OPEN UNIVERSITY MALAYSIA

HUTECH
Đại học Công nghệ Tp.HCM

MID-TERM ASSIGNMENT REPORT

CBSE4103
SOFTWARE ENGINEERING

MAR 2025

HUTECH

STUDENT'S NAME: TA DUY THANH TAI

STUDENT ID: 2254030103

CLASS: 22BOIT02

EMAIL: thanhtai12122004@gmail.com

INSTRUCTOR: **Le Viet Linh**

Table of Contents

1. Introduction

The financial industry has witnessed a significant digital transformation, leading to an increase in cyber threats. Small to medium-sized banks face unique challenges in safeguarding sensitive customer data due to limited resources compared to larger financial institutions. Cybersecurity threats such as data breaches, phishing attacks, and malware attacks have been on the rise, creating a pressing need for strong security measures.

The importance of cybersecurity in banking cannot be overstated. According to a 2023 IBM Cost of a Data Breach Report, the average cost of a data breach in the financial industry is approximately $5.85 million per incident (IBM Security, 2023). This highlights the need for small to medium-sized banks to implement robust security measures to protect sensitive financial data and maintain customer trust.

This assignment explores the development of a cybersecurity system designed to protect customer financial data from evolving cyber threats. It includes an analysis of security challenges, critical security requirements, a proposed security architecture, security testing methodologies, deployment strategies, and ethical implications of cybersecurity in banking. Additionally, real-world case studies are provided to illustrate the importance of strong cybersecurity measures in the banking sector.

2. Security Challenges in the Banking Industry

Banks face multiple cybersecurity threats, which can lead to financial losses, reputational damage, and regulatory penalties. The increasing digitization of financial transactions has opened new avenues for cybercriminals to exploit vulnerabilities.

2.1 Cyber Threats

Phishing Attacks: Phishing is a social engineering attack where attackers trick users into revealing sensitive information, such as usernames, passwords, and credit card details. Attackers commonly use fake emails and fraudulent websites that mimic legitimate banking portals. According to IBM's 2023 Cost of a Data Breach Report, phishing is the second most common attack vector, accounting for 16% of all breaches (IBM Security, 2023). A real-world example of phishing was the 2016 Bangladesh Bank heist, where hackers used phishing emails to gain access to the bank's SWIFT system, resulting in the theft of $81 million. This incident emphasizes the need for strong email security protocols, employee training programs, and phishing detection tools to mitigate such threats.

Ransomware Attacks: Ransomware encrypts a victim's data and demands payment for decryption. Financial institutions are prime targets because they store vast amounts of sensitive customer data. A notable example is the 2017 WannaCry ransomware attack, which affected businesses globally, including banks, and caused estimated damages of $4 billion (CSO Online, 2017). Ransomware prevention strategies include regular backups, endpoint protection, network segmentation, and staff training to recognize suspicious activity.

Insider Threats: Employees or contractors with access to critical systems may intentionally or unintentionally expose sensitive data. Insider threats are particularly difficult to detect as they involve authorized users misusing their privileges. The 2019 Capital One breach was caused by a former employee who exploited a misconfigured web application firewall, exposing data of over 100 million customers. Implementing role-based access control (RBAC), activity logging, and real-time anomaly detection can help reduce insider threats.

Distributed Denial of Service (DDoS) Attacks: DDoS attacks overwhelm banking systems with excessive traffic, making services unavailable to customers. This can lead to loss of customer trust and regulatory scrutiny. In 2012, major U.S. banks such as JPMorgan Chase and Bank of America suffered a large-scale DDoS attack, disrupting online banking services for weeks. DDoS mitigation strategies, such as cloud-based traffic filtering, AI-based detection, and rate-limiting mechanisms, are crucial for preventing these attacks.

Emerging Threats:

- **Deepfake Fraud**: Cybercriminals use AI-generated deepfakes to impersonate bank officials and execute fraudulent transactions.
- **Supply Chain Attacks**: Attackers target third-party vendors to gain access to a bank's infrastructure.

