LC Paper No. CB(2)811/00-01(01)

Comment and recommendation to the Inter-departmental Working Group on Computer Related Crime Report

By

Chester Soong, Chairman
Hong Kong Internet Service Provider Association

Executive Summary

On December 1st, 2000, the Inter-departmental Working Group released a report on Computer Related Crime. It becomes the attention of the HKISPA where several aspects of the report might have serious consequences to the industry if not implemented properly.

Technology such as encryption is a good and innocent technology which can help protect sensitive and critical business information from eaversdroppers. Siting examples from countries that are so different in their political backgrounds is unreal when applying to Hong Kong. In understanding that the importance of getting the decryption key and plaintext when encryption is used for criminal intent, **the association is in support of the third option for demanding the encryption key or plaintext through judicial scrutiny**.

In protecting computer data, the association is concerned the difficulty government might have dealing with internet related systems, where most of the contents, data and programs, of a server are either made available to the public. For the vast information that could be through the internet, it would be impossible for a person to first verify whether the information is authorized to be accessed by him/her beforehand. The same goes to data that are retrieved through media such as internet newsgroup in which must be proven stolen. **The association recommends a condition to be added so the person must have a criminal intent with the file accessed or disclosed**.

In many cases, "fooling" a computer without actually gaining access could cause serious consequences. **The association suggests to add the definition that "intentionally scanning and sending false data to a system which caused serious malfunction or damage" to the Computer Crimes Ordinance**.

In respect of the association, the HKISPA is supportive to the initiative done by the government in full. However, the methodology and scope of assistance would not cause interference to the ISPs to the extent that it is unbearable. The association agrees in context that certain critical information should be kept in order to help crime investigation when necessary. The length and content are very much in concern. **The association recommends the length of log to be kept at three months as a code of practice with contents of the log further discussed between government agencies and industry**. The HKISPA would like to play a more active role in assistance the fight of computer related crimes. **HKISPA would like to be involved in the Fight Crime Committee (FCC) to assist the committee to address the growing concern of computer crime**. The association is concerned with the HKCERT operation in their mode of operation and its expertise as well as experience in the subject matter.

As a key player of the IT industry, the HKISPA is here to help preserve a safe and prosperous cyber environment. We will help in any possible way to solve barriers that the government might come across and require our assistance.

Introduction

On December 1st, 2000, the Inter-departmental Working Group on Computer Related Crime of Hong Kong Government released a report on the position and proposed direction on the subject matter. It raised great deal of concern to the IT industry and general public on the level and practicality of the enforcement levied by the report. HKISPA, as the representing body of the Internet Service Providers in Hong Kong, feels responsible to present the concerns and recommendations from the industry.

The general position of HKISPA to the report and initiatives done by the government is positive. It is encouraged that the government is given serious attention to the issues related to the growing concern of computer crime. However, Information Technology is a unique area that require special care and procedure. While Hong Kong is competing with regional cities to become the internet and e-commerce hub of Asia, a solid foundation on legal and technological infrastructure are of equal importance. However, there are limitations to technologies which make investigation difficult. Although assisting the law enforcement agencies to investigate computer related crime and prosecute computer criminals are every netizen's responsibility, sometimes it is technically impossible to provide assistance to the exact level demanded by the agencies. In this commentary, I wish to bring to your attention the points that we found unacceptable to the industry and the recommended alternative if possible.

Chapter V: Encryption

Encryption is the process of transforming plaintext to ciphertext (encrypted text) through a mathematical process. This process is mathematically impossible to be reverse engineered nor decrypted without the encryption key. When used properly, encryption can bring many good things to daily life. Sensitive and critical business information could be protected from disclosure to unauthorized people, and non-repudiation could be enforced. Just like a medical needle, it is totally innocent and a beautiful technology. It is not difficult to understand that many criminals see the benefits of using encryption to commit crime. However, we have to be very careful of controlling or even taking away the right of using encryption. This will seriously damage the reputation of a democracy government which Hong Kong is trying very hard to achieve.

In the report, it pointed out several example from other jurisdictions. It is easy to pick out examples from other countries. However, all of these countries have different cultural and technological histories. The report stated that countries such as China, Russia, and Saudi Arabia prohibits the use of unauthorized encryption. These countries are so different in their political backgrounds that is unreal to compare Hong Kong with these countries. How does the government define the use of encryption and give authorization to every count of use? If this comparison is valid, why didn't Hong Kong Government allow Hong Kong residents to bear arms? The American does. Even with the newly passed Regulation of Investigatory Powers Act 2000 was heavily criticized by industry and other private sectors for overpowering the authorities.

For the options of controlling the use of encryption, the first two options mentioned in the report are very difficult to administer for its fairness. From the angle of a law enforcement officer, it would always be better to have more information at hand than less. So the urge to demand for the decryption key or plaintext would be natural even the circumstancials may not prove necessity. It would also be impossible for the Bureau Secretary to examine every such case to grant the authorization. In understanding that the importance of getting the decryption key and plaintext when encryption is used for criminal intent, **the association is in support of the third option, judicial scrutiny**. I would like to point out that requesting for plaintext alone does not make the process less serious than getting the decryption key. This is because without the right decryption key, there is no way anyone can verify the plaintext is really the one being requested.

