การกำหนดความต้องการความมั่นคงโดยใช้ไวยากรณ์ที่สร้างจากคำแนะนำส่วนต่อประสานผู้ใช้ของบริบทความมั่นคงเชิงเว็บ

นางสาวภัทรียา สิงห์พันธ์

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต
สาขาวิชาวิศวกรรมซอฟต์แวร์ ภาควิชาวิศวกรรมคอมพิวเตอร์
คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2558

DEFINING SECURITY REQUIREMENTS USING GRAMMAR GENERATED FROM USER INTERFACE GUIDELINES OF WEB SECURITY CONTEXT

Miss Pattariya Singpant

A Thesis Submitted in Partial Fulfillment of the Requirements
for the Degree of Master of Science Program in Software Engineering
Department of Computer Engineering
Faculty of Engineering
Chulalongkorn University
Academic Year 2015

หัวข้อวิทยานิพนธ์	การกำหนดความต้องการความมั่นคงโดยใช้ไวยากรณ์ที่สร้างจากคำแนะนำส่วนต่อประสานผู้ใช้ของบริบทความมั่นคงเชิงเว็บ
โดย	นางสาวภัทรียา สิงห์พันธ์
สาขาวิชา	วิศวกรรมซอฟต์แวร์
อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก	ผู้ช่วยศาสตราจารย์ นครทิพย์ พร้อมพูล

คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย อนุมัติให้นับวิทยานิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญามหาบัณฑิต

.....คณบดีคณะวิศวกรรมศาสตร์

(รองศาสตราจารย์ ดร. สุพจน์ เตชวรสินสกุล)

คณะกรรมการสอบวิทยานิพนธ์

.....ประธานกรรมการ

(รองศาสตราจารย์ ดร. ทวิตีย์ เสนีวงศ์ ณ อยุธยา)

.....อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก

(ผู้ช่วยศาสตราจารย์ นครทิพย์ พร้อมพูล)

.....กรรมการ

(รองศาสตราจารย์ ดร. เศรษฐา ปานงาม)

.....กรรมการภายนอกมหาวิทยาลัย

(รองศาสตราจารย์ ดร. วีระ บุญจริง)

ภัทรียา สิงห์พันธ์ : การกำหนดความต้องการความมั่นคงโดยใช้ไวยากรณ์ที่สร้างจากคำแนะนำส่วนต่อประสานผู้ใช้ของบริบทความมั่นคงเชิงเว็บ (DEFINING SECURITY REQUIREMENTS USING GRAMMAR GENERATED FROM USER INTERFACE GUIDELINES OF WEB SECURITY CONTEXT) อ.ที่ปรึกษาวิทยานิพนธ์หลัก: ผศ. นครทิพย์ พร้อมพูล, 207 หน้า.

ในปัจจุบันมีเว็บไซต์ลอกเลียนจำนวนมากถูกสร้างขึ้นเพื่อเพื่อโจรกรรมข้อมูลส่วนบุคคล ส่งผลให้ความเชื่อถือของการใช้บริการผ่านระบบออนไลน์ลดลง เพื่อแก้ไขปัญหาดังกล่าว ดับเบิ้ลยู สามซีจึงนำเสนอเอกสารบริบทความมั่นคงเชิงเว็บ: คำแนะนำส่วนต่อประสานผู้ใช้ หรือเอกสารดับเบิ้ลยูเอสซียูไอ ในการออกแบบตัวแทนผู้ใช้เว็บให้สามารถเข้าถึงเนื้อหาเว็บอย่างมีความปลอดภัย เพื่อให้ระบบที่พัฒนาขึ้นสอดคล้องกับเอกสารดังกล่าว ผู้พัฒนาระบบจำเป็นต้องศึกษาเนื้อหาจำนวนมาก เพื่อระบุรายการความต้องการด้านความมั่นคงของระบบ ซึ่งต้องให้เวลาในการทำความเข้าใจ

วิทยานิพนธ์นี้มีจุดประสงค์เพื่อ วิเคราะห์ประเด็นปัญหา และรวบรวมผลเฉลยจากเอกสารดับเบิ้ลยูเอสซียูไอ และองค์ความรู้ที่เกี่ยวข้อง เป็นแบบรูปบริบทความมั่นคงเชิงเว็บ และสร้างไวยากรณ์ความมั่นคง ในการพัฒนาเครื่องมือสำหรับการระบุความต้องการความมั่นคงของตัวแทนผู้ใช้เว็บ เพื่อนำไปใช้ในการออกแบบ และพัฒนาให้สอดคล้องกับเอกสารดับเบิ้ลยูเอสซียูไอ

ผู้วิจัยได้สร้างแบบรูปบริบทความมั่นคงเชิงเว็บ โดยการวิเคราะห์เนื้อหาของเอกสารดับเบิ้ลยูเอสซียูไอ เพื่อให้ได้เนื้อหาที่เหมาะสมในแต่ละองค์ประกอบของแบบรูป จากนั้นทวนสอบความครบถ้วนและความสอดคล้องไปยังเอกสารดับเบิ้ลยูเอสซียูไอ โดยหน่วยทดลองที่มีความรู้และประสบการณ์ด้านความมั่นคง ทำการประเมินเพื่อปรับปรุงแบบรูป จากนั้นจึงสร้างแผนภาพต้นไม้ความมั่นคง และแปลงเป็นไวยากรณ์ความมั่นคง เพื่อใช้ในการสร้างเครื่องมือต้นแบบสำหรับการกำหนดความต้องการความมั่นคงของตัวแทนผู้ใช้เว็บ

เครื่องมือต้นแบบทดสอบโดยหน่วยทดลอง เพื่อเปรียบเทียบความครบถ้วนระหว่างการกำหนดความต้องการด้วยมือและด้วยเครื่องมือ ผลการทดลองพบว่าเครื่องมือสามารถสนับสนุนให้ผู้ใช้งานระบุรายการความต้องการได้มากกว่า และเร็วกว่าการดำเนินการด้วยมือ

ภาควิชา วิศวกรรมคอมพิวเตอร์ ลายมือชื่อนิสิต .....

สาขาวิชา วิศวกรรมซอฟต์แวร์ ลายมือชื่อ อ.ที่ปรึกษาหลัก .....

ปีการศึกษา 2558

5570497621 : MAJOR SOFTWARE ENGINEERING

KEYWORDS: WEB SECURITY CONTEXT / SECURITY PATERNS / SECURITY GRAMMARS / WEB USER AGENT / WSC-UI

PATTARIYA SINGPANT: DEFINING SECURITY REQUIREMENTS USING GRAMMAR GENERATED FROM USER INTERFACE GUIDELINES OF WEB SECURITY CONTEXT. ADVISOR: ASST. PROF. NAKORNTHIP PROMPOON, 207 pp.

At present, a large number of forged websites were created to acquire sensitive information that leads to a decrease in trustworthy in online services. To solve this problem, W3C established Web Security Context: User Interface Guidelines or WSC-UI to provide a secure design of a web user agent for web content access. In order to develop a system that conforms to the content of WSC-UI. The developer is required to spend time studying numerous contents of this document in order to specify a system security requirements specification.

The objective of this thesis is to analyze problem issues and to collect solutions from WSC-UI and related knowledge for constructing web security context patterns. In addition, security grammar was created to develop a prototype tool. It will be used in defining security requirements for web user agents.

The web security context patterns were created based on the textual content analysis in order to provide the content of each pattern element appropriately. In addition, content completeness and conformance to WSC-UI by experts who have knowledge and experiences in security area to evaluate for improving these patterns. Then, the security tree was created and transformed to security grammar for applying in a prototype tool development, which can be used to define security requirements.

The prototype tool was tested by experimental units for content completeness between requirements created by manual and tool. The experimental result indicated that the proposed tool can support user for defining more requirements and faster than the manual approach.

Department: Computer Engineering Student's Signature .....

Field of Study: Software Engineering Advisor's Signature .....

Academic Year: 2015

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้ สำเร็จลุล่วงได้ด้วยความช่วยเหลืออย่างดียิ่งจาก ผู้ช่วยศาสตราจารย์ นครทิพย์ พร้อมพูล อาจารย์ที่ปรึกษาวิทยานิพนธ์ ขอกราบขอบพระคุณอาจารย์ที่เสียสละเวลาช่วยให้คำปรึกษาและชี้แนะแนวทางการวิจัยที่เป็นประโยชน์ยิ่งในการปรับปรุงแก้ไขจนวิทยานิพนธ์ฉบับนี้สำเร็จ รวมทั้งให้ความรู้ทั้งในด้านวิชาการ ด้านการใช้ชีวิตในสังคม ด้านคุณธรรมตลอดจนความดูแลเอาใจใส่ ความเชื่อมั่น ความเมตตา และความกรุณาที่อาจารย์มีให้กับข้าพเจ้า ทำให้ข้าพเจ้าสามารถดำเนินงานวิจัยจนกระทั่งประสบผลสำเร็จและมีคุณภาพ

ขอกราบขอบพระคุณคณะกรรมการสอบวิทยานิพนธ์ทุกท่านได้แก่ รองศาสตราจารย์ ดร. ทวิตีย์ เสนีวงศ์ ณ อยุธยา ประธานกรรมการสอบ รองศาสตราจารย์ ดร. เศรษฐา ปานงาม กรรมการผู้ทรงคุณวุฒิภายในมหาวิทยาลัย รองศาสตราจารย์ ดร. วีระ บุญจริง กรรมการผู้ทรงคุณวุฒิภายนอกมหาวิทยาลัย ที่ได้กรุณาสละเวลาให้คำแนะนาอันเป็นประโยชน์อย่างดียิ่งต่อการทำวิจัย รวมถึงขัดเกลาสำนวนภาษา และพิจารณาเนื้อหาให้ถูกต้องและครบถ้วน เพื่อให้วิทยานิพนธ์ฉบับนี้มีคุณภาพและมีความสมบูรณ์ยิ่งขึ้น

ขอขอบพระคุณคณาจารย์ในภาควิชาวิศวกรรมคอมพิวเตอร์ จุฬาลงกรณ์มหาวิทยาลัย ทุกท่าน ที่ประสิทธิ์ประสาทความรู้อันมีค่าแก่ผู้วิจัย

ขอขอบคุณสมาชิกในห้องปฏิบัติการวิศวกรรมซอฟต์แวร์ สำหรับน้ำใจ ความห่วงใย ความช่วยเหลือ ให้คำแนะนำที่มีประโยชน์แก่ผู้วิจัย และสละเวลามาช่วยเป็นหน่วยทดลองในการทำการทดลอง ทำให้งานวิจัยนี้สำเร็จลุล่วงไปได้

ความสำเร็จของการศึกษาครั้งนี้ผู้วิจัยชองอุทิศให้คุณยายจันทร์เพ็ญ สุปันนุช ผู้ล่วงลับไปแล้ว งานวิจัยเล่มนี้จะไม่สามารถสำเร็จลงได้เลยหากขาดกำลังใจที่สำคัญจากครอบครัวของผู้วิจัย โดยเฉพาะอย่างยิ่งนายพงษ์ธร สิงห์พันธ์ บิดา และนางนิตยา สิงห์พันธ์ มารดา ที่มอบโอกาสในการศึกษาต่อในระดับปริญญามหาบัณฑิต และนางสาวพัศนันท์ สิงห์พันธ์ ที่คอยสนับสนุนผู้วิจัยในทุกๆ ด้าน ทั้งยังให้ความรัก ความอบอุ่น และกำลังใจอย่างดียิ่ง ทั้งในยามทุกข์และยามสุขแก่ผู้วิจัยเสมอมา ขอขอบพระคุณทุกมือทุกใจที่คอยห่วงใยและหวังดีช่วยเหลืออยู่เบื้องหลัง โดยเฉพาะนายธนวัตร มั่นอ่องที่คอยให้คำปรึกษาในการพัฒนาเครื่องมือด้วยความอุตสาหะ ส่งผลให้ข้าพเจ้าประสบความสำเร็จได้ในวันนี้ สุดท้ายนี้ผู้วิจัยหวังเป็นอย่างยิ่งว่าวิทยานิพนธ์ฉบับนี้จะสร้างแรงบันดาลใจ และเป็นแรงผลักดันให้เกิดการพัฒนาด้านวิศวกรรมซอฟต์แวร์ต่อไป

สารบัญ

หน้า

หน้า

สารบัญตาราง

หน้า

สารบัญภาพ

หน้า

บทที่ 1
บทนำ

1.1 ที่มาและความสำคัญของปัญหา

ปัจจุบันการใช้งานผ่านระบบออนไลน์เข้ามามีบทบาทเป็นอย่างมากในชีวิตประจำวันของผู้ใช้ เนื่องจากผู้ประกอบการส่วนใหญ่ขยายช่องทางการให้ข้อมูลสินค้าและบริการผ่านเว็บไซต์มากขึ้นเพื่ออำนวยความสะดวกแก่ผู้รับบริการ โดยผู้ใช้สามารถเข้าถึงเว็บไซต์ดังกล่าวผ่านตัวแทนผู้ใช้เว็บ (Web User Agents) ที่ติดตั้งบนอุปกรณ์ เช่น คอมพิวเตอร์ส่วนบุคคล โทรศัพท์เคลื่อนที่ เป็นต้น ซึ่งบริการบางประเภทมีความจำเป็นต้องร้องขอข้อมูลส่วนบุคคลจากผู้ใช้ เช่น การทำธุรกรรมทางอิเล็กทรอนิกส์ที่ผู้ใช้ต้องนำเข้าข้อมูลหมายเลขบัตรเครดิตไปยังเว็บไซต์ผู้ให้บริการที่ผู้ใช้เชื่อถือ แม้เว็บไซต์ที่ให้บริการนั้นมีความน่าเชื่อถือแต่ก็ยังอาจตกเป็นเป้าหมายของการหลอกลวงทางอินเทอร์เน็ต (Phishing) โดยนักโจรกรรมข้อมูลสร้างเว็บไซต์ปลอมขึ้นมาจากการลอกเลียนเว็บต้นแบบ เพื่อล่อลวงให้ผู้ใช้หลงเชื่อและนำข้อมูลส่วนบุคคลเข้าสู่เว็บปลอม อีกทั้งยังมีโปรแกรมประยุกต์บนเว็บจำนวนมากที่ออกแบบโดยปราศจากการคำนึงถึงข้อกำหนดด้านความมั่นคง เว็บที่พัฒนาขึ้นจึงไม่คล้อยตามมาตรฐานความมั่นคงของเว็บ [1] ก่อให้เกิดช่องโหว่อันเสี่ยงต่อการถูกโจมตีให้เกิดความเสียหายแก่ระบบโดยผู้ไม่ประสงค์ดี อีกทั้งหากข้อมูลส่วนบุคคลของผู้ใช้ถูกโจรกรรมไปใช้ฉ้อโกงหรือก่ออาชญากรรมอันเกิดความเสียหายแก่ผู้ใช้แล้ว จะส่งผลให้ความนิยมของผู้ใช้ในการใช้บริการผ่านระบบออนไลน์ลดน้อยลงไปจนถึงยกเลิกการใช้งานในที่สุด อันเนื่องจากผู้ใช้ขาดความเชื่อมั่นในความมั่งคงของระบบ

การสร้างบริบทความมั่นคงเชิงเว็บ (Web Security Context) โดยตัวแทนผู้ใช้เว็บแสดงข้อมูลและส่งสัญญาณการเตือนภัยด้านความมั่นคงเกี่ยวกับเว็บไซต์ให้แก่ผู้ใช้ได้ทราบ เช่น เมื่อเว็บไซต์ที่ผู้ใช้กำลังติดต่อไม่มีการเข้ารหัสข้อมูลเพื่อรักษาความมั่นคงชั้นขนส่งแล้ว ตัวแทนผู้ใช้จะแสดงแถบตำแหน่ง (Location Bar) ด้วยไฮไลท์สีแดงแตกต่างจากสถานะปกติเพื่อแจ้งเตือนการรักษาบูรณภาพของระบบ เมื่อผู้ใช้สังเกตเห็นความผิดปกติดังกล่าว ผู้ใช้สามารถพิจารณาและตัดสินใจยกเลิกการติดต่อกับเว็บไซต์ที่ต้องสงสัย เพื่อความปลอดภัยของข้อมูลส่วนบุคคล ด้วยเหตุนี้ เวิลด์ไวด์เว็บคอนซอร์เทียม หรือดับเบิ้ลยูสามซี (World Wide Web Consortium: W3C) เป็นองค์กรที่กำหนดมาตรฐานด้านการพัฒนาเว็บ จึงได้นำเสนอเอกสารบริบทความมั่นคงเชิงเว็บ: คำแนะนำส่วนต่อประสานผู้ใช้ หรือดับเบิ้ลยูเอสซียูไอ (Web Security Context: User Interface Guidelines, WSC-UI) [2] โดยรวบรวมวิธีการปฏิบัติที่เป็นเลิศ (Best Practices) ในการแสดงผลบริบทความมั่นคงเชิงเว็บผ่านส่วนต่อประสานของตัวแทนผู้ใช้เว็บ เพื่อให้การเข้าถึงเนื้อหาเว็บและ

ส่งผ่านข้อมูลส่วนบุคคลด้วยตัวแทนผู้ใช้เว็บเป็นไปอย่างมีความปลอดภัย ดังนั้นการออกแบบเพื่อพัฒนาตัวแทนผู้ใช้เว็บโดยคำนึงถึงบริบทความมั่นคงเชิงเว็บจะสนับสนุนความมั่นคงของระบบพร้อมกับสร้างความมั่นใจให้แก่ผู้ใช้ในการใช้งานระบบ

วิศวกรรมความต้องการซอฟต์แวร์ถือเป็นกระบวนการสำคัญในการรวบรวมความต้องการมาวิเคราะห์เพื่อให้ได้มาซึ่งข้อกำหนดความต้องการซอฟต์แวร์ที่ใช้ในการออกแบบและพัฒนาระบบ โดยความต้องการแบ่งได้เป็น 2 ประเภท คือ ความต้องการเชิงหน้าที่ (Functional Requirements) และความต้องการเชิงคุณภาพ (Quality Requirements) ความต้องการเชิงหน้าที่กำหนดความสามารถในการประมวลผลตามหน้าที่หลักของระบบ ในขณะที่ความต้องการเชิงคุณภาพกำหนดคุณสมบัติของระบบอันสนับสนุนให้ระบบทำงานตามหน้าที่หลัก จากคำจำกัดความดังกล่าว วิธีการปฏิบัติที่เป็นเลิศในเอกสารดับเบิ้ลเอสซียูไอก็มีจุดประสงค์เพื่อลดช่องโหว่ที่เสี่ยงต่อการโจมตี ซึ่งสอดคล้องกับความต้องการด้านความมั่นคง (Security Requirements) กล่าวคือ ความต้องการเชิงคุณภาพประเภทหนึ่งที่เกี่ยวข้องกับการกำหนดความมั่นคงของระบบ ดังนั้นผู้พัฒนาควรกำหนดความต้องการด้านมั่นคงโดยใช้กระบวนการความต้องการความมั่นคงเพื่อให้ตัวแทนผู้ใช้เว็บที่พัฒนาเป็นไปตามแนวปฏิบัติที่กำหนดโดยดับเบิ้ลยูสามซี

จากการศึกษางานวิจัย [3, 4] ได้กำหนดความต้องการของระบบด้วยวิธีวิเคราะห์และสรุปความต้องการจากเนื้อหาเอกสารมาตรฐานของดับเบิ้ลยูสามซี แม้วิธีการดังกล่าวได้ผลลัพธ์รายการความต้องการ แต่ยังขาดการทวนสอบความคล้อยตามไปยังเอกสารมาตรฐานของดับเบิ้ลยูสามซี ทั้งยังอยู่ในรูปแบบที่ยากต่อการนำมาใช้ซ้ำในการระบุความต้องการของระบบที่คล้ายเคียงกัน ในขณะที่การใช้แบบรูปความมั่นคงในการรวบรวมผลเฉลยที่สอดคล้องตามประเด็นปัญหาจะช่วยให้เอกสารมีรูปแบบที่เหมาะสมต่อการนำไปประยุกต์ใช้งาน แต่การกำหนดความต้องการจากแบบรูปและการใช้ซ้ำส่วนใหญ่ยังเป็นการคัดลอกและวาง [5] เพราะฉะนั้นงานวิจัย [6] จึงสร้างไวยากรณ์จากแบบรูปความมั่นคงอันเป็นพื้นฐานของเครื่องมือสำหรับกำหนดความต้องการ อย่างไรก็ตามความต้องการที่สามารถทวนสอบความคล้อยตามไปยังมาตรฐานของดับเบิ้ลยูสามซียังเป็นสิ่งที่ท้าทาย

ดังนั้นงานวิทยานิพนธ์นี้จึงมีวัตถุประสงค์เพื่อวิเคราะห์ประเด็นปัญหาและรวบรวมผลเฉลยจากเอกสารดับเบิ้ลยูเอสซียูไอให้อยู่ในรูปแบบของแบบรูปบริบทความมั่นคงเชิงเว็บ และสร้างไวยากรณ์ความมั่นคงสำหรับพัฒนาเครื่องมือระบุความต้องการความมั่นคงเพื่อสนับสนุนการออกแบบและพัฒนาตัวแทนผู้ใช้เว็บให้สอดคล้องกับเอกสารดับเบิ้ลยูเอสซียูไอ

1.2 วัตถุประสงค์ของงานวิจัย

1) เพื่อวิเคราะห์ประเด็นปัญหาและรวบรวมผลเฉลยเพื่อสร้างแบบรูปบริบทความมั่นคงเชิงเว็บจากเอกสารเอกสารดับเบิ้ลยูเอสซียูไอ

2) เพื่อสร้างไวยากรณ์ความมั่นคงสำหรับกำหนดความต้องการความมั่นคงของตัวแทนผู้ใช้เว็บจากแบบรูปบริบทความมั่นคงเชิงเว็บที่สอดคล้องตามเอกสารดับเบิ้ลยูเอสซียูไอ

3) เพื่อสร้างเครื่องมือโดยนำไวยากรณ์ความมั่นคงที่ได้มาประยุกต์ใช้ในการระบุความต้องการความมั่นคงสำหรับตัวแทนผู้ใช้เว็บ

1.3 ขอบเขตของงานวิจัย

1) การวิจัยนี้กล่าวถึงเอกสารดับเบิ้ลยูเอสซียูไอ โดยเนื้อหาที่จะนำมาวิเคราะห์สร้างไวยากรณ์จากบทที่ 5-7 ของเอกสารดังกล่าว มีหัวข้อดังนี้

เอกสารดับเบิ้ลยูเอสซียูไอบทที่ 5 การนำการรักษาความมั่นคงชั้นขนส่งมาประยุกต์ใช้กับเว็บ

(1) การจัดการและสารสนเทศของใบรับรอง

(2) ประเภทของการรักษาความมั่นคงชั้นขนส่ง

(3) เนื้อหาผสม

(4) เงื่อนไขข้อผิดพลาด

เอกสารดับเบิ้ลยูเอสซียูไอบทที่ 6 ตัวชี้บอกและการมีปฏิสัมพันธ์

(1) การส่งสัญญาณอัตลักษณ์และจุดตรึงที่ไววางใจ

(2) สารสนเทศบริบทความมั่นคงเพิ่มเติม

(3) ตัวชี้บอกการรักษาความมั่นคงชั้นขนส่ง

(4) การจัดการข้อผิดพลาดและการส่งสัญญาณ

เอกสารดับเบิ้ลยูเอสซียูไอบทที่ 7 แนวทางที่ดีที่สุดสำหรับสภาพทนทาน

(1) การรักษาโครมด้านความมั่นคงให้ปรากฏเสมอ

(2) พึงระวังไม่ให้เนื้อหาเว็บผสมกันกับตัวชี้บอกความมั่นคง

(3) การจัดการกับความสนใจของผู้ใช้

(4) ส่วนต่อประสานโปรแกรมประยุกต์ที่เผยให้แก่เนื้อหาเว็บ

เอกสารดับเบิ้ลยูเอสซียูไอบทที่ 8 ข้อคำนึงด้านความมั่นคง

(1) การโจมตีอย่างว่องไวในขณะเริ่มต้นการมีปฏิสัมพันธ์ด้านการรักษาความมั่นคงชั้นขนส่ง

(2) ความล้มเหลวในการตรวจสอบสถานะใบรับรอง

(3) ใบรับรองยืนยันเพียงอัตลักษณ์ไม่ใช่ความมั่นคง

(4) การใช้ชื่อภาษาธรรมชาติรวมอยู่ในชื่อโดเมน

(5) ความล้าต่อการแจ้งเตือน

(6) การผสมระหว่างใบรับรองที่ได้รับประกันเสริมใบรับรองและใบรับรองที่ผ่านการตรวจสอบความสมเหตุสมผล

(7) เนื้อหาเว็บแบบพลวัตอาจเปลี่ยนแปลงคุณสมบัติด้านความมั่นคง

2) ไวยากรณ์ความมั่นคงที่สร้างอยู่ในรูปแบบอีบีเอ็นเอฟ

3) ไวยากรณ์ความมั่นคงสำหรับระบุความต้องการความมั่นคงเป็นภาษาอังกฤษเท่านั้น

1.4 ขั้นตอนการดำเนินงานวิจัย

1) ระบุที่มาและความสำคัญของงานวิจัย

2) ศึกษาทฤษฎี องค์ความรู้ และงานวิจัยที่เกี่ยวข้อง

3) วิเคราะห์โครงสร้างของเอกสารดับเบิ้ลยูเอสซียูไอ

4) สร้าง ประเมิน และปรับปรุงแบบรูปบริบทความมั่นคงเชิงเว็บ

5) สร้าง ประเมิน และปรับปรุงไวยากรณ์ความมั่นคง

6) พัฒนาเครื่องมือต้นแบบสำหรับกำหนดความต้องการความมั่นคงการจากไวยากรณ์

7) ทดสอบและวัดระดับความพึงพอใจของผู้ใช้ที่มีต่อเครื่องมือ

8) สรุปผลงานวิจัย

9) ตีพิมพ์และเผยแพร่ผลงานทางวิชาการสู่สาธารณะชน

10) จัดทำวิทยานิพนธ์

1.5 ประโยชน์ของงานวิจัย

1) แบบรูปบริบทความมั่นคงเชิงเว็บที่นำเสนอประกอบด้วยเนื้อหาจากการรวบรวมประเด็นปัญหาและผลเฉลยจากเอกสารดับเบิ้ลยูเอสซียูไอที่อยู่ในรูปแบบที่ง่ายต่อการศึกษา

2) งานวิจัยได้สร้างไวยากรณ์ความมั่นคงสำหรับสร้างเครื่องมือระบุความต้องการความมั่นคงของตัวแทนผู้ใช้เว็บ

3) เครื่องมือต้นแบบที่พัฒนาขึ้นจากไวยากรณ์ความมั่นคงสำหรับสนับสนุนการระบุความต้องการความมั่นคงของตัวแทนผู้ใช้เว็บให้สอดคล้องกับเอกสารดับเบิ้ลยูเอสซียูไอ

1.6 โครงสร้างของเนื้อหาในวิทยานิพนธ์

วิทยานิพนธ์ฉบับนี้มีโครงสร้างของเนื้อหาแบ่งออกเป็น 8 บทดังนี้

บทที่ 1 กล่าวถึงที่มาและความสำคัญของปัญหา วัตถุประสงค์ ขอบเขต ขั้นตอน และประโยชน์ของงานวิจัย

บทที่ 2 กล่าวถึง ทฤษฎี องค์ความรู้ และงานวิจัยที่เกี่ยวข้อง

บทที่ 3 กล่าวถึงรายละเอียดการสร้างแบบรูปบริบทความมั่นคงและไวยากรณ์ความมั่นคง

บทที่ 4 กล่าวถึงการประเมินแบบรูปบริบทความมั่นคงเชิงเว็บที่นำเสนอด้วยการทดลองและบันทึกผล พร้อมทั้งปรับปรุงแบบรูปตามคำแนะนำจากผู้เชี่ยวชาญด้านความมั่นคง

บทที่ 5 กล่าวถึงการประยุกต์ใช้ไวยากรณ์ความมั่นคงโดยใช้กรณีศึกษาและแสดงเส้นทางการการได้มาซึ่งรายการความต้องการโดยต้นไม้ความมั่นคง

บทที่ 6 กล่าวถึงการออกแบบและพัฒนาเครื่องมือต้นแบบพื้นฐานไวยากรณ์ความมั่นคงที่สนับสนุนการระบุความต้องการความมั่นคง

บทที่ 7 กล่าวถึงการประเมินผลลัพธ์ที่ได้จากเครื่องมือโดยเปรียบเทียบความต้องการที่ผู้ใช้ระบุด้วยมือและความต้องการที่ระบุโดยเครื่องมือ

บทที่ 8 กล่าวถึงบทสรุปของงานวิจัย ข้อจำกัดของงาน แนวการต่อยอดงานวิจัย และบทความวิชาการที่ได้รับการตีพิมพ์

บทที่ 2
ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

งานวิทยานิพนธ์ได้ศึกษาหลักการที่เกี่ยวข้องกับวิศวกรรมความต้องการซอฟต์แวร์เพื่อให้ได้มาซึ่งข้อระบุความต้องการที่สอดคล้องกับเอกสารคำแนะนำด้านความมั่นคงของระบบ โดยรวบรวมผลเฉลยในรูปแบบของแบบรูปความมั่นคง และสร้างไวยากรณ์จากแบบรูปดังกล่าวเพื่อประยุกต์ใช้ในเครื่องมือสนับสนุนแนวความคิดดังกล่าว

ทฤษฎีที่เกี่ยวข้องอันประกอบด้วยวิศวกรรมความต้องการซอฟต์แวร์ (Software Requirements Engineering) โดยเฉพาะวิศวกรรมความมั่นคงและความต้องการด้านความมั่นคง (Security Engineering and Security Requirements) พิจารณาองค์ความรู้จากเอกสารบริบทความมั่นคงเชิงเว็บ: คำแนะนำส่วนต่อประสานผู้ใช้ (Web Security Context: User Interface Guidelines) แบบรูปความมั่นคง (Security Patterns) และอีบีเอ็นเอฟ (Extended Backus-Naur Form: EBNF) ซึ่งต่อยอดจากบีเอ็นเอฟ (Backus-Naur Form: BNF)

นอกจากนี้จะกล่าวถึงงานวิจัยที่เกี่ยวข้อง ได้แก่ การกำหนดความต้องการความมั่นคงโดยใช้ไวยากรณ์ของแบบรูปความมั่นคง (Defining Security Requirements Using Grammar of Security Pattern) แบบรูปความมั่นคงความเข้าใจถึงศาสตร์เบื้องหลังศิลปะแห่งการเขียนแบบรูป (Security Requirements Patterns: Understanding the Science Behind the Art of Pattern Writing) และการจัดการแบบรูป (Organizing Security Patterns) โดยมีเนื้อหาดังนี้

2.1 ทฤษฎีและองค์ความรู้ที่เกี่ยวข้อง

2.1.1 วิศวกรรมความต้องการซอฟต์แวร์ (Software Requirements Engineering)

วิศวกรรมความต้องการซอฟต์แวร์เป็นส่วนหนึ่งของวิศวกรรมซอฟต์แวร์ ถูกกำหนดขึ้นในช่วงการเริ่มต้นของกระบวนการพัฒนาซอฟต์แวร์ โดยมีจุดหมายในการให้ได้มาซึ่งความต้องการด้านซอฟต์แวร์ที่ถูกต้อง และชัดเจนเพื่อนำไปใช้ในการการกำหนดระบบที่จะทำการพัฒนา โดยมีกระบวนการสำคัญ [7, 8] ดังนี้

1) การเก็บรวบรวมความต้องการ (Requirements Elicitation) เป็นกระบวนการที่คำนึงถึงความต้องการของระบบว่าได้มาอย่างไร และจากแหล่งใด โดยมีจุดประสงค์ในการเก็บข้อมูลเพื่อที่จะนำไปใช้ในการกำหนดหน้าที่ของระบบ

2) การวิเคราะห์ความต้องการ (Requirements Analysis) เป็นกระบวนการวิเคราะห์ความต้องการโดยคำนึงถึงผู้ที่เกี่ยวข้องกับระบบ หน้าที่การทำงานของระบบ รวมไปถึงสภาวะแวดล้อมของการใช้งานระบบ

3) การจัดทำข้อกำหนดความต้องการ (Requirements Specification) เป็นกระบวนการในการจัดทำเอกสารที่ระบุข้อกำหนดของระบบ ในรายละเอียดของระบบที่จะพัฒนาขึ้น ซึ่งเป็นผลลัพธ์ที่สำคัญที่ได้จากกระบวนการวิศวกรรมความต้องการซอฟต์แวร์

4) การตรวจสอบความสมเหตุสมผลความต้องการ (Requirements Validation) เป็นกระบวนการตรวจสอบ และทวนสอบความถูกต้องของความต้องการที่เก็บมาว่าสามารถเข้าใจได้ มีความสอดคล้อง ครบถ้วน เป็นไปตามมาตรฐาน และความต้องการของผู้ใช้หรือไม่

5) การจัดการความต้องการ (Requirements Management) เป็นการบริหารกระบวนการวิศวกรรมความต้องการซอฟต์แวร์ ควบคุม ดูแลคุณภาพและความถูกต้องของความต้องการ การผลิตความต้องการ ตลอดจนการบริหารความต้องการที่มีการเปลี่ยนแปลง (Requirements Change)

กระบวนการวิศวกรรมความต้องการซอฟต์แวร์เป็นกระบวนการหนึ่งที่มีความสำคัญในการพัฒนาซอฟต์แวร์ ความผิดพลาดหรือความไม่สมบูรณ์ที่เกิดในกระบวนการนี้มักก่อให้เกิดค่าใช้จ่ายที่สูงกว่าผลของ ความผิดพลาดที่เกิดจากกระบวนการพัฒนาซอฟต์แวร์ในส่วนอื่นๆ และมีความเกี่ยวข้องสัมพันธ์กับผู้ใช้หรือผู้พัฒนาของระบบอย่างมาก

2.1.2 วิศวกรรมความมั่นคงและความต้องการความมั่นคง (Security Engineering and Security Requirements)

วิศวกรรมความมั่นคง [9] เป็นหลักการนำทฤษฎีความมั่นคง (Security Theory) มาใช้ในกิจกรรมความมั่นคง โดยการออกแบบและสร้างระบบที่สามารถป้องกันการโจมตีต่างๆ มีวัตถุประสงค์หลักของวิศวกรรมความมั่นคง คือ เพื่อเปลี่ยนแปลงสถานะจากอันตรายเป็นสถานะความเสี่ยงที่ยอมรับได้ ซึ่งกระบวนการที่จำเป็นในวิศวกรรมความมั่นคงมีการวนซ้ำขั้นตอนที่จำเป็น ดังแสดงภาพที่ 2.1 โดยแต่ละขั้นตอนมีรายละเอียดดังนี้

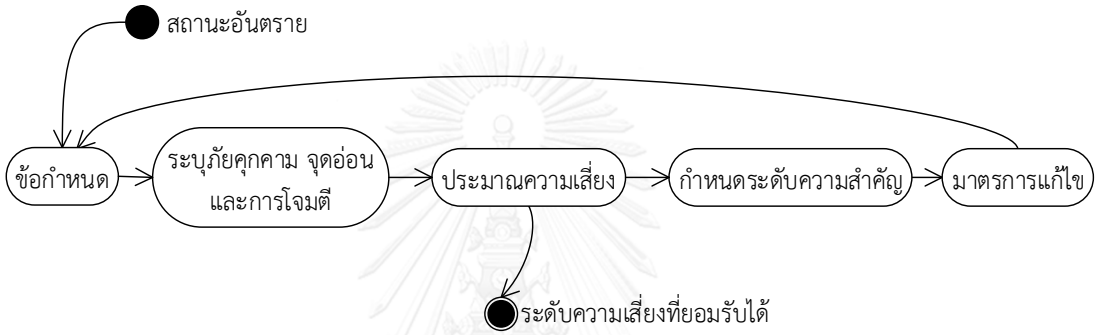
1) ข้อกำหนด (Specification) ต้องกำหนดส่วนประกอบ (Components) และส่วนต่อประสาน (Interface) ทั้งหมดให้สมบูรณ์ เพราะถ้าหากไม่ระบุให้ครอบคลุมสถาปัตยกรรมทั้งหมดของระบบจะก่อให้เกิดช่วงโหว่และถูกโจมตีในส่วนที่ยังไม่ได้ทำการระบุเป็นข้อกำหนดไว้

2) การระบุภัยคุกคาม จุดอ่อน และการโจมตี (Identification of Threats, Vulnerabilities and Attacks) เป็นการระบุภัยอันตรายและจุดอ่อนขององค์ประกอบรวมถึงส่วนต่อประสานของระบบ ซึ่งจะช่วยในการกำหนดรูปแบบการโจมตีที่จะเกิดและสามารถทำการป้องกันไว้ก่อนได้

3) ประมาณความเสี่ยง (Risk Estimation) ความเสี่ยงของการโจมตีที่อาจเกิดกับแต่ละองค์ประกอบ หรือส่วนต่อประสาน จะต้องพิจารณาตามความสัมพันธ์ระหว่างข้อกำหนดของภัยคุกคาม จุดอ่อน และรูปแบบการโจมตี

4) กำหนดระดับความสำคัญ (Prioritization) ในกรณีที่มีความเสี่ยงสูงปรากฏในจุดอ่อนที่เกี่ยวข้องกับองค์ประกอบ หรือส่วนประสาน จะต้องจัดลำดับความสำคัญไว้เป็นลำดับต้นๆ เพื่อการกำหนดมาตรการป้องกัน

5) มาตรการแก้ไข (Countermeasure) กำหนดแนวทางการแก้ไขตามภัยคุกคาม จุดอ่อน และรูปแบบการโจมตี เพื่อนำไปใช้ซ้ำในขั้นตอนการระบุข้อกำหนดเพื่อลดช่องโหว่ของระบบ



ภาพที่ 2.1 ขั้นตอนวิธีทางวิศวกรรมความมั่นคง [9]

การระบุข้อกำหนดความต้องการ (Requirements Specification) เป็นสิ่งที่สำคัญในทุกๆ โครงการ ถ้าความต้องการดังกล่าวไม่เป็นไปตามข้อกำหนดที่เหมาะสมระบบก็ไม่สามารถทำงานตามที่คาดหวังไว้ได้ เช่นเดียวกับระบบที่ต้องการความมั่นคง หากความต้องการความมั่นคงไม่ถูกกำหนดไว้อย่างเหมาะสมในช่วงแรกๆ ของการเริ่มโครงการ ความเสี่ยงและค่าใช้จ่ายก็จะเพิ่มสูงมากขึ้น และเมื่อพัฒนาผลิตภัณฑ์ไปแล้ว และปรากฏจุดอ่อนภายหลัง จะทำให้ยากต่อการแก้ไข

ความมั่นคงคือ ความสามารถในการป้องกันระบบสารสนเทศจากการขัดขวาง และการสูญเสียข้อมูล ซึ่งอาจเกิดจากการกระทำของกลุ่มผู้ก่อการร้ายข้ามชาติ หรือเหตุการณ์ที่เกิดขึ้นโดยบังเอิญ ความมั่นคงเป็นความรับผิดชอบของกลุ่มผู้พัฒนา ในการสร้างระบบใหม่ๆ นั้น ต้องมั่นใจได้ว่าความต้องการความมั่นคง (Security Requirements) ของระบบได้ถูกระบุขึ้นด้วยความระมัดระวังอย่างสมเหตุสมผลเพื่อป้องกันปัญหาที่จะเกิดขึ้น การพัฒนาความต้องการความมั่นคง โดยปกติจะเริ่มจากการประเมินมูลค่าของระบบและข้อมูล ซึ่งช่วยให้เห็นความสำคัญของระบบ ก่อให้เกิดการคำนึงถึงความเสี่ยงเสมอในระหว่างพัฒนาระบบ ความมั่นคงของระบบมักจะให้ความสำคัญกับการระบุว่าผู้ใดบ้างมีสิทธิ์เข้าถึงข้อมูล ระบุความจำเป็นในการเข้ารหัส การพิสูจน์ตัวจริง และการป้องกันไวรัสคอมพิวเตอร์

ในบริบทของเว็บหลักบริการความมั่นคง (Core Security Services: CI4A) [3] ประกอบด้วยเนื้อหาดังนี้

1) การรักษาความลับ (Confidentiality) คือ การพิจารณาควบคู่นโยบายข้อมูลส่วนบุคคลที่ถูกส่งผ่านหรือจัดเก็บภายในระบบรวมถึงสินทรัพย์ของระบบ

2) บูรณภาพ (Integrity) ความเชื่อถือได้ของข้อมูลเพื่อให้แน่ใจว่าข้อมูลที่ใช้ปราศจากการปรับเปลี่ยนแก้ไขโดยผู้ที่ไม่มีสิทธิ์

3) การพิสูจน์ตัวตน (Authentication) ระบุถึงการตรวจสอบหรือพิสูจน์บุคคล รวมถึงยืนยันว่าข้อความที่ได้รับนั้นมาจากบุคคลนั้นจริง

4) การให้อำนาจ (Authorization) มุ่งเน้นไปที่สิทธิในการเข้าถึงการทำงานและข้อมูล

5) สภาพพร้อมใช้งาน (Availability) สินทรัพย์ของระบบต้องสามารถเข้าถึงได้เมื่อถูกร้องขอโดยผู้มีสิทธ์

6) ตรวจสอบได้ (Accountability) ผู้ใช้งานระบบสามารถตรวจสอบการกระทำของตนได้ รวมถึงการห้ามปฏิเสธความรับผิดชอบ (Non-Repudiation) เพื่อป้องกันมิให้ผู้ส่งข้อมูลหรือ ผู้รับข้อมูล ปฏิเสธว่าตนไม่ได้ส่งหรือไม่ได้รับข้อมูลอิเล็กทรอนิกส์

วิศวกรรมความมั่นคงและข้อกำหนดความต้องการที่พัฒนาจากแนวทางการแก้ไขเป็นเป็นสิ่งสำคัญในการปิดจุดอ่อนที่เสี่ยงต่อการโจมตีการกำหนดความต้องการด้านความมั่นคงให้แก่ระบบ ให้ครอบคลุมทุกหลักบริการความมั่นคง

2.1.3 บริบทความมั่นคงเชิงเว็บ: คำแนะนำส่วนต่อประสานผู้ใช้ (Web Security Context: User Interface Guidelines)

กิจกรรมที่เกี่ยวข้องกับความตระหนักถึงบริบทเริ่มเกิดขึ้นตั้งแต่ปลายปี ค.ศ. 1980 นักวิจัยหลายท่านได้ใช้ความพยายามในการออกแบบและพัฒนาโครงข่าย โครงสร้างพื้นฐานของผู้ใช้ (User Infrastructure) และมิดเดิลแวร์ (Middleware) ซึ่งทำให้เกิดประสิทธิพลแก่ผู้ใช้ด้วยระบบที่ตระหนักถึงบริบท จากการศึกษางานวิจัยทำให้ทราบว่ามีผู้วิจัยจำนวนไม่น้อยให้ความสำคัญกับความตระหนักถึงบริบทของระบบ งานวิจัย [10] สำรวจงานวิจัยที่เกี่ยวข้องกับบริบทของระบบพบว่ามีงานวิจัยที่คำนึงถึงบริบทของระบบในชั้นโครงสร้างพื้นฐานผู้ใช้ (User Infrastructure Layer) ส่วนใหญ่คำนึงถึงส่วนต่อประสานกับผู้ใช้ถึง 81.3% ในขณะที่การศึกษาด้านการใช้งานยังคงมีเพียง 18.8% ทำให้ผู้วิจัยเห็นความสำคัญของการพัฒนาระบบโดยคำนึงถึงบริบทด้านการใช้งาน แต่แนวทางสำหรับการพัฒนาเว็บที่ตระหนักถึงบริบทและหลักความมั่นคง เช่น โอดับเบิ้ลยูเอเอสพี (OWASP) [11] เป็นข้อปฏิบัติเชิงเทคนิคขึ้นอยู่กับภาษาที่ใช้ในการพัฒนา ซึ่งไม่เหมาะแก่การนำมาใช้กำหนดความต้องการ เพราะจะทำให้ความต้องการที่ถูกกำหนด เกิดข้อจำกัดทางด้านเทคนิคคือสามารถพัฒนาได้เพียงภาษาใดภาษาหนึ่งเท่านั้น ดังนั้นแนวทางที่ไม่จำกัดภาษาในการพัฒนา ทั้งยังคำนึงถึงบริบทความมั่นคงโดยออกแบบส่วนต่อประสานจากการศึกษาวิธีการปฏิบัติที่เป็นเลิศด้านการใช้งาน จึงเหมาะสมในการนำมาใช้กำหนดความต้องการ

เวิลด์ไวด์เว็บคอนซอร์เทียม หรือดับเบิ้ลยูสามซี (World Wide Web Consortium: W3C) เป็นองค์กรระหว่างประเทศ ที่มีพันธกิจหลักคือ การจัดระบบมาตรฐานการใช้งานบนเวิลด์ไวด์เว็บ ทั้งการพัฒนาโพรโทคอล และวิธีการใช้งานสำหรับเวิลด์ไวด์เว็บทั้งหมด ในปี ค.ศ. 2010 ดับเบิ้ลยูสามซีได้นำเสนอบริบทความมั่นคงเชิงเว็บ: คำแนะนำส่วนต่อประสานผู้ใช้ (Web Security Context: User Interface Guidelines) หรือดับเบิ้ลยูเอสซียูไอ (WSC-UI) [2] เพื่อควบคุมและรักษาความมั่นคงและความน่าเชื่อถือในการใช้งานเว็บผ่านตัวแทนผู้ใช้ที่พัฒนาขึ้น โดยกลุ่มผลิตภัณฑ์ (Product Classes) ที่กล่าวถึงในเอกสารดับเบิ้ลยูเอสซียูไอ ประกอบด้วย ตัวแทนผู้ใช้เว็บ (Web User Agents) ส่วนขยาย (Extensions) ที่เรียกใช้การทำงานของระบบปฏิบัติการ และเทคโนโลยีอำนวยความสะดวก (Assistive Technologies) อีกนัยหนึ่งคือ เว็บเบราว์เซอร์ (Web Browser) ที่ติดตั้งปลั๊กอินส์ (Plug-ins) และส่วนขยายที่เรียกใช้การทำงานภายนอกระบบ โดยส่วนพฤติกรรมของหน้าเว็บกำหนดการแสดงผลโดยกลไกการทำงานของสคริปต์ (Script) และสไตล์ชีต (Style Sheet) ซึ่งอาจติดตั้งบนเดสก์ท็อป โทรศัพท์เคลื่อนที่ หรือเครื่องเล่นสื่อผสมก็ได้

เนื้อหาภายในเอกสารดับเบิ้ลยูเอสซียูไอ มีทั้งหมด 10 บท ส่วนที่ปรากฏข้อบังคับจะถูกนำมาวิเคราะห์ข้อกำหนด คือ บทที่ 5–8 เนื่องจากบทอื่นๆ กล่าวถึง ภาพรวม กิตติกรรมประกาศ ข้อตกลง คำอธิบาย นิยามศัพท์ และรายการอ้างอิง ส่วนที่เกี่ยวข้องกับข้อกำหนดบริบทความมั่นคง มีดังนี้

เอกสารดับเบิ้ลยูเอสซียูไอบทที่ 5 การประยุกต์ใช้การรักษาความมั่นคงชั้นขนส่งกับเว็บ (Applying TLS to the Web) การรักษาความมั่นคงชั้นขนส่งหรือเอสเอสแอล (Secure Sockets Layer: SSL) เป็นโพรโตคอลจัดการความปลอดภัยในระบบอินเทอร์เน็ตที่ใช้ในการสื่อสารข้อมูลกันระหว่างไคลเอนต์กับเซิร์ฟเวอร์ ข้อมูลจากไคลเอนต์จะถูกเข้ารหัสก่อนส่งไปที่เซิร์ฟเวอร์ รวมถึงการตรวจสอบตัวจริงของทั้งฝั่งเซิร์ฟเวอร์ผู้ให้บริการและฝั่งไคลเอนต์ผู้ใช้งาน ข้อกำหนดนี้นำประโยชน์ของเอสเอสแอลมาใช้ โดยมีหัวข้อดังนี้

1) การจัดการและสารสนเทศของใบรับรอง (Certificate Handling and Information) กำหนดเงื่อนไขในการจัดการกับใบรับรอง (Certificate) ประเภทต่างๆ ดังต่อไปนี้

(1) การยอมรับจุดตรึงที่ไว้วางใจหรือใบรับรองในเชิงโต้ตอบ (Interactively Accepting Trust Anchors or Certificates)

(2) ใบรับรองที่ได้รับการประกันเสริม (Augmented Assurance Certificates)

(3) ใบรับรองที่ผ่านการตรวจสอบความสมเหตุสมผล (Validated Certificates)

(4) ใบรับรองที่ลงนามด้วยตนเองและใบรับรองจากแหล่งที่ไม่น่าเชื่อถือ (Self-signed Certificates and Untrusted Root Certificates)

2) ประเภทของการรักษาความมั่นคงชั้นขนส่ง (Types of TLS)

3) เนื้อหาผสม (Mixed Content)

4) เงื่อนไขข้อผิดพลาด (Error conditions) โดยมีหัวข้อย่อย ดังนี้

(1) ความผิดพลาดของการรักษาความมั่นคงชั้นขนส่ง (TLS Errors)

(2) เงื่อนไขข้อผิดพลาดอิงจากบุคคลภายนอกหรือข้อมูลศึกษาสำนึก (Error Conditions based on Third Party or Heuristic Information)

(3) การส่งแบบฟอร์มไปยังผู้รับที่ไม่มั่นคง (Insecure Form Submission)

เอกสารดับเบิ้ลยูเอสซียูไอ บทที่ 6 ตัวชี้บอกและการมีปฏิสัมพันธ์ (Indicators and Interactions) การกำหนดลักษณะของสัญญาณเอกลักษณ์ เพื่อแสดงตัวชี้บอกสถานะ และการตอบโต้กับผู้ใช้โดยการแจ้งเตือนลักษณะต่างๆ มีหัวข้อดังนี้

1) การส่งสัญญาณอัตลักษณ์และจุดตรึงที่ไว้วางใจ (Identity and Trust Anchor Signaling)

(1) สัญญาณอัตลักษณ์ (Identity Signal)

(2) เนื้อหาของสัญญาณอัตลักษณ์ (Identity Signal Content)

2) สารสนเทศเชิงบริบทความมั่นคงเพิ่มเติม (Additional Security Context Information)

3) ตัวชี้บอกการรักษาความมั่นคงชั้นขนส่ง (TLS indicator)

4) การจัดการข้อผิดพลาดและการส่งสัญญาณ (Error handling and Signaling) ดังนี้

(1) ความต้องการสามัญเมื่อเกิดข้อผิดพลาดขึ้นระหว่างการมีปฏิสัมพันธ์ (Common Error Interaction Requirements)

(2) ข้อความแจ้งเตือนหรือคำเตือน (Warning/Caution Messages)

(3) ข้อความเตือนภัย (Danger Messages)

เอกสารดับเบิ้ลยูเอสซียูไอบทที่ 7 แนวทางที่ดีที่สุดสำหรับสภาพทนทาน (Robustness Best Practices) เพื่อให้ระบบมีสภาพทนทานต่อการโจมตี ระบบต้องคัดกรองลักษณะการโจมตี เพื่อหลีกเลี่ยงการกระทำของระบบที่คล้ายการโจมตี และกำหนดแนวทางที่ดีที่สุดสำหรับสภาพทนทาน โดยมีหัวข้อ ดังนี้

1) การรักษาโครมด้านความมั่นคงให้ปรากฏเสมอ (Keep Security Chrome Visible)

2) พึงระวังไม่ให้เนื้อหาเว็บผสมกันกับตัวชี้บอกความมั่นคง (Do Not Mix Content and Security Indicators)

3) การจัดการกับความสนใจของผู้ใช้ (Managing User Attention)

4) ส่วนต่อประสานโปรแกรมประยุกต์ที่เผยให้แก่เนื้อหาเว็บ (APIs Exposed to Web Content) มีหัวข้อย่อย ดังนี้

(1) การปิดบังหรือปิดใช้งานของส่วนต่อประสานผู้ใช้ด้านความมั่นคง (Obscuring or disabling Security User Interfaces)

(2) การติดตั้งซอฟต์แวร์ (Software Installation)

(3) ส่วนต่อประสานโปรแกรมประยุกต์สำหรับการคั่นหน้า (Bookmarking APIs)

(4) ส่วนต่อประสานโปรแกรมประยุกต์ของหน้าต่างแบบผุดขึ้น (Pop-up Window APIs)

เอกสารดับเบิ้ลยูเอสซียูไอบทที่ 8 ข้อคำนึงด้านความมั่นคง (Security Considerations) คำแนะนำด้านความมั่นคงที่อาจเกิดขึ้นกับระบบ

1) การโจมตีอย่างว่องไวในขณะเริ่มต้นการมีปฏิสัมพันธ์ด้านการรักษาความมั่นคงชั้นขนส่ง (Active attacks during initial TLS interactions)

2) ความล้มเหลวขณะตรวจสอบสถานะใบรับรอง (Certificate Status Checking Failures)

3) ใบรับรองยืนยันเพียงอัตลักษณ์ไม่ใช่ความมั่นคง (Certificates assure identity, not security)

4) การใช้ชื่อภาษาธรรมชาติรวมอยู่ในชื่อโดเมน (Binding "human readable" names to domain names)

5) ความล้าต่อการแจ้งเตือน (Warning Fatigue)

6) การผสมระหว่างใบรับรองที่ได้รับประกันเสริมใบรับรองและใบรับรองที่ผ่านการตรวจสอบความสมเหตุสมผล (Mixing Augmented Assurance and Validated Certificates)

7) เนื้อหาแบบพลวัตอาจเปลี่ยนแปลงคุณสมบัติด้านความมั่นคง (Dynamic content might change security properties)

เนื้อหาที่กล่าวมาข้างต้นล้วนแล้วแต่รวบรวมข้อบังคับที่ได้ระบุในเอกสารด้วยคำสงวน (Language Convention) [12] ใช้บอกระดับในการบังคับใช้ 5 ระดับ ได้แก่

(1) จำเป็นต้องปฏิบัติตาม (MUST) หมายถึง ข้อกำหนดดังกล่าวเป็นข้อบังคับ

(2) ห้ามปฏิบัติ (MUST NOT) หมายถึง ข้อกำหนดดังกล่าวเป็นข้อยกเว้นในการปฏิบัติ

(3) ควรปฏิบัติ (SHOULD) หมายถึง ข้อกำหนดดังกล่าวจะปฏิบัติตามหรือไม่ก็ได้

(4) ไม่ควรปฏิบัติ (SHOULD NOT) หมายถึง แนะนำให้หลีกเลี่ยงการปฏิบัติดังกล่าว

(5) เลือกปฏิบัติ (MAY) หมายถึง ข้อกำหนดเสริมเพื่อเพิ่มมูลค่าให้แก่ผลิตภัณฑ์

โดยคำสงวนเหล่านี้จะเป็นตัวชี้วัดระดับความคล้อยตามเอกสารดับเบิ้ลยูเอสซียูไอ ดังบทที่ 3 ข้อตกลงได้ระบุไว้ว่า ระบบใดก็ตามที่อ้างว่าได้ปฏิบัติตามข้อบังภายในเอกสารดับเบิ้ลยูเอสซียูไอแล้ว สามารถแบ่งระดับความคล้อยตาม (Conformance Level) ได้ 2 ระดับ คือ 1) ระดับพื้นฐาน (Basic Level) และ2) ระดับสูง (Advance Level) โดยระบบที่คล้อยตามระดับพื้นฐานจะต้องปฏิบัติตามทุกข้อบังคับใช้ที่ “จำเป็นต้องปฏิบัติ (MUST)” และ “ห้ามปฏิบัติ (MUST NOT)” ส่วนระบบที่คล้อยตามระดับสูงจะต้องปฏิบัติตามทุกข้อบังคับใช้ที่ “ควรปฏิบัติ (SHOULD)” และ “ไม่ควรปฏิบัติ (SHOULD NOT)”

งานวิทยานิพนธ์นำเนื้อหาจากบทที่ 5–8 ของเอกสารดับเบิ้ลยูเอสซียูไอข้างต้นมาวิเคราะห์สร้างไวยากรณ์สำหรับกำหนดความมั่นคงของตัวแทนผู้ใช้เว็บให้เป็นไปตามข้อตกลงในบทที่ 3 โดยคำสงวนดังกล่าวจะถูกมาพิจารณาในการกำกับรหัสการทวนสอบเพื่อใช้ตามรอยและประเมินความสอดคล้องของรายการความต้องการความมั่นคงที่สร้างขึ้นนอกจากนี้ยังนำกรณีศึกษาจากเอกสารดับเบิ้ลยูเอสซียูสเคส (WSC-USECASE) [13] มาประกอบการพิจารณาเพื่อเพิ่มความเข้าใจเกี่ยวกับความหมายของคำศัพท์รวมถึงข้อปฏิบัติในเอกสารข้อกำหนด

2.1.4 แบบรูปความมั่นคง (Security Patterns)

แบบรูปความมั่นคงอธิบายปัญหาด้านความมั่นคงที่มักเกิดขึ้นซ้ำๆ ในบริบทที่จำเพาะโดยนำเสนอแนวทางการแก้ไขเบื้องต้นที่สอดคล้องกันกับประเด็นปัญหา [14] เพื่อสนับสนุนการพัฒนาผลิตภัณฑ์ซอฟต์แวร์อย่างเป็นระบบ ด้วยเหตุนี้รูปแบบของแบบรูปได้ถูกพัฒนาให้มีความเหมาะสมเพื่อช่วยให้ผู้ศึกษาเข้าใจความสำคัญของแบบรูปได้โดยทันที ว่าอะไรคือปัญหาที่ระบุและผลเฉลยสะท้อนของปัญหาดังกล่าวในแบบรูป ทั้งยังให้รายละเอียดที่จำเป็นต่อการนำไปพัฒนาระบบรวมถึงประโยชน์ที่คาดว่าจะได้รับจากการประยุกต์ใช้แบบรูป รูปแบบของแบบรูปความมั่นคงที่นำเสนอโดย M. Schumacher [14] ใช้รูปแบบโพซ่าวัน (Pattern-Oriented Software Architecture series 1: POSA1) [15] เป็นแม่แบบที่ประสบความสำเร็จในด้านสถาปัตยกรรมซอฟต์แวร์ ซึ่งประกอบด้วยองค์ประกอบสำคัญที่เผยคุณลักษณะของแบบรูปความมั่นคง ได้แก่ ชื่อ (Name) เป็นที่รู้จักในนาม (Also Known As) ตัวอย่าง (Example) บริบท (Context) ประเด็นปัญหา (Problem) ผลเฉลย (Solution) โครงสร้าง (Structure) พลวัตร (Dynamics) การพัฒนา (Implementation) ตัวอย่างที่ได้รับการแก้ไข (Example Resolved) ทางเลือก (Variants) การนำไปใช้ (Known Uses) ผลที่ได้รับ (Consequences) และข้อมูลเพิ่มเติม (See Also) มีคำอธิบายดังนี้

1) ชื่อ (Name) ชื่อหรือคำอธิบายโดยย่อของแบบรูป

2) เป็นที่รู้จักในนาม (Also Known As) หากมีชื่อเรียกอื่นๆ ของแบบรูป

3) ตัวอย่าง (Example) ตัวอย่างการอธิบายปัญหาที่เกิดขึ้นจริง และความต้องการของแบบรูปในการแสดงผลเฉลยและแนวทางการประยุกต์ใช้ ซึ่งจะช่วยให้ง่ายต่อการทำความเข้าใจ

4) บริบท (Context) สถานการณ์ที่สามารถนำแบบรูปไปประยุกต์ใช้

5) ประเด็นปัญหา (Problem) ปัญหาที่ถูกระบุในแบบรูปรวมถึงการอภิปรายแรงผลักดันที่ทำให้เกิดแบบรูป

6) ผลเฉลย (Solution) หลักการและข้อปฏิบัติของผลเฉลยที่นำมารวบรวมไว้ในแบบรูป

7) โครงสร้าง (Structure) ข้อระบุที่ลงรายละเอียดในมุมมองของโครงสร้างของแบบรูปโดยใช้สัญกรที่เหมาะสม

8) พลวัตร (Dynamics) สถานการณ์จำลองทั่วไปที่ใช้อธิบายพฤติกรรมขณะที่ปฏิบัติการ

9) การพัฒนา (Implementation) แนวทางสำหรับการนำแบบรูปไปพัฒนาระบบ ซึ่งเป็นเพียงคำแนะนำเท่านั้น ไม่ถือเป็นกฎบัญญัติเพื่อให้สามารถปรับใช้ในการพัฒนาระบบให้ตรงความต้องการ

10) ตัวอย่างที่ได้รับการแก้ไข (Example Resolved) อภิปรายผลการแก้ไขที่สอดคล้องกับตัวอย่างโดยใช้แบบรูป

11) ทางเลือก (Variants) คำอธิบายโดยย่อของทางเลือกหรือการนำไปใช้แบบจำเพาะ

12) การนำไปใช้ (Known Uses) ตัวอย่างการนำแบบรูปไปประยุกต์ใช้ในระบบจริง

13) ผลที่ได้รับ (Consequences) ประโยชน์ที่ได้รับจากการประยุกต์ใช้แบบรูป

14) ข้อมูลเพิ่มเติม (See Also) การอ้างอิงถึงแบบรูปที่แก้ปัญหาที่คล้ายคลึงกัน รวมถึงข้อมูลที่ใช้ประกอบการอธิบายแบบรูปเพื่อศึกษาเพิ่มเติม

การเขียนแบบรูปเป็นสิ่งที่ยากในการบรรลุการรวบรวมข้อมูลและผ่านการตรวจทานและแก้ไขโดยผู้เชี่ยวชาญอย่างเป็นวัฏจักร

งานวิทยานิพนธ์นำเสนอแบบรูปบริบทความมั่นคงโดยใช้โพซ่าวัน (POSA1) เป็นแม่แบบซึ่งมีองค์ประกอบ คือ ชื่อของแบบรูป คำอธิบาย บริบทการนำไปใช้ ตัวอย่างปัญหา ประเด็นปัญหา การรวบรวมผลเฉลย ตัวอย่างที่ได้รับการแก้ไข ประโยชน์ที่ได้ ไปจนถึงการอ้างอิงเนื้อหาที่เกี่ยวข้อง ซึ่งองค์ประกอบดังกล่าวเหมาะสมต่อนำไปประยุกต์ใช้เป็นรูปแบบในการนำเสนอแบบรูป

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

อีบีเอ็นเอฟ [16] มีวัตถุประสงค์เพื่อเป็นสัญลักษณ์ทางการในการอธิบายไวยากรณ์ที่ไม่พึงบริบท (Context-free Grammar) ถูกนำเสนอเป็นครั้งแรกโดย John Backus ต่อมา Peter Naur ได้ปรับปรุง BNF จนได้รับความนิยมใช้จากผู้แต่งหนังสือภาษาโปรแกรม เพื่อระบุไวยากรณ์ของการโปรแกรมคอมพิวเตอร์ หลังจากนั้น Niklaus Wirth ได้นำเสนอ อีบีเอ็นเอฟ (Extended Backus-Naur Form: ENBF) ซึ่งลดความกำกวมของการใช้สัญลักษณ์ ‘<’ ‘>’ ‘|’ ‘::=’ และการวนซ้ำ (Repetition) ทำให้ใช้งานได้ง่ายขึ้น จนในที่สุดองค์การมาตรฐานสากลไอเอสโอ (International ISO) หมายเลข 14977 [17] กำหนดให้อีบีเอ็นเอฟเป็นข้อมูลอธิบายภาษาโดยพัฒนาต่อยอดมาจากบีเอ็นเอฟเดิม ในปี ค.ศ. 1977 โดยมีกฎทั่วไปดังนี้

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

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

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

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

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

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

7) ทุกกฎที่ถูกนำเสนอจะต้องแสดงใช้เครื่องหมายมหัพภาค (.) เพื่อแสดงการสิ้นสุดของกฎเสมอ

8) กรณีที่ต้องการยกเว้น (Except) ใช้เครื่องหมาย ‘-’

ตัวอย่างการใช้ภาษาอีบีเอ็นเอฟ

- ไวยากรณ์

Letter = ["A" | "B" | "C" | "D" | "E" | "F" | "G" | "H" | "I" | "J" | "K" | "L" | "M" | "N" | "O" | "P" | "Q" | "R" | "S" | "T" | "U" | "V" | "W" | "X" | "Y" | "Z"] ;

Name = [{Letter} | ? User put the researcher name ?] ;

Researcher = Name , " the researcher." ; *Name of researcher*

- ตัวอย่างผลลัพธ์

Letter: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Name: PATTARIYA

Researcher: PATTARIYA the researcher.

2.2 งานวิจัยที่เกี่ยวข้อง

2.2.1 การกำหนดความต้องการความมั่นคงโดยใช้ไวยากรณ์ของแบบรูปความมั่นคง (Defining Security Requirements Using Grammar of Security Pattern)

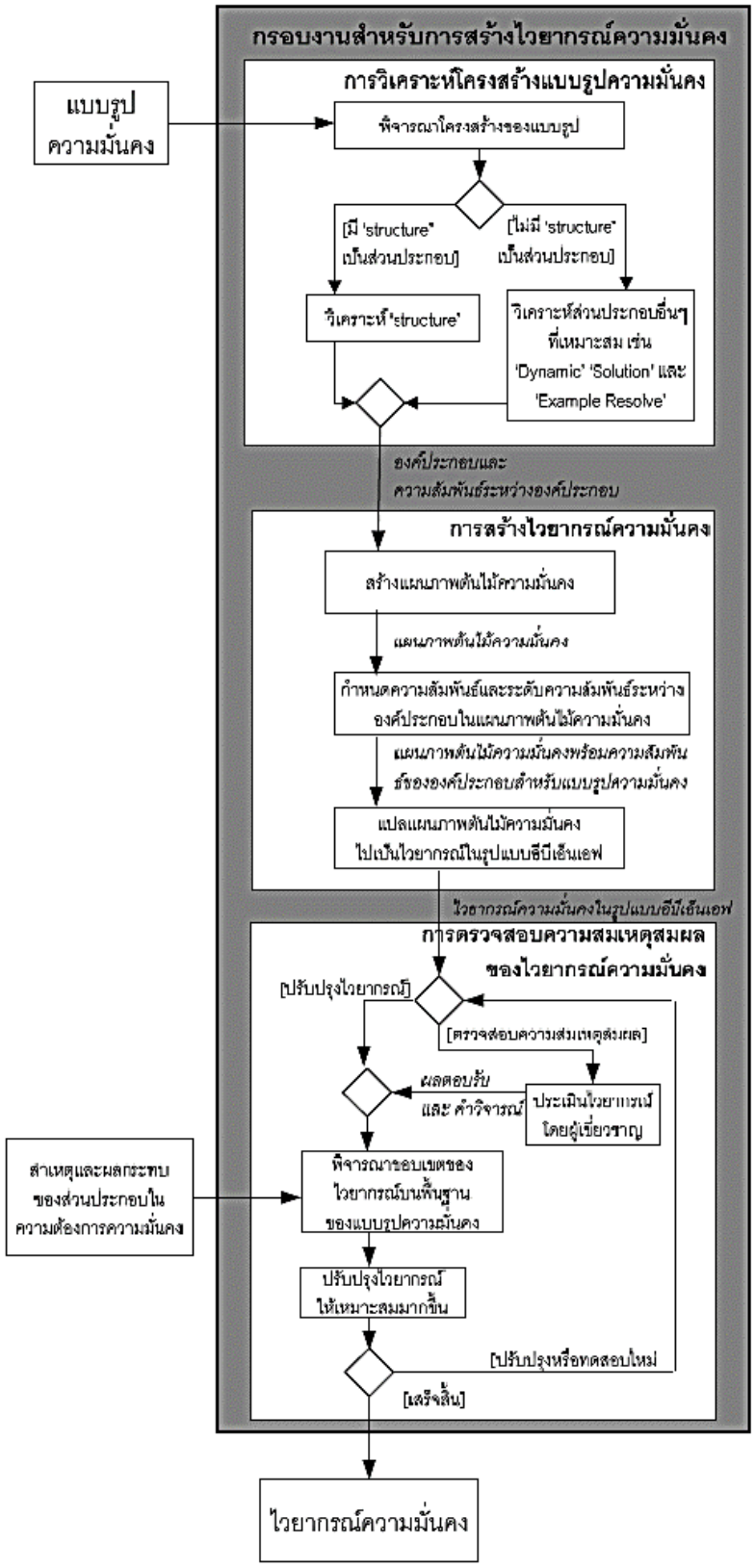
งานวิจัยนี้ [6] นำเสนอไวยากรณ์ความมั่นคงและเครื่องมือที่นำไวยากรณ์ที่ได้มาประยุกต์ใช้เพื่อกำหนดความต้องการด้านความมั่นคง โดยการสร้างแผนภาพต้นไม้ความมั่นคง ก่อนจะแปลงเป็นไวยากรณ์อีบีเอ็นเอฟตามแบบรูปความมั่นคงของ M. shumacher [9] เนื่องจากรูปแบบที่นำเสนอในลักษณะอีบีเอ็นเอฟนั้นเหมาะสำหรับผู้ที่รู้จักและเข้าใจอีบีเอ็นเอฟเท่านั้น ดังนั้นในงานวิจัยนี้จึงได้นำเสนอเครื่องมือสำหรับกำหนดความต้องการความมั่นคง กรอบงานสำหรับสร้างไวยากรณ์ความมั่นคงจากแบบรูปความมั่นคง [18] ดังแสดงในภาพที่ 2.2 แบ่งเป็น 3 ขั้นตอน ดังนี้

1) การวิเคราะห์โครงสร้างแบบรูปความมั่นคง แสดงองค์ประกอบและความสัมพันธ์ระหว่างองค์ประกอบภายใต้ขอบเขตของแบบรูปความมั่นคง โดยการวิเคราะห์โครงสร้างของแบบรูปที่ชื่อ “Structure” ซึ่งแสดงโครงสร้างแบบรูปความมั่นคงด้วยแผนภาพคลาส (Class Diagram) “Dynamic” ซึ่งแสดงพฤติกรรมของแบบรูปเพื่อนำไปใช้ โดยแสดงด้วยแผนภาพลำดับ (Sequence Diagram) และ“Example Resolved” ซึ่งแสดงตัวอย่างการนำแบบรูปไปใช้ ผลลัพธ์จากขั้นตอนนี้จะได้องค์ประกอบสำคัญ และความสัมพันธ์ระหว่างองค์ประกอบภายในแบบรูปความมั่นคง

2) การสร้างไวยากรณ์ความมั่นคง จากความสัมพันธ์ที่ได้ในขั้นตอนก่อนหน้า สร้างเป็นแผนภาพต้นไม้ เพื่อใช้เป็นตัวกลาง ในการตรวจสอบความสอดคล้องระหว่างแบบรูปความมั่นคงและไวยากรณ์ความมั่นคง และใช้ในการแปลงไปเป็นอีบีเอ็นเอฟต่อไป

3) การตรวจสอบความสมเหตุสมผลของไวยากรณ์ เพื่อปรับปรุงไวยากรณ์ให้เหมาะสมมากขึ้น โดยการพิจารณาแยกส่วนที่ซ้ำซ้อนกันขององค์ประกอบของไวยากรณ์ หรือการบูรณาการไวยากรณ์เข้าด้วยกัน และเพื่อประเมินระดับความพึงพอใจของผู้เชี่ยวชาญด้านความมั่นคง

งานวิทยานิพนธ์จะนำกรอบงานสำหรับการสร้างไวยากรณ์ความมั่นคง มาประยุกต์ใช้ในการสร้างไวยากรณ์สำหรับข้อกำหนดความมั่นคง อย่างไรก็ตาม ในขั้นตอนแรกของกรอบงานสำหรับสร้างไวยากรณ์ ยังมีข้อจำกัดในการวิเคราะห์โครงสร้าง เนื่องจากข้อมูลนำเข้าที่ใช้งานวิจัยนี้ คือ แบบรูป ซึ่งแตกต่างจากข้อมูลนำเข้าที่เป็นเอกสารข้อกำหนดดับเบิ้ลยูเอสซียูไอ ส่วนประกอบของงานวิจัยที่มีความคล้ายกับข้อมูลนำเข้าของวิทยานิพนธ์ คือ ส่วนประกอบตัวอย่างการนำแบบรูปไปใช้ (Example Resolve) ที่เป็นข้อความหรือภาษาธรรมชาติ ซึ่งงานวิทยานิพนธ์นี้ นำเสนอส่วนประกอบเพิ่มเติมเพื่อให้เหมาะสมกับข้อมูล โดยทำเอกสารนำเข้าให้อยู่ในรูปแบบของแบบรูปก่อนนำไปสร้างไวยากรณ์



ภาพที่ 2.2 กรอบงานการสร้างไวยากรณ์ความมั่นคง [18]

2.2.2 แบบรูปความต้องการความมั่นคง: ความเข้าใจถึงศาสตร์เบื้องหลังศิลปะแห่งการเขียนแบบรูป (Security Requirements Patterns: Understanding The Science Behind The Art of Pattern Writing)

แบบรูปความมั่นคงมีวัตถุประสงค์เพื่อรวบรวมผลเฉลยที่เกี่ยวข้องกับความต้องการ ที่ได้รวบรวมจากแนวปฏิบัติหรือวิธีที่เกี่ยวข้องความมั่นคง ก่อให้เกิดประโยชน์ในการใช้ซ้ำ กิจกรรมหรือกระบวนการในการสร้างแบบรูป [19] เริ่มจากการกำหนดที่มาขององค์ความรู้ (Knowledge Sources) วิธีการการสังเคราะห์องค์ความรู้และระบุแบบรูป (Knowledge Synthesis and Pattern Identification) การนำเสนอแบบรูป (Pattern Representation) การปรับปรุงแบบรูป (Pattern Refinement) และสุดท้ายการประยุกต์ใช้แบบรูป (Pattern Application) กิจกรรมดังกล่าวขึ้นอยู่กับขึ้นอยู่กับบริบทของปัญหา

งานวิจัยนี้ได้นำเสนอแบบรูปในการรวบรวมแนวปฏิบัติโดยคำนึงถึงการประยุกต์ใช้แบบรูปในการกำหนดความต้องการของระบบ

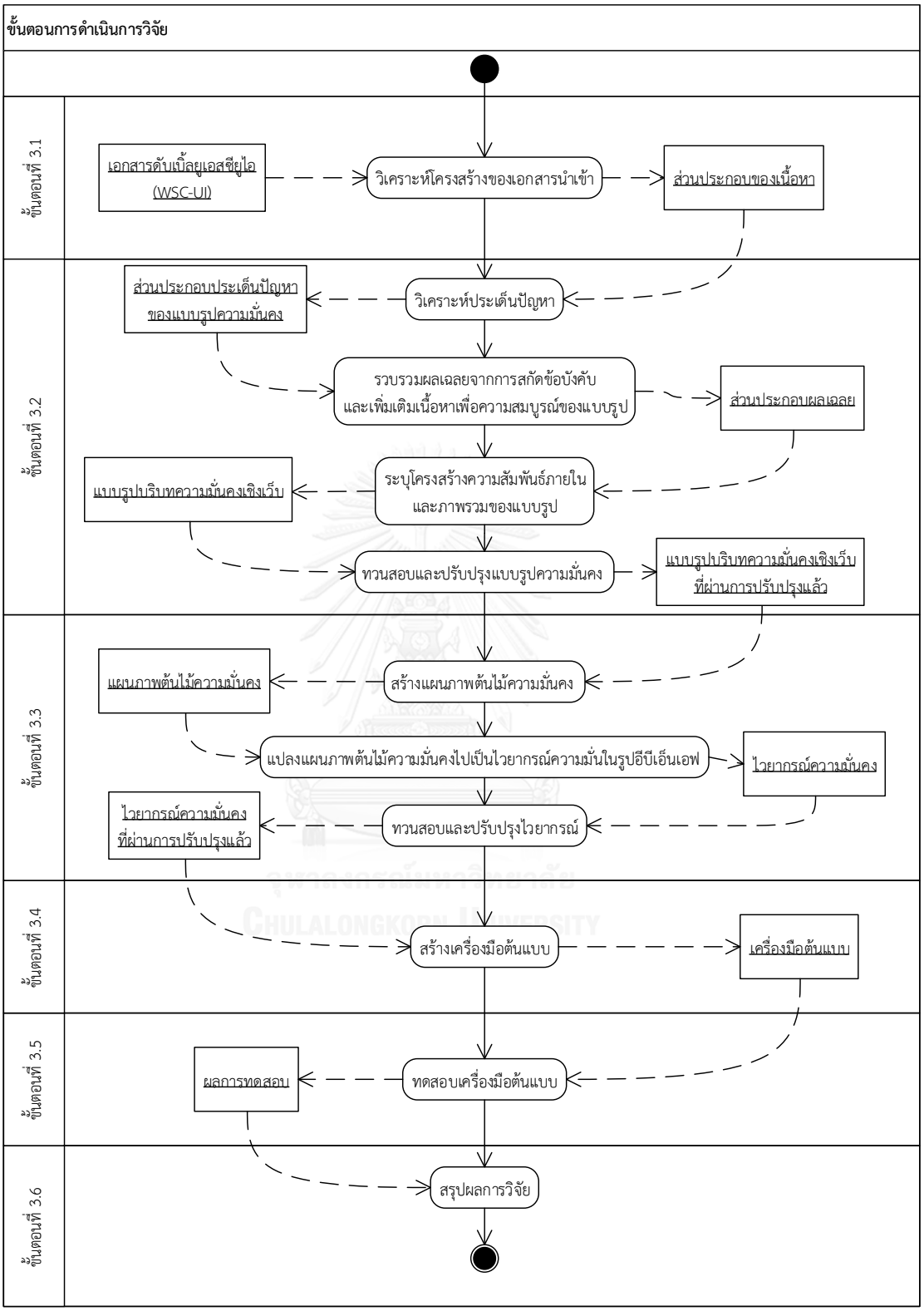
2.2.3 การจัดการแบบรูป (Organizing Security Patterns)

เพื่อให้ง่ายต่อการทำความเข้าใจภาพรวมของแบบรูป การจัดการแบบรูป (Organizing security patterns) ที่เหมาะสมจะช่วยให้ผู้นำแบบรูปไปใช้งานเข้าใจหน้าที่และความสัมพันธ์ระหว่างแบบรูป วิธีการจัดการแบบรูปที่ง่ายที่สุดทำได้โดย การระบุโดยอ้างอิงจากแนวคิดโดเมน (Domain Concepts) [20] เพื่อใช้ในการจำแนกประเภทของแบบรูป ในบริบทของเว็บหลักบริการความมั่นคง (Core Security Services) [11] ที่นิยม คือ CI4A (Confidentiality, Integrity, Authentication, Authorization, Availability, Accountability) การจำแนกดังกล่าวต้องคำนึงถึงความซ้ำซ้อนของการจัดกลุ่ม (Mutually Exclusive) รวมถึงการทำงานร่วมกันและความสัมพันธ์ระหว่างแบบรูป (Navigability) [21]

งานวิจัยนี้จะพิจารณาหลักการจัดการแบบรูปตามองค์ความรู้ด้านความมั่นคงมาจัดการกับกลุ่มของแบบรูปที่นำเสนอ เพื่อสะท้อนภาพรวมของเนื้อหาของแบบรูป

บทที่ 3
การสร้างแบบรูปบริบทความมั่นคงเชิงเว็บและไวยากรณ์ความมั่นคง

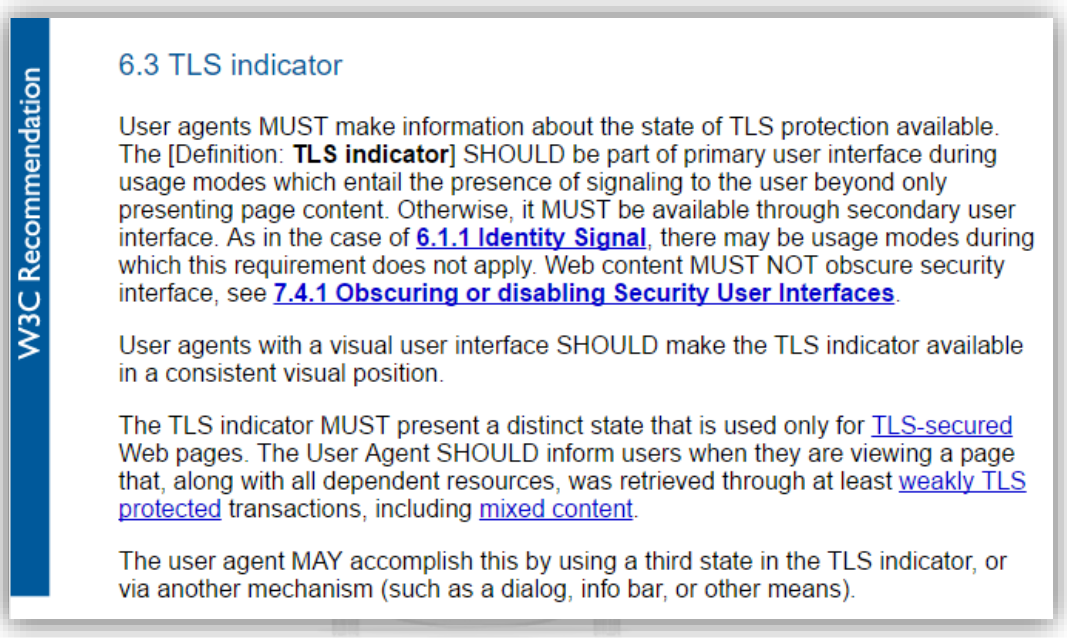
งานวิจัยนี้ มีขั้นตอนการดำเนินงานวิจัย 6 ส่วน แสดงโดยแผนภาพกิจกรรมดังภาพที่ 3.1 โดยเริ่มจากขั้นตอนที่ 3.1 การวิเคราะห์โครงสร้างของเอกสารดับเบิ้ลยูเอสซียูไอเพื่อพิจารณาส่วนประกอบของเนื้อหาในการสร้างแบบรูป สำหรับขั้นตอนที่ 3.2 วิเคราะห์ประเด็นปัญหาและรวบรวมผลเฉลยจากส่วนประกอบเนื้อหาเอกสารดับเบิ้ลยูเอสซียูไอครอบคลุมทั้ง 19 หัวข้อ ตามขอบเขตของงานวิจัย แบ่งเป็น 4 ส่วน ได้แก่ 1) การนำการรักษาความมั่นคงชั้นขนส่งมาประยุกต์ใช้กับเว็บ 2) ตัวชี้บอกและการมีปฏิสัมพันธ์ 3) แนวทางที่ดีที่สุดสำหรับสภาพทนทาน และ 4) ข้อคำนึงความมั่นคง เพื่อให้ได้มาซึ่งประเด็นปัญหาและผลเฉลยอยู่ในรูปแบบของแบบรูปบริบทความมั่นคงเชิงเว็บ แบบรูปที่ได้จะถูกนำไปทวนสอบและปรับปรุงในบทที่ 4 แล้วนำมาสร้างไวยากรณ์ความมั่นคงในขั้นตอนที่ 3.3 โดยแบ่งเป็น 2 ขั้นตอนย่อย คือ ขั้นตอนที่ 3.3.1 สร้างแผนภาพต้นไม้ความมั่นคง และขั้นตอนที่ 3.3.2 สร้างไวยากรณ์ความมั่นในรูปอีบีเอ็นเอฟ นำผลลัพธ์ไวยากรณ์ความมั่นคงจากขั้นตอนก่อนหน้ามาพิจารณาขอบเขตความมั่นคงที่เกี่ยวข้องกันและปรับปรุงไวยากรณ์ จากนั้นไวยากรณ์ความมั่นคงจะถูกนำไปยุกต์ใช้ในบทที่ 5 เพื่อนำไปสร้างและประเมินเครื่องมือต้นแบบในบทที่ 6 และ 7 ตามลำดับ และสุดท้ายสรุปผลการวิจัยในบทที่ 8 เพื่อความสะดวกในการทำความเข้าใจกระบวนการและตัวอย่างผลลัพธ์ในแต่ละขั้นตอนมีรายละเอียดดังนี้



ภาพที่ 3.1 แผนภาพกิจกรรมขั้นตอนการดำเนินการวิจัย

3.1 การวิเคราะห์โครงสร้างของเอกสารดับเบิ้ลยูเอสซียูไอ

ขั้นตอนนี้อธิบายการวิเคราะห์โครงสร้างของเอกสารดับเบิ้ลยูเอสซียูไอตามที่ได้อธิบายไว้ในบทที่ 2 เพื่อให้เข้าใจลักษณะของเอกสารนำเข้าและส่วนที่นำมาพิจารณาใช้ในการสร้างแบบรูปบริบทความมั่นคงเชิงเว็บ โดยเนื้อหาของเอกสารดับเบิ้ลยูเอสซียูไอสามารถเข้าถึงได้ผ่านหน้าเว็บซึ่งมีลักษณะดังภาพที่ 3.2 ตัวอย่างเนื้อหาบางส่วนของการนำการรักษาความมั่นคงชั้นขนส่งมาประยุกต์ใช้กับเว็บ (Applying TLS to the Web)



ภาพที่ 3.2 ตัวอย่างเนื้อหาตัวชี้บอกการรักษาความมั่นคงชั้นขนส่ง [2]

เนื้อหาเอกสารดับเบิ้ลยูเอสซียูไอที่ปรากฏผ่านหน้าเว็บดังกล่าวกำหนดการแสดงผลด้วยโครงสร้างแบบภาษากำกับข้อความ (Markup Language) โดยใช้คำสั่งป้ายระบุ (Tag) ในการแสดงผลโครงสร้างของเอกสารควบคู่กันกับลักษณะพิเศษของข้อความ คำสั่งที่นำมาวิเคราะห์โครงสร้างเพื่อสกัดเนื้อหาข้อบังคับ คำนิยาม และสถานการณ์จำลองพิจารณาได้ดังนี้

2) **ข้อบังคับ** จากข้อตกลงด้านการใช้ภาษา (Language Convention) [12] ระบุคำสงวนมีการแสดงลักษณะอักษรเป็นตัวพิมพ์ใหญ่ บ่งบอกระดับในการบังคับใช้ข้อกำหนด 5 ระดับ ได้แก่ 1) จำเป็นต้องปฏิบัติ (MUST) 2) ห้ามปฏิบัติ (MUST NOT) 3) ควรปฏิบัติ (SHOULD) 4) ไม่ควรปฏิบัติ (SHOULD NOT) และ 5) อาจเลือกปฏิบัติ (MAY)

คำสงวนดังกล่าวจะถูกมาพิจารณาในการกำกับรหัสการทวนสอบ โดยอาศัยรูปแบบคำสั่งของป้ายระบุ <span id> กำกับรหัสตำแหน่งที่ปรากฏข้อบังคับด้วยตัวเลขโรมัน “I” ดังภาพที่ 3.3 เพื่อใช้ตามรอยข้อบังคับไปยังรายการความต้องการความมั่นคงที่สร้างขึ้นได้อย่างครบถ้วน

```
<p><span id="LIX">User agents MUST make information about
the state of TLS protection available.</span> <span id=
"LX">The [<a name="tls-indicator" id="tls-indicator" title=
"">Definition</a>: <b>TLS indicator</b>] SHOULD be part of
primary user interface during usage modes which entail the
presence of signaling to the user beyond only presenting
```

ภาพที่ 3.3 รูปแบบคำสั่งในการระบุข้อบังคับของเอกสารดับเบิ้ลยูเอสซียูไอ [2]

จากการพิจารณาข้อมูลรหัสตำแหน่งที่ปรากฏข้อบังคับด้วยตัวเลขโรมันของป้ายระบุดังกล่าวพบว่า มีข้อบังคับเพียงหนึ่งรายการไม่ปรากฏรหัสกำกับ จึงต้องกำหนดรหัสการทวนสอบขึ้น การกำกับรหัสการทวนสอบจะใช้อักษรย่อแทนข้อบังคับระดับต่างๆ โดยไม่แยกระหว่างข้อปฏิบัติกับข้อห้ามเนื่องจากไม่มีผลต่อการพิจารณาระดับความสอดคล้อง จึงแบ่งรหัสการทวนสอบได้ 3 กลุ่มข้อบังคับ ดังนี้

(1) รหัสการทวนสอบขึ้นต้นด้วย “MS” แทนข้อบังคับ จำเป็นต้องปฏิบัติ (MUST) และห้ามปฏิบัติ (MUST NOT)

(2) รหัสการทวนสอบขึ้นต้นด้วย “SH” แทนข้อบังคับ ควรปฏิบัติ (SHOULD) และไม่ควรปฏิบัติ (SHOULD NOT)

(3) รหัสการทวนสอบขึ้นต้นด้วย “MY” แทนข้อบังคับ อาจเลือกปฏิบัติ (MAY)

รหัสขึ้นต้นด้วยกลุ่มข้อบังคับและตามด้วยหมายเลขลำดับของบังคับของแต่ละกลุ่ม เช่น MS01, SH01 หรือ MY01 เป็นต้น

3) **การนิยาม** (Definition) ใช้บอกความหมายของคำศัพท์ที่นิยามขึ้นใช้ภายในเอกสารดับเบิ้ลยูเอสซียูไอ การนิยามของคำศัพท์มีรูปแบบ คือ ขึ้นต้นด้วย “[Definition:” คำที่ถูกนิยามจะเป็นตัวหนา แล้วตามด้วยคำอธิบายคำศัพท์นั้น ปิดท้ายด้วย เครื่องหมาย “]” ดังภาพที่ 3.4 ซึ่งมีโครงสร้างแบบภาษากำกับข้อความ (Markup Language) ในการนิยามคำศัพท์ด้วย ดังภาพที่ 3.5

[Definition: A **Web Page** is a resource that is referenced by a URI and is not embedded in another resource, plus any other resources that are used in the rendering or intended to be rendered together with it.]

