บทที่ 2
เอกสารและงานวิจัยที่เกี่ยวข้อง

ปัจจุบันระบบอินเทอร์เน็ตมีการเติบโตอย่างรวดเร็ว ครอบคลุมทุกความต้องการ ตั้งแต่ระดับสำนักงาน สถานศึกษา ธุรกิจการค้า เป็นต้น ในมุมของผู้ใช้มีทุกระดับอายุ ทุกเพศ ทุกวัย ทุกระดับการศึกษา บริการที่มีให้ในอินเทอร์เน็ตมีอยู่มากมายหลายอย่าง เช่น ข่าวสาร ความบันเทิง การค้า และบริการอื่นๆ ที่สามารถค้นหาได้ และนับวันบริการต่างๆ ที่ปรากฏอยู่ในสังคมมีแนวโน้มของการเปลี่ยนจากการบริการแบบเดิมมาเป็นการให้บริการบนอินเทอร์เน็ตแทน การเข้าถึงอินเทอร์เน็ตเป็นเรื่องง่ายดายสำหรับทุกคน ไม่ว่าอยู่ที่ใดก็สามารถเชื่อมต่อเข้าสู่เครือข่ายอินเทอร์เน็ตได้ ด้วยปัจจัยการเอื้ออำนวยหลายอย่างที่เป็นผลมาจากความนิยมการใช้อินเทอร์เน็ต แม้แต่อินเทอร์เน็ตตามบ้านที่จะเห็นได้ว่ามีราคาค่าบริการที่ถูกมากเมื่อแลกกับความเร็วที่ได้ จึงไม่ใช่เรื่องแปลกที่อินเทอร์เน็ตมีการเติบโตอย่างมากในปัจจุบัน

ในความง่ายดายของการเข้าใช้อินเทอร์เน็ต การเข้าถึงข้อมูลและบริการได้จากทุกที่ทุกทางทำให้เกิดภัยมืดที่มองไม่เห็นอยู่อีกด้านหนึ่งของความสะดวกสบาย นั่นก็คือผู้ไม่ประสงค์ดีหรือผู้ที่อาศัยอินเทอร์เน็ตเป็นช่องทางกระทำความผิดทางกฎหมาย เช่น การโจรกรรมข้อมูล การเปลี่ยนแปลงข้อมูลให้ผู้อื่นเสียหาย การโจมตีระบบเพื่อให้บริการไม่สามารถดำเนินต่อไปได้ กลุ่มคนเหล่านี้เรารู้จักกันในนามแฮกเกอร์ (Hacker) ซึ่งนับวันข่าวการโจรกรรมข้อมูลหรือการใช้อินเทอร์เน็ตทำลายผู้อื่นทั้งทางตรงและทางอ้อมนั้น มีมากขึ้นทุกวันจากข่าวทางทีวีหรือหนังสือพิมพ์ และทุกครั้งที่มีข่าวเกิดขึ้นเจ้าพนักงานก็ไม่สามารถตามจับผู้กระทำความผิดมาลงโทษได้เนื่องจากไม่มีระบบใดๆ ที่มีการเก็บข้อมูลผู้ใช้หรือไม่มีการยืนยันตัวตนของผู้ใช้รายใดที่เข้าใช้งานอินเทอร์เน็ต ทำให้ใครก็ตามที่เชื่อมต่อระบบได้ก็สามารถใช้งานได้อย่างเสรี

2.1 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

คณะรัฐมนตรีได้เสนอร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิว-เตอร์ พ.ศ. 2550 ต่อสภานิติบัญญัติแห่งชาติในการประชุมครั้งที่ ๖/๒๕๔๙ เมื่อวันพุธที่ ๑๕ พฤศ-จิกายน ๒๕๔๙ โดยมีหลักการคือ “ให้มีกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์” (คณะกรรมการธุรกรรมทางอิเล็คทรอนิค, 2550)

และเหตุผลคือ “เนื่องจากในปัจจุบันระบบคอมพิวเตอร์ได้เป็นส่วนสำคัญของการประกอบกิจการและการดำรงชีวิตของมนุษย์ หากมีผู้กระทำด้วยประการใดๆ ให้ระบบคอมพิวเตอร์ไม่สามารถทำงานตามคำสั่งที่กำหนดไว้หรือทำให้การทำงานผิดพลาดไปจากคำสั่งที่กำหนดไว้

หรือใช้วิธีการใด ๆ เข้าล่วงรู้ข้อมูล แก้ไข หรือทำลายข้อมูลของบุคคลอื่นในระบบคอมพิวเตอร์โดยมิชอบ หรือใช้ระบบคอมพิวเตอร์เพื่อเผยแพร่ข้อมูลคอมพิวเตอร์อันเป็นเท็จหรือมีลักษณะอันลามกอนาจาร ย่อมก่อให้เกิดความเสียหาย กระทบกระเทือนต่อเศรษฐกิจ สังคม และความมั่นคงของรัฐ รวมทั้งความสงบสุขและศีลธรรมอันดีของประชาชน สมควรกำหนดมาตรการเพื่อป้องกันและปราบปรามการกระทำดังกล่าว จึงจำเป็นต้องตราพระราชบัญญัตินี้"

ที่ประชุมสภานิติบัญญัติแห่งชาติได้ลงมติรับหลักการแห่งร่างพระราชบัญญัติดังกล่าวไว้พิจารณา และตั้งคณะกรรมาธิการวิสามัญขึ้นคณะหนึ่งประกอบด้วยสมาชิกสภานิติบัญญัติแห่งชาติและผู้ทรงคุณวุฒิเกี่ยวกับวิชาการคอมพิวเตอร์และกฎหมายเพื่อพิจารณา คณะกรรมาธิการได้ประชุมพิจารณารวมทั้งสิ้น ๒๗ ครั้ง และได้เสนอต่อสภานิติบัญญัติเพื่อพิจารณาในวาระ ๒ และวาระ ๓ เมื่อวันที่ ๙ พฤษภาคม ๒๕๕๐ และได้มีมติให้ผ่านร่างพระราชบัญญัติฉบับนี้เพื่อให้มีผลบังคับใช้เป็นกฎหมายต่อไป ซึ่งต่อมาได้มีการประกาศในราชกิจจานุเบกษา เล่ม ๑๒๘ ตอน ๒๗ก. ลงวันที่ ๑๘ มิถุนายน ๒๕๕๐ (มาตรา ๒ พระราชบัญญัตินี้ให้ใช้บังคับเมื่อพ้นกำหนดสามสิบวันนับแต่วันประกาศในราชกิจจานุเบกษาเป็นต้นไป)

2.2 ความปลอดภัยบนระบบเครือข่าย

ในปัจจุบันระบบคอมพิวเตอร์ได้ถูกคุกคามมากขึ้นทั้งจากไวรัสคอมพิวเตอร์หรือจากผู้ไม่ประสงค์ดี ซึ่งความมั่นคงปลอดภัยคอมพิวเตอร์ (Computer Security) ช่วยปกป้องเครื่องคอมพิวเตอร์รวมไปถึงอุปกรณ์ต่างๆ ที่เกี่ยวข้อง และที่สำคัญยังสามารถช่วยปกป้องข้อมูลที่ได้จัดเก็บไว้ภายในระบบหรือใช้ในความหมายความปลอดภัยทางข้อมูลสารสนเทศ (Information Security) ก็ได้ จุดประสงค์หลักของความปลอดภัยทางข้อมูลคือ ความลับ (Confidentiality) ความสมบูรณ์ (Integrity) ความพร้อมใช้ (Availability) และการห้ามปฏิเสธความรับผิดชอบ (Non-Repudiation) ของข้อมูลต่างๆ ภายในองค์กร (CIA-N) โดยมีรายละเอียดดังนี้

2.2.1 การรักษาความลับ (Confidentiality) คือการรับรองว่าจะมีการเก็บข้อมูลไว้เป็นความลับ และผู้มีสิทธิเท่านั้นจึงจะเข้าถึงข้อมูลนั้นได้

2.2.2 การรักษาความสมบูรณ์ (Integrity) คือการรับรองว่าข้อมูลจะไม่ถูกเปลี่ยนแปลง หรือทำลายไม่ว่าจะเป็นโดย อุบัติเหตุหรือโดยเจตนา

2.2.3 ความพร้อมใช้ (Availability) คือการรับรองว่าข้อมูลและบริการการสื่อสารต่างๆ พร้อมที่จะใช้ได้ในเวลาที่ต้องการใช้งาน

2.2.4 การห้ามปฏิเสธความรับผิดชอบ (Non-Repudiation) คือวิธีการสื่อสารซึ่งผู้ส่งข้อมูลได้รับหลักฐานว่าได้มีการส่งข้อมูลแล้วและผู้รับก็ได้รับการยืนยันว่าผู้ส่งเป็นใคร ดังนั้นทั้งผู้ส่งและผู้รับจะไม่สามารถปฏิเสธได้ว่าไม่มีความเกี่ยวข้องกับข้อมูลดังกล่าวในภายหลัง

ในทางปฏิบัตินั้นสามารถกำหนดลักษณะของการควบคุมความมั่นคงปลอดภัย (Security Controls) ได้ 5 ระดับตามภาพ

ภาพที่ 2-1 Security Pyramid

ที่มา : สิริพร จิตต์เจริญธรรม และคณะ (2547)

และถือเป็นองค์ประกอบที่สำคัญส่วนหนึ่งของความมั่นคงปลอดภัยคอมพิวเตอร์ เพราะจัดเป็นการกำหนดและควบคุมทั้งบุคคลที่สามารถเข้าสู่ระบบและเข้าสู่ข้อมูลภายในระบบ และเพื่อกระทำการใดได้บ้าง อนุญาตตามระดับชั้นของความสำคัญของข้อมูล รวมไปถึงการจัดเก็บพฤติกรรมการใช้งานระบบของบุคคลนั้นต่อข้อมูลบนระบบทั้งหมด

2.3 **การพิสูจน์ตัวตน** (Authentication)

การพิสูจน์ตัวตน คือขั้นตอนการยืนยันความถูกต้องของหลักฐานที่แสดงว่าเป็นบุคคลที่กล่าวอ้างจริง ในทางปฏิบัติจะแบ่งออกเป็น 2 ขั้นตอน คือ

