การแสดงแบบรูปความมั่นคงโดยการขยายยูเอ็มแอลเซค

นายเกียรติศักดิ์ ไชยสมบูรณ์

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต
สาขาวิชาวิทยาศาสตร์คอมพิวเตอร์ ภาควิชาวิศวกรรมคอมพิวเตอร์
คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2551

VISUALIZING SECURITY PATTERNS BY EXTENDING UMLSEC

Mr. Kiattisak Chaisomboon

A Thesis Submitted in Partial Fulfillment of the Requirements
for the Degree of Master of Science Program in Computer Science
Department of Computer Engineering
Faculty of Engineering
Chulalongkorn University
Academic Year 2008

หัวข้อวิทยานิพนธ์	การแสดงแบบรูปความมั่นคงโดยการขยายยูเอ็มแอลเชค
โดย	นายเกียรติศักดิ์ ไชยสมบูรณ์
สาขาวิชา	วิทยาศาสตร์คอมพิวเตอร์
อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก	ผู้ช่วยศาสตราจารย์ นครทิพย์ พร้อมพูล

คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย อนุมัติให้นับวิทยานิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญามหาบัณฑิต

.... คณบดีคณะวิศวกรรมศาสตร์
(รองศาสตราจารย์ ดร. บุญสม เลิศหิรัญวงศ์)

คณะกรรมการสอบวิทยานิพนธ์

.... ประธานกรรมการ
(รองศาสตราจารย์ ดร. วันชัย ริ้วไพบูลย์)

นครทิพย์ พร้อมพูล
.... อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก
(ผู้ช่วยศาสตราจารย์ นครทิพย์ พร้อมพูล)

.... กรรมการ
(อาจารย์ ดร.ยรรยง เต็งอำนวย)

.... กรรมการภายนอกมหาวิทยาลัย
(ผู้ช่วยศาสตราจารย์ ดร. ศรัณย์ อินทโกสุม)

เกียรติศักดิ์ ไชยสมบูรณ์ : การแสดงแบบรูปความมั่นคงโดยการขยายยูเอ็มแอลเซค. (VISUALIZING SECURITY PATTERNS BY EXTENDING UMLSEC) อ.ที่ปรึกษาวิทยานิพนธ์หลัก : ผศ. นครทิพย์ พร้อมพูล, 165 หน้า.

งานวิทยานิพนธ์นี้มีวัตถุประสงค์เพื่อสร้างยูเอ็มแอลเซคเอสพีโดยการผนวกยูเอ็มแอลเซคกับยูเอ็มแอลโพรไฟล์ที่สร้างขึ้นใหม่จากแผนภาพคลาส และพัฒนาเครื่องมือสนับสนุนการนำยูเอ็มแอลเซคเอสพีมาประยุกต์ใช้ เพื่อการแสดงแบบรูปความมั่นคงจากแผนภาพคลาส โดยการวิเคราะห์องค์ประกอบของแบบรูปความมั่นคง 27 แบบรูป จาก 5 ประเภทแบบรูปความมั่นคงได้แก่ แบบจำลองการควบคุมการเข้าถึง สถาปัตยกรรมการควบคุมการเข้าถึง การควบคุมการเข้าถึงระบบปฏิบัติการ สถาปัตยกรรมไฟร์วอลล์ และการประยุกต์ใช้ความมั่นคงบนอินเตอร์เน็ต เพื่อหาข้อมูลทางโครงสร้างและข้อมูลทางความมั่นคงของแบบรูปความมั่นคงที่ใช้ในการสร้างยูเอ็มแอลเซคเอสพีให้ครอบคลุมการแสดงข้อมูลของแบบรูปความมั่นคงดังกล่าว โดยมีการตรวจสอบยูเอ็มแอลเซคเอสพีตามคุณสมบัติมาตรฐานของยูเอ็มแอลโพรไฟล์

เครื่องมือสนับสนุนการแสดงแบบรูปความมั่นคงถูกพัฒนาขึ้นบนพื้นฐานของยูเอ็มแอลเซคเอสพี โดยผลลัพธ์ที่ได้จากการใช้เครื่องมือคือ แผนภาพคลาสของแบบรูปความมั่นคงที่ใช้ยูเอ็มแอลเซคเอสพี ซึ่งผู้ใช้สามารถนำไปประยุกต์ใช้ในการออกแบบความมั่นคงของระบบต่อไปได้

ในการประเมินความซับซ้อนของแผนภาพที่ใช้ยูเอ็มแอลเซคเอสพี ได้ใช้ตัววัดความซับซ้อนของแผนภาพในการเปรียบเทียบระดับความซับซ้อนของแผนภาพคลาสทั้งสามลักษณะ คือ แผนภาพคลาสที่ใช้ยูเอ็มแอล แผนภาพคลาสที่ใช้ยูเอ็มแอลเซค และแผนภาพคลาสที่ใช้ยูเอ็มแอลเซคเอสพี โดยผลลัพธ์ของการประเมินแสดงให้เห็นว่า แผนภาพคลาสที่ใช้ยูเอ็มแอลเซคเอสพีมีระดับความซับซ้อนของแผนภาพคลาสไม่แตกต่างจากแผนภาพคลาสลักษณะอื่นในแง่ของการแสดงเส้นเชื่อมและจุดต่อของแผนภาพ แต่จะมีระดับความซับซ้อนของแผนภาพในแง่ของการแสดงตัวอักษรหรือสัญลักษณ์ที่มากกว่าแผนภาพลักษณะอื่น โดยมีสาเหตุมาจากการเพิ่มตัวอักษรหรือสัญลักษณ์เพื่อแสดงข้อมูลของแบบรูปความมั่นคง

ผลลัพธ์ที่ได้จากงานวิทยานิพนธ์นี้คือ ยูเอ็มแอลเซคเอสพี และเครื่องมือที่สนับสนุนการใช้งาน ผู้ออกแบบความมั่นคงระบบสามารถนำผลลัพธ์ดังกล่าวไปประยุกต์ใช้ในการออกแบบที่ใช้แบบรูปความมั่นคงให้มีประสิทธิภาพมากยิ่งขึ้น

ภาควิชา วิศวกรรมคอมพิวเตอร์ ลายมือชื่อนิสิต เกียรติศักดิ์ ไชยสมบูรณ์

สาขาวิชา วิทยาศาสตร์คอมพิวเตอร์ ลายมือชื่ออ.ที่ปรึกษาวิทยานิพนธ์หลัก นครทิพย์ พร้อมพูล

ปีการศึกษา 2551

4970236221 : MAJOR COMPUTER SCIENCE

KEYWORDS : SECURITY / SECURITY PATTERN / UML / UML PROFILE / UMLSEC

KIATTISAK CHAISOMBOON : VISUALIZING SECURITY PATTERNS BY EXTENDING UMLSEC. ADVISOR : ASST.PROF. NAKORNTHIP PROMPOON, 165 pp.

The objective of this thesis is to construct UMLsec-SP by combining UMLsec and the new purposed UML profiles, and to develop a tool based on UMLsec-SP in order to visualize security patterns using class diagram. The elements of each 27 patterns from 5 security pattern types; Access Control Model, System Access Control Architecture, Operating System Access Control, Firewall Architecture and Secure Internet Applications are analyzed to define pattern structural information and security information for constructing UMLsec-SP that follows such patterns. UMLsec-SP is validated against the UML profile standard specification.

A supporting tool was developed based on UMLsec-SP. The results earned from using the tool are a class diagram created from UMLsec-SP which can be applied for the design of any security system.

Case studies are used to develop class diagrams from the original UML diagram, UMLsec diagram and UMLsec-SP diagram and to compare the class diagram complexity. The results of complexity study are shown that UMLsec-SP diagram produces the same complexity in term of the number of nodes and edges, but it produces more complex than the other two diagrams in term of the number of characters and tokens. The reason is that UMLsec-SP contains a significant number of characters and tokens for presenting the security pattern-related information.

The results from this research are UMLsec-SP and a supporting tool. Security system designers can use them to improve the efficiency to design security system from applying security patterns.

Department : Computer Engineering — Student's Signature Kiattisak Chaisomboon

Field of Study : Computer Science — Advisor's Signature Nakornthip Prompoon

Academic Year : 2008

กิตติกรรมประกาศ

ขอกราบขอบพระคุณอาจารย์ที่ปรึกษา ผู้ช่วยศาสตราจารย์ นครทิพย์ พร้อมพูล ผู้เสียสละเวลาช่วยเหลือและให้คำปรึกษา คำแนะนำที่มีประโยชน์ต่องานวิจัย และความรู้ทางวิชาการอื่นๆ รวมทั้งคำสั่งสอนด้านคุณธรรมและจริยธรรมทำให้งานวิทยานิพนธ์ฉบับนี้สำเร็จลุล่วงไปด้วยดี

ขอกราบขอบพระคุณคณะกรรมการสอบวิทยานิพนธ์ รองศาสตราจารย์ ดร.วันชัย ริ้วไพบูลย์ ผู้ช่วยศาสตราจารย์ ดร.ศรัณย์ อินทโกสุม และดร.ยรรยง เต็งอำนวย ที่กรุณาสละเวลาในการให้คำแนะนำเกี่ยวกับงานวิจัยและตรวจสอบความถูกต้องสมบูรณ์ของวิทยานิพนธ์ฉบับนี้

ขอกราบขอบพระคุณมูลนิธิเพื่อการศึกษาคอมพิวเตอร์และการสื่อสาร (Computer & Communication Education Foundation) ที่ได้ให้ทุนส่งเสริมการศึกษา ทำให้ผู้วิจัยมีพลังในการสร้างสรรค์ผลงานเพื่อให้ได้มาซึ่งวิทยานิพนธ์ที่สมบูรณ์ที่สุด

ขอบคุณรุ่นพี่ เพื่อนๆ และรุ่นน้อง ที่ช่วยเหลือในทุกๆ ด้านที่เกี่ยวกับการทำวิทยานิพนธ์นี้ สุดท้ายนี้ขอกราบขอบพระคุณบิดา มารดา และเพื่อนๆ ทุกคนที่คอยให้กำลังใจและให้ความสนับสนุนมาโดยตลอด

สารบัญ

หน้า

หน้า

สารบัญตาราง

หน้า

หน้า

สารบัญภาพ

หน้า

หน้า

หน้า

บทที่ 1

บทนำ

ในบทนี้จะกล่าวถึง แนวคิดหลักของงานวิจัย อันประกอบไปด้วย ที่มาและความสำคัญ วัตถุประสงค์ ขอบเขต ขั้นตอนของการวิจัย และประโยชน์ที่คาดว่าจะได้รับ ซึ่งมีเนื้อหาดังต่อไปนี้

1.1 ที่มาและความสำคัญของงานวิจัย

การออกแบบระบบซอฟต์แวร์ (Software System Design) [1] เป็นกระบวนการในการสร้างแบบจำลองหรือรูปแบบของระบบซอฟต์แวร์ โดยเน้นเรื่องโครงสร้างข้อมูล สถาปัตยกรรม ส่วนต่อประสาน และองค์ประกอบย่อยต่างๆ ที่จำเป็นต่อการสร้างระบบตามความต้องการที่วิเคราะห์มาจากระบบดังกล่าว เช่น ความต้องการของลูกค้า ความต้องการทางธุรกิจ เป็นต้น โดยส่วนของการออกแบบระบบที่เกี่ยวข้องกับความต้องการทางด้านความมั่นคงของระบบคือ การออกแบบความมั่นคงของระบบ (System Security Design) เป็นการออกแบบที่ต้องนำหลักการความมั่นคงต่างๆ มาประยุกต์ใช้ในการออกแบบความมั่นคงของระบบให้เหมาะสมกับความต้องการและลักษณะของระบบ ดังนั้นการออกแบบความมั่นคงของระบบจึงจำเป็นต้องอาศัยผู้ที่มีความรู้และประสบการณ์ด้านการออกแบบความมั่นคงในกระบวนการดังกล่าวด้วย ถ้าผู้ออกแบบมีความรู้และประสบการณ์ด้านการออกแบบความมั่นคงไม่เพียงพอ อาจทำให้ระบบดังกล่าวเกิดจุดอ่อนที่เสี่ยงต่อการบุกรุกจากบุคคลที่ไม่พึงประสงค์ได้ ดังนั้นวิธีหนึ่งที่เป็นทางเลือกในการหลีกเลี่ยงปัญหาดังกล่าวคือ การนำแนวทางในการออกแบบความมั่นคงที่เคยประสบความสำเร็จในการป้องกันจุดอ่อนของระบบที่ใกล้เคียงมาประยุกต์ใช้กับการแก้ไขปัญหาที่คล้ายๆ กันในระบบที่กำลังพัฒนาอยู่ หรือที่รู้จักกันว่า แบบรูปความมั่นคง (Security pattern) [2] ซึ่งเป็นแบบรูปซอฟต์แวร์ (Software pattern) [3] ชนิดหนึ่งในการพัฒนาระบบซอฟต์แวร์

แบบรูปซอฟต์แวร์ คือ การรวบรวมการออกแบบซอฟต์แวร์ที่ดีที่สามารถนำกลับมาใช้ใหม่ในแง่ของการนำวัตถุประสงค์และฟังก์ชันของการออกแบบดังกล่าวมาใช้ซ้ำ โดยแบบรูปซอฟต์แวร์มีวัตถุประสงค์เพื่อนำเสนอผลเฉลย สำหรับปัญหาการออกแบบระบบซอฟต์แวร์ทั่วไปที่ปรากฏคล้ายกัน ช่วยให้ผู้พัฒนาสามารถเข้าใจและนำไปประยุกต์ใช้ได้ง่ายโดยไม่ต้องอาศัยความรู้หรือประสบการณ์มากนัก โดยแบบรูปซอฟต์แวร์ที่แก้ไขปัญหาที่เกี่ยวข้องกับการออกแบบความมั่นคงของระบบซอฟต์แวร์คือ แบบรูปความมั่นคง ที่ถูกเสนอขึ้นเพื่อช่วยแก้ไขปัญหาการออกแบบความมั่นคงของระบบซอฟต์แวร์ในส่วนต่างๆ เช่น การจัดการเกี่ยวกับสินทรัพย์และความเสี่ยง การออกแบบสถาปัตยกรรมไฟร์วอลล์ เป็นต้น แต่ในวิทยานิพนธ์นี้จะพิจารณาเพียงแบบรูปการออกแบบความมั่นคง (Security design pattern) ซึ่งเป็นแบบรูปความมั่นคงที่เสนอโครงสร้างที่ประกอบด้วยองค์ประกอบต่างๆ ในแบบรูปที่สามารถช่วยแก้ไขปัญหาทางด้านความมั่นคงจากแบบรูปได้

อย่างไรก็ตามการออกแบบและการปรับปรุงการออกแบบความมั่นคงของระบบโดยใช้แบบรูปความมั่นคงนั้นยังทำได้ค่อนข้างยาก ถ้าโครงสร้าง คุณสมบัติและเงื่อนไขบังคับของแบบรูปความมั่นคงที่ประยุกต์ใช้ในการออกแบบนั้นมิได้แสดงไว้ในแบบจำลองของการออกแบบความมั่นคงในระบบดังกล่าว เนื่องจากองค์ประกอบดังกล่าวจำเป็นต้องมีการตรวจสอบหรือจัดเก็บไว้เพื่อใช้ในการออกแบบและการปรับปรุงการออกแบบระบบโดยใช้แบบรูปความมั่นคง เช่น ในการปรับปรุงการออกแบบความมั่นคงโดยใช้แบบรูปความมั่นคงนั้น ผู้ออกแบบจำเป็นต้องทราบว่าองค์ประกอบใดบ้างในระบบที่เป็นองค์ประกอบของแบบรูปความมั่นคง จึงจะสามารถปรับปรุงองค์ประกอบดังกล่าวโดยใช้คำแนะนำจากแบบรูปความมั่นคงได้ เป็นต้น

ยูเอ็มแอลเซค (UMLsec) [4, 5] เป็นส่วนขยายของยูเอ็มแอลที่สนับสนุนการแสดงองค์ประกอบทางความมั่นคงของระบบในแผนภาพยูเอ็มแอล (Unified Modeling Language: UML) [6] ซึ่งเป็นแผนภาพที่ใช้ในกระบวนการพัฒนาระบบซอฟต์แวร์อย่างแพร่หลาย อย่างไรก็ตามการประยุกต์ใช้ยูเอ็มแอลเซคในการออกแบบความมั่นคงของระบบที่แบบรูปความมั่นคงนั้นสามารถตอบสนองความต้องการในการแสดงองค์ประกอบของแบบรูปความมั่นคงได้บางส่วนเท่านั้น เนื่องจากยูเอ็มแอลเซคยังขาดองค์ประกอบที่ใช้ในการแสดงข้อมูลของแบบรูปความมั่นคงที่จำเป็นต่อการออกแบบและปรับปรุงการออกแบบโดยใช้แบบรูปความมั่นคง กล่าวคือ ข้อมูลทางโครงสร้างและข้อมูลทางความมั่นคงของแบบรูปความมั่นคง

งานวิทยานิพนธ์นี้นำเสนอแนวคิดการปรับปรุงยูเอ็มแอลเซคเพื่อแสดงแบบรูปความมั่นคง ซึ่งแนวคิดนี้จะช่วยให้ผู้ออกแบบสามารถตรวจสอบและจัดเก็บไว้ซึ่งข้อมูลทางโครงสร้างและข้อมูลทางความมั่นคงของแบบรูปความมั่นคงในแผนภาพคลาสได้ชัดเจนยิ่งขึ้น พร้อมทั้งรู้ว่ามีคลาส (Class) การดำเนินการ (Operation) คุณลักษณะ (Attribute) หรือความสัมพันธ์ระหว่างคลาส (Relationship) ใดที่ต้องจัดเก็บไว้เพื่อตอบสนองการใช้งานเพื่อการออกแบบและปรับปรุงการออกแบบความมั่นคงของระบบโดยใช้แบบรูปความมั่นคง

ดังนั้นในงานวิทยานิพนธ์นี้มุ่งเน้นศึกษา วิเคราะห์และปรับปรุงยูเอ็มแอลเซคเพื่อแสดงแบบรูปความมั่นคง ซึ่งจะใช้แบบรูปความมั่นคงที่นำเสนอในหนังสือ แบบรูปความมั่นคง การบูรณาการความมั่นคงและวิศวกรรมระบบ (Security Patterns: Integrating Security and Systems Engineering) ที่นำเสนอโดย M. Schumacher และคณะ [2] จากนั้นจะนำยูเอ็มแอลเซคที่ปรับปรุงเพิ่มเติมมาประยุกต์ใช้ในการออกแบบพัฒนาระบบซอฟต์แวร์ตัวอย่าง พร้อมทั้งพัฒนาเครื่องมือที่สนับสนุนการแสดงแบบรูปความมั่นคงโดยใช้ยูเอ็มแอลเซคที่ปรับปรุงเพิ่มเติม ซึ่งการแสดงแบบรูปความมั่นคงโดยใช้ยูเอ็มแอลเซคที่ปรับปรุงเพิ่มเติมนั้นจะตอบสนองการออกแบบและปรับปรุงการออกแบบความมั่นคงของระบบโดยใช้แบบรูปความมั่นคงให้มีประสิทธิภาพมากยิ่งขึ้น

1.2 วัตถุประสงค์ของงานวิจัย

1) ปรับปรุงยูเอ็มแอลเซคเพื่อใช้สำหรับการแสดงแบบรูปความมั่นคงในแผนภาพคลาส

2) สร้างเครื่องมือโดยนำยูเอ็มแอลเซคที่ปรับปรุงเพิ่มเติมมาประยุกต์ใช้ในการแสดงแบบรูปความมั่นคง

1.3 ขอบเขตของงานวิจัย

1.3.1 นำเสนอยูเอ็มแอลเซคที่ปรับปรุงเพิ่มเติมเพื่อสนับสนุนการแสดงแบบรูปความมั่นคงในแผนภาพคลาส โดยใช้แบบรูปความมั่นคงที่ได้รับการออกแบบและตรวจสอบความถูกต้องแล้ว 5 กลุ่มแบบรูปดังต่อไปนี้

1) แบบจำลองควบคุมการเข้าถึง (Access Control Model)

เป็นกลุ่มแบบรูปที่มุ่งเน้นการกำหนดเงื่อนไขบังคับ (Constraints) ในระดับต่าง ๆ ไม่ว่าจะเป็นสถาปัตยกรรม โปรแกรมประยุกต์ และข้อบังคับในระดับล่าง ๆ ของการปฏิบัติงาน ซึ่งแบบรูปความมั่นคงในกลุ่มนี้ประกอบด้วย

(1) การให้อำนาจ (Authorization)

(2) การควบคุมการเข้าถึงเชิงบทบาท (Role-Based Access Control)

(3) ความมั่นคงหลายระดับ (Multilevel Security)

(4) การเฝ้าสังเกตเชิงอ้างอิง (Reference Monitor)

2) สถาปัตยกรรมการควบคุมการเข้าถึงระบบ
(System Access Control Architecture)

เป็นกลุ่มแบบรูปที่เสนอสถาปัตยกรรมของระบบที่เหมาะสมต่อการควบคุมการเข้าถึงระบบในลักษณะต่าง ๆ ซึ่งแบบรูปความมั่นคงในกลุ่มนี้ประกอบด้วย

(1) จุดเข้าระบบเดี่ยว (Single Access Point)

(2) จุดตรวจสอบ (Check Point)

(3) เซสชันทางความมั่นคง (Security Session)

(4) การควบคุมการเข้าถึงด้วยการแสดงความผิดพลาด
(Full Access with Errors)

(5) การจำกัดการเข้าถึง (Limited Access)

3) การควบคุมการเข้าถึงระบบปฏิบัติการ
(Operating System Access Control)

เป็นกลุ่มแบบรูปที่เสนอแนวคิดในการแก้ไขปัญหาทางด้านความมั่นคงของระบบปฏิบัติการโดยทั่วไป ซึ่งแบบรูปความมั่นคงในกลุ่มนี้ประกอบด้วย

(1) องค์ประกอบพิสูจน์ตัวตน (Authentication)

(2) การควบคุมการสร้างกระบวนการ (Controlled Process Creator)

(3) การควบคุมการสร้างอ็อบเจกต์ (Controlled Object Factory)

(4) การตรวจสอบการเข้าถึงอ็อบเจกต์ (Controlled Object Monitor)

(5) การควบคุมหน่วยความจำเสมือน (Controlled Virtual Address Space)

(6) การควบคุมขอบเขตกระทำการ (Execution Domain)

(7) การควบคุมสิ่งแวดล้อมที่กระทำการ (Controlled Execution Environment)

(8) การให้อำนาจในแฟ้มข้อมูล (File Authorization)

4) สถาปัตยกรรมไฟร์วอลล์ (Firewall Architecture)

เป็นกลุ่มแบบรูปที่มุ่งเน้นการกำหนดเงื่อนไขบังคับสำหรับการติดต่อระหว่างกันผ่านทางระบบเครือข่าย (Network) เพื่อป้องกันการโจมตีหรือปลอมปนทั้งจากภายนอกและภายในองค์กร ซึ่งแบบรูปความมั่นคงในกลุ่มนี้ประกอบด้วย

(1) ไฟร์วอลล์สำหรับการกรองแพ็คเกจ (Packet Filtering Firewall)

(2) ไฟร์วอลล์เชิงตัวแทน (Proxy-Based Firewall)

(3) ไฟร์วอลล์เชิงสถานะ (Stateful Firewall)

5) การประยุกต์ใช้ความมั่นคงบนอินเตอร์เน็ต (Secure Internet Applications)

เป็นกลุ่มแบบรูปที่มุ่งเน้นการแก้ไขปัญหาความมั่นคงในการสื่อสารผ่านเครือข่ายอินเตอร์เน็ตในรูปแบบต่างๆ ซึ่งแบบรูปความมั่นคงในกลุ่มนี้ประกอบด้วย

(1) การปิดบังข้อมูล (Internet Obscurity)

(2) ช่องทางความมั่นคง (Secure Channel)

(3) ผู้เป็นที่รู้จัก (Known Partners)

(4) เขตปลอดการป้องกัน (Demilitarized Zone)

(5) ตัวแทนป้องกัน (Protection Reverse Proxy)

(6) ตัวแทนบูรณาการ (Integration Reverse Proxy)

(7) ประตูหน้า (Front Door)

1.3.2 สร้างเครื่องมือที่นำยูเอ็มแอลเซคที่ปรับปรุงเพิ่มเติมจาก 1.3.1 มาประยุกต์ใช้ในการแสดงแบบรูปความมั่นคง

1.3.3 ทดสอบเครื่องมือโดยการเปรียบเทียบความสามารถของเครื่องมือต้นแบบกับเครื่องมือที่สนับสนุนการแสดงแบบรูปประเภทอื่น

1.3.4 ประเมินผลการแสดงแบบรูปความมั่นคงโดยใช้แบบรูปความมั่นคงที่ครอบคลุมแบบรูปความมั่นคงในงานวิทยานิพนธ์นี้มาแสดงในแผนภาพคลาสด้วยยูเอ็มแอล แผนภาพคลาสที่ใช้ยูเอ็มแอลเซค และแผนภาพคลาสที่ใช้ยูเอ็มแอลเซคที่ปรับปรุงเพิ่มเติม เพื่อวัดระดับความซับซ้อนของแต่ละแผนภาพโดยใช้ตัววัดความซับซ้อนของแผนภาพ จากนั้นนำผลลัพธ์จาก

การวัดระดับความซับซ้อนในแต่ละแผนภาพมาเปรียบเทียบกัน ซึ่งผลลัพธ์ที่ได้จากการเปรียบเทียบระดับความซับซ้อนของแผนภาพสามารถใช้เป็นแนวทางในการปรับปรุงยูเอ็มแอลเซคที่ปรับปรุงเพิ่มเติมหรือเครื่องมือต้นแบบ

1.4 ขั้นตอนของการวิจัย

1) ศึกษาแบบรูปความมั่นคง

2) วิเคราะห์แบบรูปความมั่นคงเพื่อหาความต้องการในการแสดงข้อมูลที่จำเป็นต่อการออกแบบและปรับปรุงการออกแบบโดยใช้แบบรูปความมั่นคง

3) วิเคราะห์หาความต้องการในการแสดงข้อมูลของแบบรูปความมั่นคงในแผนภาพคลาสที่ใช้ยูเอ็มแอลเซค

4) ปรับปรุงยูเอ็มแอลเซคให้สนับสนุนการแสดงแบบรูปความมั่นคง

5) ตรวจสอบยูเอ็มแอลเซคที่ปรับปรุงเพิ่มเติม

6) สร้างเครื่องมือที่นำยูเอ็มแอลเซคที่ปรับปรุงเพิ่มเติมมาประยุกต์ใช้ในการแสดงแบบรูปความมั่นคง

7) ทดสอบเครื่องมือเพื่อปรับปรุงประสิทธิภาพในการแสดงแบบรูปความมั่นคงโดยใช้ยูเอ็มแอลเซคที่ปรับปรุงเพิ่มเติม

8) ประเมินระดับความซับซ้อนของการแสดงแบบรูปความมั่นคง รวมทั้งวิเคราะห์การแสดงแบบรูปความมั่นคงโดยใช้ยูเอ็มแอลเซคที่ปรับปรุงเพิ่มเติม

9) นำเสนอแนวทางในการพัฒนาและสรุปผลงานวิจัย

10) จัดทำวิทยานิพนธ์

1.5 ประโยชน์ที่คาดว่าจะได้รับ

1) ได้ยูเอ็มแอลเซคที่ปรับปรุงเพิ่มเติมเพื่อสนับสนุนการแสดงแบบรูปความมั่นคงในแผนภาพคลาส

2) ได้เครื่องมือที่สนับสนุนการแสดงแบบรูปความมั่นคงที่สามารถนำไปใช้ได้จริงเพื่อประโยชน์ต่อการออกแบบและการทำให้เกิดผล (Implementation)

3) สามารถสนับสนุนการใช้แบบรูปความมั่นคงในการออกแบบและปรับปรุงการออกแบบได้อย่างมีแบบแผนและมีประสิทธิภาพมากขึ้นเพื่อนำแบบรูปความมั่นคงดังกล่าวไปใช้ในกระบวนการต่างๆ ของการพัฒนาระบบซอฟต์แวร์ต่อไปได้

บทที่ 2

ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

ในบทนี้จะกล่าวถึง ทฤษฎีที่สำคัญ ซึ่งได้นำมาประยุกต์ สนับสนุน และใช้อ้างอิงในการทำงานวิทยานิพนธ์ รวมถึงข้อดีและข้อจำกัดของงานวิจัยต่างๆ ที่เกี่ยวข้อง โดยมีเนื้อหาดังต่อไปนี้

2.1 ทฤษฎีที่เกี่ยวข้อง

2.1.1 แบบรูปความมั่นคง (Security Pattern)

แบบรูป [3] คือ ปัญหาและผลเฉลยที่เคยปรากฏในอดีต โดยการเตรียมผลเฉลยจากปัญหาหนึ่งนำมาแก้ปัญหาที่ปรากฏใหม่ซึ่งมีลักษณะคล้ายกับปัญหาเดิมในแบบรูปนั้น แบบรูปประกอบด้วยองค์ประกอบหลัก 3 ส่วน คือ ปัญหา ลักษณะ และผลเฉลย แต่การนำแบบรูปไปประยุกต์ใช้นั้นอาจต้องมีองค์ประกอบอื่นเพิ่มเติม เพื่อช่วยให้แบบรูปมีความสมบูรณ์และง่ายต่อการนำไปใช้ เช่น ชื่อแบบรูป (Pattern Name) ฟอร์ซ (Force) ผลลัพธ์เชิงบริบท (Resulting Context) แบบรูปที่เกี่ยวข้อง (Related Patterns) รวมทั้งองค์ประกอบสนับสนุนที่จะช่วยในการอธิบายผลเฉลยของแบบรูปนั้นๆ เช่น ตัวอย่าง (Example) แผนภาพคลาส (Class Diagram) ที่ใช้ในการออกแบบ เป็นต้น องค์ประกอบเหล่านี้จะขึ้นอยู่กับประเภทของการนำแบบรูปไปใช้งานเพื่อที่จะสามารถอธิบาย สนับสนุนการใช้ หรือช่วยในการทำความเข้าใจในปัญหา หรือการแก้ปัญหาที่จะนำเสนอได้ชัดเจนขึ้น

แบบรูปความมั่นคง [2, 7] คือ แบบรูปที่นำเสนอปัญหาความมั่นคงที่เคยปรากฏในอดีต รวมทั้งผลเฉลยที่พิสูจน์แล้วว่าแก้ไขปัญหาได้ แบบรูปความมั่นคงสามารถแบ่งตามลักษณะของปัญหาได้เป็น 3 ประเภทคือ

1) แบบรูปการวิเคราะห์ความมั่นคง (Security Analysis Patterns) เป็นแบบรูปที่เสนอผลเฉลยเพื่อช่วยแก้ไขปัญหาที่เกี่ยวกับการวิเคราะห์ความมั่นคงของระบบ เช่น การวิเคราะห์หาค่าความเสี่ยงของสินทรัพย์ การวิเคราะห์หาภัยคุกคามของสินทรัพย์ เป็นต้น

2) แบบรูปการออกแบบความมั่นคง (Security Design Patterns) เป็นแบบรูปที่เสนอผลเฉลยเพื่อช่วยแก้ไขปัญหาที่เกี่ยวกับการออกแบบโครงสร้างทางความมั่นคงของระบบ เช่น การออกแบบโครงสร้างในการควบคุมการเข้าถึงระบบ การออกแบบโครงสร้างของไฟร์วอลล์ประเภทต่างๆ เป็นต้น

3) แบบรูปกระบวนการความมั่นคง (Security Process Patterns) เป็นแบบรูปที่เสนอผลเฉลยเพื่อช่วยแก้ไขปัญหาที่เกี่ยวกับกระบวนการในการออกแบบความมั่นคงของระบบ เช่น กระบวนการในการวิเคราะห์ความเสี่ยงของสินทรัพย์ กระบวนการในการออกแบบโครงสร้างความมั่นคงของระบบ เป็นต้น

ในงานวิทยานิพนธ์นี้จะใช้แบบรูปความมั่นคงจากที่นำเสนอโดย M. Schumacher และคณะ [2] เนื่องจากเป็นแบบรูปความมั่นคงที่มีโครงสร้างเอกสารเหมือนแบบรูปการออกแบบที่นำเสนอโดย E. Gamma และคณะ [8] และมีโครงสร้างกับขอบเขตที่ชัดเจน โดยตารางที่ 2.1 แสดงการเปรียบเทียบระหว่างองค์ประกอบของเอกสารแบบรูปการออกแบบที่นำเสนอโดย E. Gamma และคณะ [8] กับแบบรูปความมั่นคงที่นำเสนอโดย M. Schumacher และคณะ [2]

ตารางที่ 2.1 องค์ประกอบของเอกสารแบบรูปความมั่นคงเทียบกับแบบรูปการออกแบบ [9]

แบบรูปเอกสาร (Document Patterns)	**แบบรูปการออกแบบ โดย E.Gamma**	**แบบรูปความมั่นคง โดย M. Schumacher**	**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
การนำไปปรับใช้ (Applicability)	มี	บริบท (Context)	ตัวอย่างสถานการณ์ที่นำแบบรูปไปใช้ เพื่อแสดงให้เห็นถึงการแก้ปัญหาการออกแบบที่ไม่เหมาะสม
การทำให้เกิดผล (Implementation)	มี	มี	พิจารณาถึงจุดอ่อน ผลกระทบ หรือเทคนิคที่ต้องทราบ เมื่อนำแบบรูปไปใช้
ลักษณะทางโครงสร้าง (Structure)	มี	มี	การนำเสนอแผนภาพคลาส (Class diagram)
สิ่งที่เข้ามาเกี่ยวข้อง (Participants)	มี	-	แสดงถึงคลาสหรืออ็อบเจกต์ที่เกี่ยวข้องในแบบรูป รวมทั้งหน้าที่ของคลาสหรืออ็อบเจกต์ได้
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

2.1.2 แนวคิดด้านการออกแบบ (Design Concepts)

แนวคิดด้านการออกแบบเป็นแนวคิดของการออกแบบระบบซอฟต์แวร์ที่มีการพัฒนามาอย่างยาวนานและได้รับการพิสูจน์แล้วว่าสามารถแก้ไขปัญหาของการออกแบบระบบซอฟต์แวร์ได้ จนกลายมาเป็นรากฐานของแนวคิดในการออกแบบของระบบซอฟต์แวร์ในปัจจุบัน [1] แนวคิดด้านการออกแบบในปัจจุบันมีดังต่อไปนี้

1) **การกำหนดสาระสำคัญ (Abstraction)** แบ่งเป็นการกำหนดสาระสำคัญเชิงกระบวนงาน (Procedure Abstraction) การกำหนดสาระสำคัญเชิงข้อมูล (Data Abstraction) และการกำหนดสาระสำคัญเชิงควบคุม (Control Abstraction) โดยการกำหนดสาระสำคัญเชิงกระบวนงานจะเป็นการกำหนดลำดับของคำสั่งที่ทำหน้าที่เฉพาะเจาะจงอย่างใดอย่างหนึ่ง การกำหนดสาระสำคัญเชิงข้อมูลจะเป็นการกำหนดข้อมูลที่อธิบายวัตถุข้อมูล (Data Object) และการกำหนดสาระสำคัญเชิงควบคุมจะมุ่งเน้นการกำหนดกลไกที่ควบคุมการทำงานของระบบซอฟต์แวร์

2) **การเพิ่มเติมรายละเอียด (Refinement)** เป็นกระบวนการในการลงรายละเอียดเพิ่มเติมเพื่อให้ผู้ออกแบบระบุรายละเอียดของการออกแบบในกระบวนการงาน ข้อมูล และกลไกที่ควบคุมการทำงานในระบบซอฟต์แวร์

3) **ความเป็นโมดูล (Modularity)** เป็นคุณลักษณะของซอฟต์แวร์ที่สามารถแบ่งเป็นองค์ประกอบย่อยที่มีหน้าที่ในระบบแตกต่างกัน ซึ่งเรียกว่า โมดูล (Module) ที่ทำงานร่วมกันเพื่อตอบสนองตามความต้องการในระบบซอฟต์แวร์

4) **สถาปัตยกรรมระบบซอฟต์แวร์ (Software Architecture)** เป็นโครงสร้างโดยรวมของส่วนประกอบ (Components) หรือโมดูลที่ตอบสนองการทำงานของระบบซอฟต์แวร์ให้เป็นไปตามความต้องการ

5) **การควบคุมลำดับชั้น (Control Hierarchy)** เป็นการควบคุมส่วนประกอบหรือโมดูลให้เป็นไปตามลำดับชั้นในระบบซอฟต์แวร์ โดยทั่วไปจะแสดงเป็นแผนภาพต้นไม้ที่อธิบายโครงสร้างที่ใช้ในการควบคุมส่วนประกอบหรือโมดูลในระบบซอฟต์แวร์

6) **การแบ่งส่วนโครงสร้าง (Structural Partitioning)** ประกอบไปด้วยการแบ่งส่วนโครงสร้างในแนวระดับ (Horizontal partitioning) และการแบ่งส่วนโครงสร้างในแนวตั้ง (Vertical partitioning) โดยการแบ่งส่วนโครงสร้างในแนวระดับเป็นการแบ่งฟังก์ชันหลักให้เป็นฟังก์ชันย่อยที่ง่ายต่อการพัฒนา และการแบ่งส่วนโครงสร้างในแนวตั้งเป็นการกระจายอำนาจในการควบคุมการกระบวนงานและหน้าที่ในระบบของส่วนประกอบในระบบจากบนสู่ล่าง

7) **โครงสร้างข้อมูล (Data Structure)** เป็นการแสดงความสัมพันธ์เชิงตรรกะในแต่ละส่วนย่อยของข้อมูล โดยประกอบไปด้วย การจัดระบบข้อมูล วิธีการในการเข้าถึงข้อมูล ระดับขั้นของการมีส่วนร่วมระหว่างข้อมูล (Degree of associativity) และการประมวลผลข้อมูลด้วยวิธีต่างๆ ในระบบซอฟต์แวร์

8) กระบวนงานของซอฟต์แวร์ (Software Procedure) เป็นรายละเอียดของกระบวนการทำงานของแต่ละส่วนประกอบหรือโมดูลในระบบซอฟต์แวร์ โดยประกอบไปด้วย ลำดับของเหตุการณ์ จุดตัดสินใจ การดำเนินการที่วนซ้ำ ที่สอดคล้องกับการจัดระบบข้อมูลและโครงสร้างในระบบซอฟต์แวร์

9) การซ่อนสารสนเทศ (Information Hiding) เป็นการออกแบบให้แต่ละส่วนประกอบหรือโมดูลมีอัลกอริทึมและข้อมูลบรรจุภายในตัวเท่าที่จำเป็นต่อการทำงานในระบบซอฟต์แวร์ โดยที่ไม่ยอมให้ส่วนประกอบหรือโมดูลอื่นเข้าถึงอัลกอริทึมและข้อมูลเหล่านี้โดยไม่จำเป็น

ในงานวิทยานิพนธ์นี้จะนำแนวคิดการออกแบบมาพิจารณาและปรับปรุงการออกแบบโครงสร้างของแบบรูปความมั่นคงให้เหมาะสม เนื่องจากโครงสร้างของแบบรูปความมั่นคงบางส่วนที่เสนอโดย M. Schumacher และคณะ [2] ได้เสนอเพียงโครงสร้างอย่างง่ายของแบบรูปความมั่นคงเท่านั้น จึงทำให้โครงสร้างดังกล่าวขาดองค์ประกอบบางส่วนที่จำเป็นต่อกระบวนการในแบบรูปความมั่นคง

2.1.3 วิศวกรรมความมั่นคง (Security Engineering)

วิศวกรรมความมั่นคง [7] เป็นหลักการที่นำทฤษฎีความมั่นคง (Security Theory) มาใช้ในวิธีปฏิบัติความมั่นคง (Security Practice) หรืออีกนัยหนึ่งคือ การออกแบบและสร้างระบบที่สามารถป้องกันการโจมตีต่างๆได้ โดยมีวัตถุประสงค์เพื่อเปลี่ยนแปลงสถานะจากอันตรายเป็นสถานะความเสี่ยงที่ยอมรับได้ ซึ่งกระบวนการที่จำเป็นในวิศวกรรมความมั่นคงแสดงได้ดังรูปที่ 2.1 โดยมีรายละเอียดของกระบวนการดังนี้

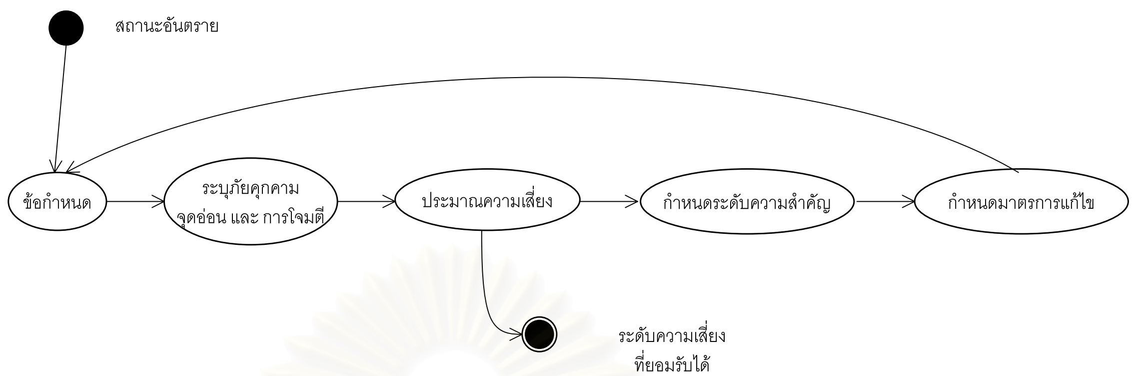
1) ข้อกำหนด (Specification) เป็นส่วนประกอบและส่วนต่อประสาน (Interface) ทั้งหมดที่ต้องกำหนดให้สมบูรณ์ เพราะถ้าหากไม่ครอบคลุมตามข้อกำหนดของสถาปัตยกรรมทั้งหมดของระบบ จะก่อให้เกิดช่องโหว่ ภัยอันตราย และการถูกโจมตี ในส่วนที่ยังไม่ได้ทำการระบุเป็นข้อกำหนดไว้

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

3) การประมาณความเสี่ยง (Risk Estimation) ความเสี่ยงของการโจมตีที่อาจเกิดกับแต่ละองค์ประกอบ หรือส่วนต่อประสาน จะต้องพิจารณาตามความสัมพันธ์ระหว่างข้อกำหนดของภัยคุกคาม จุดอ่อนและรูปแบบการโจมตี

4) การกำหนดระดับความสำคัญ (Prioritization) ในกรณีที่มีความเสี่ยงสูงปรากฏในจุดอ่อนที่เกี่ยวข้องกับองค์ประกอบ หรือส่วนประสานที่อันตราย จะต้องจัดลำดับความสำคัญไว้เป็นลำดับต้นๆ ซึ่งถือว่าขั้นตอนนี้เป็นขั้นตอนที่สำคัญมากในการกำหนดมาตรการการป้องกัน

5) มาตรการแก้ไข (Countermeasure) ซึ่งจำแนกภัยคุกคาม จุดอ่อนและรูปแบบการโจมตีทั้งนี้ขึ้นกับความสำคัญและประเภทของภัยอันตราย



รูปที่ 2.1 ขั้นตอนวิธีทางวิศวกรรมความมั่นคง

ผู้ออกแบบความมั่นคงของระบบสามารถนำแบบรูปความมั่นคงไปประยุกต์ใช้ในขั้นตอนของการระบุข้อกำหนดทางโครงสร้างความมั่นคงของระบบให้เหมาะสมกับปัญหาและลักษณะของระบบได้ เนื่องจากแบบรูปความมั่นคงเสนอโครงสร้างที่ประกอบไปด้วยองค์ประกอบที่จำเป็นสำหรับกระบวนการความมั่นคงในแต่ละแบบรูป อย่างไรก็ตามการประยุกต์ใช้แบบรูปความมั่นคงในขั้นตอนดังกล่าวนั้น ไม่สามารถตอบสนองการออกแบบและปรับปรุงการออกแบบโดยใช้แบบรูปความมั่นคงได้อย่างเต็มที่ เนื่องจากการออกแบบและปรับปรุงการออกแบบโดยใช้แบบรูปความมั่นคงนั้นจำเป็นต้องแสดงข้อมูลของแบบรูปความมั่นคงในแบบจำลองของระบบให้ชัดเจน เพื่อใช้ในการตรวจสอบและจัดเก็บไว้ซึ่งข้อมูลของแบบรูปในขั้นตอนของการออกแบบและปรับปรุงการออกแบบโดยใช้แบบรูปความมั่นคง จึงเป็นที่มาของงานวิทยานิพนธ์นี้ที่จะมุ่งเน้นการแสดงข้อมูลของแบบรูปความมั่นคงในแผนภาพคลาสให้ชัดเจนยิ่งขึ้น เพื่อตอบสนองการออกแบบและปรับปรุงการออกแบบโดยใช้แบบรูปความมั่นคง

2.1.4 ยูเอ็มแอลโพรไฟล์ (UML Profile)

ยูเอ็มแอลโพรไฟล์ [6, 10] เป็นองค์ประกอบของยูเอ็มแอลที่สามารถทำการปรับเปลี่ยนเพื่อสนับสนุนการออกแบบระบบในโดเมน (Domain) เฉพาะด้านได้ โดยงานวิจัยที่นำยูเอ็มแอลโพรไฟล์มาปรับปรุงเพื่อประยุกต์ใช้ในการออกแบบระบบในโดเมนเฉพาะด้าน เช่น J. Jürjens และคณะ [4, 5] เสนอยูเอ็มแอลโพรไฟล์ที่ช่วยแสดงองค์ประกอบทางความมั่นคงในการออกแบบความมั่นคงของระบบโดยทั่วไป J. Dong และคณะ [11] เสนอยูเอ็มแอลโพรไฟล์ที่ช่วยแสดงองค์ประกอบทางโครงสร้างของแบบรูปการออกแบบที่ใช้การพัฒนาระบบซอฟต์แวร์ เป็นต้น ยูเอ็มแอลโพรไฟล์ประกอบไปด้วยองค์ประกอบย่อยที่มีหน้าที่แตกต่างกัน ดังต่อไปนี้

1) แม่พิมพ์ต้นแบบ (Stereotype) เป็นองค์ประกอบที่ใช้ในการระบุประเภทต่างๆ ขององค์ประกอบแบบจำลอง (Model Element) ในแผนภาพยูเอ็มแอล โดยองค์ประกอบดังกล่าวมีความสำคัญต่อการทำงานในโดเมนด้านอื่น เช่น องค์ประกอบที่ใช้ในการสร้างชุดรหัส

องค์ประกอบที่ใช้ในการระบุข้อมูลของผู้ออกแบบ เป็นต้น โดยรูปแบบทั่วไปของแม่พิมพ์ต้นแบบคือ

<< ชื่อแม่พิมพ์ต้นแบบ >>

ตัวอย่างของแม่พิมพ์ต้นแบบ เช่น แม่พิมพ์ต้นแบบ “interface” เป็นแม่พิมพ์ต้นแบบที่ระบุองค์ประกอบที่เป็นส่วนต่อประสาน แม่พิมพ์ต้นแบบ “guarded” เป็นแม่พิมพ์ต้นแบบที่ระบุองค์ประกอบที่ถูกควบคุมการเข้าถึง เป็นต้น นอกจากนี้แม่พิมพ์ต้นแบบยังมีค่าป้ายระบุและเงื่อนไขบังคับที่สัมพันธ์กับแม่พิมพ์ต้นแบบดังกล่าวเพื่อใช้ในการระบุข้อมูลที่จำเพาะขององค์ประกอบดังกล่าวให้ชัดเจนยิ่งขึ้น

2) ค่าป้ายระบุ (Tagged Value) เป็นข้อมูลที่จำเพาะขององค์ประกอบแบบจำลองที่ใช้แม่พิมพ์ต้นแบบที่มีป้ายระบุสำหรับกำหนดข้อมูลดังกล่าว ค่าป้ายระบุจะถูกกำหนดในขณะที่สร้างแบบจำลองเพื่อใช้ในการกำหนดสภาพแวดล้อมที่อยู่ในโดเมนอื่นขององค์ประกอบแบบจำลองนั้น โดยข้อแตกต่างของคุณลักษณะในคลาสและค่าป้ายระบุในแม่พิมพ์ต้นแบบคือ คุณลักษณะในคลาสจำเป็นต่อการทำงานในคลาส แต่ค่าป้ายระบุในแม่พิมพ์ต้นแบบไม่จำเป็นต่อการทำงานในคลาส แต่จำเป็นต่อการกำหนดสภาพแวดล้อมสำหรับการออกแบบระบบในโดเมนอื่น ส่วนใหญ่ค่าป้ายระบุจะถูกใช้ในการระบุข้อมูลสำหรับการจัดการโครงการหรือการสร้างชุดรหัสของเครื่องมือสร้างชุดรหัส เช่น ชื่อผู้ที่สร้างองค์ประกอบในแผนภาพ ชื่อภาษาที่ใช้ในการสร้างคลาสและส่วนประกอบ เป็นต้น โดยรูปแบบทั่วไปของค่าป้ายระบุคือ

ชื่อป้ายระบุ (Tag name) = ค่าของป้ายระบุ (Value of tag)

ตัวอย่างของค่าป้ายระบุ เช่น ค่าป้ายระบุ “author=Joe” เป็นค่าป้ายระบุของแม่พิมพ์ต้นแบบ “authorship” ที่ระบุว่า ชื่อผู้ที่สร้างองค์ประกอบดังกล่าวคือ “Joe” ซึ่งจะถูกใช้ประโยชน์ในการติดตามผู้รับผิดชอบที่เกี่ยวกับการออกแบบองค์ประกอบดังกล่าว เป็นต้น

3) เงื่อนไขบังคับ (Constraint) เป็นข้อบังคับของแม่พิมพ์ต้นแบบที่จำเป็นต้องพิจารณาเมื่อมีการใช้งาน เงื่อนไขบังคับจะช่วยกำหนดขอบเขตในการใช้งานของแม่พิมพ์ต้นแบบหรือค่าป้ายระบุ โดยทั่วไปเงื่อนไขบังคับจะเขียนอยู่ในรูปของภาษาโอซีแอล (Object Constraint Language: OCL) [11] ที่เป็นภาษามาตรฐานในการระบุเงื่อนไขบังคับขององค์ประกอบแบบจำลองในแผนภาพยูเอ็มแอล เช่น แม่พิมพ์ต้นแบบ “interface” มีเงื่อนไขบังคับที่บังคับให้ผู้ใช้งานระบุชื่อคลาสทุกครั้งเมื่อสร้างคลาสขึ้นมาใหม่ คือ “self.base.name -> notEmpty” เป็นต้น

2.2 งานวิจัยที่เกี่ยวข้อง

2.2.1 ยูเอ็มแอลเซค : ส่วนขยายของยูเอ็มแอลเพื่อการพัฒนาระบบความมั่นคง (UMLsec : Extending UML for Secure System Development)

งานวิจัยนี้ได้เสนอการสร้างส่วนขยายของยูเอ็มแอลที่สร้างมาจากยูเอ็มแอลโพรไฟล์เพื่อการพัฒนาความมั่นคงของระบบ [4, 5] โดยยูเอ็มแอลเซคถูกพัฒนาขึ้นเพื่อตอบสนองตามความต้องการในการออกแบบโครงสร้างทางด้านความมั่นคงทั่วไป โดยรายละเอียดของความต้องการในการพัฒนายูเอ็มแอลเซคมีดังต่อไปนี้

1) ความต้องการหลักในการพัฒนายูเอ็มแอลเซคประกอบด้วย

1.1) *ความต้องการในการระบุความต้องการทางความมั่นคง (Security Requirement)* ประกอบไปด้วย การระบุข้อมูลที่มีลักษณะเป็นความลับ (Secrecy) ความบูรณภาพ (Integrity) และความสมจริง (Authenticity)

1.2) *ความต้องการในการระบุเหตุการณ์ที่เป็นภัยคุกคาม (Threat Scenario)* เป็นความต้องการในการระบุสถานการณ์ของระบบในหลายด้านที่เสี่ยงต่อการถูกโจมตีจากบุคคลที่ไม่พึงประสงค์

1.3) *ความต้องการในการระบุแนวคิดทางด้านความมั่นคง (Security Concept)* เป็นความต้องการในการระบุแนวคิดทางด้านความมั่นคงที่สำคัญที่ปรากฏอยู่ในส่วนต่างๆ ภายในระบบ เช่น อุปกรณ์เก็บรักษากุญแจเข้ารหัส (Temper-resistant hardware) เป็นต้น

1.4) *ความต้องการในการระบุกลไกทางด้านความมั่นคง (Security Mechanism)* เป็นความต้องการในการระบุกลไกทางความมั่นคงที่สำคัญที่ปรากฏอยู่ในส่วนต่างๆ ภายในระบบ เช่น การควบคุมการเข้าถึง (Access Control) การทำงานของโพรโตคอลทางความมั่นคง (Security Protocol) เป็นต้น

1.5) *ความต้องการในการระบุความมั่นคงพื้นฐาน (Security Primitive)* เป็นความต้องการในการระบุรายละเอียดของความมั่นคงที่เป็นพื้นฐานภายในระบบ เช่น การเข้ารหัสแบบสมมาตรและอสมมาตร (Symmetric and Asymmetric Encryption) เป็นต้น

1.6) *ความต้องการในการระบุความมั่นคงที่อยู่ภายใต้ระดับกายภาพ (Underlying Physical Security)* เป็นความต้องการในการระบุความมั่นคงที่ควบคุมการทำงานภายใต้ฮาร์ดแวร์ (Hardware) ของระบบ

1.7) *ความต้องการในการระบุข้อมูลสำหรับการจัดการทางด้านความมั่นคง (Security Management)* เป็นความต้องการในการระบุความมั่นคงที่จำเป็นต่อการจัดการความมั่นคงภายในระบบ

2) ความต้องการเสริมในการพัฒนายูเอ็มแอลเซค คือ การนำยูเอ็มแอลเซคไปประยุกต์ใช้ในโดเมนเฉพาะด้านอื่นๆ เช่น จาวา (Java) สมาร์ตคาร์ด (Smart Card) เป็นต้น

โดยรายละเอียดของแม่พิมพ์ต้นแบบและป้ายระบุของยูเอ็มแอลเซคที่สร้างมาจากความต้องการดังกล่าวแสดงในภาคผนวก ก

สิ่งที่นำมาพิจารณาใช้ในงานวิทยานิพนธ์นี้คือ การนำแม่พิมพ์ต้นแบบและป้ายระบุของยูเอ็มแอลเซคมาปรับปรุงเพิ่มเติมเพื่อให้ยูเอ็มแอลเซคสามารถรองรับการออกแบบความมั่นคงของระบบโดยใช้แบบรูปความมั่นคง เนื่องจากยูเอ็มแอลเซคไม่ได้รองรับการแสดงแบบรูปความมั่นคงได้ครบถ้วนตามความต้องการในการออกแบบและปรับปรุงการออกแบบโดยใช้แบบรูปความมั่นคง กล่าวคือ ขาดการแสดงข้อมูลทางโครงสร้างและข้อมูลทางความมั่นคงของแบบรูปความมั่นคง จึงเป็นที่มาของงานวิทยานิพนธ์นี้ที่ปรับปรุงยูเอ็มแอลเซคเพื่อการแสดงข้อมูลของแบบรูปความมั่นคงดังกล่าว

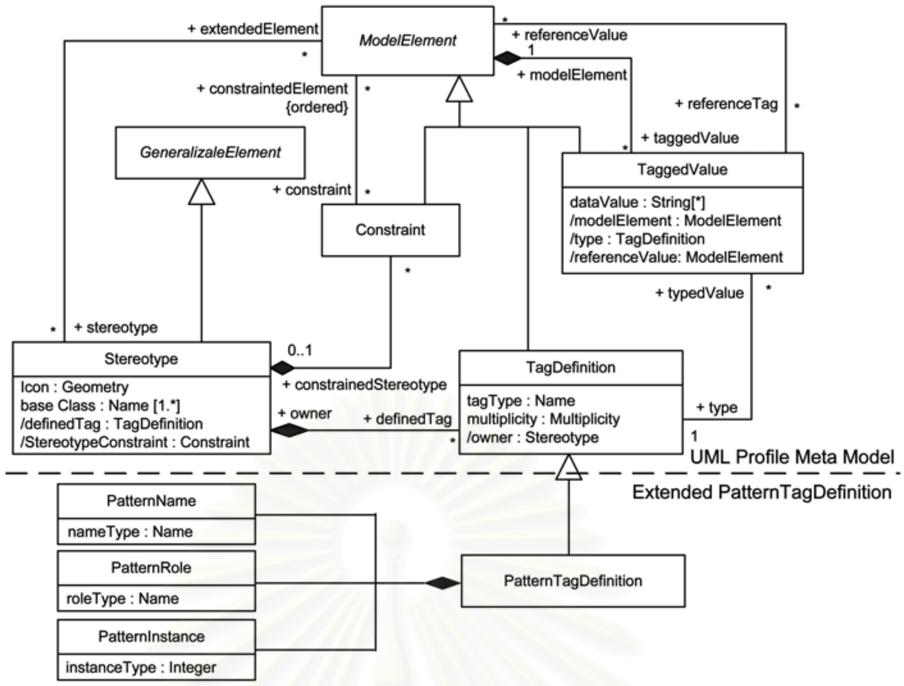
2.2.2 การแสดงแบบรูปการออกแบบในโปรแกรมประยุกต์และส่วนประกอบ (Visualizing Design Patterns in Their Application and Composition)

งานวิจัยนี้ได้เสนอยูเอ็มแอลโพรไฟล์ที่ใช้ในการแสดงแบบรูปการออกแบบในการออกแบบโปรแกรมประยุกต์และส่วนประกอบของโปรแกรมประยุกต์ [12] โดยใช้แผนภาพยูเอ็มแอลคือ แผนภาพคลาส (Class Diagram) และแผนภาพการสื่อสาร (Communication Diagram) โดยแม่พิมพ์ต้นแบบสำหรับแบบรูปการออกแบบที่ได้จากงานวิจัยนี้ แสดงในรูปที่ 2.2

Stereotype	Applies To	Definition
<<PatternClass>>	Class	Indicate that this class is a part of a design pattern
<<PatternAttribute>>	Attribute	Indicate that this attribute is a part of a design pattern
<<PatternOperation>>	Operation	Indicate that this operation is a part of a design pattern

รูปที่ 2.2 แม่พิมพ์ต้นแบบของยูเอ็มแอลโพร์ไฟล์สำหรับแบบรูปการออกแบบ

แม่พิมพ์ต้นแบบสำหรับแบบรูปการออกแบบ ประกอบด้วย แม่พิมพ์ต้นแบบ “PatternClass” ที่ใช้ในการระบุคลาสในแบบรูป แม่พิมพ์ต้นแบบ “PatternAttribute” ที่ใช้ในการระบุคุณลักษณะของคลาสในแบบรูป และแม่พิมพ์ต้นแบบ “PatternOperation” ที่ใช้ในการระบุการดำเนินการของคลาสในแบบรูป และในแต่ละแม่พิมพ์ต้นแบบจะมีป้ายระบุที่ใช้สำหรับแสดงข้อมูลทางโครงสร้างของแบบรูปการออกแบบ ซึ่งเป็นป้ายระบุที่ถูกนิยามเพิ่มเติมจากบทนิยามป้ายระบุ (Tag Defnition) ของยูเอ็มแอลโพรไฟล์เมตาโมเดล (UML Profile Metamodel) [15] เพื่อใช้สำหรับการแสดงข้อมูลทางโครงสร้างของแบบรูปโดยเฉพาะ คือ บทนิยามป้ายระบุแบบรูป (Pattern Tag Definition) แสดงดังรูปที่ 2.3



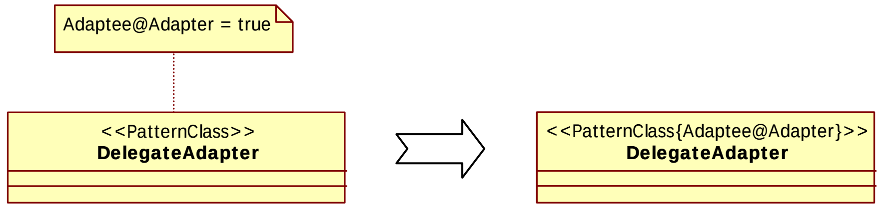
รูปที่ 2.3 ยูเอ็มแอลโพรไฟล์เมตาโมเดลและส่วนที่ถูกนิยามเพิ่มเติม

บทนิยามป้ายระบุแบบรูป ประกอบด้วย ชื่อแบบรูป (Pattern Name) บทบาทในแบบรูป (Pattern Role) และลำดับของแบบรูป (Pattern Instance) โดยองค์ประกอบดังกล่าวจะถูกใช้ในการกำหนดชื่อป้ายระบุที่ได้จากบทนิยามดังกล่าว โดยมีรูปแบบทั่วไปดังนี้

“role@name[instance]”

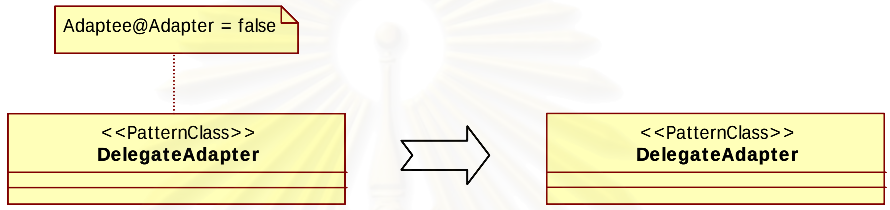
โดย “role” เป็นบทบาทขององค์ประกอบดังกล่าวในแบบรูป “name” เป็นชื่อแบบรูป และ “instance” เป็นลำดับของแบบรูปในแผนภาพ ตัวอย่างของชื่อป้ายระบุที่ได้จากบทนิยามป้ายระบุแบบรูป เช่น “Adaptee@Adapter[2]” เป็นชื่อป้ายระบุที่แสดงถึงบทบาท “Adaptee” ในแบบรูป “Adapter” ลำดับที่ “2” ในแผนภาพ เป็นต้น โดยค่าของป้ายระบุดังกล่าวเป็นบูลีน (Boolean) ซึ่งมีค่าเป็นจริง เมื่อองค์ประกอบดังกล่าวมีลักษณะตามชื่อป้ายระบุ กล่าวคือ องค์ประกอบดังกล่าวมีบทบาท “role” ในแบบรูป “name” ลำดับที่ “instance” ในแผนภาพ และมีค่าเป็นเท็จ เมื่อองค์ประกอบดังกล่าวไม่มีลักษณะตามชื่อป้ายระบุ กล่าวคือ องค์ประกอบดังกล่าวไม่ได้มีบทบาท “role” ในแบบรูป “name” ลำดับที่ “instance” ในแผนภาพ เนื่องจากค่าของป้ายระบุดังกล่าวเป็นบูลีน จึงสามารถระบุค่าของป้ายระบุได้ 2 แบบ คือ

1) ถ้าค่าของป้ายระบุเป็นจริง ผู้ออกแบบไม่จำเป็นต้องระบุชื่อและค่าป้ายระบุที่อยู่ในรูปแบบ “role@name[instance]=true” สามารถลดรูปให้เหลือเพียงการระบุชื่อป้ายระบุเท่านั้น โดยการระบุชื่อป้ายระบุนั้นสามารถระบุไว้ในเครื่องหมายของ “{” และ “}” ที่อยู่ภายในเครื่องหมาย “<<” และ “>>” ของแม่พิมพ์ต้นแบบได้ เนื่องจากป้ายระบุเป็นส่วนประกอบหนึ่งของแม่พิมพ์ต้นแบบ โดยตัวอย่างของการลดรูปของค่าป้ายระบุที่เป็นจริง แสดงดังรูปที่ 2.4



รูปที่ 2.4 การลดรูปของค่าป้ายระบุจากบทนิยามป้ายระบุแบบรูปที่มีค่าเป็นจริง

2) ถ้าค่าของป้ายระบุเป็นเท็จ ผู้ออกแบบไม่จำเป็นต้องระบุชื่อและค่าป้ายระบุดังกล่าวได้ ตัวอย่างของการลดรูปของค่าป้ายระบุที่เป็นเท็จ แสดงดังรูปที่ 2.5



รูปที่ 2.5 การลดรูปของค่าป้ายระบุจากบทนิยามป้ายระบุแบบรูปที่มีค่าเป็นเท็จ

ด้วยวิธีการลดรูปของค่าป้ายระบุดังกล่าว จะช่วยเพิ่มความสะดวกในการระบุข้อมูลของแบบรูป รวมทั้งช่วยลดความซับซ้อนของแผนภาพที่เกิดจากการระบุข้อมูลในแผนภาพมากขึ้น โดยความสัมพันธ์ระหว่างแม่พิมพ์ต้นแบบและค่าป้ายระบุที่สร้างขึ้น สามารถแสดงได้โดยใช้เมตาโมเดลเสมือน (Virtual Metamodel) แสดงดังรูปที่ 2.6 ที่สามารถอธิบายได้ว่า ค่าป้ายระบุ “role@name[instance]” เป็นคุณลักษณะที่แสดงข้อมูลของแบบรูปในแต่ละองค์ประกอบที่ใช้แม่พิมพ์ต้นแบบที่สร้างขึ้น (แม่พิมพ์ต้นแบบ “PatternClass” “PatternOperation” และ “PatternAttribute”)

รูปที่ 2.6 เมตาโมเดลเสมือนของยูเอ็มแอลโพรไฟล์สำหรับแบบรูปการออกแบบ

งานวิจัยดังกล่าวได้สร้างเงื่อนไขบังคับที่เป็นข้อบังคับในการระบุข้อมูลของแม่พิมพ์ต้นแบบและค่าป้ายระบุในรูปแบบของภาษาโอซีแอล โดยรายละเอียดของเงื่อนไขบังคับในแม่พิมพ์ต้นแบบ “PatternClass” แสดงดังรูปที่ 2.7 และเงื่อนไขบังคับของแม่พิมพ์ต้นแบบ “PatternAttribute” และ “PatternOperation” แสดงดังรูปที่ 2.8

```
1> self.taggedValue.dataValue.name -> notEmpty
2> self.taggedValue.name.role -> notEmpty
3> self.taggedValue.name.instance -> isEmpty or self.taggedValue -> exists (tv:taggedValue | tv.name.instance -> notEmpty)
4> self.taggedValue.name -> exists (v1, v2:name | v1.name = v2.name ) implies (v1.instance -> notEmpty and v2.instance ->
   notEmpty and v1.instance <> v2.instance)
```

รูปที่ 2.7 เงื่อนไขบังคับของการใช้งานแม่พิมพ์ต้นแบบ “PatternClass”

```
1> self.taggedValue->exists(tv:taggedValue,pc:PatternClass | tv.name.name = pc.taggedValue.name.name)
2> self.taggedValue->size <= PatternClass.taggedValue.dataValue ->size
3> self.taggedValue.name.role -> notEmpty
4> self.taggedValue.name.name -> isEmpty implies PatternClass.taggedValue.dataValue ->size = 1
5> self.taggedValue.name.name -> isEmpty implies self.taggedValue.name.name = PatternClass.taggedValue. name.name
6> PatternClass.taggedValue.name.instance -> isEmpty implies self.taggedValue.name.instance -> isEmpty
7> (self.taggedValue.name.instance -> isEmpty and PatternClass.taggedValue.name.instance -> notEmpty) implies
   self.taggedValue.name.instance = PatternClass.taggedValue.name.instance
```

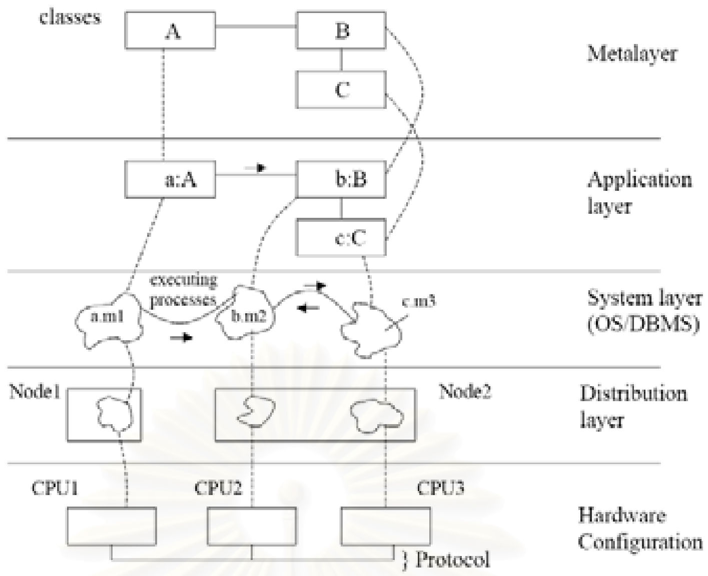
รูปที่ 2.8 เงื่อนไขบังคับของการใช้งานแม่พิมพ์ต้นแบบ “PatternAttribute”
และ “PatternOperation”

สิ่งที่นำมาพิจารณาใช้ในวิทยานิพนธ์นี้คือ บทนิยามป้ายระบุแบบรูป เงื่อนไขบังคับและเมตาโมเดลเสมือน โดยบทนิยามของป้ายระบุ และเงื่อนไขบังคับในแต่ละแม่พิมพ์ต้นแบบสามารถนำมาประยุกต์ใช้ในการสร้างยูเอ็มแอลโพรไฟล์สำหรับการแสดงข้อมูลทางโครงสร้างของแบบรูปความมั่นคงได้ และเมตาโมเดลเสมือนของงานวิจัยดังกล่าว สามารถนำมาประยุกต์ใช้ในการอธิบายความสัมพันธ์ระหว่างแม่พิมพ์ต้นแบบ และค่าป้ายระบุที่ใช้ในงานวิทยานิพนธ์นี้ได้

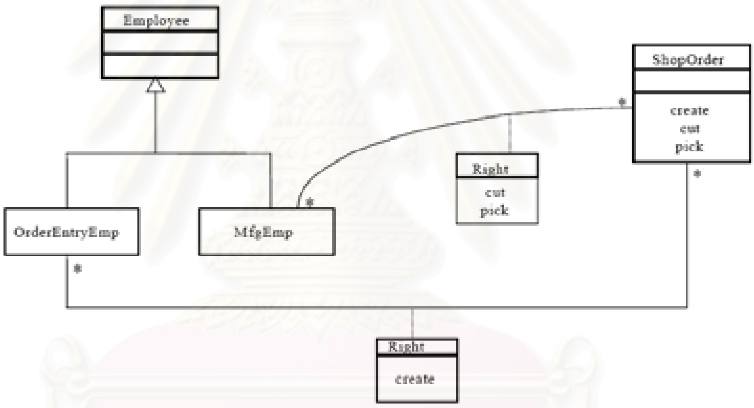
2.2.3 เมตาดาตาและแบบรูปการให้อำนาจ (Metadata and Authorization Pattern)

งานวิจัยนี้ได้เสนอการประยุกต์ใช้แบบรูปการให้อำนาจในระดับของเมตาดาตาหรือประยุกต์ใช้ในการออกแบบคลาส [13] เพื่อควบคุมพฤติกรรมและทิศทางที่นำไปสู่การออกแบบในระดับที่มีความละเอียดมากยิ่งขึ้น งานวิจัยนี้ได้เลือกใช้แบบรูปการให้อำนาจในการกำหนดโครงสร้างของระบบในระดับของคลาส เนื่องจากแบบรูปดังกล่าวเป็นแบบรูปความมั่นคงที่เป็นพื้นฐานของระบบโดยทั่วไป

จากรูปที่ 2.9 แสดงความสัมพันธ์ขององค์ประกอบในแต่ละระดับของระบบ เห็นได้ว่าการออกแบบโครงสร้างในระดับของคลาสมีผลกระทบต่อการออกแบบโครงสร้างในระดับที่ลึกลงไป เช่น การออกแบบในระดับของระบบปฏิบัติการ (Operating System) การออกแบบในระดับของฮาร์ดแวร์ เป็นต้น ดังนั้นการประยุกต์ใช้แบบรูปการให้อำนาจในการออกแบบในระดับของคลาสจะสามารถควบคุมพฤติกรรมและทิศทางของการออกแบบในระดับอื่นให้เป็นไปตามแนวคิดของแบบรูปการให้อำนาจ และจากรูปที่ 2.10 เป็นตัวอย่างของแผนภาพคลาสที่สร้างมาจากแนวคิดของแบบรูปการให้อำนาจ



รูปที่ 2.9 ความสัมพันธ์ขององค์ประกอบในแต่ละระดับของระบบ



รูปที่ 2.10 ตัวอย่างของแผนภาพคลาสที่สร้างมาจากแนวคิดของแบบรูปการให้อำนาจ

สิ่งที่นำมาพิจารณาใช้ในวิทยานิพนธ์นี้ คือ ตัวอย่างของแผนภาพคลาสที่สร้างมาจากแนวคิดของแบบรูปการให้อำนาจ ที่สามารถใช้เป็นตัวอย่างในการสร้างแผนภาพคลาสที่มาจากแนวคิดของแบบรูปความมั่นคง อย่างไรก็ตามแผนภาพคลาสที่ได้จากแนวคิดของแบบรูปการให้อำนาจมิได้ระบุรายละเอียดที่เป็นข้อมูลพื้นฐานของแบบรูปความมั่นคงให้ชัดเจน เช่น หน้าที่ของคลาสในแบบรูปการให้อำนาจ เงื่อนไขบังคับของคลาสในแบบรูปการให้อำนาจ เป็นต้น จึงทำให้ข้อมูลบางส่วนของแบบรูปอาจถูกละเลยได้

2.2.4 การกำหนดความต้องการความมั่นคงโดยใช้ไวยากรณ์ของแบบรูปความมั่นคงสำหรับองค์กร (Defining Security Requirements Using Grammar of Security Patterns for Enterprise)

งานวิจัยนี้ได้เสนอไวยากรณ์ของแบบรูปความมั่นคงเพื่อช่วยในการกำหนดความต้องการความมั่นคงขององค์กร ซึ่งประกอบด้วย [14]

1) ไวยากรณ์การระบุความต้องการความมั่นคงสำหรับสินทรัพย์ขององค์กร (Security needs identification for Enterprise Assets Grammar) เป็นไวยากรณ์ที่ช่วยค้นหาความต้องการความมั่นคงขององค์กรว่าเป็นแบบไหนและคุณลักษณะของความมั่นคงใดอยู่ในส่วนไหนขององค์กรบ้าง

2) ไวยากรณ์การกำหนดมูลค่าสินทรัพย์ (Asset Valuation Grammar) เป็นไวยากรณ์ที่ช่วยในการคำนวณหามูลค่าสินทรัพย์ที่สำคัญขององค์กรทั้งหมด

3) ไวยากรณ์การประเมินภัยคุกคาม (Threat Assessment Grammar) เป็นไวยากรณ์ที่ช่วยกำหนดภัยคุกคามที่คาดว่าจะเกิดขึ้นกับสินทรัพย์ขององค์กร

4) ไวยากรณ์การประเมินภาวะความเสี่ยง (Vulnerability Assessment Grammar) เป็นไวยากรณ์ที่ช่วยกำหนดความอ่อนแอขององค์กรที่อาจทำให้เกิดภัยคุกคามแก่สินทรัพย์ขององค์กรได้

5) ไวยากรณ์การกำหนดค่าความเสี่ยง (Risk Determination Grammar) เป็นไวยากรณ์ที่ช่วยในการคำนวณหาค่าความเสี่ยงของสินทรัพย์

6) ไวยากรณ์การกำหนดแนวคิดความมั่นคงขององค์กร (Enterprise Security Approaches Grammar) เป็นไวยากรณ์ที่ช่วยเลือกแนวคิดความมั่นคงของสินทรัพย์ที่มีความเป็นพิเศษ

7) ไวยากรณ์การกำหนดบริการความมั่นคงขององค์กร (Enterprise Security Services Grammar) เป็นไวยากรณ์ที่ช่วยเลือกบริการความมั่นคงที่ช่วยปกป้องสินทรัพย์หลังจากเลือกแนวทางความมั่นคงแล้ว

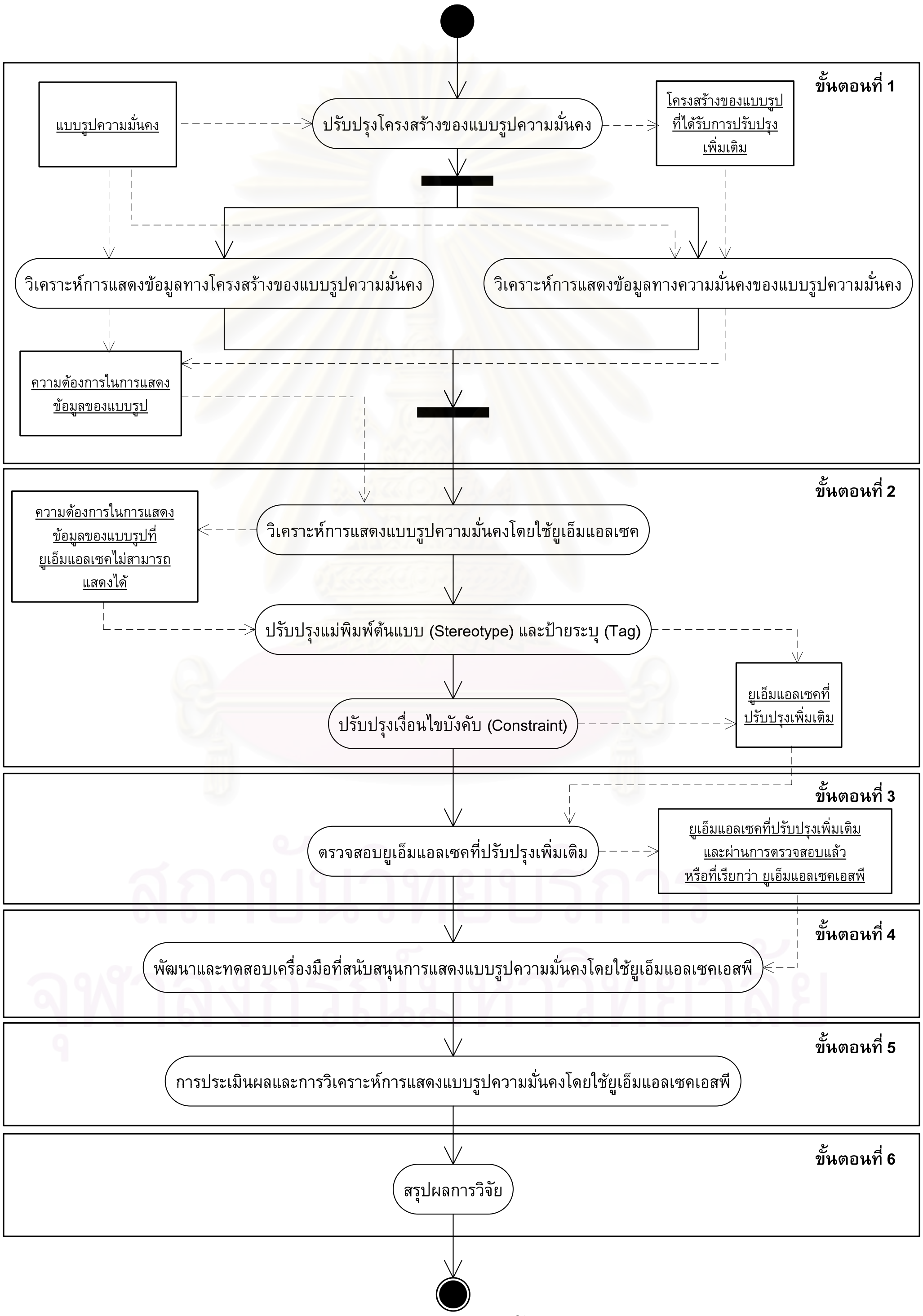
8) ไวยากรณ์การสื่อสารของผู้มีหุ้นส่วนในองค์กร (Enterprise Partner Communication Grammar) เป็นไวยากรณ์ที่ช่วยในการเลือกวิธีในการติดต่อกับองค์กรภายนอก