ภาพที่ 3.4 รูปแบบการนิยามคำภายในเอกสารดับเบิ้ลยูเอสซียูไอ [2]

```
<p>[<a name="def-page" id="def-page" title=
"">Definition</a>: A <b>Web Page</b> is a resource that is
referenced by a URI and is not embedded in another
resource, plus any other resources that are used in the
rendering or intended to be rendered together with it.]</p>
```

ภาพที่ 3.5 โครงสร้างภาษากำกับการนิยามคำในเอกสารดับเบิ้ลยูเอสซียูไอ [2]

4) **สถานการณ์จำลอง** (Scenarios) นอกเนื้อหาจากเอกสารดับเบิ้ลยูเอสซียูไอแล้ว สถานการณ์จำลองบางส่วนจากเอกสารดับเบิ้ลยูเอสซียูสเคส [13] จะถูกนำมาพิจารณาใช้สำหรับยกตัวอย่างสถานการณ์ ให้สอดคล้องกับประเด็นปัญหา ให้ผู้อ่านเข้าใจยิ่งขึ้น ดังภาพที่ 3.6

```
<li id="any-iip-1">
  <p><a href="https://www.w3.org/TR/wsc-usecases/#iip">Identified source, Identified
  destination, Providing</a></p>

  <p>Once a week, Alice pays her bills. She opens her web
  browser, follows the habitual bookmark to her bank's
  site, logs in by entering her credentials, and follows
  the routine course through the online banking
  system.</p>
</li>
```

ภาพที่ 3.6 สถานการณ์จำลองจากเอกสารดับเบิ้ลยูเอสซียูสเคส [13]

เนื้อหาของเอกสารที่มีลักษณะเด่นจากการโครงสร้างข้างต้น สามารถนำมาวิเคราะห์และรวบรวมสู่ผลเฉลยของแบบรูปในลำดับต่อไป ให้เหมาะสมกับจุดประสงค์ของแต่ละองค์ประกอบของแบบรูป โดยประโยคข้อบังคับจะถูกรวบรวมสู่ผลเฉลยของแบบรูป การนิยามจะถูกพิจารณาเพื่อสร้างโครงสร้างและความสัมพันธ์ภายในแบบรูป และสถานการณ์จำลองแสดงให้เห็นถึงตัวอย่างปัญหาและสะท้อนประเด็นปัญหาของแบบรูป

3.2 การสร้างแบบรูปบริบทความมั่นคงเชิงเว็บ

การสร้างแบบรูปบริบทความมั่นคงเชิงเว็บ เนื้อหาเอกสารดับเบิ้ลเอสซียูไอจะถูกวิเคราะห์ไปสู่องค์ประกอบของแบบรูปตามรูปแบบโพซ่าวัน (POSA1) ที่ได้กล่าวถึงในบทที่ 2 ซึ่ง ได้แก่ ชื่อของแบบรูป (Name) คำอธิบาย (Description) บริบทการนำไปใช้ (Context) ตัวอย่างปัญหา (Example) ประเด็นปัญหา (Problem) ผลเฉลย (Solution) ตัวอย่างที่ได้รับการแก้ไข (Example Resolved) ผลที่ได้รับ (Consequences) และข้อมูลเพิ่มเติม (See Also) นอกเหนือจากโพซ่าวันแล้ว องค์ประกอบของแบบรูปที่นำเสนอเพื่อให้เหมาะสมกับเนื้อหาของเอกสารดับเบิ้ลเอสซียูไอ คือ บทที่มาของเอกสารดับเบิ้ลเอสซียูไอ (Section) และหลัก (Core) ซึ่งการจำแนกตามหลักบริการความมั่นคงบริการความมั่นคง (Core Security Services: CI4A) ที่กล่าวไว้ในบทที่ 2 ผลลัพธ์ของแบบรูปบริบทความมั่นคงเชิงเว็บที่นำเสนอในงานวิจัยนี้ได้แสดงไว้ในภาคผนวก ก

โดยขั้นตอนสำหรับการสร้างแบบรูปบริบทความมั่นคงเชิงเว็บจากเอกสารดับเบิ้ลยูเอสซียูไอแบ่งได้เป็น 4 ขั้นตอน เริ่มจากการวิเคราะห์เนื้อหา การระบุความสัมพันธ์ขององค์ประกอบภายในการจำแนกกลุ่มหัวข้อของเนื้อหา และขั้นตอนสุดท้าย การทวนสอบผลลัพธ์ที่ได้โดยผู้เชี่ยวชาญ โดยมีรายละเอียดแต่ละขั้นตอนดังต่อไปนี้

3.2.1 การวิเคราะห์เนื้อหาเอกสารดับเบิ้ลยูเอสซียูไอเพื่อสร้างแบบรูป

การวิเคราะห์และจำแนกเนื้อหาจากเอกสารดับเบิ้ลยูเอสซียูไอไปยังแต่ละองค์ประกอบของแบบรูปมีหลักเกณฑ์ดังอธิบายในตารางที่ 3.1 ทั้งนี้เพื่อให้เห็นภาพได้ชัดเจนการนำเนื้อหาจากดับเบิ้ลยูเอสซียูไอในประเด็นเกี่ยวข้องกับการกำหนดตัวชี้บอกด้านความมั่นคง (TLS indicator) มาใช้เป็นตัวอย่างข้อมูลนำเข้าของกระบวนการ ได้ผลลัพธ์แบบรูปบริบทความมั่นคงเชิงเว็บดังตารางที่ 3.2

ตารางที่ 3.1 องค์ประกอบและการได้มาของเนื้อหาของแบบรูปบริบทความมั่นคงเชิงเว็บ

องค์ประกอบ	การได้มาของเนื้อหา
Core	ระบุหลักบริการความมั่นคง (CI4A) ได้จากขั้นตอนการระบุโครงสร้างภาพรวม
Section	หมวดของเนื้อหา (Section) จากเอกสารดับเบิ้ลยูเอสซียูไอ
ID	หัวข้อที่แบ่งโดยลำดับตัวเลข ใช้อ้างถึงหมายเลขบท (Section) ของเนื้อหาที่นำมาสร้างแบบรูป โดยเอกสารคำแนะนำมีความลึกของหัวข้อ 2 ระดับ และใช้อักษร “WSCP” (Web Security Context Pattern) นำหน้าตัวเลข เช่น หัวข้อ 6.3 เมื่อทำเป็นหมายเลขอ้างอิงจะได้ WSCP63
Name	ข้อความที่ใช้แสดงแทนเนื้อหาที่ปรากฏอยู่ภายใต้หัวข้อนั้นๆ โดยอยู่ต่อจากหมายเลขอ้างอิง เช่น TLS indicator จะถูกนำมาใช้เป็นหัวเรื่อง
Description	รายละเอียดโดยย่อของแบบรูปมีเนื้อหาเกี่ยวข้องกับเรื่องใด โดยผู้สกัดความต้องการทำการวิเคราะห์จากเนื้อหาเพื่อใส่รายละเอียดคำอธิบายภาพรวมลงในแบบรูป
Example	ยกตัวอย่างสถานการณ์ของปัญหา จากเอกสาร WSC-USECASES ในที่นี้สอดคล้องกับ CASE7
Context	วิเคราะห์สถานะของระบบที่ข้อกำหนดจะนำไปบังคับใช้
Problem	ระบุข้อปัญหาว่าแบบรูปนี้ใช้แก้ปัญหาใด ที่มาความสำคัญของแบบรูป
Solution	ข้อความที่ระบุระดับที่ควรปฏิบัติตาม ที่ใช้บอกระดับในการบังคับใช้ข้อกำหนด เช่น “The TLS indicator MUST present a distinct state” ข้อปฏิบัติดังกล่าวปรากฏคำสำคัญ “MUST” อยู่ภายในประโยค
Internal Structure	ระบุเอนทิตีและความสัมพันธ์ที่ได้จากการวิเคราะห์เนื้อหา
Example Resolved	อภิปรายสถานการณ์เมื่อปัญหาได้ถูกแก้ไขโดยใช้แบบรูป
Consequences	ประโยชน์ที่ได้รับจากการประยุกต์ใช้แบบรูป
See Also	เนื้อหาอื่นที่ปรากฏ หรือถูกอ้างถึงในภายในข้อกำหนดนี้ คำหรือกลุ่มคำที่เป็น Hyperlink ดังข้อความ “See 7.4.1 Obscuring or disabling Security User Interfaces.”

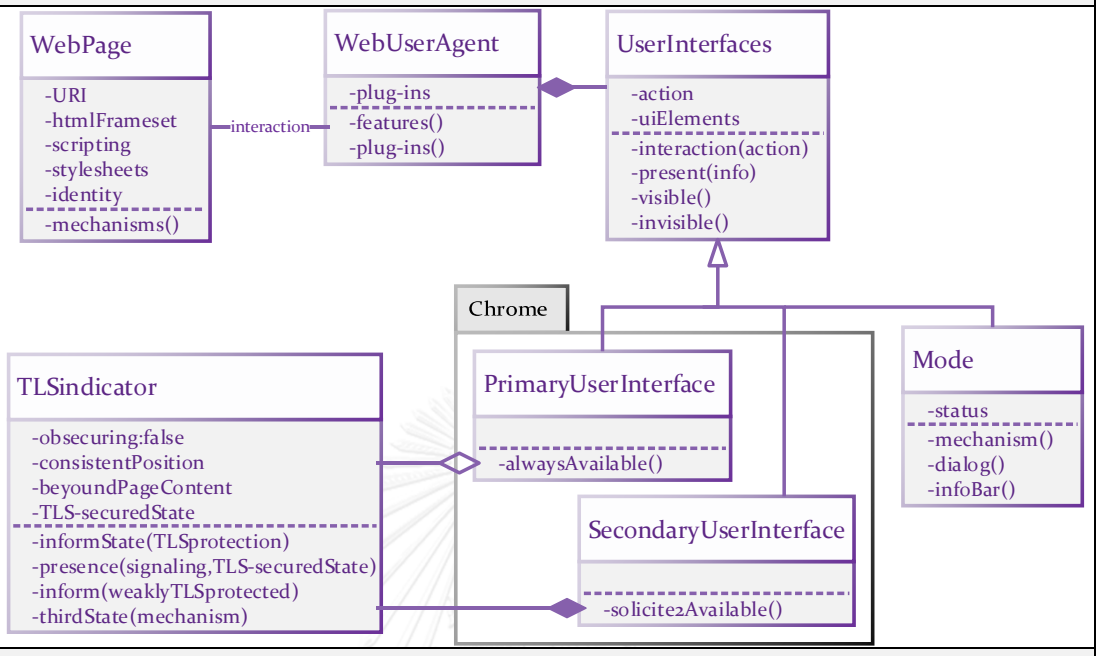
ตารางที่ 3.2 แบบรูปตัวชี้บอกความมั่นคงชั้นขนส่ง

Name	ตัวชี้บอกความมั่นคงชั้นขนส่ง	**ID**	WSCP63
Core	Availability	**Section**	Indicators and Interactions
Description			
แบบรูปนี้กล่าวถึงคุณลักษณะของตัวชี้บอกความมั่นคงชั้นขนส่งที่ใช้ในการแสดงข้อมูลเกี่ยวกับสถานะของการป้องกันการรักษาความมั่นคงชั้นขนส่งหรือสารสนเทศทางบริบทความมั่นคงของผู้บริการให้แก่ผู้ใช้ได้ทราบ			
Example			
กรณี 7 บริษัท Example Inc. มีบริการออนไลน์ที่ได้รับความนิยมและรองรับการทำรายการผ่านบัตรเครดิตมากมายในหนึ่งวัน เบ็ตตี้ใช้บริการดังกล่าวเป็นบางโอกาสและเธอเชื่อมั่นที่จะให้ข้อมูลบัตรเครดิตของเธอในการทำรายการ ในขณะที่มัลคัมมีแนวคิดที่จะโจรกรรม เขาสร้างเว็บเลียนแบบจากเว็บไซต์ของ Example และชี้นำให้ผู้ใช้เข้าสู่เว็บของเขาโดยการตั้งชื่อโดเมนของเว็บปลอมให้ใกล้เคียงกับเว็บไซต์ที่แท้จริงของ Example ดังนั้นจึงมีเหยื่อบางรายหลงเข้าสู่เว็บของเขาอย่างไม่ตั้งใจ และเบ็ตตี้เองก็กำลังป้อนข้อมูลบัตรเครดิตของเธอไปยังเว็บไซต์ที่ดูคล้ายกับเว็บของ Example			
Context			
บริบทในการนำแบบรูปนี้ไปประยุกต์ใช้เมื่อตัวแทนผู้ใช้เว็บเชื่อมต่อกับผู้ให้บริการผ่านการป้องกันการรักษาความมั่นคงชั้นขนส่งในสถานะใด ๆ			
Problem			
หากปราศจากการแจ้งเตือนเพื่อบอกสถานะเมื่อเกิดข้อผิดพลาดหรือการโจมตีระหว่างการรักษาความมั่นคงชั้นขนส่ง จะทำให้ผู้ใช้ไม่ทันระวังในการเข้าถึงเว็บไซต์ที่อาจก่อให้เกิดภัยต่อข้อมูลและระบบของผู้ใช้			
Solution			
ตัวแทนผู้ใช้เว็บจะต้องให้ข้อมูลเกี่ยวกับสถานะของการป้องกันการรักษาความมั่นคงชั้นขนส่งด้วยตัวชี้บอก อันมีคุณลักษณะดังนี้ 1. **การแสดงผล** โดยตัวชี้บอกความมั่นคงชั้นขนส่ง อาจเป็นส่วนหนึ่งของส่วนต่อประสานผู้ใช้แบบปฐมภูมิในระหว่างสถานะ (Mode, **Mode**) การใช้งานซึ่งถ่ายทอดสัญญาณให้แก่ผู้ใช้โดยแสดงอยู่ด้านบนเหนือเนื้อหาหน้าเว็บเท่านั้น มิเช่นนั้นข้อมูลดังกล่าวต้องพร้อมใช้งานผ่านทางส่วนต่อประสานผู้ใช้แบบทุติยภูมิ ตัวแทนผู้ใช้เว็บอาจทำตามข้อกำหนดนี้โดยการใช้สถานะที่สามของตัวชี้บอกความมั่นคงชั้นขนส่ง หรือโดยกลไกอื่น เช่น การใช้กล่องโต้ตอบ แถบสารสนเทศ อื่นๆ 2. **คุณภาพ** ตัวแทนผู้ใช้ที่แสดงผลผ่านส่วนต่อประสานผู้ใช้ควรจะทำให้ตัวชี้บอกความมั่นคงชั้นขนส่งพร้อมใช้งานในตำแหน่งการแสดงผลที่ต้องกัน โดยเนื้อหาเว็บจะต้องไม่คลุมเครือกับส่วนต่อประสานด้านความมั่นคงต้องกันกับแบบรูปที่ 74 3. **สถานะ** ตัวชี้บอกความมั่นคงชั้นขนส่งจะต้องแสดงสถานะความมั่นคงอย่างชัดเจนสำหรับหน้าเว็บแบบรักษาความมั่นคงชั้นขนส่งเท่านั้น ตัวแทนผู้ใช้ควรแจ้งเตือนเมื่อผู้ใช้กำลังเยี่ยมชมหน้าเว็บที่มาจากทรัพยากรพึ่งพิงทั้งหมดถูกค้นคืนผ่านช่องทางการรักษาความมั่นคงชั้นขนส่งอย่างอ่อนแอและผ่านหน้าเว็บแบบเนื้อหาผสม			

ตารางที่ 3.2 แบบรูปตัวชี้บอกความมั่นคงชั้นขนส่ง (ต่อ)

Name	ตัวชี้บอกความมั่นคงชั้นขนส่ง	ID	WSCP63

Internal Structure



Example Resolved

กรณี 7 ตัวแทนผู้ใช้เว็บแสดงตัวชี้บอกความมั่นคงชั้นขนส่งเฉพาะเมื่อเข้าถึงเว็บไซต์ที่แท้จริงของ Example เพื่อแจ้งให้กับเบ็ตตี้ได้ทราบว่าทรัพยากรของเว็บถูกค้นคืนผ่านช่องทางการรักษาความมั่นคงชั้นส่ง เบ็ตตี้ควรป้อนข้อมูลบัตรเครดิตของเธอไปยังเว็บไซต์ที่แท้จริงที่ตัวชี้บอกความมั่นคงชั้นขนส่งปรากฏเท่านั้น ในทางตรงกันข้ามหากไม่ปรากฏตัวชี้บอกดังกล่าว เบ็ตตี้จะต้องไม่ให้ข้อมูลใดๆ แก่เว็บที่ปลอมแปลง

Consequences

การแสดงผลของตัวชี้บอกที่ชัดเจนจะเตือนให้ผู้ใช้ได้ทราบถึงข้อผิดพลาดอันอาจเกิดจากการโจมตี อีกทั้งยังทำให้ผู้พิจารณาข้อมูลเพื่อใช้ตัดสินเชื่อถือหน้าเว็บดังกล่าวจากข้อมูลที่รายงานตามสถานะผ่านตัวชี้บอกที่ปรากฏให้ผู้ใช้เห็นและเข้าใจได้ทันที

See Also

- จากแบบรูป 61 ที่อาจมีโหมดการใช้งานซึ่งข้อกำหนดความต้องการนี้จะไม่ถูกนำไปใช้
- เนื้อหาของเว็บที่ทำให้ส่วนต่อประสานที่แสดงความมั่นคงมีความคลุมเครือ ศึกษาเพิ่มเติมจากแบบรูป 74
- ตัวอย่างปัญหาของแบบรูปนี้อ้างถึง Case 7 จากเอกสาร WSC-USECASES

3.2.2 การระบุความสัมพันธ์ภายในของแบบรูป

โครงสร้างและความสัมพันธ์ระหว่างเอนทิตีจะนำมาวิเคราะห์ข้อมูลสำหรับองค์ประกอบโครงสร้างภายในเนื้อหา (Internal Structure) ใช้ในการทวนสอบความสัมพันธ์ภายในเนื้อหาเพื่อให้ได้แบบรูปที่กำหนดมีต้องกัน เนื่องจากในองค์ประกอบผลเฉลยของแบบรูปจะแสดงลักษณะอักษรตัวหนาขีดเส้นเพื่อบ่งบอกถึงการกล่าวถึงเอนทิตีภายในเนื้อหาและถูกนำมาระบุในโครงสร้างภายในของแบบรูป การวิเคราะห์โครงสร้างและความสัมพันธ์ภายในเนื้อหาอธิบายโดยใช้แผนภาพคลาส จากตารางที่ 3.2 แบบรูปตัวชี้บอกความมั่นคงชั้นขนส่ง แสดงโครงสร้างและความสัมพันธ์ระหว่างเอนทิตีได้ดังองค์ประกอบโครงสร้างภายในเนื้อหา แผนภาพคลาสดังกล่าวแสดงให้เห็นความสัมพันธ์ภายในแสดงลักษณะและคุณสมบัติของ TLS-indicator และความสัมพันธ์ภายนอกแสดงโดยกลุ่มแพ็คเกจโดยกล่าวถึง Chrome ที่ระบุไว้ในแบบรูป 71 การวิเคราะห์โครงสร้างและความสัมพันธ์ดังกล่าวจะถูกนำไปทวนสอบความถูกต้องของแบบรูป

3.2.3 การระบุโครงสร้างภาพรวมของแบบรูป

โครงสร้างภาพรวม (Global Structure) เพื่อให้เห็นภาพรวมของเนื้อหาของแบบรูปโดยการจำแนกกลุ่มหัวข้อดับเบิ้ลยูเอสซียูไอตามหลักบริการความมั่นคง (Core Security Services: CI4A) จากบทที่ 2 ในบริบทของตัวแทนผู้ใช้เว็บ ได้แก่ การรักษาความลับ (Confidentiality) คือ การพิจารณาควบคู่นโยบายข้อมูลส่วนบุคคลที่ถูกส่งผ่านหรือจัดเก็บภายในระบบรวมถึงสินทรัพย์ของระบบ บูรณภาพ (Integrity) ความเชื่อถือได้ของข้อมูลเพื่อให้แน่ใจว่าข้อมูลที่ใช้ปราศจากการปรับเปลี่ยนแก้ไขโดยผู้ที่ไม่มีสิทธิ์ การพิสูจน์ตัวตน (Authentication) ระบุถึงการตรวจสอบหรือพิสูจน์บุคคล รวมถึงยืนยันว่าข้อความที่ได้รับนั้นมาจากบุคคลนั้นจริง การให้อำนาจ (Authorization) มุ่งเน้นไปที่สิทธิในการเข้าถึงการทำงานและข้อมูล สภาพพร้อมใช้งาน (Availability) สินทรัพย์ของระบบต้องสามารถเข้าถึงได้เมื่อถูกร้องขอโดยผู้มีสิทธ์ ตรวจสอบได้ (Accountability) ผู้ใช้งานระบบสามารถตรวจสอบการกระทำของตนได้ รวมถึงการห้ามปฏิเสธความรับผิดชอบ (Non-Repudiation) เพื่อป้องกันมิให้ผู้ส่งข้อมูลหรือ ผู้รับข้อมูล ปฏิเสธว่าตนไม่ได้ส่งหรือไม่ได้รับข้อมูลอิเล็กทรอนิกส์ จากหลักบริการความมั่นคงข้างต้น เนื้อหา ดับเบิ้ลยูเอสซียูไอ จำแนกตามหัวข้อได้ดังตารางที่ 3.3 ความสัมพันธ์ดังกล่าวได้จากการพิจารณาความสอดคล้องกับหลักบริการความมั่นคงของเอนทิตีที่ได้จากการวิเคราะห์องค์ประกอบภายใน ตัวอย่างเช่นจากโครงสร้างภายในเนื้อหาของแบบรูป 63 ปรากฏคุณสมบัติของ TLS indicator ที่ระบุว่าต้องสามารถเข้าถึงได้โดยผู้ใช้ตลอดเวลา จึงจัดให้แบบรูปดังกล่าวอยู่ในกลุ่มสภาพพร้อมใช้งาน (Availability) ตามหลักบริการความมั่นคง

ตารางที่ 3.3 หัวข้อของเอกสารดับเบิ้ลยูเอสซียูไอจำแนกตามหลักบริการความมั่นคง

Web Security Context - User Interface Guidelines		**Core Security Service Classes**
Section 5 Applying TLS to the Web		
WSCP-51	Certificate Handling and Information	Authentication
WSCP-52	Types of TLS	Authorization
WSCP-53	Mixed Content	Authorization
WSCP-54	Error conditions	Integrity
Section 6 Indicators and Interactions		
WSCP-61	Identity and Trust Anchor Signaling	Confidentiality
WSCP-62	Additional Security Context Information	Accountability
WSCP-63	TLS indicator	Availability
WSCP-64	Error handling and signaling	Accountability
Section 7 Robustness Best Practices		
WSCP-71	Keep Security Chrome Visible	Availability
WSCP-72	Do not mix content and security indicators	Integrity
WSCP-73	Managing User Attention	Confidentiality
WSCP-74	APIs Exposed To Web Content	Confidentiality
Section 8 Security Considerations		
WSCP-81	Active attacks during initial TLS interactions	Integrity
WSCP-82	Certificate Status Checking Failures	Integrity
WSCP-83	Certificates assure identity, not security	Authentication
WSCP-84	Binding "human readable" names to domain names	Authentication
WSCP-85	Warning Fatigue	Confidentiality
WSCP-86	Mixing Augmented Assurance and Validated Certificates	Authorization
WSCP-87	Dynamic content might change security properties	Integrity

3.2.4 การทวนสอบและปรับปรุงแบบรูป

จากหลักการทวนสอบความเหตุสมผลของแบบรูปด้วยเป้าหมาย (Goal) ที่มา (Source) และการนำเสนอ (Representation) ที่ได้กล่าวไว้ในบทที่ 2 เป็นหลักในการทวนสอบแบบรูป โดยในงานวิจัยนี้ได้นำเสนอ การทวนสอบด้วยขั้นตอนระหว่างการสร้างแบบรูป (Transformation) และการประยุกต์ใช้แบบรูป (Application) เพื่อให้แบบรูปที่สร้างมีความน่าเชื่อถือมากยิ่งขึ้น จากหลักการดังกล่าวนำไปสู่การประเมินแบบรูปในบทที่ 4 และการปรับปรุงแบบรูปในภาคผนวก ง

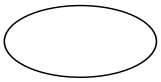
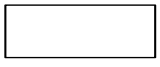
3.3 การสร้างไวยากรณ์ความมั่นคง

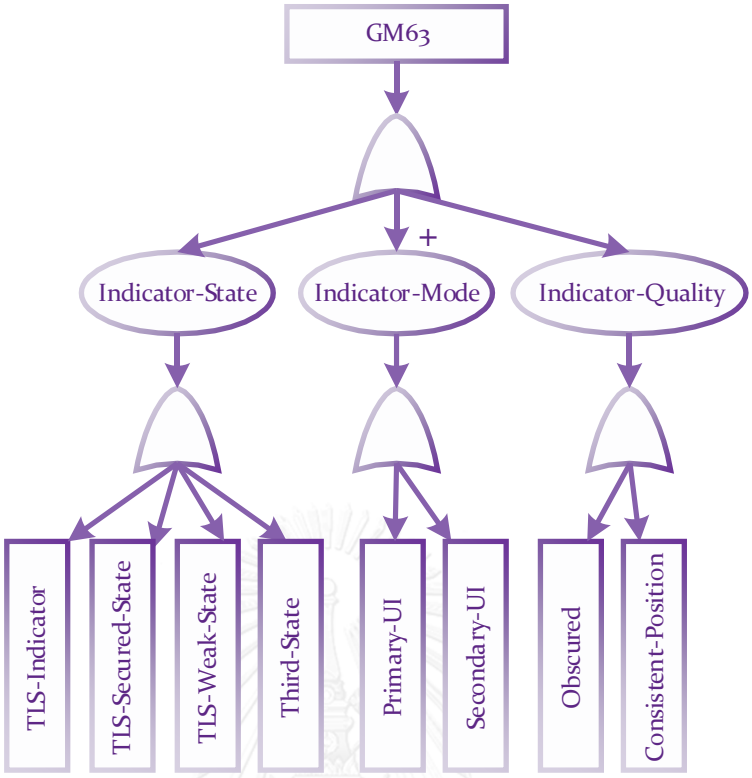
การสร้างไวยากรณ์ความมั่นคงเริ่มจากแผนภาพต้นไม้ความมั่นคงเพื่อตรวจสอบความต้องกันระหว่างองค์ประกอบที่ปรากฏในข้อกำหนดและที่ปรากฏในไวยากรณ์ความมั่นคงที่สร้างขึ้น เพื่อบรรลุจุดประสงค์ในการสร้างแบบรูปให้สามารถนำไปประยุกต์ใช้ในการกำหนดความต้องการเพื่อใช้ในการออกแบบบริบทความมั่นคงเชิงเว็บของตัวแทนผู้ใช้งานเว็บ ผลลัพธ์ที่ได้จากวิเคราะห์ความสัมพันธ์ระหว่างองค์ประกอบไปสร้างไวยากรณ์พื้นฐานสำหรับพัฒนาเครื่องมือเพื่อใช้กำหนดความต้องการด้านความมั่นคงของระบบตัวแทนผู้ใช้งานเว็บต่อไป โดยผลลัพธ์ของไวยากรณ์ความมั่นคงที่นำเสนอในงานวิจัยนี้ได้แสดงไว้ในภาคผนวก ข

3.3.1 การสร้างแผนภาพต้นไม้ความมั่นคง

แผนภาพต้นไม้ความมั่นคงนั้นสร้างเพื่อเป็นตัวกลางในการทวนสอบความต้องกันระหว่างแบบรูปความมั่นคงและไวยากรณ์ความมั่นคงที่ได้สร้างขึ้น โดยมีสัญลักษณ์ตามตารางที่ 3.4

ตารางที่ 3.4 สัญลักษณ์ ชื่อ และความหมายของสัญลักษณ์ที่ใช้ในแผนภาพต้นไม้ความมั่นคง

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



ภาพที่ 3.7 แผนภาพต้นไม้ความมั่นคงสำหรับกำหนดตัวชี้บอกการรักษาความมั่นคงชั้นขนส่ง

การสร้างแผนภาพต้นไม้ คือ การพิจารณาองค์ประกอบที่ต้องปรากฏใน 1 ประโยคความต้องการเท่านั้น จากความต้องการของตัวชี้บอกการรักษาความมั่นคงชั้นขนส่ง (TLS indicator) สามารถนำมาสร้างเป็นแผนภาพต้นไม้ความมั่นได้ดังภาพที่ 3.7 โดยพิจารณาตามข้อกำหนดต่อไปนี้ รายการความต้องการ “GM63” ต้องเลือกอย่างน้อย 1 รายการ จาก “Indicator-State” “Indicator-Mode” และ “Indicator-Quality” ซึ่งเป็นการกำหนดคุณสมบัติด้านสถานะ โหมด และคุณภาพของตัวชี้บอกการรักษาความมั่นคงชั้นขนส่ง

3.3.2 การสร้างไวยากรณ์ความมั่นคง

จากแผนภาพต้นไม้ดังภาพที่ 3.7 ทำให้เราทราบถึงองค์ประกอบและความสัมพันธ์ระหว่างองค์ประกอบภายในข้อกำหนด ซึ่งช่วยในการทวนสอบความสอดคล้องระหว่างองค์ประกอบที่ได้จากข้อกำหนดความมั่นคงกับไวยากรณ์ความมั่นคง ในขั้นตอนนี้จะทำการแปลงแผนภาพต้นไม้ความมั่นคงดังกล่าว ไปเป็นไวยากรณ์ไม่พึ่งบริบท โดยมีแนวคิดและกฎ ซึ่งอ้างอิงจาก ISO/IEC 14977:1996 [17] ในการแปลงจากแผนภาพต้นไม้ดังนี้

1) องค์ประกอบของข้อกำหนดที่แสดงในแผนภาพต้นไม้จะต้องมีครบ แต่ไม่จำกัดลำดับขององค์ประกอบ

2) องค์ประกอบย่อยที่ประกอบกันเป็นองค์ประกอบใหญ่จะต้องมีจำนวนครบตามเครื่องหมายบอกจำนวนที่แสดง เช่น เครื่องหมาย '+' ซึ่งแสดงจำนวนตั้งแต่ 0 ขึ้นไปเมื่ออยู่ภายใต้เครื่องหมาย OR gate และในทางกลับกัน จะแสดงจำนวนตั้งแต่ 1 ขึ้นไปเมื่ออยู่ภายใต้เครื่องหมาย AND gate

3) ใช้เครื่องหมาย '|' แทน OR gate

4) ใช้เครื่องหมาย ',' แทนการเชื่อมต่อสัญลักษณ์ หรือประโยค (ใช้แทน AND gate ได้)

5) ใช้เครื่องหมาย ';' แสดงการสิ้นสุดของทุกกฎ

6) ใช้เครื่องหมาย '?...?' แสดงถึงสัญลักษณ์หรืออักขระพิเศษ

7) ใช้เครื่องหมาย '=' แทนการนิยามค่า

8) ใช้เครื่องหมาย ' "..." ' ครอบสัญลักษณ์หรือข้อมูลที่ไม่สามารถแตกย่อยได้อีก

9) ใช้ตัวหนา สำหรับสัญลักษณ์หรือข้อมูลที่สามารถแตกย่อยได้อีก (ถูกนิยามไว้ใน [6] เพื่อให้เห็นความแตกต่างกับข้อความปกติ)

10) ใช้เครื่องหมาย '[...]' ครอบทางเลือกทุกทางภายใต้ OR gate

11) ใช้เครื่องหมาย '{...}' แทนทางเลือก ที่สามารถปรากฏได้ตั้งแต่ 0 ครั้งขึ้นไป

12) ใช้เครื่องหมาย '(*...*)' แทนข้อคิดเห็นที่จะแสดงในไวยากรณ์และไม่ถูกนำมาแปลงเป็นผลลัพธ์ของไวยากรณ์

เมื่อพิจารณาแผนภาพต้นไม้ร่วมกับแนวคิดและกฎข้างต้นจะได้ไวยากรณ์ความมั่นคงสำหรับตัวชี้บอกการรักษาความมั่นคงชั้นขนส่งได้ตารางที่ 3.5 สามารถอธิบายได้ว่า "GM63" สำหรับกำหนดคุณสมบัติของ TLS Indicator ในแต่ละด้านคือ "Indicator-State" "Indicator-Mode" และ "Indicator-Quality" เช่น การกำหนดโหมดการทำงานของตัวชี้บอก "Indicator-Mode" โดยเลือกอย่างน้อย 1 รายการ จากนอนเทอร์มินัล "List-Mode" หากเลือกทั้งหมดจะได้ผลลัพธ์ความต้องการคือ "TLS indicator shall be part of secondary user interface. Otherwise, it shall be available through primary user interface during usage modes which entail the presence of signaling to the user beyond only presenting page content."

ตารางที่ 3.5 ไวยากรณ์ความมั่นคงของตัวชี้บอกการรักษาความมั่นคงชั้นขนส่ง

ไวยากรณ์ความมั่นคง
(1) **GM63** = [**Indicator-State** | **Indicator-Mode** | **Indicator-Quality**];
(2) **Indicator-State** = [**TLS-Indicator** | **TLS-Secured-State** | **TLS-Weak-State**];
(3) **TLS-Indicator** = **Web-User-Agent** , “shall provide information about the state of TLS protection available by TLS indicator.”;
(4) **Web-User-Agent** = ?User define client name from beginning of the project?;
(5) **TLS-Secured-State** = “TLS indicator shall be present a distinct state that is used only for TLS-secured web pages. ”;
(6) **TLS-Weak-State** = “TLS indicator shall inform users when they are viewing a page that, along with all dependent resources, was retrieved through at least weakly TLS protected transactions, including mixed content”, {“ by using ”, **Third-State** }, “. ”;
(7) **Indicator-Mode** = “TLS indicator shall be part of ”, **List-Mode** , {“Otherwise, it shall be available through ”, **List-Mode** };
(8) **List-Mode** = [**Primary-UI** | **Secondary-UI**];
(9) **Primary-UI** = “primary user interface during usage modes which entail the presence of signaling to the user beyond only presenting page content.”;
(10) **Secondary-UI** = “secondary user interface.”;
(11) **Third-State** = “a third state in the TLS indicator, or via another mechanism (such as a dialog, info bar, or other means)”;
(12) **Indicator-Quality** = [**Obscured** | **Consistent-Position**];
(13) **Obscured** = “TLS indicator shall not be obscured by web content.”;
(14) **Consistent-Position** = “TLS indicator shall be available in a consistent visual position.”;
ตัวอย่างผลลัพธ์
TLS indicator shall be part of secondary user interface. Otherwise, it shall be available through primary user interface during usage modes which entail the presence of signaling to the user beyond only presenting page content.

3.3.3 การทวนสอบไวยากรณ์ความมั่นคง

การตรวจสอบไวยากรณ์ความมั่นคงประกอบด้วย 3 ขั้นตอน ได้แก่ การตรวจสอบความสมเหตุสมผลของไวยากรณ์ความมั่นคง การวิเคราะห์ความสัมพันธ์ภายในไวยากรณ์ความมั่นคง และการวิเคราะห์ความสัมพันธ์ระหว่างไวยากรณ์ความมั่นคง โดยใช้ตารางการตามรอย

3.3.4 การตรวจสอบความสมเหตุสมผลของไวยากรณ์ความมั่นคง

การตรวจสอบความสมเหตุสมผลของไวยากรณ์ความมั่นคง มีจุดประสงค์เพื่อตรวจสอบความถูกต้องของผลลัพธ์ที่ได้จากไวยากรณ์ คือตรวจสอบความถูกต้องของความต้องการความมั่นคงที่กำหนดจากไวยากรณ์ความมั่นคง ว่ามีความต้องกันกับเนื้อหาข้อกำหนดที่ถูกนำมาสร้างไวยากรณ์หรือไม่ การพิจารณาต้องอาศัยผู้เชี่ยวชาญที่มีประสบการณ์ด้านความมั่นคงของเว็บและตัวแทนผู้ใช้เว็บ ในการแสดงความคิดเห็น การให้คำแนะนำและข้อเสนอแนะในการปรับปรุงไวยากรณ์ให้มีความถูกต้อง สมเหตุสมผล และใกล้เคียงกับเนื้อหาข้อกำหนดที่นำมาสร้างได้ เมื่อพิจารณาวิเคราะห์ความสมเหตุสมผลของไวยากรณ์เพื่อนำมาปรับปรุงแล้ว การปรับปรุงอาจเกิดจากการเพิ่มหรือลดองค์ประกอบ เนื่องจากอาจมีเนื้อหาที่ต้องนำเนื้อหาจากส่วนอื่นมาเพิ่มหรือผนวกรวมไวยากรณ์เข้าด้วยกันเพื่อความสมบูรณ์มากขึ้น ซึ่งอาจส่งผลกระทบกับไวยากรณ์อื่น ดังนั้นจึงต้องพิจารณาความสัมพันธ์ทั้งภายในไวยากรณ์เอง และความสัมพันธ์ระหว่างไวยากรณ์ เพื่อตรวจสอบความสมเหตุสมผลของไวยากรณ์ความมั่นคง

3.3.5 การวิเคราะห์ความสัมพันธ์ภายในไวยากรณ์

การวิเคราะห์ความสัมพันธ์ภายในไวยากรณ์ มีจุดประสงค์เพื่อพิจารณาความซ้ำซ้อนขององค์ประกอบที่ปรากฏในไวยากรณ์ โดยสังเกตได้จากวัตถุประสงค์หรือหน้าที่ของไวยากรณ์

จากตัวอย่างไวยากรณ์ พบว่ามีการปรากฏซ้ำขององค์ประกอบจึงต้องทำการปรับปรุงไวยากรณ์โดยการลดรูป ออกไปเมื่อทำการสร้างไวยากรณ์ นอกเหนือจากการการพิจาณาความสัมพันธ์ภายในไวยากรณ์แล้ว ยังต้องพิจารณาความสัมพันธ์ระหว่างไวยากรณ์เพื่อดูผลกระทบที่อาจเกิดขึ้นกับไวยากรณ์อื่นเมื่อมีการปรับปรุงไวยากรณ์ใดๆ

3.3.6 การวิเคราะห์ความสัมพันธ์ระหว่างไวยากรณ์

การวิเคราะห์ความสัมพันธ์ระหว่างไวยากรณ์ มีจุดประสงค์เพื่อพิจารณาผลกระทบที่อาจเกิดขึ้นกับไวยากรณ์อื่นเมื่อมีการปรับปรุงไวยากรณ์ใดๆ ซึ่งพิจารณาได้จากส่วนประกอบ 2 ส่วน คือ เงื่อนไขก่อนการใช้งานและการอ้างถึง โดยจะมีรหัสข้อกำหนดที่ถูกอ้างถึงกำกับบอก โดยส่วนประกอบเงื่อนไขก่อนการใช้ กล่าวถึงไวยากรณ์ที่ต้องกำหนดไว้ก่อนเพื่อนำมาใช้ในไวยากรณ์นี้ และส่วนประกอบการอ้างถึงไวยากรณ์นี้ กล่าวถึงไวยากรณ์ที่สามารถใช้เป็นเป็นส่วนเสริมให้ไวยากรณ์นี้มีเนื้อหาสมบูรณ์ขึ้น สามารถนำมาวิเคราะห์ความสมเหตุสมผล และความสัมพันธ์ระหว่างไวยากรณ์ได้ เมื่อพิจารณาข้อกำหนดที่มีความเกี่ยวข้องกันโดยใช้องค์ประกอบร่วมกัน

บทที่ 4
การประเมินแบบรูปบริบทความมั่นคงเชิงเว็บ

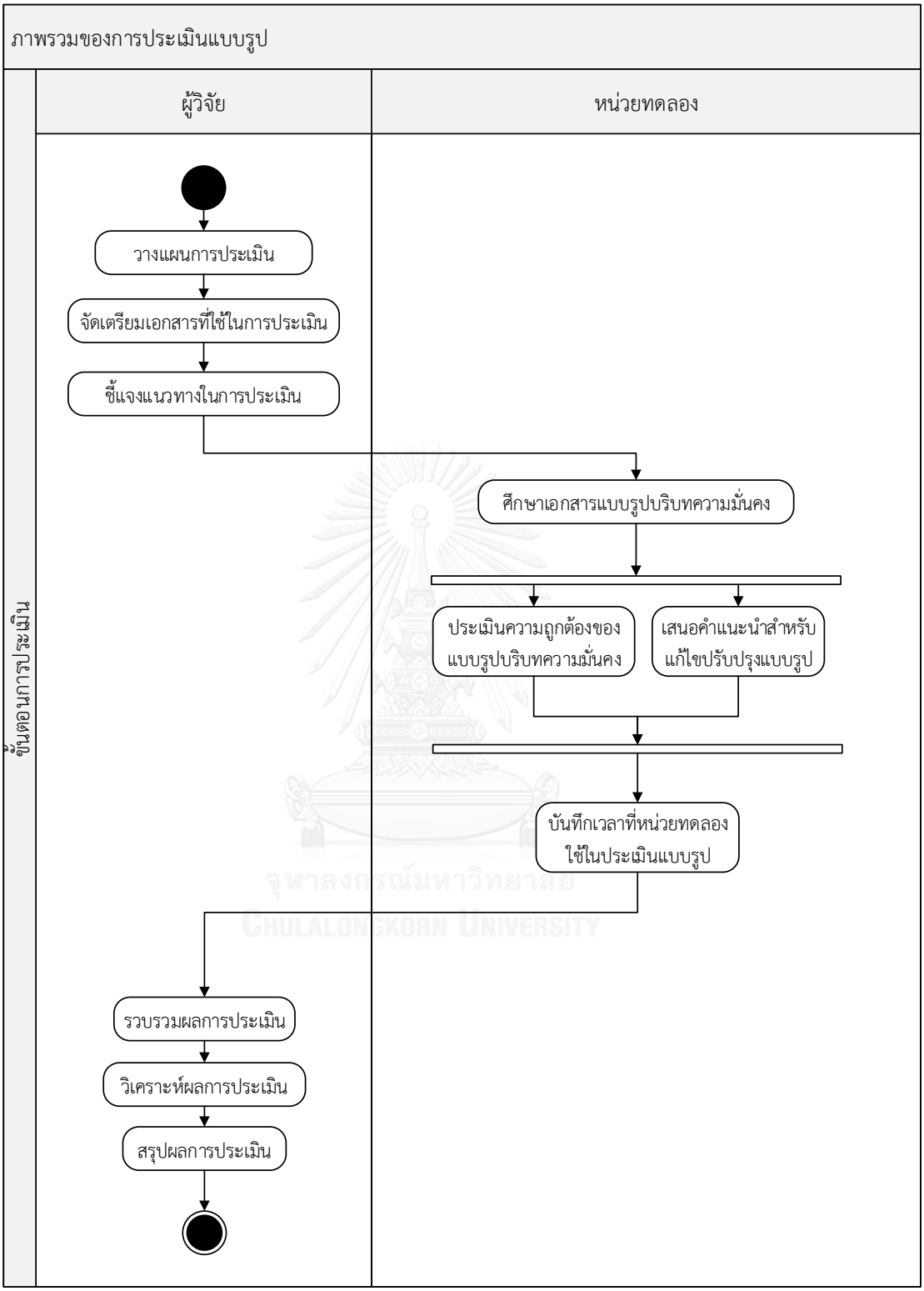
เนื้อหาบทนี้กล่าวถึงรายละเอียดการประเมินแบบรูปบริบทความมั่นคงที่สร้างโดยการวิเคราะห์เอกสารคำแนะนำบริบทความมั่นคงเชิงเว็บของส่วนต่อประสานผู้ใช้ เพื่อประเมินว่าแบบรูปที่ได้นำเสนอมีความครบถ้วน ถูกต้อง และสมบูรณ์ตามหลักความมั่งคงหรือไม่มากน้อยเพียงใด โดยให้ผู้เชี่ยวชาญทวนสอบแบบรูปที่นำเสนอและตอบรายการคำถาม รายละเอียดของการประเมินตั้งแต่ภาพรวมของการประเมิน วัตถุประสงค์ของการประเมิน การวางแผนการประเมิน ดำเนินการตามแผนที่ได้วางไว้ ผลการทดลอง การวิเคราะห์ผลการทดลอง การสรุปผลการทดลอง ไปจนถึงรายการปัญหาที่พบและการแก้ไข โดยมีรายละเอียดดังนี้

4.1 ภาพรวมของการประเมินแบบรูป

การพิจารณาเอกสารคำแนะนำบริบทความมั่นคงเชิงเว็บของส่วนต่อประสานผู้ใช้หรือดับเบิ้ลยูเอสซียูไอ เพื่อนำมาออกแบบระบบนั้นต้องใช้เวลาในและทรัพยากรจำนวนมากในการศึกษาเอกสารดังกล่าว หากรวบรวมประเด็นปัญหาและผลเฉลยไว้ในรูปแบบของแบบรูปความมั่นคง จะสามารถช่วยให้ผู้ออกแบบระบบนำไปใช้ซ้ำในการวิเคราะห์เพื่อออกแบบระบบใดๆ ได้โดยง่าย แต่จะทราบได้อย่างไรว่าการรวบรวมผลเฉลยดังกล่าวนั้นครบถ้วนและสอดคล้องตามเอกสารดับเบิ้ลยูเอสซี-ยูไอ เหมาะสมต่อการนำไปประยุกต์ใช้ งานวิจัยนี้จึงต้องจัดการประเมินเพื่อให้ผู้ที่มีความรู้และประสบการณ์เป็นผู้ประเมินและทวนสอบแบบรูปที่ได้นำเสนอ เมื่อตั้งวัตถุประสงค์ของการประเมินแล้ว มีขั้นตอนในเตรียมการและดำเนินการประเมิน คือ 1) การวางแผนการประเมิน 2) การดำเนินการประเมิน 3) ผลการประเมิน 5) วิเคราะห์ผลการประเมิน และ 6) สรุปผลการประเมิน ดังแสดงรายละเอียดโดยแผนภาพกิจกรรมในภาพที่ 4.1 รายละเอียดของขั้นตอนต่างๆ มีดังนี้

4.2 วัตถุประสงค์ของการประเมินแบบรูป

การประเมินนี้มีวัตถุประสงค์เพื่อสำรวจความคิดเห็นของผู้เชี่ยวชาญด้านความมั่นคงเกี่ยวกับความสมเหตุสมผลตามหลักความมั่นคงของแบบรูปความมั่นคงเชิงเว็บที่ได้รวบรวมผลเฉลยจากเอกสารคำแนะนำส่วนต่อประสานผู้ใช้บริบทความมั่นคงเชิงเว็บ (Web Security Context: User Interface Guidelines: WSC-UI) ทั้งหมด 4 กลุ่ม จำนวน 18 แบบรูป เพื่อประเมินภาพรวมและเนื้อหาของแบบรูป ตลอดจนถึงประโยชน์จากการประยุกต์ใช้แบบรูปที่นำเสนอ



ภาพที่ 4.1 ภาพรวมของการประเมินแบบรูป

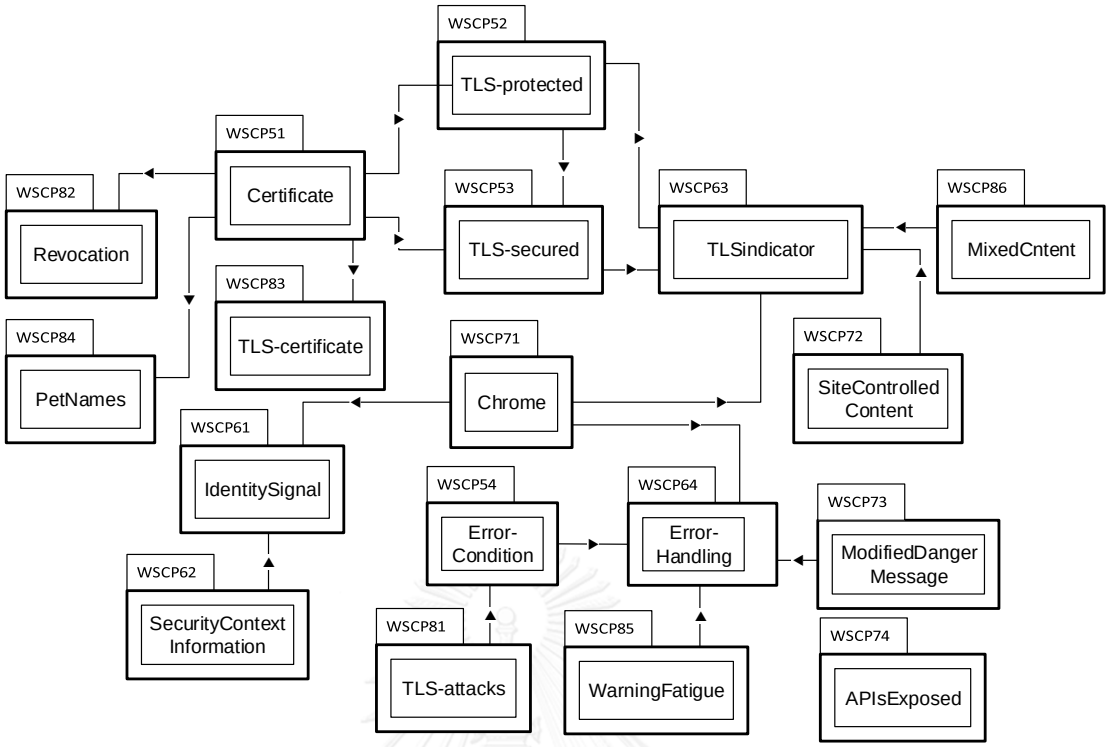
4.3 การวางแผนการประเมิน

4.3.1 สิ่งทดลอง

สิ่งทดลองในการประเมินนี้คือ เอกสารแบบรูปบริบทความมั่นคงเชิงเว็บ ที่มีโครงสร้างเนื้อหาประกอบด้วย บทนำ รายการคำศัพท์ เอกสารที่เกี่ยวข้อง การจัดกลุ่มของแบบรูป และแบบรูปที่นำเสนอทั้งหมด 18 แบบรูป

ตารางที่ 4.1 แบบรูปและการกระจายของจำนวนหน้า

รหัสแบบรูป	ชื่อแบบรูป	จำนวนหน้า	การกระจายของจำนวนหน้า			
			กลุ่ม 1	กลุ่ม 2	กลุ่ม 3	กลุ่ม 4
51	สารสนเทศและการจัดการใบรับรองอิเล็กทรอนิกส์	5	5	5	5	5
52	ระดับการรักษาความมั่นคงชั้นขนส่ง	4	4	-	-	-
53	ประเภทของเว็บจากการรักษาความมั่นคงชั้นขนส่ง	2	2	-	-	-
54	การจัดการสถานการณ์ข้อผิดพลาดเบื้องต้น	4	-	4	-	-
61	การส่งสัญญาณอัตลักษณ์	4	-	-	4	-
62	ข้อมูลเสริมบริบทความมั่นคงเชิงเว็บ	3	-	-	3	-
63	ตัวชี้บอกความมั่นคงชั้นขนส่ง	2	2	-	-	-
64	การจัดการและการส่งสัญญาณความผิดพลาด	3	-	3	-	-
71	การนิยามส่วนต่อประสานผู้ใช้โครม	3	3	3	3	3
72	การป้องกันตัวชี้บอกความมั่นคงจากการลอกเลียนโดยเนื้อหาเว็บ	2	2	-	-	-
73	การจัดการกับความสนใจของผู้ใช้	2	-	2	-	-
74	ส่วนต่อประสานโปรแกรมประยุกต์ของตัวแทนผู้ใช้เว็บ-ที่เรียกใช้ได้โดยเนื้อหาเว็บ	3	-	-	3	-
81	การป้องกันการโจมตีระหว่างการรักษาความมั่นคง-ชั้นขนส่ง	2	-	-	-	2
82	ความล้มเหลวในการตรวจสอบสถานะใบรับรอง	2	-	-	-	2
83	ข้อพึงระวังในการพิจารณาใบรับรองของเว็บ	2	-	-	-	2
84	การใช้ชื่อภาษาธรรมชาติรวมอยู่ในชื่อโดเมน	2	-	-	-	2
85	ความล้าในการแจ้งเตือน	2	-	2	-	-
86	การใช้ร่วมกันระหว่างใบรับรองที่ได้รับประกันเสริมและใบรับรองที่ผ่านการตรวจสอบความสมเหตุสมผล	2	-	-	-	2
รวม		**49**	**28**	**29**	**28**	**28**



ภาพที่ 4.2 ความสัมพันธ์ระหว่างแบบรูป

เนื่องจากเอกสารแบบรูปมีปริมาณเนื้อหาทั้งหมดจำนวนมาก เพื่อลดความผิดพลาดอันเกิดจากปริมาณของเอกสารและความล้าในการศึกษาเอกสารแบบรูปของหน่วยทดลองจึงต้องแบ่งกลุ่มโดยพิจารณาจากความเกี่ยวข้องของเนื้อหาและจำนวนหน้า โดยแต่ละกลุ่มจะต้องได้รับแบบรูปที่มีเนื้อหาเกี่ยวข้องกันและจำนวนหน้าโดยเฉลี่ยใกล้เคียงกัน

เมื่อพิจารณาความสัมพันธ์ระหว่างแบบรูปดังภาพที่ 4.2 แสดงแผนภาพคลาสโดยแทนแต่ละแบบรูปด้วยแพ็คเก็จภายในปรากฏออบเจ็กต์ผลลัพธ์ของแบบรูป จะเห็นว่าแบบรูปที่ 51, 71, 63 และ 64 นิยมถูกเรียกใช้งานจากแบบรูปอื่น ประกอบกับข้อมูลการกระจายของจำนวนหน้าของแต่ละแบบรูปดังตารางที่ 4.1 จากความสัมพันธ์โดยการเรียกใช้ออบเจ็กต์ระหว่างแบบรูป

เอกสารแบบรูปแบ่งได้เป็น 4 กลุ่ม โดยกลุ่มที่ 1 ประกอบด้วยแบบรูป 51, 52, 53, 63 และ 71, 72 กลุ่มที่ 2 ประกอบด้วยแบบรูป 51, 54, 64, 71, 73 และ 85 กลุ่มที่ 3 ประกอบด้วยแบบรูป 51, 61, 62, 71 และ 74 กลุ่มที่ 5 ประกอบด้วยแบบรูป 51, 71, 81-84 และ 86

โดยแต่ละกลุ่มจะมีแบบรูปพื้นฐาน 2 แบบรูป คือ แบบรูป 51 และ 71 จากข้อมูลการกระจายจองจำนวนหน้าของแต่ละแบบรูป จำนวนหน้าโดยเฉลี่ยของเอกสารแบบรูปที่แต่ละกลุ่มได้ศึกษาประมาณ 28 หน้า

4.3.2 หน่วยทดลอง

หน่วยทดลองในการประเมินนี้ มีจำนวนทั้งหมด 16 คน โดยแบ่งเป็นนิสิตภาคในเวลาราชการ 8 คน และนิสิตภาคนอกเวลาราชการ 8 คน ซึ่งมีคุณสมบัติ คือ เป็นนิสิตระดับบัณฑิตศึกษา ที่มีประสบการณ์หรือความชำนาญระบบที่เกี่ยวข้องกับความมั่นคงของซอฟต์แวร์หรือระบบ หรือผ่านการเรียนวิชาความมั่นคงด้านสารสนเทศ (Information Security) ของภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย หรือสาขาวิชาที่เกี่ยวข้อง และมีระดับผลการเรียนในรายวิชาดังกล่าวไม่ต่ำกว่า B

4.3.3 การให้ความรู้แก่หน่วยทดลอง

เพื่อให้หน่วยทดลองเข้าใจถึงจุดประสงค์การประเมิน ภาพรวมของงานวิจัย องค์ความรู้ที่เกี่ยวข้องกับบริบทความมั่นคงเชิงเว็บ และองค์ความรู้ที่เกี่ยวข้องกับการสร้างแบบรูป ผู้วิจัยจึงได้ทำการให้ความรู้แก่หน่วยทดลองก่อนการประเมิน เพื่อเป็นการปรับพื้นฐานความรู้ด้านความมั่นคง โดยดำเนินการตามลำดับดังนี้

1) แสดงให้เห็นถึงที่มาและความสำคัญ และอธิบายแบบรูปจากภาพรวมของของงานวิจัย พร้อมบอกเป้าหมายของการประเมิน

2) นำเสนอองค์ความรู้ที่เกี่ยวข้องกับบริบทความมั่นคงเชิงเว็บทั้งนิยามและโครงสร้างของเนื้อหา อธิบายการพัฒนาแบบรูป ตลอดจนแนะนำโครงสร้างและองค์ประกอบของแบบรูปบริบทความมั่นคง

3) แนะนำแนวทางในการประเมิน โดยอธิบายขั้นตอนและเอกสารประกอบการประเมิน ชี้แจงผลที่คาดว่าจะได้รับจากการประเมิน

4.3.4 ปัจจัยที่ใช้ในการประเมิน

ในการประเมินจะพิจารณาจากกลุ่มปัจจัยต่อไปนี้ ได้แก่ ภาพรวมของเอกสารแบบรูป เนื้อหาของแต่ละแบบรูป และการนำแบบรูปไปประยุกต์ใช้ โดยจำแนกปัจจัยในแต่ละกลุ่มดังนี้

1) กลุ่มปัจจัยด้านภาพรวมของเอกสารแบบรูป
   (1) ความเหมาะสมของเนื้อหา
   (2) ความเข้าใจก่อนได้รับคำอธิบายเกี่ยวกับที่มาและความสำคัญของแบบรูป
   (3) ความเข้าใจหลังได้รับคำอธิบายเกี่ยวกับที่มาและความสำคัญของแบบรูป
   (4) ความเข้าใจก่อนได้รับคำอธิบายเกี่ยวกับเนื้อหาของเอกสารดับเบิ้ลยูเอสซียูไอ
   (5) ความเข้าใจหลังได้รับคำอธิบายเกี่ยวกับเนื้อหาของเอกสารดับเบิ้ลยูเอสซียูไอ

(6) ความเข้าใจโครงสร้างและส่วนประกอบที่ใช้ในการสร้างแบบรูป

(7) ภาพรวมและความสัมพันธ์ระหว่างแบบรูปง่ายต่อการทำความเข้าใจ

2) กลุ่มปัจจัยด้านเนื้อหาของแต่ละแบบรูป

(1) เนื้อหาของแบบรูปง่ายต่อการทำความเข้าใจ

(2) สอดคล้องตามองค์ความรู้ด้านความมั่นคง

(3) ระบุปัญหาและรวมรวบผลเฉลยที่สอดคล้องกัน

(4) แผนภาพคลาสแสดงโครงสร้างภายในได้สะท้อนปัญหาและผลเฉลย

(5) ระบุปัญหาและการแก้ไขได้ชัดเจน ง่ายต่อการทำความเข้าใจ

3) กลุ่มปัจจัยด้านการนำแบบรูปไปประยุกต์ใช้

(1) แบบรูปที่นำเสนอง่ายต่อการทำความเข้าใจและการนำไปประยุกต์ใช้เมื่อเทียบกับเอกสารดับเบิ้ลยูเอสซียูไอ (WSC-UI)

(2) แบบรูปที่นำเสนอช่วยเพิ่มความเข้าใจในการประยุกต์ใช้คำแนะนำด้านความมั่นคงของตัวแทนผู้ใช้เว็บ

(3) ประโยชน์ต่อการวิเคราะห์/ออกแบบด้านความมั่นคงของระบบ

4.3.5 วิธีการเก็บรวบรวมข้อมูล

การประเมินนี้จะดำเนินการเก็บรวบรวมข้อมูลโดยให้หน่วยทดลองทวนสอบแบบรูปบริบทความมั่นคงพร้อมทั้งกรอกผลลัพธ์ตามระดับความคิดเห็นลงในแบบสอบถามเพื่อการประเมินความสมเหตุสมผลของแบบรูปที่นำเสนอ ดังแสดงในภาคผนวก ค.1 ในการประเมินจะวิเคราะห์จากระดับความคิดเห็นว่าเห็นด้วยกับปัจจัยต่างๆ ในระดับใด โดยกำหนดให้มีระดับดังต่อไปนี้

5 หมายถึง หน่วยทดลองเห็นด้วยมากที่สุด

4 หมายถึง หน่วยทดลองเห็นด้วยมาก

3 หมายถึง หน่วยทดลองเห็นด้วยปานกลาง

2 หมายถึง หน่วยทดลองเห็นด้วยน้อย

1 หมายถึง หน่วยทดลองเห็นด้วยน้อยมาก

4.4 การดำเนินการประเมิน

จากแผนการประเมินที่ได้ออกแบบไว้ในหัวข้อที่ 4.3 ได้ดำเนินการการจัดการประเมินกับหน่วยทดลองตามคุณสมบัติที่ได้ระบุไว้ในหัวข้อที่ 4.3.2 ทั้งหมด 16 คน โดยข้อมูลเบื้องต้นของผู้ประเมินแสดงดังตารางที่ 4.2 โดยมีรายละเอียดในการจัดการประเมินดังนี้

ตารางที่ 4.2 ข้อมูลเบื้องต้นของหน่วยทดลอง

ลำดับ	รายการ	ความถี่	ร้อยละ
1. สถานภาพนิสิต			
1.1.	ภาคในเวลาราชการ	8	50.00
1.2.	ภาคนอกเวลาราชการ	8	50.00
รวมทั้งหมด		**16**	**100.00**
2. ผลการเรียน security/network			
2.1.	A	7	43.75
2.2.	B+	5	31.25
2.3.	B	4	25.00
รวมทั้งหมด		**16**	**100.00**
3. ประสบการณ์การทำงาน			
3.1.	น้อยกว่า 2	11	68.75
3.2.	3-5 ปี	4	25.00
3.3.	มากกว่า 5 ปี	1	6.25
รวมทั้งหมด		**16**	**100.00**
4. ตำแหน่งปัจจุบัน			
4.1.	System/Network Engineer	2	12.50
4.2.	BA/SA	3	18.75
4.3.	Programmer/ SE	4	25.00
4.4.	PM	1	6.25
4.5.	QA/Tester	1	6.25
4.6	DB admin	1	6.25
4.7	other	5	31.25
รวมทั้งหมด		**16**	**100.00**
5. ตำแหน่งในอดีต			
5.1.	System/Network Engineer	0	0.00
5.2.	BA/SA	2	12.50
5.3.	Programmer/ SE	9	56.25
5.4.	PM	0	0.00
5.5.	QA/Tester	2	12.50
5.6	DB admin	0	0.00
5.7	other	6	37.50
รวมทั้งหมด		**16**	**100.00**

ตารางที่ 4.2 ข้อมูลเบื้องต้นของหน่วยทดลอง (ต่อ)

ลำดับ	รายการ	ความถี่	ร้อยละ
6. ความถนัดภาษาอังกฤษ			
6.1.	มาก	5	31.25
6.2.	ปานกลาง	11	68.75
6.3.	น้อย	0	0.00
รวมทั้งหมด		**16**	**100.00**

1) หน่วยทดลองตอบแบบสอบถามเกี่ยวกับข้อมูลเบื้องต้น จัดกลุ่มหน่วยทดลองเป็น 4 กลุ่ม ตามรายการแบบรูปที่ออกแบบไว้ในหัวข้อที่ 4.3.1 กลุ่มละ 4 คน โดยแต่ละกลุ่มจะมีนิสิตภาคในเวลาและนิสิตภาคนอกเวลากลุ่มละ 2 คน เท่าๆ กัน

2) ผู้วิจัยแจกเอกสารประกอบการประเมินให้แก่หน่วยทดลอง ดังนี้

(1) แบบรูปบริบทความมั่นคงเชิงเว็บที่นำเสนอ โดยแจกตามกลุ่มของแบบรูปที่กำหนดไว้ในหัวข้อที่ 4.3.1 คือ กลุ่มที่ 1 จะได้รับแบบรูป 51, 52, 53, 63 และ 71, 72 กลุ่มที่ 2 จะได้รับแบบรูป 51, 54, 64, 71, 73 และ 85 กลุ่มที่ 3 จะได้รับแบบรูป 51, 61, 62, 71 และ 74 กลุ่มที่ 5 จะได้รับแบบรูป 51, 71, 81-84 และ 86

(2) รายการคำถามเพื่อการประเมินความสมเหตุสมผลของแบบรูปบริบทความมั่นคงเชิงเว็บ ดังแสดงในภาคผนวก ค.1

(3) เอกสารการตามรอยที่มาของผลเฉลยของแบบรูป (Traceability Matrix) โดยการนำเอาข้อความต้นฉบับจากเอกสารคำแนะนำส่วนต่อประสานผู้ใช้บริบทความมั่นคงเชิงเว็บ (WSC-UI) มารวบรวมไว้ หากมีข้อสงสัยเกี่ยวกับที่มาของเนื้อหาในแบบรูป ผู้ประเมินสามารถทวนสอบไปยังเอกสารการตามรอยที่มาของผลเฉลยของแบบรูปได้

ตารางที่ 4.3 ตารางการจัดกลุ่มทดลองและกระจายของสิ่งทดลอง

กลุ่มทดลอง	หน่วยทดลอง	แบบรูปบริบทความมั่นคงเชิงเว็บที่ได้รับ	ตารางการตามรอย
กลุ่มที่ 1	4 คน	51, 52, 53, 61, 71, 72	ใช้
กลุ่มที่ 2	4 คน	51, 54, 64, 71, 73, 85	ใช้
กลุ่มที่ 3	4 คน	51, 61, 62, 71, 74	ใช้
กลุ่มที่ 4	4 คน	51, 71, 81, 82, 83, 84, 86	ใช้
ทั้งหมด 4 กลุ่ม	ทั้งหมด 16 คน	ทั้งหมด 18 แบบรูป	ทั้งหมด 18 ตาราง

3) ผู้วิจัยให้ความรู้แก่หน่วยทดลองเกี่ยวกับการสร้างแบบรูปและแนะนำแนวทางการประเมิน ตามที่ได้วางแผนไว้ในหัวข้อ 4.3.3 หลังจากให้ความรู้เสร็จถึงจะเริ่มต้นจับเวลาที่หน่วยทดลองใช้ในการทำแบบประเมิน

4) หน่วยทดลองศึกษาเอกสารแบบรูปบริบทความมั่นคงที่แสดงดังภาคผนวก ก โดยหน่วยทดลองจะประเมินความถูกต้องเฉพาะแบบรูปที่อยู่ในกลุ่มของตนเองเท่านั้น เช่น หน่วยทดลองที่จัดอยู่ในกลุ่มที่ 3 จะประเมินแบบรูป 51, 61, 62, 71 และ 74 เป็นต้น

5) หน่วยทดลองประเมินระดับความคิดเห็นในปัจจัยต่างๆ ตามเกณฑ์ที่ได้กำหนดไว้ พร้อมทั้งให้คำแนะนำหรือข้อเสนอแนะ ระหว่างการประเมินผู้วิจัยได้คอยตอบคำถามและให้แนะนำเพิ่มเติมในส่วนที่หน่วยทดลองสงสัย

6) รวบรวมผลการประเมิน พร้อมทั้งสรุปเวลาที่แต่ละหน่วยทดลองใช้ในการประเมิน

4.5 ผลการประเมิน

ผลการประเมินแบบรูปบริบทความมั่นคงเชิงเว็บที่นำเสนอในงานวิจัยนี้เป็นระดับความเห็นของหน่วยทดลองที่มีต่อภาพรวมของเอกสารแบบรูป การประยุกต์ใช้แบบรูป และเนื้อหาของแบบรูป ได้ดังตาราง 4.4 โดยแสดงคะแนนรายปัจจัยในการประเมินจาก 16 หน่วยทดลอง พร้อมแสดงค่าเฉลี่ยและส่วนเบี่ยงเบนมาตรฐานต่อกลุ่มและรายปัจจัยไว้คอลัมน์ขวาสุดของตาราง

ตารางที่ 4.4 ผลการประเมินระดับความเห็นของหน่วยทดลองที่มีต่อแบบรูปในรายปัจจัย

ลำดับ	หน่วยทดลอง / ปัจจัย	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	ค่าเฉลี่ย	ส่วนเบี่ยงเบนมาตรฐาน
1.	**ความคิดเห็นต่อภาพรวมของเอกสารแบบรูปที่นำเสนอ**																	**3.81**	**0.85**
1.1	ความเหมาะสมของเนื้อหา	5	5	5	5	5	4	4	5	4	5	4	5	5	5	5	5	4.75	0.43
1.2	ความเข้าใจที่มาและความสำคัญก่อนได้รับคำอธิบาย	2	3	5	3	2	2	2	5	5	1	3	2	3	2	2	3	2.81	1.18
1.3	ความเข้าใจที่มาและความสำคัญหลังได้รับคำอธิบาย	4	5	5	5	4	4	4	5	4	5	5	4	4	4	5	4	4.44	0.50
1.4	ความเข้าใจเนื้อหาของเอกสาร WSC-UI ก่อนได้รับคำอธิบาย	2	4	5	1	1	2	1	4	2	1	3	3	2	2	2	1	2.25	1.20
1.5	ความเข้าใจเนื้อหาของเอกสาร WSC-UI หลังได้รับคำอธิบาย	4	5	5	4	4	3	3	5	4	4	5	5	4	4	4	5	4.25	0.66
1.6	ความเข้าใจโครงสร้างและส่วนประกอบของแบบรูป	4	5	4	4	4	3	4	4	4	4	5	4	4	5	2	5	4.06	0.75
1.7	การทำความเข้าใจภาพรวมและความสัมพันธ์ระหว่างแบบรูป	5	4	5	5	5	3	3	4	4	5	4	5	4	4	1	5	4.13	1.05
2.	**ความคิดเห็นที่มีต่อการนำแบบรูปไปประยุกต์ใช้**																	**4.46**	**0.16**
2.1	ง่ายต่อการนำไปประยุกต์ใช้เมื่อเทียบกับเอกสาร WSC-UI	5	5	5	5	5	4	4	4	4	4	4	4	4	5	4	5	4.44	0.50
2.2	แบบรูปที่นำเสนอช่วยในการประยุกต์ใช้มากขึ้น	4	4	5	5	5	4	4	5	5	5	5	4	4	4	4	4	4.44	0.50
2.3	มีประโยชน์ต่อการวิเคราะห์/ออกแบบด้านความมั่นคง	5	4	5	5	5	4	4	5	4	5	5	5	4	4	4	4	4.50	0.50

ตารางที่ 4.4 ผลการประเมินระดับความเห็นของหน่วยทดลองที่มีต่อแบบรูปในรายปัจจัย (ต่อ)

ลำดับ	หน่วยทดลอง / ปัจจัย	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	ค่าเฉลี่ย	ส่วนเบี่ยงเบนมาตรฐาน
3.	**ความคิดเห็นต่อเนื้อหาของแบบรูป 51 สารสนเทศและการจัดการใบรับรองอิเล็กทรอนิกส์**																	**4.23**	**0.20**
3.1	เนื้อหาง่ายต่อการทำความเข้าใจ	4	4	4	5	4	3	3	4	4	4	4	5	4	4	5	5	4.13	0.60
3.2	เนื้อหาสอดคล้องตามองค์ความรู้ด้านความมั่นคง	5	5	5	5	4	3	4	5	4	4	5	5	5	4	5	5	4.56	0.61
3.3	ระบุปัญหาและรวมรวบผลเฉลยที่สอดคล้องกัน	5	4	5	5	4	3	3	5	3	4	5	4	5	4	5	4	4.25	0.75
3.4	แผนภาพโครงสร้างภายในสะท้อนปัญหาและผลเฉลย	4	4	5	5	4	4	3	4	4	4	5	4	4	3	5	4	4.13	0.60
3.5	ตัวอย่างแสดงปัญหาและการแก้ไขได้ชัดเจน	5	4	4	4	4	3	3	4	4	4	5	3	4	4	5	5	4.06	0.66
4.	**ความคิดเห็นต่อเนื้อหาของแบบรูป 71 การนิยามส่วนต่อประสานผู้ใช้โครม**																	**4.40**	**0.12**
4.1	เนื้อหาง่ายต่อการทำความเข้าใจ	5	5	4	5	4	4	5	5	5	3	5	5	5	4	5	4	4.56	0.61
4.2	เนื้อหาสอดคล้องตามองค์ความรู้ด้านความมั่นคง	5	5	4	5	5	4	5	4	5	4	5	5	4	4	5	3	4.50	0.61
4.3	ระบุปัญหาและรวมรวบผลเฉลยที่สอดคล้องกัน	5	5	4	4	5	4	4	3	5	4	5	4	5	4	5	3	4.31	0.68
4.4	แผนภาพโครงสร้างภายในสะท้อนปัญหาและผลเฉลย	4	4	5	4	4	5	4	4	4	4	5	4	5	4	5	3	4.25	0.56
4.5	ตัวอย่างแสดงปัญหาและการแก้ไขได้ชัดเจน	5	5	4	4	5	4	4	4	4	4	5	5	4	4	5	4	4.38	0.48

ตารางที่ 4.4 ผลการประเมินระดับความเห็นของหน่วยทดลองที่มีต่อแบบรูปในรายปัจจัย (ต่อ)

ลำดับ	แบบรูปและหน่วยทดลอง / ปัจจัยในการประเมิน	แบบรูป 52				แบบรูป 53				แบบรูป 54				แบบรูป 61			
		1	2	3	4	1	2	3	4	5	6	7	8	9	10	11	12
5.1	เนื้อหาง่ายต่อการทำความเข้าใจ	4	3	4	4	4	4	5	5	4	4	3	5	3	4	5	5
5.2	เนื้อหาสอดคล้องตามองค์ความรู้ด้านความมั่นคง	5	3	5	5	5	5	5	4	5	3	4	4	4	4	5	4
5.3	ระบุปัญหาและรวมรวบผลเฉลยที่สอดคล้องกัน	5	4	5	5	5	5	5	5	5	3	4	5	5	4	5	4
5.4	แผนภาพโครงสร้างภายในสะท้อนปัญหาและผลเฉลย	4	4	5	5	5	5	4	4	5	4	4	3	3	4	5	4
5.5	ตัวอย่างแสดงปัญหาและการแก้ไขได้ชัดเจน	5	4	4	4	5	5	5	5	5	4	4	5	3	3	5	4
ค่าเฉลี่ยรายบุคคล		4.60	3.60	4.60	4.60	4.80	4.80	4.80	4.60	4.80	3.60	3.80	4.40	3.60	3.80	5.00	4.20
ส่วนเบี่ยงเบนมาตรฐาน		0.43				0.09				0.48				0.54			
ค่าเฉลี่ยความพึงพอใจที่มีต่อแบบรูป		**4.35**				**4.75**				**4.15**				**4.15**			

ลำดับ	แบบรูปและหน่วยทดลอง / ปัจจัยในการประเมิน	แบบรูป 62				แบบรูป 63				แบบรูป 64				แบบรูป 72			
		9	10	11	12	1	2	3	4	5	6	7	8	1	2	3	4
6.1	เนื้อหาง่ายต่อการทำความเข้าใจ	3	3	5	4	5	5	3	4	4	4	4	5	5	5	5	5
6.2	เนื้อหาสอดคล้องตามองค์ความรู้ด้านความมั่นคง	4	4	5	5	5	5	5	5	5	4	4	3	5	5	4	5
6.3	ระบุปัญหาและรวมรวบผลเฉลยที่สอดคล้องกัน	4	4	5	4	5	3	5	4	5	3	4	5	5	3	4	5
6.4	แผนภาพโครงสร้างภายในสะท้อนปัญหาและผลเฉลย	3	4	4	4	4	3	3	4	4	4	4	5	5	3	5	4
6.5	ตัวอย่างแสดงปัญหาและการแก้ไขได้ชัดเจน	2	2	5	4	5	4	4	5	5	4	4	3	5	4	4	5
ค่าเฉลี่ยรายบุคคล		3.20	3.40	4.80	4.20	4.80	4.00	4.00	4.40	4.60	3.80	4.00	4.20	5.00	4.00	4.40	4.80
ส่วนเบี่ยงเบนมาตรฐาน		0.64				0.33				0.30				0.38			
ค่าเฉลี่ยความพึงพอใจที่มีต่อแบบรูป		**3.90**				**4.30**				**4.15**				**4.55**			

ตารางที่ 4.4 ผลการประเมินระดับความเห็นของหน่วยทดลองที่มีต่อแบบรูปในรายปัจจัย (ต่อ)

ลำดับ	แบบรูปและหน่วยทดลอง / ปัจจัยในการประเมิน	แบบรูป 73				แบบรูป 74				แบบรูป 81				แบบรูป 82			
		5	6	7	8	9	10	11	12	13	14	15	16	13	14	15	16
7.1	เนื้อหาง่ายต่อการทำความเข้าใจ	4	4	5	5	5	4	4	5	5	5	2	5	4	5	5	5
7.2	เนื้อหาสอดคล้องตามองค์ความรู้ด้านความมั่นคง	5	4	5	4	5	4	5	5	5	4	5	5	5	5	5	5
7.3	ระบุปัญหาและรวมรวบผลเฉลยที่สอดคล้องกัน	5	5	4	2	5	4	5	4	5	5	1	5	5	4	5	5
7.4	แผนภาพโครงสร้างภายในสะท้อนปัญหาและผลเฉลย	5	5	4	4	5	4	5	4	4	5	3	5	4	4	4	5
7.5	ตัวอย่างแสดงปัญหาและการแก้ไขได้ชัดเจน	5	4	4	5	5	4	5	5	5	5	1	5	5	4	4	5
ค่าเฉลี่ยรายบุคคล		4.80	4.40	4.40	4.00	5.00	4.00	4.75	4.50	4.80	4.80	2.40	5.00	4.60	4.50	4.75	5.00
ส่วนเบี่ยงเบนมาตรฐาน		0.28				0.37				1.07				0.22			
ค่าเฉลี่ยความพึงพอใจที่มีต่อแบบรูป		**4.40**				**4.60**				**4.25**				**4.65**			

ลำดับ	แบบรูปและหน่วยทดลอง / ปัจจัยในการประเมิน	แบบรูป 83				แบบรูป 84				แบบรูป 85				แบบรูป 86			
		13	14	15	16	13	14	15	16	5	6	7	8	13	14	15	16
8.1	เนื้อหาง่ายต่อการทำความเข้าใจ	5	5	4	4	4	5	3	4	4	5	4	4	4	5	4	4
8.2	เนื้อหาสอดคล้องตามองค์ความรู้ด้านความมั่นคง	5	5	5	5	4	5	3	5	5	4	5	4	4	5	5	5
8.3	ระบุปัญหาและรวมรวบผลเฉลยที่สอดคล้องกัน	5	4	4	3	5	4	3	5	5	4	4	4	5	5	4	5
8.4	แผนภาพโครงสร้างภายในสะท้อนปัญหาและผลเฉลย	4	4	5	5	4	4	3	5	5	4	4	4	5	4	4	5
8.5	ตัวอย่างแสดงปัญหาและการแก้ไขได้ชัดเจน	5	5	4	5	5	5	3	3	5	3	4	4	5	5	4	4
ค่าเฉลี่ยรายบุคคล		4.80	4.60	4.40	4.40	4.40	4.60	3.00	4.40	4.80	4.00	4.20	4.00	4.60	4.80	4.20	4.60
ส่วนเบี่ยงเบนมาตรฐาน		0.17				0.64				0.33				0.22			
ค่าเฉลี่ยความพึงพอใจที่มีต่อแบบรูป		**4.55**				**4.10**				**4.25**				**4.55**			

4.6 การวิเคราะห์ผลการประเมิน

จากระดับความคิดเห็นที่มีต่อเอกสารแบบรูปบริบทความมั่นคงเชิงเว็บนำมาเขียนเป็นตารางคะแนนความคิดเห็นแบบรายปัจจัยได้ดังตารางที่ 4.5 สรุปผลการทดลองได้ดังนี้

1) ความเห็นของหน่วยทดลองที่มีต่อภาพรวมของเอกสารแบบรูปบริบทความมั่นคงเชิงเว็บพบว่า หน่วยทดลองส่วนใหญ่มีความเห็นในระดับค่อยข้างดีต่อภาพรวมของเอกสารแบบรูป ซึ่งมีระดับความเห็นเฉลี่ยรวมทั้งหมดที่ 3.81 แบ่งช่วงความเห็นก่อนได้รับคำอธิบายจากผู้วิจัยเป็น 3.60 และหลังจากได้รับการอธิบายได้ 4.33 เมื่อเปรียบเทียบคะแนนความเห็นเฉลี่ยก่อนและหลังการให้ความรู้แก่หน่วยทดลอง ระดับความเข้าใจหลังการได้รับการอธิบายเพิ่มขึ้น 0.73 แสดงถึงหน่วยทดลองมีความเข้าใจมากขึ้นจนมีความเห็นในระดับดี

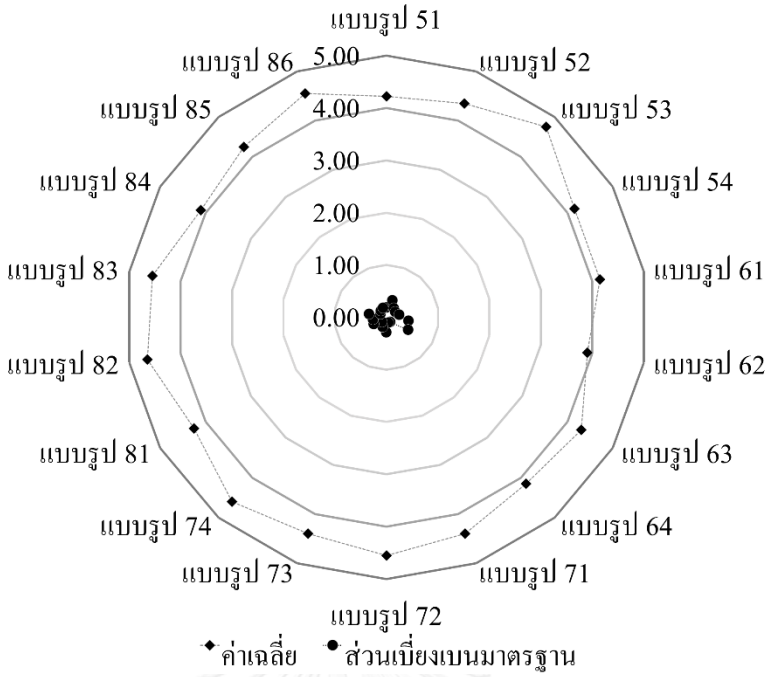
2) ความเห็นของหน่วยทดลองที่มีต่อการประยุกต์ใช้แบบรูปบริบทความมั่นคงเชิงเว็บพบว่าแบบรูปมีประโยชน์ต่อการวิเคราะห์ออกแบบด้านความมั่นคงของระบบในระดับดี ด้วยค่าเฉลี่ยของปัจจัยดังกล่าวเท่ากับ 4.50 ทั้งนี้แบบรูปช่วยให้หน่วยทดลองเกิดการเรียนรู้ในการกำหนดความต้องการความมั่นคงมากขึ้น ทำให้ช่วยลดระยะเวลาและแรงงานในการกำหนดความต้องการความมั่นคงได้ในระดับดีด้วยระดับความพึงพอใจเฉลี่ยเท่ากับ 4.44 ดังนั้น การประยุกต์ใช้แบบรูปโดยรวมอยู่ในระดับดี ด้วยค่าเฉลี่ย 4.46

3) ความเห็นของหน่อยทดลองที่มีต่อเนื้อหาของแบบรูปบริบทความมั่นคงเชิงเว็บพบว่า แบบรูปส่วนใหญ่อยู่ในระดับดี โดยมีค่าเฉลี่ยของแบบรูปทั้งหมดอยู่ที่ 4.35 ในขณะที่แบบรูปที่ 62 อยู่ในระดับค่อนข้างดี ด้วยคะแนนเฉลี่ย 3.90

ตารางที่ 4.5 คะแนนเฉลี่ยรายปัจจัยของหน่วยทดลองที่มีต่อแบบรูปบริบทความมั่นคง

กลุ่มปัจจัย	ปัจจัยในการประเมิน	ค่าเฉลี่ยรายปัจจัย	ค่าเฉลี่ยโดยรวม
ด้านภาพรวม	ความเหมาะสมของเนื้อหา	4.75	3.81/ 4.33
	ความเข้าใจที่มาและความสำคัญก่อนได้รับคำอธิบาย	2.81	
	ความเข้าใจที่มาและความสำคัญหลังได้รับคำอธิบาย	4.44	
	ความเข้าใจเนื้อหาของเอกสาร WSC-UI ก่อนได้รับคำอธิบาย	2.25	
	ความเข้าใจเนื้อหาของเอกสาร WSC-UI หลังได้รับคำอธิบาย	4.25	
	ความเข้าใจโครงสร้างและส่วนประกอบของแบบรูป	4.06	
	การทำความเข้าใจภาพรวมและความสัมพันธ์ระหว่างแบบรูป	4.13	
ด้านการประยุกต์ใช้	ง่ายต่อการนำไปประยุกต์ใช้เมื่อเทียบกับเอกสาร WSC-UI	4.44	4.46
	แบบรูปที่นำเสนอช่วยในการประยุกต์ใช้มากขึ้น	4.44	
	มีประโยชน์ต่อการวิเคราะห์/ออกแบบด้านความมั่นคงของระบบ	4.50	

	แบบรูป / ปัจจัย	51	52	53	54	61	62	63	64	71	72	73	74	81	82	83	84	85	86	ค่าเฉลี่ย	ส่วนเบี่ยงเบนมาตรฐาน
ด้านเนื้อหา	ความเข้าใจ	4.13	3.75	4.50	4.00	4.25	3.75	4.25	4.25	4.56	5.00	4.50	4.50	4.25	4.75	4.50	4.00	4.25	4.25	4.35	0.31
	หลักความมั่นคง	4.56	4.50	4.75	4.00	4.25	4.50	5.00	4.00	4.50	4.75	4.50	4.75	4.75	5.00	5.00	4.25	4.50	4.75	4.65	0.30
	ปัญหาและผลเฉลย	4.25	4.75	5.00	4.25	4.50	4.25	4.25	4.25	4.31	4.25	4.00	4.50	4.00	4.75	4.00	4.25	4.25	4.75	4.29	0.28
	โครงสร้างภายใน	4.13	4.50	4.50	4.00	4.00	3.75	3.50	4.25	4.25	4.25	4.50	4.50	4.25	4.25	4.50	4.00	4.25	4.50	4.21	0.28
	การแสดงตัวอย่าง	4.06	4.25	5.00	4.50	3.75	3.25	4.50	4.00	4.38	4.50	4.50	4.75	4.00	4.50	4.75	4.00	4.00	4.50	4.27	0.41
	ค่าเฉลี่ยแบบรูป	4.23	4.35	4.75	4.15	4.15	3.90	4.30	4.15	4.40	4.55	4.40	4.60	4.25	4.65	4.55	4.10	4.25	4.55	4.35	



ภาพที่ 4.3 แผนภูมิเรดาร์ค่าเฉลี่ยระดับความคิดเห็นของแบบรูป

4.7 สรุปผลการประเมิน

ค่าเฉลี่ยความพึงพอใจของหน่วยทดลองที่มีต่อแบบรูปในแต่ละด้านอยู่ในระดับดี-ดีมาก (คะแนนเฉลี่ยอยู่ระหว่าง 4-5) โดยภาพรวมของเอกสารหลังจากได้รับการอธิบายจากผู้วิจัยมีค่าเฉลี่ยเท่ากับ 4.33 ด้านการประยุกต์ใช้มีค่าเฉลี่ยเท่ากับ 4.46 และด้านเนื้อหาของแบบรูปทั้งหมดมีค่าเฉลี่ยเท่ากับ 4.35 และส่วนเบี่ยงเบนมาตรฐานเท่ากับ 0.22 แบบรูปที่มีค่าเฉลี่ยสูงสุด คือแบบรูป 53 ด้วยค่าเฉลี่ย 4.75 ในขณะที่ค่าเฉลี่ยต่ำสุด คือแบบรูป 62 จากผลการประเมินชี้ให้เห็นว่าแบบรูปที่นำเสนอได้รับความพึงพอใจอย่างสูงโดยหน่วยทดลอง อย่างไรก็ตามผลสะท้อนของหน่วยทดลองลงความเห็นว่าแบบรูปบริบทความมั่นคงเชิงเว็บยากต่อการทำความเข้าใจเนื่องจากการใช้ภาษาและคำศัพท์ทางเทคนิคที่ปรากฏในแบบรูปมีจำนวนมาก สำหรับคำแนะนำที่ได้จากหน่วยทดลองถูกรวบรวม สรุปและนำไปปรับปรุงแบบรูป ได้แสดงรายละเอียดไว้ในภาคผนวก ง

บทที่ 5
การประยุกต์ใช้ไวยากรณ์ความมั่นคง

ไวยากรณ์ความมั่นคงเป็นพื้นฐานของเครื่องมือที่สำหรับสร้างรายการความต้องการ เพื่อให้มั่นใจได้ว่าไวยากรณ์ที่ออกแบบสามารถนำไปประยุกต์ใช้ได้อย่างครบถ้วน ในบทนี้จะแสดงแนวทางการประยุกต์ใช้ไวยากรณ์ความมั่นคงร่วมกับกรณีศึกษาทั้งหมด 3 ระบบ คือ ธนาคารอิเล็กทรอนิกส์ (E-Banking) ระบบสำรองที่พักและการเดินทาง (Hotels and Flights Booking) และระบบค้นดูเว็บ (Web Browser) โดยคำอธิบายของระบบจะกล่าวถึงในหัวข้อที่ 5.1 และทุกเส้นทางของไวยากรณ์จะถูกประยุกต์ในหัวข้อ 5.2 มีรายละเอียด ดังนี้

5.1 กรณีศึกษา

เนื่องจากความสามารถของเว็บบราวเซอร์ที่ติดตั้งบนคอมพิวเตอร์ส่วนบุคคลในปัจจุบันมีคุณสมบัติครบถ้วนตามเอกสารดับเบิ้ลยูเอสซียูไอ แต่แอพพลิเคชันบนอุปกรณ์มือถือยังมีข้อจำกัดและจำเป็นต้องออกแบบให้สอดคล้องตามเอกสารดับเบิ้ลยูเอสซียูไอ ดังนั้น คุณลักษณะพื้นฐานของระบบที่นำมาใช้เป็นกรณีศึกษา คือ โปรแกรมประยุกต์ตัวแทนผู้ใช้เว็บที่ติดตั้งทั้งบนอุปกรณ์มือถือสำหรับเข้าถึงเนื้อหาเว็บ โดยการพิจารณากรณีศึกษาจากประเภทของเว็บตามที่ได้นิยามไว้ในแบบรูป 53 แบ่งได้เป็น เว็บที่มีการปกป้องด้วยการรักษาความมั่นคงชั้นขนส่ง โดยแต่ละกรณีมีความต้องการด้านระดับความมั่นคงที่กันตามบริบทการใช้งานเพื่อให้ครบคลุมทุกไวยากรณ์ ดังนี้

5.1.1 ธนาคารอิเล็กทรอนิกส์ (E-Banking)

ระบบอัพทูมี (UP2ME) เป็นแอพพลิเคชันเกี่ยวข้องกับการจัดการด้านธุรกรรมโดยการผูกบัญชีเงินฝากของผู้ใช้เพื่อการทำรายการฝากเงิน รายการโอนเงิน และรายการจ่ายเงินสำหรับสินค้าและบริการผ่านธนาคารอิเล็กทรอนิกส์ (E-Banking) ระบบดังกล่าวมีความต้องการด้านความมั่นคงสูงเนื่องจากมีเว็บไซต์ปลอมเป็นจำนวนมาก (Phishing) พยายามเลียนแบบและชักจูงให้เข้าสู่เว็บที่ปลอมด้วยกลไกต่างๆ ตัวแทนเว็บจึงจำเป็นต้องคัดกรองและติดต่อเพียงเว็บที่แท้จริงเท่านั้น ซึ่งจะต้องมีการตรวจสอบการปกป้องด้วยการรักษาความมั่นคงชั้นขนส่งอย่างแข็งแกร่ง (Strongly TLS-protected) กับผู้ให้บริการเว็บที่ติดต่อด้วย เช่น SCBeasy.com

5.1.2 ระบบสำรองห้องพักและเที่ยวบิน (Rooms and Flights Reservation)

ระบบให้คำปรึกษาด้านการเดินทาง (TripAdvisor) โดยผู้ใช้สืบค้นสำหรับราคาตั๋วเครื่องบิน โรงแรม จากนั้นระบบจะค้นคืนข้อมูลจากแหล่งผู้ให้บริการเว็บที่หลากหลายภายนอกระบบเพื่อ

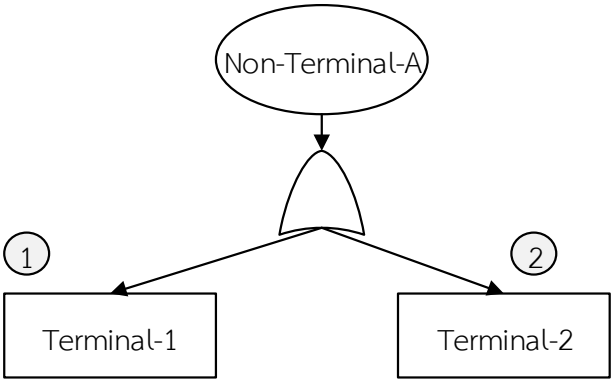
เปรียบเทียบราคาและข้อเสนอที่ดีที่สุด ซึ่งการทำรายการอาจเชื่อมโยงไปยังการทำธุรกรรมและข้อมูลสำคัญของผู้ใช้ หรือนำพาผู้ใช้ไปสู่เว็บไซต์ภายนอกระบบอันเสี่ยงต่อการโจมตี ระบบดังกล่าวจึงควรพิจารณาความมั่นคงของการปกป้องด้วยการรักษาความมั่นคงชั้นขนส่งอย่างอ่อนแอ (Weak TLS-protected) เพื่อแจ้งเตือนให้แก่ผู้ใช้เมื่อมีการเชื่อมต่อไปภายนอกระบบ กับผู้ให้บริการเว็บที่ติดต่อด้วย เช่น Agoda.com, Booking.com หรือ Hotels.com

5.1.3 ระบบค้นดูเว็บ (Web Browser)

ดอล์ฟินเว็บเบราว์เซอร์ (Dolphin Web Browser) เป็นโปรแกรมสำหรับค้นดูเว็บและสืบค้นข้อมูลบนอินเตอร์เนต ซึ่งไม่จำกัดระดับความปลอดภัย (Mix content) แต่สามารถตรวจสอบระดับความน่าเชื่อถือของเว็บและแจ้งเตือนความผิดปกติให้แก่ผู้ใช้ได้ กับผู้ให้บริการเว็บที่ติดต่อด้วยทุกเว็บ

5.2 แนวทางการประยุกต์ใช้ไวยากรณ์ความมั่นคง

แนวทางการประยุกต์ใช้ไวยากรณ์ความมั่นคงแสดงให้เห็นถึงการได้มาซึ่งความต้องการด้านความมั่นคงจากไวยากรณ์ความมั่นคง เพื่อให้เข้าใจการประยุกต์ใช้ไวยากรณ์ความมั่นคงในการสร้างเครื่องมือต้นแบบ อีกทั้งเป็นการทวนสอบความครบถ้วนของรายการความต้องการความมั่นคงที่ได้โดยไวยากรณ์ที่นำเสนอสร้างจากแบบรูปความมั่นคงตามขอบเขตของงานวิจัยได้แสดงรายละเอียดไว้ในภาคผนวก ข ทั้งหมด 18 ไวยากรณ์ จำแนกเป็น 4 กลุ่ม คือ 1) การนำการรักษาความมั่นคงของชั้นขนส่งมาประยุกต์ใช้กับเว็บ 2) ตัวชี้บอกและการมีปฏิสัมพันธ์ 3) แนวทางที่ดีที่สุดสำหรับสภาพทนทาน และ 4) ข้อคำนึงด้านความมั่นคง แต่ละไวยากรณ์จะถูกนำมาสร้างเส้นทางที่เป็นไปได้ทั้งหมดเพื่อให้ง่ายต่อการทำความเข้าใจแผนภาพต้นไม้ความมั่นคง ดังเช่นภาพที่ 5.1 จะถูกนำมาทวนสอบเส้นทางและผลลัพธ์จากไวยากรณ์



ภาพที่ 5.1 ตัวอย่างการประยุกต์ใช้ไวยากรณ์ความมั่นคง

เส้นทางของต้นไม้ความมั่นคงพิจารณาจากบนลงล่างและเส้นทางที่เป็นไปได้ภายใต้ทางเลือกที่เป็นไปได้เท่านั้น (OR Gate) เนื่องจากภายใต้เครื่องหมายเลือกทั้งหมด (AND Gate) จะถือเป็นการเลือกโดยปริยาย โดยกำหนดให้

1) เครื่องหมาย (ข้อความ) หมายถึง นอนเทอร์มินัลโนด (Non-terminal Node) หรือบัพที่ยังไม่สิ้นสุด กล่าวคือสามารถแตกเป็นนอนเทอร์มินัลหรือเทอร์มินัลได้อีก

2) เครื่องหมาย [ข้อความ] หมายถึง เทอร์มินัลโนด (Terminal Node) หรือบัพปลายทางที่ไม่สามารถแตกเป็นโนดย่อยได้อีก

3) เครื่องหมาย (n) หมายถึง ตัวเลขแสดงลำดับของการท่องไปยังแต่ละโนดของต้นไม้

ความต้องการทั้งหมดจากการประยุกต์ใช้ไวยากรณ์ความมั่นคง สำหรับกรณีศึกษาทั้ง 3 กรณี ทั้งหมด 78 รายการความต้องการ โดยกรณีศึกษาที่ 1 ธนาคารอิเล็กทรอนิกส์มีรายการความต้องการลำดับที่ 1-20 ในตารางที่ 5.1 กรณีศึกษาที่ 2 มีรายการความต้องการลำดับที่ 21-51 ในตารางที่ 5.2 และกรณีศึกษาที่ 3 มีรายการความต้องการลำดับที่ 52-78 ในตารางที่ 5.3

ตารางที่ 5.1 รายการความต้องการของกรณีศึกษาที่ 1 ธนาคารอิเล็กทรอนิกส์

กรณีศึกษาที่ 1 ธนาคารอิเล็กทรอนิกส์		
ลำดับ	**ความต้องการความมั่นคง**	**ไวยากรณ์**
1	UP2ME shall support Authentication, where the issuer asserts that the subject entity, by validate the certificate chain for a certificate up to a trust root and recognize the trust root as augmented assurance qualified. Certificate information from additional assurance of Certificate Authority is presenting on Primary Security Indicator that contains following: Organization (O) and Country (C) Subject-Field and Handling by marking Trust Anchor using application-specific out-of-band mechanism or specially marked by specific policy object identifier for Augmented Assurance Certificate from SCB website.	GM51
2	UP2ME shall communicate with SCB website. The server used Validated Certificate that matches the dereferenced URI though strongly TLS-protected that the https URL was used, strong TLS algorithms were negotiated with protocol version at least SSLv3.	GM52
3	UP2ME shall present UI indicator to signal the presence of Augmented Assurance certificates for the TLS-secured web page.	GM53

ตารางที่ 5.1 รายการความต้องการของกรณีศึกษาที่ 1 ธนาคารอิเล็กทรอนิกส์ (ต่อ)

กรณีศึกษาที่ 1 ธนาคารอิเล็กทรอนิกส์		
ลำดับ	**ความต้องการความมั่นคง**	**ไวยากรณ์**
4	SCB website present their certificate during TLS negotiation, but does not match with the URI corresponding to the transaction. UP2ME shall handling the error condition by using error signaling class of Danger Messages.	GM54
5	SCB website present their certificate during TLS negotiation, was fails. UP2ME shall handling the error condition by using error signaling class of Danger Messages.	
6	SCB website present their certificate then the possible danger assessed by Third party services and heuristic approaches UP2ME shall handling the error condition by using error signaling class of Danger Messages.	
7	UP2ME shall display information from validated certificates that is not taken from unauthenticated or untrusted sources as part of the identity signal.	GM61
8	During interactions with a TLS-secured Web page, the following information derived from augmented assurance certificate shall be displayed in the Identity Signal: To inform the user about the owner of the Web page, including human-readable information about the certificate subject at least an applicable DNS name that matches either the subject's Common Name attribute or its subjectAltName extension shorten such a DNS name by displaying only a suffix. To inform the user about the party responsible for that information, including the Issuer field's Organization attribute. Subject logotypes shall be rendered only derived from augmented assurance certificate.	
9	UP2ME shall provide information about the state of TLS protection available by TLS indicator.	GM63
10	TLS indicator shall be part of secondary user interface. Otherwise, it shall be available through primary user interface during usage modes which entail the presence of signaling to the user beyond only presenting page content.	
11	TLS indicator shall be present a distinct state that is used only for TLS-secured web pages.	
12	UP2ME shall have Danger Messages for situations when there is a positively identified danger to the user.	GM64
13	Messages shall interrupt the user's current task, such that the user has to acknowledge the message.	

