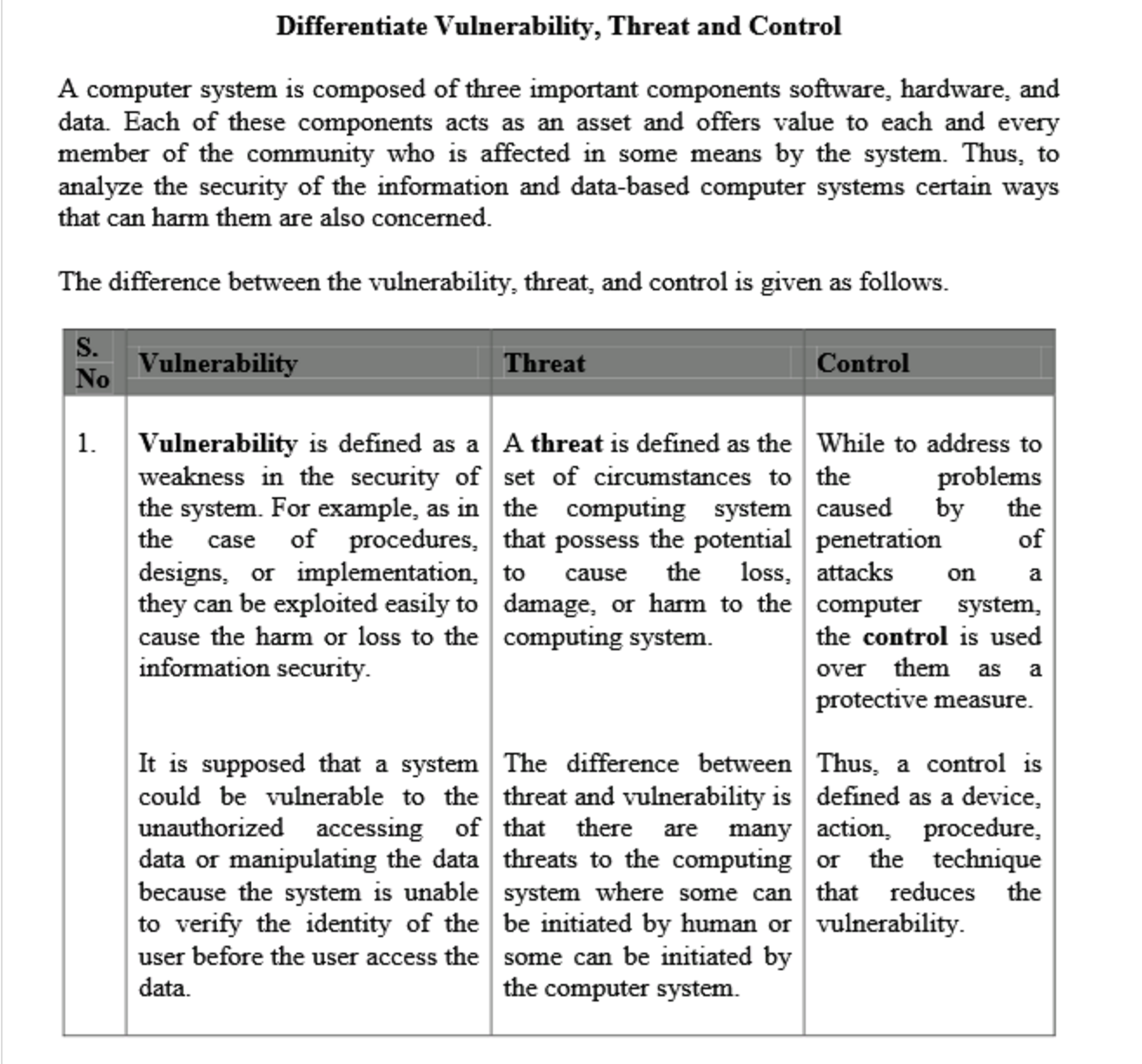
# CPS 633 – Chapter 1

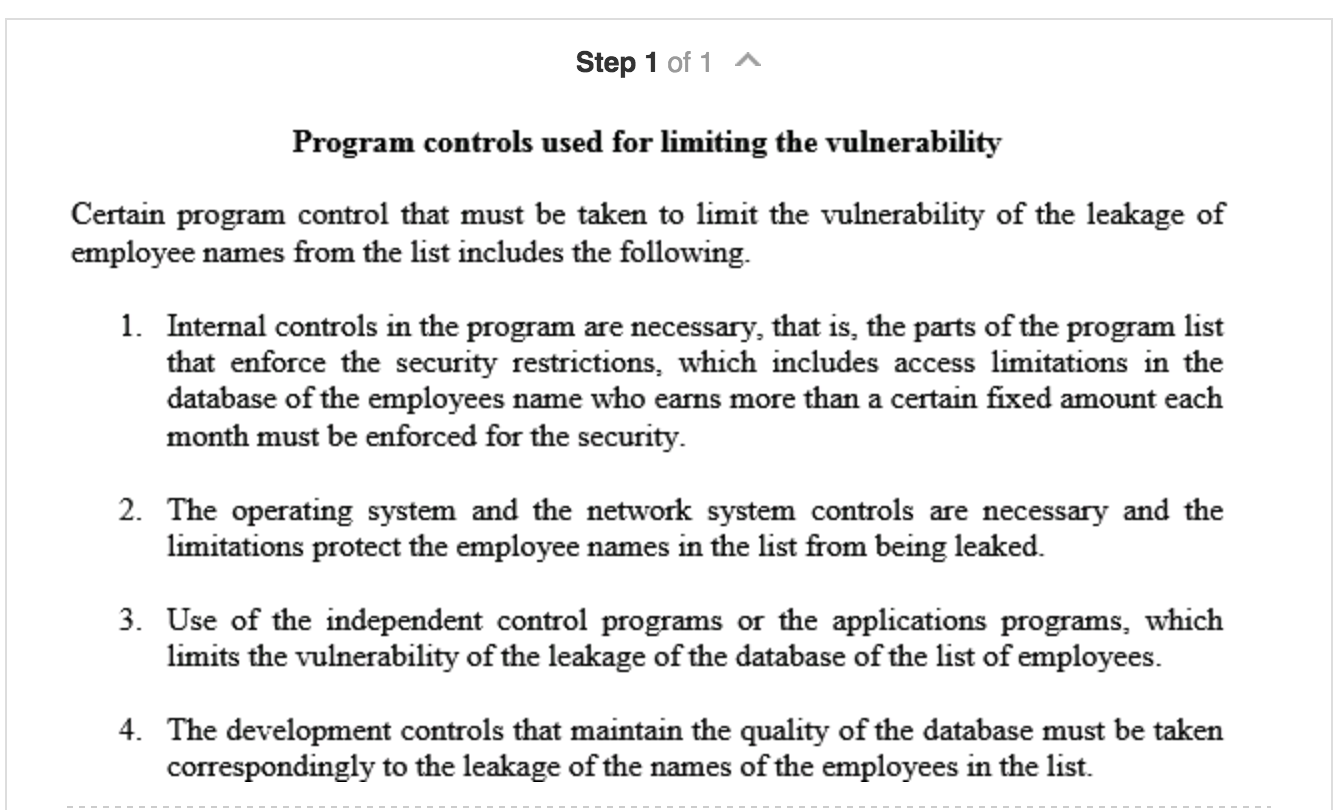
|  |  |  |
| --- | --- | --- |
|  |  |  |

1. Distinguish between vulnerability, threat, and control.

* Vulnerability – an aspect where there could be a threat, this means a flaw in the system. Where if it is exploded then the asset could be harmed.
* Threat – circumstance where the vulnerability can be exploded. (Attack is when someone of something – an subject actually tries to exploit that vulnerability)
* Control – the counter measure of the system, to protect again attack. For the situations where vulnerability can be exploited.  
  ^ So vulnerability – weakness in the security of the system. And threat is set of situation or happening that can potentially cause harm to the system. Or in other words exploit the vulnerability. Control – counter measure for the exploit of the vulnerability.

