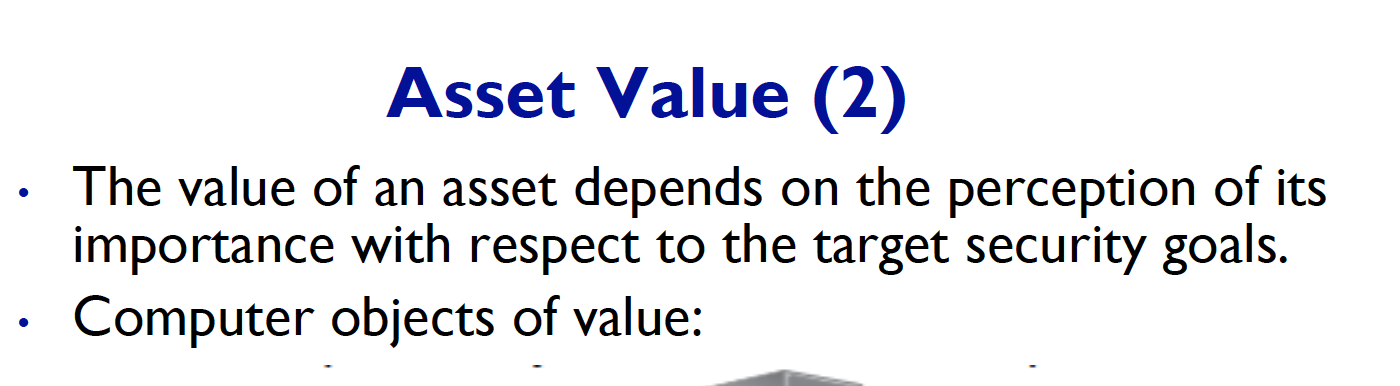
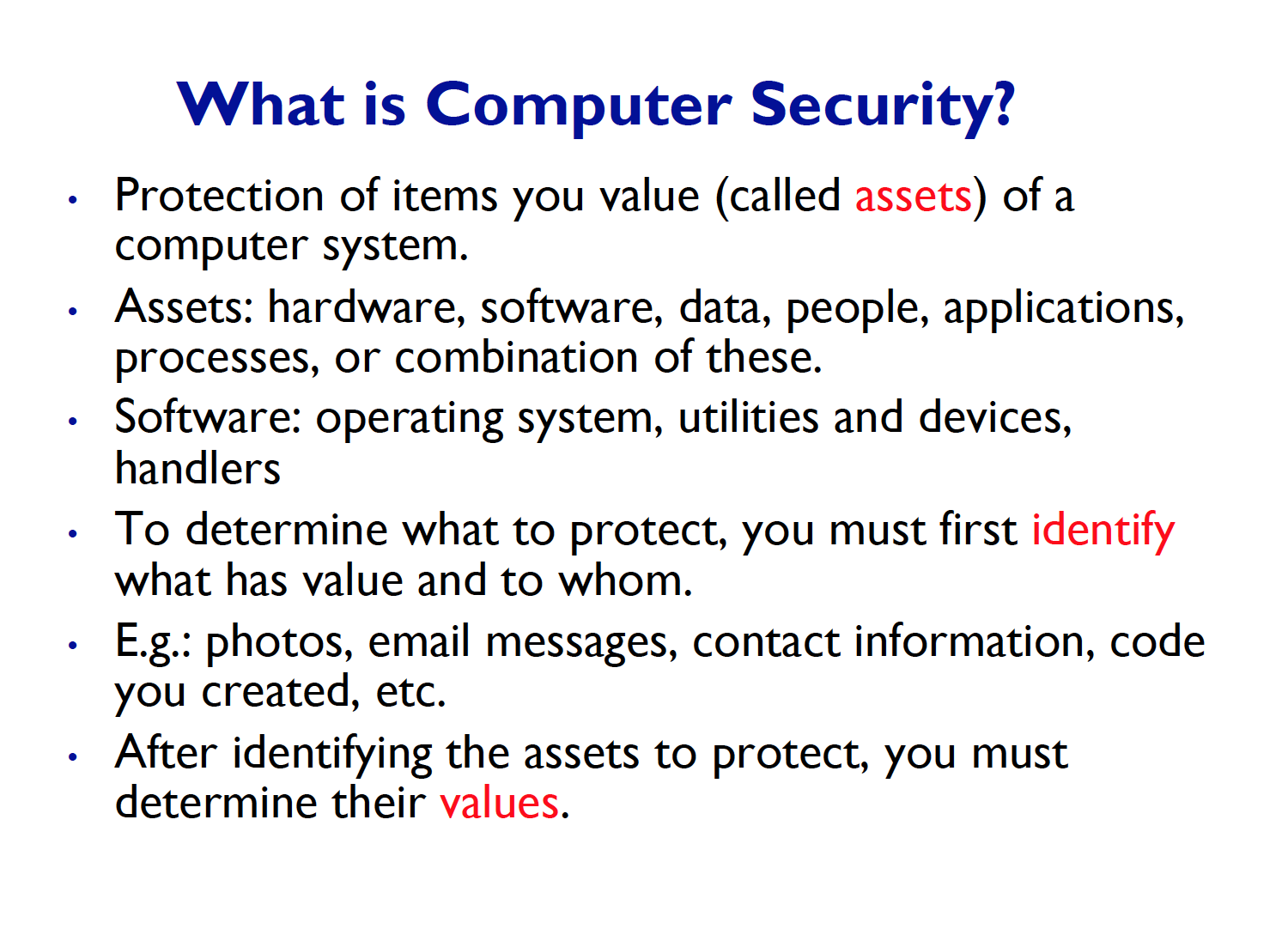
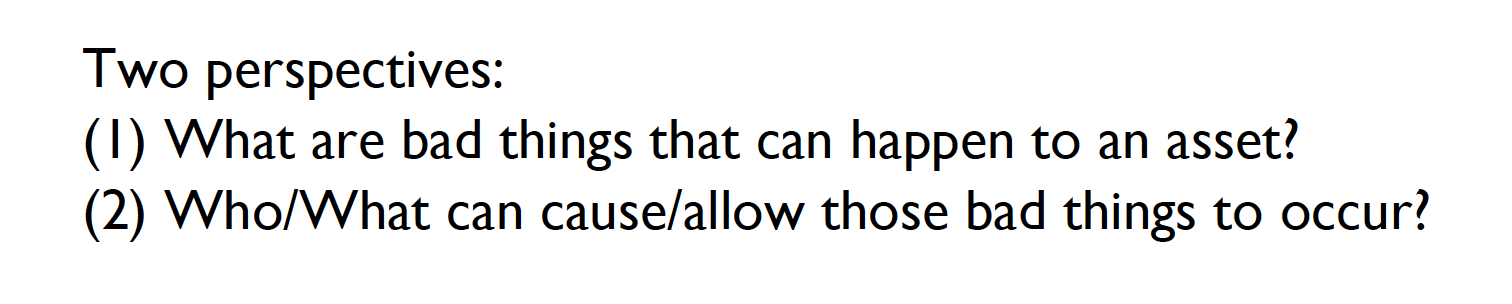
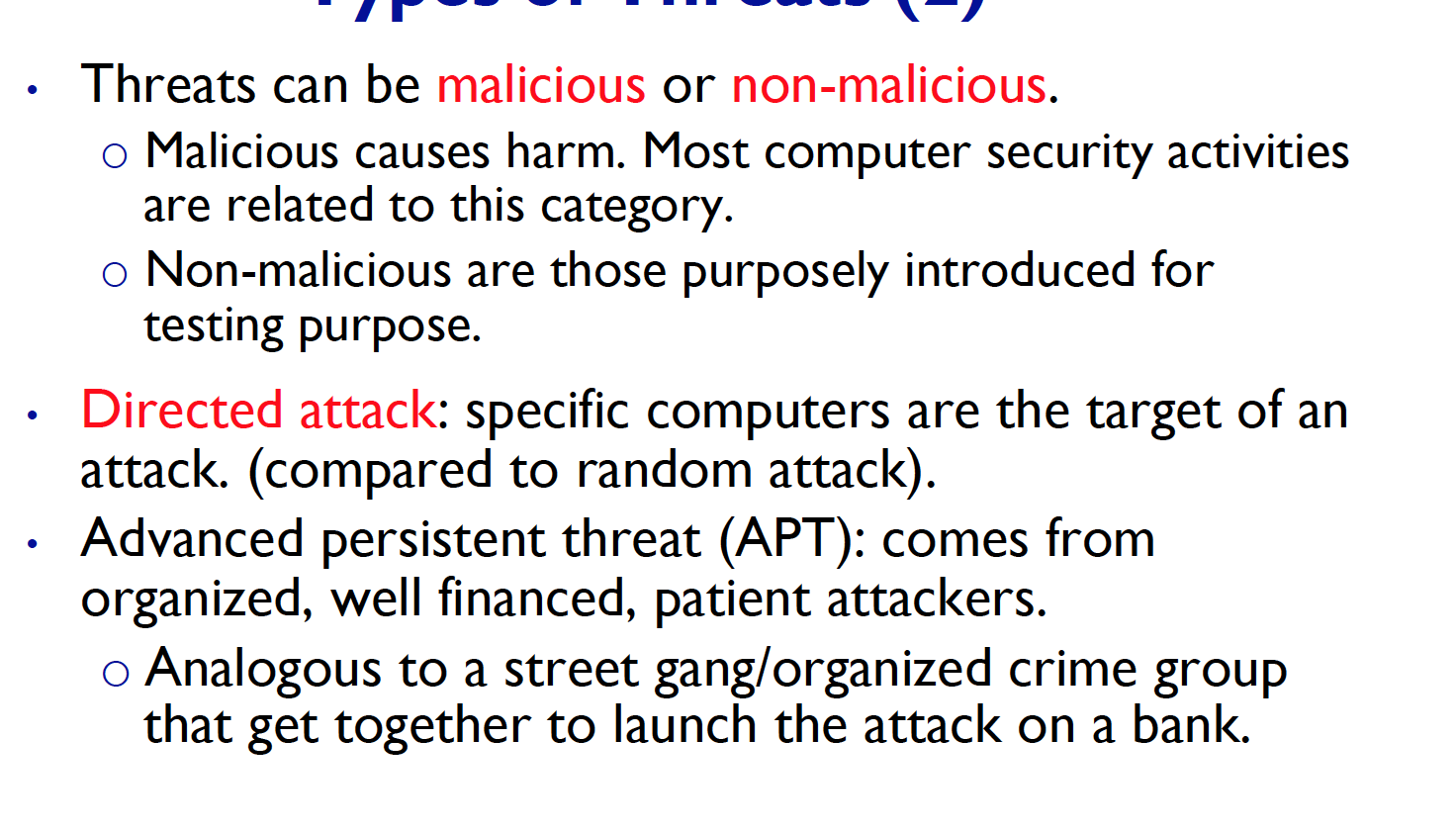
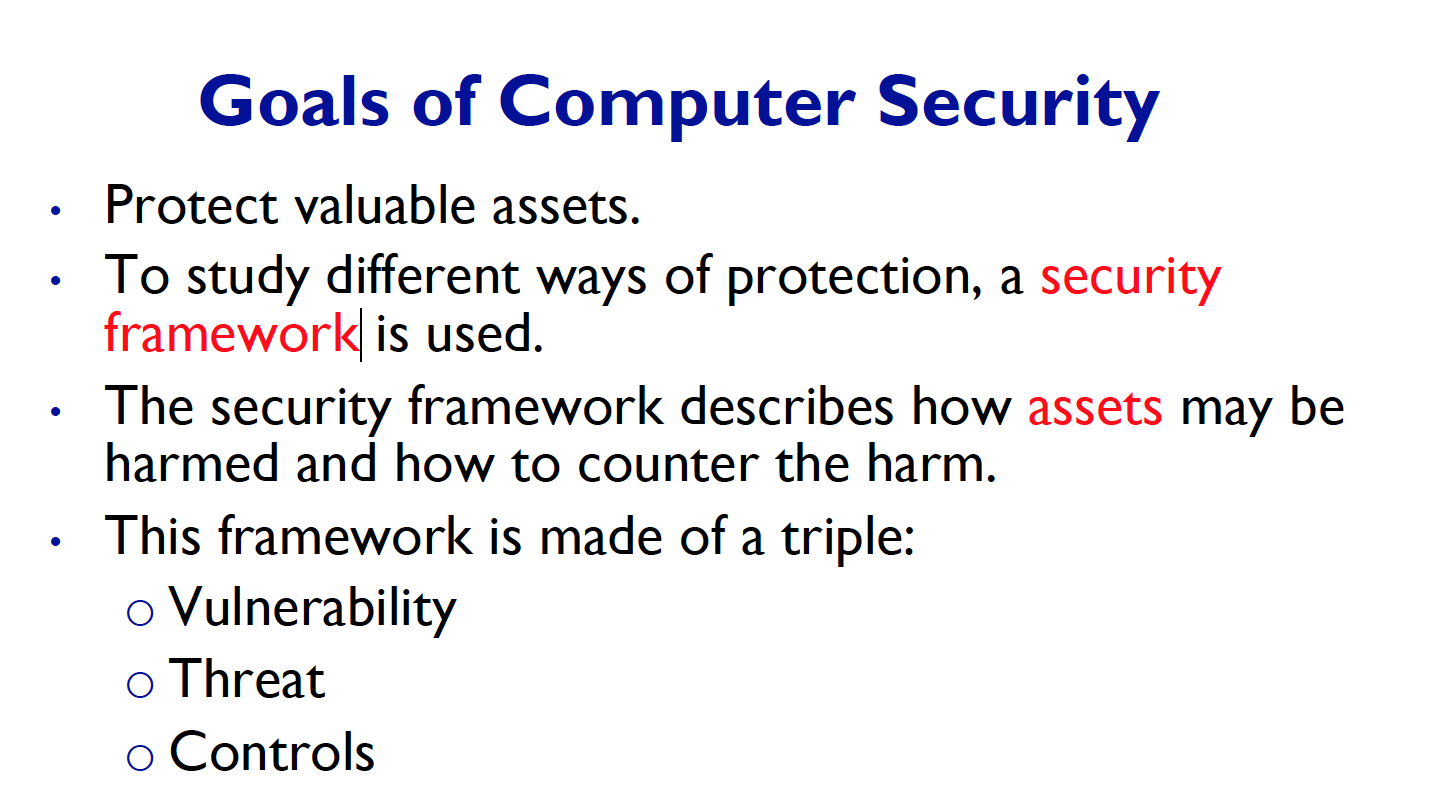
|  |  |  |
| --- | --- | --- |
|  |  | CPS 633 – note questions  Jae Duk Seo |

