Student id: Rashed Qazizada

Home-exam: 2021-03-05. 1DV700

1.

a. The CIA module stands for confidentiality integrity and availability. It is a module used by security experts to check, audit, and evaluate computer systems. The goals of this module is to achieve a balance between confidentiality integrity and availability but also it achieves other goals such as non-repudiation and authentication. These goals are achieved by studying the system itself then evaluating the best countermeasures after finishing a cost benefit and a risk analysis.

b. Ransomware attacks: These attacks consist of a malicious software that gets deployed in a a victim's machine, usually by a dropper. The malware then proceeds to encrypt all or some of the files and documents in the victim's computer using a symmetric encryption mechanism. After that it sends the key to a master server where it gets stored. The malware then asks the victim to send money in order to receive the encryption key and retrieve their files. Brute forcing the encrypted files is usually useless. Most of the time, you victim is forced to pay, and they might not even get their files back if the master server is already dead. The reason for this attack is simply to extort money, so it's an economical reason.

Social engineering attacks: these attacks are meant to deceive the victim to give some form of credentials which the attackers later use for all kinds of gains, usually financial gains. The social engineering attacks are usually done through phishing emails.

Cryptocurrency botnets: These attacks consist of a master attacker that has a main machine used a herder. This machines commands all of the various infected machines which are zombies. They follow the herder server no matter what. The incentive behind these attacks is to mine cryptocurrency by using the CPU power of the infected machines to do the calculations and then sending the gained cryptocurrencies to the master server. This attack is done for financial gains.

2.

a. stenography: is a method in which we hide information in plain site inside of other media such as videos, audios or photos. There are many methods used to achieve this such as stuffing the least significant bit into the media. This is usually used when we do not want the adversaries to know that the information exists.

Encryption: is an old concept used since forever. It is used to obfuscate information so that third parties have a hard time or no time at all to decipher its meaning. There are several types of the stenography such as symmetric, asymmetric. The symmetric one is a one key encryption while the other one is a two-key encryption. This concept is used to reserve the integrity and confidentiality of information at rest and in transit.

Digital watermarking: is a technique similar to stenography but instead of hiding information, we stuff a hash, or any unique value to a media file. This is used to protect the copyright rights of the owner of the file. There are two types of digital watermarking, visible and invisible. The second type is the one where we stuff a hash or another unique value inside the media.

b.

If the quantity of the data is big, and the data is at rest, I would use AES as it is considered the best symmetric encryption at the moment. If the data is not that big, It might be possible to use asymmetric encryption such as RSA. In any case, the data should be protected in transit and at rest. We also need to make sure that we preserve its availability integrity and confidentiality. For these reasons, we might be better off using a mixture of symmetric and asymmetric encryption to achieve a balance between all the requirements.

c.

Asymmetric algorithms can be used for key distribution, as they are used to distribute symmetric algorithms keys from one party to the other. An example of this is the diffle-hellman algorithm for key distribution. They are also used for certificate signing, by using the private key on the document, anyone who has the public key can verify that it was produced by the correct party. Finally, they're used for encryption. However only if the data is not too big as the encryption becomes exponential otherwise.

3.

a.

The two objects are:

1. How to ensure that the system are free from flaws. In other words, avoiding bugs in system. We are aware of the fact that there are flaws in programs, we see updates on program continuously, Many of them are bugs or flaws discovered that need to be patch. These flaws potentially can break the program or misuse the system. The overall goal is to minimize the bugs.
2. how to shield or safeguard computing resources from malicious software. Now, we know that that there are something outside of our program that have flaws or malicious attack. They are attempting to attack our application in different way. So, what we can to do to avoid and strengthen our program or being attacked

b. Type of testing are as follows: Regression testing, Unit testing, System testing, integration testing etc.

The main object of Regression testing and component testing or Unit testing is to make sure that the code written follows the design appropriately. Meanwhile, System testing has different purpose. It ensures that the system should do what the client wants to do.

Regression testing, a part of system testing which is especially significant for security purposes. Any changes made to fix a bug or a problem or even adding a new modules in the program to enhance the system. Regression testing make sures that the entire components works properly. Also, that performances have not been downgraded or corrupted by the changes.

Unit testing, tests the smallest unit or component of the design.

Regression testing, any changes made to the program ensures the system performances is not degraded.

Integration testing ensures that the modules work properly together.

System testing ensures that the program works fine with the different kind of OS.

Problems with testing:

Testing can show the presence of an issue, however passing tests do not show the absence of issue or the problem.

Testing usually cannot test what the program should not do but instead checks what the program must do.

Testing just recognize the effect not the internal design of an item or a product. Also, Testing cannot guarantee the completeness of a product.

Testing usually fail to test complex models or it makes it really hard for the testers to monitor.

Testing within an appropriate time is hard because you cannot test all possible combination of inputs.

Testing complex system requires monitoring all states. This makes it difficult to testers to analyse the problem.

c.

Fault tolerance, indicate to the power or ability of a system to keep working without interference when at least one of its segments fails. The goal of making fault-tolerance system is to stop interruptions emerging from a single or isolated purpose of failure. Fault-tolerance ensures that no loss of data. Like hardware system backups by identical system. For instance, a server can be used as fault-tolerance by running similar server together with main server with all its operation mirroring the backup to main sever. Similarly, Software system backups by other software. For instance, a database with patient information could repeatedly duplicated to another system. In case the primary DB fails. The operation will be automatically redirected to the secondary DB. Finally, Power sources could take care of electricity fails.

