

TABLE OF CONTENTS

CHAPTER I

INTRODUCTION.....	1
I.1 Background.....	1
I.2 Problem Statement.....	4
I.3 Research Objectives.....	4
I.4 Research Scopes.....	5
I.5 Research Benefit.....	5
I.6 Systematization of Writing.....	5

CHAPTER II

LITERATURE REVIEW.....	8
II.1 Vulnerabilities and Threat in Banking.....	8
II.2 STRIDE Methodology.....	9
II.3 MITRE ATT&CK.....	9
II.4 Attack Category Analysis Framework.....	10
1. STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege).....	10
2. DREAD (Damage Potential, Reproducibility, Exploitability, Affected Users, Discoverability).....	11
3. PASTA (Privilege Escalation, Authentication, Session Management, Tampering, Authorization, Sensitive Data, Trust).....	11
II.5 Attack Techniques Analysis Framework.....	12
1. MITRE ATT&CK.....	12
2. Cyber Kill Chain.....	13
1. Diamond Model of Intrusion Analysis.....	13
II.6 Reasons for choosing STRIDE and MITRE ATT&CK.....	14

CHAPTER III

METHODS.....	23
III.1 Conceptual Framework.....	23

III.2 Systematization of Problem Solving.....	26
III.3 Data Collection.....	29
III.4 Data Processing.....	30
III.5 Evaluation Method.....	31
CHAPTER IV	
RESULTS AND DISCUSSION.....	33
IV.1 Architecture Analysis.....	33
IV.1.1 Current Architecture Overview.....	34
IV.1.2 Current Architecture Security Analysis.....	35
IV.1.3 Security Requirements Analysis.....	39
IV.2 Threat Analysis.....	41
IV.2.1 System Decomposition.....	42
IV.2.4 MITRE ATT&CK Mapping.....	53
IV.2.5 Risk Assessment.....	57
IV.2.6 Security Zone Network Architecture.....	61
IV.2.7 Security Threat Architecture.....	64
IV.3 Attack Scenario.....	67
IV.3.1 Mitigation Solution Based on Attack Scenario.....	73
CHAPTER V	
EVALUATION.....	79
V.1 Threat Scenarios and Mitigation Overview.....	79
V.2 Expert Evaluation.....	85
CHAPTER VI	
CONCLUSION AND SUGGESTION.....	89
VI.1 CONCLUSION.....	89
VI.2 SUGGESTION.....	91
REFERENCES.....	93