Misuse Case Of Banking System

By:- Assignwise

Table of Contents

Task 1

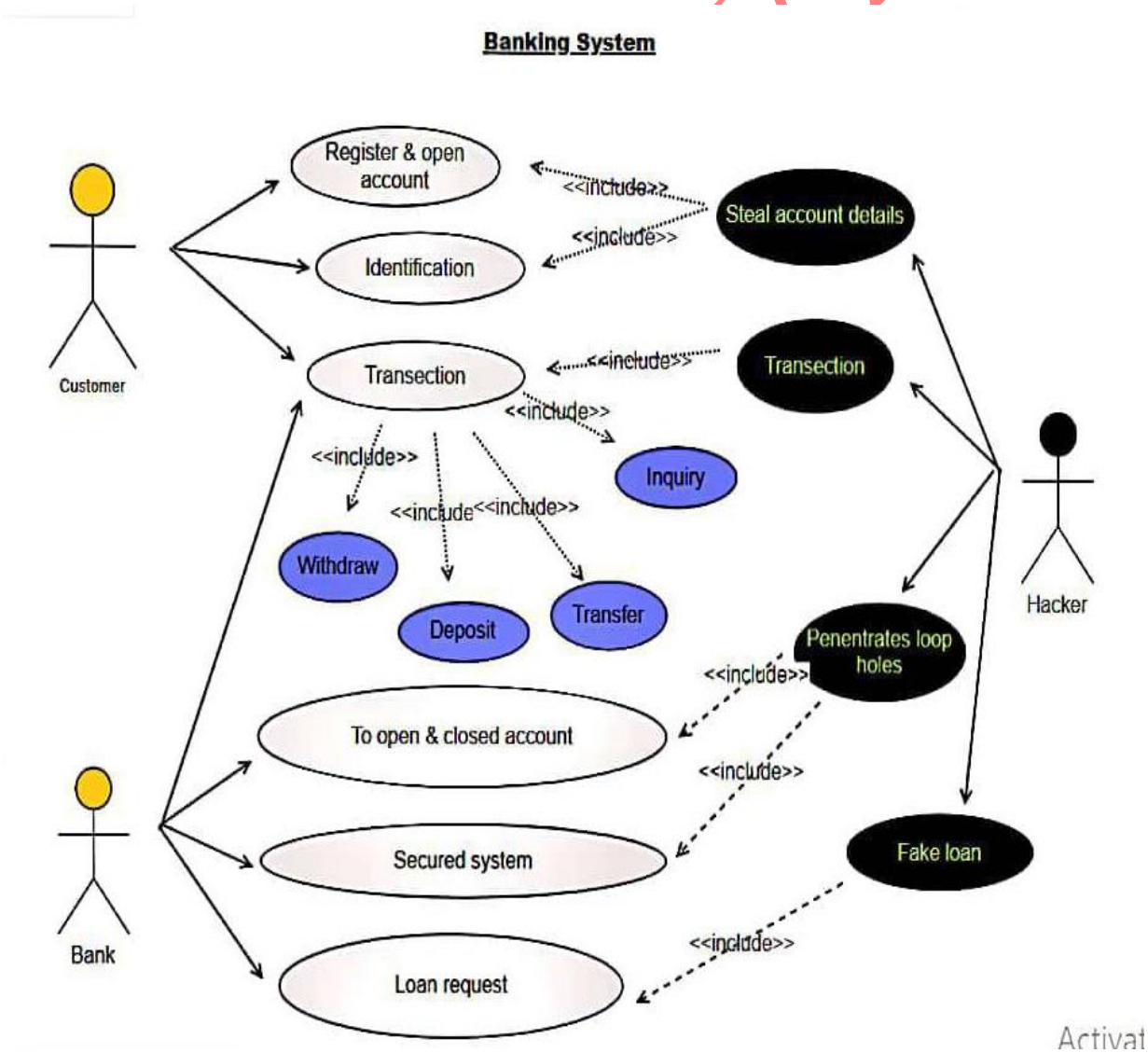
Increasing use of Information Technology (IT) in banks and development of technologically complex products require systematic monitoring and management of technology risks in banks. Also, it is necessary to add restrictions on a particular network of the entire bank as bank frauds are increasing day by day. In this context,

a. **Draw a misuse case for Banking Management system (BMS) to demonstrate the possible attacks that can occur in Banking Management System (BMS).**
b. **List five threats and five attacks that may occur in the banking system.**
c. **Identify five ways in which you could reduce the risk of the threat occuring (Preventions).**
d. **Include five controls that would assist with the detection of these threats.**

