เอกสารคำสอนวิชา

Network Security

โดย

อาจารย์ ธนัญชัย ตรีภาค

ภาควิชาวิศวกรรมคอมพิวเตอร์

คณะวิศวกรรมศาสตร์

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

Contents

สารบัญตาราง

สารบัญรูป

แผนการสอน

สัปดาห์ที่	หัวข้อการสอนและเนื้อหาวิชาโดยสังเขป
1	บทนำ
2	ปัญหาความปลอดภัยในระบบเครือข่าย
3	Confidentiality , Integrity , Availability
4	Access Control
5	Firewall
6	Network Address Translation
7	IP Security
8	Web Application Security
9	Wireless LAN Security
10	การ Monitor และ ตรวจสอบระบบ : IDS / IPS
11	Hi-Availability System and Network : Load Balancing
12	การจัดการระบบการรักษาความปลอดภัยข้อมูล
13	การกำหนดนโยบายการรักษาความปลอดภัยตามมาตรฐานสากล
14	พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ 2550 กับการดูแลระบบสารสนเทศ
15	ทบทวน

บทที่ 1. บทนำ

ระบบสารสนเทศประกอบด้วยองค์ประกอบหลักๆ 3 ประการคือ ระบบฮาร์ดแวร์ ระบบซอฟต์แวร์ ระบบเครือข่าย ซึ่งองค์ประกอบทั้งสามต้องทำงานสอดประสานร่วมกันเป็นอย่างดี การทำงานตามที่ได้ออกแบบไว้จึงจะมีประสิทธิภาพและประสิทธิผล เมื่อมองในมุมของการรักษาความปลอดภัยระบบสารสนเทศจะเริ่มต้นจากการวิเคราะห์ช่องโหว่ขององค์ประกอบย่อยต่างๆ ทั้งหมด รวมถึงผู้ที่มีส่วนเกี่ยวข้องกับระบบ ซึ่งสามารถทำได้โดยการหาข้อมูลองค์ประกอบทั้งหมดของระบบไม่ว่าจะเป็นองค์ประกอบในระบบฮาร์ดแวร์ ความสามารถและการทำงานของซอฟต์แวร์ โพรโตคอลที่ใช้รวมถึงกฎการใช้งานระบบเครือข่าย ความรู้ความสามารถของผู้ที่มีส่วนเกี่ยวข้องในระบบ นอกจากนี้ยังต้องมีการวิเคราะห์ถึงการกฎระเบียบ และกระบวนการทำงานของผู้ใช้งานในระบบสารสนเทศนั้นๆ ด้วย จึงจะสามารถวิเคราะห์ถึงปัญหาในการรักษาความปลอดภัยในระบบสารสนเทศและแนวทางในการแก้ไขปัญหาต่อไป

ในการทำงานของผู้ใช้งานระบบโดยทั่วไป สามารถวิเคราะห์ปัญหาด้านการรักษาความปลอดภัยระบบได้ในลักษณะเดียวกันกับการวิเคราะห์ระบบ แต่ผลลัพธ์ที่จะได้นั้นขึ้นอยู่กับความรู้ความสามารถของผู้วิเคราะห์ว่ามีความรู้ในกระบวนการทำงานของฮาร์ดแวร์ ซอฟต์แวร์ และระบบเครือข่ายในระดับลึกมากน้อยเพียงใด ยกตัวอย่างเช่นกรณีที่ผู้ใช้งานเชื่อมต่อเข้าไปยังเว็บไซต์ของหน่วยงานเพื่ออ่าน E-mail ของบริษัทผ่านหน้าเว็บเพจในร้านบริการให้เช่าอินเตอร์เน็ตหรืออินเตอร์เน็ตคาเฟ่ ซึ่งหลายๆ คนอาจเคยเจอปัญหาถูกขโมยรหัสผ่านเมื่อใช้งานในอินเตอร์เน็ตคาเฟ่มาแล้ว ในการวิเคราะห์ปัญหาดังกล่าวจะทำได้โดยการแยกแยะในเบื้องต้นว่าระบบที่ใช้มีองค์ประกอบย่อยและการทำงานอะไรบ้าง แล้วพิจารณาว่าองค์ประกอบหรือการทำงานเหล่านั้นทำให้เกิดปัญหาอะไรขึ้นได้บ้าง ดังตารางที่ 1

องค์ประกอบ	การทำงาน	กรณีปัญหาที่อาจเกิดขึ้นได้
ฮาร์ดแวร์	เครื่องคอมพิวเตอร์ของร้านบริการซึ่งให้บริการกับบุคคลทั่วๆ ไป	ระบบคอมพิวเตอร์ของร้านค้ามีเสถียรภาพต่ำ อาจมีอุปกรณ์ชำรุด และระบบไฟฟ้าไม่

		มีความเสถียร ความน่าเชื่อถือในระบบต่ำ
ซอฟต์แวร์	ซอฟต์แวร์ระบบ โปรแกรมอินเตอร์เน็ตบราวเซอร์ที่ใช้ ระบบปลายทาง	ซอฟต์แวร์ระบบติดตั้งโดยใช้การติดตั้งตามค่าเริ่มต้น(Default) ไม่มีการปรับแต่งค่าให้ปลอดภัย หรือการป้องกันที่ดีเท่าที่ควร ความน่าเชื่อถือในระบบต่ำ ซอฟต์แวร์ต่างๆ มีช่องโหว่ที่ต้องแก้ไข
ระบบเครือข่าย	เครือข่ายของร้านให้บริการกับผู้ใช้งานทั่วๆไป	ไม่สามารถบ่งบอกถึงจุดประสงค์ของผู้ใช้งานแต่ละคนได้ ความน่าเชื่อถือในเครือข่ายต่ำ โพรโตคอลต่างๆ มีปัญหาความปลอดภัย
การใช้งานระบบ	ใช้บริการในสถานที่สาธารณะ	การดักจับข้อมูลสำคัญทำได้ง่ายดายโดยการอ่าน และการแอบดูรหัสผ่าน

ตารางที่ 1 การวิเคราะห์ปัญหาความปลอดภัยเบื้องต้น

ปัญหาต่างๆ ที่เกิดขึ้นในระบบ

ในระบบสารสนเทศซึ่งประกอบด้วยองค์ประกอบที่หลากหลาย ไม่ว่าจะเป็นฮาร์ดแวร์ที่มีความหลากหลายสูง ระบบซอฟต์แวร์ที่ต้องมีการทำงานสอดประสานกันระหว่างระบบปฏิบัติการ และระบบเครือข่ายที่มีการใช้อุปกรณ์เครือข่าย และโพรโตคอลทางเครือข่ายที่แตกต่างกันมาทำงานร่วมกัน จากองค์ประกอบเหล่านี้เมื่อพิจารณาการทำงานในส่วนย่อยแล้วจะพบว่ามีปัญหาด้านความปลอดภัยอยู่มากเช่นกัน

สำหรับโพรโตคอลต่างๆ ที่ใช้งานกันอยู่ในปัจจุบัน ไม่ว่าจะเป็นโพรโตคอล IP ในชั้น Network Layer โพรโตคอล TCP และ UDP ในชั้น Transport Layer โพรโตคอลต่างๆ ในชั้นที่สูงขึ้นไปเช่น HTTP, SMTP ในชั้น Application Layer หรือแม้กระทั่ง IEEE 802.11 และ Bluetooth ในโลกของเครือข่ายไร้สาย ต่างก็มีช่องโหว่

ที่ทำให้เกิดการโจมตีได้ทั้งสิ้น ไม่ว่าจะเป็นปัญหาการดักจับข้อมูล การปลอมแปลงข้อมูล การเข้าใช้งานระบบโดยไม่ขออนุญาต การโจมตีเพื่อปิดบริการโดยใช้โพรโตคอลต่างๆ

สำหรับในระบบคอมพิวเตอร์ซึ่งประกอบด้วยโปรแกรมระบบ หรือระบบปฏิบัติการเช่น Microsoft Windows, Linux และโปรแกรมสำหรับการใช้งานต่างๆ เช่น Office, Internet Browser ต่างก็มีจุดบกพร่องที่ต้องทำการ patch เพื่อปิดช่องโหว่อยู่เสมอๆ เช่นกันซึ่งเราจะสังเกตได้จากในระบบปฏิบัติการ หรือโปรแกรมต่างๆ มักจะมีการทำงานในลักษณะ Live Update ติดมากับระบบหรือโปรแกรมนั้นๆ เสมอ เมื่อใดก็ตามที่ระบบมีการทำ Live Update ที่มีนัยสำคัญสูงสุดจะหมายถึงเกิดช่องโหว่ที่ต้องรีบแก้ไขโดยทันทีนั่นเอง

ในการใช้งานระบบซึ่งขึ้นอยู่กับนโยบายการใช้งานของหน่วยงานหรือนิสัยการใช้งานของผู้ใช้งาน ก็อาจทำให้เกิด ก็อาจทำให้เกิดปัญหาความปลอดภัยในระบบคอมพิวเตอร์ได้เช่นกัน โดยเฉพาะอย่างยิ่งในสถานที่ใช้งานระบบแบบ open เช่นอินเตอร์เน็ตคาเฟ่ที่ให้บริการกับบุคคลทั่วไป จะเป็นสถานที่ให้บริการที่ไม่มีกฎการใช้งาน หรือนโยบายการให้บริการใดๆ ทำให้เกิดปัญหาความปลอดภัยเช่นไวรัส เวิร์ม การขโมยรหัสผ่าน การขโมยข้อมูลภายในร้านอินเตอร์เน็ตคาเฟ่อยู่เป็นประจำ หรือแม้กระทั่งในที่ทำงานซึ่งการดูแลระบบหละหลวม ก็มักจะเกิดการกระจายตัวของไวรัสและการเจาะระบบอยู่เสมอๆ ยิ่งร้ายไปกว่านั้น ระบบสารสนเทศขนาดใหญ่ที่ขาดแคลนบุคลากรที่มีความรู้ความสามารถเพียงพอ ก็จะตกเป็นเหยื่อของผู้ไม่หวังดีที่จะเจาะระบบเพื่อขโมยข้อมูลหรือทำลายข้อมูลได้โดยง่าย โดยเฉพาะอย่างยิ่งหน่วยงานราชการที่ระบบต้องทำงานตลอด 24 ชั่วโมงแต่จะมีช่วงเวลาในการดูแลระบบอยู่จำกัดเฉพาะเวลาทำงานเท่านั้น

<u>ทำความรู้จัก Confidentiality, Integrity และ Availability (CIA)</u>

เมื่อพิจารณาถึงปัญหา ในระบบโดยเฉพาะปัญหาที่เกิดจากระบบเครือข่าย และซอฟต์แวร์ต่างๆ โดยทั่วๆ ไปจะเกิดจากโพรโตคอล หรือซอฟต์แวร์เหล่านั้นไม่ได้ถูกออกแบบมาเพื่อการใช้งานอย่างปลอดภัย แต่ออกแบบมาเพื่อการใช้งานที่หลากหลายของผู้ใช้งานมากกว่า โดยโพรโตคอลต่างๆ ถูกออกแบบมาเพื่อเชื่อมต่อเครือข่ายต่างๆ เข้าด้วยกันและโปรแกรมต่างๆ ที่ใช้งานกันอยู่ในปัจจุบันถูกออกแบบมาเพื่อใช้งานเท่านั้น โดยขาดความสามารถในการรักษาความปลอดภัยในระบบ และการใช้งานระบบ

ในระบบที่มีความปลอดภัยสูง จำเป็นต้องออกแบบให้ระบบหรือองค์ประกอบโดยรวมของระบบ มีการทำงานใน 3 ลักษณะคือ มีกระบวนการในการสร้างความเชื่อมั่นให้กับผู้ใช้งานระบบว่าการใช้งานและข้อมูลต่างๆ จะต้องเป็นความลับ (Confidentiality) มีข้อมูลมีความถูกต้อง (Integrity) และสามารถใช้งานได้เมื่อต้องการ (Availlability) ซึ่งถ้าระบบใดๆ มีการออกแบบและพัฒนาขึ้นโดยคำนึงถึงปัจจัยทั้ง 3 ข้อนี้จะทำให้ระบบหรือการทำงานนั้นมีความปลอดภัยมากขึ้น

สำหรับ Confidentiality จะหมายถึงการทำงานใดๆ ที่ผู้ใช้งานดำเนินอยู่และข้อมูลใดๆ จะเป็นความลับไม่เปิดเผย ข้อมูลต่างๆ ที่ส่งผ่านระหว่างระบบจะต้องไม่ถูกดักจับไปใช้ประโยชน์ได้ การสร้าง Confidentiality ให้เกิดขึ้นมาในระบบได้นั้น สามารถทำได้โดยการเพิ่มกระบวนการเข้ารหัสลับ (Encryption) ในขณะที่ส่งข้อมูลจากจุดหนึ่งไปยังอีกจุดหนึ่ง ในการรับส่งข้อมูลที่ถูกเข้ารหัสแล้วนั้น ผู้ที่ดักจับข้อมูลไปจะไม่สามารถใช้งานข้อมูลนั้นๆ ได้เนื่องจากข้อมูลดังกล่าวจะเป็นข้อมูลที่ไม่สามารถแปลความหมายได้ด้วยโปรแกรมใดๆ

ในประเด็นทางด้าน Integrity จะหมายถึงการทำงานใดๆ หรือข้อมูลใดๆ ที่ผู้ใช้งานจะได้รับ จะต้องมีความถูกต้องไม่มีการเปลี่ยนแปลง เป็นข้อมูลที่เหมือนกับข้อมูลที่ส่งมาจากแหล่งข้อมูลต้นทาง ในการสร้าง Integrity ให้เกิดขึ้นในการทำงาน สามารถทำได้โดยการเพิ่มข้อมูลเพิ่มเติมสำหรับตรวจสอบความถูกต้องของข้อมูลต้นฉบับและมีกระบวนการในการตรวจสอบข้อมูลก่อนการใช้งาน โดยกระบวนการที่ใช้คือ Message Integrity Code ได้แก่การทำ CheckSum , MD5 , SHA , SHA1 ,MAC และ Digital Signature โดยกระบวนการดังกล่าวจะมีขั้นตอนในการสร้างข้อมูลเพิ่มเติมสำหรับตรวจสอบความถูกต้องของข้อมูลต้นฉบับ และกระบวนการที่ใช้ในการตรวจสอบ

ในการทำให้ระบบมี Availlability จำเป็นต้องมีกระบวนการต่างๆ เพื่อสร้างให้ระบบมีเสถียรภาพและสามารถตอบสนองต่อการร้องขอบริการจากผู้ใช้งานได้ ซึ่งจำเป็นต้องพึ่งพากระบวนการต่างๆ เพื่อให้ผู้ใช้งานสามารถระบบทำงานได้อย่างต่อเนื่องได้แก่

1. Access Control เพื่อควบคุมไม่ให้การโจมตีใดๆ เข้าสู่ระบบ รวมถึงการควบคุมการเข้าถึงการทำงาน โปรแกรม หรือข้อมูลใดๆ โดยจะอนุญาตเฉพาะบุคคลเท่านั้นที่จะผ่านและใช้งานได้ การใช้งานระบบคอมพิวเตอร์จะมีการทำ Access Control โดยจะควบคุมการเข้าใช้งานของผู้ใช้งานโดยใช้ระบบบัญชีผู้ใช้ การเข้าถึงระบบจะต้องมีการกรอกรหัสผ่าน เป็นต้น สำหรับระบบเครือข่ายจะทำ Access Control

โดยควบคุมการเชื่อมต่อจากเครื่องคอมพิวเตอร์ต้นทางไปยังเครื่องคอมพิวเตอร์ปลายทางโดยใช้ Firewall ซึ่ง Identity ในที่นี้คือหมายเลขไอพีแอดเดรสของเครื่องคอมพิวเตอร์ต้นทางและปลายทาง เป็นต้น

2. การ Monitor และการตรวจตราระบบ เพื่อให้ทราบความเสี่ยงต่างๆ ที่อาจทำให้ระบบหยุดการทำงาน และสามารถดำเนินการแก้ไขได้อย่างทันท่วงที
3. การออกแบบระบบคอมพิวเตอร์และเครือข่ายให้มีความทนทานสูง เพื่อให้ระบบสามารถให้บริการกับความต้องการต่างๆ ของผู้ใช้งานได้อย่างเพียงพอ และเหมาะสม ตลอดจนทำให้ระบบสามารถดำเนินการได้อย่างต่อเนื่อง
4. การวางแผนการบริหารความเสี่ยงและการประเมินความเสี่ยง เพื่อทำให้ทราบความเสี่ยงในระบบและดำเนินการปรับลดความเสี่ยงต่างๆ ในระบบให้อยู่ในขอบเขตที่เหมาะสม
5. การกำหนดนโยบายการรักษาความปลอดภัยตามมาตรฐานสากล เพื่อให้ระบบสามารถทำงานได้อย่างปลอดภัยตามมาตรฐานสากล
6. การพัฒนาบุคลากรให้มีความสามารถ เพื่อลดความเสี่ยงของปัญหาต่างๆ ที่จะเกิดขึ้นในระบบ

การประยุกต์ใช้ CIA เพื่อเพิ่มความปลอดภัยในระบบเครือข่าย

ในการเพิ่มความปลอดภัยให้กับระบบเครือข่าย ทำได้โดยการเพิ่มกระบวนการของ CIA ในโพรโตคอลต่างๆ ที่ใช้ในปัจจุบันให้มีความปลอดภัยมากขึ้นดังตัวอย่างในตารางที่ 2

การทำงาน	เทคนิคที่เพิ่มความปลอดภัย	CIA ที่เพิ่มขึ้น
IP	IP Security	Confidentiality , Integrity
Web	Secure Socket Layer	Confidentiality , Integrity
IEEE 802.11	WEP,WPA,WPA2	Confidentiality , Integrity
IEEE 802.11	MAC Address Filtering	Availability
Network Flow	Firewall	Availlability

ตารางที่ 2 การเพิ่มความปลอดภัยให้กับการทำงานต่างๆ ในระบบโดยยึดหลัก CIA

ถึงแม้ว่า CIA เป็นกระบวนการที่ช่วยให้ระบบมีความปลอดภัยมากขึ้นและสามารถประยุกต์เข้ากับงานทั่วๆ ไปเพื่อเพิ่มความปลอดภัยให้ระบบได้ แต่การทำงานหลายอย่างไม่สามารถเพิ่ม CIA เข้าไปในระบบได้โดยตรงเนื่องจากมีการใช้งานอยู่ในปัจจุบันและไม่สามารถปรับเปลี่ยนการใช้งานได้โดยง่ายเช่น โพรโตคอลพื้นฐานต่างๆ ที่ใช้งานในปัจจุบัน ระบบเครือข่ายที่มีความเกี่ยวข้องกับหน่วยงานหลายหน่วยงานทำให้ไม่สามารถดำเนินการปรับเปลี่ยนอุปกรณ์และโพรโตคอลต่างๆ ได้ง่ายนัก การเพิ่ม CIA ในระบบจึงไม่สามารถทำได้ ระบบการทำงานยังต้องใช้โพรโตคอลที่ยังมีช่องโหว่ ทำให้ยังมีการโจมตีผ่านเครือข่ายรูปแบบต่างๆ , ระบบปฏิบัติการทำให้ยังมี Virus Worm ต่างๆ และกระบวนการทำงานบางอย่างของผู้ใช้งานระบบตามความเคยชินจึงทำให้ต้องมีการดูแลระบบอย่างสม่ำเสมอ ดังนั้นการทำงานของผู้ดูแลระบบจึงต้องมีหน้าที่และความสามารถต่างๆ ดังต่อไปนี้

1. ต้องทราบความสามารถของอุปกรณ์เครือข่าย และระบบของตนเองว่าต้องการการรักษาความปลอดภัยในระบบได้อย่างไรบ้าง
2. สามารถใช้งานเครื่องมือต่างๆ เพื่อช่วยดูแลระบบให้ปลอดภัยมากขึ้น

3. ต้องมีความรู้ความสามารถในการวิเคราะห์ถึงปัญหาทางด้านความปลอดภัยกับบริการเฉพาะเช่น การบริการเว็บไซต์ การบริการเครือข่ายไร้สาย และบริการเฉพาะอื่นๆ
4. มีความรู้ทางเทคนิคต่างๆที่จำเป็นในระบบ
5. สามารถการควบคุมดูแลการใช้งานระบบของผู้ใช้งานระบบโดยการวางแผนการรักษาความปลอดภัยและประกาศใช้นโยบายต่างๆ

บทที่ 2. ปัญหาด้านความปลอดภัยที่เกิดขึ้นในระบบเครือข่าย

ในการพัฒนาระบบเครือข่ายสำหรับระบบสารสนเทศจำเป็นต้องใช้องค์ประกอบสองส่วนด้วยกันคือ โพรโตคอลต่างๆ ที่ให้บริการในระบบ และอุปกรณ์เครือข่ายต่างๆ ซึ่งปัญหาด้านการรักษาความปลอดภัยในระบบจำเป็นต้องพิจารณาถึงจุดบกพร่องต่างๆ ในโพรโตคอลตลอดจนการดูแลและตั้งค่าความปลอดภัยในอุปกรณ์ต่างๆ

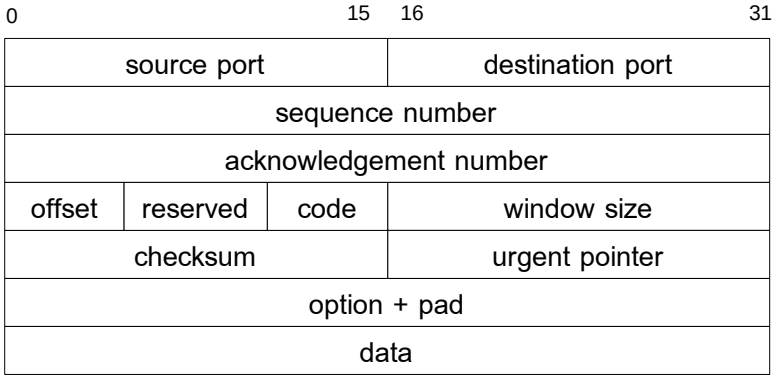
โพรโตคอลที่ใช้ในระบบเครือข่ายได้แก่โพรโตคอล TCP, IP, UDP, ICMP, IEE802.3, HTTP, FTP และโพรโตคอลอื่นๆ อีกมากมาย ซึ่งแต่ละโพรโตคอลถูกออกแบบมาเพื่อจุดประสงค์ในการเชื่อมต่อเท่านั้น โดยไม่ได้มองถึงปัญหาด้านการรักษาความปลอดภัยเลย ทำให้เกิดปัญหาต่างๆ ตามมาในภายหลัง นอกจากนี้อุปกรณ์เครือข่ายเช่น Hub , Switch , Router จะมีรูปแบบการทำงานและการดูแลที่แตกต่างกัน ซึ่งการทำงานต่างๆ จะมีจุดบกพร่องอยู่เช่นกัน ซึ่งจำเป็นต้องมีการตั้งค่าต่างๆ เพื่อป้องกันระบบด้วย

<u>โพรโตคอลเครือข่าย ช่องโหว่ และแนวทางการป้องกัน</u>

ในการทำงานของระบบคอมพิวเตอร์และเครือข่ายมีการใช้งานโพรโตคอลต่างๆ มากมาย แต่โดยการทำงานหลักของระบบทั้งหมดจะอยู่ที่โพรโตคอล TCP, UDP, IP และ ICMP ที่ใช้งานกันอย่างมากในอินเตอร์เน็ต นอกจากนี้ยังมี IEEE 802.11 ที่จำเป็นต้องใช้ในการใช้งานระบบเครือข่ายไร้สายด้วย ในหัวข้อนี้จะทำการศึกษาการทำงานทั่วๆไปของโพรโตคอลเหล่านั้น วิเคราะห์ปัญหาที่เกิดขึ้น และนำเสนอแนวทางการป้องกัน

Transmission Control Protocol : TCP

โพรโตคอลทีซีพีเป็นโพรโตคอลที่มีการใช้งานสูงมาก เพราะเป็นโพรโตคอลที่มีความสามารถในการรับประกันการส่งข้อมูล (Guarantee Delivery) โดยสามารถตรวจสอบความผิดปกติของข้อมูลที่ส่ง และส่งซ้ำเมื่อพบความผิดปกติ สามารถรับรองความครบถ้วนของข้อมูลที่ส่ง เช่น หากส่งข้อมูลเป็นไฟล์ขนาด 10 กิโลไบต์ โพรโตคอลทีซีพีจะแบ่งข้อมูลออกเป็นส่วน ๆ เรียกว่า เซ็กเมนต์ (Segment) เช่น หากกำหนดให้ขนาดของเซ็กเมนต์เป็น 1 กิโลไบต์ ก็จะต้องส่งทั้งหมด 10 ครั้ง ในการส่ง 10 ครั้งนี้ หากมีความผิดพลาดเกิดขึ้นที่เซ็กเมนต์ใด ก็จะส่งเซ็กเมนต์นั้นใหม่ และหากไม่สามารถส่งให้ครบได้ ก็จะแจ้งความผิดพลาด โดยจะไม่มีกรณีที่รับข้อมูลได้ไม่ครบถ้วนอย่างเด็ดขาด โดยรูปแบบเซ็กเมนต์ของทีซีพี แสดงดัง รูปที่ 1



รูปที่ 1 *เซ็กเมนต์ของทีซีพี*

สำหรับรายละเอียดต่างๆ ในเซ็กเมนต์ของทีซีพีมีรายละเอียดดังนี้

- Source Port มีขนาด 16 บิต เป็นหมายเลขพอร์ตของฝั่งต้นทาง
- Destination Port มีขนาด 16 บิต เป็นหมายเลขพอร์ตของฝั่งปลายทาง
- Sequence Number มีขนาด 32 บิต ใช้ในการบอกลำดับการส่งของเซ็กเมนต์ในการส่งชุดเดียวกัน รายละเอียดจะอธิบายในหัวข้อการสร้างการเชื่อมต่อและการส่งข้อมูล
- Acknowledgement Number มีขนาด 32 บิต ใช้บอกการตอบรับในการรับชุดเดียวกัน รายละเอียดจะอธิบายในหัวข้อการสร้างการเชื่อมต่อและการส่งข้อมูล
- Offset มีขนาด 4 บิต บอกตำแหน่งเริ่มต้นของข้อมูล หรือ จุดสิ้นสุดของส่วนเฮดเดอร์ ดังนั้นจึงใช้บอกขนาดของเฮดเดอร์ได้ ค่าของข้อมูลเป็นหน่วยของ 4 ไบต์ เช่น หากมีค่า 5 หมายถึงเฮดเดอร์ยาว 20 ไบต์

- Reserved มีขนาด 4 บิต สำรองใช้ในอนาคต
- Code มีขนาด 8 บิต ประกอบด้วย 6 ฟิลด์ย่อย ดังรูปที่ 2

URG	ACK	PSH	RST	SYN	FIN	N/A	N/A

รูปที่ 2 บิตควบคุมการทำงานของโพรโตคอลทีซีพี

  - URGent ใช้บอกว่ามีข้อมูลเร่งด่วน โดยหากบิตนี้มีค่าเป็น 1 หมายถึง ในฟิลด์ Urgent Pointer มีข้อมูลเร่งด่วนบรรจุอยู่
  - ACKnowledgement ใช้บอกการตอบรับการส่งข้อมูล โดยหากเซ็กเมนต์ใดที่มีบิตนี้เป็น 1 หมายความว่าเซ็กเมนต์นั้นบรรจุข้อมูลการตอบรับเอาไว้
  - PuSH ใช้บอกความเร่งด่วน โดยหากเซ็กเมนต์ใดที่บิตนี้เป็น 1 หมายความว่าให้ส่งเซ็กเมนต์นั้นไปยังระดับชั้นแอปพิลเคชันทันที โดยไม่ต้องรอให้บัฟเฟอร์เต็ม บิตนี้จะมีประโยชน์สำหรับแอปพลิเคชันที่ต้องการการตอบสนองที่รวดเร็ว เช่น โปรแกรมเทลเน็ต เป็นต้น
  - ReSeT ใช้ในการยกเลิกการเชื่อมต่อครั้งนี้ โดยหากบิตนี้เป็น 1 หมายถึงให้ยกเลิกการเชื่อมต่อครั้งนี้ไปก่อน อาจเนื่องจากความผิดพลาด และหากต้องการส่งข้อมูลต่อ ก็จะต้องสร้างการเชื่อมต่อขึ้นใหม่
  - SYNchronize ใช้ในการสร้างการเชื่อมต่อ จะกล่าวถึงรายละเอียดในเรื่องการสร้างการเชื่อมต่อ
  - FINish ใช้ในการจบการเชื่อมต่อ โดยบิตนี้ของเซ็กเมนต์ใดที่มีค่าเป็น 1 หมายถึง ให้สิ้นสุดการเชื่อมต่อ บิตนี้จะต่างจาก Reset ตรงที่บิตนี้จะหมายถึงจบการเชื่อมต่อแบบถาวร ในขณะที่ Reset มักจะใช้ในการจบการเชื่อมต่อชั่วคราว
- Window Size มีขนาด 16 บิต ใช้ในการกำหนดขนาดของบัฟเฟอร์ที่ใช้ในการเชื่อมต่อแต่ละครั้ง
- Checksum มีขนาด 16 บิต ใช้ในการตรวจสอบความผิดปกติของเซ็กเมนต์ ซึ่งส่วนของ Checksum ของทีซีพีจะต่างจากไอพี เพราะ Checksum ของทีซีพีเป็นการตรวจสอบทั้งส่วนหัวและส่วนข้อมูล

- Urgent Pointer ทำหน้าที่เป็นตัวชี้ตำแหน่งในส่วนข้อมูล ที่เป็นข้อมูลเร่งด่วน เพื่อให้แอปพลิเคชั่นสามารถนำข้อมูลนั้นไปใช้ทันที
- Options มีขนาดไม่แน่นอน ใช้ในการกำหนดงานเพิ่มเติมให้กับทีซีพี
- Pad มีขนาด 0-3 ไบต์ ใช้เพิ่มส่วนที่เหลือของ Options เพื่อให้ส่วนหัวของเฮดเดอร์หารด้วย 4 ลงตัว
- Data เป็นส่วนข้อมูลของทีซีพี

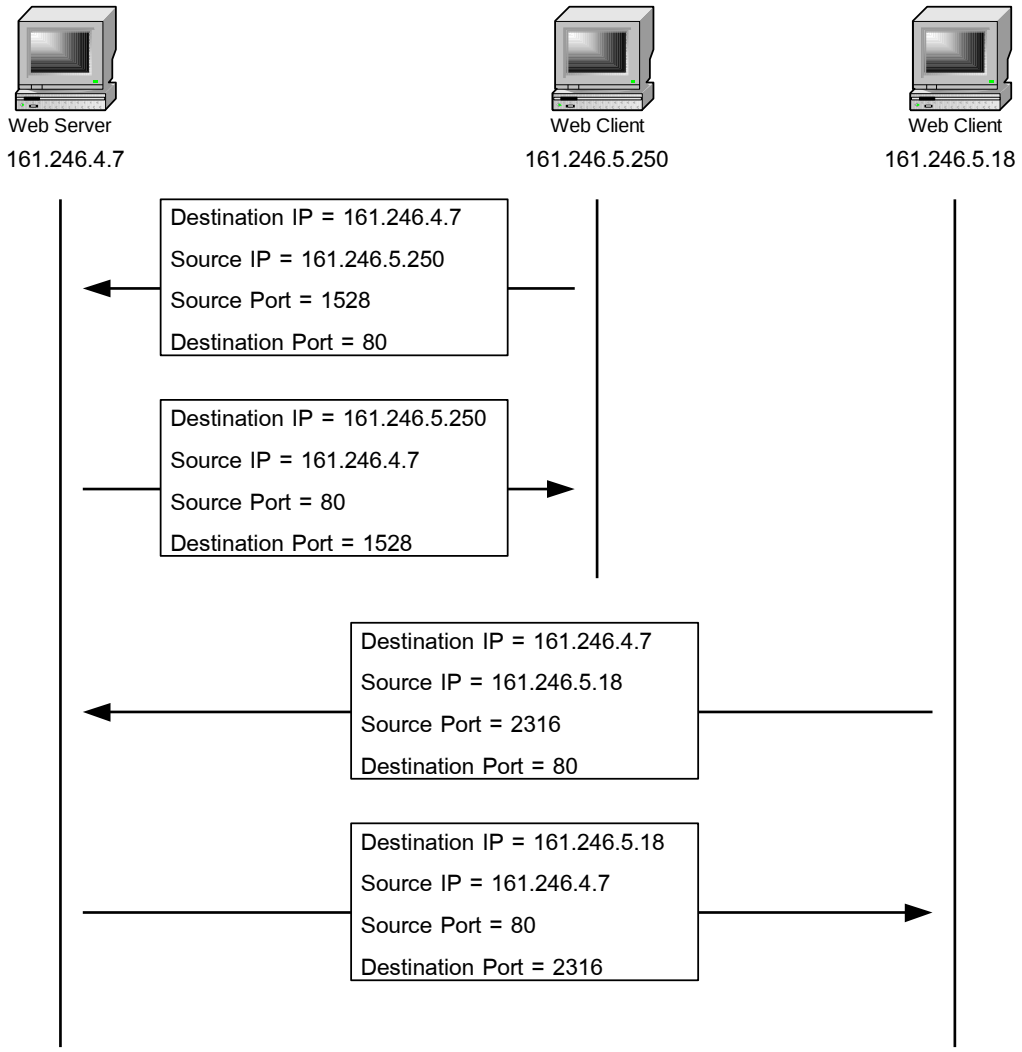
เนื่องจากทีซีพีมีภาระหน้าที่ที่ต้องรับผิดชอบมาก โดยต้องส่งข้อมูลอย่างถูกต้อง ไม่มีข้อผิดพลาด การทำงานของทีซีพีจึงมีความซับซ้อน โดยเฉพาะบทบาทของแฟล็กต่าง ๆ ในฟิลด์ Code ดังนั้นเพื่อให้เข้าใจการทำงานมากขึ้น จะอธิบายการทำงานในแต่ละขั้นตอน

พอร์ตและหน้าที่ของพอร์ต

เซ็กเมนต์ของทีซีพีจะเริ่มต้นด้วยพอร์ตต้นทางและพอร์ตปลายทาง พอร์ตถือเป็นช่องทางการสื่อสารที่ทำหน้าที่แยกข้อมูลที่สื่อสารกับแต่ละแอปพลิเคชันออกจากกัน และส่งไปยังแต่ละแอปพลิเคชันได้อย่างถูกต้อง เช่น สมมติว่ามีเครื่องเซิร์ฟเวอร์หนึ่ง ที่ทำหน้าที่เป็นทั้งเว็บเซิร์ฟเวอร์และเมล์เซิร์ฟเวอร์ แพ็กเกจไอพีที่มาขอใช้บริการเว็บและเมล์จากเซิร์ฟเวอร์นี้ ย่อมต้องใช้หมายเลข ไอพีเดียวกัน แต่เมื่อแพ็กเกจไอพีมาถึงเซิร์ฟเวอร์นี้ เซิร์ฟเวอร์จะต้องแยกแพ็กเกจออกจากกัน เพื่อส่งไปยังโปรแกรมเว็บเซิร์ฟเวอร์ และโปรแกรมเมล์เซิร์ฟเวอร์ได้อย่างถูกต้อง การแยกแพ็กเกจออกจากกันนี้จะดูจากหมายเลขพอร์ต

ในแพ็กเกจที่ส่งมายังเว็บเซิร์ฟเวอร์นั้น จะระบุหมายเลขพอร์ตปลายทางเป็น 80 แต่แพ็กเกจที่ส่งมายังเมล์เซิร์ฟเวอร์จะระบุหมายเลขพอร์ตปลายทางเป็น 25 ดังนั้นเมื่อเซิร์ฟเวอร์พิจารณาจากหมายเลขพอร์ตปลายทาง ก็จะสามารถส่งแพ็กเกจที่เข้ามา ไปยังแอปพลิเคชันที่เหมาะสมได้ นี่เป็นหน้าที่ของพอร์ตปลายทาง แต่สำหรับพอร์ตต้นทางนั้น หน้าที่จะต่างออกไป ทั้งนี้เนื่องจากในการขอใช้บริการใด ๆ จากเซิร์ฟเวอร์นั้น เพียงระบุหมายเลขพอร์ตปลายทางให้ถูกต้อง ก็ย่อมจะสามารถเข้าถึงแอปพลิเคชันนั้น และขอใช้บริการได้ ดังนั้นใน

การขอใช้บริการพอร์ตต้นทางดูเหมือนไม่มีความจำเป็น ดังนั้นเพื่อให้เข้าใจหน้าที่ของพอร์ตต้นทาง ขอให้ดูรูปตัวอย่างการทำงานของการติดต่อระหว่างเซิร์ฟเวอร์กับไคลเอนต์ดังรูปที่ 3



รูปที่ 3 ตัวอย่างการติดต่อระหว่างเซิร์ฟเวอร์และไคลเอนต์

จากรูปที่ 3 แสดงการติดต่อไปยังเว็บเซิร์ฟเวอร์ที่มีหมายเลขไอพีแอดเดรส 161.246.4.7 โดยในการติดต่อครั้งแรกมาจากเครื่องที่มีไอพี 161.246.5.250 โดยจะเห็นว่ามีพอร์ตปลายทางเป็น 80 ซึ่งหมายถึงพอร์ตของเว็บ (Server Port) สำหรับพอร์ตต้นทางนั้น (Client Port) เครื่องไคลเอนต์จะสุ่มขึ้นมา เพื่อให้ฝั่งเซิร์ฟเวอร์ใช้เป็นพอร์ตปลายทางเมื่อส่งข้อมูลกลับมา ดังนั้นจะเห็นได้ว่าในการติดต่อครั้งหลังของไคลเอนต์ 161.246.5.18 นั้นจะ

มีหมายเลขพอร์ตต้นทางเป็นคนละหมายเลขกัน เพราะเป็นการเลือกค่าแบบสุ่ม และในกรณีที่เครื่องไคลเอนต์เปิดโปรแกรมเว็บบราวเซอร์ขึ้นมาหลาย ๆ วินโดว์นั้น แต่ละวินโดว์ของเว็บบราวเซอร์ก็จะใช้หมายเลขพอร์ตต้นทางเป็นคนละหมายเลขกันอีกด้วย ทั้งนี้เพื่อให้เครื่องไคลเอนต์สามารถแยกได้ว่า ข้อมูลที่ส่งมาจากเว็บเซิร์ฟเวอร์เป็นข้อมูลที่ส่งมาให้ที่โปรแกรมเว็บบราวเซอร์ในวินโดว์ใด

ดังนั้นจะเห็นได้ว่าพอร์ตนั้นเป็นหมายเลขที่ใช้ในการแยกข้อมูลที่ส่งมายังคอมพิวเตอร์นั้น ๆ ให้ส่งไปยังปลายทางที่ถูกต้องได้ และเนื่องจากตัวเลขที่ใช้ระบุพอร์ตมีขนาด 16 บิต ดังนั้นจึงสามารถมีค่าได้ตั้งแต่ 1-65534 (ค่า 0 กับ 65535 ไม่ใช้) แต่โดยทั่วไปแล้ว พอร์ตที่มีหมายเลขตั้งแต่ 1-1024 จะเป็นพอร์ตของแอปพลิเคชันพื้นฐาน ดังนั้นพอร์ตต้นทางที่เกิดจากการสุ่มก็จะไม่สุ่มให้มีหมายเลขน้อยกว่า 1024 โดยทั่วไปหมายเลขของพอร์ตต้นทางที่เกิดจากการสุ่มมักมีค่าตั้งแต่ 1024-5000 แต่ก็มีบางแอปพลิเคชันที่ใช้งานพอร์ตหมายเลขมากกว่า 1024 เช่นกัน และบางแอปพลิเคชันก็สุ่มค่าที่มากกว่า 5000 ได้เช่นกัน

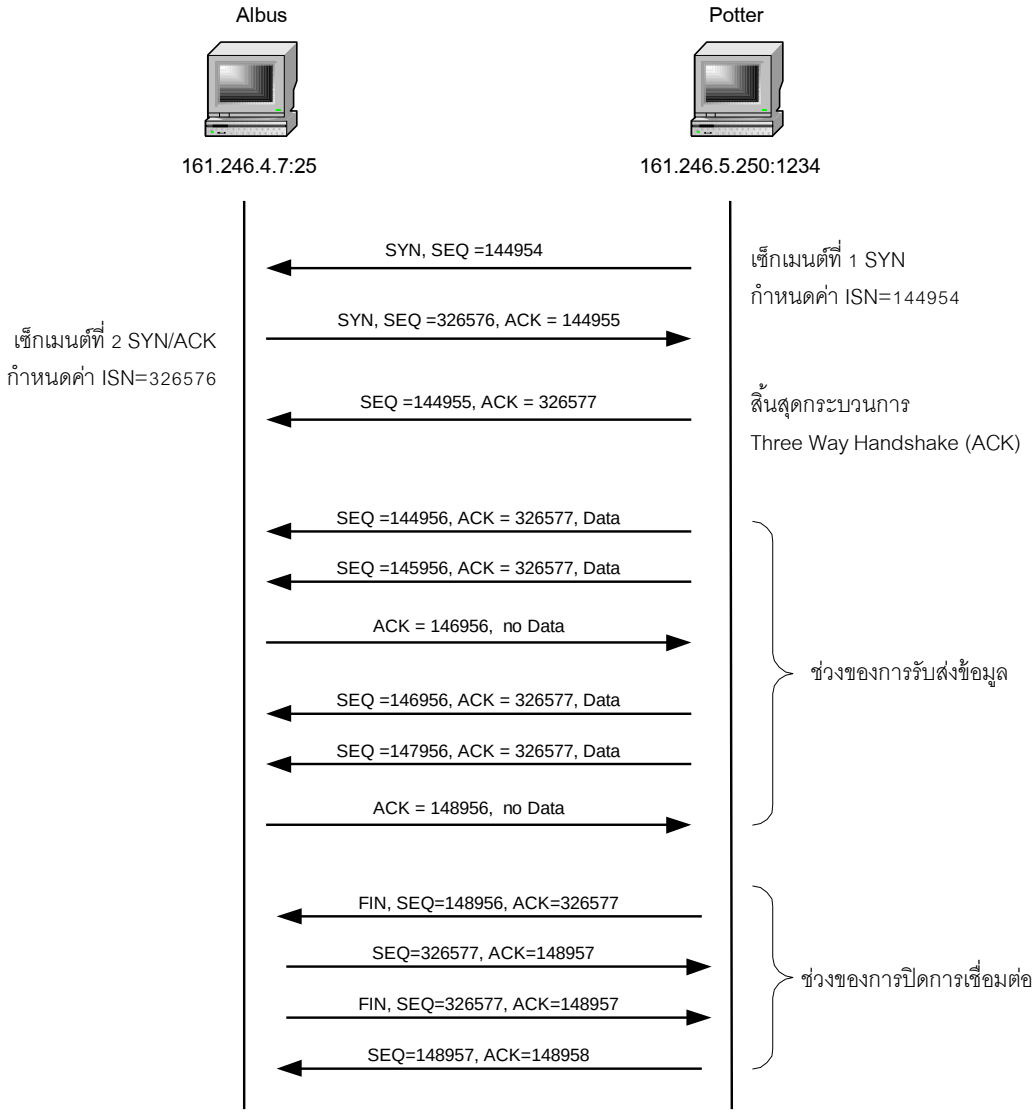
ดังนั้นในทุก ๆ เครื่องคอมพิวเตอร์ ก็จะมีพอร์ตที่สามารถเชื่อมต่อแบบทีซีพีได้ทั้งหมด 65534 พอร์ต แต่ไม่ได้หมายความว่าเครื่องของเราสามารถสื่อสารได้ทุกพอร์ต เพราะพอร์ตจะถูกใช้ก็ต่อเมื่อมีแอปพลิเคชันรอรับข้อมูลอยู่ที่พอร์ตนั้น ซึ่งเราจะเรียกพอร์ตที่มีแอปพลิเคชันรอรับข้อมูลว่า “พอร์ตเปิด” ดังนั้นจึงเรียกพอร์ตที่ไม่มีแอปพลิเคชันรอรับว่า “พอร์ตปิด” ดังนั้นพอร์ตที่เปิดอยู่ในเครื่องจึงหมายความถึงแอปพลิเคชันที่เปิดรออยู่ในเครื่องด้วย ดังนั้นหากเราทราบว่าคอมพิวเตอร์เครื่องนั้นมีพอร์ตอะไรเปิดอยู่บ้าง เราก็จะรู้ว่าคอมพิวเตอร์เครื่องนั้นรันโปรแกรมอะไรอยู่บ้าง หรือบางครั้งอาจทราบถึงว่าเป็นเครื่องที่ใช้ระบบปฏิบัติการใด เพราะในระบบปฏิบัติการหนึ่ง จะมีการเปิดพอร์ตที่ไม่เหมือนกัน

อย่างไรก็ตามความสัมพันธ์ระหว่างแอปพลิเคชันกับพอร์ตไม่ได้เป็นสิ่งตายตัว แม้ว่าโดยทั่วไปเว็บเซิร์ฟเวอร์มักใช้พอร์ตหมายเลข 80 เป็นช่องทางในการติดต่อ แต่ก็ไม่มีใครห้ามหากเราต้องการใช้พอร์ตหมายเลขอื่นในการติดต่อกับเว็บ โดยเฉพาะกรณีที่เว็บนั้นใช้ในวงจำกัด ซึ่งจะทำให้ปลอดภัยมากขึ้นด้วย เพราะหากบุคคลภายนอกไม่ทราบว่าเว็บของเราติดต่อผ่านทางพอร์ตหมายเลขใด ก็จะติดต่อเข้ามายังเว็บของเราไม่ได้ นอกจากนั้นการปิดพอร์ต นอกเหนือจากความหมายของการไม่มีแอปพลิเคชันทำงานในพอร์ตนั้นแล้ว ปัจจุบันยังสามารถจะปิดพอร์ตผ่านโปรแกรมประเภทไฟร์วอลล์ที่ทำงานในเครื่องได้อีกด้วย จึงทำให้ความหมายของการปิดเปิดพอร์ตเปลี่ยนไป

การใช้งานพอร์ตต่าง ๆ ในปัจจุบันนั้น มีการใช้งานกันอย่างมากมาย นอกเหนือจากแอปพลิเคชันที่เราต้องการใช้แล้ว บางครั้งยังถูกเปิดจากระบบปฏิบัติการเอง ถูกเปิดจากแอปพลิเคชันที่ติดตั้งโดยไม่รู้ตัว และยังอาจถูกเปิดจากโปรแกรมประเภทโทรจันอีกด้วย ดังนั้นการตรวจสอบการใช้งานพอร์ต จึงเป็นสิ่งแรก ๆ ที่ควรทำในการสำรวจระบบ ทั้งในแง่ของการป้องกัน และทั้งในแง่ของการโจมตี

การสร้างการเชื่อมต่อ

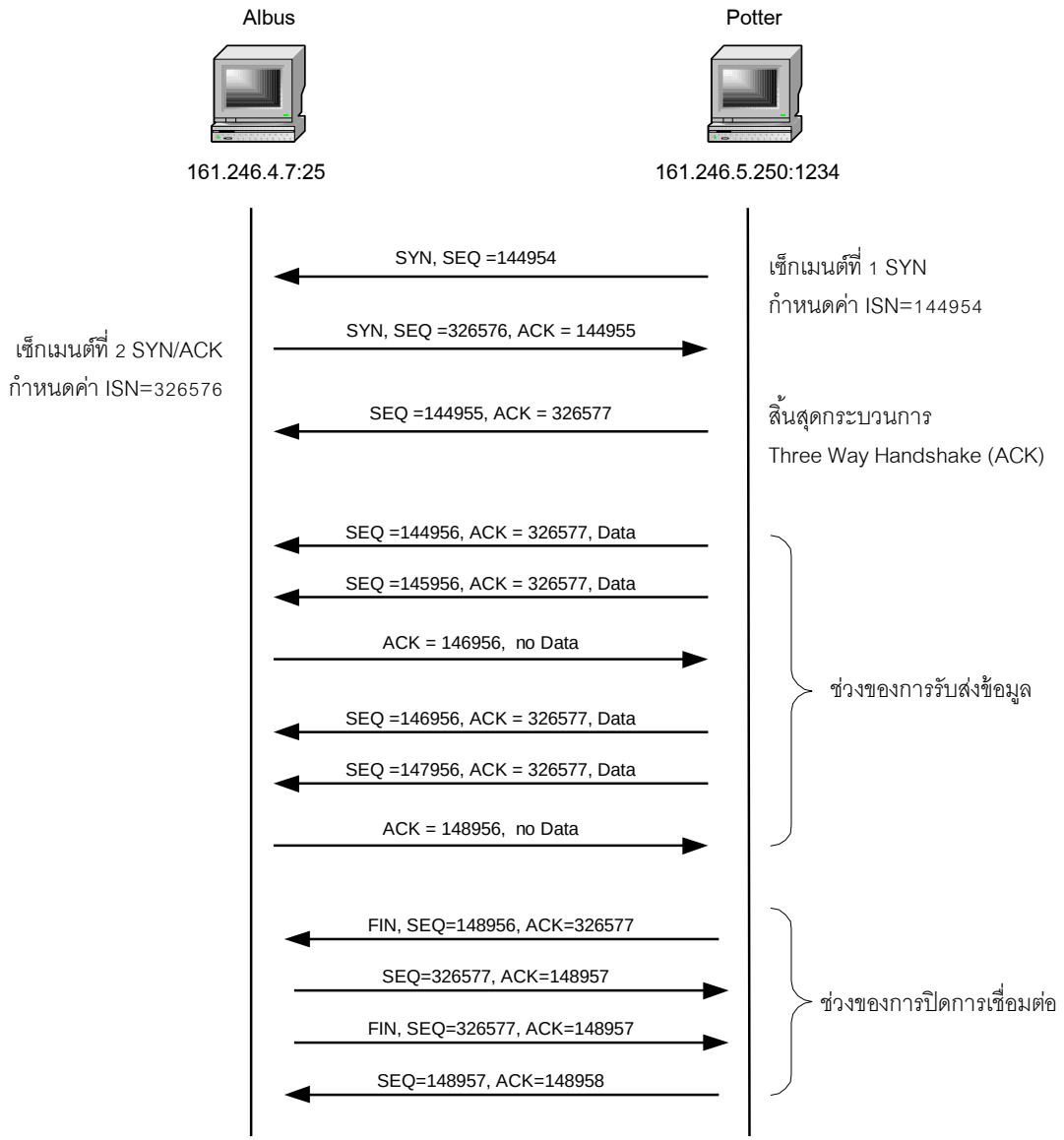
โพรโตคอลทีซีพีเป็นโพรโตคอลที่ทำงานในแบบที่ต้องสร้างการเชื่อมต่อขึ้นก่อนจึงจะส่งข้อมูลได้ (Connection Oriented) และต้องปิดการเชื่อมต่อเมื่อส่งข้อมูลเสร็จสิ้น ดังนั้นในกระบวนการเชื่อมต่อแบบทีซีพีเราอาจมองว่าประกอบด้วย 3 ขั้นตอนหลัก ได้แก่ ขั้นตอนสร้างการเชื่อมต่อ ขั้นตอนการส่งข้อมูล และ ขั้นตอนการปิดการเชื่อมต่อ สำหรับเหตุผลของการสร้างการเชื่อมต่อขึ้นก่อนจะส่งข้อมูลนั้น ก็เพื่อให้ทั้งฝั่งรับและฝั่งส่งมีการตั้งค่าพารามิเตอร์ที่เหมือนกัน และตระเตรียมบัพเฟอร์สำหรับการส่งข้อมูลให้มีขนาดเหมาะสมทั้ง 2 ฝั่ง



รูปที่ 4 ตัวอย่างการสร้างการเชื่อมต่อ

เพื่อให้สามารถเข้าใจการทำงานของการเชื่อมต่อแบบทีซีพี จะขอยกตัวอย่างประกอบการอธิบายดัง รูปที่ 4 โดยสมมติว่ามีคอมพิวเตอร์จำนวน 2 เครื่อง ต้องการติดต่อกัน โดยอาจเป็นการส่งไฟล์ ดังนั้นจะมีคอมพิวเตอร์เครื่องหนึ่งเป็นผู้ส่งข้อมูล และคอมพิวเตอร์อีกเครื่องหนึ่งเป็นผู้รับข้อมูล โดยจะตั้งชื่อคอมพิวเตอร์ทั้ง 2 ว่า Albus และ Potter โดย Potter จะเป็นฝ่ายเริ่มการติดต่อกับ Albus เพื่อขอส่งเมล์

ในขั้นแรก Potter จะต้องสุ่มเลือกเลขลำดับเริ่มต้น (Initial Sequence Number) เพื่อใช้เป็นเลขลำดับในการส่งข้อมูล จากนั้นจะส่งเซ็กเมนต์เริ่มการเชื่อมต่อไปยังเครื่อง Albus โดยจากรูปจะสมมติว่าเลขที่สุ่มได้จากเครื่อง Potter คือ 144954 โดยในเซ็กเมนต์นี้จะเซ็ตแฟล็ก SYN เอาไว้ด้วย เพื่อแสดงความหมายว่าต้องการเริ่มการติดต่อ จากนั้นเมื่อเครื่อง Albus ได้รับการติดต่อในลักษณะนี้ ก็สนองตอบกลับโดยการสุ่มหมายเลข ISN ในฝั่งของตัวเองขึ้นมาชุดหนึ่งเช่นกัน โดยในรูปจะเป็นหมายเลข 326576 จากนั้นก็ส่งเซ็กเมนต์กลับโดยเซ็ตแฟล็ก ACK เพื่อแสดงการตอบรับการเชื่อมต่อ และแฟล็ก SYN เพื่อให้ฝั่งผู้ร้องขอการเชื่อมต่อส่งการยืนยันกลับมา โดยในเซ็กเมนต์ที่ส่งนี้จะใช้เลขลำดับเป็นเลขลำดับที่สร้างขึ้น และใช้หมายเลขตอบรับเป็นหมายเลขลำดับของฝั่ง Potter บวกด้วย 1 เครื่อง Potter เมื่อได้รับเซ็กเมนต์ SYN/ACK นี้แล้ว ก็ยืนยันการเชื่อมต่อด้วยการส่งเซ็กเมนต์ ACK โดยเซ็ตแฟล็ก ACK เพื่อยืนยันการตอบรับ โดยใช้หมายเลขลำดับต่อจากหมายเลขลำดับก่อนหน้านี้ และใช้หมายเลขตอบรับเป็นหมายเลขลำดับของเซ็กเมนต์ที่ได้รับมาบวกด้วย 1 เมื่อการเชื่อมต่อมาถึงตรงนี้ ถือได้ว่าได้สร้างการเชื่อมต่อเสร็จสิ้นแล้ว และเรียกกระบวนการสร้างการเชื่อมต่อนี้ว่า Three Way Handshake



รูปที่ 5 แสดงการเชื่อมต่อตามขั้นตอนของ TCP

จากนั้นทั้ง 2 ฝั่งก็จะสามารถส่งข้อมูลถึงกันได้ โดยอาจเริ่มจากฝ่ายใดฝ่ายหนึ่งก็ได้ แต่โดยทั่วไปมักเกิดจากฝั่งที่ร้องขอการติดต่อมากกว่า การส่งข้อมูลนี้จะเริ่มจากการส่งข้อมูลเซ็กเมนต์แรกไป และอาจตามด้วยข้อมูลเซ็กเมนต์ถัดไป หรืออาจรอให้มีการตอบรับเกิดขึ้นก่อนก็ได้ ขึ้นกับ Window Size แต่เมื่อถึงคราวที่มีการส่งข้อมูลแล้ว บทบาทของหมายเลขลำดับจะเปลี่ยนไป เพราะในช่วงของการสร้างการเชื่อมต่อนั้น หมายเลขลำดับจะใช้บ่งบอกถึงลำดับ แต่เมื่อถึงการส่งข้อมูลแล้ว หมายเลขลำดับจะทำหน้าที่บอกตำแหน่งของข้อมูล เช่น จากตัวอย่างทางฝั่ง Potter ได้ส่งข้อมูลทั้งหมด 4 ครั้ง ครั้งละ 1000 ไบต์

โดยจากรูปเป็นการส่งข้อมูล 2 ครั้ง ซึ่งจะเห็นว่าหมายเลขลำดับมีการเพิ่มค่าครั้งละ 1000 ไบต์ และเมื่อฝั่ง Albus มีการตอบกลับมา ก็จะตอบเพียงเซ็กเมนต์ตอบรับโดยใช้หมายเลขตอบรับเป็น 146956 ซึ่งก็คือหมายเลขของตำแหน่งข้อมูลที่คาดว่าจะได้รับถัดไปนั่นเอง จากนั้นจะเป็นการส่งข้อมูลอีก 2 เซ็กเมนต์ และมีการตอบรับอีกครั้ง ก็หมดข้อมูลที่จะส่ง ก็จะจบการเชื่อมต่อ ในการเริ่มการเชื่อมต่อมีการตอบรับทั้ง 2 ด้าน ในตอนจบก็จะต้องมีการตอบรับทั้ง 2 ด้านเช่นกัน โดยเริ่มจากทางฝั่งร้องขอจะส่งเซ็กเมนต์ FIN/ACK ไปยังเครื่อง Albus เครื่อง Albus ก็จะส่งเซ็กเมนต์ ACK กลับมา แล้วตามด้วยเซ็กเมนต์ FIN/ACK เพื่อบอกว่าจบการเชื่อมต่อด้วยเช่นกัน เมื่อเครื่อง Potter ได้รับก็จะส่งเซ็กเมนต์ตอบรับจบการเชื่อมต่อ ก็จะเป็นการจบการเชื่อมต่อโดยสมบูรณ์

หน้าที่ของฟิลด์ Option

ในส่วนของฟิล์ดออปชันนั้น มีความสำคัญกับการทำงานของทีซีพีพอสมควร ขนาดของฟิลด์ออปชันมีขนาดไม่แน่นอน ข้อมูลในออปชันอาจมีเพียง 1 ข้อมูล หรือหลายข้อมูลก็ได้ โดยหากมีหลายข้อมูลจะเรียงต่อ ๆ กันไป โดยออปชันจะมีอยู่ด้วยกัน 2 แบบ คือ ออปชันที่มีความยาวไบต์เดียว ได้แก่ ออปชัน 0 ซึ่งมีความหมายว่าไม่มีรายการออปชันต่อจากนี้แล้ว และออปชัน 1 ซึ่งเป็นออปชันไม่ต้องทำอะไร (No Operation) ออปชันประเภทนี้มักใช้เติมให้ความยาวออปชันหารด้วย 4 ลงตัวเท่านั้น

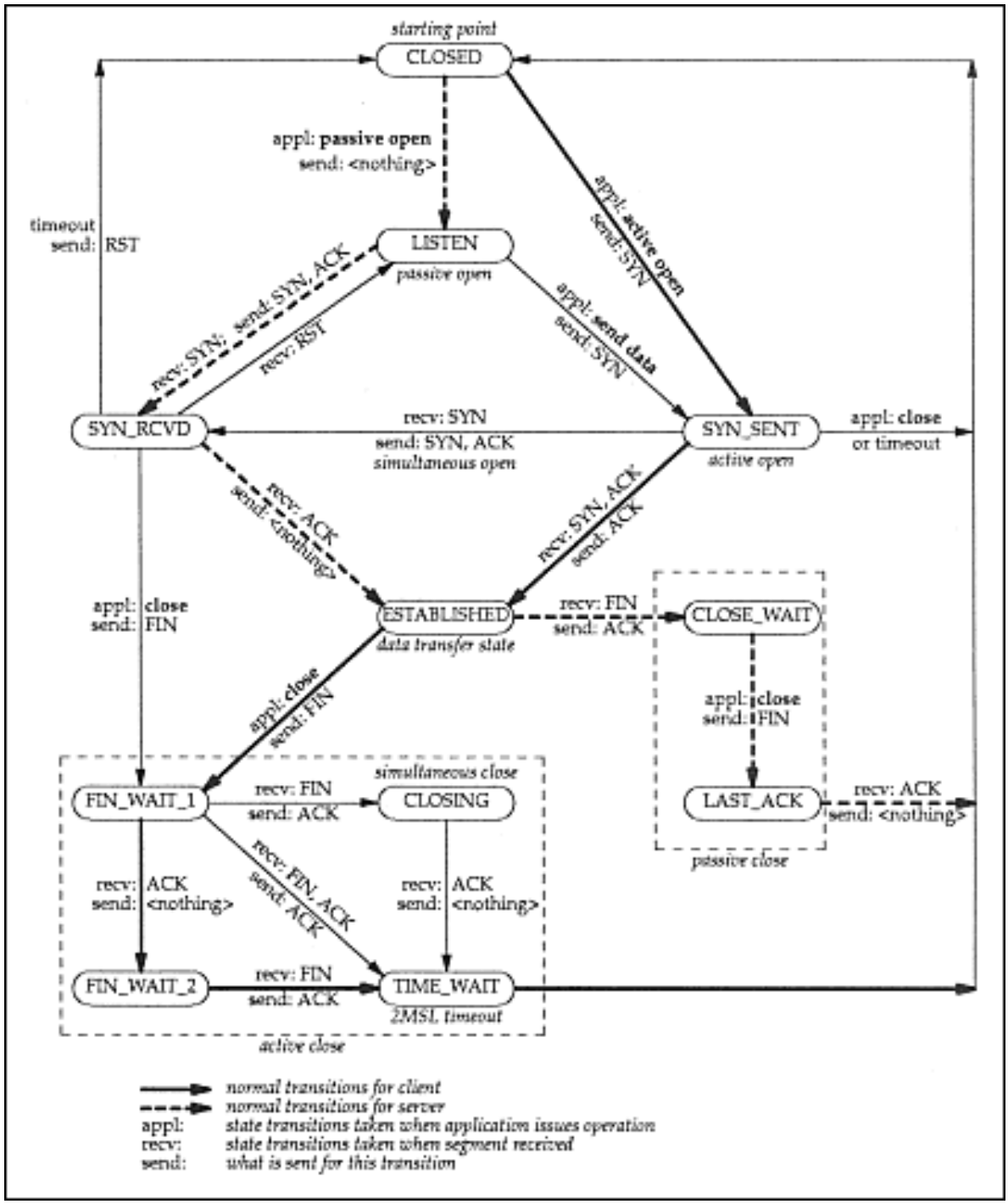
ออปชันอีกประเภทหนึ่ง คือ ออปชันที่มีความยาวหลายไบต์ ออปชันประเภทนี้ ไบต์แรกจะทำหน้าที่ระบุประเภทของออปชัน และไบต์ที่ 2 จะระบุความยาวของออปชันนั้น ๆ ดังนั้นออปชันที่มีความยาวหลายไบต์จะต้องมีความยาวอย่างน้อย 3 ไบต์เสมอ และสำหรับวิธีการพิจาณาว่าเป็นออปชันแบบใดนั้น ก็ดูจากค่าหากเป็น 0 หรือ 1 ก็หมายถึงออปชัน 1 ไบต์ แต่ถ้าเป็นเลขอื่นก็หมายถึงออปชันหลายไบต์ ออปชันหลายไบต์นี้จะเกี่ยวกับการติดต่อระหว่างทีซีพีอยู่ 2 แบบ โดยออปชันแบบแรกจะมีรหัสชนิดเป็น 2 ซึ่งหมายถึง (MSS) Maximum Segment Size ซึ่งเป็นค่าขนาดสูงสุดของเซ็กเมนต์ของระบบนั้น ๆ ออปชันนี้จะใช้เฉพาะตอนที่มีการสร้างการเชื่อมต่อ เพื่อให้ทั้งฝั่งรับและฝั่งส่งตกลงกันว่าจะใช้ขนาดของ Segment Size เท่าใด

ออปชันอีกตัวหนึ่งที่มีการใช้งานในระหว่างการเชื่อมต่อคือ Time Stamp ซึ่งจะใช้รหัส 8 โดยในออปชันนี้จะทำหน้าที่เก็บเวลาของแพ็กเกจของทั้ง 2 ด้าน เพื่อใช้ในการคำนวณค่าต่าง ๆ เช่น Time Out ดังนั้นในทุก ๆ เซ็กเมนต์จะมีการบันทึกเวลานี้เสมอ

