Professional Practices
HU-511(BSCS), HU-601(BSIT)

Dr. Arbab Waseem Abbas

ICS/IT, FMCS, The University of Agriculture, Peshawar.

Lecture 4(week 9 & 10)

Lecture # 4

Computer Misuse and The Criminal Law,
&
Anonymity, security, privacy, and civil liberties

Contents

- Introduction
- Types of Computer misuse
- How to prevent Computer misuse
- Computer misuse and Criminal law
- Real world Cases of Computer Misuse

Introduction

- Businesses, government and academic institutions are increasingly reliant on the Internet for their day-to-day business, while consumers are using e-commerce more and more for purchasing goods and services.
- All these modern business processes are utilizing computer software and hardware.
- With increased use of computers, there has been a sharp rise in the number of crimes involving computing; and the internet has undoubted create new security risks

Types of Computer Misuse

- Computer misuse involves the use of computer and network in attacking computers and networks as well.
- One of the earliest and the most common types of cybercrime activity is hacking.
- It roughly started in the 1960s.
- It involves stealing identities and important information, violating privacy, and committing fraud, among others.

Types of Computer Misuse

- Some of the most common types of computer misuse are
- **Fraud:** Fraud is a general term used to describe a cybercrime that intends to deceive a person in order to gain important data or information. Fraud can be done by altering, destroying, stealing, or suppressing any information to secure unlawful or unfair gain.

Types of Computer Misuse

- **Hacking:** Hacking involves the partial or complete acquisition of certain functions within a system, network, or website. It also aims to access to important data and information, breaching privacy. Most "hackers" attack corporate and government accounts.

Types of Computer Misuse

- **Identity Theft:** Identify theft is a specific form of fraud in which cybercriminals steal personal data, including passwords, data about the bank account, credit cards, debit cards, social security, and other sensitive information. Through identity theft, criminals can steal money. According to the U.S. Bureau of Justice Statistics (BJS), more than 1.1 million Americans are victimized by identity theft.

Types of Computer Misuse

- **Scamming:** Scam happens in a variety of forms. In cyberspace, scamming can be done by offering computer repair, network troubleshooting, and IT support services, forcing users to shell out hundreds of money for cyber problems that do not even exist. Any illegal plans to make money falls to scamming.
- **Computer Viruses:** Most criminals take advantage of viruses to gain unauthorized access to systems and steal important data. Mostly, highly-skilled programs send viruses, malware, and Trojan, among others to infect and destroy computers, networks, and systems. Viruses can spread through removable devices and the internet.

Types of Computer Misuse

- **Ransomware:** Ransom ware is one of the most destructive malware-based attacks. It enters your computer network and encrypts files and information through public-key encryption. In 2016, over 638 million computer networks are affected by ransom ware. In 2017, over $5 billion is lost due to global ransom ware.

Types of Computer Misuse

- **DDoS Attack:** DDoS or the Distributed Denial of Service attack is one of the most popular methods of hacking. It temporarily or completely interrupts servers and networks that are successfully running. When the system is offline, they compromise certain functions to make the website unavailable for users. The main goal is for users to pay attention to the DDoS attack, giving hackers the chance to hack the system
- The main difference between the two is that while a DoS attack hinders the targeted system using one device, DDoS attacks are conducted through multiple devices operating on different networks that usually form a botnet.
- The term botnet is a hybrid, from the words robot and network and each infected device is called a bot.
- A botnet is a group of Internet-connected devices, which have been infected by malware, have come under the control of a malicious actor and runs one or more bots. Botnets can be used to perform Distributed Denial-of-Service attacks, steal data, send spam, and allow the attacker to access the device and its connection. The owner can control the botnet using command and control software

Types of Computer Misuse

- **Phishing:** Phishers act like a legitimate company or organization. They use “email spoofing” to extract confidential information such as credit card numbers, social security number, passwords, etc. They send out thousands of phishing emails carrying links to fake websites. Users will believe these are legitimate, thus entering their personal information.

Types of Computer Misuse

- **Malvertising:** Malvertising is the method of filling websites with advertisements carrying malicious codes. Users will click these advertisements, thinking they are legitimate. Once they click these ads, they will be redirected to fake websites or a file carrying viruses and malware will automatically be downloaded.

Types of Computer Misuse

- **Cyberstalking:** Cyberstalking involves following a person online anonymously. The stalker will virtually follow the victim, including his or her activities. Most of the victims of cyberstalking are women and children being followed by men.

