RAMAIAH UNIVERSITY OF APPLIED SCIENCES

Assignment

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

Name of the Student	**Deepak R**
Reg. No.	**18ETCS002041**
Semester/Year	**6th/2021**
Course Leader(s)	**Prof. N. D. Gangadhar**

Declaration Sheet				
Student Name	Deepak R			
Reg. No	18ETCS002041			
Programme	B.Tech	Semester/Year	6th/2021	
Course Code	19CSC315A			
Course Title	Information Security and Protection			
Course Date		to		
Course Leader	Prof. N. D. Gangadhar			

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

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		

Assignment-01			
Reg.No.	18ETCS002041	Name of Student	Deepak R

Marking Scheme		Mark		
		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

Security and Protection of Examination Section on RUAS Portal

RUAS Portal has several overlapping operational sections. One set of functionalities of the portal covers the operation and information flow involving data and information related to the Examinations and Assessment of students. Data and information related to question papers, answer scripts, student reports and presentations, attendance records, time tables, marks sheets and certificates are handled by the section. Owing to the sensitive and confidential nature of the data and information, it is essential that it is well protected with security policies and mechanisms.

The student is required to perform an analysis of the information system along the following lines:

1. Identify the assets to be protected and actors involved
2. Determine the specific Confidentiality, Integrity and Availability security services required for the assets
3. Analyze the threats to the system based on the determined security requirements
4. Recommend specific security policies to counter the threats and attempt a synthesis of them into an overarching policy
5. Determine specific security mechanisms to implement the recommended policy/policies with the goal of prevention of attacks
6. Discuss the assumptions and role of trust in the recommendations
7. Discuss the role of law and University Regulations

Solution for 1 Identify the assets to be protected and actors involved

Assets to be Protected are Data and information related to **Question papers, Answer scripts, Student reports, Attendance records and Marks sheets.**

Actors involved are **Teachers** (One who works in the university and teaches Specific Subject), **Student** (One who studies in the University) and **HOD** (Head of Department), **Administrator** (Engineer who maintains Portal and do work of Maintenance of portal).

Solution for 2 Determine the specific Confidentiality, Integrity and Availability security services required for the assets

For Answer Script Asset

Confidentiality - Answer Scripts Record should be Visible only to Teacher of Specific Subject and No other Teacher from other Subject can Access it.

Integrity - Student Should not be given Privilege to alter Answer Script after Examination.

Availability - Answer Scripts Should be Available to Teacher after Exam.

For Attendance Record Asset

Confidentiality - Attendance Record should be Visible only to Teacher of Specific Subject and No other Teacher from other Subject can Access it.

Integrity - Teacher of one Subject cannot change Attendance Record of Student of another Subject.

Availability - Attendance Record Should be Available to Teacher and HOD Whenever they Require.

For Student Reports Asset

Confidentiality - Student reports should be Visible only to respective Student and Teacher.

Integrity - Here Students Should not be given Privilege to alter Student Report.

Availability - Assets like Student Report should be Available to Student whenever they Require.

For Marks Card Asset

Confidentiality – Student reports should be Visible only to respective Student and Teacher.

Integrity – Here Students Should not be given Privilege to alter Marks Card.

Availability - Assets like Marks card should be Available to Student whenever they Require.

For Question paper Asset

Confidentiality – Question Paper should be visible only to the teacher who set the Question Paper until the exam time.

Integrity – No one except the teacher who set the Question Paper should be able to modify (including replace) the Question Paper.

Availability - Question Paper should be available for students to download at the beginning of the examination.

Solution for 3 Analyze the threats to the system based on the determined security requirements

For Answer Script Asset

Snooping – A person other than Teacher gains Unauthorized Access to download Answer Script.

Modification – A person other than the Student modifies Answer Script before Uploading.

Spoofing – Someone impersonates the student who writes in the Answer Script.

Repudiation of origin – The Student says the Answer Script is not uploaded by him/her.

Denial of Receipt – Teacher says he/she didn't receive the Answer Script even though he/she received or Downloaded.

Delay – Answer Script is not available(delayed) for one or more Teacher to download after the examination.

Denial of service - Answer Script is not available for Teacher to download.

For Attendance Record Asset

Snooping – A person other than Teacher gains Unauthorized Access to Attendance Record of a Student.

