# Possible FInal Questions – cps 633 + Jo Mak Questions

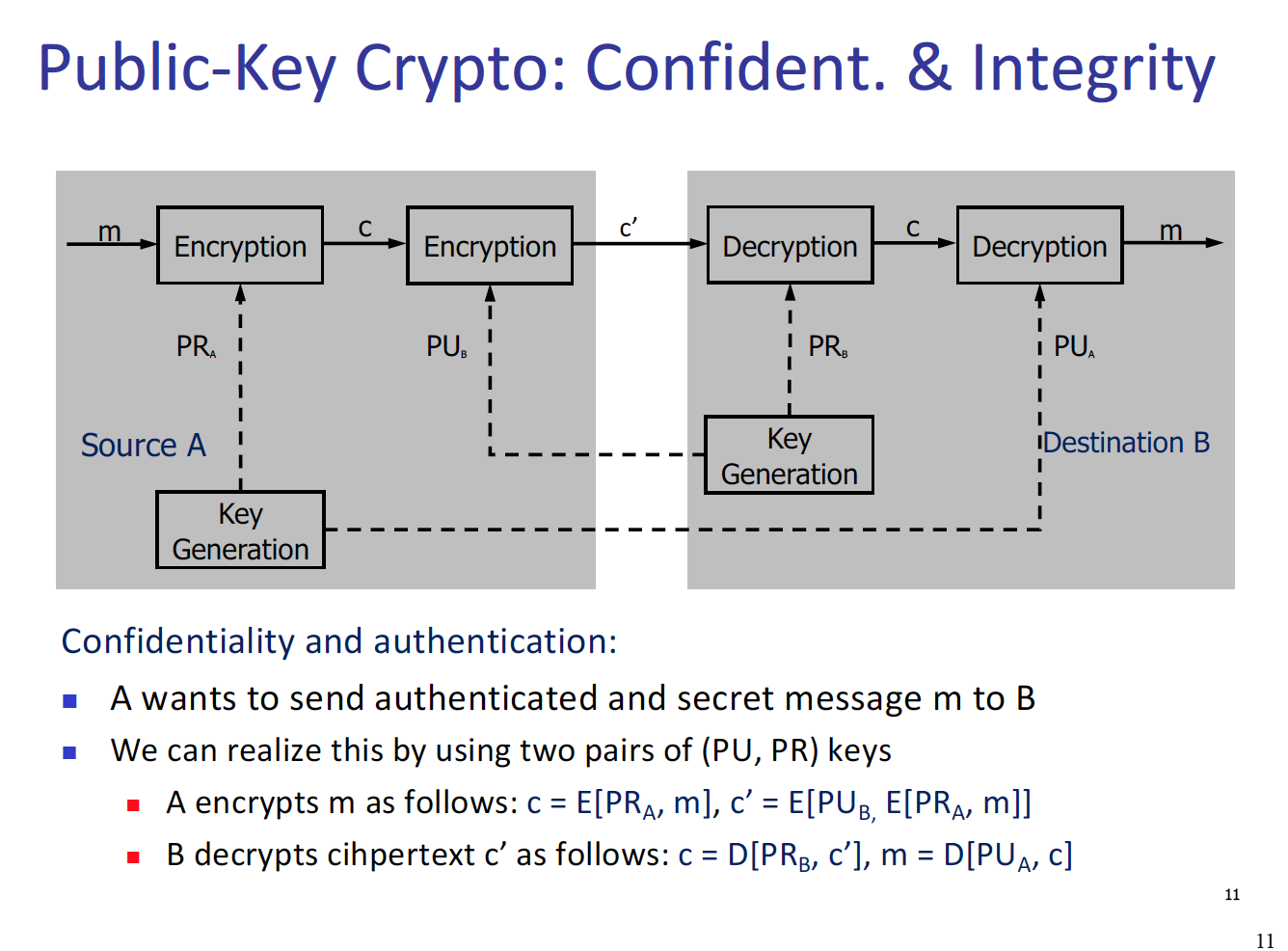
1. **The test will consists exclusively of Multiple Choice Questions (MCQs). These**

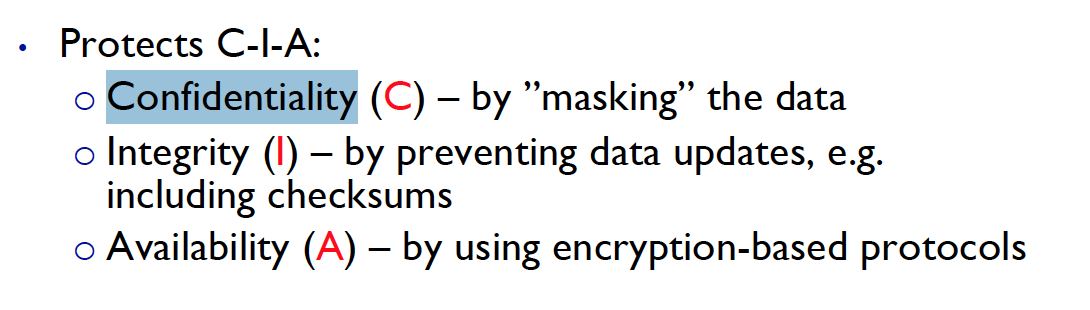
**questions will be related to your understanding of the various concepts learned**

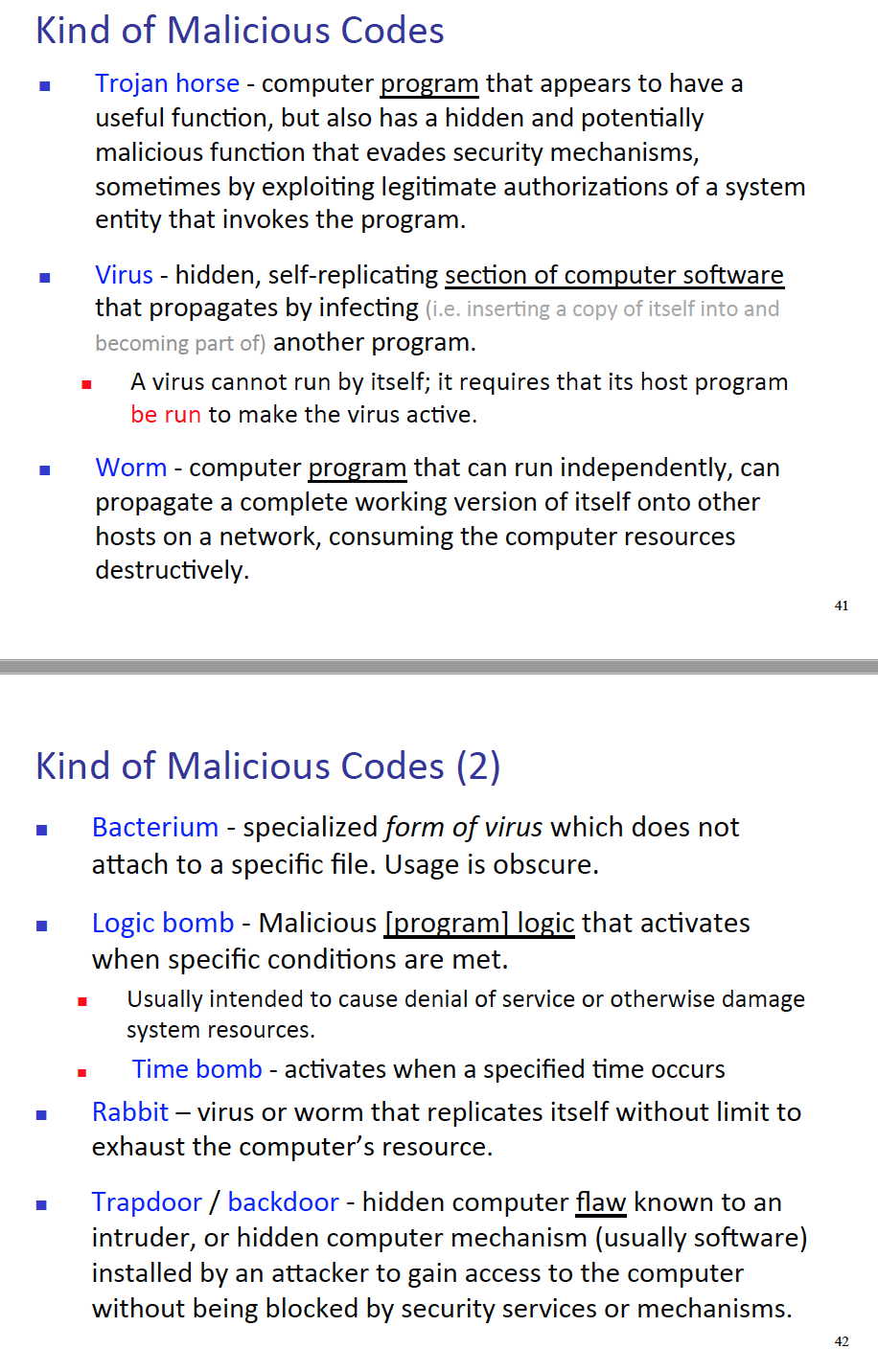
**in class.   
  
As an example, a scenario can be described which involves the use of**

**cryptosystem to share a key between two parties. The steps to realize such**

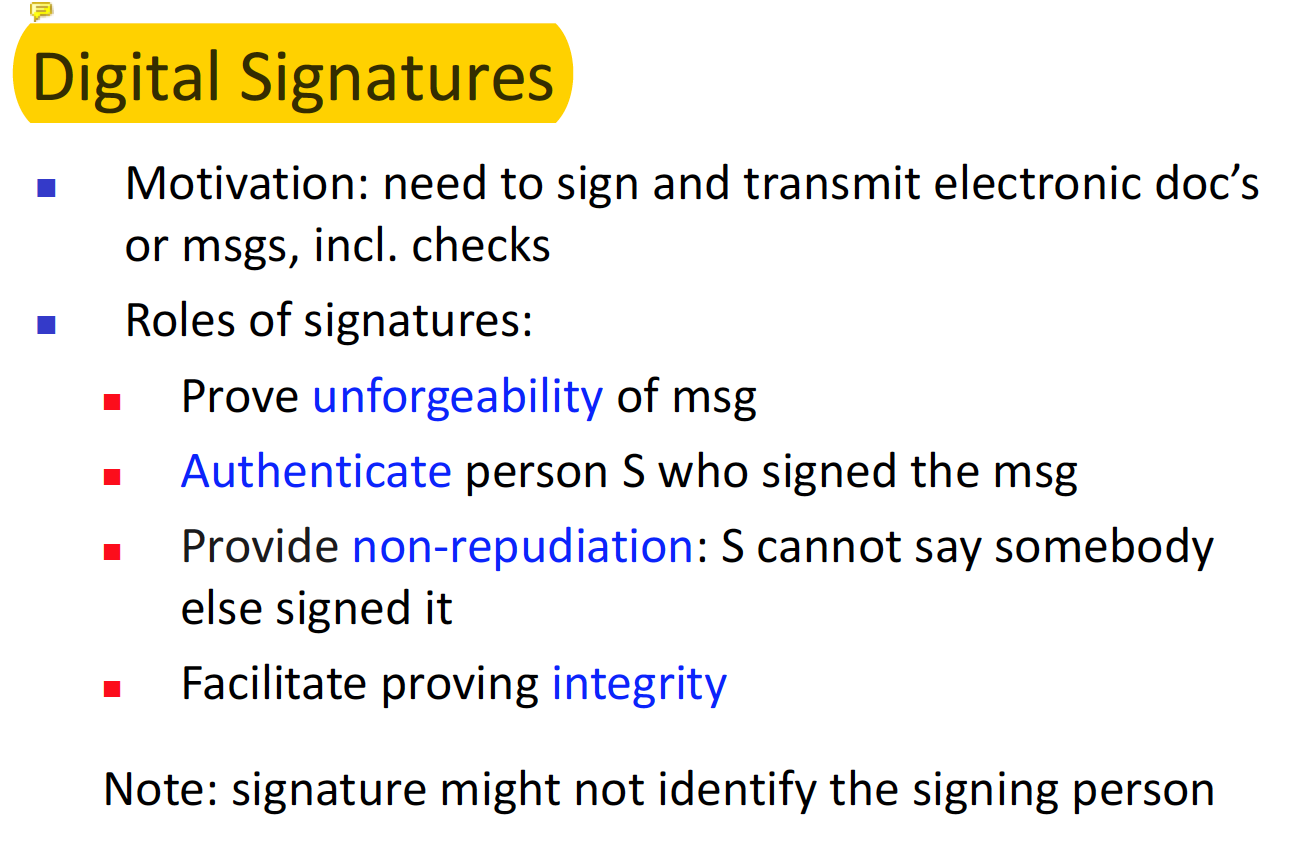
**communication can be given but with a missing step, and you can be asked to**

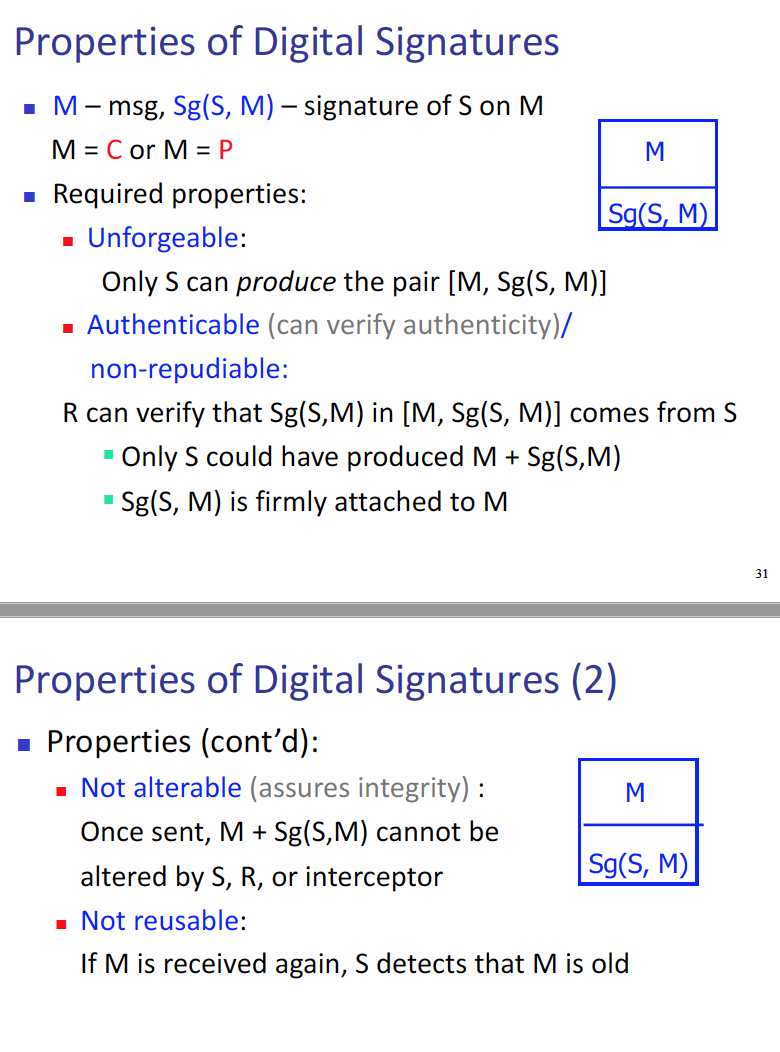
**clarify the missing step.** – Jae: This is covered in lecture 4 PPT, on shared encryption keys.  
- I am going to cover PKE, in this section. There is 4 steps to public key encryption   
(A symmetric encryption) - We will assume sender is A, receiver is B.1. A encrypts plain text P with their private key   
2. A again encrypts the cipher with B’s public Key.  
3. B receives the cipher text by A, and decrypt the first layer with B’s private key.  
4. Finally, fully decrypts the message with A’s public key to get the plain text.  


