In Proceedings of ACM Conference on Computer and Communications Security, pp. 62-67, March 1996.

The Failure of Anti-Hacking Legislation: a Hong Kong Perspective

Invited Paper

Rynson W.H. Lau * Kwok-Yan Lam † Siu-Leung Cheung ‡

Abstract

This paper observes the Hong Kong Government's position on Internet issues, and discusses why present computer-related legislation fails to attain its goal of anti-hacking. The paper gives a Hong Kong perspective to government's effort to curb intrusion of businesses on the Internet. The Internet has grown dramatically in recent years with tens of millions of people having access to it. There are also increases in both varieties and number of businesses operating on the Internet. It is therefore more profitable for serious intruders to break into the global network and obtain illegal access to network resources. The situation will only deteriorate if not handled promptly and in a proper manner.

1 Introduction

In recent years, the Internet has grown to be a major component of network infrastructure, linking millions of machines and tens of millions of users around the world. In Hong Kong there is an estimate of around 10,000 public users on the Internet. As the number of commercial Internet services providers increases, the price for accessing the global network will drop substantially due to harsh market competition. This is likely to encourage more people to subscribe to the cyberspace which results in a more significant expansion of the local user community in the near future.

In Hong Kong, the varieties and number of businesses operating on the Internet are also experiencing a remarkable growth. As a business and financial hub in the Far East Asia, Hong Kong has been famous for her ability to deploy new technology to establish businesses and/or to improve competitiveness. Broadly speaking, there are two kinds of businesses operating on the Internet in Hong Kong – one that offers Internet service, such as electronic mail (Email), to users, and one that carries out businesses on the network such as catalogue sales and on-line shopping.

Wide popularity and ever expanding user community on the Internet lead to a greater potential for computer-related crime in Hong Kong. It is perceived that abuses by hackers to commit computer-related crimes via the Internet is on the rise. Firstly, the increasing application of computers to almost every aspect of business activities creates more opportunities for computer abuses. Secondly, the increasing computer literacy amongst the populace also means that the skills and knowledge required to commit such crimes will spread. Computer criminals will have little difficulties in acquiring the level of skills to commit these crimes.

As more businesses depending on access to the Internet are built, the amount of money being transacted daily on the network will experience a significant pace of growth. Therefore, the financial returns for breaking the network will attract more sophisticated intruders to the arena.

It can be foreseen that continuous growth of the Internet community will eventually make users activities outside the control of the authority. This may lead to the detrimental consequences that proper business operations on the Internet be jeopardised.

In order to protect interests of users and sustain growth of the industry, the Hong Kong government realised the earnest needs for ensuring the integrity of the Internet. For example, a young man, who successfully gained unauthorised access to a number of Internet sites, was convicted in April 1995, for the first time in Hong Kong's history, under the Computer Crime Ordinance 1993. Although the first prosecution of its kind in Hong Kong, a deterrent sentence was imposed upon the convicted, a first offender. The excerpt of the court sentence is as the following [1]:

> Although a deterrent sentence is not usually imposed upon a first offender there is no absolute bar. There are appropriate cases in which it may be done. These are offences with ... the potential of extremely serious consequences. There should be a serious effort to stop these offences becoming commonplace and this partially can be done by imposing a deterrent sentence in this matter so that others similarly tempted appreciate the possible outcome of their actions.

Besides, on another occasion, the HK Commercial Crime Bureau raided seven unlicensed Internet service providers with their software, hardware and communication equipments seized by the authority. As it was pointed out by the HK Commercial Crime Bureau, the reason police initiated the action is that these organisations have been used for hacking.

This paper gives a Hong Kong perspective to means of maintaining integrity of businesses on the Internet and discusses the insufficiency of present legislation to attain this goal. Measures are based on strict enforcement of the relevant legislation to regulate the behaviour of network users.

*Dept of Computing, HK Polytechnic University, HONG KONG
†DISCS, National University of Singapore, SINGAPORE
‡School of Business & Administration, OLI, HONG KONG

However, stern difficulties are expected to be encountered when implementing such measures to achieve the intended goal. This is mostly due to the novelty of the technology to law-enforcement agents. The Internet technology is relatively new to the law-enforcement agents in Hong Kong, hence special training is needed for officers to collect evidence in the cyberspace. Furthermore, it is perceived that regulating the behaviour of network users is not sufficient. Considerable effort must be paid to regulate the operations of service providers at the same time. Therefore, the authority took steps to require Internet service providers to operate with a valid licence. However, this goal can hardly be achieved due to insufficiency of the legislation in this area.