Types of Computer Misuse

- **Software Piracy:** The internet is filled with torrents and other programs that illegally duplicate original content, including songs, books, movies, albums, and software. This is a crime as it translates to copyright infringement. Due to software piracy, companies and developers encounter huge cut down in their income because their products are illegally reproduced.

How to Prevent Computer Misuse???

- The most popular ways to prevent computer misuse are
- **Keep your software updated**
  - This is a critical requirement for any computer system and application. Always keep your OS system, services and applications updated to have the latest bugs and vulnerabilities patched.
  - This advice applies to smart phones, tablets, local desktop computers, notebooks, online servers and all applications they run internally.

How to Prevent Computer Misuse???

- **Enable your system firewall**
  - Most operating systems include a full pre-configured firewall to protect against malicious packets from both the inside and the outside. A system firewall will act as the first digital barrier whenever someone tries to send a bad packet to any of your open ports.

<u>How to Prevent Computer Misuse???</u>

- **Use different/strong passwords**
  - Never use the same password on more than one website, and always make sure it combines letters, special characters and numbers.
  - The best way to sort this out is to use a password manager like 1Password, LastPass or Keepass, which will help you generate strong passwords for each website, and at the same time store them in an encrypted database.

How to Prevent Computer Misuse???

- **Use antivirus and anti-malware software**
  - This is an excellent measure for both desktop and corporate users. Keeping antivirus and anti-malware software up to date and running scans over local storage data is always recommended.
  - While free antivirus/antimalware solutions can be helpful they are often merely trial software, and don’t offer full protection against most common virus/malware and other network threats.

How to Prevent Computer Misuse???

- **Activate your email's anti-spam blocking feature**
  - A lot of computer hacking takes place whenever you open an unsolicited email containing suspicious links or attachments.
  - First enable the anti-spam feature of your email client; and second (and most important) never open links or attachments from unsolicited recipients. This will keep you safe from phishing attacks and unwanted infections.

How to Prevent Computer Misuse???

- **Shop only from secure and well-known websites**
  - To prevent you from being a victim of man-in-the-middle attacks and crimes against your credit cards or online wallets, first make sure that the site you’re shopping on is encrypted with HTTPS.
  - Also make sure you’re shopping on a well-known site, such as Amazon, Ebay, Walmart, etc.

Computer Misuse and Criminal Law

- The Computer Misuse Act 1990 (CMA) is an act of the UK Parliament passed in 1990.
- CMA is designed to frame legislation and controls over computer crime and Internet fraud.
- The legislation was created to
  - Criminalize unauthorized access to computer systems.
  - Deter serious criminals from using a computer in the commission of a criminal offence or seek to hinder or impair access to data stored in a computer

Computer Misuse and Criminal Law

- CMA introduced three criminal offences
  - Accessing computer material without permission, e.g. looking at someone else's files.
  - Accessing computer material without permission with intent to commit further criminal offences, e.g. hacking into the bank's computer and wanting to increase the amount in your account.
  - Altering computer data without permission, e.g. writing a virus to destroy someone else's data, or actually changing the money in an account.

Computer Misuse and Criminal Law

- These offences are punishable as follows
  - Offence 1. Up to 6 months' prison and up to £5,000 in fines.
  - Offences 2 and 3. Up to 5 years in prison and any size of fine (there is no limit).

Real World Cases of Computer Misuse

WannaCry virus hits the NHS, 2017

- The most widespread cyber attack ever, hackers managed to gain access to the NHS' computer system in mid-2017, causes chaos among the UK's medical system.
- The same hacking tools were used to attack world-wide freight company FedEx and infected computers in 150 countries.
- Ransomware affectionately named "WannaCry" was delivered via email in the form of an attachment.
- Once a user clicked on the attachment, the virus was spread through their computer, locking up all of their files and demanding money before they could be accessed again.
- As many as 300,000 computers were infected with the virus.
- It was only stopped when a 22-year-old security researcher from Devon managed to find the kill switch, after the NHS had been down for a number of days.

Hackers steal £650 million from global banks, 2015

- For a period of two years, ending in early 2015, a group of Russian-based hackers managed to gain access to secure information from more than 100 institutions around the world.
- The cyber criminals used malware to infiltrate banks' computer systems and gather personal data
- They were then able to impersonate online bank staff to authorise fraudulent transfers, and even order ATM machines to dispense cash without a bank card.
- It was estimated that around £650 million was stolen from the financial institutions in total.

