­Jae Duk Seo

chapter 3 – programming security

1. **Suppose you are a customs inspector. You are responsible for checking suitcases for secret compartments in which bulky items such as jewelry might be hidden. Describe the procedure you would follow to check for these compartments.**

* I would basically document all of my actions in video or some kind of clear recording that shows me that if anything gets stolen from the bag, I can prove to the customer that I am not the one who stole an item in the bag.

Answer was very similar, the owner of the suit case can be in the present when I am, performing the search. But anyhow, this question does not so much on reflecting what we learned in this course.

1. **Your boss hands you a microprocessor and its technical reference manual. You are asked to check for undocumented features of the processor. Because of the number of possibilities, you cannot test every operation code with every combination of operands. Outline the strategy you would use to identify and characterize unpublicized operations.**

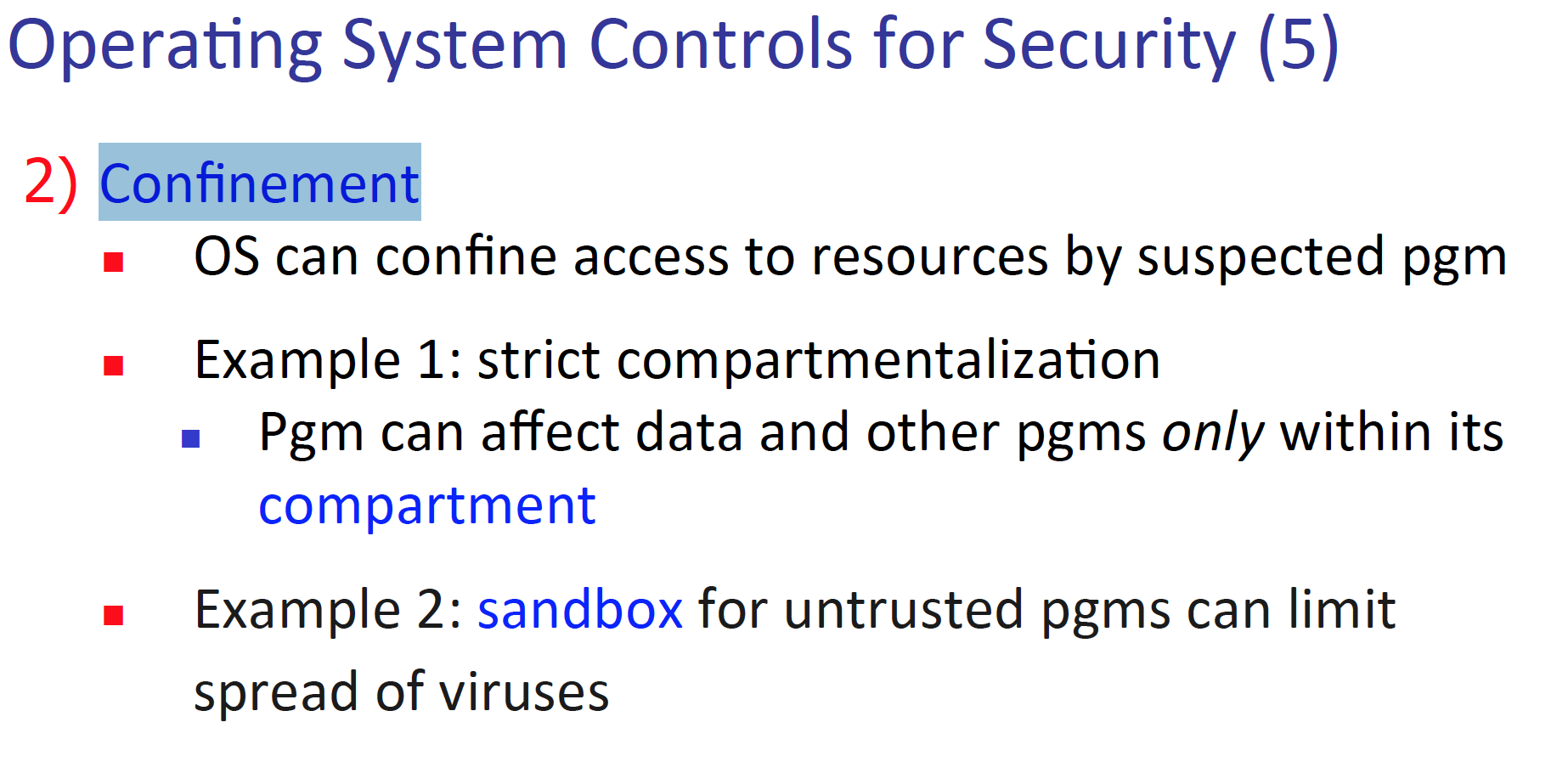
I would google examples of a situation where a microprocessor behaved unexpectly, if the search result is very recent. Then that implies that the manufacture is not aware of the situation yet, so it would not be in the manual.   
  
