香 港 電 腦 學 會
Hong Kong Computer Society

Founder Member
South East Asia Regional Computer Confederation
SEARCC

HONGKONG COMPUTER SOCIETY

Rm 1915
China Merchants Tower
Shun Tak Centre
168 Connaught Road Central
Hong Kong

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

Comments on "Inter-departmental Working Group on Computer Related Crime Report"

Introduction

As a leading IT professional body in the HKSAR, the Hong Kong Computer Society (HKCS) welcomes the opportunity to actively participate in this consultation process and give our opinion.

The rapid growth of Internet-based applications has re-invented e-business, which has created tremendous opportunities for the IT industry, business sectors and home users. However, the security threat is still a great concern of consumers, as shown in numerous surveys, analyst reports or even peer talk. A prudent legal framework on computer related crime is definitely one of the essential enablers for promoting local, regional and global e-business developments. We feel that the Inter-departmental Working Group has prepared a comprehensive report, which is a necessary and timely review of the legal issues on computer related crime.

We present our specific comments and suggestions concerning the report.

Terminology

While we welcome the standardization of the term "information system" instead of "computer" or "computer system", we feel that it is necessary to provide a more comprehensive definition of "information system" in order to reduce the possibility of misinterpretation by readers in terms of its meaning and scope of coverage. (see comments on Sections 7.4 and 7.10).

Chapter 5: Encryption

We agree that regulating encryption programs is of limited use and that it is more appropriate to require the production of the decryption tool or decrypted text (see Section 5.14). However, we feel that the recommendation to make disclosure of the decryption tools available for more serious offences need to be looked at carefully. The execution of this recommendation, if accepted, would require clear definition and boundaries for what serious offences meant (e.g. pure commercial crime vs. crime of political nature) and how the disclosure of such tools is made.

Take the example of confidential email using PKI, we may look at three possible solutions to meet this requirement:

- the mail sender has to keep the clear text and the decrypted text for a period. How long should he/she keep? How to enforce?
- Government can control the encryption algorithm, like China or Russia. There is always a back door to decrypt the encrypted e-mail. It is not preferred. It will inhibit technology innovation, as Government control and endorsement is needed. New technology cannot be deployed fast.
- The private key of the mail receiver has to be escorted by a trusted third party. Currently, there is no such trusted party. Who can do that? Anyone can generate a private key a PC or even a smart card. How can we ensure that he/she must submit this private key for escorting? Further investigation is needed.

Also, there is a great danger in specifying a heavy penalty ($100,000 and imprisonment for one year, see Section 5.20) for failing to comply with a production order. The burden of proof appears to be on the accused: How does the subject of the "production order" (referred to as "Subject") prove they are incapable of decrypting the material? Would it be fair for the Subject to prove that the decrypted text provided actually came from the encrypted files?

Therefore, we think it is necessary that it be made quite clear that the burden of proof for failure to comply with a production order is firmly with the prosecution. For example, the prosecutor would need to prove that the encrypted file did contain incriminating evidence. In many cases, this evidence could be obtained by forensic examination or surveillance. We also feel that it is reasonable if the Subject convicted of non-compliance would be required to pay for the costs of the examination or surveillance in addition to the fine or imprisonment imposed.

Another issue that is not dealt with in this chapter is multi-use keys, for example, where a person uses the same private key for signing documents as for decrypting documents sent to them. Provision for issuing a certificate revocation for the relevant key should be built into the procedures of production orders.

Chapter 6: Protection of Computer Data

Section 6.19(a) unnecessarily uses "the Internet" – or does the report seek to exclude data on other telecommunications networks?

The wording and intent of 6.19(a) is unclear – what is "unauthorized interception"? For example, could an ISP authorize its staff to install a sniffer on its network to monitor the traffic statistics? Would this change if the purpose of the sniffer was to monitor the content of the traffic? Who can provide authorization, does the traffic belong to the sender, recipient or the carrier?