One billion user accounts stolen from Yahoo, 2013

- In one of the largest cases of data theft in history, Yahoo had information from more than one billion user accounts stolen in 2013.
- Personal information including names, phone numbers, passwords and email addresses were taken from the internet giant.
- Yahoo claimed at the time that no bank details were taken.
- Releasing information of the breach in 2016, it was the second time Yahoo had been targeted by hackers, after the accounts of nearly 500 million users were accessed in 2014.

ANONYMITY, SECURITY, PRIVACY, AND CIVIL LIBERTIES

Outline

- Anonymity
- Security
- Privacy
- Ethical and legal framework for information

Introduction

- Dramatical increase of information due to social, economical, and technological advances
- New challenges due to increased demand and easy access to information
- Information is a treasure in itself
- Information can be a liability
  - We constantly need the methods to acquire, keep, and dispose of the information
- We need anonymity, security, privacy, and the safeguard of our civil liberties
- Main contributing factors
  - High digitalization of information and increasing bandwidth
  - Declining costs of digital communication
  - Increased miniaturization of mobile computing devices and other communications equipment
  - Greater public awareness by the news media of the potential abuse of digital communication

Anonymity

- The state of being nameless
- How will be the life with total anonymity?
- Types of anonymity
  - Pseudo identity
    - Individual is identified by a certain pseudonym, code, or number
  - Untraceable identity
    - One is not known by any name
  - Anonymity with a pseudo address to receive and send correspondence with others
- Anonymity and the Internet
  - Internet has created a fertile ground for all faceless people to come out in the open
  - Anonymous servers
    - Full anonymity servers: no identifying information is forwarded in packet headers
    - Pseudonymous servers: put pseudonym in forwarded packet headers, keeping the real identity behind a pseudonym
  - Anonymous users

Advantages and Disadvantages of Anonymity

- Advantages
  - Good for whistle-blowers
  - Good in case of national security
  - When there is intimidation(fear) and fear of reprisals(punishment)
  - Good for some relationships and the security of some people
- Disadvantages
  - Criminals and embezzlers can use it to their advantage, especially in online social networks
  - Lots of disputes could be solved if information from individuals party to these disputes can reveal the necessary information
- Legal view of anonymity
  - In the current environment of the Internet, there are serious debates on the freedoms of individuals on the Internet and how these freedoms can be protected in the onslaught of people under the anonymity in cyberspace.

Security

- To prevent unauthorized access, use, alteration, and theft or physical damage to property
- Confidentiality
  - To prevent unauthorized disclosure of information to third parties
    - medical, financial, academic, and criminal records.
- Integrity
  - To prevent unauthorized modification of files and maintain the status quo(current situation). It includes system, information, and personnel integrity. The alteration of information may be caused by a desire for personal gain or a need for revenge.
- Availability
  - To prevent unauthorized withholding of information

Physical Security

- A facility is physically secure if it is surrounded by a barrier
- Physical security can be guaranteed if the following four mechanisms are in place
  - Deterrence: by creating an atmosphere intended to scare intruders
  - Prevention: by trying to stop intruders from gaining access
  - Detection: to “see” that intruder who has gained or who is trying to gain access
  - Response: to respond to the failure of the first three mechanisms
- Physical access controls
  - Physical security barriers
    - Fence made of barbed wire, brick walls, natural trees, mounted noise or vibration sensors, security lighting, close circuit television (CCTV), buried seismic sensors, or different photoelectric and microwave systems
    - Locks and keys, window breakage detectors, infrared and ultrasonic detectors, interior microwave systems, animal like dogs, and human barriers like security guards and others

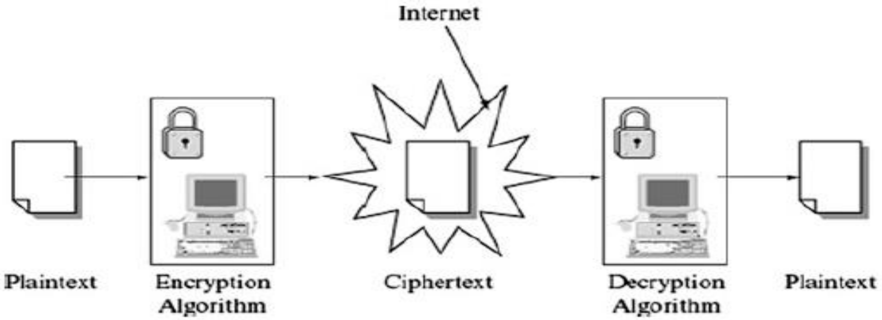
Electronic access controls

- Password
  - Never publicize a password.
  - Never write a password down anywhere.
  - Never choose a password that is easy to guess.
  - Never keep the same password for an extended period of time.
- Firewalls
  - packet filters
    - These are packet-level filters. They contain gates that allow packets to

      pass through if they satisfy a minimum set of conditions and choke or prevent those packets that do not meet the entry conditions. The minimum conditions may include to have permissible origin or destination addresses
  - proxy servers
  - stateful inspection
    - Combine both filter and proxy function

