CSE-4805 || **Computer Ethics** || Final Term Note

By- Main Uddin, *C201091 &* Sorowar Mahabub, *C201032*

Part-A

Segment-4

Question| What is the Therac-25 & what was incident happened about it? Write the case study of Therac-25 for this incident.

Answer: The Therac-25 was a software-controlled radiation-therapy machine used to treat people with cancer. Between 1985 and 1987, Therac-25 machines at four medical centres gave massive overdoses of radiation to six patients. In some cases, the operator repeated an overdose because the machine's display said that no dose had been given. Medical personnel later estimated that some patients received between 13,000 and 25,000 rads," where the intended dose was in the 100-200 rad range. These incidents caused severe and painful injuries and the deaths of three patients.

Case Study:

Software and Design problems:

Re-used software from older systems, unaware of bugs in previous software. Weaknesses in design of operator interface. There were bugs in software. Allowed beam to deploy when table not in proper position. Ignored changes and corrections operators made at console.

Observations and Perspective:

Minor design and implementation errors usually occur in complex systems, they are to be expected. The problems in the Therac-25 case were not minor and suggest irresponsibility. Accidents occurred on other radiation treatment equipment without computer controls when the technicians:

- Left a patient after treatment started to attend a party.
- Did not properly measure the radioactive drugs.
- Confused micro-curies and milli-curies.

AU-21|1.a| Assume that the family of one of the victims of the Therac-25 has filed 10 three lawsuits. They are suing a hospital that used the machine, the company that made the machine (AECL), and the programmer who wrote the Therac-25 software. As a programmer what you will do?

Answer: As a programmer who is hypothetically being sued in association with the Therac-25 incidents, the following steps should be considered:

1. **Legal Counsel:** Immediately seek expert legal advice.
2. **Documentation:** Gather all relevant documentation including:

- Software design documents
- Code repositories
- Version control history
- Communication with the employer and clients
- Test plans and test results
- Documentation of known bugs and the steps taken to solve them

3. **Communication:** Public statements can be used in court and it is best to let your attorney handle all communication.
4. **Insurance:** Check if there is professional liability that might needed for legal defence and any possible settlements or judgments.
5. **Expert Witnesses:** Your attorney might want to employ expert witnesses in the field of software engineering, specifically those with experience in safety-critical systems, to testify about the complexity of software development.
6. **Review the Allegations:** With your attorney, carefully review each lawsuit's allegations for elements such as duty of care, breach, causation, and damages.
7. **Emotional Support:** Consider seeking emotional and psychological support, as being involved in a lawsuit, particularly one as serious as this, is a major stressor.

SP-22|1.b| Discuss few current cases similar with Therac-25. Give some remedies to overcome from such cases in future.

Answer: There are no specific cases that have gained as much notoriety as the Therac-25 accidents that occurred in the 1980s, but few cases from different periods that, while not directly similar to the Therac-25 incidents, do involve similar themes of technology-driven risk:

1. **Boeing 737 MAX crashes:** The two fatal crashes involving the Boeing 737 MAX, Lion Air Flight 610 and Ethiopian Airlines Flight 302, were linked to the Manoeuvring Characteristics Augmentation System (MCAS). The MCAS was designed to activate based on input from a single angle of attack sensor, which, in these cases, provided wrong data, leading the system to forcefully and repeatedly push the nose of the plane down.

2. **St. Jude Medical's cardiac devices:** These devices were found to have vulnerabilities that could potentially allow a hacker to consume the. This raised concerns about the cybersecurity of insert medical devices.

3. **Volkswagen emissions scandal:** this case involved Volkswagen cars equipped with software that could detect when they were undergoing official emissions testing and alter the performance accordingly to improve results. While not a safety issue per se, it was a massive ethics and compliance failure with indirect health implications due to increased pollution.