In this paper, we observe the government's responses on the Internet issues. Section 2 presents the relevant legislation in Hong Kong that effects the regulations of computer users. Section 3 provides information on the HK Government's recent moves against malicious network users. This is followed by a discussion on how present computer-related legislation fails to attain its goal of anti-hacking.

2 Hong Kong Legislation

Hong Kong Legislation relevant to the protection of integrity of businesses on the Internet is mainly covered by the Computer Crimes Ordinance. The Hong Kong Computer Crimes Ordinance 1993 (CCO'93) [2] was enacted on 23 April 1993 to clarify and amend the law relating to the misuse of computers. Issues concerning computer fraud and computer abuses which constitute major threats to information systems security were addressed by the Ordinance. The CCO'93 is the first legislation of its kind in Hong Kong and, in fact, in the Far East Asia.

Prior to the CCO'93, there has never been any specific legislation in Hong Kong regulating computer-related activities. Anticipating the growing use of computers in a highly dynamic and efficient international trading and financial centre as Hong Kong, the Hong Kong Government realised the potential threats posed by computer crimes and the importance of a legislation designed to guard against misuses.

The CCO'95 consists of a number of amendments to existing legislation; namely the Telecommunication Ordinance, the Crimes Ordinance, and the Theft Ordinance. The effect of these amendments is to either create new offences or include in various existing offences, by extending the definition of "property", the protection of computers, storage media, programs and data.

2.1 Telecommunication Ordinance

A new offence of "Unauthorised access to a computer by telecommunication" has been added to the Telecommunication Ordinance [3]. The amendment is provided by a new section 27A which reads as follows:

> Any person who by telecommunication, knowingly causes a computer to perform any function to obtain unauthorised access to any program or data held in a computer commits an offence and is liable on conviction to a fine of $20,000.

This amendment makes hacking an illegal act by anyone not authorised to access a computer, its program or data. As defined by the ordinance, access of any kind by a person to any program or data held in a computer is unauthorised if he/she is not entitled to control access of the kind in question to the program or data held in the computer and

- he/she has not been authorised to obtain access of the kind in question to the program or data held in the computer by any person who is entitled;
- he/she does not believe that he/she has been so authorised; and
- he/she does not believe that he/she would have been so authorised if he had applied for the appropriate authority.

For the purposes of the amendment, unauthorised access alone constitutes an offence under the Telecommunication Ordinance regardless of the intent of the intruder. The intent of the person need not be directed at

- any particular program or data;
- a program or data of a particular kind; or
- program or data held in a particular computer.

It should be noted that "Access with criminal or dishonest intent" is a separate offence which carries a heavier punishment.

2.2 Crime Ordinance

The traditional crime law concept needs to be adjusted in order to allow computers and data to be protected under the Crime Ordinance [4]. One reason being that traditional legal principles invariably focus on protection of property of a tangible kind. Thus in situations where corruption of data or interruption of computer programs is involved, it is uncertain as to how a charge may be raised on grounds of criminal damage because neither program nor data is regarded as property in the criminal law context.

The CCO'93 amended the Criminal Ordinance where the definition of "property" was extended to capture the notion of computer data. Section 59(1) of the Crime Ordinance which provides a definition of "property" in relation to "Criminal Damage" is repealed and replaced by a new subsection which includes any program or data held in a computer or in a computer storage medium, whether or not the program or data is property of a tangible nature.

Firstly, a new subsection 59(1A) has been added so that, in relation to a computer, "to destroy or damage any property" includes the misuse of a computer. In this subsection, "misuse of a computer" means:

(a) to cause a computer to function other than as it has been established to function by or on behalf of its owner, notwithstanding that the misuse may not impair the operation of the computer or a program held in the computer or the reliability of the data held in the computer;

(b) to alter or erase any program or data held in a computer or in a computer storage medium;

(c) to add any program or data to the contents of a computer or a computer storage medium.