Misuse Cases

Answer

Unauthorized Transfer of Funds Actor: Attacker



Stakeholder

- Customer:- The individual who owns the account from which the unlawful transfer was made.
- Bank:- The financial organization in charge of maintaining accounts and assuring their security.

Actor

- Hacker:- The individual or entity responsible for the unlawful movement of money.

Description:-

- The malevolent user accesses the BMS without authorization by using stolen login information or by taking advantage of flaws in the system.
- The malicious user can examine private client data once they are into the system, including account balances, transaction history, and personal data.
- The malevolent user has the ability to withdraw money, move money between accounts, and carry out other illicit operations.
- By altering or erasing transaction records or by initiating fraudulent transactions, the malevolent user might hide their trail.
- Also, the malevolent user has the ability to take private information for identity theft and other illicit uses, including credit card details, social security numbers, and other sensitive data.
- The bank employee could not be aware of the illegal access or might unintentionally provide the malicious person further login information.

Preconditions:-

- It is possible to take advantage of security flaws or vulnerabilities in the BMS.
- The malevolent individual has access to login information or is able to locate a workaround for login restrictions.
- The bank employee could not have received the necessary security protocol training or they might have been careless in their tasks.

Basic Flow:-

- The hacker obtains access to the customer's account information by either breaking into the bank's system or gaining the information in another way.
- The hacker starts a transfer of funds from the customer's account to another account, often one that the hacker controls.
- The transfer is processed by the bank's system, and the monies are transferred to the other account.
- The consumer becomes aware of the unlawful transfer and notifies the bank.
- The bank staff looks into the problem and attempts to reverse the transfer and collect the stolen monies.

Post conditions:-

- The malicious user may have stolen sensitive information or carried out fraudulent activities after gaining unauthorized access to the BMS.
- Customers' faith in the bank and its reputation may suffer.
- The bank may incur financial damages as a result of fraudulent transactions.
- If it is shown that the bank was careless with its security standards, legal action may be taken against it.

Alternative Flow:-

- The attacker tries to transfer funds but is caught by the system's fraud detection function.
- The mechanism prevents the transfer and notifies the bank's security staff.
- The bank is unable to retrieve the stolen monies, either because the hacker withdrew them or because they were moved to an account outside of the bank's jurisdiction. In this instance, the bank may be required to repay the consumer for the lost monies.

Mitigation:-

- Further security measures, such as two-factor authentication, password resets on a regular basis, and monitoring for odd account activity, can be implemented by the bank.
- Customers may be educated and trained on how to secure their account information and prevent falling prey to phishing and other scams by the bank.
- The bank can collaborate with law authorities to find and prosecute the hackers who were responsible for the illicit transfer.

Common threats and attacks

Answer

Some of the threats and attacks that may occur in the banking system are as follow:-

Common threats

- **Phishing**:- Phishing attacks include duping consumers into disclosing sensitive information, such as login passwords, account numbers, or other personal information, via bogus emails or websites that look to be authentic.
- **Malware**:- Malware is harmful software that may infect computers or mobile devices and steal personal data or login credentials, frequently without the user's awareness.
- **Insider threats:-** Insider threats to banking systems include employees who misuse their access to sensitive information or engage in illegal activities, which can result in financial loss and reputational damage.
- **Credit risk**:- When lending money to clients who are unable to pay back their loans, which can result in financial losses and bankruptcy, banks are exposed to credit risk.
- **System failures**:- Banks rely on complex information technology systems, and any failure or glitch can result in significant financial losses or operational disruptions.

