บทที่ 5
สรุปผลและการประยุกต์ใช้

จากการศึกษาถึงภัยคุกคาม และ วิธีการรักษาความปลอดภัยของข้อมูลในการทำธุรกรรม และ ข้อมูลที่ส่งผ่านเครือข่ายของระบบพาณิชย์อิเล็กทรอนิกส์แล้ว ในบทนี้จะเป็นการสรุปผลการศึกษา และ ประยุกต์ใช้ความรู้ที่ได้จากการศึกษามาใช้ในการพัฒนาการรักษาความปลอดภัยของพาณิชย์อิเล็กทรอนิกส์ทั้งในส่วนของผู้ซื้อและผู้ประกอบการ โดยส่วนแรกของรายงาน ในหัวข้อ 5.1 จะเป็นสรุปผลการศึกษา ส่วนหัวข้อที่เหลือจะกล่าวถึงการประยุกต์ใช้ระบบการรักษาความปลอดภัยของพาณิชย์อิเล็กทรอนิกส์

5.1 สรุปผล

ผลการศึกษาเมื่อพิจารณาภัยคุกคามที่อาจเกิดขึ้นกับพาณิชย์อิเล็กทรอนิกส์ อาจแบ่งภัยคุกคามออกได้ 2 ประเภทใหญ่ ๆ คือ ภัยคุกคามข้อมูลในการทำธุรกรรม และ ภัยคุกคามที่อาจเกิดขึ้นภายในระบบเครือข่าย

5.1.1 การคุกคามข้อมูลในการทำธุรกรรม

การที่ข้อมูลที่เป็นความลับส่งผ่านออกจากระบบเครือข่ายคอมพิวเตอร์ โดยผ่านสื่อที่ไม่ปลอดภัยนั้น เราจำเป็นจะต้องสร้างเกราะความปลอดภัยให้กับข้อมูลเพื่อรักษาข้อมูลให้เป็นความลับก่อนที่จะส่งออกไป โดยอาศัยวิธีการเข้ารหัสและถอดรหัสข้อมูล วิธีการแต่ละวิธีจะมีข้อดีและข้อเสียแตกต่างกันออกไป ขึ้นกับระดับความปลอดภัยที่ต้องการ ทรัพยากรทั้งฮาร์ดแวร์ และซอฟต์แวร์ที่ต้องใช้สนับสนุน

5.1.2 การคุกคามในระบบเครือข่าย

การที่ระบบเครือข่ายเป็นระบบเปิดที่ถูกออกแบบมาให้ใช้กับคนจำนวนมาก ความสลับซับซ้อนของระบบที่นำมาต่อเชื่อม และการกำหนดตัวแปรของอุปกรณ์ในเครือข่ายที่ไม่ถูกต้องส่งผลให้เกิดการคุกคามโดยอาชญากรคอมพิวเตอร์

วิธีการปกป้องภัยคุกคามที่เกิดขึ้นโดยพิจารณาจากความเสี่ยงที่เกิดขึ้นมีด้วยกัน 4 เรื่องดังนี้

5.1.3 การระบุตัวบุคคล

ข้อมูลที่ใช้ในการซื้อขายสินค้าผ่านสื่ออิเล็กทรอนิกส์ เช่นข้อมูลบัตรเครดิต เป็นข้อมูลสำคัญที่อาจนำไปสู่ความเสียหายต่อทรัพย์สิน หรือการถูกฟ้องร้องทางกฎหมายได้ แม้ว่าการชำระเงินด้วยบัตรเครดิตผ่านทางอินเตอร์เน็ตจะสร้างความสะดวกสบายให้ผู้ซื้อ แต่ถ้าเกิดปัญหาใด ๆ ขึ้นมาทางสถาบันเจ้าของบัตรกลับถือเป็นความรับผิดชอบของผู้ขาย เนื่องจากไม่มีลายเซ็นของผู้ซื้อที่ยืนยันว่าเป็นผู้ซื้อตัวจริง ทางออกสำหรับเรื่องนี้ประกอบด้วย 2 ส่วน ส่วนแรกจะต้องมีโปรแกรมที่สามารถตรวจพบเมื่อมีการแอบอ้างใช้บัตร และอีกส่วนหนึ่งคือการติดตั้ง SET โปรโตคอลที่สามารถตรวจสอบสถานภาพ และความน่าเชื่อถือ รวมทั้งการตรวจสอบตัวตนของผู้เกี่ยวข้องกับการซื้อขายทุกฝ่ายโดยอาศัยลายเซ็นดิจิตอล

5.1.4 การรักษาความถูกต้องของข้อมูล

ข้อมูลโดยเฉพาะหมายเลขบัตรเครดิตหรือความลับต่าง ๆ ต้องสามารถรักษาความถูกต้องของข้อมูลมิให้มีการแก้ไขโดยไม่ปรากฏร่องรอยได้ โดยอาศัยวิธีการดังนี้

(1) ใช้ Checksum เพื่อตรวจสอบการเปลี่ยนแปลงข้อมูลในระหว่างการส่ง

(2) ใช้ Parity Bit เพื่อตรวจสอบความถูกต้องของข้อมูลก่อนและหลังการส่ง

(3) ใช้ลายเซ็นอิเล็กทรอนิกส์ของข้อมูลตรวจสอบก่อนและหลังการส่ง

5.1.5 การรักษาความลับของข้อมูล

ข้อมูลของลูกค้าจากร้านค้าออนไลน์ที่ถูกละเมิด มักจะเกิดขึ้นกับร้านค้าออนไลน์ที่รีบร้อนนำธุรกิจของตนออนไลน์โดยที่ยังไม่ได้ติดตั้งอุปกรณ์เพื่อความปลอดภัยต่อพาณิชย์อิเล็กทรอนิกส์ ผู้ประกอบการควรว่าจ้างผู้เชี่ยวชาญในเรื่องระบบการรักษาความปลอดภัยของข้อมูลบนอินเตอร์เน็ต เพื่อรักษาความลับมิให้มีผู้อื่นแอบดูข้อมูลที่เก็บไว้ หรือข้อมูลที่ส่งผ่านไปทางเครือข่าย

วิธีการที่จะรักษาความลับของข้อมูลที่ส่งผ่านระบบเครือข่ายคือการเข้ารหัส และการถอดรหัสข้อมูล ซึ่งการเข้ารหัสแต่ละวิธีจะส่งผลต่อระดับความปลอดภัยที่ได้รับ โดยมีข้อแนะนำดังนี้

(1) วิธีการเข้ารหัสที่มีความซับซ้อนมาก ระดับความปลอดภัยของข้อมูลก็จะสูงตามไปด้วย

(2) การนำวิธีการเข้ารหัสไปใช้ควรจะง่าย และสะดวก

(3) ไม่ควรมีข้อจำกัดในการเลือกใช้กุญแจเข้ารหัส

(4) ความผิดพลาดจากการเข้ารหัส ณ จุดใดจุดหนึ่งของข้อมูล ต้องไม่ขยายไปสู่ส่วนอื่น ๆ

(5) ขนาดข้อมูลที่เข้ารหัสแล้ว ต้องไม่ใหญ่กว่าขนาดของ Clear Text

(6) วิธีการเข้ารหัสต้องเหมาะสมกับทรัพยากรของเซิร์ฟเวอร์ที่ใช้งาน

วิธีการที่จะรักษาความปลอดภัยในระบบเครือข่ายเพื่อไม่ให้มีภัยคุกคามต่อข้อมูล มีข้อแนะนำดังนี้