ไวยากรณ์ความมั่นคงจากงานวิจัยนี้ได้มาจากการวิเคราะห์องค์ประกอบทางโครงสร้างของแบบรูปความมั่นคงจากส่วนประกอบต่างๆ ของแบบรูปความมั่นคง คือส่วนประกอบ “Structure” “Dynamic” และ “Example Resolved” ซึ่งสามารถใช้เป็นแนวทางในการวิเคราะห์ส่วนประกอบของแบบรูปความมั่นคงเพื่อหาองค์ประกอบทางโครงสร้างของแบบรูปที่นำมาพิจารณาใช้ในงานวิทยานิพนธ์นี้

บทที่ 3

การวิเคราะห์แบบรูปความมั่นคงและการขยายยูเอ็มแอลเซค

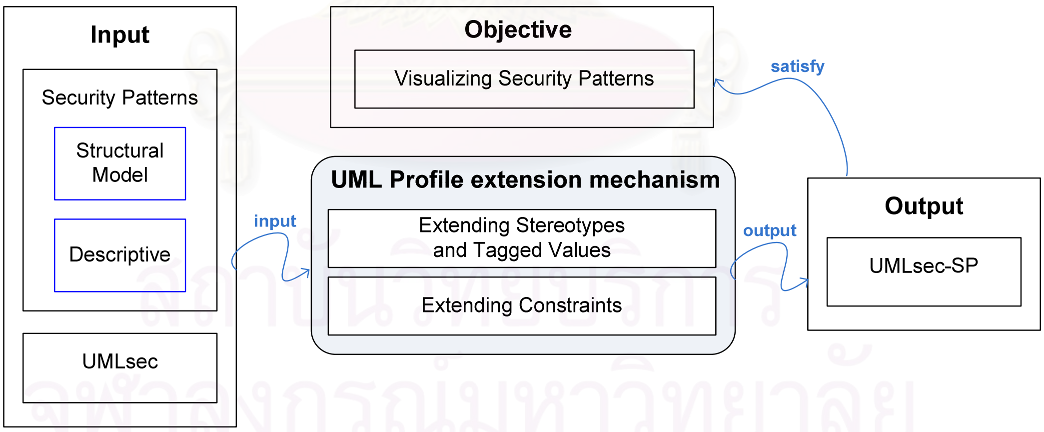
งานวิจัยนี้แบ่งขั้นตอนการดำเนินงานวิจัยออกเป็น 6 ส่วน สามารถแสดงโดยแผนภาพกิจกรรม (Activity Diagram) ดังรูปที่ 3.1



รูปที่ 3.1 แผนภาพกิจกรรมแสดงขั้นตอนการดำเนินงานวิจัย

จากรูปที่ 3.1 ขั้นตอนที่ 1 เป็นขั้นตอนเริ่มต้นของการดำเนินงาน โดยเริ่มจากการปรับปรุงโครงสร้างของแบบรูปความมั่นคง และการวิเคราะห์การแสดงแบบรูปความมั่นคงที่ประกอบไปด้วย การวิเคราะห์การแสดงข้อมูลทางโครงสร้างของแบบรูปความมั่นคง และการวิเคราะห์การแสดงข้อมูลทางความมั่นคงของแบบรูปความมั่นคง ซึ่งผลลัพธ์จากขั้นตอนนี้คือความต้องการในการแสดงข้อมูลทางโครงสร้างและข้อมูลทางความมั่นคงของแบบรูปความมั่นคง ขั้นตอนที่ 2 เป็นขั้นตอนของการปรับปรุงยูเอ็มแอลเซคเพื่อแสดงแบบรูปความมั่นคง กล่าวคือ การปรับปรุงยูเอ็มแอลเซคเพื่อตอบสนองความต้องการในการแสดงข้อมูลของแบบรูปที่ได้จากขั้นตอนก่อนหน้า โดยการวิเคราะห์การแสดงแบบรูปความมั่นคงโดยใช้ยูเอ็มแอลเซคเพื่อหาความต้องการในการแสดงข้อมูลของแบบรูปความมั่นคงที่ยูเอ็มแอลเซคไม่สามารถแสดงได้ ซึ่งความต้องการดังกล่าวจะถูกใช้ในการปรับปรุงแม่พิมพ์ต้นแบบ ป้ายระบุ และเงื่อนไขบังคับของยูเอ็มแอลเซค ขั้นตอนที่ 3 เป็นขั้นตอนของการตรวจสอบยูเอ็มแอลเซคที่ปรับปรุงเพิ่มเติมเพื่อให้มีความถูกต้องและสมบูรณ์มากยิ่งขึ้น ซึ่งผลลัพธ์จากขั้นตอนนี้คือ ยูเอ็มแอลเซคที่ปรับปรุงเพิ่มเติมและผ่านการตรวจสอบแล้ว หรือที่เรียกว่า ยูเอ็มแอลเซคเอสพี (UMLsec for Security Patterns: UMLsec-SP) โดยรายละเอียดทั้ง 3 ขั้นตอนข้างต้น จะแสดงรายละเอียดทั้งหมดในหัวข้อที่ 3.3 สำหรับรายละเอียดในขั้นตอนที่ 4 5 และ 6 ที่เกี่ยวข้องกับการพัฒนาและทดสอบเครื่องมือเพื่อสนับสนุนการแสดงแบบรูปความมั่นคงโดยใช้ยูเอ็มแอลเซคเอสพี การประเมินผลและการวิเคราะห์การแสดงแบบรูปความมั่นคงโดยใช้ยูเอ็มแอลเซคเอสพี และการสรุปผลการวิจัย จะกล่าวถึงต่อไปในบทที่ 4 บทที่ 5 และบทที่ 6 ตามลำดับ

โดยภาพรวมของการสร้างยูเอ็มแอลเซคเอสพี สามารถแสดงได้ดังรูปที่ 3.2



รูปที่ 3.2 ภาพรวมของการสร้างยูเอ็มแอลเซคเอสพี

จากรูปที่ 3.2 ในการสร้างยูเอ็มแอลเซคเอสพีนั้นจะมีข้อมูลนำเข้าอยู่สองส่วนคือ แบบรูปความมั่นคง และยูเอ็มแอลเซค โดยส่วนประกอบของแบบรูปความมั่นคงที่เป็นข้อมูลนำเข้าคือแบบจำลองเชิงโครงสร้าง (Structural Model) ที่เป็นแผนภาพคลาสจากส่วนประกอบ "Structure" ของแบบรูป และข้อมูลที่ได้จากส่วนประกอบอื่นของแบบรูป และส่วนประกอบของยูเอ็มแอลเซคที่เป็นข้อมูลนำเข้าคือ ยูเอ็มแอลโพรไฟล์ของยูเอ็มแอลเซค ซึ่งข้อมูลนำเข้าเหล่านี้จะถูกใช้ในกลไกมาตรฐานในการขยายยูเอ็มแอลที่ประกอบไปด้วย การขยายแม่พิมพ์ต้นแบบ

และค่าป้ายระบุ และการขยายเงื่อนไขบังคับ โดยผลลัพธ์ที่ได้คือ ยูเอ็มแอลเซคเอสพีที่ประกอบไปด้วยแม่พิมพ์ต้นแบบ ค่าป้ายระบุ และเงื่อนไขบังคับ ที่สามารถนำมาประยุกต์ใช้ในการแสดงแบบรูปความมั่นคงในแผนภาพคลาสได้

ในบทนี้จะกล่าวถึง กลไกมาตรฐานในการขยายยูเอ็มแอล และการวิเคราะห์การแสดงแบบรูปความมั่นคง ที่จำเป็นต้องทำความเข้าใจ จากนั้นเป็นขั้นตอนของการขยายยูเอ็มแอลเซคเพื่อแสดงแบบรูปความมั่นคงซึ่งได้รวมขั้นตอนที่ 1 2 และ 3 ในแผนภาพกิจกรรมข้างต้นตามลำดับ ดังรายละเอียดต่อไปนี้

3.1 กลไกมาตรฐานในการขยายยูเอ็มแอล (Standard UML extension mechanism)

ในปัจจุบันยูเอ็มแอลเป็นภาษาที่ได้รับความนิยมในการพัฒนาระบบซอฟต์แวร์เชิงวัตถุ เนื่องจากเป็นภาษาที่สามารถทำการออกแบบระบบซอฟต์แวร์เชิงวัตถุได้หลากหลายประเภท เช่น การออกแบบระบบซอฟต์แวร์เชิงพาณิชย์ การออกแบบระบบซอฟต์แวร์ที่สนับสนุนการจัดการองค์ความรู้ เป็นต้น อย่างไรก็ตามยูเอ็มแอลยังไม่สามารถรองรับการออกแบบระบบซอฟต์แวร์บางประเภทหรือบางโดเมนของการออกแบบระบบซอฟต์แวร์ได้ เช่น การออกแบบระบบทำงานแบบทันที (Real-time System) การออกแบบความมั่นคงของระบบ (System Security) เป็นต้น ดังนั้นยูเอ็มแอลได้จัดเตรียมกลไกมาตรฐานในการขยายยูเอ็มแอลเพื่อประยุกต์ใช้ในการออกแบบระบบซอฟต์แวร์หรือโดเมนของระบบซอฟต์แวร์ที่มีลักษณะเฉพาะ คือ การปรับปรุงยูเอ็มแอลโพรไฟล์ (UML Profile) ที่สนับสนุนการออกแบบในโดเมนที่มีลักษณะเฉพาะ ยูเอ็มแอลโพรไฟล์จะช่วยปรับแต่งยูเอ็มแอลให้เข้ากับโดเมนที่ต้องการได้ โดยการเพิ่มองค์ประกอบชนิดใหม่ พร้อมทั้งคุณลักษณะ และเงื่อนไขในการใช้งานขององค์ประกอบที่อยู่ในโดเมนที่ต้องการ อย่างไรก็ตามกลไกดังกล่าวไม่เหมาะสมสำหรับการปรับแต่งยูเอ็มแอลในส่วนที่เกี่ยวกับโครงสร้างของยูเอ็มแอล [10] ซึ่งในกรณีนี้ผู้พัฒนาจะต้องพัฒนาภาษาใหม่เพื่อรองรับการปรับแต่งดังกล่าว โดยภาษาที่พัฒนาจะต้องประกอบด้วย โครงสร้างพื้นฐานของยูเอ็มแอล และโครงสร้างขององค์ประกอบภายในภาษาใหม่ที่ปรับแต่งขึ้น การปรับปรุงยูเอ็มแอลโพรไฟล์สามารถแบ่งออกเป็น 2 ขั้นตอน โดยมีรายละเอียดดังต่อไปนี้

1) การปรับปรุงแม่พิมพ์ต้นแบบและป้ายระบุ เป็นการกำหนดองค์ประกอบที่ใช้ระบุประเภทขององค์ประกอบและลักษณะขององค์ประกอบดังกล่าวในโดเมนที่ต้องการ โดยขั้นตอนในการปรับปรุงแม่พิมพ์ต้นแบบและป้ายระบุมีรายละเอียดดังต่อไปนี้

1.1) กำหนดความต้องการในการแสดงข้อมูลในแผนภาพยูเอ็มแอล

1.2) วิเคราะห์หาข้อมูลที่ต้องการแสดงในแผนภาพยูเอ็มแอลจากความต้องการที่กำหนดไว้ในขั้นตอนข้างต้น

1.3) สร้างแม่พิมพ์ต้นแบบและป้ายระบุเพื่อตอบสนองข้อมูลที่ต้องการแสดงในแผนภาพยูเอ็มแอล

2) การปรับปรุงเงื่อนไขบังคับ (Constraint) เป็นการระบุข้อบังคับของแม่พิมพ์ต้นแบบที่จำเป็นต้องพิจารณาเมื่อมีการใช้งาน เงื่อนไขบังคับจะช่วยกำหนดขอบเขตของการออกแบบโดยใช้แม่พิมพ์ต้นแบบหรือค่าป้ายระบุของแม่พิมพ์ต้นแบบดังกล่าวได้ โดยขั้นตอนในการปรับปรุงเงื่อนไขบังคับมีรายละเอียดดังต่อไปนี้

2.1) ระบุข้อบังคับในการใช้งานของแต่ละแม่พิมพ์ต้นแบบที่ได้จากขั้นตอนของการปรับปรุงแม่พิมพ์ต้นแบบและค่าป้ายระบุ

2.2) ระบุนิพจน์ของข้อบังคับในการใช้งานแม่พิมพ์ต้นแบบให้เป็นนิพจน์ในภาษาโอซีแอล

โดยรายละเอียดของการปรับปรุงยูเอ็มแอลโพรไฟล์จะกล่าวในขั้นตอนของการขยายยูเอ็มแอลเซคต่อไป

3.2 การวิเคราะห์การแสดงแบบรูปความมั่นคง

การวิเคราะห์การแสดงแบบรูปความมั่นคง แบ่งออกเป็น การวิเคราะห์การแสดงข้อมูลทางโครงสร้างของแบบรูปความมั่นคง และการวิเคราะห์การแสดงข้อมูลทางความมั่นคงของแบบรูปความมั่นคง โดยการวิเคราะห์การแสดงแบบรูปความมั่นคงในงานวิทยานิพนธ์นี้จะมุ่งเน้นการวิเคราะห์การแสดงแบบรูปความมั่นคงในแผนภาพคลาสเท่านั้น เนื่องจากการแสดงข้อมูลของแบบรูปความมั่นคงในงานวิจัยนี้เป็นการแสดงข้อมูลของแบบรูปในระดับเมตาดาตาของระบบ ซึ่งเหมาะแก่การแสดงข้อมูลโดยใช้แผนภาพคลาส โดยรายละเอียดของข้อมูลทางโครงสร้างและข้อมูลทางความมั่นคงของแบบรูปความมั่นคงที่พิจารณามีดังนี้

1) ข้อมูลทางโครงสร้างของแบบรูปความมั่นคง เป็นข้อมูลที่อธิบายโครงสร้างของแบบรูปความมั่นคง โดยข้อมูลดังกล่าวจะช่วยให้ผู้ออกแบบสามารถตรวจสอบและจัดเก็บข้อมูลที่เกี่ยวข้องกับโครงสร้างของแบบรูปความมั่นคงเพื่อใช้การออกแบบและปรับปรุงการออกแบบโครงสร้างโดยใช้แบบรูปความมั่นคง เช่น การกำหนดชื่อแบบรูปความมั่นคงในการออกแบบระบบ จะช่วยให้ผู้ออกแบบทราบว่าโครงสร้างทางความมั่นคงของระบบเป็นไปตามแบบรูปความมั่นคงใดบ้างและผู้ออกแบบสามารถออกแบบและปรับปรุงการออกแบบความมั่นคงของระบบให้พัฒนาต่อยอดจากแบบรูปความมั่นคงที่ใช้อยู่ได้อย่างไรบ้าง เป็นต้น หากผู้ออกแบบละเลยการแสดงข้อมูลทางโครงสร้างของแบบรูปความมั่นคงอาจทำให้เกิดปัญหาที่เกี่ยวข้องกับการออกแบบความมั่นคงของระบบดังนี้

1.1) การตรวจสอบองค์ประกอบที่จำเป็นต้องจัดเก็บไว้ของแบบรูปความมั่นคงในกรณีที่มีการปรับปรุงการออกแบบจะทำได้ยาก เนื่องจากไม่มีการระบุว่าองค์ประกอบแบบจำลองใดเป็นองค์ประกอบทางโครงสร้างของแบบรูปความมั่นคง จึงทำให้ผู้ออกแบบไม่สามารถทราบได้ว่าองค์ประกอบแบบจำลองใดบ้างเป็นองค์ประกอบทางโครงสร้างของแบบรูปความมั่นคง

1.2) การสื่อสารกับผู้อื่นโดยใช้แบบรูปความมั่นคงที่ประยุกต์ใช้ในระบบจะทำได้ยาก เนื่องจากไม่มีการระบุแบบรูปความมั่นคงที่ประยุกต์ใช้ในระบบ จึงทำให้ผู้ออกแบบไม่สามารถทราบได้ว่ามีแบบรูปความมั่นคงใดบ้างที่ประยุกต์ใช้ในระบบ

1.3) การปรับปรุงการออกแบบความมั่นคงของระบบจากคำแนะนำของแบบรูปความมั่นคงที่ประยุกต์ใช้ในระบบจะทำได้ยาก เนื่องจากไม่มีการระบุองค์ประกอบทางโครงสร้างของแบบรูปความมั่นคงที่ประยุกต์ใช้ในระบบ จึงทำให้ผู้ออกแบบไม่สามารถทราบได้ว่าองค์ประกอบใดบ้างที่สามารถปรับปรุงการออกแบบตามคำแนะนำของแบบรูปได้

2) ข้อมูลทางความมั่นคงของแบบรูปความมั่นคง เป็นข้อมูลทางความมั่นคงที่ปรากฏภายในแบบรูปความมั่นคง โดยงานวิทยานิพนธ์นี้ได้พิจารณาข้อมูลทางความมั่นคงของแบบรูปตามความต้องการในการพัฒนายูเอ็มแอลเซคที่มุ่งเน้นการแสดงข้อมูลในแผนภาพคลาสเท่านั้น โดยข้อมูลทางความมั่นคงของแบบรูปที่พิจารณา ประกอบไปด้วย

(1) ข้อมูลที่แสดงแนวคิดทางด้านความมั่นคง เช่น ไฟร์วอลล์ (Firewall) องค์ประกอบที่จัดเส้นทางของแพ็คเกจ (Router) เป็นต้น

(2) ข้อมูลที่แสดงความมั่นคงพื้นฐาน เช่น การเข้ารหัสแบบสมมาตรและอสมมาตร (Symmetric and Asymmetric Encryption) เป็นต้น

(3) ข้อมูลที่แสดงความมั่นคงที่อยู่ภายใต้ระดับกายภาพของระบบ เช่น การกำหนดพร็อกซี่ (Proxy) ภายในไฟร์วอลล์เชิงตัวแทน (Proxy-Based Firewall) การกำหนดองค์ประกอบที่เก็บสถานะของผู้เข้าใช้ไฟร์วอลล์ เป็นต้น

(4) ข้อมูลสำหรับการจัดการทางด้านความมั่นคง เช่น การกำหนดทรัพยากรที่อนุญาตให้เข้าใช้ได้ การกำหนดผลิตภัณฑ์ของไฟร์วอลล์และพอร์ท (Port) ที่เปิดให้ใช้งาน เป็นต้น

หากผู้ออกแบบละเลยการแสดงข้อมูลทางความมั่นคงดังกล่าวอาจทำให้เกิดปัญหาที่เกี่ยวกับการออกแบบความมั่นคงของระบบดังนี้

2.1) ผู้ออกแบบอาจละเลยการตรวจสอบองค์ประกอบทางความมั่นคงที่สำคัญได้ เนื่องจากไม่มีการระบุองค์ประกอบทางความมั่นคงในระบบ จึงทำให้ผู้ออกแบบไม่สามารถทราบได้ว่าองค์ประกอบใดเป็นองค์ประกอบทางความมั่นคงในระบบ

2.2) การจัดการทางด้านความมั่นคงของระบบอาจทำได้ไม่สมบูรณ์ ถ้าผู้ออกแบบละเลยการกำหนดข้อมูลที่มีความสำคัญต่อการจัดการทางด้านความมั่นคงในระบบ

โดยรายละเอียดของการวิเคราะห์การแสดงแบบรูปความมั่นคงจะกล่าวในขั้นตอนของการขยายยูเอ็มแอลเซคเพื่อแสดงแบบรูปความมั่นคงต่อไป

3.3 การขยายยูเอ็มแอลเซคเพื่อแสดงแบบรูปความมั่นคง

ในขั้นตอนนี้เป็นการขยายยูเอ็มแอลเซคโดยใช้กลไกมาตรฐานในการขยายยูเอ็มแอลซึ่งประกอบไปด้วย การปรับปรุงแม่พิมพ์ต้นแบบ ป้ายระบุ และเงื่อนไขบังคับของยูเอ็มแอลเซคเพื่อ

แสดงข้อมูลทางโครงสร้างและข้อมูลทางความมั่นคงของแบบรูปความมั่นคง โดยขั้นตอนของการขยายยูเอ็มแอลเซคแสดงดังรูปที่ 3.3

ขั้นตอนวิธี การขยายยูเอ็มแอลเซคเพื่อแสดงแบบรูปความมั่นคง

ข้อมูลนำเข้า : ยูเอ็มแอลเซค, แบบรูปความมั่นคง

ข้อมูลนำออก : ยูเอ็มแอลเซคที่ปรับปรุงเพิ่มเติม

ข้อกำหนด : {แผนภาพคลาส}

เงื่อนไขก่อน : -

พิจารณาในแต่ละแบบรูปความมั่นคง

1. ปรับปรุงโครงสร้างของแบบรูปความมั่นคง
2. วิเคราะห์การแสดงแบบรูปความมั่นคง
    - 2.1. วิเคราะห์การแสดงข้อมูลทางโครงสร้างของแบบรูปความมั่นคง
    - 2.2. วิเคราะห์การแสดงข้อมูลทางความมั่นคงของแบบรูปความมั่นคง
3. วิเคราะห์การแสดงแบบรูปความมั่นคงโดยใช้ยูเอ็มแอลเซค
4. ปรับปรุงยูเอ็มแอลเซคเพื่อแสดงแบบรูปความมั่นคง
    - 4.1. ปรับปรุงแม่พิมพ์ต้นแบบและป้ายระบุของยูเอ็มแอลเซค
        - 4.1.1. ระบุข้อมูลของแบบรูปความมั่นคงที่ต้องการแสดง
        - 4.1.2. ปรับปรุงแม่พิมพ์ต้นแบบและป้ายระบุ
        - 4.1.3. กำหนดรูปแบบของแม่พิมพ์ต้นแบบและค่าป้ายระบุ
    - 4.2. ปรับปรุงเงื่อนไขบังคับของยูเอ็มแอลเซค
5. ตรวจสอบยูเอ็มแอลเซคที่ปรับปรุงเพิ่มเติม

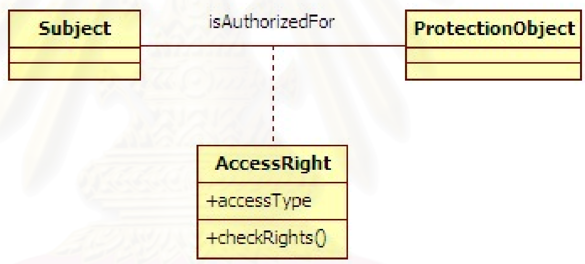
เงื่อนไขหลัง : ยูเอ็มแอลเซคที่ปรับปรุงเพิ่มเติมสามารถแสดงข้อมูลทางโครงสร้างและข้อมูลทางความมั่นคงของแบบรูปความมั่นคงได้

รูปที่ 3.3 ขั้นตอนการขยายยูเอ็มแอลเซคเพื่อแสดงแบบรูปความมั่นคง

ในการขยายยูเอ็มแอลเซคนั้น ผู้วิจัยได้กำหนดข้อมูลนำเข้าคือ ยูเอ็มแอลเซคและแบบรูปความมั่นคง ซึ่งขอบเขตของการขยายยูเอ็มแอลเซคนั้นจะครอบคลุมเพียงแผนภาพคลาสเท่านั้น โดยขั้นตอนแรกของการขยายยูเอ็มแอลเซค คือ การปรับปรุงโครงสร้างของแบบรูปความมั่นคง โดยการพิจารณาจากส่วนประกอบต่างๆ ในแบบรูปความมั่นคง จากนั้นเป็นขั้นตอนที่ 2 ที่เป็นการวิเคราะห์การแสดงแบบรูปความมั่นคงโดยแบ่งเป็น การวิเคราะห์การแสดงข้อมูลทางโครงสร้างของแบบรูปความมั่นคง และการวิเคราะห์ข้อมูลทางความมั่นคงของแบบรูปความมั่นคง ขั้นตอนที่ 3 คือ การปรับปรุงยูเอ็มแอลเซคโดยแบ่งเป็น การปรับปรุงแม่พิมพ์ต้นแบบและป้ายระบุ และการปรับปรุงเงื่อนไขบังคับ ขั้นตอนที่ 4 คือ การตรวจสอบยูเอ็มแอลเซคที่ปรับปรุงเพิ่มเติมโดยการตรวจสอบจากคุณสมบัติมาตรฐานของยูเอ็มแอลโพรไฟล์ เพื่อความสะดวกในการทำความเข้าใจในขั้นตอนการขยายยูเอ็มแอลเซค ผู้วิจัยได้ใช้แบบรูปการให้อำนาจซึ่งเป็นแบบรูปความมั่นคงในกลุ่มแบบจำลองการควบคุมการเข้าถึงมาเป็นกรณีศึกษา เนื่องจากแบบรูปดังกล่าวเป็นแบบรูปความมั่นคงพื้นฐานที่ใช้ในการออกแบบความมั่นคงของระบบโดยทั่วไป โดยรายละเอียดของขั้นตอนการขยายยูเอ็มแอลเซคมีดังต่อไปนี้

1) ปรับปรุงโครงสร้างของแบบรูปความมั่นคง

การปรับปรุงโครงสร้างของแบบรูปความมั่นคง เป็นการนำโครงสร้างของแบบรูปความมั่นคงจากส่วนประกอบ “Structure” ที่แสดงลักษณะทางโครงสร้างของแบบรูปมาปรับปรุงโดยการพิจารณาจากส่วนประกอบอื่นของแบบรูป เนื่องจากโครงสร้างของแบบรูปความมั่นคงที่ได้จากส่วนประกอบดังกล่าวนั้นอาจไม่ครอบคลุมองค์ประกอบทางโครงสร้างที่ปรากฏอยู่ในส่วนประกอบอื่นของแบบรูป ซึ่งองค์ประกอบเหล่านี้อาจถูกเพิ่มขึ้นมาเพื่อใช้ในบางกรณีของแบบรูปความมั่นคง ดังนั้นในการขยายยูเอ็มแอลเซคจึงจำเป็นต้องพิจารณาองค์ประกอบจากส่วนประกอบอื่นของแบบรูปความมั่นคงเพื่อให้ยูเอ็มแอลเซคที่ปรับปรุงเพิ่มเติมสามารถแสดงองค์ประกอบของแบบรูปความมั่นคงได้ครบทุกกรณีภายในแบบรูปความมั่นคง ผู้วิจัยได้ใช้แบบรูปการให้อำนาจซึ่งเป็นแบบรูปความมั่นคงในกลุ่มแบบจำลองการควบคุมการเข้าถึงมาเป็นกรณีศึกษา โดยแบบรูปการให้อำนาจเป็นแบบรูปที่อธิบายเกี่ยวกับการให้อำนาจแก่ผู้เข้าใช้ทรัพยากรของระบบในกรณีที่ระบบมีทรัพยากรที่ต้องควบคุมการเข้าถึง เนื่องจากทรัพยากรดังกล่าวนั้นเป็นทรัพยากรที่มีความสำคัญต่อระบบ โดยแผนภาพคลาสที่แสดงโครงสร้างของแบบรูปการให้อำนาจจากส่วนประกอบ “Structure” ของแบบรูป แสดงดังรูปที่ 3.4



รูปที่ 3.4 แผนภาพคลาสที่แสดงโครงสร้างของแบบรูปการให้อำนาจจากส่วนประกอบ “Structure” ของแบบรูป

โครงสร้างของแบบรูปการให้อำนาจประกอบด้วยองค์ประกอบที่สำคัญคือ ผู้ใช้ทรัพยากร (คลาส “Subject”) เป็นผู้ที่ต้องการเข้าใช้ทรัพยากรในระบบ ทรัพยากรในระบบ (คลาส “ProtectionObject”) เป็นทรัพยากรที่ต้องควบคุมการเข้าถึง และองค์ประกอบที่ควบคุมการเข้าถึงทรัพยากร (คลาส “AccessRight”)

โดยส่วนประกอบอื่นของแบบรูปความมั่นคงที่นำมาพิจารณาหาองค์ประกอบทางโครงสร้างของแบบรูปความมั่นคงในงานวิจัยนี้ ประกอบด้วย ส่วนประกอบ “Dynamic” “Implementation” “Solution” “Example Resolved” และ “Variant” โดยรายละเอียดของแต่ละส่วนประกอบมีดังต่อไปนี้

(1) ส่วนประกอบ “Dynamic” เป็นส่วนที่แสดงสถานการณ์จำลองที่สามารถนำแบบรูปไปประยุกต์ใช้ได้ ซึ่งแสดงให้เห็นถึงพฤติกรรมของแบบรูป ส่วนใหญ่เสนอโดยแผนภาพลำดับ (Sequence Diagram) เพื่อแสดงให้เห็นว่าแบบรูปต้องทำอะไรบ้าง และมีการติดต่อกันระหว่างองค์ประกอบใด

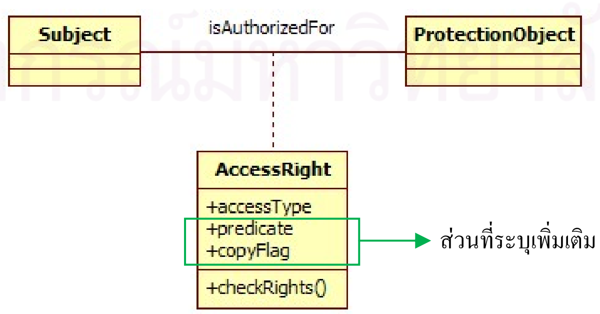
(2) ส่วนประกอบ “Implementation” เป็นส่วนที่แสดงแนวทางในการนำแบบรูปไปใช้งาน ส่วนใหญ่เสนอเป็นขั้นตอนของการนำแบบรูปไปประยุกต์ใช้ในการแก้ไขปัญหาของระบบ

(3) ส่วนประกอบ “Solution” เป็นส่วนที่เสนอผลเฉลย (Solution) ตามหลักการพื้นฐานของแบบรูปดังกล่าว โดยการเสนอรายการของสิ่งที่จำเป็นต้องปฏิบัติตาม หรือส่วนประกอบพร้อมคำอธิบาย

(4) ส่วนประกอบ “Example Resolved” เป็นส่วนที่แสดงคุณลักษณะสำคัญ หรือตัวอย่างผลลัพธ์ที่ได้จากการแก้ปัญหาซึ่งอยู่นอกเหนือจากส่วนประกอบ “Structure” “Dynamic” และ “Implementation”

(5) ส่วนประกอบ “Variant” เป็นส่วนที่เสนอรูปแบบพิเศษของแบบรูปความมั่นคงที่แสดงให้เห็นถึงรูปแบบอื่นของแบบรูปความมั่นคง ส่วนใหญ่จะเป็นการนำแบบรูปความมั่นคงไปประยุกต์ให้มีความเหมาะสมในการใช้งานมากยิ่งขึ้น

จากการพิจารณาส่วนประกอบอื่นของแบบรูปการให้อำนาจพบว่า ในส่วนประกอบ “Variant” ของแบบรูปดังกล่าวได้เสนอ ลักษณะขององค์ประกอบที่ควบคุมการเข้าถึงทรัพยากรเพิ่มเติม คือ ลักษณะที่อธิบายเงื่อนไขที่เป็นข้อห้ามของการให้อำนาจ (Predicate) เป็นเงื่อนไขที่จำเป็นต้องพิจารณาเพื่อป้องกันการละเมิดข้อกำหนดภายในองค์กร เช่น การเข้าใช้ทรัพยากรในระบบจะต้องอยู่ในช่วงเวลาทำงานขององค์กรเสมอ เป็นต้น และลักษณะที่อธิบายการอนุญาตให้ผู้อื่นคัดลอกอำนาจของผู้ใช้งานดังกล่าวได้ (Copy flag) เป็นลักษณะที่แสดงว่าอำนาจในการเข้าใช้ทรัพยากรของบุคคลดังกล่าวสามารถถูกคัดลอกได้หรือไม่ โดยลักษณะดังกล่าวจะถูกใช้ในการกำหนดคุณลักษณะของบุคคลที่มีความสำคัญต่อระบบได้ เช่น อำนาจในการเข้าใช้ทรัพยากรของผู้ใช้งานทั่วไปสามารถถูกคัดลอกได้ แต่อำนาจในการเข้าใช้ทรัพยากรของผู้ดูแลระบบจะไม่สามารถถูกคัดลอกได้ เป็นต้น ดังนั้นลักษณะดังกล่าวจะถูกนำมาพิจารณาในการปรับปรุงโครงสร้างของแบบรูปการให้อำนาจโดย การเพิ่มคุณลักษณะ “predicate” ที่อธิบายเงื่อนไขที่เป็นข้อห้ามในการให้อำนาจ และคุณลักษณะ “copyFlag” ที่อธิบายการอนุญาตให้ผู้อื่นคัดลอกอำนาจของผู้ใช้งานดังกล่าวได้ ในคลาส “AccessRight” ของแบบรูป โดยโครงสร้างของแบบรูปการให้อำนาจที่เพิ่มเติมคุณลักษณะดังกล่าว แสดงดังรูปที่ 3.5



รูปที่ 3.5 แผนภาพคลาสของแบบรูปการให้อำนาจที่ปรับปรุงเพิ่มเติม

2) วิเคราะห์การแสดงแบบรูปความมั่นคง

การวิเคราะห์การแสดงแบบรูปความมั่นคง เป็นการนำโครงสร้างของแบบรูปความมั่นคงที่ได้รับการปรับปรุงเพิ่มเติมผนวกกับข้อมูลจากส่วนประกอบของแบบรูปมาวิเคราะห์หาความต้องการในการแสดงข้อมูลทางโครงสร้างและข้อมูลทางความมั่นคงของแบบรูปความมั่นคง โดยการวิเคราะห์จะแบ่งออกเป็น การวิเคราะห์การแสดงข้อมูลทางโครงสร้างของแบบรูปความมั่นคง และการวิเคราะห์การแสดงข้อมูลทางความมั่นคงของแบบรูปความมั่นคง โดยมีรายละเอียดดังต่อไปนี้

2.1) วิเคราะห์การแสดงข้อมูลทางโครงสร้างของแบบรูปความมั่นคง

การวิเคราะห์การแสดงข้อมูลทางโครงสร้างของแบบรูปความมั่นคง เป็นการวิเคราะห์หาความต้องการในการแสดงข้อมูลที่อธิบายโครงสร้างของแบบรูปความมั่นคง โดยลักษณะของความต้องการในการแสดงข้อมูลทางโครงสร้างของแบบรูปความมั่นคงที่นำมาพิจารณาในการปรับปรุงยูเอ็มแอลเซค ประกอบไปด้วย

(1) <u>ความต้องการในการแสดงข้อมูลทางโครงสร้างโดยรวมของแบบรูป</u> เป็นความต้องการในการแสดงข้อมูลที่อธิบายลักษณะที่เป็นภาพรวมของแบบรูปความมั่นคง จากการพิจารณาแบบรูปการให้อำนาจ ได้ความต้องการในการแสดงข้อมูลทางโครงสร้างโดยรวมของแบบรูป ดังต่อไปนี้

(1.1) *ความต้องการในการแสดงชื่อแบบรูปความมั่นคง* เป็นความต้องการในการแสดงชื่อแบบรูปความมั่นคงที่ใช้ในแผนภาพ เพื่อใช้ในการระบุแบบรูปความมั่นคงในระบบ จากแบบรูปตัวอย่าง ชื่อแบบรูปความมั่นคง คือ การให้อำนาจ (Authorization)

(1.2) *ความต้องการในการแสดงลำดับของแบบรูปความมั่นคงที่ประยุกต์ใช้ในกรณีที่มีการใช้แบบรูปที่ซ้ำกัน* เป็นความต้องการในการแสดงลำดับที่จำเป็นต้องกำหนดในแต่ละแบบรูป เพื่อใช้ในจำแนกแบบรูปในกรณีที่มีการใช้แบบรูปที่ซ้ำกัน

(2) <u>ความต้องการในการแสดงข้อมูลทางโครงสร้างขององค์ประกอบแบบจำลองในแบบรูป</u> เป็นความต้องการในการแสดงข้อมูลที่อธิบายลักษณะขององค์ประกอบแบบจำลองในแบบรูป จากการพิจารณาแบบรูปการให้อำนาจ ได้ความต้องการในการแสดงข้อมูลทางโครงสร้างขององค์ประกอบแบบจำลองในแบบรูป ดังต่อไปนี้

(2.1) ความต้องการในการแสดงองค์ประกอบแบบจำลองในแบบรูปความมั่นคง จากการพิจารณาแบบรูปการให้อำนาจ ชนิดองค์ประกอบแบบจำลองในแบบรูป คือ คลาส แบบชนิดข้อมูล (Data type) และความสัมพันธ์ระหว่างคลาส

(2.2) ความต้องการในการแสดงบทบาทขององค์ประกอบแบบจำลองในแบบรูปความมั่นคง จากแบบรูปการให้อำนาจ บทบาทของแต่ละองค์ประกอบแบบจำลองในแบบรูป คือ คลาส “Subject” เป็นผู้เข้าใช้ทรัพยากร คลาส “ProtectionObject” เป็นทรัพยากรที่ถูกควบคุม คลาส “AccessRight” เป็นองค์ประกอบที่ควบคุมการเข้าใช้ทรัพยากร คุณลักษณะ “accessType” เป็นลักษณะของการเข้าถึงทรัพยากร คุณลักษณะ “predicate” อธิบายข้อห้าม

ในการให้อำนาจ คุณลักษณะ “copyFlag” อธิบายการอนุญาตให้ผู้อื่นคัดลอกอำนาจของผู้ใช้งานดังกล่าว และการดำเนินการ “checkRights” เป็นการดำเนินการที่ใช้ในการตรวจสอบอำนาจของผู้ใช้งาน

จากความต้องการในการแสดงข้อมูลทางโครงสร้างของแบบรูปความมั่นคงข้างต้น จะถูกนำมาใช้ในขั้นตอนของการวิเคราะห์การแสดงแบบรูปความมั่นคงโดยใช้ยูเอ็มแอลเซค ต่อไป

2.2) วิเคราะห์การแสดงข้อมูลทางความมั่นคงของแบบรูปความมั่นคง

การวิเคราะห์การแสดงข้อมูลทางความมั่นคงของแบบรูปความมั่นคง เป็นการวิเคราะห์หาความต้องการในการแสดงข้อมูลที่เป็นองค์ประกอบทางด้านความมั่นคงของแบบรูป โดยลักษณะของความต้องการในการแสดงข้อมูลทางความมั่นคงของแบบรูปความมั่นคงที่นำมาพิจารณาในการปรับปรุงยูเอ็มแอลเซค ประกอบไปด้วย

(1) <u>ความต้องการในการแสดงองค์ประกอบทางความมั่นคง</u> เป็นความต้องการในการแสดงองค์ประกอบแบบจำลองที่มีนัยสำคัญทางด้านความมั่นคง จากการพิจารณาแบบรูปการให้อำนาจ ได้ความต้องการในการแสดงองค์ประกอบทางความมั่นคงในแบบรูปดังนี้

(1.1) *ความต้องการในการแสดงผู้เข้าใช้ทรัพยากรในระบบ* ผู้เข้าใช้ทรัพยากรของระบบ ประกอบไปด้วย ผู้ใช้ (User) และกระบวนการในระบบ (Process)

(1.2) *ความต้องการในการแสดงทรัพยากรที่ถูกควบคุมการเข้าถึง* เช่น รายการเปลี่ยนแปลง (Transaction) ข้อมูลสารสนเทศ (Information) หน่วยความจำ (Memory) อุปกรณ์รับเข้า/ส่งออก (I/O devices) แฟ้มข้อมูล (File) เป็นต้น

(1.3) *ความต้องการในการระบุองค์ประกอบที่ควบคุมการเข้าถึงทรัพยากร* องค์ประกอบดังกล่าวจะมีคุณลักษณะที่อธิบายลักษณะในการเข้าถึงทรัพยากร และมีการดำเนินการที่ใช้ในการตรวจสอบผู้เข้าใช้ทรัพยากร

(1.4) *ความต้องการในการระบุลักษณะในการเข้าถึงทรัพยากร* เช่น การอ่านเอกสาร การสร้างแฟ้มข้อมูล เป็นต้น

(1.5) *ความต้องการในการระบุเงื่อนไขที่เป็นข้อห้ามของการให้อำนาจ* เช่น ผู้ใช้งานสามารถเข้าใช้สินทรัพย์ขององค์กรได้ในช่วงเวลาที่กำหนดไว้เท่านั้น เป็นต้น

(1.6) *ความต้องการในการระบุลักษณะในการอนุญาตให้ผู้อื่นคัดลอกอำนาจของผู้ใช้งานดังกล่าวได้* เป็นการอธิบายว่าอำนาจในการเข้าใช้ทรัพยากรของผู้ใช้งานใดบ้างที่สามารถถูกคัดลอกได้ เช่น ระบบสามารถกำหนดอำนาจในการเข้าใช้ทรัพยากรของนาย ก ให้เหมือนกับอำนาจในการเข้าใช้ทรัพยากรของนาย ข ได้ เป็นต้น

(2) <u>ความต้องการในการแสดงลักษณะขององค์ประกอบทางความมั่นคง</u> เป็นความต้องการในการแสดงข้อมูลที่อธิบายลักษณะขององค์ประกอบทางความมั่นคงให้ชัดเจนมากยิ่งขึ้น จากการพิจารณาแบบรูปการให้อำนาจ จะได้ความต้องการในการแสดงลักษณะขององค์ประกอบแบบจำลองทางความมั่นคงในแบบรูปดังนี้

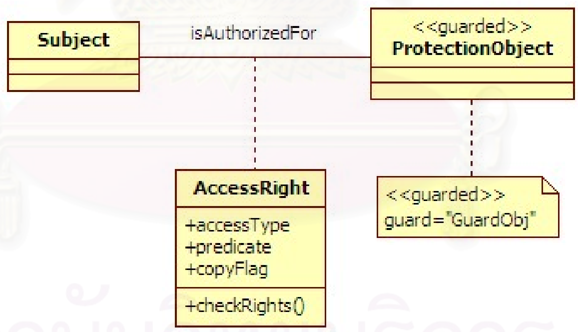
(2.1) *ความต้องการในการแสดงอ็อบเจกต์ที่ควบคุมการเข้าถึงทรัพยากร* เป็นการกำหนดหน้าที่ให้แก่อ็อบเจกต์ที่ควบคุมการเข้าถึงทรัพยากรที่ต้องการโดยเฉพาะ

(2.2) *ความต้องการในการแสดงประเภทขององค์ประกอบที่ควบคุมการเข้าถึงทรัพยากร* เช่น องค์ประกอบที่ควบคุมทรัพยากรโดยใช้รายการควบคุมการเข้าถึง (Access Control Lists: ACLs) ที่ประกอบไปด้วยคู่ลำดับของผู้เข้าใช้ทรัพยากรและการดำเนินการที่สามารถกระทำได้ องค์ประกอบที่ควบคุมทรัพยากรโดยใช้รายการที่แสดงสมรรถนะของผู้เข้าใช้ (Capabilities) ที่ประกอบไปด้วยคู่ลำดับของผู้เข้าใช้ทรัพยากรและสิทธิ์ในการเข้าถึงทรัพยากรเป็นต้น

จากความต้องการในการแสดงข้อมูลทางความมั่นคงของแบบรูปความมั่นคงข้างต้นจะถูกนำมาใช้ในขั้นตอนของการวิเคราะห์การแสดงแบบรูปความมั่นคงโดยใช้ยูเอ็มแอลเซคต่อไป

3) วิเคราะห์การแสดงแบบรูปความมั่นคงโดยใช้ยูเอ็มแอลเซค

ในขั้นตอนนี้เป็นการวิเคราะห์การแสดงแบบรูปความมั่นคงโดยใช้ยูเอ็มแอลเซค โดยการวิเคราะห์การแสดงข้อมูลของแบบรูปความมั่นคงตามความต้องการที่ได้จากขั้นตอนข้างต้นโดยใช้ยูเอ็มแอลเซคช่วยแสดงข้อมูลดังกล่าว จากการประยุกต์ใช้ยูเอ็มแอลเซคในการแสดงข้อมูลของแบบรูปการให้อำนาจ จะได้แผนภาพคลาสของแบบรูปการให้อำนาจที่ใช้ยูเอ็มแอลเซคแสดงดังรูปที่ 3.6



รูปที่ 3.6 แผนภาพคลาสของแบบรูปการให้อำนาจที่ใช้ยูเอ็มแอลเซค

จากรูปที่ 3.6 ยูเอ็มแอลเซคช่วยแสดงข้อมูลทางความมั่นคงของแบบรูปการให้อำนาจโดยการระบุทรัพยากรที่ป้องกันโดยใช้แม่พิมพ์ต้นแบบ “guarded” กำกับคลาสในที่นี้คือ คลาส “ProtectionObject” นอกจากนี้ยูเอ็มแอลเซคช่วยแสดงองค์ประกอบที่ควบคุมการเข้าถึงทรัพยากรโดยการระบุชื่ออ็อบเจกต์ที่ควบคุมการเข้าถึงทรัพยากรดังกล่าวในค่าป้ายระบุ “guard” (guard=”GuardObj”) เห็นได้ว่า ยูเอ็มแอลเซคมีแม่พิมพ์ต้นแบบและค่าป้ายระบุที่สามารถตอบสนองได้เพียงความต้องการในการแสดงทรัพยากรที่ถูกควบคุมการเข้าถึง และความต้องการในการแสดงองค์ประกอบที่ควบคุมการเข้าถึงทรัพยากรดังกล่าวเท่านั้น แต่ไม่สามารถตอบสนองความต้องการในการแสดงข้อมูลทางโครงสร้างและข้อมูลทางความมั่นคงของ

แบบรูปได้ทั้งหมด ดังนั้นความต้องการในการแสดงข้อมูลทางโครงสร้างและข้อมูลทางความมั่นคงของแบบรูปที่ไม่สามารถแสดงได้โดยใช้ยูเอ็มแอลเซค จะถูกนำไปพิจารณาในการปรับปรุงยูเอ็มแอลเซคต่อไป

4) ปรับปรุงยูเอ็มแอลเซคเพื่อแสดงแบบรูปความมั่นคง

ในขั้นตอนนี้เป็นการปรับปรุงยูเอ็มแอลเซคโดยการนำความต้องการในการแสดงข้อมูลทางโครงสร้างและข้อมูลทางความมั่นคงของแบบรูปความมั่นคงที่ยูเอ็มแอลเซคไม่สามารถแสดงได้มาพิจารณาในการปรับปรุงยูเอ็มแอลเซคโดยใช้กลไกมาตรฐานในการขยายยูเอ็มแอล ที่แบ่งเป็น 2 ขั้นตอน คือ การปรับปรุงแม่พิมพ์ต้นแบบและป้ายระบุของยูเอ็มแอลเซค และการปรับปรุงเงื่อนไขบังคับของยูเอ็มแอลเซค โดยมีรายละเอียดดังต่อไปนี้

4.1) ปรับปรุงแม่พิมพ์ต้นแบบและป้ายระบุของยูเอ็มแอลเซค

การปรับปรุงแม่พิมพ์ต้นแบบและป้ายระบุ เป็นการแก้ไขแม่พิมพ์ต้นแบบและป้ายระบุของยูเอ็มแอลเซค หรือสร้างแม่พิมพ์ต้นแบบและป้ายระบุขึ้นมาใหม่ที่นอกเหนือจากยูเอ็มแอลเซคและองค์ประกอบมาตรฐานของยูเอ็มแอล (UML standard element) [16] การปรับปรุงแม่พิมพ์ต้นแบบและป้ายระบุของยูเอ็มแอลเซคมีจุดประสงค์เพื่อให้ยูเอ็มแอลเซคสามารถแสดงประเภทและลักษณะเฉพาะขององค์ประกอบแบบจำลองที่มาจากความต้องการในการแสดงข้อมูลทางโครงสร้างและข้อมูลทางความมั่นคงของแบบรูปความมั่นคงได้ โดยขั้นตอนของการปรับปรุงแม่พิมพ์ต้นแบบและป้ายระบุของยูเอ็มแอลเซคเป็นดังนี้

4.1.1) ระบุข้อมูลของแบบรูปความมั่นคงที่ต้องการแสดง

ในขั้นตอนนี้เป็นการระบุข้อมูลทางโครงสร้างและข้อมูลทางด้านความมั่นคงของแบบรูปความมั่นคงจากความต้องการในการแสดงข้อมูลของแบบรูปความมั่นคงที่ยูเอ็มแอลเซคไม่สามารถแสดงได้ จากการพิจารณาความต้องการในการแสดงข้อมูลของแบบรูปการให้อำนาจที่ยูเอ็มแอลเซคไม่สามารถแสดงได้ จะได้ข้อมูลของแบบรูปการให้อำนาจที่ต้องการแสดงดังต่อไปนี้

(1) ข้อมูลทางโครงสร้างของแบบรูปความมั่นคงที่ต้องการแสดง คือ
- (1.1) ชื่อแบบรูปความมั่นคง
- (1.2) ลำดับของแบบรูปความมั่นคงที่ประยุกต์ใช้ในกรณีที่มีการใช้แบบรูปที่ซ้ำกัน
- (1.3) องค์ประกอบแบบจำลองในแบบรูปความมั่นคง
- (1.4) บทบาทขององค์ประกอบแบบจำลองในแบบรูปความมั่นคง

(2) ข้อมูลทางความมั่นคงของแบบรูปความมั่นคง คือ
- (2.1) ผู้เข้าใช้ทรัพยากร
- (2.2) องค์ประกอบที่ควบคุมการเข้าถึงทรัพยากร
- (2.3) ลักษณะในการเข้าถึงทรัพยากร

(2.4) เงื่อนไขที่เป็นข้อห้ามการให้อำนาจ

(2.5) ลักษณะในการอนุญาตให้ผู้อื่นคัดลอกอำนาจของผู้ใช้งานดังกล่าว

(2.6) ประเภทขององค์ประกอบที่ควบคุมการเข้าถึงทรัพยากร

จากข้อมูลของแบบรูปความมั่นคงที่ต้องการแสดงข้างต้น จะถูกนำมาใช้ในการปรับปรุงแม่พิมพ์ต้นแบบและป้ายระบุต่อไป

4.1.2) ปรับปรุงแม่พิมพ์ต้นแบบและป้ายระบุ

หลังจากได้ข้อมูลของแบบรูปความมั่นคงที่ต้องการแสดงแล้ว ต่อไปเป็นขั้นตอนของการปรับปรุงแม่พิมพ์ต้นแบบและป้ายระบุเพื่อใช้ในการแสดงข้อมูลดังกล่าว โดยการปรับปรุงแม่พิมพ์ต้นแบบเป็นการปรับปรุงองค์ประกอบที่ใช้ในการระบุประเภทขององค์ประกอบแบบจำลอง และการปรับปรุงป้ายระบุเป็นการปรับปรุงองค์ประกอบที่ใช้ในการระบุลักษณะขององค์ประกอบแบบจำลองดังกล่าว โดยขั้นตอนในการปรับปรุงแม่พิมพ์ต้นแบบและป้ายระบุ มีรายละเอียดดังต่อไปนี้

(1) สร้างแม่พิมพ์ต้นแบบเพื่อใช้ในการระบุข้อมูลที่ระบุประเภทขององค์ประกอบแบบจำลอง จากการพิจารณาข้อมูลของแบบรูปการให้อำนาจที่ต้องการแสดง จะได้แม่พิมพ์ต้นแบบดังนี้

(1.1) ข้อมูลทางโครงสร้างของแบบรูปการให้อำนาจที่เป็นข้อมูลที่ระบุประเภทขององค์ประกอบแบบจำลอง คือ องค์ประกอบแบบจำลองในแบบรูปความมั่นคง ที่สามารถจำแนกเป็น คลาสในแบบรูป แบบชนิดข้อมูลในแบบรูป และความสัมพันธ์ระหว่างคลาสในแบบรูป จากข้อมูลของแบบรูปดังกล่าว จะได้แม่พิมพ์ต้นแบบดังนี้

– แม่พิมพ์ต้นแบบ “spc” (<u>S</u>ecurity <u>P</u>attern <u>C</u>lass: spc) เป็นแม่พิมพ์ต้นแบบที่ใช้ในการระบุคลาสที่เป็นองค์ประกอบในแบบรูปความมั่นคง

– แม่พิมพ์ต้นแบบ “spt” (<u>S</u>ecurity <u>P</u>attern data <u>T</u>ype: spt) เป็นแม่พิมพ์ต้นแบบที่ใช้ในการระบุแบบชนิดข้อมูลในแบบรูปความมั่นคง

– แม่พิมพ์ต้นแบบ “spr” (<u>S</u>ecurity <u>P</u>attern <u>R</u>elationship: spr) เป็นแม่พิมพ์ต้นแบบที่ใช้ในการระบุความสัมพันธ์ที่เป็นองค์ประกอบในแบบรูปความมั่นคง

(1.2) แม่พิมพ์ต้นแบบที่ได้จากข้อมูลทางความมั่นคงของแบบรูปการให้อำนาจ มีดังนี้

– แม่พิมพ์ต้นแบบ “subject” เป็นแม่พิมพ์ต้นแบบที่ใช้ระบุคลาสที่เป็นผู้เข้าใช้ทรัพยากร

– แม่พิมพ์ต้นแบบ “accessRight” เป็นแม่พิมพ์ต้นแบบที่ใช้ในการระบุคลาสที่เป็นองค์ประกอบที่ควบคุมการเข้าถึงทรัพยากร

– แม่พิมพ์ต้นแบบ “accessType” เป็นแม่พิมพ์ต้นแบบที่ใช้ในการระบุคลาสที่เป็นแบบชนิดข้อมูลที่อธิบายลักษณะในการเข้าถึงทรัพยากร

— แม่พิมพ์ต้นแบบ “restrictedRule” เป็นแม่พิมพ์ต้นแบบที่ใช้ในการระบุคลาสที่เป็นแบบชนิดข้อมูลที่อธิบายเงื่อนไขที่เป็นข้อห้ามของการให้อำนาจ

— แม่พิมพ์ต้นแบบ “copyFlag” เป็นแม่พิมพ์ต้นแบบที่ใช้ในการระบุคลาสที่เป็นแบบชนิดข้อมูลที่อธิบายการอนุญาตให้ผู้อื่นคัดลอกอำนาจของผู้ใช้งานดังกล่าว

(2) สร้างป้ายระบุของแม่พิมพ์ต้นแบบที่ได้จากขั้นตอนข้างต้นเพื่อใช้ในการระบุข้อมูลที่อธิบายลักษณะขององค์ประกอบจากขั้นตอนข้างต้น จากการพิจารณาข้อมูลของแบบรูปการให้อำนาจที่ต้องการแสดง จะได้ป้ายระบุของแม่พิมพ์ต้นแบบดังนี้

(2.1) สร้างป้ายระบุจากบทนิยามป้ายระบุแบบรูป [12] ที่เป็นป้ายระบุสำหรับแสดงข้อมูลทางโครงสร้างของแบบรูปโดยเฉพาะ เพื่ออธิบายลักษณะขององค์ประกอบในแบบรูปความมั่นคง กล่าวคือ สร้างป้ายระบุ “role@name[instance]” ที่มีค่าเป็นบูลีนในแม่พิมพ์ต้นแบบ “spc” “spt” และ “spr” และแม่พิมพ์ต้นแบบที่ได้จากข้อมูลทางความมั่นคงทั้งหมด โดยชื่อป้ายระบุมีรูปแบบดังนี้

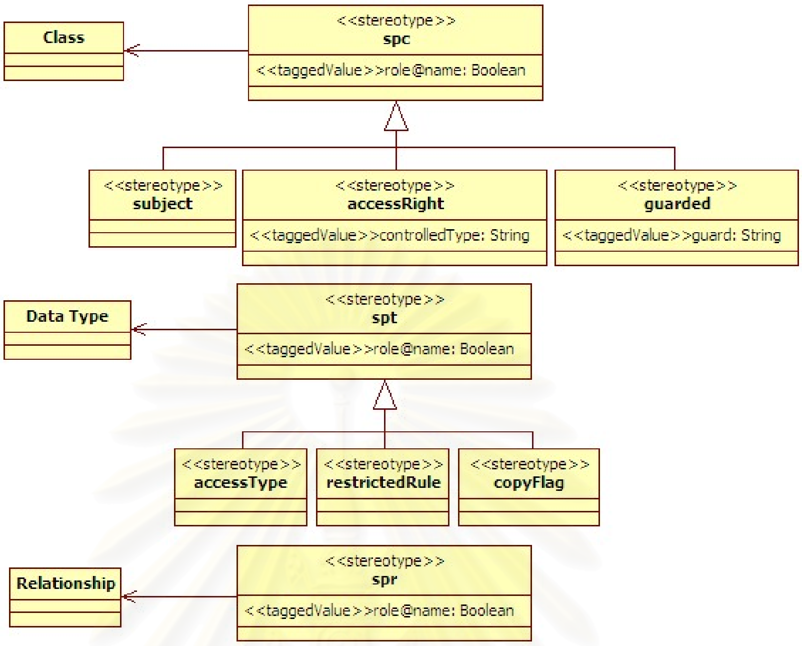
“role@name[instance]”

โดย “role” เป็นบทบาทขององค์ประกอบดังกล่าวในแบบรูปความมั่นคง “name” เป็นชื่อแบบรูปความมั่นคง และ “instance” เป็นลำดับของแบบรูปความมั่นคงในแผนภาพ ตัวอย่างของชื่อป้ายระบุขององค์ประกอบในแบบรูปความมั่นคง เช่น “subject@authorization[2]” เป็นชื่อป้ายระบุที่แสดงถึงบทบาท “subject” ในแบบรูป “authorization” ลำดับที่ “2” ในแผนภาพ เป็นต้น โดยค่าของป้ายระบุดังกล่าวเป็นบูลีน (Boolean) จะมีค่าเป็นจริง เมื่อองค์ประกอบดังกล่าวมีลักษณะตามชื่อป้ายระบุ กล่าวคือ องค์ประกอบดังกล่าวมีบทบาท “role” ในแบบรูป “name” ลำดับที่ “instance” ในแผนภาพ และจะมีค่าเป็นเท็จ เมื่อองค์ประกอบดังกล่าวไม่ได้มีลักษณะตามชื่อป้ายระบุ กล่าวคือ องค์ประกอบดังกล่าวไม่ได้มีบทบาท “role” ในแบบรูป “name” ลำดับที่ “instance” ในแผนภาพ

(2.2) ป้ายระบุที่ได้จากข้อมูลทางความมั่นคงของแบบรูปความมั่นคง มีดังต่อไปนี้

— ป้ายระบุ “controlledType” เป็นป้ายระบุในแม่พิมพ์ต้นแบบ “accessRight” ที่ใช้ในการระบุประเภทขององค์ประกอบที่ควบคุมการเข้าถึงทรัพยากร

โดยความสัมพันธ์ระหว่างแม่พิมพ์ต้นแบบและป้ายระบุสามารถแสดงเป็นเมตาโมเดลเสมือน ดังรูปที่ 3.7 ที่ได้อธิบายว่า ป้ายระบุ “role@name[instance]” เป็นคุณลักษณะในแต่ละแม่พิมพ์ต้นแบบ “spc” “spt” และ “spr” ซึ่งแม่พิมพ์ต้นแบบที่ได้จากข้อมูลทางความมั่นคงทั้งหมด ประกอบด้วย แม่พิมพ์ต้นแบบ “subject” “accessRight” “accessType” “restrictedRule” “copyFlag” รวมทั้งแม่พิมพ์ต้นแบบ “guarded” ของยูเอ็มแอลเซค จะมีป้ายระบุดังกล่าวเช่นกัน เนื่องจากแม่พิมพ์ต้นแบบดังกล่าวสืบทอดมาจากแม่พิมพ์ต้นแบบ “spc” “spt” และ “spr” นอกจากนี้แม่พิมพ์ต้นแบบ “accessRight” จะมีป้ายระบุ “controlledType” สำหรับระบุประเภทขององค์ประกอบที่ควบคุมการเข้าถึงทรัพยากร



รูปที่ 3.7 เมตาโมเดลเสมือนแสดงความสัมพันธ์ระหว่างแม่พิมพ์ต้นแบบและป้ายระบุที่สร้างขึ้น

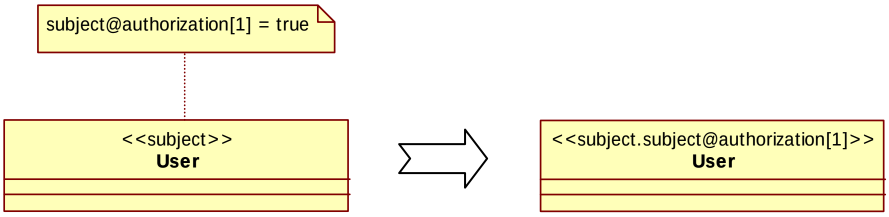
นอกจากการระบุคลาส แบบชนิดข้อมูล และความสัมพันธ์ระหว่างคลาสภายในแบบรูปความมั่นคงแล้ว การระบุการดำเนินการที่ใช้ภายในแบบรูปความมั่นคงก็มีความสำคัญเช่นกัน เนื่องจากเป็นการดำเนินการที่จำเป็นต้องใช้ในกระบวนการภายในแบบรูปความมั่นคง ดังนั้นการดำเนินการที่ใช้ภายในแบบรูปความมั่นจะมีการกำหนดข้อมูลทางโครงสร้างของแบบรูปความมั่นคงโดยใช้นิพจน์ “@ ชื่อแบบรูป [ลำดับของแบบรูป]” ต่อท้ายชื่อของการดำเนินการดังกล่าวเพื่อแสดงข้อมูลทางโครงสร้างของแบบรูปความมั่นคง ตัวอย่างของการดำเนินการที่ใช้ภายในแบบรูปการให้อำนาจ เช่น การดำเนินการ “checkRights” ในคลาส “AccessRight” ของแบบรูปการให้อำนาจจะมีการเพิ่มนิพจน์ต่อท้ายชื่อของการดำเนินการดังกล่าวเป็น “checkRights@authorization” เพื่อระบุว่าเป็นการดำเนินการที่ใช้ภายในแบบรูปการให้อำนาจ เป็นต้น

4.1.3) กำหนดรูปแบบของแม่พิมพ์ต้นแบบและค่าป้ายระบุ

การกำหนดรูปแบบของแม่พิมพ์ต้นแบบและค่าป้ายระบุ มีวัตถุประสงค์เพื่อความสะดวกในการแปลความหมายและลดความซับซ้อนของแผนภาพที่เกิดจากการระบุข้อมูลของแบบรูปความมั่นคง โดยมีรายละเอียดดังต่อไปนี้

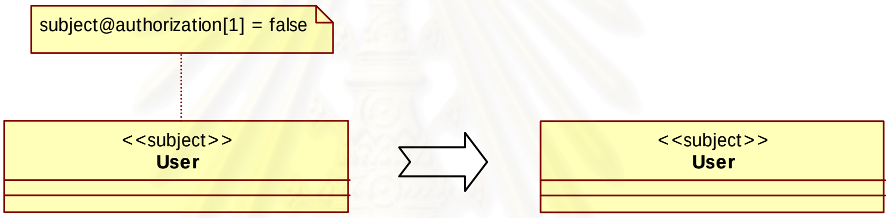
1) ถ้าค่าของป้ายระบุจากบทนิยามป้ายระบุแบบรูปเป็นจริง ผู้ออกแบบไม่จำเป็นต้องระบุชื่อและค่าป้ายระบุที่อยู่ในรูปแบบ “role@name[instance]=true” สามารถลดรูปให้เหลือเพียงการระบุชื่อป้ายระบุเท่านั้น โดยการระบุชื่อป้ายระบุนั้นสามารถระบุไว้ใน

เครื่องหมายของ “<<” และ “>>” ของแม่พิมพ์ต้นแบบที่มีเครื่องหมาย “.” คั่นไว้ได้ โดยตัวอย่างของการลดรูปของค่าป้ายระบุที่เป็นจริง แสดงดังรูปที่ 3.8



รูปที่ 3.8 การลดรูปของค่าป้ายระบุที่มีค่าเป็นจริงของยูเอ็มแอลเซคที่ปรับปรุงเพิ่มเติม

2) ถ้าค่าของป้ายระบุจากบทนิยามป้ายระบุแบบรูปเป็นเท็จ ผู้ออกแบบไม่จำเป็นต้องระบุชื่อและค่าของป้ายระบุดังกล่าวได้ ตัวอย่างของการลดรูปของค่าป้ายระบุที่เป็นเท็จ แสดงดังรูปที่ 3.9



รูปที่ 3.9 การลดรูปของค่าป้ายระบุที่มีค่าเป็นเท็จของยูเอ็มแอลเซคที่ปรับปรุงเพิ่มเติม

ด้วยวิธีการลดรูปของค่าป้ายระบุดังกล่าว จะช่วยเพิ่มความสะดวกในการระบุข้อมูลของแบบรูปเนื่องจากผู้ใช้งานไม่จำเป็นต้องระบุค่าของป้ายระบุที่เป็นบูลีน รวมทั้งช่วยลดความซับซ้อนของแผนภาพในแง่ของการลดจำนวนองค์ประกอบที่ใช้ในแผนภาพ

จากขั้นตอนของการปรับปรุงแม่พิมพ์ต้นแบบและค่าป้ายระบุข้างต้น จะได้แม่พิมพ์ต้นแบบและค่าป้ายระบุที่ใช้ในการแสดงข้อมูลทางโครงสร้างและข้อมูลทางความมั่นคงของแบบรูปความมั่นคง อย่างไรก็ตามการนำแม่พิมพ์ต้นแบบดังกล่าวมาประยุกต์ใช้จริงนั้นจำเป็นต้องมีการกำหนดข้อบังคับที่ต้องพิจารณาก่อนการใช้งาน ซึ่งข้อบังคับดังกล่าวจะถูกสร้างในขั้นตอนของการปรับปรุงเงื่อนไขบังคับต่อไป

4.2) ปรับปรุงเงื่อนไขบังคับของยูเอ็มแอลเซค

ในขั้นตอนนี้เป็นการปรับปรุงเงื่อนไขบังคับของแม่พิมพ์ต้นแบบที่ได้จากการขั้นตอนข้างต้น เงื่อนไขบังคับจะถูกนำไปพิจารณาเมื่อเกิดการประยุกต์ใช้แม่พิมพ์ต้นแบบเพื่อลดความผิดพลาดในการประยุกต์ใช้แม่พิมพ์ต้นแบบดังกล่าว โดยรายละเอียดของการปรับปรุงเงื่อนไขบังคับ มีดังต่อไปนี้

(1) ระบุข้อบังคับในการใช้งานของแต่ละแม่พิมพ์ต้นแบบที่ได้จากขั้นตอนข้างต้น ผู้วิจัยได้เลือกแม่พิมพ์ต้นแบบ “spc” เป็นตัวอย่างในการปรับปรุงเงื่อนไขบังคับ เนื่องจาก

แม่พิมพ์ต้นแบบดังกล่าวแสดงองค์ประกอบหลักทางโครงสร้างของแบบรูปความมั่นคง โดยข้อบังคับในการใช้งานของแม่พิมพ์ต้นแบบ “spc” คือ

— ค่าของป้ายระบุของแม่พิมพ์ต้นแบบไม่สามารถเป็นค่าว่างได้

— ค่าป้ายระบุที่แสดงลำดับของแบบรูปความมั่นคงในแม่พิมพ์ต้นแบบสามารถเป็นค่าว่างได้ ถ้าแบบรูปดังกล่าวไม่ซ้ำกันในแผนภาพคลาส

— ค่าป้ายระบุที่แสดงลำดับของแบบรูปความมั่นคงในแม่พิมพ์ต้นแบบไม่สามารถเป็นค่าว่างได้ ถ้าแบบรูปความมั่นคงดังกล่าวซ้ำกันในแผนภาพคลาส

(2) ระบุนิพจน์ตามข้อบังคับในการใช้งานของแม่พิมพ์ต้นแบบให้เป็นนิพจน์ในภาษาโอซีแอล จากแม่พิมพ์ต้นแบบ “spc” จะได้นิพจน์ที่ระบุข้อบังคับในการใช้งานคือ

— นิพจน์ “ค่าของป้ายระบุของแม่พิมพ์ต้นแบบไม่สามารถเป็นค่าว่างได้” ถูกเปลี่ยนเป็นนิพจน์ในภาษาโอซีแอล คือ

self.taggedValue.dataValue.name -> notEmpty

— นิพจน์ “ค่าป้ายระบุที่แสดงลำดับของแบบรูปความมั่นคงในแม่พิมพ์ต้นแบบสามารถเป็นค่าว่างได้ ถ้าแบบรูปดังกล่าวไม่ซ้ำกันในแผนภาพคลาส” ถูกเปลี่ยนเป็นนิพจน์ในภาษาโอซีแอล คือ

self.taggedValue.name->forall(v1, v2:name | v1.name <> v2.name)
implies (v1.instance->isEmpty and v2.instance->isEmpty)

— นิพจน์ “ค่าป้ายระบุที่แสดงลำดับของแบบรูปความมั่นคงในแม่พิมพ์ต้นแบบไม่สามารถเป็นค่าว่างได้ ถ้าแบบรูปความมั่นคงดังกล่าวซ้ำกันในแผนภาพคลาส” ถูกเปลี่ยนเป็นนิพจน์ในภาษาโอซีแอล คือ

self.taggedValue.name->exist(v1, v2:name | v1.name = v2.name) implies (v1.instance->notEmpty and v2.instance->notEmpty and v1.instance <> v2.instance)

จากขั้นตอนของการปรับปรุงยูเอ็มแอลเซคเพื่อแสดงแบบรูปการให้อำนาจ จะได้รายการของแม่พิมพ์ต้นแบบ และรายการของป้ายระบุที่ใช้ในแบบรูปการให้อำนาจ โดยแบ่งเป็นรายการของแม่พิมพ์ต้นแบบและป้ายระบุสำหรับแสดงข้อมูลทางโครงสร้างของแบบรูปการให้อำนาจในตารางที่ 3.1 และ 3.2 ตามลำดับ และรายการของแม่พิมพ์ต้นแบบและป้ายระบุสำหรับแสดงข้อมูลทางความมั่นคงของแบบรูปการให้อำนาจในตารางที่ 3.3 และ 3.4 ตามลำดับ โดยรายการของแม่พิมพ์ต้นแบบ ประกอบไปด้วย ชื่อแบบรูปความมั่นคง คำอธิบายของแบบรูปความมั่นคง แม่พิมพ์ต้นแบบ คลาสพื้นฐาน (Base class) ที่ใช้แม่พิมพ์ต้นแบบ ป้ายระบุที่ใช้ในแม่พิมพ์ต้นแบบ เงื่อนไขบังคับของแม่พิมพ์ต้นแบบ และคำอธิบายของแม่พิมพ์ต้นแบบ ส่วนรายการของป้ายระบุ ประกอบไปด้วย ชื่อแบบรูปความมั่นคง ป้ายระบุ แม่พิมพ์ต้นแบบที่ใช้ ค่าของป้ายระบุ

ตัวอย่างค่าของป้ายระบุ มัลติพลิซิที (Multiplicity) คำอธิบายของป้ายระบุ โดยแผนภาพคลาสของแบบรูปการให้อำนาจที่ใช้ยูเอ็มแอลเซคที่ปรับปรุงเพิ่มเติม แสดงดังรูปที่ 3.10

ตารางที่ 3.1 รายการของแม่พิมพ์ต้นแบบและเงื่อนไขบังคับสำหรับแสดงข้อมูลทางโครงสร้างของแบบรูปการให้อำนาจ

แม่พิมพ์ต้นแบบ	คลาสพื้นฐาน	ป้ายระบุ	เงื่อนไขบังคับ	คำอธิบาย
spc (Security Pattern Class)	Class	"role@name[instance]"	1> self.taggedValue.dataValue.name -> notEmpty 2> self.taggedValue.name -> forall(v1, v2:name | v1.name <> v2.name) implies (v1.instance -> isEmpty and v2.instance -> isEmpty) 3> self.taggedValue.name -> exists(v1, v2:name | v1.name = v2.name) implies (v1.instance -> notEmpty and v2.instance -> notEmpty and v1.instance <> v2.instance)	คลาสที่เป็นองค์ประกอบภายในแบบรูปความมั่นคง
spt (Security Pattern data Type)	Class	"role@name[instance]"		คลาสที่เป็นแบบชนิดข้อมูลภายในแบบรูปความมั่นคง
spr (Security Pattern Relationship)	Relationship	"role@name[instance]"		ความสัมพันธ์ระหว่างคลาสที่เป็นองค์ประกอบภายในแบบรูปความมั่นคง

ตารางที่ 3.2 รายการของป้ายระบุสำหรับแสดงข้อมูลทางโครงสร้างของแบบรูปการให้อำนาจ

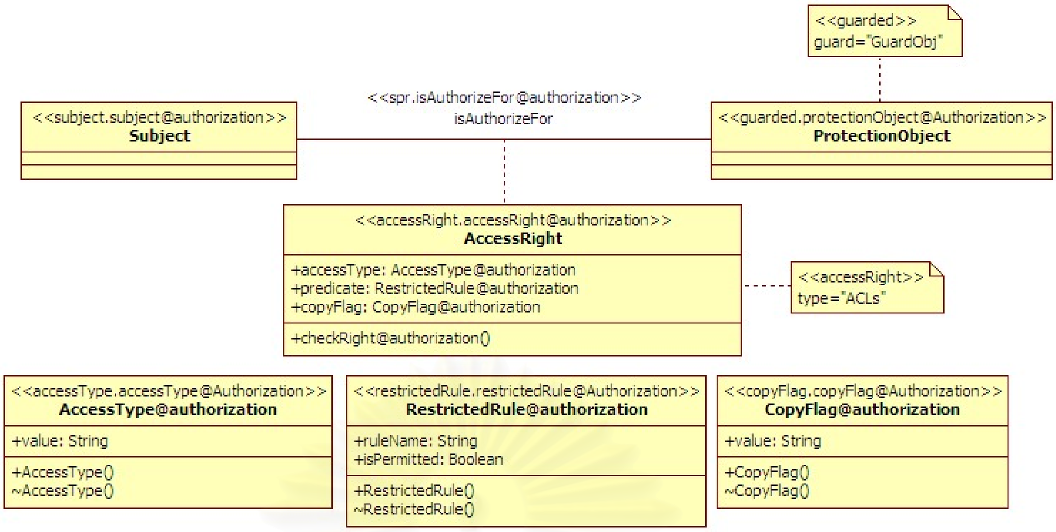
ป้ายระบุ	แม่พิมพ์ต้นแบบ	ค่าของป้ายระบุ	ตัวอย่างค่าของป้ายระบุ	มัลติพลิซิที	คำอธิบาย
"role@name[instance]"	แม่พิมพ์ต้นแบบที่สร้างทั้งหมด	บูลีนแสดงลักษณะองค์ประกอบดังกล่าวในแบบรูป	true หรือ false	*	ระบุว่า องค์ประกอบดังกล่าวมีบทบาท "role" ในแบบรูป "name" ลำดับที่ "instance" ในแผนภาพหรือไม่

ตารางที่ 3.3 รายการของแม่พิมพ์ต้นแบบและเงื่อนไขบังคับสำหรับแสดงข้อมูลทางความมั่นคงของแบบรูปการให้อำนาจ

แบบรูปความมั่นคง	คำอธิบายของแบบรูปความมั่นคง	แม่พิมพ์ต้นแบบ	คลาสพื้นฐาน	ป้ายระบุ	เงื่อนไขบังคับ	คำอธิบาย
การให้อำนาจ (Authorization)	เป็นแบบรูปที่เสนอการกำหนดสิทธิ์ของผู้เข้าใช้ทรัพยากรในระบบ	subject	Class	"role@name[instance]"		ผู้เข้าใช้ทรัพยากรของระบบ
		accessRight	Class	controlledType และ "role@name[instance]"	1> self.taggedValue -> forall(tv|tv.name = "controlledType" and (tv.dataValue = "ACLs" or tv.dataValue = "Capability"))	องค์ประกอบที่ควบคุมการเข้าถึงทรัพยากร
		accessType	Class	"role@name[instance]"		ลักษณะของการเข้าใช้ทรัพยากร
		restrictedRule	Class	"role@name[instance]"		เงื่อนไขที่เป็นข้อห้ามในการให้อำนาจแก่ผู้ใช้งาน
		copyFlag	Class	"role@name[instance]"		การอนุญาตผู้อื่นคัดลอกอำนาจของผู้ใช้งานดังกล่าว

ตารางที่ 3.4 รายการของป้ายระบุสำหรับแสดงข้อมูลทางความมั่นคงของแบบรูปการให้อำนาจ

แบบรูปความมั่นคง	ป้ายระบุ	แม่พิมพ์ต้นแบบ	ค่าของป้ายระบุ	ตัวอย่างค่าของป้ายระบุ	มัลติพลิซิที	คำอธิบาย
การให้อำนาจ (Authorization)	controlledType	accessRight	ประเภทขององค์ประกอบที่ควบคุมการเข้าถึงทรัพยากร	รายการควบคุมการเข้าถึง (Access Control Lists: ACLs) รายการแสดงสมรรถนะของผู้เข้าใช้ (Capabilities)	1	ประเภทขององค์ประกอบที่ควบคุมการเข้าถึงทรัพยากร



รูปที่ 3.10 แผนภาพคลาสของแบบรูปการให้อำนาจที่ใช้ยูเอ็มแอลเซคที่ปรับปรุงเพิ่มเติม

จากรูปที่ 3.10 ยูเอ็มแอลเซคที่ปรับปรุงเพิ่มเติมช่วยแสดงข้อมูลทางโครงสร้างและข้อมูลทางความมั่นคงของแบบรูปการให้อำนาจ โดยใช้แม่พิมพ์ต้นแบบและค่าป้ายระบุ “<<subject.subject@authorization>>” กำกับที่คลาส “Subject” เพื่อระบุว่าคลาสดังกล่าวเป็นผู้เข้าใช้ทรัพยากรและเป็นองค์ประกอบในแบบรูป แม่พิมพ์ต้นแบบและค่าป้ายระบุ “<<guarded.protectionObject@authorization>>” กำกับที่คลาส “ProtectionObject” เพื่อระบุว่าคลาสดังกล่าวเป็นทรัพยากรที่ถูกควบคุมโดยอ็อบเจ็กต์ในระบบที่ถูกระบุไว้ในป้ายระบุ “guard” และเป็นองค์ประกอบในแบบรูป แม่พิมพ์ต้นแบบและค่าป้ายระบุ “<<accessRight.accessRight@authorization>>” กำกับที่คลาส “AccessRight” เพื่อระบุว่าคลาสดังกล่าวเป็นองค์ประกอบที่ควบคุมการเข้าถึงทรัพยากรที่ระบุประเภทขององค์ประกอบไว้ในป้ายระบุ “controlledType” และเป็นองค์ประกอบในแบบรูป แม่พิมพ์ต้นแบบและค่าป้ายระบุ “<<accessType.accessType@authorization>>” กำกับคลาสที่เป็นแบบชนิดข้อมูล “AccessType” เพื่อระบุว่าแบบชนิดข้อมูลดังกล่าวอธิบายลักษณะการเข้าถึงทรัพยากรที่ใช้ในคุณลักษณะ “accessType” ของคลาส “AccessRight” แม่พิมพ์ต้นแบบและค่าป้ายระบุ “<<restrictedRule.restrictedRule@authorization>>” กำกับคลาสที่เป็นแบบชนิดข้อมูล “RestrictedRule” เพื่อระบุว่าแบบชนิดข้อมูลดังกล่าวอธิบายเงื่อนไขที่เป็นข้อห้ามของการให้อำนาจที่ใช้ในคุณลักษณะ “predicate” ของคลาส “AccessRight” แม่พิมพ์ต้นแบบและค่าป้ายระบุ “<<copyFlag.copyFlag@authorization>>” กำกับคลาสที่เป็นแบบชนิดข้อมูล “CopyFlag” ที่ใช้ในคุณลักษณะ “copyFlag” ของคลาส “AccessRight” เพื่อระบุว่าคุณลักษณะดังกล่าวเป็นคุณลักษณะที่อธิบายการอนุญาตให้ผู้อื่นคัดลอกอำนาจของผู้ใช้งานดังกล่าว และการดำเนินการ “checkRight@authorization” ของคลาส “AccessRight” เป็นการดำเนินการที่ใช้ในการตรวจสอบอำนาจของผู้ใช้ทรัพยากรในแบบรูปการให้อำนาจ

