CS 573 Fundamentals of Cybersecurity: Midterm

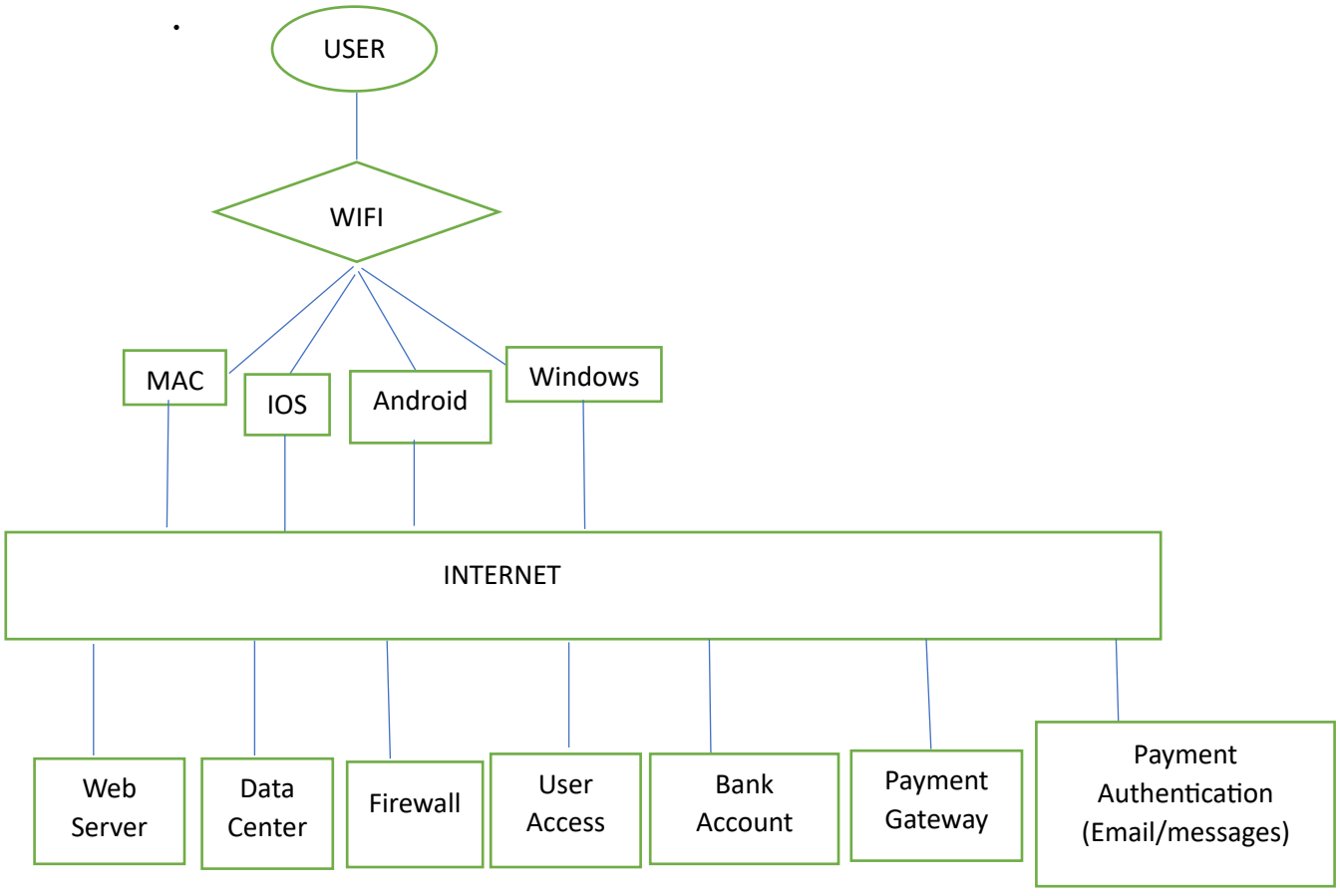
Poorvi Raut: 20009560

Banking Application:

A Banking application is one which allows users to access their bank account, complete all transactions, check balance, view payment history and perform all such operations. The goal of such application is to provide key Banking services to the user remotely. Users use various devices like Windows, MACOS, IOS, Android to access the application. All these devices are connected via Internet/Wireless Communication (WIFI). A Banking Application allows authorized users to login to their account and perform necessary transactions online. But due to security breaches at times, the information becomes accessible to unauthorized users who take advantage and possess threat to the system.

Therefore, in this assignment we are trying to understand probable threats to our application and understand the risk possessed to valuable assets.

