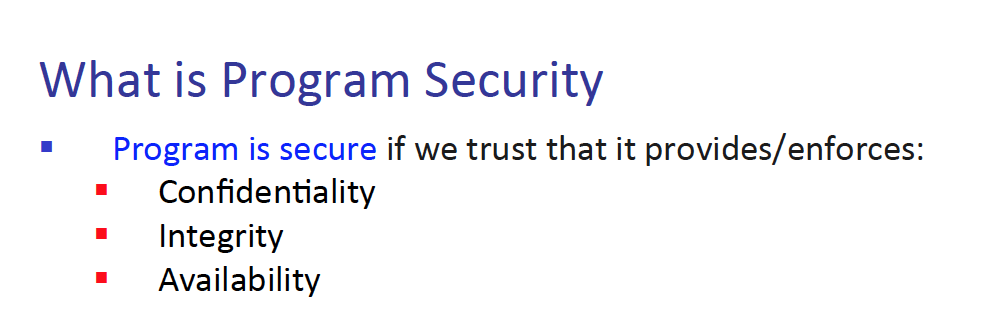
|  |  |  |
| --- | --- | --- |
|  |  | CPS 633 – note questions  Jae Duk Seo |

# Lecture 5 – program security

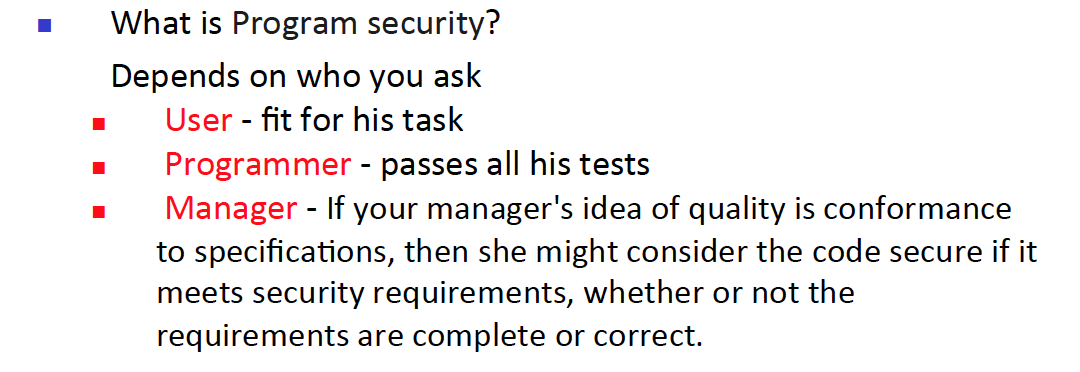
1. When do we say the program is secure?
2. Can program security be different depending on the person you ask?
3. What are flaw, fault, error, bug, and failure?
4. How can we temporally fix up the above problems? Also, is this a permanent solution?
5. What are unexpected behaviors and why do we need to know them?
6. Name some security flaws and describe what buffer overflow is.
7. There are four places where overflown bit can go, describe each of them.
8. How can an attacker abuse the return address?
9. What is the main defense mechanism of web server attack?
10. In incomplete mediation what kind of data are exposed?
11. What are some possible solution for web mediation?
12. Example of client side mediation?
13. Is client mediation good enough?
14. What is TOCTTOU, explain it (what is the other name of this?)
15. What does TOCTTOU exploit?
16. Example of preventing TOCTTOU?
17. What are 1) Undocumented access point 2) off by one on bit error 3) Integrity overflow 4) Race condition?
18. What does malicious code exploit in a program?
19. Name and briefly describe all of malicious type of code.
20. How does virus spread from A to B?
21. What are 1) Append 2) Surrounding 3) Integrated 4) Polymorphic 5) Encrypting virus.
22. Where can virus hide?
23. Can virus be invisible, if not what do they leave out?
24. Explain virus removal process and describe trap door and salami attacks.
25. What are cover channels and 2 major of cover channels - describe each of them.
26. Example of storage channel?
27. What are 2 ways to detect cover channel, explain them.
28. Developing a secure software requires what kind of people?
29. Describe modulation and cohesion and coupling.
30. Describe peer review, hazard analysis, testing and, majority voting.
31. What are some reasons for software modification?
32. What is OS control for security and key characteristic of trusted OS?
33. Describe and explain ‘administrative control for security’.

# Lecture 5 – soltions

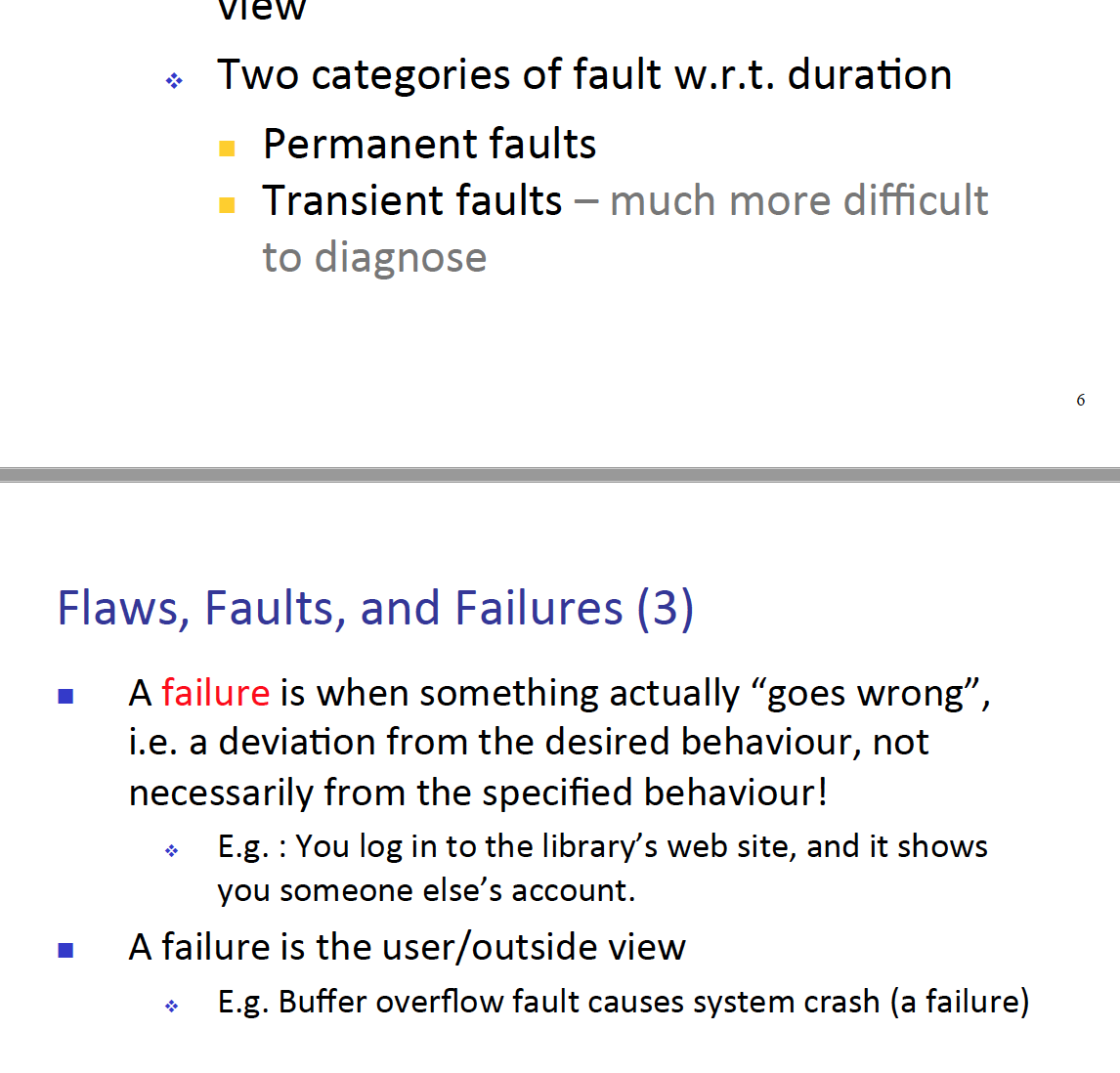
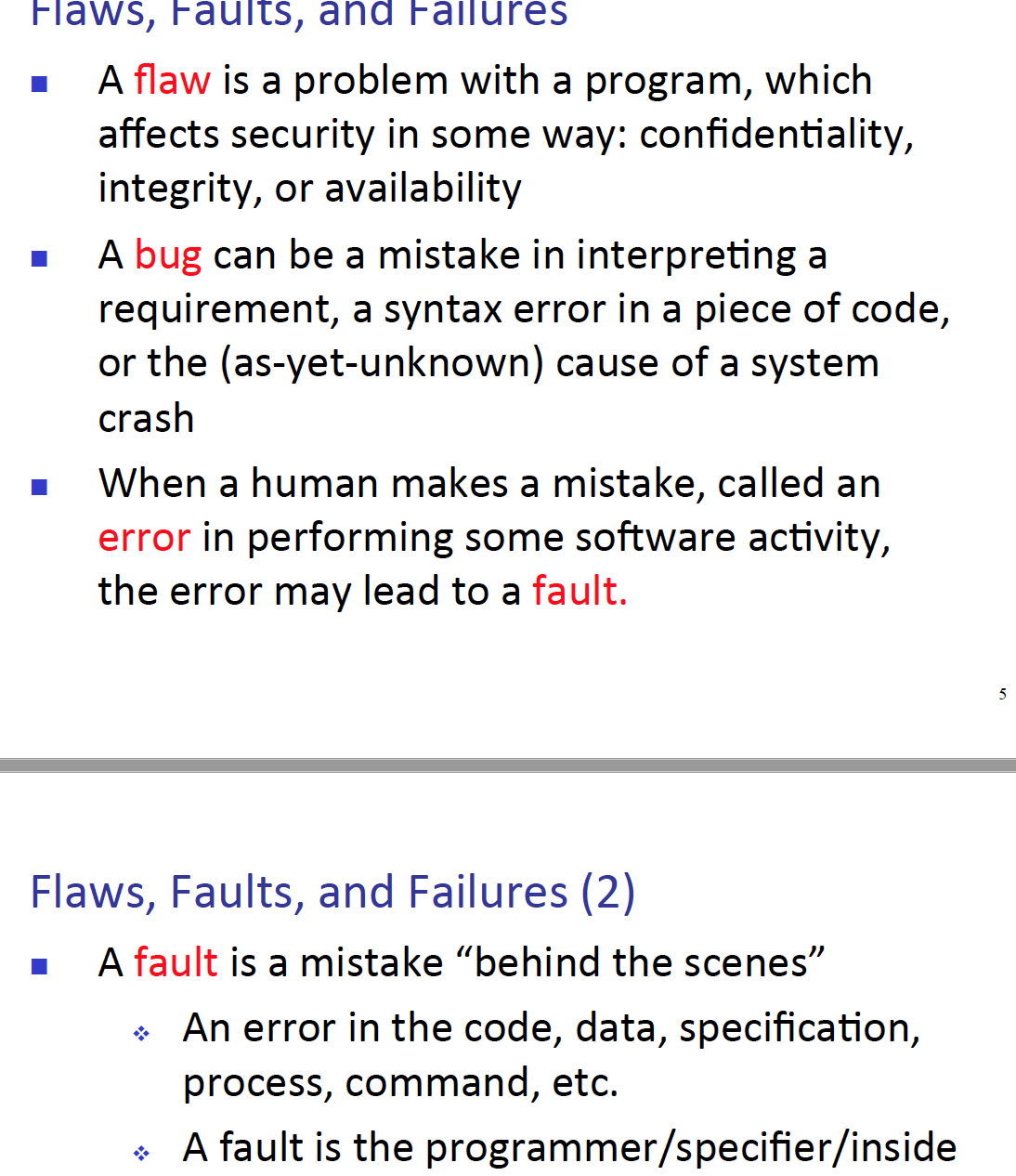
1. When do we say the program is secure?

* We say a program is secure when it is successfully, providing all of the CIA triad. So other words, the program protects security, integrity and availability of the concealed data. 