สถานะทีซีพี

เพื่อให้เข้าใจการทำงานของโพรโตคอลทีพีซี เราควรจะต้องศึกษาสถานะต่างๆ ของโพรโตคอลทีซีพี (TCP State) ซึ่งแสดงดังในรูปที่ 6 จากรูปจะเห็นว่าสถานะของทีซีพีมีอยู่ด้วยกัน 11 สถานะ โดยในรูปจะมีเส้นที่แสดงการเปลี่ยนสถานะอยู่ 3 แบบ โดยเส้นที่เป็นเส้นหนาจะแสดงการเปลี่ยนสถานะกรณีที่เป็นฝ่ายติดต่อไปก่อน (Client Side) เส้นประจะแสดงการเปลี่ยนแปลงที่เกิดขึ้นได้กรณีที่รอการติดต่อ (Server Side) เส้นบางจะแสดงการเปลี่ยนแปลงที่เกิดได้กับทั้งไคลเอนต์และเซิร์ฟเวอร์

สำหรับการทำงานในฝั่งเซิร์ฟเวอร์นั้น จะเริ่มที่สถานะ LISTEN จากนั้นเมื่อได้รับ SYN จะส่ง SYN/ACK กลับไปและเข้าสู่สถานะ SYN_RCVD ซึ่งหากได้รับ RST ก็จะกลับไปอยู่ในสถานะ Listen เหมือนเดิม แต่ถ้าได้รับ SYN อีกครั้งจะเปลี่ยนไปอยู่ในสถานะ ESTABLISHED ซึ่งเป็นสถานะที่การเชื่อมต่อสมบูรณ์ จากสถานะนี้ข้อมูลจะรับส่งได้ตามปกติ และหากได้รับ FIN ก็จะส่ง ACK กลับไปและเปลี่ยนไปอยู่สถานะ CLOSE_WAIT และส่ง FIN กลับไปยืนยันอีกครั้ง และหากได้รับ ACK กลับมาก็จะกลับไปอยู่สถานะ LISTEN อีกครั้ง สำหรับฝั่งไคลเอนต์นั้นสถานะจะคล้ายกัน แต่จะเริ่มการทำงานจากสถานะ SYN_SENT และหากได้รับ SYN/ACK ก็จะส่ง ACK กลับไปและอยู่ในสถานะ ESTABLISHED



รูปที่ 6 สถานะทีซีพี

จุดอ่อนและการโจมตี

ในการทำงานตามมาตรฐานของของโพรโตคอล TCP สำหรับบริการใดๆ ก็ตามที่รันอยู่ในเครื่องเซิร์ฟเวอร์ จะทำการสร้างพอร์ตเปิดไว้รอรับการร้องขอจากเครื่อง Client และจะตอบสนองต่อเซ็กเมนต์ที่มี SYN Flag ด้วย SYN/ACT เสมอ ดังนั้นปัญหาความปลอดภัยที่เกิดขึ้นจากการดำเนินการดังกล่าวจะทำได้ใน 2 กรณีคือ

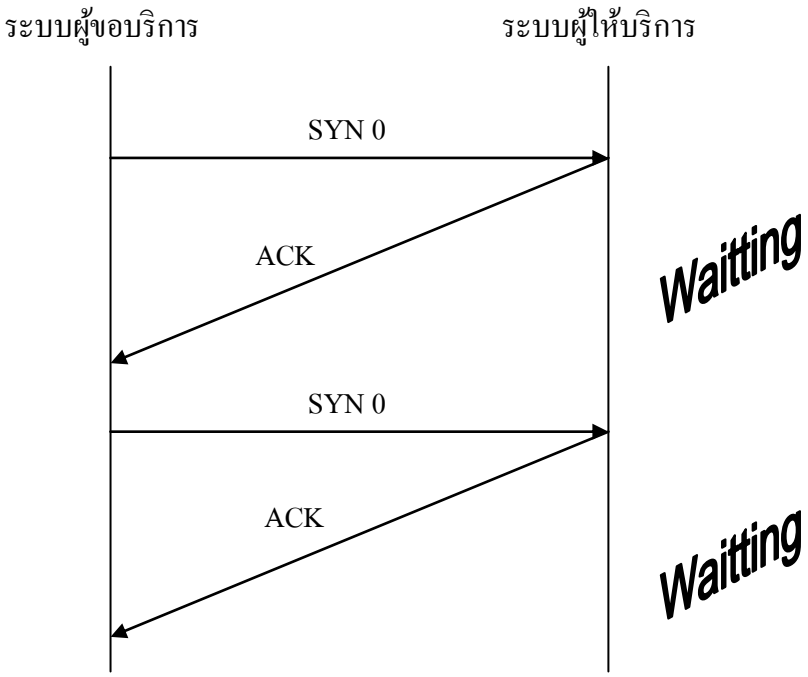
1. การโจมตีทางเครือข่ายเพื่อให้เครื่องเซิร์ฟเวอร์ไม่สามารถให้บริการได้
2. การตรวจหาข้อมูลของบริการต่างๆ โดยการสแกนพอร์ต
3. การทำ Session Hijack

การโจมตีทางเครือข่ายโดยใช้ TCP

การโจมตีในระดับชั้นทีซีพี ยังสามารถแบ่งได้เป็น 2 แบบย่อย คือ การโจมตีด้วยแพ็กเกจปริมาณมาก การโจมตีแบบนี้เป็นการส่งแพ็กเก็ตปริมาณมากเข้าไปยังระบบเป้าหมาย อาจทำให้ระบบเป้าหมายไม่สามารถให้บริการบางอย่าง หรือไม่สามารถทำงานต่อไปได้ ซึ่งแพ็กเก็ตที่ส่งออกไปนี้สามารถแบ่งออกได้เป็น การโจมตีด้วยแพ็กเก็ตข้อมูล การโจมตีวิธีนี้ทำได้โดยการส่งแพ็กเก็ตข้อมูลปริมาณมาก เมื่อข้อมูลเข้ามาสู่เครื่องเป้าหมายก็เก็บไว้ในบัฟเฟอร์ก่อนนำมาประมวลผลอีกครั้ง ดังนั้นหากส่งแพ็กเก็ตเข้ามาเป็นปริมาณมาก อาจทำให้บัฟเฟอร์ของเครื่องเป้าหมายไม่เพียงพอที่จะสามารถรองรับแพ็กเก็ตเหล่านั้นได้ทั้งหมด ซึ่งอาจทำให้เครื่องเป้าหมายให้บริการได้ช้าลง หรือต้องหยุดการให้บริการไปเลย

การโจมตีอีกรูปแบบหนึ่ง คือ การโจมตีด้วยแพ็กเก็ตควบคุม (Control Packets) ตัวอย่างของการโจมตีแบบนี้ ได้แก่ การทำ SYN Flooding การโจมตีลักษณะเป็นการทำ 3-way handshake ไม่สมบูรณ์ กล่าวคือ เครื่องที่ขอบริการส่งสัญญาณ SYN ไป แต่เมื่อได้รับสัญญาณ SYN/ACK จากเครื่องที่ให้บริการแล้ว ไม่ส่งสัญญาณ ACK ตอบกลับไป ทำให้เครื่องที่ให้บริการต้องเปิดการเชื่อมต่อรอการตอบกลับ ดังรูปที่ 6 ซึ่งการเปิดการเชื่อมต่อรอเอาไว้นี้ต้องใช้ทรัพยากรของระบบส่วนหนึ่ง โดยเฉพาะทรัพยากรประเภทหน่วยความจำ ซึ่งจะเรียกการเชื่อมต่อที่เปิดค้างไว้นี้ว่า Backlog Queue และหากมีการส่งสัญญาณในลักษณะนี้มากๆ และจำนวนของ

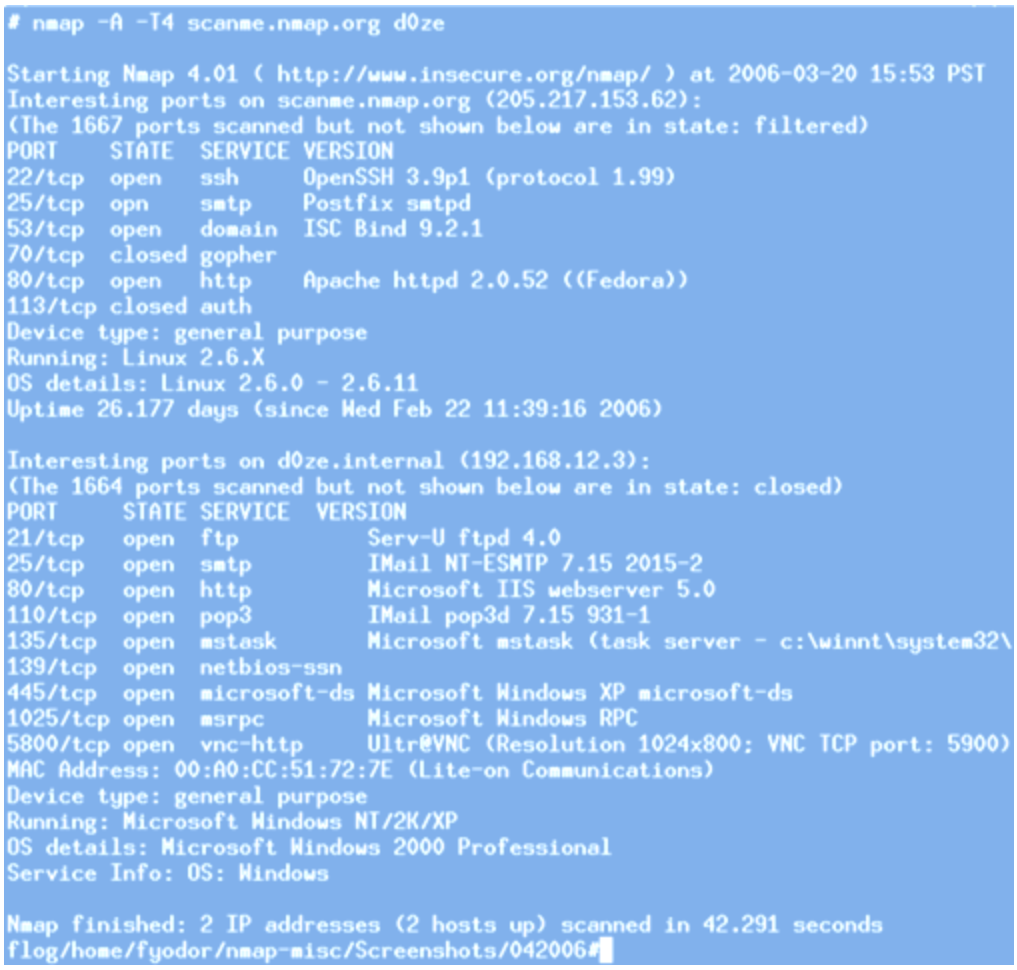
Backlog Queue มีมากเข้า ทรัพยากรของระบบอาจไม่เพียงพอ อาจทำให้ระบบไม่สามารถให้บริการอย่างอื่นหรือให้บริการกับผู้ร้องขอรายอื่นได้



รูปที่ 7 การเกิด Backlog Queue

การตรวจหาข้อมูลของบริการต่างๆ โดยการสแกนพอร์ต

จากการทำงานตามมาตรฐานของโพรโตคอล TCP ที่จะทำการตอบสนองต่อการกระตุ้นโดย SYN ด้วย SYN/ACT เสมอนั้น จึงทำให้ผู้โจมตีระบบสามารถทราบข้อมูลการให้บริการของเครื่องคอมพิวเตอร์ต่างๆ ได้ โดยการส่ง SYN ไปยังพอร์ตทุกๆ พอร์ตแล้วรอรับ SYN/ACT ซึ่งหากมี SYN/ACT ตอบกลับมาจากพอร์ตใดจะแสดงว่าพอร์ตนั้นเปิดให้บริการอยู่ ในการโจมตีระบบสามารถเข้าถึงระบบได้จากพอร์ตที่เปิดนั้นๆ ได้ สำหรับเครื่องมือที่สามารถใช้สแกนพอร์ตที่ใช้งานกันอย่างแพร่หลายได้แก่โปรแกรมชื่อ NMAP



```
# nmap -A -T4 scanme.nmap.org d0ze

Starting Nmap 4.01 ( http://www.insecure.org/nmap/ ) at 2006-03-20 15:53 PST
Interesting ports on scanme.nmap.org (205.217.153.62):
(The 1667 ports scanned but not shown below are in state: filtered)
PORT    STATE  SERVICE VERSION
22/tcp  open   ssh     OpenSSH 3.9p1 (protocol 1.99)
25/tcp  opn    smtp    Postfix smtpd
53/tcp  open   domain  ISC Bind 9.2.1
70/tcp  closed gopher
80/tcp  open   http    Apache httpd 2.0.52 ((Fedora))
113/tcp closed auth
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.0 - 2.6.11
Uptime 26.177 days (since Wed Feb 22 11:39:16 2006)

Interesting ports on d0ze.internal (192.168.12.3):
(The 1664 ports scanned but not shown below are in state: closed)
PORT     STATE SERVICE  VERSION
21/tcp   open  ftp          Serv-U ftpd 4.0
25/tcp   open  smtp         IMail NT-ESMTP 7.15 2015-2
80/tcp   open  http         Microsoft IIS webserver 5.0
110/tcp  open  pop3         IMail pop3d 7.15 931-1
135/tcp  open  mstask       Microsoft mstask (task server - c:\winnt\system32\
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds Microsoft Windows XP microsoft-ds
1025/tcp open  msrpc        Microsoft Windows RPC
5800/tcp open  vnc-http     Ultr@VNC (Resolution 1024x800; VNC TCP port: 5900)
MAC Address: 00:A0:CC:51:72:7E (Lite-on Communications)
Device type: general purpose
Running: Microsoft Windows NT/2K/XP
OS details: Microsoft Windows 2000 Professional
Service Info: OS: Windows

Nmap finished: 2 IP addresses (2 hosts up) scanned in 42.291 seconds
flog/home/fyodor/nmap-misc/Screenshots/042006#
```

รูปที่ 8 ตัวอย่างผลลัพธ์การทำงานของโปรแกรม NMAP

โดยความสามารถของโปรแกรม NMAP สามารถสแกนเครื่องคอมพิวเตอร์แล้วให้ข้อมูลต่างๆ ต่อไปนี้

1. หมายเลขไอพีแอดเดรสของคอมพิวเตอร์ที่อยู่ในระบบเครือข่าย
2. บริการต่างๆ ที่เครื่องคอมพิวเตอร์ในเครือข่ายให้บริการ
3. พอร์ตต่างๆ ที่คอมพิวเตอร์ในเครือข่ายให้บริการ
4. รายละเอียดของโปรแกรมที่ระบบใช้ในการให้บริการนั้นๆ
5. ระบบปฏิบัติการของคอมพิวเตอร์เป้าหมาย
6. รายละเอียดอื่นๆเช่น Up Time , Device Type เป็นต้น

ตัวอย่างโหมดการทำงานโปรแกรม Nmap ที่นิยมใช้มีดังนี้

1. TCP Sync Scanning : : อาศัยเทคนิคที่เรียกว่า "Half-Open" โดยโปรแกรมจะส่ง SYN Packet ออกไปยังโฮสต์เป้าหมาย ทันทีที่เกิดการคอนเน็คขึ้น โปรแกรมจะยุติการติดต่อทันที ซึ่งเทคนิคเช่นนี้จะทำให้โฮสต์เป้าหมายส่วนใหญ่ยังไม่ทันได้บันทึกเหตุการณ์นี้ไว้ใน Log จึงเป็นการแสกนที่ไม่ทิ้งร่องรอยไว้นั่นเอง
2. TCP connect( ) : วิธีการนี้เป็นวิธีขั้นพื้นฐานที่โปรแกรม Port Scanner ทั่วไปนิยมปฏิบัติกัน (เช่น โปรแกรม Port Scanner ในกลุ่มวินโดวส์) ซึ่งเป็นการจำลองกรกะบวนการร้องขอเพื่อการติดต่อขอใช้บริการจากเครื่องลูกข่ายตามปรกติ วิธีการนี้จึงง่ายต่อการตรวจจับโดยโฮสต์ปลายทางและบันทึกเข้าสู่ Log
3. Stealth FIN , Xmas Tree ,Null Scanning : : เป็นวิธีแสกนพอร์ตที่มีวิธีการที่แตกต่างจาก 2 วิธีแรก เนื่องจากการส่งแพคเก็ต *SYN จะถูกปฏิเสธได้โดยไฟร์วอลล์ ดังนั้นจึงอาศัยวิธีส่งแพคเก็ตด้วยแฟล็กชนิดอื่น ๆ หรือไม่มีการเซ็ตแฟลกใด ๆ เลยไปแทน ซึ่งจะมีความเป็นไปได้ว่าจะสามารถเล็ดลอดการตรวจจับและปฏิเสธของไฟร์วอลล์ไปได้ นอกจากนี้ผลการตอบสนองต่อแพคเก็ตเหล่านี้จากระบบปฏิบัติการต่าง ๆ จะมีผลลัพธ์ที่ไม่เหมือนกัน พฤติกรรมที่แตกต่างกันนี้เองจึงเป็นประโยชน์ในทางอ้อมที่ช่วยให้สามารถประเมินได้ว่าโฮสต์เป้าหมายนั้นใช้ระบบปฏิบัติการใดอยู่ นับว่าเป็นข้อมูลที่น่าสนใจอีกประการหนึ่งด้วย
4. UDP Scanning : การแสกนในโหมดนี้จะตรวจสอบเฉพาะพอร์ตที่ให้บริการแบบ UDP (User Datagram Protocol) โดยเฉพาะ ซึ่งปรกติแล้ว Nmap จะไม่รายงานเกี่ยวกับพอร์ตชนิดนี้ให้ทราบจนกว่าผู้ใช้จะกำหนดให้ทำงานในโหมดนี้
5. IP Protocol Scanning : ใช้เพื่อการวิเคราะห์โฮสต์เป้าหมายว่ากำลังใช้ IP Protocol ใดอยู่บ้าง เช่น icmp, igmp ,tcp ,udp ข้อมูลที่ปรากฏขึ้นจะใช้เพื่อการเดา (Guessing) ประเภท และหน้าที่ของโฮสต์นั้น ๆ ซึ่งอาจจะไม่ใช่เครื่องเซิร์ฟเวอร์ แต่อาจเป็นอุปกรณ์เครือข่ายบางประเภทก็เป็นได้

เทคนิคของ Port scanning ที่นิยมใช้มีดังนี้

1. Address Resolution Protocol (ARP) scans จะตรวจหาอุปกรณ์ที่ทำงานในเครือข่ายโดยการส่งชุด ARP broadcasts Packet และเพิ่มค่าของฟิลด์ที่บรรจุ IP address ของเหยื่อเป้าหมายในแต่ละ broadcast packet การสแกนชนิดนี้จะได้รับผลตอบสนองจากอุปกรณ์ที่มี IP บนเครือข่ายออกมาในรูปแบบของ IP address ของแต่ละอุปกรณ์ การสแกน แบบนี้จึงทำการ map out ได้ทั้งเครือข่ายอย่างมีประสิทธิภาพ แต่มีข้อจำกัดคือสามารถใช้ได้ในเครือข่ายเดียวกันเท่านั้น

2. The Vanilla TCP connect scan เป็นเทคนิคการสแกนพอร์ตขั้นพื้นฐานและง่ายที่สุด คือจะใช้ connect system call ของระบบปฏิบัติการไปบนระบบเหยื่อเป้าหมาย ด้วยกลไกมาตรฐานที่เรียกว่า TCP three-way handshake (ดังรูปที่ 1) เพื่อเปิดการเชื่อมต่อไปยังทุกๆ พอร์ตที่เปิดอยู่ การสแกนชนิดนี้สามารถจับได้ง่ายมาก โดยการล็อก (log) ต่าง ๆ ของระบบที่เป็นเหยื่อเป้าหมายจะแสดงการร้องขอการเชื่อมต่อ (connection requests) และข้อความแสดงข้อผิดพลาด (error messages) สำหรับบริการที่ตอบรับการเชื่อมต่อนั้น หรืออาจป้องกันโดยติดตั้งไฟล์วอลล์

3. The TCP SYN (Half Open) scans เทคนิคนี้บางครั้งถูกเรียกว่า half open scanning เพราะว่าเป็นการ connectionที่ไม่สมบูรณ์ โดยระบบที่ทำการโจมตีไม่ได้ปิดการเชื่อมต่อที่ได้เปิดไว้ scanner จะส่ง SYN packet ไปยังเหยื่อเป้าหมายและรอการตอบสนอง ถ้าพอร์ตถูกเปิดไว้เป้าหมายก็จะส่ง SYN/ACK กลับมา ซึ่งก็สรุปได้ว่าพอร์ตดังกล่าวอยู่ในสถานะ listening แต่ถ้าพอร์ตถูกปิดอยู่ เป้าหมายก็จะส่ง RST (Reset) กลับมาแทน เทคนิคการสแกนรูปแบบนี้สามารถทำการสแกนเหยื่อเป้าหมายได้อย่างรวดเร็ว และยากต่อการตรวจจับ ปกติเครื่องที่เป็นเหยื่อเป้าหมายจะทำหน้าที่ปิดการเชื่อมต่อที่เปิดไว้ และส่วนใหญ่จะไม่มีระบบการ ล็อกที่เหมาะสมในการตรวจจับการสแกนชนิดนี้

4. The TCP FIN scan เทคนิคนี้สามารถที่จะทะลุผ่านไฟล์วอลล์ส่วนใหญ่, packet filters และโปรแกรมตรวจจับการสแกนไปได้โดยไม่ถูกตรวจพบ เพราะระบบที่ทำการโจมตีจะส่ง TCP packets ที่เซตค่า flag FIN เป็น 1 (TCP FIN) ไปยังระบบของเหยื่อเป้าหมาย สำหรับพอร์ตต่าง ๆ ที่ปิดอยู่จะตอบสนองกลับไปด้วย RST ส่วนพอร์ตที่เปิดจะไม่สนใจ packets เหล่านั้นเลย ดังนั้นเครื่องที่ทำการโจมตีก็จะได้ข้อมูลว่ามันได้รับ RST จาก

พอร์ตไหนบ้างและไม่ได้ RST จากพอร์ตไหนบ้าง (ทำให้ทราบหมายเลขพอร์ตที่ไม่ได้เปิดให้บริการ) โดยปกติแล้ว เทคนิคนี้มักใช้ได้กับเครื่องปลายทางที่รันบนยูนิกซ์

5. The TCP Reverse Ident scans เป็นเทคนิคที่สามารถตรวจหาชื่อของเจ้าของแต่ละโพรเซสที่เป็นการเชื่อมต่อด้วย TCP บนเครื่องเหยื่อเป้าหมาย เทคนิคการสแกนชนิดนี้จะทำให้ระบบที่ทำการโจมตีสามารถเชื่อมต่อเข้าไปยังพอร์ตที่เปิดอยู่และใช้ ident protocol ในการค้นหาว่าใครเป็นเจ้าของโพรเซสบนเครื่องเหยื่อเป้าหมายได้

6. The TCP XMAS ถูกใช้เพื่อหาพอร์ตบนเครื่องเหยื่อเป้าหมายที่อยู่ในสถานะ listening โดยจะไม่ส่ง TCP packet ทั้ง 3 ตัวซึ่งเป็นที่สังเกตง่าย คือ SYNC-ACK-RST แต่จะใช้ flag เป็น URG, PSH และ FIN ใน TCP header ไปยังพอร์ตของเครื่องเป้าหมาย ทั้งนี้เพื่อหลบหลีกการตรวจจับให้มากที่สุด ซึ่งถ้าพอร์ต TCP ของเครื่องเป้าหมายปิดอยู่ พอร์ตนั้นก็จะส่ง RST กลับมา แต่ถ้าพอร์ตเปิดอยู่ก็จะไม่สนใจ packet นั้นเลย

7. The TCP NULL scan เทคนิคนี้จะไม่ใช้ flag ในการสแกนเลย โดยจะส่ง TCP packet ที่มี sequence number แต่ไม่มี flag ออกไปยังเครื่องเป้าหมาย ถ้าพอร์ตปิดอยู่จะส่ง กลับมา RST packet กลับมา แต่ถ้าพอร์ตเปิดอยู่ ก็จะไม่สนใจ packet นั้นเลย โดยทั่วไปแล้ว TCP packet ประเภทนี้จะไม่มีอยู่ในข้อกำหนดของ potocol จึงไม่มีผู้สนใจ นอกจากนี้ยังทำให้ potocol ใน layer ชั้นสูงขึ้นไปไม่ทราบว่ามีการส่ง packet เข้ามาด้วย นอกจากการใช้ packet เหล่านี้เพื่อการสแกนพอร์ตแล้วยังสามารถนำ packet เหล่านี้ไปใช้ในการตรวจสอบระบบปฏิบัติการของเหยื่อเป้าหมายได้อีกด้วย เนื่องจากระบบปฏิบัติการแต่ละแบบจะมีการตอบสนองที่ไม่เหมือนกัน

8. The TCP ACK scan เป็นเทคนิคที่ใช้ค้นหาเว็บไซต์ที่เปิดบริการอยู่ แต่ปฏิเสธการตอบสนองต่อ ICMP ping หรือเพื่อค้นหากฎ (rule) หรือนโยบาย (policy) ต่าง ๆ ที่ตั้งไว้ที่ไฟล์วอลล์เพื่อตรวจสอบดูว่าไฟล์วอลล์นั้นๆ ทำหน้าที่แค่เพียงสามารถกรอง packet อย่างง่าย ๆ หรือเป็นไฟล์วอลล์ที่มีความฉลาดพอสมควร และใช้เทคนิคการกรอง packet ขั้นสูง โดยเทคนิคการสแกนแบบนี้จะใช้ TCP packet ที่มี flag เป็น ACK ส่งไปยังพอร์ตเครื่องปลายทาง ถ้าพอร์ตเปิดอยู่ เครื่องเป้าหมายจะส่ง RST กลับมา แต่ถ้าปิดอยู่ก็จะไม่สนใจ packet นั้น

9. TCP Windows scan เทคนิคการสแกนนี้จะตรวจสอบพอร์ตที่เปิดอยู่ รวมทั้งตรวจดูว่า พอร์ตใดบ้างที่ถูก filter เอาไว้ไม่ให้ผ่านเข้าไปถึง และพอร์ตหมายเลขใดได้รับการอนุญาตไว้บ้าง โดยอาศัยช่องโหว่จากความผิดปกติบางอย่างในการแจ้งค่า TCP Windows Size ของ TCP/IP protocol

10. TCP RPC scan เทคนิคการสแกนนี้ใช้งานได้เฉพาะกับเครื่องปลายทางที่รันบนยูนิกซ์เท่านั้น มันถูกใช้เพื่อตรวจสอบดูว่ามีเซอร์วิสใดทำงานอยู่บนเซอร์วิส RPC บ้าง รวมทั้งตรวจดูเวอร์ชันของเซอร์วิสนั้น และโปรแกรมอื่นที่เกี่ยวข้อง

11. The FTP Bounce Attack จะใช้ FTP protocol สำหรับสร้างการเชื่อมต่อบริการ FTP ของ ตัวกลาง (proxy) เทคนิคการสแกนแบบนี้ ผู้โจมตีจะสามารถซ่อนตัวอยู่หลัง FTP server และสแกนเป้าหมายอื่น ๆ ได้โดยไม่ถูกตรวจจับ ดังนั้น FTP servers ส่วนใหญ่จะมีการ disable บริการของ FTP เพื่อความปลอดภัยของระบบ

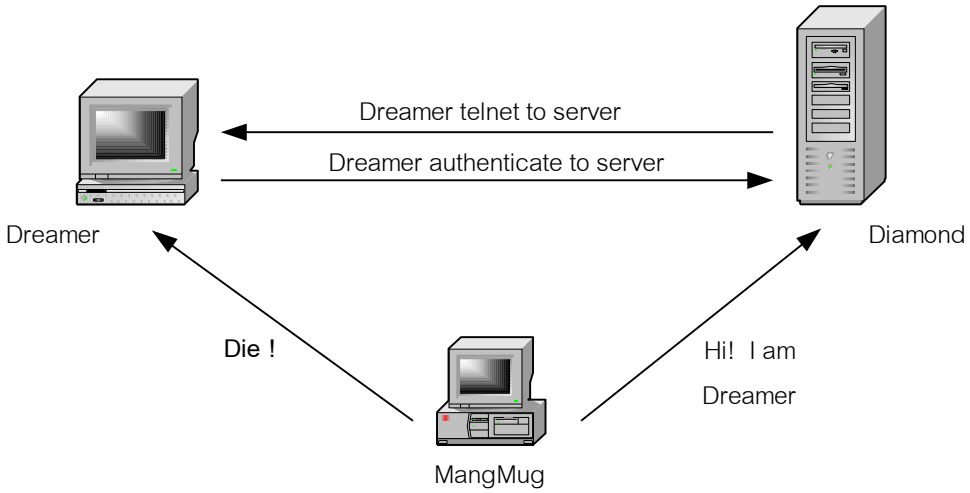
12. The UDP ICMP Port scanning ใช้ UDP potocol โดยมันจะส่ง UDP packet ไปยังพอร์ตเป้าหมาย ถ้าพอร์ตที่ปิดอยู่นั้นจะตอบกลับมาด้วย ICMP type PORT UNREACHABLE packet ถ้าพอร์ตนั้นเปิดอยู่มันจะไม่ส่ง packet กลับมา เทคนิคนี้ใช้ในการสแกนหาพอร์ตหมายเลขสูง ๆ โดยเฉพาะในระบบ Solaris แต่จะช้าและไม่น่าเชื่อถือ เนื่องจาก UDP protocol เป็นลักษณะ connectionless คือไม่รับรองว่า packet ที่ส่งไปจะถึงเครื่องปลายทางครบถ้วนหรือไม่

13. The ICMP ping-sweeping scan จะใช้คำสั่ง ping เพื่อกวาดดูว่ามีระบบไหนที่เปิดใช้งานอยู่ เครือข่ายส่วนใหญ่จึงมีการกรองหรือ disabled

การทำ Session Hijack

การขโมยเซสชันเป็นวิธีการหนึ่งที่ทำให้เราได้สิทธิการเข้าถึงระบบใดระบบหนึ่ง อันที่จริงวิธีการในการเข้าถึงระบบใดระบบหนึ่งนั้น วิธีการดักจับรหัสผ่านถือเป็นวิธีการที่ง่ายที่สุด แต่ในปัจจุบันเทคโนโลยีด้านการรักษาความปลอดภัยมีมากขึ้น ทำให้มีการนำวิธีการพิสูจน์ตน (Authentication) ที่มีความปลอดภัยมากขึ้น อาทิ ระบบ One Time Password ที่แม้จะดักจับรหัสผ่านได้ แต่เนื่องจากรหัสผ่านนั้น ใช้ครั้งเดียวทิ้ง รหัสผ่านที่ดักจับได้จึงไม่มีประโยชน์อะไร หรือการนำวิธีการเข้ารหัสมาใช้ในระหว่างการพิสูจน์ตน โดยการเข้ารหัสข้อมูลส่วนที่เป็นรหัสผ่าน ทำให้แม้ดักจับมาได้ ก็ไม่สามารถแกะรหัสผ่านออกมาได้ เพราะหากใช้วิธีการที่มีความปลอดภัยสูงอย่าง 3DES หรือ AES แล้ว ต้องใช้เวลานับเป็นล้านปี จึงจะสามารถแกะรหัสผ่านได้ ซึ่งเราคงรอจนถึงตอนนั้นไม่ได้

ดังนั้นวิธีการที่มักจะนำมาใช้เพื่อเข้าสู่ระบบในกรณีแบบนี้ คือ การขโมยเซสชัน วิธีการนี้เป็นการขโมยการเชื่อมต่อเซสชันที่กำลังมีการเชื่อมต่อกันอยู่ ซึ่งทำให้เราสามารถข้ามกระบวนการพิสูจน์ตนไปได้ และสามารถเข้าใช้งานระบบได้เลย ในการขโมยเซสชันนั้น ขั้นตอนแรกแฮกเกอร์จะต้องดักจับข้อมูลที่เกิดขึ้นในเซสชันจริง ๆ ตรวจสอบและวิเคราะห์ จากนั้นก็หาทางสร้างเซสชันเพื่อเชื่อมเข้ากับเซสชันที่มีอยู่เดิม ดังนั้นการโจมตีแบบนี้จะสามารถทำได้กับแอปพลิเคชันที่ทำงานในแบบเซสชันเท่านั้น เช่น เวปแอพลิเคชัน เทลเน็ต FTP เป็นต้น แนวคิดของการขโมยเซสชัน แสดงให้เห็นในรูปที่ 9



รูปที่ 9 *แนวคิดของการขโมยเซสชัน*

จากรูปจะเห็นได้ว่าการขโมยเซสชัน ก็คือ การโจมตีให้เซสชันที่กำลังเชื่อมต่ออยู่เกิดการหยุดชะงัก ซึ่งจากรูปเครื่อง MangMug จะทำการโจมตีเครื่อง Dreamer ให้หยุดการทำงาน หรือหยุดการติดต่อ จากนั้นจะส่งข้อมูลเพื่อทำการติดต่อไปยังเครื่อง Diamond แทน ซึ่งการทำเช่นนี้เครื่อง MangMug จะต้องปลอมตัวเองเป็นเครื่อง Dreamer ด้วย ดังนั้นเครื่อง Diamond ก็จะคิดว่าเครื่อง MangMug เป็นเครื่อง Dreamer และยอมเชื่อมต่อและทำงานต่อจากที่หยุดชะงักไป

ขโมยเซสชันประกอบด้วยขั้นตอน 6 ขั้นตอน คือ 1) เลือกเป้าหมาย 2) เรียนรู้การเปลี่ยนแปลงของหมายเลขลำดับ 3) หาเซสชันที่เชื่อมต่ออยู่ 4) ทำนายหมายเลขลำดับ 5) ทำให้ฝั่งหนึ่งหยุดการเชื่อมต่อ และ 6) ครอบครองเซสชัน เพื่อให้เข้าใจการทำงาน จะขอยกตัวอย่างการขโมยเซสชัน โดยสมมติว่ามีผู้ที่กำลังเทลเน็ตไปที่ Diamond ตามในรูปที่ 1 แล้วผู้บุกรุกก็จะเริ่มหาข้อมูล เพื่อจะได้สร้างรูปแบบของหมายเลขลำดับ ทั้งนี้

เนื่องจากหมายเลขลำดับนั้น มีส่วนเกี่ยวข้องกับระบบปฏิบัติการอย่างมาก ดังนั้นแฮกเกอร์จะพยายามหาข้อมูลว่าเป็นระบบปฏิบัติการอะไรเสียก่อน (อาจใช้คำสั่ง NMAP –O *ip-address*)

หลังจากนั้นผู้บุกรุกก็จะทดลองติดต่อไปยังเครื่องเป้าหมายหลาย ๆ ครั้ง เพื่อดูการเปลี่ยนแปลงของค่าหมายเลขลำดับที่เปลี่ยนไปในการติดต่อแต่ละครั้ง โดยตัวอย่างต่อไปนี้เป็นการเชื่อมต่อไปยังเครื่องลีนุกซ์จากระบบปฏิบัติการวินโดว์

การเชื่อมต่อครั้งที่ 1

03:52:46.202589000 eth0 P 161.246.70.239.1447 > 161.246.4.3.telnet: S 1881721336: 1881721336(0) win 64240 < mss 1460, nop, nop, sackOK> (DF)

03:52:46.204274000 eth0 P 161.246.4.3.telnet > 161.246.70.239.1447 S 1156928000: 1156928000(0) ack 1881721337 win 32768 < mss 1460

การเชื่อมต่อครั้งที่ 2

03:52:51.145662000 eth0 P 161.246.70.239.1448 > 161.246.4.3.telnet: S 1882982486: 1882982486 (0) win 64240 < mss 1460, nop, nop, sackOK> (DF)

03:52:46.147212000 eth0 P 161.246.4.3.telnet > 161.246.70.239.1448 S 1157248000: 1157248000(0) ack 1882982487 win 32768 < mss 1460

การเชื่อมต่อครั้งที่ 3

03:52:56.742647000 eth0 P 161.246.70.239.1449 > 161.246.4.3.telnet: S 1884422564: 1884422564 (0) win 64240 < mss 1460, nop, nop, sackOK> (DF)

03:52:56.744337000 eth0 P 161.246.4.3.telnet > 161.246.70.239.1449 S 1157376000: 1157376000 (0) ack 1884422565 win 32768 < mss 1460

การเชื่อมต่อครั้งที่ 4

03:53:00.909787000 eth0 P 161.246.70.239.1450 > 161.246.4.3.telnet: S 1885526759: 1885526759 (0) win 64240 < mss 1460, nop, nop, sackOK> (DF)

03:53:00.911478000 eth0 P 161.246.4.3.telnet > 161.246.70.239.1448 S 1157568000: 1157568000(0) ack 1885526760 win 32768 < mss 1460

ซึ่งเมื่อเรานำหมายเลขลำดับของแพ็กเกจมาพิจารณาดู จะได้ผลลัพธ์ดังตารางที่ 3

Connection Number	Windows Client	Diamond Server
1	1881721336	1156928000
2	1882982486	1157248000
3	1884422564	1157376000
4	1885526759	1157568000

ตารางที่ 3 ตัวอย่าง Sequence Number และ Acknowledge Number

และผลลัพธ์จากตารางเป็นการยืนยันให้เห็นว่าหมายเลขลำดับของวินโดว์นั้น ง่ายต่อการคาดเดามากกว่าลีนุกซ์จริง ๆ และเมื่อเราได้ข้อมูลเบื้องต้นดังกล่าวแล้ว เราก็จะเข้าสู่การทำงานในขั้นที่ 3 คือ หาเซสชันเป้าหมายที่จะโจมตี โดยทั่วไปผู้บุกรุกมักจะกระทำในช่วงเวลาที่มีการใช้งานมาก ๆ เพราะมีเซสชันให้เลือกมาก

นอกจากนั้นในระหว่างการขโมยเซสชันอาจต้องมีการทำซ้ำหลายครั้งกว่าจะสำเร็จ การมีเซสชันมาก ๆ จะทำให้คนไม่สงสัยว่าเกิดอะไรขึ้น เพราะหากมีอยู่เซสชันเดียว และปรากฏว่ามีการหลุดจากการติดต่อบ่อย ๆ ก็อาจเป็นที่สงสัยได้

จากนั้นก็จะเข้าสู่ขั้นตอนที่ 4 คือการคาดเดาหมายเลขลำดับของแพ็กเกจ ทั้งนี้เนื่องจากในระหว่างการเข้าไปสวมรอยเพื่อขโมยเซสชันนั้น หากหมายเลขลำดับแพ็กเกจที่ผู้บุกรุกส่งไปไม่สอดคล้องกับหมายเลขลำดับที่เซิร์ฟเวอร์คาดหมายว่าจะได้รับแล้ว เซิร์ฟเวอร์จะไม่สามารถดำเนินการในเซสชันนั้นต่อได้ และจะทำการ Re-Sync ใหม่ ซึ่งจะทำให้การสวมรอยล้มเหลวได้ ดังนั้นผู้บุกรุกจะต้องคอยเฝ้าดูหมายเลขลำดับเอาไว้ตลอดเวลา เมื่อสามารถติดตามการเปลี่ยนแปลงของหมายเลขลำดับได้แล้วก็จะเข้าสู่ขั้นตอนที่ 5 คือการโจมตีให้ฝ่ายหนึ่งหยุดการทำงาน หรือหยุดการเชื่อมต่อไป โดยส่วนใหญ่แล้วฝ่ายที่เราจะโจมตีให้หยุดมักจะเป็นไคลเอนต์ เพราะเราต้องการจะเข้าสู่เซิร์ฟเวอร์

โดยทั่วไปวิธีที่ทำให้ข้างหนึ่งหยุดการทำงานไป มักจะใช้วิธีการ DoS (Denial of Service Attack) ซึ่งเรียกเป็นภาษาไทยว่า การโจมตีเพื่อปิดบริการ เมื่อเราสามารถโจมตีให้ฝั่งไคลเอนต์หยุดการทำงานชั่วคราวแล้ว ผู้บุกรุกจะทำการส่งแพ็กเกจไปที่เซิร์ฟเวอร์ซะเองเสมือนกับเป็นเครื่องไคลเอนต์ติดต่อ โดยการปลอมไอพีตัวเองไปเป็นเครื่องไคลเอนต์ อย่างไรก็ตามหากในระหว่างที่ผู้บุกรุกพยายามติดต่อกับเซิร์ฟเวอร์ แล้วเครื่องไคลเอนต์ตัวจริงกลับมาติดต่อกับเซิร์ฟเวอร์อีก อาจเกิดเหตุการ ACK Storm ได้

สำหรับวิธีที่ใช้ในการขโมยเซสชัน ก็มีวิธีการอยู่หลายวิธี ตั้งแต่การเขียนโปรแกรมขึ้นมาเอง หรือการนำเอาเครื่องมือที่มีผู้พัฒนาเอาไว้มาใช้งาน เช่น Juggernaut, Hunt, TTY Watcher และ IP Watcher ซึ่งจากที่กล่าวมาทั้งหมด คงพอจะเข้าใจกระบวนการทั้งหมด และเห็นได้ว่าการขโมยเซสชันไม่ใช่เรื่องยาก โดยเฉพาะเมื่อมีเครื่องมือให้ใช้

แนวทางการแก้ปัญหา

ในการแก้ปัญหาการทำ Denial of Servce จะสามารถใช้ Firewall และ NIDS โดย Firewall จะทำหน้าที่เป็นตัวกรองแพ็กเก็ตต่างๆ ที่จะเข้าและออกจากเครือข่ายที่ผู้ดูแลระบบดูแล เมื่อไฟร์วอลล์ตรวจจับได้ว่าแพ็กเก็ตใดๆ เป็นแพ็กเก็ตที่มีปัญหาจะทำการคัดกรองข้อมูลนั้นออกจากเครือข่ายทันที ซึ่งจะทำการศึกษาเกี่ยวกับไฟร์

วอลล์ในรายละเอียดในหัวข้อถัดไป สำหรับ NIDS เป็นระบบการตรวจจับความผิดปกติในระบบเครือข่าย ในการทำงานจะทำการดึงข้อมูลจากระบบเครือข่ายมาประมวลผลด้วยเทคนิควิธีการต่างๆ และให้ผลลัพธ์เป็นการแจ้งเตือนว่ามีความผิดปกติในระบบเครือข่ายหรือไม่ ในการทำงานในการดูแลระบบเครือข่ายมักจะใช้เครื่องมือทั้งสองนี้ร่วมกัน นอกจากนี้

ในการแก้ปัญหาการScan จะสามารถทำได้โดยการปิดพอร์ตที่ไม่ใช้งาน หรือไม่เปิดบริการที่ไม่มีความจำเป็น กระบวนการนี้สามารถทำได้โดยการตั้งค่าระบบ หรือใช้ไฟร์วอลล์เพื่อช่วยคัดกรองแพ็กเก็ตและปิดพอร์ตที่ไม่จำเป็น การใช้โปรแกรมที่ทำงานในลักษณะ Port Scan Attack Detector นอกจากนี้ยังมีอีกวิธีการหนึ่งคือการเปิดพอร์ดหลอกการ Scan โดยจะทำการตอบสนองต่อ SYN ที่เข้ามายังพอร์ตต่างๆ ทุกพอร์ต ทำให้ผลลัพธ์ที่ได้จากการ Scan ไม่สามารถนำไปใช้งานได้เป็นต้น

สำหรับการทำ Session Hijack ในการตรวจจับและป้องกันโดยใช้อุปกรณ์เช่นไฟร์วอลล์หรือ NIDS อาจทำได้ยากเนื่องจากการทำงานของเครื่องมือดังกล่าวดำเนินการโดยอาศัยข้อมูลจากโพรโตคอลและการทำงานต่างๆ ในปัจจุบัน แต่การตรวจจับและป้องกันการทำ Session Hijack ได้นั้นจำเป็นต้องพึ่งพากระบวนการที่ทำให้เกิด Confidentiality และ Integrity ใน OSI Layer ต่างๆ เช่นการทำ IP Security หรือใช้โปรแกรมที่มีการเข้ารหัสและสามารถตรวจสอบ session ได้เสมอ เช่น Secure Shell, Secure FTP, VPN หรือ IPSec ซึ่งจะกล่าวถึงต่อไป

User Datagram Protocol: UDP

โพรโตคอลยูดีพีเป็นโพรโตคอลที่ทำงานในชั้น Transport อีกโพรโตคอลหนึ่ง โพรโตคอลยูดีพีย่อมาจาก User Datagram Protocol โดยโพรโตคอลนี้จะมีลักษณะเป็น Datagram กล่าวคือ ทำงานเป็นแพ็กเกจเดี่ยว ๆ ไม่มีการสร้างการเชื่อมต่อ และไม่มีการรับรองความถูกต้องของการส่งข้อมูล โพรโตคอลยูดีพี เมื่อจะส่งข้อมูลก็จะส่งทันที โดยไม่สนใจว่าปลายทางในขณะนั้น พร้อมจะรับข้อมูลหรือไม่ หรือส่งไปแล้วปลายทางได้รับข้อมูลอย่างถูกต้องหรือไม่ โพรโตคอลนี้จะทำหน้าที่ส่งผ่านโพรโตคอลไอพีเพียงอย่างเดียวเท่านั้น หน้าที่อื่น ๆ โพรโตคอลระดับแอปพลิเคชัน จะต้องทำเอาเอง

Source Port	Destination Port
Length	Checksum
Data	

รูปที่ 10 UDP Datagram

โพรโตคอลยูดีพี มักจะใช้ในกรณีที่เป็นการส่งข้อมูลขนาดสั้น ๆ เพียงแพ็กเกจเดียว ซึ่งจะทำให้ส่งได้รวดเร็วกว่า เพราะไม่มีการทำงานที่ซับซ้อนเหมือนทีซีพี หรือใช้กับข้อมูลที่ไม่สนใจเรื่องความถูกต้องของข้อมูลมากนัก เช่น การส่งข้อมูลประเภทเสียง รูปแบบของดาต้าแกรมยูดีพีไม่ซับซ้อน เพราะไม่มีภาระงานอะไรมีเพียงพอร์ตต้นทาง พอร์ตปลายทาง ความยาวของแพ็กเกจทั้งหมด และส่วนตรวจสอบความผิดพลาดเท่านั้น ดังแสดงในรูปที่ 10

สำหรับโพรโตคอลยูดีพีแล้ว ข้อแตกต่างกับโพรโตคอลทีซีพีประการหนึ่ง คือ ความยาวของแพ็กเกจในแบบ UDP จะมีความยาวได้ไม่จำกัด (จำกัดที่ขนาดของแพ็กเกจ IP) โดยความยาวของข้อมูลที่ส่งแต่ละครั้งโปรแกรมแอปพลิเคชันที่เรียกใช้โพรโตคอลยูดีพี จะต้องเป็นผู้กำหนดเอง ซึ่งอาจทำให้เกิดผลเสียได้ เพราะหากกำหนดไว้ยาวมากเกินไป จะทำให้เกิดภาระงานที่ระดับชั้นไอพี โดยจะต้อง Fragment ออกเป็นแพ็กเกจเล็ก ๆ จำนวนมาก ดังนั้นหากต้องใช้โพรโตคอลยูดีพีแล้ว ควรคำนึงขนาดข้อมูลที่ไม่ก่อให้เกิดการ Fragment ด้วย

จุดอ่อนและการโจมตี

โพรโตคอล UDP เป็นโพรโตคอลที่ออกแบบมาเพื่อการเชื่อมต่อที่รวดเร็ว จึงไม่มีกฎเกณฑ์ที่เข้มงวดในการควบคุมการเชื่อมต่อเหมือน TCP ซึ่งการที่ UDP ไม่มีความเข้มงวดในการควบคุมนี่เองทำให้ UDP กลายเป็นเครื่องมือสำคัญในการโจมตีระบบ โดยผู้โจมตีระบบสามารถสร้าง IP Packet หุ้มข้อมูล UDP โดยทำการปลอมแปลงข้อมูลในเฮดเดอร์ของ IP Packet ให้ผ่านไฟร์วอลล์ได้ แล้วส่ง UDP Packet ไปยังเครื่องเป้าหมาย เนื่องจากสำหรับไฟร์วอลล์นั้นอาจป้องกันการโจมตีของ UDP ได้ยากเนื่องจากมีบริการที่จำเป็นต้องใช้โพรโตคอลนี้อยู่ในทุกๆ ระบบคือ DNS (UDP port 53) นอกจากนี้ยังมีการโจมตีระบบในลักษณะการส่งข้อมูลปริมาณมากเข้าสู่ระบบ และการ Scan port ที่สามารถใช้ UDP เป็นโพรโตคอลหลักในการทำการโจมตีได้

แนวทางการแก้ปัญหา

แนวทางการแก้ปัญหาการโจมตีโดยใช้โพรโตคอล UDP ยังคงต้องใช้เครื่องมือในการคัดกรองข้อมูลในเครือข่ายและตรวจจับความผิดปกติในเครือข่ายโดยการไฟร์วอลล์ และ NIDS

Internet Protocol: IP

โพรโตคอล IP เป็นโพรโตคอลหลักในการรับส่งข้อมูลระหว่างอุปกรณ์ข้ามเครือข่ายผ่านอินเตอร์เน็ต รูปแบบของแพ็กเกจหรือที่เรียกว่าดาตาแกรมของไอพีนั้น แสดงดัง**Error! Reference source not found.**

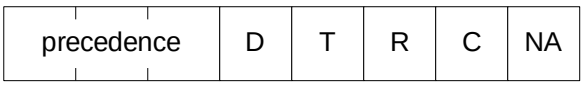
Version	IHL	Type of Service	Total Length
Identification		Flags	Fragmemt Offset
Time to Live	Protocol	Header Checksum	
Source IP Address			
Destination IP Address			
Options + Padding			
Data			
...			

รูปที่ 11 รูปแบบของแพ็กเก็ตไอพี

รายละเอียดของแต่ละฟิลด์ภายในแพ็กเกจไอพีได้แก่

- Version มีขนาด 4 บิต ทำหน้าที่แสดงเวอร์ชันของโพรโตคอล โดยเวอร์ชันที่ใช้งานในปัจจุบัน คือ เวอร์ชันที่ 4
- IHL (Internet Header Length) ทำหน้าที่บอกความยาวของแพ็กเกจ เฉพาะในส่วนของเฮดเดอร์ โดยส่วนของเฮดเดอร์จะเริ่มรับตั้งแต่ฟิลด์ Version จนถึงไบต์ก่อนจะถึงฟิลด์ข้อมูล โดยข้อมูลในฟิลด์นี้จะมีหน่วยเป็น 32 บิต หรือ 4 ไบต์ เช่น หากในฟิลด์ IHL มีค่าเป็น 6 จะมีความหมายว่าส่วนเฮดเดอร์นั้นยาว 24 ไบต์ ดังนั้นความยาวของส่วนหัวจะต้องมีความยาวเป็นจำนวนเท่าของ 4 ไบต์เสมอ และหากข้อมูลในส่วนหัวมีความยาวไม่เป็นจำนวนเท่าของ 4 ไบต์ จะมีการเพิ่มความยาวจนครบจำนวนเท่าของ 4 ไบต์ โดยฟิลด์ Padding จะทำหน้าที่นี้

- TOS (Type of Service) มีขนาด 8 บิต ฟิลด์นี้ใช้กำหนดชนิดของการให้บริการ โดยฟิลด์นี้ มีรูปแบบข้อมูลดังรูปที่ 12



รูปที่ 12 *รายละเอียดของฟิลด์ TOS*

ในฟิลด์ Precedence นั้นจะใช้กำหนดระดับความสำคัญของแพ็กเกจ ซึ่งมีได้ 8 ระดับ โดยระดับ 0 จะต่ำที่สุด และระดับ 7 จะสูงที่สุด โดยอุปกรณ์เลือกเส้นทางใช้ข้อมูลในส่วนนี้ในการจัดลำดับความสำคัญในการส่งต่อข้อมูล อย่างไรก็ตามจนถึงปัจจุบันฟิลด์นี้ก็ยังไม่ได้มีการนำมาใช้งานในการรับส่งข้อมูล นอกจากนั้นอุปกรณ์เลือกเส้นทางส่วนใหญ่ ก็ไม่ได้ใช้ฟิลด์นี้ในการจัดลำดับความสำคัญของการส่งต่อข้อมูล

ในฟิลด์ D (Minimize Delay) นั้นหากมีค่า 1 จะหมายถึงแพ็กเกจนี้ต้องการเส้นทางที่มี Delay น้อยที่สุด ฟิลด์ T (Maximum Throughput) หากมีค่า 1 หมายถึงแพ็กเกจนี้ต้องการเส้นทางที่มีขนาดการส่งข้อมูลมากที่สุด ฟิลด์ R (Maximum Reliability) หากฟิลด์นี้เป็น 1 หมายถึงแพ็กเกจนี้ต้องการเส้นทางที่มีความเชื่อถือได้สูง และฟิลด์ C (Minimize Monetary Cost) หากฟิลด์นี้เป็น 1 หมายถึงแพ็กเกจนี้ ต้องการเส้นทางที่มี Cost ต่ำที่สุด สำหรับฟิลด์ NA หมายถึงไม่ได้มีการใช้งาน

ในบิตทั้ง 4 ข้างต้นนั้น จะมีบิตที่เป็น 1 ได้เพียงบิตเดียวเท่านั้น เช่น Telnet และ FTP จะให้บิต D เป็น 1 SNMP จะกำหนดให้บิต R เป็น 1 และ NNTP จะกำหนดให้บิต C เป็น 1 เป็นต้น และหากบิตทั้ง 4 มีค่าเป็น 0 ก็หมายถึงเป็นแพ็กเกจข้อมูลทั่วไป ไม่มีความพิเศษอะไร

- Total Length ฟิลด์นี้จะหมายถึงความยาวทั้งหมดของแพ็กเกจที่รวมทั้งส่วนเฮดเดอร์ และ ส่วนของข้อมูล แต่จะต่างกับ IHL ตรงที่มีหน่วยนับเป็นไบต์ และเนื่องจากฟิลด์นี้มีความยาว 16 บิต ดังนั้นจึงสามารถระบุความยาวสูงสุดของแพ็กเกจได้เท่ากับ FFFFh หรือ 65535 ซึ่งจะหมายความว่าขนาดของแพ็กเกจจะมีความยาวเกินกว่า 65535 ไม่ได้

- Identification, Flags และ Fragment Offset เป็นฟิลด์ที่ทำงานร่วมกัน ใช้ในการแบ่งดาตาแกรมออกเป็นแพ็กเกจย่อย ๆ เพื่อให้สามารถส่งผ่านไปยังเครือข่ายที่มีค่า MTU (Maximum Transmission Unit) ได้ ซึ่งเรื่องนี้จะกล่าวถึงในหัวข้อถัดไป
- TTL (Time to Live) มีขนาด 8 บิต ใช้สำหรับป้องกันการวนลูปไม่สิ้นสุดของแพ็กเกจ โดยเครื่องคอมพิวเตอร์หรืออุปกรณ์ที่ส่งแพ็กเกจไอพี จะทำหน้าที่กำหนดตัวเลขนี้ขึ้นมา โดยตัวไปจะใช้ตัวเลข 64,128 หรือ 255 เมื่อแพ็กเกจผ่านอุปกรณ์เลือกเส้นทาง 1 ครั้ง ก็จะลดตัวเลขนี้ในแพ็กเกจลง 1 และหากเกิดลูปในการส่งต่อแพ็กเกจขึ้น ตัวเลขนี้จะลดลงเรื่อย ๆ ทีละ 1 จนกระทั่งเป็น 0 ก็จะทิ้งแพ็กเกจนี้ไป ดังนั้นตัวเลขนี้ นอกเหนือจากป้องกันการเกิดการวนลูปส่งต่อไม่สิ้นสุดแล้ว ยังสามารถบอกจำนวนอุปกรณ์เลือกเส้นทางที่แพ็กเกจนี้วิ่งผ่านมาได้อีกด้วย
- Protocol มีขนาด 8 บิต ทำหน้าที่บอกโพรโตคอลในระดับที่สูงกว่าที่เรียกใช้โพรโตคอล IP เช่น 1 หมายถึง ICMP, 6 หมายถึง TCP และ 8 หมายถึง UDP เป็นต้น
- Header Checksum มีขนาด 16 บิต จะเป็นค่าที่คำนวณเพื่อหาความผิดพลาดของส่วนเฮดเดอร์
- Source IP Address มีขนาด 32 บิต เป็นหมายเลขไอพี ของต้นทาง
- Destination IP Address มีขนาด 32 บิต เป็นหมายเลขไอพี ของปลายทาง
- Option มีขนาดไม่คงที่ ใช้สำหรับส่งข้อมูลเพิ่มเติม ซึ่งจะกล่าวถึงต่อไป
- Padding มีขนาด 0-3 ไบต์ มีหน้าที่เติมข้อมูลในส่วนเฮดเดอร์ในครบเป็นจำนวนเท่าของ 4 ไบต์
- Data มีขนาดเท่าไรก็ได้ แต่ไม่เกิน 65535 ลบด้วยขนาดของเฮดเดอร์

Fragmentation and Reassemble

ในการส่งแพ็กเกจไอพีไปยังผู้รับที่อยู่ในที่ต่าง ๆ ของโลกนั้น จำเป็นต้องผ่านเครือข่ายที่หลากหลาย ทั้งเครือข่ายแบบ LAN และเครือข่ายแบบ WAN ทั้งเทคโนโลยีต่าง ๆ ซึ่งในบรรดาเครือข่ายต่างๆ นั้นแม้ว่าจะมีความสามารถในการรองรับแพ็กเกจไอพี เหมือนกันหมด แต่เนื่องจากสถาปัตยกรรมของเทคโนโลยีเหล่านั้นต่างกัน ทำให้ค่าขนาดของข้อมูลที่ขนส่งได้ใน 1 ครั้งต่างกัน เช่น ในเครือข่ายอีเทอร์เน็ตมีค่าขนาดของข้อมูลที่ขนส่งได้ระหว่าง 64 ไบต์ถึง 1500 ไบต์ แต่เครือข่าย FDDI มีค่าขนาดข้อมูลที่ขนส่งได้สูงถึง 8000 ไบต์ ซึ่งค่า

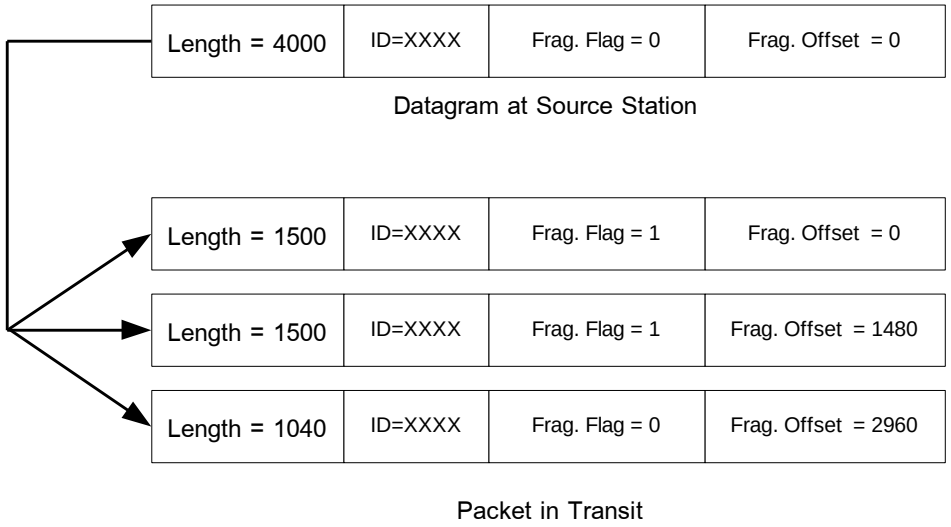
ขนาดข้อมูลที่ขนส่งได้ หรือ MTU (Maximum Transmission Unit) ที่แตกต่างกันนี่เอง ที่ทำให้การขนส่งแพ็กเกจไอพีระหว่างเครือข่ายที่ต่างกันมีปัญหาได้ เช่น สมมติว่าข้อมูลเริ่มส่งจากเครือข่าย FDDI ที่มีขนาด MTU 4325 ไบต์ พอแพ็กเกจนั้นมาถึงฝั่งผู้รับที่เป็นเครือข่ายอีเทอร์เน็ต ซึ่งมี MTU เพียง 1500 ไบต์ ก็จะไม่สามารถส่งแพ็กเกจได้

ดังนั้นเพื่อให้กระบวนการขนส่งจากต้นทางไปยังปลายทาง ไม่มีอุปสรรคในเรื่องที่เกี่ยวกับ MTU ทางผู้ออกแบบโพรโตคอลไอพี จึงได้กำหนดขั้นตอนขึ้นมาขั้นตอนหนึ่ง ซึ่งจะใช้กรณีที่เกิดเหตุการณ์ที่ 2 เครือข่ายมีค่า MTU ไม่เท่ากัน โดยเฉพาะการส่งจากเครือข่ายที่มีค่า MTU มาก ไปยังเครือข่ายที่มีค่า MTU น้อย ขั้นตอนนี้มีชื่อเรียกว่า Fragmentation ซึ่งก็คือกระบวนการแตกแพ็กเกจไอพีออกเป็นแพ็กเกจย่อย ๆ ที่มีขนาดเล็กลง เพื่อให้สามารถผ่านสู่เครือข่ายที่มีค่า MTU น้อยกว่าได้ วิธีการเช่นนี้ ทำให้การส่งผ่านแพ็กเกจไอพีไปยังเครือข่ายใด ๆ สามารถทำได้โดยไม่มีข้อจำกัด

ในการ ทำ Fragmentation นั้นจะอาศัยฟิลด์ในแพ็กเกจไอพี จำนวน 3 ฟิลด์ คือ Identification, Flags และ Fragment Offset โดยฟิลด์ Identification มีความยาว 16 บิต ทำหน้าที่เป็นเลขประจำดาตาแกรม (หมายถึงข้อมูลก่อนการ Fragment) โดยแพ็กเกจไอพีที่แตก (Fragment) ออกจากดาตาแกรมเดียวกัน จะมีหมายเลขเดียวกัน หมายเลขนี้จะทำหน้าที่บอกกับอุปกรณ์ปลายทางว่าแพ็กเกจที่ได้รับเกิดจากดาตาแกรมเดียวกันหรือไม่ โดยหากมีหมายเลข Identification เดียวกัน แสดงว่าเกิดจาก Datagram เดียวกัน ดังนั้นเมื่อแพ็กเกจส่งถึงปลายทาง ก็จะนำแพ็กเกจที่เกิดจากดาตาแกรมเดียวกัน กลับมารวมกันเป็นดาตาแกรมเดิม

ฟิลด์ Flags ควบคุมและบอกรายละเอียดของการ Fragment โดยฟิลด์ Flags นี้จะมี 3 บิต บิตแรกไม่ใช้งาน และต้องมีค่าเป็น 0 เสมอ บิตที่ 2 (D) เป็นบิตที่บอกว่าดาตาแกรมนี้สามารถ Fragment ได้หรือไม่ โดยหากมีค่าเป็น “0” หมายถึงให้อุปกรณ์เลือกเส้นทางสามารถทำการ Fragment ดาตาแกรมนี้ได้หากจำเป็น หากมีค่าเป็น “1” หมายถึงห้ามมิให้มีการ Fragment ดาต้าแกรมนี้ ซึ่งหากกรณีที่บิตนี้มีค่าเป็น 1 และดาตาแกรมต้องวิ่งผ่านเครือข่ายที่มี MTU น้อยกว่าขนาดของดาตาแกรม อุปกรณ์เลือกเส้นทางจะทิ้งดาต้าแกรมนั้นไป พร้อมแจ้งข้อผิดพลาด โดยทั่วไปบิตนี้จะมีค่าเป็น “0” สำหรับบิตที่ 3 (M) นั้นจะทำหน้าที่บอกว่าแพ็กเกจนี้เป็นแพ็กเกจสุดท้ายของดาต้าแกรมหรือไม่ โดยหากเป็น “0” หมายถึงเป็นแพ็กเกจสุดท้าย

