บทที่ 4

ผลการวิจัย

ในบทนี้จะกล่าวถึงกระบวนการแปลงแบบจำลองการออกแบบที่อิสระจากแพลตฟอร์ม (Platform Independent Model: PIM) ที่มีการเพิ่มคุณสมบัติด้านความปลอดภัยเป็นแบบจำลองที่เฉพาะเจาะจงกับแพลตฟอร์ม (Platform Specific Model: PSM) ที่มีคุณสมบัติด้านความปลอดภัยด้วย โดยในงานวิจัยนี้กำหนดให้มีแบบจำลอง PSM จำนวน 2 แพลตฟอร์มคือ จาวาเว็บเซอร์วิส (Java Web Service) และจาวาเซิร์ฟเล็ต (Java Servlet) ที่รองรับคุณสมบัติด้านความปลอดภัย ซึ่งในการแปลงแบบจำลองจะนำเสนอกฎการแปลง (Transformation Rule) สำหรับทั้งสองแพลตฟอร์ม และการพัฒนาแอพพลิเคชั่นกรณีศึกษาเพื่อวัดผลความถูกต้องและครอบคลุมในการขยายแบบจำลองการออกแบบที่อิสระแพลตฟอร์มให้มีคุณสมบัติด้านความปลอดภัย และการสรุปผลการแปลงแบบจำลอง

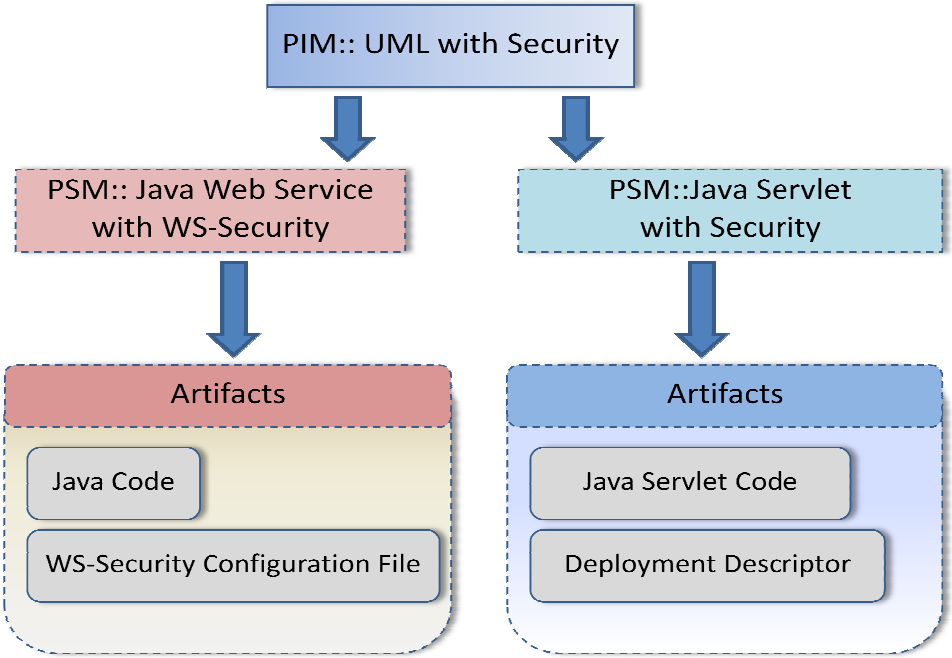
4.1 การนิยามกฎการแปลงแบบจำลอง (Transformation Rule)

การกำหนดกฎการแปลงจะแยกออกเป็น 2 ระดับคือกฎสำหรับใช้ในการแปลงแบบจำลอง (Model Transformation) จากแบบจำลอง PIM ไปเป็นแบบจำลอง PSM ซึ่งเป็นการแปลงแบบจำลองแบบ Model-to-Model และระดับที่สองคือการแปลงจากแบบจำลอง PSM เป็นซอร์สโค้ดหรือไฟล์คอนฟิกกูเรชั่น (Configuration File) ซึ่งเป็นการแปลงแบบจำลองแบบ Model-to-Code การแปลงเริ่มต้นจากนำแบบจำลอง PIM ที่มีคุณสมบัติด้านความปลอดภัย เข้าสู่กระบวนการแปลงให้ได้เป็นแบบจำลอง PSM คือจาวาเว็บเซอร์วิส และจาวาเซิร์ฟเล็ต ที่ทั้งคู่มีคุณสมบัติด้านความปลอดภัย และถัดมาแบบจำลองจาวาเว็บเซอร์วิสจะถูกนำไปสร้าง (Generate) เป็นซอร์สโค้ดของจาวา และไฟล์คอนฟิกกูเรชั่นสำหรับใช้ในการรักษาความปลอดภัยของเว็บเซอร์วิส (WS-Security) และแบบจำลองจาวาเซิร์ฟเล็ตจะถูกนำไปสร้างเป็นจาวาเซิร์ฟเล็ตและไฟล์ Deployment Descriptor เช่นไฟล์ web.xml ที่เป็นส่วนของการรักษาความปลอดภัยของเซิร์ฟเล็ตตามลำดับ ดังแสดงภาพที่ 4.1

