Ruth Abeselom

# Software Security

The assignments are Review Question 11.1 on page 393, Review Question 11.2 on page 393, Review Question 17.1 on page 546, Review Question 19.1 on page 602, and Review Question 19.2 on page 602 of the textbook (Chapters 11, 17, 19). For your convenience, the questions are shown below. Please write your answers to the questions. Please upload this document on Canvas by the due date.

11.1 Define the difference between software quality and reliability and software security.

The unforeseen failure of a program due to theoretically random, unexpected input, system interaction, or usage of faulty code is the primary concern of software quality and reliability. It is anticipated that these errors will occur according to a probability distribution. Using some type of systematic design and testing to find and remove as many defects as possible from a program is the standard technique to enhance software quality. The goal of testing is to reduce the amount of bugs that would be encountered in everyday use by varying the likely inputs and common errors. The frequency with which bugs are activated and lead to program failure is more concerning than the overall quantity of bugs in a program. However, software security is different in that the attacker selects the probability distribution, focusing on particular defects that lead to a failure that the attacker can take advantage of. These vulnerabilities are unlikely to be found by standard testing techniques since they are frequently caused by inputs that deviate significantly from what is typically expected.

11.2 Define defensive programming.

The process of developing and running software to ensure that it keeps working even in the face of an attack is known as defensive or secure programming. Defensive programming aims to improve software system reliability, stability, and security. Software developed with this technique can identify false conditions brought on by an attack and can decide whether to proceed safely or terminate gracefully. Defensive programming's essential principle is to never make assumptions; instead, you should verify every assumption and address any potential error conditions. Any assumptions regarding a program's operation and the kinds of input it will handle should be made clear. By applying defensive programming techniques, developers can reduce the likelihood of software bugs, improve error detection and recovery, enhance system resilience, and mitigate potential security risks. The goal is to create software that is more reliable, maintainable, and secure in the face of unforeseen situations and adverse conditions.

17.1 What are the benefits of a security awareness, training, and education program for an organization?

A security awareness training program aims to educate and concentrate employees' attention on security risks within the organization. The objective is to equip employees with the

knowledge and abilities needed to carry out IT-related duties more safely. Training covers a wide range of abilities, from fundamental computer skills to highly specialized capabilities, depending on the user's function. Employees are encouraged to operate appropriately because they are aware of their obligations to uphold security and the limitations placed on their actions for that reason. Awareness initiatives can help to foster user support, IT staff enthusiasm, and management buy-in, as there is a constant stream of new dangers to deal with. In addition to communicating the information security policies and procedures that must be adhered to, awareness serves as the basis for any disciplinary measures and actions that may be applied for non-compliance.

19.1 Describe a classification of computer crime based on the role that the computer plays in the criminal activity.

The term computer crime refers to criminal action wherein computers or computer networks are utilized as a weapon, a target, or a location for illicit activity. While computer crime may or may not involve networks, cybercrime expressly refers to the use of networks. A computer system can be the target of a crime if it is intended to obtain information stored on it, take control of it without permission or payment (known as theft of service), change the integrity of data, or prevent the computer or server from operating as intended. An attack on data confidentiality, availability, privacy, or system integrity is a component of this type of crime. Examples include hacking, malware attacks, distributed denial-of-service (DDoS) attacks, and data breaches. The aim is to compromise the security and integrity of computer systems or steal sensitive information.

19.2 Define three types of property.

Three main categories of property are distinguished by the U.S. legal system in the U.S. as real, personal, and intellectual property. Real property consists of both land and objects that are permanently bound to it, such as buildings, trees, and mobile homes that are immobile. Personal property includes portable commodities and personal things like cars, bank accounts, earnings, securities, furniture, insurance policies, jewelry, patents, and pets. Any intangible asset derived from human knowledge and ideas is referred to as intellectual property. Software, data, books, sound recordings, the creation of an original sort of invention, or the discovery of a medical remedy are a few examples.