INTEGRITY
AVAILABILITY
CONFIDENTIALITY

IDENTIFY
PROTECT
DETECT
RESPOND
RECOVER

VIT®
Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

PMCA605L : Cyber Security

Module 7: Cybercrime and Cyber Terrorism - Social, Political, Ethical and Psychological Dimensions

Courtesy: Nina Godbole, Sunit Belapure & *Other Sources of Internet*

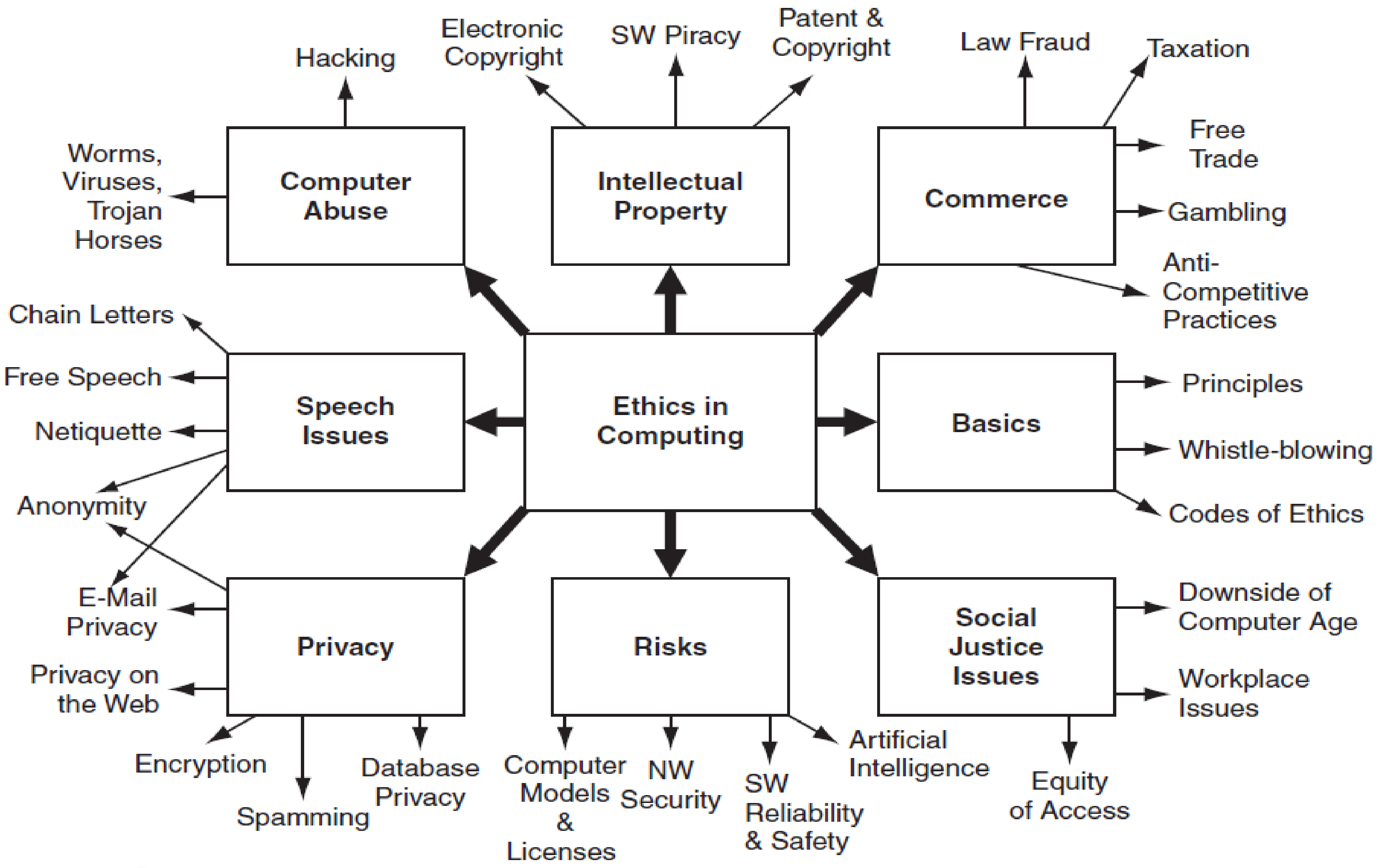
Dr. R. K. Nadesh

Ethics in Computing

- Ethics in computing refers to the moral principles and professional conduct that guide the responsible use, development, and impact.

