บทที่ 2

แนวคิดและทฤษฎีที่เกี่ยวข้อง

2.1 เทคนิคการเข้ารหัส (encryption technique)

การเข้ารหัส (cryptography) เป็นเทคนิคที่ใช้ในการแปลงข้อมูลหรือข้อความที่สามารถอ่านเข้าใจได้ (plain text หรือ clear text) เช่น แฟ้มตัวอักษร (text file) เสียง ภาพ เป็นต้น ให้เป็นข้อมูลที่เข้ารหัสแบบข้อมูลตัวอักษร (text) หรือข้อมูลไบนารี่ (binary) ที่ไม่สามารถอ่านเข้าใจได้ (ciphertext) ดังรูปที่ 2.1 [3]

รูปที่ 2.1 แสดงการทำงานของการเข้ารหัสและการถอดรหัส

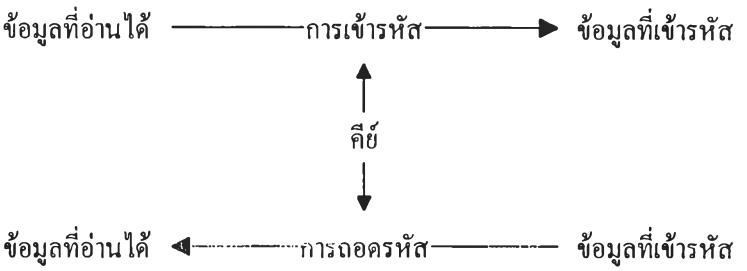
เทคนิคที่ใช้ในการเข้ารหัสสามารถแบ่งออกได้เป็น 3 ประเภท

- แฮชชิงฟังก์ชัน (hashing function)
- การเข้ารหัสโดยใช้คีย์ลับเฉพาะ (secret key cryptography)
- การเข้ารหัสโดยใช้คีย์สาธารณะ (public key cryptography)

เทคนิคทั้ง 3 แบบ มีความแตกต่างกันที่จำนวนคีย์ที่ใช้ในการเข้ารหัส โดยแฮชชิงฟังก์ชัน การเข้ารหัสโดยใช้คีย์ลับเฉพาะ และ การเข้ารหัสโดยใช้คีย์สาธารณะ จะมีการใช้จำนวนคีย์ในการเข้ารหัสและถอดรหัส 0 1 และ 2 คีย์ตามลำดับ สำหรับวิทยานิพนธ์นี้จะใช้เทคนิคการเข้ารหัสแบบใช้คีย์สาธารณะในการพิสูจน์ตัวจริง (authentication) และใช้เทคนิคการเข้ารหัสแบบใช้คีย์ลับเฉพาะในการเข้ารหัสข้อมูลเพื่อป้องกันการดักฟัง[4]

2.1.1 การเข้ารหัสแบบใช้คีย์ลับเฉพาะ (secret key cryptography)

การเข้ารหัสแบบใช้คีย์ลับเฉพาะ เป็นเทคนิคการเข้ารหัสที่ใช้คีย์เพียงคีย์เดียวทั้งในการเข้ารหัสและถอดรหัสทำให้จำเป็นต้องเปิดเผยคีย์ให้กับผู้ใช้ทั้งสองฝั่งทราบโดยมีการทำงาน ดังรูปที่ 2.2[4]



รูปที่ 2.2 แสดงการทำงานของการเข้ารหัสและการถอดรหัสแบบใช้คีย์ลับเฉพาะ

จากการทำงานในลักษณะดังกล่าวทำให้เทคนิคการเข้ารหัสแบบใช้คีย์ลับเฉพาะไม่เหมาะสมในการนำมาใช้ในการพิสูจน์ตัวจริงเนื่องจากมีปัญหาเรื่องการรักษาความปลอดภัยของคีย์และการแจกจ่ายคีย์ แต่ได้มีการใช้วิธีการพิสูจน์ตัวจริงเคอเบอรอส (kerberos authentication system)[6] มาแก้ปัญหาดังกล่าว

ข้อดีของการเข้ารหัสแบบใช้คีย์ลับเฉพาะ คือเทคนิคนี้จะมีประสิทธิภาพและความเร็วในการทำงานสูง จึงมีความเหมาะสมที่จะนำมาใช้เพื่อการเข้ารหัสข้อมูลที่รับส่งไปมา (session)

2.1.2 การเข้ารหัสแบบใช้คีย์สาธารณะ (public key cryptography)

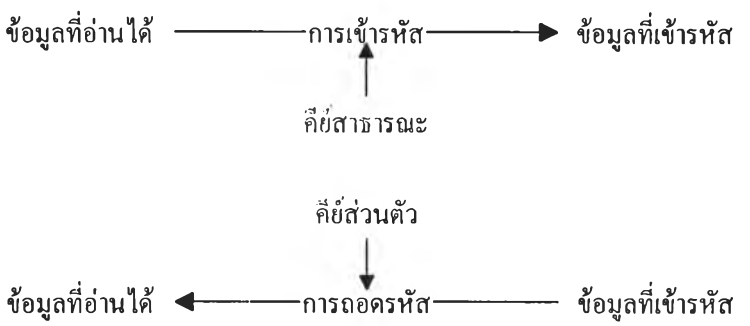
การเข้ารหัสแบบใช้คีย์สาธารณะเป็นเทคนิคการเข้ารหัสที่ประกอบด้วยคีย์จำนวน 2 ตัว

- คีย์ส่วนตัว (private key)
- คีย์สาธารณะ (public key)

การทำงานของการเข้ารหัสแบบใช้คีย์สาธารณะจะแตกต่างจากการเข้ารหัสแบบใช้คีย์ลับเฉพาะที่การเข้ารหัสและการถอดรหัสจะใช้คีย์คนละตัวกันจึงมีชื่อเรียกอีกชื่อว่า asymmetric cryptography และมีรูปแบบการใช้งาน 2 รูปแบบ คือ [4]

