การประเมินความเสี่ยงของความต้องการด้านความมั่นคงของระบบสารสนเทศทางการธนาคารโดยอิงแบบรูปการโจมตี

นายกฤษดา รองรัตน์

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

บทคัดย่อและแฟ้มข้อมูลฉบับเต็มของวิทยานิพนธ์ตั้งแต่ปีการศึกษา 2554 ที่ให้บริการในคลังปัญญาจุฬาฯ (CUIR)
เป็นแฟ้มข้อมูลของนิสิตเจ้าของวิทยานิพนธ์ ที่ส่งผ่านทางบัณฑิตวิทยาลัย
The abstract and full text of theses from the academic year 2011 in Chulalongkorn University Intellectual Repository (CUIR)
are the thesis authors' files submitted through the University Graduate School.

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต
สาขาวิชาวิศวกรรมซอฟต์แวร์ ภาควิชาวิศวกรรมคอมพิวเตอร์
คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2559
ลิขสิทธิ์ของจุฬาลงกรณ์มหาวิทยาลัย

RISK ASSESSMENT OF SECURITY REQUIREMENTS OF BANKING INFORMATION SYSTEM BASED ON ATTACK PATTERNS

Mr. Krissada Rongrat

A Thesis Submitted in Partial Fulfillment of the Requirements
for the Degree of Master of Science Program in Software Engineering
Department of Computer Engineering
Faculty of Engineering
Chulalongkorn University
Academic Year 2016

Copyright of Chulalongkorn University

หัวข้อวิทยานิพนธ์	การประเมินความเสี่ยงของความต้องการด้านความมั่นคงของระบบสารสนเทศทางการธนาคารโดยอิงแบบรูปการโจมตี
โดย	นายกฤษดา รองรัตน์
สาขาวิชา	วิศวกรรมซอฟต์แวร์
อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก	รองศาสตราจารย์ ดร.ทวิตีย์ เสนีวงศ์ ณ อยุธยา

คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย อนุมัติให้นับวิทยานิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญามหาบัณฑิต

.....คณบดีคณะวิศวกรรมศาสตร์

(รองศาสตราจารย์ ดร.สุพจน์ เตชวรสินสกุล)

คณะกรรมการสอบวิทยานิพนธ์

.....ประธานกรรมการ

(รองศาสตราจารย์ ดร.วิวัฒน์ วัฒนาวุฒิ)

.....อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก

(รองศาสตราจารย์ ดร.ทวิตีย์ เสนีวงศ์ ณ อยุธยา)

.....กรรมการ

(ผู้ช่วยศาสตราจารย์ ดร.เกริก ภิรมย์โสภา)

.....กรรมการภายนอกมหาวิทยาลัย

(ผู้ช่วยศาสตราจารย์ ดร.ชวลิต ศรีสถาพรพัฒน์)

กฤษดา รองรัตน์ : การประเมินความเสี่ยงของความต้องการด้านความมั่นคงของระบบสารสนเทศทางการธนาคารโดยอิงแบบรูปการโจมตี (RISK ASSESSMENT OF SECURITY REQUIREMENTS OF BANKING INFORMATION SYSTEM BASED ON ATTACK PATTERNS) อ.ที่ปรึกษาวิทยานิพนธ์หลัก: รศ. ดร.ทวิตีย์ เสนีวงศ์ ณ อยุธยา, 128 หน้า.

การประเมินความเสี่ยงด้านความมั่นคงถือเป็นกระบวนการที่สำคัญสำหรับการดำเนินงานของระบบสารสนเทศใด ๆ รวมถึงระบบในภาคการธนาคาร เมื่อธนาคารเริ่มต้นหรือดำเนินการโครงการระบบสารสนเทศ วิศวกรด้านความมั่นคงหรือนักวิเคราะห์ทางธุรกิจในโครงการจะดำเนินการตรวจสอบความสมเหตุสมผลของข้อกำหนดความต้องการด้านความมั่นคง ว่าเป็นไปตามข้อกำหนดด้านความมั่นคงของภาคการธนาคารหรือไม่ ก่อนที่จะมีการตรวจสอบโดยผู้ตรวจสอบ

งานวิจัยนำเสนอวิธีการประเมินความเสี่ยงเบื้องต้นเพื่อช่วยทีมงานของโครงการในการตรวจสอบข้อกำหนดความต้องการด้านความมั่นคง โดยอาศัยการวิเคราะห์ความคล้ายคลึงกันของข้อความเพื่อระบุว่าข้อบังคับด้านความมั่นคงข้อใดที่ขาดหายไปจากความต้องการด้านความมั่นคงของธนาคารและมีการเสนอแบบจำลองความเสี่ยงเชิงปริมาณเพื่อกำหนดระดับความเสี่ยงที่เกี่ยวข้องกับข้อบังคับที่ขาดหายไปจากข้อกำหนดความต้องการ ระดับความเสี่ยงขึ้นอยู่กับระดับอันตรายใดๆ ที่อาจเกิดขึ้นจากการโจมตีระบบสารสนเทศเมื่อข้อบังคับด้านความมั่นคงที่ขาดหายไปนั้นไม่ได้รับการพัฒนาในระบบสารสนเทศ จากกรณีศึกษาในภาคการธนาคารในประเทศไทย ผู้วิจัยได้ประยุกต์ใช้วิธีที่เสนอในการประเมินความต้องการด้านความมั่นคงของธนาคารพาณิชย์ไทยกับแนวปฏิบัติที่ดีด้านเทคโนโลยีสารสนเทศของธนาคารแห่งประเทศไทย ผู้วิจัยประเมินประสิทธิภาพของการตรวจสอบการปฏิบัติตามข้อบังคับด้านความมั่นคงโดยใช้การวิเคราะห์ค่าเอฟ-เมเชอร์ และค่าความแม่น รวมทั้งตรวจสอบความสมเหตุสมผลของการประเมินความเสี่ยงโดยวิธีที่เสนอโดยใช้สหสัมพันธ์กับการประเมินความเสี่ยงโดยผู้เชี่ยวชาญด้านความมั่นคง

จากผลการประเมินสรุปได้ว่า การตรวจสอบการปฏิบัติตามข้อบังคับด้านความมั่นคงมีประสิทธิภาพสูงมาก และผลการประเมินระดับความเสี่ยงจากข้อบังคับด้านความมั่นคงที่ขาดหายไปมีสหสัมพันธ์ในเชิงบวกกับผลการประเมินโดยผู้เชี่ยวชาญ

ภาควิชา วิศวกรรมคอมพิวเตอร์ ลายมือชื่อนิสิต .....

สาขาวิชา วิศวกรรมซอฟต์แวร์ ลายมือชื่อ อ.ที่ปรึกษาหลัก .....

ปีการศึกษา 2559

5870902721 : MAJOR SOFTWARE ENGINEERING
KEYWORDS: SECURITY REQUIREMENT / RISK ASSESSMENT / ATTACK PATTERN / REGULATORY COMPLIANCE / TEXT SIMILARITY / BANKING

KRISSADA RONGRAT: RISK ASSESSMENT OF SECURITY REQUIREMENTS OF BANKING INFORMATION SYSTEM BASED ON ATTACK PATTERNS. ADVISOR: ASSOC. PROF. TWITTIE SENIVONGSE, Ph.D., 128 pp.

Security risk assessment is an important process for the implementation of any information systems including those in the banking sector. When a bank initiates or implements an information system project, requirements engineers or business analysts in the project conduct an initial validation of system security requirements to check if they comply with banking security regulations before an audit takes place.

This research presents an initial risk assessment method to assist the project team in validating security requirements of a banking information system. Text similarity analysis is used to identify which security regulations are missing from the security requirements of the bank, and a quantitative risk index model is also proposed to determine the level of risk associated with the regulations missing from the requirements. The risk level is based on the harm any potential attacks can do to the information system if the missing regulations are not implemented. Using a case study of banking in Thailand, we apply the method to assess security requirements of Thai commercial banks against the IT Best Practices of the Bank of Thailand. We evaluate the performance of security compliance checking in terms of F-measure and accuracy, and validity of risk assessment in terms of correlation with security expert judgment.

The evaluation results show that the performance of security compliance checking is very high and the level of risk resulting from the missing regulations has positive correlation with security expert judgment.

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

Department:	Computer Engineering	Student's Signature	.....
Field of Study:	Software Engineering	Advisor's Signature	.....
Academic Year:	2016		

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้สำเร็จลุล่วงเป็นอย่างดีได้ด้วยความกรุณาอย่างยิ่งจาก รองศาสตราจารย์ ดร.ทวิตีย์ เสนีวงศ์ ณ อยุธยา อาจารย์ที่ปรึกษาหลัก ซึ่งได้ให้โอกาสและแนวคิดในการทำวิทยานิพนธ์ ตลอดจนทักษะ แนวทางการแก้ไขปัญหาและความอดทนให้การวิจัยลุล่วงและประสบความสำเร็จ มาโดยตลอดระยะเวลาการศึกษาและการวิจัย ขอกราบขอบพระคุณเป็นอย่างสูงไว้ ณ ที่นี้ด้วย

ขอขอบพระคุณ รองศาสตราจารย์ ดร.วิวัฒน์ วัฒนาวุฒิ ประธานกรรมการสอบวิทยานิพนธ์ ผู้ช่วยศาสตราจารย์ ดร.เกริก ภิรมย์โสภา และผู้ช่วยศาสตราจารย์ ดร.ชวลิต ศรีสถาพรพัฒน์ กรรมการสอบวิทยานิพนธ์ที่ได้ให้คำแนะนำและชี้แนะแนวทางที่เป็นประโยชน์ต่อการทำวิทยานิพนธ์ในครั้งนี้

ขอขอบพระคุณคณาจารย์ทุกท่านที่ อบรม สั่งสอน ให้ความรู้ต่างๆ มากมายจนมีวันนี้

ขอกราบขอบพระคุณคุณพ่อ คุณแม่ ครอบครัวอันเป็นที่รัก และญาติๆ ทุกคน ที่ค่อยให้ความห่วงใย ทำให้มีความสุขทั้งกายและใจ และเป็นกำลังใจในการดำเนินชีวิตมาโดยตลอด

ขอขอบคุณ คุณปุณยนุช ขำนิล คุณศิริขวัญ ตรีทิพยรักษ์ และคุณอัลวิน หว่อง ที่ช่วยเหลือ สนับสนุน และให้กำลังใจในการเรียนและการทำวิทยานิพนธ์ในครั้งนี้

ขอขอบคุณ คุณวณัชณันท์ นักร้อง คุณสมปอง พรสุรทิน คุณจิราภรณ์ มุทิตา คุณธงเอก ศรจิตต์ คุณอานนท์ ฟุ้งนาคมรกต คุณพัสสุดา เอกวิทยานนทวี คุณไกร วิชรัตน์ และผู้ที่ให้ความช่วยเหลือทุกท่านในการประสานงานและตอบแบบสอบถามงานวิจัยให้เป็นผลสำเร็จ

ขอบคุณเพื่อนๆ พี่ๆ น้องๆ ห้องปฏิบัติการวิศวกรรมซอฟต์แวร์ ที่ภาควิชาวิศวกรรมคอมพิวเตอร์ทุกคน ที่ร่วมทุกข์ร่วมสุข แลกเปลี่ยนความรู้ แง่คิดต่างๆ ตลอดระยะเวลาที่ดำเนินการวิจัย ซึ่งให้ความสนุกสนาน และความอบอุ่นตลอดระยะเวลาที่อยู่ด้วยกัน

สารบัญ

หน้า

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

หน้า

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

หน้า

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

สารบัญตาราง

หน้า

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

สารบัญภาพ

หน้า

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ในปัจจุบันการพัฒนาด้านความมั่นคงของระบบสารสนเทศของการธนาคารในประเทศไทยจะต้องมีการสร้างข้อกำหนดความต้องการด้านความมั่นคง โดยอ้างอิงตามแนวปฏิบัติที่ดีสำหรับการควบคุมความเสี่ยงของระบบงานเทคโนโลยีสารสนเทศที่สนับสนุนธุรกิจหลัก (IT Best Practices) (ต่อไปนี้ขอเรียกว่า แนวปฏิบัติที่ดีฯ) ซึ่งแนวปฏิบัติที่ดีฯ นี้เป็นข้อตกลงร่วมกันระหว่างธนาคารแห่งประเทศไทยและธนาคารพาณิชย์ในประเทศไทย ดังนั้นก่อนที่ธนาคารพาณิชย์จะพัฒนาระบบสารสนเทศใด ๆ จะต้องตรวจสอบข้อกำหนดความต้องการด้านความมั่นคงกับแนวปฏิบัติที่ดีฯ นี้ก่อนโดยตรวจสอบด้วยผู้ตรวจสอบภายใน (Internal Auditor) ของธนาคารพาณิชย์ ในบางกรณีธนาคารพาณิชย์อาจพัฒนาระบบสารสนเทศก่อน แต่อย่างไรก็ตามระบบจะต้องได้รับการตรวจสอบโดยผู้ตรวจสอบภายในในภายหลัง และรายงานผลการตรวจสอบต่อธนาคารแห่งประเทศไทย

ในทางปฏิบัติข้อกำหนดความต้องการด้านความมั่นคงของระบบสารสนเทศจะถูกทวนสอบโดยวิศวกรความต้องการหรือนักวิเคราะห์ธุรกิจ (Requirement Engineer or Business Analyst) ในโครงการก่อนที่จะถูกตรวจสอบโดยผู้ตรวจสอบภายใน การทวนสอบจะทำให้มั่นใจได้ว่าข้อกำหนดความต้องการเป็นไปตามแนวปฏิบัติที่ดีฯ แต่เนื่องจากข้อกำหนดความต้องการด้านความมั่นคงมักจะถูกเขียนอยู่ในรูปแบบภาษาธรรมชาติ จึงทำให้การทวนสอบกับแนวปฏิบัติที่ดีฯ เป็นไปได้ยาก ส่งผลกระทบต่อเวลาที่ใช้ทวนสอบ อีกทั้งผลลัพธ์ที่ได้จากการทวนสอบยังขึ้นอยู่กับระดับความสามารถของวิศวกรความต้องการ จึงทำให้อาจเกิดความเสี่ยงต่อระบบที่จะพัฒนาขึ้นตามข้อกำหนดความต้องการหากข้อกำหนดความต้องการบางข้อขาดหายไปหรือยังไม่ครบถ้วนสมบูรณ์ ทำให้ระบบที่พัฒนาขึ้นอาจถูกโจมตีด้านความมั่นคงได้ ดังนั้นเพื่อเป็นการลดความเสี่ยงให้กับระบบที่จะพัฒนา การประเมินความเสี่ยงด้านความมั่นคงจากข้อกำหนดความต้องการด้านความมั่นคงจึงเป็นส่วนสำคัญในการป้องกันหรืออย่างน้อยเพื่อลดอันตรายที่จะเกิดขึ้นในอนาคตจากการโจมตีเหล่านั้น

งานวิจัยนี้นำเสนอแนวคิดและเครื่องมือในการวิเคราะห์ความเสี่ยงด้านความมั่นคงจากความต้องการด้านความมั่นคง โดยเริ่มจากการกำหนดความต้องการด้านความมั่นคงที่พึงจะมีสำหรับระบบสารสนเทศทางการธนาคาร โดยทำการวิเคราะห์ความต้องการด้านความมั่นคงสำหรับการธนาคารจากแนวปฏิบัติที่ดีฯ และนำเสนอเป็นข้อกำหนดความต้องการด้านความมั่นคงที่พึงจะมีซึ่งอยู่ในรูปแบบภาษาธรรมชาติ จากนั้นทำการวิเคราะห์ว่าแต่ละความต้องการด้านความมั่นคง สามารถ

ป้องกันแบบรูปการโจมตีแบบใดบ้าง โดยใช้ฐานข้อมูลแบบรูปการโจมตีจากองค์กรไมเทอร์ (MITRE) ทำให้สามารถนำมาคำนวณดัชนีความเสี่ยงด้านความมั่นคงได้หากมีข้อกำหนดความมั่นคงบางส่วนขาดหายไปหรือยังไม่ครบถ้วนสมบูรณ์ ดังนั้นในการประเมินความเสี่ยงของระบบสารสนเทศทางการธนาคารใด ๆ จะทำโดยการเปรียบเทียบความคล้ายของความต้องการด้านความมั่นคงของระบบสารสนเทศนั้นกับความต้องการด้านความมั่นคงที่พึงจะมีที่กำหนดไว้ตามแนวปฏิบัติที่ดีฯ ซึ่งความแตกต่างระหว่างความต้องการด้านความมั่นคงที่พบจะสะท้อนถึงข้อบกพร่องของความต้องการด้านความมั่นคงที่กำหนดให้กับระบบสารสนเทศ และสามารถนำไปคำนวณความเสี่ยงโดยรวมต่อการถูกโจมตีตามแบบรูปการโจมตีที่เกี่ยวข้องกับข้อบกพร่องนั้นได้

1.2 วัตถุประสงค์ของการวิจัย

1.2.1 เพื่อสร้างแบบจำลองการประเมินความเสี่ยงของความต้องการด้านความมั่นคงของระบบสารสนเทศทางการธนาคารโดยอิงแบบรูปการโจมตี และพัฒนาเครื่องมือสนับสนุนแบบจำลอง

1.3 ขอบเขตของการวิจัย

1.3.1 สร้างแบบจำลองการประเมินความเสี่ยงของความต้องการด้านความมั่นคงของระบบสารสนเทศทางการธนาคารโดยอิงแบบรูปการโจมตี

1.3.2 พิจารณาข้อมูลแบบรูปการโจมตีจากคาเปก [1] (ในเบื้องต้นพิจารณาการโจมตี 38 แบบ)

1.3.3 พิจารณาความต้องการด้านความมั่นคงที่พึงจะมีสำหรับการธนาคารจากแนวปฏิบัติที่ดีสำหรับการควบคุมความเสี่ยงของระบบเทคโนโลยีสารสนเทศที่สนับสนุนธุรกิจหลักจากธนาคารแห่งประเทศไทย

1.3.4 รองรับข้อกำหนดความต้องการด้านความมั่นคงที่อยู่ในรูปแบบภาษาธรรมชาติและเป็นภาษาอังกฤษเท่านั้น

1.3.5 พัฒนาเครื่องมือสนับสนุนแบบจำลองในรูปแบบโปรแกรมประยุกต์ ซึ่งสามารถนำเข้าเอกสารความต้องการด้านความมั่นคงของการธนาคารเพื่อประเมินความเสี่ยงและจัดลำดับความเสี่ยงตามประเภทของความต้องการ

1.3.6 ทดสอบและประเมินผลแบบจำลอง 4 ด้าน ดังนี้

1. ความถูกต้องของการจับคู่ของความมั่นคงที่พึงจะมีกับวิธีการบรรเทาการโจมตี
2. ประสิทธิภาพของการหาความแตกต่างระหว่างความต้องการด้านความมั่นคงที่พึงจะมีกับเอกสารความต้องการด้านความมั่นคงของการธนาคาร

3. ความสอดคล้องของค่าความเสี่ยงของความต้องการด้านความมั่นคงที่ขาดหายไปซึ่งได้จากเครื่องมือกับค่าความเสี่ยงจากผู้เชี่ยวชาญ

4. การวิเคราะห์ต้นทุนและผลประโยชน์

1.4 ประโยชน์ที่คาดว่าจะได้รับ

1.4.1 ได้แบบจำลองและต้นแบบเครื่องมือการประเมินความเสี่ยงของความต้องการด้านความมั่นคงสำหรับระบบสารสนเทศทางการธนาคาร

1.4.2 วิศวกรความต้องการหรือวิศวกรความมั่นคง สามารถนำผลการประเมินความเสี่ยงและความรู้จากการใช้งานแบบจำลองไปเป็นแนวทางในการพิจารณาความเสี่ยงด้านความมั่นคงและปรับปรุงข้อกำหนดความต้องการ

1.4.3 สามารถนำหลักการของแบบจำลองไปประยุกต์ใช้สำหรับความต้องการด้านความมั่นคงในธุรกิจอื่น

1.5 วิธีดำเนินการวิจัย

1.5.1 ศึกษาข้อมูลเอกสารและงานวิจัยที่เกี่ยวข้องกับหัวข้อการประเมินความเสี่ยงจากความต้องการ

1.5.2 ศึกษาข้อมูลความต้องการด้านความมั่นคงสำหรับการธนาคาร

1.5.3 ศึกษาข้อมูลแบบรูปการโจมตีที่ส่งผลกระทบต่อซอฟต์แวร์ และฮาร์ดแวร์ที่เกี่ยวข้องกับการธนาคาร

1.5.4 ออกแบบแบบจำลองการประเมินความเสี่ยงจากความต้องการด้านความมั่นคงสำหรับการธนาคาร

1.5.5 พัฒนาเครื่องมือสนับสนุนแบบจำลองการการประเมินความเสี่ยงจากความต้องการด้านความมั่นคงสำหรับการธนาคาร

1.5.6 ทดสอบแบบจำลองการการประเมินความเสี่ยงจากความต้องการด้านความมั่นคงสำหรับการธนาคารและเครื่องมือสนับสนุน

1.5.7 สรุปผลการวิจัย

1.5.8 เรียบเรียงและจัดทำบทความวิชาการ

1.5.9 เรียบเรียงและจัดทำวิทยานิพนธ์

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

1.6 ผลงานตีพิมพ์

ส่วนหนึ่งของวิทยานิพนธ์นี้ได้ตีพิมพ์และนำเสนอในการประชุมวิชาการดังนี้

1.6.1 บทความชื่อ “Risk Assessment of Security Requirements of Banking Information System Based on Attack Patterns” [2]

1. ชื่อผู้แต่ง Krissada Rongrat และ Twittie Senivongse
2. ตีพิมพ์ในวารสาร Studies in Computational Intelligence (SCI) สำนักพิมพ์ Springer
3. นำเสนอในงานประชุมวิชาการชื่อ 5th International Conference on Applied Computing & Information Technology (ACIT2017) ซึ่งจัดขึ้นในวันที่ 9-13 กรกฎาคม 2560 ณ เมืองฮามามัตสึ (Hamamatsu) ประเทศญี่ปุ่น

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

บทที่ 2
ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

2.1 ทฤษฎีที่เกี่ยวข้อง

ทฤษฎีที่เกี่ยวข้องอันเป็นประโยชน์ในการทำวิจัยแบ่งออกเป็น 6 ส่วน ได้แก่ การประเมินความเสี่ยง, วิศวกรรมความมั่นคงและความต้องการด้านความมั่นคง, มาตรฐานความมั่นคงที่เกี่ยวข้องกับสถาบันการธนาคาร คาเปก การสืบค้นสารมนเทศ และดัชนีความเสี่ยง

2.1.1 การประเมินความเสี่ยง

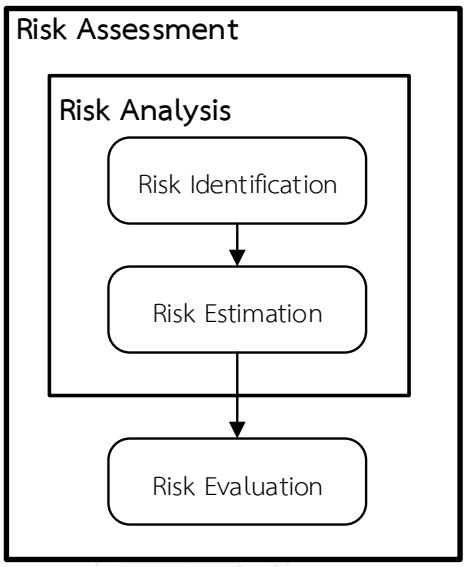
การประเมินความเสี่ยง (Risk Assessment) [3] เป็นกระบวนการแรกในกระบวนการบริหารจัดการความเสี่ยง องค์กรใช้การประเมินความเสี่ยงเพื่อกำหนดขอบเขตของโอกาสที่จะเกิดภัยคุกคาม และการมีส่วนร่วมของความเสี่ยงในระบบเทคโนโลยีสารสนเทศ (Information Technology system: IT system) ผ่านทางวัฏจักรการพัฒนาซอฟต์แวร์ (Software Development Life Cycle: SDLC) ซึ่งผลลัพธ์ของกระบวนการประเมินความเสี่ยงจะช่วยให้องค์กรสามารถระบุกระบวนการควบคุมได้อย่างเหมาะสม ทั้งในด้านการลด (Reducing) และการกำจัด (Eliminating) ความเสี่ยง ในระหว่างการดำเนินกระบวนการบรรเทาความเสี่ยง (Risk Mitigation)

เนื่องจากการประเมินความเสี่ยงให้ข้อมูลที่สำคัญในการคาดการณ์ความผิดพลาดที่อาจเกิดขึ้นได้อย่างมีประสิทธิภาพ ซึ่งการวิเคราะห์ความเสี่ยงต้องคำนึงถึงองค์ประกอบหลัก 3 ประการ [4] ได้แก่

1. ผลกระทบของความเสี่ยง (Risk Impact) โดยการพิจารณาความเสี่ยงของจุดบกพร่องต่าง ๆ ว่าเกิดผลกระทบต่อองค์กรอย่างไรบ้าง อาทิเช่น ทำให้เสียเวลาและค่าใช้จ่ายในการทำงาน ทำให้สูญเสียการควบคุมการทำงาน เป็นต้น ซึ่งจุดบกพร่องต่าง ๆ มีผลกระทบต่อระบบแตกต่างกันไปตามประเภทของจุดบกพร่อง
2. ความน่าจะเป็นของความเสี่ยงในการเกิดปัญหา (Problem) มีค่า ตั้งแต่ 0 ถึง 1 ตามระดับความน่าจะเป็นในการเกิดจุดบกพร่องนั้น
3. ความสามารถในการควบคุมความเสี่ยงที่เกิดขึ้น (Risk Control) เช่น การป้องกันไม่ให้ปัญหาของไวรัสคอมพิวเตอร์แพร่กระจายไปยังส่วนต่าง ๆ ภายในองค์กร เป็นต้น

กระบวนการในการประเมินความเสี่ยง [3] ประกอบด้วยกิจกรรม 2 กิจกรรมหลัก ดังภาพที่ 2.1 ได้แก่

1. การวิเคราะห์ความเสี่ยง (Risk Analysis) ซึ่งประกอบด้วย 2 กิจกรรมย่อย คือ การระบุความเสี่ยง (Risk Identification) และการประมาณความเสี่ยง (Risk Estimation)
2. การประเมินผลความเสี่ยง (Risk Evaluation)



ภาพที่ 2.1 กระบวนการบริหารจัดการความเสี่ยง [5]

2.1.1.1 การระบุความเสี่ยง

องค์กรควรระบุแหล่งความเสี่ยง ส่วนที่ได้รับผลกระทบ เหตุการณ์ (รวมถึงการเปลี่ยนแปลงของสภาพการณ์) สาเหตุของการเกิด และศักยภาพของผลสืบเนื่องที่อาจเกิดขึ้น จุดมุ่งหมายของขั้นตอนนี้คือการจัดทำบัญชีความเสี่ยงที่ครอบคลุมเหตุการณ์ต่าง ๆ ที่อาจส่งเสริม ขัดขวาง ลด เร่ง หรือชะลอการบรรลุวัตถุประสงค์ การระบุความเสี่ยงเป็นเรื่องสำคัญที่ต้องดำเนินการโดยไม่ต้องอ้างถึงโอกาสที่จะเกิด การระบุอย่างครอบคลุมเป็นสิ่งที่สำคัญมากเพราะความเสี่ยงที่ไม่ได้ถูกระบุในขั้นตอนนี้จะไม่ถูกนำไปวิเคราะห์ในขั้นตอนต่อไป

2.1.1.2 การประมาณการความเสี่ยง

การประมาณการความเสี่ยงเกี่ยวข้องกับการทำความเข้าใจความเสี่ยง ซึ่งจะทำให้ได้ข้อมูลสำหรับใช้ในการประเมินผลความเสี่ยงและการตัดสินใจขจัดความเสี่ยงด้วยวิธีการและกลยุทธ์ที่เหมาะสมที่สุด การประมาณการความเสี่ยงยังสามารถให้ข้อมูลนำเข้าสำหรับตัดสินใจทางเลือกในการจัดการความเสี่ยงในประเภทและระดับความเสี่ยงที่แตกต่างกันด้วย

การประมาณการความเสี่ยงเกี่ยวข้องกับการพิจารณาถึงสาเหตุและแหล่งความเสี่ยง ผลสืบเนื่องทั้งทางบวกและทางลบ รวมถึงโอกาสที่ผลสืบเนื่องเหล่านั้นจะเกิดขึ้น นอกจากนี้ควรทำการระบุปัจจัยที่มีผลต่อโอกาสและผลสืบเนื่อง ความเสี่ยงจากผลสืบเนื่อง รวมถึงปัจจัยร่วมอื่น ๆ ที่มีผลต่อความเสี่ยง สำหรับเหตุการณ์ที่มีผลสืบเนื่องหลายอย่างที่สามารถส่งผลต่อวัตถุประสงค์นั้น ต้องพิจารณาถึงประสิทธิผลและประสิทธิภาพของมาตรการควบคุมที่มีอยู่

แนวทางในการกำหนดเกณฑ์ผลสืบเนื่องและโอกาส รวมถึงแนวทางในการนำเกณฑ์ทั้งสองอย่างมาพิจารณาร่วมกันเพื่อกำหนดระดับความเสี่ยงนั้น ควรสะท้อนประเภทของความเสี่ยง สารสนเทศที่มี และจุดมุ่งหมายที่จะนำผลการประเมินความเสี่ยงไปใช้ แนวทางนี้ควรสอดคล้องกับเกณฑ์ความเสี่ยง ซึ่งควรพิจารณาความเกี่ยวโยงของความเสี่ยงและแหล่งความเสี่ยงที่แตกต่างกันเป็นสิ่งสำคัญ

2.1.1.3 การประเมินผลความเสี่ยง

จุดมุ่งหมายของการประเมินผลความเสี่ยง เพื่อช่วยในการตัดสินใจว่าความเสี่ยงใดต้องมีการจัดการและ จัดลำดับความสำคัญเพื่อดำเนินการจัดการความเสี่ยงบนพื้นฐานของผลลัพธ์ของการวิเคราะห์ความเสี่ยง การประเมินผลความเสี่ยงเป็นการเปรียบเทียบระดับความเสี่ยงที่พบระหว่างกระบวนการวิเคราะห์ความเสี่ยงกับเกณฑ์ความเสี่ยงที่กำหนดขึ้นเมื่อบริบทได้รับการพิจารณา โดยผลจากการเปรียบเทียบนี้ทำให้เห็นความจำเป็นในการจัดการความเสี่ยง

2.1.2 วิศวกรรมความมั่นคงและความต้องการด้านความมั่นคง

วิศวกรรมความมั่นคง [6] เป็นหลักการนำทฤษฎีความมั่นคง มั่นคง (Security Engineering and Security Requirements) มาใช้ในกิจกรรมความมั่นคง โดยการออกแบบและสร้างระบบที่สามารถป้องกันการโจมตีต่าง ๆ มีวัตถุประสงค์หลัก คือ เพื่อเปลี่ยนแปลงสถานะจากอันตรายเป็นสถานะความเสี่ยงที่ยอมรับได้ ซึ่งกระบวนการที่จำเป็นในวิศวกรรมความมั่นคงมีการวนซ้ำขั้นตอนที่จำเป็น ดังภาพที่ 2.2 โดยแต่ละขั้นตอนมีรายละเอียดดังนี้

1. ข้อกำหนด (Specification) ต้องกำหนดส่วนประกอบ (Components) และส่วนต่อประสาน (Interface) ทั้งหมดให้สมบูรณ์ เพราะถ้าหากไม่ระบุให้ครอบคลุมสถาปัตยกรรมทั้งหมดของระบบจะก่อให้เกิดช่องโหว่และถูกโจมตีในส่วนที่ยังไม่ได้ทำการระบุเป็นข้อกำหนดไว้

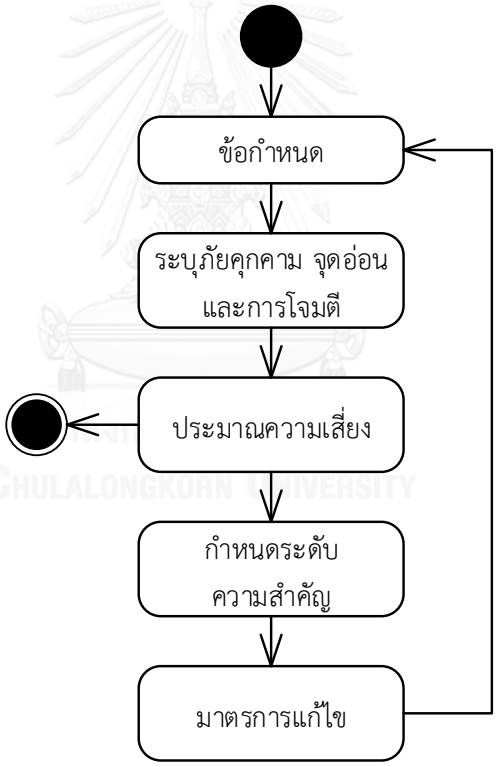
2. การระบุภัยคุกคาม ช่องโหว่ และการโจมตี (Identification of Threats, Vulnerabilities, and Attacks) เป็นการระบุภัยอันตรายและช่องโหว่ของส่วนประกอบรวมถึงส่วน

ต่อประสานของระบบ ซึ่งจะช่วยในการกำหนดรูปแบบการโจมตีที่จะเกิดและสามารถทำการป้องกันไว้ก่อนได้

3. การประมาณความเสี่ยง (Risk Estimation) ความเสี่ยงของการโจมตีที่อาจเกิดกับแต่ละส่วนประกอบ หรือส่วนต่อประสาน จะต้องพิจารณาตามความสัมพันธ์ระหว่างข้อกำหนดของภัยคุกคาม ช่องโหว่ และรูปแบบการโจมตี

4. กำหนดระดับความสำคัญ (Prioritization) ในกรณีที่มีความเสี่ยงสูงปรากฏในช่องโหว่ที่เกี่ยวข้องกับส่วนประกอบ หรือส่วนต่อประสาน จะต้องจัดลำดับความสำคัญไว้เป็นลำดับต้นๆ เพื่อการกำหนดมาตรการป้องกัน

5. มาตรการแก้ไข (Countermeasure) กำหนดแนวทางการแก้ไขตามภัยคุกคาม ช่องโหว่ และรูปแบบการโจมตี เพื่อนำไปใช้ซ้ำในขั้นตอนการระบุข้อกำหนดเพื่อลดช่องโหว่ของระบบ



ภาพที่ 2.2 ขั้นตอนทางวิศวกรรมความมั่นคง [6]

การระบุข้อกำหนดความต้องการ (Requirements Specification) เป็นสิ่งที่สำคัญในทุกๆ โครงการ ถ้าความต้องการดังกล่าวไม่เป็นไปตามข้อกำหนดที่เหมาะสม ระบบก็ไม่สามารถทำงานตามที่คาดหวังไว้ได้ เช่นเดียวกับระบบที่ต้องการความมั่นคง หากความต้องการด้านความ

มั่นคงไม่ถูกกำหนดไว้อย่างเหมาะสมในช่วงแรกๆ ของการเริ่มโครงการ ความเสี่ยงและค่าใช้จ่ายก็จะเพิ่มสูงขึ้น และ เมื่อพัฒนาผลิตภัณฑ์ไปแล้วและปรากฏช่องโหว่ภายหลัง จะทำให้ยากต่อการแก้ไข

ความมั่นคงคือ ความสามารถในการป้องกันระบบสารสนเทศจากการขัดขวาง และการสูญเสียข้อมูล ซึ่งอาจเกิดจากการกระทำของกลุ่มผู้ประสงค์ร้าย หรือเหตุการณ์ที่เกิดขึ้นโดยบังเอิญ ความมั่นคงเป็นความรับผิดชอบของกลุ่มผู้พัฒนา ในการสร้างระบบนั้น ต้องมั่นใจได้ว่า ความต้องการด้านความมั่นคง (Security Requirements) ของระบบได้ถูกกำหนดขึ้นด้วยความระมัดระวัง อย่างสมเหตุสมผลเพื่อป้องกันปัญหาที่จะเกิดขึ้น การพัฒนาความต้องการด้านความมั่นคงโดยปกติจะเริ่มจากการประเมินมูลค่าของระบบและข้อมูล ซึ่งช่วยให้เห็นความสำคัญของระบบ ก่อให้เกิดการคำนึงถึงความเสี่ยงเสมอในระหว่างพัฒนาระบบ ความมั่นคงของระบบมักจะให้ความสำคัญกับการระบุว่าผู้ใดบ้างมีสิทธิ์เข้าถึงข้อมูล ระบุความจำเป็นในการเข้ารหัส การพิสูจน์ตัวจริง และการป้องกันไวรัสคอมพิวเตอร์ ซึ่งได้มีการนำเสนอวัตถุประสงค์สำหรับความต้องการด้านความมั่นคงไว้ดังนี้ [7]

1. เพื่อให้มั่นใจได้ว่าผู้ใช้ (User) และเครื่องรับบริการโปรแกรมประยุกต์ (Client Application) ได้มีการระบุตัวตน (Identify) และมีการทวนสอบ (Verify) อย่างถูกต้อง
2. เพื่อให้มั่นใจได้ว่าผู้ใช้และเครื่องรับบริการโปรแกรมประยุกต์สามารถเข้าถึงข้อมูลและบริการตามการอนุญาต (Authorize) การเข้าถึงได้อย่างถูกต้อง
3. เพื่อตรวจจับการพยายามบุกรุก (Intrusion) โดยบุคคลและเครื่องคอมพิวเตอร์สำหรับโปรแกรมประยุกต์ที่ไม่ได้รับอนุญาต (Unauthorized)
4. เพื่อให้มั่นใจได้ว่าโปรแกรมที่ประสงค์ร้าย (Malicious) ที่ไม่ได้รับอนุญาตในการเข้าถึง เช่น ไวรัสคอมพิวเตอร์ เป็นต้น ไม่มีการติด (Infect) ไปยังโปรแกรมประยุกต์หรือส่วนประกอบของโปรแกรมประยุกต์
5. เพื่อให้มั่นใจได้ว่าการสื่อสาร (Communication) และข้อมูลจะไม่เกิดความเสียหายโดยเจตนา
6. เพื่อให้มั่นใจได้ว่าบุคคลที่จะโต้ตอบ (Interaction) กับโปรแกรมหรือส่วนของโปรแกรมไม่สามารถปฏิเสธความรับผิดชอบการโต้ตอบนั้นได้ในภายหลัง
7. เพื่อให้มั่นใจได้ว่าการสื่อสารและข้อมูลที่เป็นความลับจะถูกรักษาไว้ซึ่งความเป็นส่วนตัว
8. เพื่อให้มั่นใจได้ว่าบุคลากรด้านความมั่นคงสามารถตรวจสอบ (Audit) สถานะและการใช้งานกลไกการรักษาความมั่นคง (Security Mechanism)
9. เพื่อให้มั่นใจได้ว่าโปรแกรมประยุกต์และศูนย์ข้อมูลรอดพ้นจากการโจมตี (Attack) หรือ การตกอยู่ในภาวะอ่อนลง (Degraded Mode)

Chulalongkorn University

10. เพื่อให้มั่นใจได้ว่าศูนย์ข้อมูล ส่วนประกอบ และบุคลากร ได้รับการป้องกันจากการทำลาย (Destruction) การทำให้เกิดความเสียหาย (Damage) การโจรกรรม (Theft) หรือการแฝงตัวซ่อนเร้น (Surreptitious Replacement) เช่น การทำลายทรัพย์สิน (Vandalism) การก่อวินาศกรรม (Sabotage) การก่อการร้าย (Terrorism)

11. เพื่อให้มั่นใจได้ว่าการบำรุงรักษาระบบไม่ได้ตั้งใจทำลายกลไกการรักษาความมั่นคงของโปรแกรมประยุกต์ส่วนประกอบ หรือศูนย์ข้อมูล

เพื่อให้บรรลุวัตถุประสงค์ ได้มีการนำเสนอความต้องการด้านความมั่นคงที่สอดคล้องกับวัตถุประสงค์ดังนี้

1. ความต้องการด้านการระบุตัวตน (Identification Requirements)
2. ความต้องการด้านการพิสูจน์ตัวจริง (Authentication Requirements)
3. ความต้องการด้านการอนุญาต (Authorization Requirements)
4. ความต้องการด้านภูมิคุ้มกัน (Immunity Requirements)
5. ความต้องการด้านบูรณภาพ (Integrity Requirements)
6. ความต้องการด้านการตรวจจับการบุกรุก (Intrusion Detection Requirements)
7. ความต้องการด้านการไม่ให้มีการปฏิเสธ (Nonrepudiation Requirements)
8. ความต้องการด้านความเป็นส่วนตัว (Privacy Requirements)
9. ความต้องการด้านการตรวจสอบความมั่นคง (Security Auditing Requirements)
10. ความต้องการด้านความอยู่รอด (Survivability Requirements)
11. ความต้องการด้านการป้องกันทางกายภาพ (Physical Protection Requirements)
12. ความต้องการด้านความมั่นคงสำหรับการบำรุงรักษาระบบ (System Maintenance Security Requirements)