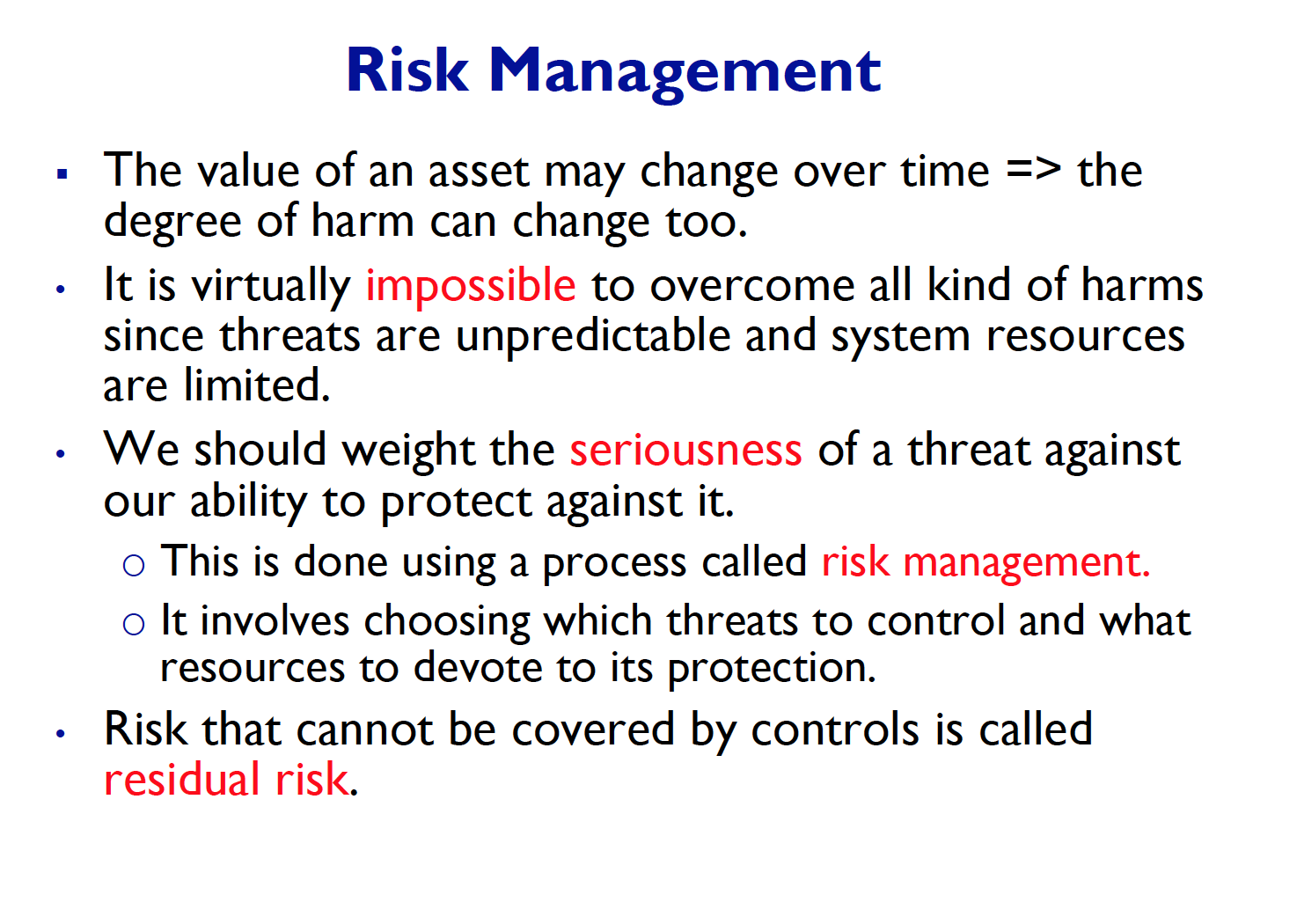
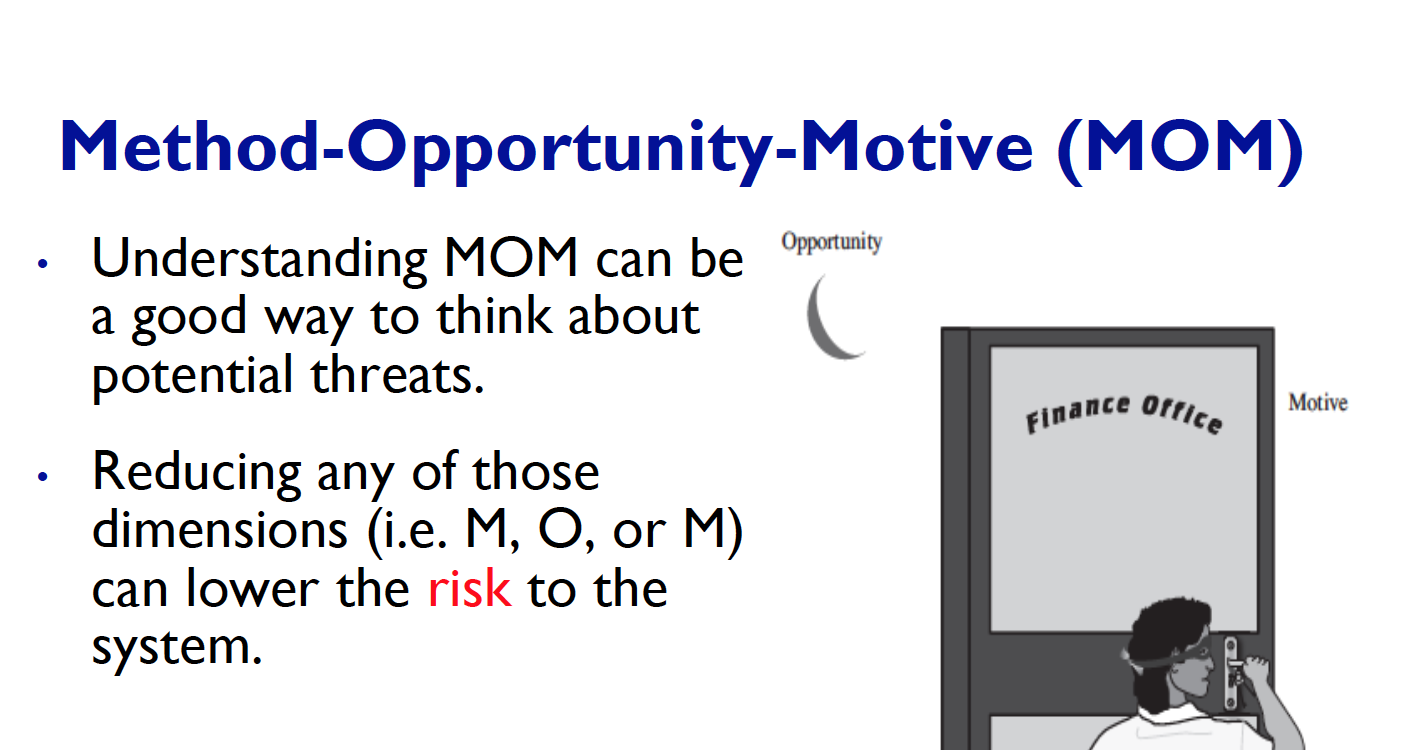
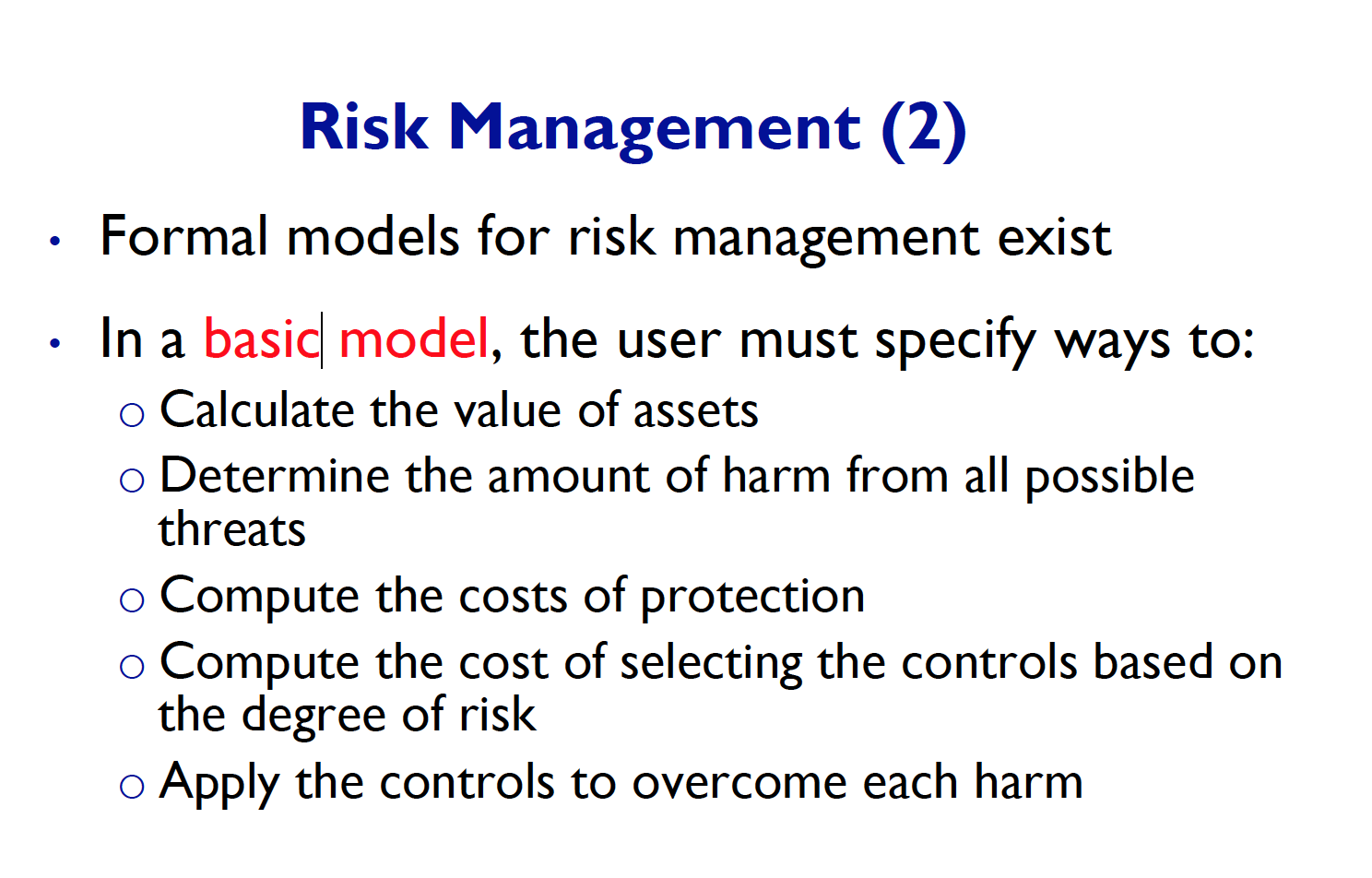
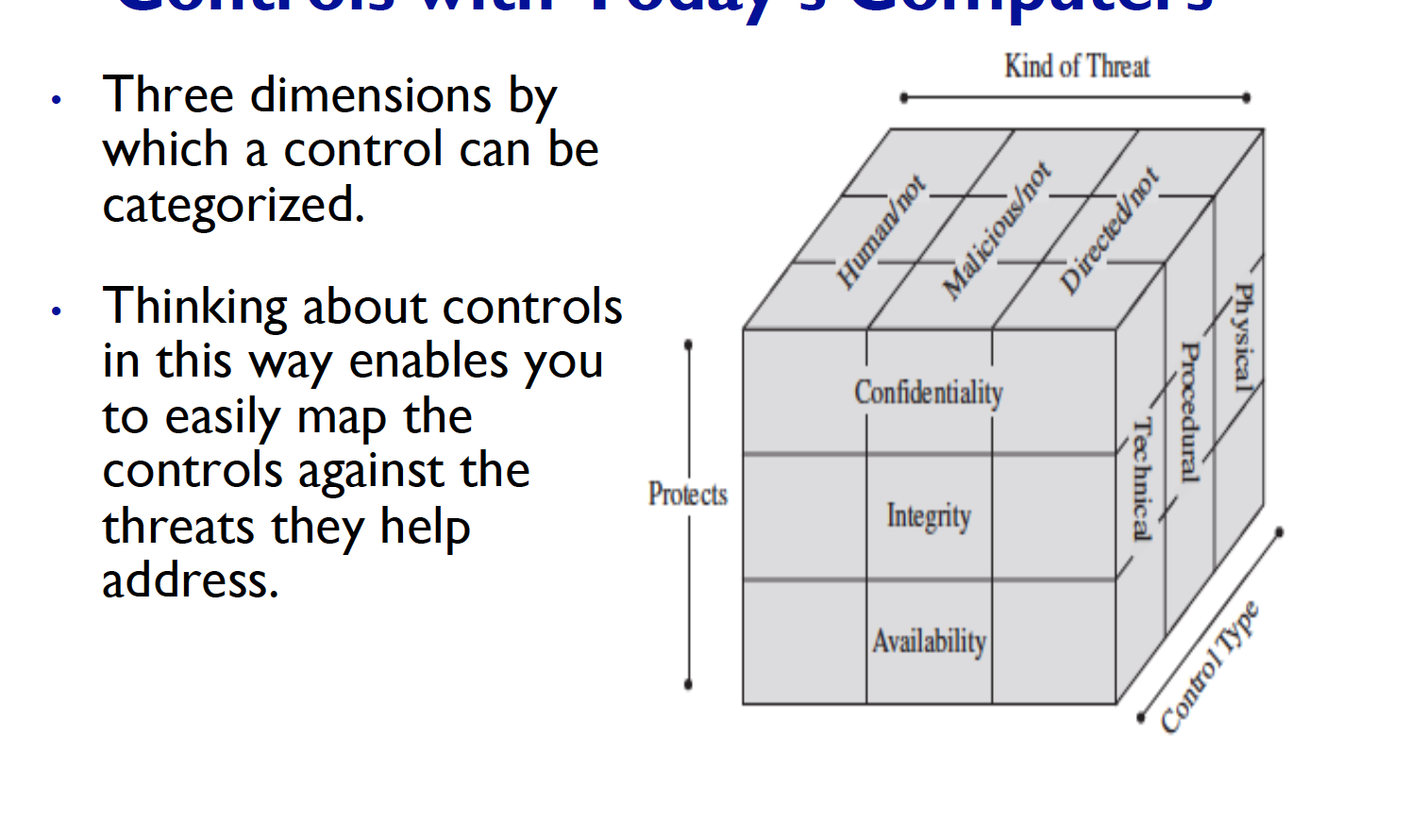
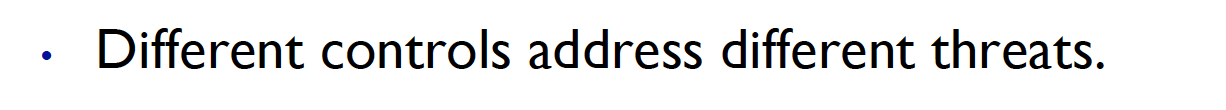