5) ตรวจสอบยูเอ็มแอลเซคที่ปรับปรุงเพิ่มเติม

ในขั้นตอนนี้เป็นการตรวจสอบยูเอ็มแอลเซคที่ปรับปรุงเพิ่มเติมโดยการพิจาณาจากคุณสมบัติมาตรฐานของยูเอ็มแอลโพรไฟล์ [15] โดยรายละเอียดของคุณสมบัติมาตรฐานของยูเอ็มแอลโพรไฟล์มีดังต่อไปนี้

(1) เป็นซับเซต (Subset) ของยูเอ็มแอลเมตาโมเดล (UML Metamodel) - ยูเอ็มแอลเซคที่ปรับปรุงเพิ่มเติมได้สร้างมาจากกลไกมาตรฐานในการขยายยูเอ็มแอลที่เป็นกลไกภายในยูเอ็มแอลเมตาโมเดล ดังนั้นยูเอ็มแอลเซคที่ปรับปรุงเพิ่มเติมจึงเป็นซับเซตของยูเอ็มแอลเมตาโมเดล

(2) มีกฎในการควบคุมรูปแบบการใช้งาน (Well-formness rules) ขององค์ประกอบที่ได้สร้างไว้ - ยูเอ็มแอลเซคที่ปรับปรุงเพิ่มเติมได้กำหนดเงื่อนไขบังคับในการควบคุมรูปแบบการใช้งานของแม่พิมพ์ต้นแบบที่อยู่ในรูปของภาษาโอซีแอลที่แสดงในรายการของแม่พิมพ์ต้นแบบในตารางที่ 3.1 และ 3.3

(3) ใช้ระบุองค์ประกอบที่นอกเหนือจากองค์ประกอบมาตรฐานของยูเอ็มแอล - แม่พิมพ์ต้นแบบ ค่าป้ายระบุ และเงื่อนไขบังคับที่ได้ผ่านการตรวจสอบการซ้อนทับกับองค์ประกอบมาตรฐานของยูเอ็มแอล

(4) มีการกำหนดความหมายของแต่ละองค์ประกอบที่ได้สร้างไว้ - ยูเอ็มแอลเซคที่ปรับปรุงเพิ่มเติมได้กำหนดคำอธิบายที่แสดงความหมายของแต่ละองค์ประกอบในรายการของแม่พิมพ์ต้นแบบในตารางที่ 3.1 และ 3.3 และรายการของป้ายระบุในตารางที่ 3.2 และ 3.4

(5) มีการกำหนดองค์ประกอบแบบจำลองที่ใช้ในองค์ประกอบที่ได้สร้างไว้ - ยูเอ็มแอลเซคที่ปรับปรุงเพิ่มเติมได้กำหนดคลาสพื้นฐานของแต่ละแม่พิมพ์ต้นแบบที่แสดงถึงประเภทองค์ประกอบแบบจำลองที่สามารถใช้ยูเอ็มแอลเซคที่ปรับปรุงเพิ่มเติมได้ในรายการของแม่พิมพ์ต้นแบบในตารางที่ 3.1 และ 3.3

จากการตรวจสอบยูเอ็มแอลเซคที่ปรับปรุงเพิ่มเติมจากคุณสมบัติมาตรฐานของยูเอ็มแอลโพรไฟล์ เห็นได้ว่า ยูเอ็มแอลเซคที่ปรับปรุงเพิ่มเติมมีข้อมูลและลักษณะขั้นพื้นฐานของยูเอ็มแอลโพรไฟล์ไม่แตกต่างจากยูเอ็มแอลโพรไฟล์ทั่วไป

จากการปรับปรุงยูเอ็มแอลเซคโดยพิจารณาจากแบบรูปความมั่นคงในขอบเขต จะได้ยูเอ็มแอลเซคที่ปรับปรุงเพิ่มเติมเพื่อแสดงแบบรูปความมั่นคง หรือเรียกว่า ยูเอ็มแอลเซคเอสพี (UMLsec for Security Patterns: UMLsec-SP) โดยรายละเอียดของยูเอ็มแอลเซคเอสพี แสดงในภาคผนวก ข และในภาคผนวก ค แสดงการประยุกต์ใช้ยูเอ็มแอลเซคเอสพีในแต่ละแบบรูปความมั่นคงที่เป็นการอธิบายแบบรูปความมั่นคงที่อยู่ในแผนภาพคลาสโดยใช้ยูเอ็มแอลเซคเอสพี นอกจากนี้ในภาคผนวก ง แสดงกรณีศึกษาที่ประยุกต์ใช้ยูเอ็มแอลเซคเอสพีในการแสดงข้อมูลทางโครงสร้างและข้อมูลทางความมั่นคงของแบบรูปความมั่นคงที่ประยุกต์ใช้ในกรณีศึกษาดังกล่าว

บทที่ 4

การพัฒนาและทดสอบเครื่องมือต้นแบบ
สำหรับแสดงแบบรูปความมั่นคงโดยใช้ยูเอ็มแอลเซคเอสพี

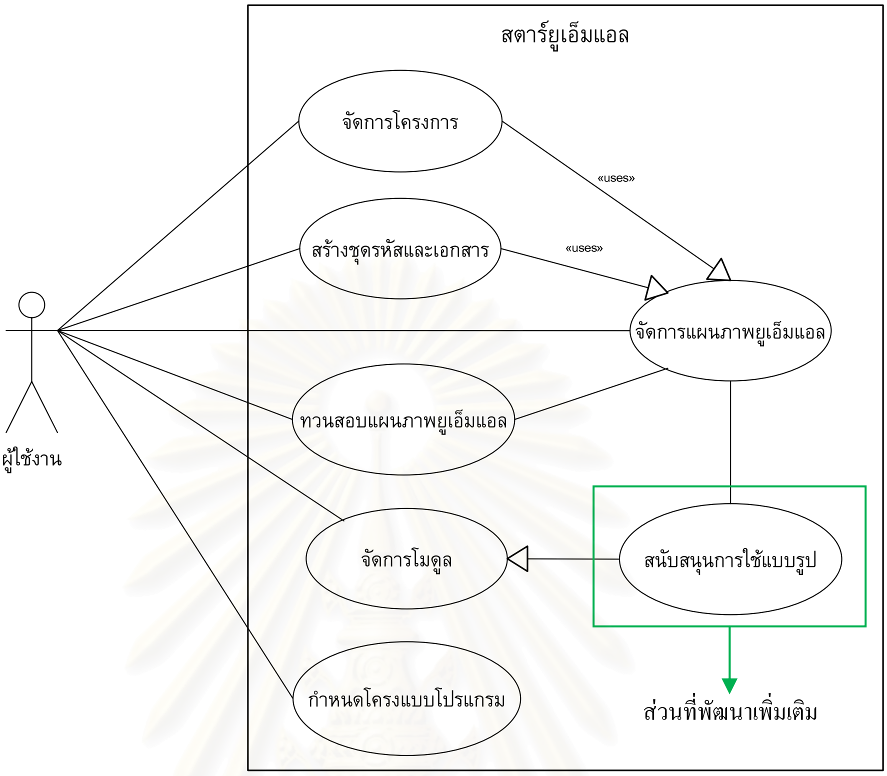
ภายหลังจากการขยายยูเอ็มแอลเซคเพื่อแสดงแบบรูปความมั่นคงแล้ว การนำยูเอ็มแอลเซคที่ปรับปรุงเพิ่มเติม หรือ ยูเอ็มแอลเซคเอสพี ไปประยุกต์ใช้โดยผู้ใช้งานทั่วไปนั้นทำได้ยาก ดังนั้นเพื่อช่วยให้ผู้ใช้งานเกิดความสะดวกในการใช้ยูเอ็มแอลเซคเอสพีในการแสดงแบบรูปความมั่นคงในแผนภาพคลาส ผู้วิจัยจึงได้พัฒนาเครื่องมือต้นแบบที่อยู่บนพื้นฐานของยูเอ็มแอลเซคเอสพี ในบทนี้จะกล่าวถึงการพัฒนาและทดสอบเครื่องมือต้นแบบสำหรับแสดงแบบรูปความมั่นคงโดยใช้ยูเอ็มแอลเซคเอสพี ประกอบไปด้วย การพัฒนาแบบรูปความมั่นคงเพิ่มลงในส่วนสนับสนุนการใช้แบบรูปของสตาร์ยูเอ็มแอล การทำงานของส่วนสนับสนุนการใช้แบบรูปความมั่นคงของสตาร์ยูเอ็มแอล การทดสอบเครื่องมือต้นแบบ และสภาพแวดล้อมในการพัฒนาเครื่องมือต้นแบบ โดยมีรายละเอียดดังนี้

4.1 การพัฒนาแบบรูปความมั่นคงเพิ่มลงในส่วนสนับสนุนการใช้แบบรูปของสตาร์ยูเอ็มแอล

ในปัจจุบันได้มีเครื่องมือที่ใช้ในการเขียนแผนภาพยูเอ็มแอลมากมาย เช่น เรชันแนลโรส (Rational Rose) วิชวลพาราดาม (Visual Paradigm) เป็นต้น อย่างไรก็ตามการนำเครื่องมือดังกล่าวมาพัฒนาเพิ่มเติมเพื่อตอบสนองการแสดงแบบรูปความมั่นคงนั้นจำเป็นต้องมีชุดรหัสของเครื่องมือเพื่อใช้ในการพัฒนาด้วย ดังนั้นผู้วิจัยจึงมีแนวคิดที่จะพัฒนาเครื่องมือต้นแบบโดยการพัฒนาส่วนเพิ่มเติมจากเครื่องมือที่ใช้ในการเขียนยูเอ็มแอลที่เป็นซอฟต์แวร์เปิดเผยรหัส (Open Source Software) ซึ่งเป็นซอฟต์แวร์ที่มีการเปิดเผยชุดรหัสเพื่อเปิดโอกาสให้ผู้พัฒนาทุกคนสามารถปรับเปลี่ยนตามความต้องการได้ เช่น สตาร์ยูเอ็มแอล (StarUML) อาร์โกยูเอ็มแอล (ArgoUML) เป็นต้น

ในงานวิทยานิพนธ์นี้ผู้วิจัยได้เลือก สตาร์ยูเอ็มแอล เป็นเครื่องมือต้นแบบในการพัฒนาส่วนเพิ่มเติมเพื่อสนับสนุนการแสดงแบบรูปความมั่นคงโดยใช้ยูเอ็มแอลเซคเอสพี เนื่องจากสตาร์ยูเอ็มแอลมีส่วนที่สนับสนุนการใช้แบบรูปในการออกแบบ เช่น แบบรูปการออกแบบ แบบรูปอีเจบี (Enterprise JavaBeans: EJB) เป็นต้น พร้อมทั้งมีโอเพนเอพีไอ (Open API) ที่เป็นฟังก์ชันในการพัฒนาส่วนต่อเติมของโปรแกรม ผู้วิจัยได้มีแนวคิดในการเพิ่มแผนภาพคลาสที่ใช้ยูเอ็มแอลเซคเอสพีของแบบรูปความมั่นคงลงในส่วนที่สนับสนุนการใช้แบบรูปในการออกแบบของสตาร์ยูเอ็มแอลโดยใช้โอเพนเอพีไอ รวมทั้งการเพิ่มส่วนที่อธิบายแบบรูปความมั่นคงโดยการสร้างเว็บเพจ (Web Page) ของแบบรูป โดยหน้าที่การทำงานหลักและส่วนที่สนับสนุนการใช้แบบรูปในการออกแบบของสตาร์ยูเอ็มแอลสามารถนำเสนอด้วยแผนภาพยูสเคส (Use Case

Diagram) ซึ่งเป็นแผนภาพที่อธิบายการติดต่อกันระหว่างผู้ใช้งาน (Actors) กับฟังก์ชันงานต่างๆ ที่ปรากฏในโปรแกรม ดังรูปที่ 4.1 โดยมีรายละเอียดดังนี้



รูปที่ 4.1 แผนภาพยูสเคสแสดงส่วนสนับการใช้แบบรูปในการออกแบบของสตาร์ยูเอ็มแอล

1) ส่วนจัดการโครงการ เป็นส่วนที่เกี่ยวกับกระบวนการในการจัดการโครงการที่สร้างจากโปรแกรม

2) ส่วนจัดการแผนภาพยูเอ็มแอล เป็นส่วนที่เกี่ยวกับการสร้างแผนภาพยูเอ็มแอลในโครงการที่กำหนด

3) ส่วนสร้างชุดรหัสและเอกสาร เป็นส่วนที่สร้างชุดรหัสที่มาจากแผนภาพยูเอ็มแอล โดยภาษาของชุดรหัสที่สามารถสร้างได้ ประกอบไปด้วย ภาษาซีชาร์ป (C#) ภาษาซีพลัสพลัส (C++) และภาษาจาวา (Java) และเป็นส่วนที่สร้างเอกสารของโครงการที่สามารถกำหนดแผ่นแบบ (Template) ของเอกสารได้

4) ส่วนทวนสอบแผนภาพยูเอ็มแอล เป็นส่วนที่ทวนสอบความถูกต้องของแผนภาพยูเอ็มแอลที่สร้าง โดยการพิจารณาจากกฎในการตรวจสอบแผนภาพยูเอ็มแอล

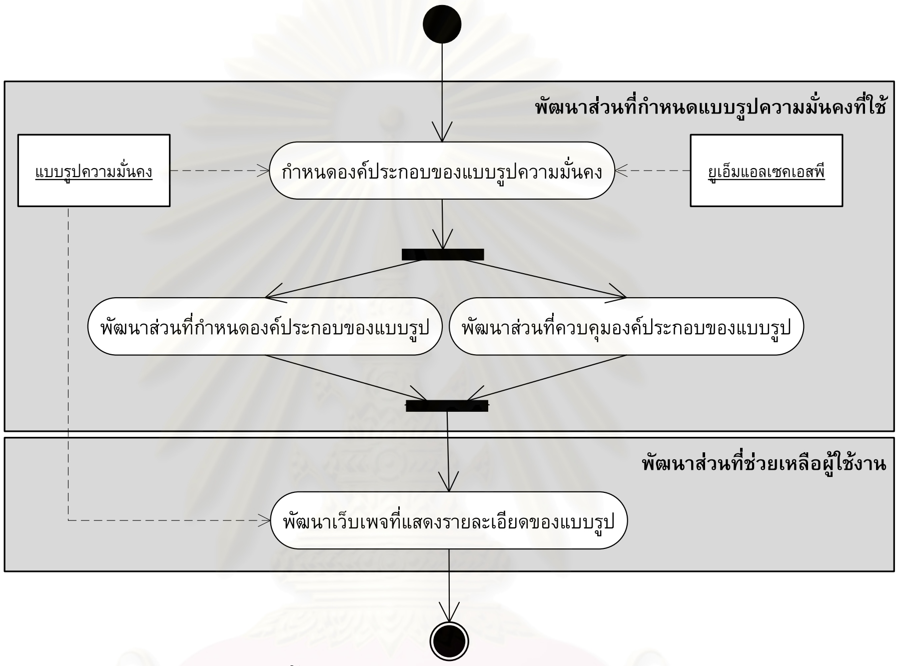
5) ส่วนจัดการโมดูล เป็นส่วนที่เกี่ยวกับการจัดการโมดูลต่างๆ ของสตาร์ยูเอ็มแอล ประกอบไปด้วย การติดตั้งโมดูล และการถอนการติดตั้งโมดูล

6) ส่วนกำหนดโครงแบบ (Configuration) โปรแกรม เป็นส่วนที่เกี่ยวกับการกำหนดค่าต่างๆ ของการทำงานในสตาร์ยูเอ็มแอล

7) ส่วนสนับสนุนการใช้แบบรูป เป็นส่วนที่เกี่ยวกับการใช้แบบรูปในการออกแบบคลาสของระบบ ซึ่งประกอบไปด้วย ส่วนที่กำหนดแบบรูปที่ใช้ เป็นส่วนที่ช่วยกำหนดโครงสร้างของ

แบบรูปในการออกแบบคลาส และส่วนที่ช่วยเหลือผู้ใช้งาน เป็นส่วนที่แสดงให้เห็นถึงรายละเอียดของแต่ละแบบรูปความมั่นคง โดยแบบรูปที่ใช้ในส่วนนี้สามารถพัฒนาเพิ่มเติมตามความต้องการของผู้ใช้งานได้

ผู้วิจัยได้มีแนวคิดในการพัฒนาเครื่องมือต้นแบบโดยการพัฒนาแบบรูปความมั่นที่ประกอบด้วย องค์ประกอบของแบบรูปความมั่นคงที่ใช้ยูเอ็มแอลเซคเอสพี เพิ่มลงในส่วนสนับสนุนการใช้แบบรูปของสตาร์ยูเอ็มแอล โดยขั้นตอนของการพัฒนาแบบรูปความมั่นคงเพิ่มลงในส่วนที่สนับสนุนการใช้แบบรูปของสตาร์ยูเอ็มแอล แสดงดังรูป 4.2 โดยมีรายละเอียดดังนี้



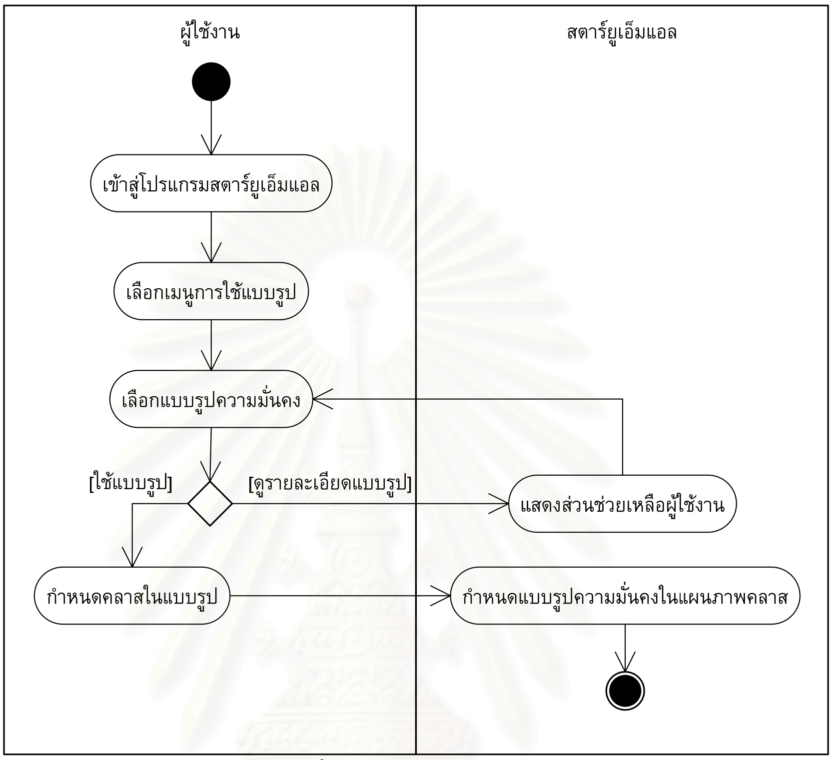
รูปที่ 4.2 แผนภาพกิจกรรมแสดงขั้นตอนการพัฒนาแบบรูปความมั่นคงเพิ่มลงในสตาร์ยูเอ็มแอล

1) การพัฒนาส่วนที่กำหนดแบบรูปความมั่นคงที่ใช้ ประกอบไปด้วย การพัฒนาส่วนที่กำหนดองค์ประกอบของแบบรูปความมั่นคง เป็นการพัฒนาโดยใช้ ภาษาเอกซ์เอ็มแอล (Extensible Markup Language: XML) ระบุองค์ประกอบของแบบรูปความมั่นคง และการพัฒนาส่วนที่ควบคุมองค์ประกอบของแบบรูปความมั่นคง เป็นการพัฒนาโดยใช้ ภาษาจาวาสคริปต์ (JavaScript) ร่วมกับโอเพนเอพีไอ ควบคุมองค์ประกอบของแบบรูปความมั่นคง รวมทั้งกำหนดแม่พิมพ์ต้นแบบ ค่าป้ายระบุ และเงื่อนไขบังคับของยูเอ็มแอลเซคเอสพีในแต่ละองค์ประกอบของแบบรูปความมั่นคง

2) การพัฒนาส่วนที่ช่วยเหลือผู้ใช้งาน เป็นการพัฒนาเว็บเพจที่แสดงรายละเอียดของแต่ละแบบรูปความมั่นคง โดยภาษาที่ใช้ในการพัฒนา คือ ภาษาเอชทีเอ็มแอล (Hyper Text Markup Language: HTML)

4.2 การทำงานของส่วนสนับสนุนการใช้แบบรูปความมั่นคงของสตาร์ยูเอ็มแอล

การทำงานของส่วนสนับสนุนการใช้แบบรูปความมั่นคงของสตาร์ยูเอ็มแอล ประกอบไปด้วย การทำงานในส่วนที่กำหนดแบบรูปความมั่นคงที่ใช้ และการทำงานในส่วนที่ช่วยเหลือผู้ใช้งาน ซึ่งแสดงเป็นแผนภาพกิจกรรม ดังรูปที่ 4.3

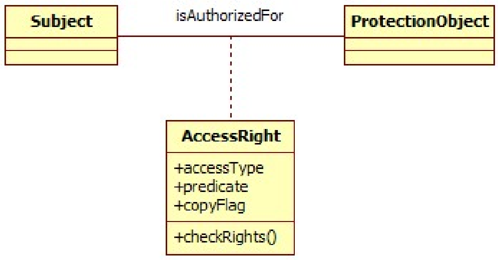


รูปที่ 4.3 แผนภาพกิจกรรมแสดงขั้นตอนการใช้แบบรูปความมั่นคงในสตาร์ยูเอ็มแอล

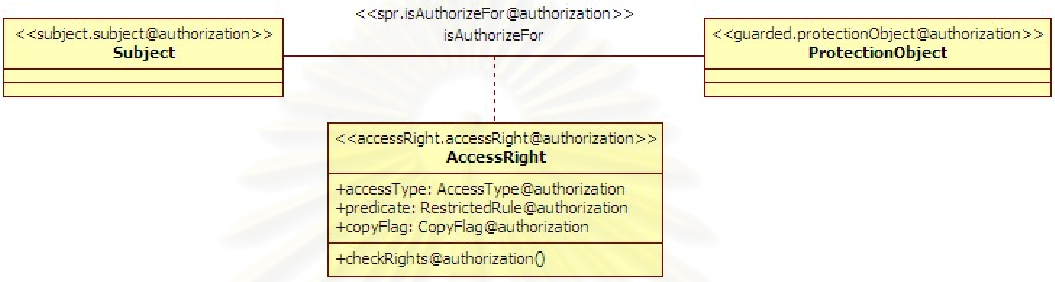
โดยรายละเอียดของการทำงานของส่วนสนับสนุนการใช้แบบรูปความมั่นคงของสตาร์ยูเอ็มแอลในแต่ละส่วนมีดังต่อไปนี้

1) ส่วนกำหนดแบบรูปความมั่นคงที่ใช้

เป็นส่วนหลักของส่วนสนับสนุนการใช้แบบรูปความมั่นคงซึ่งมีหน้าที่ในการช่วยกำหนดโครงสร้างของแบบรูปความมั่นคงในการออกแบบคลาส โดยผู้ใช้งานสามารถเลือกแบบรูปความมั่นคงที่ต้องการประยุกต์ใช้ และสามารถเลือกสร้างองค์ประกอบของแบบรูปขึ้นมาใหม่ หรือเลือกองค์ประกอบที่มีอยู่แล้วในแผนภาพให้เป็นองค์ประกอบในแบบรูปที่เลือก จากนั้นสตาร์ยูเอ็มแอลจะสร้างองค์ประกอบของแบบรูปความมั่นคงที่ใช้ยูเอ็มแอลเซคเอสพีเพื่อแสดงแบบรูปความมั่นคงในแผนภาพ ในที่นี้จะยกตัวอย่างแผนภาพคลาสของแบบรูปการให้อำนาจที่เป็นต้นแบบ และแผนภาพคลาสของแบบรูปการให้อำนาจที่สร้างมาจากส่วนสนับสนุนการใช้แบบรูปความมั่นคงของสตาร์ยูเอ็มแอล แสดงดังรูปที่ 4.4 และ 4.5 ตามลำดับ โดยในแต่ละองค์ประกอบของแบบรูปการให้อำนาจที่สร้างมาจากเครื่องมือจะแสดงให้เห็นถึงข้อมูลทางโครงสร้างและข้อมูลทางความมั่นคงของแบบรูปการให้อำนาจโดยใช้ยูเอ็มแอลเซคเอสพี



รูปที่ 4.4 แผนภาพคลาสของแบบรูปการให้อำนาจที่เป็นต้นแบบ



รูปที่ 4.5 แผนภาพคลาสของแบบรูปการให้อำนาจที่สร้างมาจากเครื่องมือ

2) ส่วนช่วยเหลือผู้ใช้งาน

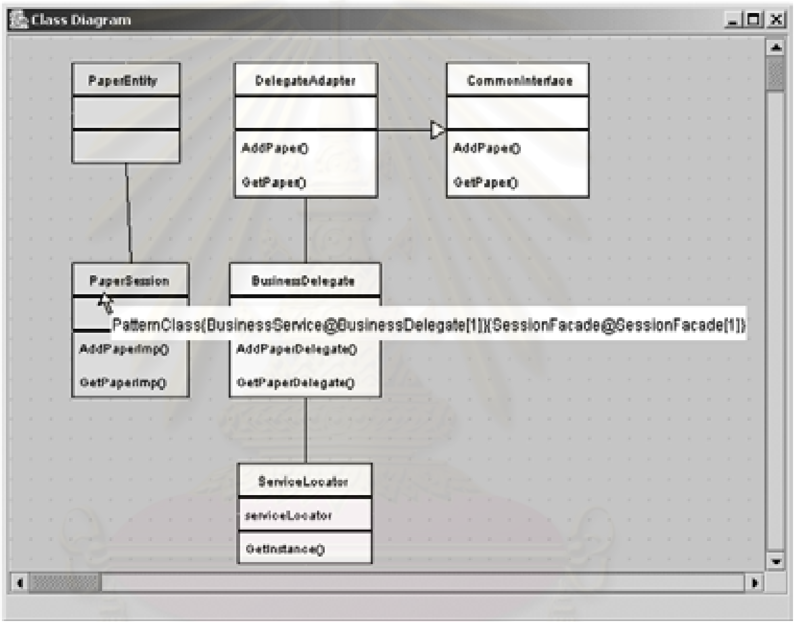
เป็นส่วนที่แสดงรายละเอียดของแต่ละแบบรูปความมั่นคง ประกอบไปด้วย จุดประสงค์ในการใช้แบบรูป (Purpose) โครงสร้างของแบบรูป (Structure) ตัวอย่างของการประยุกต์ใช้แบบรูป (Known Uses) และประโยชน์ที่จะได้รับ (Consequence) โดยรายละเอียดดังกล่าวจะเป็นประโยชน์ต่อผู้ใช้งาน เมื่อผู้ใช้งานเกิดข้อสงสัยที่เกี่ยวกับแบบรูปความมั่นคงที่เลือกใช้ โดยตัวอย่างของส่วนช่วยเหลือของแบบรูปการให้อำนาจ แสดงดังรูปที่ 4.6

รูปที่ 4.6 ส่วนช่วยเหลือของแบบรูปการให้อำนาจ

รายละเอียดตัวอย่างการใช้งานเครื่องมือต้นแบบและผลลัพธ์ที่ได้จากเครื่องมือ แสดงไว้ใน ภาคผนวก จ

4.3 การทดสอบเครื่องมือต้นแบบ

การทดสอบเครื่องมือต้นแบบมีวัตถุประสงค์เพื่อ ทดสอบความสามารถของเครื่องมือต้นแบบ ว่ามีฟังก์ชันการทำงานที่ช่วยเหลือผู้ใช้งานมากน้อยเพียงใด โดยการนำเครื่องมือต้นแบบเปรียบเทียบความสามารถกับเครื่องมือวิสดีพี (Visualize Design Pattern: VisDP) [17] ที่เป็นส่วนเสริมในการแสดงข้อมูลทางโครงสร้างของแบบรูปการออกแบบของเครื่องมือที่ใช้ในการเขียนแผนภาพยูเอ็มแอล เช่น แรชชันนัลโรส และอาร์โกยูเอ็มแอล เป็นต้น ตัวอย่างผลลัพธ์ของการแสดงข้อมูลทางโครงสร้างของแบบรูปการออกแบบจากเครื่องมือวิสดีพีที่แสดงข้อมูลของแบบรูปบิสเนสดีลีเกต (Business Delegate) และแบบรูปเซสชันฟาซาด (Session Facade) แสดงดังรูปที่ 4.7 โดยผลของการเปรียบเทียบความสามารถของเครื่องมือแสดงให้เห็นในตารางที่ 4.1



รูปที่ 4.7 ตัวอย่างการแสดงข้อมูลทางโครงสร้างของแบบรูปการออกแบบจากเครื่องมือวิสดีพี

ตารางที่ 4.1 การเปรียบเทียบความสามารถของเครื่องมือ

ฟังก์ชันการทำงาน	เครื่องมือ VisDP	เครื่องมือต้นแบบ สำหรับแสดงแบบรูปความมั่นคง
1. การกำหนดข้อมูลและองค์ประกอบของแบบรูป	ผู้ใช้งานเป็นผู้กำหนดทั้งหมด	เครื่องมือช่วยกำหนดบางส่วน
2. การตรวจสอบข้อมูลและองค์ประกอบของแบบรูป	ผู้ใช้งานเป็นผู้ตรวจสอบทั้งหมด	เครื่องมือช่วยตรวจสอบบางส่วน
3. การแสดงข้อมูลและองค์ประกอบของแบบรูป	ข้อความพลวัต	ข้อความ

จากผลของการเปรียบเทียบความสามารถของเครื่องมือ เห็นได้ว่า การกำหนดข้อมูลและองค์ประกอบของแบบรูปการออกแบบในเครื่องมือวิสดีพี เป็นหน้าที่ของผู้ใช้งานที่ต้องกำหนดเอง รวมทั้งตรวจสอบข้อมูลและองค์ประกอบดังกล่าวด้วยตัวเอง อาจทำให้เกิดความผิดพลาด

จากผู้ใช้งานได้ง่าย ในขณะที่การกำหนดข้อมูลและองค์ประกอบของแบบรูปความมั่นคงจากเครื่องมือต้นแบบที่นำเสนอนั้น เป็นการกำหนดของผู้ใช้งานบางส่วนและเป็นการกำหนดจากเครื่องมือต้นแบบที่ช่วยกำหนดข้อมูลและองค์ประกอบของแบบรูปความมั่นคงคือ องค์ประกอบแบบจำลองของแบบรูป รวมทั้งกำหนดแม่พิมพ์ต้นแบบ ค่าป้ายระบุ และเงื่อนไขบังคับในองค์ประกอบดังกล่าว ซึ่งจะช่วยลดความผิดพลาดในการกำหนดข้อมูลและองค์ประกอบของแบบรูปความมั่นคงจากผู้ใช้งาน นอกจากนี้เครื่องมือต้นแบบจะช่วยตรวจสอบข้อมูลของแบบรูปความมั่นคงในส่วนของการตรวจสอบคลาสของแบบรูปความมั่นคงที่เลือก ให้ถูกต้องและสอดคล้องกับคลาสในแผนภาพ อย่างไรก็ตามเครื่องมือต้นแบบที่นำเสนอยังมีจุดอ่อนในส่วนของการขาดองค์ประกอบที่เป็นบันทึกสำหรับแสดงค่าป้ายระบุ และการแสดงข้อมูลของแบบรูปเป็นข้อความที่ทำให้เกิดความซับซ้อนของแผนภาพเพิ่มมากขึ้น เนื่องจากจำนวนของตัวอักษรในแผนภาพเพิ่มมากขึ้น ซึ่งต่างจากการแสดงข้อมูลของแบบรูปเป็นข้อความพลวัตในเครื่องมือ วิสดีพีที่จะแสดงข้อมูลของแบบรูปเมื่อมีการเลือกชี้ที่องค์ประกอบแบบจำลองของแบบรูปเท่านั้น ด้วยวิธีการดังกล่าวจะช่วยลดจำนวนของตัวอักษรที่ปรากฏในแผนภาพได้ ดังนั้นแนวทางในการแสดงข้อมูลของแบบรูปในเครื่องมือดังกล่าว จะนำมาใช้เป็นแนวทางในการปรับปรุงเครื่องมือต้นแบบต่อไป

4.4 สภาพแวดล้อมในการพัฒนาเครื่องมือต้นแบบ

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

4.4.1 สภาพแวดล้อมในการพัฒนาเครื่องมือด้านฮาร์ดแวร์

เครื่องคอมพิวเตอร์ตั้งโต๊ะ 1 เครื่อง

1) หน่วยประมวลผล Intel Atom N270 ความเร็ว 1.60 กิกะเฮิร์ซ (GHz)
2) หน่วยความจำหลัก DDR2 ขนาด 1024 เมกกะไบต์ (MB)
3) ฮาร์ดดิสก์ความเร็ว 4,200 รอบ/วินาที ขนาด 160 กิกะไบต์ (GB)

4.4.2 สภาพแวดล้อมในการพัฒนาเครื่องมือด้านซอฟต์แวร์

1) ระบบปฏิบัติการวินโดส์เอ็กซ์พี เซอร์วิสแพ็ค 3 (Microsoft Windows XP Service Pack 3) เป็นระบบปฏิบัติการของเครื่องที่ใช้พัฒนา
2) สตาร์ยูเอ็มแอล เวอร์ชัน 5.0.2.1570 เป็นแกนหลักในการพัฒนาเครื่องมือต้นแบบ
3) อะโดบี ดรีมวีฟเวอร์ ซีเอสทรี (Adobe Dreamweaver CS3) สำหรับพัฒนาเครื่องมือต้นแบบส่วนที่เป็นเว็บเพจ และส่วนที่เป็นโปรแกรมทั้งหมด

บทที่ 5

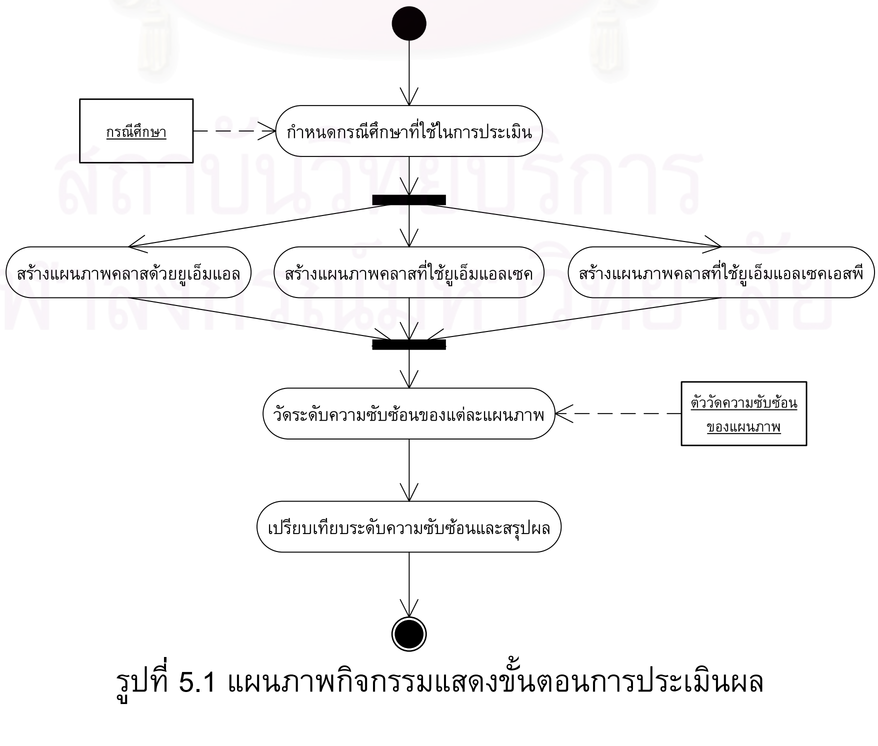
การประเมินผลและการวิเคราะห์การแสดงแบบรูปความมั่นคง โดยใช้ยูเอ็มแอลเซคเอสพี

ในบทนี้จะกล่าวถึง การประเมินผลของการแสดงแบบรูปความมั่นคงโดยการเปรียบเทียบระดับความซับซ้อนของแผนภาพคลาสที่ใช้ยูเอ็มแอลเซคเอสพีกับแผนภาพคลาสในลักษณะอื่น และการวิเคราะห์การแสดงแบบรูปความมั่นคงโดยใช้ยูเอ็มแอลเซคเอสพี เป็นการวิเคราะห์การแสดงข้อมูลทางโครงสร้างและข้อมูลทางความมั่นคงในแต่ละแบบรูปความมั่นคงของแผนภาพคลาสที่ใช้ยูเอ็มแอลเซคเอสพีกับแผนภาพคลาสในลักษณะอื่น โดยมีรายละเอียดดังนี้

5.1 การประเมินผลของการแสดงแบบรูปความมั่นคง

เนื่องจากการประยุกต์ใช้ยูเอ็มแอลเซคเอสพีในการแสดงแบบรูปความมั่นคง เป็นการเพิ่มรายละเอียดของข้อมูลในแผนภาพคลาส ดังนั้นแผนภาพคลาสที่ใช้ยูเอ็มแอลเซคเอสพีจะมีการแสดงข้อมูลในแผนภาพที่เพิ่มมากขึ้น จึงทำให้แผนภาพดังกล่าวมีความซับซ้อนของแผนภาพเพิ่มมากขึ้น จึงเป็นที่มาของวัตถุประสงค์ในการประเมินผลคือ เพื่อวิเคราะห์ระดับความซับซ้อนของแผนภาพคลาสที่ประยุกต์ใช้ยูเอ็มแอลเซคเอสพีในการแสดงแบบรูปความมั่นคง ว่ามีระดับความซับซ้อนของแผนภาพที่เพิ่มขึ้นจากแผนภาพคลาสในลักษณะอื่นมากน้อยเพียงใด เพื่อนำมาสรุปและพิจารณาในการปรับปรุงยูเอ็มแอลเซคเอสพีหรือเครื่องมือต้นแบบต่อไป

จากวัตถุประสงค์ที่กล่าวมาข้างต้นสามารถแสดงขั้นตอนการประเมินผลที่แสดงด้วยแผนภาพกิจกรรมดังรูปที่ 5.1 โดยมีรายละเอียดดังนี้



รูปที่ 5.1 แผนภาพกิจกรรมแสดงขั้นตอนการประเมินผล

5.1.1 การกำหนดกรณีศึกษาที่ประยุกต์ใช้แบบรูปความมั่นคง

กรณีศึกษาที่ใช้ในการประเมินผล เป็นกรณีศึกษาที่มีการประยุกต์ใช้แบบรูปความมั่นคงตามกลุ่มแบบรูปความมั่นคงในขอบเขตทั้งหมด ประกอบไปด้วย

(1) ระบบเอทีเอ็ม (Automatic Teller Machine: ATM) เป็นระบบฝากและถอนเงินของธนาคารผ่านตู้เอทีเอ็ม เป็นกรณีศึกษาที่ประยุกต์ใช้แบบรูปความมั่นคงในกลุ่มสถาปัตยกรรมการควบคุมการเข้าถึง

(2) กระบวนการความมั่นคงในระบบปฏิบัติการ (Secure Process) เป็นกระบวนการที่มีการควบคุมและตรวจสอบการเข้าถึงหน่วยความจำเสมือนให้เป็นไปตามสิทธิ์ของกระบวนการ เป็นกรณีศึกษาที่ประยุกต์ใช้แบบรูปความมั่นคงในกลุ่มแบบจำลองการควบคุมการเข้าถึง และกลุ่มการควบคุมการเข้าถึงระบบปฏิบัติการ

(3) ไฟร์วอลล์สำหรับการกรองเอกซ์เอ็มแอล (XML Firewall) เป็นไฟร์วอลล์ที่กรองข้อความเอกซ์เอ็มแอลที่เป็นอันตรายต่อระบบ เป็นกรณีศึกษาที่ประยุกต์ใช้แบบรูปความมั่นคงในกลุ่มสถาปัตยกรรมไฟร์วอลล์

(4) เครือข่ายส่วนตัวเสมือน (Virtual Private Network: VPN) เป็นการสร้างเครือข่ายเฉพาะขององค์กรโดยใช้กระบวนการในการเข้ารหัส เป็นกรณีศึกษาที่ประยุกต์ใช้แบบรูปความมั่นคงในกลุ่มการประยุกต์ใช้ความมั่นคงบนอินเตอร์เน็ต

โดยรายละเอียดของกรณีศึกษาที่ใช้ในการประเมิน แสดงในภาคผนวก ง

5.1.2 การสร้างแผนภาพคลาสด้วยยูเอ็มแอล แผนภาพคลาสที่ใช้ยูเอ็มแอลเซค และแผนภาพคลาสที่ใช้ยูเอ็มแอลเซคเอสพี ของกรณีศึกษา

ในขั้นตอนนี้เป็นการสร้างแผนภาพคลาสด้วยยูเอ็มแอล แผนภาพคลาสที่ใช้ยูเอ็มแอลเซค และแผนภาพคลาสที่ใช้ยูเอ็มแอลเซคเอสพี ของกรณีศึกษาที่ใช้ในการประเมินผล โดยรายละเอียดของแผนภาพคลาสในลักษณะต่างๆ ของกรณีศึกษาที่ใช้ในการประเมิน แสดงในภาคผนวก ง โดยกรณีศึกษาระบบเอทีเอ็ม ไฟร์วอลล์สำหรับการกรองเอกซ์เอ็มแอลและเครือข่ายส่วนตัวเสมือน จะไม่มีแผนภาพคลาสที่ใช้ยูเอ็มแอลเซค เนื่องจากยูเอ็มแอลเซคไม่ได้รองรับการแสดงองค์ประกอบทางสถาปัตยกรรมจำเพาะแบบรูปความมั่นคงที่ถูกประยุกต์ใช้ในกรณีศึกษาดังกล่าว

5.1.3 การวัดระดับความซับซ้อนของแผนภาพโดยใช้ตัววัด

การวัดระดับความซับซ้อนของแผนภาพคลาส เป็นการวัดระดับความซับซ้อนของแผนภาพโดยใช้ตัววัดความซับซ้อนของแผนภาพ (Graphic metric) [18, 19] ประกอบไปด้วย

1) จำนวนเส้นเชื่อมและจุดต่อ (Edge and Node) คือ จำนวนเส้นเชื่อมและจุดต่อที่เกิดขึ้นในแผนภาพ

2) จำนวนอักขระ (Character) คือ จำนวนของตัวอักษรที่เกิดขึ้นในแผนภาพ

3) จำนวนสัญลักษณ์ (Token) คือ จำนวนของสัญลักษณ์ที่เกิดขึ้นในแผนภาพ

4) ตัววัดแมกเคบ (McCabe metric) เป็นการวัดระดับความซับซ้อนของแผนภาพจากจำนวนของบล็อกที่เกิดขึ้นในแผนภาพ โดยมีสูตรดังนี้

*ค่าแมกเคบ หรือ ค่าไซโคลเมติก (Cyclomatic Number) = จำนวนของเส้นเชื่อม – จำนวนของจุดต่อ + (2 * จำนวนขององค์ประกอบที่เชื่อมติดกันโดยรอบ (Connected Component))*

5) จำนวนกราฟฟิคโทเคน (Graphic token) เป็นการวัดระดับความซับซ้อนของแผนภาพจากจำนวนสัญลักษณ์ทางกราฟิคที่เกิดขึ้นในแผนภาพ โดยมีสูตรดังนี้

จำนวนกราฟฟิคโทเคน คือ จำนวนของจุดต่อ + จำนวนของเส้นเชื่อม + จำนวนของสัญลักษณ์ที่เป็นตัวอักษร + จำนวนขององค์ประกอบที่ซ้อนอยู่ในองค์ประกอบอื่น (Containment) + จำนวนขององค์ประกอบที่อยู่ติดกัน (Adjoinment)

โดยผลลัพธ์ของการใช้ตัววัดในการวัดระดับความซับซ้อนของแผนภาพในลักษณะต่างๆ ของกรณีศึกษา ระบบเอทีเอ็ม กระบวนการความมั่นคงในระบบปฏิบัติการ ไฟร์วอลล์สำหรับการกรองเอกซ์เอ็มแอล และเครือข่ายส่วนตัวเสมือน แสดงดังตารางที่ 5.1 5.2 5.3 และ 5.4 ตามลำดับ

ตารางที่ 5.1 ผลลัพธ์ของการวัดระดับความซับซ้อนของกรณีศึกษา ระบบเอทีเอ็ม

ประเภทของแผนภาพคลาส	จำนวนเส้นเชื่อมและจุดต่อ	จำนวนอักขระ	จำนวนโทเคน	ตัววัดแมกเคบ	จำนวนกราฟฟิคโทเคน
แผนภาพคลาสจากยูเอ็มแอล	52	2243	371	10	2666
แผนภาพคลาสที่ใช้ยูเอ็มแอลเซคเอสพี	60	2536	447	10	3043

ตารางที่ 5.2 ผลลัพธ์ของการวัดระดับความซับซ้อนของกรณีศึกษา กระบวนการความมั่นคงในระบบปฏิบัติการ

ประเภทของแผนภาพคลาส	จำนวนเส้นเชื่อมและจุดต่อ	จำนวนอักขระ	จำนวนโทเคน	ตัววัดแมกเคบ	จำนวนกราฟฟิคโทเคน
แผนภาพคลาสจากยูเอ็มแอล	29	433	46	5	508
แผนภาพคลาสที่ใช้ยูเอ็มแอลเซค	31	472	54	5	557
แผนภาพคลาสที่ใช้ยูเอ็มแอลเซคเอสพี	39	1252	264	5	1555

ตารางที่ 5.3 ผลลัพธ์ของการวัดระดับความซับซ้อนของกรณีศึกษา ไฟร์วอลล์สำหรับการกรองเอกซ์เอ็มแอล

ประเภทของแผนภาพคลาส	จำนวนเส้นเชื่อมและจุดต่อ	จำนวนอักขระ	จำนวนโทเคน	ตัววัดแมกเคบ	จำนวนกราฟฟิคโทเคน
แผนภาพคลาสจากยูเอ็มแอล	44	455	53	6	552
แผนภาพคลาสที่ใช้ยูเอ็มแอลเซคเอสพี	48	744	137	6	929

ตารางที่ 5.4 ผลลัพธ์ของการวัดระดับความซับซ้อนของกรณีศึกษา เครือข่ายส่วนตัวเสมือน

ประเภทของแผนภาพคลาส	จำนวนเส้นเชื่อมและจุดต่อ	จำนวนอักขระ	จำนวนโทเคน	ตัววัดแมกเคบ	จำนวนกราฟฟิคโทเคน
แผนภาพคลาสจากยูเอ็มแอล	19	159	20	7	198
แผนภาพคลาสที่ใช้ยูเอ็มแอลเซคเอสพี	21	288	117	7	426

5.1.4 การเปรียบเทียบระดับความซับซ้อนของแผนภาพและการสรุปผล

จากผลลัพธ์ของการวัดระดับความซับซ้อนของกรณีศึกษาที่ใช้ในการประเมิน พบว่า แผนภาพคลาสที่ใช้ยูเอ็มแอลเซคเอสพีจะมีระดับของจำนวนอักขระ โทเคน และกราฟฟิคโทเคนที่มากกว่าแผนภาพอื่น แต่จำนวนของเส้นเชื่อมและจุดต่อ และตัววัดแมกเคบของแผนภาพดังกล่าวนั้นมีระดับเท่าๆ กันกับแผนภาพอื่น จากผลลัพธ์ดังกล่าวแสดงให้เห็นว่า แผนภาพคลาสที่ใช้ยูเอ็มแอลเซคเอสพีจะมีความซับซ้อนจากการแสดงอักขระหรือสัญลักษณ์ที่มากกว่าแผนภาพอื่น เนื่องจากการแสดงข้อมูลทางโครงสร้างและข้อมูลทางความมั่นคงของแบบรูปความมั่นคง อย่างไรก็ตามการแสดงเส้นเชื่อมและจุดต่อของแผนภาพดังกล่าวนั้นไม่ได้ต่างจากแผนภาพลักษณะอื่น ดังนั้นแผนภาพคลาสที่ใช้ยูเอ็มแอลเซคเอสพีมีความซับซ้อนของแผนภาพที่ไม่แตกต่างจากแผนภาพลักษณะอื่นในแง่ของการแสดงเส้นเชื่อมและจุดต่อของแผนภาพ แต่จะมีระดับความซับซ้อนในแง่ของการแสดงอักขระหรือสัญลักษณ์ที่มากกว่าแผนภาพในลักษณะอื่น เนื่องมาจากการแสดงข้อมูลทางโครงสร้างและข้อมูลทางความมั่นคงของแบบรูปความมั่นคงในแผนภาพ

5.2 การวิเคราะห์การแสดงแบบรูปความมั่นคงโดยใช้ยูเอ็มแอลเซคเอสพี

ในขั้นตอนนี้เป็นการวิเคราะห์การแสดงข้อมูลทางโครงสร้างและข้อมูลทางความมั่นคงในแต่ละแบบรูปความมั่นคงของแผนภาพคลาสทั้งสามลักษณะ คือ แผนภาพคลาสจากยูเอ็มแอล แผนภาพคลาสที่ใช้ยูเอ็มแอลเซค และแผนภาพคลาสที่ใช้ยูเอ็มแอลเซคเอสพีที่ได้จากงานวิทยานิพนธ์นี้ เพื่อเปรียบเทียบประสิทธิภาพของการแสดงข้อมูลของแบบรูปความมั่นคง โดยแบ่งเป็น การเปรียบเทียบการแสดงข้อมูลทางโครงสร้างของแบบรูปความมั่นคง และการเปรียบเทียบการแสดงข้อมูลทางความมั่นคงในแต่ละแบบรูปความมั่นคง โดยรายละเอียดของการเปรียบเทียบแสดงในภาคผนวก ฉ

จากผลลัพธ์ของการเปรียบเทียบการแสดงข้อมูลทางโครงสร้างและข้อมูลทางความมั่นคงของแบบรูปความมั่นคงจากแผนภาพคลาสทั้งสามลักษณะ พบว่า แผนภาพคลาสจากยูเอ็มแอลไม่สามารถแสดงข้อมูลทางความมั่นคงของแบบรูปได้ ในขณะที่แผนภาพคลาสที่ใช้ยูเอ็มแอลเซคสามารถแสดงข้อมูลทางความมั่นคงของแบบรูปได้เพียงบางส่วนเท่านั้น นอกจากนี้แผนภาพคลาสจากยูเอ็มแอลและแผนภาพคลาสที่ใช้ยูเอ็มแอลเซคไม่สามารถแสดงข้อมูลทางโครงสร้างของแบบรูปความมั่นคงได้ จากผลลัพธ์ดังกล่าวแสดงให้เห็นว่า แผนภาพคลาสจากยูเอ็มแอลและแผนภาพคลาสที่ใช้ยูเอ็มแอลเซคไม่สามารถแสดงข้อมูลของแบบรูปความมั่นคงได้ครบถ้วนตามความต้องการที่มาจากแบบรูปความมั่นคง เนื่องจากแผนภาพลักษณะดังกล่าวนั้น

ไม่ได้รองรับการแสดงข้อมูลทางโครงสร้างและข้อมูลทางความมั่นคงของแบบรูปความมั่นคงต่างจากแผนภาพคลาสที่ใช้ยูเอ็มแอลเซคเอสพีที่สามารถแสดงข้อมูลทางโครงสร้างและข้อมูลทางความมั่นคงของแบบรูปความมั่นคงได้ครบถ้วนตามความต้องการที่มาจากแบบรูปความมั่นคง และใน ภาคผนวก ช แสดงแผนภาพคลาสที่เกิดจากการบูรณาการของแบบรูปความมั่นคงที่อยู่ในขอบเขตทั้งหมด โดยแต่ละองค์ประกอบในแผนภาพจะใช้ยูเอ็มแอลเซคเอสพีในการแสดงข้อมูลทางโครงสร้างและข้อมูลทางความมั่นคงในแต่ละแบบรูปความมั่นคง

บทที่ 6

สรุปผลการวิจัย

ในบทนี้กล่าวถึงส่วนสุดท้ายที่ได้จากผลงานวิจัย คือ บทสรุปของผลงานวิจัย รวมทั้งงานวิจัยในอนาคต และบทความวิชาการที่ตีพิมพ์ โดยมีรายละเอียดดังต่อไปนี้

6.1 บทสรุปของผลงานวิจัย

งานวิจัยนี้ได้ทำการวิเคราะห์และปรับปรุงยูเอ็มแอลเซคเพื่อแสดงแบบรูปความมั่นคงที่นำเสนอโดย M. Schumacher และคณะ [2] ซึ่งครอบคลุม 5 กลุ่มแบบรูปความมั่นคง ได้แก่ แบบจำลองการควบคุมการเข้าถึง สถาปัตยกรรมการควบคุมการเข้าถึงระบบ การควบคุมการเข้าถึงระบบปฏิบัติการ สถาปัตยกรรมไฟร์วอล์ และการประยุกต์ใช้ความมั่นคงบนอินเตอร์เน็ต เป็นกลุ่มแบบรูปที่มีการนำไปประยุกต์ใช้อย่างแพร่หลาย โดยยูเอ็มแอลเซคที่ได้จากปรับปรุงเพิ่มเติมนั้น เรียกว่า ยูเอ็มแอลเซคเอสพี ที่ประกอบไปด้วย 58 แม่พิมพ์ต้นแบบและ 25 ป้ายระบุ นอกจากนี้ผู้วิจัยได้พัฒนาเครื่องมือต้นแบบที่อยู่บนพื้นฐานของยูเอ็มแอลเซคเอสพีที่ช่วยให้ผู้ใช้งานเกิดความสะดวกในการใช้ยูเอ็มแอลเซคเอสพีในการแสดงแบบรูปความมั่นคงในแผนภาพคลาสโดยใช้สตาร์ยูเอ็มแอล

การประเมินระดับความซับซ้อนของแผนภาพคลาสที่ใช้ยูเอ็มแอลเซคเอสพีเปรียบเทียบกับแผนภาพคลาสในลักษณะอื่นโดยใช้ตัววัดระดับความซับซ้อนของแผนภาพ คือ จำนวนเส้นเชื่อมและจุดต่อ จำนวนอักขระ จำนวนสัญลักษณ์ ตัววัดแมกเคบ และจำนวนกราฟฟิคโทเคน จากนั้นเป็นการวิเคราะห์การแสดงแบบรูปความมั่นคงของยูเอ็มแอลเซคเอสพีโดยการเปรียบเทียบกับแผนภาพคลาสในลักษณะอื่น เพื่อเปรียบเทียบการแสดงข้อมูลทางโครงสร้างและข้อมูลทางความมั่นคงตามความต้องการจากแบบรูปความมั่นคง

จากผลการประเมินยูเอ็มแอลเซคเอสพีและการวิเคราะห์การแสดงแบบรูปความมั่นคงโดยใช้ยูเอ็มแอลเซคเอสพี สามารถสรุปได้ดังนี้

1) แผนภาพคลาสที่ใช้ยูเอ็มแอลเซคเอสพีจะมีระดับความซับซ้อนของแผนภาพที่มากกว่าแผนภาพคลาสในลักษณะอื่นในแง่ของการแสดงข้อความที่เพิ่มมากขึ้น แต่ระดับความซับซ้อนจากเส้นเชื่อมและจุดต่อต่างๆ ไม่ได้แตกต่างจากแผนภาพในลักษณะอื่น

2) การแสดงข้อมูลของแบบรูปความมั่นคงโดยใช้ยูเอ็มแอลเซคเอสพีสามารถแสดงข้อมูลทางโครงสร้างและข้อมูลทางความมั่นคงของแบบรูปได้ครบถ้วนตามความต้องการจากแบบรูปความมั่นคงที่ได้เสนอไว้

ผลลัพธ์ที่ได้จากงานวิทยานิพนธ์นี้จะได้ ยูเอ็มแอลเซคเอสพีสำหรับแสดงข้อมูลทางโครงสร้างและข้อมูลทางความมั่นคงของแบบรูปความมั่นคงตามความต้องการจากแบบรูปความมั่นคงซึ่งครอบคลุม 5 กลุ่มแบบรูป การแสดงแบบรูปความมั่นคงโดยใช้ยูเอ็มแอลเซคเอสพีนั้น

จะตอบสนองการออกแบบและปรับปรุงการออกแบบความมั่นคงของระบบโดยใช้แบบรูปความมั่นคงให้มีประสิทธิภาพมากยิ่งขึ้น

6.2 งานวิจัยในอนาคต

งานวิจัยนี้ได้ปรับปรุงยูเอ็มแอลเซคเพื่อให้สนับสนุนการแสดงแบบรูปความมั่นคงทั้งหมด 27 แบบรูป ซึ่งจัดเป็น 5 กลุ่ม จากทั้งหมด 8 กลุ่มแบบรูปความมั่นคงที่นำเสนอไว้โดย M. Schumacher และคณะ [2] ซึ่งเป็นแบบรูปที่ได้จากการประชุมวิชาการโดยผู้เชี่ยวชาญด้านความมั่นคง และแบบรูปความมั่นคง ดังนั้นการขยายขอบเขตงานให้ครอบคลุมทั้ง 8 กลุ่มแบบรูปความมั่นคง ถือเป็นสิ่งที่มีความท้าทาย และช่วยให้ยูเอ็มแอลเซคที่ปรับปรุงเพิ่มเติม หรือยูเอ็มแอลเซคเอสพี มีความสมบูรณ์มากขึ้น นอกจากนี้การปรับปรุงยูเอ็มแอลเซคเอสพีหรือเครื่องมือต้นแบบที่ทำให้แผนภาพคลาสที่ใช้ยูเอ็มแอลเซคเอสพีมีระดับความซับซ้อนของแผนภาพน้อยลง ก็เป็นสิ่งที่มีความท้าทายเช่นกัน เนื่องจากยูเอ็มแอลเซคเอสพีและเครื่องมือต้นแบบที่นำเสนอทำให้เกิดความซับซ้อนของแผนภาพที่ค่อนข้างมาก โดยมีเหตุมาจากจำนวนของตัวอักษรในแผนภาพที่เพิ่มมากขึ้น

6.3 บทความวิชาการที่ตีพิมพ์

ในการวิจัยนี้ ผู้วิจัยได้ส่งผลงานวิชาการร่วมกับคณะผู้วิจัย เป็นบทความวิชาการจากการประชุมวิชาการในประเทศ รวมเป็น 3 บทความ (แสดงใน ภาคผนวก ซ) ได้แก่

1) บทความวิชาการเรื่อง “การออกแบบและการแสดงแบบรูปของแบบจำลองการควบคุมการเข้าถึงโดยการขยายยูเอ็มแอลเซค (Design and Visualization of Access Control Model Patterns by Extending UMLsec)” ซึ่งได้รับการคัดเลือกเพื่อนำเสนอและตีพิมพ์ในงาน “การประชุมวิชาการร่วมสาขาวิทยาการคอมพิวเตอร์และวิศวกรรมซอฟต์แวร์ ครั้งที่ 5 (The 5^{th} International Joint Conference on Computer Science and Software Engineering: JCSSE 2008)” ระหว่างวันที่ 7 – 9 พฤษภาคม 2551 ณ โรงแรมเฟลิกซ์ริเวอร์แควรีสอร์ท กาญจนบุรี

2) บทความวิชาการเรื่อง “เครื่องมือสำหรับการกำหนดข้อมูลและโครงสร้างแบบรูปของแบบจำลองการควบคุมการเข้าถึง (Access Control Model Pattern Information and Structure Definition Tool)” ซึ่งได้รับการคัดเลือกเพื่อนำเสนอและตีพิมพ์ในงาน “การประชุมวิชาการทางวิทยาการคอมพิวเตอร์และวิศวกรรมคอมพิวเตอร์ในระดับชาติ ครั้งที่ 12 (The 12^{th} National Computer Science and Engineering Conference: NCSEC 2008)” ระหว่างวันที่ 20 – 21 พฤศจิกายน 2551 ณ โรงแรมลองบีชการ์เดนรีสอร์ทแอนด์สปา ชลบุรี

3) บทความวิชาการเรื่อง “UMLsec-SP: An Extension of UMLsec for System Security Modeling based on Security Patterns” ซึ่งได้รับการคัดเลือกเพื่อนำเสนอและตีพิมพ์ในงาน “การประชุมวิชาการร่วมสาขาวิทยาการคอมพิวเตอร์และวิศวกรรมซอฟต์แวร์ ครั้งที่ 6

(The 6th International Joint Conference on Computer Science and Software Engineering: JCSSE 2009)” ระหว่างวันที่ 13 – 15 พฤษภาคม 2552 ณ โรงแรมลากูน่าบีชรีสอร์ท ภูเก็ต

รายการอ้างอิง

[1] Pressman, R. S. Software Engineering: A Practitioner's Approach. 5^{th} ed. McGraw-Hill, 2001.

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

[3] Coplien, J.O., and Schmidt, D.C. Pattern Languages of Program Design. Addison-Wesley, 1995.

[4] Jürjen, J. Security Systems Development with UML. Springer, 2005.

[5] Jürjen, J. UMLsec: Extending UML for Secure System Development. Springer, 2002.

[6] Rumbaugh, J., Jacobson, I., and Booch, G. The Unified Modeling Language Reference Manual. 2^{nd} ed. Addison-Wesley, 2005.

[7] Shumacher, M. Security Engineering with Patterns. Spinger-Verlag, 2002.

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

[9] Supaporn, K., Prompoon, N., and Rojkangsadan, T. An Approach: Constructing the Grammar from Security Patterns, Proceedings of the 4^{th} International Joint Conference on Computer Science and Software Engineering(JCSSE '07)., 2007

[10] Object Management Group. OMG Unified Modeling Language Infrastructure version 2.1.2 [Computer file]. Available from: http://www.omg.org [2009, March 27].

[11] Object Management Group. UML 2.0 OCL Specification [Computer file]. Available from: http://www.omg.org [2009, March 27].

[12] Dong, J., Yang, S., and Zhang, K. Visualizing Design Patterns in Their Application and Composition. IEEE Transactions on Software Engineering 33 (July 2007): 433-453.

[13] Fernandez, E.B. Metadata and Authorization Pattern [Computer file]. Available from: http://www.cse.fau.edu/~ed/MetadataPatterns.pdf [2009, March 27].

[14] Supaporn, K., Prompoon, N., and Rojkangsadan, T. Enterprise Assets Security Requirements Construction from ESRMG Grammar based on Security Patterns, Proceedings of the 14^{th} Asia-Pacific Software Engineering Conference (APSEC '07)., 2007

[15] Object Management Group. UML Profile Specifications [Computer file]. Available from: http://www.omg.org [2009, March 27].

[16] Object Management Group. UML Standard Elements [Computer file]. Available from: http://www.omg.org [2009, March 27].

[17] Dong, J. VisDP: A Web Service for Visualizing Design Pattern on Demand [Computer program]. Available from http://www.utdallas.edu/~jdong/VisDP [2009, March 27].

[18] McCabe, T. A Software Complexity Measure. IEEE Transaction on Software Engineering 2 (December 1976): 308-320.

[19] Nickerson, J.V. Visual Programming. PhD dissertation, New York, 1994.

[20] การุณี บวรประเสริฐ. การสร้างกรณีทดสอบจากแผนภาพสเตทชาร์ต. วิทยานิพนธ์ปริญญามหาบัณฑิต, ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2547.

[21] Fernandez, E.B., Sorgente, T., and Larrondo-Petrie, M.M. Even more patterns for secure operating systems, Proceedings of the Pattern Languages of Programs Conference., 2006.

[22] Delessy-Gassant, N., Fernandez, E.B., Rajput, S., and Larrando-Petrie, M.M. Patterns for Application Firewalls, Proceedings of the Pattern Languages of Programs Conference., 2004.

ภาคผนวก

ภาคผนวก ก
แม่พิมพ์ต้นแบบและป้ายระบุของยูเอ็มแอลเซค

ตารางที่ ก.1 แม่พิมพ์ต้นแบบของยูเอ็มแอลเซค

แม่พิมพ์ต้นแบบ	คลาสพื้นฐาน	ป้ายระบุ	ข้อบังคับ	คำอธิบาย
fair exchange	ระบบย่อย (Subsystem)	start, stop, adversary	หลังจากเข้าสู่กิจกรรมเริ่มต้นของระบบย่อย ระบบจะต้องมุ่งเข้าสู่กิจกรรมสิ้นสุดของระบบย่อยเสมอ	การแลกเปลี่ยนที่กำหนดกิจกรรมเริ่มต้นและกิจกรรมสิ้นสุดของระบบย่อย
provable	ระบบย่อย	action, cert, adversary	มีกิจกรรมที่ไม่สามารถละเว้นได้	การกำหนดกิจกรรมที่ไม่สามารถละเว้นได้
rbac	ระบบย่อย	protected, role, right	มีการควบคุมกิจกรรมของผู้ใช้งานให้เป็นไปตามบทบาท	การควบคุมการเข้าถึงเชิงบทบาทของผู้ใช้งาน
Internet	เส้นเชื่อมโยง (Link)			การเชื่อมโยงผ่านเครือข่ายอินเตอร์เน็ต
encrypted	เส้นเชื่อมโยง			การเชื่อมโยงที่มีการเข้ารหัสข้อมูล
LAN	เส้นเชื่อมโยง และจุดต่อ (Node)			การเชื่อมโยงภายในเครือข่าย
wire	เส้นเชื่อมโยง			สายเชื่อม
smart card	จุดต่อ			สมาร์ตคาร์ด
POS device	จุดต่อ			อุปกรณ์พีโอเอส
Issuer node	จุดต่อ			จุดจ่ายข้อมูลที่สำคัญ
secrecy	การพึ่งพา (Dependency)			การรักษาความลับของข้อมูล
integrity	การพึ่งพา			การรักษาความบูรณภาพของข้อมูล
high	การพึ่งพา			การรักษาข้อมูลที่มีความสำคัญสูง
critical	อ็อบเจกต์ (Object) และระบบย่อย	secret, integrity, authenticity, high, fresh		อ็อบเจกต์ที่มีความเสี่ยงต่อการบุกรุก
secure link	ระบบย่อย	adversary	มีการควบคุมความมั่นคงของเส้นเชื่อมโยงให้เป็นไปตามที่กำหนดไว้	การเชื่อมโยงที่กำหนดความมั่นคง
secure dependency	ระบบย่อย		มีการควบคุมความมั่นคงขององค์ประกอบโดยใช้ <<call>> และ <<send>>	การกำหนดความมั่นคงที่สัมพันธ์กับความมั่นคงขององค์ประกอบอื่น
data security	ระบบย่อย	adversary, integrity, authenticity	มีการกำหนดความลับ ความบูรณภาพ ความสมจริง และความบริสุทธิ์ของข้อมูล	ข้อมูลที่ต้องป้องกันจากภัยคุกคามที่อาจเกิดขึ้น

ตารางที่ ก.1 แม่พิมพ์ต้นแบบของยูเอ็มแอลเซค (ต่อ)

แม่พิมพ์ต้นแบบ	คลาสพื้นฐาน	ป้ายระบุ	ข้อบังคับ	คำอธิบาย
no down-flow	ระบบย่อย		ป้องกันการรั่วไหลของข้อมูล	การป้องกันข้อมูลที่มีระดับความลับต่ำมีผลกระทบต่อข้อมูลที่มีระดับความลับสูง
no up-flow	ระบบย่อย		ป้องกันการรั่วไหลของข้อมูล	การป้องกันข้อมูลที่มีระดับความลับสูงมีผลกระทบต่อข้อมูลที่มีระดับความลับต่ำ
guarded access	ระบบย่อย		ถ้ามีการเข้าถึงคลาสที่ถูกควบคุม จะต้องมีการตรวจสอบจากอ็อบเจกต์ที่ควบคุมคลาสดังกล่าว	การควบคุมการเข้าถึงโดยใช้อ็อบเจกต์ควบคุม
guarded	อ็อบเจกต์	guard		อ็อบเจกต์ที่ถูกควบคุม

ตารางที่ ก.2 ป้ายระบุของยูเอ็มแอลเซค

ป้ายระบุ	แม่พิมพ์ต้นแบบ	ชนิด	มัลติพลิซิที	คำอธิบาย
start	fair exchange	กิจกรรม (Activity)	*	กิจกรรมเริ่มต้น
stop	fair exchange	กิจกรรม	*	กิจกรรมสิ้นสุด
adversary	fair exchange	ผู้บุกรุกที่ถูกจำลอง (Adversary Model)	1	ผู้บุกรุก
action	provable	กิจกรรม	*	กิจกรรมที่ต้องการพิสูจน์การทำงาน
cert	provable	ตัวแปร	*	ตัวแปรที่ใช้เป็นใบรับรอง (Certificate) ของกิจกรรมที่ต้องการพิสูจน์การทำงาน
adversary	provable	ผู้บุกรุกที่ถูกจำลอง	*	ผู้บุกรุก
protected	rbac	กิจกรรม	*	กิจกรรมที่ต้องการควบคุม
role	rbac	(ผู้แสดง (Actor), บทบาท (Role))	*	การกำหนดบทบาทให้แก่ผู้แสดง
right	rbac	(บทบาท, กิจกรรม)	*	การกำหนดกิจกรรมให้แก่บทบาท
secrecy	critical	ตัวแปร	*	ตัวแปรที่มีการรักษาความลับของข้อมูล
integrity	critical	(ตัวแปร, ค่าที่เป็นไปได้ของตัวแปร)	*	ตัวแปรที่มีการรักษาความบูรณภาพของข้อมูล
authenticity	critical	(ตัวแปร, ค่าตัวแปรเริ่มต้น)	*	ตัวแปรที่มีการรักษาความสมจริงของข้อมูล
high	critical	ชื่อการดำเนินการของคลาส	*	การดำเนินการที่มีความสำคัญสูง
fresh	critical	ตัวแปร	*	ตัวแปรที่มีการใช้ ณ เวลาที่จำเพาะ
adversary	secure links	ผู้บุกรุกที่ถูกจำลอง	1	ผู้บุกรุก
adversary	data security	ผู้บุกรุกที่ถูกจำลอง	1	ผู้บุกรุก
integrity	data security	(ตัวแปร, ค่าที่เป็นไปได้ของตัวแปร)	*	ตัวแปรที่มีการรักษาความบูรณภาพของข้อมูล

ตารางที่ ก.2 ป้ายระบุของยูเอ็มแอลเซค (ต่อ)

ป้ายระบุ	แม่พิมพ์ต้นแบบ	ชนิด	มัลติพลิซิที	คำอธิบาย
authenticity	data security	(ตัวแปร, ค่าตัวแปรเริ่มต้น)	*	ตัวแปรที่มีการรักษาความสมจริงของข้อมูล
guard	guarded	ชื่ออ็อบเจกต์	1	อ็อบเจกต์ที่ควบคุม

ภาคผนวก ข
ยูเอ็มแอลเซคเอสพี

ยูเอ็มแอลเซคเอสพีที่ได้จากแบบรูปความมั่นคงในขอบเขตงานวิจัยนี้ ประกอบด้วย 58 แม่พิมพ์ต้นแบบและ 25 ป้ายระบุจาก 27 แบบรูปความมั่นคง จาก 5 กลุ่มแบบรูปความมั่นคง ซึ่งสามารถจำแนกตามกลุ่มของแบบรูปความมั่นคงได้ดังนี้

กลุ่มที่ 1 แบบจำลองการควบคุมการเข้าถึง ประกอบด้วย

1) การให้อำนาจ
2) การควบคุมการเข้าถึงเชิงบทบาท
3) ความมั่นคงหลายระดับ
4) การเฝ้าสังเกตเชิงอ้างอิง

กลุ่มที่ 2 สถาปัตยกรรมการควบคุมการเข้าถึงระบบ ประกอบด้วย

1) จุดเข้าระบบเดี่ยว
2) จุดตรวจสอบ
3) เซสชันทางความมั่นคง
4) การควบคุมการเข้าถึงด้วยการแสดงความผิดพลาด
5) การจำกัดการเข้าถึง

กลุ่มที่ 3 การควบคุมการเข้าถึงระบบปฏิบัติการ ประกอบด้วย

1) องค์ประกอบพิสูจน์ตัวตน
2) การควบคุมการสร้างกระบวนการ
3) การควบคุมการสร้างอ็อบเจกต์
4) การตรวจสอบการเข้าถึงอ็อบเจกต์
5) การควบคุมหน่วยความจำเสมือน
6) การควบคุมขอบเขตกระทำการ
7) การควบคุมสิ่งแวดล้อมที่กระทำการ
8) การให้อำนาจในแฟ้มข้อมูล

กลุ่มที่ 4 สถาปัตยกรรมไฟล์วอลล์ ประกอบด้วย

1) ไฟล์วอลล์สำหรับการกรองแพ็คเกจ
2) ไฟล์วอลล์เชิงตัวแทน
3) ไฟล์วอลล์เชิงสถานะ

กลุ่มที่ 5 การประยุกต์ใช้ความมั่นคงบนอินเตอร์เน็ต ประกอบด้วย

1) การปิดบังข้อมูล
2) ช่องทางความมั่นคง
3) ผู้เป็นที่รู้จัก

4) เขตปลอดการป้องกัน
5) ตัวแทนป้องกัน
6) ตัวแทนบูรณาการ
7) ประตูหน้า

ยูเอ็มแอลเซคเอสพีจะแบ่งออกเป็นสองประเภทคือ ยูเอ็มแอลเซคเอสพีสำหรับแสดงข้อมูลทางโครงสร้างของแบบรูปความมั่นคง และยูเอ็มแอลเซคเอสพีสำหรับแสดงข้อมูลทางความมั่นคงของแบบรูปความมั่นคง โดยรายละเอียดของแต่ละแม่พิมพ์ต้นแบบ ประกอบไปด้วย ชื่อแบบรูปความมั่นคง คำอธิบายของแบบรูปความมั่นคง ชื่อแม่พิมพ์ต้นแบบ คลาสพื้นฐาน ป้ายระบุที่ใช้อธิบายแม่พิมพ์ต้นแบบ เงื่อนไขบังคับที่จำเป็นต้องพิจารณา คำอธิบายของแม่พิมพ์ต้นแบบ และในรายละเอียดของแต่ละป้ายระบุ ประกอบไปด้วย ชื่อแบบรูปความมั่นคง ชื่อป้ายระบุ แม่พิมพ์ต้นแบบที่ใช้ป้ายระบุ ค่าของป้ายระบุ ตัวอย่างค่าของป้ายระบุ คำอธิบายของป้ายระบุ โดยมีรายละเอียดดังต่อไปนี้

ตารางที่ ข.1 แม่พิมพ์ต้นแบบสำหรับแสดงข้อมูลทางโครงสร้างของแบบรูปความมั่นคง

แม่พิมพ์ต้นแบบ	คลาสพื้นฐาน	ป้ายระบุ	เงื่อนไขบังคับ	คำอธิบาย
spc (Security Pattern Class)	Class	"role@name[instance]"	1> self.taggedValue.dataValue.name -> notEmpty 2> self.taggedValue.name -> forall(v1, v2:name | v1.name <> v2.name) implies (v1.instance -> isEmpty and v2.instance -> isEmpty) 3> self.taggedValue.name -> exists(v1, v2:name | v1.name = v2.name) implies (v1.instance -> notEmpty and v2.instance -> notEmpty and v1.instance <> v2.instance)	คลาสที่เป็นองค์ประกอบภายในแบบรูปความมั่นคง
spt (Security Pattern data Type)	Class	"role@name[instance]"		คลาสที่เป็นแบบชนิดข้อมูลภายในแบบรูปความมั่นคง
spr (Security Pattern Relationship)	Relationship	"role@name[instance]"		ความสัมพันธ์ระหว่างคลาสที่เป็นองค์ประกอบภายในแบบรูปความมั่นคง

ตารางที่ ข.2 ป้ายระบุสำหรับแสดงข้อมูลทางโครงสร้างของแบบรูปความมั่นคง

ป้ายระบุ	แม่พิมพ์ต้นแบบ	ค่าของป้ายระบุ	ตัวอย่างค่าของป้ายระบุ	มัลติพลิซิที	คำอธิบาย
"role@name[instance]"	แม่พิมพ์ต้นแบบที่สร้างทั้งหมด	บูลีนแสดงลักษณะองค์ประกอบดังกล่าวในแบบรูป	true หรือ false	*	ระบุว่า องค์ประกอบดังกล่าวมีบทบาท "role" ในแบบรูป "name" ลำดับที่ "instance" ในแผนภาพหรือไม่

ตารางที่ ข.3 แม่พิมพ์ต้นแบบสำหรับแสดงข้อมูลทางความมั่นคงของแบบรูปความมั่นคง

แบบรูปความมั่นคง	คำอธิบายของแบบรูปความมั่นคง	แม่พิมพ์ต้นแบบ	คลาสพื้นฐาน	ป้ายระบุ	เงื่อนไขบังคับ	คำอธิบาย
การให้อำนาจ (Authorization)	เป็นแบบรูปที่เสนอการกำหนดสิทธิ์ของผู้เข้าใช้ทรัพยากรในระบบ	subject	Class	"role@name[instance]"		ผู้เข้าใช้ทรัพยากรของระบบ
		accessRight	Class	controlledType และ "role@name[instance]"	1> self.taggedValue -> forall(tv|tv.name = "controlledType") implies (tv.dataValue = "ACLs" or tv.dataValue = "Capabilities"))	องค์ประกอบที่ควบคุมการเข้าถึงทรัพยากร
		accessType	Class	"role@name[instance]"		ลักษณะของการเข้าใช้ทรัพยากร
		restrictedRule	Class	"role@name[instance]"		เงื่อนไขที่เป็นข้อห้ามในการให้อำนาจแก่ผู้ใช้งาน
		copyFlag	Class	"role@name[instance]"		การอนุญาตให้ผู้อื่นคัดลอกอำนาจของผู้ใช้งานดังกล่าว
การควบคุมการเข้าถึงเชิงบทบาท (Role-Based Access Control)	เป็นแบบรูปที่เสนอการกำหนดสิทธิ์ของผู้เข้าใช้ทรัพยากรในระบบตามบทบาทที่กำหนดไว้	role	Class	"role@name[instance]"		บทบาทของผู้เข้าใช้ทรัพยากรในระบบ
		adminRole	Class	"role@name[instance]"		บทบาทของผู้ดูแลระบบ
		adminRight	Class	"role@name[instance]"		องค์ประกอบที่ควบคุมการเข้าถึงทรัพยากรของผู้ดูแลระบบ

ตารางที่ ข.3 แม่พิมพ์ต้นแบบสำหรับแสดงข้อมูลทางความมั่นคงของแบบรูปความมั่นคง (ต่อ)