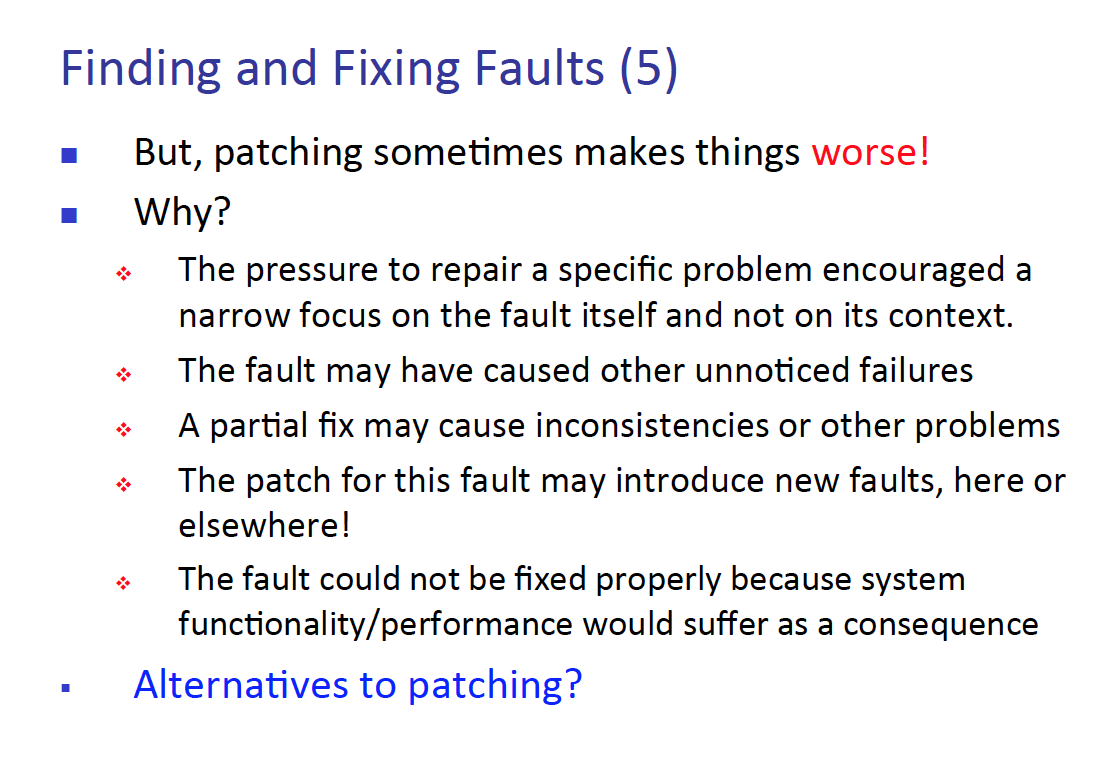
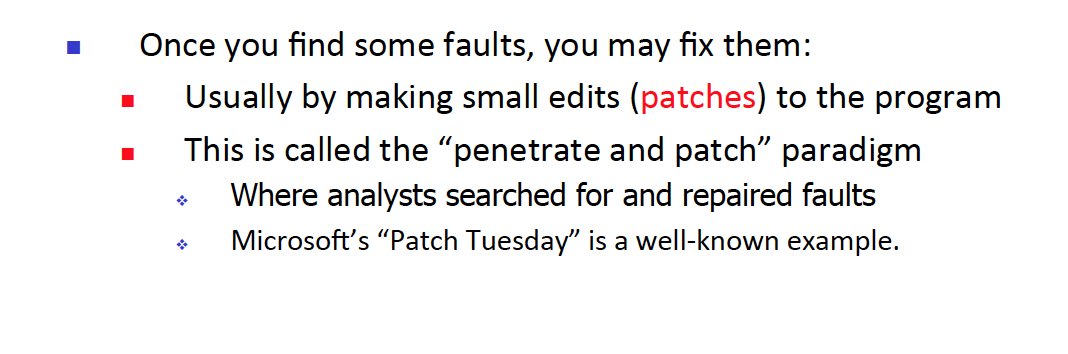
1. Can program security be different depending on the person you ask?

* Yes, like how assets depend on the perspective of security that we are trying to protect, the definition of program security differ from which person you ask to. 

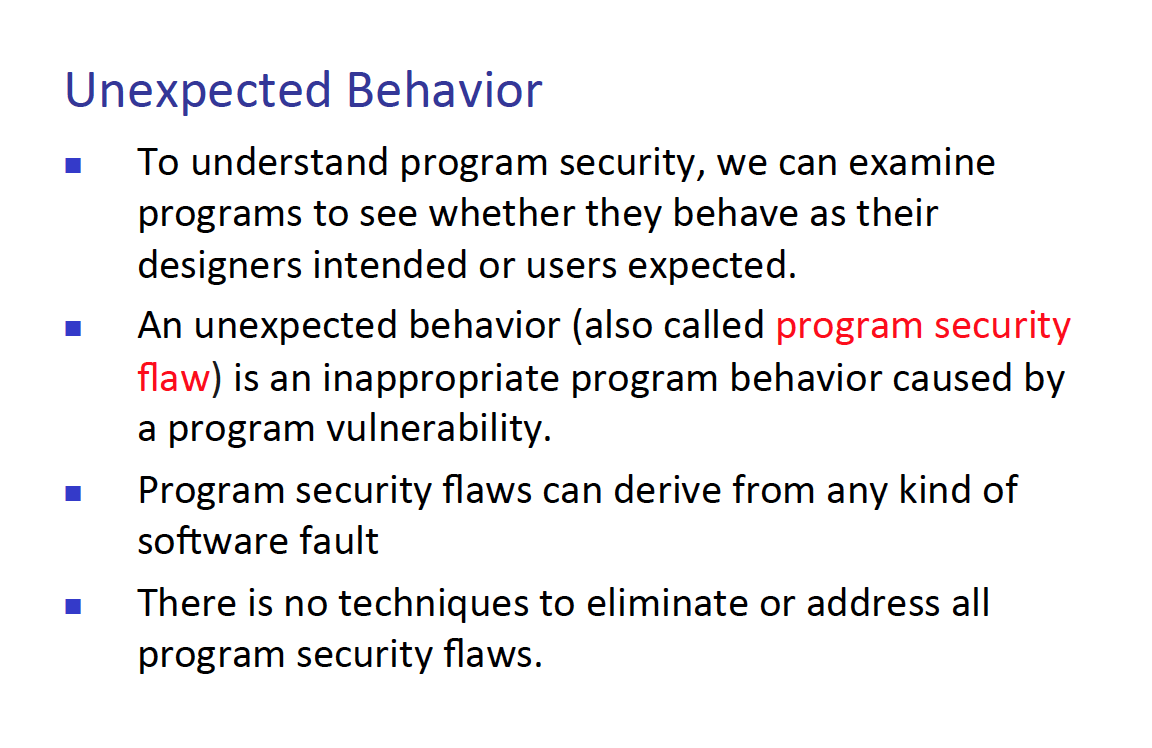
1. What are flaw, fault, error, bug, and failure?

* Flaw – the program has some wrong functioning or something
* Fault – either from human or program, a mistake behind the scene
* Error – human mistake under the branch of Fault.
* Bug – Any cause that makes the system crash.
* Failure - when something actually goes wrong.

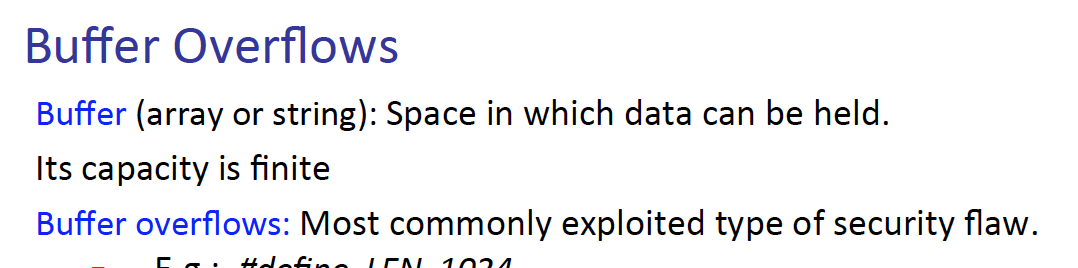
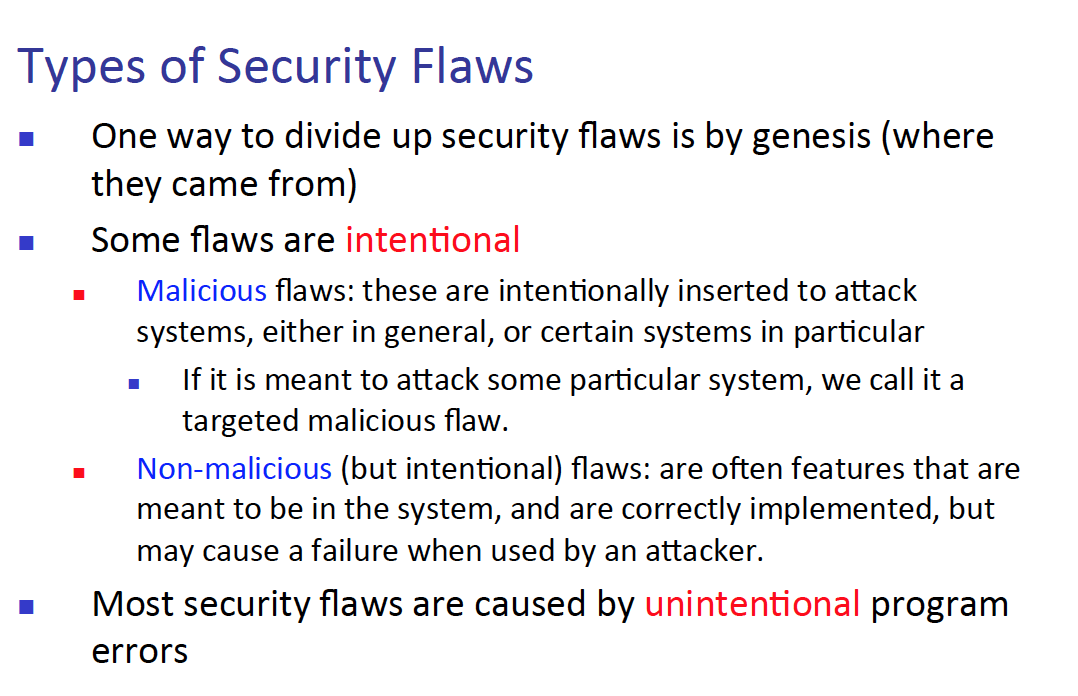
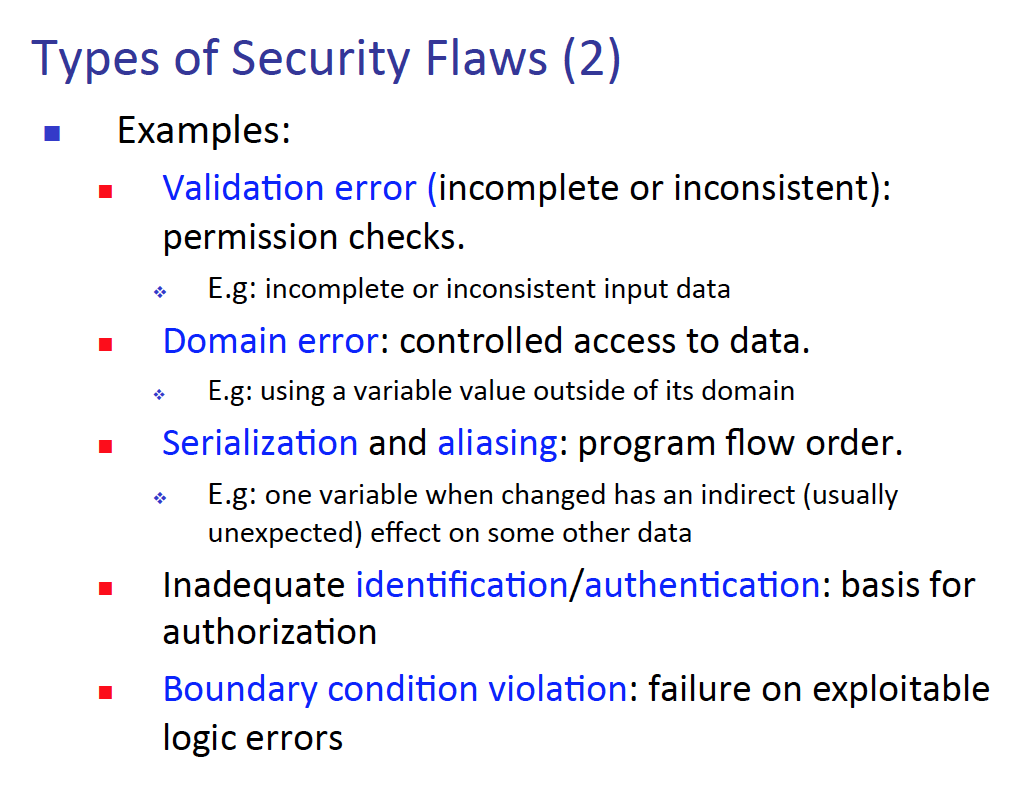
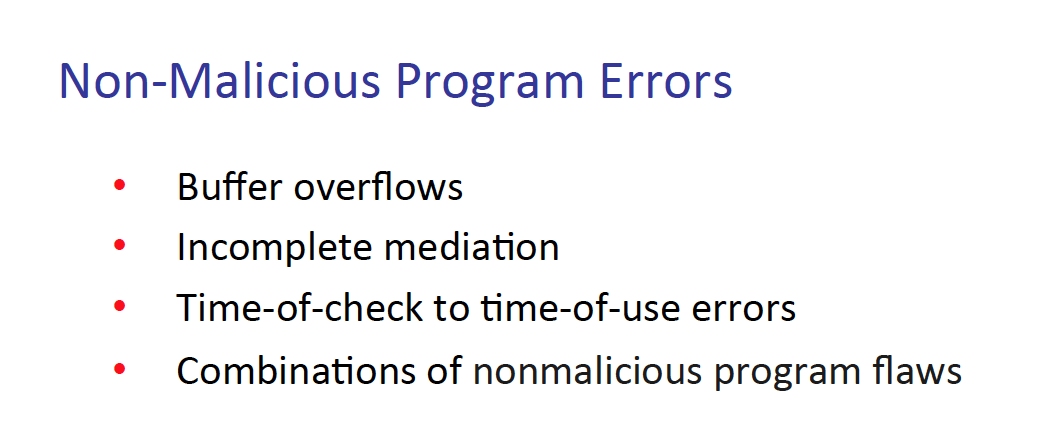
1. How can we temporally fix up the above problems? Also, is this a permanent solution?