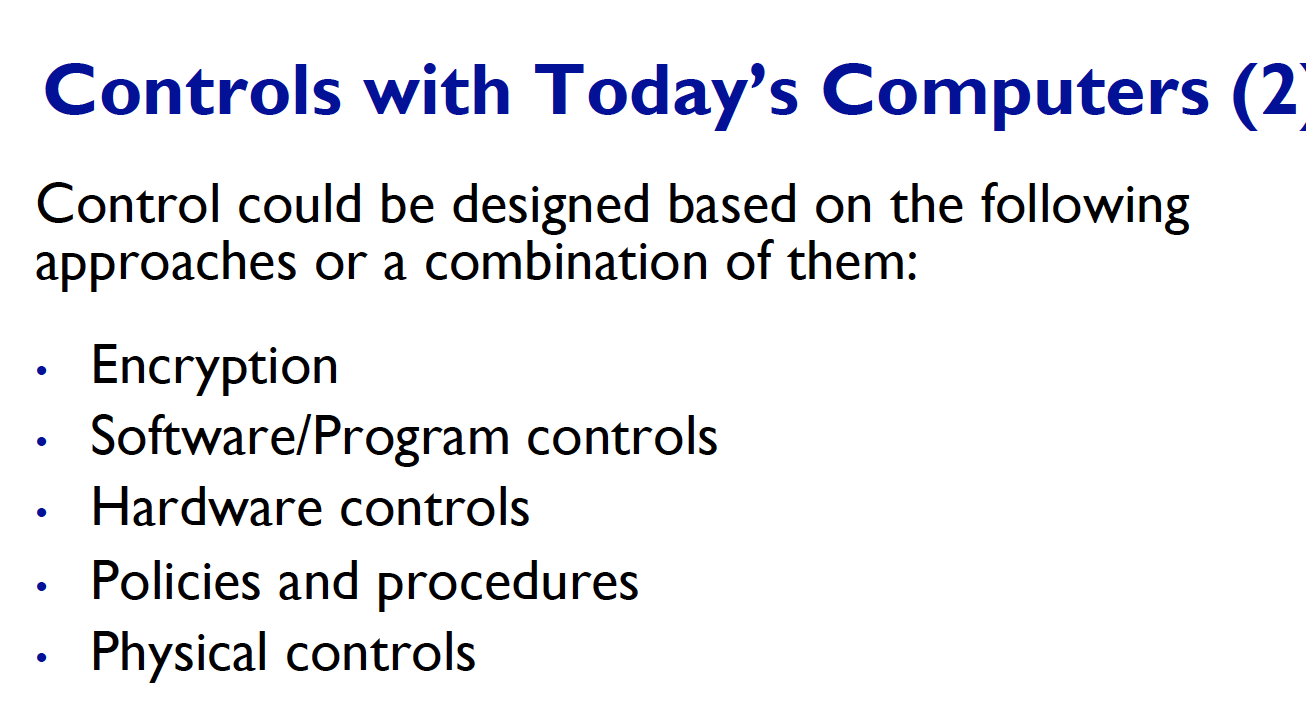
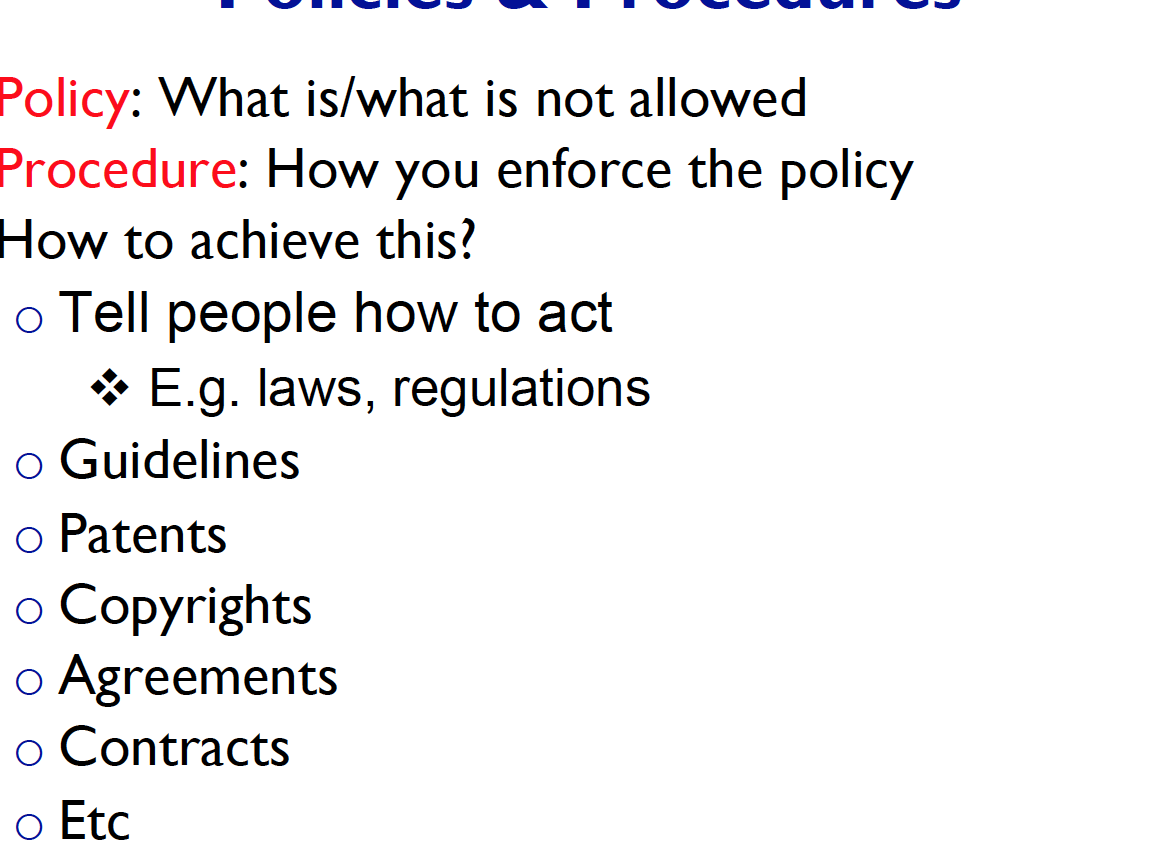
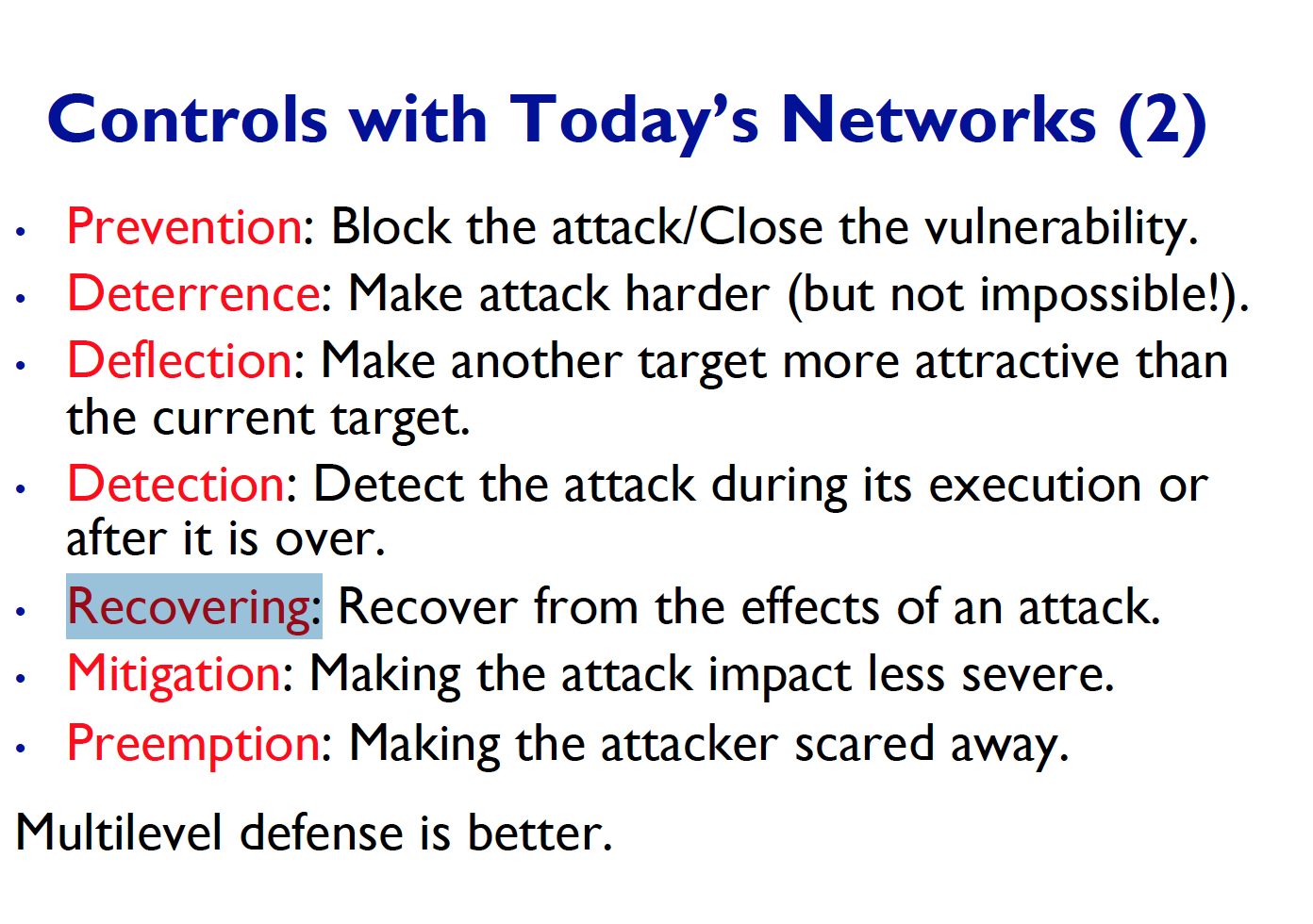
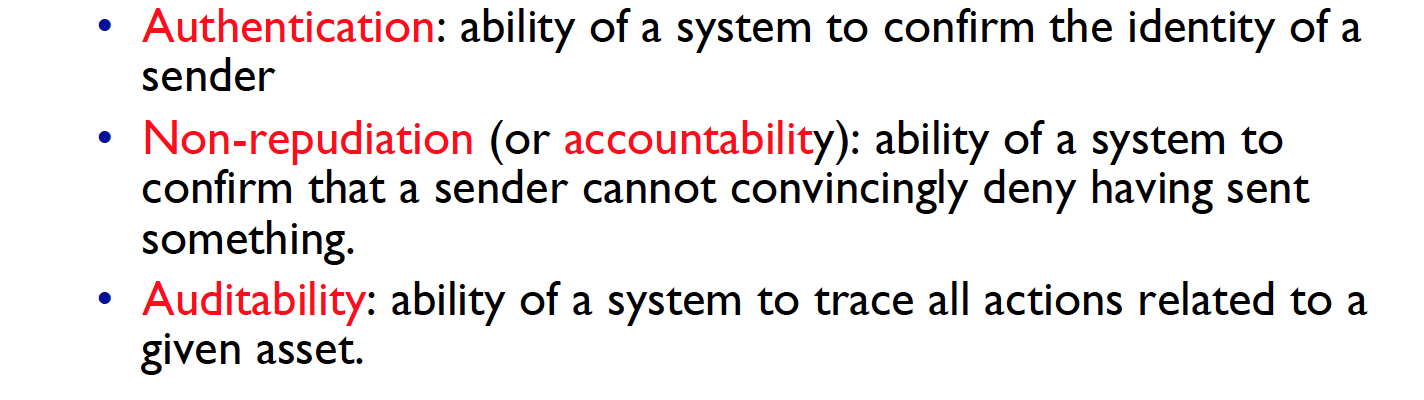
# Lecture 1 – intro to security