- As computing continues to influence nearly every aspect of society, ethical considerations become essential in ensuring fairness, security, and the well-being of individuals and communities.

Ethics in Computing



VIT
Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

Dr. R. K. Nadesh

Key Ethical Principles in Computing

- Privacy and Confidentiality
- Fairness and Non-Discrimination
- Security and Cyber Ethics
- Intellectual Property and Copyright
- Responsibility of Software Developers
- Impact on Society and Employment
- Environmental Sustainability
- Misinformation and Digital Ethics

Privacy and Confidentiality

- Protecting personal and sensitive data.
- Ensuring informed consent for data collection.
- Preventing unauthorized surveillance and breaches.

Fairness and Non-Discrimination

- Avoiding bias in AI algorithms and decision-making systems.
- Ensuring equal access to technology for all individuals.
- Avoiding discrimination in hiring, credit scoring, and law enforcement AI.

Security and Cyber Ethics

- Developing secure software to prevent hacking and cybercrimes.
- Ethical hacking (penetration testing) to improve security.
- Preventing and combating malware, phishing, and identity theft.

Intellectual Property and Copyright

- Respecting software licenses, patents, and copyrights.

- Avoiding software piracy and plagiarism.

- Encouraging open-source contributions while ensuring fair use.

Responsibility of Software Developers

- Writing reliable and ethical code.
- Avoiding deceptive or harmful software practices.
- Following professional codes of conduct (e.g., ACM, IEEE ethics guidelines).

Impact on Society and Employment

- Addressing job displacement due to automation and AI.

- Ensuring fair labor practices in the tech industry.

- Developing technology that enhances rather than harms human well-being.

Environmental Sustainability

- Reducing the carbon footprint of data centers and computing infrastructure.
- Encouraging energy-efficient algorithms and hardware.
- Promoting responsible e-waste disposal and recycling.

Misinformation and Digital Ethics

- Preventing the spread of fake news and deepfakes.
- Ethical moderation of social media content.
- Encouraging responsible AI-driven content generation.

Intellectual property (IP) in cyberspace

- Intellectual property (IP) in cyberspace refers to the legal rights that protect creations of the mind.

- Given the borderless nature of the internet, protecting and enforcing IP rights in cyberspace presents unique challenges.

Types of Intellectual Property in Cyberspace

- Copyright – Protects original works such as software, e-books, articles, music, videos, and websites.

- Trademarks – Protects brand names, logos, and slogans used online.

- Patents – Protect new inventions and technological innovations, including software and digital processes.

- Trade Secrets – Protects confidential business information, such as algorithms, formulas, and databases.

- Trade Name

- Domain Name

Copyright

“Copyright” – The creator holds the rights to reproduce, distribute, or adapt the work. ©

Legal framework that protects original works, including software, digital content, and creative materials, from unauthorized use.

It ensures that creators retain control over their intellectual property (IP) and receive credit and compensation for their work.

(https://copyright.gov.in)

Patent

- A **patent** is a legal right granted to an inventor, giving them exclusive ownership over an invention for a certain period.

Software-based Innovations – Unique algorithms

Hardware Innovations – New processors, chips, or electronic devices.

Cybersecurity Techniques – New encryption or authentication methods.

Internet & Networking Technologies – Novel data transmission methods

Utility Patents – Protects new processes, machines, or software innovations.
Design Patents – Covers the visual design of a product (e.g., unique UI layouts)

Trademark

- A **trademark** is a **symbol, word, phrase, logo, or design** that distinguishes the products or services of a company from others.

- ® Registered Trademark – legal registration of a brand or product name

- ™ Trademark – indicates a brand, even if not officially registered

Major Emerging Threats to IP in Cyberspace & E-Commerce

Digital Piracy & Unauthorized Reproduction

- **Threat**: Copying and distributing digital content (e-books, music, movies, software) without authorization.

Counterfeiting & Brand Imitation

- **Threat**: Fake products are sold online using stolen brand names and logos.

Major Emerging Threats to IP in Cyberspace & E-Commerce

Cyber Espionage & Trade Secret Theft

- **Threat**: Hackers infiltrate company networks to steal confidential data (product designs, formulas).

