การกำหนดความต้องการความมั่นคงโดยใช้ไวยากรณ์ของแบบรูปความมั่นคง

นายกวิน สุภาพร

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต
สาขาวิชาวิศวกรรมซอฟต์แวร์ ภาควิชาวิศวกรรมคอมพิวเตอร์
คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2550

DEFINING SECURITY REQUIREMENTS USING GRAMMAR OF SECURITY PATTERNS

Mr. Kawin Supaporn

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 Computer Engineering

Chulalongkorn University

Academic Year 2007

หัวข้อวิทยานิพนธ์	การกำหนดความต้องการความมั่นคงโดยใช้ไวยากรณ์ของแบบรูปความมั่นคง
โดย	นายกวิน สุภาพร
สาขาวิชา	วิศวกรรมซอฟต์แวร์
อาจารย์ที่ปรึกษา	อาจารย์ นครทิพย์ พร้อมพูล
อาจารย์ที่ปรึกษาร่วม	อาจารย์ ธงชัย โรจน์กังสดาล

คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย อนุมัติให้นับวิทยานิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญามหาบัณฑิต

.....คณบดีคณะวิศวกรรมศาสตร์
(ศาสตราจารย์ ดร. ดิเรก ลาวัณย์ศิริ)

คณะกรรมการสอบวิทยานิพนธ์

.....ประธานกรรมการ
(อาจารย์ ดร.ยรรยง เต็งอำนวย)

.....อาจารย์ที่ปรึกษา
(อาจารย์ นครทิพย์ พร้อมพูล)

.....อาจารย์ที่ปรึกษาร่วม
(อาจารย์ ธงชัย โรจน์กังสดาล)

.....กรรมการ
(รองศาสตราจารย์ ดร. พรศิริ หมื่นไชยศรี)

กวิน สุภาพร: การกำหนดความต้องการความมั่นคงโดยใช้ไวยากรณ์ของแบบรูปความมั่นคง. (DEFINING SECURITY REQUIREMENTS USING GRAMMAR OF SECURITY PATTERNS) อ.ที่ปรึกษา: อาจารย์นครทิพย์ พร้อมพูล, อ.ที่ปรึกษาร่วม: อ. ธงชัย โรจน์กังสดาล, 159 หน้า.

วิทยานิพนธ์นี้มีวัตถุประสงค์เพื่อสร้างไวยากรณ์ความมั่นคงจากแบบรูปความมั่นคง และเครื่องมือที่นำไวยากรณ์ที่ได้มาประยุกต์ใช้ เพื่อใช้กำหนดความต้องการความมั่นคง โดยเริ่มจากการวิเคราะห์ส่วนประกอบในแบบรูปเพื่อหาองค์ประกอบสำคัญจาก 20 แบบรูป ภายใต้แบบรูปความมั่นคง 4 กลุ่ม ได้แก่ การจัดการความมั่นคงองค์กรและการจัดการความเสี่ยง การระบุตัวตนและการพิสูจน์ตัวจริง แบบจำลองควบคุมการเข้าถึง และสถาปัตยกรรมไฟล์วอลล์ แล้วสร้างเป็นแผนภาพต้นไม้ความมั่นคงเพื่อแสดงความสัมพันธ์ระหว่างองค์ประกอบของแบบรูปความมั่นคง เพื่อแปลงไปเป็นไวยากรณ์ความมั่นคงในรูปอีบีเอ็นเอฟ ทั้งนี้ไวยากรณ์ที่สร้างขึ้นได้ตรวจสอบความสมเหตุสมผลของไวยากรณ์และความสัมพันธ์ของไวยากรณ์กับผู้เชี่ยวชาญและมีประสบการณ์ด้านความมั่นคง เพื่อปรับปรุงไวยากรณ์ให้มีความถูกต้องและสมบูรณ์มากขึ้น

ผู้วิจัยได้สร้างเครื่องมือบนพื้นฐานไวยากรณ์ความมั่นคงที่สร้างขึ้น เพื่อนำเงื่อนไขบังคับของไวยากรณ์มาประยุกต์ใช้ และให้ผู้ใช้สามารถป้อนข้อมูลนำเข้าที่จำเป็นต่อการสร้างความต้องการความมั่นคง ผลลัพธ์ที่ได้จากเครื่องมือคือ ความต้องการที่มีองค์ประกอบด้านความมั่นคงในรูปประโยคภาษาอังกฤษ จากนั้นผู้วิจัยได้ทดสอบไวยากรณ์ความมั่นคงโดยให้หน่วยทดลอง 12 คนที่มีประสบการณ์ด้านความมั่นคง ทดลองใช้เครื่องมือเพื่อกำหนดความต้องการความมั่นคงสำหรับสถานการณ์จำลอง 3 ระบบ ได้แก่ ระบบบริการเอฟทีพี ระบบธนาคารออนไลน์ และระบบสำหรับห้องปฏิบัติการ แล้วให้หน่วยทดลองประเมินระดับความพึงพอใจต่อปัจจัยที่พิจารณาต่างๆ พร้อมทั้งเสนอปัญหาและข้อเสนอแนะจากการใช้เครื่องมือที่สร้างขึ้น ผลการทดลองแสดงให้เห็นว่า คุณภาพของความต้องการความมั่นคงเพิ่มขึ้นมากกว่าการไม่ใช้เครื่องมือ ช่วยให้ผู้ใช้เกิดการเรียนรู้ในการกำหนดความต้องการ และสนับสนุนการนำกลับมาใช้ใหม่ได้

ผลที่ได้รับจากงานวิจัยนี้คือ ไวยากรณ์ความมั่นคงจากแบบรูปความมั่นคง และเครื่องมือในการกำหนดความต้องการความมั่นคง สามารถใช้เป็นแนวทางในการกำหนดความต้องการความมั่นคงได้อย่างถูกต้อง ครบถ้วน มีคุณภาพมากขึ้น และช่วยลดเวลาและค่าใช้จ่ายที่จะต้องใช้ในกระบวนการวิศวกรรมความต้องการในการระบุความต้องการด้านความมั่นคงได้

ภาควิชา วิศวกรรมคอมพิวเตอร์	ลายมือชื่อนิสิต กวิน สุภาพร
สาขาวิชา วิศวกรรมซอฟต์แวร์	ลายมือชื่ออาจารย์ที่ปรึกษา นครทิพย์ พร้อมพูล
ปีการศึกษา 2550	ลายมือชื่ออาจารย์ที่ปรึกษาร่วม

4870215021 : MAJOR SOFTWARE ENGINEERING
KEYWORD: SOFTWARE REQUIREMENTS ENGINEERING / SECURITY / SECURITY REQUIREMENTS / PATTERNS / SECURITY PATTERNS / REQUIREMENTS PATTERN / REQUIREMENT DEFINITION

KAWIN SUPAPORN: (DEFINING SECURITY REQUIREMENTS USING GRAMMAR OF SECURITY PATTERN) THESIS ADVISOR: NAKORNTIP PROMPOON THESIS COADVISOR: THONGCHAI ROJKANGSADAN, 159 pp.

The objective of this thesis is to construct security grammars from security patterns and a tool based on the constructed security grammars in order to define security requirements. The elements of each 20 pattern from 4 security pattern types; Enterprise Security and Risk Management, Identification and Authentication, Access Control Model and Firewall Architecture are analyzed to develop a security tree. Each tree represents the relationship among elements of a single security pattern and is used to construct the security grammars in Extended Backus-Naur Form (EBNF). To improve the correctness and completeness, the security grammars and their relations are validated.

A supporting tool is also developed with security grammar constraints. The results obtained from using the tool are security requirements in English language which a user may have to input the required components.

To test the quality of security grammars, 12 security experts are selected as sample units to use the tool in the simulated scenarios from FTP System, On-line Banking System and Laboratory Supporting System. After using the tool, they evaluate the satisfaction level in various factors and also identify problems and recommendations. The experimental results are that the quality of security requirements created from tools is better than the creation without it. Also, it directly helps users learn to define the security requirements and reuse the constructed security requirements.

The results from this research are security grammars based on security patterns and a supporting tool. They can be used to improve defining security requirements in both correctness and completeness factor, and also reduce cost and time in requirements engineering process.

Department Computer Engineering	Student's signature Kawin Supaporn
Field of Study Software Engineering	Advisor's signature Nakorntip Prompoon
Academic Year 2007	Co-advisor's signature Thongchai Roj

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้สำเร็จลุล่วงไปได้ด้วยความช่วยเหลือจาก อาจารย์นครทิพย์ พร้อมพูล อาจารย์ที่ปรึกษาวิทยานิพนธ์ของข้าพเจ้า และอาจารย์ธงชัย โรจน์กังสดาล อาจารย์ที่ปรึกษาร่วมของข้าพเจ้า ขอกราบขอบพระคุณอาจารย์ทั้งสองท่านที่ได้ให้คำแนะนำทางด้านการศึกษา คุณธรรม จริยธรรมและข้อเสนอแนะต่างๆ ตลอดจนคอยดูแลให้การทำวิทยานิพนธ์นี้สำเร็จลุล่วงด้วยดี

ขอกราบขอบพระคุณอาจารย์ ดร.ยรรยง เต็งอำนวย เป็นประธานกรรมการสอบวิทยานิพนธ์ และรองศาสตราจารย์ ดร.พรศิริ หมื่นไชยศรี เป็นกรรมการสอบวิทยานิพนธ์ ซึ่งได้สละเวลาและให้คำแนะนำต่างๆ ในการสอบวิทยานิพนธ์ของข้าพเจ้าอย่างดียิ่ง

ขอบคุณรุ่นพี่ เพื่อนๆ และรุ่นน้อง ที่ช่วยสละเวลามาทดสอบในงานวิทยานิพนธ์ชิ้นนี้ สุดท้ายนี้ขอกราบขอบพระคุณบิดา มารดา และเพื่อนๆ ทุกคนที่คอยให้กำลังใจและให้ความสนับสนุนมาโดยตลอด

สารบัญ

หน้า

หน้า

หน้า

สารบัญรูปภาพ

หน้า

หน้า

หน้า

สารบัญตาราง

หน้า

หน้า

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญ

วิศวกรรมความต้องการซอฟต์แวร์ถือเป็นกระบวนการสำคัญในกระบวนการพัฒนาซอฟต์แวร์ ซึ่งมุ่งเน้นการรวบรวมข้อกำหนดความต้องการต่างๆ จากผู้ที่เกี่ยวข้อง มาวิเคราะห์เพื่อออกแบบระบบให้ถูกต้องและครบถ้วนตามความต้องการที่ได้ แต่เนื่องจากข้อกำหนดความต้องการนั้นมีหลายประเภท อีกทั้งมีความซับซ้อนและมีความต้องการที่หลากหลาย ส่งผลให้ผู้พัฒนาระบบต้องหาเครื่องมือหรือขั้นตอนวิธีเพื่อบริหารจัดการกับความต้องการดังกล่าวให้เป็นไปอย่างเหมาะสม จากความต้องการที่มีหลากหลายประเภทนี้เองทำให้ผู้พัฒนาระบบส่วนใหญ่มักมุ่งเน้นการวิเคราะห์และออกแบบความต้องการเชิงหน้าที่ (Functional Requirements) มากกว่าความต้องการไม่ใช่หน้าที่ (Non-Functional Requirements) หรือเรียกอีกอย่างหนึ่งว่าความต้องการเชิงคุณภาพ (Quality Requirements) เพราะความต้องการเชิงหน้าที่เป็นความต้องการหลักที่ผู้ใช้ต้องการในการทำงาน และเป็นความต้องการที่มองเห็นผลลัพธ์การทำงานได้อย่างชัดเจน แม้ปัจจุบันจะมีเครื่องมือช่วยในการวิเคราะห์ ออกแบบ และพัฒนาระบบให้มีประสิทธิภาพมากขึ้นแล้วก็ตาม กลับพบว่าระบบไม่สามารถทำงานได้ตามความต้องการของผู้ใช้ ซึ่งเกิดจากการละเลยความต้องการเชิงคุณภาพบางอย่าง โดยเฉพาะความต้องการด้านความมั่นคง (Security Requirements) ซึ่งเป็นความต้องการเชิงคุณภาพประเภทหนึ่ง ที่เกี่ยวข้องกับจุดอ่อนของระบบ และวิธีป้องกันจุดอ่อนดังกล่าวจากการโจมตีระบบ ซึ่งหากมีการพิจารณาและการจัดการที่ถูกต้อง จะทำให้ช่วยลดเวลาและค่าใช้จ่ายในการแก้ปัญหาและกู้คืนระบบจากการโจมตีได้ในระดับหนึ่ง

ความต้องการความมั่นคง เป็นความต้องการที่เกี่ยวข้องกับการตรวจหาจุดอ่อนที่อาจปรากฏในระบบ ว่ามีความเสี่ยงในการถูกโจมตีเพียงใด และจะมีผลกระทบอย่างไรบ้างหากถูกโจมตีในจุดดังกล่าว รวมถึงการเสนอแนวทางป้องกันและกู้คืนระบบจากการโจมตี จึงถือว่าเป็นความต้องการที่จำเป็นและขาดไม่ได้ในการพัฒนาระบบ ปัจจุบันจึงมีการสนับสนุนให้ความต้องการความมั่นคงเป็นหนึ่งในกระบวนการวิศวกรรมความต้องการซอฟต์แวร์เชิงหน้าที่ ภายใต้ตัววัดคุณภาพผลิตภัณฑ์ (Product Quality Metric) [1] โดยความต้องการนี้จะครอบคลุม ทั้ง 2 มุมมอง ได้แก่ ความมั่นคงของข้อมูลสารสนเทศ และเทคโนโลยีที่ใช้ในระบบ ซึ่งสอดคล้องกับนโยบายความมั่นคงในองค์กร ปัจจุบันนโยบายด้านความมั่นคงที่นิยมกันมาก คือ ISO/IEC 17799 [2] ซึ่งพัฒนาต่อยอดมาจากมาตรฐาน BS 7799 (ปัจจุบันคือ ISO/IEC 17799:2005) โดยประเทศญี่ปุ่นมีองค์กรมากกว่า 900 องค์กรที่ได้รับการรับรองมาตรฐาน BS 7799 และ

BS 7799-2 (ปัจจุบันคือ ISO/IEC 27001) แสดงถึงการให้ความสำคัญด้านความมั่นคงขององค์กรต่างๆ เป็นลำดับต้นๆ ขององค์กร [NECTEC]

อย่างไรก็ตามการกำหนดความต้องการด้านความมั่นคงนั้นอาจทำได้ยาก เนื่องจากผู้ใช้หรือผู้พัฒนาอาจมีความรู้และประสบการณ์ด้านความมั่นคงนั้นไม่เพียงพอ อีกทั้งความต้องการดังกล่าวล้วนแล้วแต่มีผลต่อการวิเคราะห์และออกแบบระบบจากความต้องการเชิงหน้าที่ ดังนั้นวิธีหนึ่งที่สามารถทำได้ คือ การใช้ความต้องการที่ผู้ชำนาญการเคยออกแบบไว้กับระบบที่ใกล้เคียงมาประยุกต์ใช้กับระบบที่กำลังพัฒนาอยู่ และรองรับการใช้ซ้ำได้ (Reuse) จึงสามารถนำมาแก้ปัญหาที่คล้ายๆ กันได้ หรือที่รู้จักกันว่า แบบรูป (Pattern)

แบบรูป [3],[4] คือ การรวบรวมการออกแบบที่ดีที่สามารถนำกลับมาใช้ใหม่ได้ในแง่ของการนำวัตถุประสงค์และฟังก์ชันมาใช้ซ้ำ (Objective and Function Reuse) โดยแบบรูปมีวัตถุประสงค์เพื่อนำเสนอผลเฉลย (Solution) สำหรับปัญหาการออกแบบทั่วไปที่ปรากฏคล้ายกัน ช่วยให้ผู้พัฒนาสามารถเข้าใจและนำไปใช้ได้ โดยไม่ต้องอาศัยความรู้หรือประสบการณ์มากนัก เนื่องจากแบบรูปนั้นมีหลากหลายประเภท ดังนั้นแบบรูปจึงสามารถนำไปใช้ได้ในทุกๆ ขั้นตอนของกระบวนการพัฒนาซอฟต์แวร์ได้เป็นอย่างดี แต่ในวิทยานิพนธ์นี้จะพิจารณาเพียงแบบรูปความต้องการ (Requirements Pattern) ซึ่งเป็นตัวกลางในการถ่ายทอดองค์ความรู้ ที่สามารถนำไปใช้แก้ปัญหาในกระบวนการวิศวกรรมความต้องการซอฟต์แวร์ได้ เพื่อเพิ่มความไว้วางใจอันเนื่องมาจากความสำเร็จของระบบก่อนหน้าเป็นประกัน ทั้งยังช่วยลดความเสี่ยง และค่าใช้จ่ายในการพัฒนาได้อีกด้วย สำหรับความต้องการความมั่นคงก็มีแบบรูป ที่เรียกว่า แบบรูปความต้องการความมั่นคง (Security Requirements Pattern) [5] ซึ่งช่วยแก้ปัญหาด้านความมั่นคงที่เคยปรากฏมาแล้วในอดีต ทำให้การพัฒนาซอฟต์แวร์โดยใช้แบบรูปความมั่นคง มีความถูกต้องครอบคลุมปัญหา และมีความรวดเร็วในการพัฒนา โดยเฉพาะอย่างยิ่งระบบความมั่นคง ที่เคร่งครัดในเรื่องการป้องกัน (Prevention) การตรวจหา (Detection) และ การกู้คืน (Recovery) ของระบบ

จากการศึกษางานวิจัยที่สนับสนุนกระบวนการความต้องการซอฟต์แวร์ พบว่างานวิจัยส่วนใหญ่มุ่งเน้น การนำเสนอเทคนิคและขั้นตอนวิธี ในการให้ได้มาซึ่งความต้องการ และการวิเคราะห์ความต้องการ แต่มีส่วนน้อยให้การสนับสนุนความต้องการด้านความมั่นคง เช่น N. R. Mead และคณะ [8] ได้นำเสนอขั้นตอนสำหรับการรวบรวม จัดกลุ่ม และลำดับความสำคัญให้กับความต้องการความมั่นคงในโครงการพัฒนาซอฟต์แวร์ เพื่อช่วยให้สามารถเข้าใจความต้องการความมั่นคงขององค์กรได้ และ A.V. Lamsweerde และคณะ [9] ได้นำเสนอการพิจารณาองค์ประกอบด้านความมั่นคงต่างๆ เพื่อเป็นแนวทางในการรวบรวมความต้องการความมั่นคง อย่างไรก็ตามหากนำขั้นตอนดังกล่าวไปปฏิบัติจริง จะต้องมีการศึกษาขั้นตอนการดำเนินการ

เพื่อที่จะสร้างความต้องการความมั่นคง กอปรกับข้อจำกัดด้านเวลาและค่าใช้จ่ายในการพัฒนา จึงอาจมีโอกาสน้อยมากที่จะนำขั้นตอนวิธีดังกล่าวไปใช้ในโครงการพัฒนาซอฟต์แวร์ทั่วๆ ไป

ดังนั้นในงานวิทยานิพนธ์นี้จะมุ่งเน้นศึกษาและวิเคราะห์แบบรูปความมั่นคง ที่มีการนำเสนอไว้ในหนังสือแบบรูปความมั่นคง การบูรณาการความมั่นคงและวิศวกรรมระบบ (Security Patterns: Integrating Security and Systems Engineering) [6] นำมาสร้างเป็นไวยากรณ์สำหรับกำหนดความต้องการความมั่นคง เพื่อแก้ปัญหาการกำหนดความต้องการความมั่นคงให้มีความเหมาะสมกับระบบที่กำลังพิจารณาได้ตั้งแต่เริ่มแรกของกระบวนการพัฒนาซอฟต์แวร์ พร้อมทั้งพัฒนาเครื่องมือที่นำไวยากรณ์ดังกล่าวมาใช้กำหนดความต้องการความมั่นคงที่มีอยู่จริง ซึ่งสามารถสนับสนุนการพัฒนาระบบความมั่นคงตามความต้องการดังกล่าวได้อย่างเหมาะสมและมีประสิทธิภาพมากยิ่งขึ้น

1.2 วัตถุประสงค์ของการวิจัย

1) สร้างไวยากรณ์เพื่อใช้สำหรับสร้างข้อกำหนดความต้องการด้านความมั่นคงจากแบบรูปความมั่นคง

2) สร้างเครื่องมือโดยนำไวยากรณ์ที่ได้มาประยุกต์ใช้ เพื่อใช้ในการกำหนดความต้องการความมั่นคงของระบบที่เกี่ยวข้องกับความมั่นคง

1.3 ขอบเขตของงานวิจัย

1.3.1 นำเสนอไวยากรณ์สำหรับการสร้างความต้องการความมั่นคง โดยใช้แบบรูปความมั่นคงที่ได้รับการออกแบบและตรวจสอบความถูกต้องแล้ว 4 กลุ่มแบบรูปดังต่อไปนี้

1) **การจัดการความมั่นคงองค์กรและการจัดการความเสี่ยง (Enterprise Security and Risk Management)**

เป็นกลุ่มแบบรูปความมั่นคงที่เกี่ยวข้องกับการจัดการ 4 เรื่อง ได้แก่ การระบุความจำเป็นพื้นฐาน การประเมินความเสี่ยง แนวคิดและการบริการความมั่นคง และการให้ความสำคัญกับติดต่อกับภายนอกองค์กร ซึ่งแบบรูปความมั่นคงในกลุ่มนี้ประกอบด้วย

(1) การระบุความต้องการความมั่นคงสำหรับสินทรัพย์ขององค์กร (Security Needs Identification for Enterprise Assets)

(2) การประเมินมูลค่าสินทรัพย์ (Asset Valuation)

(3) การประเมินภัยคุกคาม (Threat Assessment)

(4) การประเมินภาวะเสี่ยง (Vulnerability Assessment)

(5) การกำหนดความเสี่ยง (Risk Determination)

(6) แนวคิดความมั่นคงขององค์กร (Enterprise Security Approaches)

(7) บริการความมั่นคงขององค์กร (Enterprise Security Services)

(8) การสื่อสารของผู้มีหุ้นส่วนในองค์กร (Enterprise Partner Communication)

2) **การระบุตัวตนและการพิสูจน์ตัวจริง (Identification and Authentication: I&A)**

เป็นกลุ่มแบบรูปความมั่นคงที่มุ่งเน้นการตรวจสอบปฏิสัมพันธ์ต่างๆ ระหว่างผู้ใช้กับระบบ ซึ่งรองรับการบริการด้านการระบุและยืนยันตัวตนแบบต่างๆ ตามความต้องการที่ระบุไว้กลุ่มแบบรูปการจัดการความมั่นคงองค์กรและการจัดการความเสี่ยง ซึ่งแบบรูปความมั่นคงในกลุ่มนี้ประกอบด้วย

(1) ความต้องการด้านการระบุและการพิสูจน์ตัวตน (I&A Requirements)

(2) ทางเลือกการออกแบบสำหรับการระบุและการพิสูจน์ตัวตนแบบอัตโนมัติ (Automated I&A Design Alternatives)

(3) การออกแบบและใช้รหัสผ่าน (Password Design and Use)

(4) ทางเลือกการออกแบบสำหรับแบบชีวมิติ (Biometric Design Alternatives)

3) **แบบจำลองควบคุมการเข้าถึง (Access Control Model)**

แบบรูปในกลุ่มนี้มุ่งเน้นการกำหนดเงื่อนไขบังคับ (Constraints) ในระดับต่างๆ ไม่ว่าจะเป็นสถาปัตยกรรม โปรแกรมประยุกต์ และข้อบังคับในระดับล่างๆ ของการปฏิบัติงาน ซึ่งแบบรูปความมั่นคงในกลุ่มนี้ประกอบด้วย

(1) การให้อำนาจ (Authorization)

(2) การควบคุมการเข้าถึงเชิงบทบาท (Role-Based Access Control)

(3) ความมั่นคงหลายระดับ (Multilevel Security)

(4) การตรวจสอบการเข้าถึงทรัพยากร (Reference Monitor)

(5) การกำหนดสิทธิ์ให้กับบทบาท (Role Right Definition)

4) **สถาปัตยกรรมไฟร์วอลล์ (Firewall Architecture)**

แบบรูปในกลุ่มนี้มุ่งเน้นการการกำหนดเงื่อนไขบังคับสำหรับการติดต่อระหว่างกันผ่านทางระบบเครือข่าย (Network) เพื่อป้องกันการโจมตีหรือปลอมปนทั้งจากภายนอกและภายในองค์กร ซึ่งแบบรูปความมั่นคงในกลุ่มนี้ประกอบด้วย

(1) ไฟร์วอลล์สำหรับการกรองแพ็คเกจ (Packet Filtering Firewall)

(2) ไฟร์วอลล์เชิงตัวแทน (Proxy-Based Firewall)

(3) ไฟร์วอลล์เชิงสถานะ (Stateful Firewall)

1.3.2 สร้างเครื่องมือเพื่อนำไวยากรณ์ที่ได้จาก 3.1 มาประยุกต์ใช้ในการกำหนดความต้องการความมั่นคงของระบบ

1.3.3 ทดสอบเครื่องมือ โดยใช้ผู้ทดลอง 12 คนที่มีประสบการณ์ด้านความมั่นคง มากำหนดความต้องการความมั่นคงจากสถานการณ์จำลองที่ครอบคลุมแบบรูปความมั่นคงในงานวิทยานิพนธ์นี้ เพื่อวัดระดับความพึงพอใจ และรับข้อเสนอแนะจากผู้ทดลอง เพื่อทำการปรับปรุงไวยากรณ์

1.4 ขั้นตอนการวิจัย

1) ศึกษาความต้องการความมั่นคง แบบรูปความมั่นคง และวิศวกรรมความต้องการซอฟต์แวร์สำหรับระบบความมั่นคง

2) วิเคราะห์แบบรูปความต้องการความมั่นคงเพื่อหาโครงสร้าง องค์ประกอบหลัก และความสัมพันธ์ระหว่างองค์ประกอบ

3) สร้างไวยากรณ์ความมั่นคงที่สอดคล้องกับแบบรูปความมั่นคงได้อย่างสมเหตุสมผล

4) บูรณาการไวยากรณ์ ที่สร้างจากแบบรูปความมั่นคง เพื่อให้เกิดความสมบูรณ์ของไวยากรณ์

5) สร้างเครื่องมือเพื่อนำไวยากรณ์ความมั่นคงมาใช้ในการกำหนดความต้องการความมั่นคงได้

6) ทดสอบเครื่องมือ เพื่อวัดระดับความพึงพอใจ และข้อเสนอแนะจากผู้ทดลองที่ใช้เครื่องมือในการสร้างความต้องการความมั่นคง

7) ปรับปรุงไวยากรณ์สำหรับการกำหนดความมั่นคง นำเสนอแนวทางในการพัฒนา และสรุปผลงานวิจัย

8) จัดทำวิทยานิพนธ์

1.5 ประโยชน์ที่คาดว่าจะได้รับ

1) ได้ไวยากรณ์เพื่อใช้สำหรับสร้างข้อกำหนดความต้องการด้านความมั่นคง

2) ได้เครื่องมือที่นำไวยากรณ์ที่ได้ไปใช้จริงเพื่อสร้างข้อกำหนดความต้องการด้านความมั่นคง

3) สามารถสนับสนุนการกำหนดความต้องการด้านความมั่นคงได้อย่างมีประสิทธิภาพและถูกต้องมากขึ้น เพื่อนำความต้องการความมั่นคงดังกล่าวไปใช้ในกระบวนการต่างๆ ของการพัฒนาซอฟต์แวร์ต่อไปได้

บทที่ 2
ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

ในบทนี้จะกล่าวถึงทฤษฎีที่เกี่ยวข้องกับการกำหนดความต้องการความมั่นคง ซึ่งประกอบด้วยวิศวกรรมความต้องการซอฟต์แวร์ แบบรูปและแบบรูปสำหรับซอฟต์แวร์ วิศวกรรมความมั่นคงและความต้องการความมั่นคง และอีบีเอ็นเอฟ (EBNF) นอกจากนี้จะกล่าวถึงงานวิจัยที่เกี่ยวข้อง ได้แก่ กรอบงานสำหรับวิศวกรรมความต้องการความมั่นคง แบบรูปข้อกำหนดแบบเรียลไทม์ โครงแบบความมั่นคงของเว็บเซอร์วิส และออนโทโลจี (Ontology) ความต้องการความมั่นคงในเอกสารควบคุมในเอกสารที่มีการควบคุม ซึ่งมีรายละเอียดดังต่อไปนี้

2.1 ทฤษฎีที่เกี่ยวข้อง

2.1.1 วิศวกรรมความต้องการซอฟต์แวร์ (Software Requirements Engineering)

วิศวกรรมความต้องการซอฟต์แวร์เป็นส่วนหนึ่งของวิศวกรรมซอฟต์แวร์ ถูกกำหนดขึ้นในช่วงการเริ่มต้นของกระบวนการพัฒนาซอฟต์แวร์ โดยมีจุดหมายในการให้ได้มาซึ่งความต้องการด้านซอฟต์แวร์ที่ถูกต้อง และชัดเจนเพื่อนำไปใช้ในการกำหนดระบบที่จะทำการพัฒนา โดยมีกระบวนการสำคัญ [10] มีดังนี้

1) การเก็บรวบรวมความต้องการ (Requirements Elicitation) เป็นกระบวนการที่จะเข้าไปเกี่ยวข้องกับผู้ใช้ระบบโดยตรง โดยมีจุดประสงค์ในการเก็บข้อมูลที่จะนำมาใช้ในการกำหนดตัวระบบ

2) การวิเคราะห์ความต้องการ (Requirements Analysis) เป็นกระบวนการวิเคราะห์ความต้องการว่าใครบ้างที่เกี่ยวข้องกับระบบ ระบบจะทำอะไร และระบบจะถูกใช้เมื่อไรและใช้อย่างไร

3) การจัดทำข้อกำหนดความต้องการ (Requirements Specification) เป็นกระบวนการใน การจัดทำข้อกำหนดตัวระบบ ให้ได้รายละเอียดของระบบที่จะพัฒนาขึ้น ซึ่งเป็นผลลัพธ์ที่สำคัญที่ได้จากกระบวนการวิศวกรรมความต้องการซอฟต์แวร์

4) การประเมินความต้องการ (Requirements Validation) เป็นการตรวจสอบความถูกต้องของความต้องการที่เก็บมา เช่น ความต้องการที่เก็บมาได้นั้นมีความสอดคล้องกันหรือไม่ มีการจัดระดับความสำคัญของความต้องการอย่างไร

5) การบริหารความต้องการ (Requirements Management) เป็นการบริหารกระบวนการวิศวกรรมความต้องการซอฟต์แวร์ ควบคุม ดูแลคุณภาพและความถูกต้องของความ

ต้องการ การผลิตความต้องการ ตลอดจนการบริหารความต้องการที่มีการเปลี่ยนแปลง (Requirements Change)

กระบวนการวิศวกรรมความต้องการซอฟต์แวร์เป็นกระบวนการหนึ่งที่มีความสำคัญในการพัฒนาซอฟต์แวร์ ความผิดพลาดหรือความไม่สมบูรณ์ที่เกิดในกระบวนการนี้มักก่อให้เกิดค่าใช้จ่ายที่สูงกว่าผลของ ความผิดพลาดที่เกิดจากกระบวนการพัฒนาซอฟต์แวร์ในส่วนอื่นๆ และมีความเกี่ยวข้องสัมพันธ์กับผู้ใช้หรือผู้พัฒนาของระบบอย่างมาก โดยท้ายที่สุดแล้ววัตถุประสงค์ของวิศวกรรมความต้องการซอฟต์แวร์นั้น เพื่อให้ได้ ผลลัพธ์ 3 สิ่ง คือ การยอมรับในความต้องการ (Agreed Requirements) ข้อกำหนดของระบบ (System Specification) และแบบจำลองระบบ (System Model)

2.1.2 แบบรูปและแบบรูปสำหรับซอฟต์แวร์ (Patterns and Software Patterns)

แบบรูปถูกนำเสนอครั้งแรกเพื่อใช้แก้ปัญหางานด้านสถาปัตยกรรม หลังจากนั้น Ward Cunningham และ Kent Beck ได้นำแบบรูปมาใช้ในการออกแบบส่วนประสานผู้ใช้โดยใช้ภาษาสมอล์ลทอล์ค (Smalltalk) เป็นครั้งแรกและได้รับความนิยมเป็นอย่างมาก หลังจากนั้นก็มีการนำแบบรูปไปใช้ในวงการซอฟต์แวร์อย่างแพร่หลาย เช่น แบบรูปการวิเคราะห์ระบบ แบบรูปการเขียนโปรแกรม แบบรูปสถาปัตยกรรม เป็นต้น

แบบรูป [11] คือ ปัญหาและผลเฉลย ที่เคยปรากฏในอดีต โดยการเตรียมผลเฉลยจากปัญหาหนึ่ง นำมาแก้ปัญหาที่ปรากฏใหม่ซึ่งมีลักษณะคล้ายกับปัญหาเดิมในแบบรูปนั้น แบบรูปประกอบด้วยองค์ประกอบหลัก 3 ส่วน คือ ปัญหา ลักษณะ และผลเฉลย แต่การนำแบบรูปไปใช้นั้นอาจต้องมีองค์ประกอบอื่นเพิ่มเติม เพื่อช่วยให้แบบรูปมีความสมบูรณ์และง่ายต่อการนำไปใช้ เช่น ชื่อแบบรูป (Pattern Name) ฟอร์ซ (Force) ผลลัพธ์เชิงบริบท (Resulting Context) แบบรูปที่เกี่ยวข้อง (Related Patterns) รวมทั้งองค์ประกอบสนับสนุนที่จะช่วยในการอธิบายผลเฉลยของแบบรูปนั้นๆ เช่น ตัวอย่าง (Example) แผนภาพคลาส (Class Diagram) ซึ่งใช้ในแบบรูปการออกแบบ เป็นต้น องค์ประกอบเหล่านี้จะขึ้นอยู่กับประเภทของการนำแบบรูปไปใช้งาน เพื่อที่จะสามารถอธิบาย สนับสนุนการใช้ หรือช่วยในการทำความเข้าใจในปัญหา หรือการแก้ปัญหาที่จะนำเสนอได้ชัดเจนขึ้น

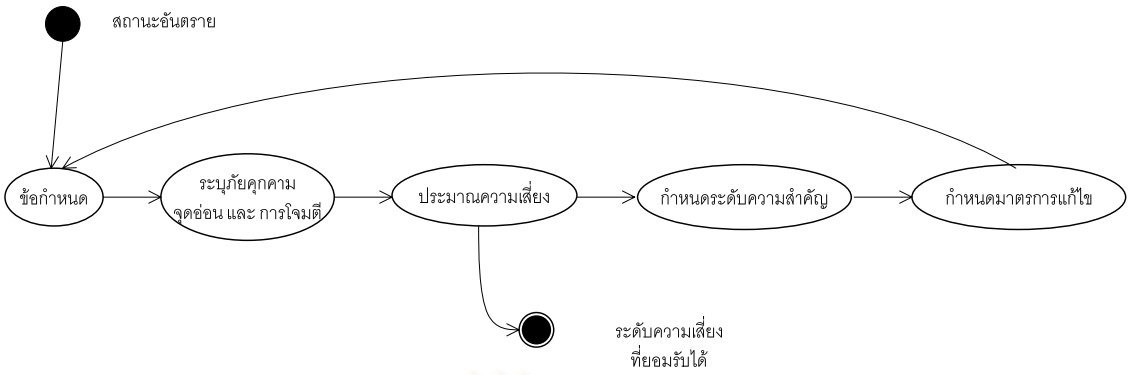
แบบรูปการออกแบบ (Design Pattern) เป็นแบบรูปที่ได้รับความนิยมในการนำไปใช้อย่างกว้างขวาง และเป็นแบบรูปที่นำมาใช้กับกระบวนการพัฒนาซอฟต์แวร์อย่างได้ผล แบบรูปการออกแบบที่ใช้กันแพร่หลายที่สุด คือ แบบรูปที่นำเสนอโดย E. Gamma และคณะ [12] ซึ่งมีองค์ประกอบของแบบรูปการออกแบบโดยเปรียบเทียบกับแบบรูปความมั่นคงที่นำเสนอโดย M. Schumacher [6] ดังแสดงให้เห็นในตารางที่ 2.1 (ความหมายของแต่ละองค์ประกอบแสดงไว้ในภาคผนวก ก)

ตารางที่ 2.1 องค์ประกอบของเอกสารแบบรูปความมั่นคงเทียบกับแบบรูปการออกแบบ

แบบรูปเอกสาร (Document Patterns)	**แบบรูปการออกแบบ โดย** E.Gamma	**แบบรูปความมั่นคง โดย** M. Schumacher
ชื่อแบบรูป (Pattern name)	มี	มี
ชื่อที่รู้จัก (Also Known As)	มี	มี
แรงบันดาลใจ (Motivate)	มี	ปัญหา (Problem)
เจตนา (Intent)	มี	-
ผลที่ได้(Consequence)	มี	มี
แบบรูปที่เกี่ยวข้อง (Related pattern)	มี	คล้ายกับ (See also)
การนำไปใช้ที่ทราบ (Known Use)	มี	ตัวอย่าง (Example)
ตัวอย่างโปรแกรม (Sample Code)	มี	ผลเฉลย (Solution)
การนำไปปรับใช้ (Applicability)	มี	บริบท (Context)
การทำให้เกิดผล (Implementation)	มี	มี
ลักษณะทางโครงสร้าง (Structure)	มี	มี
สิ่งที่เข้ามาเกี่ยวข้อง (Participants)	มี	-
การร่วมมือ (Collaboration)	มี	-
ไดนามิก (Dynamic)	-	มี
ตัวอย่างการแก้ไข (Example Resolved)	-	มี
รูปแปร (Variants)	-	มี

2.1.3 **วิศวกรรรมความมั่นคง และความต้องการด้านความมั่นคง** (Security Engineering and Security Requirements)

วิศวกรรมความมั่นคง เป็นหลักการนำทฤษฎีความมั่นคง (Security Theory) มาใช้ในกิจกรรมความมั่นคง (Security Practice) หรืออีกนัยหนึ่ง คือ การออกแบบและสร้างระบบที่สามารถป้องกันการโจมตีต่างๆ ได้ โดยมีวัตถุประสงค์เพื่อเปลี่ยนแปลงสถานะจากอันตรายเป็นสถานะความเสี่ยงที่ยอมรับได้ ซึ่งกระบวนการที่จำเป็นในวิศวกรรมความมั่นคง [11, 13] แสดงได้ดังรูปที่ 2.1 โดยมีรายละเอียดดังนี้



รูปที่ 2.1ขั้นตอนวิธีทางวิศวกรรมความมั่นคง

1) ข้อกำหนด (Specification) เป็นส่วนประกอบ (Components) และ ส่วนต่อประสาน (Interface) ทั้งหมดที่ต้องกำหนดให้สมบูรณ์ เพราะถ้าหากไม่ครอบคุลมข้อกำหนดของสถาปัตยกรรมทั้งหมดของระบบ จะก่อให้เกิดช่วงโหว่ ภัยอันตราย และการถูกโจมตี ในส่วนที่ยังไม่ได้ทำการระบุเป็นข้อกำหนดไว้

2) ระบุภัยคุกคาม จุดอ่อน และการโจมตี (Identification of Threats, Vulnerabilities and Attacks) เป็นการระบุภัยอันตรายและจุดอ่อนของแต่ละองค์ประกอบ รวมถึงส่วนต่อประสานของระบบที่ระบุไว้แล้ว ซึ่งจะช่วยในการกำหนดรูปแบบการโจมตีที่จะเกิดและสามารถทำการป้องกันไว้ได้ก่อนได้

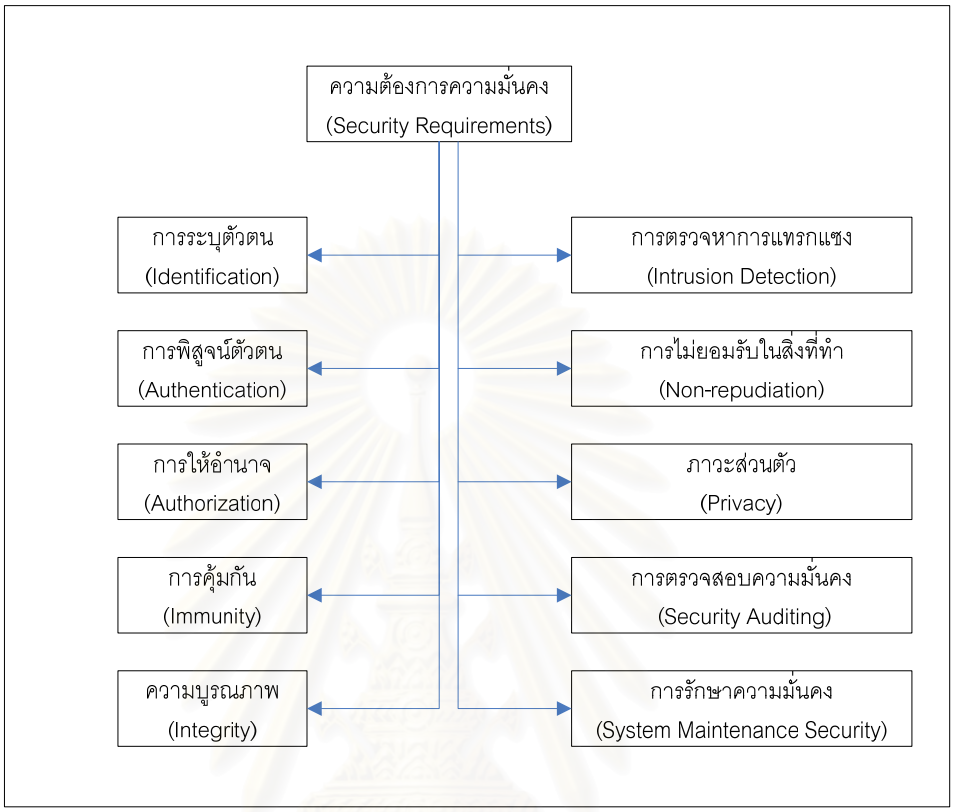
3) ประมาณความเสี่ยง (Risk Estimation) ความเสี่ยงของการโจมตีที่อาจเกิดกับแต่ละองค์ประกอบ หรือส่วนต่อประสาน จะต้องพิจารณาตามความสัมพันธ์ระหว่าง ข้อกำหนดของภัยคุกคาม จุดอ่อน และรูปแบบการโจมตี

4) กำหนดระดับความสำคัญ (Prioritization) ในกรณีที่มีความเสี่ยงสูงปรากฏในจุดอ่อนที่เกี่ยวข้องกับองค์ประกอบ หรือส่วนประสานที่อันตราย (Jeopardize) จะต้องจัดลำดับความสำคัญไว้เป็นลำดับต้นๆ ซึ่งถือว่าขั้นตอนนี้เป็นขั้นตอนที่สำคัญมากในการกำหนดมาตรการป้องกัน

5) มาตรการแก้ไข (Countermeasure) ซึ่งจำแนกตามภัยคุกคาม จุดอ่อน และรูปแบบการโจมตีทั้งนี้ขึ้นกับความสำคัญและประเภทของภัยอันตราย

การระบุข้อกำหนดความต้องการ (Requirements Specification) เป็นสิ่งที่สำคัญในทุกๆ โครงการ ถ้าความต้องการดังกล่าวไม่เป็นไปตามข้อกำหนดที่เหมาะสม ระบบก็ไม่สามารถทำงานตามที่คาดหวังไว้ได้ เช่นเดียวกับระบบที่ต้องการความมั่นคง หากความต้องการความมั่นคงไม่ถูกกำหนดไว้อย่างเหมาะสมในช่วงแรกๆ ของการเริ่มโครงการ ความเสี่ยงและค่าใช้จ่ายก็จะเพิ่มสูงมากขึ้น และเมื่อพัฒนาผลิตภัณฑ์ไปแล้ว และปรากฏจุดอ่อนภายหลัง จะทำให้ยากต่อ

การแก้ไข โดย D.G. Firesmith ได้เสนอประเภทของความต้องการความมั่นคงโดยแยกตามประเภทของภัยคุกคามได้ 10 ประเภท [17] ดังรูปที่ 2.2 รายละเอียดโดยสังเขปมีดังนี้



รูปที่ 2.2 ประเภทของความต้องการด้านความมั่นคง

1) การระบุตัวตน (Identification) เป็นการกำหนดให้ระบุตัวตนผู้ใช้ก่อนเข้าใช้งานระบบ เพื่อให้ระบบจำแนกได้ว่าเป็นใคร ก่อนที่ระบบจะติดต่อด้วย

2) การพิสูจน์ตัวตน (Authentication) เป็นการกำหนดว่าจะพิสูจน์ผู้ใช้ที่เข้ามาใช้งานระบบนั้นมิได้ปลอมแปลงเข้ามา

3) การให้อำนาจ (Authorization) เป็นการกำหนดว่า ผู้ใช้หรือกลุ่มผู้ใช้แต่ละประเภทมีสิทธิ์ในการเข้าถึงและใช้งานภายในระบบในระดับใด

4) การคุ้มกัน (Immunity) เป็นการกำหนดให้ระบบมีความสามารถในการป้องกันตนเองจากโปรแกรมหรือสิ่งที่ไม่พึงประสงค์ เช่น ไวรัส เป็นต้น

5) ความบูรณภาพ (Integrity) เป็นการกำหนดความสามารถของระบบว่าสารสนเทศใดบ้างที่ควรมีการป้องกันจากผู้ที่ไม่มีสิทธิ์

6) การตรวจหาการแทรกแซง (Intrusion Detection) เป็นการกำหนดระดับของระบบในการพยายามตรวจสอบ บันทึก และเฝ้าสังเกตการโจมตี

7) การไม่ยอมรับในสิ่งที่ทำ (Non-repudiation) เป็นการกำหนดให้ระบบสามารถตรวจสอบเพื่อป้องกันการปฏิเสธการกระทำจากการกระทำผู้ที่ไม่พึงประสงค์ได้

8) ภาวะส่วนตัว (Privacy) เป็นการกำหนดให้ระบบสามารถป้องกันกลุ่มผู้ใช้ที่ไม่มีสิทธิ์เข้าถึงข้อมูลที่ส่วนตัวได้

9) การตรวจสอบความมั่นคง (Security Auditing) เป็นการกำหนดให้ระบบสามารถตรวจสอบสถานะและการใช้งานกระบวนการความมั่นคง (Security Mechanism) ตามเหตุการณ์ที่เกิด

10) การรักษาความมั่นคง (System Maintenance Security) เป็นการกำหนดให้กับระบบว่า การควบคุมความมั่นคงของระบบสารสนเทศสามารถทำงานร่วมกันได้

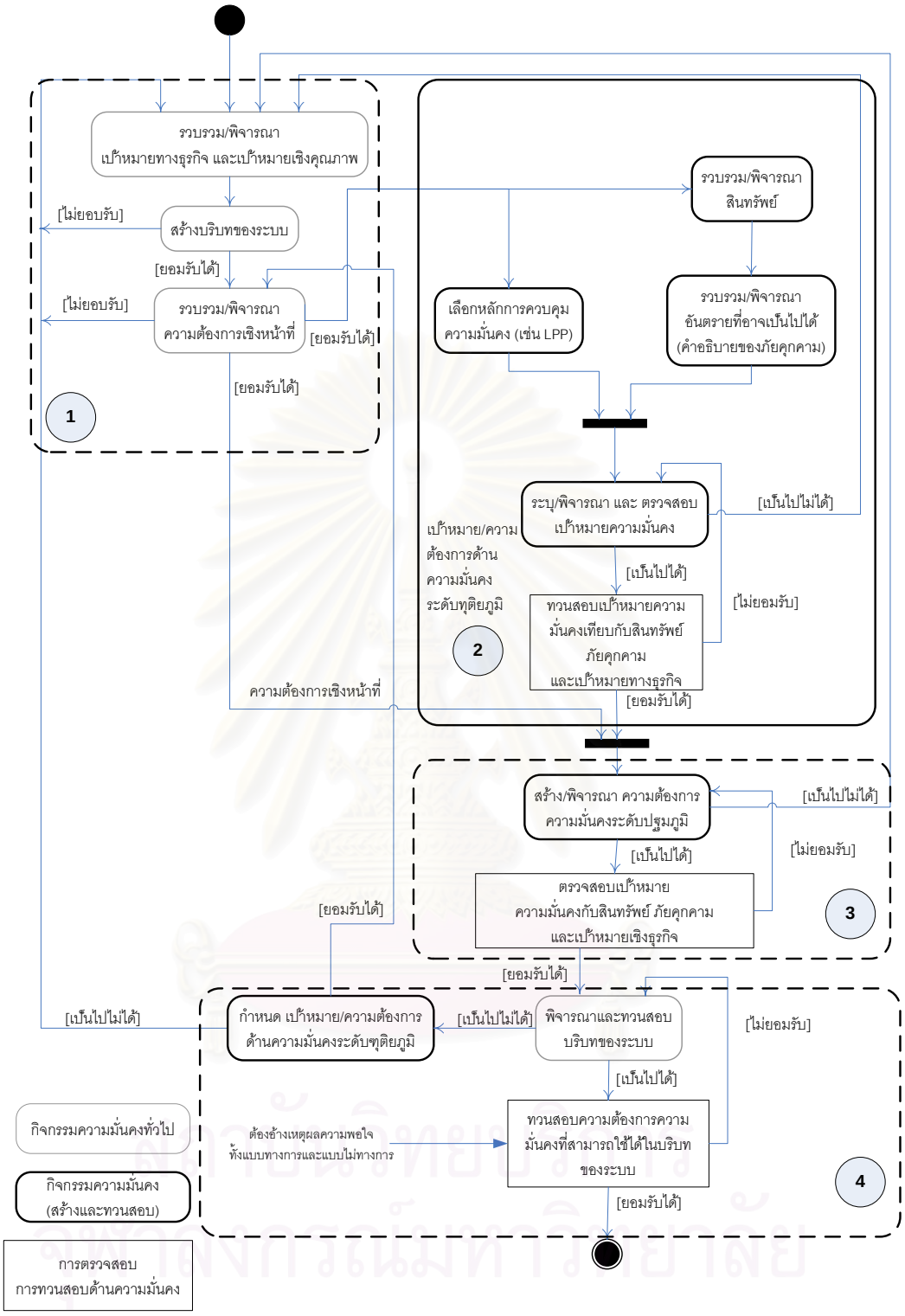
ข้อกำหนดความต้องการที่กล่าวมาข้างต้นนั้น จะมีหลายระดับและหลายแขนงตามนโยบายความมั่นคง ซึ่งจะต้องมีการประเมินความเสี่ยงด้านความมั่นคง (Security Risk Assessment) หรือกล่าวอีกนัยหนึ่ง คือ สิ่งไม่ดีต่อระบบที่อาจจะเกิดขึ้นนั้น จะมีผลกระทบอย่างไร ดังนั้นการระบุข้อกำหนดความต้องการ เป็นกระบวนการสำคัญ เพราะต้องดูความเหมาะสมและความเป็นไปได้ของความต้องการก่อน จึงจะกำหนดกิจกรรมต่างๆ ภายใต้กรอบงานของความมั่นคง (Security Framework) ดังตัวอย่างในรูปที่ 2.3 ซึ่งแสดงกิจกรรมต่างๆ ที่เกิดในกรอบงาน โดยแบ่งออกเป็น 4 ส่วน ได้แก่

1) กำหนดความต้องการเชิงหน้าที่ (Identify Functional Requirements) ซึ่งครอบคลุมกิจกรรมทั่วไปในการเก็บความต้องการเชิงหน้าที่

2) ระบุเป้าหมายความมั่นคงให้เหมาะสม (Identify Appropriate Security Goals) ประกอบด้วยกระบวนการย่อยดังนี้

(1) ระบุสินทรัพย์ที่เป็นไปได้ (Identify Candidate Assets)

เป็นการหาอ็อบเจกต์ (Object) ทั้งหมดในบริบทของระบบที่มีอยู่ ไม่ว่าจะเป็นทั้งทางตรงและทางอ้อม โดยทั่วไปแล้ว สินทรัพย์ คือ อ็อบเจกต์ของสารสนเทศ (Information Object) ที่เก็บไว้ หรือสามารถเข้าถึงได้โดยระบบและจับต้องได้ อ็อบเจกต์ทางตรง หมายถึง อ็อบเจกต์ที่เมื่อเกิดภัยคุกคามแล้วมีผลต่ออ็อบเจกต์ดังกล่าวโดยตรง ส่วนอ็อบเจกต์ทางอ้อม หมายถึง อ็อบเจกต์ ที่เมื่อเกิดภัยคุกคามแล้วมีผลต่อสินทรัพย์อย่างอื่น เช่น รายได้ (Revenue) ค่าใช้จ่าย (Cost) และ ชื่อเสียง (Reputation) เป็นต้น



รูปที่ 2.3 กิจกรรมที่เกิดภายในกระบวนการความต้องการความมั่นคง [14]

(2) สร้างรายละเอียดภัยคุกคาม (Generate Threat Descriptions)

โดยทั่วไปแล้วภัยอันตราย (Harm) มักเกิดจากการละเลยความต้องการความมั่นคงตั้งแต่ 1 อย่างขึ้นไป ซึ่งความมั่นคงที่เกี่ยวกับสินทรัพย์สารสนเทศจะประกอบด้วย การถือความลับ ความบูรณภาพ และสภาพพร้อมใช้งาน ซึ่งคล้ายกับสินทรัพย์ที่จับต้องได้ทั่วไปที่ประกอบด้วย การยอมรับ (Exposure) การแก้ไขเพิ่มเติม (Modification) และ ภาวะเพิกถอนสิทธิ์ (Deprivation) โดยจะสอดคล้องกับคำถามที่ว่า "*ภัยอันตรายใดที่มาจากการละเมิด [ส่วนความมั่นคงที่เกี่ยวข้อง] ของ [สินทรัพย์]*" โดยคำตอบจะอยู่ในรูปของความสัมพันธ์ คือ {กิจกรรม (action), สินทรัพย์ (Asset), ภัยอันตราย (Harm)}

(3) ประยุกต์ใช้กับหลักการการจัดการ (Apply Management Principles)

รายการของเป้าหมายความมั่นคง (A list of Security Goals) ที่ได้มานั้นเป็นหลักการในการนำไปประยุกต์ใช้กับสินทรัพย์และเป้าหมายเชิงธุรกิจ เพื่อให้ได้ผลลัพธ์ที่จะนำไปใช้เป็นเซตของการบรรลุ (Achieve) เป้าหมายของระบบ

(4) กำหนดเป้าหมายความมั่นคง (Determine Security Goals)

เป็นขั้นตอนการกำหนดเป้าหมายความมั่นคงสำหรับองค์กร หรือระบบภายในองค์กร หลังจากที่ได้รับการตรวจสอบความเป็นไปได้ และเหมาะสมกับเป้าหมายเชิงธุรกิจ

ผลลัพธ์ที่ได้จากขั้นตอนนี้ คือ เซตของเป้าหมายความมั่นคง (Set of Security Goals) ซึ่งผ่านการตรวจสอบความสมเหตุสมผลแล้วว่าเป็นไปตามเป้าหมายเชิงธุรกิจ และมีระดับที่น่าพอใจ

3) ระบุความต้องการความมั่นคง (Identify Security Requirements)

เป็นขั้นตอนที่เราต้องกำหนดความต้องการความมั่นคง เสมือนเป็นเงื่อนไขบังคับให้กับความต้องการเชิงหน้าที่ ให้เป็นไปตามระดับความพอใจของเป้าหมายความมั่นคง โดยการพิจารณาสินทรัพย์ใดเกี่ยวข้องกับความต้องการเชิงหน้าที่ใด แล้วแสดงเป็นรายการสินทรัพย์ออกมาเพื่อดูว่าจะมีภัยคุกคามใดบ้างที่เกี่ยวข้อง และจะนำความต้องการความมั่นคงไปประยุกต์ใช้อย่างไร

4) ตรวจสอบความสมเหตุสมผลของบริบทในระบบ (Validation of System Context)

เป็นการทวนสอบ (Verification) ในแต่ละขั้นตอนในกรอบงาน และเป็นการแสดงให้เห็นถึงระดับความพอใจของความต้องการความมั่นคง โดยการสร้างการให้เหตุผล (Argumentation) ทั้งที่เป็นทางการ (Formal) และไม่เป็นทางการ (Informal) เพื่อการตรวจสอบ

ความสัมพันธ์ด้านความมั่นคงกับคุณสมบัติภายในระบบ และพิจารณาถึงผลกระทบของความมั่นคงของระบบ

2.1.4 บีเอ็นเอฟ (Backus-Naur Form: BNF) และอีบีเอ็นเอฟ (Extended Backus-Naur Form: EBNF)

บีเอ็นเอฟ [20] ถูกนำเสนอครั้งแรกโดย John Backus ในรายงานการประชุม UNESCO บน ALGOL 58 ต่อมา ได้รับการปรับปรุงโดย Peter Naur จนได้ไวยากรณ์ของภาษาโปรแกรม ALGOL 60 นับแต่นั้นมา ผู้แต่งหนังสือภาษาโปรแกรมเกือบทุกคนได้ใช้ BNF ในการระบุกฎไวยากรณ์ของภาษา ซึ่งบีเอ็นเอฟมีวัตถุประสงค์เพื่อเป็นสัญลักษณ์ทางการในการอธิบายไวยากรณ์ไม่พึ่งบริบท (Context-free Grammar) โดยสัญลักษณ์ที่ใช้ในบีเอ็นเอฟมีหลากหลายขึ้นกับการใช้งาน โดยงานวิจัยนี้จะใช้รูปแบบของอีบีเอ็นเอฟ ซึ่งใช้งานได้ง่ายกว่าและไม่กำกวมมากกว่าบีเอ็นเอฟแบบเดิม เนื่องจากปัญหาในเรื่องของการใช้สัญลักษณ์ ‘<’ ‘>’ ‘|’ ‘::=’ และการวนซ้ำ (Repetition) ในประโยคยาวๆ ที่ค่อนข้างวกวน [22]

อีบีเอ็นเอฟ [22] เป็นข้อมูลอภิบายภาษาที่กำหนดโดยองค์กรมาตรฐานสากลไอเอสโอ (International ISO) ในปี 1977 โดยพัฒนาต่อยอดมาจากบีเอ็นเอฟเดิม โดยมีกฎทั่วไปดังนี้

1) เทอร์มินอลซิมโบล (Terminal Symbol) จะถูกกำหนดอยู่ภายใต้เครื่องหมายอัญประกาศ (“…”) เสมอ

2) เครื่องหมาย ‘[’ และ ‘]’ เป็นสัญลักษณ์ทางเลือก (Option) หมายความว่าสัญลักษณ์ภายในอาจปรากฏหรือไม่ก็ได้

3) เครื่องหมาย ‘{’ และ ‘}’ เป็นสัญลักษณ์การวนซ้ำ หมายความว่า สัญลักษณ์ภายในจะปรากฏได้มากกว่า 1 ครั้ง

4) สามารถใช้เครื่องหมาย ‘(’ และ ‘)’ เพื่อจัดกลุ่มของสัญลักษณ์ได้ ซึ่งมีความหมายเหมือนแนวคิดทางคณิตศาสตร์

5) กรณีที่ต้องใช้สัญลักษณ์พิเศษนอกหรือข้อมูลอื่นๆ จะต้องใช้ภายใต้เครื่องหมาย ‘?...?’ เพื่อแสดงสัญลักษณ์พิเศษ

6) กรณีที่ต้องการใส่ข้อคิดเห็น (Comment) จะต้องใช้ภายใต้เครื่องหมาย ‘(*’ และ ‘*)’ เท่านั้น ซึ่งจะไม่ถูกนำไปแปลงเป็นผลลัพธ์ภายหลัง

7) ทุกกฎที่ถูกนำเสนอจะต้องแสดงใช้เครื่องหมายมหัพภาค (.) เพื่อแสดงการสิ้นสุดของกฎเสมอ

8) กรณีที่ต้องการยกเว้น (Except) ใช้เครื่องหมาย ‘-’

ตัวอย่างการใช้ภาษาอีบีเอ็นเอฟ

- ไวยากรณ์

```
letter =    "A" | "B" | "C" | "D" | "E" | "F"
          | "G" | "H" | "I" | "J" | "K" | "L" | "M"
          | "N" | "O" | "P" | "Q" | "R" | "S" | "T"
          | "U" | "V" | "W" | "X" | "Y" | "Z";
vowel =     "A" | "E" | "I" | "O" | "U";
consonant = letter - vowel;
ee =        {"A"}-, "E";
```

- ตัวอย่างผลลัพธ์

```
letter:     A B C D E F G H I J
vowel:      A E I O U
consonant:  B C D F G H J K L M
ee:         AE AAE AAAE AAAAE AAAAAE
```

2.2 งานวิจัยที่เกี่ยวข้อง

2.1.1 กรอบงานสำหรับวิศวกรรมความต้องการความมั่นคง (A Framework for Security Requirements Engineering)

งานวิจัยนี้ได้นำเสนอกรอบงานสำหรับการรวบรวมและวิเคราะห์ความต้องการโดยอาศัยการสร้างบริบทของระบบและการให้เหตุผลความพอใจ (Satisfaction Argument) สำหรับความมั่นคงของระบบประกอบด้วย [14]

1) การวิเคราะห์สินทรัพย์และเป้าหมายความมั่นคงสามารถทำให้เสร็จสิ้นในบริบทเชิงธุรกิจ (Business Context) ของระบบ

2) การเข้าใจผลกระทบของความต้องการความมั่นคงต่อความต้องการเชิงหน้าที่

3) การออกแบบเงื่อนไขบังคับมีการบันทึกไว้

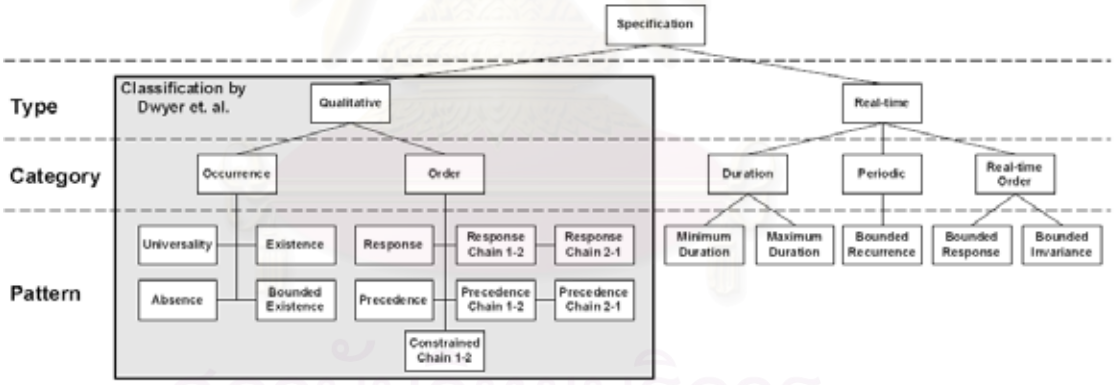
4) ความถูกต้องของความต้องการความมั่นคง โดยการใช้การให้เหตุผลความพอใจ

จากนั้น C. B. Haley และคณะได้นำเสนอ การให้เหตุผลความพอใจ ซึ่งแบ่งออกเป็นสองส่วนได้แก่ ส่วนแรก เป็นการให้เหตุผลทางการ (Formal Argument) เพื่อดูว่า ระบบดังกล่าวเหมาะสมกับความต้องการความมั่นคงหรือไม่ และอีกส่วน คือ การให้เหตุผลไม่เป็นทางการเชิงโครงสร้าง (Structured Informal Argument) เพื่อรองรับนิพจน์สมมติฐานในการเหตุผลทางการ

สิ่งที่นำมาพิจารณาใช้ในวิทยานิพนธ์นี้คือ การเก็บรวบรวมและวิเคราะห์ความต้องการความมั่นคง ซึ่งเสนอในรูปของกรอบงานแสดงกิจกรรมดังแสดงให้เห็นในรูปที่ 2.3 นั้น การดำเนินการตามกรอบงานดังกล่าวอาจทำได้ยาก เนื่องจากการวิเคราะห์ความสัมพันธ์ระหว่างความต้องการความมั่นคงและความต้องการเชิงหน้าที่นั้นต้องใช้บุคคลในการพิจารณา ซึ่งบุคคลดังกล่าวจะต้องมีความรู้และประสบการณ์ทั้งการวิเคราะห์ความต้องการ และความต้องการด้านความมั่นคง

2.1.2 **แบบรูปข้อกำหนดแบบเรียลไทม์** (Real-time Specification Patterns)

งานวิจัยนี้ [7] เป็นส่วนงานที่พัฒนาต่อมาจากการพัฒนาแบบรูปข้อกำหนดเชิงคุณภาพของ ของ Dwyer et.at [19] โดย S. Konrad, Betty และ H.C. Cheng ได้นำเสนอการจัดกลุ่มของแบบรูปข้อกำหนดโดยการเพิ่มแบบรูปข้อกำหนดแบบเรียลไทม์เข้าไปเป็นส่วนขยายงานเดิมของ Dwyer et al. (พื้นที่สีเทาของรูปที่ 2.4) ที่นำเสนอแบบรูปเชิงคุณภาพ (Qualitative Patterns) โดยมีเป้าหมายช่วยเติมเต็มแบบรูปข้อกำหนดสำหรับกระบวนการความต้องการได้มากขึ้น เนื่องจากความต้องการด้านเวลามักปรากฏในระบบฝังตัว (Embedded System) และระบบที่มีความเสี่ยงสูง โดยในงานวิจัยประกอบด้วย 2 ส่วน คือ ส่วนแรก เป็นการวิเคราะห์ความต้องการด้านเวลา เพื่อช่วยในการสร้างแบบรูปข้อกำหนดแบบเรียลไทม์ (Real-time Specification Pattern) โดยนำเสนอข้อกำหนดในรูปตรรกศาสตร์เชิงเวลาทั้ง 3 แบบ ได้แก่ แอลทีแอล (Line Time Temporal Logic : LTL) ซีทีอาร์ (Computer Tree logic : CTR) และ จีไอแอล(Graphical Interval Logic : GIL) ส่วนที่สอง เน้นความเข้าใจในข้อกำหนดความมั่นคงโดยการนำเสนอไวยากรณ์ภาษาอังกฤษที่รองรับคุณสมบัติแบบรูปเรียลไทม์ และมีการสาธิตการนำแบบรูปไปใช้จริงตามระบบฝังตัวที่มีอยู่ในปัจจุบัน แบบรูปข้อกำหนดแบบเรียลไทม์ในงานวิจัยนี้เป็นการขยายขอบเขตของงานวิจัยเดิม โดยมีขอบเขตดังแสดงดังรูปที่ 2.4

