Assignment 1 - Software Security Requirements

João André Gomes Marques
Department of Informatic Engineering, University of Coimbra
uc2017225818@student.uc.pt

Leonardo Oliveira Pereira
Department of Informatics Engineering, University of Coimbra
uc2020239125@student.uc.pt

Introduction

In today's evolving digital landscape, ensuring the security of software systems is critical. This report analyses into the meticulous process of identifying, analyzing, and validating security requirements for a home-banking application using the Security Quality Requirements Engineering (SQUARE) Methodology. The SQUARE methodology, developed at Carnegie Mellon University, provides a systematic approach to integrating security requirements into the early stages of software development.

This report, centers on a structured journey through the SQUARE Methodology, focusing on steps 2, 3, 4, 6, and 7. By identifying misuse scenarios, building attack trees and formulating strict security requirements, the aim is to strengthen the home-banking application against potential threats. Through a demanding validation process, the effectiveness of the security measures designed is guaranteed.

While progressing through the SQUARE Methodology, this report aims to illuminate the multifaceted approach required to secure modern home-banking applications. By integrating security considerations from the start and promoting collaboration, SQUARE ensures the development of secure and client-approved software solutions.

Step 2: Identify Security Goals

The purpose of Step 2 in SQUARE is for the stakeholders to formally agree on a set of prioritized security goals for the project. Without overall security goals for the project, it is impossible to identify the priority and relevance of any security requirements that are generated. In addition, the establishment of security goals scopes the rest of the SQUARE process.

Business Goal

The home-banking application should combine advanced security features with user-friendly functionalities, ensuring a safe and convenient banking experience for customers, while promoting trust and loyalty in the online banking platform.

Security Goals

- **Confidentiality:** The system should guarantee that user data, including personal information and transaction details, is confidential and accessible only to authorized users.
- **Integrity:** The system should ensure the integrity of user data and transactions, preventing unauthorized modifications.

- **Availability:** Ensure the availability of banking services, with minimal disruptions.
- **Authentication:** All the users should be authenticated to access the home-banking application and perform operations.
- **Authorization:** The system should have proper authorization controls to restrict user actions based on their roles and privileges.

Step 3: Develop Artifacts

Before the requirements engineering team and stakeholders can generate a comprehensive set of security requirements, the team must collect a complete set of artifacts of the system. This work focus only on **misuse case scenarios/diagrams** and **attack trees** as artifacts that should be collected.

Misuse Case Scenarios

Number:	MC1	
Name:	Unauthorized Acess	
Scope:	User Authorization Concerns	
Priority:	_ Low _ Medium _x_ High	
Deployment Environment:	_x_ Intranet __ Extranet/Internet	
Security Attributes Afefected:	_x_ Confidentiality _x_ Integrity __ Availability	
Description:	An attacker attempts to access another user's account by exploiting weak passwords, stolen credentials, or bypassing authentication mechanisms.	
Post-conditions:	Worst Case Threat:	The unauthorized users logs onto another user's account.
	Wanted Prevention Guarantee:	Multi-factor authentication.
	Wanted Detection Guarantee:	User receives notifications that they are trying to access the account.
	Wanted Recovery Guarantee:	Freezing of all possible operations in the application.

Figure 1: MC1) Unauthorized Access

Number:	MC2	
Name:	Phishing Attack	
Scope:	User Credentials Concerns	
Priority:	_ Low _ Medium _x_ High	
Deployment Environment:	__ Intranet _x_ Extranet/Internet	
Security Attributes Afefected:	_x_ Confidentiality _x_ Integrity __ Availability	
Description:	A malicious entity tries to mislead users by sending fake emails or messages, posing as the bank, to trick them to reveal their login credentials or sensitive information.	
Post-conditions:	Worst Case Threat:	The malicious entety gets the login credentials and sensitive information.
	Wanted Prevention Guarantee:	Multi-factor authentication.
	Wanted Detection Guarantee:	User receives notifications that they are trying to access the account.
	Wanted Recovery Guarantee:	Freezing of all possible operations in the application.

Figure 2: MC2) Phishing Attack

Number:	MC3	
Name:	Data Manipulation	
Scope:	User Data Concerns	
Priority:	_ Low _ Medium _x_ High	
Deployment Environment:	_x_ Intranet __ Extranet/Internet	
Security Attributes Afefected:	_x_ Confidentiality _x_ Integrity __ Availability	
Description:	An insider attacker attempts to modify user data, transaction details, or account balances to mess up financial records or commit fraud.	
Post-conditions:	Worst Case Threat:	The inside attacker has privileges to do what he wants. His actions are never caught.
	Wanted Prevention Guarantee:	Implement strict access control policies limiting modification rights.
	Wanted Detection Guarantee:	Data modifications are monitorized by system administrators.
	Wanted Recovery Guarantee:	Remove privileges rights from the inside attacker.