**Another example is a scenario describing a situation for which you need to provide your own opinion with respect to a targeted objective and on your own judgement.**– Jae: LOL, I believe this question is heavily based on the either violation of CIA. – Highly believe that this question will be in a format where we are given a scenario and we need to use our own judgment to figure out, which of CIA have been violated.  
- I think it is best to review the definitions of CIA and do some practice questions regarding different scenario where each of the characteristics are violated.

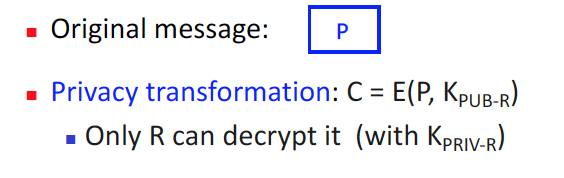
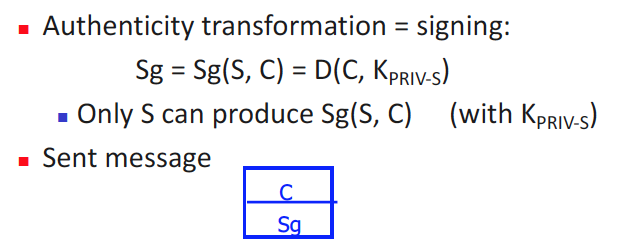
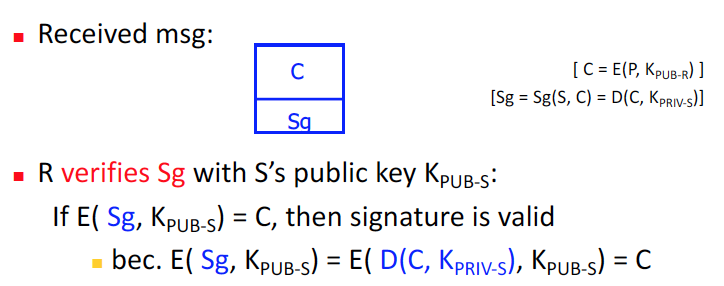
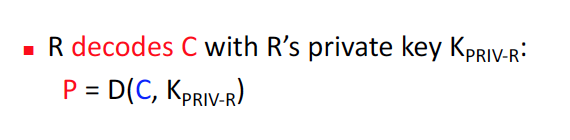
**2. Study the various types of malicious codes and how they act.**- There are couple of malicious codes these codes are written with purpose to harm the system, or exploit the flaws of a program.

**3. Study how message authentication and/or digital signatures can be used for authentication purpose. – Jae: This is covered in, lecture 4.**

- Let’s review what authentication or digital signatures are.   
My understanding of digital signatures is very like signatures. When two companies work with each other, usually upper management comes in play. And it becomes obvious that we need mechanism to ensure that each document is approved by the CEO, so we get their signature. This concept can be applied to digital signature.

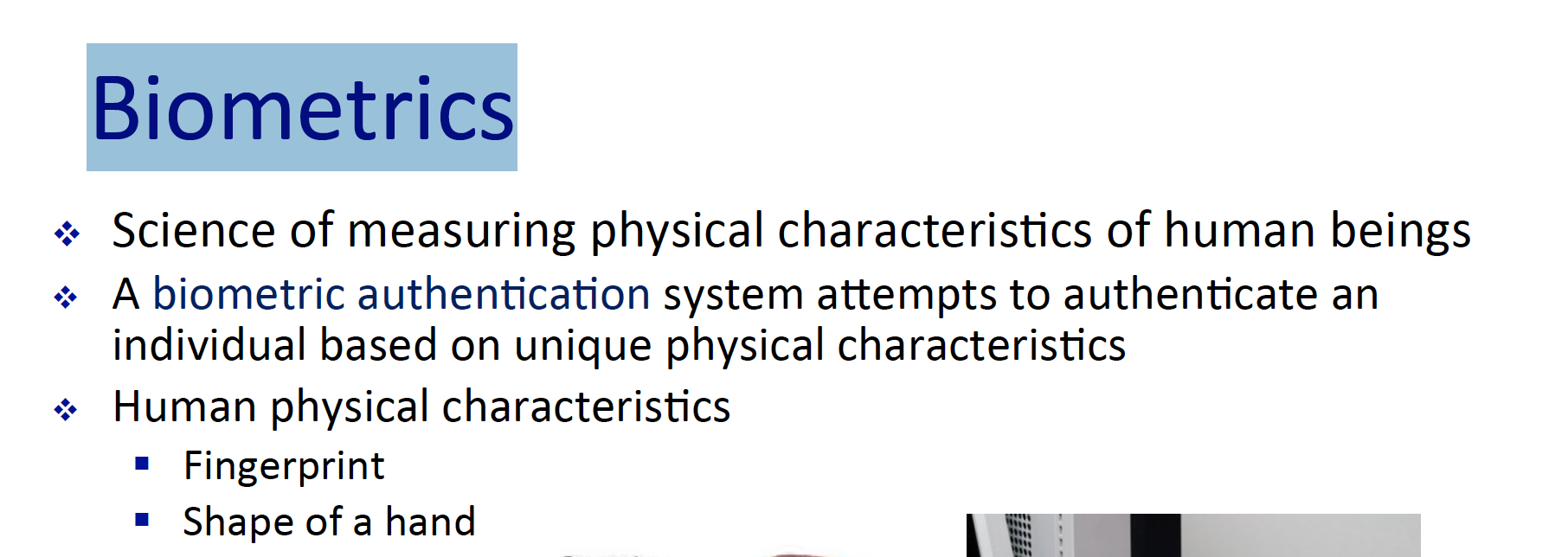
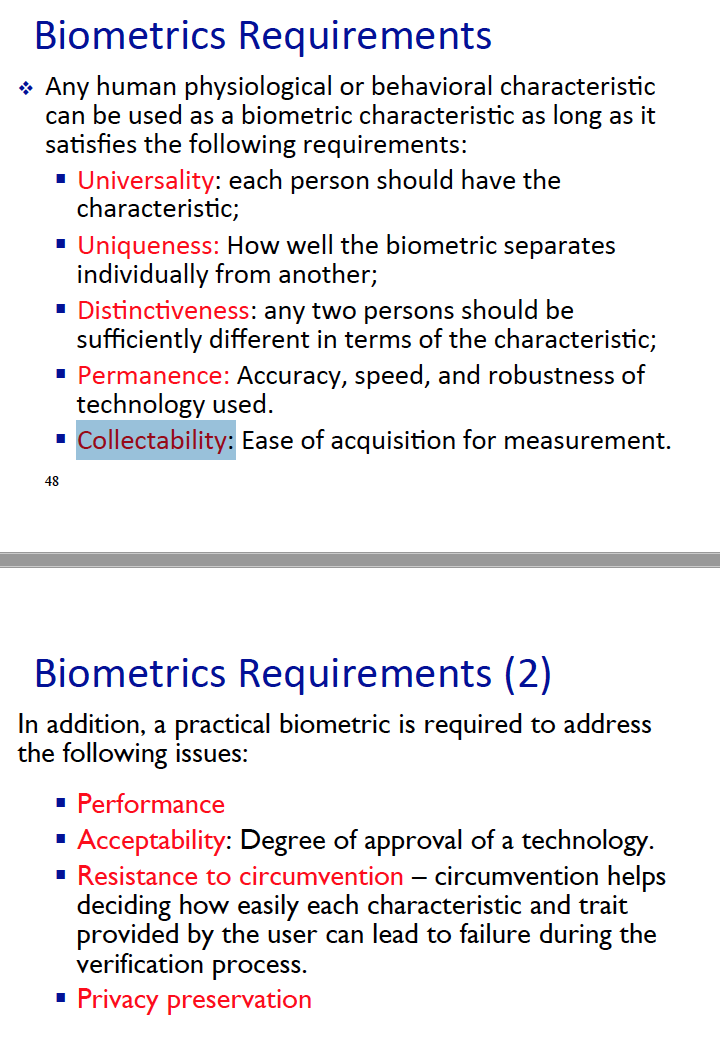
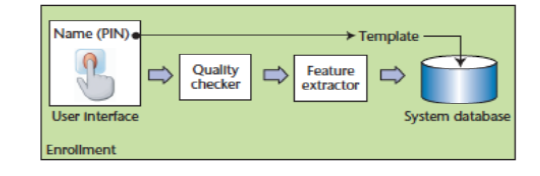
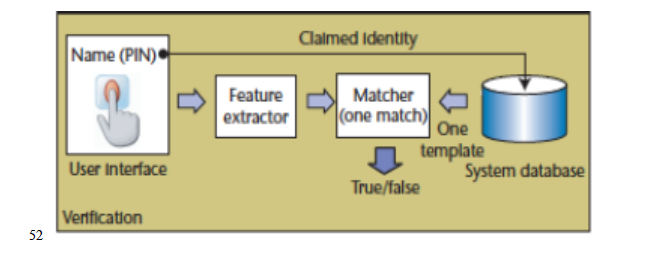
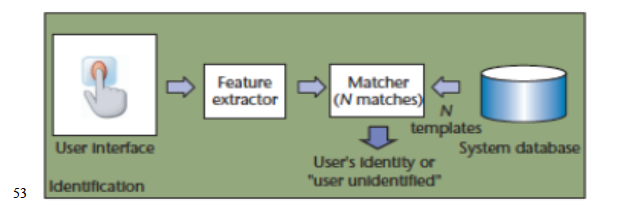
Digital Signature without PKE - very basic step  
1. Send have message p.  
2. Sign that message with the function Sg 

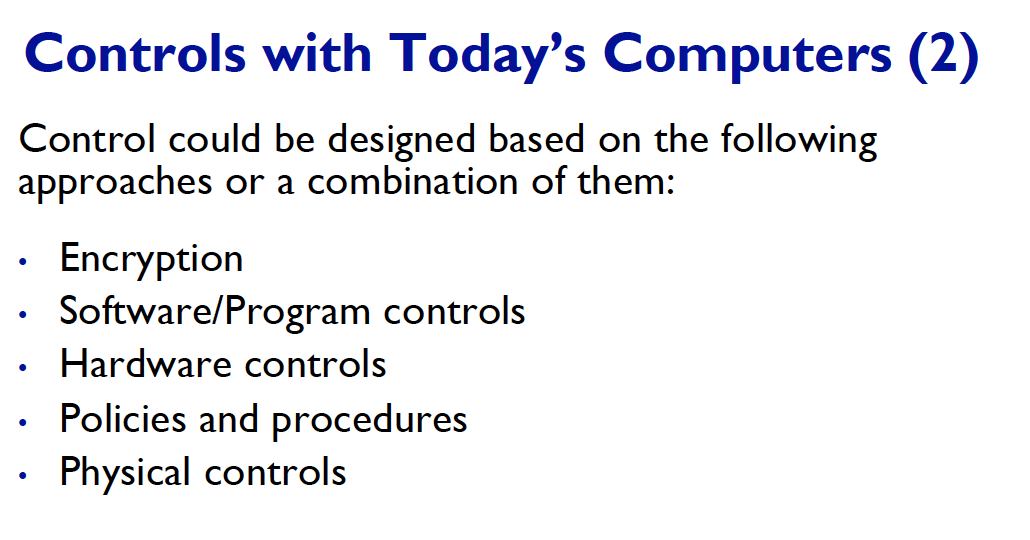
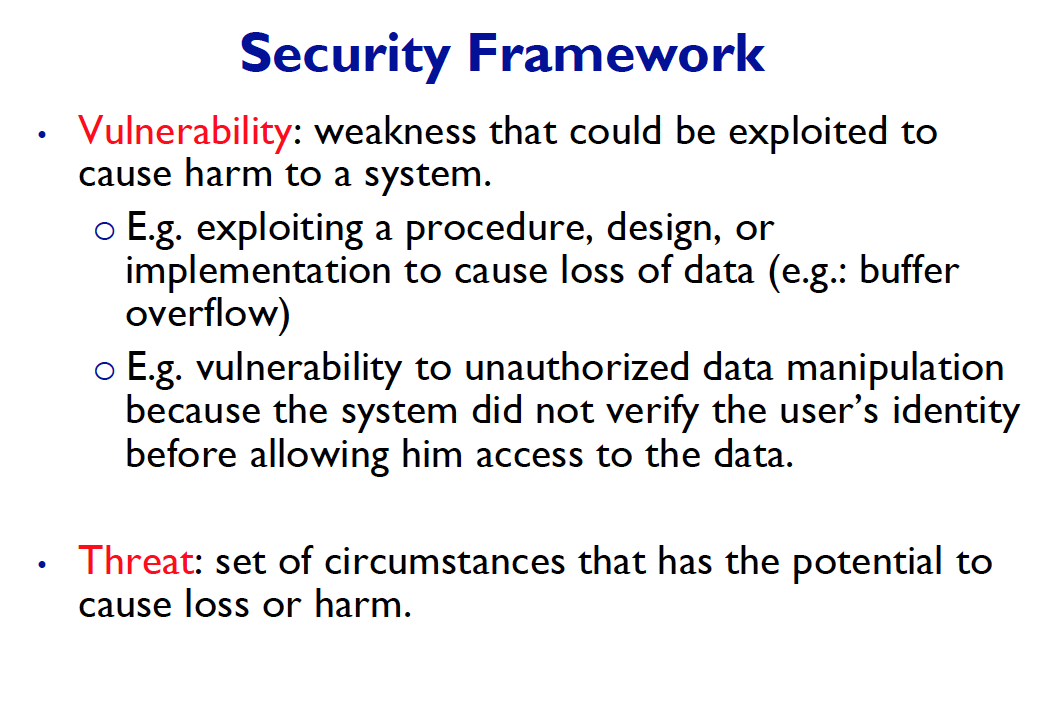
Digital Signature with PKE – there are four steps for this process