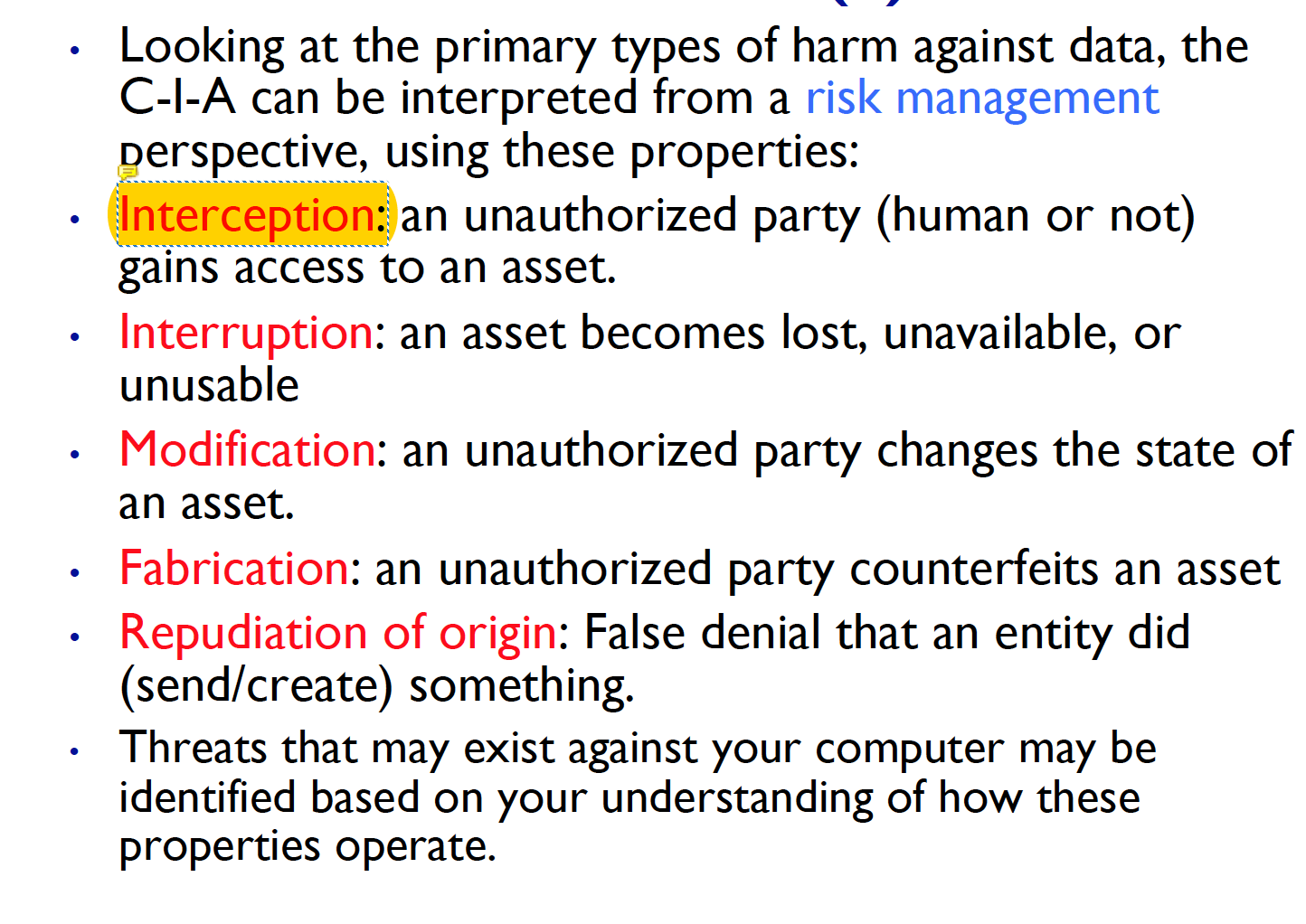
1. What is computer security and how can we determine a value of asset?
2. What are the 2 question that we must ask when detecting potential harm to an asset.
3. When do we do non – malicious attack? Difference between the direct attack and advance persistent attack?
4. Why do we use framework and what 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 1 – soltions