Common attacks

- **Phishing attacks**:- Phishing attacks are attempts to obtain personal and financial information using bogus emails, text messages, or websites that look to be from a reputable entity.
- **Malware attacks**:- Malware attacks are software attacks that are intended to harm or exploit computer systems. Malware has the ability to steal data such as login passwords and personal identification numbers (PINs).
- **Insider attacks**:- Insider attacks are defined as attacks carried out by workers, contractors, or other insiders who use their access rights to steal or corrupt sensitive data.
- **ATM skimming**:- ATM skimming is the use of an ATM-attached device that can read and save information from credit or debit cards used in the machine.

- **Man-in-the-middle**:- Man-in-the-middle attacks are a sort of cyber assault in which an attacker intercepts communication between two parties in order to steal or change data.

Risk of the threat

Answer

We could reduce the risk of the threat occurring (preventions) are given below:-

- **Use strong passwords**:- Encourage the use of strong passwords that are difficult to guess or crack, and implement two-factor authentication to add an extra layer of security.
- **Regularly update software and systems**:- Keep all software and systems up to date with the latest security patches and updates to address any vulnerabilities.
- **Backup important data**:- Backup critical data on a regular basis to prevent data loss due to cyberattacks or hardware failure.
- **Monitor network activity**:- Use network monitoring tools to detect suspicious activity and respond quickly to threats.
- **Use encryption**:- Encrypt sensitive data and communications to prevent unauthorized access.

Assist

Answer

The ways to controls that would assist with the detection of these threats are as follow:-

- **Antivirus software**:- Antivirus software can identify and get rid of several kinds of malware, such as Trojans, worms, and spyware. Additionally, it has the ability to identify questionable activities and notify security teams.
- **Firewall**:- A firewall may keep an eye on incoming and outgoing network traffic and prevent anyone from entering the network without authorization.
- **Security Information and Event Management (SIEM) system**:- To detect security risks and abnormalities, a SIEM system can gather and examine security-related data from numerous sources, including network devices, servers, and apps.
- **Access control**:- Access control tools like role-based access, password rules, and two-factor authentication can stop unauthorized users from accessing critical information and systems.
- **Data backup and recovery**:- Consistent data backups can aid firms in quickly regaining access to lost data following a security breach or other catastrophes.

Task 2

You are going to join a new startup company. The startup company has 35 employees who work from home. Each employee is provided with a computer device and a cell phone. The company is developing a subscription-based application for time management. Basic ideas are to define lineup items and then track the time that is spent on completing them. Each lineup item can have a title, a description, a deadline, and an estimate of how much time it is expected to take. These lineup items can also be assigned to other users of the platform. Before using this app, the user needs to sign up by providing basic information, such as their name, email address, and credit card details. After registration, the user can interact with the application via a mobile app or via a website. All these details are stored in the backend database and are accessed via an API (Application Programmer's Interface). It is expected that the organization needs an infrastructure of approximately 15 servers during its startup stage. There is a corporate office with a data center as well.

a. **Identify the common five vulnerabilities and five threats and explain each of them.**
b. **Develop a threat model for the application.**
c. **What five controls must be implemented to secure this application?**
d. **Discuss the Confidentiality, Integrity, Availability and Privacy security issues in cloud computing?**
e. **Explain the solutions for the above security issues in the cloud.**
f. **Explain five ways to secure data while transferring on the cloud?**

Answer

The common five vulnerabilities and five threats are given below:-

Common vulnerabilities

- **Insecure Password Storage**:- The program may store user credentials insecurely, such as in plaintext or with inadequate hashing techniques, allowing attackers to quickly access user passwords.
- **Lack of Proper Authentication**:- The application may lack a sufficient authentication system, allowing unwanted access to critical data.
- **Lack of Proper Authorization**:- The application may lack an appropriate authorization mechanism, allowing unauthorized access to important data or functionality.
- **SQL Injection**:- The application's database may be vulnerable to SQL injection attacks, which allow attackers to view or alter data.
- **Insufficient Input Validation**:- If the program does not adequately check user input, attackers may be able to submit malicious data and potentially take control of the application or steal user data.

Common threats

- **Phishing**:- Attackers may employ phishing emails or social engineering techniques to deceive victims into disclosing their login information or credit card information.
- **Malware**:- Malware may be used by attackers to infect users' computers or mobile devices, steal their data, or seize control of their devices.