1. Sender encrypts the data with receivers public key.
2. Sender decrypts that cipher with it’s own private key. (THIS IS SIGNIING!)
3. Receiver encrypts the received message with public key of sender – this validates the message was sent by the SENDER – AUTHENTICATION.
4. Receiver decrypts the message with their private key to get the plain text 
5. **Learn about design principles that apply to protection mechanisms, i..e   
   Economy of mechanism,   
   Fail-safe defaults,   
   Complete mediation,   
   Separation of privilege,   
   Least privilege, and   
   Psychological acceptability. – Jae: This is covered in lecture 5.**

* It looks like there are six examples. Unfortunately, there is only incomplete mediation in the ppt. ( I will come back to this question)

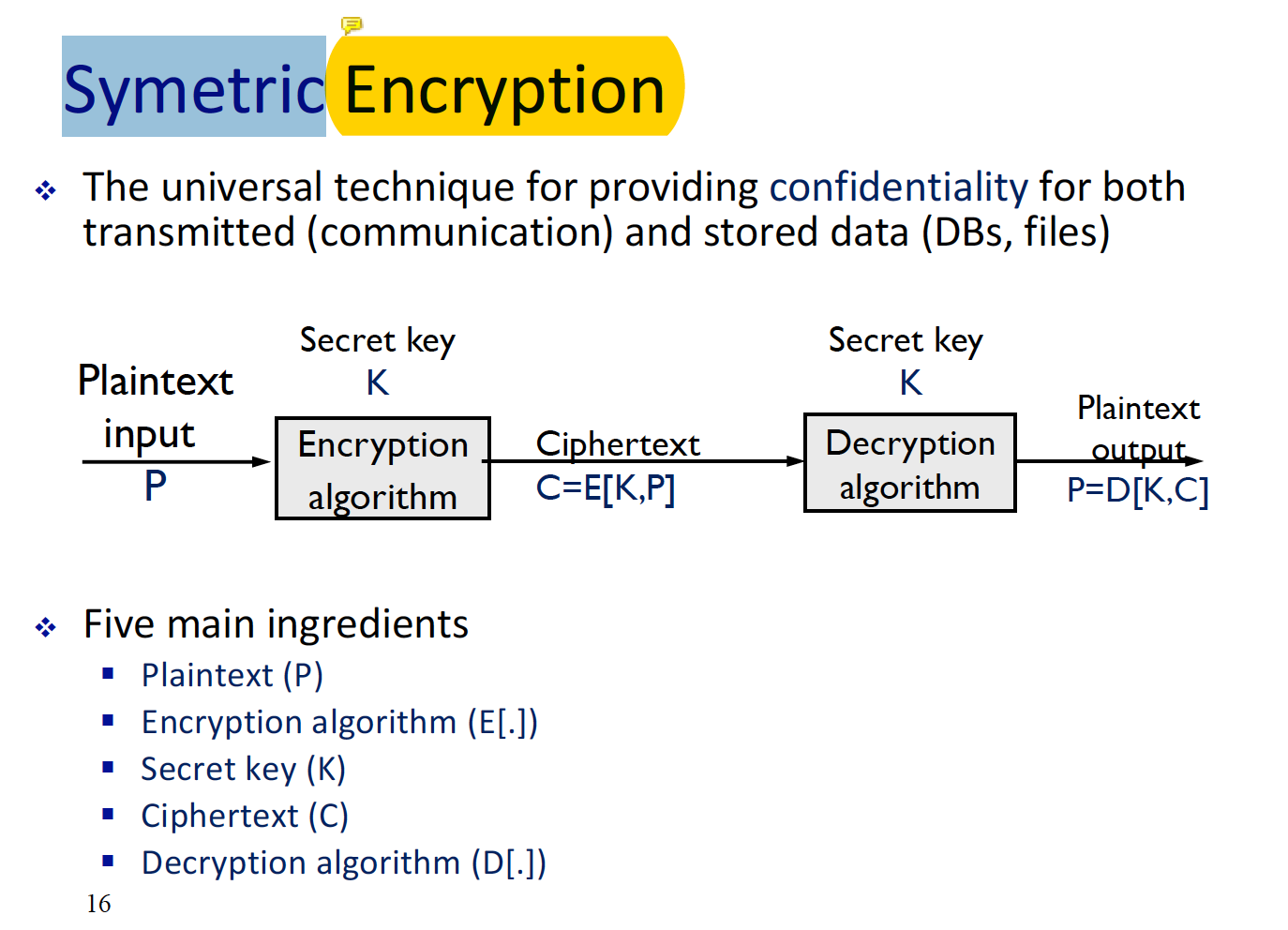
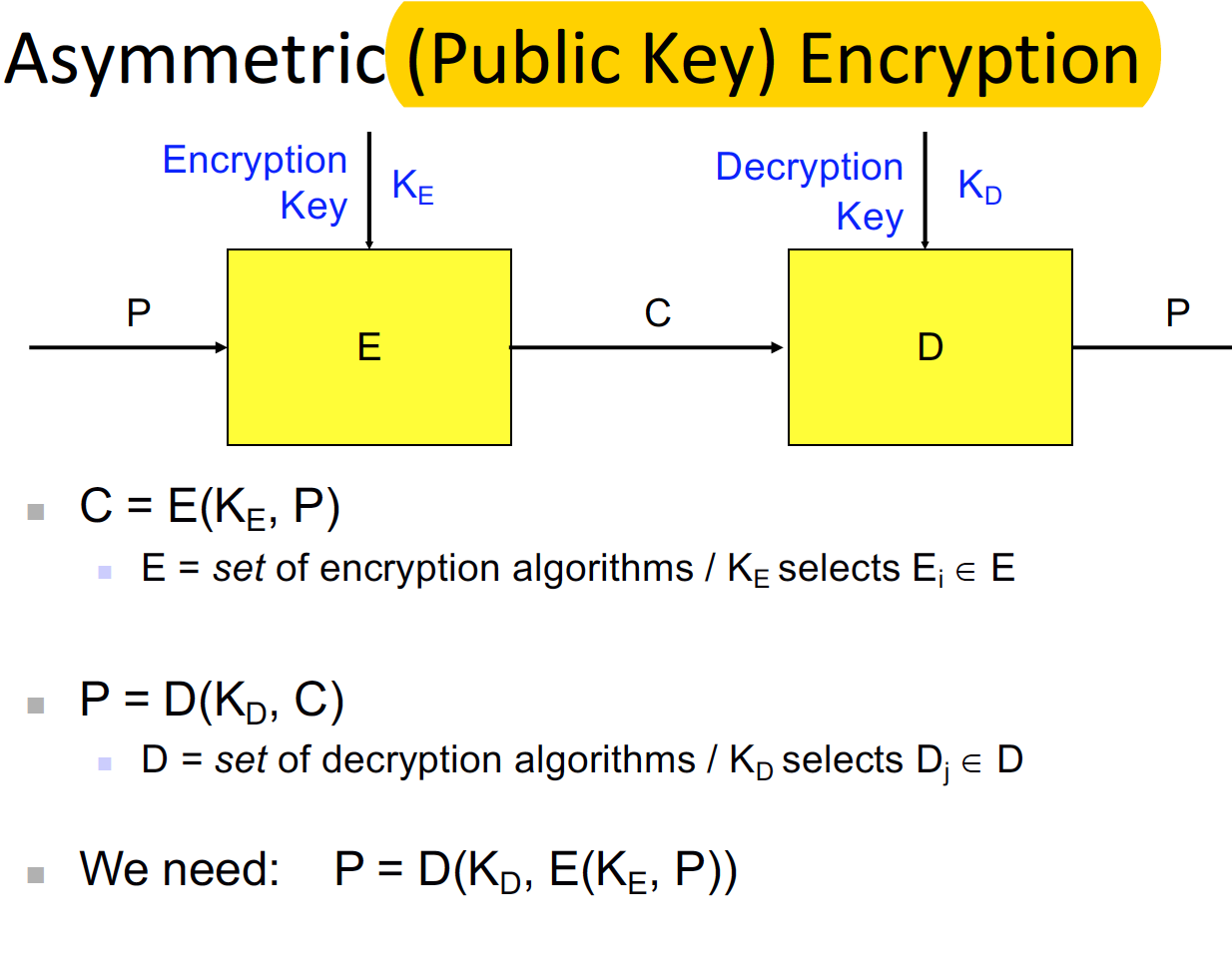
1. **Learn about biometric system design – Jae: This is covered in lecture 2.**

* Let’s review what biometric system is, I will define biometric system as a mechanism to capture human characteristics and use them to authenticate user.   
  As seen above it is the definition from the ppt. Now let’s consider requirements of biometric system.   
  1. Each human have to have different characteristics eg) DNA - universality  
  2. Each physical characteristic must be different from each other, eg) finger print cannot be the same as Shape of a hand – uniqueness  
  3. Each human can have different traits and they have to be far apart from each other for machine to distinguish them – distinctiveness  
  4. The bio system, must perform fast and accurate – performance   
  5. It should be easy to collect human traits – collectivity  
  6. People should be okay with the bio tech – acceptability   
  7. The system, should not be effective to common circumstances eg) user have a cold so their voice change, the system will have to overcome that fact that the user have a cold. – Robustness/Resistance to circumvention  
  8. Users data must be protected – privacy  
  Finally, lets consider the process of biometric system. There are three main steps for bio system. 1) Enrollment 2) Verification 3) Identification.  
  1) when user first register into the system, the system collects traits that can identify and authenticate the user.  
    
  2) When a user claims their identity, in which it is among the user stored in the database.   
    
  3) If the system recognize the user from hundreds of templates, compare the extracted features from the user and stored data.

**6. Learn about threats and vulnerabilities and their countermeasures**- This material is covered in lecture 1.   
In a nutshell   
threats: situation where vulnerabilities can be exploited and abused  
vulnerabilities: weak point in the system, when exploited can cause harm to the system  
counter measures: (control) – Counter measures to protect assets. (In lecture one we covered – encryption, hardware control, software control, policies, and physical etc…)