2.2 Regulatory and Compliance Challenges

Small to medium-sized banks must comply with various regulations to ensure customer data protection:

- **General Data Protection Regulation (GDPR)** (General Data Protection Regulation, n.d.) mandates strict data protection measures.
- **ISO/IEC 27001: Information Security Management** (International Organization for Standardization, n.d.) provides guidelines for implementing security controls.
- **Federal Financial Institutions Examination Council (FFIEC) Cybersecurity Guidelines** (Federal Financial Institutions Examination Council, n.d.) set cybersecurity standards for financial institutions.

2.3 Necessity of a Robust Cybersecurity System

A well-designed cybersecurity system is essential to:

- Prevent financial losses and reputational damage.
- Protect customer-sensitive information from breaches.
- Ensure compliance with national and international regulations.
- Maintain uninterrupted banking operations.

3. Critical Security Requirements

A robust cybersecurity system must ensure data confidentiality, integrity, and availability.

3.1 Data Confidentiality

- **Encryption**: Implementation of AES-256 encryption for data in transit and at rest.
- **Secure Communication**: Use of TLS 1.3 for encrypting online transactions.
- **Access Control**: Enforcing role-based access control (RBAC) to ensure only authorized personnel can access sensitive data.

3.2 Data Integrity

- **Cryptographic Hashing**: Utilizing SHA-256 hashing to prevent unauthorized data modifications.
- **Digital Signatures**: Ensuring the integrity of transactions through cryptographic authentication mechanisms.
- **Audit Logs**: Maintaining detailed logs of all transactions for compliance verification and forensic analysis.

3.3 Data Availability

- **Redundant Systems**: Implementing cloud-based failover solutions to ensure service continuity.
- **DDoS Protection**: Deploying traffic filtering mechanisms and AI-based threat detection systems to prevent service disruptions.
- **Automated Incident Response**: Utilizing AI-driven threat mitigation tools to detect and neutralize cyber threats in real-time.

4. Layered Security Architecture

A multi-layered cybersecurity approach ensures comprehensive protection by integrating different security controls at various levels of the IT infrastructure. This layered defense strategy is crucial in safeguarding customer financial data against cyber threats.

4.1 Perimeter Security

- **Firewalls**: Act as a barrier between internal and external networks, filtering malicious traffic.
- **Virtual Private Networks (VPNs)**: Encrypt internet connections to ensure secure remote access for bank employees.
- **Intrusion Detection and Prevention Systems (IDS/IPS)**: Monitor network activity and prevent unauthorized access (MITRE Corporation, n.d.).

4.2 Network Security

- **Zero Trust Architecture (ZTA)**: Assumes no user or system is trustworthy by default, requiring continuous verification.
- **Network Segmentation**: Dividing the bank's network into separate zones to minimize the spread of cyber threats.
- **Access Control Lists (ACLs)**: Restrict traffic flow based on predefined security policies.

4.3 Application Security

- **Secure Software Development Life Cycle (SDLC)**: Incorporating security at every stage of software development.
- **Web Application Firewalls (WAFs)**: Protect against common web-based attacks such as SQL injection and cross-site scripting (XSS).
- **Multi-Factor Authentication (MFA)**: Requires users to verify identity through multiple authentication methods.

4.4 Data Security

- **Encryption Techniques**: Utilizing AES-256 and TLS 1.3 for secure data transmission and storage.
- **Database Security Measures**: Implementing database access controls, data masking, and regular audits.
- **Data Loss Prevention (DLP)**: Prevents unauthorized sharing of sensitive information.

4.5 Endpoint Security

- **Antivirus and Endpoint Detection and Response (EDR)**: Protects workstations, mobile devices, and servers from malware.
- **Bring Your Own Device (BYOD) Policies**: Ensures security of personal devices accessing the bank's systems.
- **Mobile Device Management (MDM)**: Controls access to sensitive data from mobile devices.

5. Security Testing

Security testing is a critical component of a cybersecurity strategy, ensuring the banking system is resilient against cyber threats. It helps identify vulnerabilities before attackers can exploit them, ensuring data integrity, confidentiality, and availability.

5.1 Importance of Security Testing

Security testing is essential to:

- **Identify Vulnerabilities**: Detect security flaws before they can be exploited.
- **Ensure Regulatory Compliance**: Meet industry standards such as ISO 27001, GDPR, and PCI DSS.
- **Strengthen Risk Management**: Reduce the likelihood of financial loss due to cyberattacks.
- **Maintain Operational Continuity**: Ensure that banking services remain available and secure.
- **Boost Customer Trust**: Demonstrate a proactive approach to protecting customer data.