กฎการแปลงแบบจำลองที่เกี่ยวข้องกับเรื่องความปลอดภัยสามารถนิยามออกมาเป็นกฎที่สำคัญได้ทั้งหมด 6 กฎ แบ่งเป็นกฎการแปลงเป็นแบบจำลองจาวาเซิร์ฟเล็ตที่มีคุณสมบัติ

ด้านความปลอดภัยมีการนิยามกฎการแปลงที่เกี่ยวข้องกับความปลอดภัยทั้งหมด 3 กฎ ดังแสดงในตารางที่ 4.1

ภาพที่ 4.1
แผนภาพแสดงการแปลงจากแบบจำลอง PIM เป็นแบบจำลอง PSM
และจาก PSM สร้างเป็นชิ้นงานต่างๆ ที่เกี่ยวข้อง



ตารางที่ 4.1
สรุปจำนวนกฎการแปลงแบบจำลองในส่วนคุณสมบัติ
ด้านความปลอดภัยของสองแพลตฟอร์ม

แพลตฟอร์ม	จำนวน (กฎ)
จาวาเว็บเซอร์วิส	3
จาวาเซิร์ฟเล็ต	5

4.1.1 การแปลงแบบจำลองจากแบบจำลอง UML ที่มีคุณสมบัติด้านความปลอดภัยเป็นแบบจำลองจาวาเว็บเซอร์วิสที่มีการรักษาความปลอดภัย (WS-Security)

การแปลงแบบจำลอง UML ที่มีคุณสมบัติความปลอดภัยเป็นแบบจำลองจาวาเว็บเซอร์วิสที่มีการรักษาความปลอดภัยนั้น จะแบ่งการนิยามกฎการแปลงแยกออกเป็น 3 ด้าน ตามคุณสมบัติความปลอดภัยที่เมตาโมเดลรองรับคือการพิสูจน์ตัวจริง (Authentication) การรักษาความลับ (Confidentiality) และการรักษาความสมบูรณ์ (Integrity) โดยในงานวิจัยนี้เน้นการแสดงให้เห็นถึงการแปลงแบบจำลอง PIM เป็นแบบจำลอง PSM เฉพาะส่วนที่เกี่ยวกับคุณสมบัติด้านความปลอดภัย ดังนั้นรายละเอียดในส่วนของกฎการแปลงแบบจำลอง UML พื้นฐานเป็นแบบจำลองภาษาจาวาสามารถดูรายละเอียดการจับคู่ของอิลิเมนต์ (บางส่วน) ดังแสดงในตารางที่ 4.2 ส่วนกฎการแปลงแบบจำลองจาก UML พื้นฐานเป็นจาวาดูรายละเอียดได้จากภาคผนวก ก.

ตารางที่ 4.2
การจับคู่อิลิเมนต์ของเมตาโมเดลเพื่อแปลงแบบจำลอง
คลาสของ UML พื้นฐานเป็นแบบจำลองจาวา

เมตาโมเดลของแบบจำลอง PIM	เมตาโมเดลของแบบจำลองจาวา
Package	JavaPackage
- Class	- JavaClass
- Operation	- Method
- Parameter	- JavaParameter
- Attribute	- Field
- AssociationEnd	- Field

การนิยามกฎการแปลงจากแบบจำลอง PIM เป็นแบบจำลองจาวาเว็บเซอร์วิสที่มีคุณสมบัติด้านความปลอดภัย กำหนดให้อิลิเมนต์ Class ของเมตาโมเดลของแบบจำลอง PIM แปลงเป็นคลาส JavaWebService ดังที่อธิบายไว้ในกฎชื่อ ClassToJWClass ในภาพที่ 4.2 โดยคุณสมบัติด้านความปลอดภัยจะถูกกำหนดในระดับของ Operation เพราะความต้องการของระบบจะเป็นความปลอดภัยในการให้บริการที่เว็บเซอร์วิสเปิดใช้งาน