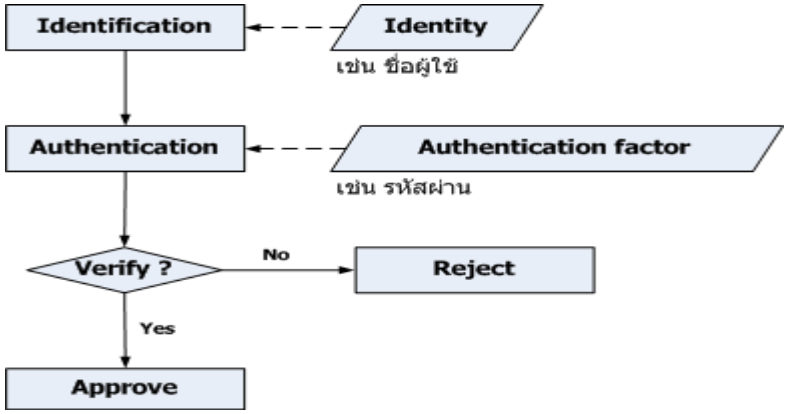
2.3.1 การระบุตัวตน (Identification) คือขั้นตอนที่ผู้ใช้แสดงหลักฐานว่าตนเองคือใคร เช่น ชื่อผู้ใช้ (Username) โดยมีกลไกของการพิสูจน์ตัวตน (Authentication Mechanisms) ซึ่งสามารถแบ่งออกได้เป็น 3 ลักษณะคือ

2.3.1.1 สิ่งที่คุณมี (Possession Factor) เช่น กุญแจหรือเครดิตการ์ดเป็นต้น

2.3.1.2 สิ่งที่คุณรู้ (Knowledge factor) เช่น รหัสผ่าน (passwords) หรือการใช้พิน (PINs)

2.3.1.3 สิ่งที่คุณเป็น (Biometric factor) เช่น ลายนิ้วมือ รูปแบบเรตินา (retinal patterns) หรือใช้รูปแบบเสียง (voice patterns) เป็นต้น

2.3.2 การพิสูจน์ตัวตน (Authentication) คือขั้นตอนที่ตรวจสอบหลักฐานเพื่อแสดงว่าเป็นบุคคลที่กล่าวอ้างจริง



ภาพที่ 2-2 แผนผังแสดงกระบวนการการพิสูจน์ตัวตน

ที่มา : สิริพร จิตต์เจริญธรรม และคณะ (2547)

จากแผนผังแสดงกระบวนการพิสูจน์ตัวตน ในขั้นแรกผู้ใช้จะทำการแสดงหลักฐานที่ใช้ในการพิสูจน์ตัวตนต่อระบบ ซึ่งในขั้นนี้คือการระบุตัวตน และในขั้นตอนต่อมาระบบจะทำการตรวจสอบหลักฐานที่ผู้ใช้นำมากล่าวอ้างซึ่งก็คือการพิสูจน์ตัวตน หลังจากระบบได้ทำการตรวจสอบหลักฐานเรียบร้อยแล้วถ้าหลักฐานที่นำมากล่าวอ้างถูกต้องจึงอนุญาตให้เข้าสู่ระบบได้ หากหลักฐานที่นำมากล่าวอ้างไม่ถูกต้องผู้ใช้จะถูกปฏิเสธจากระบบ และหลักฐานที่ผู้ใช้นำมากล่าวอ้างที่เกี่ยวกับเรื่องของความปลอดภัยนั้นสามารถจำแนกได้ 2 ชนิด ดังนี้

2.3.2.1 Actual identity คือหลักฐานที่สามารถบ่งบอกได้ว่าในความเป็นจริงบุคคลที่กล่าวอ้างนั้นเป็นใคร

2.3.2.2 Electronic identity คือหลักฐานทางอิเล็กทรอนิกส์ซึ่งสามารถบ่งบอกข้อมูลของบุคคลนั้นได้ แต่ละบุคคลอาจมีหลักฐานทางอิเล็กทรอนิกส์ได้มากกว่า 1 หลักฐาน ตัวอย่างเช่น บัญชีชื่อผู้ใช้

กระบวนการพิสูจน์ตัวตนนั้น จะนำหลักการข้างต้นมาใช้ในการยืนยันหลักฐานที่นำมากล่าวอ้าง ทั้งนี้ขึ้นอยู่กับระบบ วิธีการที่นำมาใช้เพียงลักษณะอย่างใดอย่างหนึ่ง (Single-factor authentication) นั้น มีข้อจำกัดในการใช้ ตัวอย่างเช่น สิ่งที่คุณมี (Possession factor) นั้นอาจจะสูญหายหรือถูกขโมยได้ สิ่งที่คุณรู้ (Knowledge factor) อาจจะถูกดักฟัง เดา หรือขโมยจากเครื่อง

คอมพิวเตอร์ สิ่งที่คุณเป็น (Biometric factor) จัดได้ว่าเป็นวิธีที่มีความปลอดภัยสูงอย่างไรก็ตาม การที่จะใช้เทคโนโลยีนี้ได้นั้นจำเป็นต้องมีการลงทุนที่สูง ดังนั้นจึงได้มีการนำแต่ละคุณลักษณะมาใช้ร่วมกัน (multi-factor authentication) ตัวอย่างเช่น ใช้สิ่งที่มีกับสิ่งที่รู้มาใช้ร่วมกัน เช่น การใช้ลายมือชื่อร่วมกับการใช้บัตรเครดิตหรือการใช้รหัสผ่านร่วมกับการใช้บัตร ATMเป็นต้น การนำแต่ละลักษณะของการพิสูจน์ตัวตนมาใช้ร่วมกันมากกว่า 1 ลักษณะ จะช่วยเพิ่มประสิทธิภาพในการรักษาความปลอดภัยของข้อมูล

2.4 **การกำหนดสิทธิ์** (Authorization)

การกำหนดสิทธิ์ คือขั้นตอนในการอนุญาตให้แต่ละบุคคลสามารถเข้าถึงข้อมูลหรือระบบใดได้บ้าง ก่อนอื่นต้องทราบก่อนว่าบุคคลที่กล่าวอ้างนั้นคือใครตามขั้นตอนการพิสูจน์ตัวตนและต้องให้แน่ใจด้วยว่าการพิสูจน์ตัวตนนั้นถูกต้อง

2.5 **การเข้ารหัส** (Encryption)

การเข้ารหัส คือการเก็บข้อมูลให้เป็นส่วนบุคคลจากบุคคลอื่นที่ไม่ได้รับอนุญาต ส่วนประกอบ 2 ส่วนที่สำคัญที่จะช่วยทำให้ข้อมูลนั้นเป็นความลับได้ก็คือ การกำหนดสิทธิ์และการพิสูจน์ตัวตนเพราะว่าก่อนการอนุญาตให้บุคคลที่กล่าวอ้างเข้าถึงข้อมูลหรือถอดรหัสข้อมูลนั้นต้องสามารถแน่ใจได้ว่าบุคคลที่กล่าวอ้างนั้นเป็นใครและได้รับอนุญาตให้สามารถเข้ามาดูข้อมูลได้หรือไม่ ในการเข้ารหัสนั้นวิธีการหนึ่งที่ทำได้คือการเข้ารหัสในรูปแบบของกุญแจลับ (Secret key) ซึ่งในการใช้คีย์รูปแบบนี้ต้องเฉพาะผู้ที่มีกุญแจลับนี้เท่านั้นที่สามารถรับข้อมูลที่เข้ารหัสแล้วได้

2.6 **การรักษาความสมบูรณ์** (Integrity)

การรักษาความสมบูรณ์ คือการรับรองว่าข้อมูลจะไม่ถูกเปลี่ยนแปลงหรือทำลายไปจากต้นฉบับ (Source) ไม่ว่าจะเป็นโดยบังเอิญหรือดัดแปลงโดยเจตนาที่อาจส่งผลเสียต่อข้อมูล การคุกคามความสมบูรณ์ของข้อมูลคือการที่บุคคลที่ไม่ได้รับอนุญาตสามารถที่จะเข้าควบคุมการจัดการของข้อมูลได้

2.7 **การตรวจสอบ** (Audit)

การตรวจสอบ คือการตรวจสอบหลักฐานทางอิเล็กทรอนิกส์ ซึ่งสามารถใช้ในการติดตามการดำเนินการเพื่อตรวจสอบความถูกต้องและแม่นยำ ตัวอย่างเช่นการตรวจสอบบัญชีชื่อผู้ใช้ โดยผู้ตรวจบัญชี ซึ่งการตรวจสอบความถูกต้องของการดำเนินการเพื่อให้แน่ใจว่าหลักฐานทางอิเล็กทรอนิกส์นั้นได้ถูกสร้างและสั่งให้ทำงานโดยบุคคลที่ได้รับอนุญาต และในการเชื่อมต่อ

เหตุการณ์เข้ากับบุคคลจะต้องทำการตรวจสอบหลักฐานของบุคคลนั้นด้วย ซึ่งถือเป็นหลักการพื้นฐานของขั้นตอนการทำงานของการพิสูจน์ตัวตนด้วย

การพิสูจน์ตัวตนจัดเป็นการตรวจสอบหลักฐานขั้นพื้นฐานที่สำคัญที่สุดใน 5 ระดับชั้นของการควบคุมความปลอดภัย ดังนั้นการพิสูจน์ตัวตนดีจะช่วยเพิ่มความมั่นคงปลอดภัยขั้นพื้นฐานให้กับระบบมากยิ่งขึ้น

2.8 **ประเภทของการพิสูจน์ตัวตน** (Authentication Types)

ส่วนประกอบพื้นฐานของการพิสูจน์ตัวตนสามารถแบ่งออกได้เป็นส่วนต่างๆ ดังนี้

2.8.1 การพิสูจน์ตัวตน (Authentication) คือส่วนที่สำคัญที่สุดเพราะเป็นขั้นตอนแรกของการเข้าใช้ระบบ ผู้เข้าใช้ระบบต้องถูกยอมรับจากระบบว่าสามารถเข้าสู่ระบบได้ การพิสูจน์ตัวตนเป็นการตรวจสอบหลักฐานเพื่อแสดงว่าเป็นบุคคลนั้นจริง

การพิสูจน์ตัวตน (Authentication) มีความสำคัญที่สุดกับการเข้าใช้ระบบ จึงสามารถแจกแจงชนิดของการพิสูจน์ตัวตนที่ใช้กันอยู่ในปัจจุบัน ดังนี้

2.8.1.1 ไม่มีการพิสูจน์ตัวตน (No Authentication) ตามหลักการแล้วการพิสูจน์ตัวตนไม่มีความจำเป็น ถ้าเงื่อนไขต่อไปนี้เป็นจริง

