UNIT I
INTRODUCTION

Cyber Crime

What is cyber crime?

- The former descriptions were "computer crime“, "computer-related crime" or "crime by computer". With the pervasion of digital technology, some new terms like "high-technology" or "information-age" crime were added to the definition. Also, Internet brought other new terms, like "cybercrime" and "net" crime.
- Other forms include "digital", "electronic", "virtual" ,"IT", "high-tech" and technology-enabled" crime .

History of Cyber Crime

- The first recorded cyber crime was recorded in the year 1820.
- The first spam email took place in 1978 when it was sent over the Arpanet.
- The first Virus was installed on an Apple

  Computer in 1982.

Cyber Crime Includes

Cyber crimes includes

- Illegal access
- Illegal Interception
- System Interference
- Data Interference
- Misuse of devices
- Fraud

Advantage of cyber security

- It will defend from hacks and virus.
- The application of cyber security used in our PC needs update every week.
- The security developers will update their database every week once. Hence the new virus also deleted.

Safety Tips for cyber crime

- **Safety tips …**
- Use antivirus software
- Insert firewalls , pop up blocker
- Uninstall unnecessary software
- Maintain backup
- Check security settings
- Use secure connection
- Open attachments carefully
- Use strong passwords , don’t give personal information unless required

CYBER TERRORISM

- Cyberterrorism is defined by U.S. Federal Bureau of Investigation as a premeditated attack against a computer system, computer data, programs and other information with the sole aim of violence against clandestine agents and subnational groups. The main aim behind cyberterrorism is to cause harm and destruction.

CYBER TERRORISM CATEGORIES

- Cyberterrorism can be explained as internet terrorism. With the advent of the internet, individuals and groups are misusing the anonymity to threaten individuals,certain groups, religions, ethnicities or beliefs.

Cyberterrorism can be broadly categorized under three major categories:

1. Simple: This consists of basic attacks including the hacking of an individual system.
2. Advanced: These are more sophisticated attacks and can involve hacking multiple systems and/or networks.
3. Complex: These are coordinated attacks that can have a large-scale impact and make use of sophisticated tools.

CYBER TERRORISM EXAMPLES

Examples of cyberterrorism include:

- **Glo**bal terror networks disrupting major websites to create public

•nuisances/inconveniences or to stop traffic to websites that publish content the

•hackers disagree with.

- **Int**ernational cyberterrorists accessing and disabling or modifying the signals that

•control military technology.

- **Cybe**rterrorists targeting critical infrastructure systems, for example, to disable a water treatment plant, cause a regional power outage, or disrupt a pipeline, oil refinery or fracking operation. This type of cyberattack could disrupt major cities, cause a public health crisis, endanger the public safety of millions of people as well as cause massive panic and fatalities.

CYBER TERRORISM AFFECT YOU AND YOUR FURTURE

How does Cyber Terrorism affect you and your future?

- **Air traffic** control towers or our airlines infrastructure could be hacked into.
- **Banking systems** could be violated and all of our money could be stolen.
- **Bombs** and other explosives could be set off by remote.
- **Hospitals** could lose all of their information.
- **Learn Government** secrets and plans
- **The tampering** of our water systems.

3 most common attack methods

- IP spoofing.
- Password Cracking.
- Denial-of-service attacks.

IP Spoofing

- Refers to creation of IP packets with forged source IP address with the purpose of concealing the identity of sender.
- Mostly used in Denial-of-Service attacks.
- Most effective in corporate networks where users can log in without a username or password.

Password Cracking

- **Password cracking** can be implemented using brute-force attacks, Trojan horse programs and IP spoofing.
- Password attacks usually refer to repeated attempts to identify a user account and/or password; these repeated attempts are called brute-force attacks.
- One example is weak encryption(LM hash) used by Microsoft windows XP, can easily be attacked

Denial-of-Service attacks

- **Denial-of-service attacks** focus on making a service unavailable to intended users.
- 2 forms of DoS attacks: those that crash services and those that flood services.
- One common attack method involves saturating the target machine with communications requests such that it cannot respond to the traffic.

References

https://www.digit.in/technology-guides/fasttrack-to-cyber-crime/the-12-types-of-cyber-crime.html
https://www.exabeam.com/information-security/cyber-crime/
https://blog.logsign.com/what-are-cyberterrorism-and-cyberwarfare/

Thank You