords will be kept using the symmetric cryptographic scheme RC4 where any one with the encryption key and the encrypted file can immediately retrieve all the passwords on the file. Therefore, both the Commissioner of IRD and the taxpayer can authenticate him/herself to the IRD tax-return system as the genuine tax-payer. This weakens the evidence that IRD can provide to the court in the case of dispute.

Drafted by:
Information Security and Forensics Society Members

Ratified by:
Prof. Samuel Chanson, Chairman of ISFS
Mr. Ricci Ieong, Secretary of ISFS

Date: 17-Sept-2002