* We can use the operation called patch, however they are not a permeant solution rather a temporal bandage. The reason for that is because some unexpected errors can occur because of the made patches. 

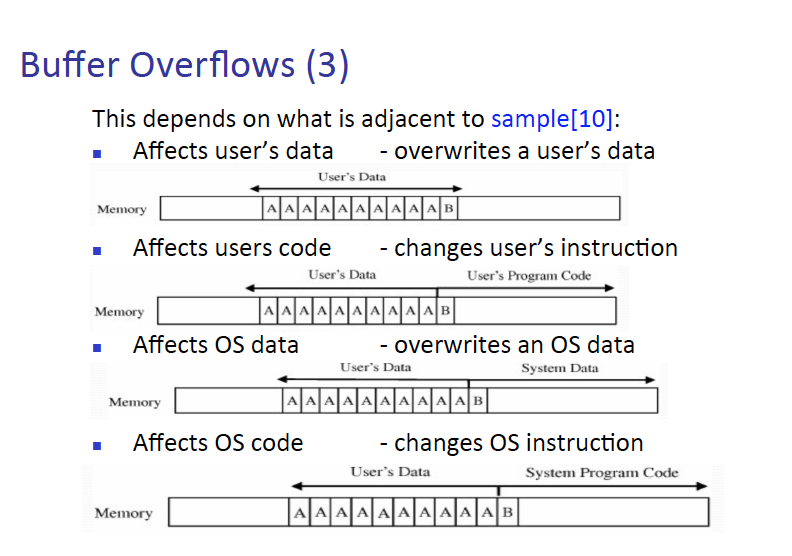
1. What are unexpected behaviors and why do we need to know them?

- Unexpected behaviors are when system or program behaves not in the way the developer expected. Also, the reason for why we need to know them are to understand program security better.

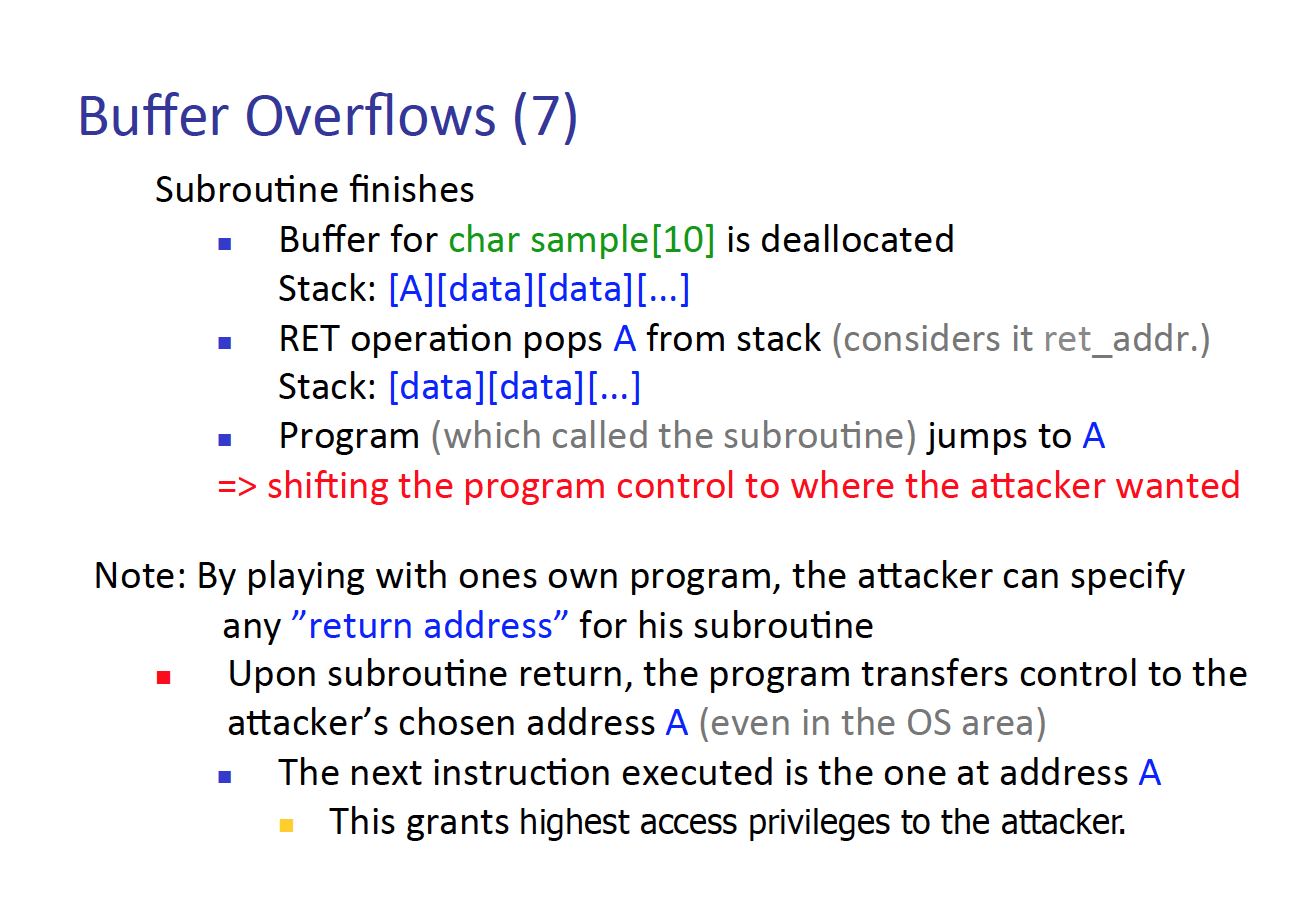
1. Name some security flaws and describe what buffer overflow is.

* Some security flaw is non/malicious intentional/non intentional errors. Also, validation error, domain error, aliasing, authentication, and boundary errors.   
  Also, buffer overflows happen when there is a fixed size of an array and the program inputs more data than the size of the length of an array. Then the final element in the array, will not be stored in the array rather, then some arbitrary area.

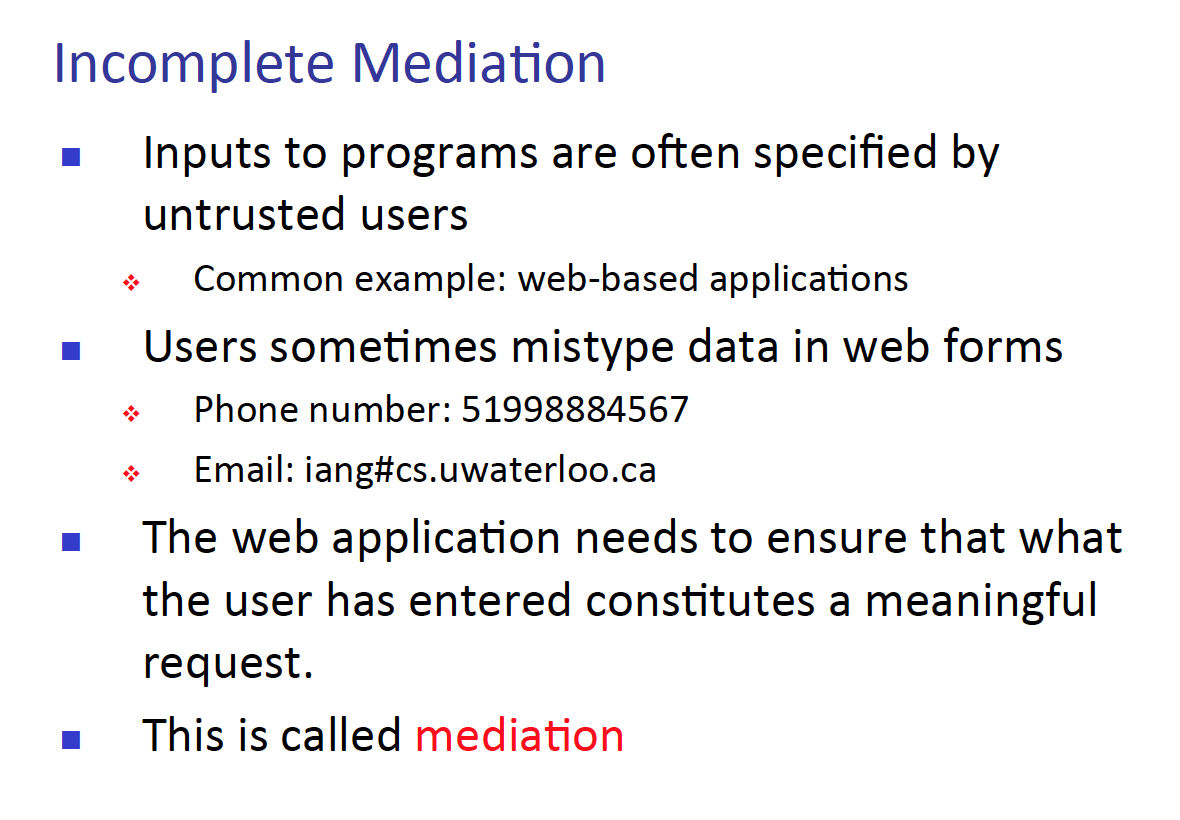
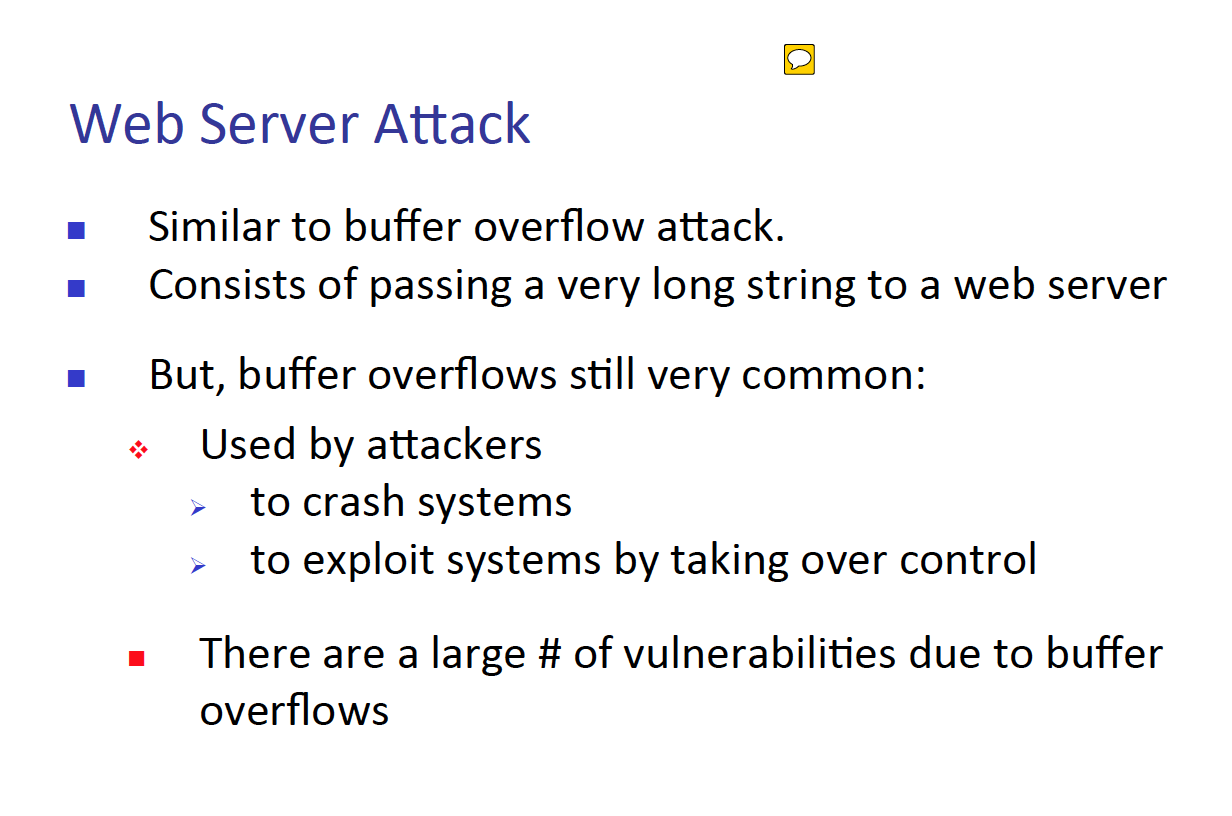
1. There are four places where overflown bit can go, describe each of them.