To overcome such cases in the future, here are some remedies and best practices:

1. **Testing and Verification:** Implement comprehensive testing procedures, including static code analysis, dynamic testing, and formal methods where appropriate, to ensure that software behaves correctly under all conditions.
2. **Redundancy and Fail-Safes:** Critical systems should have redundancy, or fail-safes, so that if one component fails, others will prevent a catastrophe. For example, in the case of the Boeing 737 MAX.
3. **Ethical Design and Corporate Responsibility:** Incorporate ethical considerations into the design and development process and establish a culture of responsibility.
4. **Cybersecurity Measures:** For connected devices, robust cybersecurity protocols are essential to protect against unauthorized access and tampering.
5. **User Training and Error Reporting:** Users of complex systems should be trained, and there should be clear protocols for reporting and addressing potential errors.

Question| What are the Increasing Reliability and Safety?

Answer:

Professional techniques:

• Importance of good software engineering and professional responsibility.
• Redundancy and self-checking.
• Testing: Include real world testing with real users.

Law, Regulation and Markets:

• Criminal and civil penalties: Provide incentives to produce good systems, but shouldn't inhibit innovation.
• Warranties for consumer software: Most are sold 'as-is'.
• Regulation for safety-critical applications.
• Professional licensing: Arguments for and against.
• Taking responsibility.

Write about Dependence, Risk and Progress?

Answer: *Dependence:* Computers are tools, they are not the only dependence, they also depend on electricity.

Risk and Progress:

• Many new technologies were not very safe when they were first developed.
• We develop and improve new technologies in response to accidents and disasters.
• We should compare the risks of using computers with the risks of other methods and the benefits to be gained.

Segment-5

Question| Discuss the difference between copyright and patent.

Answer:

Copyright	Patent
A bundle of rights granted to the creator of original work, which excludes others from performing, selling or producing the work, is known as Copyright	A legal grant given by the government to the inventor which excludes others from making, utilizing or trading the invention for a set period, is called a patent
Covers artistic and literary/writers works	Covers inventions
Copyright protection is automatic, no formality is required	Patent protection requires registration
Excludes Others from copying or trading the product	Excludes others from manufacturing or using the product
Subject matter is expression	Subject matter is ideas
Copyright, in general, is granted for 60 years	Patent is granted for 20 years

AU-22|2.b| How does new technology threaten the protection of copyrighted materials?

- The emergence of digital technologies towards the concluding decades of the twentieth century raised a whole new set of challenges to copyright regimes.
- All works can now be digitalized whether they comprise texts, images, sound or diagrams.
- Once digitalized the various elements such as images are all 'equal' and can be merged, transformed, manipulated or mixed to create an endless variety of new works.
- With the advent of the digital environment, the access, use, duplication or modification of the original work has become really easy
- Digital environment has created a platform for people for widespread cost-effective distribution of the original works, posing serious threats to the interest of the creator.
- With the emergence of the Internet and increasing use of the world wide web possibilities of infringement of copyright have become mind boggling free and easy.
- Taking content from one site, modifying it or just reproducing it on another site has been made possible by digital technology.
- Piracy occurs when copyrighted software is made available to users to download without the express permission of the copyright owner. Such illegal software is offered over online sources
- Piracy hampers creativity, hinders/decrease the development of new software and local software industry and ultimately effects e-commerce.

Question| Define Software piracy and Intellectual property.

Answer: The term "piracy" describes the act of reproducing copyrighted works without permission from the copyright owner. **Software piracy** is a term that is frequently used to describe the illegal copying, distribution or use of computer software in violation of its license (commonly referred to as an end user licensing agreement or EULA). Most software programs purchased are licensed for use by just one user or at just one computer site. Moreover, when someone buys software, he or she is known as a "licensed user" rather than as an owner of the software.

Intellectual property:

Intellectual property (IP) refers to creations of the mind, such as inventions; literary and artistic works; designs; and symbols, names and images used in commerce. Intellectual property rights (IPRs) are the rights granted to the creators of Intellectual property, and include trademarks, copyright, patents, industrial design rights, and in some jurisdictions trade secrets. Artistic works including music and literature, as well as discoveries, inventions, software, words, phrases, symbols, and designs can all be protected as intellectual property. The key to understanding intellectual property protection is to understand that the thing protected is the intangible creative work—not its particular physical form.