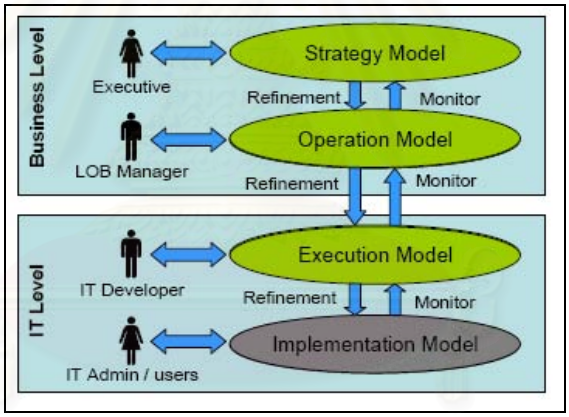


รูปที่ 2.4 การจัดกลุ่มของแบบรูปข้อกำหนด [7]

สิ่งที่นำมาพิจารณาใช้ในวิทยานิพนธ์นี้ คือ การกำหนดโครงสร้างไวยากรณ์ให้กับผู้ใช้ในการกำหนดรายละเอียดเพิ่มเติมให้เป็นไปตามโครงสร้างดังกล่าว ทำให้ได้องค์ประกอบของความต้องการที่ถูกต้อง ชัดเจน และลดความกำกวม ซึ่งเป็นแนวคิดในการสร้างไวยากรณ์สำหรับการกำหนดข้อกำหนดความมั่นคง ซึ่งสามารถเพิ่มความสมบูรณ์ให้กับแบบรูปที่นำเสนอในงานวิจัยนี้ได้ ซึ่งยังไม่ครอบคลุมความต้องการความมั่นคงแต่อย่างใด

2.1.3 **การปรับแต่งความมั่นคงของเว็บเซอร์วิส** (Web Services Security Configuration)

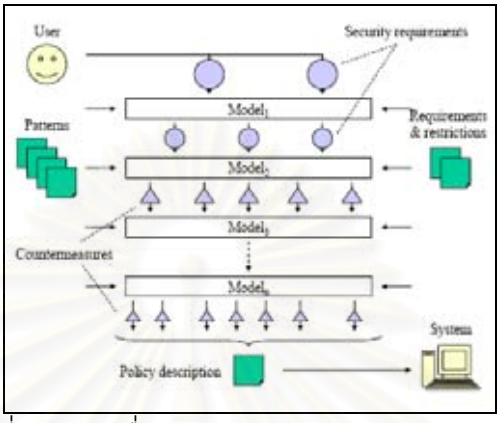
งานวิจัยนี้ [15] เป็นงานวิจัยที่ให้ความสำคัญในด้านความมั่นคงในการพัฒนาโปรแกรมประยุกต์ทางธุรกิจ และข้อกำหนดความมั่นคงของเว็บเซอร์วิส แม้ว่าส่วนใหญ่จะให้ความสำคัญด้านความมั่นคงด้านของเทคโนโลยี ซึ่งจำเป็นต้องพิจารณาความมั่นคงด้านธุรกิจควบคู่ไปด้วยกัน ซึ่งระบบงานปัจจุบันยังมีช่องว่างระหว่างความต้องการความมั่นคงของทั้งสองประเภท ส่งผลให้เกิดการปรับแต่งผิดพลาด ทำให้เกิดค่าใช้จ่ายสูง และนำไปสู่การถูกโจมตีได้ในเวลาต่อมา จึงทำการกำหนดความต้องการความมั่นคงจากมุมมองธุรกิจ (Business Perspective) ไปยังมุมมองเทคโนโลยี (Technology Perspective) ดังรูปที่ 2.5 ซึ่งแสดงความสัมพันธ์ระหว่างระดับไอที (IT Level) และระดับธุรกิจ (Business Level) ในเอสโอเอ (Service-Oriented Architecture: SOA) โดยใช้เอ็มดีเอ (Model-Driven Architecture: MDA) ทำให้ความต้องการความมั่นคงค่อยๆ มีรายละเอียดมากขึ้นช่วยในการลดช่องว่างโดยการใช้แบบรูปกิจกรรมที่ดีที่สุด (Best Practices Pattern)



รูปที่ 2.5 ความสัมพันธ์ระหว่างระดับไอที (IT) และระดับธุรกิจ ในเอสโอเอ [15]

จากรูปที่ 2.5 แสดงให้เห็นถึงกระบวนการกำหนดและปรับเปลี่ยนความต้องการ โดยเริ่มจากระดับบนหรือระดับธุรกิจ โดยมีผู้เชี่ยวชาญให้ข้อมูลและตรวจสอบกลยุทธ์ที่นำเสนอ เพื่อปรับเปลี่ยนให้สามารถดำเนินการได้โดยปรับเปลี่ยนจากแบบจำลองเชิงกลยุทธ์ (Strategy Model) เป็นแบบจำลองการดำเนินงาน (Operation Model) ในระดับเทคโนโลยีสารสนเทศ จะมีผู้พัฒนา ผู้ดูแลระบบ และผู้ใช้งาน ทำการพิจารณาความเหมาะสมในแบบจำลองการกระทำ (Execution Model) เพื่อให้ได้แบบจำลองปฏิบัติที่ได้ผล (Implement Model) อย่างไรก็ตาม การดำเนินการระหว่างแบบจำลองดังกล่าว ถือเป็นการตรวจสอบแบบจำลองก่อนหน้าว่ามีความถูกต้องเพียงใดและสามารถปรับเปลี่ยนได้ตามความเหมาะสม ซึ่งการเชื่อมต่อระหว่างแบบจำลอง ได้แสดงไว้ดังรูปที่ 2.6 ซึ่งเป็นการแสดงการเชื่อมกันระหว่างแบบจำลองเอสโอเอ โดยผู้ใช้จะให้ข้อกำหนดความ

ต้องการ แล้วจึงนำมาพัฒนาเป็นแบบจำลองในระดับต่างๆ ซึ่งจะเห็นได้ว่ามีการนำแบบรูปเข้ามาช่วยในการเชื่อมต่อระหว่างแบบจำลอง โดยมีวัตถุประสงค์เพื่อกำหนดแนวทางในการปรับปรุงและแก้ไขแบบจำลองตามมาตรการการแก้ไขที่เหมาะสม โดยผลลัพธ์จากความสัมพันธ์แต่ละแบบจำลองจะอยู่ในรูปของนโยบาย ซึ่งจะใช้สำหรับระบบเอสโอเอดังกล่าวต่อไป



รูปที่ 2.6 การเชื่อมแบบจำลองต่างในเอสโอเอ [15]

งานวิจัยดังกล่าวช่วยให้เกิดความมั่นใจในแนวคิดของวิทยานิพนธ์นี้ กล่าวคือ ผู้ใช้ระดับบนจะไม่ค่อยทราบรายละเอียดต่างๆ ในเชิงเทคโนโลยี แต่สามารถกำหนดความต้องการในระดับธุรกิจได้ ดังนั้นถ้าหากนำแบบรูปความมั่นคงเข้าไปประยุกต์ใช้ เปรียบเสมือนมิดเดิลแวร์ (Middleware) ระหว่างสองระดับ ก็จะช่วยลดช่องว่างของความต้องการความมั่นคงในระดับธุรกิจและระดับเทคโนโลยีสารสนเทศ ทั้งยังช่วยให้มีแนวทางไปในทางเดียวกันได้

2.1.4 **ออนโทโลจีจากความต้องการความมั่นคงในเอกสารควบคุม** (Ontology from Security Requirements in Regulatory Documents)

งานวิจัยนี้ [16] ได้นำเสนอการประยุกต์ใช้ขั้นตอนวิธีที่คิดขึ้น มาวิเคราะห์ร่วมกับเอกสารความต้องการความมั่นคง แล้วนำมาสร้างเป็นพีดีโอ (Problem Domain Ontology : PDO) โดยอาศัยเอกสารความต้องการความมั่นคงจากดิทซ์แคพ (Department of Defense Information Technology Security Certification and Accreditation Process : DITSCAP) โดยมีเป้าหมายเพื่อรวบรวมความต้องการได้อย่างไม่กำกวมและเข้าใจความต้องการความมั่นคงได้ตรงกัน ทั้งนี้เอกสารความต้องการความมั่นคงนั้นมีหลายระดับ และมีความเกี่ยวเนื่องกัน ดังนั้นจึงเสนอภาษาร่วม (Common Language) สำหรับพีดีโอ โดยมีการจัดกลุ่มความต้องการและกำหนดคำสำคัญภายในเอกสารเพื่อใช้ในการพิจารณาความขึ้นต่อกันระหว่างเอกสารความต้องการความมั่นคง ผลลัพธ์จากการสร้างพีดีโอ จะได้ดังรูปที่ 2.7 โดยประโยชน์จากพีดีโอนั้นสามารถช่วยในการตัดสินใจในการเลือกความต้องการความมั่นคงให้สอดคล้องกับความต้องการจากผู้ใช้ รวมถึงแสดงให้เห็นถึงปัจจัยความสี่ยงที่อาจเกิดขึ้นจากความต้องการดังกล่าวได้

DECISION POINT	CURRENT DITSCAP PRACTICES	ISSUES WITH CURRENT DITSCAP PRACTICES	BENEFITS OF THE DITSCAP DECISION SUPPORT PDO
What are the criteria to assess compliance levels of the target system with security requirements? **STAKEHOLDERS INVOLVED** Developer, Integrator, or Maintainer, User Representative, DAA, Certifier and Certification Team	• DITSCAP advocates the use of Minimum Security Activity Checklist (MSCL) as well as the Requirements Traceability Matrix (RTM) to record requirements compliance information. • DITSCAP recommends testing procedures to verify and validate the compliance levels of the target system	• *No uniform representation format* exists to collect objective, repeatable and justifiable evidences to establish the compliance level of the target system with the applicable security requirements • DITSCAP is a *long and exhaustive task of gathering target system details* related to security requirements without proper tool support. Such an approach quickly results in an *ad-hoc process* with subjective decision making to establish compliance with security requirements • The MSCL does not have an explicit mapping with the security requirements	• The requirements *compliance questionnaires* of the PDO establish *well-defined criteria to guide a systematic evaluation of compliance level* of the target system with the applicable security requirements. • The PDO supports a *holistic and uniform view of the security requirements* based on the interdependencies among them as well as with other problem domain concepts to promote a *common understanding among stakeholders.* • The PDO provides effective ways to systematically gather evidences for establishing *security requirements applicability and compliance*, *perceive related risks* in the operational environment, and *proactively reveal their relationships with other domain concepts* through the nexus of causal chains that exist in the UoD. The PDO makes these *artifacts* readily available through various inference mechanisms based on its ontological structure and semantics. As an example consider the security requirement marked as "**R1**" and the artifacts "**T1, T2, T3, and T4**" obtained from the PDO which serve as metrics and measures from various dimensions to assess the *overall impact of the security requirement* on the target system and environment.

EXAMPLE REQUIREMENT

R1 Requirement - EBRP-1 Remote Access Audit Trails for Privileged Functions

Remote access for privileged functions is discouraged, is permitted only for compelling operational needs, and is **strictly controlled**. In addition to **EBRU-1**, sessions employ security measures such as a **VPN with blocking mode enabled**. A **complete audit trail is recorded**, and the **IAM/O reviews the log** for every remote session.

ARTIFACTS INFERENCED FROM PDO THAT HELP TO ASSESS THE OVERALL IMPACT OF THE SECURITY REQUIREMENT "R1"

T1 RELATED SECURITY REQUIREMENTS

REMOTE ACCESS CONTROLS	ENCLAVE BOUNDARY CONTROLS	AUDIT TRAIL CONTROLS
• EBRU-1 Remote Access for User Functions • EBRU-1 Remote Access for User Functions use encryption • EBRU-1 Protection of remote access mechanisms for user functions	• EBPW-1 Public WAN Connection • EBBD-2 Boundary Defense • ECIM-1 Instant Messaging • ECVI-1 Voice over IP • Outsourced application subject to DoD enclave boundary defense.	• ECAR-2 Audit Record Content • ECTP-1 Audit Trail Protection • ECAT-1 Audit Trail, Monitoring, Analysis and Reporting • ECRG-1 Audit Reduction and Report Generation

T2 RELATED RISK FACTORS

ASSETS	THREATS
- DoD Information Systems - Audit Records	- Unauthorized Access - Information Leak
VULNERABILITIES	**COUNTERMEASURES**
- VPN Controls with blocking mode off - Logging mechanisms not enabled	- Monitory System Access - Logging and Reviewing Access - Information Access restriction

T3 RELATED VIEWPOINTS

- IA Service – Confidentiality
- Stakeholder Responsibility – IAM/O

T4 RELATED DITSCAP C&A GOALS

Identify the Network Connection Rules

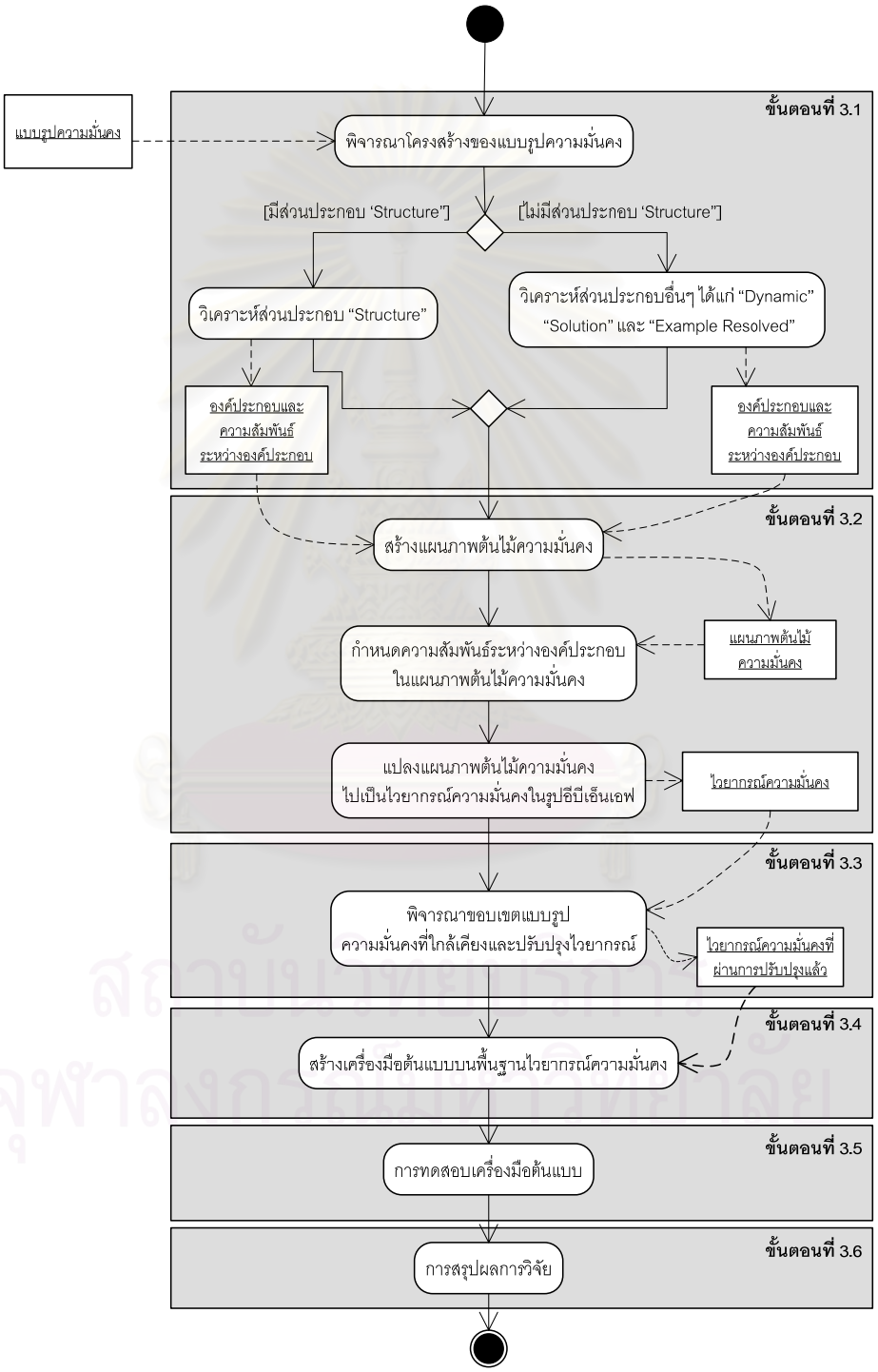
รูปที่ 2.7 ตัวอย่างบางส่วนของการสร้างตารางการตัดสินใจโดยใช้ POD [16]

จากตัวอย่างความต้องการในรูปที่ 2.7 (R1: EBRP-1 หลักฐานการตรวจสอบการเข้าถึงระยะไกลสำหรับฟังก์ชันเอกสิทธิ์ (Privilege)) โดยการกำหนด "ห้ามการใช้สิทธิ์การเข้าถึงทางไกล ซึ่งจะอนุญาตเฉพาะความการดำเนินการที่มีความจำเป็นจริงๆ เท่านั้น และต้องมีการควบคุมอย่างเข้มงวดเพิ่มเติมจาก EBRU-1 ซึ่งต้องมีการวัดระดับความมั่นคงในช่วงเวลาที่ใช้งาน เช่น การเปิดการป้องกัน วีพีเอ็น (Virtual Private Network: VPN) มีหลักฐานการตรวจสอบที่สมบูรณ์ และมีการทบทวน IAM/O ทุกๆ ช่วงเวลาที่มีการเข้าถึงทางไกล"
ข้อความความต้องการข้างต้นจะประกอบด้วยคำสำคัญที่สามารถใช้ในการอ้างถึงความต้องการ ความมั่นคง (การควบคุมการเข้าถึงทางไกล ขอบเขตการควบคุม หลักฐานการตรวจสอบ) ปัจจัยความเสี่ยง (สินทรัพย์ ภัยคุกคาม จุดอ่อน และ มาตรการการแก้ไข) ที่เกี่ยวข้อง ตลอดจนคำนึงถึงปัจจัยภายนอก (ระบบบริการ และผู้มีส่วนได้เสีย) และเป้าหมายของการรับรองเป็นลายลักษณ์อักษร (Certification) และการรับรองวิทยฐานะ (Accreditation) ที่เกี่ยวข้องด้วย ซึ่งข้อมูลที่กล่าวมานี้จะช่วยให้การตัดสินใจของผู้พัฒนาหรือผู้ออกแบบให้ทราบถึงสิ่งที่ต้องพิจารณาที่ปรากฏจากความต้องการดังกล่าวได้อย่างถูกต้องมากขึ้น

สิ่งที่นำมาพิจารณาจากงานวิจัยนี้คือ แนวคิดในการกำหนดการเชื่อมโยงระหว่างความต้องการ เนื่องจากข้อกำหนดความต้องการบางข้อ สามารถนำไปใช้ หรือ มีความสัมพันธ์ต่อข้อกำหนดความต้องการอื่นๆ ได้ ซึ่งถือว่าเป็นการตรวจสอบความถูกต้องและความสอดคล้องของข้อกำหนดความต้องการได้

บทที่ 3
การวิเคราะห์แบบรูปความมั่นคงและการออกแบบไวยากรณ์ความมั่นคง

งานวิจัยนี้แบ่งขั้นตอนการดำเนินงานวิจัยออกเป็น 6 ส่วน สามารถแสดงโดยแผนภาพกิจกรรม (Activity Diagram) ดังรูปที่ 3.1



รูปที่ 3.1 แผนภาพขั้นตอนการดำเนินการวิจัย

จากรูปที่ 3.1 ขั้นตอนที่ 3.1 เป็นขั้นตอนเริ่มต้นของการดำเนินงาน โดยการวิเคราะห์โครงสร้างแบบรูปความมั่นคง เพื่อหาส่วนประกอบสำคัญภายในแบบรูปที่แสดงให้เห็นถึงองค์ประกอบสำคัญที่ต้องพิจารณาภายในแบบรูปนั้นๆ ทั้ง 20 แบบรูป ครอบคลุม 4 กลุ่มแบบรูปความมั่นคง ได้แก่ การจัดการความมั่นคงองค์กรและการจัดการความเสี่ยง การระบุตัวตนและการพิสูจน์ตัวจริง แบบจำลองควบคุมการเข้าถึง และสถาปัตยกรรมไฟล์วอลล์ ซึ่งผลลัพธ์จากขั้นตอนนี้คือ รายการองค์ประกอบสำคัญของแบบรูปความมั่นคง ขั้นตอนที่ 3.2 แสดงขั้นตอนการสร้างไวยากรณ์ความมั่นคง ซึ่งต้องใช้รายการองค์ประกอบสำคัญของแบบรูปความมั่นคงของขั้นตอนก่อนหน้ามาใช้ เพื่อสร้างเป็นแผนภาพต้นไม้ความมั่นคง แล้วจึงทำการแปลงเป็นไวยากรณ์ไม่พึ่งบริบทต่อไป ขั้นตอนที่ 3.3 แสดงขั้นตอนการวิเคราะห์และพิจารณาความสัมพันธ์ระหว่างแบบรูปความมั่นคงเพื่อการบูรณาการไวยากรณ์ให้มีความสมบูรณ์มากขึ้น โดยรายละเอียดทั้ง 3 ขั้นตอนข้างต้น จะแสดงรายละเอียดของแต่ละขั้นตอนในหัวข้อ 3.1 3.2 และ 3.3 ตามลำดับ สำหรับรายละเอียดในขั้นตอนที่ 3.4 3.5 และ 3.6 ที่เกี่ยวข้องกับการสร้างเครื่องมือต้นแบบ การทดสอบเครื่องมือ และสรุปผลการวิจัย จะกล่าวถึงต่อไปในบทที่ 4 บทที่ 5 และ บทที่ 6 ตามลำดับ โดยภายในเล่มวิทยานิพนธ์นี้จะใช้เครื่องหมายสัญประกาศ (“…”) แสดงถึงองค์ประกอบของแบบรูปมิใช่บทบรรยายภายในเล่ม

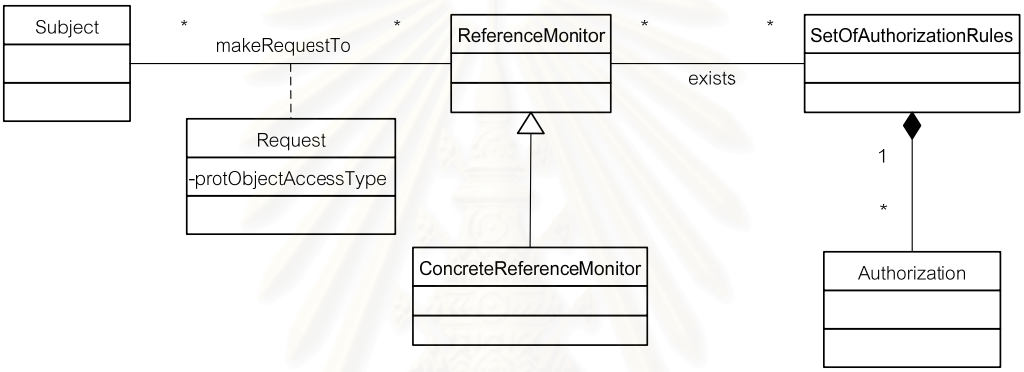
เพื่อความสะดวกในการทำความเข้าใจในการสร้างไวยากรณ์ความมั่นคงจากแบบรูปความมั่นคงในบทนี้ จึงได้ใช้แบบรูปการตรวจสอบการเข้าถึงทรัพยากรมาเป็นกรณีศึกษา ซึ่งเป็นแบบรูปความมั่นคงในกลุ่มการควบคุมการเข้าถึงที่ทำหน้าที่ตรวจสอบสิทธิ์สำหรับบทบาท มีวัตถุประสงค์เพื่อกำหนดความต้องการในการตรวจสอบการใช้สิทธิ์ของผู้ใช้ แบบรูปการตรวจสอบการเข้าถึงทรัพยากรมีส่วนประกอบสำคัญต่างๆ ในการวิเคราะห์ครบถ้วน ได้แก่ “Structure” “Dynamic” และ “Example Resolved” จึงสามารถแสดงวัตถุประสงค์ของแต่ละส่วนประกอบ ความหมาย และผลที่ได้จากการวิเคราะห์ในแต่ละส่วนประกอบ แล้วนำมาเปรียบเทียบความสอดคล้องขององค์ประกอบที่ปรากฏภายในได้ โดยมีรายละเอียดดังนี้

3.1 การวิเคราะห์โครงสร้างแบบรูปความมั่นคง

การวิเคราะห์โครงสร้างแบบรูปความมั่นคง เป็นการพิจารณาโครงสร้างหรือส่วนประกอบของเอกสารแบบรูปความมั่นคงที่นำเสนอไว้ใน [6] (โดยส่วนประกอบต่างๆ ของเอกสารแบบรูปความมั่นคงพร้อมความหมายแสดงดังภาคผนวก ก) โดยในขั้นตอนนี้จะเป็นการวิเคราะห์ส่วนประกอบสำคัญที่ช่วยให้ผู้วิจัยสามารถทราบถึงองค์ประกอบสำคัญภายในแบบรูปความมั่นคงได้ โดยมีรายละเอียดการวิเคราะห์ดังต่อไปนี้

3.1.1 การวิเคราะห์โครงสร้างแบบรูปความมั่นคงจากส่วนประกอบ “Structure”

ส่วนประกอบ “Structure” เป็นส่วนประกอบแรกที่ต้องพิจารณา เนื่องจากเป็นส่วนประกอบที่แสดงรายละเอียด และข้อกำหนดของคุณลักษณะเชิงโครงสร้างของแบบรูปด้วยสัญลักษณ์ที่เหมาะสมในรูปแบบต่างๆ ส่วนประกอบ “Structure” ส่วนใหญ่แสดงโครงสร้างของแบบรูปด้วยแผนภาพคลาส (Class Diagram) แผนภาพกิจกรรม เป็นต้น หากเป็นแผนภาพคลาสจะแสดงให้เห็นถึงข้อมูลสำคัญต่างๆ ที่ปรากฏในแบบรูปซึ่งง่ายต่อการพิจารณา และหากเป็นแผนภาพกิจกรรม แสดงให้เห็นว่าแบบรูปมีการทำงานอย่างไร และต้องมีข้อมูลสำคัญใดบ้าง ตัวอย่างแผนภาพคลาสจากแบบรูปการตรวจสอบการเข้าถึงทรัพยากรจากส่วนประกอบ “Structure” แสดงดังรูปที่ 3.2



รูปที่ 3.2 แผนภาพคลาสจากแบบรูปการตรวจสอบการเข้าถึงทรัพยากร [11]

จากรูปที่ 3.2 เราจะได้รายการองค์ประกอบสำคัญดังนี้

1) “Subject” คือ ผู้ที่ต้องการสิทธิ์เพื่อใช้ทรัพยากรเป้าหมาย อาจเป็นบุคคล กลุ่มบุคคล กระบวนการ หรือกลุ่มกระบวนการก็ได้ และเป็นผู้ที่สร้าง “Request” ซึ่งเป็นคำร้องขอใช้ดำเนินการไปยัง “ReferenceMonitor” ซึ่งทำหน้าที่เป็นตัวแทนในการติดต่อระหว่าง “Subject” และส่วนการตรวจสอบ “SetOfAuthorizationRules”

2) “SetOfAuthorzationRules” เป็นกลุ่มของบทบาทที่ถูกกำหนดโดยนโยบายองค์กร เพื่อใช้สำหรับกำหนดสิทธิ์ให้กับบทบาทว่า บทบาทดังกล่าวได้รับอนุญาตให้ทำอะไรได้บ้าง

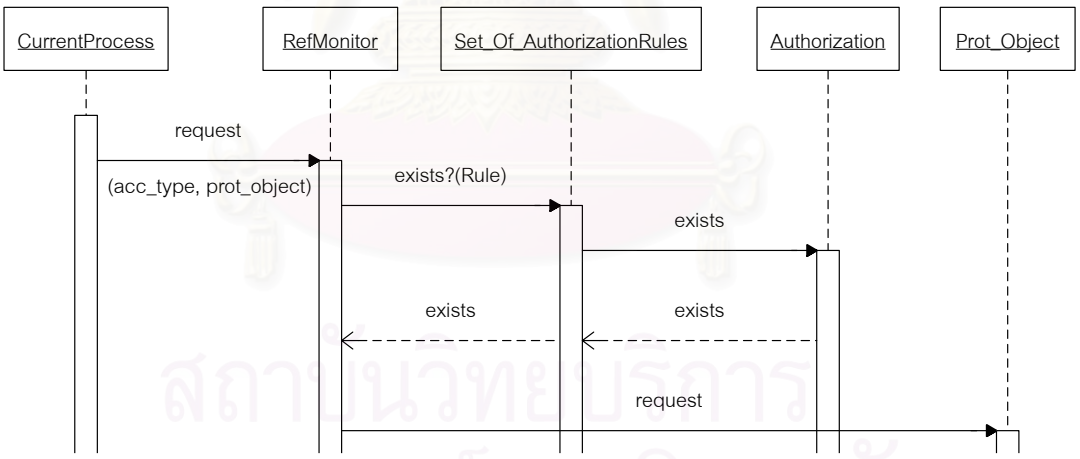
3) “Authorization” เป็นรายการอนุญาตให้ดำเนินกิจกรรมได้ ซึ่งอาจถูกกำหนดขึ้นตามนโยบายขององค์กร เพื่อใช้ในการกำหนดให้กับบทบาทต่างๆ

ดังนั้นจากรูปที่ 3.2 เราจะได้องค์ประกอบสำคัญ ได้แก่ “Subject” “SetOfAuthorizationRules” และ “Authorization” เพื่อนำไปใช้ในการสร้างแผนภาพต้นไม้ในขั้นตอนต่อไป

กรณีที่แบบรูปไม่มีส่วนประกอบ “Structure” หรือมีส่วนประกอบนี้ แต่มิได้นำเสนอในลักษณะแผนภาพยูเอ็มแอล หรือแผนภาพอื่นๆ ที่แสดงให้เห็นถึงองค์ประกอบสำคัญในแบบรูป จึงจำเป็นต้องพิจารณาส่วนประกอบสำคัญอื่นๆ ได้แก่ “Dynamic” “Solution” และ “Example Resolved” เป็นต้น

3.1.2 การวิเคราะห์โครงสร้างแบบรูปความมั่นคงจากส่วนประกอบ “Dynamic”

ส่วนประกอบ “Dynamic” เป็นส่วนที่แสดงสถานการณ์จำลองที่สามารถนำแบบรูปไปประยุกต์ใช้ได้ ซึ่งแสดงให้เห็นถึงพฤติกรรมของแบบรูป ส่วนใหญ่นำเสนอโดยแผนภาพลำดับ (Sequence Diagram) เพื่อแสดงให้เห็นว่าแบบรูปต้องทำอะไรบ้าง และมีการติดต่อกันระหว่างองค์ประกอบใด ซึ่งเราจะเห็นข้อมูลสำคัญๆ ที่ปรากฏในแผนภาพดังกล่าว อย่างไรก็ตาม ส่วนประกอบนี้อาจมีข้อมูลใกล้เคียงกับส่วนประกอบ “Implementation” ซึ่งนำเสนอแนวทางในการนำแบบรูปไปใช้เช่นกัน เราสามารถนำข้อมูลในส่วนประกอบ “Implementation” มาพิจารณาร่วมกับส่วนประกอบ “Dynamic” เพื่อตรวจสอบความถูกต้องและสอดคล้องกันกับวัตถุประสงค์ของแบบรูปความมั่นคง ตัวอย่างแผนภาพลำดับสำหรับแบบรูปความมั่นคงการตรวจสอบการเข้าถึงทรัพยากร (Reference Monitor) ซึ่งปรากฏในส่วนประกอบ “Dynamic” เพื่อแสดงการตรวจสอบอำนาจก่อนการเข้าใช้งานทรัพยากรเป้าหมายแสดงดังรูปที่ 3.3



รูปที่ 3.3 แผนภาพลำดับของแบบรูปการตรวจสอบการเข้าถึงทรัพยากร [11]

จากรูปที่ 3.3 แสดงให้เห็นถึงเงื่อนไขบังคับด้านความมั่นคงของการร้องขอเพื่อใช้ทรัพยากรเป้าหมาย (Protection Object : Prot_Object) โดยขั้นตอนคร่าวๆ ของแบบรูปดังกล่าว คือ การที่ผู้ใช้ทำการร้องขอเพื่อใช้งานทรัพยากร ซึ่งถือเป็นกระบวนการปัจจุบัน (CurrentProcess) โดยในคำร้องประกอบด้วย ประเภทบัญชี (Account Type: acc_type) และทรัพยากรเป้าหมาย ผ่านทางตัวตรวจสอบ (Reference Monitor: RefMonitor) ซึ่งจะทำการตรวจสอบว่าบทบาทของ

ผู้ใช้ดังกล่าวมีอยู่ในกลุ่มบทบาทที่มีอำนาจที่มีสิทธิ์ (Set of Authorization) ในการร้องขอหรือไม่ หากมีก็จะต้องทำการตรวจสอบการให้อำนาจสำหรับผู้ที่มาติดต่อใช้ หากมีอำนาจหรือสิทธิ์ในการเข้าใช้ทรัพยากรดังกล่าว ตัวตรวจสอบจะส่งคำร้องไปยังทรัพยากรเป้าหมายที่ทำการร้องขอไว้

ในแบบรูปความมั่นคง ผู้ร้องขอต้องการจะเข้าถึงทรัพยากรเป้าหมายนั้น จะกำหนดให้ใช้คำว่า “Subject” แทน “Current Process” ดังนั้นจากรูปที่ 3.3 เราจะได้องค์ประกอบสำคัญ ได้แก่ “Subject” “Protection Object” “Set of Authorization Rules” และ “Authorization” เพื่อนำไปใช้ในการสร้างแผนภาพต้นไม้ในขั้นตอนต่อไป

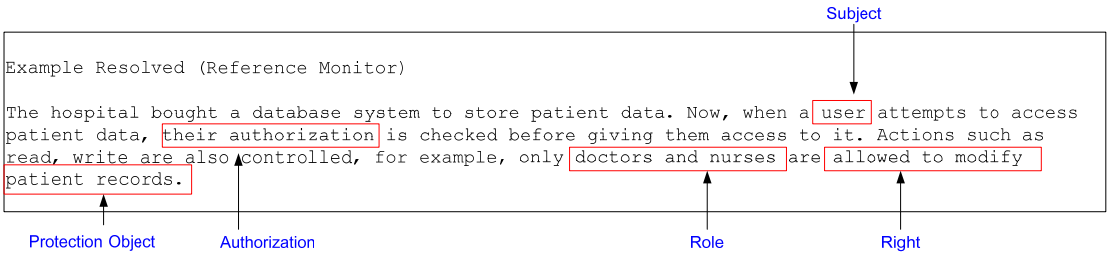
หากแบบรูปความมั่นคงไม่ได้แสดงให้เห็นถึงองค์ประกอบสำคัญทั้งในส่วนประกอบของ “Structure” และ “Dynamic” แล้ว ผู้วิจัยจำเป็นจะต้องพิจารณาส่วนประกอบสำคัญอื่นๆ ได้แก่ “Solution” และ “Example Resolved”

3.1.3 การวิเคราะห์โครงสร้างแบบรูปความมั่นคงจากส่วนประกอบ “Solution” และ “Example Resolved”

ส่วนประกอบ “Solution” เป็นการนำเสนอผลเฉลย (Solution) ตามหลักการพื้นฐานของแบบรูปความมั่นคง โดยการนำเสนอรายการของสิ่งที่จะต้องทำ หรือส่วนประกอบ พร้อมคำอธิบาย ซึ่งส่วนใหญ่เกี่ยวข้องกับหลักการด้านความมั่นคง (Security Principles) เพื่อใช้เป็นข้อมูลในการอธิบายผลลัพธ์ หรือส่วนประกอบสำคัญที่ปรากฏในส่วนประกอบ “Example Resolved” ซึ่งเป็นส่วนที่แสดงผลลัพธ์ของแบบรูปความมั่นคง และองค์ประกอบสำคัญของแบบรูปความมั่นคงก็จะปรากฏในส่วนนี้เช่นกัน

ส่วนประกอบ “Example Resolved” เป็นการพิจารณาคุณลักษณะสำคัญ หรือตัวอย่างผลลัพธ์ที่ได้จากการแก้ปัญหาซึ่งอยู่นอกเหนือจากส่วนประกอบ “Structure” “Dynamic” และ “Implementation” จากที่กล่าวมาข้างต้นพบว่า “Example Resolved” มักปรากฏองค์ประกอบสำคัญสำหรับแบบรูปความมั่นคงเสมอ แต่ที่ต้องพิจารณาหลังสุด เนื่องจากส่วนประกอบ “Example Resolved” มีความหลากหลายมาก และมิได้นำเสนอหลักการ ขอบเขต เงื่อนไขก่อนการใช้แบบรูป วัตถุประสงค์แบบรูป หลักการความมั่นคง หรือ สิ่งที่ต้องพิจารณาก่อนที่จะได้ผลลัพธ์สำหรับแบบรูปความมั่นคง ดังนั้นเราจะต้องศึกษาข้อมูลเหล่านี้ซึ่งปรากฏในส่วนประกอบ “Structure” และ “Dynamic” ดังนั้นจึงต้องพิจารณา 2 ส่วนประกอบนี้ก่อนการพิจารณาส่วนประกอบ “Example Resolved” เสมอ

ตัวอย่างส่วนประกอบ “Example Resolved” จากแบบรูปการตรวจสอบการเข้าถึงทรัพยากร แสดงรูปที่ 3.4



รูปที่ 3.4 ข้อมูลในส่วนประกอบ “Example Resolved” จากแบบการตรวจสอบการเข้าถึงทรัพยากร

จากรูปที่ 3.4 ผู้วิจัยทำการพิจารณาจากส่วนประกอบ “Example Resolved” เป็นหลัก พบว่าจะได้ส่วนประกอบสำคัญดังนี้

1) “Subject” หมายถึง ผู้ที่ต้องการเข้าถึง
2) “Role” หมายถึง บทบาทที่ผู้ต้องการเข้าถึงนั้นมีอยู่
3) “Authorization” หมายถึง สิทธิ์หรืออำนาจที่ผู้เข้าถึงต้องสามารถทำได้
4) “Protection Object” หมายถึง ทรัพยากรที่ผู้ใช้ต้องการเข้าถึง

จากรายการองค์ประกอบข้างต้น จะพบว่ามีความสอดคล้องกับผลลัพธ์ที่ได้จากการพิจารณาจากส่วนประกอบ “Structure” และ “Dynamic” อย่างไรก็ตาม ในการวิเคราะห์โครงสร้างแบบรูปความมั่นคงนั้นไม่มีรูปแบบหรือกฎเกณฑ์การวิเคราะห์ที่ตายตัว เนื่องจากแบบรูปความมั่นคงเป็นการนำเสนอการแก้ปัญหาเชิงคุณภาพที่พิสูจน์แล้วว่าสามารถแก้ปัญหาความมั่นคงได้นั้น เป็นแนวคิดที่นำเสนอโดยกลุ่มผู้ชำนาญด้านความมั่นคง วิศวกรรมความมั่นคง และวิศวกรรมซอฟต์แวร์ ซึ่งแนวคิดมีความหลากหลาย ดังนั้นในการวิเคราะห์แบบรูปความมั่นคงเพื่อจะให้ได้รายการขององค์ประกอบสำคัญๆ ในแบบรูปนั้น จะต้องพิจารณาถึงขอบเขตของแบบรูปและส่วนประกอบต่างๆ ร่วมกัน เพื่อหลีกเลี่ยงการซ้ำซ้อนกับแบบรูปความมั่นคงอื่นๆ เพื่อให้เกิดความถูกต้องในการสร้างไวยากรณ์ความมั่นคงต่อไป

3.2 การสร้างไวยากรณ์ความมั่นคง

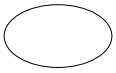
ภายหลังจากการวิเคราะห์และได้องค์ประกอบสำคัญสำหรับแบบรูปความมั่นคงใดๆ แล้ว สิ่งที่ต้องพิจารณาความสัมพันธ์ระหว่างองค์ประกอบด้วย ซึ่งหากองค์ประกอบของแบบรูปได้จากส่วนประกอบ “Structure” ที่นำเสนอโครงสร้างของแบบรูปความมั่นคงด้วยแผนภาพคลาส ผู้วิจัยจะได้ทั้งองค์ประกอบสำคัญและความสัมพันธ์ระหว่างองค์ประกอบด้วย แต่หากได้จากการพิจารณาส่วนประกอบ “Dynamic” “Solution” และ “Example Resolved” ส่วนใหญ่จะเป็นความสัมพันธ์แบบ 1 ต่อ 1 เสมอ ซึ่งไม่ต้องมีสัญลักษณ์มากำกับ บางองค์ประกอบที่อาจเกิดจากองค์ประกอบย่อย ซึ่งการพิจารณาในส่วนนี้ผู้วิจัยต้องพิจารณาร่วมกับผู้เชี่ยวชาญด้านความมั่นคง

เพื่อนำมาสร้างเป็นแผนภาพต้นไม้ความมั่นคง (Security Tree Diagram) และแปลงไปเป็นไวยากรณ์ความมั่นคงไม่พึ่งบริบทต่อไป

3.2.1 การสร้างแผนภาพต้นไม้ความมั่นคง

การสร้างแผนภาพต้นไม้ความมั่นคงนั้น มีวัตถุประสงค์เพื่อเป็นตัวกลางในการตรวจสอบความสอดคล้องระหว่างองค์ประกอบที่ปรากฏในแบบรูปและที่ปรากฏในไวยากรณ์ความมั่นคงที่ได้สร้างขึ้น โดนแผนภาพต้นไม้ในที่นี้จะนำแผนภาพเชิงเป้าหมาย (Goal Diagram) มาประยุกต์ใช้ โดยสัญลักษณ์ที่ใช้ในงานวิจัยนี้มีดังต่อไปนี้

ตารางที่ 3.1 สัญลักษณ์ ชื่อ และความหมายของสัญลักษณ์ที่ใช้ในแผนภาพต้นไม้ความมั่นคง

สัญลักษณ์	ชื่อ	ความหมาย
	AND gate	ส่วนประกอบบทเครื่องหมาย AND จะต้องประกอบด้วยส่วนประกอบทุกตัวที่ปรากฏภายใต้เครื่องหมาย AND
	OR gate	ส่วนประกอบบทเครื่องหมาย OR จะต้องประกอบด้วยส่วนประกอบบางตัวที่ปรากฏภายใต้เครื่องหมาย OR
+	PLUS	แสดงความสัมพันธ์ แบบ 0…* (ภายใต้ OR gate)
		แสดงความสัมพันธ์ แบบ 1…* (ภายใต้ AND gate)
	Non-Terminal	แสดงส่วนประกอบที่ประกอบด้วยองค์ประกอบย่อยอื่นๆ
	Terminal	แสดงส่วนประกอบที่ทราบค่า หรือไม่สามารถแยกเป็นองค์ประกอบย่อยอื่นได้อีก

จากรูปที่ 3.2 และรูปที่ 3.3 แสดงแผนภาพคลาสและแผนภาพลำดับของแบบรูปการตรวจสอบการเข้าถึงทรัพยากร สามารถนำมาสร้างเป็นแผนภาพต้นไม้ความมั่นคงได้โดยพิจารณาตามข้อกำหนดต่อไปนี้

1) การสร้างแผนภาพต้นไม้ คือ การพิจารณาองค์ประกอบที่ต้องปรากฏใน 1 ประโยคความต้องการความมั่นคงเท่านั้น

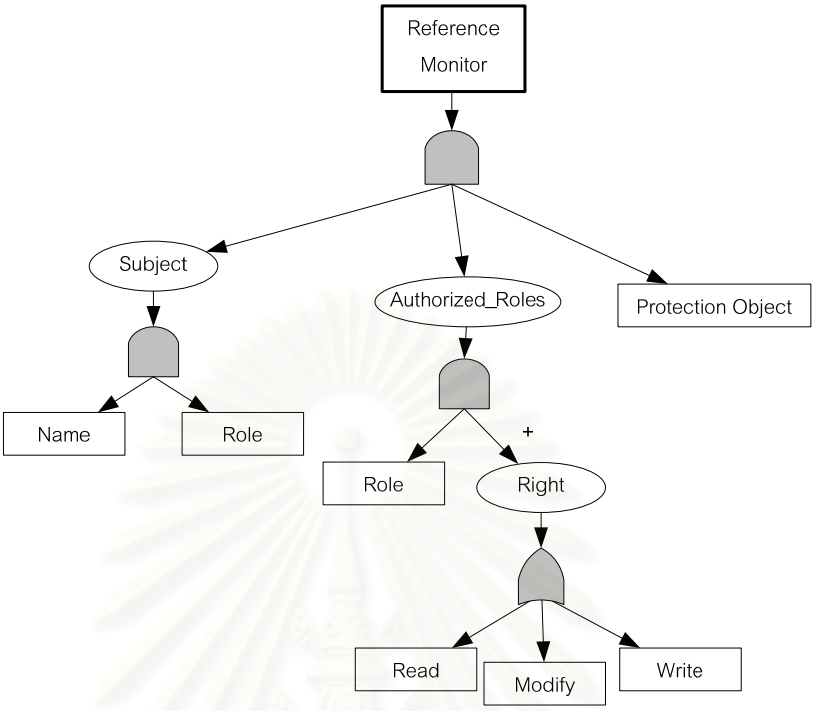
2) 1 ความต้องการมี “Subject” 1 รายการเท่านั้น

3) 1 ความต้องการมี “Protection Object” 1 รายการเท่านั้น

4) 1 ความต้องการมี “Right” สำหรับ “Role” ได้มากกว่า 1 รายการ

5) 1 ความต้องการมี “Role” 1 รายการเท่านั้น

จากข้อกำหนดข้างต้น สามารถสร้างเป็นแผนภาพต้นไม้ความมั่นคงได้ดังรูปที่ 3.5



รูปที่ 3.5 แผนภาพต้นไม้สำหรับแบบรูปการตรวจสอบการเข้าถึงทรัพยากร

จากรูปที่ 3.5 จะได้ว่าแบบรูปการตรวจสอบการเข้าถึงทรัพยากร จะต้องประกอบด้วย “Subject” “Authorized_Roles” และ “Protection Object” โดยมีรายละเอียดในภาพรวมดังนี้

“Subject” จะต้องประกอบด้วยชื่อและบทบาทที่ถือครองอยู่ เพื่อนำไปใช้เปรียบเทียบกับ “Authorized_Roles” ซึ่งเป็นชุดของการให้สิทธิ์สำหรับบทบาทแต่ละบทบาท เช่น “Doctor” เป็นบทบาทหนึ่งที่มีใน “Authorized_Roles” อาจมีสิทธิ์ในการแก้ไขข้อมูล (Modify) หรือมีสิทธิ์ทั้งอ่าน (Read) และแก้ไขข้อมูล “Protection_Object” ก็ได้ เนื่องจากสิทธิ์ดังกล่าวอยู่ภายใต้สัญลักษณ์ “OR gate”

ในทางปฏิบัติที่จะนำแบบรูปนี้ไปใช้นั้นจะต้องมีการกำหนดชุดของ “Authorized_Roles” เพื่อใช้เป็นตัวตั้งต้นสำหรับตรวจสอบผู้ที่ต้องการเข้าถึงทรัพยากรต่างๆ ว่ามีบทบาทตามที่กำหนดไว้หรือไม่ ถ้ามีก็จะได้รับสิทธิ์ตามที่ถูกกำหนดไว้ใน “Authorized_Roles” แล้วใช้สิทธิ์ดังกล่าวกับทรัพยากรเป้าหมายต่อไป

3.2.2 การสร้างไวยากรณ์ความมั่นคง

จากแผนภาพต้นไม้ดังรูปที่ 3.5 ทำให้เราทราบถึงองค์ประกอบและความสัมพันธ์ระหว่างองค์ประกอบภายในแบบรูป ซึ่งช่วยในการทวนสอบความสอดคล้องระหว่างองค์ประกอบที่ได้จากแบบรูปความมั่นคงกับไวยากรณ์ความมั่นคง ในขั้นตอนนี้จะทำการแปลงแผนภาพต้นไม้ความมั่นคงดังกล่าวไปเป็นไวยากรณ์ไม่พึ่งบริบท โดยมีแนวคิดและกฎ ซึ่งอ้างอิงจาก ISO/IEC 14977:1996 [22] ในการแปลงจากแผนภาพต้นไม้ดังนี้

1) องค์ประกอบของแบบรูปที่แสดงในแผนภาพต้นไม้จะต้องมีครบ แต่ไม่จำกัดลำดับขององค์ประกอบ

2) องค์ประกอบย่อยที่ประกอบกันเป็นองค์ประกอบใหญ่จะต้องมีจำนวนตามเครื่องหมายที่แสดง เช่น เครื่องหมาย ‘+’ ซึ่งแสดงจำนวนตั้งแต่ 0 ขึ้นไปเมื่ออยู่ภายใต้เครื่องหมาย OR gate และในทางกลับกัน จะแสดงจำนวนตั้งแต่ 1 ขึ้นไปเมื่ออยู่ภายใต้เครื่องหมาย AND gate

3) ใช้เครื่องหมาย ‘|’ แทน OR gate

4) ใช้เครื่องหมาย ‘,’ แทนการเชื่อมต่อสัญลักษณ์ หรือประโยค (ใช้แทน AND gate ได้)

5) ใช้เครื่องหมาย ‘;’ แสดงการสิ้นสุดของทุกกฎ

6) ใช้เครื่องหมาย ‘?...?’ แสดงถึงสัญลักษณ์หรืออักขระพิเศษ

7) ใช้เครื่องหมาย ‘=’ แทนการนิยามค่า

8) ใช้เครื่องหมาย ‘ “…” ’ ครอบสัญลักษณ์หรือข้อมูลที่ไม่สามารถแตกย่อยได้อีก

9) ใช้ตัวหนา สำหรับสัญลักษณ์หรือข้อมูลที่สามารถแตกย่อยได้อีก (ไม่ได้ถูกนิยามไว้ใน [22] แต่มีวัตถุประสงค์เพื่อให้เห็นความแตกต่างกับข้อความปกติ)

10) ใช้เครื่องหมาย ‘[…]’ ครอบทางเลือกทุกทางภายใต้ OR gate

11) ใช้เครื่องหมาย ‘ {…} ‘ แทนทางเลือก ที่สามารถปรากฏได้ตั้งแต่ 0 ครั้งขึ้นไป

12) ใช้เครื่องหมาย ‘ (*…*) ’ แทนข้อคิดเห็นที่จะแสดงในไวยากรณ์และไม่ถูกนำมาแปลงเป็นผลลัพธ์ของไวยากรณ์

เมื่อพิจารณารูปที่ 3.5 ร่วมกับแนวคิดและกฎข้างต้นจะได้ไวยากรณ์ความมั่นคงสำหรับการตรวจสอบการเข้าถึงทรัพยากรได้ดังรูปที่ 3.6

หากพิจารณาไวยากรณ์ที่ได้จากรูปที่ 3.6 สามารถอธิบายได้ว่า Ref-Monitor จะต้องประกอบด้วย “Subject” “Authorized-Role” และ “Protection Object” โดยแต่ละองค์ประกอบมีรายละเอียดดังนี้

Ref-Monitor	=	Subject , Authorized-Roles , Protection-Object , "." ;
Subject	=	Subject-Name , ", who acquires", Role-Name , " role, " ;
Subject-Name	=	? The name of subject such as person or process ? ;
Role-Name	=	? The defined role in organization based on its policy ? ;
Authorized-Roles	=	"is authorized to" , Right-List ;
Right-List	=	Right , {"," Right} ;
Right	=	["read" | "write" | "modify" | User-Define-Right] ;
		(* users can define a new right by themselves.
		This feature is supported by the prototyping tool *)
User-Define-Right	=	? A new right which defined by user ? ;
Protection-Object	=	? The name of asset which subject attempt to access ? ;

ตัวอย่างผลลัพธ์

Somsak, who acquires doctor role, is authorized to read, modify patient records.

Somsri, who acquires nurse role, is authorized to read the medical orders.

รูปที่ 3.6 ไวยากรณ์ความมั่นคงสำหรับแบบรูปการตรวจสอบการเข้าถึงทรัพยากรพร้อมตัวอย่างความต้องการความมั่นคง

1) "Subject" คือ ผู้ที่พยายามจะเข้าถึง "Protection Object" จะต้องมีการกำหนดว่าเป็นใครหรือกระบวนการใด พร้อมกับระบุบทบาทที่ใครหรือกระบวนการใดนั้นถือครองอยู่ เพื่อตรวจสอบกับ "Authorized-Roles" ว่า บทบาทของผู้ใช้หรือกระบวนการใดที่ส่งเข้ามานั้นมีหรือไม่ ถ้ามีจะให้สิทธิ์ตามที่กำหนดไว้เท่านั้น ถ้าบทบาทดังกล่าวไม่ปรากฏใน "Authorized-Roles" ก็จะไม่สามารถเข้าถึง "Protection-Object" ได้

2) "Authorized_Roles" ในความหมายของแบบรูป คือ กลุ่มของบทบาทที่ได้มีการกำหนดสิทธิ์ให้แล้วว่าสามารถทำอะไรได้บ้าง สำหรับในไวยากรณ์นี้จะเป็นการแสดงให้เห็นว่าง "Role" ของ "Subject" นั้นสามารถทำอะไรได้บ้าง เพื่อให้มีความสมบูรณ์ในประโยคของความต้องการความมั่นคง ดังนั้นจึงสังเกตได้ว่าในไวยากรณ์ส่วนที่เป็น "Authorized_Roles" จะละส่วนประกอบ "Role" ไว้ เนื่องจาก "Role" ที่ปรากฏใน "Authorized_Roles" จะต้องเหมือนกับ "Role" ของ "Subject" เสมอ ดังนั้น "Authorized_Roles" จึงแสดงเฉพาะรายงานของสิทธิ์ที่บทบาทนั้นๆ สามารถทำได้

3) "Protection Object" เป็นสินทรัพย์องค์กรที่ถูกกำหนดไว้แล้ว ซึ่งจะถูกเข้าถึงโดย "Subject" ที่มีสิทธิ์ตามบทบาทที่ "Subject" นั้นถือครองอยู่

จากผลลัพธ์ที่ได้ในรูปที่ 3.6 สรุปได้ว่า Somsak และ Somsri เป็น “Subject” ที่พยายามจะทำการเข้าถึงข้อมูลผู้ป่วย (Patient Records) ซึ่งเป็น “Protection Object” โดย Somsak และ Somsri จะมีสิทธิ์ตามบทบาทที่ตนเองได้รับเท่านั้น ได้แก่ “doctor” และ “nurse” ตามลำดับ ดังนั้น Somsak ที่มีบทบาทเป็น “doctor” สามารถเข้าไปอ่านและแก้ไขข้อมูลผู้ป่วยได้ ขณะที่ Somsri มีสิทธิ์เพียงอ่านข้อมูลผู้ป่วยเท่านั้น กล่าวคือ สิทธิ์ในการดำเนินการใดๆ ไม่สามารถทำได้ หากไม่ได้ถูกการกำหนดไว้ใน “Authorized_Roles”

3.3 การตรวจสอบไวยากรณ์ความมั่นคง

การตรวจสอบไวยากรณ์ความมั่นคงประกอบด้วย 3 ขั้นตอน ได้แก่ การตรวจสอบความสมเหตุสมผลของไวยากรณ์ความมั่นคง การวิเคราะห์ความสัมพันธ์ภายในไวยากรณ์ความมั่นคง และการวิเคราะห์ความสัมพันธ์ระหว่างไวยากรณ์ความมั่นคง โดยมีรายละเอียดดังต่อไปนี้

3.3.1 การตรวจสอบความสมเหตุสมผลของไวยากรณ์ความมั่นคง

การตรวจสอบความสมเหตุสมผลของไวยากรณ์ความมั่นคง มีวัตถุประสงค์เพื่อตรวจสอบความถูกต้องของความต้องการความมั่นคงที่ได้จากไวยากรณ์ความมั่นคง ว่าสอดคล้องและถูกต้องใกล้เคียงกับแบบรูปความมั่นคง โดยการพิจารณาร่วมกันกับผู้เชี่ยวชาญและมีประสบการณ์ด้านความมั่นคง เพื่อรับข้อแสนอแนะและความคิดเห็นเพื่อใช้ปรับปรุงไวยากรณ์ให้มีความถูกต้องและเหมาะสมมากขึ้น

อย่างไรก็ตามการปรับปรุงไวยากรณ์เกิดจากการวิเคราะห์และพิจารณาความสมเหตุสมผลของไวยากรณ์ของแต่ละแบบรูปว่ามีองค์ประกอบใดที่ต้องเพิ่มเติมหรือตัดทอนบ้าง การเพิ่มเติมอาจเกิดจากการเพิ่มองค์ประกอบให้มีความครบถ้วนสมบูรณ์มากขึ้นกว่าองค์ประกอบที่ได้จากแบบรูปเดิม หรือเกิดจากการผนวกรวมไวยากรณ์เข้าด้วยกัน การตรวจสอบความสมเหตุสมผลในหัวข้อของการปรับปรุงไวยากรณ์ที่ต้องพิจารณาคือ ความสัมพันธ์ที่ปรากฏขึ้นทั้งภายในและภายนอกไวยากรณ์

3.3.2 การวิเคราะห์ความสัมพันธ์ภายในไวยากรณ์

การวิเคราะห์ความสัมพันธ์ภายในไวยากรณ์ มีวัตถุประสงค์เพื่อพิจารณาบางองค์ประกอบที่ปรากฏในไวยากรณ์ว่ามีความซ้ำซ้อนขององค์ประกอบหรือไม่ ถ้ามีจะต้องดูว่าองค์ประกอบดังกล่าวมีวัตถุประสงค์หรือมีหน้าที่อะไร

จากตัวอย่างไวยากรณ์ที่แสดงดังรูปที่ 3.5 จะพบองค์ประกอบ “Role” ปรากฏทั้งใน “Authorized_Roles” และ “Subject” หากพิจารณาความหมายของ “Role” ในไวยากรณ์นี้ คือ บทบาทหรือหน้าที่ ที่ถูกกำหนดให้กับบุคคลตามนโยบายขององค์กร บุคคลที่มีบทบาทใดๆ จะ

สามารถดำเนินงานภายในองค์กรตามที่บทบาทนั้นได้รับ ดังนั้น “Role” ทั้ง 2 ตำแหน่งที่ปรากฏคือตัวเดียวกัน ดังนั้นไวยากรณ์จึงต้องมีการปรับปรุงโดยการลดรูปของ “Role” ออกไปเมื่อทำการสร้างไวยากรณ์ และจะได้ไวยากรณ์ผลลัพธ์ดังรูปที่ 3.6

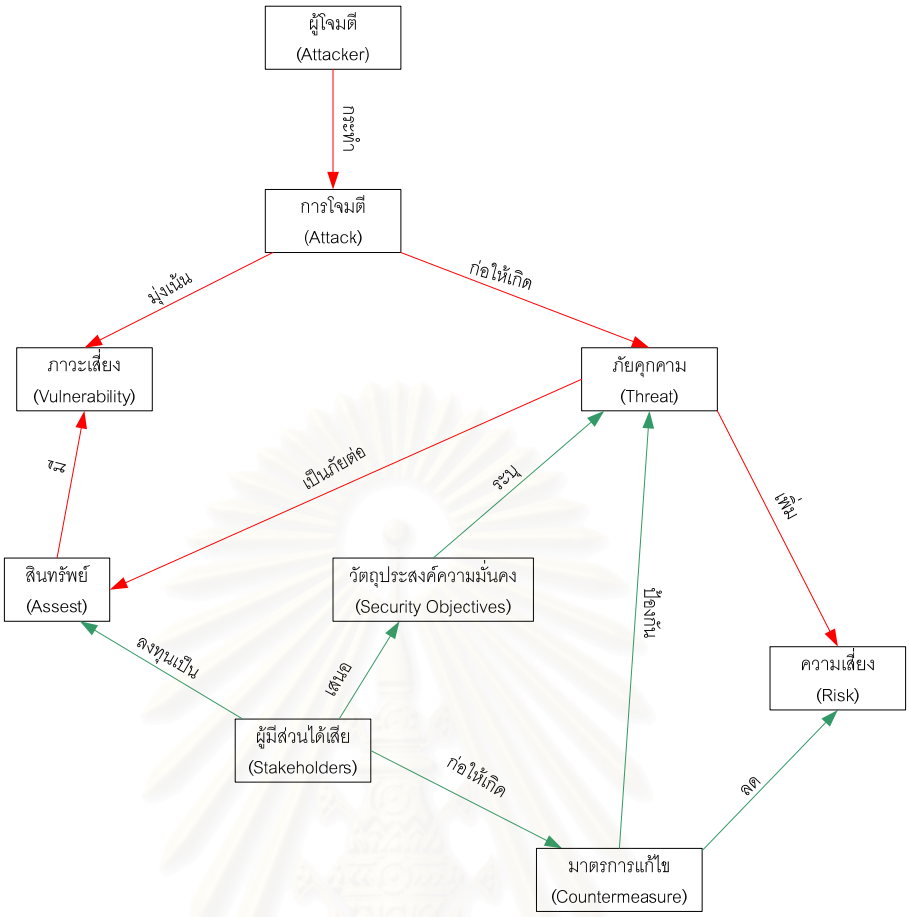
จากที่กล่าวมาข้างต้นเป็นตัวอย่างในการพิจารณาความสัมพันธ์ต่างๆ ภายในไวยากรณ์ ซึ่งช่วยให้ไวยากรณ์มีความเหมาะสมและถูกต้องมากขึ้น อย่างไรก็ตาม เมื่อพิจารณาภายในไวยากรณ์อาจไม่เพียงพอ จึงจำเป็นต้องวิเคราะห์ความสัมพันธ์ระหว่างไวยากรณ์ด้วย

3.3.3 การวิเคราะห์ความสัมพันธ์ระหว่างไวยากรณ์

นอกจากการวิเคราะห์องค์ประกอบและความสัมพันธ์ระหว่างองค์ประกอบภายในไวยากรณ์ความมั่นคงแล้ว ความสัมพันธ์ระหว่างแบบรูปความมั่นคงก็เป็นสิ่งสำคัญที่ต้องพิจารณาด้วยเช่นกัน เนื่องจากการกำหนดความต้องการความมั่นคงสำหรับสิ่งใดก็ตาม อาจได้มาจากผลลัพธ์ของแบบรูปความมั่นคงมากกว่า 1 แบบรูป ในบทนี้จะขอยกตัวอย่าง 2 แบบรูป คือ แบบรูปการตรวจสอบการเข้าถึงทรัพยากรซึ่งเป็นตัวอย่างต่อเนื่องจากขั้นตอนที่แล้ว และแบบรูปการกำหนดค่าความเสี่ยงซึ่งจะต้องอาศัยแผนภาพในรูปที่ 3.7 มาร่วมพิจารณา เนื่องจากรูปดังกล่าวมีการแสดงความสัมพันธ์ในลักษณะเป็นเหตุเป็นผลกันระหว่างส่วนประกอบความต้องการความมั่นคง เช่น สินทรัพย์ ภัยคุกคาม ภาวะเสี่ยง และค่าความเสี่ยง เป็นต้น

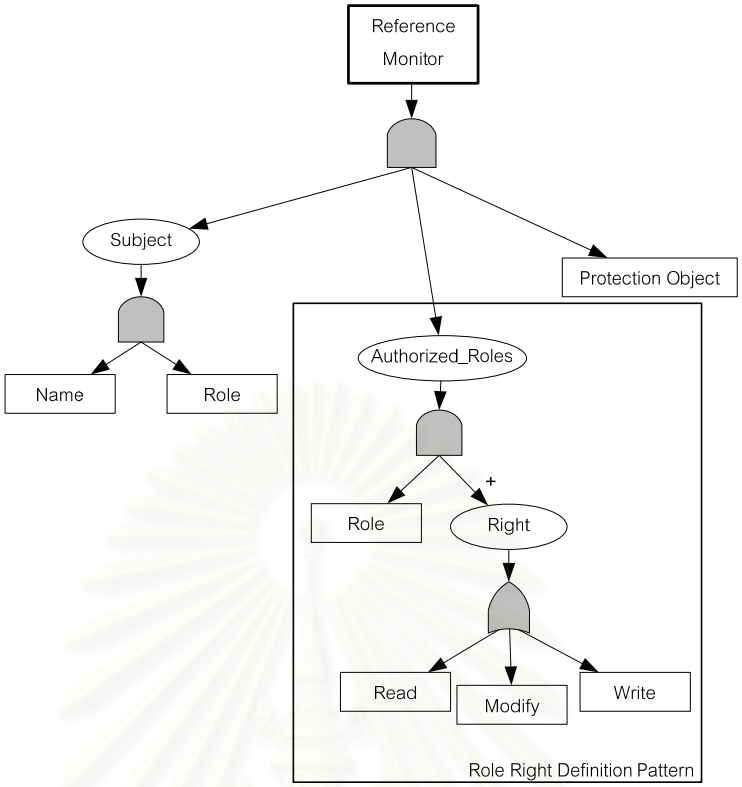
จากการศึกษาโดยผู้วิจัยและผู้ชำนาญการด้านความมั่นคงพบว่า แบบรูปการตรวจสอบการเข้าถึงทรัพยากรสามารถนำไปใช้ในทางปฏิบัติได้หากมีการกำหนดสิทธิ์ต่างๆ ให้กับแต่ละบทบาทที่ปรากฏในองค์กรไว้ก่อน แล้วจึงข้อมูลสิทธิ์สำหรับบทบาทดังกล่าวมาใช้เพื่อกำหนดความต้องการความมั่นคงจากแบบรูปการตรวจสอบการเข้าถึงทรัพยากรได้