* 1) Affect user data – over write user data
* 2) Affect user code – change user’s instruction
* 3) Affect OS data – overwrite the OS data.
* 4) Affect OS code – change the OS instruction

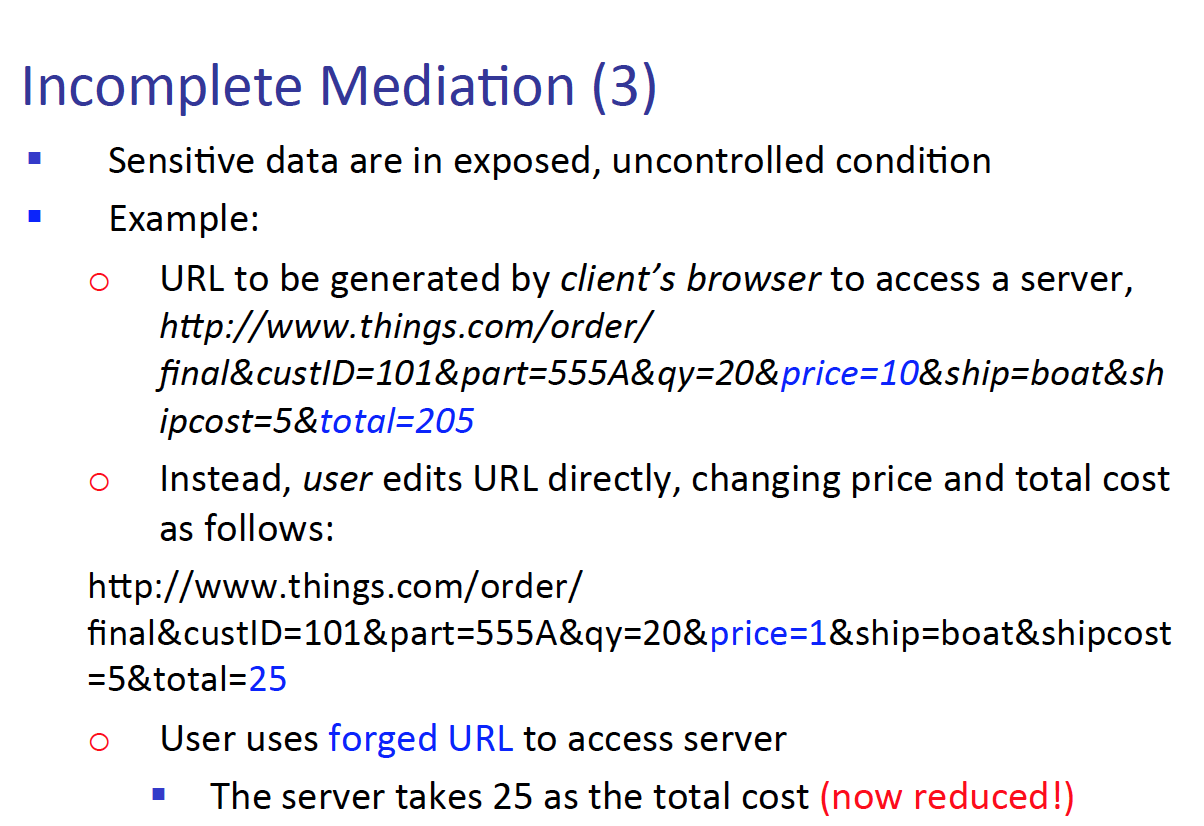
1. How can an attacker abuse the return address?

* The attacker might overwrite data where it specifies the program where to return. Normally the program will return where the user has pointed to. However, by abusing the return address, the attacker can take control of the computer. If the program returns to a process where it sends all of the data back to the attacker. Then the attacker will have all of the information.

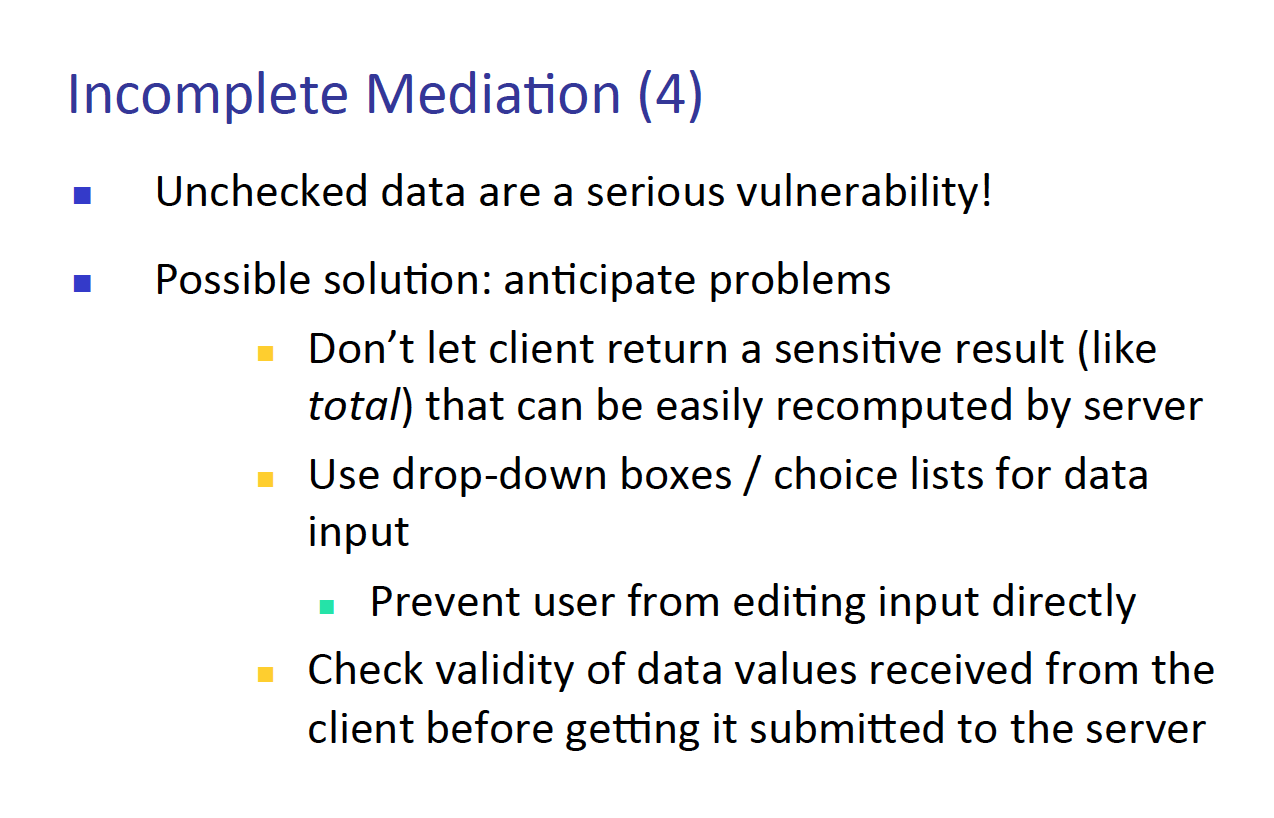
1. What is the main defense mechanism of web server attack?

* The main defense mechanism for web server attack is mediation. Mediation is something like a filter, such as filtering the user inputted data. To prevent such SQL attacks or buffer overflow attack those stuffs.

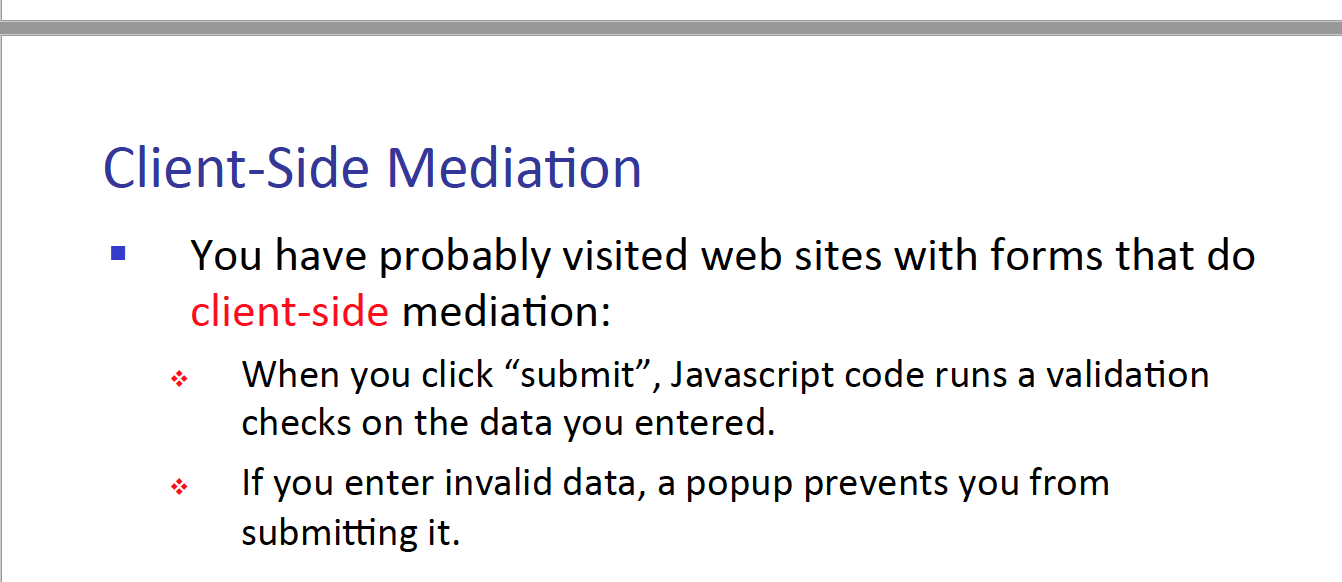
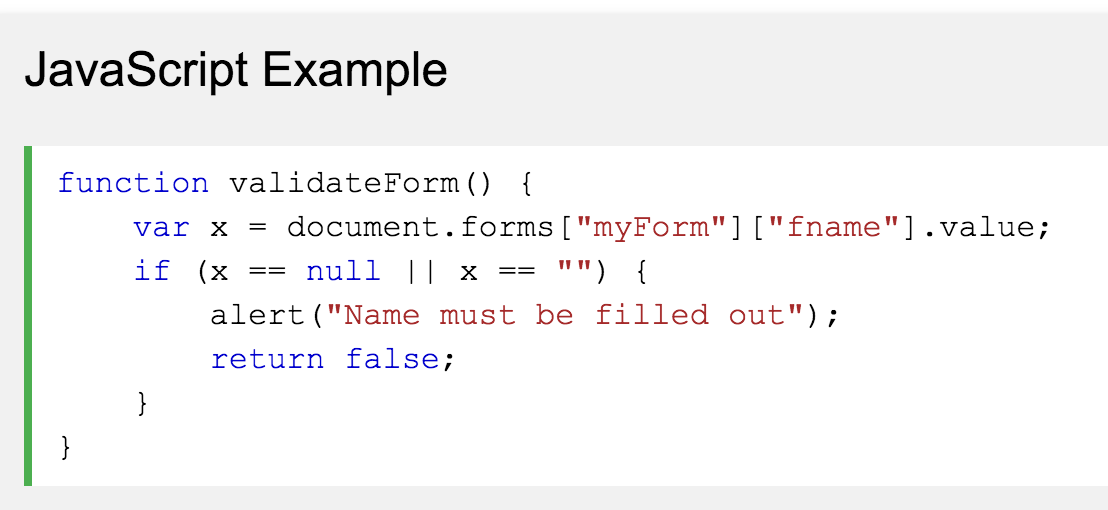
1. In incomplete mediation what kind of data are exposed?

* Sensitive data are exposed to the user, or the middle man and those information can explode the system.

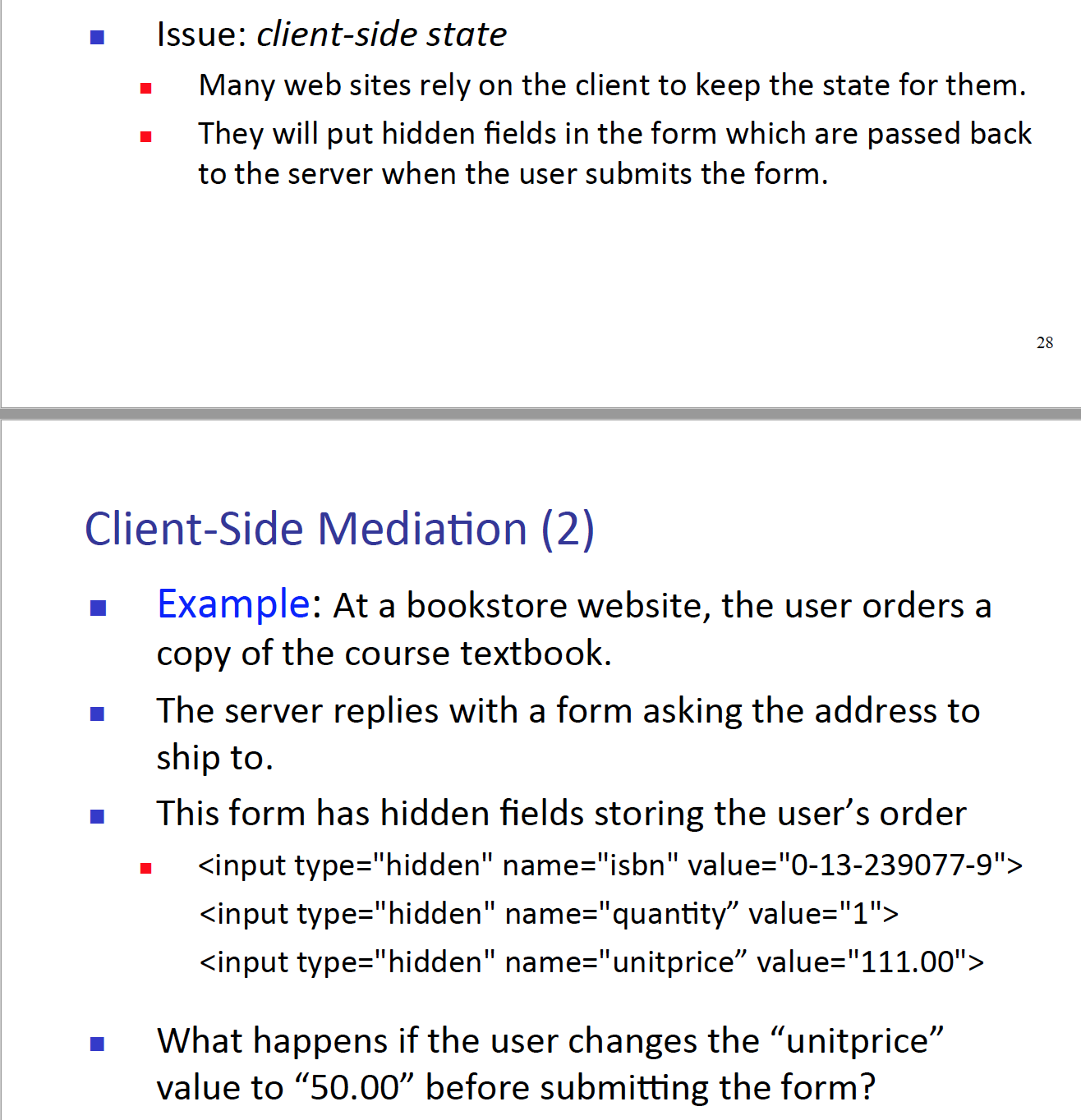
1. What are some possible solution for web mediation?