2.1.2.1 ทำการเข้ารหัสด้วยคีย์สาธารณะ และถอดรหัสด้วยคีย์ส่วนตัว

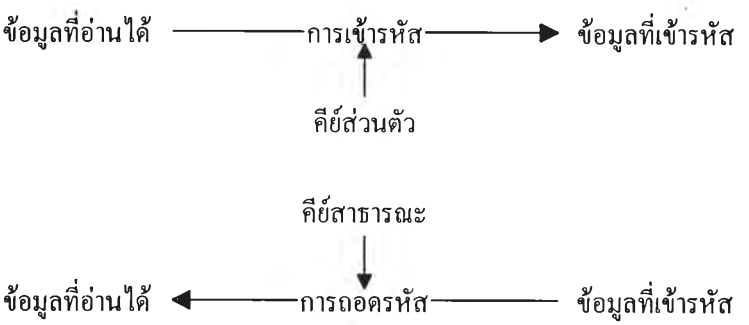
ในทางปฏิบัติคีย์สาธารณะจะถูกประกาศให้กับบุคคลทั่วไปทราบ เพื่อให้ผู้ส่งใช้เป็นคีย์ในการเข้ารหัส และส่งกลับมายังผู้รับซึ่งเป็นเจ้าของคีย์สาธารณะและรู้คีย์ส่วนตัวเป็นผู้ที่สามารถถอดรหัสออกด้วยคีย์ส่วนตัวได้เพียงผู้เดียว ดังรูปที่ 2.3 [4]



รูปที่ 2.3 แสดงการทำงานของการเข้ารหัสด้วยคีย์สาธารณะ และทำการถอดรหัสด้วยคีย์ส่วนตัว

2.1.2.2 ทำการเข้ารหัสด้วยคีย์ส่วนตัว และถอดรหัสด้วยคีย์สาธารณะ

รูปแบบการใช้งานในลักษณะนี้มีจุดประสงค์เพื่อแสดงความเป็นเจ้าของข้อมูล ซึ่งเปรียบเสมือนการลงชื่อกำกับในเอกสาร (signature) แต่ในที่นี้เป็นการลงชื่อกำกับบนข้อมูลอิเล็กทรอนิกส์ (digital signature) โดยผู้ส่งจะเข้ารหัสข้อมูลด้วยคีย์ส่วนตัวและส่งไปยังผู้รับ ผู้รับจะสามารถพิสูจน์ว่าข้อมูลที่ได้รับเป็นของผู้ส่งหรือไม่ โดยการถอดรหัสด้วยคีย์สาธารณะของผู้ส่งซึ่งไม่เป็นความลับ ดังรูปที่ 2.4 [4]



รูปที่ 2.4 แสดงการทำงานของการเข้ารหัสด้วยคีย์ส่วนตัว และทำการถอดรหัสด้วยคีย์สาธารณะ

จากเหตุผลที่การเข้ารหัสแบบใช้คีย์สาธารณะไม่จำเป็นต้องเปิดเผยคีย์ส่วนตัวให้กับผู้อื่นทราบ แต่จะเปิดเผยเฉพาะคีย์สาธารณะเท่านั้นจึงทำให้มีความปลอดภัยที่จะนำมาใช้เพื่อการพิสูจน์ตัวจริง แต่ในทางตรงกันข้ามการทำงานของการเข้ารหัสแบบใช้คีย์สาธารณะกลับมีประสิทธิภาพและความเร็วในการทำงานที่ต่ำกว่าการเข้ารหัสแบบใช้คีย์ลับเฉพาะ ทำให้ไม่เหมาะที่จะนำมาใช้เข้ารหัสข้อมูลที่ส่งไปมา

2.2 การพิสูจน์ตัวจริงโดยใช้เทคนิคการเข้ารหัส (encryption based authentication)

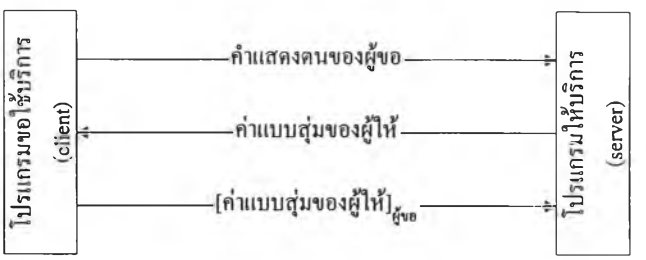
จากเหตุผลที่กล่าวมาแล้วทำให้เราเลือกใช้วิธีการพิสูจน์ตัวจริง โดยใช้เทคนิคการเข้ารหัสแบบใช้คีย์สาธารณะสำหรับวิทยานิพนธ์นี้

การพิสูจน์ตัวจริงโดยใช้เทคนิคการเข้ารหัสแบบใช้คีย์สาธารณะ สามารถแบ่งออกได้ดังนี้

1) ชนิดทางเดียว (one-way)
2) ชนิดสองทาง (two-way)

2.2.1 การพิสูจน์ตัวจริงชนิดทางเดียวโดยใช้เทคนิคการเข้ารหัสแบบใช้คีย์สาธารณะ

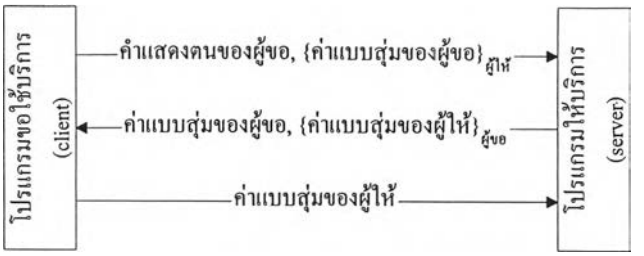
การพิสูจน์ตัวจริงชนิดทางเดียวโดยใช้เทคนิคการเข้ารหัสแบบใช้คีย์สาธารณะ มีขั้นตอนการทำงานดังรูปที่ 2.5 ดังนี้