Modification – A person other than the teacher modifies the Attendance Record.

Spoofing – Someone impersonates the Teacher who takes Attendance and writes in the Attendance Record.

Repudiation of origin – The teacher says the Attendance Record was not updated by him/her.

Denial of Receipt – HOD says he/she didn't receive the Attendance Record from teacher even though he/she received or Downloaded from Email or portal.

Delay – Attendance Record of Students is not available(delayed) to download after Teacher Updatation.

Denial of service – Attendance Record is not available for HOD to download.

For Student Reports Asset

Snooping – A person other than Student gains Unauthorized Access to download Student Report of a Student.

Modification – A person other than the teacher modifies the Student Report.

Spoofing – Someone impersonates the Teacher who writes in the Student Report.

Repudiation of origin – The teacher says the Student Report was not updated by him/her.

Denial of Receipt – Student says he/she didn't receive the Student Report even though he/she received or Downloaded from Email or portal.

Delay – Student Report is not available(delayed) for one or more students to download after the course completion.

Denial of service - Student Report is not available for one or more students to download.

For Marks Card Asset

Snooping – A person other than Student gains Unauthorized Access to download Marks Card of a Student.

Modification – A person other than the teacher modifies the Marks Card.

Spoofing – Someone impersonates the Teacher who Assign marks and writes in the Marks Card.

Repudiation of origin – The teacher says the Marks Card was not updated by him/her.

Denial of Receipt – Student says he/she didn't receive the Marks Card even though he/she received or Downloaded from Email or portal.

Delay – Marks Card is not available(delayed) for one or more students to download after the course completion.

Denial of service - Marks Card is not available for one or more students to download.

For Question paper Asset

Snooping – A person other than Teacher gains Unauthorized Access to read Question Paper when it is Uploaded or sent by mail.

Modification – A person other than the teacher modifies the Question paper.

Spoofing – Someone impersonates the teacher who set the Question paper.

Repudiation of origin – The teacher says the Question paper is not created by him/her.

Denial of Receipt – Student says he/she didn't receive the Question Paper even though he/she received or Downloaded.

Delay – Question Paper is not available(delayed) for one or more students to download at the beginning of the examination.

Denial of service - Question Paper is not available for one or more students to download.

Solution for 4 Recommend specific security policies to counter the threats and attempt a synthesis of them into an overarching policy

For Policies to Remove:

For Answer Script Asset

Snooping – Every Answer Script sent or shared should be password protected.

Modification – No one other than the Student should have privilege to modify Answer Script While writing Exam.

Spoofing – All Answer Scripts upload should be done by Student via authentication (Ex Two Factor Authentication).

Repudiation of origin – When Student Uploads Answer Script, it should take down Confirmation by sending OTP message to Student Mobile.

Denial of Receipt – All Answer Script downloaded by Teacher it should be Recorded (Date and time with IP address) in portal.

Delay – An Answer Script of Student should be available for Teachers after the examination and should not be delayed.

Denial of service - No one except portal Administrator can stop the download service of Answer Script to Teacher.

For Attendance Record Asset

Snooping – Every Attendance Record Sent to HOD should be password protected and Email Communication should be Encrypted.

Modification – No one other than the teacher should have privilege to modify Attendance Record.

Spoofing – All Attendance Record modifications should be done by teacher via authentication (Ex Two Factor Authentication).

Repudiation of origin – When Teacher Update Attendance Record it should take down Confirmation by sending OTP message to Teacher Mobile.

Denial of Receipt – Attendance Record downloaded by HOD it should be Recorded (Date and time with IP address) in portal.

Delay – An Attendance Record of Students should be available for HOD to download after Teacher Updatation and should not be delayed.

Denial of service - No one except portal Administrator can stop the download service of Attendance Record to HOD and teachers.

For Student Reports Asset

Snooping – Every Student Report sent to Student should be password protected and Email Communication should be Encrypted.

Modification – No one other than the teacher should have privilege to modify Student Report.

Spoofing – All Student Report modifications should be done by teacher via authentication (Ex Two Factor Authentication).

Repudiation of origin – When Student Report Marks Card it should take down Confirmation by sending OTP message to Teacher Mobile.

Denial of Receipt – Student Report downloaded by Student it should be Recorded (Date and time with IP address) in portal.

