Information Security and Risk Management at XYZ Bank

Posted on September 17, 2019

Part A

Security Policy

The XYZ Bank ensure the security, privacy and integrity of their customers and clientele through the deployment of necessary equipment and procedures that ensure physical and electronic security for their personal, financial and transactional information against all possible risks and threats.

The system includes the public and private sections. The public sections do not require a password or authorization and do not contain any information related to the visitor of the site. However, the system records information such as data and time of access, IP address, location and browser of the visitor. The private section of the site is password protected and requires complete authorization as it contains private and confidential data of individual clients.

Industry-approved and updated security techniques and strategies are deployed to ensure complete protection of the data that belongs to the bank and our clients. Some of these strategies include password-protected authorization, SSL encryption for Digital ID, encrypted security for Bank servers, software and hardware-based firewalls, etc.

The data belonging to clients and the Bank will remain confidential and undisclosed.

Subjects

1. Bank clients
2. Account holders
3. Branch Managers
4. Executive Members of Bank
5. Security Officials

Objects

1. Transactions
2. Requests

3. Database

Access Rights

1. Client
    - Access account information
    - Withdraw
    - Deposit
    - Request loan/remittance
2. Bank Official
    - Access client information
    - Edit/update information
    - Accept/decline requests

Part B

The given system of authentication is based on a simple Authentication Protocol that would involve the generation of public and private keys as the fingerprint impressions are input using the given device.

In the given authentication protocol, five basic steps of authentication will be followed that are described below:

1. First of all, the parameters are established for the biometric characteristics that will be used for authentication purposes. In our case, it is a fingerprint impression of the client.
2. Once the fingerprint impression has been scanned by the device, the web client station will be contacted for the fingerprint data, which will be stored on a centralized server that can be cloud-based or physical. (Joint Task Force, 2020)
3. As a response to a generated query, the server will generate a notification that contains biometric information related to the given parameters.
4. The input will be scanned and searched amongst the data on the server, and a notification regarding the match will be generated.
5. After a detailed and descriptive comparison of the records, the selected record will be returned to the client server. If no match is found, authentication will be declined.

Once the authentication process ends, the system displays the message indicating whether access is granted or denied.

In this entire process, the role of certification is to manage the public key that is generated during the process. The certification will bind the identity/fingerprint details to the cryptographic key. That will generate a token in response to it containing identity, public key, timestamp, and signature. Once the

timestamp expires, the public key expires as well.

Part C

- Intercept Transaction Process
- Intercept Bank Server
- Intercept Client PC
- Intercept Network
- Hacker
- Malicious Insider
- Spoofing
- Access LAN
- Hack System
- Keylogger
- Eavesdropping
- Bypassing Security Protocols
- Eavesdropping
- Virus / Trojan
- Trojan
- Access Servers
- Break Security Protocol
- Steal Password
- Achieve System Authorization
- Exploit Private and Confidential Data

Possible Risks And Threats

Since the Online Banking System involves highly sensitive, private and confidential financial transactions, it is also prone to several risks and threats that can put the reputation and sustainability of the Bank at stake. Because it is a financial institution, it is also a hot cake for hackers, intruders and nefarious users for malicious purposes.

One of the most common and critical risks involves the risk of data interception by hackers. In order to intercept the bank network and gain access to servers to steal confidential information, hackers may use several tactics, including phishing, spoofing, eavesdropping, Trojans and worms, viruses, SSL injections, etc. In order to protect the system from such vulnerabilities, several security protocols must be deployed in layers to make the system foolproof.

Another serious threat to the system servers is the nefarious insiders. These can be anyone, including fired employees, security officers with malicious intent, etc. These are the most critical risks and can often stay unnoticed and totally anonymous since they are very well aware of the weak spots or

loopholes of the system. Therefore, special physical and electronic security protocols must be deployed.

Part D

Audit Logs

The audit logs for the Online Banking System will contain:

1. UserType: AccountHolder, Employee, SecurityMember, ExecutiveMember, admin
2. ActionPerformed: AccessPersonalInfo, AccessAccountInfo, AccessServer, AccessBranchInfo, etc. (Basel Committee on Banking Supervision, 2021)
3. IP Address
4. Physical Location: country, city, address.
5. Time of Access
6. Date of Access
7. Duration of Access
8. Number of returns

Access Control Policy

The Audit Log is a highly sensitive and detailed data composition that must not be authorized to everyone. In order to ensure privacy of online client activities as well as transparency of online activities by various types of users, only security officials will be given access to the Audit Logs. These security officials will be highly authorized individuals who must abide by the system protocols. In order to access these logs, they must go through various levels of security, including a high-level encoded password, biometric verification, etc.

Only these officials will have access to the audit logs. However, they will not have the permission to edit or delete these logs.

Part E

Audit Logs, also known as audit trails, are the chronological order of the security-related details that are recorded over a period of time. These logs actually serve as documented evidence and proof of any suspicious or alarming activity that must be audited, investigated or inquired about by the security officials. The audit logs are helpful for system investigators and security officials as they can be interpreted to detect if any suspicious, unnoticed activity is going on in the system. The details in the log can also help in detecting the location from where these malicious attempts are being made.

Other than audit logs, multiple layered security protocols, hybrid security techniques, and strategies can also help reduce the impact of these vulnerabilities.

References

Joint Task Force. (2020). *Security and privacy controls for information systems and organizations* (NIST SP 800-53 Rev. 5). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-53r5

Basel Committee on Banking Supervision. (2021). *Principles for operational resilience*. Bank for International Settlements. https://www.bis.org/bcbs/publ/d516.htm