แบบรูปความมั่นคง	คำอธิบายของแบบรูปความมั่นคง	แม่พิมพ์ต้นแบบ	คลาสพื้นฐาน	ป้ายระบุ	เงื่อนไขบังคับ	คำอธิบาย
ความมั่นคงหลายระดับ (Multilevel Security)	เป็นแบบรูปที่เสนอการกำหนดสิทธิ์ของผู้เข้าใช้ทรัพยากรในระบบตามระดับความปลอดภัยของผู้เข้าใช้ทรัพยากรและทรัพยากร	accessLevel	Class	assign และ "role@name[instance]"	1> self.taggedValue -> forall(tv|tv.name = "assign") implies (tv.dataValue -> isNotEmpty)	ระดับการเข้าถึงของผู้เข้าใช้ทรัพยากร
		guardLevel	Class	assign และ "role@name[instance]"	1> self.taggedValue -> forall(tv|tv.name = "assign") implies (tv.dataValue -> isNotEmpty)	ระดับความปลอดภัยของทรัพยากร
การเฝ้าสังเกตเชิงอ้างอิง (Reference Monitor)	เป็นแบบรูปที่เสนอการตรวจสอบการร้องขอใช้ทรัพยากรในระบบของผู้ใช้งาน	request	Class	"role@name[instance]"		คำร้องขอใช้ทรัพยากร
		referenceMonitor	Class	"role@name[instance]"		องค์ประกอบที่ตรวจสอบการร้องขอใช้ทรัพยากร
		monitored	Relationship	monitor และ "role@name[instance]"	1> self.taggedValue -> forall(tv|tv.name = "monitor") implies (tv.dataValue -> isNotEmpty)	การเชื่อมโยงที่มีการตรวจสอบการร้องขอใช้ทรัพยากร
จุดเข้าระบบเดี่ยว (Single Access Point)	เป็นแบบรูปที่เสนอการควบคุมการเข้าถึงระบบ โดยการกำหนดให้มีช่องทางเดียวในการเข้าถึงระบบเท่านั้น	client	Class และ Component	"role@name[instance]"		ผู้ใช้งานจากภายนอกระบบ
		accessPoint	Class	method และ "role@name[instance]"	1> self.taggedValue -> forall(tv|tv.name = "method") implies (tv.dataValue -> isNotEmpty)	จุดเข้าระบบ
		appService	Class และ Component	"role@name[instance]"		บริการของโปรแกรมประยุกต์
จุดตรวจสอบ (Check Point)	เป็นแบบรูปที่เสนอการควบคุมการเข้าถึงของระบบ โดยการกำหนดจุดตรวจสอบที่ใช้ในการควบคุมการเข้าถึงบริการของระบบ	checkPoint	Class	protect และ "role@name[instance]"	1> self.taggedValue -> forall(tv|tv.name = "protect") implies (tv.dataValue -> isNotEmpty)	จุดตรวจสอบผู้ใช้งานจากภายนอกระบบ
เซสชันทางความมั่นคง (Security Session)	เป็นแบบรูปที่เสนอการใช้เซสชันทางความมั่นคงที่มีการกำหนดช่วงเวลาการใช้งาน	securitySession	Class	sessionType lifetime และ "role@name[instance]"	1> self.taggedValue -> forall(tv|tv.name = "lifetime") implies (tv.dataValue -> isNotEmpty) 2> self.taggedValue -> select(tv|tv.name = "lifetime").dataValue.oclIsTypeOf(Integer);	เซสชันทางความมั่นคง
การควบคุมการเข้าถึงด้วยการแสดงความผิดพลาด (Full Access with Errors)	เป็นแบบรูปที่เสนอการแสดงฟังก์ชันการทำงานทั้งหมดของระบบให้ผู้ใช้งานทราบ ซึ่งระบบควบคุมการเข้าใช้ฟังก์ชันโดยการแสดงข้อผิดพลาดให้ผู้ใช้งานทราบในกรณีที่ผู้ใช้งานเรียกใช้ฟังก์ชันที่ไม่มีสิทธิ์ในการเรียกใช้	errorNotification	Class	"role@name[instance]"		องค์ประกอบที่แสดงข้อผิดพลาดที่เกิดจากการเข้าถึงการดำเนินการที่ไม่มีสิทธิ์ในการเข้าถึง

ตารางที่ ข.3 แม่พิมพ์ต้นแบบสำหรับแสดงข้อมูลทางความมั่นคงของแบบรูปความมั่นคง (ต่อ)

แบบรูปความมั่นคง	คำอธิบายของแบบรูปความมั่นคง	แม่พิมพ์ต้นแบบ	คลาสพื้นฐาน	ป้ายระบุ	เงื่อนไขบังคับ	คำอธิบาย
การจำกัดการเข้าถึง (Limited Access)	เป็นแบบรูปที่เสนอการแสดงช่องทางการเข้าถึงที่แตกต่างกัน สำหรับผู้ใช้งานที่มีอำนาจในการเข้าถึงที่ต่างกัน	interfaceBuilder	Class	“role@name[instance]”		องค์ประกอบที่กำหนดส่วนต่อประสานให้แก่ผู้ใช้งาน
		enableUIElement	Class	“role@name[instance]”		คุณลักษณะที่แสดงสถานะของการมองเห็นในแต่ละองค์ประกอบของส่วนต่อประสาน
องค์ประกอบพิสูจน์ตัวตน (Authenticator)	เป็นแบบรูปที่เสนอการใช้องค์ประกอบพิสูจน์ตัวตนในการระบุตัวตนของผู้ใช้งานในระบบปฏิบัติการ	authenticator	Class	“role@name[instance]”		องค์ประกอบที่ทำการตรวจสอบตัวตนของผู้ใช้งานก่อนทำการให้อำนาจแก่ผู้ใช้งาน
		proofOfIdentity	Class	“role@name[instance]”		องค์ประกอบที่ใช้ในการแสดงตัวตนของผู้ใช้งาน
องค์ประกอบพิสูจน์ตัวตน (Authenticator)	เป็นแบบรูปที่เสนอการใช้องค์ประกอบพิสูจน์ตัวตนในการระบุตัวตนของผู้ใช้งานในระบบปฏิบัติการ	certificate	Class	“role@name[instance]”		ใบรับรองในการระบุตัวตน
		certificateAuthority	Class	“role@name[instance]”		ผู้ให้ใบรับรองในการระบุตัวตน
การควบคุมการสร้างกระบวนการ (Controlled Process Creator)	เป็นแบบรูปที่เสนอการกำหนดสิทธิ์ให้กับกระบวนการที่เกิดขึ้นใหม่ในระบบปฏิบัติการ	processCreator	Class	“role@name[instance]”		องค์ประกอบที่ควบคุมการสร้างกระบวนการ
		processDescriptor	Class	“role@name[instance]”		องค์ประกอบที่จัดเก็บสิทธิ์ของกระบวนการ
การควบคุมการสร้างอ็อบเจกต์ (Controlled Object Factory)	เป็นแบบรูปที่เสนอการกำหนดสิทธิ์ให้กับอ็อบเจกต์ที่เกิดขึ้นใหม่ในระบบปฏิบัติการ	objectFactory	Class	“role@name[instance]”		องค์ประกอบที่ควบคุมการสร้างอ็อบเจกต์
การควบคุมหน่วยความจำเสมือน (Controlled Virtual Address Space)	เป็นแบบรูปที่เสนอการควบคุมการเข้าถึงหน่วยความจำเสมือนในระบบปฏิบัติการ	vas	Class	“role@name[instance]”		หน่วยความจำเสมือนในระบบปฏิบัติการ
		vasAddress	Class	“role@name[instance]”		ที่อยู่ของเซกเมนต์
		vasSize	Class	“role@name[instance]”		จำนวนหน้าของเซกเมนต์ที่ถูกจำกัด
การควบคุมขอบเขตกระทำการ (Execution Domain)	เป็นแบบรูปที่เสนอการควบคุมขอบเขตกระทำการของกระบวนการในระบบปฏิบัติการ	domainProtection	Class	“role@name[instance]”		องค์ประกอบที่ตรวจสอบการเปลี่ยนโดเมนของกระบวนการภายในระบบปฏิบัติการ
		domainDescriptor	Class	“role@name[instance]”		องค์ประกอบที่จัดเก็บสิทธิ์ของกระบวนการในการเข้าใช้ทรัพยากรในโดเมนที่กำหนด

ตารางที่ ข.3 แม่พิมพ์ต้นแบบสำหรับแสดงข้อมูลทางความมั่นคงของแบบรูปความมั่นคง (ต่อ)

แบบรูปความมั่นคง	คำอธิบายของแบบรูปความมั่นคง	แม่พิมพ์ต้นแบบ	คลาสพื้นฐาน	ป้ายระบุ	เงื่อนไขบังคับ	คำอธิบาย
การให้อำนาจในแฟ้ม (File Authorization)	เป็นแบบรูปที่เสนอการควบคุมการเข้าถึงแฟ้มในระบบปฏิบัติการ	fileDirectory	Class และ Component	"role@name[instance]"		สารบบในระบบปฏิบัติการ
		workstation	Class และ Component	osType และ "role@name[instance]"		สถานีงานที่เข้าใช้แฟ้มข้อมูล
ไฟร์วอลล์สำหรับการกรองแพ็คเกจ (Packet Filter Firewall)	เป็นแบบรูปที่เสนอไฟร์วอลล์ที่ควบคุมการรับส่งแพ็คเกจในระดับไอพี	pfFirewall (Packet Filter Firewall)	Class และ Component	product openedPort และ "role@name[instance]"	1> self.taggedValue -> select(tv|tv.name = "openedPort").dataValue.oclIsTypeOf(Integer); 2> self.taggedValue -> forall(tv|tv.name = "openedPort") implies (tv.dataValue >= 0 and tv.dataValue <= 65535)	ไฟร์วอลล์สำหรับการกรองแพ็คเกจ
		ruleBase	Class	"role@name[instance]"		องค์ประกอบที่กรองแพ็คเกจของไฟร์วอลล์
		ipAddress	Class	"role@name[instance]"		เลขที่อยู่ไอพี
		appServer	Class และ Component	componentType และ "role@name[instance]"	1> self.taggedValue -> forall(tv|tv.name = "componentType" implies (tv.dataValue = "web component" or tv.dataValue = "business component"))	เครื่องบริการโปรแกรมประยุกต์
ไฟร์วอลล์เชิงตัวแทน (Proxy-Based Firewall)	เป็นแบบรูปที่เสนอไฟร์วอลล์ที่ควบคุมการรับส่งแพ็คเกจในระดับข้อความในแพ็คเกจ	pxFirewall (Proxy Based Firewall)	Class และ Component	product openedPort และ "role@name[instance]"	1> self.taggedValue -> select(tv|tv.name = "openedPort").dataValue.oclIsTypeOf(Integer); 2> self.taggedValue -> forall(tv|tv.name = "openedPort") implies (tv.dataValue >= 0 and tv.dataValue <= 65535)	ไฟร์วอลล์เชิงตัวแทน
		proxy	Class	"role@name[instance]"		ตัวแทนของบริการในระบบ
ไฟร์วอลล์เชิงสถานะ (Stateful Firewall)	เป็นแบบรูปที่เสนอไฟร์วอลล์ที่เก็บสถานะของแม่ข่ายภายนอกระบบเพื่อลดจำนวนการตรวจสอบแพ็คเกจ	sfFirewall (Stateful Firewall)	Class และ Component	product openedPort และ "role@name[instance]"	1> self.taggedValue -> select(tv|tv.name = "openedPort").dataValue.oclIsTypeOf(Integer); 2> self.taggedValue -> forall(tv|tv.name = "openedPort") implies (tv.dataValue >= 0 and tv.dataValue <= 65535)	ไฟร์วอลล์เชิงสถานะ
		stateTable	Class	"role@name[instance]"		องค์ประกอบที่เก็บสถานะของแพ็คเกจ

ตารางที่ ข.3 แม่พิมพ์ต้นแบบสำหรับแสดงข้อมูลทางความมั่นคงของแบบรูปความมั่นคง (ต่อ)

แบบรูปความมั่นคง	คำอธิบายของแบบรูปความมั่นคง	แม่พิมพ์ต้นแบบ	คลาสพื้นฐาน	ป้ายระบุ	เงื่อนไขบังคับ	คำอธิบาย
การปิดบังข้อมูล (Information Obscurity)	เป็นแบบรูปที่เสนอการปิดบังข้อมูลจากการเข้าถึงของกระบวนการที่ไม่พึ่งประสงค์	encryptedData	Class	“role@name[instance]”		ข้อมูลที่ถูกเข้ารหัสลับ
		encryptionComponent	Class	“role@name[instance]”		องค์ประกอบที่เข้ารหัสลับให้กับข้อมูล
		encryptionKey	Class	keyType และ “role@name[instance]”	1> self.taggedValue -> forall(tv|tv.name = “keyType”) implies (tv.dataValue = “asymmetric key” or tv.dataValue = “symmetric key”))	กุญแจที่ใช้ในการเข้ารหัสลับ
		keyProvider	Class และ Component	“role@name[instance]”		องค์ประกอบที่จัดหากุญแจที่ใช้ในการเข้ารหัสลับ
ช่องทางความมั่นคง (Secure Channels)	เป็นแบบรูปที่เสนอการแลกเปลี่ยนข้อมูลระหว่างผู้ใช้งานและเครื่องบริการเว็บ	webBrowser	Class และ Component	product และ “role@name[instance]”		เว็บเบราว์เซอร์ของผู้ใช้งาน
		webServer	Class และ Component	product abstract และ “role@name[instance]”	1> self.taggedValue -> select(tv|tv.name = “abstract”).dataValue.oclIsTypeOf(Boolean);	เครื่องบริการเว็บ
ผู้เป็นที่รู้จัก (Known Partners)	เป็นแบบรูปที่เสนอการพิสูจน์ตัวตนของผู้ใช้งานและเครื่องบริการเว็บที่ถูกใช้งาน	uivService (User Identity Verification Service)	Class	“role@name[instance]”		บริการทวนสอบของการพิสูจน์ผู้ใช้งาน
		userIdentity	Class	“role@name[instance]”		องค์ประกอบที่ใช้ในการระบุตัวตนของผู้ใช้งาน
		systemIdentity	Class	“role@name[instance]”		องค์ประกอบที่ใช้ในการระบุตัวตนของเครื่องบริการเว็บที่ถูกใช้งาน
เขตปลอดการป้องกัน (Demilitarized Zone)	เป็นแบบรูปที่เสนอการแยกฟังก์ชันการทำงานและข้อมูลที่สำคัญออกจากเว็บเซิฟเวอร์	router	Class และ Component	openedPort และ “role@name[instance]”	1> self.taggedValue -> select(tv|tv.name = “openedPort”).dataValue.oclIsTypeOf(Integer); 2> self.taggedValue -> forall(tv|tv.name = “openedPort”) implies (tv.dataValue >= 0 and tv.dataValue <= 65535)	องค์ประกอบที่จัดเส้นทางของแพ็คเกจที่เข้าออกในระบบ
ตัวแทนป้องกัน (Protection Reverse Proxy)	เป็นแบบรูปที่เสนอการใช้ตัวแทนในการป้องกันการเข้าถึงแม่ข่ายในระดับโปรแกรมประยุกต์	reverseProxy	Class	mainURL blackList whiteList และ “role@name[instance]”	1> self.taggedValue -> forall(tv1,tv2|tv1.name = “blackList” and tv2.name = “whiteList”) implies (tv1.dataValue <> tv2.dataValue)	ตัวแทนที่ป้องกันการเข้าถึงแม่ข่ายท้องถิ่น
ประตูหน้า (Front Door)	เป็นแบบรูปที่เสนอการใช้แม่ข่ายตัวแทนบูรณาการในการระบุตัวตนและการตรวจสอบผู้ใช้งาน	userDirectory	Class	“role@name[instance]”		องค์ประกอบที่จัดการข้อมูลที่ใช้ในการระบุตัวตนและการตรวจสอบผู้ใช้งาน

ตารางที่ ข.4 ป้ายระบุสำหรับแสดงข้อมูลทางความมั่นคงของแบบรูปความมั่นคง

แบบรูปความมั่นคง	ป้ายระบุ	แม่พิมพ์ต้นแบบ	ค่าของป้ายระบุ	ตัวอย่างค่าของป้ายระบุ	มัลติพลิซิที	คำอธิบาย
การให้อำนาจ (Authorization)	controlledType	accessRight	ประเภทขององค์ประกอบที่ควบคุมการเข้าถึงทรัพยากร	รายการควบคุมการเข้าถึง (Access Control Lists: ACLs) รายการแสดงสมรรถนะของผู้เข้าใช้ (Capabilities)	1	ประเภทขององค์ประกอบที่ควบคุมการเข้าถึงทรัพยากร
ความมั่นคงหลายระดับ (Multilevel Security)	assign	accessLevel	ชื่ออ็อบเจกต์ที่เป็นผู้กำหนดค่า	-	1	ชื่ออ็อบเจกต์ที่เป็นผู้กำหนดค่าระดับการเข้าถึงของผู้เข้าถึงทรัพยากร
	assign	guardedLevel	ชื่ออ็อบเจกต์ที่เป็นผู้กำหนดค่า	-	1	ชื่ออ็อบเจกต์ที่เป็นผู้กำหนดค่าระดับความปลอดภัยของทรัพยากร
การเฝ้าสังเกตเชิงอ้างอิง (Reference Monitor)	monitor	monitored	ชื่ออ็อบเจกต์ที่เป็นผู้ตรวจสอบ	-	1	ชื่ออ็อบเจกต์ที่เป็นผู้ตรวจสอบการเข้าใช้ทรัพยากร
จุดเข้าระบบเดี่ยว (Single Access Point)	method	accessPoint	วิธีการเข้าสู่ระบบ	การกรอกชื่อผู้ใช้และรหัสผ่าน	1	วิธีการเข้าสู่ระบบ
จุดตรวจสอบ (Check Point)	protect	checkpoint	บริการที่ต้องการตรวจสอบ	การเข้าถึงเอกสารลับหรือแฟ้มข้อมูลลับ	*	บริการที่ต้องการตรวจสอบโดยใช้จุดตรวจสอบ
เซสชันทางความมั่นคง (Security Session)	sessionType	securitySession	ประเภทของเซสชันทางความมั่นคง	คุกกี้ (Cookie) เซสชัน (Session)	*	ประเภทของเซสชันทางความมั่นคงของผู้ใช้งาน
	lifetime	securitySession	อายุการใช้งานของเซสชันความมั่นคง	30 นาที 1 ชั่วโมง		อายุการใช้งานของเซสชันความมั่นคง
การให้อำนาจในแฟ้ม (File Authorization)	osType	workstation	ระบบปฏิบัติการของสถานีงาน	วินโดวส์ (Windows) ลีนุกซ์ (Linux)	*	ระบบปฏิบัติการของสถานีงาน
ไฟร์วอลล์สำหรับการกรองแพ็คเกจ (Packet Filter Firewall)	product	pfFirewall	ชื่อของผลิตภัณฑ์ไฟร์วอลล์	"ARGuE" "OpenBSD Packet Filtering Firewall" "Linux Firewall"	*	ชื่อของผลิตภัณฑ์ไฟร์วอลล์
	openedPort	pfFirewall	หมายเลขพอร์ททที่เปิด	0 – 65535	*	หมายเลขพอร์ททที่เปิด
ไฟร์วอลล์เชิงตัวแทน (Proxy-Based Firewall)	product	pxFirewall	ชื่อผลิตภัณฑ์ไฟร์วอลล์	"Pipex Security Firewall" "InterGate Firewall" "Postfix"	*	ชื่อของผลิตภัณฑ์ไฟร์วอลล์
	openedPort	pxFirewall	หมายเลขพอร์ททที่เปิด	0 – 65535	*	หมายเลขพอร์ททที่เปิด
ไฟร์วอลล์เชิงสถานะ (Stateful Firewall)	product	sfFirewall	ชื่อผลิตภัณฑ์ไฟร์วอลล์	"Pipex Security Firewall" "InterGate Firewall"	*	ชื่อของผลิตภัณฑ์ไฟร์วอลล์
	openedPort	sfFirewall	หมายเลขพอร์ททที่เปิด	0 – 65535	*	หมายเลขพอร์ททที่เปิด

ตารางที่ ข.4 ป้ายระบุสำหรับแสดงข้อมูลทางความมั่นคงของแบบรูปความมั่นคง (ต่อ)

แบบรูปความมั่นคง	ป้ายระบุ	แม่พิมพ์ต้นแบบ	ค่าของป้ายระบุ	ตัวอย่างค่าของป้ายระบุ	มัลติพลิซิที	คำอธิบาย
การปิดบังข้อมูล (Information Obscurity)	keyType	encryptionKey	ชนิดของกุญแจในการเข้ารหัสลับ	สมมาตร หรือ อสมมาตร	*	ชนิดของกุญแจในการเข้ารหัสลับ
ช่องทางความมั่นคง (Secure Channels)	product	webServer	ชื่อผลิตภัณฑ์เครื่องบริการเว็บ	“Apache” “IIS”	*	ชื่อของผลิตภัณฑ์เครื่องบริการเว็บ
	abstract	webServer	บูลีนแสดงลักษณะของเครื่องบริการเว็บที่เป็นนามธรรม	true หรือ false	1	ลักษณะของเครื่องบริการเว็บที่เป็นนามธรรม
	product	webBrowser	ชื่อผลิตภัณฑ์เว็บบราวเซอร์	“IE” “Nescape” “Firefox”	*	ชื่อของผลิตภัณฑ์เว็บบราวเซอร์
เขตปลอดการป้องกัน (Demilitarized Zone)	openedPort	router	หมายเลขพอร์ทที่เปิด	0 – 65535	*	หมายเลขพอร์ทที่เปิด
	componentType	appServer	ประเภทของส่วนประกอบภายในเครื่องบริการโปรแกรมประยุกต์	ส่วนประกอบทางธุรกิจ เช่น “EJBs” ส่วนประกอบเว็บ เช่น “Servlets”	*	ประเภทของส่วนประกอบภายในเครื่องบริการโปรแกรมประยุกต์
ตัวแทนป้องกัน (Protection Reverse Proxy)	mainURL	reverseProxy	ยูอาร์แอลหลักของเครื่องบริการเว็บในระบบ	http://www.chula.ac.th	*	ยูอาร์แอลหลักของแม่ข่ายทั้งหมด
	blackList	reverseProxy	(ยูอาร์แอล, หมายเลขพอร์ท, โพรโทคอล)	(“http://www.abc.com”, 80, “TCP/IP”)	*	รายการของคำร้องขอที่ไม่ยอมรับให้เข้าสู่ระบบ
	whiteList	reverseProxy	(ยูอาร์แอล, หมายเลขพอร์ท, โพรโทคอล)	(“http://www.abc.com”, 80, “TCP/IP”)	*	รายการของคำร้องขอที่ยอมรับให้เข้าสู่ระบบได้

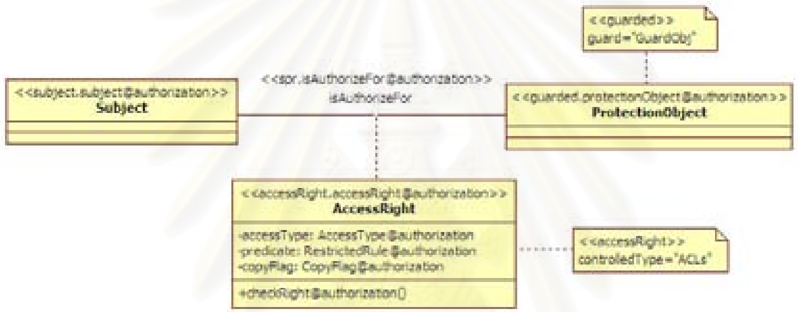
ภาคผนวก ค
การประยุกต์ใช้ยูเอ็มแอลเซคเอสพีในแต่ละแบบรูปความมั่นคง

การประยุกต์ใช้ยูเอ็มแอลเซคเอสพีในแต่ละแบบรูปความมั่นคง เป็นการแนะนำโครงสร้างเบื้องต้นของแต่ละแบบรูปความมั่นคง รวมทั้งการกำหนดยูเอ็มแอลเซคเอสพีในแต่ละองค์ประกอบของแบบรูปความมั่นคง เพื่อแสดงข้อมูลทางโครงสร้างและข้อมูลทางความมั่นคงของแบบรูปความมั่นคง โดยรายละเอียดของการประยุกต์ใช้ยูเอ็มแอลเซคเอสพีในแต่ละแบบรูปความมั่นคง ประกอบไปด้วย ชื่อแบบรูปความมั่นคง ชื่อกลุ่มแบบรูปความมั่นคง คำอธิบายของแบบรูปความมั่นคง แผนภาพคลาสของแบบรูปความมั่นคงที่ประยุกต์ใช้ยูเอ็มแอลเซคเอสพี องค์ประกอบแบบจำลองภายในแบบรูปความมั่นคง ยูเอ็มแอลเซคเอสพีที่ประยุกต์ใช้ และคำอธิบายของแต่ละองค์ประกอบแบบจำลอง โดยมีรายละเอียดดังต่อไปนี้

ตารางที่ ค.1 การประยุกต์ใช้ยูเอ็มแอลเซคเอสพีในแบบรูปการให้อำนาจ

ชื่อแบบรูปความมั่นคง	การให้อำนาจ
กลุ่มแบบรูปความมั่นคง	แบบจำลองการควบคุมการเข้าถึง
คำอธิบาย	เป็นแบบรูปที่เสนอการกำหนดสิทธิ์ของผู้เข้าใช้ทรัพยากรในระบบ

แผนภาพคลาสของแบบรูปความมั่นคงที่ประยุกต์ใช้ยูเอ็มแอลเซคเอสพี

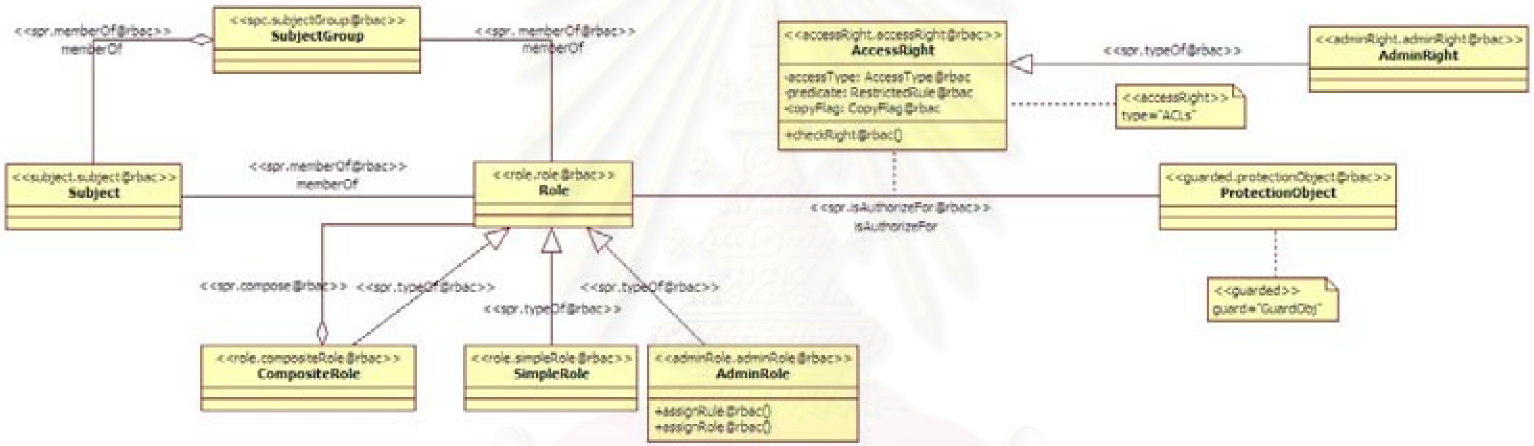


องค์ประกอบแบบจำลอง	แม่พิมพ์ต้นแบบที่ประยุกต์ใช้	คำอธิบาย
คลาส “Subject”	subject	เป็นคลาสที่เข้าใช้ทรัพยากร
คลาส “AccessRight”	accessRight	เป็นคลาสที่ควบคุมการเข้าถึงทรัพยากร จะมีการกำหนดประเภทขององค์ประกอบที่ควบคุมการเข้าถึงทรัพยากรในป้ายระบุ “controlledType”
คลาส “ProtectionObject”	guarded	เป็นทรัพยากรที่ถูกควบคุมการเข้าถึง จะมีการกำหนดอ็อบเจกต์ที่ควบคุมการเข้าถึงในป้ายระบุ “guard”
คุณลักษณะ “accessType” ของคลาส “AccessRight”	accessType	เป็นลักษณะในการเข้าถึงทรัพยากร
คุณลักษณะ “predicate” ของคลาส “AccessRight”	restrictedRule	เป็นเงื่อนไขที่แสดงข้อห้ามในการให้อำนาจแก่ผู้ใช้งาน
คุณลักษณะ “copyFlag” ของคลาส “AccessRight”	copyFlag	เป็นลักษณะของการอนุญาตให้คัดลอกสิทธิ์ของผู้ใช้งานดังกล่าวได้

ตารางที่ ค.2 การประยุกต์ใช้ยูเอ็มแอลเซคเอสพีในแบบรูปการควบคุมการเข้าถึงเชิงบทบาท

ชื่อแบบรูปความมั่นคง	การควบคุมการเข้าถึงเชิงบทบาท
กลุ่มแบบรูปความมั่นคง	แบบจำลองการควบคุมการเข้าถึง
คำอธิบาย	เป็นแบบรูปที่เสนอการกำหนดสิทธิ์ของผู้เข้าใช้ทรัพยากรในระบบตามบทบาทที่กำหนดไว้

แผนภาพคลาสของแบบรูปความมั่นคงที่ประยุกต์ใช้ยูเอ็มแอลเซคเอสพี



องค์ประกอบแบบจำลอง	แม่พิมพ์ต้นแบบที่ประยุกต์ใช้	คำอธิบาย
คลาส “Subject”	subject	เป็นคลาสที่เข้าใช้ทรัพยากร
คลาส “SubjectGroup”	spc	เป็นกลุ่มของผู้เข้าใช้ทรัพยากร
คลาส “Role”	role	เป็นบทบาทของผู้เข้าใช้ทรัพยากร
คลาส “SimpleRole”	role	เป็นบทบาทเชิงเดี่ยวของผู้เข้าใช้ทรัพยากร
คลาส “CompositeRole”	role	เป็นบทบาทเชิงรวมของผู้เข้าใช้ทรัพยากร
คลาส “AdminRole”	adminRole	เป็นบทบาทของผู้ดูแลการเข้าใช้ทรัพยากร
คลาส “AccessRight”	accessRight	เป็นคลาสที่ควบคุมการเข้าถึงทรัพยากร จะมีการกำหนดประเภทขององค์ประกอบที่ควบคุมการเข้าถึงทรัพยากรในป้ายระบุ “controlledType”
คลาส “AdminRight”	adminRight	เป็นคลาสที่ควบคุมการเข้าถึงทรัพยากร ตามสิทธิ์ของผู้ดูแลการเข้าใช้ทรัพยากร
คลาส “ProtectionObject”	guarded	เป็นทรัพยากรที่ถูกควบคุมการเข้าถึง จะมีการกำหนดอ็อบเจกต์ที่ควบคุมการเข้าถึงในป้ายระบุ “guard”
คุณลักษณะ “accessType” ของคลาส “AccessRight”	accessType	เป็นลักษณะในการเข้าถึงทรัพยากร

ตารางที่ ค.2 การประยุกต์ใช้ยูเอ็มแอลเซคเอสพีในแบบรูปการควบคุมการเข้าถึงเชิงบทบาท (ต่อ)

องค์ประกอบแบบจำลอง	แม่พิมพ์ต้นแบบที่ประยุกต์ใช้	คำอธิบาย
คุณลักษณะ “restrictedRule” ของคลาส “AccessRight”	restrictedRule	เป็นเงื่อนไขที่เป็นข้อห้ามในการให้อำนาจแก่ผู้ใช้งาน
คุณลักษณะ “copyFlag” ของคลาส “AccessRight”	copyFlag	เป็นลักษณะของการอนุญาตให้คัดลอกสิทธิ์ของผู้ใช้งานดังกล่าวได้

ตารางที่ ค.3 การประยุกต์ใช้ยูเอ็มแอลเซคเอสพีในแบบรูปความมั่นคงหลายระดับ

ชื่อแบบรูปความมั่นคง	ความมั่นคงหลายระดับ
กลุ่มแบบรูปความมั่นคง	แบบจำลองการควบคุมการเข้าถึง
คำอธิบาย	เป็นแบบรูปที่เสนอการกำหนดสิทธิ์ของผู้เข้าใช้ทรัพยากรในระบบตามระดับการเข้าถึงของผู้เข้าใช้ทรัพยากรและทรัพยากร

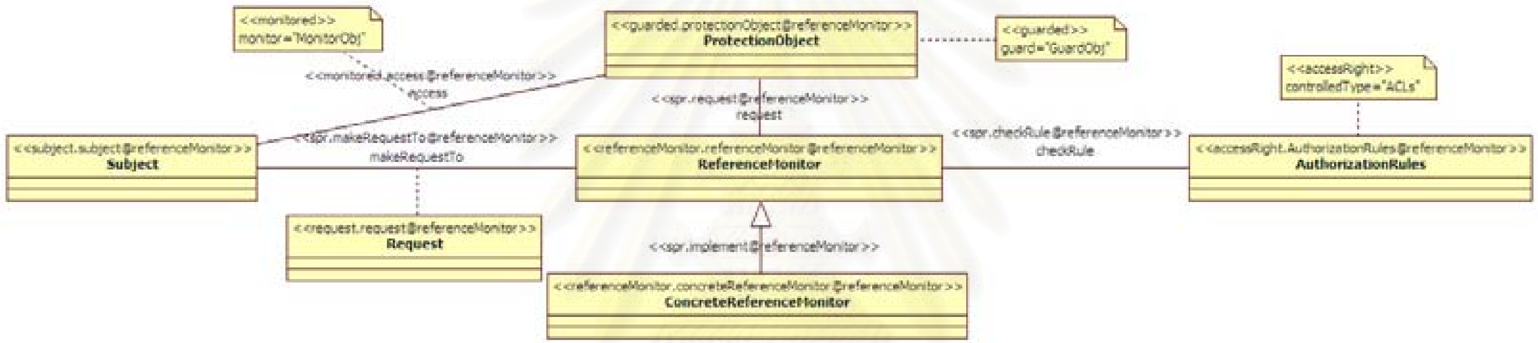
แผนภาพคลาสของแบบรูปความมั่นคงที่ประยุกต์ใช้ยูเอ็มแอลเซคเอสพี

องค์ประกอบแบบจำลอง	แม่พิมพ์ต้นแบบที่ประยุกต์ใช้	คำอธิบาย
คลาส "Subject"	subject	เป็นคลาสที่เข้าใช้ทรัพยากร
คลาส "SubjectCategory"	spc	เป็นกลุ่มของผู้เข้าใช้ทรัพยากร
คลาส "ProtectionObject"	guarded	เป็นทรัพยากรที่ถูกควบคุมการเข้าถึง จะมีการกำหนดอ็อบเจกต์ที่ควบคุมการเข้าถึงในป้ายระบุ "guard"
คลาส "ProtectionObjectCategory"	spc	เป็นกลุ่มของทรัพยากร
คลาส "TrustedProcess"	process (จากองค์ประกอบมาตรฐานของยูเอ็มแอล) และ spc	เป็นกระบวนการที่ควบคุมการกำหนดระดับการเข้าถึงของผู้เข้าใช้ทรัพยากรและทรัพยากร
คุณลักษณะ "clearanceLevel" ของคลาส "Subject"	accessLevel	เป็นระดับการเข้าถึงของผู้เข้าใช้ทรัพยากร จะมีการกำหนดอ็อบเจกต์ที่เป็นผู้กำหนดค่าในป้ายระบุ "assign"
คุณลักษณะ "classificationLevel" ของคลาส "ClearanceLevel"	guardLevel	เป็นระดับความปลอดภัยของทรัพยากร จะมีการกำหนดอ็อบเจกต์ที่เป็นผู้กำหนดค่าในป้ายระบุ "assign"

ตารางที่ ค.4 การประยุกต์ใช้ยูเอ็มแอลเซคเอสพีในแบบรูปการเฝ้าสังเกตเชิงอ้างอิง

ชื่อแบบรูปความมั่นคง	การเฝ้าสังเกตเชิงอ้างอิง
กลุ่มแบบรูปความมั่นคง	แบบจำลองการควบคุมการเข้าถึง
คำอธิบาย	เป็นแบบรูปที่เสนอการตรวจสอบการร้องขอใช้ทรัพยากรในระบบของผู้ใช้งาน

แผนภาพคลาสของแบบรูปความมั่นคงที่ประยุกต์ใช้ยูเอ็มแอลเซคเอสพี



องค์ประกอบแบบจำลอง	แม่พิมพ์ต้นแบบที่ประยุกต์ใช้	คำอธิบาย
คลาส "Subject"	subject	เป็นคลาสที่เข้าใช้ทรัพยากร
คลาส "Request"	request	เป็นคำร้องขอใช้ทรัพยากร
คลาส "ProtectionObject"	guarded	เป็นทรัพยากรที่ถูกควบคุมการเข้าถึง จะมีการกำหนดอ็อบเจกต์ที่ควบคุมการเข้าถึงในป้ายระบุ "guard"
คลาส "ReferenceMonitor"	referenceMonitor	เป็นองค์ประกอบที่ตรวจสอบการร้องขอใช้ทรัพยากร
คลาส "ConcreteReferenceMonitor"	referenceMonitor	เป็นองค์ประกอบที่ตรวจสอบการร้องขอใช้ทรัพยากรที่มีลักษณะเฉพาะ
คลาส "AuthorizationRules"	accessRight	เป็นองค์ประกอบที่ควบคุมการเข้าถึงทรัพยากร จะมีการกำหนดประเภทขององค์ประกอบที่ควบคุมการเข้าถึงทรัพยากรในป้ายระบุ "controlledType"
ความสัมพันธ์ "access"	monitored	เป็นการเชื่อมโยงที่มีการตรวจสอบการร้องขอใช้ทรัพยากร จะมีการกำหนดอ็อบเจกต์ที่ตรวจสอบคำร้องขอในป้ายระบุ "monitor"

ตารางที่ ค.5 การประยุกต์ใช้ยูเอ็มแอลเซคเอสพีในแบบรูปจุดเข้าระบบเดี่ยว

ชื่อแบบรูปความมั่นคง	จุดเข้าระบบเดี่ยว
กลุ่มแบบรูปความมั่นคง	สถาปัตยกรรมการควบคุมการเข้าถึงระบบ
คำอธิบาย	เป็นแบบรูปที่เสนอการควบคุมการเข้าถึงระบบ โดยการกำหนดให้มีช่องทางเดียวในการเข้าถึงระบบเท่านั้น

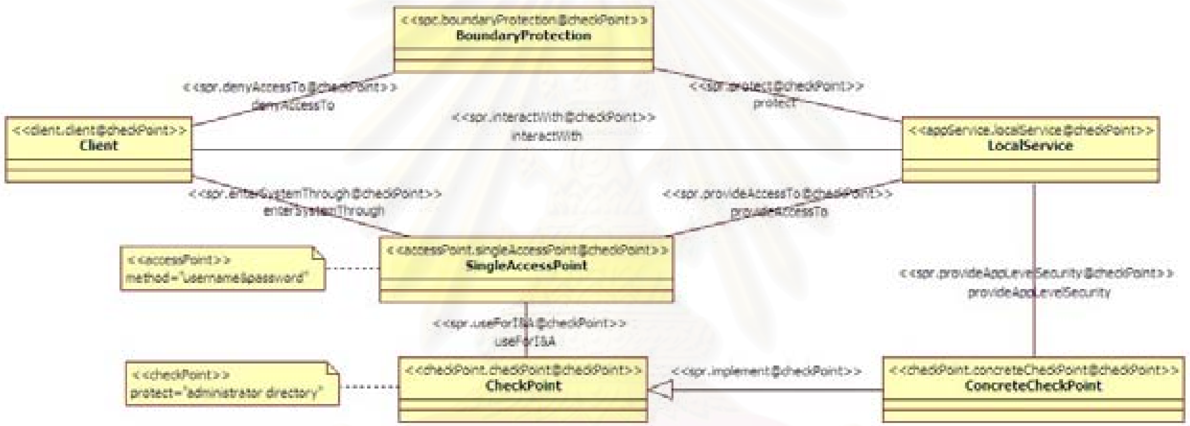
แผนภาพคลาสของแบบรูปความมั่นคงที่ประยุกต์ใช้ยูเอ็มแอลเซคเอสพี

องค์ประกอบแบบจำลอง	แม่พิมพ์ต้นแบบที่ประยุกต์ใช้	คำอธิบาย
คลาส “Client”	client	เป็นผู้เข้าใช้งานจากภายนอกระบบ
คลาส “BoundaryProtection”	spc	เป็นองค์ประกอบที่จำกัดขอบเขตของการเข้าถึงระบบ
คลาส “SingleAccessPoint”	accessPoint	เป็นจุดเข้าระบบ จะมีการกำหนดวิธีในการเข้าสู่ระบบในป้ายระบุ “method”
คลาส “LocalService”	appService	เป็นบริการของโปรแกรมประยุกต์ภายในระบบ

ตารางที่ ค.6 การประยุกต์ใช้ยูเอ็มแอลเซคเอสพีในแบบรูปจุดตรวจสอบ

ชื่อแบบรูปความมั่นคง	จุดตรวจสอบ
กลุ่มแบบรูปความมั่นคง	สถาปัตยกรรมการควบคุมการเข้าถึงระบบ
คำอธิบาย	เป็นแบบรูปที่เสนอการควบคุมการเข้าถึงของระบบ โดยการกำหนดจุดตรวจสอบที่ใช้ในการควบคุมการเข้าถึงบริการของระบบ

แผนภาพคลาสของแบบรูปความมั่นคงที่ประยุกต์ใช้ยูเอ็มแอลเซคเอสพี

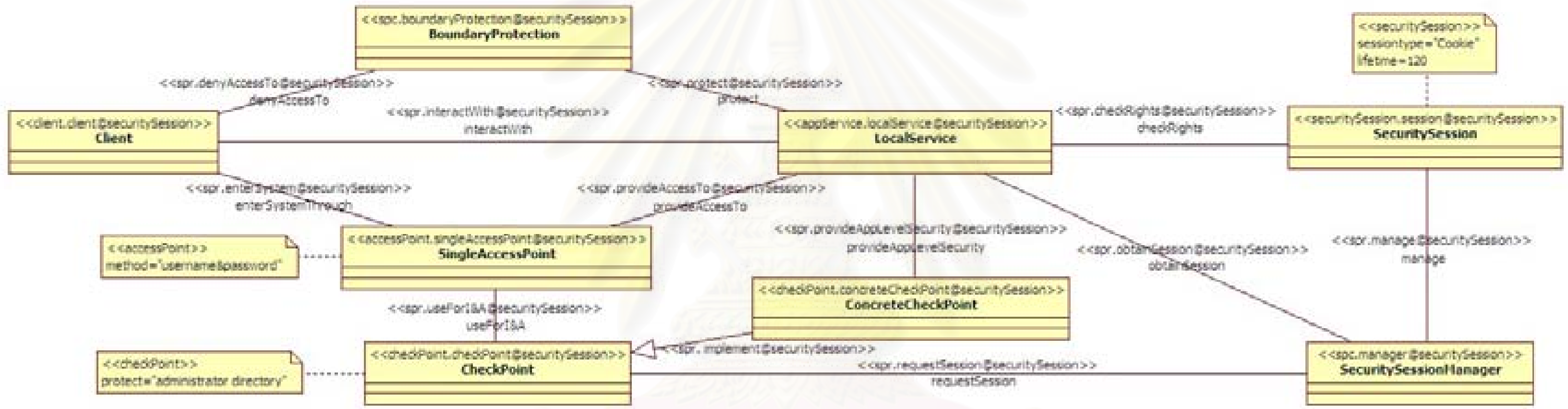


องค์ประกอบแบบจำลอง	แม่พิมพ์ต้นแบบที่ประยุกต์ใช้	คำอธิบาย
คลาส “Client”	client	เป็นผู้เข้าใช้งานจากภายนอกระบบ
คลาส “BoundaryProtection”	spc	เป็นองค์ประกอบที่จำกัดขอบเขตของการเข้าถึงระบบ
คลาส “SingleAccessPoint”	accessPoint	เป็นจุดเข้าระบบ จะมีการกำหนดวิธีในการเข้าสู่ระบบในป้ายระบุ “method”
คลาส “LocalService”	appService	เป็นบริการของโปรแกรมประยุกต์ภายในระบบ
คลาส “CheckPoint”	checkPoint	เป็นจุดตรวจสอบผู้ใช้งานจากภายนอกระบบ จะมีการกำหนดบริการที่ต้องมีการตรวจสอบจากจุดตรวจสอบในป้ายระบุ “protect”
คลาส “ConcreteCheckPoint”	checkPoint	เป็นจุดตรวจสอบการเข้าใช้บริการที่มีลักษณะเฉพาะ

ตารางที่ ค.7 การประยุกต์ใช้ยูเอ็มแอลเซคเอสพีในแบบรูปเซสชันทางความมั่นคง

ชื่อแบบรูปความมั่นคง	เซสชันทางความมั่นคง
กลุ่มแบบรูปความมั่นคง	สถาปัตยกรรมการควบคุมการเข้าถึงระบบ
คำอธิบาย	เป็นแบบรูปที่เสนอการควบคุมการเข้าถึงของระบบ โดยการจัดเก็บเซสชันทางความมั่นคงของผู้ใช้งาน

แผนภาพคลาสของแบบรูปความมั่นคงที่ประยุกต์ใช้ยูเอ็มแอลเซคเอสพี



องค์ประกอบแบบจำลอง	แม่พิมพ์ต้นแบบที่ประยุกต์ใช้	คำอธิบาย
คลาส “Client”	client	เป็นผู้เข้าใช้งานจากภายนอกระบบ
คลาส “BoundaryProtection”	spc	เป็นองค์ประกอบที่จำกัดขอบเขตของการเข้าถึงระบบ
คลาส “SingleAccessPoint”	accessPoint	เป็นจุดเข้าระบบ จะมีการกำหนดวิธีในการเข้าสู่ระบบในป้ายระบุ “method”
คลาส “LocalService”	appService	เป็นบริการของโปรแกรมประยุกต์ภายในระบบ
คลาส “CheckPoint”	checkPoint	เป็นจุดตรวจสอบผู้ใช้งานจากภายนอกระบบ จะมีการกำหนดบริการที่ต้องมีการตรวจสอบจากจุดตรวจสอบในป้ายระบุ “protect”
คลาส “ConcreteCheckPoint”	checkpoint	เป็นจุดตรวจสอบการเข้าใช้บริการที่มีลักษณะเฉพาะ
คลาส “SecuritySession”	securitySession	เป็นเซสชันทางความมั่นคง จะมีการกำหนดประเภทของเซสชันในป้ายระบุ “sessionType” และอายุการใช้งานในป้ายระบุ “lifetime”
คลาส “SecuritySessionManager”	spc	เป็นองค์ประกอบที่ควบคุมการใช้งานของเซสชันความมั่นคง

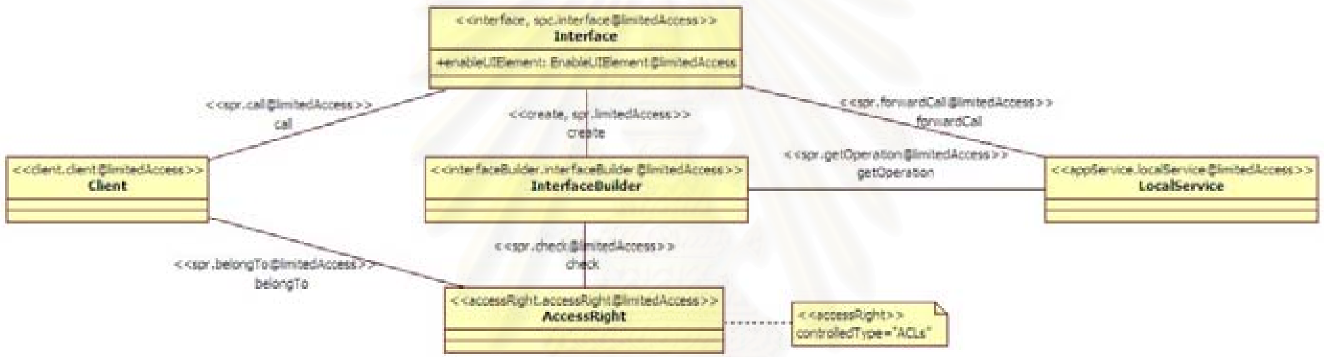
ตารางที่ ค.8 การประยุกต์ใช้ยูเอ็มแอลเซคเอสพีในแบบรูปการควบคุมการเข้าถึงด้วยการแสดงความผิดพลาด

ชื่อแบบรูปความมั่นคง	การควบคุมการเข้าถึงด้วยการแสดงความผิดพลาด	
กลุ่มแบบรูปความมั่นคง	สถาปัตยกรรมการควบคุมการเข้าถึงระบบ	
คำอธิบาย	เป็นแบบรูปที่เสนอการแสดงฟังก์ชันการทำงานทั้งหมดของระบบให้ผู้ใช้งานทราบ ซึ่งระบบควบคุมการเข้าใช้ฟังก์ชันโดยการแสดงข้อผิดพลาดให้ผู้ใช้งานทราบในกรณีที่ผู้ใช้งานเรียกใช้ฟังก์ชันที่ไม่มีสิทธิ์ในการเรียกใช้	
แผนภาพคลาสของแบบรูปความมั่นคงที่ประยุกต์ใช้ยูเอ็มแอลเซคเอสพี		
		
องค์ประกอบแบบจำลอง	แม่พิมพ์ต้นแบบที่ประยุกต์ใช้	คำอธิบาย
คลาส “Client”	client	เป็นผู้เข้าใช้งานจากภายนอกระบบ
คลาส “Interface”	interface (จากองค์ประกอบมาตรฐานของยูเอ็มแอล) และ spc	เป็นส่วนต่อประสานที่แสดงบริการในระบบ
คลาส “AccessRight”	accessRight	เป็นองค์ประกอบที่ควบคุมการเข้าถึงบริการในระบบ จะมีการกำหนดประเภทขององค์ประกอบที่ควบคุมการเข้าถึงบริการในป้ายระบุ “controlledType”
คลาส “LocalService”	appService	เป็นบริการของโปรแกรมประยุกต์ภายในระบบ
คลาส “ErrorNotification”	errorNotification	เป็นองค์ประกอบที่แจ้งข้อผิดพลาดที่เกิดขึ้นจากผู้ใช้งาน

ตารางที่ ค.9 การประยุกต์ใช้ยูเอ็มแอลเซคเอสพีในแบบรูปการจำกัดการเข้าถึง

ชื่อแบบรูปความมั่นคง	การจำกัดการเข้าถึง
กลุ่มแบบรูปความมั่นคง	สถาปัตยกรรมการควบคุมการเข้าถึงระบบ
คำอธิบาย	เป็นแบบรูปที่เสนอการแสดงส่วนต่อประสานที่ใช้ในการเข้าถึงที่แตกต่างกัน สำหรับผู้ใช้งานที่มีอำนาจในการเข้าถึงที่ต่างกัน

แผนภาพคลาสของแบบรูปความมั่นคงที่ประยุกต์ใช้ยูเอ็มแอลเซคเอสพี

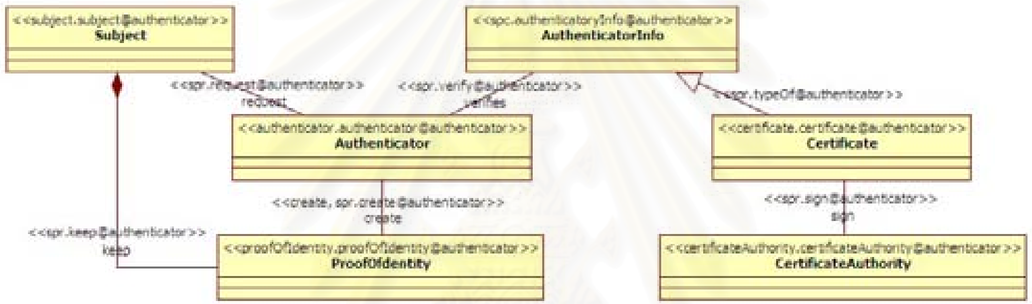


องค์ประกอบแบบจำลอง	แม่พิมพ์ต้นแบบที่ประยุกต์ใช้	คำอธิบาย
คลาส “Client”	client	เป็นผู้เข้าใช้งานจากภายนอกระบบ
คลาส “Interface”	interface (จากองค์ประกอบมาตรฐานของยูเอ็มแอล) และ spc	เป็นส่วนต่อประสานที่แสดงบริการในระบบ
คลาส “AccessRight”	accessRight	เป็นคลาสที่ควบคุมการสร้างส่วนต่อประสานให้เป็นไปตามสิทธิ์ในการใช้บริการของผู้ใช้งาน จะมีการกำหนดประเภทขององค์ประกอบที่ควบคุมการสร้างส่วนต่อประสานในป้ายระบุ “controlledType”
คลาส “InterfaceBuilder”	interfaceBuilder	เป็นคลาสที่สร้างส่วนต่อประสานตามสิทธิ์ในการใช้บริการของผู้ใช้งาน
คลาส “LocalService”	appService	เป็นบริการของโปรแกรมประยุกต์ภายในระบบ
คุณลักษณะ “enableUIElement”	enableUIElement	เป็นคุณลักษณะที่แสดงสถานะของการมองเห็นในแต่ละองค์ประกอบของส่วนต่อประสาน
ความสัมพันธ์ “create”	create (จากองค์ประกอบมาตรฐานของยูเอ็มแอล) และ spr	เป็นความสัมพันธ์ที่แสดงถึงการสร้างส่วนต่อประสานของคลาส “InterfaceBuilder”

ตารางที่ ค.10 การประยุกต์ใช้ยูเอ็มแอลเซคเอสพีในแบบรูปองค์ประกอบพิสูจน์ตัวตน

ชื่อแบบรูปความมั่นคง	องค์ประกอบพิสูจน์ตัวตน
กลุ่มแบบรูปความมั่นคง	การควบคุมการเข้าถึงระบบปฏิบัติการ
คำอธิบาย	เป็นแบบรูปที่เสนอการใช้องค์ประกอบพิสูจน์ตัวตนในการระบุตัวตนของผู้ใช้งานในระบบปฏิบัติการ

แผนภาพคลาสของแบบรูปความมั่นคงที่ประยุกต์ใช้ยูเอ็มแอลเซคเอสพี

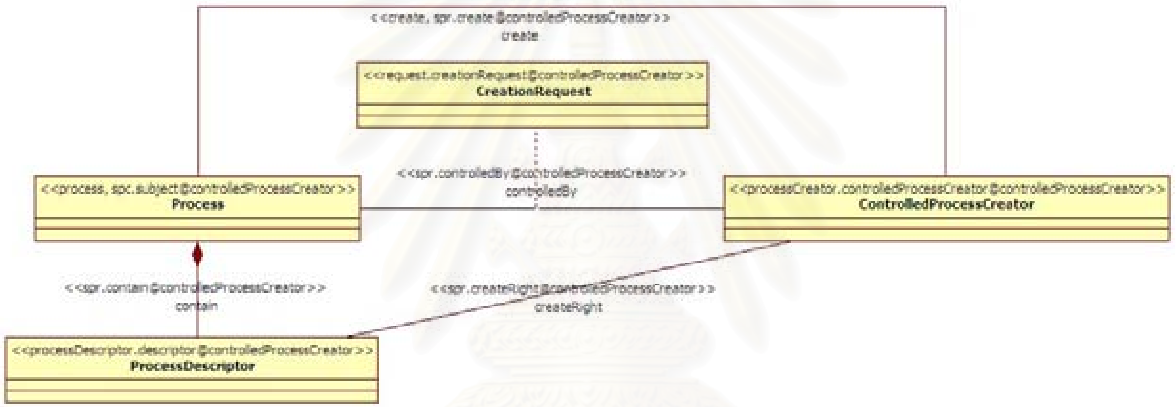


องค์ประกอบแบบจำลอง	แม่พิมพ์ต้นแบบที่ประยุกต์ใช้	คำอธิบาย
คลาส “Subject”	subject	เป็นคลาสที่ต้องการเข้าใช้ทรัพยากรในระบบปฏิบัติการ
คลาส “Authenticator”	authenticator	เป็นองค์ประกอบที่ทำการตรวจสอบตัวตนของผู้ใช้งานก่อนทำการให้อำนาจแก่ผู้ใช้งานในระบบปฏิบัติการ
คลาส “ProofOfIdentity”	proofOfIdentity	เป็นองค์ประกอบที่ใช้ในการแสดงตัวตนของผู้ใช้งานในระบบปฏิบัติการ
คลาส “AuthenticatorInfo”	spc	เป็นข้อมูลที่ใช้ในการระบุตัวตนของผู้ใช้งานในระบบปฏิบัติการ
คลาส “Certificate”	certificate	เป็นใบรับรองในการระบุตัวตนในระบบปฏิบัติการ
คลาส “CertificateAuthority”	certificateAuthority	เป็นผู้ให้ใบรับรองในการระบุตัวตนในระบบปฏิบัติการ
ความสัมพันธ์ “create”	create (จากองค์ประกอบมาตรฐานของยูเอ็มแอล) และ spr	เป็นความสัมพันธ์ที่แสดงถึงการสร้างองค์ประกอบที่ใช้ในการแสดงตัวตนของคลาส “Authenticator”

ตารางที่ ค.11 การประยุกต์ใช้ยูเอ็มแอลเซคเอสพีในแบบรูปการควบคุมการสร้างกระบวนการ

ชื่อแบบรูปความมั่นคง	การควบคุมการสร้างกระบวนการ
กลุ่มแบบรูปความมั่นคง	การควบคุมการเข้าถึงระบบปฏิบัติการ
คำอธิบาย	เป็นแบบรูปที่เสนอการกำหนดสิทธิ์ให้กับกระบวนการที่เกิดขึ้นใหม่ในระบบปฏิบัติการ

แผนภาพคลาสของแบบรูปความมั่นคงที่ประยุกต์ใช้ยูเอ็มแอลเซคเอสพี



องค์ประกอบแบบจำลอง	แม่พิมพ์ต้นแบบที่ประยุกต์ใช้	คำอธิบาย
คลาส “Process”	process (จากองค์ประกอบมาตรฐานของยูเอ็มแอล) และ spc	เป็นกระบวนการในระบบปฏิบัติการ
คลาส “ControlledProcessCreator”	processCreator	เป็นองค์ประกอบที่ควบคุมการสร้างกระบวนการใหม่ในระบบปฏิบัติการ
คลาส “CreationRequest”	request	เป็นคำร้องขอของระบบปฏิบัติการ
คลาส “ProcessDescriptor”	processDescriptor	เป็นองค์ประกอบที่จัดเก็บสิทธิ์ของกระบวนการในระบบปฏิบัติการ
ความสัมพันธ์ “create”	create (จากองค์ประกอบมาตรฐานของยูเอ็มแอล) และ spr	เป็นความสัมพันธ์ที่แสดงถึงการสร้างกระบวนการของคลาส “ControlledProcessCreator”

ตารางที่ ค.12 การประยุกต์ใช้ยูเอ็มแอลเซคเอสพีในแบบรูปการควบคุมการสร้างอ็อบเจกต์

ชื่อแบบรูปความมั่นคง	การควบคุมการสร้างอ็อบเจกต์
กลุ่มแบบรูปความมั่นคง	การควบคุมการเข้าถึงระบบปฏิบัติการ
คำอธิบาย	เป็นแบบรูปที่เสนอการกำหนดสิทธิ์ให้กับอ็อบเจกต์ที่เกิดขึ้นใหม่ในระบบปฏิบัติการ

แผนภาพคลาสของแบบรูปความมั่นคงที่ประยุกต์ใช้ยูเอ็มแอลเซคเอสพี

องค์ประกอบแบบจำลอง	แม่พิมพ์ต้นแบบที่ประยุกต์ใช้	คำอธิบาย
คลาส “Process”	process (จากองค์ประกอบมาตรฐานของยูเอ็มแอล) และ spc	เป็นกระบวนการในระบบปฏิบัติการ
คลาส “CreationRequest”	request	เป็นคำร้องขอในการสร้างอ็อบเจกต์ของระบบปฏิบัติการ
คลาส “ObjectFactory”	objectFactory	เป็นองค์ประกอบที่ควบคุมการสร้างอ็อบเจกต์ของระบบปฏิบัติการ
คลาส “Object”	guarded	เป็นอ็อบเจกต์ที่ถูกสร้างขึ้นในระบบปฏิบัติการ จะมีการกำหนดอ็อบเจกต์ที่ควบคุมการเข้าถึงในป้ายระบุ “guard”
คลาส “Subject”	subject	เป็นผู้เข้าใช้อ็อบเจกต์ที่ถูกสร้างขึ้นในระบบปฏิบัติการ

ตารางที่ ค.12 การประยุกต์ใช้ยูเอ็มแอลเซคเอสพีในแบบรูปการควบคุมการสร้างอ็อบเจกต์ (ต่อ)

องค์ประกอบแบบจำลอง	แม่พิมพ์ต้นแบบที่ประยุกต์ใช้	คำอธิบาย
คลาส “AccessRight”	accessRight	เป็นองค์ประกอบที่ควบคุมการเข้าถึงอ็อบเจกต์ในระบบปฏิบัติการ จะมีการกำหนดประเภทขององค์ประกอบที่ควบคุมการเข้าถึงอ็อบเจกต์ในป้ายระบุ “controlledType”
ความสัมพันธ์ ”create”	create (จากองค์ประกอบมาตรฐานของยูเอ็มแอล) และ spr	เป็นความสัมพันธ์ที่แสดงถึงการสร้างอ็อบเจกต์ของคลาส “ObjectFactory”

ตารางที่ ค.13 การประยุกต์ใช้ยูเอ็มแอลเซคเอสพีในแบบรูปการตรวจสอบการเข้าถึงอ็อบเจกต์

ชื่อแบบรูปความมั่นคง	การตรวจสอบการเข้าถึงอ็อบเจกต์
กลุ่มแบบรูปความมั่นคง	การควบคุมการเข้าถึงระบบปฏิบัติการ
คำอธิบาย	เป็นแบบรูปที่เสนอการตรวจสอบการเข้าถึงอ็อบเจกต์ในระบบปฏิบัติการ

แผนภาพคลาสของแบบรูปความมั่นคงที่ประยุกต์ใช้ยูเอ็มแอลเซคเอสพี

องค์ประกอบแบบจำลอง	แม่พิมพ์ต้นแบบที่ประยุกต์ใช้	คำอธิบาย
คลาส “Process”	process (จากองค์ประกอบมาตรฐานของยูเอ็มแอล) และ spc	เป็นกระบวนการที่เข้าใช้อ็อบเจกต์ในระบบปฏิบัติการ
คลาส “AccessRequest”	request	เป็นคำร้องขอในการเข้าใช้อ็อบเจกต์ในระบบปฏิบัติการ
คลาส “ReferenceMonitor”	referenceMonitor	เป็นองค์ประกอบที่ตรวจสอบการร้องขอใช้อ็อบเจกต์ในระบบปฏิบัติการ
คลาส “AccessRight”	accessRight	เป็นองค์ประกอบที่ควบคุมการเข้าถึงอ็อบเจกต์ของกระบวนการในระบบปฏิบัติการ จะมีการกำหนดประเภทขององค์ประกอบที่ควบคุมการเข้าถึงอ็อบเจกต์ในป้ายระบุ “controlledType”
คลาส “Object”	guarded	เป็นอ็อบเจกต์ที่ถูกควบคุมในระบบปฏิบัติการ จะมีการกำหนดอ็อบเจกต์ที่ควบคุมการเข้าถึงในป้ายระบุ “guard”
ความสัมพันธ์ “access”	monitored	เป็นการเชื่อมโยงที่มีการตรวจสอบการร้องขอใช้อ็อบเจกต์ในระบบปฏิบัติการ จะมีการกำหนดอ็อบเจกต์ที่ตรวจสอบคำร้องขอในป้ายระบุ “monitor”

ตารางที่ ค.14 การประยุกต์ใช้ยูเอ็มแอลเซคเอสพีในแบบรูปการควบคุมหน่วยความจำเสมือน

ชื่อแบบรูปความมั่นคง	การควบคุมหน่วยความจำเสมือน
กลุ่มแบบรูปความมั่นคง	การควบคุมการเข้าถึงระบบปฏิบัติการ
คำอธิบาย	เป็นแบบรูปที่เสนอการควบคุมการเข้าถึงหน่วยความจำเสมือนในระบบปฏิบัติการ

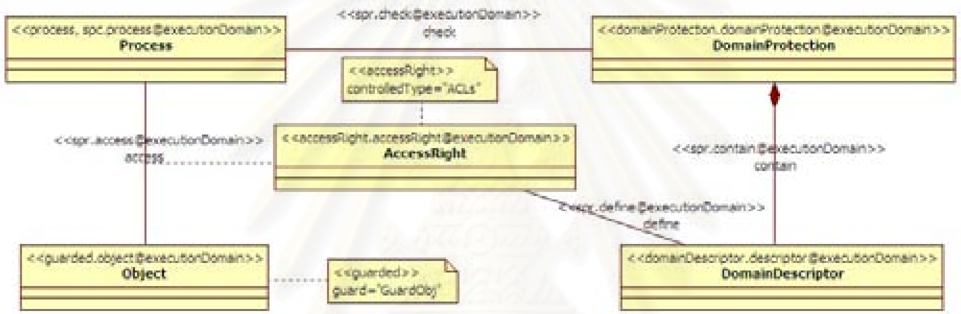
แผนภาพคลาสของแบบรูปความมั่นคงที่ประยุกต์ใช้ยูเอ็มแอลเซคเอสพี

องค์ประกอบแบบจำลอง	แม่พิมพ์ต้นแบบที่ประยุกต์ใช้	คำอธิบาย
คลาส “Process”	process (จากองค์ประกอบมาตรฐานของยูเอ็มแอล) และ spc	เป็นกระบวนการที่เข้าใช้หน่วยความจำเสมือนในระบบปฏิบัติการ
คลาส “ProcessDescriptor”	processDescriptor	เป็นองค์ประกอบที่จัดเก็บสิทธิ์ของกระบวนการในระบบปฏิบัติการ
คลาส “VirtualAddressSpace”	vas	เป็นหน่วยความจำเสมือนในระบบปฏิบัติการ
คลาส “Segment”	spc	เป็นเซกเมนต์ของหน่วยความจำเสมือนในระบบปฏิบัติการ
คุณลักษณะ “address” ของคลาส “Segment”	vasAddress	เป็นที่อยู่ของเซกเมนต์
คุณลักษณะ “size” ของคลาส “Segment”	vasSize	เป็นขนาดของเซกเมนต์
คุณลักษณะ “accessAddress” ของคลาส “ProcessDescriptor”	vasAddress	เป็นที่อยู่ของเซกเมนต์ที่เข้าถึง
คุณลักษณะ “limitPageSize” ของคลาส “ProcessDescriptor”	vasSize	เป็นขนาดของเซกเมนต์ที่ถูกจำกัด
คุณลักษณะ “accessType” ของคลาส “ProcessDescriptor”	accessType	เป็นลักษณะของการเข้าถึงเซกต์เมนต์

ตารางที่ ค.15 การประยุกต์ใช้ยูเอ็มแอลเซคเอสพีในแบบรูปการควบคุมขอบเขตกระทำการ

ชื่อแบบรูปความมั่นคง	การควบคุมขอบเขตกระทำการ
กลุ่มแบบรูปความมั่นคง	การควบคุมการเข้าถึงระบบปฏิบัติการ
คำอธิบาย	เป็นแบบรูปที่เสนอการควบคุมขอบเขตกระทำการของกระบวนการในระบบปฏิบัติการ

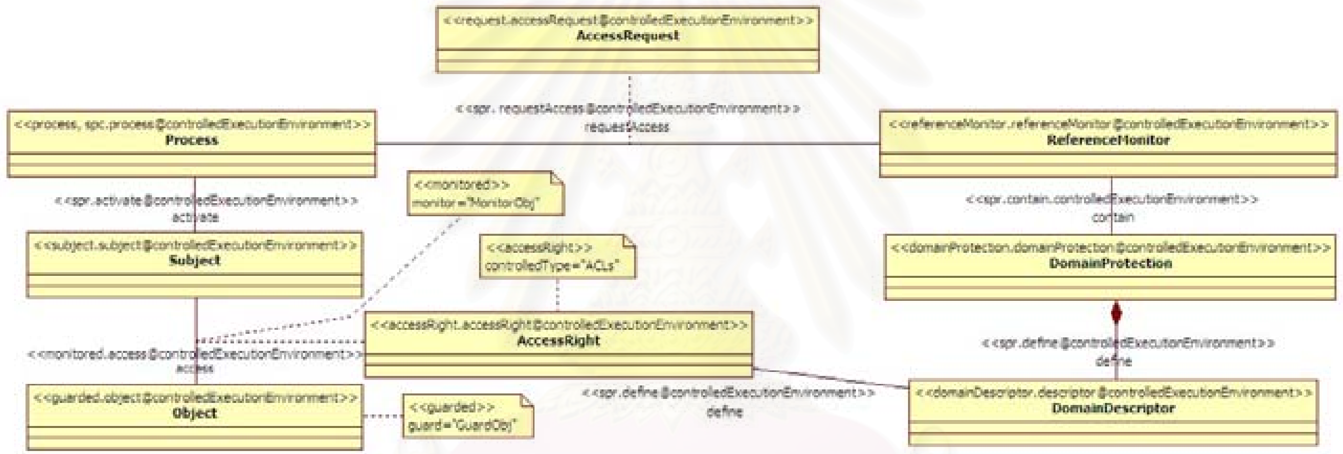
แผนภาพคลาสของแบบรูปความมั่นคงที่ประยุกต์ใช้ยูเอ็มแอลเซคเอสพี



องค์ประกอบแบบจำลอง	แม่พิมพ์ต้นแบบที่ประยุกต์ใช้	คำอธิบาย
คลาส “Process”	process (จากองค์ประกอบมาตรฐานของยูเอ็มแอล) และ spc	เป็นกระบวนการที่เข้าใช้อ็อบเจกต์ที่อยู่ต่างโดเมนกันของระบบปฏิบัติการ
คลาส “DomainProtection”	domainProtection	เป็นองค์ประกอบที่ตรวจสอบการเปลี่ยนโดเมนภายในระบบปฏิบัติการ
คลาส “DomainDescriptor”	domainDescriptor	เป็นองค์ประกอบที่จัดเก็บสิทธิ์ของกระบวนการในการเข้าใช้อ็อบเจกต์ในโดเมนที่กำหนด
คลาส “AccessRight”	accessRight	เป็นองค์ประกอบที่ควบคุมการเข้าถึงอ็อบเจกต์ของกระบวนการในระบบปฏิบัติการ จะมีการกำหนดประเภทของการควบคุมการเข้าถึงอ็อบเจกต์ในป้ายระบุ “controlledType”
คลาส “Object”	guarded	เป็นอ็อบเจกต์ที่อยู่ในแต่ละโดเมนของระบบปฏิบัติการ จะมีการกำหนดอ็อบเจกต์ที่ควบคุมการเข้าถึงในป้ายระบุ “guard”

ตารางที่ ค.16 การประยุกต์ใช้ยูเอ็มแอลเซคเอสพีในแบบรูปการควบคุมสิ่งแวดล้อมที่กระทำการ

ชื่อแบบรูปความมั่นคง	การควบคุมสิ่งแวดล้อมที่กระทำการ
กลุ่มแบบรูปความมั่นคง	การควบคุมการเข้าถึงระบบปฏิบัติการ
คำอธิบาย	เป็นแบบรูปที่เสนอการควบคุมขอบเขตการกระทำการของกระบวนการและการควบคุมการเข้าถึงอ็อบเจกต์ในระบบปฏิบัติการ
แผนภาพคลาสของแบบรูปความมั่นคงที่ประยุกต์ใช้ยูเอ็มแอลเซคเอสพี	



องค์ประกอบแบบจำลอง	แม่พิมพ์ต้นแบบที่ประยุกต์ใช้	คำอธิบายของการประยุกต์ใช้
คลาส “Process”	process (จากองค์ประกอบมาตรฐานของยูเอ็มแอล) และ spc	เป็นกระบวนการที่กระตุ้นให้องค์ประกอบอื่นทำงานในระบบปฏิบัติการ
คลาส “AccessRequest”	request	เป็นคำร้องขอในการเข้าใช้อ็อบเจกต์ในระบบปฏิบัติการ
คลาส “ReferenceMonitor”	referenceMonitor	เป็นองค์ประกอบที่ตรวจสอบการร้องขอใช้อ็อบเจกต์ในระบบปฏิบัติการ
คลาส “DomainProtection”	domainProtection	เป็นองค์ประกอบที่ตรวจสอบการเปลี่ยนโดเมนภายในระบบปฏิบัติการ
คลาส “DomainDescriptor”	domainDescriptor	เป็นองค์ประกอบที่จัดเก็บสิทธิ์ของกระบวนการในการเข้าใช้อ็อบเจกต์ในโดเมนที่กำหนด
คลาส “Subject”	subject	เป็นผู้เข้าใช้อ็อบเจกต์ที่ถูกสร้างขึ้นในระบบปฏิบัติการ
คลาส “AccessRight”	accessRight	เป็นองค์ประกอบที่ควบคุมการเข้าถึงอ็อบเจกต์ของกระบวนการในระบบปฏิบัติการ จะมีการกำหนดประเภทของการควบคุมการเข้าถึงอ็อบเจกต์ในป้ายระบุ “controlledType”

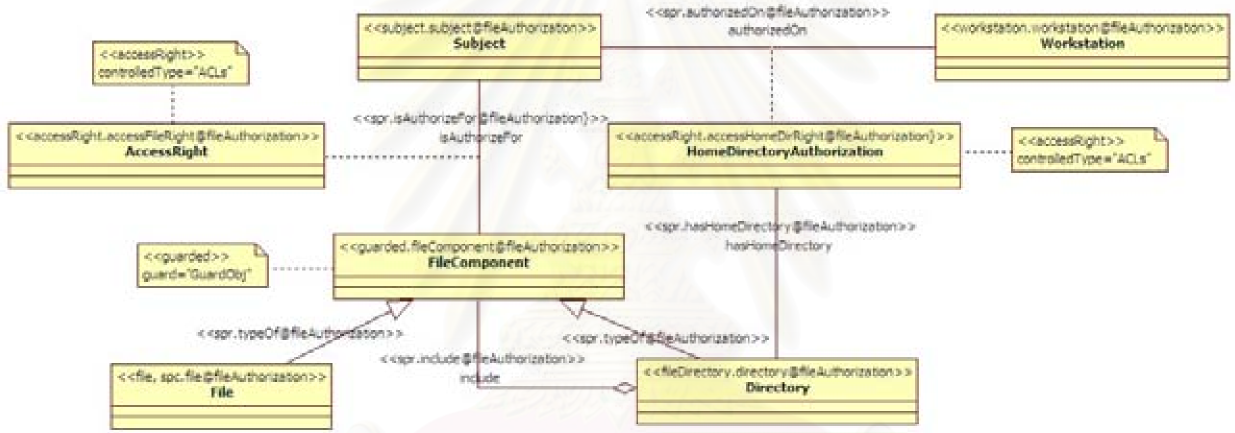
ตารางที่ ค.16 การประยุกต์ใช้ยูเอ็มแอลเซคเอสพีในแบบรูปการควบคุมสิ่งแวดล้อมที่กระทำการ (ต่อ)

องค์ประกอบแบบจำลอง	แม่พิมพ์ต้นแบบที่ประยุกต์ใช้	คำอธิบายของการประยุกต์ใช้
คลาส “Object”	guarded	เป็นอ็อบเจกต์ที่อยู่ในแต่ละโดเมนของระบบปฏิบัติการ จะมีการกำหนดอ็อบเจกต์ที่ควบคุมการเข้าถึงในป้ายระบุ “guard”
ความสัมพันธ์ “access”	monitored	เป็นการเชื่อมโยงที่มีการตรวจสอบการร้องขอใช้อ็อบเจกต์ในระบบปฏิบัติการ จะมีการกำหนดอ็อบเจกต์ที่ตรวจสอบคำร้องขอในป้ายระบุ “monitor”

ตารางที่ ค.17 การประยุกต์ใช้ยูเอ็มแอลเซคเอสพีในแบบรูปการให้อำนาจในแฟ้มข้อมูล

ชื่อแบบรูปความมั่นคง	การให้อำนาจในแฟ้มข้อมูล
กลุ่มแบบรูปความมั่นคง	การควบคุมการเข้าถึงระบบปฏิบัติการ
คำอธิบาย	เป็นแบบรูปที่เสนอการควบคุมการเข้าถึงแฟ้มข้อมูลในระบบปฏิบัติการ

แผนภาพคลาสของแบบรูปความมั่นคงที่ประยุกต์ใช้ยูเอ็มแอลเซคเอสพี

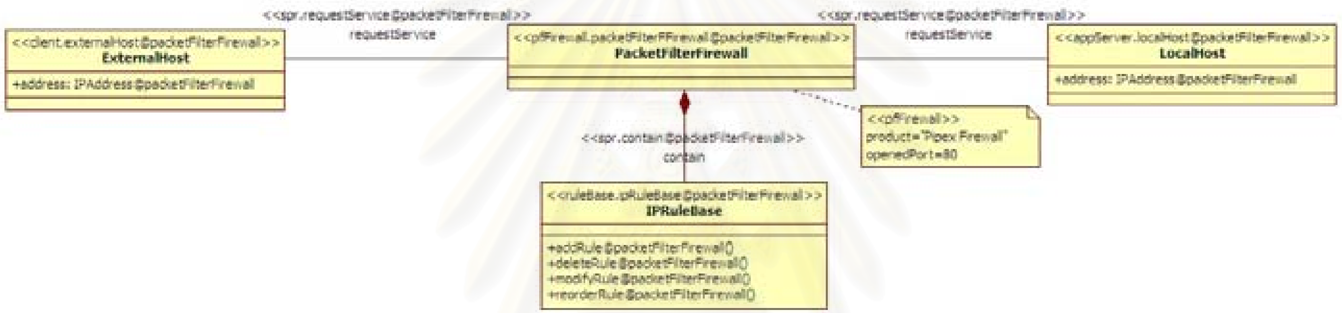


องค์ประกอบแบบจำลอง	แม่พิมพ์ต้นแบบที่ประยุกต์ใช้	คำอธิบาย
คลาส “Subject”	subject	เป็นผู้เข้าใช้แฟ้มข้อมูลในระบบปฏิบัติการ
คลาส “HomeDirectoryAuthorization”	accessRight	เป็นองค์ประกอบที่ควบคุมการเข้าถึงสารบบของผู้ใช้งานในระบบปฏิบัติการ จะมีการกำหนดประเภทขององค์ประกอบที่ควบคุมการเข้าถึงสารบบของผู้ใช้งานในป้ายระบุ “controlledType”
คลาส “Workstation”	workstation	เป็นสถานีงานในระบบปฏิบัติการ จะมีการกำหนดระบบปฏิบัติการของสถานีงานในป้ายระบุ “osType”
คลาส “AccessRight”	accessRight	เป็นองค์ประกอบที่ควบคุมการเข้าถึงแฟ้มข้อมูลและสารบบในระบบปฏิบัติการ จะมีการกำหนดประเภทของการควบคุมการเข้าถึงแฟ้มข้อมูลในป้ายระบุ “controlledType”
คลาส “FileComponent”	guarded	เป็นองค์ประกอบที่รวบรวมแฟ้มข้อมูลและสารบบในแบบรูป จะมีการกำหนดองค์ประกอบที่ควบคุมในป้ายระบุ “guard”
คลาส “File”	file (จากองค์ประกอบมาตรฐานของยูเอ็มแอล) และ spc	เป็นแฟ้มข้อมูลในระบบปฏิบัติการ
คลาส “Directory”	fileDirectory	เป็นสารบบในระบบปฏิบัติการ

ตารางที่ ค.18 การประยุกต์ใช้ยูเอ็มแอลเซคเอสพีในแบบรูปไฟร์วอลล์สำหรับการกรองแพ็คเกจ

ชื่อแบบรูปความมั่นคง	ไฟร์วอลล์สำหรับการกรองแพ็คเกจ
กลุ่มแบบรูปความมั่นคง	สถาปัตยกรรมไฟร์วอลล์
คำอธิบาย	เป็นแบบรูปที่เสนอไฟร์วอลล์ที่ควบคุมการรับส่งแพ็คเกจในระดับไอพี