Delay – A Student Report of Student should be available to them after Course Completion and should not be Delayed.

Denial of service - No one except portal Administrator and Teacher can stop the download service of Student Report to Students.

For Marks Card Asset

Snooping – Every Marks Card sent to Student should be password protected and Email Communication should be Encrypted.

Modification – No one other than the teacher should have privilege to modify Marks Card.

Spoofing – All Marks Card modifications should be done by teacher via authentication (Ex Two Factor Authentication).

Repudiation of origin – When Teacher Update Marks Card it should take down Confirmation by sending OTP message to Teacher Mobile.

Denial of Receipt – Marks Card downloaded by Student it should be Recorded (Date and time with IP address) in portal.

Delay – A Marks Card of Student should be available to them after Course Completion and should not be Delayed.

Denial of service - No one except portal Administrator and Teacher can stop the download service of Marks Card to Students.

For Question paper Asset

Snooping – Every Question Paper sent or shared should be password protected.

Modification – No one other than the teacher should have privilege to modify Question Paper.

Spoofing – All Question Paper modifications should be done by Teacher via authentication (Ex Two Factor Authentication).

Repudiation of origin – When Teacher Uploads Question Paper it should take down Confirmation by sending OTP message to Teacher Mobile.

Denial of Receipt – All Question Paper downloaded by Student it should be Recorded (Date and time with IP address) in portal.

Delay – A Question Paper should be available for all students at the beginning of the examination and should not be delayed.

Denial of service - No one except portal Administrator and Teacher can stop the download service of Question Paper to Students.

Solution for 5 Determine specific security mechanisms to implement the recommended policy/policies with the goal of prevention of attacks

For Preventing:

For Answer Script Asset

Snooping – Every Answer Script sent or shared should be password protected.

Modification – The portal should implement access control mechanism for providing read and modify access to Answer Script so that no one other than Student modify it during Exam.

Spoofing – All Answer Scripts upload should be done by Student via authentication (Ex Two Factor Authentication).

Repudiation of origin – When Student Upload Answer Script it should have OTP Verification via SMS.

Denial of Receipt – All Answer Script downloaded by Teacher it should be Recorded (Date and time with IP address) in portal.

Delay – There is a Portal Administrator who monitors any delay of service(download) of Answer Script and rectifies it

Denial of service - DOS prevention services need to be implemented on the portal and

Portal Administrator staff restarts the download service in case of a DOS attack.

For Attendance Record Asset

Snooping – Every Attendance Record Sent to HOD should be password protected and Email Communication should be Encrypted.

Modification – The portal should implement access control mechanism for providing read and modify access to Attendance Record so that no one other than Teacher modify it.

Spoofing – All Attendance Record modifications should be done by teacher via authentication (Ex Two Factor Authentication).

Repudiation of origin – When Teacher Upload Attendance Record it should have OTP Verification via SMS.

Denial of Receipt – Attendance Record downloaded by HOD it should be Recorded (Date and time with IP address) in portal.

Delay – There is a Portal Administrator who monitors any delay of service(download) of Attendance Sheet and rectifies it

Denial of service - DOS prevention services need to be implemented on the portal and

Portal Administrator staff restarts the download service in case of a DOS attack.

For Student Reports Asset

Snooping – Every Student Report sent to Student should be password protected and Email Communication should be Encrypted.

Modification – The portal should implement access control mechanism for providing read and modify access to Student Report so that no one other than Teacher modify it.

Spoofing – All Student Report modifications should be done by teacher via authentication (Ex Two Factor Authentication).

Repudiation of origin – When Teacher Upload Student Report it should have OTP Verification via SMS.

Denial of Receipt – Student Report downloaded by Student it should be Recorded (Date and time with IP address) in portal.

Delay – There is a Portal Administrator who monitors any delay of service(download) of Student Report and rectifies it

Denial of service - DOS prevention services need to be implemented on the portal and

Portal Administrator staff restarts the download service in case of a DOS attack.

For Marks Card Asset

Snooping – Every Marks Card sent to Student should be password protected and Email Communication should be Encrypted.

Modification – The portal should implement access control mechanism for providing read and modify access to Marks Card so that no one other than Teacher modify it.

Spoofing – All Marks Card modifications should be done by teacher via authentication (Ex Two Factor Authentication).