Question| Describe the benefits of copyright protection.

1. Copyright protection provides a vital incentive/security for the creation of many intellectual works.
2. Without copyright protection, it would be easy for others to exploit/use these works without paying any royalties or remuneration to the owner of the work.
3. Copyright encourages enterprise and creates a favourable climate to stimulate economic activity. 4. Copyright protection provides benefits in the form of economic rights which entitle the creators to control use of their literary and artistic material and to obtain an appropriate economic reward.
5. Creators can therefore be rewarded for their creativity and investment.
6. Copyright also gives moral rights to the creator. An author's right to object to the modification of his or her work is known as an integrity right.

Part-B

Segment-6

Question| What is hacking? Explain all the term has changed over time?

Answer: Hacking: currently defined as to gain illegal or unauthorized access to a file, computer, or network. The term has changed over time:

Phase 1: early 1960s to 1970s:

- It was a positive term.
- Hacker: creative programmer who wrote or clever code.
- Hack: was an especial clever piece of code.

Phase 2: 1970s to mid-1990s:

- Hacking took on negative sense.
- Breaking into computers for which the hacker does not have authorized access.
- Spreading worm & viruses into computers.
- Companies began using hackers to analyse and improve security.

Example: 1980's: German hacker broke into US military computers to find info to sell to Russians.

Phase 3: beginning with the mid-1990s:

- The growth of the Web changed hacking. Viruses and worms could be spread rapidly.
- Political hacking (Hacktivism) surfaced.
- Denial-of-service (DoS) attacks used to shut down Web sites.
- Zombies, used to control other computers.
- Large scale theft, of personal and financial information.

Example: In 2000: `Love Bug', email virus (MS Windows) which destroyed files, affected large corporations (FORD, NASA, Pentagon) cost $10 billion damages.

Question| Explain Hacktivism or Political Hacking? How do you determine whether something is hacktivism or simple vandalism?

Answer: This hacking is used to promote a political cause. Disagreement about whether it is civil disobedience and how it should be punished. Some use the hacktivism to hide other criminal activities. Some argue that hacktivism is a form of civil disobedience (disobey of law). Peaceful resistance vs destruction of other's property. We have freedom to speak but not the right to force others to listen & nor to shut them up.

Example: Modification of the U.S department of Justice web page to become "Department of injustice". Another example, Teenagers hacked India's atomic research centre to protest nuclear weapons.

Question| What are the laws of Catching and Punishing Hackers?

- **Catching hackers:** Law enforcement agents read hacker newsletters and participate in chat rooms undercover. They can often track a handle by looking through newsgroup archives. Security professionals set up 'honey pots' which are Web sites that attract hackers, to record and study. Computer forensic is used to retrieve evidence from computers.

• **Penalties for young hackers:** Many young hackers have matured and gone on to productive and responsible careers. Punishment depends on damage done. Most young hackers receive community service and fines. Not until 2000 did a young hacker receive time in juvenile detention.
• **Expansion of the Computer Fraud and Abuse Act:** The CFAA predates social networks, smartphones, and sophisticated invisible information gathering. Some prosecutors use the CFAA to bring charges against people or businesses that do unauthorized data collection.

AU-21|3.b| What is ethical hacking? What do you Mean by it? Should we learn it? Justify your answer.

Answer: Ethical hacking refers to the practice of bypassing system security to identify potential data breaches and threats in a network. The company that owns the system or network allows cybersecurity experts to perform such activities in order to ensure the system is secure. These cybersecurity experts are referred to as ethical hackers, and their practice is legal because they have permission to probe the system.

Ethical hacking involves a variety of methodologies to test and ensure the system's security, including:

1. **Vulnerability Scanning:** Using automated tools to scan a system against known vulnerability signatures.
2. **Penetration Testing:** Simulating cyberattacks to identify and exploit weaknesses in security, including OS, application, and improper configurations.
3. **Phishing Attempts:** Attempting managed and controlled phishing attacks to understand the risk level and to raise awareness among users.
4. **Security Auditing:** Performing audits of system security settings and policies.
5. **Risk Assessment:** Analysing the risk in the environment and assessing the impact of potential attacks.
6. Ethical Hackers also deal with other issues such as encryption, wireless security, and social engineering.