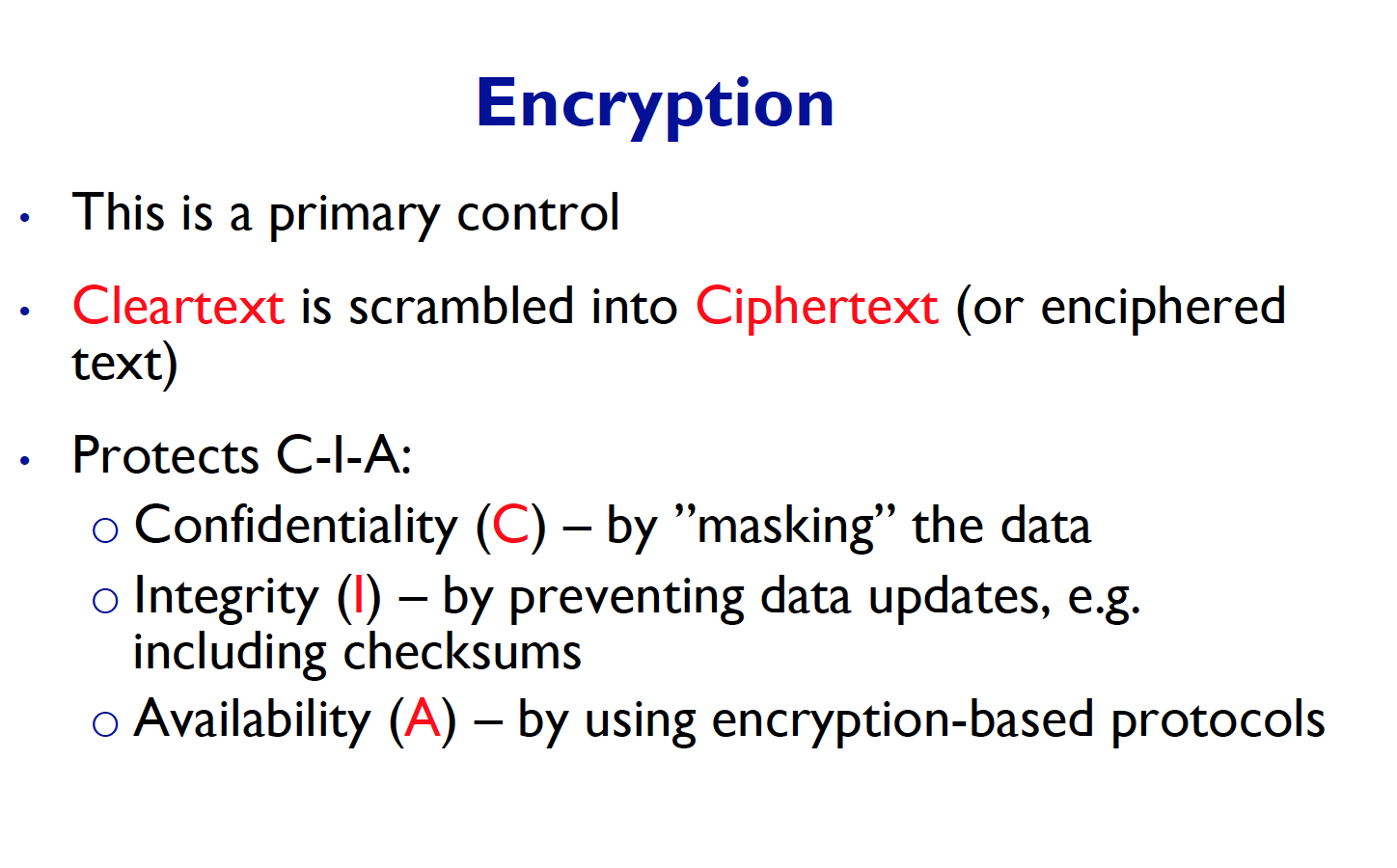
1. Computer security is protection of assets (such as h/w, s/w and even people). And the way to determine a value depends on the perspective of the security implementer. The assets can be anything, such as h/w and s/w or other things. But there value can be determined in anyway – depends on the perception of the security goal and targeted security goals.
2. Who are the ones that can cause harm to our asset and in what way can they cause harm to our assets. What can they cause.
3. We perfume non – malicious attacks when we wish to test the system out, for example a developer might want to find a security flaw in their program. And they will tried to hack their own system. Or try to penetrate their own program.   
   Also, difference between the direct attack and Advance persistent attack is, APT – are more well prepared and funded attacks, sometimes even countries sponsor them. 
4. Why do we use framework and what does framework provide us?

