Digital Crime and Legal Background of Information Security

IT5306 Principles of Information Security

Level III - Semester 5

List of sub topics

1.1 Cybercrime and Computer Crime
1.2 Intellectual Property
1.3 Privacy
1.4 Sri Lanka Computer Crimes Act
1.5 Sri Lanka Electronic Transactions Act

1.1 Cybercrime and Computer Crime

- Computer crime, or cybercrime, is a term used broadly to describe criminal activity in which computers or computer networks are a tool, a target, or a place of criminal activity.
- The term cybercrime connotes the use of computers connected by networks specifically, whereas computer crime may or may not involve networks.
- The U.S. Department of Justice categorizes computer crime based on the role that the computer plays in the criminal activity:
    - Computers as targets
    - Computers as storage devices
    - Computers as communications tools

1.1 Cybercrime and Computer Crime (cont.)

- A more specific list of crimes defined in the international Convention on Cybercrime would include:
    - Illegal access to computers
    - Illegal interception of data in transit or on storage including denial of access to data
    - Data interference
    - System interference
    - Misuse of devices
    - Computer-related forgery
    - Computer-related fraud
    - Offenses related to child pornography
    - Infringements of copyright and related rights
    - Attempt and aiding or abetting in the misuse of computers

1.1 Cybercrime and Computer Crime (cont.)

- For law enforcement agencies, cybercrime presents some unique difficulties.
- Proper investigation requires a fairly sophisticated grasp of the technology.
- Many jurisdictions lack investigators knowledgeable and experienced in dealing with this kind of crime.
- The nature of cybercrime is such that consistent success in criminal arrest and prosecution is extraordinarily difficult.
- The global nature of cybercrime is an additional obstacle: Many crimes will involve perpetrators who are remote from the target system, in another jurisdiction or even another country.

1.2 Intellectual Property

- There are three types of tangible and intangible properties:
  - **Real property:** Land and things permanently attached to the land, such as trees, buildings, and stationary mobile homes.
  - **Personal property:** Personal effects, moveable property and goods, such as cars, bank accounts, wages, securities, a small business, furniture, insurance policies, jewelry, patents, pets, and season baseball tickets.
  - **Intellectual property:** Any intangible asset that consists of human knowledge and ideas. Examples include software, data, novels, sound recordings, the design of a new type of mousetrap, or a cure for a disease.

1.2 Intellectual Property (cont.)

- There are three main types of intellectual property for which legal protection is available:
  - copyrights
  - trademarks
  - patents

- The legal protection is against **infringement**, which is the invasion of the rights secured by copyrights, trademarks, and patents.

- The right to seek civil recourse against anyone infringing his or her property is granted to the IP owner.

  - copyrights: unauthorized use
  - trademarks: unauthorized use or colorable imitation
  - patents: unauthorized making, using, or selling

1.2 Intellectual Property (cont.)

- Copyright law protects the tangible or fixed expression of an idea, not the idea itself.
- A creator can claim copyright, and file for the copyright at a national government copyright office, if the following conditions are fulfilled:
    - The proposed work is original.
    - The creator has put this original idea into a concrete form, such as hard copy (paper), software, or multimedia form.

1.2 Intellectual Property (cont.)

- The copyright owner has the following exclusive rights, protected against infringement:
  - Reproduction right: Lets the owner make copies of a work
  - Modification right: Also known as the derivative-works right; concerns modifying a work to create a new or derivative work
  - Distribution right: Lets the owner publicly sell, rent, lease, or lend copies of the work
  - Public-performance right: Applies mainly to live performances
  - Public-display right: Lets the owner publicly show a copy of the work directly or by means of a film, slide, or television image

1.2 Intellectual Property (cont.)

- A patent for an invention is the grant of a property right to the inventor.
- Different countries have their own implementation of patent laws.
- There are three types of patents:
- **Utility patents**: Granted to anyone who invents or discovers any new and useful process, machine, article of manufacture, or composition of matter, or any new and useful improvement.
- **Design patents**: Granted to anyone who invents a new, original, and ornamental design for an article of manufacture.
- **Plant patents**: Granted to anyone who invents or discovers and asexually reproduces any distinct and new variety of plant.