(1) เข้ารหัสข้อมูลที่ส่งภายในเครือข่าย

(2) ควบคุมอนุญาตบุคคลให้เข้ามาในระบบ

(3) ตรวจสอบความถูกต้องระบบคอมพิวเตอร์ในเครือข่าย

(4) ใช้ Firewall ในการรักษาความปลอดภัยในเครือข่าย

(5) กำหนดตัวแปรต่าง ๆ ให้ถูกต้องสำหรับอุปกรณ์ในเครือข่ายอื่น ๆ เช่น DNS, DHCP, Modem, Bridge, Hub, Switch เป็นต้น

(6) ติดตั้งโปรแกรมตรวจจับไวรัสคอมพิวเตอร์

(7) รักษาความปลอดภัยทางกายภาพ เช่น มีการใช้อุปกรณ์ล๊อคแบบต่าง ๆ

(8) วางแผนการกู้ข้อมูลคืนเมื่อจำเป็น

5.1.6 การปฏิเสธความรับผิดชอบ

ในกรณีที่ผู้ซื้อปฏิเสธการชำระเงิน ผู้ขายก็ไม่สามารถเรียกร้องค่าสินค้าได้ เนื่องจากไม่สามารถจะให้ผู้ซื้อลงลายมือชื่อในใบเสร็จรับเงินเพื่อเป็นหลักฐานได้ ทางเดียวที่จะช่วยได้คือการใช้ลายเซ็นดิจิตอลที่เฉพาะผู้ที่มีอำนาจจึงจะสามารถเรียกข้อมูลที่ได้รับอนุญาตให้อ่านได้เท่านั้น วิธีการนี้เป็นวิธีการเดียวที่จะทำให้ธนาคารมีหลักฐานลายเซ็นของผู้ซื้อบนสื่ออิเล็กทรอนิกส์

จากการศึกษาระบบการชำระเงินผ่านทางอินเตอร์เน็ตพบว่า ระบบ SET เป็นระบบเดียวที่มีความปลอดภัยสูงสุดในปัจจุบัน โดย SET จะอนุญาตให้เฉพาะผู้ที่ผ่านการตรวจสอบแล้วเท่านั้นจึงจะสามารถเข้าถึงข้อมูลต่าง ๆ ส่วนคนทั่วไปที่ยังกังวลว่าข้อมูลบัตรเครดิตของตนจะถูกขโมย ถูกนำไปแอบอ้างเพื่อใช้จ่าย ข้อมูลส่วนตัวจะถูกเปิดเผย รวมถึงกังวลว่าสินค้าที่ตนสั่งซื้อนั้นจะไม่มีการนำส่ง และไม่ไว้ใจร้านค้าต่าง ๆ ที่ออนไลน์ การพัฒนา SET ขึ้นมาจะช่วยแก้ไขปัญหาทั้งหมด

SET นั้นใช้ลายเซ็นดิจิตอลในการตรวจสอบความถูกต้อง และสถานภาพของผู้ที่เกี่ยวข้องว่าได้รับอำนาจในการดำเนินรายการต่าง ๆ ตามขั้นตอนการชำระค่าสินค้า ทุกรายการที่เกิดขึ้นนั้นจะไม่สามารถถูกปฏิเสธได้ เราสามารถมั่นใจได้ว่าไม่มีผู้ใดสามารถเข้าไปอ่านข้อมูลรายละเอียดต่าง ๆ ที่เป็นความลับของผู้ซื้อและผู้ขาย SET ยังช่วยเปิดกว้างให้ผู้ซื้อ ผู้ขาย และธนาคารให้สามารถติดต่อกันได้อย่างมั่นใจผ่านทางอินเตอร์เน็ตเพราะสามารถตรวจสอบได้ว่าทุกฝ่ายมีตัวตนจริง เชื่อถือได้

SET ยังตรวจสอบความถูกต้องของข้อมูลต่างๆ และยังให้ความมั่นใจด้วยว่าทุก ๆ รายการที่ดำเนินการนั้นจะเป็นความลับ 100 เปอร์เซ็นต์ เพราะจะมีการเข้ารหัสข้อมูลทุกครั้งในการส่งผ่านข้อมูล เริ่มตั้งแต่ผู้ซื้อ ผู้ขาย และสถาบันการเงิน อีกทั้งการเข้ารหัสนั้นมีความซับซ้อนซึ่งยากต่อการถอดรหัสโดยผู้ไม่ประสงค์ดี

อย่างไรก็ตาม คาดการณ์กันว่าระบบ SSL จะยังเป็นที่แพร่หลายที่สุดในระยะ 3 ปีนี้ เนื่องจาก SSL นั้นนำมาใช้งานได้ง่าย และ ประหยัด ถึงแม้จะมีช่องโหว่อีกหลายประการ เช่น ร้านค้าไม่สามารถตรวจสอบได้ หากมีคนแอบนำหมายเลขบัตรเครดิตของคนอื่นมาใช้ ทำให้ร้านค้าต้องรับความเสี่ยงหากเจ้าของบัตรปฏิเสธการจ่ายเงิน ในอนาคต SSL อาจมีการปรับปรุงพัฒนาขึ้น ส่วนราคาของ SET ก็อาจลดลงมาจนกลายเป็นมาตรฐานใหม่ที่ทุกคนสามารถใช้ได้

5.2 ความปลอดภัยในการซื้อสินค้าผ่านทางอินเตอร์เน็ต

การซื้อขายสินค้าออนไลน์บนอินเตอร์เน็ตนอกจากจะเป็นช่องทางสร้างรายได้ใหม่ให้ผู้ขายสินค้าแล้ว ยังกลายเป็นการสร้างความสะดวกสบายให้กับผู้ซื้อ เพราะสั่งซื้อสินค้าได้ง่าย มีสินค้าให้เลือกมากมาย ไม่จำเป็นต้องเดินทางไปยังร้านค้าให้เปลืองเวลาและเสียค่าเดินทาง ทำให้มูลค่าการใช้จ่ายธุรกิจบนอินเตอร์เน็ตทั่วโลกเพิ่มปริมาณขึ้นเรื่อย ๆ นับตั้งแต่ปี 2543 เป็นต้นมา[54]

ปัจจุบันวิธีการชำระเงินเมื่อซื้อสินค้าทางอินเตอร์เน็ตจะมีหลายแบบให้ลูกค้าเลือกใช้ ทั้งการจ่ายเงินสดเมื่อได้รับสินค้าแล้ว การโอนเงินผ่านบัญชี จ่ายโดยเช็ค ทำบัญชีผ่านเทเลโฟนแบงก์กิ้ง(Telephone Banking) ผ่านบัตรเครดิต บัตรเอทีเอ็ม เป็นต้น แต่การชำระเงินค่าสินค้าผ่านบัตรเครดิตจะได้รับความนิยมค่อนข้างสูง เนื่องจากลูกค้าใช้เวลาไม่กี่นาทีที่ทำรายการผ่านหน้าจอคอมพิวเตอร์ก็จะสามารถสั่งซื้อสินค้าได้ ปกติแล้วบริษัทผู้ขายจะไม่ได้เรียกเก็บเงินจากบัตรเครดิตในทันทีหลังจากที่ลูกค้าสั่งซื้อสินค้าผ่านเว็บไซต์ แต่บริษัทจะตรวจสอบวงเงินไปยังธนาคารผู้ออกบัตร เมื่อธนาคารแจ้งกลับมาว่ามีวงเงินพอที่จะจ่ายค่าสินค้าได้ ก็จะกันวงเงินนั้นไว้ก่อน หลังจากที่ได้จัดส่งสินค้าถึงมือผู้ซื้อแล้วจึงจะตัดวงเงินจากบัตรเครดิตนั้นๆ หากการทำรายการยังไม่ได้เกิดแต่มีการหักเงินจากบัตรเครดิต บางบริษัทจะปลดวงเงินให้ลูกค้าภายใน 7 วัน

