Cyber Security and Cyber Forensics (Chapter - 4 : DISSA Course) **Part 1; Introduction**

Arijit Chakraborty

Feb 19, 2022

Key points

- Indian Users :
- Data use / person
- Malware, spyware
- Cyber threat – ERM
- Rogue software

guard against IS Risks & Cyber threats

- Rapid advances in IT
- Growing access & use of computers
- Growing concern for data security
- Existence of computer fraud
- Complexity of systems and computers
- Protectors of information assets & privacy
- Black hat hacking – exponential rise
- Emergence of Data Privacy
- Detection and prevention methods
- SIEM.

Global Common Cyber Threat Outlook

- Targeted ransomware attacks becoming more common & damaging
- Attacks on specific targets -- governments & businesses.
- Surge of ransomware attacks - industrial sectors : service, manufacturing & healthcare.
- New aggressive methods to demand ransom, threatening to publish data & encrypting files.

India

- 2. **Cyber-Attacks due to COVID-19 Pandemic Induced Work Culture (India, CERT-In)**
- Attacks **targeting teleworkers** through malicious websites & emails containing malicious attachments.
- Growing risk of **corporate data leakage** from endpoint devices due to **increased teleworking.**
- Attempts to infiltrate **corporate networks** through remote network environments, such as **vulnerable VPNs**

WEF’s view

- *Cyberattacks are one of the top 10 global risks of highest concern in the next decade, with an estimated price tag of USD90 trillion if cybersecurity efforts do not keep pace with technological change.*
- *- World Economic Forum 2020*

Understanding Cyber Crime

- ***Cyber Dependent Crimes*** **=**
- digital system is the target as well as the means of attack.
- attacks on computer systems to disrupt IT infrastructure,
- stealing data over a network using malware (purpose of the data theft is usually to commit further crime).
- ***Cyber Enabled Crimes***
- ‘Existing’ crimes that have been transformed in scale or form by their use of Internet.
- Use of Internet to facilitate drug dealing, people & Arms / weapons trade/ smuggling etc

Cyber Crime

- **Computer Crime**, **E-Crime**, **Hi-Tech Crime** or **Electronic Crime**
- = where a computer is the target of a crime or is the means adopted to commit a crime.
- **Examples**
- Identity theft
- Child sexual abuse materials
- Financial theft
- Intellectual property violations
- Malware
- Malicious social engineering- Phishing
- Corporate espionage

Cyber Crime – Motivation

- Money/Greed
- Curiosity
- Revenge
- Fun
- Praise seekers
- Passtime

CYBER CRIMES

E-Mail bombing:

sending a large amount of e-mails to the victim resulting in interruption in the victims’ e-mail account or mail servers.

Data diddling:

altering raw data just before it is processed by computer and then changing it back after the processing is completed.

Salami attacks:

to make the alteration so insignificant that in a single case it would go completely unnoticed e.g. A bank employee inserts a program into bank’s servers, that deducts a small amount from the account of every customer

Denial of Service:

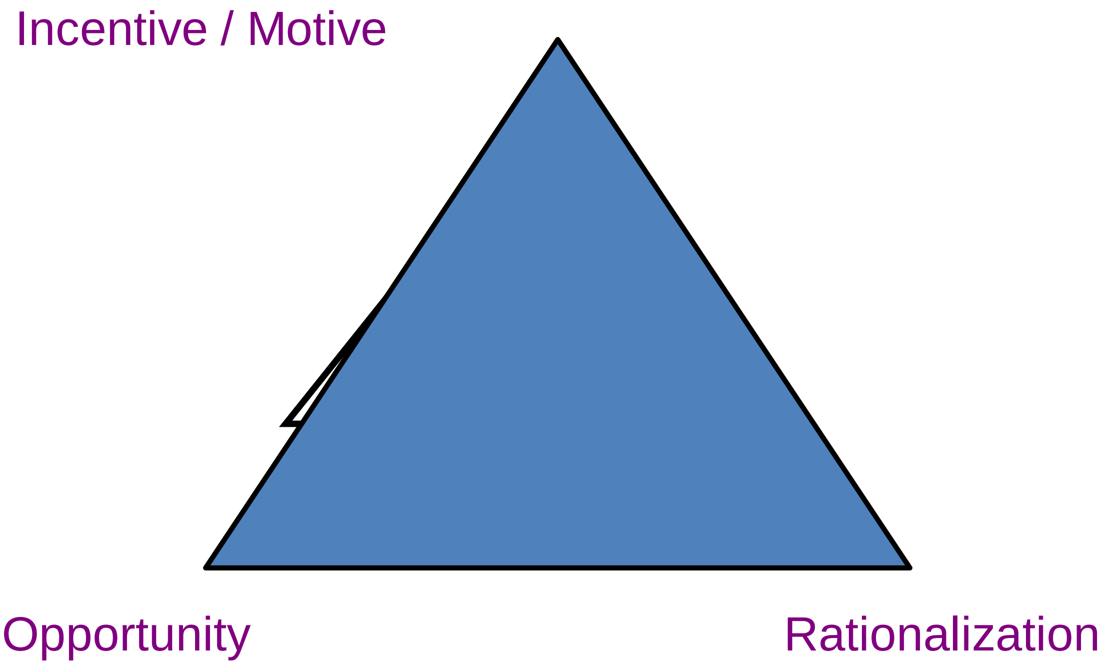
flooding computer resources with more requests than it can handle, causes resources to crash thereby denying authorized users the service offered by the resources.

CYBER CRIMES

- **Computer Based Crime-**
  - Computer used as **vehicle to commit a crime.**
  - Cyber- bullying, cyber- stalking, spamming or cyber- terrorism
- **Computer-Facilitated Crime-**
  - computer is **target of a crime.**
  - Hacking, data theft, information system is compromised.

Fraud Triangle – Psychology of Fraudster

- **Motive**
- **Rationalization**
- **Opportunity**



Hacking

- ‘Method of identifying set of vulnerabilities on target system & exploiting them systematically.
- **Ethical Hacking =** ascertains itself from hacking by adding important elements to a process - 'consent'.

1. The Process eventually **becomes a legal activity.**
2. The Ethical **Hacker seeks permission before hacking into a system** - it should be ensured hacking is **performed legally** & hacker **doesn't have any malicious intent**

Why Hacking ?

- Money extortion
- For Fun
- To Show-off
- Stealing confidential information
- To hamper privacy
- To damage System functioning
- To test security of the system