2.1.2.1 ความต้องการด้านการระบุตัวตน

ความต้องการด้านการระบุตัวตนคือ ความต้องการด้านความมั่นคงใดๆ ซึ่งมีการระบุขอบเขตของธุรกิจ โปรแกรมประยุกต์ ส่วนประกอบ หรือศูนย์ข้อมูล จะต้องมีการระบุตัวตนจากภายนอกก่อนการโต้ตอบ เช่น

“The application shall identify all of its client applications before allowing them to use its capabilities.” เป็นต้น

2.1.2.2 ความต้องการด้านการพิสูจน์ตัวจริง

ความต้องการด้านการพิสูจน์ตัวจริงคือ ความต้องการด้านความมั่นคงใดๆ ซึ่งมีการระบุขอบเขตของธุรกิจ โปรแกรมประยุกต์ ส่วนประกอบ หรือศูนย์ข้อมูล จะต้องมีการระบุตัวตนจากภายนอกก่อนการโต้ตอบ ดังนั้นวัตถุประสงค์ทั่วไปของความต้องการด้านการพิสูจน์ตัวจริงคือเพื่อให้มั่นใจได้ว่าบุคคลหรือสิ่งที่ต้องการให้มีการเชื่อมต่อนั้นเป็นตัวจริง เพื่อหลีกเลี่ยงการสูญเสียความมั่นคงจากการปลอมแปลงเป็นบุคคลอื่น (Impostor) เช่น

“The application shall verify the identity of all of its users before allowing them to update their user information.” เป็นต้น

2.1.2.3 ความต้องการด้านการอนุญาต

ความต้องการด้านการอนุญาตคือ ความต้องการด้านความมั่นคงใดๆ ที่มีการระบุถึงการเข้าถึง (Access) และสิทธิการเข้าถึงการใช้งาน (Usage Privilege) สำหรับผู้ใช้ที่ได้รับอนุญาตและเครื่องรับบริการโปรแกรมประยุกต์ วัตถุประสงค์ทั่วไปของความต้องการด้านการอนุญาตมีดังนี้

1. เพื่อให้มั่นใจได้ว่าบุคคลหรือกลุ่มบุคคล (ที่ได้รับการแต่งตั้งอย่างถูกต้องในนามขององค์กรที่เป็นเจ้าของ และควบคุมโปรแกรมประยุกต์หรือส่วนประกอบ) สามารถอนุญาตให้ผู้ใช้หรือเครื่องรับบริการโปรแกรมประยุกต์ที่ได้รับการอนุญาตสามารถเข้าถึงโปรแกรมประยุกต์ ฟังก์ชันงานของส่วนประกอบ (Component Capability) หรือสารสนเทศ โดยเฉพาะเจาะจงได้
2. เพื่อให้มั่นใจได้ว่าบุคคลหรือกลุ่มบุคคลเฉพาะรายที่ได้รับการอนุญาตจากผู้ที่ได้รับการแต่งตั้งอย่างถูกต้อง (Specific Authenticated Externals) สามารถเข้าถึงโปรแกรมประยุกต์ ฟังก์ชันงานของส่วนประกอบ (Component Capability) หรือสารสนเทศได้
3. เพื่อป้องกันผู้ใช้ที่ไม่ได้รับอนุญาตจาก
   ก. การเข้าถึงข้อมูลที่ไม่เหมาะสมหรือเป็นความลับ
   ข. การร้องขอสมรรถนะ (Performance) ที่ไม่สอดคล้อง หรือบริการที่ถูกจำกัดการใช้งาน

เช่น

“The application shall not allow any customer to access any account information of any other customer”,

“The application shall not allow customer service agents to access either the original or new customer password when emailing the new customer password to the customer’s email address.” เป็นต้น

2.1.2.4 ความต้องการด้านภูมิคุ้มกัน

ความต้องการด้านภูมิคุ้มกันคือ ความต้องการด้านความมั่นคงใดๆ ซึ่งมีการระบุถึงขอบเขตของโปรแกรมประยุกต์หรือส่วนประกอบ จะได้รับการปกป้องจากการติดโปรแกรมที่ไม่พึงประสงค์ที่ไม่ได้รับอนุญาต เช่น ไวรัสคอมพิวเตอร์ หนอน ม้าโทรจัน (Trojan horses) หรือมัลแวร์ (Malware) วัตถุประสงค์ทั่วไปของความต้องการด้านภูมิคุ้มกันคือ การป้องกันโปรแกรมที่ไม่พึงประสงค์จากการทำลายหรือสร้างความเสียหายให้กับข้อมูลหรือโปรแกรมประยุกต์ เช่น

“The application shall disinfect any file found to contain a harmful program if disinfection is possible.” เป็นต้น

2.1.2.5 ความต้องการด้านบูรณภาพ

ความต้องการด้านบูรณภาพคือ ความต้องการด้านความมั่นคงใดๆ ซึ่งมีการระบุถึงขอบเขตของโปรแกรมประยุกต์หรือส่วนประกอบ จะต้องมั่นใจได้ว่าข้อมูลหรือการสื่อสารจะไม่ถูกกระทำให้เกิดการเสียหายโดยเจตนาด้วยวิธีการสร้าง แก้ไข หรือลบ โดยผู้ที่ไม่ได้รับอนุญาต เช่น

“The application shall prevent the unauthorized corruption of data collected from customers and other external users.” เป็นต้น

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

2.1.2.6 ความต้องการด้านการตรวจจับการบุกรุก

ความต้องการด้านการตรวจจับการบุกรุกคือ ความต้องการด้านความมั่นคงใดๆ ซึ่งมีการระบุถึงขอบเขตของโปรแกรมประยุกต์หรือส่วนประกอบ จะต้องตรวจจับ และบันทึกความพยายามในการเข้าสู่ระบบหรือความพยายามในการแก้ไขโดยผู้ที่ไม่ได้รับอนุญาต เช่น

“The application shall detect and record all attempted accesses that fail identification, authentication, or authorization requirements.” เป็นต้น

2.1.2.7 ความต้องการด้านการไม่ให้มีการปฏิเสธ

ความต้องการด้านการไม่ให้มีการปฏิเสธคือ ความต้องการด้านความมั่นคงใดๆ ซึ่งมีการระบุถึงขอบเขตของโปรแกรมประยุกต์หรือส่วนประกอบ จะต้องป้องกันการปฏิเสธความรับผิดชอบจากวิธีการสื่อสารระหว่างกัน โดยมีวัตถุประสงค์เพื่อ

1. มั่นใจได้ว่าการสื่อสารซึ่งผู้ส่งข้อมูลได้รับหลักฐานว่าได้มีการส่งข้อมูลแล้ว และผู้รับก็ได้รับการยืนยันว่าผู้ส่งเป็นใคร ดังนั้นทั้งผู้ส่งและผู้รับจะไม่สามารถปฏิเสธได้ว่าไม่มีความเกี่ยวข้องกับข้อมูลดังกล่าวในภายหลัง
2. ลดโอกาสที่จะเกิดปัญหาทางด้านกฎหมายในอนาคต กรณีการตอบโต้กันในประเด็นของการสื่อสารระหว่างผู้รับและผู้ส่ง

เช่น

“The application shall make and store tamper-proof records of the following information about each order received from a customer and each invoice sent to a customer:

- The contents of the order or invoice.
- The date and time that the order or invoice was sent.
- The date and time that the order or invoice was received.
- The identity of the customer.” เป็นต้น

2.1.2.8 ความต้องการด้านความเป็นส่วนตัว

ความต้องการด้านความเป็นส่วนตัวคือ ความต้องการด้านความมั่นคงใดๆ ซึ่งมีการระบุถึงขอบเขตของโปรแกรมประยุกต์หรือส่วนประกอบ ให้มีการรักษาข้อมูลที่มีความอ่อนไหวหรือการสื่อสารที่เป็นความลับจากบุคคลจากโปรแกรมประยุกต์หรือส่วนประกอบของโปรแกรมประยุกต์ที่ไม่ได้รับอนุญาตให้มีการเข้าถึง เช่น

“The application shall not allow unauthorized individuals or programs access to any stored data.” เป็นต้น

2.1.2.9 ความต้องการด้านการตรวจสอบความมั่นคง

ความต้องการด้านการตรวจตรวจสอบความมั่นคงคือ ความต้องการด้านความมั่นคงใดๆ ซึ่งมีการระบุถึงขอบเขตของโปรแกรมประยุกต์หรือส่วนประกอบของโปรแกรมประยุกต์ ให้

มีการบันทึกกิจกรรม เหตุการณ์ หรือสถานะของการใช้งานกลไกด้านความมั่นคงต่าง ๆ โดยมีวัตถุประสงค์หลักเพื่อให้มั่นใจได้ว่าโปรแกรมประยุกต์หรือส่วนประกอบของโปรแกรมประยุกต์ ได้มีการจัดเก็บข้อมูลที่เพียงพอต่อการวิเคราะห์ และรายงานสารสนเทศต่าง ๆ ได้ เช่น

“The application shall collect, organize, summarize, and regularly report the status of its security mechanisms including:

- Identification, Authentication, and Authorization.
- Immunity.
- Privacy.
- Intrusion Detection.” เป็นต้น

2.1.2.10 ความต้องการด้านความอยู่รอด

ความต้องการด้านความอยู่รอดคือ ความต้องการด้านความมั่นคงใด ๆ ซึ่งมีการระบุถึงขอบเขตของโปรแกรมประยุกต์หรือศูนย์ข้อมูล ที่จะส่งผลให้รอดพ้นจากการตั้งใจทำให้เกิดความสูญเสียหรือการทำลายส่วนประกอบของโปรแกรมประยุกต์ โดยมีวัตถุประสงค์หลักเพื่อให้มั่นใจได้ว่าโปรแกรมประยุกต์หรือศูนย์ข้อมูลยังคงสามารถทำงานได้แม้ว่าบางส่วนได้รับความเสียหายหรือถูกทำลายโดยเจตนา เช่น

“The application shall not have a single point of failure.”,

“The application shall continue to function (possibly in degraded mode) even if a data center is destroyed.” เป็นต้น

2.1.2.11 ความต้องการด้านการป้องกันทางกายภาพ

ความต้องการด้านการป้องกันทางกายภาพคือ ความต้องการด้านความมั่นคงใดๆ ซึ่งมีการระบุถึงขอบเขตของโปรแกรมประยุกต์หรือศูนย์ข้อมูล ที่จะส่งผลให้เกิดการป้องกันการโจมตีทางกายภาพ โดยมีวัตถุประสงค์หลักเพื่อให้มั่นใจได้ว่าโปรแกรมประยุกต์หรือศูนย์ข้อมูลได้รับการป้องกันจากความเสียหายทางกายภาพ การทำลาย การโจรกรรม หรือการเปลี่ยนส่วนประกอบทางฮาร์ดแวร์ (Hardware) การตั้งใจทำลายจากบุคคล การก่อวินาศกรรม หรือการก่อการร้าย ตัวอย่างเช่น

“The data center shall protect its hardware components from physical damage, destruction, theft, or surreptitious replacement.”,

“The data center shall protect its personnel from death, injury, and kidnapping.” เป็นต้น

2.1.2.12 ความต้องการด้านความมั่นคงสำหรับการบำรุงรักษาระบบ

ความต้องการด้านความมั่นคงสำหรับการบำรุงรักษาระบบคือ ความต้องการด้านความมั่นคงใด ๆ ซึ่งมีการระบุถึงขอบเขตของโปรแกรมประยุกต์ ส่วนประกอบของโปรแกรมประยุกต์ หรือศูนย์ข้อมูล ที่จะส่งผลต่อการบำรุงรักษาจากผู้มีอำนาจ เช่น การแก้ไขข้อบกพร่อง การปรับปรุงให้ดีขึ้น หรือการปรับปรุงให้ทันสมัย เป็นต้น จากการตั้งใจเอาชนะกลไกการรักษาความมั่นคง โดยมีวัตถุประสงค์เพื่อรักษาระดับความมั่นคงที่กำหนดไว้ในข้อกำหนดความต้องการด้านความมั่นคงในระหว่างขั้นตอนในการบำรุงรักษาระบบ ตัวอย่างเช่น

“The application shall not violate its security requirements as a result of the upgrading of a data, hardware, or software component.”,

“The application shall not violate its security requirements as a result of the replacement of a data, hardware, or software component.” เป็นต้น

2.1.3 มาตรฐานด้านความมั่นคงที่เกี่ยวข้องกับสถาบันการธนาคาร

แนวปฏิบัติที่ดีสำหรับการควบคุมความเสี่ยงของระบบงานเทคโนโลยีสารสนเทศที่สนับสนุนธุรกิจหลัก (IT Best Practices) [8, 9] สำหรับธนาคารพาณิชย์ในประเทศไทย มุ่งเน้นธุรกรรมที่มีผลกระทบต่อประชาชนในวงกว้าง เพื่อให้ธนาคารพาณิชย์สามารถนำไปใช้เป็นแนวทางในการควบคุมความเสี่ยงของตนเอง ซึ่งสอดคล้องตามกรอบแนวทางมาตรฐานสากล เช่น Cybersecurity Framework ที่จัดทำโดยสถาบัน NIST (National Institute of Standards and Technology) เป็นต้น

สาระสำคัญของแนวปฏิบัติที่ดีสำหรับการควบคุมความเสี่ยงของระบบงานเทคโนโลยีสารสนเทศที่สนับสนุนธุรกิจหลักแบ่งออกเป็น 2 ส่วน ดังนี้

2.1.3.1 แนวปฏิบัติที่ดีสำหรับการควบคุมความเสี่ยงของกระบวนการทำธุรกิจหลัก (ฝาก ถอน และโอนเงิน)

ครอบคลุมกระบวนการเปิด/ปิดสาขา การเปิดบัญชีเงินฝาก และการทำธุรกรรมฝาก ถอน และโอนเงิน ผ่านชองทางสาขา เอทีเอ็ม (ATM) และอินเทอร์เน็ตแบงค์กิ้ง (Internet Banking) โดยมีการควบคุมความเสี่ยงที่ดี เช่น การใช้เครื่องมือพิสูจน์ตัวจริงของลูกค้าจาก

บัตรประชาชนอิเล็กทรอนิกส์ การกำหนดสิทธิ์ให้แก่พนักงานเท่าที่จำเป็นตามบทบาทหน้าที่ การพิสูจน์ตัวจริงของผู้อนุมัติรายการด้วยวิธีการที่มั่นคง เป็นต้น ซึ่งอาจเป็นได้ทั้งการควบคุมด้วยระบบเทคโนโลยีสารสนเทศ (Application Controls) และ/หรือ การควบคุมด้วยระเบียบวิธีปฏิบัติงาน (Operation Controls)

2.1.3.2 แนวปฏิบัติที่ดีสำหรับการควบคุมระบบเทคโนโลยีสารสนเทศที่สนับสนุนธุรกิจหลัก

ครอบคลุมโครงสร้างระบบเทคโนโลยีสารสนเทศ ที่สำคัญซึ่งประกอบด้วย ศูนย์ข้อมูล (Data Center) ระบบเครือข่ายสื่อสาร (Network) ระบบหลักธนาคาร (Core Banking) และระบบช่องทางการให้บริการต่าง ๆ โดยการควบคุมระบบ ระบบเทคโนโลยีสารสนเทศที่ดีจะครอบคลุมเรื่องสำคัญ 3 เรื่อง ได้แก่

1. Access Control คือการควบคุมระบบเทคโนโลยีสารสนเทศเพื่อป้องกันการถูกบุกรุกและเข้าถึงโดยไม่ได้รับอนุญาต เช่น การพิสูจน์ตัวจริงของผู้เข้าใช้งานระบบเทคโนโลยีสารสนเทศ การให้สิทธิ์แก่ผู้ใช้งานตามความจำเป็น เป็นต้น
2. Security Management คือการบริหารจัดการระบบเทคโนโลยีสารสนเทศให้มีความมั่นคง เพื่อให้ ระบบและข้อมูลมีความถูกต้อง เช่น การตั้งค่าความมั่นคงระบบเทคโนโลยีสารสนเทศ การควบคุมการแก้ไขหรือเปลี่ยนแปลงระบบเทคโนโลยีสารสนเทศ เป็นต้น
3. Availability Management คือการบริหารจัดการระบบเทคโนโลยีสารสนเทศ ให้มีความพร้อมในการรองรับการทำธุรกรรมอย่างต่อเนื่อง เช่น การจัดเตรียมระบบเทคโนโลยีสารสนเทศ และข้อมูลชุดสำรอง เป็นต้น

ธนาคารแห่งประเทศไทยได้มีการจัดกลุ่มแนวปฏิบัติที่ดีสำหรับการควบคุมระบบเทคโนโลยีสารสนเทศที่สนับสนุนธุรกิจหลัก ดังนี้

1. ศูนย์ข้อมูล
2. ระบบเครือข่ายสื่อสาร
3. ระบบหลักการธนาคาร
4. ระบบงานการให้บริการแก่ลูกค้า
    ก. เครื่องคอมพิวเตอร์ส่วนบุคคลที่สาขา
    ข. ATM Application Control
    ค. ตู้ Automatic Teller Machine (ATM)
    ง. Internet Banking Application Control
    จ. Internet Banking Security

2.1.4 แบบรูปการโจมตีคาเปก

คาเปก (CAPEC: Common Attack Pattern Enumerate and Classification) [1] เป็นอนุกรมวิธานการโจมตี (Attack Taxonomy) ที่ถูกพัฒนาโดยไมเทอร์ (MITRE) ได้รับการสนับสนุนจากกระทรวงความมั่นคงแห่งมาตุภูมิของสหรัฐอเมริกา (The US Department of Homeland Security) มีเป้าหมายเพื่อสร้างรายการของแบบรูปการโจมตี (Attack Patterns) ที่ถูกใช้โดยผู้โจมตีเมื่อมีการครอบครองระบบ โดยใช้สกีมาที่ครอบคลุมและอนุกรมวิธานการจำแนก ซึ่งเป็นกลไกที่มีประสิทธิภาพในการสื่อสารตามมุมมองของผู้โจมตี และมีคำอธิบายวิธีการทั่วไปของซอฟต์แวร์ที่ใช้ประโยชน์ (Exploit) เพื่อการโจมตี ซึ่งรายการเหล่านี้ได้มาจากแนวคิดของแบบรูปการออกแบบ (Design Patterns) ที่ถูกนำไปใช้ในบริบทที่เป็นการทำลาย (Destructive) มากกว่าการสร้างสรรค์และถูกสร้างขึ้นมาจากการวิเคราะห์ในเชิงลึกของตัวอย่างการใช้ประโยชน์ที่มีอยู่ในโลกความเป็นจริง ดังตารางที่ 2.1 รายการเหล่านี้สามารถนำไปใช้เพื่อช่วยในการเพิ่มการรักษาความมั่นคงตลอดช่วงวงจรชีวิตการพัฒนาซอฟต์แวร์และรองรับความต้องการของนักพัฒนา นักทดสอบ และนักวิชาการ

ตารางที่ 2.1 ตัวอย่างแบบรูปการโจมตีจากคาเปก [1]

Name	SQL Injection
Typical Severity	High
Description	This attack exploits target software that constructs SQL statements based on user input .An attacker crafts input strings so that when the target software constructs SQL statements based on the input, the resulting SQL statement performs actions other than those the application intended. SQL Injection results from failure of the application to appropriately validate input . When specially crafted user-controlled input consisting of SQL syntax is used without proper validation as part of SQL queries, it is possible to glean information from the database in ways not envisaged during application design .Depending upon the database and the design of the application, it may also be possible to leverage injection to have the database execute system-related commands of the attackers' choice .SQL Injection enables an attacker to talk directly to the database, thus bypassing the application completely .Successful injection can cause information disclosure as well as ability to add or modify data in the database .In order to successfully inject SQL and retrieve information from a database, an attacker:
Attack Prerequisites	SQL queries used by the application to store, retrieve or modify data. User-controllable input that is not properly validated by the application as part of SQL queries.

ตารางที่ 2.1 ตัวอย่างแบบรูปการโจมตีจากคาเปก [1] (ต่อ)

Typical Likelihood of Exploit	Very High
Methods of Attack	Injection
Examples-Instances	With PHP-Nuke versions 7.9 and earlier, an attacker can successfully access and modify data, including sensitive contents such as usernames and password hashes, and compromise the application through SQL Injection. The protection mechanism against SQL Injection employs a blacklist approach to input validation. However, because of improper blacklisting, it is possible to inject content such as "foo'/**/UNION" or "foo UNION/**/" to bypass validation and glean sensitive information from the database.
Attacker Skill or Knowledge Required	Low • It is fairly simple for someone with basic SQL knowledge to perform SQL injection, in general. In certain instances, however, specific knowledge of the database employed may be required.
Resources Required	None
Probing Techniques	The attacker tries to inject characters that can cause a SQL error, such as single-quote (') or keywords such as "UNION" and "OR". If the injection of such characters into the input causes a SQL error and the resulting error is displayed unfiltered, the attacker can begin to determine the nature of input validation and structure of SQL queries. A typical error resulting from such injection would look like: (Result) "You have an error in your SQL Syntax. Check your manual for the right syntax to use near') FROM db_users.user_table" With available design documentation and code, the attacker can determine whether all user-controllable inputs are being validated or not, and also the structure of SQL queries that such inputs feed into.
Indicators-Warnings of Attack	Too many false or invalid queries to the database, especially those caused by malformed input.

ตารางที่ 2.1 ตัวอย่างแบบรูปการโจมตีจากคาเปก [1] (ต่อ)

Solutions and Mitigations	Strong input validation - All user-controllable input must be validated and filtered for illegal characters as well as SQL content. Keywords such as UNION, SELECT or INSERT must be filtered in addition to characters such as a single-quote(') or SQL-comments (--) based on the context in which they appear. Use of parameterized queries or stored procedures - Parameterization causes the input to be restricted to certain domains, such as strings or integers, and any input outside such domains is considered invalid and the query fails. Note that SQL Injection is possible even in the presence of stored procedures if the eventual query is constructed dynamically. Use of custom error pages - Attackers can glean information about the nature of queries from descriptive error messages. Input validation must be coupled with customized error pages that inform about an error without disclosing information about the database or application.
Attack Motivation Consequences	Modify application data Read application data Execute unauthorized code or commands Gain privileges / assume identity
Injection Vector	User-controllable input used as part of non-parameterized SQL queries: This may include input fields on web forms, data in user-accessible files or even command-line parameters.
Payload	SQL statements intended to reveal information or run malicious code
Activation Zone	Back-end database
Payload Activation Impact	When malicious SQL content is executed by the database, it can lead to arbitrary queries being executed, causing disclosure of information, unauthorized access, privilege escalation and possibly system compromise.
CIA Impact	**Confidentiality:** High | **Integrity:** High | **Availability:** High
Related Weaknesses	CWE89-Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') CWE74-Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection') CWE20-Improper Input Validation CWE390-Detection of Error Condition Without Action CWE697-Insufficient Comparison CWE713-OWASP Top Ten 2007 Category A2 - Injection Flaws CWE707-Improper Enforcement of Message or Data Structure

ตารางที่ 2.1 ตัวอย่างแบบรูปการโจมตีจากคาเปก [1] (ต่อ)

Relevant Security Requirements	Special characters in user-controllable input must be escaped before use by the application. Only use parameterized stored procedures to query the database. Input data must be revalidated in the parameterized stored procedures. Custom error pages must be used to handle exceptions such that they do not reveal any information about the architecture of the application or the database.
Related Security Principles	Reluctance to Trust Failing Securely Defense in Depth
Related Guidelines	Never Use Input as Part of a Directive to any Internal Component Handle All Errors Safely
References	[R.66.1] [REF-3] "Common Weakness Enumeration (CWE)". CWE-89 - SQL Injection. Draft. The MITRE Corporation. 2007. <http://cwe.mitre.org/data/definitions/89.html>. [R.66.2] [REF-3] "Common Weakness Enumeration (CWE)". CWE-20 - Input Validation. Draft. The MITRE Corporation. 2007. <http://cwe.mitre.org/data/definitions/20.html>. [R.66.3] [REF-3] "Common Weakness Enumeration (CWE)". CWE-390 - Improper Error Handling. Draft. The MITRE Corporation. 2007. <http://cwe.mitre.org/data/definitions/390.html>.

2.1.5 การค้นคืนสารสนเทศ

การค้นคืนสารสนเทศ (Information Retrieval) เป็นขั้นตอนในการค้นหาสารสนเทศให้มีความใกล้เคียงหรือเกี่ยวข้องกับความต้องการของผู้ทำการค้นคืนสารสนเทศมากที่สุดออกมา เริ่มจากการที่ผู้ค้นคืน ใส่ความต้องการหรือข้อคำถาม (Query) ผ่านส่วนต่อประสานผู้ใช้ จากนั้นจะทำการแปลงข้อคำถามเป็นเซตดัชนีของข้อคำถาม และถูกนำไปเปรียบเทียบความคล้ายกับเซตของดัชนีที่เป็นตัวแทนของเอกสาร วิธีการที่ใช้ในการเปรียบเทียบความคล้ายกันระหว่างความต้องการมีหลายวิธีการ โดยวิธีการที่ใช้ในงานวิจัยนี่คือวิธีการหาค่าความคล้ายกันโดยสัมประสิทธิ์โคซายน์ (Cosine Coefficient) [10] ซึ่งเป็นวิธีที่นิยมใช้ในการวัดความคล้ายคลึงของเอกสารโดยพิจารณาจากค่าความต่างของมุมของข้อมูล 2 ชุด ที่เกิดขึ้นบนพื้นที่เว็กเตอร์ (Vector Space) ซึ่งความคล้ายคลึงกันแบบโคซายน์นี้จะมีค่าอยู่ระหว่าง 0-1 เท่านั้น วิธีการนี้จะมีประสิทธิภาพในกรณีที่เอกสาร 2 ชุด มีความยาวไม่เท่ากัน หรือทำให้มีความยุติธรรมต่อเอกสารที่สั้นกว่านั้นเอง ซึ่งมีสมการการคำนวณเป็นดังสมการ (2.1) [11]

$$S(j_a, j_b) = \frac{\sum_{i=1}^{N}[p(a,j_a,i) * p(b,j_b,i)]}{\sqrt{\sum_{i=1}^{N}[p(a,j_a,i)^2]} * \sqrt{\sum_{i=1}^{N}[p(b,j_b,i)^2]}} \quad (2.1)$$

โดยที่ $S(j_a, j_b)$ คือ ความคล้ายระหว่างความต้องการที่ j_a กับความต้องการที่ j_b

$p(a, j_a, i)$ คือ ค่าน้ำหนักของคำ i ในความต้องการ j_a ในเอกสาร a

$p(b, j_b, i)$ คือ ค่าน้ำหนักของคำ i ในความต้องการ j_b ในเอกสาร b

N คือ จำนวนคำในความต้องการ j_a และ j_b

2.1.6 ดัชนีความเสี่ยง

ดัชนีความเสี่ยง (Composite Risk Index) เป็นการประมาณระดับความเสี่ยงเชิงคุณภาพ เป็นวิธีการที่นิยมใช้ในการพิจารณาเรื่องความมั่นคงเชิงระบบ โดยมักนิยมใช้สมการ (2.2) [12] เป็นพื้นฐานในการคำนวณระดับความเสี่ยงเชิงคุณภาพ

*Composite Risk Index = Impact of Risk Event * Probability of Occurrence* (2.2)

โดยที่ *Composite Risk Index* คือ ดัชนีความเสี่ยง

Impact of Risk Event คือ ระดับผลกระทบหากความเสี่ยงนั้นเกิดขึ้นจะรุนแรงมากน้อยเพียงใด

Probability of Occurrence คือ ระดับโอกาสที่ความเสี่ยงนั้นจะเกิดขึ้นมีมากน้อยเพียงใด

โดยทั่วไปขนาด (Scale) [13] ของระดับผลกระทบที่วิเคราะห์จะมีการกำหนดไว้ที่ 1 ถึง 5 ซึ่งหมายเลข 1 หมายถึงค่าต่ำสุดของความรุนแรงหากเหตุการณ์ของความเสี่ยงนั้นปรากฏขึ้น และหมายเลข 5 หมายถึงค่าสูงสุดของความรุนแรงหากเหตุการณ์ของความเสี่ยงนั้นปรากฏขึ้น สำหรับขนาดของระดับโอกาสที่วิเคราะห์ จะมีการกำหนดค่าเป็นไปในทิศทางเดียวกันกับระดับผลกระทบ คือ หมายเลข 1 หมายถึงค่าต่ำสุดของโอกาสที่เหตุการณ์ของความเสี่ยงนั้นจะเกิดขึ้น และหมายเลข 5 คือ ค่าสูงสุดของโอกาสที่เหตุการณ์ของความเสี่ยงนั้นจะเกิดขึ้น

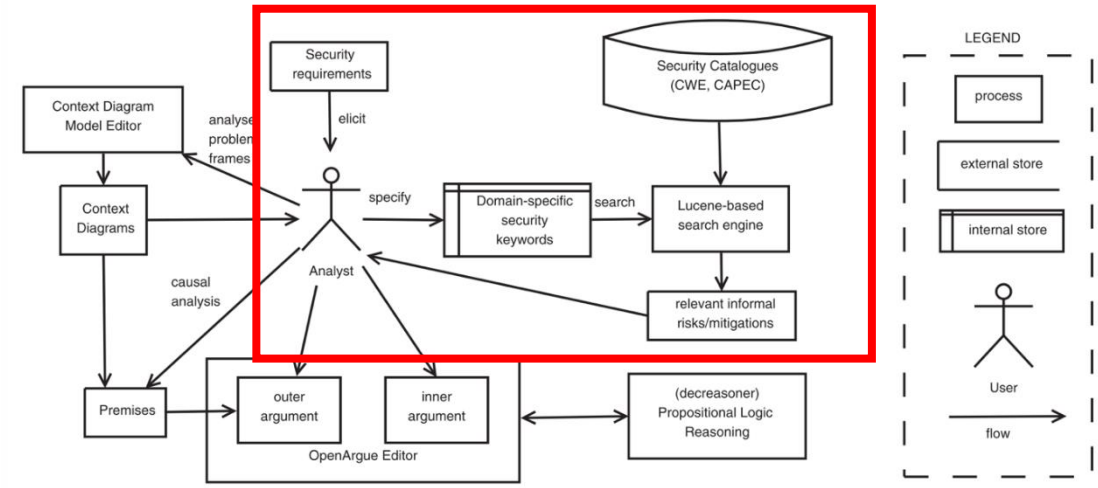
ดัชนีความเสี่ยงจะสามารถมีค่าได้ตั้งแต่ 1 ถึง 25 โดยจะมีการแบ่งเป็น 3 กลุ่ม คือ ความเสี่ยงระดับต่ำ (Low), ความเสี่ยงระดับกลาง (Medium) และ ความเสี่ยงระดับสูง (High)

2.2 เอกสารและงานวิจัยที่เกี่ยวข้อง

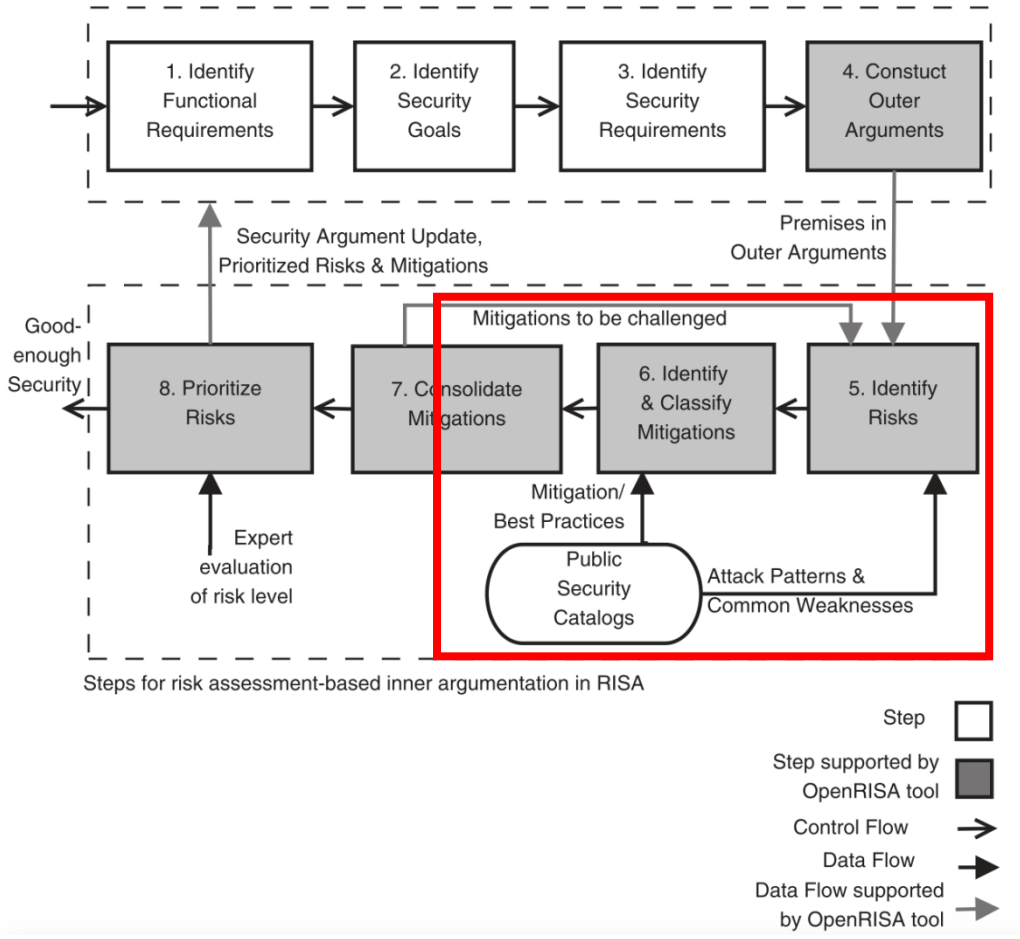
2.2.1 Automated analysis of security requirements through risk- based argumentation

งานวิจัยนี้ [14] นำเสนอแบบจำลองการประเมินความเสี่ยงโดยใช้วิธีการประเมินความเสี่ยงจากการให้เหตุผลทางด้านความมั่นคง (Risk assessment in Security Argumentation: RISA) โดยต้องอาศัยผู้เชี่ยวชาญในการสกัดความต้องการด้านความมั่นคงจากเอกสารความต้องการ แล้วจึงนำความต้องการที่ได้จากการสกัดมาค้นคืนโดยใช้เครื่องมือค้นคืนลูซีน (Lucene) เพื่อค้นคืนแบบรูปการโจมตีตามคาเปก ซึ่งจะได้ค่าข้อมูลต่าง ๆ ที่เกี่ยวข้องกับแบบรูปการโจมตีมาด้วย อาทิเช่น ค่าระดับความรุนแรง ค่าระดับโอกาสในการใช้ประโยชน์ เป็นต้น เพื่อนำมาใช้ในการคำนวณหาค่าดัชนีความเสี่ยง นอกจากนี้ยังได้มีการค้นคืนข้อมูลช่องโหว่ วิธีการบรรเทาการโจมตี และวิธีการแก้ไข (Solution) ในฐานข้อมูลกลางแบบรูปการโจมตี ดังภาพที่ 2.3 และ 2.4 จุดเด่นของงานวิจัยนี้คือการนำเสนอวิธีการประเมินความเสี่ยงโดยใช้แบบรูปการโจมตีจากคาเปก แต่วิธีการที่ใช้ยังคงต้องพึ่งความสามารถของผู้เชี่ยวชาญในการสกัดความต้องการด้านความมั่นคงจากเอกสารความต้องการ แล้วนำความต้องการด้านความมั่นคงที่สกัดได้ เข้าสู่แบบจำลองการประเมินความเสี่ยงทีละรายการความต้องการไป จึงยังคงต้องอาศัยทั้งความสามารถของผู้เชี่ยวชาญ และเวลาในการรวบรวมผลลัพธ์ในแต่ละรายการความต้องการ จากนั้นจึงนำมาประมวลผลและสรุปผลโดยผู้เชี่ยวชาญ

วิทยานิพนธ์นี้มีแนวคิดในการประเมินความเสี่ยงด้านความมั่นคงจากการวิเคราะห์ความต้องการด้านความมั่นคงโดยใช้เทคนิคการค้นคืนเอกสารและอิงตามคาเปกเช่นเดียวกัน แต่ใช้วิธีที่ต่างออกไป คือจะทำการประเมินจากความไม่สมบูรณ์ของความต้องการด้านความมั่นคง และมุ่งเน้นไปที่โดเมนของการธนาคารในประเทศไทย



ภาพที่ 2.3 ขั้นตอนการใช้เครื่องมืออาร์ไอเอสเอ [14]



ภาพที่ 2.4 แผนผังภาพรวมวิธีการประเมินความเสี่ยงจากการให้เหตุผลทางด้านความมั่นคง [14]

2.2.2 A Risk Assessment of Web Server :Impact Classification by Loss Type

งานวิจัยนี้ [15] นำเสนอวิธีการประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์โดยใช้ช่องโหว่ซีวีอี (CVE: Common Vulnerability and Exposure) ที่เกี่ยวข้องกับเว็บเซิร์ฟเวอร์เป็นพื้นฐานในการประเมิน และได้นำเสนอการกำหนดระดับผลกระทบให้แต่ละช่องโหว่ โดยจำแนกตามประเภทของผลกระทบคือ ผลกระทบต่อการรักษาความลับ (Confidentiality) ผลกระทบต่อบูรณภาพ (Integrity) และผลกระทบต่อสภาพพร้อมใช้งาน (Availability) งานวิจัยนี้ทำการพัฒนาเครื่องมือเพื่อร้องขอและรับผลการตอบสนองข้อมูลโดยใช้โปรโตคอลเอชทีทีพี (HTTP: Hypertext Transfer Protocol) ในการตรวจสอบช่องโหว่ของเว็บเซิร์ฟเวอร์ เพื่อนำผลที่ได้จากการตรวจสอบมาคำนวณค่าความเสี่ยงจากการทำงานผิดพลาดของเว็บเซิร์ฟเวอร์ โดยอาศัยค่าความน่าจะเป็นในการที่จะตรวจพบช่องโหว่ใด ๆ ในการประเมินความเสี่ยง โดยใช้สมการ (2.3)

$$\text{ความเสี่ยงของเว็บเซิร์ฟเวอร์} = \sum_{i=1}^{n} X_i W_i P_i \qquad (2.3)$$

โดยที่ X_i คือ การพบช่องโหว่ที่ i มีค่าเป็น 1 หรือ 0

W_i คือ ระดับผลกระทบของช่องโหว่ที่ i

P_i คือ ความน่าจะเป็นที่จะพบช่องโหว่ที่ i

n คือ จำนวนช่องโหว่ที่ทำการตรวจสอบ

งานวิจัยนี้เป็นอีกหนึ่งงานวิจัยที่นำเสนอการนำข้อมูลจากฐานข้อมูลสาธารณะด้านความมั่นคงมาใช้ในการประเมินความเสี่ยง โดยประยุกต์ใช้ดัชนีความเสี่ยงเช่นเดียวกัน แต่วิทยานิพนธ์นี้ใช้การประเมินความเสี่ยงจากความไม่สมบูรณ์ของความต้องการด้านความมั่นคง แทนการประเมินความเสี่ยงโดยตรงจากช่องโหว่ และประเมินในบริบทของทั้งระบบสารสนเทศและมุ่งเน้นไปที่โดเมนของการธนาคารในประเทศไทย

2.2.3 A Security Measurement Model for Web Services Based on Provision of Attack Countermeasures

งานวิจัยนี้ [16] นำเสนอแบบจำลองการวัดความมั่นคงสำหรับเว็บเซอร์วิซโดยอิงความสามารถในการจัดให้มีวิธีการรับมือการโจมตีความมั่นคง โดยการนำข้อมูลได้แก่ 1) ค่าระดับความรุนแรง 2) ค่าระดับโอกาสของการใช้ประโยชน์ 3) ค่าระดับผลกระทบด้านการรักษาความลับ 4) ค่าระดับผลกระทบด้านบูรณภาพ 5) ค่าระดับผลกระทบด้านสภาพพร้อมใช้งาน ซึ่งเป็นค่าคุณสมบัติ

การโจมตี ร่วมกับค่าความสำคัญสัมพัทธ์ของความสามารถในการจัดให้มีวิธีการรับมือต่อคุณสมบัติการโจมตี และค่าความสามารถในการจัดให้มีวิธีการรับมือ ผ่านการสร้างแบบจำลองดังสมการ (2.4)

$$S = R * (A * C) \quad (2.4)$$

โดยที่ S คือ ค่าความมั่นคงของเว็บเซอร์วิซ

R คือ ค่าความสำคัญสัมพัทธ์ของความสามารถในการจัดให้มีวิธีการรับมือต่อคุณสมบัติการโจมตี