ตารางที่ 5.1 รายการความต้องการของกรณีศึกษาที่ 1 ธนาคารอิเล็กทรอนิกส์ (ต่อ)

กรณีศึกษาที่ 1 ธนาคารอิเล็กทรอนิกส์		
ลำดับ	**ความต้องการความมั่นคง**	**ไวยากรณ์**
14	Danger Messages shall be presented in a way that makes it impossible for the user to go to or interact with the destination web site that caused the danger situation to occur, without first explicitly interacting with the Danger Message.	GM64
15	The UP2ME shall employ techniques that prevent immediate dismissal of user interfaces that used to inform users about security critical events or to solicit input by using a temporarily disabled "OK" button.	GM73
16	UP2ME shall not allow content from SCB Easy Net to obscure, hidden or disable security user interfaces. Especially when opening new windows.	GM74
17	UP2ME shall not expose programming interface which permit installation of software without the user's consent. Including when the user agent is attempting to install software outside the agent environment as a result of web content.	
18	UP2ME shall inform user and request consent when the user agent is attempting to install software outside the agent environment as a result of web content. The warning message shall be used for the interaction.	
19	The development for Online Certificate Status Protocol status checking is fragile and subject to frequent failures, so the UP2ME shall expose failures of certificate validation checks to user as danger level message.	GM82
20	The UP2ME shall support the binding between domain name/certificate and the actual real-world entity of Validated Certificate from SCBeasy.net including the identity information such as a Petname.	GM84

ตารางที่ 5.2 รายการความต้องการของกรณีศึกษาที่ 2 ระบบสำรองห้องพักและเที่ยวบิน

กรณีศึกษาที่ 2 ระบบสำรองห้องพักและเที่ยวบิน		
ลำดับ	**ความต้องการความมั่นคง**	**ไวยากรณ์**
21	TripAdvisor shall support certificates verifying that it's chaining up to a locally configured trust anchor as a Validated Certificate from Agoda website.	GM51
22	TripAdvisor shall support handling a Self-signed Certificates which are not part of the user agent's store of trust roots and essentially serve as a container for cryptographic key material in a key exchange that is not verified by any third party. By the pinning interaction that enables users to pin a certificate to a destination, but not allow to be accepted automatically for an untrusted root certificate to additional sites nor to be pinned to more than one site or Key Continuity Management (KMC) to determine consistently communicating with the same web server for self-signed certificates (or certificates that chain up to an untrusted root) from Agoda, Booking and Hotels website.	
23	TripAdvisor shall communicate with Agoda website though weakly TLS-protected when strong TLS protection could not be achieved the following reasons: certificates were used that are not either validated certificates, or self-signed certificates pinned to the destination.	GM52
24	Agoda.com website; A Web page is called mixed content if the top-level resource was retrieved through a strongly TLS protected HTTP transaction, but some dependent resources were retrieved through weakly protected.	GM53
25	Agoda website present their certificate during TLS negotiation, was neither lead to a trusted root nor pinned to the destination. TripAdvisor shall handling the error condition by using error signaling class of Warning Messages or higher and offering a possibility to pin newly encountered certificates to the destination.	GM54
26	Agoda.com website present their certificate during TLS negotiation, human-readable information from the certificate shall not be presented as trustworthy. TripAdvisor shall handling the error condition by a dialog display Organization attribute from Self-Signed-Certificate.	
27	The Identity Signal shall be part of primary user interface and available through secondary user interface during usage or presentation mode.	GM61

ตารางที่ 5.2 รายการความต้องการของกรณีศึกษาที่ 2 ระบบสำรองห้องพักและเที่ยวบิน (ต่อ)

กรณีศึกษาที่ 2 ระบบสำรองห้องพักและเที่ยวบิน		
ลำดับ	**ความต้องการความมั่นคง**	**ไวยากรณ์**
28	TripAdvisor shall inform user about the identity of the web site by using Identity Signal, in a consistent visual position and not be obscured by web content.	GM61
29	During interactions with mixed content, TripAdvisor shall not include any site identity information which is in use for unprotected HTTP transactions.	
30	During interactions with mixed content, the identity signal shall include indicators that point out any error conditions that why the web page is unprotected HTTP transactions	
31	The meaning of security context information in both primary and secondary interface shall be consistent.	GM62
32	TLS indicator shall inform users when they are viewing a page that, along with all dependent resources, was retrieved through at least weakly TLS protected transactions, including mixed content by using a third state in the TLS indicator, or via another mechanism (such as a dialog, info bar, or other means).	GM63
33	TLS indicator shall not be obscured by web content.	
34	TLS indicator shall be available in a consistent visual position.	
35	TripAdvisor shall have Warning / Caution messages for situations when the system has good reason to believe that the user may be at risk based on the current security context information, but a determination cannot positively be made.	GM64
36	Warning/Caution messages shall provide the user with distinct options for how to proceed.	
37	The options presented on these warnings shall contain following characteristic:	
	- Descriptive to the point that their respective meaning can be understood in the absence of any other information contained in the warning interaction.	
	- A succinct text component denoting which option is recommended.	

ตารางที่ 5.2 รายการความต้องการของกรณีศึกษาที่ 2 ระบบสำรองห้องพักและเที่ยวบิน (ต่อ)

กรณีศึกษาที่ 2 ระบบสำรองห้องพักและเที่ยวบิน		
ลำดับ	**ความต้องการความมั่นคง**	**ไวยากรณ์**
38	TripAdvisor shall enable the user to easily return to the page that the user was previously interacting with.	GM64
39	User interface elements within chrome which can be mimicked under the control of web content.	GM72
40	Web User Agents shall not communicate positive trust information using Site-Controlled content.	
41	Site-Controlled content which hosted in chrome are Favicon, Information Bar, and Status Bar.	
42	Site-Controlled shall not be displayed in a manner that confuses hosted content and chrome indicators in a position close to them for both primary and secondary. A not use a 16x16 image shall not be used to indicate the security status in order to avoid imitation from the favorite icon	
43	The Agoda web server are not be granted control from the security relevant notifications that users interact with.	GM73
44	The TripAdvisor shall display only a modal security dialog, e.g., prompts for user credentials, script errors, and TLS errors related to Agoda.com which user currently have focus.	
45	TripAdvisor shall prevent Agoda content from overlaying chrome.	GM74
46	When web content request to add URIs to the bookmark collection. The TripAdvisor shall not permit the URIs that do not match to the URI of the Agoda that the user currently interacts with.	
47	TripAdvisor that use a windowed interaction paradigm, shall restrict the opening of pop-up windows from the web content, particularly those not initiated by user.	
48	TripAdvisor shall support the prior designation of high-value site, which Trust Anchor, Validated and Augmented Assurance Certificate are required. Handling with the TLS errors that leads to additional exposure during the first TLS interaction with the site by a strong warning signal.	GM81

ตารางที่ 5.2 รายการความต้องการของกรณีศึกษาที่ 2 ระบบสำรองห้องพักและเที่ยวบิน (ต่อ)

กรณีศึกษาที่ 2 ระบบสำรองห้องพักและเที่ยวบิน		
ลำดับ	**ความต้องการความมั่นคง**	**ไวยากรณ์**
49	TripAdvisor which indicates SSL/TLS connections as secure for the strong encryption of communication from Self-signed certificate presented by Agoda.com, but there are distinctions between identity and security so a site may not operate in a safe manner or subject to attack.	GM83
50	TripAdvisor shall constrain the number of the Warning Message.	GM85
51	The TripAdvisor that has loaded two Web pages the first page was retrieved, an Augmented Assurance Certificate was used by the TLS session. When the second page was retrieved, under the control of content such as external script and plug-ins from the top level resource vouches for the content of all dependent resources. The network error for the different security presentation of the two pages are expressed by the indicators of identity signal.	GM86

ตารางที่ 5.3 รายการความต้องการของกรณีศึกษาที่ 3 ระบบค้นดูเว็บ

กรณีศึกษาที่ 3 ระบบค้นดูเว็บ		
ลำดับ	**ความต้องการความมั่นคง**	**ไวยากรณ์**
52	Dolphin Web Browser shall support Interactively Acceptance: while the user is focused on a primary task unrelated to trust and certificate management but not allow users to designate trust roots as augmented assurance qualified, Trust Anchor installation: that is handled by user agent vendors and device manufacturers based on out-of-band information and Trust Anchor update: that is handled as part of operating system software updates for any certificates form any website.	GM51
53	Dolphin Web Browser shall communicate with any websites though TLS-protected that the resources was identified through a URI with the https URI scheme, the TLS handshake was performed successfully through the TLS channel.	GM52
54	Any website present their certificate during TLS negotiation, then TLS error conditions occur. Dolphin Web Browser shall handling the error condition by choose to abort the connection without any further user interaction.	GM54

ตารางที่ 5.3 รายการความต้องการของกรณีศึกษาที่ 3 ระบบค้นดูเว็บ (ต่อ)

กรณีศึกษาที่ 3 ระบบค้นดูเว็บ		
ลำดับ	**ความต้องการความมั่นคง**	**ไวยากรณ์**
55	Any website present their certificate then high likelihood risks are identified, but involve further user decisions. Dolphin Web Browser shall handling the error condition by using error signaling class of Warning Messages.	GM54
56	Any website present their certificate that is validated certificate then their form submission are directed to an unsecured channel. Dolphin Web Browser shall handling the error condition by using error signaling class of Warning Messages.	
57	During interactions with mixed content, Dolphin Web Browser shall not be render any logotypes derived from certificates.	GM61
58	Dolphin Web Browser shall provide the following security context information available:	GM62
	- The Web page's domain name	
	- Owner information, consistent with Identity Signal Content.	
	- Verifier information, consistent Identity Signal Content.	
	- The reason why the displayed information is trusted (or not).	
	- An explanation of the information represented by the TLS indicator.	
	- If the Web page is weakly TLS-protected, then, what conditions cause the protection to be weak.	
	- Whether the user has visited the site in the past.	
	- Whether the user has stored credentials for this site.	
	- Whether the site content was encrypted in transmission.	
	- Whether the site content was authenticated.	
	- When the user first visited the site in the past.	
	- How often the user visited the site in the past.	
59	Error signaling that occurs as part of primary user interface shall be phrased in terms of threat to user's interests, not solely in terms of art nor technical occurrence	GM64

ตารางที่ 5.3 รายการความต้องการของกรณีศึกษาที่ 3 ระบบค้นดูเว็บ (ต่อ)

กรณีศึกษาที่ 3 ระบบค้นดูเว็บ		
ลำดับ	**ความต้องการความมั่นคง**	**ไวยากรณ์**
60	Error messages shall provide feedback or obtain assistance, not tell the user to enter the destination site that caused the error	GM64
61	Error interactions shall have an option to request a detailed description of the condition that caused the error interaction to occur.	
62	User agents shall additionally display indicators in an error situation.	
63	Chrome refer to the representation through which the user interacts with the user agent itself, as distinct from the accessed web content. This includes both primary and secondary user interface. By Primary User Interface denotes the portions of a Web user agent's user interface that are available to users without being solicited by a user interaction and Secondary User Interface denotes the portions of a Web user agent's user interface that are available to the user after they are solicited by a specific user interaction.	GM71
64	Chrome shall always be present to signal security context information.	
65	User interface elements commonly present in Dolphin Web Browser, a Web User Agents, are: Identity Signal, Navigation Button, TLS Indicator, Favicon, Information Bar, Status Bar, Page Title, Location Bar, and URL Bar.	
66	Identity signal present Identity Information about the web site.	
67	A Navigation buttons provide a drop down list of previously viewed pages. Each page is identified by the content of the corresponding HTMLTITLE element.	
68	A TLS-Indicator using padlock icon to indicate the use of SSL.	
69	A Favicon is a small graphic specified by website to act as an icon that appears in the URL bar in most desktop web browsers and on the tabs in some browsers.	
70	An information bar across the top of the web content window to communicate with users.	
71	A Status bar displays messages from the browser, such as the target of the hyperlink under the mouse cursor.	

ตารางที่ 5.3 รายการความต้องการของกรณีศึกษาที่ 3 ระบบค้นดูเว็บ (ต่อ)

กรณีศึกษาที่ 3 ระบบค้นดูเว็บ		
ลำดับ	**ความต้องการความมั่นคง**	**ไวยากรณ์**
72	A Location Bar is a widget which displays and allows input of the textual location entered as a URI of the resource being requested or displayed - after the response is received.	GM71
73	A Window title for viewing a web page and Tabs title for viewing multiple web pages using the content of the HTML TITLE element from Agoda, the displayed web page.	
74	A URL bar show current web page's URL is chosen in tandem by the creator of the referring hyperlink and the web site operator. An additional, the displayed hostname also using the current web page's URL.	
75	Dolphin Browser shall restrict window sizing and moving operations to keep security chrome visible.	GM74
76	When web content request to add bookmarks, the Dolphin Browser shall request for explicit user consent.	
77	Dolphin Browser that use a windowed interaction paradigm, shall offer a way to extend permission to individual trusted sites.	
78	Dolphin web browser shall support the prior designation of low-value site, which Self-Signed and Pinned Certificates are required, Handling with the TLS errors that could be a spoofing attack during the pinning of a new certificate to a destination by checking that DNS of a newly certificate is match to URI of the current site.	GM81

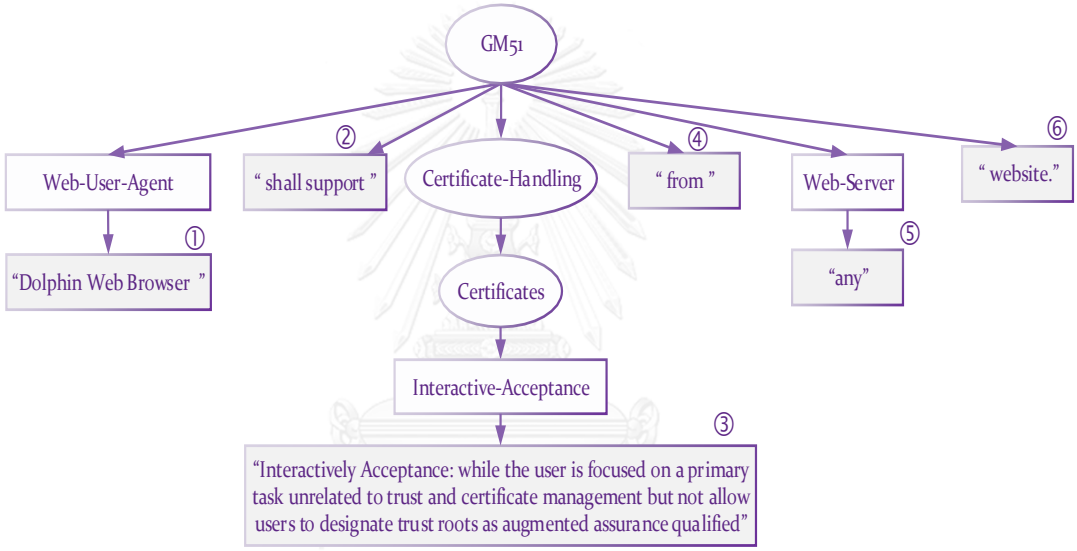
จากการประยุกต์ใช้ไวยากรณ์ความมั่นคงในการกำหนดความมั่นคงของกรณีศึกษาทั้ง 3 กรณี ได้รายการความต้องการความมั่นคงดังตารางข้างต้น ครอบคลุมทั้ง 18 ไวยากรณ์ โดยมีรายละเอียดเส้นทางของแต่ละไวยากรณ์ดังต่อไปนี้

5.2.1 การนำการรักษาความมั่นคงของชั้นขนส่งมาประยุกต์ใช้กับเว็บ

ไวยากรณ์กลุ่มนี้จะมุ่งเน้นการระบุความต้องการความมั่นคงด้านการรักษาความมั่นคงชั้นขนส่ง ประกอบด้วย 4 ไวยากรณ์ดังนี้

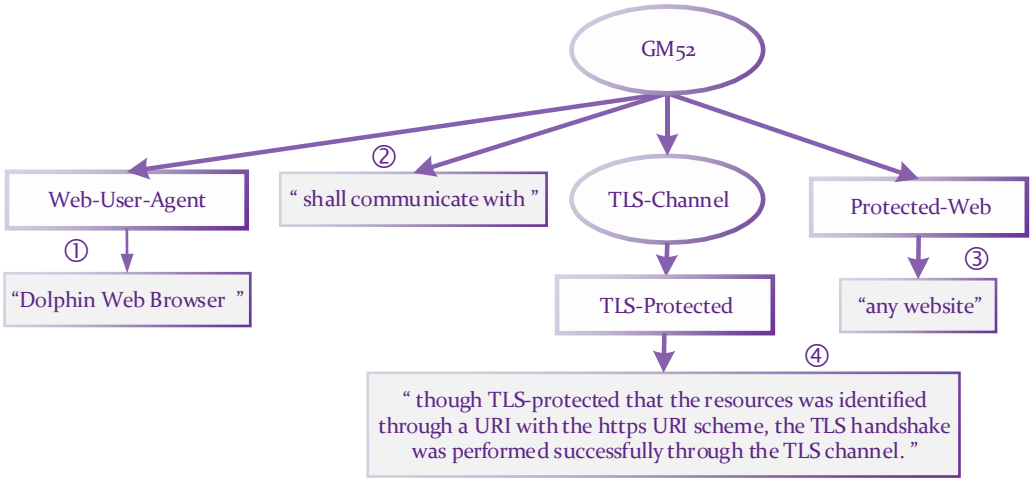
1) ไวยากรณ์ 51 การจัดการใบรับรองของเว็บ ประกอบด้วยนอนเทอร์มินัลหลัก ได้แก่ ตัวแทนผู้ใช้เว็บ (Web-User-Agent) การจัดการใบรับรอง (Certificate-Handling) และผู้ให้บริการ

เว็บ (Web-Server) ตัวอย่างความต้องการที่ได้จากไวยากรณ์นี้ คือข้อความที่ 1-4 ในตารางที่ 5.1 โดยแสดงตัวอย่างลำดับการได้มาซึ่งความต้องการปรากฏดังภาพที่ 5.2 ตัวอย่างผลลัพธ์ความต้องการความมั่นคงที่ได้จากการนำเทอร์มินัลโนดของไวยากรณ์นี้มาต่อกันโดยใช้บริบทกรณีศึกษาที่ 3 ระบบค้นดูเว็บ คือ “Dolphin Web Browser shall support Interactively Acceptance: while the user is focused on a primary task unrelated to trust and certificate management but not allow users to designate trust roots as augmented assurance qualified, Trust Anchor installation: that is handled by user agent vendors and device manufacturers based on out-of-band information and Trust Anchor update: that is handled as part of operating system software updates for any certificates form any website.”



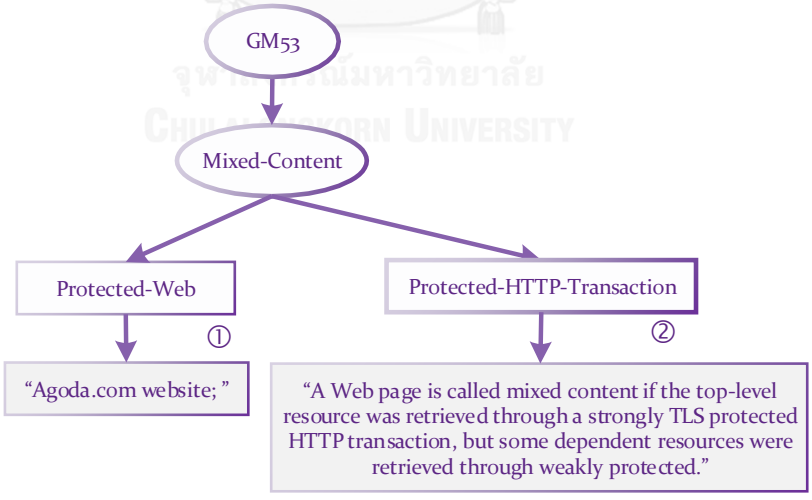
ภาพที่ 5.2 การประยุกต์ใช้ไวยากรณ์การจัดการใบรับรองเว็บ

2) ไวยากรณ์ 52 การกำหนดระดับความมั่นคงของการเชื่อมต่อกับผู้ให้บริการเว็บประกอบด้วยนอนเทอร์มินัลหลัก ได้แก่ ตัวแทนผู้ใช้เว็บ (Web-User-Agent) ช่องทางการรักษาความมั่นคงชั้นขนส่ง (TLS-Chanel) และผู้ให้บริการเว็บที่ได้รับการปกป้อง (Protected-Web) แสดงตัวอย่างลำดับการได้มาซึ่งความต้องการปรากฏดังภาพที่ 5.3 ผลลัพธ์ความต้องการความมั่นคงที่ได้จากการนำเทอร์มินัลโนดมาต่อกันโดยใช้กรณีศึกษาที่ 3 ระบบค้นดูเว็บ คือ “Dolphin Web Browser shall communicate with any websites though TLS-protected that the resources was identified through a URI with the https URI scheme, the TLS handshake was performed successfully through the TLS channel.”



ภาพที่ 5.3 การประยุกต์ใช้ไวยากรณ์การกำหนดความมั่นคงของการเชื่อมต่อผู้ให้บริการเว็บ

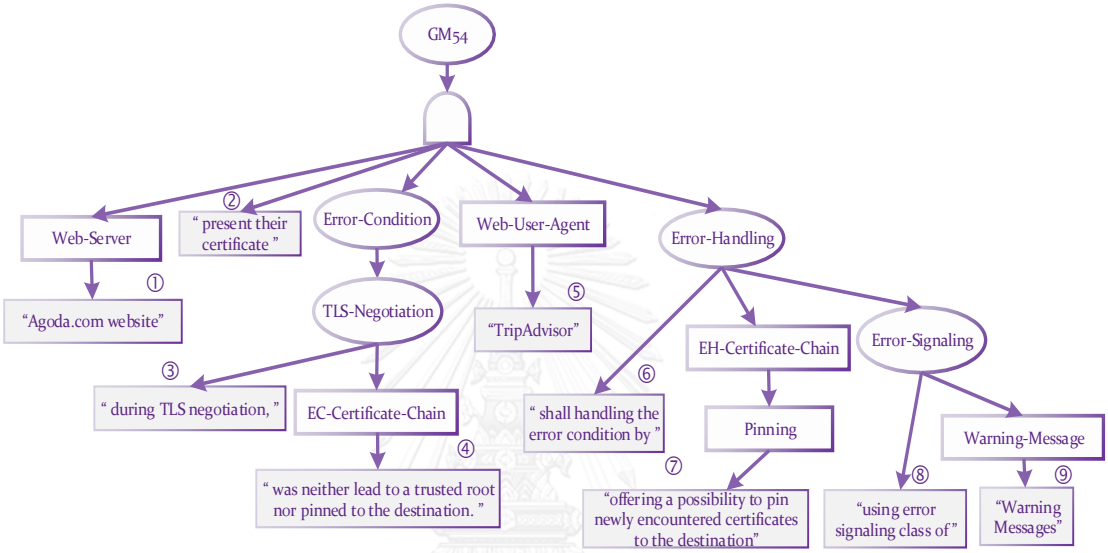
3) ไวยากรณ์ 53 การกำหนดประเภทของเว็บจากการรักษาความมั่นคงชั้นขนส่ง ประกอบด้วยนอนเทอร์มินัลหลัก ได้แก่ การรักษาความมั่นคงชั้นขนส่ง (TLS-Secured) และเนื้อหาแบบผสม (Mixed-Content) โดยแสดงตัวอย่างลำดับการได้มาซึ่งความต้องการดังภาพที่ 5.4 ผลลัพธ์ที่ได้จากการนำเทอร์มินัลโนดของไวยากรณ์นี้มาต่อกันโดยใช้บริบทกรณีศึกษาที่ 2 ระบบสำรองห้องพักและเที่ยวบิน คือ "Agoda.com website; A Web page is called mixed content if the top-level resource was retrieved through a strongly TLS protected HTTP transaction, but some dependent resources were retrieved through weakly protected."



ภาพที่ 5.4 การประยุกต์ใช้ไวยากรณ์กำหนดประเภทของเว็บจากการรักษาความมั่นคงชั้นขนส่ง

4) ไวยากรณ์ 54 ทางเลือกการจัดการข้อผิดพลาดที่เกิดขึ้นขณะเชื่อมต่อการรักษาความมั่นคงชั้นขนส่ง ประกอบด้วยนอนเทอร์มินัลหลัก ได้แก่ เงื่อนไขข้อผิดพลาด (Error-Condition) และการจัดการข้อผิดพลาด (Error-Handling) โดยแสดงตัวอย่างลำดับการได้มาซึ่งความต้องการปรากฏ

ดังภาพที่ 5.5 ผลลัพธ์ที่ได้จากการนำเทอร์มินัลโนดของไวยากรณ์นี้มาต่อกันโดยใช้บริบทกรณีศึกษาที่ 2 ระบบสำรองห้องพักและเที่ยวบิน คือ “Agoda.com website present their certificate during TLS negotiation, was neither lead to a trusted root nor pinned to the destination. TripAdvisor shall handling the error condition by using error signaling class of Warning Messages or higher and offering a possibility to pin newly encountered certificates to the destination.”

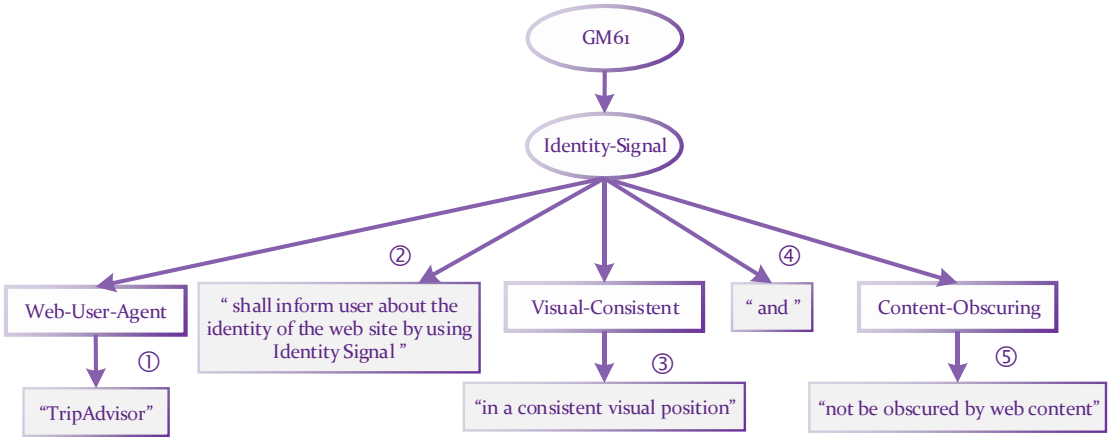


ภาพที่ 5.5 การประยุกต์ใช้ไวยากรณ์กำหนดทางเลือกการจัดการข้อผิดพลาด

5.2.2 ตัวชี้บอกและการมีปฏิสัมพันธ์

ไวยากรณ์กลุ่มนี้จะมุ่งเน้นการกำหนดความต้องการความมั่นคงของผลตัวชี้บอกเพื่อแสดงสถานะของการรักษาความมั่นคงชั้นขนส่งและการมีปฏิสัมพันธ์ ประกอบด้วย 4 ไวยากรณ์ดังนี้

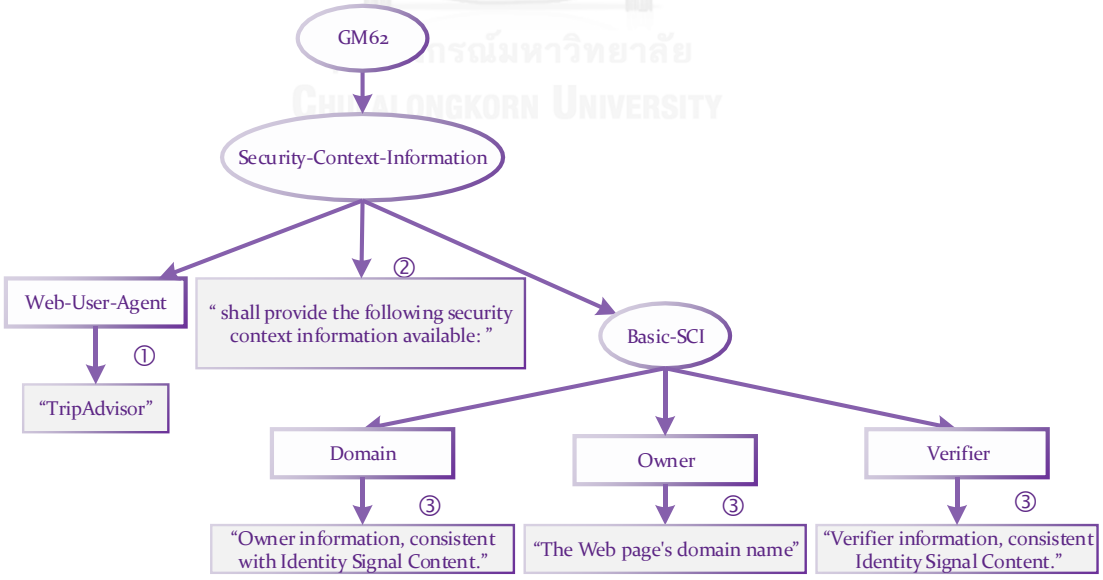
1) ไวยากรณ์ 61 การส่งสัญญาณอัตลักษณ์ของเว็บ ประกอบด้วยนอนเทอร์มินัลหลัก ได้แก่ คุณลักษณะของสัญญาณ (Signal-Specification) การส่งสัญญาณอัตลักษณ์ (Identity-Signal) และเนื้อหาของสัญญาณอัตลักษณ์ (Identity-Signal-Content) โดยแสดงตัวอย่างลำดับการได้มาซึ่งความต้องการปรากฏดัง ผลลัพธ์ที่ได้จากการนำเทอร์มินัลโนดของไวยากรณ์นี้มาต่อกันโดยใช้บริบทกรณีศึกษาที่ 2 ระบบสำรองที่พักและเที่ยวบิน คือ “TripAdvisor shall inform user about the identity of the web site by using Identity Signal, in a consistent visual position and not be obscured by web content.”



ภาพที่ 5.6 การประยุกต์ใช้ไวยากรณ์การส่งสัญญาณอัตลักษณ์ของเว็บ

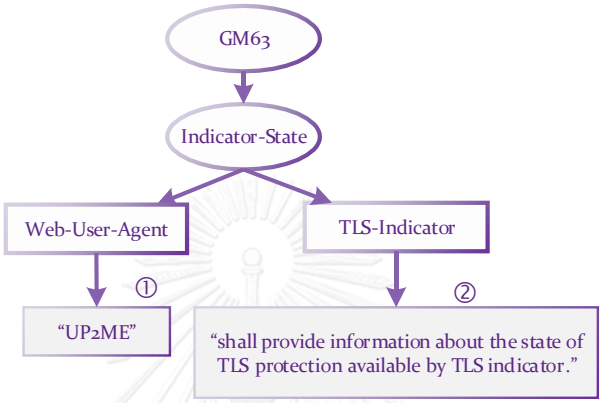
2) ไวยากรณ์ 62 การกำหนดของข้อมูลเพิ่มเติมที่เกี่ยวข้องกับบริบทความมั่นคงเชิงเว็บ ประกอบด้วยนอนเทอร์มินัลหลัก คือ ข้อมูลบริบทความมั่นคงเชิงเว็บ (Security Context Information) โดยแสดงตัวอย่างลำดับการได้มาซึ่งความต้องการปรากฏดังภาพที่ 5.7 ผลลัพธ์ที่ได้จากการนำเทอร์มินัลโนดของไวยากรณ์นี้มาต่อกันโดยใช้บริบทกรณีศึกษาที่ 2 ระบบสำรองที่พักและเที่ยวบิน คือ "TripAdvisor shall provide the following security context information available:

- The Web page's domain name
- Owner information, consistent with Identity Signal Content.
- Verifier information, consistent Identity Signal Content."



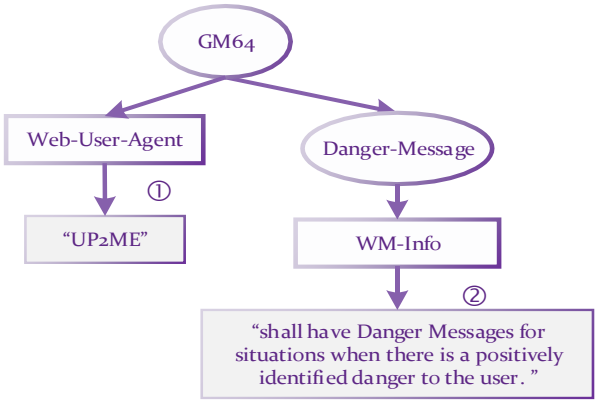
ภาพที่ 5.7 การประยุกต์ใช้ไวยากรณ์กำหนดของข้อมูลเพิ่มเติมที่เกี่ยวข้องกับบริบทความมั่นคงเชิงเว็บ

3) ไวยากรณ์ 63 การกำหนดความต้องการของตัวชี้บอกการรักษาความมั่นคงชั้นขนส่ง ประกอบด้วยนอนเทอร์มินัลทางเลือกหลัก 3 ทางเลือกได้แก่ สถานะของตัวชี้บอก (Indicator-State) คุณภาพของตัวชี้บอก (Indicator-Quality) และการแสดงผลของตัวชี้บอก (Indicator-Mode) โดยแสดงตัวอย่างลำดับการได้มาซึ่งความต้องการปรากฏดังภาพที่ 5.8 ผลลัพธ์ที่ได้จากการนำเทอร์มินัลโนดของไวยากรณ์นี้มาต่อกันโดยใช้บริบทกรณีศึกษาที่ 1 ธนาคารอิเล็กทรอนิกส์ คือ “UP2ME shall provide information about the state of TLS protection available by TLS indicator. ”



ภาพที่ 5.8 การประยุกต์ใช้ไวยากรณ์กำหนดความต้องการของตัวชี้บอกการรักษาความมั่นคงชั้นขนส่ง

4) ไวยากรณ์ 64 การจัดการข้อผิดพลาด ประกอบด้วยนอนเทอร์มินัลหลัก 4 ทางเลือกได้แก่ การส่งสัญญาณข้อผิดพลาดบนส่วนต่อประสานผู้ใช้แบบปฐมภูมิ (ES-Primary-UI) ข้อความเตือนภัย (Danger-Message) ข้อความแจ้งเตือน (Warning-Message) และตัวชี้บอกข้อผิดพลาด (Error-Indicator) โดยแสดงตัวอย่างลำดับการได้มาซึ่งความต้องการปรากฏดังภาพที่ 5.9 ผลลัพธ์ที่ได้จากการนำเทอร์มินัลโนดของไวยากรณ์นี้มาต่อกันโดยใช้บริบทกรณีศึกษาที่ 1 ธนาคารอิเล็กทรอนิกส์ คือ “UP2ME shall have Danger Messages for situations when there is a positively identified danger to the user.”

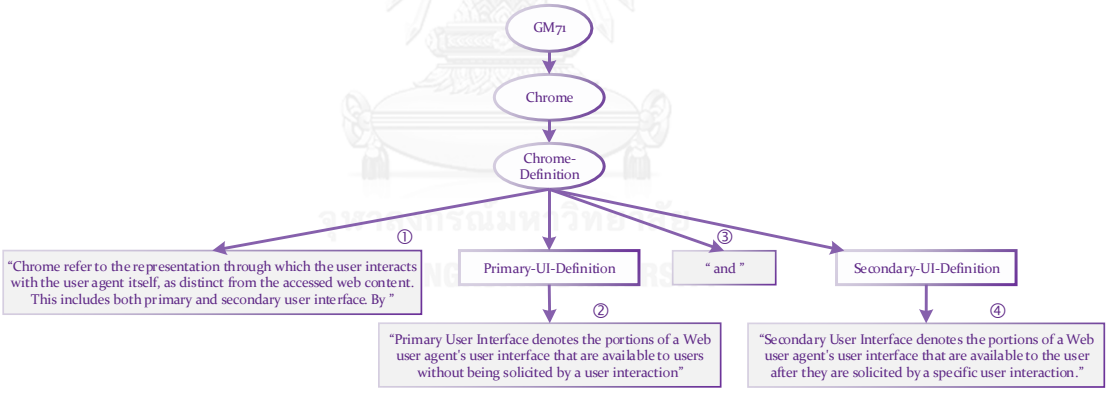


ภาพที่ 5.9 การประยุกต์ใช้ไวยากรณ์การจัดการข้อผิดพลาด

5.2.3 แนวทางที่ดีที่สุดสำหรับสภาพทนทาน

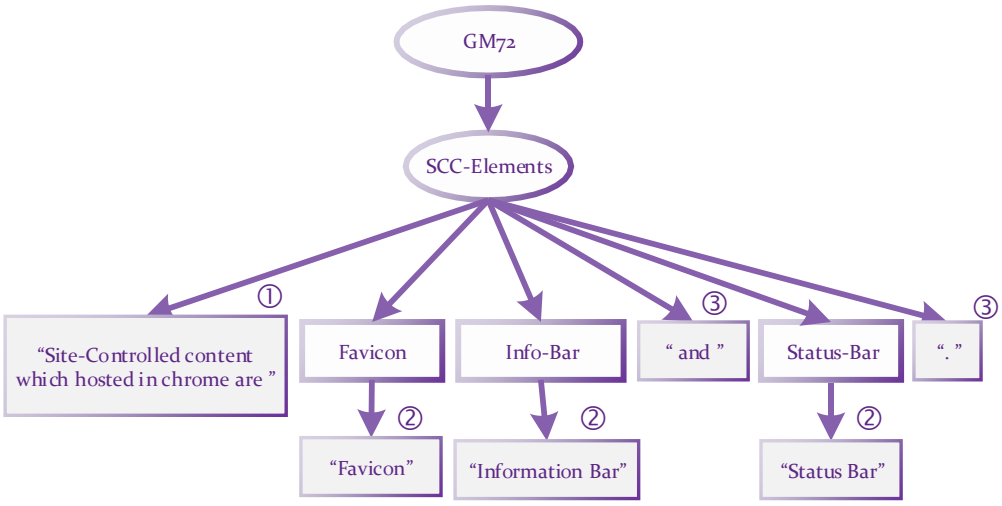
ไวยากรณ์กลุ่มนี้จะมุ่งเน้นการระบุความต้องการความมั่นคงเพื่อปิดช่องโหว่ที่เสี่ยงต่อการถูกโจมตีด้านบริบทความมั่นคงของระบบ ประกอบด้วย 4 ไวยากรณ์ดังนี้

1) ไวยากรณ์ 71 การกำหนดความต้องการส่วนต่อประสานผู้ใช้โครมประกอบด้วยนอนเทอร์มินัลหลัก ได้แก่ โครม (Chrome) และส่วนต่อประสานผู้ใช้ (User-Interface) โดยแสดงตัวอย่างลำดับการได้มาซึ่งความต้องการปรากฏดังภาพที่ 5.10 ผลลัพธ์ที่ได้จากการนำเทอร์มินัลโนดของไวยากรณ์นี้มาต่อกันโดยไม่พึ่งพิงบริบท คือ “Chrome refer to the representation through which the user interacts with the user agent itself, as distinct from the accessed web content. This includes both primary and secondary user interface. By Primary User Interface denotes the portions of a Web user agent's user interface that are available to users without being solicited by a user interaction and Secondary User Interface denotes the portions of a Web user agent's user interface that are available to the user after they are solicited by a specific user interaction.”



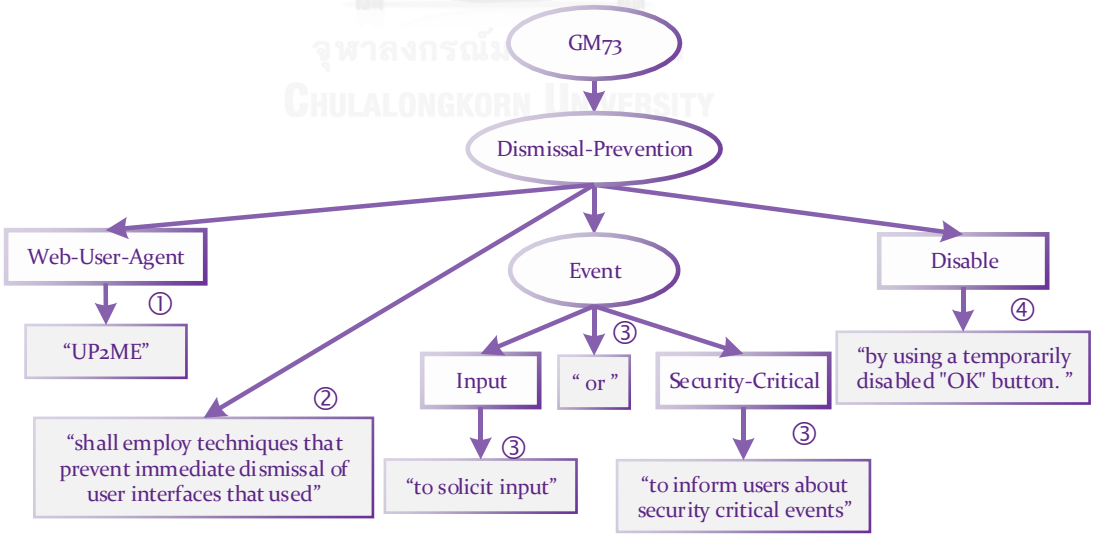
ภาพที่ 5.10 การประยุกต์ใช้ไวยากรณ์กำหนดส่วนต่อประสานผู้ใช้โครม

2) ไวยากรณ์ 72 การกำหนดความต้องการสำหรับส่วนต่อประสานผู้ใช้ที่สามารถควบคุมได้โดยเนื้อหาเว็บเพื่อป้องกันการลอกเลียนตัวชี้บอกความมั่นคงประกอบด้วยนอนเทอร์มินัลหลัก ได้แก่ องค์ประกอบที่สามารถควบคุมด้วยเนื้อหาจากเว็บไซต์ (SCC-Elements) และการเลียนแบบตัวชี้บอก (Mimic-Indicator) โดยแสดงตัวอย่างลำดับการได้มาซึ่งความต้องการปรากฏดังภาพที่ 5.11 ผลลัพธ์ที่ได้จากการนำเทอร์มินัลโนดของไวยากรณ์นี้มาต่อกันโดยไม่พึ่งพิงบริบท คือ “Site-Controlled content which hosted in chrome are Favicon, Information Bar, and Status Bar.”



ภาพที่ 5.11 การประยุกต์ใช้ไวยากรณ์กำหนดส่วนต่อประสานผู้ใช้ที่สามารถควบคุมได้โดยเนื้อหาเว็บ

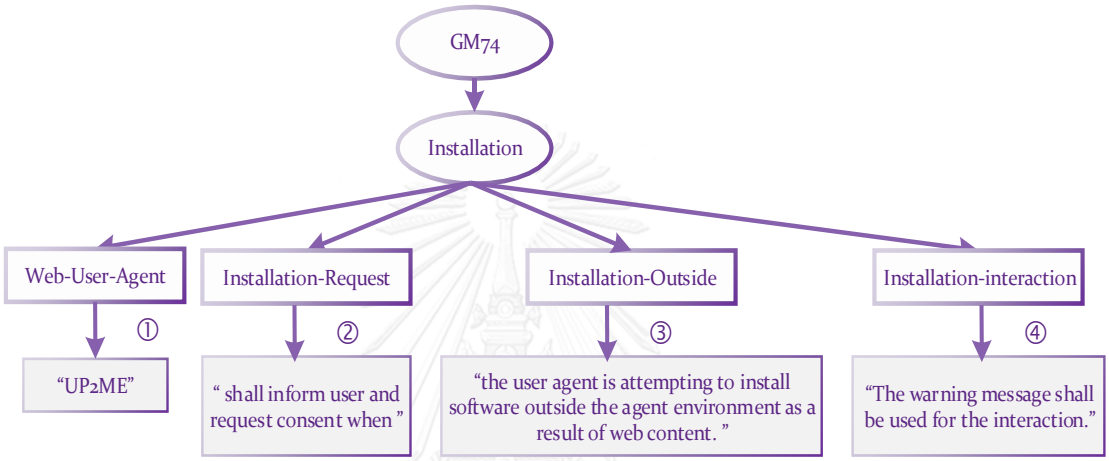
3) ไวยากรณ์ 73 การป้องการโจมตีผ่านปฏิสัมพันธ์ ประกอบด้วยนอนเทอร์มินัลหลัก ได้แก่ เทคนิคป้องกันการยกเลิกได้ทันที (Dismissal-Prevention) การยินยอมให้ควบคุม (Granted-Control) และการแสดงกล่องโต้ตอบ (Display-Dialog) โดยแสดงตัวอย่างลำดับการได้มาซึ่งความต้องการปรากฏดังภาพที่ 5.12 ผลลัพธ์ที่ได้จากการนำเทอร์มินัลโนดของไวยากรณ์นี้มาต่อกันโดยใช้บริบทกรณีศึกษาที่ 1 ธนาคารอิเล็กทรอนิกส์ คือ "The UP2ME shall employ techniques that prevent immediate dismissal of user interfaces that used to inform users about security critical events or to solicit input by using a temporarily disabled "OK" button. "



ภาพที่ 5.12 การประยุกต์ใช้ไวยากรณ์การป้องการโจมตีผ่านปฏิสัมพันธ์

4) ไวยากรณ์ 74 กำหนดความต้องการด้านความมั่นคงสำหรับตัวแทนผู้ใช้เว็บที่รองรับส่วนต่อประสานโปรแกรมประยุกต์ ประกอบด้วยนอนเทอร์มินัลหลัก ได้แก่ การปกปิดหรือคลุมเครือส่วน

ต่อประสานผู้ใช้ (Obscuring) การติดตั้งซอฟต์แวร์ (Installation) การคั่นหน้าเว็บ (Bookmarking) และส่วนต่อประสานโปรแกรมประยุกต์ของหน้าต่าง (Window-API) โดยแสดงตัวอย่างลำดับการได้มาซึ่งความต้องการปรากฏดังภาพที่ 5.13 ผลลัพธ์ที่ได้จากการนำเทอร์มินัลโนดของไวยากรณ์นี้มาต่อกันโดยใช้บริบทกรณีศึกษาที่ 1 ธนาคารอิเล็กทรอนิกส์ คือ “UP2ME shall inform user and request consent when the user agent is attempting to install software outside the agent environment as a result of web content. The warning message shall be used for the interaction. ”

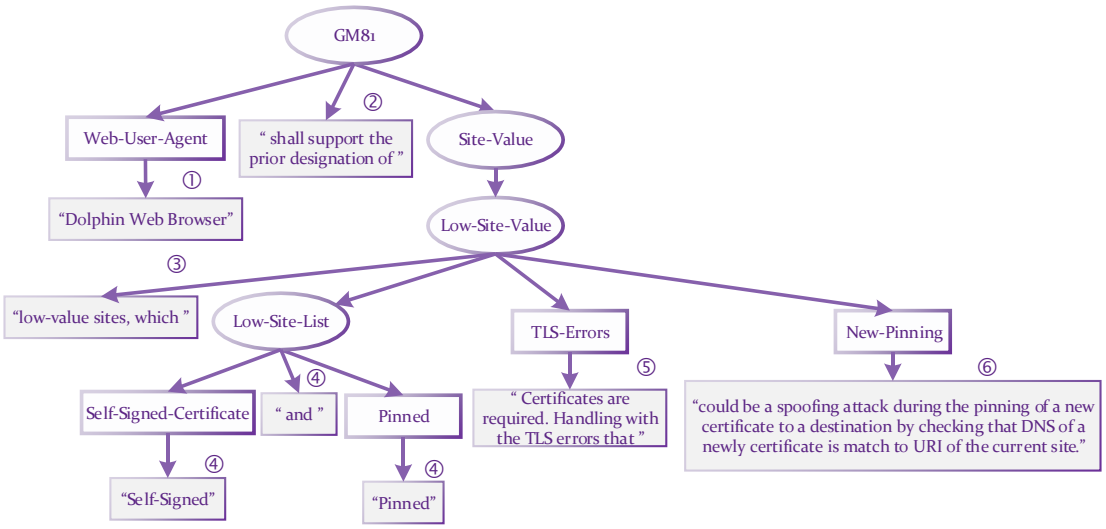


ภาพที่ 5.13 การประยุกต์ใช้ไวยากรณ์กำหนดส่วนต่อประสานโปรแกรมประยุกต์ของตัวแทนผู้ใช้เว็บ

5.2.4 ข้อคำนึงด้านความมั่นคง

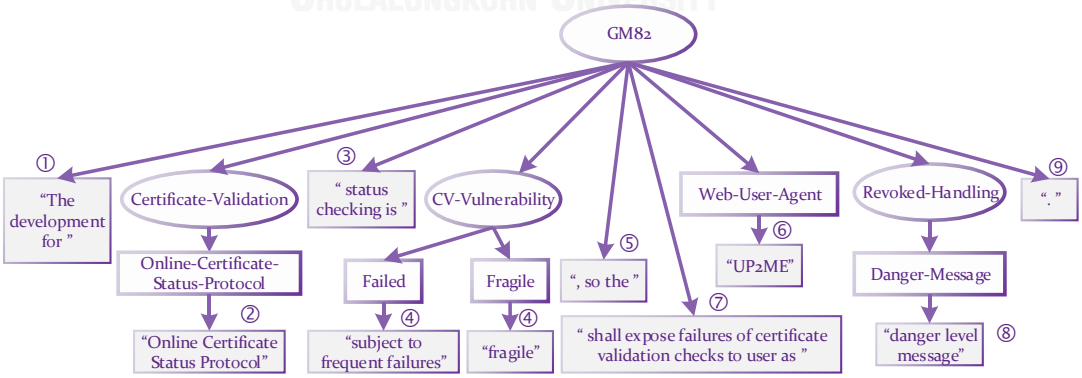
ไวยากรณ์กลุ่มนี้จะมุ่งเน้นการระบุความต้องการความมั่นคงเพื่อปิดช่องโหว่ที่เสี่ยงต่อการถูกโจมตีระบบ ประกอบด้วย 6 ไวยากรณ์ดังนี้

1) ไวยากรณ์ 81 การป้องกันการโจมตีด้วยใบรับรองระหว่างการเชื่อมต่อการรักษาความมั่นคงชั้นขนส่ง ประกอบด้วยนอนเทอร์มินัลหลัก คือการกำหนดมูลค่าของเว็บไซต์ (Site-Value) โดยแสดงตัวอย่างลำดับการได้มาซึ่งความต้องการปรากฏดังภาพที่ 5.14 ผลลัพธ์ที่ได้จากการนำเทอร์มินัลโนดของไวยากรณ์นี้มาต่อกันโดยใช้บริบทกรณีศึกษาที่ 3 ระบบค้นดูเว็บ คือ “Dolphin web browser shall support the prior designation of low-value site, which Self-Signed and Pinned Certificates are required, Handling with the TLS errors that could be a spoofing attack during the pinning of a new certificate to a destination by checking that DNS of a newly certificate is match to URI of the current site.”



ภาพที่ 5.14 การประยุกต์ใช้ไวยากรณ์การป้องกันการโจมตีด้วยใบรับรอง
ระหว่างการเชื่อมต่อการรักษาความมั่นคงชั้นขนส่ง

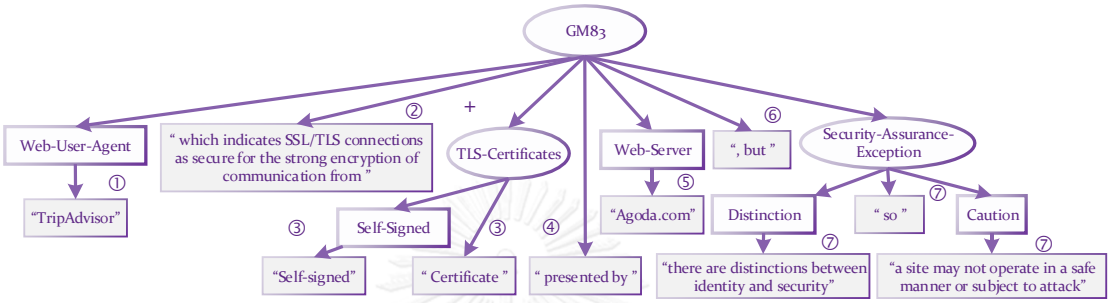
2) ไวยากรณ์ 82 การป้องกันการโจมตีการตรวจสอบสถานะใบรับรอง ประกอบด้วยนอนเทอร์มินัลหลัก ได้แก่ การตรวจสอบความถูกต้องของใบรับรอง (Certificate-Validation) จุดอ่อนของการตรวจสอบใบรับรอง (CV-Vulnerability) และการจัดการกับการเพิกถอนใบรับรอง (Revoked-Handling) โดยแสดงตัวอย่างลำดับการได้มาซึ่งความต้องการปรากฏดังภาพที่ 5.15 ผลลัพธ์ที่ได้จากการนำเทอร์มินัลโนดของไวยากรณ์นี้มาต่อกันโดยใช้บริบทกรณีศึกษาที่ 1 ธนาคารอิเล็กทรอนิกส์ คือ “The development for Online Certificate Status Protocol status checking is fragile and subject to frequent failures, so the UP2ME shall expose failures of certificate validation checks to user as danger level message.”



ภาพที่ 5.15 การประยุกต์ใช้ไวยากรณ์การป้องกันการโจมตีการตรวจสอบสถานะใบรับรอง

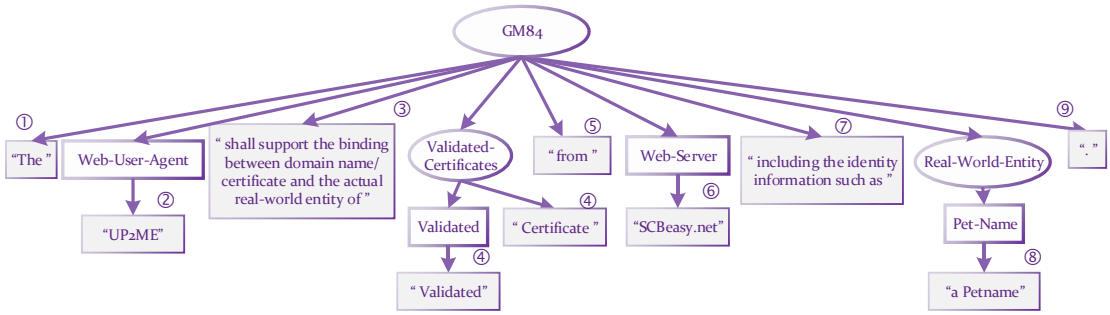
3) ไวยากรณ์ 83 การกำหนดข้อยกเว้นในการประกันความมั่นคงของเว็บ ประกอบด้วยนอนเทอร์มินัลหลัก ได้แก่ รายการใบรับรองที่ใช้ในการรักษาความมั่นคงชั้นขนส่ง (TLS-Certificates) และข้อยกเว้นการรับประกันด้านความมั่นคง (Security-Assurance-Exception) โดยแสดงตัวอย่างลำดับ

การได้มาซึ่งความต้องการปรากฏดังภาพที่ 5.16 ผลลัพธ์ที่ได้จากการนำเทอร์มินัลโนดของไวยากรณ์นี้มาต่อกันโดยใช้บริบทกรณีศึกษาที่ 2 ระบบสำรองห้องพักและเที่ยวบิน คือ “TripAdvisor which indicates SSL/TLS connections as secure for the strong encryption of communication from Self-signed certificate presented by Agoda.com, but there are distinctions between identity and security so a site may not operate in a safe manner or subject to attack. ”



ภาพที่ 5.16 การประยุกต์ใช้ไวยากรณ์กำหนดข้อยกเว้นในการประกันความมั่นคงของ

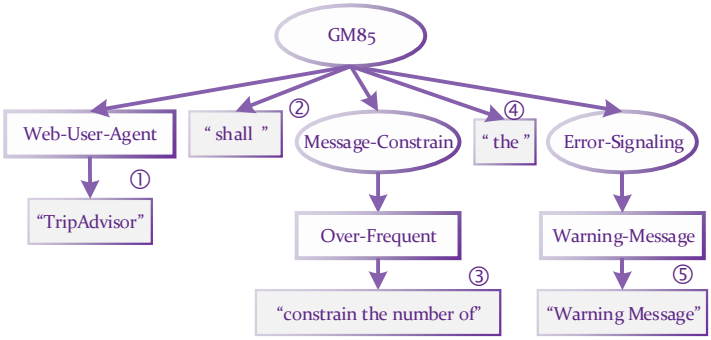
4) ไวยากรณ์ 84 การกำหนดข้อมูลอัตลักษณ์ที่สอดคล้องกับโลกความจริง ประกอบด้วยนอนเทอร์มินัลหลัก ได้แก่ ใบรับรองที่ผ่านการตรวจสอบความสมเหตุสมผล (Validated-Certificates) และข้อมูลที่สอดคล้องกับโลกความจริง (Real-World-Entity) โดยแสดงตัวอย่างลำดับการได้มาซึ่งความต้องการปรากฏดังภาพที่ 5.17 ผลลัพธ์ที่ได้จากการนำเทอร์มินัลโนดของไวยากรณ์นี้มาต่อกันโดยใช้บริบทกรณีศึกษาที่ 1 ธนาคารอิเล็กทรอนิกส์ คือ “The UP2ME shall support the binding between domain name/certificate and the actual real-world entity of Validated Certificate from SCBeasy.net including the identity information such as a Petname.”



ภาพที่ 5.17 การประยุกต์ใช้ไวยากรณ์กำหนดข้อมูลอัตลักษณ์ที่สอดคล้องกับโลกความจริง

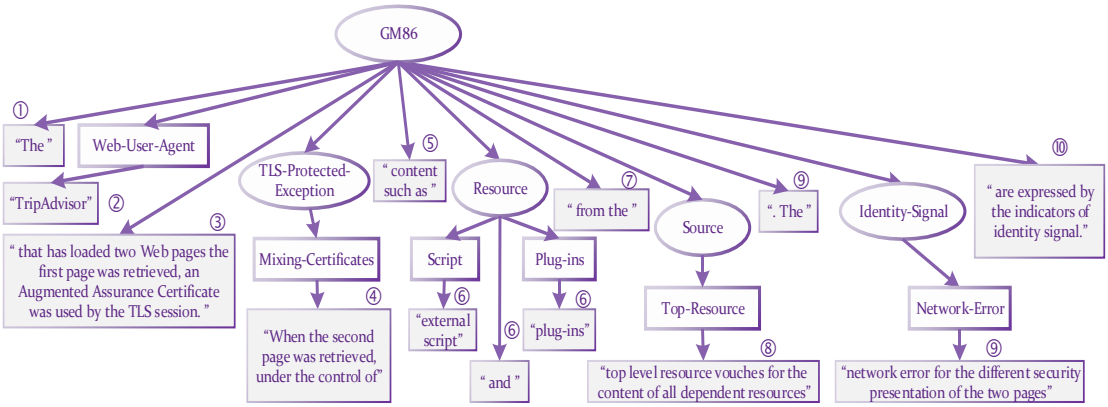
5) ไวยากรณ์ 85 การกำหนดข้อจำกัดของข้อความแจ้งเตือน ประกอบด้วยนอนเทอร์มินัลหลัก ได้แก่ การส่งสัญญาณข้อผิดพลาด (Error-Signaling) และข้อจำกัดในการแสดงข้อความ (Message-Constrain) โดยแสดงลำดับการได้มาซึ่งความต้องการปรากฏดังภาพที่ 5.18 ผลลัพธ์ที่ได้

จากการนำเทอร์มินัลโนดของไวยากรณ์นี้มาต่อกันโดยใช้บริบทกรณีศึกษาที่ 2 ระบบสำรองที่พักและเที่ยวบิน คือ “TripAdvisor shall constrain the number of the Warning Message.”



ภาพที่ 5.18 การประยุกต์ใช้ไวยากรณ์การกำหนดข้อจำกัดของข้อความแจ้งเตือน

6) ไวยากรณ์ 86 การกำหนดสัญญาณอัตลักษณ์ของเว็บที่มีการเปลี่ยนแปลงเนื้อหา ประกอบด้วยนอนเทอร์มินัลหลัก ได้แก่ ข้อยกเว้นการรักษาความมั่นคงชั้นขนส่ง (TLS-Protected-Exception) แหล่งที่มา (Source) ทรัพยากร (Resource) และสัญญาณอัตลักษณ์ (Identity-Signal) โดยแสดงลำดับการได้มาซึ่งความต้องการปรากฏดังภาพที่ 5.19 ผลลัพธ์ที่ได้จากการนำเทอร์มินัลโนดของไวยากรณ์นี้มาต่อกันโดยใช้บริบทกรณีศึกษาที่ 2 ระบบสำรองที่พักและเที่ยวบิน คือ “The TripAdvisor that has loaded two Web pages the first page was retrieved, an Augmented Assurance Certificate was used by the TLS session. When the second page was retrieved, under the control of content such as external script and plug-ins from the top level resource vouches for the content of all dependent resources. The network error for the different security presentation of the two pages are expressed by the indicators of identity signal.”

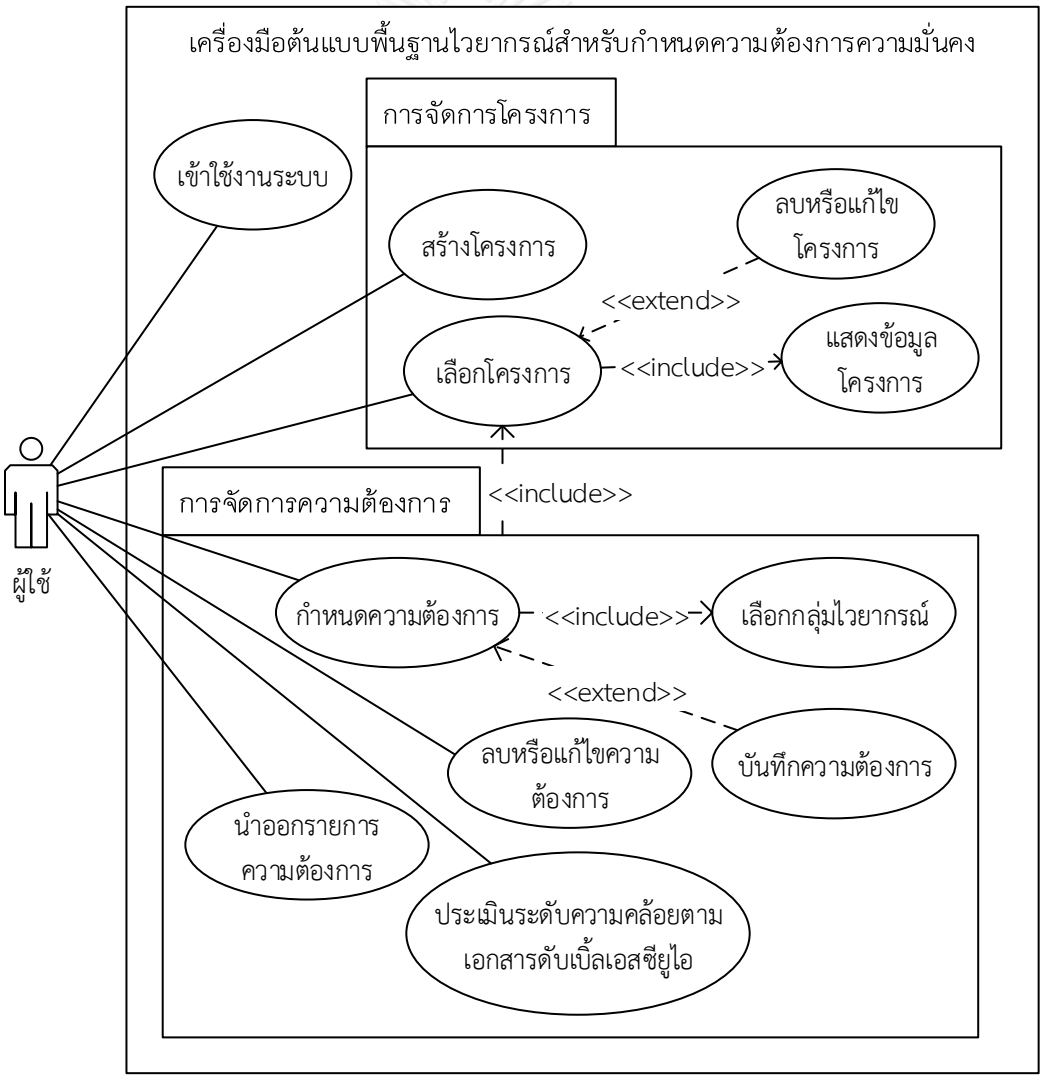


ภาพที่ 5.19 การประยุกต์ใช้ไวยากรณ์กำหนดสัญญาณอัตลักษณ์ของเว็บที่มีการเปลี่ยนแปลงเนื้อหา

บทที่ 6
การออกแบบและพัฒนาเครื่องมือต้นแบบ

ในบทนี้จะกล่าวถึงการออกแบบและพัฒนาเครื่องมือต้นแบบพื้นฐานไวยากรณ์ความมั่นคงในการกำหนดความต้องการความมั่นคงของตัวแทนผู้ใช้เว็บที่สนับสนุนแนวคิดและวิธีวิจัยข้างต้น โดยระบุความต้องการเชิงหน้าที่ของระบบ ออกแบบสถาปัตยกรรมและโครงสร้างการจัดเก็บข้อมูล ระบุเครื่องมือสนับสนุนการพัฒนา อธิบายหลักการการฝังตัวของไวยากรณ์ความมั่นคง แสดงลำดับการใช้งานและตัวอย่างส่วนต่อประสานผู้ใช้ ไปจนถึงทดสอบเครื่องมือต้นแบบ

6.1 ความต้องการเชิงหน้าที่



ภาพที่ 6.1 แผนภาพยูสเคสของเครื่องมือต้นแบบ

หน้าที่การทำงานของเครื่องมือต้นแบบที่สนับสนุนการกำหนดความต้องการความมั่นคง (Web User Agent Security Requirements Generator: WUASRG) นำเสนอด้วยแผนภาพยูสเคส (Use Case Diagram) อธิบายการติดต่อกันระหว่างผู้ใช้กับหน้าที่ของระบบ ดังภาพที่ 6.1 โดยมีรายละเอียดดังนี้

1) การเข้าใช้งานระบบ โดยผู้ใช้ทำการป้อนชื่อผู้ใช้และรหัสผ่านเพื่อเข้าใช้งาน

2) การจัดการโครงการ ผู้ใช้สามารถสร้างโครงการโดยป้อนข้อมูล ได้แก่ ชื่อโครงการ ผู้สนับสนุนโครงการ ชื่อระบบ และรายการผู้ให้บริการเว็บที่ติดต่อกับระบบ สามารถแก้ไขข้อมูลของโครงการ ไปจนถึงการลบโครงการ

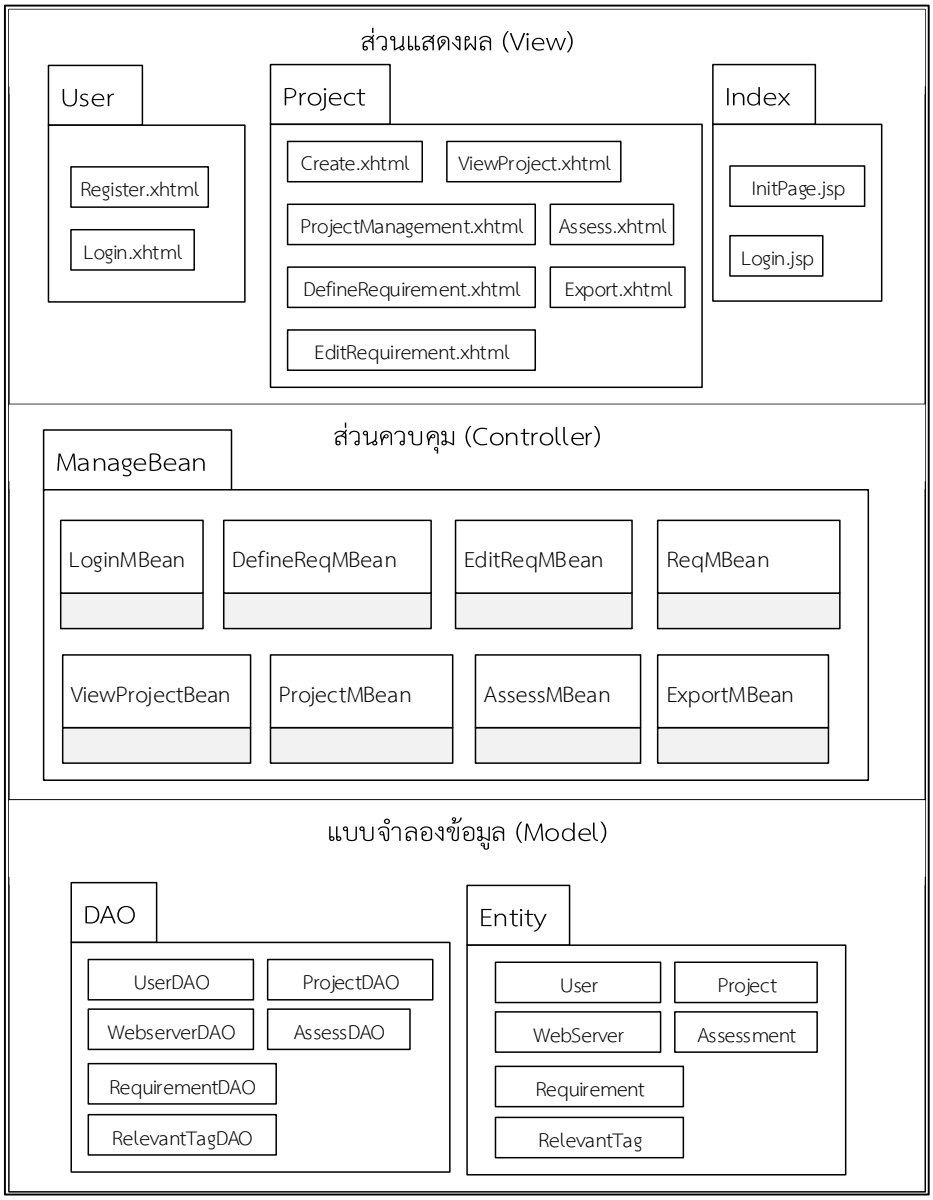
3) การจัดการรายการความต้องการของแต่ละโครงการ เมื่อผู้ใช้เลือกโครงการแล้ว ผู้ใช้สามารถกำหนดความต้องการโดยเลือกไวยากรณ์ที่ใช้ในการกำหนดความต้องการความมั่นคง เมื่อเข้าใช้งานระบบจะตรวจสอบเงื่อนไขก่อนการใช้งานว่ามีข้อมูลที่ต้องเรียกใช้จากไวยากรณ์อื่นหรือไม่ หากไม่พบข้อมูลที่ต้องกำหนดไว้ ระบบจะไม่อนุญาตให้กำหนดความต้องการจากไวยากรณ์ดังกล่าวได้ โดยการแสดงข้อความแจ้งเตือนให้ผู้ใช้กำหนดความต้องการของไวยากรณ์นั้นเสียก่อน จนกว่าข้อมูลจะครบตามเงื่อนไข ระบบจึงจะอนุญาตให้ผู้ใช้ป้อนข้อมูลและกดปุ่มยืนยันเพื่อทำการตรวจสอบความครบถ้วนของข้อมูลที่จำเป็นก่อนการบันทึก หากตรวจสอบพบว่าผู้ใช้กรอกข้อมูลที่จำเป็นไม่ครบ จะไม่สามารถบันทึกข้อมูลได้

4) การประเมินระดับความคล้อยตามเอกสารดับเบิ้ลยูเอสซียูไอ ระบบทำการตรวจสอบรายการความต้องการของแต่ละโครงการที่ผู้ใช้กำหนดว่าครอบคลุมข้อบังคับใดและเป็นจำนวนเท่าใด เมื่อเทียบกับเอกสารดับเบิ้ลยูเอสซียูไอ เพื่อประเมินระดับความคล้อยตามของโครงการ ดังที่ได้อธิบายไว้ในการวิเคราะห์เอกสารดับเบิ้ลยูเอสซียูไอในบทที่ 3 ความคล้อยตามแบ่งได้ 2 ระดับ คือ ระดับพื้นฐาน ระดับสูง โดยระดับพื้นฐานต้องกำหนดความต้องการครอบคลุมทุกข้อบังคับที่ต้องปฏิบัติ ในขณะที่ระดับสูงต้องกำหนดความต้องการครอบคลุมทุกข้อบังคับที่ต้องปฏิบัติ ทุกข้อควรปฏิบัติ และทุกข้อแนะนำ ระบบจะแสดงผลการประเมินผ่านแผงหน้าปัดสรุปจำนวนข้อกำหนดที่คล้อยตามข้อบังคับของเอกสารดับเบิ้ลยูเอสซียูไอ โดยแยกตามรหัสกำกับ “MS”, “SH” และ “MY”

5) การนำออกรายการความต้องการความมั่นคงในรูปแบบไฟล์เอกเซล (.xls) เพื่อนำไปใช้ภายนอกระบบ

6.2 การออกแบบสถาปัตยกรรมของเครื่องมือ

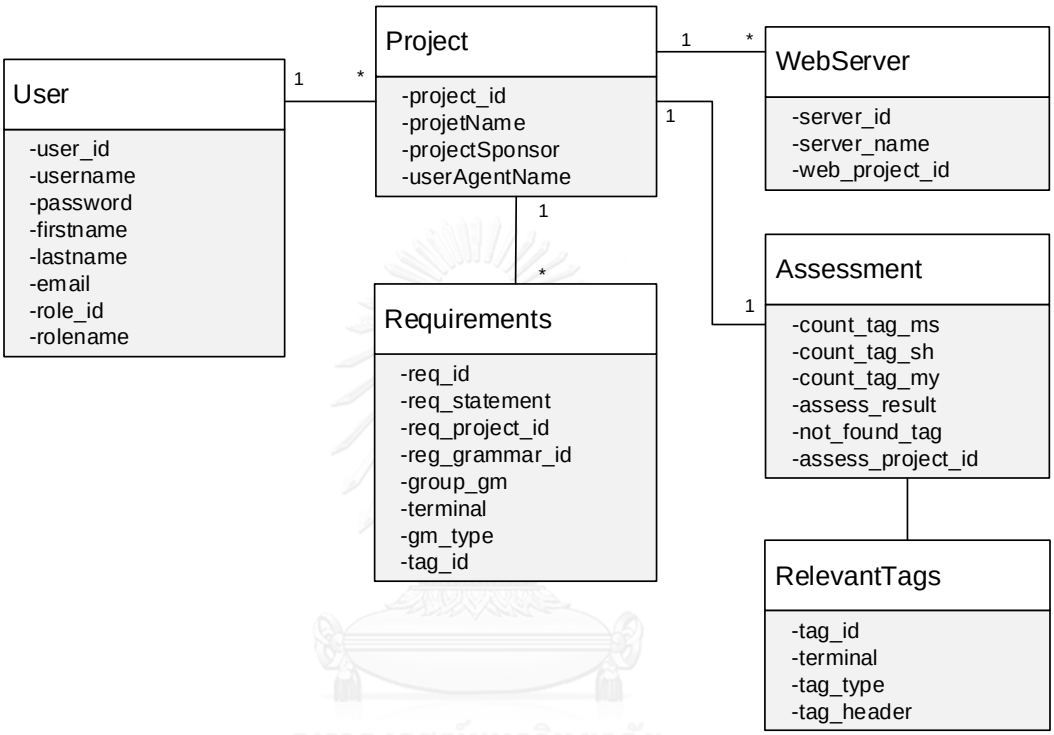
ระบบต้นแบบใช้กรอบงานจาวาเซิร์ฟเวอร์เฟส (Java Server Faces Framework) จึงได้รับคุณสมบัติด้านสถาปัตยกรรมแบบเอ็มวีซี (Model-View-Controller: MVC) ซึ่งเป็นส่วนหนึ่งของแบบรูปการออกแบบ (Design Patterns) ที่ช่วยในการแยกส่วนของของการพัฒนาโปรแกรมออกเป็น 3 ส่วน คือ ส่วนแสดงผล (View) ส่วนควบคุม (Controller) และแบบจำลองข้อมูล (Model) ดังภาพที่ 6.2 โดยส่วนแสดงผลบรรจุคำสั่งสำหรับส่วนต่อประสานที่ผู้ใช้มองเห็น ส่วนควบคุมบรรจุคลาสคำสั่งการคำนวณตรรกะเชิงธุรกิจ (Business Logic) และส่วนสุดท้ายแบบจำลองข้อมูลบรรจุคำสั่งจัดการฐานข้อมูล



ภาพที่ 6.2 สถาปัตยกรรมแบบเอ็มวีซีของระบบต้นแบบ

6.3 โครงสร้างการจัดเก็บข้อมูล

การจัดเก็บข้อมูลการกำหนดความต้องการโดยเครื่องมือต้นแบบด้วยฐานข้อมูลแบ่งออกเป็น 6 เอนทิตี คือ ข้อมูลผู้ใช้ (User) ข้อมูลโครงการ (Project) ข้อมูลผู้ให้บริการเว็บ (WebServer) ข้อมูลความต้องการ (Requirements) ข้อมูลการประเมิน (Assessment) และข้อมูลป้ายตามรอย (RelevantTags) ดังภาพที่ 6.3 แผนภาพคลาสแสดงแอตทริบิวต์และความสัมพันธ์ระหว่างเอนทิตี



ภาพที่ 6.3 แผนภาพคลาสของการจัดเก็บข้อมูลของระบบต้นแบบ

6.4 เครื่องมือสนับสนุนในการพัฒนา

การพัฒนาเครื่องมือต้นแบบใช้กรอบงานจาวาเซิร์ฟเวอร์เฟส หรือเจเอสเอฟ (Java Server Faces Framework: JSF) โดยมีซอฟต์แวร์ (Software) และฮาร์ดแวร์ (Hardware) ที่สนับสนุนมีคุณสมบัติ ดังนี้

6.4.1 ด้านซอฟต์แวร์

1) ระบบปฏิบัติการไมโครซอฟท์วินโดวส์ 10 โปร (Microsoft Windows 10 Pro)
2) โปรแกรมอีคลิปส์มาร์ส เวอร์ชัน 4.5.0 (Eclipse Mars version 4.5.0)
3) ไพร์มเฟส (PrimeFaces version 5.3) ส่วนต่อประสานผู้ใช้สำหรับกรอบงานเจเอสเอฟ

4) อะแพชีทอมแคท เวอร์ชัน 7.0.41 (Apache Tomcat version 7.0.41) โปรแกรมกำหนดสภาพแวดล้อมสำหรับภาษาจาวาเพื่อทำงานบนเว็บเซิร์ฟเวอร์ (Web Server)

5) โปรแกรมนาวิแคท พรีเมี่ยม เวอร์ชัน 9.1.8 (Navicat Premium 9.1.8) สำหรับฐานข้อมูลมายเอสคิวแอล (MySQL)

6) โปรแกรมแซมป์ เวอร์ชัน 3.2.1 (XAMPP version 3.2.1) โปรแกรมสำหรับจำลองเว็บเซิร์ฟเวอร์

6.4.2 ด้านฮาร์ดแวร์

1) เครื่องคอมพิวเตอร์ส่วนบุคคล หน่วยประมวลผลอินเทลคอร์ไอ 5 ความเร็ว 2.27 กิกะเฮิรตซ์ (Intel(R) Core(TM) i5 CPU M430 2.27GHz)

2) หน่วยความจำสำรอง (Memory) ความเร็ว 4 กิกะไบต์ (Ram 4 GB)

3) จานบันทึกแบบเข็ง (Hard disk) ความจุ 500 กิกะไบต์ (HDD 500 GB)

4) กราฟิกการ์ด (Graphic Card) อิเทล เอชดี กราฟิก (Intel HD Graphic)

6.5 การฝังตัวไวยากรณ์ความมั่นคงลงในเครื่องมือต้นแบบ

ไวยากรณ์ความมั่นคงที่นำเสนอจะถูกนำมาเป็นพื้นฐานในการสร้างเครื่องมือ การฝังตัวไวยากรณ์ความมั่นคงลงในเครื่องมือต้นแบบทำได้โดยใช้ประโยชน์จากการเขียนคำสั่งบีน (Bean) ของกรอบงานเจเอสเอฟ โดยแต่ละไวยากรณ์จะถูกนำมาเขียนบีนเพื่อควบคุมนอนเทอร์มินัลและเทอร์มินัลตามความสัมพันธ์ที่กำหนดไว้ในไวยากรณ์ แล้วรวมชุดข้อความ (Bundle Message) เพื่อแสดงผลลัพธ์ความต้องการตามที่ผู้ใช้กำหนด

ระหว่างการกำหนดความต้องการ เส้นทางของต้นไม้ความมั่นคงจะถูกท่องไปดังที่ได้แสดงไว้ในการประยุกต์ใช้ไวยากรณ์ความมั่นคงบทที่ 5 เพื่อให้ครอบคลุมทุกเส้นทางและย่นระยะทางการเข้าถึงเทอร์มินัลของไวยากรณ์ที่ต้องการใช้งาน เครื่องมือต้นแบบจะนำองค์ประกอบแบบนอนเทอร์มินัลของต้นไม้ความมั่นคงมาใช้เป็นรายการตัวเลือกในการกำหนดความต้องการของแต่ละไวยากรณ์

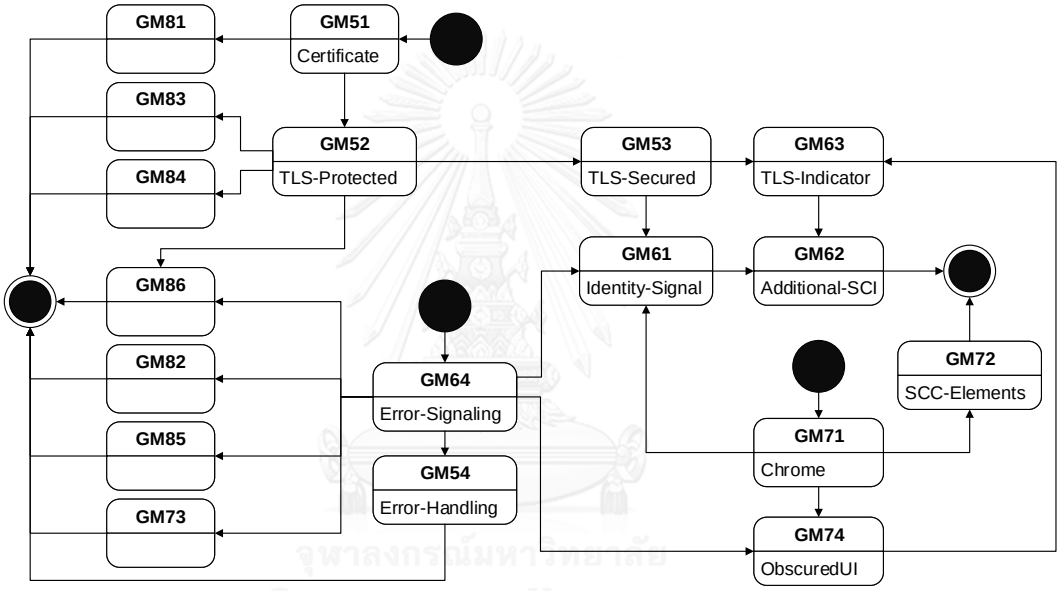
6.6 ลำดับการกำหนดความต้องการตามเงื่อนไขก่อนการใช้งานไวยากรณ์