The necessity to learn ethical hacking depends on one's personal interests and professional goals. Here are a few reasons for learning it:

1. **Cybersecurity Skill:** As our reliance on internet-connected devices grows, the importance of understanding cybersecurity and being able to defend against cyber threats also grows. Learning ethical hacking can equip you with a vital skill set in cybersecurity.
2. **Career Opportunities:** With the increase in cyber threats, there is a rising demand for professionals skilled in cybersecurity. Ethical hacking is a recognized and respected specialization within this field, and it can lead to numerous career opportunities.
3. **Understanding Threats:** The knowledge gained from learning ethical hacking allows one to understand how real-world cyber threats are constructed and how they can be countered. This is important for anyone responsible for securing information systems.
4. **Preventive Action:** By finding and fixing security vulnerabilities before malicious hackers can exploit them, ethical hacking helps to maintain strong security measures and prevent unauthorized access.
5. **Contribution to Cybersecurity:** Ethical hackers contribute to cybersecurity by constantly challenging the existing security infrastructure and finding ways to improve it.
6. **Legal and Ethical Side:** It is crucial for anyone involved in the security field to understand the legal and ethical boundaries. Learning ethical hacking ensures that one is equipped with this knowledge.

Segment-7

Question| List some job categories where the number of jobs declined drastically as a result of computerization.

Answer: Measuring the effects of computers alone is difficult, because other factors influence employment trends, but we can look at some overall numbers.

- As the use of ATMs grew, the number of bank tellers dropped by about 37% between 1983 and 1993.
- The number of telephone switchboard operators dropped from 421,000 in 1970 to 164,000 in 1996.
- The jobs of building, selling, and repairing typewriters have disappeared.
- Railroads computerized their dispatch operations and eliminated hundreds of employees.
- The jobs of electric meter readers disappeared as utility companies installed devices that send meter readings to company computers.
- Similar technology monitors vending machines and oil wells, reducing the number of people needed to check on them in person.
- Shopping on the Internet and self-service checkout systems in stores reduced the need for sales clerks.
- Hundreds of music stores closed and jobs in the printing industry declined as music, magazines, newspapers, and books went digital.

Question| List some job categories where the number of jobs increased drastically with increasing use of computers.

Answer: A successful technology eliminates some jobs, but creates others.

- Countless new products and services based on computer technology create jobs: iPods, medical devices, 3-D printers, navigation systems, smartphones and apps for them, and so on and on.
- The Facebook app industry alone accounted for between 180,000 and 235,000 fulltime jobs in the United States in 2011.
- New technologies and products create jobs in design, marketing, manufacture, sales, customer service, repair, and maintenance.
- Computer and Internet technology generated all the jobs at Google, Apple, eBay, Hulu, Amazon, Microsoft, Twitter, Zappos—and thousands more companies.

- The projected growth in employment of computer programmers is attributable to increased demand for new and updated software. By writing computer code, they turn the designs created by software developers into instructions a computer can follow.
- Computer systems analyst's workers serve as a link between IT departments and management. They analyse an organization's computer systems and recommend ways to make the business run more efficiently. Computer systems analysts employed in this industry often serve as consultants.
- Computer support specialists provide help and advice to consumers or organizations that are using computer software or equipment. Some assist customers who call the company to speak to a specialist when they are having trouble with a software program or networking device.
- Other computer support specialists work in a company's IT department and provide support for other company employees who are having computer problems.

Question| Define telecommuting. What are advantages and disadvantages of telecommuting?

Answer: Telecommuting is working from a remote location outside of a traditional office. The remote location can be from home, a coffee shop, or hotel room. The Internet, faxes, phones, webcams, and instant messaging are some of the technological advances that enable this type of work arrangement. Most telecommuters work in the financial, high-tech, and communications industries.

