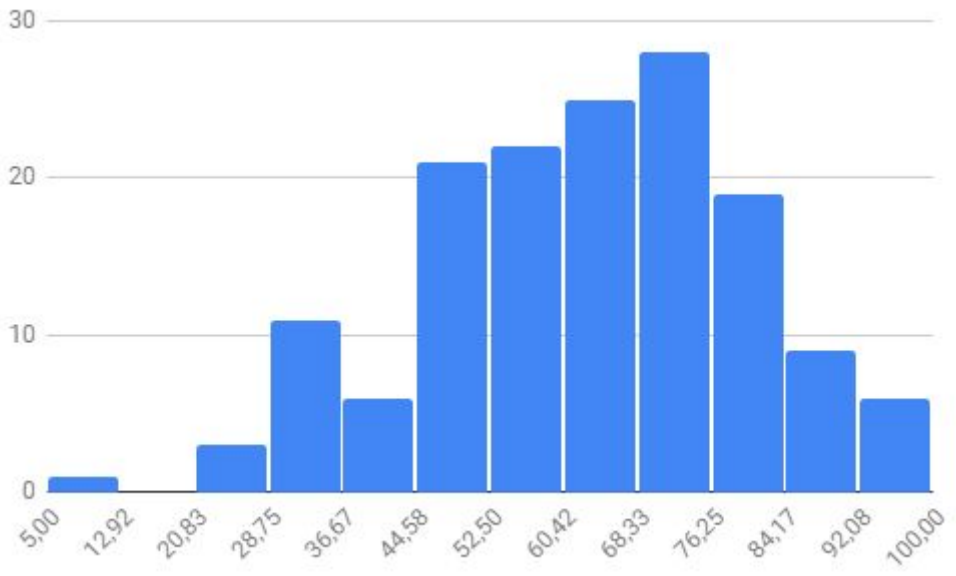
COM-301 : Computer Security
MIDTERM - 29th October

Grades distribution in Midterm



8 people above 90 this time - Mean of the class 62,8. 5 points above the 1st Midterm)

If you have been below 50 in both exams, please come to the exercise sessions. Also you should seriously consider asking for office hours to help you understand the course concepts.

.

MREs

(Most Repeated Errors)

General Advice

- Please read the instructions carefully. When it says at most 3 lines, you should not write more than 3 lines.

Q1 - True or False questions

MRE1: The best idea to keep a system safe is check that no input is trying to do anything malicious before letting any function run. ← this is FALSE
It is NOT a good idea to check that nothing is wrong. Remember, always check if the input is within the "universe of good things". Checking that it is not bad things does not provide any guarantee. You cannot enumerate all the bad things! Some are unknown.

MRE2: Having two security controls one after the other provides better security than using the security controls in parallel. **← This is TRUE**
Having two security controls one after the other provides the security *of the strongest one*, since you have to break both to attack the system.
Having two security controls in parallel provides the security of *the weakest one*, since you only have to break that one to attack the system.

MRE3: Some trojans add their code to that of existing executables residing on disk ← This is FALSE.
Trojans do need a host program to be executed, but they are *always* on the same program! (the program that "appears to perform a desirable function but it also performs undisclosed malicious activities") They do not infect any program in the disk.

Q2 Multianswer

MRE1: Malware: Once it has infected a machine the BadAss worm sends itself to all of the addresses in the Address Book of the user. This may cause…
"A Denial of Service on the computers of the infected users' contacts" is a wrong answer. Each of the contact's computers would receive one email. This barely can cause a problem for them. The correct answer was a Denial of Service on the Internet. Routers have to deal with the traffic of every infected users sending to all possible contacts. This is heavy traffic (see the example of the Slammer Worm - slide 32 here https://moodle.epfl.ch/pluginfile.php/2456736/mod_resource/content/0/COM-301-More%20attacks.pdf).