1.2 Intellectual Property (cont.)

- Intellectual property that are relevant to computers:
- **Software:** Includes programs produced by vendors of commercial software as well as shareware, proprietary software created by an organization for internal use, and software produced by individuals.
- **Databases:** A database may consist of data that is collected and organized in such a fashion that it has potential commercial value.
- **Digital content:** Includes audio files, video files, multimedia, courseware, website content, and any other original digital work that can be presented in some fashion using computers or other digital devices.
- **Algorithms:** An example of a patentable algorithm is the RSA public-key cryptosystem.

1.2 Intellectual Property (cont.)

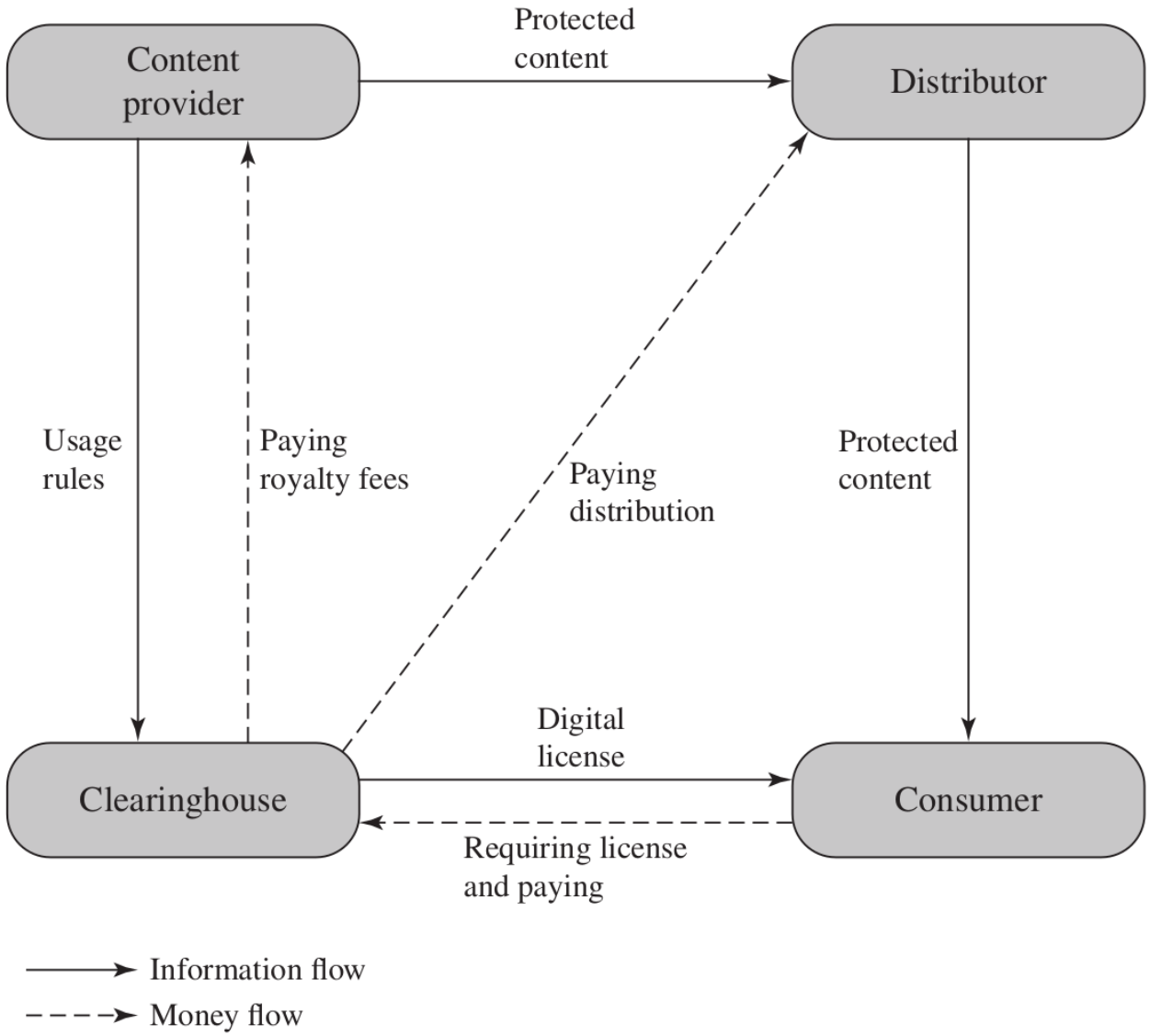
- Digital Rights Management (DRM) refers to systems and procedures that ensure that holders of digital rights are clearly identified and receive the stipulated payment for their works.