1) ข้อมูลเหล่านั้นเป็นข้อมูลสาธารณะ ที่อนุญาตให้ทุกคนเข้าใช้บริการและเปลี่ยนแปลงได้

2) ข้อมูลข่าวสารหรือแหล่งของข้อมูลนั้นๆ สามารถเข้าถึงได้เฉพาะบุคคลที่ได้รับอนุญาตเท่านั้น

2.8.1.2 การพิสูจน์ตัวตนโดยใช้รหัสผ่าน (Authentication by Passwords) รหัสผ่านเป็นวิธีการที่ใช้มานานและนิยมใช้กันแพร่หลาย รหัสผ่านควรจำกัดให้เฉพาะผู้ใช้ที่มีสิทธิเท่านั้นที่ทราบ หากแต่ว่าในปัจจุบันนี้ การใช้แค่รหัสผ่านไม่มีประสิทธิภาพมากพอที่จะรักษาความมั่นคงปลอดภัยให้กับระบบคอมพิวเตอร์หรือระบบเครือข่ายคอมพิวเตอร์ เนื่องจากการตั้งรหัสผ่านที่ง่ายเกินไป และวิทยาการและความรู้ที่ก้าวหน้าทำให้รหัสผ่านอาจจะถูกขโมยโดยระหว่างการสื่อสารผ่านเครือข่ายได้

2.8.1.3 การพิสูจน์ตัวตนโดยใช้ PIN (Authentication by PIN) PIN (Personal Identification Number) เป็นรหัสลับส่วนบุคคลที่ใช้เป็นรหัสผ่านเพื่อเข้าสู่ระบบ ซึ่ง PIN ใช้อย่างแพร่หลายโดยเฉพาะการทำธุรกรรมทางด้านธนาคาร เช่นบัตร ATM และเครดิตการ์ดต่างๆ ซึ่งการใช้ PIN ทำให้มีความปลอดภัยในการสื่อสารข้ามระบบเครือข่ายสาธารณะมากขึ้น

เนื่องจาก PIN จะถูกเข้ารหัสเอาไว้และจำเป็นต้องมีเครื่องมือที่สามารถถอดรหัสนี้ออกมาได้ เช่น ฮาร์ดแวร์ที่ออกแบบมาโดยเฉพาะ และถูกติดตั้งไว้ในเครื่องของผู้รับและผู้ส่งเท่านั้น

2.8.1.4 การพิสูจน์ตัวตนโดยใช้ Password Authenticators หรือ Token (Authentication by Password Authenticators or Tokens) เป็นฮาร์ดแวร์พิเศษที่ใช้สร้าง "รหัสผ่านซึ่งเปลี่ยนแปลงได้ (dynamic password)" ในขณะที่กำลังเข้าสู่ระบบเครือข่าย มี 2 วิธี คือ ซิงโครนัส และอะซิงโครนัส การพิสูจน์ตัวตนแบบซิงโครนัส แบ่งออกเป็น 2 ประเภทตามลักษณะของการใช้งาน คือ

1) การพิสูจน์ตัวตนแบบซิงโครนัสโดยขึ้นอยู่กับสถานการณ์ (Event-synchronous authentication) เมื่อผู้ใช้ต้องการที่จะเข้าสู่ระบบ ผู้ใช้จะต้องกด Token เพื่อให้ Token สร้างรหัสผ่านให้ จากนั้นผู้ใช้นำรหัสผ่านที่แสดงหลังจากกด Token ใส่ลงในฟอร์มเพื่อเข้าสู่ระบบ ระบบจะทำการตรวจสอบกับเซิร์ฟเวอร์ก่อน ว่ารหัสผ่านที่ใส่มีอยู่ในเซิร์ฟเวอร์จริง จึงจะยินยอมให้ผู้ใช้เข้าสู่ระบบ

2) การพิสูจน์ตัวตนแบบซิงโครนัสโดยขึ้นอยู่กับเวลา (Time-synchronous authentication) เป็นวิธีการที่สร้างรหัสผ่านโดยมีการกำหนดช่วงระยะเวลาการใช้งาน โดยปกติแล้วรหัสผ่านจะถูกเปลี่ยนทุกๆ หนึ่งนาที การสร้างรหัสผ่านจะเป็นไปอย่างต่อเนื่อง ทำให้บางครั้งรหัสผ่านที่สร้างออกมาอาจจะซ้ำกันกับรหัสผ่านตัวอื่นที่เคยสร้างมาแล้วก็ได้ เมื่อผู้ใช้ต้องการเข้าสู่ระบบก็ใส่รหัสผ่านและเวลาที่รหัสผ่านตัวนั้นถูกสร้างขึ้นมา (รหัสผ่านจะถูกสร้างขึ้นมาจาก Token) ลงในฟอร์ม เพื่อเข้าสู่ระบบ ระบบจะทำการตรวจสอบเวลาและรหัสผ่านที่ผู้ใช้ใส่ลงไป กับเซิร์ฟเวอร์ว่ารหัสผ่านที่ใส่ตรงกับเวลาที่ Token สร้าง และมีอยู่ในเซิร์ฟเวอร์จริง จึงยินยอมให้ผู้ใช้เข้าสู่ระบบ

3) การพิสูจน์ตัวตนแบบอะซิงโครนัส หรือเรียกอีกอย่างหนึ่งว่า "challenge-response" ถูกพัฒนาขึ้น เป็นลำดับแรกๆ ของระบบการใช้ "รหัสผ่านซึ่งเปลี่ยนแปลงได้" ซึ่งถือได้ว่าเป็นการป้องกันการจู่โจมที่ปลอดภัยที่สุด เพราะเนื่องจากว่าเมื่อผู้ใช้ต้องการจะเข้าสู่ระบบ ผู้ใช้จะต้องทำการร้องขอไปยังเซิร์ฟเวอร์ จากนั้นเซิร์ฟเวอร์ก็จะส่ง challenge string มาให้ผู้ใช้ เพื่อให้ผู้ใช้ใส่ลงใน Token ที่ผู้ใช้ถืออยู่ จากนั้น Token จะทำการคำนวณรหัสผ่านออกมาให้ผู้ใช้ ผู้ใช้จึงสามารถนำรหัสผ่านนั้นใส่ลงในฟอร์มเพื่อเข้าสู่ระบบได้ การพิสูจน์ตัวตนแบบซิงโครนัสทั้งไคลเอ็นต์และเซิร์ฟเวอร์จะมีรหัสผ่านเก็บเอาไว้ แต่แบบอะซิงโครนัส ไคลเอ็นต์จะต้องติดต่อเซิร์ฟเวอร์ก่อน ก่อนจะได้รับรหัสผ่านจริง ทำให้การพิสูจน์ตัวตนแบบอะซิงโครนัสมีขั้นตอนที่ซับซ้อนกว่าแบบซิงโคนัส

2.8.1.5 การพิสูจน์ตัวตนโดยใช้ลักษณะเฉพาะทางชีวภาพของแต่ละบุคคล (Authentication by Biometric traits) ลักษณะทางชีวภาพของแต่ละบุคคลเป็นลักษณะเฉพาะและลอกเลียนแบบกันไม่ได้ การนำมาใช้ในการพิสูจน์ตัวตนจะเพิ่มความน่าเชื่อถือได้มากขึ้นเช่น การใช้ลายนิ้วมือ เสียง ม่านตา เป็นต้น จึงมีการนำเทคโนโลยีนี้มาช่วยในการพิสูจน์ตัวตน เพื่อเพิ่มความปลอดภัยก่อนเข้าสู่ระบบ เช่นการใช้ควบคู่กับการใช้รหัสผ่าน ในขั้นตอนของการตรวจสอบหลักฐาน ผู้ใช้ที่ถือ token การ์ด หรือสมาร์ทการ์ด จะนำบัตรมาผ่านเครื่องอ่านบัตรและแสดงเรตินาให้เครื่องเก็บภาพ เมื่อเครื่องอ่านบัตร อ่านค่าเลขที่ได้จากบัตรแล้ว ก็จะนำไปหากุญแจ ซึ่งในขณะเดียวกันภาพเรตินาที่เครื่องเก็บไว้ได้ ก็จะนำไปแยกแยะเพื่อหาลักษณะเด่น แล้วเก็บค่าไว้เป็น template และนำ template ที่ได้ไปตรวจสอบกับ template ที่เก็บไว้เพื่อหากุญแจ และนำกุญแจที่ได้มาเปรียบเทียบกันว่าตรงกันหรือไม่ ถ้าตรงกันก็แสดงว่าผู้ที่ถือบัตรกับผู้ใช้เป็นคนเดียวกัน จึงอนุญาตให้เข้าสู่ระบบได้

2.8.1.6 การพิสูจน์ตัวตนโดยใช้รหัสผ่านที่ใช้เพียงครั้งเดียว (One-Time Password: OTP) One-Time Password ถูกพัฒนาขึ้นเพื่อหลีกเลี่ยงปัญหาที่เกิดจากการใช้รหัสผ่านเพียงตัวเดียวซ้ำๆ กัน OTP จะทำให้ระบบมีความปลอดภัยมากขึ้น เพราะรหัสผ่านจะถูกเปลี่ยนทุกครั้งก่อนที่ผู้ใช้จะเข้าสู่ระบบ การทำงานของ OTP คือเมื่อผู้ใช้ต้องการจะเข้าใช้ระบบ ผู้ใช้จะทำการร้องขอไปยังเซิร์ฟเวอร์ จากนั้นเซิร์ฟเวอร์จะส่ง challenge string กลับมาให้ผู้ใช้ จากนั้นผู้ใช้จะนำ challenge string และรหัสลับที่มีอยู่กับตัวของผู้ใช้นำไปเข้าแฮชฟังก์ชันแล้วออกมาเป็นค่า response ผู้ใช้ก็จะส่งค่านั้นกลับไปยังเซิร์ฟเวอร์ เซิร์ฟเวอร์จะทำการตรวจสอบค่าที่ผู้ใช้ส่งมาเปรียบเทียบกับค่าที่เซิร์ฟเวอร์เองคำนวณได้ โดยเซิร์ฟเวอร์ก็ใช้วิธีการคำนวณเดียวกันกับผู้ใช้ เมื่อได้ค่าที่ตรงกันเซิร์ฟเวอร์ก็จะยอมรับให้ผู้ใช้เข้าสู่ระบบ

