UTeM

اونيۏرسيتي تيکنيکل مليسيا ملاک

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

Always A Pioneer, Always Ahead

UTeM

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

MyUTeM

BITS 2523
Cyberlaw & Security Policy
Lecture 5

By

Mohd Fairuz Iskandar Othman, PhD

mohdfairuz@utem.edu.my

Internet and Computer Crime

Topics covered:

- Nature and scope of Computer Crime
- What are computer, and internet crimes?
- Classifications of cyber crimes
- The impact on law enforcement
- The elements of a crime
- The role of computers in crime
- Computer Crimes Act 1997
- Communications and Multimedia Act 1998
- Penal Code
- Example Cases

Nature and scope of Computer Crime

- Cybercrime is easy to commit (if one has the know how to do it), hard to detect (if one knows how to erase one's tracks) and often hard to locate in jurisdictional terms, given the geographical indeterminacy of the net.
- They are really very complex crimes.
- Cyber criminals exploit the country as well as victimize the fellow citizens.
- A cyber criminal can destroy web sites and portals by hacking and planting viruses, play online frauds by transfer of funds from one corner of the globe to another and gain access to highly confidential and sensitive information.

Nature and scope of Computer Crime (cont…)

- Moreover, he can cause harassment by e-mail threats or obscene material, play tax frauds, indulge in cyber pornography involving children, and commit innumerable other crimes on the Internet.
- With the growing use of the Internet, cyber crime would affect us all, either directly or indirectly.
- Cyber crime such as hacking, planting computer viruses and online financial frauds, have the potential of shaking economies.
- Thus, cyber crime is the new emerging trend of crime which has the potentiality to destroy each and every aspect of life.

What are computer, and Internet crimes

- Computer crime is a general term that embraces such crimes as phishing, credit card frauds, bank robbery, illegal downloading, industrial espionage, child pornography, kidnapping children via chat rooms, scams, cyberterrorism, creation and/or distribution of viruses, Spam and so on. All such crimes are computer related and facilitated crimes.
- Internet crime is crime committed on the Internet, using the Internet and by means of the Internet.

What are computer, and Internet crimes (cont...)

- With the evolution of the Internet, along came another revolution of crime where the perpetrators commit acts of crime and wrongdoing on the World Wide Web. Internet crime takes many faces and is committed in diverse fashions.
- They are crimes that are only committed while being on the Internet and are created exclusively because of the World Wide Web. The typical crimes in criminal history are now being brought to a whole different level of innovation and ingenuity.
    - Such new crimes devoted to the Internet are email “phishing”, hijacking domain names, virus infection, and cyber vandalism.

Classsification of cybercrimes

- Harassment via E-Mails: It is very common type of harassment through sending letters, attachments of files & folders, i.e.: e-mails. At present harassment is common as usage of social sites, i.e.: Facebook, Twitter etc. is increasing day by day.
- Cyber-Stalking: It means expressed or implied a physical threat that creates fear through the use to computer technology such as internet, e-mail, phones, text messages, webcam, websites or videos.
- Dissemination of Obscene Material: It includes Indecent exposure/ Pornography (basically child pornography), hosting of web site containing these prohibited materials. These obscene matters may cause harm to the mind of the adolescent and tend to deprave or corrupt their mind.

Classsification of cybercrimes (cont…)

- Hacking: It means unauthorized control/access over computer system and act of hacking completely destroys the whole data as well as computer programmes. Hackers usually hacks telecommunication and mobile network.
- E-Mail Spoofing: A spoofed e-mail may be said to be one, which misrepresents its origin. It shows it's origin to be different from which actually it originates.
- Child Pornography: It involves the use of computer networks to create, distribute, or access materials that sexually exploit underage children.
- Internet Phishing: Phishing is the act of attempting to acquire information such as usernames, passwords, and credit card details (and sometimes, indirectly, money) by masquerading as a trustworthy entity in an electronic communication.

Classsification of cybercrimes (cont...)