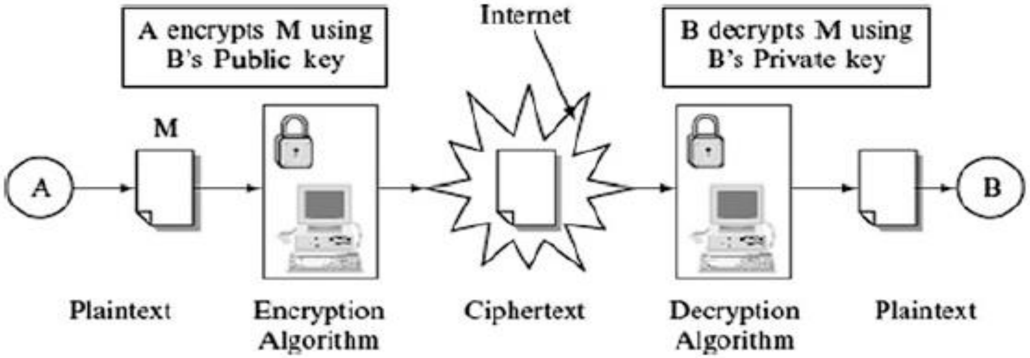
Information Security Controls

- Information security controls
  - Integrity, confidentiality, and availability of information at the servers
  - Encryption
    - Protects the communications channel from unauthorized access
      - Symmetric encryption
        - » Symmetric encryption, or secret-key encryption uses a common key and the same cryptographic algorithm to scramble and unscramble the message. The security of the transmitted data depends on the fact that eavesdroppers with no knowledge of the key are unable to read the message. One problem with symmetric encryption is the security of the keys which must be passed from the sender to the receiver.



Information Security Controls

- Asymmetric encryption
  - *Asymmetric encryption*, commonly known as public-key encryption, uses two different keys, a public key known by all and a private key known by only the sender and the receiver.
  - Both the sender and the receiver each have a pair of these keys, one public and one private.
    - » To encrypt a message, from sender A to receiver B both A and B must create their own pairs of keys.
    - » Then A and B exchange their public keys—anybody can acquire them. When A is to send a message M to B, A uses B's public key to encrypt M.
    - » On receipt of M, B then uses his or her private key to decrypt the message M.