The recommendations of 6.19 also do not address the problem of port scanning and host scanning. Host scanning is where an attacker tries to connect to a service on a large number of machines, often a range of IP addresses, in the hope of finding a vulnerable server that can be exploited. Port scanning is where an attacker tries to connect to services on a large number of ports in the hope of finding a vulnerable service. In either case, it is like trying doors in the hope of finding one unlocked. Any firewall administrator can report on the large number of port scanning and host scanning attempts taking place, for example, in a real situation a firewall logs show over 1205 attempts aimed at a company's small network on the 19 January. The firewall blocks the attempts at access, so it is unlikely that an offence under the Telecommunications Ordinance could be proven for the protected machines. However, the attacker is probably scanning many other sites, and an unprotected victim will get no warning when his machine is penetrated. The company only detects the failed attempts, so there are no grounds for further investigation and prosecution. Currently, firewall administrators can complain to the administrators of the originating network, but they are not obliged to take action, and even if it breached an ISP's service agreement, the attacker can easily get an account at another ISP and continue the attempts, especially when competition for customers is so fierce.

Therefore, we recommend that the Telecommunications Ordinance should be amended to make port scanning and host scanning a minor offence, which could then be used as grounds for investigation of the attacker's machine to find evidence of successful attempts (which would then be crimes of unauthorized access). Even a small fine could be quite effective, if it was applied per connection attempt. Naturally, the law would need to be carefully drafted to distinguish between attempts with the intent to locate vulnerable targets, and attempts to connect to services that the user honestly believed were provided for public use on those machines.

We also support the recommendation on Section 6.23.

Chapter 7: Deception of Computers

The meaning of the phrase "theft of the chose in action" in Section 7.4 may require further clarification.

Regarding Section 7.10, it can be argued that a coin-operated shoe-polishing machine could be viewed as an Information System, which has the ability to decide to polish shoes based on information about the presence or absence of a coin. The common use of microprocessors in modern electrical/electronic devices makes it even easier to regard them as Information Systems.

Chapter 8: Assistance from ISP

Regarding Section 8.3 - some medium to large companies prefer leased line to the Internet access. Do ISPs have the same kind of information logged as dial-up user? Even a leased line has a fixed IP address though it usually will have many access points, such as PCs or servers, which start the Internet session. Is responsibility to log the session detail rests with the ISP or the company? If it is the company's job, further guidelines may be required.

The computer crime investigator wish list of records that ISPs should keep referenced in Section 8.6 and listed in Annex 6 seems excessive. Mail message content is one item in the indicative wish list of law enforcement agencies, as one type of records to be kept by an ISP. Certainly, the public will have privacy concern, as it is equivalent to all telephone lines are monitored, and all private phone conversation is under watch. How is this wish list taking in law drafting process? In particular, the keeping e-mail message content is a gross violation of privacy.

The meaning of the following statements may require clarifications:

- Dial-Up Access by Modem: what exactly are the E-mail Message ID, NNTP Posting ID and Webpage Address – are these for messages sent, pages created, or messages received and pages viewed?
- Individual Audit log of clients: Is this a requirement for ISPs to run Intrusion Detection on behalf of their customers. Mail servers redirect e-mail, not clients, so what does the e-mail re-direction refer to?

Regarding Sections 8.8 and 8.9 – the meaning of "traffic data" may require further clarification; is this statistical information of the types of traffic, details of the source and destinations of each packet, or the entire contents of the traffic?

In relation to Section 8.12, it should be noted that the US Digital Millennium Copyright Act (DMCA) has been widely criticized by free-speech advocates. In particular, the takedown procedures have been used against sites that carried DeCSS, an open source program that the Motion Picture Association of America (MPAA) claimed to be of use for illegal copying of DVDs, and even against site carrying links to those sites (see http://www.2600.com/dvd/docs/2000/0808-brief1.html) The DMCA can be seen as a powerful tool that major organizations who can afford expensive lawyers (such as the MPAA) can use to intimidate individuals who hold views they dislike.

Therefore, the recommendation in Section 8.30 to limit the takedown procedures to specific offences involving copyright protection, Internet gambling and pornographic material is to be welcomed. However, even here, it must be noted there is an implied assumption of guilt – if a site is "being investigated" for these crimes, it must be removed immediately because it is guilty! There must be a clear obligation for the ISP to restore the site if it is found innocent. However, for sites reporting news or announcing events, even this may be insufficient – the information may be irrelevant and the opportunity lost by the time the wheels of justice turn. For example, a site that advertises a limited-period exhibition at an art gallery might feature examples of the art. The exhibition could be over and the business opportunity lost by the time a court decides whether or not the examples displayed were obscene. Therefore, procedures for rapid resolution must be considered.