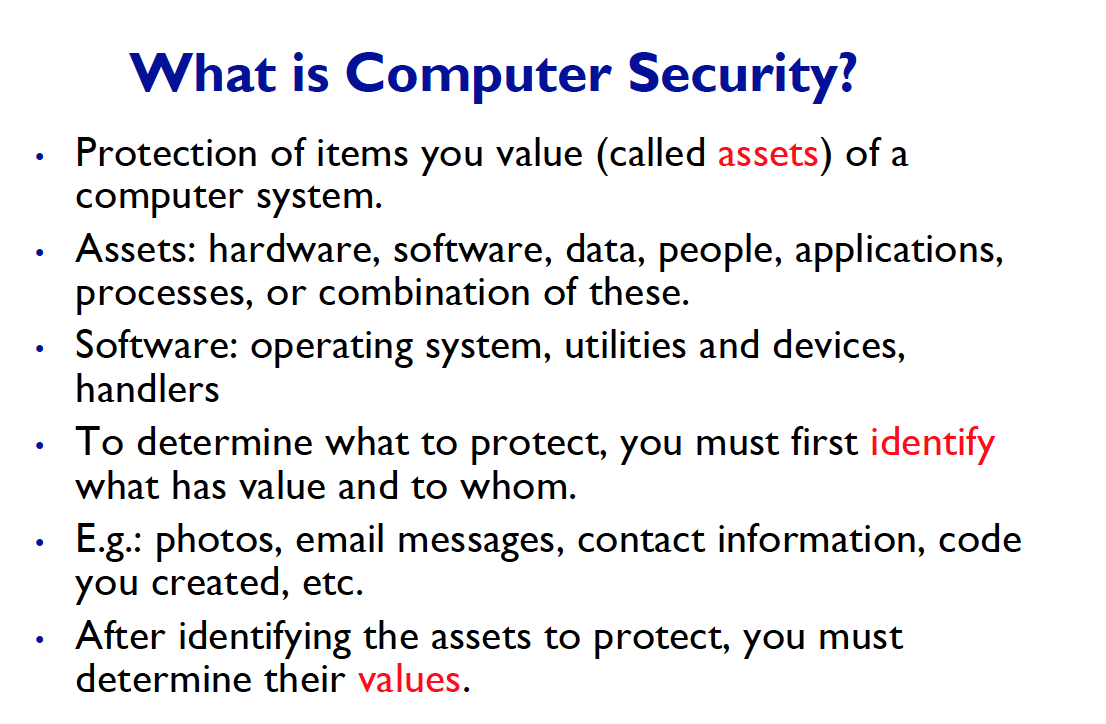
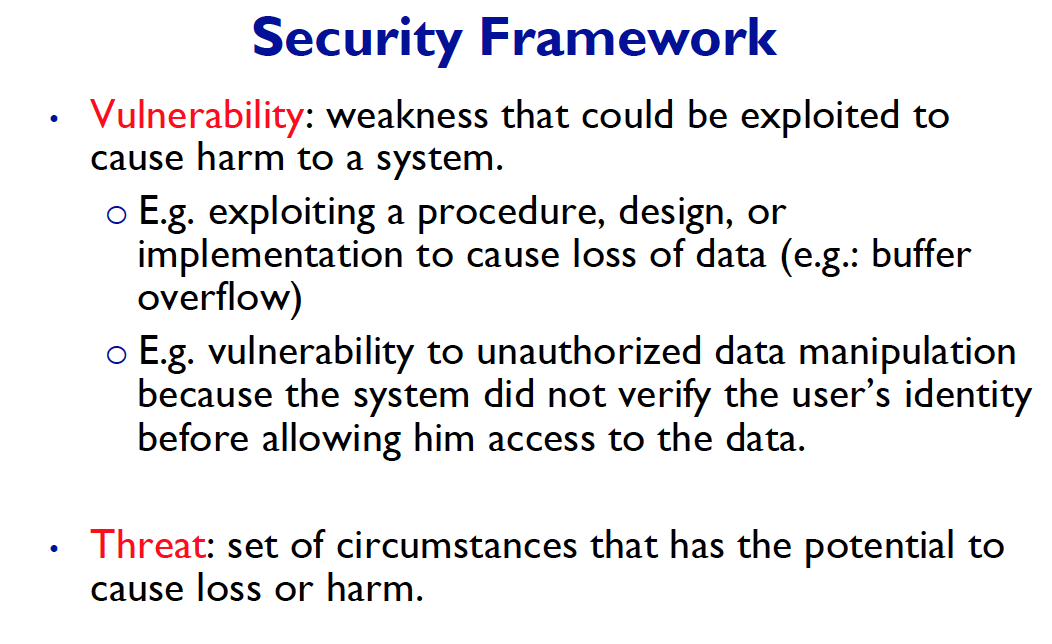
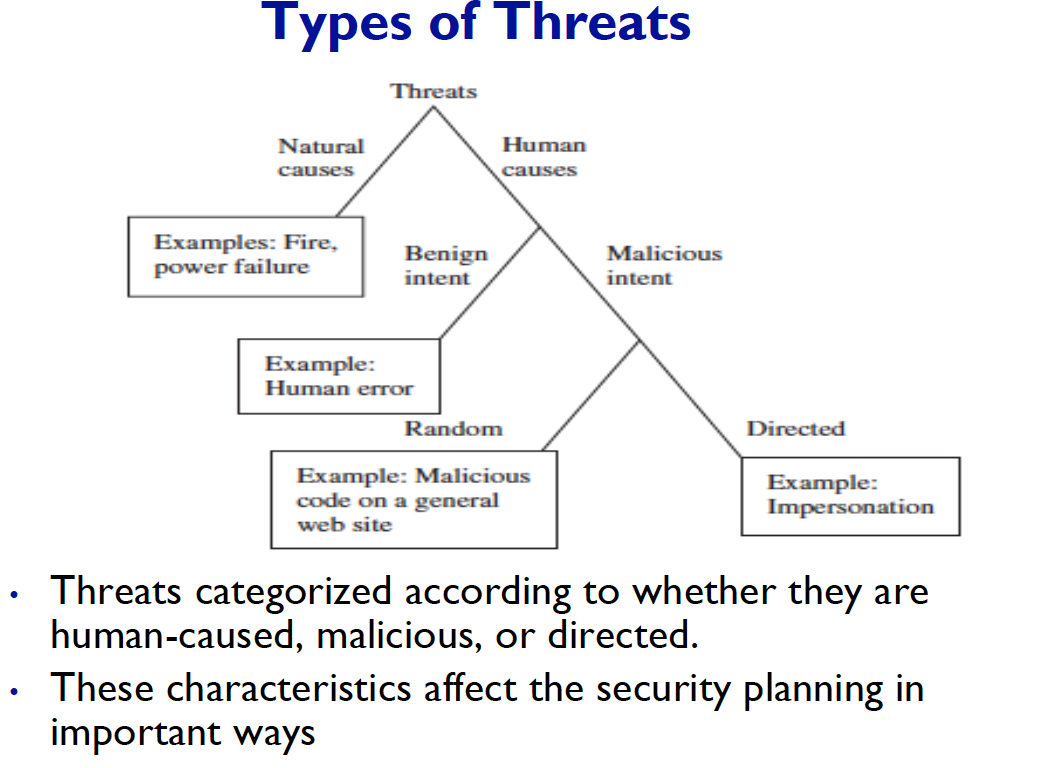
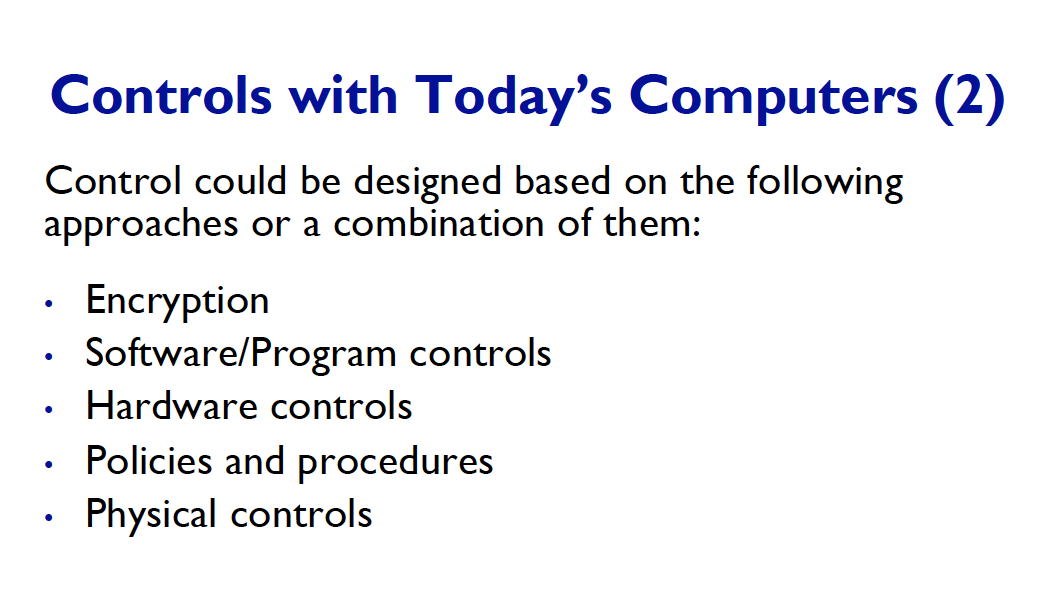
**7. Learn about IDS & Firewall design – Jae: So, this is covered in lecture 8.**- Let’s learn about what Firewall does, and the purpose of firewall.   
  
So I believe in a nut shell, firewall is use to filter out some users, who are trying to gain access to the system. ( I was not able to find anything regarding lDS in the lecture notes sowwwwi)  
  
- firewall – the way this works, is VPN – virtual private network, meaning we create a virtual dedicated network.