2.8.1.7 การพิสูจน์ตัวตนโดยการเข้ารหัสโดยใช้กุญแจสาธารณะ (Public-Key Cryptography) เป็นการรักษาความปลอดภัยของข้อมูลระหว่างการส่งข้ามเครือข่ายวิธีหนึ่งที่นิยมใช้กันอยู่ในปัจจุบัน การเข้ารหัสแบบคู่รหัสกุญแจนี้จะมีความปลอดภัยมากกว่าการเข้ารหัสข้อมูลแบบธรรมดา แต่ก็ไม่ได้หมายความว่าการเข้ารหัสแบบคู่รหัสกุญแจนี้จะเป็นวิธีที่เหมาะสมที่สุดของวิธีการเข้ารหัส ทั้งนี้ขึ้นอยู่กับประเภทงานของแต่ละองค์กรหรือบุคคล การเข้ารหัสโดยใช้กุญแจสาธารณะ ประกอบไปด้วยกุญแจสองชนิด ที่ต้องใช้คู่กันเสมอในการเข้ารหัสและถอดรหัส ได้แก่ กุญแจสาธารณะ (Public Key) เป็นกุญแจที่ผู้สร้างจะส่งออกไปให้ผู้ใช้อื่นๆ ทราบหรือเปิดเผยได้ กับกุญแจส่วนตัว (Private Key) เป็นกุญแจที่ผู้สร้างจะเก็บไว้ โดยไม่เปิดเผยให้คนอื่นรู้ โดยกระบวนการของการเข้ารหัสแบบคู่รหัสกุญแจ มีดังนี้

1) ผู้ใช้แต่ละคนจะสร้างคู่รหัสกุญแจของตัวเองขึ้นมา เพื่อใช้สำหรับการเข้ารหัสและการถอดรหัส

2) กุญแจสาธารณะจะถูกส่งออกไปยังผู้ใช้คนอื่นๆ แต่กุญแจส่วนตัวจะถูกเก็บที่ตนเอง

3) เมื่อจะส่งข้อมูลออกไปหาผู้ใช้คนใด ข้อมูลที่ส่งจะถูกเข้ารหัสด้วยกุญแจสาธารณะ ก่อนถูกส่งออกไป

4) เมื่อผู้รับได้รับข้อความแล้วจะใช้กุญแจส่วนตัวซึ่งเป็นคู่รหัสกันถอดรหัสออกมา

การเข้ารหัสโดยใช้กุญแจสาธารณะสามารถใช้ได้ทั้งในการเข้ารหัส (Encryption) และการพิสูจน์ตัวตน (Authentication)

การประยุกต์ใช้ในการเข้ารหัสข้อมูล (Encryption) เป็นการนำข้อมูลที่จะส่งไปยังผู้รับมาเข้ารหัสด้วยกุญแจสาธารณะของผู้รับ และเมื่อผู้รับได้รับข้อความนั้นแล้วจะถอดรหัสออกมาด้วยกุญแจส่วนตัว จึงจะเห็นได้ว่ามีเพียงผู้รับเท่านั้นที่จะสามารถถอดรหัสออกมาได้

การประยุกต์ใช้ในการพิสูจน์ตัวตน (Authentication) เป็นการนำข้อมูลที่ผู้ส่งต้องการส่งมาเข้ารหัสด้วยกุญแจส่วนตัวของผู้ส่ง แล้วนำข้อมูลนั้นส่งไปยังผู้รับ ซึ่งผู้รับจะใช้กุญแจสาธารณะซึ่งเป็นคู่รหัสกันถอดรหัสออกมา ผู้รับก็สามารถรู้ได้ว่าข้อความนั้นถูกส่งมาจากผู้ส่งคนนั้นจริง ถ้าสามารถถอดรหัสข้อมูลได้อย่างถูกต้อง

2.8.1.8 การพิสูจน์ตัวตนโดยการใช้ลายเซ็นอิเล็กทรอนิคส์ (Digital Signature) เป็นการนำหลักการของการทำงานของระบบการเข้ารหัสแบบใช้คู่รหัสกุญแจเพื่อการพิสูจน์ตัวตนมาประยุกต์ใช้ ระบบของลายเซ็นดิจิตอลสามารถแบ่งเป็นขั้นตอนได้ดังนี้

1) เมื่อผู้ใช้ต้องการจะส่งข้อมูลไปยังผู้รับ ข้อมูลนั้นจะถูกนำไปเข้าฟังก์ชั่นทางคณิตศาสตร์ที่เรียกว่า "แฮชฟังก์ชัน" ได้เมสเซสไดเจสต์ (Message Digest) ออกมา

2) การใช้กุญแจส่วนตัวเข้ารหัสข้อมูล หมายถึงว่าผู้ส่งได้ลงลายเซ็นดิจิตอล ยินยอมที่จะให้ผู้รับ สามารถทำการตรวจสอบด้วยกุญแจสาธารณะของผู้ส่งเพื่อพิสูจน์ตัวตนของผู้ส่งได้

3) การตรวจสอบข้อมูลว่าถูกส่งมาจากผู้ส่งคนนั้นจริงในด้านผู้รับ โดยการนำข้อมูลมาผ่านแฮชฟังก์ชันเพื่อคำนวณหาค่าเมสเซจไดเจสต์ และถอดรหัสลายเซ็นอิเล็กทรอนิคส์ด้วยกุญแจสาธารณะของผู้ส่ง ถ้าสามารถถอดได้อย่างถูกต้อง จะเป็นการยืนยัน

ข้อมูลจากผู้ส่งคนนั้นจริง และถ้าข้อมูลเมสเซจไดเจสต์ที่ได้จากการถอดรหัสเท่ากันกับค่าเมสเซจไดเจสต์ในตอนต้นที่ทำการคำนวณได้ จะถือว่าข้อมูลดังกล่าวนั้นถูกต้อง

2.8.1.9 การพิสูจน์ตัวตนโดยใช้การถาม-ตอบ (Zero-knowledge Proofs) เป็นวิธีการพิสูจน์ตัวตนโดยใช้การถาม-ตอบ เมื่อผู้ใช้เข้ามาในระบบแล้ว ระบบจะแน่ใจได้อย่างไรว่าผู้ใช้คนนั้น เป็นคนที่ได้รับอนุญาตให้เข้ามาใช้ระบบได้จริง การใช้ชื่อผู้ใช้และรหัสผ่าน ในปัจจุบันนี้ไม่มีความปลอดภัยเพียงพอต่อการเข้าใช้ระบบ เนื่องจากความรู้และวิทยาการที่ก้าวหน้าทำให้เกิดผู้ที่ต้องการจะเข้ามาละเมิดระบบต่างๆ มีมากขึ้น ทำให้ชื่อผู้ใช้และรหัสผ่าน อาจจะถูกลักลอบดักข้อมูลระหว่างการสื่อสารกันได้ การที่จะทำให้ระบบมั่นใจได้ว่า ผู้ที่เข้าไปในระบบผู้นั้นเป็นผู้ที่ได้รับอนุญาตจริง นั่นก็คือ ระบบจะใช้การถาม - ตอบ ซึ่งคำถามและคำตอบเหล่านี้ ผู้ใช้จะเป็นคนสร้างคำถามและคำตอบขึ้นมาเอง จากนั้นจะส่งให้กับเซิร์ฟเวอร์ ซึ่งคำถาม - คำตอบที่ผู้ใช้สร้างขึ้นมา ผู้ใช้เท่านั้นจะเป็นคนที่ทราบคำตอบของแต่ละคำถามที่ถูกสร้าง และเมื่อผู้ใช้คนนั้นๆ เข้าสู่ระบบได้ ระบบจะถามสุ่มคำถามเหล่านั้นที่ผู้ใช้คนนั้นๆ สร้างขึ้นมา ถามผู้ใช้คนนั้นๆ ก่อนที่จะยอมให้เข้าใช้ระบบได้จริง การให้ใช้ระบบได้จริงจะได้รับการยินยอมก็ต่อเมื่อการตอบคำตอบที่ผู้ใช้ตอบ นั้นสัมพันธ์กับคำตอบที่มีอยู่ในเซิร์ฟเวอร์ ยกตัวอย่างเช่น นาย ก. กับ นาย ข. รู้จักกันมานานละสนิทกัน นาย ก. และ นาย ข. ย่อมมีความสนิทกันเป็นส่วนตัวเมื่อนาย ก. และนาย ข. เล่น MSN กัน ต่างฝ่ายต่างจะแน่ใจได้อย่างไรว่า คนที่ตนคุยอยู่เป็นบุคคลเดียวกันกับที่ตนรู้จัก เพราะว่านาย ก. หรือ นาย ข. อาจจะทำการเข้าระบบทิ้งไว้ หรือ อาจจะมีบุคคลอื่นสามารถดักจับหลักฐานและข้อมูลที่สามารถเข้าสู่ระบบของคนใดคนหนึ่งไว้ได้ แล้วทำการสวมรอยแทน นั่นก็คือการใช้คำถามและคำตอบที่มีเพียงนาย ก. และ นาย ข. เท่านั้นที่ทราบ

วิธีการพิสูจน์ตัวตนวิธีนี้ เป็นวิธีการที่ต้องใช้ความรู้ขั้นสูงในการนำมาใช้ เนื่องจากระบบจะใช้การเรียนรู้จากข้อมูลที่ได้รับ อาจจะเรียกระบบนี้ได้ว่าเป็นการนำความรู้ด้าน AI (Artificial Intelligence) มาใช้นั่นเอง

2.8.1.10 โพรโตคอลในการพิสูจน์ตัวตน (Authentication Protocol) ในระบบเครือข่ายแบบเปิดหรืออินเตอร์เน็ต การพิสูจน์ตัวตนถือได้ว่าเป็นกระบวนการเริ่มต้นและมีความสำคัญที่สุดในการปกป้องเครือข่ายให้ปลอดภัย โพรโตคอลในการพิสูจน์ตัวตน คือ โพรโตคอลการสื่อสารที่มีกระบวนการพิสูจน์ตัวตนรวมอยู่ในชุดโพรโตคอล และโพรโตคอลการพิสูจน์ตัวตนที่นิยมใช้อย่างแพร่หลายบนอินเตอร์เน็ตในปัจจุบัน ประกอบไปด้วย

1) Secure Socket Layer (SSL) พัฒนาโดย Netscape Communications เพื่อใช้ในโพรโตคอลระดับแอพพลิเคชันคือ Hypertext Transfer Protocol

(HTTP) ซึ่งเป็นการสื่อสารผ่านเว็บให้ปลอดภัย พัฒนาในช่วงต้นของยุคการค้าอิเล็กทรอนิคส์กำลังได้รับความนิยมในโลกอินเตอร์เน็ต