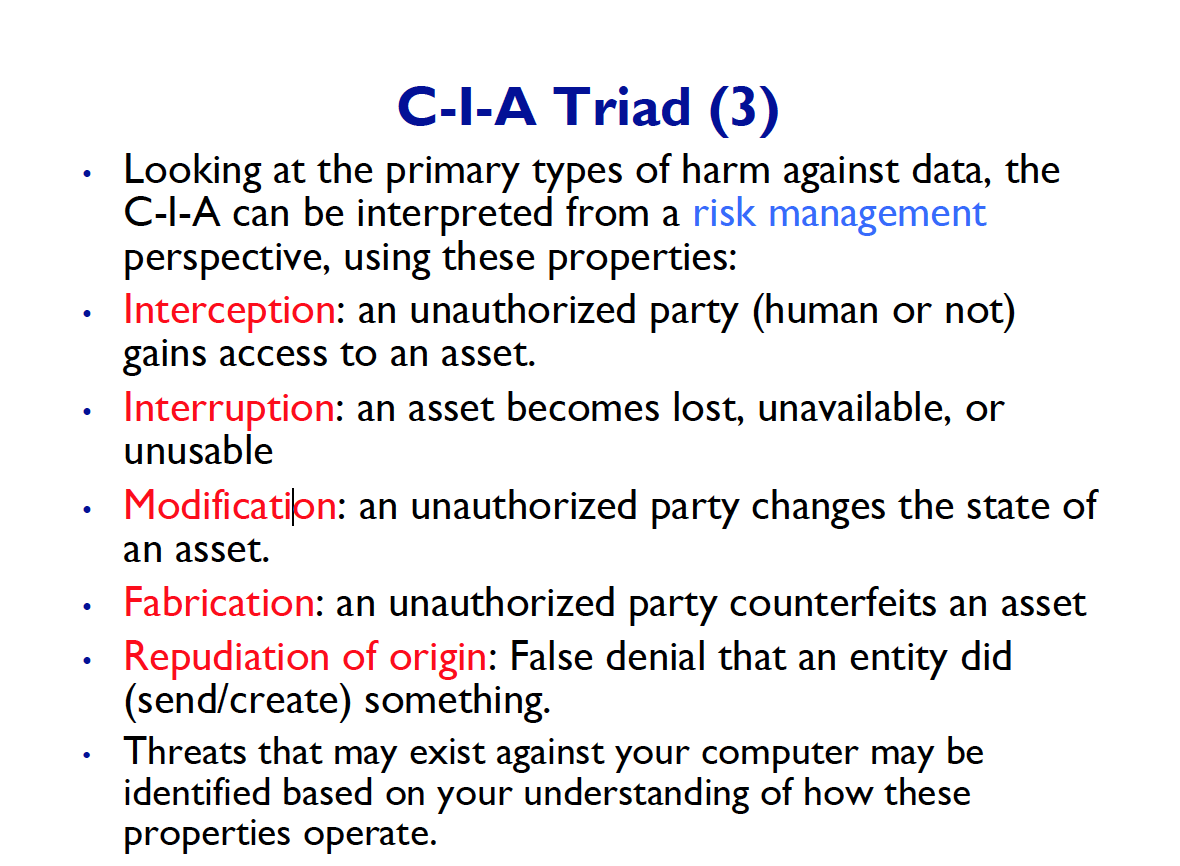
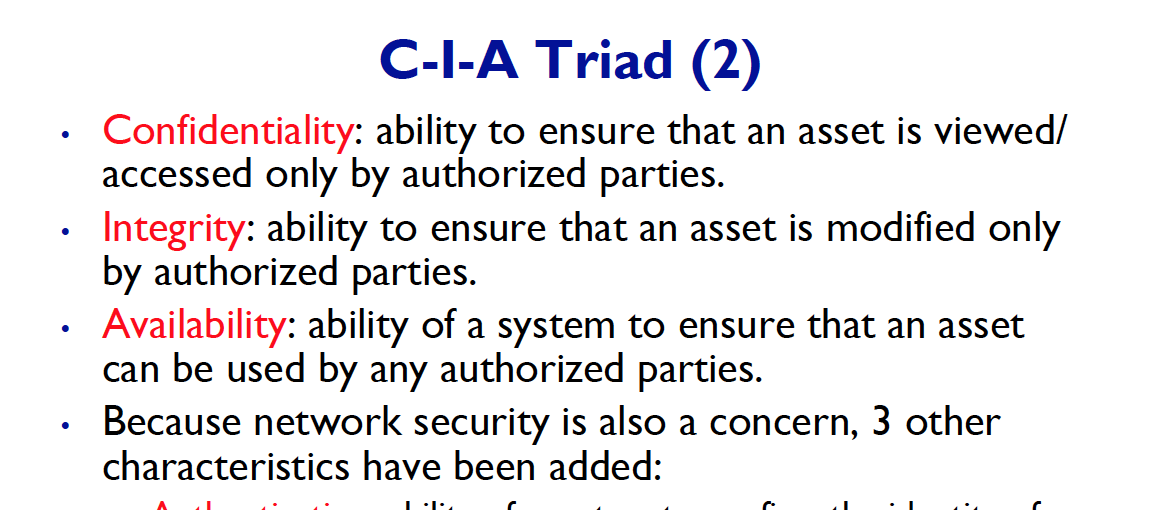
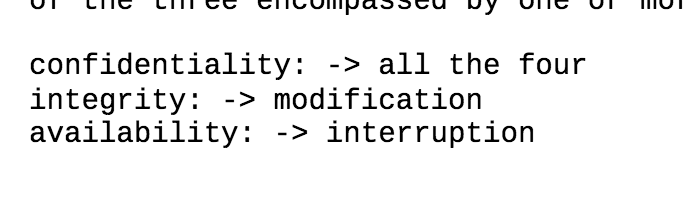
10. Suppose a program to print paychecks secretly leaks a list of names of employees