แผนภาพคลาสของแบบรูปความมั่นคงที่ประยุกต์ใช้ยูเอ็มแอลเซคเอสพี

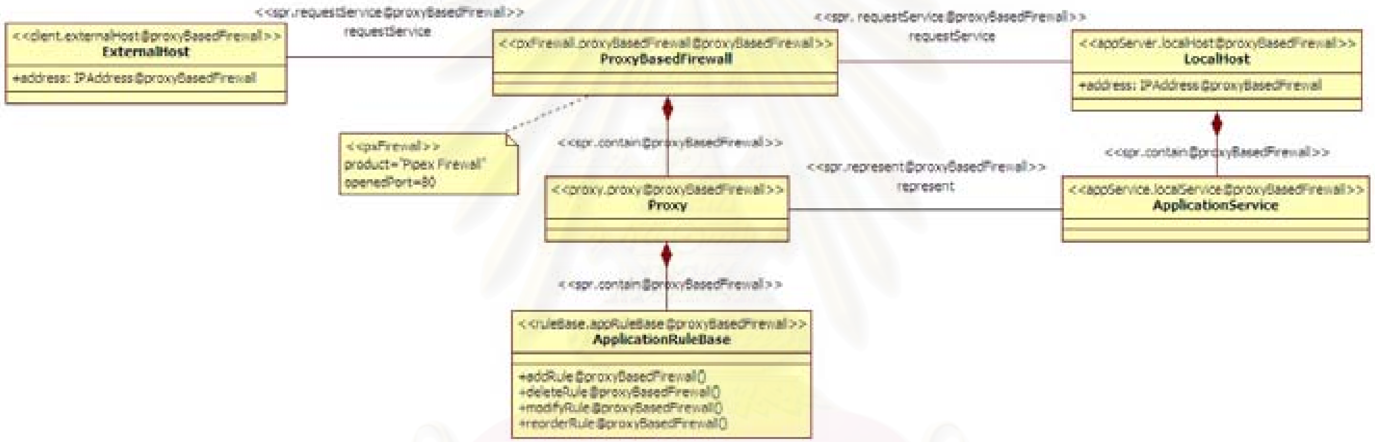


องค์ประกอบแบบจำลอง	แม่พิมพ์ต้นแบบที่ประยุกต์ใช้	คำอธิบาย
คลาส “ExternalHost”	client	เป็นผู้เข้าใช้ระบบจากภายนอก
คลาส “PacketFilterFirewall”	pfFirewall	เป็นไฟร์วอลล์สำหรับการกรองแพ็คเกจ จะมีการกำหนดผลิตภัณฑ์ไฟร์วอลล์ในป้ายระบุ “product” และหมายเลขพอร์ทที่เปิดในป้ายระบุ “openedPort”
คลาส “IPRuleBase”	ruleBase	เป็นองค์ประกอบที่กรองแพ็คเกจในระดับไอพี
คลาส “LocalHost”	appServer	เป็นเครื่องบริการโปรแกรมประยุกต์ในระบบ

ตารางที่ ค.19 การประยุกต์ใช้ยูเอ็มแอลเซคเอสพีในแบบรูปไฟร์วอลล์เชิงตัวแทน

ชื่อแบบรูปความมั่นคง	ไฟร์วอลล์เชิงตัวแทน
กลุ่มแบบรูปความมั่นคง	สถาปัตยกรรมไฟร์วอลล์
คำอธิบาย	เป็นแบบรูปที่เสนอไฟร์วอลล์ที่ควบคุมการรับส่งแพ็คเกจในระดับข้อความในแพ็คเกจ

แผนภาพคลาสของแบบรูปความมั่นคงที่ประยุกต์ใช้ยูเอ็มแอลเซคเอสพี

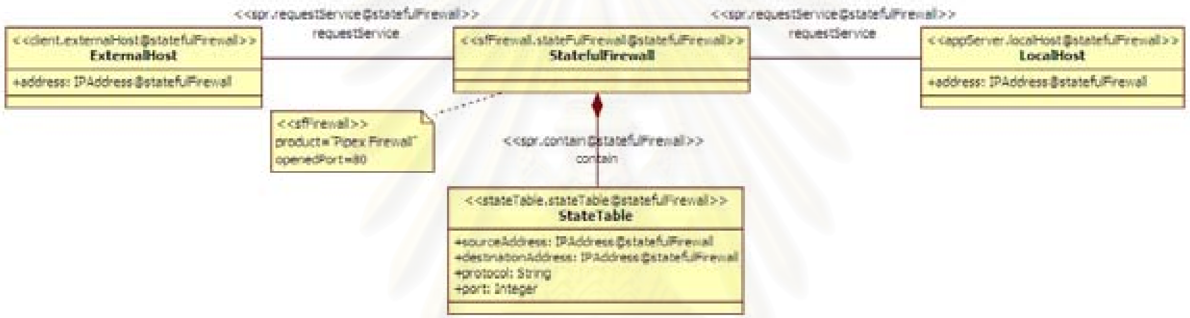


องค์ประกอบแบบจำลอง	แม่พิมพ์ต้นแบบที่ประยุกต์ใช้	คำอธิบาย
คลาส “ExternalHost”	client	เป็นผู้เข้าใช้ระบบจากภายนอก
คลาส “ProxyBasedFirewall”	pxFirewall	เป็นไฟร์วอลล์เชิงตัวแทน จะมีการกำหนดผลิตภัณฑ์ไฟร์วอลล์ในป้ายระบุ “product” และหมายเลขพอร์ทที่เปิดในป้ายระบุ “openedPort”
คลาส “Proxy”	proxy	เป็นตัวแทนของบริการในระบบ
คลาส “ApplicationRuleBase”	ruleBase	เป็นองค์ประกอบที่กรองแพ็คเกจในระดับข้อความในแพ็คเกจ
คลาส “LocalHost”	appServer	เป็นเครื่องบริการโปรแกรมประยุกต์ในระบบ
คลาส “ApplicationService”	appService	เป็นบริการของโปรแกรมประยุกต์ในระบบ

ตารางที่ ค.20 การประยุกต์ใช้ยูเอ็มแอลเซคเอสพีในแบบรูปไฟร์วอลล์เชิงสถานะ

ชื่อแบบรูปความมั่นคง	ไฟร์วอลล์เชิงสถานะ
กลุ่มแบบรูปความมั่นคง	สถาปัตยกรรมไฟร์วอลล์
คำอธิบาย	เป็นแบบรูปที่เสนอไฟร์วอลล์ที่เก็บสถานะของแม่ข่ายภายนอกระบบเพื่อลดจำนวนการตรวจสอบแพ็คเกจ

แผนภาพคลาสของแบบรูปความมั่นคงที่ประยุกต์ใช้ยูเอ็มแอลเซคเอสพี

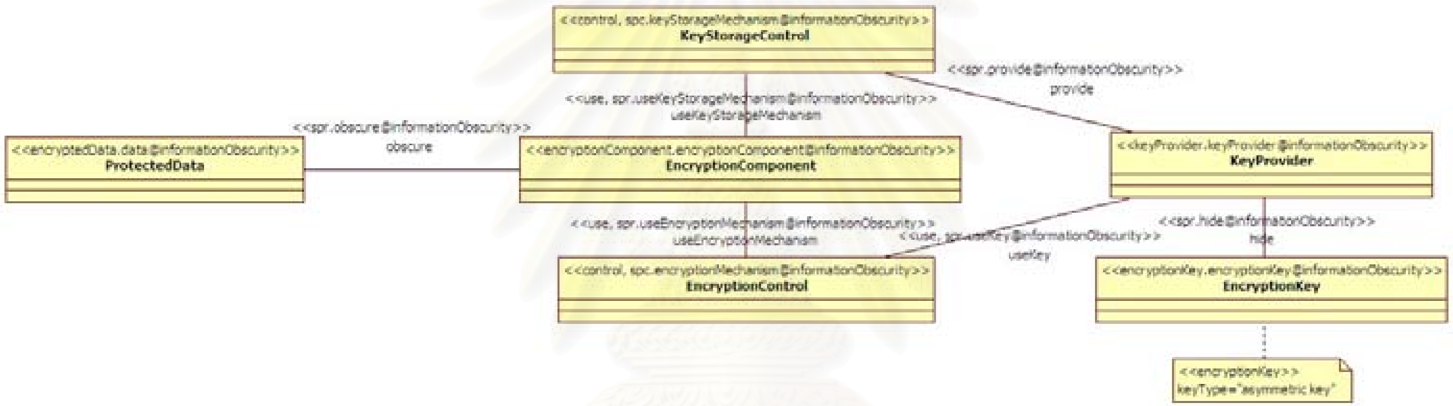


องค์ประกอบแบบจำลอง	แม่พิมพ์ต้นแบบที่ประยุกต์ใช้	คำอธิบาย
คลาส “ExternalHost”	client	เป็นผู้เข้าใช้ระบบจากภายนอก
คลาส “StatefulFirewall”	sfFirewall	เป็นไฟร์วอลล์เชิงสถานะ จะมีการกำหนดผลิตภัณฑ์ไฟร์วอลล์ในป้ายระบุ “product” และหมายเลขพอร์ทที่เปิดในป้ายระบุ “openedPort”
คลาส “StateTable”	stateTable	เป็นองค์ประกอบที่เก็บสถานะของแพ็คเกจ
คลาส “LocalHost”	appServer	เป็นเครื่องบริการโปรแกรมประยุกต์ในระบบ

ตารางที่ ค.21 การประยุกต์ใช้ยูเอ็มแอลเซคเอสพีในแบบรูปการปิดบังข้อมูล

ชื่อแบบรูปความมั่นคง	การปิดบังข้อมูล
กลุ่มแบบรูปความมั่นคง	การประยุกต์ใช้ความมั่นคงบนอินเตอร์เน็ต
คำอธิบาย	เป็นแบบรูปที่เสนอการปิดบังข้อมูลจากการเข้าถึงของกระบวนการที่ไม่พึงประสงค์

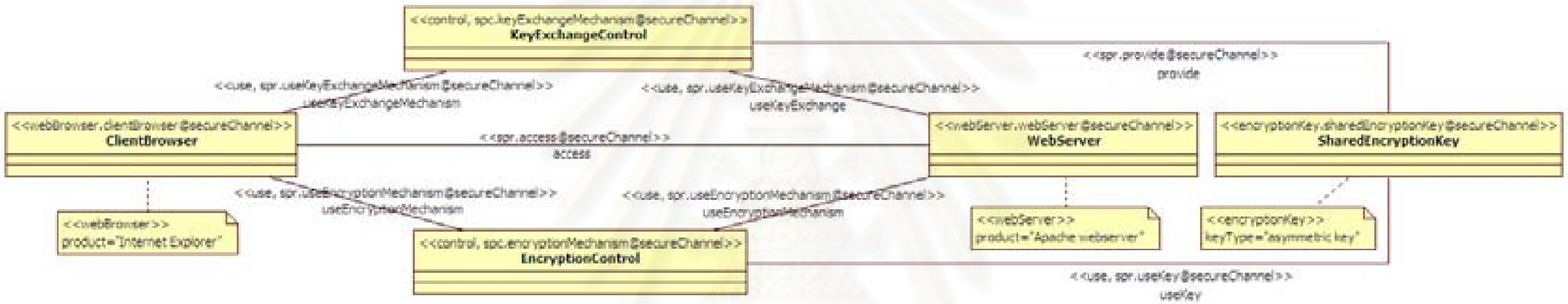
แผนภาพคลาสของแบบรูปความมั่นคงที่ประยุกต์ใช้ยูเอ็มแอลเซคเอสพี



องค์ประกอบแบบจำลอง	แม่พิมพ์ต้นแบบที่ประยุกต์ใช้	คำอธิบาย
คลาส “ProtectedData”	encryptedData	เป็นข้อมูลที่ถูกเข้ารหัสลับ
คลาส “EncryptionComponent”	encryptionComponent	เป็นองค์ประกอบที่ทำการเข้ารหัสลับให้กับข้อมูล
คลาส “KeyStorageControl”	control (จากองค์ประกอบมาตรฐานของยูเอ็มแอล) และ spc	เป็นองค์ประกอบที่ควบคุมกระบวนการจัดเก็บกุญแจ
คลาส “EncryptionControl”	control และ spc	เป็นองค์ประกอบที่ควบคุมกระบวนการเข้ารหัสลับ
คลาส “KeyProvider”	keyProvider	เป็นองค์ประกอบที่จัดหากุญแจที่ใช้ในการเข้ารหัสลับ
คลาส “EncryptionKey”	encryptionKey	เป็นกุญแจที่ใช้ในการเข้ารหัสลับ จะมีการกำหนดประเภทของกุญแจที่ใช้ในการเข้ารหัสในป้ายระบุ “keyType”
ความสัมพันธ์ ”useEncryptionMechanism”	use (จากองค์ประกอบมาตรฐานของยูเอ็มแอล) และ spr	เป็นความสัมพันธ์ที่แสดงถึงการใช้กระบวนการเข้ารหัส
ความสัมพันธ์ ”useKeyStorageMechanism”	use และ spr	เป็นความสัมพันธ์ที่แสดงถึงการใช้กระบวนการในการเก็บกุญแจที่ใช้ในการเข้ารหัส
ความสัมพันธ์ ”useKey”	use และ spr	เป็นความสัมพันธ์ที่แสดงถึงการใช้กุญแจในการเข้ารหัส

ตารางที่ ค.22 การประยุกต์ใช้ยูเอ็มแอลเซคเอสพีในแบบรูปช่องทางความมั่นคง

ชื่อแบบรูปความมั่นคง	ช่องทางความมั่นคง
กลุ่มแบบรูปความมั่นคง	การประยุกต์ใช้ความมั่นคงบนอินเตอร์เน็ต
คำอธิบาย	เป็นแบบรูปที่เสนอการแลกเปลี่ยนข้อมูลระหว่างผู้ใช้งานและเครื่องบริการเว็บ
แผนภาพคลาสของแบบรูปความมั่นคงที่ประยุกต์ใช้ยูเอ็มแอลเซคเอสพี	

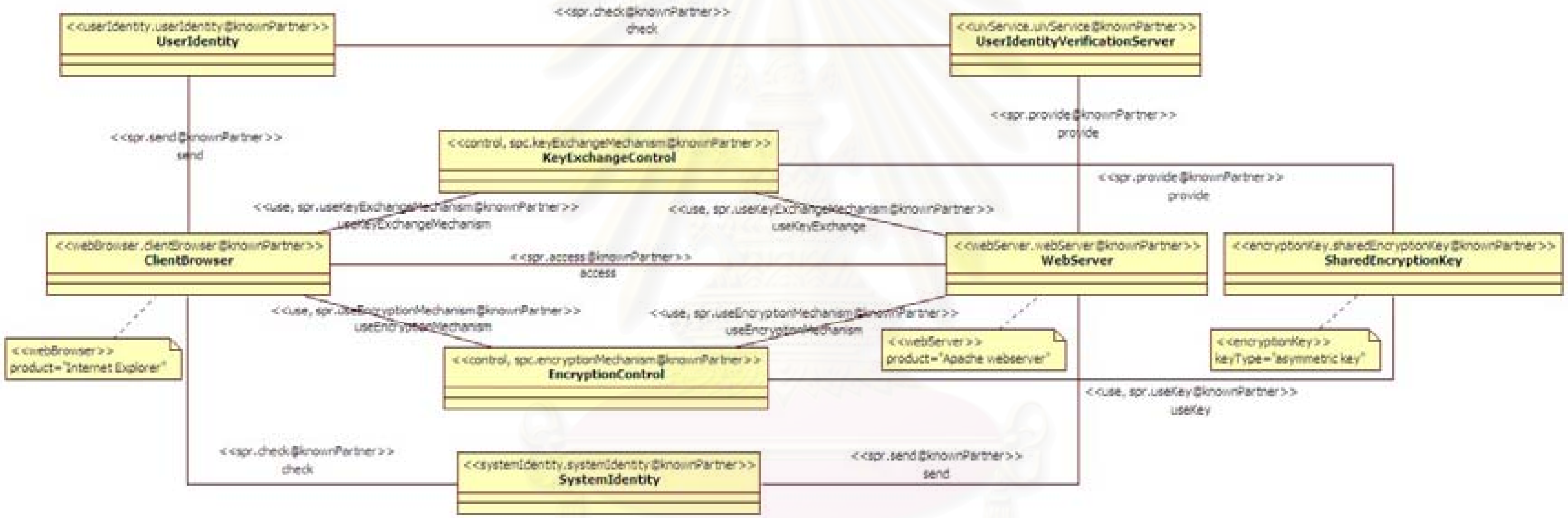


องค์ประกอบแบบจำลอง	แม่พิมพ์ต้นแบบที่ประยุกต์ใช้	คำอธิบาย
คลาส "ClientBrowser"	webBrowser	เป็นเว็บเบราว์เซอร์ของผู้ใช้งาน จะมีการกำหนดผลิตภัณฑ์ของเว็บเบราว์เซอร์ในป้ายระบุ "product"
คลาส "WebServer"	webServer	เป็นเครื่องบริการเว็บ จะมีการกำหนดผลิตภัณฑ์ของเครื่องบริการเว็บในป้ายระบุ "product"
คลาส "KeyExchangeControl"	control (จากองค์ประกอบมาตรฐานของยูเอ็มแอล) และ spc	เป็นองค์ประกอบที่ควบคุมกระบวนการแลกเปลี่ยนกุญแจที่ใช้ในการเข้ารหัส
คลาส "EncryptionControl"	control และ spc	เป็นองค์ประกอบที่ควบคุมกระบวนการเข้ารหัสลับ
คลาส "SharedEncryptionKey"	encryptionKey	เป็นกุญแจที่ใช้ในการแลกเปลี่ยน จะมีการกำหนดประเภทของกุญแจที่ใช้ในการเข้ารหัสในป้ายระบุ "keyType"
ความสัมพันธ์ "useEncryptionMechanism"	use (จากองค์ประกอบมาตรฐานของยูเอ็มแอล) และ spr	เป็นความสัมพันธ์ที่แสดงถึงการใช้กระบวนการเข้ารหัส
ความสัมพันธ์ "useKeyExchangeMechanism"	use และ spr	เป็นความสัมพันธ์ที่แสดงถึงการใช้กระบวนการในการแลกเปลี่ยนกุญแจที่ใช้ในการเข้ารหัส
ความสัมพันธ์ "useKey"	use และ spr	เป็นความสัมพันธ์ที่แสดงถึงการใช้กุญแจในการเข้ารหัส

ตารางที่ ค.23 การประยุกต์ใช้ยูเอ็มแอลเซคเอสพีในแบบรูปผู้เป็นที่รู้จัก

ชื่อแบบรูปความมั่นคง	ผู้เป็นที่รู้จัก
กลุ่มแบบรูปความมั่นคง	การประยุกต์ใช้ความมั่นคงบนอินเตอร์เน็ต
คำอธิบาย	เป็นแบบรูปที่เสนอการพิสูจน์ตัวตนของผู้ใช้งานและเครื่องบริการเว็บที่ถูกใช้งาน

แผนภาพคลาสของแบบรูปความมั่นคงที่ประยุกต์ใช้ยูเอ็มแอลเซคเอสพี



องค์ประกอบแบบจำลอง	แม่พิมพ์ต้นแบบที่ประยุกต์ใช้	คำอธิบาย
คลาส “ClientBrowser”	webBrowser	เป็นเว็บเบราว์เซอร์ของผู้ใช้งาน จะมีการกำหนดผลิตภัณฑ์ของเว็บเบราว์เซอร์ในป้ายระบุ “product”
คลาส “WebServer”	webServer	เป็นเครื่องบริการเว็บ จะมีการกำหนดผลิตภัณฑ์ของเครื่องบริการเว็บในป้ายระบุ “product”
คลาส “KeyExchangeControl”	control (จากองค์ประกอบมาตรฐานของยูเอ็มแอล) และ spc	เป็นองค์ประกอบที่ควบคุมกระบวนการแลกเปลี่ยนกุญแจที่ใช้ในการเข้ารหัส
คลาส “EncryptionControl”	control และ spc	เป็นองค์ประกอบที่ควบคุมกระบวนการเข้ารหัสลับ
คลาส “SharedEncryptionKey”	encryptionKey	เป็นกุญแจที่ใช้ในการแลกเปลี่ยน จะมีการกำหนดประเภทของกุญแจที่ใช้ในการเข้ารหัสในป้ายระบุ “keyType”
คลาส “UserIdentity”	userIdentity	เป็นองค์ประกอบที่ใช้ในการระบุตัวตนของผู้ใช้งาน

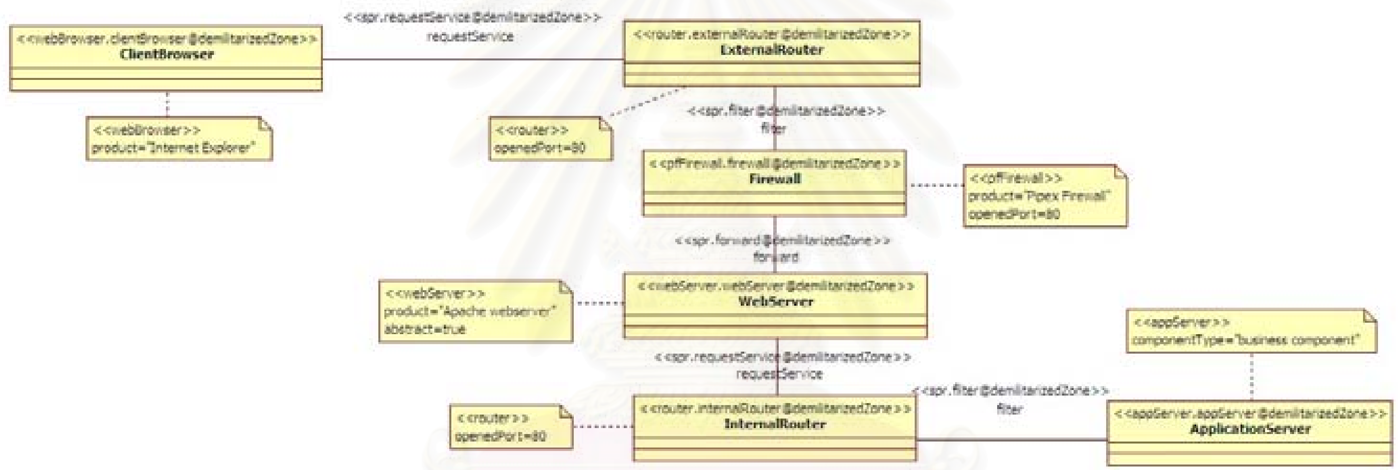
ตารางที่ ค.23 การประยุกต์ใช้ยูเอ็มแอลเซคเอสพีในแบบรูปผู้เป็นที่รู้จัก (ต่อ)

องค์ประกอบแบบจำลอง	แม่พิมพ์ต้นแบบที่ประยุกต์ใช้	คำอธิบาย
คลาส “SystemIdentity”	systemIdentity	เป็นองค์ประกอบที่ใช้ในการระบุตัวตนของเครื่องบริการเว็บที่ถูกใช้งาน
คลาส “UserIdentityVerificationService”	uivService	เป็นบริการทวนสอบของการพิสูจน์ผู้ใช้งาน
ความสัมพันธ์ “useEncryptionMechanism”	use (จากองค์ประกอบมาตรฐานของยูเอ็มแอล) และ spr	เป็นความสัมพันธ์ที่แสดงถึงการใช้กระบวนการเข้ารหัส
ความสัมพันธ์ “useKeyExchangeMechanism”	use และ spr	เป็นความสัมพันธ์ที่แสดงถึงการใช้กระบวนการในการแลกเปลี่ยนกุญแจที่ใช้ในการเข้ารหัส
ความสัมพันธ์ “useKey”	use และ spr	เป็นความสัมพันธ์ที่แสดงถึงการใช้กุญแจในการเข้ารหัส

ตารางที่ ค.24 การประยุกต์ใช้ยูเอ็มแอลเซคเอสพีในแบบรูปเขตปลอดการป้องกัน

ชื่อแบบรูปความมั่นคง	เขตปลอดการป้องกัน
กลุ่มแบบรูปความมั่นคง	การประยุกต์ใช้ความมั่นคงบนอินเตอร์เน็ต
คำอธิบาย	เป็นแบบรูปที่เสนอการแยกฟังก์ชันการทำงานและข้อมูลที่สำคัญออกจากเว็บเซิฟเวอร์

แผนภาพคลาสของแบบรูปความมั่นคงที่ประยุกต์ใช้ยูเอ็มแอลเซคเอสพี



องค์ประกอบแบบจำลอง	แม่พิมพ์ต้นแบบที่ประยุกต์ใช้	คำอธิบาย
คลาส “ClientBrowser”	webBrowser	เป็นเว็บเบราว์เซอร์ของผู้ใช้งาน จะมีการกำหนดผลิตภัณฑ์ของเว็บเบราว์เซอร์ในป้ายระบุ “product”
คลาส “ExternalRouter”	router	เป็นองค์ประกอบที่จัดเส้นทางของแพ็คเกจที่เข้าออกในระบบ จะมีการกำหนดหมายเลขพอร์ทที่เปิดในป้ายระบุ “openedPort”
คลาส “Firewall”	pfFirewall	เป็นไฟร์วอลล์สำหรับการกรองแพ็คเกจ จะมีการกำหนดผลิตภัณฑ์ของไฟร์วอลล์ในป้ายระบุ “product” และหมายเลขพอร์ทที่เปิดในป้ายระบุ “openedPort”
คลาส “WebServer”	webServer	เป็นเครื่องบริการเว็บ จะมีการกำหนดผลิตภัณฑ์ของเครื่องบริการเว็บในป้ายระบุ “product” และมีการกำหนดลักษณะของเครื่องบริการเว็บที่เป็นนามธรรมในป้ายระบุ “abstract”
คลาส “InternalRouter”	router	เป็นองค์ประกอบที่จัดเส้นทางของแพ็คเกจที่เข้าออกในระบบ จะมีการกำหนดหมายเลขพอร์ทที่เปิดในป้ายระบุ “openedPort”
คลาส “ApplicationServer”	appServer	เป็นเครื่องบริการโปรแกรมประยุกต์ จะมีการกำหนดส่วนประกอบของเครื่องบริการโปรแกรมประยุกต์ในป้ายระบุ “componentType”

ตารางที่ ค.25 การประยุกต์ใช้ยูเอ็มแอลเซคเอสพีในแบบรูปตัวแทนป้องกัน

ชื่อแบบรูปความมั่นคง	ตัวแทนป้องกัน
กลุ่มแบบรูปความมั่นคง	การประยุกต์ใช้ความมั่นคงบนอินเตอร์เน็ต
คำอธิบาย	เป็นแบบรูปที่เสนอการใช้ตัวแทนในการป้องกันการเข้าถึงแม่ข่ายในระดับโปรแกรมประยุกต์

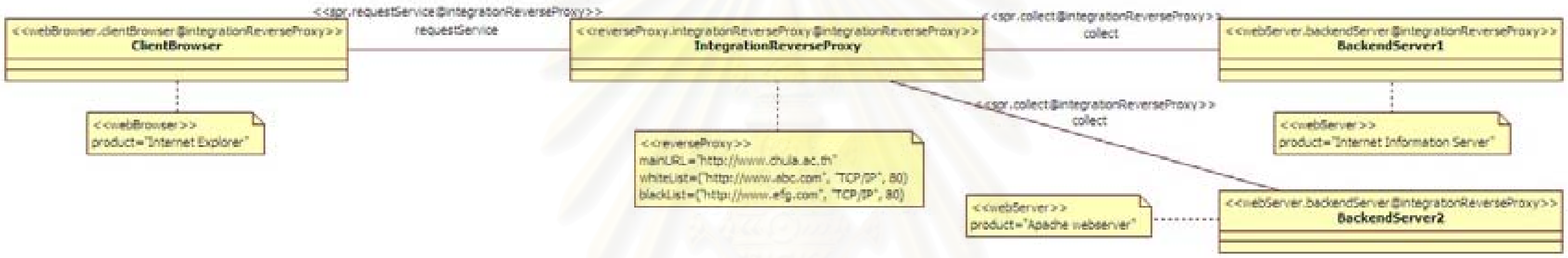
แผนภาพคลาสของแบบรูปความมั่นคงที่ประยุกต์ใช้ยูเอ็มแอลเซคเอสพี

องค์ประกอบแบบจำลอง	แม่พิมพ์ต้นแบบที่ประยุกต์ใช้	คำอธิบาย
คลาส “ClientBrowser”	webBrowser	เป็นเว็บเบราว์เซอร์ของผู้ใช้งาน จะมีการกำหนดผลิตภัณฑ์ของเว็บเบราว์เซอร์ในป้ายระบุ “product”
คลาส “ExternalPacketFilterFirewall”	pfFirewall	เป็นไฟร์วอลล์ที่ควบคุมแพ็คเกจที่ส่งไปยังเว็บเซิฟเวอร์ จะมีการกำหนดผลิตภัณฑ์ของไฟร์วอลล์ในป้ายระบุ “product” จะมีการกำหนดหมายเลขพอร์ทที่เปิดในป้ายระบุ “openedPort”
คลาส “ReverseProxy”	reverseProxy	เป็นตัวแทนที่ป้องกันการเข้าถึงแม่ข่าย
คลาส “InternalPacketFilterFirewall”	pfFirewall	เป็นไฟร์วอลล์ที่ควบคุมแพ็คเกจที่ส่งไปยังเว็บเซิฟเวอร์ จะมีการกำหนดผลิตภัณฑ์ของไฟร์วอลล์ในป้ายระบุ “product” จะมีการกำหนดหมายเลขพอร์ทที่เปิดในป้ายระบุ “openedPort”
คลาส “WebServer”	webServer	เป็นเครื่องบริการเว็บ จะมีการกำหนดผลิตภัณฑ์ของเครื่องบริการเว็บในป้ายระบุ “product”

ตารางที่ ค.26 การประยุกต์ใช้ยูเอ็มแอลเซคเอสพีในแบบรูปตัวแทนบูรณาการ

ชื่อแบบรูปความมั่นคง	ตัวแทนบูรณาการ
กลุ่มแบบรูปความมั่นคง	การประยุกต์ใช้ความมั่นคงบนอินเตอร์เน็ต
คำอธิบาย	เป็นแบบรูปที่เสนอการใช้ตัวแทนในการสร้างมุมมองเดียวสำหรับแม่ข่ายที่อยู่ภายใต้ตัวแทนทั้งหมด

แผนภาพคลาสของแบบรูปความมั่นคงที่ประยุกต์ใช้ยูเอ็มแอลเซคเอสพี



องค์ประกอบแบบจำลอง	แม่พิมพ์ต้นแบบที่ประยุกต์ใช้	คำอธิบาย
คลาส "ClientBrowser"	webBrowser	เป็นเว็บเบราว์เซอร์ของผู้ใช้งาน จะมีการกำหนดผลิตภัณฑ์ของเว็บเบราว์เซอร์ในป้ายระบุ "product"
คลาส "ReverseProxy"	reverseProxy	เป็นตัวแทนบูรณาการที่รวบรวมเครื่องบริการทั้งหมด จะมีการกำหนดยูอาร์แอลหลัก (URL) ในป้ายระบุ "mainURL" รายการที่อนุญาตให้ผ่านในป้ายระบุ "whiteList" และรายการที่ไม่อนุญาตให้ผ่านในป้ายระบุ "blackList"
คลาส "BackendServer1"	webServer	เป็นเครื่องบริการเว็บที่อยู่ภายใต้ตัวแทนบูรณาการ จะมีการกำหนดผลิตภัณฑ์ของเครื่องบริการเว็บในป้ายระบุ "product"
คลาส "BackendServer2"	webServer	เป็นเครื่องบริการเว็บที่อยู่ภายใต้ตัวแทนบูรณาการ จะมีการกำหนดผลิตภัณฑ์ของเครื่องบริการเว็บในป้ายระบุ "product"

ตารางที่ ค.27 การประยุกต์ใช้ยูเอ็มแอลเซคเอสพีในแบบรูปประตูหน้า

ชื่อแบบรูปความมั่นคง	ประตูหน้า
กลุ่มแบบรูปความมั่นคง	การประยุกต์ใช้ความมั่นคงบนอินเตอร์เน็ต
คำอธิบาย	เป็นแบบรูปที่เสนอการใช้แม่ข่ายตัวแทนบูรณาการในการระบุตัวตนและการตรวจสอบผู้ใช้งาน

แผนภาพคลาสของแบบรูปความมั่นคงที่ประยุกต์ใช้ยูเอ็มแอลเซคเอสพี

องค์ประกอบแบบจำลอง	แม่พิมพ์ต้นแบบที่ประยุกต์ใช้	คำอธิบาย
คลาส “ClientBrowser”	webBrowser	เป็นเว็บเบราว์เซอร์ของผู้ใช้งาน จะมีการกำหนดผลิตภัณฑ์ของเว็บเบราว์เซอร์ในป้ายระบุ “product”
คลาส “IntegrationReverseProxy”	reverseProxy	เป็นตัวแทนบูรณาการที่รวบรวมเครื่องบริการทั้งหมด จะมีการกำหนดยูอาร์แอลหลัก (URL) ในป้ายระบุ “mainURL” รายการที่อนุญาตให้ผ่านในป้ายระบุ “whiteList” และรายการที่ไม่อนุญาตให้ผ่านในป้ายระบุ “blackList”
คลาส “BackendServer1”	webServer	เป็นเครื่องบริการเว็บที่อยู่ภายใต้ตัวแทนบูรณาการ จะมีการกำหนดผลิตภัณฑ์ของเครื่องบริการเว็บในป้ายระบุ “product”
คลาส “BackendServer2”	webServer	เป็นเครื่องบริการเว็บที่อยู่ภายใต้ตัวแทนบูรณาการ จะมีการกำหนดผลิตภัณฑ์ของเครื่องบริการเว็บในป้ายระบุ “product”
คลาส “UserDirectory”	userDirectory	เป็นองค์ประกอบที่จัดการข้อมูลที่ใช้ในการระบุตัวตนและการตรวจสอบผู้ใช้งาน

ภาคผนวก ง
กรณีศึกษาที่ใช้ยูเอ็มแอลเซคเอสพีในการแสดงแบบรูปความมั่นคง

กรณีศึกษาที่ใช้ยูเอ็มแอลเซคเอสพีในงานวิจัยนี้ประกอบด้วย 4 กรณีศึกษา โดยแต่ละมีรายละเอียดดังต่อไปนี้

กรณีศึกษาที่ 1: ระบบเอทีเอ็ม (Automatic Teller Machine: ATM)

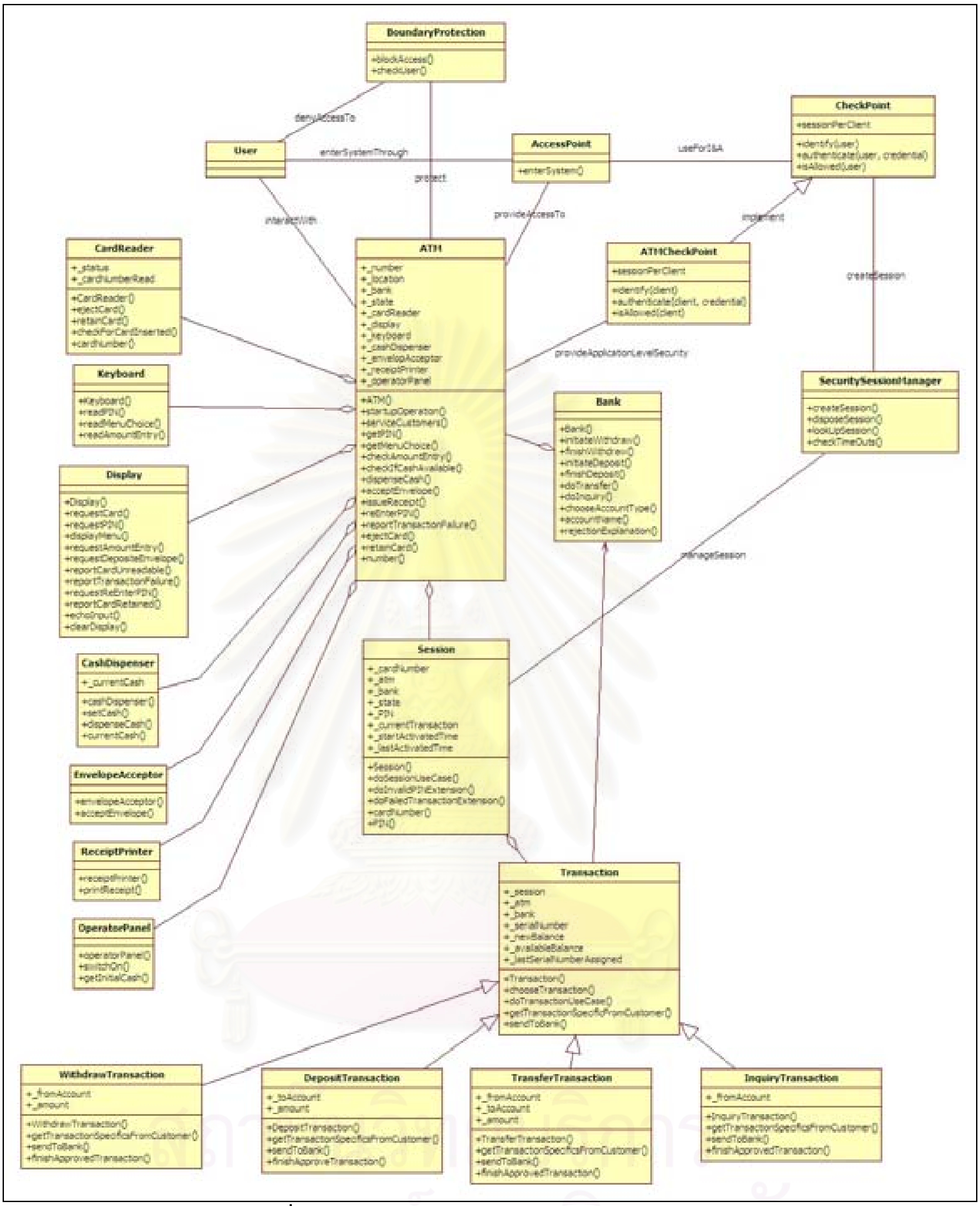
ระบบเอทีเอ็ม หรือระบบฝากและถอนเงินของธนาคารโดยอัตโนมัติ เป็นระบบที่อำนวยความสะดวกให้แก่ผู้ใช้บริการธนาคาร โดยผู้ใช้บริการสามารถทำการฝากเงินและถอนเงินผ่านตู้เอทีเอ็มของธนาคารโดยไม่ต้องไปติดต่อกับทางธนาคารโดยตรง

เนื่องจากระบบดังกล่าวเป็นระบบที่เกี่ยวข้องกับระบบการเงินของธนาคารโดยตรง จึงทำให้ระบบมีความเสี่ยงต่อการคุกคามจากผู้บุกรุกสูง ดังนั้นระบบจึงถูกออกแบบให้มีการใช้แบบรูปความมั่นคงในการออกแบบในระดับคลาส คือ แบบรูปเซสชันทางความมั่นคง ดังรูปที่ ง.1 ซึ่งแบบรูปดังกล่าวอยู่ในกลุ่มแบบรูปสถาปัตยกรรมการควบคุมการเข้าถึงระบบ โดยแบบรูปเซสชันทางความมั่นคงจะช่วยในการกำหนดข้อมูลความมั่นคงที่ใช้ในการตรวจสอบผู้ใช้งานในระหว่างที่ผู้ใช้งานติดต่อภายในระบบ

โดยความต้องการในการแสดงข้อมูลทางโครงสร้างและข้อมูลทางความมั่นคงของระบบเอทีเอ็ม ประกอบไปด้วย

1. ข้อมูลทางโครงสร้างของแบบรูป
   - 1.1. ข้อมูลที่ระบุองค์ประกอบแบบจำลองที่เป็นส่วนประกอบของแบบรูป
   - 1.2. ข้อมูลที่ระบุแบบรูปที่ใช้งาน
   - 1.3. ข้อมูลที่ระบุลำดับของแบบรูป
   - 1.4. ข้อมูลที่ระบุบทบาทของแต่ละองค์ประกอบแบบจำลองในแบบรูป
2. ข้อมูลทางความมั่นคงของแบบรูป
   - 2.1. ผู้ใช้งานจากภายนอกระบบ
   - 2.2. จุดเข้าระบบ
   - 2.3. บริการในระบบ
   - 2.4. จุดตรวจสอบผู้ใช้งาน
   - 2.5. เซสชันทางความมั่นคง
   - 2.6. วิธีในการเข้าสู่ระบบ
   - 2.7. บริการที่ต้องการตรวจสอบโดยใช้จุดตรวจสอบ
   - 2.8. ประเภทของเซสชันทางความมั่นคง
   - 2.9. อายุการใช้งานของเซสชันทางความมั่นคง

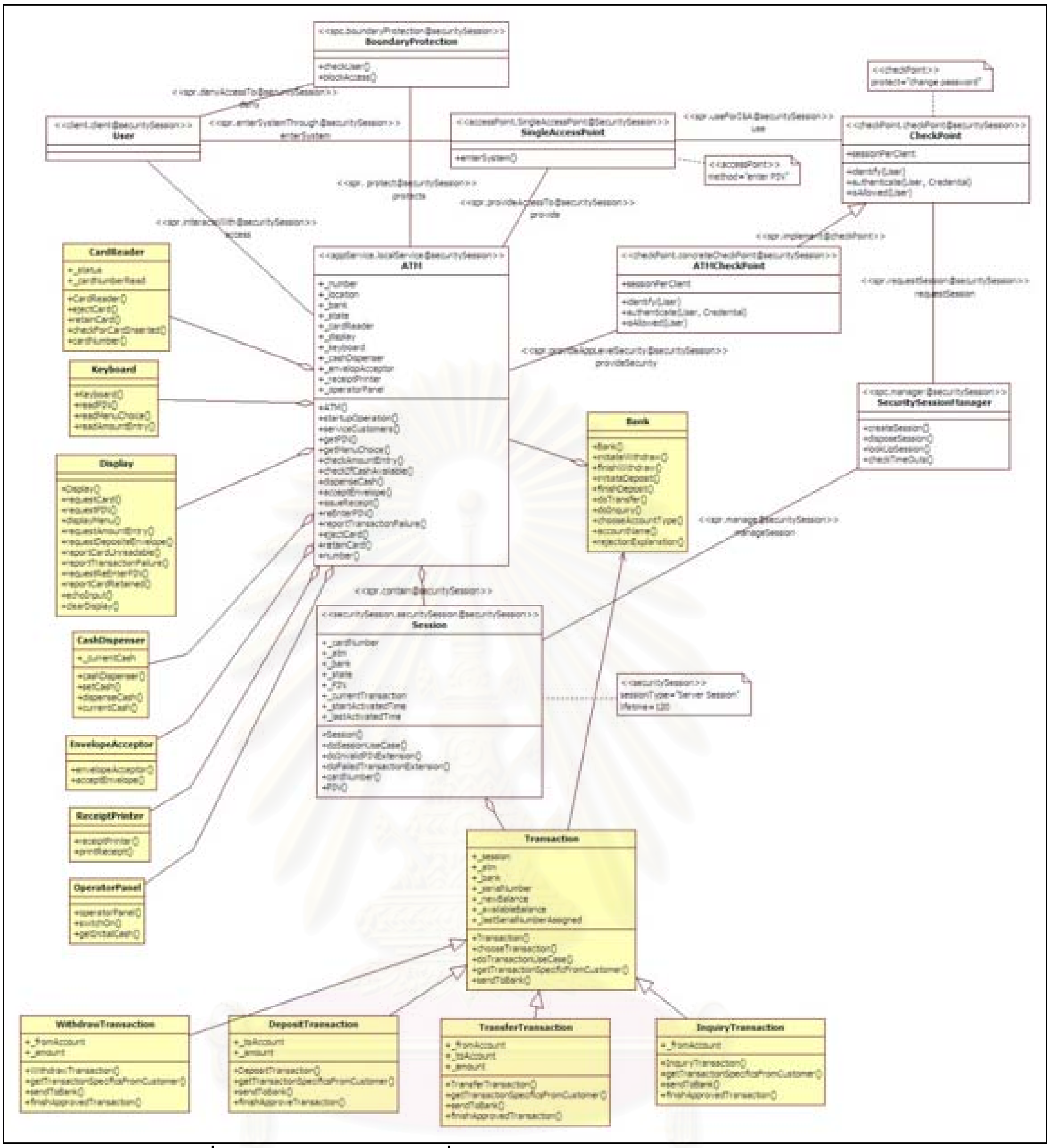
ยูเอ็มแอลเซคไม่สามารถแสดงข้อมูลของแบบรูปตามความต้องการของแบบรูปในระบบเอทีเอ็มได้ เนื่องจากขาดองค์ประกอบที่ใช้ในการแสดงข้อมูลของแบบรูปในระบบดังกล่าว



รูปที่ ง.1 แผนภาพคลาสของระบบเอทีเอ็ม [20]

จากรูปที่ ง.2 แสดงแผนภาพคลาสที่ใช้ยูเอ็มแอลเซคเอสพีของระบบเอทีเอ็ม โดยข้อมูลทางโครงสร้างและข้อมูลทางความมั่นคงของแบบรูปที่อธิบายโดยใช้ยูเอ็มแอลเซคเอสพีประกอบด้วย คลาสที่ทำหน้าที่เป็นผู้เข้าใช้ทรัพยากรจากภายนอกระบบคือ คลาส “User” ที่กำกับโดยแม่พิมพ์ต้นแบบ “client” คลาสที่ทำหน้าที่เป็นบริการภายในระบบคือ คลาส “ATM” ที่กำกับโดยแม่พิมพ์ต้นแบบ “appService” คลาสที่ทำหน้าที่ควบคุมขอบเขตของการเข้าถึงระบบคือ คลาส “BoundaryProtection” ที่กำกับโดยแม่พิมพ์ต้นแบบ ”spc” คลาสที่ทำหน้าที่เป็นจุดเข้าระบบคือ คลาส “SingleAccessPoint” ที่กำกับโดยแม่พิมพ์ต้นแบบ “accessPoint”

โดยกำหนดวิธีในการเข้าสู่ระบบคือ การกรอกรหัสประจำบัตร คลาสที่ทำหน้าที่เป็นจุดตรวจสอบของระบบคือ คลาส “CheckPoint” ที่กำกับโดยแม่พิมพ์ต้นแบบ “checkpoint” ที่จะตรวจสอบผู้ใช้งานเมื่อมีการเข้าถึงรหัสประจำบัตร คลาสที่ทำหน้าที่เป็นจุดตรวจสอบของการเข้าใช้คลาส “ATM” โดยเฉพาะคือ คลาส “ATMCheckPoint” ที่กำกับโดยแม่พิมพ์ต้นแบบ “checkPoint” คลาสที่ทำหน้าที่เป็นเซสชันทางความมั่นคงของผู้ใช้งานคือ คลาส “Session” ที่กำกับโดยแม่พิมพ์ต้นแบบ “SecuritySession” ที่มีการกำหนดชนิดของเซสชันคือ เซสชันภายในเซิฟเวอร์ และมีอายุการใช้งาน 120 วินาที และคลาสที่ควบคุมเซสชันทางความมั่นคงของผู้ใช้งานคือ คลาส “SecuritySessionManager” ที่กำกับโดยแม่พิมพ์ต้นแบบ “spc” เพื่อระบุว่าเป็นองค์ประกอบภายในแบบรูปข้อมูลเซสชันทางความมั่นคง



รูปที่ ง.2 แผนภาพคลาสที่ใช้ยูเอ็มแอลเซคเอสพีของระบบเอทีเอ็ม

กรณีศึกษาที่ 2: กระบวนการความมั่นคงในระบบปฏิบัติการ (Secure Process)

กระบวนการความมั่นคงในระบบปฏิบัติการ เป็นกระบวนการที่มีการควบคุมการเข้าถึงหน่วยความจำเสมือนของกระบวนการในระบบปฏิบัติการให้เป็นไปตามสิทธิ์ของกระบวนการนั้นๆ รวมทั้งมีการตรวจสอบการเข้าถึงหน่วยความจำเสมือนของกระบวนการ

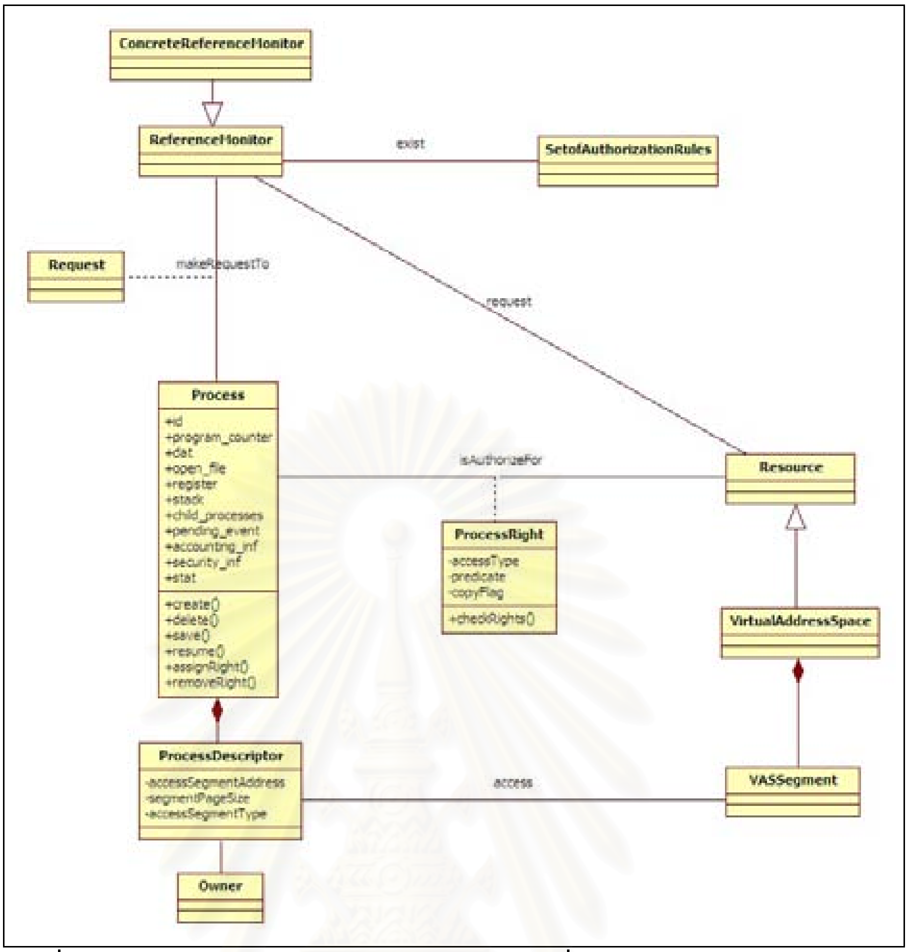
กระบวนการความมั่นคงในระบบปฏิบัติการ มีการประยุกต์ใช้แบบรูปความมั่นคงประกอบด้วย แบบรูปการให้อำนาจ แบบรูปการตรวจสอบการเข้าใช้ทรัพยากร และแบบรูปการควบคุมหน่วยความจำเสมือน ดังรูปที่ ง.3 ซึ่งแบบรูปดังกล่าวอยู่ในกลุ่มแบบรูปของแบบจำลองการควบคุมการเข้าถึงและการควบคุมการเข้าถึงระบบปฏิบัติการ โดยแบบรูปการให้อำนาจและแบบรูปการควบคุมหน่วยความจำเสมือนจะช่วยในการควบคุมการเข้าถึงหน่วยความจำเสมือนของกระบวนการให้เป็นไปตามสิทธิ์ของกระบวนการนั้นๆ และแบบรูปการตรวจสอบการเข้าใช้

ทรัพยากรจะช่วยในการตรวจสอบการเข้าใช้หน่วยความจำเสมือนของกระบวนการในระบบปฏิบัติการ

โดยความต้องการในการแสดงข้อมูลทางโครงสร้างและข้อมูลทางความมั่นคงของกระบวนการความมั่นคงในระบบปฏิบัติการ ประกอบไปด้วย

1. ข้อมูลทางโครงสร้างของแบบรูป
    1.1. ข้อมูลที่ระบุองค์ประกอบแบบจำลองที่เป็นส่วนประกอบของแบบรูป
    1.2. ข้อมูลที่ระบุแบบรูปที่ใช้งาน
    1.3. ข้อมูลที่ระบุลำดับของแบบรูป
    1.4. ข้อมูลที่ระบุบทบาทของแต่ละองค์ประกอบแบบจำลองในแบบรูป
2. ข้อมูลทางความมั่นคงของแบบรูป
    2.1. ผู้เข้าใช้ทรัพยากร
    2.2. องค์ประกอบที่ควบคุมการเข้าถึงทรัพยากร
    2.3. ทรัพยากรที่ถูกควบคุม
    2.4. ลักษณะของการเข้าถึงทรัพยากร
    2.5. เงื่อนไขต้องห้ามในการให้อำนาจแก่ผู้ใช้งาน
    2.6. ลักษณะในการอนุญาตให้ผู้อื่นคัดลอกอำนาจของผู้ใช้งานดังกล่าว
    2.7. อ็อบเจกต์ที่ควบคุมการเข้าถึงทรัพยากร
    2.8. ประเภทขององค์ประกอบที่ควบคุมการเข้าถึงทรัพยากร
    2.9. คำร้องขอใช้ทรัพยากรในระบบ
    2.10. องค์ประกอบที่ตรวจสอบการร้องขอใช้ทรัพยากร
    2.11. องค์ประกอบที่ควบคุมการตรวจสอบการร้องขอใช้ทรัพยากร
    2.12. การเชื่อมโยงที่มีการตรวจสอบการร้องขอใช้ทรัพยากร
    2.13. อ็อบเจกต์ที่ตรวจสอบคำร้องขอใช้ทรัพยากร
    2.14. กระบวนการของระบบปฏิบัติการ
    2.15. องค์ประกอบที่จัดเก็บสิทธิ์ของกระบวนการในระบบปฏิบัติการ
    2.16. หน่วยความจำเสมือนในระบบปฏิบัติการ
    2.17. ที่อยู่ของเซกเมนต์
    2.18. ลักษณะของการเข้าถึงเซกเมนต์
    2.19. ขนาดของเซกเมนต์

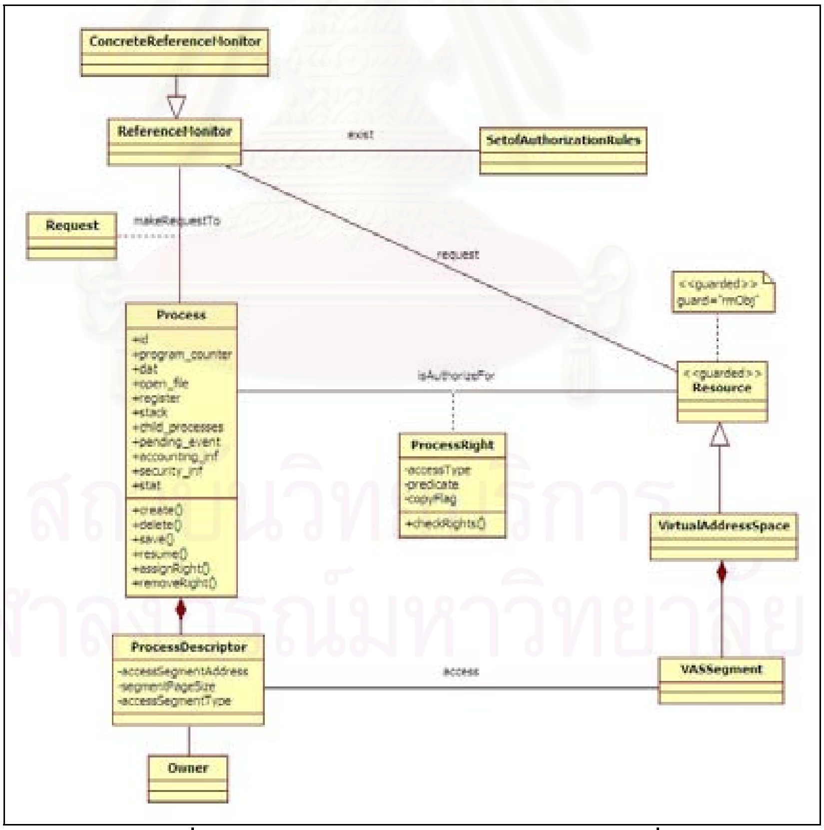
จากรูปที่ ง.4 แสดงแผนภาพคลาสที่ใช้ยูเอ็มแอลเซคของกระบวนการความมั่นคงในระบบปฏิบัติการ ยูเอ็มแอลเซคสามารถแสดงข้อมูลของแบบรูปตามความต้องการของแบบรูป คือ อ็อบเจกต์ที่ควบคุมการเข้าถึงทรัพยากร และทรัพยากรที่ถูกควบคุม ได้เท่านั้น



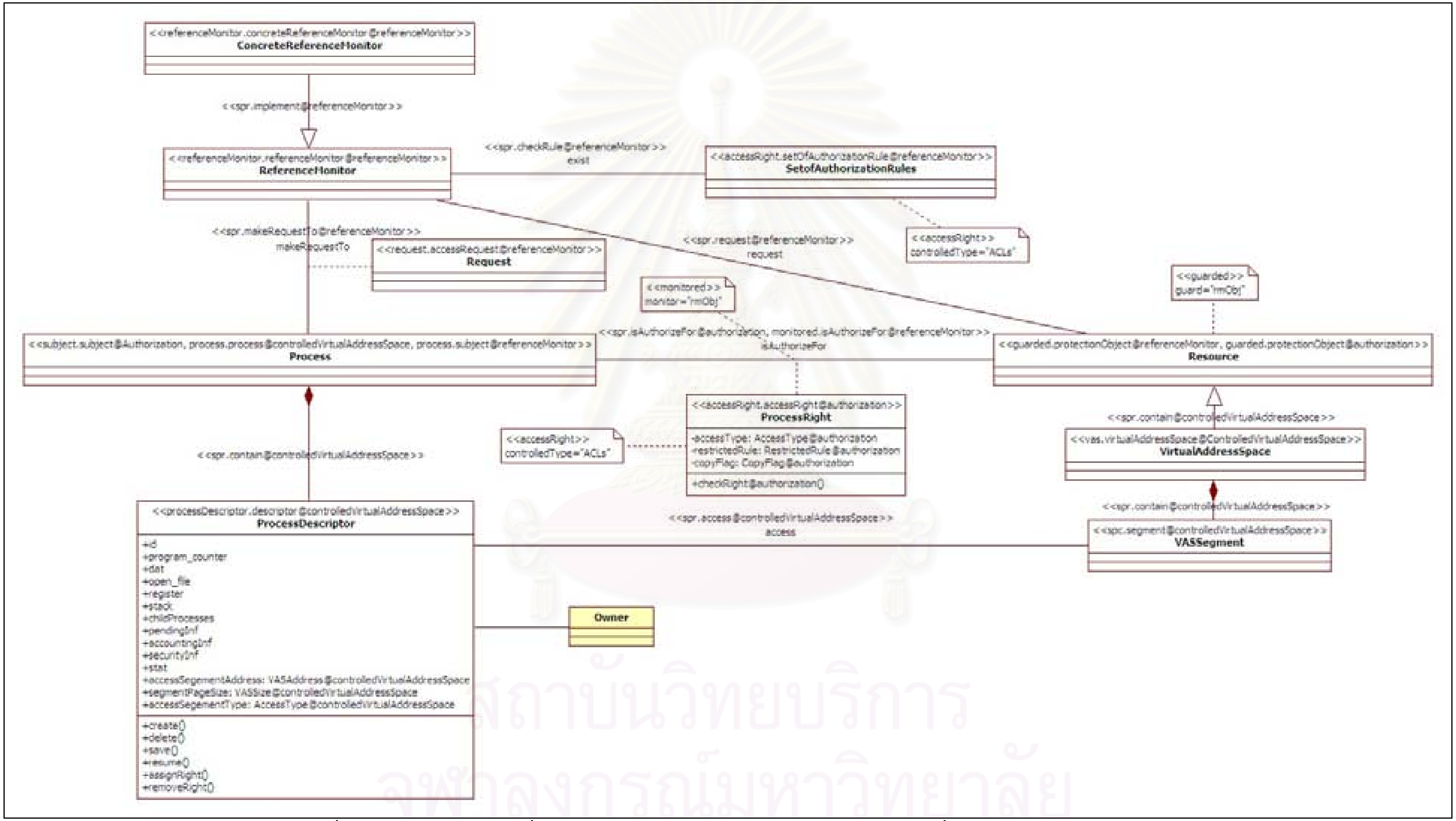
รูปที่ ง.3 แผนภาพคลาสของกระบวนการความมั่นคงในระบบปฏิบัติการ [21]

จากรูปที่ ง.5 แสดงแผนภาพคลาสที่ใช้ยูเอ็มแอลเซคเอสพีของกระบวนการความมั่นคงในระบบปฏิบัติการ โดยข้อมูลทางโครงสร้างและข้อมูลทางความมั่นคงของแบบรูปที่อธิบายโดยใช้ยูเอ็มแอลเซคเอสพี ประกอบด้วย คลาสที่ทำหน้าที่เป็นกระบวนการที่เข้าถึงหน่วยความจำเสมือนในระบบปฏิบัติการคือ คลาส “Process” ที่กำกับโดยแม่พิมพ์ต้นแบบ “process” และ “subject” และมีป้ายระบุเพื่อระบุว่าเป็นองค์ประกอบภายในแบบรูปการให้อำนาจ แบบรูปการตรวจสอบการเข้าใช้ทรัพยากร และแบบรูปการควบคุมหน่วยความจำเสมือน คลาสที่ทำหน้าที่เป็นองค์ประกอบที่จัดเก็บสิทธิ์ของกระบวนการคือ คลาส “ProcessDescriptor” ที่กำกับโดยแม่พิมพ์ต้นแบบ “processDescriptor” ที่มีคุณลักษณะ “accessSegmentAddress” แสดงที่อยู่ของเซกเมนต์ที่เข้าถึง คุณลักษณะ “segmentPageSize” แสดงจำนวนหน้าของเซกเมนต์ที่ถูกจำกัด และคุณลักษณะ “accessSegmentType” แสดงลักษณะของการเข้าถึงเซกเมนต์ คลาสที่ทำหน้าที่เป็นหน่วยความจำเสมือนในระบบปฏิบัติการคือ คลาส “VirtualAddressSpace” ที่กำกับโดยแม่พิมพ์ต้นแบบ “vas” คลาสที่ทำหน้าที่เป็นเซกเมนต์ของหน่วยความจำเสมือนคือ คลาส “VASSegment” ที่กำกับโดยแม่พิมพ์ต้นแบบ “spc” คลาสที่ทำหน้าที่เป็นทรัพยากรในระบบโดยรวมถึงหน่วยความจำเสมือนคือ คลาส “Resource” ที่กำกับโดยแม่พิมพ์ต้นแบบ “guarded” และมีป้ายระบุเพื่อระบุว่าเป็นองค์ประกอบภายในแบบรูปการให้อำนาจ และแบบ

รูปการตรวจสอบการเข้าใช้ทรัพยากร คลาสที่ทำหน้าที่เป็นองค์ประกอบที่ควบคุมการเข้าถึงทรัพยากรของกระบวนการคือ คลาส “ProcessRight” ที่กำกับโดยแม่พิมพ์ต้นแบบ “accessRight” โดยคลาสดังกล่าวจะมีคุณลักษณะ “accessType” แสดงลักษณะของการเข้าถึงทรัพยากร คุณลักษณะ “restrictedRule” แสดงเงื่อนไขต้องห้ามในการให้อำนาจแก่ผู้ใช้งาน คุณลักษณะ “copyFlag” แสดงลักษณะในการอนุญาตให้ผู้อื่นคัดลอกอำนาจของผู้ใช้งานดังกล่าว และการดำเนินการ “checkRights” แสดงการดำเนินการที่ใช้ในการตรวจสอบอำนาจของผู้ใช้ทรัพยากร คลาสที่ทำหน้าที่เป็นองค์ประกอบที่ตรวจสอบคำร้องขอใช้ทรัพยากรคือ คลาส “ReferenceMonitor” ที่กำกับโดยแม่พิมพ์ต้นแบบ “referenceMonitor” คลาสที่ทำหน้าที่เป็นคำร้องขอใช้ทรัพยากรคือ คลาส “Request” ที่กำกับโดยแม่พิมพ์ต้นแบบ “request” คลาส “ConcreteReferenceMonitor” ที่กำกับโดยแม่พิมพ์ต้นแบบ “referenceMonitor” คลาสที่ทำหน้าที่เป็นองค์ประกอบที่ควบคุมการตรวจสอบคำร้องขอใช้ทรัพยากรคือ คลาส “SetofAuthorizationRules” ที่กำกับโดยแม่พิมพ์ต้นแบบ “accessRight” และการเชื่อมโยงที่มีการตรวจสอบการร้องขอใช้ทรัพยากรคือ ความสัมพันธ์ “isAuthorizeFor” ที่กำกับโดยแม่พิมพ์ต้นแบบ “monitored” และมีการกำหนดอ็อบเจกต์ที่ตรวจสอบคำร้องขอใช้ทรัพยากรในป้ายระบุ “monitor”



รูปที่ ง.4 แผนภาพคลาสที่ใช้ยูเอ็มแอลเซคของกระบวนการความมั่นคงในระบบปฏิบัติการ



รูปที่ ง.5 แผนภาพคลาสที่ใช้ยูเอ็มแอลเซคเอสพีของกระบวนการความมั่นคงในระบบปฏิบัติการ

กรณีศึกษาที่ 3: ไฟร์วอลล์สำหรับการกรองเอกซ์เอ็มแอล (XML Firewall)

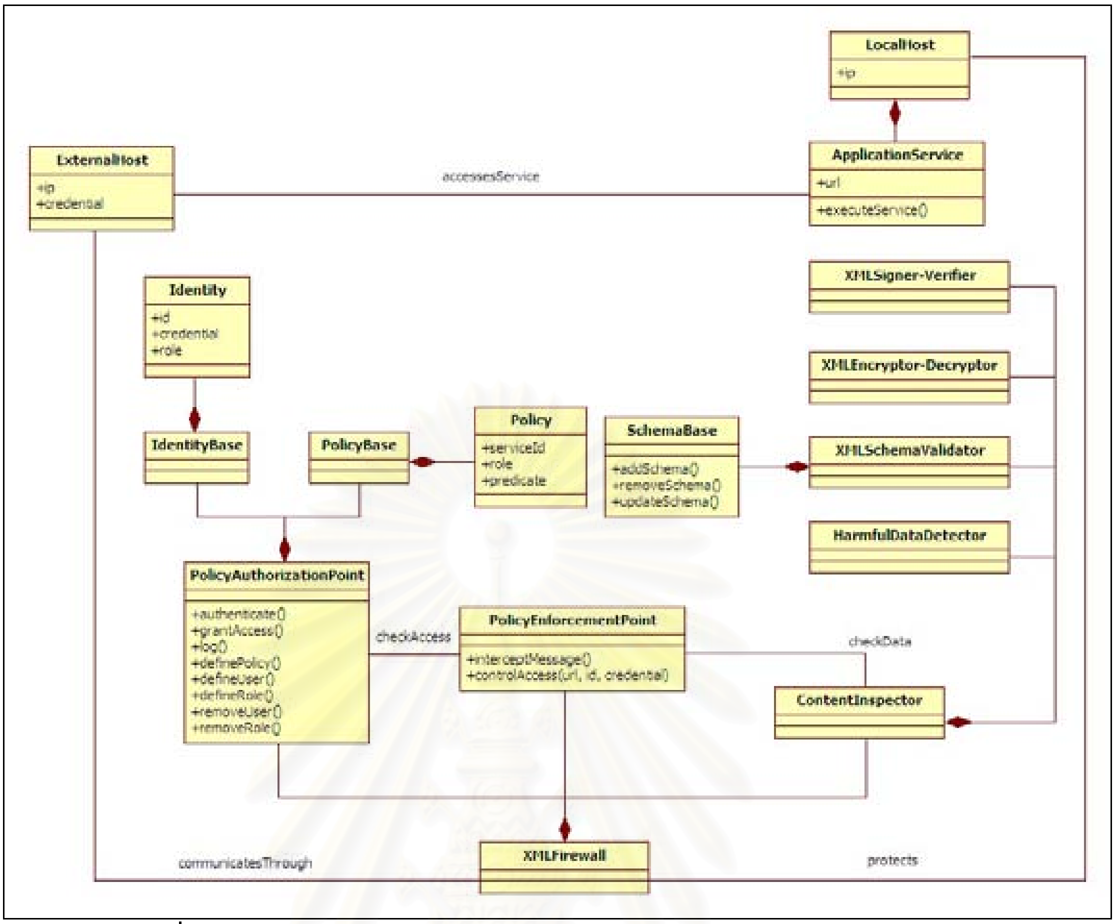
ไฟร์วอลล์สำหรับการกรองเอกซ์เอ็มแอล เป็นไฟร์วอลล์ที่ทำการกรองข้อความเอกซ์เอ็มแอลที่เป็นอันตรายต่อระบบ โดยไฟร์วอลล์ดังกล่าวจะทำงานในระดับแอพพลิเคชันเลเยอร์ (Application Layer Firewall)

ไฟร์วอลล์สำหรับการกรองเอกซ์เอ็มแอล เป็นไฟร์วอลล์ที่ประยุกต์มาจากแบบรูปไฟร์วอลล์เชิงตัวแทนซึ่งเป็นกลุ่มของแบบรูปสถาปัตยกรรมไฟร์วอลล์ ดังรูปที่ ง.6 โดยไฟล์วอลล์เชิงตัวแทนจะควบคุมการรับส่งแพ็คเกจในระดับข้อความของแพ็คเกจ

โดยความต้องการในการแสดงข้อมูลทางโครงสร้างและข้อมูลทางความมั่นคงของระบบไฟร์วอลล์สำหรับการกรองเอกซ์เอ็มแอล ประกอบไปด้วย

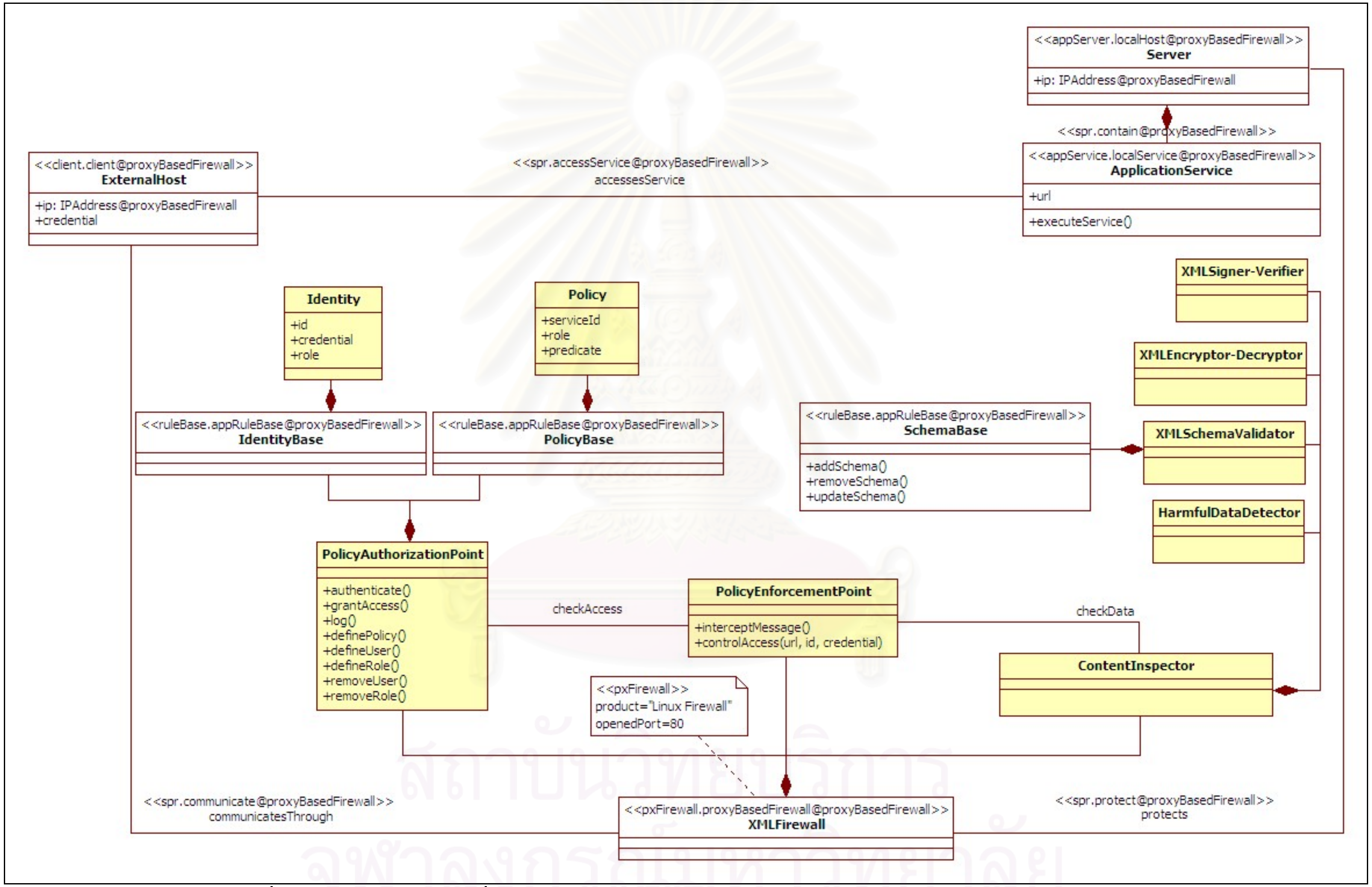
1. ข้อมูลทางโครงสร้างของแบบรูป
    - 1.1. ข้อมูลที่ระบุองค์ประกอบแบบจำลองที่เป็นส่วนประกอบของแบบรูป
    - 1.2. ข้อมูลที่ระบุแบบรูปที่ใช้งาน
    - 1.3. ข้อมูลที่ระบุลำดับของแบบรูป
    - 1.4. ข้อมูลที่ระบุบทบาทของแต่ละองค์ประกอบแบบจำลองในแบบรูป
2. ข้อมูลทางความมั่นคงของแบบรูป
    - 2.1. ผู้เข้าใช้ระบบจากภายนอก
    - 2.2. ไฟร์วอลล์เชิงตัวแทน
    - 2.3. องค์ประกอบที่กรองแพ็คเกจในระดับข้อความในแพ็คเกจ
    - 2.4. บริการของโปรแกรมประยุกต์ในระบบ
    - 2.5. เครื่องบริการโปรแกรมประยุกต์ในระบบ
    - 2.6. ผลิตภัณฑ์ของไฟร์วอลล์
    - 2.7. หมายเลขพอร์ทที่เปิด

ยูเอ็มแอลเซคไม่สามารถแสดงข้อมูลของแบบรูปตามความต้องการของแบบรูปในระบบเอทีเอ็มได้ เนื่องจากขาดองค์ประกอบที่ใช้ในการแสดงข้อมูลของแบบรูปในระบบดังกล่าว



รูปที่ ง.6 แผนภาพคลาสของไฟร์วอลล์สำหรับการกรองเอกซ์เอ็มแอล [22]

จากรูปที่ ง.7 แสดงแผนภาพคลาสที่ใช้ยูเอ็มแอลเซคเอสพีของไฟร์วอลล์สำหรับการกรองเอกซ์เอ็มแอล โดยข้อมูลทางโครงสร้างและข้อมูลทางความมั่นคงของแบบรูปที่อธิบายโดยใช้ยูเอ็มแอลเซคเอสพี ประกอบด้วย คลาสที่ทำหน้าที่เป็นผู้เข้าใช้ระบบจากภายนอกคือ คลาส “ExternalHost” ที่กำกับโดยแม่พิมพ์ต้นแบบ “client” คลาสที่ทำหน้าที่เป็นเครื่องบริการโปรแกรมประยุกต์ในระบบคือ คลาส “Server” ที่กำกับโดยแม่พิมพ์ต้นแบบ “appServer คลาสที่ทำหน้าที่เป็นบริการของโปรแกรมประยุกต์ในระบบคือ คลาส “ApplicationService” ที่กำกับโดยแม่พิมพ์ต้นแบบ “appService” คลาสที่ทำหน้าที่เป็นไฟร์วอลล์เชิงตัวแทนในการรับข้อความเอกซ์เอ็มแอลคือ คลาส “XMLFirewall” ที่กำกับโดยแม่พิมพ์ต้นแบบ “pxFirewall” ที่มีการระบุว่าเป็นไฟร์วอลล์ของลีนุกซ์ที่มีการเปิดพอร์ท 80 คลาสที่ทำหน้าที่เป็นองค์ประกอบที่ตรวจสอบข้อความของแพ็คเกจที่เป็นภาษาเอกซ์เอ็มแอลคือ คลาส “IdentityBase” คลาส “PolicyBase” และคลาส “SchemaBase” ที่กำกับโดยแม่พิมพ์ต้นแบบ “ruleBase”



รูปที่ ง.7 แผนภาพคลาสที่ใช้ยูเอ็มแอลเซคเอสพีของไฟร์วอลล์สำหรับการกรองเอกซ์เอ็มแอล

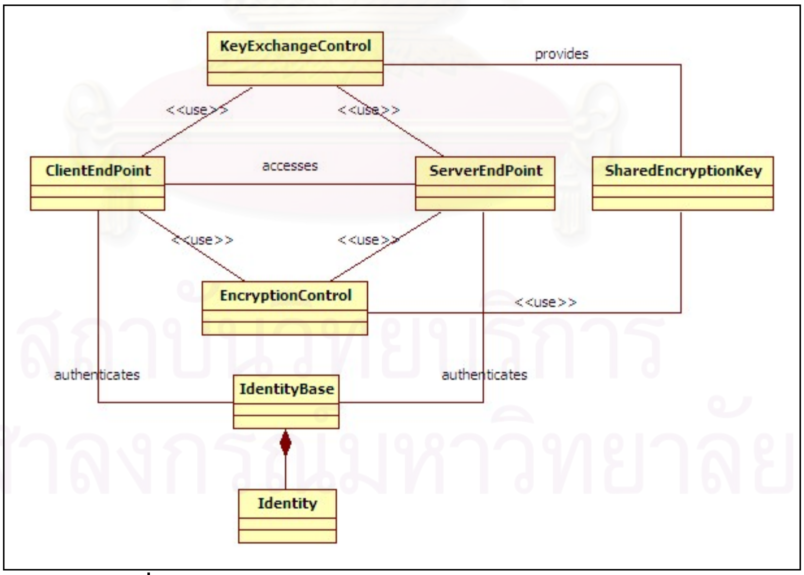
กรณีศึกษาที่ 4: เครือข่ายส่วนตัวเสมือน (Virtual Private Network: VPN)

เครือข่ายส่วนตัวเสมือน เป็นเครือข่ายที่ทำงานโดยใช้โครงสร้างของเครือข่ายสาธารณะ (Public network) หรืออาจวิ่งบนเครือข่ายไอพีก็ได้ แต่ยังสามารถคงความเป็นเครือข่ายเฉพาะขององค์กรได้ด้วยการเข้ารหัสแพ็คเกจก่อนส่งเพื่อให้ข้อมูลมีความปลอดภัยมากขึ้น

เครือข่ายส่วนตัวเสมือน เป็นเครือข่ายที่ประยุกต์มาจากแบบรูปช่องทางความมั่นคง ดังรูปที่ ง.8 ซึ่งเป็นกลุ่มของแบบรูปการประยุกต์ใช้ความมั่นคงบนอินเตอร์เน็ต โดยแบบรูปช่องทางความมั่นคงจะเสนอช่องทางที่มีความปลอดภัยในการแลกเปลี่ยนข้อมูลระหว่างผู้ใช้งานและเครื่องบริการ โดยการเข้ารหัสลับให้กับข้อมูลที่มีการส่งผ่านภายในเครือข่ายดังกล่าว

โดยความต้องการในการแสดงข้อมูลทางโครงสร้างและข้อมูลทางความมั่นคงของระบบเครือข่ายส่วนตัวเสมือน ประกอบไปด้วย

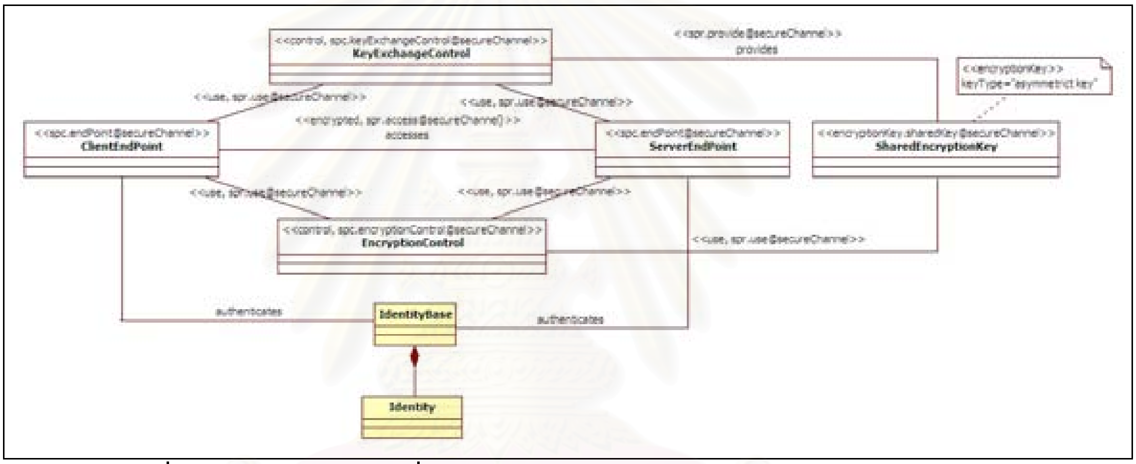
1. ข้อมูลทางโครงสร้างของแบบรูป
    1.1. ข้อมูลที่ระบุองค์ประกอบแบบจำลองที่เป็นส่วนประกอบของแบบรูป
    1.2. ข้อมูลที่ระบุแบบรูปที่ใช้งาน
    1.3. ข้อมูลที่ระบุลำดับของแบบรูป
    1.4. ข้อมูลที่ระบุบทบาทของแต่ละองค์ประกอบแบบจำลองในแบบรูป
2. ข้อมูลทางความมั่นคงของแบบรูป
    2.1. กุญแจที่ใช้ในการเข้ารหัสลับ
    2.2. ประเภทของกุญแจที่ใช้ในการเข้ารหัสลับ