Figure 3: MC3) Data Manipulation

Number:	MC4	
Name:	Denial of Service (DoS) Attack	
Scope:	Application Service Concerns	
Priority:	__ Low _x_ Medium __ High	
Deployment Environment:	__ Intranet _x_ Extranet/Internet	
Security Attributes Afefected:	__ Confidentiality __ Integrity _x_ Availability	
Description:	An attacker attempts to overwhelm the home-banking application's server resources, network bandwidth, or other system components with a flood of traffic, rendering the service unavailable to legitimate users.	
Post-conditions:	Worst Case Threat:	The attacker overwhelm the home-banking application rendering the service unavailable to legitimate users.
	Wanted Prevention Guarantee:	Configure firewalls to block suspicious IP addresses.
	Wanted Detection Guarantee:	Traffic monitoring systems to detect unusual patterns and filter out malicious traffic.
	Wanted Recovery Guarantee:	Develop a comprehensive incident response plan to quickly identify, assess, and mitigate DoS attacks, minimizing service downtime.

Figure 4: MC4) Denial of Service (DoS) Attack

Attack Trees

Attack trees provide a formal, hierarchical way of describing the security threats to a system based on the types of attacks that could happen and how they could be realized. The diagrams represent attacks in a tree structure, where an attacker's goal is listed as the root node and the leaves represent different ways to achieve that goal.