**8. Learn about symmetric/asymmetric cryptosystems – Jae: This section is covered in lecture 3**

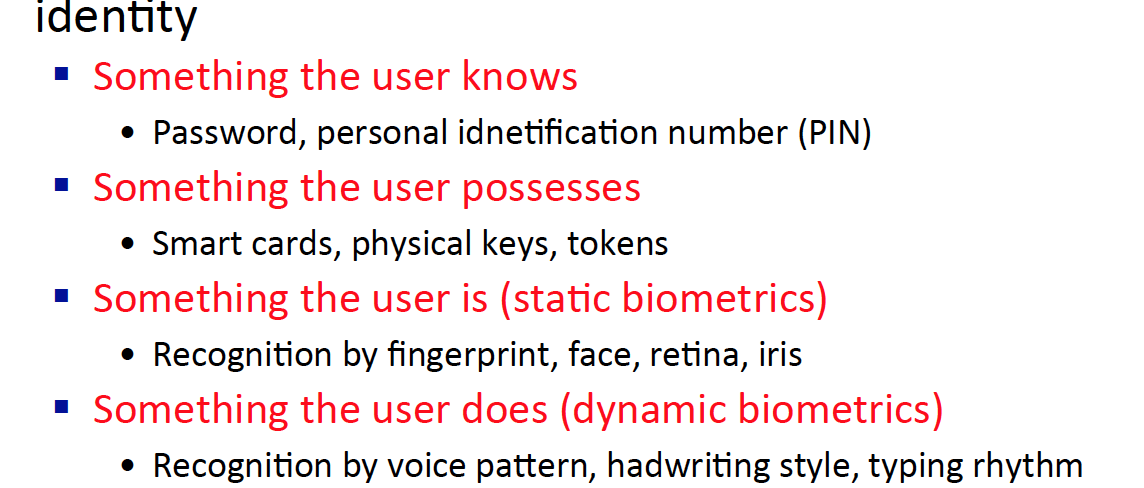
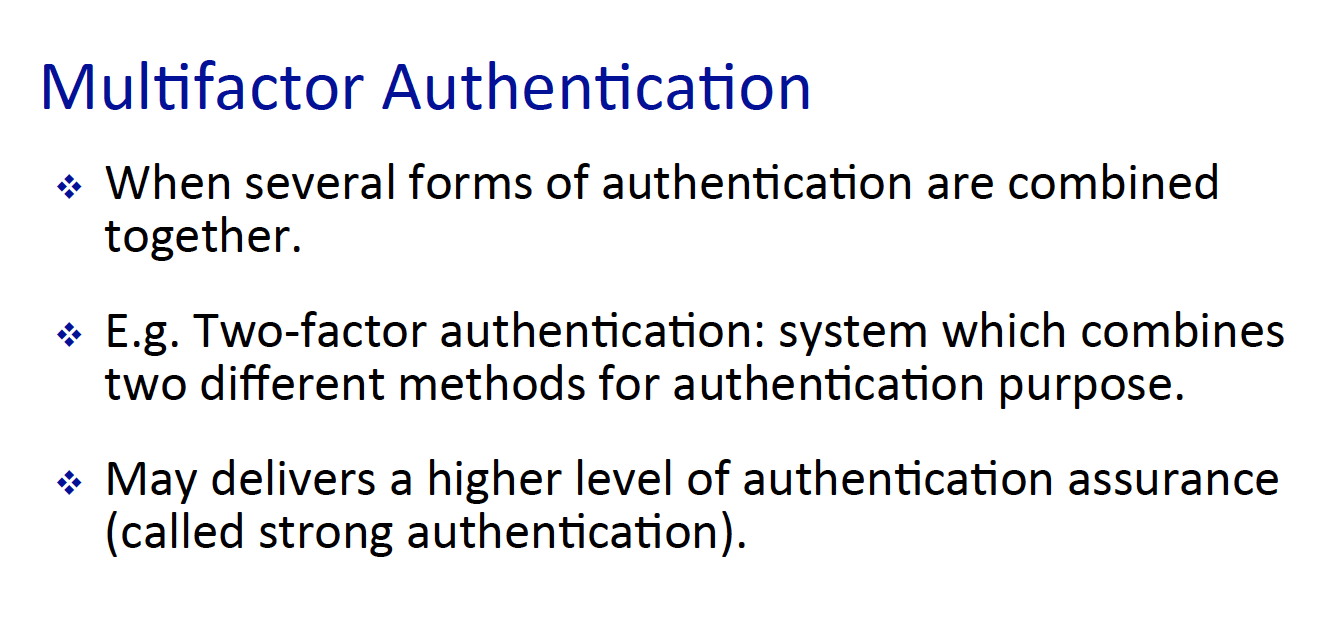
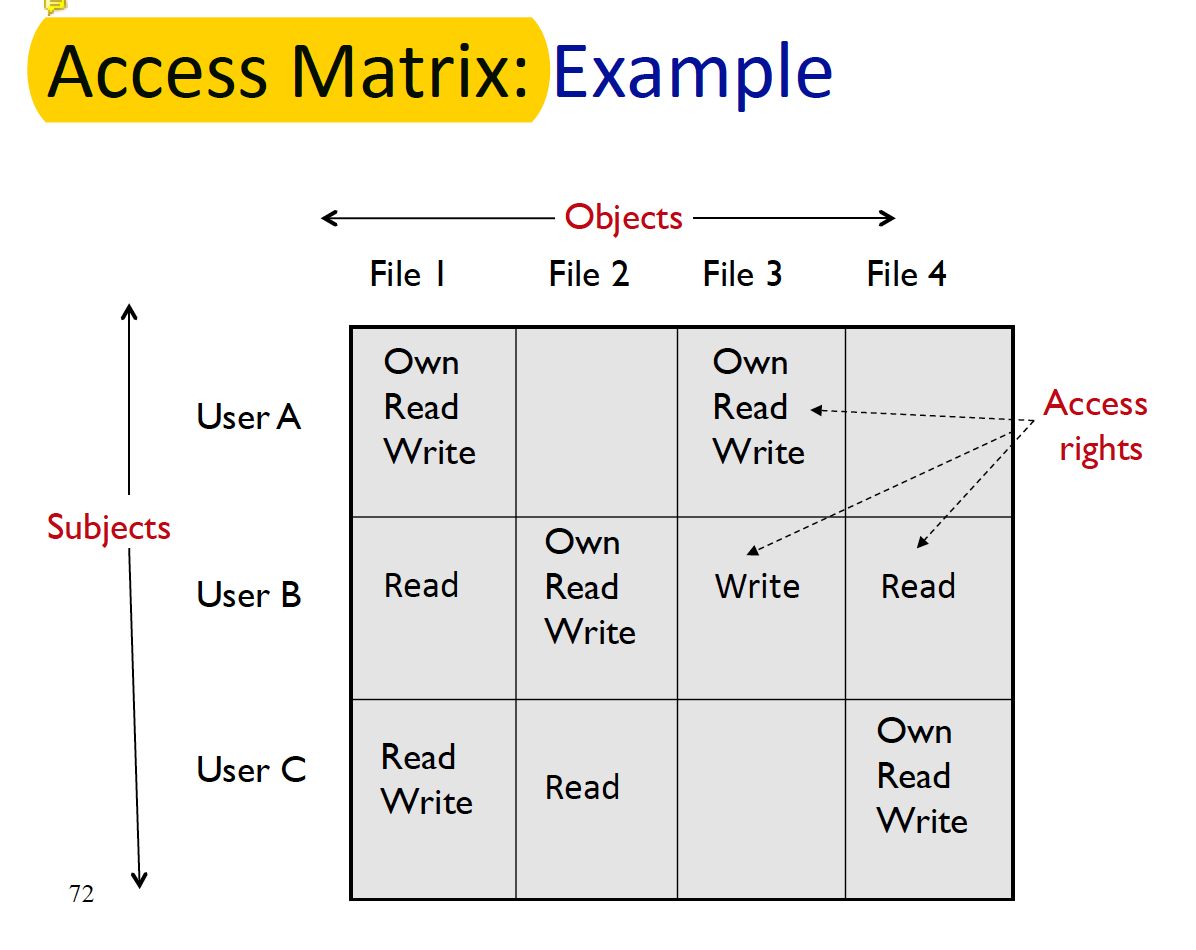
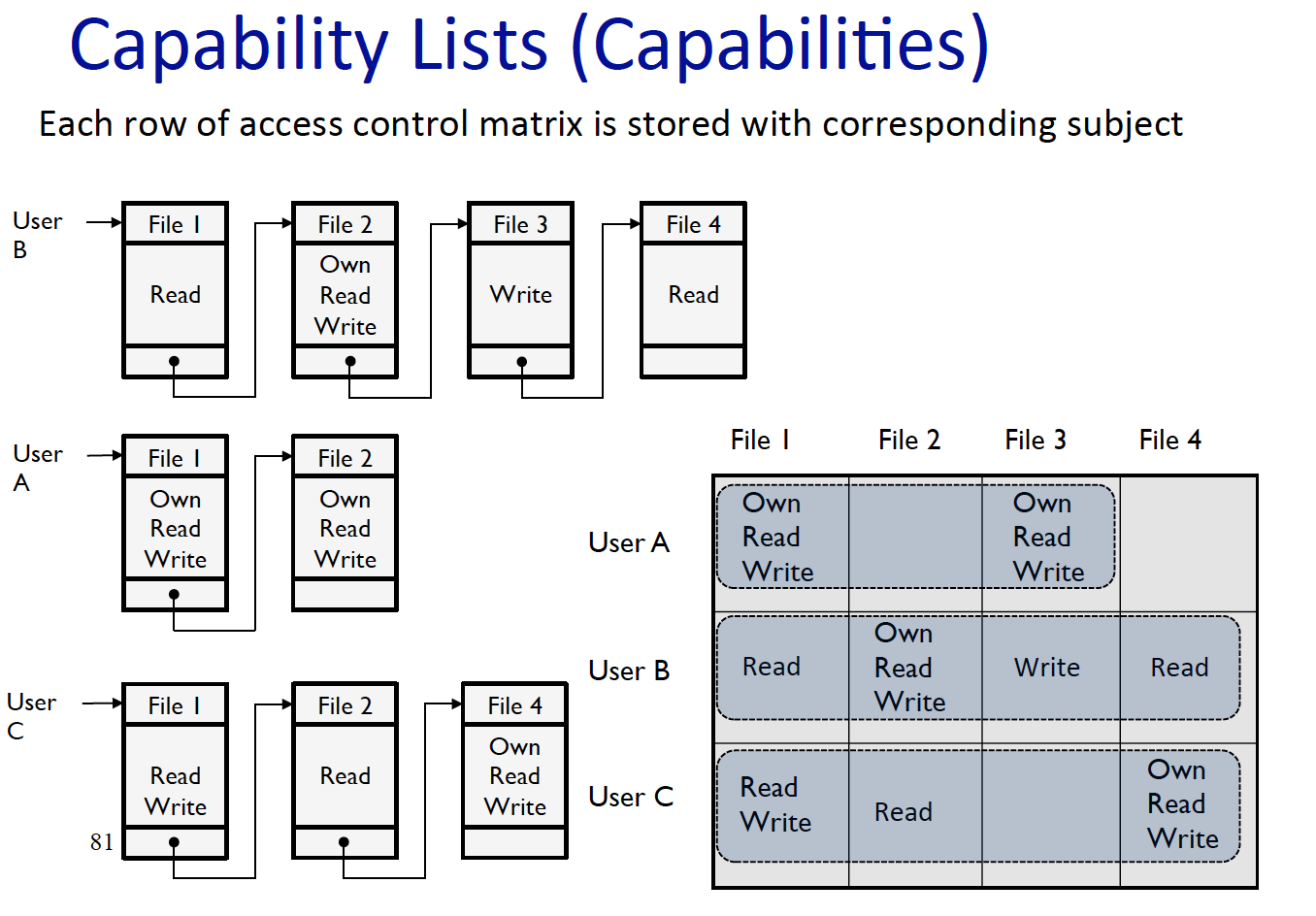
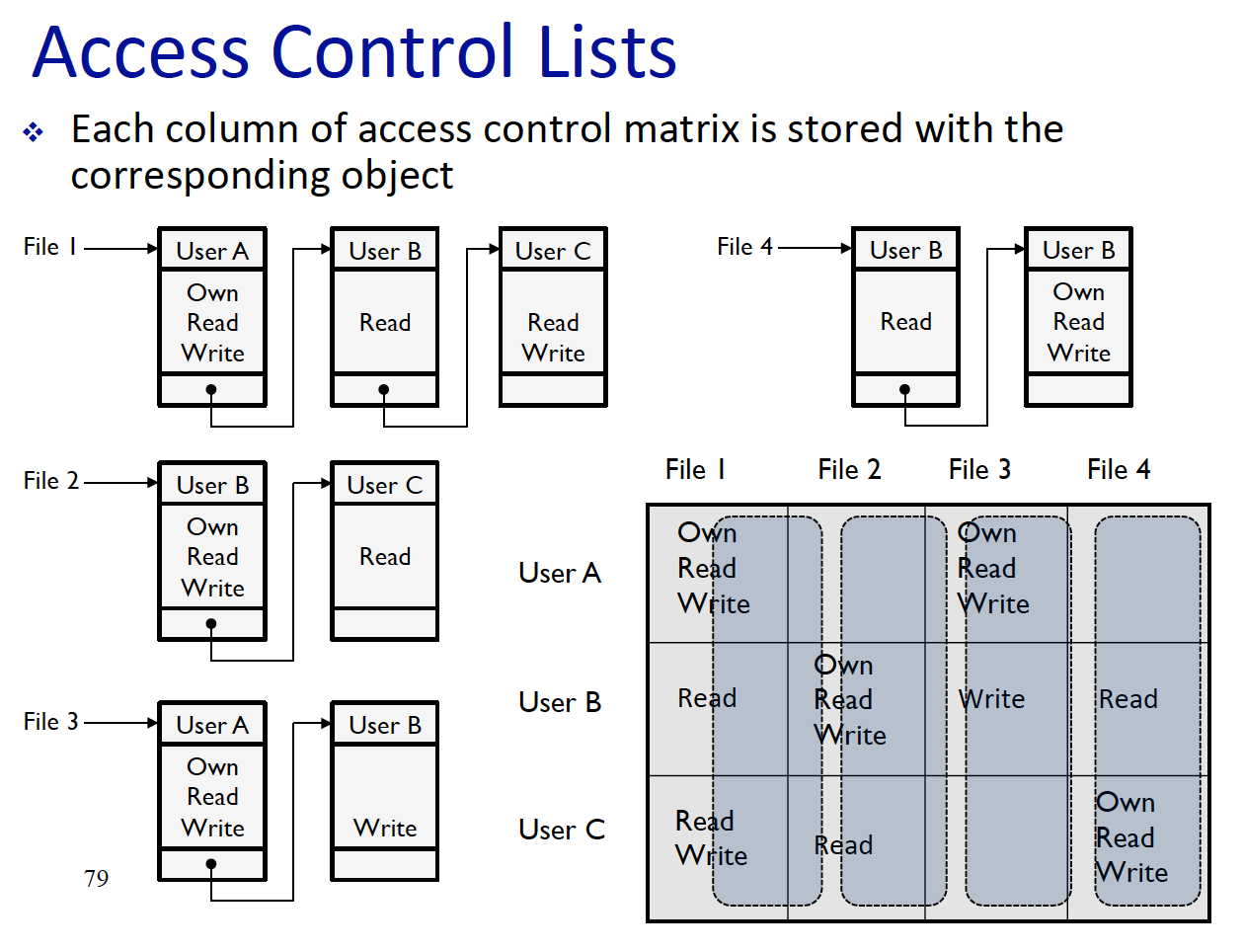
- So, lets review what symmetric and asymmetric cryptosystem are! In symmetric cryptosystems, we use the same key to encrypt and decrypted.   
Asymmetric cryptosystem is the opposite of that, we use different key to encrypt and decrypt.   
The main reason we use, asymmetric cryptosystem is because of key numbers. The number of keys we need in symmetric encryption system is n \* (n – 1 ) / 2 while in asymmetric it is just 2n!