SL ทำให้เกิดการสื่อสารอย่างปลอดภัยระหว่างไคลเอ็นต์และเซิร์ฟเวอร์ โดยการอนุญาตให้มีกระบวนการพิสูจน์ตัวตนรวมกับการใช้งานลายเซ็นดิจิตอลสำหรับการรักษาความถูกต้องของข้อมูลและการเข้ารหัสข้อมูลเพื่อป้องกันความเป็นส่วนตัวระหว่างการสื่อสารข้อมูล

โพรโตคอล SSL อนุญาตให้สามารถเลือกวิธีการในการเข้ารหัส วิธีสร้างไดเจสต์ และลายเซ็นดิจิตอล ได้อย่างอิสระก่อนการสื่อสารจะเริ่มต้นขึ้น ตามความต้องการของทั้งเว็บเซิร์ฟเวอร์และบราวเซอร์ ทั้งนี้เพื่อเพิ่มความยืดหยุ่นในการใช้งาน เปิดโอกาสให้ทดลองใช้วิธีการในการเข้ารหัสวิธีใหม่ รวมถึงลดปัญหาการส่งออกวิธีการเข้ารหัสไปประเทศที่ไม่อนุญาต

Netscape เริ่มพัฒนา SSL เวอร์ชันแรกคือเวอร์ชัน 2.0 และเวอร์ชันถัดมาเป็น 3.0 ซึ่งสนับสนุนความสามารถด้านความปลอดภัยมากขึ้น และเป็นเวอร์ชันสุดท้ายก่อนที่จะเป็นมาตรฐานกลางของโพรโตคอลบนอินเตอร์เน็ต โดยเปลี่ยนชื่อเป็น Transport Layer Security หรือ TLS ซึ่งดูแลมาตรฐานโดย Internet Engineering Task Force (IETF)

ไดเจสต์ (Digest) คือข้อความที่เกิดจากการเข้ารหัสข้อมูลด้วยฟังก์ชันแฮชเช่น MD5 หรือ SHA-1

ห่วงโซ่ Certificate (Certificate Chain) คือการเพิ่มข้อมูล Certificate ที่เกี่ยวเนื่องกันเมื่อใช้ในขั้นตอนแลกเปลี่ยนข้อมูล ซึ่งจะช่วยลดเวลาในการค้นหา Certificate จากผู้ให้บริการ Certificate Authority (CA) ที่เกี่ยวเนื่องกันมากกว่า 1 ขึ้นไป กระบวนการในการเริ่มต้นการสื่อสารผ่านชั้น SSL แบ่งเป็น 4 ขั้นตอนคือ

(1) ประกาศชุดวิธีการเข้ารหัส ไดเจสต์ และลายเซ็นดิจิตอลที่สนับสนุนของทั้งไคลเอ็นต์และเซิร์ฟเวอร์ ไคลเอ็นต์และเซิร์ฟเวอร์ส่งข้อความเริ่มต้นการสื่อสาร (Hello message) ซึ่งประกอบไปด้วยเวอร์ชันของโพรโตคอลที่ใช้ วิธีการเข้ารหัสที่เว็บเซิร์ฟเวอร์และไคลเอ็นต์สนับสนุน หมายเลขระบุการสื่อสาร (Session identifier) รวมถึงวิธีการบีบอัดข้อมูลในการสื่อสารที่สนับสนุนหมายเลขระบุการสื่อสารที่เกิดขึ้น ใช้สำหรับตรวจสอบการเชื่อมต่อระหว่างไคลเอ็นต์และเซิร์ฟเวอร์ ถ้ามีการเชื่อมต่อก่อนหน้านี้เกิดขึ้น แสดงว่าได้มีการตกลงวิธีการสื่อสารแล้ว สามารถเริ่มต้นส่งข้อมูลได้ทันที เป็นการลดเวลาติดต่อสื่อสารลง

(2) การพิสูจน์ตัวตนของเซิร์ฟเวอร์ต่อไคลเอ็นต์ ถัดมาเว็บเซิร์ฟเวอร์ทำการส่ง Certificate หรือใบยืนยันความมีตัวตนของเซิร์ฟเวอร์ ไคลเอ็นต์จะทำการ

ตรวจสอบ Certificate กับผู้ให้บริการ Certificate Authority ที่ได้ตั้งค่าไว้ เพื่อยืนยันความถูกต้องของ Certificate ของเซิร์ฟเวอร์

(3) การพิสูจน์ตัวตนของไคลเอ็นต์ต่อเซิร์ฟเวอร์ ถ้าจำเป็นเซิร์ฟเวอร์สามารถร้องขอ Certificate จากไคลเอ็นต์เพื่อตรวจสอบความถูกต้องของ Client ด้วยก็ได้ ใช้ในกรณีที่มีการจำกัดการใช้งานเฉพาะไคลเอ็นต์ที่ต้องการเท่านั้น ซึ่ง SSL สนับสนุนการตรวจสอบได้จากทั้งเซิร์ฟเวอร์และไคลเอ็นต์ ขึ้นอยู่กับการเลือกใช้งานในขณะติดต่อสื่อสารที่เกิดขึ้นนั้น

(4) ไคลเอ็นต์และเซิร์ฟเวอร์ตกลงชุดวิธีการเข้ารหัส การสร้างไดเจสต์ และการใช้ลายเซ็นดิจิตอล ขั้นตอนการตรวจสอบ Certificate ที่เซิร์ฟเวอร์ร้องขอจากไคลเอ็นต์จะมีหรือไม่มีก็ได้ ขึ้นอยู่กับการตั้งค่าบนเซิร์ฟเวอร์ หลังจากขั้นตอนการตรวจสอบเสร็จสิ้นเซิร์ฟเวอร์และไคลเอ็นต์จะตกลงการใช้งานวิธีการเข้ารหัสระหว่างกันโดยใช้ค่าที่ได้จากการประกาศในขั้นตอนแรก

วิธีการแลกเปลี่ยนกุญแจในการเข้ารหัส (Key Exchange Method) คือการกำหนดกลไกการแลกเปลี่ยนกุญแจที่ใช้ในการเข้ารหัสระหว่างการสื่อสาร โดยทั้งไคลเอ็นต์และเซิร์ฟเวอร์จะใช้กุญแจนี้ในการเข้ารหัสและถอดรหัสข้อมูล ใน SSL เวอร์ชัน 2.0 จะสนับสนุนวิธีการแลกเปลี่ยนกุญแจแบบ RSA ส่วน SSL เวอร์ชัน 3.0 ขึ้นไปจะสนับสนุนวิธีการอื่นๆ เพิ่มเติมเช่นการใช้ RSA ร่วมกับการใช้ Certificate หรือ Diffie-Hellman เป็นต้น

วิธีการเข้ารหัสในปัจจุบันแบ่งเป็นสองวิธีคือ การใช้กุญแจเดียวกันในการเข้ารหัสและถอดรหัส อาจเรียกกุญแจนี้ว่า Session key หรือ Secret key ส่วนอีกวิธีการคือ การใช้กุญแจคนละตัวในการเข้ารหัสและถอดรหัส ประกอบไปด้วยกุญแจสาธารณะและกุญแจส่วนตัวซึ่งเป็นคู่กันเสมอ เข้ารหัสด้วยกุญแจใด จะต้องถอดรหัสด้วยกุญแจที่คู่กันและตรงกันข้ามเท่านั้น มักใช้วิธีการเข้ารหัสด้วยกุญแจคนละตัวมาใช้ในการเข้ารหัส Session key และส่งไปให้ฝั่งตรงข้ามก่อนการสื่อสารจะเกิดขึ้นรวมเรียกว่าวิธีการแลกเปลี่ยนกุญแจในการเข้ารหัส

SSL ใช้วิธีการเข้ารหัสด้วยกุญแจสมมาตร หรือกุญแจเดียวในการเข้ารหัสและถอดรหัสตามที่กล่าวข้างต้น วิธีการเข้ารหัสคือ การเข้ารหัสด้วย DES และ 3DES (Data Encryption Standard), วิธีการเข้ารหัสด้วย IDEA ส่วน RC2 และ RC4 เป็นวิธีการเข้ารหัสของ RSA รวมถึงวิธีการเข้ารหัสแบบ Fortezza สำหรับความยาวของการเข้ารหัสที่ใช้คือ 40 บิต 96 บิต 128 บิต

การสร้าง Message Authentication Code (MAC) เพื่อใช้สำหรับการยืนยันความถูกต้องของข้อมูลระหว่างการสื่อสารและป้องกันการปลอมข้อมูล ส่วนฟังก์ชันสร้างไดเจสต์ที่ SSL

สนับสนุนและเลือกใช้ได้ในปัจจุบันคือ MD5 ขนาด 128 บิต และ SHA-1 (Secure Hash Algorithm) ขนาด 160 บิต ซึ่งจะได้วิธีการที่ทั้งสองฝ่ายสนับสนุนและเหมาะสมซึ่งเป็นขั้นตอนสุดท้ายก่อนการสื่อสารที่มีการเข้ารหัสจะเริ่มต้นขึ้น

2) Secure Shell (SSH) SSH เวอร์ชัน 1 พัฒนาขึ้นในปี 1995 โดย Tatu Ylonen ขณะที่เป็นนักวิจัยของมหาวิทยาลัยแห่งหนึ่งในฟินแลนด์ เพื่อแก้ปัญหาการดักจับรหัสผ่านที่เกิดขึ้นในระบบเครือข่าย และเผยแพร่ซอร์สโค้ดและเปิดให้ดาวโหลดไปใช้งานได้ฟรี ปลายปีเดียวกันได้จัดตั้งบริษัท SSH Communications Security, Ltd. (SCS) และเปิดตัว SSH เวอร์ชัน 2 ในต้นปี 1996 ในรูปของการค้า แต่ไม่สามารถทำงานร่วมกับ SSH เวอร์ชัน 1 ส่งผลให้มีการใช้งาน SSH เวอร์ชัน 1 แพร่หลายมากกว่าในเวลานั้น เนื่องจากเหตุผลเรื่องลิขสิทธิ์ ทีมพัฒนาจากระบบปฏิบัติการ FreeBSD ได้ร่วมกันพัฒนา OpenSSH ซึ่งสนับสนุนการทำงานตามมาตรฐานของทั้ง SSH เวอร์ชัน 1 และ 2 ของ SCS และได้เปิดตัวครั้งแรกในเดือนธันวาคมปี 1999 ใน OpenSSH เวอร์ชัน 1.2.2 ซึ่งสนับสนุนเฉพาะ SSH เวอร์ชัน 1 และมาพร้อมกับระบบปฏิบัติการ OpenBSD เวอร์ชัน 2.6 และในเดือนมิถุนายนปี 2000 ได้เปิดตัว OpenSSH เวอร์ชัน 2.0 ซึ่งสนับสนุน SSH ทั้งสองเวอร์ชันและมาพร้อมกับ OpenBSD เวอร์ชัน 2.7