A คือ ค่าคุณสมบัติการโจมตี

C คือ ค่าความสามารถในการจัดให้มีวิธีการรับมือ

งานวิจัยนี้เป็นอีกหนึ่งงานวิจัยที่นำเสนอการนำข้อมูลจากคาเปกมาใช้เพื่อการวัดความมั่นคง โดยในงานวิจัยได้สอบถามผู้ให้บริการเว็บเซอร์วิซถึงวิธีการรับมือการโจมตีซึ่งได้จัดหาหรือติดตั้งให้กับเว็บเซอร์วิซ โดยใช้แบบประเมินตนเอง เพื่อนำผลที่ได้มาคำนวณค่าความสามารถของผู้ให้บริการในการจัดให้มีวิธีการรับมือการโจมตี และค่าความมั่นคงของเว็บเซอร์วิซตามลำดับโดยใช้สมการ (2.4) ทั้งนี้มีแนวคิดว่า หากผู้ให้บริการสามารถจัดให้มีวิธีการรับมือการโจมตีประเภทที่ก่อให้เกิดผลกระทบมาก ย่อมแสดงว่าเว็บเซอร์วิซที่ให้บริการนั้นมีความมั่นคงมากกว่าเว็บเซอร์วิซของผู้ให้บริการที่มีวิธีการรับมือการโจมตีประเภทที่ก่อให้เกิดผลกระทบน้อยกว่า

วิทยานิพนธ์นี้มีแนวคิดในการประเมินด้านความมั่นคงโดยอิงตามคาเปกเช่นเดียวกัน แต่ใช้การประเมินความเสี่ยงจากความไม่สมบูรณ์ของความต้องการด้านความมั่นคง แทนการประเมินความมั่นคงโดยตรง และประเมินในบริบทของทั้งระบบสารสนเทศและมุ่งเน้นไปที่โดเมนของการธนาคารในประเทศไทย

2.2.4 Applying Information-Retrieval Methods to Software Reuse : A Case Study

งานวิจัยนี้ [11] นำเสนอวิธีการประยุกต์วิธีการค้นคืนข้อมูลมาใช้ในการนำซอฟต์แวร์กลับมาใช้ใหม่ (Reuse) ด้วยวิธีการหาค่าความคล้ายคลึงแบบโคไซน์ระหว่างรายการความต้องการใหม่กับรายการความต้องการเดิม ซึ่งจะช่วยให้สามารถนำรายการความต้องการเดิมกลับมาใช้ใหม่ได้ โดยงานวิจัยได้นำเสนอเป็นขั้นตอนแบบกึ่งอัตโนมัติ (Semi Automate) มีขั้นตอนดังภาพที่ 2.5 ซึ่งมีรายละเอียดดังนี้

1. ดำเนินการตัดข้อความที่ไม่ได้เป็นความต้องการออกทั้งหมด อาทิเช่น สารบัญ บทนำ อภิธานศัพท์ ภาคผนวก เป็นต้น

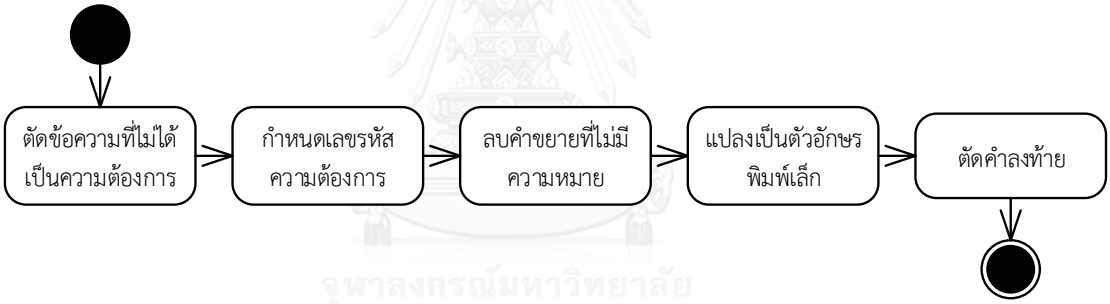
2. ดำเนินการให้เลขรายการความต้องการเป็นไปตามรูปแบบที่กำหนด เพื่อช่วยในการอ้างอิงความต้องการ

3. ดำเนินการตัดคำ (Word segmentation) และลบคำขยายที่ไม่มีความหมายในตัวเอง (Stop Word) และคำที่เกี่ยวข้องกับโดเมนนั้น โดยในงานวิจัยใช้แหล่งข้อมูลคำขยายจากเอ็มเออาร์ไออี 2 (MARIE-2)

4. แปลงตัวอักษรพิมพ์ใหญ่ให้เป็นพิมพ์เล็กทั้งหมด ยกเว้นข้อความที่เป็นตัวอักษรพิมพ์ใหญ่ทั้งหมด

5. ลบส่วนประกอบหลังคำหลัก (Suffix) อาทิเช่น –ster –eer –elle –ism เป็นต้น

จากนั้นทำการค้นคืนความต้องการ โดยใช้วิธีการหาความคล้ายคลึงแบบโคไซน์ (Cosine Similarity) ซึ่งเป็นวิธีการที่เหมาะสมทั้งในบริบทของความถูกต้องและสมรรถนะ



ภาพที่ 2.5 ขั้นตอนการเตรียมเอกสารก่อนเข้าสู่กระบวนการหาความคล้ายคลึง

งานวิจัยนี้มีความโดดเด่นในการนำเสนอวิธีการค้นคืนข้อมูลมาใช้ในการนำซอฟต์แวร์กลับมาใช้ใหม่ ซึ่งในทางกลับกัน วิธีการดังกล่าวสามารถนำมาประยุกต์ใช้ในวิทยานิพนธ์นี้ในการวิเคราะห์ความแตกต่างของรายการความต้องการได้เช่นเดียวกัน โดยประยุกต์ขั้นตอนการหาค่าความคล้ายคลึงระหว่างเอกสารความต้องการของธนาคารพาณิชย์กับเอกสารความต้องการด้านความมั่นคงที่พึงจะมีก่อน แล้วจึงนำมาหาค่าความแตกต่างของเอกสารความต้องการต่อไป ซึ่งสามารถนำไปเป็นข้อมูลส่วนหนึ่งของการประเมินความเสี่ยงได้ ดังจะกล่าวต่อไปในขั้นตอนที่ 3.6

2.2.5 A Similarity Measurement Framework for Requirements Engineering

งานวิจัยนี้ [17] นำเสนอกรอบการวัดความคล้ายคลึงกันระหว่างความต้องการที่มีอยู่เดิมกับความต้องการใหม่ เพื่อใช้ในการอ้างอิงเวลา ค่าใช้จ่าย และทรัพยากรต่าง ๆ ที่ต้องใช้ในโครงการสำหรับการพัฒนาระบบตามความต้องการใหม่ โดยงานวิจัยนำเสนอวิธีการในการวัดความคล้ายคลึงกันระหว่างความต้องการ 3 วิธีการ คือ Dice coefficient , Jaccard coefficient และ Cosine coefficient ซึ่งทั้ง 3 วิธีการให้ผลลัพธ์ที่ไม่แตกต่างกันมาก วิทยานิพนธ์นี้จึงเลือกใช้ Cosine coefficient เนื่องจากรายการความต้องการด้านความมั่นคงที่พึงจะมี และความต้องการด้านความมั่นคงของการธนาคาร มีโอกาสที่จะมีความยาวที่ไม่เท่ากัน และวิธีการดังกล่าวยังสอดคล้องกับงานวิจัย [11] ที่กล่าวมาแล้วข้างต้น

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

บทที่ 3
แนวคิดและวิธีดำเนินการวิจัย

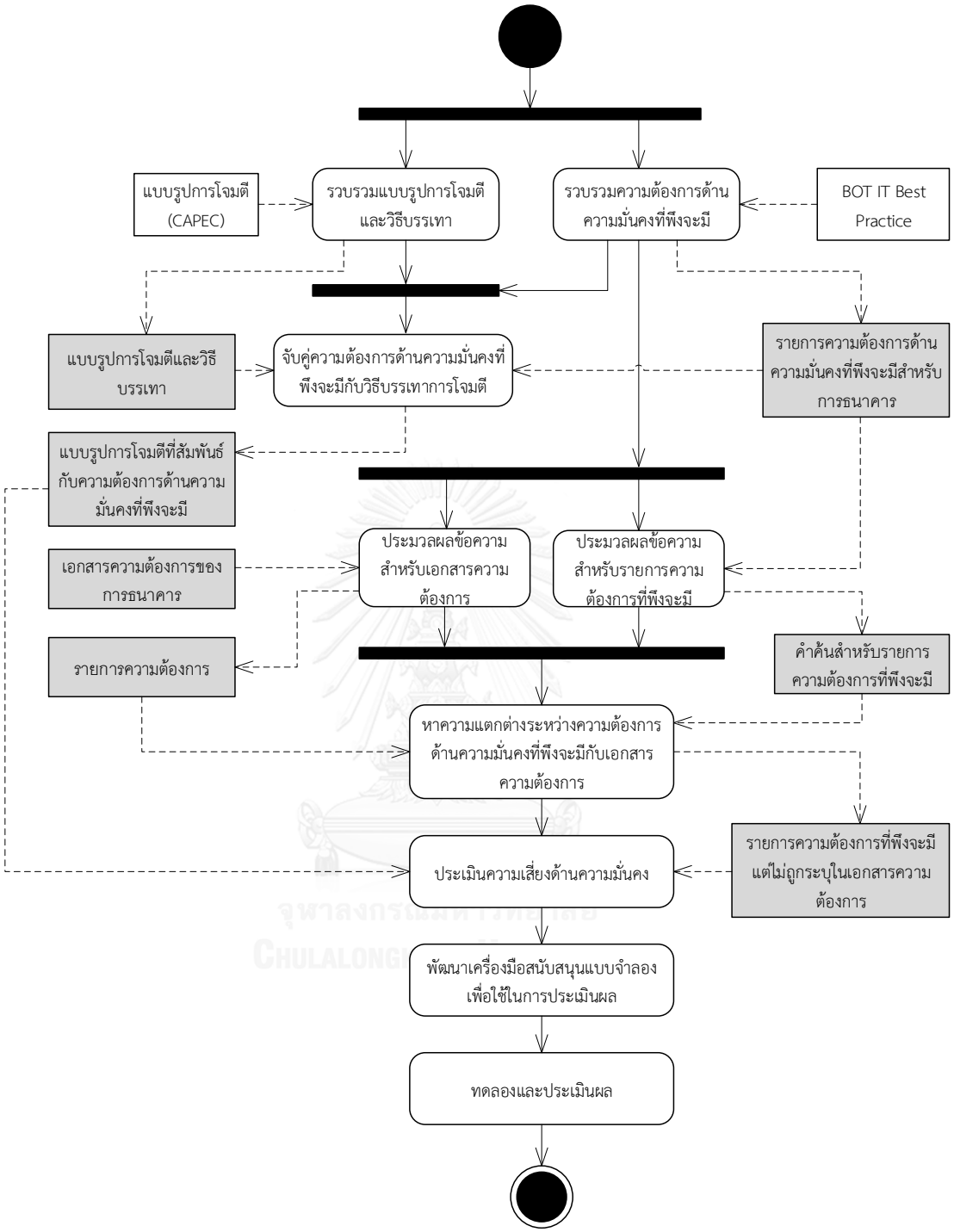
จากงานวิจัยที่เกี่ยวข้องเห็นได้ว่าได้มีการนำเสนอวิธีการประเมินความเสี่ยงด้านความมั่นคงจากแบบรูปการโจมตีของคาเปก ผู้วิจัยจึงได้แนวทางในการประยุกต์ใช้ข้อมูลแบบรูปการโจมตีและวิธีบรรเทาการโจมตีเพื่อเชื่อมโยงกับความต้องการด้านความมั่นคงสำหรับระบบสารสนเทศของการธนาคาร มาใช้ในการวิเคราะห์ความเสี่ยงที่อาจเกิดขึ้นจากการถูกโจมตี หากระบบสารสนเทศได้รับการพัฒนาตามข้อกำหนดความต้องการด้านความมั่นคงที่ไม่ครบถ้วนสมบูรณ์ ภาพรวมของการดำเนินงานวิจัย ดังภาพที่ 3.1 รายละเอียดแต่ละขั้นตอนดังนี้

3.1 รวบรวมแบบรูปการโจมตีและวิธีบรรเทา

การรวบรวมข้อมูลแบบรูปการโจมตี วิธีบรรเทา (Solutions and Mitigation) และความต้องการด้านความมั่นคงที่เกี่ยวข้อง (Relevant Security Requirements) ที่มีผลกระทบต่อระบบเทคโนโลยีสารสนเทศในการธนาคารได้รวบรวมข้อมูลจากคาเปก [1] โดยคัดเลือกเฉพาะการโจมตีที่สามารถนำมาปรับใช้ให้เข้ากับงานวิจัยได้ แต่ละการโจมตีจะมีคุณสมบัติ ได้แก่ ความรุนแรง (SEV: Typical Severity) และโอกาสการใช้ประโยชน์ (LOE: Typical Likelihood of Exploit) ซึ่งมีจำนวนทั้งสิ้น 38 แบบรูปการโจมตี ดังรายละเอียดในภาคผนวก ก

ความรุนแรง (SEV: Typical Severity) เป็นผลลัพธ์ของการโจมตีที่มีต่อระบบที่เป็นเป้าหมายว่าถ้าเกิดการโจมตีขึ้นจะมีความรุนแรงในระดับใด (ต่ำมาก ต่ำ ปานกลาง สูง สูงมาก) การกำหนดความรุนแรงนี้มีวัตถุประสงค์เพื่อการแสดงค่าเฉลี่ยโดยทั่วไปสำหรับการโจมตีแต่ละแบบเพื่อให้มีความเข้าใจและใส่ใจกับการโจมตีนั้นมากขึ้น ระดับความรุนแรงแสดงดังตารางที่ 3.1

โอกาสของการใช้ประโยชน์ (LOE: Typical Likelihood of Exploit) คือโอกาสจากการใช้ประโยชน์จากเครื่องมือ หรือโค้ดเพื่อการโจมตี โดยพิจารณาว่าโอกาสของการใช้ประโยชน์ดังกล่าวน่าจะมีค่าอยู่ในระดับใด (ต่ำมาก ต่ำ ปานกลาง สูง สูงมาก) โอกาสในการใช้ประโยชน์เพื่อการโจมตีนั้น ๆ จะพิจารณาจากความหลากหลายของบริบทและปัจจัยที่เกื้อหนุน การกำหนดโอกาสการใช้ประโยชน์นี้มีวัตถุประสงค์เพื่อแสดงค่าเฉลี่ยโดยทั่วไปสำหรับการโจมตีแต่ละแบบเพื่อให้มีความเข้าใจและใส่ใจกับการโจมตีนั้นมากขึ้น ระดับโอกาสของการใช้ประโยชน์ แสดงดังตารางที่ 3.2



ภาพที่ 3.1 แผนภาพวิธีการดำเนินการวิจัย

ตารางที่ 3.1 การกำหนดระดับความรุนแรงของการโจมตี

ความรุนแรง (Typical Severity)	
ระดับ (Levels)	**คำอธิบาย (Descriptions)**
สูงมาก (Very High)	ระดับความรุนแรงที่ได้ผ่านการพิจารณาจากคาเปก [1] แล้วว่าให้มีค่าความรุนแรงที่สูงมาก โดยในงานวิจัยนี้จะกำหนดค่าน้ำหนักเป็น 5
สูง (High)	ระดับความรุนแรงที่ได้ผ่านการพิจารณาจากคาเปก [1] แล้วว่าให้มีค่าความรุนแรงที่สูง โดยในงานวิจัยนี้จะกำหนดค่าน้ำหนักเป็น 4
ปานกลาง (Medium)	ระดับความรุนแรงที่ได้ผ่านการพิจารณาจากคาเปก [1] แล้วว่าให้มีค่าความรุนแรงที่ปานกลาง โดยในงานวิจัยนี้จะกำหนดค่าน้ำหนักเป็น 3
ต่ำ (Low)	ระดับความรุนแรงที่ได้ผ่านการพิจารณาจากคาเปก [1] แล้วว่าให้มีค่าความรุนแรงที่ต่ำ โดยในงานวิจัยนี้จะกำหนดค่าน้ำหนักเป็น 2
ต่ำมาก (Very Low)	ระดับความรุนแรงที่ได้ผ่านการพิจารณาจากคาเปก [1] แล้วว่าให้มีค่าความรุนแรงที่ต่ำมาก โดยในงานวิจัยนี้จะกำหนดค่าน้ำหนักเป็น 1
ไม่มีข้อมูล (Not Available)	คาเปก [1] ไม่ได้ระบุระดับความรุนแรงไว้ ในงานวิจัยนี้จะใช้ค่าน้ำหนักเป็นค่าปานกลางคือ 3 แทน [16]

ตารางที่ 3.2 การกำหนดระดับโอกาสของการใช้ประโยชน์จากเครื่องมือหรือโค้ดเพื่อการโจมตี

โอกาสของการใช้ประโยชน์จากเครื่องมือหรือโค้ดเพื่อการโจมตี (Typical Likelihood of Exploit)	
ระดับ (Levels)	**คำอธิบาย (Descriptions)**
สูงมาก (Very High)	ระดับโอกาสของการใช้ประโยชน์จากเครื่องมือหรือโค้ดเพื่อการโจมตีที่ได้ผ่านการพิจารณาจากคาเปก [1] แล้วว่าให้มีค่าโอกาสของการใช้ประโยชน์จากเครื่องมือหรือโค้ดเพื่อการโจมตีที่สูงมาก โดยในงานวิจัยนี้จะกำหนดค่าน้ำหนักเป็น 5
สูง (High)	ระดับโอกาสของการใช้ประโยชน์จากเครื่องมือหรือโค้ดเพื่อการโจมตีที่ได้ผ่านการพิจารณาจากคาเปก [1] แล้วว่าให้มีค่าโอกาสของการใช้ประโยชน์จากเครื่องมือหรือโค้ดเพื่อการโจมตีที่สูง โดยในงานวิจัยนี้จะกำหนดค่าน้ำหนักเป็น 4
ปานกลาง (Medium)	ระดับโอกาสของการใช้ประโยชน์จากเครื่องมือหรือโค้ดเพื่อการโจมตีที่ได้ผ่านการพิจารณาจากคาเปก [1] แล้วว่าให้มีค่าโอกาสของการใช้ประโยชน์จากเครื่องมือหรือโค้ดเพื่อการโจมตีที่ปานกลาง โดยในงานวิจัยนี้จะกำหนดค่าน้ำหนักเป็น 3
ต่ำ (Low)	ระดับโอกาสของการใช้ประโยชน์จากเครื่องมือหรือโค้ดเพื่อการโจมตีที่ได้ผ่านการพิจารณาจากคาเปก [1] แล้วว่าให้มีค่าโอกาสของการใช้ประโยชน์จากเครื่องมือหรือโค้ดเพื่อการโจมตีที่ต่ำ โดยในงานวิจัยนี้จะกำหนดค่าน้ำหนักเป็น 2
ต่ำมาก (Very Low)	ระดับโอกาสของการใช้ประโยชน์จากเครื่องมือหรือโค้ดเพื่อการโจมตีที่ได้ผ่านการพิจารณาจากคาเปก [1] แล้วว่าให้มีค่าโอกาสของการใช้ประโยชน์จากเครื่องมือหรือโค้ดเพื่อการโจมตีที่ต่ำมาก โดยในงานวิจัยนี้จะกำหนดค่าน้ำหนักเป็น 1

ตารางที่ 3.2 การกำหนดระดับโอกาสของการใช้ประโยชน์จากเครื่องมือหรือโค้ดเพื่อการโจมตี (ต่อ)

โอกาสของการใช้ประโยชน์จากเครื่องมือหรือโค้ดเพื่อการโจมตี (Typical Likelihood of Exploit)	
ระดับ (Levels)	**คำอธิบาย (Descriptions)**
ไม่มีข้อมูล (Not Available)	คาเปก [1] ไม่ได้ระบุระดับโอกาสของการใช้ประโยชน์จากเครื่องมือหรือโค้ดเพื่อการโจมตีไว้ ในงานวิจัยนี้จะใช้ค่าน้ำหนักเป็นค่าปานกลางคือ 3 แทน [16]

3.2 การรวบรวมความต้องการด้านความมั่นคงที่พึงจะมี

การรวบรวมความต้องการด้านความมั่นคงได้รวบรวมข้อมูลจากแนวปฏิบัติที่ดีฯ ซึ่งเป็นภาษาไทยและต้องมีการแปลเป็นภาษาอังกฤษ โดยคัดเลือกเฉพาะรายการความต้องการด้านความมั่นคงที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศในการธนาคาร และเป็นความต้องการที่เกี่ยวข้องกับซอฟต์แวร์เชิงระบบ ซึ่งสามารถแบ่งได้เป็น 4 ส่วน ได้แก่

3.2.1 ความต้องการด้านความมั่นคงสำหรับระบบหลักการธนาคาร

ความต้องการด้านความมั่นคงสำหรับระบบหลักการธนาคาร เป็นความต้องการด้านความมั่นคงที่เน้นไปยังระบบหลักของการธนาคารที่ควบคุมการทำรายการด้านการเงินที่แท้จริง ซึ่งส่วนใหญ่มักจะไม่ติดต่อกับลูกค้าโดยตรง หรือเป็นระบบธุรกรรมภายในที่ไม่ได้ติดต่อไปยังผู้ใช้ภายนอกธนาคาร เช่น ระบบหลักการทำธุรกรรม, ระบบเช็คเคลียริ่ง เป็นต้น ซึ่งได้มีการกำหนดความต้องการด้านความมั่นคงที่เกี่ยวข้องกับซอฟต์แวร์ไว้ ดังตารางที่ 3.3

ตารางที่ 3.3 ความต้องการด้านความมั่นคงสำหรับระบบหลักการธนาคาร

หมายเลขความต้องการ	**ความต้องการด้านความมั่นคง**
1	ในการเข้าใช้ระบบงานทุกครั้ง จะต้องมีการระบุตัวตนและพิสูจน์ตัวตนด้วยวิธีการที่เหมาะสม เช่น การใช้ User ID และ Password โดยจำกัดให้เฉพาะบุคคลที่ได้รับอนุญาตเท่านั้นที่สามารถเข้าถึงได้ในกรณีที่เป็นการเข้าใช้ ระบบงานด้วยบัญชีผู้ใช้ที่มีสิทธิ์เทียบเท่าสิทธิ์สูง ควรมีการพิสูจน์ตัวตนในลักษณะ Two-Factor Authentication
2	User ID ต้องสามารถระบุตัวตนของผู้ใช้งานได้อย่างถูกต้อง โดยต้องมีกระบวนการหรือระบบที่สามารถควบคุมไม่ให้มีการใช้ User ID ร่วมกัน
3	มีการระงับหรือยกเลิก Default Account ที่ไม่มีความจำเป็นในการใช้งานหรือไม่มีความจำเป็นต่อการทำงานของระบบ เช่น Guest Accounts เป็นต้น

ตารางที่ 3.3 ความต้องการด้านความมั่นคงสำหรับระบบหลักการธนาคาร (ต่อ)

หมายเลขความต้องการ	ความต้องการด้านความมั่นคง
4	มีการกำหนดค่ารหัสผ่านบนระบบให้เป็นไปตามมาตรฐานหรือนโยบายรหัสผ่าน โดยอย่างน้อยต้องครอบคลุม - รหัสผ่านควรบังคับเปลี่ยนสำหรับการเข้าใช้งานครั้งแรกและควรเปลี่ยนเป็นประจำดังนี้ ● รหัสผ่านสำหรับบัญชีผู้ใช้งาน (End User) และ บัญชีผู้ใช้ดูแลระบบ (IT User) ควรถูกเปลี่ยนทุก 60 วัน ● รหัสผ่านสำหรับบัญชีผู้ใช้ที่มีสิทธิ์เทียบเท่าสิทธิ์สูง (Equivalent Privilege User) ควรถูกเปลี่ยนทุก 30 วัน ● บัญชีผู้ใช้งานที่มีสิทธิ์ สูงสุด (Highest Privilege User) ควรถูกเปลี่ยนทุก 30 วัน และทุกครั้งหลังใช้งาน - รหัสผ่านควรมีความยาวไม่น้อยกว่า 8 ตัวอักษร - รหัสผ่านควรประกอบไปด้วยตัวเลข ตัวอักษร และตัวอักขระพิเศษ - รหัสผ่านถูกล็อกเมื่อมีการใส่ผิด 3 ครั้งติดกัน - รหัสผ่านไม่ควรซ้ำกับรหัสผ่านเดิมที่ใช้ 12 ครั้งที่ผ่านมา - มีการอำพรางรหัสผ่านด้วยการใช้สัญลักษณ์ เช่น สัญลักษณ์ดอกจัน เป็นต้น
5	จัดให้มีการจัดเก็บบันทึกเหตุการณ์ดังต่อไปนี้อย่างมั่นคงปลอดภัย - บันทึกร่องรอยกิจกรรมการทำธุรกรรม (Transaction Log) - บันทึกการเข้าถึงระบบงาน (Access Log) โดยบัญชีผู้ใช้ทุกประเภท - บันทึกการดำเนินงาน (Activity Log) ที่สำคัญ โดยอย่างน้อยต้องครอบคลุม ● การเปลี่ยนแปลงแก้ไขโครงสร้างฐานข้อมูล และการเปลี่ยนแปลงแก้ไขข้อมูล (Update/Insert/ Delete) ในตารางที่สำคัญ ● การเปลี่ยนแปลงการตั้งค่าความปลอดภัยของระบบ ● การเข้าถึง Object ที่สำคัญของระบบ ● การเปลี่ยนแปลงแก้ไขบัญชีและสิทธิ์ของผู้ใช้งาน
6	บันทึกดังกล่าวต้องถูกจัดเก็บเป็นระยะเวลาอย่างน้อย 90 วัน
7	มีการจัดเก็บรหัสผ่านของลูกค้าให้อยู่ในรูปแบบที่ไม่สามารถเรียกดูได้ในแบบที่ไม่มีการเข้ารหัสข้อมูลหรือสามารถถูกดักจับและอ่านข้อมูลนั้นได้ง่าย (Clear-Text)
8	มีการเข้ารหัสลับข้อมูลที่มีการจัดลำดับชั้นสูงสุดโดยเลือกใช้อัลกอริทึมในการเข้า รหัสลับที่มีความมั่นคงปลอดภัย
9	มีการควบคุมการเข้าถึง เรียกดู เปลี่ยนแปลงแก้ไข ลบข้อมูลในฐานข้อมูลลูกค้าให้ดำเนินการผ่านโปรแกรมระบบงานที่มีขั้นตอนการพิสูจน์ตัวตนของผู้ได้รับอนุญาตตามสิทธิ์ที่ได้รับมอบหมาย ก่อนเข้าถึงทุกครั้ง

3.2.2 ความต้องการด้านความมั่นคงสำหรับส่วนควบคุมกลางเอทีเอ็ม

ความต้องการด้านความมั่นคงสำหรับส่วนควบคุมเอทีเอ็ม เป็นความต้องการด้านความมั่นคงที่เน้นไปยังระบบควบคุมเอทีเอ็มในส่วนกลาง สำหรับการให้บริการตู้เอทีเอ็ม ซึ่งได้มีการกำหนดความต้องการด้านความมั่นคงที่เกี่ยวข้องกับซอฟต์แวร์ไว้ ดังตารางที่ 3.4

ตารางที่ 3.4 ความต้องการด้านความมั่นคงสำหรับควบคุมแอปพลิเคชันเอทีเอ็ม

หมายเลขความต้องการ	ความต้องการด้านความมั่นคง
1	อนุญาตเฉพาะข้อมูลที่อยู่ในรูปแบบที่กำหนดเท่านั้น เพื่อป้องกันข้อมูลที่ไม่ประสงค์ดี (เช่น ชุดคำสั่ง) ข้อมูลผิดลักษณะ/รูปแบบ ไม่สมเหตุผล หรือผิด Logic เข้าสู่ระบบ
2	มีการตรวจสอบความครบถ้วนของข้อมูล ก่อนที่จะทำการประมวลผลในขั้นตอนต่อไป เช่น จำนวนหลักของหมายเลขบัญชี ความครบถ้วนของ Mandatory Fields เป็นต้น
3	มีข้อความแจ้งเตือนผู้ใช้บริการ ในกรณีที่ผู้ใช้บริการกรอกข้อมูลไม่ถูกต้องครบถ้วน และไม่อนุญาตให้ผู้ใช้บริการข้ามขั้นตอนจนกว่าจะกรอกข้อมูลที่ถูกต้อง
4	มีการตรวจสอบเงื่อนไขการทำธุรกรรม เช่น ยอดคงเหลือ, Limit จำนวนเงินต่อครั้ง, Limit จำนวนเงินต่อวัน และค่าธรรมเนียม เป็นต้น ก่อนที่จะดำเนินรายการตามขั้นตอนที่กำหนดไว้
5	ระบบสามารถดึงข้อมูลบัญชีของลูกค้ามาจากระบบฐานข้อมูลได้อย่างถูกต้องและครบถ้วน โดยมีกระบวนการที่ทำให้มั่นใจว่าข้อมูลในฐานข้อมูลของระบบงานเป็นปัจจุบัน
6	ระบบมีการสรุปรายการเพื่อให้ลูกค้าทำการตรวจสอบความถูกต้องอีกครั้งก่อนยืนยันการทำรายการจริง
7	หากเกิดความผิดพลาดระหว่างที่ระบบประมวลผลข้อมูล ระบบจะต้องมีการแจ้งลูกค้าและต้องสามารถตรวจสอบความถูกต้องของข้อมูล (Data Integrity) เพื่อกลับไปสู่สถานะก่อนการทำรายการอย่างถูกต้อง
8	กรณีที่มีการแจ้งข้อมูลสำคัญของลูกค้า เช่น ชื่อบัญชี และหมายเลขบัญชี เป็นต้น ควรทำการปิดบังบางส่วนของข้อมูล
9	มีการควบคุมไม่ให้ข้อความแจ้งเตือน (Error Message) แสดงข้อมูลเกินความจำเป็น หรือแสดงข้อมูลที่เป็นการบ่งชี้อย่างเฉพาะเจาะจงว่าข้อมูลส่วนใดส่วนหนึ่งผิดพลาด เช่นการแจ้งเตือนว่ารหัสผ่านไม่ถูกต้อง เป็นต้น
10	มีการควบคุมให้ข้อความแจ้งเตือน (Error Message) เป็นหน้ากลางที่มีรูปแบบเดียวกันทั้งหมด โดยข้อความจะต้องสื่อสารให้ลูกค้าเกิดความเข้าใจที่ถูกต้อง และจะต้องไม่แสดงข้อมูลภายในของระบบ เช่น ยี่ห้อ และ Version ของ Web Application, Debug Message, Stack Trace, IP Address, Path เป็นต้น และควรแสดงรหัสที่บอกถึงสาเหตุของการทำงานที่ผิดพลาด ที่สามารถเข้าใจได้เฉพาะบุคลากรที่รับมอบอำนาจเท่านั้น
11	มีการควบคุมไม่ให้มีการจัดเก็บข้อมูล PIN ในบันทึกเหตุการณ์ (Log) ของระบบงานของตู้ ATM แม้ว่าจะอยู่ในรูปแบบที่เข้ารหัสแล้วก็ตาม

3.2.3 ความต้องการด้านความมั่นคงสำหรับส่วนควบคุมกลางของอินเทอร์เน็ตแบงค์กิ้ง

ความต้องการด้านความมั่นคงสำหรับส่วนควบคุมกลางอินเทอร์เน็ตแบงค์กิ้ง เป็นความต้องการด้านความมั่นคงที่เน้นไปยังระบบควบคุมระบบงานแอปพลิเคชันอินเทอร์เน็ตแบงค์กิ้งส่วนกลาง สำหรับการให้บริการอินเทอร์เน็ตแบงค์กิ้ง ซึ่งได้มีการกำหนดความต้องการด้านความมั่นคงที่เกี่ยวข้องกับซอฟต์แวร์ไว้ ดังตารางที่ 3.5

ตารางที่ 3.5 ความต้องการด้านความมั่นคงสำหรับควบคุมอินเทอร์เน็ตแบงค์กิ้ง

หมายเลขความต้องการ	ความต้องการด้านความมั่นคง
1	อนุญาตเฉพาะข้อมูลที่อยู่ในรูปแบบที่กำหนดเท่านั้น เพื่อป้องกันข้อมูลที่ไม่ประสงค์ดี (เช่น ชุดคำสั่ง) ข้อมูลผิดลักษณะ/รูปแบบ ไม่สมเหตุสมผล หรือผิด Logic เข้าสู่ระบบ
2	มีการตรวจสอบความครบถ้วนของข้อมูล ก่อนที่จะทำการประมวลผลในขั้นตอนต่อไป เช่น จำนวนหลักของหมายเลขบัญชี ความครบถ้วนของ Mandatory Fields เป็นต้น
3	มีข้อความแจ้งเตือนผู้ใช้บริการ ในกรณีที่ผู้ใช้บริการกรอกข้อมูลไม่ถูกต้องครบถ้วน และไม่อนุญาตให้ผู้ใช้บริการข้ามขั้นตอนจนกว่าจะกรอกข้อมูลที่ถูกต้อง
4	มีการตรวจสอบเงื่อนไขการทำธุรกรรม เช่น ยอดคงเหลือ, Limit จำนวนเงินต่อครั้ง, Limit จำนวนเงินต่อวัน และค่าธรรมเนียม เป็นต้น ก่อนที่จะดำเนินรายการตามขั้นตอนที่กำหนดไว้
5	ระบบสามารถดึงข้อมูลบัญชีของลูกค้ามาจากระบบฐานข้อมูลได้อย่างถูกต้องและครบถ้วน โดยมีกระบวนการที่ทำให้มั่นใจว่าข้อมูลในฐานข้อมูลของระบบงานเป็นปัจจุบัน
6	ระบบมีการสรุปรายการเพื่อให้ลูกค้าทำการตรวจสอบความถูกต้องอีกครั้งก่อนยืนยันการทำรายการจริง
7	หากเกิดความผิดพลาดระหว่างที่ระบบประมวลผลข้อมูล ระบบจะต้องมีการแจ้งลูกค้าและต้องสามารถตรวจสอบความถูกต้องของข้อมูล (Data Integrity) เพื่อกลับไปสู่สถานะก่อนการทำรายการอย่างถูกต้อง
8	กรณีที่มีการแจ้งข้อมูลสำคัญของลูกค้า เช่น ชื่อบัญชี และหมายเลขบัญชี เป็นต้น ควรทำการปิดบังบางส่วนของข้อมูล
9	มีการควบคุมไม่ให้ข้อความแจ้งเตือน (Error Message) แสดงข้อมูลเกินความจำเป็น หรือแสดงข้อมูลที่เป็นการบ่งชี้อย่างเฉพาะเจาะจงว่าข้อมูลส่วนใดส่วนหนึ่งผิดพลาด เช่นการแจ้งเตือนว่ารหัสผ่านไม่ถูกต้อง เป็นต้น

CHULALONGKORN UNIVERSITY

ตารางที่ 3.5 ความต้องการด้านความมั่นคงสำหรับควบคุมอินเทอร์เน็ตแบงค์กิ้ง (ต่อ)

หมายเลขความต้องการ	ความต้องการด้านความมั่นคง
10	มีการควบคุมให้ข้อความแจ้งเตือน (Error Message) เป็นหน้ากลางที่มีรูปแบบเดียวกันทั้งหมด โดยข้อความจะต้องสื่อสารให้ลูกค้าเกิดความเข้าใจที่ถูกต้อง และจะต้องไม่แสดงข้อมูลภายในของระบบ เช่น ยี่ห้อ และ Version ของ Web Application, Debug Message, Stack Trace, IP Address, Path เป็นต้น และควรแสดงรหัสที่บอกถึงสาเหตุของการทำงานที่ผิดพลาด ที่สามารถเข้าใจได้เฉพาะบุคลากรที่รับมอบอำนาจเท่านั้น

3.2.4 ความต้องการด้านความมั่นคงสำหรับอินเทอร์เน็ตแบงค์กิ้ง

ความต้องการด้านความมั่นคงสำหรับอินเทอร์เน็ตแบงค์กิ้ง เป็นความต้องการด้านความมั่นคงที่เน้นไปยังระบบควบคุมระบบงานอินเทอร์เน็ตแบงค์กิ้งที่ให้บริการแก่ลูกค้าของธนาคาร ซึ่งได้มีการกำหนดความต้องการด้านความมั่นคงที่เกี่ยวข้องกับซอฟต์แวร์ไว้ ดังตารางที่ 3.6

ตารางที่ 3.6 ความต้องการด้านความมั่นคงสำหรับอินเทอร์เน็ตแบงค์กิ้ง

หมายเลขความต้องการ	ความต้องการด้านความมั่นคง
1	มีการควบคุมให้ช่องทางในการทำธุรกรรมมีความปลอดภัยโดยการใช้ Protocol ที่เข้ารหัสลับในการรับส่งข้อมูลระหว่างผู้ใช้บริการ กับ Web Server เช่น HTTPs เป็นต้น โดยคำนึงถึงความปลอดภัยของช่องทางตั้งแต่จุดที่เริ่มป้อนข้อมูล ไปจนถึงเครื่องแม่ข่าย ในระบบเครือข่ายภายในที่ทำการประมวลผล (End-to-End Encryption)
2	มีการทำ End-to-End Encryption ที่ระดับ Application Layer เพื่อรักษาความลับและความปลอดภัยข้อมูลผู้ใช้บริการ เช่น รหัสผ่านของผู้ใช้บริการ,ข้อมูลบัญชีของผู้ใช้บริการ เป็นต้น
3	มีการเข้ารหัสข้อมูลรหัสผ่านของผู้ใช้บริการ ที่จัดเก็บในฐานข้อมูลที่ใช้ในการพิสูจน์ตัวตน (Authentication Database) ด้วยมาตรฐานการเข้ารหัสที่เป็นที่ยอมรับสากล โดยเลือกใช้อัลกอริทึมในการเข้ารหัสลับแบบย้อนกลับไม่ได้ (Irreversible Encryption หรือ Hashing) และมีความมั่นคงปลอดภัย ยกตัวอย่างเช่น SHA-256 แบบมี Salt เป็นอย่างน้อย
4	มีการระบุตัวตนและพิสูจน์ตัวตนของผู้ใช้บริการ โดยการใช้ Two-Factor Authentication ในขั้นตอนการเข้าใช้ระบบงานและควบคุมไม่ให้ User ID เดียวกันเข้าใช้งานระบบพร้อมกัน (Concurrent Session)
5	มีการควบคุมให้ระบบล็อกบัญชีผู้ใช้ของผู้ใช้บริการเมื่อมีการใส่ข้อมูลการพิสูจน์ตัวตน ผิดเกินจำนวน 3-5 ครั้ง โดยระบบต้องไม่เปิดเผยข้อความแจ้งเตือนที่เป็นการบ่งชี้ว่าข้อมูลพิสูจน์ตัวตนส่วนใดที่ไม่ถูกต้อง

ตารางที่ 3.6 ความต้องการด้านความมั่นคงสำหรับอินเทอร์เน็ตแบงค์กิ้ง (ต่อ)