พิจารณาจากรูปที่ 3.5 ซึ่งแสดงแผนภาพต้นไม้ความมั่นคงสำหรับแบบรูปการตรวจสอบการเข้าถึงทรัพยากร เมื่อพิจารณาโดยละเอียดพบว่า แบบรูปดังกล่าวได้ผนวกรวมเอาแบบรูปการกำหนดสิทธิ์ให้กับบทบาทเข้าไว้ด้วย ดังแสดงในรูปที่ 3.8



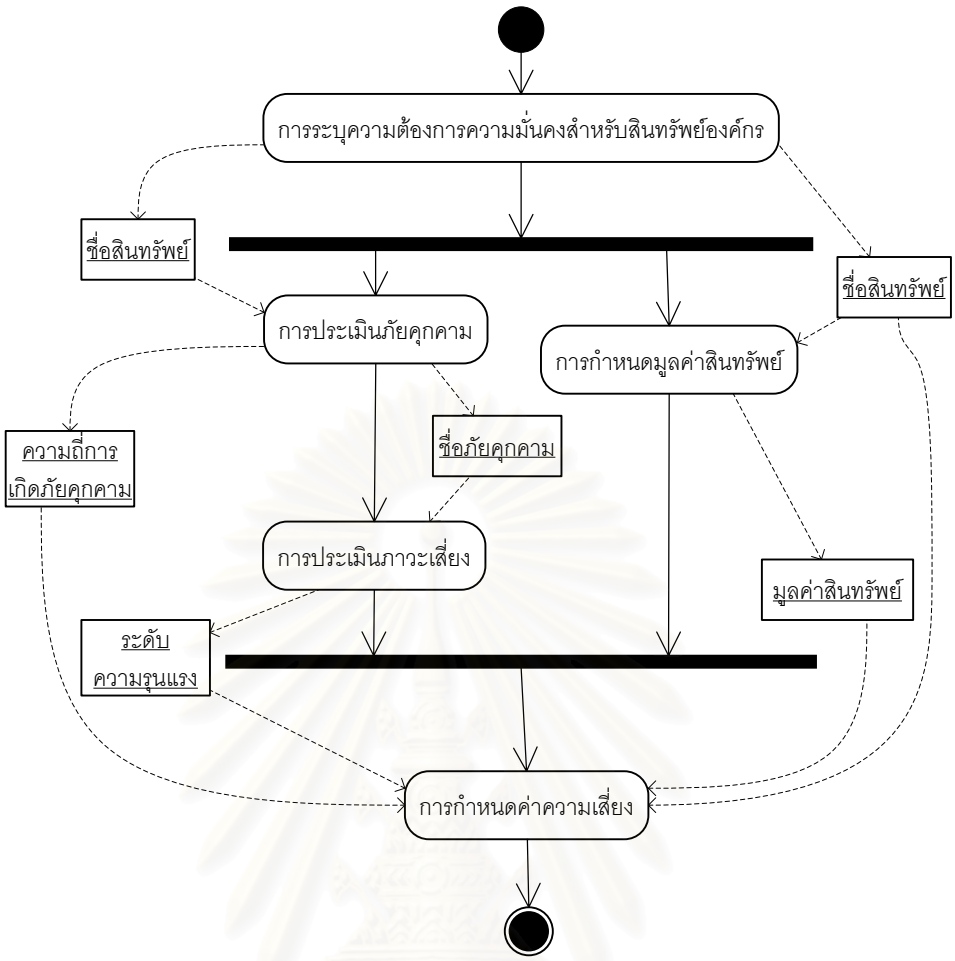
รูปที่ 3.7 แผนภาพแสดงสาเหตุและผลกระทบของส่วนประกอบในความต้องการความมั่นคง [6]

แบบรูปการกำหนดสิทธิ์ให้กับบทบาท เป็นแบบรูปความมั่นคงที่นำเสนอแนวทางในการกำหนดสิทธิ์ให้กับบทบาทตามนโยบายขององค์กร โดยอาศัยหลักการให้เอกสิทธิ์ระดับต่ำ (Least Privilege) ซึ่งเป็นหลักการพื้นฐานสำหรับระบบความมั่นคง เมื่อมีการกำหนดสิทธิ์ให้กับบทบาทแล้ว ก็สามารถนำข้อมูลดังกล่าวไปประยุกต์ใช้ในการควบคุมการเข้าถึงเชิงบทบาท (Role-Based Access Control) และการตรวจสอบการเข้าถึงทรัพยากรได้ ดังนั้นจึงมีความจำเป็นต้องใช้แบบรูปการนิยามสิทธิ์ให้กับบทบาทก่อนการใช้แบบรูปการตรวจสอบการเข้าถึงทรัพยากร และการควบคุมการเข้าถึงเชิงบทบาทได้ โดยในงานวิจัยนี้แนวคิดในการตรวจสอบลำดับ และเงื่อนไขก่อนการใช้ไวยากรณ์ความมั่นคงจากแบบรูปความมั่นคงนั้น จะเป็นหน้าที่ของเครื่องมือต้นแบบซึ่งจะกล่าวรายละเอียดในบทที่ 4



รูปที่ 3.8 แผนภาพต้นไม้ของแบบรูปการตรวจสอบการเข้าถึงทรัพยากรที่แสดงส่วนประกอบจากแบบรูปอื่น

ตัวอย่างแบบรูปความมั่นคงอีกแบบรูปหนึ่งที่มีความสัมพันธ์ในลักษณะขึ้นต่อกันที่ชัดเจนที่สุดคือ แบบรูปการกำหนดค่าความเสี่ยง เนื่องจากการกำหนดความเสี่ยงจะต้องใช้ข้อมูลสินทรัพย์ (Asset) และมูลค่าของสินทรัพย์ (Asset Value) ข้อมูลภัยคุกคาม (Threat) และความถี่ของการเกิดภัยคุกคาม (Threat Likelihood Scale) ภาวะเสี่ยงต่อการเกิดภัยคุกคาม (Vulnerability) และระดับความรุนแรงของความเสี่ยงต่อภัยคุกคาม (Severity Scale) ซึ่งข้อมูลที่กล่าวมานี้ล้วนมาจากแต่ละแบบรูปความมั่นคงที่เกี่ยวข้อง ได้แก่ การระบุความต้องการความมั่นคงสำหรับสินทรัพย์องค์กร (Security Needs Identification for Enterprise Assets) การกำหนดมูลค่าสินทรัพย์ (Asset Valuation) การประเมินภัยคุกคาม (Threat Assessment) และการประเมินภาวะเสี่ยง (Vulnerability Assessment) โดยหากพิจารณาร่วมกับแผนภาพดังรูปที่ 3.7 สามารถแสดงเป็นลำดับการใช้งานแบบรูปความมั่นคงได้ดังรูปที่ 3.9



รูปที่ 3.9 แผนภาพลำดับการใช้งานแบบรูปต่างๆ เพื่อกำหนดความเสี่ยงสำหรับสินทรัพย์องค์กร

ดังนั้นจากขอบเขตงานวิจัยทั้งหมดซึ่งได้ศึกษาโครงสร้างของแบบรูปความมั่นคงและสร้างไวยากรณ์ความมั่นคงสำหรับแบบรูปความมั่นคงโดยอาศัยองค์ประกอบและความสัมพันธ์ขององค์ประกอบระหว่างแบบรูปความมั่นคง สามารถแสดงความสัมพันธ์ระหว่างไวยากรณ์ความมั่นคงที่สร้างจากแบบรูปความมั่นคงได้ดังตารางที่ 3.2 ซึ่งแสดงให้เห็นว่าแต่ละไวยากรณ์ความมั่นคงนั้นต้องการใช้ หรือต้องมีข้อมูลใดบ้าง ก่อนการใช้งานไวยากรณ์ดังกล่าวและไวยากรณ์ใดที่ผนวกรวมไวยากรณ์อื่นเข้าไว้ด้วยกัน

จากตารางที่ 3.2 พบว่าไวยากรณ์สำหรับกำหนดค่าความเสี่ยง (GM65) จะต้องการใช้ข้อมูล ชื่อสินทรัพย์ มูลค่าของสินทรัพย์ ความถี่ของการเกิดภัยคุกคาม และระดับความรุนแรงของความเสี่ยงต่อภัยคุกคาม จากไวยากรณ์การระบุความต้องการความมั่นคงสำหรับทรัพย์สินองค์กร (GM61) ไวยากรณ์การกำหนดมูลค่าสินทรัพย์ (GM62) ไวยากรณ์การประเมินภัยคุกคาม (GM63) และไวยากรณ์การประเมินภาวะเสี่ยง (GM64) ตามลำดับ ซึ่งสอดคล้องกับรูปที่ 3.9

ในทำนองเดียวกัน ไวยากรณ์การตรวจสอบการเข้าถึงทรัพยากร (GM84) จะมีการผนวกไวยากรณ์การกำหนดสิทธิ์สำหรับบทบาท (GM85) เข้าไว้ด้วยกัน ซึ่งจะสังเกตว่ามีข้อความ “Include” ปรากฏอยู่ในคอลัมน์ของ GM85 ในแถวของ GM84 ซึ่งสอดคล้องการนำเสนอแบบรูปการตรวจสอบการเข้าถึงทรัพยากรในหัวข้อ 3.3.3

สำหรับไวยากรณ์อื่นๆ ที่ไม่ได้กล่าวในที่นี้นั้น มีแนวคิดในการพิจารณาใกล้เคียงกันโดยได้แสดงความสัมพันธ์ของไวยากรณ์อื่นๆ ดังตารางที่ 3.2 แล้ว สำหรับรายละเอียดของไวยากรณ์ความมั่นคงที่สร้างขึ้นพร้อมรายละเอียดสำหรับแต่ละไวยากรณ์แสดงดังภาคผนวก ข

ตารางที่ 3.2 ตารางสรุปความสัมพันธ์ระหว่างแบบรูปความมั่นคง

	GM61	GM62	GM63	GM64	GM65	GM66	GM67	GM68	GM71	GM72	GM73	GM74	GM82	GM83	GM84	GM85	GM121	GM122	GM123
GM61																			
GM62	AssetName																		
GM63	AssetName																		
GM64			ThreatName																
GM65	AssetName	AssetValue	LikelihoodScale	SeverityScale															
GM66	AssetName				RiskValue		Included												
GM67	AssetName																		
GM68	AssetName								IASerivce										
GM71										Include	Include	Include							
GM72									IA Service										
GM73										IA Service + Password									
GM74										IA Service + Biometric									
GM81	AssetName																		
GM82	AssetName															AuthorizedRole			
GM83	AssetName																		
GM84	AssetName															Include			
GM85	AssetName																		
GM121	AssetName																	Include	Include
GM122	AssetName																		
GM123	AssetName																		

GM61 การระบุความต้องการความมั่นคงสำหรับสินทรัพย์องค์กร (Security Needs Identification for Enterprise Assets)

GM62 การกำหนดมูลค่าสินทรัพย์ (Asset Valuation)

GM63 การประเมินภัยคุกคาม (Threat Assessment)

GM64 การประเมินภาวะเสี่ยง (Vulnerability Assessment)

GM65 การกำหนดความค่าความเสี่ยง (Risk Determination)

GM66 แนวคิดความมั่นคงองค์กร (Enterprise Security Approaches)

GM67 บริการความมั่นคงองค์กร (Enterprise Security Services)

GM68 การสื่อสารของผู้มีหุ้นส่วนองค์กร (Enterprise Partner Communication)

GM71 ความต้องการการระบุและการพิสูจน์ตัวตน (I&A Requirements)

GM72 ทางเลือกการออกแบบการระบุและการพิสูจน์ตัวตน (Automated I&A Design Alternative)

GM73 การออกแบบและใช้งานรหัสผ่าน (Password Design and Use)

GM74 ทางเลือกการออกแบบชีวมิติ (Biometric Design Alternative)

GM81 การให้อำนาจ (Authorization)

GM82 การควบคุมการเข้าถึงเชิงบทบาท (Role-Based Access Control)

GM83 ความมั่นคงหลายระดับ (Multilevel Security)

GM84 การเฝ้าสังเกตเชิงอ้างอิง (Reference Monitor)

GM85 การนิยามสิทธิ์ให้กับบทบาท (Role Rights Definition)

GM121 ไฟล์วอลล์กรองแพ็คเกจ (Packet Filter Firewall)

GM122 ไฟล์วอลล์เชิงตัวแทน (Proxy-Based Firewall)

GM123 ไฟล์วอลล์เชิงสถานะ (Stateful Firewall)

บทที่ 4
การออกแบบและพัฒนาเครื่องมือต้นแบบสำหรับ สร้างความต้องการความมั่นคงจากไวยากรณ์ความมั่นคง

ภายหลังจากการสร้างไวยากรณ์ความมั่นคงแล้ว การนำไวยากรณ์ความมั่นคงไปใช้งานโดยผู้ใช้ทั่วไปนั้นทำได้ยาก ดังนั้นเพื่อช่วยให้ผู้ใช้มีความสะดวกในการใช้ไวยากรณ์เพื่อกำหนดความต้องการความมั่นคง ผู้วิจัยจึงได้พัฒนาเครื่องมือที่อยู่บนพื้นฐานของไวยากรณ์ที่สร้างขึ้นเพื่อใช้ในการสร้างความต้องการความมั่นคง ในบทนี้จะกล่าวถึงการออกแบบและการพัฒนาเครื่องมือต้นแบบเพื่อสร้างความต้องการความมั่นคงจากไวยากรณ์ความมั่นคง ประกอบด้วย การออกแบบหน้าที่การทำงานของเครื่องมือ การออกแบบส่วนต่อประสานผู้ใช้ และสภาพแวดล้อมในการพัฒนาเครื่องมือ โดยมีรายละเอียดดังนี้

4.1 การออกแบบหน้าที่การทำงานของเครื่องมือต้นแบบ

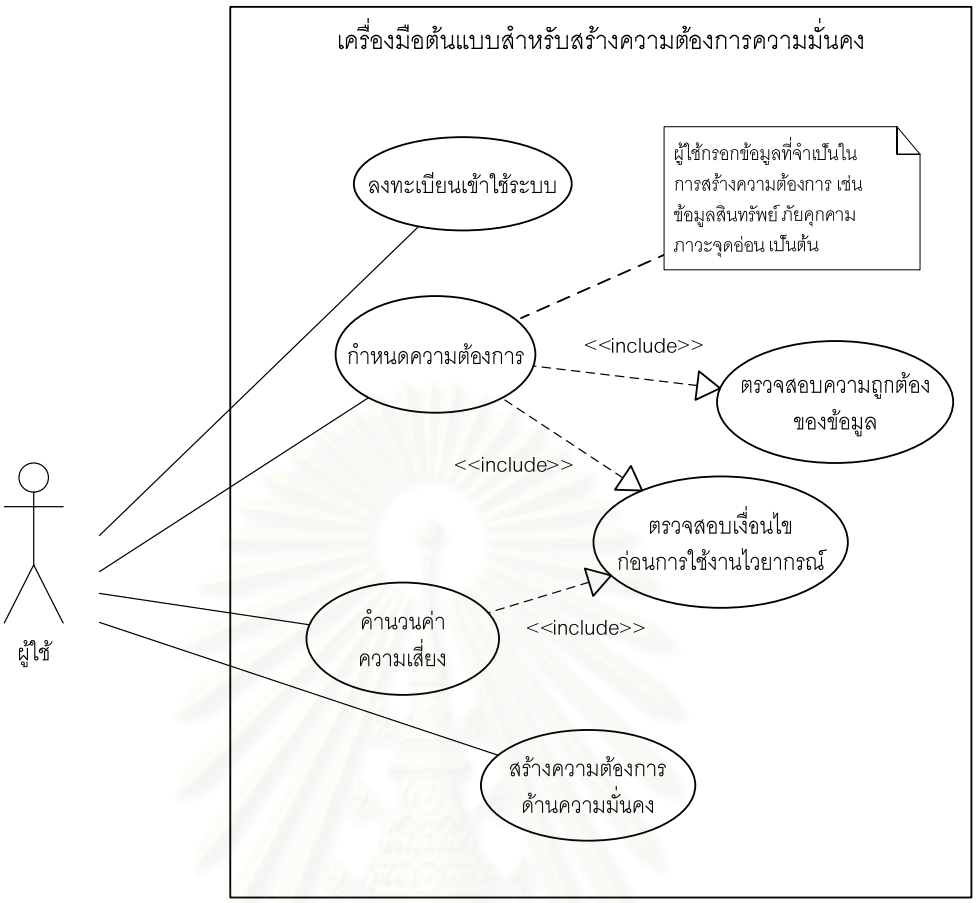
เครื่องมือต้นแบบสำหรับสร้างความต้องการความมั่นคงนั้น เป็นเครื่องมือที่สนับสนุนการดำเนินการและการจัดการความต้องการด้านความมั่นคง และอำนวยความสะดวกให้กับผู้ใช้ โดยหน้าที่การทำงานของเครื่องมือต้นแบบนี้สามารถนำเสนอด้วยแผนภาพยูสเคส (Use Case Diagram) ซึ่งเป็นแผนภาพที่อธิบายการติดต่อกันระหว่างผู้ใช้ระบบ (Actors) กับฟังก์ชันงานต่างๆ ที่ปรากฏในระบบ ดังนั้นในการพัฒนาเครื่องมือต้นแบบนี้ สามารถนำเสนอฟังก์ชันงานต่างๆ และการติดต่อระหว่างฟังก์ชันงาน หรือฟังก์ชันงานกับผู้ใช้ ดังรูปที่ 4.1 โดยมีรายละเอียดดังนี้

1) ส่วนลงทะเบียนเข้าใช้ระบบ

สำหรับให้ผู้ใช้ทำการป้อนชื่อและรหัสผ่านเพื่อเข้าใช้งานเครื่องมือ ซึ่งข้อมูลและความต้องการที่เกิดขึ้นนั้นจะจำแนกตามแต่ละบัญชีผู้ใช้

2) ส่วนการกำหนดความต้องการ

เป็นส่วนหลักของเครื่องมือต้นแบบเพื่อเลือกไวยากรณ์ที่ต้องการมากำหนดความต้องการความมั่นคง โดยการเข้าใช้งานบางไวยากรณ์จะต้องมีการตรวจสอบเงื่อนไขก่อนการใช้ไวยากรณ์ ซึ่งหากไม่ผ่านเงื่อนไขใดเงื่อนไขหนึ่งก็จะไม่สามารถใช้ไวยากรณ์ดังกล่าวได้ หากผ่านเงื่อนไขและมีการป้อนข้อมูลโดยผู้ใช้แล้ว เมื่อผู้ใช้คิดว่ากำหนดข้อมูลครบแล้วก็สามารถกดปุ่มยืนยันข้อมูล หากเครื่องตรวจสอบพบข้อผิดพลาด หรือข้อมูลสำหรับบางองค์ประกอบหายไป ก็จะไม่อนุญาตให้ทำการบันทึกข้อมูลความต้องการดังกล่าว



รูปที่ 4.1 แผนภาพยูสเคสของเครื่องมือต้นแบบการสร้างความต้องการความมั่นคง

3) ส่วนการคำนวณค่าความเสี่ยง

เป็นส่วนแสดงให้เห็นถึงค่าความเสี่ยงที่ปรากฏต่อสินทรัพย์ขององค์กร ซึ่งจะต้องใช้กับสินทรัพย์ที่มีการกำหนดมูลค่าสินทรัพย์ ภัยคุกคามและความถี่ของการเกิดภัยคุกคามของสินทรัพย์ และ ภาวะเสี่ยงและระดับความรุนแรง ผลที่ได้จะถูกนำเสนอด้วยระดับความเสี่ยงเชิงคุณภาพ (Qualitative Risk Scale) ซึ่งมี 6 ระดับ [6] ได้แก่ ไม่มีผลต่อความเสี่ยง (Negligible) มีความเสี่ยงน้อย (Low) มีความเสี่ยงปานกลาง (Medium) มีความเสี่ยงมาก (High) มีความเสี่ยงสูงมาก (Very High) มีความเสี่ยงสูงสุด (Extreme)

4) ส่วนการสร้างความต้องการด้านความมั่นคง

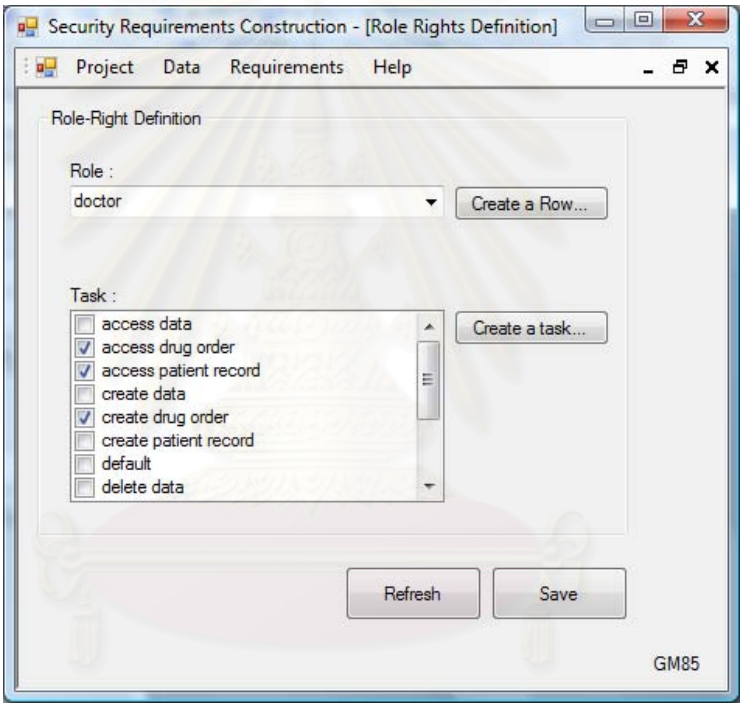
สำหรับบางไวยากรณ์จะสามารถสร้างรายงานเพื่อแสดงภาพรวมของความต้องการแต่ละประเภท เพื่อช่วยในการตัดสินใจในการเลือกแนวคิดและบริการความมั่นคงมาประยุกต์ใช้ได้อย่างเหมาะสม

4.2 การออกแบบส่วนต่อประสานผู้ใช้ของเครื่องมือ

ส่วนต่อประสานผู้ใช้ของเครื่องมือต้นแบบ ถูกพัฒนาขึ้นให้สอดคล้องกับข้อมูลองค์ประกอบของแบบรูปความมั่นคงที่นำมาสร้างเป็นไวยากรณ์ความมั่นคง โดยข้อมูลนำเข้าของแต่ละไวยากรณ์แบ่งเป็น 2 แบบ ได้แก่ ข้อมูลนำเข้า (Input) จากผู้ใช้ และข้อมูลนำเข้าจากผลลัพธ์ของไวยากรณ์อื่นที่เกี่ยวข้อง โดยมีรายละเอียดดังนี้

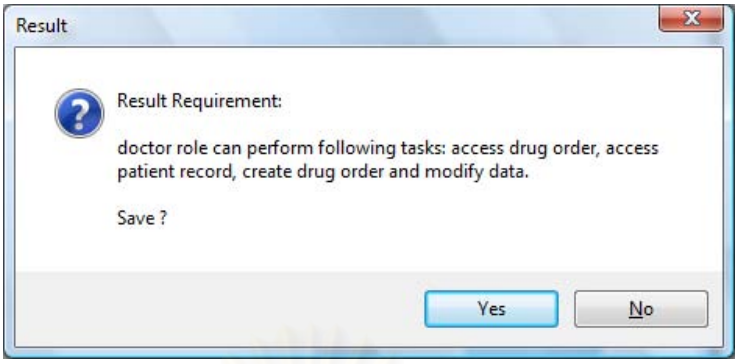
1) ส่วนต่อประสานผู้ใช้สำหรับป้อนข้อมูลนำเข้าโดยผู้ใช้

การออกแบบส่วนต่อประสานผู้ใช้ ใช้หลักการการออกแบบให้สอดคล้องกับไวยากรณ์ความมั่นคงสำหรับการรับข้อมูลนำเข้าจากผู้ใช้ ที่จำเป็นในการสร้างความต้องการความมั่นคง ตัวอย่างไวยากรณ์การนิยามสิทธิ์สำหรับบทบาท ซึ่งแสดงดังรูปที่ 4.2



รูปที่ 4.2 หน้าจอสำหรับกำหนดความต้องการจากไวยากรณ์การนิยามสิทธิ์สำหรับบทบาท

จากรูปที่ 4.2 เป็นไวยากรณ์ที่ได้จากแบบรูปการนิยามสิทธิ์สำหรับบทบาท ซึ่งประกอบด้วยองค์ประกอบหลักซึ่งสอดคล้องกับแผนภาพต้นไม้ความมั่นคงในรูปที่ 3.8 ได้แก่ “Role” ซึ่งเป็นบทบาทต่างๆ ที่ถูกกำหนดไว้ตามนโยบายขององค์กร และ “Right” ซึ่งเป็นการให้สิทธิ์ว่า “Role” ที่เลือกมานั้นสามารถดำเนินการอะไรได้บ้าง โดยปกติเครื่องมือจะกำหนดค่าโดยปริยาย (Default) ไว้ให้บางส่วน ตามที่แบบรูปความมั่นคงได้นำเสนอไว้ เช่น สิทธิ์ “Read” “Write” และ “Modify” อย่างไรก็ตาม เครื่องมือต้นแบบมีความสามารถให้ผู้ใช้สามารถเพิ่มข้อมูลบทบาทและสิทธิ์ที่ต้องการได้ด้วยตนเอง ตัวอย่างผลลัพธ์ที่ได้จากการกำหนดความต้องการจากรูปที่ 4.2 แสดงดังรูปที่ 4.3



รูปที่ 4.3 ความต้องการความมั่นคงจากไวยากรณ์การกำหนดสิทธิ์สำหรับบทบาท

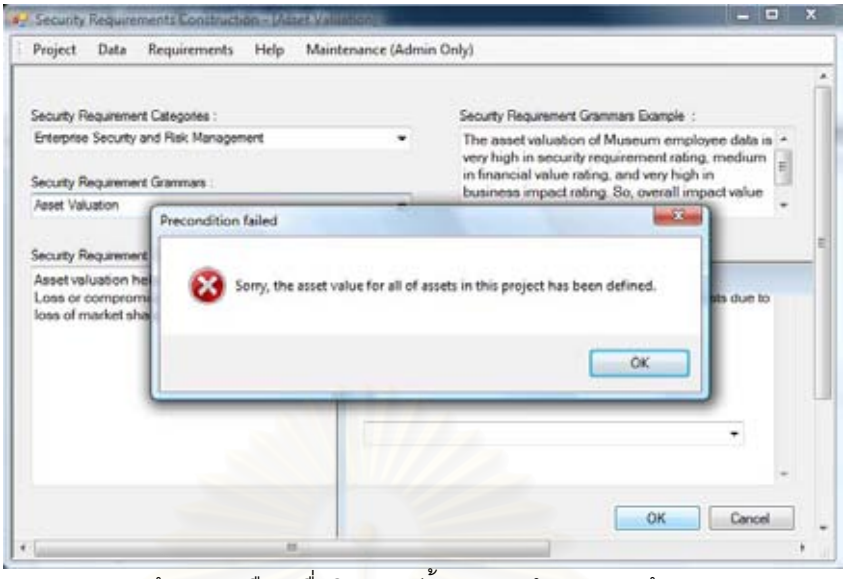
หากพิจารณาองค์ประกอบที่ปรากฏในหน้าจอพบว่า ข้อมูลที่ผู้ใช้ต้องป้อนหรือเลือกนั้นจะเป็นไปตามไวยากรณ์ที่ได้นิยามไว้แล้วจากการสร้างไวยากรณ์ความมั่นคงในบทที่ 3 ซึ่งแสดงให้เห็นถึงความสอดคล้องของไวยากรณ์ความมั่นคงกับส่วนต่อประสานผู้ใช้สำหรับไวยากรณ์นั้น

2) การใช้ข้อมูลนำเข้าจากผลลัพธ์ของไวยากรณ์อื่นๆ

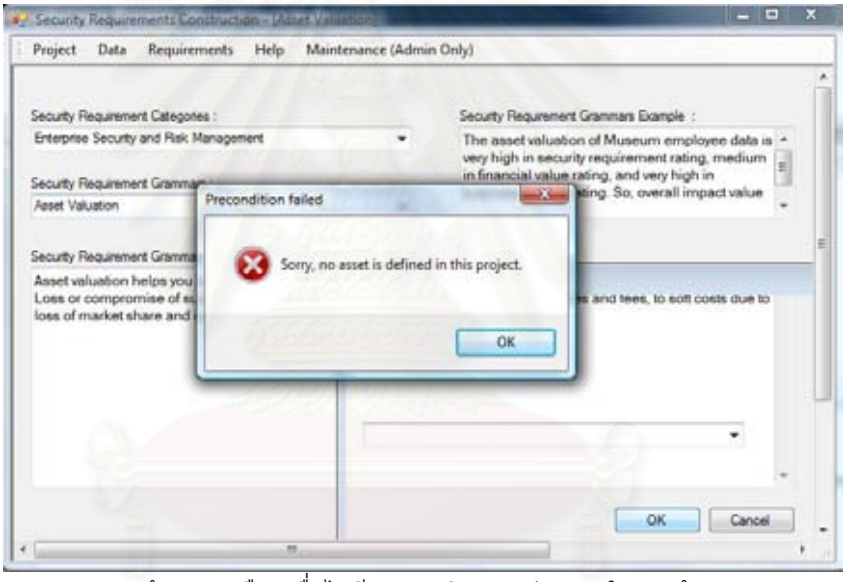
จากตารางที่ 3.2 ซึ่งเป็นตารางที่สรุปภาพรวมของไวยากรณ์ความมั่นคงในขอบเขตงานวิจัยว่า ไวยากรณ์ที่กำลังพิจารณานั้นจะต้องใช้ข้อมูลอะไรจากแบบรูปใดบ้าง ซึ่งหากไม่มีข้อมูลที่จำเป็นก่อนการใช้ไวยากรณ์ โปรแกรมจะไม่อนุญาตให้ใช้งานไวยากรณ์ดังกล่าวได้

ในที่นี้จะพิจารณาไวยากรณ์การกำหนดมูลค่าสินทรัพย์ (GM62) ซึ่งเป็นไวยากรณ์ในการกำหนดค่าให้กับสินทรัพย์ด้วยปัจจัยต่างๆ โดยจะต้องใช้ข้อมูลชื่อสินทรัพย์จากไวยากรณ์การระบุความต้องการความมั่นคงสำหรับสินทรัพย์องค์กร (GM61) หากผู้ใช้ไม่เคยสร้างข้อมูลสินทรัพย์โดยใช้ไวยากรณ์นี้มาก่อน ก็ไม่สามารถใช้ไวยากรณ์กำหนดมูลค่าสินทรัพย์ได้ และเครื่องมือจะมีกล่องข้อความแจ้งความผิดพลาดที่พบดังรูปที่ 4.4

จากรูปที่ 4.4 แสดงให้เห็นว่าเครื่องมือตรวจสอบพบว่า ในกรณีที่ข้อมูลสินทรัพย์ทั้งหมดได้ถูกกำหนดค่าสินทรัพย์แล้วทุกตัว เครื่องมือจะแจ้งให้ทราบว่าสินทรัพย์ทั้งหมดได้มีการกำหนดมูลค่าไว้หมดแล้วดังรูปที่ 4.4 (ก) ในทำนองเดียวกันหากไม่มีข้อมูลสินทรัพย์ปรากฏในฐานข้อมูล เครื่องมือจะแจ้งข้อความว่าไม่พบข้อมูลสินทรัพย์ภายในระบบดังรูปที่ 4.4 (ข)



(ก) ข้อความเตือนเมื่อสินทรัพย์ทั้งหมดถูกกำหนดค่าแล้วทุกตัว

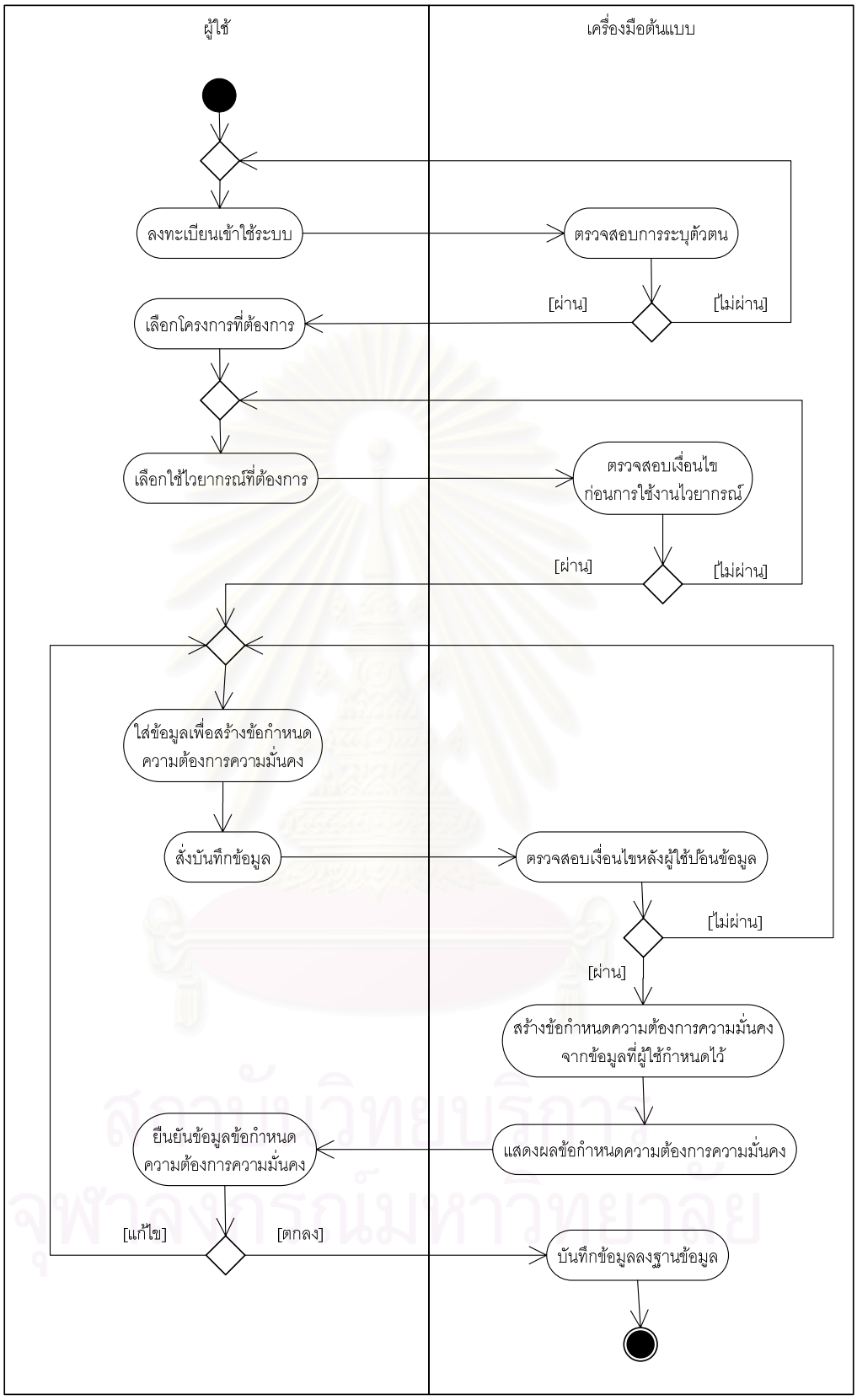


(ข) ข้อความเตือนเมื่อไม่มีรายการสินทรัพย์ปรากฏในฐานข้อมูล

รูปที่ 4.4 ข้อความเตือนจากเครื่องมือต้นแบบเมื่อพบว่าไม่ผ่านเงื่อนไขก่อนการใช้ไวยากรณ์

ส่วนต่อประสานผู้ใช้สำหรับทุกไวยากรณ์ที่มีการตรวจสอบเงื่อนไขก่อนการใช้ไวยากรณ์นั้น จะอนุญาตให้ใช้ได้เมื่อผ่านเงื่อนไขก่อนการใช้งานไวยากรณ์ดังกล่าวทุกข้อเท่านั้น โดยสามารถแสดงลำดับการทำงานปกติของไวยากรณ์เหล่านี้ได้ดังรูปที่ 4.5

รายละเอียดตัวอย่างการใช้งานไวยากรณ์ต่างๆ จากเครื่องมือต้นแบบแสดงไว้ในภาคผนวก ค



รูปที่ 4.5 แผนภาพกิจกรรมแสดงขั้นตอนการใช้งานไวยากรณ์ความมั่นคง

4.3 สภาพแวดล้อมในการพัฒนาเครื่องมือ

สภาพแวดล้อมในการพัฒนาเครื่องมือต้นแบบ จำแนกได้เป็น 2 ประเภท คือ ฮาร์ดแวร์ (Hardware) และซอฟต์แวร์ (Software) โดยมีรายละเอียดดังนี้

4.3.1 สภาพแวดล้อมในการพัฒนาเครื่องมือด้านฮาร์ดแวร์

เครื่องคอมพิวเตอร์พกพา (Notebook) 1 เครื่อง

- หน่วยประมวลผล Intel Core Duo Processor T2300 ความเร็ว 1.66 GHz
- หน่วยความจำหลัก DDR2 ขนาด 1024 เมกกะไบต์ (MB)
- ฮาร์ดดิสก์ความเร็ว 4,200 รอบ/วินาที ขนาด 80 กิกะไบต์ (GB)

4.3.2 สภาพแวดล้อมในการพัฒนาเครื่องมือด้านซอฟต์แวร์

1) ระบบปฏิบัติการวินโดส์วิสตาอัลติเมท (Microsoft Windows Vista Ultimate)
2) ไมโครซอฟท์วิสชวลสตูดิโอ 2005 (Microsoft Visual Studio 2005) สำหรับพัฒนาเครื่องมือในส่วนที่เป็นส่วนต่อประสานผู้ใช้ (Interface)
3) ไมโครซอฟท์วิสชวลซีชาร์บดอทเน็ต 2005 (Microsoft Visual C#.NET 2005) เป็นภาษาสำหรับพัฒนาเครื่องมือต้นแบบส่วนที่เป็นโปรแกรมทั้งหมด
4) ไมโครซอฟท์ดอทเน็ตเฟรมเวิร์ก (Microsoft .NET Framework) รุ่น 2.0 ขึ้นไป เพื่อใช้สำหรับการทำงานของวิสชวลสตูดิโอ และ การทำงาน (Run) ของเครื่องมือต้นแบบ
5) ไมโครซอฟท์แอกเซส 2003 (Microsoft Access 2003) สำหรับโปรแกรมและจัดการข้อมูลในฐานข้อมูล

บทที่ 5
การทดสอบเครื่องมือต้นแบบสำหรับการกำหนดความมั่นคง บนพื้นฐานของไวยากรณ์ที่สร้างจากแบบรูปความมั่นคง

เนื่องจากในการวิจัยนี้ ผู้วิจัยต้องการทราบว่าไวยากรณ์ความมั่นคงที่ได้สร้างขึ้นมานั้นมีประสิทธิภาพและประโยชน์ต่อผู้ใช้เป็นอย่างไร จึงได้พัฒนาเครื่องมือต้นแบบ ที่สามารถกำหนดความต้องการความมั่นคงบนพื้นฐานของไวยากรณ์ที่ได้สร้างขึ้น และให้ผู้ร่วมทดลองได้ทดลองใช้ ในงานวิจัยนี้ได้ทดสอบโดยการทดลองใช้เครื่องมือต้นแบบกำหนดความต้องการความมั่นคงจากสถานการณ์จำลอง (Scenario) ที่กำหนดให้ ซึ่งครอบคลุมไวยากรณ์ทั้งหมดในขอบเขตงานวิจัยนี้ และผู้วิจัยได้วิเคราะห์ผลการทดสอบ เพื่อสรุปผลการทดสอบ เพื่อใช้เป็นแนวทางในการปรับปรุงไวยากรณ์ความมั่นคงต่อไป

5.1 ภาพรวมของการทดสอบ

การกำหนดความต้องการมั่นคงนั้นทำได้ยาก หากมีเครื่องมือที่ช่วยในการกำหนดความต้องการดังกล่าวก็จะสามารถลดภาระ ค่าใช้จ่าย และเวลาได้ แต่จะทราบได้อย่างไรว่าไวยากรณ์ความมั่นคงที่ถูกสร้างขึ้นนั้นมีประสิทธิภาพและมีประโยชน์ต่อองค์กรในภาพรวมระดับใด

การทดสอบนี้มีวัตถุประสงค์เพื่อวัดระดับความพึงพอใจของหน่วยทดลองใช้เครื่องมือต้นแบบในการกำหนดความต้องการความมั่นคงจากไวยากรณ์ความมั่นคงที่ถูกสร้างขึ้นจากแบบรูปความมั่นคง ใน 4 กลุ่มปัจจัย ได้แก่ คุณภาพของความต้องการความมั่นคงที่ได้จากเครื่องมือ ประโยชน์ของเครื่องมือต่อผู้ใช้ คุณสมบัติของเครื่องมือ และการนำเครื่องมือไปประยุกต์ใช้ในองค์กร

รูปแบบและวิธีการทดสอบของงานวิจัยนี้ จะใช้ผู้ร่วมทดลอง 12 คนที่มีประสบการณ์และมีความชำนาญด้านความต้องการความมั่นคงเป็นหน่วยทดลอง มาทดลองใช้เครื่องมือในการกำหนดความต้องการความมั่นคง แล้วให้หน่วยทดลองประเมินระดับความพึงพอใจในประเด็นต่างๆ ที่กล่าวมาข้างต้น รวมถึงให้หน่วยทดลองแสดงความคิดเห็นต่อไวยากรณ์ความมั่นคง และเพื่อใช้ในการปรับปรุงไวยากรณ์ความมั่นคงต่อไปในอนาคต

ผลลัพธ์ที่ได้จากการทดลองจะเป็นระดับความพึงพอใจในแต่ละประเด็น ที่ได้กำหนดไว้ข้างต้น และข้อคิดเห็นหรือข้อเสนอแนะที่มีต่อเครื่องมือ แล้วนำมาวิเคราะห์เพื่อหาข้อสรุปเพื่อปรับปรุงไวยากรณ์ความมั่นคงหรือเครื่องมือได้

5.2 วัตถุประสงค์การทดสอบ

เพื่อให้ผู้วิจัยสามารถทราบถึงประโยชน์และประสิทธิภาพของไวยากรณ์ว่าเป็นไปตามที่ตั้งไว้หรือไม่ ระดับความพึงพอใจของหน่วยทดลองนั้นเป็นอย่างไร อยู่ในระดับใดบ้าง พร้อมทั้งข้อคิดเห็นและข้อเสนอแนะจากหน่วยทดลอง เพื่อใช้ในปรับปรุงไวยากรณ์ความมั่นคงต่อไป

วัตถุประสงค์การทดสอบคือ เพื่อวิเคราะห์ไวยากรณ์ความมั่นคง ว่ามีคุณลักษณะที่ดีหรือไม่ในด้านต่างๆ จากมุมมองของผู้ร่วมทดลองที่มีประสบการณ์ด้านความต้องการความมั่นคงมาก่อน โดยมีรายละเอียดดังนี้

1) วิเคราะห์ระดับความพึงพอใจของผู้ใช้ในกลุ่มปัจจัยต่างๆ ได้แก่ คุณภาพของความต้องการความมั่นคงที่ได้จากเครื่องมือ ประโยชน์ของเครื่องมือต่อผู้ใช้ คุณสมบัติของเครื่องมือ และการนำเครื่องมือไปประยุกต์ใช้ในองค์กร
2) รวบรวมและวิเคราะห์ความคิดเห็นและข้อเสนอแนะจากหน่วยทดลอง เพื่อนำมาสรุปและพิจารณาในการปรับปรุงไวยากรณ์หรือเครื่องมือต้นแบบ

5.3 ขั้นตอนการทดสอบ

จากภาพรวมการทดลองที่กล่าวมาข้างต้นสามารถแสดงขั้นตอนการทดลองเป็น 3 ขั้นตอน ดังแสดงด้วยแผนภาพกิจกรรมได้ดังรูปที่ 5.1 ซึ่งประกอบด้วย ขั้นตอนการเตรียมการทดลอง ขั้นตอนการดำเนินการทดลอง และ ขั้นตอนวิเคราะห์และสรุปผลการทดลอง

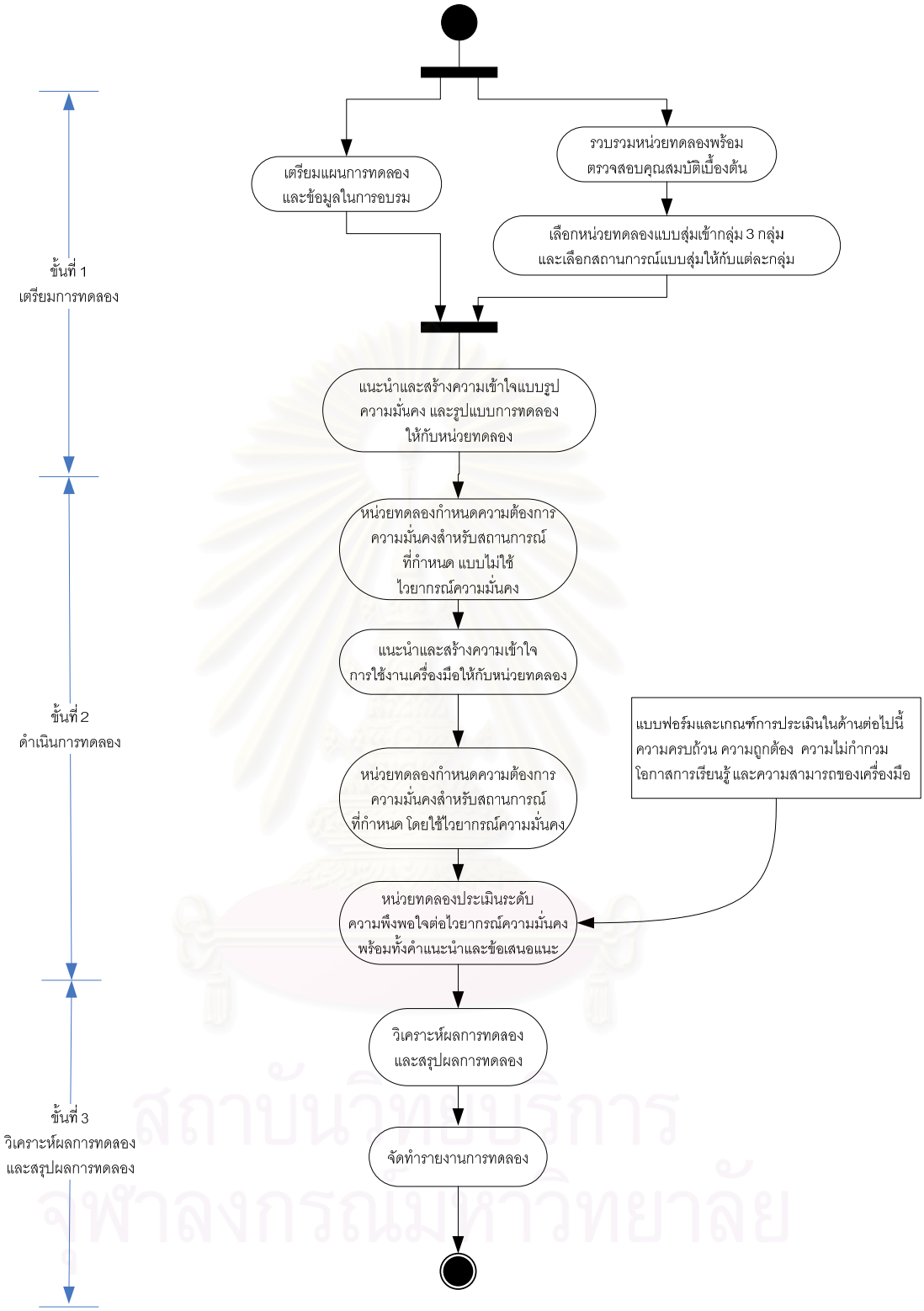
5.4 การวางแผนการทดลอง (Experimental Planning)

5.4.1 หน่วยทดลอง (Experimental Unit)

หน่วยทดลองในการทดลองนี้ มีจำนวน 12 คน ซึ่งมีคุณสมบัติดังต่อไปนี้

1) เป็นนิสิตระดับบัณฑิตศึกษาขึ้นไป ที่มีประสบการณ์หรือความชำนาญระบบที่เกี่ยวข้องกับความมั่นคง หรือ ผ่านการเรียนวิชาความมั่นคงสำหรับระบบคอมพิวเตอร์ (Computer System Security) และ/หรือ วิชาวิศวกรรมความต้องการซอฟต์แวร์ (Software Requirements Engineering) ของภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย หรือสาขาวิชาที่เกี่ยวข้อง และมีระดับผลการเรียนในรายวิชาดังกล่าวไม่ต่ำกว่า B หรือ

2) เป็นบุคลากรที่มีความเชี่ยวชาญและมีประสบการณ์ในระบบด้านความมั่นคง ที่กำลังปฏิบัติงานและมีความเชี่ยวชาญในกรอบงานของความมั่นคงที่เหมาะสม



รูปที่ 5.1 แผนภาพกิจกรรมแสดงขั้นตอนการทดลองเพื่อ
การทดสอบเครื่องมือและใช้ไวยากรณ์ความมั่นคง

5.4.2 **สิ่งทดลอง** (Treatment)

สิ่งทดลองในการทดลองนี้ คือ สถานการณ์จำลองซึ่งเป็นระบบที่ถูกกำหนดขึ้นโดยผู้วิจัย ซึ่งครอบคลุมเกี่ยวข้องกับความมั่นคง เพื่อให้หน่วยทดลองทำการกำหนดความต้องการความมั่นคงให้กับระบบดังกล่าว ในการทดลองจะกำหนด 3 สถานการณ์ ซึ่งในแต่ละสถานการณ์จำลองนั้นจะไม่มีความขึ้นต่อกันและแต่ละสถานการณ์จะถูกกำหนดให้ครอบคลุมไวยากรณ์ความมั่นคงทั้ง 3 กลุ่มที่ได้นำเสนอไว้ในขอบเขตงานวิจัย ได้แก่ การจัดการสินทรัพย์องค์กรและความเสี่ยง การระบุตัวตนและการยืนยันตน การตรวจสอบการเข้าถึง และสถาปัตยกรรมไฟล์วอลล์ โดยสถานการณ์จำลองในการทดลองนี้มีดังนี้ (รายละเอียดของแต่ละสถานการณ์จำลองแสดงดังภาคผนวก ง)

1) ระบบการให้บริการเอฟทีพี (FTP)

เป็นระบบที่เปิดบริการอัปโหลดและดาวน์โหลดข้อมูลจากพื้นที่เซิร์ฟเวอร์ผู้ให้บริการ มีทั้งประเภทพื้นที่สาธารณะและพื้นที่ส่วนบุคคล ซึ่งมีความจำเป็นที่จะต้องกำหนดความต้องการความมั่นคงสำหรับแฟ้มข้อมูลในระบบ การระบุและพิสูจน์ตัวจริง การกำหนดสิทธิ์ให้กับผู้ใช้งานตามบัญชีผู้ใช้ และเงื่อนไขบังคับในการติดต่อระบบบริการเอฟทีพีผ่านทางเครือข่าย

2) ระบบห้องปฏิบัติการ (Laboratory Management)

เป็นการสร้างห้องปฏิบัติการที่ต้องพิจารณาด้านความมั่นคง โดยสมมติให้หน่วยทดลองสามารถออกแบบระบบห้องปฏิบัติการที่ตนสังกัด โดยพิจารณาความมั่นคงร่วมด้วยแล้วกำหนดเป็นความต้องการหรือนโยบายความมั่นคงของห้องปฏิบัติการ ซึ่งต้องมีการระบุว่าใครเป็นสมาชิก และมีสิทธิ์ในการดำเนินการใดได้บ้าง หรือใช้ทรัพยากรใดบ้างที่ต้องจำกัดการใช้งานรวมถึงการติดต่อสู่ภายนอกห้องปฏิบัติการผ่านทางเครือข่าย

3) ระบบธนาคารออนไลน์ (Online Banking System)

เป็นระบบการจัดการธุรกรรมการเงินของผู้ใช้ผ่านทางระบบอินเทอร์เน็ต โดยกำหนดให้หน่วยทดลองเป็นผู้วิเคราะห์และกำหนดความต้องการความมั่นคงที่จำเป็นต้องมีในระบบนี้ มีความจำเป็นในการส่งผ่านข้อมูลที่ต้องการความปลอดภัย ผ่านการระบุและยืนยันตัวตนก่อนการดำเนินงาน สิทธิ์ของลูกค้าหรือพนักงานที่ต้องกำหนดให้ชัดเจนว่าสามารถดำเนินการใดได้บ้าง

5.4.3 **การให้ความรู้แก่หน่วยทดลอง**

เนื่องจากความเป็นไปได้ที่ผู้ใช้อาจไม่คุ้นเคยกับแบบรูปความมั่นคง และข้อมูลที่เกี่ยวข้อง ผู้วิจัยจึงได้ทำการให้ความรู้แก่หน่วยทดลองก่อนการทดลองจริง เพื่อเป็นการปรับพื้น

ฐานความรู้ด้านความมั่นคง แบบรูปความมั่นคง ไวยากรณ์ความมั่นคง และเครื่องมือต้นแบบ โดยโดยดำเนินการตามลำดับดังต่อไปนี้

1) แนะนำแบบรูปความมั่นคงในภาพรวม และอธิบายแบบรูปที่อยู่ในขอบเขตงานวิจัย และเป้าหมายของการทดลอง

2) แนะนำแบบรูปแต่ละแบบรูป โดยอธิบายความหมาย วัตถุประสงค์ ขอบเขต ข้อมูลสำคัญ พร้อมตัวอย่างประกอบ

3) แนะนำความสัมพันธ์ระหว่างแบบรูป เงื่อนไขก่อนการใช้แบบรูป ข้อจำกัดของแบบรูปบางตัว

4) แนะนำเครื่องมือ การใช้งาน และข้อจำกัดของเครื่องมือที่พัฒนาขึ้นจากไวยากรณ์ความมั่นคง รวมถึงเงื่อนไขบางประการที่ต้องพิจารณาก่อนการใช้เครื่องมือ (ขั้นตอนนี้จะดำเนินการได้ก็ต่อเมื่อ หน่วยทดลองทำการทดลองกำหนดความต้องการให้กับสถานการณ์จำลองโดยไม่ใช้ไวยากรณ์เรียบร้อยแล้ว)

5) แนะนำรูปแบบและความหมายของการประเมินผลการทดลองตามปัจจัยที่กำหนด

5.4.4 ปัจจัยที่ใช้ในการประเมินเครื่องมือ

ในการทดลองนี้ จะพิจารณาจากกลุ่มปัจจัยต่อไปนี้ ได้แก่ คุณภาพของความต้องการความมั่นคงที่ได้จากเครื่องมือ ประโยชน์ของเครื่องมือต่อผู้ใช้ คุณสมบัติของเครื่องมือ และการนำเครื่องมือไปประยุกต์ใช้ในองค์กร โดยจำแนกปัจจัยในแต่ละกลุ่มดังนี้

1) กลุ่มปัจจัยด้านคุณภาพของความต้องการความมั่นคง
   (1) ความครบถ้วน
   (2) ความถูกต้อง
   (3) ความไม่กำกวม
2) กลุ่มปัจจัยด้านประโยชน์ของเครื่องมือต่อผู้ใช้
   (1) เพิ่มการเรียนรู้
   (2) ลดระยะเวลา
   (3) ง่ายขึ้น ลดภาระ
   (4) เป็นทางเลือกที่ดีกว่ากำหนดความต้องการด้วยตนเอง
3) กลุ่มปัจจัยด้านคุณสมบัติของเครื่องมือ
   (1) สนับสนุนการนำกลับมาใช้ใหม่
   (2) ช่วยลำดับการใช้งาน

(3) ลดความยุ่งยาก

4) กลุ่มปัจจัยด้านการนำเครื่องมือไปประยุกต์ใช้ในองค์กร

(1) ความเหมาะสมในการนำไปใช้งานในองค์กร

(2) ช่วยสร้างองค์ความรู้ความมั่นคงให้กับองค์กร

ในการประเมินจะวิเคราะห์จากระดับความคิดเห็นว่าเห็นด้วยกับปัจจัยต่างๆ (เอกสารการประเมินหน่วยทดลองเครื่องมือแสดงดัง ภาคผนวก ง) ในระดับใด โดยในที่นี้กำหนดให้มีระดับดังต่อไปนี้

5 หมายถึง หน่วยทดลองเห็นด้วยมากที่สุด

4 หมายถึง หน่วยทดลองเห็นด้วยมาก

3 หมายถึง หน่วยทดลองเห็นด้วยปานกลาง

2 หมายถึง หน่วยทดลองเห็นด้วยน้อย

1 หมายถึง หน่วยทดลองเห็นด้วยน้อยมาก

5.4.5 แผนกิจกรรมการทดลอง

เพื่อให้การทดลองเป็นไปตามขั้นตอนและกำหนดเวลาที่เหมาะสม จึงมีการสร้างแผนกิจกรรมการทดสอบเครื่องมือต้นแบบเพื่อใช้เป็นข้อกำหนดในการดำเนินกิจกรรมการทดสอบเครื่องมือต้นแบบ

ตารางที่ 5.1 กำหนดการสำหรับการทดสอบเครื่องมือในงานวิจัย

ลำดับที่	วันที่	วัตถุประสงค์	ผลที่คาดว่าจะได้รับ
1.	6-8 สิงหาคม 2550	เตรียมแผนการทดลอง ข้อมูลและการนำเสนอ	ข้อมูลการนำเสนองานวิจัย และสถานการณ์จำลอง 3 แบบ
2.	10 สิงหาคม 2550	แนะนำแบบรูปความมั่นคง แนวคิด และการนำไปใช้	หน่วยทดลองเข้าใจที่มาและประโยชน์ของแบบรูปความมั่นคงและสามารถรู้จักนำไปใช้
3.	10-14 สิงหาคม 2550	แนะนำการใช้งาน และทดลองใช้เครื่องมือต้นแบบจากสถานการณ์จำลองตัวอย่าง	หน่วยทดลองเข้าใจรูปแบบการใช้งานและเงื่อนไขการใช้งานไวยากรณ์
4.	16 สิงหาคม 2550	หน่วยทดลองกำหนดความต้องการความมั่นคงสำหรับสถานการณ์จำลองที่กำหนด	ความต้องการความมั่นคงสำหรับสถานการณ์จำลองแต่ละแบบ

ตารางที่ 5.2 กำหนดการสำหรับการทดสอบเครื่องมือในงานวิจัย (ต่อ)

ลำดับที่	วันที่	วัตถุประสงค์	ผลที่คาดว่าจะได้รับ
5.	17 สิงหาคม 2550	หน่วยทดลองกำหนดความต้องการความมั่นคงสำหรับสถานการณ์จำลองที่กำหนดโดยใช้เครื่องมือต้นแบบ	ความต้องการความมั่นคงสำหรับสถานการณ์จำลองแต่ละแบบจากเครื่องมือต้นแบบ
6.	17 สิงหาคม 2550	หน่วยทดลองประเมินความพึงพอใจ และให้ข้อคิดเห็นหรือข้อเสนอแนะ	ระดับความพอใจของหน่วยทดลองและข้อคิดเห็นหรือข้อเสนอแนะจากหน่วยตัวอย่าง
7.	18-20 สิงหาคม 2550	วิเคราะห์ สรุปผล และทำรายงานผลการทดลอง	ผลการทดลองและรายงานสรุปผล

5.5 การดำเนินการทดลอง

รูปแบบการทดลองในงานวิจัยนี้ ให้หน่วยทดลองกำหนดความต้องการความมั่นคงทั้งแบบใช้เครื่องมือและไม่ใช้เครื่องมือ และให้หน่วยทดลองประเมินระดับความพึงพอใจสำหรับไวยากรณ์ความมั่นคง ซึ่งการทดลองโดยใช้เครื่องมือที่สร้างจากไวยากรณ์ความมั่นคงมาใช้ในการกำหนดความต้องการความมั่นคงโดยหน่วยทดลอง ซึ่งขั้นตอนดังกล่าวแสดงไว้แล้วดังรูปที่ 5.1 มีรายละเอียดดังต่อไปนี้

1) เนื่องจากหน่วยทดลองอาจมีลักษณะบางอย่างแตกต่างกันออกไป ไม่ว่าจะเป็นความรู้พื้นฐานด้านความมั่นคง และความสามารถด้านการกำหนดความต้องการซอฟต์แวร์ ดังนั้นจึงจัดกลุ่มหน่วยทดลองทั้งหมดเป็น 3 กลุ่ม กลุ่มละ 4 คน โดยจัดให้หน่วยทดลองคละกันไปในแต่ละกลุ่มตามความสามารถของหน่วยทดลอง โดยพิจารณาจากผลการเรียนวิชาความมั่นคงสำหรับระบบคอมพิวเตอร์และ/หรือวิชาวิศวกรรมความต้องการ และประสบการณ์ความมั่นคงที่ผ่านมา เพื่อให้แต่ละกลุ่มของหน่วยทดลองมีความสามารถใกล้เคียงกันมากที่สุด และเป็นการควบคุมการทดลองให้แต่ละกลุ่มมีความสามารถใกล้เคียงกันมากที่สุด

2) หลังจากที่แนะนำและทำความเข้าใจกับแบบรูปแล้ว ผู้วิจัยจะแนะนำความหมายของคำสำคัญต่างๆ ที่ปรากฏในงานวิจัยและในแบบรูป และเปิดโอกาสให้ซักถามข้อสงสัยที่เกี่ยวข้องกับงานวิจัย แบบรูป และความมั่นคง

3) แนะนำสถานการณ์จำลองทั้ง 3 แบบ แล้วเลือกสถานการณ์ให้กับกลุ่มผู้ทดสอบแบบสุ่ม โดยหน่วยทดลองจะไม่ทราบล่วงหน้าว่าจะได้สถานการณ์จำลองใด

4) หน่วยทดลองกำหนดความต้องการความมั่นคงสำหรับสถานการณ์ดังกล่าวด้วยตนเอง โดยจะมีรายการตรวจสอบ (Checklist) ให้เพื่อช่วยให้เกิดแนวความคิดในการสร้างความต้องการความมั่นคง โดยรายละเอียดรายการการตรวจสอบแสดงในภาคผนวก จ

5) หลังจากหน่วยทดลองทุกคนเขียนข้อกำหนดความต้องการด้วยตนเองเรียบร้อยแล้ว จะแนะนำการใช้เครื่องมือ และข้อจำกัดบางประการให้ผู้ใช้ทราบ เพื่อความเข้าใจในการใช้งาน ก่อนการใช้ในการทดลองจริง

6) หน่วยทดลองกำหนดความต้องการความมั่นคงสำหรับสถานการณ์ดังกล่าวด้วยตนเองอีกครั้ง โดยใช้เครื่องมือต้นแบบที่พัฒนาบนพื้นฐานไวยากรณ์ความมั่นคง

7) หน่วยทดลองประเมินระดับความพึงพอใจในด้านต่างๆ ตามเกณฑ์ที่ได้กำหนดไว้ พร้อมทั้งให้คำแนะนำหรือข้อเสนอแนะต่อเครื่องมือหรือไวยากรณ์ โดยใช้แบบสอบถามในภาคผนวก ฉ

5.6 **ผลการทดลอง** (Experiment Results)

ผลการทดลองในการทดสอบเครื่องมือในงานวิจัยนี้จะเป็นการวัดระดับความเห็นของหน่วยทดลองมีต่องานวิจัยนี้ในปัจจัยด้านต่างๆ เช่น ความคิดเห็นต่อผลลัพธ์ความต้องการความมั่นคงที่ได้จากเครื่องมือ ความคิดเห็นต่อความรู้ที่ได้จากการใช้เครื่องมือ ความคิดเห็นต่อความสามารถของเครื่องมือ และการความเห็นในการนำเครื่องมือที่พัฒนาขึ้นนี้ไปประยุกต์ใช้ในองค์กร โดยผลสรุปความคิดเห็นของหน่วยทดลองจำนวน 12 คนโดยแสดงความถี่ของความคิดเห็นข้องผู้ใช้จำแนกตามระดับความคิดเห็นในปัจจัยที่พิจารณาต่างๆ ดังแสดงดังตารางที่ 5.3

ตารางที่ 5.3 การแจกแจงความคิดเห็นของหน่วยทดลองจำแนกตามระดับความคิดเห็น
จากหน่วยทดลอง 12 คน

ปัจจัยที่ใช้ในการพิจารณา	ระดับความคิดเห็น				
	5	4	3	2	1
1. ความคิดเห็นต่อคุณภาพผลลัพธ์ความต้องการความมั่นคงที่ได้จากเครื่องมือ					
1.1 เครื่องมือช่วยในการกำหนดความต้องการความมั่นคงได้ครบถ้วนมากกว่าการกำหนดความต้องการดังกล่าวด้วยตนเอง	7	5	-	-	-
1.2 เครื่องมือช่วยในการกำหนดความต้องการความมั่นคงได้ถูกต้องมากกว่าการกำหนดความต้องการดังกล่าวด้วยตนเอง	3	6	3	-	-
1.3 เครื่องมือช่วยในการกำหนดความต้องการความมั่นคงได้ไม่กำกวมมากกว่าการกำหนดความต้องการดังกล่าวด้วยตนเอง	1	7	4	-	-

ตารางที่ 5.2 การแจกแจงความคิดเห็นของหน่วยทดลองจำแนกตามระดับความคิดเห็น

จากหน่วยทดลอง 12 คน (ต่อ)