ฟิลด์ Fragment Offset มีขนาด 13 บิต ทำหน้าที่บอกว่าแพ็กเกจนี้อยู่ส่วนไหนของดาตาแกรม เช่น หากมีค่า 128 หมายถึงแพ็กเกจนี้อยู่ในตำแหน่ง 1024 (128 * 8 = 1024) ของข้อมูลในดาตาแกรมนั้น จากที่กล่าวมาจะเห็นได้ว่า เราสามารถบอกได้ว่าแพ็กเกจนั้นผ่านการ Fragment มาหรือไม่ โดยดูจากค่าของ Flags (M) และค่าของ Fragment Offset หากค่าของ Flag M มีค่าเป็น 0 และฟิลด์ Fragment Offset มีค่าเป็น 0 แล้ว หมายความว่าแพ็กเกจนนี้เป็นแพ็กเกจแรกของดาตาแกรม และไม่มีแพ็กเกจต่อจากนี้ ซึ่งก็คือแพ็กเกจนี้เป็นแพ็กเกจที่ไม่ผ่านการ Fragment มา หากฟิลด์ทั้ง 2 ไม่มีค่าดังกล่าวแล้ว ย่อมหมายความว่าแพ็กเกจนั้นผ่านการ Fragmentation เพื่อให้เข้าใจการทำ Fragmentation ดีขึ้น จะขอยกตัวอย่างดังรูปที่ 13



รูปที่ 13 ตัวอย่างของการ Fragmentation

ในรูปที่ 13 แสดงให้เห็นถึงการ Fragment ดาต้าแกรมขนาด 4000 ไบต์ ไปเป็นแพ็กเกจที่มีขนาดไม่เกิน 1500 ไบต์ โดยการแยกดาต้าแกรมนั้นจะใช้วิธีการก๊อปปี้ข้อมูลส่วนหัวของดาต้าแกรม มาเป็นส่วนหัวของแพ็กเกจทั้ง 3 แพ็กเกจ ดังนั้นทั้ง 3 แพ็กเกจจะมีแอดเดรสต้นทางและแอดเดรสปลายทางเดียวกัน และทุกแพ็กเกจจะมีค่าในฟิลด์ Identification เหมือนกัน เพื่อแสดงว่าเป็นแพ็กเกจที่แยกมาจากดาต้าแกรมเดียวกัน ในแพ็กเกจแรกจะเห็นว่า Fragment Offset มีค่าเป็น 0 และ Fragment Flag มีค่าเป็น 1 แสดงให้เห็นว่าแพ็กเกจนี้เป็นแพ็กเกจแรกของดาต้าแกรม และยังมีแพ็กเกจต่อไปอีก

ในแพ็กเกจที่ 2 มีค่า Fragment Offset เป็น 1480 (เก็บข้อมูล 13 บิตด้วยค่า 1480/8 = 185) แสดงให้เห็นว่าข้อมูลในแพ็กเกจนี้อยู่ในตำแหน่งที่ 1480 ของดาต้าแกรม และมีค่า Fragment Flag เป็น 1 แสดงว่ายังไม่ใช่แพ็กเกจสุดท้าย จากแพ็กเกจที่ 2 นี้ เราอาจสังเกตเห็นว่าในขณะที่ค่าของ Length มีค่าเป็น 1500 แต่ค่า Fragment Offset ของแพ็กเกจที่ 2 กลับเริ่มต้นที่ 1480 ซึ่งแสดงให้เห็นว่าในแพ็กเกจที่ 1 นั้นบรรจุข้อมูลของดาต้าแกรมไปเพียง 1480 ไบต์เท่านั้น สำหรับ 20 ไบต์ที่หายไปนั้นไม่ได้หายไปไหน แต่เป็นข้อมูลในส่วนของเฮดเดอร์ สำหรับแพ็กเกจที่ 3 นั้น มี Length เท่ากับ 1040 แสดงให้เห็นว่ายังคงเหลือข้อมูลจากดาต้าแกรมเพียง 1040 และมีส่วนของ Fragment Flag เท่ากับ 0 แสดงให้เห็นว่าแพ็กเกจนี้เป็นแพ็กเกจสุดท้ายของดาต้าแกรมแล้ว

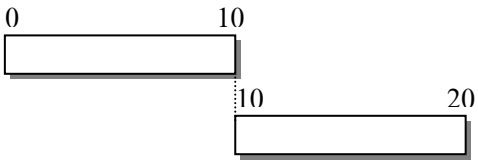
เมื่อแพ็กเกจทั้ง 3 เดินทางไปในเครือข่ายอินเตอร์เน็ต แพ็กเกจทั้ง 3 จะเป็นอิสระต่อกัน ซึ่งหมายความว่าแพ็กเกจทั้ง 3 อาจเดินทางไปคนละเส้นทางกันก็ได้ ด้วยเหตุนี้ในระหว่างการเดินทางแพ็กเกจทั้ง 3 จะไม่มีโอกาสรวมกันได้อีกเลย จนกระทั่งแพ็กเกจทั้ง 3 เดินทางมาจนถึงปลายทางแล้วเท่านั้น แพ็กเกจทั้ง 3 จึงจะกลับมารวมเป็นดาต้าแกรมเดียวกันอีกครั้ง โดยจะเรียกกระบวนการที่แพ็กเกจที่ผ่านการ Fragment กลับมารวมกันเป็นดาต้าแกรมนี้ว่า Reassemble โดยเครื่องคอมพิวเตอร์ปลายทางจะต้องจัดเตรียมบัฟเฟอร์ที่เพียงพอสำหรับดาต้าแกรมทั้งหมด เพื่อเป็นพื้นที่ที่ใช้ในการจัดเรียงแพ็กเกจ ทั้งนี้เนื่องจากแต่ละแพ็กเกจอาจเดินทางไปคนละทาง ดังนั้นแพ็กเกจของดาต้าแกรมอาจเดินทางมาถึงในเวลาไม่เท่ากัน และอาจเดินทางมาโดยไม่เป็นไปตามลำดับก่อนหลังอีกด้วย และเนื่องจากเครื่องคอมพิวเตอร์ปลายทางมักไม่ทราบว่าขนาดของดาต้าแกรมเป็นเท่าใด จึงต้องจัดเตรียมพื้นที่เท่ากับขนาดสูงสุดของดาต้าแกรม คือ 65,535 ไบต์รอเอาไว้ ซึ่งจุดนี้เองที่ได้กลายเป็นจุดโจมตีหนึ่งได้ ซึ่งจะกล่าวถึงต่อไป

จากที่กล่าวมาจะเห็นได้ว่า ในการทำ Fragment นั้น แม้มีข้อดีที่ทำให้แพ็กเกจไอพีสามารถส่งได้ในทุกเครือข่าย แต่ก็มีข้อเสีย เนื่องจากการหาเส้นทางของเครือข่ายไอพีนั้น ยึดหลักการหาเส้นทางที่ดีที่สุดในขณะนั้น ซึ่งแต่ละแพ็กเกจที่ Fragment มาจากดาตาแกรมเดียวกัน อาจถูกส่งไปคนละทิศทางกันก็ได้ และการรับข้อมูลจะสมบูรณ์ก็ต่อเมื่อฝั่งปลายทางได้รับข้อมูลทุกแพ็กเกจในดาตาแกรมนั้นทั้งหมดแล้วเท่านั้น ซึ่งหากมีแพ็กเกจใดล่าช้า ก็หมายถึงการรวมข้อมูลที่ปลายทางก็จะล่าช้าตามไปด้วย นอกจากนั้นกระบวนการรวมข้อมูลปลายทาง ก็ต้องเสียทรัพยากรส่วนหนึ่งไปเป็นพื้นที่ในการจัดเรียงแพ็กเกจอีกด้วย

ดังนั้นเพื่อให้การส่งข้อมูลมีประสิทธิภาพ และไม่เป็นภาระในการทำ Fragmentation ควรจะกำหนดการส่งข้อมูลแต่ละครั้งให้ไม่เกินค่า MTU ที่น้อยที่สุดในเส้นทางการส่ง ซึ่งหากเป็นโปรแกรมแอปพลิเคชันทั่วไป เราสามารถกำหนดค่านี้ในระบบปฏิบัติการได้ แต่หากไม่ทราบค่า MTU ที่น้อยที่สุด ข้อกำหนดของ RFC 1122 ได้แนะนำค่า MTU ที่เหมาะสมเอาไว้ที่ 576 ซึ่งมีที่มาจากข้อมูลขนาด 512 ไบต์บวกกับไอพีเฮดเดอร์ขนาด 20 ไบต์ และทีซีพีเฮดเดอร์ขนาด 20 ไบต์ และค่าอื่น ๆ ประกอบ ซึ่งค่านี้จะเป็นค่าที่สามารถผ่านทุกเครือข่ายได้โดยไม่ต้องทำ Fragmentation

จุดอ่อนและการโจมตี

การโจมตีในระดับชั้นไอพี จะอาศัยหลักการแฟร็กเมนเตชันและรีแอสเซมเบิ้ลที่กล่าวไว้ข้างต้น โดยทำให้แพ็กเก็ตนั้นต้องมีการรีแอสเซมเบิ้ล (กำหนดค่า MF flag = 0) ซึ่งปกติการรีแอสเซมเบิ้ลแพ็กเก็ตทั้งหมดต้องสามารถเชื่อมต่อกันได้สนิท ดังรูปที่ 2 แต่แพ็กเก็ตที่ผู้บุกรุกส่งไปมีการแก้ไขข้อมูลในบางฟิลด์ ทำให้เกิดความผิดปกติในกระบวนการรีแอสเซมเบิ้ล ซึ่งการโจมตีในลักษณะนี้ แบ่งได้ดังต่อไปนี้



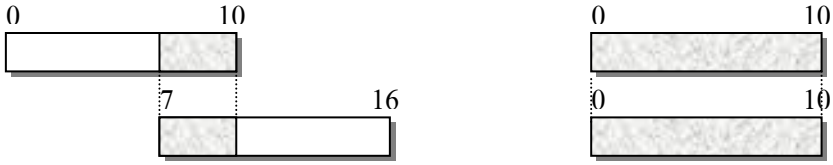
รูปที่ 14 การรีแอสเซมบลีแบบปกติ

การส่งแพ็กเก็ตที่มีลำดับผิดปกติ (Abnormal Sequences of Packets Sending) ปกติการส่งแพ็กเก็ตมักเรียงตามลำดับกันไป หากไม่เรียงลำดับก็ต้องรอจนกว่าแพ็กเก็ตก่อนหน้านี้มาถึง เพื่อเรียงลำดับแพ็กเก็ตที่เครื่องรับ แต่การโจมตีแบบนี้กลับส่งเฉพาะแพ็กเก็ตสุดท้าย เพื่อให้ระบบเป้าหมายรอแพ็กเก็ตก่อนหน้า และส่งไปเป็นปริมาณมากๆ เพื่อให้ระบบเป้าหมายไม่สามารถให้บริการอย่างอื่นได้ โดยปกติแล้วการโจมตีในรูปแบบนี้ผู้โจมตีจะแก้ไขข้อมูลในฟิลด์แสดงลำดับของแพ็กเก็ต (Fragment Offset) ของแพ็กเก็ตไอพี ซึ่งเป็นส่วนที่แสดงลำดับของข้อมูลหลังจากกระบวนการแฟร็กเมนต์เตชัน โดยแก้ให้ส่งแพ็กเก็ตสุดท้ายหรือแพ็กเก็ตหลังๆ เพียงแพ็กเก็ตเดียวเลย ทำให้ระบบเป้าหมายต้องรอแพ็กเก็ตก่อนหน้านี้

รูปที่ 15 แพ็กเก็ตสุดท้ายที่ต้องรอแพ็กเก็ตก่อนหน้า

การส่งแพ็กเก็ตที่มีขนาดเหลื่อมกัน (Overlapped Packets' Size Sending) ปกติแพ็กเก็ตที่ส่งมาต้องนำมาต่อกันที่ระบบเป้าหมายได้พอดี แต่การโจมตีแบบนี้เป็นการส่งแพ็กเก็ตที่มีขนาดเหลื่อมกัน หรือซ้อนทับกัน ทำให้ข้อมูลเมื่อมาต่อกันแล้วเกิดความผิดพลาด หรือไม่สามารถเชื่อมต่อกันได้ โดยปกติแล้วการโจมตีแบบนี้ ผู้บุกรุกสามารถแก้ไขข้อมูลได้ 2 แห่งใหญ่ๆ ได้แก่

การแก้ไขข้อมูลที่ฟิลด์แสดงลำดับของแพ็กเก็ต (Fragment Offset) ของแพ็กเก็ตไอพี หลังจากกระบวนการรีแอสเซมเบิ้ล ซึ่งทำให้ลำดับในการส่งมีความผิดพลาด และอาจเกิดการเหลื่อมล้ำของแพ็กเก็ต กระบวนการรีแอสเซทเบิ้ลอาจเกิดปัญหาได้ และการแก้ไขฟิลด์แสดงความยาวของ (Total Length) ของแพ็กเก็ตไอพี หลังจากกระบวนการรีแอสเซมเบิ้ล ขนาดของแพ็กเก็ตที่มาต่อไม่พอดีกัน ทำให้ไม่สามารถรวมแพ็กเก็ตได้ หรือหากรวมได้ ข้อมูลที่ได้ก็ไม่ถูกต้อง



รูปที่ 16 การรีแอสเซมบลีแบบแพ็กเก็ตมีขนาดเหลื่อมกัน

การส่งแพ็กเก็ตแบบวนลูป (Looping) คือ การส่งโดยกำหนดค่าแอดเดรสต้นทาง (Source Address) และแอดเดรสปลายทาง (Destination Address) ให้เหมือนกันทำให้เกิดการรับส่งวนไปวนมาอยู่ที่เครื่องเป้าหมายเอง เช่น LAND ซึ่งเป็นโปรแกรมโจมตีที่มีการกำหนดแอดเดรสต้นทาง และแอดเดรสปลายทางเป็นค่าเดียวกัน คือ เป็นแอดเดรสของเครื่องเป้าหมายนั่นเอง ทำให้เกิดการส่งวนไปวนมาอยู่ที่เครื่องเป้าหมาย

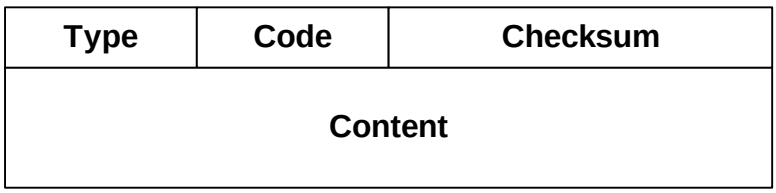
แนวทางการแก้ปัญหา

สำหรับการป้องกันปัญหาการโจมตีในระดับชั้น IP ซึ่งมักจะใช้กระบวนการออกแบบแพ็กเก็ตให้มีความผิดปกติไปจากแพ็กเก็ตมาตรฐานนั้น ควรใช้ไฟร์วอลล์ที่มีความสามารถในการตรวจสอบความผิดปกติดังกล่าว ซึ่งจะทำการ Reassemble แพ็กเก็ตต่างๆ ก่อนส่งไปยังเครื่องปลายทางเพื่อให้แพ็กเก็ตที่ผิดปกติต่างๆ ไม่สามารถเข้าถึงเครื่องปลายทางได้

Internet Control Message Protocol: ICMP

โพรโตคอล ICMP ย่อมาจาก Internet Control Message Protocol ซึ่งหากดูจากชื่อแล้ว ก็พอจะสื่อให้เห็นถึงหน้าที่ของโพรโตคอลนี้ โดย ICMP นั้นเป็นโพรโตคอลที่ใช้ในการส่งข่าวสารระหว่างอุปกรณ์ในเครือข่าย โดยข่าวสารนี้จะเป็นข่าวสารที่แสดงถึงสถานะต่างๆ ของอุปกรณ์ในเครือข่าย ซึ่งจะมีผลให้การทำงานของอุปกรณ์เปลี่ยนไปได้ เช่น หากข่าวสารจากเราเตอร์แจ้งว่ากำลังมีภาระการทำงานมาก ก็อาจทำให้เราเตอร์ตัวก่อนหน้า ชะลอความเร็วในการส่งข้อมูลลง หรืออาจเปลี่ยนเส้นทางในการส่งข้อมูลได้ ด้วยหน้าที่อันหลากหลายและมีความสำคัญของ ICMP ดังที่กล่าวมา โพรโตคอล ICMP จึงมีความสำคัญกับเรื่องของความปลอดภัยอย่างมาก

โพรโตคอล ICMP เป็นโพรโตคอลที่จัดว่าทำงานในระดับชั้นที่ 3 ของ OSI แต่โพรโตคอล ICMP ไม่มีความสามารถในการเดินทางด้วยตัวเองได้ ดังนั้นการส่งข้อมูลของโพรโตคอลจะส่งผ่านแพ็กเกจไอพีอีกทีหนึ่ง โดยรูปแบบข้อมูลในแพ็กเกจ ICMP แสดงดังในรูปที่ 17



รูปที่ 17 รูปแบบข้อมูลของแพ็กเกจ ICMP

สำหรับรายละเอียดของแต่ละฟิลด์ภายในแพ็กเกจ ICMP มีดังต่อไปนี้

- Type มีขนาด 8 บิตทำหน้าที่บอกประเภทของข้อมูลที่ส่งมา โดยมีรายละเอียดดังตารางข้างล่างนี้
- Code มีขนาด 8 บิต ทำหน้าที่บอกประเภทย่อยของข้อมูลที่ส่งมา
- Checksum มีขนาด 16 บิต ใช้สำหรับตรวจสอบความผิดพลาดของแพ็กเกจ
- Contents มีขนาดไม่คงที่ ฟิลด์นี้จะเก็บข้อความของข่าวสารหรือรายงานข้อผิดพลาดที่ส่งมา

เนื่องจากโพรโตคอล ICMP เป็นโพรโตคอลที่ใช้ในการส่งข่าวสารทั่วไป จึงมีการทำงานหลายหน้าที่ ดังนั้นเพื่อให้เข้าใจได้ง่าย จะขอแยกอธิบายเป็นกลุ่ม ๆ ไป

กลุ่มการใช้ ICMP เพื่อตรวจสอบโฮสต์ จะใช้ ICMP ที่มีรหัสเป็น 0 และ 8 โดย ICMP รหัส 0 (Echo) จะใช้ในการส่งไปยังอุปกรณ์เครือข่ายเพื่อตรวจสอบว่าอุปกรณ์เครือข่ายนั้น ๆ ทำงานในระบบ TCP/IP หรือไม่ หากอุปกรณ์นั้นได้รับแพ็กเกจ ICMP ที่มีรหัส 0 และทำงานกับโพรโตคอล TCP/IP ก็จะตอบกลับด้วยแพ็กเกจ ICMP ที่มีรหัสเป็น 8 (Echo Reply) คือหมายความว่าทำงานอยู่ โดยโปรแกรมที่ใช้ ICMP ชนิดนี้ คือ โปรแกรม Ping และ Traceroute โดยข้างล่างนี้จะแสดงผลลัพธ์ของคำสั่ง Ping ใน Linux

```
$ ping 161.246.4.3

PING 161.246.4.3 : 56 data bytes

64 bytes from 161.246.4.3: icmp_seq=0 ttl=254 time=1.1 ms

64 bytes from 161.246.4.3: icmp_seq=1 ttl=254 time=1.0 ms

64 bytes from 161.246.4.3: icmp_seq=2 ttl=254 time=1.0 ms

64 bytes from 161.246.4.3: icmp_seq=3 ttl=254 time=1.0 ms
```

กลุ่มการใช้ ICMP เพื่อรายงานความผิดพลาดกรณีที่ติดต่อปลายทางไม่ได้ จะใช้ ICMP ที่มีรหัส 3 โดยในฟิลด์ Code จะบอกถึงสาเหตุที่ติดต่อปลายทางไม่ได้ เช่น

- หาก Code เป็น 0 จะหมายถึงไม่สามารถค้นหาเครือข่ายนี้ได้ (Network Unreachable)
- หาก Code เป็น 1 หมายถึงไม่สามารถค้นหาโฮสต์ได้ (Host Unreachable)

- หาก Code เป็น 2 หมายถึงในโฮสต์นั้น ไม่สนับสนุนโพรโตคอลนั้น (Protocol Unreachable)
- หาก Code เป็น 3 หมายถึงในโฮสต์นั้น ไม่เปิด Port นั้นไว้ (Port Unreachable)
- หาก Code เป็น 4 หมายถึงหากจะไปในเครือข่ายนั้น จะต้องทำการ Fragment แต่กำหนดไว้ว่าห้าม Fragment ในแพ็กเกจนั้น (Fragmentation needed but Do Not Fragment Bit was set)

กลุ่มการใช้ ICMP ในการรายงานสถานะของเราเตอร์ จะใช้ ICMP ที่มีรหัส (Type) ดังต่อไปนี้

- หากรหัสเป็น 4 หมายถึงเราเตอร์กำลังมีภาระงานมาก อันอาจเป็นเหตุให้ทำงานไม่ทันหากยังได้รับแพ็กเกจจำนวนมากอยู่ จึงส่ง ICMP เพื่อบอกให้เราเตอร์หรือโฮสต์ตัวอื่น ๆ ที่ส่งข้อมูลมายังเราเตอร์นั้น ลดอัตราการส่งแพ็กเกจลง (Source Quench)
- หากรหัสเป็น 5 หมายถึงเราเตอร์พบว่ามีเส้นทางที่เหมาะสมกว่าสำหรับแพ็กเกจนั้น ๆ จะส่ง ICMP นี้ไปบอกให้ส่งแพ็กเกจที่มีแอดเดรสไอพีเป้าหมายนั้น ๆ ไปยังเส้นทางอื่น (Redirect)
- หากรหัสเป็น 9 และ 10 ใช้ในการตรวจหาเราเตอร์ (9=Router Advertisement, 10=Router Solicitation)

กลุ่มการใช้ ICMP ในการแจ้งข้อผิดพลาดเกี่ยวกับแพ็กเกจไอพี จะใช้ ICMP ที่มีรหัส (Type) ดังต่อไปนี้

- หากรหัสเป็น 11 จะหมายถึง แพ็กเกจนั้นเดินทางจนหมดเวลา (Time Exceed for datagram) โดย หาก Code เป็น 0 แสดงว่าสาเหตุจาก TTL=0 หาก Code เป็น 1 แสดงว่าสาเหตุจากการทำ Reassemble ไม่สมบูรณ์
- หากรหัสเป็น 12 จะหมายถึงส่วนหัวของแพ็กเกจไอพีมีความผิดปกติ (Parameter problem on datagram)

กลุ่มการใช้ ICMP เพื่อสอบถามข้อมูล จะใช้ ICMP ที่มีรหัส (Type) ดังต่อไปนี้

- หากรหัสเป็น 13 และ 14 จะเป็นการสอบถามเวลา (Time Stamp Request) และตอบเวลากลับ (Time Stamp Reply)
- หากรหัสเป็น 17 และ 18 จะเป็นการสอบถามซับเน็ตมาส์ก (Address Mask Request) และตอบกลับ (Address Mask Reply)

จากโพรโตคอล ICMP ที่อธิบายมาทั้งหมดจะเห็นว่ามีการใช้งานที่หลากหลายมาก และมีผลกระทบกับการทำงานของระบบอย่างมาก ดังนั้นหากมีการโจมตีผ่านโพรโตคอลนี้ ก็จะสามารถสร้างผลกระทบได้มาก ซึ่งจะกล่าวถึงต่อไป

จุดอ่อนและการโจมตี

เนื่องจากโพรโตคอล ICMP เป็นโพรโตคอลที่ใช้สำหรับการส่ง Message ระหว่างอุปกรณ์เพื่อแจ้งรายละเอียดต่างๆ ดังนั้นจึงมีการนำมาใช้เพื่อหาข้อมูลระบบและเครือข่ายในลักษณะต่างๆ นอกจากนี้ Message ที่ใช้ควบคุมการทำงานยังสามารถนำมาใช้ประโยชน์ในการปรับเปลี่ยนการทำงานของโพรโตคอลมาตรฐานต่างๆ ได้ยกตัวอย่างเช่น การใช้ ICMP Echo และ ICMP Reply ในการสแกนหาเครื่องคอมพิวเตอร์ในเครือข่ายว่ามีเครื่องคอมพิวเตอร์เครื่องใดเปิดใช้งานอยู่บ้าง และการใช้ คำสั่ง Traceroute ซึ่งใช้โพรโตคอล ICMP มาหาข้อมูลเกี่ยวกับแผนผังของเครือข่ายที่ใช้งานกันอยู่ได้

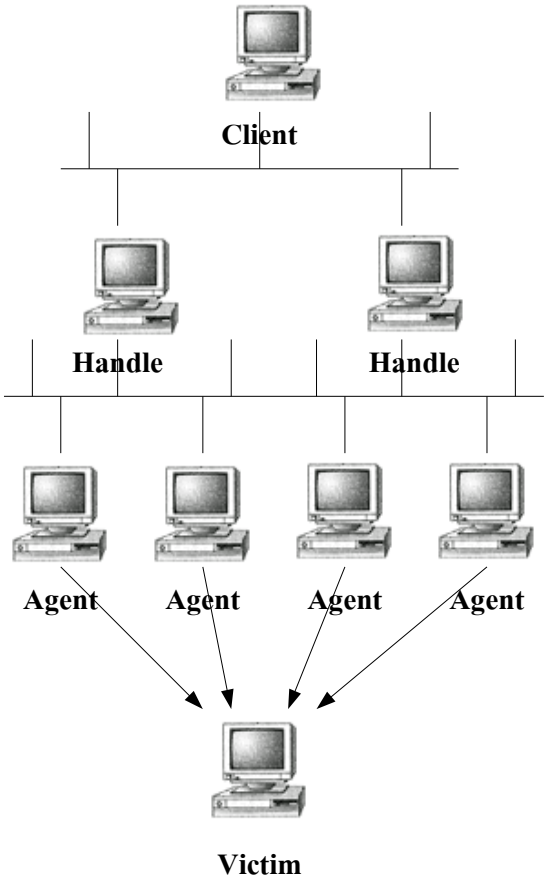
แนวทางการแก้ปัญหา

ถึงแม้ว่าการใช้งาน ICMP จะทำให้เกิดการค้นหาข้อมูลเกี่ยวกับระบบและเครือข่ายได้ง่ายขึ้น หนทางหนึ่งในการปิดการใช้บริการ ICMP คือการให้อุปกรณ์เราเตอร์ทำการคัดกรองข้อมูล ICMP ออกจากระบบซึ่งเป็นวิธีการที่ทำได้ง่าย แต่วิธีการดังกล่าวนี้จะทำให้เกิดปัญหากับการดูแลระบบได้เช่นเดียวกัน เนื่องจาก ICMP จะเป็นโพรโตคอลที่มีประโยชน์และถูกใช้งานเป็นอันดับต้นๆ ในการตรวจสอบความปิดปกติในระบบเครือข่าย

ดังนั้นกระบวนการที่ควรทำคือการออกแบบและตั้งค่าระบบให้สามารถใช้งาน ICMP ได้ในบางคำสั่งที่จำเป็นต้องใช้งาน และสามารถเรียกใช้ได้ในส่วนของระบบส่วนกลางเท่านั้น สำหรับในเครื่องเซิร์ฟเวอร์หรือเครื่องคอมพิวเตอร์ส่วนบุคคลสามารถตั้งค่าไฟร์วอลล์ส่วนบุคคล (Personal Firewall) ให้ป้องกันโพรโตคอล ICMP ทั้งหมดหรือบางส่วน จะเพิ่มความปลอดภัยได้มากขึ้น

<u>การโจมตีรูปแบบอื่นๆ</u>

การทำงานของการโจมตีเพื่อปิดบริการแบบกระจาย มีความแตกต่างจากการโจมตีเพื่อปิดบริการเล็กน้อย กล่าวคือ การโจมตีเพื่อปิดบริการจะใช้คอมพิวเตอร์เพียงเครื่องเดียว แต่การโจมตีเพื่อปิดบริการแบบกระจาย จะใช้คอมพิวเตอร์มากกว่านั้น อาจจะเป็นร้อยเป็นพันๆ เครื่อง ซึ่งแน่นอนว่า ความรุนแรงจะเพิ่มขึ้นจนทำให้เหยื่อที่ถูกการโจมตีในรูปแบบนี้ได้รับความเสียหายได้รวดเร็วยิ่งขึ้นในรูปที่ 18 นี้แสดงโครงสร้างการทำงานของ การโจมตีเพื่อปิดบริการแบบกระจาย



รูปที่ 18 โครงสร้างการทำงานของ DDoS

จากรูปเครื่องไคลเอ็นต์ คือ ผู้ควบคุมการโจมตี ซึ่งก็คือเครื่องของแฮกเกอร์ เครื่อง แฮนด์เลอร์ คือ โฮสต์ที่มีโปรแกรมพิเศษที่ทำงานบนเครื่อง โดยแต่ละเครื่องสามารถควบคุมเครื่องเอเจนต์ได้หลายเครื่อง ส่วน

เครื่องเอเจนต์ คือ โฮสต์ที่มีโปรแกรมพิเศษทำงานบนเครื่อง จะรับผิดชอบการสร้างสตรีมของแพ็กเก็ตที่ผิดปกติที่ส่งไปยังเครื่องที่ตกเป็นเหยื่อโดยตรง โดยโปรแกรมพิเศษที่ทำงานอยู่บนเครื่องแฮนด์เลอร์และเครื่องเอเจนต์นั้น แฮกเกอร์จะต้องนำไปฝังในเครื่องเหล่านั้น ซึ่งหมายความว่าแฮกเกอร์จะต้องครอบครองระบบนั้น ๆ ให้ได้ก่อน จึงจะสามารถฝังโปรแกรมได้ ดังนั้นจะเห็นได้ว่าการโจมตีในลักษณะนี้ ต้องใช้ความพยายามในการเซ็ทอัประบบอย่างมาก แต่ผลของการโจมตีก็มีความร้ายแรง และยากจะป้องกันได้ โดยการโจมตีที่เกิดขึ้นใน Distributed Denial of Service นั้นสามารถนำเอาการโจมตีทุกประเภทมารวมกัน โดยสามารถสั่งให้เครื่องเอเจนต์ต่างๆ ทำการโจมตีเหมือนๆ กัน หรือแตกต่างกันได้ตามลักษณะการทำงานของโปรแกรมที่ใช้สั่งการ ส่วนโปรแกรมที่ผู้โจมตีรู้จักกันเป็นอย่างดี คือ Trinoo , TFN , TFN2K , TFN3K , Shaft และ Mstream

การป้องกัน Distributed Denial of Service นั้นในขั้นต้นสามารถป้องกันได้โดยใช้ไฟร์วอลล์เนื่องจากแพ็กเก็ตที่ส่งมาจากเครื่องต่างๆ ที่จะโจมตีระบบได้นั้น จะมีการใช้งานโปรแกรมที่ใช้ในการโจมตี หรือออกแบบแพ็กเก็ตผิดปกติต่างๆ ในการโจมตีระบบ ซึ่งในกรณีนี้เราสามารถใช้ไฟร์วอลล์ในการป้องกันได้ โดยอนุญาตเฉพาะแพ็กเก็ตที่มีลักษณะปกติผ่านได้เท่านั้น

ถ้าในกรณีที่เครื่องเอเจนต์ต่างๆ ส่งข้อมูลปกติเป็นปริมาณมากเพื่อทำการโจมตีระบบ แพ็กเก็ตต่างๆ เหล่านี้จะสามารถทะลุไฟร์วอลล์เข้าสู่ระบบได้ ในกรณีนี้จึงจำเป็นต้องมีการออกแบบและตั้งค่าระบบให้สามารถทนทานต่อการโจมตี สามารถรองรับการร้องขอปริมาณมากได้ สามารถดำเนินการต่อการร้องขอต่างๆ ได้อย่างรวดเร็วและไม่มีการสิ้นเปลืองทรัพยากรมาก ซึ่งจำเป็นต้องมีการตั้งค่าระบบปฏิบัติการให้มีการใช้งานทรัพยากรที่ไม่เกี่ยวข้องกับบริการหลักของระบบให้น้อยที่สุด

ช่องโหว่อื่นๆ ในระบบ

เมื่อผู้บุกรุกต้องการบุกรุกระบบสามารถทำได้โดยหาช่องโหว่ภายในระบบ แล้วพยายามเข้าสู่ระบบทางช่องโหว่นั้น ๆ ช่องโหว่ของระบบมีดังนี้

1. ข้อบกพร่องของโปรแกรม

เกิดจากบักที่อยู่ในโปรแกรมซึ่งทำงานในเครื่องเซิร์ฟเวอร์, เครื่องไคลเอนต์, บนระบบปฏิบัติการ, หรือสแต็กของเน็ตเวิร์ก ช่องโหว่ของระบบซึ่งพบที่โปรแกรมจำแนกเป็นประเภทต่าง ๆ ดังนี้

- บัฟเฟอร์โอเวอร์โฟลว์ (Buffer Overflow) ช่องโหว่ที่พบในปัจจุบันเกิดจากบัฟเฟอร์โอเวอร์โฟลว์แทบทั้งสิ้น การเกิดบัฟเฟอร์โอเวอร์โฟลว์ เช่น สมมุติว่าโปรแกรมเมอร์เขียนโปรแกรมรับอินพุตเป็นชื่อผู้ใช้ และจองพื้นที่ 256 ตัวอักษรสำหรับเก็บอินพุตนี้ โปรแกรมเมอร์คาดไว้ว่าไม่มีผู้ใช้คนในที่มีชื่อยาวกว่านี้แน่ ส่วนในมุมมองของผู้บุกรุกนั้นจะพิจารณาว่าหากใส่อินพุตที่ยาวกว่า 256 ตัวอักษร แล้วตัวอักษรที่เกินมาจะถูกวางไว้ที่ส่วนใดในหน่วยความจำ ผู้บุกรุกจึงพยายามส่งตัวอักษรมากกว่า 256 ตัวอักษรติดกัน พร้อมกับแทรกโค้ดที่สามารถทำงานได้ไว้ในอินพุตนั้นด้วย ถ้าโปรแกรมเกิดแครชขึ้นผู้บุกรุกสามารถนำมาใช้เป็นจุดที่เข้าไปบุกรุกระบบได้ ซึ่งผู้บุกรุกสามารถหาช่องโหว่นี้ได้หลายทาง เช่น จากซอร์สโค้ดของเซอร์วิสต่าง ๆ ที่มีแจกให้ในอินเทอร์เน็ต ผู้บุกรุกเพียงแค่ค้นหาโปรแกรมตัวที่มีช่องโหว่นี้ จากนั้นก็ศึกษาซอร์สโค้ดแอสเซมบลีในการค้นหาช่องโหว่ และทดลองใส่ข้อมูลสุ่มเพื่อหาข้อบกพร่อง มีข้อสังเกตว่าปัญหานี้มักเกิดกับโปรแกรมที่เขียนด้วย C หรือ C++ และพบได้น้อยมากในโปรแกรมที่เขียนด้วยจาวา (JAVA) เนื่องจากจาวาไม่อนุญาตให้โปรแกรมเมอร์ไปเข้าถึงหน่วยความจำได้โดยตรง
- การใช้โปรแกรมหลายโปรแกรมทำงานร่วมกันทำให้เกิดสิ่งที่ไม่คาดคิดขึ้นในการเขียนโปรแกรม (Unexpected combinations) โปรแกรมเมอร์เขียนโดยใช้โค้ดหลาย ๆ ระดับสร้างโปรแกรมขึ้นมา โดยมีระดับระบบปฏิบัติการเป็นระดับล่างสุด ตัวอย่างช่องโหว่แบบนี้ที่สามารถเห็นได้คือโปรแกรมที่เขียนด้วยภาษาเพิร์ล ซึ่งสามารถส่งอินพุตไปยังโปรแกรมอื่นได้ เช่น " | mail < /etc/passwd " เมื่อโปรแกรมทำงานที่คำสั่งนี้ ทำให้ระบบส่งไฟล์ /etc/passwd ไปให้ผู้บุกรุกผ่านทางอีเมล์

- อินพุตที่ไม่สามารถควบคุมได้ (Unhandled input) โปรแกรมเมอร์โดยส่วนใหญ่พิจารณาถึงเฉพาะอินพุตที่ใส่อย่างถูกต้องเท่านั้น โดยไม่ได้คิดถึงการใส่อินพุตที่เป็นไปไม่ได้ด้วย นี่เป็นช่องโหว่อีกทางหนึ่งที่สามารถใช้ในการบุกรุกระบบได้
- สภาพที่มีการแข่งขัน (Race condition) ระบบปัจจุบันเป็นระบบแบบมัลติทาร์กิง (multitasking) และมัลติเธรด (multithread) คือในขณะใดขณะหนึ่งสามารถมีโปรแกรมมากกว่าหนึ่งโปรแกรมทำงานอยู่ได้ ซึ่งเป็นอันตรายต่อระบบถ้าสองโปรแกรมกำลังเข้าถึงข้อมูลเดียวกันในเวลาเดียวกัน กรณีนี้อาจทำให้ข้อมูลของโปรแกรมใดโปรแกรมหนึ่งไม่สามารถเขียนได้อย่างสมบูรณ์ เหตุการณ์นี้เกิดขึ้นน้อยมาก ผู้บุกรุกต้องใช้เวลานานสำหรับการบุกรุกด้วยช่องทางนี้

2. ข้อบกพร่องของการกำหนดค่าของระบบ

ข้อบกพร่องจากการกำหนดค่าของระบบเกิดได้จากหลายสาเหตุดังนี้

- การตั้งค่าโดยใช้ค่าเดิมที่ระบบกำหนดมาให้ (Default configure) โปรแกรมส่วนใหญ่ที่ลูกค้าซื้อมาได้กำหนดค่าการทำงานต่าง ๆ มาแล้ว และเป็นค่าที่ทำให้โปรแกรมใช้งานได้ง่าย ซึ่งการใช้งานง่ายนำไปสู่การง่ายต่อการถูกบุกรุกระบบด้วย
- เกิดจากผู้ดูแลระบบเกียจคร้าน ไม่ได้ใส่รหัสผ่านของรูต (root) หรือผู้ใช้ใดๆ ในระบบ ทำให้เป็นช่องโหว่ที่ผู้บุกรุกใช้บุกรุกเข้าระบบโดยง่าย
- โปรแกรมอาจมีช่องโหว่จากเซอร์วิสที่ทำงานอยู่ในระบบ ผู้ดูแลระบบควรปิดเซอร์วิสของระบบทุกตัวที่ไม่ได้ใช้งาน เพื่อหลีกเลี่ยงช่องโหว่ที่อาจเกิดขึ้นได้ในภายหลัง ในส่วนนี้มีโปรแกรมสำหรับตรวจสอบความปลอดภัย ซึ่งสามารถตรวจสอบและแจ้งเตือนผู้ดูแลระบบให้ไปแก้ไขได้
- เครื่องที่เชื่อถือกัน (Trust relationships) ผู้บุกรุกอาศัยช่องโหว่จากเครื่องที่ติดต่อกันแบบทรัสต์ โดยสามารถเข้าไปยังเครื่องอื่น ๆ ที่ยกเว้นการตรวจสอบสิทธิ์ของกันและกันได้ ตัวอย่างการบุกรุกทางช่องโหว่ตรงนี้คือ การบุกรุกโดยใช้ .rhost

3. ช่องโหว่ของรหัสผ่าน

ส่วนใหญ่เกิดจากผู้ใช้ส่วนใหญ่จะใช้ชื่อที่ผู้ใช้คุ้นเคย เช่นชื่อตัวเอง ชื่อเพื่อน หรือสัตว์เลี้ยง เป็นรหัสผ่าน ทำให้ผู้บุกรุกสามารถเดารหัสผ่านได้ง่าย

การบุกรุกจากเดารหัสผ่านจากคำในพจนานุกรม มักเป็นขั้นตอนที่ผู้บุกรุกทำหลังจากไม่สามารถเดารหัสผ่านได้ โดยลองใช้รหัสผ่านซึ่งได้จากการเข้ารหัสคำที่อยู่ในพจนานุกรม แล้วนำมาเปรียบเทียบกับรหัสผ่านที่เข้ารหัสในไฟล์ของระบบ ซึ่งผู้บุกรุกอาจใช้คำที่อยู่ในฐานข้อมูลพจนานุกรมคำศัพท์ภาษาอังกฤษหรือภาษาต่างประเทศอื่น ๆ ก็ได้

การบุกรุกโดย Brute Force Attack เป็นอีกวิธีหนึ่งที่ผู้บุกรุกใช้ในการเดารหัสผ่าน ผู้บุกรุกเดารหัสที่เป็นไปได้ที่เกิดขึ้นจากการสร้างรหัสผ่าน เช่นสมมุติว่ารหัสผ่านที่เป็นไปได้ของระบบเป็นตัวอักษรภาษาอังกฤษพิมพ์เล็กจำนวน 4 ตัว ผู้บุกรุกก็พยายามล็อกอินเข้าสู่ระบบโดยใช้รหัสผ่านที่เป็นไปได้ทั้งหมดจากการผสมคำ ในกรณีนี้ รหัสผ่านที่เป็นไปได้คือ 26x26x26x26 ตัว ซึ่งถ้าตั้งรหัสผ่านมีการผสมกันระหว่างตัวอักษรทั้งตัวเล็ก ตัวใหญ่ ตัวเลขและเครื่องหมายต่างๆ จะทำให้คำที่เป็นไปได้ทั้งหมดมีจำนวนมากขึ้น ดังนั้นหากผู้บุกรุกใช้วิธีนี้ในการเดารหัสผ่านก็จะใช้เวลานานยิ่งขึ้น

นอกจากนี้ผู้บุกรุกสามารถได้รหัสผ่านโดยวิธีต่อไปนี้

- การดักจับข้อมูลที่ไม่ได้เข้ารหัส (clear text sniffing) เซอร์วิสที่รันบนโพรโตคอล TCP/IP เช่น telnet มีการส่งรหัสผ่านที่ไม่เข้ารหัส ซึ่งอาจมีการดักจับโดยใช้ตัววิเคราะห์โพรโตคอล (protocol analyzer) ระหว่างทางของการส่งแพ็กเก็ตผ่านไปในเน็ตเวิร์ก ผู้บุกรุกสามารถเอารหัสผ่านที่ได้ไปล็อกอินเข้าระบบในภายหลัง
- การดักจับข้อมูลเข้ารหัส (Encrypt sniffing) ถึงแม้ว่ารหัสผ่านถูกเข้ารหัสไว้ ผู้บุกรุกสามารถทราบรหัสผ่านเหล่านั้นได้โดยนำรหัสผ่านจากคำในพจนานุกรม หรือจากการเดาคำไปเข้ารหัสเพื่อมาเปรียบเทียบกับรหัสผ่านที่ถูกเข้ารหัสไว้ (Brute force) หากผู้บุกรุกสามารถทราบรหัสผ่านเข้าสู่ระบบแล้ว ผู้นั้นก็เหมือนกับผู้ใช้ทั่วๆ ไป โดยที่ไม่อาจทราบได้เลยว่า ผู้ที่ล็อกอินเข้ามานั้นเป็นผู้ที่มีสิทธิ์คนนั้นจริงๆ หรือไม่

- การบุกรุกโดยการส่งข้อมูลซ้ำ (Replay attack) ผู้บุกรุกไม่จำเป็นต้องถอดรหัสรหัสผ่าน เพียงแต่ดักจับแพ็กเก็ตนั้น และสร้างโปรแกรมที่สามารถส่งแพ็กเก็ตของรหัสผ่านที่เข้ารหัส ของผู้ที่มีสิทธิ์ในการใช้งานที่ดักจับได้ไว้ก่อนหน้านั้น แล้วส่งแพ็กเก็ตนั้นอีกครั้งไปยังเซิร์ฟเวอร์ขณะที่กำลังตรวจสอบสิทธิ์ ทำให้การติดต่อนั้นสำเร็จด้วยโดยใช้สิทธิ์ของผู้ใช้คนอื่น
- การขโมยไฟล์รหัสผ่าน (Password file stealing) ในระบบของเครื่องเซิร์ฟเวอร์ทั่วๆ ไปจะเก็บฐานข้อมูลรหัสผ่านของผู้ใช้ให้อยู่ในไฟล์ ซึ่งในระบบปฏิบัติการลีนุกซ์อยู่ที่ไฟล์ /etc/password หรือสำหรับระบบปฏิบัติการ WindowsNT เก็บอยู่ในไฟล์ที่ชื่อว่า SAM เมื่อผู้บุกรุกกระทำการใด ๆ ก็ตามทำให้ได้ไฟล์รหัสผ่านเหล่านี้แล้ว ผู้บุกรุกสามารถนำไฟล์นี้ไปถอดรหัสโดยให้โปรแกรมถอดรหัส (Crack) หารหัสผ่านที่ใช้เข้าสู่ระบบ
- การเฝ้าสังเกต (Observation) ปัญหาพื้นฐานของระบบการรักษาความปลอดภัย คือการขโมยใช้รหัสผ่าน หากผู้ใช้ในระบบมีการกำหนดรหัสผ่านของตนให้เป็นรหัสผ่านที่ยากต่อการเดา ปัญหาที่จะเกิดกับผู้ใช้ผู้นั้นคือ ผู้ใช้ต้องจำรหัสผ่านที่ตัวเองตั้งขึ้นมาด้วย ผู้ใช้บางคนอาจเผอเรอเขียนรหัสผ่านไว้บนกระดาษแล้วทิ้งไว้ ทำให้ผู้บุกรุกได้เอกสารที่มีรหัสผ่านนั้นไปได้ อีกวิธีหนึ่งคือถามรหัสผ่านผู้ที่รู้โดยใช้วิธีหลอกถามรหัสผ่านจากผู้ที่มีสิทธิ์จริง ๆ โดยอ้างเหตุผลต่าง ๆ

นอกจากปัญหาด้านการรักษาความปลอดภัยในเครือข่ายแล้ว ยังมีปัญหาด้านความปลอดภัยอื่นๆ ที่จะเกิดขึ้นในระบบ ยกตัวอย่างเช่น

1. จะมั่นใจได้อย่างไรว่าการส่งข้อมูลในการใช้บริการต่างๆ ในอินเตอร์เน็ตเช่น เว็บ , E-mail , Instant Messaging จะเป็นความลับไม่มีใครดักจับได้
2. จะมั่นใจได้อย่างไรว่าการส่งข้อมูลในการใช้บริการต่างๆ ในอินเตอร์เน็ตเช่น เว็บ , E-mail , Instant Messaging จะไม่ถูกเปลี่ยนแปลงข้อมูล
3. จะมั่นใจได้อย่างไรว่าหน้าเว็บเพจที่เปิดขึ้นมานั้น เป็นของเว็บไซต์นั้นจริงๆ หรือบุคคลที่คุยด้วยในอินเตอร์เน็ตจะเป็นบุคคลนั้นๆ จริงๆ
4. ในบริษัทขนาดใหญ่ การ replicate ข้อมูลในฐานข้อมูลระหว่างบริษัทสาขา จะมั่นใจได้อย่างไรว่าจะไม่มีใครในอินเตอร์เน็ตดักจับได้

ทำความรู้จัก CIA

จากการทำงานของโพรโตคอลต่างๆที่ออกแบบมาเพื่อใช้งานในการเชื่อมต่ออุปกรณ์ต่างๆ และระบบต่างเข้าด้วยกันเท่านั้นจึงทำให้เกิดปัญหาความปลอดภัย ทั้งนี้เนื่องจากการออกแบบโพรโตคอลต่างๆ ไม่ได้คำนึงถึงปัจจัยในการสร้างความปลอดภัยในการใช้งานได้แก่ Confidentiality, Integrity และ Availability (ซึ่งต่อไปจะเรียกรวมกันโดยใช้ตัวย่อ CIA) ในหัวข้อนี้จะทำการศึกษาหลักการทำงานของ CIA วิธีการสร้าง CIA ให้เกิดขึ้นเพื่อใช้โพรโตคอลและการทำงานต่างๆได้อย่างปลอดภัยมากขึ้น โดย CIA ความหมายและการทำงานดังนี้

Confidentiality

คือการทำให้มั่นใจได้ว่าข้อมูลส่วนตัว หรือข้อมูลที่ควรจะเป็นความลับจะไม่ถูกเปิดเผยและจะคงสถานะการเป็นความลับตลอดการทำงาน ในการสร้าง Confidentiality ในระบบคอมพิวเตอร์และเครือข่ายจำเป็นต้องอาศัยกระบวนการ มาตรการและทฤษฎีต่างๆ โดยเฉพาะอย่างยิ่งทฤษฎีเกี่ยวกับการเข้ารหัสลับ (encryption)

Integrity

คือการทำให้ข้อมูลที่ส่งจากต้นทางไปยังปลายทางไม่ถูกเปลี่ยนแปลงระหว่างทาง โดยข้อมูลที่ผู้รับได้รับจะต้องเหมือนกับข้อมูลที่ส่งจากผู้ส่ง ไม่มีความแตกต่างและไม่ถูกแก้ไขโดยไม่ได้รับอนุญาต สำหรับการสร้าง Integrity ในระบบจำเป็นต้องอาศัยกระบวนการสร้าง Digital Signature ของข้อมูลหรือ Identity ใดๆ เพื่อตรวจสอบการเปลี่ยนแปลงของ ข้อมูล หรือ Identity นั้นๆ ซึ่งสามารถประยุกต์เข้ากับทฤษฎีการเข้ารหัสลับเพื่อต่อยอดการทำงานได้

Availability

เป็นกระบวนการต่างๆ เพื่อสร้างให้ระบบมีเสถียรภาพและสามารถตอบสนองต่อการร้องขอบริการจากผู้ใช้งานได้ ซึ่งจำเป็นต้องพึ่งพากระบวนการต่างๆ เพื่อให้ผู้ใช้งานสามารถระบบทำงานได้อย่างต่อเนื่อง โดยต้องมีการเตรียมการสำหรับเหตุการณ์ผิดปกติต่างๆ ที่อาจทำให้ระบบล่ม และการเตรียมการสำหรับตอบสนองอย่างทันท่วงทีได้แก่

1. Access Control เพื่อควบคุมไม่ให้การโจมตีใดๆ เข้าสู่ระบบ
2. การ Monitor และการตรวจตราระบบ
3. การออกแบบระบบคอมพิวเตอร์และเครือข่ายให้มีความทนทานสูง
4. การวางแผนการบริหารความเสี่ยงและการประเมินความเสี่ยง
5. การกำหนดนโยบายการรักษาความปลอดภัยตามมาตรฐานสากล
6. การพัฒนาบุคลากรให้มีความสามารถ

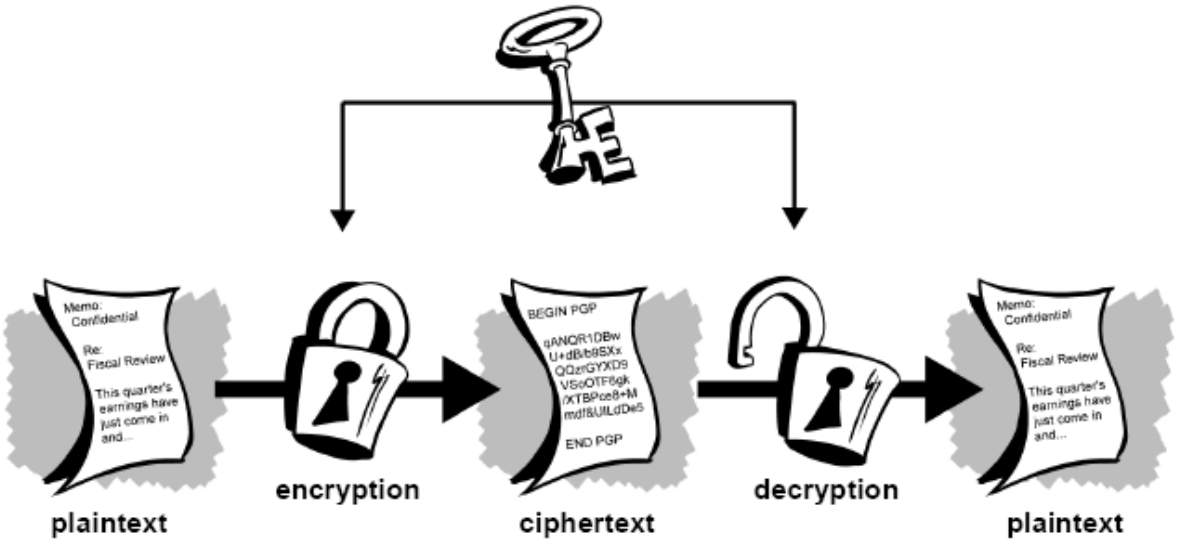
บทที่ 3. Confidentiality

ในกระบวนการสร้าง Confidentiality ในระบบคอมพิวเตอร์ จะใช้การเข้ารหัสลับเป็นกระบวนการหลัก การเข้ารหัสลับหรือ Encryption เป็นกระบวนการที่ต้องการให้ข้อมูลข่าวสารที่รับส่งนั้นเป็นความลับในขณะที่ยังไม่ถึงมือผู้รับ โดยการเข้ารหัสลับในโลกของคอมพิวเตอร์จะเป็นการเปลี่ยนรูปแบบข้อมูลออกไปเป็นข้อมูลที่ไม่สามารถแปลความหมายตามต้นฉบับได้ ซึ่งกระบวนการที่ใช้ในการเข้ารหัสลับนั้น จะมีวิธีการที่แตกต่างกันออกไปตามวัตถุประสงค์ มีความซับซ้อนในการเข้ารหัสลับต่างกัน ทำให้ระดับของการรักษาความปลอดภัยต่างกันด้วย

ในการเข้ารหัสลับเราจะเรียกข้อมูลต้นฉบับที่สามารถอ่านได้ว่า plain text หรือ clear text และจะเรียกกระบวนการที่ทำให้ข้อมูล Plaintext กลายเป็นข้อมูลที่ไม่อยู่ในรูปแบบที่สามารถอ่านได้ว่า Encryption ซึ่งข้อมูลที่ไม่อยู่ในรูปแบบที่สามารถอ่านได้นี้จะเรียกว่า ciphertext โดยในการส่งข้อมูลจะทำการส่งข้อมูล ciphertext ไปยังผู้รับแล้วจึงเข้าสู่กระบวนการ Decryption เพื่อถอดความ ciphertext สำหรับการเข้ารหัสลับจะใช้ศาสตร์ในการเข้ารหัสหรือเรียกว่า cryptography โดยทฤษฎีการเข้ารหัสลับจะแบ่งออกเป็น 2 กลุ่ม คือการเข้ารหัสลับแบบใช้คีย์ในการเข้ารหัสลับและถอดรหัสลับเหมือนกัน (Symmetric Cryptography) และการเข้ารหัสลับแบบที่ใช้คีย์ในการเข้ารหัสลับและถอดรหัสลับต่างกัน(Asymmetric Cryptography)

Symmetric Cryptography

Symmetric Cryptography เป็นกระบวนการเข้ารหัสลับและถอดรหัสลับที่มีการใช้คีย์ในการเข้ารหัสลับและถอดรหัสลับคือข้อมูลชุดเดียวกัน ตัวอย่างอัลกอริทึมในกลุ่มของ Symmetric Cryptography คือ DES (Data Encryption Standard)



รูปที่ 19 รูปการเข้ารหัสลับแบบ Symmetric Key

Data Encryption Standard (DES)

Data Encryption Standard (DES) เป็นอัลกอริทึมที่ใช้ในการเข้ารหัสที่มีการใช้งานอย่างแพร่หลาย คิดค้นขึ้นในปี 1976 โดยใช้คีย์ในการเข้ารหัสและถอดรหัสคือคีย์เดียวกัน (Symmetric Cryptography) เนื่องจาก DES มีการใช้งานคีย์ที่มีขนาด 56 บิต การถอดรหัสโดยไม่ทราบคีย์จึงต้องมีการสุ่มคีย์ทั้งหมด 72,000 ล้านล้านคีย์ ซึ่งถือว่าอัลกอริทึมดังกล่าวมีความปลอดภัยสูง ในกระบวนการเข้ารหัส DES จะทำการแบ่งข้อมูลออกเป็นบล๊อค บล๊อคละ 64 บิต แล้วทำการเข้ารหัสแต่ละบล๊อคโดยใช้คีย์ 56 บิต กระบวนการดังกล่าวจะทำการเข้ารหัสทั้งหมด 16 รอบตามกระบวนการของ DES ถึงแม้ว่า DES จะถือว่ามีความปลอดภัยสูง แต่ก็ยังมีการปรับปรุง DES ให้มีความปลอดภัยสูงขึ้นโดยการปรับเปลี่ยนเป็น "Triple DES" ซึ่งสามารถใช้คีย์ทั้งหมด 3 ชุด

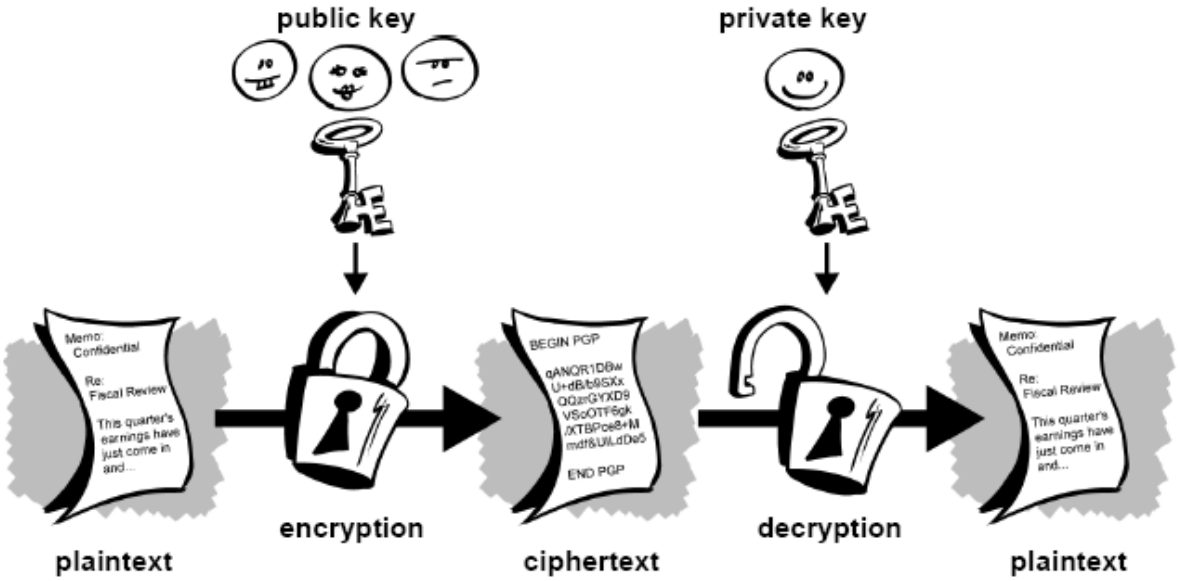
ถึงแม้ว่า DES จะมีความปลอดภัยสูงแต่ก็ยังสามารถถอดรหัสได้ โดยในปี 1997 มีนักคณิตศาสตร์ Rivest - Sharmir - Adleman (ซึ่งภายหลังทั้งสามคนคิดค้นอัลกอริทึม RSA) โดยทำการถอดรหัสข้อมูลโดยได้รับความร่วมมือจากผู้ใช้คอมพิวเตอร์ประมาณ 14,000 เครื่องในอินเตอร์เน็ต ร่วมกันถอดรหัสข้อมูลเพื่อหาคีย์ในการถอดรหัส ซึ่งภายหลังสามารถถอดรหัสได้โดยการสุ่มตรวจคีย์ทั้งสิ้น 18,000 ล้านล้านคีย์ จนได้รับรางวัล 10,000 เหรียญสหรัฐ

ภายหลังมีการคิดค้นการถอดรหัส DES ด้วยวิธีการต่างๆ ได้แก่ ในปี 1998 มีการถอดรหัส DES โดยใช้เวลา 56 ชั่วโมงโดยใช้อุปกรณ์ EEF DES Cracker ในปี 1999 มีการคิดค้นกระบวนการในการถอดรหัส DES ได้ในเวลา 22 ชั่วโมง 15 นาที และล่าสุดในวันที่ 15 มีนาคม 2007 มีการออกแบบอุปกรณ์โดยเชื่อมต่อ FPGA แบบขนานขึ้นชื่อ COPACOBANA โดย University of Bochum and Kiel , Germany ซึ่งราคารวมประมาณ 10,000 เหรียญสหรัฐและทำการถอดรหัส DES โดยใช้เวลา 6.4 วัน

หลังจากที่มีการถอดรหัสข้อมูล DES ได้มากขึ้นจึงมีการคิดค้นกระบวนการในการเข้ารหัสใหม่ คือ Advanced Encryption Standard (AES) ซึ่งอัลกอริทึมนี้ได้พัฒนาโดย Joan Daemen และ Vincent Rijmen ในปี 2000 อัลกอริทึมนี้เป็นที่ยอมรับโดยหน่วยงานมาตรฐานและเทคโนโลยีของสหรัฐ หรือ National Institute of Standard and Technology (NIST) ให้เป็นมาตรฐานในการเข้ารหัสชั้นสูงของประเทศ อัลกอริทึมมีความเร็วสูงและมีขนาดกะทัดรัดโดยสามารถใช้กุญแจที่มีความยาวขนาด 128, 192 และ 256 บิตเพื่อเพิ่มความปลอดภัยให้สูงขึ้น นอกจากนี้ยังมีอัลกอริทึมอื่นๆ ที่ได้รับการสนับสนุนให้นำไปใช้ให้แพร่หลายอีกเช่น RC6, Serpent, MARS และ Twofish

Asymmetric Cryptography

Asymmetric Cryptography คือกระบวนการเข้ารหัสลับที่มีการใช้คีย์ในการเข้ารหัสกับคีย์ในการถอดรหัสต่างกัน ในการใช้งาน หากใช้คีย์ใดในการเข้ารหัสลับจะใช้คีย์อีกคีย์หนึ่งในการถอดรหัส สำหรับคีย์ที่ใช้ทั้งสองคีย์จะมีชื่อเรียกว่า Private Key และ Public Key โดย Private Key จะเป็นคีย์ประจำตัวของผู้ใช้งานจะถูกเก็บรักษาไว้เป็นความลับ ส่วน Public Key จะเป็นคีย์ในการเข้ารหัสข้อมูลเพื่อส่งให้กับเจ้าของคีย์ สามารถแจกจ่ายให้กับบุคคลทั่วไปได้ Asymmetric Cryptography จึงมีการใช้งานในอีกชื่อหนึ่งคือ Public Key Cryptography



รูปที่ 20 รูปแบบการเข้ารหัสแบบ Asymmetric Key

ในการใช้งาน ผู้ใช้งานจะสามารถดำเนินการได้ใน 2 รูปแบบคือ

1. การ Sign ข้อมูลที่จะส่งด้วย Private Key ของผู้ส่ง ทำให้ผู้รับสามารถมั่นใจได้ว่าข้อมูลที่ได้รับจะเป็นข้อมูลที่ถูกต้องโดยการตรวจสอบความถูกต้องโดยใช้ Public Key ของผู้ส่ง
2. ทำการเข้ารหัสลับข้อมูลที่จะส่งโดยใช้ Public Key ของผู้รับ ทำให้ผู้ที่สามารถถอดรหัสข้อมูลและใช้งานข้อมูลนั้นๆ ได้คือผู้รับเท่านั้น โดยผู้รับจะทำการถอดรหัสและนำข้อมูลไปใช้งานโดยใช้ Private Key ของตนเอง

ในการใช้งานในระบบจริง การใช้งาน Asymmetric Cryptography นั้นประสบความสำเร็จได้เนื่องจากมีระบบการบริหารจัดการคีย์ (Key Management System) ซึ่งเป็นระบบเกี่ยวกับการสร้าง การเก็บและการแจกจ่าย Public Key ของผู้ใช้งานระบบได้โดยง่ายและน่าเชื่อถือ โดยระบบบริหารจัดการคีย์ที่ใช้กันอย่างแพร่หลายในปัจจุบันคือ Public Key Infrastructure หรือ PKI ซึ่งจะกล่าวถึงต่อไป ตัวอย่างของอัลกอริทึมในการเข้ารหัสแบบ Asymmetric Cryptography คือ RSA

