

LEGAL REGULATION IN SOFTWARE ENGINEERING LEVEL 200 SOFTWARE ENGINEERING (WEEK 5)

CHAPTER FIVE

Cybersecurity and Computer-Related Crimes

By Asick PECKINS



PLAN OF THE DAY

- Basics of cyber security and its importance in software engineering.
- Different types of cybercrimes, hacking, identity theft, etc
- Legal frameworks for addressing cybercrimes.
- Digital forensics and its role in investigating cyber incidents.



Basics of cyber security and its importance in software engineering.

What is cyber security?

Cyber security refers to the practice of protecting computer systems, networks, and data from digital attacks, theft, and damage. It involves implementing measures and protocols to ensure the confidentiality, integrity, and availability of information and systems.



Why is cyber security important in software engineering?

In today's digital age, software engineering plays a crucial role in the development of various applications and systems that are used in our daily lives. These systems contain sensitive information and any breach in their security can have severe consequences. Cyber security is essential in software engineering to protect these systems from cyber threats and attacks.

Types of cyber threats

There are various types of cyber threats that software engineering must be aware of, including:

- Malware: Malicious software designed to disrupt, damage, or gain unauthorized access to a computer system.
- Phishing: A fraudulent attempt to obtain sensitive information by posing as a legitimate entity through email, text messages, or other communication methods.

Types of cyber threats

- Denial of Service (DoS) attacks: An attempt to make a computer system or network unavailable to its intended users by overwhelming it with traffic.
- Man-in-the-middle (MitM) attacks: A type of attack where a hacker intercepts communication between two parties to steal information or manipulate the communication.
- SQL injection: A technique used to exploit vulnerabilities in a database-driven application by inserting malicious SQL statements.

Importance of implementing cyber security in software engineering

- Protection against cyber threats: Cyber security measures such as firewalls, encryption, and intrusion detection systems help protect software systems from various cyber threats.
- Safeguarding sensitive information: Software systems often contain sensitive information such as personal data, financial information, and trade secrets. Cyber security ensures that this information is protected from unauthorized access.
- Maintaining trust and credibility: In today's digital age, customers expect their personal information to be kept secure. Implementing robust cyber security measures can help maintain trust and credibility with customers.

Importance of implementing cyber security in software engineering

- Compliance with regulations: Many industries have regulations and laws in place that require organizations to implement cyber security measures to protect sensitive information. Failure to comply can result in legal consequences.
- Cost savings: The cost of recovering from a cyber attack can be significant, including loss of revenue, damage to reputation, and legal fees. Implementing cyber security measures can help prevent these costs.
- Business continuity: Cyber attacks can disrupt business operations and lead to downtime. By implementing cyber security measures, organizations can ensure business continuity and minimize the impact of a cyber attack.



Best practices for cyber security in software engineering

- Regular software updates: Keeping software systems up-to-date with the latest security patches is crucial in preventing vulnerabilities.
- Strong password policies: Implementing strong password policies, such as using complex passwords and changing them regularly, can help prevent unauthorized access.
- Data encryption: Encrypting sensitive data can prevent unauthorized access even if the data is compromised.
- Employee training: Educating employees on cyber security best practices can help prevent human error, which is often the cause of cyber attacks.



Best practices for cyber security in software engineering

- Regular backups: Regularly backing up data can help mitigate the impact of a cyber attack and ensure business continuity.
- Multi-factor authentication: Using multi-factor authentication adds an extra layer of security to systems and makes it harder for hackers to gain unauthorized access.

In conclusion, cyber security is crucial in software engineering to protect systems, data, and information from various cyber threats. It is essential for organizations to implement robust cyber security measures to ensure the safety and integrity of their software systems.

Different types of cybercrimes

1. Identity theft: This is when someone steals another person's personal information, such as their name, date of birth, social security number, or credit card details, to commit fraud or other illegal activities.
2. Cyber bullying: This refers to the use of technology to harass, intimidate, or bully someone. It can take place through social media, messaging apps, or other online platforms.
3. Ransom ware: This is a type of malware that encrypts a user's files and demands a ransom payment in exchange for the decryption key. If the ransom is not paid, the files may be permanently deleted.