Note: This is an open question; there is no strict answer for this question. Use the technical manual to make a list of the microprocessor's operation codes and what their expected range of operands should be. For each operation code, randomly choose a few operands to test, some within the expected range of operands, some at the extreme limits of the range and finally pick a few that are completely outside the range.

**4. A program is written to compute the sum of the integers from 1 to 10. The programmer, well trained in reusability and maintainability, writes the program so that it computes the sum of the numbers from k to n. However, a team of security specialists scrutinizes the code. The team certifies that this program properly sets k to 1 and n to 10; therefore, the program is certified as being properly restricted in that it always operates on precisely the range 1 to 10. List different ways that this program can be sabotaged so that during execution it computes a different sum, such as 3 to 20.**

* Maybe man in the middle attack? Right at the beginning of the execution of the program, if the attacker gets hold of the variable. Then they can change the k value to 2 and n to 4 or something like that.
* During execution an outside subject (either process or a hacker) can change the value of the object (variable k and n). To make the code behave unexpectly.
* Main answer: if there is no mechanism for validating the integers k or n, the user can change those two integers any time after the program have started to run.
* a) Someone changes the source code before its complication,
* b) Someone patches (i.e.,) the binary object code while it is stored on disk before execution,
* c) During execution, an outside process patches the object code.

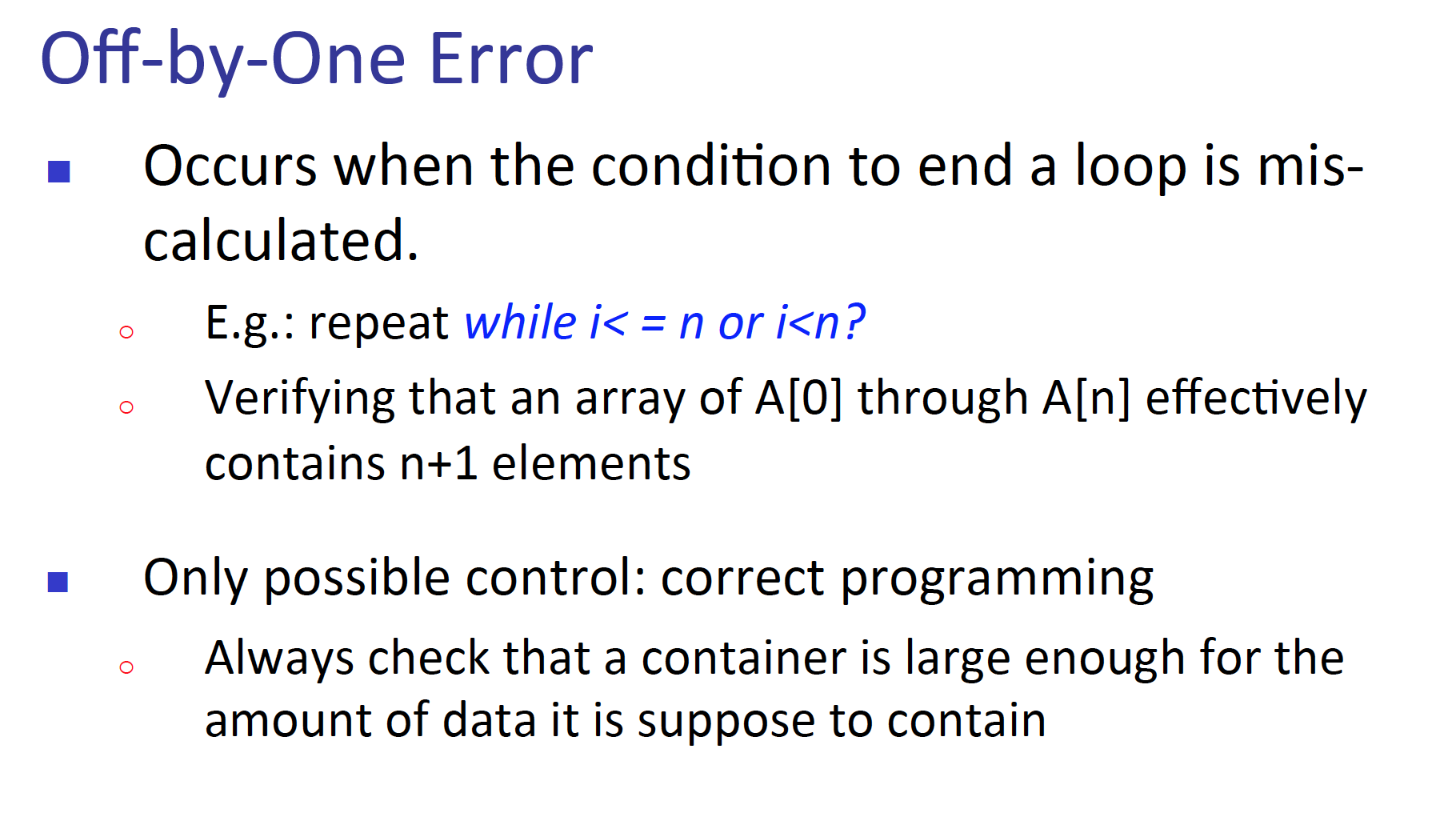
**5. One way to limit the effect of an untrusted program is confinement:**