เครื่องมือต้นแบบสร้างจากไวยากรณ์คำนึงถึงเงื่อนไขก่อนการใช้งานก่อให้เกิดลำดับการกำหนดความต้องการจากภาพที่ 6.4 แสดงเส้นทางการกำหนดความต้องการตามไวยากรณ์เริ่มต้นที่ไม่พึ่งพิงไวยากรณ์อื่น 3 ไวยากรณ์ คือ ไวยากรณ์ 51 (GM51) ไวยากรณ์ 64 (GM64) ไวยากรณ์ 71 (GM71) จากไวยากรณ์ดังกล่าว นำมาสร้างเส้นทางหลักได้ดังนี้

เส้นทางที่ 1 เริ่มต้นที่ไวยากรณ์ 51 (GM51) ไปยังไวยากรณ์ 52 (GM52) ไวยากรณ์ 83 (GM83) หรือไวยากรณ์ 84 (GM84)

เส้นทางที่ 2 เริ่มต้นที่ไวยากรณ์ 64 (GM64) ไปยังไวยากรณ์ 54 (GM54) ไวยากรณ์ 73 (GM73) ไวยากรณ์ 82 (GM82) ไวยากรณ์ 85 (GM85) หรือไวยากรณ์ 86 (GM86)

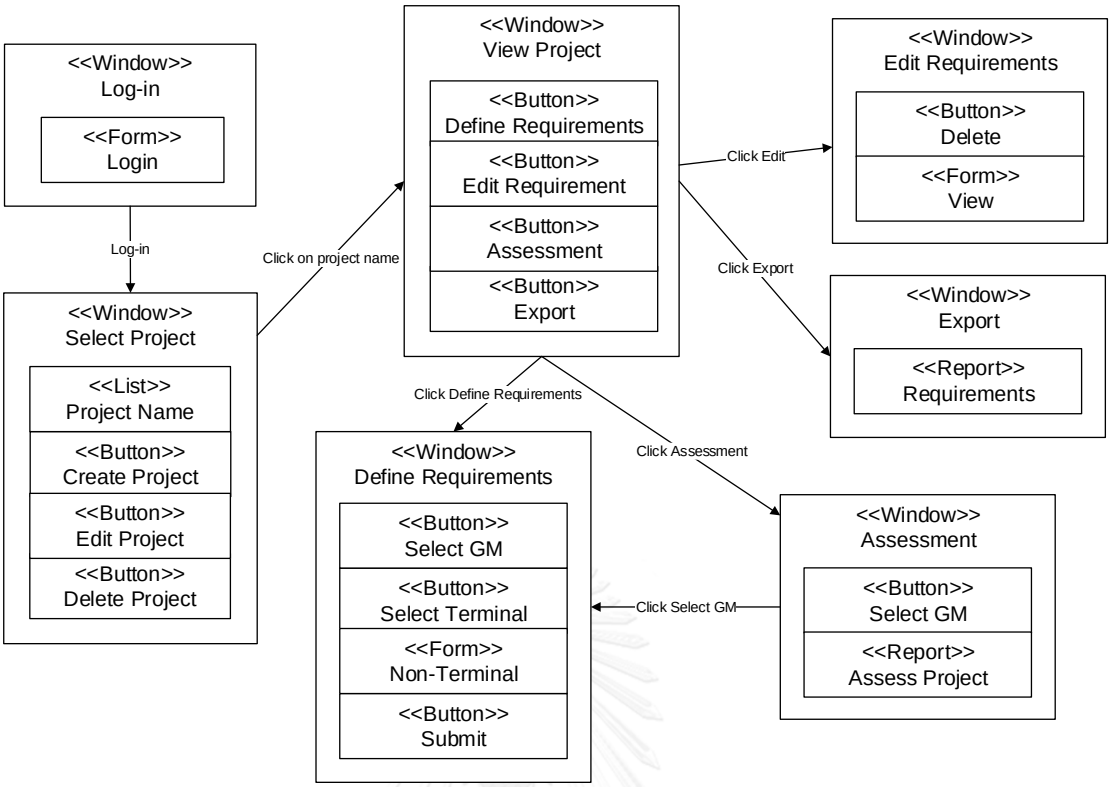
เส้นทางที่ 3 เริ่มต้นที่ไวยากรณ์ 71 (GM71) ไปยังไวยากรณ์ 72 (GM72) โดยมีเส้นทางร่วมกับไวยากรณ์ 64 (GM64) ไปยังไวยากรณ์ 74 (GM74) หรือเส้นทางร่วมไวยากรณ์ 51 (GM51) ไปยังไวยากรณ์ 53 (GM53) ไปยังไวยากรณ์ 61 (GM61) หรือไวยากรณ์ 63 (GM63) แล้วสิ้นสุดเส้นทางที่ไวยากรณ์ 62 (GM62)



ภาพที่ 6.4 แผนภาพเครื่องจักรสถานะแสดงลำดับการใช้งานไวยากรณ์

6.7 การทำงานและส่วนต่อประสานผู้ใช้ของเครื่องมือต้นแบบ

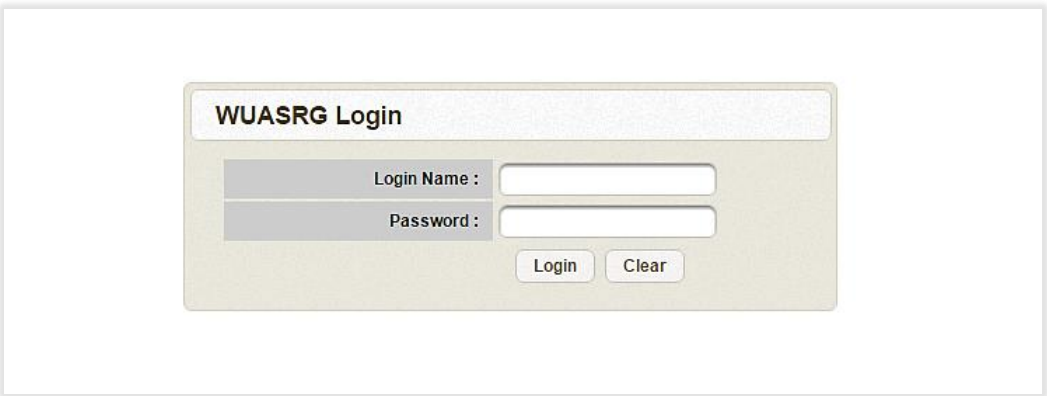
ส่วนต่อประสานผู้ใช้ของระบบแสดงผลผ่านหน้าเว็บประกอบด้วยหน้าต่างสำหรับเข้าใช้งาน หน้าต่างสำหรับจัดการโครงการ หน้าต่างสำหรับกำหนดรายการความต้องการ หน้าต่างสำหรับแก้ไขความต้องการ หน้าต่างสำหรับประเมินโครงการ และหน้าต่างสำหรับนำออกรายการความต้องการ โดยมีภาพรวมและความสัมพันธ์ระหว่างหน้าเว็บแสดงด้วยแผนภาพวินโดวนาวิเกชัน (Window-Navigation Diagram) ดังภาพที่ 6.5 โดยส่วนของการกำหนดความต้องการเป็นไปตามลำดับการใช้งานไวยากรณ์ รายละเอียดของการทำงานและส่วนต่อประสานผู้ใช้สามารถอธิบายได้ดังนี้



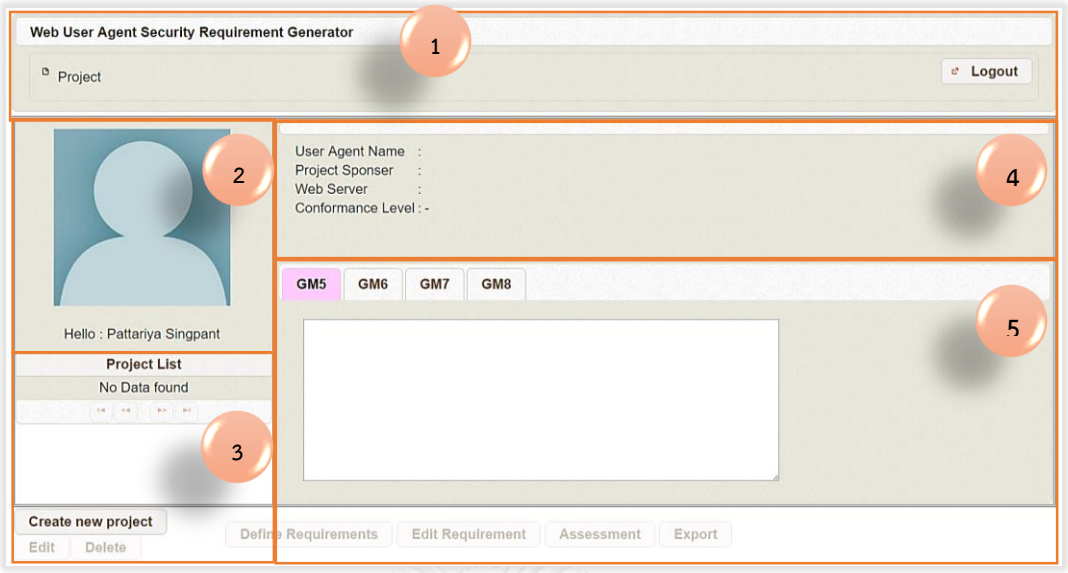
ภาพที่ 6.5 แผนภาพวินโดวนาวิเกชันแสดงส่วนต่อประสานผู้ใช้ของระบบต้นแบบ

6.7.1 การเข้าใช้งานระบบ

ก่อนการกำหนดความต้องการความมั่นคงของระบบใดๆ ผู้ใช้ต้องเข้าใช้ระบบโดยกรอกชื่อสำหรับเข้าใช้งานและรหัสผ่านที่ได้รับจากผู้ดูแลระบบ ผ่านส่วนต่อประสานดังภาพที่ 6.6 หากรหัสผ่านไม่ถูกจะไม่สามารถเข้าใช้งานระบบได้



ภาพที่ 6.6 หน้าต่างสำหรับเข้าใช้งาน



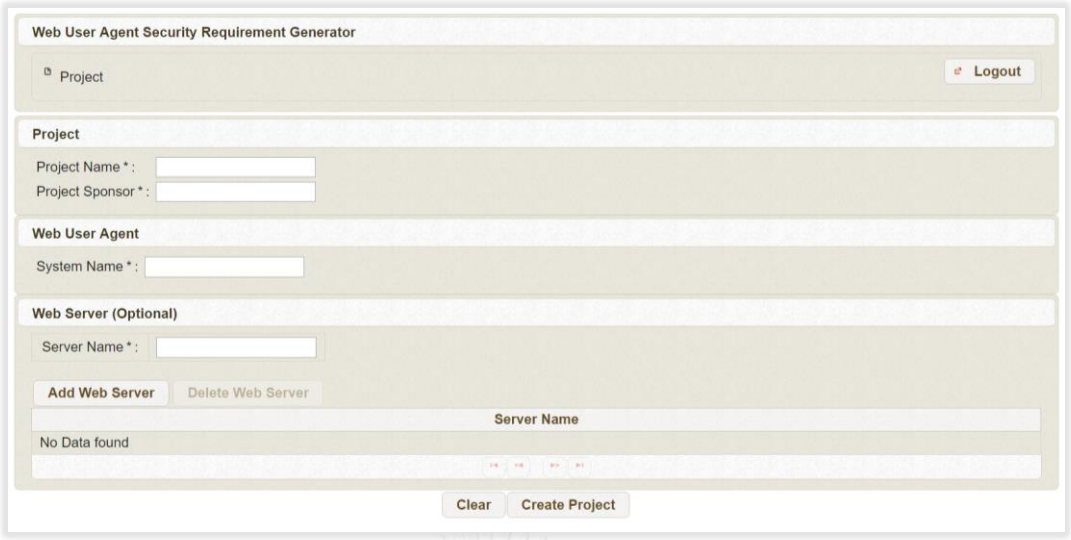
ภาพที่ 6.7 หน้าจอหลักของเครื่องมือกำหนดความต้องการความมั่นคง

เมื่อเข้าสู่ระบบผู้ใช้จะพบหน้าจอหลักสำหรับจัดการโครงการและรายการความต้องการ ดังภาพที่ 6.7 โดยแบนเนอร์ด้านบนจะปรากฏชื่อของเครื่องมือกำหนดความต้องการความมั่นคง กรอบหมายเลข 1 แสดงแถบเมนูโครงการและปุ่มเพื่อลงชื่อออกจากระบบ กรอบหมายเลข 2 สำหรับคอลัมน์ด้านซ้ายแสดงข้อมูลผู้ใช้ ส่วนกรอบหมายเลข 3 แสดงรายการโครงการพร้อมปุ่มสำหรับจัดการโครงการ กรอบหมายเลข 4 คอลัมน์ด้านขวาแสดงรายละเอียดโครงการที่เลือก และกรอบหมายเลข 5 แสดงรายการความต้องการที่กำหนดไว้แบ่งเป็นแถบตามกลุ่มไวยากรณ์ และปุ่มสำหรับจัดการรายการความต้องการ หากผู้ใช้ยังไม่เลือกโครงการปุ่มดังกล่าวจะไม่ทำงาน

6.7.2 การจัดการโครงการ

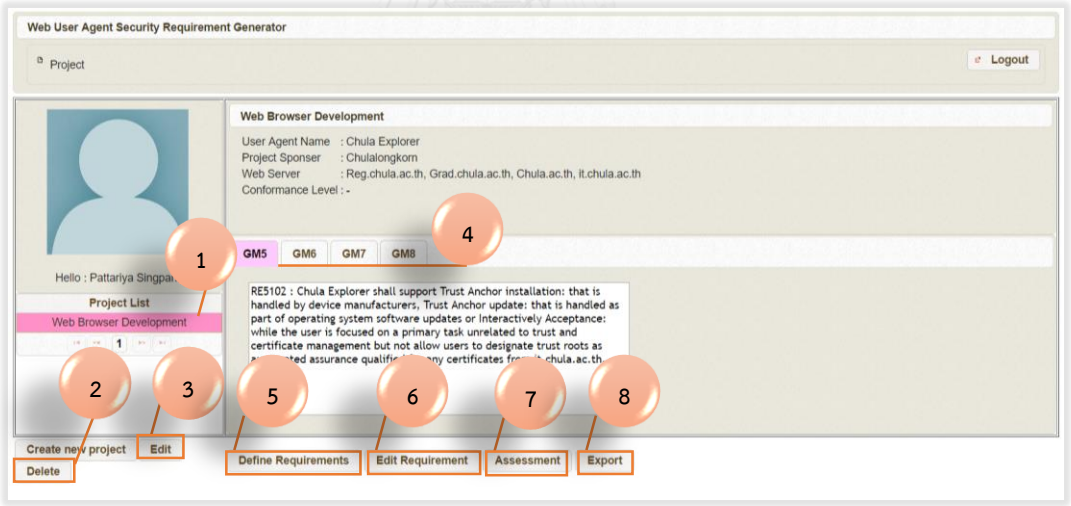
การจัดการโครงการประกอบด้วย หน้าจอการสร้างโครงการ หน้าจอการแสดงข้อมูลโครงการ หน้าจอการแก้ไขโครงการ และหน้าจอการลบโครงการ โดยมีลำดับขั้นตอนดังนี้

1) **การสร้างโครงการ** หลังจากเข้าสู่ระบบผู้ใช้สามารถสร้างโครงการจากปุ่มสร้างโครงการใหม่ (Create new project) ภายใต้กรอบหมายเลข 3 จากภาพที่ 6.7 จะปรากฏหน้าจอสำหรับการสร้างโครงการดังภาพที่ 6.8 โดยผู้ใช้ต้องกรอกข้อมูลชื่อโครงการ ผู้สนับสนุนโครงการ ชื่อระบบ และรายการผู้ให้บริการเว็บ เมื่อกรอกข้อครบถ้วนกดปุ่มสร้างโครงการ (Create Project) เพื่อบันทึกลงฐานข้อมูลโครงการ หากต้องการล้างข้อมูลที่กรอกไปกดปุ่มลบล้าง (Clear)



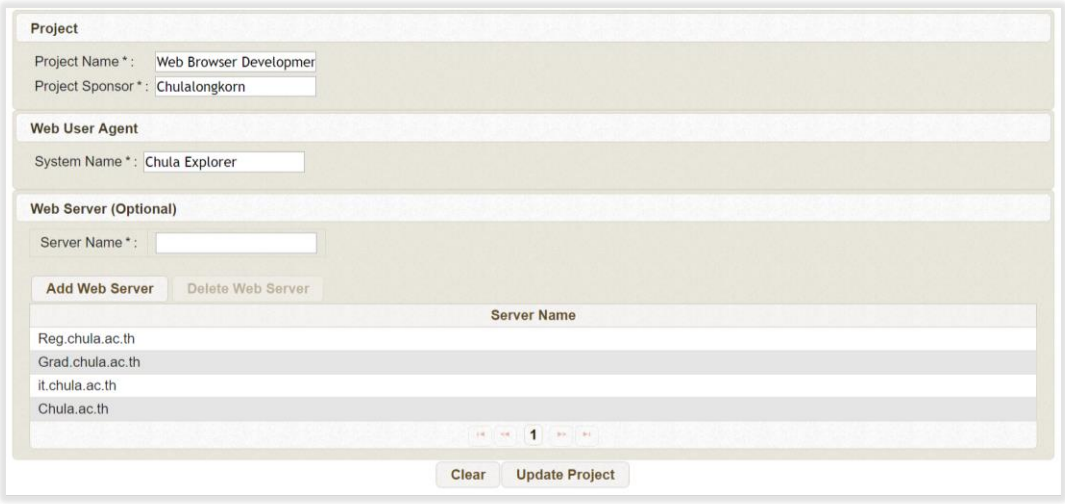
ภาพที่ 6.8 หน้าจอสำหรับสร้างโครงการ

2) **การแสดงข้อมูลโครงการ** ผู้ใช้เลือกโครงการจากรายการหมายเลข 1 ในภาพที่ 6.9 เพื่อแสดงข้อมูลชื่อโครงการ ผู้สนับสนุนโครงการ ชื่อระบบ รายการผู้ให้บริการเว็บ ระดับความคล้อยตาม และรายการความต้องการที่กำหนดของโครงการ



ภาพที่ 6.9 หน้าจอสำหรับแสดงข้อมูลโครงการ

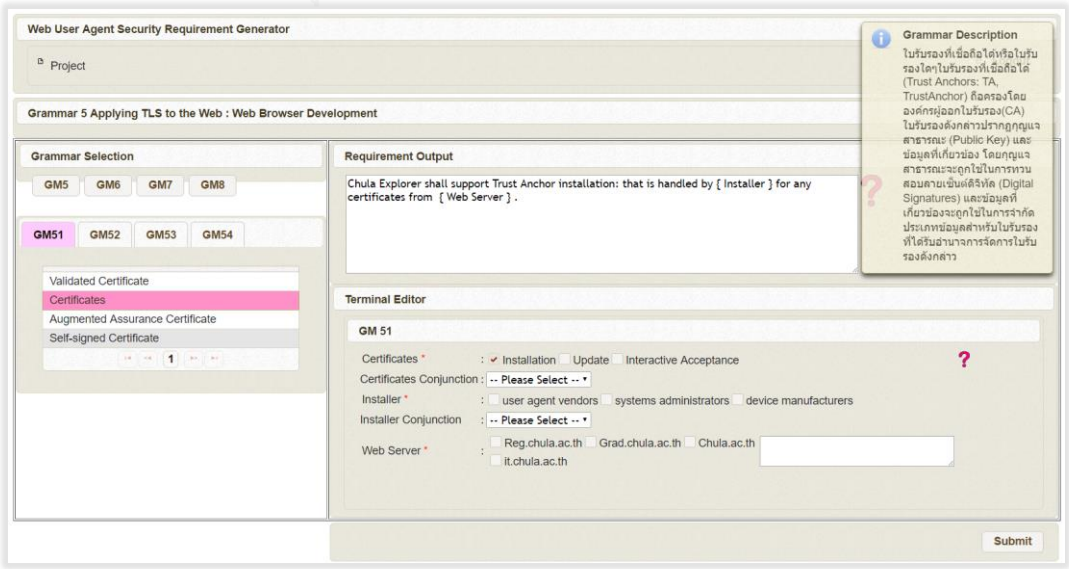
3) **การลบหรือแก้ไขข้อมูลโครงการ** จากภาพที่ 6.9 เมื่อเลือกโครงการดังหมายเลข 1 แล้ว ผู้ใช้สามารถกดปุ่มลบ (Delete) ดังหมายเลข 2 เพื่อลบข้อมูลโครงการที่เลือก หรือแก้ไขโครงการโดยกดปุ่มแก้ไข (Edit) ดังหมายเลข 3 จากนั้นระบบจะนำท่านเข้าสู่หน้าจอสำหรับปรับปรุงข้อมูลโครงการดังภาพที่ 6.10 ผู้ใช้สามารถแก้ไขและบันทึกข้อมูลโครงการที่ปรับปรุงแล้วได้โดยกดปุ่มปรับปรุงโครงการ (Update Project) หากต้องการล้างข้อมูลกดปุ่มลบล้าง (Clear)



ภาพที่ 6.10 หน้าจอสำหรับแก้ไขข้อมูลโครงการ

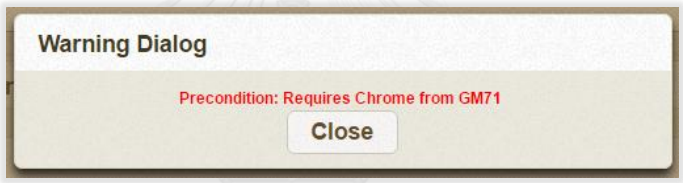
6.7.3 การจัดการรายการความต้องการ

1) **การกำหนดรายการความต้องการ** จากภาพที่ 6.9 เมื่อเลือกโครงการจากรายการหมายเลข 1 และกลุ่มไวยากรณ์จากหมายเลข 4 แล้ว ผู้ใช้สามารถกดปุ่มกำหนดความต้องการ (Define Requirements) ดังหมายเลข 5 จากนั้นระบบจะนำท่านเข้าสู่หน้าจอสำหรับกำหนดความต้องการดังภาพที่ 6.11 คอลัมน์ด้านซ้ายปรากฏกลุ่มไวยากรณ์ (Grammar Selection) และรายการนอนเทอร์มินัล ส่วนคอลัมน์ด้านขวาปรากฏตัวอย่างผลลัพธ์ความต้องการ (Requirement Output) และกลุ่มรายการเทอร์มินอลของข้อมูลที่จำเป็นต้องนำเข้า (Terminal Editor) โดยเครื่องหมายคำถาม (Question Mark) สำหรับแสดงคำอธิบายไวยากรณ์หรือข้อมูลนำเข้า



ภาพที่ 6.11 หน้าจอสำหรับกำหนดรายการความต้องการ

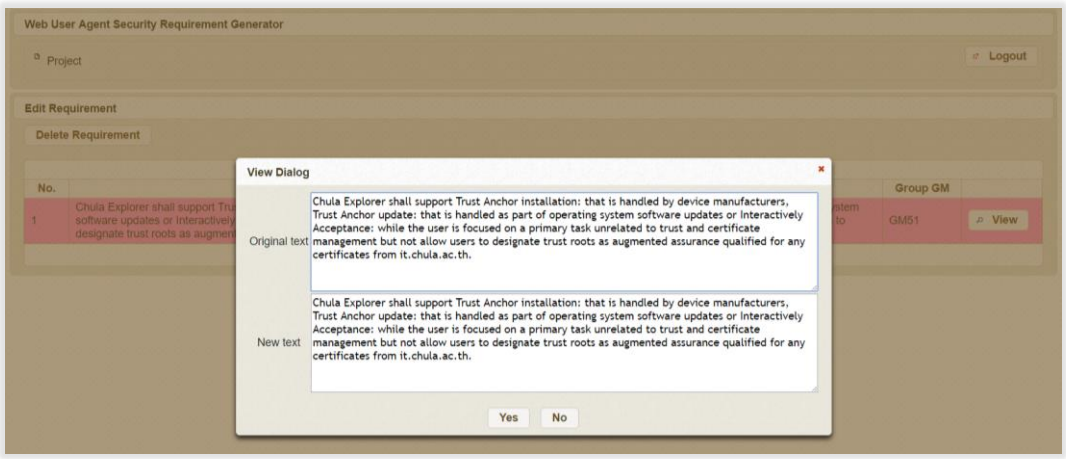
ผู้ใช้เริ่มต้นการกำหนดความต้องการโดยเลือกไวยากรณ์ที่ต้องการ หากไวยากรณ์ที่เลือกไม่ผ่านเงื่อนไขก่อนการใช้งานจะปรากฏหน้าต่างแจ้งเตือนดังภาพที่ 6.12 ผู้ใช้ต้องกำหนดความต้องการผ่านไวยากรณ์ดังกล่าวให้เรียบร้อยก่อน เมื่อผ่านเงื่อนไขก่อนการใช้งานไวยากรณ์แล้ว ผู้ใช้สามารถกำหนดความต้องการโดยนำเข้าข้อมูลที่จำเป็นในแถบการแก้ไขเทอร์มินอล (Terminal Editor) ผลลัพธ์ของการกำหนดความต้องการจะแสดงผ่านแถบผลลัพธ์ความต้องการ (Requirements Output) ดังภาพที่ 6.12 ในกรณีที่ผู้ใช้กำหนดข้อมูลที่จำเป็นต้องกรอกไม่ครบระบบจะแสดงตัวอย่างผลลัพธ์ความต้องการด้วยสัญลักษณ์กล้ามปูครอบที่ชื่อเทอร์มินอลของข้อมูลที่จำเป็นต้องก รอก เช่น ตัวอย่างข้อมูล { Web-Sever } เพื่อให้แตกต่างจากข้อความปกติและชี้นำผู้ใช้ให้กำหนดข้อมูลสำหรับเทอร์มินัลดังกล่าว หากผู้ใช้ต้องการคำอธิบายไวยากรณ์ผู้ใช้สามารถวางเมาส์ไปที่เครื่องหมายคำถาม (Question Mark) ทางด้านขวาของกล่องข้อความเพื่อแสดงข้อความช่วยเหลือ (Tool Tips) เมื่อผู้ใช้กรอกข้อมูลครบถ้วนแล้วกดปุ่มเสนอ (Submit) เพื่อบันทึกความต้องการที่ได้กำหนด หากข้อมูลไม่ครบระบบจะอนุญาตให้บันทึกความต้องการได้



ภาพที่ 6.12 หน้าจอแสดงเงื่อนไขก่อนการใช้งานไวยากรณ์

2) **การลบและแก้ไขความต้องการ** จากภาพที่ 6.9 เมื่อเลือกโครงการดังหมายเลข 1 แล้ว ผู้ใช้สามารถกดปุ่มแก้ไขความต้องการ (Edit Requirement) หมายเลข 6 ระบบจะนำท่านเข้าสู่หน้าจอสำหรับจัดการความต้องการดังภาพที่ 6.13 ปรากฏรายการความต้องการ โดยผู้ใช้สามารถ

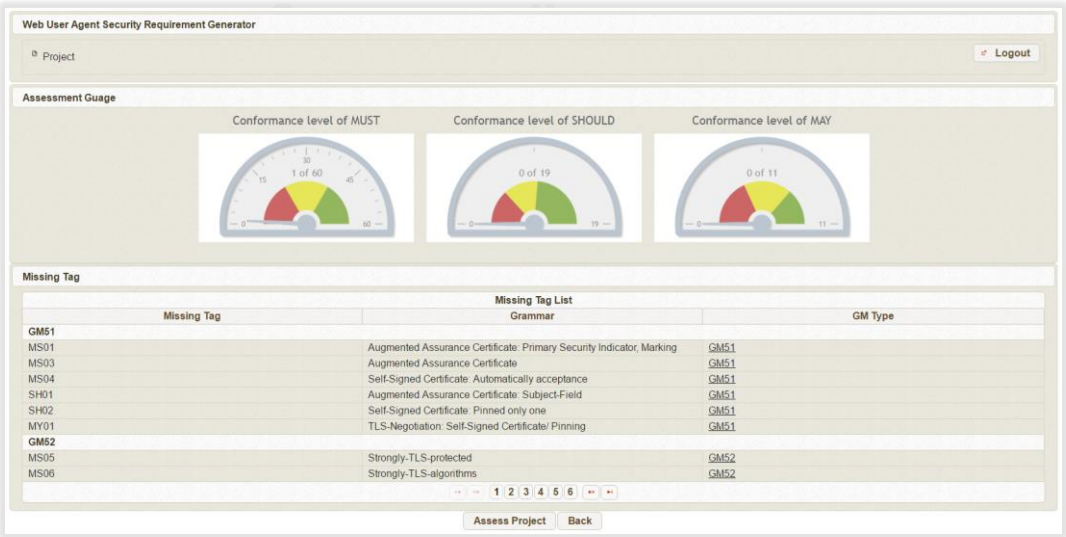
ภาพที่ 6.13 หน้าจอสำหรับจัดการรายการความต้องการ



ภาพที่ 6.14 หน้าจอสำหรับแก้ไขความต้องการ

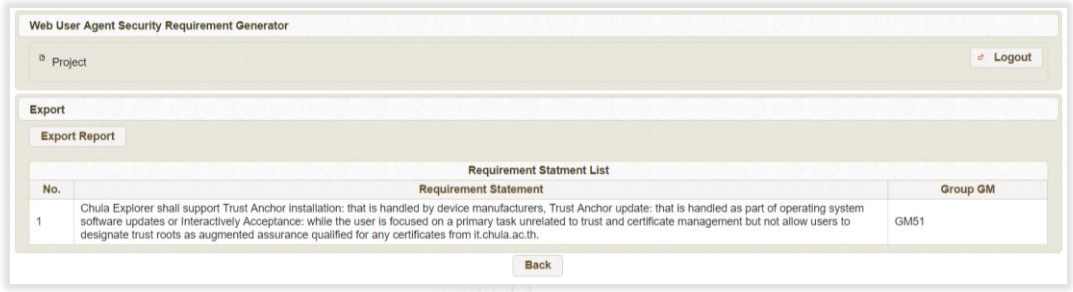
เลือกความต้องการเพื่อลบแล้วกดปุ่มลบความต้องการ (Delete Requirement) หมายเลข 1 หรือกดปุ่มเรียกดู (View) หมายเลข 2 เพื่อนำไปสู่หน้าจอสำหรับแก้ไขความต้องการดังภาพที่ 6.15

3) **การประเมินโครงการ** จากภาพที่ 6.9 เมื่อเลือกโครงการดังหมายเลข 1 แล้ว ผู้ใช้สามารถกดปุ่มการประเมิน (Assessment) ดังหมายเลข 7 ระบบจะนำท่านเข้าสู่หน้าจอการประเมินโครงการดังภาพที่ 6.15 ปรากฏแผงหน้าปัดแสดงจำนวนความต้องการที่คล้อยตามข้อบังคับของเอกสารดับเบิ้ลยูเอสซียูไอ โดยแบ่งเป็น 3 ประเภท คือ ข้อบังคับแบบต้องปฏิบัติ (MUST) ข้อบังคับแบบควรปฏิบัติ (SHOULD) และข้อบังคับแบบเลือกปฏิบัติ (MAY) พร้อมทั้งแสดงรายการที่ขาดหาย เมื่อผู้ใช้ทวนสอบข้อมูลครบถ้วนแล้วสามารถกดปุ่มประเมินโครงการ (Assess Project) เพื่อตัดสินระดับความคล้อยตามของโครงการและบันทึกผลการประเมินลงฐานข้อมูล



ภาพที่ 6.15 หน้าจอสำหรับประเมินโครงการ

4) **การนำออกรายการความต้องการ** จากภาพที่ 6.9 เมื่อเลือกโครงการดังหมายเลข 1 แล้ว ผู้ใช้สามารถกดปุ่มนำออก (Export) หมายเลข 8 จะนำท่านเข้าสู่หน้าจอการนำออกรายการความต้องการดังภาพที่ 6.16 ผู้ใช้สามารถกดปุ่มนำออก (Export) เพื่อดาวน์โหลดรายการความต้องการในรูปแบบไฟล์ไมโครซอฟท์เอกเซล (.xls) ได้



ภาพที่ 6.16 หน้าจอสำหรับนำออกรายการความต้องการ

6.8 การทดสอบเครื่องมือต้นแบบ

การทดสอบหน้าที่หลักของเครื่องมือต้นแบบเบื้องต้น ดำเนินการโดยผู้วิจัยโดยการสร้างกรณีทดสอบ (Test Case) ดังตารางที่ 6.1 โดยการทดสอบการสร้างโครงการ การแก้ไขหรือลบข้อมูลโครงการ การแสดงข้อมูลโครงการ การกำหนดความต้องการ แก้ไขหรือลบความต้องการ การประเมินโครงการ และการนำออกข้อมูล การประเมินประสิทธิผลและภาพของเครื่องมือนั้นได้อภิปรายไว้ในบทที่ 7

ตารางที่ 6.1 ผลการทดสอบหน้าที่หลักของเครื่องมือต้นแบบตามกรณีทดสอบ

รหัส	กรณีทดสอบ	ผลที่คาดหวัง	สรุปผล
TC001	การเข้าสู่ระบบ	หากผู้ใช้กรอกชื่อและรหัสถูก และแจ้งเตือนเมื่อผู้ใช้กรอกผิด	ผ่าน
TC002	สร้างโครงการลงฐานข้อมูล	สร้างโครงการเรียบร้อย	ผ่าน
TC003	เลือกปรับปรุงข้อมูลหรือลบโครงการที่มีอยู่	เมื่อเลือกปรับปรุงข้อมูลโครงการมีการเปลี่ยนแปลงตามการแก้ไข หรือเมื่อเลือกลบโครงการที่เลือกถูกลบ	ผ่าน
TC004	แสดงข้อมูลโครงการ	ข้อมูลโครงสร้างถูกแสดงครบถ้วน	ผ่าน
TC005	แก้ไขหรือลบรายการความต้องการ	เมื่อแก้ไขความต้องการ ระบบมีการบันทึกเปลี่ยนแปลง เมื่อเลือกลบ ความต้องการที่เลือกออกจากฐานข้อมูล	ผ่าน
TC006	ประเมินโครงการตามระดับความคล้อยตาม	ปรากฏผลการประเมินและจำนวนข้อบังคับที่พบได้ครบถ้วน	ผ่าน
TC007	นำออกข้อมูลรายการความต้องการในรูปแบบไฟล์ได้	ได้ไฟล์ที่บันทึกข้อมูลรายการความต้องการของโครงการที่เลือก	ผ่าน

บทที่ 7
การประเมินผลลัพธ์ที่ได้จากเครื่องมือ

จากบทที่ 5 การประยุกต์ใช้ไวยากรณ์ความมั่นคงได้แสดงทุกๆ ผลลัพธ์รายการความต้องการที่ได้ตามเส้นทางของต้นไม้ความมั่นคงได้อย่างครบถ้วน และนำไปสู่พื้นฐานของการสร้างเครื่องมือระบุความต้องการพร้อมทั้งทดสอบเบื้องต้นในบทที่ 6 เพื่อให้แน่ใจว่าเครื่องมือต้นแบบพื้นฐานไวยากรณ์ความมั่นคงสามารถระบุความต้องการความมั่นคงได้อย่างมีประสิทธิภาพ ในบทนี้เครื่องมือต้นแบบพื้นฐานไวยากรณ์ความมั่นคงที่สร้างขึ้นจะถูกเปรียบเทียบผลลัพธ์ความต้องการความมั่นคงระหว่างการกำหนดด้วยมือและการกำหนดด้วยเครื่องมือ รวมถึงประเมินระดับความพึงพอใจของผู้ใช้ที่มีต่อการใช้งานเครื่องมือ ตามขั้นตอนที่ปรากฏในภาพที่ 7.1 โดยมีรายละเอียดดังนี้

7.1 การวางแผนการประเมิน

7.1.1 จุดประสงค์การทดลอง

1) เพื่อเปรียบเทียบความต้องการความมั่นคงที่ได้จากการกำหนดด้วยมือและการกำหนดด้วยเครื่องมือ

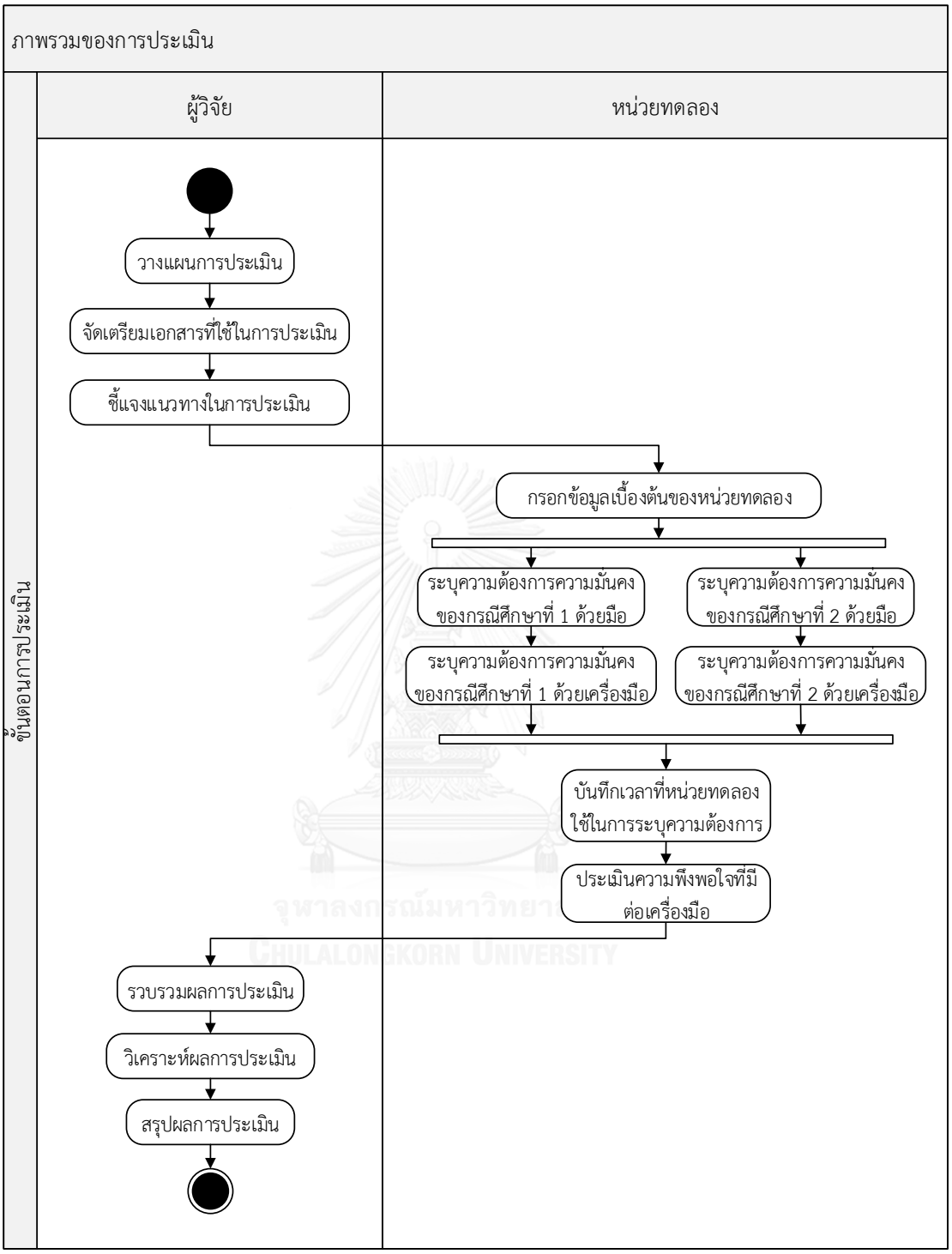
2) เพื่อประเมินความพึงพอใจของผู้ใช้ที่มีต่อการระบุความต้องการโดยเครื่องมือต้นแบบ

7.1.2 สิ่งทดลอง

สิ่งทดลองในบทนี้ คือ เครื่องมือต้นแบบสำหรับการกำหนดความต้องการ จาก 2 ไวยากรณ์ คือ ไวยากรณ์ 51 และไวยากรณ์ 71 ซึ่งเป็นไวยากรณ์พื้นฐานในการกำหนดความต้องการของระบบ โดยประยุกต์ใช้ 2 กรณีศึกษา คือ กรณีที่ 1 ทริปแอดไวซ์เซอร์ (TripAdvisor) เป็นระบบค้นหาที่พักและตั๋วเครื่องบิน และกรณีที่ 2 ดอร์ฟิน เว็บเบราว์เซอร์ (Dolphin Web Browser) เป็นระบบค้นดูเว็บ โดยหน่วยทดลองทั้ง 2 คน จะต้องกำหนดความต้องการของระบบทั้งสองกรณีด้วยมือและด้วยเครื่องมือเพื่อนำมาเปรียบเทียบ โดยใช้ความรู้จากการศึกษาแบบรูปทั้งสองประกอบ

7.1.3 หน่วยทดลอง

หน่วยทดลองจะต้องมีความรู้ด้านการระบุความต้องการและความเข้าใจแบบรูปบริบทความมั่นคงเชิงเว็บ ดังนั้นหน่วยทดลองจำนวน 2 คน จากผู้เข้าร่วมการประเมินแบบรูปบริบทความมั่นคงเชิงเว็บที่มีผลการเรียนวิชาความมั่นคงด้านสารสนเทศ (Information Security) วิชาวิศวกรรมความต้องการซอฟต์แวร์ (Software Requirements Engineering) ไม่ต่ำกว่า B



ภาพที่ 7.1 ภาพรวมการทดสอบเครื่องมือ

7.1.4 เกณฑ์การพิจารณาผลการประเมิน

เกณฑ์การพิจารณาผลการประเมินแบ่งออกเป็น 2 ส่วน คือเกณฑ์การเปรียบเทียบผลลัพธ์ความต้องการที่ระบุด้วยมือกับความต้องการที่ระบุด้วยเครื่องมือ และเกณฑ์การประเมินความพึงพอใจ โดยมีหลักการดังนี้

1) การเปรียบเทียบผลลัพธ์ความต้องการ นำผลลัพธ์ความต้องการที่ระบุด้วยมือมาพิจารณาจากรายการองค์ประกอบที่ปรากฏเทียบกับองค์ประกอบที่ปรากฏในผลลัพธ์ความต้องการที่ได้จากเครื่องมือ เนื่องจากองค์ความรู้อยู่ในแบบรูปภาษาไทย แต่รายการความต้องการเป็นภาษาอังกฤษอาจทำให้ผลลัพธ์ความต้องการที่หน่วยทดลองระบุด้วยตนเองมีความหลากหลาย เกณฑ์การพิจารณาจึงเน้นองค์ประกอบที่สกัดได้จากคลาสที่ใช้อธิบายโครงสร้างภายในแบบรูปเป็นหลัก โดยองค์ประกอบที่พบในความต้องการที่ระบุด้วยมือมากกว่าหรือน้อยกว่าที่ระบุด้วยเครื่องมือ คิดเป็นอัตราส่วนเท่าใด วิเคราะห์ผลต่าง เช่น หากระบุด้วยมือมีองค์ประกอบมากกว่าควรปรับปรุงไวยากรณ์หรือไม่

2) ปัจจัยที่ใช้ในการประเมินความพึงพอใจ

(1) กลุ่มปัจจัยด้านคุณภาพของข้อระบุความต้องการความมั่นคง
- ความครบถ้วน
- ความถูกต้อง
- ความไม่กำกวม

(2) กลุ่มปัจจัยด้านคุณสมบัติของเครื่องมือ
- สนับสนุนการนำกลับมาใช้ซ้ำ
- ลำดับการทำงาน
- ลดความยุ่งยาก

(3) กลุ่มปัจจัยด้านประโยชน์ของเครื่องมือ
- เพิ่มการเรียนรู้
- ลดระยะเวลาที่ใช้
- เป็นทางเลือกที่ดีกว่าการระบุความต้องการด้วยตนเอง

โดยเกณฑ์การประเมินความพึงพอใจแต่ละปัจจัย แบ่งออกเป็น 5 ระดับดังนี้

5 หมายถึง หน่วยทดลองเห็นด้วยมากที่สุด

4 หมายถึง หน่วยทดลองเห็นด้วยมาก

3 หมายถึง หน่วยทดลองเห็นด้วยปานกลาง

2 หมายถึง หน่วยทดลองเห็นด้วยน้อย

1 หมายถึง หน่วยทดลองเห็นด้วยน้อยมาก

7.2 ขั้นตอนการประเมิน

1) จัดเตรียมข้อมูลที่ใช้ในการทดลอง
2) แจกเอกสารและอธิบายจุดประสงค์และวิธีการให้แก่หน่วยทดลอง
3) หน่วยทดลองระบุความต้องการด้วยมือ
4) หน่วยทดลองระบุความต้องการด้วยเครื่องมือ
5) หน่วยทดลองประเมินความพึงพอใจที่มีต่อเครื่องมือ พร้อมข้อเสนอแนะ
6) บันทึกและรวมรวมผลการทดลอง
7) วิเคราะห์และสรุปผลการทดลอง

7.3 ผลการทดลอง

ผลการทดลองแบ่งเป็น 2 ส่วน คือ ผลลัพธ์ความต้องการที่กำหนดด้วยมือและผลการประเมินความพึงพอใจของผู้ใช้ที่มีต่อเครื่องมือ โดยผลลัพธ์ความต้องการ ระยะเวลาที่ใช้ และความพึงพอใจของหน่วยทดลองทั้ง 2 กรณีศึกษา แสดงในตารางที่ 7.1 ตารางที่ 7.2 และตารางที่ 7.3 ตามลำดับ สำหรับผลการประเมินระดับความพึงพอใจของผู้ใช้ที่มีต่อเครื่องมือแสดงในตารางที่ 7.4

ตารางที่ 7.1 ผลลัพธ์การกำหนดความต้องการด้วยมือสำหรับกรณีศึกษาที่ 1 เปรียบเทียบกับคำสำคัญที่ใช้ในไวยากรณ์ 51

หน่วยทดลอง	ผลลัพธ์ความต้องการที่กำหนด สำหรับกรณีศึกษาที่ 1	
	กำหนดด้วยมือ	คำสำคัญ
1	1. The system should able to use Trust Anchors issued by CA to verify digital signatures.	Trust Anchors
	2. Trust Anchors should be able installed by user agent vendors, system administrators and device manufacturers.	installed
	3. User should be able to able to accept Trust Anchor when basic path validation is failed and the system should highlight the interaction with action such as render user unable to access the website.	- accept - highlight
	4. Augmented Assurance Certificates has to be handled, user agent have to be able to verify the certificates.	Augmented Assurance Certificates
	5. User agent can use additional information from augmented assurance certificate as unique identifier for CA's approval.	- unique identifier

ตารางที่ 7.1 ผลลัพธ์การกำหนดความต้องการด้วยมือสำหรับกรณีศึกษาที่ 1 เปรียบเทียบกับคำสำคัญที่ใช้ในไวยากรณ์ 51 (ต่อ)

หน่วยทดลอง	ผลลัพธ์ความต้องการที่กำหนด สำหรับกรณีศึกษาที่ 1	
	กำหนดด้วยมือ	คำสำคัญ
	6. System should be able to handle self-signed certificate - able to handle untrusted root with Key Continuity Management and Pinning.	- self-signed certificate - Key Continuity Management -Pinning
2	จากกรณีศึกษาเบื้องต้น การร้องขอ Certificate จาก Agoda, Booking, Hotels ควรเป็น Trust Anchor ถือครองโดยองค์กรผู้ออกใบรับรอง (CA) โดยมี Public Key ที่สามารถตรวจสอบลายเซ็นดิจิทัล (Digital Signature) ได้ เมื่อทำการร้องขอและได้ไฟล์มาก็ทำการส่งให้ System Administrator เพื่อทำการ install โดยปกติแล้ว ใบรับรองที่เชื่อถือได้ (TA) จะถูกออกโดย User Agent Vendors หลังจากการทำ install สำเร็จแล้วหากใบรับรองของผู้ให้บริการเว็บใดๆ ไม่สามารถตรวจสอบได้โดยใช้วิธีอัลกอริทึมการทวนสอบวิถีขั้นต้น (Basic Path Validation Algorithm) จะเกิดการยอมรับเชิงตอบโต้ (Interactively Accepting) ระหว่างผู้ใช้งานเว็บไซต์เพื่อยืนยัน	- Trust Anchor - Install - Interactively Accepting
หน่วยทดลอง	**กำหนดด้วยมือเครื่องมือ**	**คำสำคัญ**
1	TripAdvisor shall support certificate verifying that it's chaining up to a locally configured trust anchor as a Validated Certificate for any certificates from Hotels.com, Booking.com, Agoda.com.	- trust anchor - Validated Certificate
	TripAdvisor shall support Trust Anchor installation: that is handled by user agent vendors or systems administrators and Trust Anchor update: that is handled as part of User Agent, operating system software updates, for any certificates from Hotels.com, Booking.com, Agoda.com.	- Installation - update

ตารางที่ 7.1 ผลลัพธ์การกำหนดความต้องการด้วยมือสำหรับกรณีศึกษาที่ 1 เปรียบเทียบกับคำสำคัญที่ใช้ในไวยากรณ์ 51 (ต่อ)

หน่วยทดลอง	กำหนดด้วยมือเครื่องมือ	คำสำคัญ
1	TripAdvisor shall support handling a Self-signed Certificates which are not part of the user agent's store of trust roots and essentially serve as a container for cryptographic key material in a key exchange that is not verified by any third party. By Key Continuity Management (KMC) to determine consistently communicating with the same web server or the pinning interaction that enables users to pin a certificate to a destination, but not allow to be accepted automatically for an untrusted root certificate to additional sites nor to be pinned to more than one site for any certificates for self-signed certificates (or certificates that chain up to an untrusted root) from Hotels.com, Booking.com, Agoda.com.	- Self-signed Certificates - Key Continuity Management (KMC) - the pinning
2	TripAdvisor shall support certificate verifying that it's chaining up to a locally configured trust anchor as a Validated Certificate for any certificates from Agoda.com , Booking.com, Hotels.com.	- trust anchor - Validated Certificate -
	TripAdvisor shall support Trust Anchor installation: that is handled by systems administrators and device manufacturers, Trust Anchor update: that is handled as part of User Agent, operating system software updates, and Interactively Acceptance: while the user is focused on a primary task unrelated to trust and certificate management but not allow users to designate trust roots as augmented assurance qualified for any certificates from Agoda.com , Booking.com, Hotels.com.	- Installation - Update - Interactively Acceptance

ตารางที่ 7.2 ผลลัพธ์การกำหนดความต้องการด้วยมือสำหรับกรณีศึกษาที่ 2

หน่วยทดลอง	ผลลัพธ์ความต้องการที่กำหนด สำหรับกรณีศึกษาที่ 2	
	กำหนดด้วยมือ	คำสำคัญ
1	1. The Primary User Interface has be shown to the user without request.	- The Primary User Interface
	2. Secondary User Interface will be displayed on demand from user.	- Secondary User Interface
	3. User is able to input web location to request the web site from provider in Location bar.	- Location bar
	4. User should be displayed with identity signal to verify identity information.	- identity signal
	5. The browse show the web site title in Browser Window Title using data from HTML TITLE element.	- identity signal
	6. User is able to navigate the web site with back and forward button.	- navigate
	7. The URL bar can display hyper link of the connecting web site.	- URL bar
	8. Padlock Icon is used to display secured web site (SSL).	- Padlock Icon
	9. The browser is able to display favicon to identify legitimacy of the web site.	- favicon
	10. Status bar will be used to display the web site is response when user initiation action	- Status bar
	11. Information bar or notification bar should be used to display additional information or error to user.	- Information bar
	12. The chrome user interface must always displayed to the user to prevent ambiguity.	- chrome
2	ส่วนต่อประสานผู้ใช้โครมควรมีองค์ประกอบที่สำคัญตามรายการต่อไปนี้ 1) Location Bar 2) Window Title 3) Back, Forward Buttons 4) URL Bar 5) Status Bar พร้อมทั้งควรมี UI ที่แสดงเนื้อหาและข้อมูลได้อย่างชัดเจน 6) Info Bar เพื่อแจ้งเตือนข้อความในลักษณะต่างๆ กับผู้ใช้งาน ยกตัวยอย่าง เมื่อนาย A ทำการใช้งาน Dolphin Web Browser นาย A ควรทราบถึง URL ปัจจุบัน ผ่าน URL Bar และนาย A สามารถกด Link เพื่อไปยังอีก Web Site หนึ่ง และเห็นสถานะของการเชื่อมต่อผ่าน Status Bar และเมื่อมีการแจ้งเตือนหรือทำการร้องขอนาย A สามารถเห็นได้จาก Info Bar เพื่อลดช่องโหว่ที่อาจจะเกิดขึ้นได้	- Location Bar - Window Title - Back, Forward Buttons - URL Bar - Status Bar

ตารางที่ 7.2 ผลลัพธ์การกำหนดความต้องการด้วยมือสำหรับกรณีศึกษาที่ 2 (ต่อ)

หน่วยทดลอง	กำหนดด้วยมือเครื่องมือ	คำสำคัญ
1	Chrome refer to the representation through which the user interacts with the user agent itself, as distinct from the accessed web content. This includes both primary and secondary user interface. By Primary User Interface denotes the portions of a Web user agent's user interface that are available to users without being solicited by a user interaction and Secondary User Interface denotes the portions of a Web user agent's user interface that are available to the user after they are solicited by a specific user interaction. Chrome shall always be present to signal security context information. User interface elements commonly present in Dolphin Web Browser a Web User Agents, are: Identity Signal, Navigation Button, TLS Indicator, Favicon, Information Bar, Status Bar, Page Title, Location Bar and URL Bar	- Chrome - Identity Signal - Navigation Button - TLS Indicator - Favicon - Information Bar - Status Bar - Page Title - Location Bar - URL Bar
2	Chrome refer to the representation through which the user interacts with the user agent itself, as distinct from the accessed web content. This includes both primary and secondary user interface. By Primary User Interface denotes the portions of a Web user agent's user interface that are available to users without being solicited by a user interaction and Secondary User Interface denotes the portions of a Web user agent's user interface that are available to the user after they are solicited by a specific user interaction. Chrome shall always be present to signal security context information. User interface elements commonly present in Dolphin Web Browser a Web User Agents, are: Identity Signal, Navigation Button, TLS Indicator, Favicon, Information Bar, Status Bar, Page Title, Location Bar and URL Bar	- Chrome - Identity Signal - Navigation Button - TLS Indicator - Favicon - Information Bar - Status Bar - Page Title - Location Bar URL Bar

ตารางที่ 7.3 ระยะเวลาที่ใช้ในการกำหนดความต้องการและความคิดเห็นของหน่วยทดลอง

กรณีศึกษา	หน่วยทดลอง	เวลาที่ใช้ในการกำหนดความต้องการ (นาที)		ความคิดเห็นเกี่ยวกับความแตกต่างระหว่างการกำหนดความต้องการด้วยมือและเครื่องมือ
		ด้วยมือ	ด้วยเครื่องมือ	
1	1	37	7	มีความแตกต่าง เนื่องจากการระบุความต้องการด้วยเครื่องมือ มีความสะดวกและครบถ้วนของข้อมูลมากกว่าการระบุด้วยมือ ระบบสามารถลดเวลาในการระบุความต้องการให้ถูกต้องได้อย่างมาก
	2	12	5	มีความแตกต่าง เพราะผู้ทดลองไม่ได้คำนึงถึงการอัพเดต (Update) คิดเพียงแต่ New install เลยขาดความครอบคลุมน้อยกว่าการใช้เครื่องมือ
2	1	16	1	เครื่องมือสามารถช่วยลดเวลาในการระบุความต้องการ และช่วยให้รายการความต้องการมีความถูกต้องและครบถ้วนกว่าการทำด้วยมือ
	2	10	2	มีความแตกต่าง เพราะการใช้เครื่องมือมีความครบถ้วนมากกว่า

ตารางที่ 7.4 ระดับความพึงพอใจของผู้ใช้ที่มีต่อเครื่องมือเป็นรายปัจจัย

ลำดับ	ปัจจัยในการประเมิน	หน่วยทดลอง		ค่าเฉลี่ย
		1	2	
1.	**ด้านคุณภาพของความต้องการ**			
1.1	เครื่องมือช่วยในการกำหนดความต้องการได้ครบถ้วนมากกว่าการกำหนดด้วยมือ	5	5	5.00
1.2	เครื่องมือช่วยในการกำหนดความต้องการได้ถูกต้องมากกว่าการกำหนดด้วยมือ	5	5	5.00
1.3	เครื่องมือช่วยลดความกำกวมของความต้องการได้มากกว่ากำหนดด้วยมือ	4	5	4.50
ค่าเฉลี่ยโดยรวม				**4.83**
2.	**ด้านคุณสมบัติของเครื่องมือ**			
2.1	เครื่องมือสนับสนุนการใช้ซ้ำของความต้องการความมั่นคงได้	5	5	5.00
2.2	เครื่องมือช่วยสนับสนุนการกำหนดความต้องการความมั่นคงอย่างเป็นลำดับ	5	3	4.00
2.3	เครื่องมือช่วยลดความยุ่งยากในการกำหนดความต้องการความมั่นคง	5	4	4.50
ค่าเฉลี่ยโดยรวม				**4.50**
3.	**ด้านประโยชน์จากใช้งาน**			
3.1	เครื่องมือช่วยให้เกิดความเข้าใจเกี่ยวกับการกำหนดความต้องการความมั่นคง	4	4	4.00
3.2	เวลาที่ใช้ในการกำหนดความต้องการด้วยเครื่องมือน้อยกว่าการกำหนดด้วยมือ	5	5	5.00
3.3	เครื่องมือใช้กำหนดความต้องการความมั่นคงโดยได้ดีกว่าการกำหนดด้วยตนเอง	5	5	5.00
ค่าเฉลี่ยโดยรวม				**4.67**

7.4 การวิเคราะห์ผลการทดลอง

7.4.1 การเปรียบเทียบผลลัพธ์ความต้องการของกรณีศึกษาที่ 1 กับไวยากรณ์ 51 สารสนเทศและการจัดการใบรับรองอิเล็กทรอนิกส์

ความต้องการจากไวยากรณ์นี้จะต้องปรากฏเนื้อหาที่เกี่ยวข้องกับเนื้อหาที่ใช้ในการวัดประเมิน คือ การจัดการใบรับรองเว็บแต่ละประเภท โดยแบ่งออกเป็น ประเภทใบรับรอง 4 องค์ประกอบ และการจัดการใบรับรอง 6 องค์ประกอบ รวมทั้งสิ้น 10 องค์ประกอบ ผลการเปรียบเทียบจากหน่วยทดลองทั้ง 2 คน ปรากฏดังตารางที่ 7.5

ตารางที่ 7.5 ผลลัพธ์จากการกำหนดความต้องการของกรณีศึกษาที่ 1 จากแบบรูป 51 ด้วยมือและเครื่องมือเปรียบเทียบกับองค์ประกอบของไวยากรณ์ 51

หน่วยทดลอง	การกำหนดด้วยมือ/เครื่องมือ	องค์ประกอบทั้งหมด										องค์ประกอบอื่นๆ
		ใบรับรองที่เชื่อถือได้	ใบรับรองที่ได้รับประกันเสริม	ใบรับรองที่ผ่านการตรวจสอบความสมเหตุสมผล	ใบรับรองที่ลงนามโดยตนเอง	การติดตั้งและอัพเดตใบรับรอง	การยอมรับใบรับรองเชิงโต้ตอบ	การทำเครื่องหมายพิเศษ	ตัวชี้บอกความมั่นคงแบบปฐมภูมิ	การจัดการความต่อเนื่องของกุญแจอิเล็กทรอนิกส์	การปักหมุด	
1	ด้วยมือ	✓	✓	×	✓	✓	✓	×	×	✓	✓	CA, Digital Signature
	เครื่องมือ	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
2	ด้วยมือ	✓	×	×	×	✓	✓	×	×	×	×	CA, Public Key, Digital Signature
	เครื่องมือ	✓	✓	✓	×	✓	✓	×	×	×	×	

หมายเหตุ ✓ หมายถึง พบคำสำคัญที่ต้องกันกับองค์ประกอบของไวยากรณ์

× หมายถึง พบคำสำคัญที่ต้องกันกับองค์ประกอบของไวยากรณ์

ผลการทดลองกำหนดความต้องการของกรณีศึกษาที่ 1 ของหน่วยทดลองที่ 1 กำหนดด้วยมือพบ 7 รายการ ด้วยเครื่องมือ 10 รายการ หน่วยทดลองที่ 2 กำหนดด้วยมือพบ 3 รายการ ด้วยเครื่องมือ 5 รายการ จากการเปรียบเทียบพบว่าความต้องการที่ระบุด้วยเครื่องมือมีองค์ประกอบครบถ้วนกว่าความต้องการที่ระบุด้วยมือ

7.4.2 การเปรียบเทียบผลลัพธ์ความต้องการของกรณีศึกษาที่ 2 กับไวยากรณ์ 71

เครื่องมือกำหนดความต้องการจากไวยากรณ์ 71 จะปรากฏองค์ประกอบของส่วนต่อประสานผู้ใช้โครม ที่ใช้ในการวัดประเมินทั้งหมด 10 องค์ประกอบ คือ ส่วนต่อประสานผู้ใช้โครม (Chrome) แถบแสดงตำแหน่ง (Location Bar) สัญญาณอัตลักษณ์ (Identity Signal) แถบแสดงชื่อเว็บบนหน้าต่าง (Title Bar) ปุ่มย้อนกลับและไปข้างหน้า (Back and Forward Buttons) แถบแสดงที่อยู่เว็บ (URL Bar) ตัวชี้บอกความมั่นคงชั้นขนส่ง (TLS indicator) สัญลักษณ์ของเว็บ (Favicon) แถบแสดงสถานะ (Status Bar) แถบสารสนเทศ (Information Bar) ดังตารางที่ 7.6 แถวแรกแสดงองค์ประกอบทั้งหมดที่เครื่องมือสามารถกำหนดได้ไว้ที่หัวตาราง โดยข้อมูลแต่ละแถวแสดงองค์ประกอบที่ผู้ใช้ได้กำหนดจริงด้วยมือและเครื่องมือ

ตารางที่ 7.6 ผลลัพธ์จากการกำหนดความต้องการของกรณีศึกษาที่ 2 จากแบบรูป 71 ด้วยมือและเครื่องมือเปรียบเทียบกับองค์ประกอบของไวยากรณ์ 71

หน่วยทดลอง	การกำหนดด้วยมือ/เครื่องมือ	องค์ประกอบทั้งหมด										องค์ประกอบอื่นๆ
		ส่วนต่อประสานผู้ใช้โครม	แถบแสดงตำแหน่ง	สัญญาณอัตลักษณ์	แถบแสดงชื่อเว็บบนหน้าต่าง	ปุ่มย้อนกลับและไปข้างหน้า	แถบแสดงที่อยู่เว็บ	ตัวชี้บอกความมั่นคงชั้นขนส่ง	สัญลักษณ์ของเว็บ	แถบแสดงสถานะ	แถบสารสนเทศ	
1	ด้วยมือ	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	Primary UI, Secondary UI
	เครื่องมือ	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
2	ด้วยมือ	✓	✓	✗	✓	✓	✓	✗	✗	✓	✓	-
	เครื่องมือ	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	

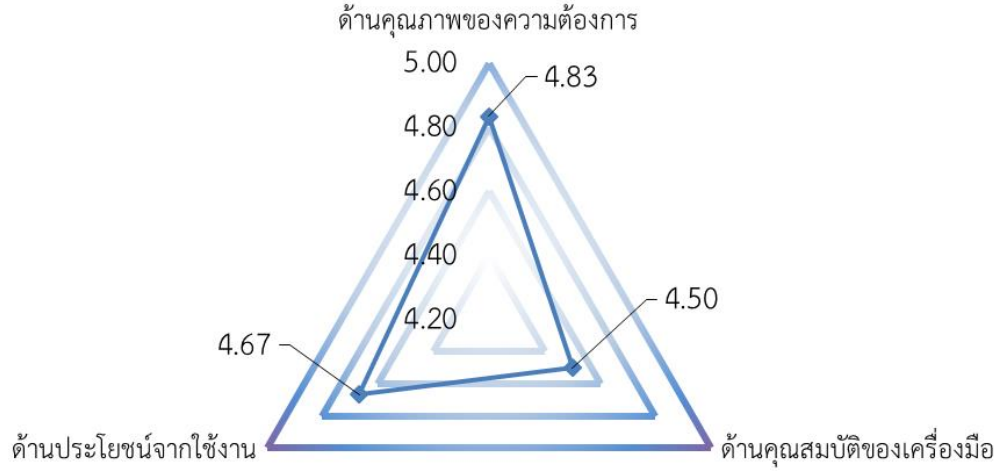
หมายเหตุ ✓ หมายถึง พบคำสำคัญที่ต้องกันกับองค์ประกอบของไวยากรณ์

✗ หมายถึง พบคำสำคัญที่ต้องกันกับองค์ประกอบของไวยากรณ์

ผลการทดลองกำหนดความต้องการของกรณีศึกษาที่ 2 ผลการทดลองของหน่วยทดลองที่ 1 กำหนดด้วยมือพบ 10 รายการ ด้วยเครื่องมือ 10 รายการ หน่วยทดลองที่ 2 กำหนดด้วยมือพบ 7 รายการ ด้วยเครื่องมือ 10 รายการ จากการเปรียบเทียบพบว่าความต้องการที่ระบุด้วยมือและเครื่องมือ ในกรณีของหน่วยทดลองที่ 1 มีองค์ประกอบเท่ากัน แต่ในหน่วยทดลองที่ 2 การใช้เครื่องมือมีองค์ประกอบครบถ้วนกว่าความต้องการที่ระบุด้วยมือ

7.4.3 การประเมินความพึงพอใจ

จากตารางที่ 7.4 ผลการประเมินความพึงพอใจของผู้ใช้ที่มีต่อการใช้งานเครื่องมือต้นแบบ ในแต่ละด้านสามารถสรุปได้ดังภาพที่ 7.2 ในด้านคุณภาพของความต้องการนั้น ผู้ใช้มีระดับความพึงพอใจโดยเฉลี่ยสูงถึง 4.83 รองลงมาคือด้านประโยชน์การใช้งาน ด้วยค่าเฉลี่ยของระดับความพึงพอใจเท่ากับ 4.67 ในขณะที่ด้านคุณสมบัติของเครื่องมือ มีระดับความพึงพอใจในน้อยที่สุด ด้วยค่าเฉลี่ยเท่ากับ 4.50



ภาพที่ 7.2 แผนภูมิเรดาร์แสดงคะแนนความพึงพอใจของผู้ใช้โดยเฉลี่ยที่มีต่อเครื่องมือแต่ละด้าน

7.5 สรุปผลการทดลอง

จากการเปรียบเทียบจะเห็นได้ว่าประสิทธิผลเครื่องมือต้นแบบที่สร้างจากพื้นฐานไวยากรณ์ความมั่นคงสามารถกำหนดความต้องการได้องค์ประกอบครบถ้วนเท่ากันหรือมากกว่าความต้องการที่ระบุด้วยมือ คำสำคัญบางคำที่ผู้ใช้ระบุแต่ไม่ได้นำมาพิจารณาในการเปรียบเทียบเนื่องจากคำสำคัญเหล่านั้นเป็นเพียงส่วนขยายความสำหรับคำนิยามเพื่ออธิบายให้ผู้อ่านเกิดความเข้าใจมากขึ้น

แม้ในกรณีศึกษาที่ 2 ของหน่วยทดลองที่ 1 มีองค์ประกอบความต้องการที่ระบุด้วยมือและเครื่องมือจำนวนเท่ากัน แต่เมื่อพิจารณาประสิทธิภาพ ระยะเวลาในการกำหนดความต้องการด้วยมือใช้เวลา 16 นาที ในขณะที่กำหนดความต้องการด้วยเครื่องมือใช้เวลาเพียง 1 นาที ในกรณีนี้การใช้เครื่องมือสามารถลดระยะเวลาในการกำหนดความต้องการได้ถึง 94 เปอร์เซ็นต์

จากการประเมินระดับความพึงพอใจของของผู้ใช้ที่มีต่อเครื่องมือในแต่ละด้านมีผลอยู่ในระดับดี-ดีมาก โดยมีค่าเฉลี่ยในแต่ละด้านมากกว่า 4 นอกจากนี้ คำแนะนำของผู้ใช้จะนำไปปรับปรุงเครื่องมือให้ง่ายต่อการใช้งานมากยิ่งขึ้น

บทที่ 8
สรุปผลการวิจัย

8.1 ผลสรุปของงานวิจัย

งานวิจัยนี้นำเสนอวิธีการสร้างแบบรูปบริบทความมั่นคงเชิงเว็บและไวยากรณ์ความมั่นคงจากเอกสารดับเบิ้ลยูเอสซียูไอ ตลอดจนพัฒนาเครื่องมือต้นแบบพื้นฐานไวยากรณ์ความมั่นคงเพื่อสนับสนุนกระบวนการวิศวกรรมความต้องการในการกำหนดความต้องการด้านความมั่นคงของระบบ

แบบรูปบริบทความมั่นคงเชิงเว็บ ที่นำเสนอในงานวิจัยนี้มีจำนวน 18 แบบรูป แบ่งเป็น 4 กลุ่ม ได้แก่ การนำการรักษาความมั่นคงของชั้นขนส่งมาประยุกต์ใช้กับเว็บ ตัวชี้บอกและการมีปฏิสัมพันธ์ แนวทางที่ดีที่สุดสำหรับสภาพทนทาน และข้อคำนึงด้านความมั่นคง แบบรูปทั้งหมดได้ผ่านการทวนสอบความครบถ้วนของเนื้อหาเมื่อเทียบกับเอกสารดับเบิ้ลยูเอสซียูไอและสอดคล้องตามองค์ความรู้ด้านความมั่นคง ด้วยหน่วยทดลองจำนวน 16 คน พร้อมทั้งให้ข้อเสนอแนะในการปรับปรุงแบบรูป สรุปผลการประเมินแบบรูปจาก 3 กลุ่มปัจจัย ดังนี้

1) กลุ่มปัจจัยด้านภาพรวมของเอกสารแบบรูป โครงสร้างของแบบรูปง่ายต่อการทำความเข้าใจหรือใช้ในการศึกษา แบบรูปช่วยให้เห็นภาพรวมได้ดี

2) กลุ่มปัจจัยด้านเนื้อหาของแต่ละแบบรูป เนื่องด้วยการนำเสนอเนื้อหาได้ใช้คำศัพท์ทางเทคนิค จึงทำให้การเรียบเรียงประโยคค่อนข้างทำความเข้าใจได้ยาก ต้องพิจารณาองค์ประกอบโครงสร้างภายในของแบบรูปจะเข้าใจได้ดีขึ้น

3) กลุ่มปัจจัยด้านการนำแบบรูปไปประยุกต์ใช้ แบบรูปสามารถช่วยให้เข้าใจรูปแบบการกำหนดความต้องการความมั่นคงได้ครบถ้วน และช่วยให้การออกแบบความต้องการด้านความมั่นคงสมบูรณ์และรวดเร็วขึ้น

ไวยากรณ์ความมั่นคงเพื่อใช้ในการสร้างรายการความต้องการด้านความมั่นคง สร้างจากแบบรูปบริบทความมั่นคงเชิงเว็บที่ผ่านการปรับปรุงตามคำแนะนำของหน่วยทดลอง โดยกำหนดองค์ประกอบและความสัมพันธ์ผ่านแผนภาพต้นไม้ แล้วแปลงเป็นไวยากรณ์ในรูปอีบีเอ็นเอฟ จากนั้นทวนสอบความครบถ้วนของการกำหนดความต้องการความมั่นคงที่ได้จากไวยากรณ์โดยการประยุกต์ใช้ไวยากรณ์ เพื่อแสดงให้เห็นถึงเส้นทางการได้มาซึ่งความต้องการผ่านต้นไม้ความมั่นคงก่อนนำไปฝังตัวในเครื่องมือต้นแบบ

เครื่องมือต้นแบบสร้างจากไวยากรณ์ความมั่นคง แบ่งตามหน้าที่หลักได้ 2 กลุ่มการทำงาน ได้แก่ จัดการโครงการและจัดการรายการความต้องการ ในส่วนของโครงการผู้ใช้สามารถสร้าง แก้ไข ลบ และประเมินรายการความต้องการของแต่ละโครงการว่ามีความคล้อยตามเอกสารดับเบิ้ลยูเอสซียูไอในระดับใด ในขณะที่ส่วนของความต้องการ ผู้ใช้สามารถสร้าง แก้ไข ลบ และนำออกรายการความต้องการของแต่ละโครงการได้ หน้าที่หลักดังกล่าวผ่านการทดสอบเชิงฟังก์ชันด้วยกรณีทดสอบโดยผู้วิจัย จากนั้นหน่วยทดลอง 2 คน กำหนดความต้องการของกรณีศึกษา 2 ระบบ กรณีศึกษา 2 ระบบ คือ ระบบธนาคารอิเล็กทรอนิกส์และระบบสำรองห้องพักและเที่ยวบิน โดยหน่วยทดสอบกำหนดความต้องการด้วยมือเปรียบเทียบกับการกำหนดด้วยเครื่องมือ แล้วประเมินระดับความพึงพอใจพร้อมให้ความคิดเห็นต่อการใช้งานเครื่องมือต้นแบบ ผลการทดลองแบ่งเป็น 2 ดังนี้

1) ผลการเปรียบเทียบรายการความต้องการที่ได้ระหว่างการกำหนดด้วยมือและการกำหนดด้วยเครื่องมือพบว่า เครื่องมือต้นแบบที่สร้างจากพื้นฐานไวยากรณ์ความมั่นคงสามารถกำหนดความต้องการได้องค์ประกอบครบถ้วนเท่าหรือหรือมากกว่าความต้องการที่ระบุด้วยมือ อีกทั้งการใช้เครื่องมือสามารถลดระยะเวลาในการกำหนดความต้องการได้ถึง 94 เปอร์เซ็นต์ แสดงให้เห็นถึงประสิทธิภาพของเครื่องมือในการกำหนดความต้องการได้อย่างครบถ้วน ในเวลาอันรวดเร็ว

2) ผลการประเมินระดับความพึงพอใจของผู้ใช้ที่มีต่อการใช้งานเครื่องมือพบว่า ความต้องการที่ได้จากการใช้เครื่องมือมีความครบถ้วน ถูกต้อง และลดความกำกวม เมื่อเทียบกับการกำหนดด้วยตนเอง เครื่องมือยังสนับสนุนให้เกิดการใช้ซ้ำลดความยุ่งยาก และช่วยให้เกิดความเข้าใจเกี่ยวกับการกำหนดความต้องการ อย่างไรก็ตามเครื่องมือควรปรับปรุงให้สนับสนุนการกำหนดความต้องการได้อย่างเป็นลำดับ

ผลลัพธ์จากงงานวิจัยนี้ คือ แบบรูปบริบทความมั่นคงเชิงเว็บที่มีเนื้อหาสอดคล้องกับเอกสารดับเบิ้ลยูเอสซียูไอและองค์ความรู้ด้านความมั่นคง ไวยาการณ์ความมั่นคงสำหรับสร้างความต้องการที่มีองค์ประกอบสำคัญครบถ้วนตามแบบรูป และเครื่องมือต้นแบบสำหรับกำหนดความต้องการให้คล้อยตามเอกสารดับเบิ้ลยูเอสซียูไอ ได้อย่างครบถ้วน ในเวลาอันรวดเร็ว ลดความยุ่งยาก และสนับสนุนการนำกลับมาใช้ซ้ำได้อีกด้วย

8.2 ข้อจำกัดของงานวิจัย

1) เครื่องมือสนับสนุนการกำหนดความต้องการความมั่นคงพื้นฐานไวยากรณ์ความมั่นคงแต่ผู้ใช้ยังต้องศึกษารายละเอียดแต่ละตัวแปรไปจนถึงศึกษาบริบทของการใช้งานจากแบบรูปความมั่นคงประกอบ

2) รายการความต้องการความมั่นคงที่ได้จากเครื่องมือต้นแบบสอดคล้องกับข้อปฏิบัติและระดับคล้อยตามในเอกสารดับเบิ้ลเอสซียูไอ อย่างไรก็ตามหากมีการแก้ไขข้อความของรายการความต้องการ อาจส่งผลให้ระดับความคล้อยตามที่ประเมินภายหลังการแก้ไขไม่ตรงตามความจริงได้

3) เครื่องมือต้นแบบได้คำนึงถึงการลดรูปประโยคโดยการพิจารณาเส้นทางของไวยากรณ์ทางเลือกที่มีการวนซ้ำหรือส่วนประกอบของต้นไม้ความมั่นคงภายใต้ตัวเลือก (OR gate) ที่มีการเลือกซ้ำได้ (PLUS) เพื่อไม่ให้เกิดความซ้ำซ้อนของประโยคความต้องการ แต่การเลือกรวมทุกความต้องการให้อยู่ภายในหนึ่งขอความจะทำให้เพิ่มความยาวของข้อความความต้องการและเกิดความซับซ้อน

4) ลำดับการกำหนดความต้องการของเครื่องมือต้นแบบที่มีเส้นทางดังได้แสดงในบทที่ 6 หัวข้อ 6.6 อยู่ภายใต้เงื่อนไขก่อนการใช้งานของแต่ละไวยากรณ์ ซึ่งในบางกรณีอาจขัดขวางการเลือกอย่างอิสระโดยผู้ใช้

8.3 งานวิจัยในอนาคต

1) เอกสารดับเบิ้ลยูเอสซียูไอหรือมาตรฐานด้านบริบทความมั่นคงเชิงเว็บในอนาคตอาจมีการปรับแก้ไข ดังนั้นแบบรูปและไวยากรณ์ความมั่นคงควรมีการปรับปรุงให้ทันสมัย

2) แบบรูปสามารถเพิ่มองค์ประกอบที่เกี่ยวข้องกับรหัสข้อบังคับได้ เพื่อให้ง่ายต่อการทวนสอบโดยตามรอย

3) เพิ่มจำนวนและความหลากหลายของหน่วยทดลองรวมทั้งกรณีศึกษาที่ใช้ในการประเมินความพึงพอใจของผู้ใช้ที่มีต่อเครื่องมือ ให้ครอบคลุมกับจำนวนไวยากรณ์ เพื่อผลตอบรับสำหรับการปรับปรุงงานวิจัยให้มีความน่าเชื่อถือมากยิ่งขึ้น

4) เครื่องมือต้นแบบสามารถพัฒนาเส้นทางและลำดับในการกำหนดความต้องการให้ง่ายต่อการใช้งานโดยการจำแนกตามกลุ่มบริการความมั่นคงจากองค์ประกอบคลาสของแบบรูปรวมถึงการจัดลำดับความสำคัญของเส้นทางในการกำหนดความต้องการ

8.4 ผลงานตีพิมพ์จากงานวิทยานิพนธ์

1) ผลงานตีพิมพ์เรื่อง “A method for web security context patterns development from user interface guidelines based on structural and textual analysis” ในการประชุมวิชาการระดับนานาชาติ “The Sixth International Conference on Information Science and Applications (6th ICISA 2015)” ซึ่งจัดขึ้นที่จังหวัดพัทยา ประเทศไทย ระหว่างวันที่ 24–26 กุมภาพันธ์ พ.ศ. 2558

2) ผลงานตีพิมพ์เรื่อง “Constructing patterns verification criteria based on quality attributes: web security context patterns case study” ในการประชุมวิชาการระดับนานาชาติ “15th IEEE/ACIS International Conference on Computer and Information Science (15th ICIS 2016)” ซึ่งจัดขึ้นที่จังหวัดโอกะยะมะ ประเทศญี่ปุ่น ระหว่างวันที่ 26–29 มิถุนายน พ.ศ. 2559

รายการอ้างอิง

1. Gordeychik, S., et al., *Web application security statistics.* The Web Application Security Consortium, 2010.
2. W3C. *Web Security Context: User Interface Guidelines*. 2010 [cited 2013 11 August]; Available from: http://www.w3.org/TR/2010/REC-wsc-ui-20100812/.
3. Bolchini, D., S. Colazzo, and P. Paolini, *Requirements for Aural Web Sites*, in *Proceedings of the Eighth IEEE International Symposium on Web Site Evolution*. 2006, IEEE Computer Society. p. 75-82.
4. Dias, A.L., R.P.d.M. Fortes, and P.C. Masiero, *Increasing the Quality of Web Systems: By Inserting Requirements of Accessibility and Usability*, in *Proceedings of the 2012 Eighth International Conference on the Quality of Information and Communications Technology*. 2012, IEEE Computer Society. p. 224-229.
5. Palomares, C., X. Franch, and C. Quer, *Requirements Reuse and Patterns: A Survey*, in *Requirements Engineering: Foundation for Software Quality*. 2014, Springer. p. 301-308.
6. Supaporn, K., *Defining Security Requirement Using Grammar of Security Patterns*, in *Computer Engineering Department, Engineering Faculty*. 2007, Chulalongkorn University.
7. Dennis, A., B.H. Wixom, and D. Tegarden, *Systems Analysis and Design with UML*. 2012: Wiley.
8. Abran, A. and P. Bourque, *SWEBOK: Guide to the software engineering Body of Knowledge*. 2004: IEEE Computer Society.
9. Schumacher, M., *Security Engineering with Patterns: Origins, Theoretical Models, and New Applications*. 2003: Springer-Verlag New York, Inc. 208.
10. Hong, J.-y., E.-h. Suh, and S.-J. Kim, *Context-aware systems: A literature review and classification.* Expert Systems with Applications, 2009. **36**(4): p. 8509-8522.

11. Lebanidze, E., *Securing enterprise web applications at the source: an application security perspective.* OWASP-The Open Web Application Security Project, 2006.
12. Bradner, S., *RFC 2119 (rfc2119): Key Words for use in RFCs to Indicate Requirement Levels*. 1997, Mar.
13. Close, T. and W.C.W.G. Note. *Web Security Experience, Indicators and Trust: Scope and Use Cases*. 2008 [cited 2013 11 August]; Available from: http://www.w3.org/TR/2008/NOTE-wsc-usecases-20080306/.
14. Schumacher, M., et al., *Security Patterns: Integrating Security and Systems Engineering*. 2013: Wiley.
15. Buschmann, F., *Pattern-Oriented Software Architecture, A System of Patterns*. 1996: Wiley.
16. Naur, P., et al., *Revised report on the algorithmic language Algol 60.* Communications of the ACM, 1963. **6**(1): p. 1-17.
17. Standard, E.S.S., *EBNF: ISO/IEC 14977: 1996 (E).* URL http://www. cl. cam. ac. uk/mgk25/iso-14977. pdf.
18. Supaporn, K., N. Prompoon, and T. Rojkangsadan, *Security Requirements Definition Tool for Security Enterprise and Risk Managements from Security Grammars based-on Security Patterns*, in *NCSEC*. 2007.
19. Riaz, M. and L. Williams. *Security requirements patterns: understanding the science behind the art of pattern writing*. in *Requirements Patterns (RePa), 2012 IEEE Second International Workshop on*. 2012.
20. Hafiz, M., P. Adamczyk, and R.E. Johnson, *Organizing security patterns.* IEEE Software, 2007. **24**(4): p. 52-60.
21. Alvi, A.K. and M. Zulkernine. *A comparative study of software security pattern classifications*. in *Proceedings - 2012 7th International Conference on Availability, Reliability and Security, ARES 2012*. 2012.