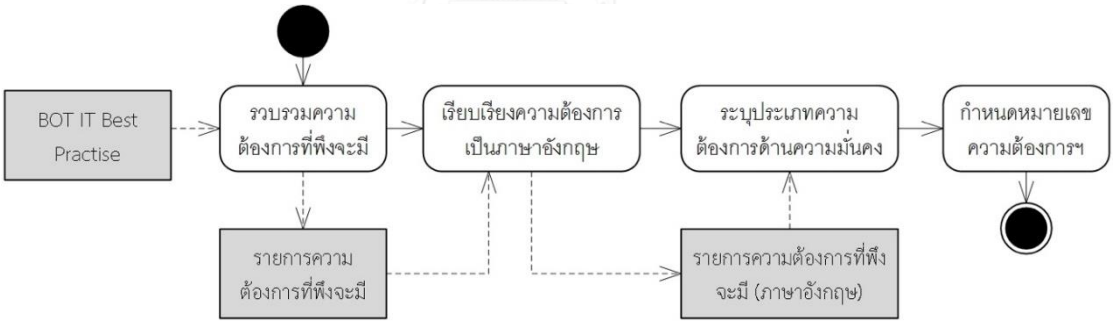
หมายเลขความต้องการ	ความต้องการด้านความมั่นคง
6	กำหนดให้ผู้ใช้บริการตั้งค่ารหัสผ่านให้มีความซับซ้อนและยากต่อการคาดเดา โดยรหัสผ่านต้องประกอบไปด้วยตัวอักษร ตัวอักขระพิเศษและตัวเลข
7	มีการบังคับให้ผู้ใช้บริการเปลี่ยนรหัสผ่านเมื่อเข้าใช้ระบบงานครั้งแรก หรือได้รับรหัสผ่านใหม่
8	หากลูกค้าลืมรหัสผู้ใช้งาน หรือรหัสผ่านต้องมีการพิสูจน์ตัวตนของลูกค้าโดยวิธี Two-Factor Authentication ก่อนให้ลูกค้าทำการ Reset รหัสผ่าน
9	มีการแสดงวันที่ และเวลาที่เข้าระบบครั้งล่าสุดเมื่อเข้าสู่ระบบ Internet Banking สำเร็จ เพื่อให้ลูกค้าได้ตรวจสอบความถูกต้องของเวลาที่มีกิจกรรมครั้งล่าสุด
10	มีการควบคุมไม่ให้มีการจัดเก็บข้อมูลที่ใช้ในการระบุตัวตนและพิสูจน์ตัวตนของผู้ใช้บริการ เช่น Session ID, User ID หรือ รหัสผ่าน ไว้ใน Cookie หรือ ใน Web Browser
11	มีการตรวจสอบสิทธิ์ของผู้ใช้บริการใหม่เมื่อมีการเข้าใช้งานฟังก์ชันที่สำคัญของระบบงาน เพื่อป้องกันการยกระดับสิทธิ์โดยไม่ได้รับอนุญาต
12	มีการบริหารจัดการ Session การใช้งานอย่างเหมาะสม โดยอย่างน้อยให้มีการควบคุมที่ลดความเสี่ยงจาก Man-in-the-Middle Attack และ Man-in-the-Browser Attack
13	มีการควบคุมไม่ให้มีการเก็บข้อมูลที่สำคัญของลูกค้าไว้ใน Session และมีการสร้าง Session Key ใหม่เมื่อมีการเปลี่ยนหน้า/ขั้นตอนการทำรายการ
14	มีการตรวจสอบลำดับของขั้นตอนการทำธุรกรรมอย่างเหมาะสม เพื่อป้องกันไม่ให้ผู้ไม่ประสงค์ดีสามารถข้ามขั้นตอนใดขั้นตอนหนึ่งได้ หากพบว่ามีการกระทำดังกล่าว จะต้องมีกระบวนการในการยับยั้งการทำธุรกรรมเช่น ทำให้ Session หมดอายุ หรือ Logout ผู้ใช้บริการออกจากระบบ
15	มีการกำหนด Time-Out ของ Session ให้ไม่เกิน 10 นาที
16	มีการพิสูจน์ตัวตนของผู้ใช้บริการอีกครั้งสำหรับการทำกิจกรรมและ/หรือการทำรายการธุรกรรมที่มีความเสี่ยงสูง โดยการใช้ Hardware Token ที่สามารถทำ Transaction Signing ได้ โดยอย่างน้อยต้องครอบคลุมกิจกรรมดังนี้ - การเปลี่ยน Profile เช่น เปลี่ยนที่อยู่ เบอร์โทร E-mail เป็นต้น - การผูกบัญชีบุคคลที่สามสำหรับทำธุรกรรมโอนเงิน การโอนเงินไปยังบุคคลที่สาม - การเปลี่ยนแปลงวงเงินการทำธุรกรรมโอนเงิน
17	ในกรณีที่มีการใช้ One-Time-Password (OTP) เพื่อยืนยันตัวตนผู้ใช้บริการ ควรกำหนดอายุการใช้งาน OTP ให้มีระยะเวลาไม่เกิน 5 นาที ซึ่ง OTP ที่ถูกสร้างขึ้นมาต้องใช้สำหรับการทำธุรกรรมรายการใดรายการหนึ่งเท่านั้น โดยไม่สามารถใช้กับรายการธุรกรรมอื่น ๆ ได้ โดยในการสร้าง OTP ควรมีการใช้ข้อมูลเกี่ยวกับธุรกรรม เช่น หมายเลขบัญชี จำนวนเงินที่ทำธุรกรรม เป็นต้น มาเป็นส่วนประกอบหนึ่งของการสร้าง OTP ด้วย

ตารางที่ 3.6 ความต้องการด้านความมั่นคงสำหรับอินเทอร์เน็ตแบงค์กิ้ง (ต่อ)

หมายเลขความต้องการ	ความต้องการด้านความมั่นคง
18	มีการแจ้งเตือนไปยังผู้ใช้งานผ่านอุปกรณ์หรือช่องทางอื่นที่ไม่ได้ใช้ทำรายการ เช่น E-mail และ SMS เป็นต้น เมื่อผู้ใช้บริการดำเนินกิจกรรมและ/หรือธุรกรรมที่มีความเสี่ยงสูงแล้วเสร็จ เช่น การ Login เข้าสู่ระบบ การเปลี่ยนแปลง Profile การเปลี่ยน Password การผูกบัญชี การโอนเงินไปยังบุคคลที่สาม เป็นต้น

ในขั้นตอนการวิจัยนี้ จะมีขั้นตอนย่อยที่จะต้องดำเนินการเพิ่มเติม ดังภาพที่ 3.2 ได้แก่

1. รวบรวมรายการความต้องการด้านความมั่นคงที่พึงจะมีจากเอกสารแนวปฏิบัติที่ดีฯ [8, 9] โดยข้อมูลที่ได้จะยังคงอยู่ในรูปแบบภาษาไทย
2. เปลี่ยนข้อความความต้องการด้านความมั่นคงที่รวบรวมได้จากภาษาไทยเป็นภาษาอังกฤษ
3. กำหนดประเภทให้กับแต่ละความต้องการด้านความมั่นคงตาม [7] ดังหัวข้อที่ 2.1.2 ซึ่งแบ่งเป็น 12 ประเภท
4. กำหนดหมายเลขรายการความต้องการ เพื่อให้ง่ายต่อการอ้างอิง



ภาพที่ 3.2 แผนผังขั้นตอนการรวบรวมความต้องการด้านความมั่นคง

จากทั้ง 4 ขั้นตอน ส่งผลให้ได้ความต้องการด้านความมั่นคงในแต่ละส่วน ซึ่งได้ผลลัพธ์ดังแสดงในตารางที่ 3.7

ตารางที่ 3.7 ความต้องการด้านความมั่นคงที่พึงจะมี ที่ผ่านการรวบรวม กำหนดประเภทความต้องการ และหมายเลขความต้องการ

หมายเลขความต้องการ	หมายเลขความต้องการด้านความมั่นคงที่พึงจะมี (SSRB_ID)	ความต้องการ	ประเภทความต้องการด้านความความมั่นคง
ความต้องการด้านความมั่นคงสำหรับระบบหลักการธนาคาร			
1	CBS_001	The system shall be used two-factor authentication for access to the system.	Authentication
2	CBS_002	The system shall be restricted shared account and test account access to the system.	Authentication
3	CBS_003	The system shall be prohibited default account (e.g. sa, guest account) access to the system.	Authentication
4	CBS_004	Password policy for login accounts: - Password age is 90 days for end user and IT user. - Password age is 30 days for equivalent privilege user. - Password age is 30 days for highest privilege user. - Highest privilege user password shall be forced change after logon. - Minimum Password Length is 8 characters. - Password must contain a mix of alphabetic and non-alphabetic characters - Account shall be locked after 3-5 failure login attempts - Password shall not be reused from last 12 password histories - Password shall be marked by symbol when displaying on screen (e.g. *, • etc.)	Authentication

ตารางที่ 3.7 ความต้องการด้านความมั่นคงที่พึงจะมี ที่ผ่านการรวบรวม กำหนดประเภทความต้องการ และหมายเลขความต้องการ (ต่อ)

หมายเลขความต้องการ	หมายเลขความต้องการด้านความมั่นคงที่พึงจะมี (SSRB_ID)	ความต้องการ	ประเภทความต้องการด้านความความมั่นคง
5	CBS_005	The system shall be recorded event as following: - Financial transaction log - User access log - User activity log	Security Auditing
5	CBS_006	The audit log shall be stored at least 90 days.	Security Auditing
6	CBS_007	The system shall encrypt or hashing password before store in configuration file or database.	Integrity
7	CBS_008	The system shall encrypt confidential information by strong encryption (e.g. AES 128 bits, AES 256 bits, RSA 2048).	Integrity
8	CBS_009	The system shall be recorded access audit log for confidential information and it has been complied with computer crime act B.E. 2550.	Security Auditing
9	CBS_010	The system restricts user access to database directly.	Authorization
9	CBS_011	The system shall restrict user access for authorized person based on role/function.	Authorization
ความต้องการด้านความมั่นคงสำหรับส่วนควบคุมกลางเอทีเอ็ม			
1, 2	ATMC_001	The system shall validate all input data to application using white list for data type, format, length, range and business rules (mandatory field) before accepting the data to be displayed or stored.	Intrusion Detection

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

ตารางที่ 3.7 ความต้องการด้านความมั่นคงที่พึงจะมี ที่ผ่านการรวบรวม กำหนดประเภทความต้องการ และหมายเลขความต้องการ (ต่อ)

หมายเลขความต้องการ	หมายเลขความต้องการด้านความมั่นคงที่พึงจะมี (SSRB_ID)	ความต้องการ	ประเภทความต้องการด้านความความมั่นคง
3	ATMC_002	If input validation is rejected. The system shall display incorrect information was customer input to the system and not allow to perform next operation.	Intrusion Detection
4	ATMC_003	The system shall validate account balance, transaction limit, amount limit or fee before perform transaction.	Authorization
5	ATMC_004	The system must ensure account information was retrieved from database are correct.	Integrity
6	ATMC_005	The system shall display confirmation information before perform transaction was customer request.	Nonrepudiation
7	ATMC_006	The system shall support rollback transaction when some task or step is unsuccessful.	Integrity
8	ATMC_007	The system shall use masking techniques while displaying sensitive personal information (e.g. account name, account number, mobile number, e-mail etc.) to users.	Privacy
9	ATMC_008	The system shall hide technical error message or input validation was invalid (e.g. password is invalid etc.)	Immunity
10	ATMC_009	The system shall hide version of Web Application, Debug Message, Stack Trace, IP Address, Path.	Immunity
11	ATMC_010	The PIN shall be escaped before write or store in ATM log file.	Privacy

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

ตารางที่ 3.7 ความต้องการด้านความมั่นคงที่พึงจะมี ที่ผ่านการรวบรวม กำหนดประเภทความต้องการ และหมายเลขความต้องการ (ต่อ)

หมายเลขความต้องการ	หมายเลขความต้องการด้านความมั่นคงที่พึงจะมี (SSRB_ID)	ความต้องการ	ประเภทความต้องการด้านความความมั่นคง
ความต้องการด้านความมั่นคงสำหรับส่วนควบคุมกลางของอินเทอร์เน็ตแบงค์กิ้ง			
1, 2	IBC_001	The system shall validate all input data to application using white list for data type, format, length, range and business rules (mandatory field) before accepting the data to be displayed or stored.	Intrusion Detection
3	IBC_002	If input validation is rejected. The system shall display incorrect information was customer input to the system and not allow to perform next operation.	Intrusion Detection
4	IBC_003	The system shall validate account balance, transaction limit, amount limit or fee before perform transaction.	Authorization
5	IBC_004	The system must ensure account information was retrieved from database are correct.	Integrity
6	IBC_005	The system shall display confirmation information before perform transaction was customer request.	Nonrepudiation
7	IBC_006	The system shall support rollback transaction when some task or step is unsuccessful.	Integrity
8	IBC_007	The system shall use masking techniques while displaying sensitive personal information (e.g. account name, account number, mobile number, e-mail etc.) to users.	Privacy

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

ตารางที่ 3.7 ความต้องการด้านความมั่นคงที่พึงจะมี ที่ผ่านการรวบรวม กำหนดประเภทความต้องการ และหมายเลขความต้องการ (ต่อ)

หมายเลขความต้องการ	หมายเลขความต้องการด้านความมั่นคงที่พึงจะมี (SSRB_ID)	ความต้องการ	ประเภทความต้องการด้านความความมั่นคง
9	IBC_008	The system shall hide technical error message or input validation was invalid (e.g. password is invalid etc.)	Immunity
10	IBC_009	The system shall hide version of Web Application, Debug Message, Stack Trace, IP Address, Path.	Immunity
ความต้องการด้านความมั่นคงสำหรับอินเทอร์เน็ตแบงค์กิ้ง			
1	IBS_001	The system shall use strong encryption and security protocols to safeguard sensitive data during transmission over open, public networks.	Privacy
2	IBS_002	The system shall encrypt confidential information (e.g. password, customer account information) by strong encryption (e.g. AES 128 bits, AES 256 bits, RSA 2048).	Privacy
3	IBS_003	The system shall apply strong one-way hashes (e.g. SHA 256 bits with salt) to customer password and store those hashes in database or a configuration file with appropriate access control.	Integrity
4	IBS_004	The system shall generate new session randomly after successful authentication by two-factor authentication methodology.	Authentication
4	IBS_005	The system shall restrict to use share user at the same time.	Identification
5	IBS_006	The system shall lock the account after 3-5 failure login attempts and do not display specific information is failure.	Authentication

ตารางที่ 3.7 ความต้องการด้านความมั่นคงที่พึงจะมี ที่ผ่านการรวบรวม กำหนดประเภทความต้องการ และหมายเลขความต้องการ (ต่อ)

หมายเลขความต้องการ	หมายเลขความต้องการด้านความมั่นคงที่พึงจะมี (SSRB_ID)	ความต้องการ	ประเภทความต้องการด้านความความมั่นคง
6	IBS_007	The system shall enforce strong password (contain a mix of alphabetic and non-alphabetic characters).	Authentication
7	IBS_008	The system shall be forced change password after first logon or after password is reset.	Authentication
8	IBS_009	The system shall be used two-factor authentication before reset password.	Authentication
9	IBS_010	The system shall display the last successful login.	Identification
10	IBS_011	No sensitive or confidential information (e.g. session ID, user ID or password) must be stored in cookies, source code, session or configuration file.	Privacy
11	IBS_012	The system shall validate authorized when customer perform access to important function.	Authorization
12, 13	IBS_013	The system shall be regenerated session upon change page or new transaction.	Authentication
14	IBS_014	The system shall lockout and inactive session automatically when transaction step is incorrect.	Intrusion Detection
15	IBS_015	The idle timeout of session less than 10 minutes.	Immunity
16	IBS_016	The system shall re-authenticate when customer perform change customer profile (e.g. address, telephone number, email) by hardware token.	Authentication
17	IBS_017	The system shall generate OTP password authentication for only one purpose.	Authentication

ตารางที่ 3.7 ความต้องการด้านความมั่นคงที่พึงจะมี ที่ผ่านการรวบรวม กำหนดประเภทความต้องการ และหมายเลขความต้องการ (ต่อ)

หมายเลขความต้องการ	หมายเลขความต้องการด้านความมั่นคงที่พึงจะมี (SSRB_ID)	ความต้องการ	ประเภทความต้องการด้านความความมั่นคง
17	IBS_018	The OTP timeout less than 5 minutes.	Authentication
18	IBS_019	The system shall push notification of important transaction to customer by other channel (e.g. E-mail, SMS).	Identification

3.3 จับคู่ความต้องการด้านความมั่นคงที่พึงจะมีกับวิธีการบรรเทาการโจมตี

จากหัวข้อที่ 3.1 สามารถนำข้อมูลการบรรเทาการโจมตี และความต้องการด้านความมั่นคงที่เกี่ยวข้อง ของแบบรูปการโจมตีตามคาเปกมาจับคู่หาความสัมพันธ์กับความต้องการด้านความมั่นคงที่พึงจะมี (หัวข้อที่ 3.2) ด้วยวิธีการทำด้วยมือ (Manual) และตรวจทานโดยผู้เชี่ยวชาญด้านความมั่นคง ดังรายละเอียดในภาคผนวก ข เพื่อแสดงให้เห็นว่าความต้องการด้านความมั่นคงที่พึงจะมีในแต่ละรายการนั้นสามารถป้องกันและ/หรือบรรเทาการโจมตีใดได้ โดยที่การโจมตีนั้นมีค่าระดับความรุนแรงและค่าระดับโอกาสในการใช้ประโยชน์ซึ่งกำหนดอยู่ในแบบรูปการโจมตีคาเปก เป็นเท่าไร ดังตารางที่ 3.8

ตารางที่ 3.8 การจับคู่ความต้องการด้านความมั่นคงที่พึงจะมีกับแบบรูปการโจมตี

หมายเลขความต้องการ (SSRB_ID)	หมายเลขแบบรูปการโจมตีตามคาเปกที่เกี่ยวข้อง (CAPEC_ID) [1]	ระดับความรุนแรงของแบบรูปการโจมตี (SEV) [1]	ระดับโอกาสของการใช้ประโยชน์ของแบบรูปการโจมตี (LOE) [1]
ความต้องการด้านความมั่นคงสำหรับระบบหลักการธนาคาร			
CBS_001	36 40	4 4	3 4
CBS_002	60	4	4
CBS_003	70 169	4 1	3 4
CBS_004	16 49 70	4 4 4	3 3 3

ตารางที่ 3.8 การจับคู่ความต้องการด้านความมั่นคงที่พึงจะมีกับแบบรูปการโจมตี (ต่อ)

หมายเลขความต้องการ (SSRB_ID)	หมายเลขแบบรูปการโจมตีตามคาเปกที่เกี่ยวข้อง (CAPEC_ID) [1]	ระดับความรุนแรงของแบบรูปการโจมตี (SEV) [1]	ระดับโอกาสของการใช้ประโยชน์ของแบบรูปการโจมตี (LOE) [1]
CBS_005	N/A	N/A	N/A
CBS_006	N/A	N/A	N/A
CBS_007	55	3	3
CBS_008	169	1	4
CBS_009	N/A	N/A	N/A
CBS_010	1	4	5
CBS_011	1	4	5
ความต้องการด้านความมั่นคงสำหรับส่วนควบคุมกลางเอทีเอ็ม			
ATMC_001	7	4	4
	37	5	5
	39	3	5
	66	4	5
	83	4	4
	88	4	4
	100	5	4
	108	5	2
	110	5	4
	135	4	4
	136	4	4
	139	4	4
	182	3	4
	250	3 (N/A)	4

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

ตารางที่ 3.8 การจับคู่ความต้องการด้านความมั่นคงที่พึงจะมีกับแบบรูปการโจมตี (ต่อ)

หมายเลขความต้องการ (SSRB_ID)	หมายเลขแบบรูปการโจมตีตามคาเปกที่เกี่ยวข้อง (CAPEC_ID) [1]	ระดับความรุนแรงของแบบรูปการโจมตี (SEV) [1]	ระดับโอกาสของการใช้ประโยชน์ของแบบรูปการโจมตี (LOE) [1]
ATMC_002	7	4	4
	37	5	5
	39	3	5
	66	4	5
	83	4	4
	88	4	4
	100	5	4
	108	5	2
	110	5	4
	135	4	4
	136	4	4
	139	4	4
	182	3	4
	250	3 (N/A)	4
ATMC_003	N/A	N/A	N/A
ATMC_004	N/A	N/A	N/A
ATMC_005	N/A	N/A	N/A
ATMC_006	N/A	N/A	N/A
ATMC_007	476	4	2
ATMC_008	7	4	4
	54	2	4
	127	3	4
	136	4	4
	139	4	4
	170	2	4
	182	3	4

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

ตารางที่ 3.8 การจับคู่ความต้องการด้านความมั่นคงที่พึงจะมีกับแบบรูปการโจมตี (ต่อ)

หมายเลขความต้องการ (SSRB_ID)	หมายเลขแบบรูปการโจมตีตามคาเปกที่เกี่ยวข้อง (CAPEC_ID) [1]	ระดับความรุนแรงของแบบรูปการโจมตี (SEV) [1]	ระดับโอกาสของการใช้ประโยชน์ของแบบรูปการโจมตี (LOE) [1]
ATMC_009	7	4	4
	54	2	4
	127	3	4
	136	4	4
	139	4	4
	170	2	4
	182	3	4
ATMC_010	37	5	5
	65	4	2
	182	3	4
ความต้องการด้านความมั่นคงสำหรับส่วนควบคุมกลางของอินเทอร์เน็ตแบงค์กิ้ง			
IBC_001	7	4	4
	37	5	5
	39	3	5
	66	4	5
	83	4	4
	88	4	4
	100	5	4
	108	5	2
	110	5	4
	135	4	4
	136	4	4
	139	4	4
	182	3	4
	250	3 (N/A)	4

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

ตารางที่ 3.8 การจับคู่ความต้องการด้านความมั่นคงที่พึงจะมีกับแบบรูปการโจมตี (ต่อ)

หมายเลขความต้องการ (SSRB_ID)	หมายเลขแบบรูปการโจมตีตามคาเปกที่เกี่ยวข้อง (CAPEC_ID) [1]	ระดับความรุนแรงของแบบรูปการโจมตี (SEV) [1]	ระดับโอกาสของการใช้ประโยชน์ของแบบรูปการโจมตี (LOE) [1]
IBC_002	7	4	4
	37	5	5
	39	3	5
	66	4	5
	83	4	4
	88	4	4
	100	5	4
	108	5	2
	110	5	4
	135	4	4
	136	4	4
	139	4	4
	182	3	4
	250	3 (N/A)	4
IBC_003	N/A	N/A	N/A
IBC_004	N/A	N/A	N/A
IBC_005	N/A	N/A	N/A
IBC_006	N/A	N/A	N/A
IBC_007	476	4	2
IBC_008	7	4	4
	54	2	4
	127	3	4
	136	4	4
	139	4	4
	170	2	4
	182	3	4

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

ตารางที่ 3.8 การจับคู่ความต้องการด้านความมั่นคงที่พึงจะมีกับแบบรูปการโจมตี (ต่อ)

หมายเลขความต้องการ (SSRB_ID)	หมายเลขแบบรูปการโจมตีตามคาเปกที่เกี่ยวข้อง (CAPEC_ID) [1]	ระดับความรุนแรงของแบบรูปการโจมตี (SEV) [1]	ระดับโอกาสของการใช้ประโยชน์ของแบบรูปการโจมตี (LOE) [1]
IBC_009	7	4	4
	54	2	4
	127	3	4
	136	4	4
	139	4	4
	170	2	4
	182	3	4
ความต้องการด้านความมั่นคงสำหรับอินเทอร์เน็ตแบงค์กิ้ง			
IBS_001	57	5	3
	65	4	2
	94	5	5
	102	4	4
IBS_002	169	1	4
IBS_003	55	3	3
IBS_004	36	4	3
	60	4	4
IBS_005	36	4	3
	60	4	4
IBS_006	2	3	4
IBS_007	16	4	3
	49	4	3
	70	4	3
IBS_008	50	4	3
	70	4	3
	169	1	4
IBS_009	50	4	3
	60	4	4
	70	4	3
	169	1	4
IBS_010	N/A	N/A	N/A

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

ตารางที่ 3.8 การจับคู่ความต้องการด้านความมั่นคงที่พึงจะมีกับแบบรูปการโจมตี (ต่อ)

หมายเลขความต้องการ (SSRB_ID)	หมายเลขแบบรูปการโจมตีตามคาเปกที่เกี่ยวข้อง (CAPEC_ID) [1]	ระดับความรุนแรงของแบบรูปการโจมตี (SEV) [1]	ระดับโอกาสของการใช้ประโยชน์ของแบบรูปการโจมตี (LOE) [1]
IBS_011	37	5	5
	65	4	1
	182	3	4
IBS_012	36	4	3
	69	5	5
	74	4	3
	87	4	4
IBS_013	21	4	4
	59	4	4
	60	4	4
	61	4	3
IBS_014	N/A	N/A	N/A
IBS_015	21	4	4
	60	4	4
IBS_016	36	4	3
	69	5	5
	74	4	3
	87	4	5
IBS_017	60	4	4
IBS_018	60	4	4
IBS_019	N/A	N/A	N/A

จากตารางที่ 3.8 จะเห็นได้ว่า เมื่อจับคู่ความต้องการด้านความมั่นคงที่พึงจะมีเข้ากับแบบรูปการโจมตีผ่านทางวิธีการบรรเทาแล้ว จะพบว่าความความสัมพันธ์ระหว่างความต้องการด้านความมั่นคงที่พึงจะมีต่อแบบรูปการโจมตี สามารถเป็นได้ในความสัมพันธ์แบบหนึ่งต่อหนึ่ง (one to one relationship) หรือความสัมพันธ์แบบหนึ่งต่อกลุ่ม (one to many relationship) ความต้องการด้านความมั่นคงที่พึงจะมีที่มีคู่ความสัมพันธ์แบบหนึ่งต่อกลุ่ม จะถูกพิจารณาค่าระดับความรุนแรง และค่าระดับโอกาสของการใช้ประโยชน์ใหม่ โดยใช้วิธีคำนวณแบบไฮวอร์เทอร์มาร์ค (High watermark) คือการใช้ค่าสูงสุดเป็นตัวแทน นอกจากนี้ยังปรากฏความต้องการด้านความมั่นคงที่พึงจะมีที่ไม่สามารถ

จับคู่ความสัมพันธ์กับแบบรูปการโจมตีใดได้ ในงานวิจัยนี้จะใช้ค่าน้ำหนักเป็นค่าปานกลางคือ 3 แทน ซึ่งทำให้ได้ค่าระดับความรุนแรง และค่าระดับโอกาสของการใช้ประโยชน์ใหม่ ดังตารางที่ 3.9

ตารางที่ 3.9 การจับคู่ความสัมพันธ์ระหว่างความต้องการด้านความมั่นคงที่พึงจะมีกับแบบรูปการโจมตีที่ผ่านการปรับค่าระดับความรุนแรงและค่าระดับโอกาสของการใช้ประโยชน์

หมายเลขความต้องการ (SREQ_ID)	ระดับความรุนแรงของแบบรูปการโจมตี (SEV) [1]	ระดับโอกาสของการใช้ประโยชน์ของแบบรูปการโจมตี (LOE) [1]
ความต้องการด้านความมั่นคงสำหรับระบบหลักการธนาคาร		
CBS_001	4	4
CBS_002	4	4
CBS_003	4	4
CBS_004	4	3
CBS_005	3 (N/A)	3 (N/A)
CBS_006	3 (N/A)	3 (N/A)
CBS_007	3	3
CBS_008	1	4
CBS_009	3 (N/A)	3 (N/A)
CBS_010	4	5
CBS_011	4	5
ความต้องการด้านความมั่นคงสำหรับส่วนควบคุมกลางเอทีเอ็ม		
ATMC_001	5	5
ATMC_002	5	5
ATMC_003	3 (N/A)	3 (N/A)
ATMC_004	3 (N/A)	3 (N/A)
ATMC_005	3 (N/A)	3 (N/A)
ATMC_006	3 (N/A)	3 (N/A)
ATMC_007	4	2
ATMC_008	4	4
ATMC_009	4	4
ATMC_010	5	5
ความต้องการด้านความมั่นคงสำหรับส่วนควบคุมกลางของอินเทอร์เน็ตแบงค์กิ้ง		
IBC_001	5	5
IBC_002	5	5
IBC_003	3 (N/A)	3 (N/A)

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

ตารางที่ 3.9 การจับคู่ความสัมพันธ์ระหว่างความต้องการด้านความมั่นคงที่พึงจะมีกับแบบรูปการโจมตีที่ผ่านการปรับค่าระดับความรุนแรงและค่าระดับโอกาสของการใช้ประโยชน์ (ต่อ)

หมายเลขความต้องการ (SREQ_ID)	ระดับความรุนแรงของแบบรูปการโจมตี (SEV) [1]	ระดับโอกาสของการใช้ประโยชน์ของแบบรูปการโจมตี (LOE) [1]
IBC_004	3 (N/A)	3 (N/A)
IBC_005	3 (N/A)	3 (N/A)
IBC_006	3 (N/A)	3 (N/A)
IBC_007	4	2
IBC_008	4	4
IBC_009	4	4
ความต้องการด้านความมั่นคงสำหรับอินเทอร์เน็ตแบงค์กิ้ง		
IBS_001	5	5
IBS_002	1	4
IBS_003	3	3
IBS_004	4	3
IBS_005	4	4
IBS_006	3	4
IBS_007	4	3
IBS_008	4	3
IBS_009	4	4
IBS_010	3 (N/A)	3 (N/A)
IBS_011	5	5
IBS_012	5	5
IBS_013	4	4
IBS_014	3 (N/A)	3 (N/A)
IBS_015	4	4
IBS_016	5	5
IBS_017	4	4
IBS_018	4	4
IBS_019	3 (N/A)	3 (N/A)

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

3.4 ประมวลผลข้อความสำหรับรายการความต้องการด้านความมั่นคงที่พึงจะมี

จากหัวข้อที่ 3.2 สามารถนำข้อมูลที่ได้จากการรวบรวมรายการความต้องการด้านความมั่นคงที่พึงจะมี มาเข้าสู่กระบวนการจัดทำคำสำคัญ โดยประยุกต์ใช้ขั้นตอนจากงานวิจัย [11] เพื่อให้ได้คำสำคัญในแต่ละรายการความต้องการด้านความมั่นคงที่พึงจะมี ประกอบด้วยขั้นตอนดังนี้

1. ดำเนินการตัดคำ (Word segmentation) และลบคำขยายให้แก่คำอื่น ๆ แต่ไม่มีความหมายในตัวเอง (Stop word) จำนวนทั้งสิ้น 619 คำ โดยในงานวิจัยใช้แหล่งข้อมูลคำขยายจาก [17] และคำที่เกี่ยวข้องกับโดเมน 39 คำ ได้แก่ “system” , “application”, “customer”, “bank”, “security”, “branch”, “software”, “company”, “employee”, “deposit”, “withdraw”, “saving”, “current”, “loan”, “money”, “cheque”, “cash”, “coin”, “interest”, “ATM” , “CDM”, “PUM”, “kiosk”, “credit”, “debit”, “BOT”, “currency”, “charge”, “overdraft”, “payin”, “slip”, “dividend”, “cashier”, “gift”, “forex”, “MLR”, “MRR”, “MOR”, “OD” ซึ่งคำเหล่านี้มักใช้ในบริบทของการกำหนดความต้องการเชิงฟังก์ชันทางธุรกิจ เช่น

“ระบบหลักการธนาคารสำหรับบัญชีออมทรัพย์ (Saving) จะต้องมีการบันทึกรายละเอียดการทำธุรกรรมและจัดเก็บไว้อย่างน้อย 90 วัน” และ

“ระบบหลักการธนาคารจะต้องมีการบันทึกรายละเอียดการทำธุรกรรมและจัดเก็บไว้อย่างน้อย 90 วัน”

ซึ่งจะพบว่าตัวอย่างแรกปรากฏคำว่า “บัญชีออมทรัพย์ (Saving)” แต่ในตัวอย่างที่สอง ซึ่งเมื่อพิจารณาเฉพาะความต้องการที่พึงจะมีที่ระบุให้จัดเก็บรายละเอียดการทำธุรกรรมไว้อย่างน้อย 90 วันนั้น คำว่า “บัญชีออมทรัพย์ (Saving)” จะไม่มีผลใดต่อการประเมินความเสี่ยงในข้อนี้เลย และอาจจะส่งผลในทางตรงกันข้ามโดยทำให้ค่า $D_{q,r}$ สูงขึ้น เนื่องจากมีการปรากฏของคำในเอกสารความต้องการของธนาคาร ซึ่งไม่ปรากฏในเอกสารความต้องการที่พึงจะมี

2. แปลงตัวอักษรพิมพ์ใหญ่ให้เป็นพิมพ์เล็กทั้งหมด ยกเว้นข้อความที่เป็นตัวอักษรพิมพ์ใหญ่ทั้งหมด เนื่องจากข้อความดังกล่าว จะเป็นคำย่อที่มีความหมายเฉพาะ อาทิเช่น SSL, HTTP เป็นต้น

3. ลบสัญลักษณ์ที่คั่นระหว่างคำ หรือท้ายคำ ได้แก่ จุด (“.”) จุลภาค (“,”) วงเล็บเปิด (“(“) และวงเล็บปิด (“)”)

4. ลบส่วนประกอบหลังคำหลัก (Suffix) อาทิเช่น –ster –eer –elle –ism เป็นต้น โดยหลักการ snowball [18]

3.5 ประมวลผลข้อความสำหรับเอกสารความต้องการด้านความมั่นคงของการธนาคาร

ขั้นตอนนี้เป็นการจัดเตรียมเอกสารความต้องการด้านความมั่นคงของการธนาคารซึ่งเป็นภาษาอังกฤษ ตามการแนะนำในงานวิจัย [11] เพื่อให้ขั้นตอนการหาความแตกต่างระหว่างความต้องการด้านความมั่นคงที่พึงจะมีกับเอกสารความต้องการด้านความมั่นคงของการธนาคารมีประสิทธิภาพมากขึ้น ประกอบด้วยขั้นตอนดังนี้

1. ตัดข้อความที่ไม่ได้เป็นความต้องการออกทั้งหมด ด้วยมือ อาทิเช่น สารบัญ บทนำ อภิธานศัพท์ ภาคผนวก เป็นต้น

2. ดำเนินการตัดคำ (Word segmentation) และลบคำขยายให้แก่คำอื่น ๆ แต่ไม่มีความหมายในตัวเอง และคำที่เกี่ยวข้องกับโดเมนนั้น โดยใช้แหล่งข้อมูลเดียวกับข้อ 1 ในหัวข้อ 3.4

3. แปลงตัวอักษรพิมพ์ใหญ่ให้เป็นพิมพ์เล็กทั้งหมด ยกเว้นข้อความที่เป็นตัวอักษรพิมพ์ใหญ่ทั้งหมด เนื่องจากข้อความดังกล่าว จะเป็นคำย่อที่มีความหมายเฉพาะ อาทิเช่น SSL, HTTP เป็นต้น

4. ลบสัญลักษณ์ที่คั่นระหว่างคำ หรือท้ายคำ ได้แก่ จุด (“.”) จุลภาค (“,”) วงเล็บเปิด (“(“) และวงเล็บปิด (“)”)

5. ลบส่วนประกอบหลังคำหลัก (Suffix) อาทิเช่น –ster –eer –elle –ism เป็นต้น โดยหลักการ snowball [18]

3.6 หาความแตกต่างระหว่างความต้องการด้านความมั่นคงที่พึงจะมีกับเอกสารความต้องการด้านความมั่นคงของการธนาคาร

นำคำสำคัญที่ได้ในหัวข้อที่ 3.4 มาหาค่าระดับความแตกต่างของความต้องการด้านความมั่นคงที่พึงจะมีกับรายการความต้องการด้านความมั่นคงของการธนาคารที่ได้ในหัวข้อที่ 3.5 ค่าระดับความแตกต่างนี้หาได้จากการประยุกต์ใช้สมการ Cosine Similarity โดยพิจารณาแบบกลับด้าน โดยนำ 1 ลบกับค่าที่ได้จากสมการ Cosine Similarity จะได้เป็นสมการความแตกต่างกันของเอกสาร ดังสมการที่ (3.1)

$$D_{q,r} = 1 - \frac{\sum_{i=1}^{N}\left(w_{q,i} * w_{r,i}\right)}{\sqrt{\sum_{i=1}^{N} w_{q,i}^{2}} * \sqrt{\sum_{i=1}^{N} w_{r,i}^{2}}} \qquad (3.1)$$

โดยที่ $w_{q,i}$ คือ น้ำหนักของคำ i ในความต้องการด้านความมั่นคงที่พึงจะมี q

$w_{r,i}$ คือ น้ำหนักของคำ i ในความต้องการ r

N คือ จำนวนคำทั้งหมด (ไม่นับซ้ำ) ในความต้องการด้านความมั่นคงที่พึงจะมี q และความต้องการ r

$D_{q,r}$ คือ ความแตกต่างระหว่างความต้องการด้านความมั่นคงที่พึงจะมี q และความต้องการ r ซึ่งจะมีค่าอยู่ระหว่าง 0 ถึง 1

โดยน้ำหนักของคำ i ทั้ง 2 ค่านั้นสามารถคำนวณได้จากค่า TF-IDF ตามสมการที่ (3.2)

$$w_{s,i} = \begin{cases} tf_{s,i} * idf_i = (1 + log_2) * log_2 \frac{D}{d_i} & \text{if } f_{s,i} > 0 \\ 0 \text{ otherwise} \end{cases} \quad (3.2)$$

โดยที่ D คือ จำนวนของความต้องการ (q หรือ r แล้วแต่กรณี)

d_i คือ จำนวนของความต้องการที่คำ i ปรากฏอยู่

เมื่อนำคำสำคัญสำหรับรายการความต้องการด้านความมั่นคงที่พึงจะมี (หัวข้อที่ 3.4) และคำสำคัญสำหรับรายการความต้องการของธนาคาร (หัวข้อที่ 3.5) มาเข้าสู่กระบวนการหาความแตกต่างระหว่างความต้องการด้านความมั่นคงที่พึงจะมีกับเอกสารความต้องการด้านความมั่นคงของการธนาคาร ค่า $D_{q,r}$ ที่ได้ในแต่ละรายการความต้องการด้านความมั่นคงที่พึงจะมี จะมีจำนวนเท่ากับรายการความต้องการด้านความมั่นคงของการธนาคาร ดังแสดงในตารางที่ 3.10 เป็นตัวอย่างการคำนวณค่า $D_{q,r}$ ของเอกสารความต้องการด้านความมั่นคงที่พึงจะมีในส่วนของความต้องการด้านความมั่นคงสำหรับอินเทอร์เน็ตแบงค์กิ้ง (SSRB) และเอกสารความต้องการด้านความมั่นคงของธนาคารแห่งหนึ่ง (SRB) ซึ่งมีจำนวนความต้องการที่สามารถสกัดได้ 18 ข้อ (รายละเอียดความต้องการด้านความมั่นคงของธนาคารแห่งนี้ แสดงในภาคผนวก ค) โดยค่า $D_{q,r}$ จะมีค่าตั้งแต่ 0 ถึง 1 ซึ่งสามารถแปลความหมายได้ดังนี้

ค่า $D_{q,r}$ เท่ากับ 0 หมายถึง ความต้องการด้านความมั่นคงของธนาคารรายการดังกล่าวสอดคล้องกับ ความต้องการด้านความมั่นคงที่พึงจะมีโดยสมบูรณ์

ค่า $D_{q,r}$ เท่ากับ 1 หมายถึง ความต้องการด้านความมั่นคงของธนาคารรายการดังกล่าวไม่สอดคล้องเลยกับความต้องการด้านความมั่นคงที่พึงจะมี

ค่า $D_{q,r}$ อยู่ระหว่าง 0 ถึง 1 หมายถึง ความต้องการด้านความมั่นคงของธนาคารรายการดังกล่าวสอดคล้องกับความต้องการด้านความมั่นคงที่พึงจะมีเพียงบางส่วน

ตารางที่ 3.10 ผลลัพธ์การหาความแตกต่าง $D_{q,r}$ ระหว่างเอกสารความต้องการด้านความมั่นคงที่พึงจะมีและเอกสารความต้องการด้านความมั่นคงของธนาคาร

SRB_ID / SSRB_ID	$D_{q,r}$					
	SRB_001	SRB_002	SRB_003	SRB_004	SRB_005	SRB_006
IBS_001	0.12961	1.0	1.0	1.0	0.75381	1.0
IBS_002	0.76905	0.75746	1.0	0.83358	0.83670	0.9
IBS_003	1.0	0.07804	1.0	1.0	0.81742	0.88819
IBS_004	1.0	1.0	0.14188	0.91637	1.0	1.0
IBS_005	1.0	1.0	1.0	1.0	1.0	1.0
IBS_006	1.0	1.0	0.91229	0.07692	1.0	1.0
IBS_007	1.0	0.91229	1.0	1.0	0.53708	0.81101
IBS_008	1.0	0.85997	0.81742	0.83987	0.76429	0.71132
IBS_009	1.0	0.89153	0.57573	1.0	0.81742	0.77639
IBS_010	1.0	1.0	0.81742	0.67974	1.0	1.0
IBS_011	0.92546	0.74951	0.83670	0.92838	0.78918	0.87090
IBS_012	1.0	0.81666	1.0	1.0	1.0	1.0
IBS_013	1.0	1.0	0.71715	1.0	1.0	1.0
IBS_014	1.0	1.0	0.88047	1.0	1.0	1.0
IBS_015	1.0	1.0	0.85857	1.0	1.0	1.0
IBS_016	1.0	1.0	0.87035	1.0	1.0	1.0
IBS_017	1.0	0.90098	0.74180	1.0	0.83333	0.79587
IBS_018	1.0	1.0	1.0	0.86132	1.0	1.0
IBS_019	1.0	0.91425	1.0	1.0	1.0	1.0

ตารางที่ 3.10 ผลลัพธ์การหาความแตกต่าง $D_{q,r}$ ระหว่างเอกสารความต้องการด้านความมั่นคงที่พึงจะมีและเอกสารความต้องการด้านความมั่นคงของธนาคาร (ต่อ)