- Cyber Squatting: It means where two persons claim for the same Domain Name either by claiming that they had registered the name first on by right of using it before the other or using something similar to that previously. For example, two similar names i.e.: www.google.com and www.gogle.com.
- Cyber Vandalism: Vandalism means deliberately destroying or damaging property of another. Thus, cyber vandalism means destroying or damaging the data when a network service is stopped or disrupted. It may include within its purview any kind of physical harm done to the computer of any person. These acts may take the form of the theft of a computer, some part of a computer or a peripheral attached to the computer.
- Virus: Viruses are programs that attach themselves to a computer or a file and then circulate themselves to other files and to other computers on a network. They usually affect the data on a computer, either by altering or deleting it. Worm attacks plays major role in affecting the computerize system of the individuals.

Classsification of cybercrimes (cont...)

- Cyber Terrorism: Cyber terrorism is a major burning issue in the domestic as well as global concern. The common form of these terrorist attacks on the Internet is by distributed denial of service attacks, hate websites and hate e-mails, attacks on sensitive computer networks etc. Cyber terrorism activities endanger the sovereignty and integrity of the nation.
- Distribution of pirated software: It means distributing pirated software from one computer to another
- Possession of Unauthorized Information: It is very easy to access any information by the terrorists with the aid of internet and to possess that information for political, religious, social, ideological objectives.

Impact on law enforcement:challenges

- Technical challenges that hinder law enforcement's ability to find and prosecute criminals operating online;
- Legal challenges resulting from out-of-date laws, and legal tools needed to investigate cyber-crime are lagging behind technological, structural and social changes;
- Operational challenges to ensure that law enforcement officers are well-trained and well-equipped to work together, including across national borders;
- Difficulty in identifying the perpetrators of these crimes as they frequently use false identities online and make use of anonymous re-mailer services; and,
- Difficulty in identifying the exact location of the crime. These crimes can be perpetrated from any location that has telephone service. Some examples include public Internet stations in airports, bus depots, libraries, cyber-cafés and convenience stores.

The elements of a crime

As in traditional crimes, for a cybercrime to exist FOUR (4) elements must be present:

1) actus reus (the prohibited act or failing to act when one is supposed to be under duty to do so);
2) mens rea (a culpable mental state);
3) attendant circumstances (the existence of certain necessary conditions); and
4) harm resulting to persons or property.

The elements of a crime (cont...)

Example:

- A cyberperpetrator enters the computer and unlawfully takes, or exercises unlawful control over, the property—the information of another (actus reus).
- The cyberperpetrator enters with the intent to commit an offense and acts with the intent of depriving the lawful owner of data (mens rea).
- By society's standards, the cyberperpetrator has no legal right to enter the computer system or to gain control over the software (attendant circumstances).
- The cybercriminal is, therefore, liable for his or her acts. The cyberperpetrator unlawfully entered the computer (that is, criminal trespass) to commit an offense (that is, theft) once inside, and as a result, the target is not able to access his or her data (that is, harm is done to the target).

The role of computers in crime

There are 3 roles that a computer can play in a criminal activity:

1. using computers as targets which is a crime that involves an attack on data integrity, system integrity, data confidentiality, privacy or availability. This form of crime targets a computer system to gain unauthorized access to stored data on the computer system by controlling the system.
2. making use of computers unlawfully as storage devices by using a computer or computer device as a passive storage medium to store stolen data such as password lists, credit card numbers, proprietary corporate information, pirated commercial software etc.
3. using computers as communication tools such as illegally selling prescribed drugs, guns, controlled substances, child pornography and gambling which is performed online.

Computer Crimes Act 1997

The CCA 1997 provides 4 types of offences, namely:

1) Unauthorized access to computer material;
2) Unauthorized access with intent to commit or facilitate commission of a further offence;
3) Unauthorized modification of the contents of any computer; and
4) Wrongful communication.

Computer Crimes Act 1997

- The CCA 1997 is modelled on the UK Computer Misuse Act 1990.
- Section 8 of the CCA 1997 provides that the provisions of the Act have an effect outside as well as within Malaysia, and where an offence under the Act is committed by any person in any place outside Malaysia, he may be dealt with in respect of such offence as if it was committed at any place within Malaysia.
- For this to apply, the computer, program or data must be in Malaysia or capable of being connected to or sent to or be used by or with a computer in Malaysia at the material time.