แต่ปัญหาของการซื้อสินค้าผ่านอินเตอร์เน็ตก็มีอยู่บ้างเช่นกัน โดยเฉพาะคำร้องเรียนของผู้สั่งซื้อสินค้าซึ่งจ่ายเงินชำระค่าสินค้าผ่านบัตรเครดิตไปเรียบร้อยแล้ว แต่กลับไม่ได้รับสินค้าตามรายการที่สั่งซื้อทางเว็บไซต์หรือรายการสินค้าที่สั่งซื้อถูกยกเลิกไปโดยไม่ทราบสาเหตุ เพื่อให้การซื้อหาสินค้าทางบนอินเตอร์เน็ตซึ่งคาดว่าน่าจะได้รับความนิยมมากขึ้นในอนาคตเป็นไปอย่างปลอดภัยและมั่นใจได้สำหรับผู้บริโภค ผู้ที่อยู่ในวงการประกอบธุรกิจขายสินค้าบนอินเตอร์เน็ตได้ให้คำแนะนำในส่วนของผู้ซื้อและและผู้ประกอบการดังนี้[55]

---

[54] จอร์จ ลี. "ทำธุรกิจผ่านเว็บให้ปลอดภัยได้อย่างไร ?". **กรุงเทพธุรกิจ**. (6 เมษายน 2000) : 9 .

[55] จิรเดช พูนมโนธรรม. "การลดความเสี่ยงของการชำระเงินผ่านเน็ต". **กรุงเทพธุรกิจ**. (15 มกราคม 2000) : 8.

5.2.1 ในส่วนของผู้ซื้อ

(1) ผู้ซื้อสินค้าควรจะซื้อสินค้าจากเว็บไซต์ที่มีชื่อเสียง และต้องมั่นใจได้ว่ามีสถานที่จำหน่ายสินค้า และที่ติดต่อแน่นอน มีชื่อเสียงเป็นที่รู้จัก ดำเนินธุรกิจจำหน่ายสินค้ามานาน ไม่ใช่เลือกซื้อจากเว็บไซต์ที่เสนอขายสินค้าในราคาถูกเพียงอย่างเดียว

(2) ลูกค้าเลือกซื้อสินค้ากับเว็บไซต์ที่มีสถานที่จำหน่าย ติดต่อได้ และเปิดดำเนินการเพื่อซื้อขายสินค้าโดยตรงจะปลอดภัยกว่า เพราะหากมีปัญหาในการส่งสินค้าหรือไม่ได้รับสินค้า ก็จะสามารถไปติดต่อตามสาขาของร้านค้านั้นได้ ตรงนี้ลูกค้าควรจะตรวจสอบ หรือค้นหาชื่อเว็บไซต์ต่าง ๆ ให้ดีก่อนที่จะตัดสินใจสั่งซื้อสินค้า

(3) เมื่อได้ตัดสินใจทำรายการสั่งซื้อสินค้าผ่านเว็บไซต์นั้น ๆ แล้ว ลูกค้าควรจะตรวจสอบขั้นตอนการดำเนินการของเว็บไซต์นั้นว่าอยู่ในขั้นตอนใด ในกรณีที่ไม่ได้รับสินค้าบริษัท จัดส่งผิดที่ หรือผิดบุคคลก็จะสามารถติดตามได้

(4) หลังจากที่ลูกค้าได้สั่งซื้อสินค้าแล้วควรจะเก็บข้อมูลที่ได้รับ เพื่อเป็นการยืนยันจากบริษัทผู้ขายสินค้าว่าได้ซื้อและจ่ายเงินเรียบร้อยแล้ว โดยการจัดพิมพ์ข้อมูลนั้นเก็บไว้ หรือการดูข้อมูลประวัติการซื้อขายที่ผ่านมา ซึ่งบริษัทได้รวบรวมไว้ นอกจากจะเป็นหลักฐานการซื้อเพื่อเก็บไว้ยืนยันกับผู้ขายได้แล้ว ยังช่วยให้ลูกค้าควบคุมงบค่าใช้จ่ายของตนเองไปในตัวด้วย

(5) หากลูกค้าเลือกใช้วิธีการชำระเงินด้วยการตัดจ่ายจากบัตรเครดิต ผู้เชี่ยวชาญบอกว่าอย่าให้ใครยืมบัตรเครดิต หรือให้ข้อมูลบัตรแก่ผู้อื่น ควรจะเก็บรักษาเอาไว้เป็นความลับส่วนตัว หากเกิดสูญหายเมื่อใดควรรีบแจ้งอายัดบัตรทันที และแจ้งความโดยเร็วที่สุด

(6) วิธีการซื้อสินค้าให้ปลอดภัยที่สุดควรเลือกชำระเงินค่าสินค้าด้วยเงินสด จะเป็นการป้องการความเสี่ยงการชำระเงินค่าสินค้าของลูกค้าได้ดีที่สุด และยังได้รับสินค้าตามที่ต้องการ เพราะเราจะชำระเงินก็ต่อเมื่อพนักงานได้นำส่งสินค้าถึงมือแล้วจึงค่อยจ่ายเงิน ทำให้ไม่ต้องกังวลว่าจะไม่ได้รับสินค้าหรือถูกหลอกลวง แต่กรณีนี้อาจจะเป็นการยากสำหรับการสั่งซื้อสินค้าจากต่างประเทศ

(7) ทางออกที่ดีที่สุดสำหรับผู้สั่งซื้อสินค้าจากเว็บไซต์ต่างประเทศแต่ยังไม่ได้รับของ ควรรีบแจ้งและสอบถามไปยังธนาคารผู้ออกบัตรทันทีว่าได้รับแจ้งการเก็บเงินจากร้านค้าหรือไม่ หากเรียกเก็บเงินแล้วก็เป็นหน้าที่ของธนาคารที่จะต้องดำเนินการต่อไป ทั้งนี้ลูกค้าจะต้องเก็บหลักฐานที่ร้านค้าตอบกลับมาเพื่อเป็นการยืนยัน ในกรณีที่ลูกค้ายังไม่ได้รับสินค้าที่ได้สั่งซื้อไปแล้วหลายวัน รวมทั้งบริษัทได้หักจ่ายเงินผ่านบัตรเครดิตไปเรียบร้อยแล้ว สิ่งที่ลูก