ปัจจัยที่ใช้ในการพิจารณา	ระดับความคิดเห็น				
	5	4	3	2	1
2.1 เครื่องมือช่วยส่งเสริมให้ท่านเกิดการเรียนรู้ด้วยตนเองเกี่ยวกับการกำหนดความต้องการความมั่นคง ทำให้เกิดความสนใจและมีความเข้าใจมากขึ้น	3	4	4	1	-
2.2 เครื่องมือช่วยให้ท่านใช้เวลาในการกำหนดความต้องการความมั่นคงน้อยกว่าเวลาที่ท่านใช้ขณะที่ไม่มีเครื่องมือ	2	5	-	4	1
2.3 เครื่องมือสามารถลดความพยายามของท่านในการกำหนดความต้องการความมั่นคงมากกว่าตอนที่ท่านกำหนดความต้องการดังกล่าวโดยไม่ใช้เครื่องมือ	3	3	4	2	-
2.4 ท่านสามารถกำหนดความต้องการความมั่นคงโดยใช้เครื่องมือได้ดีกว่าไม่ใช้เครื่องมือ	1	5	4	2	-
3. ความคิดเห็นต่อคุณสมบัติเครื่องมือ					
3.1 เครื่องมือสนับสนุนการนำกลับมาใช้ใหม่ของความต้องการความมั่นคงได้	4	5	3	-	-
3.2 เครื่องมือมีความสามารถในการตรวจสอบลำดับของการกำหนดความต้องการความมั่นคง เพื่อลดความไม่สอดคล้องกันระหว่างความต้องการ	3	4	4	1	-
3.3 เครื่องมือช่วยลดความยุ่งยากในการกำหนดความต้องการความมั่นคง	-	6	5	1	-
4. ความคิดเห็นที่มีต่อการนำเครื่องมือไปประยุกต์ใช้ในองค์กรด้านความมั่นคง					
4.1 องค์กรควรนำเครื่องมือไปประยุกต์ใช้เพื่อกำหนดความต้องการความมั่นคงและนโยบายความมั่นคงสำหรับองค์กรได้	4	7	1	-	-
4.2 องค์กรสามารถนำความต้องการความมั่นคงจากเครื่องมือมาจัดเก็บเป็นข้อมูลเพื่อสร้างเป็นองค์ความรู้สำหรับองค์กรได้	4	7	1	-	-

5.7 วิเคราะห์ผลการทดลอง

จากข้อคำถามเกี่ยวกับระดับความความคิดเห็นที่มีต่อการกำหนดความต้องการความมั่นคงตั้งแต่ข้อที่ 1.1 จนถึงข้อ 4.2 โดยมีเกณฑ์การให้คะแนนระดับความเห็นที่กำหนดในข้อ 5.4.4 สามารถนำมาเขียนเป็นตารางคะแนนความคิดเห็นแบบรายปัจจัยได้ดังตารางที่ 5.4

จากตารางที่ 5.4 สามารถสรุปผลการทดลองได้ดังนี้

1) ความเห็นของหน่วยทดลองที่มีต่อคุณภาพของความต้องการความมั่นคงที่ได้จากเครื่องมือพบว่า หน่วยทดลองส่วนใหญ่มีความเห็นในระดับดีต่อคุณภาพของความต้องการในมุมมองความครบถ้วน ความถูกต้องและความไม่กำกวม ซึ่งมีระดับความพึงพอใจเฉลี่ยที่ 4.11

2) ความเห็นของหน่วยทดลองต่อประโยชน์ของเครื่องมือที่มีต่อหน่วยทดลองพบว่า เครื่องมือช่วยให้หน่วยทดลองเกิดการเรียนรู้ในการกำหนดความต้องการความมั่นคงมากขึ้น ทำให้ช่วยลดระยะเวลาและแรงงานในการกำหนดความต้องการความมั่นคงได้ในระดับค่อนข้างดี โดยดูจากระดับความพึงพอใจที่ 3.58

ตารางที่ 5.4 คะแนนความคิดเห็นต่อเครื่องมือที่ใช้ในการกำหนดความมั่นคงเป็นรายปัจจัย

กลุ่มปัจจัย	ปัจจัย / หน่วยทดลอง	1	2	3	4	5	6	7	8	9	10	11	12	SD.	ค่าเฉลี่ยปัจจัย	ค่าเฉลี่ยกลุ่มปัจจัย
คุณภาพความต้องการ	ความครบถ้วน	5	5	4	5	4	5	4	5	5	5	4	4	0.27	4.58	4.11
	ความถูกต้อง	3	4	4	5	4	3	4	4	5	5	4	3	0.55	4.00	
	ความไม่กำกวม	3	4	4	5	4	3	4	4	4	4	3	3	0.39	3.75	
ประโยชน์ของเครื่องมือ	เพิ่มการเรียนรู้	2	3	3	3	5	5	3	4	4	5	4	4	0.93	3.75	3.58
	ลดเวลา	1	4	2	2	5	4	2	5	4	4	2	4	1.84	3.25	
	ลดความพยายาม	3	4	2	3	5	5	3	2	4	5	4	3	1.17	3.58	
	ดีกว่ากำหนดด้วยตนเอง	4	4	4	4	4	3	3	5	3	3	4	4	0.39	3.75	
คุณสมบัติของเครื่องมือ	นำกลับมาใช้ใหม่	5	5	3	4	4	5	3	4	4	5	3	4	0.63	4.08	3.75
	จัดลำดับการใช้งาน	2	5	3	4	4	3	3	5	4	5	3	4	0.93	3.75	
	ลดความยุ่งยาก	4	3	3	4	4	3	4	2	4	3	3	4	0.45	3.42	
การประยุกต์ใช้เครื่องมือ	เหมาะจะนำไปใช้ในองค์กร	4	5	4	4	4	5	3	4	5	4	4	5	0.39	4.25	4.25
	ช่วยสร้างองค์ความรู้องค์กร	4	5	4	4	4	5	3	5	4	5	4	4	0.39	4.25	

หากพิจารณาในปัจจัยด้านเวลา และแรงงานหรือความพยายามในการกำหนดความต้องการความมั่นคงโดยเครื่องมือนั้น หน่วยทดลองให้ระดับความพึงพอใจค่อนข้างหลากหลาย ค่าส่วนเบี่ยงเบนมาตรฐาน (Standard Deviation: SD) อยู่ที่ 1.84 และ 1.17 ตามลำดับ เนื่องจากหน่วยทดลองจำนวนหนึ่งไม่เห็นด้วยว่าเครื่องมือนี้จะช่วยลดเวลาและความพยายามได้ จากการสอบถามเป็นการส่วนตัวพบว่า หน่วยทดลองดังกล่าวมีเข้าใจแนวคิดของความมั่นคงสำหรับระบบดังกล่าวคลาดเคลื่อนไป รวมถึงความไม่คุ้นเคยกับคำศัพท์ทางด้านความมั่นคงบางตัว ทำให้เกิดความไม่เข้าใจและกลัวจะตีความหมายของคำศัพท์ดังกล่าวผิดเพี้ยนไป อย่างไรก็ตามหากมองในเรื่องการเรียนรู้การใช้เครื่องมือพบว่า หน่วยทดลองส่วนใหญ่สามารถเรียนรู้การใช้เครื่องมือได้ในระยะเวลาไม่นาน แต่ปัญหาที่ปรากฏกลับเป็นการกำหนดความต้องการความมั่นคงที่เป็นภาษาอังกฤษ เนื่องจากหน่วยทดลองจะต้องใช้เวลาในการเรียบเรียงและป้อนข้อมูลเข้าสู่เครื่องมือ จึงเป็นอีกสาเหตุหนึ่งที่หน่วยทดลองเห็นว่า การใช้เครื่องมืออาจจะยังไม่ได้ช่วยลดเวลาและลดความพยายามในการกำหนดความต้องการความมั่นคงลงได้

3) ความเห็นของหน่วยทดลองต่อคุณสมบัติของเครื่องมือส่วนใหญ่มีแนวโน้มไปในทางที่ดีโดยดูจากระดับความความพึงพอใจที่ 3.75 ซึ่งหน่วยทดลองเห็นว่าเครื่องมือสามารถสนับสนุนการนำกลับมาใช้ใหม่ของความต้องการความมั่นคงได้ เอื้ออำนวยให้หน่วยทดลองสามารถกำหนดความต้องการได้อย่างเป็นลำดับและมีขั้นตอน จึงช่วยลดความยุ่งยากในการกำหนดความต้องการความมั่นคงได้ดีขึ้นในระดับหนึ่ง

4) ความเห็นของหน่วยทดลองต่อการนำเครื่องมือไปประยุกต์ใช้ในองค์กรความมั่นคงพบว่า ผู้ใช้เห็นด้วยที่จะนำเครื่องมือในการทดลองนี้ไปประยุกต์ใช้ในการกำหนดความต้องการความมั่นคงขององค์กร และสามารถนำความต้องการดังกล่าวไปสร้างเป็นองค์ความรู้สำหรับองค์กรได้

5.8 สรุปและอภิปรายผลการทดลอง

จากผลการทดลองในการทดสอบเครื่องมือต้นแบบที่สร้างบนพื้นฐานไวยากรณ์ความมั่นคงสามารถสรุปเป็น 4 กลุ่มปัจจัยได้ดังนี้

1) คุณภาพของความต้องการความมั่นคงเพิ่มขึ้นเมื่อใช้เครื่องมือในการสร้างความต้องการความมั่นคง

2) เครื่องมือช่วยให้ผู้ใช้เรียนรู้ว่า ถ้าจะกำหนดความต้องการความมั่นคงจะต้องมีองค์ประกอบใดบ้างที่ต้องพิจารณา ซึ่งจะช่วยลดระยะเวลาและไม่ต้องใช้ความพยายามมากในการกำหนดความต้องการความมั่นคง

3) เครื่องมือมีความสามารถในการตรวจสอบเงื่อนไขก่อนและหลังการใช้งาน และช่วยในการลำดับการกำหนดความต้องการความมั่นคง ส่งผลให้ความต้องการความมั่นคงดังกล่าวสามารถนำกลับมาใช้ใหม่ได้ ช่วยลดภาระการตรวจสอบความสอดคล้องของความต้องการความมั่นคงได้เป็นอย่างดี

4) เครื่องมือต้นแบบที่พัฒนาบนพื้นฐานของไวยากรณ์ความมั่นคงมีความเหมาะสมที่จะนำไปประยุกต์ใช้ในองค์กร เนื่องจากสามารถนำเครื่องมือต้นแบบนี้ในการกำหนดนโยบายความมั่นคงขององค์กร หรือสร้างเป็นองค์ความรู้ความมั่นคงสำหรับองค์กรได้

5.9 ปัญหาและแนวทางแก้ไข

ปัญหาบางประการที่ปรากฏในการทดลอง จะสอดคล้องกับข้อเสนอแนะของหน่วยทดลอง 12 คน สามารถจำแนกเป็นรายข้อได้ดังนี้

1) ปัญหาที่เกิดจากความสับสนในแนวคิดความมั่นคงและคำศัพท์ทางด้านความมั่นคง

หน่วยทดลองบางคนมีความสับสนต่อแนวคิดความมั่นคง ที่จะนำมาใช้ในสถานการณ์จำลอง เช่น “Role” และ “Right” ซึ่งจากการสอบถามแบบส่วนบุคคลหลังการทดลอง พบว่า หน่วยทดลองจำนวน 3 คนเกิดความสับสนในการทำความเข้าใจความหมายของคำศัพท์ด้านความมั่นคง จึงทำให้สับสนและได้ผลลัพธ์ความต้องการที่ผิดพลาดไป

แนวทางการแก้ไข ผู้วิจัยสามารถให้ความรู้ด้านความมั่นคงเพิ่มเติมแก่หน่วยทดลองให้มีความเข้าใจมากยิ่งขึ้น หรือแนะนำแหล่งข้อมูลความมั่นคงที่หน่วยทดลองสามารถศึกษาด้วยตนเอง ซึ่งจะช่วยหลีกเลี่ยงปัญหาความสับสนที่เกี่ยวข้องกับความมั่นคง

2) ปัญหาที่เกิดความสับสนในการใช้ไวยากรณ์

ในการทดลองผู้วิจัยได้แนะนำหน่วยทดลองให้ใช้รายการตรวจสอบมาช่วยในการกำหนดความต้องการความมั่นคง เพื่อช่วยให้เรียบเรียงความคิด และความสัมพันธ์ของความต้องการความมั่นคงต่างๆ ได้ ซึ่งจะเอื้ออำนวยให้เข้าใจไวยากรณ์และลำดับการใช้ไวยากรณ์ได้ด้วย แต่หน่วยทดลอง 2 คนไม่สามารถบรรลุวัตถุประสงค์ของรายการความต้องการความมั่นคงได้

แนวทางการแก้ไข ผู้วิจัยได้สร้างเอกสารตัวอย่างการใช้งานเครื่องมือต้นแบบ เพื่ออธิบายว่าแบบฟอร์มสำหรับไวยากรณ์ใดๆ นั้นจะต้องพิจารณาหรือใช้ไวยากรณ์ใดก่อนบ้าง เพื่อลดความสับสนในการใช้งานไวยากรณ์

3) ปัญหาที่เกิดจากความไม่เข้าใจสถานการณ์จำลอง

ในการทดลองมีหน่วยทดลอง 2 คนที่ได้รับสถานการณ์จำลองไปแล้วเกิดความไม่เข้าใจว่า สถานการณ์จำลองดังกล่าวเกี่ยวข้องกับความมั่นคงได้ยังไง และไม่สามารถระบุสินทรัพย์ใด ทำให้ยากต่อการกำหนดความต้องการความมั่นคงสำหรับระบบนั้นๆ

แนวทางการแก้ไข ผู้วิจัยได้แนะนำการใช้รายการการตรวจสอบ เพื่อแนะนำให้หน่วยทดลองค่อยๆ พิจารณาทีละส่วนตามรายการการตรวจสอบที่กำหนดให้ ซึ่งจะได้ข้อมูลสินทรัพย์และความต้องการความมั่นคงที่ต้องพิจารณาในระบบดังกล่าว เพื่อนำข้อมูลนั้นมาพิจารณาด้านความมั่นคงเพื่อกำหนดความต้องการความมั่นคง

บทที่ 6
การประยุกต์ใช้เครื่องมือที่สร้างบนพื้นฐานไวยากรณ์ความมั่นคง

เพื่อให้เห็นว่าแนวคิดในการสร้างไวยากรณ์ความมั่นคงจากแบบรูปความมั่นคงสามารถนำมาประยุกต์ใช้ในกระบวนการวิศวกรรมความต้องการที่เกี่ยวข้องกับการสร้างความต้องการความมั่นคงได้ในระบบที่หลากหลาย ในบทนี้จะใช้ระบบสนับสนุนห้องปฏิบัติการเป็นกรณีศึกษา (Case Study) เนื่องจากเป็นระบบที่ครอบคลุมความต้องการความมั่นคงภายใต้ขอบเขตแบบรูปความมั่นคงทั้ง 4 กลุ่ม

6.1 ระบบสนับสนุนห้องปฏิบัติการ

ระบบสนับสนุนห้องปฏิบัติการ เป็นระบบที่มุ่งเน้นการดูแลและควบคุมการใช้สินทรัพย์ต่างๆ ที่มีในห้องปฏิบัติการ โดยทรัพยากรที่ปรากฏเป็นได้ทั้ง(Information Asset) ได้แก่ แฟ้มข้อมูลวิทยานิพนธ์ (Thesis File) เป็นต้น และสิ่งของทางกายภาพ (Physical Asset) เช่น จอมอนิเตอร์ (Monitors) ฮาร์ดดิสก์ (Hard disk) เล่มวิทยานิพนธ์ เป็นต้น ซึ่งมีความจำเป็นต้องกำหนดคุณสมบัติความมั่นคง (Security Property) และนโยบายของห้องปฏิบัติการ (Laboratory Policy) อย่างไรก็ตามผู้ที่สามารถเข้าออกห้องปฏิบัติการได้ควรเป็นสมาชิกของห้องปฏิบัติการนั้นๆ จึงมีความจำเป็นต้องมีการตรวจสอบและระบุตัวตนก่อนการเข้าใช้ห้องปฏิบัติการ และจะต้องมีการกำหนดสิทธิ์ให้เฉพาะบุคคล หรือบทบาทที่บุคคลดังกล่าวจะได้รับ เพื่อควบคุมการเข้าถึงสินทรัพย์ที่ปรากฏในห้องปฏิบัติการ สำหรับระบบเครือข่ายที่ได้ทำการติดตั้งไว้ในห้องปฏิบัติการจะต้องมีการควบคุมการใช้งานเช่นกัน เช่น การกรองแพ็คเกจการเชื่อมต่อระหว่างภายในห้องปฏิบัติการกับภายนอก เป็นต้น

6.2 การประยุกต์ใช้ไวยากรณ์ความมั่นคง

เพื่อให้เข้าใจถึงขั้นตอนการได้ความต้องการความมั่นคงจากไวยากรณ์ความมั่นคงในรูปของเครื่องมือ จึงได้แสดงขึ้นตอนการใช้ไวยากรณ์ความมั่นคง และการแปลงข้อมูลนำเข้าจากผู้ใช้งานไปเป็นความต้องการความมั่นคงได้อย่างไร ซึ่งไวยากรณ์ความมั่นคงครอบคลุมกลุ่มของแบบรูปความมั่นคง 4 กลุ่ม ได้แก่ การจัดการความมั่นคงองค์กรและการจัดการความเสี่ยง การระบุตัวตนและการพิสูจน์ตัวตน การควบคุมการเข้าถึง และสถาปัตยกรรมไฟล์วอลล์ ซึ่งรายละเอียดของไวยากรณ์ความมั่นคงทั้งหมดในขอบเขตงานวิจัยได้แสดงไว้ในภาคผนวก ข รายการความต้องการความมั่นคงที่ได้จากเครื่องมือสำหรับระบบสนับสนุนห้องปฏิบัติการจากหน่วยทดลอง 1 คนแสดงดังตารางที่ 6.1

ตารางที่ 6.1 ตัวอย่างความต้องการความมั่นคงที่ได้จากการใช้เครื่องมือสำหรับระบบสนับสนุนห้องปฏิบัติการ

ข้อที่	ความต้องการความมั่นคง	ไวยากรณ์ที่ใช้
1	Computer (or server), network device, printer, CCTV camera and office facilitate requires confidentially, integrity, availability and accountability under the auspices of business process, costs and laws or regulation.	GM61
2	Personal data requires confidentially, integrity and availability under the auspices of business process.	
3	SE Lab member requires confidentially, integrity and availability under the auspices of critical business process and mission and goals.	
4	The asset valuation of network device is extreme in security requirements rating, medium in financial value rating and extreme in business impact rating. So, the overall impact value is high.	GM62
5	The asset valuation of computer (or server) is extreme in security requirements rating, high in financial value rating and extreme in business impact rating. So, the overall impact value is high.	
6	The asset valuation of CCTV camera is extreme in security requirements rating, high in financial value rating and high in business impact rating. So, the overall impact value is high.	
7	The asset valuation of printer is negligible in security requirements rating, medium in financial value rating and high in business impact rating. So, the overall impact value is low.	
8	The asset valuation of SE lab member is very high in security requirements rating, low in financial value rating and low in business impact rating. So, the overall impact value is low.	
9	The asset valuation of critical lab data is extreme in security requirements rating, high in financial value rating and very high in business impact rating. So, the overall impact value is very high.	
10	The asset valuation of personal data is very high in security requirements rating, low in financial value rating and low in business impact rating. So, the overall impact value is low.	
11	The asset valuation of thesis is very high in security requirements rating, low in financial value rating and low in business impact rating. So, the overall impact value is low.	
12	The likelihood of error for network device is medium. Its' consequence is communication problem.	GM63
13	The likelihood of hacked (in case of server) for computer (or server) is medium. Its' consequence is denial of service.	

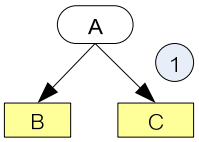
ตารางที่ 6.1 ตัวอย่างความต้องการความมั่นคงที่ได้จากการใช้เครื่องมือสำหรับระบบสนับสนุนห้องปฏิบัติการ (ต่อ)

ข้อที่	ความต้องการความมั่นคง	ไวยากรณ์ที่ใช้
14	The likelihood of lost for computer (or server) is low. Its' consequence is chaos in the lab, such as, contacting to a police, an owner of that computer cannot work at all.	GM63
15	The likelihood of lost for network device is low. Its' consequence is communication failure.	
16	The likelihood of lost for critical lab data is low. Its' consequence is the SE lab is most losing.	
17	The likelihood of lost or damaged for CCTV camera is low. Its' consequence is attacker monitoring failure.	
18	The likelihood of unauthorized access for critical lab data is medium. Its' consequence is the data is hacked.	
19	The likelihood of unauthorized modification for SE lab member is medium. Its' consequence is attacker can enter the SE room, and real SE member cannot enter the SE room.	
20	The likelihood of unauthorized modification for personal data is medium. Its' consequence is the owner of data is not satisfied, and cannot work on their work properly.	
21	The cause of unauthorized access is a not well protection policy which has extreme severity level.	GM64
22	The cause of lost is an attacker want to attack, or want to steal a device which has extreme severity level.	
23	The cause of lost or damaged is attacker want to reduce the security level of the SE lab which has very high severity level.	
24	The cause of unauthorized modification is be pretending of someone external or internal which has Very high severity level.	
25	The cause of Lost is Thief want to steal it which has Very high severity level.	
26	The cause of Lost is unexpectedly event which has Extreme severity level.	
27	The qualitative risk for cctv camera is low.	GM65
28	The qualitative risk for computer (or server) is low.	
29	The qualitative risk for critical lab data is extreme.	
30	The qualitative risk for network device is medium.	
31	The qualitative risk for personal data is low.	
32	Protect availability of computer (or server) require high level of detection, high level of prevention and high level of response with following services: accounting and access Control.	GM66,GM67

ตารางที่ 6.1 ตัวอย่างความต้องการความมั่นคงที่ได้จากการใช้เครื่องมือสำหรับระบบสนับสนุนห้องปฏิบัติการ (ต่อ)

ข้อที่	ความต้องการความมั่นคง	ไวยากรณ์ที่ใช้
33	Protect availability of network device require high level of detection, high level of prevention and high level of response with following services: security management.	GM66,GM67
34	Protect confidentiality of critical lab data require high level of detection and high level of prevention with following services: accounting, access control and security management.	
35	Protect confidentiality of SE lab member require high level of detection and high level of prevention with following services: accounting and access control.	
36	SE lab admin who acquire admin role can access critical lab data by using HTTP/HTTPS messages.	GM68
37	The service named, biometric authentication, should accurately recognize legitimate actors by using biometric.	GM71,GM72, GM73,GM74
38	SE member who acquire member role can modify personal data.	GM81,GM82, GM84
39	SE member who acquire admin role can modify SE lab member.	
40	SE member who acquire admin role can modify critical lab data.	
41	SE member who acquire member role can access thesis.	
42	SE Lab member has a medium clearance level.	GM83
43	SE Lab admin has a very high clearance level.	GM83
44	Member role can perform following tasks: download thesis file and read thesis file.	GM85
45	Admin role can perform following tasks: access thesis file, delete thesis information, download thesis file, modify thesis information and read thesis file.	
46	The request from 161.200.xxx.xxx is permitted to access the internet lab services.	GM121,GM122, GM123
47	The request from the external host is denied to access critical lab data through HTTP/HITTPS, FTP/FTPS port.	
48	The request from the P2P package is permitted to access office facilitate through P2P protocol port. the bandwidth can not more than 50KB/s	

จากตารางที่ 6.1 แสดงรายการความต้องการความมั่นคงที่ได้จากเครื่องมือที่สร้างบนพื้นฐานไวยากรณสำหรับระบบสนับสนุนห้องปฏิบัติการ ประกอบด้วย 48 ความต้องการครอบคลุมทั้ง 4 ไวยากรณ์ความมั่นคง โดยสามารถแสดงการประยุกต์ใช้ไวยากรณ์ความมั่นคงแต่ละไวยากรณ์ได้ดังต่อไปนี้ โดยกำหนดรูปแบบการใช้กฎแสดงดังรูปที่ 6.1



รูปที่ 6.1 ตัวอย่างการใช้กฎในไวยากรณ์ความมั่นคง

จากรูปที่ 6.1 แสดงตัวอย่างการใช้กฎในไวยากรณ์ แสดงให้เห็นว่า “A” เมื่อใช้กฎข้อที่ 1 จะแปลงเป็น “B” และ “C” โดยกำหนดให้

1) สัญลักษณ์ (ก) หมายถึง การใช้กฎลำดับที่ ก ในไวยากรณ์ เมื่อ ก คือ หมายเลขใดๆ

2) สัญลักษณ์ [ข้อความ] หมายถึง แสดงนอนเทอร์มินอลโหนด (Non-terminal Node) หรือโหนดที่สามรถแปลความหมายต่อได้อีก

3) สัญลักษณ์ [ข้อความ] หมายถึง แสดงเทอร์มินอลโหนด (Terminal Node) หรือโหนดที่ไม่สามรถแปลความหมายต่อได้อีก

การแสดงการประยุกต์ใช้ไวยากรณ์ในที่นี้ จะใช้ผลลัพธ์ความต้องการที่ได้จากการใช้เครื่องมือโดยหน่วยทดลอง 1 คน เพื่อแสดงให้เห็นว่าผลลัพธ์ความต้องการความมั่นคงนั้นได้มาอย่างไร ซึ่งการแสดงการประยุกต์ใช้ไวยากรณ์ต่อไปนี้ จะแสดงตามผลลัพธ์ของผู้ใช้เท่านั้น ซึ่งอาจไม่ครอบคลุมทุกกฎของทุกไวยากรณ์ที่นำเสนอภาคผนวก ข

6.2.1 กลุ่มไวยากรณ์ด้านการจัดการความมั่นคงองค์กรและการจัดการความเสี่ยง

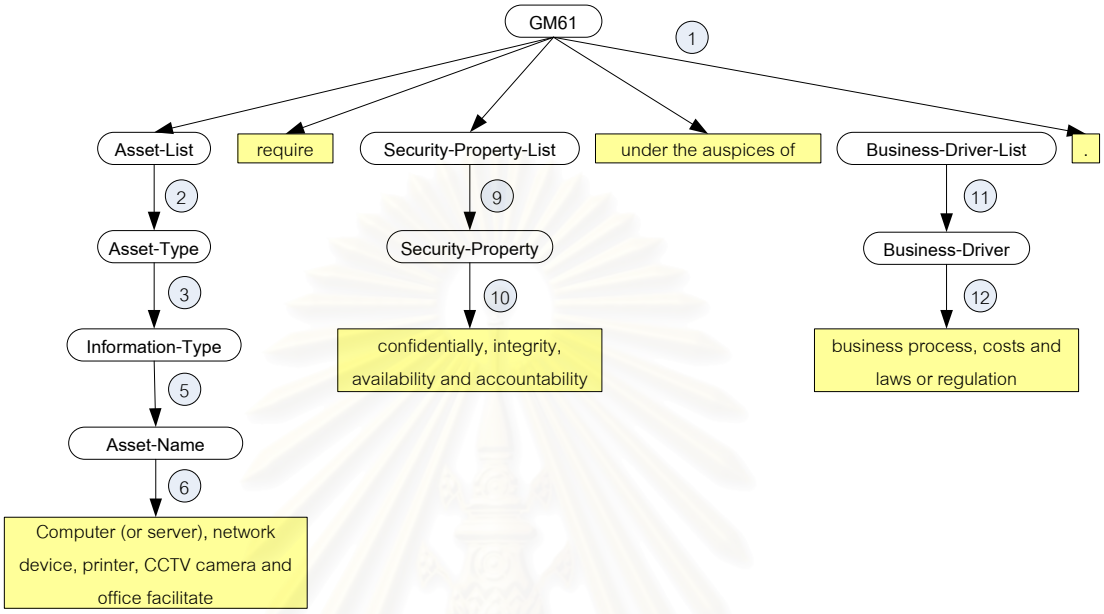
ความต้องการความมั่นคงจากไวยากรณ์กลุ่มนี้จะมุ่งเน้นการระบุความจำเป็นด้านความมั่นคงพื้นฐานให้กับสินทรัพย์ ภัยคุกคาม ความถี่ของการเกิดภัยคุกคาม และระดับความรุนแรงเมื่อสินทรัพย์ถูกโจมตี เพื่อใช้ข้อมูลดังกล่าวข้างต้นมาใช้ในการประเมินความเสี่ยง และสามารถนำข้อมูลความเสี่ยงมาใช้ในการกำหนดแนวคิดและบริการความมั่นคง โดยประกอบด้วย 8 ไวยากรณ์ดังต่อไปนี้

1) ไวยากรณ์การระบุความต้องการความมั่นคงสำหรับสินทรัพย์องค์กร

จากข้อมูลความต้องการในตารางที่ 6.3 ความต้องการข้อที่ 1-3 เป็นความต้องการที่ได้จากไวยากรณ์นี้ ซึ่งสามารถแสดงขั้นตอนการสร้างความต้องการความมั่นคงจากไวยากรณ์นี้ได้ดังรูปที่ 6.2

จากรูปที่ 6.2 แสดงให้เห็นขั้นตอนการประยุกต์ใช้ไวยากรณ์ โดยหมายเลขที่กำกับอยู่บนเส้นแสดงกฎที่ต้องใช้ในการแปลง ซึ่งผลลัพธ์ความต้องการที่ได้จากไวยากรณ์นี้เกิดจากการนำเทอร์มินอลโหนดมาเรียงต่อกันตามลำดับ จะได้ความต้องการข้อที่ 1 ดังแสดงในตารางที่ 6.1

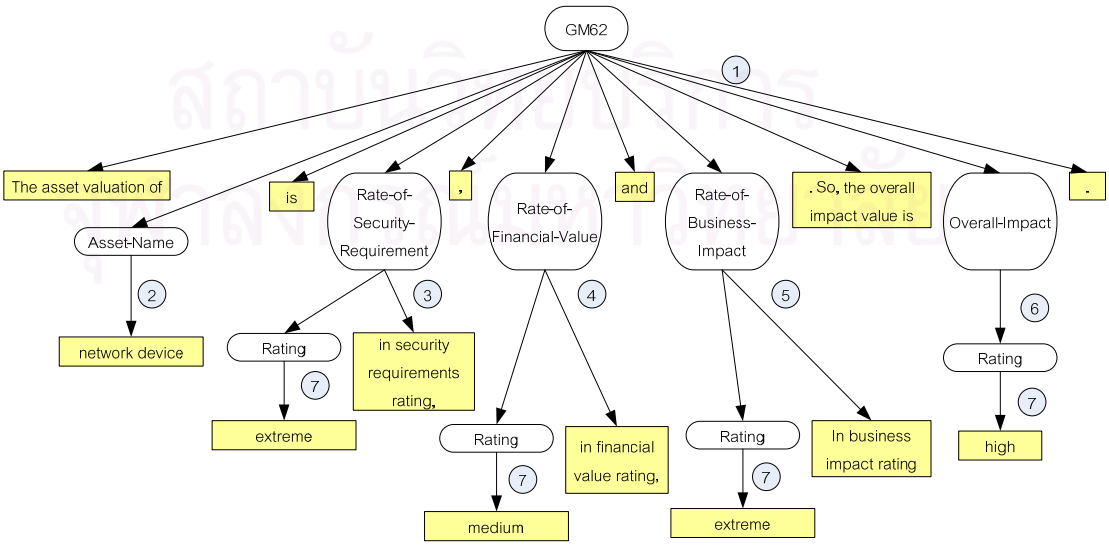
คือ *"Computer (or server), network device, printer, CCTV camera and office facilitate require confidentiality, integrity, availability and accountability under the auspices of business process, costs and laws or regulation."*



รูปที่ 6.2 การประยุกต์ใช้ไวยากรณ์การระบุความต้องการความมั่นคงสำหรับสินทรัพย์องค์กร

2) **ไวยากรณ์การกำหนดมูลค่าสินทรัพย์**

จากข้อมูลความต้องการในตารางที่ 6.1 ความต้องการข้อที่ 4-11 เป็นความต้องการที่ได้จากไวยากรณ์นี้ ซึ่งสามารถแสดงขั้นตอนการสร้างความต้องการความมั่นคงจากไวยากรณ์นี้ได้ดังรูปที่ 6.3



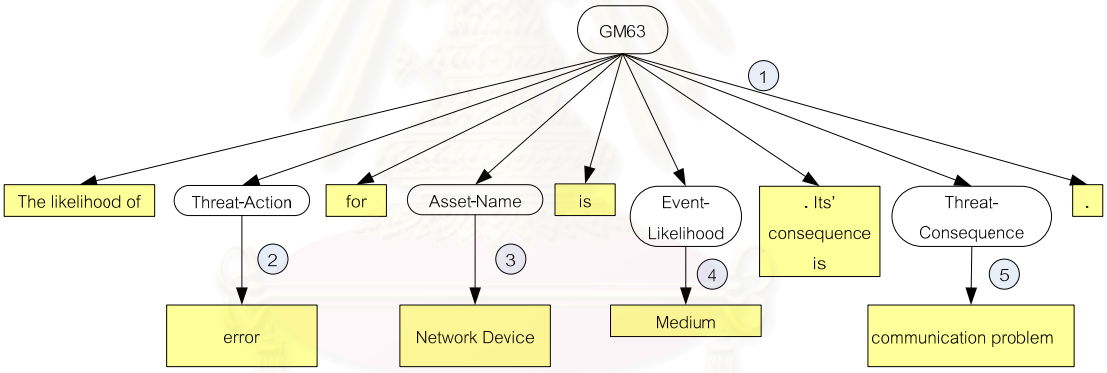
รูปที่ 6.3 การประยุกต์ใช้ไวยากรณ์การกำหนดมูลค่าสินทรัพย์

จากรูปที่ 6.3 แสดงให้เห็นขั้นตอนการประยุกต์ใช้ไวยากรณ์ โดยผลลัพธ์ที่ได้เกิดจากการนำเทอร์มินอลโหนดมาเรียงต่อกันตามลำดับ จะได้ความต้องการข้อที่ 4 ดังแสดงในตารางที่ 6.1 คือ *"The asset valuation of network device is extreme in security requirements rating, medium in financial value rating and extreme in business impact rating. So, the overall impact value is high."*

หมายเหตุ: ข้อความ "and" เป็นข้อความที่ได้จากความสามารถของเครื่องมือในการเพิ่ม "and" เข้าไปในประโยคความต้องการ สำหรับบางขอบเขตข้อมูลที่มีลักษณะเป็นรายการ เพื่อให้มีความหมายที่เหมาะสมและเป็นไปตามหลักไวยากรณ์ภาษาอังกฤษ

3) ไวยากรณ์การประเมินภัยคุกคาม

จากข้อมูลความต้องการในตารางที่ 6.1 ความต้องการข้อที่ 12-20 เป็นความต้องการที่ได้จากไวยากรณ์นี้ ซึ่งสามารถแสดงขั้นตอนการสร้างความต้องการความมั่นคงจากไวยากรณ์นี้ได้ดังรูปที่ 6.4



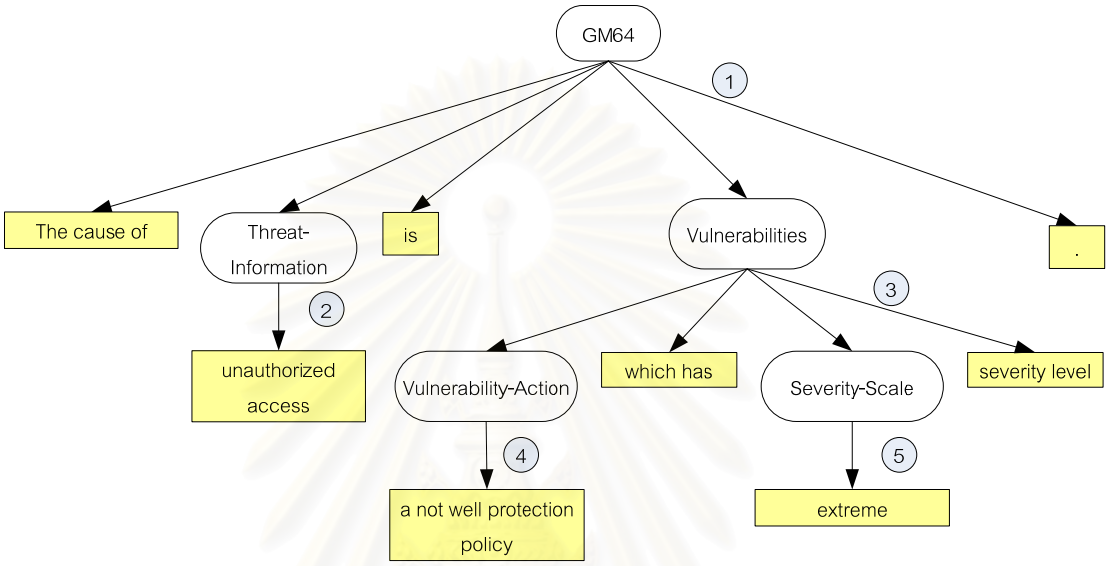
รูปที่ 6.4 การประยุกต์ใช้ไวยากรณ์การประเมินภัยคุกคาม

จากรูปที่ 6.4 แสดงให้เห็นขั้นตอนการประยุกต์ใช้ไวยากรณ์ โดยผลลัพธ์ที่ได้เกิดจากการนำเทอร์มินอลโหนดมาเรียงต่อกันตามลำดับ จะได้ความต้องการข้อที่ 12 ดังแสดงในตารางที่ 6.1 คือ *"The likelihood of error for Network Device is Medium. Its' consequence is communication problem."*

4) ไวยากรณ์การประเมินภาวะเสี่ยง

จากข้อมูลความต้องการในตารางที่ 6.1 ความต้องการข้อที่ 21-26 เป็นความต้องการที่ได้จากไวยากรณ์นี้ ซึ่งสามารถแสดงขั้นตอนการสร้างความต้องการความมั่นคงจากไวยากรณ์นี้ได้ดังรูปที่ 6.5

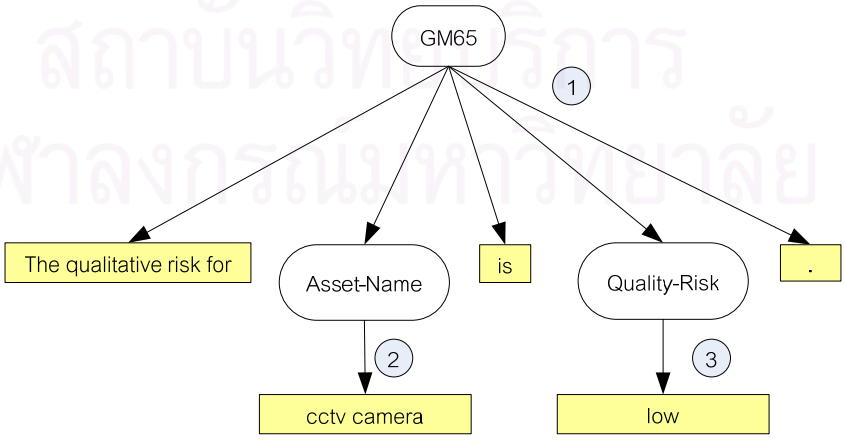
จากรูปที่ 6.5 แสดงให้เห็นขั้นตอนการประยุกต์ใช้ไวยากรณ์ โดยผลลัพธ์ที่ได้เกิดจากการนำเทอร์มินอลโหนดมาเรียงต่อกันตามลำดับ จะได้ความต้องการข้อที่ 21 ดังแสดงในตารางที่ 6.1 คือ *"The cause of unauthorized access is a not well protection policy which has extreme severity level."*



รูปที่ 6.5 การประยุกต์ใช้ไวยากรณ์การประเมินภาวะเสี่ยง

5) ไวยากรณ์การกำหนดค่าความเสี่ยง

จากข้อมูลความต้องการในตารางที่ 6.1 ความต้องการข้อที่ 27-31 เป็นความต้องการที่ได้จากไวยากรณ์นี้ ซึ่งสามารถแสดงขั้นตอนการสร้างความต้องการความมั่นคงจากไวยากรณ์นี้ได้ดังรูปที่ 6.6



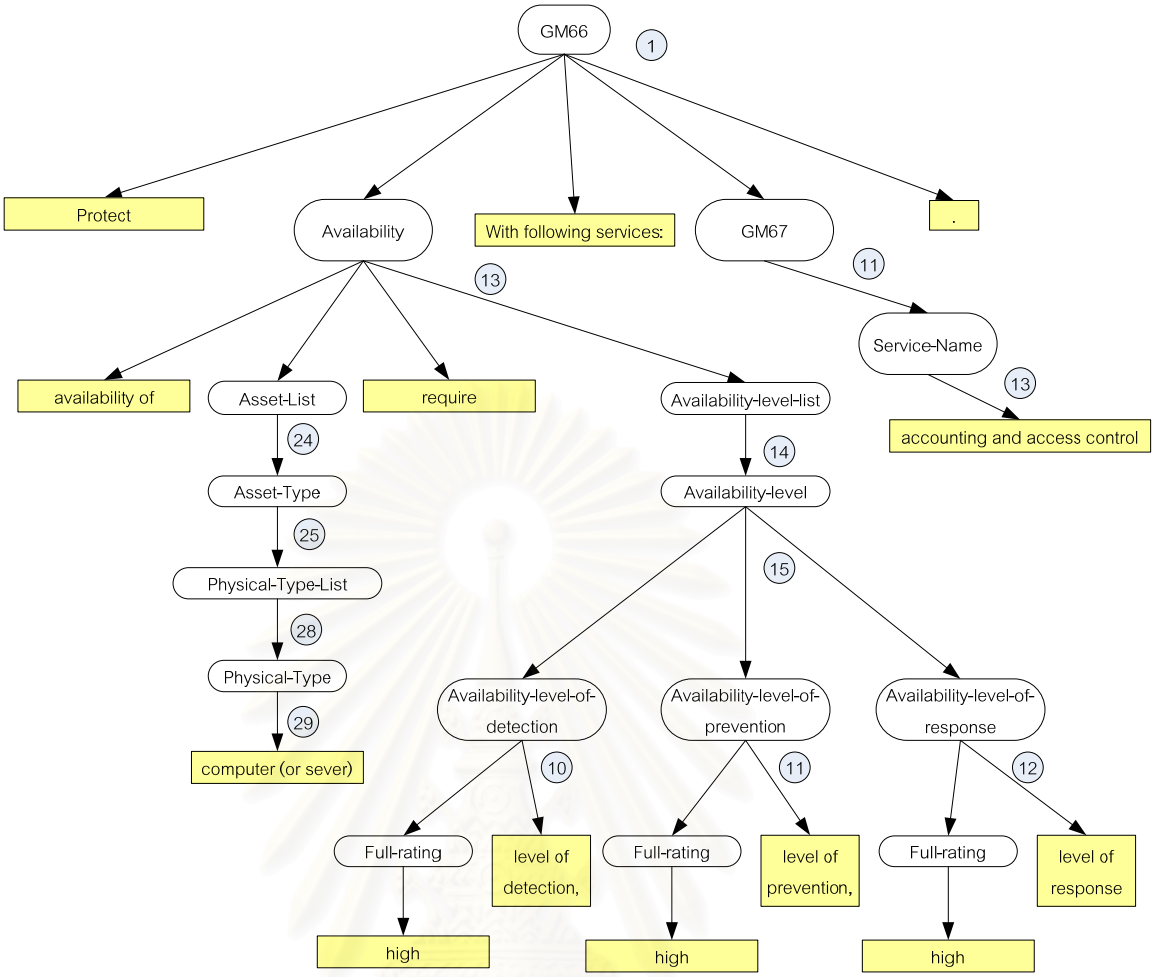
รูปที่ 6.6 การประยุกต์ใช้ไวยากรณ์การกำหนดค่าความเสี่ยง

จากรูปที่ 6.6 แสดงให้เห็นขั้นตอนการประยุกต์ใช้ไวยากรณ์ โดยผลลัพธ์ที่ได้เกิดจากการนำเทอร์มินอลโหนดมาเรียงต่อกันตามลำดับ จะได้ความต้องการข้อที่ 27 ดังแสดงในตารางที่ 6.1 คือ *“The qualitative risk for cctv camera is low.”*

หมายเหตุ: “Quality-Risk” เป็นค่าที่ได้จากการคำนวณของเครื่องมือ โดยใช้สูตรการคำนวณค่าความเสี่ยงตามที่นำเสนอไว้ใน [11] ผลลัพธ์การคำนวณมี 6 ระดับเท่านั้น ได้แก่ ระดับไม่มีความเสี่ยง (Negligible) ระดับความเสี่ยงต่ำ (Low) ระดับความเสี่ยงปานกลาง (Medium) ระดับความเสี่ยงสูง (High) ระดับความเสี่ยงสูงมาก (Extreme) และระดับความเสี่ยงสูงสุด (Extreme)

6) ไวยากรณ์แนวคิดความมั่นคงองค์กรและบริการความมั่นคงองค์กร

เนื่องจากไวยากรณ์บริการความมั่นคงองค์กรเป็นส่วนขยายของไวยากรณ์แนวคิดความมั่นคงองค์กร และกำหนดแนวคิดความมั่นคงองค์กรแล้ว จะต้องกำหนดบริการความมั่นคงองค์กรกำกับไว้เสมอ จากข้อมูลความต้องการในตารางที่ 6.1 ความต้องการข้อที่ 32-35 เป็นความต้องการที่ได้จากไวยากรณ์นี้ ซึ่งสามารถแสดงขั้นตอนการสร้างความต้องการความมั่นคงจากไวยากรณ์นี้ได้ดังรูปที่ 6.7



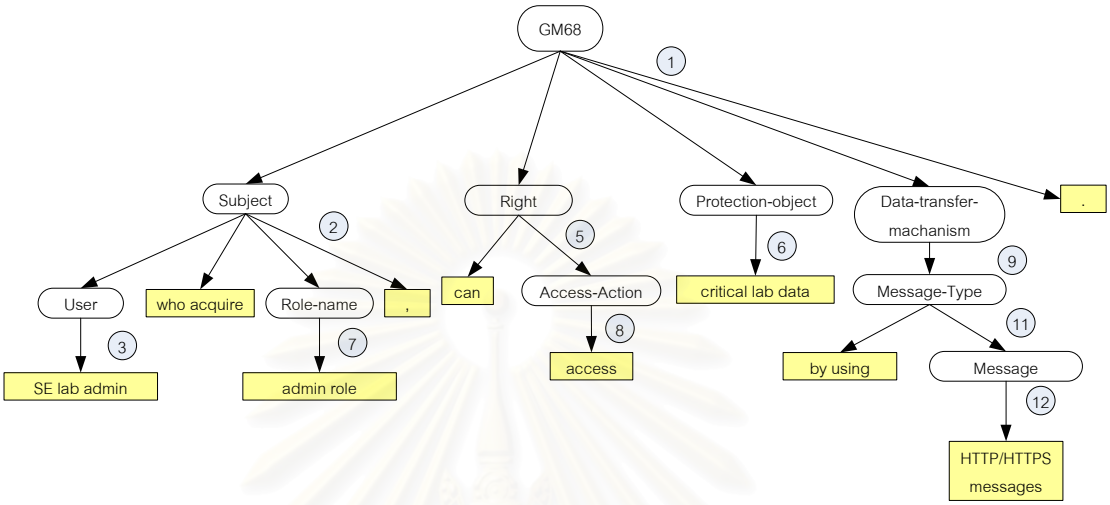
รูปที่ 6.7 การประยุกต์ใช้ไวยากรณ์แนวคิดและบริการความมั่นคงองค์กร

จากรูปที่ 6.7 แสดงให้เห็นขั้นตอนการประยุกต์ใช้ไวยากรณ์ โดยผลลัพธ์ที่ได้เกิดจากการนำเทอร์มินอลโหนดมาเรียงต่อกันตามลำดับ จะได้ความต้องการข้อที่ 32-35 ดังแสดงในตารางที่ 6.1 คือ *“Protect availability of computer (or server) require high level of detection, high level of prevention and high level of response with following services: accounting and access Control.”*

หมายเหตุ: ข้อความ “and” เป็นข้อความที่ได้จากความสามารถของเครื่องมือในการเพิ่ม “and” เข้าไปในประโยคความต้องการ สำหรับบางขอบเขตข้อมูลที่มีลักษณะเป็นรายการ เพื่อให้มีความหมายที่เหมาะสมและเป็นไปตามหลักไวยากรณ์ภาษาอังกฤษ

7) **ไวยากรณ์การสื่อสารของผู้มีหุ้นส่วนองค์กร**

จากข้อมูลความต้องการในตารางที่ 6.1 ความต้องการข้อที่ 36 เป็นความต้องการที่ได้จากไวยากรณ์นี้ ซึ่งสามารถแสดงขั้นตอนการสร้างความต้องการความมั่นคงจากไวยากรณ์นี้ได้ดังรูปที่ 6.8

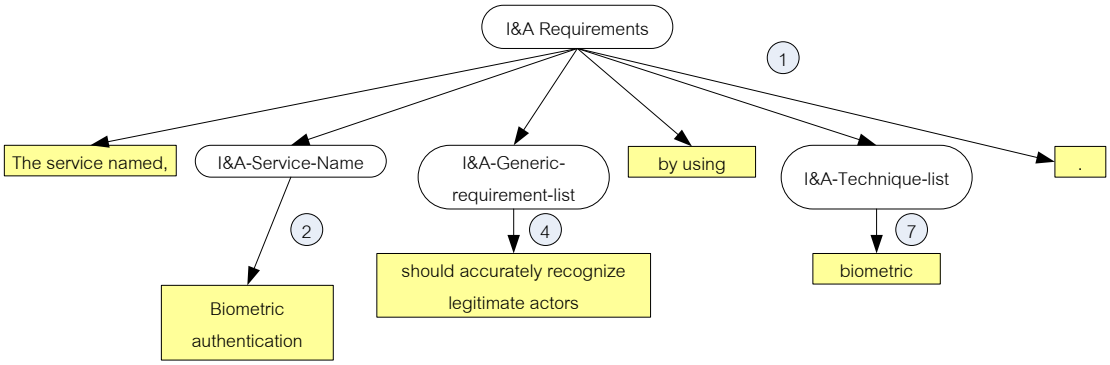


รูปที่ 6.8 การประยุกต์ใช้ไวยากรณ์การสื่อสารของผู้มีหุ้นส่วนองค์กร

จากรูปที่ 6.8 แสดงให้เห็นขั้นตอนการประยุกต์ใช้ไวยากรณ์ โดยผลลัพธ์ที่ได้เกิดจากการนำเทอร์มินอลโหนดมาเรียงต่อกันตามลำดับ จะได้ความต้องการข้อที่ 36 ดังแสดงในตารางที่ 6.1 คือ *“SE lab admin who acquire admin role can access critical lab data by using HTTP/HTTPS messages.”*

6.2.2 กลุ่มไวยากรณ์การระบุและการพิสูจน์ตัวตน

ความต้องการความมั่นคงจากไวยากรณ์กลุ่มนี้จะมุ่งเน้นการตรวจสอบการปฏิสัมพันธ์ระหว่างผู้ใช้กับระบบ โดยมีการตรวจสอบและยืนยันตัวตนก่อนการใช้งาน โดยจะมีการกำหนดความต้องการสำหรับกระบวนการดังกล่าว พร้อมทั้งนำเสนอกลยุทธ์ที่สามารถใช้ได้ในกระบวนดังกล่าวนี้ด้วย กลุ่มไวยากรณ์นี้ประกอบด้วย 4 ไวยากรณ์ที่มีความเกี่ยวเนื่องกัน ซึ่งสามารถนำมาบูรณาการเป็นไวยากรณ์เดียวกันได้ จากข้อมูลความต้องการในตารางที่ 6.1 ความต้องการข้อที่ 37 เป็นความต้องการที่ได้จากไวยากรณ์นี้ ซึ่งสามารถแสดงขั้นตอนการสร้างความต้องการความมั่นคงจากไวยากรณ์นี้ได้ดังรูปที่ 6.9



รูปที่ 6.9 การประยุกต์กลุ่มใช้ไวยากรณ์การระบุตัวตนและการพิสูจน์ตัวตน

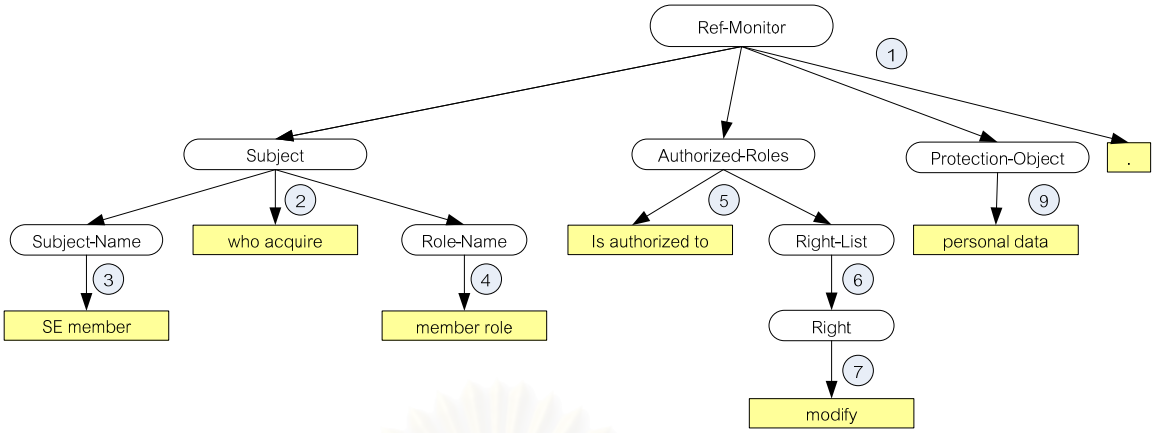
จากรูปที่ 6.9 แสดงให้เห็นขั้นตอนการประยุกต์ใช้ไวยากรณ์ โดยผลลัพธ์ที่ได้เกิดจากการนำนอนเทอร์มินอลโหนดมาต่อกันจะได้ความต้องการข้อที่ 37 ดังแสดงในตารางที่ 6.1 คือ *"The service named, biometric authentication, should accurately recognize legitimate actors by using biometric."*

6.2.3 กลุ่มไวยากรณ์การควบคุมการเข้าถึง

ความต้องการความมั่นคงจากไวยากรณ์กลุ่มนี้จะมุ่งเน้นกำหนดเงื่อนไขบังคับในการเข้าใช้งานระบบ ให้เป็นไปตามสิทธิ์หรือบทบาทที่ได้รับ รวมถึงการกำหนดระดับความมั่นคงของสินทรัพย์ ประกอบด้วย 5 ไวยากรณ์ โดยไวยากรณ์การตรวจสอบการเข้าถึงทรัพยากร จะครอบคลุมไวยากรณ์การให้อำนาจ และการควบคุมการเข้าถึงเชิงบทบาท จึงสามารถแสดงการประยุกต์ใช้ไวยากรณ์ทั้ง 3 ไวยากรณ์ได้โดยใช้ไวยากรณ์การตรวจสอบการเข้าถึงทรัพยากรเป็นหลัก สำหรับอีก 2 ไวยากรณ์ ได้แก่ การกำหนดสิทธิ์ให้กับบทบาท และการความมั่นคงหลายระดับจะแยกออกจาก 3 ไวยากรณ์ก่อนหน้านี้

1) ไวยากรณ์การตรวจสอบการเข้าถึงทรัพยากร

จากข้อมูลความต้องการในตารางที่ 6.1 ความต้องการข้อที่ 38-41 เป็นความต้องการที่ได้จากไวยากรณ์นี้ ซึ่งสามารถแสดงขั้นตอนการสร้างความต้องการความมั่นคงจากไวยากรณ์นี้ได้ดังรูปที่ 6.10

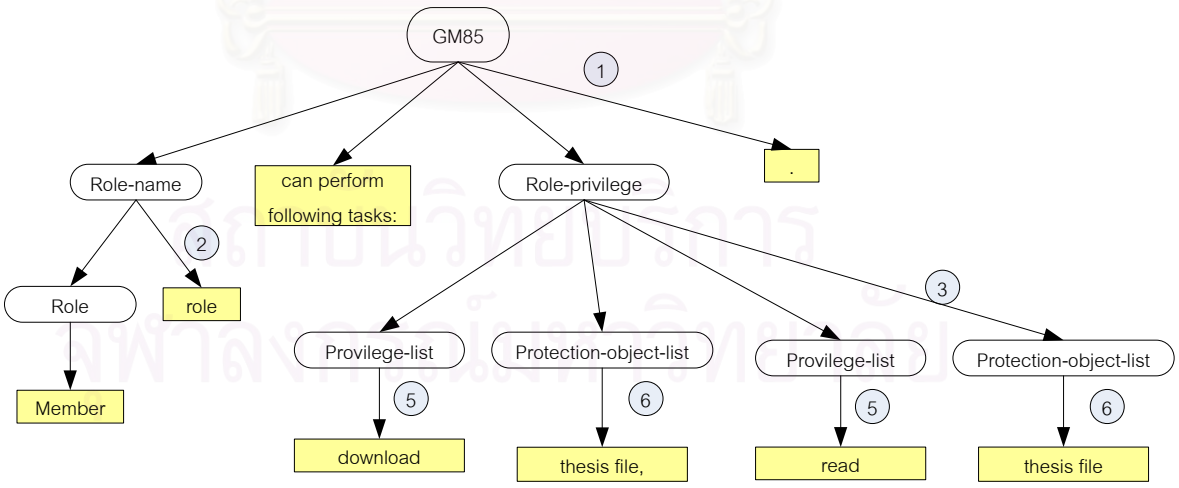


รูปที่ 6.10 การประยุกต์ใช้ไวยากรณ์การตรวจสอบการเข้าถึงทรัพยากร

จากรูปที่ 6.10 แสดงให้เห็นขั้นตอนการประยุกต์ใช้ไวยากรณ์ โดยผลลัพธ์ที่ได้เกิดจากการนำเทอร์มินอลโหนดมาเรียงต่อกันตามลำดับ จะได้ความต้องการข้อที่ 38 ดังแสดงในตารางที่ 6.1 คือ “*SE member who acquire member role is authorized to modify personal data.*”

2) **ไวยากรณ์การกำหนดสิทธิ์ให้กับบทบาท**

จากข้อมูลความต้องการในตารางที่ 6.1 ความต้องการข้อที่ 44-45 เป็นความต้องการที่ได้จากไวยากรณ์นี้ ซึ่งสามารถแสดงขั้นตอนการสร้างความต้องการความมั่นคงจากไวยากรณ์นี้ได้ดังรูปที่ 6.11



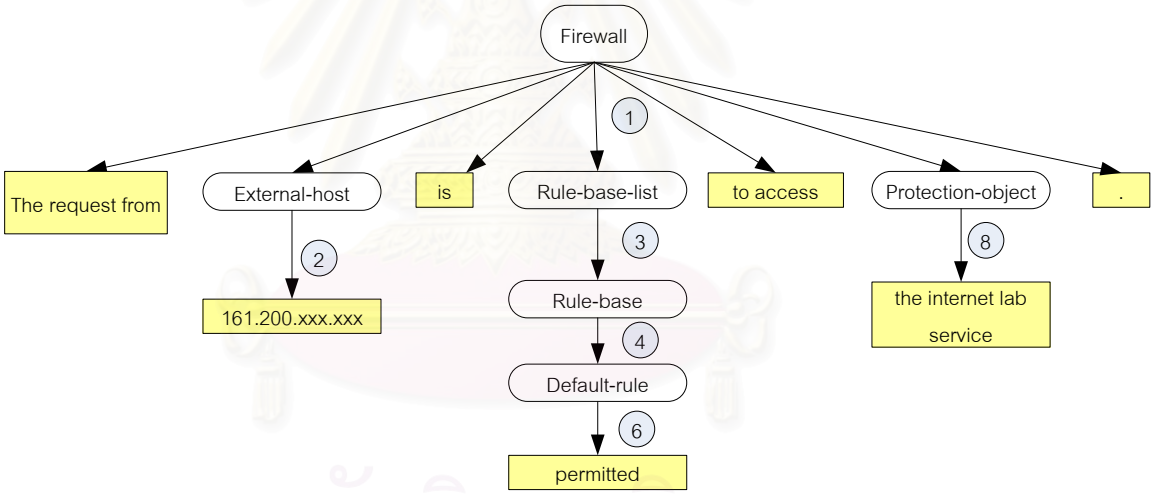
รูปที่ 6.11 การประยุกต์ใช้ไวยากรณ์การตรวจสอบการเข้าถึงทรัพยากร

จากรูปที่ 6.11 แสดงให้เห็นขั้นตอนการประยุกต์ใช้ไวยากรณ์ โดยผลลัพธ์ที่ได้เกิดจากการนำเทอร์มินอลโหนดมาเรียงต่อกันตามลำดับ จะได้ความต้องการข้อที่ 44 ดังแสดงในตารางที่ 6.1 คือ *"Member role can perform following task: download thesis file, read thesis file."*

หมายเหตุ: "Role-Privilege" ในที่นี้ถูกใช้ กฎที่ 3 สองครั้ง จึงได้ "download thesis file" และ "read thesis file"

6.2.4 กลุ่มไวยากรณ์สถาปัตยกรรมไฟล์วอลล์

ความต้องการความมั่นคงจากไวยากรณ์กลุ่มนี้จะมุ่งเน้นกำหนดเงื่อนไขบังคับในการเข้าใช้งานระบบผ่านทางเครือข่าย ประกอบด้วย 3 ไวยากรณ์ที่มีความต่อเนื่องกัน ซึ่งสามารถบูรณาการไวยากรณ์เป็นไวยากรณ์เดียวกันได้ จากข้อมูลความต้องการในตารางที่ 6.1 ความต้องการข้อที่ 46-48 เป็นความต้องการที่ได้จากไวยากรณ์นี้ ซึ่งสามารถแสดงขั้นตอนการสร้างความต้องการความมั่นคงจากไวยากรณ์นี้ได้ดังรูปที่ 6.12



รูปที่ 6.12 การประยุกต์ใช้ไวยากรณ์การตรวจสอบการเข้าถึงทรัพยากร

จากรูปที่ 6.12 แสดงให้เห็นขั้นตอนการประยุกต์ใช้ไวยากรณ์ โดยผลลัพธ์ที่ได้เกิดจากการนำเทอร์มินอลโหนดมาเรียงต่อกันตามลำดับ จะได้ความต้องการข้อที่ 46 ดังแสดงในตารางที่ 6.1 คือ *"The request from 161.200.xxx.xxx is permitted to access the internet lab services."*

จากการแสดงการประยุกต์ใช้ไวยากรณ์ความมั่นคงข้างต้น แสดงให้เห็นว่าไวยากรณ์ความมั่นคงที่นำเสนอในงานวิทยานิพนธ์นี้สามารถช่วยเหลือผู้ใช้ในการแนะนำองค์ประกอบ

สำคัญที่ควรปรากฏในความต้องการความมั่นคงแต่ละแบบ เพื่อให้ความต้องการมีความครบถ้วนและถูกต้องมากขึ้นกว่าการกำหนดโดยมือ อย่างไรก็ตาม ไวยากรณ์ความมั่นคงที่นำเสนอในงานวิจัยนี้ มีวัตถุประสงค์เพื่อนำเสนอใกล้เคียงกับการนำเสนอแผ่นแบบ (Template) เพื่อเป็นแนวทางในการกำหนดองค์ประกอบสำคัญในการสร้างความต้องการความมั่นคงเท่านั้น ผลลัพธ์ความต้องการความมั่นคงที่ได้จะมีโครงสร้างและองค์ประกอบที่ชัดเจนในเชิงวากยสัมพันธ์ (Syntax) เท่านั้น แต่ความผิดพลาดที่ปรากฏในผลลัพธ์ความต้องการความมั่นคง เช่น การสะกดผิดของคำ การป้อนข้อมูลที่ผิดความหมายไปจากเขตข้อมูล (Field) เป็นต้น ซึ่งทำให้ความหมาย (Semantic) ของความต้องการความมั่นคงผิดไปจากที่ควรเป็น ถือเป็นความผิดพลาดจากผู้ใช้ในการป้อนข้อมูล ดังนั้นการใช้งานไวยากรณ์ความมั่นคงใดก็ตาม ผู้ใช้จึงมีความจำเป็นที่จะต้องทำความเข้าใจว่าตนเองป้อนข้อมูลที่สอดคล้องกับเขตข้อมูลที่ไวยากรณ์กำหนดให้หรือไม่

บทที่ 7
การประเมินผลลัพธ์ความต้องการความมั่นคงที่ได้จากเครื่องมือ

ในบทนี้จะแสดงให้เห็นว่าความต้องการความมั่นคงที่ได้จากเครื่องมือมีคุณภาพมากขึ้นในด้านความครบถ้วน ความถูกต้อง โดยใช้การเปรียบเทียบผลลัพธ์ความต้องการความมั่นคงสำหรับระบบสนับสนุนห้องปฏิบัติการที่ได้จากหน่วยทดลอง 1 คนทั้งแบบกำหนดด้วยมือและแบบที่ใช้เครื่องมือ เพื่อเปรียบเทียบให้เห็นความแตกต่างระหว่างผลลัพธ์ทั้งสอง และเพื่อแสดงให้เห็นว่าไวยากรณ์ความมั่นคงที่นำเสนอนั้นสามารถช่วยลดปัญหาความต้องการที่ไม่ถูกต้องและครบถ้วนของความต้องการความมั่นคงด้วยมือได้

7.1 การเปรียบเทียบผลลัพธ์ความต้องการในกลุ่มความมั่นคงสินทรัพย์

ตารางที่ 7.1 แสดงผลลัพธ์ความต้องการความมั่นคงจากการกำหนดด้วยมือเปรียบเทียบกับผลลัพธ์ความมั่นคงที่ได้จากเครื่องมือที่เกี่ยวข้องกับความมั่นคงของสินทรัพย์ ส่วนประกอบที่ควรปรากฏในความต้องการสำหรับใช้ในการพิจารณาในกลุ่มแบบรูปนี้ ประกอบด้วย

1) ชื่อสินทรัพย์
2) คุณสมบัติความมั่นคง
3) มูลค่าสินทรัพย์
4) ข้อมูลภัยคุกคาม ความถี่ของภัยคุกคาม และผลกระทบจากภัยคุกคาม
5) ข้อมูลภาวะเสี่ยง และระดับความรุนแรง
6) ข้อมูลค่าความเสี่ยง
7) แนวคิดความมั่นคงองค์กร
8) บริการความมั่นคงองค์กร
9) ข้อมูลการสื่อสารของหุ้นส่วนองค์กร

ในการพิจารณาความครบถ้วนของความต้องการ จะพิจารณาว่าความต้องการความมั่นคงดังกล่าวมีองค์ประกอบครบตามที่แบบรูปความมั่นคงกำหนดไว้หรือไม่ โดยถ้าความต้องการในกลุ่มดังกล่าวมีครบทุกองค์ประกอบหรือไม่ ถ้ามีจะคิดเป็น 100% ของขอบเขตไวยากรณ์ความมั่นคง

ตารางที่ 7.1 ตารางเปรียบเทียบความต้องการความมั่นคงในกลุ่มความต้องการความมั่นคงที่เกี่ยวข้องกับความมั่นคงสินทรัพย์

ความต้องการความมั่นคงที่ได้จากการกำหนดด้วยมือ	ความต้องการความมั่นคงที่ได้จากเครื่องมือ
- Critical data require confidentiality, integrity, availability and accountability. - All computer or severs, network devices, printer require extreme of prevention, detection and response. - The error of network devices causes communication failure in the SE lab which has extreme severity level.	- Computer (or server), network device, printer, CCTV camera and office facilitate requires confidentially, integrity, availability and accountability under the auspices of business process, costs and laws or regulation. - Personal data requires confidentially, integrity and availability under the auspices of business process. - SE Lab member requires confidentially, integrity and availability under the auspices of critical business process and mission and goals. - The asset valuation of network device is extreme in security requirements rating, medium in financial value rating and extreme in business impact rating. So, the overall impact value is high. - The asset valuation of computer (or server) is extreme in security requirements rating, high in financial value rating and extreme in business impact rating. So, the overall impact value is high. - The asset valuation of CCTV camera is extreme in security requirements rating, high in financial value rating and high in business impact rating. So, the overall impact value is high. - The asset valuation of printer is negligible in security requirements rating, medium in financial value rating and high in business impact rating. So, the overall impact value is low. - The asset valuation of SE lab member is very high in security requirements rating, low in financial value rating and low in business impact rating. So, the overall impact value is low. - The asset valuation of critical lab data is extreme in security requirements rating, high in financial value rating and very high in business impact rating. So, the overall impact value is very high. - The asset valuation of personal data is very high in security requirements rating, low in financial value rating and low in business impact rating. So, the overall impact value is low. - The asset valuation of thesis is very high in security requirements rating, low in financial value rating and low in business impact rating. So, the overall impact value is low. - The likelihood of error for network device is medium. Its' consequence is communication problem.