SRB_ID / SSRB_ID	$D_{q,r}$					
	SRB_007	SRB_008	SRB_009	SRB_010	SRB_011	SRB_012
IBS_001	1.0	1.0	1.0	1.0	0.90465	1.0
IBS_002	0.84881	0.84881	0.91835	1.0	0.87350	1.0
IBS_003	0.83096	0.85092	0.90871	1.0	0.85857	0.9
IBS_004	1.0	0.89949	0.63072	0.84924	0.90465	1.0
IBS_005	1.0	1.0	1.0	1.0	1.0	1.0
IBS_006	1.0	0.90754	1.0	0.72264	0.91229	1.0
IBS_007	0.71428	0.74802	0.84569	1.0	1.0	1.0
IBS_008	0.56356	0.03774	0.64644	1.0	1.0	1.0
IBS_009	0.66193	0.55278	0.08712	1.0	1.0	1.0
IBS_010	1.0	1.0	1.0	0.13397	1.0	1.0
IBS_011	0.80481	0.82786	0.89459	1.0	0.26515	1.0
IBS_012	1.0	1.0	1.0	1.0	1.0	0.15484
IBS_013	1.0	0.85092	1.0	1.0	0.85857	1.0
IBS_014	1.0	1.0	1.0	1.0	0.88047	1.0
IBS_015	1.0	1.0	1.0	1.0	0.85857	1.0
IBS_016	1.0	0.91091	1.0	1.0	1.0	1.0
IBS_017	0.69139	0.72783	0.49999	1.0	1.0	1.0
IBS_018	0.81101	1.0	0.79587	1.0	1.0	1.0
IBS_019	1.0	1.0	1.0	1.0	1.0	0.84188

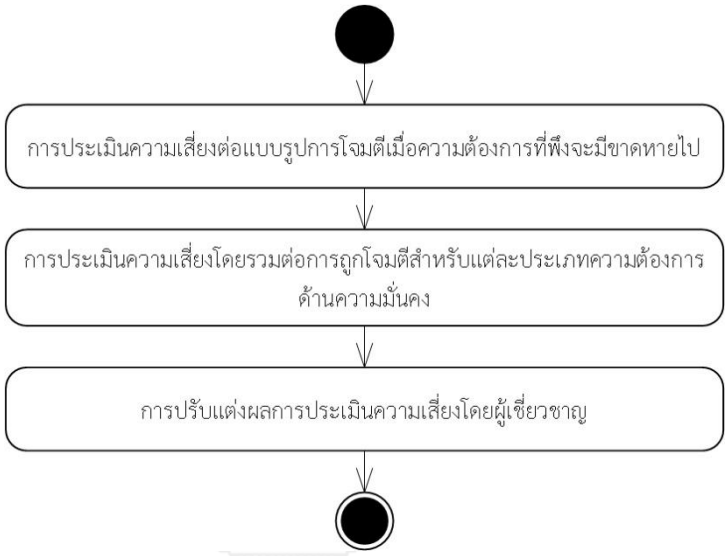
จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

ตารางที่ 3.10 ผลลัพธ์การหาความแตกต่าง $D_{q,r}$ ระหว่างเอกสารความต้องการด้านความมั่นคงที่พึงจะมีและเอกสารความต้องการด้านความมั่นคงของธนาคาร (ต่อ)

SRB_ID / SSRB_ID	$D_{q,r}$					
	SRB_013	SRB_014	SRB_015	SRB_016	SRB_017	SRB_018
IBS_001	1.0	1.0	1.0	1.0	1.0	1.0
IBS_002	1.0	1.0	1.0	0.91835	0.92928	0.92440
IBS_003	1.0	1.0	1.0	0.90871	0.92094	0.91548
IBS_004	0.86516	0.89339	0.86516	1.0	1.0	1.0
IBS_005	1.0	1.0	1.0	1.0	1.0	1.0
IBS_006	1.0	1.0	1.0	1.0	1.0	1.0
IBS_007	1.0	1.0	1.0	1.0	1.0	1.0
IBS_008	0.87090	1.0	1.0	0.88214	1.0	0.89089
IBS_009	1.0	1.0	1.0	1.0	1.0	1.0
IBS_010	1.0	1.0	1.0	1.0	1.0	1.0
IBS_011	1.0	0.81742	0.76905	1.0	1.0	1.0
IBS_012	1.0	1.0	1.0	0.69139	0.73273	0.71428
IBS_013	0.2	0.68377	0.8	0.81742	1.0	0.66193
IBS_014	0.83096	0.33184	0.83096	1.0	1.0	0.85714
IBS_015	1.0	0.84188	0.0	1.0	1.0	1.0
IBS_016	0.88047	1.0	1.0	0.23623	0.52754	0.39390
IBS_017	1.0	1.0	1.0	1.0	1.0	1.0
IBS_018	1.0	1.0	0.55278	1.0	1.0	1.0
IBS_019	0.84188	0.875	1.0	0.85566	0.875	0.73273

3.7 ประมาณความเสี่ยงด้านความมั่นคง

จากค่าความแตกต่างระหว่างความต้องการด้านความมั่นคงที่พึงจะมีกับเอกสารความต้องการของธนาคารในขั้นตอนที่ 3.6 จะสามารถนำมาใช้เป็นข้อมูลตั้งต้นในการประเมินความเสี่ยงจากการขาดหายของความต้องการด้านความมั่นคงที่พึงจะมีในเอกสารความต้องการด้านความมั่นคงของการธนาคาร 3 ขั้นตอน ดังภาพที่ 3.3



ภาพที่ 3.3 แผนผังขั้นตอนประเมินความเสี่ยงจากการขาดหายของความต้องการด้านความมั่นคงที่พึงจะมีในเอกสารความต้องการด้านความมั่นคงของการธนาคาร

3.7.1 การประเมินความเสี่ยงต่อแบบรูปการโจมตีเมื่อความต้องการด้านความมั่นคงที่พึงจะมีขาดหายไป

ผู้วิจัยจะกำหนดค่าขีดแบ่ง (Threshold) ของความแตกต่างระหว่างรายการความต้องการด้านความมั่นคงที่พึงจะมีกับรายการความต้องการในเอกสารของการธนาคารไว้ โดยจากขั้นตอนที่ 3.6 หากรายการความต้องการด้านความมั่นคงที่พึงจะมี q มีค่า $D_{q,r}$ น้อยกว่าหรือเท่ากับค่าขีดแบ่งสำหรับอย่างน้อยหนึ่งรายการความต้องการ r_j ในเอกสารของการธนาคาร จะแสดงว่ารายการความต้องการด้านความมั่นคงที่พึงจะมี q นั้นปรากฏอยู่ในเอกสารของการธนาคารแล้ว (จะกำหนดค่าให้เป็น 0) แต่หากรายการความต้องการด้านความมั่นคงที่พึงจะมี q มีค่า $D_{q,r}$ มากกว่าค่าขีดแบ่งสำหรับทุกรายการความต้องการ r_j ในเอกสารของการธนาคาร จะแสดงว่ารายการความต้องการด้านความมั่นคงที่พึงจะมี q นั้นขาดหายไปจากเอกสารของการธนาคาร โดยเราจะนำค่า $D_{q,r}$

ที่มากกว่าค่าขีดแบ่งแต่น้อยที่สุดมาคำนวณดัชนีความเสี่ยงต่อแบบรูปการโจมตี p_i ใด ๆ เมื่อความต้องการด้านความมั่นคงที่พึงจะมี q ขาดหายไป โดยใช้สมการ (3.3)

$$R_q = min(D_{q,r}) * LOE_q * SEV_q \quad (3.3)$$

โดยที่ $min(D_{q,r})$ คือ ค่าคะแนนต่ำสุดของความแตกต่างระหว่างความต้องการด้านความมั่นคงที่พึงจะมี q กับเอกสารความต้องการด้านความมั่นคงของการธนาคาร r_i

LOE_q คือค่าระดับโอกาสของการใช้ประโยชน์ของแบบรูปการโจมตีที่สอดคล้องกับความต้องการที่พึงจะมี q (ตารางที่ 3.9)

SEV_q คือ ค่าระดับความรุนแรงของแบบรูปการโจมตีที่สอดคล้องกับความต้องการที่พึงจะมี q (ตารางที่ 3.9)

การที่เรานำค่า $D_{q,r}$ ที่มากกว่าค่าขีดแบ่งแต่น้อยที่สุดมาคำนวณดัชนีความเสี่ยงนั้น มีสาเหตุมาจาก ในเอกสารความต้องการด้านความมั่นคงของการธนาคาร อาจมีรายการความต้องการอื่น (r_*) ที่นอกเหนือจากความต้องการด้านความมั่นคงที่พึงจะมีที่ธนาคารแห่งประเทศไทยกำหนดไว้ในเบื้องต้น ในกรณีนี้ในการเปรียบเทียบความเสี่ยงจากการขาดหายไปของความต้องการด้านความมั่นคงที่พึงจะมีสองความต้องการ q_1 และ q_2 ใด ๆ จะได้ค่า $D_{q1,r*}$ และ $D_{q2,r*}$ ที่มีค่าสูงทั้งคู่ แต่ค่านี้ไม่ได้สะท้อนถึงการปฏิบัติตามหรือไม่ปฏิบัติตามแนวปฏิบัติที่ดีฯ จึงทำให้ไม่สะท้อนถึงความเสี่ยงจากการไม่ปฏิบัติตามซึ่งงานวิจัยนี้ต้องการพิจารณา และทำให้การเปรียบเทียบค่า $D_{q1,r*}$ และ $D_{q2,r*}$ ว่าการขาดหายไปของ q_1 หรือ q_2 จะมีความเสี่ยงมากกว่ากันนั้นจึงไม่สื่อความหมาย ดังนั้นผู้วิจัยจึงเลือกใช้ค่า $min(D_{q,r})$ มาคำนวณดัชนีความเสี่ยง ซึ่งการเปรียบเทียบค่า $min(D_{q1,r*})$ กับค่า $min(D_{q2,r*})$ จะสะท้อนถึงระดับความเสี่ยงที่แตกต่างกันจากการขาดหายไปของ q_1 และ q_2ได้ดีกว่า

การคำนวณค่าดัชนีความเสี่ยงต่อแบบรูปการโจมตีเมื่อความต้องการด้านความมั่นคงที่พึงจะมี ขาดหายไปแสดงในตารางที่ 3.11 ซึ่งกำหนดให้ค่าขีดแบ่งเป็น 0.4

ตารางที่ 3.11 ผลลัพธ์การคำนวณหาค่าดัชนีความเสี่ยงต่อแบบรูปการโจมตี R_q

SSRB_ID	Requirement_Type	$min(D_{q,r})$	SEV	LOE	R_q
IBS_001	Privacy	0.12961 -> 0	5	5	0.0
IBS_002	Privacy	0.75746	1	4	3.02985
IBS_003	Integrity	0.07804 -> 0	3	3	0.0
IBS_004	Authentication	0.14188 -> 0	4	4	0.0

ตารางที่ 3.11 ผลลัพธ์การคำนวณหาค่าดัชนีความเสี่ยงต่อแบบรูปการโจมตี R_q (ต่อ)

SSRB_ID	Requirement_Type	$min(D_{q,r})$	SEV	LOE	R_q
IBS_005	Identification	1.0	4	4	16.0
IBS_006	Authentication	0.07692 -> 0	3	4	0.0
IBS_007	Authentication	0.53708	4	3	6.44507
IBS_008	Authentication	0.03774 -> 0	4	3	0.0
IBS_009	Authentication	0.08712 -> 0	4	4	0.0
IBS_010	Identification	0.13397 -> 0	3	3	0.0
IBS_011	Privacy	0.26515 -> 0	5	5	0.0
IBS_012	Authorization	0.15484 -> 0	5	5	0.0
IBS_013	Authentication	0.2 -> 0	4	4	0.0
IBS_014	Instrusion Detection	0.33184 -> 0	3	3	0.0
IBS_015	Immunity	0.0	4	4	0.0
IBS_016	Authentication	0.23623 -> 0	5	5	0.0
IBS_017	Authentication	0.49999	4	4	7.99999
IBS_018	Authentication	0.55278	4	4	8.84458
IBS_019	Identification	0.73273	3	3	6.59464

3.7.2 การประเมินความเสี่ยงโดยรวมต่อการถูกโจมตีสำหรับแต่ละประเภทความต้องการด้านความมั่นคง

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

เนื่องจากแต่ละประเภทความต้องการด้านความมั่นคง (12 ประเภท) มีจำนวนข้อกำหนดความต้องการที่ไม่เท่ากันและจำนวนข้อกำหนดที่ขาดหายไปแตกต่างกันด้วย ซึ่งการประเมินความเสี่ยงโดยรวมต่อการถูกโจมตีจากมุมมองของแต่ละประเภทความต้องการ c สามารถพิจารณาได้โดยหาค่าสูงสุดของความเสี่ยงในประเภทข้อกำหนดความต้องการ ดังสมการ (3.4) ดังตัวอย่างการคำนวณในตารางที่ 3.12 โดยค่า R_c เป็นค่าระดับความเสี่ยงโดยรวมต่อการถูกโจมตีสำหรับแต่ละประเภทความต้องการด้านความมั่นคง หากประเภทความต้องการด้านความมั่นคงใดมีค่า R_c มาก หมายถึงความต้องการด้านความมั่นคงประเภทนั้นมีความเสี่ยงต่อการถูกโจมตีสูง

$$R_c = max(R_q) \tag{3.4}$$

ตารางที่ 3.12 ตัวอย่างผลลัพธ์การคำนวณหาค่าความเสี่ยงโดยรวมต่อการถูกโจมตีสำหรับแต่ละประเภทความต้องการด้านความมั่นคง

SSRB_ID	Requirement_Type	$min(D_{q,r})$	SEV	LOE	R_q	R_c
IBS_004	Authentication	0.14188 -> 0	4	4	0	
IBS_006	Authentication	0.07692 -> 0	3	4	0	
IBS_007	Authentication	0.53708	4	3	6.44507	
IBS_008	Authentication	0.03774 -> 0	4	3	0	
IBS_009	Authentication	0.08712 -> 0	4	4	0	8.84458
IBS_013	Authentication	0.2 -> 0	4	4	0	
IBS_016	Authentication	0.23623 -> 0	5	5	0	
IBS_017	Authentication	0.49999	4	4	7.99999	
IBS_018	Authentication	0.55278	4	4	8.84458	
IBS_012	Authorization	0.15484 -> 0	5	5	0	0
IBS_005	Identification	1	4	4	16	
IBS_010	Identification	0.13397 -> 0	3	3	0	16
IBS_019	Identification	0.73273	3	3	6.59464	
IBS_015	Immunity	0	4	4	0	0
IBS_014	Instrusion Detection	0.33184 -> 0	3	3	0	0
IBS_003	Integrity	0.07804 -> 0	3	3	0	0
IBS_001	Privacy	0.12961 -> 0	5	5	0	
IBS_002	Privacy	0.75746	1	4	3.02985	3.02985
IBS_011	Privacy	0.26515 -> 0	5	5	0	

เมื่อได้ค่าดัชนีความเสี่ยงโดยรวมต่อการถูกโจมตีสำหรับแต่ละประเภทความต้องการด้านความมั่นคง R_c แล้ว ผู้วิจัยจะนำดัชนีความเสี่ยงมาจัดลำดับจากมากไปน้อย

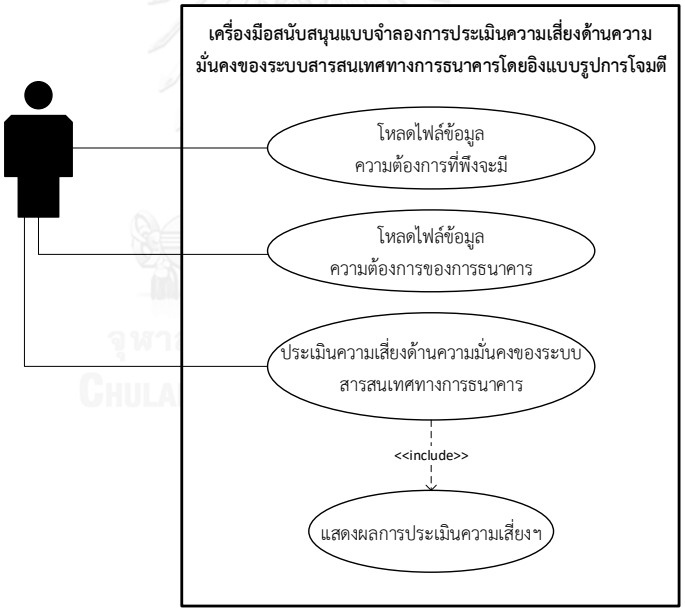
3.7.3 ปรับแต่งผลการประเมินความเสี่ยงโดยผู้เชี่ยวชาญ

เนื่องจากการประเมินความเสี่ยงจากการขาดหายของความต้องการด้านความมั่นคงที่พึงจะมีในเอกสารความต้องการด้านความมั่นคงของการธนาคาร อาจยังมีความไม่สมบูรณ์ เนื่องจากเอกสารความต้องการด้านความมั่นคงของการธนาคารอาจมีการลักษณะการเขียนที่ส่งผลให้แบบจำลองการประเมินความเสี่ยงฯ ไม่สามารถตรวจจับได้อย่างสมบูรณ์ อาทิเช่น การเขียนเอกสารความต้องการด้านความมั่นคงของการธนาคารแยกเป็น 2 ข้อ จากความต้องการด้านความมั่นคงที่พึง

จะมีเพียงข้อเดียว เป็นต้น ดังนั้นในขั้นตอนนี้จึงเป็นขั้นตอนที่ให้ผู้เชี่ยวชาญสามารถปรับแต่งค่าผลการประเมินความเสี่ยงต่อแบบรูปการโจมตีเมื่อความต้องการด้านความมั่นคงที่พึงจะมีขาดหายไป R_q เพื่อให้ได้ผลลัพธ์ของการประเมินความเสี่ยงจากการขาดหายของความต้องการด้าน ความมั่นคงที่พึงจะมีในเอกสารความต้องการด้านความมั่นคงของการธนาคาร สมบูรณ์มากที่สุด

3.8 พัฒนาเครื่องมือสนับสนุนแบบจำลอง

การพัฒนาเครื่องมือสนับสนุนแบบจำลองการประเมินความเสี่ยงด้านความมั่นคงของระบบสารสนเทศทางการธนาคารโดยอิงแบบรูปการโจมตีได้พัฒนาโดยใช้เน็ตบีนส์ ซึ่งเป็นเครื่องมือสำหรับพัฒนาแอปพลิเคชันด้วยภาษาจาวา ประกอบด้วย 3 ส่วน ได้แก่ ส่วนนำเข้าเอกสารความต้องการด้านความมั่นคงที่พึงจะมีและเอกสารความต้องการด้านความมั่นคงของการธนาคาร ส่วนประมวลความแตกต่างของรายการความต้องการด้านความมั่นคงที่พึงจะมีกับเอกสารความต้องการของการธนาคาร และค่าความเสี่ยง และส่วนการแสดงผล ดังภาพที่ 3.4



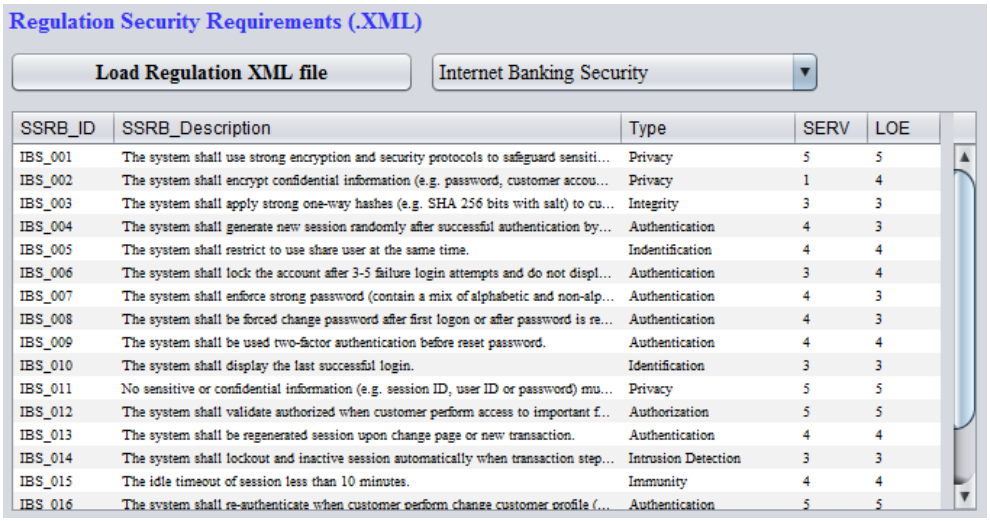
ภาพที่ 3.4 ยูสเคสแสดงความต้องการสำหรับเครื่องมือสนับสนุนแบบจำลองการประเมินความเสี่ยงด้านความมั่นคงของระบบสารสนเทศทางการธนาคารโดยอิงแบบรูปการโจมตี

3.8.1 ส่วนนำเข้าเอกสารความต้องการด้านความมั่นคงที่พึงจะมีและเอกสารความต้องการของการธนาคาร

1. ผู้ประเมินทำการนำเข้าข้อมูลความต้องการด้านความมั่นคงที่พึงจะมี ที่อยู่ในรูปแบบเอกซ์เอ็มแอล (XML) ดังภาพที่ 3.5 และส่วนแสดงรายละเอียดข้อมูลความต้องการด้านความมั่นคงที่พึงจะมีที่ผ่านการโหลดเข้าสู่เครื่องมือ ดังภาพที่ 3.6

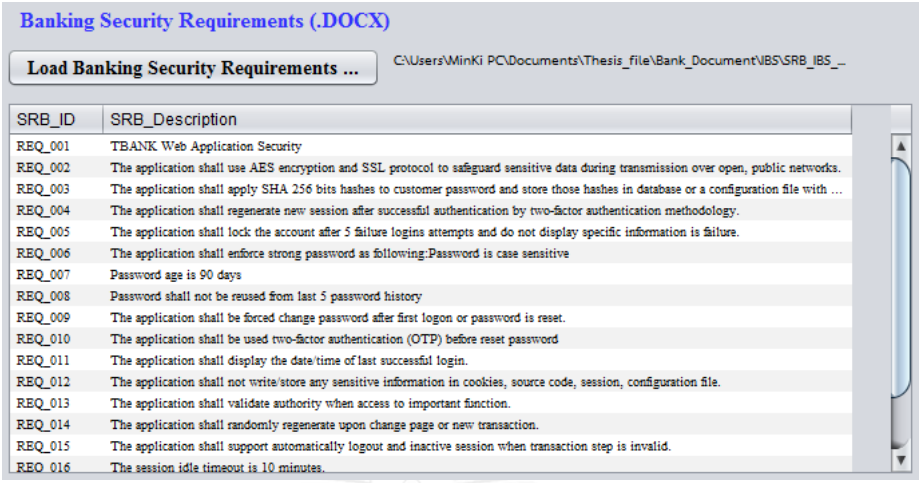
```
<?xml version="1.0" encoding="UTF-8"?>
<banksecurityreq>
  <ibs>
    <requirement>
      <id>IBS_001</id>
      <type>Integrity</type>
<desc>The system shall use strong encryption and security protocols to safeguard sensitive data during
smission over open, public networks.</desc>
      <serv>5</serv>
      <loe>5</loe>
    </requirement>
    <requirement>
      <id>IBS_002</id>
      <type>Integrity</type>
      <desc>The system shall encrypt confidential information ( e. g. password, customer account
 information) by strong encryption (e.g. AES 128 bits, AES 256 bits, RSA 2048).</desc>
      <serv>1</serv>
      <loe>4</loe>
    </requirement>
    <requirement>
      <id>IBS_003</id>
      <type>Integrity</type>
      <desc>The system shall apply strong one-way hashes ( e. g. SHA 256 bits with salt) to customer
 password and store those hashes in database or a configuration file with appropriate access
 ….
```

ภาพที่ 3.5 ข้อมูลนำเข้าความต้องการด้านความมั่นคงที่พึงจะมี ที่อยู่ในรูปแบบเอกซ์เอ็มแอล



ภาพที่ 3.6 ผลการนำเข้าข้อมูลความต้องการด้านความมั่นคงที่พึงจะมี

2. ผู้ประเมินทำการนำเข้าเอกสารความต้องการด้านความมั่นคงของการธนาคาร ที่อยู่ในรูปแบบดีโอซี (DOC) หรือดีโอซีเอกซ์ (DOCX) ดังภาพที่ 3.7



ภาพที่ 3.7 ผลการนำเข้าข้อมูลความต้องการด้านความมั่นคงของการธนาคาร

3.8.2 ส่วนประเมินความเสี่ยงด้านความมั่นคงของระบบสารสนเทศทางการธนาคาร

เมื่อผู้ประเมินนำเข้าข้อมูลเรียบร้อยแล้ว ในส่วนนี้จะนำข้อมูลนำเข้าทั้งสองส่วน (ข้อมูลนำเข้าข้อ 3.8.1 (1) และ ข้อมูลนำเข้าข้อ 3.8.1 (2)) มาคำนวณหาความแตกต่างของรายการความต้องการด้านความมั่นคงที่พึงจะมีกับเอกสารความต้องการของการธนาคารและประเมินความเสี่ยง ซึ่งการคำนวณเป็นไปตามแบบจำลองในหัวข้อที่ 3.6 และ 3.7 ซึ่งในขั้นตอนนี้ผู้ประเมินสามารถกำหนดค่าขีดแบ่งที่ยอมรับได้สำหรับค่าความแตกต่างดังภาพที่ 3.8

ภาพที่ 3.8 การกำหนดค่าขีดแบ่งและการคำนวณหาความแตกต่างของรายการความต้องการด้านความมั่นคงที่พึงจะมีกับเอกสารความต้องการของการธนาคารและค่าความเสี่ยง

3.8.3 ส่วนแสดงผลการประเมินความเสี่ยง

ในส่วนนี้ จะเป็นการแสดงผลซึ่งมีการแสดงค่าความแตกต่างของรายการความต้องการด้านความมั่นคงที่พึงจะมีกับเอกสารความต้องการด้านความมั่นคงของการธนาคาร ค่าความเสี่ยง ตามแบบจำลองในหัวข้อที่ 3.7 ประกอบด้วยค่าคะแนนต่ำสุดของความแตกต่างระหว่างความต้องการด้านความมั่นคงที่พึงจะมีกับเอกสารความต้องการด้านความมั่นคงของการธนาคาร ($min(D_{q,r})$) ค่าความเสี่ยงต่อแบบรูปการโจมตีเมื่อความต้องการด้านความมั่นคงที่พึงจะมีขาดหายไป (R_q) ดังภาพที่ 3.9

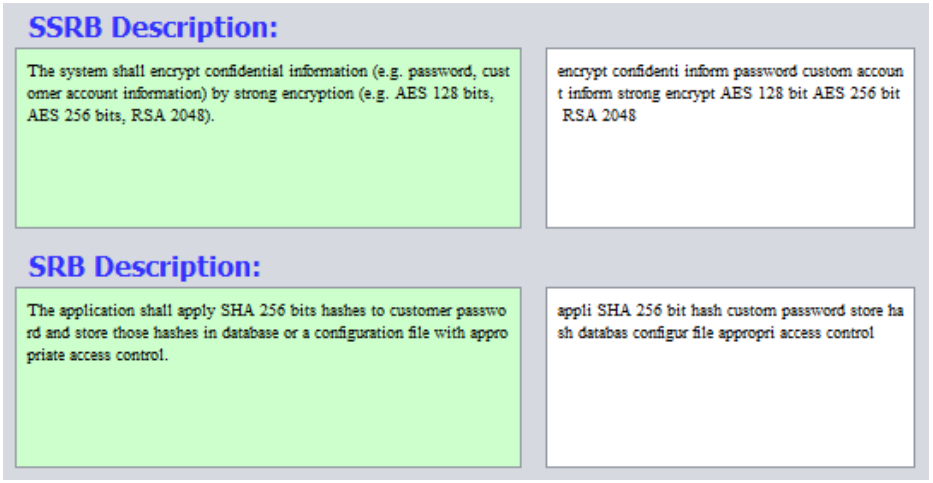
และค่าความเสี่ยงโดยรวมต่อการถูกโจมตีสำหรับแต่ละประเภทความต้องการด้านความมั่นคง (R_c) ดังภาพที่ 3.10 นอกจากนั้นเครื่องมือยังแสดงข้อความรายการความต้องการด้านความมั่นคงที่พึงจะมีกับเอกสารความต้องการของการธนาคารที่มีความแตกต่างกันน้อยที่สุดพร้อมทั้งข้อความที่ผ่านกระบวนการตามแบบจำลองในหัวข้อที่ 3.4 และ 3.5 ดังภาพที่ 3.11

SSRB_ID	SRB_ID	min(Dq,r)	Rq
IBS_001	REQ_001	0.0	0.0
IBS_002	REQ_002	0.757464374...	3.029857499...
IBS_003	REQ_002	0.0	0.0
IBS_004	REQ_003	0.0	0.0
IBS_005	REQ_001	1.0	16.0
IBS_006	REQ_004	0.0	0.0
IBS_007	REQ_005	0.537089950...	6.445079401...
IBS_008	REQ_008	0.0	0.0
IBS_009	REQ_009	0.0	0.0
IBS_010	REQ_010	0.0	0.0
IBS_011	REQ_011	0.0	0.0
IBS_012	REQ_012	0.0	0.0
IBS_013	REQ_013	0.0	0.0
IBS_014	REQ_014	0.0	0.0
IBS_015	REQ_015	0.0	0.0
IBS_016	REQ_016	0.0	0.0
IBS_017	REQ_009	0.499999999...	7.999999999...
IBS_018	REQ_015	0.552786404...	8.844582472...
IBS_019	REQ_018	0.732738758...	6.594648822...

ภาพที่ 3.9 ค่าความเสี่ยงต่อแบบรูปการโจมตีเมื่อความต้องการด้านความมั่นคงที่พึงจะมีขาดหายไป

Type	Rc
Identification	16
Authentication	8.84458
Privacy	3.02985

ภาพที่ 3.10 ค่าความเสี่ยงโดยรวมต่อการถูกโจมตีสำหรับแต่ละประเภทความต้องการด้านความมั่นคง



ภาพที่ 3.11 รายการความต้องการด้านความมั่นคงที่พึงจะมีกับเอกสารความต้องการของการธนาคารที่มีความแตกต่างกันน้อยที่สุดพร้อมทั้งข้อความที่ผ่านกระบวนการตามแบบจำลอง

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

บทที่ 4
การประเมินผลการวิจัย

ในบทนี้จะกล่าวถึงผลที่ได้จากการวิจัยตามแนวคิดและวิธีการวิจัยในบทที่ 3 ในส่วนของการทดลองและประเมินผล ซึ่งได้แบ่งเป็น 4 การประเมิน ได้แก่

1. การประเมินความถูกต้องของการจับคู่ของความมั่นคงที่พึงจะมีกับวิธีการบรรเทาการโจมตี
2. การประเมินประสิทธิภาพของการหาความแตกต่างระหว่างความต้องการด้านความมั่นคงที่พึงจะมีกับเอกสารความต้องการด้านความมั่นคงของการธนาคาร
3. การประเมินความสอดคล้องของค่าความเสี่ยงของความต้องการด้านความมั่นคงที่ขาดหายไปซึ่งได้จากเครื่องมือกับค่าความเสี่ยงจากผู้เชี่ยวชาญ
4. การวิเคราะห์ต้นทุนและผลประโยชน์

4.1 การประเมินความถูกต้องของการจับคู่ความมั่นคงที่พึงจะมีกับวิธีการบรรเทาการโจมตีและความต้องการด้านความมั่นคงที่เกี่ยวข้อง

ในการประเมินความถูกต้องของการจับคู่ความมั่นคงที่พึงจะมีกับวิธีการบรรเทาการโจมตีนี้ผู้วิจัยได้สร้างแบบสอบถามเพื่อสอบถามความเหมาะสมในการจับคู่ ซึ่งทำโดยผู้เชี่ยวชาญที่มีประสบการณ์ในการทำงานด้านความมั่นคง 12 คน (รายละเอียดการให้ข้อมูลอยู่ในภาคผนวก ข) โดยสามารถสรุปภาพรวมข้อมูลของผู้ประเมินได้ดังตารางที่ 4.1 – 4.4

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

ตารางที่ 4.1 ระดับการศึกษาของผู้ประเมิน

ระดับการศึกษา	จำนวนผู้ทำการประเมิน	ร้อยละ
ปริญญาโท	4	33.33
ปริญญาตรี	8	66.67

ตารางที่ 4.2 ตำแหน่งงานของผู้ประเมิน

ตำแหน่งงาน	จำนวนผู้ทำการประเมิน	ร้อยละ
Security Specialist	5	41.67
Security Audit	3	25.00
Security Engineer	4	33.33

ตารางที่ 4.3 ประสบการณ์ด้านความมั่นคงของผู้ประเมิน

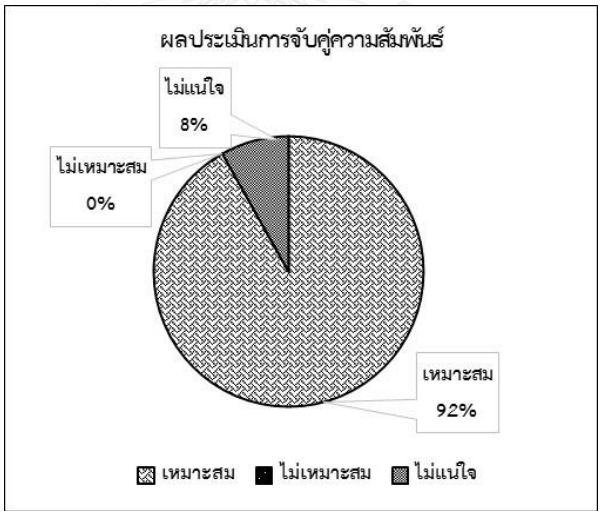
ประสบการณ์การทำงาน	จำนวนผู้ทำการประเมิน	ร้อยละ
1-3 ปี	2	16.67
4-6 ปี	3	25.00
7-10 ปี	3	25.00
มากกว่า 10 ปี	4	33.33

ตารางที่ 4.4 การรู้จักคาเปกของผู้ประเมิน

รู้จักคาเปก	จำนวนผู้ทำการประเมิน	ร้อยละ
รู้จักมาก่อน	5	41.67
ไม่รู้จักมาก่อน	7	58.33

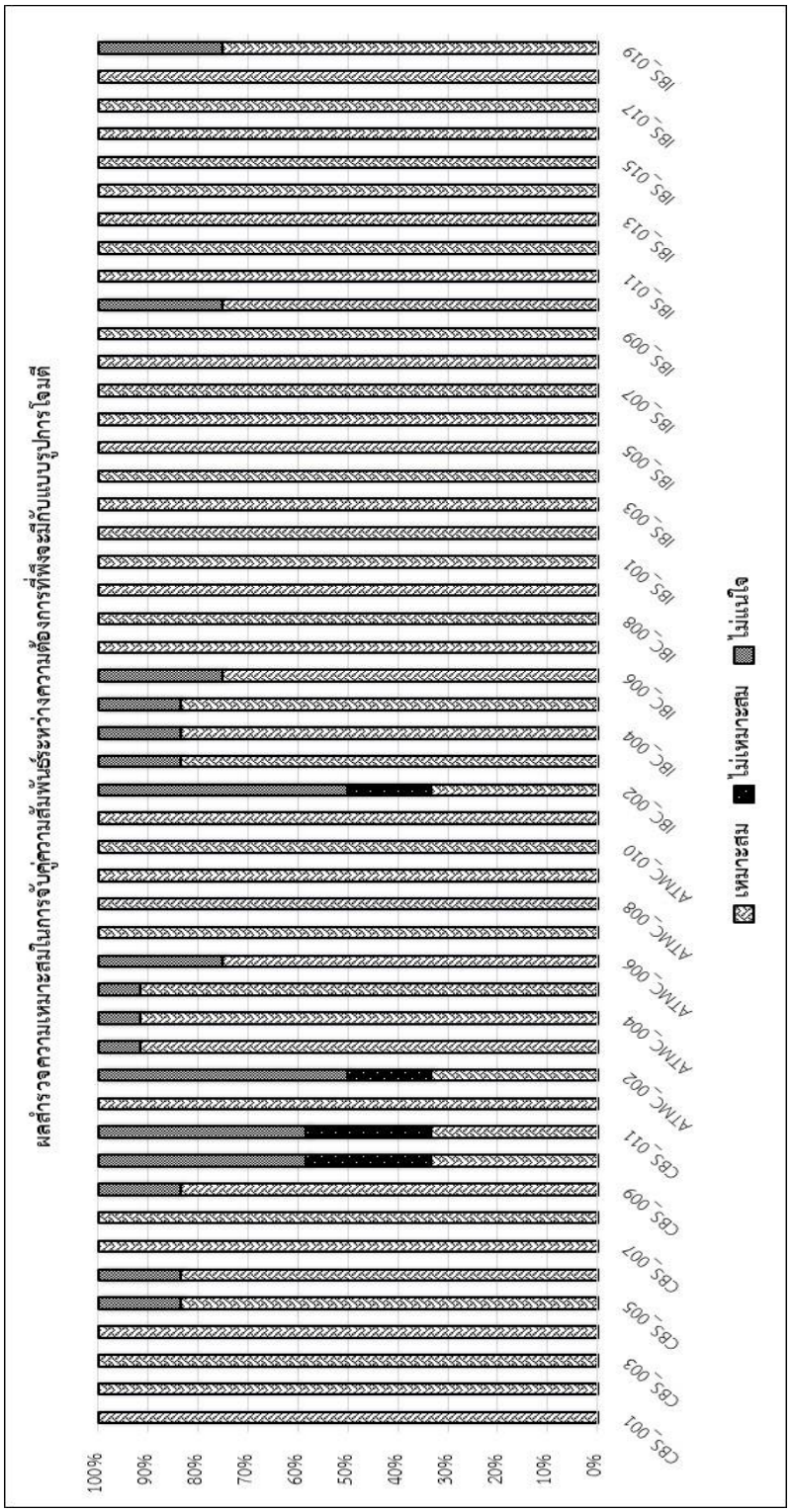
โดยผลการประเมินความถูกต้องของการจับคู่ความมั่นคงที่พึงจะมีกับแบบรูปการโจมตี มีดังนี้

จากการเก็บข้อมูลในแบบสอบถามพบว่าการจับคู่ความต้องการความต้องการด้านความมั่นคงที่พึงจะมีกับแบบรูปการโจมตีทั้ง 38 แบบ พบว่าผู้ประเมินส่วนใหญ่เห็นด้วยกับการจับคู่ฯ ดังภาพที่ 4.1 โดยความต้องการด้านความมั่นคงที่พึงจะมีจำนวน 45 ข้อ ผู้ประเมินส่วนใหญ่เห็นด้วยกับการจับคู่ฯ ซึ่งคิดเป็นร้อยละ 92% และจำนวน 4 ข้อ ที่ผู้ประเมินส่วนใหญ่ไม่แน่ใจในการจับคู่ฯ



ภาพที่ 4.1 ผลประเมินความถูกต้องของการจับคู่ของความมั่นคงที่พึงจะมีกับวิธีการบรรเทาการโจมตี

จากการประเมินในรายละเอียดพบว่ามีความต้องการด้านความมั่นคงที่พึงจะมีที่ผู้ประเมินมีความเห็นเป็นเอกฉันท์จำนวน 32 ข้อ ซึ่งคิดเป็นร้อยละ 65.31 และพิจารณาโดยใช้เสียงส่วนมากจำนวน 17 ข้อ ซึ่งคิดเป็นร้อยละ 34.69 ดังภาพที่ 4.2



ภาพที่ 4.2 ผลสำรวจความเหมาะสมในการจับคู่ความสัมพันธ์ระหว่างความต้องการด้านความมั่นคงที่พึงจะมีกับแบบรูปการโจมตี

โดยพบว่าความต้องการจำนวนทั้ง 17 ข้อ เป็นความต้องการด้านความมั่นคงที่พึงจะมีที่ผู้วิจัยไม่สามารถทำการหาคู่ความสัมพันธ์ระหว่างความต้องการด้านความมั่นคงที่พึงจะมีกับแบบรูปการโจมตีได้ ซึ่งเมื่อพิจารณาลงในรายละเอียดทั้ง 17 ข้อ ได้ผลดังตารางที่ 4.5

ตารางที่ 4.5 ความต้องการที่ผู้ประเมินมีความเห็นไม่ตรงกัน

หมายเลขความต้องการด้านความมั่นคงที่พึงจะมี	ผลสำรวจ					
	เหมาะสม	ร้อยละ	ไม่แน่ใจ	ร้อยละ	ไม่เหมาะสม	ร้อยละ
CBS_005	10	83.33	2	16.67	0	0.00
CBS_006	10	83.33	2	16.67	0	0.00
CBS_009	10	83.33	2	16.67	0	0.00
CBS_010	4	33.33	5	41.67	3	25.00
CBS_011	4	33.33	5	41.67	3	25.00
ATMC_002	4	33.33	6	50.00	2	16.67
ATMC_003	11	91.67	1	8.33	0	0.00
ATMC_004	11	91.67	1	8.33	0	0.00
ATMC_005	11	91.67	1	8.33	0	0.00
ATMC_006	9	75.00	3	25.00	0	0.00
IBC_002	4	33.33	6	50.00	2	16.67
IBC_003	10	83.33	2	16.67	0	0.00
IBC_004	10	83.33	2	16.67	0	0.00
IBC_005	10	83.33	2	16.67	0	0.00
IBC_006	9	75.00	3	25.00	0	0.00
IBS_010	9	75.00	3	25.00	0	0.00
IBS_019	9	75.00	3	25.00	0	0.00