รูปที่ ง.8 แผนภาพคลาสของเครือข่ายส่วนตัวเสมือน

ยูเอ็มแอลเซคไม่สามารถแสดงข้อมูลของแบบรูปตามความต้องการของแบบรูปในระบบเครือข่ายส่วนตัวเสมือนได้ เนื่องจากขาดองค์ประกอบที่ใช้ในการแสดงข้อมูลของแบบรูปในระบบดังกล่าว

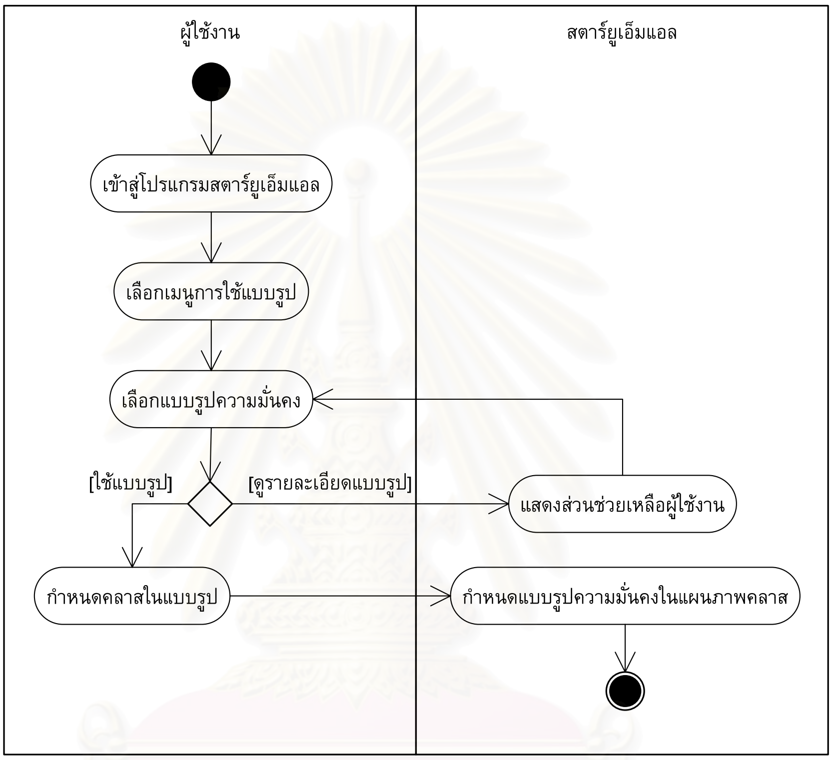
จากรูปที่ ง.9 แสดงแผนภาพคลาสที่ใช้ยูเอ็มแอลเซคเอสพีของเครือข่ายส่วนตัวเสมือน โดยข้อมูลทางโครงสร้างและข้อมูลทางความมั่นคงของแบบรูปความมั่นคงที่อธิบายโดยใช้ยูเอ็มแอลเซคเอสพี ประกอบด้วย คลาส “ClientEndPoint” ที่กำกับโดยแม่พิมพ์ต้นแบบ “spc” เพื่อระบุว่าเป็นองค์ประกอบภายในแบบรูป คลาส “ServerEndPoint” ที่กำกับโดยแม่พิมพ์ต้นแบบ “spc” เพื่อระบุว่าเป็นองค์ประกอบภายในแบบรูป คลาสที่ทำหน้าที่ควบคุมการแลกเปลี่ยนกุญแจที่ใช้ในการเข้ารหัสคือ คลาส “KeyExchangeControl” ที่กำกับโดยแม่พิมพ์ต้นแบบ “control” และ “spc” เพื่อระบุว่าเป็นองค์ประกอบภายในแบบรูป คลาสที่ทำหน้าที่ควบคุมการเข้ารหัสลับคือ คลาส “EncryptionControl” ที่กำกับโดยแม่พิมพ์ต้นแบบ “control” และ “spc” เพื่อระบุว่าเป็นองค์ประกอบภายในแบบรูป และคลาสที่ทำหน้าที่เป็นกุญแจที่ใช้ในการเข้ารหัสคือ คลาส “SharedEncryptionKey” ที่กำกับโดยแม่พิมพ์ต้นแบบ “encryptionKey” ที่เป็นกุญแจเข้ารหัสแบบอสมมาตร



รูปที่ ง.9 แผนภาพคลาสที่ใช้ยูเอ็มแอลเซคเอสพีของเครือข่ายส่วนตัวเสมือน

ภาคผนวก จ
ตัวอย่างการใช้งานเครื่องมือต้นแบบและผลลัพธ์ที่ได้จากเครื่องมือ

ภายหลังจากพัฒนาเครื่องมือต้นแบบสำหรับแสดงแบบรูปความมั่นคงแล้ว เพื่อแสดงให้เห็นถึงฟังก์ชันงานและการใช้งานของเครื่องมือ สามารถแสดงภาพรวมของการใช้เครื่องมือด้วยแผนภาพกิจกรรมดังรูป จ.1



รูปที่ จ.1 แผนภาพกิจกรรมแสดงการใช้งานเครื่องมือต้นแบบ

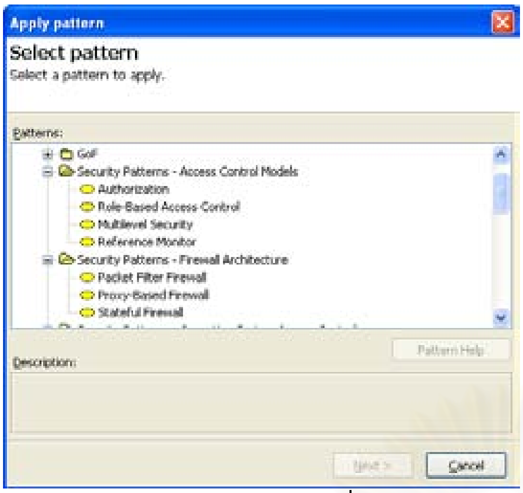
ในภาคผนวกนี้ จะนำเสนอตัวอย่างการใช้งานเครื่องมือต้นแบบได้ทำการพัฒนาไว้แล้วบนพื้นฐานของไวยากรณ์ที่สร้างขึ้น โดยจะนำเสนอ

1) ขอบเขตของแบบรูปความมั่นคงที่เครื่องมือสนับสนุน
2) ตัวอย่างการใช้งานแบบรูปการให้อำนาจและผลลัพธ์ที่ได้จากเครื่องมือ

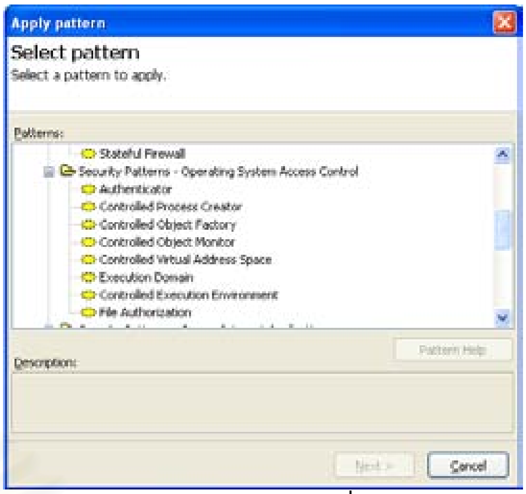
โดยมีรายละเอียดดังนี้

ง.1 ขอบเขตของแบบรูปความมั่นคงที่เครื่องมือสนับสนุน

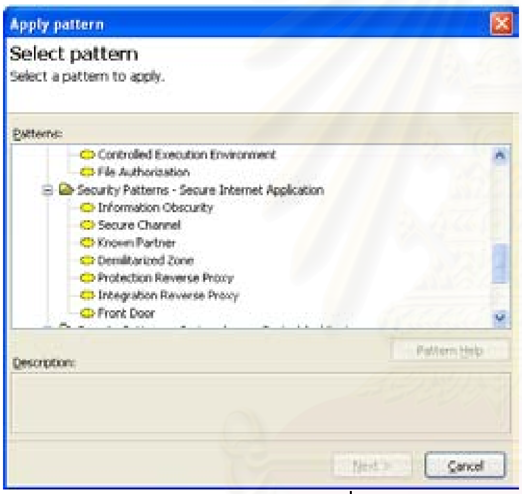
ขอบเขตแบบรูปความมั่นคงที่สนับสนุนโดยเครื่องมือนั้น จะเป็นไปตามขอบเขตงานวิจัย โดยจำแนกออกเป็น 5 กลุ่ม 27 แบบรูปความมั่นคง ดังแสดงในรูปที่ จ.2



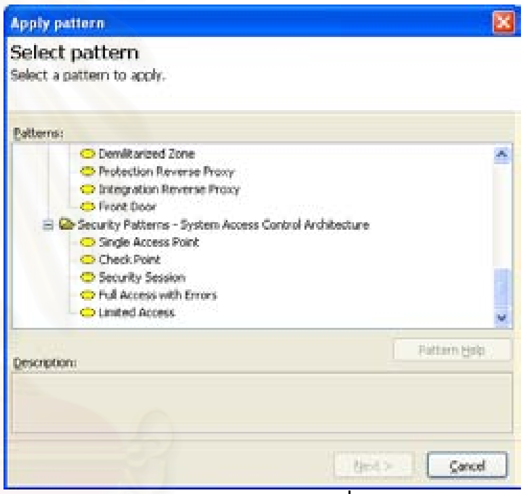
(ก) รายการแบบรูปความมั่นคง
ในกลุ่มแบบจำลองการควบคุมการเข้าถึงและ
สถาปัตยกรรมไฟร์วอลล์



(ข) รายการแบบรูปความมั่นคง
ในกลุ่มการควบคุมการเข้าถึงระบบปฏิบัติการ



(ค) รายการแบบรูปความมั่นคง
ในกลุ่มการประยุกต์ใช้ความมั่นคงบนอินเตอร์เน็ต



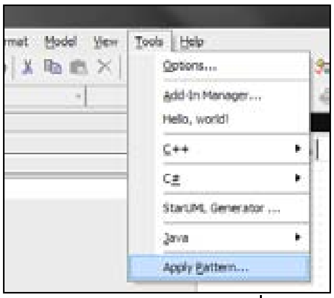
(ง) รายการแบบรูปความมั่นคง
ในกลุ่มสถาปัตยกรรมการควบคุมการเข้าถึงระบบ

รูปที่ จ.2 แบบรูปความมั่นคงที่มีในเครื่องมือต้นแบบ

ง.2 ตัวอย่างการใช้งานแบบรูปการให้อำนาจและผลลัพธ์ที่ได้จากเครื่องมือ

เพื่อแสดงให้เห็นขั้นตอนการใช้งานจริง ในที่นี้จะขอยกตัวอย่างการใช้งานรูปการให้อำนาจ เพื่อสร้างเป็นแผนภาพคลาสที่แสดงแบบรูปการให้อำนาจ โดยในการใช้งานเครื่องมือจะต้องทำการเปิดโปรแกรมสตาร์ยูเอ็มแอล และเลือกเมนูการใช้แบบรูปความมั่นคง ดังรูปที่ จ.3

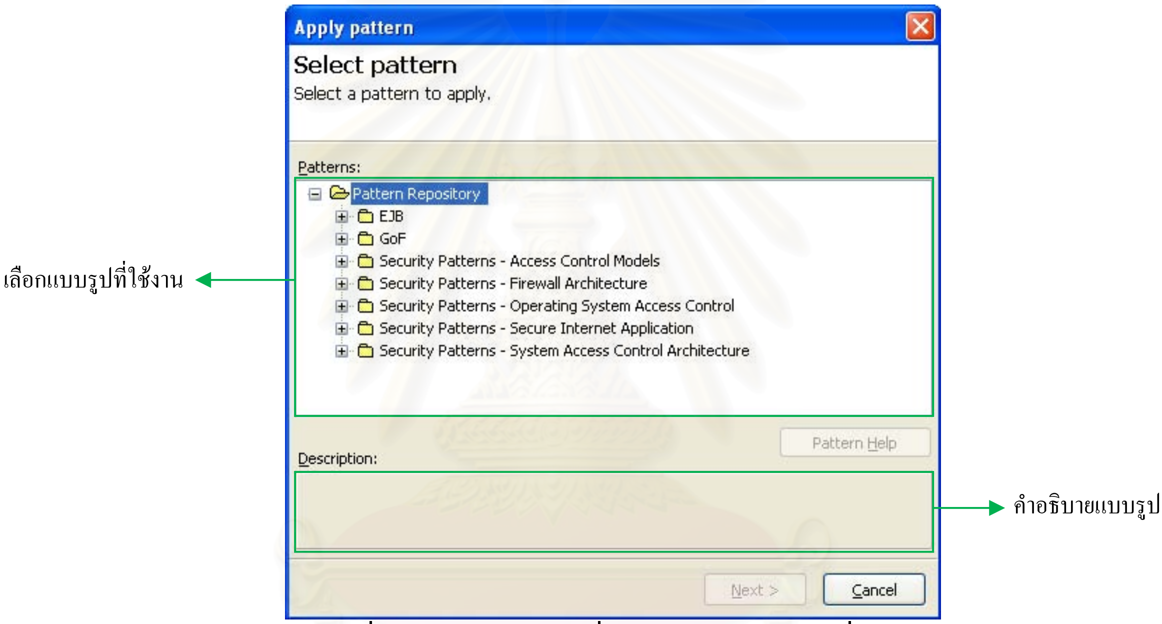
(ก) เปิดโปรแกรมสตาร์ยูเอ็มแอล



(ข) เลือกใช้แบบรูปความมั่นคง

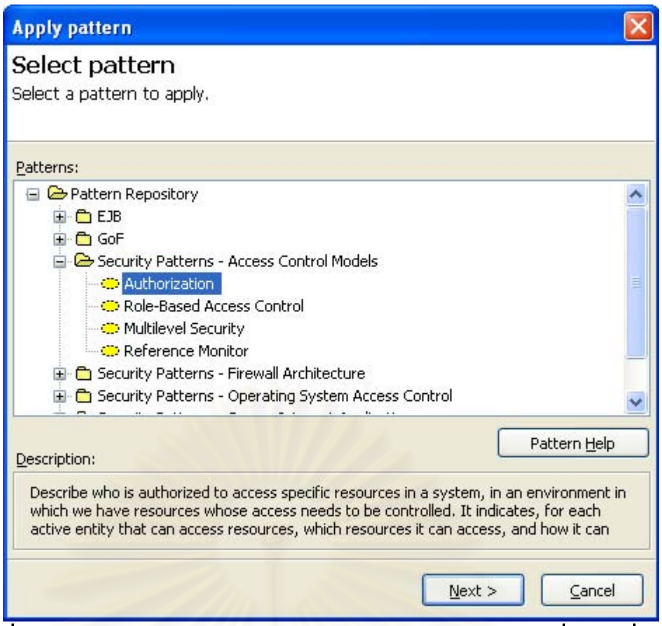
รูปที่ จ.3 ขั้นตอนการเข้าใช้แบบรูปความมั่นคงในโปรแกรมสตาร์ยูเอ็มแอล

ภายหลังขั้นตอนการเข้าใช้แบบรูปความมั่นคงในโปรแกรมแล้ว จะปรากฏหน้าจอหลักเพื่อเลือกแบบรูปความมั่นคง ดังรูปที่ จ.4



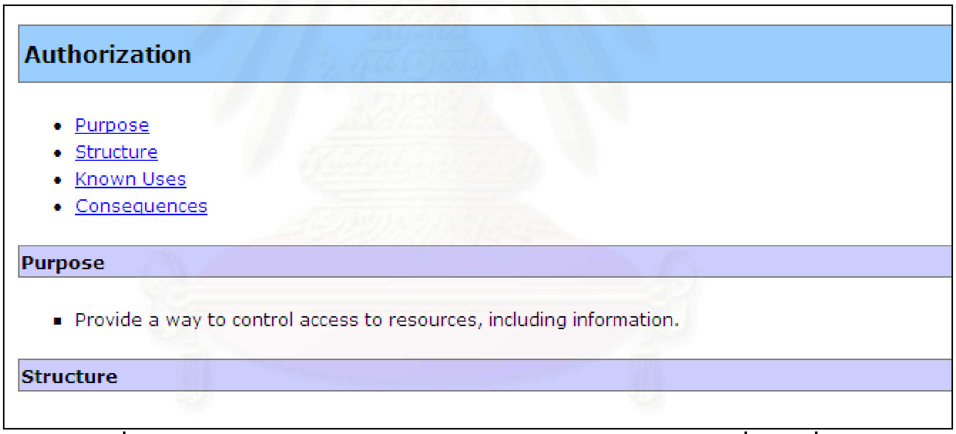
รูปที่ จ.4 หน้าจอหลักเพื่อเลือกแบบรูปความมั่นคง

เลือก “Authorization” ในกลุ่ม “Security Pattern - Access Control Models” เพื่อเลือกใช้แบบรูปการให้อำนาจ จากนั้นเครื่องมือจะแสดงคำอธิบายของแบบรูปนั้นๆ ดังรูป จ.5



รูปที่ จ.5 หน้าจอหลักแสดงคำอธิบายแบบรูปความมั่นคงที่เลือก

นอกจากคำอธิบายแบบรูปความมั่นคงแล้ว ผู้ใช้งานสามารถเข้าไปดูรายละเอียดของแต่ละแบบรูปความมั่นคงได้โดยเลือก “Pattern Help” ดังรูปที่ จ.6



รูปที่ จ.6 หน้าจอหลักแสดงรายละเอียดของแบบรูปความมั่นคงที่เลือก

โดยรายละเอียดของแบบรูปความมั่นคงประกอบด้วย

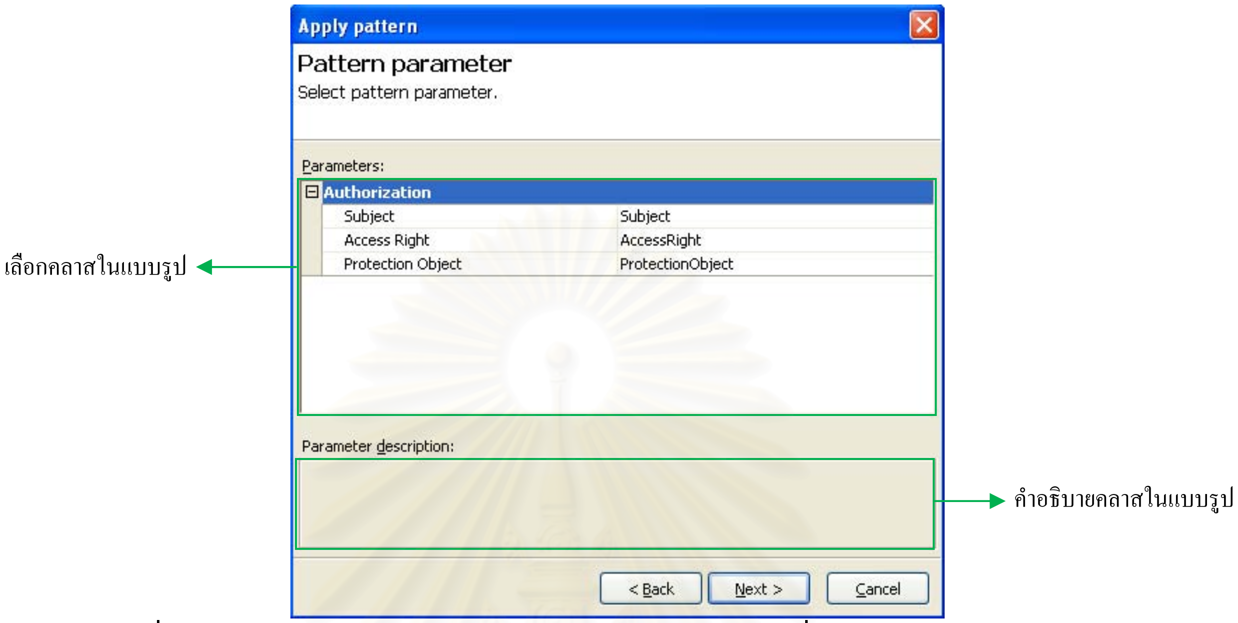
1) จุดประสงค์ในการใช้งานแบบรูป (Purpose) เป็นจุดประสงค์ของการใช้แบบรูปดังกล่าว

2) โครงสร้างของแบบรูป (Structure) เป็นโครงสร้างของการออกแบบที่ใช้ในการแก้ไขปัญหาของแบบรูป รวมทั้งรายละเอียดของแต่ละองค์ประกอบในโครงสร้าง

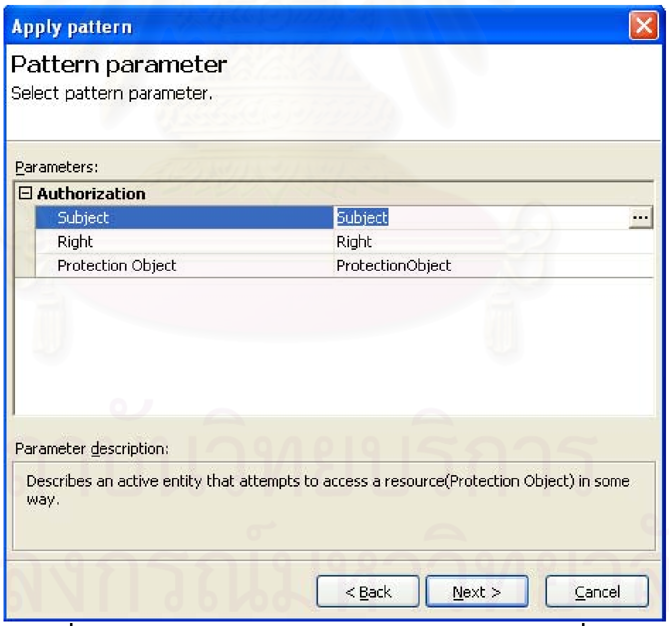
3) ตัวอย่างของการประยุกต์ใช้งาน (Known Uses) เป็นตัวอย่างที่ประยุกต์ใช้แบบรูปดังกล่าว

4) ประโยชน์ที่จะได้รับ (Consequence) เป็นประโยชน์ที่ได้รับเมื่อประยุกต์ใช้แบบรูปดังกล่าว

เมื่อผู้ใช้งานเลือกแบบรูปความมั่นคงแล้ว จะปรากฏหน้าจอหลักสำหรับการสร้างหรือเลือกคลาสที่เป็นองค์ประกอบของแบบรูปความมั่นคง ดังรูปที่ จ.7 เมื่อผู้ใช้งานเลือกคลาสในแบบรูปจะปรากฏคำอธิบายของคลาสที่เลือก ดังรูปที่ จ.8

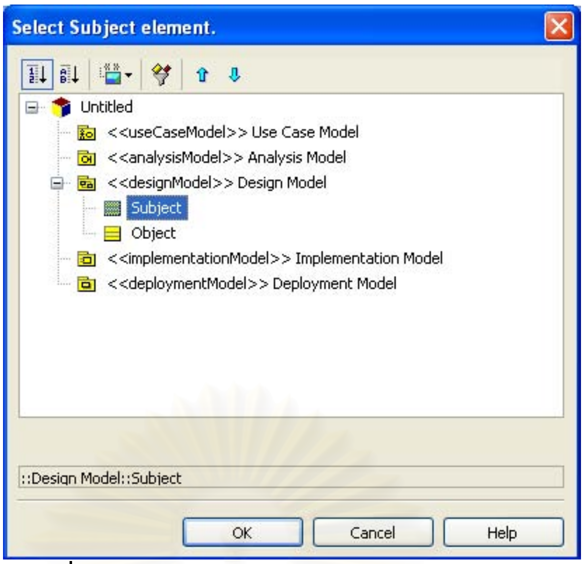


รูปที่ จ.7 หน้าจอหลักสำหรับการเลือกคลาสหรือสร้างคลาสที่เป็นองค์ประกอบในแบบรูป

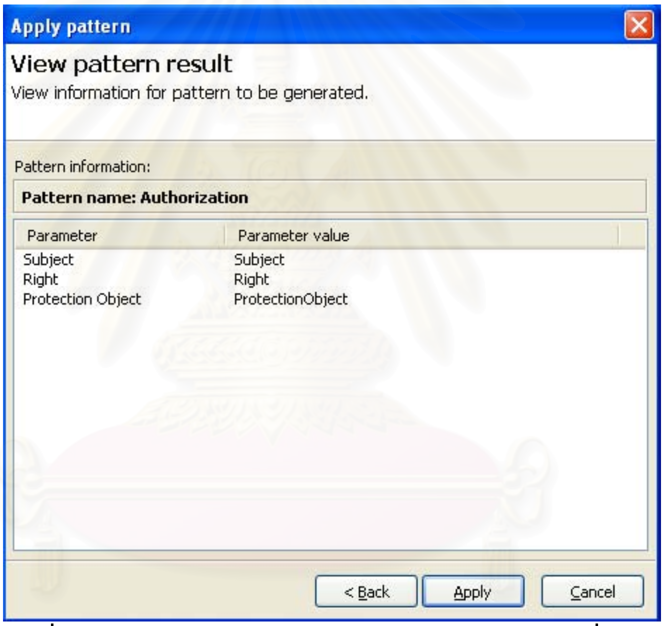


รูปที่ จ.8 หน้าจอหลักแสดงคำอธิบายของคลาสที่เลือก

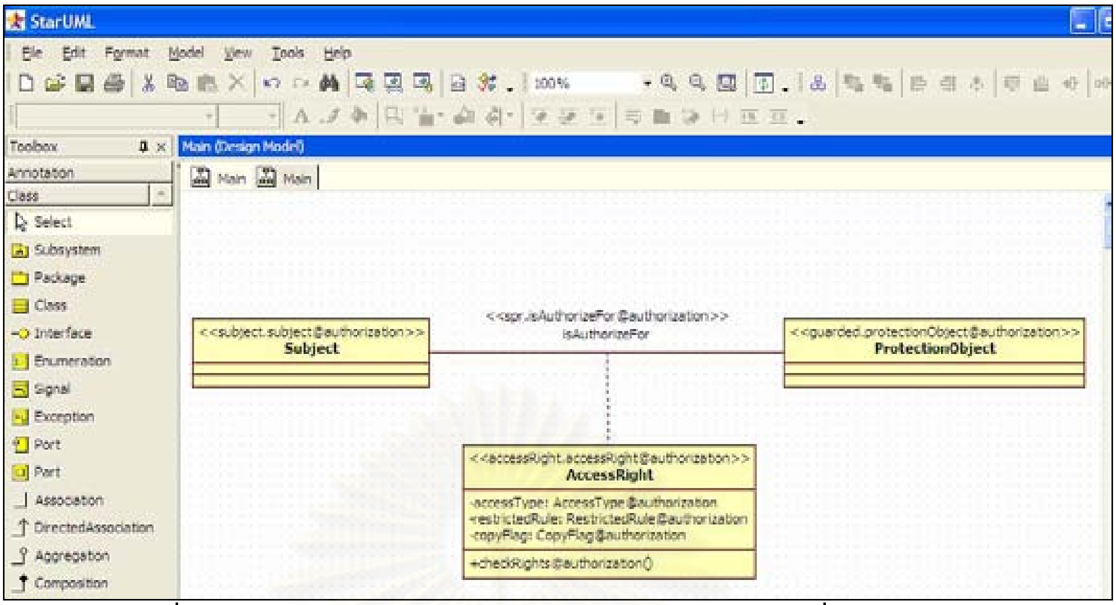
เมื่อผู้ใช้งานได้สร้างคลาสในโครงการไว้ก่อนหน้าแล้ว จะสามารถเลือกคลาสในโครงการให้เป็นคลาสในแบบรูปที่เลือกได้ดังรูปที่ จ.9 หลังจากที่เลือกคลาสในแบบรูปแล้ว จะเป็นขั้นตอนของการยืนยันการใช้แบบรูปความมั่นคงในโครงการดังรูปที่ จ.10 โดยผลลัพธ์จากการใช้แบบรูปการให้อำนาจในโครงการแสดงดังรูปที่ จ.11



รูปที่ จ.9 หน้าจอสำหรับเลือกคลาสในโครงการ



รูปที่ จ.10 หน้าจอสำหรับการยืนยันการใช้แบบรูปที่เลือก



รูปที่ จ.11 ผลลัพธ์จากการใช้แบบรูปการให้อำนาจโดยใช้เครื่องมือต้นแบบ

ภาคผนวก ฉ
การเปรียบเทียบการแสดงแบบรูปความมั่นคง
ของยูเอ็มแอล ยูเอ็มแอลเซค และยูเอ็มแอลเซคเอสพี

การเปรียบเทียบการแสดงแบบรูปความมั่นคงของยูเอ็มแอล ยูเอ็มแอลเซค และยูเอ็มแอลเซคเอสพี ประกอบไปด้วย การเปรียบเทียบการแสดงข้อมูลทางโครงสร้างของแบบรูปความมั่นคง และการเปรียบเทียบการแสดงข้อมูลทางความมั่นคงในแต่ละแบบรูปความมั่นคง โดยใช้ยูเอ็มแอล ยูเอ็มแอลเซค และยูเอ็มแอลเซคเอสพีที่ได้จากงานวิทยานิพนธ์นี้ ช่วยแสดงข้อมูลดังกล่าว โดยรายละเอียดของการเปรียบเทียบมีดังต่อไปนี้

ตารางที่ ฉ.1 การเปรียบเทียบการแสดงข้อมูลทางโครงสร้างของแบบรูปความมั่นคง

ยูเอ็มแอล	ยูเอ็มแอลเซค	ยูเอ็มแอลเซคเอสพี
ไม่ได้แสดงข้อมูลทางโครงสร้างของแบบรูปในแผนภาพคือ 1. องค์ประกอบแบบจำลองที่เป็นส่วนประกอบของแบบรูป 2. แบบรูปที่ใช้งาน 3. ลำดับของแบบรูปในแผนภาพ 4. บทบาทของแต่ละองค์ประกอบแบบจำลองในแบบรูป	เช่นเดียวกับการแสดงข้อมูลทางโครงสร้างของยูเอ็มแอล	แสดงข้อมูลทางโครงสร้างของแบบรูปคือ 1. ใช้แม่พิมพ์ต้นแบบ spc spt และ spr แสดงองค์ประกอบแบบจำลองที่เป็นส่วนประกอบของแบบรูป 2. ใช้ป้ายระบุ “role@name[instance]” แสดงบทบาทขององค์ประกอบในแบบรูป แบบรูปที่ใช้งาน และลำดับของแบบรูป

ตารางที่ ฉ.2 การเปรียบเทียบการแสดงข้อมูลทางความมั่นคงในแต่ละแบบรูปความมั่นคง

แบบรูปความมั่นคง	ยูเอ็มแอล	ยูเอ็มแอลเซค	ยูเอ็มแอลเซคเอสพี
การให้อำนาจ (Authorization)	ไม่ได้แสดงข้อมูลทางความมั่นคงในแผนภาพคือ 1. ผู้เข้าใช้ทรัพยากร 2. องค์ประกอบที่ควบคุมการเข้าถึงทรัพยากร 3. ทรัพยากรที่ถูกควบคุม 4. ลักษณะของการเข้าถึงทรัพยากร 5. เงื่อนไขต้องห้ามในการให้อำนาจแก่ผู้ใช้งาน 6. ลักษณะในการอนุญาตให้ผู้อื่นคัดลอกอำนาจของผู้ใช้งานดังกล่าว 7. อ็อบเจกต์ที่ควบคุมการเข้าถึงทรัพยากร 8. ประเภทขององค์ประกอบที่ควบคุมการเข้าถึงทรัพยากร	แสดงข้อมูลทางความมั่นคงในแผนภาพคือ 1. ใช้แม่พิมพ์ต้นแบบ “guarded” แสดงทรัพยากรที่ถูกควบคุม 2. ใช้ป้ายระบุ “guard” ของแม่พิมพ์ต้นแบบ “guarded” แสดงอ็อบเจกต์ที่ควบคุมการเข้าถึงทรัพยากร	แสดงข้อมูลทางความมั่นคงที่อยู่ในแผนภาพคือ 1. ใช้แม่พิมพ์ต้นแบบ “subject” แสดงผู้เข้าใช้ทรัพยากร 2. ใช้แม่พิมพ์ต้นแบบ “accessRight” แสดงองค์ประกอบที่ควบคุมการเข้าถึงทรัพยากร 3. ใช้แม่พิมพ์ต้นแบบ “guarded” แสดงทรัพยากรที่ถูกควบคุม 4. ใช้แม่พิมพ์ต้นแบบ “accessType” แสดงลักษณะของการเข้าถึงทรัพยากร 5. ใช้แม่พิมพ์ต้นแบบ “restrictedRule” แสดงคุณลักษณะที่แสดงเงื่อนไขต้องห้ามในการให้อำนาจแก่ผู้ใช้งาน 6. ใช้แม่พิมพ์ต้นแบบ “copyFlag” แสดงคุณลักษณะที่แสดงการอนุญาตให้ผู้อื่นคัดลอกอำนาจของผู้ใช้งานดังกล่าว 7. ใช้ป้ายระบุ “guard” ของแม่พิมพ์ต้นแบบ “guarded” แสดงอ็อบเจกต์ที่ควบคุมการเข้าถึงทรัพยากร 8. ใช้ป้ายระบุ “controlledType” ของแม่พิมพ์ต้นแบบ “accessRight” แสดงประเภทขององค์ประกอบที่ควบคุมการเข้าถึงทรัพยากร
การควบคุมการเข้าถึงเชิงบทบาท (Role-Based Access Control)	ไม่ได้แสดงข้อมูลทางความมั่นคงที่อยู่ในแผนภาพคือ 1. ผู้เข้าใช้ทรัพยากร 2. บทบาทของผู้เข้าใช้ทรัพยากร 3. บทบาทของผู้ดูแลการเข้าใช้ทรัพยากรในระบบ 4. องค์ประกอบที่ควบคุมการเข้าถึงทรัพยากร 5. องค์ประกอบที่ควบคุมการเข้าถึงทรัพยากรของผู้ดูแล 6. ทรัพยากรที่ถูกควบคุม 7. ลักษณะของการเข้าถึงทรัพยากร 8. เงื่อนไขต้องห้ามในการให้อำนาจแก่ผู้ใช้งาน 9. ลักษณะในการอนุญาตให้ผู้อื่นคัดลอกอำนาจของผู้ใช้งานดังกล่าว 10. อ็อบเจกต์ที่ควบคุมการเข้าถึงทรัพยากร 11. ประเภทขององค์ประกอบที่ควบคุมการเข้าถึงทรัพยากร	แสดงข้อมูลทางความมั่นคงในแผนภาพคือ 1. ใช้แม่พิมพ์ต้นแบบ “guarded” แสดงทรัพยากรที่ถูกควบคุม 2. ใช้ป้ายระบุ “guard” ของแม่พิมพ์ต้นแบบ “guarded” แสดงอ็อบเจกต์ที่ควบคุมการเข้าถึงทรัพยากร	แสดงข้อมูลทางความมั่นคงที่อยู่ในแผนภาพคือ 1. ใช้แม่พิมพ์ต้นแบบ “subject” แสดงผู้เข้าใช้ทรัพยากร 2. ใช้แม่พิมพ์ต้นแบบ “role” แสดงบทบาทของผู้เข้าใช้ทรัพยากร 3. ใช้แม่พิมพ์ต้นแบบ “adminRole” แสดงบทบาทของผู้ดูแลการเข้าใช้ทรัพยากร 4. ใช้แม่พิมพ์ต้นแบบ “accessRight” แสดงองค์ประกอบที่ควบคุมการเข้าถึงทรัพยากร 5. ใช้แม่พิมพ์ต้นแบบ “adminRight” แสดงองค์ประกอบที่ควบคุมการเข้าถึงทรัพยากรของผู้ดูแล 6. ใช้แม่พิมพ์ต้นแบบ “guarded” แสดงทรัพยากรที่ถูกควบคุม 7. ใช้แม่พิมพ์ต้นแบบ “accessType” แสดงลักษณะของการเข้าถึงทรัพยากร 8. ใช้แม่พิมพ์ต้นแบบ “restrictedRule” แสดงคุณลักษณะที่แสดงเงื่อนไขต้องห้ามในการให้อำนาจแก่ผู้ใช้งาน 9. ใช้แม่พิมพ์ต้นแบบ “copyFlag” แสดงคุณลักษณะที่แสดงการอนุญาตให้ผู้อื่นคัดลอกอำนาจของผู้ใช้งานดังกล่าว 10. ใช้ป้ายระบุ “guard” ของแม่พิมพ์ต้นแบบ “guarded” แสดงอ็อบเจกต์ที่ควบคุมการเข้าถึงทรัพยากร

ตารางที่ ฉ.2 การเปรียบเทียบการแสดงข้อมูลทางความมั่นคงในแต่ละแบบรูปความมั่นคง (ต่อ)

แบบรูปความมั่นคง	ยูเอ็มแอล	ยูเอ็มแอลเซค	ยูเอ็มแอลเซคเอสพี
การควบคุมการเข้าถึงเชิงบทบาท (Role-Based Access Control)			11. ใช้ป้ายระบุ "controlledType" ของแม่พิมพ์ต้นแบบ "accessRight" แสดงประเภทขององค์ประกอบที่ควบคุมการเข้าถึงทรัพยากร
ความมั่นคงหลายระดับ (Multilevel Security)	ไม่ได้แสดงข้อมูลทางความมั่นคงในแผนภาพคือ 1. ผู้เข้าใช้ทรัพยากร 2. ทรัพยากรที่ถูกควบคุม 3. ระดับการเข้าถึงของผู้เข้าใช้ทรัพยากร 4. ระดับความปลอดภัยของทรัพยากร 5. อ็อบเจกต์ที่ควบคุมการเข้าถึงทรัพยากร 6. อ็อบเจกต์ที่เป็นผู้กำหนดระดับการเข้าถึงของผู้เข้าใช้ทรัพยากร 7. อ็อบเจกต์ที่เป็นผู้กำหนดระดับความปลอดภัยของทรัพยากร	แสดงข้อมูลทางความมั่นคงในแผนภาพคือ 1. ใช้แม่พิมพ์ต้นแบบ "guarded" แสดงทรัพยากรที่ถูกควบคุม 2. ใช้ป้ายระบุ "guard" ของแม่พิมพ์ต้นแบบ "guarded" แสดงอ็อบเจกต์ที่ควบคุมการเข้าถึงทรัพยากร	แสดงข้อมูลทางความมั่นคงในแผนภาพคือ 1. ใช้แม่พิมพ์ต้นแบบ "subject" แสดงผู้เข้าใช้ทรัพยากร 2. ใช้แม่พิมพ์ต้นแบบ "guarded" แสดงทรัพยากรที่ถูกควบคุม 3. ใช้แม่พิมพ์ต้นแบบ "accessLevel" แสดงระดับการเข้าถึงของผู้เข้าใช้ทรัพยากร 4. ใช้แม่พิมพ์ต้นแบบ "guardLevel" แสดงระดับความปลอดภัยของทรัพยากรในระบบ 5. ใช้ป้ายระบุ "guard" ของแม่พิมพ์ต้นแบบ "guarded" แสดงอ็อบเจกต์ที่ควบคุมการเข้าถึงทรัพยากร 6. ใช้ป้ายระบุ "assign" ของแม่พิมพ์ต้นแบบ "accessLevel" แสดงอ็อบเจกต์ที่เป็นผู้กำหนดระดับการเข้าถึงของผู้เข้าใช้ทรัพยากร 7. ใช้ป้ายระบุ "assign" ของแม่พิมพ์ต้นแบบ "guardLevel" แสดงอ็อบเจกต์ที่เป็นผู้กำหนดระดับความปลอดภัยของทรัพยากร
การเฝ้าสังเกตเชิงอ้างอิง (Reference Monitor)	ไม่ได้แสดงข้อมูลทางความมั่นคงในแผนภาพคือ 1. ผู้เข้าใช้ทรัพยากร 2. คำร้องขอใช้ทรัพยากร 3. องค์ประกอบที่ตรวจสอบการร้องขอใช้ทรัพยากร 4. องค์ประกอบที่ควบคุมการเข้าถึงทรัพยากร 5. ทรัพยากรที่ถูกควบคุม 6. การเชื่อมโยงที่มีการตรวจสอบการร้องขอใช้ทรัพยากร 7. อ็อบเจกต์ที่ควบคุมการเข้าถึงทรัพยากร 8. อ็อบเจกต์ที่ตรวจสอบคำร้องขอ 9. ประเภทขององค์ประกอบที่ควบคุมการเข้าถึงทรัพยากร	แสดงข้อมูลทางความมั่นคงในแผนภาพคือ 1. ใช้แม่พิมพ์ต้นแบบ "guarded" แสดงทรัพยากรที่ถูกควบคุม 2. ใช้ป้ายระบุ "guard" ของแม่พิมพ์ต้นแบบ "guarded" แสดงอ็อบเจกต์ที่ควบคุมการเข้าถึงทรัพยากร	แสดงข้อมูลทางความมั่นคงที่อยู่ในแผนภาพคือ 1. ใช้แม่พิมพ์ต้นแบบ "subject" แสดงผู้เข้าใช้ทรัพยากร 2. ใช้แม่พิมพ์ต้นแบบ "request" แสดงคำร้องขอใช้ทรัพยากรในระบบ 3. ใช้แม่พิมพ์ต้นแบบ "referenceMonitor" แสดงองค์ประกอบที่ตรวจสอบการร้องขอใช้ทรัพยากร 4. ใช้แม่พิมพ์ต้นแบบ "accessRight" แสดงองค์ประกอบที่ควบคุมการเข้าถึงทรัพยากร 5. ใช้แม่พิมพ์ต้นแบบ "guarded" แสดงทรัพยากรที่ถูกควบคุม 6. ใช้แม่พิมพ์ต้นแบบ "monitored" แสดงการเชื่อมโยงที่มีการตรวจสอบการร้องขอใช้ทรัพยากร 7. ใช้ป้ายระบุ "guard" ของแม่พิมพ์ต้นแบบ "guarded" แสดงอ็อบเจกต์ที่ควบคุมการเข้าถึงทรัพยากร 8. ใช้ป้ายระบุ "monitor" ของแม่พิมพ์ต้นแบบ "monitored" แสดงอ็อบเจกต์ที่ตรวจสอบคำร้องขอ 9. ใช้ป้ายระบุ "controlledType" ของแม่พิมพ์ต้นแบบ "accessRight" แสดงประเภทขององค์ประกอบที่ควบคุมการเข้าถึงทรัพยากร

ตารางที่ ฉ.2 การเปรียบเทียบการแสดงข้อมูลทางความมั่นคงในแต่ละแบบรูปความมั่นคง (ต่อ)

แบบรูปความมั่นคง	ยูเอ็มแอล	ยูเอ็มแอลเซค	ยูเอ็มแอลเซคเอสพี
จุดเข้าระบบเดี่ยว (Single Access Point)	ไม่ได้แสดงข้อมูลทางความมั่นคงในแผนภาพคือ 1. ผู้ใช้งานจากภายนอกระบบ 2. จุดเข้าระบบ 3. บริการในระบบ 4. วิธีในการเข้าสู่ระบบ	เช่นเดียวกับการแสดงข้อมูลทางความมั่นคงของยูเอ็มแอล	แสดงข้อมูลทางความมั่นคงที่อยู่ในแผนภาพคือ 1. ใช้แม่พิมพ์ต้นแบบ “client” แสดงผู้ใช้งานจากภายนอกระบบ 2. ใช้แม่พิมพ์ต้นแบบ “accessPoint” แสดงจุดเข้าระบบ 3. ใช้แม่พิมพ์ต้นแบบ “appService” แสดงบริการในระบบ 4. ใช้ป้ายระบุ “method” ของแมพิมพ์ต้นแบบ “accessPoint” แสดงวิธีในการเข้าสู่ระบบ
จุดตรวจสอบ (Check Point)	ไม่ได้แสดงข้อมูลทางความมั่นคงในแผนภาพคือ 1. ผู้ใช้งานจากภายนอกระบบ 2. จุดเข้าระบบ 3. บริการในระบบ 4. จุดตรวจสอบผู้ใช้งาน 5. วิธีในการเข้าสู่ระบบ 6. บริการที่ต้องการตรวจสอบโดยใช้จุดตรวจสอบ	เช่นเดียวกับการแสดงข้อมูลทางความมั่นคงของยูเอ็มแอล	แสดงข้อมูลทางความมั่นคงที่อยู่ในแผนภาพคือ 1. ใช้แม่พิมพ์ต้นแบบ “client” แสดงผู้ใช้งานจากภายนอกระบบ 2. ใช้แม่พิมพ์ต้นแบบ “accessPoint” แสดงจุดเข้าระบบ 3. ใช้แม่พิมพ์ต้นแบบ “appService” แสดงบริการในระบบ 4. ใช้แม่พิมพ์ต้นแบบ “checkPoint” แสดงจุดตรวจสอบผู้ใช้งาน 5. ใช้ป้ายระบุ “method” ของแมพิมพ์ต้นแบบ “accessPoint” แสดงวิธีในการเข้าสู่ระบบ 6. ใช้ป้ายระบุ “protect” ของแม่พิมพ์ต้นแบบ “checkPoint” แสดงบริการที่ต้องการตรวจสอบโดยใช้จุดตรวจสอบ
เซสชันทางความมั่นคง (Security Session)	ไม่ได้แสดงข้อมูลทางความมั่นคงในแผนภาพคือ 1. ผู้ใช้งานจากภายนอกระบบ 2. จุดเข้าระบบ 3. บริการในระบบ 4. จุดตรวจสอบผู้ใช้งาน 5. เซสชันทางความมั่นคง 6. วิธีในการเข้าสู่ระบบ 7. บริการที่ต้องการตรวจสอบโดยใช้จุดตรวจสอบ 8. ประเภทของเซสชันทางความมั่นคง 9. อายุการใช้งานของเซสชันทางความมั่นคง	เช่นเดียวกับการแสดงข้อมูลทางความมั่นคงของยูเอ็มแอล	แสดงข้อมูลทางความมั่นคงที่อยู่ในแผนภาพคือ 1. ใช้แม่พิมพ์ต้นแบบ “client” แสดงผู้ใช้งานจากภายนอกระบบ 2. ใช้แม่พิมพ์ต้นแบบ “accessPoint” แสดงจุดเข้าระบบ 3. ใช้แม่พิมพ์ต้นแบบ “appService” แสดงบริการในระบบ 4. ใช้แม่พิมพ์ต้นแบบ “checkPoint” แสดงจุดตรวจสอบผู้ใช้งาน 5. ใช้แม่พิมพ์ต้นแบบ “securitySession” แสดงเซสชันทางความมั่นคง 6. ใช้ป้ายระบุ “method” ของแมพิมพ์ต้นแบบ “accessPoint” แสดงวิธีในการเข้าสู่ระบบ 7. ใช้ป้ายระบุ “protect” ของแม่พิมพ์ต้นแบบ “checkPoint” แสดงบริการที่ต้องการตรวจสอบโดยใช้จุดตรวจสอบ 8. ป้ายระบุ “sessionType” ของแม่พิมพ์ต้นแบบ “securitySession” แสดงประเภทของเซสชันทางความมั่นคง 9. ป้ายระบุ “lifetime” ของแม่พิมพ์ต้นแบบ “securitySession” แสดงอายุการใช้งานของเซสชัน

ตารางที่ ฉ.2 การเปรียบเทียบการแสดงข้อมูลทางความมั่นคงในแต่ละแบบรูปความมั่นคง (ต่อ)

แบบรูปความมั่นคง	ยูเอ็มแอล	ยูเอ็มแอลเซค	ยูเอ็มแอลเซคเอสพี
การควบคุมการเข้าถึงด้วยการแสดงความผิดพลาด (Full Access with Errors)	ไม่ได้แสดงข้อมูลทางความมั่นคงในแผนภาพคือ 1. ผู้ใช้งานจากภายนอกระบบ 2. องค์ประกอบที่ควบคุมการเข้าถึงส่วนต่อประสานของระบบ 3. บริการของโปรแกรมประยุกต์ภายในระบบ 4. องค์ประกอบที่แสดงข้อผิดพลาดที่เกิดจากการเข้าถึงการดำเนินการที่ไม่มีสิทธิ์ในการเข้าถึง 5. ประเภทขององค์ประกอบที่ควบคุมการเข้าถึงบริการในระบบ	เช่นเดียวกับการแสดงข้อมูลทางความมั่นคงของยูเอ็มแอล	แสดงข้อมูลทางความมั่นคงที่อยู่ในแผนภาพคือ 1. ใช้แม่พิมพ์ต้นแบบ “client” แสดงผู้ใช้งานจากภายนอกระบบ 2. ใช้แม่พิมพ์ต้นแบบ “accessRight” แสดงองค์ประกอบที่ควบคุมการเข้าถึงส่วนต่อประสานของระบบ 3. ใช้แม่พิมพ์ต้นแบบ “appService” แสดงบริการของโปรแกรมประยุกต์ภายในระบบ 4. ใช้แม่พิมพ์ต้นแบบ “errorNotification” แสดงองค์ประกอบที่แสดงข้อผิดพลาดที่เกิดจากการเข้าถึงการดำเนินการที่ไม่มีสิทธิ์ในการเข้าถึง 5. ใช้ป้ายระบุ “controlledType” ของแม่พิมพ์ต้นแบบ “accessRight” แสดงประเภทขององค์ประกอบที่ควบคุมการเข้าถึงบริการในระบบ
การจำกัดการเข้าถึง (Limited Access)	ไม่ได้แสดงข้อมูลทางความมั่นคงในแผนภาพคือ 1. ผู้ใช้งานจากภายนอกระบบ 2. องค์ประกอบที่ควบคุมการสร้างส่วนต่อประสานให้เป็นไปตามสิทธิ์ในการใช้บริการของผู้ใช้งาน 3. บริการของโปรแกรมประยุกต์ภายในระบบ 4. องค์ประกอบที่กำหนดส่วนต่อประสานให้แก่ผู้ใช้งาน 5. คุณลักษณะที่แสดงสถานะของการมองเห็นในแต่ละองค์ประกอบของส่วนต่อประสาน 6. ประเภทขององค์ประกอบที่ควบคุมการสร้างส่วนต่อประสาน	เช่นเดียวกับการแสดงข้อมูลทางความมั่นคงของยูเอ็มแอล	แสดงข้อมูลทางความมั่นคงที่อยู่ในแผนภาพคือ 1. ใช้แม่พิมพ์ต้นแบบ “client” แสดงผู้ใช้งานจากภายนอกระบบ 2. ใช้แม่พิมพ์ต้นแบบ “accessRight” แสดงองค์ประกอบที่ควบคุมการสร้างส่วนต่อประสานให้เป็นไปตามสิทธิ์ในการใช้บริการของผู้ใช้งาน 3. ใช้แม่พิมพ์ต้นแบบ “appService” แสดงบริการของโปรแกรมประยุกต์ภายในระบบ 4. ใช้แม่พิมพ์ต้นแบบ “interfaceBuilder” แสดงองค์ประกอบที่กำหนดส่วนต่อประสานให้แก่ผู้ใช้งาน 5. ใช้แม่พิมพ์ต้นแบบ “enableUIElement” แสดงคุณลักษณะที่แสดงสถานะของการมองเห็นในแต่ละองค์ประกอบของส่วนต่อประสาน 6. ใช้ป้ายระบุ “controlledType” แสดงประเภทขององค์ประกอบที่ควบคุมการสร้างส่วนต่อประสาน
องค์ประกอบพิสูจน์ตัวตน (Authenticator)	ไม่ได้แสดงข้อมูลทางความมั่นคงในแผนภาพคือ 1. ผู้เข้าใช้ทรัพยากรในระบบปฏิบัติการ 2. องค์ประกอบที่ตรวจสอบตัวตนของผู้ใช้งานก่อนให้อำนาจแก่ผู้ใช้งาน 3. องค์ประกอบที่ใช้ในการแสดงตัวตนของผู้ใช้งาน 4. ใบรับรองในการระบุตัวตน 5. ผู้ให้ใบรับรองในการระบุตัวตน	เช่นเดียวกับการแสดงข้อมูลทางความมั่นคงของยูเอ็มแอล	แสดงข้อมูลทางความมั่นคงที่อยู่ในแผนภาพคือ 1. ใช้แม่พิมพ์ต้นแบบ “subject” แสดงผู้เข้าใช้ทรัพยากรในระบบปฏิบัติการ 2. ใช้แม่พิมพ์ต้นแบบ “authenticator” แสดงองค์ประกอบที่ตรวจสอบตัวตนของผู้ใช้งานก่อนให้อำนาจแก่ผู้ใช้งาน 3. ใช้แม่พิมพ์ต้นแบบ “proofOfIdentity” แสดงองค์ประกอบที่ใช้ในการแสดงตัวตนของผู้ใช้งาน 4. ใช้แม่พิมพ์ต้นแบบ “certificate” แสดงใบรับรองในการระบุตัวตน 5. ใช้แม่พิมพ์ต้นแบบ “certificateAuthority” แสดงผู้ให้ใบรับรองในการระบุตัวตน

ตารางที่ ฉ.2 การเปรียบเทียบการแสดงข้อมูลทางความมั่นคงในแต่ละแบบรูปความมั่นคง (ต่อ)

แบบรูปความมั่นคง	ยูเอ็มแอล	ยูเอ็มแอลเซค	ยูเอ็มแอลเซคเอสพี
การควบคุมการสร้างกระบวนการ (Controlled Process Creator)	ไม่ได้แสดงข้อมูลทางความมั่นคงในแผนภาพคือ 1. คำร้องขอในการสร้างกระบวนการของระบบปฏิบัติการ 2. องค์ประกอบที่ควบคุมการสร้างกระบวนการใหม่ในระบบปฏิบัติการ 3. องค์ประกอบที่จัดเก็บสิทธิ์ของกระบวนการในระบบปฏิบัติการ	เช่นเดียวกับการแสดงข้อมูลทางความมั่นคงของยูเอ็มแอล	แสดงข้อมูลทางความมั่นคงที่อยู่ในแผนภาพคือ 1. ใช้แม่พิมพ์ต้นแบบ "request" แสดงคำร้องขอในการสร้างกระบวนการของระบบปฏิบัติการ 2. ใช้แม่พิมพ์ต้นแบบ "processCreator" แสดงองค์ประกอบที่ควบคุมการสร้างกระบวนการใหม่ในระบบปฏิบัติการ 3. ใช้แม่พิมพ์ต้นแบบ "processDescriptor" แสดงองค์ประกอบที่จัดเก็บสิทธิ์ของกระบวนการในระบบปฏิบัติการ
การควบคุมการสร้างอ็อบเจกต์ (Controlled Object Factory)	ไม่ได้แสดงข้อมูลทางความมั่นคงในแผนภาพคือ 1. คำร้องขอในการสร้างอ็อบเจกต์ของระบบปฏิบัติการ 2. องค์ประกอบที่ควบคุมการสร้างอ็อบเจกต์ของระบบปฏิบัติการ 3. อ็อบเจกต์ในระบบปฏิบัติการที่ถูกสร้างขึ้นมา 4. อ็อบเจกต์ที่ควบคุมการเข้าถึงอ็อบเจกต์ในระบบปฏิบัติการ 5. องค์ประกอบที่ควบคุมการเข้าถึงอ็อบเจกต์ในระบบปฏิบัติการ 6. ผู้เข้าใช้อ็อบเจกต์ในระบบปฏิบัติการ 7. ประเภทขององค์ประกอบที่ควบคุมการเข้าถึงอ็อบเจกต์	แสดงข้อมูลทางความมั่นคงที่อยู่ในแผนภาพคือ 1. ใช้แม่พิมพ์ต้นแบบ "guarded" แสดงอ็อบเจกต์ของระบบปฏิบัติการที่ถูกสร้างขึ้นมา 2. ใช้ป้ายระบุ "guard" ของแม่พิมพ์ต้นแบบ "guarded" แสดงอ็อบเจกต์ที่ควบคุมการเข้าถึงอ็อบเจกต์ในระบบปฏิบัติการ	แสดงข้อมูลทางความมั่นคงที่อยู่ในแผนภาพคือ 1. ใช้แม่พิมพ์ต้นแบบ "request" แสดงคำร้องขอในการสร้างอ็อบเจกต์ของระบบปฏิบัติการ 2. ใช้แม่พิมพ์ต้นแบบ "objectFactory" แสดงองค์ประกอบที่ควบคุมการสร้างอ็อบเจกต์ของระบบปฏิบัติการ 3. ใช้แม่พิมพ์ต้นแบบ "guarded" แสดงอ็อบเจกต์ในระบบปฏิบัติการที่ถูกสร้างขึ้นมา 4. ใช้ป้ายระบุ "guard" ของแม่พิมพ์ต้นแบบ "guarded" แสดงอ็อบเจกต์ที่ควบคุมการเข้าถึงอ็อบเจกต์ในระบบปฏิบัติการ 5. ใช้แม่พิมพ์ต้นแบบ "accessRight" แสดงองค์ประกอบที่ควบคุมการเข้าถึงอ็อบเจกต์ในระบบปฏิบัติการ 6. ใช้แม่พิมพ์ต้นแบบ "subject" แสดงผู้เข้าใช้อ็อบเจกต์ในระบบปฏิบัติการ 7. ใช้ป้ายระบุ "controlledType" ของแม่พิมพ์ต้นแบบ "accessRight" แสดงประเภทขององค์ประกอบที่ควบคุมการเข้าถึงอ็อบเจกต์
การตรวจสอบการเข้าถึงอ็อบเจกต์ (Controlled Object Monitor)	ไม่ได้แสดงข้อมูลทางความมั่นคงในแผนภาพคือ 1. คำร้องขอในการเข้าถึงอ็อบเจกต์ของระบบปฏิบัติการ 2. องค์ประกอบที่ตรวจสอบการร้องขอใช้อ็อบเจกต์ 3. องค์ประกอบที่ควบคุมการเข้าถึงอ็อบเจกต์ในระบบปฏิบัติการ 4. อ็อบเจกต์ที่ควบคุมการเข้าถึงอ็อบเจกต์ในระบบปฏิบัติการ	แสดงข้อมูลทางความมั่นคงที่อยู่ในแผนภาพคือ 1. ใช้แม่พิมพ์ต้นแบบ "guarded" แสดงอ็อบเจกต์ของระบบปฏิบัติการที่ถูกสร้างขึ้นมา 2. ใช้ป้ายระบุ "guard" ของแม่พิมพ์ต้นแบบ "guarded" แสดงอ็อบเจกต์ที่ควบคุมการเข้าถึงอ็อบเจกต์ในระบบปฏิบัติการ	แสดงข้อมูลทางความมั่นคงที่อยู่ในแผนภาพคือ 1. ใช้แม่พิมพ์ต้นแบบ "request" แสดงคำร้องขอในการเข้าถึงอ็อบเจกต์ของระบบปฏิบัติการ 2. ใช้แม่พิมพ์ต้นแบบ "referenceMonitor" แสดงองค์ประกอบที่ตรวจสอบการร้องขอใช้อ็อบเจกต์ 3. ใช้แม่พิมพ์ต้นแบบ "accessRight" แสดงองค์ประกอบที่ควบคุมการเข้าถึงอ็อบเจกต์ในระบบปฏิบัติการ 4. ใช้ป้ายระบุ "guard" ของแม่พิมพ์ต้นแบบ "guarded" แสดงอ็อบเจกต์ที่ควบคุมการเข้าถึงอ็อบเจกต์ในระบบปฏิบัติการ 5. ใช้แม่พิมพ์ต้นแบบ "guarded" แสดงอ็อบเจกต์ในระบบปฏิบัติการที่ถูกควบคุม

ตารางที่ ฉ.2 การเปรียบเทียบการแสดงข้อมูลทางความมั่นคงในแต่ละแบบรูปความมั่นคง (ต่อ)

แบบรูปความมั่นคง	ยูเอ็มแอล	ยูเอ็มแอลเซค	ยูเอ็มแอลเซคเอสพี
การตรวจสอบการเข้าถึงอ็อบเจกต์ (Controlled Object Monitor)	5. อ็อบเจกต์ในระบบปฏิบัติการที่ถูกควบคุม 6. การเชื่อมโยงที่มีการตรวจสอบการร้องขอใช้ทรัพยากร 7. ประเภทขององค์ประกอบที่ควบคุมการเข้าถึงอ็อบเจกต์ 8. อ็อบเจกต์ที่ตรวจสอบคำร้องขอ		6. ใช้แม่พิมพ์ต้นแบบ “monitored” แสดงการเชื่อมโยงที่มีการตรวจสอบการร้องขอใช้ทรัพยากร 7. ใช้ป้ายระบุ “controlledType” ของแม่พิมพ์ต้นแบบ “accessRight” แสดงประเภทขององค์ประกอบที่ควบคุมการเข้าถึงอ็อบเจกต์ 8. ใช้ป้ายระบุ “monitor” ของแม่พิมพ์ต้นแบบ “monitored” แสดงอ็อบเจกต์ที่ตรวจสอบคำร้องขอ
การควบคุมหน่วยความจำเสมือน (Controlled Virtual Address Space)	ไม่ได้แสดงข้อมูลทางความมั่นคงในแผนภาพคือ 1. องค์ประกอบที่จัดเก็บสิทธิ์ของกระบวนการในระบบปฏิบัติการ 2. หน่วยความจำเสมือนในระบบปฏิบัติการ 3. ที่อยู่ของเซกเมนต์ 4. ลักษณะของการเข้าถึงเซกเมนต์ 5. ขนาดของเซกเมนต์	เช่นเดียวกับการแสดงข้อมูลทางความมั่นคงของยูเอ็มแอล	แสดงข้อมูลทางความมั่นคงที่อยู่ในแผนภาพคือ 1. ใช้แม่พิมพ์ต้นแบบ “processDescriptor” แสดงองค์ประกอบที่จัดเก็บสิทธิ์ของกระบวนการในระบบปฏิบัติการ 2. ใช้แม่พิมพ์ต้นแบบ “vas” แสดงหน่วยความจำเสมือนในระบบปฏิบัติการ 3. ใช้แม่พิมพ์ต้นแบบ “vasAddress” แสดงที่อยู่ของเซกเมนต์ 4. ใช้แม่พิมพ์ต้นแบบ “accessType” แสดงลักษณะของการเข้าถึงเซกเมนต์ 5. ใช้แม่พิมพ์ต้นแบบ “vasSize” แสดงขนาดของเซกเมนต์
การควบคุมขอบเขตกระทำการ (Execution Domain)	ไม่ได้แสดงข้อมูลทางความมั่นคงในแผนภาพคือ 1. องค์ประกอบที่ตรวจสอบการเปลี่ยนโดเมนภายในระบบปฏิบัติการ 2. องค์ประกอบที่จัดเก็บสิทธิ์ของกระบวนการในการเข้าใช้ทรัพยากรในโดเมนที่กำหนด 3. องค์ประกอบที่ควบคุมการเข้าถึงอ็อบเจกต์ในระบบปฏิบัติการ 4. อ็อบเจกต์ที่ควบคุมการเข้าถึงอ็อบเจกต์ในระบบปฏิบัติการ 5. อ็อบเจกต์ในระบบปฏิบัติการที่ถูกควบคุม 6. ประเภทขององค์ประกอบที่ควบคุมการเข้าถึงอ็อบเจกต์	แสดงข้อมูลทางความมั่นคงที่อยู่ในแผนภาพคือ 1. ใช้แม่พิมพ์ต้นแบบ “guarded” แสดงอ็อบเจกต์ของระบบปฏิบัติการที่ถูกควบคุม 2. ใช้ป้ายระบุ “guard” ของแม่พิมพ์ต้นแบบ “guarded” แสดงอ็อบเจกต์ที่ควบคุมการเข้าถึงอ็อบเจกต์ในระบบปฏิบัติการ	แสดงข้อมูลทางความมั่นคงที่อยู่ในแผนภาพคือ 1. ใช้แม่พิมพ์ต้นแบบ “domainProtection” แสดงองค์ประกอบที่ตรวจสอบการเปลี่ยนโดเมนภายในระบบปฏิบัติการ 2. ใช้แม่พิมพ์ต้นแบบ “domainDescriptor” แสดงองค์ประกอบที่จัดเก็บสิทธิ์ของกระบวนการในการเข้าใช้ทรัพยากรในโดเมนที่กำหนด 3. ใช้แม่พิมพ์ต้นแบบ “accessRight” แสดงองค์ประกอบที่ควบคุมการเข้าถึงอ็อบเจกต์ในระบบปฏิบัติการ 4. ใช้ป้ายระบุ “guard” ของแม่พิมพ์ต้นแบบ “guarded” แสดงอ็อบเจกต์ที่ควบคุมการเข้าถึงอ็อบเจกต์ในระบบปฏิบัติการ 5. ใช้แม่พิมพ์ต้นแบบ “guarded” แสดงอ็อบเจกต์ในระบบปฏิบัติการที่ถูกควบคุม 6. ใช้ป้ายระบุ “controlledType” ของแม่พิมพ์ต้นแบบ “accessRight” แสดงประเภทขององค์ประกอบที่ควบคุมการเข้าถึงอ็อบเจกต์
การควบคุมสิ่งแวดล้อมที่กระทำการ (Controlled Execution Environment)	ไม่ได้แสดงข้อมูลทางความมั่นคงในแผนภาพคือ 1. คำร้องขอในการเข้าถึงอ็อบเจกต์ของระบบปฏิบัติการ 2. องค์ประกอบที่ตรวจสอบการร้องขอใช้อ็อบเจกต์	แสดงข้อมูลทางความมั่นคงที่อยู่ในแผนภาพคือ 1. ใช้แม่พิมพ์ต้นแบบ “guarded” แสดงอ็อบเจกต์ของระบบปฏิบัติการที่ถูกควบคุม	แสดงข้อมูลทางความมั่นคงที่อยู่ในแผนภาพคือ 1. ใช้แม่พิมพ์ต้นแบบ “request” แสดงคำร้องขอในการเข้าถึงอ็อบเจกต์ของระบบปฏิบัติการ 2. ใช้แม่พิมพ์ต้นแบบ “referenceMonitor” แสดงองค์ประกอบที่ตรวจสอบการร้องขอใช้อ็อบเจกต์

ตารางที่ ฉ.2 การเปรียบเทียบการแสดงข้อมูลทางความมั่นคงในแต่ละแบบรูปความมั่นคง (ต่อ)

แบบรูปความมั่นคง	ยูเอ็มแอล	ยูเอ็มแอลเซค	ยูเอ็มแอลเซคเอสพี
การควบคุมสิ่งแวดล้อมที่กระทำการ (Controlled Execution Environment)	3. การเชื่อมโยงที่มีตรวจสอบการร้องขอใช้ทรัพยากร 4. ผู้เข้าใช้อ็อบเจกต์ในระบบปฏิบัติการ 5. องค์ประกอบที่ควบคุมการเข้าถึงอ็อบเจกต์ 6. อ็อบเจกต์ที่ควบคุมการเข้าถึงอ็อบเจกต์ในระบบปฏิบัติการ 7. อ็อบเจกต์ในระบบปฏิบัติการที่ถูกควบคุม 8. องค์ประกอบที่ตรวจสอบการเปลี่ยนโดเมนภายในระบบปฏิบัติการ 9. องค์ประกอบที่จัดเก็บสิทธิ์ของกระบวนการในการเข้าใช้ทรัพยากรในโดเมนที่กำหนด 10. ประเภทขององค์ประกอบที่ควบคุมการเข้าถึงอ็อบเจกต์ 11. อ็อบเจกต์ที่ตรวจสอบคำร้องขอ	2. ใช้ป้ายระบุ "guard" ของแม่พิมพ์ต้นแบบ "guarded" แสดงอ็อบเจกต์ที่ควบคุมการเข้าถึงอ็อบเจกต์ในระบบปฏิบัติการ	3. ใช้แม่พิมพ์ต้นแบบ "monitored" แสดงการเชื่อมโยงที่มีการตรวจสอบการร้องขอใช้ทรัพยากร 4. ใช้แม่พิมพ์ต้นแบบ "subject" แสดงผู้เข้าใช้อ็อบเจกต์ในระบบปฏิบัติการ 5. ใช้แม่พิมพ์ต้นแบบ "accessRight" แสดงองค์ประกอบที่ควบคุมการเข้าถึงอ็อบเจกต์ในระบบปฏิบัติการ 6. ใช้ป้ายระบุ "guard" ของแม่พิมพ์ต้นแบบ "guarded" แสดงอ็อบเจกต์ที่ควบคุมการเข้าถึงอ็อบเจกต์ในระบบปฏิบัติการ 7. ใช้แม่พิมพ์ต้นแบบ "guarded" แสดงอ็อบเจกต์ในระบบปฏิบัติการที่ถูกควบคุม 8. ใช้แม่พิมพ์ต้นแบบ "domainProtection" แสดงองค์ประกอบที่ตรวจสอบการเปลี่ยนโดเมนภายในระบบปฏิบัติการ 9. ใช้แม่พิมพ์ต้นแบบ "domainDescriptor" แสดงองค์ประกอบที่จัดเก็บสิทธิ์ของกระบวนการในการเข้าใช้ทรัพยากรในโดเมนที่กำหนด 10. ใช้ป้ายระบุ "controlledType" ของแม่พิมพ์ต้นแบบ "accessRight" แสดงประเภทขององค์ประกอบที่ควบคุมการเข้าถึงอ็อบเจกต์ 11. ใช้ป้ายระบุ "monitor" ของแม่พิมพ์ต้นแบบ "monitored" แสดงอ็อบเจกต์ที่ตรวจสอบคำร้องขอ
การให้อำนาจในแฟ้มข้อมูล (File Authorization)	ไม่ได้แสดงข้อมูลทางความมั่นคงในแผนภาพคือ 1. ผู้เข้าใช้แฟ้มข้อมูล 2. องค์ประกอบที่ควบคุมการเข้าถึงสารบบของผู้ใช้งาน 3. สถานีงานในระบบปฏิบัติการ 4. องค์ประกอบที่ควบคุมการเข้าถึงแฟ้มข้อมูลและสารบบ 5. องค์ประกอบที่รวบรวมแฟ้มข้อมูลและสารบบ 6. สารบบในระบบปฏิบัติการ 7. อ็อบเจกต์ที่ควบคุมการเข้าถึงองค์ประกอบที่รวบรวมแฟ้มข้อมูลและสารบบ 8. ระบบปฏิบัติการของสถานีงาน 9. ประเภทขององค์ประกอบที่ควบคุมการเข้าถึงสารบบของผู้ใช้งาน	แสดงข้อมูลทางความมั่นคงในแผนภาพคือ 1. ใช้แม่พิมพ์ต้นแบบ "guarded" แสดงองค์ประกอบที่รวบรวมแฟ้มข้อมูลและสารบบ 2. ใช้ป้ายระบุ "guard" ของแม่พิมพ์ต้นแบบ "guarded" แสดงอ็อบเจกต์ที่ควบคุมการเข้าถึงองค์ประกอบที่รวบรวมแฟ้มข้อมูลและสารบบ	แสดงข้อมูลทางความมั่นคงที่อยู่ในแผนภาพคือ 1. ใช้แม่พิมพ์ต้นแบบ "subject" แสดงผู้เข้าใช้แฟ้มข้อมูล 2. ใช้แม่พิมพ์ต้นแบบ "accessRight" แสดงองค์ประกอบที่ควบคุมการเข้าถึงสารบบของผู้ใช้งาน 3. ใช้แม่พิมพ์ต้นแบบ "workstation" แสดงสถานีงานในระบบปฏิบัติการ 4. ใช้แม่พิมพ์ต้นแบบ "accessRight" แสดงองค์ประกอบที่ควบคุมการเข้าถึงแฟ้มข้อมูลและสารบบ 5. ใช้แม่พิมพ์ต้นแบบ "guarded" แสดงองค์ประกอบที่รวบรวมแฟ้มข้อมูลและสารบบ 6. ใช้แม่พิมพ์ต้นแบบ "fileDirectory" แสดงสารบบในระบบปฏิบัติการ 7. ใช้ป้ายระบุ "guard" ของแม่พิมพ์ต้นแบบ "guarded" แสดงอ็อบเจกต์ที่ควบคุมการเข้าถึงองค์ประกอบที่รวบรวมแฟ้มข้อมูลและสารบบ 8. ใช้ป้ายระบุ "osType" ของแม่พิมพ์ต้นแบบ "workstation" แสดงระบบปฏิบัติการของสถานีงาน

ตารางที่ ฉ.2 การเปรียบเทียบการแสดงข้อมูลทางความมั่นคงในแต่ละแบบรูปความมั่นคง (ต่อ)

แบบรูปความมั่นคง	ยูเอ็มแอล	ยูเอ็มแอลเซค	ยูเอ็มแอลเซคเอสพี
การให้อำนาจในแฟ้มข้อมูล (File Authorization)	10. ประเภทขององค์ประกอบที่ควบคุมการเข้าถึงแฟ้มข้อมูลและสารบบ		9. ใช้ป้ายระบุ "controlledType" ของแม่พิมพ์ต้นแบบ "accessRight" แสดงประเภทขององค์ประกอบที่ควบคุมการเข้าถึงสารบบของผู้ใช้งาน 10. ใช้ป้ายระบุ "controlledType" ของแม่พิมพ์ต้นแบบ "accessRight" แสดงประเภทขององค์ประกอบที่ควบคุมการเข้าถึงแฟ้มข้อมูลและสารบบ
ไฟร์วอลล์สำหรับการกรองแพ็คเกจ (Packet Filter Firewall)	ไม่ได้แสดงข้อมูลทางความมั่นคงในแผนภาพคือ 1. ผู้เข้าใช้ระบบจากภายนอก 2. ไฟร์วอลล์สำหรับการกรองแพ็คเกจ 3. องค์ประกอบที่กรองแพ็คเกจในระดับไอพี 4. เครื่องบริการโปรแกรมประยุกต์ในระบบ 5. ผลิตภัณฑ์ของไฟร์วอลล์ 6. หมายเลขพอร์ทที่เปิด	เช่นเดียวกับการแสดงข้อมูลทางความมั่นคงของยูเอ็มแอล	แสดงข้อมูลทางความมั่นคงที่อยู่ในแผนภาพคือ 1. ใช้แม่พิมพ์ต้นแบบ "client" แสดงผู้เข้าใช้ระบบจากภายนอก 2. ใช้แม่พิมพ์ต้นแบบ "pfFirewall" แสดงไฟร์วอลล์สำหรับการกรองแพ็คเกจ 3. ใช้แม่พิมพ์ต้นแบบ "ruleBase" แสดงองค์ประกอบที่กรองแพ็คเกจในระดับไอพี 4. ใช้แม่พิมพ์ต้นแบบ "appServer" แสดงเครื่องบริการโปรแกรมประยุกต์ในระบบ 5. ใช้ป้ายระบุ "product" ของแม่พิมพ์ต้นแบบ "pfFirewall" แสดงผลิตภัณฑ์ของไฟร์วอลล์ 6. ใช้ป้ายระบุ "openedPort" ของแม่พิมพ์ต้นแบบ "pfFirewall" แสดงหมายเลขพอร์ทที่เปิด
ไฟร์วอลล์เชิงตัวแทน (Proxy-Based Firewall)	ไม่ได้แสดงข้อมูลทางความมั่นคงในแผนภาพคือ 1. ผู้เข้าใช้ระบบจากภายนอก 2. ไฟร์วอลล์เชิงตัวแทน 3. ตัวแทนของบริการในระบบ 4. องค์ประกอบที่กรองแพ็คเกจในระดับข้อความในแพ็คเกจ 5. บริการของโปรแกรมประยุกต์ในระบบ 6. เครื่องบริการโปรแกรมประยุกต์ในระบบ 7. ผลิตภัณฑ์ของไฟร์วอลล์ 8. หมายเลขพอร์ทที่เปิด	เช่นเดียวกับการแสดงข้อมูลทางความมั่นคงของยูเอ็มแอล	แสดงข้อมูลทางความมั่นคงที่อยู่ในแผนภาพคือ 1. ใช้แม่พิมพ์ต้นแบบ "client" แสดงผู้เข้าใช้ระบบจากภายนอก 2. ใช้แม่พิมพ์ต้นแบบ "pxFirewall" แสดงไฟร์วอลล์เชิงตัวแทน 3. ใช้แม่พิมพ์ต้นแบบ "proxy" แสดงตัวแทนของบริการในระบบ 4. ใช้แม่พิมพ์ต้นแบบ "ruleBase" แสดงองค์ประกอบที่กรองแพ็คเกจในระดับข้อความในแพ็คเกจ 5. ใช้แม่พิมพ์ต้นแบบ "appService" แสดงบริการของโปรแกรมประยุกต์ในระบบ 6. ใช้แม่พิมพ์ต้นแบบ "appServer" แสดงเครื่องบริการโปรแกรมประยุกต์ในระบบ 7. ใช้ป้ายระบุ "product" ของแม่พิมพ์ต้นแบบ "pxFirewall" แสดงผลิตภัณฑ์ของไฟร์วอลล์ 8. ใช้ป้ายระบุ "openedPort" ของแม่พิมพ์ต้นแบบ "pxFirewall" แสดงหมายเลขพอร์ทที่เปิด
ไฟร์วอลล์เชิงสถานะ (Stateful Firewall)	ไม่ได้แสดงข้อมูลทางความมั่นคงในแผนภาพคือ 1. ผู้เข้าใช้ระบบจากภายนอก 2. ไฟร์วอลล์เชิงสถานะ 3. องค์ประกอบที่เก็บสถานะของผู้เข้าใช้ระบบจากภายนอก 4. เครื่องบริการโปรแกรมประยุกต์ในระบบ 5. ผลิตภัณฑ์ของไฟร์วอลล์ 6. หมายเลขพอร์ทที่เปิด	เช่นเดียวกับการแสดงข้อมูลทางความมั่นคงของยูเอ็มแอล	แสดงข้อมูลทางความมั่นคงที่อยู่ในแผนภาพคือ 1. ใช้แม่พิมพ์ต้นแบบ "client" แสดงผู้เข้าใช้ระบบจากภายนอก 2. ใช้แม่พิมพ์ต้นแบบ "sfFirewall" แสดงไฟร์วอลล์เชิงสถานะ 3. ใช้แม่พิมพ์ต้นแบบ "stateTable" แสดงองค์ประกอบที่เก็บสถานะของผู้เข้าใช้ระบบจากภายนอก 4. ใช้แม่พิมพ์ต้นแบบ "appServer" แสดงเครื่องบริการโปรแกรมประยุกต์ในระบบ 5. ใช้ป้ายระบุ "product" ของแม่พิมพ์ต้นแบบ "sfFirewall" แสดงผลิตภัณฑ์ของไฟร์วอลล์ 6. ใช้ป้ายระบุ "openedPort" ของแม่พิมพ์ต้นแบบ "sfFirewall" แสดงหมายเลขพอร์ทที่เปิด

ตารางที่ ฉ.2 การเปรียบเทียบการแสดงข้อมูลทางความมั่นคงในแต่ละแบบรูปความมั่นคง (ต่อ)

