HW6 – Cyber Security
Chen Hao Cheng

Questions not in book:
Question1) Use own sentence (no more than two) to represent each point

1) **Earn or give, but never assume, trust**
   Do not trust without validating

2) **Use an authentication mechanism that cannot be by passed or tempered with**
   Use a flawless authentication mechanism

3) **Authorize after you authenticate**
   Authorize, although authenticated

4) **Strictly separate data and control instructions, and never process control instructions received from untrusted sources**
   Isolate control instruction from data and never access the untrusted control instruction

5) **Define an approach that ensures all data are explicitly validated**
   Define a strategy that guarantees entire data are validated explicitly

6) **Use cryptography correctly**
   Define a strategy that guarantees entire data are validated explicitly

7) **Identify sensitive data and how they should be handled**
   Discover the sensitive data and find secure methods to handle them

8) **Always consider the users**
   Always think in user's prospects.

9) **Understand how integrating external components changes your attack surface**
   Aware the impact of integrating external components on the attack surface

10) **Be flexible when considering future changes to objects and actors**
    Be adaptable when considering upcoming changes to actors and objects

Question 2)
I was building a program that can analysis some certain cryptocurrecy, and my program was connecting some trading website's API such as Gdax. Gdax is well known American trading website, it is another trading website of Coinbase. However, I violate the first point of Top Flaws, "Earn or give, but never assume, trust". I assume the trading website can be trusted

because it is well known trading website in the United States. I should valid it first because I put my personal account information connecting their API so there is a possibility that my account will be accessed by unauthorized individuals.

Another example is when I took a class called Linux Administration, I made a mistake that all user can access the system root privilege which they can run “sudo” command as root. This is violating the “Authorize After You Authenticate”.

Review Questions:

16.1)
What are the principal concerns with respect to inappropriate temperature and humidity?

Computer or its related equipment’s should be kept from range 10 to 30 degrees Celsius, otherwise, it might produce unwanted results.

High room temperature:
If a computer is in the high temperature room, the internal components might be damaged because cooler inside the CPU won’t work properly.

Low room temperature:
If a computer is in the cold temperature room, the computer can have a thermal shock when it’s switched on.

High internal equipment temperature:
If the temperature of internal equipment is too high, the computer might have a shortage of power and vent blockage.

High humidity:
The electrical and electronic equipment in the computer may be damaged.

Low humidity:
The computer might lose their shape and the performance of the equipment might be affected badly.

16.7)
List and describe some measures for dealing with power loss

Electrical loss threat:

Electrical power is the main resource for computer and its related equipments. To operate any information system related with the computer without any interruption, electrical power is an essential resource for that.
Three types of threats posed by the loss of electrical power.

1. Under voltage
2. Over voltage
3. Noise

Precaution measures to deal with water damage:

- Power interruptions for small amount of time can be managed with the help of UPS (uninterruptible power supply)
- Installing UPS will provide backup to maintain the power to computer monitors, processors, and other related equipment for a certain period of time
- If you want to have longer backup for power loss, the organization must also install generators. The generators have to be maintained properly and the personnel dealing with the generators should have properly training

16.8)
List and describe some measure for dealing with human-caused physical threats.

Unauthorized physical access:

1) For some certain portions of building or complex should not be allowed entering with inappropriate authorization unless you are with an authorized individual. All the sensitive assets such as servers, mainframe computers, network equipment, and storage networks should be in restricted area. Only small number of employees can access to it.

Unauthorized physical access can lead to other threats such as theft, vandalism, or misuse

a) **Theft:** Theft of equipment and theft of data by copying. Also, theft can be at the hands of an outsider who gained unauthorized access or by an insider
b) **Vandalism:** includes destruction of equipment and data
c) **Misuse:** Resources by individuals who are authorized at all, or resources use by improper way by people who are authorized