**controlling what processes have access to the untrusted program and what access the program has to other processes and data. Explain how confinement would apply to the earlier example of the program that computes the sum of the integers 1 to 10.**

* First, let’s review on what confinement is.  
  So, we know that when OS restricts what resource can a process can access, we can call that confinement. To apply this concept to the program, above us. We can have separate variable typed int k and n. And set them to 1 and 10 respectly. Finally, give the program only read permission to those files. Then we can ensure, the program will compute the sum from 1 to 10, without any security breaches.

Assuming the only activity of the program is computing the sum from 1 to 10, confinement would achieve two things.   
First, the confining program would act as a filter between the callers and the untrusted program. A calling program would call the confining process, requesting to call the summation program. The calling program would have no direct access to the summation program.   
  
Second, the confining program would check the result to the summation program. In this simple situation, the confining process could check that the answer was exactly 55 (the sum from 1 to10).   
  
In a more realistic situation, the confining process could check the computation for reasonableness: considering the magnitude of the input values, values of other system variables, the name or owner of the calling program, etc., is the result reasonable? Are the requests for access to auxiliary system resources by the untrusted program reasonable? Confining programs such as described here do exist. They are generally called “wrappers” because they wrap the untrusted code in a trustworthy filter   
  
Jae: Never knew that wrappers are confinement programs, I though API wrappers were made only to be easily used by the user, but now if I think about it. API can be dangerous from time to time. And checking the final result of the sum program sounds like a great idea.