* We use security frame works since, they describe us on how the assets can be attacked in what way. Also, tells us how to counter attack those attacks.

1. What 3 things attacker need? And what is risk management used for, also what is residual risk?  
   - MOM – motivation, opportunity, and method. We use risk management to weight which assets to protect and which one to leave out. (Setting priories) Take into account, the seriousness of the attack and our ability to protect it. The risk that we cannot control is residual risk.
2. What are some functions of basic risk management module?   
   - Some functionality of the basic risk management includes calculating the value of an asset. This is what we talked about in the above, questions. When determining the value of an asset, we can use the risk management module to estimate the value of an asset. 
3. In today’s computer security what are the control aspect exist?   
   - Protect (confidentiality, integrity, availability)   
   - Kind of threat (non/malicious, human or not, in/direct)  
   - Control Type (physical, procedural, technical)
4. Why do we need to know different type of threat? What does it help us?  
   - Different kind of threats need different kind of control to counter measure them. So better knowledge regarding the type of threats will lead to better protection.
5. There are major five method of computer security – name all of them.  
   - Encryption – Converting plaintext into cipher text (CIA)  
   - S/W control – Operating System, Third party software  
   - H/W control – Locks Cables etc…  
   - Policy/Procedure – Policy (What people can/cannot do) procedure (how to achieve that policy.)  
   - Physical Control – human guards, wall, locks etc….  
   For detail info about each, please look at until page 24.
6. What are policies and procedures – how can we achieve this? Example of physical control?   
   - policy – what people can/cannot do  
   - procedure – how to achieve that policy  
   - we can achieve this policy, by emailing the people in the company, or morning announcements. 
7. Today control network has 7 elements that are important to security. Name and describe each of them.  
   - Deterrence – Harder Attack  
   - Detect – Recognize that there is an attack happening  
   - Deflect – Set a dummy target, easier target  
   - Preemption – Scare the attackers away.  
   - Prevent – Block the attack, before it even happens. Close vulnerability.   
   - Mitigation – the degree of the harm cause by the attack is less  
   - Recovering – After the attack, come back to the original state.
8. In network security three more aspect of security gets added, what are these and describe them.   
   - Authentication – The system need to verify the user, there are two steps process of verification. Identification and Authentication. (We will tackle this matter in another question)  
   - Non – repudiation – When a user sent another user (such as packet) some kind of information the sender cannot deny the fact that they have send it.  
   - Auditability – Ability for the system to traceback all of the operation that have happened to the system. 
9. Interception, modification, fabrication, repudiation of origin, and interception – describe each of them.