RSA

RSA เป็นอัลกอริทึมในการเข้ารหัสข้อมูลโดยการใช้คีย์ในการเข้ารหัสกับถอดรหัสคนละคีย์กัน ซึ่งจากการทำงานดังกล่าวทำให้อัลกอริทึมนี้มีการใช้งานอย่างแพร่หลายโดยเฉพาะในการสร้าง Digital Signature ของข้อมูลต่างๆ RSA ถูกคิดค้นขึ้นโดย Ron Rives, Adi Shamir และ Len Adleman สำหรับชื่อ RSA นั้นมาจากการนำเอาตัวอักษรตัวแรกของผู้คิดค้นมาเรียงต่อกันตามลำดับ สำหรับแนวคิดของ RSA คือการคิดว่าการแยกตัวประกอบของตัวเลขจำนวนเฉพาะ 2 จำนวนใดๆ เป็นสิ่งที่สามารถทำได้ยาก

การบริหารจัดการคีย์

Public Key Infrastructure: PKI

ระบบโครงสร้างพื้นฐานกุญแจสาธารณะ (Public Key Infrastructure) PKI คือ ระบบป้องกันข้อมูลที่รับส่งกันผ่านเครือข่ายอินเตอร์เนต ในการทำงานของ PKI ทำได้โดยการใช้หลักการของ Asymmetric Encryption โดยการสร้าง Public Key และ Private Key ในการเข้ารหัสและถอดรหัสข้อมูล โดยกุญแจทั้งสองนี้จะได้มาพร้อมกับใบรับรองที่ Certificate Authority (CA) เป็นผู้ออกให้ โดย Private Key จะถูกเก็บไว้ที่เจ้าของใบรับรองเท่านั้น ส่วน Public Key จะถูกแจกจ่ายโดย CA เพื่อนำไปใช้ในการติดต่อกับเจ้าของใบรับรอง ทำให้การรับส่งข้อมูลใดๆ มีความน่าเชื่อถือมากขึ้น

Certificate Authority

ในชีวิตจริง เราจะเห็นได้ว่าความน่าเชื่อถือในตัวบุคคลต่างๆ มีต่ำมาก หลายๆ หน่วยงานจะเชื่อถือในหน่วยงานของรัฐหรือหน่วยงานต้นสังกัดของคนๆ นั้นเป็นหลัก ทำให้ในการทำธุรกรรมต่างๆ ไม่ว่าจะเป็นสมัครงาน สมัครเพื่อเรียนต่อ ซื้อทรัพย์สิน กู้เงิน เปิดบัญชีธนาคาร ฯลฯ จำเป็นต้องใช้บัตรประชาชนซึ่งออกให้โดยกรมการปกครอง กระทรวงมหาดไทย หรือบัตรอื่นๆ ที่ออกโดยหน่วยงานนั้นๆ จึงจะสามารถทำธุรกรรมหากหน่วยงานต่างๆ เชื่อถือในตัวประชาชนคนนั้นๆ จริงๆ จะต้องสามารถดำเนินการธุรกรรมต่างๆ ได้โดยไม่จำเป็นต้องใช้บัตรประชาชนเลย

นั่นหมายความว่าการทำธุรกรรมต่างๆ จะมีความเชื่อถือกรมการปกครอง กระทรวงมหาดไทย มากกว่าตัวบุคคลนั้นๆ ซึ่งเมื่อมองในความเป็นจริงก็เป็นสิ่งที่ปฏิเสธไม่ได้ เนื่องจากรูปลักษณ์ภายนอกของแต่ละคนสามารถปลอมแปลงกันได้ไม่ยาก

ในการทำธุรกรรมอิเลกทรอนิกส์ให้มีความปลอดภัยสูง การไว้ใจให้ผู้ใช้บริการสามารถทำธุรกรรมได้ด้วยตนเอง โดยการสร้างคู่กุญแจในการเข้ารหัสและถอดรหัสด้วยตนเองนั้น เป็นสิ่งที่มีความเสี่ยงสูงมาก ปัจจุบันจึงมีการตั้งหน่วยงานกลางในการสร้าง การรับรองและการแจกจ่ายคู่กุญแจเหล่านั้นแทนที่จะให้ผู้ใช้งานสร้างขึ้นเอง ด้วยเหตุผลหลักเพียงข้อเดียวคือไม่เชื่อถือในผู้ใช้งานแต่เชื่อถือในผู้ประกอบการรับรอง (Certificate Authority: CA) เท่านั้น

ผู้ประกอบการรับรอง (Certification Authority) หรือผู้ให้บริการรับรอง (Certification Service Provider) ซึ่งจะทำหน้าที่เป็นตัวกลางในการให้บริการโครงสร้างพื้นฐานกุญแจสาธารณะ (PKI) เพื่อตอบสนองความต้องการพื้นฐานด้านความปลอดภัยของการทำธุรกรรมอิเล็กทรอนิกส์ CA คือผู้ประกอบกิจการรับรองการใช้ Key pairs ในรูปแบบของใบรับรอง อีกนัยก็คือผู้ที่รับรองความปลอดภัยของข้อมูลอิเลกทรอนิก และยืนยันความมีตัวตนของเจ้าของใบรับรองในการทำธุรกรรมได้ โดยหน้าที่ของผู้ออกใบรับรองฯ มีดังนี้

- สร้างคู่กุญแจ (Key pairs) ของผู้ใช้บริการ
- ออกใบรับรองฯ เพื่อยืนยันตัวผู้ใช้บริการ
- จัดเก็บและเผยแพร่กุญแจสาธารณะ
- หากมีการร้องขอให้ยืนยันตัวบุคคลเจ้าของกุญแจ จะดำเนินการยืนยันหรือปฏิเสธความเป็นเจ้าของกุญแจสาธารณะตามคำขอของบุคคลทั่วไป
- เปิดเผยรายชื่อใบรับรองฯ ที่ถูกยกเลิกแล้ว (Certificate Revocation List หรือ CRL) เพื่อเป็นการบอกแก่สาธารณชนว่าใบรับรองฯ นั้น ไม่สามารถนำมาใช้ได้อีกต่อไป

Digital Certificate

เพื่อให้ระบบมีความปลอดภัยและความน่าเชื่อถือมากขึ้น การดำเนินการต่างๆ จะมีการใช้ใบรับรองดิจิตอล (Digital Certificate) ซึ่งออกโดย CA เพื่อยืนยันในการทำธุรกรรมเพื่อรับรองว่าบุคคลที่ทำธุรกรรมนั้นเป็นบุคคลนั้นจริงตามที่ได้อ้างไว้ สำหรับรายละเอียดในใบรับรองดิจิตอลทั่วไปมีดังต่อไปนี้

- ข้อมูลของผู้ที่ได้รับการรับรอง
- ข้อมูลระบุผู้ออกใบรับรอง ได้แก่ ลายมือชื่อดิจิตอลขององค์กรที่ออกใบรับรอง หมายเลขประจำตัวของผู้ออกใบรับรอง
- กุญแจสาธารณะของผู้ที่ได้รับการรับรอง
- วันหมดอายุของใบรับรอง
- ระดับชั้นของใบรับรองดิจิตอล
- หมายเลขประจำตัวของใบรับรองดิจิตอล
- ประเภทของใบรับรองดิจิตอลซึ่งแบ่งออกเป็น 3 ประเภท คือ ใบรับรองเครื่องแม่ข่าย ใบรับรองตัวบุคคล ใบรับรองสำหรับองค์รับรองความถูกต้อง

ในส่วนของการทำ Encryption จึงแยกกระบวนการออกเป็น 2 กระบวนการหลักคือการเข้ารหัสลับ (Encryption) และการบริหารจัดการคีย์ (Key Management) ซึ่งกระบวนการทั้งสองมีส่วนเกี่ยวข้องกันคือ ระบบการเข้ารหัสจำเป็นต้องใช้คีย์ แต่ในการแจกจ่ายคีย์นั้นจำเป็นต้องมีกระบวนการในการแจกจ่าย รวมถึงการใช้งานคีย์ใดๆ ควรมีผู้รับรองว่าคีย์นั้นเป็นของบุคคลที่ต้องการติดต่อด้วยจริงๆ ไม่ใช่ แฮกเกอร์

ตัวอย่างการใช้งาน Encryption เพื่อป้องกันการโจมตีแบบต่างๆ

1. การใช้งาน IP Security ในเครือข่ายไอพี โดย IP Security จะเพิ่มความปลอดภัยในด้านการเข้ารหัสลับข้อมูล ก่อนการส่ง ซึ่งเป็นส่วนการทำงานเพิ่มเติมจาก IP Protocol
2. การใช้งาน SSL เพื่อเพิ่มความปลอดภัยในการใช้งานโพรโตคอล HTTP
3. การใช้โปรแกรมเพื่อเข้ารหัสไฟล์ข้อมูลต่างๆ ในเครื่องเพื่อป้องกันการนำข้อมูลนั้นๆ ไปใช้งาน โดยเจ้าของไฟล์ข้อมูลจะเป็นเพียงคนเดียวที่ทราบรหัสผ่านที่ใช้ในการถอดรหัสไฟล์ ก่อนนำไปใช้งาน
4. การใช้งาน WEP ในเครือข่ายไร้สาย เพื่อเข้ารหัสข้อมูลที่รับส่งในเครือข่ายไร้สาย (IEEE 802.11)
5. การใช้งาน Secure Shell แทนการเชื่อมต่อ Remote Terminal แทน Telnet เพื่อเข้ารหัสข้อมูลก่อนทำการส่ง

บทที่ 4. Message Integrity Control

สิ่งที่สำคัญที่สุดในระบบเทคโนโลยีสารสนเทศคือ “ข้อมูล” โดยองค์ประกอบทั้งหมดในระบบเทคโนโลยีสารสนเทศล้วนแล้วแต่เป็นองค์ประกอบที่ช่วยในการสร้าง ประมวลและนำส่งข้อมูลจากแหล่งข้อมูลไปยังผู้ใช้งาน ในการร้องขอข้อมูลข้อมูลต่างๆ ในระบบสารสนเทศไม่ว่าจะเป็นไฟล์ที่อยู่ในอินเตอร์เน็ต ข้อมูลในฐานข้อมูล และข้อมูลในรูปแบบอื่นๆ ผู้ร้องขอจะได้รับข้อมูลที่ต้องการในช่องทาง และในรูปแบบที่ผู้ใช้งานร้องขอ

ปัญหาหนึ่งที่เกิดขึ้นในการเรียกใช้งานข้อมูลคือ ข้อมูลที่ผู้ใช้งานร้องขอนั้นถูกเปลี่ยนแปลงระหว่างการจัดส่ง ซึ่งอาจเกิดจากปัญหาของช่องทางการรับส่งข้อมูล หรือถูกผู้ไม่หวังดีเปลี่ยนแปลงข้อมูลดังกล่าวระหว่างทาง หรือแม้กระทั้ง ข้อมูลที่ผู้ใช้งานต้องการนั้น ไม่ใช่ข้อมูลที่ถูกต้อง อาจเนื่องมาจากไม่ได้ Download จากแหล่งข้อมูลที่เชื่อถือได้ เช่นในกรณีที่ผู้ใช้งานต้องการ Download ข้อมูลจากอินเตอร์เน็ต ซึ่งไม่ใช่เว็บไซต์ของผู้ให้บริการข้อมูลนั้นๆ โดยตรง ซึ่งผู้ใช้งานจะไม่สามารถทราบได้เลยว่าไฟล์ข้อมูลนั้นคือไฟล์ข้อมูลที่ต้องการจริงหรือไม่ ไฟล์ดังกล่าวถูกปลอมแปลงบางส่วนไปอย่างไรบ้าง การนำข้อมูลที่มีปัญหาเหล่านั้นไปใช้งาน อาจทำให้เกิดความเสียหายขึ้นในอนาคต

ในการตรวจสอบความถูกต้องของข้อมูลนั้นสามารถทำได้หลากหลายรูปแบบ เช่น CheckSum , Hash Function , Message Authentication Code , Digital Signature เป็นต้น ซึ่งกระบวนการในการตรวจสอบข้อมูลในรูปแบบต่างๆ นี้มีข้อดีข้อเสียแตกต่างกันไปตามการออกแบบและวัตถุประสงค์ของการตรวจสอบข้อมูลนั้นๆ

Check sum

กระบวนการที่ง่ายที่สุดในการตรวจสอบความถูกต้องของข้อมูลคือการใช้ Checksum ซึ่ง Checksum คือการใช้ข้อมูลเพิ่มเติมแนบส่งไปกับข้อมูลหลัก ซึ่งข้อมูลเพิ่มเติมนี้จะมีความสัมพันธ์กับการจัดวางข้อมูลต่างๆ ที่ฝั่งผู้ส่งจะทำการคำนวณค่า Check sum แล้วแนบไปกับข้อมูลในการส่งครั้งเดียวหรือแยกส่งได้ เมื่อข้อมูลไปถึงมือผู้รับแล้วจะทำการตรวจสอบความถูกต้องของข้อมูลได้โดยการใช้ฟังก์ชั่นในการตรวจสอบ ในโพรโตคอล

ต่างๆ เช่น TCP , UDP , IP , ICMP ต่างก็มีฟิลด์ Checksum อยู่ทั้งสิ้น หรือการใช้ Checksum กับไฟล์ที่จะเผยแพร่ เพื่อยืนยันความเป็นต้นฉบับ การใช้ Checksum ในกระบวนการบีบอัดและขยายไฟล์ต่างๆ ก็ใช้สำหรับการตรวจสอบความถูกต้องของข้อมูลเช่นกัน

Hash function

ถึงแม้ว่า checksum จะสามารถตรวจสอบความผิดเพี้ยนในข้อมูลได้ แต่ก็ยังไม่สามารถตรวจสอบได้ทั้งหมด เนื่องจาก checksum นั้นเป็นกระบวนการคำนวณทางคณิตศาสตร์ซึ่งอาจเกิดการซ้ำซ้อนกันได้ จึงมีการคิดค้นกระบวนการที่สร้างตัวแทนของข้อมูลที่ผลลัพธ์ไม่ซ้ำซ้อนกัน และมีขนาดคงที่ คือ Hash Function

ในกระบวนการเข้ารหัส หรือการสร้าง Digital Signature ของข้อมูลต่างๆ จะมีการใช้งานฟังก์ชั่นแฮช (Hash Function) ร่วมด้วยเนื่องจากข้อมูลที่จะทำการเติม Digital Signature นั้นจะมีความยาวแตกต่างกัน บางข้อมูลที่มีความยาวสูงมากๆ จะใช้เวลาในการสร้าง Digital Signature นาน นอกจากนี้ข้อมูลที่มีความซ้ำซ้อนสูงและซับซ้อนต่ำเมื่อทำการเข้ารหัสจะส่งผลให้การถอดรหัสทำได้ง่าย ดังนั้น เพื่อเพิ่มความซับซ้อนของข้อมูลและลดขนาดข้อมูลให้มีขนาดเล็กลง จึงจำเป็นต้องใช้ฟังก์ชั่นแฮชร่วมด้วย

คุณสมบัติของฟังก์ชั่นแฮชที่ดีควรมีดังต่อไปนี้

1. ผลลัพธ์ของฟังก์ชั่นแฮชควรมีผลลัพธ์เฉพาะตัวกับข้อมูลที่ทำการแฮชนั้นๆ ข้อมูลแต่ละตัวเมื่อผ่านฟังก์ชั่นแฮชแล้วไม่ควรมีผลลัพธ์ที่เหมือนกัน
2. สามารถทำงานได้อย่างรวดเร็ว
3. มีการกระจายตัวสูง การนำข้อมูลใดๆ มาแฮชควรได้รับผลลัพธ์ที่อยู่ในช่วงที่กำหนดไว้แต่ละตำแหน่งมีความเป็นไปได้ในการเกิดเท่าๆ กัน
4. รหัสแฮช (Hash Code) ที่ได้ไม่ควรแก้กลับเป็นข้อมูลได้

ตัวอย่างฟังก์ชั่นแฮชที่มีการใช้งานได้แก่ MD5, SHA-1 และ CRC32 เป็นต้น

MD5

MD5 (Message-Digest Algorithm 5) เป็นอัลกอริทึมที่ใช้ในการสร้างแฮช หรือ digest ของข้อมูลเพื่อใช้ในการตรวจสอบความถูกต้องของข้อมูล สำหรับ MD5 ถูกนำไปใช้ในการทำงานที่หลากหลายเช่นการตรวจสอบความถูกต้องของไฟล์ที่แชร์กันในอินเตอร์เน็ต การตรวจสอบความถูกต้องของการบีบอัดและขยายข้อมูล เป็นต้น สำหรับ MD5 จะทำการสร้างข้อมูลที่เป็นตัวแทน หรือเป็นข้อมูลในการตรวจสอบข้อมูลต่างๆ ซึ่งจะมีลักษณะเป็นตัวเลขฐานสิบหกจำนวน 32 ตัว

MD5 เป็นอัลกอริทึมที่คิดค้นขึ้นโดย Ron Rivest ในปี 1991 ซึ่งมาใช้ทดแทน MD4 ต่อมาในปี 1996 มีการค้นพบช่องโหว่ของ MD5 ซึ่งขณะนั้นยังไม่ถือว่าเป็นช่องโหว่ร้ายแรงนัก แต่นักคณิตศาสตร์ก็ได้แนะนำให้ใช้ SHA-1 แทน ในปี 2004 มีการค้นพบช่องโหว่ของ MD5 ที่ถือว่าเป็นช่องโหว่ร้ายแรงทำให้ MD5 มีการใช้งานลดน้อยลงเรื่อยๆ จนกระทั่งปี 2007 มีการค้นพบกระบวนการที่ทำให้ไฟล์ 2 ไฟล์มีค่า MD5 เดียวกันได้

SHA

SHA (Secure Hash Algorithm) เป็นอัลกอริทึมในการสร้างแฮช โดย National Security Agency (NSA) และประกาศใช้เป็นมาตรฐานโดย NIST ในการทำงานของ SHA จะสร้าง Message Digest ของข้อมูลต่างๆ ซึ่งจะมีความปลอดภัยดังนี้

1. ไม่สามารถคำนวณได้ว่าข้อมูลใดคือข้อมูลต้นฉบับของ Message Digest
2. ข้อมูล 2 ข้อมูลใดๆ จะไม่มี Messag Digest ที่ตรงกันแน่นอน
3. หากมีการเปลี่ยนแปลงข้อมูลเพียงเล็กน้อย จะมีการเปลี่ยนแปลงอย่างมากใน Message Digest

สำหรับอัลกอริทึมในกลุ่มของ SHA นี้จะมีอัลกอริทึมอยู่หลาย ตัวเช่น SHA-1, SHA-224, SHA-256, SHA-384 และ SHA-512 โดยตัวเลขหลัง SHA คือตัวเลขบอกขนาดของ Message Digest ที่ได้จากการใช้อัลกอริทึมนั้นๆ ยกเว้น SHA-1 จะมี Message Digest ขนาด 160 บิต

สำหรับความปลอดภัยในการใช้ SHA-1 นั้นปัจจุบันมีการค้นพบจุดอ่อนของ SHA-1 และกระบวนการในการค้นหาข้อมูลดิบที่ผ่าน SHA-1 แล้วได้ Message Digest ที่ตรงกันได้หลากหลายวิธี

MAC

เป็นข้อมูลสารสนเทศที่ใช้ในการพิสูจน์ตนข้อมูล โดย MAC นี้มีข้อแตกต่างจากฟังก์ชั่นแฮช คือ จำเป็นต้องใช้คีย์เป็นองค์ประกอบหนึ่งในการทำงานด้วย โดยอัลกอริทึม MAC จะรับพารามิเตอร์สองตัวคือ ข้อมูลที่ต้องการรับรอง และคีย์ลับของผู้ส่ง ดังนั้นผลลัพธ์ที่ได้จากอัลกอริทึม MAC จึงสามารถรับรองได้ทั้งความถูกต้องของข้อมูลที่ส่ง และความเป็นเจ้าของข้อมูลนั้นๆ ได้

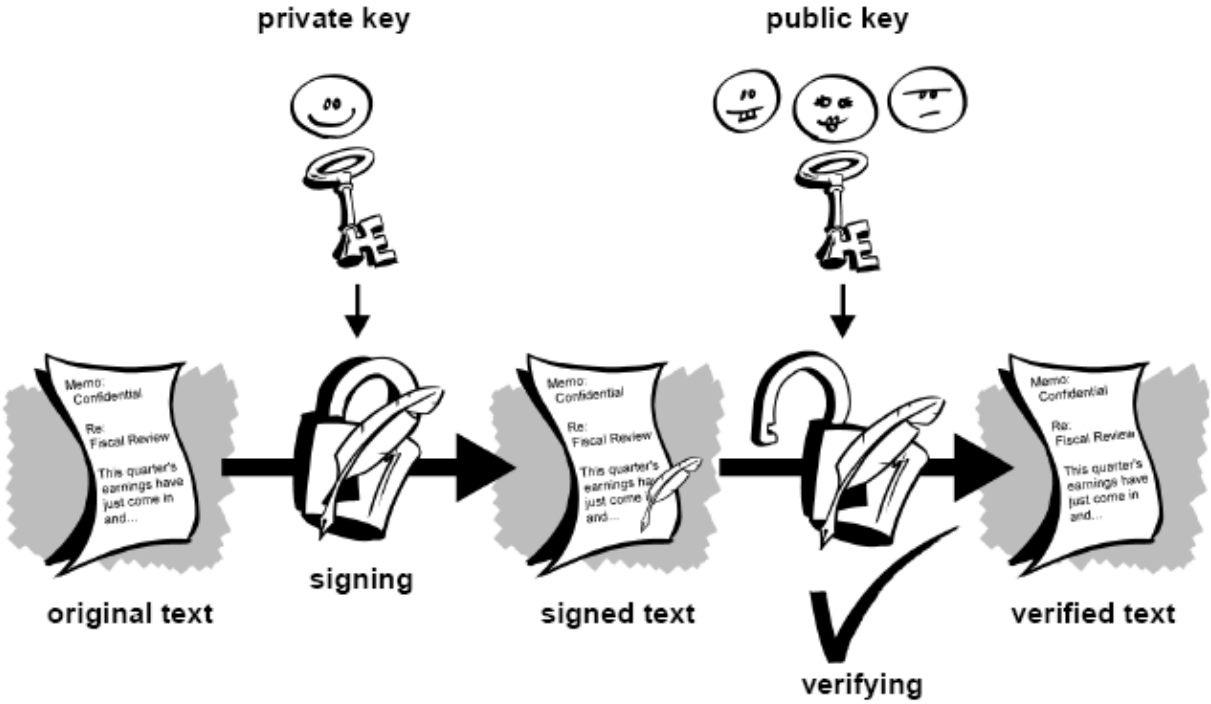
Digital Signature

ลายมือชื่อดิจิตอล (Digital Signature) คือ ข้อมูลอิเล็กทรอนิกส์ที่ได้จากการเข้ารหัสข้อมูลด้วยกุญแจส่วนตัวของผู้ส่งซึ่งเปรียบเสมือนเป็นลายมือชื่อของผู้ส่ง คุณสมบัติของลายมือชื่อดิจิตอล นอกจากจะสามารถระบุตัวบุคคล และ เป็นกลไกการป้องกันการปฏิเสธความรับผิดชอบแล้ว ยังสามารถป้องกันข้อมูลที่ส่งไปไม่ให้ถูกแก้ไข หรือ หากถูกแก้ไขไปจากเดิมก็สามารถล่วงรู้ได้

กระบวนการสร้างและลงลายมือชื่อดิจิตอลเริ่มจากการนำเอาข้อมูลที่จะส่ง ผ่านฟังก์ชันแฮชจนได้ Message Digest แล้วทำการเข้ารหัสด้วยกุญแจส่วนตัวของผู้ส่ง และผลลัพธ์ที่ได้คือ ลายมือชื่อดิจิตอล ของข้อมูลชุดนั้น จากนั้นจึงทำการส่ง ลายมือชื่อไปพร้อมกับข้อมูลต้นฉบับ ผู้รับจะตรวจสอบข้อมูลที่ได้รับว่าถูกแก้ไขระหว่างทางหรือไม่ โดยการนำข้อมูลต้นฉบับที่ได้รับ มาผ่านฟังก์ชั่นแฮชเพื่อให้ได้ Message Digest ฝั่งผู้รับ และถอดรหัสข้อมูลลายมือชื่อดิจิตอลด้วย กุญแจสาธารณะของผู้ส่ง จะได้ Message Digest ทางฝั่งผู้ส่ง แล้วทำการเปรียบเทียบ Message Digest ทั้งสองว่าเหมือนกันหรือไม่ ถ้าเหมือนกันแสดงว่าข้อมูลที่ได้รับนั้นถูกต้อง ไม่ถูกแก้ไข ถ้า Message Digest ที่ได้ แตกต่างกันจะหมายถึงข้อมูลที่ได้รับถูกเปลี่ยนแปลงระหว่างทาง

จากกระบวนการดังกล่าวเราจะพบว่าลายมือชื่อดิจิทัลจะแตกต่างกันไปตามข้อมูลต้นฉบับและบุคคลที่จะลงลายมือชื่อ กระบวนการที่ใช้จะมีลักษณะคล้ายคลึงกับการเข้ารหัสแบบอสมมาตร แต่การเข้ารหัสจะใช้

กุญแจส่วนตัวของผู้ส่ง และการถอดรหัสจะใช้กุญแจสาธารณะของผู้ส่ง ซึ่งสลับกันกับ การเข้าและถอดรหัสแบบกุญแจอสมมาตร ในการรักษาข้อมูลให้เป็นความลับ



รูปที่ 21 กระบวนการทำ Digital Signature ของข้อมูลต่างๆ

ตัวอย่างการทำงานที่มีการนำเทคนิคต่างๆ ของการตรวจสอบ Integrity มาช่วยในการตรวจสอบว่าข้อมูลมีการเปลี่ยนแปลงไปจากต้นฉบับหรือไม่ดังนี้

1. Checksum ในหน่วยความจำ และโปรแกรมต่างๆ ในอุปกรณ์อิเล็กทรอนิกส์
2. Checksum ในโปรโตคอลต่างๆ เช่น IP, TCP, ICMP, UDP
3. Checksum ในหมายเลขบัตรประชาชน หมายเลขบัตรเครดิต หรือหมายเลขบัญชีธนาคารต่างๆ
4. Checksum ในกระบวนการบีบอัดและขยายไฟล์
5. ค่า MD5 และ SHA1 ของซอฟต์แวร์ต่างๆ ที่ให้ Download ในอินเตอร์เน็ต

6. ค่า Digital Signature ของข้อมูลต่างๆ ที่ผู้ใช้งานส่งไปยังคนอื่นๆ
7. ค่า Signature ในการตรวจสอบความผิดปกติในระบบ Intrusion Detection System ที่ตรวจสอบการเปลี่ยนแปลงข้อมูลในไฟล์ระบบที่สำคัญ

บทที่ 5. Availlabiltiy

Availlability คือความสามารถในการให้บริการซึ่งตอบสนองการเรียกใช้งานได้ตลอดเวลาที่มีความต้องการเกิดขึ้นโดยการตอบสนองการเรียกใช้งานต้องสามารถตอบสนองได้อย่างสมบูรณ์ไม่ติดขัด สำหรับระบบคอมพิวเตอร์ของธุรกิจต่างๆ ที่มีผู้ใช้งานอยู่ตลอดเวลา การให้บริการแก่ผู้ใช้งานซึ่งเป็นลูกค้านั้น ถือว่ามีความสำคัญสูงมาก Availlability จึงเป็นหัวใจของการให้บริการระบบคอมพิวเตอร์ใดๆ

สำหรับปัญหาที่เกิดขึ้นในระบบที่ทำให้ระบบไม่มี Availlability แบ่งออกเป็น 2 รูปแบบคือปัญหาที่ทำให้ผู้รับบริการไม่สามารถเข้าถึงผู้ให้บริการได้ ได้แก่ ปัญหาทางระบบเครือข่ายทำให้ไม่สามารถเปิดให้บริการได้ทำให้ระบบ down และปัญหาที่ทำให้ผู้ให้บริการไม่สามารถให้บริการได้อย่างเต็มที่ เช่นระบบโดนโจมตี ทำให้ไม่สามารถบริการได้อย่างเต็มที่ เซิร์ฟเวอร์ไม่สามารถรองรับการร้องขอบริการได้อย่างเต็มที่ เป็นต้น

แนวทางการสร้าง Availlability ในระบบ ซึ่งจำเป็นต้องพึ่งพากระบวนการต่างๆ เพื่อให้ผู้ใช้งานสามารถระบบรับบริการได้อย่างต่อเนื่องได้แก่

1. Access Control เพื่อควบคุมไม่ให้การโจมตีใดๆ เข้าสู่ระบบ
2. การ Monitor และการตรวจตราระบบทำให้สามารถแก้ไขปัญหาต่างๆ ได้อย่างรวดเร็ว
3. การออกแบบระบบคอมพิวเตอร์และเครือข่ายให้มีความทนทานสูง สามารถรองรับการให้บริการได้อย่างเต็มที่
4. การวางแผนการบริหารความเสี่ยงและการประเมินความเสี่ยง
5. การกำหนดนโยบายการรักษาความปลอดภัยตามมาตรฐานสากล
6. การพัฒนาบุคลากรให้มีความสามารถ

ความสำคัญของ Availlability

ในแง่ของ Availlability ถือได้ว่ามีส่วนสำคัญอย่างยิ่งในเรื่องของการให้บริการแก่ผู้ใช้งาน และการดำเนินธุรกิจต่างๆ ในการลงทุนเพื่อพัฒนาระบบสารสนเทศหนึ่งๆ จำเป็นต้องใช้เงินลงทุนปริมาณมาก ซึ่งในการลงทุนนั้นจะมีการคาดการณ์ถึงผลลัพธ์ที่ได้ และระยะเวลาในการคืนทุนทั้งหมด โดยการคาดการดังกล่าวจะอยู่บนสมมุติฐานที่ให้ระบบสามารถดำเนินการได้โดยปกติ แต่ในการทำงานในระบบจริง การทำงานของระบบสารสนเทศต่างๆ มักจะมีปัญหาเกิดขึ้นเสมอๆ โดยเฉพาะอย่างยิ่งระบบที่ออกแบบมาโดยไม่ได้คำนึงถึง Availlability เช่น

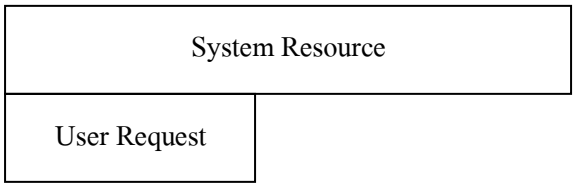
ระบบสารสนเทศที่ให้บริการ E-Commerce หนึ่งมีมูลค่าในการลงทุน 3 ล้านบาท ซึ่งคาดหวังว่าจะคืนทุนหลังจากสร้างระบบเรียบร้อยแล้วเป็นระยะเวลา 3 ปี ซึ่งการคาดการดังกล่าวอยู่บนพื้นฐานที่ว่าระบบสามารถทำงานได้ตลอด 24 ชั่วโมง แต่ภายหลังเมื่อทำงานจริง ระบบสามารถให้บริการได้เพียง 95 เปอร์เซ็นต์เท่านั้น ซึ่งก็คือระบบมีระยะเวลา Down Time คิดเป็น 5 เปอร์เซ็นต์ของระยะเวลาทำงานทั้งหมด ความเสียหายที่จะเกิดขึ้นในการลงทุนครั้งนี้ได้แก่

1. ขาดทุนเงินลงทุน เนื่องจากการลงทุนครั้งนี้ต้องการให้ได้ระบบที่สามารถทำงานได้ตลอด 24 ชั่วโมง แต่ระบบมีปัญหาคิดเป็น 5 เปอร์เซ็นต์ของระยะเวลาทำงานทั้งหมด นั่นหมายความว่าการลงทุนครั้งนี้ขาดทุนไปแล้ว 5 เปอร์เซ็นต์
2. ขาดทุนกำไร เนื่องจากการลงทุนครั้งนี้คาดว่าจะคืนทุนในระยะเวลา 3 ปี นั่นหมายความว่าระบบควรทำรายได้ให้กับเจ้าของระบบเป็นเงินโดยเฉลี่ย 1 ล้านบาทต่อปี ซึ่งหากระบบมีปัญหาในช่วงระยะเวลาการทำงาน 5 เปอร์เซ็นต์ จะหมายความว่าเจ้าของระบบจะขาดรายได้ ไปอย่างน้อย 5 เปอร์เซ็นต์ต่อปีเช่นกัน ทำให้ระยะเวลาการคืนทุนจริงๆ ของระบบต้องใช้ระยะเวลาสูงขึ้น
3. ปัญหาด้านความเชื่อมั่นในระบบซึ่งตีค่าไม่ได้ เนื่องจากระบบที่มีความสำคัญสูง หากไม่มีเสถียรภาพเพียงพอ จะทำให้ไม่สามารถบริการผู้ใช้งานได้ โดยเฉพาะอย่างยิ่งถ้าเป็นระบบที่ให้บริการทำธุรกรรมที่สำคัญเช่น ธนาคาร หรือตลาดหลักทรัพย์เป็นต้น

การสร้าง Availlability จึงมีความสำคัญอย่างมากในระบบ ในการวิเคราะห์ถึง Availlability ในระบบนั้นให้มองภาพของปัญหาง่ายๆ คือทำอย่างไรให้ระบบสามารถทำงานได้ตลอดเวลาโดยผู้ใช้งานที่ต้องการใช้งานจะต้องได้รับบริการจากระบบเสมอ ในการวิเคราะห์ถึงองค์ประกอบที่ทำให้ระบบมีAvaillability จะพบว่าคุณลักษณะของระบบที่มีเสถียรภาพสูง มีดังนี้

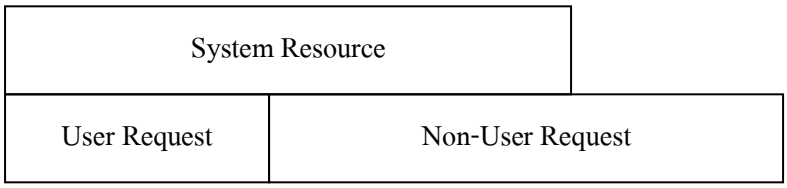
1. ระบบทั้งฮาร์ดแวร์ และซอฟต์แวร์ ต้องทำงานอย่างเป็นปกติ สามารถรองรับการร้องขอการทำงานทั้งหมดได้อย่างเหมาะสม
2. ระบบเครือข่ายต้องสามารถทำงานได้เป็นปกติและรองรับการทำงานต่างๆ ได้อย่างครบถ้วนเพียงพอ
3. ผู้ใช้งานระบบสามารถใช้งานระบบอย่างถูกต้อง ในปริมาณงานที่เหมาะสม
4. ไม่มีการโจมตีระบบในรูปแบบต่างๆ
5. ผู้ดูแลระบบสามารถคาดการถึงปัญหาและสามารถแก้ไขปัญหาต่างๆ ได้อย่างทันท่วงที

ในการทำงานของระบบสารสนเทศต่างๆ เมื่อมองว่าระบบสารสนเทศเป็นผู้ให้บริการทรัพยากร และผู้ใช้งานระบบเป็นผู้ขอใช้ทรัพยากร สำหรับระบบที่มีเสถียรภาพควรมีลักษณะการทำงานที่ระบบให้บริการทรัพยากร มากกว่าทรัพยากรที่ผู้ใช้งานระบบร้องขอ



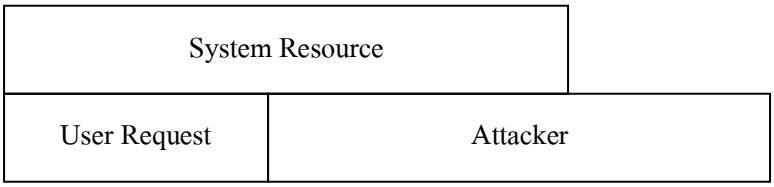
รูปที่ 22 สัดส่วนของทรัพยากรในระบบและทรัพยากรที่ผู้ใช้งานต้องการในระบบปกติ

แต่ทว่าในระบบการทำงานที่เป็น Public Service ที่ให้บริการเช่นเว็บเซิร์ฟเวอร์ที่ให้บริการผู้ใช้งานในระบบ และผู้ใช้งานทั่วไปด้วย หรือแม้กระทั่งระบบเครือข่ายที่เป็นทางผ่านของระบบย่อยอื่นๆ มักจะประสบปัญหาที่ผู้ใช้งานนอกระบบ เข้ามาร่วมใช้ทรัพยากรในระบบด้วย ทำให้ทรัพยากรของระบบไม่มีเพียงพอในการให้บริการผู้ใช้งานของระบบ ผลที่ได้ทำให้ระบบไม่มีการตอบสนองที่เพียงพอกับความต้องการของผู้ใช้งาน



รูปที่ 23 สัดส่วนของทรัพยากรในระบบและทรัพยากรที่ผู้ใช้งานต้องการในภาวะผิดปกติ

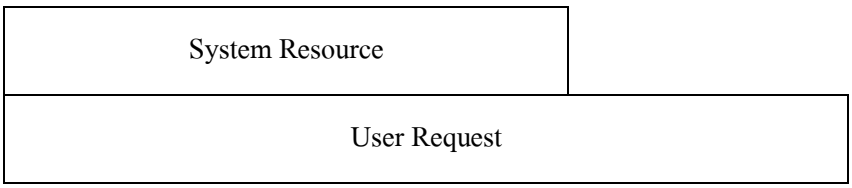
ยิ่งไปกว่านั้นหากกลุ่มผู้ใช้งานที่ไม่ใช่ผู้ใช้งานระบบนั้น เป็นผู้ไม่ประสงค์ดีต่อระบบ มีการร้องขอทรัพยากรในระบบในลักษณะที่เป็นการโจมตีระบบเช่นการโจมตีในเครือข่ายแบบ Syn Flood , Port Scan หรือ Denial of Service เป็นต้น



รูปที่ 24 สัดส่วนของทรัพยากรในระบบและทรัพยากรที่ผู้ใช้งานต้องการในภาวะผิดปกติ

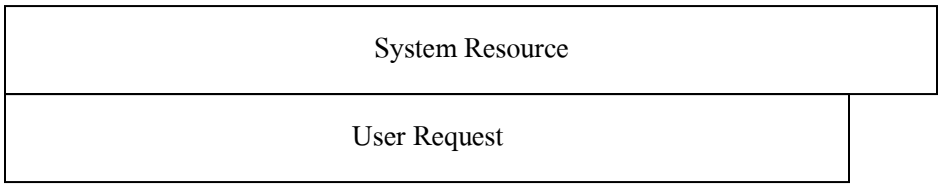
ในการทำให้ระบบยังคงสามารถให้บริการกับการร้องขอของผู้ใช้งานระบบได้ จำเป็นต้องมีการคัดกรอง (Filter) หรือการควบคุมการเข้าถึงระบบ (Access Control) โดยคัดกรองข้อมูลการร้องขอที่เป็นการโจมตีระบบไม่ให้เข้ามาในระบบ หรือการควบคุมการเข้าถึงระบบ ไม่ให้ผู้ใช้งานที่ไม่ใช่ผู้ใช้งานระบบเข้าใช้งานระบบ

เนื่องจากผู้ใช้งานระบบสารสนเทศหรือรูปแบบการใช้งานระบบสารสนเทศ มักมีการขยายตัวมากขึ้น โดยเฉพาะอย่างยิ่งระบบที่มีการใช้งานมาเป็นเวลานาน ปริมาณผู้ใช้งานที่เพิ่มมากขึ้นเรื่อยๆ จะทำให้ความต้องการทรัพยากรของระบบมีมากขึ้น จนล้นระบบ ทำให้การทำงานไม่สามารถทำงานต่อได้อย่างเป็นปกติ



รูปที่ 25 การขยายตัวของผู้ใช้งานจนความต้องการเกินกว่าทรัพยากรระบบ

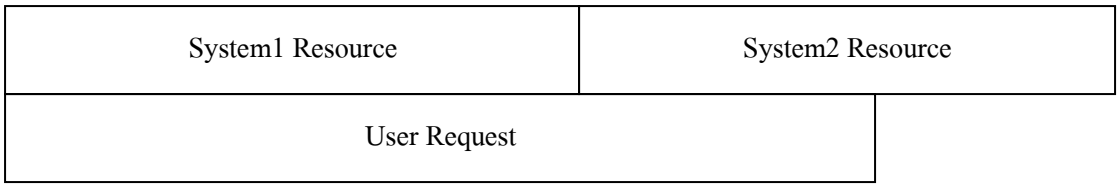
ในการปรับปรุงระบบให้สามารถรองรับการขยายตัวของความต้องการผู้ใช้งานที่ขยายตัวมากขึ้นนั้น ผู้ดูแลระบบอาจสามารถแก้ปัญหาโดยการเพิ่มทรัพยากรในระบบให้มากขึ้น โดยการเพิ่ม CPU, Memory, Network Capacityและทรัพยากรอื่นๆ ซึ่งการปรับปรุงระบบในลักษณะนี้สามารถทำได้โดยง่ายหากระบบยังมี Slot เพียงพอและยังไม่เกินขีดจำกัดของระบบที่สามารถรองรับการทำงานได้



รูปที่ 26 การขยายทรัพยากรระบบเพื่อรองรับผู้ใช้งานที่เพิ่มขึ้น

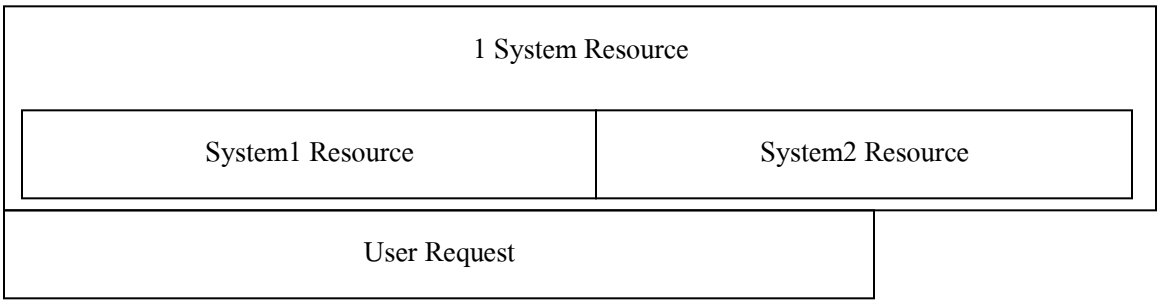
สำหรับระบบส่วนใหญ่ที่มักจะมีการจัดซื้อโดยกำหนดสเปคของเครื่องไว้สูงสุดของรุ่นนั้นๆ แล้ว จะไม่สามารถเพิ่มทรัพยากรต่างๆ ได้เลย หากต้องการเพิ่มทรัพยากรให้เพียงพอต่อการใช้งานของผู้ใช้งานนั้นจะสามารถทำได้ 2 วิธีการคือ

1. เพิ่มระบบที่ให้บริการขึ้นให้มีระบบที่ให้บริการมากกว่า 1 ระบบ แล้วทำการตั้งค่าระบบให้มีการแจกจ่ายงานของผู้ใช้งานไปยังระบบทั้งหมด รูปแบบการทำงานในลักษณะนี้จะเรียกว่า “Load Balancing” ซึ่งจำเป็นต้องใช้อุปกรณ์และการตั้งค่าระบบเพิ่มเติมเล็กน้อย



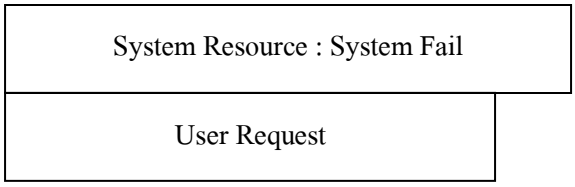
รูปที่ 27 การดำเนินการในลักษณะ Load Balance

2. ทำการเพิ่มระบบที่ให้บริการขึ้นอีกระบบหนึ่ง แล้วทำการตั้งค่าระบบให้มีการทำงานเป็น “Clustering” คือทำให้ผู้ใช้งานมองเห็นระบบที่มีอยู่เป็นระบบใหญ่ระบบเดียว แต่ในการตั้งค่าการทำงานของระบบให้เป็น “Clustering” ได้นั้น ระบบปฏิบัติการหรือระบบเครือข่ายจะต้องรองรับการทำงานแบบ Clustering ด้วย



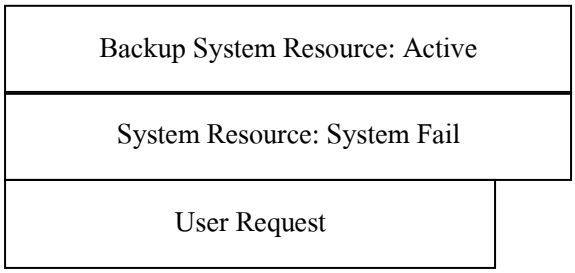
รูปที่ 28 การดำเนินการในลักษณะ Clustering

ในส่วนของการขยายขนาดระบบให้รองรับการร้องขอทรัพยากรของระบบได้นั้น ทำให้ระบบสามารถทำงานได้อย่างมีเสถียรภาพมากขึ้น แต่ในกรณีที่เกิดอุบัติเหตุทำให้ระบบต้องปิดตัวเองลงไม่ว่ากรณีใดๆ สำหรับระบบที่มีความสำคัญสูง เช่นระบบของสนามบิน หรือตลาดหุ้นที่จำเป็นต้องมีการทำงานอยู่ตลอดเวลา ผู้ดูแลระบบจำเป็นต้องออกแบบให้ระบบยังคงทำงานได้



รูปที่ 29 ภาวะที่ระบบหลักไม่สามารถให้บริการได้

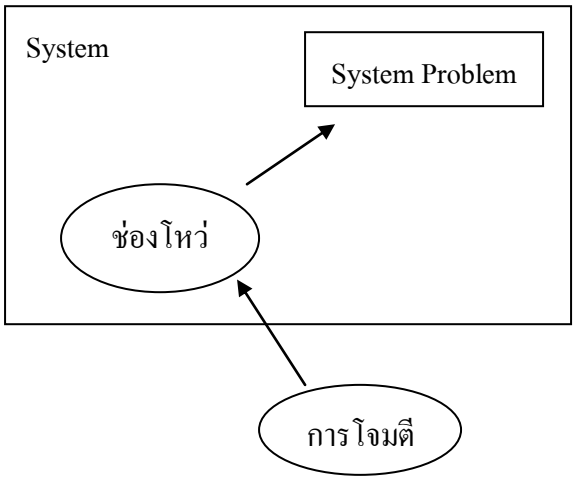
ในการออกแบบระบบให้สามารถทำงานได้ถึงแม้ว่าจะเกิดอุบัติเหตุทำให้ระบบไม่สามารถทำงานได้นั้น จำเป็นต้องมีระบบสำรองที่มีความสามารถในการทำงานเหมือนกับระบบหลัก และมีกระบวนการในการโยกย้ายการทำงานจากระบบที่มีปัญหาไปยังระบบสำรอง ซึ่งกระบวนการดังกล่าวจะมีลักษณะการทำงานแบบ “Fault Tolerant”



รูปที่ 30 การออกแบบระบบให้เป็น Fault Tolerant

ระบบที่มีปัญหาความปลอดภัย

ในการโจมตีระบบในลักษณะใดๆ จะสัมฤทธิผลขึ้นได้ก็ต่อเมื่อมีสาเหตุ และปัจจัยที่เหมาะสม ในกรณีของการโจมตีระบบที่ทำให้ระบบเกิดความผิดปกติในระบบหรือแม้กระทั่งทำให้ระบบปิดตัวเองลง จำเป็นต้องมีสาเหตุ และปัจจัยที่เหมาะสมในการโจมตีระบบเช่นเดียวกัน สำหรับสาเหตุของการโจมตีนั้นคือช่องโหว่ต่างๆ ที่มีอยู่ในระบบ ส่วนปัจจัยที่ทำให้ระบบเกิดปัญหาความปลอดภัยได้นั้นคือการโจมตีที่สอดคล้องกับช่องโหว่ที่มีอยู่ในระบบ



รูปที่ 31 การโจมตีช่องโหว่ของระบบ

โดยสรุปการโจมตีระบบจะสัมฤทธิผลได้ก็ต่อเมื่อ

ช่องโหว่ + การโจมตีช่องโหว่ = ปัญหาความปลอดภัยระบบ

จะเกิดปัญหาขึ้นได้ก็ต่อเมื่อมีองค์ประกอบของปัญหาอย่างครบถ้วน เท่านั้น ในกรณีที่มีช่องโหว่แต่ไม่มีการโจมตีระบบ หรือมีการโจมตีระบบ แต่ไม่มีช่องโหว่ ก็ยังไม่เกิดปัญหาความปลอดภัยในระบบ จากสมการดังกล่าว ทำให้ผู้ดูแลระบบต้องมีการทำงานเพื่อลดปัญหาและแก้ไขปัญหาต่างๆ ดังต่อไปนี้

1. ลดช่องโหว่ให้มีในระบบให้น้อยที่สุด
2. คัดกรองการโจมตีระบบไม่ให้เข้าสู่ระบบได้
3. ตอบสนองต่อปัญหาความปลอดภัยในระบบอย่างรวดเร็ว

กระบวนการที่จำเป็นต้องทำได้แก่

1. ทำ Assessment เพื่อทราบปริมาณของช่องโหว่ในระบบ
2. ทำ Hardening เพื่อลดปริมาณช่องโหว่ในระบบ
3. ทำการ Filter การโจมตีที่เข้ามาในระบบ
4. ทำการ Monitoring เพื่อให้ทราบถึงการโจมตีช่องโหว่ในระบบ

เหตุการณ์ต่างๆ ที่เกิดขึ้นในระบบ

1. ในกรณีที่ผู้ดูแลระบบสามารถปิดช่องโหว่ได้มาก จะทำให้ระบบมีเสถียรภาพสูง ไม่เกิดปัญหาใดๆ ถึงแม้ว่าจะมีการโจมตีที่หลากหายก็ตาม หากไม่ตรงกับช่องโหว่ก็จะไม่เกิดปัญหาใดๆ ทำให้การบริหารจัดการทำได้ง่ายและสบายขึ้น
2. ระบบที่สามารถ Filter การโจมตีได้มากจะทำให้ระบบมีเสถียรภาพสูงเช่นกัน ถึงแม้ว่าระบบจะมีช่องโหว่ แต่หากไม่มีการโจมตีที่ตรงกับช่องโหว่นั้น ก็จะไม่เกิดปัญหาความปลอดภัยขึ้นเช่นกัน
3. ในระบบที่ผู้ดูแลระบบไม่มีการปิดช่องโหว่และคัดกรองการโจมตีต่างๆ แต่ Response ปัญหาต่างๆ อย่างรวดเร็ว จะทำให้การทำงานของระบบติดขัดเป็นบางช่วงเวลา ไม่ถือว่ามีเสถียรภาพ เนื่องจากจะมีปัญหาเกิดขึ้นบ่อยครั้ง ต้นทุนการดูแลรักษาระบบสูงมาก ผู้ดูแลระบบจะไม่มีเวลาวางแผนระบบในระยะยาวได้เนื่องจากต้องคอยแก้ไขปัญหาต่างๆ อยู่ตลอดเวลา

ดังนั้นในการดูแลระบบให้มีความเสถียรเพียงพอที่จะให้บริการกับผู้ใช้งานได้ตลอดเวลาได้ จำเป็นต้องคอยตรวจสอบดูแลระบบไม่ให้เกิดปัญหาขึ้น โดยการตรวจสอบระบบนั้นผู้ดูแลระบบจะไม่สามารถคอยตรวจตราระบบได้ตลอดเวลา จึงมีการใช้ซอฟต์แวร์ช่วยในการตรวจตราระบบต่างๆ เพื่อให้ผู้ดูแลระบบสามารถทำงานได้ง่ายขึ้น การทำงานของโปรแกรมในกลุ่มนี้จะมีความสามารถในการตรวจสอบรายละเอียดการทำงานในส่วนงานที่ผู้ดูแลระบบต้องการเช่น การตรวจสอบจุดบกพร่องภายในระบบ การตรวจจับการทำงานที่ผิดปกติ การตรวจหาช่องโหว่ของระบบ ฯลฯ ซึ่งตัวอย่างโปรแกรมที่ใช้ในงานดังกล่าวได้แก่ Intrusion Detection and Prevention System, Virus Scanner และ Vulnerability Scanner

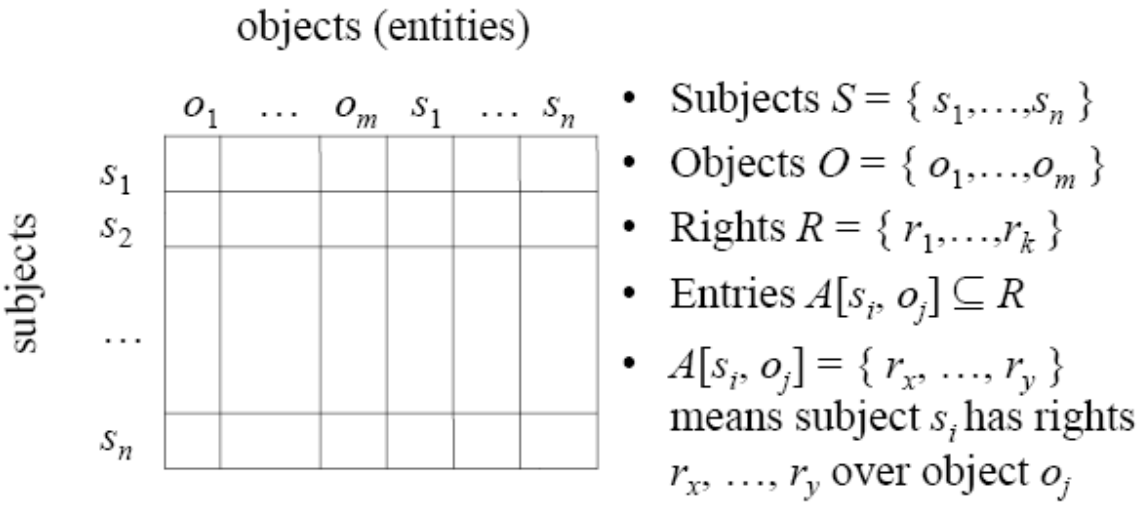
บทที่ 6. Access Control

การทำ Access Control เป็นกระบวนการที่ใช้ในการป้องกันการใช้งานทรัพยากรโดยผู้ที่ไม่ได้รับอนุญาต ซึ่งกระบวนการ Access Control นั้นมีการใช้งานในหลากหลายรูปแบบซึ่งตัวอย่างในชีวิตประจำวันเราจะเห็นได้ทั่วไปเช่น การใช้กุญแจไขปิดล๊อกประตู ซึ่งมีเพียงเจ้าของกุญแจเท่านั้นจึงจะสามารถเปิดประตูได้ การตรวจบัตรเข้าชมภาพยนตร์ซึ่งอนุญาตเฉพาะผู้ที่มีบัตรเท่านั้นจึงจะเข้าชมภาพยนตร์ได้ การใช้บัตรผ่านประตูและรหัสเปิดประตูเพื่อเข้าไปยังห้องที่เก็บข้อมูลสำคัญในธนาคาร หรือหน่วยงานต่างๆ และการใช้ Username และ Password ในการเข้าอ่าน E-mail ต่างๆ ของผู้ใช้งานแต่ละคนเป็นต้น

โดยหลักการทำงานของ Access Control มีกระบวนการดำเนินการดังนี้คือ

1. กำหนดผู้ใช้งานระบบว่ามีใครบ้าง
2. กำหนดค่าทรัพยากรที่ต้องการควบคุมการใช้งานว่ามีอะไรบ้าง
3. กำหนดกระบวนการใช้งานของผู้ใช้งานระบบว่ามีอะไรบ้าง
4. กำหนดการใช้งานของผู้ใช้งานแต่ละคนว่าผู้ใช้งานแต่ละคนสามารถทำงานอะไรได้บ้างและใช้งานทรัพยากรใดได้บ้าง

ในการดำเนินการเกี่ยวกับ Access Control จะใช้ Access Control Matrix ในการสร้างกฎหรือความสัมพันธ์ระหว่างผู้ใช้งานและทรัพยากรในระบบ โดยกระบวนการสร้าง Access Control Matrix จะเป็นการสรุปรวมนโยบายการป้องกันทรัพยากรต่างๆ หรือการกำหนดสิทธิในการเข้าใช้ทรัพยากรต่างๆ ได้โดยชัดเจน



รูปที่ 32 Access Control Matrix

สำหรับลักษณะของ Access Control Matrix คือตารางที่ประกอบด้วยส่วน Row ของ Subject และ Column ของ Object (อาจเป็น Subject ด้วย) ในตารางแต่ละช่องจะแสดงสิทธิ (Right) การใช้งานของ Subject เมื่อมีการใช้ทรัพยากรของ Object ยกตัวอย่างเช่น Access Control Matrix ของโปรแกรมสองโปรแกรมคือ X และ Y ซึ่งมีการใช้งานไฟล์ F และ G ดังรูป

	F	**G**	**P**	**Q**
P	RWO	R	RWXO	W
Q	A	RO		RWXO

รูปที่ 33 ตัวอย่าง Access Control Matrix ในการใช้งานไฟล์ระบบ

สิทธิในการใช้งานทรัพยากรของตัวอย่างนี้คือการ Read(R) , Write(W) , Execute(X) และ Owner(O) โดยการใช้งานของโปรแกรม P และ Q สามารถใช้งานไฟล์ F และ G รวมถึง การใช้งานพื้นที่ต่างๆ ในโพรเซสของ P และ Q เป็นไปดังตาราง

การใช้งาน Access Control Matrix นั้นสามารถประยุกต์ใช้กับการควบคุมการใช้งานทรัพยากรต่างๆ ได้อย่างกว้างขวาง ไม่ว่าจะเป็นการใช้งานฐานข้อมูล การใช้งานเครือข่าย การเข้าใช้งานระบบของผู้ใช้งานแต่ละคน ซึ่งการทำงานแต่ละรูปแบบถึงแม้ว่าเป็นการทำงานที่แตกต่างกัน แต่สามารถใช้หลักการเดียวกันในการควบคุมการใช้งานได้

สำหรับกระบวนการกำหนดการใช้งานทรัพยากรโดยใช้ Access Control Matrix นี้มีข้อดีคือสามารถกำหนดค่าต่างๆ ให้กับ Subject และ Object ได้อย่างครบถ้วน แต่มีเสียเล็กน้อยคือถ้า Subject และ Object มีจำนวนมาก จะทำให้ตารางมีขนาดใหญ่ การกำหนดค่าต่างๆ จะทำได้ยาก รวมถึงไม่สามารถกำหนดค่าโดยมีการกำหนดเงื่อนไขต่างๆ ได้ เช่นการกำหนด Access Control Matrix ในการใช้งานแต่ละช่วงเวลา จะไม่สามารถใช้ Access Control Matrix เพียง Matrix เดียวได้เนื่องจาก Access Control Matrix ไม่ได้มีรูปแบบหรือพื้นที่ในการกำหนดเงื่อนไขต่างๆ ได้

ในกรณีของการควบคุมการใช้ทรัพยากรระบบเครือข่าย สามารถใช้ Access Control Matrix ได้แต่โดยข้อจำกัดของ Access Control Matrix ซึ่งไม่สนับสนุนการควบคุมโดยใช้ตรรกะที่ซับซ้อนได้ การควบคุมระบบเครือข่ายจึงต้องปรับเปลี่ยนรูปแบบการควบคุม จาก Access Control Matrix ให้อยู่ในรูปของ Access Control List ที่มีรูปแบบการควบคุมที่ซับซ้อนกว่าได้ ยกตัวอย่าง Access Control List ที่ใช้ควบคุมระบบเครือข่ายให้โดยใช้ตรรกะในการควบคุมที่ซับซ้อนเช่น

```
router(config)#access-list 110 permit host 161.246.5.10 gt 1024 host –
161.246.4.7 eq 80

router(config)#access-list 110 deny tcp host any any

router(config)#interface fastethernet1

router(config-if)#ip access-group 110 in
```

คำสั่งข้างต้นเป็นคำสั่งที่ให้เครื่องคอมพิวเตอร์ 161.246.5.10 เท่านั้นที่สามารถติดต่อกับ Web Server ที่มีหมายเลขไอพี 161.246.4.7 สำหรับเครื่องอื่น ๆ จะติดต่อไม่ได้ ซึ่งจะเห็นว่าเราสามารถตั้งค่าให้กับเราเตอร์ได้ค่อนข้างหลากหลายเงื่อนไข

ถึงแม้ว่า Access Control List จะรองรับการใช้งานในการควบคุมการใช้ทรัพยากรอย่างซับซ้อนได้ แต่ก็มีรูปแบบที่เปิดมาก และไม่มีกฎตายตัวว่าจะต้องควบคุม Subject และ Object ใดบ้าง จึงทำให้เกิดปัญหาการตั้งกฎที่ควบคุมระบบได้ไม่ครบถ้วนเนื่องจากไม่มีรูปแบบควบคุมให้มีรายการของ Subject และ Object อย่างครบถ้วน และอาจเกิดปัญหา Rule Conflict ซึ่งมีกฎตั้งแต่สองกฎที่ควบคุมการใช้ทรัพยากรที่ขัดแย้งกัน

สำหรับการสร้าง Access Control ขึ้นมาในระบบอื่นๆ ที่ไม่ใช่ใน Network Protocol จำเป็นต้องมีการกำหนดตัวตนของผู้ใช้งานหรือ Identity ก่อนซึ่งต้องอาศัยกระบวนการระบุตัวตนของผู้ใช้งานต่างๆ มีการพิสูจน์ว่าผู้ใช้งานที่ใช้ Identity นั้นๆ คือเจ้าของ Identity นั้นๆ จริง แล้วจึงมีการกำหนดสิทธิการใช้งานให้กับ Identity นั้นๆ ตามนโยบายที่กำหนด

เข้าใจความหมายของ Identification Authentication Authorization

Identification หมายถึงการระบุตัวตนของสิ่งต่างๆ ในระบบ จะเป็นกระบวนการที่ผู้ใช้งานระบบจะแจ้งหลักฐาน(Identity) การมีตัวตนของตัวเอง สำหรับ Identification สำหรับผู้ใช้งานระบบสามารถใช้เช่นชื่อผู้ใช้เป็นต้นซึ่งโดยหลักการของ Identification จะต้องการสิ่งของ หรือข้อมูลใดๆ ก็ตามที่ผู้ใช้งานคนนั้นๆ “เป็นเจ้าของ” สำหรับคุณสมบัติของ Identity ที่ดีควรปลอมแปลงยาก และเป็นของบุคคลนั้นๆ เท่านั้น

Authentication หมายถึงกระบวนการในการพิสูจน์ตัวตนว่าบุคคลที่ใช้งานระบบอยู่นั้นใช่บุคคลคนนั้นๆ จริงหรือไม่ เนื่องจากการใช้งานระบบต่างๆ จะเป็นแบบการใช้งานระยะไกล ไม่สามารถพิสูจน์ตัวตนได้เนื่องจากไม่เห็นหน้า ไม่ทราบลักษณะ แต่จะเห็นเพียงข้อมูลที่วิ่งผ่านไปมาเท่านั้น ซึ่งหมายถึงการใช้งานระบบต่างๆ เป็นแบบ Logical ทั้งสิ้น กระบวนการ Authentication จึงเป็นกระบวนการที่ตรวจสอบว่า Logical ที่แทนบุคคล หรือระบบต่างๆ นั้น เป็นตัวแทนของบุคคลหรือระบบนั้นๆ จริง กระบวนการในการทำ Authentication ได้แก่ การพิสูจน์หลักฐานที่บุคคลนั้นๆ นำมาเสนอเพื่อบ่งบอกว่าคนๆ นั้นเป็นคนๆ นั้นจริงๆ เช่น Username และ Password

Authorization หมายถึงการพิสูจน์สิทธิว่าบุคคลที่ผ่านกระบวนการ Authentication นั้นมีสิทธิในการใช้งานระบบหรือทรัพยากรใดได้บ้าง จะเป็นกระบวนการที่เกี่ยวข้องกับการการตั้งค่าของสิทธิต่างๆ ของผู้ใช้งานในระบบ เพื่อให้การดำเนินการต่างๆ ถูกต้องตาม Role ของระบบที่ได้กำหนดไว้ล่วงหน้า

ทั้ง Identification, Authentication และ Authorization มีส่วนเกี่ยวข้องในการควบคุมการเข้าถึงทรัพยากร โดยในการเข้าใช้งานระบบผู้ใช้งานจะแสดง Identity ของตนเองเพื่อ Authentication และระบบจะทำการ Authorization เมื่อมีการใช้งานทรัพยากรใดๆ ในระบบ