แบบรูปความมั่นคง	ยูเอ็มแอล	ยูเอ็มแอลเซค	ยูเอ็มแอลเซคเอสพี
การปิดบังข้อมูล (Information Obscurity)	ไม่ได้แสดงข้อมูลทางความมั่นคงในแผนภาพคือ 1. ข้อมูลที่ถูกเข้ารหัสลับ 2. องค์ประกอบที่เข้ารหัสลับให้กับข้อมูล 3. องค์ประกอบที่จัดหากุญแจที่ใช้ในการเข้ารหัสลับ 4. กุญแจที่ใช้ในการเข้ารหัสลับ 5. ประเภทของกุญแจที่ใช้ในการเข้ารหัสลับ	เช่นเดียวกับการแสดงข้อมูลทางความมั่นคงของยูเอ็มแอล	แสดงข้อมูลทางความมั่นคงที่อยู่ในแผนภาพคือ 1. ใช้แม่พิมพ์ต้นแบบ “encryptedData” แสดงข้อมูลที่ถูกเข้ารหัสลับ 2. ใช้แม่พิมพ์ต้นแบบ “encryptionComponent” แสดงองค์ประกอบที่เข้ารหัสลับให้กับข้อมูล 3. ใช้แม่พิมพ์ต้นแบบ “keyProvider” แสดงองค์ประกอบที่จัดหากุญแจที่ใช้ในการเข้ารหัสลับ 4. ใช้แม่พิมพ์ต้นแบบ “encryptionKey” แสดงกุญแจที่ใช้ในการเข้ารหัสลับ 5. ใช้ป้ายระบุ “keyType” ของแม่พิมพ์ต้นแบบ “encryptionKey” แสดงประเภทของกุญแจที่ใช้ในการเข้ารหัสลับ
ช่องทางความมั่นคง (Secure Channel)	ไม่ได้แสดงข้อมูลทางความมั่นคงในแผนภาพคือ 1. เว็บเบราว์เซอร์ของผู้ใช้งาน 2. เครื่องบริการเว็บ 3. กุญแจที่ใช้ในการเข้ารหัสลับ 4. ผลิตภัณฑ์ของเว็บเบราว์เซอร์ 5. ผลิตภัณฑ์ของเครื่องบริการเว็บ 6. ประเภทของกุญแจที่ใช้ในการเข้ารหัสลับ	เช่นเดียวกับการแสดงข้อมูลทางความมั่นคงของยูเอ็มแอล	แสดงข้อมูลทางความมั่นคงที่อยู่ในแผนภาพคือ 1. ใช้แม่พิมพ์ต้นแบบ “webBrowser” แสดงเว็บเบราว์เซอร์ของผู้ใช้งาน 2. ใช้แม่พิมพ์ต้นแบบ “webServer” แสดงเครื่องบริการเว็บ 3. ใช้แม่พิมพ์ต้นแบบ “encryptionKey” แสดงกุญแจที่ใช้ในการเข้ารหัสลับ 4. ใช้ป้ายระบุ “product” ของแม่พิมพ์ต้นแบบ “webBrowser” แสดงผลิตภัณฑ์ของเว็บเบราว์เซอร์ 5. ใช้ป้ายระบุ “product” ของแม่พิมพ์ต้นแบบ “webServer” แสดงผลิตภัณฑ์เครื่องบริการเว็บ 6. ใช้ป้ายระบุ “keyType” ของแม่พิมพ์ต้นแบบ “encryptionKey” แสดงประเภทของกุญแจที่ใช้ในการเข้ารหัสลับ
ผู้เป็นที่รู้จัก (Known Partners)	ไม่ได้แสดงข้อมูลทางความมั่นคงในแผนภาพคือ 1. เว็บเบราว์เซอร์ของผู้ใช้งาน 2. เครื่องบริการเว็บ 3. กุญแจที่ใช้ในการเข้ารหัสลับ 4. ผลิตภัณฑ์ของเว็บเบราว์เซอร์ 5. ผลิตภัณฑ์ของเครื่องบริการเว็บ 6. ประเภทของกุญแจที่ใช้ในการเข้ารหัสลับ 7. บริการทวนสอบของการพิสูจน์ผู้ใช้งาน 8. องค์ประกอบที่ใช้ในการระบุตัวตนของผู้ใช้งาน 9. องค์ประกอบที่ใช้ในการระบุตัวตนของเครื่องบริการเว็บที่ถูกใช้งาน	เช่นเดียวกับการแสดงข้อมูลทางความมั่นคงของยูเอ็มแอล	แสดงข้อมูลทางความมั่นคงที่อยู่ในแผนภาพคือ 1. ใช้แม่พิมพ์ต้นแบบ “webBrowser” แสดงเว็บเบราว์เซอร์ของผู้ใช้งาน 2. ใช้แม่พิมพ์ต้นแบบ “webServer” แสดงเครื่องบริการเว็บ 3. ใช้แม่พิมพ์ต้นแบบ “encryptionKey” แสดงกุญแจที่ใช้ในการเข้ารหัสลับ 4. ใช้ป้ายระบุ “product” ของแม่พิมพ์ต้นแบบ “webBrowser” แสดงผลิตภัณฑ์ของเว็บเบราว์เซอร์ 5. ใช้ป้ายระบุ “product” ของแม่พิมพ์ต้นแบบ “webServer” แสดงผลิตภัณฑ์เครื่องบริการเว็บ 6. ใช้ป้ายระบุ “keyType” ของแม่พิมพ์ต้นแบบ “encryptionKey” แสดงประเภทของกุญแจที่ใช้ในการเข้ารหัสลับ 7. ใช้แม่พิมพ์ต้นแบบ “uivService” แสดงบริการทวนสอบของการพิสูจน์ผู้ใช้งาน 8. ใช้แม่พิมพ์ต้นแบบ “userIdentity” แสดงองค์ประกอบที่ใช้ในการระบุตัวตนของผู้ใช้งาน 9. ใช้แม่พิมพ์ต้นแบบ “systemIdentity” แสดงองค์ประกอบที่ใช้ในการระบุตัวตนของเครื่องบริการเว็บที่ถูกใช้งาน

ตารางที่ ฉ.2 การเปรียบเทียบการแสดงข้อมูลทางความมั่นคงในแต่ละแบบรูปความมั่นคง (ต่อ)

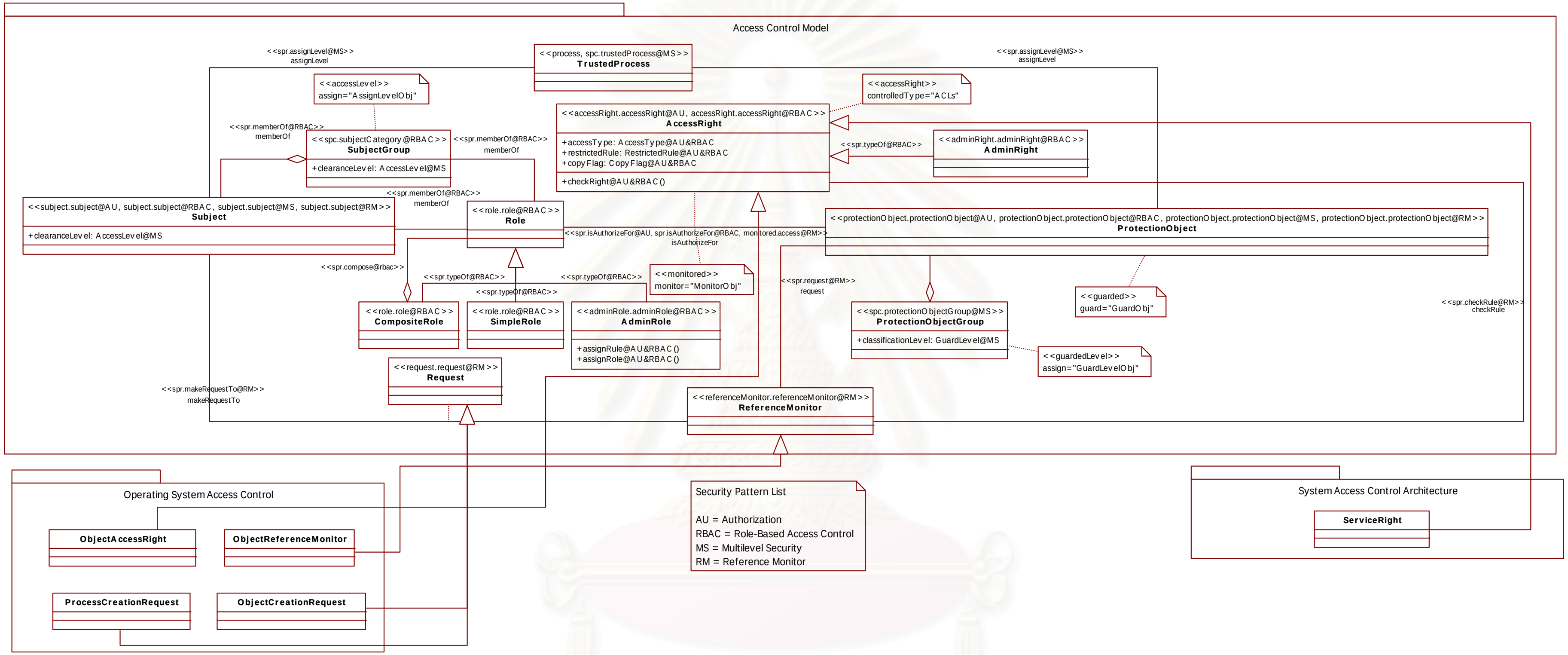
แบบรูปความมั่นคง	ยูเอ็มแอล	ยูเอ็มแอลเซค	ยูเอ็มแอลเซคเอสพี
เขตปลอดการป้องกัน (Demilitarized Zone)	ไม่ได้แสดงข้อมูลทางความมั่นคงในแผนภาพคือ 1. เว็บเบราว์เซอร์ของผู้ใช้งาน 2. องค์ประกอบที่จัดเส้นทางของแพ็คเกจที่เข้าออกในระบบ 3. ไฟร์วอลล์สำหรับการกรองแพ็คเกจ 4. เครื่องบริการเว็บ 5. เครื่องบริการโปรแกรมประยุกต์ 6. ผลิตภัณฑ์ของเว็บเบราว์เซอร์ 7. ผลิตภัณฑ์ของเครื่องบริการเว็บ 8. หมายเลขพอร์ทที่เปิดของอุปกรณ์ที่จัดเส้นทางของแพ็คเกจ 9. ผลิตภัณฑ์ของไฟร์วอลล์ 10. หมายเลขพอร์ทที่เปิดของไฟร์วอลล์ 11. ส่วนประกอบของเครื่องบริการโปรแกรมประยุกต์ 12. ลักษณะของเครื่องบริการเว็บที่เป็นนามธรรม	เช่นเดียวกับการแสดงข้อมูลทางความมั่นคงของยูเอ็มแอล	แสดงข้อมูลทางความมั่นคงที่อยู่ในแผนภาพคือ 1. ใช้แม่พิมพ์ต้นแบบ "webBrowser" แสดงเว็บเบราว์เซอร์ของผู้ใช้งาน 2. ใช้แม่พิมพ์ต้นแบบ "router" แสดงองค์ประกอบที่จัดเส้นทางของแพ็คเกจที่เข้าออกในระบบ 3. ใช้แม่พิมพ์ต้นแบบ "pfFirewall" แสดงไฟร์วอลล์สำหรับการกรองแพ็คเกจ 4. ใช้แม่พิมพ์ต้นแบบ "webServer" แสดงเครื่องบริการเว็บ 5. ใช้แม่พิมพ์ต้นแบบ "applicationServer" แสดงเครื่องบริการโปรแกรมประยุกต์ 6. ใช้ป้ายระบุ "product" ของแม่พิมพ์ต้นแบบ "webBrowser" แสดงผลิตภัณฑ์ของเว็บเบราว์เซอร์ 7. ใช้ป้ายระบุ "product" ของแม่พิมพ์ต้นแบบ "webServer" แสดงผลิตภัณฑ์เครื่องบริการเว็บ 8. ใช้ป้ายระบุ "openedPort" ของแม่พิมพ์ต้นแบบ "router" แสดงหมายเลขพอร์ทที่เปิดของอุปกรณ์ที่จัดเส้นทางของแพ็คเกจ 9. ใช้ป้ายระบุ "product" ของแม่พิมพ์ต้นแบบ "pfFirewall" แสดงผลิตภัณฑ์ของไฟร์วอลล์ 10. ใช้ป้ายระบุ "openedPort" ของแม่พิมพ์ต้นแบบ "pfFirewall" แสดงหมายเลขพอร์ทที่เปิดของไฟร์วอลล์ 11. ใช้ป้ายระบุ "componentType" ของแม่พิมพ์ต้นแบบ "appServer" แสดงส่วนประกอบของเครื่องบริการโปรแกรมประยุกต์ 12. ใช้ป้ายระบุ "abstract" ของแม่พิมพ์ต้นแบบ "webServer" แสดงลักษณะของเครื่องบริการเว็บที่เป็นนามธรรม
ตัวแทนป้องกัน (Protection Reverse Proxy)	ไม่ได้แสดงข้อมูลทางความมั่นคงในแผนภาพคือ 1. เว็บเบราว์เซอร์ของผู้ใช้งาน 2. ไฟร์วอลล์สำหรับการกรองแพ็คเกจ 3. ตัวแทนที่ป้องกันการเข้าถึงแม่ข่าย 4. เครื่องบริการเว็บ 5. ผลิตภัณฑ์ของเว็บเบราว์เซอร์ 6. ผลิตภัณฑ์ของเครื่องบริการเว็บ 7. ผลิตภัณฑ์ของไฟร์วอลล์ 8. หมายเลขพอร์ทที่เปิด	เช่นเดียวกับการแสดงข้อมูลทางความมั่นคงของยูเอ็มแอล	แสดงข้อมูลทางความมั่นคงที่อยู่ในแผนภาพคือ 1. ใช้แม่พิมพ์ต้นแบบ "webBrowser" แสดงเว็บเบราว์เซอร์ของผู้ใช้งาน 2. ใช้แม่พิมพ์ต้นแบบ "pfFirewall" แสดงไฟร์วอลล์สำหรับการกรองแพ็คเกจ 3. ใช้แม่พิมพ์ต้นแบบ "reverseProxy" แสดงตัวแทนที่ป้องกันการเข้าถึงแม่ข่าย 4. ใช้แม่พิมพ์ต้นแบบ "webServer" แสดงเครื่องบริการเว็บ 5. ใช้ป้ายระบุ "product" ของแม่พิมพ์ต้นแบบ "webBrowser" แสดงผลิตภัณฑ์ของเว็บเบราว์เซอร์ 6. ใช้ป้ายระบุ "product" ของแม่พิมพ์ต้นแบบ "webServer" แสดงผลิตภัณฑ์เครื่องบริการเว็บ 7. ใช้ป้ายระบุ "product" ของแม่พิมพ์ต้นแบบ "pfFirewall" แสดงผลิตภัณฑ์ของไฟร์วอลล์ 8. ใช้ป้ายระบุ "openedPort" ของแม่พิมพ์ต้นแบบ "pfFirewall" แสดงหมายเลขพอร์ทที่เปิด

ตารางที่ ฉ.2 การเปรียบเทียบการแสดงข้อมูลทางความมั่นคงในแต่ละแบบรูปความมั่นคง (ต่อ)

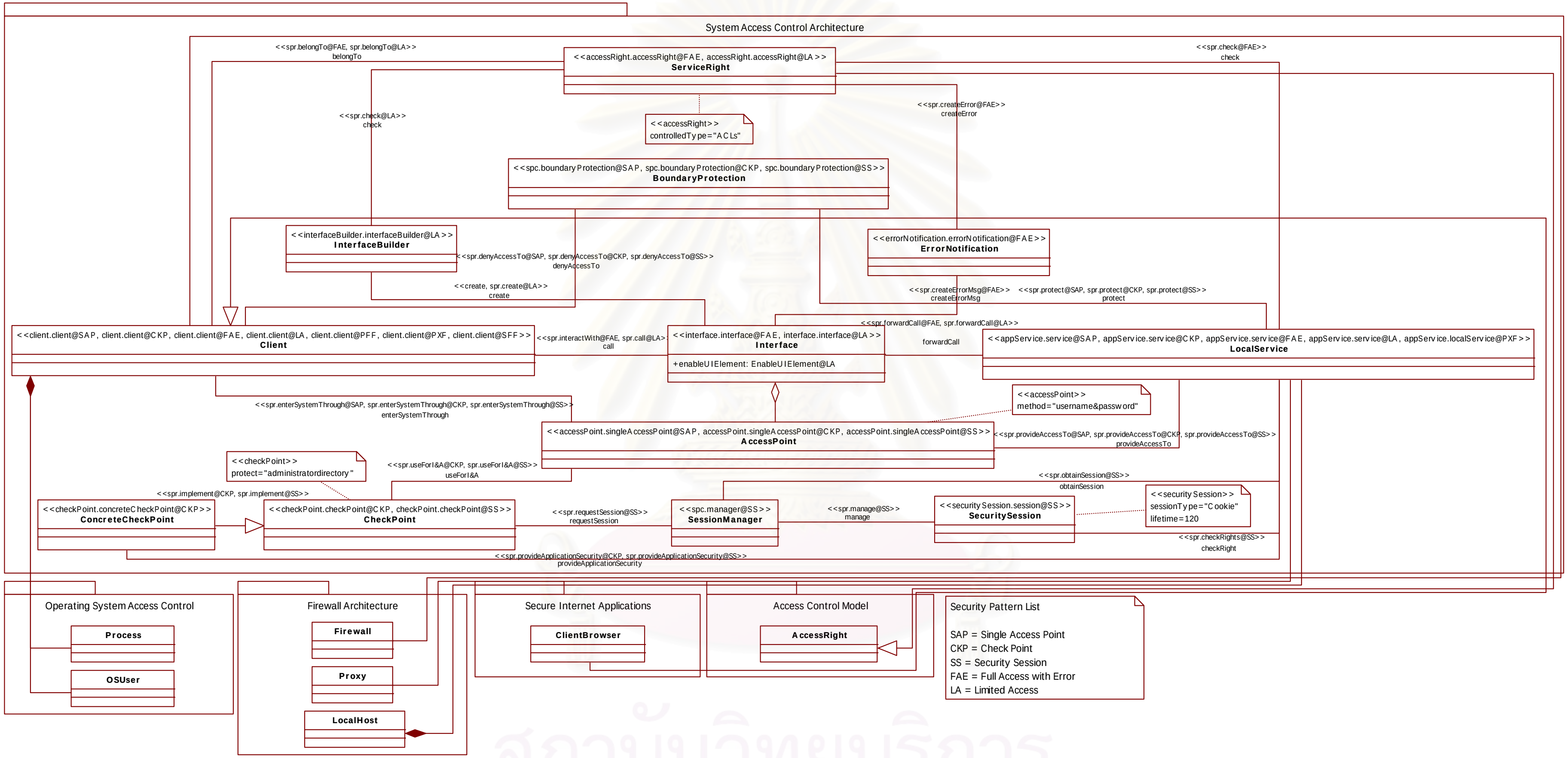
แบบรูปความมั่นคง	ยูเอ็มแอล	ยูเอ็มแอลเซค	ยูเอ็มแอลเซคเอสพี
ตัวแทนบูรณาการ (Integration Reverse Proxy)	ไม่ได้แสดงข้อมูลทางความมั่นคงในแผนภาพคือ 1. เว็บเบราว์เซอร์ของผู้ใช้งาน 2. ตัวแทนบูรณาการที่รวบรวมเครื่องบริการเว็บทั้งหมด 3. เครื่องบริการเว็บ 4. ผลิตภัณฑ์ของเว็บเบราว์เซอร์ 5. ผลิตภัณฑ์ของเครื่องบริการเว็บ 6. ยูอาร์แอลหลักของตัวแทน 7. รายการที่อนุญาตให้ผ่านตัวแทน 8. รายการที่ไม่อนุญาตให้ผ่านตัวแทน	เช่นเดียวกับการแสดงข้อมูลทางความมั่นคงของยูเอ็มแอล	แสดงข้อมูลทางความมั่นคงที่อยู่ในแผนภาพคือ 1. ใช้แม่พิมพ์ต้นแบบ “webBrowser” แสดงเว็บเบราว์เซอร์ของผู้ใช้งาน 2. ใช้แม่พิมพ์ต้นแบบ “reverseProxy” แสดงตัวแทนบูรณาการที่รวบรวมเครื่องบริการเว็บทั้งหมด 3. ใช้แม่พิมพ์ต้นแบบ “webServer” แสดงเครื่องบริการเว็บ 4. ใช้ป้ายระบุ “product” ของแม่พิมพ์ต้นแบบ “webBrowser” แสดงผลิตภัณฑ์ของเว็บเบราว์เซอร์ 5. ใช้ป้ายระบุ “product” ของแม่พิมพ์ต้นแบบ “webServer” แสดงผลิตภัณฑ์เครื่องบริการเว็บ 6. ใช้ป้ายระบุ “mainURL” ของแม่พิมพ์ต้นแบบ “reverseProxy” แสดงยูอาร์แอลของตัวแทน 7. ใช้ป้ายระบุ “whiteList” ของแม่พิมพ์ต้นแบบ “reverseProxy” แสดงรายการที่อนุญาตให้ผ่านตัวแทน 8. ใช้ป้ายระบุ “blackList” ของแม่พิมพ์ต้นแบบ “reverseProxy” แสดงรายการที่ไม่อนุญาตให้ผ่านตัวแทน
ประตูหน้า (Front Door)	ไม่ได้แสดงข้อมูลทางความมั่นคงในแผนภาพคือ 1. เว็บเบราว์เซอร์ของผู้ใช้งาน 2. ตัวแทนบูรณาการที่รวบรวมเครื่องบริการเว็บทั้งหมด 3. เครื่องบริการเว็บ 4. ผลิตภัณฑ์ของเว็บเบราว์เซอร์ 5. ผลิตภัณฑ์ของเครื่องบริการเว็บ 6. ยูอาร์แอลหลักของตัวแทน 7. รายการที่อนุญาตให้ผ่านตัวแทน 8. รายการที่ไม่อนุญาตให้ผ่านตัวแทน 9. องค์ประกอบที่จัดการข้อมูลที่ใช้ในการระบุตัวตนและการตรวจสอบผู้ใช้งาน	เช่นเดียวกับการแสดงข้อมูลทางความมั่นคงของยูเอ็มแอล	แสดงข้อมูลทางความมั่นคงที่อยู่ในแผนภาพคือ 1. ใช้แม่พิมพ์ต้นแบบ “webBrowser” แสดงเว็บเบราว์เซอร์ของผู้ใช้งาน 2. ใช้แม่พิมพ์ต้นแบบ “reverseProxy” แสดงตัวแทนบูรณาการที่รวบรวมเครื่องบริการเว็บทั้งหมด 3. ใช้แม่พิมพ์ต้นแบบ “webServer” แสดงเครื่องบริการเว็บ 4. ใช้ป้ายระบุ “product” ของแม่พิมพ์ต้นแบบ “webBrowser” แสดงผลิตภัณฑ์ของเว็บเบราว์เซอร์ 5. ใช้ป้ายระบุ “product” ของแม่พิมพ์ต้นแบบ “webServer” แสดงผลิตภัณฑ์เครื่องบริการเว็บ 6. ใช้ป้ายระบุ “mainURL” ของแม่พิมพ์ต้นแบบ “reverseProxy” แสดงยูอาร์แอลของตัวแทน 7. ใช้ป้ายระบุ “whiteList” ของแม่พิมพ์ต้นแบบ “reverseProxy” แสดงรายการที่อนุญาตให้ผ่านตัวแทน 8. ใช้ป้ายระบุ “blackList” ของแม่พิมพ์ต้นแบบ “reverseProxy” แสดงรายการที่ไม่อนุญาตให้ผ่านตัวแทน 9. ใช้แม่พิมพ์ต้นแบบ “userDirectory” แสดงองค์ประกอบที่จัดการข้อมูลที่ใช้ในการระบุตัวตนและการตรวจสอบผู้ใช้งาน

ภาคผนวก ช
แผนภาพคลาสรวมที่ใช้ยูเอ็มแอลเซคเอสพี

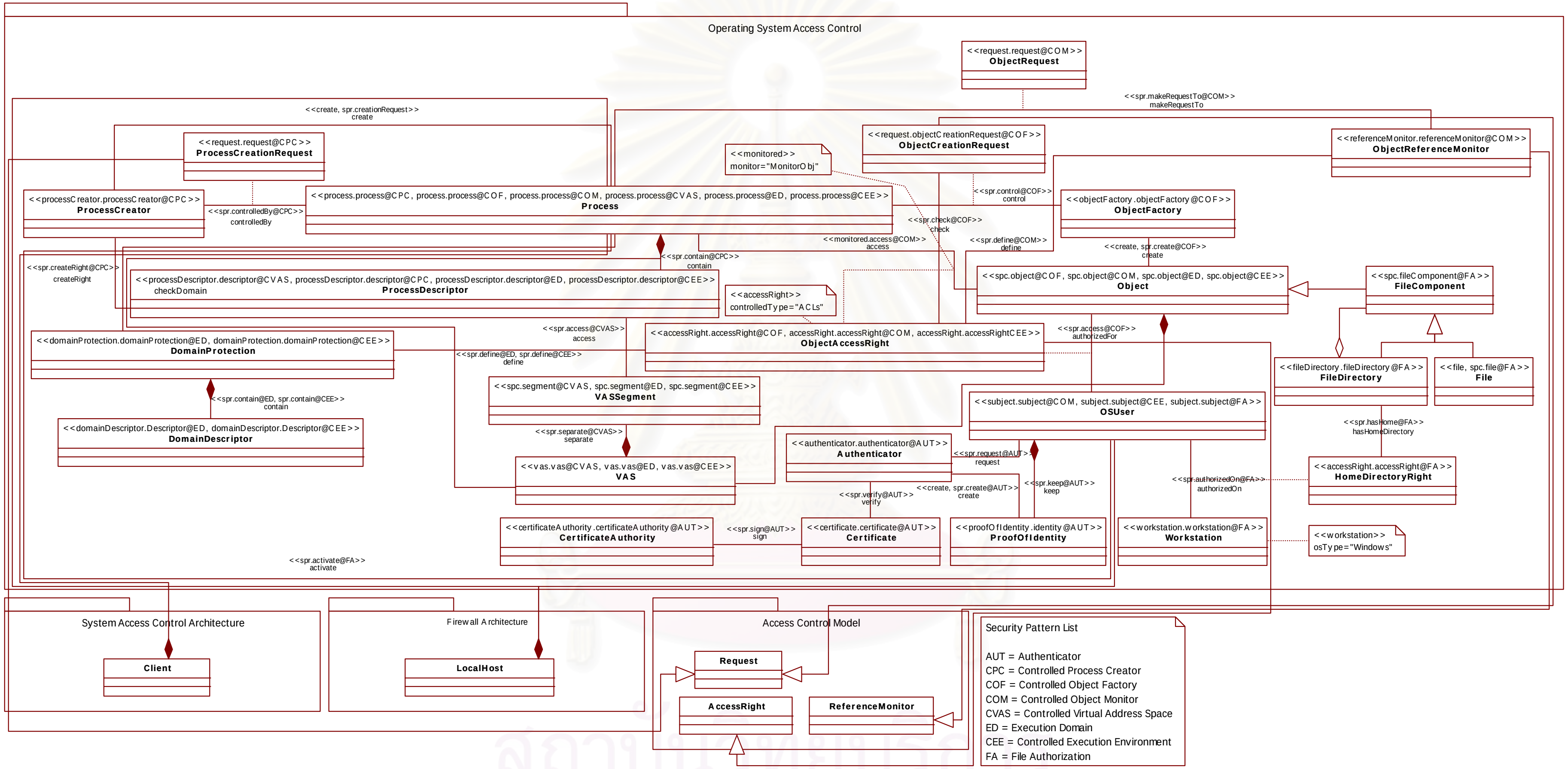
แผนภาพคลาสรวมที่ใช้ยูเอ็มแอลเซคเอสพี เป็นแผนภาพคลาสที่เกิดจากการบูรณาการของแบบรูปความมั่นคงที่อยู่ในขอบเขตทั้งหมด โดยแต่ละองค์ประกอบในแผนภาพจะใช้ยูเอ็มแอลเซคเอสพีในการแสดงข้อมูลทางโครงสร้างและข้อมูลทางความมั่นคงในแต่ละแบบรูปความมั่นคง



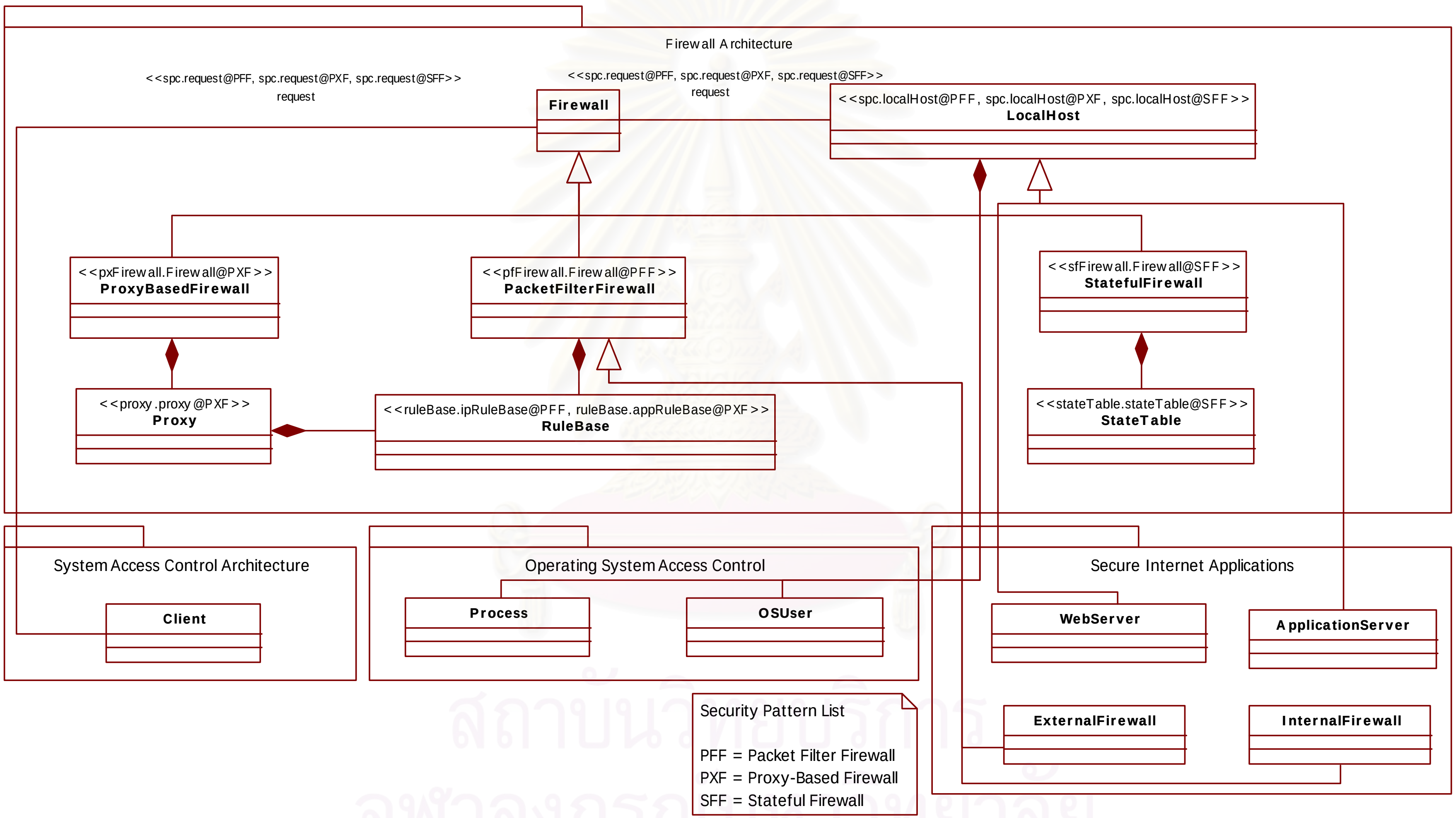
รูปที่ ช.1 แผนภาพคลาสรวมที่ใช้ยูเอ็มแอลเซคเอสพีของกลุ่มแบบรูปของแบบจำลองการควบคุมการเข้าถึง



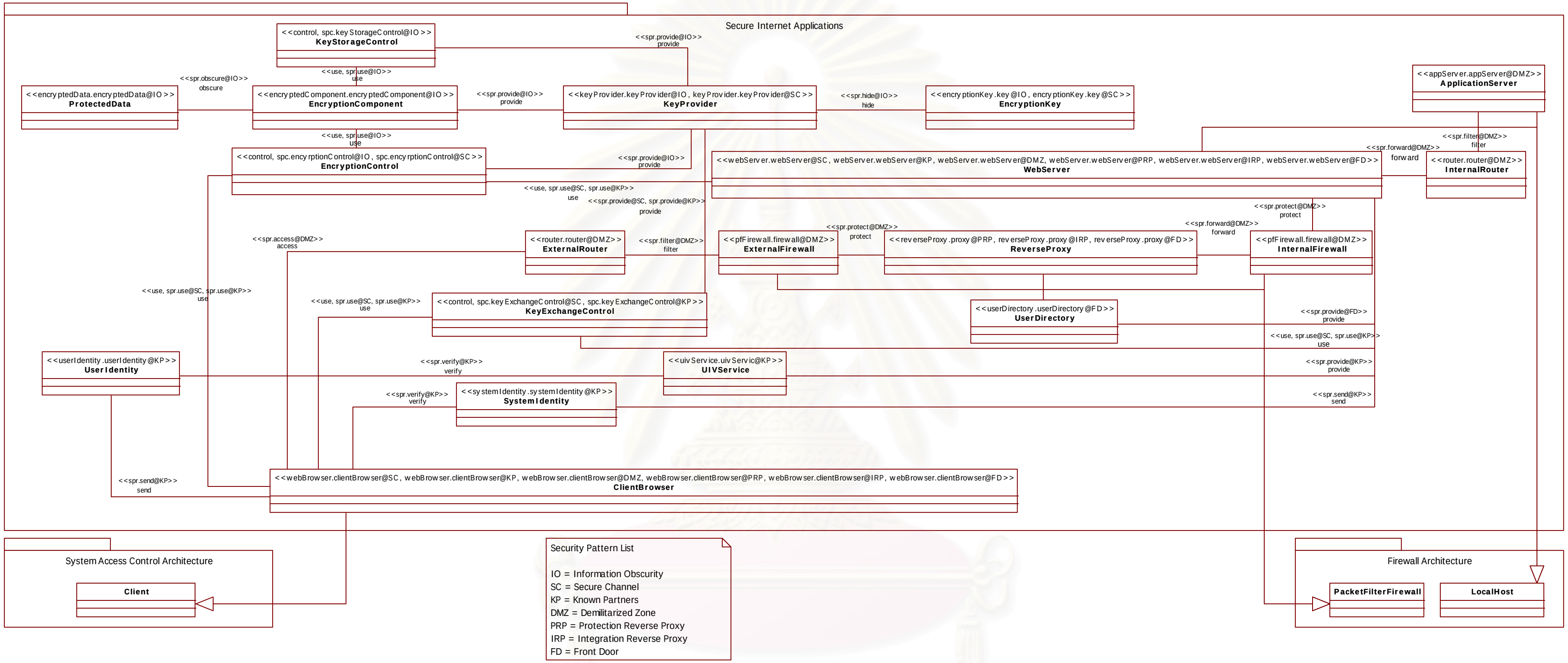
รูปที่ ช.2 แผนภาพคลาสรวมที่ใช้ยูเอ็มแอลเซคเอสพีของกลุ่มแบบรูปสถาปัตยกรรมการควบคุมการเข้าถึง



รูปที่ ช.3 แผนภาพคลาสรวมที่ใช้ยูเอ็มแอลเซคเอสพีของกลุ่มแบบรูปการควบคุมการเข้าถึงระบบปฏิบัติการ



รูปที่ ช.4 แผนภาพคลาสรวมที่ใช้ยูเอ็มแอลเซคเอสพีของกลุ่มแบบรูปสถาปัตยกรรมไฟร์วอลล์



รูปที่ ซ.5 แผนภาพคลาสรวมที่ใช้ยูเอ็มแอลเซคเอสพีของกลุ่มแบบรูปการประยุกต์ใช้ความมั่นคงบนอินเตอร์เน็ต

ภาคผนวก ซ
ผลงานตีพิมพ์

ระหว่างดำเนินงานวิจัย ผู้วิจัยได้เขียนบทความเพื่อตีพิมพ์ผลงานในวารสารวิชาการและการประชุมวิชาการในประเทศดังนี้

1) บทความวิชาการเรื่อง “การออกแบบและการแสดงแบบรูปของแบบจำลองการควบคุมการเข้าถึงโดยการขยายยูเอ็มแอลเซค (Design and Visualization of Access Control Model Patterns by Extending UMLsec)” ซึ่งได้รับการคัดเลือกเพื่อนำเสนอและตีพิมพ์ในงาน “การประชุมวิชาการร่วมสาขาวิทยาการคอมพิวเตอร์และวิศวกรรมซอฟต์แวร์ ครั้งที่ 5 (The 5^{th} International Joint Conference on Computer Science and Software Engineering: JCSSE 2008)” ระหว่างวันที่ 7 – 9 พฤษภาคม 2551 ณ โรงแรมเฟลิกซ์ริเวอร์แควรีสอร์ท กาญจนบุรี

2) บทความวิชาการเรื่อง “เครื่องมือสำหรับการกำหนดข้อมูลและโครงสร้างแบบรูปของแบบจำลองการควบคุมการเข้าถึง (Access Control Model Pattern Information and Structure Definition Tool)” ซึ่งได้รับการคัดเลือกเพื่อนำเสนอและตีพิมพ์ในงาน “การประชุมวิชาการทางวิทยาการคอมพิวเตอร์และวิศวกรรมคอมพิวเตอร์ในระดับชาติ ครั้งที่ 12 (The 12^{th} National Computer Science and Engineering Conference: NCSEC 2008)” ระหว่างวันที่ 20 – 21 พฤศจิกายน 2551 ณ โรงแรมลองบีชการ์เดนรีสอร์ทแอนด์สปา ชลบุรี

3) บทความวิชาการเรื่อง “UMLsec-SP: An Extension of UMLsec for System Security Modeling based on Security Patterns” ซึ่งได้รับการคัดเลือกเพื่อนำเสนอและตีพิมพ์ในงาน “การประชุมวิชาการร่วมสาขาวิทยาการคอมพิวเตอร์และวิศวกรรมซอฟต์แวร์ ครั้งที่ 6 (The 6^{th} International Joint Conference on Computer Science and Software Engineering: JCSSE 2009)” ระหว่างวันที่ 13 – 15 พฤษภาคม 2552 ณ โรงแรมลากูน่าบีชรีสอร์ท ภูเก็ต

การออกแบบและการแสดงแบบรูปของแบบจำลองการควบคุมการเข้าถึงโดยการขยายยูเอ็มแอลเซค

Design and Visualization of Access Control Model Patterns by Extending UMLsec

เกียรติศักดิ์ ไชยสมบูรณ์ และ นครทิพย์ พร้อมพูล
ห้องปฏิบัติการวิศวกรรมซอฟต์แวร์ ศูนย์เชี่ยวชาญเฉพาะทางด้านวิศวกรรมซอฟต์แวร์
ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
อีเมล: kiattisak.c@student.chula.ac.th และ nakornthip.s@chula.ac.th

บทคัดย่อ

แบบรูปของแบบจำลองการควบคุมการเข้าถึง เป็นกลุ่มของแบบรูปความมั่นคงที่อธิบายการออกแบบการควบคุมการเข้าถึงของระบบและเสนอคำตอบที่ได้รับการพิสูจน์แล้วเพื่อแก้ไขปัญหา อย่างไรก็ตามการนำแบบดังกล่าวมาประยุกต์ใช้ในการพัฒนาความมั่นคงของระบบนั้นค่อนข้างทำได้ยาก เนื่องจากกลุ่มแบบรูปดังกล่าวได้กำหนดโครงสร้างที่ประกอบไปด้วยส่วนประกอบและความสัมพันธ์ในระดับบน ยูเอ็มแอลเซค (UMLsec) เป็นภาคขยายของยูเอ็มแอลที่สนับสนุนการออกแบบส่วนประกอบและความสัมพันธ์ทางความมั่นคงของระบบโดยทั่วไป อย่างไรก็ตามยูเอ็มแอลเซคยังมีข้อจำกัดในการนำมาใช้กับกลุ่มแบบรูปดังกล่าว เนื่องจากส่วนประกอบและความสัมพันธ์ของกลุ่มแบบรูปนี้ไม่สามารถอธิบายได้อย่างชัดเจนด้วยการใช้ยูเอ็มแอลเซค บทความนี้ได้นำเสนอแนวคิดในการปรับปรุงยูเอ็มแอลเซคโดยการปรับปรุงจากยูเอ็มแอลโพรไฟล์ (UML profile) เพื่อการออกแบบและการแสดงแบบรูปของแบบจำลองการควบคุมการเข้าถึง ยูเอ็มแอลเซคที่ได้รับการปรับปรุงแล้วจะช่วยให้ผู้พัฒนาระบุส่วนประกอบและความสัมพันธ์ทางความมั่นคงของระบบได้อย่างละเอียดและสามารถใช้ประโยชน์ของแบบรูปของแบบจำลองการควบคุมการเข้าถึงในการออกแบบและการแสดงความมั่นคงของระบบได้อย่างเต็มที่

คำสำคัญ: ยูเอ็มแอลเซค แบบรูป แบบรูปความมั่นคง ยูเอ็มแอลโพรไฟล์

Abstract

Access Control Model Patterns (ACMP) is one group of security patterns that describes access control design of system and suggests proven answers to solved problems. However, applying ACMP in security system development is quite difficult since it defines a very high level of components and relationships. UMLSec, the extension of UML, supports the design of security system components in general. However, there are limitations in UMLSec especially when using ACMP for system security design since the core information of ACMP does not explicitly describe with UMLSec. In this paper, we present an approach to improve UMLSec by extending specific UML profiles for the design and visualization of ACMP. UMLSec with the proposed improvement may help developer to include specific security features with precision and fully use the advantage of ACMP for the design and visualization of system security.

Keyword: UMLsec, Patterns, Security Patterns, UML Profile

1. บทนำ

ในปัจจุบันได้มีการนำแบบรูปไปใช้ในวงการซอฟต์แวร์อย่างแพร่หลายเนื่องจากแบบรูปเสนอแนวทางในการแก้ไขปัญหาที่เคยปรากฏในอดีตและสนับสนุนการนำกลับมาใช้ใหม่เช่น แบบรูปการวิเคราะห์ระบบ แบบรูปการเขียนโปรแกรม แบบรูปการออกแบบ เป็นต้น และเนื่องด้วยการตระหนักถึงปัญหาการคุกคามความมั่นคงของซอฟต์แวร์ที่มีมากขึ้น จึงเป็นที่มาของแบบรูปความมั่นคง [1] ซึ่งเป็นแบบรูปที่ช่วยแก้ไขปัญหาการออกแบบความมั่นคงของซอฟต์แวร์โดยทั่วไปกลุ่มแบบรูปความมั่นคงที่ถูกใช้อย่างแพร่หลายคือ แบบรูปของแบบจำลองการควบคุมการเข้าถึงเนื่องจากกลุ่มแบบรูปความมั่นคงดังกล่าวเป็นกลุ่มแบบรูปความมั่นคงพื้นฐานที่ใช้ในการออกแบบการควบคุมการเข้าถึงซอฟต์แวร์โดยทั่วไป อย่างไรก็ตามการศึกษาและวิเคราะห์แบบรูปของแบบจำลองการควบคุมการเข้าถึงเพื่อนำมาประยุกต์ใช้ในการออกแบบซอฟต์แวร์นั้นทำได้ยากเนื่องจากกลุ่มแบบรูปดังกล่าวได้กำหนดโครงสร้างที่ประกอบไปด้วยส่วนประกอบและความสัมพันธ์ของแบบรูปของแบบจำลองการควบคุมการเข้าถึงไว้ในระดับบน ซึ่งผู้พัฒนาจะต้องศึกษาและวิเคราะห์โครงสร้างดังกล่าวของแบบรูปของแบบจำลองการควบคุมการเข้าถึงเมื่อมีนำแบบรูปของแบบจำลองการควบคุมการเข้าถึงไปประยุกต์ใช้ในการออกแบบและการปรับปรุงการออกแบบซอฟต์แวร์ หากละเลยการพิจารณาดังกล่าว จะทำให้การออกแบบและการปรับปรุงการออกแบบซอฟต์แวร์ที่เกี่ยวข้องกับแบบรูปของแบบจำลองการควบคุมการเข้าถึงนั้นจะมีจุดอ่อนที่ทำให้ผู้บุกรุก (Intruder) โจมตีได้ง่าย และอาจเกิดปัญหาต่างๆ เช่น ข้อมูลสูญหาย การเชื่อมต่อของเครือข่ายถูกรบกวน เป็นต้น

ยูเอ็มแอลเซค (UMLsec) [2] เป็นภาคขยายของยูเอ็มแอลที่สนับสนุนการออกแบบส่วนประกอบและความสัมพันธ์ทางความมั่นคงของระบบโดยทั่วไป รวมทั้งสนับสนุนการออกแบบความมั่นคงของระบบโดยใช้แบบรูปความมั่นคง [3] อย่างไรก็ตามยูเอ็มแอลเซคยังมีข้อจำกัดในการนำมาใช้กับแบบรูปของแบบจำลองการควบคุมการเข้าถึงเนื่องจากส่วนประกอบและความสัมพันธ์ของแบบรูปของแบบจำลองการควบคุมการเข้าถึงไม่สามารถอธิบายได้อย่างชัดเจนโดยใช้ยูเอ็มแอลเซค เช่น ไม่สามารถบอกได้ว่าคุณลักษณะหรือการดำเนินการใดของระบบเป็นคุณลักษณะหรือการดำเนินการของแบบรูปของแบบจำลองการควบคุมการเข้าถึง ไม่สามารถให้อิสระในการตั้งชื่อส่วนประกอบของแบบรูปของแบบจำลองการควบคุมการเข้าถึงได้ เนื่องจากผู้พัฒนาจะต้องตั้งชื่อส่วนประกอบให้สอดคล้องกับหน้าที่ในแบบรูปของแบบจำลองการควบคุมการเข้าถึงซึ่งจะนำไปสู่ปัญหาในการตัดสินใจว่าควรตั้งชื่อส่วนประกอบนั้นอย่างไร ถ้าระบบนั้นมีการใช้หลายๆแบบรูปของแบบจำลองการควบคุมการเข้าถึงและส่วนประกอบนั้นเป็นส่วนประกอบของแบบรูปของแบบจำลองการควบคุมการเข้าถึงที่มากกว่าหนึ่ง เป็นต้น ดังนั้นในบทความนี้จึงได้นำเสนอแนวคิดการปรับปรุงยูเอ็มแอลเซคสำหรับการแสดงแบบรูปของแบบจำลองการควบคุมการเข้าถึง ซึ่งสนับสนุนการกำหนดแบบรูปของแบบจำลองการควบคุมการเข้าถึงในการออกแบบซอฟต์แวร์ เพื่อช่วยให้ผู้พัฒนาระบุส่วนประกอบและความสัมพันธ์ของแบบรูปของแบบจำลองการควบคุมการเข้าถึงได้อย่างละเอียดมากยิ่งขึ้น พร้อมทั้งรู้ว่ามีการดำเนินการ (Operation) หรือคุณลักษณะ (Attribute) ใดที่ต้องจัดเก็บไว้เพื่อตอบสนองการใช้งานและการออกแบบด้านความมั่นคงของระบบให้ตรงกับความต้องการ

ในบทความนี้เสนองานวิจัยที่เกี่ยวข้องในหัวข้อที่ 2 แบบรูปของแบบจำลองการควบคุมการเข้าถึงในหัวข้อที่ 3 ยูเอ็มแอลโพรไฟล์ ในหัวข้อที่ 4 แนวคิดของการปรับปรุงยูเอ็มแอลเซคสำหรับแสดงแบบรูปของแบบจำลองการควบคุมการเข้าถึงในหัวข้อที่ 5 และใน

หัวข้อสุดท้ายเป็นบทสรุปและแนวทางในการวิจัยในอนาคต

2. งานวิจัยที่เกี่ยวข้อง

Fernandez และคณะ[4] ได้นำเสนอส่วนประกอบต่างๆ และความสัมพันธ์ที่เป็นของแบบรูปการให้อำนาจ (Authorization) ในการออกแบบซอฟต์แวร์เพื่อให้ส่วนประกอบและความสัมพันธ์ดังกล่าวนั้นช่วยควบคุมการให้อำนาจแก่ผู้ใช้ระบบเป็นไปตามลักษณะของแบบรูปการให้อำนาจ Schumacher และคณะ [1] นำเสนอแบบรูปความมั่นคงเพื่อใช้ในการแก้ไขปัญหาการออกแบบความมั่นคงของระบบทั่วไปพร้อมทั้งนำเสนอส่วนประกอบและความสัมพันธ์ที่สำคัญของแบบรูปความมั่นคงเพื่อให้เป็นแนวทางในการกำหนดส่วนประกอบและความสัมพันธ์ของแบบรูปความมั่นคงในการออกแบบซอฟต์แวร์ Supaporn และคณะ [5] ได้นำส่วนประกอบและความสัมพันธ์ของแบบรูปความมั่นคง [1] มาใช้ในการสร้างไวยากรณ์ความมั่นคงขององค์กรเพื่อช่วยให้ผู้พัฒนาสามารถกำหนดความต้องการความมั่นคงขององค์กรโดยอยู่บนพื้นฐานของแบบรูปความมั่นคง

Jürjens [2] นำเสนอภาคขยายของยูเอ็มแอลชื่อ ยูเอ็มแอลเซค (UMLsec) เพื่อสนับสนุนการออกแบบส่วนประกอบและความสัมพันธ์ทางความมั่นคงของระบบโดยทั่วไปรวมทั้งสนับสนุนการออกแบบความมั่นคงของระบบโดยใช้แบบรูปความมั่นคง [3] อย่างไรก็ตามยูเอ็มแอลเซคยังมีข้อจำกัดในการนำมาใช้กับแบบรูปความมั่นคงเนื่องจากส่วนประกอบและความสัมพันธ์ของแบบรูปความมั่นคงไม่สามารถอธิบายได้อย่างชัดเจนโดยใช้ยูเอ็มแอลเซคเซค Dong และคณะ [6] นำเสนอการปรับปรุงยูเอ็มแอลโพรไฟล์เพื่อแสดงส่วนประกอบและความสัมพันธ์ของแบบรูปการออกแบบ (Design Patterns) ในโปรแกรมประยุกต์โดยมีจุดประสงค์เพื่อให้ผู้พัฒนาได้มองเห็นส่วนประกอบและความสัมพันธ์ของแบบรูปการออกแบบที่มีมากมายในโปรแกรมประยุกต์ที่ซับซ้อนได้ชัดเจนยิ่งขึ้นซึ่งจะนำไปสู่การใช้ประโยชน์ของแบบรูปการออกแบบได้ดียิ่งขึ้น

ในบทความนี้นำเสนอแนวคิดการออกแบบและการแสดงแบบรูปของแบบจำลองการควบคุมการเข้าถึงโดยการขยายยูเอ็มแอลเซคเพื่อช่วยให้ผู้พัฒนาระบุส่วนประกอบและความสัมพันธ์ของแบบรูปของแบบจำลองการควบคุมการเข้าถึงได้อย่างละเอียดมากยิ่งขึ้น ซึ่งจะนำไปสู่การใช้ประโยชน์ของแบบรูปของแบบจำลองการควบคุมการเข้าถึงในการออกแบบและการแสดงความมั่นคงของระบบได้ดีมากยิ่งขึ้น

3. แบบรูปของแบบจำลองการควบคุมการเข้าถึง

แบบรูปของแบบจำลองการควบคุมการเข้าถึง คือกลุ่มของแบบรูปความมั่นคงที่นำเสนอผลเฉลยสำหรับการแก้ไขปัญหาการควบคุมการเข้าถึงที่ปรากฏบ่อยครั้งและสนับสนุนการนำกลับมาใช้ใหม่ ซึ่งแบบรูปความมั่นคงสามารถแบ่งได้เป็น 3 ประเภทคือ

1) แบบรูปการวิเคราะห์ความมั่นคง (Security Analysis Patterns) เป็นแบบรูปที่แก้ปัญหาการวิเคราะห์ความมั่นคงของระบบ

2) แบบรูปการออกแบบความมั่นคง (Security Design Patterns) เป็นแบบรูปที่แก้ปัญหาการออกแบบโครงสร้างความมั่นคงของระบบ

3) แบบรูปกระบวนการความมั่นคง (Security Process Patterns) เป็นแบบรูปที่แก้ปัญหาการออกแบบความมั่นคงให้กับกระบวนการของระบบ

ในบทความนี้ใช้แบบรูปของแบบจำลองการควบคุมการเข้าถึงที่มีลักษณะเป็นแบบรูปการออกแบบความมั่นคง เนื่องจากบทความนี้มุ่งเน้นการออกแบบและการแสดงส่วนประกอบและความสัมพันธ์ของแบบรูปของแบบจำลองการควบคุมการเข้าถึงโดยใช้ยูเอ็มแอลเซค ซึ่งเป็นขั้นตอนของการออกแบบ (Design Phase) และแบบรูปของแบบจำลองการควบคุมการเข้าถึงที่ใช้ในบทความนี้เป็นแบบรูปที่นำเสนอโดย Schumacher และ

คณะ [1] เนื่องจากเป็นแบบรูปของแบบจำลองการควบคุมการเข้าถึงที่มีโครงสร้างเอกสารเหมือนแบบรูปการออกแบบที่นำเสนอโดย Gammar และคณะ [7] และมีโครงสร้างกับขอบเขตที่ชัดเจน โดยแบบรูปของแบบจำลองการควบคุมการเข้าถึงประกอบด้วยแบบรูปความมั่นคงต่างๆ 4 แบบรูปดังต่อไปนี้

1) แบบรูปการให้อำนาจ (Authorization Pattern) เป็นแบบรูปความมั่นคงที่เสนอการแบ่งสิทธิ์ในการเข้าถึงทรัพยากรของผู้ใช้งานในระบบตามผู้ใช้งานรายบุคคล

2) แบบรูปการควบคุมการเข้าถึงเชิงบทบาท (Role-Based Access Control Pattern) เป็นแบบรูปความมั่นคงที่เสนอการแบ่งสิทธิ์ในการเข้าถึงทรัพยากรของผู้ใช้งานในระบบตามบทบาทของผู้ใช้งานในระบบ

3) แบบรูปความมั่นคงหลายระดับ (Multilevel Security Pattern) เป็นแบบรูปความมั่นคงที่เสนอการแบ่งสิทธิ์ในการเข้าถึงทรัพยากรของผู้ใช้งานในระบบตามบทบาทของผู้ใช้งานในระบบ

4) แบบรูปการตรวจสอบการเข้าใช้ทรัพยากร (Reference Monitor Pattern) เป็นแบบรูปความมั่นคงที่เสนอการตรวจสอบในการเข้าถึงทรัพยากรของผู้ใช้งาน

ในบทความนี้ใช้แบบรูปการให้อำนาจเป็นกรณีศึกษาในการปรับปรุงยูเอ็มแอลเซคเนื่องจากแบบรูปของแบบจำลองการควบคุมการเข้าถึงดังกล่าวสามารถความเข้าใจได้ง่ายและมักจะใช้โดยระบบทั่วๆ ไป

4. ยูเอ็มแอลโพรไฟล์

ยูเอ็มแอลโพรไฟล์ [8] เป็นภาคขยายของยูเอ็มแอลที่สนับสนุนการออกแบบที่มีลักษณะเฉพาะเนื่องจากยูเอ็มแอลโพรไฟล์สามารถขยายให้ยูเอ็มแอลรองรับการระบุข้อมูลของการออกแบบที่มีลักษณะเฉพาะได้ เช่น การออกแบบโดยใช้แบบรูปการออกแบบ การออกแบบระบบคลังข้อมูล เป็นต้น ยูเอ็มแอลโพรไฟล์ใช้องค์ประกอบย่อยในการขยายยูเอ็มแอลประกอบไปด้วย 3 ส่วนดังต่อไปนี้

1) แม่พิมพ์ต้นแบบ (Stereotype) เป็นองค์ประกอบที่ใช้ในการระบุชนิดหรือลักษณะเด่นของส่วนประกอบหรือความสัมพันธ์ในการออกแบบที่มีลักษณะเฉพาะ เช่น <<internet link>> เป็นแม่พิมพ์ต้นแบบที่แสดงถึงการเชื่อมโยงโดยใช้อินเทอร์เน็ต <<Server>> เป็นแม่พิมพ์ต้นแบบที่แสดงถึงแม่ข่าย เป็นต้น

2) ค่าป้ายระบุ (Tagged Value) เป็นองค์ประกอบที่ช่วยขยายลักษณะต่างๆของแม่พิมพ์ต้นแบบให้ชัดเจนมากยิ่งขึ้น เช่น type = adsl ของ <<internet link>> เป็นค่าป้ายระบุที่แสดงถึงชนิดของการเชื่อมโยงโดยใช้อินเทอร์เน็ตเป็นแบบเอดีเอสแอล address = 127.0.0 ของ <<Server>> เป็นค่าป้ายระบุที่แสดงถึงเลขที่อยู่ของแม่ข่าย เป็นต้น

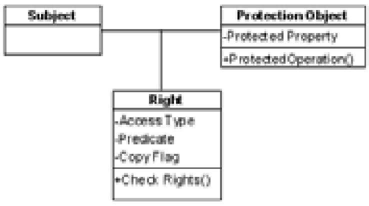
3) เงื่อนไขบังคับ (Constraint) เป็นข้อบังคับของแม่พิมพ์ต้นแบบหรือค่าป้ายระบุที่จำเป็นต้องพิจารณาเมื่อมีการใช้งาน ซึ่งเงื่อนไขบังคับจะถูกระบุเป็นภาษาโอซีแอล (OCL: Object Constraint Language) เช่น <<Server>> มีเงื่อนไขบังคับข้อที่ 1 เป็น self.taggedValue.dataValue.name -> notEmpty แสดงถึงชื่อของแม่ข่ายไม่สามารถเป็นค่าว่างได้ เป็นต้น

5. แนวคิดการปรับปรุงยูเอ็มแอลเซคสำหรับแสดงแบบรูปของแบบจำลองการควบคุมการเข้าถึง

จากความต้องการในการปรับปรุงยูเอ็มแอลเซคเพื่อแสดงแบบรูปของแบบจำลองการควบคุมการเข้าถึงสามารถแสดงขั้นตอนการดำเนินการเสนอแนวคิดการปรับปรุงยูเอ็มแอลเซคเพื่อแสดงแบบรูปของแบบจำลองการควบคุมการเข้าถึงประกอบด้วยสามส่วนหลักๆ คือ

5.1. ศึกษาแบบรูปของแบบจำลองการควบคุมการเข้าถึง

บทความนี้ใช้แบบรูปการให้อำนาจเป็นกรณีศึกษาเพื่อการปรับปรุงยูเอ็มแอลเซค ดังแสดงในรูปที่ 2



รูปที่ 2 แผนภาพคลาสแสดงโครงสร้างแบบรูปการให้อำนาจ [1]

ซึ่งจากการศึกษาแบบรูปการให้อำนาจพบว่า โครงสร้างที่สำคัญของแบบรูปการให้อำนาจประกอบไปด้วยคลาส Protection Object ซึ่งเป็นคลาสที่เป็นทรัพยากรของระบบที่จะต้องควบคุมการเข้าถึงจากคลาส Subject โดยการควบคุมสิทธิ์ในการเข้าถึงจากการใช้การดำเนินการ Check Right ของคลาส Right โดยที่คลาส Right จะมีคุณลักษณะในการเข้าถึงคือ คุณลักษณะ Access Type เป็นคุณลักษณะที่บอกถึงประเภทของการเข้าถึง คุณลักษณะ Predicate เป็นคุณลักษณะที่บอกถึงเงื่อนไขของการยกเลิกการเข้าถึงและคุณลักษณะ Copy Flag เป็นคุณลักษณะที่บอกถึงสิทธิ์ในการเข้าถึงนี้ได้รับมอบมาจากคลาส Subject อื่นหรือไม่

5.2. ปรับปรุงยูเอ็มแอลเซคเพื่อแสดงแบบรูปของแบบจำลองการควบคุมการเข้าถึง

เมื่อทำการศึกษาและวิเคราะห์แบบรูปของแบบจำลองการควบคุมการเข้าถึงแล้ว ขั้นตอนต่อไปเป็นการปรับปรุงยูเอ็มแอลเซคเพื่อแสดงแบบรูปของแบบจำลองการควบคุมการเข้าถึง ซึ่งใช้หลักการ 2 ประการในการปรับปรุงดังต่อไปนี้

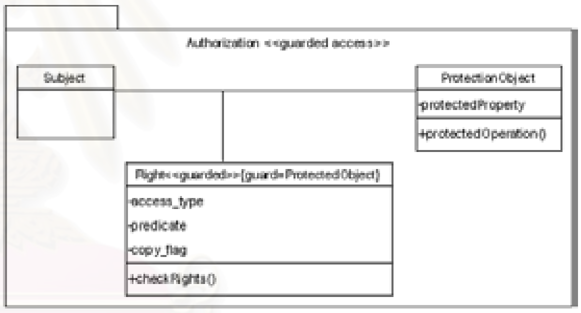
1) แสดงส่วนประกอบและความสัมพันธ์ของแบบรูปของแบบจำลองการควบคุมการเข้าถึงที่มีลักษณะเฉพาะของโครงสร้างนั้นกล่าวคือ การแสดงคลาส คุณลักษณะ การดำเนินการ และความสัมพันธ์ที่สำคัญของแบบรูปของแบบจำลองการควบคุมการเข้าถึงที่เป็นลักษณะเฉพาะของแต่ละแบบรูป

2) ลดความซับซ้อนของการแสดงแบบรูปของแบบจำลองการควบคุมการเข้าถึง กล่าวคือ เป็นการลดความซับซ้อนที่เกิดจากการแสดงข้อมูลของแบบรูปของแบบจำลองการควบคุมการเข้าถึงในยูเอ็มแอล รวมทั้งการปรับปรุงรูปแบบการแสดงของยูเอ็มเซคบางองค์ประกอบเพื่อรองรับการแสดงของแบบรูปของแบบจำลองการควบคุมการเข้าถึง

ในส่วนนี้เราใช้แบบรูปของแบบจำลองการควบคุมการเข้าถึงที่ทำการศึกษาเป็นกรณีศึกษา เพื่อการปรับปรุงยูเอ็มแอลเซคคือ แบบรูปการให้อำนาจ โดยมีขั้นตอนต่อไปนี้

5.2.1. <u>แสดงแบบรูปความมั่นคงโดยใช้ยูเอ็มแอลเซค</u>

จากรูปที่ 3 มีการใช้แม่พิมพ์ต้นแบบคือ <<guarded access>> และ <<guarded>> ซึ่งแม่พิมพ์ต้นแบบ <<guarded access>> แสดงถึงมีการใช้การป้องกันการเข้าถึงซึ่งจะมีแม่พิมพ์ต้นแบบ <<guarded>> แสดงถึงคลาสที่ทำหน้าที่ป้องกันการเข้าถึงคลาสที่ระบุในป้ายระบุ guard ซึ่งในที่นี้ก็คือคลาส ProtectionObject



รูปที่ 3 แผนภาพคลาสแสดงแบบรูปการให้อำนาจโดยใช้ยูเอ็มแอลเซค

5.2.2. <u>วิเคราะห์และปรับปรุงยูเอ็มแอลเซค</u>

จากการวิเคราะห์การแสดงแบบรูปการให้อำนาจในยูเอ็มแอลเซค พบว่า

1) ไม่สามารถบอกได้ว่าคุณลักษณะหรือการดำเนินการใดของระบบนั้นเป็นคุณลักษณะหรือการดำเนินการของแบบรูปการให้อำนาจ

2) ไม่สามารถให้อิสระในการตั้งชื่อส่วนประกอบที่เป็นของแบบรูปการให้อำนาจได้เนื่องจากผู้พัฒนาจะต้องตั้งชื่อส่วนประกอบให้สอดคล้องกับหน้าที่ในแบบรูปการให้อำนาจ ซึ่งจะนำไปสู่ปัญหาในการ

ตัดสินใจว่า ควรตั้งชื่อส่วนประกอบนั้นอย่างไร ถ้าระบบนั้นมีการใช้หลายๆ แบบรูปของแบบจำลองการควบคุมการเข้าถึง และส่วนประกอบนั้นเป็นส่วนประกอบของแบบรูปของแบบจำลองการควบคุมการเข้าถึงที่มากกว่าหนึ่ง

3) ถ้ามีการเพิ่มแม่พิมพ์ต้นแบบหรือป้ายระบุของแบบรูปความมั่นคง จะทำให้เกิดการสับสนในการระบุแม่พิมพ์ต้นแบบหรือป้ายระบุ เช่น สมมติว่าทำการเพิ่มแม่พิมพ์ต้นแบบ <<A>> ลงในคลาส Right จะทำให้ได้รูปแบบของการแสดงแม่พิมพ์ต้นแบบและป้ายระบุเป็น <<guarded>>{guard=ProtectionObject}<<A>> จะเห็นได้ว่าเกิดการสับสนในการจำแนกว่าป้ายระบุ guard เป็นของแม่พิมพ์ต้นแบบใดระหว่างแม่พิมพ์ต้นแบบ <<guarded>> หรือแม่พิมพ์ต้นแบบ <<A>> เป็นต้น

จากการวิเคราะห์ที่ได้ทำให้เกิดการปรับปรุงยูเอ็มแอลเซคดังนี้

1) ทำการเพิ่มแม่พิมพ์ต้นแบบเพื่อระบุส่วนประกอบของแบบรูปของแบบจำลองการควบคุมการเข้าถึงคือ

1.1) APC (Access control model Pattern Class) คือ แม่พิมพ์ต้นแบบที่แสดงถึงคลาสของแบบรูปของแบบจำลองการควบคุมการเข้าถึง

1.2) APA (Access control model Pattern Attribute) คือ แม่พิมพ์ต้นแบบที่แสดงคุณลักษณะของแบบรูปของแบบจำลองการควบคุมการเข้าถึง

1.3) APO (Access control model Pattern Operation) คือ แม่พิมพ์ต้นแบบที่แสดงการดำเนินการของแบบรูปของแบบจำลองการควบคุมการเข้าถึง

ทำการเพิ่มค่าป้ายระบุเพื่อระบุหน้าที่ในแต่ละแม่พิมพ์ต้นแบบที่ทำการเพิ่มคือ Pattern Role คือบทบาทในแบบรูป และ Pattern Name คือชื่อของแบบรูป

2) ทำการกำหนดรูปแบบของการแสดงแม่พิมพ์ต้นแบบและค่าป้ายระบุคือ

2.1) รูปแบบการแสดงแม่พิมพ์ต้นแบบคลาสคือ <<APC { หน้าที่ของคลาสในแบบรูปของแบบจำลองการควบคุมการเข้าถึง @ ชื่อแบบรูปของแบบจำลองการควบคุมการเข้าถึง }

2.2) รูปแบบการแสดงแม่พิมพ์ต้นแบบคุณลักษณะคือ <<APA { หน้าที่ของคลาสในแบบรูปของแบบจำลองการควบคุมการเข้าถึง @ ชื่อแบบรูปของแบบจำลองการควบคุมการเข้าถึง }

2.3) รูปแบบการแสดงแม่พิมพ์ต้นแบบการดำเนินการคือ <<APO { หน้าที่ของคลาสในแบบรูปของแบบจำลองการควบคุมการเข้าถึง @ ชื่อแบบรูปของแบบจำลองการควบคุมการเข้าถึง }

ซึ่งรูปแบบของการแสดงแม่พิมพ์ต้นแบบและค่าป้ายระบุนี้สามารถแก้ไขปัญหาการตั้งชื่อของคลาส คุณลักษณะและการดำเนินการให้สอดคล้องกับแบบรูปการให้อำนาจ ตัวอย่างเช่น คลาสชื่อ User กำกับด้วย <<APC{Subject@Authorization}>> หมายถึงคลาสนี้ทำหน้าที่เป็น Subject ในแบบรูปการให้อำนาจ เป็นต้น

3) ทำการย้ายบางป้ายระบุเข้าไปในแม่พิมพ์ต้นแบบ คือ ย้ายป้ายระบุ guard เข้าไปในแม่พิมพ์ต้นแบบ <<guarded>> จะทำให้ได้รูปแบบของแม่พิมพ์ต้นแบบและป้ายระบุเป็น <guarded{guard=ProtectionObject}>>

5.2.3. แสดงแบบรูปความมั่นคงด้วยยูเอ็มแอลเซคที่ปรับปรุงแล้ว

สามารถแสดงส่วนประกอบและความสัมพันธ์ของแบบรูปการให้อำนาจโดยใช้ยูเอ็มแอลเซคที่ปรับปรุงแล้วได้ดังแสดงในรูป ก-1 ของภาคผนวก ก ซึ่งมีการใช้แม่พิมพ์ต้นแบบและค่าป้ายระบุเพื่อระบุส่วนประกอบและความสัมพันธ์ของแบบรูปการให้อำนาจ เช่น Right<<APC{Right@Authorization}>> แสดงถึงคลาส Right ทำหน้าที่เป็นคลาส Right ในแบบรูปการให้อำนาจ เป็นต้น

เราใช้วิธีการเช่นเดียวกันกับการปรับปรุงยูเอ็มแอลเซคเพื่อแสดงส่วนประกอบและความสัมพันธ์ของแบบรูปของแบบจำลองการควบคุมการเข้าถึงส่วนที่เหลือได้แก่ แบบรูปการควบคุมการเข้าถึงเชิงบทบาท แบบรูป

ความมั่นคงหลายระดับ และแบบรูปการตรวจสอบการเข้าใช้ทรัพยากร เมื่อทำการปรับปรุงยูเอ็มแอลเซคเรียบร้อยแล้วสามารถแสดงแบบรูปของแบบจำลองการควบคุมการเข้าถึงดังกล่าวโดยใช้ยูเอ็มแอลเซคที่ปรับปรุงเพิ่มเติม ดังแสดงในรูป ก-2 ก-3 และ ก-4 ของภาคผนวก ก ตามลำดับ จากการปรับปรุงยูเอ็มแอลเซคดังกล่าว จะทำให้เกิดการเพิ่มแม่พิมพ์ต้นแบบและค่าป้ายระบุจากยูเอ็มแอลเซคเดิมเพื่อทำหน้าที่ในการระบุส่วนประกอบของแบบรูปของแบบจำลองการควบคุมการเข้าถึง ดังแสดงในตารางที่ 1 และ 2 ตามลำดับ

ตารางที่ 1 แม่พิมพ์ต้นแบบที่เพิ่มเติม

แม่พิมพ์ต้นแบบ (Stereotype)	ใช้ใน	ความหมาย
APC (Access Control Model Pattern Class)	คลาส (Class)	ใช้ระบุคลาสที่เป็นองค์ประกอบของแบบรูปของแบบจำลองการควบคุมการเข้าถึง
APA (Access Control Model Pattern Attribute)	คุณลักษณะ (Attribute)	ใช้ระบุคุณลักษณะที่เป็นองค์ประกอบของแบบรูปของแบบจำลองการควบคุมการเข้าถึง
APO (Access Control Model Pattern Operation)	การดำเนินการ (Operation)	ใช้ระบุการดำเนินการที่เป็นองค์ประกอบของแบบรูปของแบบจำลองการควบคุมการเข้าถึง

ตารางที่ 2 ค่าป้ายระบุที่เพิ่มเติม

ค่าป้ายระบุ (Tagged Value)	ใช้ในแม่พิมพ์ต้นแบบ	ความหมาย
{ หน้าที่ของคลาสในแบบรูปของแบบจำลองการควบคุมการเข้าถึง @ ชื่อแบบรูปของแบบจำลองการควบคุมการเข้าถึง }	APC	ใช้ระบุหน้าที่ของคลาสในแบบรูปของแบบจำลองการควบคุมการเข้าถึงที่กำหนด
{ หน้าที่ของคุณลักษณะในแบบรูปของแบบจำลองการควบคุมการเข้าถึง @ ชื่อแบบรูปของแบบจำลองการควบคุมการเข้าถึง }	APA	ใช้ระบุหน้าที่ของคุณลักษณะในแบบรูปของแบบจำลองการควบคุมการเข้าถึงที่กำหนด
{ หน้าที่ของการดำเนินการในแบบรูปของแบบจำลองการควบคุมการเข้าถึง @ ชื่อแบบรูปของแบบจำลองการควบคุมการเข้าถึง }	APO	ใช้ระบุหน้าที่ของการดำเนินการในแบบรูปของแบบจำลองการควบคุมการเข้าถึงที่กำหนด

5.3. ตรวจสอบยูเอ็มแอลเซคที่ปรับปรุงเพิ่มเติม

เราได้ทำการตรวจสอบยูเอ็มแอลเซคที่ปรับปรุงแล้วโดยการวัดการความซับซ้อนของการใช้ยูเอ็มแอลเซคแสดงส่วนประกอบและความสัมพันธ์ของแบบรูปของแบบจำลองการควบคุมการเข้าถึงในระบบตัวอย่างดังแสดงในรูป ก-5 ของภาคผนวก ก ซึ่งเป็นระบบการนัดหมายของแพทย์ที่มีการใช้แบบรูปของแบบจำลองการควบคุมการเข้าถึงคือ แบบรูปการให้อำนาจ ซึ่งจากการตรวจสอบพบว่าเกิดความซับซ้อนของการแสดงแม่พิมพ์ต้นแบบและค่าป้ายระบุค่อนข้างมากเนื่องจากแม่พิมพ์ต้นแบบและค่าป้ายระบุที่เพิ่มเข้าไป ซึ่งจะนำไปเป็นแนวทางในการปรับปรุงการแสดงส่วนประกอบและความสัมพันธ์ของแบบรูปของแบบจำลองการควบคุมการเข้าถึงต่อไป

6. สรุปงานวิจัยและแนวทางพัฒนาต่อ

งานวิจัยนี้ได้นำเสนอแนวคิดการปรับปรุงยูเอ็มแอลเซคสำหรับการออกแบบและการแสดงส่วนประกอบและความสัมพันธ์ของแบบรูปของแบบจำลองการควบคุมการเข้าถึงเพื่อช่วยให้ผู้พัฒนาส่วนประกอบและความสัมพันธ์ของแบบรูปของแบบจำลองการควบคุมการเข้าถึงได้ชัดเจนยิ่งขึ้น จึงทำให้ใช้ประโยชน์ของแบบรูปของแบบจำลองการควบคุมการเข้าถึงได้อย่างเต็มที่

แนวทางในการพัฒนาต่อของผู้วิจัยคือ ทำการปรับปรุงยูเอ็มแอลเซคให้สนับสนุนการออกแบบและการแสดงส่วนประกอบและความสัมพันธ์ของแบบรูปความมั่นคงในกลุ่มอื่นที่นำเสนอโดย Schumacher และคณะ [2] รวมทั้งสร้างเครื่องมือเพื่อสนับสนุนการออกแบบและการแสดงแบบรูปความมั่นคงโดยใช้ยูเอ็มแอลเซค

7. บรรณานุกรม

[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] J. Jürjens, *UMLsec: Extending UML for Secure Systems Development*, Department of Informatics, Munich University of Technology, Germany, 2002.

[3] J. Jürjens, G. Popp and G. Wimmel, *Towards Using Security Patterns in Model-based System Development*, Department of Computer Science, Munich University of Technology, Germany, 2002.

[4] E. Fernandez-Buglioni, *Metadata and authorization patterns*, Florida Atlantic University, 2000.

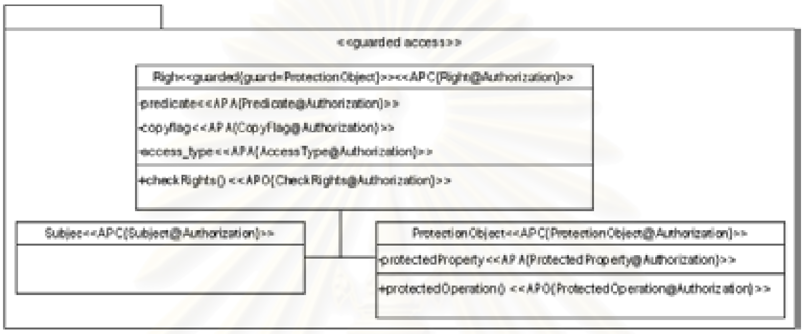
[5] K. Supaporn, N. Prompoon and T. Rojkangsadan, *Enterprise Assets Security Requirements Construction from ESRMG Grammar based on Security Patterns*, *14th Asia-Pacific Software Engineering Conference*, pages 112-119, 2007.

[6] J. Dong, S. Yang and K. Zhang, *Visualizing Design Patterns in Their Applications and Composition*, In *IEEE Transactions on Software Engineering, Vol. 33, No. 7,* pages 433-453, 2007.

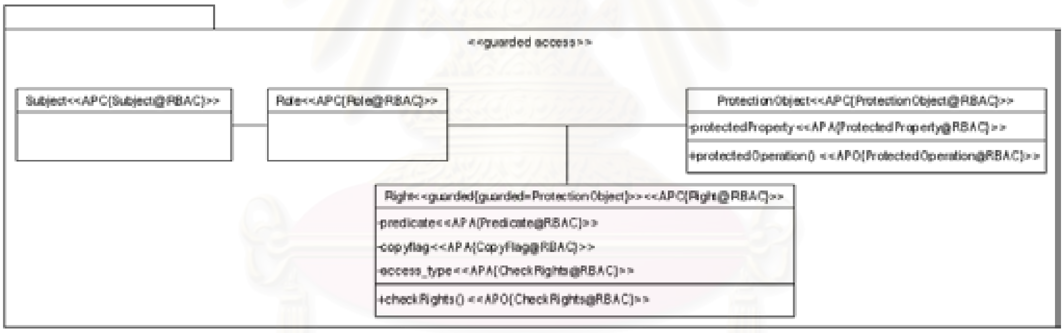
[7] E. Gamma, R. Helm, R. Johnson and J. Vlissides, *Design Patterns – Elements of Reusable Object-Oriented Software*, Addison-Wesley, 1995.

[8] K. Hamilton and R. Miles, *Learning UML 2.0*, O'Reilly, 2006.