* Some possible solutions are client/server mediation. Client side mediations are when we filter the data that was inputted from the user at the client side (moment when the data is being inputted) and the server side is when the data is transferred over to the server, we perform filtering once again. Other solutions are limiting the user input choices – such as using dropdown boxes or bullet point boxes.

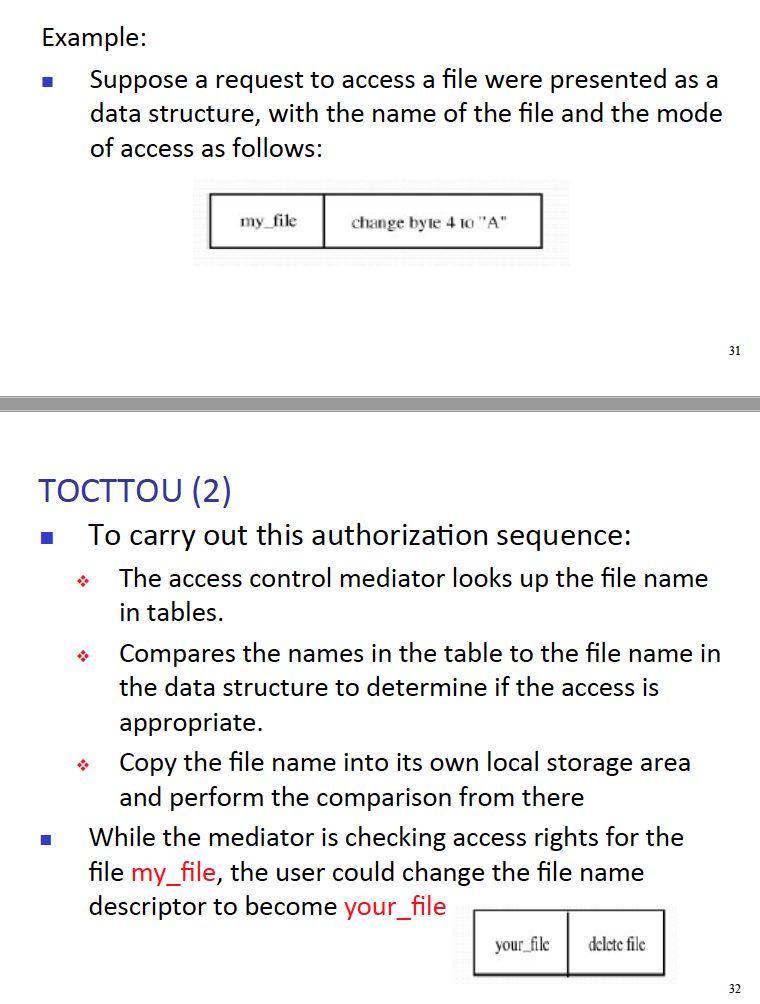
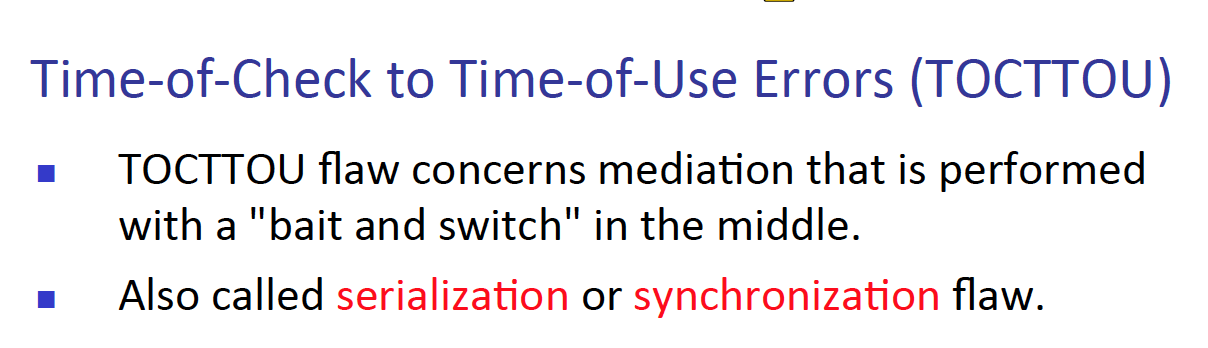
1. Example of client side mediation?

* Any filtering with java script can be an example. More preciously, we can specify the data type a function can accept and when the user inputs another data type the form would refuse that input.

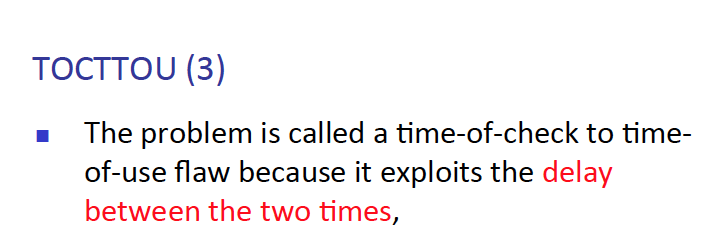
1. Is client mediation good enough?

* No, the cline side mediation is not good enough. The reason for that is because of the client side state is usually managed by the client. And a hacker who imposes as a client can put anything on the state.

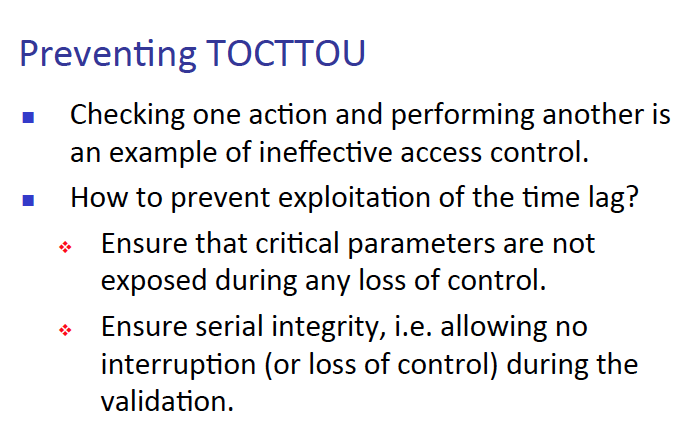
1. What is TOCTTOU, explain it (what is the other name of this?)

* Time of Check to Time of Use error (LOOOOL such a long, not needed name!) This is when hackers exploit the time delay between operations of one process to another. When operation A is happening and it needs x amount of time to access the needed resource, that interval is when the hacker can change the instruction of what kind of operations can be performed.