รูปที่ 2.5 แสดงโพรโทคอลที่ใช้ในการพิสูจน์ตัวจริงชนิดทางเดียว ด้วยเทคนิคการเข้ารหัสแบบใช้คีย์สาธารณะ

1) ผู้ขอให้บริการส่งคำแสดงตนไปยังผู้ให้บริการ
2) ผู้ให้บริการเลือกค่าแบบสุ่มขึ้นมาหนึ่งค่าแล้วส่งกลับมาให้ผู้ขอใช้บริการ
3) ผู้ขอใช้บริการนำค่าแบบสุ่มที่ได้รับมาทำการเข้ารหัสด้วยคีย์ส่วนตัวแล้วส่งกลับไปยังผู้ให้บริการ
4) ผู้ให้บริการทำการถอดรหัสด้วยคีย์สาธารณะของผู้ขอใช้บริการเพื่อการพิสูจน์ตัวจริง

2.2.2 การพิสูจน์ตัวจริงชนิดสองทางโดยใช้เทคนิคทางเข้ารหัสแบบใช้คีย์สาธารณะ มีขั้นตอนการทำงานดังรูปที่ 2.6 ดังนี้



รูปที่ 2.6 แสดงโพรโทคอลที่ใช้ในการพิสูจน์ตัวจริงชนิดสองทาง ด้วยเทคนิคการเข้ารหัสแบบใช้คีย์สาธารณะ

1) ผู้ขอใช้บริการส่งคำแสดงตน พร้อมค่าแบบสุ่มของผู้ขอใช้บริการที่เข้ารหัสด้วยคีย์สาธารณะของผู้ให้บริการ ไปยังผู้ให้บริการ
2) ผู้ให้บริการทำการถอดรหัสด้วยคีย์ส่วนตัวเพื่อให้ได้ค่าแบบสุ่มของผู้ขอใช้บริการ
3) ผู้ให้บริการส่งค่าแบบสุ่มของผู้ขอใช้บริการกลับคืนเพื่อพิสูจน์ตัวจริง พร้อมค่าแบบสุ่มของผู้ให้บริการที่เข้ารหัสด้วยคีย์สาธารณะของผู้ขอใช้บริการ ไปยังผู้ขอใช้บริการ
4) ผู้ขอใช้บริการทำการถอดรหัสด้วยคีย์ส่วนตัวของผู้ขอใช้บริการเพื่อให้ได้ค่าแบบสุ่มของผู้ให้บริการ
5) ผู้ขอใช้บริการส่งค่าแบบสุ่มของผู้ให้บริการกลับไปยังผู้ให้บริการเพื่อการพิสูจน์ตัวจริง

จากโพรโทคอล (protocol) ที่แสดงจะพบว่าการพิสูจน์ตัวจริงโดยใช้เทคนิคการเข้ารหัสแบบใช้คีย์สาธารณะชนิดสองทางเป็นรูปแบบที่มีความมั่นคงสูง

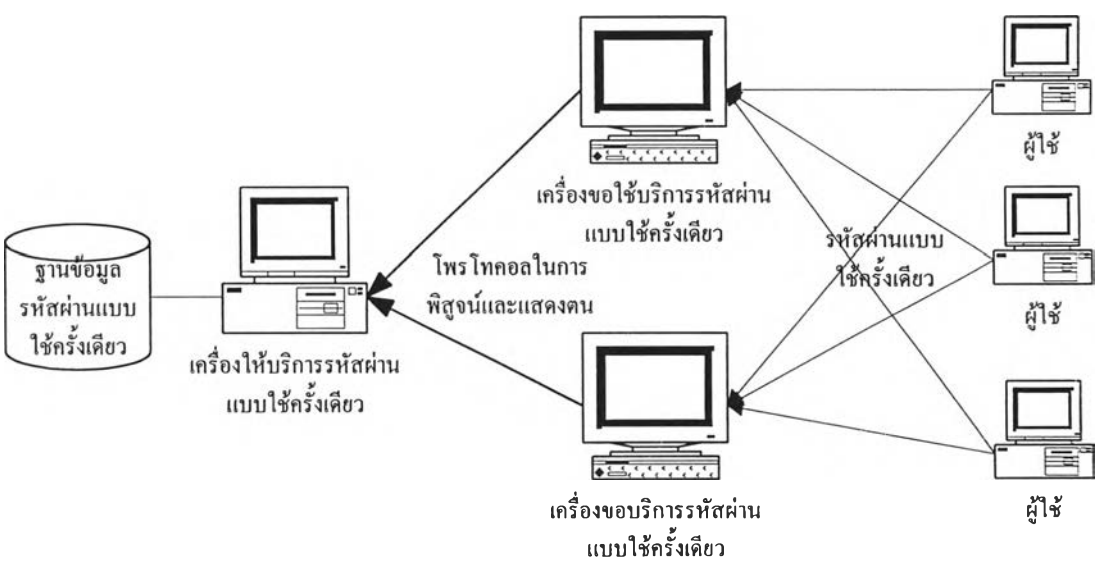
2.3 การแลกเปลี่ยนคีย์ (key exchange)