ตารางที่ 7.1 ตารางเปรียบเทียบความต้องการความมั่นคงในกลุ่มความต้องการความมั่นคงที่เกี่ยวข้องกับความมั่นคงสินทรัพย์ (ต่อ)

ความต้องการความมั่นคงที่ได้จากการกำหนดด้วยมือ	ความต้องการความมั่นคงที่ได้จากเครื่องมือ
	- The likelihood of hacked (in case of server) for computer (or server) is medium. Its' consequence is denial of service. - The likelihood of lost for computer (or server) is low. Its' consequence is chaos in the lab, such as, contacting to a police, an owner of that computer cannot work at all. - The likelihood of lost for network device is low. Its' consequence is communication failure. - The likelihood of lost for critical lab data is low. Its' consequence is the SE lab is most losing. - The likelihood of lost or damaged for CCTV camera is low. Its' consequence is attacker monitoring failure. - The likelihood of unauthorized access for critical lab data is medium. Its' consequence is the data is hacked. - The likelihood of unauthorized modification for SE lab member is medium. Its' consequence is attacker can enter the SE room, and real SE member cannot enter the SE room. - The likelihood of unauthorized modification for personal data is medium. Its' consequence is the owner of data is not satisfied, and cannot work on their work properly. - The cause of unauthorized access is a not well protection policy which has extreme severity level. - The cause of lost is an attacker want to attack, or want to steal a device which has extreme severity level. - The cause of lost or damaged is attacker want to reduce the security level of the SE lab which has very high severity level. - The cause of unauthorized modification is be pretending of someone external or internal which has Very high severity level. - The cause of Lost is Thief want to steal it which has Very high severity level. - The cause of Lost is unexpectedly event which has Extreme severity level. - The qualitative risk for cctv camera is low. - The qualitative risk for computer (or server) is low. - The qualitative risk for critical lab data is extreme. - The qualitative risk for network device is medium. - The qualitative risk for personal data is low. - Protect availability of computer (or server) require high level of detection, high level of prevention and high level of response with

ตารางที่ 7.1 ตารางเปรียบเทียบความต้องการความมั่นคงในกลุ่มความต้องการความมั่นคงที่เกี่ยวข้องกับความมั่นคงสินทรัพย์ (ต่อ)

ความต้องการความมั่นคงที่ได้จากการกำหนดด้วยมือ	ความต้องการความมั่นคงที่ได้จากเครื่องมือ
	following services: accounting and access Control. - Protect availability of network device require high level of detection, high level of prevention and high level of response with following services: security management. - Protect confidentiality of critical lab data require high level of detection and high level of prevention with following services: accounting, access control and security management. - Protect confidentiality of SE lab member require high level of detection and high level of prevention with following services: accounting and access control. - SE lab admin who acquire admin role can access critical lab data by using HTTP/HTTPS messages.

ผลการเปรียบเทียบผลลัพธ์ความต้องการแสดงดังตารางที่ 7.2

ตารางที่ 7.2 ผลการเปรียบเทียบผลลัพธ์ความต้องการในกลุ่มความมั่นคงของสินทรัพย์

ประเภทผลลัพธ์ความต้องการความมั่นคงในกลุ่มความต้องการความมั่นคงที่เกี่ยวข้องกับความมั่นคงสินทรัพย์	ชื่อสินทรัพย์	คุณสมบัติความมั่นคง	มูลค่าสินทรัพย์	ข้อมูลภัยคุกคาม: ภัยคุกคาม	ข้อมูลภัยคุกคาม: ความถี่ภัยคุกคาม	ข้อมูลภัยคุกคาม: ผลกระทบจากภัยคุกคาม	ข้อมูลภาวะเสี่ยง: ภาวะเสี่ยงสำหรับภัยคุกคาม	ข้อมูลภาวะเสี่ยง: ระดับความแข็งแกร่งของภาวะเสี่ยง	ข้อมูลค่าความเสี่ยง	แนวคิดความมั่นคงขององค์กร	ปริมาตรความมั่นคงขององค์กร	ข้อมูลชื่อสินทรัพย์ขององค์กร	เปอร์เซ็นต์ขององค์ประกอบที่ปรากฏในความต้องการเทียบกับองค์ประกอบในแบบรูปความมั่นคงทั้งหมด (%)
ความต้องการจากมือ	✓	✓					✓	✓	✓	✓			50.00
ความต้องการจากเครื่องมือ	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	100.00

จากตารางที่ 7.2 ภายในขอบเขตการพิจารณากลุ่มความต้องการความมั่นคงที่เกี่ยวข้องกับความมั่นคงสินทรัพย์พบว่า เมื่อผู้ทดลองกำหนดความต้องการความมั่นคงด้วยมือสำหรับระบบสนับสนุนห้องปฏิบัติการ จะครอบคลุมองค์ประกอบที่ควรพิจารณาตามที่นำเสนอโดยแบบรูปความมั่นคงมีสัดส่วนเพียง 50% ในขณะที่การใช้เครื่องมือสามารถเพิ่มสัดส่วนได้ถึงระดับ 100% ซึ่งแสดงให้เห็นว่าไวยากรณ์ความมั่นคงสามารถใช้เป็นแนวทางในการกำหนดความต้องการความมั่นคงได้อย่างครบถ้วน และถูกต้องมากขึ้นตามองค์ประกอบที่นำเสนอโดยแบบรูปความมั่นคง

7.2 การเปรียบเทียบผลลัพธ์ความต้องการในกลุ่มการระบุและพิสูจน์ตัวตน

จากตารางที่ 7.3 แสดงผลลัพธ์ความต้องการความมั่นคงจากการกำหนดด้วยมือเปรียบเทียบกับผลลัพธ์ความมั่นคงที่ได้จากเครื่องมือในกลุ่มการระบุและพิสูจน์ตัวตน โดยส่วนประกอบที่ควรปรากฏในความต้องการสำหรับใช้ในการพิจารณาในกลุ่มแบบรูปนี้ประกอบด้วย

1) ชื่อบริการด้านการระบุและพิสูจน์ตัวจริง
2) ความต้องการพื้นฐานสำหรับบริการด้านการระบุและการพิสูจน์ตัวจริง
3) เทคนิคการตรวจสอบการบริการด้านการระบุและการพิสูจน์ตัวจริง เช่น พีเคเอ (Public Key Interchange: PKI) ชีวมิติ ตัวระบุ (Identifier) และรหัสผ่าน (Password) เป็นต้น

ตารางที่ 7.3 ตารางเปรียบเทียบความต้องการความมั่นคงในกลุ่มความต้องการด้านการพิสูจน์และระบุตัวตน

ความต้องการความมั่นคงที่ได้จากการกำหนดด้วยมือ	**ความต้องการความมั่นคงที่ได้จากเครื่องมือ**
- All SE lab members must be authenticated by using their finger before enter to laboratory. - All SE lab members must be authenticated by using their finger print.	- The service named, biometric authentication, should accurately recognize legitimate actors by using biometric.

ผลการเปรียบเทียบผลลัพธ์ความต้องการแสดงดังตารางที่ 7.4

ตารางที่ 7.4 ผลการเปรียบเทียบผลลัพธ์ความต้องการในกลุ่มการระบุและพิสูจน์ตัวตน

ประเภทผลลัพธ์ความต้องการความมั่นคงในกลุ่มความต้องการการพิสูจน์และระบุตัวตน	ชื่อบริการ	ความต้องการพื้นฐาน	วิธีการพิสูจน์ตัวตนโดยใช้เทคโนโลยี	เปอร์เซ็นต์ขององค์ประกอบที่ปรากฏในความต้องการเทียบกับองค์ประกอบในแบบรูปความมั่นคงทั้งหมด (%)
ความต้องการจากมือ	✓		✓	66.67
ความต้องการจากเครื่องมือ	✓	✓	✓	100.00

จากตารางที่ 7.4 ภายในขอบเขตการพิจารณากลุ่มความต้องการความมั่นคงที่เกี่ยวข้องกับการระบุและพิสูจน์ตัวตน เมื่อผู้ทดลองกำหนดความต้องการความมั่นคงด้วยมือสำหรับระบบสนับสนุนห้องปฏิบัติการ จะครอบคลุมองค์ประกอบที่ควรพิจารณาตามที่นำเสนอโดยแบบรูปความมั่นคงมีสัดส่วนเพียง 66.67% ในขณะที่การใช้เครื่องมือสามารถเพิ่มสัดส่วนได้ถึงระดับ 100% ซึ่งแสดงให้เห็นว่าไวยากรณ์ความมั่นคงสามารถใช้เป็นแนวทางในการกำหนดความต้องการความมั่นคงได้อย่างครบถ้วน และถูกต้องมากขึ้นตามองค์ประกอบที่นำเสนอโดยแบบรูปความมั่นคง

7.3 การเปรียบเทียบผลลัพธ์ความต้องการในกลุ่มแบบจำลองการควบคุมการเข้าถึง

จากตารางที่ 7.5 แสดงผลลัพธ์ความต้องการความมั่นคงจากการกำหนดด้วยมือเปรียบเทียบกับผลลัพธ์ความมั่นคงที่ได้จากเครื่องมือที่เกี่ยวข้องกับแบบจำลองการควบคุมการเข้าถึง โดยส่วนประกอบที่ควรปรากฏในความต้องการสำหรับใช้ในการพิจารณาในกลุ่มแบบรูปนี้ประกอบด้วย

1) ผู้ใช้งาน หรือกระบวนการที่ต้องการใช้ทรัพยากร
2) บทบาทสำหรับผู้ใช้งานหรือ กระบวนการที่ต้องการใช้ทรัพยากร
3) กฎ
4) สิทธิ์สำหรับผู้ใช้งาน หรือสิทธิ์สำหรับบทบาท
5) ทรัพยากรหรือสินทรัพย์
6) ระดับความมั่นคงของสินทรัพย์
7) ระดับความมั่นคงของผู้ใช้งานหรือกระบวนการที่ต้องการใช้ทรัพยากร

ตารางที่ 7.5 ตารางเปรียบเทียบความต้องการความมั่นคงในกลุ่มความต้องการควบคุมการเข้าถึง

กลุ่มไวยากรณ์	ความต้องการความมั่นคงที่ได้จากการกำหนดด้วยมือ	ความต้องการความมั่นคงที่ได้จากเครื่องมือ
ความต้องการการควบคุมการเข้าถึง	- Each SE lab member can read and modify data which is their own. - Each SE lab member cannot read and modify other member data. - All SE lab members can read thesis data but cannot modify it. - All SE lab admin can read and modify data the thesis data. - All computer or severs, network devices, printer are the extreme asset for SE lab.	- SE member who acquire member role can modify personal data. - SE member who acquire admin role can modify SE lab member. - SE member who acquire admin role can modify critical lab data. - SE member who acquire member role can access thesis. - SE Lab member has a medium clearance level. - SE Lab admin has a very high clearance level. - Member role can perform following tasks: download thesis file and read thesis file. - Admin role can perform following tasks: access thesis file, delete thesis information, download thesis file, modify thesis information and read thesis file.

ผลการเปรียบเทียบผลลัพธ์ความต้องการแสดงดังตารางที่ 7.6

ตารางที่ 7.6 ผลการเปรียบเทียบผลลัพธ์ความต้องการในกลุ่มแบบจำลองการควบคุมการเข้าถึง

ประเภทผลลัพธ์ความต้องการความมั่นคงในกลุ่มความต้องการความมั่นคงที่เกี่ยวข้องกับแบบจำลองการควบคุมการเข้าถึง	ผู้ใช้งาน หรือผู้ที่ต้องการใช้ทรัพยากร	หน่วยที่ใช้ทรัพยากร	ปริมาณ	สิทธิ์	ระดับความมั่นคงของทรัพย์	ระดับความมั่นคงของผู้ใช้งาน	ทรัพยากรที่จัดเก็บทรัพย์	เปอร์เซ็นต์ขององค์ประกอบที่ปรากฏในความต้องการเทียบกับองค์ประกอบในแบบรูปความมั่นคงทั้งหมด (%)
ความต้องการจากมือ	✓	✓					✓	42.86
ความต้องการจากเครื่องมือ	✓	✓		✓		✓	✓	71.43

จากตารางที่ 7.6 ภายในขอบเขตการพิจารณากลุ่มความต้องการความมั่นคงที่เกี่ยวข้องกับแบบจำลองการควบคุมเชิงการเข้าถึง เมื่อผู้ทดลองกำหนดความต้องการความมั่นคงด้วยมือสำหรับระบบสนับสนุนห้องปฏิบัติการ จะครอบคลุมองค์ประกอบที่ควรพิจารณาตามที่นำเสนอโดยแบบรูปความมั่นคงมีสัดส่วนเพียง 42.85% ในขณะที่การใช้เครื่องมือสามารถเพิ่มสัดส่วนได้ถึงระดับ 71.43% ซึ่งแสดงให้เห็นว่าไวยากรณ์ความมั่นคงสามารถใช้เป็นแนวทางในการกำหนดความต้องการความมั่นคงได้อย่างครบถ้วน และถูกต้องมากขึ้นตามองค์ประกอบที่นำเสนอโดยแบบรูปความมั่นคง

เปอร์เซ็นต์ของการใช้เครื่องมือไม่ถึง 100% เนื่องจากผู้ทดลองไม่ได้ใช้ไวยากรณ์ทั้งหมด ทำให้องค์ประกอบของความต้องการผลลัพธ์จึงไม่ครบถ้วนตามที่เสนอไว้ในแบบรูปความมั่นคง

7.4 การเปรียบเทียบผลลัพธ์ความต้องการในกลุ่มสถาปัตยกรรมไฟล์วอลล์

ตารางที่ 7.7 แสดงผลลัพธ์ความต้องการความมั่นคงจากการกำหนดด้วยมือเปรียบเทียบกับผลลัพธ์ความมั่นคงที่ได้จากเครื่องมือที่เกี่ยวข้องกับสถาปัตยกรรมไฟล์วอลล์ โดยส่วนประกอบที่ควรปรากฏในความต้องการสำหรับใช้ในการพิจารณาในกลุ่มแบบรูปนี้ ประกอบด้วย

1) ผู้ติดต่อภายนอก
2) สินทรัพย์ที่อยู่ภายในระบบ
3) รูปแบบการติดต่อ เช่น บริการที่ใช้ และ พอร์ต เป็นต้น
4) ความต้องการพื้นฐาน
5) เงื่อนไขบังคับ
6) สิทธิ์สำหรับผู้ติดต่อ

ตารางที่ 7.7 ตารางเปรียบเทียบความต้องการความมั่นคงในกลุ่มความต้องการด้านสถาปัตยกรรมไฟล์วอลล์

กลุ่มไวยากรณ์	ความต้องการความมั่นคงที่ได้จากการกำหนดด้วยมือ	ความต้องการความมั่นคงที่ได้จากเครื่องมือ
ความต้องการด้านสถาปัตยกรรม	- Lab's firewall has to block ports of P2P program.	- The request from 161.200.xxx.xxx is permitted to access the internet lab services. - The request from the external host is denied to access critical lab data through HTTP/HITTPS, FTP/FTPS port. - The request from the P2P package is permitted to access office facilitate through P2P protocol port. the bandwidth can not more than 50KB/s

ผลการเปรียบเทียบผลลัพธ์ความต้องการแสดงดังตารางที่ 7.8

ตารางที่ 7.8 ผลการเปรียบเทียบผลลัพธ์ความต้องการในกลุ่มสถาปัตยกรรมไฟล์วอลล์

ประเภทผลลัพธ์ความต้องการความมั่นคงในกลุ่มความต้องการการสถาปัตยกรรมไฟล์วอลล์	ผู้ติดต่อจากภายนอก	สินทรัพย์ภายในระบบ	รูปแบบการติดต่อสื่อสาร	ความต้องการคุณสมบัติพื้นฐาน	สิทธิ์สำหรับผู้ติดต่อ	เงื่อนไขบังคับ	เปอร์เซ็นต์ขององค์ประกอบที่ปรากฏในความต้องการเทียบกับองค์ประกอบในแบบรูปความมั่นคงทั้งหมด (%)
ความต้องการจากมือ	✓		✓				33.33
ความต้องการจากเครื่องมือ	✓	✓	✓	✓		✓	83.33

จากตารางที่ 7.8 ภายในขอบเขตการพิจารณากลุ่มความต้องการความมั่นคงที่เกี่ยวข้องกับสถาปัตยกรรมไฟล์วอลล์ เมื่อผู้ทดลองกำหนดความต้องการความมั่นคงด้วยมือสำหรับระบบสนับสนุนห้องปฏิบัติการ จะครอบคลุมองค์ประกอบที่ควรพิจารณาตามที่นำเสนอโดยแบบรูปความมั่นคงมีสัดส่วนเพียง 33.33% ในขณะที่การใช้เครื่องมือสามารถเพิ่มสัดส่วนได้ถึงระดับ 83.33% ซึ่งแสดงให้เห็นว่าไวยากรณ์ความมั่นคงสามารถใช้เป็นแนวทางในการกำหนดความต้องการความมั่นคงได้อย่างครบถ้วน และถูกต้องมากขึ้นตามองค์ประกอบที่นำเสนอโดยแบบรูปความมั่นคง

จากการเปรียบเทียบความต้องการความมั่นคงที่เป็นผลลัพธ์จากการกำหนดด้วยมือและผลลัพธ์ความต้องการที่ได้จากเครื่องในแต่ละกลุ่มความต้องการ จะเห็นได้ว่าไวยากรณ์ความมั่นคงสามารถช่วยให้ผู้ใช้สามารถสร้างความต้องการที่มีความครบถ้วนและถูกต้องมากขึ้น โดยใช้องค์ประกอบจากแบบรูปมาใช้การพิจารณา

บทที่ 8
สรุปผลการวิจัยและแนวทางการวิจัยต่อ

ในบทนี้จะกล่าวสรุปผลการวิจัยที่ได้ดำเนินการ และเสนอแนวทางในการทำวิจัยที่สามารถต่อยอดจากงานวิจัยนี้ได้ โดยมีรายละเอียดดังนี้

8.1 สรุปงานวิจัย

กระบวนการวิศวกรรมความต้องการซอฟต์แวร์เป็นกระบวนการสำคัญในลำดับต้นๆ ของการพัฒนา เนื่องจากเกี่ยวข้องกับการรวบรวมความต้องการเพื่อนำมาวิเคราะห์และสร้างเป็นข้อกำหนดความต้องการที่ได้รับการยอมรับจากผู้ที่เกี่ยวข้องกับระบบและผู้พัฒนา ความต้องการความมั่นคงก็เป็นสิ่งสำคัญในการพิจารณาในกระบวนการวิศวกรรมความต้องการเช่นกัน เนื่องจากเป็นความต้องการที่เกี่ยวข้องกับการอยู่รอดของระบบ อย่างไรก็ตามการรวบรวมความต้องการความมั่นคงนั้นทำได้ยาก เนื่องจากจำเป็นต้องอาศัยผู้ชำนาญหรือมีประสบการณ์ด้านความมั่นคงในระบบ การนำความต้องการความมั่นคงสำหรับระบบเก่ามาประยุกต์ใช้นั้นสามารถทำได้ แต่ไม่สามารถรับรองได้ว่าความต้องการดังกล่าวมีจุดอ่อนหรือผลกระทบต่อความต้องการอื่นหรือไม่ ดังนั้นจึงมีแนวคิดที่จะนำแบบรูปความมั่นคงมาประยุกต์ใช้เพื่อแก้ปัญหาดังกล่าว

แบบรูปความมั่นคง เป็นแบบรูปที่นำเสนอผลเฉลยที่ได้รับการพิสูจน์แล้วว่าสามารถแก้ปัญหาความมั่นคงที่ปรากฏบ่อยครั้งได้ อย่างไรก็ตาม การนำแบบรูปความมั่นคงไปประยุกต์ใช้นั้นยังคงมีข้อจำกัดบางประการ เช่น ความรู้ความเข้าใจแบบรูปความมั่นคง ข้อจำกัดและเงื่อนไขบังคับสำหรับแต่ละแบบรูป ความสัมพันธ์ระหว่างแบบรูป เป็นต้น จึงจำเป็นต้องศึกษาและทำความเข้าใจทฤษฎีพื้นฐานด้านความมั่นคงและแบบรูปความมั่นคงก่อนจะนำไปประยุกต์ใช้ในกระบวนการความต้องการด้านความมั่นคงได้ จึงมีแนวคิดที่จะสร้างไวยากรณ์ความมั่นคงจากแบบรูปความมั่นคงเพื่อใช้ในการสร้างความต้องการความมั่นคง

การสร้างไวยากรณ์ความมั่นคงเกิดจากพิจารณาโครงสร้างแบบรูปความมั่นคงเพื่อวิเคราะห์หาองค์ประกอบสำคัญ และความสัมพันธ์ระหว่างองค์ประกอบที่ควรพิจารณาในแบบรูปเพื่อนำมาสร้างเป็นไวยากรณ์ความมั่นคงในรูปอีบีเอ็นเอฟ เนื่องจากอีบีเอ็นเอฟถือเป็นไวยากรณ์ไม่พึ่งบริบทที่สามารถอธิบายความหมายแบบเป็นทางการ ผลลัพธ์ของอีบีเอ็นเอฟจะอยู่ในลักษณะผลลัพธ์เชิงเส้น ซึ่งสามารถตรวจสอบความสมเหตุสมผลระหว่างไวยากรณ์ความมั่นคงและแบบรูปความมั่นคงได้

ในงานวิจัยนี้สร้างไวยากรณ์ความมั่นคงจากแบบรูปความมั่นคงจำนวน 20 แบบรูป ซึ่งครอบคลุม 4 กลุ่มแบบรูปความมั่นคง ได้แก่ การจัดการความมั่นคงองค์กรและการจัดการความ

เสี่ยง การระบุตัวตนและการพิสูจน์ตัวจริง แบบจำลองการควบคุมการเข้าถึง และสถาปัตยกรรมไฟล์วอลล์เนื่องจากแบบรูปดังกล่าวมีการนำไปประยุกต์ใช้ได้อย่างกว้างขวาง ความจำเป็นต่อการกำหนดความต้องการความมั่นคงพื้นฐานที่ทุกซอฟต์แวร์หรือทุกองค์กรต้องพิจารณาเป็นลำดับต้นๆ ผลลัพธ์ที่ได้คือ ไวยากรณ์ความมั่นคงในรูปอีบีเอ็นเอฟที่สอดคล้องกับแบบรูปความมั่นคงเดิม

อย่างไรก็ตามไวยากรณ์ความมั่นคงในรูปอีบีเอ็นเอฟ ยังคงมีข้อจำกัดในการนำไปใช้งานจริง เนื่องจากผู้ใช้จะต้องทำความเข้าใจไวยากรณ์ในรูปอีบีเอ็นเอฟเพิ่มเติม จึงได้สร้างเครื่องมือที่อยู่บนพื้นฐานของไวยากรณ์ความมั่นคงที่สร้างขึ้น โดยมีส่วนต่อประสานผู้ใช้ให้กับผู้ใช้เพื่อให้ใช้งานไวยากรณ์ได้อย่างสะดวกและรวดเร็วมากขึ้น

เครื่องมือที่สร้างขึ้นได้ผนวกเอาเงื่อนไขบังคับก่อนและหลังการใช้ไวยากรณ์ความมั่นคงเข้าไว้ด้วย เพื่อช่วยในกระบวนการตรวจสอบความถูกต้องและความสอดคล้องของความต้องการได้ และยังช่วยในการคำนวณค่าความเสี่ยงและแสดงผลในลักษณะความเสี่ยงเชิงคุณภาพ ช่วยให้ผู้ใช้สามารถทราบความเสี่ยงของแต่ละสินทรัพย์ และลำดับความสำคัญได้

เพื่อให้ทราบถึงประโยชน์จากการใช้งานไวยากรณ์ จึงได้ทำการทดสอบความสามารถในการใช้งานของเครื่องมือ โดยให้หน่วยทดลองกำหนดความต้องการโดยใช้มือสำหรับสถานการณ์จำลองที่ได้รับมอบหมาย ได้แก่ ระบบบริการเอฟทีพี ระบบสนับสนุนห้องปฏิบัติการ และระบบธนาคารออนไลน์ โดยจัดหน่วยทดลอง 12 คน ออกเป็น 3 กลุ่ม โดยให้ความสามารถเฉลี่ยของแต่ละกลุ่มเท่ากัน กำหนดความต้องการความมั่นคงให้กับระบบที่ได้รับหมอบหมายด้วยมือ แล้วจึงใช้เครื่องมือที่สร้างขึ้นในการกำหนดความต้องการความมั่นคงเป็นขั้นตอนต่อไป ภายหลังเสร็จสิ้นการทดลอง หน่วยทดลองจะให้ระดับความพึงพอใจต่อปัจจัยที่พิจารณาต่างๆ พร้อมกับแสดงข้อคิดเห็นหรือข้อเสนอแนะต่อการใช้งานเครื่องมือ

ผลจากการทดสอบความสามารถด้านการใช้งานเครื่องมือบนพื้นฐานไวยากรณ์ที่สร้างขึ้นสามารถสรุปตาม 4 กลุ่มปัจจัยที่พิจารณา ดังนี้

1) คุณภาพของความต้องการความมั่นคงเพิ่มขึ้นเมื่อใช้เครื่องมือในการสร้างความต้องการความมั่นคง

2) เครื่องมือช่วยให้ผู้ใช้เรียนรู้ว่า ถ้าจะกำหนดความต้องการความมั่นคงจะต้องมีองค์ประกอบใดบ้างที่ต้องพิจารณา ซึ่งจะช่วยลดระยะเวลาและไม่ต้องใช้ความพยายามมากในการกำหนดความต้องการความมั่นคง

3) เครื่องมือมีความสามารถในการตรวจสอบเงื่อนไขก่อนและหลังก่อนการใช้งาน และช่วยในการลำดับการกำหนดความต้องการความมั่นคง ส่งผลให้ความต้องการความมั่นคงดังกล่าวสามารถนำกลับมาใช้ใหม่ได้ ช่วยลดภาระการตรวจสอบความสอดคล้องของความต้องการความมั่นคงได้เป็นอย่างดี

4) เครื่องมือต้นแบบที่พัฒนาบนพื้นฐานของไวยากรณ์ความมั่นคงมีความเหมาะสมที่จะนำไปประยุกต์ใช้ในองค์กร เนื่องจากสามารถนำเครื่องมือต้นแบบนี้ในการกำหนดนโยบายความมั่นคงองค์กร หรือสร้างเป็นองค์ความรู้ความมั่นคงสำหรับองค์กรได้

ภายหลังการทดสอบได้มีการแสดงขั้นตอนการประยุกต์ใช้ไวยากรณ์ เพื่อแสดงให้เห็นว่าไวยากรณ์ผลลัพธ์ที่ได้จากเครื่องมือนั้น ใช้ไวยากรณ์ใด และมีขั้นตอนการสร้างความต้องการอย่างไร ผลการประยุกต์ใช้แสดงให้เห็นว่าไวยากรณ์ความมั่นคงจาก 20 แบบรูปความมั่นคง ถูกใช้งานทั้งหมด และความต้องการความมั่นคงที่เป็นผลลัพธ์จากเครื่องมือ มีความถูกต้องและครบถ้วนมากขึ้น หากพิจารณาความต้องการที่ได้จากเครื่องมือที่มีความผิดพลาดพบว่า ความผิดพลาดของความต้องการเกิดจากการป้อนข้อมูลผิดพลาดโดยผู้ใช้ หรือการป้อนข้อมูลที่ไม่สอดคล้องกับเขตข้อมูลที่กำหนดให้

เมื่อได้ความต้องการทั้งจากการกำหนดด้วยมือและด้วยเครื่องมือแล้ว จึงนำความต้องการทั้งสองมาเปรียบเทียบกันพบว่า ไวยากรณ์ความต้องการความมั่นคงสามารถผลิตความต้องการที่มีองค์ประกอบสำคัญครอบถ้วนตามแบบรูปความมั่นคง มากกว่าการกำหนดด้วยมือ อีกทั้งชุดผลลัพธ์ความต้องการมีความสอดคล้องและเป็นไปในทิศทางเดียวกัน

ผลลัพธ์จากงานวิจัยนี้ คือ ไวยากรณ์ความมั่นคงสำหรับสร้างความต้องการความมั่นคงที่มีองค์ประกอบสำคัญครบถ้วนตามที่เสนอไว้ในแบบรูปความมั่นคง และเครื่องมือสนับสนุนที่สามารถกำหนดความต้องการความมั่นคงได้อย่างมีประสิทธิภาพ รวดเร็ว สามารถนำผลลัพธ์มาสร้างเป็นองค์ความรู้ความมั่นคงสำหรับองค์กร และสนับสนุนการนำกลับมาใช้ใหม่ได้อีกด้วย

วิจัยนี้ได้รับการคัดเลือกตีพิมพ์ผลงานในวารสารวิชาการและการประชุมวิชาการทั้งในและต่างประเทศได้แก่

1) “The 4th International Joint Conference on Computer Science and Software Engineering (JCSSE 2007)” ในระหว่างวันที่ 2-4 พฤษภาคม พ.ศ. 2550 โดยมีหัวข้องานวิจัยชื่อ “An Approach: Constructing the Grammar from Security Pattern”

2) “The 14th Asia-Pacific Software Engineering Conference” ในระหว่างวันที่ 5-7 ธันวาคม พ.ศ.2550 โดยมีหัวข้องานวิจัยชื่อ “Enterprise Asset Security Requirements Construction from ESRMG Grammar based on Security Patterns”

รายละเอียดของงานวิจัยที่ได้รับการตีพิมพ์แสดงในภาคผนวก ช

8.2 แนวคิดในการพัฒนาต่อ

งานวิจัยนี้ได้สร้างไวยากรณ์ความมั่นคงจาก 20 แบบรูป ซึ่งจัดเป็น 4 กลุ่ม จากทั้งหมด 8 กลุ่มแบบรูปความมั่นคงที่นำเสนอไว้โดย Schumacher และคณะ ซึ่งเป็นแบบรูปที่ได้จากการ

ประชุมวิชาการโดยผู้เชี่ยวชาญด้านความมั่นคง และแบบรูปความมั่นคง ดังนั้นการขยายขอบเขตงานให้ครอบคลุมทั้ง 8 กลุ่มแบบรูปความมั่นคง ถือเป็นสิ่งที่มีความท้าทาย และช่วยให้ไวยากรณ์ความมั่นคงมีความสมบูรณ์แบบมากขึ้น ซึ่งมีประโยชน์อย่างมากต่อกระบวนการวิศวกรรมความต้องการ

รายการอ้างอิง

[1] ISO/IEC 9126: Product Quality Metrics.

[2] ISO/IEC 17799: Code of Practice for Information Security Management.

[3] E. Gamma, R. Helm, R. Johnson, and J. Vlissides. Design Patterns: Elements of Reusable Object-Oriented Software. Addison-Wesley, 1995.

[4] J. O. Coplien and D. C. Schmidt. Pattern Languages of Program Design. ACM Press/Addison-Wesley Publishing Co., 1995.

[5] M. Bishop. Introduction to Computer Security. Addision-Wesley, 2005.

[6] M. Schumacher, E. Fernandez-Buglioni, D.Hybertson, F. Buschmann and P. Sommerlad. Security Patterns: Integrating Security and Systems Engineering. John Wiley & Sons, 2005.

[7] S. Konrad, Betty and H.C. Cheng. Real-time Specification Pattern, Proceedings of the 27th International Conference on Software Engineering ICSE '05

[8] N. R. Mead, E. D. Hough and T. R. Stehney II. Building Trustworthy Applications: Security Quality Requirements Engineering (SQUARE) methodology, Proceedings of the 2005 Workshop on Software Engineering for Secure Systems SESS '05.

[9] A. V. Lamsweerde. Elaborating Security Requirements by Construction of Intentional Anti-Models, Proceedings of the 26th International Conference on Software Engineering

[10] A. Dennis, B. H. Wixom, and D. Tegarden. Systems Analysis and Design with UML Version 2.0: An Object-Oriented Approach 2nd edition, John Wiley & Sons, 2005.

[11] M. Shumacher. Security Engineering with Patterns. Spinger-Verlag Berlin HeidelBerg, 2002.

[12] E. Gramma, R. Helm, R. Johnson and J. Wlissides. Design Patterns Elements of Reusable Object-Oriented Software (7th Indian Reprint Edition). Pearson Education. 2002.

[13] E. Maiwald, and W. Sieglein. Security Planning & Disaster Recovery, P.82 – 89, McGraw-Hill/Osborne, 2002.

[14] C. B. Haley, J. D. Moffett, R. Laney, and B. Nuseibeh. Workshop papers: A Framework for Security Requirements Engineering, Proceedings of the 2006 international workshop on Software Engineering for secure systems SESS '06.

[15] T. Imamura, M. Tatsubori, Y. Nakamura, Christopher Giblin. Web Services Security Configuration in a Service-Oriented Architecture, ACM WWW 2005.

[16] S. W. Lee, R. Gandhi, D, Muthunrajan, D. Yavagal and G. J. Ahn. Building Problem Domain Ontology from Security Requirements in Regulatory Documents, Proceedings of the 2006 International workshop on Software engineering for secure systems SESS '06.

[17] D.G. Firesmith. Analyzing and Specifying Reusable Security Requirements, Journal of Object Technology, 2003: 56-86.

[18] E. Anderson, J Choobineh and M.R. Grimaila. An Enterprise Level Security Requirement Specification Model, Proceedings of the 38th Annual Hawaii International Conference, Page 186c – 186c, 2005.

[19] M. B. Dwyer, G. S. Avrunin, and J. C. Corbett. Patterns in property specifications for finite-state verification. Proceeding of the 21st International Conference on Software Engineering, pages 411-420. IEEE Computer Society Press, 1999.

[20] N. Peter (ed.), Revised Report on the Algorithmic Language ALGOL 60., Communications of the ACM, 3, 5(May 1960): 299-314.

[21] B. Cooper and P. Montague. Translation of Rights Expressions. 2005 Proceedings of the 2005 Australasian workshop on Grid computing and e-research - Volume 44 ACSW Frontiers '05.

[22] ISO/IEC14977:1996, Information technology-Syntactic metalanguage-Extended BNF, 1996.

ภาคผนวก

ภาคผนวก ก
องค์ประกอบของเอกสารแบบรูปความมั่นคงเทียบกับแบบรูปการออกแบบ

ตารางที่ ก.1 เปรียบเทียบองค์ประกอบของแบบรูปการออกแบบซอฟต์แวร์และแบบรูปความมั่นคง

ชื่อองค์ประกอบ	แบบรูปการออกแบบ	แบบรูปความมั่นคง	คำอธิบาย
ชื่อแบบรูป (Pattern name)	มี	มี	เป็นชื่อที่ตั้งขึ้นเพื่อให้สื่อถึงความสำคัญของแบบรูปนั้นอย่างตรงไปตรงมาตามวัตถุประสงค์ของแบบรูป
ชื่อที่รู้จัก (Also Known As)	มี	มี	ชื่ออื่นของแบบรูปที่เป็นที่รู้จักกัน
แรงบันดาลใจ (Motivate)	มี	ปัญหา (Problem)	สถานการณ์จำลองที่แสดงให้เห็นถึงปัญหาการออกแบบ และนำเสนอการกำหนดโครงสร้างของ อ็อบเจกต์เพื่อที่จะแก้ปัญหาดังกล่าวได้ ทำให้เข้าใจแบบรูปได้มากขึ้น
เจตนา (Intent)	มี	-	แสดงให้เห็นว่าแบบรูปนี้ทำอะไร มีเจตนาและเหตุผลใดที่ต้องใช้แบบรูป และแบบรูปเจาะจงในเรื่องใด
ผลที่ได้ (Consequence)	มี	มี	แบบรูปสนับสนุนวัตถุประสงค์ที่กำหนดได้อย่างไร และผลลัพธ์ที่ได้จากการใช้แบบรูปนี้
แบบรูปที่เกี่ยวข้อง (Related pattern)	มี	คล้ายกับ (See also)	แสดงถึงแบบรูปอื่นที่เกี่ยวข้อง หรือต้องพิจารณาร่วมกันเพื่อแก้ปัญหาใดปัญหาหนึ่ง
การนำไปใช้ที่ทราบ (Known Use)	มี	ตัวอย่าง (Example)	ตัวอย่างระบบจริงที่นำแบบรูปไปใช้ ซึ่งควรมีอย่างน้อย 2 โดเมนที่แตกต่างกัน
ตัวอย่างโปรแกรม (Sample Code)	มี	ผลเฉลย (Solution)	เป็นการแสดงส่วนของโปรแกรมหรือโค้ดโปรแกรม สำหรับแบบรูปความมั่นคงแสดงให้เห็นถึงผลลัพธ์จากแบบรูปที่ใช้ในการแก้ปัญหา

ตารางที่ ก.1 เปรียบเทียบองค์ประกอบของแบบรูปการออกแบบซอฟต์แวร์และแบบรูปความมั่นคง (ต่อ)

ชื่อองค์ประกอบ	แบบรูปการออกแบบ	แบบรูปความมั่นคง	คำอธิบาย
การนำไปปรับใช้ (Applicability)	มี	บริบท (Context)	ตัวอย่างสถานการณ์ที่นำแบบรูปไปใช้ เพื่อแสดงให้เห็นถึงการแก้ปัญหาการออกแบบที่ไม่เหมาะสม
การทำให้เกิดผล (Implementation)	มี	มี	พิจารณาถึงจุดอ่อน ผลกระทบ หรือเทคนิคที่ต้องทราบ เมื่อนำแบบรูปไปใช้
ลักษณะทางโครงสร้าง (Structure)	มี	มี	การนำเสนอแผนภาพคลาส (Class diagram) โดยใช้สัญลักษณ์โอเอ็มที (Object Modeling Technique:OMT) หรืออาจนำเสนอได้ในแผนภาพแสดงการโต้ตอบ (Interaction diagram)
สิ่งที่เข้ามาเกี่ยวข้อง (Participants)	มี	-	แสดงถึงคลาสหรืออ็อบเจกต์ที่เกี่ยวข้องในแบบรูป และแสดงให้เห็นถึงหน้าที่ของคลาสหรืออ็อบเจกต์ด้วย
การร่วมมือ (Collaboration)	มี	-	แสดงให้เห็นถึง สิ่งที่มาเกี่ยวข้อง (Participants) ว่ามีหน้าที่และความรับผิดชอบใดบ้าง
ไดนามิก (Dynamic)	-	มี	อธิบายพฤติกรรมของแบบรูปขณะรันไทม์ (Run-time)
ตัวอย่างการแก้ไข (Example Resolved)	-	มี	แสดงคุณลักษณะที่สำคัญในการแก้ปัญหาที่ยังไม่ครอบคลุมในผลเฉลย ลักษณะเชิงโครงสร้าง ไดนามิก และ การทำให้เกิดผล
รูปแปร (Variants)	-	มี	ข้อความอธิบายความแตกต่างหรือความเฉพาะเจาะจงของแบบรูป

ภาคผนวก ข
ไวยากรณ์ความมั่นคงจากแบบรูปความมั่นคง

ไวยากรณ์ที่สร้างจากแบบรูปความมั่นคงในขอบเขตงานวิจัยนี้ ประกอบด้วย 20 ไวยากรณ์จาก 20 แบบรูปความมั่นคง จาก 4 กลุ่มแบบรูปความมั่นคง ซึ่งสามารถจำแนกตามกลุ่มของแบบรูปความมั่นคงได้ดังนี้

กลุ่มที่ 1 การจัดการความมั่นคงองค์กรและการจัดการความเสี่ยง ประกอบด้วย

1) การระบุความต้องการความมั่นคงสำหรับสินทรัพย์องค์กร
2) การกำหนดมูลค่าสินทรัพย์
3) การประเมินภัยคุกคาม
4) การประเมินภาวะเสี่ยง
5) การกำหนดความค่าความเสี่ยง
6) แนวคิดความมั่นคงองค์กร
7) บริการความมั่นคงองค์กร
8) การสื่อสารของผู้มีหุ้นส่วนองค์กร

กลุ่มที่ 2 การระบุและการพิสูจน์ตัวตน ประกอบด้วย

1) ความต้องการการระบุและการพิสูจน์ตัวตน
2) ทางเลือกการออกแบบการระบุและการพิสูจน์ตัวตน
3) การออกแบบและใช้รหัสผ่าน
4) ทางเลือกการออกแบบชีวมิติ

กลุ่มที่ 3 การควบคุมการเข้าถึง ประกอบด้วย

1) การให้อำนาจ
2) การควบคุมการเข้าถึงเชิงบทบาท
3) ความมั่นคงหลายระดับ
4) การตรวจสอบการเข้าถึงทรัพยากร
5) การกำหนดสิทธิ์ให้กับบทบาท

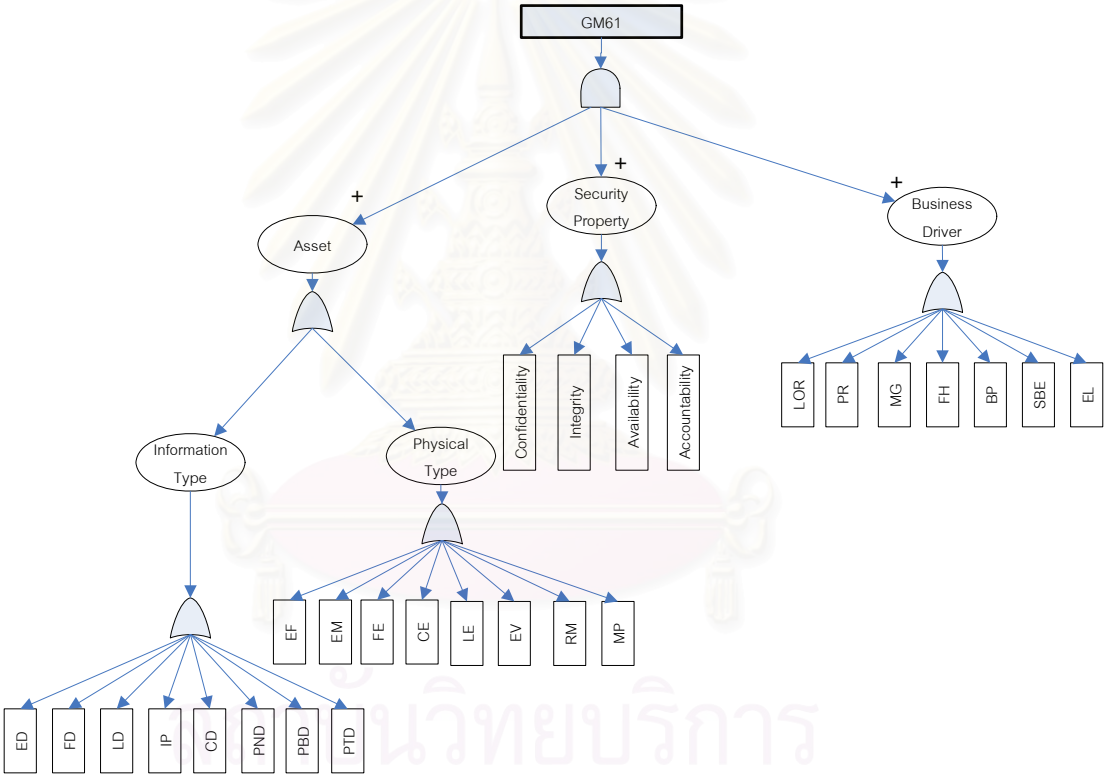
กลุ่มที่ 4 สถาปัตยกรรมไฟล์วอลล์ ประกอบด้วย

1) ไฟล์วอลล์กรองแพ็คเกจ
2) ไฟล์วอลล์เชิงตัวแทน
3) ไฟล์วอลล์เชิงสถานะ

เกณฑ์การตั้งรหัสไวยากรณ์นั้น จะขึ้นต้นด้วยคำว่า GM (Grammar) ตามด้วยรหัสตัวเลขจำนวน 2 ตัวสำหรับ 3 กลุ่มไวยากรณ์แรก โดยตัวเลขตัวแรกแสดงบทของกลุ่มเอกสารแบบรูปความมั่นคง และตัวเลขตัวที่ 2 แสดงตัวเลขสำหรับแบบรูปความมั่นคง ตัวอย่างเช่น GM61 หมายถึง ไวยากรณ์ความมั่นคงจากบทที่ 6 ข้อที่ 1 นั่นคือ แบบรูปการระบุความต้องการความมั่นคงสำหรับสินทรัพย์องค์กร สำหรับกลุ่มสถาปัตยกรรมไฟล์วอลล์ใช้ตัวเลข 3 หลัก โดย 2 ตัวแรกแสดงบทของกลุ่มเอกสารแบบรูปความมั่นคง และตัวที่ 3 แสดงตัวเลขสำหรับแบบรูปความมั่นคง ตัวอย่างเช่น GM121 หมายถึง ไวยากรณ์ความมั่นคงจากบทที่ 12 ข้อที่ 1 นั่นคือ แบบรูปไฟล์วอลล์กรองแพ็คเกจ โดยรายละเอียดแต่ละไวยากรณ์ที่สร้างขึ้นนั้น มีรายละเอียดดังต่อไปนี้

ตารางที่ ข.1 ไวยากรณ์การระบุความต้องการความมั่นคงสำหรับสินทรัพย์องค์กร

ชื่อไวยากรณ์	การระบุความต้องการความมั่นคง สำหรับสินทรัพย์องค์กร	**รหัสไวยากรณ์**	GM61
กลุ่มไวยากรณ์	การจัดการความมั่นคงองค์กรและการจัดการความเสี่ยง		
เงื่อนไขก่อนการใช้	ไม่มี		
คำอธิบาย	เป็นไวยากรณ์เริ่มต้นสำหรับการพิจารณาความมั่นคงองค์กร ซึ่งจะช่วยให้เข้าใจถึงความต้องการด้านความมั่นคงที่จะเป็นต้องมีในองค์กร เพื่อนำคุณสมบัติด้านความมั่นคง (การรักษาความลับ ความบูรณภาพ สภาพพร้อมใช้งาน และภาระรับผิดชอบ) มาประยุกต์ใช้		
แผนภาพต้นไม้ความมั่นคง			

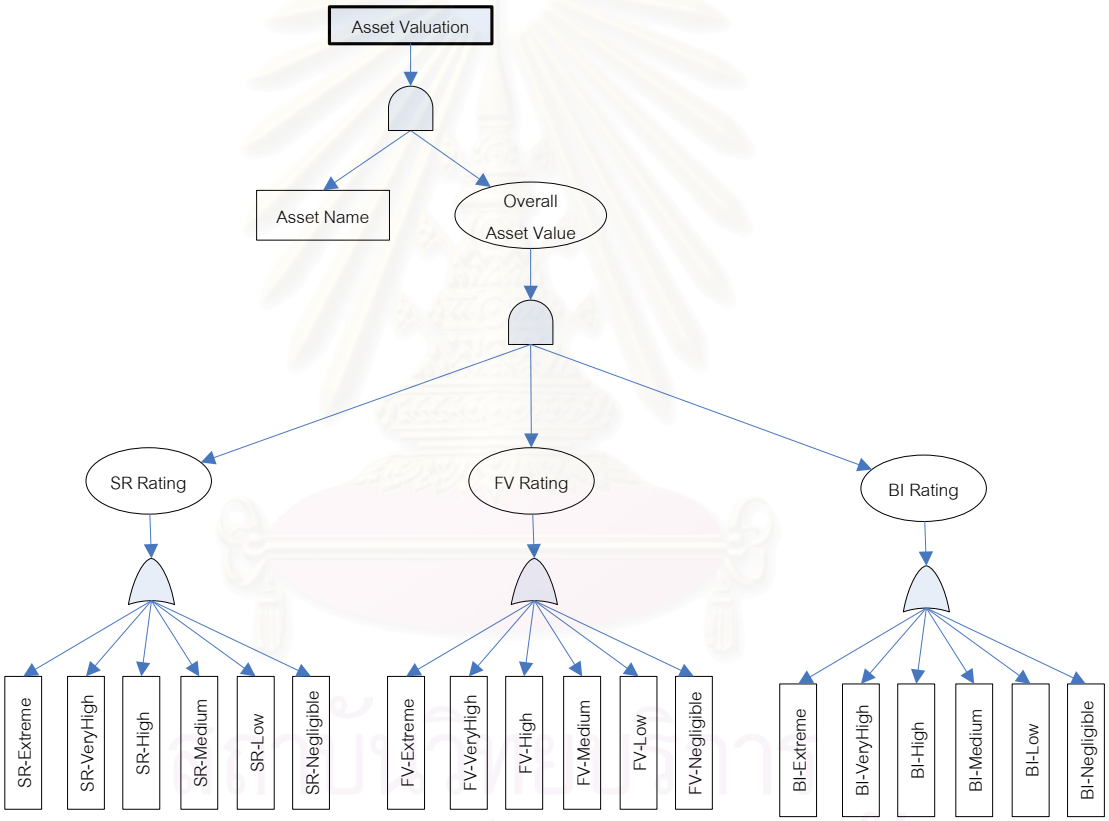


ตารางที่ ข.1 ไวยากรณ์การระบุความต้องการความมั่นคงสำหรับสินทรัพย์องค์กร (ต่อ)

ไวยากรณ์ความมั่นคง			
(1)	GM61	=	Asset-List , “require” , Security-Property-List , “under the auspices of”, Business-Driver-List , “.”;
(2)	Asset-List	=	Asset-Type , {“,” , Asset-Type } ;
(3)	Asset-Type	=	[Information-Type-List | Physical-Type-List | User-Type-List] ;
(4)	Information-Type-List	=	Information-Type , {“,” , Information-Type } ;
(5)	Information-Type	=	[“employee data” | “financial data” | “legal data” | “intellectual property” | “customer data” | “partner data” | “public data” | “protection data” | | Asset-Name] ;
(6)	Asset-Name	=	? User define an asset name ?
(7)	Physical-Type-List	=	Physical-Type , {“,” , Physical-Type } ;
(8)	Physical-Type	=	[“enterprise facility” | “enterprise employee” | “factory equipment” | “computer equipment” | “lab equipment” | “enterprise vehicles” | “raw material” | “manufactured product” | Asset-Name] ;
(9)	Security-Property-List	=	Security-Property , {“,” , Security-Property } ;
(10)	Security-Property	=	[“confidentially” | “integrity” | “availability” | “accountability”] ;
(11)	Business-Driver-List	=	Business-Driver , {“,” , Business-Driver } ;
(12)	Business-Driver	=	“laws or regulation” | “partner relations” | “mission and goals” | “financial health” | “business process” | “sensitive business event” | “enterprise location” | ? User business driver ? ;
(13)	User-Type-List	=	? User information item ? , { “,” , ? User information item ? } ;
ตัวอย่างความต้องการ			
Employee data, financial data require confidentially, integrity, accountability under the auspices of laws or regulation.			

ตารางที่ ข.2 ไวยากรณ์การกำหนดมูลค่าสินทรัพย์

ชื่อไวยากรณ์	การกำหนดมูลค่าสินทรัพย์	**รหัสไวยากรณ์**	GM62
กลุ่มไวยากรณ์	การจัดการความมั่นคงองค์กรและการจัดการความเสี่ยง		
เงื่อนไขก่อนการใช้	1. ซื้อสินทรัพย์ จาก GM61		
คำอธิบาย	การกำหนดมูลค่าสินทรัพย์จะช่วยให้สามารถกำหนดความสำคัญของสินทรัพย์ขององค์กรที่เป็นเจ้าของหรือควบคุมอยู่ เพื่อระบุว่าเมื่อเกิดความสูญเสียของสินทรัพย์จะกระทบต่อองค์กรในด้านใดบ้างและมีผลกระทบในระดับใด โดยมูลค่าสินทรัพย์จะได้จากการพิจารณาผลกระทบในด้านต่างๆ ต่อไปนี้ ได้แก่ ด้านความความต้องการความมั่นคง ด้านเศรษฐกิจ และทางด้านธุรกิจ		
แผนภาพต้นไม้ความมั่นคง			



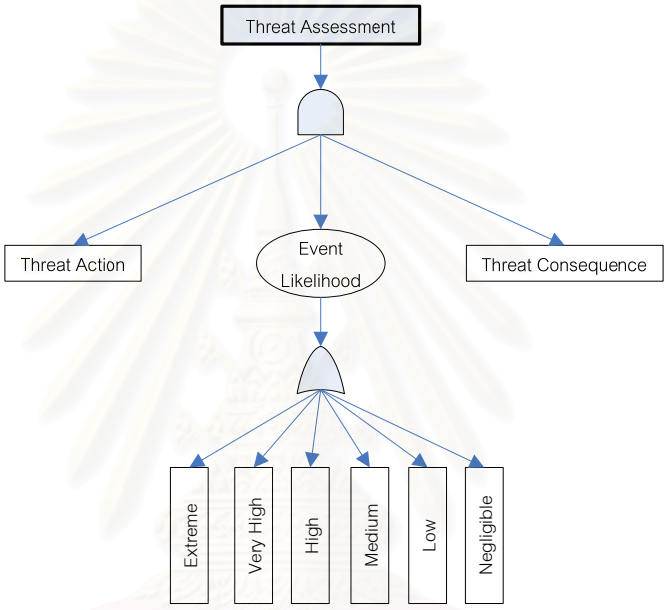
ตารางที่ ข.2 ไวยากรณ์การกำหนดมูลค่าสินทรัพย์ (ต่อ)

ไวยากรณ์ความมั่นคง			
(1)	Asset-Valuation	=	“The asset valuation of”, **Asset-Name**, “is” , **Rate-of-Security-Requirement**, **Rate-of-Financial-Value**, “and”, **Rate-of-Business-impact** , “So, overall impact value is” **Overall-Impact**, “.” ;
(2)	Asset-Name	=	? Name of asset from user ? ;
(3)	Rate-of-Security-Requirement	=	**Rating** , “in security requirement rating,” ;
(4)	Rate-of-Financial-Value	=	**Rating** , “in financial value rating” ;
(5)	Rate-of-Business-impact	=	**Rating** , “in business impact rating.” ;
(6)	Overall-Impact	=	**Rating** ;
(7)	Rating	=	[“extreme” | “very high” | “high” | “medium” | “low” | “negligible”] ;
ตัวอย่างความต้องการ			
The asset valuation of **museum employee data** is **very high** in security requirement rating, **medium** in financial value rating, and **very high** in business impact rating. So, overall impact value is **very high**.			

ตารางที่ ข.3 ไวยากรณ์การประเมินภัยคุกคาม

ชื่อไวยากรณ์	การประเมินภัยคุกคาม	**รหัสไวยากรณ์**	GM63
กลุ่มไวยากรณ์	การจัดการความมั่นคงองค์กรและการจัดการความเสี่ยง		
เงื่อนไขก่อนการใช้	1. ชื่อสินทรัพย์ จาก GM61		
คำอธิบาย	ภัยคุกคามเป็นโอกาสของอันตรายต่างๆ ที่อาจเกิดขึ้นและมีกระทบต่อสินทรัพย์องค์ ไวยากรณ์นี้จึงมีวัตถุประสงค์เพื่อกำหนดภัยคุกคาม ความถี่ของภัยคุกคามที่จะเกิดต่อสินทรัพย์ และผลกระทบเมื่อสินทรัพย์ถูกคุกคาม		

แผนภาพต้นไม้ความมั่นคง



ไวยากรณ์ความมั่นคง

(1) Threat-Assessment = “The likelihood of” , **Threat-Action** , “for” , **Asset-Name** , “is” , **Event-Likelihood** , “. Its’ consequence is” , **Threat-Consequence** , “.” ;

(2) Threat-Action = ? Name of threat action is input from user ? ;

(3) Asset-Name = ? The asset name from GM61 ? ;

(4) Event-Likelihood = [“extreme” | “very high” | “high” | “medium” | “low” | “negligible”] ;

(5) Threat-Consequence = ? The threat consequence sentence ? ;

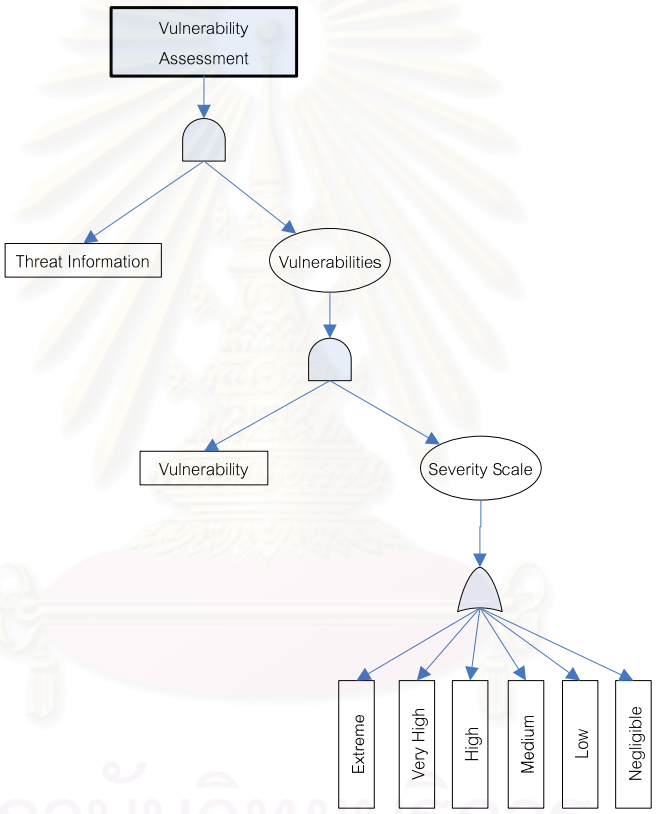
ตัวอย่างความต้องการ

The likelihood of **data entry error** for **museum employee data** is very high. Its’ consequence is **corruption of information assets.**

ตารางที่ ข.4 ไวยากรณ์การประเมินภาวะเสี่ยง

ชื่อไวยากรณ์	การประเมินภาวะเสี่ยง	**รหัสไวยากรณ์**	GM64
กลุ่มไวยากรณ์	การจัดการความมั่นคงองค์กรและการจัดการความเสี่ยง		
เงื่อนไขก่อนการใช้	1. ชื่อสินทรัพย์ จาก GM61 2. ชื่อภัยคุกคามสำหรับสินทรัพย์ในข้อ 1 ที่กำหนดไว้แล้วจาก GM63		
คำอธิบาย	จุดอ่อน (ภาวะไม่มั่นคง) เป็นจุดที่จะถูกใช้โดยภัยคุกคาม การประเมินภาวะจุดอ่อน คือ การระบุจุดอ่อนของสินทรัพย์ในองค์กร และระดับความรุนแรงเมื่อถูกภัยคุกคามโจมตีจุดอ่อนดังกล่าว		

แผนภาพต้นไม้ความมั่นคง



ไวยากรณ์ความมั่นคง

(1)	Vulnerability-Assessment	=	“The cause of” , **Threat-Information** , “is” , **Vulnerabilities**, “.” ;
(2)	Threat-Information	=	? Threat-Action from GM63 ? ;
(3)	Vulnerability	=	**Vulnerability-Action**, “which has” , **Severity-Scale**, “severity level” ;
(4)	Vulnerability-Action	=	? Name of the vulnerability action is input from user ? ;
(5)	Severity-Scale	=	[“extreme” | “very high” | “high” | “medium” | “low” | “negligible”] ;

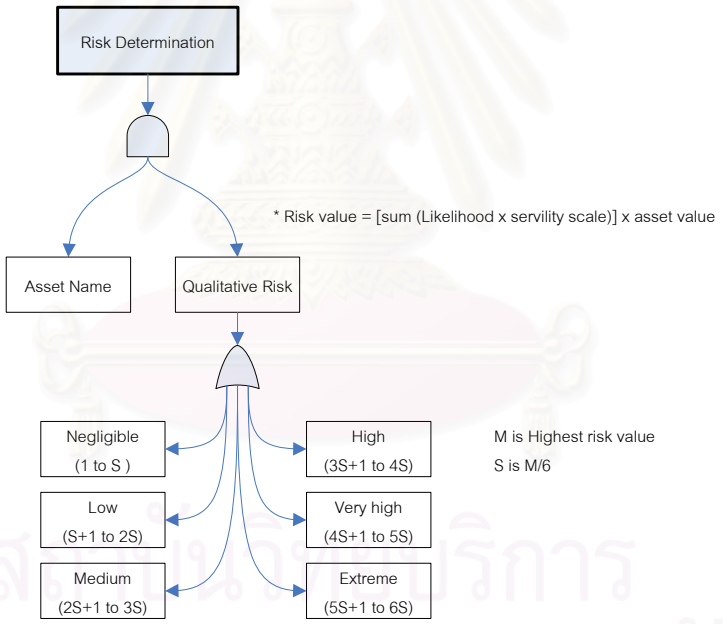
ตัวอย่างความต้องการ

The causes of museum fire are **failure of fire alarm system** which has **extreme** severity level, **failure of fire suppression system** which has **very high** severity level.

ตารางที่ ข.5 ไวยากรณ์การกำหนดค่าความเสี่ยง

ชื่อไวยากรณ์	การกำหนดค่าความเสี่ยง	**รหัสไวยากรณ์**	GM65
กลุ่มไวยากรณ์	การจัดการความมั่นคงองค์กรและการจัดการความเสี่ยง		
เงื่อนไขก่อนการใช้	1. ชื่อสินทรัพย์ จาก GM61 (เฉพาะที่ตัวที่กำหนดมูลค่าสินทรัพย์ ประเมินภัยคุกคาม และภาวะเสี่ยงแล้วเท่านั้น) 2. ความถี่ของการเกิดภัยคุกคามทุกตัวสำหรับสินทรัพย์ในข้อ 1 จาก GM63 3. ระดับความรุนแรงของภาวะเสี่ยงทุกตัวสำหรับภัยคุกคามในข้อ 2 จาก GM64 4. มูลค่าสินทรัพย์ในข้อ 1 จาก GM62		
คำอธิบาย	การกำหนดค่าความเสี่ยงเป็นขั้นตอนสุดท้ายของกระบวนการประเมินความเสี่ยง โดยการใช้ข้อมูลการประเมินมูลค่าสินทรัพย์ ภัยคุกคามและความถี่ที่เกิด ภาวะจุดอ่อนและระดับความรุนแรงมาใช้เป็นข้อมูลนำเข้า เพื่อนำมาคำนวณและแสดงผลเป็นระดับความเสี่ยงที่เหมาะสม ช่วยให้สามารถทราบความเสี่ยงของสินทรัพย์และจัดลำดับความสำคัญของสินทรัพย์ได้		

แผนภาพต้นไม้ความมั่นคง



ไวยากรณ์ความมั่นคง

(1) **Risk-Determination** = “The qualitative risk for” , **Asset-Name** , “is”, **Qualitative-Risk** , “.” ;

(2) **Asset-Name** = ? The asset name from GM61 ? ;

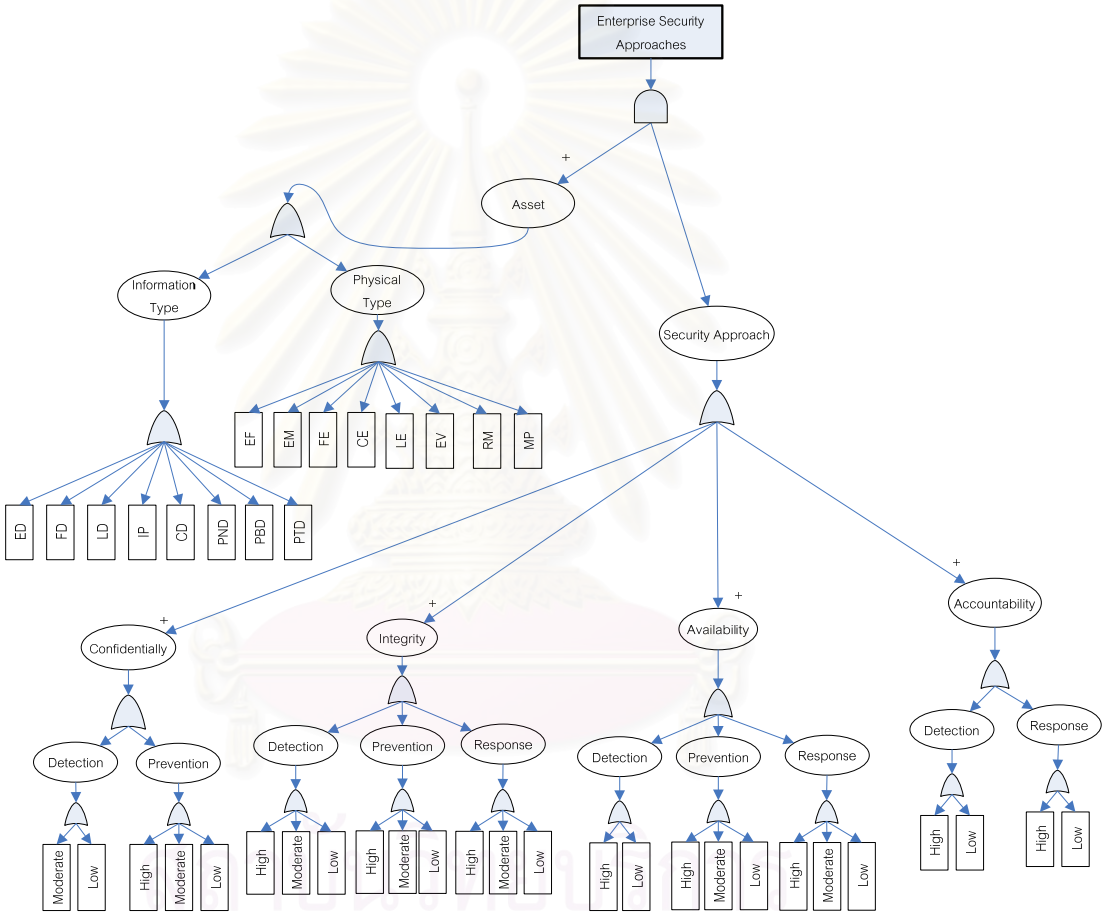
(3) **Qualitative-Risk** = [“negligible” | “low” | “medium” | “high” | “very high” | “extreme”] ;

ตัวอย่างความต้องการ

The qualitative risk for **museum collections and exhibits** are **extreme**.