Valuable Assets for Banking Application



Threat Asset Matrix for Banking Application:

P: Probability, C: Consequences, R: Risk

Range: - High:3, Medium:2, Low:1

ASSETS	CONFIDENTIALITY	INTEGRITY	AVAILIBILITY	THEFT/FRAUD
Windows	P:2, C:3, R:6	P:2, C:3, R:6	P:1, C:2, R:2	P:1, C:2, R:2
MAC	P:2, C:3, R:6	P:2, C:3, R:6	P:1, C:2, R:2	P:1, C:2, R:2
Android	P:1, C:2, R:2	P:1, C:2, R:2	P:1, C:2, R:2	P:1, C:2, R:2
IOS	P:1, C:2, R:2	P:1, C:2, R:2	P:1, C:2, R:2	P:1, C:2, R:2
Web Server	P:3, C:2, R:6	P:2, C:2, R:4	P:1, C:1, R:1	P:1, C:1, R:1
Data Center	P:3, C:3, R:9	P:3, C:3, R:9	P:3, C:3, R:9	P:3, C:3, R:9
Firewall	P:3, C:3, R:9	P:3, C:3, R:9	P:1, C:3, R:3	P:1, C:1, R:1
User Access	P:2, C:2, R:9	P:3, C:3, R:9	P:3, C:3, R:9	P:3, C:3, R:9
Bank Account (Checking/Savings)	P:1, C:2, R:2	P:1, C:2, R:2	P:1, C:1, R:1	P:2, C:2, R:4
Payment Gateway	P:2, C:3, R:6	P:1, C:2, R:2	P:1, C:1, R:1	P:1, C:1, R:1
Payment Authentication (Email/Messages)	P:3, C:3, R:9	P:2, C:3, R:6	P:1, C:3, R:3	P:3, C:3, R:9

1. Windows Devices:

- **Confidentiality**: Source code is of value to the unauthorized user, but windows OS is well protected using any anti malware system installed and Windows Microsoft in built defender.
- **Integrity**: Integrity is required to maintain the original source code. Any changes to the original code can destroy the system and will be easily accessible. But windows OS is well protected using any anti malware system installed and Windows Microsoft in built defender.
- **Availability**: Denial of source code is uncommon. Windows OS is well protected using any anti malware system installed and Windows Microsoft in built defender.
- **Theft/Fraud**: Theft or fraud of source code is uncommon. Windows systems are monitored well using Windows activity monitor and can easily be tracked using Microsoft's "Find My Device" feature.

2. MAC Devices:

- **Confidentiality**: Source code is of value to the unauthorized user, but MAC devices is well protected using Apple's Privacy policy and any Anti malware installed in system.
- **Integrity**: Integrity is required to maintain the original source code. Any changes to the original code can destroy the system and will be easily accessible. But MAC devices are well protected using Apple's Privacy policy and any Anti malware installed in system.
- **Availability**: Denial of source code is uncommon. MAC devices are well protected using Apple's Privacy policy and any Anti malware installed in system.
- **Theft/Fraud**: Theft or fraud of source code is uncommon. Windows systems are monitored well using MAC activity monitor and can easily be tracked using Apple's "Find My Device" feature. Device data can be removed if required remotely.

3. Android Devices:

- **Confidentiality**: Android devices are well protected against any unauthorized access using Password, Passcode, Biometric, and other Multi Factor Authentication features.
- **Integrity**: Integrity of Email and messages, android applications is vital, but android devices are well protected with Password, Passcode, Biometric, and other Multi Factor Authentication features.
- **Availability**: Denial of service to the android devices are uncommon as they are timely updated with latest firmware and security feature.
- **Theft/Fraud**: Theft or fraud of Android devices is uncommon. However, if required, android has many features like device tracking, remote phone lock, screen lock, theft monitoring sensors and remote data removal.

4. IOS Devices:

- **Confidentiality**: IOS devices are well protected against any unauthorized access using Password, Passcode, Biometric, and other Multi Factor Authentication features.
- **Integrity**: Integrity of Email and messages, android applications is vital, but android devices are well protected with Password, Passcode, Biometric, and other Multi Factor Authentication features.
- **Availability**: Denial of service to the android devices are uncommon as they are timely updated with latest firmware and security feature.
- **Theft/Fraud**: Theft or fraud of Android devices is uncommon. However, if required, android has many features like device tracking, remote phone lock, screen lock, theft monitoring sensors and remote data removal.

