Written Exam for IntroSec

2021-08-06 1:00 pm– 5:00 pm (4 hours)

Problem 1
What is certificate? Discuss whether and how it can be used to ensure or support the security triad of CIA.

Problem 2

Discuss the security threats brought by injection attacks with at least two different kinds of examples (i.e., two types of injection attacks). Good answers will cover principles/causes of the attacks, possible threats and countermeasures.

Problem 3

Define each of the following IT security related terms. Also, for each of these terms further illustrate the concept by choosing a closely connected IT security concept and explaining the relationship between the concepts. Furthermore, give an example of an application of these tools/threats/concepts. Give concrete examples wherever possible. Structure each of your answers with headings definition, relationship to [your chosen related concept], and example. Your answers to each part should contribute to evidence of your deep understanding of the concept. Related concepts and examples should be chosen and explained with care to maximise the depth of your answers.

Please note that in general a 50% complete answer will be required to obtain a pass mark for this problem

- STRIDE
- Access policies
- Diffie-Hellman
- Incomplete mediation

If it helps you, you may like to paste the following into your editor to help you structure your answer:

- o Definition
- o Relationship to [replace this with your chosen related concept]
- o Example

Problem 4

When you use a web system (for example, iLearn for online learning), you are often asked to input a user identification (User ID) and a password first. Explain the security functions of the User ID and the password. Give and discuss another two (different kinds of) methods that can replace or improve the security functions provided by using User ID and password.

Problem 5

During the time of Covid-19, more private data of citizens' daily life may be collected by governments/companies for tracing the passing locations of the citizens. For example, people are often required to use "checkin" apps when enter public places like cinemas, shops etc. In this case, some personal information including the personal contact information is collected and stored in a server through the apps.

Taking this as an example, discuss the requirements to PETs (Privacy Enhancing Technologies) in data storage, data transmission, data consumption or provisioning in terms of the privacy properties: anonymity, pseudonymity, unlinkability, unobservability and undetectability.