Domain Squatting & Cybersquatting

- **Threat**: Cybercriminals register domains with names similar to well-known brands to mislead users.

Major Emerging Threats to IP in Cyberspace & E-Commerce

AI-Generated IP Theft & Plagiarism

- **Threat**: AI can generate fake art, music, and articles, raising **copyright concerns**.

Fake Reviews & Reputation Manipulation

- **Threat**: Competitors use bots to flood e-commerce platforms with **fake positive or negative reviews**.

Reverse Engineering & Software Cracks

- **Threat**: Hackers analyze software code to create **free cracked versions** or exploit security weaknesses.

Network Hacking

- **Network hacking** refers to unauthorized access, manipulation, or disruption of a computer network.
- It can be used for malicious purposes (like stealing data) or ethical purposes (like security testing).
- Hacking without permission is illegal under cybercrime laws (like the IT Act, 2000 in India or the Computer Fraud and Abuse Act in the U.S.).
- Ethical hacking is legal only with prior authorization

Email spoofing

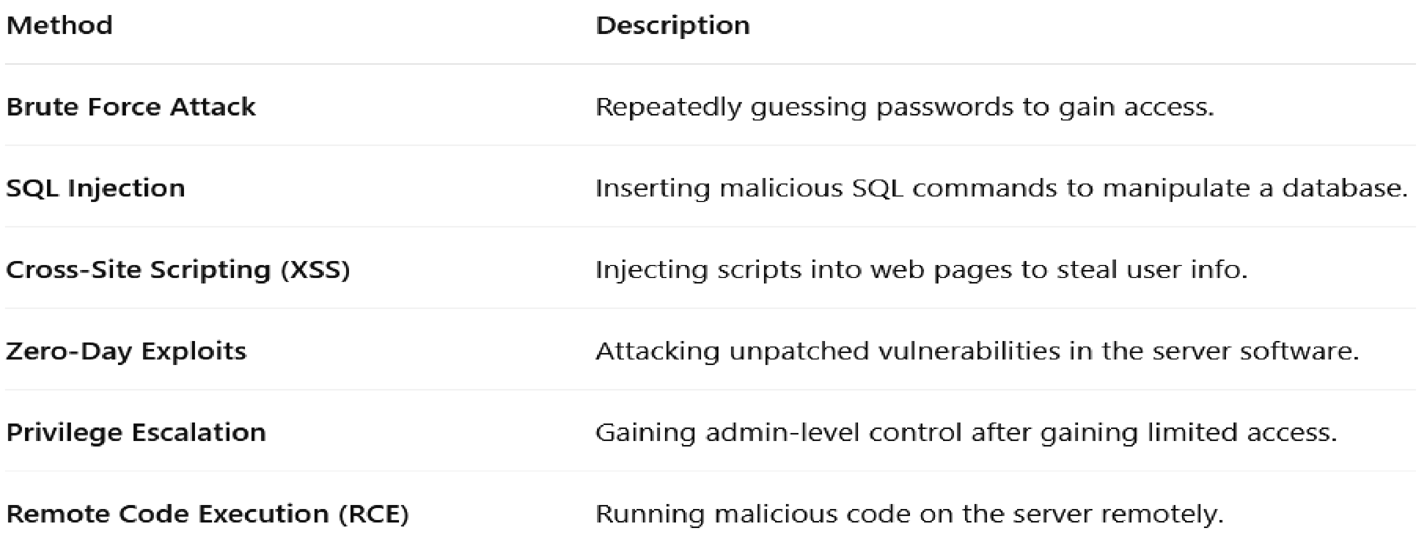
- **Email spoofing** is a type of cyber attack where the attacker forges the **sender's email address** to make the message look like it's coming from a **trusted source**.
- It's often used in **phishing, fraud, and malware attacks**.

Why is Email Spoofing Dangerous?

- Tricks people into clicking **malicious links** or downloading **malware**
- Can lead to **identity theft**, **data breaches**, and **financial fraud**
- Damages the reputation of individuals and companies
- Commonly used in **phishing campaigns**

Server Hacking

- **Server hacking** refers to unauthorized access or control over a **web server, database server, or application server** to steal data, disrupt services, or install malicious software.