Thus, any act which contributes towards causing the misuse of a computer shall be regarded as causing a criminal damage. The maximum penalty under this category is 10 years imprisonment.

Secondly, a new offence of "Access to computer with criminal or dishonest intent" has been created as section 161 of the Crime Ordinance. In many cases of computer fraud, accessing a computer is only a preliminary step in committing the fraud. The actual fraud may be committed long after accessing the computer. Since access to the computer is merely a preparatory step, it is difficult to convict the accused of even the offence of criminal attempt. The CCO'93 tackles this by making it an offence for anyone to access a computer with a criminal or dishonest intent, regardless of whether the access is authorised or not.

Section 161 states that a person commits an offence when he/she obtains access to a computer

(a) with intent to commit an offence;

(b) with a dishonest intent to deceive;

(c) with a view to dishonest gain for himself or another; or

(d) with a dishonest intent to cause loss to another,

whether on the same occasion as he/she obtains such access or on any future occasion. This offence carries a maximum penalty of five years imprisonment.

Thirdly, the Forgery offence spelt out in section 85 is adjusted. The offence of "Making false entry in a bank book, etc." is amended so that "books" include any disc, card, tape, microchip, sound track or other device on or in which information is recorded or stored.

2.3 Theft Ordinance

The Theft Ordinance [5] was amended by the CCO'93 so that the offence of "Burglary" includes trespassing with an intent to tamper with computers, programs, or data. The amendment is reflected in section 11 where a new subsection (3A) was inserted so that the offence of "Burglary" includes trespassing in a building with the intention of

(a) unlawfully causing a computer in the building not to function normally;

(b) unlawfully altering or erasing any program, or data, held in computer in the building or in a computer storage medium in the building; and

(c) unlawfully adding any program or data to the contents of a computer in the building or a computer storage medium in the building.

Any person who commits burglary shall be guilty of an offence and shall be liable on conviction upon indictment to imprisonment for 14 years.

Furthermore, section 19, which related to the offence of "False accounting" has also been amended so that "record" includes those records kept by means of a computer.

3 The Government's Position

In face of the growing threats posed on the proper functioning of businesses on the Internet, the Hong Kong Government has taken stiffer actions against offenders of IT-related legislation. Recent moves by the law-enforcement agents were targeted at both Internet users and service providers. In the case of intrusion by Internet users, the CCO'93 was used to prosecute the culprit so as to deter future intruders from challenging the legislation. When dealing with Internet service providers, the licensing requirement for operating a public telecommunication service was strictly enforced.

Recently, the government has taken a series of steps to strictly enforce the legislation relevant to the integrity of the Internet. In the earlier part of this year, the Hong Kong Commercial Crime Bureau (CCB) had successfully convicted an Internet intruder, using the CCO'93, of "unauthorised access to a computer by telecommunication". At about the same time, the CCB raided seven unlicensed Internet service providers with their hardware, software and telecommunication equipments seized.

The first court case in Hong Kong related to intrusion of Internet sites was conducted at the beginning of 1995. The hacker was charged by the CCB under the CCO'93 – Section 27A of the Telecommunication Ordinance – of "unauthorised access to computers via telecommunication means". The Accused is the son of a lecturer of a local university who came back to Hong Kong in 1993 from the US. The hacking was performed using his father's university computer account which gave him unrestricted access to the Internet. From there, he started to break into machines in other Internet sites, both local and overseas.

The hacking activity was noticed by a system administrator of a local Internet service provider who became suspicious at the beginning of the latter half of 1994 that unauthorised access was being gained to their company's service. The system administrator lodged a police report which triggered the CCB to launch an investigation attempting to locate the intruder. Various investigations were made. As a result, the Accused came under suspicion. Hence, the investigations continued with greater focus upon the Accused. In due course the police has decided to mount an intensive monitoring session in the hope of apprehending the intruder.

On 8 October 1994, the system administrator was alerted, via devices he had set, that an intrusion had occurred using a particular telephone line into his computer. The HK Telecom confirmed that, at the appropriate time, a connection was made on that line from the Accused's parents' residence at Tai Koo Shing. The police went immediately to Tai Koo Shing where, by subterfuge, they gained entry and arrested the intruder.

