บทที่ 4
การรักษาความปลอดภัยของเครือข่าย(Network Security)

ในบทนี้จะอธิบายถึงการรักษาความปลอดภัยของเครือข่าย โดยพิจารณาจากภัยคุกคามที่มีต่อระบบ การที่จะป้องกันข้อมูลที่ในอยู่ในเครือข่ายให้มีความถูกต้อง และเก็บรักษาข้อมูลนั้นให้เป็นความลับ ต้องอาศัยการควบคุมการอนุญาตให้เข้ามาในระบบ การตรวจสอบความถูกต้องของระบบคอมพิวเตอร์ในเครือข่าย การป้องกันการรั่วไหลของข้อมูลที่ถูกส่งผ่านในเครือข่าย การใช้ Firewall การใช้อุปกรณ์อื่น ๆ ในเครือข่ายเพื่อรักษาความปลอดภัย อีกทั้งการรักษาความปลอดภัยทางกายภาพ เช่น ระบบล๊อคแบบต่าง ๆ ก็เป็นส่วนสำคัญต่อการรักษาความปลอดภัยของเครือข่าย

4.1 พื้นฐานของระบบเครือข่ายคอมพิวเตอร์

ระบบเครือข่ายคอมพิวเตอร์นั้นจะประกอบไปด้วยคอมพิวเตอร์ที่มีอยู่ในระบบที่ทำการติดต่อสื่อสารกันโดยใช้อุปกรณ์สื่อสารผ่านสื่อต่าง ๆ ส่วนประกอบของระบบเครือข่ายนั้นมีทั้งที่เป็นฮาร์ดแวร์ และ ซอฟต์แวร์ มักจะมีการทำงานที่ค่อนข้างจะสลับซับซ้อน โดยปกติแล้วในการทำงานของระบบเครือข่ายคอมพิวเตอร์มีลักษณะต่อไปนี้คือ

4.1.1 โดยทั่วไปอุปกรณ์ที่ใช้ในการติดต่อเข้าสู่ระบบเครือข่ายนั้นมักจะเป็นเครื่องคอมพิวเตอร์ส่วนบุคคลหรือ Workstation ดังนั้นผู้ใช้จึงมักจะมีอุปกรณ์ที่มีขีดความสามารถค่อนข้างสูงในด้านของขนาดหน่วยความจำ(Storage) และการวิเคราะห์ข้อมูล(Processing Capability)

4.1.2 ระบบเครือข่ายนั้นมักจะไม่ได้มีเพียงแค่เครื่องไคลเอ็นต์ตัวหนึ่งที่เชื่อมต่อกับเซิร์ฟเวอร์อีกตัวหนึ่งเท่านั้น แต่มักจะประกอบด้วยไคลเอ็นต์หลายตัวที่เชื่อมต่อกับเซิร์ฟเวอร์อีกหลายตัว ดังนั้นระบบเครือข่ายจึงมักมีความสลับซับซ้อนค่อนข้างมาก

4.1.3 การใช้งานของระบบเครือข่ายนั้นมักจะมีระบบคอมพิวเตอร์หลาย ๆ ตัว มาช่วยกันทำงานเพื่อตอบสนองความต้องการในการใช้ระบบเครือข่ายจากผู้ใช้

4.1.4 โดยทั่วไปในขณะใช้งานในระบบเครือข่ายนั้น ผู้ใช้มักจะไม่รู้ถึงปริมาณในการติดต่อสื่อสารที่ใช้ และปริมาณการวิเคราะห์ข้อมูลที่ใช้โดยผ่านระบบเครือข่ายนั้นๆ เพราะระบบเครือข่ายมักถูกออกแบบมาเพื่อความสะดวกและง่ายต่อการใช้งานแก่ผู้ใช้

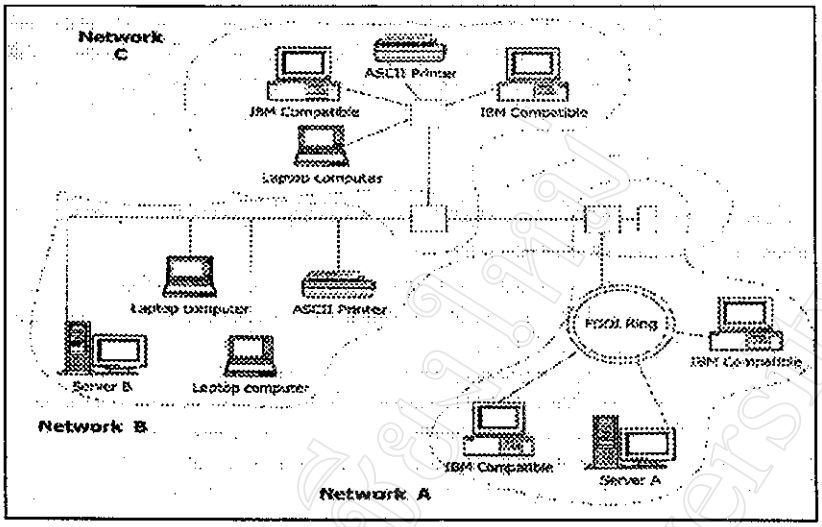
4.2 ภัยคุมคามที่มีต่อระบบเครือข่าย(Threats in Network)

การที่ระบบเครือข่ายเป็นระบบเปิดที่ถูกออกแบบมาให้นั้นมีใช้จำนวนมาก สามารถใช้งานร่วมกันได้และมีระบบการจัดการระบบที่สลับซับซ้อน ดังนั้นจึงมีจุดอ่อนอยู่หลายจุดในการรักษาความปลอดภัยของระบบดังนี้

4.2.1 การใช้งานร่วมกัน(Sharing) ก่อให้เกิดปัญหาในการจัดการที่เกี่ยวกับการให้อนุญาตแก่ผู้ใช้ภายในระบบ เพราะหากไม่มีการจัดการระบบที่ดีแล้วก็อาจมีการแอบเข้ามาใช้ระบบโดยไม่ได้รับอนุญาต ซึ่งจะก่อให้เกิดความเสียหายในเชิงธุรกิจ และการรักษาความลับของข้อมูล

4.2.2 ความสลับซับซ้อนของระบบ(Complexity) เนื่องจากว่าระบบเครือข่ายนี้เกิดจากการนำเอาระบบปฏิบัติการ (Operating System)จากคอมพิวเตอร์หลายตัวมาทำงานร่วมกัน หรืออาจเกิดจากการนำเอาระบบปฏิบัติการหลายชนิดมาทำงานร่วมกัน ก่อให้เกิดความยุ่งยากในการจัดการกับการรั่วไหลของข้อมูลจากระบบที่สลับซับซ้อนได้ อนึ่งระบบปฏิบัติการโดยทั่วไปนั้นก็มิได้ออกแบบมาเพื่อการรักษาความปลอดภัยที่สูงสุดของข้อมูล จึงมีปัญหาในตัวของมันเองในด้านการรักษาความปลอดภัยของข้อมูลในระบบ ดังนั้นหากนำระบบปฏิบัติการหลายตัวมาทำงานร่วมกัน อาจก่อให้เกิดความไม่ปลอดภัยในการรักษาความปลอดภัยของข้อมูลได้มากยิ่งขึ้น

4.2.3 การกำหนดพารามิเตอร์หรือตัวแปรของระบบเครือข่ายที่ไม่แน่นอน เนื่องจากความง่ายในการเพิ่มเติมและขยายระบบเครือข่าย ดังนั้นจึงเป็นการยากที่จะกำหนดขอบเขตและผู้ใช้ที่แน่นอนภายในระบบเครือข่ายได้ ผลก็คือการกำหนดขอบเขตและเป้าหมายที่แน่นอนในการรักษาความปลอดภัยของข้อมูลภายในระบบเครือข่ายนั้นสามารถทำได้ยากขึ้น ตัวอย่างของระบบเครือข่ายหลายเครือข่ายที่เชื่อมต่อกันโดยมิอาจกำหนดขอบเขตความแน่นอนได้นั้นอาจดูได้จากภาพที่ 15



ภาพที่ 15 แสดงรูปแบบของเครือข่ายคอมพิวเตอร์[42]

จากรูปจะเห็นได้ว่าระบบเครือข่าย A นั้นจะรู้ว่าเชื่อต่อกับระบบเครือข่าย B เท่านั้น แต่จะไม่รู้ว่าระบบเครือข่าย C นั้นอาจทำการเข้ามาทำการเชื่อมต่อได้อีกโดยผ่านระบบเครือข่าย B ดังนั้นผลที่เกิดขึ้นก็คือ ผู้ที่ไม่ได้รับอนุญาตอาจแอบเข้ามาในระบบได้โดยวิธีนี้ โดยที่เครือข่าย A นั้นอาจเข้าใจผิดว่าเป็นผู้ใช้ที่ถูกต้องที่ได้รับอนุญาตจากระบบเครือข่าย B

4.2.4 มีจุดอ่อนอยู่หลายจุดภายในระบบเครือข่าย เนื่องจากระบบเครือข่ายนั้นมีระบบคอมพิวเตอร์อยู่มากมาย ทำให้ผู้ดูแลระบบเครือข่ายไม่สามารถที่จะควบคุมดูแลผู้ที่เข้ามาใช้ทรัพยากรในระบบได้อย่างทั่วถึง เพราะการอนุญาตให้ผู้ใช้เข้ามาในระบบได้นั้น ต้องอาศัยระบบปฏิบัติงานและการควบคุมทุก ๆ ส่วนของระบบเครือข่ายนั้นทำได้ยาก

4.2.5 ไม่สามารถรู้ถึงผู้ที่เข้ามาใช้ระบบเครือข่าย(Anonymity) เนื่องจากระบบเครือข่ายคอมพิวเตอร์ในปัจจุบันได้มีการต่อเชื่อมกันเกือบทั่วทั้งโลก ดังนั้นผู้ใช้ที่มาใช้ระบบอาจมาจากสถานที่ ๆ ห่างไกลนับร้อยนับพันกิโลเมตรออกไป โดยทำการเข้ามาในระบบโดยผ่านเครือข่ายอื่น ๆ หลายเครือข่ายที่มีการต่อเชื่อมกันทางอิเล็กทรอนิกส์ การอนุญาตให้เข้ามาใช้ระบบผ่านทางเครือข่ายได้นั้นมักจะอาศัยการตรวจสอบระบบคอมพิวเตอร์ด้วยกันเองที่เรียกว่า Computer-To-Computer Authentication ซึ่ง

---

[42] ณรงค์ชัย นมิตบุญอนันต์. **Computer Security for E-Commerce.** กรุงเทพ : บริษัทซีเอ็ดยูเคชั่น จำกัด (มหาชน), 1999 : 169.