- **Man-in-the-Middle**:- Man-in-the-middle attacks allow attackers to intercept and change data sent between users and the application.
- **Insider Threats**:- Employees who have access to the application's data may purposefully or unintentionally abuse or disclose sensitive information.
- **Physical Theft or Damage**:- Physical theft or damage to servers or other infrastructure might impair application availability or result in data loss.

Threat model

Answer

We must consider the following stages while developing a threat model for an application:-

- **Define the application's scope**:- Determine the application's boundaries, components, and dependencies.
- **Determine prospective attackers**:- Identify who could want to attack the application and why. Individuals, groups, or organizations might be the perpetrators.
- **Identify prospective attack vectors**:- Finding probable attack vectors can help you to understand how an attacker might have access to the application's systems, data, and data sources. Network assaults, application attacks, social engineering attacks, and physical attacks are all potential attack vectors.
- **Determine any possible vulnerabilities**:- Determine the areas where the application is vulnerable to attack. Software problems, setup errors, weak passwords, and insecure data storage are a few examples of vulnerabilities.
- **Prioritize threats**:- Threats should be prioritized according to their effect, probability, and cost of mitigation.
- **Mitigate threats**:- Threats should be reduced, so create a strategy to do so. This plan should include putting security controls and best practices in place, updating software, and teaching users on safe conduct.
- **Monitor and review**:- Continually keep an eye out for potential threats and vulnerabilities in the application, evaluate how well the mitigation measures are working, and update the threat model as necessary.

Controls

Answer

The five controls listed below must be put into practice in order to secure an application:-

- **Access control**:- Make sure that the program and its data are only accessible to authorized users. To stop unwanted access, use role-based access restrictions and authentication procedures.
- **Data encryption**:- Protect sensitive information against unwanted access and disclosure by encrypting it both in transit and at rest. To protect the data, use encryption techniques like SSL/TLS and AES.
- **Application testing**:- Test the application often for weaknesses and fix any problems that are found right away. Penetration testing, code reviews, and vulnerability analyses can be used to accomplish this.
- **Incident response plan**:- Create and implement an incident response strategy to deal with any potential security breaches. This strategy should include measures to locate a breach, confine it, and lessen its effects.
- **Continuous monitoring**:- Keep an eye out for strange behaviour on the network and the application. Log analysis, intrusion detection systems, and other security

techniques can be used to do this. You may immediately recognize security concerns by continually monitoring the application and taking appropriate action.

Cloud computing

Answer

Cloud computing has gained popularity among numerous organizations. However, cloud computing has its own unique set of security issues, just like any other technology. Confidentiality, integrity, availability, and privacy are some of the most crucial concerns to take into account when it comes to securing cloud environments among these difficulties.

- **Confidentiality**:-The safeguarding of private information against unauthorized access is referred to as confidentiality. Data is frequently sent across several networks and stored in many places in a cloud system. It is essential to make sure that all data, whether it is at rest or in transit, is shielded from unwanted access. Access restrictions, encryption, and secure transmission protocols like SSL/TLS can all be used to accomplish this.
- **Integrity**:- The protection of data from illegal change or corruption is referred to as integrity. Data in the cloud can be changed or corrupted owing to a variety of circumstances such as hardware failures, software faults, or malicious assaults. Data integrity checks must be implemented to guarantee that data is not tampered with or manipulated. This can be accomplished by employing checksums, digital signatures, and version control systems.
- **Availability**:- The capacity of users to access data and resources when they need them is referred to as availability. Many variables, including hardware failures, network outages, or denial-of-service attacks, might have an impact on availability in a cloud environment. To guarantee that users can access data and resources at all times, cloud systems must be built to be highly accessible and robust.
- **Privacy**:- Privacy refers to the safeguarding of personal information and data from illegal access or disclosure. Personal data is frequently kept and processed in several places in a cloud environment, making it more vulnerable to unwanted access. It is critical to secure all personal data by implementing suitable access restrictions, encryption, and other security measures.