Computer Crimes Act 1997

Unauthorized access to computer material

The offence: under section 3 of the Computer Crimes Act 1997, a person shall be guilty of an offence if:

1) He causes a computer to perform any function with intent to secure access to any program or data held in any computer;
2) The access he intends to secure is unauthorized; and
3) He knows at the time when he causes the computer to perform the function that that is the case.

- A person guilty of an offence under this section shall on conviction be liable to a fine of not exceeding RM50,000 or to imprisonment for a term not exceeding five years or to both.

Computer Crimes Act 1997

Definition of securing access to program or data

- A person secures access to any program or data held in a computer if, by causing a computer to perform any function, he:
  a) Alters or erases the program or data;
  b) Copies or moves it to any storage medium other than that in which it is held or to a different location in the storage medium in which it is held;
  c) Uses it; or
  d) Causes it to be output from the computer in which it is held whether by having it displayed or in any other manner, and references to access to a program or data and to an intent to secure such access shall be construed accordingly.

Computer Crimes Act 1997

Definition of securing access to program or data

- For the purpose of para 2(c), a person uses a program if the function he causes the computer to perform:
  a) Causes the program to be executed; or
  b) Is itself a function of the program
- For the purpose of para 2(d), the form in which any program or data is output and in particular whether or not it represents a form in which, in the case of a program, it is capable of being executed or, in the case of data, it is capable of being processed by a computer is immaterial.

Computer Crimes Act 1997

Definition of securing access to program or data

- For the purpose of this Act, access of any kind by any person to any program or data held in a computer is unauthorized if:
  a) He is not himself entitled to control access of this kind in question to the program or data; and
  b) He does not have consent or exceeds any right or consent to access by him of the kind in questions to the program or data from any person who is so entitled.
- A reference to this Act to any program or data held in a computer includes a reference to any program or data held in any removable storage medium which is for the time being in the computer.

Computer Crimes Act 1997

Unauthorized access with intent to commit or facilitate commission of a further offence

The offence: under section 4 of the Computer Crimes Act 1997, a person shall be guilty of an offence if he commits an offence with the intent:

1) To commit an offence involving fraud or dishonesty or which causes injury as defined in the Penal Code; or
2) To facilitate the commission of such an offence whether by himself or by any other person

- It is immaterial whether the offence to which this section applies is to be committed at the same time when the unauthorized access is secured or on any future occasion.

Computer Crimes Act 1997

Unauthorized access with intent to commit or facilitate commission of a further offence

- A person guilty of an offence under this section shall on conviction be liable to a fine of not exceeding RM150,000 or to imprisonment for a term not exceeding ten years or to both.

Computer Crimes Act 1997

Unauthorized modification of the contents of any computer

The offence: under section 5 of the Computer Crimes Act 1997, a person shall be guilty of an offence if he does any act which he knows will cause unauthorized modification of the contents of any computer.

- For the purpose of section 5, it is immaterial that the act in question is not directed at:
  1) Any particular program or data;
  2) A program or data of any kind; or
  3) A program or data held in any particular computer.

Computer Crimes Act 1997

Unauthorized modification of the contents of any computer

- It is also immaterial whether an unauthorized modification is, or is intended to be, permanent or merely temporary.
- A person guilty of an offence under this section shall on conviction be liable to a fine not exceeding RM100,000 or to imprisonment for a term not exceeding seven years or to both; or be liable to a fine not exceeding RM150,000 or to imprisonment for a term not exceeding ten years or to both, if the act is done with the intention of causing injury as defined in the Penal Code.

Computer Crimes Act 1997

Definition of modification of the contents

- Modification of the contents of any computer takes place if, by the operation of any function of the computer concerned or any other computer:
  a) Any program or data held in the computer concerned is altered or erased;
  b) Any program or data is introduced or added to its contents; or
  c) Any events occurs which impairs the normal operation of any computer, and any act that contributes towards causing such a modification shall be regarded as causing it

Computer Crimes Act 1997

Definition of modification of the contents

- Any modification is unauthorized if:
  a) The person whose act causes it is not himself entitled to determine whether the modification should be made; and
  b) He does not have consent to the modification from any person who is so entitled.