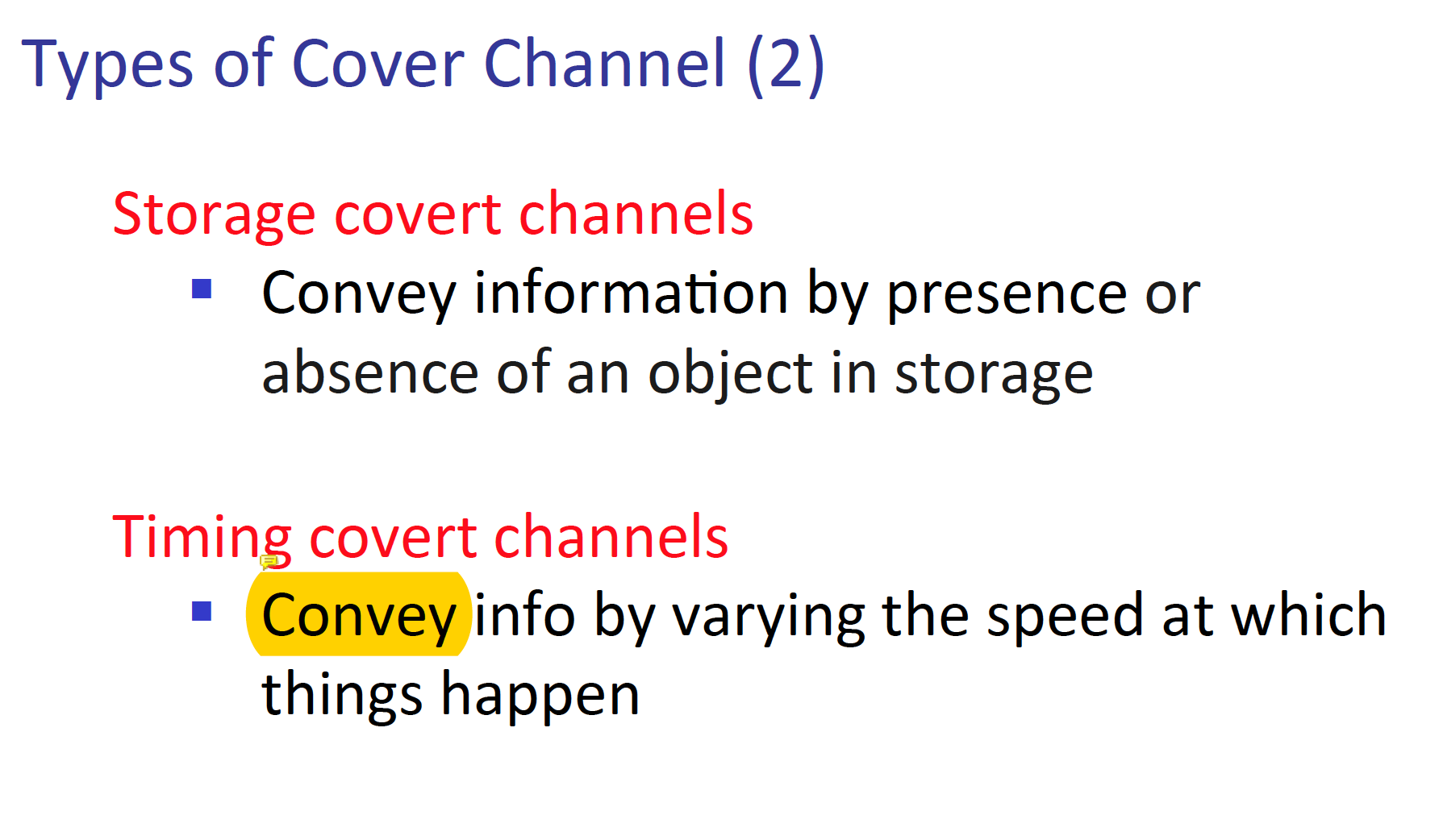
**6. List three controls that could be applied to detect or prevent off-by-one errors.**

**-** To know more about the off by one errors, look at page 36 of lecture 5.   
  
The error is when a loop or some kind of reputation algo go over the buffer by one value of the loop. Specifically, when the condition of the end a loop is over flown by one value.  
  
1) Correct programming is one way - check if the buffer is large enough for the amount of data to contain.   
2) Another way to prevent this error is to check the end condition before staring the loop.   
3) Finally, a confinement can be used to check the final output of the program. – If the array/buffer size is larger than expected we have detected the off by one error.  
  
- When we are iterating on an array, don't put <= sign on the condition, instead < sign, and the number after < sign is the number of elements in the array

- use enhanced for loop whenever possible

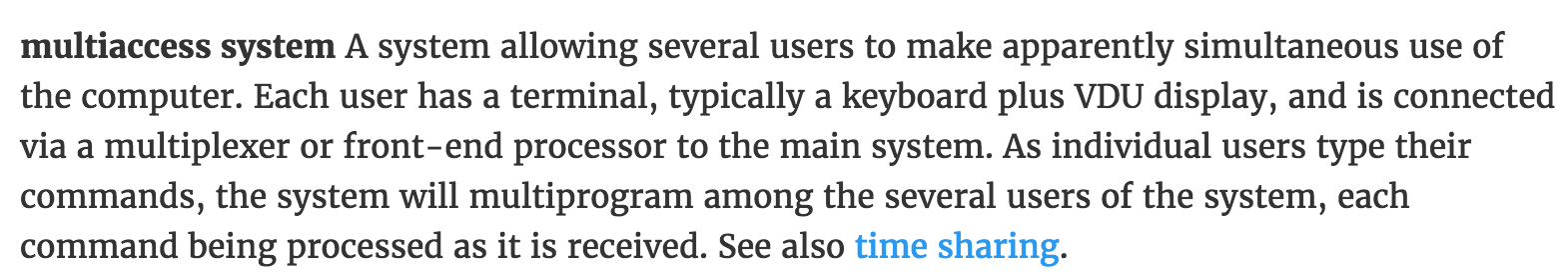
- go through the code before execution

**7. The distinction between a covert storage channel and a covert timing channel is not clearcut. Every timing channel can be transformed into an equivalent storage channel. Explain how this transformation could be done.**