ตารางที่ ข.6 ไวยากรณ์แนวคิดความมั่นคงองค์กร

ชื่อไวยากรณ์	แนวคิดความมั่นคงองค์กร	**รหัสไวยากรณ์**	GM66
กลุ่มไวยากรณ์	การจัดการความมั่นคงองค์กรและการจัดการความเสี่ยง		
เงื่อนไขก่อนการใช้	1. ชื่อสินทรัพย์ จาก GM61		
คำอธิบาย	ไวยากรณ์นี้จะช่วยเป็นตัวแนะนำในการเลือกแนวคิดความมั่นคง (การป้องกัน การตรวจหา และการตอบสนอง) ตามคุณสมบัติความมั่นคงที่เหมาะสม และระดับความเสี่ยงของสินทรัพย์ที่พิจารณา		
แผนภาพต้นไม้ความมั่นคง			



ตารางที่ ข.6 ไวยากรณ์แนวคิดความมั่นคงองค์กร (ต่อ)

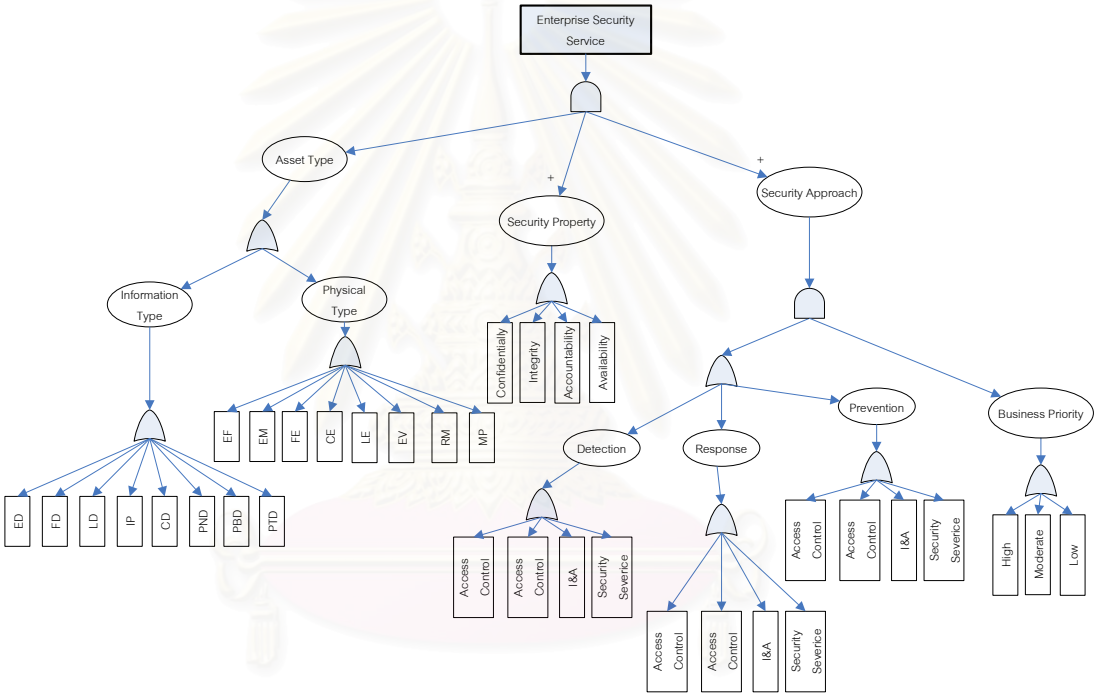
ไวยากรณ์ความมั่นคง			
(1)	Enterprise-Sec-Approach	=	“Protect”, [Confidentially | Integrity | Availability | Accountability] , “.” ;
(2)	Confidentially	=	“confidentially of” , Asset-List , [“require” | “requires”] , Confidentially-Level-List ;
(3)	Confidentially-Level-List	=	Confidentially-Level , { “,” , Confidentially-Level } ;
(4)	Confidentially-Level	=	[Confidentially-Level-of-Detection | Confidentially-Level-of-Prevention] ;
(5)	Confidentially-Level-of-Detection	=	[“moderate” | “low” , “ level of detection”] ;
(6)	Confidentially-Level-of-Prevention	=	Full-rating , “ level of prevention” ;
(7)	Integrity	=	“integrity of”, Asset-List, [“require” | “requires”] , Integrity-Level-List ;
(8)	Integrity-Level-List	=	Integrity-Level , { “,” , Integrity-Level } ;
(9)	Integrity-Level	=	[Integrity-Level-of-Detection | Integrity-Level-of-Prevention | Integrity-Level-of-Response];
(10)	Integrity-Level-of-Detection	=	Full-Rating, “ level of detection” ;
(11)	Integrity-Level-of-Prevention	=	Full-Rating, “ level of prevention” ;
(12)	Integrity-Level-of-Response	=	Full-Rating, “ level of response” ;
(13)	Availability	=	“availability of”, Asset-List, [“require” | “requires”] , Availability-Level-List ;
(14)	Availability-Level-List	=	Availability-Level , { “,” , Availability-Level } ;
(15)	Availability-Level	=	[Availability-Level-of-Detection | Availability-Level-of-Prevention | Availability-Level-of-Response] ;
(16)	Availability-Level-of-Detection	=	Full-Rating, “ level of detection” ;
(17)	Availability-Level-of-Prevention	=	Full-Rating, “ level of prevention” ;
(18)	Availability-Level-of-Response	=	Full-Rating, “ level of response” ;
(19)	Accountability	=	“accountability of” , Asset-List , [“require” | “requires”], Accountability-Level-List ;
(20)	Accountability-Level-List	=	Accountability-Level , { “,” , Accountability-Level } ;
(21)	Accountability-Level	=	[Accountability-Level-of-Detection | Accountability-Level-of-Response] ;
(22)	Accountability-Level-of-Detection	=	[“high” | “low”] , “level of detection” ;
(23)	Accountability-Level-of-Response	=	[“high” | “low”] , “level of response” ;
(24)	Asset-List	=	Asset , { “,” , Asset } ;
(25)	Asset	=	[Information-Type-List | Physical-Type-List];
(26)	Information-Type-List	=	Information-Type , {“,” , Information-Type } ;
(27)	Information-Type	=	[“employee data” | “financial data” | “legal data” | “intellectual property” | “customer data” | “partner data” | “public data” | “protection data” | ? Asset-Name from GM61 ?] ;
(28)	Physical-Type-List	=	Physical-Type , {“,” , Physical-Type } ;
(29)	Physical-Type	=	[“enterprise facility” | “enterprise employee” | “factory equipment” | “computer equipment” | “lab equipment” | “enterprise vehicles” | “raw material” | “manufactured product” | ? Asset-name from GM61 ?] ;
(30)	Full-Rating	=	[“high” | “medium” | “low”] ;

ตารางที่ ข.6 ไวยากรณ์แนวคิดความมั่นคงองค์กร (ต่อ)

ตัวอย่างความต้องการ
Protect **integrity** of **employee data**, **financial data** require **high** level of prevention, **high** level of detection, **high** level of response.

ตารางที่ ข.7 ไวยากรณ์การบริการความมั่นคงองค์กร

ชื่อไวยากรณ์	บริการความมั่นคงองค์กร	**รหัสไวยากรณ์**	GM67
กลุ่มไวยากรณ์	การจัดการความมั่นคงองค์กรและการจัดการความเสี่ยง		
เงื่อนไขก่อนการใช้	1. ชื่อสินทรัพย์ จาก GM61 (ในการพัฒนาจริงจะถูกผนวกรวมเข้ากับ GM66)		
คำอธิบาย	ไวยากรณ์นี้ต่อเนื่องจากไวยากรณ์ GM66 โดยไวยากรณ์นี้เป็นการแนะนำในการเลือกตัวบริการความมั่นคงที่จะใช้ในการป้องกันสินทรัพย์ภายหลังที่ได้กำหนดแนวคิดความมั่นคงสำหรับสินทรัพย์ดังกล่าวแล้ว ตัวอย่างบริการด้านความมั่นคง เช่น การระบุและยืนยันตัวตน (GM71) การควบคุมการเข้าถึง (GM82) เป็นต้น		
แผนภาพต้นไม้ความมั่นคง			

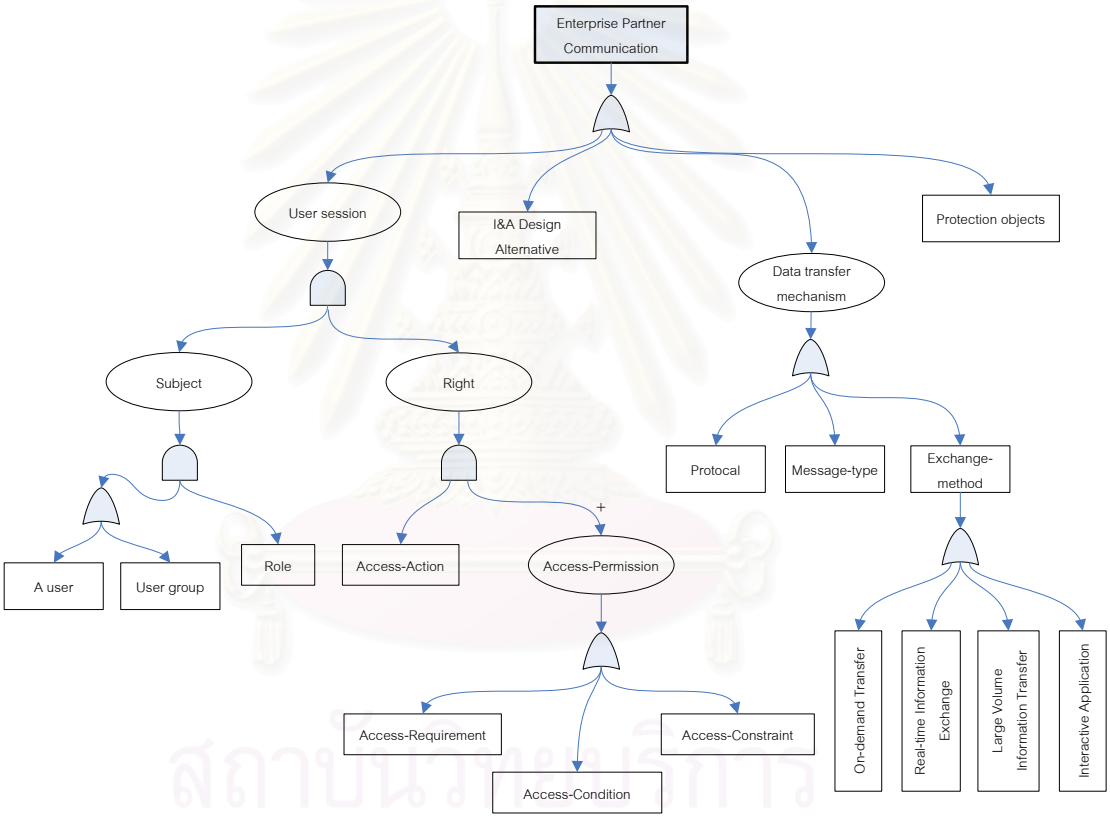


ตารางที่ ข.7 ไวยากรณ์การบริการความมั่นคงองค์กร (ต่อ)

ไวยากรณ์ความมั่นคง			
(1)	Enterprise-Security	=	Security-Property , “of” , Asset-List , [“require” | “requires”] , Security-Approach , “at” , Business-Priority, “level of business priority with following service:” , Selected-Service , “.” ;
(2)	Security-Property	=	[“confidentially” | “integrity” | “availability” | “accountability”] ;
(3)	Asset-List	=	Asset , {“,” , Asset }
(4)	Asset	=	[Information-Type-List | Physical-Type-List] ;
(5)	Information-Type-List	=	Information-Type , {“,” , Information-Type } ;
(6)	Information-Type	=	[“employee data” | “financial data” | “legal data” | “intellectual property” | “customer data” | “partner data” | “public data” | “protection data” | ? Asset-Name from GM61 ?] ;
(7)	Physical-Type-List	=	Physical-Type , {“,” , Physical-Type } ;
(8)	Physical-Type	=	[“enterprise facility” | “enterprise employee” | “factory equipment” | “computer equipment” | “lab equipment” | “enterprise vehicles” | “raw material” | “manufactured product” | ? Asset-Name from GM61 ?] ;
(9)	Security-Approach	=	[“prevention” | “detection” | “response”] ;
(10)	Business-Priority	=	[“high” | “moderate” | “low”] ;
(11)	Selected-Service	=	User-Define-Service | Default-Service ;
(12)	User-Define-Service	=	? The specified service name from user ?
(13)	Default-Service	=	[“I&A” | “accounting” | “access control” | “security management”] ;
ตัวอย่างความต้องการ			
Integrity of employee data requires prevention at high level of business priority with following service: I&A, access Control, accounting, security management.			

ตารางที่ ข.8 ไวยากรณ์การสื่อสารของผู้มีหุ้นส่วนองค์กร

ชื่อไวยากรณ์	การสื่อสารของผู้มีหุ้นส่วนองค์กร	**รหัสไวยากรณ์**	GM68
กลุ่มไวยากรณ์	การจัดการความมั่นคงองค์กรและการจัดการความเสี่ยง		
เงื่อนไขก่อนการใช้	1. ชื่อสินทรัพย์ จาก GM61 2. ชื่อบริการสำหรับระบุและยืนยันตัวตนจาก GM72		
คำอธิบาย	เมื่อองค์กรมีการติดต่อกับองค์กรภายนอก จะต้องมีการเตรียมเครื่องมือและบริการต่างๆ ไว้อำนวยความสะดวกและควบคุมการติดต่อและการแลกเปลี่ยนข้อมูล แต่การดำเนินการดังกล่าวจะต้องเลือกบริการความมั่นคงที่เหมาะสม ในการจัดการสิทธิ์การเข้าถึง รวมถึงการป้องกันข้อมูลมิให้ถูกเข้าถึงโดยผู้ที่ไม่มีสิทธิ์		
แผนภาพต้นไม้ความมั่นคง			



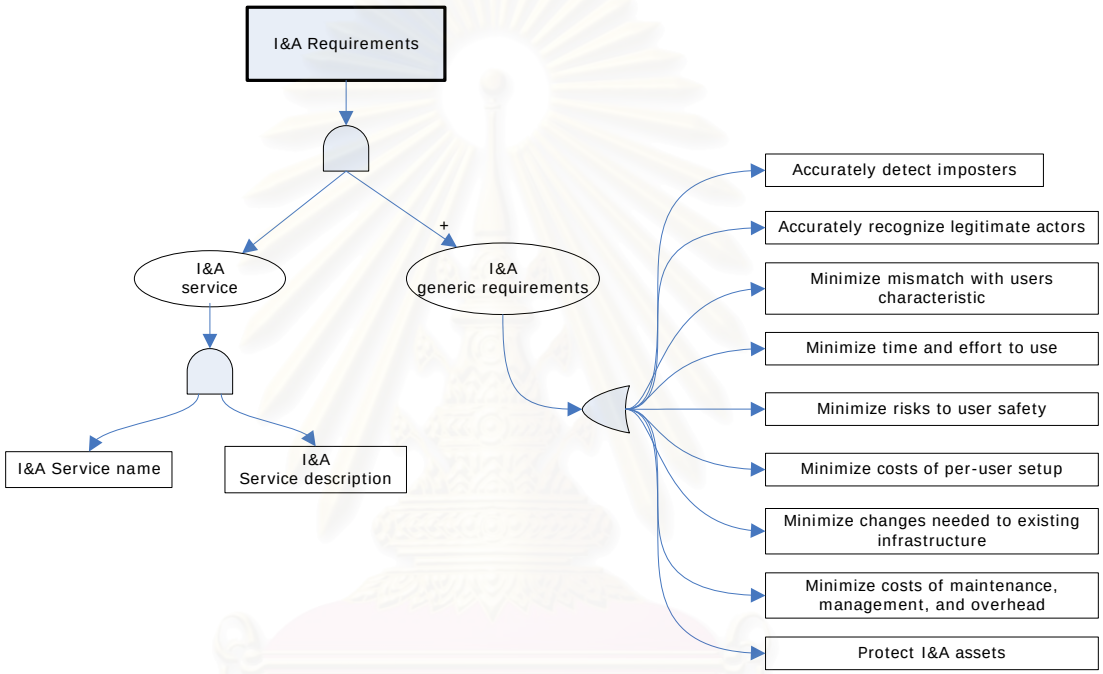
ตารางที่ ข.8 ไวยากรณ์การสื่อสารของผู้มีหุ้นส่วนองค์กร (ต่อ)

ไวยากรณ์ความมั่นคง			
(1)	EPC	=	Subject , Right , “access” , Protection-Object , Data-Transfer-Mechanism, [“for” , ? Access-Purpose ?] “.” This access requires I&A service named, ” , I&A-Name , “.” , [“Moreover” , Access-Permission , “.”] ,
(2)	Subject	=	[User | Group-User] , “, who acquire” , Role-Name , “,” ;
(3)	User	=	? The name that will access the service or data such as employee of business partner, contractors or third or forth parties. ? ;
(4)	Group-User	=	? The name of group that will access the service or data such as employee of business partner, contractors or third or forth parties. ? ;
(5)	Right	=	[“can” | “cannot”] , Access-Action , {“,” , Access-Action } ;
(6)	Protection-Object	=	? The asset or service or anything can be access by subject. ? ;
(7)	Role-Name	=	? The role which obtain one or more task for archive something ? ;
(8)	Access-Action	=	[“access” | “read” | “write” | “modify” | “delete” | ? user defined access-action ?] ;
(9)	Data-Transfer-Mechanism	=	[Protocol | Message-Type | Exchange-Method] ;
(10)	Protocol	=	“through” , Protocol-Name ;
(11)	Message-Type	=	“by using” , Message ;
(12)	Protocol-Name	=	? Specify protocol which use as a channel to exchange information such as HTTP, FTP ? ;
(13)	Message	=	? Type of message that will be exchange such as X.400 ? ;
(14)	Exchange-Method	=	[“On-demand transfer” | “Real-time information” | “Large volume information transfer” | “interaction application” | ? user defined method ?] ;
(15)	I&A-Name	=	? The name of I&A Design alternative which are define by GM72 ? ;
(16)	Access-Permission	=	Permission , { “,” , Permission };
(17)	Permission	=	[Requirement | Condition | Constraint] ;
(18)	Requirement	=	? The requirements which are considered before try to access ? ;
(10)	Condition	=	? The conditions which are consider before and/or after access the target ? ;
(20)	Constraint	=	? The conditions which are considered while access the target ? ;
ตัวอย่างความต้องการ			
The marketing of EST company, who acquire *ReaderRol*e, can access the database sever of MGT company by using X.400 message for retrieving and exchanging payment transaction. This access requires I&A service named, *IA-ExternalExchangePayment*. Moreover, this access can be schedule or automatic operations which define my system admin.			

ตารางที่ ข.9 ไวยากรณ์ความต้องการการระบุและการพิสูจน์ตัวตน

ชื่อไวยากรณ์	ความต้องการการระบุและการพิสูจน์ตัวตน	**รหัสไวยากรณ์**	GM71
กลุ่มไวยากรณ์	การระบุตัวตนและการพิสูจน์ตัวตน		
เงื่อนไขก่อนการใช้	ไม่มี		
คำอธิบาย	บริการด้านการระบุและพิสูจน์ตัวตนเป็นเซตของความต้องการสำหรับการบริการและคุณภาพของบริการ ไวยากรณ์นี้นำเสนอและสร้างความต้องการพื้นฐานสำหรับการบริการด้านการระบุและพิสูจน์ตัวตน		

แผนภาพต้นไม้ความมั่นคง



ไวยากรณ์ความมั่นคง

(1) I&A-Requirements = “The” , I&A-Service-Name, “ service for” , I&A-Service-Description , “shall” , I&A-Generic-Requirements-List , “by using” , I&A-Technique-List , “.” ;

(2) I&A-Service-Name = ? The name of service is an input from user ? ;

(3) I&A-Service-Description = ? The description of service is an input from user ? ;

(4) I&A-Generic-Requirements-List = I&A-Generic-Requirements , { “,” , I&A-Generic-Requirements } ;

(5) I&A-Generic-Requirements = [“accurately detect imposters” | “accurately recognize legitimate actors” | “minimize mismatch with user characteristics” | “minimize time and effort to use” | “minimize risks to user safety” | “minimize costs of per-user setup” | “minimize changes needed to existing infrastructure” | “minimize costs of maintenance, management, and overhead” | “protect I&A assets”] ;

(6) I&A-Technique-List = I&A-Technique , { “,” , I&A-Technique } ;

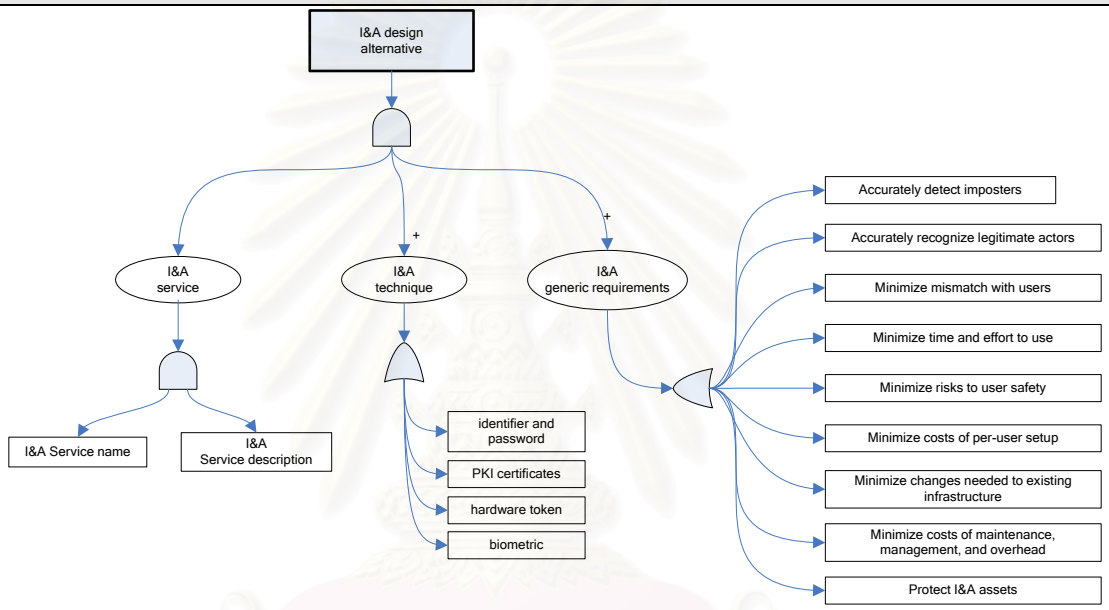
ตารางที่ ข.9 ไวยากรณ์ความต้องการการระบุและการพิสูจน์ตัวตน (ต่อ)

ตัวอย่างความต้องการ
The **client validation** service for **protection the bogus user to access the system** shall **accurately detect imposters, accurately recognize legitimate actors, and minimize time and effort to use**.

ตารางที่ ข.10 ไวยากรณ์ทางเลือกการออกแบบสำหรับการระบุและการพิสูจน์ตัวตนอัตโนมัติ

ชื่อไวยากรณ์	ทางเลือกการออกแบบสำหรับการระบุตัวตนและการพิสูจน์ตัวตนอัตโนมัติ	**รหัสไวยากรณ์**	GM72
กลุ่มไวยากรณ์	การระบุตัวตนและการพิสูจน์ตัวตน		
เงื่อนไขก่อนการใช้	1. ชื่อตัวบริการที่กำหนดไว้แล้ว จาก GM71		
คำอธิบาย	เป็นไวยากรณ์ที่ช่วยในการกำหนดเทคนิคที่จะใช้กับบริการการระบุและพิสูจน์ตัวตน เพื่อช่วยเลือกกลยุทธ์ที่เหมาะสม ให้สอดคล้องกับความต้องการด้านการระบุและพิสูจน์ตัวตน		

แผนภาพต้นไม้ความมั่นคง



ไวยากรณ์ความมั่นคง

(1) I&A-Requirements = “The” , **I&A-Service-Name**, “ service for” , **I&A-Service-Description** , “shall” , **I&A-Generic-Requirements-List** , “by using” , **I&A-Technique-list** , “.” ;

(2) I&A-Service-Name = ? The name of service is an input from user ? ;

(3) I&A-Service-Description = ? The description of service is an input from user ? ;

(4) I&A-Generic-Requirements-List = **I&A-Requirements** , { “,” , **I&A-Requirements** } ;

(5) I&A-Requirements = [“accurately detect imposters” | “accurately recognize legitimate actors” | “minimize mismatch with user characteristics” | “minimize time and effort to use” | “minimize risks to user safety” | “minimize costs of per-user setup” | “minimize changes needed to existing infrastructure” | “minimize costs of maintenance, management, and overhead” | “protect I&A assets”] ;

(6) I&A-Technique-List = **I&A-Technique** , { “,” , **I&A-Technique** } ;

(7) I&A-Technique = [“identifier and password” | “PKI certificates” | “biometric” | “hardware token”] ;

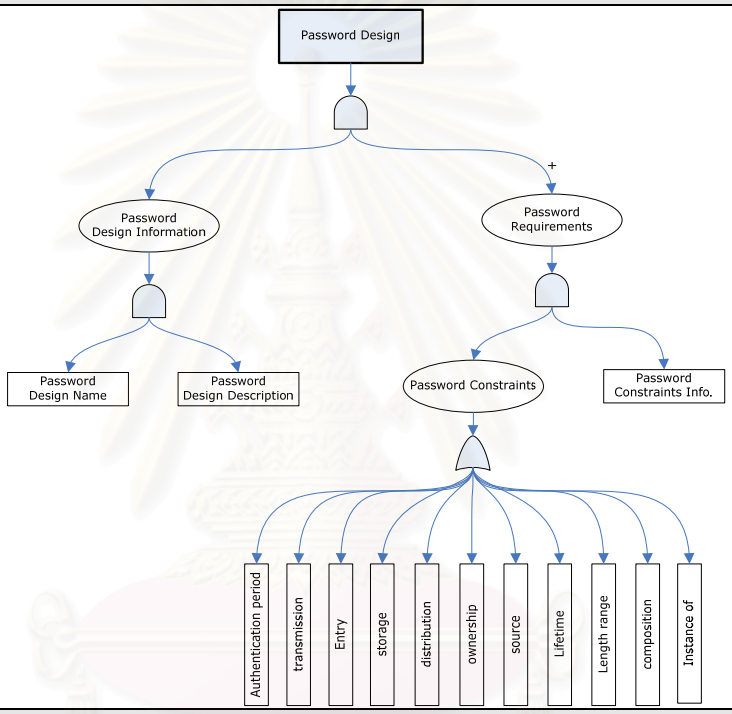
ตารางที่ ข.10 ไวยากรณ์ทางเลือกการออกแบบสำหรับการระบุและการพิสูจน์ตัวตนอัตโนมัติ (ต่อ)

ตัวอย่างความต้องการ
The **client validation** service for **protection the bogus user to access the system** shall **accurately detect imposters, accurately recognize legitimate actors, and minimize time and effort to use** by using **identifier and password and biometric.**

ตารางที่ ข.11 ไวยากรณ์การออกแบบและใช้รหัสผ่าน

ชื่อไวยากรณ์	การออกแบบและใช้รหัสผ่าน	**รหัสไวยากรณ์**	GM73
กลุ่มไวยากรณ์	การระบุตัวตนและการพิสูจน์ตัวตน		
เงื่อนไขก่อนการใช้	1. ชื่อตัวบริการที่กำหนดไว้แล้ว จาก GM71 2. ชื่อบริการที่ได้จากข้อ 1 จะต้องใช้ I&A Technique เป็น “Identifier and Password” ที่ถูกกำหนดโดย GM72		
คำอธิบาย	ไวยากรณ์นี้ใช้ในการออกแบบ การสร้าง และการจัดการการใช้รหัสผ่านสำหรับการบริการการระบุและพิสูจน์ตัวตน		

แผนภาพต้นไม้ความมั่นคง



ไวยากรณ์ความมั่นคง

(1) Password-Design = Password-Design-Information , “has value for each following factor: ” , Password-Requirements-List. , “.” ;

(2) Password-Design-Information = Password-Design-Name , “is a password system for” , Password-Design-Description ;

(3) Password-Design-Name = ? The name of the password design name is an input from user ? ;

(4) Password-Design-Description = ? The description of the password design name is an input from user ? ;

(5) Password-Requirements-List = Password-Requirements , { “,” Password-Requirements } ;

(6) Password-Requirements = Password-Constraints, “is” , Password-Constraints-Info. ;

(7) Password-Constraints = [“Instance of” | “composition” | “length range” | “lifetime” | “source” | “ownership” | “distribution” | “storage” | “entry” | “transmission” | “authentication period”] ;

(8) Password-Constraints-Info. = ? The information of password constraints is defined by user ? ;

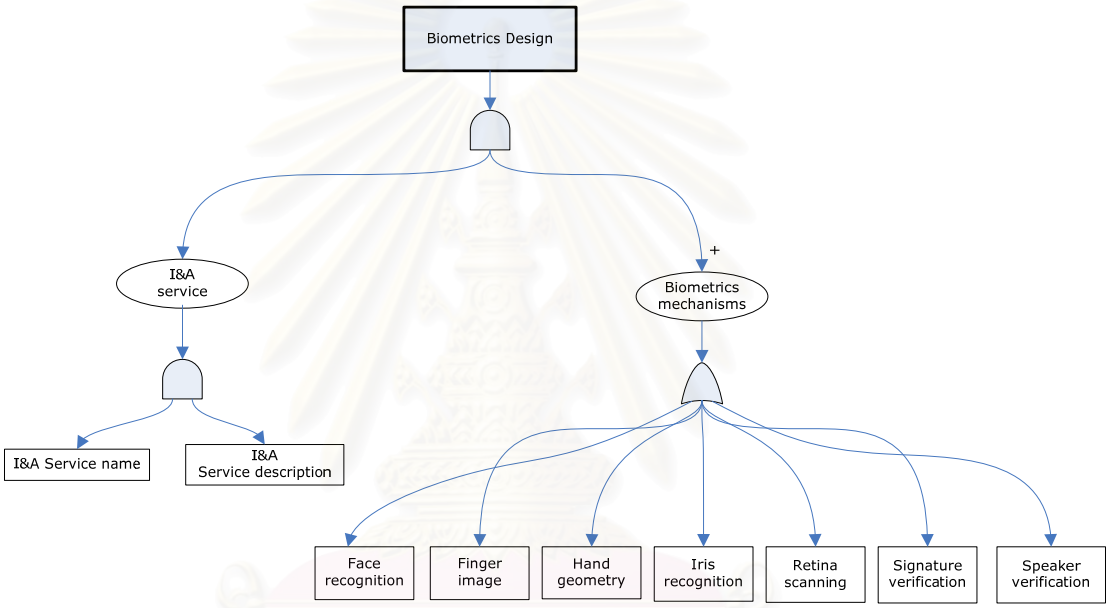
ตารางที่ ข.11 ไวยากรณ์การออกแบบและใช้รหัสผ่าน (ต่อ)

ตัวอย่างความต้องการ
Museum client validation is a password system for **access to museum intranet** has value for each following factor: Composition is **digit (0-9)**, length range is **4-6**, source is **user**, lifetime is **one year**, ownership is **individual (personal password)**, entry is **non-printing keypad**, **authorization period is each intranet session log-in, plus the end of each period of workstation inactivity that exceed thirty minutes**, distribution is **unmarked envelop by post**, storage is **central computer on-line storage as plaintext**, transmission is **plaintext**.

ตารางที่ ข.12 ไวยากรณ์ทางเลือกการออกแบบชีวมิติ

ชื่อไวยากรณ์	ทางเลือกการออกแบบชีวมิติ	**รหัสไวยากรณ์**	GM74
กลุ่มไวยากรณ์	การระบุตัวตนและการพิสูจน์ตัวตน		
เงื่อนไขก่อนการใช้	1. ชื่อตัวบริการที่กำหนดไว้แล้ว จาก GM71 2. ชื่อบริการที่ได้จากข้อ 1 จะต้องใช้ I&A Technique เป็น “Biometric” ที่ถูกกำหนดโดย GM72		
คำอธิบาย	ไวยากรณ์นี้ใช้ในการออกแบบ การสร้าง และการจัดการการใช้รหัสผ่านสำหรับการบริการการระบุและพิสูจน์ตัวตนโดยใช้วิธีการทางด้านชีวมิติ		

แผนภาพต้นไม้ความมั่นคง



ไวยากรณ์ความมั่นคง

(1) Biometrics-Design = “The” , **I&A-Service-Name**, “ service for” , **I&A-Service-Description** , “use following biometric approach: ” , **Biometric-Mechanisms-List** , “as I&A procedure.” ;

(2) I&A-Service-Name = ? The name of service defined by GM71 ? ;

(3) I&A-Service-Description = ? The description of service which defined by GM71 ? ;

(4) Biometric-Mechanisms-List = **Biometric-Mechanisms** , { “,” , **Biometric-Mechanisms** } ;

(5) Biometric-Mechanisms = [“face recognition” | “finger image” | “hand geometry” | “iris recognition” | “retina scanning” | “signature verification” | “speaker verification”] ;

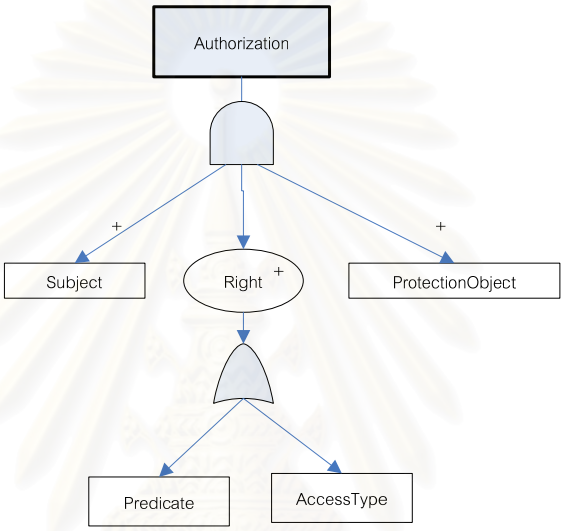
ตัวอย่างความต้องการ

The **client validation** service for **protection the bogus user to access the system** use following biometric approach: **hand geometry, finger image** as I&A procedure.

ตารางที่ ข.13 ไวยากรณ์การให้อำนาจ

ชื่อไวยากรณ์	การให้อำนาจ	**รหัสไวยากรณ์**	GM81
กลุ่มไวยากรณ์	การควบคุมการเข้าถึง		
เงื่อนไขก่อนการใช้	1. ข้อมูลสินทรัพย์จาก GM61		
คำอธิบาย	ไวยากรณ์นี้ช่วยในการกำหนดว่า ใครบ้างมิสิทธิ์ที่จะเข้าถึงทรัพยากรของระบบ ในสภาพแวดล้อมที่มีการควบคุมการเข้าถึง เพื่อแสดงให้เห็นว่าทรัพยากรใดถูกเข้าถึงและเข้าถึงได้อย่างไร		

แผนภาพต้นไม้ความมั่นคง



ไวยากรณ์ความมั่นคง

(1)	Authorization	=	Subject-List , Right-List , Protection-Object-List , “.” ;
(2)	Subject-List	=	Subject , { “,” , Subject } ;
(3)	Subject	=	? The name of subject is an input from user ? ;
(4)	Right-List	=	“can” | “cannot” , Right , { “,” , Right } ;
(5)	Right	=	Predicate | Access-Type ;
(6)	Predicate	=	? Predicate statement is defined by user ? ;
(7)	Access-Type	=	“read” | “write” | “modify” | “delete” | “create” ;
(8)	Protection-Object-List	=	Protection-Object , { “,” , Protection-Object } ;
(9)	Protection-Object	=	[? The name of protection-object is an input from user ? | ? Asset-Name from GM61 ?] ;

ตัวอย่างความต้องการ

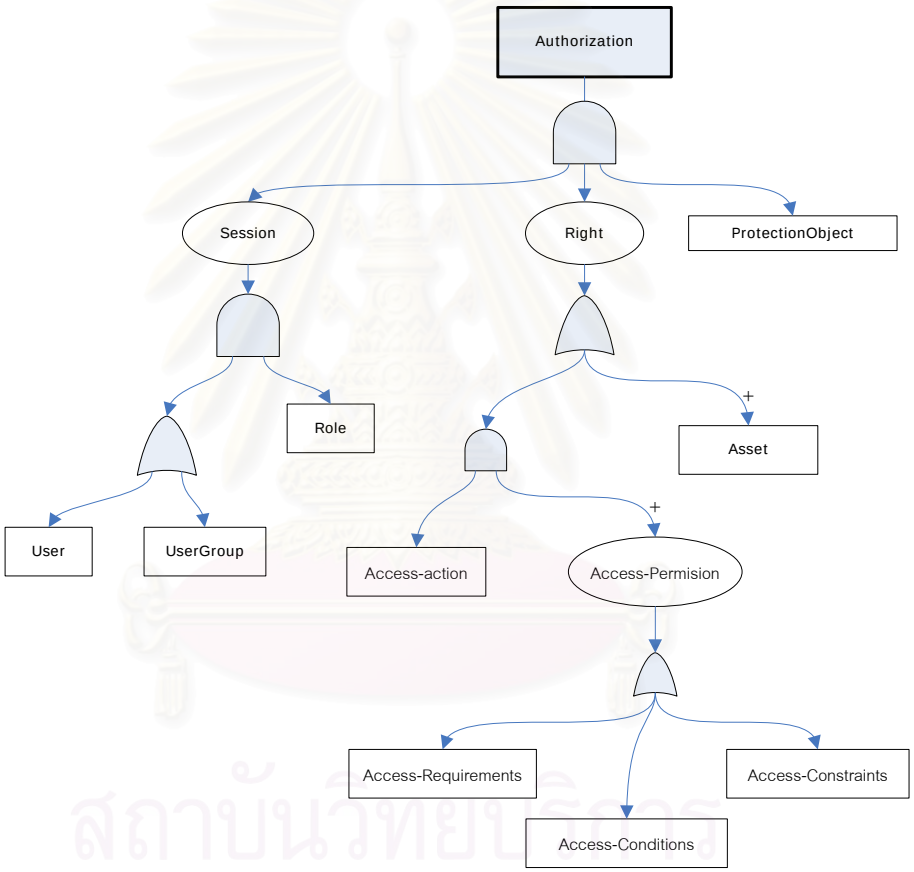
Doctor, nurse can read, modify, create the patient records.

Pharmacists cannot modify the patient records.

ตารางที่ ข.14 ไวยากรณ์การควบคุมการเข้าถึงเชิงบทบาท

ชื่อไวยากรณ์	การควบคุมการเข้าถึงเชิงบทบาท	**รหัสไวยากรณ์**	GM82
กลุ่มไวยากรณ์	การควบคุมการเข้าถึง		
เงื่อนไขก่อนการใช้	1. ข้อมูลสินทรัพย์จาก GM61 คำแนะนำ : ไวยากรณ์นี้เป็นส่วนขยายของ GM81		
คำอธิบาย	ไวยาการณ์นี้ใช้ในการกำหนดสิทธิ์บนพื้นฐานของบทบาทที่บุคคลได้รับ เพื่อใช้ในการควบคุมการเข้าถึง ซึ่งเพิ่มจาก GM81 โดยมีการนำเสนอกลุ่มบุคคล ประเภทข้อมูล และการดำเนินการที่บุคคลสามารถทำได้กับทรัพยากรที่ต้องการเข้าถึง		

แผนภาพต้นไม้ความมั่นคง



ตารางที่ ข.14 ไวยากรณ์การควบคุมการเข้าถึงเชิงบทบาท (ต่อ)

ไวยากรณ์ความมั่นคง

(1)	Role-Base-Authorization	=	Sessiont-List , Right-Info , Protection-Object , “.” ;
(2)	Session-List	=	Session , { “,” , Session } , “who obtain” , Role-Name ;
(3)	Session	=	[User-Group-List | User-List] ;
(4)	User-Group-List	=	User-Group , { “,” , User-Group } ;
(5)	User-Group	=	? The name of the user group is an input from user ? , “group” ;
(6)	User-List	=	User , { “,” , User } ;
(7)	User	=	? The name of the user is an input from user ? ;
(8)	Role-Name	=	? Role name from GM85 ? ;
(9)	Right-Info	=	Right , Access-Permission , [Asset-Name];
(10)	Right	=	[“can” | “cannot”] , Access-action , {“,” , Access-action } ;
(11)	Access-Action	=	[“access” | “read” | “write” | “modify” | “delete” | ? user defined access-action ?] ;
(12)	Access-Permission	=	[Requirements | Conditions | Constraints] ;
(13)	Requirements	=	? The information of right’s requirement is an input from user ? ;
(14)	Conditions	=	? The information of right’s conditions an input from user ? ;
(15)	Constraints	=	? The information of right’s constraints is an input from user ? ;
(16)	Asset-Name	=	[? The information of the required asset for right information is an input from user ? | ? Asset-Name from GM61 ?] (* this occur when the asset is required to achieve the access action *);
(17)	Protection-Object	=	[? The name of protection-object is an input from user ? | ? Asset from GM61) ?] ;

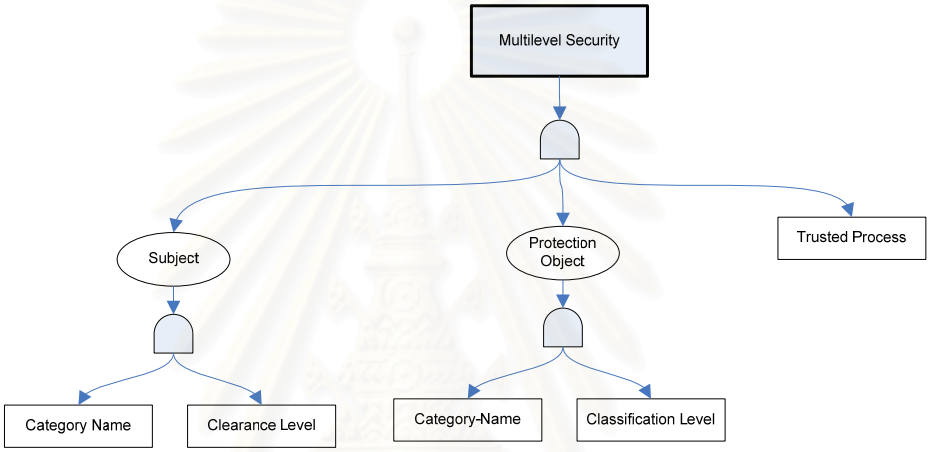
ตัวอย่างความต้องการ

- Doctor group, nurse group who obtain modify role *can read, modify and create report for* their patient record.
- Pharmacists group who obtain read role *can read and create report only of* patient record.
- ATM user group who obtain full operation role *can transfer some money into other account with fee to* difference account bank.

ตารางที่ ข.15 ไวยากรณ์ความมั่นคงหลายระดับ

ชื่อไวยากรณ์	ความมั่นคงหลายระดับ	**รหัสไวยากรณ์**	GM83
กลุ่มไวยากรณ์	การควบคุมการเข้าถึง		
เงื่อนไขก่อนการใช้	1. ข้อมูลสินทรัพย์จาก GM61		
คำอธิบาย	ในบางกรณีที่ข้อมูลหรือเอกสารมีระดับความสำคัญที่แตกต่างกันออกไป ไวยากรณ์นี้จะช่วยในการกำหนดระดับหรือกลุ่มของทรัพยากร และกำหนดระดับสิทธิ์ให้กับผู้ใช้ที่เข้ามาติดต่อทรัพยากรดังกล่าว เพื่อใช้ในการตรวจสอบการเข้าถึงว่าผู้ใช้มีระดับสิทธิ์มากพอที่จะเข้าถึงทรัพยากรดังกล่าวหรือไม่		

แผนภาพต้นไม้ความมั่นคง



ไวยากรณ์ความมั่นคง

(1) Multilevel-Security = Subject , “can access” , Protection-Object, “by” Trusted-Process .

(2) Subject = Category-Name , { “,” , Category-Name } , “which has a ” , Clearance-Level , “clearance level”;

(3) Category-Name = ? The name of category is an input from user ? ;

(4) Clearance-Level = ? The level of clearance is an input from user ? ;
(* in real case, we don’t have any detailed information of clearance level *)

(5) Protection-Object = Category-Name , { “,” , Category-Name } , “which has a ”, Classification-Level , “classification level”;

(6) Trusted-Process = ? The name of trusted process is an input from user ? ;

(7) Clearance-Level = Quality-Scale ;

(8) Classification-Level = Quality-Scale ;

(9) Quality-Scale = [“extreme” | “very high” | “high” | “low” | “negligible”] ;

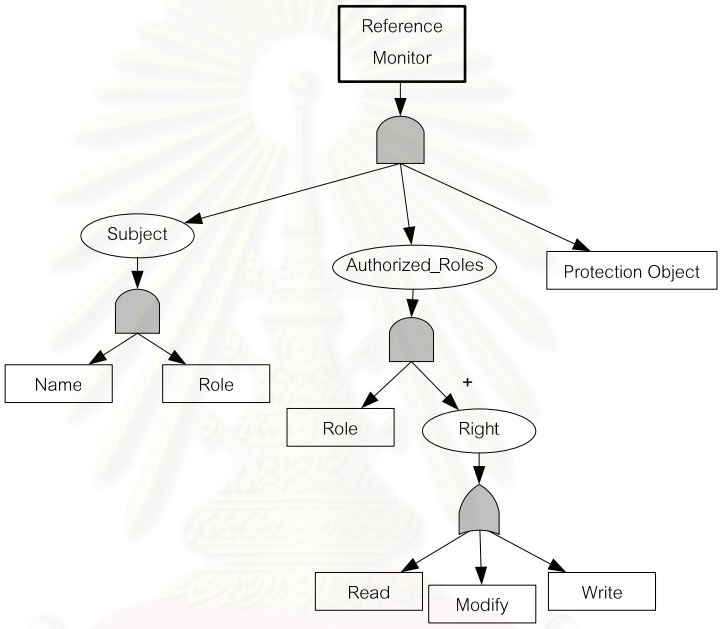
ตัวอย่างความต้องการ

Medical soldier which has a **high** clearance level can access **the biometric laboratory** which has a **high** classification level by **using personal secured card**.

ตารางที่ ข.16 ไวยากรณ์การตรวจสอบการเข้าถึงทรัพยากร

ชื่อไวยากรณ์	การตรวจสอบการเข้าถึงทรัพยากร	**รหัสไวยากรณ์**	GM84
กลุ่มไวยากรณ์	การควบคุมการเข้าถึง		
เงื่อนไขก่อนการใช้	1. ข้อมูลการดำเนินงาน (Task) สำหรับบทบาทจาก GM85		
คำอธิบาย	ไวยากรณ์นี้ใช้ในการกำหนดข้อบังคับในการใช้งานทรัพยากรเป้าหมาย ว่าคำร้องขอเข้าใช้ทรัพยากรนั้นสามารถทำได้หรือไม่ โดยการตรวจสอบกับเซตของบทบาทที่ได้รับอนุญาต และสิทธิ์สำหรับบทบาทดังกล่าว		

แผนภาพต้นไม้ความมั่นคง



ไวยากรณ์ความมั่นคง

(1)	Ref-Monitor	=	**Subject** , **Authorized-Roles** , **Protection-Object** , “.” ;
(2)	Subject	=	**Subject-Name** , “, who acquire”, **Role-Name** , “ role, ” ;
(3)	Subject-Name	=	? The name of subject such as person or process ? ;
(4)	Role-Name	=	? The defined role in organization based on its policy ? ;
(5)	Authorized-Roles	=	“is authorized to” , **Right-List** ;
(6)	Right-List	=	**Right** , {“,” **Right**} ;
(7)	Right	=	[“read” | “write” | “modify” | **User-Define-Right**] ; (* users can define a new right by themselves. This feature is supported by the prototyping tool *)
(8)	User-Define-Right	=	? A new right which defined by user ? ;
(9)	Protection-Object	=	? Asset-Name from GM61 ? ;

ตัวอย่างความต้องการ

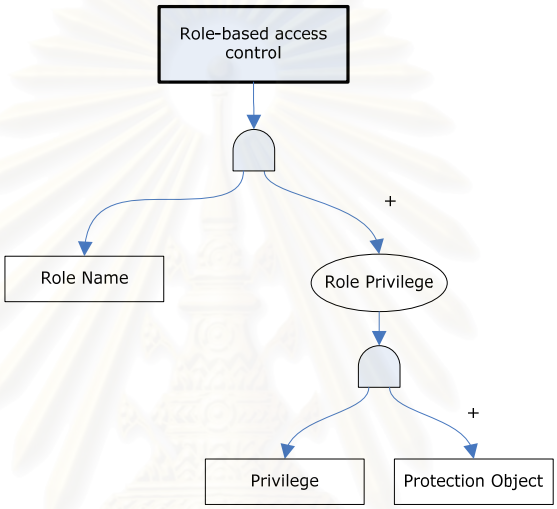
Somsak, who acquire doctor role, is authorized to read, modify patient records.

Somsri, who acquire nurse role, is authorized to read the medical orders.

ตารางที่ ข.17 ไวยากรณ์การกำหนดสิทธิ์ให้กับบทบาท

ชื่อไวยากรณ์	การกำหนดสิทธิ์ให้กับบทบาท	**รหัสไวยากรณ์**	GM85
กลุ่มไวยากรณ์	การควบคุมการเข้าถึง		
เงื่อนไขก่อนการใช้	ไม่มี		
คำอธิบาย	ไวยากรณ์นี้สนับสนุนแนวคิดการให้สิทธิ์ต่ำสุด เป็นหลักการพื้นฐานสำหรับระบบความมั่นคง แต่จะต้องมีการกำหนดสิทธ์ให้กับบทบาท เพื่อให้ทราบว่าบทบาทนี้มีสิทธิ์ในการดำเนินการอะไรกับทรัพยากรใดได้บ้าง		

แผนภาพต้นไม้ความมั่นคง



ไวยากรณ์ความมั่นคง

(1) Role-Based-Access = Role-name, Role-Privilege , “.” ;

(2) Role-Name = ? The name of role is an input from user ? , “role” ;

(3) Role-Privilege = “can perform following tasks: ” , Privilege-List;

(4) Privilege-List = Privilege , { “,” , Privilege } ;

(5) Privilege = ? The information of privilege is an input from user ? ;

(6) Protection-Object-List = Protection-Object , { “,” , Protection-Object } ;

(7) Protection-Object = [? The name of protection-object is an input from user ? |
? Asset-Name from GM61 ?];

ตัวอย่างความต้องการ

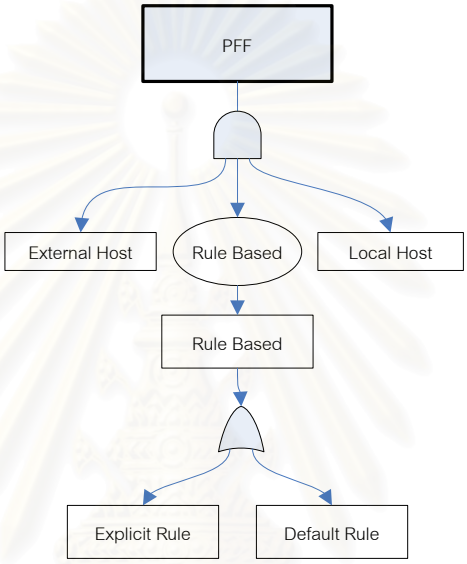
Manager role can perform following tasks: manage items, order items for digital item management system.

Salesperson role can perform following tasks: order items, register, bill for items, manage item catalog for a digital item management system.

ตารางที่ ข.18 ไวยากรณ์ไฟล์วอลล์กรองแพ็คเกจ

ชื่อไวยากรณ์	ไฟล์วอลล์กรองแพ็คเกจ	**รหัสไวยากรณ์**	GM121
กลุ่มไวยากรณ์	สถาปัตยกรรมไฟล์วอลล์		
เงื่อนไขก่อนการใช้	ไม่มี		
คำอธิบาย	ไวยากรณ์นี้ใช้ในการระบุโฮสต์ (Host) เพื่อทำการปิดกั้นหรืออนุญาตให้ผ่านไฟล์วอลล์ในระดับไอพี (IP Level)		

แผนภาพต้นไม้ความมั่นคง



ไวยากรณ์ความมั่นคง

(1) PFF = "The request from" , **External-Host** , ["is" | "are"] , **Rule-Base-List** , "to access" , **Local-Host** , "." ;

(2) External-Host = ? Host name or IP address ? ;

(3) Rule-Based-List = **Rule-Based** , { "," , **Rule-Based** } ;

(4) Rule-Base = [**Explicit-Rule** | **Default-Rule**] ;

(5) Explicit-Rule = ? Specific rule with clear and extract ? ;

(6) Default-Rule = ["permitted" | "denied" | ? User default rule ?];

(7) External-Host-List = **External-Host** , { "," , **External-Host** } ;

(8) Local-Host = ? A host name or IP address ? ;

ตัวอย่างความต้องการ

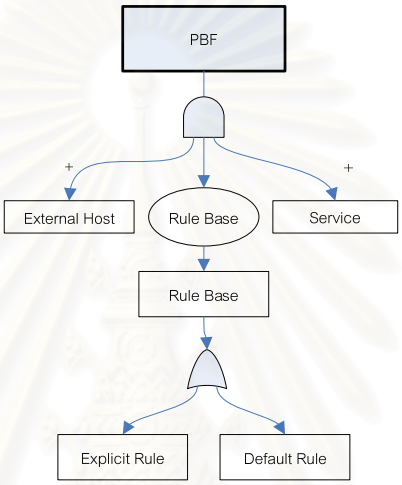
The requests from **192.22.4.4** are **permitted** to access **192.200.17.1**.

The request from **TC-HOST-NAME** is **denied** to access **SV-HOST**.

ตารางที่ ข.19 ไวยากรณ์ไฟล์วอลล์เชิงตัวแทน

ชื่อไวยากรณ์	ไฟล์วอลล์เชิงตัวแทน	**รหัสไวยากรณ์**	GM122
กลุ่มไวยากรณ์	สถาปัตยกรรมไฟล์วอลล์		
เงื่อนไขก่อนการใช้	ไม่มี		
คำอธิบาย	ไวยากรณ์นี้ใช้ในการระบุโฮสต์ เพื่อทำการปิดกั้นหรืออนุญาตให้ผ่านไฟล์วอลล์ในระดับไอพี โดยพิจารณาชื่อบริการ (Service Name) และ พอร์ต (Port)โดยมีตรวจสอบร่วมกับกฎที่ถูกกำหนดไว้		

แผนภาพต้นไม้ความมั่นคง



ไวยากรณ์ความมั่นคง

(1)	PBF	=	“The request from” , **External-Host** , [“is” | “are”] , **Rule-Base-List** , “to access” , **Service** , “.” ;
(2)	External-Host	=	? Host name or IP address ? ;
(3)	Rule-Based-List	=	**Rule-Based** , { “,” , **Rule-Based** } ;
(4)	Rule-Base	=	[**Explicit-Rule** | **Default-Rule**];
(5)	Explicit-Rule	=	? Specific rule with clear and extract ? ;
(6)	Default-Rule	=	[“permitted” | “denied” | ? User default rule ?] ;
(7)	External-Host-List	=	**External-Host** , { “,” , **External-Host** } ;
(8)	Service	=	? Service name ? , { “on” , ? or Protocol or Port ? } ;

ตัวอย่างความต้องการ

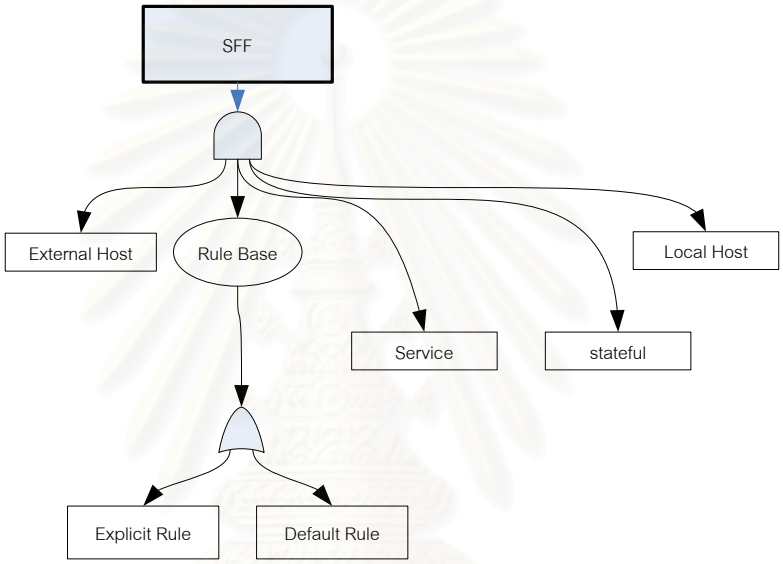
The requests from **192.22.4.4** are **permitted** to access **mail service** on **port 8080**.

The request from **255.200.3.127** is **denied** to access **ftp service**.

ตารางที่ ข.20 ไวยากรณ์ไฟล์วอลล์เชิงสถานะ

ชื่อไวยากรณ์	ไฟล์วอลล์เชิงสถานะ	**รหัสไวยากรณ์**	GM123
กลุ่มไวยากรณ์	สถาปัตยกรรมไฟล์วอลล์		
เงื่อนไขก่อนการใช้	ไม่มี		
คำอธิบาย	ไวยากรณ์นี้ใช้ในการระบุโฮสต์ เพื่อทำการปิดกั้นหรืออนุญาตให้ผ่านไฟล์วอลล์ในระดับไอพี โดยพิจารณาชื่อบริการและ พอร์ต โดยมีตรวจสอบสถานะของการเข้าถึงและกฎที่กำหนดไว้ในไฟล์วอลล์		

แผนภาพต้นไม้ความมั่นคง



ไวยากรณ์ความมั่นคง

(1) SFF = "The request from" , **External-host** , ["is" | "are"] , **Rule-base-list** , "to access" , **Service** , "while" , **Stateful** , "." ;

(2) External-host = ? Host name or IP address ? ;

(3) Rule-based-list = **Rule-based** , { "," , **Rule-based** } ;

(4) Rule-base = [**Explicit-rule** | **Default-rule**];

(5) Explicit-rule = ? Specific rule with clear and extract ? ;

(6) Default-rule = ["permitted" | "denied" | ? User default rule ?] ;

(7) External-host-list = **External-host** , { "," , **External-host** } ;

(8) Service = ? Service name ? , { "on" , ? or Protocol or Port ? } ;

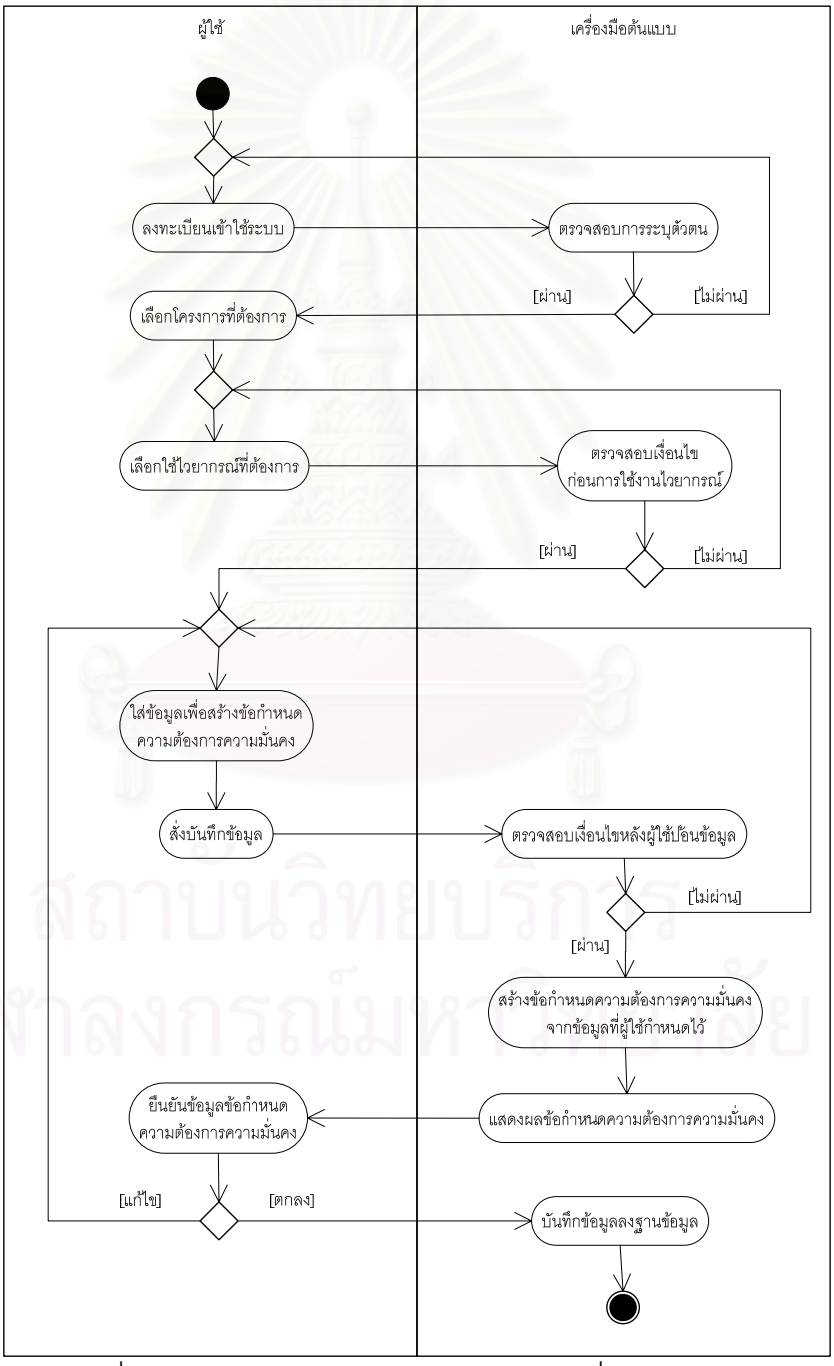
(9) Stateful = ? user statement to indicate the state of information ? ;

ตัวอย่างความต้องการ

The requests from **login host** are **permitted** to access **Mail sever** while login session is available.