Method	Description
Brute Force Attack	Repeatedly guessing passwords to gain access.
SQL Injection	Inserting malicious SQL commands to manipulate a database.
Cross-Site Scripting (XSS)	Injecting scripts into web pages to steal user info.
Zero-Day Exploits	Attacking unpatched vulnerabilities in the server software.
Privilege Escalation	Gaining admin-level control after gaining limited access.
Remote Code Execution (RCE)	Running malicious code on the server remotely.

Server Hacking

- What Hackers Can Do After Gaining Server Access ?

➢ Steal or delete user data

➢ Install backdoors or malware

➢ Hijack websites or web apps

➢ Launch DDoS attacks from the server

➢ Deface websites (change content or display messages)

➢ Distribute illegal or harmful content

Case Study

- **Equifax Hack (2017):**

A server vulnerability in Apache Struts (unpatched) led to the exposure of personal data of **147 million Americans**.

- Unpatched Vulnerability in Apache Struts.
- The hackers exploited a known vulnerability (**Common Vulnerabilities and Exposures**. (CVE-2017-5638)) in the Apache Struts web application framework.
- Although a patch was released in March 2017, Equifax failed to apply it in time.
- The attackers gained access to backend systems by sending malicious data via a web form.
- **Common Vulnerabilities and Exposures**.

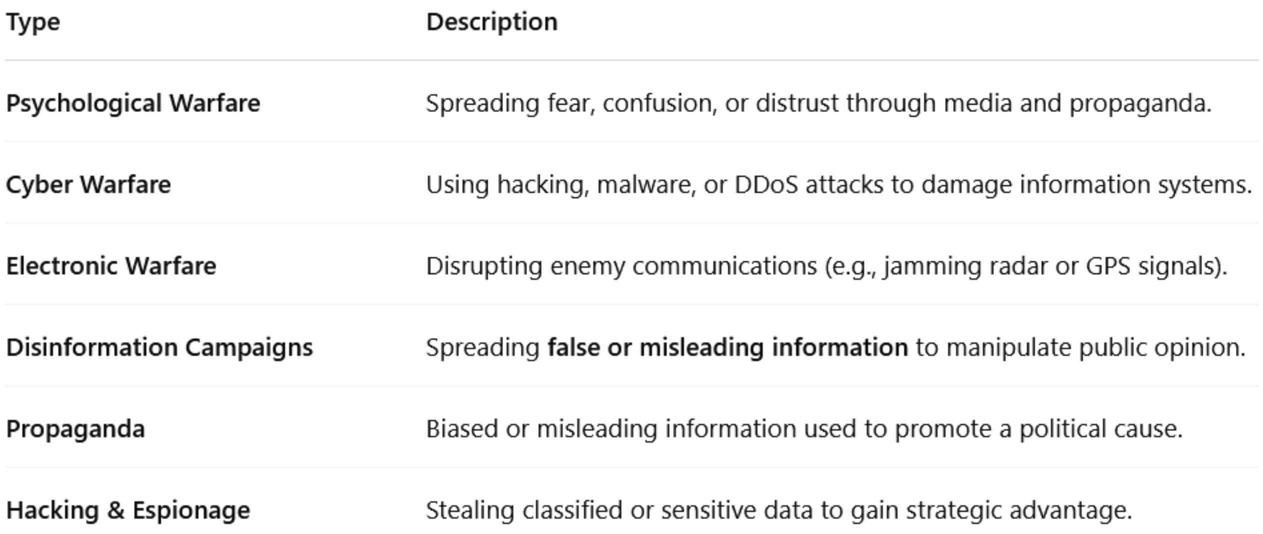
Information Warfare (IW)

- **Information Warfare (IW)** refers to the **use and manipulation of information** to gain a competitive, military, political, or psychological advantage over others.

- It involves using **data, media, and communication systems** as **weapons or tools** of conflict.