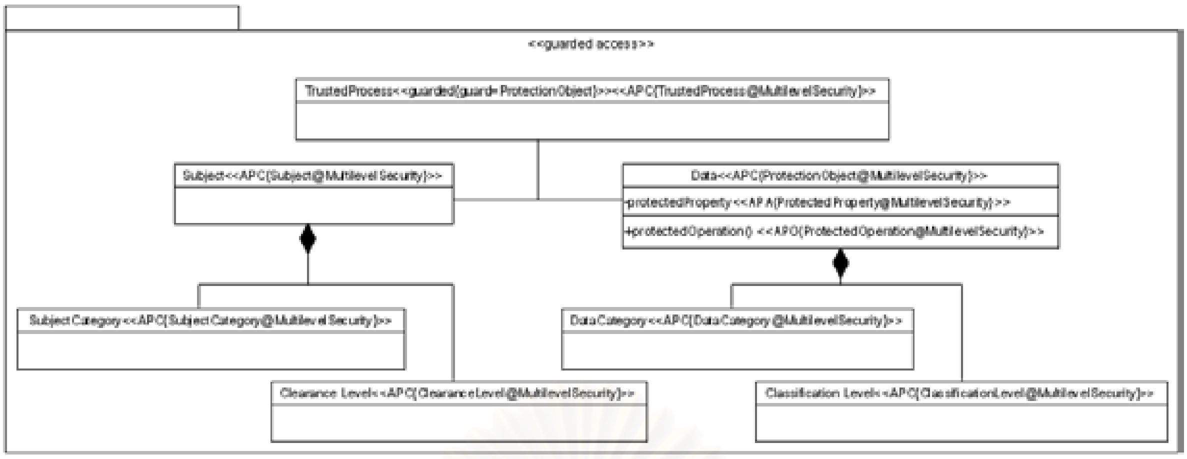
ภาคผนวก ก



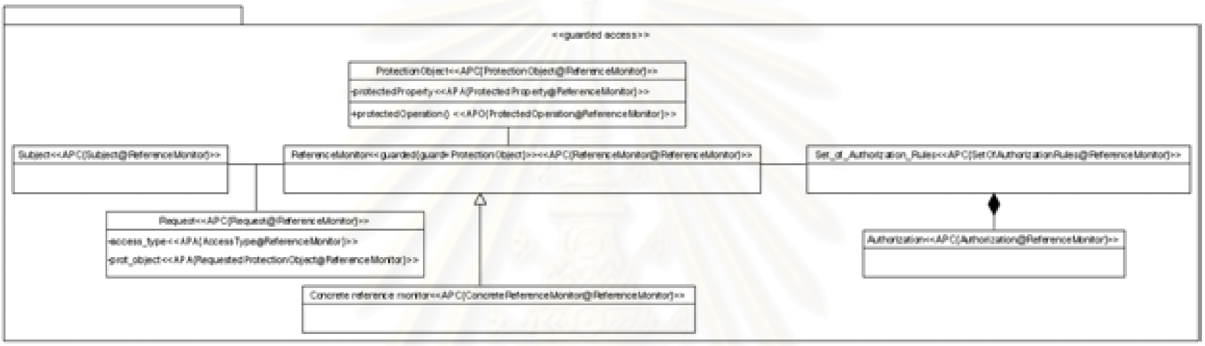
รูป ก-1 แผนภาพคลาสแสดงแบบรูปการให้อำนาจโดยใช้ยูเอ็มแอลเซคที่ปรับปรุงแล้ว



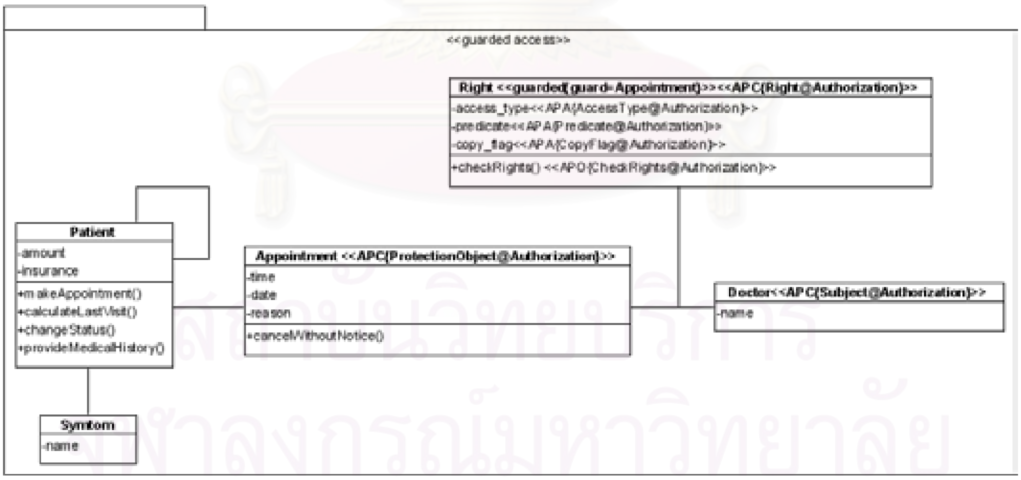
รูป ก-2 แผนภาพคลาสแสดงแบบรูปการควบคุมการเข้าถึงเชิงบทบาทโดยใช้ยูเอ็มแอลเซคที่ได้รับการปรับปรุงแล้ว



รูป ก-3 แผนภาพคลาสแสดงแบบรูปความมั่นคงหลายระดับโดยใช้ยูเอ็มแอลเซคที่ได้รับการปรับปรุงแล้ว



รูป ก-4 แผนภาพคลาสแสดงแบบรูปการตรวจสอบการเข้าใช้ทรัพยากรโดยใช้ยูเอ็มแอลเซคที่ได้รับการปรับปรุงแล้ว



รูป ก-5 ตัวอย่างของการแสดงแบบรูปการให้อำนาจโดยใช้ยูเอ็มแอลเซคที่ปรับปรุงเพิ่มเติม

เครื่องมือสำหรับการกำหนดข้อมูลและโครงสร้างแบบรูปของแบบจำลองการควบคุมการเข้าถึง

Access Control Model Pattern Information and Structure Definition Tool

เกียรติศักดิ์ ไชยสมบูรณ์ และ นครทิพย์ พร้อมพูล
ห้องปฏิบัติการวิศวกรรมซอฟต์แวร์ ศูนย์เชี่ยวชาญเฉพาะทางด้านวิศวกรรมซอฟต์แวร์
ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
อีเมล : kiattisak.c@student.chula.ac.th and nakornthip.s@chula.ac.th

บทคัดย่อ

ความมั่นคงของระบบซอฟต์แวร์กลายเป็นประเด็นสำคัญที่ต้องตระหนักในทุกองค์กรเนื่องจากการปรากฏของภัยคุกคามที่มีมากขึ้นและหลากหลายในปัจจุบัน ดังนั้นองค์กรจึงมีความจำเป็นที่จะต้องนำหลักการความมั่นคงมาประยุกต์ใช้ในองค์กรที่สอดคล้องกับความต้องการและลักษณะของระบบ ซึ่งการนำแบบรูปของแบบจำลองการควบคุมการเข้าถึงมาประยุกต์ใช้ในการพัฒนาซอฟต์แวร์นั้นเป็นอีกทางเลือกที่ดีในการแก้ปัญหาความมั่นคงของระบบซอฟต์แวร์ เนื่องจากกลุ่มแบบรูปนี้เป็นกลุ่มของแบบรูปความมั่นคงที่อธิบายการออกแบบการควบคุมการเข้าถึงของระบบและเสนอคำตอบที่ได้รับการพิสูจน์แล้วเพื่อแก้ไขปัญหารวมทั้งมีการใช้งานอย่างแพร่หลาย ดังนั้นงานวิจัยนี้จึงนำเสนอเครื่องมือสำหรับกำหนดข้อมูลและโครงสร้างแบบรูปของแบบจำลองการควบคุมการเข้าถึงรวมทั้งอาศัยยูเอ็มแอลเซค (UMLsec) ที่ปรับปรุงเพิ่มเติมเพื่อสนับสนุนให้ผู้พัฒนาระบุส่วนประกอบและความสัมพันธ์ของแบบรูปได้อย่างละเอียดมากยิ่งขึ้น เครื่องมือนี้จะช่วยให้ผู้พัฒนาสามารถใช้แบบรูปของแบบจำลองการควบคุมการเข้าถึงในการออกแบบระบบที่ต้องการความปลอดภัยได้อย่างมีประสิทธิภาพ

คำสำคัญ: ความมั่นคง แบบรูปความมั่นคง ยูเอ็มแอล ยูเอ็มแอลโพรไฟล์

Abstract

Security of software system is an important issue which many enterprises have to consider because various kinds of threats occur increasingly in present. So, they have to apply security principles align to their needs and system features. Applying access control model patterns in software development is a good choice and widely used among security engineers to solve a security problem in software system because it is one group of security patterns that describes access control design of system and suggests proven answers to solved problems. In this paper, we present a tool for defining information of access control model pattern and its structure. In addition, with the use of an extending UMLsec, this tool can help define in more details of pattern components and their relationships. A proposed tool will support developers in applying access control model patterns in security software design efficiently.

Keywords: Security, Security Pattern, UML, UML profile

1. บทนำ

ในปัจจุบันปัญหาการคุกคามความมั่นคงของระบบซอฟต์แวร์มีมากขึ้น เนื่องมาจากองค์กรส่วนใหญ่อาศัยคอมพิวเตอร์เพื่อสนับสนุนการจัดการและบริหารมากขึ้น จึงทำให้มีสินทรัพย์ (Asset) ที่เรียกว่า ข้อมูลสารสนเทศ (Information) ทางธุรกิจมีมากขึ้นตามไปด้วย ดังนั้นข้อมูลเหล่านี้จึงจำเป็นต้องเก็บไว้อย่างมั่นคงและปลอดภัยจากภัยคุกคามแบบต่างๆ จึงมีความจำเป็นต้องใช้หลักการความมั่นคง (Security Principles) มาประยุกต์ใช้ในการออกแบบระบบซอฟต์แวร์ขององค์กร

แบบรูปความมั่นคง (Security Patterns) เป็นแบบรูปที่นำเสนอแนวคิดในรูปผลเฉลยที่ได้จากการนำหลักการความมั่นคงมาประยุกต์ใช้ประกอบกับการพิสูจน์แล้วว่ามีความเหมาะสมและนำไปประยุกต์ใช้ได้จริง จึงทำให้รูปผลเฉลยนี้สามารถแก้ไขปัญหาความมั่นคงทั่วไปที่เกิดขึ้นบ่อยครั้งได้ ดังนั้นการนำแบบรูปความมั่นคงมาประยุกต์ใช้ในการออกแบบระบบซอฟต์แวร์ขององค์กรนั้น จึงเป็นอีกทางเลือกที่เหมาะสม

โดยทั่วไปกลุ่มแบบรูปความมั่นคงที่ถูกใช้อย่างแพร่หลายคือ แบบรูปของแบบจำลองการควบคุมการเข้าถึงเนื่องจากกลุ่มแบบรูปความมั่นคงดังกล่าวเป็นกลุ่มแบบรูปความมั่นคงพื้นฐานที่ใช้ในการออกแบบการควบคุมการเข้าถึงในระบบซอฟต์แวร์โดยทั่วไป อย่างไรก็ตามการศึกษาและวิเคราะห์แบบรูปของแบบจำลองการควบคุมการเข้าถึงเพื่อนำมาประยุกต์ใช้ในการออกแบบซอฟต์แวร์นั้นทำได้ยากเนื่องจากกลุ่มแบบรูปดังกล่าวได้กำหนดโครงสร้างที่ประกอบไปด้วยส่วนประกอบและความสัมพันธ์ของแบบรูปของแบบจำลองการควบคุมการเข้าถึงไว้ในระดับที่ค่อนข้างสูง ซึ่งผู้พัฒนาจะต้องศึกษาและวิเคราะห์โครงสร้างดังกล่าวของแบบรูปของแบบจำลองการควบคุมการเข้าถึงเมื่อนำแบบรูปของแบบจำลองการควบคุมการเข้าถึงไปประยุกต์ใช้ในการออกแบบและการปรับปรุงการออกแบบซอฟต์แวร์ หากละเลยการพิจารณาดังกล่าว จะทำให้การออกแบบและการปรับปรุงการออกแบบซอฟต์แวร์ที่เกี่ยวข้องกับแบบรูปของแบบจำลองการควบคุมการเข้าถึงนั้นจะมีจุดอ่อนที่ทำให้ผู้บุกรุก (Intruder) โจมตีได้ง่าย และอาจเกิดปัญหาต่างๆ เช่น ข้อมูลสูญหาย การเชื่อมต่อของเครือข่ายถูกรบกวน เป็นต้น

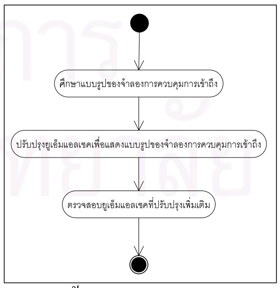
Chaisomboon และคณะ [4] ได้นำเสนอส่วนขยายของยูเอ็มแอลเซคเพื่อสนับสนุนการกำหนดโครงสร้างแบบรูปของแบบจำลองการควบคุมการเข้าถึงในการออกแบบระบบซอฟต์แวร์ ซึ่งจะช่วยให้ผู้พัฒนาระบุส่วนประกอบและความสัมพันธ์ของแบบรูปของแบบจำลองการควบคุมการเข้าถึงได้อย่างละเอียดมากยิ่งขึ้น พร้อมทั้งรู้ว่ามีการดำเนินการ (Operation) หรือคุณลักษณะ (Attribute) ใดที่ต้องจัดเก็บไว้เพื่อตอบสนองการใช้งานและการออกแบบด้านความมั่นคงของระบบให้ตรงกับความต้องการ

อย่างไรก็ตามการนำยูเอ็มแอลเซคที่ปรับปรุงเพิ่มเติมจาก [4] ยังไม่เหมาะสมที่จะนำมาใช้งานจริง เช่น ข้อมูลของแบบรูปของแบบจำลองการควบคุมการเข้าถึงมีลักษณะเป็นข้อความ ซึ่งอาจทำให้ผู้ใช้งานกำหนดข้อมูลของแบบรูปได้ไม่สะดวกและในการออกแบบระบบโดยใช้แบบรูปของแบบจำลองการควบคุมการเข้าถึงนั้น ผู้ใช้งานจะต้องทำการสร้างคลาสเพื่อประกอบเป็นโครงสร้างของแบบรูป ซึ่งจะทำให้เสียเวลาในการสร้างโครงสร้างของแบบรูป เป็นต้น ซึ่งปัญหาเหล่านี้สามารถแก้ไขได้โดยการสร้างเครื่องมือช่วยเหลือการกำหนดข้อมูลและโครงสร้างของแบบรูป ดังนั้นในงานวิจัยนี้จึง วิเคราะห์ ออกแบบ และสร้างเครื่องมือสำหรับกำหนดข้อมูลและโครงสร้างแบบรูปของแบบจำลองการควบคุมการเข้าถึง ซึ่งเครื่องมือนี้สามารถใช้ยูเอ็มแอลเซคเพิ่มเติมที่ผู้วิจัยนำเสนอไว้ใน [4] ในการระบุส่วนประกอบและความสัมพันธ์ของแบบรูปได้อย่างละเอียดมากยิ่งขึ้น เพื่อตอบสนองความต้องการผู้ใช้หรือผู้พัฒนาในการนำแบบรูปของแบบจำลองการควบคุมการเข้าถึงไปใช้ออกแบบระบบที่ต้องการความปลอดภัยได้อย่างมีประสิทธิภาพ

2. งานวิจัยที่เกี่ยวข้อง

Schumacher และคณะ [1] นำเสนอแบบรูปความมั่นคงเพื่อใช้ในการแก้ไขปัญหาการออกแบบความมั่นคงของระบบทั่วไปพร้อมทั้งนำเสนอส่วนประกอบและความสัมพันธ์ที่สำคัญของแบบรูปความมั่นคงเพื่อให้เป็นแนวทางในการกำหนดส่วนประกอบและความสัมพันธ์ของแบบรูปความมั่นคงในการออกแบบซอฟต์แวร์ ต่อมา Supaporn และคณะ [2] ได้นำส่วนประกอบและความสัมพันธ์ของแบบรูปความมั่นคง [1] มาใช้ในการสร้างไวยากรณ์ความมั่นคงขององค์กรเพื่อช่วยให้ผู้พัฒนาสามารถกำหนดความต้องการความมั่นคงขององค์กรโดยอยู่บนพื้นฐานของแบบรูปความมั่นคง Jürjens [3] นำเสนอภาคขยายของยูเอ็มแอลชื่อ ยูเอ็มแอลเซค (UMLsec) เพื่อสนับสนุนการออกแบบส่วนประกอบและความสัมพันธ์ทางความมั่นคงของระบบโดยทั่วไปรวมทั้งสนับสนุนการออกแบบความมั่นคงของระบบโดยใช้แบบรูปความมั่นคง [1] อย่างไรก็ตามยูเอ็มแอลเซคยังมีข้อจำกัดในการนำมาใช้กับแบบรูปความมั่นคงเนื่องจากส่วนประกอบและความสัมพันธ์ของแบบรูปความมั่นคงไม่สามารถอธิบายได้อย่างชัดเจนโดยใช้ยูเอ็มแอลเซค

ผู้วิจัยได้นำเสนอแนวคิดในการปรับปรุงยูเอ็มแอลเซคสำหรับการแสดงแบบรูปของแบบจำลองการควบคุมการเข้าถึง [4] แบ่งเป็น 3 ขั้นตอนสำคัญได้แก่ ศึกษาแบบรูปของแบบจำลองการควบคุมการเข้าถึง ปรับปรุงยูเอ็มแอลเซคเพื่อแสดงแบบรูปของแบบจำลองการควบคุมการเข้าถึง และ ตรวจสอบยูเอ็มแอลเซคที่ปรับปรุงเพิ่มเติม ดังแสดงในรูปที่ 1 โดยแต่ละขั้นตอนมีรายละเอียดโดยสังเขปดังนี้



รูปที่ 1 แผนภาพกิจกรรมขั้นตอนการปรับปรุงยูเอ็มแอลเซคเพื่อแสดงแบบรูปของแบบจำลองการควบคุมการเข้าถึง

1) ศึกษาแบบรูปของแบบจำลองการควบคุมการเข้าถึง

ขั้นตอนนี้มีวัตถุประสงค์เพื่อศึกษาแบบรูปของแบบจำลองการควบคุมการเข้าถึง โดยการวิเคราะห์โครงสร้างของแบบจำลองการ

ควบคุมการเข้าถึงด้วยแผนภาพคลาส (Class diagram) ทำให้ทราบถึงองค์ประกอบและความสัมพันธ์ระหว่างองค์ประกอบ โครงสร้างของแบบรูปจำลองการควบคุมการเข้าถึงที่ทำการศึกษาแสดงได้ดังต่อไปนี้

1. แบบรูปการให้อำนาจ
2. แบบรูปการควบคุมการเข้าถึงเชิงบทบาท
3. แบบรูปความมั่นคงหลายระดับ
4. แบบรูปการตรวจสอบการเข้าใช้ทรัพยากร

2) ปรับปรุงยูเอ็มแอลเซคเพื่อแสดงแบบรูปของแบบจำลองการควบคุมการเข้าถึง

เมื่อทำการศึกษาและวิเคราะห์แบบรูปของแบบจำลองการควบคุมการเข้าถึงแล้ว ขั้นตอนต่อไปเป็นการปรับปรุงยูเอ็มแอลเซคเพื่อแสดงแบบรูปของแบบจำลองการควบคุมการเข้าถึง ซึ่งใช้หลักการในการปรับปรุงดังต่อไปนี้

1) แสดงโครงสร้างแบบรูปของแบบจำลองการควบคุมการเข้าถึงที่มีลักษณะเฉพาะของโครงสร้างนั้นกล่าวคือ การแสดงคลาส คุณลักษณะ (Attribute) การดำเนินการ (Operation) และองค์ประกอบอื่นที่สำคัญของแบบรูปจำลองการควบคุมการเข้าถึงที่เป็นลักษณะเฉพาะของแต่ละแบบรูป

2) ลดความซับซ้อนของการแสดงแบบรูปของแบบจำลองการควบคุมการเข้าถึงกล่าวคือ การลดความซับซ้อนที่เกิดจากการแสดงข้อมูลของแบบรูปที่เกิดจากการใช้ยูเอ็มแอลเซคที่ปรับปรุงเพิ่มเติม รวมทั้งการปรับปรุงรูปแบบการแสดงของยูเอ็มแอลเซคบางองค์ประกอบเพื่อรองรับการแสดงข้อมูลของแบบรูป

จากหลักการดังกล่าวทำให้เกิดการเพิ่มแม่พิมพ์ต้นแบบและค่าป้ายระบุจากยูเอ็มแอลเซคเพื่อทำหน้าที่ในการระบุองค์ประกอบของแบบรูปของแบบจำลองการควบคุมการเข้าถึง ซึ่งจากหลักการดังกล่าวจึงทำให้เกิดแม่พิมพ์ต้นแบบและค่าป้ายระบุเพื่อแสดงองค์ประกอบของแบบรูปของแบบจำลองการควบคุมการเข้าถึงดังตารางที่ 1 และ 2

ตารางที่ 1 แม่พิมพ์ต้นแบบที่เพิ่มเติม

แม่พิมพ์ต้นแบบ (Stereotype)	ใช้ใน	ความหมาย
APC (Access Control Model Pattern Class)	คลาส (Class)	ใช้ระบุคลาสของแบบรูปของแบบจำลองการควบคุมการเข้าถึง
APA (Access Control Model Pattern Attribute)	คุณลักษณะ (Attribute)	ใช้ระบุคุณลักษณะในคลาสของแบบรูปของแบบจำลองการควบคุมการเข้าถึง
APO (Access Control Model Pattern Operation)	การดำเนินการ (Operation)	ใช้ระบุการดำเนินการในคลาสของแบบรูปของแบบจำลองการควบคุมการเข้าถึง

ตารางที่ 2 ค่าป้ายระบุที่เพิ่มเติม

ค่าป้ายระบุ (Tagged Value)	ใช้ในแม่พิมพ์ต้นแบบ	ความหมาย
{ หน้าที่ของคลาสในแบบรูปของแบบจำลองการควบคุมการเข้าถึง @ ชื่อแบบรูปของแบบจำลองการควบคุมการเข้าถึง }	APC	ใช้ระบุหน้าที่ของคลาสในแบบรูปของแบบจำลองการควบคุมการเข้าถึงที่กำหนด
{ หน้าที่ของคุณลักษณะในแบบรูปของแบบจำลองการควบคุมการเข้าถึง @ ชื่อแบบรูปของแบบจำลองการควบคุมการเข้าถึง }	APA	ใช้ระบุหน้าที่ของคุณลักษณะในแบบรูปของแบบจำลองการควบคุมการเข้าถึงที่กำหนด
{ หน้าที่ของการดำเนินการในแบบรูปของแบบจำลองการควบคุมการเข้าถึง @ ชื่อแบบรูปของแบบจำลองการควบคุมการเข้าถึง }	APO	ใช้ระบุหน้าที่ของการดำเนินการในแบบรูปของแบบจำลองการควบคุมการเข้าถึงที่กำหนด

3) ตรวจสอบยูเอ็มแอลเซคที่ปรับปรุงเพิ่มเติม

ขั้นตอนนี้มีวัตถุประสงค์เพื่อตรวจสอบความครบถ้วนในการแสดงโครงสร้างของแบบรูปของแบบจำลองการควบคุมการเข้าถึง โดยการใช้แม่พิมพ์ต้นแบบและค่าป้ายระบุที่เพิ่มขึ้นแสดงโครงสร้างของระบบที่ใช้แบบรูปของแบบจำลองการควบคุมการเข้าถึง

ผลลัพธ์จากการตรวจสอบคือ ยูเอ็มแอลเซคที่ปรับปรุงเพิ่มเติมสามารถแสดงองค์ประกอบของแบบรูปของแบบจำลองการควบคุมการเข้าถึง ซึ่งจะช่วยให้ผู้พัฒนาทราบโครงสร้างของแบบรูปของแบบจำลองการควบคุมการเข้าถึงได้ชัดเจนยิ่งขึ้น พร้อมทั้งรู้ว่ามีการดำเนินการ (Operation) หรือคุณลักษณะ (Attribute) ใดที่ต้องจัดเก็บไว้เพื่อตอบสนองการใช้งานและการออกแบบให้ตรงกับความต้องการ

3. แบบรูปของแบบจำลองการควบคุมการเข้าถึง

แบบรูปของแบบจำลองการควบคุมการเข้าถึง คือ กลุ่มของแบบรูปความมั่นคงที่นำเสนอผลเฉลยสำหรับการแก้ไขปัญหาการควบคุมการเข้าถึงที่ปรากฏบ่อยครั้งและสนับสนุนการนำกลับมาใช้ใหม่ โดยแบบรูปของแบบจำลองการควบคุมการเข้าถึงประกอบด้วยแบบรูปความมั่นคงต่างๆ 4 แบบรูปดังต่อไปนี้

1) แบบรูปการให้อำนาจ (Authorization Pattern) เป็นแบบรูปความมั่นคงที่เสนอการแบ่งสิทธิในการเข้าถึงทรัพยากรของผู้ใช้งานในระบบตามผู้ใช้งานรายบุคคล

2) แบบรูปการควบคุมการเข้าถึงเชิงบทบาท (Role-Based Access Control Pattern) เป็นแบบรูปความมั่นคงที่เสนอการแบ่งสิทธิในการเข้าถึงทรัพยากรของผู้ใช้งานในระบบตามบทบาทของผู้ใช้งานในระบบ

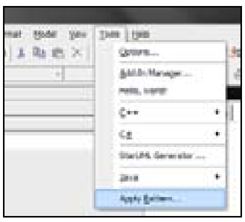
3) แบบรูปความมั่นคงหลายระดับ (Multilevel Security Pattern) เป็นแบบรูปความมั่นคงที่เสนอการแบ่งสิทธิ์ในการเข้าถึงทรัพยากรของผู้ใช้งานในระบบตามบทบาทของผู้ใช้งานในระบบ

4) แบบรูปการตรวจสอบการเข้าใช้ทรัพยากร (Reference Monitor Pattern) เป็นแบบรูปความมั่นคงที่เสนอการตรวจสอบในการเข้าถึงทรัพยากรของผู้ใช้งาน

4. การออกแบบและพัฒนาเครื่องมือ

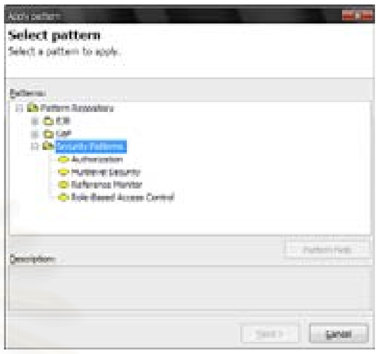
เนื่องจากการใช้งานของยูเอ็มแอลเซคที่เพิ่มเติม ยังไม่สะดวกต่อการใช้งาน เช่น ข้อมูลของแบบรูปของแบบจำลองการควบคุมการเข้าถึงมีลักษณะเป็นข้อความ ซึ่งอาจทำให้ผู้ใช้งานกำหนดข้อมูลของแบบรูปได้ไม่สะดวกและในการออกแบบระบบโดยใช้แบบรูปของแบบจำลองการควบคุมการเข้าถึงนั้น ผู้ใช้งานจะต้องทำการสร้างคลาสเพื่อประกอบเป็นโครงสร้างของแบบรูป ซึ่งจะทำให้เสียเวลาในการสร้างโครงสร้างของแบบรูป เป็นต้น ดังนั้นในงานวิจัยนี้จึง วิเคราะห์ ออกแบบ และสร้างเครื่องมือสำหรับการกำหนดข้อมูลและโครงสร้างแบบรูปของแบบจำลองการควบคุมการเข้าถึง โดยมีรายละเอียดดังนี้

4.1 แนวคิดในการกำหนดโครงสร้างแบบรูปของแบบจำลองการควบคุมการเข้าถึงในเครื่องมือ เนื่องจากปัจจุบันได้มียูเอ็มแอลที่เป็นโอเพนซอร์สมากมาย เช่น สตาร์ยูเอ็มแอล (StarUML) อาร์โกยูเอ็มแอล (ArgoUML) เป็นต้น ดังนั้นผู้วิจัยจึงมีแนวคิดในการปรับปรุงยูเอ็มแอลที่เป็นโอเพนซอร์สเพื่อใช้ในการกำหนดโครงสร้างของแบบรูปของแบบจำลองการควบคุมการเข้าถึง สตาร์ยูเอ็มแอลเป็นยูเอ็มแอลที่ใช้งานบนระบบปฏิบัติการวินโดวส์ (Windows) และรองรับการพัฒนาเพิ่มเติม เช่น การเพิ่มยูเอ็มแอลโพรไฟล์ (UML Profile) [5] การเพิ่มแบบรูป (Pattern) เป็นต้น นอกจากนี้สตาร์ยูเอ็มแอลได้มีฟังก์ชันในการกำหนดโครงสร้างแบบรูป เช่น แบบรูปการออกแบบ (Design Pattern) [6] แบบรูปอีเจบี (EJB : Enterprise Java Bean) เป็นต้น ดังนั้นเพื่อให้สตาร์ยูเอ็มแอลมีฟังก์ชันในการกำหนดโครงสร้างแบบรูปของแบบจำลองการควบคุมการเข้าถึง ผู้วิจัยจึงทำการเพิ่มแบบรูปของแบบจำลองการควบคุมการเข้าถึงในคลังเก็บแบบรูปของสตาร์ยูเอ็มแอล



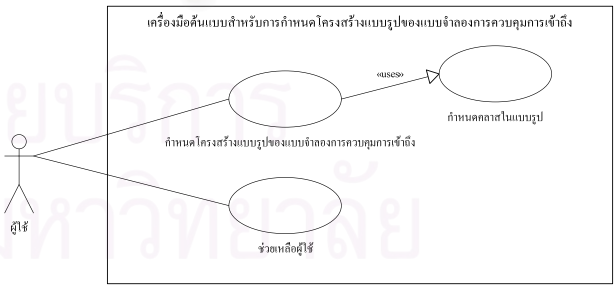
รูปที่ 2 เมนูกำหนดโครงสร้างแบบรูปของสตาร์ยูเอ็มแอล

รูปที่ 2 แสดงเมนูที่มีฟังก์ชันในการกำหนดโครงสร้างแบบรูปของสตาร์ยูเอ็มแอล ซึ่งหลังจากทำการเพิ่มแบบรูปของแบบจำลองการควบคุมการเข้าถึงในคลังเก็บแบบรูปของสตาร์ยูเอ็มแอล จะทำให้เกิดเมนูย่อยแสดงฟังก์ชันในการกำหนดโครงสร้างแบบรูปของแบบจำลองการควบคุมการเข้าถึง แสดงดังรูปที่ 3



รูปที่ 3 เมนูย่อยแสดงฟังก์ชันในการกำหนดโครงสร้างแบบรูปของแบบจำลองการควบคุมการเข้าถึง

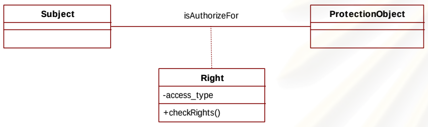
4.2 ความสามารถของเครื่องมือ ฟังก์ชันงานของการกำหนดโครงสร้างแบบรูปของแบบจำลองการควบคุมการเข้าถึงเป็นฟังก์ชันของการกำหนดโครงสร้างแบบรูปของสตาร์ยูเอ็มแอลที่สนับสนุนการกำหนดโครงสร้างของแบบรูปและอำนวยความสะดวกให้กับผู้ใช้ในการกำหนดโครงสร้างของแบบรูป โดยหน้าที่การทำงานของฟังก์ชันงานนี้สามารถนำเสนอด้วยแผนภาพยูสเคส (Use Case Diagram) ซึ่งเป็นแผนภาพที่อธิบายการติดต่อกันระหว่างผู้ใช้ระบบ (Actors) กับฟังก์ชันงานต่างๆ ที่ปรากฏในระบบ ดังรูปที่ 4 โดยมีรายละเอียดแต่ละยูสเคสดังนี้



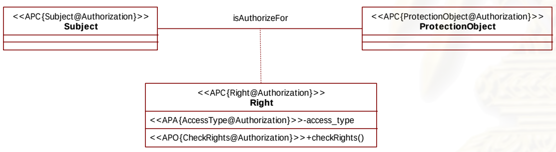
รูปที่ 4 แผนภาพยูสเคสของสตาร์ยูเอ็มแอลในส่วนของการกำหนดโครงสร้างแบบรูปของแบบจำลองการควบคุมการเข้าถึง

1) ส่วนกำหนดโครงสร้างแบบรูปของแบบจำลองการควบคุมการเข้าถึง เป็นส่วนหลักของการกำหนดแบบรูปของแบบจำลองการควบคุมการเข้าถึง โดยผู้ใช้สามารถเลือกแบบรูปของแบบจำลองการควบคุมการ

เข้าถึง เมื่อผู้ใช้ทำการเลือกแบบรูปแล้ว ผู้ใช้จะต้องกำหนดชื่อของแต่ละคลาสในแบบรูปหรือระบุให้คลาสที่มีอยู่แล้วในแผนภาพเป็นคลาสในแบบรูป จากนั้นสตาร์ยูเอ็มแอลจะทำการสร้างแบบรูปของแบบจำลองการควบคุมการเข้าถึง ในที่นี้จะยกตัวอย่างคือแบบรูปการให้อำนาจซึ่งแผนภาพคลาสของแบบรูปการให้อำนาจที่เป็นต้นแบบและที่สร้างมาจากเครื่องมือแสดงดังรูปที่ 5 และ 6 ตามลำดับ ซึ่งในแต่ละคลาสของแผนภาพคลาสที่สร้างมาจากเครื่องมือจะกำหนดข้อมูลแบบรูปของแบบจำลองการควบคุมการเข้าถึงด้วยแม่พิมพ์ต้นแบบและค่าป้ายระบุจากยูเอ็มแอลเซคที่ปรับปรุงเพิ่มเติม [4] เพื่อทำการแสดงโครงสร้างแบบรูปของแบบจำลองการควบคุมการเข้าถึงในแผนภาพ เช่น <<APC{Right@Authorization}>> Right แสดงถึงคลาส Right ทำหน้าที่เป็นคลาส Right ในแบบรูปการให้อำนาจ เป็นต้น



รูปที่ 5 แผนภาพคลาสของแบบรูปการให้อำนาจที่เป็นต้นแบบ

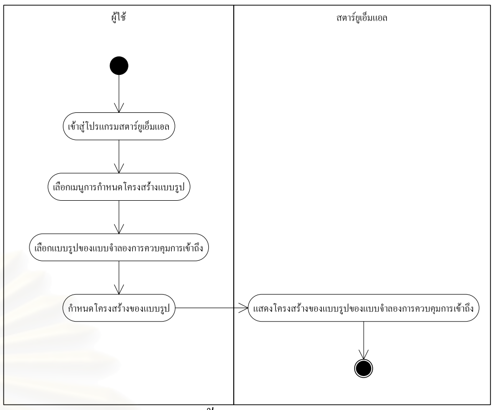


รูปที่ 6 แผนภาพคลาสของแบบรูปการให้อำนาจที่สร้างมาจากเครื่องมือ

2) ส่วนช่วยเหลือผู้ใช้ เป็นส่วนแสดงคำอธิบายของแต่ละแบบรูปประกอบไปด้วย จุดประสงค์ในการใช้งานแบบรูป โครงสร้างแบบรูป ตัวอย่างในการใช้งานแบบรูปและประโยชน์ที่จะได้รับเมื่อใช้งานแบบรูปซึ่งจะเป็นประโยชน์ต่อผู้ใช้งานแบบรูปที่เกิดข้อสงสัยเกี่ยวกับแบบรูป ซึ่งตัวอย่างของคำอธิบายแบบรูปการให้อำนาจแสดงดังรูปที่ 7

รูปที่ 7 คำอธิบายของแบบรูปการให้อำนาจ

4.3 การใช้งานเครื่องมือ ขั้นตอนการทำงานปกติของการใช้งานฟังก์ชันการกำหนดโครงสร้างแบบรูปของแบบจำลองการควบคุมการเข้าถึงระหว่างสตาร์ยูเอ็มแอลกับผู้ใช้ดังรูปที่ 8



รูปที่ 8 แผนภาพกิจกรรมแสดงขั้นตอนการใช้สตาร์ยูเอ็มแอลในส่วนของการกำหนดข้อมูลและโครงสร้างแบบรูปของแบบจำลองการควบคุมการเข้าถึง

ซึ่งรายละเอียดของแต่ละขั้นตอนเป็นดังต่อไปนี้

1.) ผู้ใช้เปิดโปรแกรมสตาร์ยูเอ็มแอล ผู้ใช้งานสามารถเปิดโปรแกรมสตาร์ยูเอ็มแอลโดยไปที่ Start -> Program -> StarUML ดังรูปที่ 9

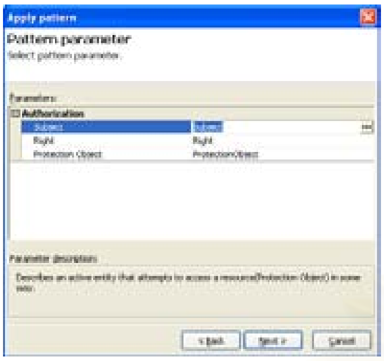
รูปที่ 9 หน้าจอแสดงการเปิดโปรแกรมสตาร์ยูเอ็มแอล

2) ผู้ใช้เลือกเมนูการกำหนดโครงสร้างแบบรูป เมื่อผู้ใช้เข้าสู่โปรแกรมสตาร์ยูเอ็มแอลแล้ว ให้เลือกเมนูการกำหนดโครงสร้างแบบรูปดังรูปที่ 2

3) ผู้ใช้เลือกแบบรูปของแบบจำลองการควบคุมการเข้าถึง ขั้นตอนต่อไปจะเป็นการเลือกแบบรูปของแบบจำลองการควบคุมการเข้าถึงจากเมนูย่อยดังรูปที่ 3 ซึ่งผู้ใช้สามารถเลือกแบบรูปของแบบจำลองการควบคุมการเข้าถึงได้ 4 แบบรูปคือ แบบรูปการให้อำนาจ (Authorization) แบบรูปความมั่นคงหลายระดับ (Multilevel Security) แบบรูปการตรวจสอบการเข้าใช้ทรัพยากร (Reference Monitor) และแบบรูปการควบคุมการเข้าถึงเชิงบทบาท (Role-Based Access Control) ตามลำดับ

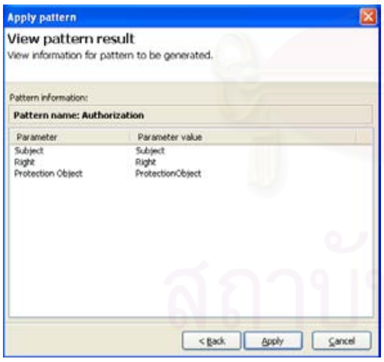
4) ผู้ใช้กำหนดโครงสร้างของแบบรูปของแบบจำลองการควบคุมการเข้าถึง เมื่อผู้ใช้ได้ทำการเลือกแบบรูปของแบบจำลองการควบคุมการเข้าถึงแล้ว ขั้นตอนต่อไปเป็นการกำหนดโครงสร้างของแบบรูปดังรูปที่ 10 ซึ่งผู้ใช้สามารถกำหนดได้ว่าจะทำการสร้างคลาสที่เป็นของแบบรูป

ขึ้นมาใหม่หรือกำหนดคลาสที่มีอยู่แล้วให้เป็นคลาสของแบบรูป ซึ่งในตัวอย่างนี้คือแบบรูปการให้อำนาจ จะมีการกำหนดคลาส 3 คลาสคือ คลาส Subject คลาส Right และคลาส Protection Object

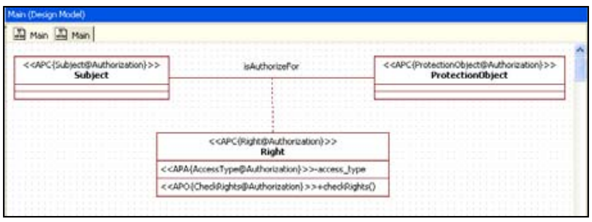


รูปที่ 10 หน้าจอแสดงการกำหนดโครงสร้างของแบบรูปของแบบจำลองการควบคุมการเข้าถึง

5) **สตาร์ยูเอ็มแอลทำการแสดงข้อมูลและโครงสร้างแบบรูปของแบบจำลองการควบคุมการเข้าถึง** เมื่อผู้ใช้ทำการกำหนดโครงสร้างของแบบรูปของแบบจำลองการควบคุมการเข้าถึงแล้ว ขั้นตอนต่อไปเป็นการยืนยันการเพิ่มแบบรูปของแบบจำลองการควบคุมการเข้าถึงดังรูปที่ 11 ซึ่งหลังจากการยืนยันแล้วจะได้ผลลัพธ์เป็นข้อมูลและโครงสร้างแบบรูปของแบบจำลองการควบคุมการเข้าถึง ซึ่งตัวอย่างของผลลัพธ์แสดงดังรูปที่ 12 ซึ่งแสดงข้อมูลและโครงสร้างแบบรูปการให้อำนาจ



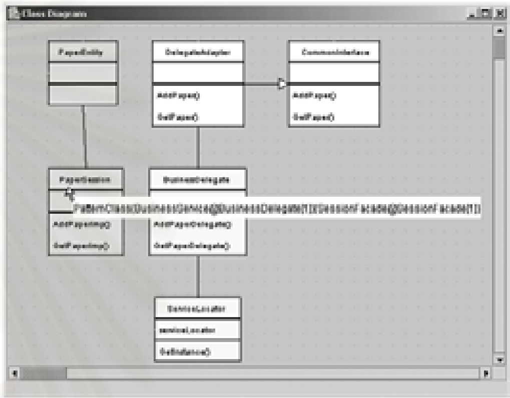
รูปที่ 11 หน้าจอยืนยันการเพิ่มแบบรูปของแบบจำลองการควบคุมการเข้าถึง



รูปที่ 12 แผนภาพคลาสแสดงข้อมูลและโครงสร้างแบบรูปการให้อำนาจ

5. การทดสอบเครื่องมือ

การทดสอบนี้มีวัตถุประสงค์เพื่อตรวจสอบความสมบูรณ์และความถูกต้องของเครื่องมือสำหรับการกำหนดข้อมูลและโครงสร้างของแบบรูปของแบบจำลองการควบคุมการเข้าถึง โดยนำเครื่องมือเปรียบเทียบกับเครื่องมือ VisDP [7] ซึ่งเป็นเครื่องมือเสริมที่ช่วยแสดงข้อมูลและโครงสร้างของแบบรูปการออกแบบของเครื่องมือเขียนแผนภาพยูเอ็มแอล เช่น แรชันนัลโรส (Rational Rose) และ อาร์โกยูเอ็มแอล เป็นต้น (ตัวอย่างของเครื่องมือแสดงดังรูปที่ 13) โดยผลของการเปรียบเทียบแสดงให้เห็นดังตารางที่ 3



รูปที่ 13 ตัวอย่างการแสดงข้อมูลและโครงสร้างของแบบรูปการออกแบบของเครื่องมือ VisDP

ตารางที่ 3 การเปรียบเทียบเครื่องมือ

ฟังก์ชันการทำงาน	เครื่องมือ VisDP	เครื่องมือสำหรับการกำหนดข้อมูลและโครงสร้างของแบบรูปของแบบจำลองการควบคุมการเข้าถึง
1. การกำหนดข้อมูลและโครงสร้างของแบบรูป	ผู้ใช้งานเป็นผู้กำหนดข้อมูล	เครื่องมือช่วยกำหนดข้อมูลและโครงสร้างบางส่วน
2. การตรวจสอบข้อมูลก่อนกำหนดเป็นข้อมูลของแบบรูป	ผู้ใช้งานเป็นผู้ตรวจสอบ	เครื่องมือช่วยตรวจสอบข้อมูลและโครงสร้าง
3. การแสดงข้อมูลของแบบรูป	แสดงข้อมูลเป็นแบบพลวัต	แสดงข้อมูลเป็นแบบตัวอักษรคงที่

ในแง่ของความสมบูรณ์ของข้อมูลและโครงสร้างของแบบรูปนั้น การกำหนดข้อมูลและโครงสร้างของแบบรูปในเครื่องมือ VisDP เป็นการกำหนดของผู้ใช้งานที่จะต้องทำการเพิ่มแม่พิมพ์ต้นแบบและค่าป้ายระบุที่บอกถึงข้อมูลและโครงสร้างของแบบรูปการออกแบบในแผนภาพซึ่งอาจเกิดความผิดพลาดจากผู้ใช้งานได้และเมื่อเกิดความผิดพลาดจากผู้ใช้งาน เครื่องมือดังกล่าวก็ไม่มีฟังก์ชันในการตรวจสอบข้อมูล ในขณะที่การกำหนดข้อมูลและโครงสร้างของเครื่องมือที่นำเสนอนั้นเป็นการ

กำหนดของผู้ใช้งานและเครื่องมือที่นำเสนอซึ่งเครื่องมือจะช่วยกำหนดข้อมูลและโครงสร้างบางส่วนเพื่อลดความผิดพลาดจากผู้ใช้งานเช่น การสร้างคลาสของแบบรูป การสร้างความสัมพันธ์ระหว่างคลาสของแบบรูปเป็นต้น นอกจากนี้เครื่องมือยังช่วยตรวจสอบความถูกต้องของข้อมูลและโครงสร้างของแบบรูปที่มาจากการกำหนดของผู้ใช้งาน แต่เครื่องมือที่นำเสนอยังมีจุดอ่อนคือ การแสดงข้อมูลเป็นแบบตัวอักษรคงที่ ซึ่งอาจทำให้ผู้ใช้งานเกิดความสับสนในการแยกแยะข้อมูลมากกว่าการแสดงข้อมูลเป็นแบบพลวัตที่เป็นการแสดงข้อมูลของเครื่องมือ VisDP ดังนั้นแนวทางในการพัฒนาต่อของผู้วิจัยคือ ทำการปรับปรุงเครื่องมือให้แสดงข้อมูลเป็นแบบพลวัตหรือแสดงข้อมูลเป็นแบบอื่นที่ช่วยให้ผู้ใช้งานแยกแยะข้อมูลของแบบรูปได้ง่ายมากขึ้น

6. สรุปผลการวิจัย

งานวิจัยนี้ได้ทำการวิเคราะห์ ออกแบบ และสร้างเครื่องมือสำหรับการกำหนดข้อมูลและโครงสร้างแบบรูปของแบบจำลองการควบคุมการเข้าถึง ซึ่งประกอบไปด้วย แบบรูปการให้อำนาจ แบบรูปการควบคุมการเข้าถึงเชิงบทบาท แบบรูปความมั่นคงหลายระดับ และแบบรูปการตรวจสอบการเข้าใช้ทรัพยากร เครื่องมือได้เสนอส่วนกำหนดโครงสร้างของแบบรูปของแบบจำลองการควบคุมการเข้าถึงซึ่งจะช่วยให้ผู้ออกแบบทำการออกแบบความมั่นคงให้กับระบบโดยใช้แบบรูปของแบบจำลองการควบคุมการเข้าถึงได้สมบูรณ์มากยิ่งขึ้น รวมทั้งได้เสนอส่วนช่วยเหลือผู้ใช้งานเพื่อช่วยให้ผู้ใช้งานนำแบบรูปของแบบจำลองการควบคุมการเข้าถึงมาใช้งานได้ถูกต้องมากยิ่งขึ้น

7. แนวทางการดำเนินงานวิจัยในอนาคต

งานวิจัยนี้ได้สร้างเครื่องมือสำหรับการกำหนดข้อมูลและโครงสร้างแบบรูปของแบบจำลองการควบคุมการเข้าถึง ซึ่งแบบรูปของแบบจำลองการควบคุมการเข้าถึงเป็นเพียง 1 กลุ่มแบบรูปใน 8 กลุ่มแบบรูปความมั่นคงที่นำเสนอไว้โดย Schumacher และคณะ [1] เท่านั้น ดังนั้นการขยายขอบเขตงานให้ครอบคลุมทั้ง 8 กลุ่มแบบรูปความมั่นคงจะช่วยให้การกำหนดข้อมูลและโครงสร้างแบบรูปความมั่นคงมีความถูกต้องมากยิ่งขึ้น ซึ่งมีประโยชน์อย่างมากต่อการใช้แบบรูปความมั่นคงในการพัฒนาระบบที่ต้องการความปลอดภัยในอนาคต

8. บรรณานุกรม

[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] K. Supaporn, N. Prompoon and T. Rojkangsadan, "Enterprise Assets Security Requirements Construction from ESRMG Grammar based on Security Patterns", *14th Asia-Pacific Software Engineering Conference*, pages 112-119, 2007.

[3] J. Jürjens, "UMLsec: Extending UML for Secure Systems Development", Department of Informatics, Munich University of Technology, Germany, 2002.

[4] K. Chaisomboon and N. Prompoon, "Design and Visualization of Access Control Model Patterns by Extending UMLsec", *International Joint Conference on Computer Science and Software Engineering*, Thailand, 2008.

[5] K. Hamilton and R. Miles, *Learning UML 2.0*, O'Reilly, 2006.

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

[7] J. Dong, S. Yang and K. Zhang, "Visualizing Design Patterns in Their Applications and Composition", In *EEE Transactions on Software Engineering, Vol. 33, No. 7*, pages 433-453, 2007.

ผศ. นครทิพย์ พร้อมพูล สำเร็จการศึกษาในระดับปริญญาโท สาขาวิชาวิทยาศาสตร์คอมพิวเตอร์ จาก George Washington University ปัจจุบันเป็นอาจารย์ประจำภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย มีความสนใจทางด้าน Software Engineering, Software Requirements Engineering, Software Process.

นายเกียรติศักดิ์ ไชยสมบูรณ์ สำเร็จการศึกษาในระดับปริญญาตรี สาขาวิชาฟิสิกส์ จากคณะวิทยาศาสตร์ มหาวิทยาลัยมหิดล ปัจจุบันกำลังศึกษาต่อในระดับปริญญาโท ณ ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย มีความสนใจทางด้าน Software Engineering, Security Patterns

UMLsec-SP: An Extension of UMLsec for System Security Modeling based on Security Patterns

Kiattisak Chaisomboon and Nakornthip Prompoon
Software Engineering Lab, Center of Excellent in Software Engineering
Department of Computer Engineering, Faculty of Engineering
Chulalongkorn University, Bangkok, Thailand
kiattisak.c@student.chula.ac.th and nakornthip.s@chula.ac.th

Abstract

***Abstract*—UMLsec, the extension of UML, supports the design of general security system components. However, there are limitations in UMLsec, especially when security patterns applied for the design of system security. It cannot express the information such as pattern-related information for overall patterns and security-related information for individual pattern which are required from security patterns and system security assessment and improvement. In this paper, we present a security design notation, which is an extension of UMLsec, called UMLsec-SP. It primarily combines UMLsec and the instantiation of UML profile from stereotypes, tagged values, and constraints to resolve such limitations. UMLsec-SP significantly supports the detail design of security pattern components and their integration architectures. Results of the case study on applying UML, UMLsec and UMLsec-SP for system security design are compared using graph complexity measurement. UMLsec-SP is beneficial for any security system designer to visualize security patterns architecture in a design of target security application.**

Keywords-Security pattern; UMLsec; UML profile;

I. INTRODUCTION

At present, the system security is an important issue in system development because the threats of attackers are arising in different ways. In addition, system security has plenty of aspects to handle and usually needs various kinds of technology and knowledge. Thus, core fundamental requirements of system security are necessary for one who is responsible for the design of security system.

Security patterns [1] are created in order to describe a particular recurring security problem that arises in specific contexts, and present a proven generic solution for it. Thus, applying security patterns for the design of security system in an appropriate way is a challenging task of the system security designer.

Each generic solution of a security pattern has the pattern components such as class, attribute, operation and relationship among classes within the pattern. The similar instantiation of pattern components must perform in a specific context of the same system security design environment. Class represents the element of patterns whereas attribute represents a specific characteristic of a single element. Operation represents the service which an element may provide. The relationship among classes represents the interaction among them to serve the target security task. The information structure of pattern must be kept and monitored since it is important in terms of the fulfillment of system security. For example, if one accidentally deletes any element of the pattern components, the system may be in a harmful situation.

UMLsec [3, 4], the extension of UML, supports the design of security system but there are some important limitations of UMLsec in expressing the security pattern components, its structure and information of the structure. This comes from the fact that UMLsec does not define stereotypes, tagged values and constraint for the identification of security pattern-related information.

In this paper, we present an extending UMLsec which combines UMLsec and our new UML profiles such as stereotypes, tagged values, and constraints for expressing security pattern-related information. The proposed extending UMLsec are beneficial for any designer to reserving and tracing the security pattern-related information in their application designs.

II. BACKGROUND

Schumacher et al. [1] proposed forty-six security patterns cover three levels: the enterprise level, the system level and the operational level, for any organization to build the security architecture. In each pattern, there are recommended pattern components used for a specific system security design. Supaporn et al. [2] applied their pattern components to construct

ESRMG grammar and tool based on the proposed grammar for defining enterprise asset security requirements.

Jürjen et al. [3, 4] proposed UMLsec, the extension of UML that allows expressing security-relevant information within diagrams in a system specification. UMLsec is defined in a form of a UML profile using the standard UML extension mechanisms. However, there are limitations in UMLsec as mention above. Dong et al. [6] proposed their extension of UML for tracing pattern components of design patterns in UML diagram using stereotype and tagged value. These new stereotypes, tagged values and constraints are attached to a model element to explicitly represent the role of model element plays in a design pattern so that the user can identify the pattern in a UML diagram.

In this paper, we use the standard UML extension mechanisms include stereotypes, tagged values and constraints to extend UMLsec for expressing pattern-related information and security-related information for individual pattern when apply security patterns for the design of the system security.

III. SECURITY PATTERNS

Security pattern describes particular recurring security problem that arise in specific context and present a well-proven generic solution for it. Security pattern helps designers to handle a problem with a related solution of security pattern which is in the same context. Security patterns can be categorized as the following: [5]

1) *Security analysis pattern* depicts a solution in a form of a part of the analysis document.

2) *Security design pattern* is a specialization of design pattern [7] for the security domain.

3) *Security process pattern* describes process parts during system development.

In this paper, we apply security patterns from [1] as an input of design because they have their characteristics which are similar to design patterns [7]. We selected security patterns which are security design patterns because we aim to visualize the security pattern-related information of their components and relationships in UML class diagram. We selected five groups composed of twenty-seven security patterns as the following:

1) Access control model defines security constraints at the application level, and enforce by the low levels, such as “Authorization”, “Role-Based Access Control”, “Multilevel Security” and “Reference Monitor”.

2) System access control architecture deals with the architecture of software systems to be secured by access control are provided, based on a generic set of access control requirements, such as “Single Access Point”, “Check Point”, “Security Session”, “Full Access with Errors” and “Limited Access”.

3) Operating system access control describes architectural patterns for access controls in operating system, such as “Authenticator”, “Controlled Process Creator”, “Controlled Object Factory”, “Controlled Object Monitor”, “Controlled Virtual Address Space”, “Execution Domain”, “Controlled Execution Environment” and “File Authorization”.

4) Firewall architecture describes different types of firewall, such as “Packet Filter Firewall”, “Proxy-Based Firewall” and “Stateful Firewall”

5) Secure internet applications describe patterns mined from internet applications, such as “Obscurity Information”, “Secure Channel”, “Known Partners”, “Demilitarized Zone”, “Protection Reverse Proxy”, “Integration Reverse Proxy” and “Front door"

IV. STANDARD UML EXTENSION MECHANISMS

UML provides extension mechanisms [8] to allow designers to model software systems if the current UML features are not semantically sufficient to express the systems. These extension mechanisms include stereotypes, tagged values, and constraints.

1) Stereotypes allow the definition of extensions to the UML vocabulary, denoted by <<*stereotype*>>. A stereotype groups tagged values and constraints under a meaningful name. When a stereotype is branded to model element, the semantic of the tagged values and the constraints associated with the stereotype are attached to that model element.

2) Tagged values extend model elements with new kinds of properties. They may be attached to a stereotype, and such an association will propagate to the model element to which the stereotype is branded. The format of a tagged value is a pair of name and an associated value, i.e., {name = value}. The tagged values attached to a stereotype must be compatible with the constraints of the stereotype’s base class.

3) Constraints add new semantic restrictions to a model element. Typically, constraints are written in the Object Constraint Language (OCL) [9]. Constraints attached to a stereotype imply that all model elements branded by that stereotype must obey the semantic restrictions of the constraints. The constraints attached to a stereotyped model element must be compatible with the constraints of the stereotype and the base class of the model element.

In this paper, we extend UMLsec by applying these mechanisms to respond the required information which is arisen by applying security pattern in secure system design.

V. LIMITATION OF UMLSEC FOR SPECIFYING SECURITY PATTERN

UMLsec is the extension of UML that allow expressing security-related information in the system design. However, applying the security patterns by using UMLsec is still lack of expressing the security-related information especially security patterns, UMLsec expresses only the security-related information for general secure domains but does not specific secure domains such as security pattern. There are two limitation issues UMLsec cannot fully express the information of security patterns as the following:

1) *Limitation of expressing pattern-related information.* The pattern-related information is the information of security pattern which explicitly specify security pattern in system designs such as the security pattern used and the role of components in security pattern, etc. There are several problems due to the lack of specification in secure system designs. First, each security pattern preserves some properties and constraints which are important for security mechanism. It is difficult for the designers to check whether these properties and constraints hold when the secure design is changed. Second, designers can only communicate at the class level instead of the pattern level because they have no mean to show the pattern-related information when they want to specify this information in the system security design. Third, each security pattern often documents some ways for future evolutions. The designers are not able to change the security design using relevant pattern-related information.

2) *Limitation of expressing security-related information for individual security pattern.* Security-related information for individual security pattern is the information that encapsulates knowledge on security pattern; for example, *Subject* is the active entity that attempts to access a resource in system and *Protection Object* is the resource to be protected in system, etc. There are several problems when there are missing the necessary specification in the system security design model. First, designers are unavoidable taking security aspect into account because they cannot look up any security-related information in system security design. Second, some security mechanisms of security patterns cannot completely implement because some constraints from security-related information are neglect.

From above limitation issues, we extend UMLsec by considering both pattern-related information expression and security-related information expression for individual security pattern.

VI. THE PROCEDURE FOR UMLSEC EXTENSION

In this section, the procedure for extending UMLsec is presented using the standard UML extension mechanisms, as shown in figure 1.

In this paper, we use an authorization pattern which is a simple security pattern that usually used in general security application as a case study to explain the UMLsec extending procedure. The steps of UMLsec extension by applying authorization pattern is as the following:

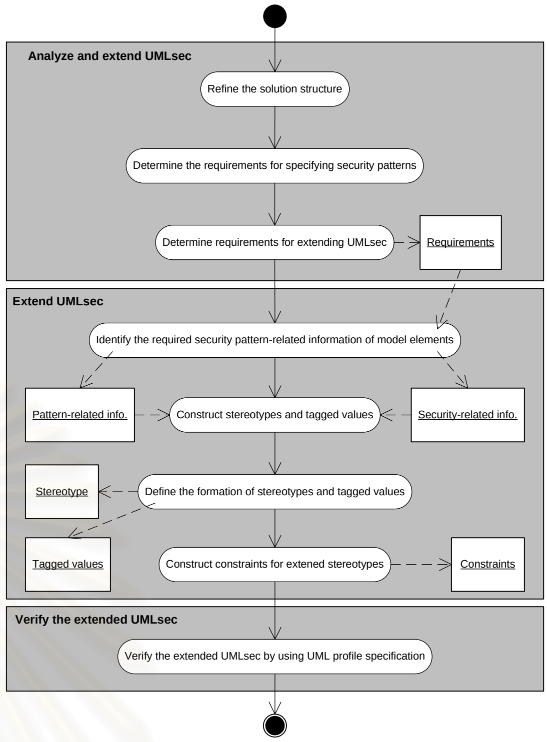


Figure 1. The UMLsec extension procedure

A. *Analyze and determine the security patterns requirements*

In this step, we refine the solution structure of each security pattern for the analysis of security pattern visualization by applying UMLsec. Next, we construct extended UMLsec requirements based on the consideration of each limitation issue. Then, we extend UMLsec from earned requirements using standard UML extension mechanisms.

a. Refine the solution structure of each security pattern.

Refining of the solution structure of each security patterns is required because the solution structure of security patterns only offers an initial structure not a complete structure. The refined solution structure of authorization pattern shows in figure 2.

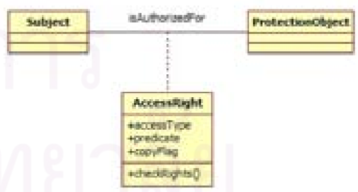


Figure 2. The refined solution structure of authorization pattern

The authorization pattern describes who accesses the specific resources need to be controlled in system, in a specific environment. The model elements of this pattern such as the

Subject class describes an active entity that attempts to access a resource (Protection Object) in some way, the *ProtectionObject* class represents the resource to be protected and the *Right* class checks the rights and describes the access type that Subject class is allowed to perform on the corresponding object.

b. Determine the requirements for specifying security pattern-related information.

We determine the requirements for specifying security pattern-related information which are required by applying security patterns in a class diagram such as pattern-related information and security-related information. The requirements for specifying authorization pattern in a class diagram can be written as the following:

1) Requirements for specifying pattern-related information.

Req.1.1 > Expressing the pattern component specification of each model elements (such as classes, attributes, operations and relationships). This information describes that specification locates pattern components in a class diagram.

Req.1.2 > Expressing the pattern name, this information identifies the pattern used in a class diagram.

Req.1.3 > Expressing the pattern role of each model elements. This information specifies the role that the model element plays in security pattern.

Req.1.4 > Expressing the pattern instance. This information distinguishes difference instances of the same security pattern which can be omitted if there is only one instance of the security pattern in the secure system design.

2) Requirements for specifying security-related information for individual security pattern.

Req.2.1 > Expressing the *Subject* class. This class attempts to access a resource in a system.

Req.2.2 > Expressing the *ProtectionObject* class. This class is a resource in a system.

Req.2.3 > Expressing the *AccessRight* class. This class protects resources in a system.

Req.2.4 > Expressing the *accessType* attribute. This attribute describes the access type of the subject is allowed to perform on the protection object.

Req.2.5 > Expressing the *predicate* attribute. This attribute indicates specific conditions which restrict the use of authorization.

Req.2.6 > Expressing the *copyFlag* attribute. This attribute indicates a boolean that allows some of the authorizations by their holders to other subjects.

Req.2.7 > Expressing the controlled type of “AccessRight” class. This information describes internal access control mechanism of “AccessRight” class.

c. Determine requirements from the deficiency of UMLsec for securitiy patterns modeling.

From the requirements of an authorization case study defined from *A.b* part in the previous section, we apply UMLsec to model the pattern requirements as shown in figure 3. It can only be modeled one stereotype which is <<*guarded*>> while the other requirements cannot be presented. The *ProtectionObject* class is branded by the <<*guarded*>> stereotype. It is protected by the *Right* class which indicates in tag *guard*. The <<*guarded*>> stereotype expresses a resource in system which is required by Req.2.2 requirement. Thus, in order to model all the requirements, it is necessary to extend the syntax of UMLsec.

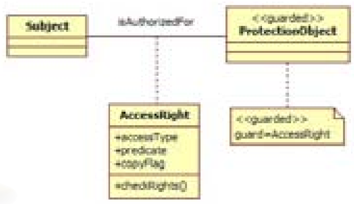


Figure 3. UMLsec class diagram for authorization pattern

B. Extend UMLsec.

We extend UMLsec by applying standard UML extension mechanism such as stereotype, tagged value and constraint in response to the requirements from previous step. The details of extending UMLsec compose of two steps: stereotype and tagged value extension and constraints extension.

i Extend stereotype and tagged value.

We construct new stereotypes and tagged values which extend from UMLsec. The details of extending stereotypes and tagged values as the following:

(1) Identify the required pattern-related information and security-related information of model elements by considering the requirements.

The pattern-related information and security-related information of model elements are required by considering the requirements for extending from previous step as the following:

1) The required pattern-related information such as pattern component specification of every model elements such as classes (including data types, operations and relationships), pattern name, pattern role and pattern instance are required from the Req.1.1., Req.1.2., Req.1.3. and Req.1.4 respectively.

2) The required security-related information of model elements such as *Subject* class, *AccessRight* class, *accessType* attribute, *predicate* attribute, *copyFlag* attribute and controlled type of *AccessRight* class are required from Req.2.1, Req.2.3, Req.2.4, Req.2.5, Req.2.6 and Req.2.7, respectively.

(2) Construct stereotypes and tagged values.

We construct the new stereotypes for defining the new UML vocabularies and the new tagged value for defining the new kinds of properties which is owned by specific UML vocabulary.

A list of stereotypes and tagged values from the considering of the required pattern-related information from the previous step is presented as follows:

1) spc (Security Pattern Class) stereotype indicates the branded class which is a part of security patterns.

2) spt (Security Pattern data Type) stereotype indicates the branded data type which is a part of security patterns.

3) spr (Security Pattern Relationship) stereotype indicates the branded relationship which is a part of security patterns.

4) PatternName tagged value indicates the pattern names of the component which is branded by specific stereotypes such as *spc*, *sp*t and *spr*.

5) PatternInstance tagged value indicates the pattern instance of the component which is branded by specific stereotypes such as *spc*, *spt* and *spr*.

6) PatternRole tagged value indicates the pattern roles of the component which is branded by specific stereotypes such as *spc*, *sp*t and *spr*.

A list of stereotypes and tagged values from the considering of the required security-related information from the previous step is as follows:

1) subject stereotype indicates the branded class that attempts to access a resource in system.

2) accessRight stereotype indicates the branded class that protects a resource in system.

3) accessType stereotype indicates the access type of the subject which is allowed to perform on the protection object.

4) restrictedRule stereotype indicates specific conditions which restrict the use of the authorization.

5) copyFlag stereotype indicates a boolean that allows some of the authorizations by their holders to other subjects.

6) controlledType tagged value indicates the internal mechanism of access controller.

In case of the pattern operation specification, we use the expression "*@PatternName[PatternInstance]*" to specify the operation which is a part of security pattern by inserting such expression to its name. For operations in authorization pattern, the *checkRights* operation is replaced by *checkRights@authorization* operation.

(3) Define the formation of stereotypes and tagged values.

We define the formation of extended UML profile to improve semantic interpretation and to express our extension when applying it in real world application.

We define all extended tagged values of pattern-related stereotype in special format and locate them in bracket "<<" and ">>" to ease the semantic interpretation of pattern-related information. The formation of the tagged values for all pattern-related stereotype (such as spc, spt and spr) is "*PatternRole@PatternName*[*PatternInstance*]" where *PatternRole* specifies the role which the stereotype plays in the pattern , *PatternName* specifies the security pattern name of the specific stereotype and *PatternInstance* specifies to which instance of the pattern the stereotype belongs. For example, *<<accessRight.accessRight@authorization>>* means the branded class is a security pattern class which plays the role of access right in authorization pattern.

ii Extend constraints

We construct constraints which are written in Object Constraint Language (OCL) to specify semantic restrictions of extended stereotypes. For example, the controlled type of "AccessRight" class which branded by *AccessRight* stereotype can only be the access control lists or the capabilities. Then the semantic constraints of *AccessRight* stereotype is as the following:

self.taggedValue -> forall(tv|tv.name = "controlledType") implies (tv.dataValue = "ACLs" or tv.dataValue = "Capabilities"))

Overall constraints of extended stereotypes of this case study is shown in table 1.

The application of the extended UMLsec class diagram for the authorization pattern shows in figure 4. This diagram applies our proposed UML profiles which extend from UMLsec for modeling authorization pattern security.

TABLE I. THE CONSTRAINTS FOR EXTENDED UMLSEC

Stereotype	Constraint	Description
spc (Security Pattern Class), spt (Security Pattern data Type) and spr (Security Patern Relationship)	1. self.taggedValue.dataValue.name -> notEmpty	Indicates that the name field of tagged values cannot be empty.
	2. self.taggedValue.name.role -> notEmpty	Indicates that the role field of tagged values cannot be empty.
	3. self.taggedValue.name.instance -> isEmpty or self.taggedValue -> exists(tv:taggedValue | tv.name.instance -> notEmpty)	Indicates that the instance field of tagged values can be empty if there is only one instance of a particular security pattern in a system design.
	4. self.taggedValue.name -> exist(v1, v2:name | v1.name = v2.name) implies (v1.instance -> notEmpty and v2.instance -> notEmpty and v1.instance <> v2.instance)	Indicates that the instance field of tagged values cannot be empty if there is multiple instances of a certain security pattern in a system design.
AccessRight	1. self.taggedValue -> forall(tv|tv.name = "controlledType") implies (tv.dataValue = "ACLs" or tv.dataValue = "Capabilities"))	Indicates that the controlled type of access right can only be the access control lists or the capabilities.

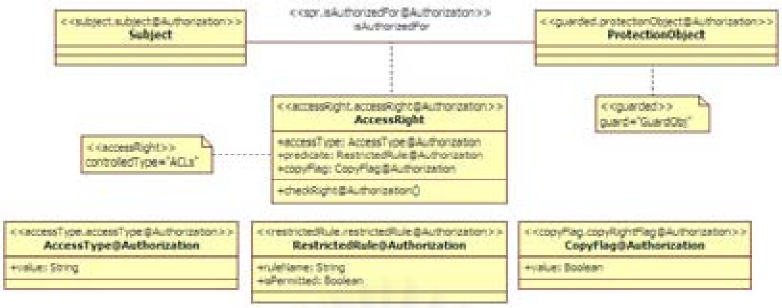


Figure 4. UMLsec-SP class diagram for authorization pattern

After we apply this procedure to extend UMLsec, we summarized our extending UMLsec for security pattern visualization, called UMLsec-SP (UMLsec Security Pattern). List of stereotypes and tagged values are shown in Appendix A.

C. Verifying the UMLsec-SP (extended UMLsec) by using UML profile specification

In this step, we use UML profile specification [10] to verify the satisfaction of UML extension criteria for our proposed model, UMLsec-SP.

1) Identifies a subset of the UML metamodel. — Our extension must follow the extension mechanisms of UML metamodel.

2) Specifies "well-formedness rules" beyond those specified by the identified subset of the UML metamodel. (Well-formedness rules describe a set of constraints written in OCL that contributes to the definition of a metamodel element.) — We define the semantic restrictions of extended stereotypes in OCL as shown in table I.

3) Specifies "standard elements" beyond those specified by the identified subset of the UML metamodel. (Standard element is a term used in the UML metamodel specification to describe a standard instance of a UML stereotype, tagged value or constraint.) — Our extension is constructed by using stereotypes, tagged values and constraints.

4) Specifies semantics, expressed in natural language, beyond those specified by the identified subset of the UML metamodel. — We express the semantic of our extension in natural language as shown in Appendix A.

5) Specifies common model elements, expressed in term of the profile. — We define the base class of extended stereotypes which are the common model elements of them.

In summary, our extension can pass all of the standard UML profile properties.

VII. DIAGRAM COMPLEXITY COMPARISON

We applied our extension on the partial design of a paper review system as shown in figure 5 using an original UML. Figure 6 depicts the diagram by attaching only security-related information of security pattern which is under the scope of UMLsec. The figure 7 depicts the resulting diagram using UMLsec-SP by statically attaching pattern-related information and security-related information from security patterns in the original UML diagram. UMLsec-SP can fully express pattern related information from security patterns, for example *SystemUser* class plays the role of *Client* in the Check Point pattern and the role of Subject in the Role-Based Access Control pattern (RBAC), and security-related information for individual pattern, for example *SystemUser* class represents an external client who needs to access resource in system (from *Client* and *Subject* stereotype).

This section reports a comparative study on graph complexity between the UMLsec-SP diagram and other diagrams such as UML and UMLsec. Five metrics [11] are used to compute the complexity of the diagrams using UML, UMLsec, and UMLsec-SP for a paper review system. They are

1) *Number of nodes* such as classes and notes.
2) *Number of edges* such as relationships among class and note links.
3) *Number of characters* such as characters in each model elements.
4) *Number of tokens* such as tokens in each model elements.
5) *Graphic token count* = number of nodes + number of edges + textual token count + number of containment + number of adjoinments, where textual token counting is the label counting based on the Levitin's textual token counting [11], a node is enclosed within another node called "Containment" and a node is directly adjoined to another node called "Adjoinment".

The result is shown in table 2. A class diagram defined from UMLsec-SP appears significantly more characters, tokens and graphic tokens than all other class. However, the number of nodes and edges are almost the same. In summary, class diagram created from UMLsec-SP produces the same complexity in term of the number of nodes and edges. It contains a significant number of characters for presenting security pattern-related information which beneficial for the system security designer who needs to trace and reserve this information.

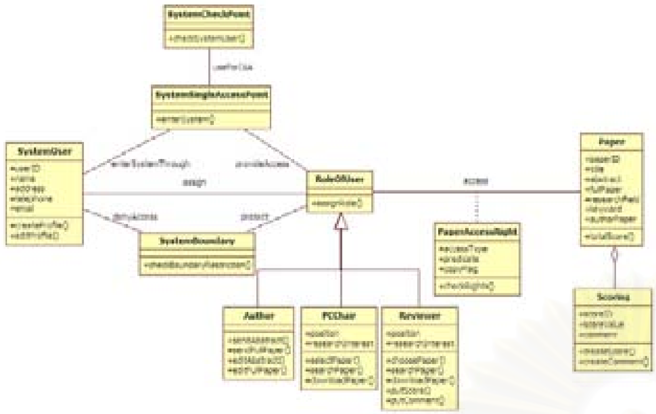


Figure 5. UML diagram for paper review system

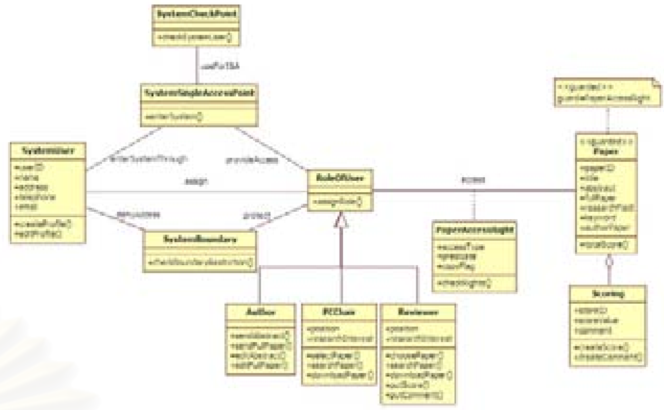


Figure 6. UMLsec diagram for paper review system

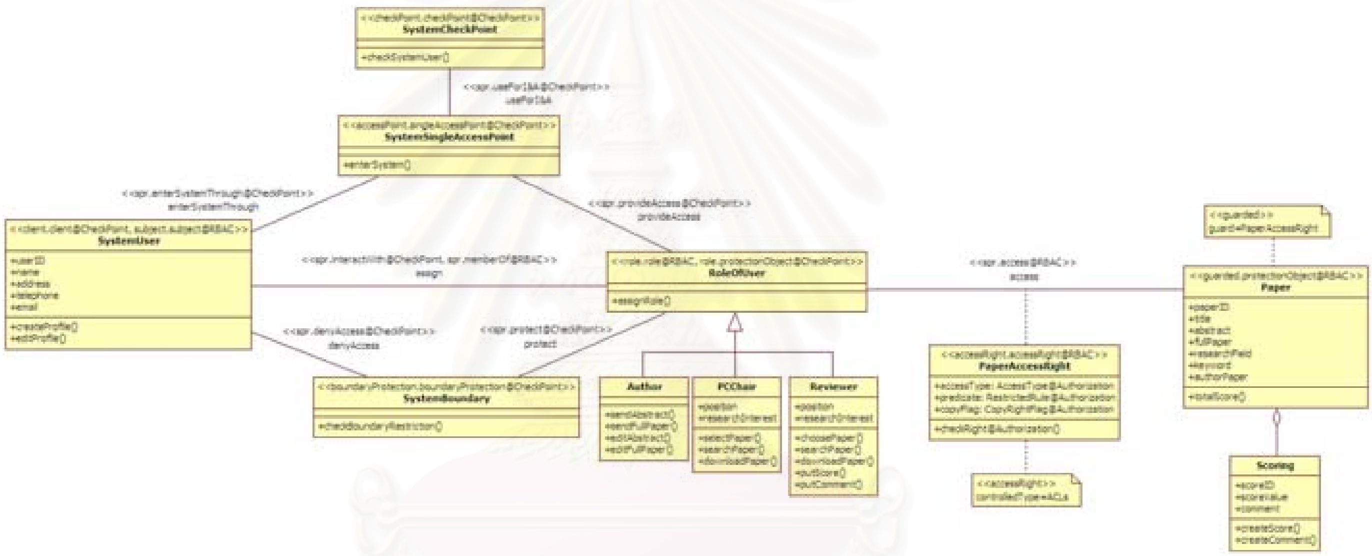


Figure 7. UMLsec-SP diagram for paper review system

TABLE II. THE RESULT OF DIAGRAM COMPLEXITY STUDY

UML types	Number of nodes	Number of edges	Number of characters	Number of tokens	Graphic token count
Original UML	18	14	660	89	782
UMLsec	20	15	695	98	826
UMLsec-SP	21	16	1287	254	1574

VIII. CONCLUSIONS AND FUTURE WORKS

We construct the extended UMLsec, called UMLsec-SP for modeling security patterns by modifying UML profile which is an extension for designing specific domain and combining with UMLsec, the extension for designing security system. UMLsec-SP is beneficial for any security designer to model, trace and reserve the pattern-related information and security-related information of security patterns in the design of security patterns.

UMLsec-SP covers only twenty-seven security patterns apart from forty-six patterns. Next, we continue to improve the UMLsec-SP coverage to cover all patterns declared in [1] based upon the same extension approach proposed. In addition, we plan to construct the supporting tool that includes all the cases of security patterns using UMLsec-SP in order for security designer to apply UMLsec-SP for designing the real world application that uses security patterns.

IX. REFERENCE

[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] K. Supaporn, N. Prompoon and T. Rojkangsadan, *Enterprise Assets Security Requirements Construction from ESRMG Grammar based on Security Patterns, 14th Asia-Pacific Software Engineering Conference*, pages 112-119, 2007.

[3] J. Jürjens, *UMLsec: Extending UML for Secure Systems Development*, Department of Informatics, Munich University of Technology, Germany, 2002.

[4] J. Jürjens, *Secure Systems Development with UML*, Springle, Germany, 2005.

[5] J. Jurjens, G. Popp, and G. Wimmel, "Towards using security patterns in model-based system development," in *Proceedings of PLoP 2002 Conference*, 2002.

[6] J. Dong, S. Yang and K. Zhang, *Visualizing Design Patterns in Their Applications and Composition*, In *IEEE Transactions on Software Engineering, Vol. 33, No. 7*, pages 433-453, 2007.

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

[8] J. Rumbaugh, I. Jacobson and G. Booch, *The Unified Modeling Language Reference Manual Second Edition*, Addison-Wesley, 2004.

[9] J. Warmer and A. Kleppe, The Object Constraint Language – Precise Modeling with UML, Addison-Wesley, 1999.

[10] Object Management Group, *Unified Modeling Language Specification Version 2.1.2*, http://www.omg.org, 2007.

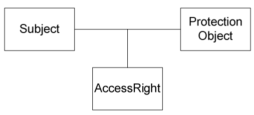
[11] J.V. Nickerson, *Visual Programming : Limits of Graphic Representation*, PhD dissertation, New York Univ., 1994.

Appendix A

TABLE III. UMLSEC-SP STEREOTYPES FOR VISUALIZING PATTERN-RELATED INFORMATION OF SECURITY PATTERN

Stereotype	Base class	Tag	Description
spc (Security Pattern Class)	Class	PatternName, PatternRole, PatternInstance	a class which is a part of security patterns
spt (Security Pattern data Type)	Class	PatternName, PatternRole, PatternInstance	a data type which is a part of security patterns
spr (Security Pattern Relationship)	Relationship	PatternName, PatternRole, PatternInstance	an relationship which is a part of security patterns

TABLE IV. UMLSEC-SP STEREOTYPES FOR VISUALIZING SECURITY-RELATED INFORMATION OF SECURITY PATTERN

Pattern	Pattern description	Stereotype	Base class	Tag	Description
Authorization 	describes who is authorized to access specific resource in system, in an environment in which we have resources whose access needs to be controlled	subject	Class		active entity that attemps to access a resource in system.
		accessRight	Class	controlledType	entity that protects a resource in system.
		accessType	Class		the access type of the subject which is allowed to perform on the protection object.
		restrictedRule	Class		specific conditions which restrict the use of the authorization.
		copyFlag	Class		a boolean that allows some of the authorizations by their holders to other subjects.

We can only present one pattern in this paper because of page limitation.

TABLE V. UMLSEC-SP TAGS FOR VISUALIZING PATTERN-RELATED INFORMATION OF SECURITY PATTERN

Tag	Stereotype	Type	Multiplicity	Description
PatternName	spc, spt and spr	pattern name	*	a pattern name of the component
PatternRole	spc, spt and spr	pattern role name	*	a pattern role of the component
PatternInstance	spc, spt and spr	number of instance	*	a pattern instance of the component

TABLE VI. UMLSEC-SP TAGS FOR VISUALIZING SECURITY-RELATED INFORMATION OF SECURITY PATTERN

Pattern	Tag	Stereotype	Type	Multiplicity	Description
Authorization	controlledType	accessRight	type of access control mechanism	1	the internal mechanism of access controller.

We can only present one pattern in this paper because of page limitation.

ประวัติผู้เขียนวิทยานิพนธ์

นายเกียรติศักดิ์ ไชยสมบูรณ์ เกิดวันที่ 1 ตุลาคม พ.ศ.2526 สำเร็จการศึกษาระดับปริญญาวิทยาศาสตรบัณฑิต สาขาฟิสิกส์ คณะวิทยาศาสตร์ มหาวิทยาลัยมหิดล ในปีการศึกษา 2548 และเข้าศึกษาต่อในหลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาวิทยาศาสตร์คอมพิวเตอร์ ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย ในปีการศึกษา 2549