earning more than a certain amount each month. What controls could be instituted to limit the vulnerability of this leakage?

* One solution might be running the program on a machine where it is not connected to the internet. (By this way we can protect the confidentiality of the system, since only certain people who have physical access to the machine can see the output data.)   
  Or another way could be filtering the output result of the program. That deletes all of the leaked information as it gets generated.   
  So combining the topics that are going to be on lecture 2 3 4 and 5. One of the way in program security is confinement of a program. This way, we can limit the resources that the program have access to. (This case = database). Or using an independent control program can stop the leaking of the data.

11. Preserving confidentiality, integrity, and availability of data is a restatement of the concern over interruption, interception, modification, and fabrication. How do the first three concepts relate to the last four? That is, is any of the four equivalent to one or more of the three? Is one of the three encompassed (surround and have or hold within.) by one or more of the four?

- confidentiality – only authorized persons can access the data, integrity – is when only authorized person can modify the data. Finally, availability is when authorized person can access the data, whenever they please to access the data.

Interruption – is when the asset gets lost, interception – is when the asset is access by another authorized person while it is being transmitted from one host to another. Modification – is when un auth person changes the value of the asset, and fabrication is when a fake version of the data is created so – making a fake copy of an asset could be this.  
Interruption – violates availability, interception – violates confidentiality, modification – violate integrity, and fabrication – violates confidentiality.  
Please look at page,29 of lecture 1.  
  
So interception, interruption, modification, and fabrication – all of these matters are based upon confidentiality.   
Did not know that interruption does not get effected by the integrity, but make sense since the original data does not get modified.

13. Describe an example (other than the ones mentioned in this chapter) of data

whose confidentiality has a short timeliness, say, a day or less. Describe an example

of data whose confidentiality has a timeliness of more than a year.

- If the data is urgent medical data, it would have a short timeliness – since other doctors must access the data in order to treat the patient quickly.

If the data is personal SIN number then it would have timeliness of more than a year.