ต้องมีการจัดการและควบคุมที่ดี มิฉะนั้นแล้วอาจเกิดการแอบเข้ามาในระบบโดยไม่ได้รับการอนุญาตได้โดยง่าย

4.3 การวิเคราะห์ความเสี่ยงด้านความปลอดภัยในระบบเครือข่าย (Security Threats Analysis)

4.3.1 ส่วนประกอบที่ต้องคำนึงถึง

ส่วนประกอบของระบบเครือข่ายภายในองค์กรที่จะต้องคำนึงถึง และต้องมีการตรวจสอบควบคุมเกี่ยวกับการรักษาความปลอดภัยของข้อมูลมีดังต่อไปนี้คือ

(1) ระบบเครือข่ายย่อยเฉพาะที่(Local Nodes)

(2) ระบบสื่อสารที่ใช้ต่อเชื่อมระบบเครือข่ายย่อย(Local communications)

(3) ระบบเครือข่ายขนาดเล็ก(Local Area Network - LAN)

(4) หน่วยเก็บข้อมูลเฉพาะที่(Local Data Storage)

(5) การทำงานและการวิเคราะห์ข้อมูลภายในระบบเครือข่ายขนาดเล็กโดยโปรแกรมต่าง ๆ

(6) อุปกรณ์ต่างๆ ภายในระบบเครือข่ายขนาดเล็ก(Local Devices)

(7) ระบบต่อเชื่อมเข้ากับเครือข่ายอื่นๆ(Network Gateway)

(8) ระบบสื่อสารที่ต่อเชื่อมเข้ากับเครือข่ายอื่นๆ(Network Communications Links)

(9) ระบบการควบคุมทรัพยากรของระบบเครือข่าย(Network control Resources)

(10)ระบบการส่งต่อ และแจกจ่ายข้อมูลของระบบเครือข่าย(Network Routers)

(11)ทรัพยากรต่างๆ ของระบบเครือข่าย(Network Resources) เช่นระบบฐานข้อมูล (Databases)

4.3.2 อันตรายที่อาจเกิดขึ้น

ในส่วนต่าง ๆ ของระบบเครือข่ายที่ได้กล่าวมาแล้วนี้ จะมีสิ่งที่อาจเกิดขึ้นได้ที่อาจสร้างความไม่ปลอดภัยให้กับข้อมูลภายในระบบ คือ

(1) การขโมยข้อมูลระหว่างการส่ง(Interception of data in transit)

(2) การเข้าไปใช้โปรแกรมและข้อมูลในระบบโดยไม่ได้รับอนุญาต(Unauthorized usage of programs or data at remote hosts)

(3) การเข้าไปเปลี่ยนแปลงแก้ไขโปรแกรมหรือข้อมูลในระบบโดยไม่ได้รับอนุญาต (Unauthorized modifications of programs or data at remote hosts)

(4) การแอบเปลี่ยนแปลงแก้ไขข้อมูลในระหว่างการส่ง(Modification of data in transit)

(5) การปลอมแปลงโดยการแอบบันทึกการสื่อสารแล้วนำกลับมาใช้ใหม่(Insertion of a repeat of a previous communication)

(6) การป้องกันการสื่อสารบางอย่าง(Blocking of selected traffics)

(7) การป้องกันการสื่อสารทั้งหมด(Blocking of all traffics)

(8) การส่งโปรแกรมเข้าไปทำงานในระบบโดยไม่ได้รับอนุญาต

4.3.3 วิธีการในการขโมยข้อมูลหรือรบกวนระบบ

การล้วงความลับหรือการรบกวนระบบเครือข่ายนั้น อาจทำได้หลายวิธี คือ

(1) การแอบดักจับสัญญาณ(Wire Tapping)

- สายเคเบิล(Cable) สามารถที่จะถูกลักขโมยสัญญาณได้โดยง่าย เช่น การใช้วิธีที่สามารถจะตรวจจับสัญญาณที่ถูกส่งผ่านสายเคเบิลได้โดยที่ไม่ต้องมีการสัมผัสกับสายเคเบิล เพียงแต่ให้อยู่ใกล้กับสายเคเบิลเท่านั้น เพราะการดักจับสัญญาณแบบนี้อาศัยการแผ่สนามแม่เหล็กไฟฟ้าจากสายเคเบิลนั้นเอง ดังนั้นจึงเป็นการยากที่จะป้องกันการขโมยสัญญาณได้หากสายเคเบิลนั้นใช้ส่งสัญญาณในระยะทางไกล ยังมีวิธีการอีกวิธีหนึ่งที่อาจนำมาใช้ในการขโมยข้อมูลจากสายเคเบิลไปได้นั้นคือวิธี Packet Sniffer ซึ่งใช้ Board ปลอมที่ถูกโปรแกรมมาเพื่อให้ส่งสัญญาณ Address ปลอมและขโมยข้อมูลที่อยู่ในรูป Packets Data ไป วิธีการนี้มักใช้ได้กับระบบเครือข่ายที่มี Address เฉพาะตัวที่ฝังอยู่บนตัวของมันเอง เช่น Ethernet Card ในระบบ LAN เป็นต้น
- สัญญาณไมโครเวฟ(Microwave) เป็นสัญญาณที่ถูกส่งออกไปในอากาศในลักษณะที่เป็นช่องสัญญาณ (Beam)ที่มีความกว้างไม่มากนัก แต่ในระหว่างการส่งนั้นอาจมีตัวรับสัญญาณปลอมมาดักรับสัญญาณในระหว่างการส่งได้
- สัญญาณผ่านดาวเทียม(Satellite Communications) เนื่องจากสัญญาณที่ถูกส่งมาจากดาวเทียมลงสู่พื้นโลกนั้น มักมีความกว้างของสัญญาณมาก จึงง่ายต่อการลักลอบขโมยสัญญาณ
- สายใยแก้วนำแสง(Optical Fiber) เป็นการส่งสัญญาณโดยใช้แสงเป็นตัวนำสัญญาณผ่านเส้นใยแก้ว วิธีการนี้ยากแก่การดักจับสัญญาณมากกว่าการใช้สายเคเบิลมาก เพราะสัญญาณแสงจะไม่ส่งสนามแม่เหล็กออกมาภายนอกเส้นใยแก้ว ดังนั้นการดักจับสัญญาณนี้จึงไม่สามารถทำได้โดยการใช้วิธีการดึงสนามแม่เหล็กออกมา ข้อดีที่สำคัญอีกประการหนึ่งในการใช้เส้นใยแก้วนำแสงก็คือหากมีการขโมยแบ่งสัญญาณแสงออกไปจากเส้นใยแก้วโดยตรงก็จะง่ายต่อการตรวจจับเพราะระดับความเข้มของแสงจะเปลี่ยนไปจนเป็นที่

สังเกตได้ แต่อย่างไรก็ตามวิธีการนี้ก็ไม่ปลอดภัยเลยเสียทีเดียว เพราะอาจมีการขโมยสัญญาณได้ ณ ที่ช่วงต่อของสายเส้นใยแก้วนำแสงได้ และหากเครื่องมือที่ใช้มีความละเอียดสูงพอ และได้รับการออกแบบมาอย่างดี ก็จะทำให้ยากแก่การตรวจจับเป็นอย่างยิ่ง

(2) การปลอมแปลงเป็นผู้ใช้ (Impersoantor)

การขโมยข้อมูลโดยการแอบดักจับสัญญาณนั้นเป็นสิ่งที่ทำได้ง่าย ยังมีอีกวิธีหนึ่งที่อาจทำได้และสามารถที่จะสร้างความเสียหายได้มากกว่านั้นคือการปลอมแปลงเป็นผู้ใช้เข้ามาในระบบ และเมื่อเข้ามาในระบบได้แล้วก็อาจแอบลักขโมยข้อมูลไปได้มากเท่าที่ต้องการตามสิทธิที่กำหนดไว้ของผู้ใช้นั้นๆ วิธีการที่ใช้มีหลายวิธี คือ

- การทำลายระบบตรวจความถูกต้องของผู้ใช้โดยการเดาสุ่มรหัสผ่าน คือการเดาสุ่มรหัสผ่านที่ผู้ใช้อาจใช้ เนื่องจากเป็นคำที่สามารถจำได้ง่าย และใช้กันอยู่ทั่วไป เช่น ชื่อหรือนามสกุลของผู้ใช้เอง หรือชื่อของดารา หรือนักร้องยอดนิยม เป็นต้น
- การทำลายระบบตรวจสอบความถูกต้องของผู้ใช้โดยการแอบขโมยรหัส เป็นวิธีการแอบขโมยรหัสผ่านจากผู้ใช้โดยที่ผู้ใช้อาจไม่รู้ตัว เช่น การแอบดูผู้ใช้ขณะทำการ Log-In เข้าสู่ระบบเครือข่าย
- การแอบเข้ามาในระบบโดยการหลบเลี่ยงระบบตรวจสอบความถูกต้องของผู้ใช้ เนื่องจากว่าบางครั้งระบบปฏิบัติการที่ใช้ในระบบเครือข่ายถูกออกแบบมาไม่ดี หรือไม่ได้รับการใช้งานอย่างถูกต้อง จึงทำให้ผู้ไม่หวังดีอาจเข้ามาในระบบโดยอาศัยจุดอ่อนเหล่านี้ได้
- การไม่มีระบบตรวจสอบผู้ใช้ จะทำให้ผู้ไม่ประสงค์ดีสามารถที่จะเข้ามาใช้ระบบได้โดยง่าย

(3) การทำลายความลับของข้อมูล (Message confidentiality Violations)

- การขนส่งข้อมูลที่ผิดพลาด(Misdelivery) เนื่องจากความผิดพลาดของระบบเครือข่ายคอมพิวเตอร์ หรือ อาจเกิดจากการให้ที่อยู่ Address ของผู้รับผิดพลาด
- การเปิดเผยข้อมูลโดยไม่ตั้งใจในระหว่างการส่ง(Message Exposure) เช่น การที่ข้อมูลถูกส่งผ่านอุปกรณ์ต่าง ๆ ภายในระบบเครือข่าย เช่น Routing

Devices, Switching Devices, หรือ Gateways เป็นต้น ข้อมูลเหล่านี้อาจถูกแอบขโมยข้อมูลไปในระหว่างการส่งผ่านอุปกรณ์เหล่านี้ได้

- การวิเคราะห์การส่งข้อมูล(Traffic Flow Analysis) บางครั้งความลับของข้อมูลก็ไม่ได้อยู่ที่ว่าข้อมูลนั้นบรรจุอะไรอยู่บ้าง แต่ความลับของข้อมูลบางอย่างอยู่ที่ว่าข้อมูลนั้นถูกส่งไปที่ใดและมีปริมาณมากน้อยเท่าใด และถูกส่งออกไป ณ เวลาใดบ้าง

(4) การทำลายความถูกต้องของข้อมูล(Message Integrity Violations) หรือเป็นการปลอมแปลงข้อมูลโดยการเปลี่ยนแปลงแก้ไขบางส่วนของข้อมูล หรือทั้งหมดของข้อมูล เช่น

- การเปลี่ยนส่วนประกอบของข้อมูล
- การเปลี่ยนแปลงข้อมูลทั้งหมด
- การแอบใช้ข้อมูลเก่า ๆ เพื่อเป็นการลวง
- การแอบเปลี่ยนสิ่งที่บอกที่มาของข้อมูล
- การแอบส่งข้อมูลไปสู่เป้าหมายอื่น ๆ
- การทำลายข้อมูลโดยตรง

(5) การโจมตีจากพวกนักเจาะระบบ พวกนี้เป็นพวกที่มีทักษะทางด้านคอมพิวเตอร์สูง สามารถที่จะทำการพัฒนาโปรแกรมต่าง ๆ ที่อาจนำมาใช้ในการขโมยข้อมูลหรือทำลายข้อมูลได้ บางครั้งพวกนี้จะอาศัยความผิดพลาดที่มีอยู่แล้วในระบบแล้วทำการแอบเข้ามาในระบบโดยอาศัยข้อบกพร่องเหล่านี้

(6) ความไม่ปลอดภัยจากตัวโปรแกรมเอง(Code Integrity) ปัญหาที่สำคัญประการหนึ่งของโปรแกรมที่ได้มาจากการ Download มาจากระบบเครือข่ายก็คือ อาจมีโปรแกรมมหาภัยแอบแฝงมาด้วย โปรแกรมพวกนี้มักจะเป็น Executable Code ที่พร้อมจะทำงานในการโจมตีระบบคอมพิวเตอร์ทันทีที่มีโอกาส

(7) การทำให้ระบบไม่สามารถทำงานที่เป็นประโยชน์ได้(Denial of Service) ในระบบเครือข่ายนั้นมีจุดอ่อนอยู่หลายจุดที่ง่ายต่อการโจมตี เพราะเป็นระบบที่ใหญ่และกระจัดกระจายกันอยู่ทั่วไป โดยทั่วไปแล้วสิ่งที่ต้องคำนึงถึงในการรักษาความปลอดภัยให้แก่ระบบเครือข่ายคือ

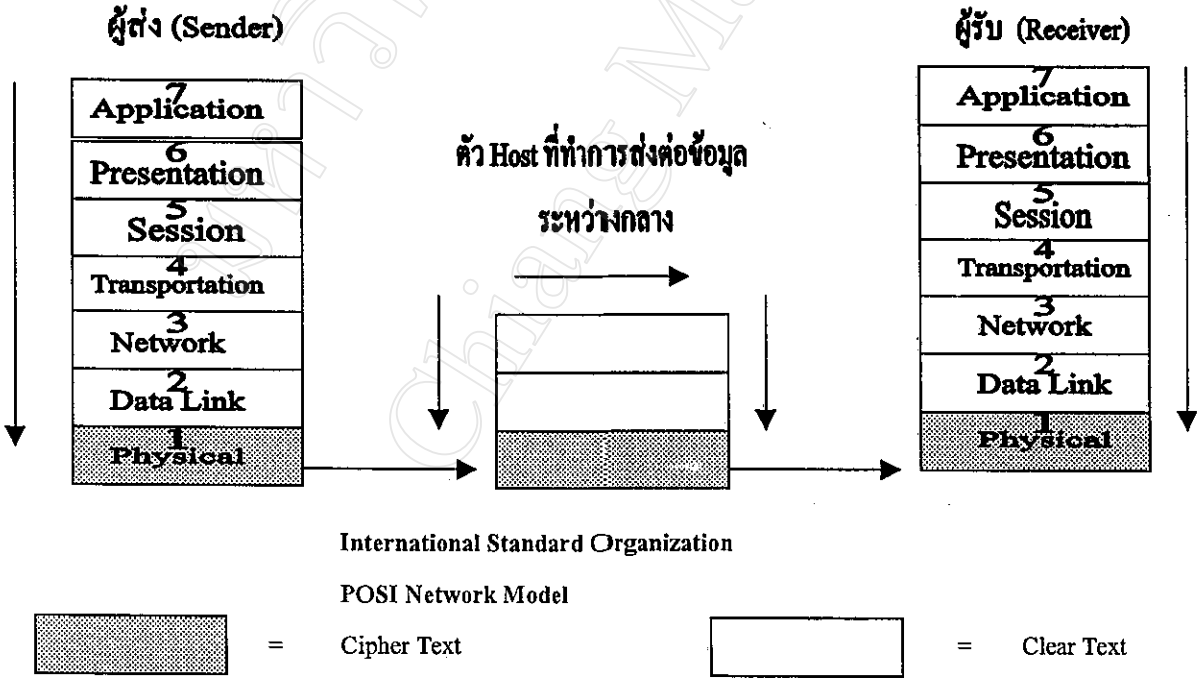
- การรบกวนที่จุดเชื่อมต่อระบบ(Connectivity) ระบบเครือข่ายเป็นระบบที่มีจุดเชื่อมต่ออยู่มากมาย โดยปกติแล้วหากจุดเชื่อมคือแต่ละจุดใดที่ไม่สามารถทำงานได้ การส่งข้อมูลก็อาจเปลี่ยนไปใช้จุดอื่นๆ แต่อย่างไรก็ตาม จุดที่สำคัญ(Critical Point) ของระบบนั้นต้องได้รับการปกป้อง และใช้งานอย่างถูกต้อง มิฉะนั้นก็จะเกิดการ Block ระบบไม่ให้ทำงานได้ตามปกติ
- Flooding วิธีที่ง่ายที่สุดวิธีหนึ่งที่สามารถนำมาใช้ในการรบกวนการทำงานของระบบก็คือ การเพิ่มปริมาณการทำงานของระบบให้มากขึ้นจนเกินขีดความสามารถของระบบ(Overloading) โดยที่ปริมาณงานที่เพิ่มขึ้นนี้อาจไม่ใช่งานที่เป็นประโยชน์ก็ได้ ดังนั้นผลก็คือระบบเครือข่ายไม่มีเวลา และทรัพยากรเพียงพอที่จะใช้ในการทำงานที่เป็นประโยชน์ได้
- Routing Problems ในระบบเครือข่ายนั้นจะมีส่วนที่เรียกว่า Routing Table ภายในตัว Host หรือ ส่วนที่เรียกว่า Router อยู่ภายในระบบเครือข่าย เพื่อที่จะเอาไว้ใช้ในการส่งข้อมูลไปยังที่ต่าง ๆ ให้ถูกต้องตามที่อยู่ของข้อมูลนั้น ๆ แต่หากข้อมูลที่อยู่ใน Routing Table หรือ Router นี้เกิดถูกทำลายหรือ เปลี่ยนแปลงแก้ไขโดยผู้ไม่ประสงค์ดีแล้ว ก็จะทำให้การสื่อสารข้อมูลภายในระบบเกิดความผิดพลาดขึ้นมาอย่างมหาศาล และทำให้ระบบเครือข่ายนั้น ๆ ไม่สามารถทำงานได้ตามปกติ

4.4 การรักษาความปลอดภัยในระบบเครือข่าย

การรักษาความปลอดภัยในระบบเครือข่ายนั้นจะต้องทำให้ทั่วถึงทั้งระบบ จะทำเฉพาะจุดใดจุดหนึ่งไม่ได้ สิ่งที่ต้องควบคุมก็คือความลับของข้อมูลที่ถูกส่งผ่านในระบบเครือข่าย และการตรวจสอบความถูกต้องของผู้ใช้ รวมถึงการตรวจสอบความถูกต้องของระบบคอมพิวเตอร์ที่จะเข้ามาทำการเชื่อมต่อเข้าสู่ระบบเครือข่าย สิ่งที่ต้องนำมาใช้ในการพิจารณาสามารถที่จะแยกออกเป็นส่วนต่าง ๆ ดังนี้

4.4.1 การเข้ารหัสข้อมูล(Encryption) เป็นวิธีที่มีประโยชน์เป็นอย่างสูงในการรักษาความปลอดภัยของข้อมูลในระบบเครือข่าย ชุดของข้อมูล(Datagram)ที่ถูกส่งผ่านระบบเครือข่ายนี้มีส่วนประกอบอยู่สองส่วนคือ ส่วนที่เป็นข้อมูลจากผู้ใช้หรือโปรแกรมต่าง ๆ (Message) และส่วนที่เป็นข้อมูลที่ใช้เป็น Headers เพื่อใช้บอกว่าข้อมูลนั้นจะถูกส่งไปที่ไหนอย่างไร และใช้กับโปรแกรมอะไรในส่วนใดบ้าง

(1) Link Encryption เป็นการเข้ารหัสข้อมูลก่อนการส่งข้อมูลออกไปสู่ระบบเครือข่าย หากดูจากมาตรฐาน OSI แล้ว จะเห็นได้ว่าการเข้ารหัสข้อมูลแบบนี้จะทำในระดับขั้นที่ 1 หรือในระดับขั้นที่ 1 กับ 2 เท่านั้น

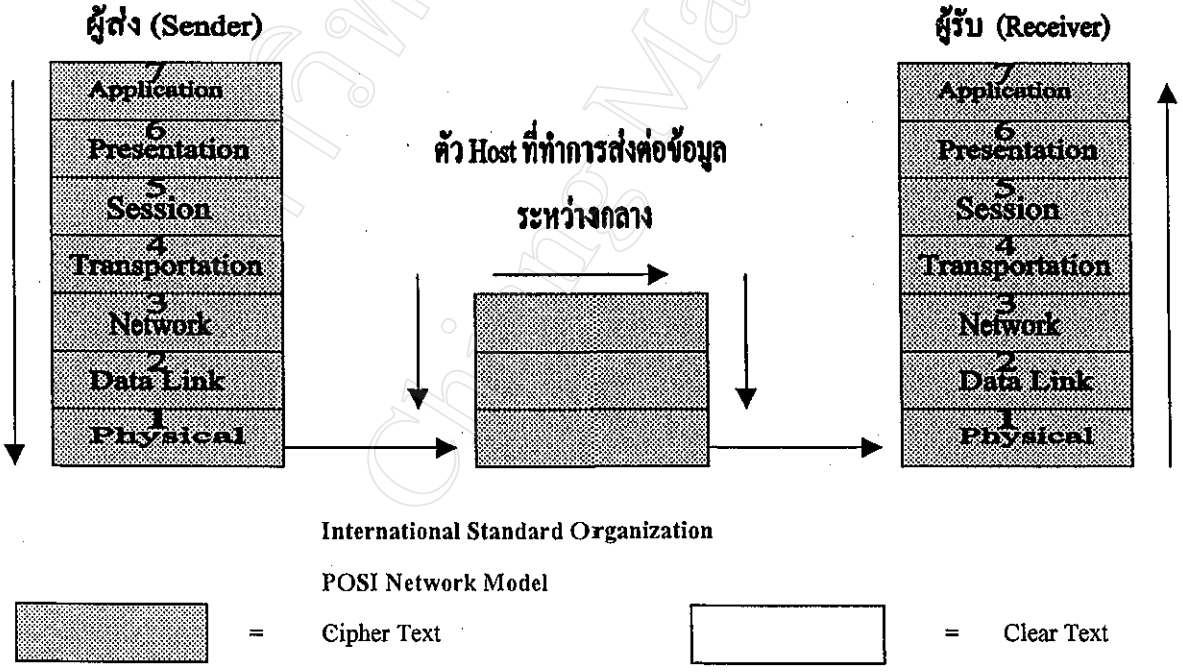


ภาพที่ 16 แสดงการส่งผ่านข้อมูลโดยวิธี Link Encryption[43]

[43] ณรงค์ชัย นิมิตบุญอนันต์. "วิเคราห์การเจาะระบบเครือข่าย". BCM. (ธันวาคม 1999) : 130.

จากภาพที่ 16 จะเห็นได้ว่าหากข้อมูล Message รวมทั้ง Headers อยู่ต่ำกว่าระดับชั้นที่ 2 นั้น ข้อมูลทุกอย่างจะถูกทำการเข้ารหัสหมด และเมื่อข้อมูลถูกส่งออกไปสู่ระบบเครือข่ายผ่านทางสื่อในระดับ Physical Level แล้วก็จะถูกส่งต่อไปยังจุดหมายปลายทางโดยตัว Router หรือ Host ที่อยู่ระหว่างกลางในระบบเครือข่าย แต่ก่อนที่จะทำการส่งต่อออกไปได้นั้น ตัว Router หรือ Host นี้จะต้องทำการอ่านข้อมูลที่เกี่ยวกับการส่งหรือที่อยู่ Address รวมทั้งตรวจสอบความถูกต้องในการส่งด้วย ดังนั้นจึงต้องทำการถอดรหัสข้อมูลเหล่านี้ และทำการอ่านค่าก่อนที่จะทำการเข้ารหัสข้อมูลอีกครั้งหนึ่ง แล้วส่งต่อไปยังจุดหมายปลายทางต่อไป หากตรวจสอบดูข้อมูลที่ถูกส่งออกไปสู่ระบบเครือข่ายโดยวิธี Link-To-Link Encryption นี่แล้วจะพบว่าข้อมูลรวมทั้ง Headers เกือบทั้งหมดนั้น จะถูกทำการเข้ารหัสข้อมูล

(2) End-To-End Encryption เป็นการเข้ารหัสข้อมูลที่ให้ความปลอดภัยสูงกว่าแบบแรก เพราะข้อมูลนั้นจะถูกทำการเข้ารหัสข้อมูลตั้งแต่ชั้นสูงสุดนั้นคือตั้งแต่ระดับชั้นที่ 7 การเข้าข้อมูลในลักษณะนี้นั้น ข้อมูลที่เป็น Headers ไม่จำเป็นต้องมีการทำการเข้ารหัสข้อมูล เพราะความลับของข้อมูลได้รับการปกป้องแล้วจากระดับชั้น OSI ที่อยู่สูงกว่าแล้ว



ภาพที่ 17 แสดงการส่งผ่านข้อมูลโดยวิธี End-To-End Encryption[44]

[44] เรื่องเดียวกัน : 131.

จากภาพที่ 17 จะเห็นได้ว่าข้อมูลนั้นจะอยู่ในรูป Cipher Text ตลอดเวลาตั้งแต่จุดเริ่มต้นไปจนถึงจุดหมายปลายทาง และในระหว่างการส่งผ่านระบบเครือข่ายนั้น ข้อมูล Message จะไม่ถูกทำการถอดรหัสเลย วิธีการนี้จึงให้ความปลอดภัยที่สูงกว่า

4.5 การควบคุมการอนุญาตให้เข้ามาในระบบ(Access Control)

วิธีการเข้ารหัสข้อมูลนั้นสามารถที่จะนำมาใช้ในการปกป้องความลับของข้อมูลได้เป็นอย่างดี แต่ไม่สามารถที่จะป้องกันการปลอมแปลงเข้ามาในระบบได้ วิธีการที่ใช้ในการป้องกันการปลอมแปลงเข้ามาในระบบเรียกว่าระบบ Access control Mechanisms สิ่งที่จะต้องคำนึงถึงในการทำ Access control ก็คือ

4.5.1 Port Protection คือการป้องกันการเข้ามาในระบบโดยผ่านช่องทางหรือ Port ต่าง ๆ ที่มีอยู่ในระบบ การเข้ามาทาง Port นี้อาจทำได้โดยการใช้สัญญาณโทรศัพท์ทำการเรียกเข้ามาในระบบ และทำการเจาะเข้ามาในระบบโดยผ่านทาง Port นี้ การป้องกันการเข้ามาใน Port โดยไม่ได้รับอนุญาตนี้จะต้องทำโดยการใช้ทั้งฮาร์ดแวร์ และ ซอฟต์แวร์ที่ถูกต้องและผ่านการตรวจสอบมาอย่างดี

4.5.2 Automatic Call-Back คือการป้องกันการเรียกเข้าในระบบโดยไม่ได้รับอนุญาต นับว่าเป็นวิธีการป้องกันที่ได้ผลดีประการหนึ่ง นั่นคือเมื่อมีการเรียกเข้ามาทางสัญญาณโทรศัพท์ที่ตัวโมเด็ม(Modem) หลังจากที่ฝ่ายที่เรียกเข้ามาได้แสดงตัวเอง และให้หมายเลขโทรศัพท์ของตัวเองไว้แล้ว ระบบคอมพิวเตอร์จะทำการตัดการติดต่อสื่อสารนั้นเสีย จากนั้นก็จะทำการตรวจสอบดูว่าหมายเลขโทรศัพท์ที่เรียกเข้ามานั้นเป็นหมายเลขที่ได้รับอนุญาตหรือเปล่า หากเป็นหมายเลขที่ได้รับอนุญาตอย่างถูกต้องก็จะทำการเรียกกลับไปแล้วอนุญาตให้ทำการต่อเชื่อมได้

4.5.3 Differetiated Access Rights คือการกำหนดระดับสิทธิในการเข้าถึงข้อมูลที่ต่างกัน เช่น การกำหนดสิทธิในการเข้าถึงข้อมูลบางส่วนเท่านั้นสำหรับผู้ที่มีสิทธิน้อย แต่ให้สามารถเข้าถึงข้อมูลได้ทั้งหมดสำหรับผู้ใช้ที่มีสิทธิมาก หรืออาจกำหนดให้ผู้ใช้ที่มีสิทธิน้อยมีความสามารถเพียงแต่ในการอ่านข้อมูลเท่านั้น แต่ไม่มีสิทธิในการเปลี่ยนแปลงแก้ไขข้อมูลเป็นต้น

4.6 การตรวจสอบความถูกต้องระบบคอมพิวเตอร์ในระบบเครือข่าย(Authentication in Distributed System)

เนื่องจากระบบเครือข่ายนั้นเกิดจากการต่อเชื่อมระบบคอมพิวเตอร์เข้าด้วยกันหลาย ๆ ตัว หรือ หลาย ๆ ระบบ อีกทั้งยังมีการติดต่อสื่อสารกันค่อนข้างมากด้วย เพื่อป้องกันการปลอมแปลงจากระบบคอมพิวเตอร์ที่ไม่ได้รับอนุญาตให้เข้ามาในระบบได้ จึงต้องมีวิธีการตรวจสอบความถูกต้องของระบบที่เข้ามาต่อเชื่อม อุปสรรคสำคัญประการหนึ่งที่ทำให้การตรวจสอบความถูกต้องในลักษณะนี้นั้นทำได้ยากกว่าการตรวจสอบความถูกต้องของผู้ใช้นั้นคือผู้ใช้ระบบสามารถที่จะมีรหัสผ่าน(Password) เป็นตัวบ่งบอกถึงสิทธิในการเข้ามาในระบบได้ ระบบของการตรวจสอบที่อาจนำมาใช้ในการตรวจสอบความถูกต้องของระบบนั้นต้องสามารถที่จะบอกถึงสิ่งต่อไปนี้ได้คือ

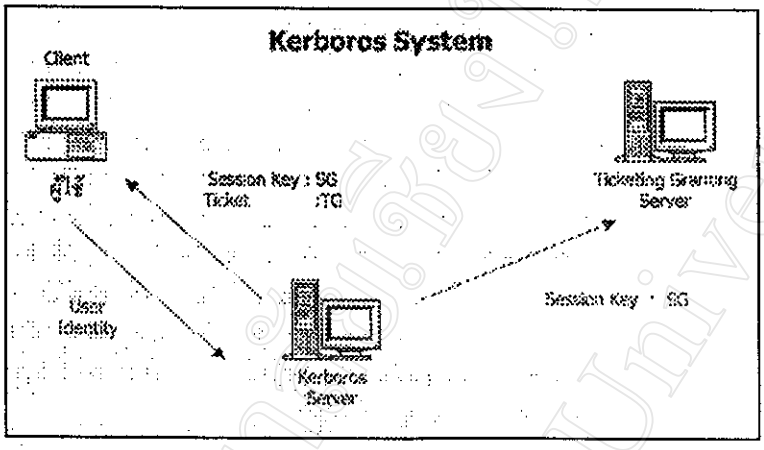
(1) ป้องกันการปลอมแปลงตัวเซิร์ฟเวอร์จากระบบเครือข่ายอื่น ๆ ที่จะเข้ามาทำการเชื่อมต่อได้

(2) ป้องกันการขโมยหรือแอบดัดแปลงข้อมูลในระหว่างที่มีการติดต่อสื่อสารระหว่างตัวเซิร์ฟเวอร์ได้

(3) ป้องกันการแอบบันทึกข้อมูลการขออนุญาตเข้ามาในระบบอย่างถูกต้อง แล้วแอบนำกลับเอามาใช้ใหม่ในการเจาะเข้ามาในระบบได้ (Replay of previous authentication)

ปัจจุบันได้มีการพัฒนาระบบการตรวจสอบขึ้นมาหลายระบบเพื่อใช้ในการตรวจสอบความถูกต้องของระบบในการเชื่อมต่อกัน ตัวอย่างมีดังนี้คือ

4.6.1 ระบบ Kerboros เป็นระบบที่ได้รับการออกแบบโดยสถาบัน MIT-Masschusetts Institute of Technology เพื่อใช้ในการตรวจสอบความถูกต้องในการเชื่อมต่อกันของระบบเครือข่าย ในตอนแรกนั้นระบบ Kerboros ได้ถูกออกแบบมาโดยใช้ Symmetric-Key Encryption เป็นตัวช่วยรักษาความปลอดภัยของระบบ แต่ต่อมาก็ได้มีการใช้ Public-Key Encryption มาใช้ในการรักษาความปลอดภัยของระบบ



ภาพที่ 18 แสดงระบบ Kerboros[45]

ระบบ Kerboros มักถูกใช้ในการตรวจสอบความถูกต้องระหว่าง Processor ที่ทำการติดต่อสื่อสารระหว่างกัน เช่น ในระบบ Client-Server โดยจะมีหลักการทำงานคือ Kerboros Server จะอนุญาตให้ไคลเอ็นต์เข้ามาทำการติดต่อสื่อสารโดยใช้บัตรผ่าน(Ticket : TG) ซึ่งออกให้โดย Kerboros Server เท่านั้น และจะใช้ Session Key : SG เป็นตัวบ่งบอกถึงการติดต่อสื่อสารในแต่ละครั้งเป็นครั้ง ๆ ไป เพื่อป้องกันการแอบเอาข้อมูลเดิมที่ใช้ในการติดต่อสื่อสารครั้งที่แล้วมาใช้อีกครั้งหนึ่ง

---

[45] ณรงค์ชัย นมิตบุญอนันต์. **Computer Security for E-Commerce.** กรุงเทพ : บริษัทซีเอ็ดยูเคชั่น จำกัด (มหาชน), 1999 : 181.

ข้อดีของระบบ Kerboros คือ

(1) ไม่ต้องมีการใช้ Password ในระบบเครือข่ายเพื่อตรวจสอบความถูกต้องในการติดต่อสื่อสาร

(2) ใช้การเข้ารหัสข้อมูลเพื่อป้องกันการแอบขโมยข้อมูล

(3) บัตรผ่าน(Ticket : TG)นั้นมีอายุกำหนดเป็นระยะเวลาที่แน่นอน เพื่อป้องกันการทำลายกุญแจรหัสลับโดยวิธีการ Cryptanalysis ซึ่งอาจต้องใช้ระยะเวลาหนึ่งในการค้นหากุญแจรหัสลับ

(4) มีความตรวจสอบความถูกต้องกันทั้งสองฝ่าย(Mutual Authentication) คือตัวเซิร์ฟเวอร์สามารถที่จะตรวจสอบความถูกต้องของตัวไคลเอ็นต์ได้ และในทางกลับกันตัวไคลเอ็นต์ก็สามารถที่จะทำการตรวจสอบความถูกต้องของตัวเซิร์ฟเวอร์ได้ด้วย

4.6.2 ระบบ DCE

เป็นระบบที่ได้รับการพัฒนาโดย OSF(Open Software Foundation) ซึ่งเป็นสมาคมของบริษัทผู้ผลิตซอฟต์แวร์กว่า 200 บริษัท ระบบ DCE ได้รับการสนับสนุนในการพัฒนาโดยบริษัทยักษ์ใหญ่ เช่น Digital Equipment Corp., Hewlett-Packkard และ IBM จุดประสงค์ในการพัฒนาระบบ DCE นี้ก็เพื่อให้สามารถทำการพัฒนาระบบเครือข่ายให้มีความปลอดภัยสูง ระบบ DCE นี้เป็นระบบที่ได้รับการพัฒนาจากระบบ Kerboros แต่มีข้อแตกต่างคือ มีการรวมกันระหว่าง Authentication Server และ Ticket Granting Server เข้าไว้ด้วยกันเป็น Security Server เพียงตัวเดียว ซึ่งเป็นการง่ายต่อการบริหารและจัดการ ระบบ DCE นี้ยังใช้ผ่าน Ticket เหมือนกับระบบ Kerboros แต่มีข้อแตกต่างคือจะใช้บัตรผ่านที่เป็นแบบ Privilege Attribute Certificate เพื่อที่จะสามารถบอกถึงสิทธิในการใช้และเข้าถึงข้อมูลได้สำหรับผู้ใช้แต่ละคน ดังนั้นจึงสามารถที่จะรักษาความปลอดภัยของข้อมูลได้เป็นอย่างดี สำหรับเทคโนโลยีที่ใช้ในการเข้ารหัสข้อมูลนั้นส่วนมากก็จะเน้นหนักในการใช้ Symmetric-key Encryption Technology เป็นหลัก[46]

---

[46] Williams, Sawyer, Hutchinson. **Using Information Technology**. NewYork, 2nd edition : Irwin/McGraw-Hill, 1996 : 234.

4.6.3 SESAME

เป็นระบบที่พัฒนาขึ้นมาโดยสถาบัน European Research and Development Agency การทำงานของระบบ SEASAME นี้ก็จะคล้าย ๆ กันกับระบบ Kerboros และ ระบบ DCE แต่จะมีข้อแตกต่างที่สำคัญคือในการทำการพิสูจน์ทราบ(Authentication)นั้นจะใช้ระบบ Public-Key Cryptography ซึ่งสามารถที่นำมาใช้ได้สะดวกกว่าและยังให้ความปลอดภัยที่สูงมากด้วย[47]

4.7 การป้องกันการรั่วไหลของข้อมูลจากการส่งข้อมูลผ่านระบบเครือข่าย (Traffic control)

วิธีการหนึ่งที่สามารถนำมาใช้ในการขโมยข้อมูลก็คือ การวิเคราะห์การส่งข้อมูล(Traffic Flow Analysis) โดยการพิจารณาข้อมูลดูว่าถูกส่งไป ณ ที่ใด ในเวลาใดบ้างและมีปริมาณข้อมูลมากน้อยเพียง หรือบางครั้งผู้ไม่ประสงค์ดีอาจทำการเจาะความลับของข้อมูลโดยการใช้ Convert Channel ซึ่งหมายถึงวิเคราะห์ความลับข้อมูลโดยการพิจารณาจากสิ่งที่เป็นส่วนประกอบของข้อมูลอยู่แล้ว โดยส่วนที่นำมาใช้ในการพิจารณานี้อาจเป็นสิ่งที่ถูกเติมเข้าไปในข้อมูล เช่น การเพิ่มบิต = 1 สำหรับข้อมูลที่ถูกส่งไปยัง Host ตัวหนึ่งในระบบเครือข่าย และหากข้อมูลนั้นถูกส่งไปสู่ Host อื่นๆ ในระบบเครือข่ายก็ให้บิต = 0 เป็นต้น วิธีการต่อต้านการวิเคราะห์ข้อมูลเหล่านี้นั้นสามารถทำได้ดังต่อไปนี้คือ

4.7.1 Pad Traffic คือ การเพิ่มการส่งข้อมูลเข้าไปในระบบเครือข่ายในลักษณะการสุ่ม (Spurious Message) เพื่อจุดประสงค์ในการกลบเกลื่อนลักษณะการส่งข้อมูลที่แท้จริง การกระทำเช่นนี้สามารถทำให้การวิเคราะห์การส่งข้อมูล (Traffic Flow Analysis) นั้นทำได้ยากขึ้นหรืออาจทำไม่ได้เลย

4.7.2 Routing Control คือวิธีการหนึ่งที่อาจนำมาใช้ในการต่อต้าน Covert Channel ที่อาจมีอยู่ในระบบ ซึ่งอาจทำได้โดยการส่งข้อมูลในลักษณะที่กลับกันกับ Covert Channel ที่ตรวจพบในระบบ หรือ อาจใช้วิธีการส่งต่อข้อมูลออกไปเป็นทอดๆ หลายๆ ครั้งก่อนที่จะส่งไปยังจุดหมายปลายทาง เป็นต้น

---

[47] เรื่องเดียวกัน : 234.

4.8 การรักษาความถูกต้องของข้อมูลที่ถูกส่งผ่านระบบเครือข่าย (Data Integrity)

ภัยคุมคามที่สำคัญอย่างหนึ่งของข้อมูลที่ถูกส่งผ่านระบบเครือข่ายก็คือ การแอบดัดแปลงแก้ไขข้อมูลในระหว่างการส่ง สำหรับวิธีการแก้ไขป้องกันก็อาจทำได้ดังต่อไปนี้ คือ

4.8.1 การใช้โปรโตคอล คือการนำวิธีการติดต่อสื่อสารที่มีขั้นตอนและรูปแบบที่แน่นอนที่ได้รับการตกลงกันไว้ก่อนแล้วมาใช้ในการติดต่อระหว่างระบบคอมพิวเตอร์ภายในเครือข่าย สำหรับการรักษาความลับของข้อมูลนั้นอาจใช้ วิธีการ Link-to-Link Encryption หรือ End-To-End Encryption มาช่วยในการรักษาความปลอดภัยของข้อมูลในระหว่างการสื่อสาร

4.8.2 การใช้ Checksums คือการตรวจสอบความถูกต้องของข้อมูลโดยการใช้ฟังก์ชันทางคณิตศาสตร์ที่เรียกว่า Checksums เพื่อตรวจสอบดูว่ามีการเปลี่ยนแปลงข้อมูลในระหว่างการส่งหรือไม่

4.8.3 การใช้ Parity Bit คือ การตรวจสอบความถูกต้องของข้อมูลในตอนก่อนส่ง และหลังส่งโดยการนับจำนวน บิตที่เป็น 1 (หรือ 0)

4.8.4 การใช้ลายเซ็นทางอิเล็กทรอนิกส์ (Digital Signature) คือการตรวจสอบลายเซ็นทางอิเล็กทรอนิกส์ของข้อมูลว่าตรงกันในทั้งตอนก่อนส่งหรือหลังส่งหรือไม่ หากลายเซ็นของข้อมูลไม่มีการเปลี่ยนแปลงก็แสดงว่าข้อมูลนั้นถูกต้อง

4.9 การใช้ Firewall ในการรักษาความปลอดภัยของระบบเครือข่าย

Firewall คือเครื่องมือที่ใช้ในการตรวจสอบหรือปิดกั้น(Filter)การเชื่อมต่อของข้อมูลระหว่างภายนอกระบบเครือข่ายกับภายใน ระบบเครือข่ายหลักที่สำคัญที่มีการใช้ Firewall คือการป้องกันสิ่งที่อาจเป็นอันตรายจากภายนอกระบบไม่ให้สามารถเข้ามาในระบบได้ หลักปรัชญาในการออกแบบ Firewall มีอยู่ 2 วิธีคือ[48] ข้อมูล โปรแกรม หรือผู้ใช้ ที่ไม่ได้รับการห้ามไว้จะสามารถเข้ามาในระบบผ่าน Firewall ได้ และวิธีที่สอง ข้อมูล โปรแกรม หรือผู้ใช้ที่ไม่ได้รับการอนุญาตไว้ก่อนล่วงหน้าจะไม่สามารถเข้ามาในระบบโดยผ่าน Firewall ได้

การใช้ Firewall ในการรักษาความปลอดภัยของระบบนั้นยังเป็นการนำหลักทฤษฎีที่ใช้ในการรักษาความปลอดภัยที่เรียกว่า Reference Monitor Concept มาใช้ร่วมด้วยเพราะ Firewall มีคุณสมบัติดังนี้ คือ เป็นระบบการรักษาความปลอดภัยที่ทำงานอยู่ตลอดเวลา (Always Invoked) เป็นระบบที่ไม่สามารถจะทำการดัดแปลงแก้ไขได้โดยง่าย จากผู้ที่ไม่ประสงค์ดี (Tamper Proof) เป็นระบบที่มี

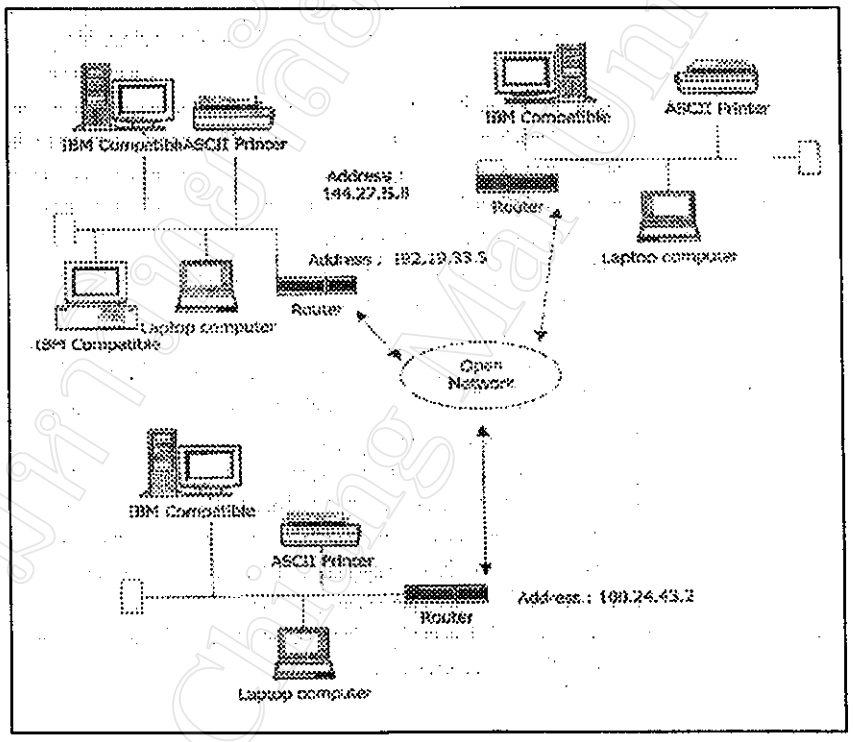
---

[48] นงนุช อนันต์โสภณสกุล. "ค้นหาความหมายของ Firewall". BCM. (กุมภาพันธ์ 1997) : 157.

ขนาดเล็กและมีการทำงานที่ไม่สลับซับซ้อนมากนั้น ซึ่งทำให้ง่ายต่อการวิเคราะห์และตรวจสอบขีดความสามารถในการรักษาความปลอดภัยของระบบ Firewall

4.9.1 ชนิดของ Firewall

(1) Screening Routers คืออุปกรณ์ที่ใช้ในการตรวจสอบว่า ข้อมูลในรูป Data Packets นั้นจะถูกส่งไปที่ใด และมาจากไหน และได้รับอนุญาตอย่างถูกต้องหรือไม่ ตัว Screening Router จะมีข้อมูลที่เรียกว่า Routing Table เพื่อเอาไว้ตรวจสอบข้อมูลที่ถูกส่งผ่านทั้งเข้ามาในระบบเครือข่าย และออกไปจากระบบเครือข่าย การตรวจสอบนั้นสามารถทำได้โดยการตรวจดู Address ที่ Headers ของข้อมูลที่ในรูป Packet Data แล้วเปรียบเทียบกับข้อมูล Address ที่มีอยู่ก่อนแล้วใน Routing Table

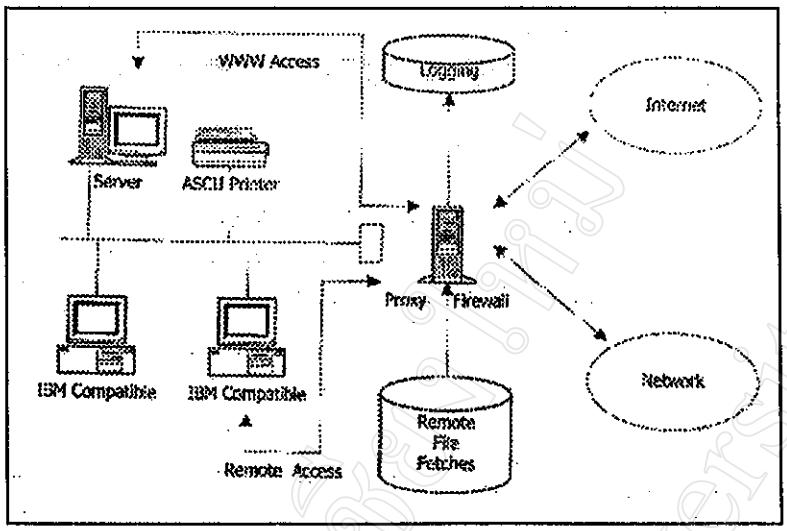


ภาพที่ 19 แสดงการทำงานของ Screening Router[49]

[49] ณรงค์ชัย นมิตบุญอนันต์. **Computer Security for E-Commerce**. กรุงเทพ : บริษัทซีเอ็ดยูเคชั่น จำกัด (มหาชน), 1999 : 185.

จากภาพที่ 19 จะเห็นได้ว่าในการเชื่อมต่อระบบเครือข่าย LAN เข้าสู่ระบบเครือข่ายขนาดใหญ่นั้น จะใช้ตัว Router เป็นตัวที่ทำหน้าที่ตรวจสอบข้อมูลก่อนที่จะเข้าหรือออกจากระบบตัวอย่างของการใช้งานโดยการใช้ Screening Router ก็คือ ระบบเครือข่ายที่มี Address : 100.24.43.2 นั้นสามารถที่จะกำหนดได้ว่า ข้อมูลสามารถที่จะออกไปสู่ระบบเครือข่าย 192.19.33.5 และ 144.27.5.8 ได้เท่านั้น และจะไม่สามารถออกไปสู่ระบบเครือข่ายอื่นๆ ได้ส่วนในการรับข้อมูลเข้าสู่ระบบนั้นสามารถจะกำหนดได้เช่นเดียวกัน คือ อาจมีการอนุญาตให้ข้อมูลที่มาจาก 192.19.33.5 เท่านั้นที่สามารถผ่าน Screening Router เข้าไปได้ แต่ข้อมูลที่มาจาก Address อื่นๆ นั้น จะไม่สามารถผ่านเข้าไปได้เลย ดังนั้นจึงเป็นการตัดปัญหาที่อาจเกิดขึ้นจากการบุกรุกเข้ามาในระบบของผู้ที่ไม่ประสงค์ดีจากระบบอื่นๆ

(2) Proxy Gateway คือระบบที่นำมาใช้ในการตรวจสอบข้อมูล โดยจะตรวจสอบทั้งข้อมูล Address ที่อยู่ใน Headers และจะสอบข้อมูลที่เป็น Data อีกด้วย สาเหตุสำคัญที่ทำให้การใช้ Proxy Gateway นี้สามารถให้ความปลอดภัยที่สูงกว่า Screening Router อีกประการหนึ่งคือ จะทำการตรวจสอบความถูกต้องของข้อมูลโปรแกรมใช้งาน (Applications) ที่ถูกส่งผ่านระบบเครือข่ายด้วย โดยจะใช้วิธีการที่เรียกว่า Pseudo-Applications ซึ่งจะอนุญาตให้ข้อมูลหรือคำสั่งที่ได้รับมาจากระบบเครือข่ายนั้นสามารถทำงานได้ตามที่ได้รับอนุญาตเท่านั้น ดังนั้นจึงตัดปัญหาว่าข้อมูลโปรแกรมจากภายนอกระบบอาจเข้ามาสร้างความเสียหายต่างๆ ให้กับส่วนต่างๆ ภายในระบบได้ เนื่องจากว่า Proxy Gateway นี้สามารถทำการใช้งาน Pseudo-Applications นี้ได้ บางครั้งจะเรียกว่า Bastion Host



ภาพที่ 20 แสดงการทำงานของ Proxy Gateway[50]

จากภาพที่ 20 จะเห็นได้ว่าในการเชื่อมต่อระบบเครือข่ายย่อยที่มี Proxy Firewall กั้นอยู่นั้น จะสามารถรักษาความปลอดภัยให้กับระบบภายในได้เป็นอย่างดี เพราะว่าในการติดต่อข้อมูลข่าวสาร หรือการใช้งานของ ไฟล์ต่าง ๆ นั้นจะมี Proxy Firewall ทำหน้าที่แทนระบบเครือข่ายแทบทั้งหมด แม้กระทั่งการเข้าสู่ WWW หรือ การทำ Remote Access ก็จะต้องใช้บริการของ Proxy Firewall ซึ่งจะทำหน้าที่แทน และเป็นตัวกลางระหว่างระบบเครือข่ายภายในและระบบเครือข่ายภายนอกทั้งหมด

(3) Guard คือระบบ Proxy Firewall ที่มีขีดความสามารถในการรักษาความปลอดภัยที่ดีมากยิ่งขึ้นไปอีก แต่ในขณะเดียวกันก็มีความสลับซับซ้อนที่มากเพิ่มขึ้นไปด้วย การทำงานของ Guard โดยทั่วไปแล้วนั้นก็เหมือนกันกับ Proxy Firewall นั่นคือจะทำการวิเคราะห์โปรโตคอลที่ผ่านเข้าหรือออกจากระบบเครือข่ายแล้วทำการสั่งงานตามสิ่งที่โปรโตคอลเหล่านั้นต้องการเพื่อที่จะให้ได้ Services ได้ตามที่ต้องการ ทั้งนี้ตัว Guard เองอาจใช้ Protocol อันเดียวกันกับที่ได้รับมาจากระบบเครือข่ายหรือโปรโตคอลที่คล้ายกันที่แต่สามารถทำงานได้เหมือนกัน และให้ผลลัพธ์ตามที่ต้องการได้

---

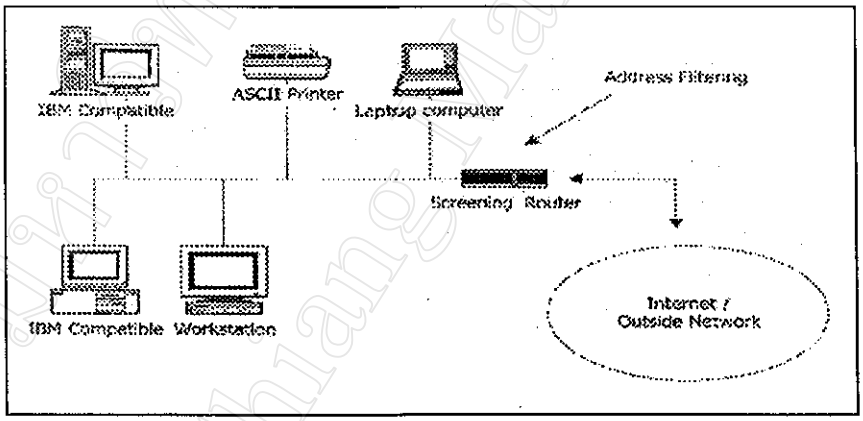
[50] เรื่องเดียวกัน : 187.

ตารางที่ 8 แสดงข้อมูลเปรียบเทียบระหว่าง Screening Router, Proxy Gateway, Guard[51]

Screening Router	Proxy Gateway	Guard
1.) เป็นระบบที่ง่ายและไม่สลับซับซ้อน	1.) เป็นระบบที่สลับซับซ้อนมาก	1.) เป็นระบบที่สลับซับซ้อนมากที่สุด
2.) ตรวจสอบเฉพาะที่อิเล็กทรอนิกส์ (Address) และชนิดของโปรโตคอลที่ใช้	2.) ทำการตรวจสอบข้อมูลทั้งหมดในระหว่างการติดต่อสื่อสาร	2.) ทำการตรวจสอบข้อมูลทั้งหมดในระหว่างการติดต่อสื่อสาร
3.) ยากต่อการแก้ไขปรับปรุง	3.) สามารถที่ปรับปรุงเปลี่ยนแปลงแก้ไขการทำงานได้โดยง่าย	3.) สามารถที่ปรับปรุงเปลี่ยนแปลงแก้ไขการทำงานได้โดยง่าย
4.) หลักการตรวจสอบจะดูที่การต่อเชื่อมของระบบ (Connection Rule)	4.) หลักการตรวจสอบจะขึ้นอยู่กับการทำงานของ Proxy (i.e.Proxy Behavior)	4.) หลักการตรวจสอบจะขึ้นอยู่กับลักษณะการทำงานของข้อมูลทั้งหมด (Interpretation of Message content)
5.) หากระบบที่อยู่อิเล็กทรอนิกส์ (Address) ที่ใช้นั้นสลับซับซ้อนก็อาจทำให้การใช้งานยุ่งยาก (Configuration Difficulty)	5.) Proxy แบบง่ายๆ ก็สามารถที่จะทำหน้าที่ในการตรวจสอบ Address ได้เหมือน กับ Screening Router	5.) ความสลับซับซ้อนของระบบอาจทำให้การตรวจสอบเพื่อรับรองระดับความปลอดภัยนั้นทำได้ยากมากขึ้น (Limit Assurance)

4.9.2 ตัวอย่างการใช้งานของ Firewall กับระบบ LAN

(1) การใช้งานของ Firewall กับระบบ LAN



ภาพที่ 21 แสดงการทำงานของ Firewall กับระบบ LAN[52]

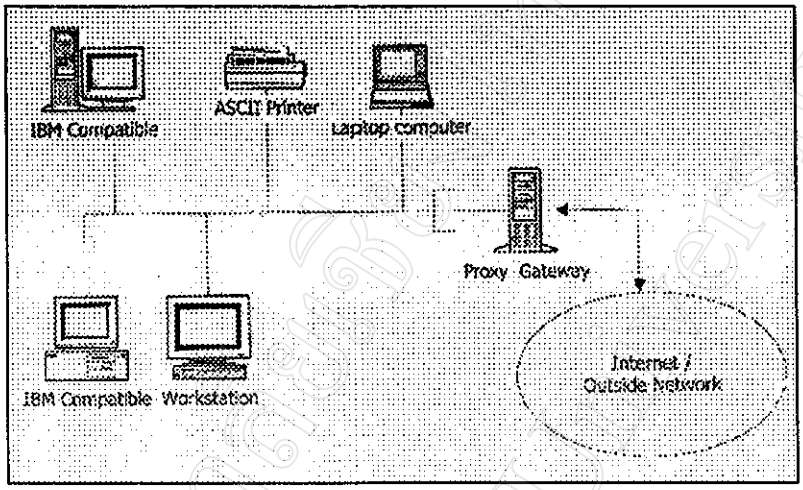
Screening Router จะทำการตรวจสอบที่อยู่ (Address) ของ Data Packets ที่จะผ่านเข้าและออกจากระบบ LAN ดังนั้นหากมี Address ใดในระบบเครือข่ายที่ไม่เป็นที่พึง

[51] เรื่องเดียวกัน : 188.

[52] เรื่องเดียวกัน : 189.

ประสงค์ เพราะอาจมีปัญหาด้านการรักษาความปลอดภัยของข้อมูลก็อาจจะถูกปิดกั้น (Block) ไว้ ทำให้ไม่สามารถทำการต่อเชื่อมผ่านระบบเครือข่ายได้

(2) การใช้ Proxy Gateway มาทำเป็น Firewall



ภาพที่ 22 แสดงการใช้ Proxy Gateway มาทำเป็น Firewall[53]

เนื่องจาก Screening Router เป็นระบบที่ไม่มีความสลับซับซ้อนมากนัก ดังนั้นหากระบบ LAN ต้องทำการจัดการหรือตรวจสอบเกี่ยวกับ Address ที่มีความสลับซับซ้อนสูงจนเกินไป ก็ไม่สามารถที่จะทำงานได้อย่างมีประสิทธิภาพมากนัก ผลก็คืออาจมี Address ที่ไม่ได้รับอนุญาตจากระบบเครือข่ายที่ไม่ปลอดภัยสามารถส่งข้อมูลหรือโปรแกรมเข้าและออกจากระบบ LAN ได้ ทำให้ระบบ LAN นี้มีความเสี่ยงเพิ่มขึ้น ดังนั้นวิธีแก้วิธีหนึ่งก็คือ การนำเอา Proxy Gateway มาใช้ในการเพิ่มระดับความปลอดภัยให้กับระบบ โดยอาจทำการสั่งให้ Proxy Gateway นี้อนุญาตให้ Address ที่มีอยู่ใน LAN นี้เท่านั้นสามารถที่ส่งข้อมูลออกไปติดต่อสื่อสารกับโลกภายนอกได้ และข้อมูลที่จะเข้ามาใน LAN ก็จะต้องมีที่อยู่ Address ที่มีอยู่แล้วใน LAN เท่านั้น เป็นต้น

การใช้ Proxy Gateway และ Screening Router มาทำเป็น Firewall จึงเป็นการป้องกันการโจมตีระบบแบบ Flooding Attack ซึ่งก็คือการส่งข้อมูลจำนวนมาก ๆ มาที่ระบบ และทำให้ระบบไม่สามารถทำงานในการรักษาความปลอดภัยได้ตามปกติ เนื่องจากต้องใช้

---

[53] เรื่องเดียวกัน : 189.

ทรัพยากรที่มีอยู่ในการปฏิเสธข้อมูลที่ไม่ถูกต้องเหล่านี้ แต่ตัว Screening Router จะทำหน้าที่กลั่นกรองข้อมูลเสียก่อนที่จะไปถึงตัว Proxy Firewall

แต่อย่างไรก็ตาม หากมีการทำลายการรักษาความปลอดภัยของ Screening Router นี้ได้แล้ว ระบบ LAN ก็ยังมีความปลอดภัยอยู่เพราะว่าข้อมูลหรือโปรแกรมจากภายนอกก็ยังไม่สามารถที่เข้าไปถึงข้อมูลสำคัญภายในระบบ LAN ได้ เนื่องจากว่า Proxy Firewall จะทำหน้าที่เป็นตัวกลางในการวิเคราะห์ รับ-ส่ง ข้อมูลแทนส่วนต่างๆ ของระบบ LAN ดังนั้นก็จะมีเพียงแต่ข้อมูลหรือโปรแกรมต่างๆ ที่อยู่ใน Proxy Firewall เท่านั้นที่อาจมีผลกระทบจากการบุกรุกเข้ามาในระบบผ่าน Screening Router

4.9.3 ข้อจำกัดของ Firewall

(1) Firewall สามารถจะป้องกันส่วนต่างๆ ของระบบที่มี Firewall เป็นตัวกลางเชื่อมต่อเท่านั้นแต่จะไม่สามารถป้องกันระบบจากการเชื่อมต่อโดยตรงกับโลกภายนอกได้ เช่น การทำ Remote Log-in โดยไม่ผ่าน Firewall เป็นต้น

(2) Firewall สามารถที่ทำการรักษาความปลอดภัยของข้อมูล และส่วนต่างๆ ที่อยู่ภายในระบบเท่านั้น ดังนั้นหากข้อมูลหรือโปรแกรมถูกส่งออกนอกระบบไปแล้วข้อมูลเหล่านั้นก็จะไม่ได้รับการป้องกันจาก Firewall อีกต่อไป

(3) Firewall นั้นเป็นจุดที่มักได้รับการโจมตีจากระบบภายนอกเพราะเป็นส่วนเดียวที่ระบบภายนอกอาจเข้าถึงได้ ดังนั้นหาก Firewall นี้ถูกทำลายลงแล้วก็อาจทำให้ระบบทั้งระบบถูกทำลายลงไปด้วย ด้วยเหตุนี้จึงไม่ควรที่จะใช้ Firewall แต่เพียงอย่างเดียวในการรักษาความปลอดภัยของระบบ แต่ควรใช้หลักปรัชญา Defense-In-Depth ซึ่งหมายถึงการป้องกันรักษาในทุกๆ ส่วนของระบบพร้อมๆ กันไปด้วย

(4) Firewall นั้นได้รับการออกแบบมาให้มีระบบการทำงานที่ง่าย และไม่สลับซับซ้อน ด้วยเหตุผลที่ว่าหากมันถูกโจมตี และถูกทำลายลงไปแล้ว ก็จะไม่มีระบบอื่นๆ มาสนับสนุนการโจมตีทำลายระบบต่อไป เช่น Compliers, Linkers, Loaders เป็นต้น

(5) Firewall จะต้องได้รับการติดตั้งและใช้งานอย่างถูกต้อง ค่าตัวแปร (Parameters) จะต้องถูกใช้อย่างถูกต้องด้วย และหากมีการเปลี่ยนแปลงของโปรแกรมหรือส่วนต่างๆ (Environments) ของทั้งระบบแล้ว ตัว Firewall เองก็จะต้องได้รับการพิจารณาติดตั้งปรับเปลี่ยนด้วย

(6) เมื่อข้อมูลหรือโปรแกรมต่างผ่าน Firewall เข้ามาในระบบแล้ว ตัว Firewall ก็จะไม่มีอำนาจในการควบคุมสิ่งเหล่านี้มากมายนัก ตัวนั้นสิ่งเหล่านี้จะต้องได้รับการตรวจสอบดูแลทางด้านความปลอดภัยโดยระบบภายในเอง

4.10 การรักษาความปลอดภัยกับอุปกรณ์อื่น ๆ ในเครือข่าย

4.10.1 การรักษาความปลอดภัยสำหรับ DNS และ DHCP

(1) DNS ของระบบเครือข่ายภายใน ควรจะได้รับการปกป้องจาก Firewall และ ระบบเครือข่ายภายนอกควรจะมองเห็น Address ของ Host ผ่านทาง Firewall เท่านั้นและไม่ควรจะมองเห็นข้อมูลอื่นๆ ที่อยู่ข้างในระบบเครือข่ายภายในได้เลย

(2) ตัวไคลเอ็นต์ที่มีการต่อเชื่อมไม่มากนั้น ไม่ควรจะมี DNS

(3) DNS ควรจะได้รับการจัดให้เป็น Class

(4) ควรมีการใช้ Secondary Server เพื่อเพิ่มความปลอดภัยให้กับระบบในกรณีที่มีการทำงานบกพร่องของ Primary Server

(5) DHCP (Dynamic Host Configuration Protocol) เป็นการเปลี่ยนแปลงที่อยู่ Address ของระบบที่มีไคลเอ็นต์ที่มีการเคลื่อนย้ายไปตามสถานที่ต่าง ๆ อยู่ตลอดเวลา เช่น การใช้ Labtop computer ในการเชื่อมต่อเข้ากับระบบเครือข่าย โดยปกติแล้วระบบเครือข่ายจะมีการต่อเชื่อมกันโดยใช้ Fixed Address ที่ไม่มีการเปลี่ยนแปลงซึ่งจะให้ความปลอดภัยที่สูงกว่า DHCP เพราะจะปลอมแปลงได้ยากขึ้น

(6) IP Address ควรจะใช้กับเครื่องคอมพิวเตอร์ตัวใดตัวหนึ่งเท่านั้น เพื่อป้องกันการปลอมแปลงเข้ามาในระบบ

(7) หากมีความจำเป็นต้องนำ DHCP มาใช้ก็ควรจะให้เซิร์ฟเวอร์มี IP Address ที่คงที่ไม่เปลี่ยนแปลง

4.10.2 การรักษาความปลอดภัยสำหรับอุปกรณ์เครือข่าย

การป้องกันโดยทั่วไปไม่ควรมีโปรแกรม "Sniffer" หรือ "Network Analyzer" อยู่บน PC ที่เป็นไคลเอ็นต์ เพราะอาจเกิดการรั่วไหลของข้อมูลหรือจุดอ่อนของระบบได้ ในระบบบางระบบ เช่น Sun OS หรือ Solaris นั้นจะมีซอฟต์แวร์ที่เป็น Standard อยู่ด้วย ดังนั้นหากตัว Software Components หรือ Utilities ที่ไม่ได้ใช้ก็ควรจะลบทิ้ง หรือควรจะปรับเปลี่ยน Permission ใหม่ให้เหมาะสม

(1) Ethernet

- ควรจะใช้ Hubs แทนที่จะใช้ Thin Ethernet
- ไม่ควรมี Unused-Lived Connection
- ควรทำการ Disconnected เมื่อไม่ได้ใช้งาน
- อุปกรณ์ในระบบเครือข่ายควรมีการป้องกันรักษาความปลอดภัยอย่างดี

(2) Leased-Line

- สายเชื่อมต่อที่เป็นทองแดง ควรจะมีอุปกรณ์สำหรับใช้ในการเข้ารหัสข้อมูลโดยเฉพาะ FDDI
- เป็นระบบที่สามารถให้ความปลอดภัยที่สูงมาก เพราะไม่มีการแผ่สนามแม่เหล็กไฟฟ้าออกมาจากสายใยแก้วนำแสง จึงไม่อาจทำการดักฟังได้โดยง่าย
- อย่างไรก็ตามควรมีการตรวจสอบระบบอยู่สม่ำเสมอ เพื่อหาความผิดปกติอาจเกิดขึ้นได้จากการดักจับสัญญาณโดยวิธีอื่นๆ

(3) Hubs

- ควรใช้ Active Hubs (Switching Hubs) แทนที่ Repeater Hubs เพราะให้ความปลอดภัยที่สูงกว่า และโปรแกรม Sniffer ไม่สามารถที่จะทำการโจมตีได้ และก็จะทำให้ประสิทธิภาพของระบบดีขึ้นด้วย เพราะอุปกรณ์ Switching Hubs จะทำการส่งข้อมูลแบบ Host-To-Host แทนที่จะทำการส่งข้อมูลแบบ Broadcast ที่ใช้โดย Repeater Hubs

(4) Bridges

- เป็นอุปกรณ์ที่ใช้ในการแบ่งแยก Subnets ออกเป็นส่วนย่อยๆ Segments ซึ่งมีประโยชน์ในการตรวจสอบความผิดพลาดของระบบว่าอยู่ ณ ที่ใดในระบบ
- จำกัดการสื่อสารข้อมูลลงเป็นส่วนย่อย ๆ (Segments) สามารถที่เพิ่มขีดความสามารถในการรักษาความปลอดภัยของข้อมูลได้เพราะจะมีการติดต่อสื่อสารกันในวงที่แคบลง จึงสามารถทำการตรวจสอบได้ง่าย

(5) Routers

- ไม่ควรอนุญาตให้ข้อมูลในรูปของ NetBEUI Packets หรือ TCP/IP Broadcast ผ่านไปได้เพราะต้องใช้ Bandwidth ที่สูงมาก และเป็นการเสี่ยงต่อการรักษาความปลอดภัยของระบบด้วย
- ควรใช้ในการป้องกัน Subnet โดยการตรวจสอบที่อยู่ Address
- Router สามารถที่จะทำการโปรแกรมการทำงาน Configurations ผ่าน Telnet ได้ ดังนั้นจึงควรเลือกใช้ Password ที่ดี (Strong Password)

(6) Modem

- Modem ที่ใช้สำหรับการเรียกสายออกไปข้างนอกเท่านั้น (Out-going call) ควรจะทำการปลดความสามารถในการเรียกสายเข้ามา (Deactivated In-coming Call)

4.11 ระบบรักษาความปลอดภัยแบบอื่น ๆ

นอกเหนือจากการรักษาความปลอดภัยทางเครือข่ายแล้ว ปัจจัยภายนอกอื่น ๆ ยังเสริมความปลอดภัยให้กับองค์กรได้อีกเช่น การรักษาอุปกรณ์รอบนอกคอมพิวเตอร์ ให้พ้นจากภัยธรรมชาติและภัยจากสิ่งแวดล้อม เช่นไฟไหม้และขโมย มีการใช้อุปกรณ์ล๊อคแบบต่าง ๆ เช่น การ์ดแถบแม่เหล็ก การตรวจสอบลายนิ้วมือเป็นต้น