- There is no single DRM standard or architecture; DRM encompasses a variety of approaches to intellectual property management and enforcement by providing secure and trusted automated services to control the distribution and use of content.

- Users in a typical DRM model (see figure next slide):

    - Content provider
    - Distributor
    - Consumer
    - Clearinghouse

1.2 Intellectual Property (cont.)



1.3 Privacy

- In a global information economy, it is likely that the most economically valuable electronic asset is “aggregated information” on individuals.
- Individuals have become increasingly aware of the extent to which government agencies, businesses, and even Internet users have access to their personal information and private details about their lives and activities.
- Concerns about the extent to which personal privacy has been and may be compromised have led to a variety of legal and technical approaches to reinforcing privacy rights.
- A number of international organizations and national governments have introduced laws and regulations intended to protect individual privacy.

1.3 Privacy (cont.)

- Privacy can be broken down into four major areas:
- **Anonymity:** Ensures that a user may use a resource or service without disclosing the user's identity.
- **Pseudonymity:** Ensures that a user may use a resource or service without disclosing its user identity, but can still be accountable for that use.
- **Unlinkability:** Ensures that a user may make multiple uses of resources or services without others being able to link these uses together.
- **Unobservability:** Ensures that a user may use a resource or service without others, especially third parties, being able to observe that the resource or service is being used.

1.4 Sri Lanka Computer Crimes Act

- Computer Crimes Act, No.24 of 2007 covers the computer-related crimes and their legal consequences in Sri Lanka.
- It identifies several actions committed by people, or organisations as punishable offenses in accordance with the provisions of the Code of Criminal Procedure Act, No. 15 of 1979.
- The law is applicable irrespective of whether the considered crime is conducted in Sri Lanka or outside Sri Lanka.

1.4 Sri Lanka Computer Crimes Act (cont.)

- Some of the types of computer crimes identified by the act:
  - Securing unauthorised access to a computer
  - Doing any act to secure unauthorised access in order to commit an offence
  - Causing a computer to perform a function without lawful authority
  - Offences committed against national security
  - Dealing with data that are unlawfully obtained
  - Illegal interception of data
  - Use of illegal devices
  - Unauthorised disclosure of information enabling access to a service

1.4 Sri Lanka Computer Crimes Act (cont.)

- In order to facilitate investigations on computer crimes, experts can be appointed to assist police officers.

- Such experts are basically appointed from universities that are established through the Universities Act, No. 16 of 1978.

- Once appointed, such experts can:
  - enter upon any premises along with a police officer not below the rank of a sub-inspector
  - access any information system, computer or computer system or any programme, data or information held in such computer to perform any function or to do any such other thing
  - require any person to disclose any traffic data
  - orally examine any person
  - do such other things as may be reasonably required

1.4 Sri Lanka Computer Crimes Act (cont.)

- Any person who is required to make any disclosure or to assist in an investigation under this Act, shall comply with such requirement.

- A person who obstructs the lawful exercise of the powers conferred on an expert or a police officer or fails to comply with such request made by such expert or police officer during an investigation shall be guilty of an offence and shall on conviction be liable to a fine or imprisonment.

- For example, when a computer system is locked through a login, or certain data are encrypted, the owner of the device/data are obliged to surrender the password/cryptographic key to the investigators.

1.5 Sri Lanka Electronic Transactions Act

- The Electronic Transactions Act, No. 19 of 2006 is concerned with
  - facilitating domestic and international electronic commerce by eliminating legal barriers and establishing legal certainty
  - encouraging the use of reliable forms of electronic commerce
  - facilitating electronic filing of documents with Government and to promote efficient delivery of Government services by means of reliable forms of electronic communications
  - promoting public confidence in the authenticity, integrity and reliability of data messages, electronic documents, electronic records or other communications