Identity

โปรแกรมหรือระบบต่างๆ มักมีการทำงานโดยมีรายการของผู้ใช้งานระบบซึ่งมักจะประกอบด้วยรายละเอียดต่างๆ ดังต่อไปนี้

- Username / User ID
- Credential (Password, Certificate, และอื่น)
- Directory Attribute (Name , E-Mail , Phone , Address, และอื่นๆ)
- Organization
- Group
- Application Right
- Policy

สำหรับข้อมูลต่างๆ ของผู้ใช้งานนี้ระบบจำเป็นต้องมีการจัดเก็บเพื่อใช้ในระบบ Authentication โดยกระบวนการ Authentication คือการที่ผู้ใช้งานระบบพิสูจน์ Identity ของตัวเองโดยใช้ Credential ซึ่ง Credential ที่นิยมใช้กันมากที่สุดคือการใช้ Username ร่วมกับรหัสผ่าน ภายหลังจากผ่านกระบวนการ Authentication แล้วระบบหรือโปรแกรมนั้นๆ จะทำการ Authorization โดยดึงข้อมูล Identity และข้อมูลอื่นๆ ที่เกี่ยวข้องเพื่อ

ตัดสินใจว่าผู้ใช้งานนั้นจะสามารถใช้งานระบบหรือโปรแกรมนั้นๆ ได้หรือไม่ ซึ่งกระบวนการ Authorization นี้สามารถดำเนินการได้โดยใช้ข้อมูล Group , Membership , Organization และ Application Right

Identity Management

ในกระบวนการ Authentication และ Authorization ของระบบหรือโปรแกรมต่างๆ จำเป็นต้องมีการดึงข้อมูล Identity ต่างๆ ของผู้ใช้งานระบบ นั่นหมายความว่าโปรแกรมหรือระบบต่างๆ จะต้องดึงข้อมูลจากแหล่งข้อมูลใดก็ตามในระบบ ซึ่งอาจเป็นฐานข้อมูลผู้ใช้งานของโปรแกรมนั้นๆ ในกรณีที่มีการเก็บ Identity ของผู้ใช้งานระบบถูกเก็บอยู่ในฐานข้อมูลย่อยต่างๆ หลากหลายแหล่ง จะทำให้การบริหารจัดการทำได้ยากมากขึ้น โดยปัญหาสำคัญที่จะเกิดขึ้นเมื่อมีการบริหารจัดการฐานข้อมูลผู้ใช้งานที่กระจายตัวกันคือเมื่อมีการเปลี่ยนแปลงข้อมูลจากจุดใดจุดหนึ่งต้องมีการ update ที่ฐานข้อมูลอื่นๆ ด้วย จากปัญหาดังกล่าวจึงทำให้มีการใช้งานโปรแกรมจำพวก Identity Management โดยโปรแกรมจำพวก Identity Management นี้จะสร้างสภาวะที่โปรแกรมต่างๆ สามารถดึงข้อมูลผู้ใช้งานเสมือนกับเป็นฐานข้อมูลผู้ใช้งานของตนเองได้ ทำให้โปรแกรมหรือระบบต่างๆ สามารถทำงานได้เหมือนเดิม หรือในบางกรณีที่โปรแกรมนั้นๆ จำเป็นต้องใช้ฐานข้อมูลของโปรแกรมเท่านั้น Identity Managent จะทำการ Update ฐานข้อมูลของโปรแกรมนั้นๆ อัตโนมัติหากมีการเปลี่ยนแปลงข้อมูลบางอย่างในระบบที่เกี่ยวข้องกับโปรแกรม นอกจากนี้ Identity Management จะมีกลไกที่เอื้อสำหรับการบริหารจัดการผู้ใช้งานในระบบต่างๆ แบบควบคุมจากศูนย์กลางได้ โดยเป้าหมายของโปรแกรม Identity Management คือต้องการให้ผู้ใช้งานสามารถใช้รหัสผ่านเดียวกันในระบบหรือโปรแกรมต่างๆ

Directories และ LDAP

ในการทำงานของ Identity Management จำเป็นอย่างยิ่งที่จะต้องสร้างฐานข้อมูลผู้ใช้งานกลางขึ้น เพื่อใช้ในการ Update ฐานข้อมูลผู้ใช้งานของแต่ละระบบหรือแต่ละโปรแกรม ฐานข้อมูลผู้ใช้งานกลางนี้จะเก็บข้อมูลของผู้ใช้งานในระบบทั้งหมด ซึ่งฐานข้อมูลนี้มักเรียกกันในชื่อ “Directory” ซึ่ง Directory นี้จะสามารถ

เข้าถึงได้โดยใช้ LDAP (Lightweight Directory Access Protocol) ซึ่งเป็นมาตรฐานกลางในการเข้าถึง Directory ต่างๆ และสามารถ Query , Read และ Update ได้โดยผ่านโพรโตคอลนี้

Directory จะมีการทำงานในฐานะฐานข้อมูลผู้ใช้งานกลางในองค์กร ระบบและโปรแกรมต่างๆ สามารถดึงข้อมูลของ Identity ต่างๆ จาก Directory ในบางระบบหรือโปรแกรมจึงออกแบบมาให้รองรับการใช้งาน Directory โดยไม่มีฐานข้อมูลผู้ใช้งานของระบบหรือโปรแกรมนั้นๆ ซึ่งแนวโน้มของระบบหรือโปรแกรมจะเป็นไปในแนวทางนี้ ขณะเดียวกันถึงแม้ว่า LDAP จะเป็นโพรโตคอลมาตรฐานในการเข้าถึง Directory แต่ก็ไม่มีมาตรฐานใดที่กำหนดว่าโครงสร้างข้อมูลที่เก็บอยู่ใน Direcoty ควรมีลักษณะอย่างไร โดยทั่วไป ในการออกแบบโครงสร้างข้อมูลต่างๆ ที่เก็บอยู่ใน Directory นั้น จะขึ้นอยู่กับความต้องการของระบบหรือโปรแกรมต่างๆ และ ความต้องการข้อมูลของบุคลากรต่างๆ ในองค์กรด้วย

การ Log On เพื่อเข้าสู่ระบบ

สำหรับกระบวนการ Log On เพื่อเข้าสู่ระบบนั้น ระบบสามารถทำได้โดยการแสดงหน้าต่างสำหรับกรอก Username และ Password หากตรวจสอบแล้วข้อมูลทั้งสองตรงกันกับข้อมูลที่เก็บใน Directory หรือฐานข้อมูลผู้ใช้งานของระบบแล้ว แสดงว่าผู้ใช้งานนั้นเป็นผู้ใช้งานในระบบจริง และสิ้นสุดกระบวนการ Authentication เพื่อเพิ่มความปลอดภัยในการใช้งานระบบจึงมักมีการกำหนดนโยบายเกี่ยวกับการ Log On เช่น

- กำหนดให้ผู้ใช้งานต้องมีการเปลี่ยนรหัสผ่านเมื่อทำการ Log On ครั้งถัดไป
- กำหนดให้มีวันหมดอายุของรหัสผ่าน
- กำหนดระยะเวลาการใช้งานของรหัสผ่าน
- กำหนดความซับซ้อนของรหัสผ่าน
- กำหนดให้มีการจัดเก็บประวัติของรหัสผ่านเพื่อไม่ให้มีการตั้งรหัสผ่านซ้ำกับที่เคยใช้งาน
- กำหนดกระบวนการ Logout

เมื่อผู้ใช้งานเข้าใช้งานระบบจะมีการตรวจสอบตามนโยบายการรักษาความปลอดภัยดังกล่าว ถ้ารหัสผ่านหมดอายุระบบจะดำเนินการให้ผู้ใช้งานเปลี่ยนรหัสผ่าน ซึ่งรหัสผ่านใหม่ที่ได้ตั้งขึ้นนั้นจะต้องถูกตรวจสอบความซับซ้อนของรหัสผ่าน และประวัติของรหัสผ่าน หลังจากการเปลี่ยนรหัสผ่านเสร็จสมบูรณ์ จะมีการ update ข้อมูลประวัติของรหัสผ่าน สำหรับการใช้งาน Directory ในการเก็บข้อมูลรหัสผ่าน จะมีการกำหนดนโยบายเกี่ยวกับรหัสผ่านไว้ใน Directory และนำไปใช้สำหรับโปรแกรมต่างๆ ด้วยเพื่อความสะดวกในการบริหารจัดการ โดยนโยบายที่กำหนดใน Directory นั้นจะขึ้นอยู่กับบริษัทผู้ผลิตโปรแกรม Directory Service นั้นๆ

หากต้องการความปลอดภัยมากขึ้นในการ logon เข้าสู่ระบบ ผู้ดูแลระบบสามารถกำหนดให้ผู้ใช้งานระบบต้องใช้การ logon ด้วยกระบวนการอื่นๆ เช่น Certificate , SecureID , Biometric หรืออุปกรณ์อื่นๆ) ซึ่งการที่จะดำเนินการเช่นนี้ได้ ทุกๆ ระบบที่เกี่ยวข้องจะต้องรองรับกระบวนการ Logon ด้วยรูปแบบต่างๆ อย่างเท่าเทียมกันและควรจะมีกระบวนการ logon ที่ผู้ใช้งานมองเห็นเป็นกระบวนการเดียวกัน

การทำ Single Sign On

ในกรณีที่ผู้ใช้งานจำเป็นต้องเข้าใช้งานระบบต่างๆ มากกว่า 1 ระบบ จะเริ่มเกิดความยุ่งยากสำหรับผู้ใช้งานหากจำเป็นต้องจำชื่อผู้ใช้งานและรหัสผ่านของระบบต่างๆ ที่ตนเองมีสิทธิเข้าใช้งาน ซึ่งจะนำไปสู่ปัญหาการลืมรหัสผ่าน การตั้งรหัสผ่านที่คาดเดาได้ง่ายเกินไป หรือการจดรหัสผ่าน ซึ่งเป็นปัญหาความปลอดภัยในระบบเช่นกัน ในสถานการณ์เช่นนี้ผู้ดูแลระบบควรตั้งค่าระบบให้ผู้ใช้งานสามารถใช้ชื่อผู้ใช้งานและรหัสผ่านเพียงชุดเดียวในหลายๆ ระบบ หรือ Single Sign-On (SSO) โดยกระบวนการของ SSO นั้นจะเป็นการแยกส่วนของ Authentication / Authorization Component ออกจาก Application

สำหรับการสร้างระบบ Single Sign-On นั้นสามารถทำได้โดยใช้ผลิตภัณฑ์ต่างๆ ในท้องตลาด หรือ Open Source Project ซึ่งเจ้าของผลิตภัณฑ์ด้าน Identity Management ที่มีขนาดใหญ่ในท้องตลาดจะมีฟังก์ชั่นการทำ SSO อยู่แล้ว ซึ่งโดยทั่วไป Identity Management และ SSO Component ของผลิตภัณฑ์เดียวกันจะมีการใช้งาน Directory Service ร่วมกัน ซึ่ง Identity Management จะให้บริการการบูรณาการข้อมูลต่างๆ ใน Directory

นอกจากนี้ ผู้ใช้งานระบบอาจจำเป็นต้องมีการใช้งานข้อมูลข้ามองค์กร ซึ่งเป็นระบบการ Authentication / Authorization ที่ซับซ้อนมาก ผู้ใช้งานจากระบบหนึ่งขององค์กรหนึ่ง จะสามารถเข้าใช้งานอีกระบบหนึ่งในอีกองค์กรหนึ่ง ซึ่งในการสร้างระบบ SSO ให้สามารถทำ Authentication และ Authentication ข้ามองค์กรได้นั้นจำเป็นต้องมี Federation Service ในแต่ละระบบแล้วสร้าง Trust System ขึ้นระหว่างระบบ ปัจจุบันมีผลิตภัณฑ์ในท้องตลาดที่รองรับมาตรฐานการทำ Federation Service อยู่มากมาย แต่สามารถจัดกลุ่มได้เป็น 2 กลุ่มหลักคือ

1. กลุ่มผลิตภัณฑ์เกี่ยวกับการจัดการ Identity และ SSO ที่มีการเพิ่มเติมความสามารถการทำ Federation ในภายหลัง
2. กลุ่มผลิตภัณฑ์ที่ทำงานเกี่ยวกับการจัดการ Federation Service โดยเฉพาะ

กลุ่มผลิตภัณฑ์เกี่ยวกับการจัดการ Identity และ SSO ที่มีการเพิ่มเติมความสามารถ Federation

1. Oracle (Oracle Federated Identity Solution)
2. IBM (IBM Tivoli Federated Identity Manager)
3. Sun (Sun Java System Federation Manager)
4. CA (Ca eTrust SiteMinder Federation Security Services)
5. HP (HP OpenView Select Federation)

โดยผลิตภัณฑ์ทั้งหมดรองรับมาตรฐาน SAML 1.1 และ 2.0 นอกจากนี้ยังสนับสนุน WS-Federation และ มาตรฐานของ Liberty Alliance เช่นกัน สำหรับผลิตภัณฑ์ของ Microsoft นั้นมีการเพิ่ม Active Directory Federation Services ใน Windows 2003 Server ซึ่งมีการทำงานตามมาตรฐาน WS-* เช่น WS-Federation และ WS-Trust

กลุ่มผลิตภัณฑ์ที่ทำงานเกี่ยวกับการจัดการ Federation Service โดยเฉพาะ

ยกตัวอย่างเช่น PingFederation ของ Ping Identity และ Federated Access Manager ของ Symlabs ซึ่งสนับสนุนตามมาตรฐาน SAML 1.1 และ 2.0 , WS-Federation สามารถทำงานทั้ง Identity Provider และ Service Provider

นอกจากนี้ยังมีผลิตภัณฑ์ชื่อ Ping Trust ของ Ping Identity ที่มีการทำงานตาม WS-Trust เพื่อทำ security token service

นอกจากผลิตภัณฑ์ที่มีอยู่ในท้องตลาดทั้งสองกลุ่มแล้ว ยังมีซอฟต์แวร์ในกลุ่ม Open Source ที่สามารถทำงาน Federation Services ได้แก่

1. Shibboleth
2. OpenSAML
3. SourceID toolkits
4. Guanxi
5. OpenSSO

Shibboleth เป็นโปรเจคหนึ่งของ Internet2 networking consortium โดยการทำงานของ Shibboleth จะสามารถสร้าง Identity Provider และ Service Provider บนพื้นฐานของมาตรฐาน SAML 1.1 และ 2.0 นอกจากนี้ Shibboleth ยังมีซอฟต์แวร์เพิ่มเติมสำหรับการทำงานตามมาตรฐาน WS-Federation เพื่อรองรับการทำงานร่วมกับระบบ Active Diretory Federation Service (ADFS)

OpenSAML เป็นโปรเจคหนึ่งของ Internet2 networking consortium ซึ่งมีไลบรารีในภาษา Java และ C++ เพื่อการสื่อสารในมาตรฐาน SAML 1.1 และ 2.0

SourceID เป็นโปรเจคหนึ่งของ Ping Identity ที่ให้บริการการเชื่อมต่อตามมาตรฐาน SAML , ID-FF และ WS-Federation สำหรับ Platform ต่างๆ

Guanxi เป็นระบบการทำงานที่ให้บริการการเชื่อมต่อ SAML สำหรับ Java web application โดยรองรับการทำงานเป็น Identity Provider และ Service Provider Guanxi ทำให้ Java web application ต่างๆ สามารถเชื่อมต่อกับ Identity Provider อื่นๆ เช่น Shibboleth ได้ผ่าน SAML

OpenSSO เป็นผลิตภัณฑ์ที่พัฒนาโดยบริษัท Sun ที่มีการพัฒนาจาก Sun Java System Access Manager และ Sun Java Federation Manager เพื่อเป็นโครงสร้างการทำงานที่ทำให้เกิด Federation Service สำหรับ OpenSSO สามารถทำงานร่วมกับ Shibboleth และ ADFS ได้

สำหรับกรณีของระบบเครือข่าย การควบคุมการเข้าถึงระบบจะหมายถึงการคัดกรองข้อมูลในเครือข่ายว่าข้อมูลใดจะสามารถผ่านเข้าระบบได้ และข้อมูลใดไม่สามารถผ่านเข้าออกระบบได้ อุปรณ์ที่ใช้ในการคัดกรองข้อมูลดังกล่าวคือ “Firewall”

บทที่ 7. Firewall

ในบทที่ผ่านมา เราได้กล่าวถึงรายละเอียดวิธีการโจมตีทางเครือข่ายหลายวิธีการ สำหรับในบทนี้เราจะกล่าวถึงเครื่องมือหลักที่ถือได้ว่าเป็นทัพหน้าของเครื่องมือที่ใช้ในการป้องกันการโจมตี นั่นก็คือ ไฟร์วอลล์ เพราะไฟร์วอลล์นับเป็นเครื่องมือแรกที่เกิดขึ้นมาในโลกของ Security เป็นเครื่องมือที่พัฒนาไปมากที่สุด เป็นที่รู้จักกันมากที่สุด และเป็นเครื่องมือตัวแรกที่มักจะใส่เข้าไปในระบบเพื่อป้องกัน เพราะหากไม่มีไฟร์วอลล์ทำหน้าที่ป้องกันไว้ชั้นหนึ่งแล้ว เครื่องมืออย่าง IDS (Intrusion Detection System) อาจต้องรับภาระหนักขึ้น หรือต้องกลายเป็นเป้าในการโจมตีซะเอง

Firewall เป็นอุปกรณ์หรือซอฟต์แวร์ที่ทำหน้าที่ในการคัดกรองข้อมูลภายในเครือข่าย โดยตรวจสอบเพ็กเก็ตที่วิ่งผ่านไปมาในเครือข่าย ซึ่งเป็นองค์ประกอบในระบบสารสนเทศที่ทำหน้าที่ในการสร้าง Access Control สำหรับแพ็กเก็ตต่างๆ ในระบบเครือข่าย ไฟร์วอลล์นั้น หากจะกล่าวในมุมกว้าง ก็อาจกล่าวได้ว่าเป็น Smart Router เพราะไฟร์วอลล์จะต้องทำหน้าที่เป็นเราเตอร์ โดยทำหน้าที่เป็นเกตเวย์ของเครือข่ายที่มันป้องกันอยู่ ปัจจุบันไฟร์วอลล์ได้รับการพัฒนาไปมาก จนมีความสามารถพิเศษต่าง ๆ เพิ่มขึ้นมากมาย ซึ่งเราจะกล่าวในภายหลัง สำหรับในส่วนแรกนี้เราจะกล่าวถึงประเภทของไฟร์วอลล์ ซึ่งแบ่งออกเป็น 3 ประเภท ได้แก่ 1) Packet Filtering 2) Stateful Inspection และ 3) Application Proxy ว่ามีหลักการทำงานที่ต่างกันอย่างไร

Packet Filtering Firewall

ไฟร์วอลล์ชนิดนี้ เป็นไฟร์วอลล์ที่มีรูปแบบการทำงานง่ายที่สุด และเป็นไฟร์วอลล์ที่เก่าแก่ที่สุด ปัจจุบันไฟร์วอลล์ประเภทนี้แทบไม่มีการนำไปใช้งานจริง ๆ แล้ว ที่ยังมีใช้งานอยู่มักจะเป็นฟังก์ชั่นหนึ่งของเราเตอร์ โดยเราเตอร์ที่มีความสามารถนี้ นอกจากจะสามารถหาเส้นทางได้แล้ว ยังสามารถกรองแพ็กเกจได้อีกด้วย กล่าวคือ สามารถจะอนุญาตหรือไม่อนุญาตให้แพ็กเกจผ่านเราเตอร์ได้ โดยการกำหนดเป็นกฎขึ้นมา เช่น

```
router(config)#access-list 11 deny 161.246.20.0 0.0.0.255
router(config)#access-list 11 permit any
router(config)#interface fastethernet1
router(config-if)#ip access-group 11 in
```

คำสั่งข้างต้นเป็นคำสั่งที่ใช้ในการตั้งค่าให้กับเราเตอร์ของ Cisco ดังนั้นหากเป็นเราเตอร์ยี่ห้ออื่น รูปแบบคำสั่งอาจต่างออกไป แต่หลักการของการตั้งค่า จะยังคงเป็นหลักการเดียวกัน สำหรับคำสั่งข้างต้นนั้น บรรทัดแรกเป็นคำสั่งที่ใช้ในการกำหนด access-list หมายเลข 11 โดยกำหนดให้ปฏิเสธไอพีแอดเดรสหมายเลข 161.246.20.0 โดยให้ปฏิเสธทั้ง Class C เลย คือ จะหมายถึงไอพีหมายเลขตั้งแต่ 161.246.20.1-161.246.20.255 สำหรับบรรทัดถัดมาเป็นการกำหนดว่าจะตั้งค่าให้กับพอร์ต Fast Ethernet หมายเลข 1 และในบรรทัดสุดท้าย จะเป็นการกำหนดว่าให้นำ access-list ที่ได้กำหนดไว้ก่อนหน้านี้มาใช้กับพอร์ต Fast Ethernet 1 โดยให้ Filter เฉพาะฝั่ง inbound ซึ่งหมายถึง แพ็กเกจใด ๆ ที่มี Source IP Address อยู่ในช่วงดังกล่าวจะผ่านเราเตอร์นี้มาไม่ได้ แต่ยังสามารถส่งออกไปได้

รูปแบบข้างต้นเรียกว่าเป็น Standard ACL (Access Control List) แต่เราเตอร์ของ Cisco ยังมี ACL อีกรูปแบบหนึ่ง คือ Extend ACL ดังตัวอย่างต่อไปนี้

```
router(config)#access-list 110 deny tcp host 161.246.4.3 smtp
router(config)#access-list 110 deny tcp host 161.246.4.3 ftp
router(config)#access-list 110 permit tcp host any any
router(config)#interface fastethernet1
router(config-if)#ip access-group 110 in
```

จากคำสั่งข้างต้น บรรทัดแรก เป็นคำสั่งกำหนด Extend ACL หมายเลข 110 โดยกำหนดให้ห้ามการเชื่อมต่อชนิด TCP ที่มีหมายเลข IP เป็น 161.246.4.3 และมีหมายเลขพอร์ตเป็นพอร์ตของ SMTP (25) และ TCP (23) โดยกำหนดให้มีผลกับพอร์ต Fast Ethernet 1 สำหรับการเชื่อมต่ออื่น ๆ สามารถผ่านได้ ซึ่งจะเห็นได้ว่าการกำหนด Extend ACL เราสามารถจะกำหนดลงไปยังหมายเลขพอร์ตได้ ว่าจะอนุญาตหรือไม่อนุญาตการเชื่อมต่อไปยังพอร์ตใด ๆ ได้ ซึ่งทำให้เราสามารถกำหนดได้ว่าจะให้แอดเดรสหรือช่วงแอดเดรสใด ติดต่อกับแอปพลิเคชันแบบใดได้ ซึ่งจะเห็นได้ว่า การกำหนดในแบบ Extend ACL นี้ มีประโยชน์อย่างมาก นอกจากนั้น ยังสามารถกำหนดกฎในลักษณะเช่นนี้ได้อีกด้วย

```
router(config)#access-list 110 permit host 161.246.5.10 gt 1024 host –161.246.4.7 eq 80
router(config)#access-list 110 deny tcp host any any
router(config)#interface fastethernet1
router(config-if)#ip access-group 110 in
```

คำสั่งข้างต้นเป็นคำสั่งที่ให้เครื่องคอมพิวเตอร์ 161.246.5.10 เท่านั้นที่สามารถติดต่อกับ Web Server ที่มีหมายเลขไอพี 161.246.4.7 สำหรับเครื่องอื่น ๆ จะติดต่อไม่ได้ ซึ่งจะเห็นว่าเราสามารถตั้งค่าให้กับเราเตอร์ได้ค่อนข้างหลากหลายเงื่อนไข นอกจากนั้นแล้ว คำสั่งที่เป็น Extend ACL นี้ ยังสามารถกำหนดในบล็อก ICMP เช่น

```
router(config)#access-list 110 deny icmp any any echo-request
router(config)#access-list 110 permit tcp host any any
router(config)#interface fastethernet1
router(config-if)#ip access-group 110 in
```

ในการกำหนด Access List นั้น หากจะกำหนดให้ครบถ้วน มักจะต้องมีการป้องกันแอดเดรสต่อไปนี้ด้วย คือ แอดเดรสที่ใช้งานเป็นหมายเลข Private IP Address ซึ่งได้แก่หมายเลขแอดเดรสที่มีหมายเลข 10.0.0.0-10.255.255.255, 172.16.0.0-172.31.255.255 และ 192.168.0.0-192.168.255.255 เอาไว้ด้วย เพราะเนื่องจากหมายเลขเหล่านี้เป็นหมายเลขที่ใช้งานภายใน ดังนั้นหากปรากฏเป็นหมายเลขของ Source IP Address แล้ว ก็หมายความว่าแพ็กเกจนั้นมีการปลอมหมายเลข Source IP Address มา นอกจากนั้น ก็ควรจะมีการ Filter หมายเลข IP Address ที่เป็นหมายเลขขององค์กรไว้ด้วย เพราะการติดต่อเข้ามายังองค์กรนั้น ย่อมจะต้องไม่มีหมายเลข Source IP Address เป็นหมายเลขภายในองค์กรแน่ ๆ เช่น หากภาควิชาฯ จะป้องกันตามรูปแบบข้างต้น ก็จะสามารถสร้าง ACL ได้เป็น

```
router(config)#access-list 11 deny 10.0.0.0 0.255.255.255
router(config)#access-list 11 deny 127.0.0.0 0.255.255.255
router(config)#access-list 11 deny 172.16.0.0 0.0.255.255
```

```
router(config)#access-list 11 deny 192.168.0.0 0.0.255.255
router(config)#access-list 11 deny 161.246.4.0 0.0.0.255
router(config)#access-list 11 deny 161.246.5.0 0.0.0.255
router(config)#access-list 11 deny 161.246.6.0 0.0.0.255
router(config)#access-list 11 deny 161.246.70.0 0.0.0.255
router(config)#access-list 11 permit any
router(config)#interface fastethernet1
router(config-if)#ip access-group 11 in
```

Stateful Inspection Firewall

ในไฟร์วอลล์แบบ Packet filtering ที่ได้กล่าวมานั้น จะเห็นได้ว่าเราสามารถตั้งค่าเพื่อกรองแพ็กเกจที่ไม่ต้องการออกไป แต่ไฟร์วอลล์ดังกล่าวก็ยังไม่ปลอดภัยมากพอ เพราะแม้ว่าเราสามารถจำกัดการเชื่อมต่อให้เหลือแต่พอร์ต 80 เท่านั้นที่ติดต่อเข้ามาได้ แต่ไฟร์วอลล์ข้างต้นก็ไม่ได้ตรวจสอบว่า การเชื่อมต่อผ่านพอร์ต 80 นั้นเป็นการเชื่อมต่อตามปกติหรือไม่ คือ หากเป็นพอร์ต 80 แล้วก็จะปล่อยผ่านหมด ทั้งที่อาจเป็นแพ็กเกจโจมตีก็ได้ เพราะแฮกเกอร์อาจเทลเน็ตไปยังพอร์ต 80 เพื่อรันโปรแกรม Backdoor ก็ได้ นอกจากนั้นกรณีที่แพ็กเกจที่ผ่านไฟร์วอลล์มาเป็นแพ็กเกจที่มีการทำ Fragmentation มาด้วยแล้ว ไฟร์วอลล์ประเภทนี้จะไม่สามารถตรวจสอบอะไรได้เลย (เราเตอร์บางตัวสามารถกำหนดให้ไม่ส่งผ่านแพ็กเกจแบบ Fragment ได้)

และหากเป็นกรณีที่เป็นการโจมตีโดยการกำหนดแพ็กเกจที่ผิดปกติแล้ว ไฟร์วอลล์แบบนี้ก็จะไม่สามารถตรวจสอบได้เช่นกัน เพราะหากหมายเลขไอพีผ่าน และพอร์ตผ่าน ไฟร์วอลล์แบบ Packet filtering ก็ยอมให้ผ่านได้ทันที และหากมีการปลอมหมายเลขไอพีด้วยแล้ว ก็ยิ่งทำให้การป้องกันของไฟร์วอลล์มีความสามารถลดลง นอกจากนั้นสำหรับพอร์ตที่มีหมายเลขมากกว่า 1024 ไฟร์วอลล์ดังกล่าวจะต้องเปิดพอร์ตเหล่านั้นไว้ตลอดเวลา เพราะไฟร์วอลล์ไม่รู้ว่าแอปพลิเคชันใดจะใช้งานพอร์ตหมายเลขใดบ้าง ซึ่งถือเป็นความไม่ปลอดภัยอีกเช่นกัน

ซึ่งข้อบกพร่องทั้งหมดนี้ ไฟร์วอลล์แบบ Stateful Inspection สามารถป้องกันได้ (ต่อไปจะเรียกว่าสเตทฟูล) โดยไฟร์วอลล์ ก็จะมีการตั้งกฎขึ้นมาเช่นเดียวกัน แต่ไฟร์วอลล์ประเภทนี้จะมีความสามารถในการติดตาม

State ตามการเชื่อมต่อ โดยเฉพาะการเชื่อมต่อแบบ TCP ที่ได้อธิบายไปในบทก่อนหน้านี้ โดยในระหว่างการเชื่อมต่อไฟร์วอลล์จะทำการสร้าง State Table ที่จะเก็บสถานะของการเชื่อมต่อในทุกๆ การเชื่อมต่อเอาไว้ เช่น การเชื่อมต่อในแบบ TCP จะต้องเริ่มด้วย 3 Way Handshake ไฟร์วอลล์สเตทฟูลก็จะตรวจสอบว่าแพ็กเกจแรกเป็น SYN หรือไม่ และแพ็กเกจตอบกลับเป็น SYN/ACK หรือไม่ และแพ็กเกจยืนยันเป็น ACK หรือไม่ และแต่ละแพ็กเกจมีลำดับของ Sequence Number ถูกต้องหรือไม่ นอกจากในระหว่างการเชื่อมต่อไฟร์วอลล์สเตทฟูลยังมีการตรวจสอบหมายเลขลำดับ หมายเลขตอบรับและแฟล็กต่าง ๆ ตลอดเวลา ดังนั้นจะเห็นได้ว่าการสร้างแพ็กเกจแปลกปลอมให้ผ่านไฟร์วอลล์สเตทฟูลจะยากขึ้นมาก

สำหรับกรณีของแพ็กเกจที่มีการ Fragmentation มานั้น ไฟร์วอลล์สเตทฟูลจะรอจนครบทั้ง Datagram แล้วจึงทำการ Reassemble แล้วจึงตรวจสอบว่าถูกต้องหรือไม่ ดังนั้นการโจมตีโดยวิธีการแบ่งเป็น Fragment ย่อย ๆ เพื่อหลอกไฟร์วอลล์ก็จะทำได้ยากขึ้น และไฟร์วอลล์แบบสเตทฟูลไม่จำเป็นต้องเปิดพอร์ตหมายเลข 1024 ขึ้นไป ทิ้งเอาไว้ด้วย เพราะเมื่อไฟร์วอลล์สามารถติดตามสเตทได้แล้ว ก็ย่อมจะรู้ว่าการเชื่อมต่อนั้น ๆ ฝั่งไคลเอนต์มีการใช้งานพอร์ตใด ก็จะเปิดพอร์ตนั้น “เฉพาะ” สำหรับไคลเอนต์นั้น และเมื่อการเชื่อมต่อจบลง ก็จะปิดพอร์ตนั้นไว้เหมือนเดิม ทำให้ระบบมีความปลอดภัยเพิ่มขึ้นมาก

อย่างไรก็ตามไฟร์วอลล์แบบสเตทฟูลนั้น ไม่ได้ทำงานเหมือนกันไปหมด ไฟร์วอลล์สเตทฟูลบางตัวจะขยับไปทำงานที่ชั้นแอปพลิเคชันในบางโพรโตคอล เช่น ในโพรโตคอล FTP นั้นจะมีการใช้พอร์ต 2 พอร์ต คือ พอร์ต 21 ใช้งานเป็นพอร์ตควบคุม และพอร์ต 20 เป็นพอร์ตข้อมูล ดังนั้นในการทำงานแบบสเตทฟูลนั้น สมมติว่าในครั้งแรกเครื่องไคลเอนต์ 161.246.5.10 ติดต่อมายังพอร์ต 21 ของเซิร์ฟเวอร์ 161.246.4.3 โดยจะสุ่มค่าพอร์ตฝั่งไคลเอนต์มาด้วย เช่น 1234 ซึ่งไฟร์วอลล์ก็จะกำหนดใน State Table ว่า ไอพี 161.246.4.3 พอร์ต 21 กับไอพี 161.246.5.10 พอร์ต 1234 มีการเชื่อมต่อกัน ไฟร์วอลล์ก็จะเปิดพอร์ตทั้ง 2 เอาไว้ แต่เมื่อมีการส่งข้อมูลเครื่องไคลเอนต์กลับติดต่อมายังพอร์ต 20 ซึ่งไฟล์วอลล์ที่ไม่เข้าใจการทำงานของโพรโตคอล FTP ก็จะบล็อกข้อมูล ทำให้ไม่สามารถเชื่อมต่อได้

หรือในการส่งข้อมูลประเภทมัลติมีเดีย เช่น H.323 นั้น พอร์ตควบคุมกับพอร์ตที่ใช้ในการส่งข้อมูล ก็จะเป็นคนละพอร์ตเช่นเดียวกับ FTP และบางครั้งยังเป็นการใช้พอร์ต UDP อีกด้วย ดังนั้นหากไฟร์วอลล์ไม่มีการทำงานในชั้นแอปพลิเคชั้น หรือไม่เข้าใจโพรโตคอลนั้น ๆ แล้ว ก็จะใช้งานแอปพลิเคชันนั้น ๆ ไม่ได้ หรือหาก

ต้องการจะทำให้ได้ ก็จะต้องเปิดพอร์ตนั้นทิ้งเอาไว้ถาวร นอกจากนั้นในไฟร์วอลล์หลายตัว จะมีการติดตามสถานะการทำงานของ HTTP เป็นพิเศษ เพราะเป็นที่ทราบกันดีว่าข้อมูลในโลกนี้ มีบทบาทของ HTTP อยู่ไม่น้อย และมีการโจมตีผ่านทางเว็บมาก ดังนั้นการติดตามสถานะของ HTTP ก็จะทำให้ระบบเครือข่ายมีความปลอดภัยมากขึ้น

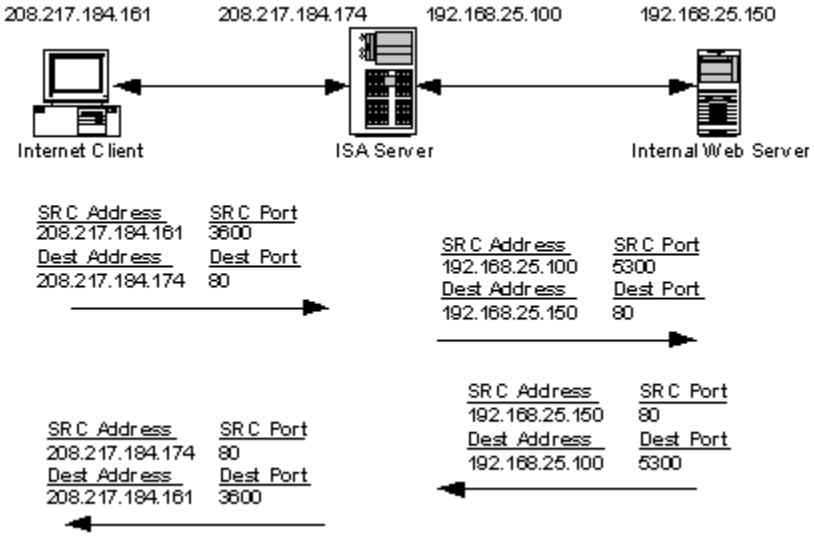
แต่แม้ว่าไฟร์วอลล์แบบสเตทฟูลจะมีความปลอดภัยเพิ่มขึ้นมากแล้วก็ตาม ไฟร์วอลล์ประเภทนี้ยังไม่สามารถป้องกันการโจมตีที่แทรกซึมมากับการเชื่อมต่อตามปกติได้ เช่น โพรโตคอล FTP นั้น แม้ว่าไฟร์วอลล์แบบสเตทฟูลจะมีการติดตามให้มีการเปิดพอร์ต 20 และ 21 อย่างถูกต้อง แต่หากมีการส่งข้อมูลอื่น ๆ ที่ไม่ใช่ข้อมูล FTP แทรกมาในระหว่างการเชื่อมต่อ ไฟร์วอลล์ประเภทนี้ก็จะไม่รู้ ดังนั้นหากต้องการให้ไฟร์วอลล์มีความสามารถในการติดตามการทำงานของชั้นแอปพลิเคชันมากขึ้น โดยทราบว่าการติดต่อเป็นการติดต่อตามรูปแบบของโพรโตคอลนั้น ๆ อย่างถูกต้องหรือไม่ ไฟร์วอลล์นั้นจะต้องก้าวขึ้นไปทำงานในชั้นแอปพลิเคชัน โดยจะเรียกไฟร์วอลล์ชนิดนี้ว่า Application Proxy Firewall

Application Proxy Firewall

ไฟร์วอลล์ประเภทนี้ จะทำงานในระดับชั้นแอปพลิเคชันเป็นสำคัญ โดยไฟร์วอลล์ประเภทนี้จะทำหน้าที่เป็นตัวแทน (Proxy) ในการส่งต่อ การเชื่อมต่อใด ๆ ไปยังเซิร์ฟเวอร์ เช่น เมื่อไคลเอนต์ 161.246.5.10 ติดต่อไปยังเว็บเซิร์ฟเวอร์ 161.246.4.7 ผ่านทางไฟร์วอลล์ 161.246.5.1 ไฟร์วอลล์จะทำหน้าที่รับแพ็กเกจที่ขอเชื่อมต่อจาก 161.246.5.10 เอาไว้ จากนั้นก็ถอดแพ็กเกจเดิมออก แล้วสร้างแพ็กเกจใหม่ โดยอาศัยข้อมูลร้องขอเดิม ไปยัง 161.246.4.7 เสมือนกับว่าไฟร์วอลล์เป็นผู้ร้องขอเอง ดังนั้นข้อดีประการแรกของไฟร์วอลล์ประเภทนี้ คือ บุคคลภายนอกจะไม่รู้หมายเลขไอพีของเครือข่ายภายในที่ขอเชื่อมต่อออกมาภายนอก และเมื่อเว็บเซิร์ฟเวอร์ตอบกลับ มันก็จะส่งผลลัพธ์กลับไปยังเครื่อง 161.246.5.10

และโดยการที่มันทำหน้าที่เป็นตัวแทนในการเชื่อมต่อนี่เอง ทำให้การติดต่อผ่านไฟร์วอลล์ทุกครั้ง ไฟร์วอลล์ก็จะทำหน้าที่ในการตรวจสอบรูปแบบการติดต่อ ว่ามีรูปแบบที่ถูกต้องตามโพรโตคอลนั้น ๆ หรือไม่ ทำให้มีความปลอดภัยเพิ่มขึ้น นอกจากนั้นไฟร์วอลล์แบบนี้ยังป้องกันการปลอมไอพีได้โดยเด็ดขาด เพราะมันจะทำหน้าที่ในการส่งต่อเสียเอง แต่การติดต่อแบบนี้ก็มีข้อเสียเช่นกัน โดยข้อเสียแรก คือ ไฟร์วอลล์แบบนี้จะ

ทำงานได้ช้ากว่า เพราะมีการตรวจสอบมากกว่า และยังต้องสร้างแพ็กเกจใหม่ในทุก ๆ ครั้งด้วย และหากกรณีที่ในการเชื่อมต่อหนึ่งมีการแบ่งเป็น Segment หลาย ๆ Segment ด้วยแล้ว ไฟร์วอลล์ประเภทนี้ต้องรอให้ทุก Segment ส่งมาจนครบก่อน จึงจะส่งต่อได้ ทำให้เกิดความล่าช้าในการทำงานขึ้น



รูปที่ 34 ตัวอย่าง Application Proxy Firewall

นอกจากนั้นการที่ไฟร์วอลล์ประเภทนี้ทำงานในระดับชั้นแอปพลิเคชัน หมายความว่า มันจะส่งต่อได้เฉพาะโพรโตคอลที่มันรู้จักเท่านั้น หากโพรโตคอลใดที่มันไม่รู้จัก ก็จะไม่สามารถส่งต่อได้เลย ในขณะที่หากเป็นไฟร์วอลล์แบบสเตทฟูลแล้ว เราสามารถตั้งค่าให้เปิดพอร์ตต่าง ๆ ทำให้สามารถเชื่อมต่อได้ แต่ไฟร์วอลลแบบ Application Proxy จะไม่สามารถติดต่อได้เลย หากไฟร์วอลล์ไม่รู้จักกับโพรโตคอลนั้น

และจากข้อดีของไฟร์วอลลแบบสเตทฟูล ที่มีความรวดเร็วในการทำงาน และข้อดีของไฟร์วอลล์แบบ Application Proxy ที่มีความปลอดภัยสูง จึงทำให้มีผู้สร้างไฟร์วอลล์ที่ผสมผสานความสามารถของไฟร์วอลล์ทั้งสองขึ้น และเรียกไฟร์วอลล์แบบใหม่นี้ว่า Hybrid Firewall หรือบางผู้ผลิตจะเรียกว่า Adaptive Firewall โดยไฟร์วอลล์แบบใหม่นี้ จะแตกต่างกันไปตามผู้ผลิต บางผลิตภัณฑ์ก็ทำงานในแบบ Proxy สำหรับโพรโตคอลหลัก ๆ และแบบสเตทฟูลสำหรับโพรโตคอลทั่ว ๆ ไป บางผลิตภัณฑ์ก็ทำงานในแบบ Proxy ในช่วงแรกของการ

เชื่อมต่อ เพราะมีความปลอดภัยสูง และต่อมาหากเชื่อว่าการเชื่อมต่อนั้น เป็นการเชื่อมต่อตามปกติ ก็จะขยับลงมาทำงานในแบบสเตทฟูล เพราะมีความรวดเร็วในการทำงานมากกว่า

ไฟร์วอลล์ในปัจจุบันมีการพัฒนาไปมาก จนอาจกล่าวได้ว่าไม่มีผลิตภัณฑ์ไฟร์วอลล์ใด ที่เป็นแบบใดแบบหนึ่ง นอกจากนั้นผลิตภัณฑ์ไฟร์วอลลหลาย ๆ ตัวก็มักจะมีการทำงานร่วมกับแอปพลิเคชันด้านความปลอดภัยอื่น ๆ เช่น ทำงานร่วมกับ Antivirus ทำให้ไฟร์วอลล์ส่งข้อมูลของเมล์ไปตรวจสอบไวรัสก่อนจะส่งต่อ หรือทำงานร่วมกับ IDS เพื่อตรวจสอบการบุกรุก ไฟร์วอลล์บางตัวสามารถตั้งให้ทำงานตามเวลา ตามผู้ใช้ บางตัวสามารถกำหนดทราฟฟิกให้กับแอปพลิเคชันไม่เท่ากันได้ด้วย ไฟร์วอลล์บางตัวสามารถล็อกการใช้งานของผู้ใช้ให้สามารถเชื่อมต่อกับไซต์ที่กำหนดไว้เท่านั้นได้

แนวทางการออกแบบ

เป้าหมายหลักของการออกแบบโครงสร้างความปลอดภัย ก็เพื่อที่จะปกป้องทรัพย์สินขององค์กร ให้สามารถใช้งานได้ โดยที่ไม่มีใครสามารถมาโจมตีได้ ซึ่งแนวทางในการออกแบบจะประกอบด้วย 4 ขั้นตอน คือ ออกแบบระบบ (Design) สร้างระบบ (Deploy) นำไปใช้งานใช้งาน (Manage) และประเมินผล (Assess) โดยขั้นตอนทั้ง 4 จะมีลักษณะเป็นงานที่ต่อเนื่องไปเรื่อย ๆ ไม่รู้จบ ทั้งนี้เพราะการออกแบบระบบนั้นหลังจากนำไปใช้งาน อาจไม่เหมาะสมกับการใช้งาน เช่น อาจทำให้ระบบปลอดภัยจริง แต่ทำให้ผู้ใช้ไม่สะดวกต่อการใช้งาน อย่างนี้ก็ต้องปรับการออกแบบใหม่ หรืออาจสะดวกต่อการใช้งาน แต่เมื่อประเมินแล้ว มีความปลอดภัยไม่เพียงพอ ดังนั้นจึงต้องมีการปรับจนกว่าจะลงตัว นอกจากนั้นก็ยังจะต้องมีการตรวจประเมินเป็นระยะ ๆ ดังนั้นคงไม่ผิดนัก หากจะกล่าวว่า วงจรความปลอดภัยข้างต้นเป็นเรื่องที่ต้องทำไปเรื่อย ๆ ตราบเท่าที่องค์กรนั้นยังคงอยู่

นอกจากนั้นการออกแบบนั้นควรจะต้องเป็นไปตาม Policy และแนวทางขององค์กร แต่หากองค์กรใดยังไม่มี Policy ก็จะต้องออกแบบและสร้างขึ้นก่อนที่จะสร้างโครงสร้างความปลอดภัย

การแบ่งเครือข่าย

การแบ่งเครือข่าย หรือ Network Partition นี้ ถือเป็นขั้นตอนแรกของการออกแบบ โดยก่อนที่จะทำงานในขั้นตอนนี้กัน เราจะต้องมีผังของระบบคอมพิวเตอร์ และผังของระบบเครือข่ายขององค์กรก่อน สำหรับจุดประสงค์ของการแบ่งเครือข่ายนี้ ก็เพื่อจะจัดระดับความสำคัญของเครือข่ายในแต่ละส่วน ซึ่งโดยทั่วไปก็จะถือว่าเครือข่ายที่เครื่องเซิร์ฟเวอร์อยู่ มีความสำคัญสูงที่สุด และเครือข่ายที่เครื่องไคลเอนต์อยู่ ก็มีความสำคัญรองลงมา โดยเครื่องของผู้บริหารอาจจะจัดให้มีความสำคัญมากกว่าเครื่องของพนักงานก็ว่ากันไป

คราวนี้เมื่อได้ระดับความสำคัญต่าง ๆ ของระบบเครือข่ายแล้ว ก็จะหาทางปกป้องเครือข่ายต่อไป โดยยึดหลักที่ว่าส่วนของเครือข่ายที่สำคัญมาก็ต้องปกป้องมาก ส่วนของเครือข่ายที่สำคัญน้อยก็ป้องน้อยหน่อย แต่โดยทั่ว ๆ ไปแล้ว จะแบ่งส่วนของเครือข่ายออกเป็น 3 ส่วนหลัก ๆ คือ ส่วนของเครือข่ายที่มีเซิร์ฟเวอร์ที่ไม่ได้ติดต่อกับภายนอกเป็นส่วนหนึ่ง ส่วนของเครือข่ายที่มีเซิร์ฟเวอร์ที่ต้องติดต่อกับภายนอกเป็นอีกส่วนหนึ่ง และอีกส่วนหนึ่งก็คือส่วนของผู้ใช้

สำหรับเหตุผลของการแบ่งเครือข่ายในส่วนของเซิร์ฟเวอร์ออกเป็น 2 ส่วน ก็เนื่องจากเซิร์ฟเวอร์ที่ทำหน้าที่ติดต่อกับภายนอก อย่างเช่น เว็บเซิร์ฟเวอร์ภายนอก หรือ เมล์เซิร์ฟเวอร์นั้น เป็นเซิร์ฟเวอร์ที่จะต้องติดต่อกับข้างนอก หรือเรียกว่า “เข้าถึงได้” จากภายนอก อย่างหลีกเลี่ยงไม่ได้ ซึ่งการป้องกันก็จะไม่สามารถทำได้อย่างเต็มที่ ประกอบกับการที่เซิร์ฟเวอร์เหล่านี้ เข้าถึงหรือเห็นได้จากภายนอก ทำให้มันกลายเป็นเป้าโจมตี และมีความเสี่ยงที่จะถูกเจาะเข้ามาได้ ในขณะที่เซิร์ฟเวอร์อย่างเซิร์ฟเวอร์ฐานข้อมูลนั้น ไม่จำเป็นต้องติดต่อกับภายนอก และไม่จำเป็นต้องให้ “เข้าถึงได้” จากภายนอก หรือพูดง่าย ๆ คือ ไม่ควรจะมองเห็นจากภายนอก เซิร์ฟเวอร์ในกลุ่มนี้จึงมีความเสี่ยงน้อยกว่า ดังนั้นหากนำเซิร์ฟเวอร์ 2 กลุ่มนี้ไปไว้ด้วยกันแล้ว เมื่อมีการเจาะเข้ามาได้จากเซิร์ฟเวอร์กลุ่มแรก ก็อาจจะสูญเสียเซิร์ฟเวอร์ทั้งหมด แต่หากมีการแบ่งเป็น 2 กลุ่ม เมื่อเซิร์ฟเวอร์กลุ่มแรกถูกเจาะเข้ามาได้ เซิร์ฟเวอร์ในกลุ่มที่ 2 ก็ยังจะมีความปลอดภัยต่อไป จนกว่าแฮกเกอร์จะเจาะเข้ามาในเซิร์ฟเวอร์กลุ่มหลังได้สำเร็จ ซึ่งจะเจาะได้ยากกว่ามาก เพราะการที่มันไม่ต้องติดต่อกับภายนอกทำให้เราสามารถป้องกันเครือข่ายส่วนนี้ได้อย่างเต็มที่มากกว่า

อย่างไรก็ตาม ในองค์กรที่มีขนาดไม่ใหญ่นัก อาจมีการแบ่งเครือข่ายออกเป็นเพียง 2 กลุ่ม คือจะรวมเอาส่วนของเครือข่ายที่เป็นเซิร์ฟเวอร์ภายในกับเครือข่ายของผู้ใช้เข้าด้วยกัน เพราะอันที่จริงเหตุผลที่เขาแยกส่วน

ของเครือข่ายผู้ใช้ออกจากส่วนของเครือข่ายเซิร์ฟเวอร์ภายในนั้น ก็เพราะไม่ไว้ใจผู้ใช้ภายในว่าอาจทำอันตรายเซิร์ฟเวอร์ได้ แต่ในองค์กรขนาดเล็ก ที่สามารถไว้ใจผู้ใช้ได้ หรือสามารถควบคุมผู้ใช้โดยวิธีการอื่นได้ ก็อาจรวมเอาเครือข่าย 2 ส่วนนี้เข้าด้วยกันได้ เพื่อเป็นการประหยัดค่าใช้จ่าย

รูปที่ 35 การแบ่งเครื่องคอมพิวเตอร์ในเครือข่ายออกเป็น 3 ส่วน

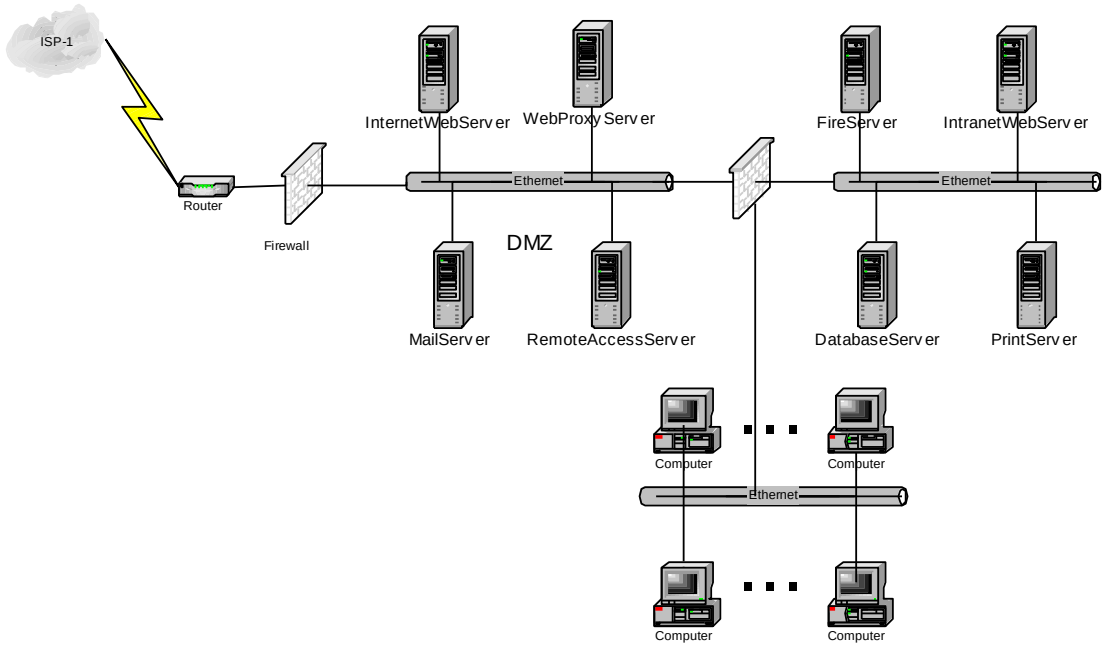
หลังจากที่เราแบ่งเครือข่ายแล้ว จะมีศัพท์อยู่คำหนึ่งที่มักพูดถึงกันในวงการรักษาความปลอดภัย นั่นก็คือ ศัพท์คำว่า Trust ซึ่งภาษาไทย ก็น่าจะแปลว่าความเชื่อถือ คำนี้มีความหมายว่าเราจะเชื่อถือเครื่องคอมพิวเตอร์เครื่องนั้นได้มากน้อยเพียงใด ว่าในระหว่างที่ติดต่อกันนั้น จะไม่เป็นอันตรายต่อเรา ซึ่งโดยทั่วไป ก็มักจะให้คอมพิวเตอร์กลุ่มที่ 2 มีความน่าเชื่อถือสูงที่สุด เพราะดูแลโดยผู้ดูแลระบบเอง จากนั้นก็ตามมาด้วยคอมพิวเตอร์ในกลุ่มที่ 1 หรือกลุ่มที่ 3 ขึ้นอยู่กับว่าองค์กรนั้นเป็นลักษณะใด อย่างองค์กรของผมเป็นสถานศึกษา ผมก็จะเชื่อว่าคอมพิวเตอร์กลุ่มที่ 1 น่าเชื่อถือกว่า เพราะถึงแม้จะมีความเสี่ยงอันเนื่องมาจากการต้องติดต่อกับภายนอก แต่ก็ยังเป็นเครื่องที่ดูแลเอง แต่ผมไม่สามารถเชื่อในตัวนักศึกษาได้เลย ว่าจะไม่พยายามทำอันตรายต่อองค์กร ทั้งนี้เพราะนักศึกษามักจะมีนิสัยชอบทดลอง แต่หากเป็นองค์กรที่ผู้ใช้ค่อนข้างจะธรรมดา ไม่ค่อยมีคน

เก่งคอมพิวเตอร์ ก็อาจวางใจได้ว่า ผู้ใช้ไม่มีศักยภาพพอที่จะทำอันตรายต่อระบบในองค์กรได้ ในกรณีก็อาจเชื่อคอมพิวเตอร์ในกลุ่มที่ 3 มากกว่า สำหรับเครือข่ายที่ไม่น่าเชื่อถือเลย ก็คือเครือข่ายภายนอกองค์กร

การแบ่งเครือข่ายโดยใช้ไฟร์วอลล์

เมื่อเราจัดกลุ่มเครื่องคอมพิวเตอร์เรียบร้อย พร้อมทั้งจัดอันดับความน่าเชื่อถือแล้ว เราก็จะมาหาทางแบ่งกลุ่มคอมพิวเตอร์เหล่านั้นออกจากกัน โดยเป้าหมายของการแบ่งก็คือ ให้เครือข่ายส่วนต่าง ๆ สามารถติดต่อใช้งานกันได้ตามปกติ แต่ไม่อนุญาตให้การใช้งานที่ผิดปกติผ่านเข้าไปได้ ซึ่งตรงนี้เราจะต้องกำหนดกฎการเข้าออก (Rule) โดยกฎที่กำหนดนี้ก็จะเป็นแนวทางที่ตั้งร่วมกันว่าจะอนุญาตหรือไม่อนุญาตการสื่อสารประเภทใดบ้าง ที่ข้ามระหว่างเครือข่ายแต่ละส่วนที่ได้แบ่งออกจากกัน

สำหรับการนำไฟร์วอลล์มาใช้ ก็จะนำมาตั้งในตำแหน่งที่แบ่งเครือข่ายแต่ละส่วนออกจากกัน อย่างเครือข่ายตัวอย่างของผม ซึ่งแบ่งออกเป็น 3 ส่วน ก็สามารถออกแบบได้ 2 วิธี โดยวิธีแรกจะใช้ไฟร์วอลล์ 2 ตัว โดยไฟร์วอลล์ตัวแรก จะทำหน้าที่กั้นระหว่างเครือข่ายภายนอกกับองค์กร และไฟร์วอลล์ตัวที่ 2 จะทำหน้าที่กั้นระหว่างเครือข่ายกลุ่มที่ 1 กลุ่มที่ 2 และกลุ่มที่ 3 โดยจะได้โครงสร้างตามรูปที่ 36 วิธีการออกแบบลักษณะนี้จะเรียกว่า Screening Subnet หรือบางทีก็เรียกว่า Three Homed Computer



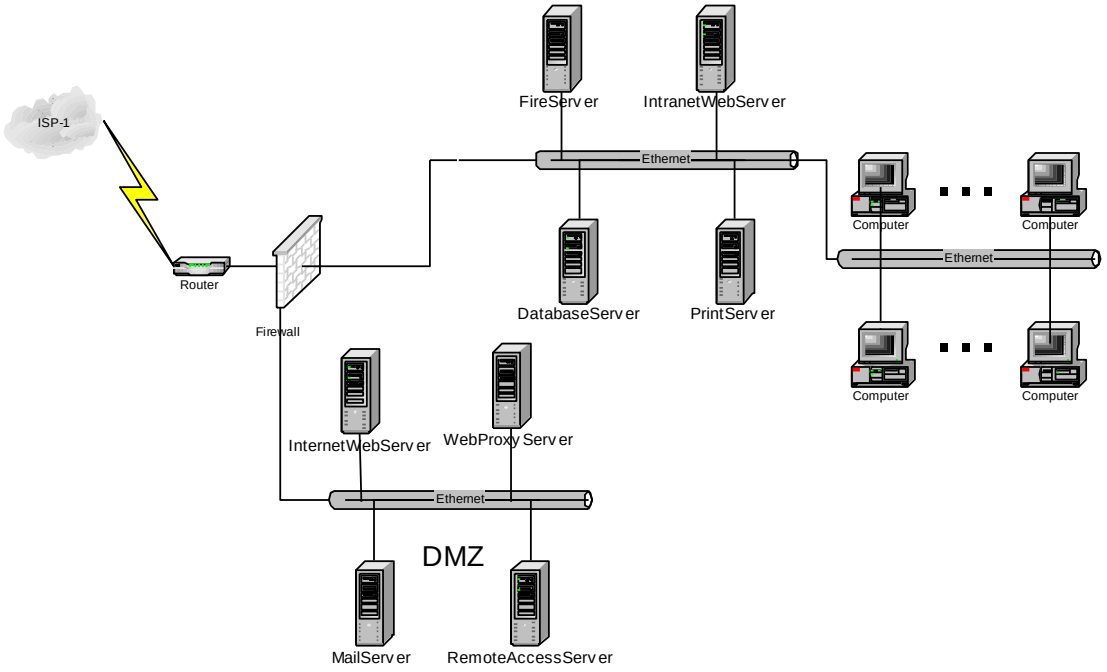
รูปที่ 36 การแบ่งเครือข่ายด้วยไฟล์วอลล์ 2 ตัว

สำหรับเหตุผลของการออกแบบข้างต้นนั้น ไฟร์วอลล์ตัวแรกนั้นคงไม่มีปัญหาอะไร คือ เห็นได้ชัดเจนว่าทำหน้าที่ในการกั้นระหว่างเครือข่ายที่เชื่อถือไม่ได้เลย คือ เครือข่ายอินเตอร์เน็ตกับเครือข่ายภายในองค์กร สำหรับไฟล์วอลล์ตัวที่ 2 นั้นจะมี 3 ขา โดยจะทำหน้าที่กั้นระหว่างเครือข่ายภายในทั้ง 3 โดยเครือข่ายกลุ่มที่ 1 ที่ต้องเชื่อมต่อกับอินเตอร์เน็ตนั้น จะอยู่นอกสุด คือ มีไฟร์วอลล์กั้นเพียงตัวเดียว เครือข่ายส่วนนี้ จะมีชื่อเรียกอีกอย่างว่า DMZ หรือ De-Militarize Zone ซึ่งหากจะแปลก็น่าจะแปลได้ว่า เขตปลอดทหาร ทั้งนี้ก็เนื่องจากว่าส่วนนี้จะเสมือนกับเป็นเขตชายแดน หรือเขตกันชนระหว่างเครือข่ายอินเตอร์เน็ตกับเครือข่ายภายใน ซึ่งจะมีการควบคุมเข้มงวดน้อยกว่าส่วนของเครือข่ายภายใน

เขต DMZ นี้เป็นเขตที่เราถือว่าเป็นเขตที่มีความปลอดภัยน้อย เพราะการตั้งกฎที่ไฟร์วอลล์ตัวนอก จะไม่สามารถตั้งอย่างเข้มงวดได้ เนื่องจากต้องติดต่อกับเครือข่ายอินเตอร์เน็ต ประกอบกับเป็นเครือข่ายที่คนข้างนอกสามารถมองเห็น และสามารถเป็นเป้าของการโจมตีได้ ซึ่งหากผู้ดูแลระบบดูแลระบบไม่ดีพอ หากเจอกับแฮกเกอร์ที่เก่ง ๆ ก็อาจทำให้สูญเสียเซิร์ฟเวอร์ตัวใดตัวหนึ่งไปได้

สำหรับเขตที่อยู่ภายในเครือข่ายถัดมา จะเป็นเครือข่ายที่ปลอดภัยมากกว่า เพราะมีไฟร์วอลล์กั้นอยู่อีกชั้นหนึ่ง และเครือข่ายส่วนนี้จะใช้กฎที่เข้มงวดมากกว่า จนกระทั่งไม่สามารถมองเห็นได้จากภายนอก เพราะหากคนในองค์กรจะส่งเมล์ ก็จะติดต่อกับเมล์เซิร์ฟเวอร์ใน DMZ หรือหากคนในองค์กรต้องการเล่นเว็บก็ต้องผ่านทาง Web Proxy ที่อยู่ใน DMZ เช่นเดียวกัน หรือแม้กระทั่งใน DMZ เองก็ยังไม่สามารถมองเห็นเครือข่ายภายในได้ตลอดเวลา โดยจะเห็นเฉพาะที่มีการเชื่อมต่อเท่านั้น ซึ่งตรงนี้จะอธิบายอีกครั้งในเรื่องชนิดของไฟร์วอลล์ ดังนั้นเครือข่ายภายในจะมีความปลอดภัยสูงมาก

นอกจากนั้นไฟร์วอลล์ตัวในก็ยังทำหน้าที่ในการกั้นระหว่างเครือข่ายของผู้ใช้กับเครือข่ายของเซิร์ฟเวอร์ภายใน ซึ่งจะทำให้เครือข่ายของเซิร์ฟเวอร์มีความปลอดภัยจากการกระทำของผู้ใช้มากขึ้น เพราะได้มีการสำรวจพบในอเมริกาว่ามากกว่าครึ่งของความไม่ปลอดภัย มักเกิดจากคนในมากกว่าคนนอก แต่นั่นก็เป็นสภาพแวดล้อมในอเมริกา สภาพแวดล้อมในประเทศไทยก็อาจต่างออกไปได้ บางองค์กรที่ผู้ใช้ค่อนข้างจะรู้คอมพิวเตอร์มาก ก็อาจจะออกแบบอย่างในรูปข้างต้น แต่ในบางองค์กรที่ผู้ใช้สามารถเชื่อใจได้ หรือองค์กรที่ผู้ใช้ไม่มีความรู้ด้านคอมพิวเตอร์มากนัก ก็อาจจะรวมเอาเครือข่ายผู้ใช้กับเครือข่ายของเซิร์ฟเวอร์ภายในเข้าด้วยกันได้ ซึ่งจะเป็นผลให้สามารถลดไฟร์วอลล์ลงได้ 1 ตัว โดยจะได้เครือข่ายที่มีรูปแบบตามรูปที่ 37