**9. Administrative, law and ethical issues ARE NOT COVERED.**

**♡ Chapter 1: Introduction to Security**Lecture 1

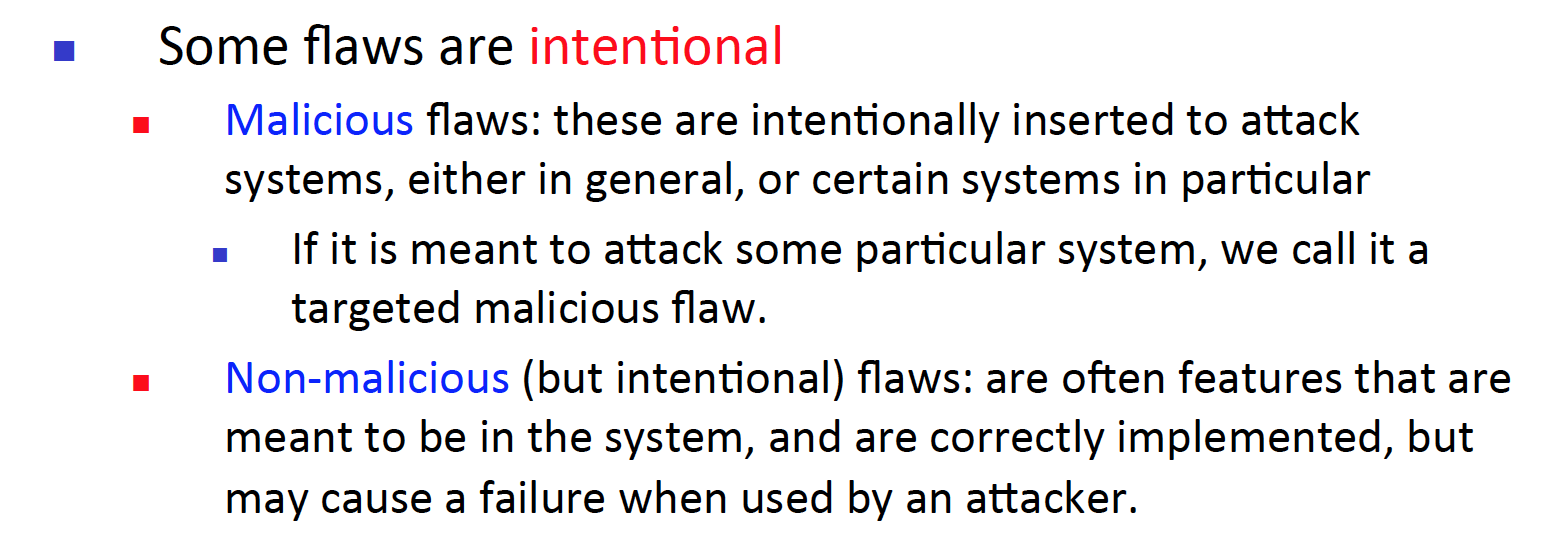
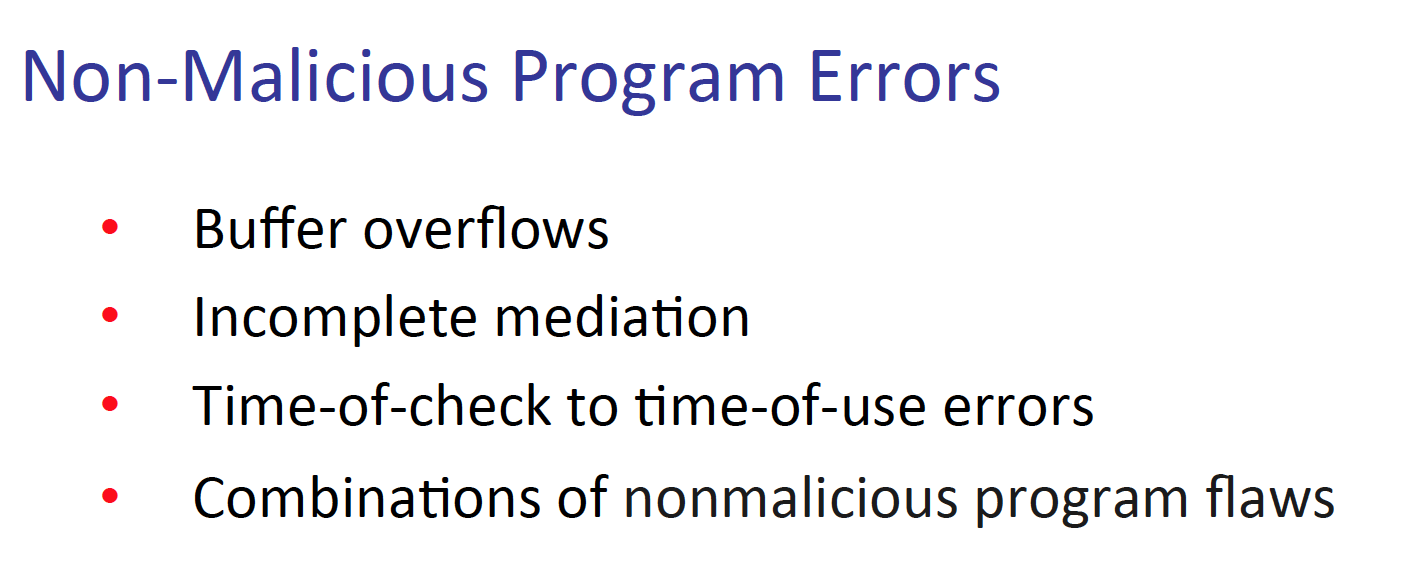
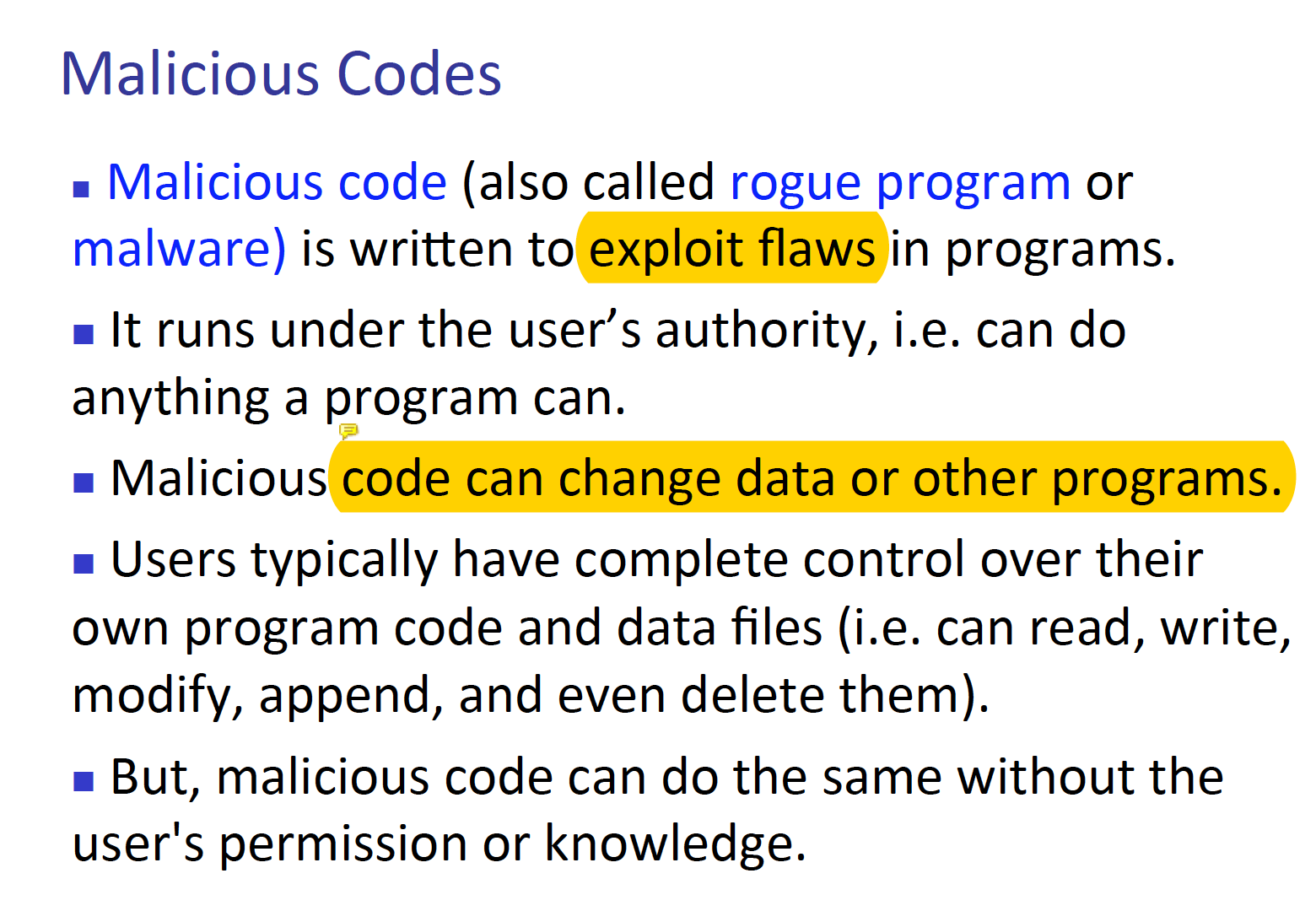
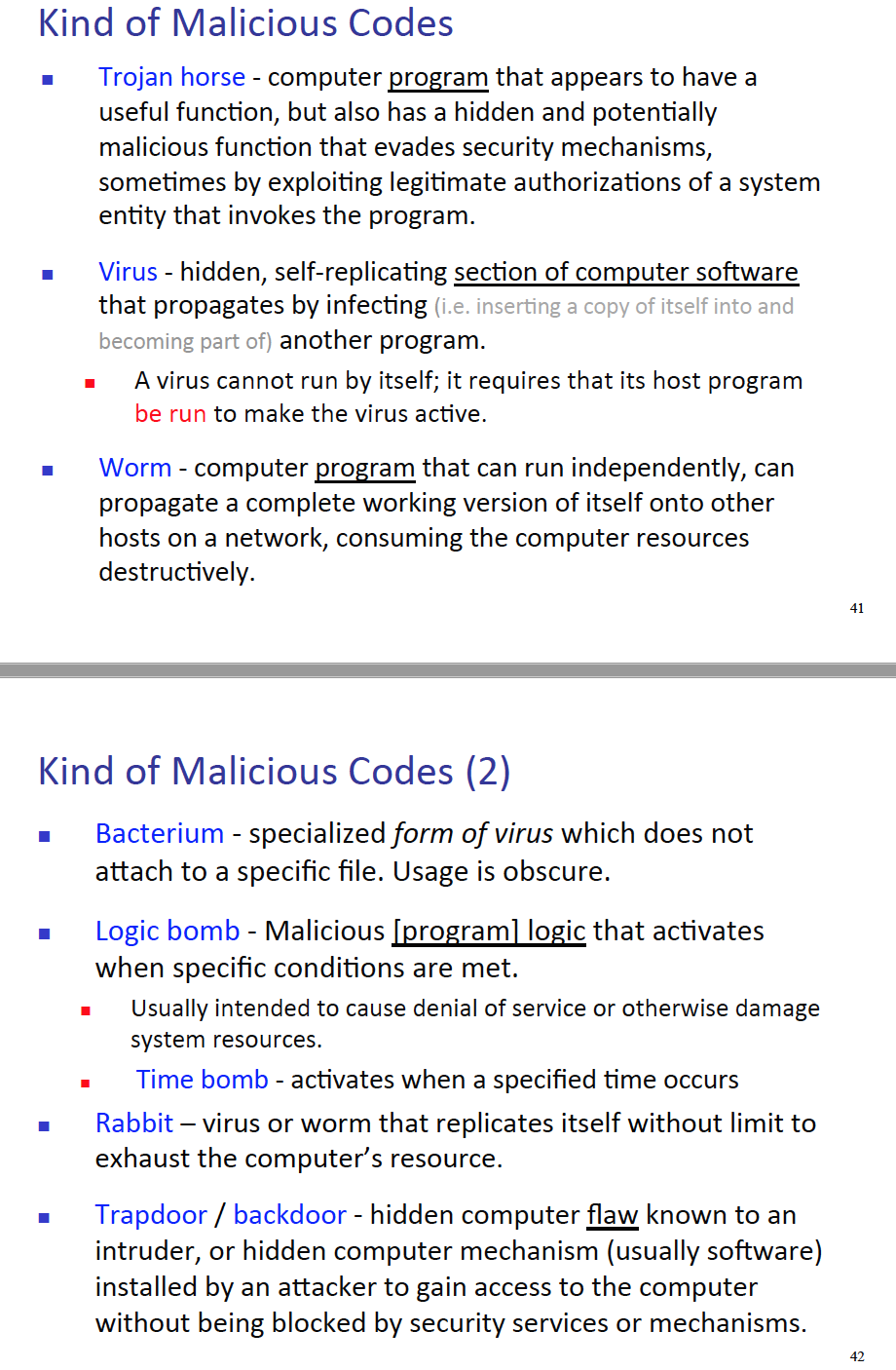
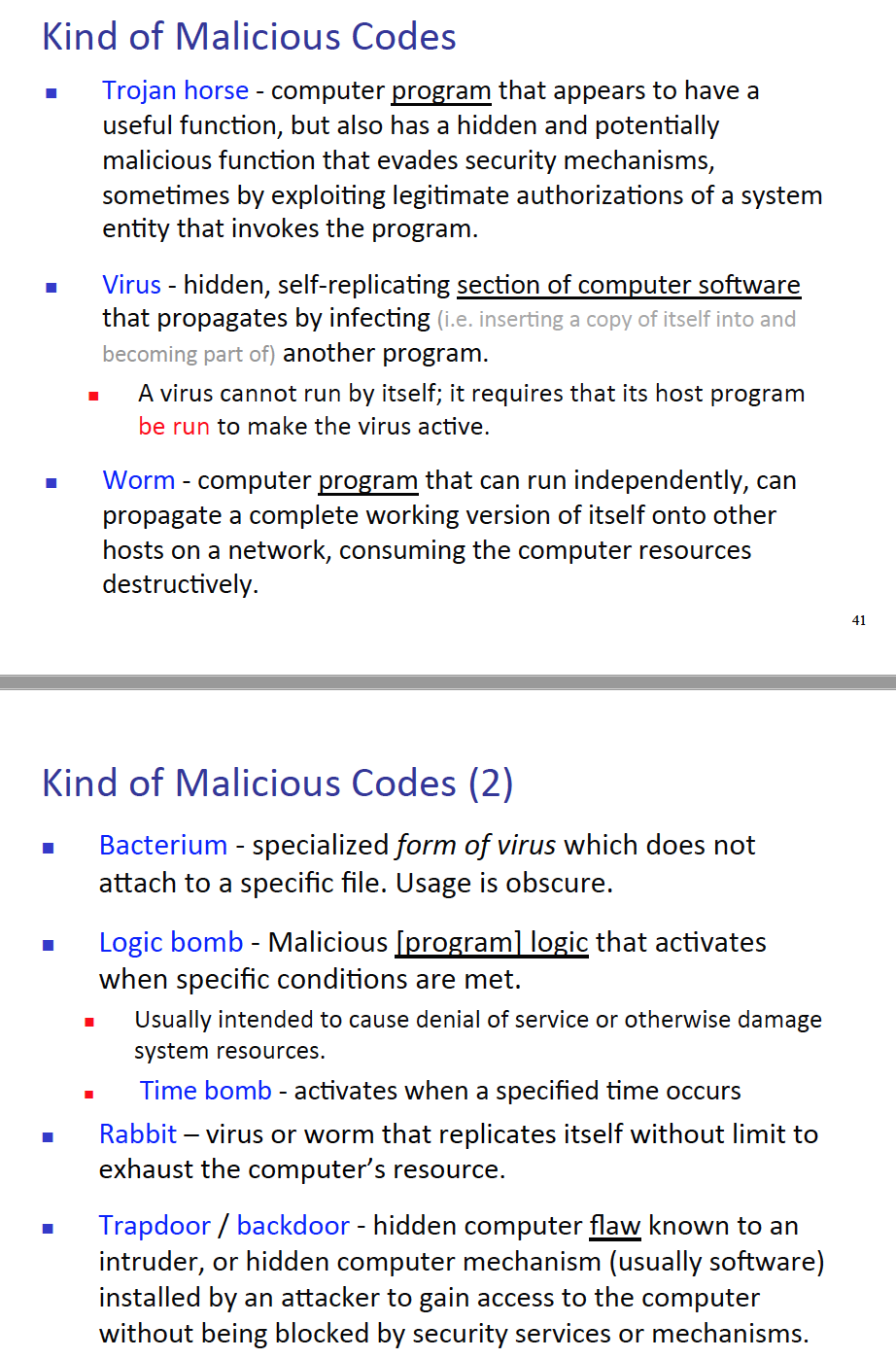
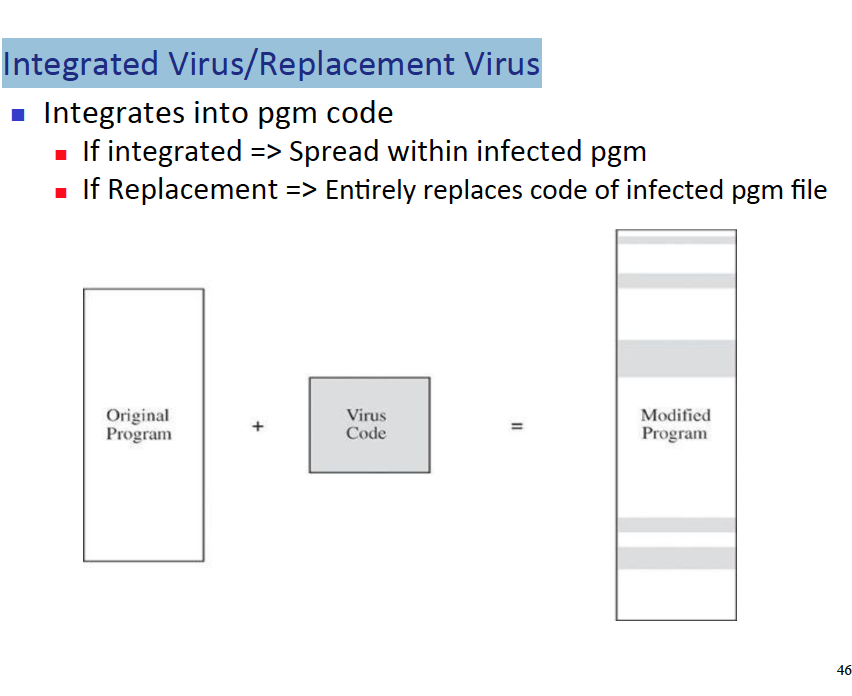
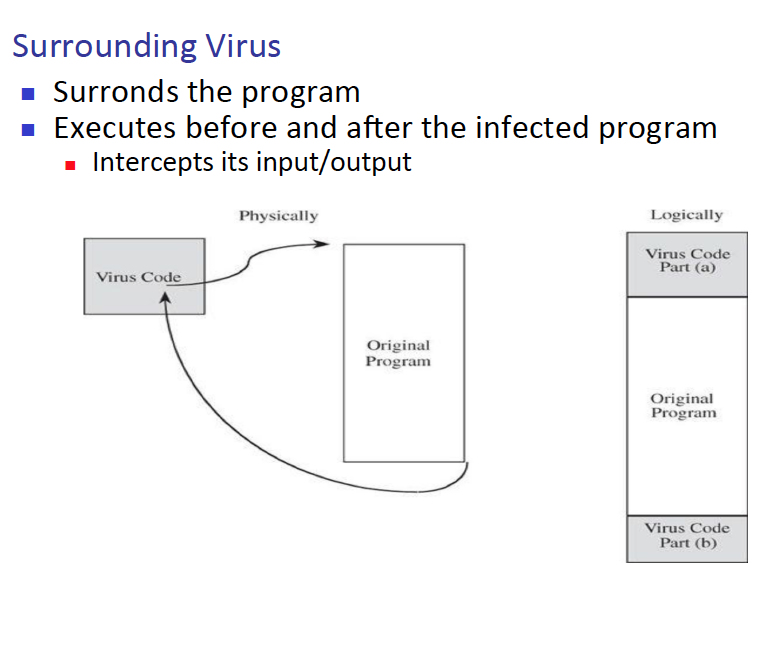
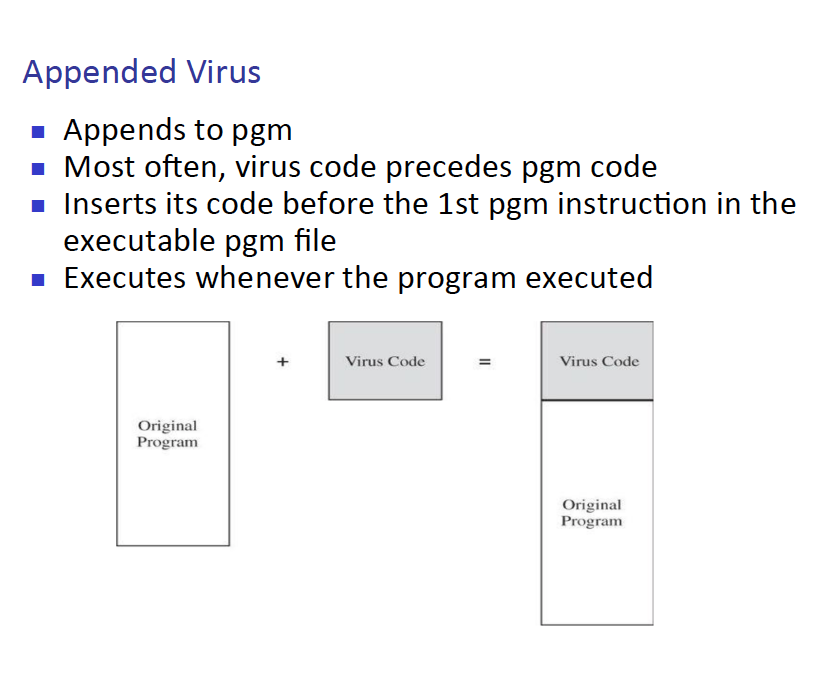
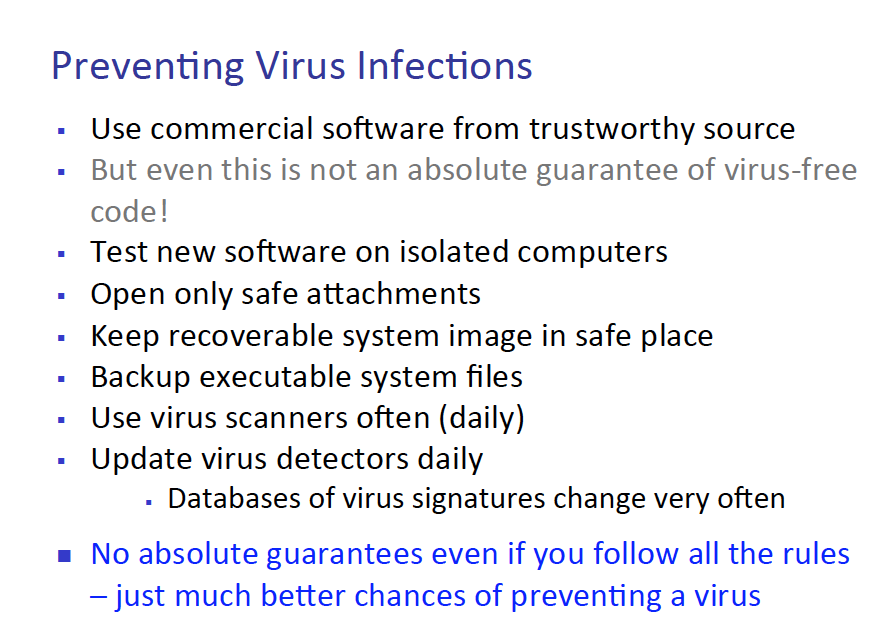
* What an asset means  
  - Asset can be anything, from software to hardware, any object that we have assigned value to. 
* Vulnerability  
  - Weak point or flaw in the system in which can cause harm to the system, and THREAT is situation when someone or something takes advantage of that vulnerability. 
* Different type of threats  
  - There are many type of threats, but the biggest type difference can be.1) Non-malicious and 2) malicious.  
  1) Developers want to test the system, so intentionally takes advantage of vulnerabilities.   
  2) Hackers want to hack the system.
* Everything on chapter 1 – Jae: OKIE!
* Read content on lecture notes, refer to textbook for more concepts (threats, vulnerabilities, CIA, how to achieve these properties) – Jae: Ummm, I am not going to do this, but if you want to read the textbook sure go ahead!
* Controls  
  - Controls are counter measures they are the way to protect assets from threats. And there are lots of them. Here I will give one example software controls - virtual machine (this way, we restricts what a process can access and what it cannot access.)    
  Here is the 4-main method of control.
* Read and understand, do not memorize – Okie!
* Focuses on the understanding, not the definitions – Okie!