จากตารางที่ 4.5 พบว่าความต้องการมี 4 ข้อ ที่ ผู้ประเมินซึ่งเป็น Security Specialist ซึ่งมีประสบการณ์สูง 3 ปี 1 คน และมากกว่า 7 ปี 2 คน และรู้จักคาเปกด้วย มีความเห็นว่าการจับคู่ยังไม่เหมาะสม โดยให้ความเห็นเพิ่มดังนี้

1. CBS_010 และ CBS_011 เป็นความต้องการเชิงหน้าที่การทำงานของระบบงาน ซึ่งอาจจะไม่สามารถจับคู่โดยตรงกับคาเปกได้ แต่สามารถจับคู่โดยการเทียบเคียงได้ โดยผู้ประเมินให้ความเห็นว่าควรจะจับคู่กับแบบรูปการโจมตีหมายเลข 1 จึงจะเหมาะสมมากกว่า

2. ATMC_002 และ IBC_002 ซึ่งเป็นความต้องการที่เหมือนกัน แต่อยู่ในหมวดความต้องการด้านความมั่นคงที่พึงจะมีที่แตกต่างกันเท่านั้น ทั้งคู่เป็นความต้องการเชิงหน้าที่การทำงานของ

ระบบงาน เช่นเดียวกับข้อ 1 จึงควรจะจับคู่กับแบบรูปการโจมตีเช่นเดียวกับข้อ ATMC_001 และ IBC_001 ตามลำดับ เนื่องจากความต้องการดังกล่าว เป็นความต้องการที่ต่อเนื่องมาจาก ATMC_001 และ IBC_001

ผู้วิจัยจึงทำการปรับการจับคู่กับแบบรูปการโจมตีสำหรับหมายเลขความต้องการด้านความมั่นคงที่พึงจะมี CBS_010, CBS_011, ATMC_002 และ IBC_002 ตามความเห็นดังกล่าว

สำหรับผลสำรวจที่ผู้ประเมินให้ความเห็นเป็นไม่แน่ใจนั้น ทางผู้วิจัยได้สอบถามย้อนกลับถึงสาเหตุ โดยได้รับคำตอบเป็นดังนี้

1. ไม่ค่อยเข้าใจ และความรู้ในเรื่อง Attack Pattern ของผู้กรอกยังมีน้อย
2. ไม่มีความรู้ในเรื่องของแบบรูปการโจมตีมากนัก
3. ผู้วิจัยไม่ได้แสดงเหตุผลที่ไม่สามารถจับคู่กับแบบรูปการโจมตีได้
4. อาจจะมีแบบรูปการโจมตีขององค์กรอื่น หรืออะไรที่คล้ายกัน สามารถนำมาใช้ในงานวิจัยได้

ในส่วนนี่ผู้วิจัยเห็นสมควรให้ใช้ค่าเดิมที่ผู้วิจัยนำเสนอ เนื่องจากความเห็นไม่แน่ใจดังกล่าวไม่สามารถนำไปสู่การปรับการจับคู่แบบรูปการโจมตีได้

4.2 การประเมินประสิทธิภาพของการหาความแตกต่างระหว่างความต้องการด้านความมั่นคงที่พึงจะมีกับเอกสารความต้องการด้านความมั่นคงของการธนาคาร

ในการประเมินประสิทธิภาพของการหาความแตกต่างระหว่างความต้องการด้านความมั่นคงที่พึงจะมีกับเอกสารความต้องการด้านความมั่นคงของการธนาคาร ผู้วิจัยได้ใช้เอกสารความต้องการของระบบสารสนเทศของธนาคารพาณิชย์ 9 เอกสาร เพื่อประเมินว่าเครื่องมือที่พัฒนาขึ้นสามารถระบุความต้องการด้านความมั่นคงที่พึงจะมีที่หายไปจากเอกสารความต้องการด้านความมั่นคงของการธนาคารได้อย่างไร โดยเครื่องมือจะคำนวณคะแนนความแตกต่างของคู่ความต้องการด้านความมั่นคงที่พึงจะมีและความต้องการด้านความมั่นคงของการธนาคารที่ตรงกันที่สุด และกำหนดว่าความต้องการด้านความมั่นคงที่พึงจะมีนั้นพบหรือขาดหายไปโดยใช้เกณฑ์ (ค่าขีดแบ่ง) โดยผลการทำนายที่ได้จากเครื่องมือจะนำไปทวนสอบกับผลเฉลยจากการตรวจประเมินของผู้ตรวจสอบ (Auditor) ซึ่งมีอยู่แล้ว โดยวัดประสิทธิภาพโดยค่าเอฟ-เมเชอร์ (F-measure) ดังสมการที่ (4.1) และค่าความแม่น (Accuracy) ดังสมการที่ (4.2)

$$F\text{-}measure = \frac{2 * Precision * Recall}{Precisio + Recall} \quad (4.1)$$

โดยที่ *Precision* คือ $\frac{True\ Positive}{True\ Positive + False\ Positive} * 100$

Recall คือ $\frac{True\ Positive}{True\ Positive + False\ Negative} * 100$

และ $$Accuracy = \frac{\sum True\ Positive + \sum True\ Negative}{Number\ of\ SSRB} * 100 \quad (4.2)$$

เมื่อ *True Positive* คือ ผลการทำนายของเครื่องมือว่าจริง และผลเฉลยบอกว่าจริง

True Negative คือ ผลการทำนายของเครื่องมือว่าไม่จริง และผลเฉลยบอกว่าไม่จริง

False Negative คือ ผลการทำนายของเครื่องมือว่าจริง แต่ผลเฉลยบอกว่าไม่จริง

False Negative คือ ผลการทำนายของเครื่องมือว่าไม่จริง แต่ผลเฉลยบอกว่าจริง

ตารางที่ 4.6 และ 4.7 แสดงประสิทธิภาพของเครื่องมือในการทำนายว่าความต้องการที่พึงจะมีข้อใดขาดหายไป (Missing) หรือไม่ขาดหายไป (Not Missing) จากรายการความต้องการของธนาคารบ้าง โดยวัดค่าเอฟ-เมเชอร์ของการทำนายว่าขาดหายไปและไม่ขาดหายไปตามลำดับ ส่วนตารางที่ 4.8 แสดงประสิทธิภาพของเครื่องมือในแง่ความแม่น ภาพที่ 4.3 แสดงผลการทดลองรูปของกราฟค่าเฉลี่ย

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

ตารางที่ 4.6 ค่าเอฟเมเชอร์ของการทำนายความต้อ-งการด้านความมั่นคงที่พึงจะมีที่ขาดหายไป

ค่าขีดแบ่ง	หมายเลขเอกสาร								
	Doc_1	Doc_2	Doc_3	Doc_4	Doc_5	Doc_6	Doc_7	Doc_8	Doc_9
0.05	52.17	80.00	11.11	50.00	83.87	57.14	66.67	57.14	40.00
0.10	60.00	82.76	13.33	54.55	86.67	61.54	66.67	61.54	40.00
0.15	70.59	85.71	14.29	57.14	89.66	61.54	66.67	61.54	45.45
0.20	80.00	88.89	16.67	63.16	92.86	61.54	66.67	61.54	52.63
0.25	85.71	92.31	20.00	66.67	92.86	66.67	76.92	50.00	55.56
0.30	92.31	92.31	22.22	77.78	96.55	66.67	76.92	54.55	71.43
0.35	100.00	92.31	25.00	75.00	92.86	66.67	76.92	60.00	76.92
0.40	100.00	92.31	40.00	80.00	96.30	66.67	76.92	60.00	100.00
0.45	100.00	96.00	66.67	92.31	96.30	72.73	76.92	60.00	75.00

ตารางที่ 4.6 ค่าเอฟ-เมเชอร์ของการทำนายความต้องการด้านความมั่นคงที่พึงจะมีที่ขาดหายไป (ต่อ)

ค่าขีดแบ่ง	หมายเลขเอกสาร								
	Doc_1	Doc_2	Doc_3	Doc_4	Doc_5	Doc_6	Doc_7	Doc_8	Doc_9
0.50	90.91	100.00	100.00	92.31	96.30	72.73	90.91	60.00	75.00
0.55	80.00	95.65	100.00	92.31	96.30	60.00	90.91	44.44	75.00
0.60	66.67	80.00	100.00	92.31	88.00	50.00	90.91	50.00	33.33
0.65	66.67	58.82	100.00	80.00	78.26	57.14	80.00	57.14	33.33
0.70	66.67	50.00	100.00	66.67	78.26	57.14	66.67	57.14	33.33
0.75	50.00	40.00	100.00	N/A	63.16	40.00	66.67	N/A	N/A
0.80	28.57	40.00	100.00	N/A	55.56	40.00	50.00	N/A	N/A
0.85	28.57	15.38	N/A	N/A	26.67	N/A	28.57	N/A	N/A
0.90	28.57	N/A	N/A	N/A	14.29	N/A	N/A	N/A	N/A
0.95	28.57	N/A	N/A	N/A	14.29	N/A	N/A	N/A	N/A
1.00	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A

ตารางที่ 4.7 ค่าเอฟ-เมเชอร์ของการทำนายความต้องการด้านความมั่นคงที่พึงจะมีที่ไม่ขาดหายไป

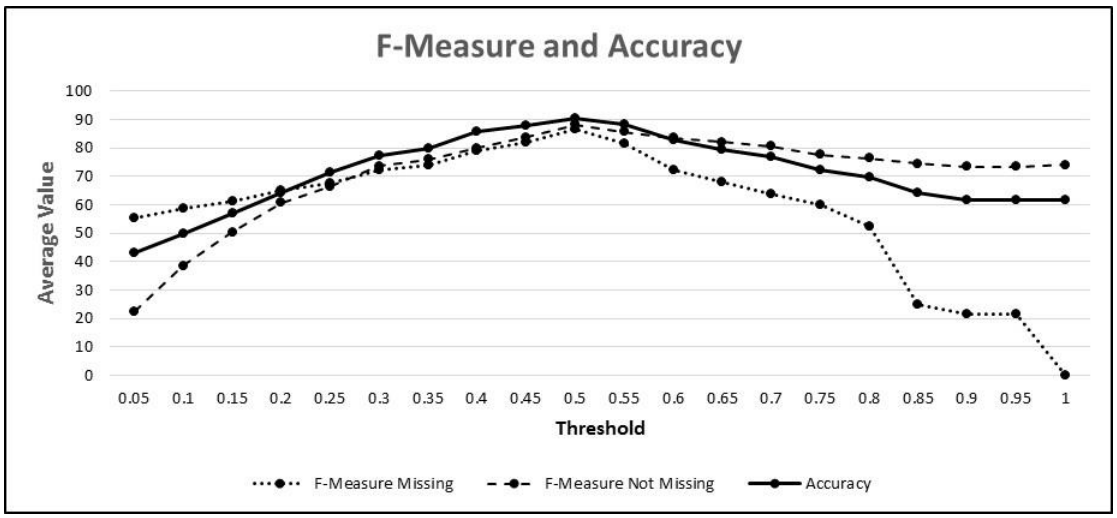
ค่าขีดแบ่ง	หมายเลขเอกสาร								
	Doc_1	Doc_2	Doc_3	Doc_4	Doc_5	Doc_6	Doc_7	Doc_8	Doc_9
0.05	26.67	25.00	20.00	14.29	28.57	0.00	0.00	0.00	21.05
0.10	55.56	44.44	43.48	37.50	50.00	28.57	0.00	28.57	21.05
0.15	76.19	60.00	50.00	47.06	66.67	28.57	0.00	28.57	45.45
0.20	86.96	72.73	61.54	63.16	80.00	28.57	0.00	28.57	64.00
0.25	91.67	83.33	71.43	70.00	80.00	50.00	57.14	25.00	69.23
0.30	96.00	83.33	75.86	80.00	88.89	50.00	57.14	44.44	86.67
0.35	100.00	83.33	80.00	81.82	80.00	50.00	57.14	60.00	90.32
0.40	100.00	83.33	90.91	86.96	90.91	50.00	57.14	60.00	100.00
0.45	100.00	92.31	97.14	96.00	90.91	66.67	57.14	60.00	94.44
0.50	96.30	100.00	100.00	96.00	90.91	66.67	88.89	60.00	94.44
0.55	92.86	93.33	100.00	96.00	90.91	60.00	88.89	54.55	94.44
0.60	89.66	77.78	100.00	96.00	76.92	66.67	88.89	66.67	89.47
0.65	89.66	66.67	100.00	92.86	66.67	76.92	80.00	76.92	89.47
0.70	89.66	63.64	100.00	89.66	66.67	76.92	72.73	76.92	89.47
0.75	86.67	60.87	100.00	81.25	63.16	80.00	72.73	66.67	87.18

ตารางที่ 4.7 ค่าเอฟ-เมเชอร์ของการทำนายความต้องการด้านความมั่นคงที่พึงจะมีที่ไม่ขาดหายไป (ต่อ)

ค่าขีดแบ่ง	หมายเลขเอกสาร								
	Doc_1	Doc_2	Doc_3	Doc_4	Doc_5	Doc_6	Doc_7	Doc_8	Doc_9
0.80	83.87	60.87	100.00	81.25	60.00	80.00	66.67	66.67	87.18
0.85	83.87	56.00	97.30	81.25	52.17	75.00	61.54	75.00	87.18
0.90	83.87	53.85	97.30	81.25	50.00	75.00	57.14	75.00	87.18
0.95	83.87	53.85	97.30	81.25	50.00	75.00	57.14	75.00	87.18
1.00	81.25	53.85	97.30	81.25	48.00	75.00	66.67	75.00	87.18

ตารางที่ 4.8 ค่าความแม่นของการทำนาย

ค่าขีดแบ่ง	หมายเลขเอกสาร								
	Doc_1	Doc_2	Doc_3	Doc_4	Doc_5	Doc_6	Doc_7	Doc_8	Doc_9
0.05	42.11	68.42	15.79	36.84	73.68	40.00	50.00	28.00	31.82
0.10	57.89	73.68	31.58	47.37	78.95	50.00	50.00	28.00	31.82
0.15	73.68	78.95	36.84	52.63	84.21	50.00	50.00	40.00	45.45
0.20	84.21	84.21	47.37	63.16	89.47	50.00	50.00	52.00	59.09
0.25	89.47	89.47	57.89	68.42	89.47	60.00	70.00	56.00	63.64
0.30	94.74	89.47	63.16	73.68	89.47	60.00	70.00	72.00	81.82
0.35	100.00	89.47	68.42	78.95	89.47	60.00	70.00	76.00	86.36
0.40	100.00	89.47	84.21	84.21	94.74	60.00	70.00	88.00	100.00
0.45	100.00	94.74	94.74	94.74	94.74	70.00	70.00	80.00	90.91
0.50	94.74	100.00	100.00	94.74	94.74	70.00	90.00	80.00	90.91
0.55	89.47	94.74	100.00	94.74	94.74	60.00	90.00	80.00	90.91
0.60	84.21	78.95	100.00	94.74	84.21	60.00	90.00	72.00	81.82
0.65	84.21	63.16	100.00	89.47	73.68	70.00	80.00	72.00	81.82
0.70	84.21	57.89	100.00	84.21	73.68	70.00	70.00	72.00	81.82
0.75	78.95	52.63	100.00	68.42	63.16	70.00	70.00	68.00	77.27
0.80	73.68	52.63	100.00	68.42	57.89	70.00	60.00	68.00	77.27
0.85	73.68	42.11	94.74	68.42	42.11	60.00	50.00	68.00	77.27
0.90	73.68	36.84	94.74	68.42	36.84	60.00	40.00	68.00	77.27
0.95	73.68	36.84	94.74	68.42	36.84	60.00	40.00	68.00	77.27
1.00	68.42	36.84	94.74	68.42	31.58	60.00	50.00	68.00	77.27



ภาพที่ 4.3 ค่าเฉลี่ยเอฟเมเชอร์-และค่าความแม่น

จากผลการประเมินพบว่าค่าขีดแบ่งที่จะทำให้ได้ค่าเอฟ-เมเชอร์ของการทำนายว่าขาดหายไปที่ประมาณ 80% นั้นอยู่ที่ 0.4 และจะได้ค่าเอฟ-เมเชอร์สูงสุดเป็น 86.46% เมื่อค่าขีดแบ่งเป็น 0.5 และค่าความแม่นถึง 90.56% ซึ่งเป็นค่าที่สูงที่เครื่องมือสามารถประเมินได้จากเอกสารตัวอย่างทั้ง 9 เอกสาร

จากการวิเคราะห์กราฟในภาพที่ ช่วงดังนี้ 3 จะสามารถแบ่งค่าขีดแบ่งได้เป็น 4.3

ช่วงที่ 1 คือ 0.00 ถึง 0.39 เป็นช่วงที่เครื่องมือจะให้ประสิทธิภาพต่ำกว่า 80%

ช่วงที่ 2 คือ 0.40 ถึง 0.50 เป็นช่วงที่เครื่องมือให้ประสิทธิภาพสูง ตั้งแต่ 80%-90%

ช่วงที่ 3 คือ 0.51 ถึง 1.00 เป็นช่วงที่ประสิทธิภาพของเครื่องมือเริ่มลดลง โดยสามารถแบ่งย่อยได้อีก 2 ช่วงคือ

0.51 ถึง 0.65 เป็นช่วงที่ประสิทธิภาพยังคงมากกว่า 80% แต่ในช่วงนี้จะทำให้เกิดความผิดพลาดที่ไม่สามารถยอมรับได้ (Type II Error) เนื่องจากจะทำให้เกิดรายการความต้องการด้านความมั่นคงที่พึงจะมีที่ขาดหายไป แต่เครื่องมือทำนายว่าพบความต้องการด้านความมั่นคงที่พึงจะมีนั้น (Flase Negative)

0.66 ถึง 1.00 เป็นช่วงที่เครื่องมือจะให้ประสิทธิภาพต่ำกว่า 80%

เมื่อพิจารณาในรายละเอียดของผลเฉลยจากการตรวจประเมินของผู้ตรวจสอบ ซึ่งมีอยู่แล้วและความแตกต่างของเอกสารที่วัดได้โดยเครื่องมือ สำหรับเอกสารที่นำเข้ามาประเมินทั้ง 9 เอกสาร ดังตารางที่ 4.9 จะพบว่าค่าขีดแบ่งที่น้อยที่สุด ที่จะเริ่มทำให้เกิดความผิดพลาดที่ไม่สามารถยอมรับได้ (False Nagative) คือค่าขีดแบ่งที่ 0.54 (จากเอกสารที่ 1, 2, 6 และ 8)

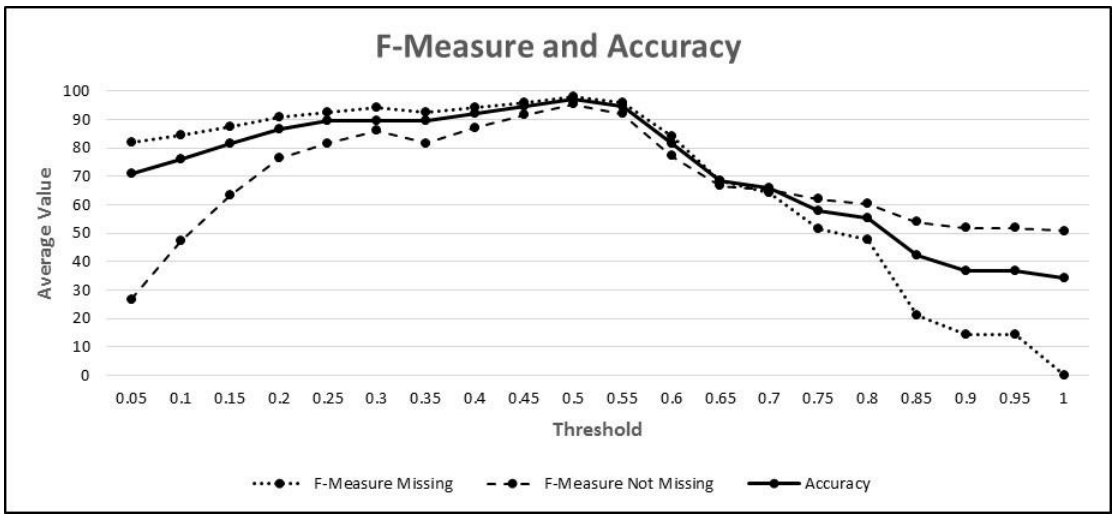
ตารางที่ 4.9 ค่าความแตกต่างและค่าผลเฉลย ของการจับคู่เอกสารความต้องการด้านความมั่นคงของธนาคารกับความต้องการที่พึงจะมี

ค่าความแตกต่างและค่าผลเฉลย																	
Doc_1		Doc_2		Doc_3		Doc_4		Doc_5		Doc_6		Doc_7		Doc_8		Doc_9	
0.13	NM	0.14	NM	0.00	NM	0.18	NM	0.00	NM	0.65	NM	0.24	NM	0.06	NM	0.59	M
0.76	M	0.55	M	0.40	NM	0.65	NM	0.55	M	0.06	NM	0.63	M	0.59	NM	0.18	NM
0.08	NM	0.16	NM	0.25	NM	0.40	NM	0.16	NM	0.59	M	0.84	M	0.54	M	0.29	NM
0.14	NM	0.25	NM	0.14	NM	0.14	NM	0.14	NM	0.54	M	0.76	M	0.71	M	0.33	NM
1.00	M	0.62	M	0.82	M	0.75	M	0.62	M	0.71	M	0.68	M	0.21	M	0.43	M
0.08	NM	0.80	M	0.08	NM	0.21	NM	0.86	M	0.21	NM	1.00	NM	0.82	NM	0.43	M
0.54	M	0.07	NM	0.00	NM	0.43	NM	0.73	NM	0.82	M	0.23	NM	0.72	M	0.00	NM
0.04	NM	0.00	NM	0.08	NM	0.08	NM	0.73	M	0.72	NM	0.50	NM	0.33	NM	0.00	NM
0.09	NM	0.55	M	0.20	NM	0.20	NM	0.58	M	0.58	NM	0.50	NM	0.65	NM	0.27	NM
0.13	NM	0.71	M	0.33	NM	0.00	NM	0.82	M	0.44	NM	0.89	M	0.29	NM	0.16	NM
0.27	NM	0.54	M	0.36	NM	0.36	NM	0.36	NM							0.27	NM
0.15	NM	0.49	NM	0.43	NM	0.62	M	0.71	M							0.14	NM
0.20	NM	0.63	M	0.09	NM	0.09	NM	0.09	NM							0.71	M
0.33	NM	0.62	M	0.48	NM	0.62	M	0.62	M							0.13	NM
0.00	NM	0.40	NM	0.38	NM	0.33	NM	0.78	M							0.29	NM
0.24	NM	0.82	M	0.24	NM	0.28	NM	0.82	M							0.13	NM
0.54	M	0.59	M	0.18	NM	0.71	M	0.74	M							0.23	NM
0.55	M	0.67	M	0.25	NM	0.70	M	1.00	M							0.40	NM
0.73	M	0.88	M	0.37	NM	0.73	M	0.82	M							0.38	NM
																0.38	NM
																0.60	M
																0.15	NM

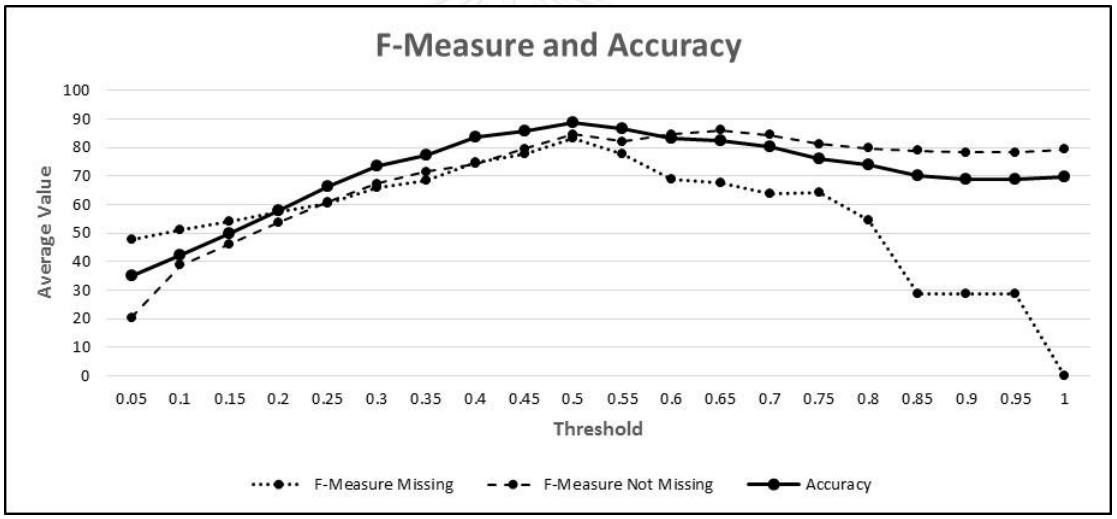
หมายเหตุ: NM=ไม่ขาดหาย (Not Missing), M=ขาดหาย (Missing)

นอกจากนี้ยังพบว่าความต้องการด้านความมั่นคงของธนาคาร ในเอกสารที่ 2 และ 5 นั้น จะได้ค่าเอฟ-เมเชอร์ทั้งในส่วนการทำนายความต้องการด้านความมั่นคงที่พึงจะมีที่ไม่ขาดหายไปและที่ขาดหายไป และค่าความแม่น มีค่าสูงกว่าเอกสารอื่น ตามข้อมูลในตารางที่ 4.6 – 4.8

จากภาพที่ 4.4 แสดงเฉลี่ยของค่าเอฟ-เมเชอร์และค่าความแม่นของเอกสารที่ 2 และ 5 ซึ่งจะพบว่าค่า เฉลี่ยของค่าเอฟ-เมเชอร์ของการทำนายความต้องการด้านความมั่นคงที่พึงจะมีที่ขาดหายไปและค่าความแม่น มีค่าสูงกว่าเอกสารอื่น ซึ่งแสดงในภาพที่ 4.5 อันมีสาเหตุมาจากรายการความต้องการด้านความมั่นคงที่พึงจะมีส่วนมากจะมีการระบุ ข้อความ หรือวิธีการที่ใช้คำทางเทคนิคมากกว่า ซึ่งในเอกสารที่ 2 และ 5 ก็มีการใช้คำทางเทคนิค ตัวอย่างเปรียบเทียบ เช่น



ภาพที่ 4.4 ค่าเฉลี่ยค่าเอฟ-เมเชอร์และค่าความแม่นของเอกสารที่ 2 และ 5



ภาพที่ 4.5 ค่าเฉลี่ยค่าเอฟ-เมเชอร์และค่าความแม่นของเอกสารที่อื่น

รายการความต้องการด้านความมั่นคงที่พึงจะมี:

“The system shall encrypt confidential information (e.g. user ID, password encryption key, database user id, database password) by strong encryption (e.g. AES 128 bits, AES 256 bits, RSA 2048).”

รายการความต้องการด้านความมั่นคงของธนาคาร:

เอกสารที่ 1

"The application shall apply strong encryption to encrypt confidential information and store in a database or configuration file with appropriate access control"

เอกสารที่ 5

"The application shall use AES 256 bits encryption to encrypt system user id, password, database user id, and password before storing those hashes in a configuration file"

จากรายการความต้องการข้างต้น จะพบว่าเอกสารที่ 5 มีโอกาสที่คะแนนความแตกต่าง จะน้อยกว่าเอกสารที่ 1 เนื่องจากมีการใช้คำทางเทคนิคร่วมด้วยคือ AES 256 bits ซึ่งส่งผลให้มีความสอดคล้องกับความต้องการด้านความมั่นคงที่พึงจะมีมากกว่าเอกสารที่ 1 ทั้งนี้ค่าเอฟ-เมเซอร์ของการทำนายความต้องการด้านความมั่นคงที่พึงจะมีที่ขาดหายไป และค่าความแม่น นั้นจะเริ่มต้นด้วยค่าที่ค่อนข้างต่ำ โดยจะมีค่าเอฟ-เมเซอร์และค่าความแม่นที่มากกว่า 80% ตั้งแต่ค่าขีดแบ่งที่ 0.15 เป็นต้นไป จนถึง 0.50 ดังแสดงในภาพที่ 4.4 และสำหรับรายการความต้องการที่ไม่ได้ระบุคำทางเทคนิคมากนักจะเริ่มที่ 0.4 ถึง 0.50 ดังแสดงในภาพที่ 4.5

4.3 การประเมินความสอดคล้องของค่าความเสี่ยงของความต้องการด้านความมั่นคงที่ขาดหายไป ซึ่งได้จากเครื่องมือกับค่าความเสี่ยงจากผู้เชี่ยวชาญ

ผู้วิจัยทำการประเมินความสอดคล้องของค่าความเสี่ยงของความต้องการด้านความมั่นคงที่พึงจะมีที่ขาดหายไป โดยการทวนสอบผลที่ได้จากเครื่องมือเมื่อใช้ค่าขีดแบ่งที่ 0.5 กับค่าความเสี่ยงจากผู้เชี่ยวชาญที่ได้จากการรวบรวมดังในภาคผนวก ข ตารางที่ 4.10 แสดงค่าดัชนีความเสี่ยงที่ได้จากเครื่องมือ

ตารางที่ 4.10 ดัชนีความเสี่ยงของความต้องการด้านความมั่นคงที่พึงจะมีที่ขาดหายไปจากแต่ละเอกสารความต้องการของธนาคารที่ค่าขีดแบ่ง 0.5

ดัชนีความเสี่ยงในแต่ละเอกสาร								
Doc_1	Doc_2	Doc_3	Doc_4	Doc_5	Doc_6	Doc_7	Doc_8	Doc_9
0.00	0.00	0.00	0.00	0.00	16.23	0.00	0.00	9.47
3.03	2.21	0.00	2.60	2.21	0.00	15.87	14.79	0.00
0.00	0.00	0.00	0.00	0.00	5.33	7.53	4.84	0.00

ตารางที่ 4.10 ดัชนีความเสี่ยงของความต้องการด้านความมั่นคงที่พึงจะมีที่ขาดหายไปจากแต่ละเอกสารความต้องการของธนาคารที่ค่าขีดแบ่ง 0.5 (ต่อ)

ดัชนีความเสี่ยงในแต่ละเอกสาร								
Doc_1	Doc_2	Doc_3	Doc_4	Doc_5	Doc_6	Doc_7	Doc_8	Doc_9
0.00	0.00	0.00	0.00	0.00	4.84	6.88	6.40	0.00
16.00	9.95	13.17	12.00	9.95	6.40	6.08	0.00	0.00
0.00	9.65	0.00	0.00	10.34	0.00	9.00	7.36	0.00
6.45	0.00	0.00	0.00	8.79	6.54	0.00	5.76	0.00
0.00	0.00	0.00	0.00	8.73	11.52	0.00	0.00	0.00
0.00	8.84	0.00	0.00	9.21	9.34	0.00	10.39	0.00
0.00	6.40	0.00	0.00	7.36	0.00	0.00	0.00	0.00
0.00	13.45	0.00	0.00	0.00				0.00
0.00	0.00	0.00	15.55	17.86				0.00
0.00	10.16	0.00	0.00	0.00				8.57
0.00	5.60	0.00	5.60	5.60				0.00
0.00	0.00	0.00	0.00	12.42				0.00
0.00	20.52	0.00	0.00	20.55				0.00
0.00	9.47	0.00	11.38	11.87				0.00
8.84	10.67	0.00	11.18	16.00				0.00
6.59	7.94	0.00	6.59	7.41				0.00
								0.00
								12.00
								0.00

จากตารางที่ 4.10 สามารถหาดัชนีความเสี่ยงสำหรับแต่ละเอกสารความต้องการด้านความมั่นคงของธนาคาร โดยใช้ค่าความเสี่ยงสูงสุดในเอกสารนั้นๆ เป็นตัวแทนตามหลักการไฮวอร์เทอร์มาร์ค และจับคู่กับผลสำรวจระดับความเสี่ยงของแต่ละรายการความต้องการด้านความมั่นคงที่พึงจะมีที่ได้จากผู้เชี่ยวชาญ ดังในภาคผนวก ข ผลการจับคู่เป็นดังตารางที่ 4.11 ทั้งนี้ค่าดัชนีความเสี่ยงจะถูกปรับเป็นค่ามาตราอันดับ (Oridinal Scale) ในช่วง 1-5 ตามตารางที่ 4.12 และ 4.13 สำหรับการประเมินความสอดคล้องโดยการวิเคราะห์สหสัมพันธ์

ตารางที่ 4.11 ดัชนีความเสี่ยงในแต่ละเอกสารความต้องการด้านความมั่นคงของธนาคารและผลสำรวจระดับความเสี่ยงในแต่ละเอกสารจากผู้เชี่ยวชาญ

ลำดับที่เอกสารความต้องการ	ระดับความเสี่ยงจากผู้เชี่ยวชาญ		ดัชนีความเสี่ยงจากเครื่องมือ	
	ดั้งเดิม	ใหม่	ดั้งเดิม	ใหม่
1	High	4	16.00	4
2	Very High	5	20.52	5
3	High	4	13.17	3
4	Very High	5	15.55	4
5	Very High	5	20.55	5
6	Very High	5	16.23	4
7	Medium	3	15.87	4
8	Medium	3	14.79	3
9	Low	2	12.00	3

ตารางที่ 4.12 การเปลี่ยนค่าระดับความเสี่ยงจากผู้เชี่ยวชาญ

ระดับความเสี่ยงจากผู้เชี่ยวชาญ	
ดั้งเดิม	ใหม่
Very Low	1
Low	2
Medium	3
High	4
Very High	5

ตารางที่ 4.13 การเปลี่ยนค่าดัชนีความเสี่ยงจากเครื่องมือ

ดัชนีความเสี่ยงจากเครื่องมือ	
ดั้งเดิม	ใหม่
มากกว่า 0.00 ถึง 5.00	1
มากกว่า 5.00 ถึง 10.00	2
มากกว่า 10.00 ถึง 15.00	3
มากกว่า 15.00 ถึง 20.00	4
มากกว่า 20.00 ถึง 25.00	5

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

จากข้อมูลในตารางที่ 4.11 ผู้วิจัยได้ทำการตรวจสอบความสอดคล้องของค่าความเสี่ยงระหว่างผู้เชี่ยวชาญ และเครื่องมือ โดยใช้สัมประสิทธิ์สหสัมพันธ์แบบลำดับที่ของสเปียร์แมน (Spearman's rank order correlation) โดยมีกำหนดสมมติฐานดังนี้

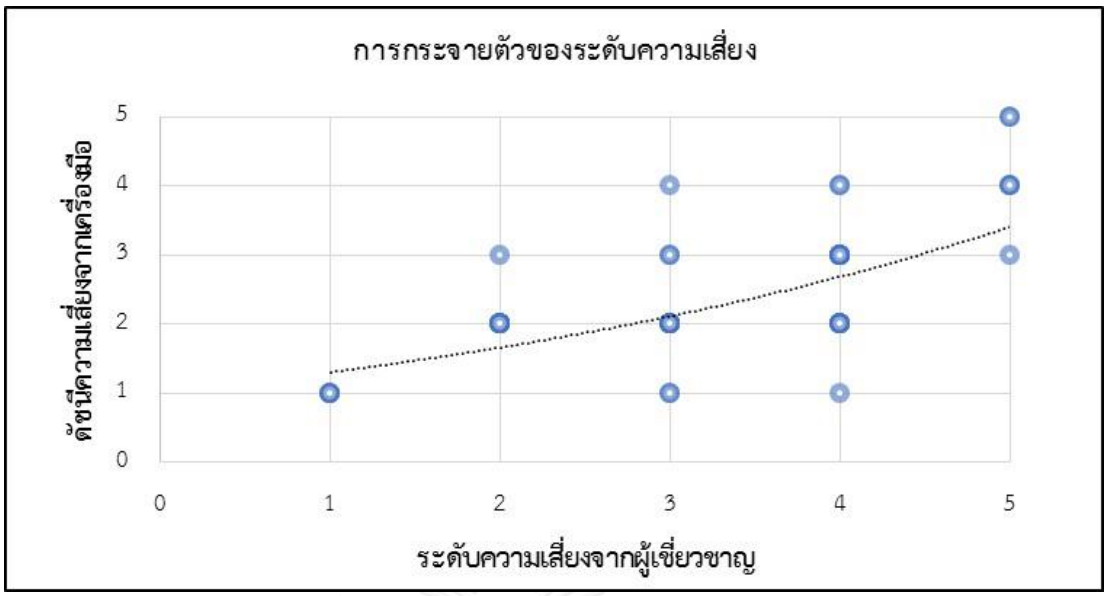
สมมติฐาน:

H_0 : ไม่มีความสัมพันธ์กันระหว่างระดับความเสี่ยงที่ได้จากผู้เชี่ยวชาญและเครื่องมือ (ρ_s=0)

H_1 : มีความสัมพันธ์กันระหว่างระดับความเสี่ยงที่ได้จากผู้เชี่ยวชาญและเครื่องมือ ($\rho_s \neq 0$)

ค่าสัมประสิทธิ์สหสัมพันธ์ของทั้ง 9 เอกสาร คือ 0.74186 ซึ่งมีค่ามากกว่าสัมประสิทธิ์สหสัมพันธ์วิกฤตคือ 0.618 ที่ระดับนัยสำคัญทางสถิติเท่ากับ 0.05 [19] ดังนั้นเราจึงปฏิเสธ H_0 และยอมรับ H_1 คือค่าระดับความเสี่ยงจากผู้เชี่ยวชาญและเครื่องมือมีความสัมพันธ์กัน ที่ระดับนัยสำคัญทางสถิติเท่ากับ 0.05 โดยจากค่าสัมประสิทธิ์สหสัมพันธ์ที่ได้ สรุปได้ว่ามีความสัมพันธ์สอดคล้องกันในเชิงบวกในระดับสูง

ทั้งนี้เมื่อผู้วิจัยได้ตรวจสอบลงในระดับความต้องการด้านความมั่นคงที่พึงจะมีที่ขาดหายไปของทั้ง 9 เอกสาร ซึ่งเครื่องมือสามารถตรวจจับได้ 61 รายการ แล้วนำมาวิเคราะห์สหสัมพันธ์แบบลำดับที่ของสเปียร์แมนเพิ่มเติมกับระดับความเสี่ยงจากผู้เชี่ยวชาญ พบว่าค่าสัมประสิทธิ์สหสัมพันธ์ที่ได้คือ 0.63824 ซึ่งมีค่ามากกว่าสัมประสิทธิ์สหสัมพันธ์วิกฤตคือ 0.252 ที่ระดับนัยสำคัญทางสถิติเท่ากับ 0.05 จึงปฏิเสธ H_0 และยอมรับ H_1 เช่นเดียวกัน ดังนั้นจึงสามารถสรุปได้ว่า ค่าความเสี่ยงของความต้องการด้านความมั่นคงที่พึงจะมีที่ขาดหายไปซึ่งได้จากเครื่องมือกับค่าความเสี่ยงจากผู้เชี่ยวชาญมีความสอดคล้องกันในเชิงบวกในระดับสูง ดังแสดงในภาพที่ 4.6



ภาพที่ 4.6 การกระจายตัวของคู่ความสัมพันธ์สำหรับระดับความเสี่ยงของรายการความต้องการด้านความมั่นคงที่พึงจะมีที่ขาดหายไป 61 รายการ

4.4 การวิเคราะห์ต้นทุนและผลประโยชน์

จากผลการสำรวจค่าใช้จ่ายในการประเมินความเสี่ยงด้านความมั่นคงของรายการความต้องการของธนาคารซึ่งดำเนินการอยู่ในปัจจุบัน ตามตารางที่ ข.2 ซึ่งทำโดยผู้เชี่ยวชาญที่มีประสบการณ์ในการทำงานด้านความมั่นคงและมีส่วนร่วมในการประเมินความเสี่ยงจำนวน 9 ราย โดยสามารถสรุปภาพรวมข้อมูลของผู้ประเมินได้ดังตารางที่ 4.14

ตารางที่ 4.14 บทบาทหน้าที่ในการประเมินความเสี่ยง

ส่วนร่วมในการประเมินฯ	จำนวนผู้ทำการประเมิน	ร้อยละ
ผู้บริหารจัดการ	6	66.67
ผู้ดำเนินการ	3	33.33

จากผลการสำรวจ จะได้ค่าใช้จ่ายเฉลี่ยอยู่ที่ 31,333 บาทต่อโครงการ และระยะเวลาในการดำเนินการเฉลี่ย 1.33 วันต่อโครงการ และจะได้ค่าใช้จ่ายต่อวันจำนวน 23,558.65 บาท/วัน

เมื่อคำนวณค่าใช้จ่ายในการดำเนินการตามแบบจำลอง ซึ่งใช้ระยะเวลาประมาณการโดยผู้วิจัยตลอดระยะเวลาในการทำวิจัยในแต่ละขั้นตอนจะได้ผลดังตารางที่ 4.15