- Please look at page 64 of the lecture 5 ppt. Timing convert channel take advantage of the time delay that happens between two processes. And storage extract information from the presence of an object in the system or not present in the system.   
  
covert - not openly acknowledged or displayed.

One way a timing channel can be a storage channel is, at one time an object is absent so during that time the time channel can report the absent of an object to a hacker. And after a time have passed, the timing channel can report a present of an object.   
Covert channels typically require access to a shared clock to time when bits become available in the covert resource and when bits can be replaced. Thus, even with pure storage channels, there is an element of timing. A covert timing channel works by modulating the time at which something occurs. But the something (which might be an interrupt or access to the CPU or unlocking a semaphore, for example)   
is itself a resource (the interrupt, the processing, or the semaphore),   
represented by a storage table entry. Thus, the table entry or the something itself becomes the shared resource visible to the two cooperating processes form which the covert channel is built.

**8. List the limitations on the amount of information leaked per second through a covert channel in a multi access computing system.**

- Let’s see what multi access computing system is.  
So, we know that different person accessing one host, or one computer. Now let’s think about the limitations on the amount of information leaked per second through a covert channel.   
  
The two primary factors that limit the amount of information that can be leaked are speed at which the retrieving process can recognize that a bit has been posted to the covert channel, and the speed at which sending process can be certain the retrieving process has had time to retrieve a bit. This time is the synchronization time between the two processes.  
  
Jae: So in other words, the time to write the data and the time to receive the data, if those two process are not in sync then hacking? Through a covert channel will fail.

**9. An electronic mail system could be used to leak information. First, explain how the leakage could occur. Then, identify controls that could be applied to detect or prevent the leakage.  
  
-** There are plenty of ways that email information could be leaked. One is man in the middle attack, host A send email to host B. But during the travel of that email, attacker C hijacks the email from A, save the content and send it to B.   
One way to prevent this attack, is to use encryption. Host A can use B’s public key and own private key to encrypt the email. Then only B can decrypt that email.

From organizations point of view, when an employee forward an email to someone outside of the organization. That can be considered as a leakage. To prevent this attack management can monitor the email process.

