বাংলাদেশ ইউনিভার্সিটি অব প্রফেশনালস্

সেকশন/গ্রুপ Section-A

ইনভিজিলেটরের স্বাক্ষর

মোট পৃষ্ঠা সংখ্যা 11 টি

BSc. in CSE-17 Exam Spring Final Feb-21 পরীক্ষা(Examination), 20 21

বিষয় (Subj): Data and Network Security পত্র/কোর্স নং (Paper/Course No): CSE-429

পত্র/কোর্সের নাম (Paper/Course Name): CSE-17 কেন্দ্র (Center): MIST

রেজিঃ নম্বর (Regn No): 131401170018 শিক্ষাবর্ষ (Session): 2019-20

রোল নম্বর (Roll No): 201714018 তারিখ (Date): 07-02-21

INSTRUCTIONS FOR EXAMINEE

1. Examinees are forbidden to write their names either on outer cover page or anywhere of the answer scripts. In case of violation, the answer script will not be evaluated.
2. Examinees must mention their roll and registration number along with session on the outer cover page of the answer scripts clearly. Otherwise, answer scripts may not be evaluated.
3. Students will write his examination roll number on the top left corner and section-A/B on the top right corner of each page. All pages must be numbered chronologically at the bottom center in x of y format. (for example: 1 of 21)
4. In no case, an examinee will be allowed to start the examination half an hour after the commencement of examination.
5. The Camera of the examinee MUST always be ON during the examination and answer script submission. If Camera is OFF then that online examination will be treated as CANCELLED.
6. The focus of the camera should be such that the invigilator(s) can see the script and examinee with his/her surroundings.
7. Students are to share their entire screen of desktop/laptop to the invigilator throughout the online examination. .
8. Browsing any files other than the given question paper (PDF) and/or online sites other than the respective allowed examination platform (e,g Zoom, Google classroom etc.) is strictly prohibited.
9. Online invigilators reserve the right to take remote access of the examinee's desktop/laptop and investigate as needed at any point during the examination or even after the examination
10. Students without laptop/desktop cannot appear exam online by using mobile phone. Students not possessing laptop/desktop, will have to appear examination Physically at MIST.

পরীক্ষক কর্তৃক পূরণীয়

প্রশ্ন নম্বর	প্রদত্ত নম্বর
১	
২	
৩	
৪	
৫	
৬	
৭	
৮	
৯	
১০	
১১	
১২	
১৩	
১৪	
মোট	

পরীক্ষকের স্বাক্ষর

নিরীক্ষকের স্বাক্ষর

Continued.....

INSTRUCTIONS FOR EXAMINEE

11. Examinees must abide by the instructions of chief invigilator if there are no definite instructions on any subject/matter.

12. No examinee will be allowed to leave the examination session until an hour has elapsed from the commencement of examination.

13. Legal action will be taken against the examinees those are trying to adopt/adopting unfaimeans/exibiting unbecoming conduct in the examination hall and found guilty for any breach of discipline as per rule.

14. Invigilators will have complete authority of deducting marks from any student attempting unfair means.

15. All rough works should be done in the same paper used as answer scripts. Answer scripts should be submitted intact. Papers used for rough work should be pen through by the examinees and submitted along with the answer script.

16. The answer scripts submitted beyond specified time will be treated as CANCELLED.

17. The examinee will send his/her scanned examination script in PDF format to the following e-mail addresses:

(a) e-mail address of subject invigilator/examiner.

(b) Central Database Scheme (coursecode@mist.ac.bd)
Example: EECE433@mist.ac.bd

18. The examinee has to preserve the original answer script of every examination and be ready to submit whenever asked for.

19. Answer script should be the A4 size papers with a cover page provided by Department. Examinee has to fill up his/her necessary details on the cover page. Section A and section B must be clearly marked on the cover page like. **Section A** or **Section B**

20. Examination duration for each subject will be two hours (section-A for one hour + section B for One hour). In between students will get 15 minutes time to submit the answer script of section A and 5 minutes time to issue the question for section B . After completion of 01 hour examination time for section B, students will get 15 minutes to submit the answer script of section B.

21. After completion of written examination (online/physical), viva will be conducted by the respective faculty of that subject.

Section-A

Ans. to the ques. no.- 01(a)

Although CIA triad covers allmost all the dimensions of security, some additional components of security might also need to be employed.

CIA triad consists of three security requirements and ~~by~~ they are:

① Confidentiality
② Integrity
③ Availability.

Now we will discuss the dimensions of security covered by these three:

① Confidentiality:

It assures both data confidentiality and privacy. Data confidentiality covers for the secrecy of data for an organization or individual. Where, privacy covers the permission to use individual data to be used and the control and influence of

data that to be used by whom to whom and how that data will be used.

② Integrity:

Integrity assures that changes done in the system are done by authorized persons or individual in a systematic way. Integrity also covers for data integrity where data changes by the authorized person is assured.

③ Availability:

It assures the system works promptly without any issues and Denial of service (DoS) attack does not occur.

In addition to these three two additional requirements are needed: ④ Authenticity ⑤ Accountability.

④ Authenticity:

Authenticity covers the requirement

P.T.O.

where file senders and modification consists the authentication ~~information~~ information so that receiver can trust the message or file that it has been really sent by the sender.