**♡ Chapter 2: - Toolbox, Authentication, access control, and Cyptography  
Lecture 2**

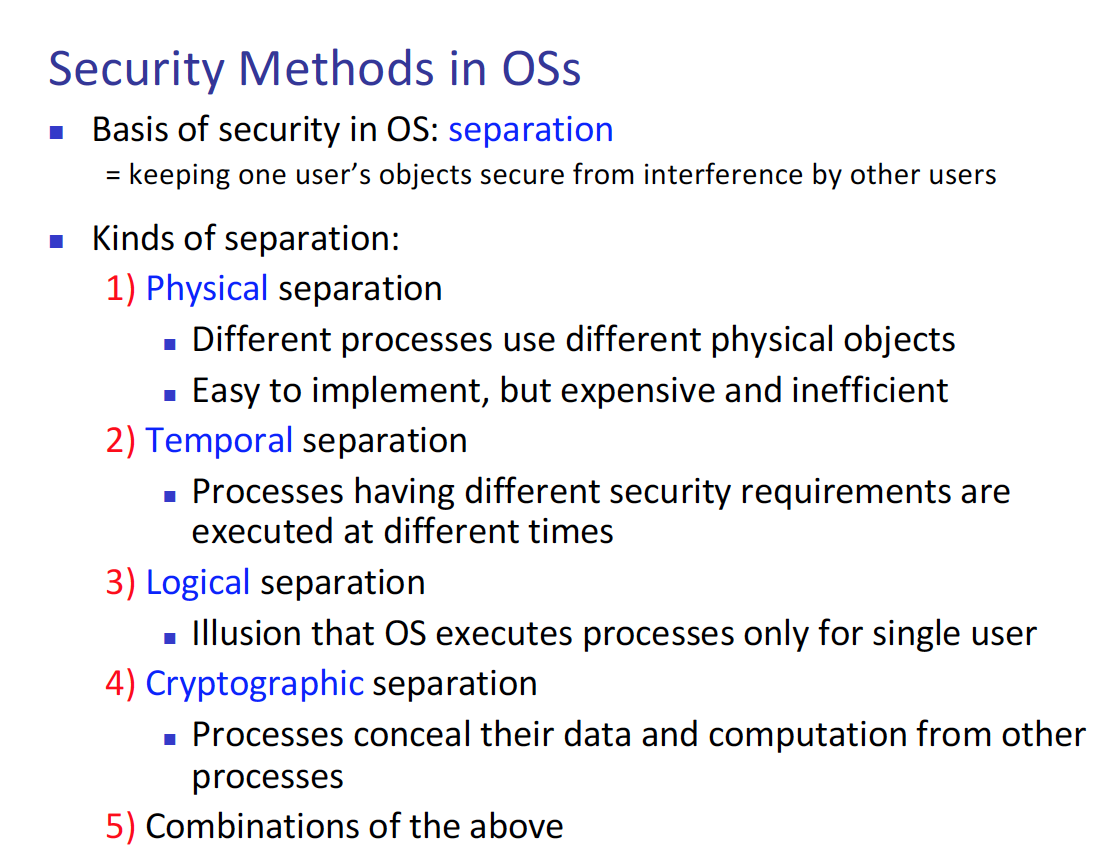
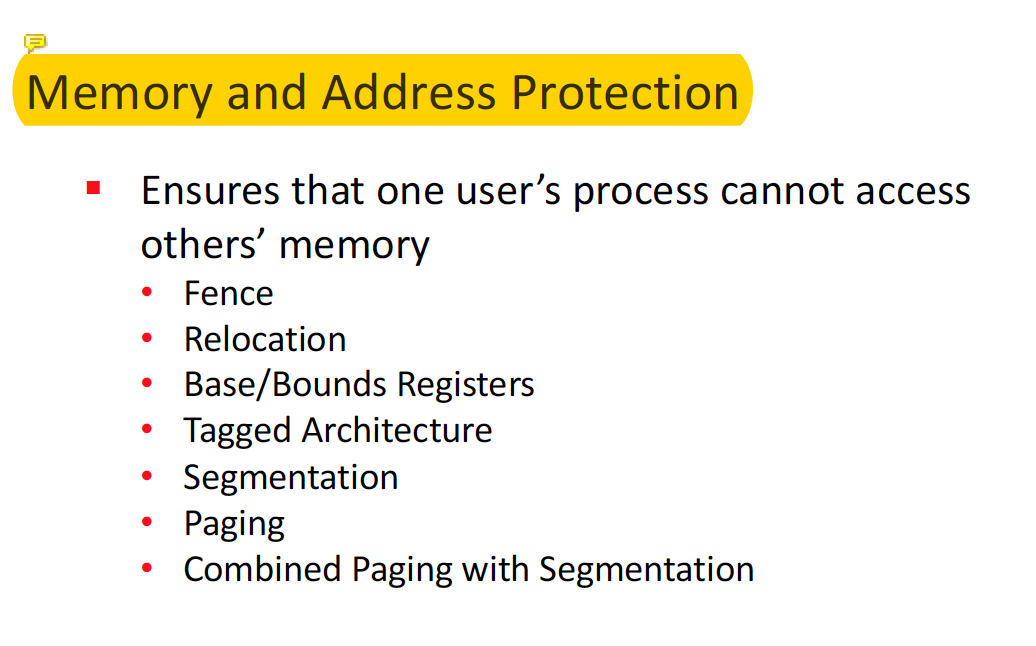
* **Authentication**
* Authentication and identification are two different things! It can be confusing since the process of authentication involves two steps. 1. Identification and 2. Authentication.   
  In a nutshell, identification is user saying who they are. And authentication is validating their claim. Whether they really are who they claim to be.
* **Not all sections – Jae: So…. Jo, tell us which section is not included LOL.**
* **Different ways to authenticate a user (password, especially biometrics, how they are designed, what are the different kinds and components of biometric systems)**- We already looked at bio metric systems, now let’s look at other authentication methods. There are 4 major categories in which bio metric system is under the section ‘what user is’ and ‘what user does’.  
  1) user know – password or some kind of unique memory that the only user has   
  2) user owns - security token or security card, some kind of token that unique user possess   
  3) user is – static biometric such as DNA – user cannot change the DNA   
  4) user do – dynamic biometric such as voice – user have the speak to get validation
* **For instance,   
  enrolment module,   
  verification module,   
  processing module, how do these 3 modules interact together**- These three steps are covered in biometric system – please scroll up to ‘**Learn about biometric system design’**
* **Understand different modules**- Different modules? Jae: I was not able to find any module in the lecture 2 ppt.
* **Authentication based on Tokens**- This is under the category of what user has, such as security card or token.  
  Some security mechanism combine both what user know and what user have – this is other words called – **Multifactor Authentication**.
* **Do not need Federated Identity Management – Jae: Thank you!**
* **Multifactor Authentication**
* A great example of this can be debit card – since not only we need the card itselfl, but also PIN number to buy certain product.
* **Secure Authentication**
* For this part, there is no page called ‘secure authentication’. So, will skip this part.
* **Access Control**
* We have a lot to cover here, but let’s keep things short. ACM – access control matrix, is a matrix that contains both subject, object, and their access level.  
  If we divide this matrix in to separate rows, then we get capability list – in which what each user is capable of.  
  And if we divide the ACM in to respected columns we get ACL – point of view of the object rather than the subject. **Lecture 3 - 4**
* **Cryptography - Public Key, symmetric key, user public key to exchange key, public key cryptosystem to share they key**  
  ^ So basically, just public key, symmetric key, User Public Key to exchange key, and public key cryptosystem – lecture 4 ppt.