ตารางที่ 4.15 ระยะเวลาในการพัฒนาเครื่องมือตามแบบจำลอง

ประเภทค่าใช้จ่าย	กิจกรรม	ระยะเวลา (วัน)
พัฒนาเครื่องมือ	รวบรวมความต้องการที่พึงจะมี	5
พัฒนาเครื่องมือ	รวบรวมแบบรูปการโจมตี	5
พัฒนาเครื่องมือ	จับคู่ความต้องการที่พึงจะมีกับแบบรูปการโจมตีที่รวบรวมมาได้และประเมินการจับคู่ฯ	25
พัฒนาเครื่องมือ	พัฒนาเครื่องมือ (รวมการสร้างไฟล์ XML)	10
ใช้งานเครื่องมือ	จัดเตรียมเอกสารความต้องการของธนาคาร	0.5
ใช้งานเครื่องมือ	ดำเนินการประเมินความเสี่ยงด้วยเครื่องมือ	0.125

จากตารางที่ 4.15 ผู้วิจัยใช้เวลาในการดำเนินการพัฒนาเครื่องมือทั้งสิ้น 45 วัน ซึ่งเมื่อพิจารณาเป็นมูลค่าทางการเงิน โดย 1 วันมีมูลค่า 1,833.33 บาท (55,000/30) ซึ่งเป็นอัตราค่าตอบแทนรายเดือนสำหรับวิศวกรความมั่นคงที่มีประสบการณ์ 3-5 ปี [20] จะได้ค่าใช้จ่ายในการดำเนินการพัฒนาตามแบบจำลองทั้งสิ้น 82,499.85 บาท (45*1,833.33) นอกจากนี้ยังมีค่าใช้จ่ายในการใช้งานเครื่องมือตามแบบจำลองซึ่งเกิดจากขั้นตอนการจัดเตรียมเอกสารความต้องการของธนาคารและดำเนินการประเมินความเสี่ยงด้วยเครื่องมือ คิดเป็นเงิน 1,145.83 ((0.5+0.125)*1,833.33) ซึ่งเมื่อพิจารณาจุดคุ้มทุนในการใช้งานแบบจำลองทดแทนวิธีการเดิมที่ใช้วิธีการทวนสอบโดยปราศจากเครื่องมือ จะคุ้มค่าเมื่อเครื่องมือถูกนำไปใช้งานจำนวน 3 โครงการเป็นต้นไป ดังรายละเอียดในตารางที่ 4.16

ตารางที่ 4.16 จุดคุ้มทุนในการใช้งานเครื่องมือเทียบกับวิธีเดิม

โครงการลำดับที่	1	2	3	4
เครื่องมือ				
ค่าใช้จ่ายเริ่มในการพัฒนาเครื่องมือ	82,499.85	-	-	-
ค่าใช้จ่ายจากการใช้งานเครื่องมือ	1,145.83	1,145.83	1,145.83	1,145.83
ค่าใช้จ่ายสะสม	83,646.68	84,792.51	85,938.34	87,084.17
วิธีเดิม				
ค่าใช้จ่ายวิธีเดิม	31,333.00	31,333.00	31,333.00	31,333.00
ค่าใช้จ่ายวิธีเดิมสะสม	31,333.00	62,666.00	93,999.00	125,332.00
ค่าใช้จ่ายเครื่องมือสะสม - ค่าใช้จ่ายวิธีเดิมสะสม	52,313.68	22,126.51	-8,060.66	-38,247.83

บทที่ 5
บทสรุป

ในบทนี้จะกล่าวถึงสรุปผลการวิจัย ปัญหาและข้อจำกัดที่พบจากการวิจัย และข้อเสนอแนะจากการเสนอการประเมินความเสี่ยงของความต้องการด้านความมั่นคงของระบบสารสนเทศทางการธนาคารโดยอิงแบบรูปการโจมตี

5.1 สรุปผลการวิจัย

งานวิจัยนี้ได้นำเสนอการสร้างแบบจำลองการประเมินความเสี่ยงด้านความมั่นคงของระบบสารสนเทศทางการธนาคาร เพื่อประเมินให้เห็นถึงระดับความเสี่ยงของระบบสารสนเทศทางการธนาคารตั้งแต่กระบวนการกำหนดความต้องการด้านความมั่นคง นำเสนอวิธีการเป็นการรวมองค์ความรู้ในส่วนของรายการความต้องการความต้องการด้านความมั่นคงที่พึงจะมี ที่นำเสนอโดยธนาคารแห่งประเทศไทย และแบบรูปการโจมตีที่นำเสนอโดยคาเปก มาทำการพิจารณาหาความสัมพันธ์และทำการวัดผลอยู่ในรูปของดัชนีความเสี่ยง อีกทั้งได้นำแบบจำลองนี้มาพัฒนาเป็นเครื่องมือสนับสนุนที่เห็นเป็นรูปธรรม ซึ่งช่วยให้ผู้ประเมินความเสี่ยง สามารถนำผลการประเมินความเสี่ยงและความรู้จากการใช้งานแบบจำลองไปเป็นแนวทางในกำหนดความต้องการด้านความมั่นคงที่เหมาะสมกับโครงการต่างๆ ภายในธนาคาร เพื่อให้สอดคล้องกับแนวปฏิบัติที่ดี และกระตุ้นให้ธนาคาร มีความสนใจและตระหนักถึงประเด็นความเสี่ยงในการขาดหายไปของรายการความต้องการที่พึงจะมี รวมทั้งผู้ประเมินอาจนำค่าความเสี่ยงที่ได้แจ้งต่อธนาคารแห่งประเทศไทยเพื่อเป็นข้อมูลประกอบการพิจารณาในการตรวจสอบ หลักการของแบบจำลองนี้สามารถนำไปประยุกต์ใช้ในการประเมินความเสี่ยงในด้านอื่นๆ หรือขยายแบบจำลองให้รองรับการประเมินความเสี่ยงในบริบทที่มากขึ้นได้

จากการทดสอบพบว่าแบบจำลองและเครื่องมือสนับสนุนที่ได้ออกแบบไว้สามารถนำไปประยุกต์ใช้งานได้จริง โดยได้ทดลองกับเอกสารความต้องการด้านความมั่นคง และทำแบบสอบถามเพื่อประเมินความถูกต้องของการจับคู่ของความมั่นคงที่พึงจะมีกับวิธีการบรรเทาการโจมตี และสำรวจความเห็นต่อความเสี่ยงของการขาดหายไปของความต้องการด้านความมั่นคงที่พึงจะมี โดยได้ผลตอบรับที่ดีจากการวิศวกรความมั่นคง ดังในภาคผนวก ข นอกจากนี้ยังได้ทำการวิเคราะห์หาต้นทุนและผลประโยชน์จากการใช้งานเครื่องมือ ซึ่งสามารถสรุปได้เป็น 4 ส่วนดังนี้

5.1.1 ผลสรุปความถูกต้องของการจับคู่ของความมั่นคงที่พึงจะมีกับวิธีการบรรเทาการโจมตีและความต้องการด้านความมั่นคงที่เกี่ยวข้อง

จากจำนวนความต้องการที่พึงจะมีที่ผ่านการจับคู่กับแบบรูปการโจมตีทั้งหมด พบว่ามีจำนวน 32 รายการที่มีความเหมาะสม และได้รับคะแนนเสียงเป็นเอกฉันท์คิดเป็นร้อยละ 65.31, มีจำนวน 13 รายการ ที่มีความเหมาะสมแต่มีผู้ประเมินบางส่วนเห็นว่าไม่แน่ใจในการจับคู่ คิดเป็นร้อยละ 26.53 และ มี 4 รายการที่ผู้ประเมินให้ความเห็นไม่แน่ใจเป็นเสียงส่วนใหญ่ คิดเป็นร้อยละ 8.16 จึงสรุปได้ว่าการจับคู่ของความมั่นคงที่พึงจะมีกับวิธีการบรรเทาการโจมตีนั้นค่อนข้างเหมาะสม เนื่องจากไม่มีคู่ความสัมพันธ์ใดที่เสียงส่วนใหญ่มีความเห็นว่าไม่เหมาะสม โดยผู้วิจัยได้นำผลการประเมินนี้มาปรับการจับคู่ให้เหมาะสมมากยิ่งขึ้น

5.1.2 ผลสรุปประสิทธิภาพของแบบจำลองและเครื่องมือ

จากเอกสารความต้องการด้านความมั่นคงจำนวน 9 ฉบับ ที่นำเข้าสู่เครื่องมือตามแบบจำลอง พบว่าสามารตรวจจับความต้องการที่พึงจะมีที่ขาดหายไปได้โดยมีประสิทธิภาพที่ดีที่สุดในแง่ของค่าเอฟ-เมเชอร์และค่าความแม่นที่ค่าขีดแบ่งที่ 0.5 แต่ทั้งนี้หากต้องการประสิทธิภาพที่ 80% สามารถเริ่มใช้ค่าขีดแบ่งได้ที่ระดับ 0.4 และยังพบว่าการระบุข้อความในเอกสารความต้องการด้านความมั่นคงนั้น หากใช้คำทางเทคนิคในการอธิบายหรือกำหนดวิธีการทางความมั่นคงที่จะพัฒนาอย่างชัดเจน จะส่งผลให้การตรวจหาความต้องการที่พึงจะมีที่ขาดหายไปได้มีประสิทธิภาพที่ดี โดยใช้ค่าขีดแบ่งไม่สูงมากนัก

5.1.3 ผลสรุปความสอดคล้องของค่าความเสี่ยงระหว่างเครื่องมือและผู้เชี่ยวชาญ

ในการประเมินค่าดัชนีความเสี่ยงที่ได้จากเครื่องมือ โดยใช้การเปรียบเทียบสัมประสิทธิ์สหสัมพันธ์แบบลำดับที่ของสเปียร์แมนกับระดับความเสี่ยงจากผู้เชี่ยวชาญในแต่ละรายการความต้องการด้านความมั่นคงนั้น พบว่าทั้งในระดับของเอกสารและระดับรายการความต้องการด้านความมั่นคง มีความสอดคล้องในระดับสูง จึงสามารถสรุปได้ว่าค่าดัชนีความเสี่ยงที่ได้จากเครื่องมือนั้นสามารถประมาณค่าความเสี่ยงได้อย่างเหมาะสม

5.1.4 ผลสรุปการวิเคราะห์ต้นทุนและผลประโยชน์

การวิเคราะห์ต้นทุนและผลประโยชน์ พบว่าจากการสำรวจค่าใช้จ่ายในการประเมินความเสี่ยงด้านความมั่นคงด้วยเอกสารความมั่นคงนั้น จะมีค่าใช้จ่ายเฉลี่ยโครงการละ 31,333 บาท ซึ่งเมื่อพิจารณาค่าใช้จ่ายในการพัฒนาเครื่องมือตามแบบจำลอง และการใช้งาน ซึ่งอยู่ที่ 82,499.85

บาท และมีค่าใช้จ่ายในการใช้งานแต่ละครั้งอยู่ที่ 1,145.83 บาท พบว่าการพัฒนาเครื่องมือตามแบบจำลอง จะต้องมีการนำไปใช้งานในโครงการตั้งแต่ 3 โครงการขึ้นไป ถึงจะคุ้มค่ากับการลงทุน

5.2 ปัญหาและข้อจำกัดที่พบจากการวิจัย

สามารถแบ่งเป็นประเด็นหลักๆ ได้ 2 หัวข้อ ดังนี้

5.2.1 แบบจำลองงานวิจัย

1. จำนวนแบบรูปการโจมตีที่อ้างอิงในแบบจำลองนี้อาจไม่สามารถครอบคลุมแบบรูปที่เกี่ยวข้องกับความต้องการด้านความมั่นคงที่พึงจะมี เนื่องจากว่าผู้วิจัยได้สืบค้นข้อมูลเท่าที่จะสามารถทำได้เท่านั้น โดยรวบรวมมาเพียง 38 แบบรูป จากแบบรูปการโจมตีของคาเปกทั้งหมด 542 แบบรูป
2. จากข้อมูลการจับคู่ระหว่างรายการความต้องการด้านความมั่นคงที่พึงจะมีกับแบบรูปการโจมตี พบว่ายังมีบางส่วนที่ไม่สามารถจับคู่ได้ อาจเนื่องมาจากที่ผู้วิจัยได้สืบค้นข้อมูลแบบรูปการโจมตีมาเพียง 38 แบบรูป และรวบรวมมาจากคาเปกเท่านั้น
3. ในการขยายความสามารถของเครื่องมือให้ครอบคลุมแบบรูปการโจมตีมากขึ้น จำเป็นต้องอาศัยผู้ที่มีความรู้ความเข้าใจเป็นอย่างดีในด้านความมั่นคง ความต้องการด้านความมั่นคง และแบบรูปการโจมตี
4. ในการวิเคราะห์ความต้องการด้านความมั่นคงนั้น แบบจำลองยังไม่ได้พิจารณาถึงรูปแบบของการเขียนความต้องการด้านความมั่นคงที่พึงจะมี ที่มีการใช้คำว่า shall หรือ should ในการกำหนดความต้องการ ซึ่งคำทั้งสองควรจะส่งผลที่แตกต่างกันต่อการพิจารณาความเสี่ยง

Chulalongkorn University

5.2.2 ผลการทดลองที่ได้จากการตอบแบบสอบถาม

1. ความรู้ด้านความมั่นคงและแบบรูปการโจมตีของผู้ตอบแบบสอบถามในกลุ่มตัวอย่างการทดลองไม่เท่ากัน อาจทำให้ผลการทดลองที่ได้มีความคลาดเคลื่อนจากความจริงก็เป็นได้
2. จำนวนของผู้ตอบแบบสอบถามในแต่ละกลุ่มการทดลองเมื่อมีการแบ่งตามตำแหน่งต่างๆ แล้วมีจำนวนไม่เท่ากัน เพราะมีข้อจำกัดในการหาผู้ที่จะมาตอบแบบสอบถามให้มีจำนวนในแต่ละตำแหน่งเท่ากัน

5.3 ข้อเสนอแนะ

งานวิจัยนี้สามารถพัฒนาเพิ่มเติมในหลายด้าน ดังนี้

1. ขยายแบบจำลองให้รองรับลักษณะความต้องการในโดเมนอื่นนอกเหนือไปจากด้านความมั่นคง

2. ควรมีการศึกษาแบบรูปการโจมตีจากแหล่งอื่น เพื่อนำมาประยุกต์ใช้สามารถ ให้สามารถจับคู่กับความต้องการด้านความมั่นคงที่พึงจะมีได้อย่างครบถ้วน

3. ปรับปรุงแบบจำลองให้พิจารณารูปแบบของการเขียนความต้องการด้านความมั่นคงที่พึงจะมีร่วมด้วย เช่น ควรจะให้ค่าน้ำหนักความเสี่ยงแก่ความต้องการด้านความมั่นคงที่พึงจะมีที่ถูกระบุด้วยคำว่า shall และขาดหายไป มากกว่าความต้องการที่ถูกระบุด้วยคำว่า should

4. สามารถนำแบบจำลองและเครื่องมือไปประยุกต์ใช้ได้ตั้งแต่ช่วงต้นของโครงการ โดยเริ่มตั้งแต่ขั้นตอนการกำหนดความต้องการได้เลย โดยไม่ต้องรอจนถึงขั้นตอนการตรวจสอบภายใน

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

รายการอ้างอิง

[1] The MITRE Corporation, "CAPEC - Common Attack Pattern Enumeration and Classification", [Online], 2016, Available from: https://capec.mitre.org, [5 November .[2016

[2] K. Rongrat and T.Senivongse, "Risk Assessment of Security Requirements of Banking Information System Based on Attack Patterns", J.SCI., Springer, .2017

[3] Gary Stoneburner, Alice Goguen, and Alexis Feringa, "Risk Management Guide for Information Technology Systems : Recommendations of the National Institute of Standards and Technology", J. Syst. Softw., vol.30, no.4, pp.22-1, .2013

[4] Charles P. Pfleeger, Shari Lawrence Pfleeger, "Security in computing", Practise Hall Professional Reference, Upper Sandle River, New Jersey, US, .1997

[5] pp. 64-1, International Organization for Standardization (ISO), "SO/IEC 27005 Information technology - Security Techniques - Requirements for bodies providing audit and ceritification of information security management systems", pp.64-1, .2015

[6] M. Schumacher and U. Roedig, "Security Engineering with Patterns", J. Engineering, vol.2754, pp.208-1, .201

[7] D. G. Firesmith, "Engineering security requirements", J. Object Technol., vol.2, no.1, pp. 68-53, .2003

[8] Bank of Thailand, "IT Best Practice Phase I", .2013

[9] Bank of Thailand, "IT Best Practice Phase II", .2014

[10] Yates Baeza and Neto Ribeiro, "Modern Information Retrieval", Addison-Wesley, .1999

[11] E. J. Stierna and N. C. Rowe, "Applying information-retrieval methods to software reuse: A case study", J. Inf. Process. Manag., vol.39, no.1, pp. 74-67, .2003

[12] Can Akdeniz, "Risk Management Explained", ISBN-10:1507681852,ISBN--13:978 1507681855, Baderstrasse, 55 D-53489 Bad Bodendorf Germany, .2015

[13] Paul R. Garvey, "Analytical Methods for Risk Management: A Systems Engineering Perspective", ISBN-10:1420011391,ISBN-13:9781420011395, CRC Press, .2008

[14] Y. Yu, V. N. L. Franqueira, T. Than Tun, R. J. Wieringa, and B. Nuseibeh, "Automated analysis of security requirements through risk-based argumentation", J. Syst. Softw., vol.106, pp.116-102, .2015

[15] K. Piromsopa, T. Rojkangsadan and N. Prompoon, "A Risk Assessment of Web Server : Impact Classification by Loss Type", The IASTED Internation Conference on Network and Communication System(NCS), .2005

[16] T. Banklongsi and T. Senivongse, “A Security Measurement Model for Web Services Based on Provision of Attack Countermeasures”, 15th International ANnual Symposium on Computational Science and Engineering (ANSCSE (15 pp. 593–598, .2011

[17] Muhammad Ilyas and Josef Küng, "A Similarity Measurement Framework for Requirements Engineering", 4th International Multi-Conference on Computing in the Global Information Technology, .2009

[18] M.F. Poter, "Snowball: A language for stemming algorithms", [Online], 2001, Available from: http://www.snowball.tartarus.org/texts/introduction.html., [10 June .[2017

[19] Wiley Online Library, "Statistic Table", [Online], 2013, Available from: http://onlinelibrary.wiley.com/doi/.9781118643624/10.1002app/2pdf, [10 June .[2017

[20] Adecco, "Thailand Salary Guide "2017, [Online], 2017, Available from: https://adecco.co.th/salary-guide/00001/2017, [13 June .[2017

ภาคผนวก

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

ภาคผนวก ก แบบรูปการโจมตีที่ใช้งานวิจัย

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

ตารางที่ ก.1 แบบรูปการโจมตี วิธีการบรรเทา และความต้องการด้านความมั่นคงที่เกี่ยวข้อง

หมายเลขแบบรูปการโจมตี	1	**ชื่อแบบรูปการโจมตี**	Accessing Functionality Not Properly Constrained by ACL
ค่าคุณสมบัติแบบรูปการโจมตี	**ความรุนแรง :** High **โอกาสการใช้ประโยชน์ :** Very High		
วิธีการบรรเทา/ความต้องการด้านความมั่นคงที่เกี่ยวข้อง	**ความต้องการด้านความมั่นคงที่เกี่ยวข้อง** • All resources must be constrained to be inaccessible by default followed by selectively allowing access to resources as dictated by application and business logic • In addition to a central controller, every resource must also restrict, wherever possible, incoming accesses as dictated by the relevant ACL.		
หมายเลขแบบรูปการโจมตี	2	**ชื่อแบบรูปการโจมตี**	Inducing Account Lockout
ค่าคุณสมบัติแบบรูปการโจมตี	**ความรุนแรง :** Medium **โอกาสการใช้ประโยชน์ :** High		
วิธีการบรรเทา/ความต้องการด้านความมั่นคงที่เกี่ยวข้อง	**วิธีการบรรเทา** • Implement intelligent password throttling mechanisms such as those which take IP address into account, in addition to the login name. • When implementing security features, consider how they can be misused and made to turn on themselves.		
หมายเลขแบบรูปการโจมตี	7	**ชื่อแบบรูปการโจมตี**	Blind SQL Injection
ค่าคุณสมบัติแบบรูการโจมตี	**ความรุนแรง :** High **โอกาสการใช้ประโยชน์ :** High		
วิธีการบรรเทา/ความต้องการด้านความมั่นคงที่เกี่ยวข้อง	**ความต้องการด้านความมั่นคงที่เกี่ยวข้อง** • Custom error pages must be used to handle exceptions such that they do not reveal any information about the architecture of the application or the database. • Special characters in user-controllable input must be escaped before use by the application. • Employ application-level safeguards to filter data and handle exceptions gracefully.		

ตารางที่ ก.1 แบบรูปการโจมตี วิธีการบรรเทา และความต้องการด้านความมั่นคงที่เกี่ยวข้อง (ต่อ)

หมายเลขแบบรูปการโจมตี	16	**ชื่อแบบรูปการโจมตี**	Exploitation of Trusted Credentials
ค่าคุณสมบัติแบบรูปการโจมตี	**ความรุนแรง :** High **โอกาสการใช้ประโยชน์ :** High		
วิธีการบรรเทา/ความต้องการด้านความมั่นคงที่เกี่ยวข้อง	**วิธีการบรรเทา** • Create a strong password policy and ensure that your system enforces this policy. • Implement an intelligent password throttling mechanism. Care must be taken to assure that these mechanisms do not excessively enable account lockout attacks such as CAPEC-02.		
หมายเลขแบบรูปการโจมตี	21	**ชื่อแบบรูปการโจมตี**	Dictionary-based Password Attack
ค่าคุณสมบัติแบบรูปการโจมตี	**ความรุนแรง :** High **โอกาสการใช้ประโยชน์ :** Medium		
วิธีการบรรเทา/ความต้องการด้านความมั่นคงที่เกี่ยวข้อง	**วิธีการบรรเทา** • Design: utilize strong federated identity such as SAML to encrypt and sign identity tokens in transit. • Implementation: Use industry standards session key generation mechanisms that utilize high amount of entropy to generate the session key. Many standard web and application servers will perform this task on your behalf. • Implementation: If the session identifier is used for authentication, such as in the so-called single sign on use cases, then ensure that it is protected at the same level of assurance as authentication tokens. • Implementation: If the web or application server supports it, then encrypting and/or signing the session ID (such as cookie) can protect the ID if intercepted. • Design: Use strong session identifiers that are protected in transit and at rest. • Implementation: Utilize a session timeout for all sessions, for example 20 minutes. If the user does not explicitly logout, the server terminates their session after this period of inactivity. If the user logs back in then a new session key is generated. Implementation: Verify of authenticity of all session IDs at runtime.		
หมายเลขแบบรูปการโจมตี	36	**ชื่อแบบรูปการโจมตี**	Using Unpublished APIs
ค่าคุณสมบัติแบบรูปการโจมตี	**ความรุนแรง :** High **โอกาสการใช้ประโยชน์ :** Medium		
วิธีการบรรเทา/ความต้องการด้านความมั่นคงที่เกี่ยวข้อง	ความต้องการด้านความมั่นคงที่เกี่ยวข้อง • Authenticate every request or message to a service • Do not rely on lack of discoverability to protect privileged functions within the service		

ตารางที่ ก.1 แบบรูปการโจมตี วิธีการบรรเทา และความต้องการด้านความมั่นคงที่เกี่ยวข้อง (ต่อ)

หมายเลขแบบรูปการโจมตี	37	**ชื่อแบบรูปการโจมตี**	Retrieve Embedded Sensitive Data
ค่าคุณสมบัติแบบรูปการโจมตี	**ความรุนแรง :** Very High **โอกาสการใช้ประโยชน์ :** Very High		
วิธีการบรรเทา/ความต้องการด้านความมั่นคงที่เกี่ยวข้อง	**ความต้องการด้านความมั่นคงที่เกี่ยวข้อง** • No sensitive or confidential information must be stored in client distributions. This includes content such as passwords or encryption keys. In cases where this is necessary, avoid storing any such information in plaintext • All information arriving from a client must be validated before use.		
หมายเลขแบบรูปการโจมตี	39	**ชื่อแบบรูปการโจมตี**	Manipulating Opaque Client-based Data Tokens
ค่าคุณสมบัติแบบรูปการโจมตี	**ความรุนแรง :** Medium **โอกาสการใช้ประโยชน์ :** Very High		
วิธีการบรรเทา/ความต้องการด้านความมั่นคงที่เกี่ยวข้อง	**ความต้องการด้านความมั่นคงที่เกี่ยวข้อง** • Sensitive information stored client side must be integrity checked upon return before use		
หมายเลขแบบรูปการโจมตี	49	**ชื่อแบบรูปการโจมตี**	Password Brute Forcing
ค่าคุณสมบัติแบบรูปการโจมตี	**ความรุนแรง :** High **โอกาสการใช้ประโยชน์ :** Medium		
วิธีการบรรเทา/ความต้องการด้านความมั่นคงที่เกี่ยวข้อง	**วิธีการบรรเทา** • Implement a password throttling mechanism. This mechanism should take into account both the IP address and the log in name of the user. • Put together a strong password policy and make sure that all user created passwords comply with it. • Alternatively automatically generate strong passwords for users. • Passwords need to be recycled to prevent aging, that is every once in a while a new password must be chosen.		

ตารางที่ ก.1 แบบรูปการโจมตี วิธีการบรรเทา และความต้องการด้านความมั่นคงที่เกี่ยวข้อง (ต่อ)

หมายเลขแบบรูปการโจมตี	50	**ชื่อแบบรูปการโจมตี**	Password Recovery Exploitation
ค่าคุณสมบัติแบบรูปการโจมตี	**ความรุนแรง :** High **โอกาสการใช้ประโยชน์ :** Medium		
วิธีการบรรเทา/ความต้องการด้านความมั่นคงที่เกี่ยวข้อง	**วิธีการบรรเทา** • Use multiple security questions (e.g. have three and make the user answer two of them correctly). • Let the user select their own security questions or provide them with choices of questions that are not generic. • E-mail the temporary password to the registered e-mail address of the user rather than letting the user reset the password online. • Ensure that your password recovery functionality is not vulnerable to an injection style attack.		
หมายเลขแบบรูปการโจมตี	54	**ชื่อแบบรูปการโจมตี**	Query System for Information
ค่าคุณสมบัติแบบรูปการโจมตี	**ความรุนแรง :** Low **โอกาสการใช้ประโยชน์ :** High		
วิธีการบรรเทา/ความต้องการด้านความมั่นคงที่เกี่ยวข้อง	**ความต้องการด้านความมั่นคงที่เกี่ยวข้อง** • Custom error pages must be used to handle exceptions such that they do not reveal any information about the architecture of the application or the database. • Employ application-level safeguards to filter data and handle exceptions gracefully.		
หมายเลขแบบรูปการโจมตี	55	**ชื่อแบบรูปการโจมตี**	Rainbow Table Password Cracking
ค่าคุณสมบัติแบบรูปการโจมตี	**ความรุนแรง :** Medium **โอกาสการใช้ประโยชน์ :** Medium		
วิธีการบรรเทา/ความต้องการด้านความมั่นคงที่เกี่ยวข้อง	**วิธีการบรรเทา** • Use salt when computing password hashes. That is, concatenate the salt (random bits) with the original password prior to hashing it.		
หมายเลขแบบรูปการโจมตี	57	**ชื่อแบบรูปการโจมตี**	Utilizing REST's Trust in the System Resource to Register Man in the Middle
ค่าคุณสมบัติแบบรูปการโจมตี	**ความรุนแรง :** Very High **โอกาสการใช้ประโยชน์ :** Medium		
วิธีการบรรเทา/ความต้องการด้านความมั่นคงที่เกี่ยวข้อง	**วิธีการบรรเทา** • Implementation: Implement message level security such as HMAC in the HTTP communication • Design: Utilize defense in depth, do not rely on a single security mechanism like SSL • Design: Enforce principle of least privilege		

ตารางที่ ก.1 แบบรูปการโจมตี วิธีการบรรเทา และความต้องการด้านความมั่นคงที่เกี่ยวข้อง (ต่อ)

หมายเลขแบบรูปการโจมตี	59	**ชื่อแบบรูปการโจมตี**	Session Credential Falsification through Prediction
ค่าคุณสมบัติแบบรูปการโจมตี	**ความรุนแรง :** High **โอกาสการใช้ประโยชน์ :** High		
วิธีการบรรเทา/ความต้องการด้านความมั่นคงที่เกี่ยวข้อง	**วิธีการบรรเทา** • Use a strong source of randomness to generate a session ID. • Use adequate length session IDs • Do not use information available to the user in order to generate session ID (e.g., time). • Ideas for creating random numbers are offered by Eastlake [RFC1750] • Encrypt the session ID if you expose it to the user. For instance session ID can be stored in a cookie in encrypted format.		
หมายเลขแบบรูปการโจมตี	60	**ชื่อแบบรูปการโจมตี**	Reusing Session IDs (aka Session Replay)
ค่าคุณสมบัติแบบรูปการโจมตี	**ความรุนแรง :** High **โอกาสการใช้ประโยชน์ :** High		
วิธีการบรรเทา/ความต้องการด้านความมั่นคงที่เกี่ยวข้อง	**วิธีการบรรเทา** • Always invalidate a session ID after the user logout. • Setup a session time out for the session IDs. • Protect the communication between the client and server. For instance it is best practice to use SSL to mitigate man in the middle attack. • Do not code send session ID with GET method, otherwise the session ID will be copied to the URL. In general avoid writing session IDs in the URLs. URLs can get logged in log files, which are vulnerable to an attacker. • Encrypt the session data associated with the session ID. • Use multifactor authentication.		

ตารางที่ ก.1 แบบรูปการโจมตี วิธีการบรรเทา และความต้องการด้านความมั่นคงที่เกี่ยวข้อง (ต่อ)

หมายเลขแบบรูปการโจมตี	61	**ชื่อแบบรูปการโจมตี**	Session Fixation
ค่าคุณสมบัติแบบรูปการโจมตี	**ความรุนแรง :** High **โอกาสการใช้ประโยชน์ :** Medium		
วิธีการบรรเทา/ความต้องการด้านความมั่นคงที่เกี่ยวข้อง	**ความต้องการด้านความมั่นคงที่เกี่ยวข้อง** • Regenerate session identifiers upon each new request. This ensures that fixated session identifiers are rendered obsolete. • Regenerate a session identifier every time a user enters an authenticated session and destroy the identifier when the user logs out of an authenticated session. • et appropriate expiry times on cookies that contain session identifiers. This helps limit the window of opportunity for an attacker to use the identifier. • Do not use session identifiers as part of URLs or hidden form fields. It becomes easy for an attacker to trick a user into a fixated session when session identifiers are easily accessible. • Authenticate every transaction by requesting credentials. This ensures that only a legitimate user of the application can proceed with the transaction. If an attacker seeks to perform any such authenticated transaction, valid credentials will be required even though session fixation may have been successful earlier.		
หมายเลขแบบรูปการโจมตี	65	**ชื่อแบบรูปการโจมตี**	Sniff Application Code
ค่าคุณสมบัติแบบรูปการโจมตี	**ความรุนแรง :** N/A **โอกาสการใช้ประโยชน์ :** N/A		
วิธีการบรรเทา/ความต้องการด้านความมั่นคงที่เกี่ยวข้อง	**ความต้องการด้านความมั่นคงที่เกี่ยวข้อง** • Do not store secrets in client code • All potentially sensitive data, including code, transmitted to the client must be encrypted		
หมายเลขแบบรูปการโจมตี	69	**ชื่อแบบรูปการโจมตี**	Target Programs with Elevated Privileges
ค่าคุณสมบัติแบบรูปการโจมตี	**ความรุนแรง :** Very High **โอกาสการใช้ประโยชน์ :** Very High		
วิธีการบรรเทา/ความต้องการด้านความมั่นคงที่เกี่ยวข้อง	**ความต้องการด้านความมั่นคงที่เกี่ยวข้อง** • A user must be authenticated if she invokes a privileged program.		

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

ตารางที่ ก.1 แบบรูปการโจมตี วิธีการบรรเทา และความต้องการด้านความมั่นคงที่เกี่ยวข้อง (ต่อ)

หมายเลขแบบรูปการโจมตี	70	**ชื่อแบบรูปการโจมตี**	Try Common(default) Usernames and Passwords
ค่าคุณสมบัติแบบรูปการโจมตี	**ความรุนแรง :** High **โอกาสการใช้ประโยชน์ :** Medium		
วิธีการบรรเทา/ความต้องการด้านความมั่นคงที่เกี่ยวข้อง	**วิธีการบรรเทา** • Delete all default account credentials that may be put in by the product vendor. • Implement a password throttling mechanism. This mechanism should take into account both the IP address and the log in name of the user. • Put together a strong password policy and make sure that all user created passwords comply with it. • Alternatively automatically generate strong passwords for users. • Passwords need to be recycled to prevent aging, that is every once in a while a new password must be chosen.		
หมายเลขแบบรูปการโจมตี	74	**ชื่อแบบรูปการโจมตี**	Manipulating User State
ค่าคุณสมบัติแบบรูปการโจมตี	**ความรุนแรง :** High **โอกาสการใช้ประโยชน์ :** Medium		
วิธีการบรรเทา/ความต้องการด้านความมั่นคงที่เกี่ยวข้อง	**ความต้องการด้านความมั่นคงที่เกี่ยวข้อง** • Protect user state that is stored client-side with integrity checks to ensure that a malicious user cannot gain unauthorized access to parts of the application • Authenticate every request to ensure that it is coming from a legitimate user and that the request is a valid one in the current context.		
หมายเลขแบบรูปการโจมตี	83	**ชื่อแบบรูปการโจมตี**	XPath Injection
ค่าคุณสมบัติแบบรูปการโจมตี	**ความรุนแรง :** High **โอกาสการใช้ประโยชน์ :** High		
วิธีการบรรเทา/ความต้องการด้านความมั่นคงที่เกี่ยวข้อง	**ความต้องการด้านความมั่นคงที่เกี่ยวข้อง** • Special characters in user-controllable input must be escaped before use by the application. Only use parameterized XPath expressions to query the XML database. • Custom error pages must be used to handle exceptions such that they do not reveal any information about the architecture of the application or the database.		

ตารางที่ ก.1 แบบรูปการโจมตี วิธีการบรรเทา และความต้องการด้านความมั่นคงที่เกี่ยวข้อง (ต่อ)

หมายเลขแบบรูปการโจมตี	87	**ชื่อแบบรูปการโจมตี**	Forceful Browsing
ค่าคุณสมบัติแบบรูปการโจมตี	**ความรุนแรง :** High **โอกาสการใช้ประโยชน์ :** Very High		
วิธีการบรรเทา/ความต้องการด้านความมั่นคงที่เกี่ยวข้อง	**วิธีการบรรเทา** • Authenticate request to every resource. In addition, every page or resource must ensure that the request it is handling has been made in an authorized context. • Forceful browsing can also be made difficult to a large extent by not hard-coding names of application pages or resources. This way, the attacker cannot figure out, from the application alone, the resources available from the present context.		
หมายเลขแบบรูปการโจมตี	88	**ชื่อแบบรูปการโจมตี**	OS Command Injection
ค่าคุณสมบัติแบบรูปการโจมตี	**ความรุนแรง :** High **โอกาสการใช้ประโยชน์ :** High		
วิธีการบรรเทา/ความต้องการด้านความมั่นคงที่เกี่ยวข้อง	**วิธีการบรรเทา** • Use language APIs rather than relying on passing data to the operating system shell or command line. Doing so ensures that the available protection mechanisms in the language are intact and applicable. • Filter all incoming data to escape or remove characters or strings that can be potentially misinterpreted as operating system or shell commands • All application processes should be run with the minimal privileges required. Also, processes must shed privileges as soon as they no longer require them.		
หมายเลขแบบรูปการโจมตี	94	**ชื่อแบบรูปการโจมตี**	Man in the Middle Attack
ค่าคุณสมบัติแบบรูปการโจมตี	**ความรุนแรง :** Very High **โอกาสการใช้ประโยชน์ :** Very High		
วิธีการบรรเทา/ความต้องการด้านความมั่นคงที่เกี่ยวข้อง	**วิธีการบรรเทา** • Get your Public Key signed by a Certificate Authority • Encrypt your communication using cryptography (SSL,...) • Use Strong mutual authentication to always fully authenticate both ends of any communications channel. • Exchange public keys using a secure channel		

ตารางที่ ก.1 แบบรูปการโจมตี วิธีการบรรเทา และความต้องการด้านความมั่นคงที่เกี่ยวข้อง (ต่อ)

หมายเลขแบบรูปการโจมตี	100	**ชื่อแบบรูปการโจมตี**	Overflow Buffers
ค่าคุณสมบัติแบบรูปการโจมตี	**ความรุนแรง :** Very High **โอกาสการใช้ประโยชน์ :** High		
วิธีการบรรเทา/ความต้องการด้านความมั่นคงที่เกี่ยวข้อง	**ความต้องการด้านความมั่นคงที่เกี่ยวข้อง** • All user-controllable input must be strictly validated for enforcement of length and semantic checks • All exception conditions (such as ArrayIndexOutOfBounds) in applications must be gracefully handled through use of available exception handling mechanisms. • All applications and processes must be run with minimum privileges necessary so as to avoid an escalation of privilege in case of a successful exploit.		
หมายเลขแบบรูปการโจมตี	102	**ชื่อแบบรูปการโจมตี**	Session Sidejacking
ค่าคุณสมบัติแบบรูปการโจมตี	**ความรุนแรง :** High **โอกาสการใช้ประโยชน์ :** High		
วิธีการบรรเทา/ความต้องการด้านความมั่นคงที่เกี่ยวข้อง	**ความต้องการด้านความมั่นคงที่เกี่ยวข้อง** • Ensure that SSL is used for all communication between the client and the target system where sensitive data and/or operations are available. • Ensure that session cookies are only transmitted via SSL pipes by setting the cookie's secure attribute to true.		
หมายเลขแบบรูปการโจมตี	108	**ชื่อแบบรูปการโจมตี**	Command Line Execution through SQL Injection
ค่าคุณสมบัติแบบรูปการโจมตี	**ความรุนแรง :** Very High **โอกาสการใช้ประโยชน์ :** Low		
วิธีการบรรเทา/ความต้องการด้านความมั่นคงที่เกี่ยวข้อง	**ความต้องการด้านความมั่นคงที่เกี่ยวข้อง** • Validate all data syntactically and semantically before writing it to the database • Do not implicitly trust database data and validate it to ensure that it is safe in the context in which it is being used		
หมายเลขแบบรูปการโจมตี	110	**ชื่อแบบรูปการโจมตี**	SQL Injection through SOAP Parameter Tampering
ค่าคุณสมบัติแบบรูปการโจมตี	**ความรุนแรง :** Very High **โอกาสการใช้ประโยชน์ :** High		
วิธีการบรรเทา/ความต้องการด้านความมั่นคงที่เกี่ยวข้อง	**ความต้องการด้านความมั่นคงที่เกี่ยวข้อง** • Always safely access the database through prepared statements that leverage parameter binding • Properly validate all SOAP parameters to ensure that their values are as expected • Reject bad user input (do not try to sanitize it)		

ตารางที่ ก.1 แบบรูปการโจมตี วิธีการบรรเทา และความต้องการด้านความมั่นคงที่เกี่ยวข้อง (ต่อ)

หมายเลขแบบรูปการโจมตี	127	**ชื่อแบบรูปการโจมตี**	Directory Indexing
ค่าคุณสมบัติแบบรูปการโจมตี	**ความรุนแรง :** Medium **โอกาสการใช้ประโยชน์ :** High		
วิธีการบรรเทา/ความต้องการด้านความมั่นคงที่เกี่ยวข้อง	**วิธีการบรรเทา** • Using blank index.html: putting blank index.html simply prevent directory listings from displaying to site visitors. • Preventing with .htaccess in Apache web server: In .htaccess, write "Options-indexes". • Suppressing error messages: using error 403 "Forbidden" message exactly like error 404 "Not Found" message.		
หมายเลขแบบรูปการโจมตี	135	**ชื่อแบบรูปการโจมตี**	Format String Injection
ค่าคุณสมบัติแบบรูปการโจมตี	**ความรุนแรง :** High **โอกาสการใช้ประโยชน์ :** High		
วิธีการบรรเทา/ความต้องการด้านความมั่นคงที่เกี่ยวข้อง	**ความต้องการด้านความมั่นคงที่เกี่ยวข้อง** • User-controllable input shall not be used directly inside a formatting string function e.g., fprintf(user_controllable). Special formatting characters in user-controllable input must be escaped before use by the application in a formatting string function. • Ensure that all format string functions are passed a static string which cannot be controlled by the user and that the proper number of arguments are always sent to that function as well. If at all possible, use functions that do not support the %n operator in format strings.		
หมายเลขแบบรูปการโจมตี	136	**ชื่อแบบรูปการโจมตี**	LDAP Injection
ค่าคุณสมบัติแบบรูปการโจมตี	**ความรุนแรง :** High **โอกาสการใช้ประโยชน์ :** High		
วิธีการบรรเทา/ความต้องการด้านความมั่นคงที่เกี่ยวข้อง	**ความต้องการด้านความมั่นคงที่เกี่ยวข้อง** • Special characters in user-controllable input must be escaped before use by the application. • Custom error pages must be used to handle exceptions such that they do not reveal any information about the architecture of the application or the LDAP structure.		