ค้าควรทำได้ก็คือติดต่อธนาคารผู้ออกบัตร เพื่อธนาคารจะได้ตรวจสอบต่อไป รวมถึงติดต่อสอบถามผู้ขายด้วยว่า รายการที่ซื้อแต่ไม่ได้รับสินค้าไปนั้น ทำไมบัตรถึงถูกหักยอดเงินออกไป โดยปกติแล้วกรณีที่ลูกค้าจ่ายเงินซื้อสินค้าผ่านอินเตอร์เน็ตแล้ว แต่ยังไม่ได้รับสินค้า ลูกค้าสามารถเรียกร้องรับเงินคืนได้ โดยยืนยันเอกสารที่ได้รับจากบริษัท

5.2.2 ในส่วนของผู้ประกอบการ

จะต้องมีการจัดโครงสร้างพื้นฐานธุรกิจที่ทำพาณิชย์อิเล็กทรอนิกส์ ขั้นตอนแรกคือการกำหนดแนวทางหรือมาตรการรักษาความปลอดภัย จะต้องมีการกำหนดปัจจัยและองค์ประกอบอย่างชัดเจน เช่น องค์กรต้องการปกป้องข้อมูลส่วนใดบ้าง และบุคคลใดสามารถเข้าไปดูข้อมูลของบริษัทในระดับต่าง ๆ กันออกไป การดำเนินขั้นตอนเพื่อรักษาความปลอดภัยนี้จะเริ่มต้นด้วยการแต่งตั้งเจ้าหน้าที่ผู้รับผิดชอบโดยรวม จัดหาพนักงานที่ได้รับการอบรมในเรื่องการรักษาความปลอดภัยทางข้อมูลและเครือข่าย

ผู้เชี่ยวชาญด้านความปลอดภัยทางข้อมูลและเครือข่ายของไอบีเอ็มได้ให้แนวทางในการตรวจสอบสำหรับการรักษาความปลอดภัยภายในบริษัทดังนี้[56]

(1) จัดทำมาตรการเพื่อรักษาความปลอดภัยทางข้อมูลและเครือข่ายอย่างละเอียด ความปลอดภัยในที่นี้มิใช่ความรับผิดชอบของผู้ที่ได้รับมอบหมายให้ดูแลความปลอดภัยทางข้อมูลและเครือข่ายเพียงอย่างเดียวแต่เป็นความรับผิดชอบของพนักงานทุกคนในบริษัท ซึ่งสามารถส่งผลไปทั่วทั้งองค์กร การควบคุมจะต้องครอบคลุมถึงไฟร์วอลล์ ควบคุมข้อมูลที่สามารถเข้าและออกจากเครือข่าย

(2) รณรงค์ให้ตระหนักถึงมาตรการความปลอดภัย เตือนพนักงานให้ทราบถึงความรับผิดชอบของตนที่ต้องดูแล เช่น การใช้อีเมล ไม่ควรเปิดอีเมลของผู้ที่ไม่รู้จัก

(3) ติดตั้งไฟร์วอลล์ไว้รอบนอกสุด และควรติดตั้งไว้ภายในองค์กรด้วย เช่น ระหว่างแผนกบุคคลและแผนกวิศวกรรม ที่สำคัญต้องเปลี่ยนค่า Default Settings เพราะเป็นจุดอ่อนที่โจมตีได้ง่าย

(4) ใช้ซอฟต์แวร์ตรวจจับการบุกรุก ทั้งนี้เหมือนกับสัญญาณกันขโมย หรือเครื่องตรวจจับการเคลื่อนไหว แต่เป็นการใช้กับเครือข่ายขององค์กรโดยที่มีไฟร์วอลล์ จึงมีความจำเป็นที่จะต้องมีซอฟต์แวร์ตรวจจับการบุกรุกจากเครือข่ายภายในและภายนอก

---

[56] BlueNet. "อี-คอมเมิร์ซ กับอุปสรรคที่ท้าทาย". BCM. (เมษายน 1999) : 139.

(5) แจกจ่ายซอฟต์แวร์เพื่อป้องกันไวรัส เพราะเป็นวิธีป้องกันไวรัสที่ดีและง่ายที่สุด

(6) การกำหนดกฎระเบียบสำหรับการใช้รหัสผ่าน(password) กำหนดแนวทางที่ชัดเจนสำหรับการเลือกใช้รหัสผ่าน เช่น ตัวอักษร 6 ตัว ควรมีตัวเลขอย่างน้อย 1 ตัว และกำหนดวิธีการง่าย ๆ ในการตรวจสอบรหัสผ่านว่าถูกต้องหรือไม่ และรหัสผ่านนี้ควรเปลี่ยนในระยะเวลาที่กำหนด

(7) ดำเนินการตรวจสอบ(audit)ระบบรักษาความปลอดภัยในเครือข่ายอย่างสม่ำเสมอ ทั้งนี้ไม่ควรประกาศ หรือแจ้งให้ทราบล่วงหน้า อาจทำการสุ่ม

(8) แต่งตั้งผู้ดูแลเครือข่ายและข้อมูล ขั้นตอนในการรายงานผล ให้สอดคล้องกับระบบความปลอดภัยที่วางไว้ พนักงานทั่วไปจะต้องแจ้งผู้ดูแลเครือข่ายทันทีหากเกิดปัญหาด้านความปลอดภัยทางเน็ตเวิร์กและข้อมูล

(9) ผู้ดูแลระบบ(System Administrator) จะต้องเป็นที่ปรึกษาและเห็นความสำคัญของความปลอดภัยในเครือข่าย โดยจะต้องมีการเปลี่ยนแปลงโครงสร้างรหัสผ่านภายในกำหนดระยะเวลาอย่างเคร่งครัด ผู้ดูแลเครือข่ายจะต้องเป็นบุคคลแนวหน้า ที่จะต้องกระตือรือร้นปฏิบัติงานอย่างรวดเร็วหากเกิดปัญหาด้านความปลอดภัย

(10)มีนโยบายที่ชัดเจนในการดำเนินการ เมื่อพนักงานลาออก ไม่ว่าด้วยเหตุผลใดๆ จะต้องมีมาตรการดำเนินการอย่างรวดเร็วเพื่อปกป้องมิให้พนักงานเก่าสามารถเข้าใช้คอมพิวเตอร์หรือเข้าถึงข้อมูลในเครือข่ายได้ นอกจากนั้นต้องเปลี่ยนแปลงหรือยกเลิกรหัสผ่านต่าง ๆ ที่พนักงานผู้นั้นทราบ

5.3 ขั้นตอนการสร้างความปลอดภัยสำหรับพาณิชย์อิเล็กทรอนิกส์

ในส่วนนี้จะเสนอวิธีการรักษาความปลอดภัยสำหรับการทำพาณิชย์อิเล็กทรอนิกส์โดยวิธี SSL และ SET นั่นคือการรักษาความปลอดภัยข้อมูลที่ถูกส่งผ่านหน้าเว็บจากฝั่งลูกค้าที่กรอกลงบนเว็บเบราเซอร์ และส่งมายังเครื่อง เซิร์ฟเวอร์ ซึ่งเราเรียกว่า Web Security

Web Security เป็นการรักษาความปลอดภัยสำหรับข้อมูลบนหน้าเว็บ ซึ่งปัจจุบันมีการพัฒนารูปแบบ Web Security นี้หลายรูปแบบ โดยใช้โปรโตคอลสำหรับความปลอดภัยต่างๆ กัน โดยจะขอยกมา 2 โปรโตคอลว่าแต่ละอย่างทำงานอย่างไร และจะนำมาประยุกต์เข้ากับระบบได้อย่างไร