หลังจากที่เครื่องที่ขอใช้บริการรหัสผ่านแบบใช้ครั้งเดียว สามารถพิสูจน์ตัวจริงกับเครื่องที่ให้บริการรหัสผ่านแบบใช้ครั้งเดียวได้ ขั้นตอนต่อไปเป็นการสร้างคีย์เพื่อใช้การเข้ารหัสข้อมูลที่ส่งไปมา ซึ่งเรียกว่าเซสชั่นคีย์ (session key) สำหรับการสร้างเซสชั่นคีย์ในระบบการพิสูจน์ตัวจริงโดยใช้เทคนิคการเข้ารหัสแบบใช้คีย์สาธารณะชนิดสองทางมีด้วยกันหลายวิธี วิธีหนึ่งง่ายแต่ได้ผลคือ ทั้งสองฝั่งต่างเลือกค่าแบบสุ่ม (random) ขึ้นมาข้างละหนึ่งค่า แล้วทำการเข้ารหัสด้วยคีย์สาธารณะของฝั่งตรงข้ามแล้วแลกเปลี่ยนซึ่งกันและกัน หลังจากนั้นต่างฝ่ายจะสามารถคำนวณหาเซสชั่นคีย์ได้

2.4 ระบบรหัสผ่านแบบใช้ครั้งเดียว (one-time password)

2.4.1 องค์ประกอบของระบบรหัสผ่านแบบใช้ครั้งเดียว

ระบบรหัสผ่านแบบใช้ครั้งเดียวมีองค์ประกอบดังรูปที่ 2.7 ดังนี้



รูปที่ 2.7 แผนผังแสดงการทำงานของระบบรหัสผ่านแบบใช้ครั้งเดียว

2.4.1.1 ผู้ให้บริการรหัสผ่านแบบใช้ครั้งเดียว เป็นผู้ที่ทำหน้าที่

1) ให้บริการตรวจสอบรหัสผ่านแบบใช้ครั้งเดียว

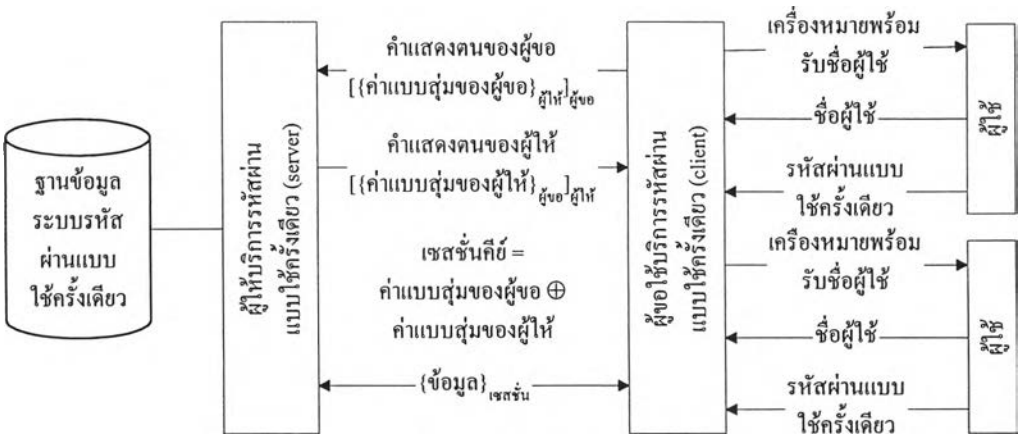
2) ให้บริการบำรุงรักษาระบบรหัสผ่านแบบใช้ครั้งเดียว

2.4.1.2 ผู้ขอใช้บริการรหัสผ่านแบบใช้ครั้งเดียว เป็นผู้ที่ทำการร้องขอการตรวจสอบรหัสผ่านแบบใช้ครั้งเดียวจากผู้ให้บริการรหัสผ่านแบบใช้ครั้งเดียว เมื่อมีผู้ใช้ขอล็อกอิน

2.4.1.3 ผู้ใช้ หมายถึง ผู้ทำการล็อกอินเข้าเครื่องแม่ข่าย ผ่านทางเทอร์มินอล หรือ เครื่องคอมพิวเตอร์ที่ทำงานเลียนแบบเทอร์มินอล เพื่อใช้ทรัพยากรบนเครื่องแม่ข่ายดังกล่าว

2.4.2 โพรโทคอลระบบรหัสผ่านแบบใช้ครั้งเดียว (one-time password protocol)

เมื่อนำเทคนิคการเข้ารหัสมาเพิ่มความมั่นคงให้กับระบบรหัสผ่านแบบใช้ครั้งเดียว ทำให้มีความจำเป็นต้องมีการปรับเปลี่ยนโพรโทคอลระหว่างเครื่องขอให้บริการรหัสผ่านแบบใช้ครั้งเดียวกับเครื่องให้บริการรหัสผ่านแบบใช้ครั้งเดียว ดังรูปที่ 2.8 ดังนี้



รูปที่ 2.8 แสดงการทำงานของโพรโทคอลที่ใช้ในระบบรหัสผ่านแบบใช้ครั้งเดียวที่ปรับปรุงด้วยเทคนิคการเข้ารหัส

2.4.2.1 เมื่อผู้ใช้ได้รับเครื่องหมายพร้อมรับชื่อผู้ใช้ (prompt) ผู้ใช้จะทำการพิมพ์ชื่อผู้ใช้ และรหัสผ่านแบบใช้ครั้งเดียว ซึ่งจะถูกส่งไปยังเครื่องที่ผู้ใช้ต้องการขอล็อกอิน

2.4.2.2 เครื่องที่ถูกล็อกอิน (ผู้ขอใช้บริการ) จะทำการขอการตรวจสอบรหัสผ่านแบบใช้ครั้งเดียวกับผู้ให้บริการรหัสผ่านแบบใช้เดียว โดยมีขั้นตอนดังนี้