In addition, a number of administrative measures/guidelines for ISPs are suggested. It is important to note that such measures/guidelines though useful should not be restricted to ISPs as many different forms of relevant electronic service providers also exists and play an important role in e-Business.

Chapter 9: Protection of Critical Infrastructures

Regarding Section 9.7 - critical infrastructures are mostly not Government-run, and also, most of them are built by contractors, selected through open tendering process, as required by WTO procurement guidelines. Unless there is a very careful security design consideration in the tender, for low cost seek, contractors may not propose the most secured solution although they know how to do it. Even worse, some security assessment service tenders for those critical infrastructure systems are going through the same "the lowest price selection process". As there is no objective guideline for contractor security understanding and capability, the tenderer should pay more attention to company track record, contractor staff experience and other relevant certification. Otherwise, our critical infrastructure will be in-born vulnerable.

Regarding Section 9.16 - "crime prevention" is always more effective than "crime fighting". Adequate and effective impact analysis, risk assessment and security design for our critical infrastructure will be more important than a CERT establishment. In this aspect, IT, as a profession, similar to doctor, accountant and architect, should play a more active role to protect society critical infrastructure. The present problem is that IT is still quite new to develop a statutory recognized status and endorsement process for critical system design and commissioning. More work should be done as a joint effort by Government and IT industry. A good starting point is "CA assessor" in Electronic Transaction Ordinance. This model can be further developed and promoted.

The support of Section 9.21 of the Report for setting up a CERT in Hong Kong is welcome. However, it must be recognized that the recommendation in Section 9.22 for the CERT to cover the critical infrastructure is a significant additional responsibility above and beyond the proposals currently under consideration. If this recommendation is adopted, additional funds will be required to provide adequate cover.

Chapter 10: Public Education

These initiatives are by all means welcomed. For example, the HKCS has set up the Security Committee for some time. We hope Government can give us more support. The figure of US$10 billion for the estimated costs of the VBS/LoveLetter outbreak quoted in Section 10.3 is highly speculative and has been widely criticized. However, it is true that the costs of computer crime are high and growing.

Chapter 11: The Private Sector's Role

We (HKCS and our Special Interest Group on Information Security) have engaged in many of the activities listed in Section 11.7 such as in enhancing the awareness of IT professionals (e.g. seminars) and the general public at large of the IT security concerns (e.g. HKCS-RTHK's TV Programmes: IT Files and IT Files II). We encourage that the Report in Sections 10.7 and 11.9 should not only limits private involvement in public education via cash or kind, but not also expertise and professional support. In particular, Section 11.7 (b) suggests

developing guidelines for SMEs without addressing the need for input from security experts. Perhaps the government could establish a framework for security experts to work with such groups and permit the high cost of the experts to be spread across the beneficiaries, with government sponsorship. However, the commercial viability of many courses on information security is in question, especially as those who would benefit most from them are those who are least aware of the risks and problems, and may not be willing to pay sufficiently to cover the costs. Therefore, more concrete details of how the recommendation of 11.8 to encourage these efforts further will be implemented would be welcome.

In Section 11.3, the availability of Filter software is mentioned, but not the associated problems that the size of Hong Kong makes local commercial development infeasible but overseas products often fail to filter Chinese language sites and that this essentially puts censorship control in the hands of an unregulated, unreachable company that might have a hidden agenda. Also, security is often not a "standard feature" of Internet software, but a poorly implemented last-thought.

Chapter 12: Resources and Capabilities

In Section 12.11, the choice of name of the Anti-Internet Piracy Team is unfortunate – or is it really a team of pirates aimed against the Internet? Perhaps the name Internet Anti-Piracy Team is better.

Conclusion

We are very pleased that the introduction of more comprehensive laws on Computer Related Crime will be beneficial to Hong Kong as a commerce centre and IT hub. As a leading IT professional body in the HKSAR, we welcome the challenge and hope that the Government will co-lead the social and technical changes along with the industry, in a period of uncertainty and fast-changing environment.

Yours sincerely,

Daniel Lai

President
Hong Kong Computer Society

c.c.

Dr. Louis Ma	Vice-President,	HKCS
Mr. Bill Fok	Council Member,	HKC