5.3.1 SSL : Secure Sockets Layer Protocol

การจัดระบบรักษาความปลอดภัยโดย SSL จะจัดช่องทางหรือ Session ที่ปลอดภัยสำหรับการติดต่อส่งข้อมูล โดยในปัจจุบัน SSL ถูกนำไปพัฒนาและมีการใช้งานในหลายรูปแบบ ซึ่งรูปแบบส่วนใหญ่จะเป็นการติดต่อส่งข้อมูลระหว่างเครื่อง เว็บเซิร์ฟเวอร์ กับโปรแกรมเบราเซอร์เพื่อการติดต่อส่งข้อมูลทาง World Wide Web ให้ปลอดภัยกันมากขึ้น ซึ่ง SSL ได้รับความนิยมในการนำมาเป็นส่วนรักษาความปลอดภัยในการติดต่อระหว่างผู้ขายกับผู้ซื้อในการพาณิชย์อิเล็กทรอนิกส์ โดยจะเห็นได้จากเว็บเบราเซอร์และซอฟต์แวร์สำหรับทำเว็บเซิร์ฟเวอร์ทุกยี่ห้อรองรับการทำงานของโพรโตคอล SSL ทั้งนั้น

โพรโตคอล SSL ทำงานอยู่เหนือชั้น Transport หรือชั้นที่ 4 ใน OSI Model ซึ่งจะคอยจัดช่องทางที่ปลอดภัยระหว่างชั้น Transport กับแอพพลิเคชันที่อยู่เหนือขึ้นไป โดยปกติเครื่องคอมพิวเตอร์ 2 เครื่องจะติดต่อกันข้ามเครือข่ายผ่านทางช่องทางหรือ Socket ที่กำหนดกันไว้ล่วงหน้า เช่น เว็บเบราเซอร์ของผู้ใช้งานจะติดต่อไปยังเว็บเซิร์ฟเวอร์ที่เก็บเว็บไซต์ที่ผู้ใช้งานเรียกไปโดยใช้โพรโตคอล HTTP ทางพอร์ต 80 แต่ SSL จะจัดพอร์ตการติดต่อที่ต่างออกไปจากพอร์ตธรรมดานี้ คือจะให้ติดต่อกันที่พอร์ต 443 แทน ดังนั้น SSL จึงสามารถนำไปใช้งานกับโพรโตคอลในชั้นแอพพลิเคชันอื่นๆ ได้ เช่น FTP, TELNET, gopher, NNTP และ SMTP

ใน SSL เครื่อง 2 เครื่อง จะตกลงเพื่อร่วมกันสร้างกุญแจสำหรับช่องทางการติดต่อแต่ละครั้งโดยเฉพาะ ซึ่งจะเรียกขั้นตอนนี้ว่าการทำ Handshake เริ่มจาก Client (ในกรณีนี้เป็นเว็บเบราเซอร์) ร้องขอเปิดการติดต่อไปยังเซิร์ฟเวอร์ จะตอบกลับยืนยันกุญแจสาธารณะส่วนเซิร์ฟเวอร์ อัลกอริธึม และวิธีการบีบอัดข้อมูล รวมทั้งเซิร์ฟเวอร์จะส่งหนังสือรับรองว่า เซิร์ฟเวอร์ที่ไคลเอนต์กำลังติดต่ออยู่นี้เป็นตัวตนจริง ๆ กับที่ไคลเอนต์ต้องการติดต่อด้วย

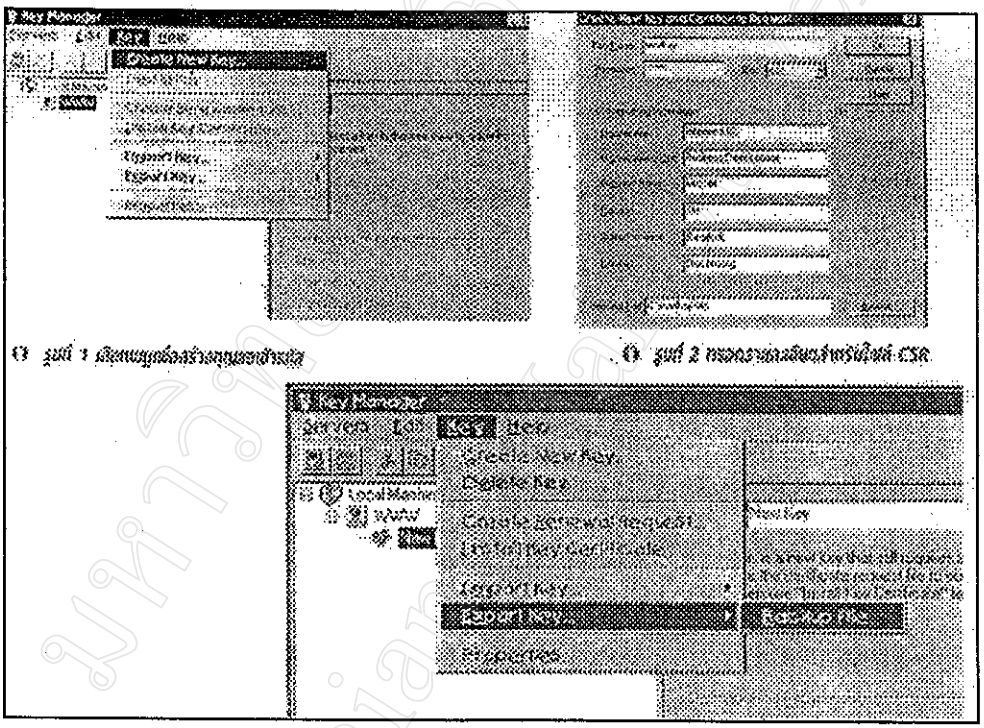
ไคลเอนต์ตรวจสอบหนังสือรับรองแล้ว ก็จะเอากุญแจสาธารณะที่ได้รับมาเข้ารหัสด้วยกุญแจที่ไคลเอนต์สร้างขึ้นมาเอง สิ่งที่ได้ก็คือกุญแจสำหรับการติดต่อในครั้งนั้น หรือ Session Key ซึ่งไคลเอนต์จะส่งให้เซิร์ฟเวอร์เพื่อให้ทั้ง 2 ฝ่ายใช้ Session Key เข้ารหัสในการติดต่อครั้งนั้นๆ (ในขณะเดียวกันหากเซิร์ฟเวอร์ต้องการขอตรวจสอบหนังสือรับรองของไคลเอนต์ ก็จะส่งไปให้เซิร์ฟเวอร์พร้อมๆ กันนี้เลย)

จะเห็นได้ว่าเซิร์ฟเวอร์จะต้องมีใบรับรองที่ออกโดยองค์กรผู้ออกใบรับรอง หรือ Certifticate Authority(CA) ดังนั้นหากต้องการสร้างเว็บไซต์สำหรับขายสินค้าแบบ พาณิชย์อิเล็กทรอนิกส์ และต้องการติดตั้งเครื่องเซิร์ฟเวอร์สำหรับร้านค้า พาณิชย์อิเล็กทรอนิกส์ จะต้องปฏิบัติตามขั้นตอนต่าง ๆ เพื่อให้เว็บไซต์มี SSL รักษาความปลอดภัย มีแนวทางในการปฏิบัติดังนี้