MRE2: Malware - The BadAss virus attaches itself to the Chrome browser. Whenever a web requires a login, the browser gets the password stored in windows password manager. The virus steals the user's passwords stored in windows password manager. Who is acting as confused deputy.
Here Chrome is acting as confused deputy. The BadAss virus is using the fact that Chrome has privileges to access the windows password manager content to steal the user's passwords. For instance, if the BadAss virus was infecting MSWord, it would not be able to steal any password.
(See slide 31 here:
https://moodle.epfl.ch/pluginfile.php/2469225/mod_resource/content/0/COM-301-More%20attacks%20-%20animated.pdf)

MRE3: Chinese Wall Policy
The Chinese Wall Policy does not allow information flow *between* items with labels in the same conflict set. Working with the same clients as before does not generate a flow between items. Previous clients are included in the set of possible future clients.

(See slide 62 here:
https://moodle.epfl.ch/pluginfile.php/2316223/mod_resource/content/1/COM-301%20-%20Security%20policy%20models%20-%20handouts.pdf)

MRE4: Using only one vector (false, true) as input is a good testing strategy.
This strategy is not good, regardless of whether we find the bug or not, a testing strategy with just one vector is never adequate. The fact that there is a lucky case does not make the strategy good in generalb. (The hint was very relevant, please read the hints.)

Q3 Short answers

MRE1: Use hybrid encryption in the OTP case
This is wrong in two senses:

- First, we cannot encrypt 1Mb with asymmetric encryption. Recall that there are no "chaining" methods for the assymetric case. Therefore, we can only encrypt messages smaller than a block which depends on the key size (e.g., 1024 bits, 2048 bits, 4096 bits, all of them much smaller than the Mb!).

- Second, if you are encrypting the OTP key with an asymmetric key, then your security is reduced to that of the asymmetric encryption! You are just losing the advantages that OTP gives you. (See MRE2 in Q1, the adversary just needs to break the weakest of the mechanisms!

MRE2: Encrypting the passwords
Many answers said "symmetric encryption requires a shared key". Note that in this case, the key is shared between the password administrator and himself! The user never sees the key that encrypt the password. The problem is that the key is stored along the passwords, so stealing one means that you can steal the other effectively providing not security. (See slide 58 here:

https://moodle.epfl.ch/pluginfile.php/2325213/mod_resource/content/1/COM-301%20-%20Authentication%20-%20animations.pdf)

MRE3: AES or AES-CBC provide integrity.
This is incorrect. AES is an encryption algorithm, and as such only provides confidentiality. CBC is just a mode to enable long messages to be encrypted using AES. You need to add a MAC or a Signature to ensure integrity (it is true that CBC-MAC, a way of creating a MAC can be used, but this is different than AES in CBC mode).

MRE3: Enc(PKbob,k), AES(M,k), MAC(M,k) provides integrity
This is incorrect. Since the symmetric key is encrypted using the Public key of Bob, anybody can create this sequence. That is, a Man in the middle is possible that just intercepts the full sequence and creates a new one. Therefore, when Bob receives the message he cannot be sure that M did not change since Alice sent it.

MRE4: Enc(PKBob,k), Enc(PKAlice,k) provides key integrity
Many answers suggested that this provided key integrity because Bob could decrypt the key k with his secret key, then encrypt it with PKAlice and check that the obtained value is equal to Enc(PKAlice,k).
This was a cute idea :) but sadly it does not work. The fact that the key is encrypted twice does not provide a guarantee of integrity. As before, both of these encryptions are done with public keys. Anybody can create a tuple Enc(PKBob,k), Enc(PKAlice,k) that would verify the test above. Thus Man in the Middle is still available.

MRE5: The commitment scheme needs collision resistance to avoid that Joe Doe cheats.
Collision resistance is not needed. Collision resistance would avoid that the professor would have a secret second grade for Joe. However, the question specified that we worried about Joe cheating. By the time Joe needs to cheat the hash has already been submitted to the central services. Therefore, he is constrained to find a second pre-image to that hash. The needed property is *second pre-image resistance*.

Also, some people said pre-image resistance was needed to protect the grade from the central services. This is correct, but it is orthogonal to Joe cheating.