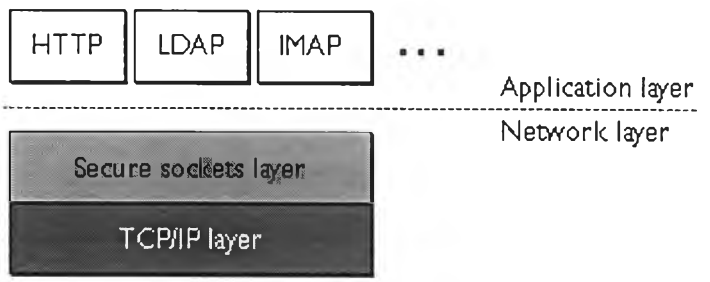
1) เครื่องที่ถูกล็อกอิน ทำการพิสูจน์ตัวจริงผู้ให้บริการรหัสผ่านแบบใช้ครั้งเดียว พร้อมสร้างเซสชั่นคีย์ เพื่อใช้ในการเข้ารหัสข้อมูล
2) เครื่องที่ถูกล็อกอินกับผู้ให้บริการรหัสผ่านแบบใช้ครั้งเดียวทำการแลกเปลี่ยนข้อมูลซึ่งกันและกัน เพื่อการตรวจสอบรหัสผ่านแบบใช้ครั้งเดียว โดยใช้เซสชั่นคีย์ในการเข้ารหัสเพื่อรักษาความปลอดภัย

2.5 โพรโทคอล เอสเอสแอล

โพรโทคอล เอสเอสแอล (SSL : Secure Socket Layer)[7] ถูกพัฒนาขึ้นโดยบริษัท Netscape Communications เพื่อจุดประสงค์ในการพิสูจน์ตัวจริงและการเข้ารหัสข้อมูลสำหรับการใช้งาน World Wide Web ต่อมาได้ถูกกำหนดขึ้นเป็นมาตรฐานโดยองค์กร Internet Engineering Task Fore (IETF) ภายใต้ชื่อ โพรโทคอล ทีแอลเอส (TLS : Transport Layer Security)[7]

2.5.1 หลักการทำงานของโพรโทคอล เอสเอสแอล

โพรโทคอล เอสเอสแอล ถูกสร้างขึ้นเพื่อเพิ่มความปลอดภัยให้กับชั้น ทีซีพี (TCP : Transmission Control Protocol) ของโพรโทคอล ทีซีพี/ไอพี (TCP/IP : Transmission Control Protocol/Internet Protocol) โดยการแทรกตัวอยู่เหนือชั้น ทีซีพี และอยู่ใต้ชั้นโปรแกรมประยุกต์ (Application Layer) เช่น HyperText Transport Protocol (HTTP), Lightweight Directory Access Protocol (LDAP), Internet Messaging Protocol (IMAP) เป็นต้น ดังแสดงในรูปที่ 2.9



รูปที่ 2.9 แสดงหลักการทำงานของโพรโทคอล เอสเอสแอล

โพรโทคอล เอสเอสแอล ประกอบด้วยโปรแกรมสองส่วน คือ ส่วนของผู้ให้บริการ (server) และส่วนของผู้ขอใช้บริการ (client) โปรแกรมทั้งสองฝั่งจะต้องมีการแทรกชั้นของโพรโทคอล เอสเอสแอล อยู่เหนือชั้น ทีซีพี เพื่อเพิ่มความปลอดภัยใช้กับโปรแกรมประยุกต์ที่ทำงานแบบระบบรับ-ให้บริการ (client-server)

บริการความปลอดภัยที่โพรโทคอล เอสเอสแอล สามารถให้บริการได้แก่

2.5.1.1 บริการพิสูจน์ตัวจริงของผู้ให้บริการ (server authentication)

เป็นบริการที่ผู้ให้บริการทำการพิสูจน์ตัวจริงต่อผู้ขอใช้บริการ โดยอาศัยเทคนิคการเข้ารหัสแบบสาธารณะ เพื่อให้ผู้ขอใช้บริการมั่นใจว่ากำลังคุยอยู่กับผู้ให้บริการตัวจริง ตัวอย่างเช่น การส่งเลขที่บัตรเครดิตให้กับผู้ขายผ่านทางเครือข่าย เป็นต้น

2.5.1.2 บริการพิสูจน์ตัวจริงของผู้ขอใช้บริการ (client authentication)

เป็นบริการทางเลือก (option) บนโพรโทคอล เอสเอสแอล ที่ให้ผู้ขอใช้บริการต้องทำการพิสูจน์ตัวจริงต่อผู้ให้บริการเช่นกัน เสริมจากการพิสูจน์ตัวจริงของผู้ให้บริการ ซึ่งเป็นข้อบังคับ ตัวอย่างเช่น ธนาคารต้องการความมั่นใจว่าข้อมูลทางการเงินถูกส่งถึงลูกค้าตัวจริงผ่านทางเครือข่าย เป็นต้น

2.5.1.3 บริการช่องทางสื่อสารแบบเข้ารหัส (encrypted SSL connection)

เป็นบริการที่ทำให้เกิดช่องทางสื่อสารที่มีการเข้ารหัสเพื่อป้องกันการดักฟัง โดยอาศัยเทคนิคการเข้ารหัสแบบใช้คีย์ลับเฉพาะ ซึ่งถูกสร้างขึ้นทุกครั้งที่มีการติดต่อสื่อสาร (session)

2.5.2 องค์ประกอบของโพรโทคอล เอสเอสแอล

โพรโทคอล เอสเอสแอล ประกอบด้วยชั้นย่อย (sublayer) สองชั้นคือ

2.5.2.1 ชั้นย่อย SSL Record เป็นโพรโทคอลที่กำหนดรูปแบบของข้อมูลที่ส่งผ่านระหว่างกัน

2.5.2.2 ชั้นย่อย SSL Handshake เป็นโพรโทคอลที่กำหนดขั้นตอนการติดต่อสื่อสารระหว่างผู้ให้บริการแบบ เอสเอสแอล (SSL-enabled server) และผู้ขอใช้บริการแบบ เอสเอสแอล (SSL-enabled client) ในชั้นย่อย SSL Handshake นี้ประกอบด้วยขั้นตอนต่างๆ ดังนี้