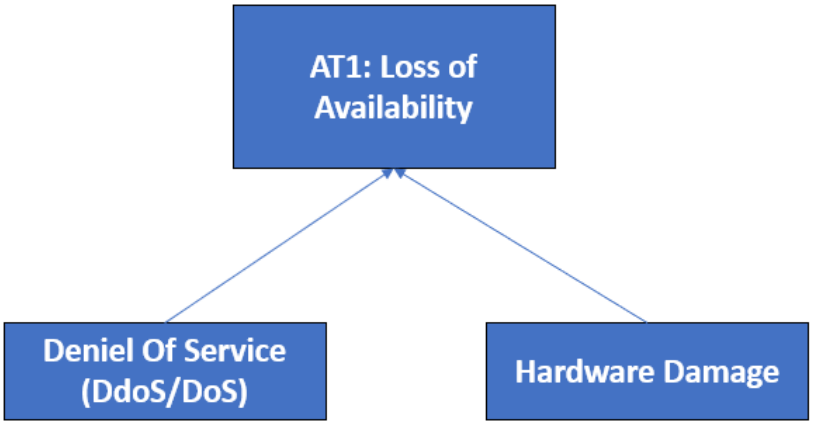

Figure 5: AT1) Loss of Availability

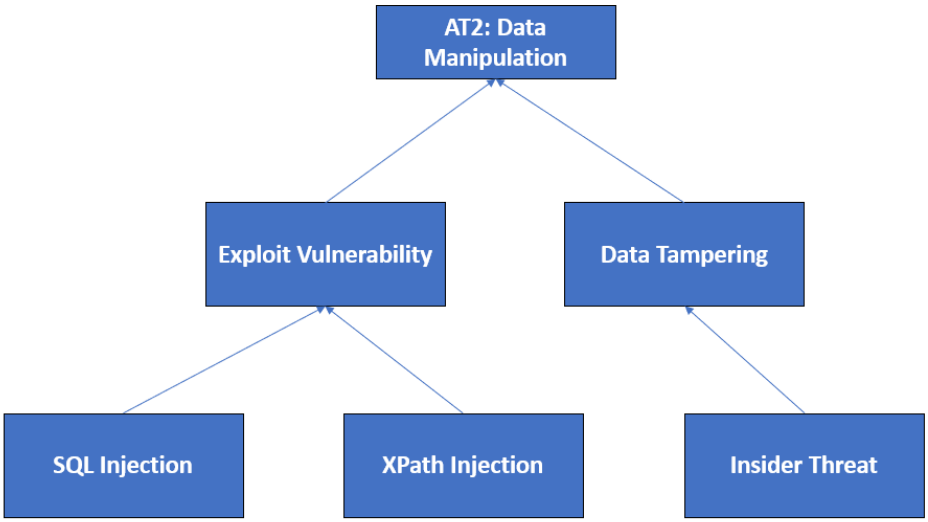

Figure 6: AT2) Data Manipulation

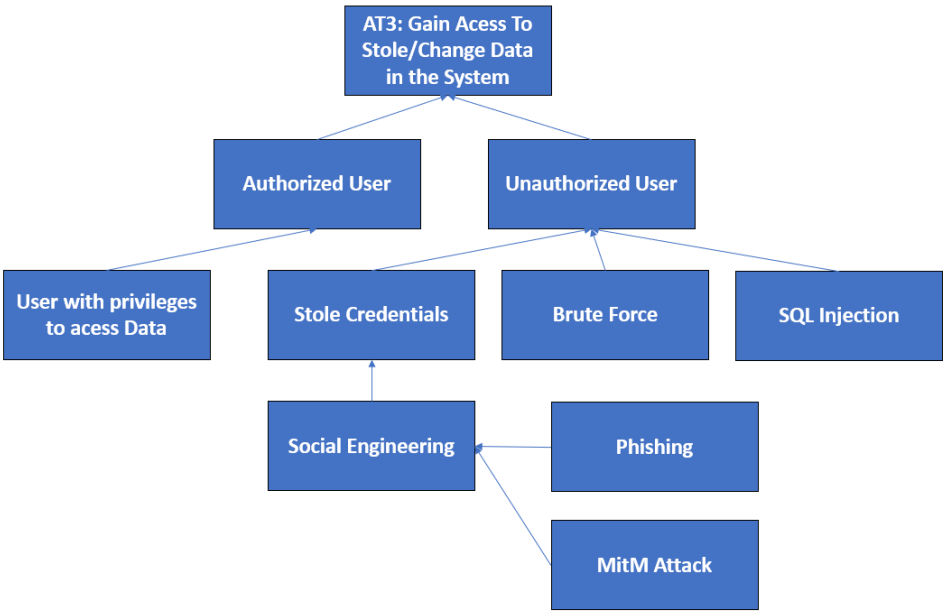

Figure 7: AT3) Gain Access To Stole/Change Data in the System

Misuse Case	Attack Trees
MC4	AT1
MC3	AT2
MC1, MC2	AT3

Figure 8: Mapping Between Misuse Cases and Attack Trees

Step 4: Perform Risk Assessment

The purpose of this step in the SQUARE process is to identify the vulnerabilities and threats that face the system, the likelihood that the threats will materialize as real attacks, and any potential consequences of an attack.

Asset Valuation

- **A1-User Account Data:** Personal information of customers including names, addresses, contact details, social security numbers, and financial data.
- **A2-Network Infrastructure:** Routers, switches, and communication channels facilitating data exchange.
- **A3-Application Servers:** The servers hosting the home-banking application and the database servers storing user data.

ID Asset	Information Asset	Criterion 1: Impact to Revenue	Criterion 2: Impact to Profitability	Criterion 3: Impact to Public Image	Weighted Score
	Weights	*50*	*30*	*20*	*100*
A1	User Account Data	0.8	0.7	1	81
A2	Network Infrastructure	0.7	0.7	0.5	66
A3	Application Servers	0.7	0.7	0.5	66

Figure 9: Asset Valuation

Threat Identification

A list of general threats should be compiled and reviewed by those most knowledgeable about the system to identify applicable threats.

Threat	Threat	Example
T1	CyberSecurity Breaches	Data breaches, malware, phishing attacks, MitM attacks, XSS attacks,information disclosure of confidential or private planning documents
T2	Insider Threats	Employees with mailicious purposes
T3	Compromised Servers	Denial of Service (DoS) Attacks, hardware damage

Figure 10: Threats examples

Vulnerability Identification

Identifying vulnerabilities allows organizations to understand their risks and take proactive measures.

Threat ID	Threat Description	Vulnerability	Possible Vulnerabilities
T1	CyberSecurity Breaches	V1	Poorly Sanitized Inputs
		V2	No backup system
		V3	Lack of encryption
T2	Insider Threats	V4	Lack of monitoring
		V5	Inadequate Access Controls
T3	Compromised Servers	V6	Lack of DoS Protection

Figure 11: Vulnerabilities examples

Threat and Vulnerability Assessment (TVA)

A comprehensive evaluation of an organization's information security infrastructure.

				User Account Data	Network Infrastructure	Application Servers				
				A1	A2	A3				
		CyberSecurity Breaches	T1	V1 V2 V3	V1 V3	V1 V2 V3				
		Insider Threats	T2	V4 V5	V4 V5	V4 V5				
		Compromised Servers	T3		V6	V6				
			number of vulnerabilities	5	5	6				
Priority of Controls	1	less priority	2		3		4		5	higher priority

Figure 12: TVA table followed by the number of vulnerabilities on each column and the range of the priority of controls

Risk Control

Risk control strategies are used to manage, mitigate, or eliminate risks.