Advantages of Telecommuting:

- No Commuting: Depending on your current commute, this can save you anywhere from minutes to hours every day, which you can spend doing things you enjoy, like sleeping, spending more time with your kids or spouse, going to the dog park, or any other activity you'd like to have more time for.
- Increased Independence: Working from home puts the onus on you to complete your work without constant reminders, which some people absolutely love. No office politics, no boss breathing down your neck, no distracting co-workers.
- Increased Savings: Most people who work from home have very little need for professional clothing, which not having to buy can save lots of money every year. Other things you'll find less need for: gas or public transit passes for commuting, lunches out, dry cleaning, and child care (depending on your situation).
- More Flexibility: Again, this depends on the type of job you'll have at home, but many work-from-home jobs allow for a flexible schedule, so if you need to go grocery shopping or do a load of laundry in the middle of the day, it's simple: you can. Or, if you're a morning person or a night owl, you can adjust your work schedule accordingly.

Disadvantages of Telecommuting:

- Decreased human interaction: If you're the sort of person who thrives on interactions with other people, working from home can feel isolating. It's possible to remedy this feeling with e-mail, phone calls, instant messaging, and video conferencing, but it's no substitute for face-to-face interaction.
- Blurring Work and Personal Life: When you work from home, you can't always shut out your personal life while you're working, or turn off your work life while you're "off the clock."
- Difficulty Demonstrating Workload: If you're a telecommuter working for a company with a traditional office, your office-bound co-workers might perceive you as doing less work simply because you're at home.

Question| Write the reasons for monitoring employee communications.

Answer: Purposes of monitoring employee communications include training, measuring or increasing productivity, checking compliance with rules for communications, and detecting behaviour that threatens the employer in some way. The below list a variety of purposes:

- Protect security of proprietary information and data.
- Prevent or investigate possible criminal activities by employees. (This can be work related, such as embezzlement, or not work related, such as selling illegal drugs.)
- Check for violations of company policy against sending offensive or pornographic messages.
- Investigate complaints of harassment.
- Comply with legal requirements in heavily regulated industries.
- Prevent personal use of employer facilities (if prohibited by company policy).
- Locate employees.
- Find needed business information when the employee is not available.

Segment-8

AU-22|5.a| What is "Professional Ethics"? Write the importance of CSE graduates knowing and flowing professional ethics.

Answer: Computer Science and Engineering (CSE) graduates are central to the design, development, and maintenance of the software and systems that underpin modern society. As they work on technologies that affect a wide range of industries and personal lives, it is vital for CSE graduates to know and abide by professional ethics for several fundamental reasons:

Public Safety and Welfare: CSE graduates often develop systems and applications that are integral to industries such as healthcare, transportation, and financial services, where safety and welfare are paramount. Ethical consideration is essential to ensure that the systems are reliable, safe, and do not endanger human life or well-being.

Trust: Trust in technology is fundamentally tied to how it is created and used. Ethical behaviour in design, development, and implementation fosters trust between technology users, companies, and broader society. When users trust that technology is built and maintained to ethical standards, they are more likely to adopt and integrate these technologies into their daily lives.

Data Privacy: With big data analytics and the widespread use of personal information in computing applications, CSE graduates need to ethically manage data privacy. Respecting user consent, securing data against unauthorized access, and responsibly reporting data breaches are all ethical concerns that are paramount to retaining public trust.
Intellectual Property: Understanding and upholding ethical standards is crucial to respect intellectual property rights. This includes recognizing and crediting the contributions of others, not plagiarizing code or content, and adhering to licensing agreements. These practices foster innovation, collaboration, and fair competition.
Long-term Accountability: CSE professionals should consider the long-term implications of the systems they create, including sustainability, environmental impact, and how their work may affect future generations. Ethical foresight is necessary to prevent harm and ensure that technological progress is aligned with humanity's best interests.
Adherence to Laws and Regulations: Ethics often align with legal requirements, but going beyond compliance to understand the spirit of the law is important. Helping employers or clients abide by relevant laws, such as those governing data protection (e.g., GDPR), reflects not just on personal integrity but also on the reputation and legality of the business operations.
Professional Integrity: Upholding ethics is also about personal and professional integrity. This can include continuous learning to keep skills up-to-date, honesty in reporting results (e.g., in testing and quality assurance), and transparency in decisions and mistakes.
Collaboration: Working ethically includes collaborating with others in a respectful and fair manner, acknowledging diverse perspectives and contributions, and maintaining a culture of mutual respect and learning within teams and the broader professional community.
Role Modelling: As emerging leaders in technology, CSE graduates have an opportunity to serve as role models for responsible and ethical behaviour. This can inspire others and set a standard for aspiring computer scientists and engineers.

