CHAPTER I
INTRODUCTION

I.1 Background

In this digital era, most business processes and data are stored in computer systems (Slavković, Pavlović, Mamula Nikolić, Vučenović, & Bugarčić, 2023). With the increasing digitalization, this brings both benefits and risks to a company (Zolkover, Kharkiv, Stashkevych, & Mehdizade, 2022). A cybercriminal can disrupt business processes or even steal important company and customer data (Hasham, Joshi, & Mikkelsen, 2019).

Systemic cybersecurity risks in banking context are noteworthy because they encompass cyber incidents which can disrupt the business in question and could threaten the business and the financial stability of the larger organization (Dupont, 2019). The danger is exacerbated owing to the interconnectivity and cross-border nature among information systems, where cyber warfare can permeate and reach multiple business processes cumulatively within the least amount of time (Luo, 2022). All major economic business processes such as *payment services*, money withdrawal, balance checking, and settlement services can be disrupted or even stopped due to a cyberattack that attacks the entire information system running at a bank (Wewege, Lee, & Thomsett, 2020).

Indonesia itself has recently experienced several shocking cyber-attacks, one of which is the ransomware attack on *Bank Syariah Indonesia* (Fitriani, Subagiyo, & Asiyah, 2023). This attack caused almost all business activities of *Bank Syariah Indonesia* to come to a halt, with services being disrupted (Hartono, 2023). Apart from the halted services, the hackers also claimed to have access to all sensitive data belonging to *Bank Syariah Indonesia* and its customers (Fitriani, Subagiyo, & Asiyah, 2023).

The second phenomenon is an attack on the Electoral Commission's *(KPU)* system during the 2024 general election *(PEMILU)* (Nurkamiden, 2024). In this

attack, the *KPU* claimed that there were hundreds of millions of requests for access to the *KPU* website, which was the work of a hacker (Vitorio Mantalean, 2024). This phenomenon resulted in the *KPU* website being inaccessible and the data from the calculations being unable to be updated on the *KPU* website (Anggi Muliawati, 2024).

Cyberattacks are an attack on the lifeblood regions of any cooperative structure and these incidents shed light on that (Lis & Mendel, 2019). The intrusion on *Bank Syariah Indonesia* through ransomware not only caused a halt on the operation, but it also caused other sensitive details to be released which caused a breach of trust and had years' worth of legal and out a firm in financial trouble to deal with (Fitriani, Subagiyo, & Asiyah, 2023). The 2020 attack on Indonesia's *KPU*, during its general election, roused unnecessary conspiracy theories about the deteriorating state of politics in the nation. Such events are enough to warrant for remarkable measures to be in place in safeguarding public institutions especially in the current global phenomenon of digitization.

Along with the increasing digitalization of business processes, a leading Indonesian state-owned bank prepared a business product in application form, namely Digital Merchant Point of Sale (POS) Platform. This platform is an application that assists the course of business activities by offering payment option facilities, recording sales, preparing inventory management, and disbursing sales proceeds straight to the owner's account. Due to the continuous growth of users and business transactions, the platform requires security to be its highest priority.

Developed by one of the leading banks in Indonesia, the Digital Merchant POS Platform encompasses a variety of features to streamline the businesses. Such integration encompasses WebAPI, *WebStore*, *Payment Service* as well as *Checkout Service*, implying that there is a need to secure the transmission of data as well as the integration pathways across various security zones. Unlike the system previously mentioned, the architecture of the platform makes use of multicategory security zones which are: *Public Zone*, *DMZ (Demilitarized*

Zone), *Trusted Zone* and *Restricted Zone*. Each category and zone support diverse components of the system with each having particular security objectives.

Currently, attention to system security is often overlooked during the development process (Heidt, Gerlach, & Buxmann, 2019). System architecture and security frequently do not receive maximum focus and review due to time constraints. Companies or organizations tend to prioritize the performance of their business processes and potential profits. Nevertheless, system security is an issue that allows the smooth running of business operations of an organization without being hampered. A system that is designed with security since the inception of development may not require much caution against attacks from any quarter (Sean Peek, 2023). The likelihood of adverse effects on a system by internal and external attacks may thus be minimal (Butun, Osterberg, & Song, 2020).

The solution selected is the MITRE ATT&CK framework considering it is able to map attack patterns based on real-world cyber incidents (Al-Sada, Sadighian, & Oligeri, 2024). As opposed to conventional security frameworks, this ATT&CK framework allows for the detailing of the tactics, techniques, and procedures (TTP) of an attacker, which can then be used to bolster the corresponding defenses (Georgiadou, Mouzakitis, & Askounis, 2021). This is very pertinent to the recent cyber attacks in Indonesia. These include the ransomware attack on BSI and the DDoS attack on the *KPU* system, where understanding the inner workings of the attacks could serve as a barrier for similar occurrences in the future (Fitriani, Subagiyo, & Asiyah, 2023).

With an integrated service system and numerous security zones which includes the *Public Zone*, DMZ, *Trusted Zone*, and even *Restricted Zones*, the Digital Merchant POS Platform has highly complex architecture that requires a complete and systematic security approach (Betancourt, Glock, Kharitonov, Kern, Liu, Sax, & Becker, 2020). The integration of the MITRE ATT&CK framework with harm profiling methodology allows for the structuring of

security analysis for every system component as well as each security zone and their interactions (Pell, Moschoyiannis, Panaousis, & Heartfield, 2021). This platform earns special attention due to its complex architecture that deals with sensitive transactions as well as customer data across various security boundaries (Strom, Battaglia, Kemmerer, Kupersanin, Miller, Wampler, Whitley, & Wolf, 2017).