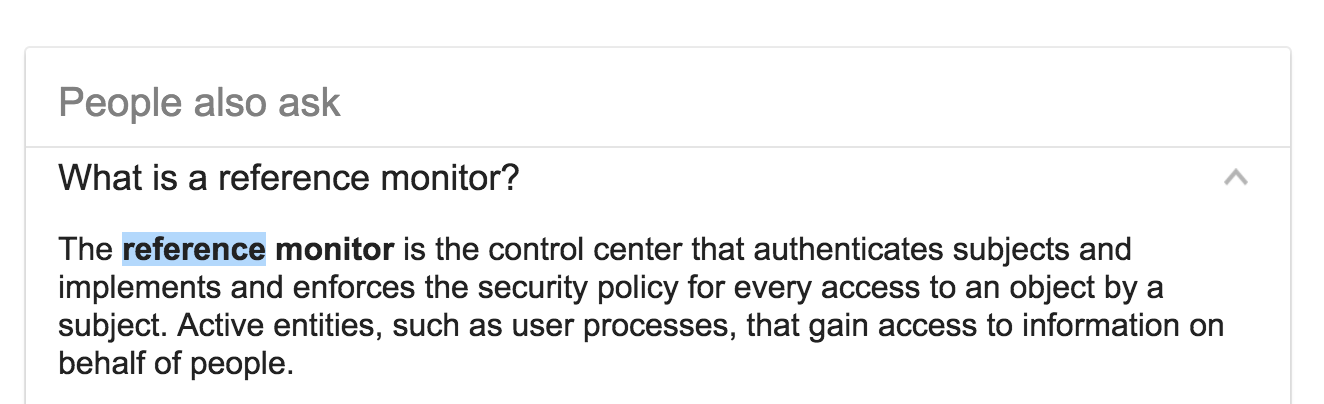
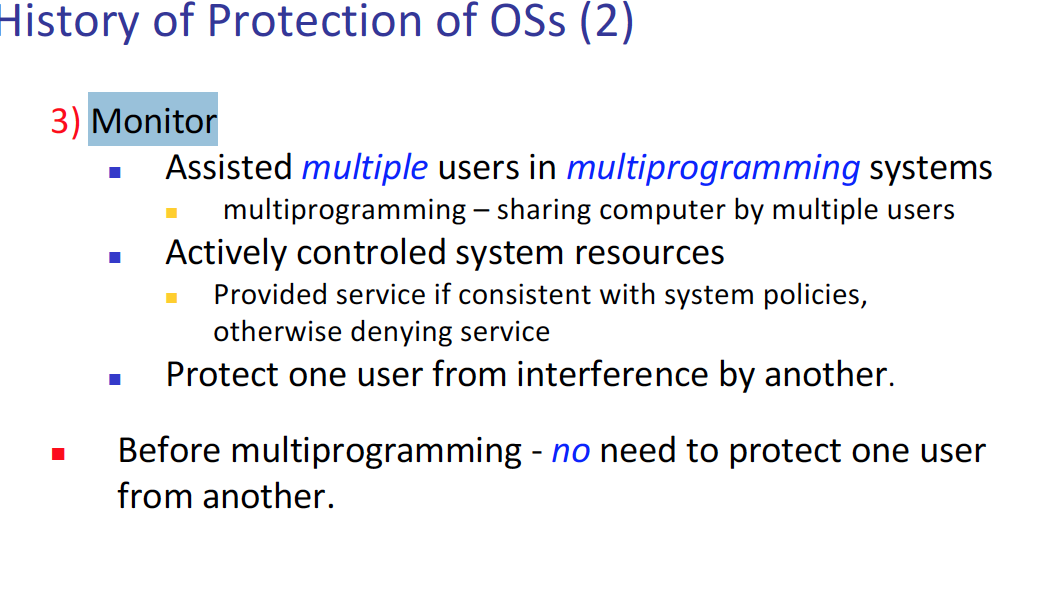
Let’s review what each of it is.

**♡ Chapter 3: Programs and Programming**Lecture 5

* **Just look for non-malicious code vs malicious code**  
  - Let’s review the definition of what non-malicious and malicious is.  
  So now, we can assume that malicious code is done by an attacker and non-malicious codes are not written with bad intentions rather, a vulnerability in the system.  
  Here we can see some examples of non-malicious program errors, again these errors are not intentional, rather some part of the system that an attacker can abuse.   
  Here we can see some examples of malicious codes, these codes are written in the intention to attack. Below there is a screen shot of some examples of malicious codes.  
   
* **What does it mean, what are the different types of malware (worms, trojan horses, etc) do not memorize definitions, but what these types of codes how do they perform in a program and what are the intentions, and what do they DO is the most important? How are they designed and what do they do**- Here is the full list of each malware and what they do, I think it is better to understand them and know what they do as stated in the question rather memorizing them.
* **For instance, if you want to insert a malicious code can you do it in the beginning, middle, end, what are the consequences of each type**
  + I believe this question is tackling places where attacker can append virus. There are 3 major places to append a virus 1) Append 2) Surrounding 3) Integrated Virus/Replacement Virus.
* **Ways to overcome (3.3)**
  + This section is huge, so I will just put two pdf pages that I PERSONALLY think is the best way to explain ways to overcome virus attacks.

**♡ Chapter 5: Operating systems**Lecture 6

• **Different ways to segment or organize memory in order to secure the OS, we mention segmentation, base and bound registers (5.1)**- First of all, to tackle the segmentation problem, here is way to perform separation.   
There are couple of different methods that is similar to base and bound registers.  
Let talk about   
Fence – just like fences in real life, set boundary points where the process can access.   
Relocation – every time process gets created, relocate their memory space ID to insure, there is no overlapping of memory.  
Base/Bound – Fence mechanism however, can divide multiple users   
Tagged – Base/Bound cannot share resources among users, so have a tagged system in other for them to share resources. This requires special hard ware.  
Segmentation - division of program into several pieces.  
paging – just like segmentation, however the program is divided into equal size.

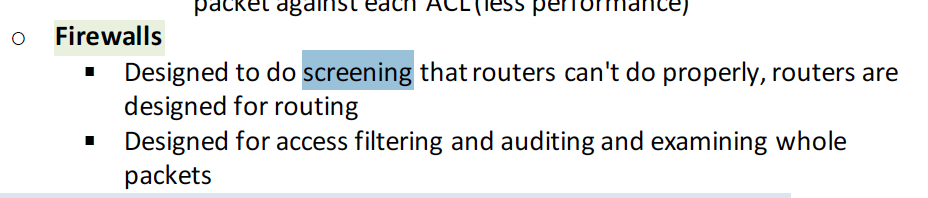
**• 5.2: Only reference monitor (did not study other sections), trusted systems – Jae: THANKS JO!**- In lecture 5 there is no section called reference monitor. But we did learned this from OS class, simply put. One gate way all of the user as well as process have to go through central security unit.

**• Did not talk about 5.3 Rootkit – Jae: THANK YOU LORD**

♡ **Chapter 6: Networks**Lecture 7 and 8

* **6.1: Concepts, need to know what a network is, different types of nodes, communication links, fiber, optics, and so on, what are their capacities**- Let’s start with shape of network. One client and one server is the simplest network.  
  And now terms.  
  node – number of host in the network, host – a device that communicates with one another, and finally, link – connection line between each hosts.  
    
  Media’s   
    
  1) Cable - phone cable, the old way of communication, 10 mbps  
  2) Optical fiber – convert light signals to electrical signals  
  3) Wireless – short radio communication, 802.11  
  4) Microwave – radio form of communication  
  5) Infrared -   
  6) Satellite – use of satellite, either GEO or LEO  
    
  Some type of protocols   
    
  There is the theoretical protocol and the real world protocol.  
  1) physical – data link – network - transport - session – presentation – application (this is theory).  
  2) TCP/IP – real world implementation, which have five layers  
  physical – data link – network – transport – application.

* **6.2: Threats to networks - port scanning, vulnerabilities, modification, etc.**  
    
  - We are going to talk about   
  1) network weak points (or words vulnerability)   
  2) what does attackers do to prepare for an attack.   
  3) type of attack that can happen in the network.  
    
  1) There are multiple weak points in the network   
  attacker anonymity – we do not know, who the attacker is exactly   
  many point of attack – the attacker can start the attack anywhere around the world  
  Resource and network share – many host in the node connected by link are sharing resources as well as, connected to one another.  
  Network complexity – the thing about, network is that it is very complex, no one knows exactly what each component is doing   
  non-uniform policy – there is no one rule that defines how the internet must work with each other.  
    
  2) There are also couple of things that an attacker can do prepare for an attack  
    
  port scan – scan the port of host, using software such as wireshark, see the incoming and outgoing packets.  
    
  Social engineering – to exploit human errors.  
    
  Reconnaissance - to collect discrete data from multiple source of place and hold them together to create new data.  
    
  os/app finger print - google data and background information regarding os or app and take advantage of that.  
    
  3) Finally, there are also couple of attacks in network  
    
  Impersonation – since attacker identity is anonymity, attacker can exploit this property.   
    
  spoofing – there are a lot of packets that is send and received in the network, attacker can spoof these packets and start attacking.  
    
  message confidentiality – any method to gain access to a message  
    
  message integrity – anything to modify/fabricate a message, even adding noise to the message  
    
  Website attack – SQL injection, or buffer overflow, server side attack, anything on those lines.
* 6.3: Did not talk about Wireless Security, not on exam
* 6.4: DoS did not talk about - DOS
* 6.5: Did not talk about – DDOS (Distributed)
* **6.6 Cryptography in Network Security - different types of network encryption,   
  link-to-link, pros and cons, IP sec suite protocol,**- Just like encryption, network encryption can be counted as the most useful tool for a security, expert.  
    
  There are main two models in network security.  
  1) link encryption – this is where data gets encrypted right before it is on the physical median to go to the receiver.  
  2) end to end - this is where there is a secure channel, throughout the two communicating host.   
    
  But there is problem with both encryption methods.   
  Link encryption – the receiver must be able to decrypt the message, otherwise it is useless.  
  end to end – the secure key management channel problem occurs here once again  
    
  Different types of encryptions methods  
  1) SSH – Operating system’s security mechanism comes into play.  
  2) SSL and TLD – SSL commutate between web browser and the server, TLD – client and the server talk to one another to decide the encryption algo that they are going to use.   
  3) SSL session – commonly known as HTTPS  
  4) Onion Routing – How onion browser operates, each node in the network do decryption, so the middle man does not know who the final reception is.  
  5) VPN – virtual private network - just as the name suggests, this is how a firewall operate. Lay a virtual dedicated network link between one host and another.

* **firewalls (6.7), **- Lets look at what fire wall is – we can think of it as a reference monitor, but that exist in the network rather than os.  
  And there are seems to be 6 biggest firewalls.  
  1. Packet Filtering Gateway – this is the simplest way, in UDP send packets from one host to another, if there is one filter existing in the mid way then the packets will not be able to go through. Do not see the packet, rather based upon IP address block the packet.  
  2. Stateful Inspection Firewall – this is more advanced packet filtering, this is done via filtering individual packet by one by one.  
  3. Application proxy – this time, only look at the header of the packet and filter it out  
  4. Circuit level gate way – Allow, one network to be extension of other  
  5. Guard – any set of programmable conditions  
  6. Personal Firewalls – Program that runs on a single host, and mediate all of the in/out going traffic

* **intrusion detection and prevention systems (6.8)**
  + **IDS –** intruder detection system, we need this system since, some of the conection can get passed away from fire walls

There are several ways to do this   
  
signature know base – limited to known patterns  
  
  
heuristic Intrusion detection – look for behaviours that are out of the oridinary.  
  
Stateful protocol analysis – this is something like filtering out the individual packets|  
  
  
There are mainly two types of protection methods  
host based – this is based on one end host system, and collects and filter data, respected to that host (end systems)  
  
Network based – this is based on the whole network, trying to monitor the whole network, and find malicious packets **Intrusion Prevent system – IPS, this is different in the IDS in the way, in which. Prevention rather then detection.**

* 6.9 Did not mention, not on exam – Network Management

# Additional Materials

* How RSA works : given some parameter, can create file n, check prime numbers one question on exam that involves RSA - just study what are the different parameters and how is it used in a typical example
* Given n, p, q
* (p-1)\*(q-1) =   
  1 < e < phi(n)
* (d\*e)%phi(n) = 1, d\* x mod y
* Look up formula

♡ Check for syntax/may put wrong code/key

* Linked encryption - data is encrypted at physical layer T/F - false, application
* N-to-n application layer
* Link-to-link is data-ing layer

* Not much calculation, only RSA, everything else is sentences and understanding scenarios of concepts.

Steps to perform RSA algo.