ภาคผนวก

ภาคผนวก ก
แบบรูปบริบทความมั่นคงเชิงเว็บ

แบบรูปบริบทความมั่นคงเชิงเว็บที่สร้างจากเอกสารดับเบิ้ลยูเอสซียูไอ (WSC-UI) ในขอบเขตงานวิจัยนี้ ทั้งหมด 18 แบบรูป ซึ่งจำแนกตามที่มาของเนื้อหาได้ 4 กลุ่ม ดังนี้

กลุ่มที่ 1 การนำการรักษาความมั่นคงของชั้นขนส่งมาประยุกต์ใช้กับเว็บ

1) สารสนเทศและการจัดการใบรับรองอิเล็กทรอนิกส์
2) ระดับการรักษาความมั่นคงชั้นขนส่ง
3) ประเภทของเว็บจากการรักษาความมั่นคงชั้นขนส่ง
4) การจัดการสถานการณ์ข้อผิดพลาดเบื้องต้น

กลุ่มที่ 2 ตัวชี้บอกและการมีปฏิสัมพันธ์

1) การส่งสัญญาณอัตลักษณ์
2) ข้อมูลเสริมบริบทความมั่นคงเชิงเว็บ
3) ตัวชี้บอกความมั่นคงชั้นขนส่ง
4) การจัดการและการส่งสัญญาณความผิดพลาด

กลุ่มที่ 3 แนวทางที่ดีที่สุดสำหรับสภาพทนทาน

1) การนิยามส่วนต่อประสานผู้ใช้โครม
2) การป้องกันตัวชี้บอกความมั่นคงจากการลอกเลียนโดยเนื้อหาเว็บ
3) การจัดการกับความสนใจของผู้ใช้
4) ส่วนต่อประสานโปรแกรมประยุกต์ของตัวแทนผู้ใช้เว็บที่เรียกใช้ได้โดยเนื้อหาเว็บ

กลุ่มที่ 4 ข้อคำนึงด้านความมั่นคง

1) การป้องกันการโจมตีระหว่างการรักษาความมั่นคงชั้นขนส่ง
2) ความล้มเหลวในการตรวจสอบสถานะใบรับรอง
3) ข้อพึงระวังในการพิจารณาใบรับรองที่น่าเชื่อถือ
4) การใช้ชื่อภาษาธรรมชาติรวมอยู่ในชื่อโดเมน
5) การป้องกันความล้าของผู้ใช้ต่อการแจ้งเตือน
6) การรับมือกับการเปลี่ยนแปลงเนื้อหาระหว่างการเชื่อมต่อด้วยใบรับรองที่ได้รับประกันเสริม

เกณฑ์การตั้งรหัสแบบรูปนั้นจะขึ้นต้นด้วย “WSCP” (Web Security Context Pattern) ตามด้วยรหัสตัวเลข 2 หลัก โดยหลักสิบอ้างถึงหมายเลขบทของเนื้อหาจากเอกสาร WSC-UI ที่นำมาสร้างแบบรูป และตัวเลขหลักหน่วยแสดงลำดับที่สำหรับแบบรูปความมั่นคง เช่น หัวข้อ 6.3 เมื่อทำเป็นหมายเลขอ้างอิงจะได้ WSCP63 โดยแบบรูปที่นำเสนอมีรายละเอียดดังต่อไปนี้

ตารางที่ ก.1 แบบรูปสารสนเทศและการจัดการใบรับรองอิเล็กทรอนิกส์

Name	สารสนเทศและการจัดการใบรับรองอิเล็กทรอนิกส์	**ID**	WSCP51
Core	Authentication	**Section**	Applying TLS to the Web
Description			
แบบรูปนี้กล่าวถึงกระบวนการจัดการและนิยามที่เกี่ยวข้องกับใบรับรองอิเล็กทรอนิกส์ (Public Key Certificates, **Certificate**) ที่นิยมใช้ในการรักษาความมั่นคงชั้นขนส่ง (Transport Layer Security: TLS) เพื่อให้เข้าใจถึงคุณลักษณะและการจัดการเบื้องต้นของใบรับรองแต่ละประเภทโดยตัวแทนผู้ใช้เว็บประเภทใบรับรองและการจัดการใบรับรองดังกล่าวจะถูกนำมาใช้เป็นข้อมูลพื้นฐานในการแสดงบริบทความมั่นคงเชิงเว็บ (Web Security Context) รวมถึงการจัดการกับข้อผิดพลาดหรือจุดอ่อนที่อาจเกิดขึ้นในระหว่างการรักษาความมั่นคงชั้นขนส่ง (TLS) ในแบบรูปลำดับต่อไป			
Example			
กรณีที่ 12 เบ็ตตี้กำลังวางแผนการท่องเที่ยวไปต่างประเทศจากการสืบค้นผ่านเว็บ เธอค้นเจอบริษัทนำเที่ยวที่ได้รับการแนะนำอย่างกว้างขวางในท้องถิ่น เมื่อเธอเชื่อมต่อกับเว็บไซต์ของบริษัทนำเที่ยว ตัวแทนผู้ใช้เว็บของเธอไม่รู้จักองค์กรที่ออกใบรับรองให้แก่เว็บบริษัทนำเที่ยวนั้น **กรณีที่ 8** เบ็ตตี้เยี่ยมชมเว็บไซต์ example.com เป็นบางครั้ง ในแต่ละครั้งที่เชื่อมต่อ ตัวแทนผู้ใช้เว็บของเธอจะได้รับใบรับรองของผู้ให้บริการในการรักษาความมั่นคงชั้นส่งจากองค์กรผู้ออกใบรับรองเดียวกัน ในการเชื่อมต่อครั้งนี้ ใบรับรองที่ได้รับถูกออกโดยองค์กรผู้ออกใบรับรองอื่น			
Context			
ใบรับรองอิเล็กทรอนิกส์ของผู้ให้บริการเว็บ (Web Server, **WebServer**) ที่อนุมัติโดยองค์กรผู้ออกใบรับรอง (Certificate Authority: CA, **CertificateAuthority**) ถูกนำมาใช้ในการการรักษาความมั่นคงชั้นขนส่ง (TLS) เมื่อตัวแทนผู้ใช้ติดต่อกับผู้ให้บริการเว็บ ตัวแทนผู้ใช้ต้องตรวจสอบใบรับรองและทวนสอบไปยังห่วงโซ่ใบรับรองผู้อนุมัติใบรับรองดังกล่าว (Certificate Chain) ตัวแทนผู้ใช้เว็บจำเป็นต้องจัดการกับการยอมรับหรือปฏิเสธใบรับรองดังกล่าว			
Problem			
ตัวแทนผู้ใช้เว็บ (Web User Agents, **WebUserAgent**) ในปัจจุบัน ใบรับรองอิเล็กทรอนิกส์นิยมใช้ในการรักษาความมั่นคงชั้นขนส่งเมื่อเกิดข้อผิดพลาดหรือสิ่งผิดปกติในระหว่างการเชื่อมต่อตัวแทนผู้ใช้ในส่วนใหญ่รองรับการจัดการกับเหตุการณ์ดังกล่าวได้โดยแสดงข้อมูลใบรับรองพร้อมเสนอตัวเลือกให้แก่ผู้ใช้เพื่อพิจารณาและตอบสนองตัวเลือกเหล่านั้นในระหว่างการใช้งานเว็บอย่างไรก็ตามผู้ใช้ส่วนใหญ่ยังเพิกเฉยต่อการตัดสินใจในสถานการณ์ดังกล่าว เนื่องจากขาดข้อมูลที่แสดงถึงความน่าเชื่อถือของใบรับรองที่ใช้ในการพิสูจน์ตัวจริงของผู้ให้บริการว่าเป็นเว็บที่ผู้ใช้ต้องการเข้าถึงจริงหรือไม่ กล่าวคือ เมื่อระบบให้ผู้ใช้พิจารณายอมรับใบรับรองของเว็บใดๆ ผู้ใช้อาจเกิดละเลยการคำนึงถึงความมั่นคง โดยเฉพาะผู้ใช้ที่ไม่มีความรู้เกี่ยวข้องกับความมั่นคงอาจตัดสินใจโดยปราศจากการพิจารณาบริบทความมั่นคงเชิงเว็บ อีกทั้งกิจกรรมและข้อมูลต่างๆ ในการออกใบรับรองโดยองค์กรผู้ออกใบรับรอง (CA) มีความหลากหลาย ทำให้ตัวแทนผู้ใช้เว็บไม่สามารถนำมาข้อมูลจากใบรับรองมากใช้ประโยชน์ในการแสดงบริบทความมั่นคงเชิงเว็บได้เท่าที่ควร			

ตารางที่ ก.1 แบบรูปสารสนเทศและการจัดการใบรับรองอิเล็กทรอนิกส์ (ต่อ)

Name	สารสนเทศและการจัดการใบรับรองอิเล็กทรอนิกส์	**ID**	WSCP51
Solution			

ตัวแทนผู้ใช้ต้องจำแนกและจัดการกับใบรับรองอิเล็กทรอนิกส์แต่ละประเภท เพื่อคัดกรองข้อมูลที่จะนำมาแสดงบริบทความมั่นคงให้แก่ผู้ใช้ในการพิจาณาความมั่นคงของเว็บที่กำลังเข้าถึง ใบรับรองแต่ละประเภทที่มีระดับความมั่นคงต่างกันขึ้นอยู่กับลักษณะข้อมูลและผู้บริการออกใบรับรองการจัดการใบรับรองเบื้องต้นทำได้โดยการจัดเก็บใบรับรองที่เชื่อถือได้ไว้ภายในพื้นที่จัดเก็บของตัวแทนผู้ใช้ รวมถึงการพิจารณาจากการตอบสนองหรือปฏิสัมพันธ์ของผู้ใช้ที่เคยเกิดขึ้นกับใบรับรองนั้นๆ ตลอดจนการทวนสอบห่วงโซ่ใบรับรองที่อนุมัติโดยองค์กรผู้ออกใบรับรอง (CA) การจัดการใบรับรองและประเภทมีรายละเอียด ดังนี้

1. **ใบรับรองที่เชื่อถือได้หรือใบรับรองใดๆ** ใบรับรองที่เชื่อถือได้ (Trust Anchors: TA, **TrustAnchor**) ถือครองโดยองค์กรผู้ออกใบรับรอง(CA) ใบรับรองดังกล่าวปรากฏกุญแจสาธารณะ (Public Key) และข้อมูลที่เกี่ยวข้อง โดยกุญแจสาธารณะจะถูกใช้ในการทวนสอบลายเซ็นต์ดิจิทัล (Digital Signatures) และข้อมูลที่เกี่ยวข้องจะถูกใช้ในการจำกัดประเภทข้อมูลสำหรับใบรับรองที่ได้รับอำนาจการจัดการใบรับรองดังกล่าวทำได้ 2 วิธี ดังนี้

1.1 **การติดตั้งและอัพเดตใบรับรองที่เชื่อถือได้** (Trust Anchor Installation and update, **TAinstallation**) โดยปกติการติดตั้ง ใบรับรองที่เชื่อถือได้ (TA) ไว้ในพื้นที่จัดเก็บจะถูกจัดการโดยผู้จำหน่ายตัวแทนผู้ใช้ (User Agent Vendors) ผู้ดูแลระบบ (Systems Administrators) และผู้ผลิตอุปกรณ์ (Device Manufacturers) นอกเหนือจากการติดตั้งใบรับรองที่เชื่อถือได้ (TA) แล้วยังอาศัยข้อมูลนอกแถบ (Out-of-band Information) เพื่อใช้ในการอัพเดตใบรับรองที่เชื่อถือได้ (TA) ดังนั้นการจัดการส่วนใหญ่จึงอยู่ในส่วนของตัวแทนผู้ใช้เว็บหรือการอัพเดตซอฟต์แวร์ของระบบปฏิบัติการ (Operating System Software Updates)

1.2 **การยอมรับใบรับรองเชิงโต้ตอบ** (Interactively Accepting**, InteractivelyAccepting**) หากใบรับรองของผู้ให้บริการเว็บใดๆ ที่ไม่สามารถตรวจสอบได้โดยใช้อัลกอริทึมการทวนสอบวิถีขั้นต้น (Basic Path Validation Algorithm) ข้อผิดพลาดนี้อาจกระตุ้นให้ตัวแทนผู้ใช้เว็บเสนอตัวเลือกให้กับผู้ใช้เพื่อตอบรับใบรับรองดังกล่าวสำหรับระยะเวลาสั้นๆ หรือ บางครั้งตลอดช่วงเวลาที่สื่อสารกับใบรับรองนั้นๆ ไปจนถึงจดจำการติดต่อกับใบรับรองดังกล่าวในอนาคต โดยการยอมรับเชิงโต้ตอบสำหรับใบรับรองที่เชื่อถือได้ (TA) หรือใบรับรองใดๆ นั้นจะต้องเกิดขึ้นในระหว่างการมีปฏิสัมพันธ์ของผู้ใช้ ซึ่งผู้ใช้ให้ความสนใจกับการใช้งานหลักอย่างการเข้าถึงเนื้อหาเว็บไม่รวมถึงในระหว่างที่ผู้ใช้จัดการใบรับรองโดยการตั้งค่าความมั่นคงของตัวแทนผู้ใช้เว็บ

การพัฒนาต้องไม่เปิดทางให้ผู้ใช้กำหนดใบรับรองลำดับบนสุดที่เชื่อถือได้ (Trusted Root) ด้วยวิธี Augmented Assurance Qualified ในขณะที่ผู้ใช้ไม่ได้ปฏิสัมพันธ์กับระบบ เนื่องจากวิธีดังกล่าวต้องกระทำโดยระบบเท่านั้น ผู้ใช้สามารถกำหนดรากใบรับรองที่เชื่อถือได้จากวิธีการยอมรับเชิงโต้ตอบ (Interactively Accepted) เพียงช่องทางเดียว

ตารางที่ ก.1 แบบรูปสารสนเทศและการจัดการใบรับรองอิเล็กทรอนิกส์ (ต่อ)

Name	สารสนเทศและการจัดการใบรับรองอิเล็กทรอนิกส์	**ID**	WSCP51
Solution			
2. **ใบรับรองที่ได้รับประกันเสริม** (Augmented Assurance Certificates; AAC**, AugmentedAssurance-Certificates**) คือ ใบรับรองอิเล็กทรอนิกส์ที่องค์กรผู้ออกใบรับรองนั้นยืนยันได้ว่าเนื้อหาของผู้ร้องขอใบรับรองได้ถูกพิสูจน์ตัวจริงโดยกระบวนการที่ระบุในรายการความต้องการของการรับประกันเสริม (EVTLSCERT) ใบรับรองที่อยู่ภายใต้ห่วงโซ่ใบรับรองดังกล่าวต้องถูกทวนสอบไปยังรากของใบรับรองที่เชื่อถือได้ (Trusted Root) ตรงตามเงื่อนไขการประกันเสริม ใบรับรองจะถูกจำแนกได้โดยตัวแทนผู้ใช้เว็บ และข้อมูลจากใบรับรองประเภทนี้จะถูกนำมาใช้ให้เกิดบริบทความมั่นคงของตัวแทนผู้ใช้เว็บ โดยมีรายละเอียดการจัดการ (**HandlingAAC**) ดังนี้ 2.1 **การจำแนกใบรับรองที่ได้รับประกันเสริม** ตัวแทนผู้ใช้เว็บจะพิจารณาคุณสมบัติของใบรับรองที่ได้รับประกันเสริม (Augmented Assurance Qualified) ซึ่งเป็นขั้นตอนความมั่นคงที่สำคัญและส่วนใหญ่มักจะเกี่ยวข้องกับการใช้โปรแกรมจำเพาะนอกแถบ (Application-specific Out-of-band) เพิ่มเติมจากการกำหนดกระบวนการนอกแถบ (Out of band Mechanism) ที่ได้กล่าวในการติดตั้งและอัพเดตใบรับรองที่เชื่อถือได้ข้างต้น ใบรับรองที่ได้รับประกันเสริม (AAC) ที่เป็นส่วนหนึ่งของห่วงโซ่ใบรับรองที่เชื่อมโยงไปยังใบรับรองที่เชื่อถือได้ (TA) อาจต้องทำเครื่องหมายพิเศษ (Specially Marked) โดยตัวระบุอ็อบเจกต์นโยบายจำเพาะ (Specific Policy Object Identifiers) 2.2 **การแสดงบริบทความมั่นคงเชิงเว็บจากใบรับรองที่ได้รับประกันเสริม** เนื่องจากใบรับรองดังกล่าวมีความน่าเชื่อถือสูงจึงสมควรสามารถนำข้อมูลมาใช้ในตัวชี้บอกความมั่นคงแบบปฐมภูมิ (Primary Security Indicators) ซึ่งเป็นส่วนต่อประสานผู้ใช้ที่ต้องปรากฏสถานะความมั่นคงของเว็บโดยปราศจากการร้องขอจากผู้ใช้ ตัวแทนผู้ใช้ควรใช้ข้อมูลที่สามารถอ่านได้จากใบรับรองประกันเสริม เช่น องค์กร (Organization) ประเทศ (Country) เป็นลักษณะประจำโดยข้อมูลที่ใช้จะต้องรับรองโดยประกันเสริมขององค์กรผู้ออกใบรับรอง (CA) ในอนาคตใบรับรองประเภทนี้อาจเป็นที่นิยมมากขึ้นเมื่อความน่าเชื่อถือของอัต-ลักษณ์ของผู้ถือครองเพิ่มมากขึ้น ตัวแทนผู้ใช้สามารถใช้ประโยชน์จากระดับการรับประกันเพิ่มเติมและข้อมูลอัตลักษณ์ที่ไม่ขัดแย้งกับข้อกำหนดนี้ เช่น ในอนาคตใบรับรองสามารถรับประกันเสริมแบบรายบุคคลได้ 3. **ใบรับรองที่ผ่านการตรวจสอบความสมเหตุสมผล (Validated Certificates: VC, ValidatedCertificate)** เพื่ออธิบายใบรับรองที่ได้ถูกทวนสอบแล้วว่าห่วงโซ่ใบรับรองนั้นได้เชื่อมโยงไปยังรากที่เชื่อถือได้ (Trusted Root) ที่ตรงกับใบรับรองที่เชื่อถือได้ (TA) ที่ตั้งค่าไว้ภายในตัวแทนผู้ใช้ ใบรับรองประเภทนี้รับรองได้เพียงแค่ชื่อโดเมนที่ลงทะเบียนและกุญแจอิเล็กทรอนิกส์นั้นสัมพันธ์กันไม่รับรองลักษณะประจำอื่นๆ ใบรับรองอื่นๆ เช่น ใบรับรองประกันเสริม (AAC) ที่ถูกต้อง นั้นถือว่าเป็นใบรับรองที่ผ่านการตรวจสอบความสมเหตุสมผลด้วยเช่นกัน			

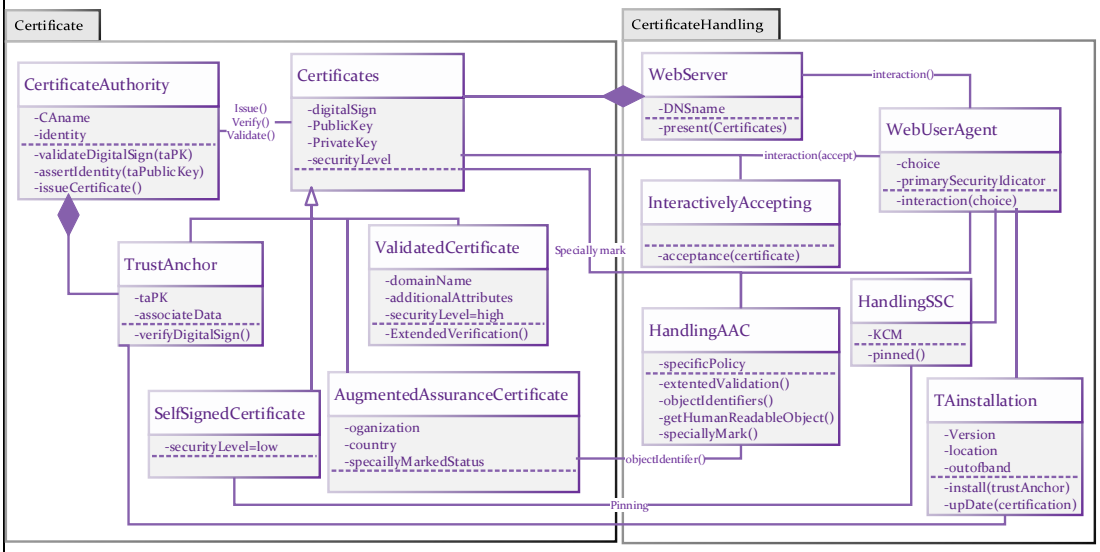
ตารางที่ ก.1 แบบรูปสารสนเทศและการจัดการใบรับรองอิเล็กทรอนิกส์ (ต่อ)

Name	สารสนเทศและการจัดการใบรับรองอิเล็กทรอนิกส์	**ID**	WSCP51
Solution			
4. **ใบรับรองที่ลงนามโดยตนเองและใบรับรองที่เชื่อมโยงไปยังรากเชื่อถือไม่ได้ (Self-signed Certificates: SSC and Untrusted Root Certificates)**ใบรับรองที่ลงนามโดยตนเอง (SSC, **SelfSignedCertificate**) เป็นใบรับรองที่ไม่มั่นคง นิยมใช้สำหรับเว็บไซต์ที่ให้บริการกับผู้ใช้กลุ่มเล็กๆ และให้บริการในรูปแบบของการใช้กุญแจเข้ารหัส (Cryptographic Key Material) ในการแลกเปลี่ยนข้อมูลการเข้ารหัส (Key Exchange) ที่ไม่ถูกตรวจสอบโดยองค์กรผู้ออกใบรับรองใดๆ (Third Party) รวมทั้งห่วงโซ่ใบรับรองที่เชื่อมโยงไปยังรากใบรับรองที่ไม่ตรงกันกับใบรับรองที่เชื่อถือได้ (TA) ในพื้นที่จัดเก็บรากที่เชื่อถือได้ของตัวแทนผู้ใช้ก็นับว่าเป็นใบรับรองที่เชื่อถือไม่ได้เช่นเดียวกัน ใบรับรองที่เชื่อถือไม่ได้ ไม่ควรจัดเก็บอยู่ภายในพื้นที่ของใบรับรองที่เชื่อถือ การจัดการใบรับรองที่เชื่อถือไม่ได้ (**HandlingSSC**) ทำได้ 2 วิธี ดังนี้ 4.1 **การจัดการความต่อเนื่องของกุญแจอิเล็กทรอนิกส์ (Key Continuity Management: KCM)** ช่วยจัดการกับใบรับรองที่ไม่ได้เชื่อมโยงไปยังรากที่เชื่อถือไม่ได้ (Untrusted Root) หรือใบรับรองที่ลงนามโดยตนเอง (SSC) โดยตัวแทนผู้ใช้สามารถใช้ใบรับรองดังกล่าวเพื่อตัดสินว่าช่องทางการสื่อสารมีความต้องกันกับผู้ให้บริการเว็บที่ผู้ใช้ได้เข้าถึงก่อนหน้านี้หรือไม่ เพื่อป้องกันการโจมตีโครงข่าย (Passive Attack) กล่าวคือ ผู้ให้บริการเว็บแสดงใบรับรองที่มีความต้องกันนั่นหมายถึงการสื่อสารดังกล่าวปราศจากโจมตีเครือข่าย ในทางตรงกันข้าม หากมีการเปลี่ยนแปลงใดที่เกิดขึ้นกับใบรับรองของผู้ให้บริการเดียวกันนี้ ก็สามารถแสดงได้ว่ามีการโจมตีเกิดขึ้นอีกนัยหนึ่งคือผู้ให้บริการเว็บที่ปฏิบัติถูกต้องตามกฎนั้นมีการเปลี่ยนแปลงใบรับรองหลายใบ 4.2 **การปักหมุด (Pinning)** ตัวแทนผู้ใช้อาจรองรับการปักหมุดใบรับรองที่ลงนามโดยตนเอง (SSC) หรือใบรับรองใดๆ ที่เชื่อมโยงไปยังรากเชื่อถือไม่ได้ (Untrusted Root) ไปยังเว็บไซต์นั้น โดยอาศัยการมีปฏิสัมพันธ์ที่ช่วยให้ผู้ใช้สามารถปักหมุดใบรับรองไปยังเว็บไซต์ปลายทางและจดจำสถานะของใบรับรองดังกล่าวเพื่อไม่ให้แสดงข้อความแจ้งเตือนซ้ำเมื่อเว็บไซต์ดังกล่าวแสดงใบรับรองที่ต้องกันกับเว็บไซต์ที่เยี่ยมชมก่อนหน้า ระบุโดยโดเมน (Domain) เค้าร่างยูอาร์ไอ (URI schema) และพอร์ต (Port) แต่การมีปฏิสัมพันธ์ดังกล่าวไม่ควรก่อให้เกิดการปักหมุดใบรับรองไปยังปลายทางมากกว่าหนึ่งเว็บไซต์ และไม่ก่อให้เกิดการยอมรับใบรับรองจากแหล่งที่ไม่น่าเชื่อถืออย่างอัตโนมัติ			

ตารางที่ ก.1 แบบรูปสารสนเทศและการจัดการใบรับรองอิเล็กทรอนิกส์ (ต่อ)

Name	สารสนเทศและการจัดการใบรับรองอิเล็กทรอนิกส์	ID	WSCP51

Internal Structure



แผนภาพคลาสแสดงโครงสร้างของรับรองและความสัมพันธ์ระหว่างการจัดการกับใบรับรองแต่ละเภท

Example Resolved

กรณีที่ 12 เบ็ตตี้กำลังวางแผนการท่องเที่ยวไปต่างประเทศจากการสืบค้นผ่านเว็บ เธอค้นเจอบริษัทนำเที่ยวที่ได้รับการแนะนำอย่างกว้างขวางในท้องถิ่น เมื่อเธอเชื่อมต่อกับเว็บไซต์ของบริษัทนำเที่ยว ตัวแทนผู้ใช้เว็บที่ติดตั้งและปรับปรุงฐานข้อมูลของใบรับรองที่เชื่อถือได้แล้วจะสามารถตรวจสอบความสมเหตุสมผลของใบรับรองและทำเครื่องหมายพิเศษสำหรับใบรับรองที่ได้รับประกันเสริมได้ ทั้งยังนำข้อมูลจากใบรับรองดังกล่าวไปใช้ในการแสดงบริบทความมั่นคงเชิงเว็บ หากใบรับรองของเว็บบริษัทนำเที่ยวนั้นไม่ปรากฏในฐานข้อมูลใบรับรองที่เชื่อถือได้ ตัวแทนผู้ใช้เว็บอาจเสนอข้อมูลและตัวเลือกให้ผู้ใช้พิจารณายอมรับใบรับรอง รวมถึงจดจำสถานะโดยการปักหมุดใบรับรองดังกล่าวเพื่อไม่ให้แสดงข้อความแจ้งเตือนซ้ำ

กรณีที่ 8 เบ็ตตี้เยี่ยมชมเว็บไซต์ example.com เป็นบางครั้ง ในแต่ละครั้งที่เชื่อมต่อ ตัวแทนผู้ใช้เว็บของเธอจะได้รับใบรับรองจากผู้ให้บริการเว็บเพื่อการรักษาความมั่นคงชั้นส่งจากองค์กรผู้ออกใบรับรองเดียวกัน ในการเชื่อมต่อครั้งนี้ ใบรับรองที่ได้รับถูกออกโดยองค์กรผู้ออกใบรับรองอื่น ตัวแทนผู้ใช้เว็บที่มีการจัดการความต่อเนื่องของกุญแจอิเล็กทรอนิกส์ (Key Continuity Management: KCM) ช่วยจัดการกับใบรับรองหากมีการเปลี่ยนแปลงใดที่เกิดขึ้นกับใบรับรองของผู้ให้บริการเดียวก็สามารถแสดงได้ว่ามีการโจมตีเกิดขึ้น

ตารางที่ ก.1 แบบรูปสารสนเทศและการจัดการใบรับรองอิเล็กทรอนิกส์ (ต่อ)

Name	สารสนเทศและการจัดการใบรับรองอิเล็กทรอนิกส์	**ID**	WSCP51
Known Uses			
หัวข้อต่อไปนี้กล่าวถึงคำแนะนำเพิ่มเติมจากผลเฉลยของแบบรูป 1. การยอมรับเชิงโต้ตอบ (Interactively Acceptance) เกิดขึ้นเมื่อใบรับรองของผู้ให้บริการเว็บถูกแสดงขึ้นเพื่อร้องขอการยอมรับจากผู้ใช้ในระหว่างการมีปฏิสัมพันธ์ทั่วไปกับเว็บแล้วใบรับรองนั้นถูกยอมรับโดยผู้ใช้ แต่ถ้าผู้ดูแลระบบหรือผู้ใช้เป็นผู้กระทำการเพิ่มใบรับรองที่เชื่อถือได้เข้าสู่พื้นที่จัดเก็บใบรับรองที่เชื่อถือของตัวแทนผู้ใช้เว็บแล้วใบรับรองนั้นจะไม่ถูกพิจารณาให้เป็นการยอมรับเชิงโต้ตอบ 2. ใบรับรองประกันเสริม (AAC) ที่ยอมรับและนิยมปฏิบัติตามในปัจจุบัน คือ Extended Validation Certificates 3. แนวความคิดของใบรับรองที่ผ่านการตรวจสอบความสมเหตุสมผล (VC) ในข้อกำหนดนี้สัมพันธ์กับใบรับรองความสมเหตุสมผลของโดเมน (Domain validated certificate) ที่ติดตั้งบนผู้ให้บริการ ตัวอย่างของการพิจารณาใบรับรองที่ผ่านการตรวจสอบความสมเหตุสมผล 3.1 ใบรับรองประกันเสริม (AAC) ที่ถูกต้องนั้นถือว่าเป็นใบรับรองที่ผ่านการตรวจสอบความสมเหตุสมผลด้วยเช่นกัน แนวคิดของใบรับรองในข้อกำหนดนี้สัมพันธ์กับใบรับรองความสมเหตุสมผลของโดเมน (Domain validated certificate) 3.2 ใบรับรองหรือห่วงโซ่ใบรับรองที่ปักหมุดไปยังปลายทาง (Pinned) จะไม่ถูกพิจารณาว่าเป็นใบรับรองที่ผ่านการตรวจสอบความสมเหตุสมผลเนื่องจากคุณสมบัติของการปักหมุด 3.3 ใบรับรองที่ลงนามโดยตนเอง (SSC) และใบรับรองที่ออกโดยองค์กรที่ไม่น่าเชื่อถือ (Untrusted Root Certificates) มีการรักษาความมั่นคงชั้นขนส่ง (TLS) ในการปกป้องบริการจากผู้โจมตีระบบ แต่ไม่มีการยืนยันข้อมูลอัตลักษณ์โดยองค์กรที่ออกใบรับรองใดๆไปยังกุญแจในการเข้ารหัส ใบรับรองดังกล่าวจะไม่ถูกพิจารณาว่าเป็นใบรับรองที่ผ่านการตรวจสอบความสมเหตุสมผล		
Consequences			
ข้อมูลผู้ถือครองเว็บส่งผลต่อการความไว้ใจของผู้ใช้ในการมีปฏิสัมพันธ์กับเว็บ การจัดการใบรับรองโดยตัวแทนผู้ใช้จะช่วยให้ลดภาระการตัดสินใจของผู้ใช้สร้างบริบทความมั่นคงที่สนับสนุนการตัดสินใจของผู้ใช้ ทั้งยังเตือนเมื่อเข้าถึงเว็บที่มีการโจมตีหรือสวมรอยโดยผู้ให้บริการรายอื่น			
See Also			
- ศึกษาข้อมูลหรือกลไกนอกแถบ (Out-of-band information and mechanism) ได้จากเอกสาร Online Certificate Status Protocol (OCSP) หรือ Certificate Revocation List (CRL) ภายนอกแบบรูป - แบบรูปได้กำหนดความต้องการในการจัดการกับใบรับรองประกันเสริม (AAC) ที่ศึกษาได้จากเอกสารมาตรฐาน Guidelines for the Issuance and Management of Extended Validation Certificates (EVTLSCERT) - ตัวอย่างปัญหาของแบบรูปนี้อ้างถึง Case 8, 12 จากเอกสาร WSC-USECASES			

ตารางที่ ก.2 แบบรูประดับการรักษาความมั่นคงชั้นขนส่ง

Name	ระดับการรักษาความมั่นคงชั้นขนส่ง	**ID**	WSCP52
Core	Confidentiality	**Section**	Applying TLS to the Web
Description			
แบบรูปนี้อธิบายระดับการรักษาความมั่นคงชั้นขนส่ง (TLS) ขณะที่ตัวแทนผู้ใช้เชื่อมต่อกับผู้ให้บริการเว็บโดยใช้ยูอาร์ไอ (URI) ในการระบุทรัพยากรเว็บที่ต้องการเข้าถึงกลไกการประยุกต์ใช้การรักษาความมั่นคงชั้นขนส่งในปัจจุบันที่ได้รับการปรับปรุงเกณฑ์วิธีขนส่งข้อความหลายมิติให้ดีขึ้น (Upgrading to TLS Within HTTP/1.1) ถือเป็นอีกตัวเลือกหนึ่งแต่ไม่เป็นที่นิยมนำไปใช้หรือแทบที่จะไม่ถูกใช้งานเลยในขณะที่กลไกพื้นฐานเค้าร่างเกณฑ์วิธีขนส่งข้อความหลายมิติที่มั่นคงยูอาร์ไอ (https URI scheme) เป็นที่นิยมใช้และเป็นที่รู้จักดี การรักษาความมั่นคงชั้นขนส่งภายในแบบรูปนี้เป็นไปตามเอกสารการรักษาความมั่นคงชั้นขนส่งระหว่างติดต่อกับเว็บ			
Example			
กรณีที่ 11 เบ็ตตี้พยายามเชื่อมต่อเว็บไซต์ที่ <https://www.example.com/> การพัฒนาความมั่นคงชั้นขนส่งในตัวแทนผู้ใช้ของเธอตรวจพบว่าชื่อโดเมนที่ระบุไว้ในใบรับรองต่างจาก www.example.com			
Context			
ตัวแทนผู้ใช้ที่ประยุกต์ใช้การรักษาความมั่นคงชั้นขนส่ง (TLS) ประเภทใดก็ตามระหว่างการเชื่อมต่อผู้ให้บริการเว็บ (HTTP transaction) โดยเฉพาะเมื่อที่อยู่ของเว็บ (http URI) นั้นอ้างอิงกลับ (Dereferenced)			
Problem			
ยูอาร์แอลที่ถูกนำมาใช้อ้างถึงทรัพยากรเว็บส่วนใหญ่ไม่ประยุกต์ใช้ความมั่นคงชั้นขนส่งหรือการป้องกันที่คล้ายกันนั้น ผู้โจมตีที่เข้าถึงชั้นโครงข่าย (Network Layer) สามารถแทนที่ยูอาร์แอลที่ผู้ใช้ร้องขอด้วยยูอาร์แอลใหม่ที่เลือกโดยผู้โจมตี เปลี่ยนได้แม้กระทั่งข้อความเชื่อมโยงหลายมิติ (hyper-link) ที่อ้างถึงหน้าเว็บปลายทางที่ผู้ใช้ประสงค์จะเข้าถึง ให้เป็นหน้าเว็บที่ผู้โจมตีเลือกการนำทางที่ไร้การป้องกันดังกล่าวหากผู้ใช้ไม่ได้รับข้อมูลหรือสถานะของเว็บที่เข้าถึงว่ามีการรักษาความมั่นคงชั้นขนส่ง รวมถึงการเชื่อมต่อการรักษาความมั่นคงชั้นขนส่งสำเร็จหรือล้มเหลว ผู้ใช้จะแน่ใจได้อย่างไรว่าข้อมูลที่ถูกส่งผ่านเว็บดังกล่าวได้รับการเข้ารหัสให้ยากต่อการโจมตี			
Solution			
เพื่อให้เกิดความมั่นคงของตัวแทนผู้ใช้ในระหว่างการเชื่อมต่อผู้ให้บริการเว็บ (HTTP transaction, **HTTPtransaction**) การเชื่อมต่อใดๆ ที่ได้รับการปกป้องการเชื่อมต่อจะถูกเรียกว่าการปกป้องด้วยความมั่นคงชั้นขนส่ง (TLS-protected, **TLSprotected**) เมื่อทรัพยากรเว็บนั้นถูกระบุด้วยยูอาร์ไอ (URI) ผ่านเค้าร่างเกณฑ์วิธีขนส่งข้อความหลายมิติที่มั่นคงยูอาร์ไอ (https URI scheme) และ การติดต่อการรักษาความมั่นคงชั้นขนส่ง (TLS handshake) ได้ถูกกระทำอย่างเสร็จสมบูรณ์แล้วนั้นการเชื่อมต่อผู้ให้บริการเว็บ (HTTP transaction) ดังกล่าวได้เชื่อมต่อผ่านช่องทางที่รักษาความมั่นคงชั้นขนส่ง (TLS channel) แม้ด้วยขั้นตอนวิธีอย่างง่าย (weak algorithms)			

ตารางที่ ก.2 แบบรูประดับการรักษาความมั่นคงชั้นขนส่ง (ต่อ)

Name	ระดับการรักษาความมั่นคงชั้นขนส่ง	**ID**	WSCP52
Solution			

เกณฑ์วิธีการรักษาความมั่นคงของชั้นขนส่ง (TLS protocol) ถูกแบ่งเวอร์ชันตามการหน้าที่งาน (features) และชุดรหัส (cipher suites) ที่พร้อมใช้งานโดยความแข็งแกร่งของชุดรหัสขึ้นอยู่กับขั้นตอนวิธี (Algorithm) และความยาวของกุญแจ (Key length) ที่ใช้ในการเข้ารหัส (cryptographic function)

ขั้นตอนวิธีในการรักษาความมั่นคงชั้นขนส่งที่แข็งแกร่ง (Strong TLS Algorithms, **Strongly-TLSalgorithm**) ต้องปฏิบัติตามเงื่อนไขดังต่อไปนี้

1. เกณฑ์วิธีการรักษาความมั่นคงของชั้นขนส่ง (TLS protocol) ที่ได้นำมาใช้ต้องเป็นเวอร์ชันที่ไม่มีข้อบกพร่องด้านความมั่นคง เช่น เวอร์ชันของเอสเอสเอล (Secure Socket Layer, SSL) ที่ต่ำกว่า SSLv3 ต้องไม่ถูกพิจารณาว่าแข็งแกร่ง
2. ชุดรหัส (Cipher suite) ที่เลือกมีความแข็งแกร่งของกุญแจ (key) และขั้นตอนวิธี (algorithm) สัมพันธ์กับวิธีปฏิบัติของภาคอุตสาหกรรม ในขณะที่ร่างเอกสารนี้การนำออกชุดรหัส (export cipher suites) นั้นเป็นสิ่งต้องห้าม ต้องไม่ถูกนำมาพิจารณาว่าแข็งแกร่ง

การกำหนดความแข็งแกร่งและความสามารถของเกณฑ์วิธีการรักษาความมั่นคงของชั้นขนส่ง (TLS protocol) และกลไกการเข้ารหัส (cryptographic) ที่นำมาใช้จะทำให้เกิดความมั่นคงและความเป็นส่วนตัว (Privacy) ของการเชื่อมต่อระหว่างตัวแทนผู้ใช้และผู้ให้บริการเว็บโดยระดับความมั่นคงระหว่างการเชื่อมต่อที่รักษาความมั่นคงชั้นขนส่งแบ่งได้ 2 ประเภท ตามความแข็งแกร่งของการปกป้องความมั่นคงชั้นขนส่ง มีรายละเอียดดังนี้

1. **การปกป้องด้วยความมั่นคงชั้นขนส่งอย่างแข็งแกร่ง** (Strongly TLS-protected**, StronglyTLSprotected**) นั้นคือการปกป้องด้วยความมั่นคงชั้นขนส่ง (TLS-protected) ที่ใช้ขั้นตอนวิธีในการรักษาความมั่นคงชั้นขนส่งที่แข็งแกร่ง (Strong TLS Algorithm) มีการต่อรองสำหรับการป้องด้านการรักษาความลับ (confidentiality) และบูรณภาพของระบบ (Integrity) โดยถูกต้องตามเงื่อนไขดังต่อไปนี้อย่างน้อย 1 ข้อ

1.1 ผู้ให้บริการเว็บ (Server) ได้ใช้ใบรับรองที่ผ่านการตรวจสอบความสมเหตุสมผล (Validated Certificate, **VC**) ที่ตรงกับยูอาร์ไอที่อ้างอิงกลับ (Dereferenced URI) หรือ

1.2 ผู้ให้บริการเว็บ (Server) ได้ใช้ใบรับรองโดยตนเอง (Self-Signed Certificate, **SSC**) ที่ถูกปักหมุด (Pinning) ไปยังที่อยู่เว็บปลายทาง หรือ

1.3 ผู้ให้บริการเว็บ (Server) ได้ใช้ห่วงโซ่ใบรับรอง (Certificate Chain) ที่เชื่อมโยงไปยังใบรับรองที่ไม่น่าเชื่อถือ (Untrusted Root) ที่ถูกปักหมุด (Pinned) ไปยังที่อยู่เว็บปลายทาง

2. **การปกป้องด้วยความมั่นคงชั้นขนส่งอย่างอ่อนแอ** (weakly TLS-protected**, WeaklyTLSprotected**) เมื่อมีการปกป้องด้วยความมั่นคงชั้นขนส่ง (TLS-protected) แต่ไม่สามารถทำตามเงื่อนไขการปกป้องด้วยความมั่นคงชั้นขนส่งอย่างแข็งแกร่ง (strongly TLS-protected) ได้เนื่องจากสาเหตุหนึ่งในต่อไปนี้

ตารางที่ ก.2 แบบรูประดับการรักษาความมั่นคงชั้นขนส่ง (ต่อ)

Name	ระดับการรักษาความมั่นคงชั้นขนส่ง	ID	WSCP52

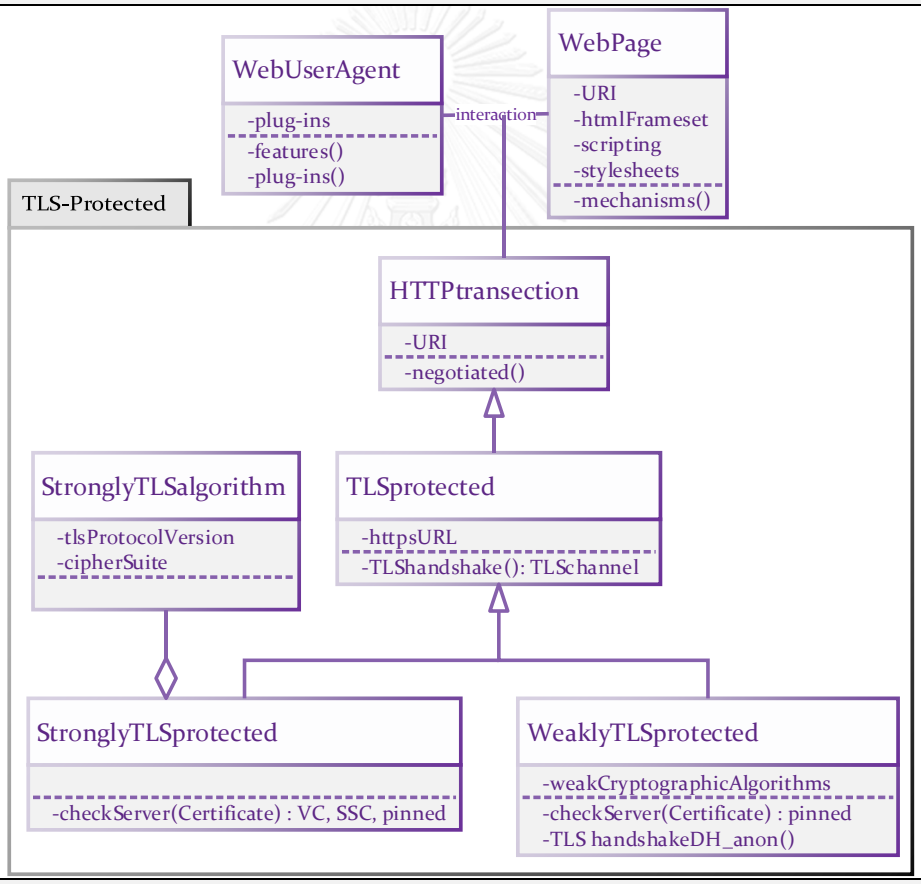
Solution

2.1 การติดต่อการรักษาความมั่นคงชั้นขนส่ง (TLS handshake) ด้วยขั้นตอนวิธีการแลกเปลี่ยนกุญแจนิรนาม (Anonymous Key Exchange Algorithm) เช่น DH_anon

2.2 การต่อรองโดยขั้นตอนวิธีเข้ารหัสลับ (Cryptographic Algorithms Negotiated) ไม่ได้รับการพิจารณาว่าเป็นวิธีที่แข็งแกร่ง

2.3 ประเภทใบรับรองที่ใช้ไม่เป็นทั้งใบรับรองที่ผ่านการตรวจสอบความสมเหตุสมผล (Validated Certificate) หรือ ใบรับรองโดยตนเอง (Self-Signed Certificate) แต่ปักหมุดไปยังที่อยู่เว็บปลายทาง (Pinned)

Internal Structure



Example Resolved

เบ็ตตี้พยายามเชื่อมต่อเว็บไซต์ที่ <https://www.example.com/> การพัฒนาความมั่นคงชั้นขนส่งในตัวแทนผู้ใช้ของเธอตรวจพบว่าชื่อโดเมนที่ระบุไว้ในใบรับรองต่างจาก www.example.com ตัวแทนผู้ใช้ต้องแจ้งให้เธอทราบข้อมูลดังกล่าว โดยระบุให้การเชื่อมต่อผู้ให้บริการเว็บถูกพิจารณาว่ามีการป้องกันความมั่นคงชั้นคงส่ง (TLS protect) แม้ไม่ได้รักษาความมั่นคงอย่างแข็งแกร่งหรืออ่อนแอเพื่อให้ผู้ใช้พิจารณาว่าเว็บดังกล่าวผู้ผู้โจมตีเปลี่ยนแปลงข้อมูลหรือไม่

ตารางที่ ก.2 แบบรูประดับการรักษาความมั่นคงชั้นขนส่ง (ต่อ)

Name	ระดับการรักษาความมั่นคงชั้นขนส่ง	ID	WSCP52
Consequences			
การกำหนดระดับความมั่นคงของการเชื่อมต่อการรักษาความมั่นคงชั้นขนส่ง (Type of TLS) จะช่วยจัดการความเสี่ยงและก่อให้เกิดความทนทานต่อการโจมตีระบบได้ แม้การเชื่อมต่อนั้นไม่สามารถรักษาความมั่นคงอย่างแข็งแกร่ง (Strong TLS protection) ได้แล้ว แต่การมีปฏิสัมพันธ์แบบอย่างอ่อนแอ (Weakly TLS-protected) สามารถรักษาคุณสมบัติด้านความมั่นคง (Security Services) เช่น การป้องกันรักษาความลับ (Confidentiality) หรือการป้องกันบูรณภาพของระบบ (Integrity) ต่อการโจมตีที่ไม่ทำให้เกิดการเปลี่ยนสถานะ (Passive attackers) ได้เช่นกัน			
See Also			
- ศึกษาการรักษาความมั่นคงชั้นขนส่งได้จากเอกสาร HTTP Over TLS [RFC 2818] แต่งโดย E. Rescorla เข้าถึงได้ที่ http://www.ietf.org/rfc/rfc2818.txt - การรักษาความมั่นคงชั้นขนส่งที่ได้ถูกพัฒนาต่อยอดศึกษาได้จากเอกสาร Upgrading to TLS Within HTTP/1.1 - RFC2817 - การนำออกชุดรหัส (Export Cipher Suites) ตามภาคผนวก A.5 ของ TLS v11 - ใบรับรองที่กล่าวถึงในแบบรูปนี้ เป็นไปตามเงื่อนไขที่ระบุในแบบรูป WSCP51 - ตัวอย่างปัญหาของแบบรูปนี้อ้างถึง Case 11 จากเอกสาร WSC-USECASES			

ตารางที่ ก.3 แบบรูปประเภทของเว็บจากการรักษาความมั่นคงชั้นขนส่ง

Name	ประเภทของเว็บจากการรักษาความมั่นคงชั้นขนส่ง	**ID**	WSCP53
Core	Authorization	**Section**	Applying TLS to the Web

Description

แบบรูปนี้กำหนดประเภทของเว็บที่ตัวแทนผู้ใช้ติดต่อผ่านช่องทางที่รักษาความมั่นคงชั้นขนส่ง (TLS channel) จากประเภทของความมั่นคงชั้นขนส่ง (Type of TLS) ที่กล่าวไว้ในแบบรูปที่ 52 (WSCP52) ประเภทของเว็บแบ่งตามระดับความมั่นคงของเนื้อหาที่มีเรียกผ่านช่องทางช่องทางที่รักษาความมั่นคงชั้นขนส่งระดับต่างๆ เนื่องจากเว็บประกอบด้วยทรัพยากรเพียงแหล่งเดียวแล้วเนื้อหาทั้งหมดที่ขึ้นอยู่กับแหล่งที่มานั้นจะมีคุณสมบัติด้านความมั่นคงสืบทอดจากการเชื่อมต่อผู้ให้บริการเว็บที่ใช้ในการเข้าถึงข้อมูล

Example

กรณี 10 เบ็ตตี้เยี่ยมชมหน้าเว็บที่ <https://www.example.com/> หน้าเว็บ HTML ที่ได้รับปรากฏเนื้อหาที่ได้รับจาก <http://www.example.com/> รวมอยู่ด้วย กล่าวคือเนื้อหาที่ได้รับมีบริบทความมั่นคงที่ต่างกัน

Context

เมื่อตัวแทนผู้ใช้ติดต่อกับเว็บผ่านช่องทางที่รักษาความมั่นคงชั้นขนส่ง (TLS channel) ได้สำเร็จแล้ว คุณสมบัติด้านความมั่นคงของเนื้อหาเว็บทั้งหมดสืบทอดจากระดับความมั่นคงของช่องทางที่ใช้ในการเข้าถึงข้อมูล

Problem

หากเว็บสืบทอดคุณสมบัติด้านความมั่นคงจากการเชื่อมต่อผู้ให้บริการเว็บที่เข้าถึงข้อมูลทรัพยากรที่ไม่มั่นคงโดยปราศจากการพิจารณาให้ผู้ใช้ทราบถึงสถานะของหน้าเว็บดังกล่าวว่าไม่มั่นคง ผู้ใช้อาจให้ข้อมูลส่วนตัวไปยังเว็บที่ไม่มั่นคงได้

Solution

ตัวแทนผู้ใช้ที่ติดต่อกับเว็บผ่านช่องทางที่รักษาความมั่นคงชั้นขนส่งสามารถจำแนกได้ว่าหน้าเว็บเหล่านั้นมีความมั่นคงหรือไม่ โดยพิจารณาได้จากที่มาของทรัพยากรเว็บดังนี้

1. **หน้าเว็บแบบรักษาความมั่นคงชั้นขนส่ง** (TLS-secured, **TLSsecured**) เมื่อทรัพยากรเว็บระดับบนสุด (top-level resource) และทรัพยากรเว็บอื่นๆ ทั้งหมดที่มีผลกระทบหรือควบคุมเนื้อหาและการนำเสนอของหน้าเว็บ ได้ถูกค้นคืนผ่านการเชื่อมต่อผู้ให้บริการเว็บที่ปกป้องด้วยความมั่นคงชั้นขนส่งอย่างแข็งแกร่ง (Strongly TLS protected, **StronglyTLSprotected**) กล่าวคือ ทรัพยากรเนื้อหา (Content, **Content**) ทั้งหมดอันได้แก่ รูปภาพ การแสดงผล และเฟรมเนื้อหาของหน้าเว็บที่มั่นคงนั้นจะต้องถูกค้นคืนจาก การเชื่อมต่อผู้ให้บริการเว็บที่ปกป้องด้วยความมั่นคงชั้นขนส่งอย่างแข็งแกร่งเพื่อให้หน้าเว็บโดยรวมถูกพิจารณาว่าเป็นหน้าเว็บแบบรักษาความมั่นคงชั้นขนส่ง (TLS-secured)
2. **หน้าเว็บแบบเนื้อหาผสม (**Mixed content, **MixedContent)** เมื่อทรัพยากรเว็บระดับบนสุด (Top-level resource) ได้ถูกค้นคืนผ่านการเชื่อมต่อผู้ให้บริการเว็บที่ปกป้องด้วยความมั่นคงชั้นขนส่งอย่างแข็งแกร่ง (Strongly TLS protected) แต่มีทรัพยากรเว็บแบบพึ่งพิง (Dependent resources) บางรายการถูกค้นคืนผ่านการเชื่อมต่อผู้ให้บริการเว็บที่ปกป้องด้วยความมั่นคงชั้นขนส่งอย่างอ่อนแอ (Weakly protected, **WeaklyTLSprotected**) หรือไร้การปกป้อง (Unprotected HTTP transaction, **UnprotectedHTTP**)

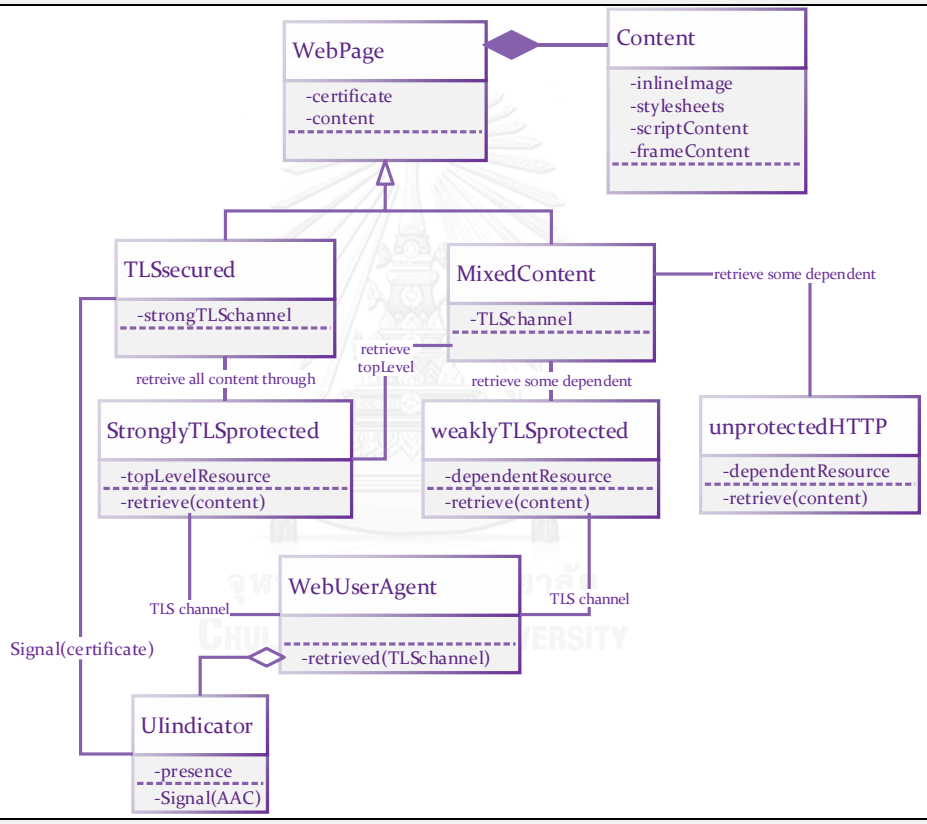
ตารางที่ ก.3 แบบรูปประเภทของเว็บจากการรักษาความมั่นคงชั้นขนส่ง (ต่อ)

Name	ประเภทของเว็บจากการรักษาความมั่นคงชั้นขนส่ง	ID	WSCP53

Solution

การประยุกต์ใช้ข้อมูลดังกล่าวด้วยตัวชี้บอกส่วนต่อประสานผู้ใช้ (UI indicator, **UIindicator**) จะต้องไม่แสดงสัญญาณของใบรับรองใดๆ จนกว่าหน้าเว็บนั้นได้ถูกพิจารณาว่าเป็นหน้าเว็บแบบรักษาความมั่นคงชั้นขนส่ง (TLS-secured) ผ่านการปกป้องด้วยความมั่นคงชั้นขนส่งอย่างแข็งแกร่ง (strongly TLS-protected) โดยแสดงสัญญาณข้อมูลของใบรับรองที่ได้รับประกันเสริม (AAC) ตัวอย่างเช่น ทุกๆส่วนของหน้าเว็บถูกโหลดจากผู้ให้บริการที่ถือใบรับรองที่ไม่ต่ำกว่าใบรับรองที่ผ่านการตรวจสอบความสมเหตุสมผล (VC)

Internal Structure



Example Resolved

กรณี 10 เบ็ตตี้เยี่ยมชมหน้าเว็บที่ <https://www.example.com/> หน้าเว็บดังกล่าวมีการรักษาความมั่นคงชั้นขนส่ง ในขณะที่หน้าเว็บ HTML ที่ได้รับปรากฏเนื้อหาที่ได้รับจาก <http://www.example.com/> ไม่มีการรักษาความมั่นคงชั้นขนส่ง กล่าวคือ เนื้อหาที่ได้รับมีบริบทความมั่นคงที่ต่างกัน ตัวแทนผู้ใช้จะต้องจำแนกหน้าเว็บดังกล่าวได้ว่าเป็นหน้าเว็บแบบเนื้อหาผสมและตัวชี้บอกส่วนต่อประสานผู้ใช้จะต้องไม่แสดงข้อมูลจากใบรับรองของเว็บดังกล่าว

Consequences

เมื่อหน้าเว็บถูกจำแนกไปตามคุณลักษณะความมั่นคง จะช่วยให้ผู้ใช้ตัดสินและพิจารณาได้ว่าควรเชื่อถือหน้าเว็บดังกล่าวหรือไม่

ตารางที่ ก.3 แบบรูปประเภทของเว็บจากการรักษาความมั่นคงชั้นขนส่ง (ต่อ)

Name	ประเภทของเว็บจากการรักษาความมั่นคงชั้นขนส่ง	**ID**	WSCP53
See Also			
- ใบรับรองที่ได้รับประกันเสริม (Augmented Assurance Certificates, AAC) ศึกษาได้จากแบบรูป 51 - ประเภทของความมั่นคงชั้นขนส่ง (Type of TLS) ศึกษาได้จากแบบรูป 52 - สำหรับข้อคำนึงถึงความมั่นคงที่เกี่ยวข้อศึกษาเพิ่มเติมได้ที่แบบรูป 86 - ตัวอย่างปัญหาของแบบรูปนี้อ้างถึง Case 10 จากเอกสาร WSC-USECASES			

ตารางที่ ก.4 แบบรูปการจัดการสถานการณ์ข้อผิดพลาดเบื้องต้น

Name	การจัดการสถานการณ์ข้อผิดพลาดเบื้องต้น	**ID**	WSCP54
Core	Integrity	**Section**	Applying TLS to the Web
Description			
แบบรูปนี้กล่าวถึงสถานการณ์ข้อผิดพลาดที่เกี่ยวกับการรักษาความมั่นคงชั้นขนส่ง (TLS) เพื่อให้เข้าใจถึงเหตุการณ์และปัญหาที่เกิดขึ้นระหว่างการรักษาความมั่นคงชั้นขนส่งพร้อมทั้งการจัดการกับแต่ละข้อผิดพลาดที่เกิดขึ้นโดยการส่งสัญญาณ ดังที่ได้กำหนดไว้ในแบบรูป 64 การจัดการและการส่งสัญญาณเกี่ยวข้องกับข้อผิดพลาดจะต้องถูกนำมาใช้			
Example			
กรณี 21 เบ็ตตี้พยายามเชื่อมต่อไปยังเว็บไซต์ <http://www.example.com/> ที่เธอเข้าเยี่ยมชมเป็นประจำเพื่ออ่านข่าวสารและบทความ เมื่อครั้งสุดท้ายที่เธอเยี่ยมชมเว็บไซต์ example.com ได้ถูกดัดแปลงไปจากเดิมและผู้เข้าเยี่ยมชมรายอื่นได้พบว่าได้ถูกติดตั้งโปรแกรมที่น่าสงสัยจากการเข้าถึงเว็บไซต์ดังกล่าว ในขณะที่ส่งการเรียกขอบริการในครั้งนี้ ตัวแทนผู้ใช้เว็บของเบ็ตตี้มีข้อมูลที่กล่าวได้ example.com เป็นเว็บที่ต้องสงสัยและมีความเสี่ยง ตัวแทนผู้ใช้เว็บจะแจ้งให้เบ็ตตี้ทราบได้อย่างไร			
Context			
แบบรูปนี้ครอบคลุม 3 บริบทที่อาจเกิดความผิดพลาด คือข้อผิดพลาดระหว่างการเชื่อมต่อการรักษาความมั่นคงของชั้นขนส่งข้อผิดพลาดจากการประเมินโดยองค์กรที่เกี่ยวข้องและข้อผิดพลาดขณะการส่งข้อมูลผ่านแบบฟอร์มไปยังเว็บไซต์ที่ไม่มั่นคง			
Problem			
การติดต่อระหว่างตัวแทนผู้ใช้และผู้ให้บริการอาจเกิดปัญหาหรือข้อผิดพลาด บางครั้งเป็นข้อผิดพลาดเล็กน้อย บางครั้งเป็นข้อผิดพลาดที่รุนแรง หากปราศจากความเข้าใจลักษณะปัญหาและการจัดการที่เหมาะสม อาจทำให้ผู้ใช้ไม่สามารถจัดการกับข้อผิดพลาดที่เกิดขึ้นได้และเกิดความเสียหายต่อข้อมูลหรือระบบของผู้ใช้เอง เช่น เมื่อตัวแทนผู้ใช้เว็บอนุญาตให้ใบรับรองที่ไม่น่าเชื่อถือได้ถูกจัดเก็บในฐานข้อมูลโดยปราศจากการพิจารณาโดยผู้ใช้แล้วจะเป็นการเปิดช่องให้ผู้โจมตี (man-in-the-middle) เปลี่ยนแปลงการตั้งค่าใบรับรองได้			

ตารางที่ ก.4 แบบรูปการจัดการสถานการณ์ข้อผิดพลาดเบื้องต้น (ต่อ)

Name	การจัดการสถานการณ์ข้อผิดพลาดเบื้องต้น	**ID**	WSCP54
Solution			

การทำความเข้าใจข้อผิดพลาดที่อาจเกิดขึ้นในบริบทต่างๆ จะช่วยให้ผู้พัฒนารับมือกับปัญหาที่เกิดขึ้นได้อย่างเหมาะสม โดยตัวแทนผู้ใช้เว็บอาจเลือกที่จะยกเลิกการเชื่อมต่อกับเว็บโดยปราศจากการถามผู้ใช้ก็เป็นได้แต่แนวทางปฏิบัติภายในแบบรูปนี้จะถูกนำไปประยุกต์ใช้เมื่อตัวแทนผู้ใช้เว็บเลือกที่จะให้ผู้ใช้พิจารณาและจัดการกับข้อผิดพลาดนั้นด้วยตนเอง ในกรณีที่การรักษาความมั่นคงชั้นขนส่งเกิดข้อผิดพลาดการส่งสัญญาณระดับภัยต่างๆ ตามที่ระบุไว้ในแบบรูป 64 จะต้องถูกนำมาใช้ตามสถานการณ์ข้อผิดพลาดซึ่งแบ่งได้ตามบริบทของเงื่อนไขข้อผิดพลาด 3 กลุ่ม ดังนี้

1. ความผิดพลาดที่เกิดขึ้นจากการรักษาความมั่งคงระดับโพรโตคอล (TLS Errors) ตัวแทนผู้ใช้เว็บอาจเลือกที่จะยกเลิกการเชื่อมต่อกับเว็บโดยปราศจากการถามผู้ใช้ เมื่อเกิดข้อผิดพลาดจากการเชื่อมต่อการรักษาความมั่นคงระชั้นขนส่ง ตัวแทนผู้ใช้รับมือกับข้อผิดพลาดที่เกิดขั้นตาม 5 เงื่อนไข ได้ดังนี้

เงื่อนไขข้อผิดพลาดที่ 1 ระหว่างการเชื่อมต่อความมั่นคงชั้นขนส่ง (TLS negotiation) ผู้ให้บริการเว็บแสดงห่วงโซ่ใบรับรอง (Certificate Chain) ที่ไม่ได้เชื่อมโยงไปยังใบรับรองลำดับบนสุดที่เชื่อถือได้ (Trusted Root) และห่วงโซ่ใบรับรองที่แสดงนั้นยังไม่ได้ถูกปักหมุดไปยังปลายทาง (Pinning) ตัวแทนผู้ใช้เว็บควรปฏิบัติต่อไปนี้

1) ตัวแทนผู้ใช้เว็บจะต้องส่งสัญญาณข้อผิดพลาดโดยกลุ่มการแจ้งเตือน (Warning/Caution Messages) หรือการเตือนภัย (Danger Messages) เพื่อแสดงรายละเอียดสถานการณ์ข้อผิดพลาดที่เกิดขึ้น

2) ตัวแทนผู้ใช้เว็บอาจต้องเสนอทางเลือกที่เป็นไปได้ให้ผู้ใช้พิจาณาในการปักหมุดใบรับรองไปยังเว็บปลายทาง (Pinning)

เงื่อนไขข้อผิดพลาดที่2 สารสนเทศของใบรับรอง (Certificate Information) ที่อยู่ในลักษณะข้อมูลภาษาธรรมชาติ (Human-readable) จะต้องไม่ปรากฏในลักษณะที่น่าเชื่อถือจนกว่าจะได้รับการยืนยัน เช่น ข้อมูลชื่อสามัญ (Common Name) หรือลักษณะองค์กร (Organization attribute) จากใบรับรองที่ลงนามด้วยตนเอง (SSC) จะต้องไม่ถูกนำมาแสดงผล ถึงแม้ใบรับรองนั้นจะถูกปักหมุดไว้ยังปลายทางแล้วก็ตาม

เงื่อนไขข้อผิดพลาดที่ 3 ขณะเชื่อมต่อการรักษาความมั่นคงชั้นขนส่ง (TLS negotiation) ผู้ให้บริการเว็บได้แสดงใบรับรองของตน แล้วพบว่าใบรับรองหรือหนึ่งในใบรับรองตัวกลาง (Intermediate Certificates) ที่อยู่ในห่วงโซ่ใบรับรอง (Certificate Chain) ได้ถูกเพิกถอนหรือหมดอายุแล้ว ตัวแทนผู้ใช้เว็บต้องแสดงสัญญาณข้อผิดพลาดโดยกลุ่มเตือนภัย (Danger Messages)

เงื่อนไขข้อผิดพลาดที่ 4 เมื่อตำแหน่งที่อยู่หรือยูอาร์ไอ (URI) ของเว็บที่กำลังทำรายการนั้นไม่ตรงกันกับชื่อโดเมนที่ปรากฏในใบรับรองที่แสดงโดยผู้ให้บริการเว็บ และใบรับรองดังกล่าวเป็นใบรับรองที่ผ่านการตรวจสอบความสมเหตุสมผล (Validated Certificate) ตัวแทนผู้ใช้เว็บจะต้องการส่งสัญญาณข้อผิดพลาดโดยกลุ่มเตือนภัย (Danger Messages)

เงื่อนไขข้อผิดพลาดที่ 5 หากการเชื่อมต่อการรักษาความมั่นคงชั้นขนส่งล้มเหลว ตัวแทนผู้ใช้เว็บต้องส่งสัญญาณข้อผิดพลาดระดับเตือนภัย (Danger Messages)

ตารางที่ ก.4 แบบรูปการจัดการสถานการณ์ข้อผิดพลาดเบื้องต้น (ต่อ)

Name	การจัดการสถานการณ์ข้อผิดพลาดเบื้องต้น	ID	WSCP54

2. เงื่อนไขข้อผิดพลาดพื้นฐานจากองค์กรที่เกี่ยวข้องหรือข้อมูลศึกษาสำนึก (Error Conditions based on Third Party or Heuristic Information)

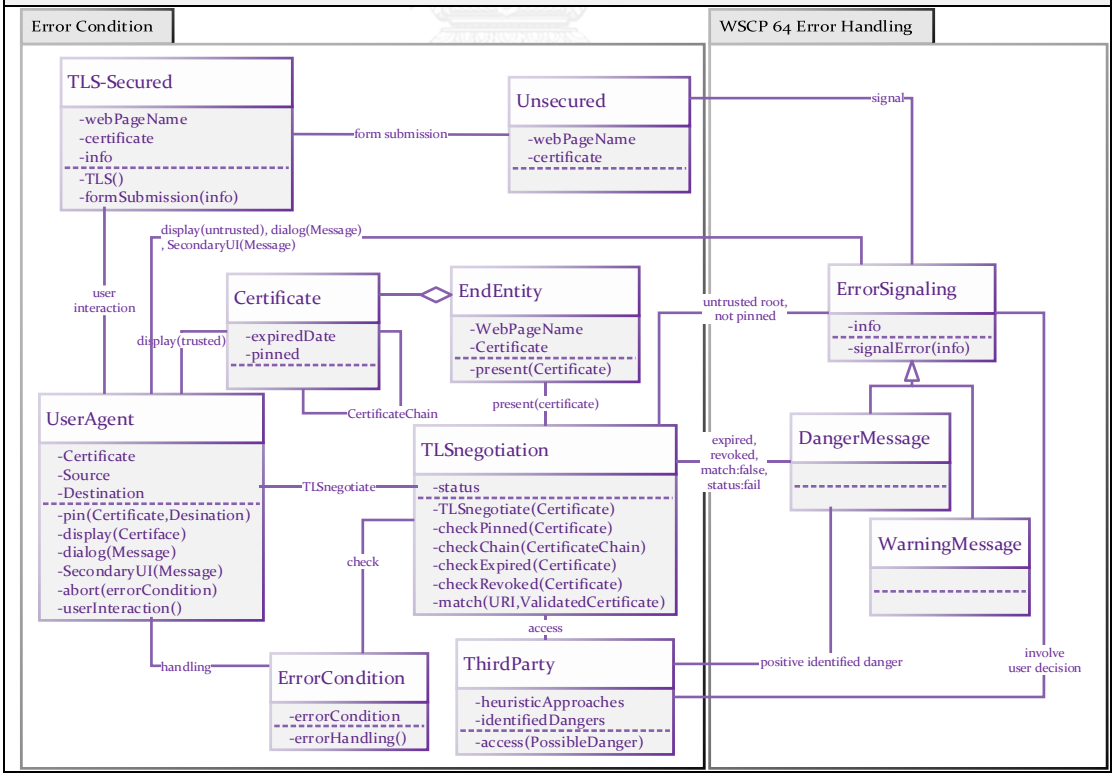
เงื่อนไขข้อผิดพลาดที่ 6 ตัวแทนผู้ใช้เว็บที่ใช้บริการองค์กรภายนอก (Third Party) หรือวิธีการศึกษาสำนึก (Heuristic Approach) ในการประเมินความเป็นไปได้ของภัยที่จะเกิดขึ้นจากเว็บที่กำลังเชื่อมต่อ ตัวแทนผู้ใช้เว็บต้องส่งสัญญาณโดยใช้กลุ่มข้อความเตือนภัย (Danger Message) ที่แสดงรายละเอียดประสบภัยที่ได้กำหนดไว้

เงื่อนไขข้อผิดพลาดที่ 7 หากภัยที่จะเกิดขึ้นจากเว็บที่กำลังเข้าถึงนั้นเกี่ยวข้องกับการตัดสินใจของผู้ใช้ที่จะต้องทำในลำดับต่อไป ตัวแทนผู้ใช้เว็บจะต้องส่งสัญญาณข้อผิดพลาดผ่านการแจ้งเตือน (Warning/Caution Messages) หรือการเตือนภัย(Danger Messages)

3. ข้อผิดพลาดจากการส่งข้อมูลผ่านแบบฟอร์มไปยังเว็บที่ไม่มั่นคง (Insecure form submission) หน้าเว็บที่รักษาความมั่นคงชั้นขนส่ง (TLS-secured) มีเข้ารหัสเพื่อการป้องการการโจมตี ทำให้ข้อมูลที่ส่งผ่านระหว่างการงานเว็บเหล่านั้นจะถูกปกป้องอย่างแข็งแกร่งด้วยการรักษาความมั่นคงชั้นขนส่ง

เงื่อนไขข้อผิดพลาดที่ 8 เมื่อแบบฟอร์มจากหน้าเว็บที่มั่นคง (TLS-secured) ถูกส่งไปยังช่องทางที่ไม่มั่นคง (Unsecured channel) ตัวแทนผู้ใช้เว็บอาจใช้การแจ้งเตือน (Warning/Caution Messages) หรือการเตือนภัย (Danger Messages) เพื่อแสดงรายละเอียดให้แก่ผู้ใช้

Internal Structure



ตารางที่ ก.4 แบบรูปการจัดการสถานการณ์ข้อผิดพลาดเบื้องต้น (ต่อ)

Name	การจัดการสถานการณ์ข้อผิดพลาดเบื้องต้น	**ID**	WSCP54
Example Resolved			
จากกรณี 21 เบ็ตตี้พยายามเชื่อมต่อไปยังเว็บไซต์ <http://www.example.com/> ที่เธอเข้าเยี่ยมชมเป็นประจำเพื่ออ่านข่าวสารและบทความ เมื่อครั้งสุดท้ายที่เธอเยี่ยมชมเว็บไซต์ example.com ได้ถูกดัดแปลงไปจากเดิมและผู้เข้าเยี่ยมชมรายอื่นได้พบว่าติดตั้งโปรแกรมที่น่าสงสัยจากการเข้าถึงเว็บไซต์ดังกล่าว ในขณะที่ส่งการเรียกขอบริการในครั้งนี้ ตัวแทนผู้ใช้เว็บของเบ็ตตี้ต้องส่งสัญญาณโดยใช้กลุ่มข้อความเตือนภัย (Danger Message) ที่แสดงรายละเอียดประสบภัยจากการติดตั้งโปรแกรมที่น่าสงสัย ที่ได้กำหนดไว้ตามเงื่อนไขข้อผิดพลาดที่ 6			
Known Uses			
- ใบรับรอง SSC จะต้องไม่ถูกนำมาแสดงผลข้อมูลชื่อสามัญหรือลักษณะองค์กร ถึงแม้ใบรับรองนั้นจะถูกปักหมุดไว้ยังปลายทางแล้วก็ตาม - ตัวแทนผู้ใช้อาจแสดงผลข้อมูลข้อผิดพลาดที่เกิดขึ้นผ่านกล่องข้อความ (dialog) หรือส่วนต่อประสานทุติยภูมิ (Secondary UI) ที่เข้าถึงได้โดยการแจ้งเตือนหรือข้อความแสดงข้อผิดพลาดตามที่ระบุไว้ - ตัวอย่างประสบภัยที่ได้กำหนดไว้เช่น การดาวน์โหลดสิ่งไม่พึงประสงค์ที่ได้กำหนดไว้หรือการโจมตีช่องโหว่ของตัวแทนผู้ใช้ - ตัวอย่างการพบภัยที่เกี่ยวข้องกับการตัดสินใจของผู้ใช้ เช่น เว็บถูกปลอมแปลง (Phishing)			
Consequences			
การเข้าใจเงื่อนไขข้อผิดพลาดและแนวทางการจัดการเมื่อเกิดข้อผิดพลาดดังกล่าว จะช่วยให้ผู้พัฒนาป้องกันข้อผิดพลาดและรายงานข้อผิดพลาดนั้นไปยังผู้ใช้ได้อย่างเหมาะสมกับความรุนแรงของข้อผิดพลาดใดๆ ที่เกิดขึ้นในขณะเชื่อมต่อกับผู้ให้บริการ			
See Also			
- ศึกษาการจัดการกับใบรับรองได้จากแบบรูป 51 - ศึกษาประเภทของเว็บได้จากแบบรูป 53 - ศึกษาการจัดการข้อผิดพลาด (Error Handling) จากแบบรูป 64 - ดูเพิ่มแบบรูป 81 การโจมตีในระหว่างการเชื่อมต่อการรักษาความมั่นคงชั้นขนส่ง สำหรับข้อมูลเพิ่มเติมในกรณีดังกล่าว - ตัวอย่างปัญหาของแบบรูปนี้อ้างถึง Case 21 จากเอกสาร WSC-USECASES			

ตารางที่ ก.5 แบบรูปการส่งสัญญาณอัตลักษณ์

Name	การส่งสัญญาณอัตลักษณ์	**ID**	WSCP61
Core	Availability	**Section**	Indicators and Interactions
Description			
แบบรูปนี้ กล่าวถึงแนวปฏิบัติสำหรับตัวแทนผู้ใช้เว็บในการส่งสัญญาณแสดงรายละเอียดข้อมูลอัตลักษณ์จากใบรับรองของผู้ให้บริการเว็บที่ผู้ใช้กำลังเข้าถึงผ่านส่วนต่อประสานผู้ใช้ สัญญาณที่กำหนดนี้มีลักษณะไร้การตอบโต้ (Passive) อย่างไรก็ตามข้อกำหนดนี้ยังไม่คำนึงถึงการป้องกันการเลียนแบบจากการโจมตีระบบได้			
Example			
กรณี 10: เบ็ตตี้เข้าเยี่ยมชมหน้าเว็บที่ <https://www.example.com/> หน้าเฮททีเอ็มเอลที่ได้รับมีเนื้อหาที่ได้รับจาก <http://www.example.com/> เช่น เนื้อหาที่ได้รับใช้บริบทความมั่นคงที่ต่างกัน **กรณี 11**: เบ็ตตี้พยายามเชื่อมต่อเว็บไซต์ที่ <https://www.example.com/> การพัฒนาความมั่นคงชั้นขนส่งในตัวแทนผู้ใช้ของเธอตรวจพบว่าชื่อโดเมนที่ระบุไว้ในใบรับรองต่างจาก www.example.com **กรณี 14**: เบ็ตตี้ท่องเที่ยวไปยังต่างประเทศ ในร้านกาแฟแห่งหนึ่ง เธออ่านเว็บไซต์การเมืองประจำประเทศของเธอ เธอเกิดข้อสงสัยว่าข้อมูลที่เธอกำลังได้รับนั้นเป็นเว็บจริงหรือไม่ หรือมีการรั่วไหลของข้อมูลระหว่างการใช้งานเว็บหรือไม่			
Context			
บริบทของการประยุกต์ใช้แบบรูปเมื่อมีการเชื่อมต่อข้อมูลกับผู้ให้บริการเว็บหรือระหว่างการเข้าถึงเนื้อหาเว็บในสถานะใดๆ แล้วตัวแทนผู้ใช้เว็บได้รับการยืนยันตัวจริงโดยการแสดงใบรับรองจากผู้ให้บริการเว็บ			
Problem			
ผู้ใช้เข้าถึงเนื้อหาเว็บโดยปราศจากการรับรู้ถึงที่มาของข้อมูลหรืออัตลักษณ์ของผู้ให้บริการเว็บใดๆ เป็นเหตุให้ผู้ใช้ตัดสินใจเชื่อถือข้อมูลดังกล่าวและเปิดโอกาสให้ผู้ประสงค์ร้ายโจมตีระบบอันก่อให้เกิดเกิดภัยต่อข้อมูลผู้ใช้งานได้			
Solution			
เพื่อให้ผู้ใช้ทราบถึงที่มาของเว็บที่กำลังเข้าถึง ตัวแทนผู้ใช้จะต้องทำให้ข้อมูลที่ใช้ในการยืนยันตัวของผู้ให้บริการเว็บปรากฏและพร้อมใช้งาน โดยการแสดงข้อมูลอัตลักษณ์ของเว็บให้แก่ผู้ใช้ได้ทราบนั้นต้องพิจารณาวิธีการนำเสนอข้อมูลรวมถึงข้อมูลใดบ้างที่จะต้องปรากฏ ซึ่งมีรายละเอียดดังนี้ 1. **คุณลักษณะของสัญญาณ (Signal Specification)** วิธีการนำเสนอข้อมูลอัตลักษณ์ของเว็บขึ้นอยู่กับสถานะของระบบ เช่น สถานะ “การใช้งาน” การปรากฏข้อมูลอัตลักษณ์ควรเป็นส่วนหนึ่งของส่วนต่อประสานผู้ใช้ปฐมภูมิ (Primary User Interface, **PrimaryUserInterface**) ซึ่งจะทำให้สัญญาณอัตลักษณ์นั้นปรากฏแก่ผู้ใช้แบบหลีกเลี่ยงไม่ได้ เนื่องจากส่วนต่อประสานดังกล่าวต้องปรากฏอยู่เสมอในขณะใช้งานระบบ มิเช่นนั้นข้อมูลอัตลักษณ์ดังกล่าวจะต้องพร้อมใช้งานจากการเรียกใช้ส่วนต่อประสานผู้ใช้ทุติยภูมิ (Secondary User Interface, **SecondaryUserInterface**) ซึ่งส่วนต่อประสานดังกล่าวมีลักษณะซ่อนอยู่ภายใต้แถบเครื่องมือ ผู้ใช้ต้องเรียกใช้งานผ่านส่วนต่อประสานปฐมภูมิเพื่อให้ส่วนต่อประสานทุติยภูมิปรากฏ การทำงานร่วมกันของส่วนต่อประสานทั้งสองแบบนั้นรวมเรียกว่าส่วนต่อประสานโครม (Chrome) ซึ่งบางสถานะของการใช้งานไม่อาจนำสัญญาณอัตลักษณ์ตามข้อกำหนดนี้ไปประยุกต์ใช้ได้ ตัวอย่างสถานะ เช่น ตัวแทนผู้ใช้เว็บมีการ			

ตารางที่ ก.5 แบบรูปการส่งสัญญาณอัตลักษณ์ (ต่อ)

Name	การส่งสัญญาณอัตลักษณ์	**ID**	WSCP61

เปลี่ยนแปลงจากสถานะใดๆ ไปยังสถานะนำเสนอสื่อผสม (Presentation Mode) ที่ไม่มีการแสดงส่วนต่อประสานโครม จึงที่ไม่สามารถปรากฏตัวชี้บอกความมั่นคงไว้ในส่วนต่อประสานผู้ใช้ปฐมภูมิ อีกทั้งตัวแทนผู้ใช้เว็บบนอุปกรณ์บางประเภทมีข้อจำกัดในการแสดงผลจึงไม่อาจนำสัญญาณอัตลักษณ์ตามข้อกำหนดนี้ไปประยุกต์ใช้ได้ ตัวอย่างอุปกรณ์ เช่น สมาร์ทโฟน จอบันเทิงส่วนตัวที่ติดตั้งหลังเก้าอี้โดยสารบนเครื่องบิน หรือชุดทีวี ตัวแทนผู้ใช้เว็บของอุปกรณ์ดังกล่าวออกแบบองค์ประกอบส่วนต่อประสารโครมให้ปรากฏน้อยที่สุดแต่ยังมองเห็น (Minimal) จึงไม่จำเป็นต้องแสดงตัวชี้บอกความมั่นคงในระหว่างสถานะเหล่านั้น

2. **การส่งสัญญาณอัตลักษณ์ (Identity Signal, IdentitySignal)** หากเมื่อใดก็ตามที่มีการแสดงส่วนต่อประสานของตัวแทนผู้ใช้เว็บ สัญญาณอัตลักษณ์จะต้องถูกแสดงในตำแหน่งการมองเห็นที่ต้องกันเสมอและเนื้อหาของเว็บจะต้องไม่แทรกแซงการทำงานใดๆ ที่ก่อให้เกิดความคลุมเครือของส่วนต่อประสานที่แสดงความมั่นคงนี้

3. **เนื้อหาของสัญญาณอัตลักษณ์ (Identity Signal Content)** ข้อมูลที่จะถูกแสดงในการส่งสัญญาณอัตลักษณ์จะต้องได้รับมาจากใบรับรองที่ผ่านการตรวจสอบความสมเหตุสมผล (VC, **ValidatedCertificate**) หรือจากการระบุโดยตัวแทนผู้ใช้เว็บ ซึ่งจะต้องไม่นำข้อมูลจากแหล่งที่ไม่น่าเชื่อถือหรือไม่ถูกยืนยันตัวจริงมาใช้ ดังนั้นข้อมูลอัตลักษณ์ขึ้นอยู่กับประเภทของเว็บที่ผู้ใช้กำลังเข้าถึง จากแบบรูปที่ 53 แบ่งได้ 2 ประเภท คือ หน้าเว็บแบบรักษาความมั่นคงชั้นขนส่ง (TLS-Secured) และหน้าเว็บแบบเนื้อหาผสม (Mixed Content) รายละเอียดข้อมูลที่นำมาใช้สำหรับเว็บประเภทดังกล่าว มีดังนี้

3.1 **หน้าเว็บแบบรักษาความมั่นคงชั้นขนส่ง (TLS-secured, TLS-secured)** ระหว่างการเชื่อมต่อกับเว็บที่มั่นคงนี้ทรัพยากรระดับบน (Top-level Resource) ถูกค้นคืนผ่านการปกป้องด้วยความมั่นคงชั้นขนส่งอย่างแข็งแกร่ง (strongly TLS-protected) ผู้ให้บริการเว็บแสดงใบรับรองที่ได้รับประกันเสริม (AAC, **AugmentedAssuranceCertificate**) และทรัพยากรที่พึ่งพิง (Dependence Resource) ทั้งหมดถูกค้นคืนผ่านช่องทางที่รักษาความมั่นคงชั้นขนส่งนั้นผู้ให้บริการเว็บได้แสดงใบรับรองที่ผ่านการตรวจสอบความสมเหตุสมผล (VC) เมื่อติดต่อกับหน้าเว็บลักษณะดังกล่าวตัวแทนผู้ใช้เว็บต้องปฏิบัติดังนี้

1) ข้อมูลที่เป็นภาษาธรรมชาติ (Human readable) ที่ได้จากใบรับรองที่ได้รับประกันเสริม (AAC) เกี่ยวกับผู้ครอบครองหน้าเว็บนั้น จะต้องถูกนำมาแสดงสัญญาณอัตลักษณ์

2) หากไม่ปรากฏข้อมูลภาษาธรรมชาติจากใบรับรองที่ได้รับประกันเสริมแล้ว ตัวแทนผู้ใช้เว็บจะต้องประยุกต์โดยนำชื่อโดเมน (DNS) ที่ตรงกับชื่อสามัญของหน้าเว็บ หรือส่วนขยาย “subjectAltName” จากใบรับรอง ซึ่งตัวแทนผู้ใช้อาจย่อชื่อโดเมนให้สั้นลงโดยแสดงเฉพาะส่วนท้าย (Suffix)

3) ข้อมูลองค์กรของผู้ออกใบรับรอง (Third Party) จะต้องถูกแสดงในสัญญาณอัตลักษณ์ หรือในส่วนต่อประสานผู้ใช้ทุติยภูมิ เพื่อแจ้งให้ผู้ใช้ทราบเกี่ยวกับผู้มีหน้าที่รับผิดชอบต่อข้อมูลเว็บนั้น

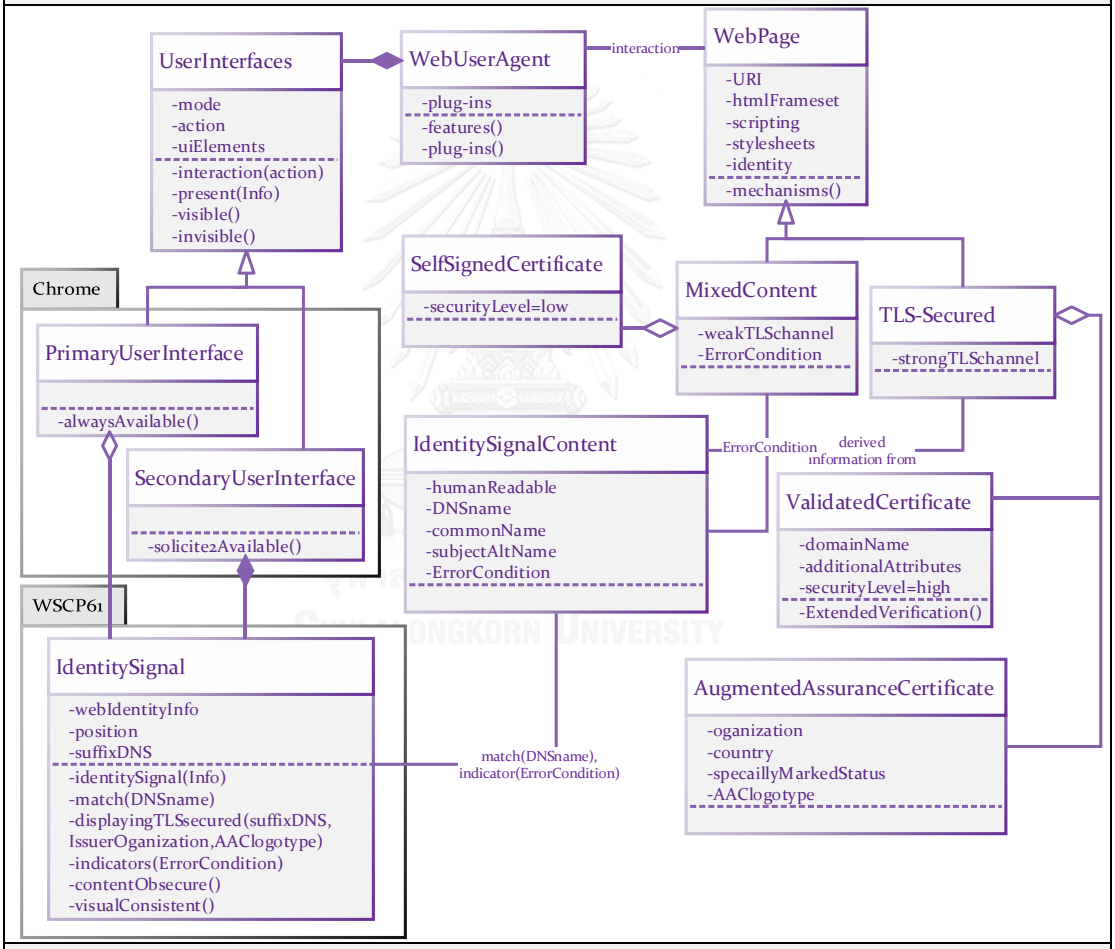
4) ข้อมูลโลโก้ (logotypes) ที่ถูกนำมาใช้ ต้องได้จากใบรับรองใบรับรองที่ได้รับประกันเสริม (AAC) เท่านั้น

ตารางที่ ก.5 แบบรูปการส่งสัญญาณอัตลักษณ์ (ต่อ)

Name	การส่งสัญญาณอัตลักษณ์	ID	WSCP61

3.2 **หน้าเว็บที่มีเนื้อหาแบบผสม (Mixed Content, MixedContent)** ข้อมูลของเว็บไซต์ที่เชื่อมต่อแบบไร้การป้องกัน (unprotected HTTP transactions) จะต้องไม่ถูกนำมาแสดงสัญญาณอัตลักษณ์และตัวแทนผู้ใช้เว็บจะต้องไม่ประมวลผลข้อมูลประเภทโลโก้ (Logotypes) ที่ได้รับจากใบรับรองของเว็บดังกล่าว ข้อมูลจากใบรับรองที่ลงนามโดยตนเอง (SSC, **SelfSignedCertificate**) หรือห่วงโซ่ใบรับรองที่เชื่อมโยงไปยังใบรับรองลำดับบนสุดที่ไม่น่าเชื่อถือ (Untrusted Root) ต้องไม่ถูกนำมาใช้ในสัญญาณอัตลักษณ์ ในสถานการณ์เช่นนี้ตัวแทนผู้ใช้เว็บอาจใช้ตัวชี้บอก (จากแบบรูป 63) เพื่อให้เห็นถึงเงื่อนไขข้อผิดพลาดที่เกิดขึ้น

Internal Structure



Example Resolved

กรณี 10: เมื่อเนื้อหาที่ได้รับใช้บริบทความมั่นคงที่ต่างกัน การส่งสัญญาณอัตลักษณ์ต้องแสดงเพียงเว็บที่มีการรักษาความมั่นคงชั้นขนส่ง <https://www.example.com/> เท่านั้น จะต้องแจ้งเตือนและไม่แสดงข้อมูลอัตลักษณ์ของหน้าเฮททีเอ็มเอลที่ได้รับจาก http://www.example.com/

กรณี 11: เมื่อตัวแทนผู้ใช้ตรวจพบว่าชื่อโดเมนที่ระบุไว้ในใบรับรองต่างจาก www.example.com จะต้องแจ้งเตือนและไม่แสดงข้อมูลอัตลักษณ์ของหน้า <https://www.example.com/>

ตารางที่ ก.5 แบบรูปการส่งสัญญาณอัตลักษณ์ (ต่อ)

Name	การส่งสัญญาณอัตลักษณ์	**ID**	WSCP61
Example Resolved			
กรณี 14: เมื่อผู้ใช้ต้องการทราบถึงข้อมูลที่กำลังได้รับนั้นเป็นเว็บจริงหรือไม่ หรือมีการรั่วไหลของข้อมูลระหว่างการใช้งานเว็บหรือไม่ ผู้ใช้สามารถเรียกดูข้อมูลอัตลักษณ์เพิ่มเติมได้จากส่วนต่อประสานแบบทุติยภูมิของตัวแทนผู้ใช้			
Consequences			
การแสดงข้อมูลอัตลักษณ์ของเว็บที่ผู้ใช้กำลังเชื่อมต่อจะช่วยให้ผู้ใช้พิจารณาและตัดสินใจได้ว่าเว็บดังกล่าวน่าเชื่อถือหรือไม่ จากการคัดกรองข้อมูลที่เกี่ยวข้องกับผู้ให้บริการโดยตัวแทนผู้ใช้เว็บจะช่วยลดภาระในการพิจารณาที่มาของเว็บให้แก่ผู้ใช้ได้			
See Also			
- ศึกษาการกำหนดประเภทของเว็บจากการปกป้องด้วยความมั่นคงชั้นขนส่งเพิ่มเติมได้จากแบบรูป 53 - เงื่อนไขข้อผิดพลาด ศึกษาได้จากแบบรูป 54 Error Condition - ตัวชี้บอกที่ใช้แสดงสถานะ ศึกษาได้จาก แบบรูป 63 Indicator - เนื้อหาของเว็บที่ทำให้ส่วนต่อประสานที่แสดงความมั่นคงมีความคลุมเครือ ศึกษาเพิ่มเติมจากแบบรูป 74 - ตัวอย่างปัญหาของแบบรูปนี้อ้างถึง Case 10-11, 14 จากเอกสาร WSC-USECASES			

ตารางที่ ก.6 แบบรูปข้อมูลเสริมบริบทความมั่นคงเชิงเว็บ

Name	ข้อมูลเสริมบริบทความมั่นคงเชิงเว็บ	**ID**	WSCP62
Core	Availability	**Section**	Indicators and Interactions
Description			
นอกเหนือจากข้อมูลอัตลักษณ์ที่ได้กำหนดไว้ในแบบรูป 61 แบบรูปนี้นำเสนอข้อมูลเพิ่มเติมด้านบริบทความมั่นคงเชิงเว็บที่ตัวแทนผู้ใช้เว็บควรนำมาประยุกต์ใช้เพื่อแสดงสถานะความมั่นคงของเว็บ			
Example			
กรณี 14 เบ็ตตี้ท่องเที่ยวไปยังต่างประเทศ ในร้านกาแฟแห่งหนึ่ง เธออ่านเว็บไซต์การเมืองประจำประเทศของเธอ เธอเกิดข้อสงสัยว่าข้อมูลที่เธอกำลังได้รับนั้นเป็นเว็บจริงหรือไม่ หรือมีการรั่วไหลของข้อมูลระหว่างการใช้งานเว็บหรือไม่			
Context			
บริบทของการนำแบบรูปนี้ไปประยุกต์ใช้เมื่อตัวแทนผู้ใช้เว็บยอมรับข้อมูลอัตลักษณ์จากผู้ให้บริการเว็บในการแสดงข้อมูลบริบทความมั่นคงผ่านส่วนต่อประสานผู้ใช้ทั้งแบบปฐมภูมิหรือทุติยภูมิ			
Problem			
หากผู้ใช้พิจารณาเพียงข้อมูลอัตลักษณ์ของผู้ให้บริการเว็บโดยปราศจากการพิจารณาข้อมูลทางบริบทความมั่นคงเพิ่ม อาจไม่เพียงพอต่อการแยกแยะระหว่างเว็บจริงและเว็บปลอมแปลง ผู้ใช้อาจตีความหมายหรือเข้าใจข้อมูลที่คลุมเครือผิดจนเข้าสู่เว็บไซต์ที่อาจเป็นภัยต่อข้อมูลและระบบของผู้ใช้ได้			

ตารางที่ ก.6 แบบรูปข้อมูลเสริมบริบทความมั่นคงเชิงเว็บ (ต่อ)

Name	ข้อมูลเสริมบริบทความมั่นคงเชิงเว็บ	**ID**	WSCP62
Solution			

นอกเหนือจากข้อมูลอัตลักษณ์ของเว็บ ข้อมูลที่เป็นประโยชน์เพื่อให้ผู้ใช้พิจารณาความมั่นคงของเว็บก่อนดำเนินการเข้าถึงเนื้อหาเว็บต่อไป ข้อมูลด้านบริบทความมั่นคงเชิงเว็บจะถูกนำมาใช้ในส่วนต่อประสานผู้ใช้ทั้งแบบปฐมภูมิและทุติยภูมิ ความหมายของการปรากฏข้อมูลดังกล่าวจะต้องมีความต้องกันหรือไม่ถูกนำไปใช้เพื่อจุดประสงค์อื่น แนวปฏิบัติที่ดีที่สุดที่จะช่วยหลีกเลี่ยงการแสดงผลที่ไม่ต้องกันคือ การไม่ใช้รูปแบบเดียวกันหรือไอคอน (Icon) ที่มีความหมายคล้ายกันสำหรับข้อมูลที่ต่างกันในตำแหน่งที่ต่างกัน ข้อมูลบริบทความมั่นคงเชิงเว็บแบ่งได้ 3 ระดับ ดังนี้

1. **ข้อมูลบริบทความมั่นคงเชิงเว็บเบื้องต้น** (Basic Security Context Information, **BasicSCI**) ตัวแทนผู้ใช้เว็บจะต้องทำให้ข้อมูลบริบทเชิงความมั่นคงต่อไปนี้พร้อมใช้งาน:

   1.1 ชื่อโดเมนของหน้าเว็บ

   1.2 ข้อมูลผู้ถือครองหรือข้อมูลผู้ตรวจสอบนั้นต้องสอดคล้องกันกับเนื้อหาของสัญญาณอัตลักษณ์ที่กำหนดในแบบรูปที่ 61