1. กฎ ClassToJavaWSClass

กฎ ClassToJavaWSClass คือกฎที่นิยามสำหรับใช้แปลง Class เป็น Web Service Class โดยอิลิเมนต์ Class ของแบบจำลอง PIM ที่มีประเภทของคลาส ClassType แบบ service จะถูกสร้างอิลิเมนต์ WebServiceClass ในแบบจำลองจาวาเว็บเซอร์วิส และหลังจากที่สร้างอิลิเมนต์ WebServiceClass แล้วภายใต้กฎนี้จะตรวจสอบว่าอิลิเมนต์ Class ของแบบจำลอง PIM มี Operation ใดที่กำหนดความต้องการด้านความปลอดภัยกำกับมากับอิลิเมนต์ของ Operation หรือไม่ โดยมีการนิยามโดยใช้กฎชื่อ SecOperationToMethodAuth แทนการแปลงแบบจำลองความปลอดภัยเรื่องการพิสูจน์ตัวจริง และSecOperationToMethodConf แทนการแปลงแบบจำลองความปลอดภัยเรื่องการรักษาความลับ และ SecOperationToMethodIntegrity แทนการแปลงแบบจำลองความปลอดภัยเรื่องการรักษาความสมบูรณ์ กฎแสดงในภาพที่ 4.2

ภาพที่ 4.2
กฎการแปลงอิลิเมนต์ Class เป็น Web Sevice Class
ในแพลตฟอร์มจาวาเว็บเซอร์วิส

```
relation ClassToJavaWSClass {
          cn: String;
          isAbstract : Boolean;

          checkonly domain umlsec c:umlsec::Class{
             type = umlsec::ClassType::service,
             name = cn,
             isAbstract = isAbstract
          };

          enforce domain javaws jc:javasec::WebServiceClass {
             name = cn,
             isAbstract = isAbstract,
             typeKind = javasec::TypeKind::TypeClass
          };

          where {
             SecureAttributeToField(c, jc);
             SecureOperationToMethod(c, jc);
             SecOperationToMethodAuth(c, jc);
             SecOperationToMethodConf(c, jc);
             SecOperationToMethodIntegrity(c, jc);
          }
}
```

2. กฎการแปลงแบบจำลอง PIM ที่มีคุณสมบัติด้านความปลอดภัย
ในการพิสูจน์ตัวจริง

เมตาโมเดลของแบบจำลอง PIM ในส่วนความต้องการด้านความปลอดภัยในการพิสูจน์ตัวจริงแทนด้วยอิลิเมนต์ Authentication ซึ่งได้ถ่ายทอดคุณสมบัติมาจากอิลิเมนต์ SecurityRequirement การจับคู่กันระหว่างเมตาโมเดลสามารถแยกออกเป็นกรณีทั้งหมดได้ 4 กรณี ตามประเภทของ UserIdentity ดังแสดงในตารางที่ 4.3 UserIdentity แบบ Credentials สามารถจับคู่เมตาโมเดลของเว็บเซอร์วิสในส่วนของ UsernameToken ในการจัดการด้านการพิสูจน์ตัวจริง