5.2 Types of Security Testing

5.2.1 Vulnerability Assessment

Vulnerability assessments are crucial for identifying and prioritizing potential security weaknesses in a bank's network, applications, and infrastructure. These assessments involve automated scanning tools that evaluate the security posture by checking for known vulnerabilities and recommending remediation measures. Common tools used in vulnerability assessments include:

- **Nessus**: A widely used vulnerability scanner that detects and categorizes security flaws across various platforms, including servers, databases, and network devices. Nessus provides comprehensive reports detailing vulnerabilities and suggested fixes.
- **OpenVAS**: An open-source vulnerability scanning tool that identifies security issues and provides remediation recommendations. OpenVAS is known for its extensive vulnerability database, which is regularly updated to include new security threats.
- **Qualys**: A cloud-based vulnerability management tool that offers continuous monitoring and assessment of network security. Qualys provides detailed insights into vulnerabilities and helps prioritize them based on severity and potential impact.

These tools perform scans to identify weaknesses such as outdated software, misconfigurations, missing patches, and weak passwords. The results of vulnerability assessments guide IT teams in prioritizing and addressing vulnerabilities to enhance the overall security posture of the bank.

5.2.2 Penetration Testing (Ethical Hacking)

Penetration testing, also known as ethical hacking, involves simulating real-world cyberattacks to evaluate the effectiveness of security defenses and identify exploitable vulnerabilities. Ethical hackers, also known as white-hat hackers, use various attack techniques to attempt to breach the bank's systems. Penetration testing typically includes the following phases:

1. **Planning and Reconnaissance**: This phase involves gathering information about the target system, including network topology, IP addresses, and potential entry points. Ethical hackers use tools such as Nmap, Wireshark, and Metasploit to conduct reconnaissance.
2. **Scanning**: Ethical hackers use scanning tools to identify open ports, services, and vulnerabilities. Tools such as Nessus, OpenVAS, and Nikto are commonly used in this phase.
3. **Exploitation**: In this phase, ethical hackers attempt to exploit identified vulnerabilities to gain unauthorized access to the system. Techniques include SQL injection, cross-site scripting (XSS), and buffer overflow attacks.
4. **Post-Exploitation**: Once access is gained, ethical hackers assess the extent of the breach and attempt to escalate privileges to gain deeper access to the system. This phase helps determine the potential impact of a successful attack.
5. **Reporting and Remediation**: After completing the tests, ethical hackers compile a detailed report outlining vulnerabilities, attack vectors, and recommendations for remediation. The report helps the bank's IT team implement necessary security measures to mitigate identified risks.

Regular red team vs. blue team exercises further enhance the bank's security posture. The red team (ethical hackers) simulates adversarial attacks, while the blue team (defenders) responds to these attacks, improving incident response capabilities and identifying areas for improvement.

5.2.3 Security Code Review

Security code review involves a thorough analysis of application source code to identify security weaknesses and ensure that secure coding practices are followed. The review process includes:

- **Static Analysis**: Automated tools, such as SonarQube, Fortify, and Veracode, are used to scan the source code for common security vulnerabilities like SQL injection, cross-site scripting (XSS), buffer overflows, and insecure API usage. These tools provide detailed reports highlighting potential issues and suggesting remediation steps.
- **Manual Code Review**: Security experts manually inspect the source code to identify complex security flaws that automated tools might miss. This review focuses on areas such as authentication, authorization, input validation, error handling, and secure data storage.
- **Secure Coding Guidelines**: The review ensures that the code adheres to secure coding practices, such as those outlined in the OWASP Top 10. These guidelines help developers minimize risks and create more secure applications.

By conducting regular security code reviews, banks can identify and address vulnerabilities early in the development lifecycle, reducing the risk of security breaches in production environments.