Assets	Selected Control	Selected Metric
A1 - User Account Data A2 - Network Infrastructure A3 - Application Servers	Defence - Document/implement/monitor policies for data operations (authentication, encryption)	Cost of implementation (price of HW, price of SW) Cost of maintenance (costs with equipment, goods, ...) Number of attacks attempts detected Number of attacks attempts unsuccessful Number of attacks successful
A1 - User Account Data A2 - Network Infrastructure A3 - Application Servers	Defence - Implement vigilance/logging system	Cost of implementation Cost of maintenance Number of attacks attempts detected Number of attacks attempts unsuccessful Number of attacks successful
A2 - Network Infrastructure A3 - Application Servers	Defence - Implement Rate Limiting and Throttling/ and Employ Intrusion Detection and Prevention Systems (IDPS)	Cost of implementation Cost of maintenance Number of attacks attempts detected Number of requests Number of attacks successful

Figure 13: Controls strategies

Step 6: Elicit Security Requirements

This step involves the elicitation of security requirements.

R-01	The system shall implement multi-factor authentication (MFA) to ensure secure user login.
R-02	The system shall implement secure communication protocols to prevent man-in-the-middle attacks.
R-03	The system shall implement role-based access control (RBAC) to restrict access based on user roles and privileges.
R-04	The system should encrypt sensitive data both at rest and in transit to protect user information from unauthorized access.
R-05	A patch management process should be establish to promptly address known vulnerabilities.
R-06	Establish real-time monitoring to detect and respond to suspicious activities promptly.
R-07	Develop an incident response plan to handle security incidents, including data breaches and unauthorized access attempts.
R-08	Configure servers, databases, and network devices securely, following industry best practices and disabling unnecessary services.
R-09	The system shall deploy DDoS mitigation services to detect and mitigate large-scale Distributed Denial of Service attacks, ensuring uninterrupted service availability.
R-10	The system shall implement regular data backups and establish a disaster recovery plan to restore services and data in the event of a breach or system failure.

Figure 14: Security Requirements

Step 7: Categorize Requirements

Security requirements are categorized into groups with a unique name for each.

Group A: Authentication and Access Control 1. The system shall implement multi-factor authentication (MFA) to ensure secure user login. 2. Role-based access control (RBAC) implementation.	**Group B: Data Protection** 1. The system should encrypt sensitive data both at rest and in transit to protect user information from unauthorized access.
Group C: Infrastructure and Software Security 1. A patch management process should be establish to promptly address known vulnerabilities. 2. The system shall deploy DDoS mitigation services to detect and mitigate large-scale Distributed Denial of Service attacks, ensuring uninterrupted service availability.	**Group D: Data Backup and Recovery** 1. Develop an incident response plan to handle security incidents, including data breaches and unauthorized access attempts. 2. The system shall implement regular data backups and establish a disaster recovery plan to restore services and data in the event of a breach or system failure.
Group E: Network and Communication Security 1. The system shall implement secure communication protocols to prevent man-in-the-middle attacks. 2. Configure servers, databases, and network devices securely, following industry best practices and disabling unnecessary services.	**Group F: Monitoring and Incident Response** 1. Establish real-time monitoring to detect and respond to suspicious activities promptly.

Figure 15: Categorization Requirements

Conclusion

This in-depth analysis and evaluation of the security of the home-banking application provided valuable information on the intricate web of challenges and opportunities in the digital financial domain.

Through the systematic application of methodologies such as the SQUARE (Security Quality Requirements Engineering) model, security requirements were meticulously identified, analysed and validated. These requirements cover various domains, including robust authentication mechanisms, secure communication protocols, strict access controls and proactive monitoring and incident response strategies.

The assets, threats and vulnerabilities identified emphasise the complex landscape in which the home-banking application operates. By categorising and addressing these security requirements, the application is strengthened against potential risks, guaranteeing a secure environment for users to carry out their financial transactions.

The strategies and countermeasures outlined in this analysis serve not only as defensive measures, but as a testament to the unwavering commitment to security and customer satisfaction. By adopting these principles, the home-banking application not only fulfils regulatory requirements but also exceeds user expectations, establishing itself as a model of excellence in the field of online banking.

In conclusion, this thorough security analysis has fortified the home-banking application against diverse threats. By adopting a proactive stance, staying abreast of emerging threats, and continuously refining security measures, the home-banking application stands as a resilient and trustworthy platform in the dynamic landscape of online banking, prioritizing customer safety and satisfaction.

#Link to access general google sheet!

#Link to access the Risk Assessment!