รูปที่ 37 การแบ่งเครือข่ายด้วยไฟล์วอลล์เพียงตัวเดียว

อย่างไรก็ตามในการกั้นระหว่างเครือข่ายของเซิร์ฟเวอร์ภายในกับผู้ใช้นั้น ตามในรูปที่ 2 นั้น ในการนำไปใช้งานจริง จะค่อนข้างมีความยุ่งยากอยู่บ้าง ทั้งนี้เพราะการสื่อสารระหว่างผู้ใช้กับเซิร์ฟเวอร์ภายในบางครั้งก็มีความซับซ้อน โดยเฉพาะกับองค์กรที่ใช้ไมโครซอฟต์วินโดว์ และใช้งานในระบบของโดเมน ทั้งนี้เพราะในการสื่อสารระหว่างเครื่องที่เป็นสมาชิกของโดเมน และเครื่องโดเมนคอนโทรลเลอร์นั้น จะมีการติดต่อที่ซับซ้อน ผ่านทางพอร์ตหลายพอร์ต ดังนั้นในการใช้งานอาจมีปัญหาในเรื่องของการติดต่อกันไม่ได้เกิดขึ้นได้ อย่างไรก็ตามหากมีการปรับแต่งกฎของไฟร์วอลล์ให้เหมาะสมแล้ว ก็ยังสามารถใช้งานในรูปแบบนี้ได้

จะเห็นว่าเครือข่ายจะแบ่งออกเป็นเพียง 3 ส่วน คือ เครือข่ายภายนอกองค์กร เครือข่าย DMZ และเครือข่ายภายในองค์กร ซึ่งรวมเอาเซิร์ฟเวอร์ภายในและเครื่องไคลเอนต์เข้าไว้ด้วยกัน รูปแบบนี้จัดว่าเป็นรูปแบบที่ประหยัด เพราะใช้ไฟร์วอลล์เพียงตัวเดียว แม้จะมีความเสี่ยงมากกว่าแบบที่ใช้ไฟร์วอลล์ 2 ตัวก็ตาม แต่หากเลือกใช้ไฟร์วอลล์ที่ดีหน่อย และมีการดูแลรักษาอย่างเคร่งครัด และถือได้ว่ามีความปลอดภัยที่เทียบเท่าได้กับไฟร์วอลล์ 2 ตัวเลยทีเดียว วิธีการออกแบบนี้จะเรียกว่า Screening Router หรือ Dual Homed Computer

และในทำนองเดียวกัน หากต้องการความปลอดภัยมากขึ้นไปอีก ก็สามารถทำได้ โดยการเพิ่มไฟร์วอลล์ขึ้นอีกตัวหนึ่ง เพื่อกั้นระหว่างเครือข่ายภายในและเครือข่ายของเซิร์ฟเวอร์ภายในองค์กร ซึ่งก็จะกลายเป็นไฟร์วอลล์ 3 ชั้น ซึ่งบางคนอาจจะบอกว่า โอเวอร์ไปหรือเปล่า ก็ต้องขอตอบว่าในเรื่องของความปลอดภัยแล้ว ไม่มีคำว่า โอเวอร์ หรอกครับ เพราะยิ่งเราป้องกันมากขึ้น ความปลอดภัยก็ยิ่งเพิ่มมากขึ้น แต่ก็ต้องแลกกับค่าใช้จ่ายที่ต้องเสียเพิ่มขึ้นด้วย บางองค์กรมีการใช้ไฟร์วอลล์ตั้ง 7-8 ชั้นก็ยังมีเลย เพราะเขาต้องการความมั่นใจจนถึงที่สุดว่าเครือข่ายของเขาจะปลอดภัยมากที่สุดเท่าที่จะทำได้ ไม่ว่าจะเสียค่าใช้จ่ายมากแค่ไหนก็ตาม อย่างเช่น ธุรกิจธนาคารที่มีมูลค่าธุรกิจนับแสนล้านบาทเป็นเดิมพันนี่คงเรียกว่าโอเวอร์ไม่ได้เหมือนกัน

สำหรับความแตกต่างของการมีไฟร์วอลล์มากชั้น กับไฟร์วอลล์น้อยชั้นนั้น จะไม่แตกต่างกันในแง่ของความปลอดภัย หากไฟร์วอลล์ไม่ถูกเจาะซะเอง แต่หากเมื่อไรก็ตามที่ไฟร์วอลล์ถูกเจาะสำเร็จแล้ว ไฟร์วอลล์ที่มีจำนวนชั้นมากกว่า ก็จะมีความปลอดภัยมากกว่าอย่างแน่นอน เพราะอย่างน้อยแฮกเกอร์ก็จะต้องเสียเวลาเจาะไฟร์วอลล์ตัวถัดไปเพิ่มขึ้น ทั้งนี้แม้ว่าไฟร์วอลล์จะเป็นซอฟต์แวร์เพื่อความปลอดภัย ที่ตัวมันเองจะต้องมีความปลอดภัยสูง ซึ่งที่ผ่านมาไฟร์วอลล์แต่ละยี่ห้อก็รักษาชื่อเสียงด้านนี้ได้เป็นอย่างดี

แต่อย่างไรเสียไฟร์วอลล์ก็เป็นซอฟต์แวร์ตัวหนึ่ง ที่อาจจะมีข้อบกพร่องหรือจุดโหว่ได้เช่นเดียวกัน แม้ว่าจะมีน้อยกว่า เพราะมีการตรวจสอบกันอย่างเข้มงวดมาก จนถึงปัจจุบันก็อาจกล่าวได้ว่าไฟร์วอลล์ชื่อดังส่วนใหญ่ ล้วนแต่เคยมีการรายงานข้อผิดพลาดมาแล้วทั้งสิ้น แม้แต่ไฟร์วอลล์ที่ถือว่าเป็นอันดับหนึ่งอย่าง Firewall-1 ก็ยังเคยมีการรายงานข้อผิดพลาด แต่ผู้อ่านก็ไม่ต้องตกใจไปหรอกนะครับ เพราะนาน ๆ ทีจึงจะมีเหตุการณ์แบบนี้เกิดขึ้น และเมื่อเกิดขึ้นทางผู้ผลิตก็แก้ไขกันอย่างรวดเร็วอยู่แล้ว ดังนั้นหากเราดูแลระบบดี ๆ แล้วเราก็ยังสามารถเชื่อถือในไฟร์วอลล์ได้เต็มร้อย

ดังนั้นเมื่อมีจำนวนชั้นของไฟร์วอลล์มากกว่าก็จะปลอดภัยมากกว่า และในบางองค์กรมีการออกแบบให้ใช้ไฟร์วอลล์ต่างยี่ห้อกันในแต่ละชั้นของไฟร์วอลล์ด้วยแล้ว ก็ยิ่งเป็นการยากเข้าไปอีกที่จะสามารถเจาะทะลุไฟร์วอลล์หลาย ๆ ยี่ห้อเข้าไปได้

ที่กล่าวมาทั้งหมดนั้น เป็นการกล่าวในแง่ของความปลอดภัยจากการโจมตี แต่ไม่ได้กล่าวในแง่ของระบบที่ไม่ล้มเหลว ที่ภาษาอังกฤษเรียกว่า High Availability เพราะเครื่องคอมพิวเตอร์ที่รันโปรแกรมไฟร์วอลล์ก็เป็นคอมพิวเตอร์เครื่องหนึ่ง ที่แม้จะเป็นยี่ห้อที่น่าเชื่อถือสักเท่าใด มีราคาสูงสักเท่าใด คอมพิวเตอร์เครื่องนั้นก็สามารถล้มเหลวได้ แม้จะเป็นเปอร์เซ็นต์ที่น้อยก็ตาม ดังนั้นหากต้องการความมั่นคงของไฟร์วอลล์ ให้มากขึ้นก็ต้องเพิ่มไฟร์วอลล์เข้าไปอีกให้ทำงานขนานกัน ซึ่งจะมีชื่อเรียกไฟร์วอลล์แบบนี้ว่า Load-Balanced Firewall ซึ่งแน่นอนว่าจะทำให้ราคาของระบบสูงขึ้นไปอีก

การเลือกใช้ไฟร์วอลล์

หลังจากที่เราได้ออกแบบโครงสร้างที่แบ่งเครือข่ายออกเป็นส่วน ๆ เรียบร้อยแล้ว คราวนี้เราจะมาพิจารณาแนวทางการเลือกใช้ไฟร์วอลล์กัน เพื่อจะได้จัดหาไฟร์วอลล์ที่เหมาะสมมาใช้กับองค์กร ไฟร์วอลล์นั้นสามารถแบ่งเป็นประเภทได้หลายอย่าง โดยอาจแบ่งตามรูปแบบเป็น 2 แบบ คือ แบบที่เป็นฮาร์ดแวร์ และแบบที่เป็นซอฟต์แวร์

ไฟร์วอลล์แบบที่เป็นฮาร์ดแวร์นั้น อันที่จริงแล้วก็เป็นแบบซอฟต์แวร์นั่นแหละ เพียงแต่ตอนที่เขาขายนั้นเขาขายมาพร้อมกับฮาร์ดแวร์ โดยซอฟต์แวร์ของไฟร์วอลล์แบบนี้จะสร้างขึ้นมาเพื่อให้ทำงานกับฮาร์ดแวร์

นั้น ๆ โดยเฉพาะ ดังนั้นการทำงานระหว่างซอฟต์แวร์และฮาร์ดแวร์ก็จะเข้ากันได้เป็นอย่างดี และมีความปลอดภัยมากกว่า เพราะซอฟต์แวร์ของไฟร์วอลล์แบบนี้ จะไม่ได้ทำงานอยู่บนระบบปฏิบัติการทั่วไป แต่จะรันอยู่บนระบบปฏิบัติการที่เขียนขึ้นมาเฉพาะ โดยบางบริษัทจะพัฒนาขึ้นมาใหม่ทั้งหมด แต่บางบริษัทก็นำระบบปฏิบัติการประเภทยูนิกซ์มาดัดแปลง ซึ่งทำให้การหาข้อมูลเกี่ยวกับฮาร์ดแวร์และระบบปฏิบัติการเหล่านั้นทำได้ยากขึ้น ทำให้การเจาะเข้าไปในไฟร์วอลล์ประเภทนี้ยากขึ้นไปด้วย

ไฟร์วอลล์อีกประเภทหนึ่ง คือ ไฟร์วอลล์ที่มีลักษณะเป็นซอฟต์แวร์อย่างเดียว โดยไฟร์วอลล์แบบนี้จะทำงานอยู่บนเครื่องคอมพิวเตอร์เซิร์ฟเวอร์ และระบบปฏิบัติการทั่วไป โดยอาจมีการเข้าไปแก้ไขส่วนประกอบของระบบปฏิบัติการบางส่วน โดยเฉพาะส่วนที่ทำหน้าที่ติดต่อกับเครือข่าย ทั้งนี้เพื่อให้ไฟร์วอลล์สามารถควบคุมการสื่อสารได้โดยตรง และช่วยให้คอมพิวเตอร์ที่รันโปรแกรมไฟร์วอลล์มีความแข็งแกร่งมากขึ้น ดังนั้นเครื่องคอมพิวเตอร์ที่จะใช้ทำเป็นไฟร์วอลล์จึงควรจะใช้เป็นไฟร์วอลล์เพียงอย่างเดียว ไม่ควรให้ทำหน้าที่อื่นร่วมด้วย เพราะมักจะมีปัญหาเกิดขึ้นเสมอ หากให้เครื่องคอมพิวเตอร์ที่ใช้เป็นไฟร์วอลล์ ทำหน้าที่ให้บริการอย่างอื่นด้วย

สำหรับแนวทางการเลือกระหว่างไฟร์วอลล์ประเภทซอฟต์แวร์กับฮาร์ดแวร์นั้น ไฟร์วอลล์ประเภทซอฟต์แวร์จะมีข้อดีที่มีความยืดหยุ่นในการใช้งานมากกว่า กล่าวคือ เนื่องจากทำงานบนเครื่องคอมพิวเตอร์ จึงมีการติดต่อผู้ใช้เป็นแบบกราฟิก และเนื่องจากเป็นซอฟต์แวร์ ดังนั้นจึงสามารถเลือกเครื่องคอมพิวเตอร์ที่จะติดตั้งให้เหมาะสมกับประสิทธิภาพที่ต้องการได้ เช่น หากเครือข่ายมีความเร็วไม่มากนัก ก็อาจจะใช้เครื่องสเปกทั่วไปได้ แต่หากเครือข่ายมีความเร็วสูง ก็อาจจะหาเครื่องประสิทธิภาพสูง ๆ มาใช้แทนได้ เครื่องเดิมก็สามารถนำไปใช้งานอย่างอื่นต่อไป แต่ไฟร์วอลล์แบบฮาร์ดแวร์จะทำไม่ได้ แต่สิ่งที่คุณจะได้จากไฟร์วอลล์แบบฮาร์ดแวร์คือ ความปลอดภัยที่สูงกว่า จากเหตุผลที่ได้กล่าวไปแล้ว และอีกประการหนึ่ง คือ ค่าใช้จ่าย เพราะไฟร์วอลล์ประเภทฮาร์ดแวร์มีแนวโน้มที่จะมีราคาสูงกว่า

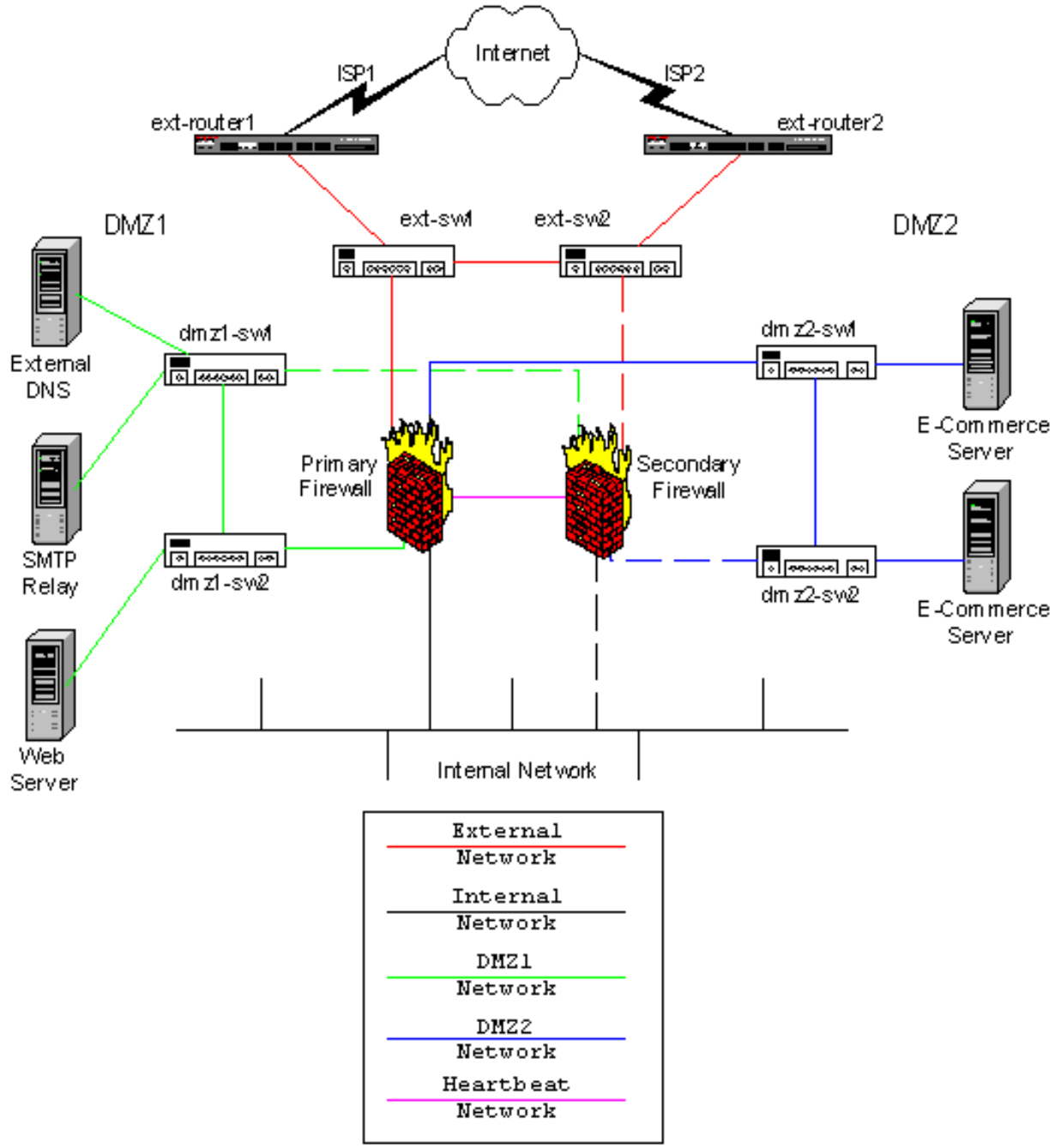
ในระบบที่ออกแบบ จะเลือกไฟร์วอลล์ประเภท Stateful Inspection แล้วจะออกแบบเงื่อนไขการทำงานไว้แบบนี้ครับ คือ สำหรับไฟร์วอลล์ตัวนอก จะเปิดเฉพาะพอร์ตที่มีการใช้งาน ซึ่งในที่นี้ก็จะมีเพียงเมล์และเว็บเท่านั้น ดังนั้นนอกเหนือจากช่องทางทั้งสองแล้วแฮกเกอร์ก็จะโจมตีระบบไม่ได้เลย หากไม่โจมตีไฟร์วอลล์เสียก่อน เพราะไฟร์วอลล์จะช่วยป้องกันเอาไว้ สำหรับไฟร์วอลล์ตัวใน ผมก็จะยิ่งตั้งเงื่อนไขให้เข้มงวดอีกว่า

การติดต่อระหว่างไคลเอนต์ภายในเพื่อใช้งานเว็บ หรือ ใช้งานเมล์ จะต้องเริ่มการติดต่อจากข้างในมาข้างนอกเท่านั้น ซึ่งด้วยความที่เป็นไฟร์วอลล์ประเภท Stateful Inspection มันจะเสมือนกับเป็นการปิดพอร์ตทั้งหมดจากภายนอก และจะเปิดใช้งานบางพอร์ตเฉพาะระหว่างการติดต่อเท่านั้น ดังนั้นการโจมตีเข้ามาข้างในก็จะสามารถทำได้เฉพาะเวลาที่ติดต่อกับข้างนอกเท่านั้น และจะโจมตีได้เฉพาะเครื่องที่กำลังติดต่อเท่านั้นด้วย ดังนั้นจะเห็นได้ว่าจะปลอดภัยมาก

สำหรับไฟร์วอลลที่มีจำหน่ายในปัจจุบันนั้น ได้พัฒนาก้าวหน้าไปมาก มีฟังก์ชันต่าง ๆ เพิ่มขึ้นมากมาย และส่วนใหญ่จะไม่ได้เป็นประเภทใดประเภทหนึ่งซะทีเดียว แต่จะเป็นแบบผสมผสาน โดยไฟล์วอลล์ที่จัดว่าเป็นแบบ Stateful ได้แก่ Firewall-1 ของ Checkpoint, Symactec Enterprise Firewall (Raptor) ของ Symantec, Bulletproof ของ CA, PIX Firewall ของ Cisco และ ISA Server ของไมโครซอฟต์ ไฟล์วอลล์ที่จัดว่าเป็น Application Proxy จริง ๆ ก็น่าจะเป็น Gaunlet ของบริษัท Network Associate

นอกเหนือจากที่ได้กล่าวมา ก็ควรจะพิจารณาความสามารถอื่น ๆ ของไฟร์วอลล์ประกอบด้วย เช่น บางยี่ห้อมีการทำงานในระดับ User ด้วย คือ ผู้ใช้แต่ละคนจะผ่านไฟร์วอลล์ได้ไม่เท่ากัน บางยี่ห้อสามารถกระจาย Policy ไปยังไฟร์วอลล์ตัวอื่น ๆ ได้ บางยี่ห้อสามารถทำงานกับแอปพลิเคชันอื่นได้ เช่น ทำงานร่วมกับโปรแกรมแอนตี้ไวรัสในการตรวจสอบไวรัสบนเมล์หรือเว็บ หรือทำงานร่วมกับโปรแกรมตรวจจับการบุกรุกได้ บางยี่ห้อสามารถตั้งปฏิทินการทำงานให้ใช้กฎ ที่ต่างกันในแต่ละช่วงเวลาได้ บางยี่ห้อมีการเพิ่มส่วนตรวจสอบเว็บ (Content Filter) เพื่อกรองข้อมูลที่ผ่านเว็บเป็นพิเศษ และอื่น ๆ อีกมากมาย

ตัวอย่างการออกแบบ



รูปที่ 38 ตัวอย่างเครือข่าย

รูปข้างต้นเป็นการออกแบบ High Available Firewall โดยการใช้ไฟร์วอลล์ 2 ตัวทำหน้าที่กั้นระหว่างเครือข่าย โดยไฟร์วอลล์ 2 ตัวนี้จะทำงานแบบ Load Balancing คือ ใช้ Virtual IP เดียวกัน แบ่งภาระการทำงาน

โดยหากเป็นไมโครซอฟต์จะเรียกการเชื่อมต่อระหว่างเซิร์ฟเวอร์ 2 ตัวนี้ว่า Heartbeat โดยจะคอยตรวจสอบการทำงานของไฟร์วอลล์ทั้ง 2 หากมีตัวใดตัวหนึ่งผิดปกติ จะทำการ Failover ทันที ระบบนี้จะเหมาะสำหรับองค์กรที่ต้องการ

ไฟร์วอลล์สำหรับ Host

ไฟร์วอลล์สำหรับนี้ เรามักได้ยินคำว่า Personal Firewall มากกว่า โดยไฟร์วอลล์ประเภทนี้จะทำหน้าที่ป้องกันเฉพาะคอมพิวเตอร์เครื่องใดเครื่องหนึ่งมากกว่าจะป้องกันเครือข่าย ผลิตภัณฑ์เหล่านี้ส่วนใหญ่มักออกแบบมาเพื่อใช้กับระบบปฏิบัติการในตระกูลวินโดว์ เพราะเป็นระบบปฏิบัติการที่มีการใช้งานเป็นไคลเอนต์มากที่สุด ผลิตภัณฑ์เหล่านี้มักมีราคาถูก และบางตัวก็ให้ดาวน์โหลดได้ฟรี นอกจากนั้นบางตัวยังมีความสามารถด้าน IDS แบบง่าย ๆ อีกด้วย โปรแกรมเหล่านี้แม้ว่าจะทำให้การใช้งานคอมพิวเตอร์มีความยุ่งยากมากขึ้น แต่ก็มีประโยชน์เพราะสามารถตรวจสอบได้ว่ามีการสแกนเข้ามาในเครื่องของเรา หรือมีความ พยายามแฮกเข้ามาในเครื่องของเราหรือไม่ นอกจากนั้นผลิตภัณฑ์เหล่านี้ ส่วนใหญ่มีการใช้งานง่าย สามารถเพิ่มกฎเข้าไปได้เอง โดยไม่จำเป็นต้องมีความรู้มากนัก ตัวอย่างของโปรแกรมเหล่านี้ได้แก่

- Zone Alarm
- Tiny Personal Firewall
- Norton Personal Firewall
- Sygate Personal Firewall
- Conseal PC Firewall
- VPN-1 Secure Client

และนอกเหนือจากโปรแกรมที่กล่าวมาข้างต้นแล้ว ยังมีโปรแกรมที่ทำหน้าที่ป้องกันเซิร์ฟเวอร์ด้วย เช่น โปรแกรม IP Filter, SunScreen Lite Firewall, Firewall-1 Secure Server และ Packet Filtering via IPSec in Windows 2000

บทที่ 8. Network Address Translation

Network Address Translation (NAT) คือวิธีการทางเครือข่ายที่จะเปลี่ยนค่า Network Address จากหมายเลขหนึ่งไปเป็นอีกหมายเลขหนึ่ง ซึ่งทำให้เกิดการเชื่อมต่อไปยังเครื่องปลายทางได้ โดยเครื่องต้นทางไม่จำเป็นต้องเปลี่ยนแปลงค่าทางเครือข่าย การทำ NAT ช่วยให้การใช้งานเครือข่ายทำได้อย่างมีประสิทธิภาพมากขึ้นกว่าที่เป็นอยู่ รวมทั้งมีส่วนในการรักษาความปลอดภัยในเครือข่ายได้ด้วย ซึ่งโดยทั่วไปจะเป็นความสามารถหนึ่งในไฟร์วอลล์ หรืออุปกรณ์เครือข่ายทั่วไปอยู่แล้ว

จุดประสงค์ของการทำ NAT

ที่มาของการทำ NAT นั้นเกิดจากความคิดที่จะนำ Private IP ซึ่งเป็นหมายเลขไอพีแอดเดรสที่ใช้สำหรับเครือข่ายเฉพาะ ซึ่งไม่มีการใช้งานข้ามเครือข่ายได้ (ไม่มีการ route ไปยังเครือข่ายอื่นๆ) และนำมาใช้เพื่อแก้ปัญหาการขาดแคลนหมายเลขไอพีแอดเดรสในอนาคตด้วย ซึ่งภายหลัง การทำงานของ NAT สามารถเพิ่มความสามารถในการรักษาความปลอดภัย และนำมาใช้ในการแก้ปัญหาในกรณีที่หมายเลขไอพีแอดเดรสในองค์กรมีจำนวนจำกัด

Private IP Address

เนื่องจากการใช้งานระบบเครือข่ายนั้น ในบางครั้งก็ไม่จำเป็นที่จะต้องเชื่อมต่อกับเครือข่ายอื่นๆ เลย ยกตัวอย่างเช่นเครือข่ายภายในบริษัท ซึ่งจะติดต่อสื่อสารกันเฉพาะภายในบริษัทเท่านั้น ไม่จำเป็นต้องติดต่อกับบริษัทอื่นๆ หรือเครือข่ายอินเทอร์เน็ต แต่การติดต่อสื่อสารเพื่อใช้งานแอปพลิเคชั่นต่างๆ ก็ยังจำเป็นต้องใช้หมายเลขไอพีแอดเดรสเช่นเดียวกัน ปัญหาที่เกิดขึ้นก็คือถ้ามีการจัดแบ่งหมายเลขไอดีแอดเดรสที่มีอยู่ให้กับเครือข่ายในลักษณะนี้ จะทำให้เกิดปัญหาหมายเลขไอดีแอดเดรสไม่เพียงพอ การตรวจสอบและจัดสรรทำได้ยาก รวมถึงการรักษาความปลอดภัยในเครือข่ายจะทำได้ยากขึ้นด้วย

จากปัญหาดังกล่าวองค์กรที่มีชื่อว่า Internet Assigned Number Authority (IANA) ซึ่งเป็นผู้รับผิดชอบ ดูแลในการจัดสรรหมายเลขไอพีแอดเดรสให้กับผู้ใช้งานทั่วโลก ได้กำหนดช่วงของหมายเลขไอพีแอดเดรสที่ ทุกๆ คน สามารถนำไปใช้ได้โดยไม่จำเป็นต้องขึ้นทะเบียนก่อนเรียกว่าช่วง Private IP ซึ่งหมายเลขไอพีแอดเดรสในช่วงนี้จะไม่สามารถนำมาเชื่อมต่อกับเครือข่ายอื่นๆ ได้โดยตรง

ช่วงของหมายเลขไอพีแอดเดรสที่เป็น Private IP นั้น จะแบ่งเป็น 3 กลุ่มด้วยกันคือ

1. ช่วงหมายเลข 10.0.0.0 – 10.255.255.255 (10 / 8)
2. ช่วงหมายเลข 172.16.0.0 – 172.32.255.255 (172.16 / 12)
3. ช่วงหมายเลข 192.168.0.0 – 192.168. 255.255 (192.168 / 16)

คุณสมบัติของอุปกรณ์ NAT

อุปกรณ์เครือข่าย หรือโปรแกรมที่ใช้ในการทำ NAT จะต้องมีความสามารถในการทำงานต่างๆ เหล่านี้คือ

1. สามารถกำหนดหมายเลขไอพีแอดเดรสได้ (Transparent address assignment)
2. สามารถส่งผ่านแพ็กเก็ตของข้อมูลที่มีการเปลี่ยนแปลงแอดเดรสได้ (Transparent address routing through address transition)
3. สามารถเปลี่ยนแปลงข้อมูลของ ICMP payload ได้ (ICMP error message payload translation)

<u>สามารถกำหนดหมายเลขไอพีแอดเดรสได้ (Transparent address assignment)</u>

อุปกรณ์ที่จะทำ NAT นั้นจะต้องสามารถเปลี่ยนค่าหมายเลขไอพีแอดเดรสของข้อมูลในเครือข่าย ซึ่งเป็นหมายเลขไอพีเอดเดรสในกลุ่มของ Private IP ให้กลายเป็นหมายเลขไอพีแอดเดรสที่ใช้ในเครือข่ายอินเทอร์เน็ต และสามารถเปลี่ยนหมายเลขไอพีแอดเดรสที่ใช้ในเครือข่ายอินเทอร์เน็ตให้กลายเป็นหมายเลขไอพีแอดเดรสในช่วย Private IP ได้อย่างถูกต้อง ซึ่งในบางกรณีอาจจำเป็นต้องเปลี่ยนแปลงค่าข้อมูลในชั้น Transport

บางส่วนด้วยเช่นหมายเลขพอร์ตของ TCP และ UDP ในการเปลี่ยนแปลงค่าไอพีแอดเดรสนั้นสามารถทำได้ 2 แบบคือแบบ Static และแบบ Dynamic

static address assignment

เป็นการเปลี่ยนแปลงค่าหมายเลขไอพีแอดเดรสโดยมีการจับคู่กันของหมายเลขไอพีแอดเดรสตลอดการทำงานของอุปกรณ์ ซึ่งจะเปลี่ยนแปลงค่าไอพีแอดเดรสจาก Private IP เป็นหมายเลขไอพีภายนอก และเปลี่ยนจากหมายเลขไอพีแอดเดรสภายนอกเป็น Private IP แบบหนึ่งต่อหนึ่งไปตลอด

dynamic address assignment

เป็นการเปลี่ยนแปลงค่าหมายเลขไอพีแอดเดรสโดยมีการจับคู่กันของหมายเลขไอพีแอดเดรสที่เป็น Private IP กับหมายเลขไอพีแอดเดรสภายนอกเพียงชั่วคราวเท่านั้น โดยอุปกรณ์ NAT จะจับคู่หมายเลขไอพีแอดเดรสในช่วงเวลาที่ session มีการเชื่อมต่อกันอยู่เท่านั้น หลังจากที่ใช้งาน session เสร็จเรียบร้อยแล้วจะไม่เก็บข้อมูลการจับคู่นั้นไว้อีก เมื่อมีการเชื่อมต่อกับเครือข่ายภายนอกอีกครั้ง อุปกรณ์ NAT จะเลือกหมายเลขไอพีแอดเดรสภายนอกใหม่อีกครั้งหนึ่ง ซึ่งไม่จำเป็นต้องซ้ำกับหมายเลขเดิม

<u>สามารถส่งผ่านแพ็กเก็ตของข้อมูลที่มีการเปลี่ยนแปลงแอดเดรสได้ (Transparent address routing through address transition)</u>

เนื่องจากอุปกรณ์ที่ทำ NAT นั้นจะอยู่ระหว่างระบบหมายเลขแอดเดรส 2 ระบบคือ Private Address และไอพีแอดเดรสที่จดทะเบียนอย่างถูกต้อง ดังนั้นสิ่งที่อุปกรณ์ NAT จะต้องคำนึงถึงก็คือ การทำงานที่ไม่ขัดต่อการทำงานของระบบหมายเลขแอดเดรสทั้งสองระบบ และต้องไม่เป็นปัญหาในการหาเส้นทางและการรับส่งข้อมูลด้วย โดยข้อควรระวังข้อหนึ่งในการใช้อุปกรณ์ NAT คือการป้องกันการส่งข้อมูล routing information

ข้ามเครือข่าย (จากเครือข่ายภายนอก ส่งมายังเครือข่ายภายใน หรือจากเครือข่ายภายในส่งไปยังเครือข่ายภายนอก) เนื่องจากจะทำให้ระบบโดยรวมมีปัญหาทันที

กระบวนการในการเปลี่ยนหมายเลขไอพีแอดเดรสมีขั้นตอนทั้งหมด 3 ขั้นตอนหลักคือ ขั้นตอนในการจับคู่หมายเลขไอพีแอดเดรส ขั้นตอนในการเปลี่ยนแปลงหมายเลขไอพีแอดเดรสขณะที่มีการเชื่อมต่อกันแล้ว และกระบวนการเมื่อสิ้นสุดการทำงาน

การทำงานในการจับคู่หมายเลขไอพีแอดเดรส (address binding)

ขั้นตอนนี้เป็นขั้นตอนที่อุปกรณ์ NAT เปลี่ยนแปลงหมายเลขไอพีแอดเดรสจาก Private IP ให้กลายเป็นไอพีที่จดทะเบียนไว้แล้ว และเปลี่ยนแปลงหมายเลขไอพีแอดเดรสจากไอพีที่จดทะเบียนไว้แล้วให้กลายเป็น Privatte IP ซึ่งสามารถทำได้ทั้งแบบ Static และ Dynamic ซึ่งในการ binding นั้นจะมีการเปลี่ยนแปลงหมายเลขไอพีแอดเดรสคู่นั้นๆ ไปจนกว่าจะปิดการเชื่อมต่อ

กระบวนการนี้เริ่มต้นเมื่อเริ่มต้นการเชื่อมต่อ (ซึ่งยังไม่มีการเชื่อมต่อกันมาก่อน) โดยเครื่องที่ส่งข้อมูลจะส่งข้อมูลผ่านอุปกรณ์ NAT ซึ่งอุปกรณ์ NAT จะมีการกำหนดหมายเลขไอพีแอดเดรสให้กับข้อมูลนั้นใหม่อีกครั้งหนึ่ง โดยการกำหนดหมายเลขไอพีแอดเดรสที่มีการจดทะเบียนให้แทน แล้วจะจำไว้ว่าได้มีการจับคู่หมายเลขไอพีแอดเดรสภายนอกอะไร กับหมายเลข Private IP อะไรบ้าง ตัวเลขคู่นี้จะกำหนดไปจนกว่าจะจบการเชื่อมต่อ สำหรับกรณีที่มีการเชื่อมต่อมากกว่า 1 การเชื่อมต่อในช่วงเวลาเดียวกันก็จะมีการจับคู่หมายเลขแอดเดรสแบบเดียวกัน

การทำงานขณะมีการเชื่อมต่อกันแล้ว (address lookup and translation)

หลังจากที่ session มีการเชื่อมต่อกันแล้ว เมื่อการส่งข้อมูลถัดๆ มาจะมีการเปลี่ยนแปลงหมายเลขไอพีแอดเดรสโดยใช้วิธีการค้นหาในหน่วยความจำว่าเคยจับคู่กับหมายเลขไอพีแอดเดรสอะไร

การทำงานเมื่อสิ้นสุดการเชื่อมต่อ (address unbinding)

เป็นกระบวนการที่เกิดขึ้นเมื่อสิ้นสุดการเชื่อมต่อแล้ว โดยอุปกรณ์ NAT จะมีกระบวนการในการตรวจจับว่ามีการสิ้นสุด session ของคู่ไอพีแอดเดรสนั้นๆ หรือไม่ ซึ่งถ้ามีการสิ้นสุดแล้วจะลบข้อมูลการจับคู่ออกจากหน่วยความจำ

สามารถเปลี่ยนแปลงข้อมูลของ ICMP payload ได้ (ICMP error message payload translation)

การทำงานในเครือข่าย TCP/IP นั้น เมื่อมีการทำงานที่ผิดพลาดเกิดขึ้น จะมีการส่งรายละเอียดต่างๆ ไปกับแพ็กเก็ต ICMP ซึ่งในกรณีที่มีการใช้งาน NAT และเกิดการทำงานที่ผิดพลาดหรือผิดปกติเกิดขึ้นในเครือข่าย ตัวอุปกรณ์ NAT ต้องสามารถเปลี่ยนแปลงข้อมูลในแพ็กเก็ต ICMP ให้ถูกต้องด้วย เช่น Destination Unreachable , Source-Quench , Time-Exceed และ Parameter-Problem แต่ NAT ไม่ควรเปลี่ยนแปลงค่าข้อมูลใน Redirect Message

การเปลี่ยนแปลงค่าในแพ็กเก็ต ICMP นั้นจะหมายรวมถึงค่าของหมายเลขไอพีแอดเดรสต้นทางใน ICMP payload ด้วย ซึ่งก็หมายความว่าต้องเปลี่ยนค่า checksum ทั้งใน ICMP header และ IP header ด้วยเช่นกัน

รูปแบบของการทำงานของ NAT

เนื่องจากการทำงานของระบบและการใช้งานเครือข่ายมีหลากหลายรูปแบบ การทำ NAT จึงมีวิธีการหลายรูปแบบเพื่อให้เหมาะสมกับการทำงานแบบต่างๆ โดยการทำ NAT แบบต่างๆ มีดังนี้คือ

Traditional NAT (outbound NAT)

เป็นการทำ NAT แบบหนึ่งที่ออกแบบให้มีการเชื่อมต่อจากเครือข่ายภายใน ออกสู่เครือข่ายภายนอกเท่านั้น โดย outbound NAT แบ่งออกเป็น 2 แบบคือ Basic NAT และ Network Address Port Translation (NAPT)

basic NAT

เป็นการทำ NAT โดยเปลี่ยนแปลงข้อมูลของเครือข่ายภายในซึ่งเป็นเครือข่ายที่เริ่มการเชื่อมต่อ ให้กลายเป็นข้อมูลที่เหมาะสมในการเชื่อมต่อ โดยอุปกรณ์ NAT จะเปลี่ยนแปลงข้อมูลหมายเลขไอพีต้นทาง และข้อมูลที่เกี่ยวข้องอื่นๆ เช่น TCP , UDP , ICMP header checksum เป็นต้น ซึ่งหลังจากที่มีการเชื่อมต่อกันเรียบร้อยแล้ว ข้อมูลที่ตอบกลับมาจากเครือข่ายภายนอกก็จะถูกเปลี่ยนแปลงให้เหมาะสมในการเชื่อมต่อกับเครือข่ายภายในเช่นกัน

Network Address Port Translation (NAPT)

Network Address Port Translation (NAPT) คือกระบวนการที่คล้ายกับการทำ NAT แต่จะมีการเปลี่ยนแปลงข้อมูลในชั้น transport ด้วยเช่น TCP port , UDP port และ ICMP query identification เป็นต้น ซึ่งกระบวนการดังกล่าวจะช่วยให้สามารถทำ NAT โดยใช้หมายเลขไอพีแอดเดรสที่จดทะเบียนเพียงหมายเลขเดียวได้

Bi-Directianal NAT (Two-way NAT)

เป็นการทำ NAT ที่สามารถเชื่อมต่อจากเครือข่ายภายนอกเข้ามายังเครือข่ายภายในได้ เช่นเดียวกับการเชื่อมต่อจากเครือข่ายภายในออกไปยังเครือข่ายภายนอก ในการจับคู่หมายเลขไอพีแอดเดรสสามารถทำได้ทั้งแบบ static และ dynamic สำหรับการเชื่อมต่อจากต้นทางไปยังปลายทางนั้นจำเป็นต้องใช้ DNS ในการบอกหมายเลขไอพีในการเชื่อมต่อด้วยโดยเฉพาะในการทำงานแบบ Dynamic

Twice-NAT

การทำงานของ Traditional NAT และ Bi-Directional NAT นั้นมีการเปลี่ยนแปลงเฉพาะค่าของหมายเลขไอพีแอดเดรสต้นทางหรือหมายเลขไอพีแอดเดรสปลายทาง อย่างใดอย่างหนึ่งเท่านั้น ซึ่งในการทำงานบางอย่างจำเป็นต้องมีการทำงานมากกว่านี้ เช่นในกรณีที่หมายเลขไอพีแอดเดรสภายในซ้ำกับหมายเลขไอพี

แอดเดรสภายนอก (กรณีที่มีการเปลี่ยน ISP แต่ไม่ต้องการให้เปลี่ยนแปลง configuration ในองค์กร) ซึ่งปัญหาที่เกิดขึ้นก็คือไม่สามารถเชื่อมต่อไปยังเครือข่ายภายนอกได้ เพราะถือว่าเป็นการทำงานใน local เท่านั้น สำหรับปัญหานี้จำเป็นต้องมีการทำ NAT ที่มีการเปลี่ยนแปลงทั้งหมายเลขไอพีแอดเดรสต้นทางและปลายทางพร้อมๆ กัน ซึ่งต้องใช้การทำงานของ DNS มาช่วยในการเชื่อมต่อด้วย

ยกตัวอย่างเช่นในกรณีที่เครือข่ายภายในเป็นเครือข่าย 200.200.200.0/24 ต้องการเชื่อมต่อไปยังเครื่องในเครือข่ายภายนอกหมายเลขไอพีแอดเดรสคือ 200.200.200.100 จะมีการทำงานคือ

1. ต้องทำให้เครื่องต้นทางส่งข้อมูลไปยังหมายเลขไอพีแอดเดรสในเครือข่ายภายนอกให้ได้เพื่อให้แพ็กเก็ตผ่านอุปกรณ์ NAT ซึ่งต้องให้เป็นภาระการทำงานของ DNS และ
2. ต้องให้อุปกรณ์ NAT เปลี่ยนแปลงหมายเลขไอพีแอดเดรสปลายทางไปยัง ปลายทางที่แท้จริง และเปลี่ยนแปลงหมายเลขไอพีต้นทางเป็นหมายเลยไอพีแอดเดรสที่จดทะเบียนอย่างถูกต้อง

ในการทำงานข้อแรก เครื่องคอมพิวเตอร์ในเครือข่ายภายในร้องขอไปยัง DNS เมื่อ DNS รับการร้องขอแล้ว DNS จะส่งหมายเลขไอพีแอดเดรสปลอมซึ่งเป็นหมายเลขไอพีแอดเดรสของเครือข่ายภายนอกไปให้เครื่องคอมพิวเตอร์ที่ร้องขอ พร้อมกับส่งข้อมูลการร้องขอและหมายเลขไอพีแอดเดรสปลายทางที่แท้จริงไปให้อุปกรณ์ NAT

หลังจากนั้นเครื่องต้นทางจะส่งข้อมูลเพื่อร้องขอไปยังหมายเลขไอพีที่ได้ เมื่อแพ็กเก็ตส่งไปยังอุปกรณ์ NAT ได้แล้ว หลังจากนั้นอุปกรณ์ NAT จะเปลี่ยนหมายเลขไอพีแอดเดรสปลายทางให้กลายเป็นหมายเลขปลายทางที่แท้จริง และเปลี่ยนแปลงหมายเลขไอพีต้นทางให้เป็นหมายเลขไอพีที่จดทะเบียนอย่างถูกต้อง ซึ่งถ้าอุปกรณ์ NAT ได้รับข้อมูลตอบกลับมาแล้ว จะเปลี่ยนแปลงข้อมูลกลับไปเป็นแบบเดิมอีกครั้งหนึ่ง ซึ่งจะทำให้การเชื่อมต่อเป็นไปได้อย่างถูกต้องทั้งทางฝั่งผู้รับและผู้ส่ง

Multihomed NAT

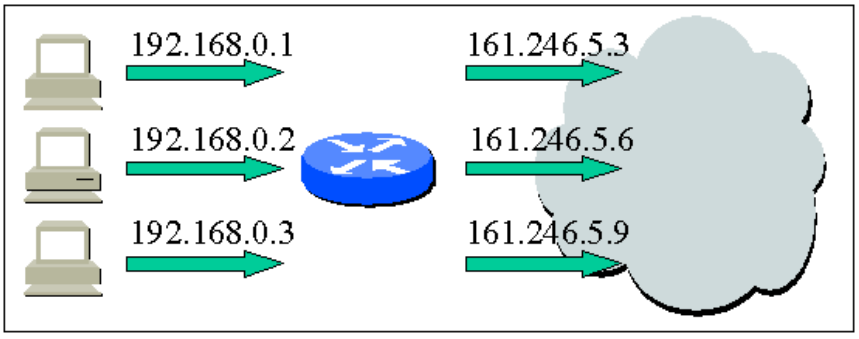
จากการออกแบบเครือข่ายที่ทำให้ NAT เป็นเสมือนกับช่องทางเชื่อมต่อไปยังเครือข่ายภายนอกเพียงช่องทางเดียวซึ่งทำให้เป็นจุดอ่อนในระบบ (single point of failure) วิธีการแก้ปัญหานี้ก็สามารถทำได้โดยการ

ออกแบบให้มีอุปกรณ์ NAT มากกว่าหนึ่งชิ้นในเครือข่าย ซึ่งอุปกรณ์ทั้งหมดต้องสามารถส่งข้อมูลสถานะการทำงานเช่นข้อมูลการจับคู่หมายเลขไอพีแอดเดรส และต้องมีความสามารถในการสวิทช์การทำงานไปยังอุปกรณ์ตัวอื่นๆ ได้ในกรณีที่มีอุปกรณ์หลักมีปัญหาได้

<u>การใช้งาน NAT</u>

- Static NAT (static assignment and basic NAT)

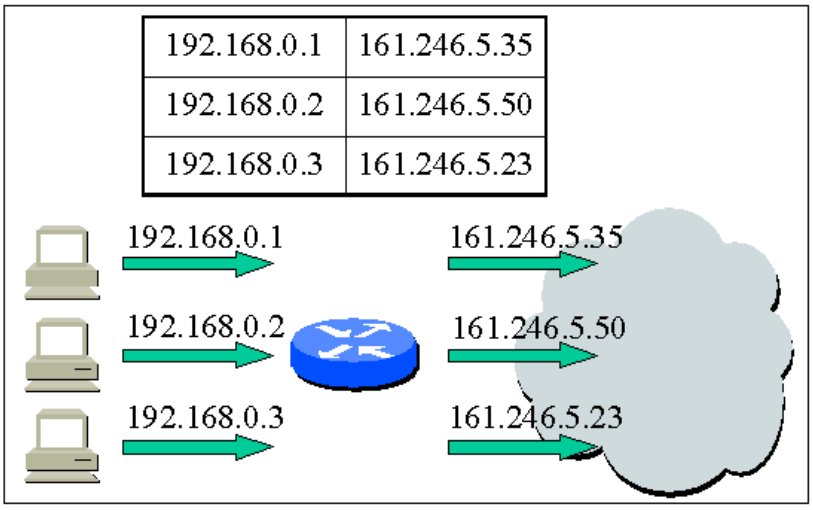
เป็นการทำ NAT ที่ช่วยให้เครื่องคอมพิวเตอร์ที่มีหมายเลขไอพีแอดเดรสอยู่ในช่วง private IP หรือหมายเลขไอพีแอดเดรสที่ไม่ได้จดทะเบียนอย่างถูกต้อง สามารถติดต่อกับเครือข่ายอื่นๆ ได้ โดยการทำงานของ Static NAT นั้นจะจับคู่ระหว่างหมายเลขไอพีแอดเดรสภายในเครือข่าย กับหมายเลขไอพีแอดเดรสที่ได้รับการจดทะเบียนแบบหนึ่งต่อหนึ่ง ในการทำงานลักษณะนี้มีประโยชน์เพื่อความสะดวกในการจัดการหมายเลขไอพีแอดเดรสในเครือข่ายที่มักจะมีการปรับเปลี่ยนบ่อยๆ และทำให้เครื่องคอมพิวเตอร์ภายนอกเครือข่ายสามารถติดต่อเข้ามาในเครือข่ายได้ด้วย



รูปที่ 39 Static NAT

- Dynamic NAT (dynamic assignment and basic NAT)

เป็นการทำ NAT ที่ใช้วิธีการเปลี่ยนแปลงหมายเลขไอพีแอดเดรสที่ใช้ในเครือข่าย ให้กลายเป็นหมายเลขไอพีแอดเดสรที่จดทะเบียนแล้ว โดยการสุ่มเลือกหมายเลขไอดีแอดเดรสซึ่งการทำงานลักษณะนี้จะช่วยให้เครือข่ายที่มีหมายเลขไอพีแอดเดรสในช่วง private IP หรือเป็นเครือข่ายที่มีการตั้งค่าหมายเลขไอพีแอดเดรสเองโดยไม่ได้จดทะเบียน สามารถติดต่อไปยังเครือข่ายอื่นๆ ได้ แต่การทำ Dynamic NAT นี้เครื่องคอมพิวเตอร์จากภายนอกเครือข่ายจะไม่สามารถติดต่อเข้ามายังเครื่องคอมพิวเตอร์ภายในเครือข่ายได้ เนื่องจากเครื่องคอมพิวเตอร์ภายนอกจะไม่สามารถทราบได้เลยว่าหมายเลขไอพีแอดเดรสของเครื่องที่จะเชื่อมต่อด้วยนั้นคือหมายเลขอะไร ซึ่งการทำ Dynamic NAT ก็สามารถนำมาใช้เพื่อรักษาความปลอดภัยในเครือข่ายได้

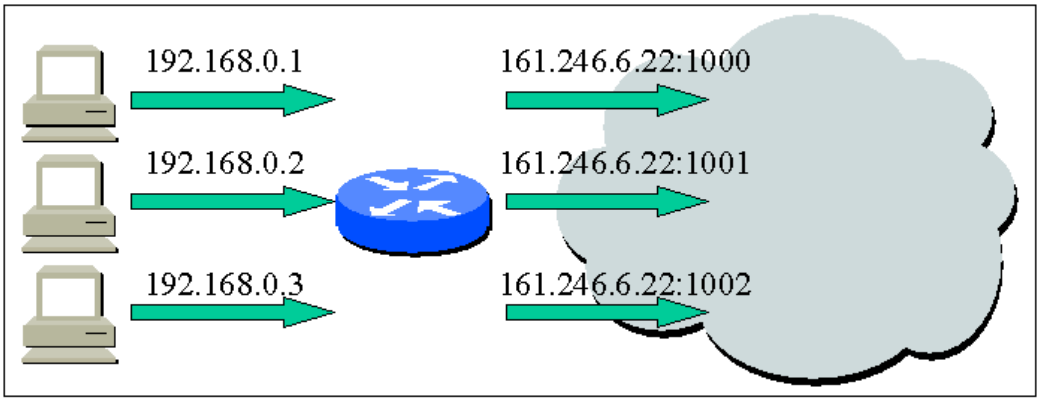


รูปที่ 40 Dynamic NAT

- Network Address Port Translation

จากการทำงานของ Static NAT และ Dynamic NAT นั้นจะเห็นได้ว่าจำนวนของหมายเลขไอพีแอดเดรสที่จดทะเบียน จะต้องเท่ากับจำนวนหมายเลขไอพีแอดเดรสภายในเครือข่าย ซึ่งทำให้ยังจำเป็นต้องใช้จำนวนไอพีแอดเดรสจำนวนมากอยู่เช่นเดิม วิธีการหนึ่งที่ช่วยให้ประหยัดหมายเลขไอพีแอดเดรสคือการนำเอา

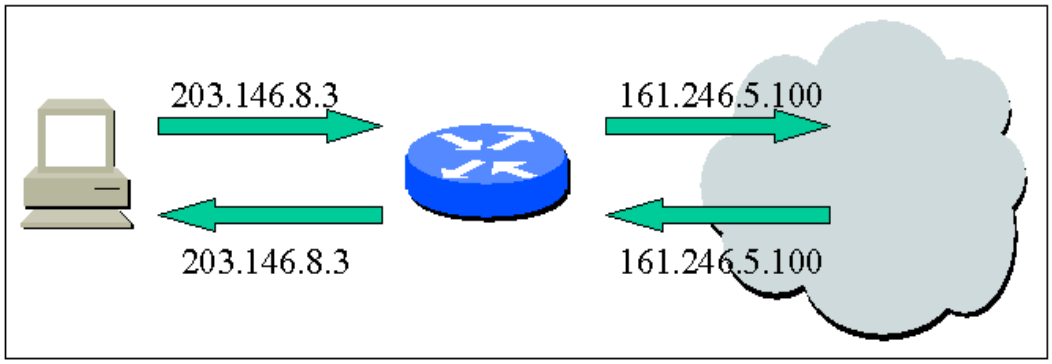
วิธีการของ NAPT มาใช้ โดยเครื่องคอมพิวเตอร์ในเครือข่ายที่เป็น Private IP เมื่อติดต่อไปยังเครือข่ายอื่นๆ จะถูกเปลี่ยนเป็นหมายเลขไอพีแอดเดรสเพียงหมายเลขเดียวแต่มีการเปลี่ยนแปลงหมายเลขพอร์ตต้นทางในการเชื่อมต่อแทน เมื่อมีการตอบกลับจากเครื่องภายนอกเครือข่ายแล้ว ที่อุปกรณ์ NAT จะดูหมายเลขพอร์ตปลายทางในส่วนหัวของข้อมูลว่าเป็นหมายเลขอะไร แล้วจึงเปลี่ยนข้อมูลส่วนหัวให้ตรงกับเครื่องคอมพิวเตอร์ที่ทำการร้องขออีกครั้ง



รูปที่ 41 Network Address Port Translation

- Twice-NAT

ในกรณีที่หมายเลขไอพีแอดเดรสในเครือข่าย เป็นหมายเลขไอพีแอดเดรสซึ่งใช้งานอยู่ในเครือข่ายอื่นๆ หรือเป็นหมายเลขไอพีแอดเดรสที่เรานำมาใช้งานกันเอง โดยไม่ได้จดทะเบียนขอใช้งาน เมื่อมีการเชื่อมต่อกับเครือข่ายอื่นๆ จะทำให้เกิดปัญหาขึ้นในระบบเครือข่าย แต่การใช้งานในลักษณะนี้ก็ยังสามารถใช้งานได้ แต่ต้องทำ NAT ให้กลายเป็นหมายเลขไอพีที่จดทะเบียนถูกต้องเสียก่อน



รูปที่ 42 Twice NAT

ข้อจำกัดของการทำ NAT

1. โปรแกรมที่มีข้อมูลของหมายเลขไอพีแอดเดรสอยู่ในชั้น Application Layer

เนื่องจากการทำ NAT มีการเปลี่ยนแปลงข้อมูลของเฮดเดอร์ของแพ็กเก็ต จึงทำให้การทำงานของโปรแกรมบางโปรแกรมที่มีข้อมูลของหมายเลขไอพีแอดเดรสที่จะต้องติดต่อด้วยอยู่ในส่วนของข้อมูลทำงานไม่ได้เนื่องจากไม่สามารถทำงานตามการทำงานโดยปกติได้ เนื่องจากข้อมูลหมายเลขไอพีในเนื้อข้อมูลเป็นหมายเลขไอพีแอดเดรสของเครื่องในเครือข่ายภายใน ซึ่งเป็นหมายเลข private IP ถ้าการทำงานต้องมีการเชื่อมต่อไปยังหมายเลขไอพีแอดเดรสดังกล่าว โปรแกรมนั้นจะไม่สามารถทำงานได้เลย ยกตัวอย่างเช่น SNMP เป็นต้น

นอกจากนี้ในกรณีที่โปรแกรมต้องมีการแลกเปลี่ยนหมายเลขพอร์ตกันโดยใช้การทำงานในชั้น Application Layer หรือมีการรับส่งข้อมูลหมายเลขพอร์ตกันในเนื้อข้อมูลชั้นแอปพลิเคชั่น ก็จะทำให้การทำงานของโปรแกรมมีปัญหาได้ในกรณีที่มีการทำ NAPT เพราะจะได้หมายเลขพอร์ตที่ผิดไปได้

2. โปรแกรมที่มีความสัมพันธ์ระหว่าง control session กับ data session

การทำงานของอุปกรณ์ NAT นั้นอยู่บนสมมุติฐานที่ว่าแต่ละ session นั้นมีการทำงานแยกจากกันโดยอิสระ ไม่มีความสัมพันธ์กันระหว่าง session ใดๆ หมายถึง เมื่อมีการสร้าง session ใดๆ จะมีหมายเลขไอพีแอดเดรสต้นทาง , หมายเลขไอพีแอดเดรสปลายทาง, โพรโตคอล , หมายเลขพอร์ตต้นทาง และหมายเลขพอร์ต

ปลายทาง เป็นตัวเลขที่ไม่ขึ้นกับหมายเลข หรือข้อมูลใน session อื่นๆ ถ้ามีโปรแกรมที่มีการสร้าง session ใหม่โดยขึ้นอยู่กับการควบคุมของ session อื่นๆ จะทำงานไม่ได้ถ้ามีการทำ NAT เนื่องจากภายหลังจากการทำ NAT ข้อมูลของ session จะถูกเปลี่ยนไปทั้งหมดนั่นเอง

ตัวอย่างของโปรแกรมที่มีการทำงานที่มีความสัมพันธ์ระหว่าง control session และ data session เช่น โปรแกรมที่ใช้ H.323 ซึ่งโปรแกรมประเภทนี้จะใช้ control session ในการกำหนดลักษณะการทำงานของ session อื่นๆโดยใช้ข้อมูลใน control session นั้น

3. การตรวจจับหาความผิดปกติต่างๆ ในระบบเครือข่าย

เนื่องจากการทำ NAT จะมีการเปลี่ยนแปลงข้อมูลจากหมายเลขไอพีแอดเดรสภายในเครือข่ายให้เป็นหมายเลขไอพีแอดเดรสที่มีการจดทะเบียน โดยมีการใช้งานหมายเลขไอพีแอดเดรสต่างๆ แบบสุ่ม และเปลี่ยนแปลงไปตลอดเวลา ทำให้การตรวจจับหาผู้กระทำผิดเช่นการส่ง SPAM Mail หรือการโจมตีไปยังเครือข่ายอื่นๆ ทำได้ยากเนื่องจากข้อมูลมีการเปลี่ยนแปลงอยู่ตลอดเวลา

4. การประมวลผลในอุปกรณ์ NAT

เนื่องจากการทำงานในอุปกรณ์ NAT จะต้องมีการคำนวณหาค่า checksum ของข้อมูลทุกๆ แพ็กเก็ต จึงทำให้การทำงานในเครือข่ายที่มีการทำ NAT ช้าลงได้

ตัวอย่างปัญหาอื่นๆ ที่เกิดขึ้นในการทำ NAT

- เป็นการปกปิดรายละเอียดของเครือข่ายภายในองค์กรแต่ก็ยังมีปัญหาในการทำงานอื่นๆเช่นการทำงานของโปรแกรมบางโปรแกรม
- มีปัญหากับการทำงานของ DNS (“A” and “PTR” query) , SNMP , FTP (port command , PASV command), โปรแกรมที่มี content ที่เป็นหมายเลขไอพีแอดเดรส, การทำ IPSec (ipsec tunnel ทำได้ถ้าให้ nat router เป็น tunnel end point)

- มีปัญหากับ App เช่น H.323 ที่ใช้ control หลาย session ซึ่งต้องใช้ การทำงานพิเศษเช่น payload interpretion gateway เข้าช่วย
- ไม่สนับสนุน ICMP , NetBIOS over TCP/IP , Real Audio , Video Live , IP multi cast
- มีปัญหากับ routing table update , DNS , Zone transfer , Bootp , Ntalk , talk

Security Consideration

- เพื่อไม่ให้ผู้บุกรุกเห็นว่ามีการใช้ NAT device จึงไม่ควรมีข้อมูลของ private ip ส่งออกไปยังเครือข่าย internet
- ควรตรวจสอบทั้งหมายเลขไอพีแอดเดรสต้นทาง , หมายเลขไอพีแอดเดรสปลายทาง , พอร์ตต้นทาง และพอร์ตปลายทางที่ใช้ในการเชื่อมต่อด้วยเพื่อป้องกันการปลอมแปลงหมายเลขไอพีแอดเดรสและพอร์ต ได้ เพราะอาจมีผู้ไม่หวังดีทำการ ปลอมหมายเลขไอพีแอดเดรสให้เหมือนกับมาจากเครื่องคอมพิวเตอร์ที่เครือข่ายภายในแล้วเชื่อมต่อไปยังเครื่องของตน แล้วเข้าเข้ามาโจมตีเครือข่าย
- การใช้ multicast session อาจทำให้เกิดปัญหาความปลอดภัยใน basic NAT ได้เนื่องจากระบบจะไม่สามารถทราบได้เลยว่าข้อมูลที่ตอบกลับมานั้นเป็นข้อมูลที่ตอบกลับมาจากการร้องขอจากเครื่องคอมพิวเตอร์ภายในเครือข่ายภายในหรือจากผู้บุกรุก
- อุปกรณ์ NAT เป็นเป้าหมายในการโจมตีเช่นเดียวกับ server จึงควรมีการป้องกันในระดับเดียวกับการป้องกัน server

บทที่ 9. IP Security

ในสังคมอินเตอร์เน็ต ได้มีความตระหนักในเรื่องของความปลอดภัยและความเป็นส่วนตัวมานานแล้ว ดังจะเห็นได้จากความพยายามในการสร้างระบบความปลอดภัยสำหรับงานต่าง ๆ ขึ้นมา เช่น E-Mail Security (PGP, S/MIME), Authentication (Kerberos), Web Access (SSL : Secure Socket Layer) และระบบอื่น ๆ อย่างไรก็ตาม ในการเชื่อมต่อระหว่างคอมพิวเตอร์ คงไม่ได้มีเพียงแอปพลิเคชันดังที่ได้กล่าวมาเท่านั้น และการสร้างระบบความปลอดภัยให้กับแต่ละแอปพลิเคชัน ก็เป็นเรื่องที่ไม่ง่าย เพราะจะเกี่ยวข้องกับการกำหนดมาตรฐานใหม่ ๆ ขึ้นเป็นจำนวนมาก ดังนั้นวิธีการหนึ่งที่ดีกว่า คือ การนำระบบความปลอดภัย ใส่เข้าไปในระดับ IP เสียเลย ซึ่งทำให้แอปพลิเคชันอะไรก็ตามที่ทำงานอยู่บนระดับ IP ก็จะได้อานิสงค์ แห่งความปลอดภัยนั้นไปด้วย

ระบบความปลอดภัยในระดับ IP หรือเรียกย่อ ๆ ว่า IPSec นั้น มีหน้าที่ในการให้บริการอยู่ 3 หน้าที่ด้วยกัน คือ ระบบการพิสูจน์ตน (Authentication) ซึ่งมีหน้าที่ในการพิสูจน์ว่าแพ็กเกจนั้นถูกส่งมาจากใคร และมีการเปลี่ยนแปลงเนื้อหาระหว่างทางหรือไม่ การรักษาความลับ (Confidential) มีหน้าที่เข้ารหัสข้อมูลเพื่อป้องกันไม่ให้ผู้อื่นสามารถอ่านได้ และการบริหารคีย์ (Key Management) ทำหน้าที่ในการแลกเปลี่ยนคีย์ระหว่างทั้ง 2 ฝั่งอย่างปลอดภัย