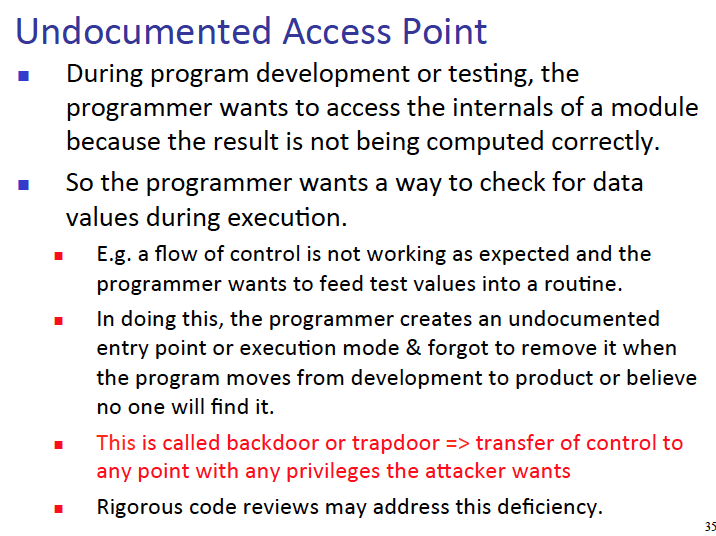
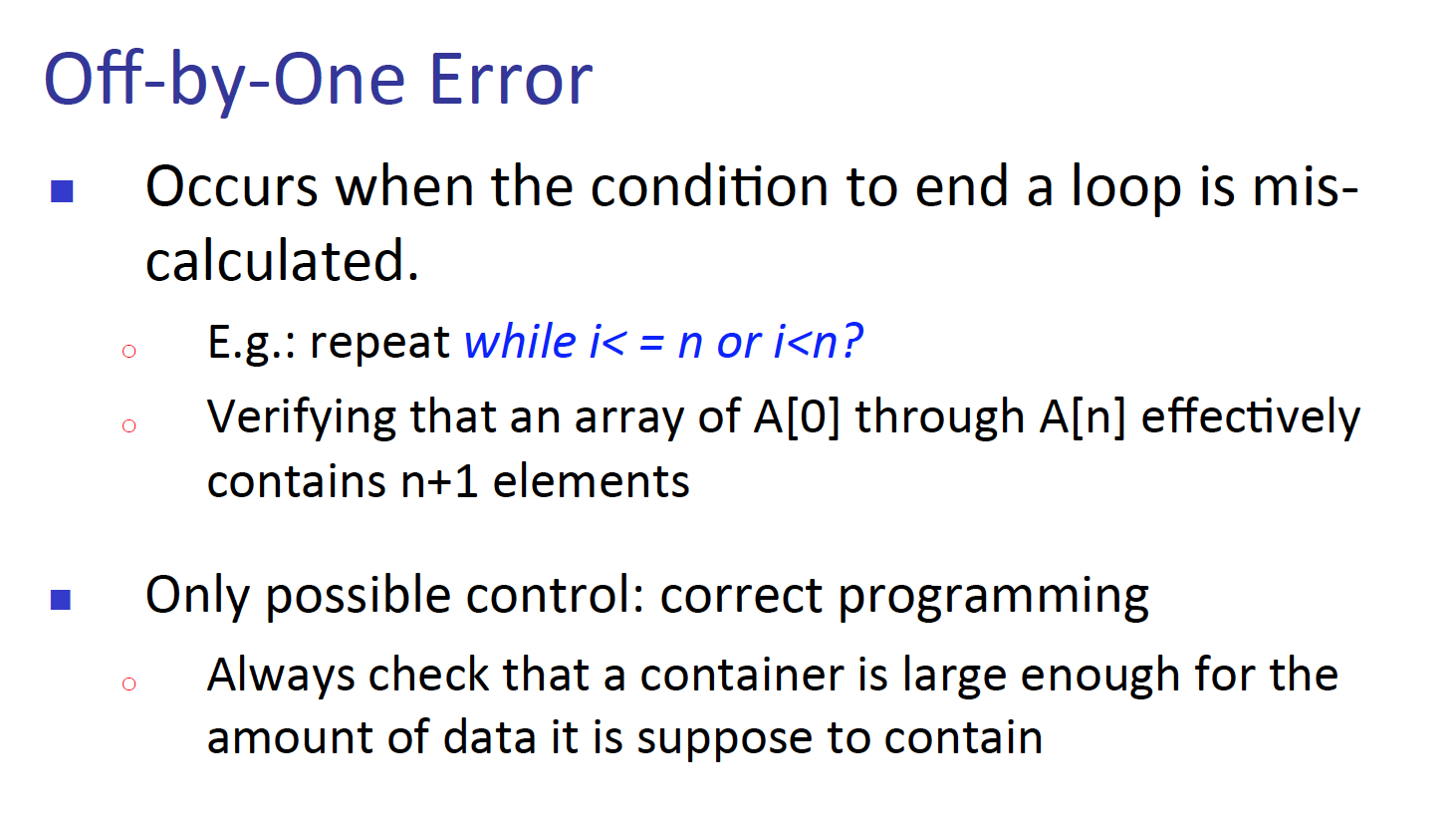
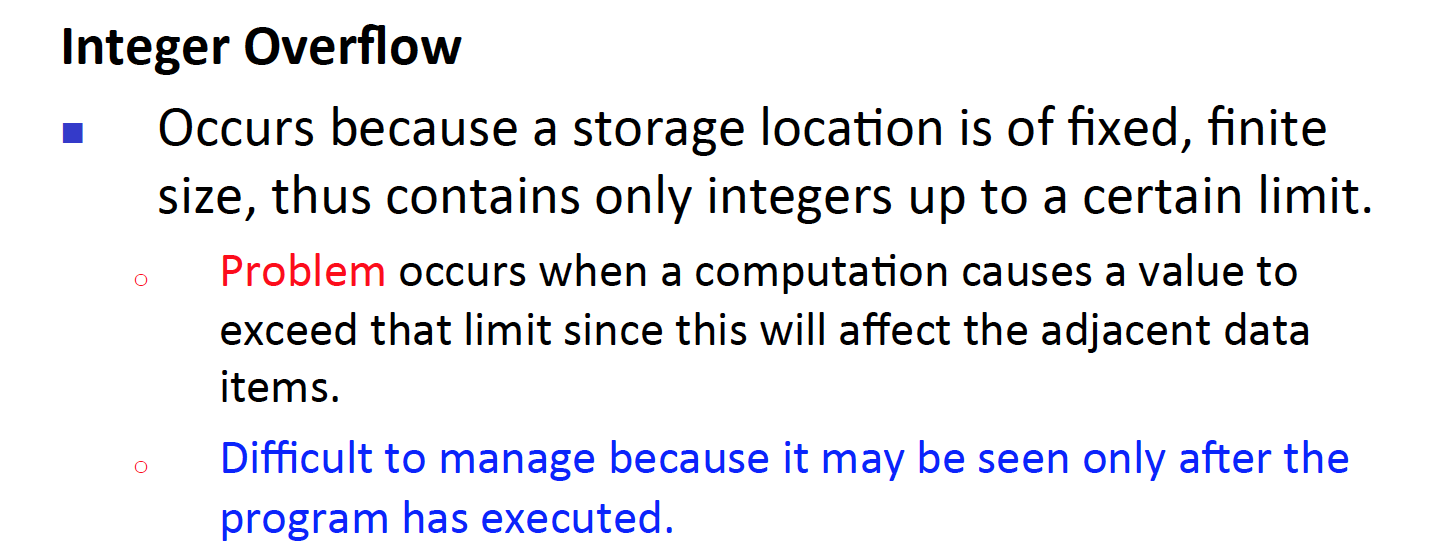
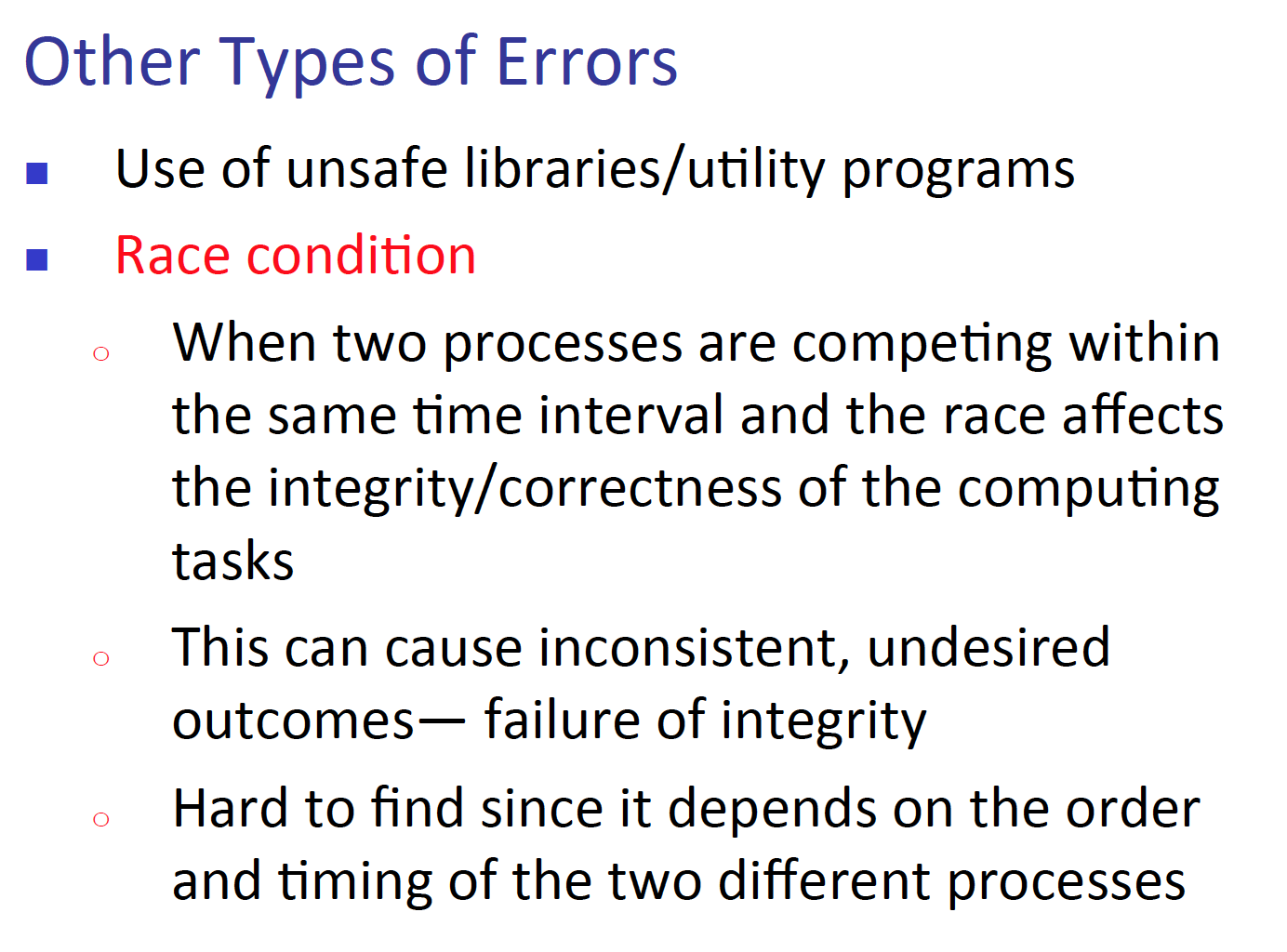
1. What does TOCTTOU exploit?

* Time of Check to Time of Use error – exploit the time delay that happens between operations.

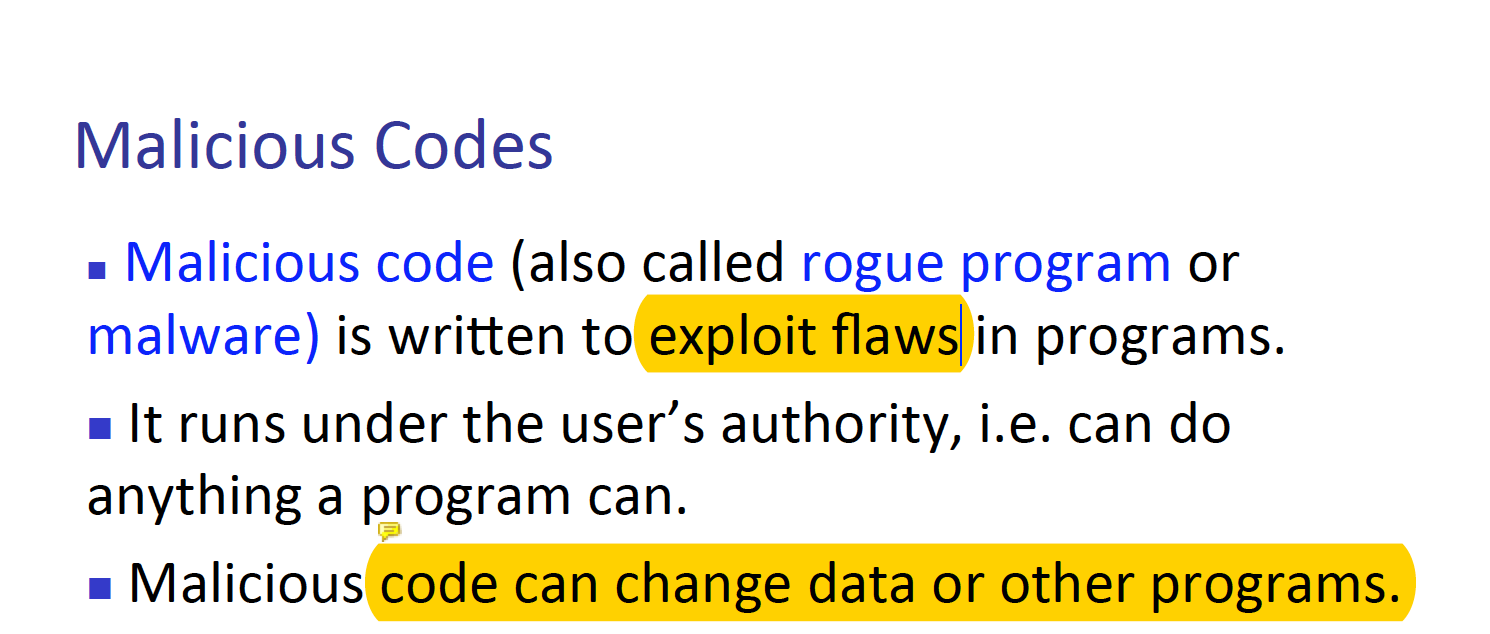
1. Example of preventing TOCTTOU?

* Make sure during those between operation time, there are no interruption happening and no sensitive data are exposed to the public.

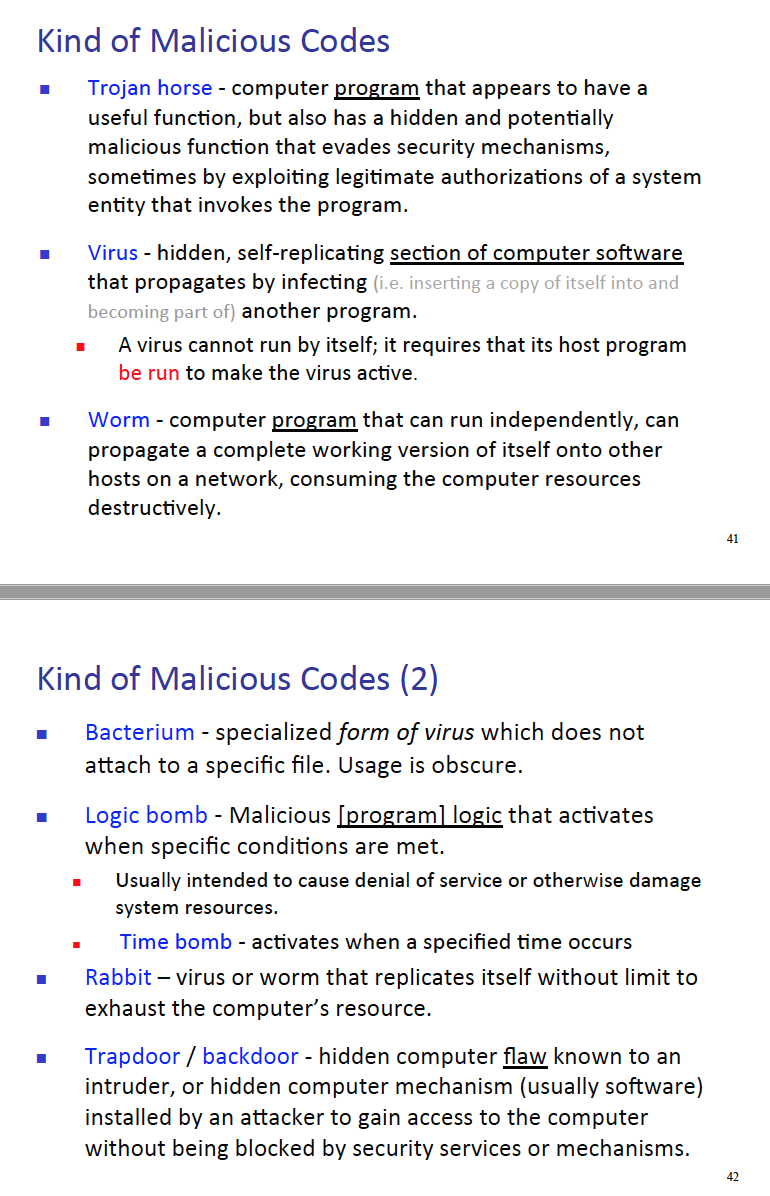
1. What are 1) Undocumented access point 2) off by one on bit error 3) integer overflow 4) Race condition?

* 1) When the developer makes an access point in the developing phase of a program, and never closes that hole, this becomes very critical access point. With this access point hackers can exploit any security flaw in the program. 
* 2) When a loop is go over the end condition by value of one.
* 3) This error is similar to buffer overflow, meaning there is a finite space of area that a data can be inputted. However, sometimes that space gets overflowed with data. And buffer overflow occurs.
* 4) Like how we learned in the OS class, when 2 process does not let go of one resource and they both try to finish their operation first. Race condition occurs.