Computer Crimes Act 1997

Wrongful communication

The offence: under section 6 of the Computer Crimes Act 1997, a person shall be guilty of an offence if he communicated directly or indirectly a number, code, password, or other means of access to a computer to any person other than a person to whom he is duly authorized to communicate.

- A person guilty of an offence under this section shall on conviction be liable to a fine not exceeding RM25,000 or to imprisonment for a term not exceeding three years or to both.

Computer Crimes Act 1997

Presumption of custody or control

- Section 8 of the CCA 1997 provides that a person who has in his custody or control any program, data or other information which is held in any computer or retrieved from any computer which he is not authorized to have in his custody or control, shall be deemed to have obtained unauthorized access to such program, data or information unless the contrary is proved.
- This section is relevant when an accused's computer is seized during an investigation. The presumption will apply if the program, data or information is found on the accused's computer.

Computer Crimes Act 1997

Presumption of custody or control

- For example, in a case where there had been unauthorized access to a computer and certain files have been downloaded by the accused, if the same files are found in the accused's computer, the presumption would apply.
- What if the information was found in a cloud server instead? For example, in the accused's email inbox which was accessed using a third party's computer. The determining factor here would be whether the information was in the custody or control of the accused. It does not need to be in the accused's own computer.

Computer Crimes Act 1997

Presumption of custody or control

- However, what if the accused merely has a hyperlink to the information? For example, a third party had compromised a computer and sent the files to the accused via a hyperlink to another online storage area. In this scenario, technically there is no information in the custody or control of the accused but merely access to the information. Thus, the presumption should not apply in this kind of scenario.

Communications and Multimedia Act 1998

Scope

- The scope of CMA 1998 covers communications over electronic media but not the print media. It also does not affect the general application of existing laws on national security, illegal content, defamation and copyright. Such laws are still applicable to all forms of content, regardless of the medium.
- The CMA 1998 establishes a framework for regulatory intervention to promote Malaysia's national policy objectives for the communications and multimedia industry.
- The activities and services regulated under the CMA 1998 include traditional broadcasting, telecommunications, and online services, including the facilities and networks used in providing such services, as well as the content which is supplied via the facilities and networks.

Communications and Multimedia Act 1998

Objectives of the Act

Section 3 of the CMA 1998 provides the objectives of the Act:

1) To promote national policy objectives for the communications and multimedia industry;
2) To establish a licensing and regulatory framework in support of national policy objectives for the communications and multimedia industry;
3) To establish the powers and functions for the Malaysian Communications and Multimedia Commission (commonly known as the MCMC or SKMM); and
4) To establish powers and procedures for the administration of the Act

Communications and Multimedia Act 1998

National policy objectives

National policy objectives are:

1) To establish Malaysia as a major global centre and hub for communications and multimedia information and content services;
2) To promote a civil society where information-based services will provide the basis of continuing enhancement to the quality of work and life;
3) To grow and nurture local information resources and cultural representation that facilitate the national identity and global diversity;
4) To regulate for the long-term benefit of the end-user;
5) To promote a high level of consumer confidence in service delivery from the industry;
6) To ensure an equitable provision of affordable services over ubiquitous national infrastructure;

Communications and Multimedia Act 1998

National policy objectives

National policy objectives are:

7) To create a robust applications environment for end-users;
8) To facilitate the efficient allocation of resources such as skilled labor, capital, knowledge and national assets;
9) To promote the development of capabilities and skills within Malaysia's convergence industries, and
10) To ensure information security and network reliability and integrity.

Communications and Multimedia Act 1998

Regulations of content published over a network: sections 211 and 233

Section 211 deals with offensive content and provides:

211. Prohibition on provision of offensive content

1) No content applications provider, or other person using a content applications service, shall provide content which is indecent, obscene, false, menacing, or offensive in character with intent to annoy, abuse, threaten or harass any person
2) A person who contravenes subsection (1) commits an offence and shall, on conviction, be liable to a fine not exceeding RM50,000 or to imprisonment for a term not exceeding one year or to both and shall also be liable to a further fine of RM1,000 for every day or part of a day during which the offence is continued after conviction.