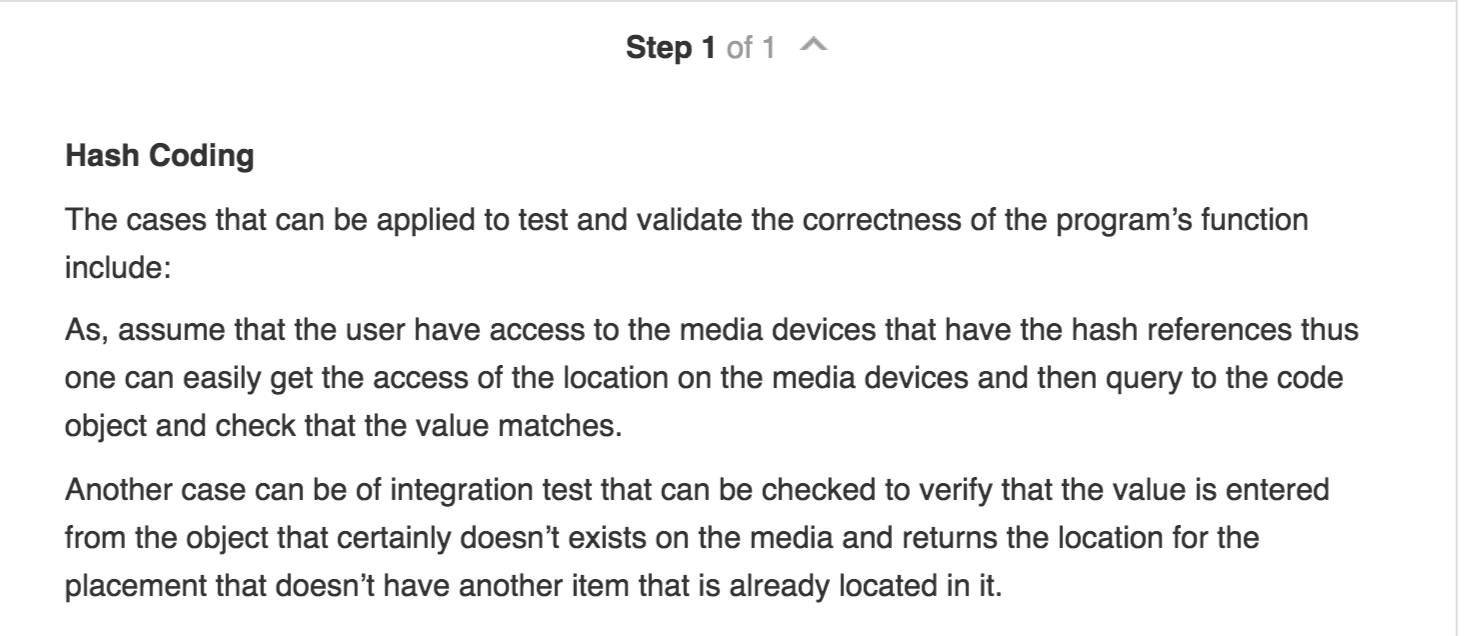
**10. Modularity can have a negative as well as a positive effect. A program that is over modularized performs its operations in very small modules, so a reader has trouble acquiring an overall perspective on what the system is trying to do. That is, although it may be easy to determine what individual modules do and what small groups of modules do, it is not easy to understand what they do in their entirety as a system. Suggest an approach that can be used during program development to provide this perspective.**

**-** A hierarchy approach of grouping each module on what they do and which class they are belong at, will help the situation since it will make it much easier for the user to see the higher view of the picture. So, the user can see the bigger picture as well as the details if they wanted to see which module does what.

This is a common problem across technology as a whole. Since most applications and solutions are built on a scope that would be incredibly difficult for an individual to understand on every level, we modularize. Using **layers of abstraction** to organize these modules makes it mentally easier to conceptualize. Project management uses this often, where requirements are taken; from requirements are made class diagrams; from class diagrams are made the actual pieces of the solution. While the more knowledge you have the better, it shouldn't be necessary to understand every piece of the lowest level to see how the solution as a whole functions; nor should it be necessary to understand the entirety of a solution in order to create a small feature of it.

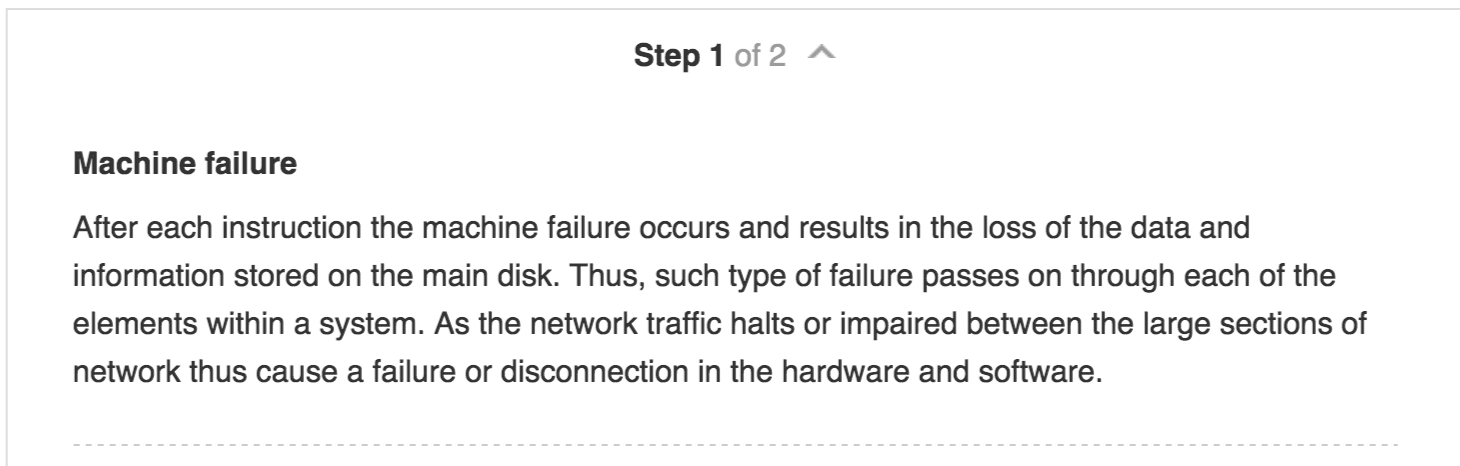
**11. You are given a program that purportedly (to claim) manages a list of items through hash coding. The program is supposed to return the location of an item if the item is present or to return the location where the item should be inserted if the item is not in the list.   
(Above is very similar to the function of storage covert channel.)  
Accompanying the program is a manual describing parameters such as the expected format of items in the table, the table size, and the specific calling sequence. You have only the object code of this program, not the source code. List the cases you would apply to test the correctness of the program’s function.**