1) การพิสูจน์ตัวจริงของผู้ให้บริการต่อผู้ขอใช้บริการ
2) การกำหนดเทคนิคการเข้ารหัสร่วมกันระหว่างผู้ให้บริการและผู้ขอใช้บริการ สำหรับช่องทางสื่อสารแบบเข้ารหัส
3) การพิสูจน์ตัวจริงของผู้ขอใช้บริการต่อผู้ให้บริการ
4) การสร้างคีย์ร่วม (session key) สำหรับช่องทางสื่อสารแบบเข้ารหัส
5) การสร้างช่องทางสื่อสารแบบเข้ารหัส (encrypted SSL connection)

2.5.3 มาตรฐานการแลกเปลี่ยนคีย์และการเข้ารหัสบนโพรโทคอล เอสเอสแอล

เนื่องจากโพรโทคอล เอสเอสแอล มีขีดความสามารถในการเข้ารหัสหลายแบบด้วยกัน เช่น

- DES. (Data Encryption Standard).
- DSA. (Digital Signature Algorithm).
- KEA. (Key Exchange Algorithm).

- MD5. (Message Digest algorithm).
- RC2 and RC4. (Rivest encryption ciphers).
- RSA. (Rivest, Shamir, and Adleman).
- RSA key exchange.
- SHA-1. (Secure Hash Algorithm).
- SKIPJACK.
- Triple-DES.

เทคนิคการเข้ารหัสเหล่านี้ที่ถูกนำเอามาใช้ในขั้นตอนต่างๆ คือ การพิสูจน์ตัวจริง (authenticating) การส่งใบรับรอง (certificate transmitting) การกำหนดคีย์ร่วม (session keys) เป็นต้น ดังนั้นจึงจำเป็นที่จะต้องการการทำความตกลง (negotiate) การใช้เทคนิคการเข้ารหัสให้สอดคล้องกันระหว่างผู้ให้บริการและผู้ขอใช้บริการ การทำความตกลงการใช้เทคนิคการเข้ารหัสจะขึ้นอยู่กับปัจจัยหลายประการเช่น เวอร์ชันของโพรโทคอล เอสเอสแอล, นโยบายของผู้ใช้ (policy), ข้อจำกัดทางด้านกฎหมาย เป็นต้น ทำให้เราสามารถจัดชุดของเทคนิคการเข้ารหัสได้ดังนี้

2.5.3.1 ชุดเข้ารหัสแบบแข็งแรงสูงสุด (strongest cipher suites)

– Triple DES 168-bit Encryption, SHA-1 message authentication

อนุญาตให้ใช้ภายในประเทศสหรัฐอเมริกาเท่านั้น เหมาะสำหรับหน่วยงานที่มีการส่งข้อมูลที่สำคัญมากๆ เช่น ธนาคาร เป็นต้น

2.5.3.2 ชุดเข้ารหัสแบบแข็งแรง (strong cipher suites)

– RC4 128-bit Encryption, MD5 message authentication

– RC2 128-bit Encryption, MD5 message authentication

– DES 56-bit Encryption, SHA-1 message authentication

อนุญาตให้ใช้ภายในประเทศสหรัฐอเมริกาเท่านั้น เหมาะสำหรับธุรกิจและหน่วยงานของรัฐ

2.5.3.3 ชุดเข้ารหัสแบบปานกลาง (exportable cipher suites)

– RC4 40-bit Encryption, MD5 message authentication

– RC2 40-bit Encryption, MD5 message authentication

เป็นชุดเข้ารหัสที่อนุญาตนำออกไปใช้นอกประเทศสหรัฐอเมริกาได้

2.5.3.4 ชุดเข้ารหัสแบบอ่อนแอ (weakest cipher suite)

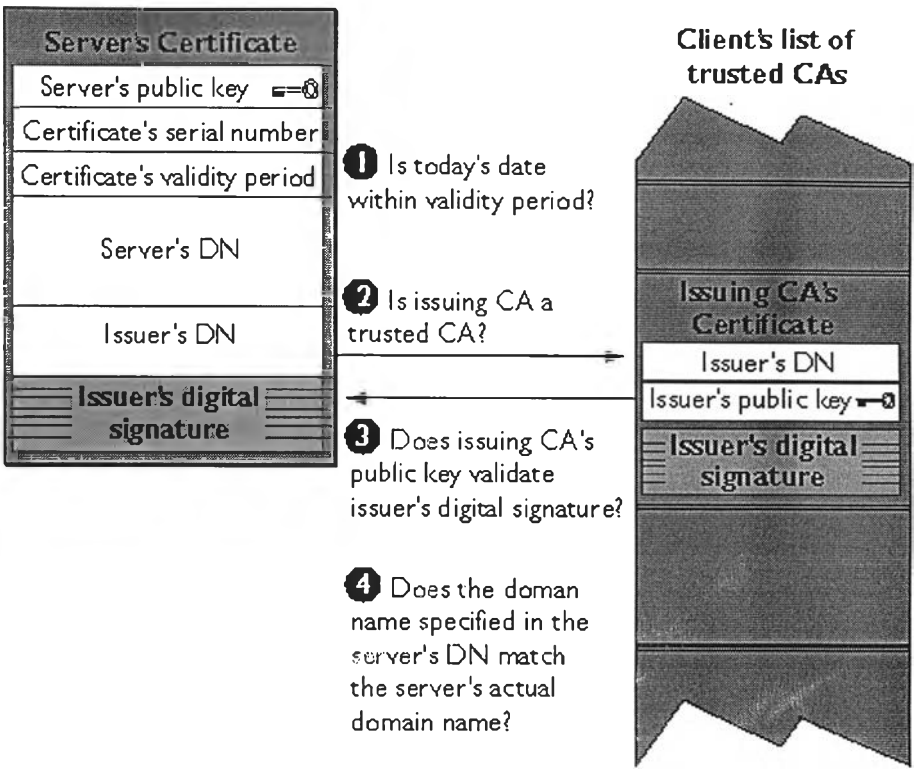
– No Encryption, MD5 message authentication