   1.3 เหตุผลในการพิจารณาเมื่อตัวแทนผู้ใช้ได้รับแจ้งว่าข้อมูลของผู้ให้บริการเชื่อถือได้หรือเชื่อถือไม่ได้ เช่น ควรหรือไม่ที่จะยอมรับใบรับรองเชิงตอบโต้ ควรหรือไม่ที่นำใบรับรอง SSC ปักหมุด และควรหรือไม่ที่การตั้งค่าเกี่ยวข้องกับความน่าเชื่อถือของตัวแทนผู้ใช้สามารถกระทำได้โดยผู้ใช้

2. **ข้อมูลบริบทความมั่นคงเชิงเว็บที่พึงมี** (Advance Security Context Information, **AdvanceSCI**) ตัวแทนผู้ใช้เว็บควรจะทำให้ข้อมูลบริบทเชิงความมั่นคงต่อไปนี้พร้อมใช้งาน:

   2.1 ตัวชี้บอกการรักษาความมั่นคงชั้นขนส่งถูกใช้ในการเข้าถึงคำอธิบายข้อมูลด้านบริบทความมั่นคงเชิงเว็บ

   2.2 เงื่อนไขใดที่ก่อให้เกิดการปกป้องด้วยความมั่นคงชั้นขนส่งอย่างอ่อนแอของหน้าเว็บจากแบบรูป 53

   2.3 ผู้ใช้เคยเยี่ยมชมเว็บไซต์ดังกล่าวในอดีตหรือไม่

   2.4 ผู้ใช้เคยจัดเก็บข้อมูลการยืนยันตัวสำหรับเว็บไซต์หรือไม่

   2.5 เนื้อหาเว็บไซต์ได้ถูกเข้ารหัสในระหว่างขนส่งข้อมูลหรือไม่

   2.6 เนื้อหาเว็บไซต์ดังกล่าวได้ถูกยืนยันตัวบุคคลแล้วหรือไม่

3. **ข้อมูลบริบทความมั่นคงเชิงเว็บเพิ่มเติม** (Additional Security Context Information,**AdditionalSCI**) แหล่งข้อมูลอาจทำให้สารสนเทศของบริบทความมั่นคงพร้อมใช้งาน มีดังนี้

   3.1 ผู้ใช้เข้าเยี่ยมชมเว็บไซต์เป็นครั้งแรกในอดีตเมื่อใด

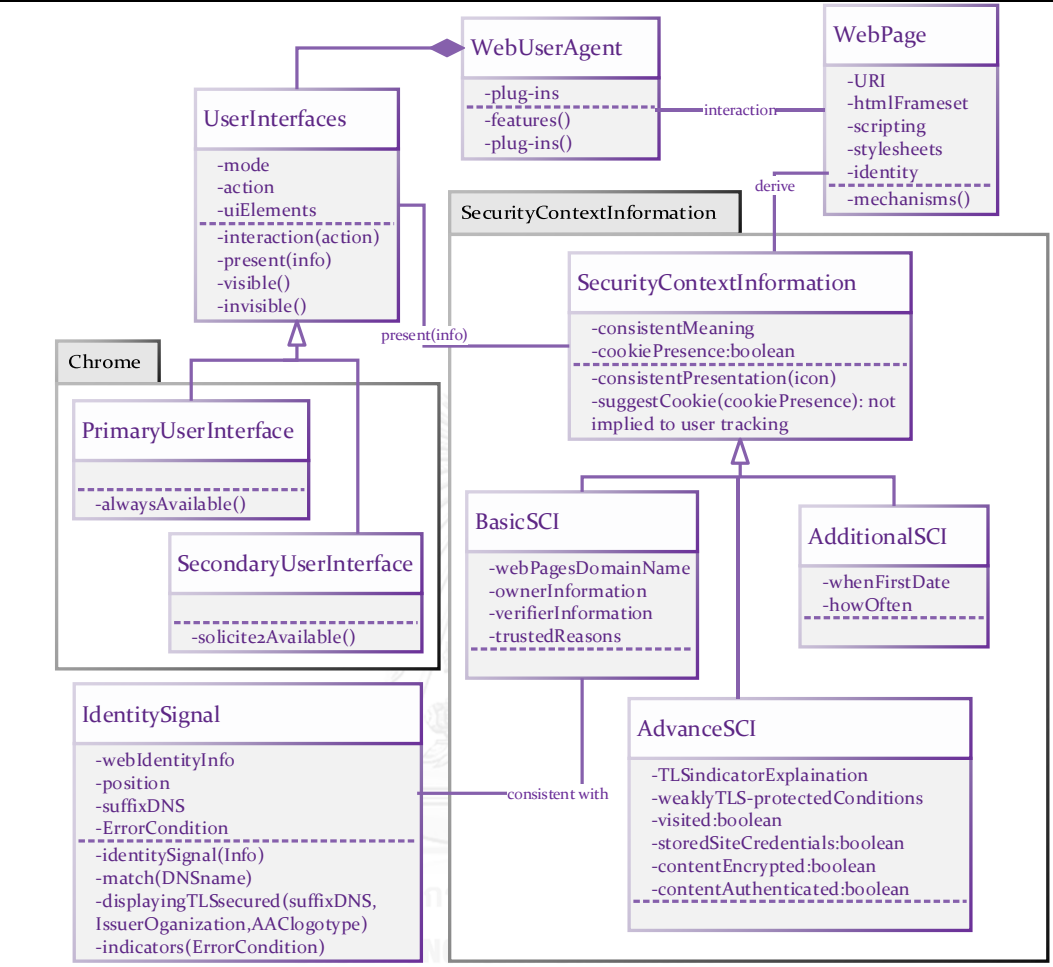
   3.2 ผู้ใช้เข้าเยี่ยมชมเว็บไซต์ดังกล่าวบ่อยหรือไม่

ตัวแทนผู้ใช้เว็บจะต้องไม่แนะนำผู้ใช้ว่าหน้าเว็บที่กำลังเข้าถึงปราศจากการติดตามพฤติกรรมไม่พบการปรากฏของข้อมูลคุกกี้ เนื่องจากยังมีเทคนิคการจัดการการใช้งานการติดตามการใช้งานและพฤติกรรมของผู้ใช้จำนวนมากที่ไม่อาศัยข้อมูลคุกกี้

ตารางที่ ก.6 แบบรูปข้อมูลเสริมบริบทความมั่นคงเชิงเว็บ (ต่อ)

Name	ข้อมูลเสริมบริบทความมั่นคงเชิงเว็บ	ID	WSCP62

Internal Structure



Example Resolved

กรณี 14: เมื่อผู้ใช้ต้องการทราบถึงข้อมูลที่กำลังได้รับนั้นเป็นเว็บจริงหรือไม่ หรือมีการรั่วไหลของข้อมูลระหว่างการใช้งานเว็บหรือไม่ ผู้ใช้สามารถเรียกดูข้อมูลบริบทความมั่นคงเพิ่มเติมนอกเหนือจากข้อมูลอัตลักษณ์ของเว็บในการพิจารณาการเชื่อถือเว็บ

Consequences

ข้อมูลเสริมจากแบบรูปนี้ จะช่วยให้ข้อมูลอันเป็นประโยชน์ต่อการตัดสินใจของผู้ใช้ที่กำลังทำการเชื่อมต่อกับผู้ให้บริการ ให้สามารถไว้ใจหรือเข้าถึงเว็บไซต์ดังกล่าวอย่างระมัดระวัง

See Also

- ศึกษาการนิยามประเภทของเว็บจาก แบบรูป 53
- ข้อมูลพื้นฐานในการแสดงความมั่นคงเชิงเว็บศึกษาได้จาก แบบรูป 61 เนื้อหาของสัญญาณอัตลักษณ์
- ตัวชี้บอกที่ใช้แสดงสถานะ ศึกษาได้จาก แบบรูป 63 Indicator
- ตัวอย่างปัญหาของแบบรูปนี้อ้างถึง Case 14 จากเอกสาร WSC-USECASES

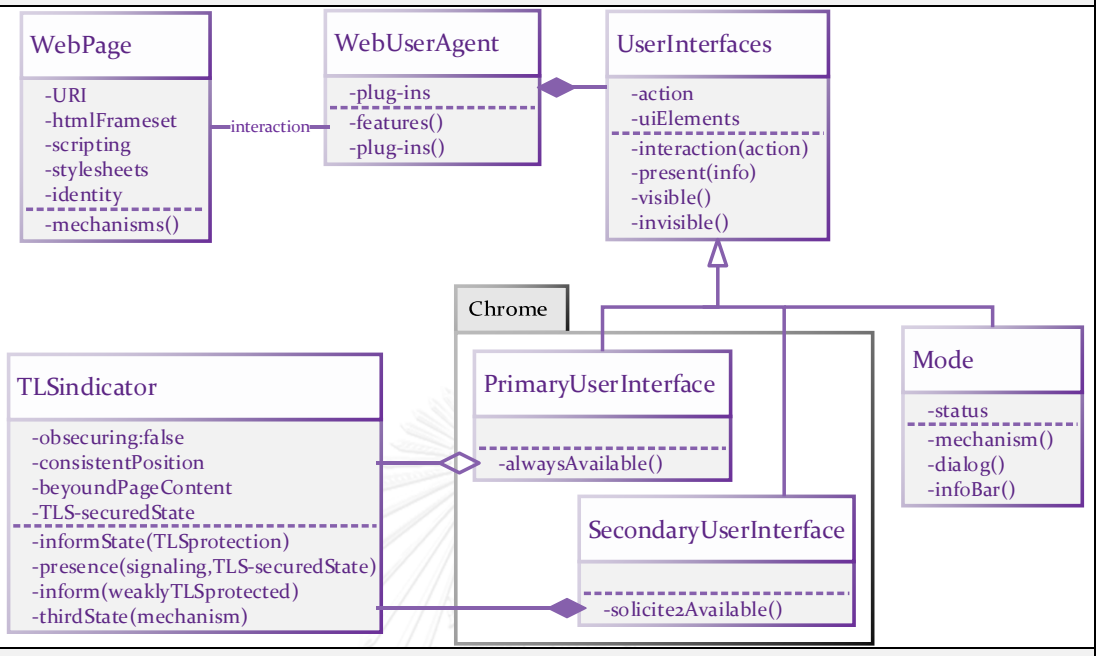
ตารางที่ ก.7 แบบรูปตัวชี้บอกความมั่นคงชั้นขนส่ง

Name	ตัวชี้บอกความมั่นคงชั้นขนส่ง	**ID**	WSCP63
Core	Availability	**Section**	Indicators and Interactions
Description			
แบบรูปนี้กล่าวถึงคุณลักษณะของตัวชี้บอกความมั่นคงชั้นขนส่งที่ใช้ในการแสดงข้อมูลเกี่ยวกับสถานะของการป้องกันการรักษาความมั่นคงชั้นขนส่งหรือสารสนเทศทางบริบทความมั่นคงของผู้บริการให้แก่ผู้ใช้ได้ทราบ			
Example			
กรณี 7 บริษัท Example Inc. มีบริการออนไลน์ที่ได้รับความนิยมและรองรับการทำรายการผ่านบัตรเครดิตมากมายในหนึ่งวัน เบ็ตตี้ใช้บริการดังกล่าวเป็นบางโอกาสและเธอเชื่อมั่นที่จะให้ข้อมูลบัตรเครดิตของเธอในการทำรายการ ในขณะที่มัลคัมมีแนวคิดที่จะโจรกรรม เขาสร้างเว็บเลียนแบบจากเว็บไซต์ของ Example และชี้นำให้ผู้ใช้เข้าสู่เว็บของเขาโดยการตั้งชื่อโดเมนของเว็บปลอมให้ใกล้เคียงกับเว็บไซต์ที่แท้จริงของ Example ดังนั้นจึงมีเหยื่อบางรายหลงเข้าสู่เว็บของเขาอย่างไม่ตั้งใจ และเบ็ตตี้เองก็กำลังป้อนข้อมูลบัตรเครดิตของเธอไปยังเว็บไซต์ที่ดูคล้ายกับเว็บของ Example			
Context			
บริบทในการนำแบบรูปนี้ไปประยุกต์ใช้เมื่อตัวแทนผู้ใช้เว็บเชื่อมต่อกับผู้ให้บริการผ่านการป้องกันการรักษาความมั่นคงชั้นขนส่งในสถานะใด ๆ			
Problem			
หากปราศจากการแจ้งเตือนเพื่อบอกสถานะเมื่อเกิดข้อผิดพลาดหรือการโจมตีระหว่างการรักษาความมั่นคงชั้นขนส่ง จะทำให้ผู้ใช้ไม่ทันระวังในการเข้าถึงเว็บไซต์ที่อาจก่อให้เกิดภัยต่อข้อมูลและระบบของผู้ใช้			
Solution			
ตัวแทนผู้ใช้เว็บจะต้องให้ข้อมูลเกี่ยวกับสถานะของการป้องกันการรักษาความมั่นคงชั้นขนส่งด้วยตัวชี้บอก อันมีคุณลักษณะดังนี้ 4. **การแสดงผล** โดยตัวชี้บอกความมั่นคงชั้นขนส่ง อาจเป็นส่วนหนึ่งของส่วนต่อประสานผู้ใช้แบบปฐมภูมิในระหว่างสถานะ (Mode, **Mode**) การใช้งานซึ่งถ่ายทอดสัญญาณให้แก่ผู้ใช้โดยแสดงอยู่ด้านบนเหนือเนื้อหาหน้าเว็บเท่านั้น มิเช่นนั้นข้อมูลดังกล่าวต้องพร้อมใช้งานผ่านทางส่วนต่อประสานผู้ใช้แบบทุติยภูมิ ตัวแทนผู้ใช้เว็บอาจทำตามข้อกำหนดนี้โดยการใช้สถานะที่สามของตัวชี้บอกความมั่นคงชั้นขนส่ง หรือโดยกลไกอื่น เช่น การใช้กล่องโต้ตอบ แถบสารสนเทศ อื่นๆ 5. **คุณภาพ** ตัวแทนผู้ใช้ที่แสดงผลผ่านส่วนต่อประสานผู้ใช้ควรจะทำให้ตัวชี้บอกความมั่นคงชั้นขนส่งพร้อมใช้งานในตำแหน่งการแสดงผลที่ต้องกัน โดยเนื้อหาเว็บจะต้องไม่คลุมเครือกับส่วนต่อประสานด้านความมั่นคงต้องกันกับแบบรูปที่ 74 6. **สถานะ** ตัวชี้บอกความมั่นคงชั้นขนส่งจะต้องแสดงสถานะความมั่นคงอย่างชัดเจนสำหรับหน้าเว็บแบบรักษาความมั่นคงชั้นขนส่งเท่านั้น ตัวแทนผู้ใช้ควรแจ้งเตือนเมื่อผู้ใช้กำลังเยี่ยมชมหน้าเว็บที่มาจากทรัพยากรพึ่งพิงทั้งหมดถูกค้นคืนผ่านช่องทางการรักษาความมั่นคงชั้นขนส่งอย่างอ่อนแอและผ่านหน้าเว็บแบบเนื้อหาผสม			

ตารางที่ ก.7 แบบรูปตัวชี้บอกความมั่นคงชั้นขนส่ง (ต่อ)

Name	ตัวชี้บอกความมั่นคงชั้นขนส่ง	ID	WSCP63

Internal Structure



Example Resolved

กรณี 7 ตัวแทนผู้ใช้เว็บแสดงตัวชี้บอกความมั่นคงชั้นขนส่งเฉพาะเมื่อเข้าถึงเว็บไซต์ที่แท้จริงของ Example เพื่อแจ้งให้กับเบ็ตตี้ได้ทราบว่าทรัพยากรของเว็บถูกค้นคืนผ่านช่องทางการรักษาความมั่นคงชั้นส่ง เบ็ตตี้ควรป้อนข้อมูลบัตรเครดิตของเธอไปยังเว็บไซต์ที่แท้จริงที่ตัวชี้บอกความมั่นคงชั้นขนส่งปรากฏเท่านั้น ในทางตรงกันข้ามหากไม่ปรากฏตัวชี้บอกดังกล่าว เบ็ตตี้จะต้องไม่ให้ข้อมูลใดๆ แก่เว็บที่ปลอมแปลง

Consequences

การแสดงผลของตัวชี้บอกที่ชัดเจนจะเตือนให้ผู้ใช้ได้ทราบถึงข้อผิดพลาดอันอาจเกิดจากการโจมตี อีกทั้งยังทำให้ผู้พิจารณาข้อมูลเพื่อใช้ตัดสินเชื่อถือหน้าเว็บดังกล่าวจากข้อมูลที่รายงานตามสถานะผ่านตัวชี้บอกที่ปรากฏให้ผู้ใช้เห็นและเข้าใจได้ทันที

See Also

- จากแบบรูป 61 ที่อาจมีโหมดการใช้งานซึ่งข้อกำหนดความต้องการนี้จะไม่ถูกนำไปใช้
- เนื้อหาของเว็บที่ทำให้ส่วนต่อประสานที่แสดงความมั่นคงมีความคลุมเครือ ศึกษาเพิ่มเติมจากแบบรูป 74
- ตัวอย่างปัญหาของแบบรูปนี้อ้างถึง Case 7 จากเอกสาร WSC-USECASES

ตารางที่ ก.8 แบบรูปการจัดการและการส่งสัญญาณความผิดพลาด

Name	การจัดการและการส่งสัญญาณความผิดพลาด	**ID**	WSCP64
Core	Accountability	**Section**	Indicators and Interactions
Description			
แบบรูปนี้จะกล่าวถึงการรับมือกับข้อผิดพลาดและวิธีการในการส่งสัญญาณข้อผิดพลาด โดยเรียงลำดับตามความรุนแรงน้อยไปถึงความรุนแรงมาก โดยเริ่มจากการแจ้งข้อผิดพลาดทั่วไป ไปยังการแจ้งเตือน จนถึงระดับการเตือนภัยโดยการรับมือกับข้อผิดพลาดที่ได้กล่าวถึงในแบบรูปนี้ส่วนใหญ่เกี่ยวข้องกับการสื่อสารผ่านข้อมูลด้านบริบทความมั่นคงเชิงเว็บ			
Example			
กรณี 22 แฟรงค์มักจะอ่านอีเมลของเขาในยามเช้า เช้านี้เขาได้รับอีเมลฉบับหนึ่งซึ่งอ้างว่ามาจากธนาคารของเขาและร้องขอให้เขายืนยันรายการที่ได้ทำล่าสุดโดยการคลิกไปยังลิงค์ที่ฝังมาในอีเมล ลิงค์ดังกล่าวไม่ได้แสดงยูอาร์แอลปกติที่เขาเคยใช้ในการเข้าถึงเว็บไซต์ธนาคารแต่ปรากฏชื่อธนาคารของเขา เขาคลิกเข้าสู่ลิงค์และนำไปยังเว็บปลอมแปลง เว็บปลอมแปลงดังกล่าวถูกปิดลงเนื่องจากพบว่าเป็นเว็บไซต์หลอก ดังนั้นเมื่อแฟรงค์เข้าสู่เว็บดังกล่าวเขาจึงได้รับเพียงข้อความแสดงข้อผิดพลาดทั่วไป <Error 404: File Not Found> แฟรงค์เองก็ไม่มั่นใจว่าเกิดอะไรขึ้น			
Example			
กรณี 13 เช่นเดียวกับผู้ใช้ท่านอื่นๆ เบ็ตตี้มีความเคยชินในการกดปิดอย่างรวดเร็วเมื่อตัวแทนผู้ใช้แสดงกล่องข้อความแจ้งเตือน จากพฤติกรรมดังกล่าว เบ็ตตี้ได้ละเลยการแจ้งเตือนจนทำให้เธอเข้าสู่หน้าเว็บที่ต้องสงสัยอย่างไม่ทันรู้ตัว			
Context			
แบบรูปนี้จะถูกประยุกต์ใช้เมื่อเกิดข้อผิดพลาดขึ้นระหว่างตัวแทนผู้ใช้เว็บขณะเชื่อมต่อกับผู้ให้บริการเว็บ และเมื่อตรงตามเงื่อนไขข้อผิดพลาดที่ได้นิยามในแบบรูป 54			
Problem			
เมื่อมีข้อผิดพลาดเกิดขึ้น หากตัวแทนผู้ใช้เว็บขาดการจัดการหรือการแจ้งเตือนที่เหมาะสมกับระดับความรุนแรงของข้อผิดพลาดที่มีผลต่อการรับรู้ของผู้ใช้ เช่น การแจ้งเตือนและเสนอตัวเลือกที่แนะนำให้ผู้ใช้ละเลยข้อความแจ้งเตือน จะทำให้ผู้ใช้ไม่เข้าใจความรุนแรงของข้อผิดพลาดที่เกิดขึ้นและละเลยการจัดการกับข้อผิดพลาด อันอาจเกิดภัยกับข้อมูลของผู้ใช้หรือระบบ			
Solution			
ตัวแทนผู้ใช้เว็บอาจสื่อสารข้อมูลข้อผิดพลาดผ่านตัวชี้ข้อผิดพลาด (Error Indicator, **ErrorIndicator**) หรือส่งสัญญาณผ่านส่วนต่อประสานผู้ใช้แบบปฐมภูมิหรือทุติยภูมิรวมถึงการใช้กลไกอื่นๆ โดยวิธีการในการส่งสัญญาณข้อผิดพลาดแบ่งเป็น 3 ระดับ คือ การรับมือกับข้อผิดพลาดทั่วไป ระดับการแจ้งเตือน และระดับการเตือนภัย มีรายละเอียดดังนี้ 1. **การรับมือกับความผิดพลาดทั่วไป (Error Signaling, ErrorSignaling)** เมื่อการส่งสัญญาณข้อผิดพลาดที่เกิดขึ้นเป็นส่วนหนึ่งของส่วนต่อประสานผู้ใช้ปฐมภูมิ ควรมีคุณลักษณะ ดังนี้			

ตารางที่ ก.8 แบบรูปการจัดการและการส่งสัญญาณความผิดพลาด (ต่อ)

Name	การจัดการและการส่งสัญญาณความผิดพลาด	**ID**	WSCP64

Solution

1)ข้อความแสดงข้อผิดพลาดผ่านส่วนต่อประสานผู้ใช้ปฐมภูมิควรจะถ่ายถอดในลักษณะเรียกร้องความสนใจจากผู้ใช้ ไม่ใช้คำศัพท์เชิงเทคนิคเฉพาะ

2)ข้อความแสดงข้อผิดพลาดผ่านส่วนต่อประสานผู้ใช้ปฐมภูมิจะต้องไม่ถ่ายถอดโดยใช้รูปภาพเพียงอย่างเดียว

3)ไม่ควรแนะนำผู้ใช้ให้เข้าสู่เว็บไซต์ปลายทางที่อาจก่อให้เกิดข้อผิดพลาด เช่น เพื่อให้ผลสะท้อนหรือได้รับคำแนะนำ

4)เมื่อข้อความแสดงข้อผิดพลาดขัดขวางกระแสงานของผู้ใช้ ตัวแทนผู้ใช้เว็บควรเสนอทางเลือกให้ผู้ใช้กลับไปยังหน้าเว็บก่อนหน้าอย่างง่ายดาย

5)สำหรับผู้ใช้ที่มีความชำนาญ การรับมือกับข้อผิดพลาดอาจจะมีทางเลือกให้สามารถเรียกดูรายละเอียดคำอธิบายของเงื่อนไขที่เป็นสาเหตุของข้อผิดพลาดให้เกิดขึ้นได้

2. **ข้อความการแจ้งเตือน (WarningMessage)** ข้อความแจ้งเตือนมีจุดประสงค์เพื่อแจ้งผู้ใช้ให้ทราบถึงสถานการณ์ที่ระบบประเมินความเป็นไปได้ว่าผู้ใช้อาจตกอยู่ในความเสี่ยง โดยอ้างอิงจากข้อมูลด้านบริบทความมั่นคงเชิงเว็บขณะนั้น ถึงแม้ไม่พบการโจมตีเกิดขึ้นก็สามารถแจ้งเตือนได้ ข้อความแจ้งเตือนควรมีลักษณะ ดังนี้

1) ข้อความแจ้งเตือนจะต้องขัดขวางการทำงานของผู้ใช้ในขณะนั้น เพื่อที่ผู้ใช้จะได้รับรู้ข้อความเหล่านั้น

2) ข้อความแจ้งเตือนจะต้องให้ตัวเลือกที่ชัดเจนแก่ผู้ใช้ว่าจะทำขั้นตอนอย่างไรต่อไป

3) ตัวเลือกที่ได้เสนอผ่านการแจ้งเตือนจะต้องอธิบายถึงประเด็นตามลำดับความหมายที่สามารถเข้าใจถึงการไม่ปรากฏของสารสนเทศอื่นๆ ที่รวมอยู่ในการมีปฏิสัมพันธ์เพื่อการแจ้งเตือน

4) หนึ่งในตัวเลือกที่เสนอควรจะได้รับการแนะนำให้ผู้ใช้เลือก และข้อความแจ้งเตือนควรมีความกระชับให้เห็นความแตกต่างของตัวเลือกที่ได้แนะนำให้แก่ผู้ใช้

5) ในกรณีที่ไม่ปรากฏตัวเลือกที่แนะนำ การแจ้งเตือนจะต้องนำเสนอวิธีการที่ผู้ใช้สามารถค้นพบข้อมูลเพิ่มเติมหากตัวเลือกที่มีอยู่คลุมเครือ หรือไม่สื่อความหมาย ผู้ใช้ไม่สามารถทำความเข้าใจได้

3. **ข้อความการเตือนภัย (DangerMessage)** การเตือนภัยมีจุดประสงค์เพื่อเตือนผู้ใช้ถึงภัยในสถานการณ์ที่มีภัยเกิดขึ้นกับข้อมูลของผู้ใช้ไม่ใช่เพียงแค่มีความเสี่ยงเท่านั้น การมีปฏิสัมพันธ์เพื่อสื่อสารข้อความเหล่านั้นจะต้องถูกออกแบบให้ขัดขวางการทำงานของผู้ใช้ การมีปฏิสัมพันธ์เหล่านั้นจะต้องถูกนำเสนอในลักษณะที่ไม่สามารถให้ผู้ใช้เข้าถึงหรือกระทำการใดๆ กับเว็บไซต์ปลายทางที่ก่อให้เกิดสถานการณ์ที่เป็นภัยได้ โดยปราศจากการแสดงการรับรู้ที่ชัดเจนต่อข้อความการเตือนภัย

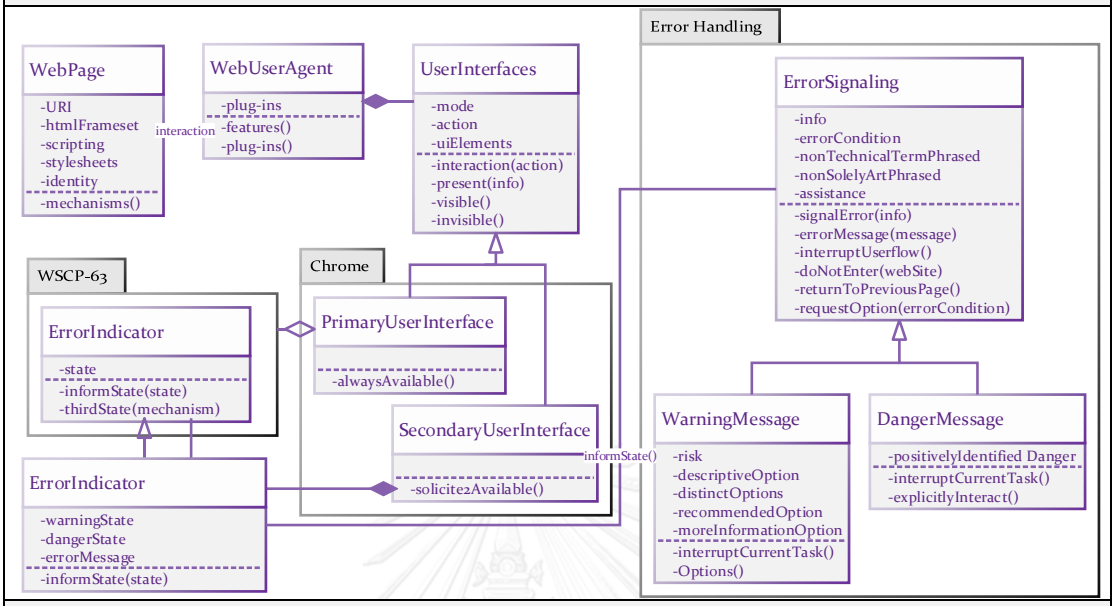
Consequences

การแบ่งการจัดการข้อผิดพลาดตามระดับจะช่วยให้ผู้ใช้ทำความเข้าใจกับข้อผิดพลาดและระดับความรุนแรงของข้อผิดพลาด ไปจนถึงจัดการกับข้อผิดพลาดดังกล่าวได้อย่างเหมาะสมตามความต้องการของผู้ใช้

ตารางที่ ก.8 แบบรูปการจัดการและการส่งสัญญาณความผิดพลาด (ต่อ)

Name	การจัดการและการส่งสัญญาณความผิดพลาด	ID	WSCP64

Internal Structure



Example Resolved

กรณี 22 แฟรงค์คลิกเข้าสู่ลิงค์และนำไปยังเว็บปลอมแปลง เว็บปลอมแปลงดังกล่าวถูกปิดลง ดังนั้นเมื่อแฟรงค์เข้าสู่เว็บดังกล่าว เขาควรรับข้อความแสดงข้อผิดพลาดเฉพาะเจาะจงถึงเหตุผลในการแจ้งปิดเนื่องจากพบว่าเป็นเว็บไซต์หลอก

กรณี 13 กล่องข้อความแจ้งเตือนขัดขวางการทำงานหลักและไม่ควรแนะนำผู้ใช้ให้เข้าสู่เว็บไซต์ปลายทางที่อาจก่อให้เกิดข้อผิดพลาด จนเบ็ตตี้ไม่สามารถละเลยการแจ้งเตือนและทำให้เธอหลีกเลี่ยงการเข้าสู่หน้าเว็บที่ต้องสังสัยอย่างไม่ทันรู้ตัวได้

Known Uses

- ตัวอย่างการหลีกเลี่ยงการใช้คำศัพท์เชิงเทคนิคเฉพาะ หากใบรับรองปรากฏข้อมูลชื่อดีเอ็นเอสในส่วนขยาย subjectAltNameที่ไม่ตรงกันกับ URI ของเว็บไซต์ที่ผู้ใช้พยายามเข้าเยี่ยมชม ข้อความแสดงข้อผิดพลาดสามารถอธิบายว่าผู้ใช้กำลังไปถึงเว็บไซต์ที่ต่างออกไป แทนที่จะรายงานว่า subjectAltName ไม่ตรงกัน
- ตัวอย่างตัวเลือกที่ชัดเจนต่อผู้ใช้ว่าจะทำขั้นตอนต่อไปเช่น ข้อความเหล่านั้นจะต้องไม่นำไปสู่สถานการณ์ที่มีตัวเลือกใดตัวเลือกหนึ่งที่ถูกเสนอแก่ผู้ใช้เพื่อยกเลิกการแจ้งเตือนและดำเนินการต่อ
- วิธีการที่ผู้ใช้สามารถค้นพบข้อมูลเพิ่มเติม เช่น การใช้การเชื่อมโยง การใช้หน้าต่างชั่วคราว อื่นๆ

See Also

- จากแบบรูป 61 ที่อาจมีโหมดการใช้งานซึ่งข้อกำหนดความต้องการนี้จะไม่ถูกนำไปใช้
- เนื้อหาของเว็บที่ทำให้ส่วนต่อประสานที่แสดงความมั่นคงมีความคลุมเครือ ศึกษาเพิ่มเติมจากแบบรูป 74
- ตัวอย่างปัญหาของแบบรูปนี้อ้างถึง Case 13 และ 22 จากเอกสาร WSC-USECASES

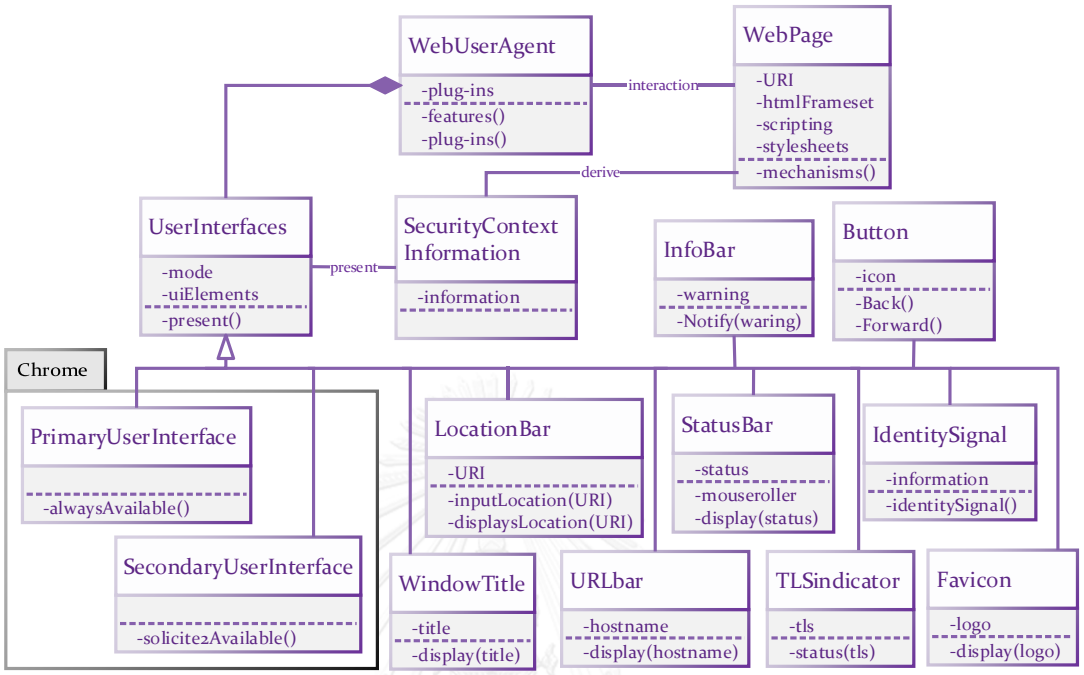
ตารางที่ ก.9 แบบรูปการนิยามส่วนต่อประสานผู้ใช้โครม

Name	การนิยามส่วนต่อประสานผู้ใช้โครม	**ID**	WSCP71
Core	Availability	**Section**	Robustness Best Practices
Description			
แบบรูปนี้นิยามส่วนต่อประสานผู้ใช้และอธิบายความสำคัญของการปรากฏของส่วนต่อประสานโครมของตัวแทนผู้ใช้เว็บ			
Example			
กรณี 6 ในขณะเร่งด่วน อลิสนึกขึ้นได้ว่าเธอจำเป็นต้องทำรายการธุรกรรมออนไลน์ ครั้งก่อนเธอเคยใช้อุปกรณ์มือถือของเธอในการค้นคืนข้อมูลจากเว็บไซต์ แต่ในครั้งนี้เธอตัดสินใจที่จะใช้อุปกรณ์มือถือของเธอในการทำธุรกรรมออนไลน์เนื่องจากเหตุฉุกเฉิน เธอเริ่มต้นใช้ตัวแทนใช้เว็บผ่านอุปกรณ์มือถือและกรอกยูอาร์แอลที่เธอจำได้จากที่เคยพบผ่านตัวแทนผู้ใช้เว็บในคอมพิวเตอร์ตั้งโต๊ะของเธอ หลังจากที่ใช้เวลาในการค้นคืนมากกว่าปกติ มือถือของเธอเริ่มปรากฏหน้าเว็บ แต่เนื่องจากขนาดของหน้าจอ อลิสจึงประมาณจากเลเอาท์ที่สังเกตพบว่ามีความคล้ายคลึงกันแต่ไม่เหมือนเลยซะทีเดียวกับเว็บไซต์ที่เธอพบผ่านคอมพิวเตอร์ตั้งโต๊ะ อีกทั้งเธอไม่สามารถมองเห็นยูอาร์แอลแบบเต็มได้ อลิสเลื่อนหน้าจอไปยังจุดที่มีลิงค์เชื่อมโยงไปยังหน้าเว็บที่ใช้ทำรายการและกดเข้าสู่ลิงค์ หลังจากความล่าช้า มือถือของเธอแสดงหน้าเว็บที่ร้องขอข้อมูลในการเข้าสู่ระบบของธนาคารปกติ อลิสจะทราบได้อย่างไรว่าเธอสามารถกรอกข้อมูลสู่หน้าเว็บดังกล่าวได้อย่างปลอดภัย			
Context			
แบบรูปนี้ประยุกต์ใช้สำหรับตัวแทนผู้ใช้เว็บที่มีส่วนต่อประสานผู้ใช้เชิงภาพ			
Problem			
การพัฒนาตัวแทนผู้ใช้เว็บหากขาดการนิยามตำแหน่งและหน้าที่ของส่วนต่อประสานผู้ใช้อาจทำให้เกิดช่องโหว่ เช่น หากขาดการกำหนดส่วนต่อประสานผู้ใช้ที่แสดงบริบทด้านความมั่นคง ส่วนต่อประสานดังกล่าวอาจถูกควบคุมได้จากเนื้อหาเว็บ ทำให้ผู้ใช้ได้รับข้อมูลบริบทความมั่นคงของเว็บที่ถูกปลอมแปลงจากผู้โจมตีระบบ หรือหากปราศจากส่วนต่อประสานผู้ใช้ที่มีหน้าที่รักษาความมั่นคง ผู้ใช้จะไม่สามารถรับรู้ถึงข้อมูลหรือการเตือนภัยได้			
Solution			
ส่วนต่อประสานผู้ใช้เป็นตัวกลางในการนำเสนอข้อมูลและรองรับคำสั่งจากผู้ใช้ กลุ่มผลิตภัณฑ์ด้านการแสดงผลของตัวแทนผู้ใช้แบ่งเป็น 2 ประเภท คือ ส่วนต่อประสานผู้ใช้ปฐมภูมิ (Primary User Interface, **PrimaryUI**) และส่วนต่อประสานผู้ใช้ทุติยภูมิ (Secondary User Interface, **SecondaryUI**) โดยส่วนต่อประสานผู้ใช้ปฐมภูมิจะปรากฏแก่ผู้ใช้โดยปราศจากการร้องขอ ในขณะที่ส่วนต่อประสานผู้ใช้ทุติยภูมิต้องอาศัยการร้องขอจากผู้ใช้ในการแสดงผล ส่วนต่อประสานทั้งสองแบบนี้ รวมเรียกว่า ส่วนต่อประสานโครม (Chrome) ส่วนต่อประสานแต่ละตำแหน่งมีหน้าที่ต่างกัน จำแนกตามหน้าที่ได้ดังนี้ 1. **แถบแสดงตำแหน่ง** (Location Bar, **LocationBar**) ใช้ป้อนข้อมูลที่อยู่เว็บเพื่อร้องขอทรัพยากรจากผู้ให้บริการ 2. **สัญญาณอัตลักษณ์** (Identity Signal, **IdentitySignal**) ใช้สำหรับแสดงข้อมูลอัตลักษณ์ (Identity Information) ที่เกี่ยวข้องกับเว็บ			

ตารางที่ ก.9 แบบรูปการนิยามส่วนต่อประสานผู้ใช้โครม (ต่อ)

Name	การนิยามส่วนต่อประสานผู้ใช้โครม	**ID**	WSCP71
Solution			
3. **แถบแสดงชื่อเว็บบนหน้าต่างของตัวแทนผู้ใช้เว็บ** (Browser Window Title, **WindowTitle**) ใช้แสดงชื่อของเว็บที่กำลังเข้าเยี่ยมชม ข้อมูลชื่อได้รับจากเนื้อหาของเว็บ (HTML TITLE element) 4. **ปุ่มย้อนกลับและไปข้างหน้า** (Back and forward buttons, **Button**) ใช้สำหรับการนำทางจากบันทึกการเข้าชมเว็บ โดยรายการการเยี่ยมชมนำเข้าข้อมูลชื่อได้รับจากเนื้อหาของเว็บ (HTML TITLE element) มาแสดง 5. **แถบแสดงที่อยู่เว็บ** (URL bar, **URLbar**) ใช้แสดงการเชื่อมโยงหลายมิติของผู้ให้บริการเว็บที่กำลังเชื่อมต่อตัวแทนผู้ใช้อาจนำข้อมูลชื่อผู้ให้บริการ (Hostname) มาแสดง 6. **สัญลักษณ์แม่กุญแจ** (Padlock Icon, **TLSindicator**) ใช้แสดงสถานะของการรักษาความมั่นชั้นขนส่ง (SSL) 7. **สัญลักษณ์ของเว็บ (**Favicon**, Favicon)** ผู้ให้บริการเว็บสามารถใช้ข้อมูลภาพแสดงโลโก้ที่เป็นเอกลักษณ์ของเว็บตนเองแสดงบนแถบแสดงที่อยู่เว็บเพื่อให้ผู้ใช้จดจำได้ บางครั้งตัวแทนผู้ใช้เว็บแสดงข้อมูลดังกล่าวในตำแหน่งเดียวกันกับสัญลักษณ์แม่กุญแจ 8. **แถบแสดงสถานะ (**Status Bar**, StatusBar)** ใช้แสดงข้อความที่ตัวแทนผู้ใช้เว็บต้องการสื่อสารกับผู้ใช้ เช่น เมื่อผู้ใช้วางเมาส์บนการเชื่อมโยงหลายมิติ ตัวแทนผู้ใช้จะแสดงปลายทางของการเชื่อมโยงนั้นผ่านแถบแสดงสถานะ 9. **แถบสารสนเทศ (**Information Bar**, InfoBar) หรือแถบการแจ้งเตือน (**Notification Bar**)** ปรากฏอยู่ด้านบนเหนือหน้าต่างแสดงเนื้อหาเว็บเพื่อสื่อสารกับผู้ใช้ ข้อความที่แสดงจำเพาะเกี่ยวข้องกับหน้าต่างเนื้อหาที่ผู้ใช้กำลังเข้าชม โดยปกติจะใช้เตือนภัยเมื่อมีการกระทำที่ไม่พึงประสงค์เกิดขึ้น เช่นการติดตั้งซอฟต์แวร์อัตโนมัติในหน้าต่างเนื้อหาใหม่ 10. **ส่วนต่อประสานโครมของตัวแทนผู้ใช้เว็บ (Chrome)** จะต้องปรากฏอยู่เสมอเพื่อส่งสัญญาณสารสนเทศทางบริบทความมั่นคง ตามบทบาทและหน้าที่ที่ได้กำหนดไว้ เพื่อไม่ให้เกิดความกำกวมหรือถูกนำไปใช้โดยผู้โจมตีในการระงับหรือแทนที่การทำงานของส่วนต่อประสานด้านความมั่นคง		
Example Resolved			
จากกรณี 6 ในขณะเร่งด่วน อลิสนึกเริ่มต้นใช้ตัวแทนผู้ใช้เว็บในการทำธุรกรรมผ่านอุปกรณ์มือถือและกรอกยูอาร์แอลที่เธอจำได้ มือถือของเธอเริ่มปรากฏหน้าเว็บเนื่องจากขนาดของหน้าจอ อลิสจึงประมาณจากเลเอาท์ที่สังเกตพบว่ามีความคล้ายคลึงกันแต่ไม่เหมือนเลยซะทีเดียวกับเว็บไซต์ที่เธอพบผ่านคอมพิวเตอร์ตั้งโต๊ะ อีกทั้งเธอไม่สามารถมองเห็นยูอาร์แอลแบบเต็มได้ แต่ตัวแทนผู้ใช้เว็บปรากฏสัญญาณอัตลักษณ์ (Identity Signal) เพื่อแสดงข้อมูลอัตลักษณ์ (Identity Information) ที่เกี่ยวข้องกับเว็บ อลิสเลื่อนหน้าจอไปยังจุดที่มีลิงค์เชื่อมโยงไปยังหน้าเว็บที่ใช้ทำรายการและกดเข้าสู่ลิงค์ หลังจากความล้าช้า อุปกรณ์มือถือของเธอแสดงหน้าเว็บที่ร้องขอข้อมูลในการเข้าสู่ระบบของธนาคารปกติและแสดงสัญลักษณ์แม่กุญแจ (Padlock Icon) เพื่อแจ้งสถานะของการรักษาความมั่นชั้นขนส่ง (SSL) อลิสจึงสามารถกรอกข้อมูลสู่หน้าเว็บดังกล่าวได้อย่างปลอดภัย			

ตารางที่ ก.9 แบบรูปการนิยามส่วนต่อประสานผู้ใช้โครม (ต่อ)

Internal Structure

Variants
- ข้อกำหนดนี้จะไม่ถูกประยุกต์ใช้เมื่อ ส่วนต่อประสานผู้ใช้ถูกยกเลิกอย่างชัดเจนโดยผู้ใช้
Consequences
การเข้าใจนิยามและหน้าที่ของส่วนต่อประสานผู้ใช้จะช่วยให้ผู้ออกแบบลดช่องโหว่ที่อาจเกิดจากการเรียกใช้โดยผู้โจมตีระบบผ่านเนื้อหาเว็บที่กระตุ้นการทำงานของส่วนต่อประสานด้านบริบทความมั่นคง เมื่อส่วนต่อประสานด้านความมั่นคงปรากฏผู้ใช้สามารถรับทราบสถานะของหน้าเว็บได้อย่างทันที
See Also
- แบบรูปที่ 63 เพื่อเข้าใจถึงความสำคัญของการส่งสัญญาณสารสนเทศทางบริบทความมั่นคง - นิยามของผลิตภัณฑ์ส่วนต่อประสานผู้ใช้และตัวอย่างปัญหาของแบบรูปนี้อ้างถึงเอกสาร WSC-USECASES

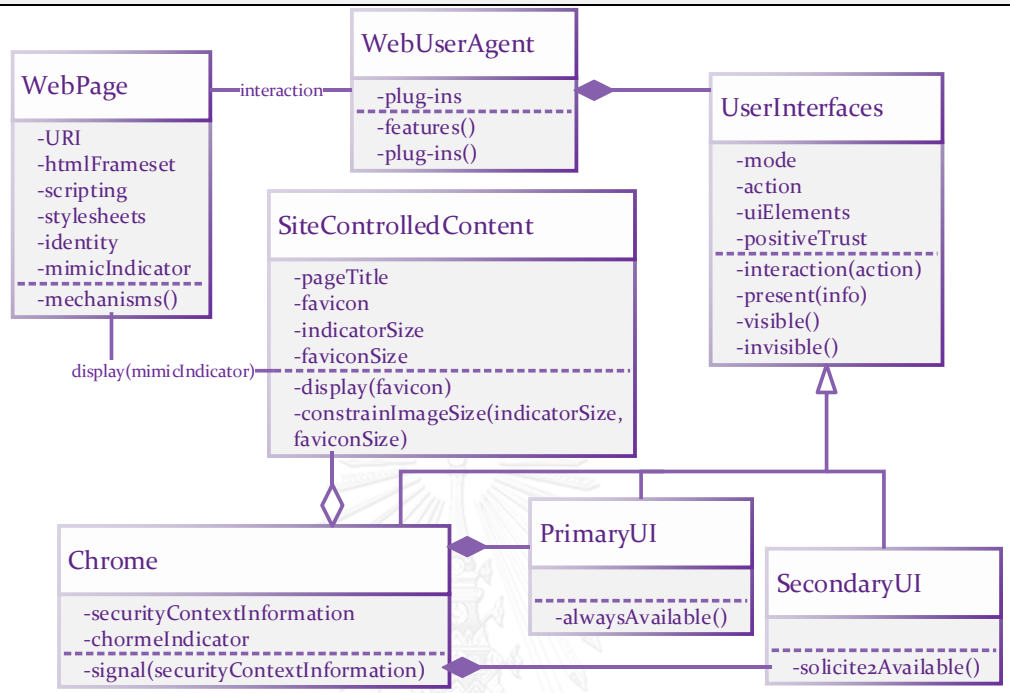
ตารางที่ ก.10 แบบรูปการป้องกันตัวชี้บอกความมั่นคงจากการลอกเลียนโดยเนื้อหาเว็บ

Name	การป้องกันตัวชี้บอกความมั่นคงจากการลอกเลียนโดยเนื้อหาเว็บ	**ID**	WSCP72
Core	Integrity	**Section**	Robustness Best Practices
Description			
แบบรูปนี้อธิบายถึงคำแนะนำสำหรับตัวชี้บอกความมั่นคงของตัวแทนผู้ใช้เว็บเพื่อป้องกันการถูกเนื้อหาเว็บพยายามลอกเลียน โดยตัวชี้บอกไม่ควรปะปนกับเนื้อหาเว็บ			
Example			
ดัดแปลงจากกรณี 3 อลิสชำระบิลของเธออาทิตย์ละครั้ง เธอเปิดตัวแทนผู้ใช้เว็บของเธอขึ้น และทำตามความเคยชินโดยการเข้าเว็บไซต์ธนาคารของเธอผ่านที่คั่นหน้าบุ๊คมาร์ค (Bookmark) คั่นหน้าดังกล่าวชี้ไปยังเว็บไซต์ที่เธอไม่คุ้นเคยด้วยโดเมนใหม่ หน้าเว็บดังกล่าวประกาศให้ทราบว่าธนาคารของเธอได้เปิดใช้งานเว็บใหม่และเปลี่ยนแปลงชื่อไปเล็กน้อยและสัญลักษณ์ประจำของเว็บ (Favicon) มีลักษณะคล้ายสัญลักษณ์แม่กุญแจ (Padlock) เธอถูกร้องขอให้กรอกข้อมูลส่วนตัวเพื่อยืนยันตัวจริงและเข้าสู่ระบบธุรกรรมออนไลน์ใหม่ในทันใด			
Context			
แบบรูปนี้นำไปประยุกต์ใช้กับตัวแทนผู้ใช้เว็บที่แสดงส่วนต่อประสานผู้ใช้ที่สามารถควบคุมโดยเนื้อหาเว็บ เมื่อเนื้อหาเว็บพยายามที่จะควบคุมส่วนต่อประสานผู้ใช้โครมหรือแสดงผลในบริเวณที่ใกล้เคียง			
Problem			
แถบแสดงตำแหน่ง (Location Bar) มักจะพบอยู่บนตัวแทนผู้ใช้เว็บถูกใช้แสดงทั้งตัวชี้บอกความมั่นคงผ่านสัญลักษณ์แม่กุญแจ (Padlock) และบางครั้งก็แสดงสัญลักษณ์ประจำของเว็บ (Favicon) ซึ่งสัญลักษณ์ประจำของเว็บสามารถควบคุมโดยเนื้อหาเว็บและถูกใช้ในการคัดลอกให้แสดงในลักษณะของสัญลักษณ์แม่กุญแจได้โดยง่าย ซึ่งจะเกิดการดึงดูดความสนใจให้ผู้ใช้เข้าใจผิดได้เพื่อให้ผู้ใช้สนใจตัวชี้บอกความมั่นคงแบบสถิต (Static Passive) ทำให้ผู้ใช้รับรู้และความเข้าใจตัวชี้บอกดังกล่าวเป็นสิ่งที่ยากเมื่อการนำเสนอดังกล่าวที่ถูกใช้สำหรับตัวชี้บอกความมั่นคงยังสามารถถูกควบคุมได้โดยเนื้อหาเว็บ			
Solution			
เพื่อหลีกเลี่ยงการลอกเลียนหรือซ้อนทับส่วนต่อประสานผู้ใช้โดยเนื้อหาเว็บ ตัวแทนผู้ใช้เว็บจะต้องไม่นำเสนอข้อมูลในลักษณะที่น่าเชื่อถือโดยใช้องค์ประกอบส่วนต่อประสานผู้ใช้ ซึ่งเนื้อหาเว็บสามารถควบคุมหรือลอกเลียนแบบกับส่วนต่อประสานโครมได้ การควบคุมเนื้อหาจากเว็บไซต์ (Site Controlled Content, **SiteControlledContent**) เช่น ชื่อหน้าเว็บ (Page Title) สัญลักษณ์ประจำ (Favicon) อาจวางอยู่บนส่วนต่อประสานผู้ใช้โครม (Chrome, **Chrome**) แต่เนื้อหาดังกล่าวจะต้องไม่แสดงในลักษณะที่สร้างความสับสนระหว่างเนื้อหาเว็บและตัวชี้บอกความมั่นคง (Indicator) โดยเฉพาะอย่างยิ่งหากเนื้อหาดังกล่าวลอกเลียนลักษณะตัวชี้บอกในตำแหน่งที่ใกล้เคียง ตัวแทนผู้ใช้เว็บไม่ควรจะใช้รูปภาพขนาด 16x16 ในส่วนต่อประสานผู้ใช้เพื่อชี้บอกสถานะด้านความมั่นคง หากทำเช่นนั้นอาจก่อให้เกิดการลอกเลียน ได้ ข้อกำหนดนี้จะถูกนำไปประยุกต์ใช้ในทั้งส่วนต่อประสานแบบปฐมภูมิ (Primary User Interface, **PrimaryUI**) และทุติยภูมิ (Secondary User Interface, **SecondaryUI**) ของการแสดงผลส่วนต่อประสานผู้ใช้			

ตารางที่ ก.10 แบบรูปการป้องกันตัวชี้บอกความมั่นคงจากการลอกเลียนโดยเนื้อหาเว็บ (ต่อ)

Name	การป้องกันตัวชี้บอกความมั่นคงจากการลอกเลียนโดยเนื้อหาเว็บ	ID	WSCP72

Internal Structure



Example Resolved

จากกรณี 3 อลิสชำระบิลของเธออาทิตย์ละครั้ง เธอเปิดตัวแทนผู้ใช้เว็บของเธอขึ้น และทำตามความเคยชินโดยการเข้าเว็บไซต์ธนาคารของเธอผ่านที่คั่นหน้าบุ๊คมาร์ค (Bookmark) คั่นหน้าดังกล่าวชี้ไปยังเว็บไซต์ที่เธอไม่คุ้นเคยด้วยโดเมนใหม่ หน้าเว็บดังกล่าวประกาศให้ทราบว่าธนาคารของเธอได้เปิดใช้งานเว็บใหม่และเปลี่ยนแปลงชื่อไปเล็กน้อย ตัวแทนผู้ใช้ควรระงับการแสดงสัญลักษณ์ประจำของเว็บ (Favicon) ที่มีลักษณะคล้ายสัญลักษณ์แม่กุญแจ (Padlock) และแจ้งเตือนเธอก่อนถูกร้องขอให้กรอกข้อมูลส่วนตัวเพื่อยืนยันตัวจริงและเข้าสู่ระบบธุรกรรมออนไลน์ใหม่ในทันใด

Consequences

หลีกเลี่ยงการถูกปลอมแปลงหรือลอกเลียนตัวชี้บอกความมั่นคงจากเนื้อหาเว็บเพื่อไม่ให้ผู้ใช้สับสนและหลงเชื่อเนื้อหาเว็บที่ปลอมแปลง

See Also

- ตัวอย่างปัญหาของแบบรูปนี้อ้างถึง Case 3 จากเอกสาร WSC-USECASES

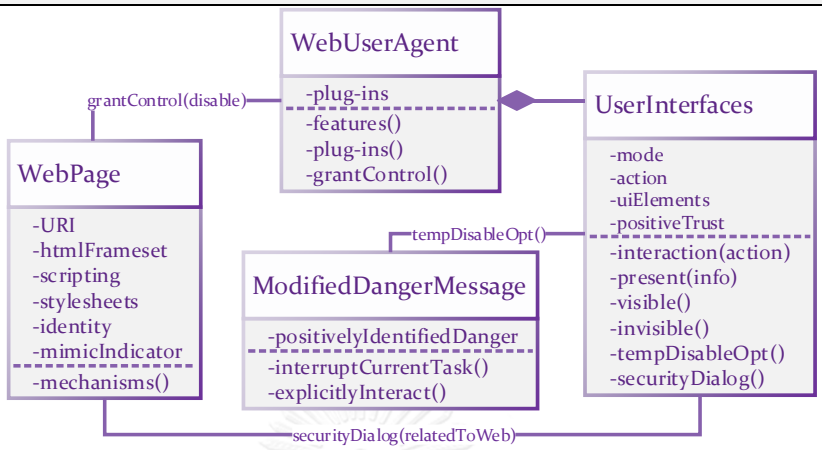
ตารางที่ ก.11 แบบรูปการจัดการกับความสนใจของผู้ใช้

Name	การจัดการกับความสนใจของผู้ใช้	**ID**	WSCP73
Core	Accountability	**Section**	Robustness Best Practices
Description			
แบบรูปนี้อธิบายพฤติกรรมของผู้ใช้ต่อการตัดสินใจเมื่อระบบแสดงกล่องข้อความที่ผู้ใช้จำเป็นต้องโต้ตอบซ้ำๆ จำนวนมากจนเกิดการละเลยการพิจารณาข้อความดังกล่าว ทั้งยังแนะนำวิธีการจัดการกับความสนใจของผู้ใช้เพื่อให้หน้าต่างแจ้งเตือนทำงานอย่างมีประสิทธิผล			
Example			
กรณี 13 เช่นเดียวกับผู้ใช้ท่านอื่นๆ เบ็ตตี้มีความเคยชินในการกดปิดอย่างรวดเร็วเมื่อตัวแทนผู้ใช้แสดงกล่องข้อความแจ้งเตือน จากพฤติกรรมดังกล่าว เบ็ตตี้ได้ละเลยการแจ้งเตือนจนทำให้เธอเข้าสู่หน้าเว็บที่ต้องสังสัยอย่างไม่ทันรู้ตัว			
Context			
แบบรูปนี้ประยุกต์ใช้เมื่อตัวแทนผู้ใช้เว็บหรือเนื้อหาเว็บเรียกร้องให้ผู้ใช้ตัดสินใจผ่านกล่องโต้ตอบซ้ำๆ เป็นจำนวนมาก			
Problem			
การโจมตีด้วยปฏิสัมพันธ์จำนวนมากแสดงให้เห็นถึงเว็บไซต์ที่มีเจตนามุ่งร้ายในการกระทำการที่ไม่พึงประสงค์ (เช่น การติดตั้งซอฟต์แวร์ที่อาจแอบแฝงการยอมรับจากผู้ใช้โดยการกดปุ่ม "OK" บนหน้าต่างแจ้งเตือน) หรือแสวงหาประโยชน์จากการดึงดูดความสนใจจากผู้ใช้ไปจากการใช้งานหลัก เว็บไซต์ที่ทำการเปิดหน้าต่างขึ้นใหม่จำนวนมากเกินกว่าความต้องการของเนื้อหาเว็บและอาศัยการกระทำที่ไม่พึงประสงค์ที่ได้กระทำเมื่อผู้ใช้พยายามที่จะปิดหน้าต่างที่เกิดขึ้นใหม่เหล่านั้นหรือการเลือกที่กล่องโต้ตอบที่แสดงถึงการตัดสินใจที่ระบบแนะนำ จากการสังเกตวิธีการเชิงปฏิสัมพันธ์ในระหว่างระยะเวลาสั้นๆ ผู้ใช้ส่วนใหญ่ทราบวิธีการใช้งานตัวเลือกโดยปริยายหรือคีย์ลัด เช่น เมื่อกดปุ่มตกลง (Enter) ซ้ำๆ ไปจนกว่าหน้าต่างโต้ตอบที่กีดขวางผู้ใช้จากปฏิสัมพันธ์ที่ผู้ใช้ต้องการจะสิ้นสุดลง พฤติกรรมดังกล่าวของผู้ใช้จะทำให้ละเลยการพิจารณาข้อผิดพลาดที่เกิดขึ้น			
Solution			
เพื่อให้ผู้ใช้เห็นความสำคัญของข้อความเตือนภัย ส่วนต่อประสานผู้ใช้ถูกใช้ในการแจ้งให้ผู้ใช้ทราบถึงเหตุการณ์วิกฤติด้านความมั่นคงหรือใช้เพื่อร้องขอการนำเข้าข้อมูล จำเป็นต้องอาศัยเทคนิคป้องกันการยกเลิกได้ทันทีของส่วนต่อประสานผู้ใช้ (Dismissal Prevention) เมื่อผู้ใช้เผชิญกับการแจ้งเตือนเกี่ยวกับความมั่นคง ตัวแทนผู้ใช้เว็บจะต้องไม่ยินยอมให้กล่องตอบโต้ของตัวแทนผู้ใช้เว็บถูกควบคุมได้โดยเนื้อหาเว็บ (Granted-Control) และตัวแทนผู้ใช้เว็บไม่ควรจะแสดงกล่องโต้ตอบความมั่นคง (Modal Security Dialog) เกี่ยวข้องกับหน้าเว็บที่ผู้ใช้ไม่ได้สนใจในขณะนั้น			

ตารางที่ ก.11 แบบรูปการจัดการกับความสนใจของผู้ใช้ (ต่อ)

Name	การจัดการกับความสนใจของผู้ใช้	ID	WSCP73

Internal Structure



Example Resolved

จากกรณี 13 เช่นเดียวกับผู้ใช้ท่านอื่นๆ เบ็ตตี้มีความเคยชินในการกดปิดอย่างรวดเร็วเมื่อตัวแทนผู้ใช้แสดงกล่องข้อความแจ้งเตือน ตัวแทนผู้ใช้ป้องกันการยกเลิกได้ทันทีของส่วนต่อประสานผู้ใช้จากพฤติกรรมดังกล่าว เพื่อให้เบ็ตตี้ได้พิจารณาข้อความการแจ้งเตือนไม่ให้เธอเข้าสู่หน้าเว็บที่ต้องสังสัยอย่างไม่ทันรู้ตัว

Known Uses

- เทคนิคของส่วนต่อประสานผู้ใช้ ที่ป้องกันการยกเลิกได้ทันที เช่น ปิดกั้นการใช้ปุ่ม "OK" ชั่วคราวบนส่วนต่อประสานผู้ใช้จะทำให้การมีปฏิสัมพันธ์ที่ดึงดูดความสนใจของผู้ใช้ดังกล่าวพร้อมใช้งาน
- กล่องโต้ตอบความมั่นคง (Security Dialog) ปรากฏข้อความพร้อมรับ (Prompt) สำหรับหนังสือรับรองของผู้ใช้ ข้อผิดพลาดของสคริปต์และข้อผิดพลาดของการรักษาความมั่นคงชั้นขนส่ง

Consequences

การจัดการกับความสนใจของผู้ใช้จะช่วยให้ผู้ใช้ได้รับทราบข้อความสำคัญด้านความมั่นคงในยามจำเป็น

See Also

- ศึกษาเพิ่มเติมเกี่ยวกับการแจ้งเตือนล่วงหน้าเกี่ยวกับความมั่นคงได้จากแบบรูป 64 ข้อความแจ้งเตือน
- ตัวอย่างปัญหาของแบบรูปนี้อ้างถึง Case 13 จากเอกสาร WSC-USECASES

ตารางที่ ก.12 แบบรูปส่วนต่อประสานโปรแกรมประยุกต์ของตัวแทนผู้ใช้เว็บ

Name	ส่วนต่อประสานโปรแกรมประยุกต์ของตัวแทนผู้ใช้เว็บที่เรียกใช้ได้โดยเนื้อหาเว็บ	**ID**	WSCP74
Core	Accountability	**Section**	Robustness Best Practices
Description			
แบบรูปนี้รวบรวมคำแนะนำเกี่ยวกับข้อจำกัดในการปรับแต่งตัวแทนผู้ใช้โดยเนื้อหาเว็บให้เป็นไปอย่างเหมาะสม และแนวปฏิบัติสำหรับป้องกันการโจมตีจากเว็บไซต์ที่ประสงค์ร้ายจากการเรียกใช้ส่วนต่อประสานโปรแกรมประยุกต์ของตัวแทนผู้ใช้			
Example			
กรณี 16 แฟรงค์มักจะอ่านบทความ ในขณะที่เขากำลังจิบกาแฟแก้วแรกในยามเช้า เขาคลิกไปยังลิงค์และเดินละจากคอมพิวเตอร์ไปยังเครื่องชงกาแฟเพื่อเติมกาแฟ หลังจากกลับมายังคอมพิวเตอร์ เขาพบว่าหน้าจอได้ปรากฏหน้าต่างแบบผุดขึ้นแสดงโฆษณาโปรแกรมการจัดการเช็คแบบใหม่ซึ่งเสนอโดยธนาคารที่เขาเป็นลูกค้า พร้อมเสนอให้ดาวน์โหลดโปรแกรมทดลองไปใช้ได้ฟรี โฆษณาดังกล่าวมาจากตัวแทนฝ่ายขายมิใช่จากธนาคารโดยตรง **กรณี 20** อลิสชำระบิลของเธออาทิตย์ละครั้ง เธอเปิดตัวแทนผู้ใช้เว็บของเธอขึ้น และทำตามความเคยชินโดยการเข้าเว็บไซต์ธนาคารของเธอผ่านที่คั่นหน้าบุ๊คมาร์ค (Bookmark) กระบวนการดาวน์โหลดได้เริ่มขึ้นและหน้าต่างแบบผุดขึ้นแจ้งอลิสให้ติดตั้งซอฟต์แวร์ไปยังคอมพิวเตอร์ของเธอเพื่อใช้ในการทำรายการกับธนาคารในอนาคต			
Context			
ตัวแทนผู้ใช้ที่รองรับการเรียกใช้ส่วนต่อประสานโปรแกรมประยุกต์จากเนื้อหาเว็บ เช่น การปรับคั่นหน้า (Bookmark) ให้ทันสมัย ตัวแทนผู้ใช้ที่รองรับการจัดการและหน้าที่งานบางประการของส่วนต่อประสานผู้ใช้ เช่น การเปิดหน้าต่างใหม่ การปรับขนาดหน้าต่าง อื่นๆไปจนถึงการดาวน์โหลดซอฟต์แวร์เพื่อติดตั้งภายนอกของบริบทตัวแทนผู้ใช้เว็บในภายหลัง			
Problem			
ความสามารถบางประการของส่วนต่อประสานโปรแกรมประยุกต์ของตัวแทนผู้ใช้เว็บอาจก่อให้เกิดปัญหาดังนี้ **ปัญหาด้านการปกปิดปลอมแปลงข้อมูล** ตัวแทนผู้ใช้เว็บยอมให้เนื้อหาเว็บใช้การทำงานซ่อนส่วนต่อประสานด้านความมั่นคงของตัวแทนผู้ใช้จะอำนวยความสะดวกให้การโจมตีแบบรูปภาพในรูปภาพ (Picture-in-Picture attack) ที่ซึ่งส่วนต่อประสานโครมปลอมถูกจัดเตรียมโดยเนื้อหาเว็บได้นำมาวางแทนที่ส่วนต่อประสานที่ได้ซ่อนไว้ (โดยปกติจะชี้ให้เห็นถึงสถานะความมั่นคงที่พบ) โดยการปกปิดหรือคลุมเครือองค์ประกอบสำคัญของส่วนต่อประสานตัวแทนผู้ใช้เว็บดังกล่าวเพื่อหลอกลวงผู้ใช้ให้กระทำการที่อันตรายต่อระบบ **ปัญหาจากการดาวน์โหลดซอฟต์แวร์** เว็บไซต์อาจเรียกใช้การดาวน์โหลดซอฟต์แวร์โดยปราศจากการยอมรับจากผู้ใช้ หรือหลอกลวงให้ผู้ใช้ยอมรับการดาวน์โหลด **ปัญหาจากการปรับแต่งคั่นหน้า** หากการยอมรับการปรับคั่นหน้าปราศการตรวจสอบอาจก่อให้เกิดความสับสนแก่ผู้ใช้ เมื่อมีการปลอมแปลงข้อมูลของเว็บให้ใกล้เคียงกับเว็บที่จริงที่ผู้ใช้สนใจ **ปัญหาของหน้าต่างแบบผุดขึ้น** การสร้างหน้าต่างผุดขึ้นจำนวนมากเกินไปในทางเทคนิคนั้นสามารถทำให้เกิดเงื่อนไขที่ผู้ใช้ละเลยกล่องตอบโต้ไปอย่างรวดเร็ว วิธีอาจถูกนำไปใช้ในการโจมตีด้วยปฏิสัมพันธ์ที่ต่อเนื่องอย่าง			

ตารางที่ ก.12 แบบรูปส่วนต่อประสานโปรแกรมประยุกต์ของตัวแทนผู้ใช้เว็บ (ต่อ)

Name	ส่วนต่อประสานโปรแกรมประยุกต์ของตัวแทนผู้ใช้เว็บที่เรียกใช้ได้โดยเนื้อหาเว็บ	**ID**	WSCP74
Problem			
มากมายความล้มเหลวในความพยายามดังกล่าวจะทำให้ผู้ใช้ที่ประสงค์จะใช้งานไปยังเว็บไซต์เหล่านั้นปิดการทำงานในส่วนของการป้องกันกับเว็บอื่นเช่นกัน			
Solution			
หน้าที่การทำงานของตัวแทนผู้ใช้เว็บที่รองรับการเรียกใช้งานโดยเนื้อหาเว็บ อาจเกิดช่องโหว่ให้เนื้อหาเว็บโจมตีหรือฉวยโอกาส เพื่อปิดช่องโหว่ดังกล่าวตัวแทนผู้ใช้เว็บควรมีข้อจำกัดเพื่อป้องกันการใช้งานที่ไม่พึงประสงค์ ข้อจำกัดด้านความสามารถบางประการของส่วนต่อประสานโปรแกรมประยุกต์ของตัวแทนผู้ใช้เว็บเพื่อป้องกันการโจมตี แบ่งเป็น 4 กลุ่มตามความสามารถ คือ ด้านการปกปิดส่วนต่อประสานความมั่นคง การดาวน์โหลดซอฟต์แวร์ การใช้คั่นหน้า และ หน้าต่างแบบผุดขึ้น มีรายละเอียดดังนี้ **1. การปกปิดหรือคลุมเครือส่วนต่อประสานความมั่นคง (Obscuring or Disabling Security User Interfaces, ObscuringSecurityUI)** ตัวแทนผู้ใช้เว็บจะต้องป้องกันส่วนต่อประสานผู้ใช้ที่แสดงสารสนเทศของบริบทความมั่นคงจากการทำให้เกิดความคลุมเครือ ถูกปกปิดหรือใช้การไม่ได้จากการควบคุมโดยเนื้อหาเว็บ เว้นแต่เป็นการตอบสนองต่อคำสั่งของผู้ใช้ โดยปฏิบัติดังนี้ - ตัวแทนผู้ใช้เว็บจะต้องจำกัดการปรับขนาดหรือการเคลื่อนย้ายหน้าต่างและส่วนต่อประสานผู้ใช้ที่ต้องปรากฏอยู่เสมอ - ตัวแทนผู้ใช้เว็บจะต้องไม่อนุญาตให้เนื้อหาเว็บเปิดหน้าต่างใหม่ที่มีการซ่อนส่วนต่อประสานด้านความมั่นคงของตัวแทนผู้ใช้ - ตัวแทนผู้ใช้เว็บจะต้องป้องกันเนื้อหาเว็บจากการซ้อนทับแทนที่ส่วนต่อประสานผู้ใช้โครม 2. **การติดตั้งซอฟต์แวร์ (Software Installation, SoftwareInstallation)** ตัวแทนผู้ใช้เว็บจะต้องไม่เปิดเผยส่วน**ต่อ**ประสานของชุดคำสั่งใดที่อนุญาตให้ติดตั้งซอฟต์แวร์โดยปราศจากการยอมรับโดยผู้ใช้และจะต้องร้องขอการอนุญาตจากผู้ใช้เมื่อตัวแทนผู้ใช้เว็บพยายามที่จะติดตั้งซอฟต์แวร์ภายนอกการควบคุมของตัวแทนผู้ใช้เว็บที่เป็นผลมาจากการควบคุมโดยเนื้อหาเว็บ โดยการมีปฏิสัมพันธ์การแจ้งเตือนที่ใช้จะต้องเป็นไปตามข้อกำหนดจากแบบรูป 64 การแจ้งเตือน อย่างไรก็ตามตัวแทนผู้ใช้ไม่ควรรองรับการเรียกใช้งานติดตั้งซอฟต์แวร์จากเนื้อหาเว็บโดยไม่ผ่านการยอมรับจากผู้ใช้ 3. **ส่วนต่อประสานโปรแกรมประยุกต์ของการคั่นหน้าเว็บ (Bookmarking APIs, BookmarkingAPIs)** การคั่นหน้า (Bookmark) ผ่านทางส่วนต่อประสานโปรแกรมประยุกต์ เช่น อีซีเอ็มเอสคริปต์ (ECMAScript API) ตัวแทนผู้ใช้เว็บจะต้องไม่ยอมให้เนื้อหาเว็บเพิ่มคั่นหน้าโดยปราศจากการอนุญาตอย่างชัดเจนจากผู้ใช้ และตัวแทนผู้ใช้เว็บจะต้องไม่อนุญาตให้เนื้อหาเว็บเพิ่ม URI ไปยังที่จัดเก็บคั่นหน้าหากURI ดังกล่าวไม่ตรงกับ URI ของหน้าเว็บที่ผู้ใช้กำลังปฏิสัมพันธ์อยู่			

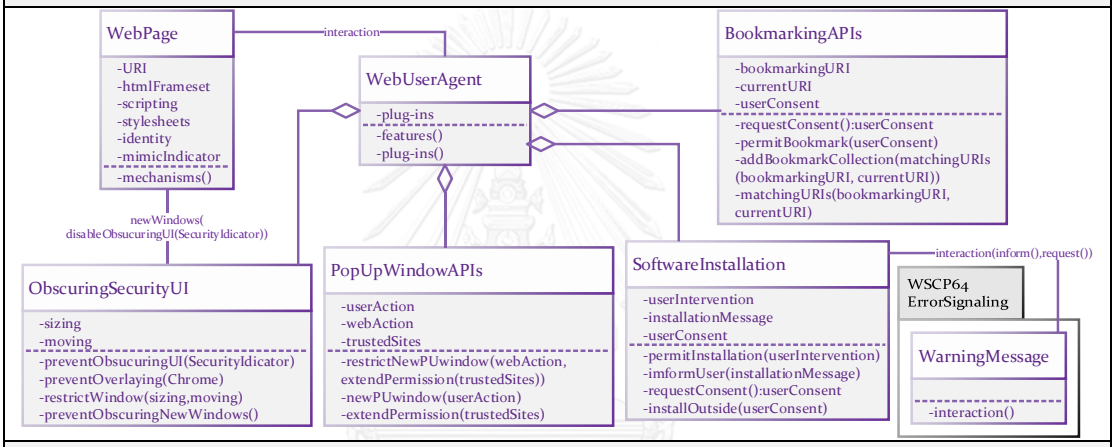
ตารางที่ ก.12 แบบรูปส่วนต่อประสานโปรแกรมประยุกต์ของตัวแทนผู้ใช้เว็บ (ต่อ)

Name	ส่วนต่อประสานโปรแกรมประยุกต์ของตัวแทนผู้ใช้เว็บที่เรียกใช้ได้โดยเนื้อหาเว็บ	ID	WSCP74

Solution

4. **ส่วนต่อประสานโปรแกรมประยุกต์ของหน้าต่างแบบผุดขึ้น** (Pop-up Window APIs, PopUp-WindowAPIs) สำหรับส่วนต่อประสานผู้ใช้ที่แสดงผลผ่านหน้าต่าง ตัวแทนผู้ใช้งานควรจะจำกัดการเปิดหน้าต่างผุดขึ้น (Pop-up Window) จากเนื้อหาเว็บ โดยเฉพาะหน้าต่างที่ไม่ได้ถูกเปิดขึ้นจากการกระทำของผู้ใช้ ทั้งนี้ตัวแทนผู้ใช้เว็บที่กำหนดให้มีความเข้มงวดดังกล่าวควรเสนอวิธีหรือตัวเลือกที่เพิ่มส่วนขยายในการเรียกขอสิทธิ์สำหรับเว็บไซต์ที่เชื่อถือได้เป็นรายไป เพื่อหลีกเลี่ยงความล้มเหลวอันเกิดจากการเข้มงวดที่จะทำให้ผู้ใช้ที่ประสงค์จะใช้งานไปยังเว็บไซต์เหล่านั้นปิดการทำงานในส่วนของการป้องกันจากเว็บอื่นทั้งหมด

Internal Structure



Example Resolved

จากกรณี 16 แฟรงค์มักจะอ่านบทความ ในขณะที่เขากำลังจิบกาแฟแก้วแรกในยามเช้า เขาคลิกไปยังลิงค์และเดินละจากคอมพิวเตอร์ไปยังเครื่องชงกาแฟเพื่อเติมกาแฟ หลังจากกลับมายังคอมพิวเตอร์ เขาพบว่าหน้าจอได้ปรากฏหน้าต่างแบบผุดขึ้นแสดงโฆษณาโปรแกรมการจัดการเช็คแบบใหม่ซึ่งเสนอโดยธนาคารที่เค้าเป็นลูกค้า พร้อมเสนอให้ดาวน์โหลดโปรแกรมทดลองไปใช้ได้ฟรี ตัวแทนผู้ใช้เว็บตรวจพบโฆษณาดังกล่าวมาจากตัวแทนฝ่ายขายมิใช่จากธนาคารโดยตรงจึงถามความสมัครใจของเขาก่อนดำเนินการต่อ

จากกรณี 20 อลิสชำระบิลของเธออาทิตย์ละครั้ง เธอเปิดตัวแทนผู้ใช้เว็บของเธอขึ้น และทำตามความเคยชินโดยการเข้าเว็บไซต์ธนาคารของเธอผ่านที่คั่นหน้าบุ๊คมาร์ค (Bookmark) กระบวนการดาวน์โหลดรอการตัดสินใจจากอลิสก่อนหน้าต่างแบบผุดขึ้นแจ้งอลิสให้ติดตั้งซอฟต์แวร์ไปยังคอมพิวเตอร์ของเธอเพื่อใช้ในการทำรายการกับธนาคารในอนาคต

Consequences

แบบรูปนี้จะป้องกันการโจมตีในส่วนต่อประสานโครมของตัวแทนผู้ใช้เว็บที่คลุมเครือจากการเคลื่อนย้ายหน้าต่างเกินไปจากขอบเขตของหน้าจอแสดงผลให้มั่นใจว่าปฏิสัมพันธ์ที่ผู้ใช้รับรู้นั้นนำไปสู่ส่วนต่อประสานโครมของตัวแทนผู้ใช้ มิใช่เปลี่ยนทิศทางไปยังเว็บประยุกต์

ตารางที่ ก.12 แบบรูปส่วนต่อประสานโปรแกรมประยุกต์ของตัวแทนผู้ใช้เว็บ (ต่อ)

Name	ส่วนต่อประสานโปรแกรมประยุกต์ของตัวแทนผู้ใช้เว็บที่เรียกใช้ได้โดยเนื้อหาเว็บ	**ID**	WSCP74
See Also			
- ส่วนต่อประสานผู้ใช้ปรากฏอยู่เสมอให้ต้องกันกับข้อกำหนดจากแบบรูป 71 - การแจ้งเตือนที่นำไปใช้จะต้องเป็นไปตามข้อกำหนดจากแบบรูป 64 - ตัวอย่างปัญหาของแบบรูปนี้อ้างถึง Case 16 และ 20 จากเอกสาร WSC-USECASES			

ตารางที่ ก.13 แบบรูปการป้องกันการโจมตีระหว่างการรักษาความมั่นคงชั้นขนส่ง

Name	การป้องกันการโจมตีระหว่างการรักษาความมั่นคงชั้นขนส่ง	**ID**	WSCP81
Core	Authentication	**Section**	Security Considerations
Description			
ข้อผิดพลาดที่เกิดขึ้นระหว่างเชื่อมต่อการรักษาความมั่นคงชั้นขนส่ง (TLS Error) จากเงื่อนไขข้อผิดพลาดที่ได้ระบุในแบบรูป 54 อาจก่อให้เกิดช่องโหว่ แบบรูปนี้พิจารณาแนวทางในการป้องกันการโจมตีโดยการสวมทับใบรับรองในระหว่างการเชื่อมต่อการรักษาความมั่นคงชั้นขนส่ง			
Example			
กรณี 11 เบ็ตตี้พยายามเชื่อมต่อไปยังเว็บไซต์ <https://www.example.com/> แต่การพัฒนาความมั่นคงชั้นขนส่งในตัวแทนผู้ใช้ของเธอตรวจพบว่าชื่อโดเมนที่ระบุไว้ในใบรับรองดังกล่าวไม่ตรงกันกับชื่อของเว็บไซต์ www.example.com			
Context			
แบบรูปนี้ประยุกต์ใช้กับตัวผู้ใช้เว็บในระหว่างการพิจารณาใบรับรองที่ใช้ในการยืนยันตัวจริงเชื่อมต่อการรักษาความมั่นคงชั้นขนส่ง			
Problem			
จากแบบรูป 54 ข้อผิดพลาดระหว่างการเชื่อมต่อการรักษาความมั่นคงชั้นขนส่ง (TLS errors) ที่นำไปสู่โอกาสเสี่ยงภัยอื่นๆ เช่นการโจมตีในสถานการณ์ ดังนี้ **การส่งสัญญาณเตือนภัยอย่างอ่อนแก่ผู้ใช้ (Weak Warning Signals)** ขณะปฏิสัมพันธ์กับเว็บไซต์ครั้งแรกแม้เว็บไซต์ดังกล่าวจะมีการทวนสอบหรือใช้ส่วนขยายในการทวนสอบใบรับรองแล้วก็ตาม ผู้โจมตีสามารถแสดงใบรับรองที่ลงนามโดยตนเอง ตัวแทนผู้ใช้เว็บทั่วไปจะปฏิบัติต่อเหตุการณ์เช่นนี้ด้วยกล่องโต้ตอบที่ขัดขวางกระแสงานของผู้ใช้แต่ผู้ใช้มักกดข้ามข้อความ **การปักหมุดของใบรับรองใหม่ไปยังปลายทาง (Pinning)** อาจเป็นการโจมตีเบื้องต้นโดยการหลอก (Spoofing) หรืออาจแทนที่ด้วยใบรับรองที่ลงนามโดยตนเอง (SSC) ที่ใหม่กว่า			

ตารางที่ ก.13 แบบรูปการป้องกันการโจมตีระหว่างการรักษาความมั่นคงชั้นขนส่ง (ต่อ)

Name	การป้องกันการโจมตีระหว่างการรักษาความมั่นคงชั้นขนส่ง	ID	WSCP81

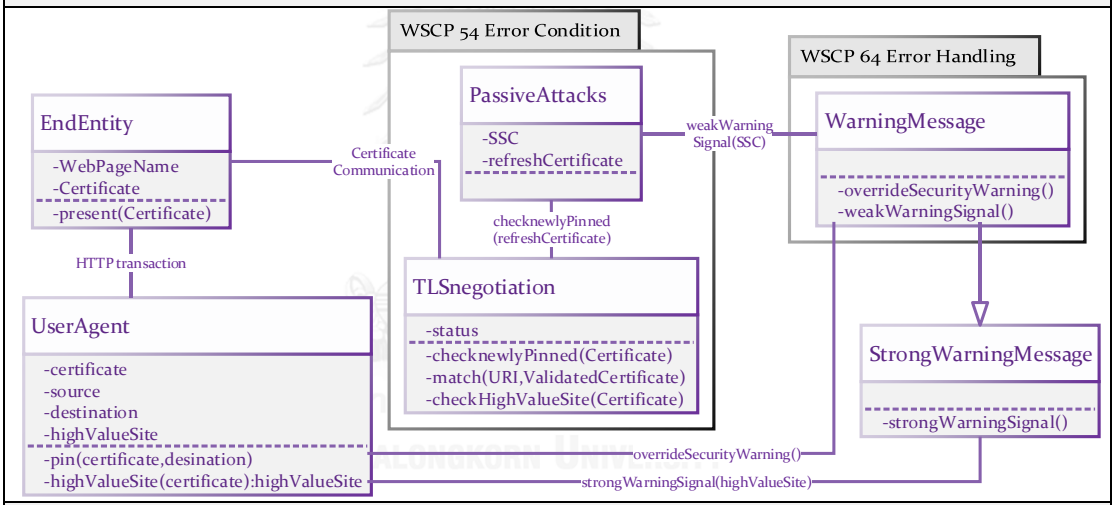
Solution

การรับมือกับภัยคุกคามจากการส่งสัญญาณเตือนภัยอย่างอ่อนให้ผู้ใช้โดยการกำหนดมูลค่าของเว็บไซต์ ดังนี้

เว็บไซต์ที่มีมูลค่าสูง (High-Value Site) เพื่อคัดกรองเว็บไซต์ที่มีมูลค่าสูงซึ่งจะต้องแสดงใบรับรองที่ผ่านการตรวจสอบความสมเหตุสมผลหรือใบรับรองที่ได้รับประกันเสริม เพื่อให้เกิดการส่งสัญญาณแจ้งเตือนที่แข็งแกร่ง (Strong warning signal) โดยการสื่อสารของใบรับรองและการรักษาความมั่นคงชั้นขนส่งโดยกลไกควรแยกออกจากโปรโตคอล (HTTP) เช่น จากบันทึกการยืนยันตัวตนผ่าน DNS

เว็บไซต์ที่มีมูลค่าต่ำ (Low-Value-Site) ใช้ใบรับรองที่ลงนามโดยตนเอง (SSC) ต้องตรวจสอบการแทนที่ด้วยใบรับรองที่ใหม่กว่าเมื่อมีการปักหมุดของใบรับรองใหม่ไปยังปลายทางเพื่อเพื่อป้องกันการสวมทับใบรับรอง การโจมตีโดยการหลอก หรืออาจแทนที่ด้วยใบรับรองที่ลงนามโดยตนเองที่ใหม่กว่า เพื่อให้เกิดการส่งสัญญาณแจ้งเตือนที่แข็งแกร่ง

Internal Structure



Example Resolved

จากกรณี 11 เบ็ตตี้พยายามเชื่อมต่อไปยังเว็บไซต์ <https://www.example.com/> การพัฒนาความมั่นคงชั้นขนส่งในตัวแทนผู้ใช้ของเธอตรวจพบว่าชื่อโดเมนที่ระบุไว้ในใบรับรองดังกล่าวไม่ตรงกันกับชื่อของเว็บไซต์ www.example.com เมื่อพบข้อผิดพลาดดังกล่าวการกำหนดมูลค่าของใบรับรองที่น่าเชื่อถือจากเว็บไซต์จะส่งผลต่อความเข้มแข็งของการแจ้งเตือน สำหรับใบรับรองที่ลงนามด้วยตนเองการปักหมุดต้องถูกระงับเพื่อป้องกันการทับซ้อนหรือสวมใบรับรอง

Consequences

การพิจารณาการโจมที่อาจเกิดขึ้นระหว่างการเชื่อมต่อการรักษาความมั่นคงขั้นขนส่งจะช่วยป้องกันระบบจากการโจมตีได้ และปิดช่องโหว่ในการสับเปลี่ยนใบรับรองหลังการทวนสอบอันเป็นการให้ข้อมูลเท็จของผู้ให้บริการ

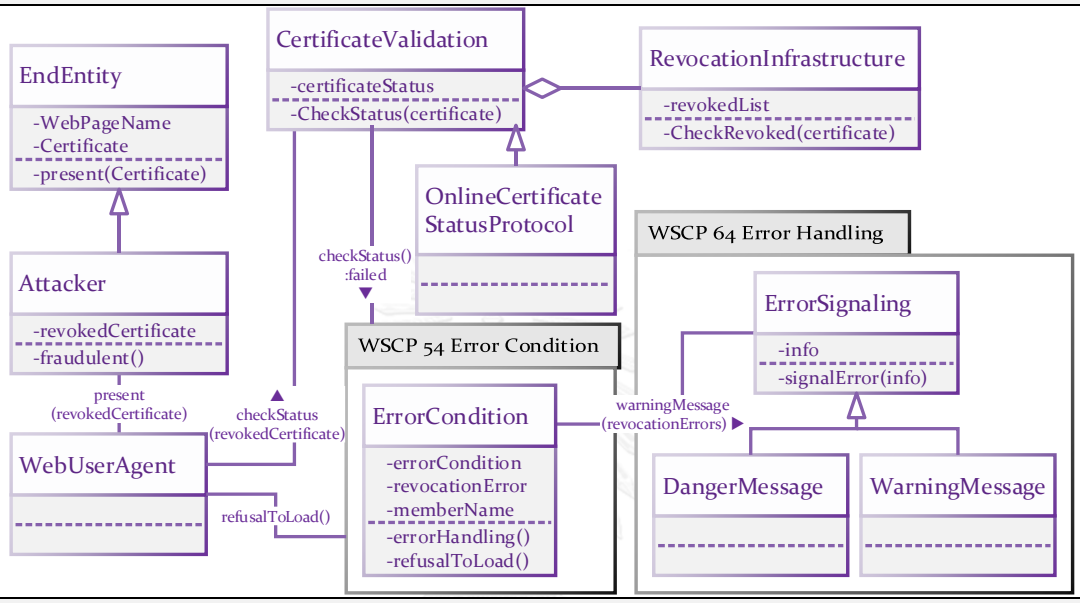
ตารางที่ ก.13 แบบรูปการป้องกันการโจมตีระหว่างการรักษาความมั่นคงชั้นขนส่ง (ต่อ)

Name	การป้องกันการโจมตีระหว่างการรักษาความมั่นคงชั้นขนส่ง	**ID**	WSCP81
See Also			
- ศึกษาการปักหมุดใบรับรอง (Pinning) ได้จากแบบรูป 51 - ศึกษาข้อผิดพลาดระหว่างการเชื่อมต่อการรักษาความมั่นคงขั้นขนส่ง (TLS errors) ได้จากแบบรูป 54 - ศึกษาการจัดการข้อผิดพลาด (Error Handling) ได้จากแบบรูป 64 - ตัวอย่างปัญหาของแบบรูปนี้อ้างถึง Case 11 จากเอกสาร WSC-USECASES			