Although penalties from computer related crimes were increased over the years, the association still feels the need for strengthening the legislation by increasing the penalties for serious and organized crime using or targeting a computer.

Chapter VI: Protection of Computer Data

In Options Section, the association is concerned the difficulty government might have dealing with internet related systems, where most of the contents, data and programs, of a server are either made available to the public. Some programs, on the otherhand, are required to be accessed technically in order to retrieve other information/data from the server or other servers on the internet. The explicit rights of these files are usually not clearly defined under contractual agreement. While the protection of information should cover all forms (being stored, during processing, or being transmitted), it is extremely difficult, if not impossible, to catch all computer data at all stages of storage or transmission. Problem may also arise when a person accidentally accesses certain private information without authorization. For the vast information that could be through the internet, it would be impossible for a person to first verify whether the information is authorized to be accessed by him/her beforehand. The same goes to data that are retrieved through media such as internet newsgroup in which must be proven stolen. **The association recommends a condition to be added so the person must have a criminal intent with the file accessed or disclosed**.

Chapter VII" "Deception" of Computers

As similar to other technical issues, deception of computers is very hard to define in many cases. Some could be mis-configuraiton of the target system itself, and may not well be the fault of the person who "got into" the target system. In many cases, "fooling" a computer without actually gaining access could cause serious consequences. Incidents of "Denial of Service" (DOS) attacks which caused many giant websites, such as CNN, Yahoo!, Amazon.com, etc, to be down for hours is one good example. The process of a DOS attack usually begin with a scanning of target system to find system bugs and mis-confirgurations, and the cracker will then send large amount of false data packets to flood the communication channels and system resources of target computer to crash it. These kind of compute vandals never require to gain access to launch an attack. **The association suggests to add the definition that "intentionally scanning and sending false data to a system which caused serious malfunction or damage" to the Computer Crimes Ordinance**. However, the prosecutor must proof that the sender's action is intentional with malicious intent.

Chapter VIII: Assistance from Internet Service Providers (ISPs)

In respect of the association, the HKISPA is supportive to the initiative done by the government in full. However, the methodology and scope of assistance would not cause interference to the ISPs to the extent that it is unbearable. ISPs, in many cases, are being defined as the conveyor of information. Unfortunately, computer crime and illegal contents were also transmitted through ISPs sometimes. This makes the false impression that ISPs should hold the key to unlock many puzzles in this regards. For example, taking down an offending site seems to help with preventing the crime, but it may actually tip off the suspect depending on the nature of the crime. Log keeping is another major concern from the industry. The length and content of the log raised not only concern the industry with heavy maintenance costs, but also legal consequence of invasion of privacy. Viewing the content of a customer's access log may reveal copyrighted information that could put the ISP in legal actions.

During the consultation before the report was finished, HKISPA explained the difficulty and costs of retrieving caller's number during the logon process. Unless the fixed network provider provides such information free of charge, otherwise the ISP would have to invest its own equipment and labor to capture such information. With the large number of modem lines and users for a ISP, this cost could be unbearable. Technically speaking, the fixed network providers would be in the best position to capture and provide such inform. Such information is also unavailable when the user gets his/her connection using pre-paid access cards, pre-paid Mobil sim cards, and international roaming service.

The association agrees in context that certain critical information should be kept in order to help crime investigation when necessary. The length and content are very much in concern. Although the report suggests that record should be kept for six months, the amount could be huge if not constrained on kind of information to be logged. Some of the items in the Indicative Wish List from the report are not only ridiculous, but also technically impossible. Any ISP requires to keep such composite of log must invest large sum of capital in computer security tools and expertise. **The association recommends the length of log to be kept at three months as a code of practice with contents of the log further discussed between government agencies and industry**.

Multiple logins purport the problem of account misuse. This practice is currently up to each individual ISP to decide whether or not enable such function. **The association supports its member to disable such function by default unless difficult technical barriers exist**.

In summary, the HKISPA would like to play a more active role in assistance the fight of computer related crimes. The association has been in dialog with various law enforcement agencies, especially the Commercial Crime Bureau of Hong Kong Police. We would like to continue such interaction. We feel, however, that the ISPA is in a passive role when any government agency think of something, it would release a consultation paper for us to comment. The response is then passed to the respected agency for review. The process goes on for a couple rounds, but we never get to really contribute any idea before the ideas from the government are put together to form various reports. We believe it will help the government to better tackle many social and technical problems in regards to computer crimes with our technical expertise at the initial phase of any such exercise. **HKISPA would like to be involved in the Fight Crime Committee (FCC) to assist the committee to address the growing concern**.

Other areas of concerns

The association glad to see the government is finally decided to build a CERT (Computer Emergency Response Team) operation in Hong Kong. But the association is concerned with the mode of operation and its expertise as well as experience in the subject matter. The neutrality of the operation also raised concern to the security consulting and training industries where the operation will be in direct competition with them.

Conclusion

Computer related crime is inevitably a growing problem. The technological advancement makes it become a race against time. As a key player of the IT industry, the HKISPA is here to help preserve a safe and prosperous cyber environment. We will help in any possible way to solve barriers that the government might come across and require our assistance.