Moreover, integrating the MITRE ATT&CK framework helps meet fundamental security prerequisites of the platform such as PCI DSS and ISO/IEC 27001:2022 (Kinnunen, 2022). The framework helps with the audit and documentation requirements imposed by these standards through security vulnerabilities identification and remediating them evidentially (Legoy, Caselli, Seifert, & Peter, 2020). This approach enhances the security of the platform and helps in achieving regulatory compliance, which is important for the management of trust of stakeholders and business operations in the financial technology industry (Darem, Alhashmi, Alkhaldi, Alashjaee, Alanazi, & Ebad, 2023).

International Bank's current platform requires a considerable change when it comes to its structure. Although it is functional in nature, International Bank has been enforcing security measures such as multi-factor authentication and management of encrypted *end-to-end*, building sessions and recording and logging audits' accurately. Also, due to security regulations like PCI DSS and ISO/IEC 27001:2022 that the architecture must meet.

To solve these issues, this research seeks to develop a security architecture for the capstones' digital Merchant POS Platform using the harm profiling method employed within the MITRE ATT&CK framework. The STRIDE method was created by Microsoft in the late 1990 to classify types of threats a computer system or application could be vulnerable to. The MITRE ATT&CK framework rounds this out by giving a detailed matrix about real-life attack patterns, techniques and plans of how to mitigate those, all based on how attackers have acted in the past.

In any case, such a security architecture integrated into the existing architecture of the application will ensure significant benefit for the application owners through the reduction of potential losses from attacks in the future. Ensuring the integrity of sensitive financial data is a must, and only the correct implementation of robust security architecture would allow the Digital Merchant POS Platform to maintain user and business partner trust while complying with regulatory requirements and industry security standards.

I.2 Problem Statement

Based on the background that has been revealed, the problem statement in this study are as follows:

1. What are the potential threats and vulnerabilities in the Digital Merchant Point of Sale (POS) Platform based on the STRIDE and MITRE ATT&CK frameworks?
2. How can a security architecture be designed for the Digital Merchant POS Platform to ensure comprehensive protection through a defense-in-depth strategy?
3. How effective is a comprehensive threat modeling architecture in identifying attack vectors and enhancing security measures across the Digital Merchant POS Platform?

I.3 Research Objectives

Based on the problem statement, the objectives of this study are as follows:

1. Identify and analyze potential threats to the Digital Merchant POS Platform using the STRIDE method and map them to different architectural zones.
2. Design a comprehensive threat modeling architecture that incorporates STRIDE and MITRE ATT&CK frameworks to identify potential attack vectors and enhance the security measures of the Digital Merchant POS Platform.

3. Implement appropriate security controls and mitigation strategies based on the identified threats within each security zone.

I.4 Research Scopes

1. The object of this research focuses on the Digital Merchant Point of Sale (POS) Platform owned by a leading Indonesian state-owned bank.
2. This research focuses on the domain of application security architecture with emphasis on the four-zone security model and integration with existing platform components.
3. The design focuses on a multi-layered defense strategy for securing the platform, addressing key components, attack vectors, and threat scenarios.

I.5 Research Benefit

Based on the problem statement and research objectives, this research is expected to provide the following benefits:

1. For the bank, this research is useful in designing and implementing a security architecture for the Digital Merchant POS Platform that supports secure business processes and protects sensitive financial data.
2. For Telkom University, this research is expected to be an opportunity to establish cooperation from the results of internships that have been carried out by students at the bank.
3. For researchers, this research can improve their understanding and ability to apply theory in creating secure architecture with defense-in-depth strategies, particularly in financial technology systems.
4. For other researchers, it is hoped that this research can be a reference and source of information in implementing and creating secure architecture for similar banking application systems, especially within the Indonesian banking context.

I.6 Systematization of Writing

This research is described with the following systematic writing:

Chapter I. Introduction

This chapter explains the problem of the research with the help of background information, objectives, scope of the research, advantages of the study, and even the structure of the writing . As a result, it outlines the importance of the topic relating to cybersecurity threat modeling on financial systems and mentions the most important gaps in the available research.

Chapter II. Literature Review

This chapter provides the theoretical underpinnings of the work by presenting relevant literature as well as research done in the past. In addition, the chapter outlines the STRIDE and MITRE ATT&CK frameworks. as well as cyber security hygiene and threat modeling techniques. A thorough evaluation of previous work is done to support the appropriate choice of the frameworks utilized in this study.

Chapter III. Methods

This chapter describes the research methodology employed to achieve the study objectives. It includes the problem-solving framework, data collection techniques, data processing methods, and the evaluation criteria. The Design Science Research Methodology (DSRM) is used as the primary approach, outlining each step taken from problem identification to solution implementation.

Chapter IV. Results and Discussion

This chapter analyzes the current security structure of the Digital Merchant POS Platform, highlighting any weaknesses or gaps. It is described in detail how threat modeling was carried out, using the STRIDE and MITRE ATT&CK frameworks. Also in this chapter, a proposed security architecture is discussed along with evaluation of its effectiveness through several assessments, focusing on the effectiveness of the multi-layered approach.

Chapter V. Evaluation

The chapter encompasses an evaluation of security architecture in interlocking with the expert's reviews and test results. Furthermore, it discusses the deviation

of performance metrics and the measures in relation to the performance rating of the industry. This is done by triangulating the performance indicators, expert reports and conducting tests on the system in order to validate the efficiency of the security solution.

Chapter VI. Conclusion and Suggestion

This chapter is prepared with the conclusions arrived from the research accompanied by the findings and analysis discussed previously. It also answers the questions that were formulated at the start of this research and highlights the major contributions this research was able to achieve. In addition, suggestions are given with respect to strengthening the security of digital financial platforms and avenues for future research are outlined.