เป็นชุดเข้ารหัสที่ไม่มีการสร้างช่องทางสื่อสารแบบเข้ารหัส แต่ยังคงมีการพิสูจน์ตัวจริง และการลงลายเซ็นอิเล็กทรอนิกส์ เหมาะสำหรับการส่งข้อมูลที่ไม่ต้องการป้องกันการดักฟัง

ชุดเข้ารหัสที่กล่าวมาแล้วทั้งหมดนี้ จะใช้เทคนิคการแลกเปลี่ยนคีย์แบบ อาร์เอสเอ (RSA key–exchange) นอกจากชุดการเข้ารหัสที่กล่าวมาแล้วทั้งหมดนี้ ยังมีชุดการเข้ารหัสอีกแบบคือ FORTEZZA Cipher Suite ซึ่งใช้เทคนิคการแลกเปลี่ยนคีย์แบบ เคอีเอ (KEA key-exchange) แต่จะไม่ขอกล่าวในการวิจัยนี้ เนื่องจากถูกจำกัดการใช้อยู่เฉพาะหน่วยงานรัฐบาลของประเทศสหรัฐอเมริกาเท่านั้น

2.5.4 การพิสูจน์ตัวจริงของผู้ให้บริการ (server authentication)

โพรโทคอล เอสเอสแอล กำหนดให้ผู้ขอใช้บริการร้องขอให้ผู้ให้บริการพิสูจน์ตัวจริง โดยผู้ให้บริการจะต้องส่งใบรับรอง (certificate) ของผู้ให้บริการให้กับผู้ขอใช้บริการ เมื่อผู้ขอใช้บริการได้รับใบรับรองแล้วจะทำการตรวจสอบดังแสดงในรูปที่ 2.10



รูปที่ 2.10 แสดงลำดับการทำงานของการพิสูจน์ตัวจริงของผู้ให้บริการ

2.5.4.1 ตรวจสอบอายุของใบรับรอง (validity period) ผู้ขอใช้บริการจะทำการตรวจสอบว่า ขณะที่ใช้ใบรับรองนั้นเป็นช่วงเวลาที่ระบุในอายุของใบรับรองหรือไม่ ถ้าวันที่ ณ เวลาที่ใช้อยู่ก่อนวันเริ่มต้นของอายุใบรับรอง แสดงว่าใบรับรองยังไม่ถึงเวลาใช้ แต่ถ้าอยู่หลังวันสิ้นสุดของอายุใบรับรอง แสดงว่าใบรับรองหมดอายุ

2.5.4.2 ตรวจสอบว่าผู้ออกใบรับรอง (CA : Certification Authorities) เชื่อถือได้หรือไม่ ตามปกติผู้ขอใช้บริการจะมีรายชื่อผู้ออกใบรับรองที่เชื่อถือได้เก็บอยู่ ผู้ขอใช้บริการจะทำการตรวจสอบว่าชื่อผู้ออกใบรับรอง (issuer's Distinguished Name) ที่ระบุในใบรับรองที่ถูกส่งมาว่า อยู่ในรายชื่อผู้ออกใบรับรองที่เชื่อถือได้หรือไม่ ถ้าอยู่ในรายชื่อแสดงว่าผู้ออกใบรับรองเชื่อถือได้

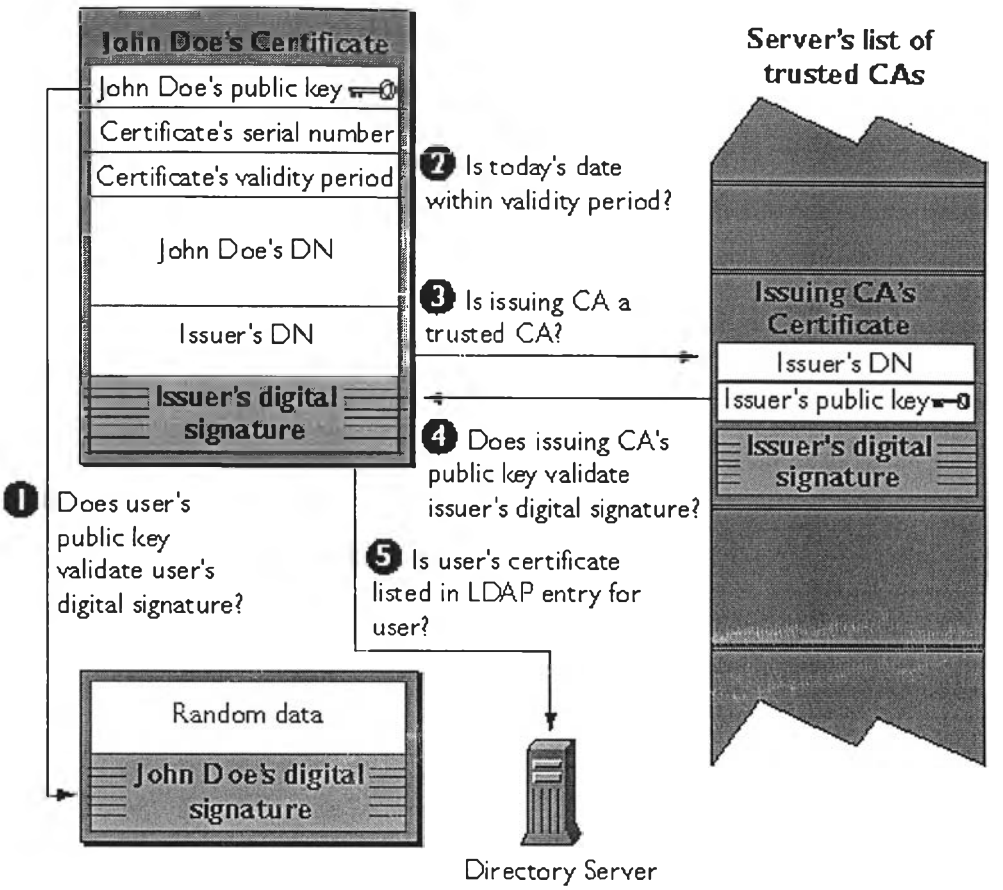
2.5.4.3 ตรวจสอบลายเซ็นอิเล็กทรอนิกส์ของผู้ออกใบรับรอง ผู้ขอใช้บริการจะใช้คีย์สาธารณะที่เก็บอยู่ในรายชื่อผู้ออกใบรับรองที่เชื่อถือได้ทำการตรวจสอบลายเซ็นอิเล็กทรอนิกส์ของผู้ออกใบรับรอง ถ้าลายเซ็นอิเล็กทรอนิกส์ไม่ถูกต้องแสดงว่าใบรับรองอาจถูกแก้ไข หรือใบรับรองอาจถูกออกโดยผู้ออกใบรับรองตัวปลอม ถ้าลายเซ็นอิเล็กทรอนิกส์ถูกต้อง ผู้ขอใช้บริการจะยอมรับใบรับรองและคีย์สาธารณะในใบรับรอง