In parallel to these events, evidences related to the case were collected by a member of the academic staff of another local university who was suspicious that the UNIX network in his department was intruded. The academic first noticed that someone had executed a password cracking program on one of the departmental machines more than once. He immediately suggested the possibility of intrusion by some (possibly unauthorised) user, and started his own investigation during the summer of 1994. He then discovered that most of the departmental computers contained programs that allow someone to become a "superuser" upon entry to these computers. Among them, there were programs that

- monitors and collects passwords from the network,
- allows access to users' accounts via the sendmail loophole, and
- cracks users' passwords.

In addition, password files from some overseas universities with cracked password were also discovered. The intruder hided most of these programs and files in directories of occasional users. The intruder also modified these users' **.rhosts** files in order to gain access to the UNIX systems freely.

After a lengthy trial process, the police successfully convicted the hacker under section 27A of the Telecommunication Ordinance, which carries a maximum fine of $20,000. Although the first prosecution of its kind in Hong Kong, a deterrent sentence was imposed upon the convicted, a first offender.

The successful prosecution of the Internet intruder may help the CCO'93 achieve some desired deterrent effect against computer-related crimes. The abovementioned case is likely to have a positive impact on the enforcement of the legislation related to data and information security. However, protection of computer systems and data cannot totally rely on anti-hacking law and punishment against intruders, it also depends heavily on the strength of security measures that the systems used to safeguard themselves from being abused and misused by their users. Present Legislation, however, seems to be insufficient to address this aspect of the Internet security issue.

On 3 March 1995, the CCB of the Royal Hong Kong Police launched a series of raids on seven local commercial Internet service providers. Equipment and computer data from two of the ten premises searched were seized. Seven men and one woman were detained for questioning and later released on bail. No charges had been laid however.

The police's action was taken on grounds that these Internet service providers were operating without a valid licence. The search warrant used by the Commercial Crime Bureau to gain access to at least two of these companies' premises stated that they were "maintaining any means of telecommunication without licence" in contravention of Caption 106 Section 8(1)(a) of the Telecommunications Ordinance. The raids were assisted by personnel from the Telecommunication Authority (TA) who took the role of technical advisor to the police to make sure the equipment and data seized were related to the investigation.

4 Insufficiency of Legislation

Although negative comments towards the authority's actions against unlicensed service providers were raised both locally and internationally, the government's movement on this issue may still be justified from the point of maintaining integrity of Internet service providers. After the raids, thousands of Internet users were unimpressed that their links to the global "information highway" were severed. It was inevitable that the raids on the Internet service providers had not only triggered a lot of chaos and confusions amongst the Internet users community, but also aroused deep concerns from the general public on the rational behind the whole action taken by the authority. According to statements released by the police after the raids, their actions may be justifiable. Firstly, they were acting on complaints by the Telecommunication Authority that the companies were operating without a designated licence. Secondly, according to a statement made by a CCB spokesman, it was believed that the services provided by these unlicensed organisations have been used for hacking, and the raids were also related to an investigation into computer-related crime cases. Furthermore, the rapid growth of the Internet service providing business also raised concerns from the authority. As it was pointed out by the police spokesman:

> In the last few months, the Internet area has grown wild. Suddenly a large number of unlicensed providers came on the market. We felt now was the time to do something rather than wait till it becomes a very huge and out of control commercial enterprise. It is vital that the services providers operate on a commercial footing.

It did not seem to be a coincidence that the prosecution of the abovementioned Internet intruder and the raids by the police happened at a very close period of time. In fact, security is one of the most neglected aspects in the systems operated by most of the commercial Internet providers. According to our survey done on the services provided by some of these companies (see Figure 1), all of the providers allow users to utilise their Internet services through accounts which possess full UNIX programming environment. However, when asked about the kind of security measures being employed, their answers have not been satisfactory. Those organisations being surveyed either refused to respond or were reluctant to respond to question concerning security. Among those who responded, most of them did not understand the meaning of those security measures being surveyed. Thus, the competence of those dedicated security administrators are also questionable. Unfortunately, under this restriction-free environment, with uncertain security measures, users with computer hacking experience may break the system's security mechanisms and gain access to other users' account and even other computers. The security impact on the cyberspace due to this open mode of operation of the commercial service providers will become more severe if the user-base maintains its present growth rate.