Classes of Information Warfare

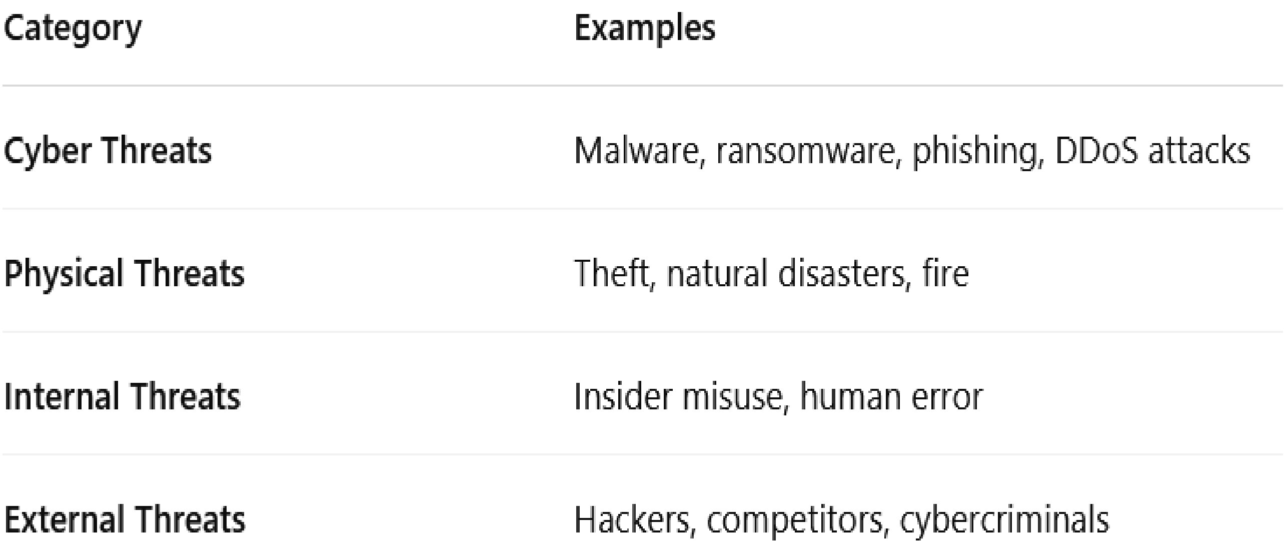
- Personal Information Warfare
- Corporate Information Warfare
- Global Information Warfare



Type	Description
Psychological Warfare	Spreading fear, confusion, or distrust through media and propaganda.
Cyber Warfare	Using hacking, malware, or DDoS attacks to damage information systems.
Electronic Warfare	Disrupting enemy communications (e.g., jamming radar or GPS signals).
Disinformation Campaigns	Spreading **false or misleading information** to manipulate public opinion.
Propaganda	Biased or misleading information used to promote a political cause.
Hacking & Espionage	Stealing classified or sensitive data to gain strategic advantage.

Threat Mitigation

- **Threat mitigation** refers to the process of **identifying, assessing, and reducing** the impact of security threats to protect systems, networks, and data from harm.
- This includes **preventive, detective, and corrective measures** to protect organizational assets.



Category	Examples
Cyber Threats	Malware, ransomware, phishing, DDoS attacks
Physical Threats	Theft, natural disasters, fire
Internal Threats	Insider misuse, human error
External Threats	Hackers, competitors, cybercriminals

Key Threat Mitigation Strategies

- Risk Assessment
- Patch Management
- Firewalls and Intrusion Detection Systems (IDS/IPS)
- Data Encryption
- Multi-Factor Authentication (MFA)
- User Awareness Training
- Backup and Disaster Recovery
- Access Control

Risk Assessment & Threat Modeling

- Identify **potential threats** (cyberattacks, data breaches, malware, natural disasters).
- Assess **vulnerabilities** in networks, systems, and applications.
- Develop **risk prioritization** based on impact and likelihood.
- **Example:** A financial institution conducts a **penetration test** to identify weaknesses in its online banking system.

Cybersecurity Measures

- Implement **firewalls, intrusion detection systems (IDS), and encryption**.
- Use **multi-factor authentication (MFA)** for secure access.
- Regularly update and **patch software** to close security gaps.

Example: A company enforces **zero-trust security**, requiring users to verify their identity before accessing internal systems.

Employee Awareness & Training

- Conduct **security awareness programs** on phishing, social engineering, and password security.
- Implement **data handling guidelines** to prevent accidental data leaks.

Example: An organization provides **monthly cybersecurity training**, reducing incidents of employee-related security breaches.