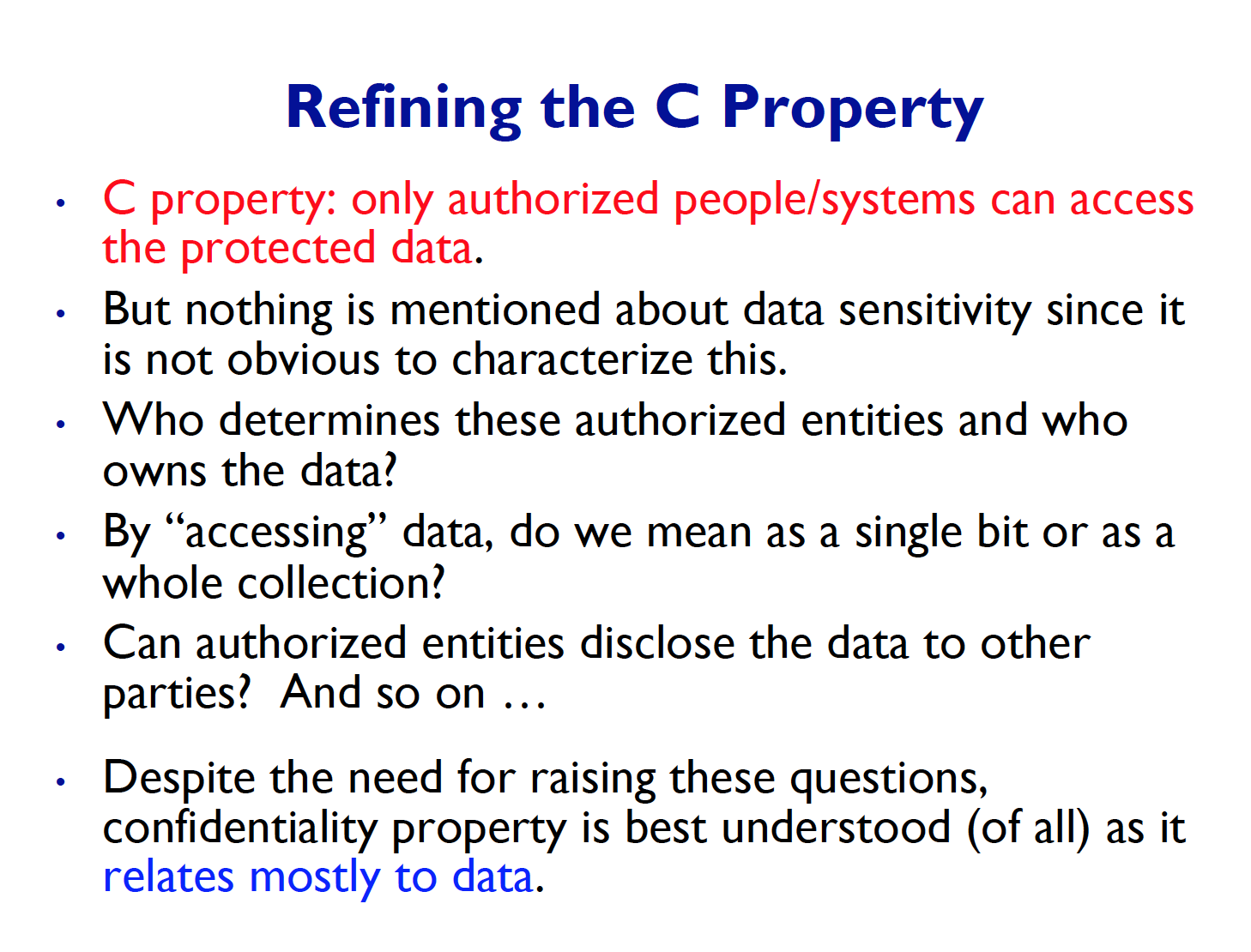
* Interception – when unauth user access a private data
* Modification – when unauth entity change the content of data.
* Fabrication – when unauth entity, fakes the data
* Repudiation of Origin – when entity deny the falsely deny something.
* Interruption – when an asset becomes lost and now not available anymore.
* JUST GOOD TO KNOW - Interception - break C
* Interruption - break C and A (Since unavailable of the asset.)
* Modification - break C and I
* Fabrication - break C
* Interception – break C