(1) เตรียมเครื่องเซิร์ฟเวอร์ : เมื่อจัดเตรียมเครื่องคอมพิวเตอร์เพื่อนำมาใช้งานโดยการติดตั้งระบบปฏิบัติการสำหรับต่อเชื่อมกับอินเตอร์เน็ตเรียบร้อยแล้ว จะต้องติดตั้งซอฟต์แวร์สำหรับการทำเป็นเครื่องเว็บเซิร์ฟเวอร์ ซึ่งมีให้เลือกมากมายหลายยี่ห้อขึ้นอยู่กับว่าระบบปฏิบัติการของเครื่องเซิร์ฟเวอร์เป็นอะไร เช่น ถ้าท่านใช้ Windows NT อาจเลือก Microsoft IIS, Netscape Enterprise, Lotus Domino และ อื่นๆ แต่หากเลือก Linux แล้วอาจใช้ Apache สำหรับทำงานด้านการให้บริการเว็บเซิร์ฟเวอร์นี้ซึ่งปัจจุบันเกือบทุกยี่ห้อรองรับการทำงานตามโพรโตคอล SSL และรองรับการติดตั้งหนังสือรับรองจากค่ายต่างๆ ด้วย นอกจากนี้ท่านจะต้องเตรียมการเชื่อมต่อเข้าสู่อินเตอร์เน็ตเพื่อเปิดเว็บไซต์สู่สาธารณะ

(2) เตรียมเอกสาร : การที่จะสร้างเว็บไซต์ให้น่าเชื่อถือโดยการมีหนังสือรับรองเว็บไซต์ได้ จะต้องดำเนินการขอหนังสือรับรองจากสถาบันผู้มีสิทธิออกหนังสือรับรอง ซึ่งสถาบันผู้ออกหนังสือเหล่านั้นจะตรวจสอบว่าท่านเป็นเจ้าของชื่อโดเมนที่จะจัดตั้งขายสินค้า และมีชื่อบริษัท ที่อยู่ และเอกสารอื่นๆ ครบถ้วนถูกต้องหรือไม่ ซึ่งเอกสารที่สถาบันแต่ละแห่งต้องการอาจแตกต่างกันไปในแต่ละที่ ซึ่งตรวจสอบเสียก่อนว่าสถาบันนั้นๆ ต้องการเอกสารประกอบอะไรบ้างและเตรียมให้พร้อม(เอกสารทุกชิ้นต้องเป็นภาษาอังกฤษ)

(3) สร้างคำร้องขอมีกุญแจ(Certificate Signing Request : CSR) : CSR จะต้องถูกสร้างจากเครื่องเว็บเซิร์ฟเวอร์ โดยซอฟต์แวร์ที่ใช้ทำงานด้านการให้บริการเว็บเซิร์ฟเวอร์จะต้องมีตัวเลือกด้านการสร้างกุญแจสำหรับการเข้ารหัส เพื่อนำกุญแจที่ได้ไปใช้ในการขอหนังสือรับรอง ตัวอย่างการสร้างกุญแจใน Windows ถ้าติดตั้ง Microsoft Internet Information Server(IIS) แล้ว ใน Toolbar เลือก Microsoft Internet Server แล้วเลือก Key Manger เมื่อโปรแกรมถูกเปิดขึ้นมา ให้เลือก "www" แล้วไปที่เมนู Key เลือก "Create New Key" ดังภาพที่ 23



ภาพที่ 23 แสดงการสร้างกุญแจใน Windows[57]

กรอกรายละเอียดและ Password แล้วเลือกว่าจะเก็บไฟล์ CSR นี้ที่ไหน เพื่อเป็นการไม่ประมาท ควรทำสำรองไฟล์ที่ได้นี้อีกหนึ่งชุด เพราะไฟล์นี้เป็นไฟล์กุญแจสำหรับถอดรหัส หากไฟล์สูญหาย ข้อมูลต่าง ๆ จะไม่สามารถถูกถอดรหัส

---

[57] ธีรา ทานตวณิช. "Web Security ขั้นตอนการสร้างความปลอดภัยสำหรับ E-Commerce". **Microcomputer**. (เมษายน 2000) : 85.

ได้ การสำรองโดยการ Backup ก็เพียงคลิกที่กุญแจที่สร้างไว้ แล้วเลือกเมนู Key, Export Key...Back cup File ดังรูปด้านล่างสุด

(4) **ขอใบรับรอง : เมื่อได้ไฟล์ CSR ตามขั้นที่ 3 แล้ว ต้องนำรายละเอียดที่เขียนไว้ในไฟล์ไปใส่ในแบบฟอร์มการขอมีหนังสือรับรอง ซึ่งจะต้องเข้าไปยังโฮมเพจของสถาบันผู้ออกหนังสือรับรอง บน โฮมเพจของแต่ละสถาบันจะเปิดให้สมัครเพื่อขอหนังสือรับรองโดยจะต้องกรอกข้อมูลขององค์กร และต้องอ่านข้อกำหนดด้านกฎหมายให้เข้าใจก่อน ในส่วนสำคัญของการสมัคร ผู้สมัครจะต้องใส่ CSR ลงบนแบบฟอร์มในโฮมเพจนั้นด้วย เพื่อให้นำ CSR ไปสร้างหนังสือรับรองอีกที**

สถาบันที่รับออกหนังสือรับรองเพื่อใช้กับโพรโตคอล SSL มีหลายแห่ง และราคาแตกต่างกันออกไป จะต้องเลือกดูว่าสถาบันที่มีหนังสือรับรองที่สามารถติดตั้งบนระบบปฏิบัติการของเซิร์ฟเวอร์ขององค์ได้จริง ตัวอย่างของสถาบันที่ออกหนังสือรับรองมีดังนี้

- Verisign : www.verisign.com
- Thawte Consulting : www.thawte.com
- CertiSign Certilfcadora Digital Ltda : www.certisign.com.br
- IKS GmbH : www.iks-jena.de
- BeIsign NV/SA : www.belsign.de
- TC TrustCenter : www.trustcenter.de
- Deutsches Forschungsnetz : www.pca.dfn.de
- 128i Ltd. (New Zealand) : www.128i.com
- Entrust.net Ltd. : www.entrust.net

การใส่ CSR ทำได้โดยการเปิดไฟล์ CSR ที่สร้างและเก็บไว้ เช่น newkey.req ด้วยโปรแกรม Notepad ซึ่งคัดลอก CSR คือตั้งแต่คำว่า "BEGUB BEW CERTIFICATE REQUEST" ถึงคำว่า "END NEW CERTIFICATE REQUEST " ดังนั้น CSR ก็คือส่วนท้ายของไฟล์ CSR นั่นเอง ดังภาพที่ 24

ภาพที่ 24 แสดง CDR[58]

หลังจากนั้นนำส่วนที่คัดลอกไว้ไปใส่ในช่องของแบบฟอร์มในหน้าเว็บเพจ เช่น ที่ Thawte จะมีช่องสำหรับให้ใส่ CSR จากนั้นให้ส่งเอกสารประกอบการสมัครที่เตรียมไว้ทางแฟกซ์และส่งเอกสารตัวจริงตามไปโดยทางไปรษณีย์ตามที่อยู่ที่สถาบันกำหนด หลังจากกรอกรายละเอียดด้านการชำระเงิน ก็เป็นอันเสร็จสิ้นขั้นตอนการสมัคร

[58] เรื่องเดียวกัน : 86.