จากการนับสถิติการใช้งานโพรโตคอล SSH ในอินเตอร์เน็ตด้วยโปรแกรม ScanSSH ที่พัฒนาโดย Niels Provos ในเดือนเมษายนปี 2002 จากจำนวน 2.4 ล้านเครื่องในอินเตอร์เน็ต พบว่า·มากกว่า 59% ใช้ OpenSSH เวอร์ชัน 1.99 และ 17.9% ใช้ SSH เวอร์ชัน 1.5 (เป็น SSH ของบริษัท SCS)

การใช้งาน SSH เป็นการติดต่อสื่อสารโดยใช้การพิสูจน์ตัวตนร่วมกับลายเซ็นดิจิตอล และมีการเข้ารหัสการสื่อสาร ตรงกันข้ามกับการสื่อสารแบบเก่าเช่น Telnet หรือ R Utilities เป็นต้น

การเข้ารหัสแบบกุญแจสาธารณะจะใช้ร่วมกับการใช้ฟังก์ชันแฮชในการสร้างไดเจสต์สำหรับการแลกเปลี่ยน Secret key ก่อนการเข้ารหัสจะเริ่มต้นขึ้น การเริ่มต้นการติดต่อสื่อสารตามโพรโตคอล SSH เป็นไปตามขั้นตอนสรุปได้ ดังนี้

(1) ไคลเอ็นต์เริ่มถามเวอร์ชันของโพรโตคอล SSH บนเซิร์ฟเวอร์ ถ้าใช้ SSH เวอร์ชันเดียวกันถือว่าสื่อสารกันได้

(2) ไคลเอ็นต์จะประกาศวิธีการเข้ารหัส วิธีการสร้างไดเจสต์ และการแลกเปลี่ยนกุญแจในการเข้ารหัสที่สนับสนุน

(3) เซิร์ฟเวอร์จะทำหน้าที่เลือกชุดวิธีการทั้งหมดที่ไคลเอ็นต์สนับสนุน

(4) ไคลเอ็นต์และเซิร์ฟเวอร์เริ่มต้นแลกเปลี่ยนกุญแจในการเข้ารหัส ตามรูปแบบวิธีการแลกเปลี่ยนกุญแจด้วยวิธีการกุญแจสาธารณะเช่นการใช้วิธี Diffie-Hellman เป็นต้น

(5) เมื่อแลกเปลี่ยนกุญแจสำหรับการเข้ารหัสด้วยวิธีการแลกเปลี่ยนกุญแจแล้ว ทั้งไคลเอ็นต์และเซิร์ฟเวอร์จะสามารถเริ่มต้นติดต่อสื่อสารด้วยการเข้ารหัสด้วยกุญแจที่ได้จากการแลกเปลี่ยนกุญแจและสามารถใช้การบีบอัดข้อมูลร่วมได้

โพรโตคอล SSH ยังสนับสนุนการพิสูจน์ตัวตนของทั้งเซิร์ฟเวอร์และไคลเอ็นต์ในขั้นตอนการแลกเปลี่ยนกุญแจด้วย กล่าวคือในขั้นตอนการแลกเปลี่ยนกุญแจนั้น ทั้งไคลเอ็นต์และเซิร์ฟเวอร์จะสร้างคู่รหัสกุญแจ ประกอบไปด้วยกุญแจสาธารณะและกุญแจส่วนตัว ซึ่งกุญแจส่วนตัวของทั้งไคลเอ็นต์และเซิร์ฟเวอร์นี้เองที่ใช้ในการพิสูจน์ตัวตนได้ตามหลักการพิสูจน์ตัวตนด้วยวิธีการใช้กุญแจสาธารณะ ถ้าตรวจสอบได้ว่ามีการส่งข้อมูลด้วยกุญแจที่เปลี่ยนไปจากเดิมอาจจะแสดงได้ว่าการสื่อสารนี้ไม่ปลอดภัยแล้วปัจจุบันมีซอฟต์แวร์ที่สนับสนุนการทำงานตามโพรโตคอล SSH ให้เลือกใช้มากอาทิเช่น OpenSSH จากผู้พัฒนา OpenBSD ในระบบปฏิบัติการตระกูลยูนิกซ์ ส่วนในตระกูลวินโดวส์เช่นโปรแกรม Putty ของ Simon Tatham หรือ Window SSH Secure Shell จาก www.ssh.com เป็นต้น

การสื่อสารด้วยโพรโตคอล SSH สนับสนุนการเข้ารหัสการสื่อสาร และการพิสูจน์ตัวตนที่ดีในองค์กรคือการเปลี่ยนมาใช้การสื่อสารด้วย SSH แทนการสื่อสารแบบเดิมเช่นการใช้ R Utilities เช่น rlogin หรือ rcp บนตระกูลยูนิกซ์และการใช้งาน telnet และที่สำคัญคือการใช้งาน ftp ควรจะเปลี่ยนมาใช้งานโปรแกรม scp (Secure Copy) หรือ WinSCP แทนในการแลกเปลี่ยนไฟล์เป็นต้น

3) Internet Security (IPSEC) IPsec เป็นส่วนเพิ่มขยายของ Internet Protocol (IP) ในชุดโพรโตคอล TCP/IP พัฒนาเพื่อเป็นส่วนหนึ่งของมาตรฐานของ IPv6 ซึ่งเป็นโพรโตคอลที่พัฒนาเพื่อใช้แทน IPv4 ที่ใช้ในปัจจุบันและกำหนดหมายเลข RFC เป็น RFC2401

IPsec ใช้โพรโตคอล 2 ชุดคือ Authentication Header (AH) และ Encapsulated Security Payload (ESP) เพื่อรองรับการพิสูจน์ตัวตน (Authentication) การรักษาความถูกต้อง

ของข้อมูล (Integrity) และการรักษาความลับ (Confidentiality) ในระดับชั้นของ IP โดยการใช้งานสามารถเลือกใช้ได้สองรูปแบบ

(1) Tunnel mode เป็นการนำส่วนแพ็กเก็ตเดิมทั้งหมดมาครอบด้วย IP โพรโตคอลชุดใหม่ที่เป็นไปตามชุดโพรโตคอล IPsec สังเกตได้จากมีการเพิ่มเฮดเดอร์ IP และ AH เข้าไปข้างหน้าแพ็กเก็ตชุดเดิม

(2) Transport mode นำเฉพาะข้อมูลของโพรโตคอล IP ซึ่งจะประกอบด้วยข้อมูลของชั้น Transport (TCP หรือ UDP) และชั้นแอพพลิเคชัน โดยเพิ่มโพรโตคอล AH และเพิ่มข้อมูลใน IP เดิมให้เหมาะสมตามมาตรฐาน IPsec

การรักษาความถูกต้องของข้อมูลของ IP ดาตาแกรม (IP Datagram) ในชุดโพรโตคอล IPsec ใช้ Hash Message Authentication Codes หรือ HMAC ด้วยฟังก์ชันแฮชเช่น MD5 หรือ SHA-1 ทุกครั้งที่มีการส่งแพ็กเก็ตจะมีการสร้าง HMAC และใช้การเข้ารหัสไปด้วยทุกครั้ง เพื่อให้ปลายทางสามารถตรวจสอบได้ตามหลักการลายเซ็นดิจิตอลว่าต้นทางเป็นผู้ส่งแพ็กเก็ตนั้นมาจริง ส่วนการรักษาความลับของข้อมูลนั้น จะใช้การเข้ารหัส IP ดาตาแกรมด้วยวิธีการเข้ารหัสด้วยกุญแจสมมาตร ด้วยวิธีการมาตรฐานที่เป็นรู้จักกันดีเช่น 3DES AES หรือ Blowfish เป็นต้น

ปัญหาหนึ่งของ IPsec คือการส่งกุญแจที่ใช้ในการเข้ารหัสไปกับแพ็กเก็ต ซึ่งจัดว่าไม่ปลอดภัย นอกจากนี้การแลกเปลี่ยนกุญแจนำไปสู่ปัญหาของการดูแลระบบที่ใช้ IPsec เพราะทั้งระบบต้องสนับสนุนการใช้งานโพรโตคอล IPsec เดียวกัน จะทำอย่างไรให้สามารถส่งกุญแจในการเข้ารหัสไปกับแพ็กเก็ตถ้าไม่มีการเข้ารหัสแพ็กเก็ตแต่อย่างใด เพื่อแก้ปัญหาจึงได้พัฒนาโพรโตคอลในการแลกเปลี่ยนกุญแจหรือ Internet Key Exchange Protocol (IKE)

IKE จะทำการพิสูจน์ตัวตนของปลายทางก่อนการสื่อสาร ในขั้นตอนถัดมาจึงสามารถแลกเปลี่ยนและตกลง Security Association และกุญแจในการเข้ารหัสได้ด้วยวิธีการแลกเปลี่ยนกุญแจตามวิธีการแลกเปลี่ยนกุญแจด้วยการใช้กุญแจสาธารณะเช่น Diffie-Hellmann เป็นต้น ซึ่งชุดโพรโตคอล IKE จะตรวจสอบกุญแจที่ใช้ในการเข้ารหัสระหว่างการติดต่อสื่อสารเป็นระยะตลอดการสื่อสารข้อมูลที่เกิดขึ้นแต่ละครั้ง ชุดโพรโตคอล IPsec ประกอบจากโพรโตคอลหลักสองโพรโตคอลคือ Authentication Header (AH) และ Encapsulated Security Payload (ESP)

AH หรือ Authentication Header ทำหน้าที่รักษาความถูกต้องของ IP ดาต้าแกรม โดยการคำนวณ HMAC กับทุก IP ดาต้าแกรม

ESP หรือ Encapsulated Security Payload ใช้สำหรับรักษาความถูกต้องของแพ็กเก็ตโดยใช้ HMAC และการเข้ารหัสร่วมด้วย