1. What does malicious code exploit in a program?

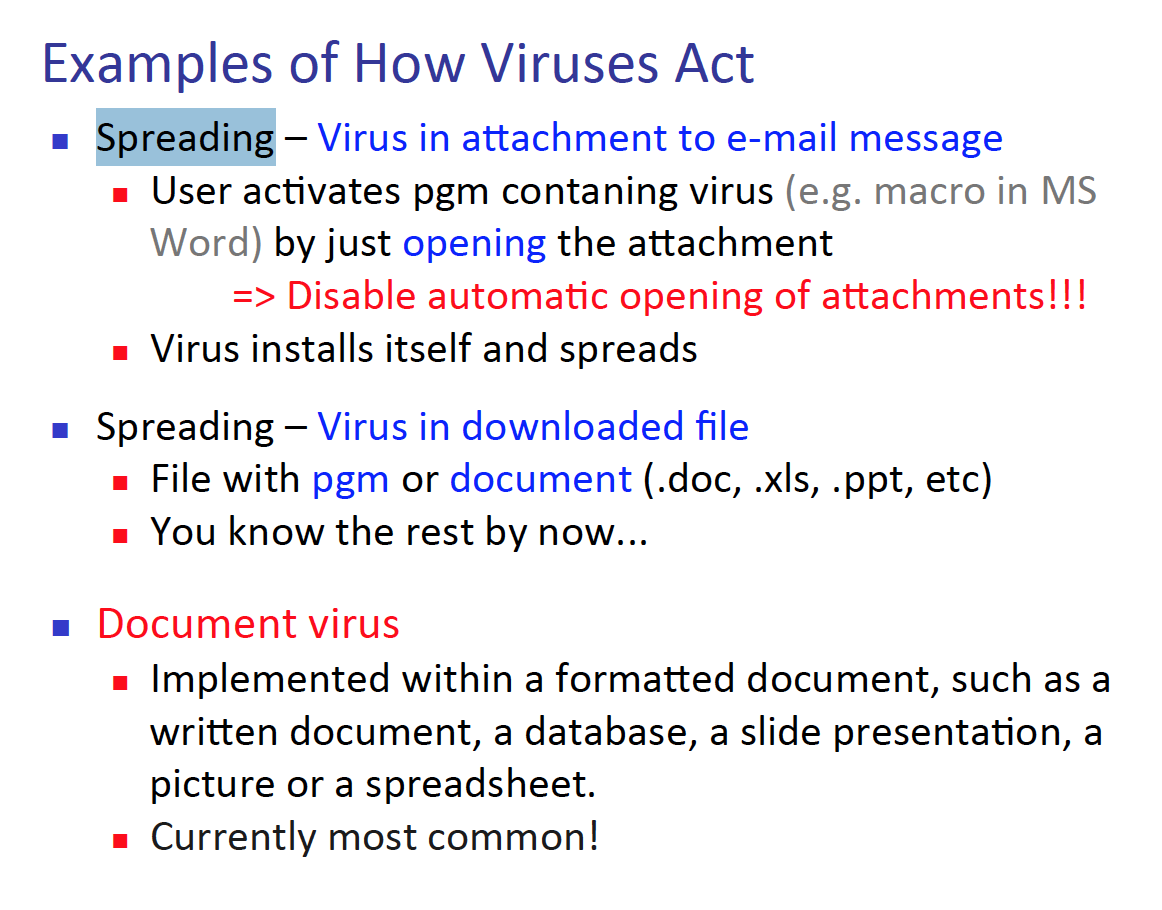
* Malicious code in the program exploit program flaw – this make sense since flaw is a problem in the program.

1. Name and briefly describe all of malicious type of code.

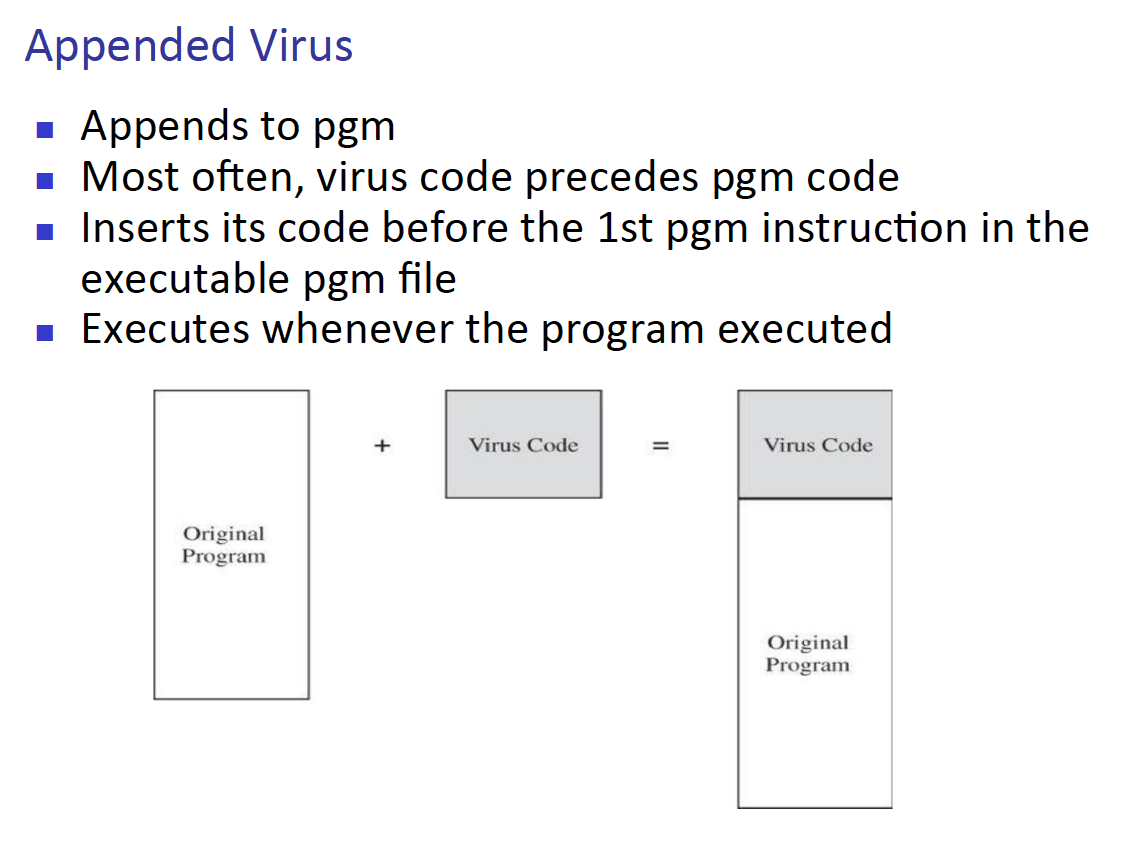
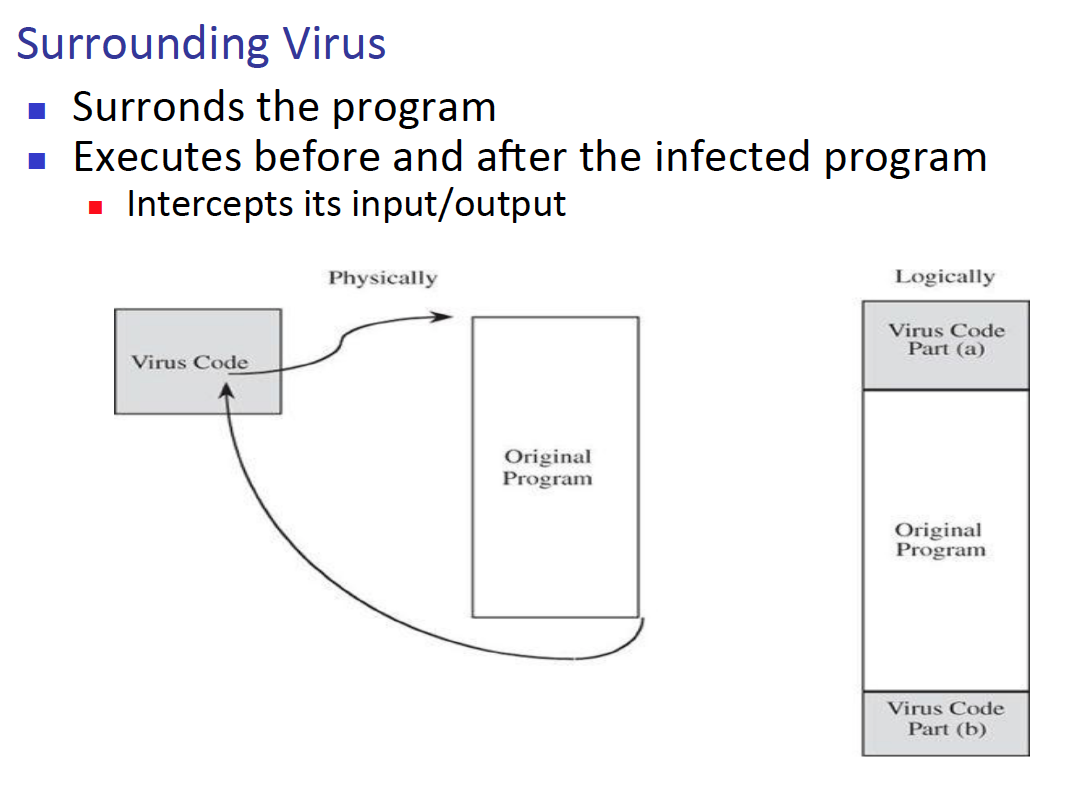
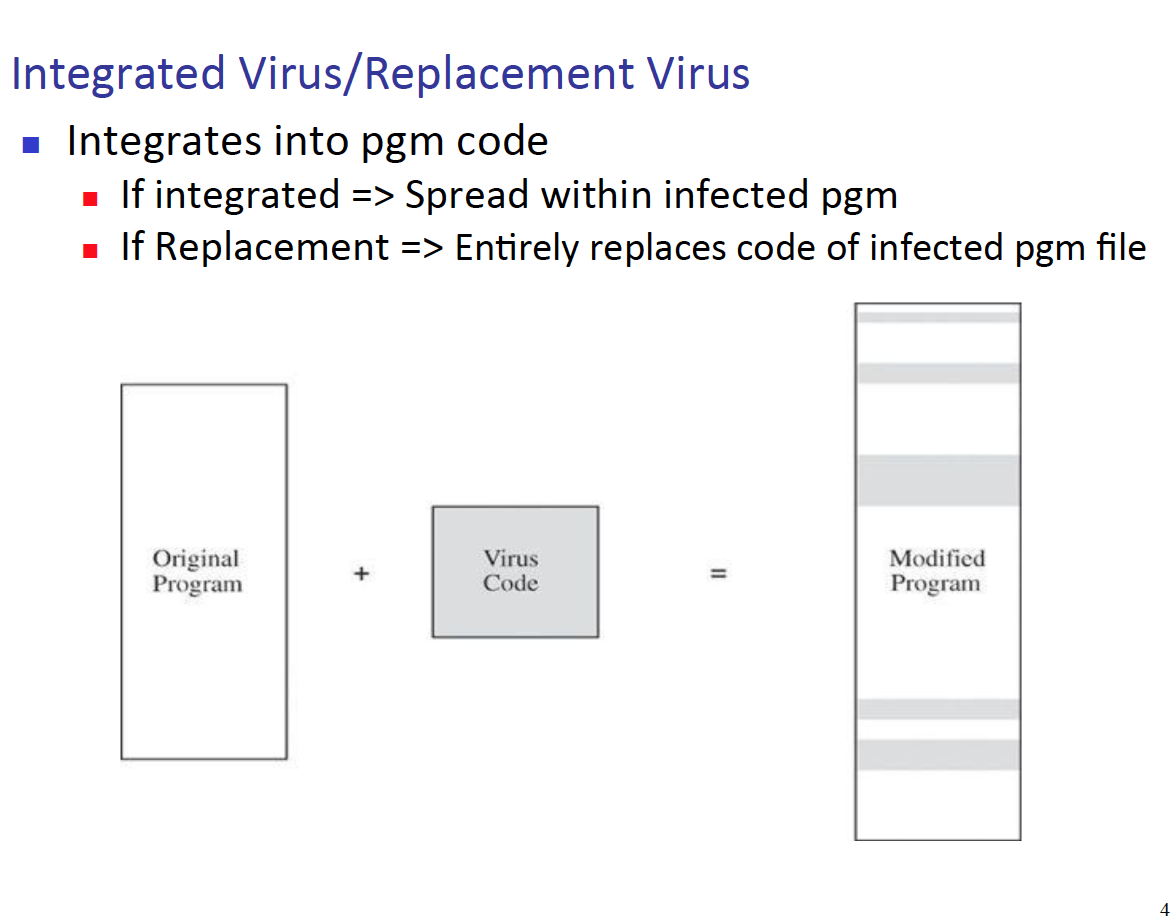
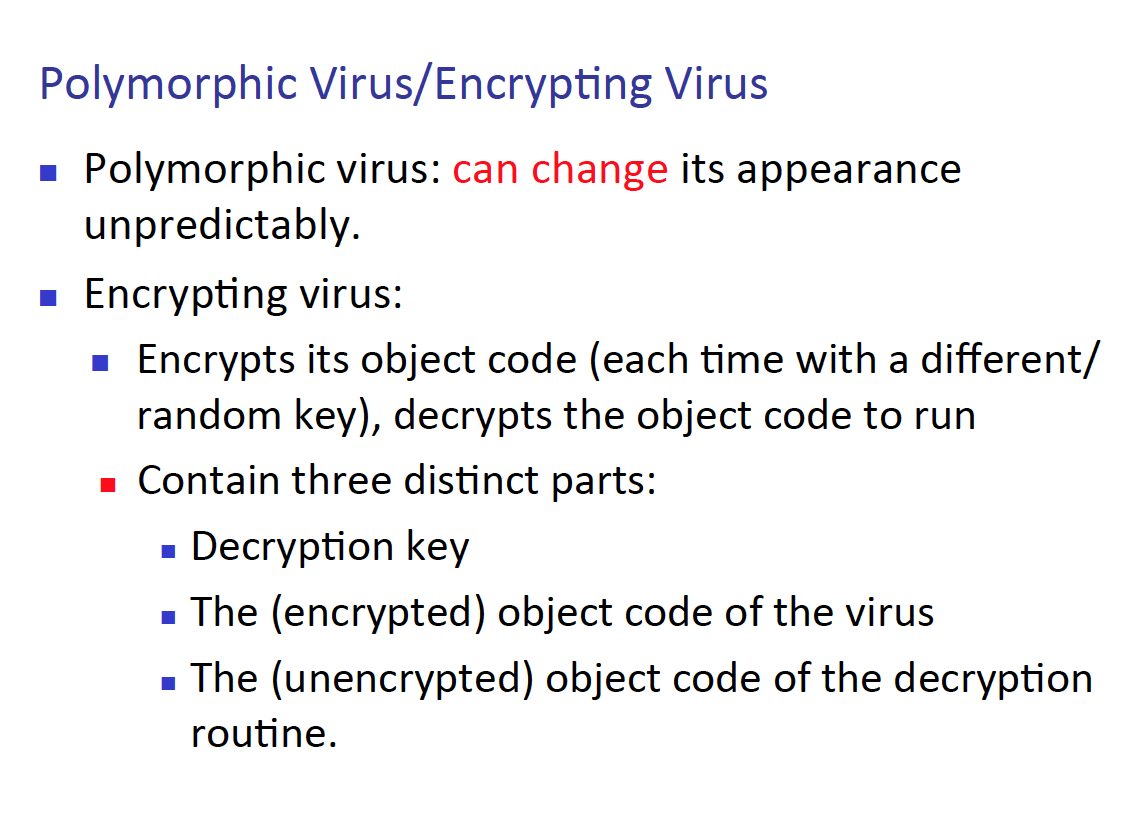
* 