(5) ติดตั้งใบรับรองลงบนเซิร์ฟเวอร์ : หนังสือรับรองจะถูกส่งมาในรูปแบบไฟล์ จะต้องเก็บรักษาไฟล์ที่ได้เป็นอย่างดี และนำไฟล์นั้นมาติดตั้งลงบนเว็บเซิร์ฟเวอร์ ซึ่งไฟล์หนังสือรับรองจะมีรูปแบบดังภาพที่ 25

ภาพที่ 25 แสดงใบรับรองที่จะนำมาติดตั้งในเซิร์ฟเวอร์[59]

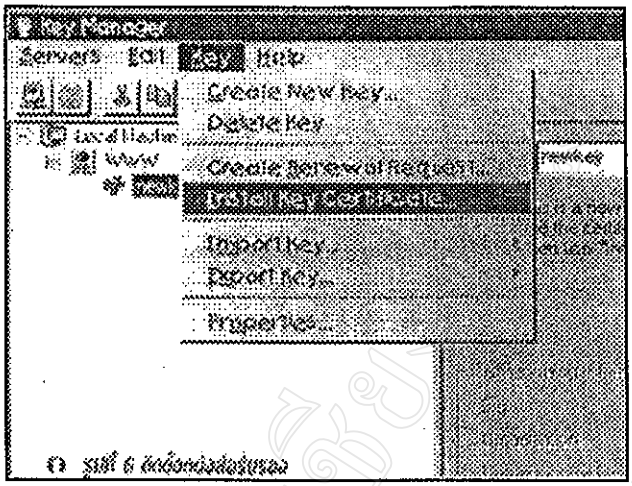
การติดตั้งไฟล์หนังสือรับรอง มีขั้นตอนคือดังนี้ พิจารณาภาพที่ 26

- ใน Key Manager คลิกไปที่กุญแจที่สร้างไว้ แล้วไปที่เมนู Key เลือก "Install Key Certificate..."
- เลือกไฟล์หนังสือรับรองที่เก็บไว้ และใส่ Password ที่กำหนดไว้ตอนสร้างไฟล์ CSR เพื่อยืนยันอีกรอบ

  ส่วนการนำ SSL เข้าไปใช้ในไดเรคทอรีที่ต้องการ ทำได้โดย
- เลือก Internet Service Manager ใน Toolbar จากนั้นดับเบิลคลิกที่ "www" เพื่อแสดงหน้า Properties
- เลือก tab Directories เลือกไดเรคทอรีที่ต้องการ แล้วคลิก "Edit Properties"
- ในช่อง "Access" ให้เลือก "Require Secure SSL Channel"

---

[59] เรื่องเดียวกัน : 87.



ภาพที่ 26 แสดงการติดตั้ง Key Certificate[60]

เพียงเท่านี้เว็บเซิร์ฟเวอร์ก็สามารถใช้งาน SSL ได้แล้ว ซึ่งหากใช้ซอฟต์แวร์เว็บเซิร์ฟเวอร์ยี่ห้ออื่นๆ จะต้องศึกษาขั้นตอนการสร้างไฟล์ CSR และการติดตั้งหนังสือรับรองจากคู่มือซอฟต์แวร์

5.3.2 SET : Secure Electronic Transaction

SET เป็นรูปแบบการชำระเงินที่ค่อนข้างซับซ้อนและต้องการโปรแกรมประกอบมากกว่า SSL เนื่องจาก SET ถูกออกแบบขึ้นมาเพื่ออุดช่องโหว่และข้อบกพร่องของ SSL การชำระเงินแบบ SET จะต้องมีการตรวจสอบกันและกัน โดยผู้ขายจะต้องตรวจสอบว่าบัตรเครดิตที่ผู้ซื้อใช้ชำระเงิน เป็นบัตรที่ใช้งานได้จริง มียอดเงินคงเหลือเพียงพอ ในขณะที่ฝ่ายผู้ซื้อก็ต้องตรวจสอบว่าผู้ขายเป็นผู้ที่ไว้ใจได้ ไม่นำบัตรเครดิตของตนไปใช้ในทางที่ไม่ควรดังนั้น SET จึงใช้วิธีแต่งตั้งบุคคลที่ 3 เป็นผู้ออกใบรับรองทั้ง 2 ฝั่ง รวมทั้งวิธีการป้องกันกับกรณีผู้ขายแอบนำหมายเลขบัตรเครดิตที่ได้มาไปใช้โดยไม่ได้รับอนุญาตอีกด้วย ซึ่งอาจสรุปได้ว่า SET จะต้องมีผู้ร่วมทำธุรกรรมทั้งหมด 4 ฝ่าย และแต่ละฝ่ายมีโปรแกรมสำหรับทำหน้าที่ของตนดังต่อไปนี้

---

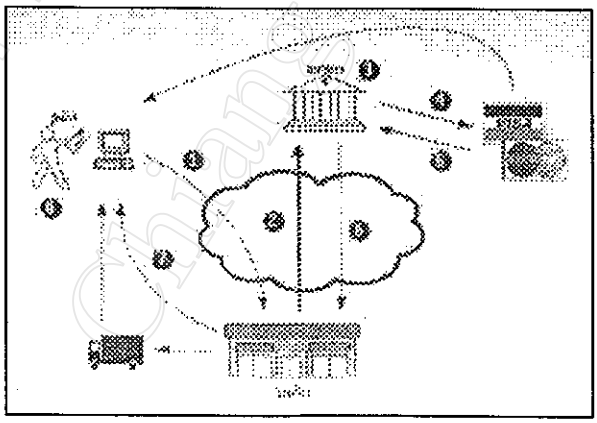
[60] เรื่องเดียวกัน : 88.

(1) ผู้ซื้อกับโปรแกรม E-Wallet เป็นโปรแกรมไคลเอนต์ที่ใช้ติดต่อกับโปรแกรมทางฝั่งเซิร์ฟเวอร์โดยอัตโนมัติ เพื่อตรวจสอบว่าเซิร์ฟเวอร์ที่ต้องการสั่งซื้อสินค้านี้มีใบรับรองว่าเป็นตัวจริงๆหรือไม่ อีกทั้งโปรแกรม E-Wallet จะตรวจสอบว่าเซิร์ฟเวอร์นี้มีการติดต่อกับสถาบันการเงินที่ไหน เป็นสถาบันที่มีใบรับรองหรือไม่

(2) ผู้ขายกับโปรแกรมฝ่ายขายหรือ Merchant Server เป็นโปรแกรมที่รวมเอาเทคโนโลยีด้านความปลอดภัยของข้อมูลเข้าไว้ด้วยกัน เนื่องจาก Merchant Server นี้จะต้องติดต่อกับทั้งผู้ซื้อ และสถาบันการเงินของผู้ซื้อ รวมทั้ง Merchant Server จะควบคุมการแลกเปลี่ยนและตรวจสอบใบรับรองก่อนที่จะมีการซื้อขายอีกด้วย

(3) ธนาคารกับโปรแกรมการชำระเงินหรือ Payment Gateway Server นี้จะช่วยให้ธนาคารสามารถดำเนินการรับชำระเงินจากผู้ซื้อได้ Payment Gateway Server ช่วยเชื่อมผู้ซื้อและผู้ขายในการซื้อขายเข้ากับระบบการชำระเงิน เพื่อให้การซื้อขายนั้นสำเร็จลุล่วง