ตารางที่ ก.14 แบบรูปความล้มเหลวในการตรวจสอบสถานะใบรับรอง

Name	ความล้มเหลวในการตรวจสอบสถานะใบรับรอง	**ID**	WSCP82
Core	Authentication	**Section**	Security Considerations
Description			
แบบรูปนี้กล่าวถึงช่องโหว่และแนวทางในการป้องกันตัวแทนผู้ใช้เว็บที่ล้มเหลวในการตรวจสอบสถานะใบรับรองผู้ให้บริการเว็บจากโครงข่าย เนื่องจากใบรับรองดังกล่าวถูกเพิกถอน ที่อยู่นอกเหนือจากข้อผิดพลาดระหว่างการเชื่อมต่อการรักษาความมั่นคงขั้นขนส่งที่ระบุในแบบรูป 54			
Example			
ดัดแปลงกรณี 8 เบ็ตตี้เยี่ยมชมเว็บไซต์ example.com เป็นบางครั้ง ในแต่ละครั้งที่เชื่อมต่อ ตัวแทนผู้ใช้เว็บของเธอจะได้รับใบรับรองของผู้ให้บริการในการรักษาความมั่นคงชั้นขนส่งจากองค์กรผู้ออกใบรับรองเดียวกัน ในการเชื่อมต่อครั้งนี้ ใบรับรองที่ได้รับถูกเพิกถอนโดยองค์กรผู้ออกใบรับรองอื่น			
Context			
เมื่อตัวแทนผู้ใช้เว็บเกิดความล้มเหลวในการตรวจสอบสถานะของใบรับรองระหว่างการเชื่อมต่อการรักษาความมั่นคงขั้นขนส่ง โดยใช้วิธีระงับข้อผิดพลาดของการเพิกถอนใบรับรองโดยตัวแทนผู้ใช้เว็บ			
Problem			
ในการตรวจสอบสถานะของใบรับรองออนไลน์ (Online Certificate Status Protocol: OCSP) ยังเปราะบางและอาจเกิดความล้มเหลวบ่อยครั้ง จึงไม่เหมาะสมอย่างยิ่งที่จะร้องขอให้ตัวแทนผู้ใช้เว็บปฏิบัติต่อความล้มเหลวดังกล่าวในลักษณะการแจ้งเตือนหรือข้อผิดพลาด แต่หากหลีกเลี่ยงการปฏิบัติต่อความล้มเหลวก็จะก่อให้เกิดโอกาสในการโจมตี เว็บไซต์ที่ใช้ใบรับรองที่หลอกลวงหรือถูกเพิกถอนอาจพยายามโจมตีโครงสร้างพื้นฐานการเพิกถอนใบรับรอง (Revocation Infrastructure, **RevocationInfrastructure**) ของผู้มีอำนาจอนุมัติใบรับรอง			
Solution			
ตัวแทนผู้ใช้เว็บมีมาตรการตอบโต้ต่อจุดอ่อน (Vulnerability) โดยการแสดงรายละเอียดความล้มเหลว (Exposing Failures) ของการตรวจสอบความถูกต้องของใบรับรอง (Certificate Validation) ให้แก่ผู้ใช้โดยการส่งข้อความคำนึงถึงความเหมาะสมของการร้องขอให้ตัวแทนผู้ใช้เว็บปฏิบัติต่อความล้มเหลวดังกล่าวในลักษณะ			

ตารางที่ ก.14 แบบรูปความล้มเหลวในการตรวจสอบสถานะใบรับรอง (ต่อ)

Name	ความล้มเหลวในการตรวจสอบสถานะใบรับรอง	ID	WSCP82
Solution			
การแจ้งเตือน (Warning Message) การเตือนภัย (Danger Message) ไปจนถึงการปฏิเสธที่จะโหลดข้อมูล (Refusal) จากเว็บไซต์ที่ล้มเหลวในการตรวจสอบ			
Internal Structure			
			
Example Resolved			
ดัดแปลงจากกรณี 8 เบ็ตตี้เยี่ยมชมเว็บไซต์ example.com เป็นบางครั้ง ในแต่ละครั้งที่เชื่อมต่อ ตัวแทนผู้ใช้เว็บของเธอจะได้รับใบรับรองของผู้ให้บริการในการรักษาความมั่นคงชั้นขนส่งจากองค์กรผู้ออกใบรับรอง ในการเชื่อมต่อครั้งนี้ ใบรับรองที่ได้รับถูกเพิกถอนโดยองค์กรผู้ออกใบรับรอง ตัวแทนผู้ใช้เว็บจะต้องส่งข้อความเหตุผลในการเพิกถอนในระดับเตือนภัยของการเพิกถอนใบรับรองดังกล่าว			
Consequences			
การพิจารณาข้อผิดพลาดที่เกิดจากการตรวจสอบใบรับรองอันมีสาเหตุจากการโจมตีช่วยในป้องกันจุดอ่อนของระบบจากผู้โจมตีที่ใช้ใบรับรองที่ถูกเพิกถอนในการเชื่อมต่อ			
See Also			
- ศึกษาข้อผิดพลาดระหว่างการเชื่อมต่อการรักษาความมั่นคงขั้นขนส่งได้จากแบบรูป 54 - ตัวอย่างปัญหาของแบบรูปนี้อ้างถึง Case 8 จากเอกสาร WSC-USECASES			

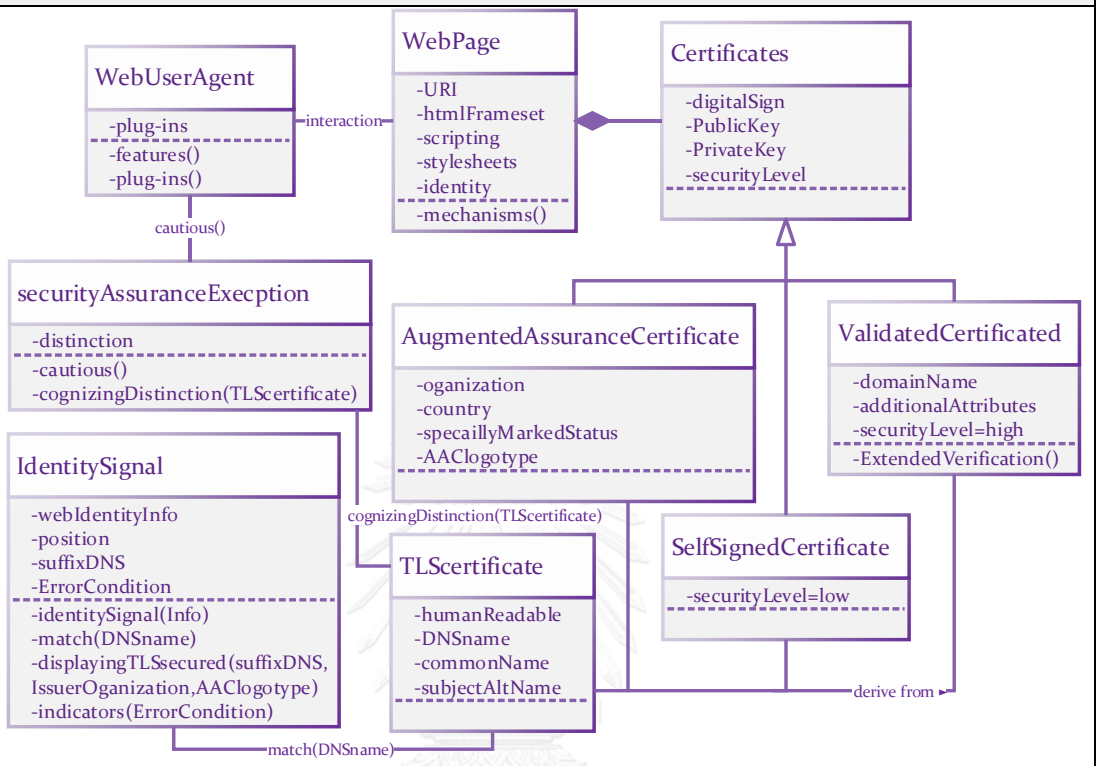
ตารางที่ ก.15 แบบรูปข้อพึงระวังในการพิจารณาใบรับรองที่น่าเชื่อถือ

Name	ข้อพึงระวังในการพิจารณาใบรับรองที่น่าเชื่อถือ	**ID**	WSCP83
Core	Availability	**Section**	Security Considerations
Description			
เว็บไซต์ที่แสดงใบรับรองที่น่าเชื่อถือมักถูกอนุญาตให้เนื้อหาของเว็บดังกล่าวเข้าถึงทรัพยากรของผู้ใช้ จนอาจก่อให้เกิดความละหลวมในการป้องกัน หากเกิดช่องโหว่ก็อาจก่อให้เกิดความเสียหายแก่ระบบได้ แบบรูปนี้จึงอธิบายข้อพึงระวังในการพิจารณาข้อมูลจากใบรับรองโดยเฉพาะอย่างยิ่งใบรับรองที่ได้ถูกพิจารณาว่ามีความน่าเชื่อถือ อย่างไรก็ตามการแสดงสถานะของเว็บจากข้อมูลใบรับรองดังกล่าว ยืนยันได้เพียงอัตลักษณ์และผู้ถือครองของเว็บ ไม่ควรนำมาตัดสินสถานะด้านความมั่นคง			
Example			
เสริมจากกรณี 12 เบ็ตตี้เยี่ยมชมหน้าเว็บที่ <https://www.example.com/> หน้าเว็บ HTML ที่ได้รับปรากฏเนื้อหาที่ได้รับจาก <http://www.example.com/> รวมอยู่ด้วย กล่าวคือเนื้อหาที่ได้รับมีบริบทความมั่นคงที่ต่างกัน ตัวแทนผู้ใช้เว็บนำเสนอสถานะความมั่นคงที่ได้จาก <https://www.example.com/> แล้วสรุปได้ว่าเว็บดังกล่าวน่าเชื่อถือ ในขณะที่เนื้อหาบางส่งของเว็บไม่ผ่านรักษาความมั่นคงชั้นขนส่ง			
Context			
บริบทการนำแบบรูปนี้ไปประยุกต์ใช้เมื่อตัวแทนผู้ใช้เว็บใช้ข้อมูลใบรับรองจากเว็บในการพิจารณาบริบทความมั่นคงเพื่อแสดงสถานะของการเชื่อมต่อการรักษาความมั่นคงชั้นขนส่ง (SSL/TLS)			
Problem			
ใบรับรองที่ผ่านการตรวจสอบความสมเหตุสมผลและใบรับรองที่ได้รับประกันเสริม ข้อมูลดังกล่าวยืนยันได้เพียงว่าได้มีการทวนสอบอัตลักษณ์ของผู้ถือครองบางระดับเท่านั้น แต่ไม่ได้กล่าวถึงการรับประกันว่าเว็บไซต์ดังกล่าวได้กระทำการในลักษณะที่ปลอดภัย หรือปราศจากการโจมตีหรือไม่			
Solution			
ใบรับรองที่รักษาความมั่นคงชั้นขนส่ง (**TLScertificate**) ทุกชนิด (เช่น ใบรับรองที่ลงนามโดยตนเอง ใบรับรองที่ผ่านการตรวจสอบความสมเหตุสมผล หรือ ใบรับรองที่ได้รับประกันเสริม) แม้มีการเข้ารหัสการสื่อสารอย่างแข็งแกร่ง แต่ต้องไม่ถูกเข้าใจหรือปฏิบัติกับใบรับรองดังเสมือนข้อมูลถูกห่อหุ้มด้วยการประกันความมั่นคง แนวปฏิบัติพิจารณาจากข้อมูลความมั่นคงและอัตลักษณ์จะถูกสรุปรวมคร่าวๆ โดยตัวแทนผู้ใช้เว็บซึ่งแสดงสถานะของการเชื่อมต่อการรักษาความมั่นคงชั้นขนส่ง (SSL/TLS) ว่า "ปลอดภัย" ข้อกำหนดนี้แนะนำให้ผู้พัฒนาระวังและจัดการกับความแตกต่างดังกล่าว (**SecurityAssuranceException**) โดยการจำแนกลักษณะความแตกต่างระหว่างเนื้อหาที่ถูกเข้ารหัสความมั่นคงและเนื้อหาทั่วไป เมื่อพบความแตกต่างดังกล่าวการแจ้งระดับความปลอดภัยให้แก่ผู้ใช้ไม่ควรสรุปรวมว่าเว็บดังกล่าวปลอดภัย			

ตารางที่ ก.15 แบบรูปข้อพึงระวังในการพิจารณาใบรับรองที่น่าเชื่อถือ (ต่อ)

Name	ข้อพึงระวังในการพิจารณาใบรับรองที่น่าเชื่อถือ	ID	WSCP83

Internal Structure



Example Resolved

เสริมจากกรณี 12 เบ็ตตี้เยี่ยมชมหน้าเว็บที่ <https://www.example.com/> หน้าเว็บ HTML ที่ได้รับปรากฏเนื้อหาที่ได้รับจาก <http://www.example.com/> รวมอยู่ด้วย กล่าวคือเนื้อหาที่ได้รับมีบริบทความมั่นคงที่ต่างกัน ตัวแทนผู้ใช้เว็บนำเสนอสถานะความมั่นคงที่ได้จาก <http://www.example.com/> แทนที่จะแสดงจากแหล่งที่มีความน่าเชื่อถือสูง

Consequences

แบบรูปนี้จะช่วยให้ผู้ใช้ออกแบบการนำเสนอบริบทความมั่นคงของเว็บที่ใช้ข้อมูลจากใบรับรองได้อย่างรัดกุม

See Also

- ศึกษาข้อมูลใบรับรอง (Certificates) ได้จากแบบรูป 52
- ศึกษาการส่งสัญญาณอัตลักษณ์ (Identity Signal) ได้จากแบบรูป 61
- ตัวอย่างปัญหาของแบบรูปนี้อ้างถึง Case 12 จากเอกสาร WSC-USECASES

ตารางที่ ก.16 แบบรูปการใช้ชื่อภาษาธรรมชาติรวมอยู่ในชื่อโดเมน

Name	การใช้ชื่อภาษาธรรมชาติรวมอยู่ในชื่อโดเมน	ID	WSCP84
Core	Availability	Section	Security Considerations

Description

แบบรูปนี้อธิบายข้อควรระวังในการแสดงชื่อโดเมนของเว็บให้แก่ผู้ใช้ เนื่องจากเว็บไซต์อาจมีจุดประสงค์ในการสวมรอยใช้ชื่อโดเมนที่ใกล้เคียงกับชื่อที่ผู้ใช้คุ้นเคย ทำให้ผู้ใช้เข้าใจผิดและเชื่อว่ากำลังติดต่ออยู่กับผู้ให้บริการที่ผู้ใช้คุ้นเคย แบบรูปนี้จึงนำเสนอการเลือกข้อมูลเพื่อให้ผู้ใช้ให้ทราบถึงอัตลักษณ์ของผู้ถือครองเว็บ

Example

กรณี 9 เบ็ตตี้คลิกไปยังลิงค์ที่เชื่อมโยงสู่หน้าเว็บ <https://www.example.com/> หน้าเว็บที่ได้รับประกอบด้วยเนื้อหาที่ได้รับจาก <https://www.example.net/> ตัวแทนผู้ใช้เว็บของเบ็ตตี้ไม่พบความสัมพันธ์ใดๆ ระหว่างเว็บไซต์ www.example.com และ www.example.net

Context

แบบรูปนี้จะถูกนำไปประยุกต์ใช้กับตัวแทนผู้ใช้เว็บที่แสดงข้อมูลอัตลักษณ์ของเว็บ

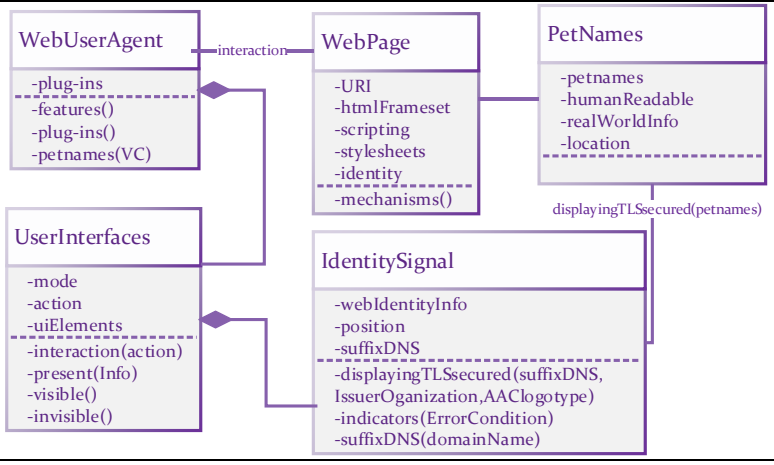
Problem

เมื่อผู้ใช้ต้องการข้อมูลที่สอดคล้องกับความจริงหรือข้อมูลที่ผู้ใช้คุ้นเคย ในกรณีที่ใบรับรองที่ได้รับประกันเสริมข้อมูลอัตลักษณ์ที่มีให้อาจถูกพิจารณาว่าเพียงพอต่อวัตถุประสงค์นี้ แต่ใบรับรองที่ผ่านการตรวจสอบความสมเหตุสมผลไม่สามารถยืนยันได้ว่าข้อมูลอัตลักษณ์ที่ให้นั้นสอดคล้องกับข้อมูลที่ผู้ใช้ได้รับในโลกความจริง

Solution

การที่ผู้ใช้จะระลึกถึงตัวจริงของผู้ถือครองเว็บที่ผู้ใช้คุ้นเคยได้ จำเป็นต้องมีข้อมูลที่สอดคล้องกับโลกความจริงที่ผู้ใช้รับรู้ (Human Readable) โดยใบรับรองที่ได้รับประกันเสริม (Augmented Assurance Certificate) นั้นมีข้อมูลที่เพียงพอ แต่ใบรับรองที่ผ่านการตรวจสอบความสมเหตุสมผล (Validated Certificate) อื่นๆ อาจไม่มีข้อมูลดังกล่าว ตัวแทนผู้ใช้เว็บที่ประสงค์จะให้มีกลไกที่ผู้ใช้สามารถสร้างการเชื่อมโยงข้อมูลที่ผู้ใช้รับรู้จากโลกความจริงกับข้อมูลอัตลักษณ์ด้วยตนเอง ให้พิจารณาวิธีการตั้งชื่อที่ชื่นชอบ (Petnames, **PetNames**) (ดูเพิ่มเติมที่ [PETNAMES]) เพื่อนิยามความสัมพันธ์หรือให้คำจำกัดความของเว็บไซต์ใดๆ

Internal Structure



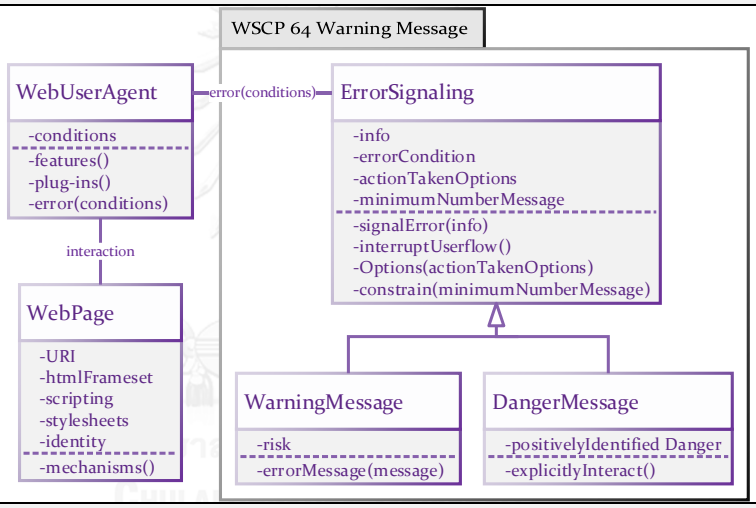
ตารางที่ ก.16 แบบรูปการใช้ชื่อภาษาธรรมชาติรวมอยู่ในชื่อโดเมน (ต่อ)

Name	การใช้ชื่อภาษาธรรมชาติรวมอยู่ในชื่อโดเมน	**ID**	WSCP84
Example Resolved			
จากกรณี 9 เบ็ตตี้คลิกไปยังลิงค์ที่เชื่อมโยงสู่หน้าเว็บ <https://www.example.com/> หน้าเว็บที่ได้รับประกอบด้วยเนื้อหาที่ได้รับจาก <https://www.example.net/> ตัวแทนผู้ใช้เว็บของเบ็ตตี้ให้ข้อมูลของ example.com ที่นอกเหนือจากการแสดงใบรับรองที่ผ่านการตรวจสอบความสมเหตุสมผลแต่ยังเป็น Example Inc. จากประเทศนอร์เวย์ ซึ่งผู้ใช้คาดหวังที่จะติดต่อด้วย			
Consequences			
ข้อมูลดังกล่าวจะเป็นประโยชน์ในการช่วยเหลือผู้ใช้ให้เข้าถึงเว็บไซต์ที่ผู้ใช้ระลึกถึงโดยคำนึงถึงข้อควรระวังหากเว็บดังกล่าวเป็นการลอกเลียน			
See Also			
- แบบรูป 61 เนื้อหาที่ใช้ในการส่งสัญญาณอัตลักษณ์ - เอกสารภายนอก PetNames (http://www.hpl.hp.com/techreports/2005/HPL-2005-148.html) โดยเฮ็ชพีแลป (HP Lab) - ตัวอย่างปัญหาของแบบรูปนี้อ้างถึง Case 9 จากเอกสาร WSC-USECASES			

ตารางที่ ก.17 แบบรูปการป้องกันความล้าของผู้ใช้ต่อการแจ้งเตือน

Name	การป้องกันความล้าของผู้ใช้ต่อการแจ้งเตือน	**ID**	WSCP85
Core	Accountability	**Section**	Security Considerations
Description			
แบบรูปนี้ส่งเสริมประสิทธิภาพของการแจ้งเตือนเพิ่มเติมจากความต้องการที่ระบุในแบบรูป 64 เกี่ยวข้องกับข้อความแจ้งเตือน เมื่อมีเหตุอันควรเป็นไปตามเงื่อนไขของตัวแทนผู้ใช้เว็บ			
Example			
กรณี 13 เบ็ตตี้มีความเคยชินในการกดปิดอย่างรวดเร็วเมื่อตัวแทนผู้ใช้แสดงกล่องข้อความแจ้งเตือนเช่นเดียวกับผู้ใช้ท่านอื่นๆ จากพฤติกรรมดังกล่าวเบ็ตตี้ได้ละเลยการแจ้งเตือน จนทำให้เธอเข้าสู่หน้าเว็บที่ต้องสงสัยอย่างไม่ทันรู้ตัว			
Context			
ตัวแทนผู้ใช้ที่มีการส่งสัญญาณข้อผิดพลาดโดยการใช้ข้อความแจ้งเตือนหรือข้อความเตือนภัย			
Problem			
ข้อสำคัญที่พึงระวังเมื่อพัฒนาส่วนต่อประสานผู้ใช้ที่จะทำให้ผู้ใช้เคยชินกับการแจ้งเตือนที่บ่อยเกินไปจนละเลยการแจ้งเตือนสำคัญ ทำให้เกิดผลกระทบของการแสดงข้อความและความสามารถที่จะขัดขวางกระแสการทำงานของผู้ใช้ได้อย่างมีประสิทธิผลต่ำลง			

ตารางที่ ก.17 แบบรูปการป้องกันความล้าของผู้ใช้ต่อการแจ้งเตือน (ต่อ)

Name	การป้องกันความล้าของผู้ใช้ต่อการแจ้งเตือน	ID	WSCP85
Problem			
ข้อสำคัญที่พึงระวังเมื่อพัฒนาส่วนต่อประสานผู้ใช้ที่จะทำให้ผู้ใช้เคยชินกับการแจ้งเตือนที่บ่อยเกินไปจนละเลยการแจ้งเตือนสำคัญ ทำให้เกิดผลกระทบของการแสดงข้อความและความสามารถที่จะขัดขวางกระแสการทำงานของผู้ใช้ได้อย่างมีประสิทธิผลต่ำลง			
Solution			
เพื่อให้การแจ้งเตือนที่มีประสิทธิภาพ การดึงดูดความสนใจหรือขัดขวางผู้ใช้จนเกินไปทำให้ผู้ใช้ไม่เห็นความสำคัญและละเลยการแจ้งเตือน ดังนั้น ตัวแทนผู้ใช้เว็บจะถูกแนะนำให้จำกัดจำนวนของการแจ้งเตือนและการแสดงข้อผิดพลาดให้อยู่ในปริมาณที่น้อยที่สุดเพื่อให้เหมาะสมกับคำแนะนำด้านความมั่นคงอื่นๆทั้งยังแนะนำให้ตัวแทนผู้ใช้เว็บใช้ประโยคที่สื่อถือการกระทำต่อการแจ้งเตือนนั้นของตัวเลือก			
Internal Structure			
			
Example Resolved			
จากกรณี 13 เมื่อจำนวนข้อความการแจ้งเตือนลดลง เบ็ตตี้สามารถพิจารณาข้อความการแจ้งเตือนที่จำเป็นและมีความสำคัญเท่านั้น จึงไม่ละเลยการแจ้งเตือนทำให้เธอหลีกเลี่ยงเข้าสู่หน้าเว็บที่ต้องสังสัยอย่างไม่ทันรู้ตัว			
Known Uses			
ประโยคที่สื่อถือการกระทำต่อการแจ้งเตือนนั้นของตัวเลือก (เช่น "ละเลยการแจ้งเตือน" "ไว้ใจเว็บไซต์นี้") มากกว่าการใช้เพียงป้ายทั่วไป (เช่น "ตกลง" "ยกเลิก")			
Consequences			
จำนวนการแสดงข้อความการแจ้งเตือนที่เหมาะสม จะทำให้ผู้ใช้ไม่เบื่อหน่ายหรือละเลยการแจ้งเตือนที่สำคัญ			
See Also			
- ศึกษาการแจ้งเตือนได้จาก แบบรูป 64 ข้อความแจ้งเตือน/ข้อความเตือนภัย - ตัวอย่างปัญหาของแบบรูปนี้อ้างถึง Case 13 จากเอกสาร WSC-USECASES			

ตารางที่ ก.18 แบบรูปการรับมือเมื่อเกิดการเปลี่ยนแปลงเนื้อหาระหว่างการเชื่อมต่อด้วยใบรับรองที่ได้รับประกันเสริม

Name	การรับมือเมื่อเกิดการเปลี่ยนแปลงเนื้อหาระหว่างการเชื่อมต่อด้วยใบรับรองที่ได้รับประกันเสริม	**ID**	WSCP86
Core	Authorization	**Section**	Security Considerations
Description			
แบบรูปนี้อธิบายถึงข้อควรระวังเมื่อผู้ให้บริการเว็บ (Web Server) ได้แสดงใบรับรองที่ได้รับประกันเสริม (Augmented Assurance Certificate: AAC) แล้วมีการแสดงเนื้อหาบางส่วนจากผู้ให้บริการเว็บที่ถือครองใบรับรองที่ผ่านการตรวจสอบความสมเหตุสมผล (Validated Certificate: VC) เนื่องจากใบรับรองที่กล่าวมานั้นมีระดับความมั่นคงต่างกัน (TLS-Protected) เพื่อไม่ให้เกิดความสับสนในการนำข้อมูลที่ได้จากใบรับรองที่ได้รับประกันเสริม (AAC) ไปใช้เป็นใบเบิกทางเพื่อให้ตัวแทนผู้ใช้ตัดสินว่าหน้าเว็บดังกล่าวมีปกป้องข้อมูลด้วยการรักษาความมั่นคงชั้นขนส่งอย่างแข็งแกร่ง (Strongly TLS-protected) แล้วแสดงข้อมูลจากแหล่งผู้ให้บริการเว็บอื่นในภายหลัง ดังนั้น การแสดงสัญญาณอัตลักษณ์ (Identity Signaling) โดยตัวแทนผู้ใช้เว็บ (Web User Agent) ต้องแสดงเพียงองค์ผู้อนุมัติใบรับรอง (CA) ที่รับผิดชอบโดยตรงต่อทรัพยากรระดับบน (Top-level Resource) ของหน้าเว็บเท่านั้น		
Example			
กรณี 12 เบ็ตตี้เยี่ยมชมหน้าเว็บที่ <https://www.example.com/> หน้าเว็บ HTML ที่ได้รับปรากฏเนื้อหาที่ได้รับจาก <http://www.example.com/> รวมอยู่ด้วย กล่าวคือเนื้อหาที่ได้รับมีบริบทความมั่นคงที่ต่างกัน ตัวแทนผู้ใช้เว็บจะต้องแสดงสถานะผ่านตัวชี้บอกความมั่นคงชั้นขนส่งอย่างไร			
Context			
แบบรูปนี้นำไปประยุกต์ใช้กับตัวแทนผู้ใช้เว็บที่แสดงสถานการณ์รักษาความมั่นคงชั้นขนส่ง (TLS Indicator) ในกรณีที่หน้าเว็บแรกถูกค้นคืนด้วยใบรับรองที่ได้รับประกันเสริม (AAC) ได้ถูกใช้ในระหว่างการเชื่อมต่อการรักษาความมั่นคงของชั้นขนส่ง (TLS session) ขณะที่หน้าเว็บที่สองถูกค้นคืนโดยใช้ใบรับรองอื่น			
Problem			
เมื่อตัวแทนผู้ใช้เว็บได้โหลดหน้าเว็บจำนวน 2 หน้า จาก "https://www.example.com/" แล้วหน้าเว็บแรกถูกค้นคืนโดยใช้ใบรับรองที่ได้รับประกันเสริม (AAC) ในระหว่างการเชื่อมต่อการรักษาความมั่นคงชั้นขนส่ง (TLS session) และหน้าเว็บที่สองถูกค้นคืนโดยใช้ใบรับรองอื่น แม้หน้าเว็บแรกจะถูกค้นคืนผ่านการรักษาความมั่นคงชั้นขนส่งอย่างแข็งแกร่ง (Strongly TLS-protected) แต่หน้าเว็บที่สองสามารถอ่านและเขียนหน้าเว็บแรกได้อย่างอิสระ ดังนั้น หากมีการใช้เนื้อหาจากองค์กร (CA) อื่นๆ จะทำให้ความน่าเชื่อถือของเอกสารหลักอยู่เหนือกว่าระดับความมั่นคงขององค์กรที่มีส่วนเกี่ยวข้องทั้งที่สามารถอ่านและแก้ไขสถานะของกันและกันได้โดยอิสระ เปิดโอกาสให้เกิดการโจมตีเบื้องต้นต่อบริการ อีกทั้งการแสดงสถานะดังกล่าวมักจะไม่เปลี่ยนแปลงหลังจากโหลดเนื้อหาจากหน้าเว็บเสร็จสมบูรณ์ทำให้เกิดช่องโหว่ในการโจมตีคุณสมบัติด้านความมั่นคง (Security Properties) ของหน้าเว็บแบบพลวัตร (Dynamic) ภายใต้การควบคุมของสคริปต์ได้			

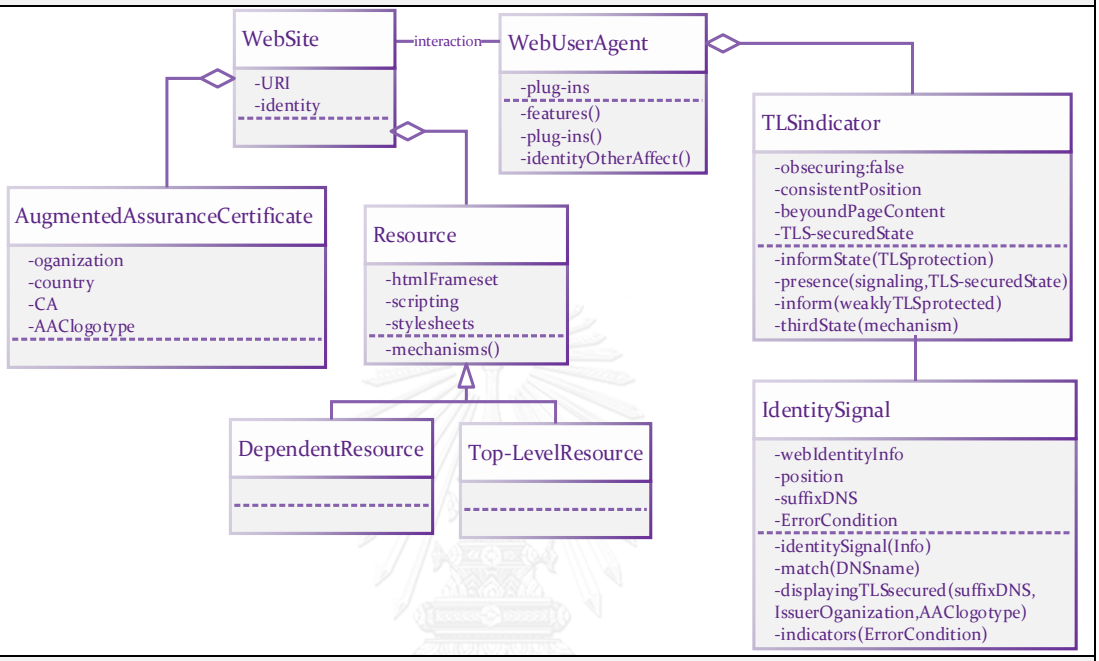
ตารางที่ ก.18 แบบรูปการรับมือเมื่อเกิดการเปลี่ยนแปลงเนื้อหาระหว่างการเชื่อมต่อด้วยใบรับรองที่ได้รับประกันเสริม (ต่อ)

Name	การรับมือเมื่อเกิดการเปลี่ยนแปลงเนื้อหาระหว่างการเชื่อมต่อด้วยใบรับรองที่ได้รับประกันเสริม	**ID**	WSCP86
Solution			
เมื่อตัวแทนผู้ใช้ตัดสินว่าหน้าเว็บใดๆ มีการปกป้องข้อมูลด้วยการรักษาความมั่นคงชั้นขนส่งอย่างแข็งแกร่ง (Strongly TLS-protected) แล้วอาจเกิดการเปลี่ยนแปลงได้ 2 กรณี คือ การค้นคืนทรัพยากรจากแหล่งอื่น และการเปลี่ยนแปลงคุณสมบัติด้านความมั่นคงของหน้าเว็บแบบพลวัตร มีรายละเอียด ดังนี้ 1. **การค้นคืนทรัพยากรจากแหล่งอื่น** (Mixing Augmented Assurance and Validated Certificates) ตัวแทนผู้ใช้เว็บค้นคืนทรัพยากร (Resource, **Resource**) ที่ควบคุมเนื้อหาของหน้าเว็บ เช่น สคริปต์จากภายนอก (External script) การตกแต่งหน้าเว็บ (Styling) กรอบเนื้อหาเว็บ (Layout) รวมถึงปลั๊กอินส์ (Plug-ins) ที่สามารถเปลี่ยนแปลงการแสดงผลของทั้งเอกสาร ซึ่งแหล่งของทรัพยากร แบ่งได้ 2 ระดับ คือ ทรัพยากรระดับบน (Top-Level Resource, **Top-LevelResource**) และทรัพยากรพึ่งพิง (Dependent Resource, **Dependent-Resource**) โดยทรัพยากรระดับบนรับรองเนื้อหาจากทรัพยากรที่พึ่งพิงทั้งหมดในการพิสูจน์ตัวจริงโดยการใช้ URIs และโดเมนจากผู้มีอนุมัติใบรับรอง (CA) ในขณะที่ทรัพยากรพึ่งพิงอยู่ภายใต้การควบคุมของทรัพยากรระดับบน หากทรัพยากรพึ่งพิงบนมีการปกป้องด้วยความมั่นคงชั้นขนส่งอย่างแข็งแกร่ง (Strongly TLS-protected) แต่ไม่ได้ถือครองใบรับรองที่ได้รับประกันเสริม (AAC) แล้วทรัพยากรที่พึ่งพิงจะต้องแสดงใบรับรองที่ถูกต้อง (VC) และเอกสารส่วนนั้นจะไม่สามารถระบุได้ว่าเป็นขอบเขตเดียวกันกับเอกสารหลัก ตัวแทนผู้ใช้เว็บควรแสดงสัญญาณอัตลักษณ์ (Identity Signal, **IdentitySignal**) ผ่านตัวชี้บอก (Indicator, **Indicator**) โดยใช้ข้อมูลของผู้ให้บริการเว็บจากใบรับรองการประกันเสริม (AAC) เพื่อแจ้งให้ผู้ใช้ทราบถึงผู้ครอบครองและผู้ประพันธ์หน้าเว็บที่กำลังแสดงผล 2. **การเปลี่ยนแปลงคุณสมบัติด้านความมั่นคงของหน้าเว็บแบบพลวัตร** (Dynamic content might change security properties) เมื่อตัวแทนผู้ใช้เว็บตัดสินสถานะของการรักษาความมั่นคงชั้นขนส่งและแสดงสถานะดังกล่าวผ่านตัวชี้บอก (Indicator, **Indicator**) แล้ว สถานะที่แสดงคุณสมบัติด้านความมั่นคงจะไม่เปลี่ยนแปลงหลังจากการโหลดเนื้อหน้าเว็บเสร็จสิ้น ซึ่งอาจเป็นช่องโหว่ให้หน้าเว็บแบบพลวัตร (Dynamic pages) ซึ่งโหลดสคริปต์และข้อมูลจากแหล่งใดก็ได้ตลอดเวลา ค้นคืนข้อมูลจากแหล่งที่ไม่ปลอดภัย ตัวแทนผู้ใช้เว็บอาจรับมือกับสถานการณ์ดังกล่าวได้โดยการแจ้งปัญหาเกี่ยวข้องกับเครือข่าย (Network Error) หรือการแจ้งเตือนผู้ใช้ (Error Signaling)			

ตารางที่ ก.18 แบบรูปการรับมือเมื่อเกิดการเปลี่ยนแปลงเนื้อหาระหว่างการเชื่อมต่อด้วยใบรับรองที่ได้รับประกันเสริม (ต่อ)

Name	การรับมือเมื่อเกิดการเปลี่ยนแปลงเนื้อหาระหว่างการเชื่อมต่อด้วยใบรับรองที่ได้รับประกันเสริม	ID	WSCP86

Internal Structure



Example Resolved

จากกรณี 12 เบ็ตตี้เยี่ยมชมหน้าเว็บที่ <https://www.example.com/> หน้าเว็บ HTML ที่ได้รับปรากฏเนื้อหาที่ได้รับจาก <http://www.example.com/> รวมอยู่ด้วย กล่าวคือเนื้อหาที่ได้รับมีบริบทความมั่นคงที่ต่างกัน ตัวแทนผู้ใช้เว็บนำเสนอสถานะความมั่นคงที่ได้จาก <http://www.example.com/> แทนที่จะแสดงจากแหล่งที่มีความน่าเชื่อถือสูงตัวแทนผู้ใช้เว็บที่ระบุข้อมูลจากใบรับรองที่ได้รับประกันเสริม ผ่านตัวชี้บอกการประกันเสริมที่แจ้งให้ผู้ใช้ทราบถึงผู้ครอบครองหน้าเว็บที่กำลังแสดงผล ให้ผู้ใช้พึงระวังในการเชื่อถือเนื้อหาจากที่มาของเว็บดังกล่าว

Consequences

การพิจารณาถึงการเปลี่ยนแปลงเนื้อหาหน้าเว็บโดยการควบคุมจากเว็บอื่น จะทำให้เกิดบูรณภาพของระบบและปิดช่องโหว่ในการโจมตีหน้าเว็บผ่านการควบคุมเนื้อหาจากแหล่งที่มาที่ไม่น่าเชื่อถือ

See Also

- ตัวอย่างปัญหาของแบบรูปนี้อ้างถึง Case 12 จากเอกสาร WSC-USECASES
- การพิจารณาการรักษาความมั่นคงชั้นขนส่งศึกษาได้จากแบบรูป 51-53

ภาคผนวก ข
ไวยากรณ์ความมั่นคง

ไวยากรณ์ความมั่นคงสร้างแบบรูปบริบทความมั่นคงเชิงเว็บ (WSCP) เกณฑ์การตั้งรหัสไวยากรณ์นั้นจะขึ้นต้นด้วย “GM” (Grammar) ตามด้วยรหัสตัวเลข 2 หลัก โดยหลักสิบอ้างถึงรหัสแบบรูปต้นฉบับที่นำมาสร้างไวยากรณ์ ในขอบเขตงานวิจัยนี้ ทั้งหมด 18 ไวยากรณ์ จำแนกได้ 4 กลุ่ม ดังนี้

กลุ่มที่ 1 การนำการรักษาความมั่นคงของชั้นขนส่งมาประยุกต์ใช้กับเว็บ

1) การจัดการใบรับรองของเว็บ
2) การกำหนดระดับความมั่นคงของการเชื่อมต่อกับผู้ให้บริการเว็บ
3) การกำหนดประเภทของเว็บจากการรักษาความมั่นคงชั้นขนส่ง
4) ทางเลือกการจัดการข้อผิดพลาดที่เกิดขึ้นขณะเชื่อมต่อการรักษาความมั่นคงชั้นขนส่ง

กลุ่มที่ 2 ตัวชี้บอกและการมีปฏิสัมพันธ์

1) การส่งสัญญาณอัตลักษณ์ของเว็บ
2) การกำหนดของข้อมูลเพิ่มเติมที่เกี่ยวข้องกับบริบทความมั่นคงเชิงเว็บ
3) การกำหนดความต้องการของตัวชี้บอกการรักษาความมั่นคงชั้นขนส่ง
4) การจัดการข้อผิดพลาด

กลุ่มที่ 3 แนวทางที่ดีที่สุดสำหรับสภาพทนทาน

1) การกำหนดความต้องการส่วนต่อประสานผู้ใช้โครม
2) การกำหนดความต้องการสำหรับส่วนต่อประสานผู้ใช้ที่สามารถควบคุมได้โดยเนื้อหาเว็บเพื่อป้องกันการลอกเลียนตัวชี้บอกความมั่นคง
3) การป้องการโจมตีผ่านปฏิสัมพันธ์
4) กำหนดความต้องการด้านความมั่นคงสำหรับตัวแทนผู้ใช้เว็บที่รองรับส่วนต่อประสานโปรแกรมประยุกต์

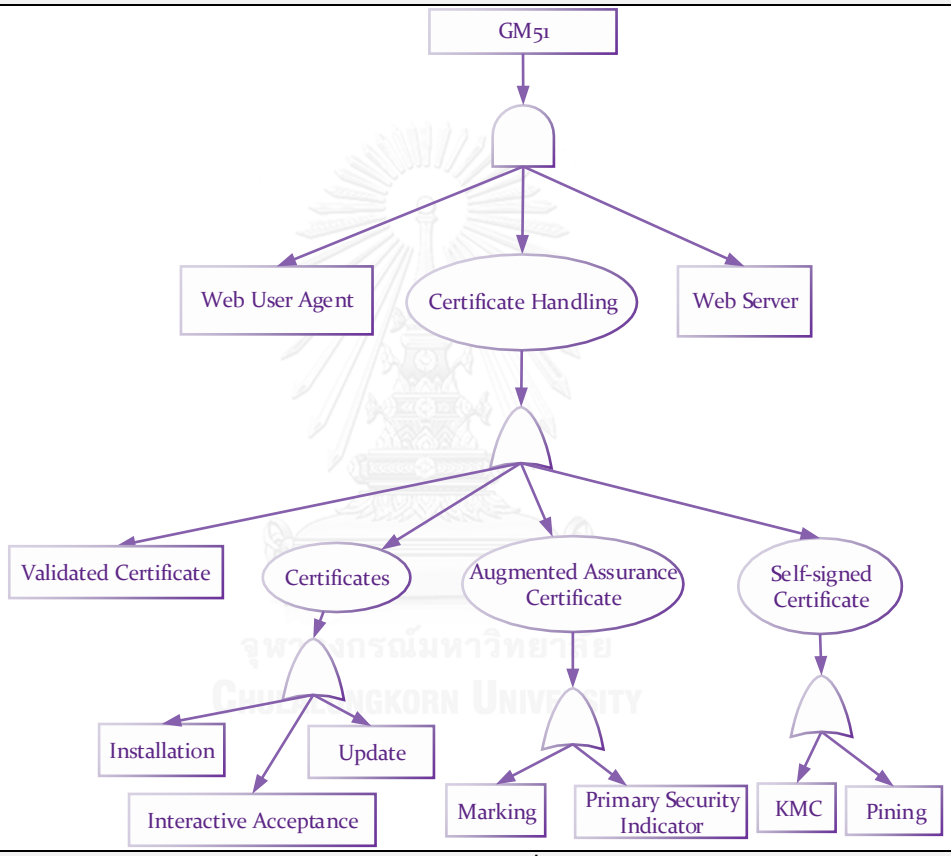
กลุ่มที่ 4 ข้อคำนึงด้านความมั่นคง

1) การป้องกันการโจมตีด้วยใบรับรองระหว่างการเชื่อมต่อการรักษาความมั่นคงชั้นขนส่ง
2) การป้องกันการโจมตีการตรวจสอบสถานะใบรับรอง
3) การกำหนดข้อยกเว้นในการประกันความมั่นคงของเว็บ
4) การกำหนดข้อมูลอัตลักษณ์ที่สอดคล้องกับโลกความจริง
5) การกำหนดข้อจำกัดของข้อความแจ้งเตือน
6) การกำหนดสัญญาณอัตลักษณ์ของเว็บที่มีการเปลี่ยนแปลงเนื้อหาระหว่างการรักษาความมั่นคงชั้นขนส่ง

ตารางที่ ข.1 ไวยากรณ์การจัดการใบรับรองของเว็บ

ชื่อไวยากรณ์	การจัดการใบรับรองของเว็บ	**รหัสไวยากรณ์**	GM51
กลุ่มไวยากรณ์	การรักษาความมั่นคงชั้นขนส่ง		
เงื่อนไขก่อนการใช้	ข้อมูลเบื้องต้นของโครงการ		
คำอธิบาย	ไวยากรณ์สำหรับพิจารณาการจัดการใบรับรองแต่ละประเภท ให้เข้าใจถึงใบรับรองแต่ละประเภทมีระดับความมั่นคงต่างกัน เพื่อกำหนดความต้องการด้านความมั่นคงในการจัดการกับใบรับรองระดับต่างๆ อย่างเหมาะสม		

แผนภาพต้นไม้ความมั่นคง



ไวยากรณ์ความมั่นคง

(1) **GM51** = **Web-User-Agent**, “shall support”, **Certificate-Handling**, “from”, **Web-Server**, “.”;

(2) **Web-User-Agent** = ?User define client name from beginning of the project? ;

(3) **Web-Server** = [“any” | ?User define server name or select at least 1 from serverNameList* of the project?] ;

ตารางที่ ข.1 ไวยากรณ์การจัดการใบรับรองของเว็บ (ต่อ)

ชื่อไวยากรณ์	การจัดการใบรับรองของเว็บ	**รหัสไวยากรณ์**	GM51

(4) **Certificate-Handling** = [**Validated-Certificate** | **Certificates** | **Augmented-Assurance-Certificate** | **Self-Signed-Certificate**];

(5) **Validated-Certificate** = “certificate verifying that it's chaining up to a locally configured trust anchor as a Validated Certificate” ;

(6) **Certificates** = **Certificates-List ,** {**Conjunction , Certificates-List**} ,“ for any certificates” ;

(7) **Certificates-List** = [**Installation** | **Update** | **Interactive-Acceptance**] ;

(8) **Installation** = “Trust Anchor installation: that is handled by ” , **Installer** , {**Conjunction** , **Installer**} , “ based on out-of-band information” ;

(9) **Installer** = [“user agent vendors”| “systems administrators”| “device manufacturers”| ?User define who will responsible for install Trust Anchor repository?] ;

(10) **Update** = “Trust Anchor update: that is handled as part of ” , **Update-Space** , {**Conjunction** , **Update-Space**} ;

(11) **Update-Space** = [“User Agent” | “operating system software updates” |?User define which part of user agent system will responsible for update Trust Anchor?] ;

(12) **Interactive-Acceptance** = “Interactively Acceptance: while the user is focused on a primary task unrelated to trust and certificate management but not allow users to designate trust roots as augmented assurance qualified”;

(13) **Augmented-Assurance-Certificate** = “Authentication, where the issuer asserts that the subject entity, by validate the certificate chain for a certificate up to a trust root and recognize the trust root as augmented assurance qualified. ”, **AAC-List** , {**Conjunction** , **AAC-List**} , “ for Augmented Assurance Certificate”;

(14) **AAC-List** = [**Marking** | **Primary-Security-Indicator**];

(15) **Marking** = “Handling by marking Trust Anchor using application-specific out-of-band mechanism” , {**Conjunction** , “specially marked by specific policy object identifier”} ;

(16) **Primary-Security-Indicator** = “Certificate information from additional assurance of Certificate Authority is presenting on Primary Security Indicator that contains following: ” **Subject-Field** , {**Conjunction** , **Subject-Field**} , “Subject-Field” ;

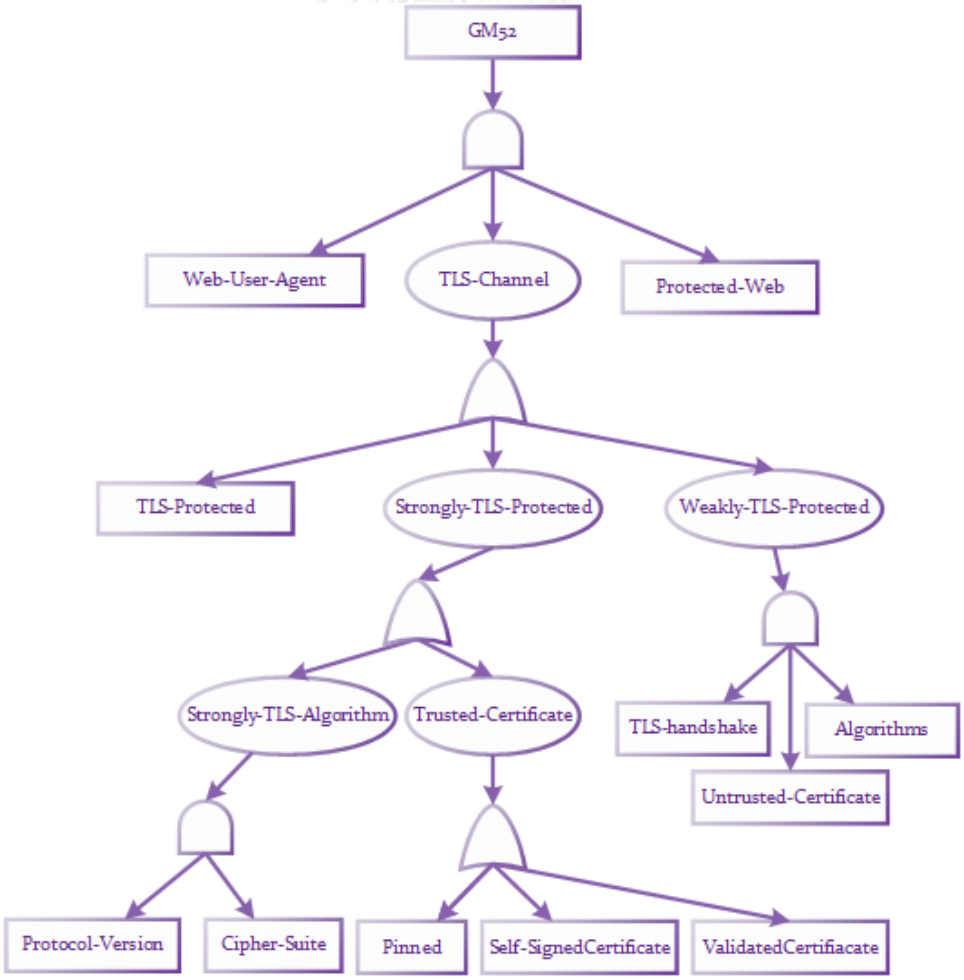
(17) **Subject-Field** = [“Organization (O)” | “Country (C)” |?User define subject-field that will present by Indicator from the Certificate?];

ตารางที่ ข.1 ไวยากรณ์การจัดการใบรับรองของเว็บ (ต่อ)

ชื่อไวยากรณ์	การจัดการใบรับรองของเว็บ	**รหัสไวยากรณ์**	GM51
(18) **Self-Signed-Certificate** = “handling a Self-signed Certificates which are not part of the user agent's store of trust roots and essentially serve as a container for cryptographic key material in a key exchange that is not verified by any third party. By ” , **SSC-List** , {**Conjunction** , **SSC-List**} , “ for self-signed certificates (or certificates that chain up to an untrusted root)” ; (19) **SSC-List** = [**KCM** | **Pinning**]; (20) **KCM** = “Key Continuity Management (KMC) to determine consistently communicating with the same web server” ; (21) **Pinning** = “the pinning interaction that enables users to pin a certificate to a destination, but not allow to be accepted automatically for an untrusted root certificate to additional sites nor to be pinned to more than one site” ; (22) **Conjunction** = [**Many** | **Last-One**]; (23) **Many** = “, ” ; **Last-One** = [“ and ” | “ or ”];			
ตัวอย่างความต้องการ			
UP2ME shall support Authentication, where the issuer asserts that the subject entity, by validate the certificate chain for a certificate up to a trust root and recognize the trust root as augmented assurance qualified. Certificate information from additional assurance of Certificate Authority is presenting on Primary Security Indicator that contains following: Organization (O) and Country (C) Subject-Field and Handling by marking Trust Anchor using application-specific out-of-band mechanism or specially marked by specific policy object identifier for Augmented Assurance Certificate from SCB website.			

ตารางที่ ข.2 ไวยากรณ์การกำหนดระดับความมั่นคงของการเชื่อมต่อกับผู้ให้บริการเว็บ

ชื่อไวยากรณ์	การกำหนดระดับความมั่นคงของการเชื่อมต่อกับผู้ให้บริการเว็บ	**รหัสไวยากรณ์**	GM52
กลุ่มไวยากรณ์	การรักษาความมั่นคงชั้นขนส่ง		
เงื่อนไขก่อนการใช้	ประเภทใบรับรอง (Certificates) จากไวยากรณ์ 51 การระบุความต้องการความมั่นคงในการจัดการกับใบรับรองเว็บ		
คำอธิบาย	ไวยากรณ์สำหรับกำหนดระดับความมั่นคงของการเชื่อมต่อของผู้ให้บริการเว็บเพื่อให้เข้าใจเว็บที่มีการรักษาความมั่นคงชั้นขนส่งที่ตัวแทนผู้ใช้ติดต่อด้วยแต่ละประเภทว่ามีการตรวจสอบอย่างไรสำหรับระดับความมั่นคงแข็งแกร่งหรืออ่อนแอ เนื่องจากช่องทางการติดต่อระหว่างตัวแทนผู้ใช้เว็บและผู้ให้บริการเว็บจำเป็นรักษาความมั่นคงในการเชื่อมต่อผู้พัฒนาจึงต้องกำหนดการระดับรักษาความมั่นคงอย่างแข็งแกร่งหรืออ่อนแอโดยระบุชนิดของใบรับรองหรืออัลกอริทึมสำหรับรายการหน้าเว็บที่ตัวแทนผู้ใช้ที่เชื่อมต่อ		
แผนภาพต้นไม้ความมั่นคง			



ตารางที่ ข.2 ไวยากรณ์การกำหนดระดับความมั่นคงของการเชื่อมต่อกับผู้ให้บริการเว็บ (ต่อ)

ชื่อไวยากรณ์	การกำหนดระดับความมั่นคงของการเชื่อมต่อกับผู้ให้บริการเว็บ	**รหัสไวยากรณ์**	GM52

ไวยากรณ์ความมั่นคง

(1) **GM52** = **Web-User-Agent** , " shall communicate with " , **TLS-Channel**;

(2) **User-Agent** = ?User define client name from beginning of the project? ;

(3) **Web-Server** = ["any websites" |?User define server name or select at least 1 from serverNameList];

(4) **Protected-Web** = **Web-Server** , {**Conjunction** , **Web-Server**};

(5) **Strongly-Protected-Web** = **Web-Server** , {**Conjunction** , **Web-Server**};

(6) **TLS-Channel** = **TLS-Channel-List** , {**Conjunction** , **TLS-Channel-List**};

(7) **TLS-Channel-List** = [**TLS-Protected** | **Strongly-TLS-Protected** | **Weakly-TLS-Protected**];

(8) **TLS-Protected** = **Protected-Web**," though TLS-protected that the resources was identified through a URI with the https URI scheme, the TLS handshake was performed successfully through the TLS channel." ;

(9) **Strongly-TLS-Protected** = **Strongly-Protected-Web** ,". The server used " , **Trusted-Certificate**, " though strongly TLS-protected that the https URL was used, strong TLS algorithms were negotiated" , **Strong-TLS-Algorithm** , ".";

(10) **Strong-TLS-Algorithm** = " with protocol version at least SSLv3" , **Protocol-Version**, {**Conjunction**, **Protocol-Version**}, " and Cipher suite are " , **Cipher-Suite** , { **Conjunction** , **Cipher-Suite**} ;

(11) **Protocol-Version** = ["SSLv3"| ? user define protocol version at least SSLv3 ?] ;

(12) **Cipher-Suite** = ["not TLSv11"| ?user define Cipher suite neither export nor TLSv11?];

(13) **Trusted-Certificate** = **Trusted-Certificate-List** , { "; or " , **Trusted-Certificate-List**};

(14) **Trusted-Certificate-List** = ["Validated Certificate that matches the dereferenced URI"| "Self-signed Certificate that was pinned to the destination" | "Certificate chain leading to an untrusted root certificate that was pinned to the destination"] ;

(15) **Weakly-TLS-Protected** = **Protected-Web** , ", though weakly TLS-protected when strong TLS protection could not be achieved the following reasons: " , **Weakly-TLS-Reasons** , {"."} ;

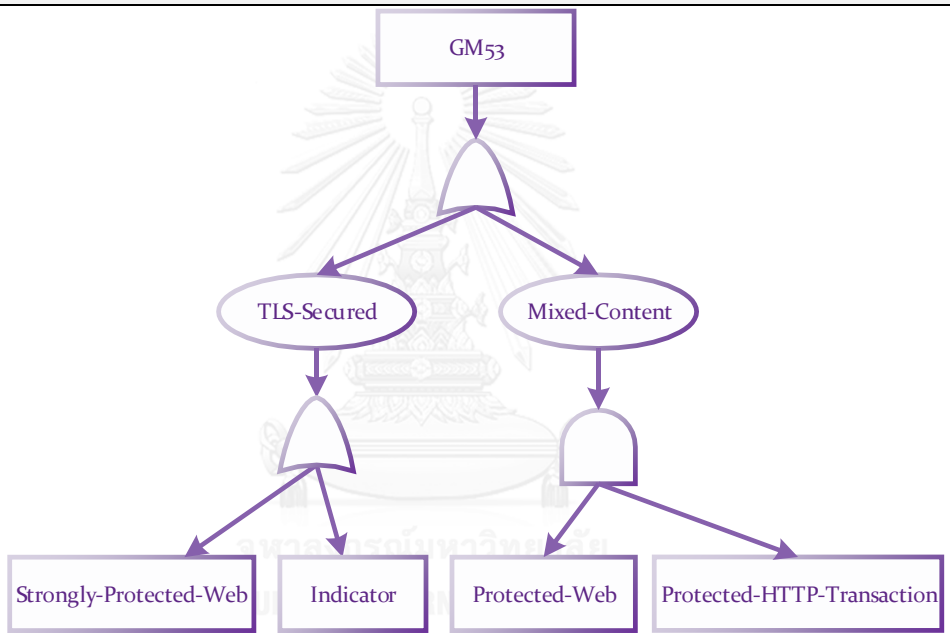
ตารางที่ ข.2 ไวยากรณ์การกำหนดระดับความมั่นคงของการเชื่อมต่อกับผู้ให้บริการเว็บ (ต่อ)

ชื่อไวยากรณ์	การกำหนดระดับความมั่นคงของการเชื่อมต่อกับผู้ให้บริการเว็บ	**รหัสไวยากรณ์**	GM52
(16) **Weakly-TLS-Reasons** = **Reasons-List** , {**Conjunction** , **Reasons-List**}; (17) **Reasons-List** = [“TLS handshake used an anonymous key exchange algorithm such as DH_anon” | “the cryptographic algorithms negotiated are not considered strong” | “certificates were used that are not either validated certificates, or self-signed certificates pinned to the destination”] ; (18) **Conjunction** = [**Many** | **Last-One**]; (19) **Many** = “, ” ; (20) **Last-One** = [“ and ” | “ or ”] ;			
ตัวอย่างความต้องการ			
UP2ME shall communicate with **SCB website**. The server used **Validated Certificate** that matches the dereferenced URI though strongly TLS-protected that the https URL was used, strong TLS algorithms were negotiated with protocol version at least SSLv3.			

ตารางที่ ข.3 ไวยากรณ์การกำหนดประเภทของเว็บจากการรักษาความมั่นคงชั้นขนส่ง

ชื่อไวยากรณ์	การกำหนดประเภทของเว็บจากการรักษาความมั่นคงชั้นขนส่ง	**รหัสไวยากรณ์**	GM53
กลุ่มไวยากรณ์	การรักษาความมั่นคงของชั้นขนส่ง		
เงื่อนไขก่อนการใช้	ต้องมีการนิยามข้อมูลการปกป้องด้วยความมั่นคงชั้นขนส่ง (TLS-Protected) จากไวยากรณ์ 52 ระดับความมั่นคงของการเชื่อมต่อ		
คำอธิบาย	ไวยากรณ์สำหรับกำหนดประเภทของเว็บที่ตัวแทนผู้ใช้มีปฏิสัมพันธ์จากช่องการติดต่อทีเอลเอส (TLS channel) เพื่อเข้าใจเว็บที่มีการติดต่อผ่านช่องทางที่มั่นคงมีลักษณะอย่างไร		

แผนภาพต้นไม้ความมั่นคง



ไวยากรณ์ความมั่นคง

(1) **GM53** = [**TLS-Secured** | **Mixed-Content**];

(2) **Protected-Web** = **Web-Server** , {**Conjunction** , **Web-Server**} , “ web site; ”;

(3) **Web-User-Agent** = ?User define client name from beginning of the project? ;

(4) **Web-Server** = [“any websites” | ?User define server name or select at least 1 from serverNameList of the project or derived from Protected-Web of GM52?] ;

(5) **Strongly-Protected-Web** = **Protected-Web**, “A Web page is called TLS-secured if the top-level resource and all other resources that can affect or control the page's content and presentation was retrieved through strongly TLS protected HTTP transactions.” ?Checking for Strongly-TLS-Protected terminal output of GM52 ?;

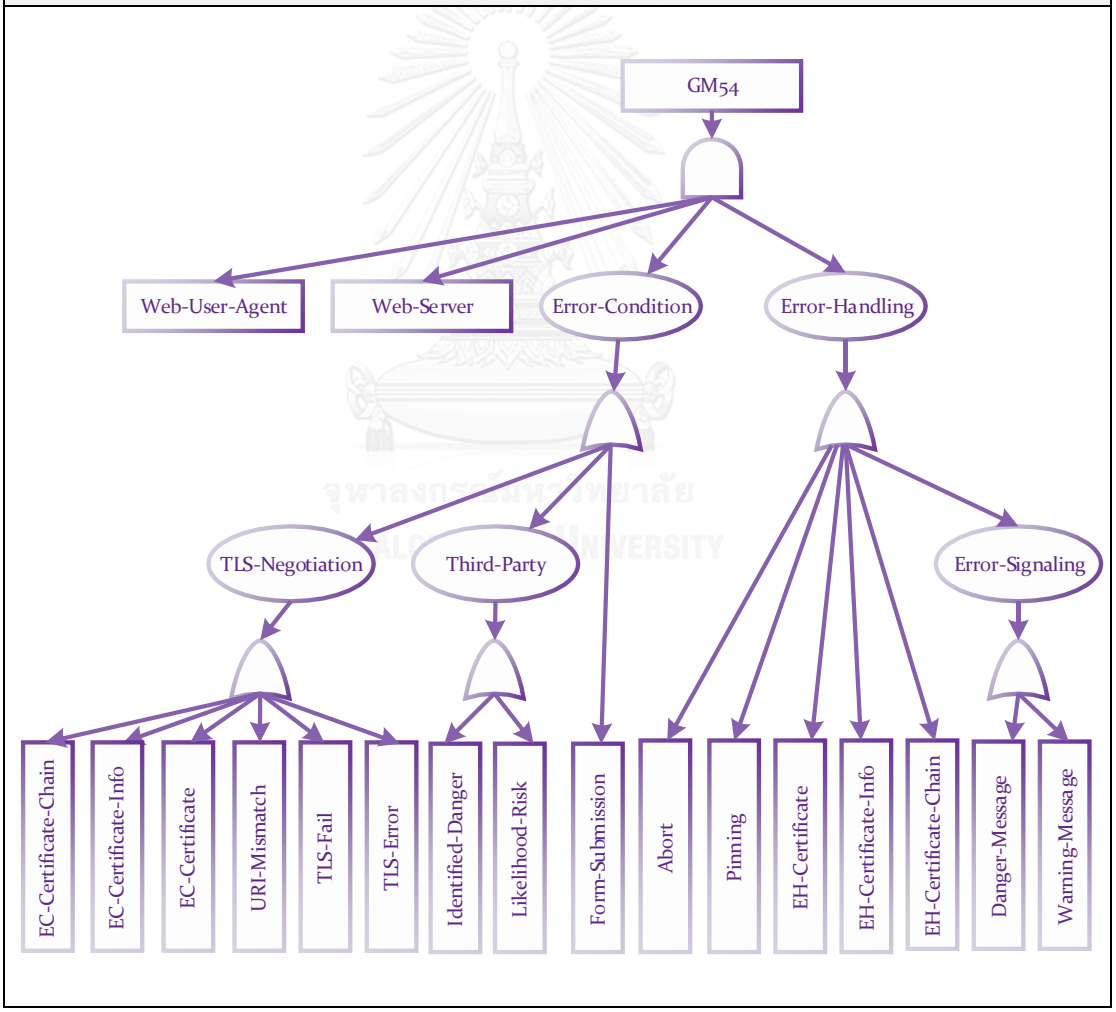
(6) **TLS-Secured** = [**Strongly-Protected-Web** | **Indicator**];

ตารางที่ ข.3 ไวยากรณ์การกำหนดประเภทของเว็บจากการรักษาความมั่นคงชั้นขนส่ง (ต่อ)

ชื่อไวยากรณ์	การกำหนดประเภทของเว็บจากการรักษาความมั่นคงชั้นขนส่ง	**รหัสไวยากรณ์**	GM53
(7) **Indicator** = **Web-User-Agent** , “ shall present UI indicator to signal the presence of Augmented Assurance certificates for the TLS-secured web page.”; (8) **Mixed-Content** = **Protected-Web**, “A Web page is called mixed content if the top-level resource was retrieved through a strongly TLS protected HTTP transaction, but some dependent resources were retrieved through ”, **Protected-HTTP-Transaction** ; (9) **Protected-HTTP-Transaction** = [“weakly protected.” | “unprotected HTTP transaction.”];			
ตัวอย่างความต้องการ			
SCB website; A Web page is called TLS-secured if the top-level resource and all other resources that can affect or control the page's content and presentation was retrieved through strongly TLS protected HTTP transactions. UP2ME shall present UI indicator to signal the presence of Augmented Assurance certificates for the TLS-secured web page.			

ตารางที่ ข.4 ไวยากรณ์ทางเลือกการจัดการข้อผิดพลาดที่เกิดขึ้นขณะเชื่อมต่อการรักษาความมั่นคงชั้นขนส่ง

ชื่อไวยากรณ์	ทางเลือกการจัดการข้อผิดพลาดที่เกิดขึ้นขณะเชื่อมต่อการรักษาความมั่นคงชั้นขนส่ง	**รหัสไวยากรณ์**	GM54
กลุ่มไวยากรณ์	การรักษาความมั่นคงชั้นขนส่ง		
เงื่อนไขก่อนการใช้	ข้อมูลการส่งสัญญาณข้อผิดพลาด (Error-Signaling) จากไวยากรณ์ GM64 การจัดการข้อผิดพลาดต้องถูกนิยามไว้แล้ว		
คำอธิบาย	ไวยากรณ์สำหรับกำหนดเงื่อนข้อผิดพลาดและการจัดการกับข้อผิดพลาดนั้น ให้เข้าใจถึงเงื่อนไขที่อาจเกิดข้อผิดพลาดขณะทำการเชื่อมต่อการรักษาความมั่นคงชั้นขนส่งและเลือกแนวทางการจัดการกับข้อผิดพลาดดังกล่าวได้อย่างเหมาะสม		
แผนภาพต้นไม้ความมั่นคง			



ตารางที่ ข.4 ไวยากรณ์ทางเลือกการจัดการข้อผิดพลาดที่เกิดขึ้นขณะเชื่อมต่อการรักษาความมั่นคงชั้นขนส่ง (ต่อ)

ชื่อไวยากรณ์	ทางเลือกการจัดการข้อผิดพลาดที่เกิดขึ้นขณะเชื่อมต่อการรักษาความมั่นคงชั้นขนส่ง	**รหัสไวยากรณ์**	GM54

ไวยากรณ์ความมั่นคง

(1) **GM54** = **Web-Server** , " present their certificate " , **Error-Condition** ;

(2) **Web-Server** = ["Any websites" | ?User define server name or select at least 1 from serverNameList* of the project?] ;

(3) **Web-User-Agent** = ?User define client name from beginning of the project? ;

(4) **Error-Handling** = **Web-User-Agent** , " shall handling the error condition by " ;

(5) **Error-Condition** = [**TLS-Negotiation** | **Third-Party** | **Form-Submission**] ;

(6) **TLS-Negotiation** = "during TLS negotiation, " , [**EC-Certificate-Chain**|**EC-Certificate-Info**|**EH-Certificate**|**URI-Mismatch**|**TLS-Fail**|**TLS-Error**] ;

(7) **EC-Certificate-Chain** = "was neither lead to a trusted root nor pinned to the destination. ", **EH-Certificate-Chain** ;

(8) **EH-Certificate-Chain** = **Error-Handling**, **Chain-Handling-List**, {**Conjunction**, **Chain-Handling-List**}, ".";

(9) **Chain-Handling-List** = [**Warning-Message** | **Pinning**];

(10) **Error-Signaling** = "using error signaling class of " ;

(11) **Danger-Message** = **Error-Signaling** , "Danger Messages" ;

(12) **Warning-Message** = **Error-Signaling** , ["Warning Messages" | "Warning Messages or higher"] ;

(13) **Pinning** = "offering a possibility to pin newly encountered certificates to the destination";

(14) **EC-Certificate-Info** = "human-readable information from the certificate shall not be presented as trustworthy." , **Error-Handling** , **EH-Certificate-Info** , " display " , **Certificate-Attribute** , " attribute from" , **Certificate-Type** , "." ;

(15) **EH-Certificate-Info** = ["a dialog" | "secondary user interfaces reachable from the warning messages"];

(16) **Certificate-Attribute** = ["Common Name" | "Organization" | ?user defines more attribute?];

(17) **Certificate-Type** = ["any certificates" | "Self-Signed-Certificate" | "Augmented-Assurance-Certificate" | "Validated-Certificate"];

ตารางที่ ข.4 ไวยากรณ์ทางเลือกการจัดการข้อผิดพลาดที่เกิดขึ้นขณะเชื่อมต่อการรักษาความมั่นคงชั้นขนส่ง (ต่อ)

ชื่อไวยากรณ์	ทางเลือกการจัดการข้อผิดพลาดที่เกิดขึ้นขณะเชื่อมต่อการรักษาความมั่นคงชั้นขนส่ง	**รหัสไวยากรณ์**	GM54

(18) **EH-Certificate** = “one of the intermediate certificates in the certificate chain are found to have been expired or revoked then ” , **Error-Handling** , **Danger-Message** , “.” ;

(19) **URI-Mismatch** = "but does not match with the URI corresponding to the transaction." , **Error-Handling** , **Danger-Message** , “.”;

(20) **TLS-Fail** = “was fails. ” , **Error-Handling** , **Danger-Message** , “.” ;

(21) **TLS-Error** = “then TLS error conditions occur. ” , **Error-Handling** , “choose to abort the connection without any further user interaction.”;

(22) **Third-Party** = [**Identified-Danger** | **Likelihood-Risk**] ;

(23) **Identified-Danger** = “then the possible danger assessed by ” , **Assessor** , { **Conjunction** , **Assessor**} , “. ”, **Error-Handling** , **Danger-Message** , “.”;

(24) **Assessor** = [“Third party services” | “heuristic approaches” | ?User define risk assessor?];

(25) **Likelihood-Risk** = “then high likelihood risks are identified, but involve further user decisions. ” , **Error-Handling** , **Warning-Message** ,

(26) **Form-Submission** = “that is validated certificate then their form submission are directed to an unsecured channel. ” , **Error-Handling** , **Warning-Message**;

(27) **Conjunction** = [**Many** | **Last-One**];

(28) **Many** = “, ” ;

(29) **Last-One** = [“ and ” | “ or ”] ;

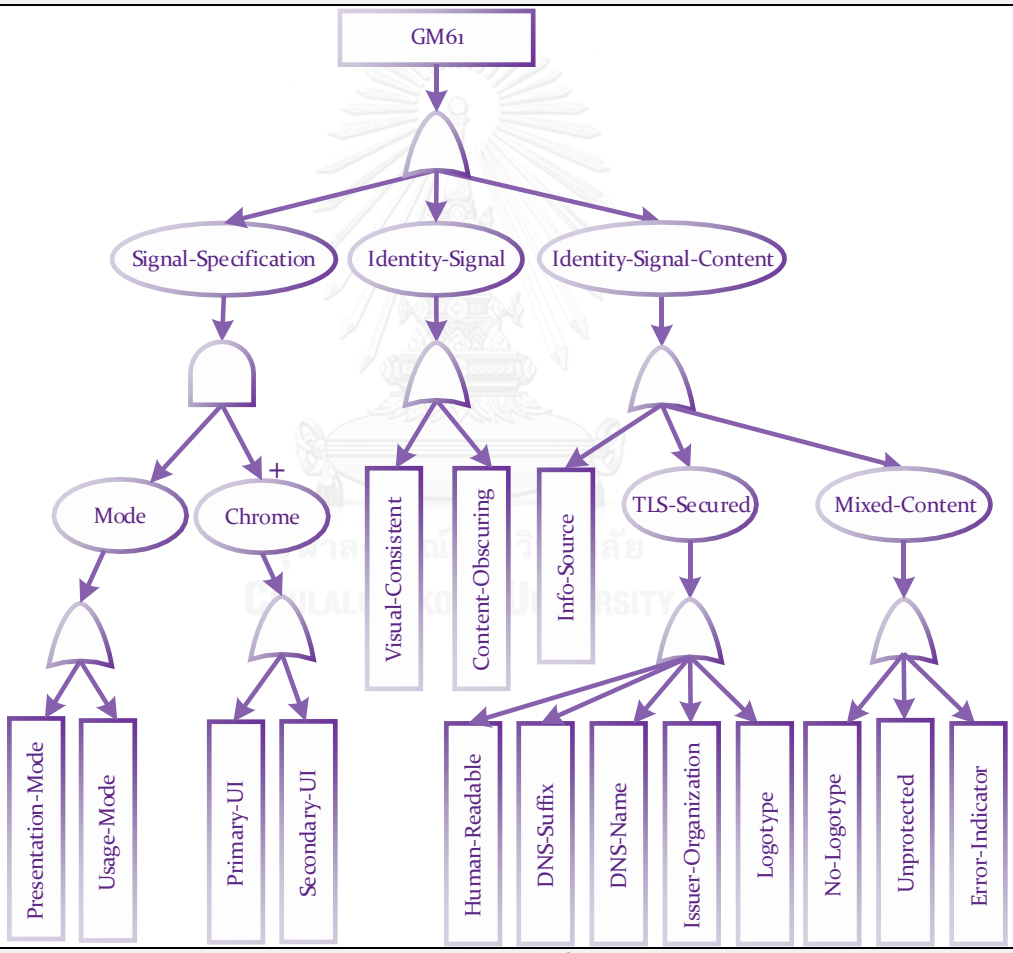
ตัวอย่างความต้องการ

Agoda website present their certificate during TLS negotiation, was neither lead to a trusted root nor pinned to the destination. **TripAdvisor** shall handling the error condition by using error signaling class of Warning Messages or higher and offering a possibility to pin newly encountered certificates to the destination.

ตารางที่ ข.5 ไวยากรณ์การส่งสัญญาณอัตลักษณ์ของเว็บ

ชื่อไวยากรณ์	การส่งสัญญาณอัตลักษณ์ของเว็บ	**รหัสไวยากรณ์**	GM61
กลุ่มไวยากรณ์	ตัวชี้บอกและการมีปฏิสัมพันธ์		
เงื่อนไขก่อนการใช้	ต้องมีการนิยามประเภทเว็บจากไวยากรณ์ 53 และต้องทีการนิยามส่วนต่อประสานโครมจากไวยากรณ์ 71		
คำอธิบาย	ไวยากรณ์สำหรับกำหนดวิธีการส่งสัญญาณอัตลักษณ์ของเว็บและเนื้อหาอัตลักษณ์ของเว็บ รวมถึงที่มาของเนื้อหาที่จะถูกนำมาใช้ส่งสัญญาณอัตลักษณ์ดังกล่าว เพื่อให้เกิดความเข้าใจถึงข้อมูลผู้ถือครองเว็บที่จะนำมาเสนอแก่ผู้ใช้ โดยข้อมูลดังกล่าวต้องมีความมั่นคงและมาจากแหล่งที่น่าเชื่อถือได้เท่านั้น		

แผนภาพต้นไม้ความมั่นคง



ไวยากรณ์ความมั่นคง

(1) **GM61** = [**Identity-Signal** | **Signal-Specification** | **Identity-Content**] ;

(2) **Identity-Signal** = **Web-User-Agent** , " shall inform user about the identity of the web site by using Identity Signal" , {**Conjunction** , **Signal-Quality**} , ". " ;

(3) **Web-User-Agent** = ?User define client name from beginning of the project? ;

(4) **Signal-Quality** = [**Visual-Consistent** | **Content-Obscuring**];

ตารางที่ ข.5 ไวยากรณ์การส่งสัญญาณอัตลักษณ์ของเว็บ (ต่อ)

ชื่อไวยากรณ์	การส่งสัญญาณอัตลักษณ์ของเว็บ	**รหัสไวยากรณ์**	GM61

(5) **Visual-Consistent** = “in a consistent visual position”;

(6) **Content-Obscuring** = “not be obscured by web content” ;

(7) **Signal-Specification** = “The Identity Signal shall be ” , Chrome , {**Conjunction**, **Chrome**} ,“ during ” , Mode , {**Conjunction**, **Mode**} , “ mode.” ;

(8) **Chrome** = [**Primary-UI** | **Secondary-UI**]; ?Check Chrome in GM71?

(9) **Primary-UI** = “part of primary user interface” ;

(10) **Secondary-UI** = “available through secondary user interface” ;

(11) **Mode** = [“usage” | “presentation” | “any” | ?User defines Mode?] ;

(12) **Identity-Signal-Content** = [**Info-Source** | **TLS-Secure** | **Mix-Content**];

(13) **Info-Source** = **Web-User-Agent** , “ shall display information from validated certificates ” , {**Conjunction** , **Certificate-List**} , “ that is not taken from unauthenticated or untrusted sources as part of the identity signal. ” ;

(14) **Certificate-List** = ?Certificates List from Grammar 51?

(15) **TLS-Secure** = “During interactions with a TLS-secured Web page, the following information derived from augmented assurance certificate shall be displayed in the Identity Signal: ”, **Human-Readable** , “. ” , **Issuer-Organization** , {**Render-Logotype**} ;

(16) **Human-Readable** = “To inform the user about the owner of the Web page, including human-readable information about the certificate subject” , {**Conjunction** , **DNS-List**} ;

(17) **DNS-List** = [**DNS-Name** | **DNS-Suffix**] ;

(18) **DNS-Name** = “ at least an applicable DNS name that matches either the subject's Common Name attribute or its subjectAltName extension” ;

(19) **DNS-Suffix** = “ shorten such a DNS name by displaying only a suffix” ;

(20) **Issuer-Organization** = “To inform the user about the party responsible for that information, including the Issuer field's Organization attribute. ” ;

(21) **Render-Logotype** = “Subject logotypes shall be rendered only derived from augmented assurance certificate. ” ;

(22) **Mix-Content** = “During interactions with mixed content, ” , [**Not-Render-Logotype** | **Unprotected-transaction** | **Error-Indicator**] ;

(23) **Not-Render-Logotype** = **Web-User-Agent** , “shall not be render any logotypes derived from certificates.” ;

(24) **Unprotected** = **Web-User-Agent** , “shall not include any site identity information which is in use for unprotected HTTP transactions.” ;

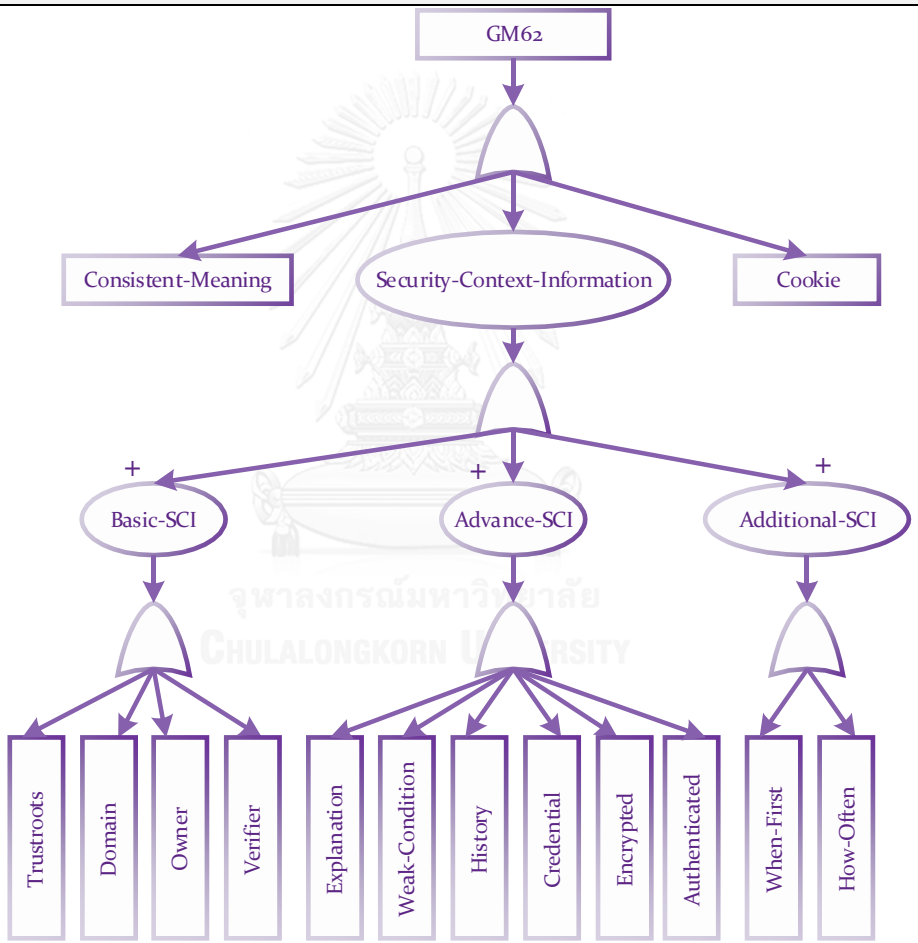
ตารางที่ ข.5 ไวยากรณ์การส่งสัญญาณอัตลักษณ์ของเว็บ (ต่อ)

ชื่อไวยากรณ์	การส่งสัญญาณอัตลักษณ์ของเว็บ	**รหัสไวยากรณ์**	GM61
(25) **Error-Indicator** = “the identity signal shall include indicators that point out any error conditions that why the web page is unprotected HTTP transactions” ; (26) **Conjunction** = [**Many** | **Last-One**]; (27) **Many** = “, ” ; (28) **Last-One** = [“ and ” | “ or ”]			
ตัวอย่างความต้องการ			
- [RE6101] The Identity Signal shall be part of primary user interface and available through secondary user interface during usage or presentation mode. - [RE6102] **TripAdvisor** shall inform user about the identity of the web site by using Identity Signal, in a consistent visual position and not be obscured by web content. - [RE6103] **UP2ME** shall display information from validated certificates that is not taken from unauthenticated or untrusted sources as part of the identity signal. - [RE6108] During interactions with mixed content, **Dolphin Web Browser** shall not be render any logotypes derived from certificates. - [RE6109] During interactions with mixed content, **TripAdvisor** shall not include any site identity information which is in use for unprotected HTTP transactions. - [RE6110] During interactions with mixed content, the identity signal shall include indicators that point out any error conditions that why the web page is unprotected HTTP transactions			

ตารางที่ ข.6 ไวยากรณ์การกำหนดข้อมูลเพิ่มเติมที่เกี่ยวข้องกับบริบทความมั่นคงเชิงเว็บ

ชื่อไวยากรณ์	การกำหนดของข้อมูลเพิ่มเติมที่เกี่ยวข้องกับบริบทความมั่นคงเชิงเว็บ	**รหัสไวยากรณ์**	GM62
กลุ่มไวยากรณ์	ตัวชี้บอกและการมีปฏิสัมพันธ์		
เงื่อนไขก่อนการใช้	ต้องมีการนิยามสัญญาณอัตลักษณ์ของเว็บจากไวยากรณ์ 61		
คำอธิบาย	ไวยากรณ์สำหรับระบุข้อมูลที่ใช้ในการแสดงบริบทความมั่นคงของเว็บ เพื่อช่วยให้ผู้พัฒนาระบุข้อมูลของเว็บและการแสดงบริบทความมั่นคงของเว็บที่พึงแสดงให้แก่ผู้ใช้ได้อย่างครบถ้วน		

แผนภาพต้นไม้ความมั่นคง



ไวยากรณ์ความมั่นคง

(1) **GM62** = [**Consistent-Meaning** | **Security-Context-Information** | **Cookie**];

(2) **Consistent-Meaning** = “The meaning of security context information in both primary and secondary interface shall be consistent. ” ;

(3) **Cookie** = **Web-User-Agent**, “ shall not claim that the absence of cookies implies an absence of any user tracking. ” ;

ตารางที่ ข.6 ไวยากรณ์การกำหนดข้อมูลเพิ่มเติมที่เกี่ยวข้องกับบริบทความมั่นคงเชิงเว็บ (ต่อ)

ชื่อไวยากรณ์	การกำหนดของข้อมูลเพิ่มเติมที่เกี่ยวข้องกับบริบทความมั่นคงเชิงเว็บ	**รหัสไวยากรณ์**	GM62

(4) **Web-User-Agent** = ?User define client name from beginning of the project? ;

(5) **Security-Context-Information** = **Web-User-Agent** , " shall provide the following security context information available: " , **Basic-SCI** , {**Conjunction**, **Basic-SCI**} , {**Conjunction**, **Advance-SCI**} , {**Conjunction**, **Additional-SCI**} ;

(6) **Basic-SCI** = [**Domain** | **Owner** | **Verifier** | **Trustroots**];

(7) **Domain** = "The Web page's domain name. " ;

(8) **Owner** = "Owner information, consistent with Identity Signal Content. " ;

(9) **Verifier** = "Verifier information, consistent Identity Signal Content. " ;

(10) **Trustroots** = "The reason why the displayed information is trusted (or not). " ;

(11) **Advance-SCI** = [**Explanation** | **Weak-Condition** | **History** | **Credential** | **Encrypted** | **Authenticated**];

(12) **Explanation** = "An explanation of the information represented by the TLS indicator. " ;

(13) **Weak-Condition** = "If the Web page is weakly TLS-protected, then, what conditions cause the protection to be weak. " ;

(14) **History** = "Whether the user has visited the site in the past. " ;

(15) **Credential** = "Whether the user has stored credentials for this site. " ;

(16) **Encrypted** = "Whether the site content was encrypted in transmission. " ;

(17) **Authenticated** = "Whether the site content was authenticated. " ;

(18) **Additional-SCI** = [**When-First** | **How-Often**];

(19) **When-First** = "When the user first visited the site in the past. " ;

(20) **How-Often** = "How often the user visited the site in the past. " ;

(21) **Conjunction** = **New-Line** , **Indent** ;

(22) **New-Line** = "</br>" ; ?Start new Line?

(23) **Indent** = "- " ;

ตัวอย่างความต้องการ

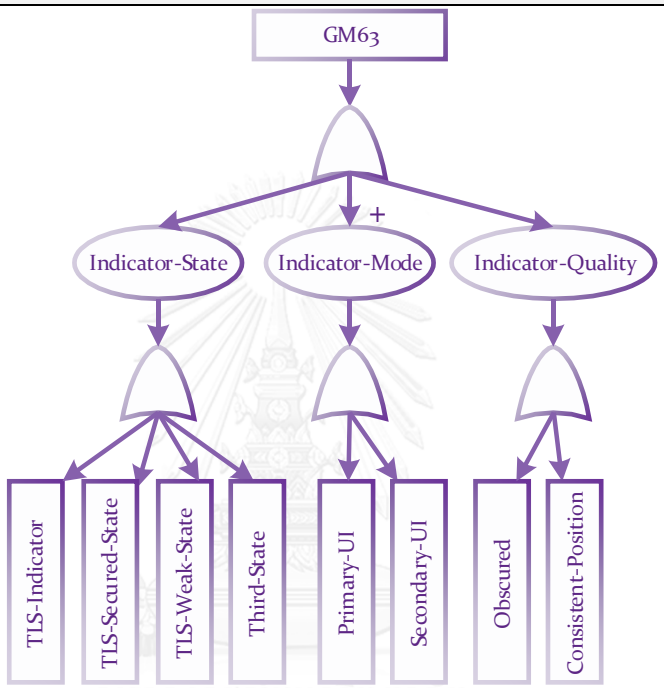
Dolphin Web Browser shall provide the following security context information available:

- Whether the user has stored credentials for this site.
- Whether the site content was encrypted in transmission.
- Whether the site content was authenticated.
- How often the user visited the site in the past.