1. How does virus spread from A to B?

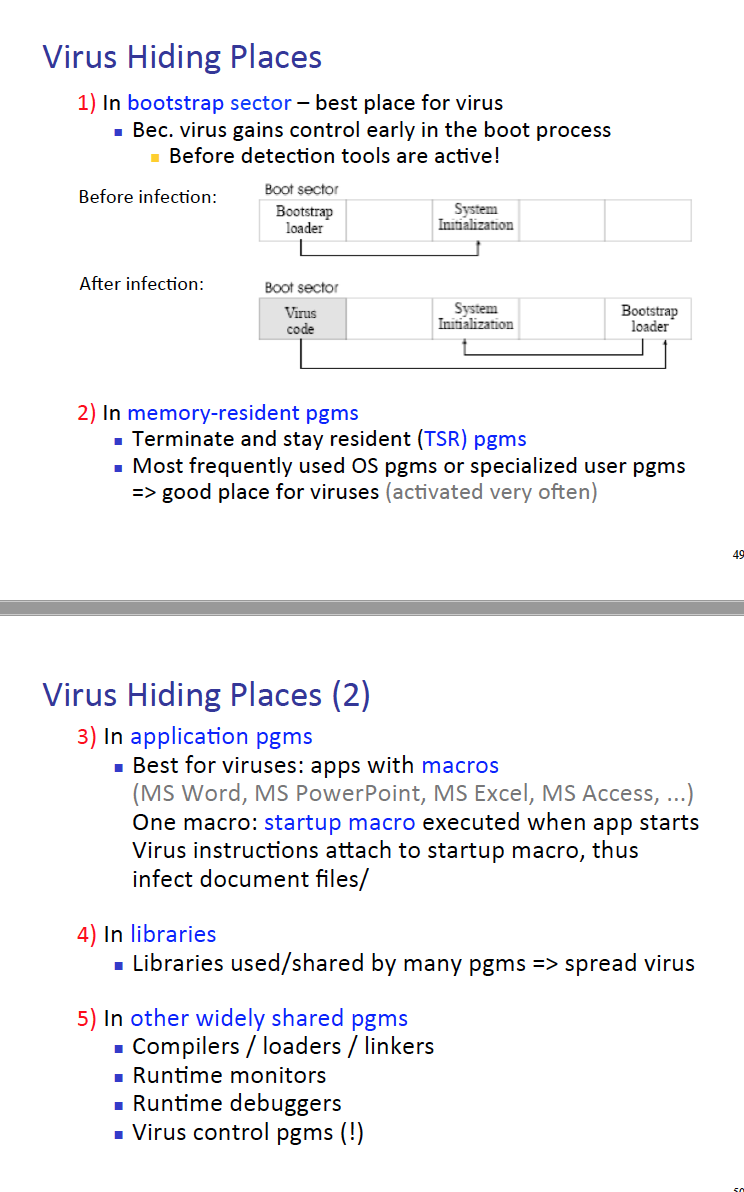
* There are many ways a virus can spread from one target to another target. Now days it is more done on the web, since the increase use of mobile devices have increased dramatically. Mainly, a virus can replicate itself, meaning it does not need any host to replicate it self (these are called worms and when they need some kind of execution for the virus to activate then it is called virus)



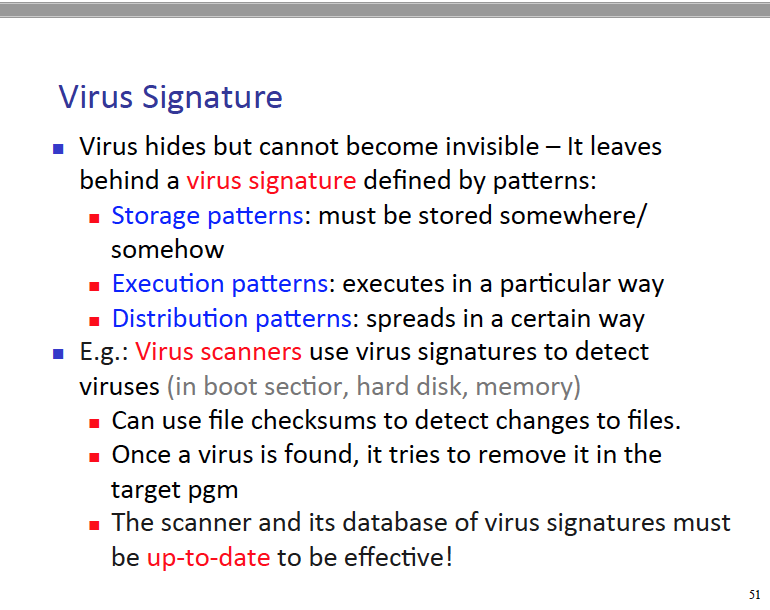
1. What are 1) Append 2) Surrounding 3) Integrated 4) Polymorphic 5) Encrypting virus.

* 1) Append are typical way of how a virus gets spread from one place to another – An attacker will attach a virus to a file. And when the file is opened, the virus will activate.
* 2) This is more advance version of append virus. This version of append makes the virus run, before and after running the program.
* 3) Malicious program is dived into parts, and integrated with the program, so while running the program the virus activates.   
  The virus either can be integrated or completely replace the original program.
* 4) When a virus changes form unpredictably, it is called, polymorphic virus.
* 5) When a virus encrypts the data then it is called, encrypting virus.

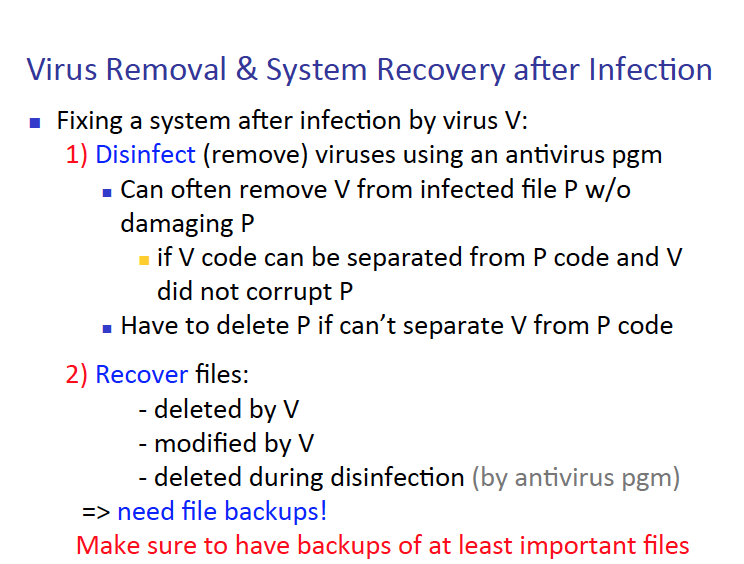
1. Where can virus hide?

* There are a lot of places where a virus can hide, but to describe it briefly some part of the program, or bootstrap (web application), library, document programs such as excel or word doc.

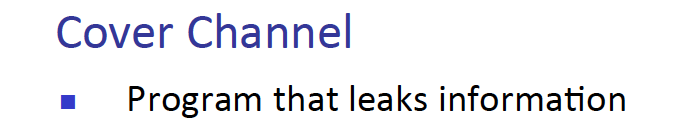
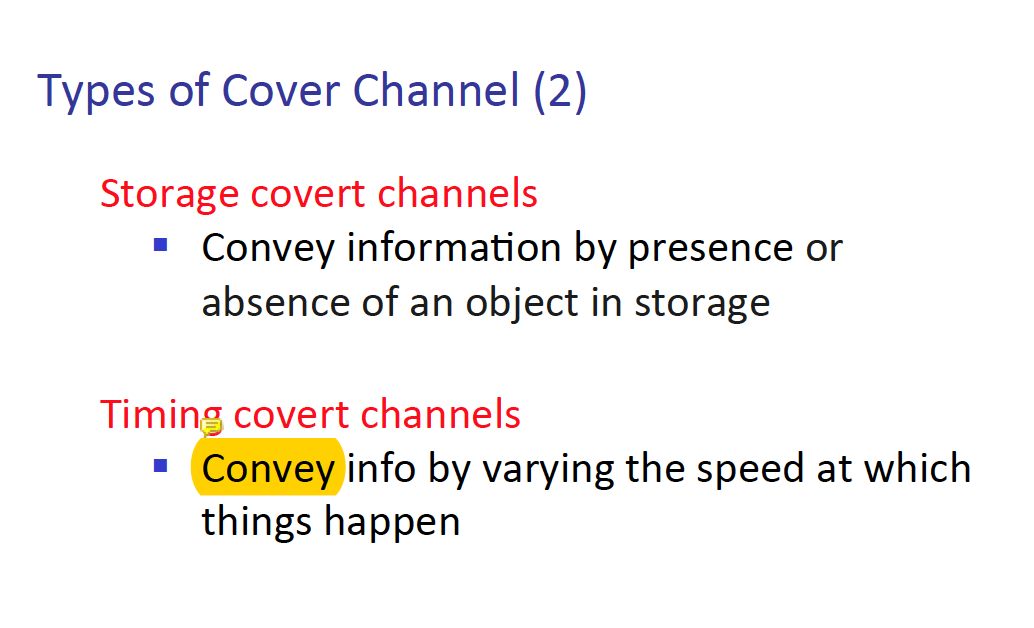
1. Can virus be invisible, if not what do they leave out?

* Virus may be able hard to find, but it never can be invisible. It will leave traces that a security program can detect and trace back to the root of the program. Such as patterns that can be studies and there are 3 type of patterns   
  1) Storage 2) execution 3) Distribution pattern.

1. Explain virus removal process and describe trap door and salami attacks.

* Removal 1) Disinfect the program, that contains the virus, other words removal of the virus. Then 2) Recovery of the system – if any files were deleted because of the virus we need a way to recover those files, more specifically backup files are needed in order to make the recovery happen.
* Trap doors -
* Salami attack -

1. What are cover channels and 2 major of cover channels - describe each of them.

* Cover channels are channels within the computer in which takes data and exploits them into the world. Other words leak the information.
* The two major cover channels are   
  1) Storage Channels – this channel look at the present of an object or not, then report back to the host, that is requesting the information.  
  2) Timing Convert Channels – this channel, report back to the main host, via time sequence of operations happening in the computer.

1. Example of storage channel?
2. What are 2 ways to detect cover channel, explain them.
3. Developing a secure software requires what kind of people?
4. Describe modulation and cohesion and coupling.
5. Describe peer review, hazard analysis, testing and, majority voting.
6. What are some reasons for software modification?
7. What is OS control for security and key characteristic of trusted OS?
8. Describe and explain ‘administrative control for security’.