AU-22|5.b| Describe the ACM code of ethics and discuss the potential challenges associated with its implementation in the field of computer science.

Answer: The ACM, or Association for Computing Machinery, code of ethics is a collection of principles and guidelines designed to help computing professionals make decisions that are ethically responsible and beneficial to society. The ACM Code of Ethics and Professional Conduct ("the Code") expresses the conscience of the profession and outlines a set of behaviours for ACM members and serves as a model for other individuals who work in the field of computing.

The Code is anchored in four primary values:

1. Honesty: Being truthful and transparent in one's dealings.
2. Fairness: Ensuring fairness and not discriminating against individuals or groups.
3. Respect for People: Treating all individuals with dignity and preserving the privacy of others.
4. Integrity: Upholding the highest standards of work and avoiding conflicts of interest.

It also addresses issues such as privacy, system abuse, intellectual property, and the importance of avoiding harm to others.

Implementing the ACM Code of Ethics in the field of computer science presents various challenges:

1. **Rapid Technological Change:** Computer science is a field characterized by rapid advancements. Ethical guidelines that are relevant today may become obsolete or require substantial revision as new technologies are developed. This makes it hard to create and maintain a set of ethical guidelines that are both specific and enduringly relevant.
2. **Cultural Differences:** The ACM Code of Ethics needs to be globally applicable. However, cultural perceptions of privacy, censorship, and workers' rights, for example, vary greatly from one country to another. This diversity can lead to conflicts when trying to apply a universal ethical code.
3. **Interpretation and Enforcement:** Even with a clear set of ethical guidelines, individual interpretation can vary. Enforcing ethics is also a significant challenge. The ACM can revoke membership, but the actual power to prevent unethical behaviour is limited, and the consequences for violating the Code may not be severe or deterrent enough.
4. **Complex Stakeholder Relationships:** Modern computing projects often involve a variety of stakeholders with their own interests and ethical standards. Balancing these interests in a way that adheres to the ACM Code can be complex and difficult.
5. **Education and Awareness:** Not all practitioners may be aware of the Code or understand how to apply it in specific situations. Continuous education around ethical issues in computer science is required to ensure that professionals understand and can implement ethical decisions effectively.
6. **Whistleblowing:** Situations may arise where adhering to the Code could mean speaking out against one's employer or colleagues. This could have professional or personal repercussions for the individual, discouraging them from taking the ethically correct action.
7. **Evolving Definitions of Harm:** The Code advises avoiding harm to others, but as technology becomes increasingly integrated into daily life, the definition of "harm" becomes more complex and nuanced. For example, the indirect effects of social media on mental health are a harm that would have been difficult to anticipate in previous decades.
8. **Balancing Business and Ethics:** Practitioners may often find themselves in situations where business objectives conflict with ethical practices. Choosing to prioritize ethical considerations may come at the cost of competitive edge or profit.

Note Regarding Question: *jototuku khobor jani j question besirbag analytical hbe, I mean topics buja lagbe- tailei answer kra jabe. So this notes covers all topics suggested by* **Arfanul Islam** *sir and also some previous questions.*
***Special Acknowledgement** to* **Main Uddin**, *7CM, C201091 for his effort.*
Sorowar Mind kriona, Mind krle Shine krte parbana, hihiheheheehe!

Thank You. Assalamualaikum Waa Rahmatullah.

By- Main Uddin, *C201091* & Sorowar Mahabub, *C201032*