ภาคผนวก ค
ตัวอย่างการใช้งานเครื่องมือต้นแบบและผลลัพธ์ความต้องการจากเครื่องมือ

ภายหลังจากพัฒนาเครื่องมือต้นแบบสำหรับสร้างไวยากรณ์ความมั่นคงแล้ว เพื่อแสดงให้เห็นถึงฟังก์ชันงานและการใช้งานของเครื่องมือ สามารถแสดงภาพรวมของการใช้เครื่องมือด้วยแผนภาพกิจกรรมดังรูป ค.1



รูปที่ ค.1 แผนภาพกิจกรรมแสดงการใช้งานเครื่องมือต้นแบบ

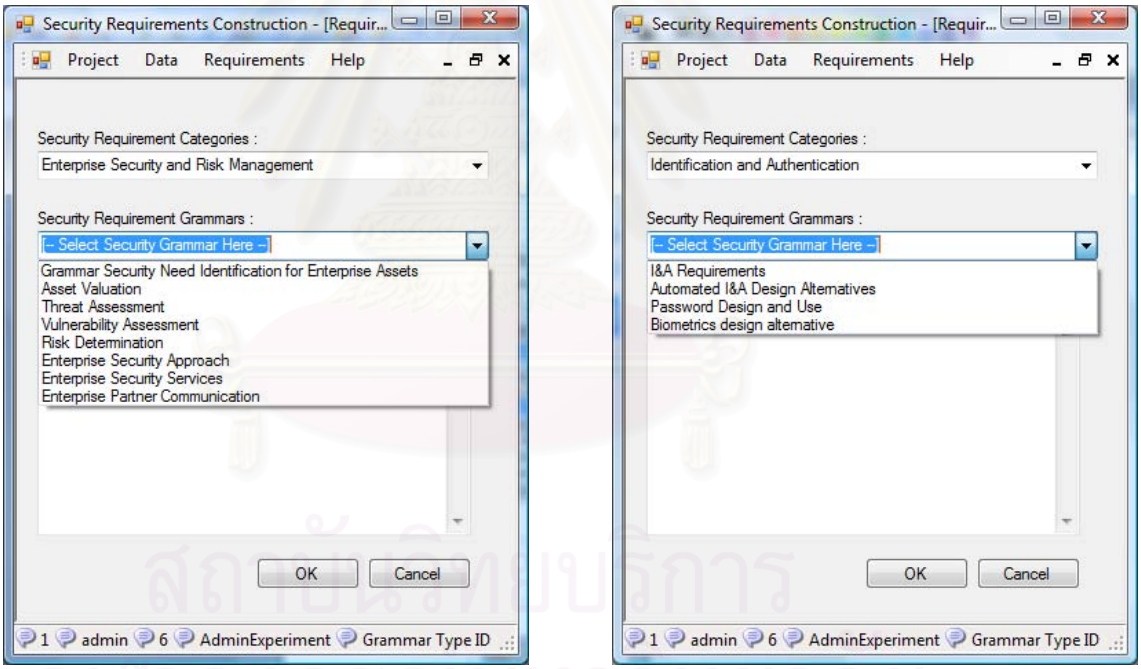
ในภาคผนวก ค จะนำเสนอตัวอย่างการใช้งานเครื่องมือต้นแบบได้ทำการพัฒนาไว้แล้วบนพื้นฐานของไวยากรณ์ที่สร้างขึ้น โดยจะนำเสนอ

1) ขอบเขตของไวยากรณ์ที่เครื่องมือสนับสนุน
2) ตัวอย่างการใช้งานกลุ่มไวยากรณ์การระบุและพิสูจน์ตัวตน
3) ตัวอย่างผลลัพธ์ความต้องการความมั่นคงที่ได้จากเครื่องมือ จำแนกตามไวยากรณ์ความมั่นคง

โดยมีรายละเอียดดังนี้

ค.1 ขอบเขตของไวยากรณ์ที่เครื่องมือสนับสนุน

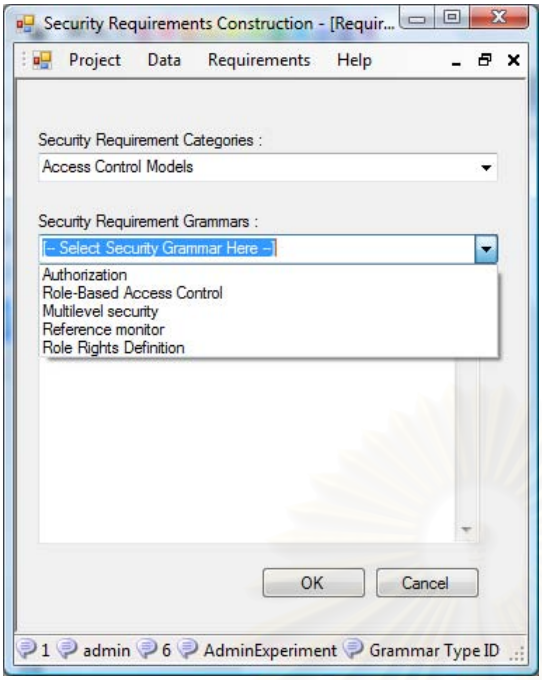
ขอบเขตไวยากรณ์ความมั่นคงที่สนับสนุนโดยเครื่องมือนั้น จะเป็นไปตามขอบเขตงานวิจัย โดยจำแนกออกเป็น 4 กลุ่ม 20 แบบรูปความมั่นคง ดังแสดงในรูปที่ ค.2



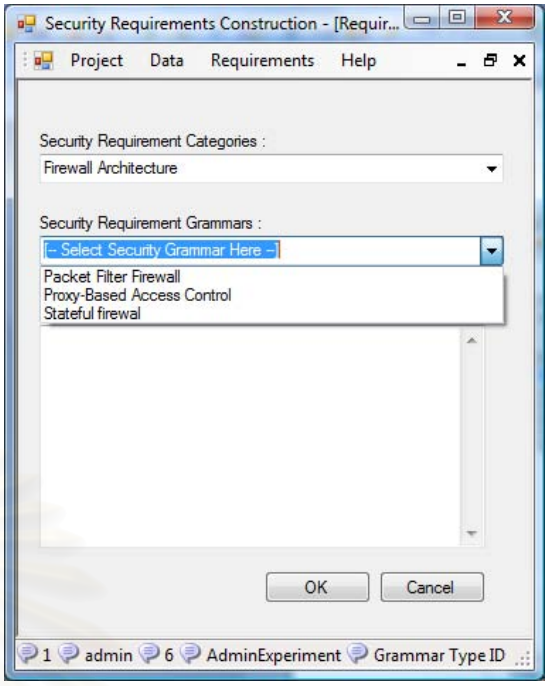
(ก) รายการไวยากรณ์สำหรับกลุ่มความมั่นคงองค์กรและการจัดการความเสี่ยง

(ข) รายการไวยากรณ์สำหรับกลุ่มการระบุและยืนยันตัวตน

รูปที่ ค.2 ไวยากรณ์ที่มีในเครื่องมือต้นแบบ



(ค) รายการไวยากรณ์สำหรับกลุ่มการควบคุมการเข้าถึง

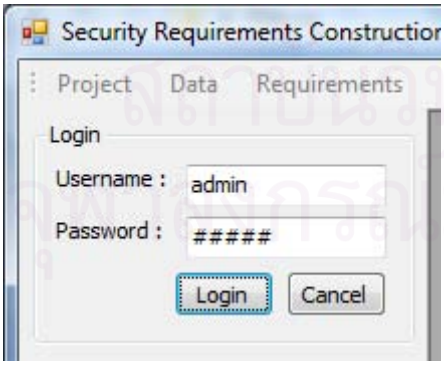


(ง) รายการไวยากรณ์สำหรับกลุ่มสถาปัตยกรรมไฟล์วอลล์

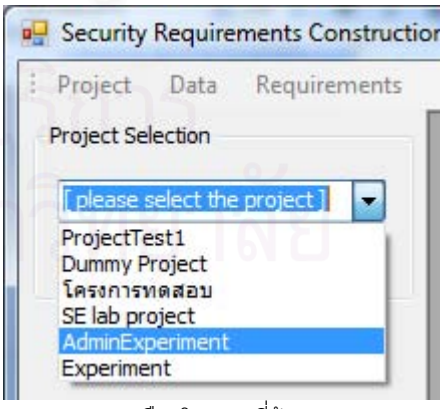
รูปที่ ค.2 ไวยากรณ์ที่มีในเครื่องมือต้นแบบ (ต่อ)

ค.2 ตัวอย่างการใช้งานกลุ่มไวยากรณ์การระบุและพิสูจน์ตัวตน

เพื่อแสดงให้เห็นขั้นตอนการใช้งานจริง ในที่นี้จะขอยกตัวอย่างการใช้งานเครื่องมือกลุ่มไวยากรณ์การระบุและพิสูจน์ตัวตน เพื่อสร้างเป็นความต้องการความมั่นคงสำหรับการระบุและพิสูจน์ตัวตน โดยในการใช้งานเครื่องมือ จะต้องทำการลงทะเบียนเพื่อเข้าระบบ และเลือกโครงการที่ต้องการกำหนดความต้องการความมั่นคง ดังรูปที่ ค.3



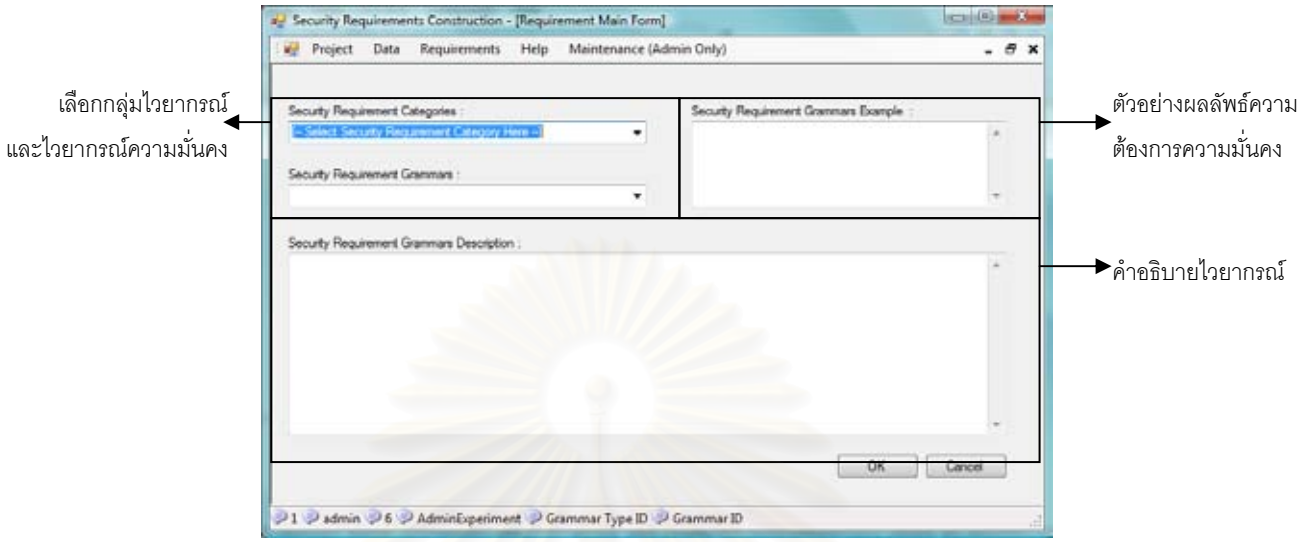
(ก) ลงทะเบียนเพื่อเข้าใช้งานระบบ



(ข) เลือกโครงการที่ต้องการ

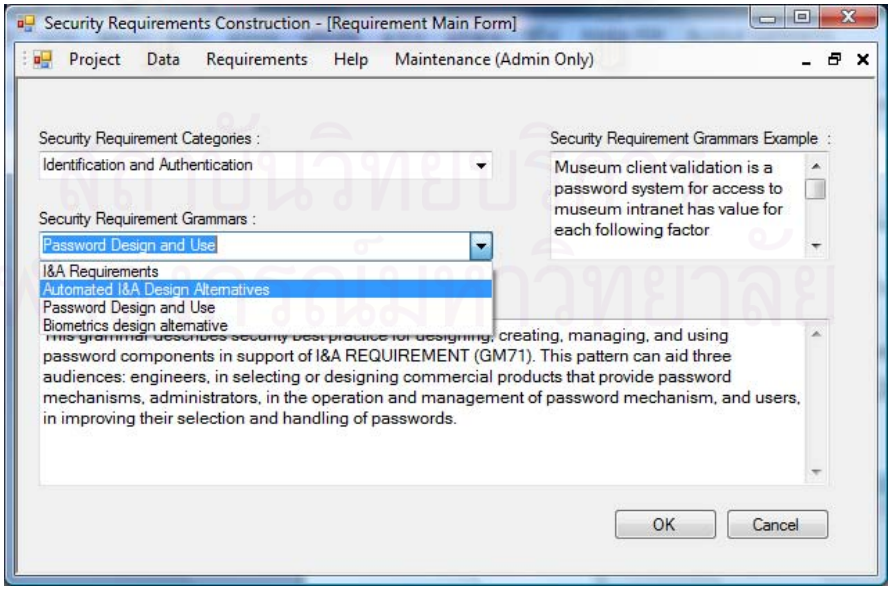
รูปที่ ค.3 ขั้นตอนการลงทะเบียนเข้าระบบก่อนการใช้งานเครื่องมือ

ภายหลังขั้นตอนการลงทะเบียนเข้าใช้ระบบแล้ว ให้เลือก เลือกเมนู Requirements และ New Requirements… จะได้หน้าจอหลักดังรูป ค.4



รูปที่ ค.4 หน้าจอหลักเพื่อเลือกไวยากรณ์ความมั่นคง

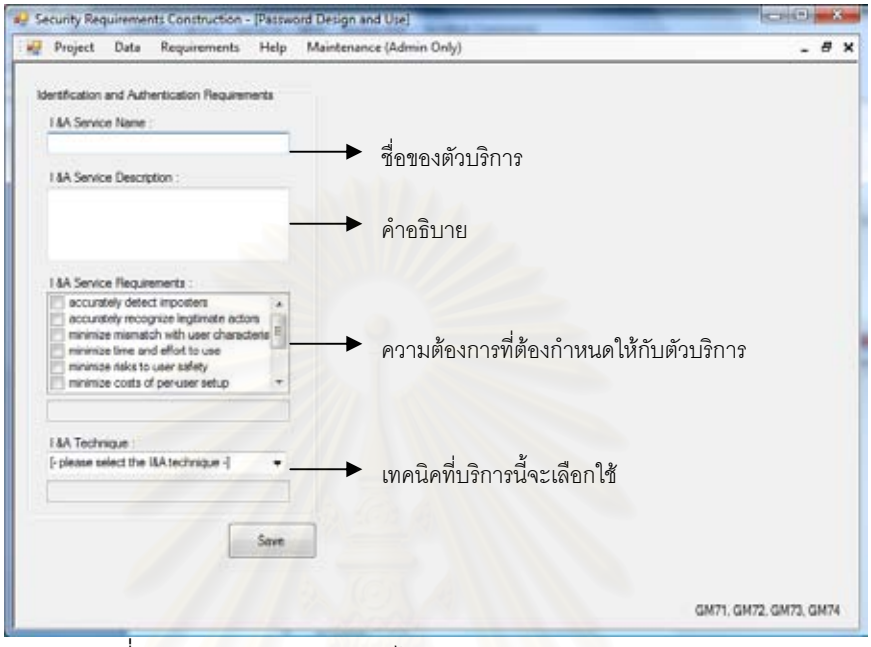
เลือก “Security Requirement Categories” ในกลุ่ม “Identification and Authentication” (ภายหลังการปรับปรุงไวยากรณ์ ทุกไวยากรณ์ในกลุ่มนี้ถูกผนวกเราเข้าเป็นไวยากรณ์เดียว รายละเอียดของไวยากรณ์แสดงดังภาคผนวก ข) แล้วจึงเลือก “Automated I&A Design Alternatives” เพื่อกำหนดความต้องการความมั่นคงสำหรับการระบุและพิสูจน์ตัวตน จากนั้นเครื่องมือจะแสดงคำอธิบายและตัวอย่างสำหรับไวยากรณ์นั้นๆ ดังรูปที่ ค.5



รูปที่ ค.5 หน้าจอหลักแสดงคำอธิบายไวยากรณ์ที่เลือก

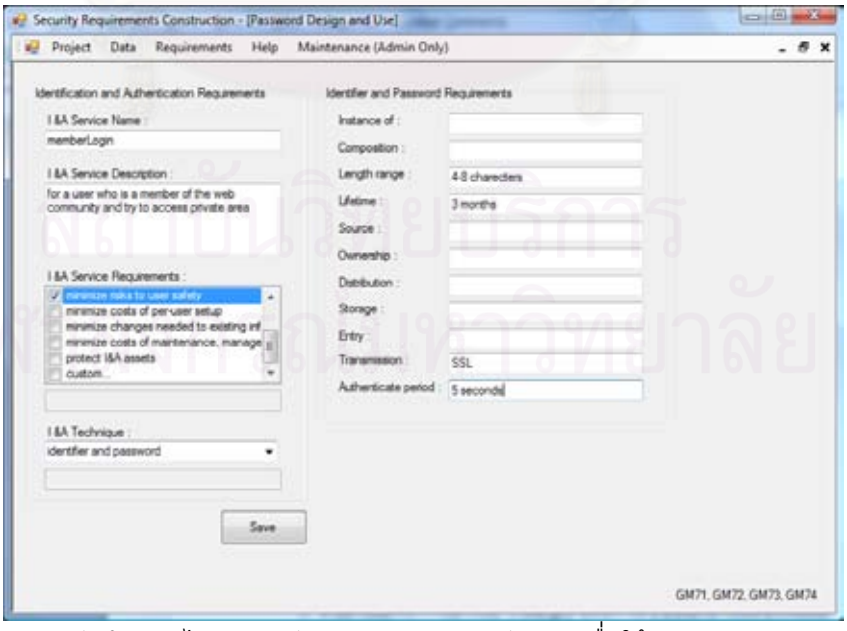
ในที่นี้จะแสดงตัวอย่างการใช้งานเครื่องมือเพื่อกำหนดความต้องการความมั่นคงด้านการระบุและพิสูจน์ตัวตน

1) เมื่อเลือกไวยากรณ์ตามรูปที่ ค.5 จะได้ผลลัพธ์เป็นดังนี้

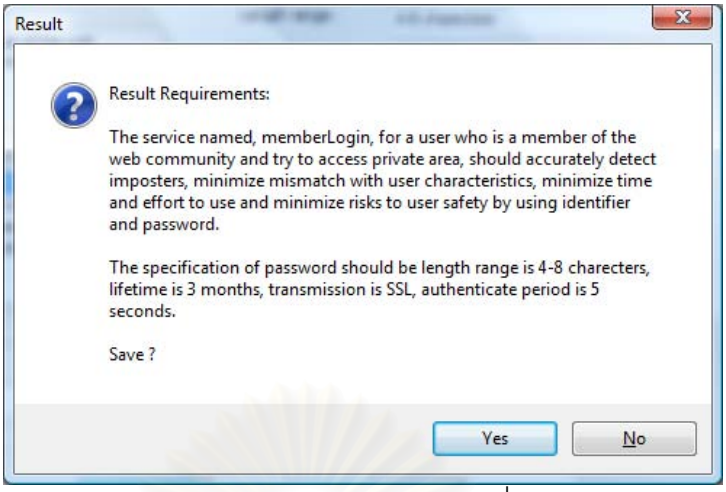


รูปที่ ค.6 แบบฟอร์มสำหรับไวยากรณ์การระบุและพิสูจน์ตัวตน

2) กำหนดชื่อบริการ พร้อมคำอธิบาย(อาจไม่ใส่ก็ได้) แล้วเลือกข้อกำหนดความต้องการสำหรับตัวบริการนี้ และเลือกเทคนิคที่จะใช้ตามลำดับ ในกรณีที่เลือก “Identifier and Password” จะได้แบบฟอร์มดังรูปที่ ค.7 และจะได้ผลลัพธ์ความต้องการดังรูปที่ ค.13

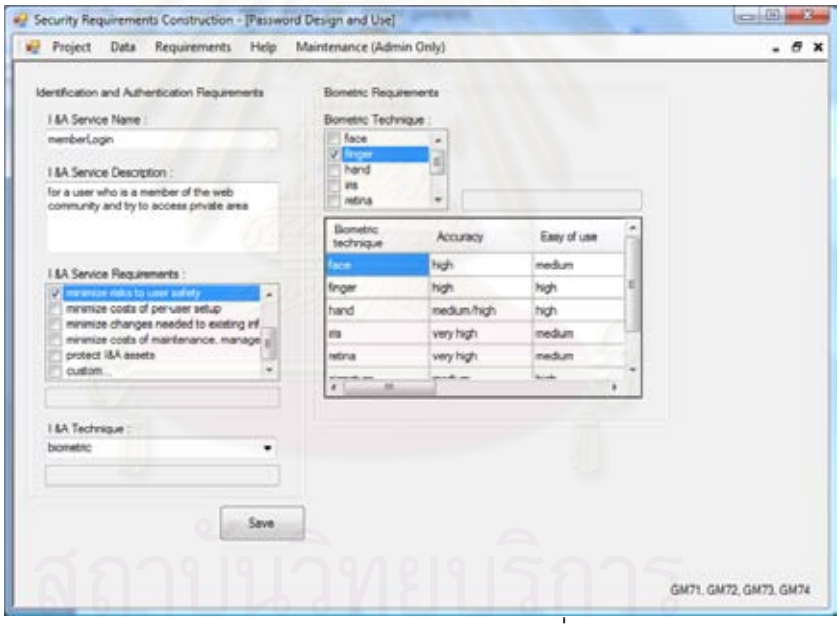


รูปที่ ค.7 แบบฟอร์มสำหรับไวยากรณ์การระบุและพิสูจน์ตัวตนเมื่อใช้ “Identifier and Password”

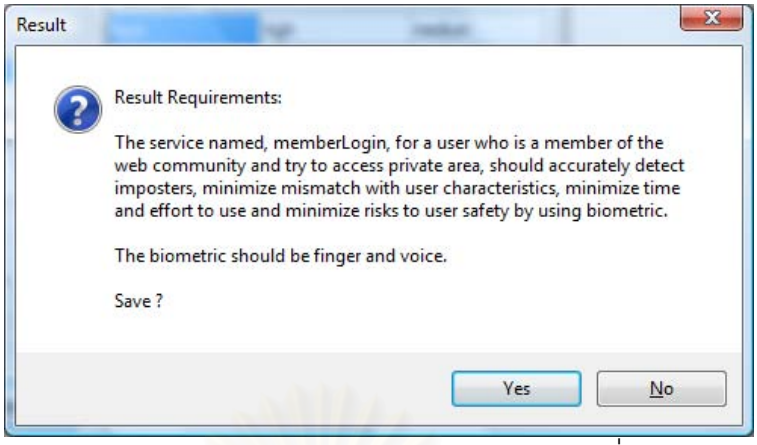


รูปที่ ค.8 ผลลัพธ์จากไวยากรณ์การระบุและพิสูจน์ตัวตนเมื่อใช้ “Identifier and Password”

ในกรณีที่เลือก “Biometric” จะได้แบบฟอร์มดังรูปที่ ค.9 ซึ่งจะปรากฏเทคนิคที่ใช้ในทางชีวมิติให้เลือก พร้อมข้อมูลเชิงคุณภาพสำหรับแต่ละเทคนิค โดยผลลัพธ์ของความต้องการแสดงดังรูปที่ ค.9



รูปที่ ค.9 ผลลัพธ์จากไวยากรณ์การระบุและพิสูจน์ตัวตนเมื่อใช้ “Identifier and Password”

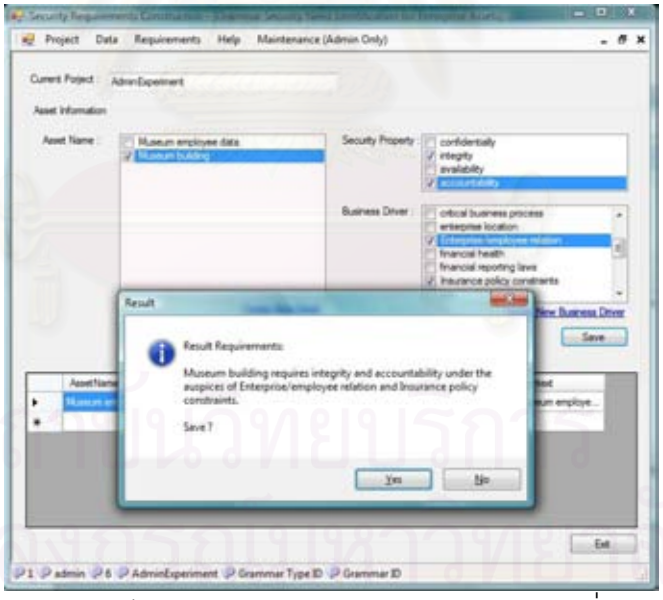


รูปที่ ค.10 ผลลัพธ์จากไวยากรณ์การระบุและพิสูจน์ตัวตนเมื่อใช้ “Biometric”

ค.3 ตัวอย่างผลลัพธ์ความต้องการความมั่นคงที่ได้จากเครื่องมือ จำแนกตามไวยากรณ์ความมั่นคง

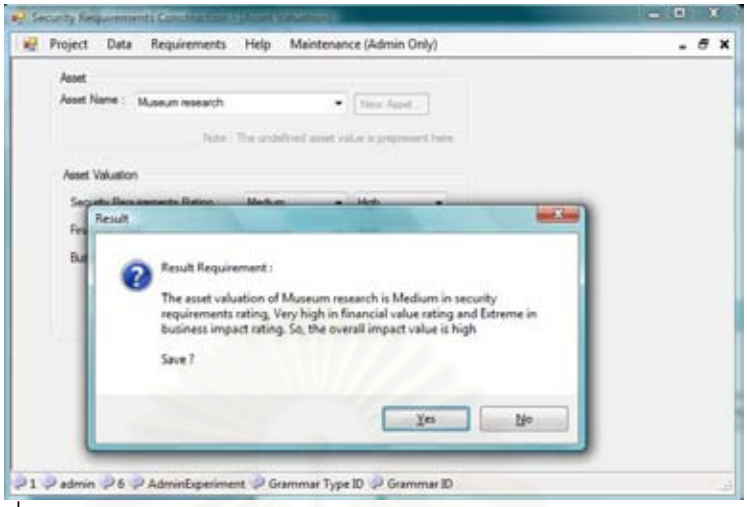
ผลลัพธ์ความต้องการความมั่นคงที่กำหนดโดยใช้เครื่องมือจำแนกตามไวยากรณ์แต่ละประเภท มีรายละเอียดดังนี้

1) ตัวอย่างผลลัพธ์จากไวยากรณ์ “การระบุความต้องการความมั่นคงสำหรับสินทรัพย์ขององค์กร”



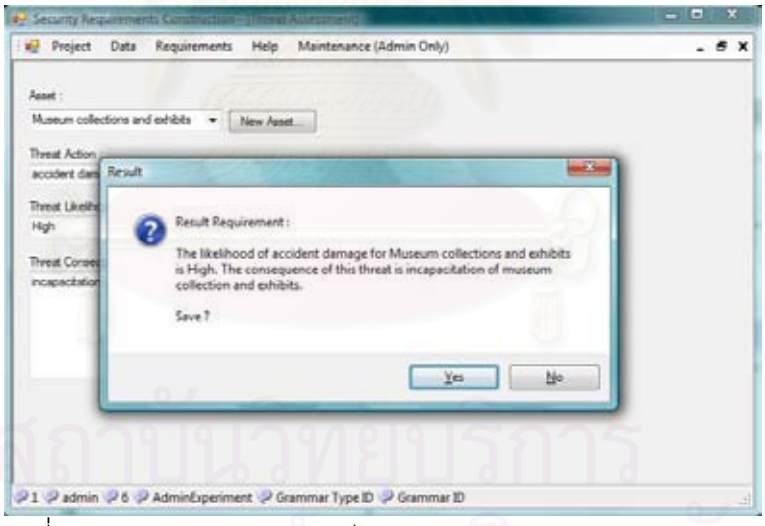
รูปที่ ค.11 ตัวอย่างผลลัพธ์จากไวยากรณ์ “การระบุความต้องการความมั่นคงสำหรับสินทรัพย์ขององค์กร”

2) ตัวอย่างผลลัพธ์จากไวยากรณ์ “การประเมินมูลค่าสินทรัพย์”



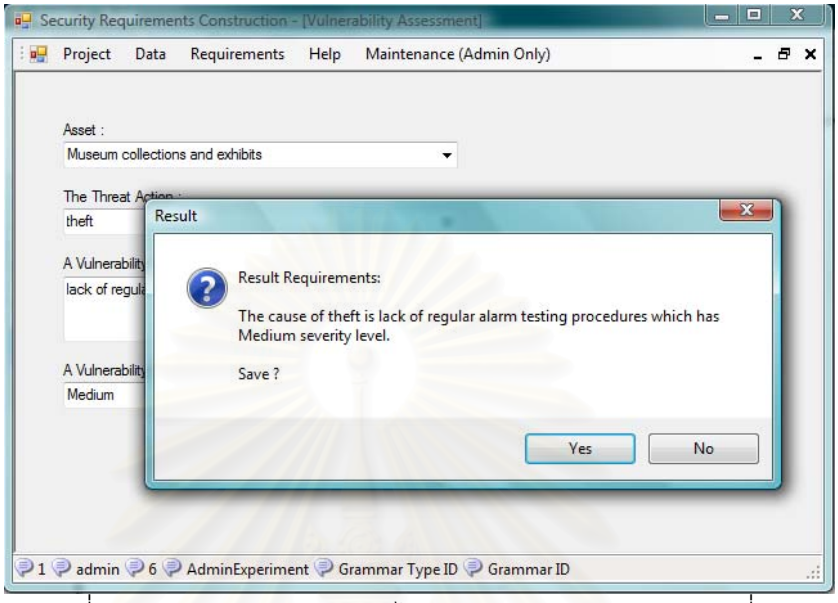
รูปที่ ค.12 ตัวอย่างผลลัพธ์จากไวยากรณ์ “การประเมินมูลค่าสินทรัพย์”

3) ตัวอย่างผลลัพธ์จากไวยากรณ์ “การประเมินภัยคุกคาม”



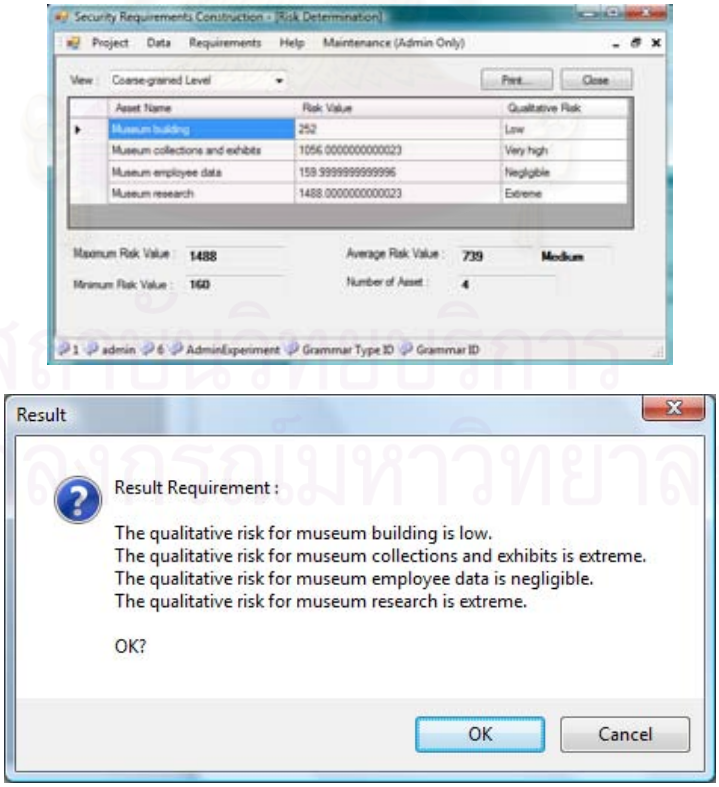
รูปที่ ค.13 ตัวอย่างผลลัพธ์จากไวยากรณ์ “การประเมินภัยคุกคาม”

4) ตัวอย่างผลลัพธ์จากไวยากรณ์ “การประเมินภาวะเสี่ยง”



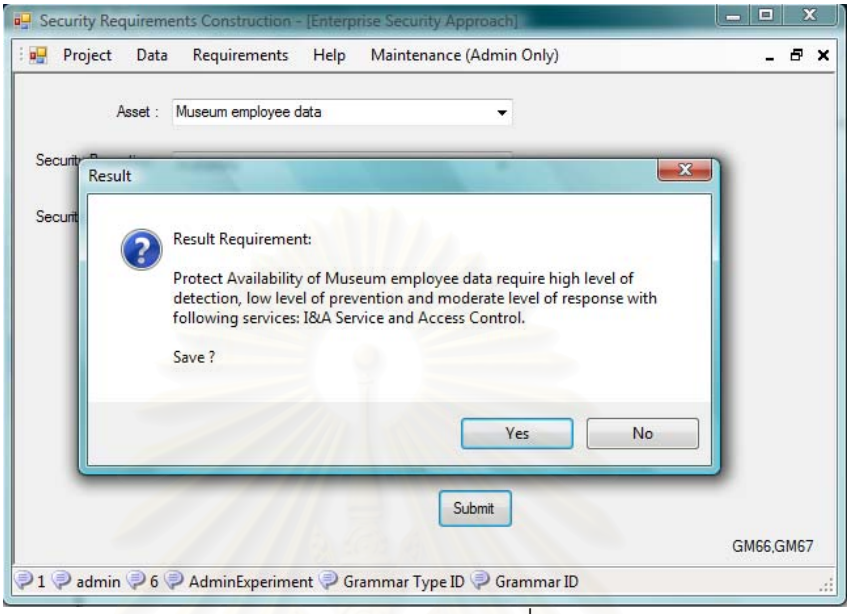
รูปที่ ค.14 ตัวอย่างผลลัพธ์จากไวยากรณ์ “การประเมินภาวะเสี่ยง”

5) ตัวอย่างผลลัพธ์จากไวยากรณ์ “การประเมินความเสี่ยง”



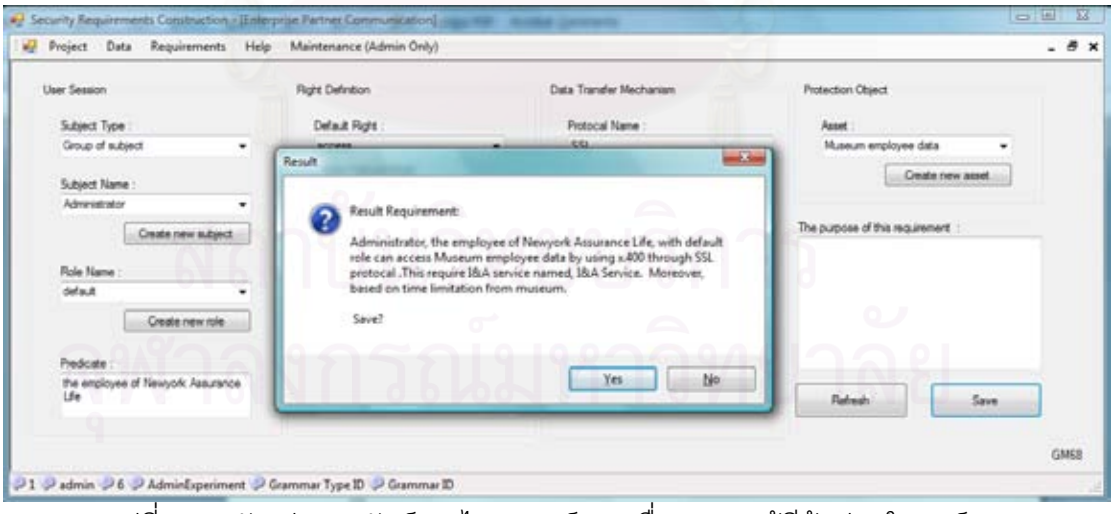
รูปที่ ค.15 ตัวอย่างผลลัพธ์จากไวยากรณ์ “การประเมินความเสี่ยง”

6) ตัวอย่างผลลัพธ์จากไวยากรณ์ “แนวคิดความมั่นคงองค์กร” ร่วมกับไวยากรณ์ “บริการความมั่นคงองค์กร”



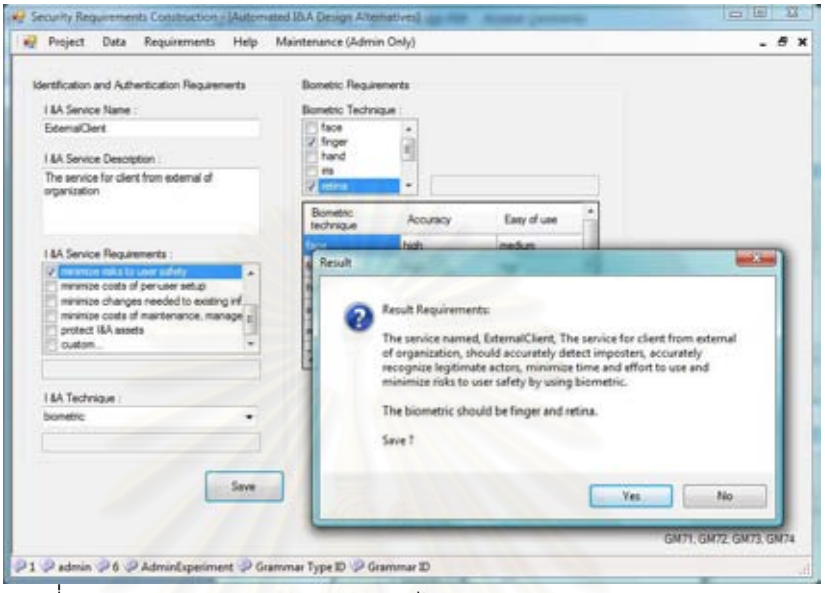
รูปที่ ค.16 ตัวอย่างผลลัพธ์จากไวยากรณ์ “แนวคิดความมั่นคงองค์กร” ร่วมกับไวยากรณ์ “บริการความมั่นคงองค์กร”

7) ตัวอย่างผลลัพธ์จากไวยากรณ์ “การสื่อสารของผู้มีหุ้นส่วนในองค์กร”



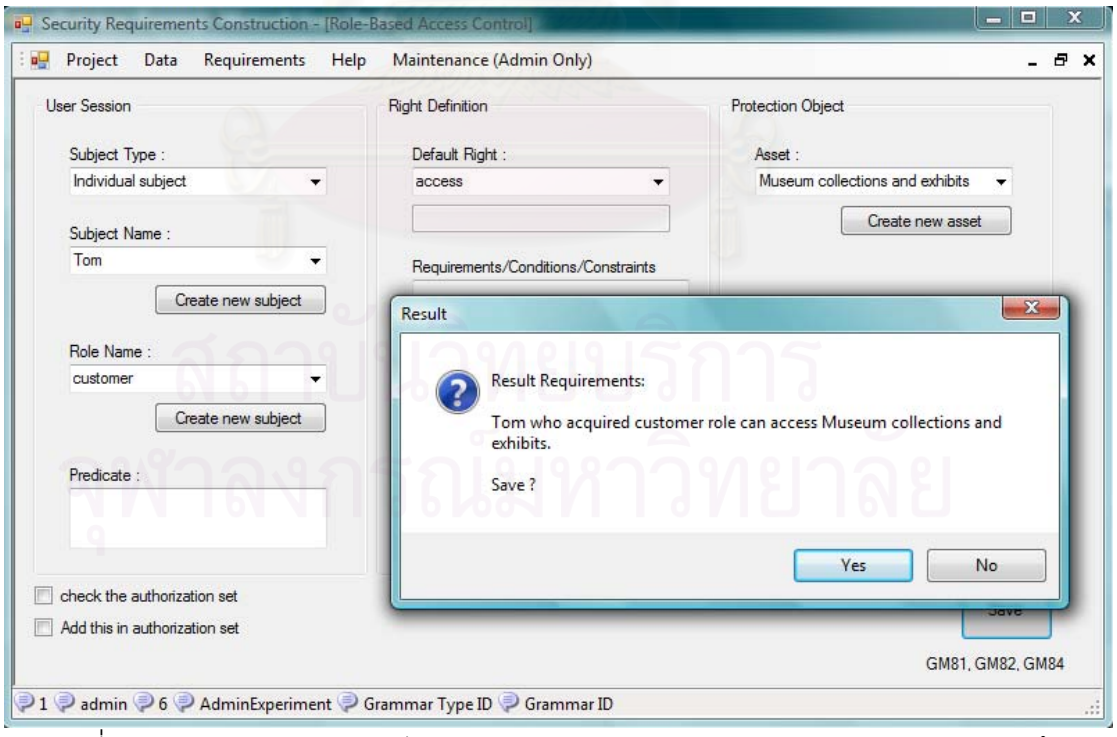
รูปที่ ค.17 ตัวอย่างผลลัพธ์จากไวยากรณ์ “การสื่อสารของผู้มีหุ้นส่วนในองค์กร”

8) ตัวอย่างผลลัพธ์จากไวยากรณ์ “ความต้องการด้านการระบุและการพิสูจน์ตัวตน” “ทางเลือกการออกแบบสำหรับการระบุและการพิสูจน์ตัวตนแบบอัตโนมัติ” “การออกแบบและใช้งานรหัสผ่าน” และ “ทางเลือกการออกแบบสำหรับชีวมิติ”



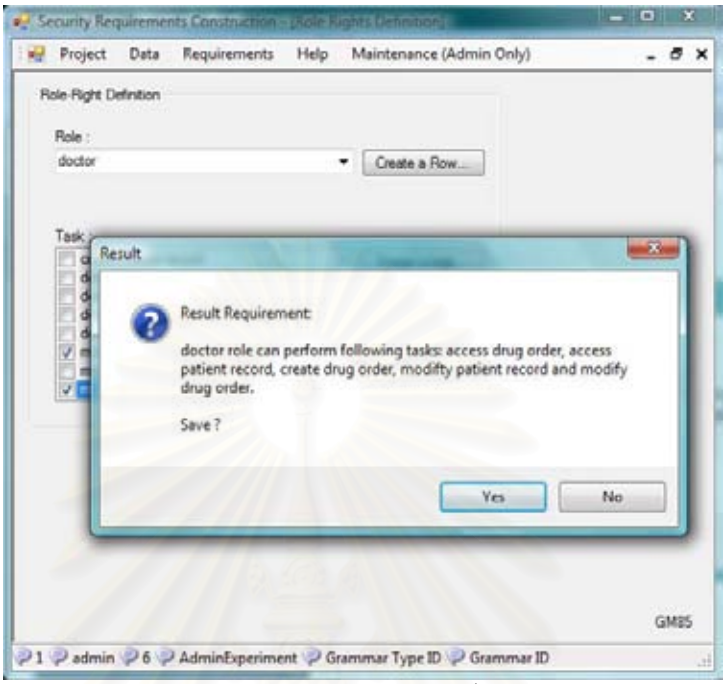
รูปที่ ค.18 ตัวอย่างผลลัพธ์จากกลุ่มไวยากรณ์การระบุและพิสูจน์ตัวตน

9) ตัวอย่างผลลัพธ์จากไวยากรณ์ “การให้อำนาจ” และ “การควบคุมบทบาทการเข้าถึง



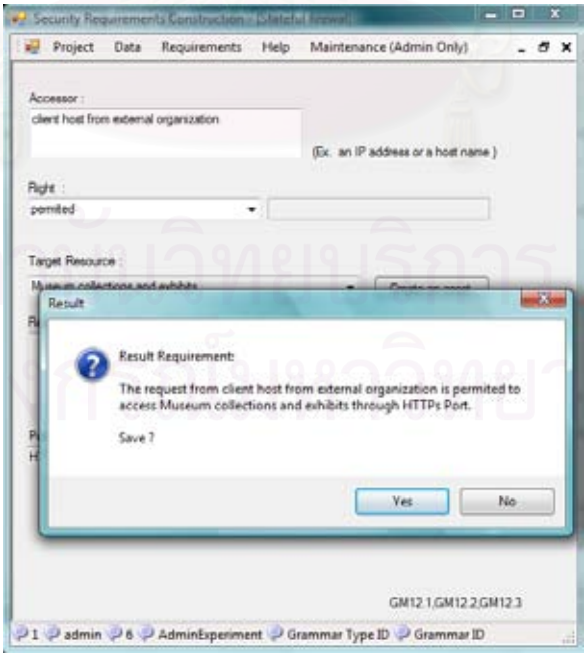
รูปที่ ค.19 ตัวอย่างผลลัพธ์จากไวยากรณ์การให้อำนาจและการควบคุมบทบาทการเข้าถึง

10) ตัวอย่างผลลัพธ์จากไวยากรณ์ “การกำหนดสิทธิ์สำหรับบทบาท” และ “การตรวจสอบการเข้าถึงทรัพยากร”



รูปที่ ค.20 ตัวอย่างผลลัพธ์จากไวยากรณ์การกำหนดสิทธิ์สำหรับบทบาทและการตรวจสอบการเข้าถึงทรัพยากร

11) ตัวอย่างผลลัพธ์จากกลุ่มไวยากรณ์ “สถาปัตยกรรมไฟล์วอลล์”



รูปที่ ค.21 ตัวอย่างผลลัพธ์จากกลุ่มไวยากรณ์ “สถาปัตยกรรมไฟล์วอลล์”

ภาคผนวก ง
สถานการณ์จำลองที่ใช้ในการทดลอง

สถานการณ์จำลองที่ใช้ในการทดลองเครื่องมือในงานวิจัยนี้ประกอบด้วย 3 สถานการณ์จำลอง โดยแต่ละสถานการณ์มีรายละเอียดดังต่อไปนี้

สถานการณ์จำลองที่ 1: การให้บริการไฟล์ประเภทเอฟทีพี

การเปิดให้บริการไฟล์ผ่านทางระบบเครือข่ายซึ่งใช้กันอย่างแพร่หลายในหลายองค์กร เนื่องจากเปรียบเสมือนเป็นคลังข้อมูลที่ให้บุคคลจากเครื่องคอมพิวเตอร์ต่างๆ สามารถเข้าถึงและจัดการข้อมูลกับแฟ้มข้อมูลที่ต้องการได้ อย่างไรก็ตามการให้บริการดังกล่าวต้องพิจารณาถึงความสำคัญของข้อมูลว่ามีระดับชั้นความลับเป็นอย่างไร โดยทั่วไปแล้วเอฟทีจะเปิดให้บริการ 2 ลักษณะ คือ เอฟทีพีแบบนิรนาม (Anonymous FTP) และเอฟทีพีแบบบัญชีผู้ใช้ (Account)

เอฟทีพีแบบนิรนามจะกำหนดให้ผู้ใช้ได้รับอนุญาตสมบูรณ์แบบ (Full Permission) เป็นลักษณะการกำหนดพื้นที่ส่วนหนึ่งให้สามารถเข้าถึงข้อมูลได้แบบสมบูรณ์ เอฟทีพีแบบบัญชีผู้ใช้จะเพิ่มเติมการจัดการเกี่ยวกับการกำหนดสิทธิ์ (Right) ให้กับแต่ละบัญชีหรือกลุ่มบัญชีได้ โดยสิทธิ์พื้นฐานที่เป็นไม่ได้คือ อนุญาต (Permit) และ ไม่อนุญาต (Deny) แฟ้มข้อมูลต่างๆ สามารถถือเป็นสินทรัพย์ของระบบได้ โดยผู้ที่เข้าถึงในที่นี้เรียกว่า ผู้กระทำ (Subject หรือ Actor)

สำหรับข้อมูลที่ปรากฏในเอฟทีพี เราสามารถกำหนดระดับความสำคัญได้โดยการจัดจำแนกไฟล์ไว้ตามโฟลเดอร์ (Folder) ที่กำหนด เปรียบเสมือนการกำหนดประเภท (Category) ของแฟ้มข้อมูล แล้วกำหนดสิทธิ์ให้กับโฟลเดอร์ดังกล่าว ก็จะมีผลกับโฟลเดอร์ย่อย (Sub-Folder) ด้วย สำหรับแฟ้มข้อมูลที่ปรากฏในเอฟทีพีนั้นเป็นได้หลายแบบ เช่น .doc .xls .ppt .exe เป็นต้น เราสามารถกำหนดความสำคัญให้แต่ละแฟ้มข้อมูลต่างกันได้ โดยเฉพาะ .exe ซึ่งถือเป็นแฟ้มข้อมูลที่สามารถทำงานได้ โดยปกติจะไม่อนุญาตให้กระทำการ (Execute) แฟ้มข้อมูลดังกล่าวได้โดยตรง

เอฟทีพีโพรโตคอลสำหรับการเชื่อมต่อผ่านทางเครือข่าย ได้แก่ เอฟทีพีโพรโตคอล (FTP Protocal) และ เอฟทีบีบนเอสเอสแอล (FTP over SSL: FTPs) ซึ่งเมื่อเปิดบริการแล้วก็สามารถเข้าถึงได้ทั้งภายในและภายนอกองค์กร จึงอาจต้องมีการติดตั้งไฟล์วอลล์ไว้สำหรับป้องกันหรือจำกัดการเข้าถึงจากบางส่วนของหน่วยงาน จากเครื่องที่ระบุไว้เฉพาะเจาะจง หรือจากองค์กรภายนอก

จากข้อมูลข้างต้น หากท่านเป็นผู้รับผิดชอบการเปิดให้บริการแฟ้มข้อมูลข้อมูล (FTP Service) ท่านจะมีการเสนอความต้องการความมั่นคงใน 4 ประเภท (การกำหนดสินทรัพย์องค์กร

และการจัดการความเสี่ยง การควบคุมการเข้าถึง การระบุและยืนยันตัวตน และสถาปัตยกรรมไฟล์วอลล์) ได้อย่างไร

สถานการณ์จำลองที่ 2: การจัดการห้องปฏิบัติการ

กำหนดให้ท่านเป็นผู้ดูแลห้องปฏิบัติการในภาควิชาวิศวกรรมคอมพิวเตอร์ ซึ่งเป็นห้องปฏิบัติการสำหรับให้นิสิตระดับบัณฑิตศึกษาเข้ามาใช้งานอุปกรณ์ต่างๆ ภายในระบบ ซึ่งสินทรัพย์ภายในห้องปฏิบัติการมีหลายอย่าง เช่น อุปกรณ์คอมพิวเตอร์ต่างๆ เครื่องเซิร์ฟเวอร์ โต๊ะ เก้าอี้ หลอดไฟ และอื่นๆ เป็นต้น ซึ่งแต่ละอุปกรณ์ล้วนแล้วแต่เกี่ยวข้องกับความมั่นคงได้ทั้งสิ้น หากท่านต้องการให้ห้องปฏิบัติการมีความมั่นคงมากขึ้น จะต้องกำหนดความต้องการด้านความมั่นคงได้อย่างไร

สิ่งแรกที่ต้องพิจารณาคือ ใครบ้างที่จะสามารถเข้าห้องปฏิบัติการได้ ซึ่งการเข้าห้องปฏิบัติการได้นั้นจะต้องมีวิธีการสำหรับการระบุตัวตนหรือยืนยันตัวตนก่อน หากระบบตรวจสอบแล้วสามารถระบุตัวตนได้ก็สามารถเข้าห้องปฏิบัติการได้ และเมื่อเข้าได้แล้วจะสามารถเข้าใช้งานอุปกรณ์หรือทรัพยากร (Resource) ได้ตามสิทธิ์ที่ได้รับมอบหมายเท่านั้น

ภายในห้องปฏิบัติการ มีระบบเครือข่ายซึ่งสามารถติดต่อกับภายนอกได้ อย่างไรก็ตาม ข้อมูลที่มีภายในห้องปฏิบัติการ อาจมีได้ทั้งข้อมูลสำคัญ ข้อมูลส่วนบุคคล หรือข้อมูลงานวิทยานิพนธ์ ซึ่งอาจจะต้องมีการกำหนดไฟล์วอลล์เพื่อกรองหรือป้องกันการติดต่อสู่ภายนอก เช่น การไม่อนุญาตให้มีข้อมูลผ่านทางโปรโตคอลบางตัว หรือ บางพอร์ต (Port) เช่น โปรแกรมประเภทเพียร์ทูเพียร์ (P2P) เป็นต้น

จากข้อมูลข้างต้น หากท่านเป็นผู้รับผิดชอบจัดการห้องปฏิบัติการ ท่านจะมีการเสนอความต้องการความมั่นคงใน 4 ประเภท (การกำหนดสินทรัพย์องค์กรและการจัดการความเสี่ยง การควบคุมการเข้าถึง การระบุและยืนยันตัวตน และสถาปัตยกรรมไฟล์วอลล์) ได้อย่างไร โดยในสถานการณ์นี้ท่านสามารถออกแบบความต้องการได้ตามต้องการโดยไม่ต้องยึดติดกับห้องปฏิบัติการปัจจุบันที่ท่าสังกัดอยู่

สถานการณ์จำลองที่ 3: ระบบธนาคารออนไลน์

เนื่องจากระบบการจัดการข้อมูลการเงินผ่านทางอินเทอร์เน็ตเป็นที่นิยมกันมาก ดังนั้นสถานการณ์นี้จะเป็นการสมมติให้หน่วยทดลองเป็นผู้วิศวกรความต้องการที่จะต้องกำหนดความต้องการต่างๆ ที่เกี่ยวข้องกับความมั่นคงระบบธนาคารออนไลน์ ซึ่งเป็นระบบที่เปิดให้ลูกค้าของธนาคารสามารถทำธุรกรรมด้านการเงินต่างๆ ได้ เช่น การโอนเงินระหว่างบัญชีของลูกค้าเอง การโอนเงินไปยังบัญชีอื่นๆ ภายใต้ธนาคารเดียวกัน เป็นต้น ลูกค้าสามารถดูข้อมูลส่วนตัว ข้อมูลรหัส

ข้อมูลยอดเงินคงเหลือ รายการการใช้จ่ายได้เช่นกัน อย่างไรก็ตามลูกค้าจะแก้ไขข้อมูลบางส่วนได้เท่านั้น เช่น ข้อมูลรหัสผ่านเพื่อใช้งานระบบ เป็นต้น โดยไม่มีสิทธิ์ที่จะทำการเปลี่ยนแปลงข้อมูลอื่นๆ ที่กล่าวมาข้างต้นได้ ทั้งนี้ข้อกำหนดดังกล่าวเป็นไปตามนโยบายขององค์กรของแต่ละธนาคารโดยปกติ ระบบธนาคารออนไลน์จะต้องมีการล็อกอิน (Login) ก่อนเข้าใช้งาน โดยการถ่ายโอนข้อมูลระหว่างผู้ใช้และระบบธนาคารจะมีการเข้ารหัสผ่านทางเอสเอสแอลโปรโตคอล (SSL Protocol)

อนึ่งเจ้าหน้าที่ธนาคารสามารถเข้าถึงข้อมูลข้อลูกค้าได้ด้วย เช่น ข้อมูลบัญชีธนาคารต่างๆ เช่น ชื่อเจ้าของบัญชี จำนวนบัตรเดบิตหรือบัตรเครดิตสำหรับบัญชีดังกล่าว วงเงินการจ่าย/ถอนสูงสุด และชื่อผู้ใช้ (Username) สำหรับการล็อกอินได้ แต่เจ้าหน้าที่ธนาคารไม่สามารถเข้าดูข้อมูลรายการใช้จ่าย ยอดเงินในระบบ รหัสผ่าน หรือการยกเลิกหรือระงับบัญชีดังกล่าว เว้นเสียจะได้รับการอนุญาตจากเจ้าของบัญชีอย่างเป็นลายลักษณ์อักษร และไม่มีสิทธิ์ในการแก้ไขรายการใช้จ่ายยอดเงินในบัญชีได้ๆ

จากข้อมูลข้างต้น หากท่านเป็นผู้รับผิดชอบในการกำหนดความต้องการด้านความมั่นคงสำหรับระบบ ธนาคารออนไลน์ ท่านจะมีการเสนอความต้องการความมั่นคงใน 4 ประเภท (การกำหนดสินทรัพย์องค์กรและการจัดการความเสี่ยง การควบคุมการเข้าถึง การระบุและยืนยันตัวตน และสถาปัตยกรรมไฟล์วอลล์) ได้อย่างไร ในสถานการณ์นี้ท่านสามารถออกแบบความต้องการได้ตามต้องการโดยไม่ต้องยึดติดกับระบบธนาคารออนไลน์ที่ท่านใช้บริการอยู่

ภาคผนวก จ

รายการการตรวจสอบก่อนการกำหนดความต้องการความมั่นคง

ค.1 กลุ่มรายการตรวจสอบสำหรับ 'การจัดการสินทรัพย์องค์กรและความเสี่ยง'

1) ระบบประกอบด้วยสินทรัพย์ (Asset / Protection object / essential data) อะไรบ้าง
2) จากข้อ 1 แต่ละสินทรัพย์จะต้องดำเนินการเกี่ยวข้องกับปัจจัยทางธุรกิจ (Business Factor) ใด
3) แต่ละสินทรัพย์ต้องการคุณสมบัติความมั่นคง (Security Properties) อะไรบ้าง เพราะอะไร
4) จากข้อ 1 และ 4 เราควรเลือก Security Approach ใด สำหรับสินทรัพย์ที่กำหนด และควรใช้ในระดับใด
5) จากข้อ 1 สินทรัพย์ดังกล่าวมักมีคุณค่า (Asset Value) ที่แตกต่างกันในมุมมองของความมั่นคง (Security) มุมมองทางธุรกิจ (Business Impact) และ มุมมองทางเศรษฐกิจ (Financial value) กรุณาระบุคุณค่าของสินทรัพย์ในมุมมองดังกล่าวเป็นตัวเลข 1-5 โดย 1 คือมีคุณค่าน้อยมาก ขณะที่ 5 มีคุณค่าหรือมีผลกระทบสูงสุด
6) จากข้อ 1 คุณคิดว่าจะมีภัยคุกคามใดบ้างที่จะมีผลต่อสินทรัพย์ที่คุณได้กำหนดไว้ กรุณาระบุภัยคุกคามต่อสินทรัพย์ และผลที่ตามมา พร้อมทั้งระบุโอกาสหรือความถี่ที่ภัยคุกคามดังกล่าวจะปรากฏ
7) จากข้อ 5 ภัยคุกคามใดๆ ย่อมมีผลกระทบต่อสินทรัพย์ในความรุนแรงที่แตกต่างกัน กรุณาระบุจุดอ่อนของสินทรัพย์และระดับความรุนแรงเชิงคุณภาพในระดับใดดังกล่าวว่า
8) จากข้อ 5-7 ท่านสามารถคำนวณค่าความเสี่ยงได้หรือไม่ ถ้าได้คำนวณอย่างไร แต่ละสินทรัพย์มีความค่าความเสี่ยงเท่าไหร่ และมีระดับความเสี่ยงเชิงคุณภาพในระดับใด
9) ระบบต้องติดต่อกับระบบภายนอก (3rd party) หรือไม่ ถ้ามี ชื่ออะไร
10) ข้อมูล 3rd party ควรเป็นข้อมูล subject หรือไม่ (ถ้าเป็นก็เพิ่มเข้าไป)
11) กรณีที่มีการติดต่อกับ 3rd party กรุณากำหนดรายการติดต่อว่า 3rd party ต้องการติดต่อกับสินทรัพย์ใดในองค์กร โดยวิธีการใด มีการส่ง message format ในรูปแบบไหน ผ่าน protocol อะไร

ตัวอย่างความต้องการความมั่นคงด้านการจัดการสินทรัพย์องค์กรและความเสี่ยง

- Employee data, financial data require confidentially, integrity, accountability under the auspices of laws or regulation.
- The likelihood of data entry error for museum employee data is very high.
- The causes of museum fire are failure of fire alarm system which has extreme severity level, failure of fire suppression system which has very high severity level.
- Protect integrity of employee data, financial data require high level of prevention, high level of detection, high level of response
- The marketing of company-A, who acquire ReaderRole, can access the database sever of company-B for retrieving and exchanging payment transaction using X.400 message. This access requires I&A service named, IA-ExternalExchangePayment. Moreover, this access can be schedule or automatic operations which define my system admin.

ค.2 กลุ่มรายการตรวจสอบสำหรับ 'การควบคุมการเข้าถึง'

12) จากข้อ 1 ในด้านของความมั่นคง เราควรกำหนดค่าระดับความมั่นคงสำหรับ Asset (Specification level) ในระดับใด ในช่วง 1-6 (น้อยไปมาก)
13) ระบบมีผู้ติดต่อ (Subject) อะไรบ้าง
14) จากข้อ 13 ในด้านของความมั่นคง เราควรกำหนดค่าระดับความมั่นคงสำหรับ Subject (Clearance level) ในระดับใด ในช่วง 1-6 (น้อยไปมาก)
15) ระบบนี้มีสิทธิ์ (Right) ให้สำหรับผู้ติดต่ออะไรบ้าง
16) ระบบนี้มีบทบาทอะไรบ้าง (Role) และบทบาทดังกล่าวมีสิทธิ์ทำอะไรได้บ้าง
17) จากข้อ 12-16 ผู้ติดต่อสามารถใช้สิทธิ์ เพื่อดำเนินการอะไรได้บ้าง กับสินทรัพย์ที่กำหนดไว้
18) จากข้อ 12-16 ผู้ติดต่อสามารถใช้สิทธิ์ เพื่อไม่สามารถดำเนินการอะไรได้บ้าง กับสินทรัพย์ที่กำหนดไว้

ตัวอย่างความต้องการความมั่นคงด้านการควบคุมการเข้าถึง

- Doctor group, nurse group who obtain modify role can read and modify and create report for their patient record.

- Tom who acquire customer role can access museum collections and exhibits.

ค.3 กลุ่มรายการตรวจสอบสำหรับ 'การระบุและพิสูจน์ตัวตน'

19) หาระบบมีการตรวจสอบการระบุและพิสูจน์ตัวตน (Identification and Authentication) ท่าจะมีวิธีการใดบ้าง และมีความต้องการเชิงคุณภาพ (Quality Requirements) อย่างไร (ถ้ามี)

20) จากข้อ 17 กรณีที่มีการใช้การระบุตัวตนแบบใช้ชื่อและรหัสผ่าน (username and password) กรุณากำหนดความต้องการของ password ว่าจะต้องมีอะไรบ้าง

21) จากข้อ 17 กรณีที่มีการใช้การระบุตัวแบบใช้ชีวมิติ (Biometric) กรุณาเลือกวิธีการว่าจะใช้ Biometric ตัวใด

<u>ตัวอย่างความต้องการความมั่นคงด้านการระบุและพิสูจน์ตัวตน</u>

- The service named, ExternalClient, for client from external of organization, should accurately detect imposters, accurately recognize legitimate actors, minimize time and effort to use and minimize risks to user safety by using biometric.

D. กลุ่มรายการตรวจสอบสำหรับ 'สถาปัตยกรรมไฟร์วอลล์'

22) ระบบนี้มีข้อกำหนดในเรื่องของไฟล์วอลล์ไว้หรือไม่ ถ้ามีควรมีอะไรบ้าง

<u>ตัวอย่างความต้องการความมั่นคงด้านสถาปัตยกรรมไฟล์วออล์</u>

- The requests from login host are permitted to access Mail sever while login session is available.
- The requests from 192.22.4.4 are permitted to access 192.200.17.1.

<u>แนวคำถาม</u>

จากระบบที่ท่านได้รับมอบหมาย หากสมมติให้ท่านเป็นผู้บริหารจัดการด้านไอทีของบริษัทแห่งหนึ่ง ได้ต้องรับผิดชอบกับระบบที่ได้รับมอบหมาย ท่านจะสามารถกำหนดความต้องการความมั่นคงในด้านต่างๆ ว่าอย่างไร โดยใช้รายการตรวจสอบข้างต้นมาช่วยท่านในการพิจารณากรุณาระบุความต้องการด้านความมั่นคงในแต่ละกลุ่มไม่น้อยกว่า 5 ประโยค (ข้อ) โดยกำหนดให้ 1 ประโยค คือ 1 ความต้องการเท่านั้น โดยความต้องการความมั่นคงที่จะท่านจะนำเสนอนั้นจะต้องอยู่ใน 4 กลุ่มความต้องการความมั่นคงตามที่ได้นำเสนอไว้ข้างต้นเท่านั้น

ภาคผนวก ฉ

แบบสอบถาม

แบบฟอร์มการประเมินการทดสอบเครื่องมือสำหรับกำหนดความต้องการความมั่นคง จากไวยากรณ์ความมั่นคงที่สร้างจากแบบรูปความมั่นคง

ให้ท่านทำเครื่องหมาย ✓ ลงในช่องว่างทางขวามือ ตรงกับความคิดเห็นของท่าน ในการใช้เครื่องมือที่สร้างบนพื้นฐานของไวยากรณ์ความมั่นคงเพื่อกำหนดความต้องการด้านความมั่นคง ซึ่งมี 5 ระดับ

5 หมายถึง เห็นด้วยมากที่สุด

4 หมายถึง เห็นด้วยมาก

3 หมายถึง เห็นด้วยปานกลาง

2 หมายถึง เห็นด้วยน้อย

1 หมายถึง เห็นด้วยน้อยที่สุด

ชื่อผู้ทดลอง _____ สถานการณ์จำลอง _____

ปัจจัยที่ใช้ในการพิจารณา	ระดับความคิดเห็น				
	5	4	3	2	1
1. ความคิดเห็นต่อคุณภาพผลลัพธ์ความต้องการความมั่นคงที่ได้จากเครื่องมือ					
1.1 เครื่องมือช่วยในการกำหนดความต้องการความมั่นคงได้ครบถ้วนมากกว่าการกำหนดความความต้องการดังกล่าวด้วยตนเอง					
1.2 เครื่องมือช่วยในการกำหนดความต้องการความมั่นคงได้ถูกต้องมากกว่าการกำหนดความต้องการดังกล่าวด้วยตนเอง					
1.3 เครื่องมือช่วยในการกำหนดความต้องการความมั่นคงได้ไม่กำกวมมากกว่าการกำหนดความต้องการดังกล่าวด้วยตนเอง					
2. ความคิดเห็นต่อประโยชน์ของเครื่องมือที่มีต่อหน่วยทดลองภายหลังจากการใช้เครื่องมือ					
2.1 เครื่องมือช่วยส่งเสริมให้ท่านเกิดการเรียนรู้ด้วยตนเองเกี่ยวกับการกำหนดความต้องการความมั่นคง ทำให้เกิดความสนใจและมีความเข้าใจมากขึ้น					
2.2 เครื่องมือช่วยให้ท่านใช้เวลาในการกำหนดความต้องการความมั่นคงน้อยกว่าเวลาที่ท่านใช้ขณะที่ไม่มีเครื่องมือ					
2.3 เครื่องมือสามารถลดความพยายามของท่านในการกำหนดความต้องการความมั่นคงมากกว่าตอนที่ท่านกำหนดความต้องการดังกล่าวโดยไม่ใช้เครื่องมือ					

ปัจจัยที่ใช้ในการพิจารณา	ระดับความคิดเห็น				
	5	4	3	2	1
2.4 ท่านสามารถกำหนดความต้องการความมั่นคงโดยใช้เครื่องมือได้ดีกว่าไม่ใช้เครื่องมือ					
3. ความคิดเห็นต่อคุณสมบัติเครื่องมือ					
3.1 เครื่องมือสนับสนุนการนำกลับมาใช้ใหม่ของความต้องการความมั่นคงได้					
3.2 เครื่องมือมีความสามารถในการตรวจสอบลำดับของการกำหนดความต้องการความมั่นคง เพื่อลดความไม่สอดคล้องกันระหว่างความต้องการ					
3.3 เครื่องมือช่วยลดความยุ่งยากในการกำหนดความต้องการความมั่นคง					
4. ความคิดเห็นที่มีต่อการนำเครื่องมือไปประยุกต์ใช้ในองค์กรด้านความมั่นคง					
4.1 องค์กรควรนำเครื่องมือไปประยุกต์ใช้เพื่อกำหนดความต้องการความมั่นคงและนโยบายความมั่นคงสำหรับองค์กรได้					
4.2 องค์กรสามารถนำความต้องการความมั่นคงจากเครื่องมือมาจัดเก็บเป็นข้อมูลเพื่อสร้างเป็นองค์ความรู้สำหรับองค์กรได้					

ความคิดเห็นและข้อเสนอแนะ

ภาคผนวก ช
ผลงานตีพิมพ์

ระหว่างดำเนินงานวิจัย ผู้วิจัยได้เขียนบทความเพื่อตีพิมพ์ผลงานในวารสารวิชาการและการประชุมวิชาการทั้งในและต่างประเทศดังนี้

1. K. Supaporn, N. Prompoon and T. Rojkangsadan, “An Approach: Constructing the Grammar from Security Pattern”. The 4th International Joint Conference on Computer Science and Software Engineering (JCSSE 2007), Khonkaen University, Khonkaen, Thailand, May 2-4, 2007.