ตารางที่ ก.1 แบบรูปการโจมตี วิธีการบรรเทา และความต้องการด้านความมั่นคงที่เกี่ยวข้อง (ต่อ)

หมายเลขแบบรูปการโจมตี	139	**ชื่อแบบรูปการโจมตี**	Relative Path Traversal
ค่าคุณสมบัติแบบรูปการโจมตี	**ความรุนแรง :** High **โอกาสการใช้ประโยชน์ :** High		
วิธีการบรรเทา/ความต้องการด้านความมั่นคงที่เกี่ยวข้อง	**ความต้องการด้านความมั่นคงที่เกี่ยวข้อง** • Special characters in user-controllable input must be escaped before use by the application. • Custom error pages must be used to handle exceptions such that they do not reveal any information about the architecture of the application or the LDAP structure.		
หมายเลขแบบรูปการโจมตี	169	**ชื่อแบบรูปการโจมตี**	Footprinting
ค่าคุณสมบัติแบบรูปการโจมตี	**ความรุนแรง :** Very Low **โอกาสการใช้ประโยชน์ :** High		
วิธีการบรรเทา/ความต้องการด้านความมั่นคงที่เกี่ยวข้อง	**วิธีการบรรเทา** • Keep patches up to date by installing weekly or daily if possible. Shut down unnecessary services/ports. • Change default passwords by choosing strong passwords. • Curtail unexpected input. • Encrypt and password-protect sensitive data. • Avoid including information that has the potential to identify and compromise your organization's security such as access to business plans, formulas, and proprietary documents.		
หมายเลขแบบรูปการโจมตี	170	**ชื่อแบบรูปการโจมตี**	Web Application Fingerprinting
ค่าคุณสมบัติแบบรูปการโจมตี	**ความรุนแรง :** Low **โอกาสการใช้ประโยชน์ :** High		
วิธีการบรรเทา/ความต้องการด้านความมั่นคงที่เกี่ยวข้อง	**วิธีการบรรเทา** • Implementation: Obfuscate server fields of HTTP response. • Implementation: Hide inner ordering of HTTP response header. • Implementation: Customizing HTTP error codes such as 404 or 500. • Implementation: Hide URL file extension. • Implementation: Hide HTTP response header software information filed. • Implementation: Hide cookie's software information filed. • Implementation: Appropriately deal with error messages. • Implementation: Obfuscate database type in Database API's error message.		

ตารางที่ ก.1 แบบรูปการโจมตี วิธีการบรรเทา และความต้องการด้านความมั่นคงที่เกี่ยวข้อง (ต่อ)

หมายเลขแบบรูปการโจมตี	182	**ชื่อแบบรูปการโจมตี**	Flash Injection
ค่าคุณสมบัติแบบรูปการโจมตี	**ความรุนแรง :** Medium **โอกาสการใช้ประโยชน์ :** High		
วิธีการบรรเทา/ความต้องการด้านความมั่นคงที่เกี่ยวข้อง	**วิธีการบรรเทา** • Implementation :remove sensitive information such as user name and password in the SWF file. • Implementation :use validation on both client and server side. • Implementation :remove debug information. • Implementation :use SSL when loading external data • Implementation :use crossdomain.xml file to allow the application domain to load stuff or the SWF file called by other domain.		
หมายเลขแบบรูปการโจมตี	250	**ชื่อแบบรูปการโจมตี**	XML Injection
ค่าคุณสมบัติแบบรูปการโจมตี	**ความรุนแรง :** N/A **โอกาสการใช้ประโยชน์ :** High		
วิธีการบรรเทา/ความต้องการด้านความมั่นคงที่เกี่ยวข้อง	**ความต้องการด้านความมั่นคงที่เกี่ยวข้อง** • Special characters in user-controllable input must be escaped before use by the application. • Custom error pages must be used to handle exceptions such that they do not reveal any information about the architecture of the application or the database.		
หมายเลขแบบรูปการโจมตี	476	**ชื่อแบบรูปการโจมตี**	Signature Spoofing by Misrepresentation
ค่าคุณสมบัติแบบรูปการโจมตี	**ความรุนแรง :** High **โอกาสการใช้ประโยชน์ :** Low		
วิธีการบรรเทา/ความต้องการด้านความมั่นคงที่เกี่ยวข้อง	**วิธีการบรรเทา** • Ensure the application is using parsing and data display techniques that will accurately display control characters, international symbols and markings, and ultimately recognize potential homograph attacks.		

ภาคผนวก ข แบบสอบถามและผลการตอบแบบสอบถาม

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

แบบสอบถามงานวิจัย

แบบสอบถามนี้เป็นส่วนหนึ่งของวิทยานิพนธ์ ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย

ชื่อวิทยานิพนธ์

ชื่อภาษาไทย: การประเมินความเสี่ยงของความต้องการด้านความมั่นคงของระบบสารสนเทศทางการธนาคารโดยอิงแบบรูปการโจมตี

ชื่อภาษาอังกฤษ :Risk Assessment of Security Requirements of Banking Information System Based on Attack Pattern

อาจารย์ที่ปรึกษาวิทยานิพนธ์: รองศาสตราจารย์ ดร.ทวิตีย์ เสนีวงศ์ ณ อยุธยา

ผู้ทำวิจัย: นายกฤษดา รองรัตน์

อีเมลล์ :krissada.ro@student.chula.ac.th, krissada.r@protonmail.com

แบบสอบถามนี้ประกอบด้วย 2 แบบประเมิน ดังนี้

แบบสอบถามที่ 1 เพื่อประเมินความถูกต้องของการจับคู่ของความมั่นคงที่พึงจะมีกับวิธีการบรรเทาการโจมตี และสำรวจความเห็นความเสี่ยงของการขาดหายไปของความต้องการด้านความมั่นคงที่พึงจะมีในแต่ละข้อ มีส่วนย่อย 4 ส่วน

1) ความต้องการด้านความมั่นคงที่พึงจะมีสำหรับระบบหลักการธนาคาร
2) ความต้องการด้านความมั่นคงที่พึงจะมีสำหรับระบบควบคุมเอทีเอ็ม (ATM)
3) ความต้องการด้านความมั่นคงที่พึงจะมีสำหรับระบบควบคุมอินเตอร์เน็ตแบงค์กิ้ง (Internet Banking)
4) ความต้องการด้านความมั่นคงที่พึงจะมีสำหรับระบบอินเตอร์เน็ตแบงค์กิ้ง (Internet Banking)

วัตถุประสงค์

1.) เพื่อประเมินความถูกต้องของการจับคู่ของความต้องการด้านความมั่นคงที่พึงจะมีกับแบบรูปแบบการโจมตีที่เสนอโดยผู้วิจัย มีความเหมาะสมหรือไม่
2.) เพื่อสำรวจความเห็นของการขาดหายไปของความต้องการด้านความมั่นคงที่พึงจะมีแต่ละข้อ และความเสี่ยงที่เกิดขึ้นจากการขาดหายไป

2) แบบสอบถามที่ 2 เพื่อสำรวจค่าใช้จ่ายในการประเมินความเสี่ยงของระบบสารสนเทศทางการธนาคารจากเอกสารความต้องการ

วัตถุประสงค์

1.) เพื่อประเมินความถูกต้องของการจับคู่ของความต้องการด้านความมั่นคงที่พึงจะมีกับแบบรูปแบบการโจมตีที่เสนอโดยผู้วิจัย มีความเหมาะสมหรือไม่

คำอธิบายในการกรอกแบบสอบถาม

โปรดกากบาทใน ☐ หน้าตัวเลือกที่ท่านต้องการ โดย double click ที่ ☐ ที่ต้องการเลือก แล้วเลือกค่า Default Value เป็น “Checked”

ข้อมูลผู้ตอบแบบสอบถาม

ระดับการศึกษา : ☐กว่าปริญญาตรี ☐ ปริญญาตรี ☐ ปริญญาโท ☐ ปริญญาเอก

ตำแหน่งงาน: ☐ Security Specialist ☐Security Engineer ☐ Security Audit
☐ Business Analyst
☐ อื่น ๆ (โปรดระบุ)_____

ท่านมีประสบการณ์ด้านความมั่นคงหรือไม่ ☐ ไม่มี ☐ มี โปรดระบุ_____ปี

รู้จักแบบรูปการโจมตีคาเปกหรือไม่ ☐ ไม่รู้จัก ☐ รู้จัก

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

<u>แบบสอบถามที่</u> 1 .หลังจากที่ท่านได้ทำการศึกษาความต้องการด้านความมั่นคงที่พึงจะมีและแบบรูปการโจมตีที่ผู้วิจัยรวบรวมจากคาเปก ท่านมีความเห็นด้วยหรือไม่กับการจับคู่ความสัมพันธ์ และหากความต้องการด้านความมั่นคงที่พึงจะมีนั้นขาดหายไปท่านเห็นว่าในแต่ละข้อมีความเสี่ยงในระดับใด (โปรดให้ความเห็นทั้ง 2 หัวข้อ)

SSRB_ID	ความเห็นต่อการจับคู่ความสัมพันธ์ระหว่างความต้องการด้านความมั่นคงที่พึงจะมีกับแบบรูปการโจมตี			ระดับความเสี่ยง				
	เห็นด้วย	ไม่เห็นด้วย	ไม่แน่ใจ	Very High	High	Medium	Low	Very Low
1. ความต้องการด้านความมั่นคงที่พึงจะมีสำหรับระบบหลักการธนาคาร								
CBS_001	☐	☐	☐	☐	☐	☐	☐	☐
CBS_002	☐	☐	☐	☐	☐	☐	☐	☐
CBS_003	☐	☐	☐	☐	☐	☐	☐	☐
CBS_004	☐	☐	☐	☐	☐	☐	☐	☐
CBS_005	☐	☐	☐	☐	☐	☐	☐	☐
CBS_006	☐	☐	☐	☐	☐	☐	☐	☐
CBS_007	☐	☐	☐	☐	☐	☐	☐	☐
CBS_008	☐	☐	☐	☐	☐	☐	☐	☐
CBS_009	☐	☐	☐	☐	☐	☐	☐	☐
CBS_010	☐	☐	☐	☐	☐	☐	☐	☐
2. ความต้องการด้านความมั่นคงที่พึงจะมีสำหรับระบบควบคุมเอทีเอ็ม								
ATMC_001	☐	☐	☐	☐	☐	☐	☐	☐
ATMC_002	☐	☐	☐	☐	☐	☐	☐	☐
ATMC_003	☐	☐	☐	☐	☐	☐	☐	☐
ATMC_004	☐	☐	☐	☐	☐	☐	☐	☐
ATMC_005	☐	☐	☐	☐	☐	☐	☐	☐
ATMC_006	☐	☐	☐	☐	☐	☐	☐	☐
ATMC_007	☐	☐	☐	☐	☐	☐	☐	☐
ATMC_008	☐	☐	☐	☐	☐	☐	☐	☐
ATMC_009	☐	☐	☐	☐	☐	☐	☐	☐
ATMC_010	☐	☐	☐	☐	☐	☐	☐	☐
ATMC_011	☐	☐	☐	☐	☐	☐	☐	☐
3. ความต้องการด้านความมั่นคงที่พึงจะมีสำหรับระบบควบคุมอินเตอร์เน็ตแบงค์กิ้ง								
IBC_001	☐	☐	☐	☐	☐	☐	☐	☐
IBC_002	☐	☐	☐	☐	☐	☐	☐	☐
IBC_003	☐	☐	☐	☐	☐	☐	☐	☐
IBC_004	☐	☐	☐	☐	☐	☐	☐	☐

SSRB_ID	ความเห็นต่อการจับคู่ความสัมพันธ์ระหว่างความต้องการด้านความมั่นคงที่พึงจะมีกับแบบรูปการโจมตี			ระดับความเสี่ยง				
	เห็นด้วย	ไม่เห็นด้วย	ไม่แน่ใจ	Very High	High	Medium	Low	Very Low
IBC_005	☐	☐	☐	☐	☐	☐	☐	☐
IBC_006	☐	☐	☐	☐	☐	☐	☐	☐
IBC_007	☐	☐	☐	☐	☐	☐	☐	☐
IBC_008	☐	☐	☐	☐	☐	☐	☐	☐
IBC_009	☐	☐	☐	☐	☐	☐	☐	☐
IBC_010	☐	☐	☐	☐	☐	☐	☐	☐
4. ความต้องการด้านความมั่นคงที่พึงจะมีสำหรับระบบอินเตอร์เน็ตแบงค์กิ้ง								
IBS_001	☐	☐	☐	☐	☐	☐	☐	☐
IBS_002	☐	☐	☐	☐	☐	☐	☐	☐
IBS_003	☐	☐	☐	☐	☐	☐	☐	☐
IBS_004	☐	☐	☐	☐	☐	☐	☐	☐
IBS_005	☐	☐	☐	☐	☐	☐	☐	☐
IBS_006	☐	☐	☐	☐	☐	☐	☐	☐
IBS_007	☐	☐	☐	☐	☐	☐	☐	☐
IBS_008	☐	☐	☐	☐	☐	☐	☐	☐
IBS_009	☐	☐	☐	☐	☐	☐	☐	☐
IBS_010	☐	☐	☐	☐	☐	☐	☐	☐
IBS_011	☐	☐	☐	☐	☐	☐	☐	☐
IBS_012	☐	☐	☐	☐	☐	☐	☐	☐
IBS_013	☐	☐	☐	☐	☐	☐	☐	☐
IBS_014	☐	☐	☐	☐	☐	☐	☐	☐
IBS_015	☐	☐	☐	☐	☐	☐	☐	☐
IBS_016	☐	☐	☐	☐	☐	☐	☐	☐
IBS_017	☐	☐	☐	☐	☐	☐	☐	☐
IBS_018	☐	☐	☐	☐	☐	☐	☐	☐
IBS_019	☐	☐	☐	☐	☐	☐	☐	☐

<u>แบบสอบถามที่</u> 2

1. ท่านมีส่วนร่วมในการประเมินความเสี่ยงด้านความมั่นคงในองค์กรหรือไม่
   ☐ มีส่วนร่วม
   ☐ ไม่มีส่วนร่วม

2. ท่านมีส่วนร่วมในการประเมินความเสี่ยงด้านความมั่นคงในหน้าที่ใด (ตอบกรณีมีส่วนร่วมในการประเมิน)
   ☐ บริหารจัดการ (วางแผน จัดสรรงบประมาณ)
   ☐ ผู้ดำเนินการประเมิน

3. ในการประเมินความเสี่ยงด้านความมั่นคงจากเอกสารความต้องการ มีค่าใช้จ่ายในการดำเนินกิจกรรมประมาณเท่าไหร่ (ตอบกรณีมีส่วนร่วมในการประเมิน)
   .....บาท/โครงการ

4. ในการประเมินความเสี่ยงด้านความมั่นคงจากเอกสารความ ต้องใช้เวลานานเท่าไหร่ (ตอบกรณีมีส่วนร่วมในการประเมิน)
   .....วัน/โครงการ

ข้อคิดเห็น ข้อเสนอแนะเพิ่มเติม

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

ตารางที่ ข.1 ผลการสำรวจการจับคู่กับแบบรูปการโจมตีและระดับความเสี่ยงในการขายหายไปของรายการความต้องการที่พึงจะมี

Position	Education	CAPEC	Experience	CBS_001	CBS_002	CBS_003	CBS_004	CBS_005	CBS_006	CBS_007	CBS_008	CBS_009	CBS_010	CBS_011	ATMC_001	ATMC_002	ATMC_003	ATMC_004	ATMC_005	ATMC_006	ATMC_007	ATMC_008	ATMC_009	ATMC_010	IBC_001	IBC_002	IBC_003	IBC_004	IBC_005	IBC_006	IBC_007	IBC_008	IBC_009	IBS_001	IBS_002	IBS_003	IBS_004	IBS_005	IBS_006	IBS_007	IBS_008	IBS_009	IBS_010	IBS_011	IBS_012	IBS_013	IBS_014	IBS_015	IBS_016	IBS_017	IBS_018	IBS_019
Security Specialist	Master	Y	>10	A	A	A	A	A	A	A	A	A	DA	DA	A	DA	A	A	A	A	A	A	A	A	A	DA	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A
				M	H	H	M	VL	VL	L	L	VL	VH	VH	VH	M	M	M	L	L	L	H	H	VH	VH	M	M	M	M	M	L	H	H	H	VL	L	H	H	M	M	M	H	VL	VH	VH	H	L	H	VH	H	H	VL
Security Audit	Master	N	7-10	A	A	A	A	A	A	A	A	A	UC	UC	A	UC	A	A	A	UC	A	A	A	A	A	UC	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A
				H	H	H	H	VL	VL	L	L	VL	VL	L	VH	VH	VH	VH	VH	VH	L	H	H	VH	VH	VH	VH	VH	VH	VH	L	H	H	H	VL	L	H	H	M	M	M	H	VL	H	H	H	M	H	H	H	H	VL
Security Audit	Master	Y	>10	A	A	A	A	A	A	A	A	A	UC	UC	A	UC	A	A	A	A	A	A	A	A	A	UC	UC	UC	UC	UC	A	A	A	A	A	A	A	A	A	A	A	A	UC	A	A	A	A	A	A	A	A	UC
				M	H	H	M	VL	VL	L	L	VL	L	L	VH	M	M	M	M	M	L	H	H	VH	VH	M	M	M	M	M	L	H	H	H	VL	L	H	H	M	M	M	H	VL	VH	VH	H	L	H	VH	H	H	VL
Security Engineer	Bachelor	N	4-6	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A
				H	H	H	M	VL	VL	M	M	VL	VL	H	VH	VH	VH	VH	VH	VH	L	H	H	H	VH	VH	VH	VH	VH	VH	L	H	H	H	L	VL	M	M	M	M	M	M	L	H	H	H	M	H	H	H	H	L
Security Audit	Bachelor	Y	4-6	A	A	A	A	A	A	A	A	A	UC	UC	A	UC	A	A	A	A	A	A	A	A	A	UC	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	UC	A	A	A	A	A	A	A	A	UC
				M	H	H	M	L	L	L	L	L	L	L	VH	M	M	M	M	M	L	H	H	VH	VH	M	M	M	M	M	L	H	H	H	VL	L	H	H	M	M	M	H	L	VH	VH	H	L	H	VH	H	H	L
Security Engineer	Bachelor	N	4-6	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A
				H	H	H	M	L	L	M	M	H	H	M	H	VH	VH	VH	VH	VH	M	M	M	H	H	VH	VH	VH	VH	VH	M	M	M	H	L	VL	M	M	M	M	M	M	L	H	H	H	M	H	H	H	H	L
Security Specialist	Bachelor	Y	7-10	A	A	A	A	A	A	A	A	A	DA	DA	A	DA	A	A	A	A	A	A	A	A	A	DA	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A
				M	H	H	M	VL	VL	L	L	VL	L	L	VH	M	M	M	M	M	L	H	H	VH	VH	M	M	M	M	M	L	H	H	H	VL	L	H	H	M	M	M	H	L	VH	VH	H	L	H	VH	H	H	L
Security Engineer	Master	N	7-10	A	A	A	A	UC	UC	A	A	UC	UC	UC	A	UC	A	A	A	UC	A	A	A	A	A	UC	A	A	A	UC	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A
				M	H	H	M	VL	VL	L	L	VL	VL	H	VH	M	M	M	M	M	M	M	M	VH	VH	M	M	M	M	M	M	M	M	H	VL	L	H	H	M	M	M	H	VL	VH	VH	H	L	H	VH	H	H	L
Security Engineer	Bachelor	N	1-3	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A
				M	M	M	M	M	M	M	M	H	H	H	H	H	H	H	H	H	M	M	M	VH	H	H	H	H	H	H	M	M	M	M	L	VL	M	M	M	M	M	M	VL	H	H	H	M	H	H	H	H	VL
Security Specialist	Bachelor	N	1-3	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A
				M	M	M	M	M	M	M	M	H	H	H	H	H	H	H	H	H	M	M	M	VH	H	H	H	H	H	H	M	M	M	M	L	VL	M	M	M	M	M	M	VL	H	H	H	M	H	H	H	H	VL
Security Specialist	Bachelor	N	1-3	A	A	A	A	UC	UC	A	A	UC	UC	UC	A	UC	UC	UC	UC	UC	A	A	A	A	A	UC	UC	UC	UC	UC	A	A	A	A	A	A	A	A	A	A	A	A	UC	A	A	A	A	A	A	A	A	UC
				M	M	M	M	M	M	M	M	H	H	M	H	H	H	H	H	H	M	M	M	VH	H	H	H	H	H	H	M	M	M	M	L	VL	M	M	M	M	M	M	L	H	H	H	M	H	H	H	H	VL
Security Specialist	Bachelor	Y	1-3	A	A	A	A	A	A	A	A	A	DA	DA	A	UC	A	A	A	A	A	A	A	A	A	UC	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A
				M	H	H	M	VL	VL	L	L	VL	L	L	VH	M	M	M	M	M	L	H	H	VH	VH	M	M	M	M	M	L	H	H	H	VL	VH	VH	H	L	H	VH	H	H	VL								
คะแนนเสี่ยงสูงสุด (แบบรูป)				A	A	A	A	A	A	A	A	A	UC	UC	A	UC	A	A	A	A	A	A	A	A	A	UC	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A
คะแนนเสี่ยงสูงสุด (ความเสี่ยง)				M	H	H	M	VL	VL	L	L	VL	L	L	VH	M	M	M	M	H	L	H	H	VH	VH	M	M	M	M	H	L	H	H	H	VL	L	H	H	M	M	M	H	VL	VH	VH	H	L	H	VH	H	H	VL

หมายเหตุ :A-Agree, DA-Disagree, UC-Uncertain

ตารางที่ ข.2 ผลการสำรวจค่าใช้จ่ายในการประเมินความเสี่ยงด้านความมั่นคงในแต่ละโครงการ

ตำแหน่ง	ประสบการณ์	มีส่วนร่วมในการประเมินฯ	บทบาท/หน้าที่	ค่าใช้จ่าย	ระยะเวลาดำเนินการ (วัน)
Security Specialist	>10	Y	Management	50,000.00	2
Security Audit	7-10	Y	Management	40,000.00	2
Security Audit	>10	Y	Management	40,000.00	2
Security Engineer	4-6	N			
Security Audit	4-6	Y	Management	15,000.00	1
Security Engineer	4-6	N			
Security Specialist	7-10	Y	Management	25,000.00	1
Security Engineer	7-10	Y	Management	18,000.00	1
Security Engineer	1-3	N			
Security Specialist	1-3	Y	Operator	-	1
Security Specialist	1-3	Y	Operator	-	1
Security Specialist	1-3	Y	Operator	-	1

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

ข้อคิดเห็น ข้อเสนอแนะเพิ่มเติม

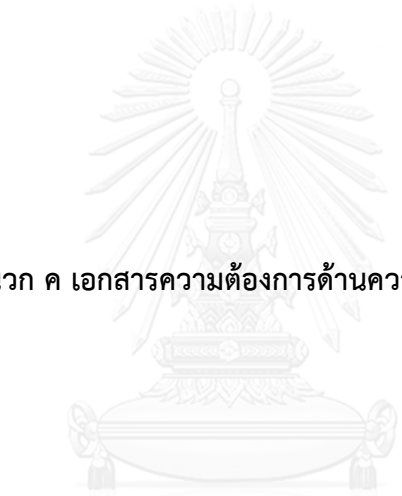
1. ไม่ค่อยเข้าใจ และความรู้ในเรื่อง Attack Pattern ของผู้กรอกยังมีน้อย
2. ไม่มีความรู้ในเรื่องของแบบรูปการโจมตีมากนัก จึงไม่แน่ใจเรื่องความเสี่ยง
3. ผู้วิจัยไม่ได้แสดงเหตุผลที่ไม่สามารถจับคู่กับแบบรูปการโจมตีได้
4. อาจจะมีแบบรูปการโจมตีขององค์กรอื่น หรืออะไรที่คล้ายกัน สามารถนำมาใช้ในงานวิจัยได้
5. ความต้องการบางข้อสามารถจับคู่กับ CAPEC อื่นได้ ถึงแม้จะไม่ตรงก็ตาม CBS010, CBS011 จับคู่ CAPAC#1
6. อยากให้ลองนำมาใช้ในการทำงานจริง เพื่อประเมินว่าสามารถใช้ได้จริงหรือไม่ ถ้าทำได้จะประหยัดค่าใช้จ่ายมาก
7. แบบจำลองมีประโยชน์ มีแนวโน้มใช้งานได้จริง แต่อยากให้พิจารณาฐานข้อมูลด้านความมั่นคงอื่นด้วย เช่น CWE ซึ่งน่าจะได้ข้อมูลที่มากขึ้น
8. แบบจำลองดี แต่ถ้าไม่ต้องตัดเอกสารส่วนที่ไม่เกี่ยวข้องออก จะดีมาก ประมาณได้เอกสารแล้วนำเข้าระบบได้เลย

9. ลองพิจารณาการคำนวณค่าความเสี่ยงอีกครั้ง เพราะหากใช้ค่า min จะเป็นการลดค่าความเสี่ยงหรือไม่ ถ้าได้ผลยังงั้ยกลับมาด้วยนะ

10. แบบจำลองเหมาะสม ครอบคลุมดี แต่ถ้าให้คนที่มีประสบการณ์ใช้ อาจจะเสียเวลามากกว่าเพราะต้องมาตัดส่วนที่ไม่เกี่ยวข้อง ส่วนที่ไม่เกี่ยวข้องเช่น bizz function req. มีเยอะกว่า security req.

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

ภาคผนวก ค เอกสารความต้องการด้านความมั่นคงของธนาคาร



จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

เอกสารความต้องการด้านความมั่นคงของการธนาคาร

ความต้องการด้านความมั่นคงสำหรับอินเทอร์เน็ตแบงค์กิ้ง

ฉบับที่ 1 (Doc_1)

SRB_001: The application shall use AES encryption and SSL protocol to safeguard sensitive data during transmission over open, public networks.

SRB_002: The application shall apply SHA 256 bits hashes to customer password and store those hashes in database or a configuration file with appropriate access control.

SRB_003: The application shall regenerate new session after successful authentication by two-factor authentication methodology.

SRB_004: The application shall lock the account after 5 failure logins attempts and do not display specific information is failure.

SRB_005: The application shall enforce strong password as following:

- Password is case sensitive.

SRB_006:

- Password age is 90 days.

SRB_007:

- Password shall not be reused from last 5 password histories

SRB_008: The application shall be forced change password after first logon or password is reset.

SRB_009: The application shall be used two-factor authentication)OTP (before reset password .

SRB_010: The application shall display the date/time of last successful login.

SRB_011: The application shall not write/store any sensitive information in cookies, source code, session, configuration file.

SRB_012: The application shall validate authority when access to important function.

SRB_013: The application shall randomly regenerate upon change page or new transaction.

SRB_014: The application shall support automatically logout and inactive session when transaction step is invalid.

SRB_015: The session idle timeout is 10 minutes.

SRB_016: The application shall re-authenticate when customer perform change profile by token.

SRB_017: The application shall re-authenticate when customer perform add favorite person for transfer money by token.

SRB_018: The application shall re-authenticate when customer perform change transaction limit by token.

ฉบับที่ 2 (Doc_2)

Detail of Minimum Web Application Security Requirements

Data Storing

1.) Minimum standard data storing for application systems specified in BOT requirements, it shall be complied with “attachment no.7 minimum standard data for application systems of commercial bank”

Logging & Audit Trail

1.) Application/System log has been complied with Computer Crime Act B.E.2550 and Appendix B of Ministerial Rule of Network Traffic Logging by Service Provider 2007.

Input Validation

1.) Validate all input data the application using white list)what is allowed to input (for data type, format, length, and business rules before accepting the data to displayed or stored .Reject if invalid.
2.) Sanitize all the potential area where untrusted inputs can enter as follows:
    a. User supplied data; GET, POST, HTTP Header and cookies.
    b. Anything read from the network, environment variables, reverse DNS lookups, query result, request headers, URL components, e-mail, files, filenames, database, and any external systems that provide data to the application.
3.) For any security checks that are performed on the client side, ensure that these must be checked on the server side.
4.) Do not concatenate user input data to a query or command.
    Use prepare Statement mechanism before doing any data manipulation with database.
5.) Prevent Cross-Site Request Forgery (CSRF) by not automatically submitted, add random token to all sensitive requests .Tokes should be cryptographically strong or random .
    When user perform a dangerous operation, send a separate confirmation request to ensure that the user intended to perform that operation.

Encryption

1.) Hard-coded credentials information are prohibited .If need, it shall be encrypted by strong encryption.
2.) Password shall apply strong one-way hashes to password and store those hashes in database or configuration file with appropriate access control.
3.) Use randomly assigned salts for each separate has that you generate.

Error Handling

1.) Avoid detailed error message page that are useful and/or exceed need information to an attacker.
    Utilize custom error pages in order to guarantee that the application will never leak error messages to an attacker .Provide useful error message in business view for users to know cause of error but not useful or exceed need in the security breach.

Information Leakage

1.) Do not store any confidential information in cookies.
2.) Prevent sensitive data from being cached on the client side.
3.) Ensure that confidential information is transmitted by using HTTP POST method.
4.) Ensure proper masking techniques are used while displaying sensitive personally identification information to users.
5.) Do not leak sensitive information in banner or comment.
6.) Do not store ant confidential information in log entries unless encrypted or masked.
7.) Path traversal shall be prohibited .Path name shall be verified before accessing any file .
8.) Directory indexing shall be prohibited.

Session Management

1.) Ensure that a new session is randomly regenerated upon successful authentication .Do not reuse the old session .Generate the new on after successful authentication.
2.) Use idle timeout periods not more than 30 minute that automatically logs out an inactive session .And session time out based on business requirements.
3.) To help mitigation XSS attacks against the user's session cookies, set the session cookies to ne HTTP only.

Transport Layer Protection

1.) Ensure your certificate is invalid, not expired, not revoked, and matches all domains used by the site.
2.) Strong encryption (e.g. AES, RSA) and security protocols (e.g. TLS, VPN-SSL) shall be used to safeguard sensitive data during transmission over open, public networks.
Web applications have authentication function and/or sensitive information shall use HTTPS to secure communication channel.
Require TLS 1.2 or higher for all sensitive pages .Non-SSL requests to these pages shall be redirected to the SSL page.

Secure URL redirection

1.) If redirection or forward required, do not use user supplied parameters in calculating URL destination.
2.) If the application could redirect to external sites, use an intermediate disclaimer page that provides the user with a clear warning that they are leaving your site .Implement a pause time period before the redirect occurs, or force the user to click on the link.

Misconfiguration

1.) Default value/configurations that they are well-known information shall be changed and default system accounts shall be disabled or change their user-name and password, if applicable.

Prevent unrestricted upload of file with dangerous type

1.) Allow uploading only with permitted file extension.
2.) Application shall validate access authorization to uploaded files.

Application Vulnerabilities Prevention – other

1.) Web application exposed to customers or internet are required for penetration test before the 1st time deployment, after every major change or conduct the test annually.
2.) Hardening and security configuration setting have to perform on the application and related system before deployment.

1.) Password Policy of "Customer login Accounts"
Minimum Password Length is 8 characters.
Password is case sensitive.
Password age is 90 days.
Password shall not be reused from last 5 password histories
Password shall not be allowed to be the same as user account name.
Password shall be forced change after first logon or after password is reset.
Password age is 15 days after generated from the system.
Password age is 7 days after password reset.
2.) Password Policy of "Login Account"
Minimum Password Length is 8 characters.
Enforce strong password)contain a mix of alphabetic and non-alphabetic(
Password age is 90 days.
Shared account is not allowed.
Password shall not be reused from last 5 password histories
Password shall not be allowed to be the same as user account name.
Password shall be forced change after first logon or after password is reset.
Password age is 15 days after generated from the system.
Password age is 7 days after password reset.
Default user and password shipped by application or system shall be changed according to password policy.
3.) Random function to generate password or key shall be used.

Connection to host or database as privilege account shall be prohibited.

Shared account and test account shall be prohibited on production environment.

4.) Prohibited excessive authentication attempts.

5.) Application should authenticate bank user with centralized LDAP.

6.) Segregate function between administrative function and user function.

Separate administrative page from other pages.

Administrator page shall be accessed from allowed network zone or IP address.

7.) Restrict user access for authorized person based on role/function.

Preventing unauthorized URL access requires selecting an approach for requiring proper authentication and proper authentication for each page.

The enforcement mechanism shall deny all access by default, requiring explicit grants to specific users and roles for access to every page .Completely disallow requests to unauthorized page types.

Predictable location of sensitive resource should not be predicted with URL direct access.

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

ฉบับที่ 3 (Doc_3)

Functional

The OTP timeout is 3 minutes.
The system shall generate OTP for one purpose only.
The system shall notify important transaction to E-mail and SMS.
The system shall lock the account after 3-5 failure login attempts and do not display specific information is failure.
The system shall be forced change password after first logon.
The system shall be forced change password after password is reset.
The system shall be used two-factor authentication before reset password.
The system shall display the last successful access.
The system shall support idle timeout less than 10 minutes before automatically logout and inactive session when transaction step is invalid.
The system shall re-authenticate when customer perform change profile by token.
The system shall re-authenticate when customer perform add favorite person for transfer money by token.
The system shall re-authenticate when customer perform change transaction limit by token.

Non-functional

The system shall use strong encryption and security protocols to safeguard sensitive data during transmission over open or public network.
The system shall encrypt information as follow: - user ID - password encryption key - database user id - database password by AES 128 bits encryption.
The system shall apply SHA 256 bits to customer password and store those hashes in database.
The system shall regenerate new session randomly when successful authentication by two-factor authentication methodology.
The system shall enforce strong password which contain a mix of alphabetic and non-alphabetic characters.
The system shall not write/store user ID and password in cookies, source code, or configuration file.
The system shall re-authority validate after access to higher authority function.
The system shall be regenerated session when change web page or new transaction.
The system shall be regenerated session when create a new transaction.

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

ฉบับที่ 4 (Doc_4)

Functional

The system will lock the account after 3 failure logins attempts and do not display information is invalid.
The system will be forced change password after first logon.
The system will be forced change password after password is reset.
The system will be used two-factor authentication before reset password.
The system will display the last login successful.
The system will support idle timeout 10 minutes before logout session when transaction step is invalid.
The system will re-authenticate when customer change profile by token.
The system will re-authenticate when customer add favorite person for transfer money by token.
The system will re-authenticate when customer perform change transaction limit by token.

Non-functional

The system will use AES encryption and SSL protocol to safeguard data during transmission over open, public networks.
The system will encrypt sensitive system information as following: - System user ID - System password - Password encryption key - Database user ID - Database password
The system will be used SHA256 to hashing customer password and store those hashes in database.
The system will regenerate new session randomly when successful authentication by two-factor authentication methodology.
The system will enforce strong password policy as following: - Minimum Password Length is 8 characters. - Password is case sensitive - Password age is 90 days. - Password shall not be reused from last 5 password histories - Password shall be forced change after first logon or after password is reset.
The system will not write/store user ID and password in cookies, source code, or configuration file.
The system will be regenerated session when change web page or new transaction.
The system will be regenerated session when create a new transaction.

ฉบับที่ 5 (Doc_5)

Internet Banking Security Requirements

Validate all input data the application using white list (what can input) for data type, format, length, and business rules before accepting the data to displayed or stored. Reject if invalid.
Minimum password requirements: Passwords must be 8 characters or longer and have at least: - 1 number - 1 lowercase letter - 1 uppercase letter - 1 special character - Change passwords every six months - Do not use the last five passwords - Do not share passwords except in emergency circumstances or when there is an overriding operational necessity.
Strong encryption and security protocols shall be used to safeguard sensitive data during transmission over open, public networks.
Web applications have authentication function and/or sensitive information shall use HTTPS to secure communication channel.
Require TLS 1.2 or higher for all sensitive pages. Non-SSL requests to these pages shall be redirected to the SSL page.
Restrict user access for authorized person based on role/function.
The enforcement mechanism shall deny all access by default, requiring explicit grants to specific users and roles for access to every page.
Completely disallow requests to unauthorized page types.
Preventing unauthorized URL access requires selecting an approach for requiring proper authentication and proper authentication for each page.
Predictable location of sensitive resource should not be predicted with URL direct access.
Hard-coded credentials information are prohibited. If need, it shall be encrypted by strong encryption.
Password shall apply strong one-way hashes to password and store those hashes in database or configuration file with appropriate access control
Use randomly assigned salts for each separate has that you generate.
Application should authenticate bank user with centralized LDAP.
Do not store any confidential information in cookies.
Use AES encryption and SSL protocol to safeguard data during transmission over open, public networks.
Use SHA256 to hashing customer password and store those hashes in database.
Regenerate new session randomly when successful authentication by two-factor authentication methodology.
Do not write/store user ID and password in cookies, source code, or configuration file.
Regenerate session when change web page or new transaction.
Regenerate session when create a new transaction.

ฉบับที่ 6 (Doc_6)

Internet Banking (SME)
Input Validation:

1. Validate all input data to the application using white list (What is allowed) for type, format, length, range, and business rules before accepting the data to be displayed or store .Reject if invalid.
2. Concatenate user input shall escape to a query or command.
3. Avoid detailed input validation error message e.g .invalid user login or password etc.

Information Confirmation:

1. Display confirmation before perform transaction.

Information Masking and Hiding:

1. Masking sensitive data while displaying or printing by star or X character
2. Avoid detailed technical error message e.g .version and name of application, database, operating system, IP address, File Name Domain Account etc.

ฉบับที่ 7 (Doc_7)

1. All input data shall validate before accepting the data to be displayed or store .Reject if invalid.
2. The detailed of technical and input error message shall avoid before displaying or printing.
3. When the user performs a dangerous operation, send a separate confirmation request to ensure that user intended to perform that operation.
4. X character shall use for masking personal information (account number, mobile number, e-mail).

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

ฉบับที่ 8 (Doc_8)

ATM
Input Validation:

1. Validate all input data to the application using white list (What is allowed) for type, format, length, range, and business rules before accepting the data to be displayed or store. Reject if invalid.
2. Concatenate user input shall escape to a query or command.
3. Avoid detailed input validation error message e.g .invalid user login or password etc.

Information Confirmation:

1. Display confirmation before perform transaction.

Information Masking and Hiding:

1. Masking sensitive data while displaying or printing by star or X character
2. Avoid detailed technical error message e.g .version and name of application, database, operating system, IP address, File Name Domain Account etc.
3. Escape store the card verification value or PIN in ATM log file.

ฉบับที่ 9 (Doc_9)

1. Shared account and test account access shall be prohibited on the production.
2. Default value or configurations that they are well-known information e.g .sa, guest account, default system account etc .shall be disabled.
3. Password Policy of "Login Account"
   - Minimum Password Length is 8 characters.
   - Enforce strong password)contain a mix of alphabetic and non-alphabetic(
   - Password age is 90 days.
   - Shared account is not allowed.
   - Password shall not be reused from last 15 password histories
   - Password shall not allowed to be the same as user account name.
   - Password shall be forced change after first logon or after password is reset.
   - Password age is 15 days after generated from the system.
   - Password age is 7 days after password reset.
   - Default user and password shipped by application or system shall be changed according to password policy.
   - Highest privilege user password shall be forced change after logon.
4. Login Account shall be locked after 3 failure login attempts.
5. Application or System log has be complied with Computer Crime Act B.E.2550
6. Application or System log has be recorded activity as follow:
   - Financial transaction log
   - All access log.
   - User activity log.

   And store at least 90 days.
7. Restrict all access for authorized based on role/function.
8. Password shall apply strong one-way hashes by SHA 256 bits and store those hashes in database or a configuration file with appropriate control
9. Confidential information shall be encrypted by RSA 2048.

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

ประวัติผู้เขียนวิทยานิพนธ์

นายกฤษดา รองรัตน์ เกิดเมื่อวันที่ 4 ตุลาคม พ.ศ. 2525 สำเร็จการศึกษาระดับปริญญาอุตสาหกรรมศาสตรบัณฑิต สาขาวิชาวิทยาการอิเล็กทรอนิกส์ จากวิทยาลัยเทคโนโลยีอุตสาหกรรม สถาบันเทคโนโลยีพระจอมเกล้าพระนครเหนือ และเข้าทำงานเป็นผู้วิเคราะห์ความต้องการด้านธุรกิจสำหรับระบบเทคโนโลยีสารสนเทศทางการธนาคาร และได้เข้าศึกษาต่อในหลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาวิศวกรรมซอฟต์แวร์ ณ ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย ในปีการศึกษา 2558 ปัจจุบันปฏิบัติงานในหน้าที่วิศวกรซอฟต์แวร์สำหรับโครงการด้านระบบเทคโนโลยีสารสนเทศทางการธนาคาร

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University