⑤ Accountability:

Accountability covers the requirement that individual actions are traced back to that individual or entity. So that every action needs the authentication information of ~~that actio~~ entity, who performs the action.

So, CIA triad does not cover all dimensions of security. CIA with authenticity and accountability covers all the dimension.

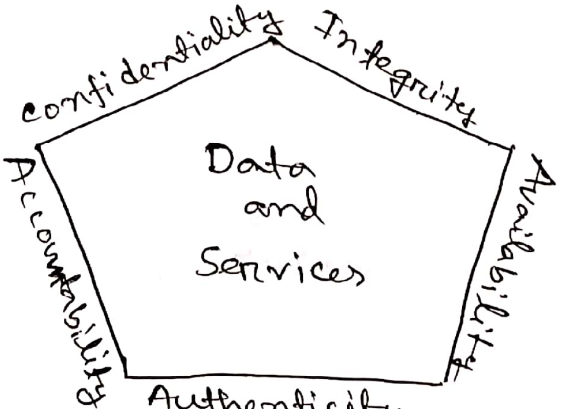

Fig: Security Requirements.

Ans. to the ques. no. - 01(b)

Real life examples where security objectives are needed :

(i) Data confidentiality:

A webapp based system where students marks and all necessary information of an Institute is being stored by Admin and can be shown on on to by students. So, for students personal information also students marks (before result publication) needs to be kept confidential (secret). So, Data confidentiality is needed here.

Security mechanism: security mechanism to be applied for Data confidentiality are: Encryption of the marks and all classified data and then store the encrypted data in the database. so no one without the decryption key can have the classified data.

(ii) Data Integrity:

Again for the same example, data (marks) can be updated only by the related course teachers. so the Data integrity ~~needs~~ objective states that the change of these marks must be done with authorization and only by teachers.

Security mechanism: Access Control and ~~Authentication~~ Authorization is needed to ensure Data Integrity. Can be done using checking the digital signature of the teacher and on the marks.

(iii) Data Authentication:

For the same example as before, the website is public. So, in order to only the particular student can retreive their information and no one else, Data Authentication is needed.

Security mechanism: Authentication can be done by using students ~~Private~~ public key to encrypt students info. Only a particular student with his/here private key can access that information, No one else.

Ans. to the ques. no.-01(c)

Attackers knowledge refers to the knowledge needed to perform an attack to a system or algorithm used by a system.

~~of~~

Attack sophistication requires the actions done by the ~~attacker~~ to perform the attack to a system or algorithm.

In a present day attack scenario:

most of the attacks are in high level of attack sophistication with high level of attackers knowledge.

since, modern systems are already built on modern security measures, more and more sophistication is required to attack the system. More high level knowledge is required to attack a system in present day scenario. Attacks on present day time like: DDos, Malware, steganography file with worms needs high level of attackers knowledge with high level of attack sophistication.

Ans. to the ques. no. - 02(a)

Unconditional security or perfect security is where no cryptanalysis can be done to get the key of the decryption of ciphertext (or plaintext can not be acheived without knowing the key used in encryption).

Analysis of the encryption or decryption algorithms almost always provides some weakness of the algorithm and these weakness or vulnerabilities can be exploited to generate the original plaintext or sometimes the key.

If encryption can be done using one-time pad and ~~aft~~ each time encryption a new one-time pad is deployed and these one-time pads are totally random then perhaps the ~~word~~ un conditional security might be acheived. But in reality

A total ~~number~~ random numbers for pad generation is not possible, because perfect random number can not be acheived and also one-time pad technique is not effecient.

So, we can say that unconditional security can not be acheived. Atleast it is not acheived by now. Almost all modern systems nowadays ~~are~~ have strong security but none of them 100% perfect security.

Ans. to the ques. no.-02(b)

Mechanisms to acheive diffusion and confusion are given below:

Diffusion:

Diffusion is the property of an encryption method that hides the relationship between ciphertext and plaintext. Diffusion can be acheives by using iterated Transposition of the plaintext to generate the ciphertext. Transposition changes the position of symbols from plaintext to ciphertext. So multiple times transposition will make the convention from ciphertext to plaintext very very harder and more complex.

Confusion:

Confusion is the property of an encryption method that hides the relationship between ciphertext and key.

P.T.O.

Confusion can be acheived by using the substitution cipher. Substitution cipher substitutes the plaintext with the help of key to generate the ciphertext. The more level of substitution is being used the more complex relationship between key and ciphertext is being acheives.

To design ciphers both confusion and Diffusion is needed. Diffusion is needed so that attacker can not get the plaintext from ciphertext. Confusion is needed so that attacker can not generate the key from ciphertext. That is why confusion and diffusion is needed while designing encryption methods.

Ans. to the ques. no. - 02(c)

Different kinds of cryptanalysis attacks are:

1. Known plaintext
2. Chosen ciphertext
3. Ciphertext only
4. Chosen plaintext.

① Known plaintext:

When attacker knows the plaintext of the ciphertext and uses this information to find the key. (knows ciphertext and plaintext)

② Chosen ciphertext:

When attacker ~~know~~ chooses some ciphertext to decrypt and get the plaintext to find the key.

③ Ciphertext only:

When attacker only have ciphertext and finds the plaintext or key.

④ Chosen plaintext:

When attacker chooses plaintexts to generate some ciphertexts to find the characteristics of encryption algo to find the weakness of encryption algorithm or key.