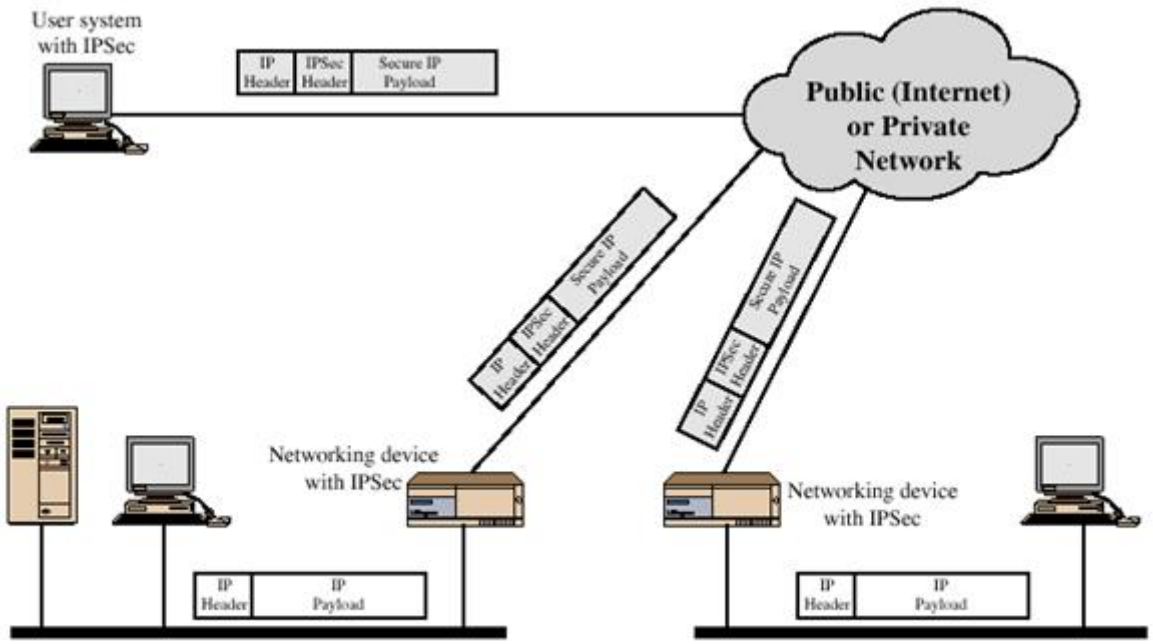
IP Security Overview

ในปี 1994 IAB (Internet Architecture Board) ได้มีการจัดทำรายงานขึ้นฉบับหนึ่ง มีชื่อว่า Security in the Internet Architecture (RFC 1636) โดยในรายงานดังกล่าวชี้ให้เห็นว่า มีความต้องการให้เครือข่ายอินเตอร์เน็ตมีความปลอดภัยมากยิ่งขึ้น และรายงานฉบับดังกล่าวยังได้ชี้จึงจุดต่าง ๆ ที่ควรจะมีการปรับปรุงอีกด้วย ซึ่งหนึ่งในความต้องการ คือ ต้องการให้มีความปลอดภัยในระดับโครงสร้างพื้นฐาน (Infrastructure) โดยควรจะป้องกันการลักลอบแอบดูข้อมูล และ การพิสูจน์ผู้ส่งได้

นอกจากนั้นในปี 1988 CERT (Computer Emergency Response Team) ก็ได้รายงานว่าได้รับรายงานมากกว่า 1300 รายงาน ในการโจมตีมากกว่า 20,000 แห่ง ว่ารูปแบบการโจมตีที่พบมาก คือ การโจมตีโดยการปลอม IP (IP Spoofing) โดยผู้โจมตีจะใช้วิธีสร้างแพ็กเกจ โดยปลอมหมายเลข IP ขึ้นมา แล้วเข้าโจมตีในบางแอปพลิเคชัน ที่อ้างอิงความปลอดภัยกับหมายเลข IP และรูปแบบการโจมตีที่พบมากอีกอย่างหนึ่ง คือ การใช้โปรแกรมลักษณะ Sniffer เพื่อดักดูข้อมูลต่าง ๆ

และจากรายงานดังกล่าว IAB ได้ตัดสินใจจะเพิ่มความสามารถทางด้าน Authentication และ Encryption เข้าไปใน Ipv6 นอกจากนั้นยังได้ออกแบบระบบความปลอดภัยให้สามารถใช้ได้ทั้ง Ipv6 และ Ipv4 อีกด้วย ซึ่งหมายความว่า หากต้องการความสามารถต่าง ๆ เหล่านี้ ก็ไม่จำเป็นต้องรอ IPv6 โดยสามารถนำมาใช้กับ Ipv4 ได้ทันที โดยจะเรียกความสามารถด้านความปลอดภัยใน Ipv4 ว่า IPSec

สำหรับรูปแบบการใช้งานของ IPSec นั้น เราอาจใช้ IPSec ในการเชื่อมต่อระหว่างสำนักงานสาขา (Branch Office) โดยผ่านเครือข่ายอินเตอร์เน็ต หรือ ใช้ในการทำเชื่อมต่อระยะไกล (Remote Access) ผ่านเครือข่ายอินเตอร์เน็ต หรือ ใช้ในการเชื่อมต่อระหว่างเครือข่ายแบบ Intranet และ Extranet ระหว่างองค์กร หรือใช้ในการสื่อสารแบบ Electronics Commerce ทั้งนี้เนื่องจาก IPSec นั้นสามารถทั้งด้าน Authentication และ Encryption ในทุก ๆ การสื่อสารที่มีพื้นฐานบนระดับ IP ในรูปที่ 43 ได้แสดงรูปแบบการใช้งานปกติของ IPSec โดยการสื่อสารภายในวง LAN แต่ละวงจะเป็นการสื่อสารตามปกติ แต่เมื่อการสื่อสารได้ก้าวข้ามออกไปภายนอก ไม่ว่าจะเป็นเครือข่ายแบบ Private หรือ Public ก็ตาม ก็จะมีการใช้ IPSec โดยการนำ IPSec มาใช้นี้ จะเริ่มที่ Router, Firewall หรืออุปกรณ์เครือข่ายที่ทำหน้าที่เป็นจุดออก (Gateway) ของเครือข่าย โดยจะมีการเข้ารหัสข้อมูล แล้วจึงส่งออกไป และเมื่อถึงปลายทางก็จะถอดรหัสออกมา ซึ่งการทำงานทั้งหมดนี้ จะเกิดขึ้นโดยที่เครื่องคอมพิวเตอร์ไม่มีส่วนรับทราบเลย นอกจากนั้น IPSec ยังสามารถใช้งานในกรณีที่ผู้ใช้การเชื่อมต่อแบบ Dial-Up ได้อีกด้วย ไม่ว่าจะเป็นการเชื่อมต่อเข้ามาที่หน่วยงานนั้น ๆ โดยตรง หรือเป็นการเชื่อมต่อผ่านอินเตอร์เน็ต



รูปที่ 43 รูปแบบการใช้งาน IP Security

ประโยชน์ของ IPSec

- เมื่อมีการนำ IPSec มาใช้ที่ Firewall หรือ Router จะทำให้มีระบบความปลอดภัยที่แข็งแกร่ง ที่สามารถใช้ได้กับทุกการสื่อสาร โดยการสื่อสารภายในจะไม่มี Overhead ของ IPSec
- เมื่อมีการใช้ IPSec กับ Firewall ทุกการสื่อสารจะไม่สามารถข้าม IPSec ได้ เพราะการสื่อสารกับภายนอกต้องใช้ IP ซึ่งหมายความว่าต้องใช้ IPSec ด้วย และเนื่องจาก Firewall เป็นเพียงจุดเดียวที่เชื่อมต่อกับภายนอก ดังนั้นการติดต่อระหว่างภายในและภายนอกก็จะต้องทำโดยผ่าน IPSec เท่านั้น
- เนื่องจาก IPSec ทำงานอยู่ใต้ TCP และ UDP ดังนั้นแอปพลิเคชันที่ทำงานบน TCP และ UDP จึงต้องทำงานผ่าน IPSec ไปด้วย และไม่ต้องรับรู้ถึงการมีอยู่ของ IPSec ดังนั้นโปรแกรมต่าง ๆ ก็ไม่ต้องเขียนขึ้นมาใหม่
- การทำงานของ IPSec ไม่กระทบกับผู้ใช้ โดยผู้ใช้จะไม่รับรู้ถึงการมีอยู่ของ IPSec เลย ดังนั้นจึงไม่ต้องเสียค่าใช้จ่ายในการสอนผู้ใช้

- IPSec สามารถจะสร้างความปลอดภัยในระดับผู้ใช้ได้ ซึ่งเป็นผลดีที่ทำให้สามารถจะระบุถึงผู้ใช้แต่ละคนที่เข้ามาใช้งานจากระยะไกลได้

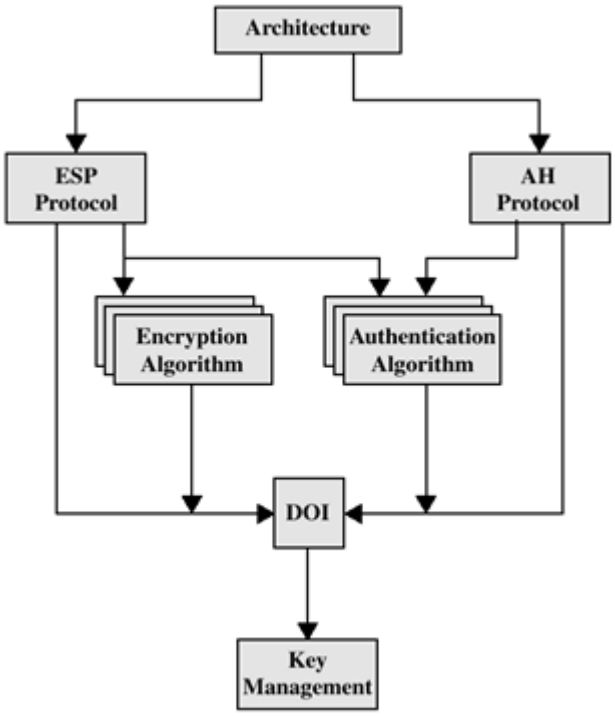
นอกจากนั้น IPSec ยังช่วยให้การทำงานของ Routing Protocol มีความปลอดภัยมากยิ่งขึ้น เพราะช่วยให้การทำงานต่าง ๆ ไม่ว่าจะเป็น Router Advertisement, Neighbor Advertisement หรืออื่น ๆ สามารถใช้ความสามารถของ IPSec ในการเข้ารหัสข้อมูล และพิสูจน์ถึง Router จริง ๆ ได้

IP Security Architecture

ข้อกำหนดของ IPSec นั้น ถือได้ว่ามีความซับซ้อนมากพอสมควร โดยได้ถูกกำหนดไว้ในเอกสารดังต่อไปนี้

- RFC 2401 : An overview of a security architecture
- RFC 2402 : Description of a packet authentication extension to Ipv4 and Ipv6
- RFC 2406 : Description of a packet encryption extension to Ipv4 and Ipv6
- RFC 2408 : Specification of key management capability

ข้อกำหนดดังกล่าวถือเป็นข้อบังคับของ IPV6 และเป็นออปชันของ IPV4 โดยการใช้ IPSec ในทั้ง 2 รูปแบบ จะใช้ในลักษณะของการขยายส่วนหัว โดยส่วนหัวนี้จะทำหน้าที่ Authentication ด้วย โดยส่วนของข้อมูลที่เข้ารหัสจะเรียกว่า Encapsulating Security Payload (ESP) และนอกจาก RFC ทั้ง 4 ฉบับที่กล่าวไปแล้ว ยังมีการจัดตั้ง IP Security Protocol Working Group ขึ้นโดย IETF เพื่อกำหนดมาตรฐานอื่น ๆ ที่เกี่ยวข้อง โดยได้มีการแบ่งออกเป็น 7 กลุ่ม ดังรูปที่ 44



รูปที่ 44 องค์ประกอบของ IP Security

ในการทำงานของ IPSec นั้นจะมีส่วนการทำงานอยู่ 2 ส่วนหลักด้วยกัน โดยส่วนแรกก็คือ Authentication Header หรือ AH และส่วนที่ 2 คือ ESP โดยจะมีงานที่ส่วนต่าง ๆ เกี่ยวของอยู่ทั้งหมด 6 งาน ด้วยกัน ดังแสดงในตาราง

	AH	ESP (Encryption Only)	ESP (Encryption and Authentication)
Access Control	Y	Y	Y
Connectionless Integrity	Y		Y
Data Origin Authentication	Y		Y
Rejection of Replayed Packets	Y	Y	Y
Confidentiality		Y	Y
Limited Traffic Flow Confidentiality		Y	Y

ในการสื่อสารระหว่าง 2 ฝั่ง จะมีการสร้าง Security Associations (SA) ขึ้น โดย SA นี้จะเป็นความสัมพันธ์แบบทางเดียว ดังนั้นหากต้องการสื่อสารทั้ง 2 ทาง ก็จะต้องสร้าง SA ขึ้นในทั้ง 2 ทิศทาง โดยแต่ละ SA จะระบุโดยข้อมูล 3 ตัวร่วมกัน คือ

- SPI (Security Parameter Index) เป็น Bit String ที่กำหนดให้กับ SA โดย SPI นี้จะส่งไปพร้อมกับ IPSec Packet เพื่อให้ฝั่งตรงข้าม สามารถเลือก SA ที่ถูกต้องมาใช้งานได้
- IP Destination Address เป็น IP Address ของเครื่องหรืออุปกรณ์เป้าหมาย
- Security Protocol Identifier เป็นตัวบอกว่า SA นี้สัมพันธ์กับส่วนของ AH หรือ ESP ดังนั้นถ้าจะใช้ทั้งคู่ ก็ต้องใช้ SA จำนวน 2 ชุด

ดังนั้นใน IP Packet ใด ๆ จึงมี SA Identifier ที่ไม่ซ้ำกันเลย โดยในระบบ IPSec แต่ละระบบนั้น จะมีฐานข้อมูลที่ทำหน้าที่เก็บ SA (Security Association Database) โดยจะเก็บ SA แต่ละตัว และพารามิเตอร์ของแต่ละ SA นั้น สำหรับพารามิเตอร์ของ SA จะมีดังต่อไปนี้

- Sequence Number Counter เป็นเลข 32 บิต ทำหน้าที่สร้างเลขลำดับใน AH หรือ ESP Header
- Sequence Number Overflow เป็นเฟล็กที่บอกว่า Sequence Number เกิด Overflow ขึ้น
- Anti-Replay Windows ทำหน้าที่บอกว่า AH หรือ ESP นี้เกิดจากการ Replay หรือไม่
- AH Information ทำหน้าที่บอกอัลกอริทึมของ AH, Key, Key Lifetime และอื่น ๆ (AH)
- ESP Information ทำหน้าที่บอกอัลกอริทึมของการเข้ารหัสและ Authentication, Key, ค่าเริ่มต้น, Key Lifetime และอื่น ๆ (ESP)
- Lifetime of this Security Association บอกระยะเวลาหรือจำนวนไบต์ ที่จะเปลี่ยน SA ใหม่ หรือเลิกใช้ SA ปัจจุบัน
- IPSec Protocol Mode ทำหน้าที่ระบุโหมดการทำงานของ IPSec (Transport หรือ Tunnel)
- Path MTU ทำหน้าที่เก็บค่า MTU ที่จะสามารถส่งได้โดยไม่ต้อง Fragmentation

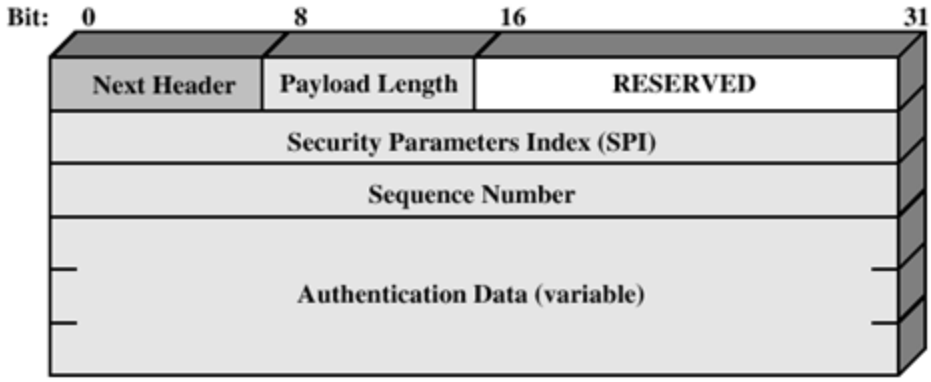
โดยในการสื่อสารนั้น อาจจะมีการสื่อสารได้ทั้งแบบที่ใช้ IPSec (ซึ่งต้องระบุ SA) และไม่ใช้ IPSec (ซึ่งไม่ต้องระบุ SA) โดยจะมี SPD (Security Policy Database) ทำหน้าที่กำกับการสื่อสาร โดยใน SPD จะมีรายการ

สื่อสารต่าง ๆ โดยรายการใดที่เป็นการสื่อสารแบบ IPSec ก็จะมีตัวชี้ไปยัง SA ที่เหมาะสมด้วย ซึ่งอาจมีหลายการสื่อสารที่ชี้ไปยัง SA เดียวกันก็ได้ โดยการเลือกการแต่ละรายการที่เหมาะสมกับแต่ละการสื่อสารนั้น จะใช้หมายเลข IP Address และค่าต่าง ๆ ในโพรโตคอลที่อยู่ในระดับที่สูงขึ้นไป ของแพ็กเกจที่ส่งออกไป โดยจะเรียกข้อมูลทั้ง 2 ว่า SA Selector โดยในแต่ละการส่ง จะมีการเข้าไปค้นหาใน SPD และจะตรวจสอบว่ามีการชี้ไปยัง SA ใด ๆ หรือไม่ หากชี้ก็จะนำพารามิเตอร์ของ SA นั้นมาใช้ แต่หากไม่ชี้ ก็จะส่งแบบปกติ โดยข้อมูลที่จะใช้ในการกำหนดแต่ละรายการใน SPD จะมีดังนี้

- Destination IP Address อาจเป็นหมายเลขเดียว หรือเป็น Wildcard (mask) หรือเป็นช่วงก็ได้
- Source IP Address อาจเป็นหมายเลขเดียว หรือเป็น Wildcard (mask) หรือเป็นช่วงก็ได้
- UserID ส่วนนี้ไม่ได้เป็นข้อมูลใน IP Packet แต่อนุญาตให้ใช้ หากระบบปฏิบัติการต้องการเพิ่มส่วนนี้เข้าไป
- Data Sensitivity Level ใช้ในระบบที่มีการให้ระดับความปลอดภัยของข้อมูล เช่น Secret หรือ Unclassified
- Transport Layer Protocol นำมาจากฟิลด์ในส่วนหัวของ Ipv4 หรือ Ipv6
- IPSec Protocol (AH หรือ ESP หรือ AH/ESP) ถ้ามี หมายความว่านำมาจาก ส่วนหัวของ Ipv4 หรือ Ipv6
- Source and Destination Port เป็นหมายเลขพอร์ตที่ติดต่อ
- Ipv6 Class นำมาจากฟิลด์ในส่วนหัวของ Ipv6
- Ipv6 Flow Label นำมาจากฟิลด์ในส่วนหัวของ Ipv6
- Ipv4 Type of Service นำมาจากฟิลด์ในส่วนหัวของ Ipv4

Authentication Header

ส่วนของ AH จะสนับสนุนทั้งส่วน Data Integrity และส่วน Authentication โดยสามารถจะรับรองได้ว่าข้อมูลที่ส่งจะไม่มีการแก้ไขระหว่างทาง ที่ตรวจสอบไม่ได้ และสามารถพิสูจน์ผู้ส่งได้ ว่าส่งจากเครื่องใด จากผู้ใช้คนใด หรือจากแอปพลิเคชันใด นอกจากนั้นยังสามารถป้องกัน Spoofing Attack และ Replay Attack ได้ด้วย ซึ่งส่วนของ Authentication Header ดูจากรูปที่ 45



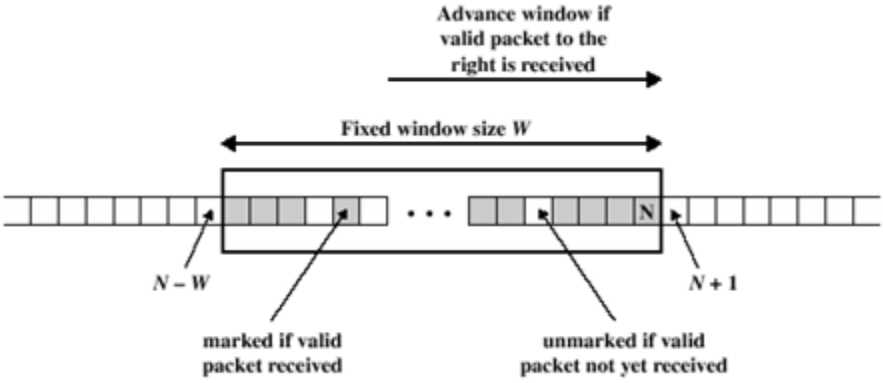
รูปที่ 45 Authentication Header

จากรูปจะมีรายละเอียดดังนี้

- Next Header (8 bit) ทำหน้าที่ระบุชนิดของ Header ว่าเป็น AH หรือ ESP
- Payload Length (8 bit) ทำหน้าที่ระบุความยาวของ AH โดยหน่วยเป็น 32 bitword –2
- Reserved (16 bit) สำรองไว้ในในอนาคต
- Security Parameter Index (32 bit) ทำหน้าที่ระบุ SA
- Sequence Number (32 bit) เป็นเลขลำดับการส่ง
- Authentication Data (Variable) เป็นข้อมูลสำหรับตรวจสอบความถูกต้อง หรือ MAC ของแพ็กเกจ

การโจมตีอย่างหนึ่งที่ IPSec จะยอมให้เกิดขึ้นไม่ได้ คือ Replay Attack ซึ่งจะใช้ฟิลด์ Sequence Number ในการตรวจสอบลำดับของแพ็กเกจ โดยหลังจากที่เชื่อมต่อโดยใช้ SA แล้วฝั่งส่งจะมีการสร้าง Sequence Number ค่า 1 และเพิ่มขึ้นเรื่อย ๆ โดยจะไม่มีการกลับมาใช้ใหม่ อย่างไรก็ตาม เนื่องจาก IP ทำงานแบบ Connectionless ดังนั้นการส่งอาจไม่เป็นไปตามลำดับ ดังนั้นฝั่งรับจะต้องสร้าง Windows ขึ้นมา โดยมีขนาด 64

(Default) ดังนั้นหากลำดับของ Sequence Number ยังอยู่ในช่วงของ Windows ก็ถือว่าลำดับถูกต้อง และจะส่งไปตรวจสอบต่อไป โดยรูปที่ 46 แสดงการทำงานของ Windows ใน IPSec



รูปที่ 46 การป้องกัน Replay Attack โดย Sliding Windows

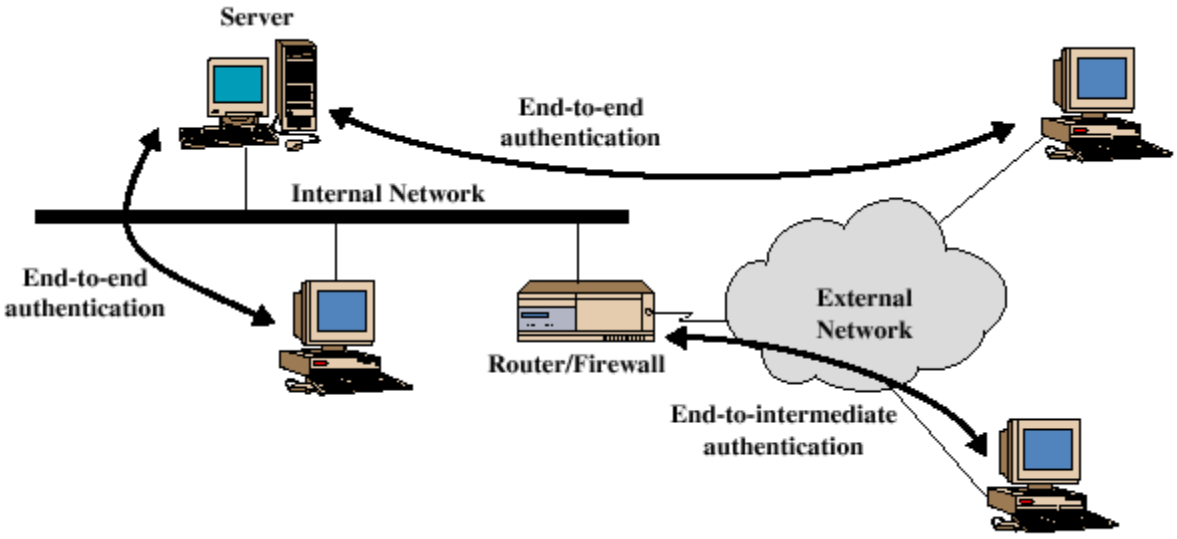
สำหรับการตรวจสอบความถูกต้องนั้น จะใช้อัลกอริทึม MAC โดยสามารถใช้ได้ทั้ง HMAC-MD5 และ HMAC-SHA-1 โดยทั้ง 2 วิธีจะใช้ความยาวของ Message Digest เพียง 96 บิตเท่านั้น (โดยการ Truncate) โดยจะทำทั้งส่วนของ IP Header, AH และ ส่วนของ Payload หรืออัลกอริทึมอื่น ๆ ก็ได้

ในการทำงานของทั้ง AH และ ESP จะมีโหมดการทำงานให้ใช้อยู่ 2 โหมดด้วยกัน ดังนี้

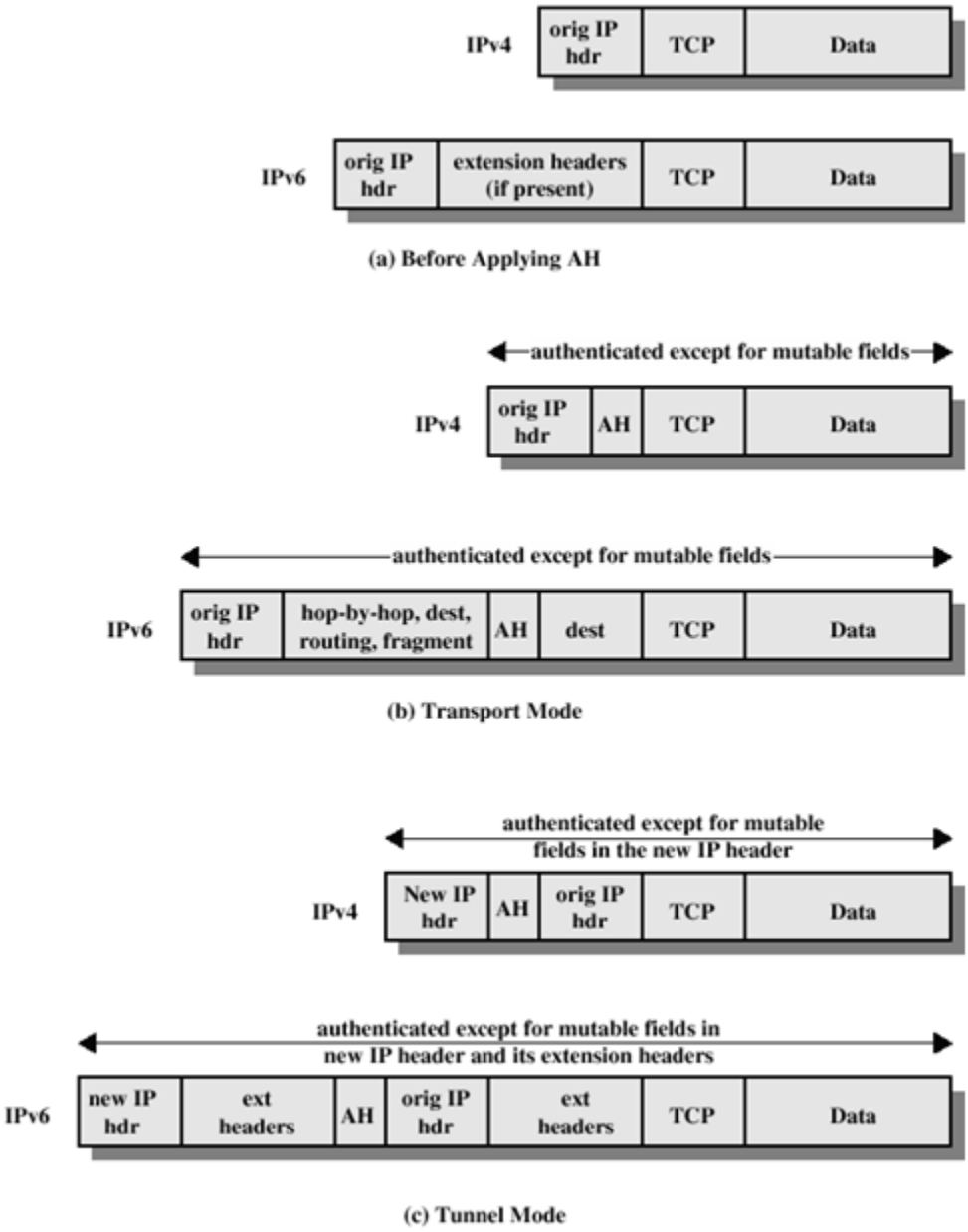
- โหมด Transport มีเป้าหมายที่จะป้องกันส่วนของข้อมูลที่อยู่ในชั้นที่สูงขึ้นไป ได้แก่ TCP, UDP และ ICMP โดยทั่วไปจะใช้ในลักษณะ End to End ระหว่างเครื่องคอมพิวเตอร์ 2 เครื่อง โดยเครื่องทั้ง 2 เครื่องอาจมีการ Authenticate โดยใช้ Shared Key หรือโดย PKI ก็ได้ โดยรูปที่ 47 แสดงลักษณะการทำงานของโหมดนี้ และรูปที่ **48** แสดงลักษณะแพ็กเกจที่แตกต่างของทั้ง 2 โหมด
- โหมด Tunnel มีเป้าหมายในการป้องกันทั้งแพ็กเกจ โดยเมื่อมีการปะส่วนของ AH และ ESP แล้วจะมองว่าข้อมูลทั้งหมดจะเป็นส่วนของ Payload ที่ต้องปกป้อง ดังนั้นจะมีการสร้างแพ็กเกจ IP ขึ้นมาใหม่ และนำ Payload ไปใส่ในแพ็กเกจใหม่นี้ สำหรับการใช้งานในโหมดนี้ มักจะใช้ในกับ Router หรือ Firewall โดยเครื่องคอมพิวเตอร์หรือ User จะต้อง Authenticate กับ Router หรือ Firewall เพื่อขอใช้บริการเพื่อออกสู่ภายนอก สำหรับ Firewall หรือ Router ของทั้ง 2 ฝั่ง ก็จะต้องมีการ Authenticate ซึ่งกันและกันเอง โดยเมื่อแพ็กเกจไปถึง Firewall หรือ Router ก็จะมีการจับใส่

Packet ใหม่ และเมื่อถึง Router หรือ Firewall ปลายทาง ก็จะมีการถอดแพ็กเกจข้างนอกออก ให้เหลือแต่แพ็กเกจข้างใน แล้วส่งต่อไป

ในทั้ง 2 โหมดนี้ ตามปกติหากเป็นการติดต่อในลักษณะจาก Client ไปยัง Server หรือลักษณะของ Dial Up ก็จะใช้โหมด Transport แต่หากเป็นการเชื่อมต่อระหว่างสำนักงานสาขาแล้ว มักจะใช้โหมด Tunnel โดยในโหมด Tunnel นั้นจะมีข้อดีที่เครื่องคอมพิวเตอร์ที่อยู่ภายใน จะไม่ต้องรับรู้ถึงการใช้งาน IPSec เลย เพราะ IPSec จะสร้างที่ Gateway แต่วิธีการนี้มีข้อเสีย คือ ไม่สามารถป้องกัน การลักลอบอ่าน หรือปลอมแปลง ที่เกิดจากเครือข่ายภายในได้ แต่สำหรับแบบ Transport แล้วระบบจะต้องสนับสนุน IPSec โดยตรง และจะต้องมีการเข้าไปกำหนด Configuration การทำงานอีกด้วย



รูปที่ 47 รูปแบบการ Authentication

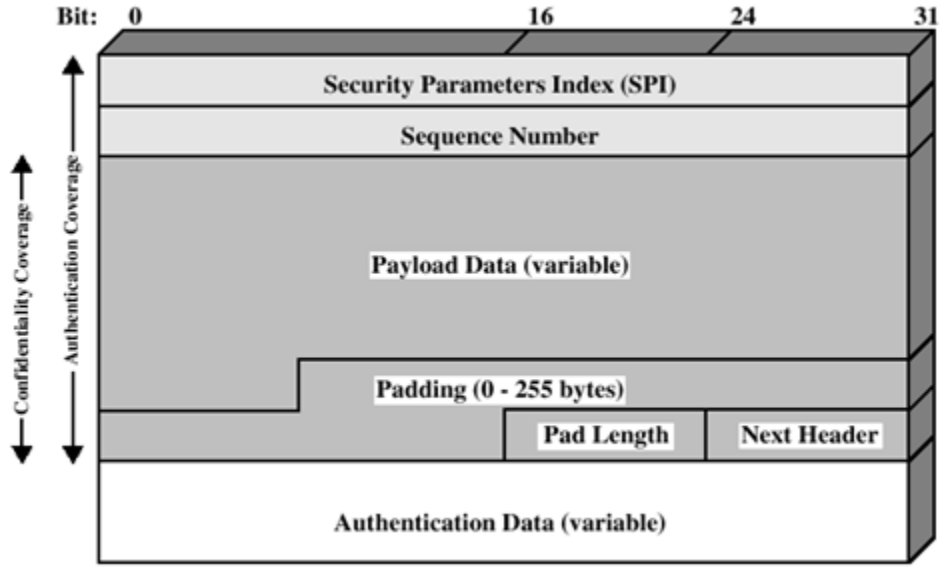


รูปที่ 48 Scope of AH Authentication

Encapsulation Security Payload (ESP)

สำหรับส่วนของ ESP ซึ่งทำหน้าที่ให้บริการการเข้ารหัสนั้น มีลักษณะของฟิลด์อยู่ในรูปที่ 49 โดยรายละเอียดของฟิลด์ต่าง ๆ มีดังต่อไปนี้

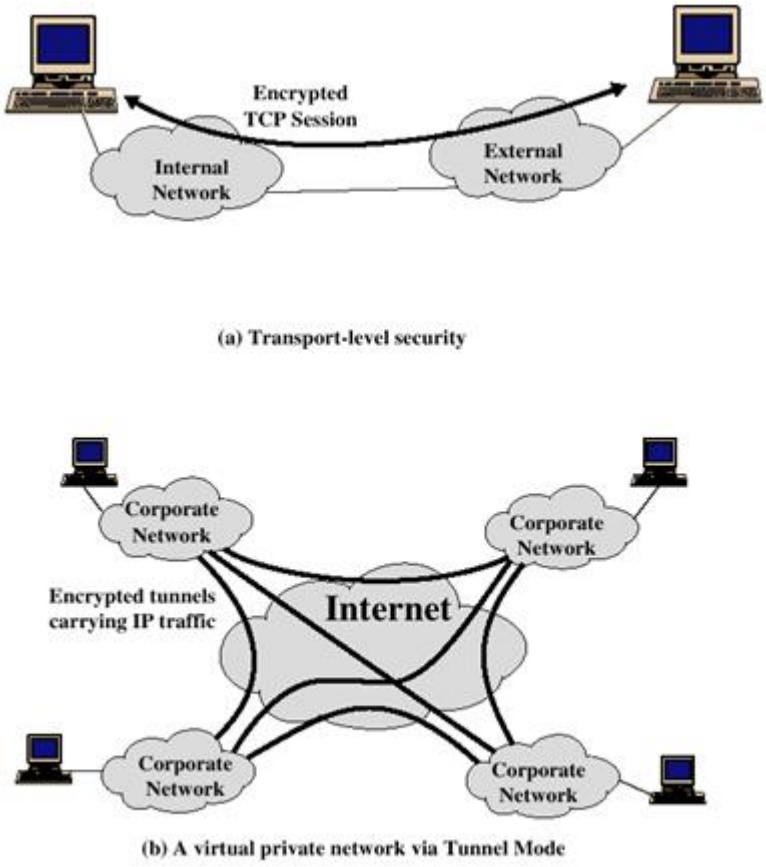
- Security Parameters Index (32 bit) ทำหน้าที่ระบุ SA
- Sequence Number (32 bit) เป็นหมายเลขลำดับ เพื่อป้องกัน Replay Attack
- Payload Data (Variable) ส่วนของข้อมูลที่เข้ารหัส
- Padding (0-255 byte) ข้อมูลที่เพิ่มเข้าไปกรณีที่เป็น Block Encryption และเพื่อให้หารด้วย 32 บิตลงตัว
- Pad Length (8 bit) เป็นความยาวของข้อมูลที่ Pad
- Next Header (8 bit) ทำหน้าที่ระบุชนิดของ Header ในแพ็กเกจถัดไป
- Authentication Data (Variable) เป็นส่วนที่ใช้ตรวจสอบผู้ส่ง และความถูกต้อง



รูปที่ 49 ESP Format

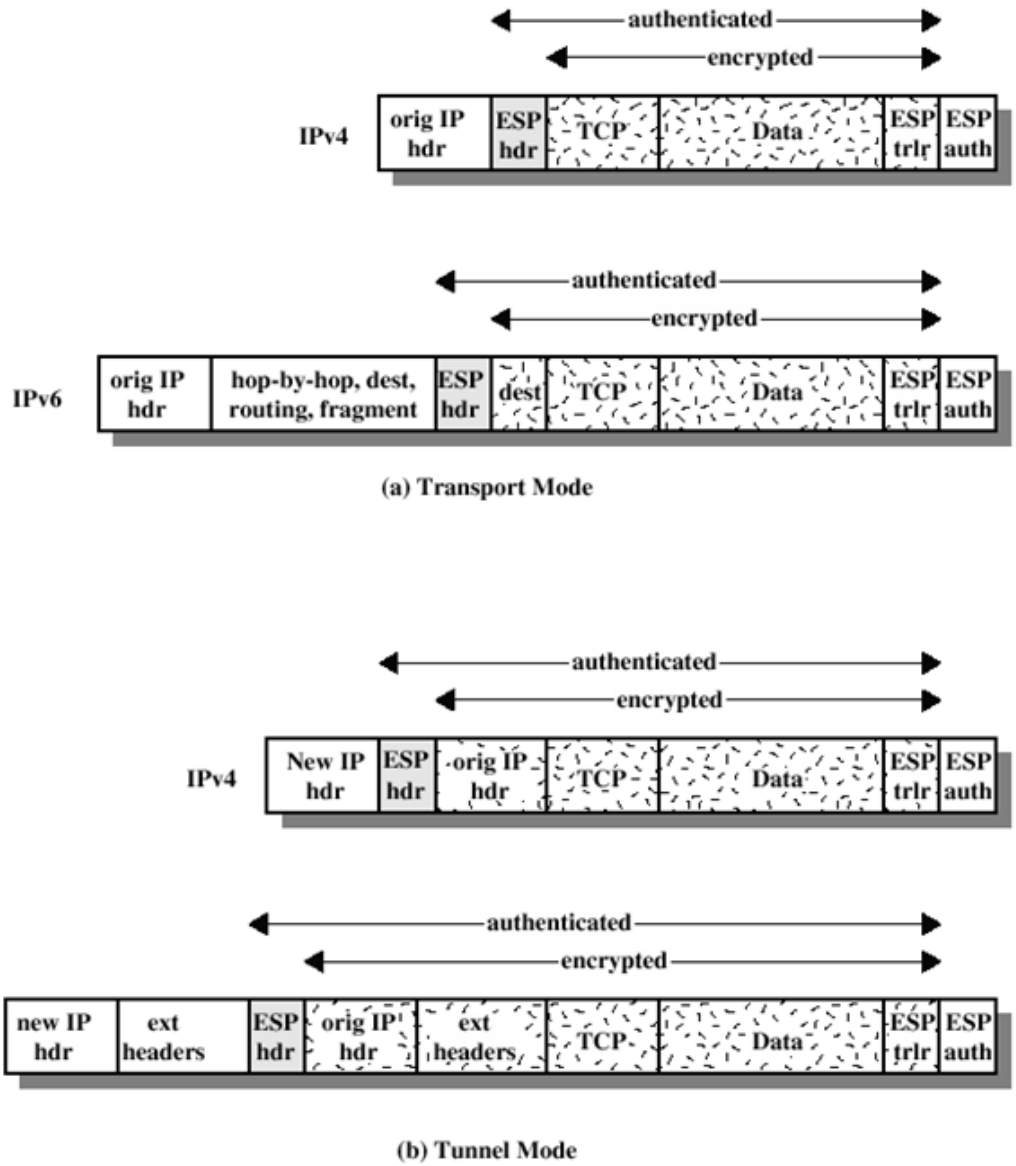
ในส่วนของการเข้ารหัสนั้น จะเข้ารหัสในส่วนของ Payload Data, Padding, Pad Length และ Next Header โดยสามารถใช้อัลกอริทึม DES, 3DES, RC5, IDEA, 3IDEA, CAST และ Blowfish โดยทำงานในโหมด

Cipher Block Chaining และสำหรับส่วน Authentication จะเหมือนกับ AH โดยในรูปที่ **50** แสดงการทำงานของโหมด Transport และ Tunnel ใน ESP



รูปที่ 50 Transport Mode & Tunnel Mode

จากรูปที่ 50(a) แสดงการทำงานของ ESP แบบ Transport โดยจะมีการเข้ารหัส (โดยมีการ Authenticate เป็นตัวเลือก) ระหว่างคอมพิวเตอร์ทั้ง 2 ฝั่ง และรูปที่ 50(b) แสดงการทำงานในแบบ Tunnel ซึ่งสามารถใช้ IPSec ในโหมดนี้ในการสร้าง Virtual Private Network หรือ VPN ได้ โดยจากรูปจะสมมติว่ามีสาขาอยู่ 4 สาขา และมีการกำหนด VPN ระหว่างสาขาผ่านเครือข่ายอินเตอร์เน็ต โดยลักษณะของแพ็กเกจที่ใช้แสดงในรูปที่ **51** ซึ่งจะสังเกตว่าจะมีการเพิ่มส่วน ESP Trailer และ ESP Authen ต่อท้ายแพ็กเกจไว้ด้วย ซึ่ง ESP Trailer เป็นส่วน Padding, Pad Length และ Next Header) และส่วน ESP Authen. จะใช้ตรวจสอบทั้งส่วนที่เป็นข้อมูลและส่วนของ ESP Header (กรณีที่ไม่ต้องการ Authentication ก็จะไม่มีการเพิ่มส่วนของ ESP Authen เข้าไป



รูปที่ 51 Scope of ESP Encryption and Authentication

Combining Security Associations

ในแต่ละ SA นั้นสามารถใช้ได้กับ AH หรือ ESP อย่างใดอย่างหนึ่งเท่านั้น จะใช้ทั้ง 2 แบบไม่ได้ แต่เนื่องจากบางครั้งการส่งข้อมูลก็ต้องการทั้งบริการ AH และ ESP ซึ่งในกรณีนี้ จะต้องมีการใช้หลาย ๆ SA ต่อหนึ่งการสื่อสาร โดยจะเรียกว่า SA Bundle โดยแต่ละ SA จะถูกนำมาใช้งาน ณ จุดที่ต้องการใช้ และอาจจะสิ้นสุดการใช้ในจุดเดียวกัน หรือคนละจุดก็ได้ โดยการใช้ SA ร่วมกันนั้น จะมีวิธีการอยู่ 2 วิธีการ คือ

- Transport Adjacency ซึ่งจะเป็นการนำ SA หลาย ๆ SA ไปใช้กับ IP Packet เดียวกัน โดยไม่มีการทำ Tunneling ซึ่งวิธีการแบบนี้จะทำให้การรวมกันระหว่าง AH และ ESP สามารถทำได้เพียงชั้นเดียว
- Iterated Tunneling วิธีการนี้จะสามารถซ้อน AH หรือ ESP ได้หลายชั้น ซึ่งจะใช้ในกรณีที่มีการใช้งาน IPSec ซ้อนกันในลักษณะ Gateway ซ้อนหลาย ๆ ชั้น โดยแต่ละชั้นมีความต้องการไม่เหมือนกัน

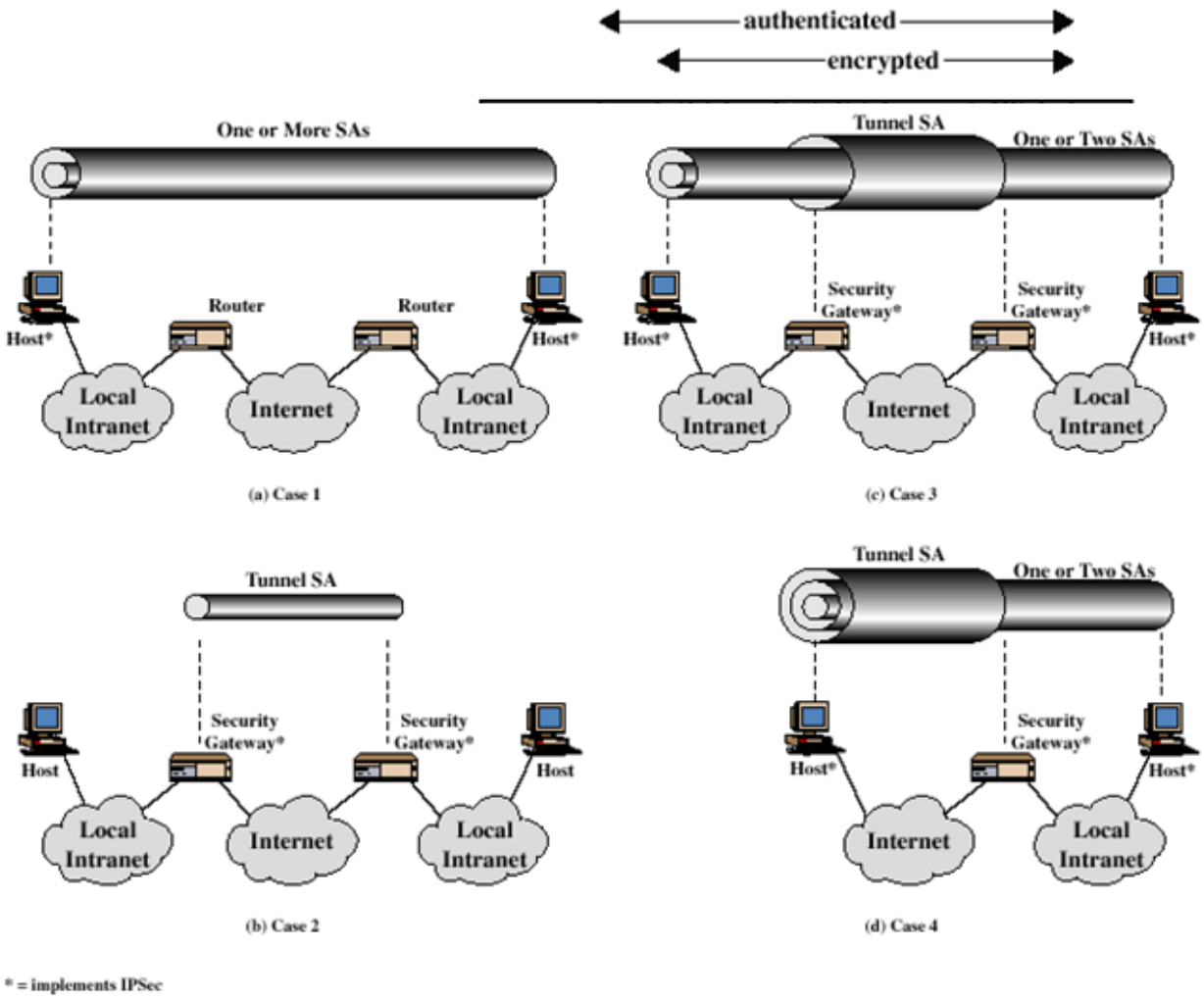
นอกจากนั้นวิธีการทั้ง 2 แบบ ยังสามารถใช้งานร่วมกันได้อีกด้วย เช่น มีการใช้ Transport SA ระหว่าง Host โดยผ่าน Tunneling ที่สร้างขึ้นระหว่าง Gateway ซึ่งทั้งหมดนี้ทำให้เกิดคำถามว่า ในการทำงานจริง ๆ จะมีการทำงานในรูปแบบใดกันแน่นี้ลองมายกตัวอย่างดู สมมติว่าต้องการส่งข้อมูลที่มีการเข้ารหัส และมีการ Authenticate ด้วย จะใช้วิธีการไหน เพราะสามารถจะใช้ได้ตั้งแต่ 1) ESP with authentication option ซึ่งหากเป็นกรณีเป็นการเชื่อมต่อจาก Host ไปยัง Host ก็ใช้แบบ Transport ESP หรือหากเป็นแบบ Gateway ก็ใช้แบบ Tunnel Mode ESP (แต่การ Authenticate จะเป็นการ Authenticate กับ Ciphertext) หรือ 2) Transport Adjacency โดยจัดให้มีการใช้ SA แบบ Transport Mode จำนวน 2 ครั้งโดยข้างในให้ใช้ ESP และข้างนอกให้ใช้ AH โดยการใช้ ESP ในกรณีนี้ จะไม่มีการใช้ Authentication Option ซึ่งหากเปรียบเทียบวิธีนี้กับวิธีแรกแล้ว วิธีการนี้จะครอบคลุมฟิลด์ที่ Authenticate มากกว่า โดยครอบคลุมไปถึง Source IP และ Destination IP ด้วย แต่ข้อเสียคือจะมี Overhead มากกว่า

แบบที่ 3 คือ ใช้ Transport –Tunnel Bundle โดยจะมีการใช้ AH ก่อน ทั้งนี้เพื่อให้การ Authenticate กระทำกับข้อมูลที่ยังไม่เข้ารหัส เพราะข้อมูลที่เข้ารหัสนั้น ปกติก็เปลี่ยนแปลงระหว่างทางได้ยากอยู่แล้ว จึงไม่จำเป็นต้อง Authenticate และการนำ Authenticate ไว้ข้างในจะทำให้สามารถเก็บข้อมูลที่ใช้ Authenticate ไว้ใช้ภายหลังได้อีกด้วย โดยใช้ Transport SA ที่ทำ AH ไว้ข้างในและ ESP Tunnel SA ไว้ข้างนอก สำหรับสาเหตุที่ใช้แบบ Tunnel ก็เพื่อให้มีการใช้ AH กับทั้ง Packet จากนั้นก็จะนำข้อมูลที่ได้ไปเข้ารหัส

คราวนี้เราจะมาดูตัวอย่างการใช้งาน โดยจะมีตัวอย่างให้ 4 แบบ ซึ่งแสดงไว้ในรูปที่ 52 โดยด้านบนจะแสดงลักษณะของการเชื่อมต่อ และด้านล่างจะแสดงลักษณะทางกายภาพของการใช้งาน สำหรับในกรณีที่ 1

ความปลอดภัยจะอยู่ที่ปลายทางทั้งสอง ซึ่งอาจจะโดยการใช้ Secret Key ร่วมกัน โดยอาจเป็นการทำงานได้หลายอย่าง เช่น Transport AH, Transport ESP, AH แล้วตามด้วย ESP สำหรับในกรณีที่ 2 นั้น จะมีระบบความปลอดภัยเฉพาะส่วนของ Gateway โดยไม่มีระบบ IPSec ที่ปลายทาง ซึ่งจะเป็นการทำงานในลักษณะของ VPN ซึ่งรูปแบบที่เหมาะสมกับการทำงานแบบนี้ ก็คือ การทำ Tunnel ชั้นเดียว ซึ่ง Tunnel นี้ อาจจะสนับสนุน AH หรือ ESP หรือ ESP with Authentication Option ก็ได้

ในแบบที่ 3 นี้ จะมีการใช้งาน IPSec ทั้งในส่วนของ Gateway และที่ปลายทางทั้งสอง โดยในส่วนของ Gateway นั้นสามารถจะใช้ได้ทั้งการ Authenticate หรือเข้ารหัส หรือทั้งสองแบบ โดยจะให้ความปลอดภัยกับทุก ๆ การสื่อสารระหว่างทางของ Gateway แต่ความปลอดภัยโดยรวมนี้ อาจไม่พอเพียงกับความต้องการของบ้าง Host เช่น หากที่ Gateway ทำให้เฉพาะการเข้ารหัส แต่ที่ Host ต้องการ Authenticate ด้วย ก็จะต้องใช้การทำงานในลักษณะเช่นนี้ สำหรับแบบที่ 4 จะใช้กรณีที่ Remote Host มีการเชื่อมต่อกับองค์กรผ่านทางอินเตอร์เน็ต โดยเชื่อมต่อกับ Router หรือ Firewall ของบริษัท ซึ่งจะมีการสร้าง VPN ระหว่าง Remote Host กับ Router หรือ Firewall จากนั้นหาก Remote Host ต้องการติดต่อกับเครื่องคอมพิวเตอร์ภายในที่มีการใช้งาน IPSec ก็จะต้องมีการสร้างการเชื่อมต่อแบบ IPSec ขึ้น โดยอาจจะเป็นการทำงานแบบเข้ารหัสอย่างเดียว หรือการทำงานแบบที่ใช้ Authentication ด้วยก็ได้



รูปที่ 52 Basic Combinations of Security Associations

Key Management

ส่วนของ Key Management เป็นส่วนของ IPSec ที่ทำหน้าที่วางนโยบายและกระจาย Secret Key โดยปกติจะมีการใช้ Key ทั้งหมด 4 Key ในการสื่อสารระหว่าง 2 เครื่อง ในแต่ละแอปพลิเคชัน โดยจะใช้ 2 คีย์กับ AH โดยเป็นการส่ง 1 คีย์และเป็นการรับอีก 1 คีย์ สำหรับ ESP ก็ใช้ 2 คีย์ทำนองเดียวกัน โดยในระบบของ IPSec จะมีระบบการบริหารคีย์อยู่ 2 แบบ คือ แบบ Manual และ Automated โดยในแบบ Manual นั้นผู้ดูแลระบบจะต้องกำหนดคีย์ให้กับแต่ละระบบ ซึ่งจะเหมาะสมสำหรับระบบที่เล็ก และไม่มีการเปลี่ยนแปลงมากนัก

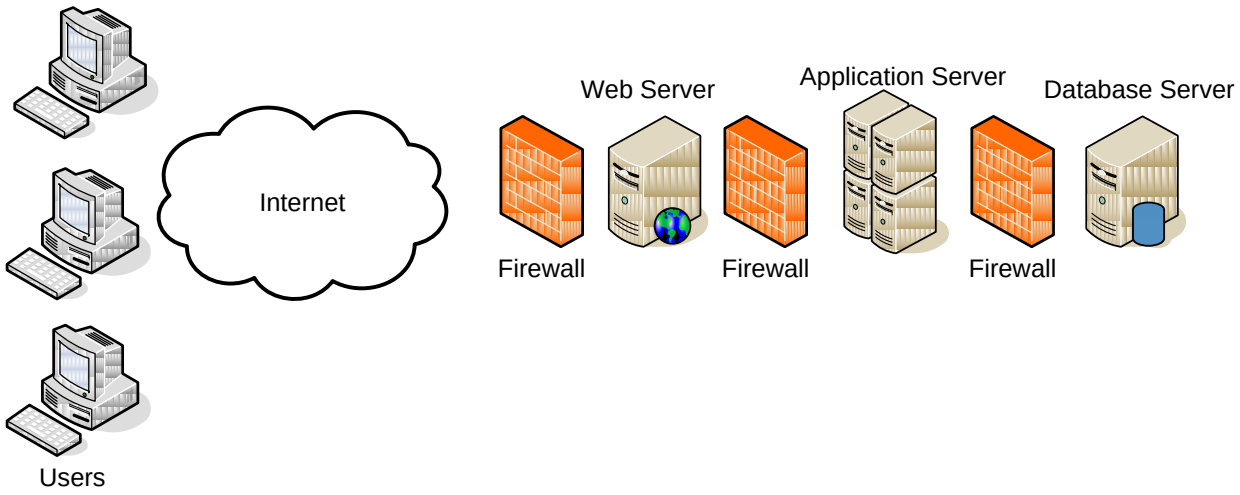
สำหรับระบบ Automated จะมีการสร้างคีย์ตามที่แต่ละ SA จะขอมาโดยอัตโนมัติ ซึ่งจะเหมาะสมสำหรับระบบที่ใหญ่ ที่มีการเปลี่ยนแปลงการใช้งานอยู่เสมอ

สำหรับโพรโตคอลที่ใช้ในการบริหารคีย์ สำหรับ IPSec จะใช้โพรโตคอล ISAKMP/Oakley โดยจะประกอบด้วย 2 ส่วน คือโพรโตคอล Oakley โดยเป็นโพรโตคอลที่ใช้ในการแลกเปลี่ยนคีย์ โดยมีพื้นฐานบนอัลกอริทึม Diffie-Hellman แต่มีการเพิ่มระดับของความปลอดภัยให้มากขึ้น สำหรับโพรโตคอล Oakley นี้ไม่มีการกำหนดรูปแบบที่แน่นอน สำหรับส่วนที่ 2 คือ ISAKMP (Internet Security Association and Key Management Protocol) โดยจะใช้สำหรับบริหารคีย์ในเครือข่ายอินเตอร์เน็ต สำหรับ ISAKMP นั้นไม่ได้กำหนดโพรโตคอลที่ใช้แลกเปลี่ยนคีย์ โดยสามารถเลือกใช้ได้หลายวิธีการ

บทที่ 10. Web Application Security

เว็บแอปพลิเคชั่นหมายถึง แอปพลิเคชั่นที่สามารถเข้าใช้งานผ่านเว็บบราวเซอร์ หรือ HTTP(s) agent (พอร์ต 80 หรือ 443) องค์ประกอบของเว็บแอปพลิเคชั่นนั้นประกอบด้วย

- Web Application เป็นซอฟต์แวร์หลักที่ให้ผลลัพธ์เป็นข้อมูลและการทำงานต่างๆ ทำงานอยู่ใน Application Server
- Web Server เป็นเซิร์ฟเวอร์ที่ให้บริการคือการตอบสนองต่อการร้องขอการทำงานต่างๆ ผ่านเว็บ
- Application Server เป็นเซิร์ฟเวอร์ที่ Web Application ทำงาน
- Database Server เป็นเซิร์ฟเวอร์ฐานข้อมูลที่เก็บข้อมูลต่างๆ ของ Web Application



รูปที่ 53 Web Architecture

นอกจากองค์ประกอบหลักของระบบแล้วอาจมีส่วนเสริมให้ระบบทำงานอย่างมีประสิทธิภาพมากขึ้น โดยเพิ่มเติม Firewall, Load Balancer, Reverse Proxy Server, Cache System และองค์ประกอบอื่นๆ ปัญหาที่

อาจจะเกิดขึ้นในแต่ละส่วนของเว็บแอปพลิเคชั่นสามารถเกิดขึ้นได้ทุกๆ ส่วนในการทำงานตั้งแต่ web client ไปจนถึง database sever ดังสรุปในตาราง

Layer	ปัญหาในระบบ
HTTP Client / User	การโจมตีแบบ Cross-Site Scripting ถูกโจมตีโดยการปลอมแปลงหน้าเพจ หรือผู้ใช้งาน (Spoofing) การใช้ Javascript Injection เพื่อเปลี่ยนแปลงข้อมูลใน Browser
Transport Layer HTTP(s)	การดักจับข้อมูล (Passive Monitoring) การโจมตีจากคนกลาง (Man-in-the-Middle Attack) การขโมย Session (Session Hijack)
Firewall	การโจมตีระบบผ่าน SSL Session
Web Server	การทำ Buffer Overflow และ Format String การทำ Directory Traversal การตั้งค่า Default Accounts การตั้งค่า Default ใน Applications
Web Applications	การป้อนค่า Metacharacters การป้อนค่า Null Characters การทำ Buffer Overflow
Firewall	การโจมตีจาก Internal Network ซึ่งสามารถผ่าน Firewall ได้
Database	การทำ Direct SQL Commands หรือ SQL Injection การเข้าไป Query ใน Restricted Database การทำ Database Exploit

การโจมตีระบบ

ในการโจมตีระบบเว็บแอปพลิเคชั่นนั้นสามารถโจมตีได้หลายๆ อย่าง โดยมีสาเหตุจาก

- ความผิดพลาดของผู้ดูแลระบบที่ติดตั้งและตั้งค่าระบบต่างๆ ไม่ดีพอ
- ความผิดพลาดจากผู้เขียนซอฟต์แวร์ที่เกี่ยวข้องกับการทำงานเช่น MS IIS เป็นต้น
- ความผิดพลาดจากผู้เขียนเว็บแอปพลิเคชั่นและองค์ประกอบที่เกี่ยวข้องอื่นๆ ที่ไม่ได้ตระหนักถึงการทำงานให้เกิดความปลอดภัยในระบบ

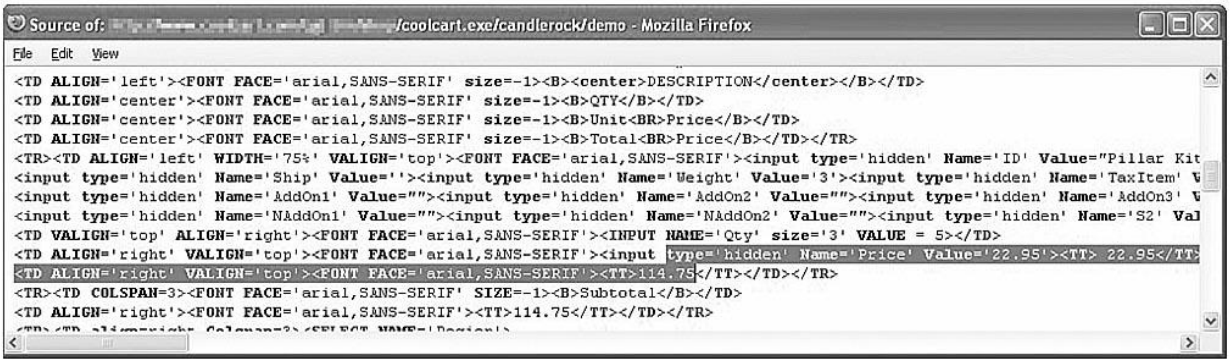
ตัวอย่างเทคนิคต่างๆ ที่ใช้ในการโจมตีเว็บแอปพลิเคชั่น

- Hidden Field Manipulation
- Cookie Poisoning
- Backdoors and debug options
- Application buffer overflows
- Stealth commanding
- 3rd party misconfigurations
- Known vulnerabilities
- Parameter tempering
- Cross site scripting
- Forceful browsing
- Hacking over SSL
- Sourcecode Disclosure
- Web Server Architecture Attack
- SQL Injection
- Java Script Injection

Hidden Field

สาเหตุเกิดจากเว็บแอปพลิเคชั่น ส่งข้อมูลส่วนหนึ่งไปเก็บไว้ที่ไคลเอนต์ โดยใช้ hidden field แล้วนำค่าดังกล่าวมาใช้งานอีกครั้งหนึ่งตอนโพรเซสเพื่อแสดงหน้าเพจถัดไป ในการทำงานลักษณะนี้ผู้บุกรุกสามารถเปลี่ยนแปลงค่า hidden field เพื่อ สร้างความเสียหาย เปลี่ยนแปลงการทำงานของเว็บแอปพลิเคชั่น หรือให้ได้

ผลลัพธ์ที่ต้องการ ในการโจมตีในลักษณะนี้ผู้โจมตีจะดูโค้ดของเว็บเพจนั้นๆ (View Source) แล้วแก้ไข Tag HIDDEN ให้กลายเป็นค่าอื่นๆ ที่สามารถนำไปประมวลผลต่อในเซิร์ฟเวอร์ หรือ Application ได้



รูปที่ 54 Hidden Field

Cookie Poisoning

ในการเก็บข้อมูลของ Cookie สำหรับการให้บริการเว็บนั้น โดยวัตถุประสงค์คือการเก็บข้อมูลรายละเอียดบางอย่างของผู้ใช้งานเว็บเพจนั้นๆ หรือผู้ใช้คนนั้นๆ ว่ามีความสนใจด้านใดเป็นพิเศษ ต้องการปรับแต่งค่าการนำเสนอข้อมูลอย่างไร รวมถึงอาจมีการเก็บข้อมูลเกี่ยวกับ Session ของการเชื่อมต่อไปยังเว็บแอปพลิเคชั่น เมื่อมีการเปลี่ยนแปลงค่าใน cookie ย่อมสามารถเปลี่ยนแปลงค่าต่างๆ แม้กระทั่งการเปลี่ยนแปลงค่า Session ID ของการเชื่อมต่อได้ ซึ่งทำให้เกิดปัญหาการเข้าถึงทรัพยากรของบุคคลอื่นๆ ได้ สำหรับข้อมูลที่เก็บอยู่ใน cookie นั้นจะไม่มีความปลอดภัยหากไม่มีการเข้ารหัส หรือเข้ารหัสไว้ไม่ดีพอ