2.5.4.4 ตรวจสอบชื่อโดเมน ผู้ขอใช้บริการจะทำการตรวจสอบชื่อโดเมนตามที่ระบุในใบรับรองว่าตรงกับชื่อโดเมนจริงๆ ของผู้ให้บริการที่ส่งใบรับรองให้หรือไม่ ถ้าไม่ตรงแสดงว่ามีการปลอมตัวเป็นผู้ให้บริการซึ่งอาจจะมุ่งร้ายด้วยวิธี Man-in-the-Middle

2.5.5 การพิสูจน์ตัวจริงของผู้ขอใช้บริการ (client authentication)

ตามปกติผู้ให้บริการจะไม่ขอให้ผู้ขอใช้บริการพิสูจน์ตัวจริง แต่ในบางกรณีเราสามารถกำหนดให้ผู้ให้บริการขอให้ผู้ขอใช้บริการพิสูจน์ตัวจริงได้ เป็นผลให้ผู้ขอใช้บริการต้องจัดส่งใบรับรอง, ข้อมูลแบบสุ่ม และลายเซ็นอิเล็กทรอนิกส์ ให้กับผู้ให้บริการเพื่อการพิสูจน์ตัวจริงของผู้ขอใช้บริการ

ในการสร้างลายเซ็นอิเล็กทรอนิกส์ ผู้ขอใช้บริการจะสร้างข้อมูลแบบสุ่ม (random data) ขึ้น แล้วใช้แฮชชิงฟังก์ชัน (hashing function) และคีย์ส่วนตัวของผู้ขอใช้บริการในการสร้างลายเซ็นอิเล็กทรอนิกส์ ขั้นตอนการตรวจสอบในการพิสูจน์ตัวจริงของผู้ขอใช้บริการ แสดงได้ดังรูปที่ 2.11



รูปที่ 2.11 แสดงลำดับการทำงานของการพิสูจน์ตัวจริงของผู้ขอใช้บริการ

2.5.5.1 การตรวจสอบลายเซ็นอิเล็กทรอนิกส์ด้วยคีย์สาธารณะ ผู้ให้บริการจะใช้คีย์สาธารณะในใบรับรองที่ได้รับเพื่อตรวจสอบลายเซ็นอิเล็กทรอนิกส์ที่ส่งมาพร้อมกัน ถ้าลายเซ็นอิเล็กทรอนิกส์ถูกต้องแสดงว่าผู้ขอใช้บริการถือคีย์ส่วนตัวที่สอดคล้องกับคีย์สาธารณะที่อยู่ในใบรับรอง

2.5.5.2 การตรวจสอบอายุของใบรับรอง ถ้า ณ เวลาที่ใช้ใบรับรองอยู่ในช่วงเวลาของอายุใบรับรอง แสดงว่าใบรับรองยังคงใช้งานได้

2.5.5.3 การตรวจสอบว่าผู้ออกใบรับรองเชื่อถือได้หรือไม่ ผู้ให้บริการจะมีรายชื่อของผู้ออกใบรับรองที่เชื่อถือได้ ถ้าชื่อผู้ออกใบรับรองตามที่ระบุในใบรับรองไม่อยู่ในรายชื่อ แสดงว่าไม่สามารถเชื่อถือใบรับรองได้ แต่ถ้ามีอยู่ในรายชื่อจะต้องทำการตรวจสอบใบรับรองต่อไป

2.5.5.4 การตรวจสอบลายเซ็นอิเล็กทรอนิกส์ของผู้ออกใบรับรอง ผู้ให้บริการจะใช้คีย์สาธารณะที่เก็บอยู่ในรายชื่อผู้ออกใบรับรองที่เชื่อถือได้ในการตรวจสอบลายเซ็นอิเล็กทรอนิกส์ของผู้ออกใบรับรอง ถ้าลายเซ็นอิเล็กทรอนิกส์ถูกต้องแสดงว่าคีย์สาธารณะของผู้ขอใช้บริการตามที่ระบุในใบรับรองจริง ถ้าลายเซ็นอิเล็กทรอนิกส์ไม่ถูกต้องแสดงว่าใบรับรองอาจถูกแก้ไข หรือใบรับรองอาจถูกออกโดยผู้ออกใบรับรองตัวปลอม