4) Kerberos การพิสูจน์ตัวตนแบบ Kerberos พัฒนาขึ้นโดย Massachusetts Institute of Technology หรือ MIT ระบบ Kerberos ประกอบขึ้นจากสองส่วนหลักคือ ส่วนที่เรียกว่า Ticket ใช้สำหรับการพิสูจน์ตัวตนของผู้ใช้ในระบบ และการเข้ารหัสข้อมูลกับ ส่วนที่เรียกว่า Authenticator ใช้ในการตรวจสอบ Ticket ว่าเป็นผู้ใช้คนเดียวกันที่ใช้ Ticket เป็นใบเบิกทางเข้าสู่ระบบและเป็นผู้ใช้ที่ระบบสร้างให้อย่างถูกต้อง กระบวนการใช้งานระบบ Kerberos มีลำดับดังนี้

(1) ผู้ใช้จะทำการพิสูจน์ตัวตนครั้งแรกกับ Authentication service ของ Kerberos ซึ่งจะได้กุญแจสมมาตรซึ่งจะใช้ในการเข้ารหัสข้อมูลในการติดต่อสื่อสาร

(2) ก่อนผู้ใช้จะเข้าไปใช้บริการใด ๆ ในระบบได้ต้องมี Ticket ก่อน ด้วยการติดต่อไปที่ Ticket Granting Service เพื่อให้ออก Ticket ที่เหมาะสมกับการเข้าไปใช้บริการบนเซิร์ฟเวอร์ในระบบได้

(3) ผู้ใช้นำ Ticket สำหรับไปใช้กับการร้องขอการติดต่อการบริการจากเซิร์ฟเวอร์ในระบบ

ปัญหาสำคัญของการใช้ระบบ Kerberos คือการขยายระบบเนื่องจากเซิร์ฟเวอร์ Kerberos ต้องเก็บกุญแจของผู้ใช้ทุกคนที่เข้ามาในระบบ ถ้าระบบใหญ่มากขึ้น มีการกระจายตัวมากกว่าหนึ่งจุด ย่อมส่งผลเสียต่อการใช้งานระบบโดยรวม แต่การนำระบบ Kerberos มาใช้จะเพิ่มความสะดวกในการพิสูจน์ตัวตนได้มากขึ้น มักเรียกการใช้งาน Kerberos ว่าเป็นระบบ Single Sign-On แบบหนึ่ง คือการเข้าถึงการใช้บริการของระบบทั้งหมดได้ด้วยการพิสูจน์ตัวตนยงครั้งเดียว

2.8.2 การกำหนดสิทธิ์ (Authorization) คือข้อจำกัดของบุคคลที่เข้ามาในระบบ ว่าบุคคลคนนั้นสามารถทำอะไรกับระบบได้บ้าง

2.8.3 การบันทึกการใช้งาน (Accountability) คือการบันทึกรายละเอียดของการใช้ระบบและรวมถึงข้อมูลต่างๆที่ผู้ใช้กระทำลงไปในระบบ เพื่อผู้ตรวจสอบจะได้ตรวจสอบได้ว่า ผู้ใช้ที่เข้ามาใช้บริการได้เปลี่ยนแปลงหรือแก้ไขข้อมูลในส่วนใดบ้าง (สิริพร จิตต์เจริญธรรม, เสาวภา ปานจันทร์ และเลอศักดิ์ ลิ้มวิวัฒน์กุล, 2547)

2.9 ล็อกไฟล์

ล็อกไฟล์(Log Files) หมายถึงข้อมูลจราจรทางคอมพิวเตอร์ ที่เก็บข้อมูลการสื่อสารที่เกิดขึ้นกับระบบคอมพิวเตอร์เพื่อนำข้อมูลดังกล่าวไว้เป็นหลักฐานในการหาข้อมูลเกี่ยวกับคอมพิวเตอร์ ล็อกไฟล์เป็นข้อมูลที่ความสำคัญมากที่สุด เป็นตัวที่บ่งชี้ถึงเหตุการณ์ที่เกิดขึ้นใน

ช่วงเวลาหนึ่ง ทำให้ผู้ดูแลระบบสามารถค้นหาข้อบกพร่องหรือตรวจจับเหตุการณ์ที่ผิดปกติได้ และยังเป็นหลักฐานที่สำคัญเมื่อมีเหตุการณ์ละเมิดความปลอดภัยคอมพิวเตอร์เกิดขึ้น สำหรับผู้ดูแลระบบที่เป็นยูนิกซ์หรือลินุกซ์โดยทั่วไปแล้วก็จะมีความคุ้นเคยกับ Syslog เป็นอย่างดี เพราะผู้ดูแลระบบต้องจับตาดูความเป็นไปของระบบเป็นประจำ syslogd เป็นกลไกที่ใช้ในการเก็บข้อมูลล็อกของ kernel และ application บนระบบยูนิกซ์และลินุกซ์ เป็น daemon ที่ถูกติดตั้งมาให้พร้อมกับระบบปฏิบัติการในเกือบทุกระบบ โดยผู้ดูแลระบบสามารถปรับแต่งไฟล์ configuration เพื่อควบคุมการทำงานของ syslogd ได้ เช่น ให้ syslogd เก็บข้อมูลไปไว้ที่ไฟล์ใด หรือให้ส่งข้อมูลล็อกนี้ไปเก็บไว้ยังเครื่องอื่นในเครือข่าย (ภูวดล ด่านระหาญ, 2544)

2.10 โอเพ่นซอร์ซ

โอเพ่นซอร์ซ(Open Source) เป็นซอฟต์แวร์ใด ๆ ก็ตามที่ผู้เขียนเปิดเผยซอร์สโค้ดให้กับสาธารณชนได้เห็น เพื่อที่ให้โปรแกรมเมอร์อื่นๆ สามารถเขียนเพิ่มต่อหรือแก้ไขตัวโปรแกรมเดิมที่มีอยู่แล้วให้สามารถใช้งานได้ดีหรือเหมาะสมกับผู้ใช้มากยิ่งขึ้นได้ตามความพอใจ โดยโปรแกรมเมอร์ที่อยู่กันคนละมุมโลก อาจจะได้ร่วมกันวิเคราะห์ปัญหาและ พัฒนาให้เกิดเป็นซอฟต์แวร์ที่มีประสิทธิภาพมากยิ่งขึ้นได้ หรือช่วยกันต่อเติมจากตัวโปรแกรมเดิมที่มีอยู่ให้มีฟังก์ชั่นการทำงานที่หลากหลายมากขึ้น เหมาะสมกับผู้ใช้ มากขึ้น และตรงตามความต้องการมากขึ้น อีกทั้งยังมีประโยชน์ในการช่วยส่งเสริมให้เกิดสังคมของ ผู้ พัฒนาซอฟต์แวร์ให้กว้างขวางยิ่งขึ้น ได้แลกเปลี่ยนความรู้ ความคิดเห็นซึ่งกันและกัน ซึ่งจะทำให้เกิด แนวคิดใหม่ๆ ตามมา และสร้างสรรค์สิ่งใหม่ๆ ให้เกิดบนโลกได้มากมายมหาศาล

โอเพ่นซอร์ซเริ่มเข้ามามีบทบาทมากขึ้นในโลกเรา เนื่องจากปัจจุบันไมโครซอฟต์ได้ครองตลาดซอฟต์แวร์ส่วนใหญ่และมีผู้ใช้มากที่สุดในโลก แต่เราจะต้องเสียค่าลิขสิทธิ์ให้กับบริษัทไมโครซอฟต์ด้วย ซึ่งถือว่าเป็นค่าใช้จ่ายที่ค่อนข้างสูงและต้องเสียอย่างต่อเนื่องอีกด้วยกับการ Upgrade ซอฟแวร์ให้ทันสมัยอยู่เสมอ ดังนั้นตลาด Open Source จึงเกิดขึ้นมาเพื่อหลีกเลี่ยงการเสียค่าลิขสิทธิ์ เหล่านี้ ซึ่งหากเราหันมาใช้ ซอฟต์แวร์ที่เป็น Open Source กันมากขึ้นเท่าใดจะยิ่งเป็นผลดีต่อเรามาก ขึ้นเท่านั้น เพราะผู้พัฒนาจะมีกลุ่มใหญ่ขึ้นและสามารถพัฒนาซอฟต์แวร์ให้มีประสิทธิภาพและเป็น ที่พอใจแก่ผู้ใช้มากขึ้นตามไปด้วย ซึ่งถ้าซอฟต์แวร์ Open Source มีการใช้งานได้ง่ายและสะดวกเหมือน ที่เราใช้กันอยู่ปัจจุบันของซอฟต์ แวร์ที่เสียค่าลิขสิทธิ์ ผู้คนก็จะหันมาเห็นความสำคัญและเลือกใช้ ซอฟต์แวร์ประเภทนี้กันมากขึ้น และการใช้ Open Source มาทดแทนซอฟต์แวร์ที่ต้องเสียค่าลิขสิทธิ์นี้ จะช่วยให้ประหยัดงบประมาณใน การจัดซื้อซอฟต์แวร์ได้

มากด้วย และยังลดปัญหาการละเมิดลิขสิทธิ์ ซอฟต์แวร์ได้อีกประการหนึ่ง จะทำให้ลดปัญหาได้อีกมากมายหลายเรื่องตามมา