(4) สถาบันผู้ออกบัตรเครดิตให้ผู้ซื้อกับโปรแกรมออกใบรับรองหรือ Certificate Authority เมื่อผู้ซื้อที่ถือบัตรเครดิตต้องการซื้อสินค้าด้วยโพรโตคอล SET นี้ จะต้องติดต่อสถาบันผู้ออกบัตรเครดิตของตนให้ออกใบรับรอง หรือ Certificate Authority นี้จะช่วยให้สถาบันการเงินเหล่านั้นใช้ออกใบรับรองดิจิตอลให้กับผู้ถือบัตรเครดิตและบรรดาร้านค้า เพื่อเป็นมาตรฐานในการตรวจสอบกันและกันระหว่างผู้ซื้อกับผู้ขาย



ภาพที่ 27 แสดงขั้นตอนการชำระเงินตามโพรโตคอล SET[61]

[61] BlueNet. "อี-คอมเมิร์ซ กับอุปสรรคที่ท้าทาย". BCM. (เมษายน 1999) : 139.

ขั้นตอนการทำ Transaction ตามโพรโตคอล SET ดังภาพที่ 27

(1) เมื่อผู้ซื้อเลือกสินค้าที่ต้องการได้แล้ว ก็จะยืนยันว่าพร้อมชำระเงิน โดยการคลิกที่หน้าเว็บแสดงสินค้านั้น โปรแกรม E-Wallet ซึ่งติดตั้งพร้อมใบรับรองผู้ซื้อบนเครื่องคอมพิวเตอร์ที่ผู้ซื้อใช้อยู่นั้นจะถูกเปิดขึ้นเพื่อให้ผู้ซื้อเลือกบัตรเครดิตที่ต้องการใช้ เมื่อผู้ซื้อเลือกบัตรเครดิตที่ต้องการแล้ว โปรแกรม E-Wallet จะจัดการนำหมายเลขบัตรเครดิตเข้ารหัสด้วยกุญแจสาธารณะของธนาคารที่ได้มา แล้วส่งไปยังเครื่องเว็บเซิร์ฟเวอร์ของผู้ขาย

(2) โปรแกรม Merchant ได้รับรายละเอียดดังกล่าว ก็จะส่งต่อไปยังธนาคารที่ผู้ขายมีบัญชีอยู่เพื่อให้ธนาคารรับการจ่ายเงินจากผู้ซื้อ เนื่องจากโปรแกรม Merchant นี้ไม่สามารถถอดรหัสหมายเลขบัตรเครดิตได้

(3) โปรแกรม Payment Gateway ที่ติดตั้งที่ธนาคารได้รับรายละเอียดจากที่ Merchant ส่งผ่านมาจะทำการถอดรหัสจนได้หมายเลขบัตรเครดิตที่ผู้ซื้อต้องการใช้ชำระเงิน

(4) Payment Gateway ส่งต่อหมายเลขบัตรเครดิตให้สถาบันผู้ออกบัตรตรวจสอบว่าบัตรนี้ใช้ชำระเงินได้ตามจำนวนที่สั่งซื้อหรือไม่ จะต้องเข้ารหัสข้อมูลก่อนส่งด้วยกุญแจสาธารณะของสถาบันผู้ออกบัตร

(5) สถาบันผู้ออกบัตรอนุมัติการชำระเงินผ่านบัตรตามหมายเลขที่ได้ พร้อมทั้งหักยอดเงินในบัญชีบัตรเครดิตของผู้ซื้อตามจำนวนที่ได้สั่งซื้อ จากนั้นส่งคำยืนยันการอนุมัติกลับไปยังธนาคาร

(6) ธนาคารนำฝากเงินใส่ในบัญชีของผู้ขายตามจำนวนที่ขายสินค้า และตอบยืนยันกลับไปยังโปรแกรม Merchant เพื่อยืนยันการชำระเงิน

(7) Merchant ยืนยันการขายให้โปรแกรม E-Wallet

(8) ผู้ซื้อจะได้รับใบแจ้งหนี้บัตรเครดิตที่ได้สั่งซื้อ

5.3.3 การตัดสินใจ

จะเห็นได้ว่า SSL นั้นนำมาใช้งานได้ง่ายและประหยัด เพียงแต่เสียค่าใช้จ่ายเฉพาะค่าจดทะเบียนหนังสือรับรองสำหรับร้านค้าเท่านั้น ผู้ซื้อก็สามารถใช้ SSL กับผู้ขายได้โดยไม่ต้องเสียค่าโปรแกรมและหนังสือรับรอง รวมทั้งไม่ต้องติดตั้งโปรแกรมเพิ่มเติมลงบนเครื่องคอมพิวเตอร์ก่อนทำการซื้อ อย่างไรก็ตาม SSL ยังมีช่องโหว่อีกหลายประการ เช่น หากมีคนแอบนำหมายเลขบัตรเครดิตของคนอื่นมาใช้ ร้านค้าก็ไม่สามารถตรวจสอบได้เลย ทำให้ร้านค้าต้องรับความเสี่ยงหากเจ้าของบัตรปฏิเสธการจ่ายเงินนั้น

SET ช่วยอุดช่องโหว่เหล่านี้ เนื่องจาก SET มีระบบการตรวจสอบที่รัดกุม แต่ข้อเสียของ SET ก็คือ ความยุ่งยากในการสั่งซื้อ เนื่องจากผู้ซื้อต้องติดตั้งโปรแกรมเพิ่มเติม และปัญหาที่สำคัญคือค่าใช้จ่าย เนื่องจากซอฟต์แวร์และหนังสือรับรองตามโพรโตคอล SET มีราคาสูงมาก

มีการคาดการณ์กันว่า SSL จะยังเป็นโพรโตคอลสำหรับการทำพาณิชย์อิเล็กทรอนิกส์ที่แพร่หลายที่สุดในระยะเวลา 3 ปีนี้ ซึ่งเมื่อถึงเวลานั้น ราคาของ SET อาจลดลงมาจนเป็นมาตรฐานใหม่ที่ทุกคนสามารถใช้ได้ แต่ก่อนจะถึงเวลานั้น SSL ก็ได้มีการปรับปรุงและพัฒนาขึ้นเรื่อยๆ โดยเมื่อเดือนกรกฎาคม 2541 Netscape Communications ได้มอบสิทธิความเป็นเจ้าของโพรโตคอล SSL ให้กับ Internet Engineering Task Force(IETF) ซึ่งเป็นหน่วยงานกลางทำงานด้านความปลอดภัยทางอินเตอร์เน็ต ซึ่ง IETF ได้ปรับปรุง SSL และเปลี่ยนชื่อเป็น Transport Layer Security (TLS)[62] TLS นี้จะถูกปรับแต่งให้มีตัวเลือกเสริมด้านการตรวจสอบว่าผู้ที่ติดต่อด้วยเป็นตัวตนจริงๆ กับที่อ้างไว้หรือไม่ ซึ่งการตรวจสอบนี้จะใช้การตรวจหนังสือรับรองตามมาตรฐาน X.509 ซึ่งเราก็ต้องจับตาดูกันต่อไปว่า TLS อาจจะมาเป็นคู่แข่ง SET ในวันข้างหน้า

---

[62] เรื่องเดียวกัน : 141.