5.2.4 Security Audits and Compliance Testing

Security audits and compliance testing are essential for ensuring that the bank's security framework, policies, and response mechanisms meet industry standards and regulatory requirements. The process includes:

- **Internal Audits**: Conducted by the bank's internal security team, these audits assess the effectiveness of security controls, policies, and procedures. The team reviews documentation, interviews personnel, and examines system configurations to identify gaps and areas for improvement.
- **External Audits**: Third-party auditors, such as certified public accountants (CPAs) or specialized security firms, conduct external audits to provide an unbiased assessment of the bank's security posture. These audits often focus on compliance with regulations such as ISO 27001, GDPR, PCI DSS, and the FFIEC Cybersecurity Guidelines.
- **Compliance Testing**: Involves testing the bank's systems and processes to ensure they meet regulatory requirements. This includes reviewing data protection measures, access controls, incident response plans, and employee training programs.

Regular security audits and compliance testing help banks identify and address security gaps, ensuring continuous improvement and adherence to industry standards.

5.2.5 Threat Modeling

Threat modeling involves mapping potential cyber threats and their impact on banking operations. It provides a structured methodology for assessing cybersecurity risks and improving defensive measures. The process includes:

- **Asset Identification**: Identify critical assets, such as customer data, financial transactions, and IT infrastructure, that need protection.
- **Threat Identification**: Identify potential threats, including cybercriminals, insider threats, and third-party risks. Use resources such as the MITRE ATT&CK Framework to understand adversarial tactics and techniques.
- **Vulnerability Identification**: Assess vulnerabilities within the banking system that could be exploited by identified threats. This includes software vulnerabilities, misconfigurations, and human factors.
- **Risk Analysis**: Evaluate the impact and likelihood of each threat, and prioritize them based on risk levels. Tools such as STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege) can help categorize and assess threats.
- **Mitigation Strategies**: Develop and implement security controls to mitigate identified risks. This includes measures such as encryption, access controls, network segmentation, and employee training.

By regularly performing threat modeling, banks can stay ahead of evolving cyber threats and enhance their security posture. This proactive approach helps identify potential risks and develop effective strategies to mitigate them before they can be exploited by attackers.

6. Deployment Process

The deployment of a cybersecurity system in banking follows a structured approach to integrate security at every phase.

6.1 Implementation Phases

- **Planning Phase**: Identify security requirements, conduct risk assessments, and define access control measures.
- **Development Phase**: Implement secure coding practices and integrate security within the software development lifecycle.
- **Testing Phase**: Conduct penetration testing, vulnerability assessments, and security audits before deployment.
- **Deployment Phase**: Roll out security controls, monitor real-time threats, and implement security policies.
- **Maintenance and Monitoring**: Continuously update security controls, monitor for threats, and apply patches.

6.2 Patch Management and Updates

- **Automated Patch Deployment**: Utilize automated tools to ensure timely deployment of security patches and updates, minimizing the risk of vulnerabilities.
- **Change Management Policies**: Implement change management policies to document and review security updates before implementation, ensuring they do not introduce new vulnerabilities.
- **Security Information and Event Management (SIEM)**: Use SIEM solutions for real-time monitoring and analysis of security events, enabling quick detection and response to threats.

6.3 Incident Response and Recovery

A well-defined Incident Response Plan (IRP) ensures swift action in case of cyberattacks, minimizing the impact on banking operations.

1. **Detection and Analysis**: Identify security breaches through monitoring tools and analyze the extent of the attack.
2. **Containment and Mitigation**: Isolate affected systems to prevent the spread of the attack and mitigate its impact.
3. **Eradication and Recovery**: Remove the threat from the systems and restore affected services to normal operation.
4. **Post-Incident Review**: Conduct a thorough review of the incident to identify lessons learned and improve security measures.

Banks should also establish Disaster Recovery Plans (DRP) to ensure business continuity in the event of cyberattacks, including regular backups, failover solutions, and communication plans.

7. Ethical Implications of Cybersecurity

Cybersecurity practices must align with ethical considerations to protect customers, employees, and institutions while upholding legal and moral responsibilities.

7.1 Data Privacy and Consent

Financial institutions handle vast amounts of sensitive customer data, including personal details, financial transactions, and credit history. To ensure ethical data management, banks must:

- **Obtain Informed Consent**: Clearly communicate how customer data will be used and obtain explicit consent.
- **Ensure GDPR Compliance**: Comply with privacy regulations such as the General Data Protection Regulation (GDPR).
- **Limit Data Collection**: Only collect necessary data to minimize exposure in the event of a breach.
- **Data Encryption**: Use strong encryption protocols to secure personal information, ensuring data confidentiality.