**-** What does it mean by the object code? – black box or something very similar to the black box situation? – whatever that means.

Some situation where we want to check the correctness of the program is when. There is no present of the program, the program is not present at the location. I have no fucking clue, on what the answer means LOOL. 

**12. You are writing a procedure to add a node to a doubly linked list. The system on which this procedure is to be run is subject to periodic hardware failures.**

**The list your program is to maintain is of great importance. Your program must ensure the integrity of the list, even if the machine fails in the middle of executing your procedure. Supply the individual statements you would use in your procedure to update the list. (Your list should be fewer than a dozen statements long.) Explain the effect of a machine failure after each instruction. Describe how you would revise this procedure so that it would restore the integrity of the basic list after a machine failure.**

**-** A situation where this system can fail is when, the user gets the man in the middle attack. When the user wants to know if a certain object is located at certain directory. The user will make a request call to this system, however if a man in the middle. Gets the information. Then attacker will know if a certain program is present or not. 

**13. Explain how information in an access log could be used to identify the true identity of an impostor who has acquired unauthorized access to a computing system. Describe several different pieces of information in the log that could be combined to identify the impostor.**

**-** Maybe the pattern of what the user does after, they have been authorized. This can be different for a real user and another someone, the real user might have specific reason for accessing the system. And maybe another attacker will come and perform different operations.

**Questions to 633 TA**

1. **Tref - Is this the first enrolment set or is this the verification set?**

Use the Ter set for the enrolment set

phase of your system, and the rest for the verification phase.

1. **Compare the first (enrolment set) to the rest five other 2 - 6 verification set.**

**- I did it the opposite way. Meaning, that this is not the correct way. For the first set compare with the. Rest of the set.**

**3) Total number of verification trials - The number of this is different from FRR and FAR?**

**specifically, for FRR - Compare to own 2 - 6 set this would be 500 \* 5, because 500 data set for each set and we have five set. – 5 for FR**

**For FAR we would have 4 \* (500 \* 5) which is 4 \* 2500 = 10000, since we have 4 users and each of user have 2500 data set. (Which is their own verification set 2 - 6) – 25 for FA, why is this 25? Should it be 20? Since each user have 5 comparisons and there are 4 users to compare against. So 4 \* 5 = 20.**

**^ NO NO NO the verification number for the FAR is 25! WHY?**

**Since we compare 5 verification set for 4 users? Isn’t it 20?**

**4) For Dwell time we have 2 Dwell time, can we only use one Dwell time which is first key Dwell time?   
- No Second Dwell time.**

**5) In the email you wrote there is a word called "scan code" - cannot find anything related to this in the lab 2 pdf.**

**- Scan code is the key code (We do not use it).**

**6) Can I see the output the part 2 of the program, such as the derivation value and the FRR FAR each for comparison.**

**- Derivation is around 70, 67 (The value for** Digram **is NOT around 70 and 60, it was more like around the value of 500 – 600. )**

**- Monograph around 178**

**FRR and FAR is around 0.7 ~ 0.2**

**Also, there 25 sets   
the first set is comparing to user itself and the other 4 is compare to other user.**

1. The user id have to be entered while running the program.
2. The derivation is something like the array retuned with 5 elements.
3. User1 or User2, then the file name of the file which the user want to access, then finally the right (mode) of which the user is accessing the file.
4. For the files, we can creating any random files.