ตารางที่ ข.7 ไวยากรณ์การกำหนดความต้องการของตัวชี้บอกการรักษาความมั่นคงชั้นขนส่ง

ชื่อไวยากรณ์	การกำหนดความต้องการของตัวชี้บอกการรักษาความมั่นคงชั้นขนส่ง	**รหัสไวยากรณ์**	GM63
กลุ่มไวยากรณ์	ตัวชี้บอกและการมีปฏิสัมพันธ์		
เงื่อนไขก่อนการใช้	ต้องมีการนิยามสัญญาณอัตลักษณ์ของเว็บจากไวยากรณ์ 61		
คำอธิบาย	ไวยากรณ์สำหรับการกำหนดคุณลักษณะของตัวชี้บอกความมั่นคงของชั้นขนส่ง		

แผนภาพต้นไม้ความมั่นคง



ไวยากรณ์ความมั่นคง

(15) **GM63** = [**Indicator-State** | **Indicator-Mode** | **Indicator-Quality**];

(16) **Indicator-State** = [**TLS-Indicator** | **TLS-Secured-State** | **TLS-Weak-State**];

(17) **TLS-Indicator** = **Web-User-Agent** , “shall provide information about the state of TLS protection available by TLS indicator.”;

(18) **Web-User-Agent** = ?User define client name from beginning of the project?;

(19) **TLS-Secured-State** = “TLS indicator shall be present a distinct state that is used only for TLS-secured web pages. ”;

(20) **TLS-Weak-State** = “TLS indicator shall inform users when they are viewing a page that, along with all dependent resources, was retrieved through at least weakly TLS protected transactions, including mixed content”, {“ by using ”, **Third-State** }, “. ”;

(21) **Indicator-Mode** = “TLS indicator shall be part of ”, **List-Mode** , {“Otherwise, it shall be available through ”, **List-Mode** };

(22) **List-Mode** = [**Primary-UI** | **Secondary-UI**];

ตารางที่ ข.7 ไวยากรณ์การกำหนดความต้องการของตัวชี้บอกการรักษาความมั่นคงชั้นขนส่ง (ต่อ)

ชื่อไวยากรณ์	การกำหนดความต้องการของตัวชี้บอกการรักษาความมั่นคงชั้นขนส่ง	**รหัสไวยากรณ์**	GM63

(23) **Primary-UI** = “primary user interface during usage modes which entail the presence of signaling to the user beyond only presenting page content.”;

(24) **Secondary-UI** = “secondary user interface.”;

(25) **Third-State** = “a third state in the TLS indicator, or via another mechanism (such as a dialog, info bar, or other means)”;

(26) **Indicator-Quality** = [**Obscured** | **Consistent-Position**];

(27) **Obscured** = “TLS indicator shall not be obscured by web content.”;

(28) **Consistent-Position** = “TLS indicator shall be available in a consistent visual position.”;

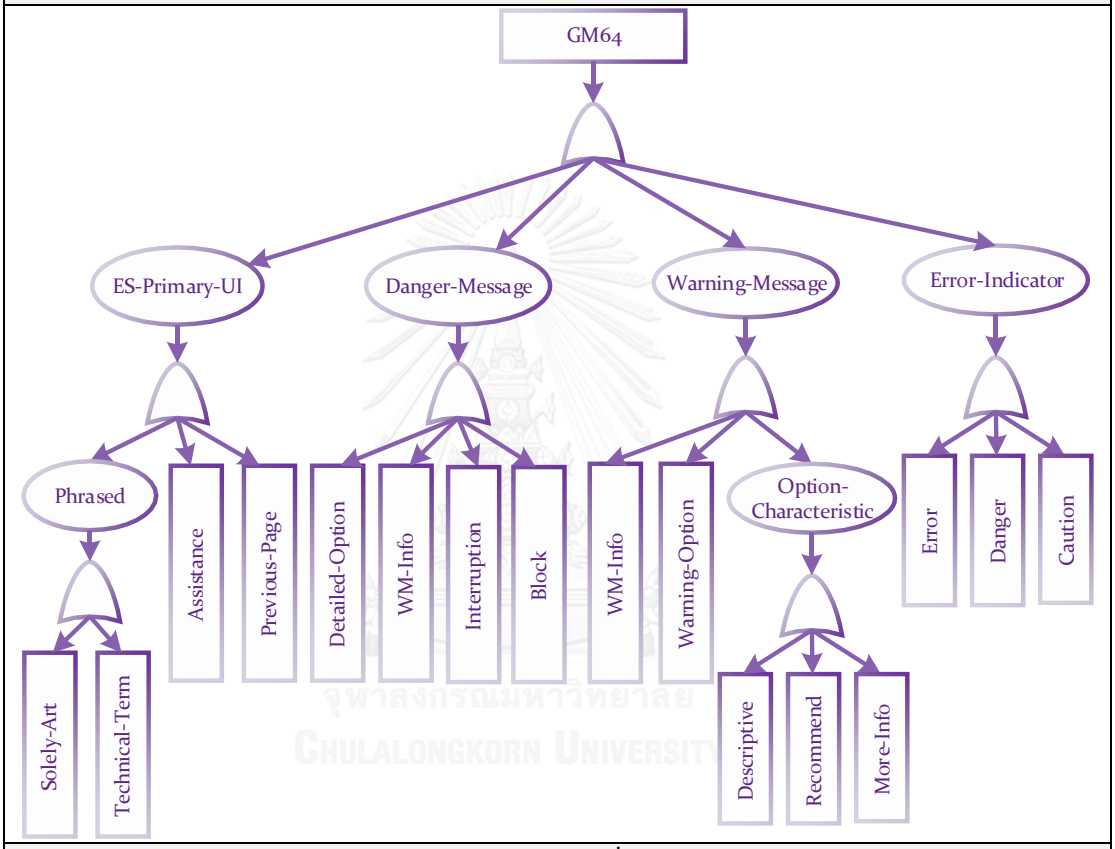
ตัวอย่างความต้องการ

TLS indicator shall be part of secondary user interface. Otherwise, it shall be available through primary user interface during usage modes which entail the presence of signaling to the user beyond only presenting page content.

ตารางที่ ข.8 ไวยากรณ์การจัดการข้อผิดพลาด

ชื่อไวยากรณ์	การจัดการข้อผิดพลาด	**รหัสไวยากรณ์**	GM64
กลุ่มไวยากรณ์	ตัวชี้บอกและการมีปฏิสัมพันธ์		
เงื่อนไขก่อนการใช้	ต้องมีการนิยามตัวชี้บอกความมั่นคงชั้นขนส่ง จากไวยากรณ์ 62		
คำอธิบาย	ไวยากรณ์สำหรับกำหนดความต้องการเกี่ยวกับการส่งสัญญาณข้อผิดพลาดและคุณลักษณะของการส่งสัญญาณแต่ละระดับ		

แผนภาพต้นไม้ความมั่นคง



ไวยากรณ์ความมั่นคง

(1) **GM64** = [**Danger-Message** | **Warning-Message** | **ES-Primary-UI** |**Error-Indicator**];

(2) **Web-User-Agent** = ?User define client name from beginning of the project? ;

(3) **Danger-Messages** = [**WM-Info** | **Interruption** | **Block**];

(4) W**M-Info** = **Web-User-Agent** , “shall have Danger Messages for situations when there is a positively identified danger to the user. ”;

(5) **Interruption** = “Messages shall interrupt the user's current task, such that the user has to acknowledge the message.”;

(6) **Block** = “Danger Messages shall be presented in a way that makes it impossible for the user to go to or interact with the destination web site that caused the danger situation to occur, without first explicitly interacting with the Danger Message.”;

ตารางที่ ข.8 ไวยากรณ์การจัดการข้อผิดพลาด (ต่อ)

ชื่อไวยากรณ์	การจัดการข้อผิดพลาด	**รหัสไวยากรณ์**	GM64

(7) **Warning-Message** = [**WM-Info** | **Warning-Option** | **Option-Characteristic**];

(8) **WM-Info** = **Web-User-Agent** , “ shall have Warning / Caution messages for situations when the system has good reason to believe that the user may be at risk based on the current security context information, but a determination cannot positively be made. ”;

(9) **Warning-Option** = “Warning / Caution messages shall provide the user with distinct options for how to proceed. ”;

(10) **Option-Characteristic** = “ The options presented on these warnings shall contain following characteristic: - ” , **Opt-Char-List** , { “ - ”, **Opt-Char-List** } ;

(11) **Opt-Char-List** = [**Descriptive** | **Recommend** | **More-Info**];

(12) **Descriptive** = “Descriptive to the point that their respective meaning can be understood in the absence of any other information contained in the warning interaction. ”;

(13) **Recommend** = A succinct text component denoting which option is recommended.”;

(14) **More-Info** = “In the absence of a recommended option, a method of finding out more information shall be provided if the options cannot be understood. ”;

(15) **ES-Primary-UI** = [**Phrased** |**Assistance** | **Previous-Page** | **Detailed-Option**];

(16) **Phrased** = “Error signaling that occurs as part of primary user interface shall be phrased in terms of threat to user's interests, not ”,**Solely-Art**, {“ nor ”,**Technical-Term**} ,“. ”;

(17) **Technical-Term** = “technical occurrence”;

(18) **Solely-Art** = “solely in terms of art”;

(19) **Assistance** = “Error messages shall provide feedback or obtain assistance, not tell the user to enter the destination site that caused the error ”;

(20) **Previous-Page** = **Web-User-Agent**, “ shall enable the user to easily return to the page that the user was previously interacting with.”;

(21) **Detailed-Option** = “Error interactions shall have an option to request a detailed description of the condition that caused the error interaction to occur. ”;

(22) **Error-Indicator** = **Web-User-Agent** , “ shall additionally display indicators in a” , [“n error”| “ danger” | “ caution”] , “ situation.”;

(23) **Conjunction** = [**Many** | **Last-One**];

(24) **Many** = “, ” ;

(25) **Last-One** = [“ and ” | “ or ”] ;

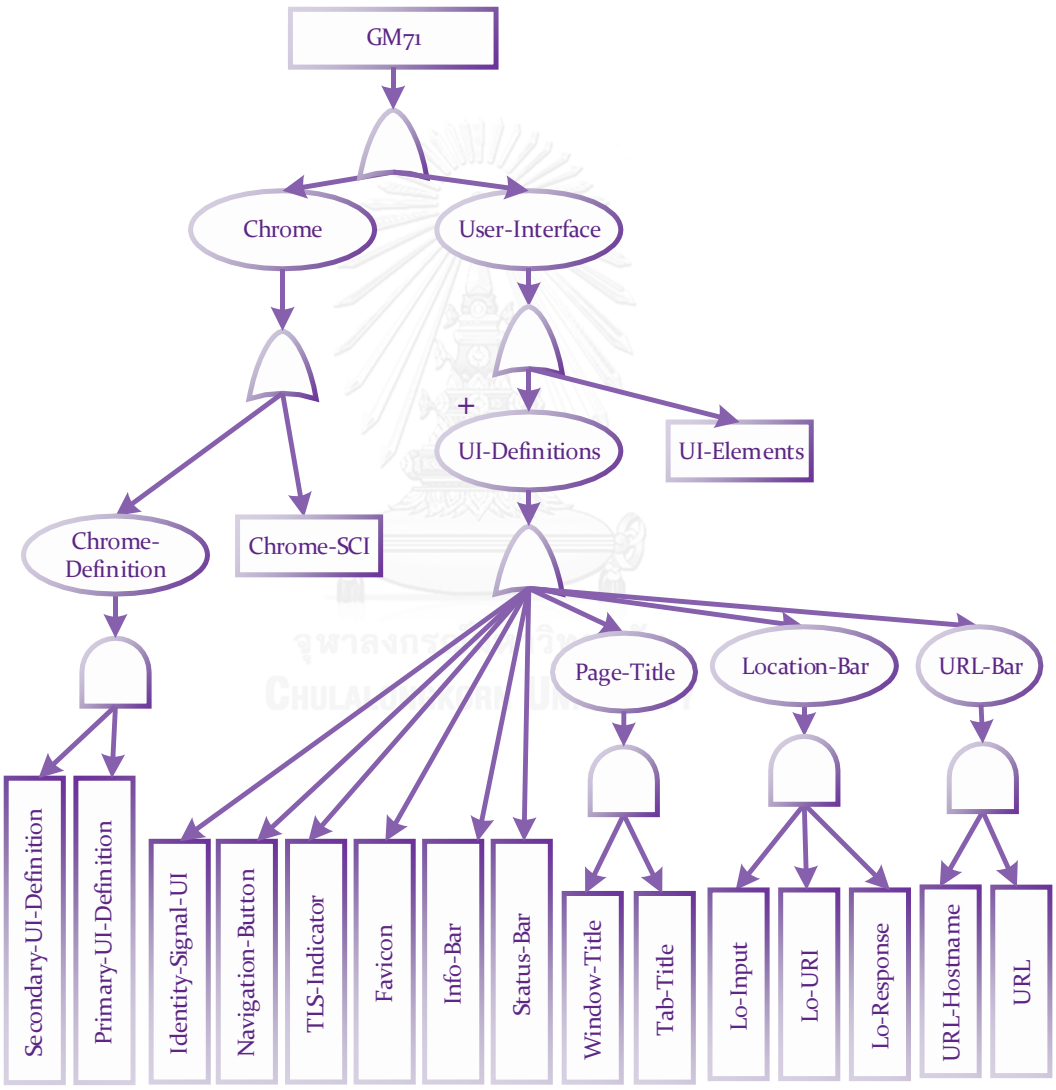
ตัวอย่างความต้องการ

UP2ME shall have Danger Messages for situations when there is a positively identified danger to the user.

ตารางที่ ข.9 ไวยากรณ์การกำหนดความต้องการส่วนต่อประสานผู้ใช้โครม

ชื่อไวยากรณ์	การกำหนดความต้องการส่วนต่อประสานผู้ใช้โครม	**รหัสไวยากรณ์**	GM71
กลุ่มไวยากรณ์	แนวปฏิบัติที่ดีที่สุดสำหรับสภาพทนทานของระบบ		
เงื่อนไขก่อนการใช้	ไม่มี		
คำอธิบาย	ไวยากรณ์สำหรับกำหนดความต้องการของส่วนต่อประสานสำหรับตัวแทนผู้ใช้เว็บตามนิยามของส่วนต่อประสานแต่ละองค์ประกอบ		

แผนภาพต้นไม้ความมั่นคง



ไวยากรณ์ความมั่นคง

(1) **GM71** = [**Chrome** | **User-Interfaces**];

(2) **Chrome** = [**Chrome-Definition** | **Chrome-SCI**];

ตารางที่ ข.9 ไวยากรณ์การกำหนดความต้องการส่วนต่อประสานผู้ใช้โครม (ต่อ)

ชื่อไวยากรณ์	การกำหนดความต้องการส่วนต่อประสานผู้ใช้โครม	**รหัสไวยากรณ์**	GM71

(3) **Chrome-Definition** = “Chrome refer to the representation through which the user interacts with the user agent itself, as distinct from the accessed web content. This includes both primary and secondary user interface. By ”, **Primary-UI-Definition** , “ and ”, **Secondary-UI-Definition** ;

(4) **Primary-UI-Definition** = “Primary User Interface denotes the portions of a Web user agent's user interface that are available to users without being solicited by a user interaction”

(5) **Secondary-UI-Definition** = “Secondary User Interface denotes the portions of a Web user agent's user interface that are available to the user after they are solicited by a specific user interaction.”

(6) **Chrome-SCI** = “Chrome shall always be present to signal security context information.”;

(7) **User-Interface** = [**UI-Elements** | **UI-Definition**];

(8) **UI-Elements** = “User interface elements commonly present in ”, **Web-User-Agent**, “, a Web User Agents, are: ” , **UI-List**, {**Conjunction**, **UI-List** } ;

(9) **UI-List** = [“Identity Signal” | “Navigation Button” | “TLS Indicator” | “Favicon” | “Information Bar” | “Status Bar” | “Page Title” | “Location Bar” | “URL Bar”];

(10) **UI-Definitions** = [**Identity-Signal-UI** | **Navigation-Button** | **TLS-Indicator** | **Favicon** | **Info-Bar** | **Status-Bar** | **Page-Title** | **Location-Bar** | **URL-Bar**];

(11) **Identity-Signal-UI** = “An Identity signal presents Identity Information about the web site.”;

(12) **Navigation-Button** = “A Navigation buttons provide a drop down list of previously viewed pages. Each page is identified by the content of the corresponding HTMLTITLE element.”;

(13) **TLS-Indicator** = “A TLS-Indicator using padlock icon to indicate the use of SSL.”;

(14) **Favicon =** “A Favicon is a small graphic specified by website to act as an icon that appears in the URL bar in most desktop web browsers and on the tabs in some browsers. ”;

(15) **Info-Bar** = [“An information” | “A Notification”] ,“ bar across the top of the web content window to communicate with users. ”;

(16) **Status-Bar** = “A Status bar displays messages from the browser, such as the target of the hyperlink under the mouse cursor. ”;

ตารางที่ ข.9 ไวยากรณ์การกำหนดความต้องการส่วนต่อประสานผู้ใช้โครม (ต่อ)

ชื่อไวยากรณ์	การกำหนดความต้องการส่วนต่อประสานผู้ใช้โครม	**รหัสไวยากรณ์**	GM71
(17) **Location-Bar** = “A Location Bar is a widget which displays ”, Lo-Input , Lo-URI , Lo-Response , “.”; (18) **Lo-Input** = “and allows input ”; (19) **Lo-URI** = “of the textual location entered as a URI ”; (20) **Lo-Response** = “of the resource being requested or displayed - after the response is received”; (21) **Page-Title** = **Window-Title**, {“ and ” , **Tab-Title**} , “using the content of the HTML TITLE element from ”, **Web-Sever** , “, the displayed web page. ” (22) **Window-Title** = “A Window title for viewing a web page” (23) **Tab-Title** = “Tabs title for viewing multiple web pages”; (24) **URL-Bar** = “A URL bar show current web page's URL is chosen in tandem by the creator of the referring hyperlink and the web site operator. ”, {“ An additional” , **URL-Hostname**}; (25) **URL-Hostname** = “the displayed hostname also using the current web page's URL. ”;			
ตัวอย่างความต้องการ			
Chrome refer to the representation through which the user interacts with the user agent itself, as distinct from the accessed web content. This includes both primary and secondary user interface. By Primary User Interface denotes the portions of a Web user agent's user interface that are available to users without being solicited by a user interaction and Secondary User Interface denotes the portions of a Web user agent's user interface that are available to the user after they are solicited by a specific user interaction.			

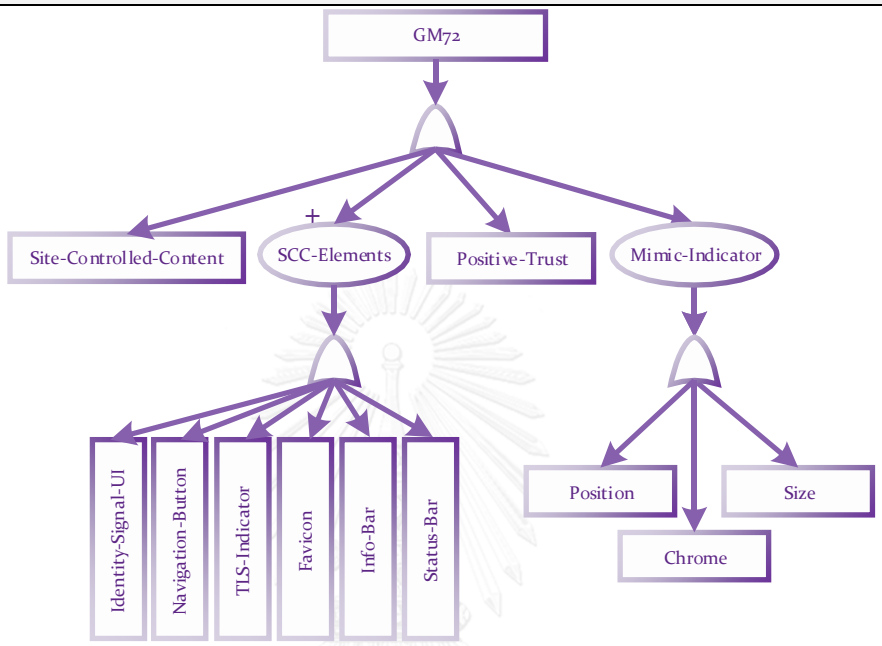
ตารางที่ ข.10 การกำหนดความต้องการสำหรับส่วนต่อประสานผู้ใช้ที่สามารถควบคุมได้โดยเนื้อหาเว็บเพื่อป้องกันการลอกเลียนตัวชี้บอกความมั่นคง

ชื่อไวยากรณ์	การกำหนดความต้องการสำหรับส่วนต่อประสานผู้ใช้ที่สามารถควบคุมได้โดยเนื้อหาเว็บเพื่อป้องกันการลอกเลียนตัวชี้บอกความมั่นคง	**รหัสไวยากรณ์**	GM72
กลุ่มไวยากรณ์	แนวปฏิบัติที่ดีที่สุดสำหรับสภาพทนทานของระบบ		
เงื่อนไขก่อนการใช้	รายการส่วนต่อประสานผู้ใช้โครมต้องถูกกำหนดไว้ในไวยากรณ์ 71		
คำอธิบาย	ไวยากรณ์สำหรับกำหนดความต้องการของส่วนต่อประสารผู้ใช้ที่สามารถควบคุมได้โดยเนื้อหาเว็บ เพื่อหลีกเลี่ยงการถูกลอกเลียนตัวชี้บอกความมั่นคงที่กำหนดได้จากไวยากรณ์ 63 การกำหนดให้ส่วนต่อประสารดังกล่าวมีลักษณะต่างจากตัวชี้บอกความมั่นคงจะทำให้ผู้ใช้ไม่เกิดความสับสนในการรับข้อมูลสถานะความมั่นคงเมื่อมีการปลอมแปลงจากเว็บ		

ตารางที่ ข.10 การกำหนดความต้องการสำหรับส่วนต่อประสานผู้ใช้ที่สามารถควบคุมได้โดยเนื้อหาเว็บเพื่อป้องกันการลอกเลียนตัวชี้บอกความมั่นคง (ต่อ)

ชื่อไวยากรณ์	การกำหนดความต้องการสำหรับส่วนต่อประสานผู้ใช้ที่สามารถควบคุมได้โดยเนื้อหาเว็บเพื่อป้องกันการลอกเลียนตัวชี้บอกความมั่นคง	**รหัสไวยากรณ์**	GM72

แผนภาพต้นไม้ความมั่นคง



ไวยากรณ์ความมั่นคง

(1) **GM72** = [**Site-Controlled-Content** | **SCC-Elements** | **Positive-Trust** | **Mimic-Indicator**];

(2) **Site-Controlled-Content** = “User interface elements within chrome which can be mimicked under the control of web content. ” ;

(3) **SCC-Elements** = “Site-Controlled content which hosted in chrome are ” , **UI-List** ,? from **GM71** ? , {**Conjunction** , **UI-List**} ;

(4) **UI-List** = [“Identity Signal” | “Navigation Button” | “TLS Indicator” | “Favicon” | “Information Bar” | “Status Bar”];

(5) **Positive-Trust** = “Web User Agents shall not communicate positive trust information using Site-Controlled content. ” ;

(6) **Mimic-Indicator** = “Site-Controlled Content shall not be displayed in a manner that confuses hosted content and chrome indicators” , { **Avoid-Mimic**} , “. ” ;

(7) **Avoid-Mimic** = [**Mimic-Position** | **Mimic-Chrome** | **Mimic-Size**];

(8) **Mimic-Position** = “ in a position close to them” ;

(9) **Mimic-Chrome** = “ for both primary and secondary” ;

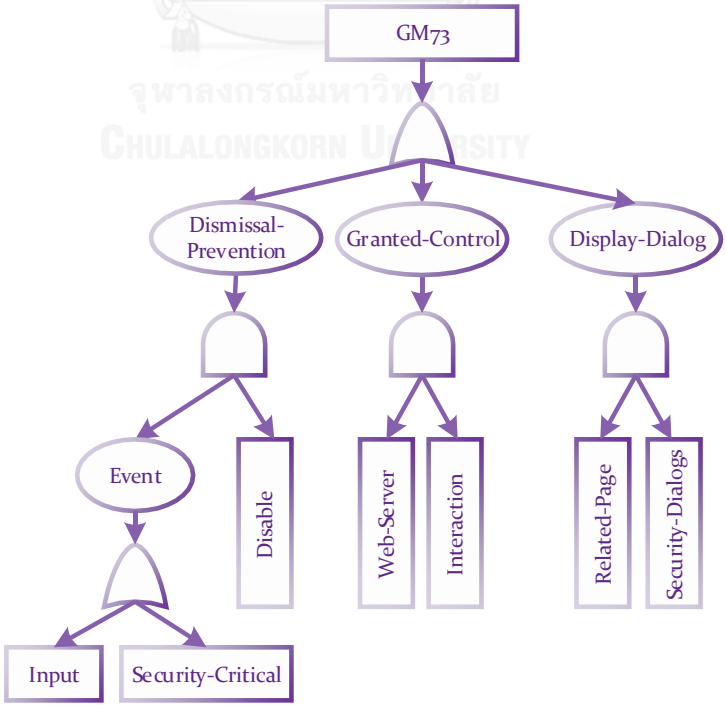
(10) **Mimic-Size** = “. A not use a 16x16 image shall not be used to indicate the security status in order to avoid imitation from the favorite icon” ;

ตารางที่ ข.10 การกำหนดความต้องการสำหรับส่วนต่อประสานผู้ใช้ที่สามารถควบคุมได้โดยเนื้อหาเว็บเพื่อป้องกันการลอกเลียนตัวชี้บอกความมั่นคง (ต่อ)

ชื่อไวยากรณ์	การกำหนดความต้องการสำหรับส่วนต่อประสานผู้ใช้ที่สามารถควบคุมได้โดยเนื้อหาเว็บเพื่อป้องกันการลอกเลียนตัวชี้บอกความมั่นคง	**รหัสไวยากรณ์**	GM72
ตัวอย่างความต้องการ			
Site-Controlled Content shall not be displayed in a manner that confuses hosted content and chrome indicators in a position close to them for both primary and secondary. A not use a 16x16 image shall not be used to indicate the security status in order to avoid imitation from the favorite icon			

ตารางที่ ข.11 ไวยากรณ์การป้องการโจมตีผ่านปฏิสัมพันธ์

ชื่อไวยากรณ์	การป้องการโจมตีผ่านปฏิสัมพันธ์	**รหัสไวยากรณ์**	GM73
กลุ่มไวยากรณ์	แนวปฏิบัติที่ดีที่สุดสำหรับสภาพทนทานของระบบ		
เงื่อนไขก่อนการใช้	ต้องมีการนิยามการส่งสัญญาณข้อผิดพลาดจากไวยากรณ์ 64		
คำอธิบาย	ไวยากรณ์สำหรับการกำหนดความต้องการเพื่อป้องกันการมีปฏิสัมพันธ์ในลักษณะการโจมตีระบบโดยเนื้อหาเว็บ		
แผนภาพต้นไม้ความมั่นคง			



ตารางที่ ข.11 ไวยากรณ์การป้องการโจมตีผ่านปฏิสัมพันธ์ (ต่อ)

ชื่อไวยากรณ์	การป้องการโจมตีผ่านปฏิสัมพันธ์	**รหัสไวยากรณ์**	GM73
ไวยากรณ์ความมั่นคง			
(1) **GM73** = [**Dismissal-Prevention** | **Granted-Control** | **Security-Dialogs**] ; (2) **Dismissal-Prevention** = **Web-User-Agent**, “shall employ techniques that prevent immediate dismissal of user interfaces that used” , **Events** , {**Events**} , **Disable** ; (3) **Web-User-Agent** = ?User define client name from beginning of the project? ; (4) **Events** = [“to inform users about security critical events” | “ or ” | “to solicit input”] ; (5) **Disable** = “by using a temporarily disabled "OK" button. ”; (6) **Granted-Control** = **{**“The ”,**Web-Server}** , “ web server are not be granted control from ” , **Interaction** ,“ that users interact with”, (7) **Web-Server** = ?User define sever name from beginning of the project? ; (8) **Interaction** = [“security relevant notifications” | “Warning Message” | “Caution Message” | “Danger Message”]; ?Check for the Error-Signaling from GM64? (9) **Display-Dialog** = “The ”, **Web-User-Agent** , “ shall display only a modal security dialog” , {**Conjunction** , **Security-Dialog**} , **Related-Page** ; (10) Related-Page = “related to ” , **Web-Server** , “ which user currently have focus.”; (11) Security-Dialogs = [“e.g.” | “prompts for ” | “user credentials” | “script errors” | “TLS errors”]			
ตัวอย่างความต้องการ			
The **UP2ME** shall employ techniques that prevent immediate dismissal of user interfaces that used to inform users about security critical events or to solicit input by using a temporarily disabled "OK" button.			

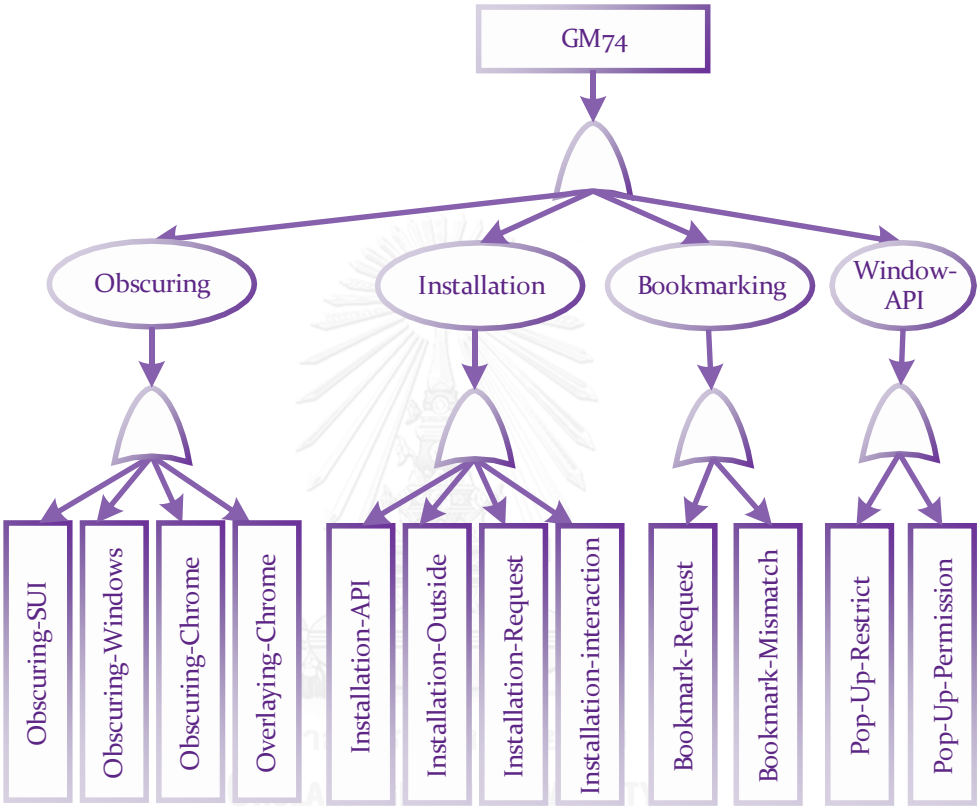
ตารางที่ ข.12 ไวยากรณ์กำหนดความต้องการด้านความมั่นคงสำหรับตัวแทนผู้ใช้เว็บที่รองรับส่วนต่อประสานโปรแกรมประยุกต์

ชื่อไวยากรณ์	กำหนดความต้องการด้านความมั่นคงสำหรับตัวแทนผู้ใช้เว็บที่รองรับส่วนต่อประสานโปรแกรมประยุกต์	**รหัสไวยากรณ์**	GM74
กลุ่มไวยากรณ์	แนวปฏิบัติที่ดีที่สุดสำหรับสภาพทนทานของระบบ		
เงื่อนไขก่อนการใช้	ต้องมีการนิยามข้อความเตือนภัยจากไวยากรณ์ 64 และการปรากฏของส่วนต่อประสานโครมที่แสดงสารสนเทศทางความมั่นคงจากไวยากรณ์ 71		
คำอธิบาย	ไวยากรณ์สำหรับกำหนดขอบเขตความสามารถของส่วนต่อประสานโปรแกรมประยุกต์ที่เรียกใช้โดยเนื้อหาเว็บ เพื่อให้เข้าใจถึงจุดอ่อนที่สามารถเสี่ยงต่อการนำส่วนต่อประสานโปรแกรมประยุกต์ของตัวแทนผู้ใช้เว็บไปใช้เพื่อโจมตีหรือขัดขวางการใช้งานของผู้ใช้		

ตารางที่ ข.12 ไวยากรณ์กำหนดความต้องการด้านความมั่นคงสำหรับตัวแทนผู้ใช้เว็บที่รองรับส่วนต่อประสานโปรแกรมประยุกต์ (ต่อ)

ชื่อไวยากรณ์	กำหนดความต้องการด้านความมั่นคงสำหรับตัวแทนผู้ใช้เว็บที่รองรับส่วนต่อประสานโปรแกรมประยุกต์	**รหัสไวยากรณ์**	GM74

แผนภาพต้นไม้ความมั่นคง



ไวยากรณ์ความมั่นคง

(1) **GM74** = [**Obscuring** | **Installation** | **Bookmark** | **Window-API**] ;

(2) **Web-User-Agent** = ?User define client name from beginning of the project? ;

(3) **Web-Server** = ?User define sever name from beginning of the project? ;

(4) **Obscuring** = [**Obscuring-SUI** | **Obscuring-Chrome**];

(5) **Obscuring-SUI** = **Web-User-Agent** , " shall not allow content from " , **Web-Server** , " to " , **Obscuring-Action** , { **Conjunction** , **Obscuring-Action**} , " security user interface. ", {**Obscuring-Windows**} ;

(6) **Obscuring-Action** = ["obscure" | "hidden" | "disable"];

(7) **Obscuring-Windows** = " Especially when opening new windows. ";

(8) **Obscuring-Chrome** = [**Restrict-Window** | **Overlaying-Chrome**];

ตารางที่ ข.12 ไวยากรณ์กำหนดความต้องการด้านความมั่นคงสำหรับตัวแทนผู้ใช้เว็บที่รองรับส่วนต่อประสานโปรแกรมประยุกต์ (ต่อ)

ชื่อไวยากรณ์	กำหนดความต้องการด้านความมั่นคงสำหรับตัวแทนผู้ใช้เว็บที่รองรับส่วนต่อประสานโปรแกรมประยุกต์	**รหัสไวยากรณ์**	GM74

(9) **Restrict-Window** = **Web-User-Agent** , “ shall restrict window” , **Window-Operations** , { **Conjunction** , **Window-Operations**} , “operations” , **Chrome-SCI** , “. ” ;

(10) **Window-Operations** = [“sizing” | “moving”];

(11) **Chrome-SCI** = “ to keep security chrome visible”; ?check for existing of Chrome-SCI from GM71?

(12) **Overlaying-Chrome** = **Web-User-Agent** , “ shall prevent ” , **Web-Server** , “ content from overlaying chrome. ”;

(13) **Installation** = [**Installation-API** | **Installation-Request** | **Installation-Interaction**];

(14) **Installation-API** = **Web-User-Agent** , “shall not expose programming interface which permit installation of software without the user's consent. ” , { “Including when ” , **Installation-Outside**} ;

(15) **Installation-Outside** = “the user agent is attempting to install software outside the agent environment as a result of web content. ” ;

(16) **Installation-Request** = **Web-User-Agent** “ shall inform user and request consent when ” , **Installation-Outside** , {**Installation-Interaction**};

(17) **Installation-Interaction** = “The warning message shall be used for the interaction.”; ?check for existing of Warning-Message from GM64?

(18) **Bookmark** = “When web content request to add ” , [**Bookmark-Request** | **Bookmark-Mismatch**]

(19) **Bookmark-Request** = “bookmarks, the ”, **Web-User-Agent** , “ shall request for explicit user consent.” ;

(20) **Bookmark-Mismatch** = “URIs to the bookmark collection. The ” , **Web-User-Agent** , “ shall not permit the URIs that do not match to the URI of the ” , **Web-Server** , “ that the user currently interacts with. ” ;

(21) **Window-API** = **Web-User-Agent** , “ that use a windowed interaction paradigm, ”, [**Pop-Up-Restrict** | **Pop-Up-Permission**] ;

(22) **Pop-Up-Restrict** = “shall restrict the opening of pop-up windows from the web content, particularly those not initiated by user.” ;

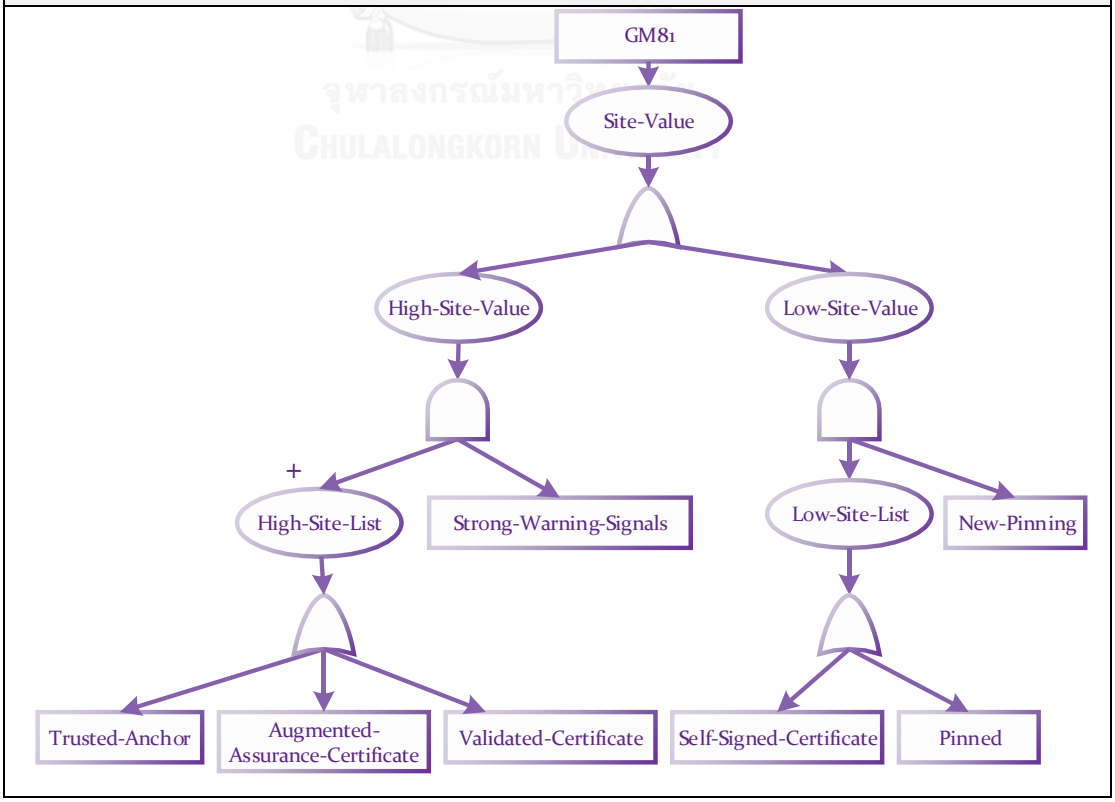
(23) **Pop-Up-Permission** = “shall offer a way to extend permission to individual trusted sites. ”;

ตารางที่ ข.12 ไวยากรณ์กำหนดความต้องการด้านความมั่นคงสำหรับตัวแทนผู้ใช้เว็บที่รองรับส่วนต่อประสานโปรแกรมประยุกต์

ชื่อไวยากรณ์	กำหนดความต้องการด้านความมั่นคงสำหรับตัวแทนผู้ใช้เว็บที่รองรับส่วนต่อประสานโปรแกรมประยุกต์	**รหัสไวยากรณ์**	GM74
ตัวอย่างความต้องการ			
UP2ME shall not expose programming interface which permit installation of software without the user's consent. Including when the user agent is attempting to install software outside the agent environment as a result of web content.			

ตารางที่ ข.13 ไวยากรณ์กำหนดการป้องกันการโจมตีด้วยใบรับรองระหว่างการเชื่อมต่อการรักษาความมั่นคงชั้นขนส่ง

ชื่อไวยากรณ์	กำหนดการป้องกันการโจมตีด้วยใบรับรองระหว่างการเชื่อมต่อการรักษาความมั่นคงชั้นขนส่ง	**รหัสไวยากรณ์**	GM81
กลุ่มไวยากรณ์	ข้อคำนึงด้านความมั่นคง		
เงื่อนไขก่อนการใช้	ต้องมีการกำหนดการจัดการใบรับรองจากไวยากรณ์ 51		
คำอธิบาย	ไวยากรณ์สำหรับกำหนดความต้องการเพื่อป้องกันการโจมตีระหว่างการเชื่อมต่อการรักษาความมั่นคง โดยกำหนดมูลค่าของผู้ให้บริการเว็บและการจัดการกับเว็บไซต์แต่ละมูลค่าตามประเภทของใบรับรอง		
แผนภาพต้นไม้ความมั่นคง			



ตารางที่ ข.13 ไวยากรณ์กำหนดการป้องกันการโจมตีด้วยใบรับรองระหว่างการเชื่อมต่อการรักษาความมั่นคงชั้นขนส่ง (ต่อ)

ชื่อไวยากรณ์	กำหนดการป้องกันการโจมตีด้วยใบรับรองระหว่างการเชื่อมต่อการรักษาความมั่นคงชั้นขนส่ง	**รหัสไวยากรณ์**	GM81

ไวยากรณ์ความมั่นคง

(1) **GM81** = **Web-User-Agent** , “ shall support the prior designation of ” , **Site-Value**;

(2) **Web-User-Agent** = ?User define client name from beginning of the project? ;

(3) **Site-Value** = [**High-Site-Value** | **Low-Site-Value**];

(4) **High-Site-Value** = “high-value sites, which ” , **High-Site-List** , {**Conjunction**, **High-Site-List**}, **TLS-Errors**, **Strong-Warning-Signal**;

(5) **High-Site-List** = [“Trust Anchor” | “Validated” | “Augmented Assurance”] ? The certificates were defined from GM51 ? ;

(6) **TLS-Errors** = “ Certificates are required. Handling with the TLS errors that ”;

(7) **Strong-Warning-Signals** = “leads to additional exposure during the first TLS interaction with the site by a strong warning signal.”;

(8) **Low-Site-Value** = “low-value sites, which ” , **Low-Site-List**, {**Conjunction**, **Low-Site-List**}, **TLS-Errors**, **New-Pinning**;

(9) **Low-Site-List** = [“Self-Signed” | “Pinned”] ?The certificates from GM51 ? ;

(10) **New-Pinning** = “could be a spoofing attack during the pinning of a new certificate to a destination by checking that DNS of a newly certificate is match to URI of the current site.”;

(11) **Conjunction** = [**Many** | **Last-One**];

(12) **Many** = “, ” ;

(13) **Last-One** = [“ and ” | “ or ”] ;

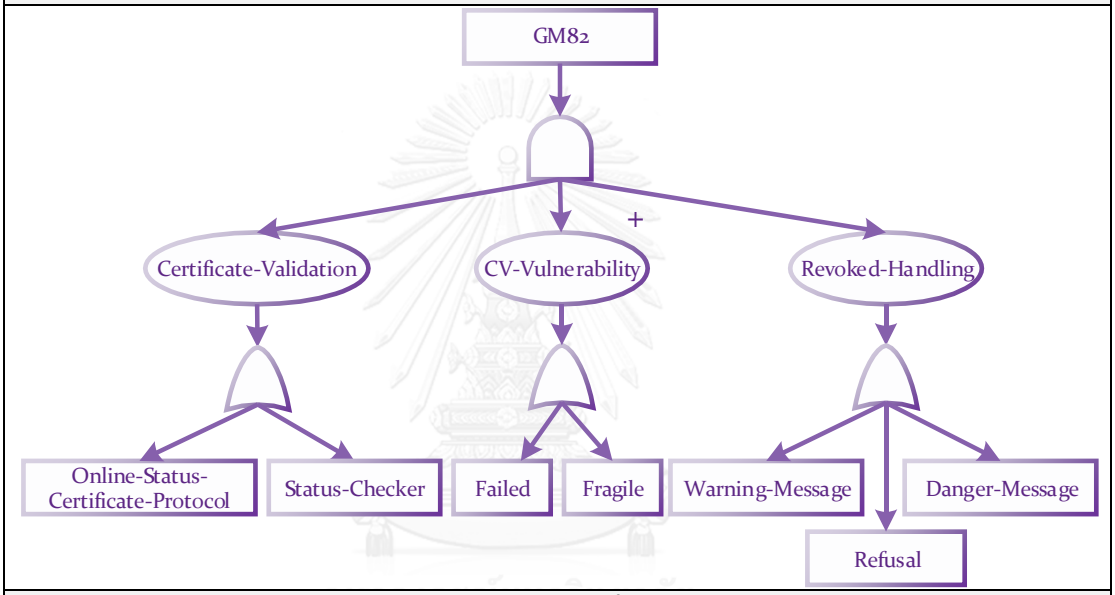
ตัวอย่างความต้องการ

Dolphin web browser shall support the prior designation of low-value site, which Self-Signed and Pinned Certificates are required, Handling with the TLS errors that could be a spoofing attack during the pinning of a new certificate to a destination by checking that DNS of a newly certificate is match to URI of the current site.

ตารางที่ ข.14 ไวยากรณ์ 82 การป้องกันการโจมตีการตรวจสอบสถานะใบรับรอง

ชื่อไวยากรณ์	การป้องกันการโจมตีการตรวจสอบสถานะใบรับรอง	**รหัสไวยากรณ์**	GM82
กลุ่มไวยากรณ์	ข้อคำนึงด้านความมั่นคง		
เงื่อนไขก่อนการใช้	ต้องมีการกำหนดการส่งสัญญาณข้อผิดพลาดจากไวยากรณ์ 64		
คำอธิบาย	ไวยากรณ์สำหรับกำหนดความต้องการเพื่อป้องกันการโจมตีการตรวจสอบความสมเหตุสมผลของใบรับรองด้วยการใช้ใบรับรองที่ถูกเพิกถอนอันก่อให้เกิดข้อผิดพลาดระหว่างการเชื่อมต่อการรักษาความมั่นคงนอกเหนือจากที่ได้ระบุไว้ในแบบรูป 54 โดยการกำหนดรูปแบบในการนำเสนอข้อมูลของข้อผิดพลาดที่เกิดขึ้นให้แก่ผู้ใช้		

แผนภาพต้นไม้ความมั่นคง



ไวยากรณ์ความมั่นคง

(1) **GM82** = “The development for ” , **Certificate-Validation** ,“ status checking is ” , **CV-Vulnerability** , {**Conjunction**, **CV-Vulnerability** } ,“, so the ”, **Web-User-Agent** , “ shall expose failures of certificate validation checks to user as ” , **Revoked-Handling** , “. ” ;

(2) **Certificate-Validation** = [“Online Certificate Status Protocol” | ?Defined new certificate status checker?];

(3) **CV-Vulnerability** = [“fragile”| “subject to frequent failures” | ?User define new vulnerability for certificate status checker?] ;

(4) **Revoked-Handling** = [“warning level message”| “danger level message” | “ refusal to load the sites that fail”] ? The Error-Signaling identified from GM64?;

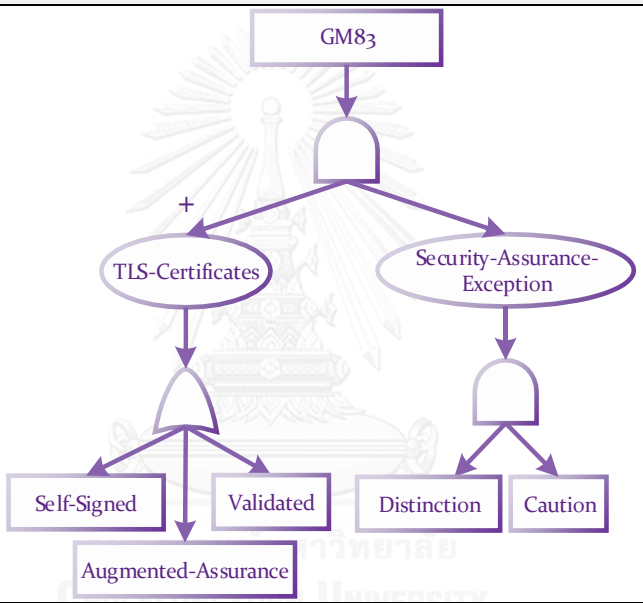
ตัวอย่างความต้องการ

The development for Online Certificate Status Protocol status checking is fragile and subject to frequent failures, so the UP2ME shall expose failures of certificate validation checks to user as danger level message.

ตารางที่ ข.15 ไวยากรณ์การกำหนดข้อยกเว้นในการประกันความมั่นคงของเว็บ

ชื่อไวยากรณ์	การกำหนดข้อยกเว้นในการประกันความมั่นคงของเว็บ	**รหัสไวยากรณ์**	GM83
กลุ่มไวยากรณ์	ข้อคำนึงด้านความมั่นคง		
เงื่อนไขก่อนการใช้	ใบรับรองที่เชื่อถือได้ต้องถูกนิยามไว้จากไวยากรณ์ 52		
คำอธิบาย	ตัวแทนผู้ใช้เว็บที่แสดงสถานะมั่นคงสำหรับเว็บไซต์ที่มีการรักษาความมั่นคงชั้นขนส่งโดยพิจารณาจากใบรับรองที่น่าเชื่อถือ แต่ข้อมูลจากใบรับรองไม่เพียงพอที่จะยืนยันได้ว่าเว็บไซต์ดังกล่าวนั้นปราศจากการโจมตี ผู้พัฒนาจึงต้องพิจารณาความแตกต่างระหว่างการใช้ใบรับรองเพื่อยืนยันอัตลักษณ์และการรักษาความมั่นคงของเว็บ โดยใช้ไวยากรณ์สำหรับกำหนดข้อยกเว้นการประกันความมั่นคงของเว็บ		

แผนภาพต้นไม้ความมั่นคง



ไวยากรณ์ความมั่นคง

(1) **GM83** = **Web-User-Agent** ,“ which indicates SSL/TLS connections as secure for the strong encryption of communication from ” , **TLS-Certificates-List** , “ presented by ” , **Web-Server** , “, but ” , **Security-Assurance-Exception** ,“ .”;

(2) **TLS-Certificates-List** = **TLS-Certificates** , {**Conjunction** , **TLS-Certificates**} , “ Certificate ” ;

(3) **Web-User-Agent** = ?User define client name from beginning of the project? ;

(4) **Web-Server** = [“any websites” | ?User define server name or select at least 1 from serverNameList of the project?] ;

(5) **TLS-Certificates** = [“Validated”| “Self-signed” | “Augmented Assurance”]; ? Check for the Trusted-Certificate from GM52 ?

(6) **Security-Assurance-Exception** = **Distinction** , “ so ” , **Caution** ;

(7) **Distinction** = “there are distinctions between identity and security”;

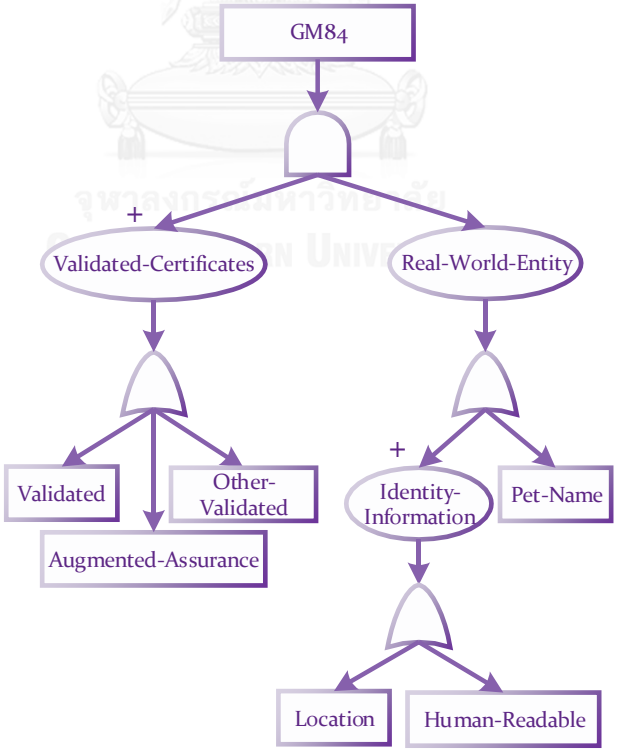
(8) **Caution** = “a site may not operate in a safe manner or subject to attack”;

ตารางที่ ข.15 ไวยากรณ์การกำหนดข้อยกเว้นในการประกันความมั่นคงของเว็บ (ต่อ)

ชื่อไวยากรณ์	การกำหนดข้อยกเว้นในการประกันความมั่นคงของเว็บ	**รหัสไวยากรณ์**	GM83
ตัวอย่างความต้องการ			
TripAdvisor which indicates SSL/TLS connections as secure for the strong encryption of communication from Self-signed certificate presented by Agoda.com, but there are distinctions between identity and security so a site may not operate in a safe manner or subject to attack.			

ตารางที่ ข.16 ไวยากรณ์การกำหนดข้อมูลอัตลักษณ์ที่สอดคล้องกับโลกความจริง

ชื่อไวยากรณ์	การกำหนดข้อมูลอัตลักษณ์ที่สอดคล้องกับโลกความจริง	**รหัสไวยากรณ์**	GM84
กลุ่มไวยากรณ์	ข้อคำนึงด้านความมั่นคง		
เงื่อนไขก่อนการใช้	รายการใบรับรองที่ผ่านการตรวจสอบความสมเหตุสมผลจากไวยากรณ์ 52		
คำอธิบาย	เว็บลอกเลียนมักใช้ชื่อโดเมนคล้ายกับชื่อเว็บที่ได้รับความนิยมเพื่อสร้างความสับสนและล่อลวงผู้ใช้ให้เข้าสู่เว็บของผู้โจมตี ไวยากรณ์นี้จึงสนับสนุนการกำหนดข้อมูลอัตลักษณ์ที่สอดคล้องกับโลกความจริงเพื่อแสดงความสัมพันธ์ระหว่างชื่อโดเมนของเว็บและข้อมูลที่ผู้ใช้คุ้นเคย ให้ผู้ใช้ได้พิจารณาเลือกเว็บไซต์ที่ได้รับสิทธ์อย่างถูกต้อง		
แผนภาพต้นไม้ความมั่นคง			



ตารางที่ ข.16 ไวยากรณ์การกำหนดข้อมูลอัตลักษณ์ที่สอดคล้องกับโลกความจริง (ต่อ)

ชื่อไวยากรณ์	การกำหนดข้อมูลอัตลักษณ์ที่สอดคล้องกับโลกความจริง	**รหัสไวยากรณ์**	GM84

ไวยากรณ์ความมั่นคง

(1) **GM84** = “The ”, **Web-User-Agent** ,“ shall support the binding between domain name/certificate and the actual real-world entity of ” , **Validated-Certificates-List** , “ from ” , **Web-Server** , “ including the identity information such as ” , **Real-World-Entity** ,“. ”;

(2) **Web-User-Agent** = ?User define client name from beginning of the project? ;

(3) **Web-Server** = [“any websites” | ?User define server name or select at least 1 from serverNameList of the project?] ;

(4) **Validated-Certificates-List** = **Validated-Certificates** , {**Conjunction** , **Validated-Certificates**} , “ Certificate ” ;

(5) **Validated-Certificates** = [“Validated”| “other Validated” | “Augmented Assurance”]; ? Check for the Trusted-Certificate from GM52 ?

(6) **Real-World-Entity** = [**Identity-Information-List** | **Pet-Name**];

(7) **Identity-Information-List** = **Identity-Information** , {**Conjunction** , **Identity-Information**} , “ information” ;

(8) **Identity-Information** = [“location” | “human readable” | ?Define new real world identity information?];

(9) **Pet-Name** = “a Petname”;

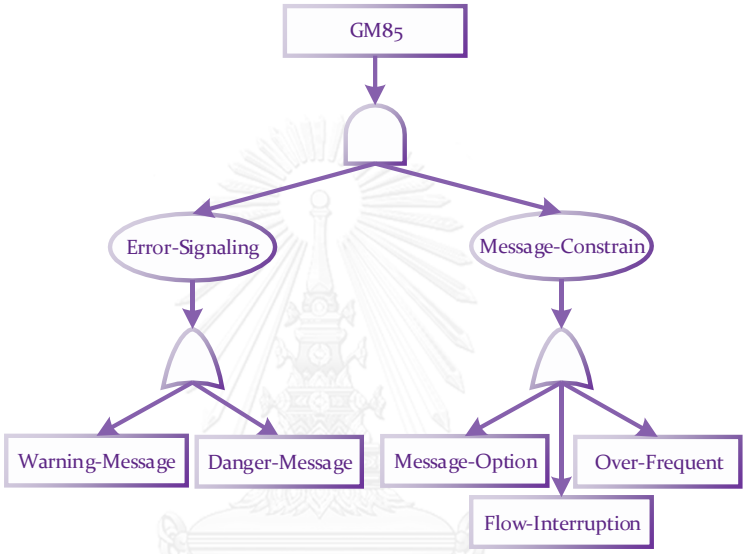
ตัวอย่างความต้องการ

The UP2ME shall support the binding between domain name/certificate and the actual real-world entity of Validated Certificate from the SCBeasy.net including the identity information such as a Petname.

ตารางที่ ข.17 ไวยากรณ์การกำหนดข้อจำกัดของข้อความแจ้งเตือน

ชื่อไวยากรณ์	การกำหนดข้อจำกัดของข้อความแจ้งเตือน	**รหัสไวยากรณ์**	GM85
กลุ่มไวยากรณ์	ข้อคำนึงด้านความมั่นคง		
เงื่อนไขก่อนการใช้	ต้องมีการกำหนดการส่งสัญญาณข้อผิดพลาดจากไวยากรณ์ 64		
คำอธิบาย	ข้อความแจ้งเตือนระดับต่างๆ มีความสำคัญต่อการนำเสนอข้อมูลแก่ผู้ใช้ แต่ผู้ใช้เคยชินต่อการละเลยข้อความดังกล่าว ไวยากรณ์นี้จึงกำหนดคุณลักษณะของข้อความแจ้งเตือนแต่ละประเภทเพื่อช่วยให้ข้อความแจ้งเตือนดังกล่าวทำงานได้อย่างมีประสิทธิภาพมากยิ่งขึ้น		

แผนภาพต้นไม้ความมั่นคง



ไวยากรณ์ความมั่นคง

(1) **GM85** = **Web-User-Agent** , “ shall ” , **Message-Constrain**,“ the ” , **Error-Signaling** , “. ”;

(2) **Web-User-Agent** = ?User define client name from beginning of the project? ;

(3) **Error-Signaling** = [“Warning Message” | “Danger Message”]; ?Check for existing of Error-Signaling from GM64?

(4) **Message-Constrain** = [**Message-Option** | **Over-Frequent** | **Flow-Interruption**];

(5) **Message-Option** = “phrase options in these message in terms of the action taken rather than using generic labels for” ;

(6) **Over-Frequent** = “constrain the number of”;

(7) **Flow-Interruption** = “effectively interrupt the user's task flow for”;

(8) **Conjunction** = [**Many** | **Last-One**];

(9) **Many** = “, ” ;

(10) **Last-One** = [“ and ” | “ or ”] ;

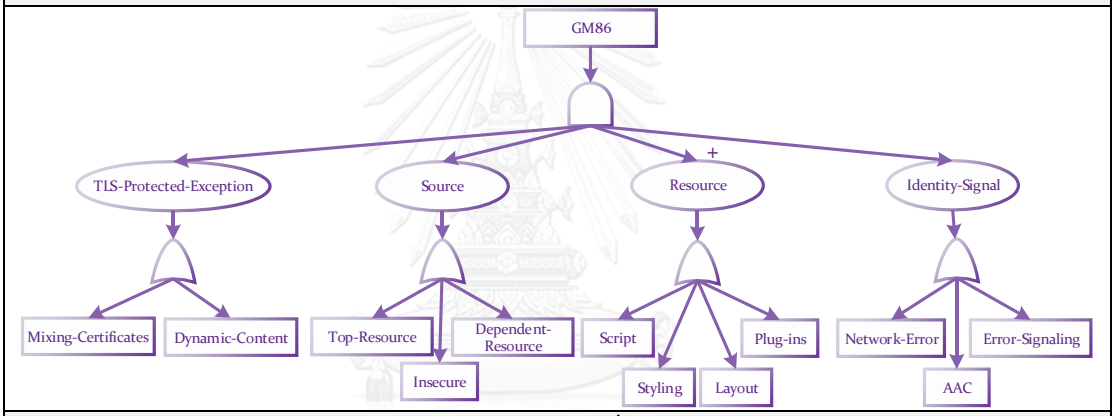
ตัวอย่างความต้องการ

TripAdvisor shall constrain the number of the Warning Message.

ตารางที่ ข.18 ไวยากรณ์การกำหนดสัญญาณอัตลักษณ์ของเว็บที่มีการเปลี่ยนแปลงเนื้อหาระหว่างการรักษาความมั่นคงชั้นขนส่ง

ชื่อไวยากรณ์	การกำหนดสัญญาณอัตลักษณ์ของเว็บที่มีการเปลี่ยนแปลงเนื้อหาระหว่างการรักษาความมั่นคงชั้นขนส่ง	**รหัสไวยากรณ์**	GM86
กลุ่มไวยากรณ์	ข้อคำนึงด้านความมั่นคง		
เงื่อนไขก่อนการใช้	ระดับความมั่นคงของเว็บจากไวยากรณ์ 52 และการจัดการข้อผิดพลาดจากไวยากรณ์ 64 ต้องถูกกำหนดไว้		
คำอธิบาย	ไวยากรณ์สำหรับกำหนดการส่งสัญญาณอัตลักษณ์ของเว็บที่มีการปกป้องข้อมูลด้วยการรักษาความมั่นคงชั้นขนส่งที่แข็งแกร่งแต่มีการเปลี่ยนแปลงเนื้อหาระหว่างการรักษาความมั่นคงชั้นขนส่ง		

แผนภาพต้นไม้ความมั่นคง



ไวยากรณ์ความมั่นคง

(1) **GM86** = “The ”, **Web-User-Agent** , “ that has loaded two Web pages the first page was retrieved, an Augmented Assurance Certificate was used by the TLS session. ” , **TLS-Protected-Exception**, “ content such as ” , **Resource-List** , “ from the ”, **Source** , “. The” , **Identity-Signal** , “ are expressed by the indicators of identity signal.”;

(2) **Web-User-Agent** = ?User define client name from beginning of the project? ;

(3) **TLS-Protected-Exception** = [**Mixing-Certificates** | **Dynamic-Content**]; ?Check for existing of TLS-Protected from GM52?

(4) **Mixing-Certificates** = “When the second page was retrieved, under the control of”;

(5) **Dynamic-Content** = “The security properties will not change in a significant way once it has finished loading. Dynamic pages can load”;

(6) **Source** = [**Top-Resource** | **Dependent-Resource** | **Insecure**];

(7) **Top-Resource** =“top level resource vouches for the content of all dependent resources”;

(8) **Dependent-Resource** = “dependent resources using validated certificates”;

ตารางที่ ข.18 ไวยากรณ์การกำหนดสัญญาณอัตลักษณ์ของเว็บที่มีการเปลี่ยนแปลงเนื้อหาระหว่างการรักษาความมั่นคงชั้นขนส่ง (ต่อ)

ชื่อไวยากรณ์	การกำหนดสัญญาณอัตลักษณ์ของเว็บที่มีการเปลี่ยนแปลงเนื้อหาระหว่างการรักษาความมั่นคงชั้นขนส่ง	**รหัสไวยากรณ์**	GM86
(9) **Insecure** = “insecure web site”; (10) **Resource-List** = **Resource** , {**Conjunction** , **Resource**} ; (11) **Resource** = [“external script” | “styling” | “layout” | “plug-ins”] ; (12) **Identity-Signal** = [**Network-Error** | **Error-Signaling** | **AAC**]; (13) **Network-Error** = “network error for the different security presentation of the two pages”; (14) **Error-Signaling** = [“warning message” | “danger message”]; ?Check for existing of the Error-Signaling from **GM64** ? (15) **AAC** = “identity information of the owner and author of the Web page from Augmented Assurance Certificates”; (16) **Conjunction** = [**Many** | **Last-One**]; (17) **Many** = “, ” ; (18) **Last-One** = [“ and ” | “ or ”] ;			
ตัวอย่างความต้องการ			
The TripAdvisor that has loaded two Web pages the first page was retrieved, an Augmented Assurance Certificate was used by the TLS session. When the second page was retrieved, under the control of content such as external script and plug-ins from the top level resource vouches for the content of all dependent resources. The network error for the different security presentation of the two pages are expressed by the indicators of identity signal.			

ภาคผนวก ค

แบบสอบถาม

ค.1 แบบประเมินความสมเหตุสมผลของแบบรูปบริบทความมั่นคงเชิง

คำถามเกี่ยวกับข้อมูลเบื้องต้นของผู้ตอบแบบสอบถาม

คำชี้แจง โปรดทำเครื่องหมาย ✓ ลงใน ☐ ที่ตรงตามความเป็นจริงเกี่ยวกับตัวท่านมากที่สุด

1. สถานภาพนิสิต

   1) ☐ นิสิตภาคในเวลาราชการ 2) ☐ นิสิตภาคนอกเวลาราชการ

2. ระดับผลการเรียนวิชาความมั่นคงด้านสารสนเทศ (Information Security)

   1) ☐ A 2) ☐ B+ 3) ☐ B

3. ประสบการณ์การทำงานด้านความมั่นคงของซอฟต์แวร์/ระบบ

   1) ☐ น้อยกว่า 2 ปี 2) ☐ 3 – 5 ปี 3) ☐ มากกว่า 5 ปี

4. ตำแหน่งงานปัจจุบันด้านเทคโนโลยีสารสนเทศ (Information Technology: IT) ของท่าน (เลือกได้มากกว่า 1 ข้อ)

   1) ☐ System/ Network Engineer 2) ☐ Business/ System Analyst

   3) ☐ Programmer/ Software Engineer 4) ☐ Project Manager

   5) ☐ Quality Assessor/ Tester 6) ☐ Database Administrator

   7) ☐ อื่นๆ.....

5. ตำแหน่งงานในอดีตด้านเทคโนโลยีสารสนเทศ (IT) ของท่าน (เลือกได้มากกว่า 1 ข้อ)

   1) ☐ System/ Network Engineer 2) ☐ Business/ System Analyst

   3) ☐ Programmer/ Software Engineer 4) ☐ Project Manager

   5) ☐ Quality Assessor/ Tester 6) ☐ Database Administrator

   7) ☐ อื่นๆ.....

6. คะแนนผลการสอบภาษาอังกฤษ

   1) ☐ CU-TEP.....คะแนน 2) ☐ TOEFL.....คะแนน

   3) ☐ TOEIC.....คะแนน 4) ☐ อื่นๆ โปรดระบุ.....

คำถามเพื่อใช้ประเมินความสมเหตุสมผลของแบบรูปที่รวบรวมผลเฉยจากมาตรฐาน

โปรดทำเครื่องหมาย ✓ลงในตารางทางขวามือที่ตรงกับระดับความคิดเห็นของท่านมากที่สุด โดย

5 = เห็นด้วยเป็นอย่างยิ่ง 4 = เห็นด้วย 3 = ปานกลาง

2 = ไม่เห็นด้วย 1 = ไม่เห็นด้วยเป็นอย่างยิ่ง

ลำดับ	คำถาม	5	4	3	2	1
1. ความคิดเห็นต่อภาพรวมของเอกสารแบบรูปที่นำเสนอ						
1.1.	เอกสารแบบรูปที่นำเสนอแบ่งส่วนเนื้อหาได้อย่างเหมาะสม					
1.2.	ก่อนได้รับคำอธิบาย ผู้ประเมินมีความเข้าใจเกี่ยวกับที่มาและความสำคัญของแบบรูป					
1.3.	หลังได้รับคำอธิบาย ผู้ประเมินมีความเข้าใจเกี่ยวกับที่มาและความสำคัญของแบบรูป					
1.4.	ก่อนได้รับคำอธิบาย ผู้ประเมินเข้าใจเนื้อหาของเอกสารคำแนะนาส่วนต่อประสานผู้ใช้ด้านบริบทความมั่นคงเชิงเว็บหรือดับเบิ้ลยูเอสซียูไอ (WSC-UI) ที่ใช้ในการสร้างแบบรูป					
1.5.	หลังได้รับคำอธิบายผู้ประเมินเข้าใจเนื้อหาของเอกสารคำแนะนาส่วนต่อประสานผู้ใช้ด้านบริบทความมั่นคงเชิงเว็บหรือดับเบิ้ลยูเอสซียูไอ (WSC-UI) ที่ใช้ในการสร้างแบบรูป					
1.6.	ผู้ประเมินเข้าใจโครงสร้างและส่วนประกอบที่ใช้ในการสร้างแบบรูป					
1.7.	ภาพรวมและความสัมพันธ์ระหว่างแบบรูปง่ายต่อการทำความเข้าใจ					
2. ความคิดเห็นต่อเนื้อหาของแบบรูป						
2.1.	เนื้อหาของแบบรูปมีความชัดเจน ง่ายต่อการทำความเข้าใจ					
2.2.	เนื้อหาของแบบรูปสอดคล้องตามองค์ความรู้ด้านความมั่นคง					
2.3.	แบบรูปได้ระบุปัญหาและรวมรวบผลเฉลยที่สอดคล้องกัน					
2.4.	แผนภาพคลาสแสดงโครงสร้างภายในของแบบรูปได้สะท้อนปัญหาและผลเฉลย					
2.5.	ตัวอย่างของแบบรูปแสดงปัญหาและการแก้ไขได้ชัดเจน ง่ายต่อการทำความเข้าใจ					

ลำดับ	คำถาม	5	4	3	2	1
3. ความคิดเห็นที่มีต่อการนำแบบรูปไปประยุกต์ใช้						
3.1	แบบรูปที่นำเสนอง่ายต่อการทำความเข้าใจและการนำไปประยุกต์ใช้เมื่อเทียบกับเอกสารมาตรฐานบริบทความมั่นคงเชิงเว็บ (WSC-UI)					
3.2	แบบรูปที่นำเสนอช่วยให้ท่านมีความเข้าใจในการประยุกต์ใช้คำแนะนำด้านความมั่นคงของตัวแทนผู้ใช้เว็บมากขึ้น					
3.3	แบบรูปที่นำเสนอมีประโยชน์ต่อการวิเคราะห์/ออกแบบด้านความมั่นคงของระบบ					

ข้อเสนอแนะเกี่ยวกับโครงสร้างและส่วนประกอบของแบบรูป

.....

.....

.....

ข้อเสนอแนะเกี่ยวกับเนื้อหาที่ใช้อธิบายในแบบรูป

.....

.....

.....

ข้อเสนอแนะโดยรวม

.....

.....

.....

ข้อเสนอแนะเพิ่มเติม

.....

.....

.....

ค.2 แบบประเมินการทดสอบเครื่องมือสำหรับกำหนดความต้องการความมั่นคง

ส่วนที่ 1 คำถามเกี่ยวกับข้อมูลเบื้องต้นของผู้ตอบแบบสอบถาม

คำชี้แจงส่วนที่ 1 โปรดทำเครื่องหมาย ✓ ลงใน ☐ ที่ตรงตามความเป็นจริงเกี่ยวกับตัวท่านมากที่สุด

1. สถานภาพนิสิต

1) ☐ นิสิตภาคในเวลาราชการ 2) ☐ นิสิตภาคนอกเวลาราชการ

2. ระดับผลการเรียนวิชาความมั่นคงด้านสารสนเทศ (Information Security)

1) ☐ A 2) ☐ B+ 3) ☐ B

3. ระดับผลการเรียนวิชาวิศวกรรมความต้องการซอฟต์แวร์ (Software Requirements Engineering)

1) ☐ A 2) ☐ B+ 3) ☐ B

4. ประสบการณ์การทำงานด้านความมั่นคงของซอฟต์แวร์/ระบบ

1) ☐ น้อยกว่า 2 ปี 2) ☐ 3 – 5 ปี 3) ☐ มากกว่า 5 ปี

5. ตำแหน่งงานปัจจุบันด้านเทคโนโลยีสารสนเทศ (Information Technology: IT) ของท่าน (เลือกได้มากกว่า 1 ข้อ)

1) ☐ System/ Network Engineer 2) ☐ Business/ System Analyst 3) ☐ Programmer/Software Engineer
4) ☐ Project Manager 5) ☐ Quality Assessor/Tester 6) ☐ Database Administrator
7) ☐ อื่นๆ.....

6. ตำแหน่งงานในอดีตด้านเทคโนโลยีสารสนเทศ (IT) ของท่าน (เลือกได้มากกว่า 1 ข้อ)

1) ☐ System/ Network Engineer 2) ☐ Business/ System Analyst 3) ☐ Programmer/Software Engineer
4) ☐ Project Manager 5) ☐ Quality Assessor/Tester 6) ☐ Database Administrator
7) ☐ อื่นๆ.....

7. ความถนัดด้านการเขียนภาษาอังกฤษ

1) ☐ เชี่ยวชาญ 2) ☐ ปานกลาง 3) ☐ ไม่ถนัด

ส่วนที่ 2 คำถามเพื่อระบุความต้องการความมั่นคง

คำชี้แจงส่วนที่ 2 โปรดระบุความต้องการความมั่นคงตามหัวข้อที่กำหนดจากสถานการณ์ดังนี้

1. จากแบบรูป 51 (ศึกษาได้จากส่วนที่ 4 ของเอกสารประเมินฉบับนี้) โปรดระบุความต้องการของการจัดการใบรับรองของเว็บที่ให้บริการข้อมูลแก่ระบบต่อไปนี้

ระบบให้คำปรึกษาด้านการเดินทาง (TripAdvisor) โดยผู้ใช้สืบค้นสำหรับราคาตั๋วเครื่องบิน โรงแรม ร้านอาหาร จากนั้นระบบจะค้นคืนข้อมูลจากแหล่งผู้ให้บริการเว็บที่หลากหลากภายนอกระบบเพื่อเปรียบเทียบราคาและข้อเสนอที่ดีที่สุด ซึ่งการทำรายการอาจเชื่อมโยงไปยังการทำธุรกรรมและข้อมูลสำคัญของผู้ใช้ หรือนำพาผู้ใช้ไปสู่เว็บไซต์ภายนอกระบบอันเสี่ยงต่อการโจมตี ผู้ให้บริการเว็บที่ติดต่อด้วย เช่น Agoda.com, Booking.com หรือ Hotels.com

1.1 โปรดระบุความต้องการของการจัดการใบรับรองของเว็บที่ให้บริการข้อมูลด้วยมือ

บันทึกเวลาในการเริ่มต้นระบุความต้องการ _____

_____

_____

_____

_____

_____

_____

บันทึกเวลาในการสิ้นสุดการระบุความต้องการ _____

1.2 ระยะเวลาที่ใช้ในการระบุความต้องการด้วยมือทั้งหมด _____นาที

1.3 โปรดระบุความต้องการของการจัดการใบรับรองของเว็บด้วยเครื่องมือและบันทึกผลผ่านระบบ บันทึกเวลาในการเริ่มต้นระบุความต้องการ_____

บันทึกเวลาในการสิ้นสุดการระบุความต้องการ_____

ระยะเวลาที่ใช้ในการระบุความต้องการด้วยเครื่องมือทั้งหมด _____นาที

1.4 ตามความเห็นของท่านผลลัพธ์ความต้องการที่ระบุด้วยมือและเครื่องมือมีความแตกต่างกันหรือไม่ อย่างไร

_____

_____

2. จากแบบรูป 71 (ศึกษาได้จากส่วนที่ 4 ของเอกสารประเมินฉบับนี้) โปรดระบุความต้องการของส่วนต่อประสานผู้ใช้โครมของระบบต่อไปนี้

ดอล์ฟินเว็บเบราว์เซอร์ (Dolphin Web Browser) เป็นโปรแกรมสำหรับค้นดูเว็บและสืบค้นข้อมูลบนอินเตอร์เนต ซึ่งไม่จำกัดระดับความปลอดภัยแต่สามารถตรวจสอบระดับความน่าเชื่อถือของเว็บและแจ้งเตือนความผิดปกติให้แก่ผู้ใช้ได้ กับผู้ให้บริการเว็บที่ติดต่อด้วยทุกเว็บ

2.1 โปรดระบุความต้องการของการจัดการใบรับรองของเว็บที่ให้บริการข้อมูลด้วยมือ

บันทึกเวลาในการเริ่มต้นระบุความต้องการ _____

_____

_____

_____

_____

_____

_____

บันทึกเวลาในการสิ้นสุดการระบุความต้องการ _____

2.2 ระยะเวลาที่ใช้ในการระบุความต้องการด้วยมือทั้งหมด _____นาที

2.3 โปรดระบุความต้องการของการจัดการใบรับรองของเว็บด้วยเครื่องมือและบันทึกผลผ่านระบบ บันทึกเวลาในการเริ่มต้นระบุความต้องการ_____

บันทึกเวลาในการสิ้นสุดการระบุความต้องการ_____

ระยะเวลาที่ใช้ในการระบุความต้องการด้วยเครื่องมือทั้งหมด _____นาที

2.4 ตามความเห็นของท่านผลลัพธ์ความต้องการที่ระบุด้วยมือและเครื่องมือมีความแตกต่างกันหรือไม่ อย่างไร

_____

_____

_____

ส่วนที่ 3 คำถามเพื่อประเมินเครื่องมือระบุความต้องการความมั่นคง

คำชี้แจงส่วนที่ 3 โปรดทำเครื่องหมาย □ ลงในตารางทางขวามือที่ตรงกับระดับความคิดเห็นของท่านมากที่สุด โดย 5 = เห็นด้วยเป็นอย่างยิ่ง 4 = เห็นด้วย 3 = ปานกลาง 2 = ไม่เห็นด้วย หรือ 1 = ไม่เห็นด้วยเป็นอย่างยิ่ง

ลำดับ	คำถาม	5	4	3	2	1
1.	**ความคิดเห็นต่อคุณภาพของรายการความต้องการความมั่นคงที่ได้จากเครื่องมือ**					
1.1	เครื่องมือช่วยในการกำหนดความต้องการได้ครบถ้วนมากกว่าการกำหนดด้วยตนเอง					
1.2	เครื่องมือช่วยในการกำหนดความต้องการได้ถูกต้องมากกว่าการกำหนดด้วยตนเอง					
1.3	เครื่องมือช่วยลดความกำกวมในการกำหนดความต้องการได้มากกว่ากำหนดด้วยตนเอง					
2.	**ความคิดเห็นต่อคุณสมบัติของเครื่องมือ**					
2.1	เครื่องมือสนับสนุนการใช้ซ้ำของความต้องการความมั่นคงได้					
2.2	เครื่องมือช่วยสนับสนุนการกำหนดความต้องการความมั่นคงอย่างเป็นลำดับ					
2.3	เครื่องมือช่วยลดความยุ่งยากในการกำหนดความต้องการความมั่นคง					
3.	**ความคิดเห็นต่อเครื่องมือด้านประโยชน์จากใช้งาน**					
3.1	เครื่องมือช่วยให้เกิดความเข้าใจเกี่ยวกับการกำหนดความต้องการความมั่นคงมากขึ้น					
3.2	เครื่องมือใช้เวลาในการกำหนดความต้องการความมั่นคงน้อยกว่าการกำหนดด้วยตนเอง					
3.3	เครื่องมือใช้กำหนดความต้องการความมั่นคงโดยได้ดีกว่าการกำหนดด้วยตนเอง					

ข้อเสนอแนะเพิ่มเติม

.....

.....

.....

.....

ภาคผนวก ง
รายการปรับปรุงแบบรูป

คำแนะนำที่ได้จากการประเมินแบบรูปบริบทความมั่นคงเชิงเว็บของทุกหน่วยทดลองจะถูกรวบรวมและนำมาพิจารณาเพื่อปรับปรุงแบบรูป รายการคำแนะนำแบ่งเป็นด้านภาษาและการใช้คำ ด้านเนื้อหาและองค์ความรู้ด้านความมั่นคง และด้านการออกแบบแผนภาพคลาสเพื่อสะท้อนแนวทางการแก้ไข นำไปสู่รายการการปรับปรุงแบบรูปสรุปได้ดังตารางที่ ง.1

ตารางที่ ง.1 รายการคำแนะนำและการปรับปรุงแบบรูป

ลำดับ	รายการคำแนะนำ	การปรับปรุง
ด้านโครงสร้างและส่วนประกอบของแบบรูป		
1	หากเป็นไปได้ อยากให้จัดเรียงลำดับหัวข้อภายใน Pattern ใหม่ เพื่อให้เนื้อหามีความร้อยเรียง และผู้ใช้สามารถทำความเข้าใจได้ง่ายขึ้น เช่น ย้ายหัวข้อ Example มาไว้ถัดจากหัวข้อ Problem เป็นต้น	ปรับปรุง
2	แบบรูปช่วยให้เห็นภาพรวมได้ดี แต่ทำความเข้าใจได้ยากนิดหน่อย เพราะต้องอ่านเนื้อหาก่อนถึงจะเข้าใจได้ดีขึ้น	ไม่กระทบ
3	โครงสร้างง่ายต่อการทำความเข้าใจหรือใช้ในการศึกษา ซึ่งไม่มาก/น้อยจนเกินไป	ไม่กระทบ
ด้านความครบถ้วนและความต้องกันของเอกสารต้นฉบับเทียบกับเนื้อหาของแบบรูป		
4	ตามรอย S018, S079 และ S080 ไม่ปรากฏในเอกสารแบบรูป	แก้ไขแบบรูป 61
5	S098 และ S104 เนื้อหาบางส่วนขาดหายไป	แก้ไขแบบรูป 62
6	S106 ถึง S111 เป็น Solution ที่กระจายไว้ในแบบรูป แต่ไม่ได้ระบุใน Part of pattern	ปรับปรุงตารางการตามรอย
7	S163, S167 consequence part ไม่ปรากฏอยู่ในแบบรูป	แก้ไขแบบรูป 74
ด้านการใช้ภาษา		
8	ควรตรวจสอบคำผิด การเขียนคำเชื่อม/ประโยค และแก้ไขให้ถูกต้อง	ตรวจสอบแล้ว
9	ควรตรวจสอบการเว้นวรรคประโยคและแก้ไขให้อ่านง่ายขึ้น	ตรวจสอบแล้ว
10	เนื่องด้วยการนำเสนอเนื้อหาได้ใช้คำศัพท์ทางเทคนิค จึงทำให้การเรียบเรียงประโยคค่อนข้างทำความเข้าใจได้ยาก แม้ว่าจะมีตารางคำศัพท์ที่ระบุความหมายก็ตาม ดังนั้นจึง - ควรใช้คำแปลภาษาไทยจากใจความหลักของเนื้อหาที่สื่อ เช่น แบบรูป 74 software installation เปลี่ยนใช้คำที่เข้าใจมากกว่านี้ - ควรใช้คำทับศัพท์ในบางคำที่เป็นพื้นฐาน หรือ ภาษาอังกฤษวงเล็บกำกับให้ เช่น แบบรูป 61 ทุติยภูมิของตัวแทนผู้ใช้	ใช้วงเล็บภาษาอังกฤษกำกับ

ตารางที่ ง.1 รายการคำแนะนำและการปรับปรุงแบบรูป (ต่อ)

ลำดับ	รายการคำแนะนำ	การปรับปรุง
11	ควรดูความสอดคล้องของคำศัพท์ของภาษาไทยที่แปลมาใช้ตลอดทั้งแบบรูปนั้น เช่น แบบรูป 71 โทรศัพท์เคลื่อนที่/อุปกรณ์มือถือ เลือกใช้คำใดคำหนึ่งแล้วใช้อธิบายไปตลอด	แก้ไขโดยเลือกคำใช้คำที่สอดคล้อง
ด้านการอธิบายเนื้อหาของแบบรูป		
12	ตัวแทนผู้ใช้เว็บแสดงตัวชี้บอกความมั่นคงชั้นขนส่งของเว็บไซต์ที่แท้จริง - จะทราบได้อย่างไรว่าเว็บไหนคือเว็บที่แท้จริง	เพิ่มการตรวจสอบเว็บไซต์ที่แท้จริงในแบบรูปที่ 63
13	แบบรูป 73 ส่วนของ Solution อาจจะเพิ่มเนื้อหาเป็นขั้นตอนอย่างชัดเจน เป็นข้อ 1,2...	แบ่งลำดับผลเฉลยของแบบรูป 73
14	ผลเฉลยไม่สอดคล้องกับประเด็นปัญหา เขียนป้องกันเรื่องพฤติกรรมของผู้ใช้ด้วย	ปรับปรุงผลเฉลยของแบบรูป 85
15	แบบรูป 73 เพิ่มเติม การแก้ไข solution ไม่ชัดเจนหากการจัดการของตัวแทนผู้ใช้ หรือ CA จะเป็นผู้จัดการ pop-up ที่เกิดขึ้น	ปรังปรุงผลเฉลยของแบบรูป 73
16	แบบรูป 71 Solution มีการแก้ไขจากการดัดแปลงและการเปลี่ยนแปลงจาก web responsive ควรแยกเคสระหว่างการดัดแปลง web หรือ web responsive หรือไม่	ไม่กระทบขอบเขตสำหรับ web responsive
17	แบบรูป 54 เงื่อนไขที่ 7 ควรเขียนชี้แจงว่าเงื่อนไขข้อผิดพลาดใดที่ผู้ใช้จะเป็นคนตัดสินใจว่าจะไม่เข้า หรือตัวแทนผู้ใช้เป็นคนตัดสินใจ	ระบุให้ตัดสินโดยผู้ใช้ในแบบรูป 54
18	แบบรูป 64 error handling ควรจะต้องครอบคลุมมากกว่านี้ message อาจไม่เพียงพอกับการแจ้งเตือน	ขึ้นอยู่กับการออกแบบระบบ

ตารางที่ ง.1 รายการคำแนะนำและการปรับปรุงแบบรูป (ต่อ)

ลำดับ	รายการคำแนะนำ	การปรับปรุง
ด้านความต้องกันของแผนภาพคลาสแสดงแบบจำลองเชิงโครงสร้างและผลเฉลยของแบบรูป		
19 19 (ต่อ)	แบบรูป 51 ควรทบทวนเส้นความสัมพันธ์ของ 5 class ดังนี้ 1) Certificates 2) TrustAnchor 3) ValidatedCertificate 4) SelfSignedCertificate 5) AugmentedAssuranceCertificate โดยโครงสร้างใน Class Diagram ระหว่าง Certificates กับ ValidatedCertificate ที่มีความสัมพันธ์แบบ Generalization กับ AugmentedAssuranceCertificate นั้นควรจะลบเส้นระหว่าง Certificate<-Augmented เนื่องจาก Augment รับทอดคุณสมบัติจาก Validated ซึ่งรับทอดจาก Cert อยู่แล้ว - ปรับรูปโครงสร้าง Class Diagram	ปรับปรุงความสัมพันธ์ระหว่างคลาสของแบบรูป 51
20	แบบรูป 64 ควรทบทวนเส้นความสัมพันธ์ของ class - Indicator - ErrorIndicator - PrimaryUserInterface เนื่องจากเส้นความสัมพันธ์ซ้อนทับกับเส้นขอบทำให้เกิดความกำกวม	จัดเรียงคลาสเพื่อให้เส้นความสัมพันธ์ไม่ซ้อนทับกัน
21	ตรวจสอบ Object ใน Diagram กับคำบรรยายว่ามีครบตรงกัน มีบางกรณีตัวอย่างมี จำนวน Object ไม่ตรงกัน เช่น แบบรูป 71 Class ดังต่อไปนี้ไม่ปรากฏ - Button - InformationBar - WebUserAgent - UserInterfaces	เพิ่มคลาสในแผนภาพเพื่อให้ครบตามที่ระบุในผลเฉลย
22	จากแบบรูป 85 Internal Structure แบ่งแยก error message ได้ชัดเจน แต่ไม่มีความต้องกันกับ pattern 54 เพราะไม่แน่ใจว่าใช่ pattern เดียวกันไหม	ไม่เหมือนกันกับ 54 เนื่องจากเป็นการขยายความ
23	แบบรูป 51 ส่วนของ Internal Structure แบ่งกลุ่มได้ชัดเจน แนะนำเพิ่มเติมให้ใส่เลขหัวข้อเพื่อบ่งบอกว่าส่วนไหนเป็นส่วนไหน เพื่อง่ายต่อการทำความเข้าใจ	ไม่แก้ไขเนื่องจากเลขหัวข้อจะซ้ำกัน

ตารางที่ ง.1 รายการคำแนะนำและการปรับปรุงแบบรูป (ต่อ)

ลำดับ	รายการคำแนะนำ	การปรับปรุง
24	แบบรูป 54 จะต้องเพิ่ม Attribute ใน Class ErrorSignaling เพื่อใช้เป็นตัวแปรรองรับการ Pass value จาก Method ที่ได้จาก UserAgent เช่น InfoMessage	เพิ่ม Attribute
25	การเน้น ตัวหนา ขีดเส้นใต้ ทำให้สามารถทำความเข้าใจมองเห็นความสัมพันธ์ต่อเนื่องจาก solution ไปยังฝั่ง internal structure ได้ดี แต่ควรตรวจสอบ Class Diagram บางตัวไม่สัมพันธ์กับคำอธิบาย บางอันใช้คำไม่ตรงกัน บางตัวไม่ได้มีการขีดเส้นใต้เพื่อแสดงว่าอยู่ใน Class Diagram	ตรวจสอบการใช้การไฮไลท์สำหรับชื่อคลาสที่ปรากฏในผลเฉลย
26	ควรทวนสอบอักษรพิมพ์ใหญ่/เล็ก class ส่วนของ Attribute	ตรวจแล้ว
ด้านการประยุกต์ใช้และกรณีตัวอย่างของแบบรูป		
27	แบบรูป 71 อธิบายส่วนประกอบของระบบ จากหัวข้อที่นำเสนอควรมีรูปภาพประกอบแต่ละส่วนของส่วนต่อประสานโครม	การใส่ภาพการออกแบบส่วนต่อประสารจะเป็นการจำกัดความคิดสร้างสรรค์ของผู้ออกแบบ
28	ถ้าเป็นไปได้ในส่วนของ Example และ Example Resolved อยากให้เพิ่มรูปภาพที่เกี่ยวข้องกับปัญหา (Capture Screen) ของปัญหาเพื่อให้ user สามารถนึกภาพการใช้งานที่เป็นปัญหาได้ เช่น การเข้าลิงค์ผ่านทางโทรศัพท์เคลื่อนที่โดยมองไม่เห็น URL ทั้งหมด หรือข้อความแจ้งเตือน เมื่อมีการ Download โปรแกรม	
29	สามารถช่วยให้เข้าใจรูปแบบการกำหนดความต้องการความมั่นคงได้ครบถ้วน และช่วยให้การออกแบบความต้องการด้านความมั่นคงสมบูรณ์และรวดเร็วขึ้น	ไม่พบรายการที่ต้องปรับปรุง
30	แบบรูป 71 Example ควรให้ความสำคัญกับคำว่าดัดแปลงหรือ web responsive เพราะในปัจจุบัน UI ของ Desktop และ Mobile มีความต่างกัน	การพิจารณา Responsive ขึ้นอยู่กับการออกแบบ
31	จากแบบรูป 64 Example เพิ่มปัญหาที่เกิดขึ้นจาก Link หลอก	ปรับปรุงตัวอย่าง
32	แบบรูป 51 กรณี 10 ยังไม่เห็นความต่างของบริบทว่าต่างกันอย่างไร ควรทำไฮไลท์ที่แสดงถึงความแตกต่างของบริบท	ปรับปรุงตัวอย่าง
33	แบบรูปแสดงได้เหมาะสมแต่ถ้าแสดงในรูปโปรแกรมน่าจะทำความเข้าใจได้ง่ายกว่า เช่น กดที่ class แล้วมีคำอธิบายเพิ่มเติมให้	พิจารณาปรับปรุงสำหรับงานวิจัยในอนาคต
34	แบบรูป 85 ส่วนของ Example Resolved ควรเพิ่มเติมรายละเอียดให้ชัดเจนมากขึ้น	ปรับปรุงตัวอย่างของแบบรูป 85

ตารางที่ ง.1 รายการคำแนะนำและการปรับปรุงแบบรูป (ต่อ)

ลำดับ	รายการคำแนะนำ	การปรับปรุง
ด้านอื่น ๆ		
ด้านความเหมาะสมของตารางการตามรอยที่ใช้ประกอบการทวนสอบแบบรูป		
35	ตารางการตามรอยเข้าใจค่อยข้างยากในการตามรอยเนื้อหามายังแบบรูป	
ด้านความเหมาะสมของรายการคำถาม		
36	ข้อคำถามน่าจะให้ประเมินย่อยก่อนแล้วประเมินภาพรวมทีหลัง	

ประวัติผู้เขียนวิทยานิพนธ์

นางสาวภัทรียา สิงห์พันธ์ เกิดเมื่อวันพุธที่ 28 ธันวาคม พ.ศ. 2531 ที่โรงพยาบาลสรรพสิทธิประสงค์ จังหวัดอุบลราชธานี สำเร็จการศึกษาในหลักสูตรวิทยาศาสตรบัญฑิต สาขาวิชาวิศวกรรมซอฟต์แวร์ สำนักวิชาเทคโนโลยีสารสนเทศ มหาวิทยาลัยแม่ฟ้าหลวง เมื่อปีการศึกษา 2554 ด้วยเกียรตินิยมอันดับ 1 เหรียญทอง และเข้าศึกษาต่อในหลักสูตรวิทยาศาสตรมหาบัณฑิต คณะวิศวกรรมศาสตร์ สาขาวิศวกรรมซอฟต์แวร์ จุฬาลงกรณ์มหาวิทยาลัย ในปีการศึกษา 2555