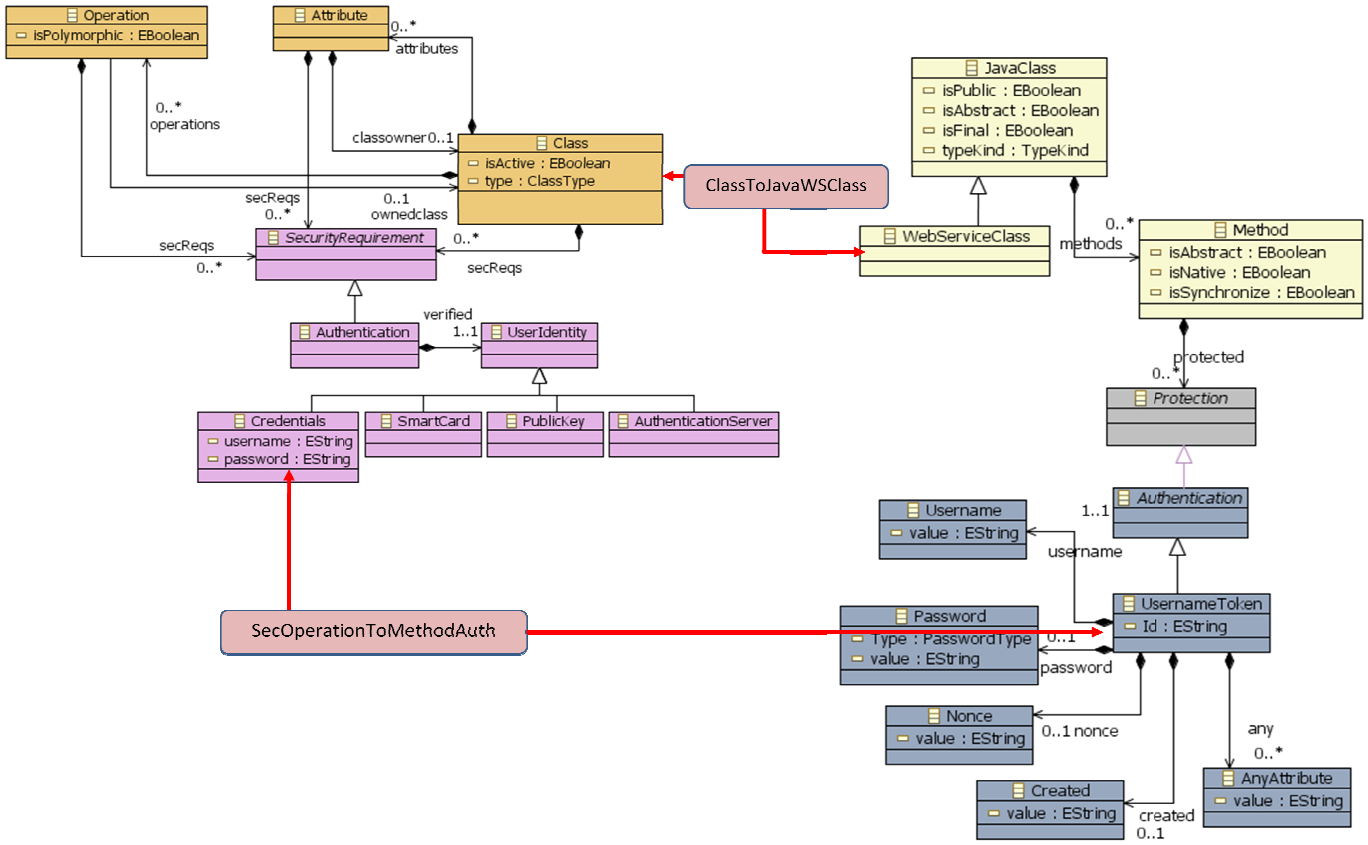
ตารางที่ 4.3
การจับคู่อิลิเมนต์สำหรับจัดการความปลอดภัย
ด้านการพิสูจน์ตัวจริง

เมตาโมเดลของแบบจำลอง PIM	เมตาโมเดลจาวาเว็บเซอร์วิส
Class	WebServiceClass
- ClassType=“service”	-
- Operation	- Method
- Authentication	-
- Credential:UserIdentity	- UsernameToken
- Username	- Username
- Password	- Password
-	- Nonce
-	- Created
- Authentication	-
- PublicKey:UserIdentity	-ไม่สามารถจับคู่กับอิลิเมนต์ใดๆได้
- Authentication	-
- SmartCard:UserIdentity	-ไม่สามารถจับคู่กับอิลิเมนต์ใดๆได้
- Authentication	-
- AuthenticationServer:UserIdentity	-ไม่สามารถจับคู่กับอิลิเมนต์ใดๆได้

ภาพที่ 4.3

การจับคู่ระหว่างเมตาโมเดลของ PIM กับเมตาโมเดลของจาวา

เว็บเซอร์วิสที่มีความปลอดภัยด้านการพิสูจน์ตัวจริง



คำอธิบายกฎ SecOperationToMethodAuth

กฎ SecOperationToMethodAuth คือกฎที่นิยามสำหรับแปลงอิลิเมนต์ Operation ของเมตาโมเดลของแบบจำลอง PIM ที่กำหนดความต้องการด้านความปลอดภัยเรื่องการพิสูจน์ตัวจริง เป็น Method ที่มีคุณสมบัติความปลอดภัยด้านการพิสูจน์ตัวจริงในแบบจำลองจาวาเว็บเซอร์วิส ถ้ามีการกำหนด Authentication ด้วยวิธีการตรวจสอบแบบ Credentials ก็จะเป็นใช้ชื่อผู้ใช้และรหัสผ่านเป็นกลไกในการตรวจสอบตัวตนของผู้ใช้ ในส่วนของเว็บเซอร์วิสการพิสูจน์ตัวจริงก็จะแทนด้วยการใช้ UsernameToken ดังแสดงในกฎที่ 4.4