Incident Response Planning (IRP)

- Establish a Cyber Incident Response Team (CIRT).
- Define detection, containment, and recovery steps.
- Conduct tabletop exercises and simulations to improve preparedness.
- Example: A government agency simulates a ransomware attack to test response procedures

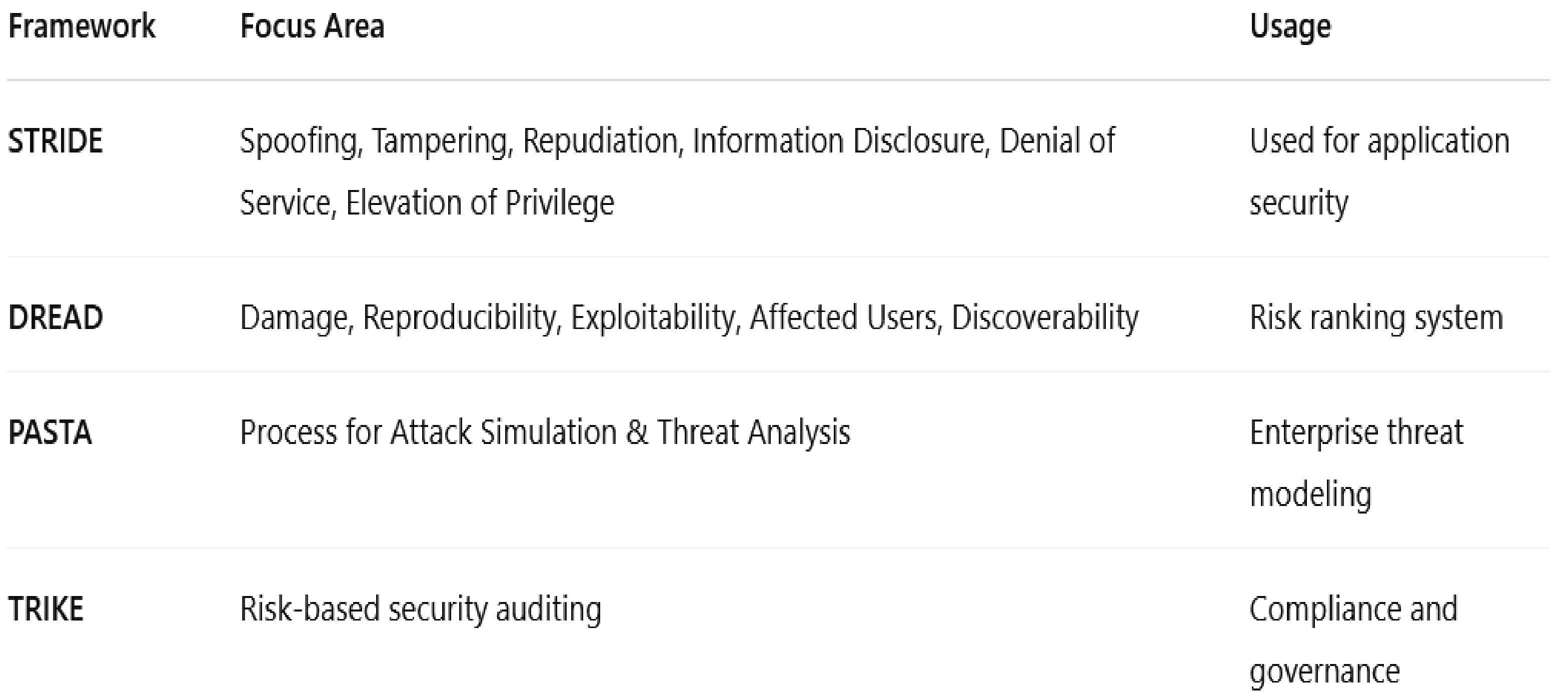
Threat Modeling

- A Proactive Approach to Cybersecurity

- **Threat modeling** is a structured process used to **identify, analyze, and mitigate** potential security threats to a system before they can be exploited.

- It helps organizations anticipate risks and strengthen their defenses.

Common Threat Modeling Frameworks



Framework	Focus Area	Usage
STRIDE	Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege	Used for application security
DREAD	Damage, Reproducibility, Exploitability, Affected Users, Discoverability	Risk ranking system
PASTA	Process for Attack Simulation & Threat Analysis	Enterprise threat modeling
TRIKE	Risk-based security auditing	Compliance and governance

Organizing the threats using STRIDE

- **S**poofing identity
- **T**ampering with data
- **R**epudiation (refuse to do with, dispute)
- **I**nformation disclosure
- **D**enial of service
- **E**scalation of privilege

Spoofing identity

- illegally obtaining access and use of another person’s authentication information
  - Man in the middle
  - URL phishing
  - Email address spoofing (email spam)

Tampering with data

- Malicious modification of the data
- Often hard and costly to detect
  - – you might not find the modified data until some time has passed;
  - – once you find one tampered item, you'll have to thoroughly check all the other data on your systems

Repudiation

- a legitimate transaction will be disowned by one of the participants
  - You sign a document first; and refused to confirm the signature
  - Need a trusted third party to mitigate

Information/data disclosure

- An attacker can gain access, without permission, to data that the owner doesn't want him or her to have.