Repudiation of origin – When Teacher Upload Marks Card it should have OTP Verification via SMS.

Denial of Receipt – Marks Card downloaded by Student it should be Recorded (Date and time with IP address) in portal.

Delay – There is a Portal Administrator who monitors any delay of service(download) of Marks Card and rectifies it.

Denial of service - DOS prevention services need to be implemented on the portal and

Portal Administrator staff restarts the download service in case of a DOS attack.

For Question paper Asset

Snooping – Every Question Paper sent or shared should be password protected and all the communication Should be encrypted.

Modification – The portal should implement access control mechanism for providing read and modify access to Question Paper so that no one other than Teacher modify it.

Spoofing – All Question Paper modifications should be done via a authentication (Ex Two Factor Authentication) via mobile OTP

Repudiation of origin – When Teacher Upload Question Paper it should have OTP Verification via SMS.

Denial of Receipt – All downloads of Question Paper are Recorded (Date and time with IP address) in portal.

Delay – There is a Portal Administrator who monitors any delay of service(download) of Question Paper and rectifies it

Denial of service - DOS prevention services need to be implemented on the portal and

Portal Administrator staff restarts the download service in case of a DOS attack.

Solution for 6 Discuss the assumptions and role of trust in the recommendations

For Answer Script Asset

Assumption

It is assumed that Student uploads Answer Script and it is well protected in portal Environment against unauthorised access. But when Portal Administrator during Maintenance or Routine Scanning Deletes Answer Script of a Student and make it unavailable for Teacher this Assumption Becomes Failed.

Role of Trust

In above assumption the portal Administrator is trustworthy i.e., Portal Administrator during Maintenance or Routine Scanning do not Delete Answer Script of a Student then the above assumption becomes True.

For Attendance Record Asset

Assumption

It is assumed that Teacher updates Attendance Record Correctly and it is well protected in portal Environment against unauthorised access. But if Teacher updates the Attendance Record wrongly this Assumption get failed.

Role of Trust

In the above assumption the Teacher is Trustworthy i.e., Teacher updates the Attendance Record Correctly Without any Mistake then above Assumption is True.

For Student Reports Asset

Assumption

It is assumed that Teacher uploads Student Report of Respective Student in his portal and it is well protected in portal Environment against unauthorised access. But if Teacher upload Student Report of Student A in Student B s Portal, then Assumption gets failed.

Role of Trust

In the above assumption Teacher is Trustworthy i.e., Teacher uploads Student Report of Student to portal of Correct Student then above assumption is True.

For Question paper Asset

Assumption

It is assumed that Question paper is well Protected with Password before Examination and Only it is accessible to Teacher and HOD in portal before Examination. But if Teacher or HOD tells Password to any other person Assumption gets false.

Role of Trust

Here teacher and HOD are Trustworthy i.e., Teacher or HOD don't share their login credential with anyone so that no one can access Question paper then above Assumption is true.

For Marks Card Asset

Assumption

It is assumed that Teacher uploads Marks Card of Respective Student in his portal and it is well protected in portal Environment against unauthorised access. But if Teacher upload Marks Card of Student A in Student B s Portal, then Assumption gets failed.

Role of Trust

In the above assumption Teacher is Trustworthy i.e., Teacher uploads Marks Card of Student to portal of Correct Student then above assumption is True.

Solution for 7 Discuss the role of law and University Regulations

Students, Teacher, HOD and other Actors are not Supposed to share login Credential with others.

University has all Rights to Suspend Students if he shares login Credential with others and login with 2 or more device during online exam.

Every actor's login time and logout time should be strictly monitored and recorded so that helps when threats happens and which device logged in.

Every actor's data should be confidential and strong fire walls should be used so that any malicious activity should be seen and caught.

The policy forbids the reading or disclosing of these communications without permission of the holder, except in specific enumerated circumstances:

• when required by law;

• when there is reliable evidence that the law or University policies are

being violated;

• when not doing so may result in significant harm, loss of significant evidence of violations of law or University policy, or significant liability to the University or the members of its community; and

• when not doing so would seriously hamper the administrative or teaching obligations of the University.

BIBILOGRAPHY

1. BishopSullivanRuppel-Computer Security_ Art And Science (2019) Text Book
2. WhitmanMattord-Principles of Information Security-Cengage Learning (6ed, 2017) Text Book