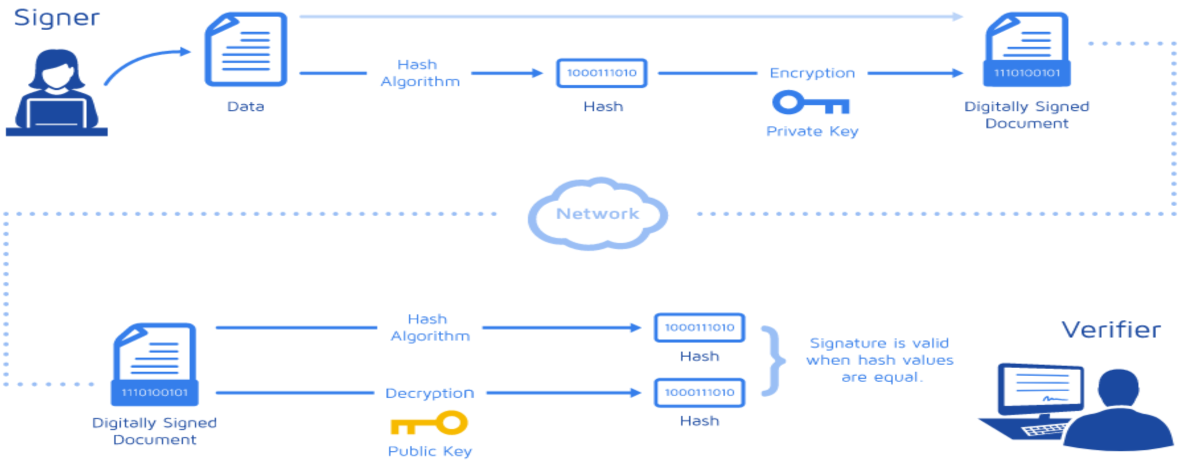


Information Security Controls

- Hash function
  - A *hash function* takes an input message *M* and creates a code from it. The code commonly is referred to as a *hash* or a *message*. A one-way hash function is used to create a digital signature of the message—just like a human fingerprint. The hash function is therefore used to provide the message's integrity and authenticity.
- Authentication
  - Authentication is a process whereby the system gathers and builds up information about the user to assure that the user is genuine. The digital signature is similar to a handwritten signature in printed documents.
  - Just like handwritten signatures, digital signatures ensure that the person whose signature the system is authenticating is indeed the right person, but digital signatures provide a greater degree of security than handwritten signatures. Also, digital signatures once submitted can never be disowned by the signer of a document claiming the signature was forged. This is called **non-repudiation**.
  - A secure digital signature system consists of two parts: (1) a method of signing a document and (2) authentication that the signature was actually generated by whoever it represents.

Information Security Controls

- The process of signing the document, that is, creating a digital signature, involves a sender **A** passing the original message **M** into a hash function **H** to produce a message digest. Then **A** encrypts **M** together with the message digest using either symmetric or asymmetric encryption, and then sends the combo to **B**.
- Upon receipt of the package, **B** separates the digital signature from the encrypted message. The message **M** is put into a one-way hash to produce a message digest, and **B** compares the output of the hash function with the message digest **A** sent. If they match, then the integrity of the message **M** and the signature of the sender are both valid



https://www.docusign.com/how-it-works/electronic-signature/digital-signature/digital-signature-faq

Information Security Controls

- Operational security
  - Operation security involves policies and guidelines that organizations including all employees must do to safeguard the assets of the organization including its workers.
  - These policy guidelines are spelt out in a document we call a security policy. It also includes guidelines for security recovery and response in case of a security incident.

Privacy

- A human value consisting of four elements (rights)
  - Solitude: the right to be alone without disturbances
  - Anonymity: the right to have no public personal identity
  - Intimacy: the right not to be monitored
  - Reserve: The right to control one’s personal information including the methods of dissemination of that information
- It depends on things like culture, geographical location, political systems, religious beliefs etc.

Types of Privacy

- Personal privacy
  - Privacy of personal attributes
  - Prevention of anyone or anything that would intrude or violate that personal space
  - Law exists to protect it
- Informational privacy
  - Protection of unauthorized access to information itself
  - Personal information
  - Financial information
  - Medical information
  - Internet
- Institutional privacy
  - Protection of organizational data

Value of Privacy

- Privacy has traditionally been perceived as valuable and has gained more importance in the information age. It has following attributes:
- Personal identity
  - When information becomes more precious, it is more important to safeguard personal identity
- Autonomy
  - The less personal information people have about an individual, the more autonomous that individual can be
  - People usually tend to establish relationships and associations with individuals and groups that will respect their personal autonomy
- Social relationships
  - Collection of information as much as possible before building the relationship
  - Sometimes people try to hide information that may lead to breakup of the relationship

Privacy Implications of Database System

- We help information seekers in gathering information from us
- The collected information is put into databases and is later sold to the highest bidder
- Information gathering is a very serious business
- Individuals, companies and governments are all competing, sometimes for the same information
- Internet crawlers are in action visiting our machines stealthy and gathering a wealth of information
- US law enforce organizations to disclose:
  - Privacy policy
  - Right to opt out
  - Safeguards

Privacy Violations

- Causes of violations
  - Consumers willingly give up information about themselves
  - Consumers lack the knowledge of how what they consider a little bit of information can turn into a big invasion of privacy
  - Inadequate privacy policies
  - Failure of companies and institutions to follow their own privacy policies
  - Internet temptation that enables businesses to reach individuals in a very short time in the privacy of their homes and offices
- Different types of violations
  - Intrusion
  - Misuse of information
  - Interception of information
  - Information matching

Privacy Protection and Civil Liberties

- The most accepted set of civil liberties are grouped into the following:
  - Criminal justice that includes police powers, personal liberty, and the right to a fair trial
  - Basic freedoms of speech, assembly, association, movement, and no discrimination
  - Freedom of information
  - Communications and privacy
- The guidelines that safeguard and protect privacy rights are classified into the following”
  - Technical
  - Contractual
  - Legal