Features	Percentage
full UNIX programming environment	100
system monitoring	30
dedicated security administrator	50
holding a valid licence	90

Figure 1: Features of Internet service providers

Nevertheless, the police's movement has been proven to be ineffective in regulating the healthy operation of Internet service providers due to shortcomings of the existing legislation. Shortly after the police's raids, six of the seven service providers had been granted a designated licence by the TA immediately upon receipt of their applications. The whole incident was ended without a single person being charged by law of any kind. This embarrassing action taken by the authority, even though its intention can be well justified, suggested that the present legislation cannot provide enough control over this fast expanding technological business and adequate protection to the interest of the users of the services and the general public.

It is believed that the Internet issue cannot be solved by simply imposing the required licensing conditions upon service providers. The major problem is the lagging behind of the present legislation vis-a-vis the rapid growth of the Internet business. The confusing actions of the police was due to the fact that while there was a perceived need to slow

down the growth of Internet-related businesses, the most suitable licence for the provision of Internet services to the public was not designed to regulate the operation of Internet service providers. Thus, the licensing conditions required to be met by licence holders were not helpful to evaluate the fitness of applicants. Due to pressure from the public to allow these service providers to resume their operations, each of them was granted a licence by the authority before the licensing conditions were clarified.

The appropriate licence for the provision of Internet service to the public is the Public Non-Exclusive Telecommunication Service (PNETS) licence provided for under the Telecommunication Regulations [3]. In order to maintain the integrity of Internet service upon which businesses are operated, there are sound reasons for requiring public Internet service providers to be licensed and thus regulated by the TA. For example, to protect the confidentiality of user data and the messages sent by users through the Internet, to protect users from discriminatory or unfair treatment, and to enforce compliance with international obligations and local regulatory framework.

However, the PNETS licensing conditions are unlikely to help achieve the goal of anti-hacking due to the lack of guidelines on evaluating the security standard of computer systems deployed by the licence applicants. The present PNETS licensing conditions [6] are mainly directed towards services such as international long-distance call dial-back services, which are closely related to traditional telecommunication technologies. The interpretations of "vague" wordings in the general licensing criteria created lots of confusion that even the authority found it difficult to evaluate the fitness of the PNETS licence applicants. For example, conditions such as "The service proposed must be technically sound and compatible with the local environment" is hardly relevant to the aim of requiring integrity and security of computer systems operated by the service providers.

In face of this shortcoming of the present legislation, a new set of licensing conditions and guidelines should be imposed. The new conditions and guidelines should be formulated in accordance with the present advances in computer and networking technology. It is also important to ensure that the holders of the licence can adequately circumscribe the operations of the Internet service business in the light of maintaining reasonable security and integrity.

5 Discussion

The wide publicity of the recent Internet issue not only corrected the attitude of the public towards computer and communications security, it also raised the concern of the law-making bodies on the importance of prompt responses to new technology. While the series of incidents exposed the weaknesses of existing legislation in maintaining the healthy functioning of the "information superhighway", there are important lessons to be learned both by the authority and the public.

These events educated the public to be more cautious when security issue is involved. Prior to these incidents, people tended to ignore the importance of system security or had the misconception that computer security meant computer virus which was only confined to personal computers.

The maximum fine carried by the offence of "unauthorised access to computers" is hardly enough to have any deterrent effect on professional hackers who are determined to intrude for a profit. The maximum fine of $20,000 on conviction of the Telecommunication Ordinance section 27A is insignificant when compared with the average income of a typical programmer. In Hong Kong, a fresh computer science graduate makes around $10,000 to $12,000 per month on average. It is not unusual that someone with two years experience in programming can earn a monthly salary of more than $20,000 at this moment. It is therefore suggested that the maximum fine carried by the offence be revised regularly so as to achieve its deterrent effect.