4.

a.

Logical separation is the method of separating the different users or the different processes inside the same machine. There are several methods to achieve this. One way is to have more than one user where each user has their own group policy rights, this way each user has access to only his own files unless otherwise allowed by an admin. Another way to achieve logical separation is by employing virtualization to create an environment that mimics the real machine, but it is actually contained, and it does not allow anything to escape it, this is sometimes called sandboxing. Finally, there is also compartments which are used by Oss to create resources for a process without exposing the actual machine to the process itself. Basically, giving the process what it needs to function but nothing more.

b.

Memory protection is important as it keeps attackers from gaining privileges of root in an operating system. There are several methods to achieve memory protection, one of them is to have a physical boundary between the OS code and the user code, however this is usually impractical. Another method is to use a logical barrier in a register that can be moved from time to time. This gives more flexibility to the space allocated to the user and the OS. There's also the method of using a pair of registers, one is a bound and the other is a base. This dictates exactly where the space for the user is. Nowadays there is paging and segmentation for memory protection. Paging is when the memory is split up to equal sized compartments, a translation table is used to convert the page address to the actual physical address. Segmentation is similar to paging however each compartment varies in size. Segmentation and paging alone each have flaws, therefore they're both combined as paged segments which have the protection of the segments and pages without their flaws.

c.

Authentication is done with the use of three methods. It is done either with something you know, something you have or something you are. In an operating system, a something you know could be by example a password which you entre and the operating system compares to a secure database it has somewhere in its system. The something you have is by example a key, a USB or a token that the operating system recognizes and allows you access. The something you are could be by example biometrics that the operating system accepts and allows the user in. Another way an operating system could authenticate a person is through the use of single sign-on or federated identity management.

5.

a.

Two phase update is a method used by database management systems where instead of immediately update and execute a query and risk errors and inconsistencies, they first do all what is necessary in phase one without actually changing anything. So, opening files, indexing, parsing the query etc. This phase can be repeated as many times as needed in case of an error. At the end of phase one the DBMS commits to the change and enters phase 2 where it starts to actually apply and do the changes to the database. This phase is also repeatable as much as possible if there are any errors. We do this two phase update so that we do not have inconsistencies in our database.

b.

Data could be sensitive for many reasons such as; it might be coming from a sensitive source, such as a spy in an enemy country. Sometimes the data could be sensitive on itself like the location of weapons of mass 0destruction. Data could also be sensitive in relation to already released information because it might reveal information that should not be revealed. There are some data that is considered sensitive for cultural reasons such as the salary in certain countries. Some typical examples of sensitive data is medical data that is generated from a patient's visit to the hospital. Data that belongs to spying agencies that might be harming to the country itself or personal and identifying data of employees.

c.

Inference attack is an attack where some data Y can be used to arrive to another piece of data X where X is much more confidential than Y. So the goal is basically to use non confidential data to derive partial or complete sensitive data. The inference attack is done in many ways, one of them is direct inference attacks such as infer data from running queries directly or after hiding the queries using logic. Sometimes it is possible to have the n item k percent rule where you can conclude sensitive information if you arrive to a query that gives low frequency results. The other type of inference attacks is indirect attacks which are used to indirectly acquire information. These are such as inferring data from statistics such as the sum, the average and the count. Tracker attacks where we run several queries and we take the intersection of their results to reveal new information. Finally, we can also use linear equations to do a linear attack on the database and solve for the unknowns which in this case represent the sensitive data.

6.

a.

Policy: this part of the security plan is where we will find the security needs and priorities of the company. In other words, the goals for the security plan is usually found in the policy part. This part should also specify clearly what resources should be protected, who should be allowed access to what resources and with what type of access are they allowed. The policy should also mention who is responsible of the security and it should also show the commitment for security by mandating regular updates to the security plan.

Accountability: The security plan should clearly state who is responsible of which part of security in each part of the company, as without people responsible no wone will take action and people will be confused in the case of emergencies. The responsibility can and should be divided up between all involved parties where each handles their own side of it by example the users are responsible for their personal computers while the managers are responsible for their teams and making sure their team members follow the security instructions. Database administrators are responsible for the integrity and confidentiality of the data in their databases and information security officers are responsible of the privacy of users.

Maintenance: The security plan must have a plan for maintenance inside of it. As the security plan needs to adapt to all the changing factors of the company. Without periodic maintenance the security plan will quickly become useless and will fail to achieve its goals.

b.

Risk	Control	Exposure	Exposure after reduction	leverage	savings
1	1	2000	1900	0,5	-100
	2	2000	1000	1	0

For this risk, we are better off choosing the second control as it has a higher leverage and we also do not lose any money if we choose it as we break even while we lose 100 if we go with the first control.

Risk	Control	Exposure	Exposure after reduction	leverage	savings
2	1	20000	10000	1	0
	2	20000	20000	0	-5000

For this risk, the choice of a control is obvious, we should go with control 1 as it has a much higher leverage and we break even without losing any money while control 2 doesn't change the probability of the risk which means it has a leverage of 0 and we will actually lose money if we implement it.

Risk	Control	Exposure	Exposure after reduction	leverage	savings
3	1	800	100	7	600
	2	800	200	3	400

This time, the choice is also clear. We should go with control 1 for risk 3 as it has a leverage of 7 and we save up to 600, while control 2 has only a leverage of 3 and we only save up to 400.