Solutions for Security Issues

Answer

The following are some popular solutions:-

- **Data Security**:- The startup must always guarantee that the user's data is protected because it is a crucial concern. For the company to guarantee the privacy, availability, and integrity of user data, appropriate access control rules, encryption technologies, and routine backups must be put in place.
- Access Control:- To limit access to sensitive data and resources, the company should create stringent access control regulations. To make certain that only authorized workers have access to sensitive data and resources, they should implement multi-factor authentication, role-based access control, and access control lists.
- Compliance:- Depending on the nature of the application and the data stored, the company must guarantee compliance with different rules such as GDPR, HIPAA, and

PCI DSS. To guarantee compliance, they should also put in place suitable auditing and reporting processes.

- **Network Security**:- To avoid unwanted access, the startup should adopt suitable network security measures such as firewalls, intrusion detection and prevention systems, and network segmentation.
- **Application Security**:- To prevent attacks such as SQL injection, cross-site scripting, and other vulnerabilities, the startup should adopt effective application security measures. Companies must use secure coding techniques and conduct frequent security testing and audits.
- **Disaster Recovery**:- To recover fast from any interruptions or calamities, the startup should develop effective disaster recovery and business continuity strategies. They should perform frequent backups, deploy redundant systems, and practice disaster recovery exercises on a regular basis.

Security ways while data transfer on the cloud

Answer

Some of the ways to secure data while transferring on the cloud are as follows:-

- **Use a secure connection**:- To encrypt data during transport, use a secure connection such as HTTPS or SSL.
- **Encrypt data at rest and in transport**:- Encrypt data at rest and in transit. To encrypt data, several encryption algorithms such as AES, RSA, and SSL can be used.
- **Use multi-factor authentication**:- To access data in the cloud, you must use multi-factor authentication. This can protect your data from illegal access.
- **Use firewalls**:-Employ firewalls to safeguard your network from unwanted access and to prevent harmful traffic.
- **Monitor activity logs**:-Keep an eye on activity records to detect any illegal access or questionable activities.

Conclusion

In this project, we learnt how perpetrators might launch cyber assaults against the Banking Management System, as well as preventive measures to safeguard the bank's data. This assignment teaches us how to handle misuse cases at a bank. We investigated how the perpetrator can attack or access our data through many types of assaults such as phishing, Botnets, viruses and worms, DoS attacks, and many more, and we also learnt how to protect our data from such attacks. We've also learnt about the advantages of the Misuse instance. We'll look at why record security is so important in order to keep our data safe from hackers. We also learn more about the CIA and how it safeguards the information contained in the Crystal Solution. We also talked about the requirement for Crystal Solution to regularly replace the encryption keys on the workplace PCs. It must be updated periodically to stop hackers from accessing our accounts or data. The effects of backdoor assaults, proxy firewalls, and possible dangers to the company's data were explained to us.

To summarize, this assignment showed us that hackers or intruders may enter our system at any moment, therefore we need to safeguard our devices by often changing the encryption key. It also taught us the effects of a backdoor attack on any business and how to use proxy firewalls to defend our system. I also learned about a Banking Management System abuse example from this project.

References

- **University slides (Online)**

[March 10, 2023]

- **Software Security (Book)**

Author:Er. Shankar N Adhikari Buddha publication
[March 11, 2023]

- **Application security(Online)**

https://courses.lumenlearning.com/suny-hccc-ma-124-1/chapter/discussion-problem-solving-application/
[March 11, 2023]

- **Cloud Computing(Online)**

https://byjus.com/bank-exam/basics-of-cloud-computing-for-ibps-so-and-sbi-so-exam/
[March 12, 2023]

- **Misuse case diagram(Online)**

https://online.visual-paradigm.com/app/diagrams/#diagram:proj=0&type=UseCaseDiagram&width=11&height=8.5&unit=inch
[March 12, 2023]

Report
Marking Scheme

Student ID : _____ **Student Name: _____**

Criteria	Marks Allocated	Student Mark
Task 1 • Misuse case • Threats (5*1mark=5) • Attacks (5*1mark=5) • Risk Reduction ways (5*1mark=5) • Controls (5*1mark=5)	 10 5 5 5 5	
Task 2 • Common Vulnerabilities and Threats • Threat Model • Security Controls • CIA Security Issues in the cloud • Solutions for Security Issues • Security ways while data transfer on the cloud	 10 10 10 10 10 10	
Conclusion	**5**	
References	**5**	
Total	**100**	