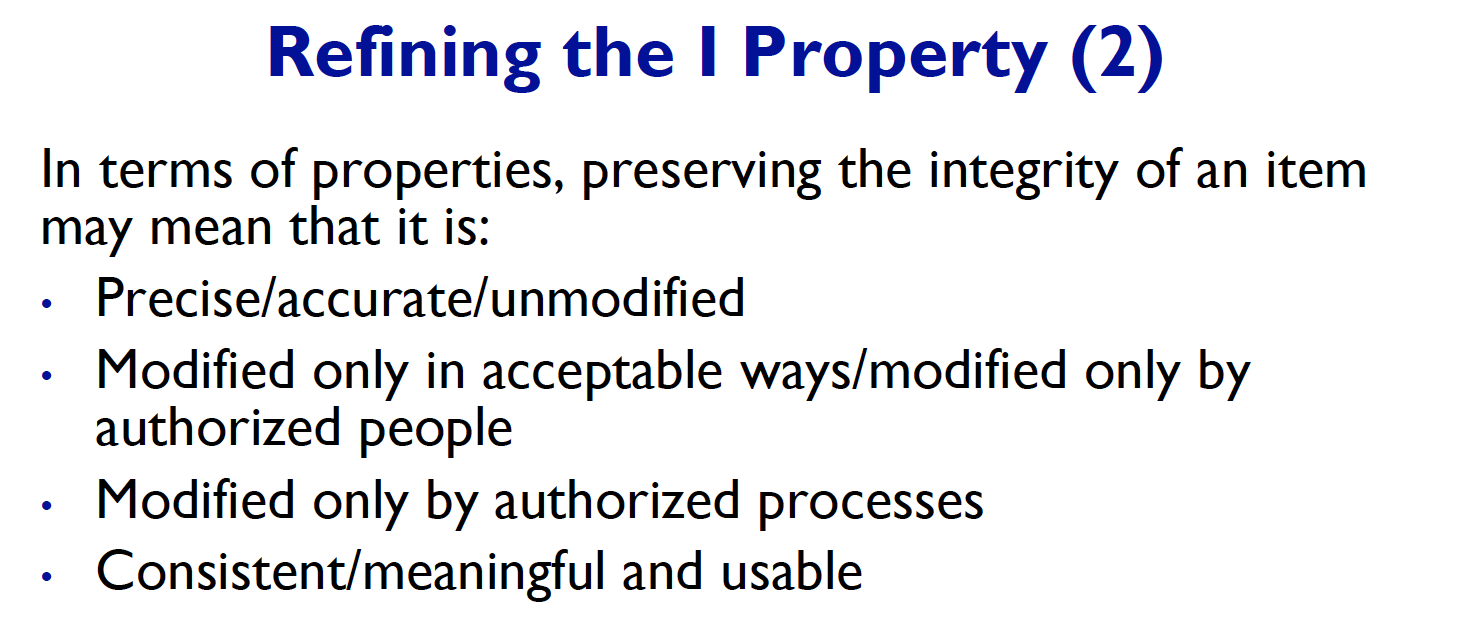
1. Example of encryption, s/w control, h/w control. What does encryption protect among CIA triad?

* Encryption protects every CIA triad.
* Confidentiality – since only auth users can access the content of data
* Integrity – hash function to perform checksums, block unauth change of data.
* Availability – encryption based protocols, so the communication among host are safe. Assets such as server is protected from DOS attacks. 
* S/W (OS) H/W (Smart Cards)

1. When does each CIA fail? (Interception, modification, fabrication etc…)

* Confidentiality – fails when unauth user intercepts the data, or interrupts the data
* Integrity – fails when unauth modify the data or fabricate the data
* Availability – fails when Interruption happens

1. Why do we need to redefine the C property?  
   - We need to redefine the C property since, the border line of confidentiality is not a clean cut. Such as when an unauth person acces 1 bit of data, is it same as accessing all of the data? Who gives these authorizations to access the datas? 
2. Example of integrity failures, and can the meaning of integrity change?

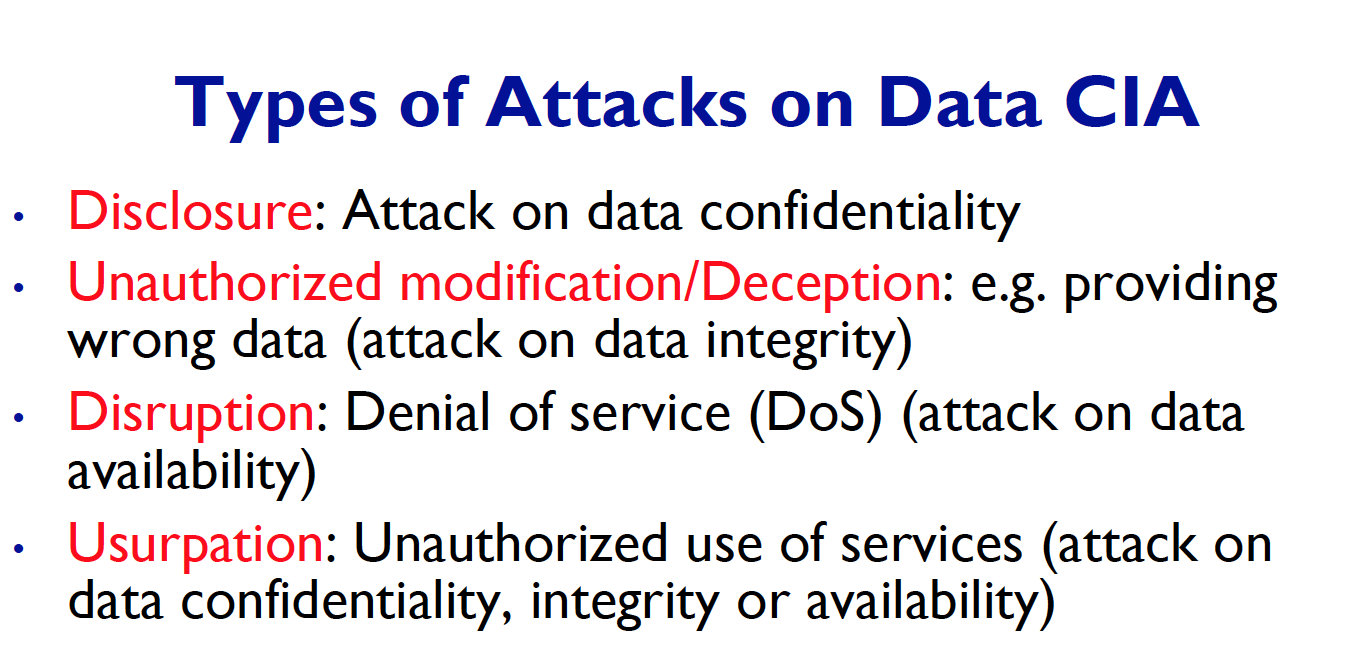
* When a hacker changes the content of the document, this could be considered as failure of integrity.
* Finally, the meaning of integrity changes over the perspective of the security goal.

1. For A property, when do we say that A have failed?

- Example of the availability failure is interruption. (Rather than interception – this is when unauth user snoop the data, rather change the content of the data.)

- when an asset is not available at the time when the user wants to access / use the data. This could also be situation such as a process not giving up the resource, a dead lock happening can also be a case when availability failes.

1. What are some attacks on CIA? – Example of each attack and tell which among the CIA triad have failed.

* 

1. Four principal of computer security, name them and describe them.

* 