2. K. Supaporn, N. Prompoon and T. Rojkangsadan, “Enterprise Assets Security Requirements Construction from ESRMG Grammar based on Security Patterns”. The 14th Asia-Pacific Software Engineering Conference (APSEC 2007), Nagoya, Japan, December 5-7, 2007.

An Approach: Constructing the Grammar from Security Pattern

Kawin Supaporn, Nakornthip Prompoon, Thongchai Rojkangsadan
Software Engineering Lab, Center of Excellence in Software Engineering
Department of Computer Engineering
Chulalongkorn University, Bangkok, Thailand
Kawin.S@student.chula.ac.th, Nakornthip.S@chula.ac.th, Thongchai.R@chula.ac.th

ABSTRACT

Security requirement is one of essential requirements for the currently information system. Since, the system without security is risk to attack or fail. Consequently, stakeholders and developers must concern with security requirements. However, the security requirement is rather difficult to define correctly and completely because it requires experience and knowledge from stakeholders and developers with security background. In order to avoid the miss-configuration of system from requirements that gather from stakeholders. One of alternative solutions is security patterns which are guidance that include security requirements of a common security system. We propose an approach to construct a grammar in an extended-BNF form which helps to create security requirements of a system. A prototyping tool based on our proposed grammar is also presented.

1. INTRODUCTION

Software requirements engineering is an important process in software development life cycle since the purpose of it is to gather the requirements from all related stakeholders in order to produce requirements will be used as a contract among them. However, the variation and complexity of the system in today computing technology projects are still major problems for requirements engineer to earn a complete, correct and unambiguity system requirements which are the main characteristics of system requirements specification [1]. The project manager and requirements engineer have to find methodologies and/or tools to handle these problems. Generally time and cost factor constraints are the major concerns of the organization and the development team. Consequently, they always pay attention to functional requirements than non-functional requirements (or quality requirements) because the functional requirements are the services of the system that visible to users. Security requirement is one of quality requirements that requires developers with deep experience in different security aspects. In many organizations, there are insufficient of developers who have such characteristic. Thus, security requirements of the system may be defined far from complete and correct. This explicitly leads to earn a system have many channels attacked from any harms.

Generally, in the organizations, manager has the alternate goal to maintain the system in a secure state. Thus, they can study from heuristic requirements with security concern from previously developed system and apply them into their new system development. The new system will have a high level of withstanding from attack and threat if they have been proven. If any organization does not have a well-defined way to manage the system from attack, it will lead to unexpected calamity. Thus, learning from past experience and applying knowledge and best practice to protect the system from unexpected harm from internal and external attack is very important.

A recent study [2] found that security requirements and security analysis should be introduced in an early system development stage because they are the starting point that finally affects the secure state of the system. However, identify a complete and practical security requirements is a difficult and challenge task of an organization. Solving the security problem requires an integration of all security aspects into overall system lifecycle. In requirements engineering process, we can identify security requirements from security expertise and experienced developer. In practice, it is rather difficult to have security knowledge from new employees, so the novices do not know unexpected pitfall or side effect. However, the solution of this problem is contributed by security patterns [2] which are collected the necessary guidelines help implement security policies.

Security patterns represent proven and practiced experience with security concern and reuse solution to recurring problems that can be implemented in many different ways, so that developers can understand and concentrate on the problem and the solution. With patterns, developers are more confident of avoiding problems or resolving well and novice can solve problems in a structured way [3].

Even though, security patterns provide such significant benefits, developers have to spend a lot of time to study and apply it to the real business situation. Moreover, we always cannot use a single security pattern to help resolve complex security problem. Security patterns are usually integrated into another appropriate pattern to solve another problem. So, it is quite difficult to apply in a real case. One possible solution is to develop a tool that supports a mapping mechanism from security patterns to security requirements specification of the system. Thus, the purpose of this research is to build a grammar in an extended-BNF form from security patterns in order to translate from security needs of any projects or organizations to system security requirements. Also the prototype of software tool is also proposed based on our proposed grammar.

The remainder of the paper is organized as follows. Section 2 provides an overview of related works. Section 3 provides a brief overview of security requirements, patterns and security patterns. Section 4 presents our approach for constructing grammar of security patterns. Section 5 presents a supporting tool development. Finally, section 6 presents our initial findings and highlights the future works.

2. RELATED WORKS

There are various researches concern how to define security requirements and present methodologies to tackle challenge problems in security field. For example, [4] presents complex and diverse Characteristics of Certification and Accreditation (C&A) security requirements and related domain knowledge. They apply their methodology to build problem domain ontology from regulatory documents enforced by the Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP). This methodology is useful for technicians or experienced users who know security requirements of a system. However, they must know keyword which is a key for mapping related security requirements and security aspects. Users who use this methodology have to spend a lot of time to learn all keywords in order to improve usability.

In another research, SQUARE [5] proposes nine steps that generate a final deliverable of categorized and prioritized security requirements. This research is useful for experience participants and large-scale design project. Although they propose a template used to gather the requirements and the steps to operate them, this methodology still needs developer with vast amount experiences with system security to define security requirements. Thus, under cost and time limitation, it is quite difficult to apply this approach.

Then, [6] proposes refining security requirements from business to technology, leveraging the concepts of Service-Oriented Architecture (SOA) and Model-Driven Architecture (MDA) and transforming to more detailed ones or countermeasures by bridging the gap between them using best practice patterns. This research can solve the gap between business requirements and security technology contributed by pattern. This research motivates us to use pattern as a middleware to get security information from user to define security requirements.

[7] proposes the real-time specification patterns in terms of three commonly used real-time temporal logics and offer a structured English grammar that mainly supports real-time properties. This research paper and the two books named, “Security pattern” by [2] and “Security Engineering Patterns” by [3] motivate us to create a mechanism to help developers define security requirements of the system.

3. BACKGROUND

In this section, we provide the essential backgrounds knowledge in security and pattern which are a fundamental of our research. It is compose of goal of security, security requirements, patterns, software patterns, and security patterns.

3.1. GOAL OF SECURITY

Security goal is aim to protect assets from harm and operate them into security requirements, which take the form of a set of constraints on the functional requirements sufficient to protect the assets from the harms identified [8]. The security mechanism perspectives that can prevent the attack, detect the attack, or recover from the attack can be used together or separately. Each strategy is descripted by the following:

Prevention means that an attack will fail if we can protect an asset from harm. For example, if one attempt to break into a host over the Internet and that host is not connect to the Internet, the attack has been prevented. Typically, prevention involves implementation of mechanisms that user cannot override and that are trusted to be implemented in a correct and unalterable way, so that attacker cannot defeat the mechanism by changing it.

Detection is the most useful when an attack cannot be prevented, but it can also indicate the effectiveness of preventative measures. Detection mechanisms accept that an attack will occur. The goal is to determine that attack is under way, or has occurred, and reports it. The resource protected by the detection mechanism is continuously or periodically monitored for security problems.

Recovery has two forms. First is to stop an attack and the second is to assess and repair any damage caused by attack. For example, if the attacker deletes a file, one recovery mechanism would be to restore the file from the backup tape. In practice, recovery is far more complex because the nature of attack is unique. Moreover, the attacker may return. In all these cases, the system functioning is inhibited by the attack. By definition, recovery requires assumption of correct operation.

In the second form of recovery, the system continues to function correctly while an attack is under way. This type of recovery is quite difficult to implement because of the complexity of computer systems. It draws on techniques of fault tolerance as well as techniques of security and it typically used in safety-critical system.

3.2. SECURITY ENGINEERING

Security engineering means to put security theory into security requirements [3]. The main objective of security engineering is to change from a state of danger to a state of acceptable risk. As illustrated in figure 1, several iterations including the following steps might be necessary:

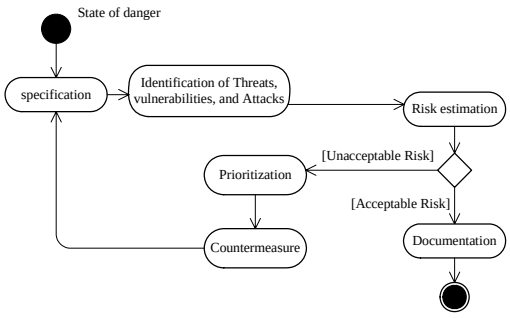


Figure 1. Security engineering approach

1.) Specification. All components and interfaces of the system have to be determined completely. If the specification of the system architecture does not cover all relevant components, some threats, vulnerabilities, and attacks may not be identified later.

2.) Identification of threats, vulnerabilities and attacks. The basic threats and vulnerabilities for each component and interface of a system have to be identified. These help determine the corresponding attacks which can be expected.

3.) Risk estimation. The risk for potential attack has to be determined for all components and interfaces. Hereby, bias effects as a result of relationships between specific threats, vulnerabilities and attacks should be considered.

4.) Prioritization. If a particular risk is too high, the corresponding vulnerabilities have to be prioritized. Vulnerabilities of a particularly jeopardized component or interface get a high priority. This step is very important in order to get an efficient order for carrying out the countermeasures.

5.) Documentation. If a particular risk is acceptability. The documentation must be done. It can be helped the project manager to archive and use to track the progress of asset risk among consecutive risk assessments.

Appropriate countermeasures that eliminate the identified threats, vulnerabilities and attack or at least minimize their effects have countermeasures to be selected and carried out. Thereby, the requirements of the owner of the system have to be considered (e.g. costs, usability, performance, etc.)

Solving a security problem requires incorporate of all security aspects into the overall system life-cycle. For the following discussions we look at an engineering scenario where we can observe different responsibilities and backgrounds of people who solve a security problem together. As indicated in figure 2, it is basically possible to assign security engineering steps to system engineering steps.

Figure 2 shows the subsequent phases of security engineering and system engineering on the axes of the diagram. It is confirming that security is concerned in all phases of system engineering. The bubbles show possible overlap of the two processes that security engineering and system engineering are not integrated yet because there is no defined integrated process today that is commonly accepted.

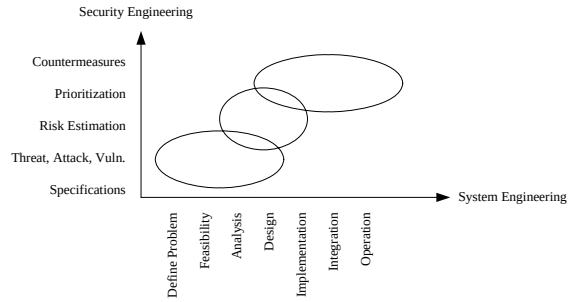


Figure 2. Security engineering approach [3]

We should pay attention in early phases of security engineering and system engineering because the state of danger many occur in early phases. We can prevent it before it could come more danger and cost in later phases. Our approach mainly supports the integration of both in security engineering and system engineering which concentrates on specification phase and threat, attack and vulnerabilities specification phase in security engineering principle and on define problem phase, feasibility phase and analysis phase in system engineering. This integration help reduce threats and vulnerabilities that possible occur in system development process by applying security requirements.

3.3. SECURITY REQUIREMENTS

A security requirement is one of functional requirements under the product quality metric [9]. Security requirements tend to be even more standardized than their security mechanisms such as ISO17799 which is direct descendant of the British Standard Institute (BSI) Information Security Management Standard BS7799. ISO17799 is published by the International Organization for Standardization in December 2000 [10]. Security requirements are characterized as the preservation of Confidentiality, Integrity and Availability. Confidentiality is an ensuring that information is accessible only to those authorized to have. Integrity is a safeguarding the accuracy and completeness of information and processing methods. Availability is an ensuring that authorized users have access to information and associated assets when required.

Security requirements are categorized by D.Firesmith, there are presented here in a shot descript as follow:

Identification is the degree to which a thing identifies its externals before interacting with them.

Authentication is the degree to which something verifies the asserted identity of its externals before interacting with them.

Authorization is the degree to which access and usage privileges of authenticated externals exist and are enforced.

Immunity is the degree to which a thing protects itself from infection by unauthorized malicious programs.

Integrity is the degree to which communications or components are protected from intentional corruption.

Intrusion Detection is the degree to which attempted or successful access or modification by intruders is detected, recorded, and notified.

Non-repudiation is the degree to which a party to an interaction is prevented from successfully denying having participated in all or part of the interaction.

Privacy is the degree to which sensitive data and communications are kept private from unauthorized individuals and programs

Security Auditing is the degree to which security personnel are enabled to audit the status and use of security mechanisms by analyzing security-related events.

System Maintenance Security defines system to have information security control cooperation

Security requirement can be quality requirement that specifies a required amount of security in terms of a system-specific criterion and a minimum level of an associated quality measure that is necessary to meet one or more security policies [11]. Defining requirements in terms of function leaves out key information: *what* objects need protecting and, more importantly, *why* the objects need protecting [12]. So, we should be applying each security requirement type in situation appropriately in order to achieve the secure state of system.

3.4. PATTERNS

Patterns are loosely structured documents which capture the knowledge of domain experts. As patterns show relations to other patterns, a hierarchy of patterns relation is built which guarantees a sense of complete coverage of the problem space if certain boundary conditions hold. Patterns are useful for both parties that are professional and novice. Professionals can apply existent patterns for handle problem more efficiently. They help improve the skill of novices. Less experience developers can solve problems in a structured way, without missing side-effect and being sure that no piece of available expert knowledge has been missed.

The original idea of patterns was laid down by C. Alexander [13] in context of urban planning and building. Alexander and his team identified patterns that are ordered, beginning with the very largest building, building room and alcoves and ending with details of construction. Furthermore, they identified the context-problem-solution structure of patterns, known as the Alexandrian form.

3.5. SOFTWARE PATTERN

However, the previous patterns which known as the Alexandrian form are inadequacy for software development. Because patterns, which are applied require more than context-problem-solution structure. W. Cunningham and K. Beck were first team that applied the pattern approach to software development. In 1987, they decided to have an experiment with a couple of their patterns for user interface design with Smalltalk during a consulting job. Eventually, staff members of their customers could finish a problematical design with this small collection of patterns.

In 1991 and 1992, B. Anderson arranged a workshop at OOPSLA where many key figures of the pattern community met together. At the same time, the Gang of Four (GoF) worked on compilation of patterns that was being discussed by the growing pattern community. After that, the GoF finished the work on their patterns and publish the textbook “Design Pattern – Elements of reusable Object-Oriented Software” [14]. And another book is “Pattern Oriented Software Architecture – A System of Patterns”, known as POSA book was presented next, which written by leading practitioners in software development.

3.6. SECURITY PATTERN

J. Yoder and J. Barcalow presented the first research in security pattern [15]. They included a variety of patterns useful in different aspects of security. They used the GoF template to describe security aspects and to structure their patterns as a pattern language.

Security patterns describe a particular recurring security problem that arises in specific contexts, and presents a well-proven generic solution for it. The solution consists of a set of interacting roles that can be arranged into multiple concrete design structures, as well as a process to create one particular structure [2], [3]. However, security patterns are structured patterns which are rather different such as pattern components from design pattern. The list of patterns elements components is illustrated in table 1.

Table 1 indicates some differences between original design patterns by [14] and security patterns by [2]. Checking symbol (✓) indicates that component is a member of pattern, and cross symbol (×) indicates that component does not occur in pattern. Some components of security pattern have the same name with design pattern while some elements have difference names.

In [2], they proposed forty-six patterns which categorized into eight groups of patterns. They are 1) Enterprise Security and Risk Management, 2) Identification and Authentication (I&A), 3) Access Control Models, 4) System Access Control Architecture, 5) Operating System Access Control, 6) Accounting, 7) Firewall Architecture and 8) Secure Internet Applications. In our research scope, we select four groups that as shown in table 2 based on their widely use as security policies in many organizations. Moreover, these patterns are basic patterns can be used with other security requirements and may be applied with other security patterns in order to solve the specific security problems.

Table 1 Compare document pattern components between software design patterns and security patterns

Document Patterns	Design Pattern (By GoF)	Security Patterns (by M. Schumacher et. al)
Pattern name	✓	✓
Also Known As	✓	✓
Motivate	✓	Problem
Intent	✓	×
Consequence	✓	✓
Related pattern	✓	See also
Known Use	✓	Example
Sample Code	✓	Solution
Applicability	✓	Context
Implementation	✓	✓
Structure	✓	✓
Participants	✓	×
Collaboration	✓	×
Dynamic	×	✓
Example Resolved	×	✓
Variants	×	✓

Table 2. Lists of security patterns used in the research scope

Pattern Category	Patterns
Enterprise Security and Risk Management	• Security Needs Identification for Enterprise Assets • Asset Vulnerability • Threat Assessment • Vulnerability Assessment • Risk Determination • Enterprise Security Approaches • Enterprise Security Services • Enterprise Partner Communication
Identification and Authentication	• Identification and Authentication Requirements • Automated Identification and Authentication Design Alternatives • Password Design and Use • Biometric Design Alternatives
Access Control Models	• Authorization • Role-Based Access Control • Multilevel Security • Reference Monitor • Role Rights Definition
Firewall Architecture	• Packet Filter Firewall • Proxy-Based Firewall • Stateful Firewall

4. OUR APPROACH

We provide an overview of our framework for constructing security grammars from security patterns in order to define security requirements as shown in figure 3.

Security patterns from [2] are sources of our approach. We analyze the structure which one of security pattern elements of each pattern to obtain the pattern components and their relations which will be presented in tree diagram. Then, the grammar, in the extended-BNF form, used to construct security requirement is created based on the pattern component and their relations. Next, grammar validation must be processed to improve the quality of defined grammar.

4.1 THE ANALYSIS OF SECURITY PATTERN STRUCTURE

This process starts from analyzing each pattern in order to find the components and their relations. Almost security patterns defined in [2] have structure that shown components and their relations, some patterns that do not provide, we must consider and create by ourselves. When the pattern does not have structure, we should consider some important elements such as *Dynamic*, *Example Resolve*, and *Solution*. *Dynamic* indicates what run-time behavior of pattern should be and when there is an appropriate situation to apply. *Example Resolve* indicates examples or scenarios which applicable by pattern and other important aspect for resolving the pattern. *Solution* indicates the solution principle underlying the pattern. After that, we consider the keyword from the content of all components in a specific pattern and their relations in order to construct the extended-BNF.

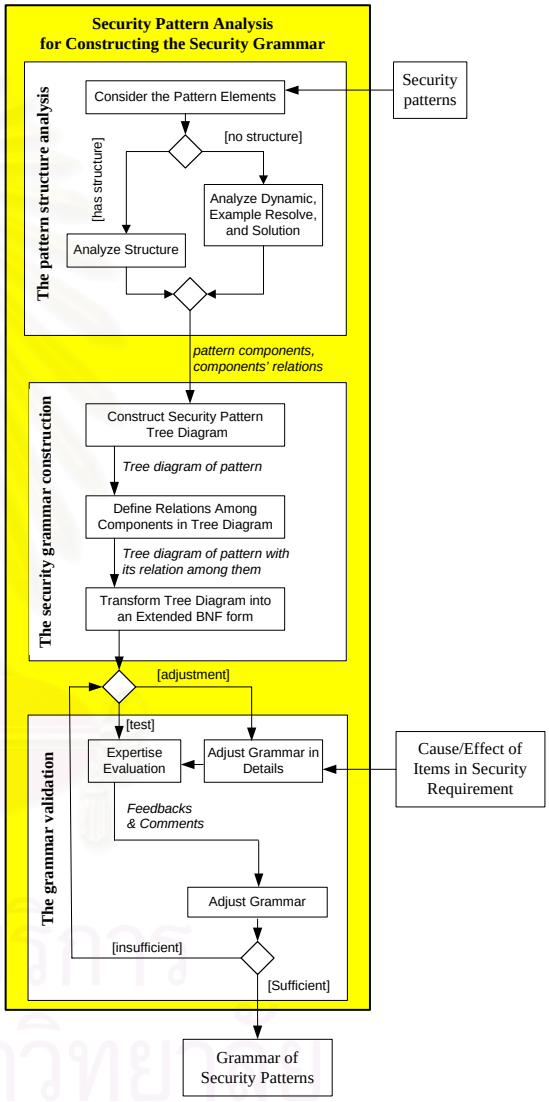


Figure 3. The security grammar constructing framework

In order to clarify our approach, we present a single example of an authorization pattern which one of security patterns. This pattern describes who is authorized to access specific resource in a system, in an environment which we have resource whose access needs to be controlled. It indicates, for each active entity that can access resource, which resources it can access, and how it can access them. Figure 4 shows items and their relation in authorization pattern using UML class diagram. The authorization pattern has three items as

Subject, *ProtectionObject* and *Right*. The relation among *Subject* and *ProtectionObject* is many to many relationships and controlled by right.

From figure 4, we could analyze and give the description of authorization pattern as follows. *Subject* is something or someone tries to access *ProtectionObject*. *ProtectionObject* is function, process, data or etc. which is accessed by *Subject*. *Right* is the permission or constraint granted by security administrator according to his/her role in a particular project when *Subject* tries to access *ProtectionObject*.

Right checking for *Subject* who tries to access *ProtectionObject* is done by *CheckingRight*. It verifies the required information for access i.e. *Access_Type*, *Predicate*, and *Copy_Flag*. *Access_Type* is a type of accession of Subject that provides by admin such as read, write or modify. *Predicate* is a necessary information to identify the subject in order to know who tries to access *ProtectionObject*. *Copy_Flag* is similar to delegation. Particularly, the value of *Copy_Flag* should be true or false.

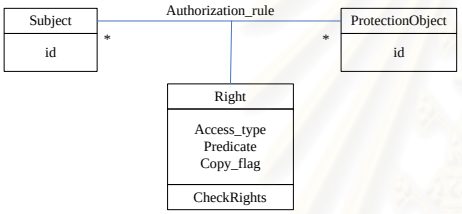


Figure 4. The structure of authorization security pattern [2]

In summary, this step intends to analyzes a structure of pattern and give the results as pattern components and their relations. These results are input for a later step. Although, some of security pattern does not provide a structure so we will pay attention to three components of pattern which are dynamic, example resolve and solution of security patterns in order to find keywords and their relations.

4.2 The Security Grammar Construction

Figure 4, we obtain three initial component classes and their relations. In this step, we will transform the structure of authorization pattern into tree diagram. The symbols used to represent pattern components and relation among them are defined as follows: rectangle symbol (▭) is a terminal node that means component value has been known or no any sub-components inside, circle symbol (○) is unknown value or has sub-components inside. In order to present the component information, we apply attack tree symbols which are defined by [5]. We use AND symbol and OR symbol. The AND symbol (◠) shows that above component is composed of all sub-components, and OR symbol (△) shows that above component is composed of an only one alternative sub-components. Then, we present items and their relations of authorization pattern in a tree diagram as shown in figure 5. We use numeric superscript attached above the item in a tree diagram. An asterisk (*) superscript denotes zero or more repetitions and a plus (+) superscript indicates one or more repetitions.

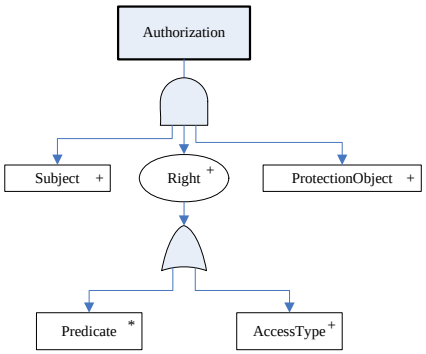


Figure 5. A grammar tree of authorization security pattern

In figure 5, Authorization must be composed of *Subject*, *Right* and *ProtectionObject* which are occur at least one. The *Right* alternates between *Predicate* and *AccessType* or composed of both of them. *Predicate* is optional, but *AccessType* must be occurred at least one. From this tree diagram, we can transform it to an extended-BNF as shown in figure 6. The reason of transformation is to provide security grammars in the extended-BNF format. They can be used to develop an automate tool for security requirement generating which will be presented in section 5.

```
<Authorization> ::= <Subject> <Right> <ProtectionObject> “.”
<Subject>       ::= Subject_Name
<ProtectionObject> ::=  Object_Name
<Right>          ::= <Predicate>|<AccessType>
<Predicate>     ::= {Predicate_statement}*
<AccessType>    ::= “can”|“cannot” “read”|“modify”
```

Figure 6. An extended-BNF of authorization security pattern

Figure 6 shows a grammar of authorization pattern in an extended-BNF format which creates from authorization pattern. In this example, *Subject* and *ProtectionObject* are known value components that predefined by user *and Predicate_statement* is also defined by user. The using of this pattern may be integrated to other patterns in order to solving the security problem. They must follow the project policy for right assignment to access system components. According to project policy of this example, *AccessType* have four types as follows: ‘can read’, ‘can modify’, ‘cannot read’ and ‘cannot write’.

In order to illustrate the applicability of our approach, we apply our grammar to some examples of security requirements from industry. In this paper, we apply our defined grammar to the hospital system. In a medical information system, we usually keep authorization access right to sensitive information about patients. Unrestricted disclosure of this data would violate the privacy of the patients, while unrestricted modification could jeopardize the cure for the patients. Thus, developers have to pay attention to authorization requirements in order to indicate for each active entity that can access resource, which resource who can access and how. In this example, only doctor and nurse who are responsible

for a specific patient can modify patient records. An example of authorization requirements that generated from the defined grammar and security requirements (policies) presented in figure 7.

```
Doctor and Nurse   can modify      patient records.
Pharmacist          cannot modify   patient records.

|----<Subject>----|----<Right>-----|--<ProtectionObject>-|
```

Figure 7. An example of security requirements generated from authorization grammar in extend BNF format

In summary, this step produces the extended-BNF from security pattern in order to define security requirements.

4.3 THE GRAMMAR VALIDATION

This propose of grammar validation is to validate our grammar whether it provides an adequate coverage for common security requirements which should be used to describe security requirements aspects of the IT system environment.

Figure 8 describes relations among aspects of security requirements as cause and effect between them. It helps review the grammar generated in the previous stage whether it covers the necessary security aspects. There are three main objectives. The first objective is to validate aspects which obtain from a security pattern whether it conforms to the characteristic of aspects in security requirements. For example, authorization pattern uses asset information in order to define authorization requirements. So, asset information should be composed of asset's name, asset's vulnerabilities and asset's threats.

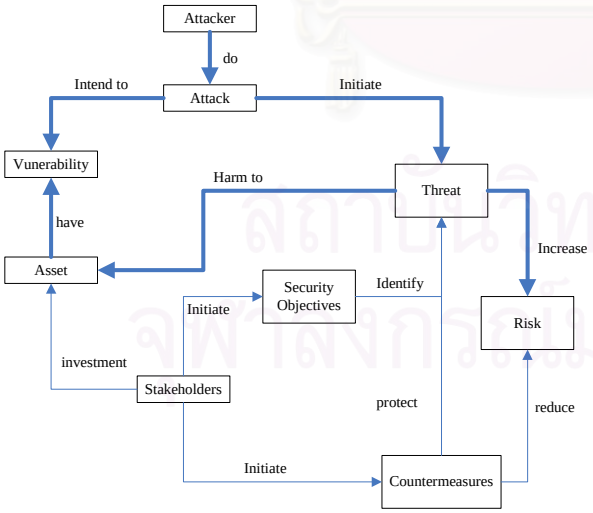


Figure 8. The relations (cause/effect) of aspects in security requirements

The second objective is the consequence of the first objective. Their relations of the entities defined in figure 8 are used as a guideline to elaborate security grammar step-by-step and to check whether there is an additional grammar needed. From the first step of grammar validation, we realize that the necessary information of asset is needed. We cannot define asset information in an authorization grammar because it is out of its scope. Authorization scope is defining authorization requirements for accessing the asset but it does not cover defining the asset information. Thus, if the asset information does not exist we have to use a grammar for defining asset information before using authorization grammar.

The third objective is to clarify the proposed grammar. We should pay attention to the unclear aspects which are obtained from a security pattern. For example, authorization pattern has *Subject* which is unclear aspect because we do not know information boundary of it. [16] proposes right expression which is similar to our authorization grammar. It has a precise definition. We can apply this right expression into our authorization grammar. Figure 9 shows the expansion of *Subject* and *Right* in authorization pattern. *Subject* is expanded to user *(User)* or group of user *(UserGroup)* which has own role. We call both of them as *Session*. Likewise, *Right* is expanded to *Permission* and *Asset*. It shows that some permissions require the asset information in order to achieve the *Right* to access *ProtectionObject*. Moreover, permission is expanded to three types as *Requirement*, *Condition* and *Constraint*. These expansions help significantly reduce the ambiguity of grammar. An improvement of an extended-BNF for authorization is indicated in figure 10.

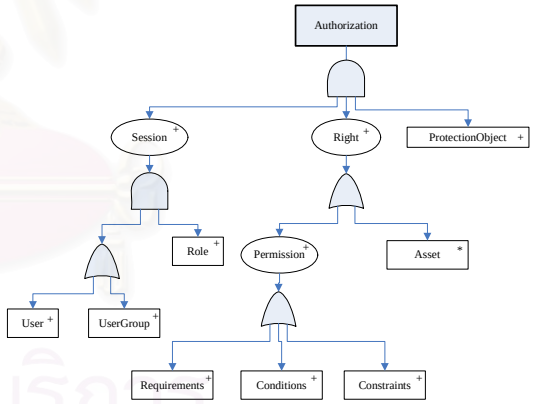


Figure 9. An improvement of a tree represents an authorization security pattern

```
<Authorization> ::= <Session> who acquire <Right>
                    <ProtectionObject>
<Session>       ::= {<GroupUser>|<User>}+ <Role>+
<GroupUser>     ::= {<User>}*
<User>          ::=  User_name
<Role>          ::=  Role_name
<Right>         ::=  <Permission> {<Asset>}*
<Permission>    ::= {<Requirement>|<Condition>|<Constraint>}+
<ProtectionObject>::=  Object_name
<Requirement>    ::= Requirement_statement
<Condition>      ::= Condition_statement
<Constraint>     ::= Constraint_statement
```

Figure 10. An improvement of an extended-BNF of authorization security pattern

In figure 10, we represent an extended-BNF which translates from a tree diagram in figure 9. In order to apply our grammar, we still use requirements from hospital system. An example of improved requirements that support authorization is shown in figure 11.

```
Doctor and Nurse who acquire ModifyRole can read and modify
|-------<user>--------|---------<Role>---------|-----<constraint>-----|

his/her patient record.
|--<ProtectionObject>---|

Pharmacist who acquires ReadRole can read only the patient records.
|----<user>-----|-------<Role>-------|----<constraint>--|---<ProtectionObject>--|
```

Figure 11. An example of an improvement of authorization security requirements

5. A SUPPORTING TOOL DEVELOPMENT

In order to support the applying our grammar to generate security requirements, we propose a prototyping tool for defining security requirements based on our security grammars. There are four main functions as follow:

1.) Security Requirement Type Selection Function. This is the first step for user to select type of security requirements. System provides the list of security types within our scope. When user selects type of security requirements, the system will provide the list of related security patterns for user to select.

2.) Security Pattern Selection Function. When user selects a type of security requirements, user will see the list of security patterns. After user selected a security pattern, the system will display the forms for user to fill in the necessary information. These forms are consistent with our grammar.

3.) Predefined Validation Function. We have previously discussed that some security patterns have to concern with another patterns to help define a more complete and unambiguous security requirements. In practice, user has to define asset from grammar of asset identification in order to use the defined asset information in authorization grammar for determining access right for any assets. Thus, when user selects security pattern to define security requirements, system has to precheck some aspect which must be defined before use a selected grammar. An example of predefine aspect in authorization security pattern are asset's name, Session (user' name who wants to access the protection object) and ProtectionObject (the objects that user try to access). After the system knows the existing assets and session, user is allowed to define authorization requirements.

4.) Requirement Statement Generating Function is a module to generate a security requirements statement from user entering information that is filled in grammar forms from the previous steps.

We illustrate the interaction between user and our tool as shown in figure 12. It shows the sequence of defining security requirements with our prototyping tool.

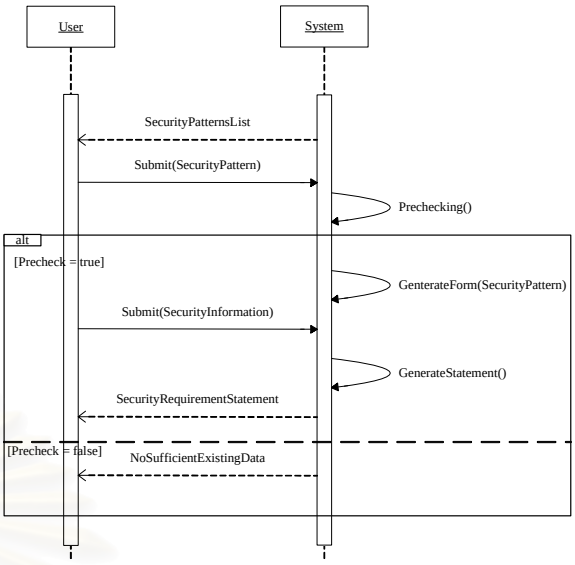


Figure 12. A simple sequence diagram for defining authorization requirements

A simple example GUI is shown in figure 13. It presents GUI of authorization pattern that consistent with our authorization grammar. In order to understand how to define requirements, we will present the process step by step. First, user chooses a security requirement type. Second, user chooses pattern in a scope of a selected security requirements type, then the system presents GUI in a form that automatically generates from our authorization defined grammar. Third, user defines values for the modifiable items. Finally, user defines all essential values. The result of this GUI is the same as the requirement statements that show in figure 11.

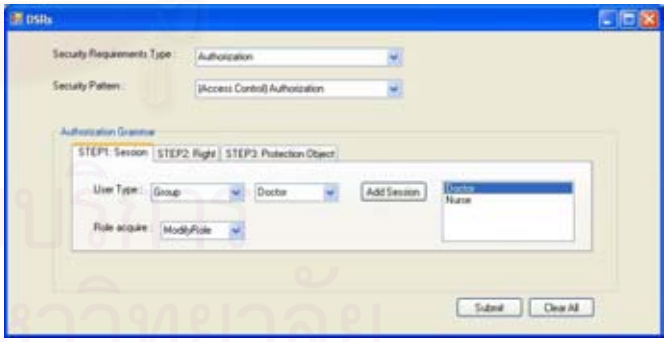


Figure 13. An example of GUI for authorization pattern based on authorization grammar

6. CONCLUSIONS AND FUTURE WORK

Our works propose a grammar in an extended-BNF form for security requirements developments based on security patterns. We also propose a prototyping tool developed based on the proposed grammars. We do not claim that our proposed grammars are perfect or completely. Our research yields two main contributions

in defining system security requirements which always a challenged problem in practice. First, the proposed tool directly enables developers to express the security requirements and properties of the system in a precise way and to earn security requirements of the system in a natural language representation which many used as a fundamental of any organization security view and be improved later. Second, the proposed tool has a feedback feature that developers may put any comments which are used as an important input help improve the existing proposed grammar.

We continue to finish completing grammar construction for all twenty security patterns. It is covered Enterprise Security and Risk management, Identification and Authentication, Access Control Models, and Firewall Architecture. Then, we will validate our proposed grammar by accepting feedback in a formal-defined evaluation form from security domain expert. The feedback helps improve the quality of our grammar in term of completeness and correctness.

7. REFERENCES

[1] International Standard ISO/IEC 17799:2000, Code of Practice for Information Security Management

[2] M. Schumacher, E. Fernandez-Buglioni, D.Hybertson, F. Buschmann and P. Sommerlad, "Security Patterns: Integrating Security and Systems Engineering", John Wiley & Sons, 2005.

[3] M. Shumacher, "Security Engineering with Patterns", Spinger-Verlag Berlin Heidelberg, 2002.

[4] T. Imamura, M. Tatsubori, Y. Nakamura, Christopher Giblin, "Web Services Security Configuration", *Service-Oriented Architecture ACM WWW*, 2005.

[5] N. R. Mead, E. D. Hough and T. R. Stehney II, "Building Trustworthy Applications: Security Quality Requirements Engineering (SQUARE) methodology", *Proceedings of the 2005 workshop on Software Engineering for Secure Systems*.

[6] S. W. Lee, R. Gandhi, D, Muthunrajan, D. Yavagal and G. J. Ahn, "Building Problem Domain Ontology from Security Requirements in Regulatory Documents", *Proceedings of the 2006 International workshop on Software engineering for secure systems*.

[7] S. Konrad, Betty and H.C. Cheng, "Real-time Specification Pattern",*Proceedings of the 27th International Conference on Software Engineering*, 2005

[8] C. B. Haley, J. D. Moffett, R. Laney, and B. Nuseibeh. "A Framework for Security Requirements Engineerin", *Proceedings of the 2006 international workshop on Software Engineering for secure systems SESS '06*.

[9] ISO/IEC 9126: Product Quality Metrics.

[10] ISO/IEC 17799: Code of Practice for Information Security Management.

[11] D.G. Firesmith, "Analyzing and Specifying Reusable Security Requirements", *Journal of Object Technology*, Page 56-68, 2003.

[12] E. Maiwald, and W. Sieglein, "Security Planning & Disaster Recovery", P.82 – 89, McGraw-Hill/Osborne, 2002.

[13] C.Alexander, S. Ishikawa, M. Silverstein, M. Jacobson I. FiksdahI-King, and S. Angel. "A Pattern Language", Oxford University Press, New York, 1977

[14] E. Gamma, R. Helm, R. Johnson, and J. Vlissides, "Design Patterns: Elements of Reusable Object-Oriented Software", Addison-Wesley, 1995.

[15] J. Yoder, J. Barcalow, "Architectural Patterns for Enabling Application Security", *Procerdings of PLoP*, 1997

[16] B. Cooper and P. Montague. "Translation of Rights Expressions", *Proceedings of the 2005 Australasian workshop on Grid computing and e-research*, Volume 44, ACSW Frontiers '05.

Enterprise Assets Security Requirements Construction from ESRMG Grammar based on Security Patterns

Kawin Supaporn, Nakornthip Prompoon and Thongchai Rojkangsadan
Software Engineering Laboratory, Center of Excellence in Software Engineering
Department of Computer Engineering, Faculty of Engineering
Chulalongkorn University, Bangkok, Thailand
Kawin.S@student.chula.ac.th, Nakornthip.S@chula.ac.th, Thongchai.R@chula.ac.th

Abstract

One of the highest priorities of system requirements needed in software development industry is security requirements. However, to identify the complete and correct software security requirements is a challenging task especially creating enterprise assets security requirements. Enterprise assets security requirements are to identify security basic needs, to assess risks, to establish security approach and service, and to specify external enterprise consideration including confidentiality, integrity, availability, and accountability concerns. Moreover, these may be applied to other security requirements such as identification and authentication, access control, firewall architecture, etc. Security patterns may be used to create this security requirements but understanding, analyzing and transforming from security patterns to security requirements are difficult to accomplish. We proposed a grammar, called ESRMG (Enterprise Security and Risk Management Grammar), and a prototyping tool based on security patterns in a scope of enterprise asset identification and risk managements which are the fundamental of enterprise security requirements. The proposed grammar and tool are beneficial for any organization to construct enterprise security requirements and may help reduce cost and time in overall of system development.

1. Introduction

As businesses become more dependent on computers (and more distributed), there is a growing appreciation of the need of security [1], [2]. The most important asset that most businesses hold today is information. This could be information on customers, contracts, personals and products. The security of this information is normally entrusted to business managers. Many of them have little experience in control and protection of information. These managers may also have other responsibilities which relates to security issues. Thus, security knowledge is unavoidable in a managing task.

In software development, requirements engineering process is one of early stages which pay attention to gathering business information and its' requirements from all related stakeholders in order to produce requirement specifications for each project. We have known that security has become an important topic for many software systems. We can imagine such a list of questions of security concern, but how do we define them into security requirements. So, the discrepancy is occurred. For example, how do you identify organization's or system's security needs, and how do you define an appropriate security approach to meet these needs? Is confidentiality a security property you need in your system, or confidentiality, integrity, availability, or accountability? Or even a mixture of the four? And how do you ensure these properties by appropriate means of prevention, detection and response? It is rather difficult to have precise security knowledge from stakeholders and developer team. It is also difficult to have heuristic experience from previous projects to define such security requirements for enterprise assets.

In this paper, we present security grammars which are constructed by our framework [5] from security patterns in a scope of Enterprise Security and Risk Management. Our grammars are supported in requirements engineering that is useful for enterprises to elicit, to define security requirement specifications in a precise way and to manage their assets with security concerns. Moreover, the generated requirements are the fundamental awareness of an organization to select security approaches (prevention, detection, and response) which are driven by security properties (confidentially, integrity, and availability).

2. Background

According to our previous research [5], we have proposed the framework for constructing the security grammar based on security pattern. A slight improvement of our framework is shown in figure 1.

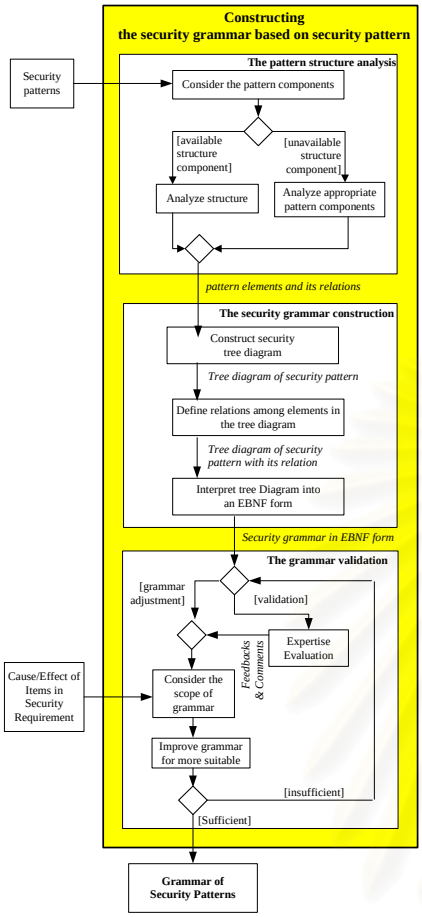


Figure 1. A security grammar constructing framework.

This framework presents security grammars using security patterns from [1] as an input. The result of it is a set of grammars with respect to security patterns which can be used to generate the requirements of the security. This framework consists of three major steps. The first step is the security pattern structure analysis which results in the pattern elements and their relations. The second step is the security grammar construction which uses the result from the previous step to construct grammar trees in order to reveal the hierarchy among elements and their relations. Then, the grammar trees are transformed into an Extended Backus–Naur Form (EBNF) which will be used to create the security requirements. The third step is grammar validation. The purpose of this step is to improve the quality of grammar under the scope of security patterns from domain expert comments and participant feedback.

Schumacher et al. [1] proposed forty-six security patterns cover the enterprise level, the system level and the operational level for any organization to build the security architecture. We pay attention to the enterprise level because the enterprise information security become an increasingly important system quality that must be carefully managed but it is still lack of an adequate support for top management decision making.

Risk determination is also a main part of our research since it helps project manager consider and decide for asset management in any operations required the enterprise assets.

However, the applications of the security patterns for implementation in the real business cases is a difficult task and consume a lot of time and effort to understand their contained specific information.

In this paper, we present security grammars for constructing security requirements based on enterprise security and risk management. These proposed grammars can help user or developer as a guideline to address the enterprise-wide security issues. Moreover, we could apply them as a root of security requirements for all enterprise security concerns [3] and as guidance an enterprise to select appropriate security approaches and services.

3. The Enterprise Security and Risk Management grammars

Enterprise Security and Risk Management consist of eight patterns [1] as shown in table 1. In order to obtain security grammars for these patterns, we recommend to follow the processes presented in our framework. The brief of each grammar are the following:

Pattern Category	Grammar name
Enterprise Security and Risk Management (ESRM)	• Security Needs Identification for Enterprise Assets (SNIEA) • Asset Valuation (AV) • Threat Assessment (TA) • Vulnerability Assessment (VA) • Risk Determination (RD) • Enterprise Security Approaches (ESA) • Enterprise Security Services (ESS) • Enterprise Partner Communication (EPC)

Table 1. List of Enterprise Security and Risk Management Grammar

3.1. Security Needs Identification for Enterprise Assets (SNIEA) Grammar

This is the root grammar for all enterprise security concerns. It helps resolve the issue of whether security is really needed and, if it is, what properties of security should be applied for a particular enterprise. Security properties considered include confidentiality, integrity, availability, and accountability.

3.2. Asset Valuation (AV) Grammar

This grammar determines the overall importance of what an enterprise places on the assets. Loss or compromise of such assets may result in anything from hard costs, such as fines and fees, to soft costs, such as loss of market share and consumer confidence.

3.3. Threat Assessment (TA) Grammar

This grammar defines threats which are the likelihood of, or potential for, hazardous events occurring. They can affect any asset or object on which an enterprise places value. An enterprise threat assessment identifies the threats posed to the enterprise asset, and determines the likelihood or frequency of their occurrences.

3.4 Vulnerability Assessment (VA) Grammar

This grammar defines vulnerabilities which are the weakness that could be exploited by a threat, causing the violation of an asset's security property. Conducting an enterprise vulnerability assessment helps to identify the weaknesses of the enterprise's assets and the systems that enable access to them, and evaluates the severity if vulnerability were to be exploited.

3.5 Risk Determination (RD) Grammar

This grammar is the final stage of risk assessment process. The use of this grammar must incorporate the results from an asset valuation, a threat assessment and a vulnerability assessment. Using the input of these grammars, the enterprise is able to evaluate and prioritize the risks of assets.

3.6 Enterprise Security Approaches (ESA) Grammar

This grammar guides an enterprise in selecting the security approaches, which are driven by the security properties (confidentiality, integrity, and availability) for a specific asset.

3.7 Enterprise Security Services (ESS) Grammar

This grammar guides an enterprise in selecting security services for protecting its assets, after the required security approaches have been identified. It helps establish the level of strength or confidence for each security service should offer, based on priorities. Primary examples of such services are identification and authentication, accounting/auditing, access control/authorization, and security management.

3.8 Enterprise Partner Communication (EPC) Grammar

Enterprises often partner third parties to support their business process. These third parties may include application and managed service providers, consulting firms, vendors, outsourcing development teams, and satellite offices. As part of this relationship, access must be granted to allow data to travel between the organizations. Without attention to the protection of that data and the methods by which they are transferred, one or both organizations may be at risk.

In appendix A, we present all security grammars of enterprise security and risk management with practical examples.

In practice, we cannot define security requirements all at once from these security patterns. In order to apply these security pattern to define enterprise security requirements and risk management, organization should follow the sequence of processes as shown in figure 2.

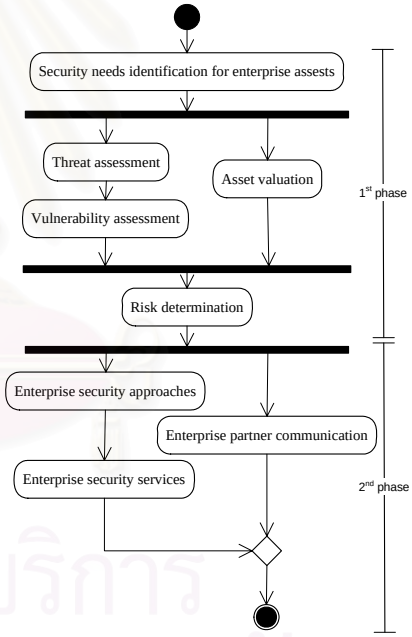


Figure 2. The Enterprise Security and Risk Management Flow

First of all, we must identify asset information using SNIEA grammar. Then, we use this asset information to determine its value from AV grammar and its threat from TA grammar. The vulnerability assessment is a next step from threat assessment to determine severity scale of vulnerability for a single threat using VA grammar. The last step of the first

phase is risk determination that uses all information gained to calculate the risk value and assign the qualitative risk ratings for overall enterprise assets.

The last three steps are to define enterprise security approaches and services for any asset with related risk consideration. Moreover, we could apply those approaches and services to specify the external enterprise communication. These operations are supported by our grammar such as the security requirements construction for enterprise security approaches and services by ESA grammar and ESS grammar, and external enterprise communication requirements by EPC grammar.

We concentrate on RD grammar because it is the final process of a risk assessment process (1st phase as shown in figure 2). Then, we can use the result of it as a guideline to consider the asset management with security concern in later phase.

4. Risk Determination in Security Patterns

Risk determination is the final stage of a risk-assessment process, and incorporates the results from an asset valuation, a threat assessment and a vulnerability assessment [7]. Using the outputs of these grammars, the enterprise is able to evaluate and prioritize risks.

Risk determination mainly concern with the evaluation of the three factors: 1) the threat that can affect an asset 2) the vulnerabilities that can be exploited by a threat 3) the asset value having impacts on an asset. The conceptual illustration is shown in figure 3.

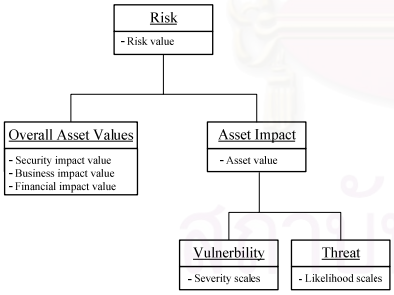


Figure 3. The risk determination factors

All of main factors of risk determination in figure 3 are supported by our grammars. The TA grammar produces threat action and its likelihood scale. The likelihood scale presents in numeric estimation based on six ratings defined by [8]: Extreme, Very High, High, medium, Low and Negligible.

The VA grammar produces vulnerabilities and their severity scale for each threat action. There could be several vulnerabilities for one threat. However, there are several variations of severity scale. CERT [9] uses a purely quantitative scale of 0 to 180 for ranking the severity of vulnerability but they did not present the qualitative values. In our grammar, we use the CVSS [10] which is an open framework that can be used by any security or application. They also propose a six rating system.

The AV grammar produces asset name and its overall importance value of three sub-factors. They are security value, business impact value and financial value. All of them have to later translate qualitative value into six rating scales. The ratings may be modified according to the preference of the enterprise or followed to standard such as NIST SP800-30 [11] and ISO/IEC 17799:2000 [12].

Asset Impact Factor is produced the summation of all severity of vulnerabilities for each threat that affects on an asset. The asset impact value for one asset can be computed from the following equation:

$$Asset\ Impact = \sum_{1}^{t}\sum_{1}^{s}(ThreatLikelihood_{t} \times Vuln.Severity_{ts})$$

When, ***ThreatLikelihood*** presents a qualitative value in numeric estimation for the frequency of threat occur. ***Vuln.Severity*** presents a qualitative value in numeric estimate of severity scale for which threat exists. ***t*** is a number of threat for each existing asset. ***s*** is a number of vulnerability for which threat exists.

The Risk Value for each asset is the asset value multiply by the asset impact value. So, the risk value for one asset is

$$Risk = AssetValue \times AssetImpact$$

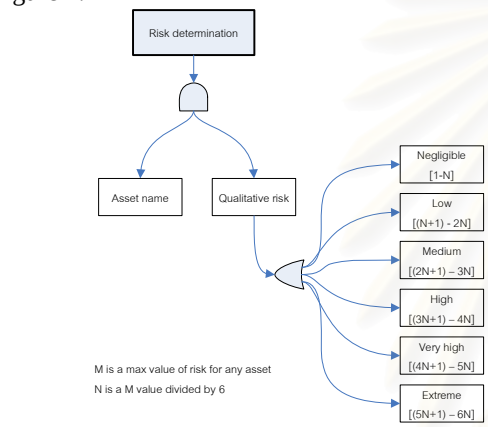
The presentation of computation results, six equally divided ranges have been created in order to indicate the qualitative security scale. For example, the computation risk value of one enterprise, the lowest value of asset risk value is 1 and the highest value is 786. Thus, the six-equal intervals of each qualitative risk level are shown in table 2.

Table 2. An example of qualitative risk translation

Level	Level/Qualitative Value	Example of Risk Value
Extreme	6	656-786
Very high	5	525-655
High	4	394-534
Medium	3	263-393
Low	2	132-262
Negligible	1	1-131

5. Risk Determination Grammar

In order to obtain RD grammar, we start constructing a grammar tree that can reveal the relationship among elements and indicate the degree of relationship. However, we use only symbols which according to ISO standard ISO/IEC14977:1996 [13] for EBNF. We use a plain arrow, if it is a one-to-one relationship, an arrow with a plus (+) symbol, if it is a one-to-many relationship. We use 'AND Gate' to indicate that the above element must consist of all under elements and 'OR Gate' to indicate that above element may consist of some alternative elements of all under elements. The grammar tree diagram and example of EBNF for Risk Determination is shown in figure 4.



Risk-determination = "The qualitative risk for" , Asset-name , "is" | "are" , Quality-risk , "." ;

Asset-name = ? The asset name which defined by SNIGA grammar ? ;

Quality-risk = "negligible" | "low" | "medium" | "high" | "very high" | "extreme" ;

Figure 4. Grammar of Risk Determination

The result of this grammar determines the six-level risk for each asset of an enterprise. Such as "*The qualitative risk for patient records is extreme*". Extreme is a qualitative value computed by using our proposed tool which will be presented in case study.

6. Case study

We use the threat-vulnerability for asset in netcentric environment as an example of risk determination because it is widely applied in any enterprise. The basic netcentric environment is shown in figure 5.

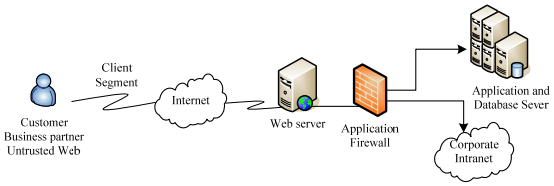


Figure 5. The netcentric environment

In order to elaborate our approach, a selected security domain expert explores our grammar and also identifies the value of three main assets, likelihood of threats and severity level of vulnerabilities. From the expert evaluation, the asset value of database server, web server and login member information are six, five and five respectively. The rest of the values are shown in table 3.

Table 3. Threat-vulnerability for netcentric assets

Threat action	Likelihood Scale	Vulnerability	Severity Scale
Application and Database Sever			
ID and password was takeover	4	Inadequate hardware control	4
		Encryption devices do not used	5
		Poor password management program	4
Data entry error	5	Lack of data validation from input process	2
Leaking confidential information	3	Exposure information asset	3
Theft of information	3	Susceptibility of employee to bribery	3
		Lack of proper physical controls for document storage (lock, safe)	4
Web sever			
Sever down	3	Inadequate audit trail review of system activity	3
		Lack of monitoring devices to detect unauthorized intrusions	4
Unauthorized access system	5	Full audit trail is not implemented	4
		Departing employees' system access privileges are not immediately revoked.	3
		Individual passwords are not unique or contain few characters.	5
		Poor password management program	4
Data entry error	5	Lack of data validation during from input	3
Member Information			
ID and password was takeover	4	Inadequate hardware control	4
		Encryption devices do not used	5
		Poor password management program	4
Data entry error	5	Lack of data validation from input process	3
Theft of information	3	Susceptibility of employee to bribery	3
		Lack of proper physical controls for document storage (lock, safe)	4

According to risk determination equation that proposed in section 4, risk of application and database server can be written as follows:

$$Risk_{(ApplicationAndDatabaseSever)} = AssetValue_{(ApplicationAndDatabaseSever)} \times AssetImpact_{(ApplicationAndDatabaseSever)}$$
$$Risk_{(ApplicationAndDatabaseSever)} = 6 \times [(4 \times 4) + (4 \times 5) + (4 \times 4) + (5 \times 2) + (3 \times 3) + (3 \times 3) + (3 \times 4)]$$
$$Risk_{(ApplicationAndDatabaseSever)} = 6 \times [16 + 20 + 16 + 10 + 9 + 9 + 12]$$
$$Risk_{(ApplicationAndDatabaseSever)} = 6 \times 92$$
$$Risk_{(ApplicationAndDatabaseSever)} = 552$$

In a similar computation, web sever and member information risk values are 580 and 440 respectively. We assume that the netcentric environment has the qualitative ranges as shown in table 2. Consequently, the qualitative risk value of these asset are in a very high level for database sever and web sever, and in a high level for member information.

These qualitative values of each asset can guide the user or developer to pay attention to planning and building security control of enterprise assets with appropriate technical control in order to achieve a good security level, specified security profile, best practice, and enterprise policy.

7. Conclusion

Before an enterprise can protect its assets, information about what assets it owns and what type of protection they need must be realized. We propose the security grammars in a scope of the enterprise security and risk management. They are beneficial to help organization or developer to define security requirements specification. These grammars are composed of Security Needs Identification for Enterprise Assets, Asset Valuation, Threat Assessment, Vulnerability Assessment, Risk Determination, Enterprise Security Approaches, Enterprise Security Services and Enterprise Partner Communication. These are the root grammars for all enterprise security concerns. The risk determination grammar in this paper assists in deciding how much protection is needed for each business asset type and a support formal way of accounting them.

8. Future works

We continue to validate and improve our grammars from security domain experts in different aspects. We also improve the supporting tool in order to increase its flexibility in automatic providing the necessary basic information needed for security requirements specification. Moreover, the generated results from our tool will be formally evaluated by some participants who have experience in security area. A collected feedback will be analyzed to improve tool quality.

Some parts of our tool allow users to define some information by themselves. These may lead to invalid input information type. This is a weak point of our tools. So, we continue to add some appropriate constraints to avoid this problem.

9. References

[1] M. Schumacher, E. Fernandez-Buglioni, D. Hybertson, F. Buschmann and P. Sommerlad, *Security Patterns: Integrating Security and Systems Engineering*, John Wiley & Son Ltd, England, 2005.

[2] Dean Adams, *Security Survival: A Source Book from the Open Group*, X/Open Company Ltd, UK, 1996.

[3] M. Schumacher et al, *Security Engineering with Patterns: Origins, Theoretical Model, and New Applications*, Springer, Germany, 2003.

[4] S. Konrad and B. Cheng, "Real-time Specification Patterns", *International Conference on Software Engineering*, ACM, USA, 2005.

[5] K. Supaporn, N. Prompoon and T. Rojkangsadan, "An Approach: Constructing the Grammar from Security Pattern", *International Joint Conference on Computer Science and Software Engineering*, Thailand, 2007.

[6] M. Schumacher, *Security Engineering with Patterns* Spinger-Verlag Berlin Heidelberg, 2002.

[7] CCTA, *CRAMM User's Guide (Version 2.0)*, The UK Central Computer and Telecommunications Agency, 1991.

[8] D. S. Herrmann, *Security Engineering and Information Assurance*, Auerbach Publication, USA, 2002.

[9] US-CERT, *Vulnerability Note Field Description*, Carnegie Mellon University, USA, 2002 http://www.kb.cert.org/buls/html/fieldhelp.

[10] Common Vulnerability Scoring System, 2005 http://www.first.org/cvss.

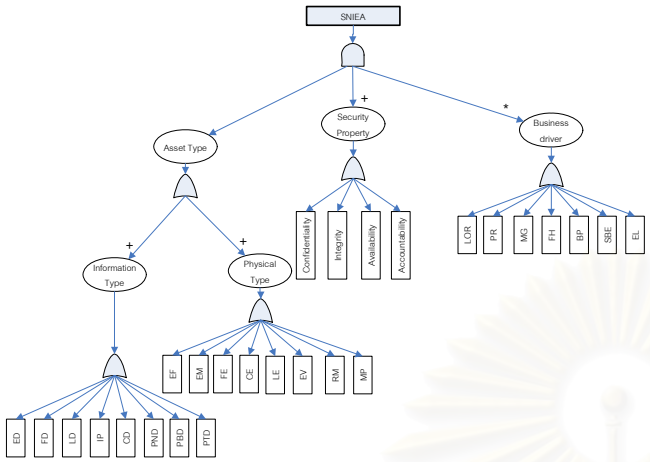
[11] G. Stoneburner, A. Goguen and A. Feriga, *Risk Management Guide for Information Technology System*, NIST Special Publication SP800-30, National Institute of Standards and Technology (NIST), 2001.

[12] International Organization for Standardization, *Information Technology Code of Practice for Information Security Management ISO/IEC 17799:2000*, re-released 2005.

[13] ISO/IEC14977:1996, *Information technology-Syntactic metalanguage-Extended BNF*.

Appendix A

The Security Needs Identification for Enterprise Asset Grammar (GM61)



SNIEA = Asset-Type, "require" ,Security-Property-List, "under the auspices of", Business-Driver-List, ".";

Asset-Type = Information-Type-List | Physical-Type-List | User-Type-List ;

Information-Type-List = Information-Type , {"," , Information-Type } ;

Information-Type = "employee data" | "financial data" | "legal data" | "intellectual property" | "customer data" | "partner data" | "public data" | "protection data" | ? User information type ? ;

Physical-Type-List = Physical-Type , {"," , Physical-Type } ;

Physical-Type = "enterprise facility" | "enterprise employee" | "factory equipment" | "computer equipment" | "lab equipment" | "enterprise vehicles" | "raw material" | "manufactured product" | ? User physical type ? ;

Security-Property-List = Security-Property , {"," , Security-Property } ;

Security-Property = "confidentially" | "integrity" | "availability" | "accountability" ;

Business-Driver-List = Business-Driver , {"," , Business-Driver } ;

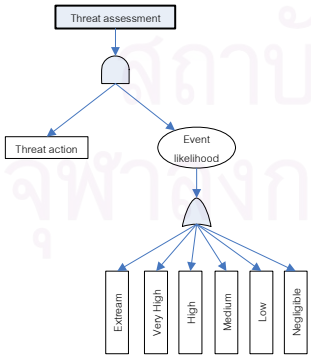
Business-Driver = "laws or regulation" | "partner relations" | "mission and goals" | "financial health" | "business process" | "sensitive business event" | "enterprise location" | ? User business driver ? ;

User-Type-List = ? User information item ? , { "," , ? User information item ? } ;

Example

Employee data, financial data require **confidentially, integrity, accountability** under the auspices of **laws or regulation**.

Threat assessment Grammar (GM63)



Threat-assessment = "The likelihood of" , Threat-action , "is" , Event-likelihood , "." ;

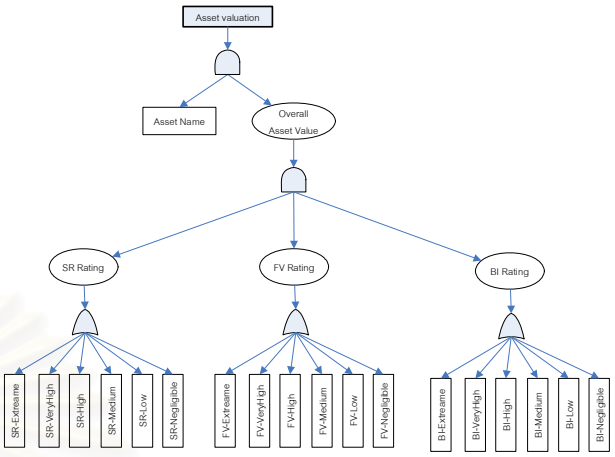
Threat-action = ? Name of threat action is input from user ? ;

Event-likelihood = "extreme" | "very high" | "high" | "low" | "negligible" ;

Example

The likelihood of **Data entry error** for **Museum employee data** is very high.

Asset valuation Grammar (GM62)



Asset-Valuation = "The asset valuation of", Asset-Name, "is" , Rate-of-Security-Requirement, Rate-of-Financial-Value, "and", Rate-of-Business-impact , "So, overall impact value is" Overall-Impact, "." ;

Asset-Name = ? Name of asset from user ? ;

Rate-of-Security-Requirement = Rating , "in security requirement rating," ;

Rate-of-Financial-Value = Rating , "in financial value rating" ;

Rate-of-Business-impact = Rating , "in business impact rating." ;

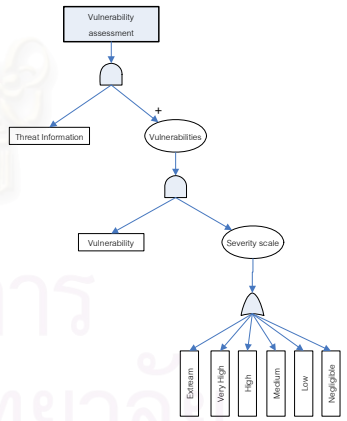
Overall-Impact = Rating ;

Rating = "extreme" | "very high" | "high" | "medium" | "low" | "negligible" ;

Example

The asset valuation of **Museum employee data** is **very high** in security requirement rating, **medium** in financial value rating, and **very high** in business impact rating. So, overall impact value is **very high**.

Vulnerability assessment Grammar (GM64)



Vulnerability-assessment = { "The cause of" , Threat-Information , "is" , Vulnerabilities-List , "." } | { "The causes of" , Threat-Information , "are" , Vulnerabilities-List , "." } ;

Threat-Information = ? Threat information from output of GM63 ? ;

Vulnerabilities-List = Vulnerability , { "," , Vulnerability } ;

Vulnerability = Vulnerability-Action, "which has" , Severity-Scale, "severity level" ;

Vulnerability-Action = ? Name of the vulnerability action is input from user ? ;

Severity-Scale = "extreme" | "very high" | "high" | "low" | "negligible" ;

Example

The causes of museum fire are **failure of fire alarm system** which has **extreme** severity level, **failure of fire suppression system** which has **very high** severity level.

ประวัติผู้เขียนวิทยานิพนธ์

นายกวิน สุภาพร เกิดวันที่ 12 กุมภาพันธ์ พ.ศ.2526 สำเร็จการศึกษาระดับปริญญาตรี หลักสูตรวิทยาศาสตรบัณฑิต เกียรตินิยมอันดับ 2 สาขาวิทยาการคอมพิวเตอร์ ภาควิชาคอมพิวเตอร์ คณะวิทยาศาสตร์ มหาวิทยาลัยสงขลานครินทร์ วิทยาเขตหาดใหญ่ เมื่อปีการศึกษา 2547 และเข้าศึกษาต่อระดับปริญญาโท ในปีการศึกษา 2548 หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิศวกรรมซอฟต์แวร์ ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย