ด้านความปลอดภัย

เครือข่ายอินเทอร์เน็ต เป็นเครือข่ายสาธารณะที่อนุญาตให้บุคคลใดก็ได้สามารถเชื่อมต่อเพื่อใช้งาน ดังนั้นทุกๆ คนบนโลกใบนี้ ไม่ว่าจะอยู่ในประเทศใด ทวีปใดบนโลก ก็สามารถเข้าถึงระบบ คอมพิวเตอร์ที่เชื่อมต่อกับอินเทอร์เน็ตได้ทั้งสิ้น และการที่อนุญาตให้มีการเชื่อมต่อในระดับสากลระหว่างระบบคอมพิวเตอร์และเครือข่าย ก็จะมีทั้งด้านดีและด้านเสีย

ในด้านดีของอินเทอร์เน็ต ทำให้ผู้ใช้สามารถเปิดโลกทรรศน์ตัวเอง ผู้คนสามารถค้นหาแหล่งความรู้ที่ต้องการ สามารถเข้าถึงข้อมูลหรือเอกสารเผยแพร่ที่มีประโยชน์หรือเอกสารที่หายาก เช่น เราสามารดาวน์โหลดไฟล์เอกสารจากทวีปยุโรปข้ามมายังทวีปเอเชียได้ในชั่วพริบตา หรือใช้สำหรับติดต่อสื่อสารผ่านจดหมายอิเล็กทรอนิกส์พูดคุยสนทนาผ่านเว็บออดิโอ รวมถึงการดำเนิน ธุรกรรม และการบริการอื่นๆ ที่มีอยู่จำนวนมาก

และด้วยการเปิดกว้างเช่นนี้จึงมีกลุ่มผู้ใช้บางคนที่มีจุดประสงค์หรือเป้าหมายที่แตกต่างไปจากบุคคลทั่วไป เช่น ต้องการขัดขวาง หรือจ้องทำลายระบบมิให้สามารถใช้งานได้ การใช้ประโยชน์จากเครือข่ายเพื่อวัตถุประสงค์ก่อการร้ายที่ส่งผลกระทบต่อความมั่นคงของประเทศชาติ การขโมยข้อมูลสำคัญของคู่แข่งขันทางธุรกิจ รวมถึงการล้างความลับทางราชการ โดยผู้ที่เข้าถึงระบบเครือข่ายส่วนตัวโดยไม่ได้รับการอนุญาต เราเรียกบุคคลเหล่านั้นว่า **แฮกเกอร์ (Hacker)**

ในความเป็นจริง คงไม่ใช่เพียงแต่ระบบอินเทอร์เน็ตเท่านั้นที่มีปัญหาด้านความปลอดภัย ซึ่งปกติทุกวันนี้ในชีวิตประจำวัน ไม่ว่าจะเป็นตัวเราที่ได้อาศัยอยู่ในบ้านเรือน ก็ยังต้องมีระบบความปลอดภัยพื้นฐานที่ทำให้ตัวเรารู้สึกปลอดภัย เช่น การปิดประตูบ้าน การปิดสวิตช์เครื่องใช้ไฟฟ้าทุกชนิด และล็อคกลอนประตูทุกครั้งก่อนออกจากบ้าน และหากมองในด้านของระบบคอมพิวเตอร์ตามสถาบันหรือหน่วยงานต่างๆ เช่น ศูนย์คอมพิวเตอร์ ตัวอย่างเช่น การใช้บัตรผ่านเฉพาะบุคคลภายใน เพื่อป้องกันมิให้ผู้อื่นหรือบุคคลที่ไม่เกี่ยวข้องสามารถเข้าไปในศูนย์คอมพิวเตอร์ การมียามที่คอยตรวจตราอุปกรณ์ เพื่อป้องกันมิให้ผู้ไม่หวังดีขโมยอุปกรณ์หรือข้อมูลออกไปจากศูนย์ นอกจากนี้ บุคคลากรภายในจัดเป็นปัจจัยสำคัญอย่างยิ่ง ที่อาจมีการจ้องทำลาย การเป็นสายลับ รวมถึงการลักลอบข้อมูลภายในไปใช้ หรือเผยแพร่ให้กับผู้อื่นโดยมิชอบ

ดังนั้น เนื้อหาต่อไปนี้ จะกล่าวถึงความปลอดภัยบนเครือข่าย โดยมุ่งเน้นถึงมาตรการความปลอดภัยขั้นพื้นฐานที่ควรทราบ , หลักการเข้ารหัสและการถอดรหัสข้อมูล (Encryption/Decryption), เทคโนโลยีกุญแจสาธารณะ (Public Key) และไฟร์วอลล์ (Firewall)

มาตรการความปลอดภัยขั้นพื้นฐาน

(Basic Security Measures)

ระบบคอมพิวเตอร์ทุกระบบ จำเป็นต้องมีมาตรการความปลอดภัยขั้นพื้นฐาน ยกตัวอย่างง่ายๆ เช่น คอมพิวเตอร์ที่ผู้คนส่วนใหญ่ใช้กันอยู่นั้น มักจะมีโปรแกรมป้องกันไวรัสเพื่อป้องกันมิให้ไวรัสเข้าสู่ระบบ โดยไวรัสคอมพิวเตอร์สามารถทำลายข้อมูลสำคัญบนเครื่องคอมพิวเตอร์ได้ และในบางครั้งเราอาจจำเป็นต้องมีการล็อคเครื่องคอมพิวเตอร์เพื่อป้องกันมิให้ผู้อื่นเข้ามาเปิดใช้งาน การล็อคกลอนประตู และรวมถึงการเข้ารหัสข้อมูลสำคัญๆ เพื่อป้องกันมิให้ใครแอบลักลอบข้อมูลไปใช้งาน สิ่งเหล่านี้จัดเป็นการป้องกันความปลอดภัยซึ่งแต่ละคนก็อาจจะใช้เทคนิคที่แตกต่างกันไปตามความเหมาะสม อย่างไรก็ตาม เนื้อหาต่อไปนี้ จะทำให้ทราบถึงมาตรการความปลอดภัยขั้นพื้นฐานที่พึงมี ซึ่งแต่ละมาตรการก็จะมีเทคนิควิธีที่แตกต่างกันไป โดยสามารถแบ่งออกได้เป็น 7 ประเภทด้วยกัน คือ

1. ความปลอดภัยด้านภายนอก (External Security)

2. ความปลอดภัยด้านการปฏิบัติงาน (Operational Security)

3. การตรวจตราเฝ้าระวัง (Surveillance)

4. การใช้รหัสผ่าน และระบบแสดงตัวตน (Passwords and ID Systems)

5. การตรวจสอบ (Auditing)

6. การกำหนดสิทธิการใช้งาน (Access Rights)

7. การป้องกันไวรัส (Guarding Against Viruses)

ความปลอดภัยด้านภายนอก (External Security)

ความปลอดภัยภายนอก เป็นลักษณะทางกายภาพที่ต้องการป้องกันระบบคอมพิวเตอร์ อุปกรณ์ หรือเครือข่ายเกิดความเสียหาย ตัวอย่างเช่น การป้องกันไฟไหม้ อุทกภัย แผ่นดินไหว ไฟตก/ไฟกระชาก และการถูกทำลาย ปกติเทคนิคการป้องกันความปลอดภัยด้านภายนอกนั้นมีหลายวิธีด้วยกัน แล้วก็พอเพียงต่อการนำไปใช้เพื่อให้เกิดความปลอดภัยได้ เช่น ศูนย์คอมพิวเตอร์ หรือศูนย์ปฏิบัติการคอมพิวเตอร์และเครือข่าย จะต้องปิดประตูและใส่กลอนเสมอ เพื่อป้องกันบุคคลอื่นหรือขโมยที่ต้องการลักลอบเข้าไป การจัดวางสายเคเบิลต่างๆ จะต้องมิดชิดไม่ระเกะระกะ เนื่องจากอาจทำให้ผู้คนเดินผ่านสะดุดหกล้มได้ ทำให้สายเคเบิลขาด และอาจก่อให้ระบบเกิดความเสียหายได้ สำหรับการป้องกันภัยธรรมชาติ ไม่ว่าจะเป็นแผ่นดินไหว อุทกภัยหรือไฟไฟม้ สามารถป้องกันได้ด้วยการออกแบบเครือข่าย โดยเฉพาะเครื่องเซิร์ฟเวอร์ให้มีระบบสำเนาข้อมูลแบบสมบูรณ์ (Redundant Network) และเครื่องสำเนาระบบนี้อาจติดตั้งไว้สถานที่อีกแห่งหนึ่งที่ปลอดภัย โดยแนวทางดังกล่าวก็จัดเป็นแนวทางหนึ่งที่นิยม

สำหรับกรณีที่ศูนย์ปฏิบัติการคอมพิวเตอร์ จำเป็นต้องบริการแก่บุคคลทั่วไป จะต้องได้รับการเอาใจใส่มากขึ้นกว่าเดิม เช่น อาจจำเป็นต้องมีการยึดอุปกรณ์ ไม่ว่าจะเป็นคอมพิวเตอร์ เครื่องพิมพ์ หรืออุปกรณ์อื่นๆ เหล่านั้นติดกับโต๊ะสำนักงาน เพื่อมิให้มีการเคลื่อนย้าย และป้องกันผู้ไม่หวังดีสามารถขโมยออกไปจากศูนย์ได้ เช่นบางศูนย์ปฏิบัติการ มีเครื่องคอมพิวเตอร์โน้ตบุ๊ค เครื่องพีดีเอ และอุปกรณ์ไร้สายต่างๆ ให้ใช้งาน โดยอุปกรณ์ดังกล่าวมีขนาดเล็ก บาง สามารถนำใส่ในกระเป๋า ถุง หรือย่ามได้ ดังนั้นควรมีการยึดอุปกรณ์เหล่านั้นไว้กับโต๊ะ ซึ่งอาจใช้วิธีการยึดด้วยสกรู หรือการใช้เชือกเหล็กคล้องกับโต๊ะและล็อคด้วยกลอนอีกชั้นหนึ่ง เพื่อมิให้ใครสามารถเคลื่อนย้ายอุปกรณ์ หรือลักขโมยไปได้

นอกจากนี้อุณหภูมิภายในศูนย์คอมพิวเตอร์จำเป็นต้องมีเครื่องปรับอากาศ เพื่อให้อากาศภายในมีอุณหภูมิในระดับที่พอเหมาะ เพราะความร้อนเป็นปัจจัยหนึ่งที่ส่งผลต่ออุปกรณ์อิเล็กทรอนิกส์หรือคอมพิวเตอร์ ให้มีอายุการใช้งานสั้นลง เนื่องจากอุณหภูมที่สูงเกินมาตรฐานอาจทำลายแผงวงจรไฟฟ้า และเกิดอาการลัดวงจรได้ ดังนั้นหากภายในห้องมีหน้าต่างหรือกระจกที่ทำให้สามารถรับแสงแดดมากเกินความจำเป็น ควรจะมีผ้าม่านเพื่อบังแดดซึ่งก็เป็นวิธีหนึ่งที่กระทำได้ไม่ยาก

สำหรับการป้องกันทางไฟฟ้าเป็นสิ่งที่ไม่ควรมองข้าม กระแสไฟฟ้าที่ไม่คงที่จะส่งผลต่ออุปกรณ์อิเล็กทรอนิกส์โดยตรง ดังนั้นจะเห็นได้ว่า ศูนย์คอมพิวเตอร์ส่วนใหญ่มักจะมีแหล่งจ่ายไฟที่มีตัวอุปกรณ์กรองสัญญาณไฟฟ้า ซึ่งอุปกรณ์ดังกล่าวจะช่วยปรับกระแสไฟฟ้าที่จ่าย

ไป ให้มีแรงดันทางไฟฟ้าอยู่ในระดับแรงดันที่เหมาะสม และยังป้องกันไฟตก ไฟกระชาก ซึ่งสิ่งเหล่านี้หากไม่มีมาตรการป้องกัน อุปกรณ์อิเล็กทรอนิกส์ต่างๆ อาจเสียหายได้ทันทีภายในพริบตา

ความปลอดภัยด้านกาปฏิบัติงาน (Operational Security)

ความปลอดภัยด้านการปฏิบัติงานบนเครือข่ายคอมพิวเตอร์ จะเป็นการพิจารณาด้วยการสร้างข้อจำกัดจของบุคคลใดบุคคลหนึ่งในการเข้าถึงระบบ ตัวอย่างเช่น ในองค์กรขนาดใหญ่ที่มีจำนวนพนักงานมากๆ จำเป็นต้องมีการกำหนดระดับการใช้งานของยูสเซอร์ทุกๆ ฝ่าย ตัวอย่างเช่น ยูสเซอร์หรือพนักงานที่ปฏิบัติงานในหน้าที่เกี่ยวกับการบันทึกข้อมูลของฝ่ายขาย ก็ไม่ควรให้ยูสเซอร์เหล่านั้นสามารถเข้าถึงข้อมูลเงินเดือนของฝ่ายการเงินในทำนองเดียวกัน ยูสเซอร์ระดับพนักงานที่ทำงานด้านเงินเดือนพนักงาน สามารถเข้าถึงฐานข้อมูลเงินเดือนได้แต่ไม่ใช่สามารถเข้าไปดูรายละเอียดหรือเปลี่ยนแปลงข้อมูลเงินเดือนได้ ซึ่งผู้ที่มีสิทธิในการเข้าถึงดังกล่าว ควรจะเป็นผู้จัดการฝ่ายการเงินเท่านั้น เป็นต้น ในขณะที่ผู้จัดการฝ่ายการเงิน หากต้องการเข้าถึงข้อมูลฝ่ายอื่นๆ ก็อาจมีข้อจำกัดในด้านการเข้าถึงข้อมูลเพียงระดับหนึ่ง ดังนั้น ผู้บริหารฐานข้อมูลหรือผู้บริหารเครือข่าย จะต้องปฏิบัติตามนโยบายด้านความปลอดภัย ด้วยการกำหนดระดับในการเข้าถึงข้อมูลของบุคคลต่างๆ ภายในบริษัท ตามที่ผู้บริหารระดับสูงได้กำหนดไว้

และด้วยเครือข่ายท้องถิ่นและระบบฐานข้อมูลนี้เอง จึงทำให้ง่ายต่อการกำหนดสิทธิการเข้าถึงข้อมูลได้อย่างยืดหยุ่นเลยทีเดียว โดยการกำหนดสิทธิการใช้งานให้กับยูสเซอร์นั้น จะเป็น การสร้างข้อจำกัดในการเข้าถึงระบบและไฟล์ข้อมูล ซึ่งทำให้เกิดความปลอดภัยด้านการปฏิบัติงานมากขึ้น และด้วยความสามารถของโปรแกรมระบบปฏิบัติการเครือข่าย สามารถที่จะทำการกำหนดสิทธิการใช้งานเป็นกลุ่มได้ ดังนั้น หากต้องการเปลี่ยนแปลงสิทธิเฉพาะกลุ่ม ก็สามารถกำหนดหรือยกเลิกสิทธิเฉพาะกลุ่มได้เพียงขั้นตอนเดียว ก็สามารถทำให้สมาชิกในกลุ่มเป็นไปตามที่กำหนดไว้ทั้งหมด ซึ่งกระบวนการดังกล่าวนำไปใช้ประโยชน์ได้มากในกรณีที่บริษัทมีพนักงานจำนวนมากประกอบด้วยหลายๆ ผ่าย หรือหลายแผนก นอกจากนี้ยังสามารถกำหนดวันเวลาการปฏิบัติงานของพนักงานได้ เช่น การกำหนดวันเวลาทำงานให้กับพนักงานระดับปฏิบัติการ สามารถเข้าถึงระบบได้เฉพาะวันเวลาทำการเท่านั้น ซึ่งพิจารณาจากรูปที่ 9.1 เป็นการกำหนดวันเวลาในการทำงานของพนักงาน ด้วยโปรแกรมบนระบบปฏิบัติการเครือข่าย Novell NetWare ซึ่งผลจากการกำหนดดังกล่าวจะส่งผลให้พนักงานสามารถเข้าถึงระบบได้ในช่วงเวลาที่กำหนดไว้เท่านั้น หากมีการเข้าถึงหรือล็อกอินเข้าสู่ระบบในวันเวลาที่นอกเหนือจากนั้น ก็จะไม่สามารถเข้าระบบได้

การตรวจตราเฝ้าระวัง (Surveillance)

ผู้บริหารเครือข่ายส่วนใหญ่ต้องมีกระบวนการตรวจตราเฝ้าระวัง เพื่อมิให้ระบบคอมพิวเตอร์ถูกทำลายหรือถูกลักขโมย ศูนย์ปฏิบัติการคอมพิวเตอร์บางศูนย์ ได้มีการติดตั้งกล้องโทรทัศน์วงจรปิดตามจุดสำคัญต่างๆ ในบริเวณห้อง ซึ่งทำให้สามารถตรวจตราเฝ้าระวังผ่านจอโทรทัศน์ตามบริเวณที่กล้องได้ติดตั้งอยู่ ทำให้สามารถสังเกตพฤติกรรม และเหตุการณ์ความเคลื่อนไหวของบุคคลภายในที่ต้องการลักลอบหรือขโมยข้อมูล ก็อาจจะต้องคิดหนัก หรือยากต่อการจัดการเนื่องจากทราบว่ามีกล้องคอยจับพฤติกรรมหรือเหตุการณ์อยู่ตลอดเวลา แต่วิธีนี้ก็ใช้งานได้ไม่ดีนักสำหรับในกรณีละเมิดสิทธิส่วนบุคคลได้ ทั้งนี้ก็คงต้องขึ้นอยู่กับความเหมาะสมและกฎหมายของแต่ละประเทศด้วย นอกจากการตรวจตราเพื่อเฝ้าระวังด้วยการใช้กล้องโทรทัศน์วงจรปิดแล้ว ยังมีวิธีอื่นๆ อีก เช่น การส่งสัญญาณไปยังเพจเจอร์เพื่อรายงานเหตุการณ์ฉุกเฉินไปยังเจ้าหน้าที่ทันที ในกรณีที่ห้องคอมพิวเตอร์ที่ได้ล็อคไว้ถูกเปิด เป็นต้น

การใช้รหัสผ่าน และระบบแสดงตัวตน (Passwords and ID Systems)

เกือบทุกระบบ ที่จะต้องมีการใช้รหัสผ่านก่อนเข้าสู่ระบบ รวมถึงรหัสผ่านสำหรับเรียกดูข้อมูลสำคัญๆ บางอย่าง การใช้รหัสผ่านเป็นมาตรการหนึ่งของความปลอดภัยขั้นพื้นฐานที่นิยมใช้กันมานาน แต่อย่างไรก็ตามรหัสผ่านที่เป็นความลับของบุคคลหนึ่ง อาจจะไม่ใช่ความลับอีกต่อไป หากรหัสผ่านนั้นผู้อื่นได้รับทราบ และนำไปใช้ในทางมิชอบ

ดังนั้น สำหรับหน่วยงานที่ต้องการระดับความปลอดภัยมากกว่าที่จะใช้รหัสผ่าน จึงได้มีระบบที่ใช้สำหรับแสดงตัวตน โดยใช้คุณสมบัติทางกายภาพของแต่ละบุคคลที่มีความแตกต่างกัน และไม่สามารถมีซ้ำหรือเลียนแบบกันได้ ซึ่งเรียกว่า **ไบโอเมตริก (Biometric Techniques)** เช่น ลายนิ้วมือ เลนส์ม่านตา เป็นต้น ซึ่งแต่ละบุคคลก็จะมีลายนิ้วมือ หรือเลนส์ม่านตาที่แตกต่างกัน

อย่างไรก็ตาม ระบบการใช้รหัสผ่าน ก็จัดได้ว่าเป็นระบบป้องกันที่มีการใช้งานอย่างแพร่หลาย เนื่องจากหากใช้ระบบแสดงตัวตนด้วยการใช้สแกนลายนิ้วมือ หรือเลนส์ม่านตานั้น อาจจำเป็นต้องมีกระบวนการที่ยุ่งยากและสิ้นเปลืองค่าใช้จ่าย ซึ่งเหมาะกับหน่วยงานที่ต้องการความปลอดภัยในกรณีพิเศษ นอกจากนี้การกำหนดรหัสผ่าน ยังมีกระบวนการปลีกย่อยต่างๆ เข้ามาควบคุมเพื่อสร้างข้อจำกัด (Password Restriction) เช่น การกำหนดอายุการใช้งานของรหัสผ่า การตั้งรหัสผ่านใหม่ทุกๆ กี่วัน การตั้งรหัสผ่านที่ต้องไม่ตรงกับชื่อ และการป้อนรหัสผ่านที่ผิดพลาดได้ไม่เกินจำนวนครั้งที่กำหนด เป็นต้น

การตรวจสอบ (Auditing)

การตรวจสอบระบบคอมพิวเตอร์ เป็นแนวทางหนึ่งที่ใช้งานอย่างได้ผลในกรณีป้องกันผู้ไม่หวังดีหรือก่อการร้าย ระบบการตรวจสอบส่วนใหญ่มักใช้ซอฟต์แวร์เพื่อตรวจสอบหรือเฝ้าระวังทุกๆ ทรานแซกชันที่เข้ามายังระบบโดยทรานแซกชันแต่ละทรานแซกชันจะมีการบันทึกเป็นหลักฐานไว้ในล็อกไฟล์ (Log File) ซึ่งมีรายละเอียดที่บันทึกไว้ เช่น วันที่ เวลา และเจ้าของทรานแซกชันหรือบุคคลที่เข้ามาใช้งาน สิ่งเหล่านี้ททำให้เราสามารถตรวจสอบย้อนหลังได้ ว่า ณ วันหนึ่งๆ มีทรานแซกชันจากที่ไหนได้พยายามเข้ามาในระบบ และเข้ามาเมื่อไร เวลาใด ทำให้เราสามารถสังเกตพฤติกรรมเจ้าของทรานแซกชันนั้นได้

การกำหนดสิทธิการใช้งาน (Access Rights)

ระบบคอมพิวเตอร์สมัยใหม่และเครือข่ายคอมพิวเตอร์ อนุญาตให้ยูสเซอร์มากกว่าหนึ่งคนเข้าถึงเพื่อใช้งานทรัพยากรที่มีอยู่ในระบบ เช่น ๆ ไฟล์ เทป เครื่องพิมพ์ และอุปกรณ์ต่อพ่วงอื่นๆ และหลายครั้งที่จำเป็นต้องมีการจำกัดสิทธิการใช้งานทรัพยากรบนเครือข่าย เช่น มีการกำหนดสิทธิการใช้งานของอุปกรณ์บางอย่างให้กับยูสเซอร์บางกลุ่ม หรือไฟล์ข้อมูลส่วนนี้ ฝ่ายปฏิบัติการสามารถอ่านได้อย่างเดียว และดูรายละเอียดได้บางอย่างเท่านั้น รวมถึงไม่สามารถเข้าไปแก้ไขข้อมูลในไฟล์นั้นได้ เป็นต้น สิ่งเหล่านี้เรียกว่า การกำหนดสิทธิการใช้งาน และโดยปกติผู้บริหารเครือข่ายจะเป็นผู้กำหนดอำนาจสิทธิการใช้งานของยูสเซอร์หรือกลุ่มยูสเซอร์ตามความเหมาะสม หรือปฏิบัติตามนโยบายของฝ่ายบริหารระดับสูง โดยการกำหนดสิทธิการใช้งานจะพิจารณาจากปัจจัยอยู่ 2 ปัจจัยด้วยกันคือ ใคร และ อย่างไร (Who and How) โดยที่

ใคร (Who)

หมายถึงควรกำหนดสิทธิการใช้งานให้กับใคร เช่น ควรกำหนดให้กับยูสเซอร์ หรือกลุ่มของยูสเซอร์แผนกใดบ้าง

อย่างไร (How)

หมายถึงเมื่อใครผู้นั้นได้สิทธิในการเข้าถึงทรัพยากร แล้วจะกำหนดให้เขาเข้าถึงข้อมูลได้อย่างไร เช่น อ่านได้อย่างเดียว เขียนบันทึกได้ แก้ไขได้ เพิ่มข้อมูลได้ สั่งพิมพ์ผ่านเครือข่ายได้ เป็นต้น

ตัวอย่างการกำหนดสิทธิการใช้งานให้กับยูสเซอร์หรือกลุ่มยูสเซอร์ใน Novell NetWare เช่น

w **Supervisor** มีสิทธิสูงสุดเทียบเท่าซูเปอร์ไว้เซอร์ หากมีการกำหนดสิทธินี้ให้กับใครแล้วสิทธิที่เหลือไม่จำเป็นต้องกำหนด

w **Red** มีสิทธิในการเปิดไฟล์อ่านข้อมูลได้

w **Write** มีสิทธิในการเปิดไฟล์และทำการบันทึกข้อมูลลงในไฟล์ได้

w **Create** มีสิทธิในการสร้างไฟล์ข้อมูล หรือสร้างไดเรกทอรีได้

w **Erase** มีสิทธิในการลบไฟล์ข้อมูล และลบได้เรกทอรีได้

w Modify มีสิทธิในการเปลี่ยนแอตตริบิวต์ของไฟล์หรือไดเรกทอรีได้

w File Scan มีสิทธิในการเห็นรายชื่อไฟล์และไดเรกทอรีย่อยต่างๆ ได้

w **Access Control** มีสิทธิในการเปลี่ยนแปลงแก้ไขสิทธิต่างๆ ของตนเองและผู้อื่นได้ แต่ไม่สามารถกระทำกับซูเปอร์ไวเซอร์ได้

การป้องกันไวรัส (Guarding Against Viruses)

ไวรัสคอมพิวเตอร์เป็นโปรแกรมขนาดเล็กที่จะเข้าไปแก้ไขเปลี่ยนแปลงการทำงานของคอมพิวเตอร์ ทำให้คอมพิวเตอร์ที่ใช้งานอยู่นั้นมีปัญหา ซึ่งปัญหาที่เกิดขึ้นจากไวรัสคอมพิวเตอร์ ก็จะแตกต่างกันไปตามลักษณะอาการของไวรัสแต่ละชนิดหรือแต่ละสายพันธ์ ไวรัสบางชนิดไม่ได้มุ่งทำร้ายข้อมูลแต่อย่างใด แต่จะสร้างความยุ่งยากและความรำคาญให้กับผู้ใช้ ด้วยการเข้าไปแก้ไขโปรแกรมที่ใช้งานให้ทำงานผิดเพี้ยนไปจากเดิม ในขณะที่ไวรัสบางตัวมุ่งทำร้ายข้อมูลโดยเฉพาะ ซึ่งผลของการกระทำของไวรัสประเภทนี้อาจส่งผลให้ระบบคอมพิวเตอร์เสียหายทันที สำหรับในปัจจุบันได้มีไวรัสหลายชนิดด้วยกัน เช่น มาโครไวรัส บูตเซกเตอร์ไวรัส หนอนไวรัส และโทร-จันเป็นต้น

จากการที่ไวรัสในปัจจุบันมีจำนวนมากมาย ดังนั้น คอมพิวเตอร์แทบทุกเครื่องจำเป็นต้องมีการติดตั้งโปรแกรมป้องกันไวรัสไว้ในเครื่องเพื่อตรวจจับไวรัสจากไฟล์ข้อมูลและโปรแกรมต่างๆ และที่สำคัญ ผู้ใช้จำเป็นต้องทำการอัปเดตโปรแกรมไวรัสเวอร์ชันใหม่ๆ อยู่เสมอ เพราะว่าในแต่ละวันจะมีไวรัสสายพันธ์ใหม่เกิดขึ้นอยู่ตลอดเวลา ดังนั้น การอัปเดตโปรแกรมป้องกันไวรัสจะทำให้โปรแกรมสามารถตรวจจับ และทำลายไวรัสชนิดใหม่ๆ ได้

เทคนิคพื้นฐานการเข้ารหัสข้อมูลและการถอดรหัสข้อมูล

(Basic Encryption and Decryption Techniques)

ทุกๆ ครั้งเมื่อมีการถ่ายโอนข้อมูลจากจุดหนึ่งไปยังจุดอื่นๆ ในเครือข่ายคอมพิวเตอร์ ต้องคำนึงถึงความมั่นใจด้านของความปลอดภัยของข้อมูล ที่จะต้องเดินทางไปยังกลุ่มเครือข่ายต่างๆ มากมาย ซึ่งความปลอดภัยในที่นี้ได้ครอบคลุมความหมายอยู่ 2 ประการด้วยกัน คือ

1. ในระหว่างการส่งข้อมูล จะต้องไม่มีใครคนใดที่จะสามารถเข้าไปลักลอบหรือสกัดข้อมูล และทำการคัดลอกข้อมูลไปใช้งาน

2. ในระหว่างการส่งข้อมูล จะต้องไม่มีใครคนใดที่จะสามารถเข้าไปเพิ่มเติม หรือเปลี่ยนแปลงข้อมูลต้นฉบับให้ผิดเพี้ยนไปจากเดิม

ข้อมูลหรือทรานแซกชันที่เกี่ยวกับการเงินการคลัง และทางทหาร จึงเป็นตัวอย่างที่ดีที่จะต้องได้รับความปลอดภัยในข้อมูลที่ส่งผ่านบนเครือข่าย ดังนั้น สายไฟเบอร์ออปติคจึงเป็นสายสัญญาณหลักที่มักนำมาใช้งาน เนื่องจากมีความปลอดภัย และยากต่อการลักลอบนำข้อมูลไปใช้งาน ในขณะที่สายทองแดงอย่างสายโคแอเชียลหรือสายคู่บิดเกลียว จะง่ายต่อการดักเพื่อลักลอบข้อมูลไปใช้งาน อย่างไรก็ตาม

เนื้อหาสาระต่อไปนี้คงไม่ใช่การกล่าวถึงตัวกลางส่งข้อมูลที่มีความปลอดภัย แต่จะกล่าวถึงการเข้ารหัสข้อมูล (Encrypt) ก่อนที่จะส่งไปยังปลายทาง โดยปลายทางที่ได้รับข้อมูลหากไม่มีรหัสที่ใช้สำหรับการถอดรหัสข้อมูล (Decrypt) ก็จะไม่สามารถนำข้อมูลเหล่านี้ไปใช้งานได้ ซึ่งเทคนิควิธีต่างๆ ที่ใช้สำหรับการเข้ารหัสข้อมูล และการถอดรหัสข้อมูลนี้เรียกว่า **ครพโตกราฟิ (Cryptography)** โดยแนวคิดพื้นฐานของคริพโตกราฟีก็คือ การจะจัดการกับข้อมูลข่าวสารนี้อย่างไร เพื่อให้อ่านไม่ออก หรืออ่านไม่รู้เรื่อง

คริพโตกราฟี เป็นทั้งศิลป์และศาสตร์ ที่ได้ราวมหลักการและกรรมวิธีของการแปลงรู้ (Transforming) ข้อมูลข่าวสารต้นฉบับ ให้อยู่ในรูปแบบของข้อมูลข่าวสารที่ได้ผ่านการเข้ารหัส และการนำข่าวสารนี้ไปใช้งาน จะต้องได้รับการแปลงรูปใหม่ (Retransforming) เพื่อให้กลับมาเป็นข้อมูลข่าวสารเหมือนต้นฉบับเดิม ดังนั้น หากผู้รับไม่มีรหัสที่ใช้สำหรับการถอดรหัสข้อมูลก็จะไม่สามารถนำข้อมูลเหล่านี้ไปใช้งานได้ เนื่องจากอ่านไม่รู้เรื่อง โดยศัพท์เทคนิคพื้นฐานที่เกี่ยวกับ คริพโตกราฟีประกอบด้วย

w เพลนเท็กซ์ หรือเคลียร์เท็กซ์ (Plaintext/Cleartext)

คือ ข้อมูลหรือข่าวสารต้นฉบับ ซึ่งหมายถึงข้อความภาษาที่มนุษย์สามารถอ่านแล้วเข้าใจ แล้วใครๆ ก็สามารถนำไปใช้ให้เกิดประโยชน์ได้

w อัลกอริทึมในการเข้ารหัส (Encryption Algorithm)

คือ อัลกอริทึมในโปรแกรมคอมพิวเตอร์ที่ใช้สำหรับการแปลงเพลนเท็กซ์ ให้อยู่ในรูปแบบข้อมูลที่ได้รับการเข้ารหัส

w ไซเฟอร์เท็กซ์ (Ciphertext)

คือ ข้อมูลหรือข่าวสารที่ได้รับการแปลงรูปหรือการเข้ารหัส ทำให้อ่านไม่รู้เรื่อง ดังนั้น เมื่อมีการนำไปเปิดอ่านก็จะไม่สามารถอ่านได้อย่างเข้าใจ และนำไปใช้ประโยชน์ไม่ได้

w คีย์ (Key)

เป็นกุญแจหรือคีย์เฉพาะที่ใช้ร่วมกับอัลกอริทึมในการเข้ารหัสเพื่อสร้างไซเฟอร์เท็กซ์ รวมถึงการถอดรหัสจากไซเฟอร์เท็กซ์กลับมาเป็นเพลนเท็กซ์

สำหรับเทคนิคหรือแนวทางในการเข้ารหัสข้อมูล เพื่อเปลองเพลนเท็กซ์ไปเป็นไซเฟอร์เท็กซ์ สามารถแบ่งออกได้เป็น 2 เทคนิควิธี คือ

1. เทคนิคการแทนที่ (Substitution Techniques)

2. เทคนิคการสับเปลี่ยน (Transposition Techniques)

เทคนิคการแทนที่ (Substitution Techniques)

สำหรับการแทนที่ มีอยู่หลายวิธีด้วยกัน โดยในที่นี้จะขอกล่าวถึง 2 วิธีด้วยกัน คือ การเข้ารหัสด้วยวิธีการแทนที่แบบ “ โมโนอัลฟาเบติค” และ “ โฟลีอัดฟาเบติค” โดยมีรายละเอียดดังต่อไปนี้

การเข้ารหัสด้วยวิธีการแทนที่แบบโมโนอัลฟาเบติค

(Monoalphabetic Substitution-Based Cipher)

เป็นเทคนิควิธีการเข้ารหัสข้อมูลอย่างง่าย ด้วยการใช้วิธีการแทนที่ข้อความหรืออักขระเดิมให้เป็นอีกข้อความหรือกัขระหนึ่ง ซึ่งได้มีการจับคู่ไว้เป็นที่เรียบร้อยแล้ว กล่าวคือ แต่ละตัวอักขระของเพลนเท็กซ์จะมีการจับคู่กับตัวอักขระที่ผ่านการไซเฟอร์

How about lunch at noon

ก็จะถูกเข้ารหัสเป็น

EGV POGNM KNHIE PH HGGH

วิธีดังกล่าว แต่ละตัวอักขระจะมีการจับคู่กันเสมอ ดังนั้น ตัวอักขระต่างๆ ก็จะมีคู่ของตนที่แน่นอน ซึ่งทำให้เกิดการซ้ำกันของตัวอักขระ เช่น เพลนเท็กซ์ที่เป็นตัวอักษร 0 เมื่อผ่านการเข้ารหัสก็จะเป็นตัวอักษร G ตลอดเป็นต้น อย่างไรก็ตาม การเข้ารหัสที่ดีก็ควรกำจัดช่องว่างออกไปด้วย เพื่อมิให้เห็นการแยกคำที่ชัดเจน

การเข้ารหัสด้วยวิธีแทนที่แบบโพลีอัลฟาเบติค

(Polyalphabetic Substitution-Based Cipher)

วิธีการเข้ารหัสแบบโมโนอัลฟาเบติคมีข้อเสียตรงที่มีการจับคู่แบบคงที่หรือตายตัว ทำให้ตัวอักขระซ้ำกันได้และง่ายต่อการถอดรหัส ดังนั้น จึงมีการนำมาปรับปรุงเป็นการเข้ารหัสด้วยวิธีโพลีอัลฟาเบติค ซึ่งวิธีนี้ความจริงมีความคล้ายคลึงกันแบบแรกมาก แต่จะมีความแตกต่างกันตรงที่จะมีคีย์เข้ามาเกี่ยวข้อง และจะใช้แมทริกซ์เข้าช่วย

เทคนิคการสับเปลี่ยน (Transposition Techniques)

เทคนิคการสับเปลี่ยนจะมีวิธีการเข้ารหัสที่แตกต่างจากเทคนิคการแทนที่ โดยจะมีประสิทธิภาพที่ดีกว่าเนื่องจากทำให้ไม่เกิดการซ้ำกันของตัวอักษร รวมถึงยากต่อการถอดรหัส ในที่นี้จะขอกล่าวเพียง 2 วิธีดังด้วยกัน คือ “ การเข้ารหัสด้วยวิธีการสับเปลี่ยนแบบเรลเฟ็นซ์” และ “ การสับเปลี่ยนแบบคอลัมน์” ดังรายละเอียดต่อไปนี้

การเข้ารหัสด้วยวิธีการสับเปลี่ยนแบบเรลเฟ็นซ์ (Rail Fence Transposition Cipher)

วิธีนี้เป็นการเข้ารหัสอย่างง่าย โดยจะเข้ารหัสในลักษณะ Row-by-Row หรืออาจเรียกวิธีนี้ว่า “ วิธีซิกแซ็ก”(Zigzag) ก็ได้ ตัวอย่าเช่น เพลนเท็กซ์คำว่า

Come home tomorrow

จะถูกเข้ารหัสเป็น

Cmemtmrooeoeoorw

การเข้ารหัสด้วยวิธีการสับเปลี่ยนแบบคอลัมน์ (Columnar Transposition Cipher)

วิธีนี้จะเป็นการเข้ารหัสที่มีประสิทธิภาพวิธีหนึ่ง โดยจะใช้ร่วมกับคีย์ที่กำหนดขึ้น เช่น ในที่นี้ได้กำหนดคำว่า COMPUTER เป็นคีย์ และด้วยคีย์ที่กำหนดขึ้นมานี้จะเห็นได้ว่าไม่มีตัวอักษรใดที่ซ้ำกันเลย การใช้เทคนิคการเข้ารหัสด้วยวิธีนี้ จะทำให้ตัวอักษรเดียวกันเมื่อผ่านการเข้ารหัสแล้วจะไม่มีการซ้ำกัน ทำให้ยากต่อการถอดรหัส

วิธีการขั้นแรกที่หลังจากมีการกำหนดคีย์เพื่อใช้งานแล้ว ให้กำหนดตำแหน่งลำดับของแต่ละคอลัมน์ขึ้นมาซึ่งปกตินิยมเรียงตำแหน่งตามลำดับของแต่ละตัวอักษร

จากนั้นให้นำเพลนเท็กซ์ที่ต้องการซึ่งในที่นี้คือ ประโยคคำว่า

“this is the best class I have ever taken”

มาเข้ารหัส ด้วยการนำมาเขียนตามลำดับ หากครบจำนวนคอลัมน์ก็ให้ปัดขึ้นเป็นบรรทัดใหม่

หลังจากที่ได้วางเพลนเท็กซ์ไปยังตำแหน่งคอลัมน์จนครบแล้ว ก็ดำเนินการเข้ารหัสตามคีย์ โดยจะอ่านตามลำดับของแต่ละคอลัมน์ ซึ่งคอลัมน์เบอร์ 1 จะได้ **TESV** ส่วนคอลัมน์เบอร์ 2 จะได้ **TLEE** ดังนั้นเพลนเท็กซ์ที่ได้เข้ารหัสเป็นไซเฟอร์เท็กซ์ก็จะได้

TESVTLEEIEIRHBSESSHTHAENSCVKITAA

และจากเทคนิควิธีการเข้ารหัสหลายๆ วิธีข้างต้น จะเห็นได้ว่าแต่ละวิธีก็จะมีอัลกอริทึมยากง่ายแตกต่างกันไป ดังนั้น ด้วยการนำเสอนตัวอย่างเทคนิควิธีการเข้ารหัสดังกล่าว คงทำให้ผู้ศึกษาสามารถนำไปประยุกต์ใช้เพื่อการเขียนโปรแกรมเข้ารหัสและถอดรหัสข้อมูลในระดับเบื้องต้นได้

การเข้ารหัสกุญแจสาธารณะ (Public Key Cryptography)

เทคนิคในการเข้ารหัสตั้งแต่ดั้งเดิมนั้น มักใช้อัลกอริทึมหรือกุญแจในการเข้ารหัสและถอดรหัสในตัวเดียวกันซึ่งเรียกวิธีนี้ว่า **ระบบการเข้ารหัสแบบซิมเมตริก (Symmetric Cryptosystems)** กล่าวคือจะมีกุญแจในการเข้ารหัสและถอดรหัสในตอกเดียวกันทั้งฝ่ายรับและฝ่ายส่ง แล้วลองคิดดูว่า หากมีผู้หนึ่งผู้ใดสามารถขโมยหรือนำกุญแจดอกนี้ไป ก็จะสามารถนำไปใช้ถอดรหัสข้อมูลของเราได้ เช่นเดียวกับกุญแจบ้านที่สามารถใช้ล็อคหรือเปิดประตูบ้านได้ หากมีใครขโมยกุญแจกดอกนี้ไป ก็จะสามารถเปิดประตูบ้านเราได้นั่นเอง และจำเป็นต้องมีดอกกุญแจมากขึ้นเมื่อมีกลอนประตูมากขึ้น ดังนั้นก็อาจทำให้เกิดความสับสนได้ว่า จะใช้กุญแจกแต่ละดอกในพวงกุญแจนี้ใช้สำหรับเปิดกับกลอนประตูใด ซึ่งเปรียบเสมือนกับเรา ที่มีการติดต่อส่งแมสเสจที่ผ่านการเข้ารหัสกับผู้อื่นยิ่งมากเท่าใดก็จำเป็นต้องมีคีย์ในการเข้ารหัสและถอดรหัสของแต่ละคนเพิ่มขึ้นเท่านั้นเอง

ในขณะที่อีกวิธีหนึ่งซึ่งเรียกว่า **ระบบการเข้ารหัสแบบอะซมเมตริก (Asymmetric Cryptosystems)** นั้นจะมีกุญแจอยู่เพียงสองดอก โดยกุญแจดอกแรกจะใช้สำหรับเข้ารหัส (Public Key) และกุญแจดอกที่สองจะใช้สำหรับการถอดรหัส (Private Key) และที่สำคัญ กุญแจที่ใช้เข้ารหัสจะนำมาถอดรหัสไม่ได้ วิธีนี้มักเรียกอีกชื่อหนึ่งว่า “ การเข้ารหัสกุญแจกสาธารณะ” โดยหลักการเข้ารหัสกุญแจกสาธารณะมีอยู่ว่า จะมีกุญแจกหรือคีย์อยู่สองดอกด้วยกันคือ **กุญแจสาธารณะ (Public Key)** และ **กุญแจส่วนตัว (Private Key)** ซึ่งกุญแจทั้งสองดอกนี้จะใช้งานควบคู่กันเสมอ โดยกุญแจสาธารณะจะเป็นกุญแจที่เจ้าของสามารถแจกจ่ายไปให้กับบุคคลใดๆ ที่ต้องการสื่อสาร ในขณะที่กุญแจส่วนตัว เจ้าของจะเก็บไว้ส่วนตัวไม่เผยแพร่ให้กับใคร

ลายเซ็นดิจิตอล (Digital Signatures)

ปัญหาหนึ่งจากการใช้เทคนิคการเข้ารหัสด้วยกุญแจสาธารณะนั้นก็คือ จะรับประกันได้อย่างไรว่าจดหมายที่ได้รับมานั้นจะมาจากผู้ส่งรายนั้นจริงๆ เนื่องจากว่าเราได้มีการส่ง Public Key นี้ให้กับบุคคลทั่วไปที่เราต้องการติดต่อ ดังนั้น จดหมายอิเล็กทรอนิกส์หรืออีเมลที่ส่งมา อาจมีการปลอมแปลงลายเซ็นว่ามาจากผู้นั้น ผู้นี้ ก็เป็นได้

การใช้เทคโนโลยีลายเซ็นดิจิตอลเพื่อเซ็นกำกับข่าวสารที่มากับอีเมลนั้น กำลังเป็นที่นิยมมากสำหรับการดำเนินธุรกิจบนเว็บ เช่น อีคอมเมิร์ซ โดยเฉพาะการโอนเงินผ่านเว็บซึ่งจำเป็นต้องมีระบบความปลอดภัยที่เชื่อถือได้เทคโนโลยีลายเซ็นดิจิตอลจะใช้เทคนิคการเข้ารหัสกุญแจสาธารณะเช่นเดียวกัน แต่จะใช้ในทางตรงกันข้าม

ที่มา : http://dit.dru.ac.th/task/network/topology.html

http://web.ku.ac.th/schoolnet/snet1/hardware/

http://www.burapaprachin.ac.th/network/index.htm

http://www. Nectec.or.th