|  |  |  |
| --- | --- | --- |
|  |  | CPS 633 – note questions  Jae Duk Seo |

# Lecture 1 – intro to security

1. What is computer security and how can we determine a value of asset?
2. What are the 2 question that we must ask when detecting potential harm to an asset.
3. When do we do non – malicious attack? Difference between the direct attack and advance persistent attack?
4. Why do we use framework and what does framework provide us.
5. What 3 things attacker need? And what is risk management used for, also what is residual risk?
6. What are some functions of basic risk management module?
7. In today’s computer security what are the control aspect exist?
8. Why do we need to know different type of threat? What does it help us?
9. There are major five method of computer security – name all of them.
10. What are policies and procedures – how can we achieve this? Example of physical control?
11. Today control network has 7 elements that are important to security. Name and describe each of them.
12. In network security three more aspect of security gets added, what are these and describe them.
13. Interception, modification, fabrication, repudiation of origin, and interception – describe each of them.
14. Example of encryption, s/w control, h/w control. What does encryption protect among CIA triad?
15. When does each CIA fail? (Interception, modification, fabrication etc…)
16. Why do we need to redefine the C property?
17. Example of integrity failures, and can the meaning of integrity change?
18. For A property, when do we say that A have failed?
19. What are some attacks on CIA? – Example of each attack and tell which among the CIA triad have failed.
20. Four principal of computer security, name them and describe them.

# Lecture 2 – access control

1. What are the tools for security professionals? When computer tries to recognize individual what do they rely on?
2. What distinguish between the pretenders and the real identity?
3. Determining an induvial involves 2 steps what are does? Also what is the difference among those two?
4. Why is remote authentication researched among the recent years? Also, over the years computing power have increased, how does this affect in the security industry?
5. There are 4 means of authentication, what are those?
6. What is the difference between multi server authentication and single server authentication?
7. In formal analysis what two kind of methods exist? Also what is formal analysis?
8. In AVISPA what metrics are used?
9. Name the two methods that we learned regarding ‘something user knows’.
10. There are four different type of attacks towards password, what are they? (name and describe them)
11. What is the difference between popular password attack and single account password attack?
12. In BAN logic there are three steps of verification name and describe them in order.
13. Name 4 more attacks on password (Different from the above ones.)
14. How do we store a password? Also in a nut shell, explain the dictionary attack.
15. What is a concealed passwords and what are rainbow tables? (Describe an attack involving the rainbow table.)
16. What are salt values and why do we need them?
17. Describe the Brute Force attack, and what three factors can reduce the amount of time needed to solve a password in brute force attack?
18. In a Linux system, what are the steps to store a password. Also, what does salt values provide?