Communications and Multimedia Act 1998

Regulations of content published over a network: sections 211 and 233

Section 233 covers improper use of network facilities or services and provides:

233. improper use of network facilities or network services, etc.

1) A person who –

a) By means of any network facilities or network service or applications service knowingly –

i. Makes, creates, or solicits; and

ii. Initiates the transmission of, any comment, request, suggestion or other communication which is obscene, indecent, false, menacing, or offensive in character with intent to annoy, abuse, threaten or harass another person; or

b) Initiates communication using any applications service, whether continuously, repeatedly, or otherwise, during which communication may or may not ensue, with or without disclosing his identity and with intent to annoy, abuse, threaten, or harass any person at any number or electronic address, commits an offence.

Communications and Multimedia Act 1998

Regulations of content published over a network: sections 211 and 233

Section 233 covers improper use of network facilities or services and provides:

233. improper use of network facilities or network services, etc.

2) A person who knowingly –

a) By means of a network service or applications service provides any obscene communication for commercial purposes to any person; or

b) Permits a network service or applications service under a person's control to be used for an activity described in para a), commits an offence.

3) A person who commits an offence under this section shall, on conviction, be liable to a fine not exceeding RM50,000 or to imprisonment for a term not exceeding one year or to both and shall also be liable to a further fine of RM1,000 for every day during which the offence is continued after conviction.

Communications and Multimedia Act 1998

Regulations of content published over a network: sections 211 and 233

- Section 211 applies to a content service provider or a person who uses the content application service. Section 233, on the other hand, applied to any person who uses network facilities or a network service or applications service.
- Section 233 (1)(a) is commonly used to prosecute those who misuse the Internet. It basically makes it an offence for a person to provide electronic content which is obscene, indecent, false, menacing, or offensive in character with intent to annoy, abuse, threaten, or harass another person.
- There must be an "intent to" annoy, abuse, threaten or harass another person.

Penal Code

- In cases where computer-/internet-related crime activities are involved, but do not specifically fall within the ambit of any of the aforementioned statutes (for example, online fraud, cheating, criminal defamation, intimidation, gambling, pornography, etc.), such offences may be charged under the Penal Code, which is the main statute that deals with a wide range of criminal offences and procedures in Malaysia.

Example Cases

Unauthorized access: Section 3, CCA 1997

- In PP v Vishnu Devarajan [2016] 1 LNS 1066, the accused was charged under section 3 of the CCA for accessing, without authorization, the servers of a broadcast centre and the server database of a Malaysian radio network company. However, all charges were dropped due to technical and procedural errors in the prosecution of the case.

Example Cases

Unauthorized access: Section 4, CCA 1997

- In Basheer Ahmad Maula Sahul Hameed v PP [2016] 6 CLJ 422, the two accused persons, who were husband and wife, where the wife worked in a bank, were convicted under section 4(1) of the CCA for using a debit card belonging to an airplane accident victim to withdraw cash from an ATM machine and for transferring money from several other victims' online banking accounts without authorization.

Example Cases

Denial of service attacks: Section 233(1)(b), CMA 1998

- There is no specific provision which provides for denial-of-service attacks. However, under section 233(1)(b) of the Communications and Multimedia Act 1998 ("CMA"), a person who continuously, repeatedly or otherwise initiates a communication using any applications services with the intent to annoy, abuse, threaten or harass any person at any number or electronic address commits an offence, regardless of whether the communication ensued and whether or not the person initiating such communication disclosed their identity.
- To date, there have been no reported cases under section 233(1)(b) of the CMA which specifically relate to denial-of-service attacks.

Example Cases

Phishing: Section 416, Penal Code

- There are no specific offences regarding phishing. However, other statutory provisions may be applicable in tackling phishing offences. Under section 416 of the Malaysian Penal Code, any person is said to "cheat by personation", if he cheats by pretending to be some other person, or by knowingly substituting one person for another, or representing that he or any other person is a person other than he or such other person really is. The offence of cheating by personation is punishable with imprisonment for a term which may extend to seven years and/or a fine.
- To date, there are no reported cases specifically in relation to phishing.