Denial of service

- An explicit attempt to prevent legitimate users from using a service or system. It involves the overuse of legitimate resources.

- You can stop all such attacks by removing the resource used by the attacker, but then real users can’t use the resource either.

Distributed Denial of Service (DDoS)

- A Distributed Denial of Service (DDoS) attack is a malicious attempt to disrupt the normal functioning of a targeted server, service, or network by overwhelming it with a flood of internet traffic.

- Unlike a traditional Denial of Service (DoS) attack, which is carried out from a single source, a DDoS attack involves multiple sources, often geographically distributed and controlled by different attackers or automated systems.

Escalation of privilege

- an unprivileged user gains privileged access.
  - E.g. unprivileged user who contrives a way to be added to the Administrators group
  - Escalation of privilege in the context of security refers to the situation where an attacker gains higher-level access or permissions than they are initially granted.
  - This unauthorized elevation allows the attacker to perform actions that were not intended by the system's designers or administrators.

Disaster Recovery (DR)

- Disaster recovery focuses on restoring IT systems and business operations after an incident, ensuring minimal downtime and data loss.

- A set of policies, tools, and procedures that enable the **recovery or continuation of vital technology infrastructure and systems** following a disaster.

Common Disasters

- Cyberattacks (e.g., ransomware)
- Natural disasters (e.g., floods, earthquakes)
- Hardware failures
- Power outages
- Human errors

Key Components of a Disaster Recovery Plan

- Risk Assessment - Identify potential threats and vulnerabilities.
- Recovery Point Objective (RPO) - The maximum acceptable amount of data loss (measured in time).
- Recovery Time Objective (RTO) - The target time to restore operations after a disruption.

Key Components of a Disaster Recovery Plan

- Backup Strategy - Regular and secure data backups (offsite, cloud-based, etc.).

- Redundant Systems - Duplicate critical systems (e.g., in a different data center).

- Communication Plan- Define who communicates what, when, and how during a disaster.

- Testing & Drills- Regularly test the DR plan to ensure effectiveness.

Disaster Recovery Strategies

- **Disaster recovery** focuses on restoring IT operations after a **cyberattack, natural disaster, or system failure**. It ensures **business continuity** with minimal downtime and data loss.

✓ **Business Continuity Planning (BCP)**

✓ **Data Backup & Redundancy**

✓ **Disaster Recovery Sites & Failover Mechanisms**

✓ **DR Testing & Continuous Improvement**

Business Continuity Planning (BCP)

- Develop a **Business Continuity Plan (BCP)** to ensure critical functions continue during disruptions.

- Identify **essential IT infrastructure** and operations.

- Establish **alternate work environments** (e.g., remote work options during crises).

A retail company sets up backup servers in another location to ensure continued service after a cyberattack.

Data Backup & Redundancy

- Implement **automated data backup solutions** (cloud, on-premise).
- Store **multiple copies of critical data** in **different locations**.
- Use **real-time data replication** for instant recovery.

A retail company maintains **encrypted cloud backups** to prevent data loss.

Disaster Recovery Sites & & Failover Mechanisms

- **Hot Site:** Fully functional backup location, ready for immediate use.
- **Warm Site:** Partially equipped site with infrastructure that requires updates.
- **Cold Site:** Basic infrastructure in place, but no pre-installed systems.

A retail company maintains a **hot site** to restore operations within **minutes of an outage**.

Disaster Recovery Testing & Continuous Improvement

- Conduct **regular disaster recovery drills** to assess plan effectiveness.
- Update DR strategies based on **new threats and business changes**.
- Document lessons learned and improve **response time.**

A retail company **simulates a cyberattack** to test its response strategy and improve weak points.

Summary

- Ethics in Computing
- IP in Cyberspace
- Hacking
- Threat Mitigation
- Disaster Recovery