With the present level of technical sophistication, charging the culprit with a more serious offence is still not realistic. Even though there are other offences created by the CCO'93 that carry a jail sentence, the prosecution will be formidable due to the difficulties of collecting evidence in the cyberspace. According to the Telecommunication Ordinance Section 27A, the proof of "unauthorised access" by the accused is sufficient to cause a conviction (see Section 2.1). However, in order to convict the accused under a more serious charge that carries a jail term, such as the Crime Ordinance Subsection 59(1A), the prosecution needs to prove that the accused indeed had a criminal intention when acting on the offence. The process of collecting evidence to prove the criminal intention of the accused is necessarily much more difficult than the proof of "unauthorised access". It is perceived that more advanced training is needed by the police in order to make this feasible.

In addition, there are more work to be done by the authority on the guidelines for evaluating PNETS applicants. Security and integrity, by and large, cannot be maintained by measures such as simple password-type access control. A more stringent set of security standards should be imposed to all the public Internet service providers. The raids and strict enforcement of the licensing policy on the service providers indicated that the authority did realise the necessity of imposing control of some kind towards this emerging business built upon technology which is by no mean fully knowledgeable to the majority of the general public and even to the authority itself. The government is therefore suggested develop the strength in this area and prepare vivid security requirements based upon which the granting of the PNETS licence will be considered.

In Hong Kong, there exist another kind of vulnerable Internet service providers which are not regulated by the legislation. Apart from those commercial service providers, there are seven universities providing access to the Internet to their staffs and students. The number of users from these institutions is in fact much bigger than that of subscribers of commercial service providers. However, the operation of Internet service by these universities are not subject to the licensing requirements of the Telecommunication Ordinance. This is because access to the Internet via local universities is generally not available to the public and hence is not regarded as a public service. It is therefore essential to require local universities to step up their efforts to protect their systems from hacking in order to achieve the anti-hacking goal of the authority. The government and the universities' administrations should put more emphasis on the network security issue and provide more resources to address this issue properly.

6 Conclusion

Advances in information technology not only created a lot of convenience in life and business opportunities to the general public but also attracted new kinds of criminal offences which are collectively known as "computer crimes". Because of the novelty of the technology and the fast growth of the number of people involved in activities related to information technology, computer crimes are difficult to detect or prevent.

The new Hong Kong Computer Crimes Ordinance 1993 (CCO'93) was enacted on 23 April 1993 which clarify and amend the existing law to cope with crimes in the area of Information Technology committed in the colony. The success of this computer crimes legislation will rely on whether it can be enforced effectively which in turn depends on the effectiveness of the techniques for detection and investigation in face of this ever changing technology.

The Internet raids incidence indicated that the present legislation is not sufficient to provide appropriate guidelines for maintaining security and integrity of the Internet business. Like most other criminal issues, prevention is always a better approach than punishment. The raids of the seven unlicensed Internet service providers by the HK Commercial Crime Bureau indicated clearly that the authority is aware of the necessity of keeping stiff regulation on the operation of this fast-growing IT business. However, under the current legislation, the only control the Government can impose on the operations of this business is through the granting of the PNETS licence. Due to the novelty of the Internet technology, the PNETS licensing conditions, which are targeted towards certain traditional telecommunication services, are not aimed at regulating the operations of Internet service providers.

More legal issues have to be addressed in order to maintain Kong Kong's competitiveness in the business world through use of information technology which are both effective and trustworthy.

7 Acknowledgement

The authors would like to thank the Royal Hong Kong Police Commercial Crimes Bureau for providing us with valuable information concerning some of the Internet incidents. We are indebt to Detective Senior Inspector Steve Yau and members of his team especially Sergeant Pau and Sergeant Chan for their kind assistance during the course of this research.

References

[1] *HK Court Case* Number E18679

[2] *Computer Crimes Ordinance*, Ordinance no. 23, HK Government Gazette, 23 April 1993 Cap 106, Laws of Hong Kong.

[3] *Telecommunication Ordinance*, Cap 106, Laws of Hong Kong.

[4] *Crime Ordinance*, Cap 200, Laws of Hong Kong.

[5] *Theft Ordinance*, Cap 210, Laws of Hong Kong.

[6] Telecommunication Authority, Hong Kong. *Guidelines for the Application for Telecommunication Licences to Operate Public Telecommunication Services in Hong Kong*, Issue No. 9, March 1995.