Example Cases

Infection of IT systems with malware (incl ransomware, spyware, worms trojans, and viruses): Section 5, CCA 1997

- In PP v Roslan and Anor [2016] 1 LNS 651, the accused who worked as a Systems Analyst in the IT Department of the Malaysian Hajj Pilgrims Fund Board, was convicted under section 5(1) of the CCA for modifying pilgrims' records in the organisation's database without authorization.
- In PP v Vishnu Devarajan [2016] 1 LNS 1066, the accused was charged under section 5 of the CCA for, amongst others, carrying out the following without authorization: downloading and launching software; running and stopping certain processes on servers; and running certain programs on the database server of a broadcast centre. However, all charges were dropped due to technical and procedural errors in the prosecution of the case.

Example Cases

Infection of IT systems with malware (incl ransomware, spyware, worms trojans, and viruses): Section 5, CCA 1997

- In Kangaie Agilan Jammany v PP [2017] 1 LNS 1640, the accused, an employee of AirAsia, a low-cost airline carrier company, was charged under section 5 of the CCA where he used the Air Asia reservation system without authorization to modify passenger flight schedules, in order to help family members and friends obtain airline tickets at lower rates.

Example Cases

Possession or use of hardware, software or other tools used to commit cybercrime: Section 236 & 240, CMA 1998

- Under section 236 of the CMA, it is an offence for a person to possess or use any counterfeit access devices, unauthorized access devices (e.g. lost, stolen, expired, or obtained with the intention to defraud), any device-making equipment intended to make counterfeit access devices, or any other equipment or device modified or altered or intended to alter or modify such other equipment or device in order to obtain unauthorized access to any network services, etc.
- Possession or use of the above is an offence and the offender would be liable to a fine not exceeding RM500,000 or to imprisonment not exceeding five years, or both.

Example Cases

Possession or use of hardware, software or other tools used to commit cybercrime: Section 236 & 240, CMA 1998

- Under section 240 of the CMA, it is an offence to distribute or advertise any communications equipment or device for interception of communication. An offence under this section would render the offender liable to a fine not exceeding RM100,000 or to imprisonment not exceeding two years, or both.
- To date, there have been no reported cases either under section 236 or section 240 of the CMA.

Example Cases

Identity theft or identity fraud: Section 416, Penal Code

- The Penal Code contains provisions on cheating by personation. Although not cyber-specific, section 416 of the Penal Code may apply to identity theft. Under section 416 of the Penal Code, it is an offence to "cheat by personation", i.e. where a person cheats by pretending to be some other person, or by knowingly substituting one person for another, or representing that he or any other person is a person other than he or such person really is.
- To date, while there has been news of individuals committing identity theft or fraud, such cases have, however, usually been tried on the basis of contravening national registration regulations (in relation to impersonating or theft of identification cards). There have been no reported cases for actions on identity theft or identity fraud specifically in the context of cybersecurity or cybercrimes.

Example Cases

Any other activity that adversely affects or threatens the security, CIA of any IT systems, infra, comm network, device or data: CMA 1998

- Activities which adversely affect or threaten security, confidentiality, integrity or availability of IT systems, infrastructures, etc. are prohibited or regulated under the CMA.
- For example, it is an offence to: use any apparatus or device with the intent to obtain information regarding the contents, sender or addressee of any communication without an approval by a registered certifying agency (section 231 of the CMA); possess or create a system designed to fraudulently use or obtain any network facilities, network service, applications service or content applications service (section 232(2) of the CMA); intercept, attempt to intercept, or procure any other person to intercept or attempt to intercept, any communications (section 234 of the CMA); and extend, tamper with, adjust, alter, remove, destroy or damage any network facilities or any part thereof (section 235 of the CMA).
- A person who is found liable for any of the above offences under CMA may, upon conviction, be held liable to a maximum fine ranging from RM50,000 to RM300,000 or imprisonment not exceeding two to three years, or both.
- To date, there have been no reported cases prosecuted under any of the abovementioned provisions of the CMA

Thank You

MyUTeM

www.utem.edu.my