ปัจจุบันมีหลายประเทศที่พยายามผลักดันให้ระบบปฏิบัติการสากลของประเทศเป็นระบบปฏิบัติการประเภท Open Source เพื่อให้ผู้ใช้ในประเทศได้ทำความเข้าใจและหัดใช้ระบบปฏิบัติการ ประเภทนี้ให้เคยชิน เพราะจะช่วยลดค่าใช้จ่ายเรื่องลิขสิทธิ์ของประเทศได้เป็นจำนวนเงินมหาศาล ซึ่งต่อไปในอนาคตหากมีผู้ใช้กันมากขึ้นเท่าใดในโลก จะช่วยลดการผูกขาดการขายของระบบ ปฏิบัติการเดิมที่ใช้กันอยู่ปัจจุบัน และค่าลิขสิทธิ์ของซอฟต์แวร์อาจจะถูกลงหรืออาจจะไม่มีการเก็บค่า ลิขสิทธิ์อีกเลยก็เป็นได้ จะทำให้เกิดการแข่งขันกันอย่างแท้จริงในเรื่องการพัฒนาซอฟต์แวร์ ก็จะเป็นผล ดีกับผู้ใช้อีก เพราะเราจะมีซอฟต์แวร์ที่ใช้ง่ายและสนองความต้องการได้มากที่สด และจะเกิดการพัฒนา ซอฟต์แวร์จากกลุ่ม นักพัฒนาทั้งอาชีพและสมัครเล่นอีกมากมายตามมา ทำให้เราสามารถเลือก ซอฟต์แวร์ที่เหมาะกับการใช้งานของเราได้มากยิ่งขึ้นด้วย และหากมีการเปิดเผยซอร์สโค้ดให้บุคคล ทั่วไปได้รู้ได้เห็น จะยิ่งมีประโยชน์กับผู้ที่ต้องการเรียนรู้ด้วยตัวเองได้ศึกษาตัวโปรแกรมและลองหัด พัฒนา หรือปรับเปลี่ยน แก้ไขตัวโปรแกรมเองได้ เป็นการเพิ่มขีดความสามารถในส่วนบุคคลอีก ประการหนึ่ง นอกจากระบบปฏิบัติการแล้วยังมีซอฟต์แวร์อื่น ๆ อีกมากมายที่เป็น Open Source ทั้งเป็นตัวโปรแกรมและฐานข้อมูล ที่ให้เราสามารถเลือกใช้ได้ตามความต้องการ โดยการ Download ตามเว็บไซต์ หรือซื้อแผ่นโปรแกรมมาลงเองก็ได้ ระบบปฏิบัติการประเภท Open Sorce ที่นิยมกันมากในปัจจุบัน คือ ระบบปฏิบัติการลีนุกซ์ ซึ่งมีวัตถุประสงค์เพื่อพัฒนามาใช้ทดแทนวินโดวส์ของไมโครซอฟต์นั่นเอง แต่ปัจจุบัน Interface ในการใช้งานอาจยังไม่ง่าย หรือไม่ค่อยคุ้นมือเหมือนวินโดวส์ แต่หากเราได้ลองใช้งานบ่อยๆ ก็จะเกิดความเคยชิน และง่ายไปเอง และหากมีคนหันมาใช้กันมากเท่าใด ก็จะยิ่งเร่งเวลาให้ลีนุกซ์มี เวอร์ชั่นที่ใช้งานง่ายกับเราตามออกมาเร็วขึ้นเท่านั้น และตัวลีนุกซ์เองก็ยังมีเวอร์ชั่นอีกมากมายหลาย เวอร์ชั่นของหลายค่าย ไม่ว่าจะเป็นลีนุกซ์ทะเล แมนเดรก Red hat เป็นต้น ซึ่งแต่ละค่ายก็มีความสามารถในตัวโปรแกรมที่แตกต่างกันไป มีลักษณะเด่นเฉพาะตัวของแต่ละค่ายที่เหมาะกับผู้ใช้งาน หลายประเภทอีกเช่นกัน ส่วนโปรแกรมอื่น ๆ ที่เป็น Open Source ก็อย่างเช่น PHP, My SQL, Star Office หรือ ออฟฟิศปลาดาว เป็นต้น ซึ่งเราจะสามารถหาซื้อแผ่นโปรแกรมมาใช้ได้ตามผู้จัดจำหน่ายต่าง ๆ ที่เริ่มจะมีมากขึ้นในประเทศของเรา ราคาแผ่นโปรแกรมก็ไม่แพงมากนัก เป็นราคาปกติทั่วไปตาม ท้องตลาด และไม่เสียค่าลิขสิทธิ์แต่อย่างใด (http://www.nectec.or.th/rd/rd-opensource-th.html, สืบค้นวันที่ 5 สิงหาคม 2553)

2.11 งานวิจัยที่เกี่ยวข้อง

ชัยวัฒน์ นิลวรรณ (2549) พัฒนาระบบจัดการสควิดพร็อกซี่โดยผ่านเว็บอินเตอร์เฟส ซึ่งใช้วิธีบริหารจัดการ การทำงานของผู้ดูแลระบบผ่านทางหน้าเว็บเพจ ซึ่งพัฒนาด้วยภาษาพีเอชพี การทำงานของสควิดพร็อกซี่ติดตั้งอยู่บนระบบปฏิบัติการลินุกซ์เซิร์ฟเวอร์ การพัฒนาระบบจัดการสควิดพร็อกซี่โพลีซีโดยผ่านเว็บอินเตอร์เฟส แบ่งออกเป็น 2 ส่วนหลักคือ ส่วนของการจัดการกับแฟ้มข้อมูลหลักของสควิดส์พร็อกซี่ และส่วนของการจัดการกับกลุ่มของข้อมูลที่เป็นเงื่อนไข โดยกลุ่มของข้อมูลแต่ละกลุ่มจะถูกมองเหมือนกับเป็นอ็อพเจ็ค แต่ละอ็อพเจ็คจะแยกออกจากกัน อย่างอิสระ อ็อพเจ็คแต่ละอ็อพเจ็คจะนำมาประกอบกันตามเงื่อนไขที่ต้องการ เพื่อที่จะให้สควิด พร็อกซี่นำไปเป็นส่วนของการฟิลเตอร์ข้อมูลต่างๆ ที่วิ่งผ่านสควิดพร็อกซี่ ผลการทดลองเมื่อนำระบบงานที่ได้พัฒนา ไปทำการทดสอบเพื่อหาระดับความพึงพอใจของระบบจากผู้เชี่ยวชาญด้านการดูแลระบบ และผู้ดูแลระบบ สามารถสรุปผลการประเมินหาประสิทธิภาพได้ว่าเป็นระบบที่พัฒนาโดยมีประสิทธิภาพอยู่ในระดับดี

อุทัย วังชัยศรี และคณะ (2551) ได้นำเสนอระบบเก็บข้อมูลการใช้เครือข่ายและข้อมูลผู้ใช้เพื่อการพิสูจน์ตัวตนสำหรับเป็นหลักฐานทางกฎหมายที่รองรับ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 ในส่วนอินเทอร์เน็ตคาเฟ่ โดยผู้วิจัยได้นำเสนอสถาปัตยกรรมเครือข่ายอย่างง่ายสำหรับผู้ให้บริการอินเทอร์เน็ตคาเฟ่เพื่อรองรับการจัดเก็บข้อมูลกิจกรรมการใช้เครือข่ายและการตรวจสอบสิทธิ์การใช้งาน เพื่อนำข้อมูลที่จัดเก็บมาใช้สืบค้นหาผู้กระทำผิด ซึ่งในงานวิจัยนี้พัฒนาระบบงานโดยใช้ระบบปฏิบัติการ Linux Fedora เวอร์ชั่น 5 มีระบบฐานข้อมูลสำหรับเก็บข้อมูลผู้ใช้งานอินเทอร์เน็ตคาเฟ่ ซึ่งผู้วิจัยได้พัฒนาระบบขึ้นโดยใช้ภาษา PHP โปรแกรม Radius และ Chillispot เพื่อใช้ในการพิสูจน์ตัวตนในการเข้าสู่ระบบ ผลการทดสอบหาผู้กระทำความผิด(โดยการใช้ข้อมูลสมมุติ)ได้ผลลัพธ์เป็นที่น่าพอใจ

พันธ์รัตน์ อักษรศรีกุล และ ศิฟาณี นุชิตประสิทธิชัย (2552) ได้ออกแบบระบบคลังข้อมูลจาก Log File ของการใช้งานอินเทอร์เน็ต ซึ่งงานวิจัยนี้นำเสนอการออกแบบระบบสารสนเทศ และการพัฒนาคลังข้อมูล จากข้อมูล Log File ของการใช้งานอินเทอร์เน็ตที่อยู่ในลักษณะ Text-Based File ให้ อยู่ในลักษณะฐานข้อมูลเชิงสัมพันธ์และใช้เทคนิค Online – Analytic Processing (OLAP) ในการวิเคราะห์ข้อมูลในมุมมองและองค์ประกอบที่เกี่ยวข้อง เช่น ห้วงเวลา และหน่วยงาน เป็นต้น นำเสนอผ่านเว็บบราวเซอร์ ภายในเครือข่ายอินทราเน็ต ด้วยภาษาPHP, MySQL และทำการประเมินความพึงพอใจด้วยแบบประเมินตามวิธีของไลเคอร์ท โดยผลการประเมินด้านความสามารถทำงานตรงความต้องการมีค่าเฉลี่ย 4.07 ด้านหน้าที่ของระบบมี

ค่าเฉลี่ย 4.25 ด้านการใช้งานระบบมีค่าเฉลี่ย 4.11 ด้านประสิทธิภาพของระบบมีค่าเฉลี่ย 4.13 และด้านความปลอดภัยของระบบมีค่าเฉลี่ย 4.17 และสรุปได้ว่า พบว่าผู้ใช้งานระบบมีความพึงพอใจต่อระบบอยู่ในระดับดี ระบบสามารถนำไปใช้งานได้จริง

โดม เจริญยศ (2551) ใช้ Radius ในการพิสูจน์ตัวตนโดยมีการจัดการข้อมูลสมาชิกผ่าน Web Browser โดยระบบได้ทำการเก็บข้อมูลผู้ใช้บริการจากชื่อผู้ใช้และรหัสผ่านเท่านั้นด้วยวิธีการกรอกข้อมูล ซึ่งระบบนี้ไม่มีการกำหนดให้เก็บข้อมูลอย่างอื่นเช่น จากหมายเลขบัตรประจำตัวประชาชน นอกจากนี้ยังไม่มีระบบสำรองข้อมูล และยากสำหรับการค้นหาและระบุตัวตนที่แท้จริงของผู้ใช้งานอินเทอร์เน็ตในภายหลัง

จากการศึกษางานวิจัยที่เกี่ยวข้องพบว่า มีการพัฒนาระบบจัดเก็บข้อมูลหรือร่องรอยของผู้ใช้งานอินเทอร์เน็ต (Log File) ในรูปแบบต่างๆ เพื่อให้สามารถใช้งานและรองรับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 นั้น พบว่ายังไม่มีการพูดถึงการนำเอาโอเพ่นซอร์สมาใช้งานหรือประยุกต์ใช้กันอย่างจริงจัง และนอกจากนั้นส่วนสำคัญที่สุดที่จะต้องพิจารณาในการพัฒนาระบบคือ การออกแบบที่ให้ความสำคัญกับข้อมูลรายละเอียดของผู้ใช้แต่ละรายเพื่อใช้ในการตรวจสอบและติดตามได้อย่างมีประสิทธิภาพ ผู้วิจัยจึงนำเสนอวิธีการโดยนำโอเพ่นซอร์สที่มีอยู่จำนวนมากมาใช้ในการจัดเก็บข้อมูลและแก้ปัญหาดังกล่าว