7.2 Employee Surveillance and Ethical Monitoring

Banks implement security monitoring tools to detect insider threats, but excessive surveillance can infringe on employee privacy. Ethical cybersecurity practices should:

- **Define Clear Policies**: Inform employees about monitoring practices and the reasons behind them.
- **Implement Least Privilege Access**: Restrict system access based on job roles to reduce misuse risks.
- **Ensure Transparency**: Use ethical oversight to prevent excessive or discriminatory monitoring.

7.3 AI and Automation in Cybersecurity

The use of Artificial Intelligence (AI) and Machine Learning (ML) in cybersecurity has ethical implications, including:

- **Bias in AI Algorithms**: Fraud detection systems must avoid unfairly targeting specific demographics.
- **AI-Powered Cyberattacks**: Criminals are leveraging AI to create sophisticated phishing and malware attacks, requiring banks to enhance their AI-driven defenses.
- **Automated Decision-Making**: AI should be used to assist human analysts, not replace critical security decision-making.

7.4 Responsible Disclosure of Security Vulnerabilities

Banks should encourage ethical hacking and responsible disclosure programs where security researchers can report vulnerabilities safely.

- **Bug Bounty Programs**: Offering incentives for ethical hackers to report security issues.
- **Cooperation with Regulators**: Promptly addressing security flaws in collaboration with industry regulators.
- **Public Transparency**: Communicating security improvements to customers without revealing exploitable details.

A notable example is the Facebook-Cambridge Analytica (2018) scandal, which highlighted the risks of unethical data collection. Banks must prioritize responsible data handling to avoid similar issues.

8. Conclusion

The financial sector is increasingly vulnerable to cyber threats, making cybersecurity a top priority for small to medium-sized banks. Implementing a robust cybersecurity framework requires a layered security approach, encompassing network security, application security, endpoint protection, and data encryption.

Key recommendations for improving cybersecurity in banks include:

- **Zero Trust Architecture (ZTA)**: Ensuring no system or user is automatically trusted, requiring continuous verification.
- **Regular Penetration Testing and Vulnerability Assessments**: Identifying security flaws before attackers can exploit them.
- **Employee Security Training**: Raising awareness about phishing, ransomware, and insider threats.
- **Multi-Factor Authentication (MFA)**: Strengthening identity verification for customers and employees.
- **Cloud-Based Security Solutions**: Enhancing data redundancy and backup protection through cloud-based services.
- **AI-Driven Cybersecurity**: Leveraging AI-powered tools for fraud detection, threat intelligence, and real-time threat monitoring.

Cybersecurity is an ongoing process, requiring banks to continuously update their security measures, adopt best practices, and comply with evolving regulatory requirements. By doing so, they can protect customer data, maintain operational continuity, and safeguard their reputation in the financial industry.

The ethical implications of cybersecurity practices must also be considered to ensure responsible data handling and avoid potential misuse of security systems. Financial institutions must prioritize data privacy, transparency, and cooperation with ethical hackers and regulators to build a secure and trustworthy banking environment.

9. References

- IBM Security. (2023). *Cost of a data breach report*. Retrieved from https://www.ibm.com/security/data-breach
- General Data Protection Regulation (GDPR). Retrieved from https://gdpr.eu/
- International Organization for Standardization. (n.d.). *ISO/IEC 27001: Information security management*. Retrieved from https://www.iso.org/isoiec-27001-information-security.html
- Federal Financial Institutions Examination Council (FFIEC). (n.d.). *Cybersecurity*. Retrieved from https://www.ffiec.gov/cybersecurity.htm
- MITRE Corporation. (n.d.). *MITRE ATT&CK cybersecurity framework*. Retrieved from https://attack.mitre.org/
- SANS Institute. (n.d.). *Security research white papers*. Retrieved from https://www.sans.org/white-papers/
- Open Web Application Security Project (OWASP). (n.d.). *Security testing guide*. Retrieved from https://owasp.org/www-project-web-security-testing-guide/
- Hern, A. (2018, March 20). *Cambridge Analytica scandal*. BBC News. Retrieved from https://www.bbc.com/news/technology-55855379