Different types of cybercrimes

4. Cyber stalking: This is the use of technology to track, monitor, or harass someone. It can include sending threatening or unwanted messages, posting personal information online, or using spyware to track someone's online activity.
5. Online scams: These are fraudulent schemes that trick individuals into giving away their money or personal information. This can include fake emails, websites, or social media posts that appear to be from a legitimate source.
6. Cyber espionage: This is when hackers gain unauthorized access to a computer system or network to steal confidential information for political, economic, or military purposes.
7. Intellectual property theft: This refers to the unauthorized use or theft of someone else's creative work, such as copyrighted material, trademarks, or trade secrets.



Different types of cybercrimes

8. Hacking: This is when an individual gains unauthorized access to a computer system or network to steal information, disrupt operations, or cause damage.
9. Cyber terrorism: This is the use of technology to carry out acts of violence or create fear and panic in society. It can include attacks on critical infrastructure, such as power grids or transportation systems.
10. Child exploitation: This refers to the use of technology to exploit children for sexual purposes, such as sharing child pornography or grooming children for sexual abuse.



Legal frameworks for addressing cybercrimes

1. National laws: Each country has its own laws and regulations to address cybercrimes. These laws may include provisions for criminalizing specific cybercrimes, defining penalties, and establishing law enforcement agencies responsible for investigating and prosecuting cybercrimes.
2. International cooperation: As cybercrimes can occur across borders, international cooperation is crucial in addressing them. Countries may have agreements or treaties in place to share information and assist in investigations and prosecutions of cybercrimes.
3. Cybercrime conventions: The Council of Europe's Convention on Cybercrime is the first international treaty to address cybercrimes comprehensively. It provides a framework for countries to harmonize their laws, cooperate in investigations, and establish effective measures to combat cybercrimes.

Legal frameworks for addressing cybercrimes

4. Data protection laws: These laws regulate the collection, use, and storage of personal data by organizations and individuals. They aim to protect individuals' privacy and prevent the misuse of personal information, which can lead to cybercrimes such as identity theft.
5. Cybersecurity laws: These laws require organizations to implement security measures to protect their networks and systems from cyber attacks. They also define the responsibilities of organizations in the event of a data breach or cyber attack.
6. Intellectual property laws: These laws protect intellectual property rights and provide legal remedies for cases of intellectual property theft, such as copyright infringement and trademark violations.
7. Anti-money laundering laws: These laws aim to prevent criminals from using the internet to launder money gained from illegal activities. They require financial institutions to implement measures to detect and report suspicious transactions.



Legal frameworks for addressing cybercrimes

- 8. Computer crime laws: These laws specifically address crimes committed using computers or computer networks, such as hacking, malware distribution, and denial-of-service attacks.
- 9. Consumer protection laws: These laws aim to protect consumers from fraudulent or deceptive practices online, such as online scams and false advertising.
- 10. Law enforcement training: As cybercrimes are constantly evolving, it is essential for law enforcement agencies to receive training on the latest technologies and techniques used by cybercriminals. This enables them to effectively investigate and prosecute cybercrimes.



Digital forensics and its role in investigating cyber incidents

Digital forensics is the process of collecting, analyzing, and preserving electronic data for use as evidence in a criminal investigation. It plays a crucial role in investigating cyber incidents, as it allows law enforcement to gather and analyze digital evidence to identify the perpetrator and build a case against them.



Some key aspects of digital forensics in investigating cyber incidents include

- 1. Identifying and preserving evidence:** Digital forensics experts use specialized tools and techniques to identify and preserve digital evidence, such as computer logs, network traffic, and deleted files. This evidence can then be analyzed to determine how the cyber incident occurred and who may be responsible.
- 2. Recovering deleted or encrypted data:** Cybercriminals often try to cover their tracks by deleting or encrypting data. Digital forensics experts have the skills and tools to recover this data, which can provide valuable evidence in an investigation.
- 3. Tracking the source of an attack:** With the help of digital forensics, law enforcement can trace the source of a cyber attack back to the perpetrator. This involves analyzing network traffic, IP addresses, and other digital footprints left behind by the attacker.



Some key aspects of digital forensics in investigating cyber incidents include

4. Reconstruction of events: Digital forensics can help reconstruct the sequence of events leading up to a cyber incident. This includes identifying the actions taken by the perpetrator and the methods used to carry out the attack.

5. Expert testimony: In legal proceedings, digital forensics experts can provide expert testimony on their findings and analysis of digital evidence. This can help strengthen the prosecution's case against the perpetrator.

Overall, digital forensics plays a critical role in investigating cyber incidents and is essential in gathering and preserving evidence for successful prosecution. It is constantly evolving as technology advances, and law enforcement agencies must stay updated with the latest tools and techniques to effectively combat cybercrime.