5. Web Server:

- **Confidentiality**: Web Servers are middleware between users and the application they want to access. They are gateway to interface API in the backend. Users use internet to access the severs. Hence it is important that the access needs to be secured using SSL/TLS i.e., the connection can be made using HTTP requests.
- **Integrity**: Web Servers are interface between users and the application they want to access. Hence Integrity needs to be maintained. For this input validation needs to be implemented to preserve integrity.
- **Availability**: Web Servers need to be always available for the usability of users based on requirement. For this, we can use multiple Web Servers and distribute the load between these servers using a load Balancer.
- **Theft/Fraud**: Using SSL certificate (authorized by authority) can help to prevent fraud posing banking applications.

6. Data Center:

- **Confidentiality**: Data Centers are of utmost importance as all information is stored here which are sensitive to users related to banking operations. Methods like access control list, Role based access Control, Principle of privilege can be used here to retain confidentiality.
- **Integrity**: Data needs to be preserved in original form and even a minor change can affect the entire transaction. Encrypting data using encryption keys, symmetric/asymmetric key cryptographic algorithms, hashing techniques, Digital Signatures can help to maintain integrity of data in data centers.
- **Availability**: Data Center should always maintain data available to the user. Data availability can be preserved by using techniques like redundancy, fault tolerance to ensure data is available from data center always.
- **Theft/Fraud**: Using above features we can prevent loss of data.

7. Firewall:

- **Confidentiality**: Firewall helps to preserve confidentiality. It is vital defense mechanism. It separates intranet from the internet and helps to monitor any incoming or outgoing traffic using features like stateless and stateful AL's.
- **Integrity**: Data on the internet, can be intercepted and hacked. Therefore, it is important that the customer always initiate a connection using https.
- **Availability**: Using Virtual IP we can use two firewalls. This can preserve availability incase if one the firewall fails to work.
- **Theft/Fraud**: Firewalls can help prevent Theft/Fraud of data. Firewall security features need to be implemented in order to prevent loss of information.

8. User Access:

- **Confidentiality**: Using authentication mechanism we can protect user's data.
- **Integrity**: Data on the internet, can be intercepted and hacked. Therefore, it is important that the customer always initiate a connection using https.
- **Availability**: Authenticated user should be able to always access the bank application and access authorized information.
- **Theft/Fraud**: Using above features we can prevent loss of data.

9. Bank Account (Checking /Savings)

- **Confidentiality**: Banking applications preserve confidentiality of bank accounts using security standards and PCI/DSS Standards. Customer's PII needs to be always protected.
- **Integrity**: Using Security protocols can preserve integrity.
- **Availability**: Using above mentioned techniques can preserve availability of data to users all time.
- **Theft/Fraud**: Bank Account theft is possible. Unauthorized access of Bank details can be available easily to unauthorized user. It can be prevented using security practices and PCI/DSS standards.

10. Payment Gateway:

- **Confidentiality**: Payment gateway include card payments(credit,debit,visa) , online UPI's ,wallets. For smooth transaction confidentiality needs to be preserved. Using authentication, authorization protocols and Auditing (AAA) framework confidentiality can be obtained.
- **Integrity**: Payment gateways help in maintaining integrity of data.
- **Availability**: Payment Gateways are available mostly, except at times when the bank server are unavailable or in case of some emergency or holiday. Otherwise, payment gateways are available and fault tolerant.
- **Theft/Fraud**: Payment gateways help in reducing chances of theft /fraud.

11. Payment authentication (Email/Messages):

- **Confidentiality**: Authorized users should be able to access data like One time password sent via email or messages.
- **Integrity**: Messages and email are a service on their own that follow the security best practices, to ensure that the data set via these services are not modified.
- **Availability**: Since Messaging and Email are separate services, we do not have a direct control over its Availability. However, the service providers ensure that they always provide the service.
- **Theft/Fraud**: Data sent to users via email, messages should be sent to authorized user only and should be accessible.

ASSETS	ESTIMATED RISK
Windows	Total risk = 16 – 4th Highest Risk Asset
MAC	Total risk = 16 – 4th Highest Risk Asset
Android	Total risk = 8 – 8th Highest Risk Asset
IOS	Total risk = 8 – 8th Highest Risk Asset
Web Server	Total risk = 12 – 5th Highest Risk Asset
Data Center	Total risk = 36 – 1st Highest Risk Asset
Firewall	Total risk = 22 – 3rd Highest Risk Asset
User Access	Total risk = 36 – 1st Highest Risk Asset
Bank Account (Checking/Savings)	Total risk = 9 – 7th Highest Risk Asset
Payment Gateway	Total risk = 10 – 6th Highest Risk Asset
Payment authentication (Email/messages)	Total risk = 27 – 2nd Highest Risk Asse