SENG2250 A3

Date: . .
Page:

1,

a) - It states that a customer can use the mobile app via a WIFI connection, this may be a security issue as wireless networks are more vulnerable to attacks, these threats may include:
- Eavesdropping
- Jamming
- MITM attacks
- Rogue clients
- Cryptographic threats

A possible countermeasure to theause threats could be the use of WPA (Wi-Fi protected access), which provides stronger data encryption compared to WEP and and also has user authentication

- It states that both a customer & employee may access banking operations via a website. The potential security issues here are:
- Eavesdropping
- stealing data
- Trojan horse

A possible countermeasure for these threats could be the use of SSL (Secure Socket Layer), which will provide both confidentiality and integrity between user->server interaction.

b)

If a bank employee were to be told to modify a customers daily cash transfer limit the following steps must be taken for the employee (Access Control Mechanisms)

1, Identification, this is usually provided by the employee with an ID. The system needs to know who its working with

2, Authentication, this is provided by the employee with a secret (password). This gives user access to syst with 2FA

3, Authorisation, This will determine if the employee has the correct permission to perform the task. This is based off ACL

4, Accountability, This ensures all actions taken by the employee are linked to an authorised account (system logs)

With all these steps performed/passed employee may do task as long as customer passes their checks.

Date: . .
Page:

c) SAML would be the best option in my opinion. This was a toss up between SAML and Kerberos as they both provide authentication and authorisation services. As a bank is a high security entity SAML would be a better choice for online bank management as the relying party and identity provider can be digitally signed & verified by both parties.

The issue I found with Kerberos was that in a larger domain, if it was compromised, it would take longer to rectify and higher risk

OAuth does not provide authentication to a high level thus this option was ruled out also.

Date:
Page:

d) IPsec is the chosen secure connection service for travelling / remote employees as it boasts the highest degree of security among its competitors (SSL & SSH). This was a tossup between IPsec and SSL/TLS as they both support certificate-based user authentication. Another advantage with IPsec is that it encrypts / authenticates all traffic at the IP level which I believe is the most logical placement of security

Although SSL/TLS was an attractive option it is generally considered a lower security deployment and thus marginally ruled out as a banking environment is considered high security

Although SSH is commonly used for remote access to resources there have been numerous examples of vulnerabilities such as trickbot, cryptosink and kaji malware which essentially abuse the SSH keys, this history turned me away from this option.