ภาพที่ 4.4

กฎการแปลงอิลิเมนต์ Operation เป็น Method ในแบบจำลองจาวา

เว็บเซอร์วิสที่รองรับความปลอดภัยด้านการพิสูจน์ตัวจริง

```
relation SecOperationToMethodAuth {
          on, uname, pass : String;
          checkonly domain umlsec c:umlsec::Class {
             operations = so:umlsec::Operation {
                   name = on,
                   secreqs = req : umlsec::Authentication {
                         verified =  cred : umlsec::Credentials{
                               username = uname,
                               password = pass
                         }
                   }
             }
          };

          enforce domain javaws jc:javase::WebServiceClass {
             methods = jm:javase::Method{
                   name = on,
                   protected = pt:javase::UsernameToken{
                         username = u:javase::Username{
                               value = uname
                         },
                         password = ps : javase::Password {
                               value = pass
                         },
                         nonce = nonce:javase::Nonce{},
                         created = cd:javase::Created{}
                   }
             }
          };
          where {
             parameterToInputJavaParameter(so, jm);
             parameterToReturnJavaParameter(so, jm);
          }
}
```

3. กฎการแปลงแบบจำลองที่มีคุณสมบัติด้านความปลอดภัยในการรักษาความลับ

คุณสมบัติด้านความปลอดภัยในการรักษาความลับสามารถกำหนดโดยเพิ่มอิลิ-เมนต์ Confidentiality ให้กับอิลิเมนต์ Operation กำกับลงไปในแบบจำลอง PIM โดยในการแปลงเป็นแบบจำลองจาวาเว็บเซอร์วิสที่มีการรักษาความปลอดภัย จะสร้างอิลิเมนต์ Method ที่มีอิลิเมนต์ Confidentiality กำกับไว้ภายใน กลไกการรักษาความลับตามข้อกำหนดของ WS-Security กำหนดโดยใช้วิธีการระบุ EncryptedKey การจับคู่ของอิลิเมนต์ระหว่างเมตาโมเดลของแบบจำลอง PIM กับเมตาโมเดลของแบบจำลอง PSM สามารถจับคู่ได้ 1 กรณีคือกรณีที่กำหนด UserIdentity เป็น PublicKey ดังแสดงในตารางที่ 4.4 สำหรับกฎที่ใช้ในการแปลงแบบจำลองด้านนี้ใช้ชื่อกฎ SecOperationToMethodConf ในภาพที่ 4.6

ตารางที่ 4.4
การจับคู่อิลิเมนต์สำหรับจัดการความปลอดภัย
ด้านการรักษาความลับ

เมตาโมเดลของแบบจำลอง PIM	เมตาโมเดลจาวาเว็บเซอร์วิส
Class: - ClassType=“service”	WebServiceClass
- Operation	- Method
- Confidentiality	- Confidentiality
- PublicKey:UserIdentity	- EncryptedKey
- Individual:AuthorizedParty	- KeyInfo
	- EncryptionMethod
	- CipherData
	- ReferenceList
- Confidentiality	- Confidentiality
- Credentials:UserIdentity	-ไม่สามารถจับคู่กับอิลิเมนต์ใดๆได้
- Individual:AuthorizedParty	
- Confidentiality	- Confidentiality
- SmartCard:UserIdentity	-ไม่สามารถจับคู่กับอิลิเมนต์ใดๆได้
- Individual:AuthorizedParty	

ตารางที่ 4.4 (ต่อ)
การจับคู่อิลิเมนต์สำหรับจัดการความปลอดภัย
ด้านการรักษาความลับ

เมตาโมเดลของแบบจำลอง PIM	เมตาโมเดลจาวาเว็บเซอร์วิส
- Confidentiality	- Confidentiality
- AuthenticationServer:UserIdentity	-ไม่สามารถจับคู่กับอิลิเมนต์ใดๆ ได้
- Individual:AuthorizedParty	

คำอธิบายกฎ SecOperationToMethodConf

กฎที่นิยามสำหรับแปลงอิลิเมนต์ Operation ของแบบจำลอง PIM ที่มีการเพิ่มความต้องการด้านความปลอดภัยเรื่องการรักษาความลับโดยใช้อิลิเมนต์ Confidentiality จะสร้างอิลิเมนต์ Method ของแบบจำลอง PSM ที่ภายใน Method มีการระบุกลไกการรักษาความลับตามมาตรฐาน WS-Security โดยใช้อิลิเมนต์ EncryptedKey ที่มีการกำหนดรายละเอียดที่เกี่ยวข้องกับการเข้ารหัสข้อมูล เช่นอัลกอริทึมที่ใช้ด้วยอิลิเมนต์ EncryptionMethod หรือการกำหนดรายละเอียดของคีย์โดยการใช้ KeyInfo