Back Door & Debug Options

สำหรับแอปพลิเคชั่นที่พัฒนาขึ้นโดย Developing Environment สมัยใหม่มีหลายๆ แอปพลิเคชั่น จะมีฟังก์ชั่นในการ debug การทำงานของระบบที่พัฒนาขึ้นโดยการป้อนพารามิเตอร์บางอย่างเข้าไปในระบบ หรือการใช้งานลิงค์พิเศษในการ Debug การทำงานและส่งผลลัพธ์การ Debug ผ่านทางหน้าเว็บเพจ ซึ่งทำให้ผู้พัฒนาและผู้ดูแลระบบทราบค่าตัวแปรและการทำงานของแอปพลิเคชั่นนั้นๆ ได้ ทำให้ง่ายต่อการแก้ไขความผิดพลาด

ต่างๆ ในระบบ โดยโค้ดส่วน Debug นี้ผู้พัฒนาเว็บแอปพลิเคชั่นจะเป็นคนใส่ในระบบเอง นอกจากนี้ผู้พัฒนาระบบอาจสร้าง back door เพื่อใช้เป็นช่องทางในการติดต่อเข้าไปในระบบด้วย

การทำงานในลักษณะนี้จะเป็นช่องทางอีกช่องทางหนึ่งที่แฮกเกอร์สามารถเข้าใช้งานระบบได้โดยได้สิทธิในทรัพยากรทุกๆ อย่างในระบบ ซึ่งปกติจะได้สิทธิสูงสุดในระบบ ในการพัฒนาเว็บแอปพลิเคชั่นจึงควร disable debug mode และไม่ควรมี back door ในระบบ ด้วย

Application Buffer Overflow

การโจมตีเว็บแอปพลิเคชั่นในอีกรูปแบบหนึ่งคือการทำ Buffer Overflow โดยจะทำตรงส่วนของ text box ที่รับข้อมูลจากผู้ใช้งานเว็บเพจนั้นๆ การโจมตีทำได้โดยการป้อนอินพุทที่ระบบไม่สามารถจัดเก็บข้อมูลได้ลงในช่อง หรือส่วนในการรับอินพุทจากหน้าเว็บเพจ เมื่อเว็บเพจนั้นส่งข้อมูลไปยังเซิร์ฟเวอร์แล้ว ข้อมูลที่มีขนาดมากกว่าที่กำหนดไว้ จะไปทำให้แอปพลิเคชั่นหยุดการทำงานได้ การป้องกันก็คือที่ฝั่งเซิร์ฟเวอร์ควรมีการตรวจสอบขนาดของข้อมูลที่รับเข้ามาด้วย ไม่ให้เกินจากค่าที่กำหนดไว้

Stealth Commanding

เป็นการโจมตีสู่เว็บเซิร์ฟเวอร์โดยการส่งคำสั่งการทำงานต่างๆ แนบไปกับข้อมูลในช่องรับข้อมูลต่างๆ ในระบบ โดยการทำลักษณะนี้ได้นั้นเกิดจากการที่เว็บแอปพลิเคชั่นคิดว่าข้อมูลที่ได้รับมานั้นเป็นเพียงข้อมูลที่ไม่สามารถเอ็กซีคิวได้ ความเสียหายที่อาจจะเกิดขึ้นได้กับระบบก็คือ การถูกเปลี่ยนหน้าเว็บเพจ การปิดบริการ หรือการขโมยข้อมูลจากเซิร์ฟเวอร์ โดยการพัฒนาระบบในปัจจุบันจะมีการใช้งานระบบฐานข้อมูล และติดต่อฐานข้อมูลโดยใช้ SQL Command การส่ง Command ไปยังระบบส่วนใหญ่จะเป็นการส่ง SQL Command เพื่อให้ได้ผลลัพธ์ที่ตนเองต้องการ เป็นต้น

3rd Party Misconfiguration

ความผิดพลาดอีกข้อหนึ่งที่ทำให้เกิดช่องโหว่ในระบบได้คือการตั้งค่าต่างๆ ในระบบไม่เหมาะสม หรือมีความผิดพลาดขณะติดตั้งโปรแกรม ซึ่งอาจทำให้เกิดปัญหาเช่น ยังมีการใช้ Default password อยู่ หรือค่าบางอย่างที่ทำให้เกิดความปลอดภัยไม่ถูกเซตไว้ ทำให้ผู้ที่โจมตีระบบสามารถใช้ช่องโหว่นี้มาโจมตีระบบได้

Known Vulnerabilities

ความไม่ปลอดภัยในลักษณะนี้เกิดจากจุดอ่อนในโปรแกรมที่เรานำมาใช้งาน ซึ่งโปรแกรมบางอย่างที่มีการใช้งานกันอย่างแพร่หลายก็อาจมีบักในโปรแกรมได้เช่นกัน เช่นโปรแกรม Microsoft IIS ซึ่งปัญหาที่เกิดขึ้นอาจเกิดในจุดเล็กๆ ในระบบแต่ทำให้ระบบเกิดความไม่ปลอดภัยขึ้นได้

การแก้ปัญหานี้จะต้อง Patch โปรแกรมที่มีปัญหา โดยการนำโปรแกรมสำหรับแก้ไขจุดอ่อน (patch) ที่ออกโดยผู้พัฒนาแอปพลิเคชั่นนั้นๆ ซึ่งปกติแล้วจะมีการออก patch ออกมาอย่างรวดเร็ว แต่ปัญหาก็ไม่ได้อยู่ที่ว่าจะออก patch มาเร็วหรือไม่ แต่ปัญหาอยู่ที่ผู้พัฒนาแอปพลิเคชั่นยกภาระการแก้ไขจุดอ่อนในระบบให้กับผู้ดูแลระบบเอง ซึ่งจะทำช้ามากและมักจะไม่ทันการทุกที

อันตรายจากปัญหาลักษณะนี้มักลุกลามอย่างรวดเร็ว โดยเฉพาะอย่างยิ่งเมื่อเกิดกับโปรแกรมที่มีการใช้งานกันอย่างแพร่หลายเช่น Microsoft IIS โดยสาเหตุที่ทำให้การลุกลามเป็นไปอย่างรวดเร็วนั้นจะเกิดจากผู้ดูแลระบบไม่ได้ติดตามข่าวจุดอ่อนของระบบที่ตัวเองดูแลอยู่อย่างสม่ำเสมอ แต่แฮกเกอร์กลับตามข่าวเหล่านี้อยู่เสมอๆ เมื่อมีบักชนิดหนึ่งเกิดขึ้น ก็จะมีผู้ประกาศตามหน้าเว็บไซต์ทางด้านความปลอดภัยต่างๆ ซึ่งผู้ที่ทราบก่อนมักจะเป็นแฮกเกอร์ มากกว่าผู้ดูแลระบบ

Parameter Tempering

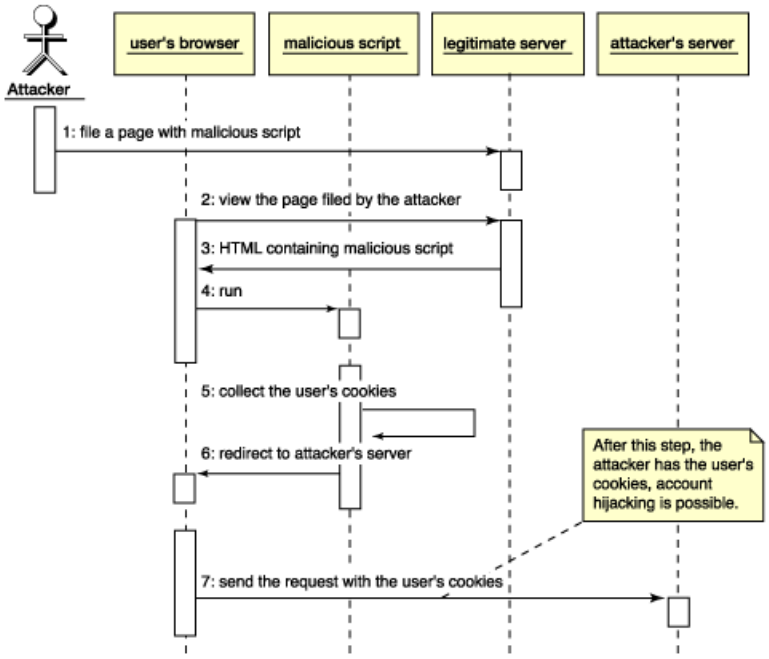
ปัญหานี้เกิดจากการที่เว็บแอปพลิเคชั่นใช้ค่าพารามิเตอร์จากไคลเอนต์ซึ่งการเปลี่ยนค่าพารามิเตอร์นั้นสามารถทำได้อย่างง่ายดาย ซึ่งผู้เขียนเว็บแอปพลิเคชั่นนั้น มักจะคิดว่าค่าต่างๆ จะเป็นค่าที่ถูกต้องแล้ว จะมีน้อยคนนักที่จะคำนึงถึงการเปลี่ยนแปลงพารามิเตอร์จะทำให้ระบบมีปัญหาอย่างไร

ปัญหาที่เกิดขึ้นจากการเปลี่ยนค่าพารามิเตอร์ไปเป็นค่าที่ไม่ถูกต้องนั้น ทำให้เกิดความไม่ปลอดภัยในข้อมูลหลายๆ อย่างเช่นการดึงข้อมูลของลูกค้าคนอื่นๆ ได้ การเปลี่ยนสิทธิของตนเองไปเป็นของคนอื่นๆ เพื่อดึงข้อมูลส่วนตัวของคนอื่นๆ เป็นต้น

Cross Site Script

cross site script เป็นกระบวนการหนึ่งที่อาศัยจุดอ่อนของโฮสที่ไม่มีการตรวจสอบว่าพารามิเตอร์ที่ป้อนเข้ามานั้นคือพารามิเตอร์จากไคลเอนต์จริงหรือไม่ จากจุดอ่อนดังกล่าวทำให้แฮกเกอร์สามารถโจมตีระบบได้โดยการฝาก script ไปรันที่เครื่องเป้าหมาย โดยผู้ใช้งานทางฝั่งไคลเอนต์เป็นผู้นำพา script ไปยังเครื่องเป้าหมายได้

โดยการโจมตีจะมีการสร้างลิ้ง หรือ การทำ sends an email ที่เว็บบอร์ด หรือหน้าเว็บเพจต่างๆ แล้วป้อนพารามิเตอร์เป็น javascript รอให้คนอื่นๆ ติดต่อจากเครื่องไคลเอนต์ทำการคลิก แล้วสคริปต์จะทำงานทันที โดยความสามารถของสคริปต์นั้นจะมีตั้งแต่การขโมยข้อมูลเล็กๆ น้อยๆ ไปจนถึงการขโมย session หรือข้อมูล Username และ Password ภายในเครื่องเป้าหมาย ตัวอย่างกระบวนการขโมย Cookie โดย Cross Site Script



รูปที่ 55 Cross Site Script

Forceful Browsing

การโจมตีลักษณะนี้แฮกเกอร์จะใช้การคาดเดาว่าข้อมูลนั้นๆ อยู่ในไดเรกทอรีไหน แล้วป้อนตำแหน่งของข้อมูลนั้นๆ โดยตรง ซึ่งทำให้แฮกเกอร์สามารถดึงเอาข้อมูลนั้นๆ ออกมาได้โดยตรง ปัญหานี้เกิดจาก การใช้ Default file ขณะติดตั้งโปรแกรม และไม่มีการลบไฟล์ที่ไม่ใช้ออกไปจากระบบ

ผลที่เกิดจากปัญหานี้คือข้อมูลต่างๆ เช่น ลอกไฟล์ โค้ดต้นแบบของโปรแกรมต่างๆ อาจถูกขโมยไปได้ ถ้าเปิดสิทธิให้สามารถอ่านไฟล์หรือไดเรกทอรี่นั้นๆ ได้

Hacking Over SSL

SSL มีประโยชน์อย่างยิ่งในการเข้ารหัสข้อมูลบนเว็บเพจต่างๆ แต่ก็เป็นประโยชน์ต่อแฮกเกอร์ด้วยเช่นกัน ในการตรวจสอบการบุกรุกระบบนั้น ไฟร์วอล และระบบตรวจจับผู้บุกรุกนั้น จะตรวจสอบ content ของข้อมูลที่รับส่งกัน ซึ่งการบุกรุกระบบหลายๆ กรณีสามารถตรวจจับได้โดยง่าย

ในการหลีกเลี่ยงการตรวจสอบโดยไฟร์วอล และระบบตรวจจับผู้บุกรุกนั้น จะสามารถใช้ SSL มาช่วยหลบหลีกได้เช่นกัน โดยแฮกเกอร์จะใช้เทคนิคการบุกรุกระบบโดยปกติ แต่จะใช้การเชื่อมต่อที่เป็น SSL เพื่อเข้ารหัสการบุกรุก ทำให้ไฟร์วอล หรือระบบตรวจจับผู้บุกรุกไม่สามารถอ่านข้อมูลจริงๆ และตรวจหาสัญญาณของการบุกรุกได้

Source Code Disclosures

การทำ Source Code Disclosure เป็นการใช้จุดอ่อนในการออกแบบแอปพลิเคชั่น ทำให้ผู้บุกรุกสามารถดึกข้อมูลของ configuration file หรือข้อมูลอื่นๆ ได้ ซึ่งปัญหาดังกล่าว ปัจจุบันมีการแก้ไขทั้งหมดแล้ว แต่ก็ควรศึกษาไว้

ตัวอย่างของการทำ Source Code Disclosures

บักใน WebLogic / WebSpere โดยบักนี้ทำให้ผู้บุกรุกสามารถดึงข้อมูลของไฟล์ที่นามสกุล JSP และ JHTML ได้ ซึ่งเกิดจากการตั้งค่าในเว็บเซิร์ฟเวอร์ผิดพลาด โดยการดึงข้อมูลนั้นสามารถทำได้โดยการเปลี่ยนตัวอักษร “jsp” ใน URL ให้กลายเป็นตัวอักษรตัวพิมพ์ใหญ่ จะทำให้เซิร์ฟเวอร์ส่งรายละเอียดในไฟล์ .jsp มาแทนผลลัพธ์ในการทำงานของไฟล์ .jsp นั้น

การทำ Source Code Disclosures จะเป็นบักใน Microsoft IIS ซึ่งมีปัญหากับไฟล์ “.HTR” โดยผู้บุกรุกสามารถดูรายละเอียดในไฟล์นามสกุล .ASA และ .ASP ได้ ยกตัวอย่าง URL ที่ทำให้เกิดปัญหาคือ

http://10.0.0.1/global.asa+.htr

โดยเมื่อเว็บเซิร์ฟเวอร์ได้รับการร้องขอ URL ดังกล่าวแล้วจะทำงานโดย .htr ทำให้ ISM.DLL ทำงานกับ URL ดังกล่าว และเครื่องหมาย + จะทำให้ ISM.DLL ไม่ประมวลผล ตัวอักษรหลังเครื่องหมาย + นั้น ปัญหาของ Microsoft IIS showcode.asp ซึ่งเป็นโปรแกรมในการดูรายละเอียดในโค้ดของไฟล์ต่างๆ ได้ โดย

showcode.asp จะถูก bundled กับ IIS ของ Windows NT Option Pack 4.0 โดยผู้บุกรุกที่ต้องการดูข้อมูลของไฟล์ต่างๆ ในระบบสามารถดูได้จากการป้อน URL เช่น

http://10.0.0.1/msadc/showcode.asp? Source=/msadc/../../../../../path/to/file.name

Web Server Architecture Attack

ในบางครั้งก็มีปัญหาในการออกแบบสถาปัตยกรรมของเว็บเซิร์ฟเวอร์ ทำให้เกิดช่องโหว่ขณะใช้งานเว็บเซิร์ฟเวอร์ได้ การโจมตีช่องโหว่ทางสถาปัตยกรรมของเว็บเซิร์ฟเวอร์นี้ จะใช้วิธีการ bypass การทำงานบางส่วนของเว็บเซิร์ฟเวอร์ แล้วไปใช้งาน built-in procedure ของเว็บเซิร์ฟเวอร์โดยตรง การแก้ปัญหานี้สามารถทำได้โดยการตรวจสอบสถาปัตยกรรมของเว็บเซิร์ฟเวอร์ให้ละเอียด เพื่อตรวจสอบดูว่าจะมีการทำงานที่นอกเหนือจากการทำงานปกติเกิดขึ้นในกรณีไหนบ้าง แล้วทำการแก้ไข

ในสถาปัตยกรรมเว็บเซิร์ฟเวอร์นั้นจะมีการตั้งค่าให้ handler ต่างๆ รับผิดชอบการประมวลผลไฟล์ต่างๆ ในระบบเมื่อถูกร้องขอเช่น html handler จะทำงานเกี่ยวกับการรับส่งข้อมูลภายในไฟล์ html ไปยังเครื่องที่ร้องขอ แต่ cgi handler จะรับผิดชอบในการเรียกให้ cgi ทำงาน แต่บางกรณีจะมี default handler สำหรับการทำงานกับข้อมูลที่อยู่นอกเหนือหน้าที่ของ handler อื่นๆ ซึ่งอาจทำให้ผู้บุกรุกสามารถเรียกใช้ default handler นี้เพื่อทำการอ่านไฟล์ cgi ขึ้นมาแสดงผลได้ หรืออาจส่งค่าไฟล์ html ไปยัง jsp handler ทำให้ระบบคอมไพล์ไฟล์ html โดย java compiler และเอ็กซีคิวต์โดย java run-time ในกรณีนี้ก็ทำให้ผู้บุกรุกสามารถมีการทำงานบางอย่างในระบบได้ ดังตัวอย่างการทำ handler forcing ใน Sun Java Web Server โดยผู้บุกรุกสามารถป้อน URL ดังตัวอย่าง

http://10.0.0.2/servlet/com.sun.server.http.pagecompile.jsp.runtime.JspServlet/path/to/file.html

โดยจะมีการเรียกให้ servlet ทำงานจากการป้อน path /servlet/ แล้วเรียก PageCompile handler (Servlet) มา handle ไฟล์ข้อมูลข้างหลัง แล้วป้อน path ไปยังไฟล์ของข้อมูลที่ต้องการให้ handle ซึ่งในทางปฏิบัติผู้บุกรุกอาจจะป้อนข้อมูลที่เป็นโปรแกรมสำหรับการเชื่อมต่อทางไกลส่งไปให้ java run-time เป็นตัวเอ็กซีคิวต์ แล้วเปิดพอร์ทขึ้นรอรับการเชื่อมต่อจากผู้บุกรุก สำหรับการทำในลักษณะนี้จะทำให้การเชื่อมต่อนั้นมีสิทธิเทียบเท่า root ในระบบทันที

SQL Poisoning & Injections

เป็นการโจมตีโดยใช้จุดอ่อนของการเขียนแอปพลิเคชั่น ที่มีการใช้งาน sql statement โดยรับข้อมูลจากไคลเอนต์แต่ไม่ได้ตรวจสอบก่อนว่าข้อมูลที่รับเข้ามานั้นถูกต้องหรือไม่ ซึ่ง sql statement จะเชื่อมต่อไปยัง DBMS โดยตรง (ผ่าน SQL Query) ทำให้ผู้บุกรุกสามารถเพิ่มเติมและเปลี่ยนแปลง sql statement เพื่อให้ทำงานอื่นได้

ยกตัวอย่างเช่นโค้ดในการดึงข้อมูลจาก database คือ

```
Dim sql_con , result, sql_qry
Const CONNECT_STRING =
“Provider=SQLOLEDB;SERVER=WEB_DB;UID=sa; PWD=xyzzy”

sql_qry = “SELECT * FROM PRODUCT WHERE ID =”
& Request.QueryString(“ID”)

Set objCon = Server.CreateObject(“ADODB.Connection”)
ObjCon.Open CONNECT_STRING
Set objRS – objCon.Execute(strSQL);
```

จากตัวอย่างโค้ดที่อยู่ในเว็บแอปพลิเคชั่นนั้น จะเห็นได้ว่าไม่มีการตรวจสอบค่าของอินพุทที่รับเข้ามาเลย ดังนั้นถ้ามีการร้องขอในลักษณะ

http://10.0.0.3/showtable.asp?ID=3+OR+1=1

ผลลัพธ์เมื่อโปรแกรมทำงานใน Query Statement คือ SELECT * FROM PRODUCT WHERE ID=3 OR 1=1 ซึ่งทำให้ระบบส่งผลลัพธ์คือข้อมูลทั้งหมดใน PRODUCT ออกมา จากข้อผิดพลาดในระบบในลักษณะนี้ยังสามารถส่งการทำงานอื่นๆ เข้ามาในระบบได้อีกเช่น

http://10.0.0.3/showtable.asp?ID=3%01DROP+TABLE+PRODUCT

ซึ่งจะส่งผลให้มีการทำงานคำสั่งต่อไปนี้ที่แอปพลิเคชั่นเซิร์ฟเวอร์

SELECT * FROM PRODUCT WHERE ID=3

DROP TABLE PRODUCT

นอกจากจะสามารถส่งคำสั่งเพื่อทำงานกับ SQL statement ได้แล้ว ยังสามารถ ส่งคำสั่งเพื่อการทำงานอื่นๆ ได้ด้วยเช่นกันยกตัวอย่างเช่น

http://10.0.0.3/showtable.asp?ID=3%01EXEC+master..xp_cmdshell+'copy+\winnt\system32\cmd.exe+\inetpub\scripts'

ซึ่งจะส่งคำสั่งไปทำงานที่ฝั่งเซิร์ฟเวอร์คือ

Copy \winnt\system32\winnt\cmd.exe \inetpub\scripts

เนื่องจากการทำงานของระบบสารสนเทศส่วนใหญ่จะมีการใช้ข้อมูลจากฐานข้อมูลเป็นหลัก ทำให้การโจมตีโดยใช้ SQL Injection สร้างความเสียหายให้กับระบบได้มากมาย เช่น การเข้าระบบโดยสร้างข้อมูลผู้ใช้งานจากการ Inject คำสั่งต่างๆ หรือการสร้าง Backdoor จากการ Inject คำสั่งเพื่อสร้างไฟล์ หรือปรับเปลี่ยนข้อมูลในไฟล์ระบบ เป็นต้น

Microsoft IIS Unicode bug

สำหรับ bug ที่สร้างความเสียหายต่อองค์กรธุรกิจอย่างมาก เห็นจะไม่พ้น Unicode bug ใน Microsoft IIS ซึ่งช่องโหว่นี้ทำให้ผู้บุกรุกสามารถส่งคำสั่งต่างๆ ไปทำงานที่เซิร์ฟเวอร์ได้อย่างง่ายดาย เพียงแค่ส่ง URL ที่มี Unicode ที่มีปัญหาเข้าสู่ระบบ แล้วให้ระบบรับคำสั่งจาก URL ไปทำงาน เช่น

http://10.0.0.3/scripts/..%c0%af../winnt/system32/cmd.exe?c+dir

ซึ่งจะส่งคำสั่ง dir ไปทำงานที่เว็บเซิร์ฟเวอร์ และส่งผลลัพธ์การทำงานมาที่หน้าจอบราวเซอร์

Java Script Injection

โดยหลักการของ Javascript Injection เป็นการใช้ Javascript เป็นเครื่องมือในการปรับเปลี่ยนค่าต่างๆ ในเอกสารเว็บนั้นๆ ทั้งนี้ความสามารถของ Java Script Injection นี้สามารถปรับเปลี่ยนค่าต่างๆ ได้โดยยังคงสถานะของ Session อยู่ซึ่งดีกว่าการแก้ Hidden Field ต่างๆ ที่ทำให้ค่า Session นั้น Invalid ได้ แต่ทั้งนี้ทั้งนั้นจำเป็นต้องมีความรู้ด้าน Javascript และโครงสร้างของเอกสาร HTML ในมุมมองของ Javascript พอสมควร คำสั่งพื้นฐานที่ใช้สำหรับดูข้อมูลต่างๆ เช่น การดูข้อมูล Cookies ในเอกสารสามารถใช้คำสั่ง

javascript:alert(document.cookie)

การตั้งค่าต่างๆ ที่อยู่ในเอกสารเช่นการเปลี่ยนค่า Document.title โดยใช้คำสั่ง

javascript:void(document.title="KMITL")

เป็นต้น

การสร้างความปลอดภัยในระบบ

จากสาเหตุที่ทำให้เกิดการโจมตี 3 ข้อที่ได้กล่าวมาแล้วนั้น การที่เราจะสร้างความปลอดภัยในระบบจึงต้องมีกระบวนการเพื่อแก้ปัญหาสองข้อคือ

- ใช้ System Scanner and Security Infrastructure Software
- Secure Coding

System Scanner and Security Infrastructure Software

ในการตรวจสอบทั้งความผิดพลาดจากการตั้งค่าต่างๆ ในระบบ และความผิดพลาดของจากผู้เขียนซอฟต์แวร์ที่เกี่ยวข้องกับการทำงาน เราจะใช้เครื่องมือช่วยตรวจสอบที่เรียกว่า System Scanner ในการตรวจสอบการตั้งค่าต่างๆ ไม่ว่าจะเป็น permission ต่างๆ , การตั้งค่าความปลอดภัยในระบบ และเว็บเซิร์ฟเวอร์ ตัวอย่าง Scanner ที่ใช้เช่น Whisker , Nikto , Stealth , Twwwscanและ AppScan เป็นต้น โดยการทำงานของเครื่องมือเหล่านี้จะสแกนหารายละเอียดต่างๆ ในเว็บไซต์แล้วเปรียบเทียบกับฐานข้อมูลว่ามีจุดอ่อนในระบบตรงจุดไหนบ้าง และจะรายงานผลการตรวจสอบพร้อมวิธีแก้ไขปัญหา

นอกจากจะใช้โปรแกรมสำหรับตรวจสอบระบบแล้ว การใช้ซอฟต์แวร์เพื่อสร้างเกราะป้องกันสำหรับเว็บเซิร์ฟเวอร์และเว็บแอปพลิเคชั่นก็เป็นสิ่งที่ควรทำอย่างยิ่ง โดยซอฟต์แวร์ดังกล่าวจะมีกระบวนการในการตรวจสอบข้อมูลต่างๆ ที่ส่งเข้ามายังเว็บเซิร์ฟเวอร์ว่ามีความผิดปกติต่างๆ หรือไม่ ถ้ามีก็จะ reject การทำงานนั้นๆ โดยอัตโนมัติ ตัวอย่างโปรแกรมที่ทำหน้าที่นี้ยกตัวอย่างเช่น AppShield เป็นต้น

การทำงานทั้งสองแบบจะช่วยแก้ไขปัญหาที่เกิดขึ้นจากความผิดพลาดจากการตั้งค่าต่างๆ ในระบบ และความผิดพลาดจากผู้เขียนซอฟต์แวร์ต่างๆ ที่เกี่ยวข้องแต่ยังไม่สามารถแก้ไขปัญหาจากผู้เขียนเว็บแอปพลิเคชั่นได้ ซึ่งการแก้ไขปัญหาจากการเขียนโค้ดที่มีช่องโหว่นั้น ต้องแก้ไขที่ตัวผู้เขียนเว็บแอปพลิเคชั่นเอง

Secure Coding

สำหรับปัญหาที่นอกเหนือจากปัญหาการตั้งค่าต่างๆ ในเว็บเซิร์ฟเวอร์ และปัญหาเกี่ยวกับเครือข่ายก็คือปัญหาในการเขียนโค้ดในเว็บแอปพลิเคชั่น ซึ่งสาเหตุที่ทำให้เกิดปัญหานี้ได้นั้นก็อยู่ที่โปรแกรมเมอร์ที่พัฒนาเว็บแอปพลิเคชั่นยังไม่ได้คำนึงถึงการป้องกันการทำงานที่ไม่ได้อยู่ในการควบคุมของโปรแกรม เช่นการควบคุมพารามิเตอร์บางอย่างและการตรวจสอบข้อมูลที่รับเข้ามาว่าเป็นข้อมูลที่ถูกต้องและเป็นปกติหรือไม่

ในการเขียนโค้ดให้เกิดความปลอดภัยนั้นเราจะต้องเพิ่มเติมการทำงานจากการทำงานปกติคือ

- การทำ input & output validation
- การใช้ SSL
- การใช้ HTML forms
- การใช้ Cookies
- การใช้ HTTP REFERER Header
- การใช้ POST & GET method
- มีกระบวนการในการทำ logout (logout machanism)
- Error Handling

การทำ input & output validation

ในการทำงานโดยปกติของเว็บแอปพลิเคชั่น จะมีการรอรับข้อมูลบางอย่างจากยูสเซอร์เพื่อใช้ในการทำงานแล้วจึงส่งผลลัพธ์ไปให้ยูสเซอร์ ซึ่งอินพุทจากยูสเซอร์ก็เป็นสาเหตุหลัก ที่จะทำให้ระบบเกิดความไม่ปลอดภัยได้ โดยผู้เขียนเว็บแอปพลิเคชั่นพึงระลึกไว้เสมอว่าไม่ควรเชื่อถือข้อมูลใดๆ ที่ส่งมาจากฝั่งไคลเอนต์ (NEVER TRUST CLIENT SIDE DATA)

สำหรับ Client Side Script ที่มีการใช้งานกันอยู่ในปัจจุบันนั้นยกตัวอย่างเช่น JavaScript , VBScript , Java Applets , Flash , Active X , CSS และ XML/XSL ซึ่งสามารถมีการเปลี่ยนแปลงได้โดยยูสเซอร์ดังนั้นจึงไม่ควรเชื่อถือในผลลัพธ์ที่ได้จาก script เหล่านี้ แต่ script เหล่านี้ก็ยังมีประโยชน์ในแง่การทดสอบประสิทธิภาพ และปรับปรุงการตอบสนองต่างๆ ในการทำงานด้วย

ทำ Sanity Checking โดยการตรวจสอบอินพุททุกอย่างที่เข้ามาในระบบ เพื่อตรวจดูว่าข้อมูลที่เราต้องการมีอะไรบ้าง ยกตัวอย่างเช่นถ้าอินพุทที่ต้องการใช้งานนั้นเป็นเพียงค่า YES หรือ NO เท่านั้น ก็ทำการ drop ข้อมูลอื่นๆ ที่รับเข้ามาทิ้งไป หรือถ้าข้อมูลที่ต้องการรับเข้ามาเป็นเพียงตัวเลขที่อยู่ในช่วงตัวเลขช่วงหนึ่งก็ต้องมีการตรวจสอบค่าตัวเลขที่รับเข้ามาก่อนที่จะนำเอาไปใช้งาน

ควรมีการตรวจสอบตัวอักขระพิเศษต่างๆ ด้วย เพราะตัวอักขระพิเศษต่างๆ มักจะเป็นต้นกำเนิดของปัญหาการใช้ฟังก์ชั่น หรือ system call ที่ผิดปกติ การทำ directory traversal โดยเฉพาะอย่างยิ่ง NULL character ซึ่งปกติแล้วจะไม่มีการใช้งาน

ถ้าเว็บแอปพลิเคชั่นไม่จำเป็นต้องใช้งานตัวอักษร HTML ต่างๆ ก็ควรทำการกรองตัวอักษร HTML ก่อน และเปลี่ยนรูปแบบอักขระให้อยู่ในรูปอื่นๆ ที่ปลอดภัยกว่า ก่อนที่จะนำเข้ามาเป็นอินพุทของเว็บแอปพลิเคชั่น เช่น

>	เปลี่ยนเป็น	>
<	เปลี่ยนเป็น	<
“	เปลี่ยนเป็น	"
&	เปลี่ยนเป็น	&

ในกรณีที่จำเป็นต้องให้ยูสเซอร์ สามารถป้อน HTML tag ส่งเข้ามาเป็นอินพุทได้ เช่นในกรณีที่ทำ web-mail , message board หรือ chat ควรมีการทำ HTML Allow List เพื่ออนุญาตเฉพาะ HTML tag ที่ควรอยู่ในการทำงานนั้นผ่านเข้ามาในระบบ และ drop HTML tag อื่นๆ ทิ้ง สำหรับ tag ที่อาจจะมีปัญหาใน HTML คือ <APPLET> , <BASE> , <BODY> , <EMBED> , <FRAME> , <FRAMESET> , <HTML> , <IFRAME> , <IMG> , <LAYER> , <META> , <OBJECT> , <P> , <SCRIPT> , <STYLE> และ HTML tag ที่มี attributes ต่อไปนี้ <STYLE> , <SRC> , <HREF> , < TYPE>

การดึงข้อมูลจากฐานข้อมูลแล้วแสดงผลให้กับยูสเซอร์ควรมีการกรองข้อมูล และเปลี่ยนแปลงค่าตัวอักขระที่อยู่ในข้อมูล HTML ก่อน เพื่อป้องกันการส่งคำสั่งมาทำงานที่เซิร์ฟเวอร์

การใช้ SSL

โพรโตคอล HTTP ที่ใช้งานกันอยู่ในปัจจุบันมีจุดบกพร่องในด้านการรักษาความปลอดภัย 2 ประการหลักๆ คือข้อมูล HTTP เป็นข้อมูล Plaintext ซึ่งสามารถดักจับได้โดยโปรแกรม Sniffer ต่างๆ และโพรโตคอล HTTP ยังไม่สามารถตรวจสอบความถูกต้องของข้อมูลที่รับส่งนั้นๆ ในการรักษาความปลอดภัยในโพรโตคอล HTTP SSL (Secure Socket Layer) เป็นระบบการรักษาความปลอดภัยในการสื่อสารระหว่าง Web Client กับ Web Server สำหรับ SSL นั้นเป็นการทำงานในชั้น transport ที่ช่วยในการสร้างความปลอดภัย 3 ข้อคือ

1. การเข้ารหัสข้อมูล
2. การทำ Client & Server Authentication
3. การทำ Data Integrity

การเข้ารหัสของ SSL นั้นมีได้ 2 แบบการใช้คีย์ในการเข้ารหัส 40 บิตและ 128 บิต (โดยทั่วไปจะเป็น 40 บิต) หลักการทำงานของ SSL ก็คือ จะทำการเข้ารหัสข้อมูลจาก Web Browser โดยใช้ Public Key จาก Server มาเข้ารหัสกับคีย์ที่ Browser สร้างขึ้น จากนั้นนำคีย์ที่ได้มาเข้ารหัสข้อมูลที่จะส่งไปยัง Server เมื่อส่งข้อมูลเรียบร้อยแล้ว Server จะทำการถอดรหัสข้อมูลเป็นข้อมูลปกติ

การทำงานของ SSL เริ่มจากผู้ใช้งานเริ่มกระบวนการติดต่อ ไปยังเว็บเซิร์ฟเวอร์ที่มีระบบ SSL หลังจากนั้นเซิร์ฟเวอร์จะส่งใบรับรอง (Server Certificate) กลับมาพร้อมกับเข้ารหัส ด้วยกุญแจสาธารณะ (Public Key) ของเซิร์ฟเวอร์ หลังจากนั้นคอมพิวเตอร์ฝั่งผู้รับจะทำการตรวจสอบใบรับรองนั้นอีกทีเพื่อตรวจสอบตัวตนของเซิร์ฟเวอร์หลังจากนั้นจะทำการสร้างกุญแจสมมาตรโดยการสุ่มและทำการเข้ารหัสกุญแจสมมาตรด้วยกุญแจสาธารณะของเซิร์ฟเวอร์ที่ได้รับมา เพื่อส่งกลับไปยังเซิร์ฟเวอร์เมื่อเซิร์ฟเวอร์ได้รับแล้วก็จะทำการถอดรหัสด้วยกุญแจส่วนตัว (Private Key) ก็จะได้กุญแจสมมาตรของลูกค้ามาไว้ใช้ในการติดต่อสื่อสาร หลังจากนั้นในการติดต่อสื่อสารกันก็ใช้การเข้ารหัสติดต่อสื่อสารกันได้อย่างปลอดภัย

การใช้ HTML forms

การใช้ hidden form element นั้นช่วยให้การทำงานหลายๆ อย่างทำได้สะดวกมากขึ้น โดยระบบจะมองข้อมูลที่อยู่ใน hidden เป็นเหมือนกับข้อมูลที่รับมาจากยูสเซอร์ แต่การใช้งาน hidden element ไม่ควรใช้กับ

ข้อมูลที่มีความสำคัญมากๆ เช่น ราคาสินค้า รหัสที่แทนผู้ใช้งาน ค่าพารามิเตอร์ต่างๆ ที่มีผลต่อการทำงานของเว็บแอปพลิเคชั่น

การใช้งาน password element ควรใช้งานควบคู่กับ SSL เนื่องจากข้อมูลที่รับส่งกันยังเป็น plain text และในการรับส่งข้อมูลของ password element ไม่ควรใช้ method HTTP/GET ควรใช้ HTTP/POST แทน

สำหรับ MaxSize Attribute (<input MaxSize="##">) นั้นควรใช้ในการตรวจสอบความถูกต้องของข้อมูลในลำดับที่สองเท่านั้น ซึ่งจะมีลักษณะเดียวกับการตรวจสอบโดย VB/Jscripts เนื่องจากการนำ MaxSize มาเป็นตัวบังคับขนาดของข้อมูลในลำดับแรกนั้น จะใช้ไม่ได้ผลเนื่องจาก ค่าดังกล่าวสามารถเปลี่ยนแปลงได้โดยยูสเซอร์ ซึ่งจะส่งผลให้ระบบถูกโจมตีในลักษณะของการทำ buffer overflow ได้

การใช้ Cookies

Cookies เป็นเนื้อที่ในการเก็บข้อมูลในการทำงานบางส่วนไว้ที่ไคลเอนต์โดย Cookie มีอยู่ 2 ประเภทคือ
persistent : เป็น Cookie ที่ไม่มีการลบข้อมูลออกแม้ว่าจะปิดแอปพลิเคชั่นไปแล้วก็ตาม
non-persistent : เป็น Cookie ที่จะลบข้อมูลออกจากไคลเอนต์เมื่อหมดเวลา หรือเมื่อปิดแอปพลิเคชั่นไปแล้ว
Cookies นั้นมีประโยชน์สำหรับเว็บแอปพลิเคชั่นในการทำงาน 3 ลักษณะคือ

- User Authentication
- State Management
- Saving user preference

หลักการในการใช้งาน Cookies เพื่อความปลอดภัย

- ไม่ควรเก็บข้อมูลใน Cookies เป็น Plaintext หรือเข้ารหัสข้อมูลแบบหลวมๆ
- ควรคำนึงไว้เสมอๆ ว่าข้อมูลใน Cookies นั้นไม่ปลอดภัย
- ถ้าใช้งาน Cookies ควรระมัดระวังสองกรณีคือ ไม่ควรมีคนอื่นๆ มาใช้งาน Cookies ได้ และไม่ควรมีใครรู้ข้อมูลใน Cookies ไม่ว่ากรณีใดๆ
- ควรมีการเซต restrictive path ใน Cookies

- ในการตรวจสอบ Authentication นั้นไม่ควร valid ถ้าทำงานเกินช่วงเวลาที่ตั้งไว้
- ข้อมูลที่เก็บไว้ใน Cookies ควรเป็นข้อมูลที่ใช้ชั่วคราวเท่านั้น
- ในการสร้าง Token ID ควรใช้อัลกอริทึมที่มีประสิทธิภาพ ไม่สามารถคาดเดาได้
- ใช้ Cookies Timeout สำหรับลบ Cookies ที่ไม่มีการใช้งานออกจากระบบ
- การทำ Authentication ควรใช้ข้อมูลของไอพีแอดเดรสมาประกอบด้วยโดย สำหรับ Business Intranet ควรใช้ไอพีแอดเดรสทั้ง 32 บิต สำหรับการใช้งานเว็บทั่วๆ ไป ควรใช้ข้อมูล 16 บิต มาประกอบการทำ authentication ด้วย
- ในการทำ Authentication ควรใช้ข้อมูลเกี่ยวกับไคลเอนต์มาประกอบด้วยเช่นการใช้ header ที่เป็นค่าคงที่และแตกต่างกันในแต่ละไคลเอนต์เช่น User-Agent , Accept-Language , Etc.
- สำหรับ Authentication Cookies ถ้านำมาใช้งานครั้งหนึ่งแล้ว ก็ไม่ควรนำมาใช้งานอีก

การใช้ HTTP REFERER Header

การป้องกัน script attack อีกทางหนึ่งที่สามารถป้องกัน script attack ได้บ้างคือการใช้ HTTP REFERER header แต่ก็ไม่สามารถป้องกันได้ทั้งหมด เนื่องจาก HTTP REFERER นั้นก็ยังเป็นข้อมูลในฝั่งไคลเอนต์ที่สามารถปลอมแปลงได้เช่นกัน

การใช้ POST & GET method

ไม่ควรใช้ method GET ในการส่งข้อมูลที่มีความสำคัญ เนื่องจากข้อมูลจะไปปรากฏในอุปกรณ์หลายๆ อย่างในเส้นทางที่แพ็กเก็ตผ่านไปเช่น Proxy Server, Firewall , Web Servers log เป็นต้น ในกรณีที่เว็บแอปพลิเคชั่นมีการใช้งาน POST เท่านั้น ก็ควรตั้งค่าให้เว็บเซิร์ฟเวอร์ตอบสนองเฉพาะ POST เท่านั้น และไม่ตอบสนองต่อ method อื่นๆ เลย การทำเช่นนี้สามารถป้องกันการโจมตีโดยใช้ client side script ได้ ถึงแม้ว่า POST method จะใช้งานได้ดีและปลอดภัยมากกว่า GET แต่ก็ยังไม่สามารถป้องกันการดักจับข้อมูลได้

มีกระบวนการในการทำ logout (logout machanism)

การเพิ่มกระบวนการในการ logout ในการทำงานต่างๆ ในเว็บแอปพลิเคชั่นนั้น มีประโยชน์ในการลบ Cookies หรือทำให้ Cookies ที่ฝั่งไคลเอนต์ไม่สามารถทำงานได้ จัดการกับ session ทางฝั่งเซิร์ฟเวอร์เพื่อป้องกันการขโมย session ในกรณีที่ Cookies ที่ไคลเอนต์ยังไม่หมดอายุ

Error Handling Mechanism

การทำ Error Handling ที่มีการแจ้ง Error Description นั้นเป็นประโยชน์ในการดีบักปัญหาต่างๆ แต่ไม่ควรส่ง Error Description ต่างๆ ไปให้ยูสเซอร์ เนื่องจากจะทำให้ผู้บุกรุกสามารถรู้รายละเอียดในระบบได้ ในกรณีที่จำเป็นต้องส่ง Error Desciption ต่างๆ ไปให้ยูสเซอร์ ก็ควรมีการกรองข้อมูลก่อนที่จะส่งด้วย ในการแจ้ง Error Desciption ก็ไม่ควรแจ้งลงรายละเอียดมากเกินไปจนทำให้ผู้บุกรุกสามารถคาดเดาได้ว่าระบบมีข้อมูล และการทำงานอย่างไร เช่น การแจ้งปัญหาในการลอกอินสู่ระบบ ถ้ามียูสเซอร์ป้อนรหัสผ่านผิด ก็ควรแจ้งว่ามีปัญหาในการลอกอิน โดยปัญหาอาจเกิดจาก Username หรือ Password แต่ไม่ควรแจ้งว่าปัญหาอยู่เฉพาะ Password เพราะจะทำให้ผู้บุกรุกระบบทราบว่าในระบบมี Username นี้อยู่ในระบบทันที

บทที่ 11. Wireless LAN Security

Wireless Lan คือการสื่อสารผ่านเครือข่าย LAN โดยใช้สื่อกลางคืออากาศ โดยมาตรฐานที่ใช้ในการเชื่อมต่อระหว่างเครือข่ายไร้สายโดยทั่วไปในปัจจุบันคือมาตรฐาน 802.11 โดยมาตรฐาน IEEE 802.11 มีการกำหนด Specfication สำหรับอุปกรณ์ WLAN ในส่วนของ Physical Layer และ Media Access Control Layer โดยในส่วนของ Physical Layer กำหนดให้อุปกรณ์มีความสามารถในการรับส่งข้อมูลด้วยความเร็ว 1, 2, 5.5, 11 และ 54 Mbps โดยมีความสามารถในการใช้งานคลื่นวิทยุที่ความถี่สาธารณะ 2.4 และ 5 GHz, และ อินฟราเรด(1 และ 2 Mbps เท่านั้น) สำหรับในส่วนของ MAC Layer ได้กำหนดให้มีกลไกการทำงานที่เรียกว่า CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) ซึ่งมีความคล้ายคลึงกับหลักการ CSMA/CD (Collision Detection) ของมาตรฐาน IEEE 802.3 นอกจากนี้ในมาตรฐาน IEEE802.11 ยังกำหนดให้มีกลไกการเข้ารหัสข้อมูล (Encryption) และการตรวจสอบผู้ใช้ (Authentication) ที่มีชื่อเรียกว่า WEP (Wired Equivalent Privacy)

มาตรฐาน IEEE 802.11 ได้รับการตีพิมพ์ครั้งแรกในปี พ.ศ. 2540 ซึ่งในเวอร์ชันแรกนั้น มีประสิทธิภาพค่อนข้างต่ำและไม่มีการรองรับหลักการ Quality of Service (QoS) อีกทั้งกลไกการรักษาความปลอดภัยที่ใช้ยังมีช่องโหว่อยู่มาก IEEE จึงได้จัดตั้งคณะทำงาน (Task Group) ขึ้นมาหลายชุดเพื่อทำการปรับปรุงเพิ่มเติมมาตรฐานให้มีศักยภาพสูงขึ้น โดยคณะทำงานกลุ่มที่มีผลงานที่รู้จักกันดีได้แก่ IEEE 802.11a, IEEE 802.11b, IEEE 802.11e, IEEE 802.11g, และ IEEE 802.11i

การทำงานของคณะทำงานชุด IEEE 802.11b ได้ตีพิมพ์มาตรฐานเพิ่มเติมนี้เมื่อปี พ.ศ. 2542 ซึ่งเป็นที่รู้จักกันดีและใช้งานกันอย่างแพร่หลายมากที่สุด มาตรฐาน IEEE 802.11b ใช้เทคโนโลยีที่เรียกว่า CCK (Complimentary Code Keying) ผนวกกับ DSSS (Direct Sequence Spread Spectrum) เพื่อปรับปรุงความสามารถของอุปกรณ์ให้รับส่งข้อมูลได้ด้วยความเร็วสูงสุดที่ 11 Mbps ผ่านคลื่นวิทยุความถี่ 2.4 GHz (เป็นย่านความถี่ที่เรียกว่า ISM (Industrial Scientific and Medical) ซึ่งสามารถใช้งานทั่วไป ไม่ว่าจะเป็นด้านวิทยาศาสตร์ อุตสาหกรรม และการแพทย์ โดยอุปกรณ์ที่ใช้ความถี่ย่านนี้เช่น IEEE 802.11, Bluetooth, โทรศัพท์ไร้สาย, และเตาไมโครเวฟ

คณะทำงานชุด IEEE 802.11a ได้ตีพิมพ์มาตรฐานเพิ่มเติมนี้เมื่อปี พ.ศ. 2542 มาตรฐาน IEEE 802.11a ใช้เทคโนโลยีที่เรียกว่า OFDM (Orthogonal Frequency Division Multiplexing) เพื่อปรับปรุงความสามารถของอุปกรณ์ให้รับส่งข้อมูลได้ด้วยความเร็วสูงสุดที่ 54 Mbps แต่จะใช้คลื่นวิทยุที่ความถี่ 5 GHz ซึ่งเป็นย่านความถี่สาธารณะสำหรับใช้งานในประเทศสหรัฐอเมริกาที่มีสัญญาณรบกวนจากอุปกรณ์อื่นน้อยกว่าในย่านความถี่ 2.4 GHz อย่างไรก็ตามข้อเสียหนึ่งของมาตรฐาน IEEE 802.11a ที่ใช้คลื่นวิทยุที่ความถี่ 5 GHz ก็คือในบางประเทศย่านความถี่ดังกล่าวไม่สามารถนำมาใช้งานได้อย่างสาธารณะ ตัวอย่างเช่น ประเทศไทยไม่อนุญาตให้มีการใช้งานอุปกรณ์ IEEE 802.11a เนื่องจากความถี่ย่าน 5 GHz ได้ถูกจัดสรรสำหรับกิจการอื่นอยู่ก่อนแล้ว นอกจากนี้ข้อเสียอีกอย่างหนึ่งของอุปกรณ์ IEEE 802.11a WLAN ก็คือรัศมีของสัญญาณมีขนาดค่อนข้างสั้น (ประมาณ 30 เมตร ซึ่งสั้นกว่ารัศมีสัญญาณของอุปกรณ์ IEEE 802.11b WLAN ที่มีขนาดประมาณ 100 เมตร สำหรับการใช้งานภายในอาคาร) อีกทั้งอุปกรณ์ IEEE 802.11a WLAN ยังมีราคาสูงกว่า IEEE 802.11b WLAN ด้วย ดังนั้นอุปกรณ์ IEEE 802.11a WLAN จึงได้รับความนิยมน้อยกว่า IEEE 802.11b WLAN มาก

คณะทำงานชุด IEEE 802.11g ได้ใช้นำเทคโนโลยี OFDM มาประยุกต์ใช้ในช่องสัญญาณวิทยุความถี่ 2.4 GHz ซึ่งอุปกรณ์ IEEE 802.11g WLAN มีความสามารถในการรับส่งข้อมูลด้วยความเร็วสูงสุดที่ 54 Mbps ส่วนรัศมีสัญญาณของอุปกรณ์ IEEE 802.11g WLAN จะอยู่ระหว่างรัศมีสัญญาณของอุปกรณ์ IEEE 802.11a และ IEEE 802.11b เนื่องจากความถี่ 2.4 GHz เป็นย่านความถี่สาธารณะสากล อีกทั้งอุปกรณ์ IEEE 802.11g WLAN สามารถทำงานร่วมกับอุปกรณ์ IEEE 802.11b WLAN ได้ (backward-compatible) ดังนั้นจึงมีแนวโน้มสูงว่าอุปกรณ์ IEEE 802.11g WLAN จะได้รับความนิยมอย่างแพร่หลายและน่าจะมาแทนที่ IEEE 802.11b ในที่สุด IEEE 802.11g ได้รับการตีพิมพ์กลางปี พ.ศ. 2546

คณะทำงาน IEEE 802.11e ได้รับมอบหมายให้ปรับปรุง MAC Layer ของ IEEE 802.11 เพื่อให้สามารถรองรับการใช้งานหลักการ Qualitiy of Service สำหรับ application เกี่ยวกับมัลติมีเดีย (Multimedia) เนื่องจาก IEEE 802.11e เป็นการปรับปรุง MAC Layer ดังนั้นมาตรฐานเพิ่มเติมนี้จึงสามารถนำไปใช้กับอุปกรณ์ IEEE 802.11 WLAN ทุกเวอร์ชันได้

คณะทำงาน IEEE 802.11i ได้รับมอบหมายให้ปรับปรุง MAC Layer ของ IEEE 802.11 ในด้านความปลอดภัย เนื่องจากเครือข่าย IEEE 802.11 WLAN มีช่องโหว่อยู่มากโดยเฉพาะอย่างยิ่งการเข้ารหัสข้อมูล

(Encryption) ด้วย key ที่ไม่มีการเปลี่ยนแปลง คณะทำงานชุด IEEE 802.11i จะนำเอาเทคนิคขั้นสูงมาใช้ในการเข้ารหัสข้อมูลด้วย key ที่มีการเปลี่ยนค่าอยู่เสมอและการตรวจสอบผู้ใช้ที่มีความปลอดภัยสูง มาตรฐานเพิ่มเติมนี้จึงสามารถนำไปใช้กับอุปกรณ์ IEEE 802.11 WLAN ทุกเวอร์ชันได้

*Wi-Fi เป็นใบรับรองของ WECA (Wireless Ethernet Compatability Alliance) ที่ออกให้แก่อุปกรณ์ต่างๆ เพื่อบ่งบอกว่าอุปกรณ์ยี่ห้อและรุ่นดังกล่าวทำงานได้ตรงตามมาตรฐานของ wireless lan ซึ่งก็หมายถึงว่า เราสามารถใช้งานอุปกรณ์นั้นในการเชื่อมต่อกับอุปกรณ์อื่นๆ ที่ได้รับใบรับรอง Wi-Fi ได้นั่นเอง

อุปกรณ์ที่ใช้ในการเชื่อมต่อเครือข่ายไร้สาย

การ์ดเครือข่ายแบบไร้สาย : มีลักษณะคล้ายกับการ์ดเครือข่ายโดยทั่วๆ ไปแต่การเชื่อมต่อระหว่างการ์ดกับอุปกรณ์อื่นๆ จะใช้อุปกรณ์รับส่งข้อมูลแบบไร้สายตามมาตรฐาน 802.11 แบบต่างๆ แทน

รูปที่ 56 อุปกรณ์ในการเชื่อมต่อเครือข่ายไร้สาย

อุปกรณ์ Access Point : มีลักษณะเป็นเหมือนกับฮับหรืออุปกรณ์ Switching ในเครือข่ายแบบมีสาย แต่จะใช้อุปกรณ์รับสัญญาณการเชื่อมต่อจากการ์ดเครือข่ายแบบไร้สายแทน

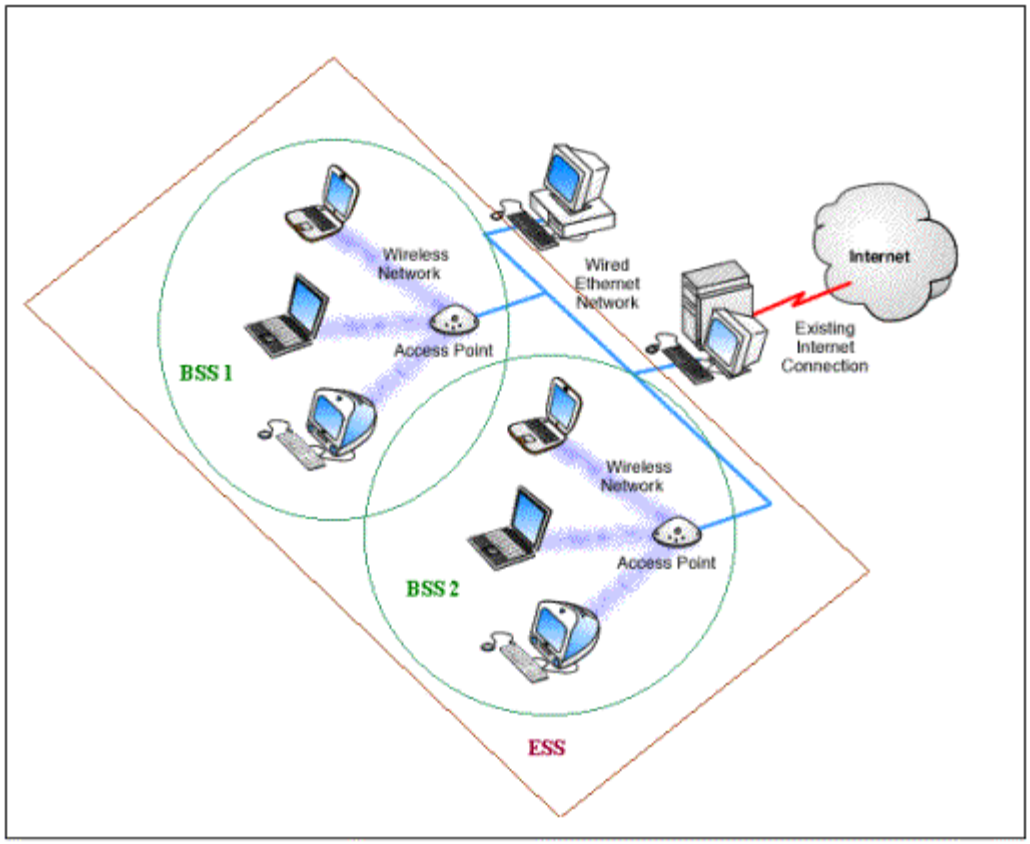
รูปที่ 57 Access Point

ลักษณะการเชื่อมต่อของอุปกรณ์ IEEE 802.11 WLAN

มาตรฐาน IEEE 802.11 ได้กำหนดลักษณะการเชื่อมต่อของอุปกรณ์ภายในเครือข่าย WLAN ไว้ 2 ลักษณะคือโหมด Infrastructure และโหมด Ad-Hoc หรือ Peer-to-Peer

โหมด Infrastructure

โดยทั่วไปแล้วอุปกรณ์ในเครือข่าย IEEE 802.11 WLAN จะเชื่อมต่อกันในลักษณะของโหมด Infrastructure ซึ่งเป็นโหมดที่อนุญาตให้อุปกรณ์ภายใน WLAN สามารถเชื่อมต่อกับเครือข่ายอื่นได้ ในโหมด Infrastructure นี้เครือข่าย IEEE 802.11 WLAN จะประกอบไปด้วยอุปกรณ์ 2 ประเภทได้แก่ สถานีผู้ใช้ (Client Station) ซึ่งก็คืออุปกรณ์คอมพิวเตอร์ (Desktop, Laptop, หรือ PDA ต่างๆ) ที่มีอุปกรณ์ Client Adapter เพื่อใช้รับส่งข้อมูลผ่าน IEEE 802.11 WLAN และสถานีแม่ข่าย (Access Point) ซึ่งทำหน้าที่ต่อเชื่อมสถานีผู้ใช้เข้ากับเครือข่ายอื่น (ซึ่งโดยปกติจะเป็นเครือข่าย IEEE 802.3 Ethernet LAN) การทำงานในโหมด Infrastructure มีพื้นฐานมาจากระบบเครือข่ายโทรศัพท์มือถือ กล่าวคือสถานีผู้ใช้จะสามารถรับส่งข้อมูลโดยตรงกับสถานีแม่ข่ายที่ให้บริการแก่สถานีผู้ใช้นั้นอยู่เท่านั้น ส่วนสถานีแม่ข่ายจะทำหน้าที่ส่งต่อ (forward) ข้อมูลที่ได้รับจากสถานีผู้ใช้ไปยังจุดหมายปลายทางหรือส่งต่อข้อมูลที่ได้รับจากเครือข่ายอื่นมายังสถานีผู้ใช้



รูปที่ 58 BSS และESS (อ้างอิงจาก http://www.winncom.com/html/wireless.shtml)

Basic Service Set (BSS)

Basic Service Set (BSS) หมายถึงบริเวณของเครือข่าย IEEE 802.11 WLAN ที่มีสถานีแม่ข่าย 1 สถานี ซึ่งสถานีผู้ใช้ภายในขอบเขตของ BSS นี้ทุกสถานีจะต้องสื่อสารข้อมูลผ่านสถานีแม่ข่ายดังกล่าวเท่านั้น

Extended Service Set (ESS)

Extended Service Set (ESS) หมายถึงบริเวณของเครือข่าย IEEE 802.11 WLAN ที่ประกอบด้วย BSS มากกว่า 1 BSS ซึ่งได้รับการเชื่อมต่อเข้าด้วยกัน สถานีผู้ใช้สามารถเคลื่อนย้ายจาก BSS หนึ่งไปอยู่ในอีก BSS หนึ่งได้โดย BSS เหล่านี้จะทำการ Roaming หรือติดต่อสื่อสารกันเพื่อทำการโอนย้ายการให้บริการสำหรับสถานีผู้ใช้ดังกล่าว

โหมด Ad-Hoc หรือ Peer-to-Peer

เครือข่าย IEEE 802.11 WLAN ในโหมด Ad-Hoc หรือ Peer-to-Peer เป็นเครือข่ายที่ปิดคือไม่มีสถานีแม่ข่ายและไม่มีการเชื่อมต่อกับเครือข่ายอื่น บริเวณของเครือข่าย IEEE 802.11 WLAN ในโหมด Ad-Hoc จะถูกเรียกว่า Independent Basic Service Set (IBSS) ซึ่งสถานีผู้ใช้หนึ่งสามารถติดต่อสื่อสารข้อมูลกับสถานีผู้ใช้อื่นๆ ในเขต IBSS เดียวกันได้โดยตรงโดยไม่ต้องผ่านสถานีแม่ข่าย แต่สถานีผู้ใช้จะไม่สามารถรับส่งข้อมูลกับเครือข่ายอื่นๆได้

รูปที่ 59 การทำงานในโหมด Adhoc หรือ Peer-to-Peer Mode (อ้างอิงจาก http://www.winncom.com/html/wireless.shtml)

การเข้าใช้ช่องสัญญาณด้วยกลไก CSMA/CA

บทบาทหนึ่งของ MAC Layer ในมาตรฐาน IEEE 802.11 คือการจัดสรรการเข้าใช้ช่องสัญญาณซึ่งแต่ละสถานีใน BSS หรือ IBSS จะต้องแบ่งกันใช้ช่องสัญญาณที่ถูกกำหนดมาสำหรับใช้งานร่วมกันอย่างเป็นธรรม มาตรฐาน IEEE 802.11 ได้กำหนดให้ใช้กลไก CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) เพื่อจัดสรรการใช้ช่องสัญญาณร่วมกันดังกล่าว

CSMA with Random Back-Off

กลไก CSMA (Carrier Sense Multiple Access) with Random Back-Off เป็นเทคนิคอย่างง่ายสำหรับจัดสรรการเข้าใช้ช่องสัญญาณของผู้ใช้แต่ละคน (ซึ่งต้องแบ่งกันใช้ช่องสัญญาณร่วมนี้) อย่างยุติธรรม กลไกนี้เป็นที่ยอมรับและนิยมใช้กันอย่างแพร่หลาย เช่น ในมาตรฐาน IEEE 802.3 Ethernet LAN หลักการทำงานของกลไก CSMA คือ เมื่อสถานีหนึ่งต้องการเข้าใช้ช่องสัญญาณ สถานีดังกล่าวจะต้องตรวจสอบช่องสัญญาณก่อนว่ามีสถานีอื่นทำการรับส่งสัญญาณข้อมูลอยู่หรือไม่และรอจนกว่าช่องสัญญาณจะว่าง เมื่อช่องสัญญาณว่างแล้วสถานีที่ต้องการเข้าใช้ช่องสัญญาณจะต้องรอต่อไปอีกระยะหนึ่ง (Random Back-Off) ซึ่งแต่ละสถานีได้กำหนดระยะเวลาในการรอดังกล่าวไว้แล้วด้วยการสุ่มค่าหลังจากเสร็จการใช้ช่องสัญญาณครั้งก่อน สถานีที่สุ่มได้ค่าระยะเวลาในการรอน้อยกว่าก็จะมีสิทธิในการเข้าใช้ช่องสัญญาณก่อน แต่อย่างไรก็ตามในบางกรณีกลไกดังกล่าวอาจจะกำหนดให้สถานีมากกว่าหนึ่งสถานีส่งข้อมูลในเวลาพร้อมๆ กันซึ่งจะทำให้เกิดการชนกันของสัญญาณได้ ซึ่งหากเกิดการชนกันของสัญญาณขึ้นจะต้องมีการส่งสัญญาณข้อมูลเดิมซ้ำอีกครั้งด้วยกลไกที่กล่าวมาแล้วข้างต้น

CSMA/CD

กลไก CSMA/CD (Collision Detection) เป็นเทคนิคที่รู้จักกันดีซึ่งถูกนำมาใช้ในมาตรฐาน IEEE 802.3 Ethernet LAN ซึ่งการทำงานกลไก CSMA/CD โดยหลักแล้วเป็นเช่นเดียวกับที่กล่าวไว้ในส่วนของ CSMA with Random Back-Off แต่จะมีรายละเอียดเพิ่มเติมเกี่ยวกับการตรวจสอบว่าเกิดการชนกันของสัญญาณหรือไม่ ในกรณีนี้สถานีที่กำลังทำการส่งสัญญาณข้อมูลอยู่จะต้องคอยตรวจสอบด้วยว่ามีการชนกันของสัญญาณเกิดขึ้นหรือไม่ (ในขณะเดียวกันกับที่ทำการส่งสัญญาณข้อมูล) โดยการตรวจวัดระดับ voltage ของสัญญาณในสายสัญญาณว่ามีค่าสูงกว่าปกติหรือไม่ ซึ่งหากระดับ voltage ของสัญญาณในสายสัญญาณในสายสัญญาณมีค่าสูงกว่าค่าที่กำหนดแสดงว่าเกิดการชนกันของสัญญาณขึ้น ในกรณีดังกล่าวสถานีที่กำลังส่งสัญญาณข้อมูลอยู่จะต้องยกเลิกการส่งสัญญาณทันทีและปฏิบัติตามกลไกที่กล่าวมาแล้วข้างต้นเพื่อทำการส่งข้อมูลเดิมซ้ำอีกต่อไป

CSMA/CA with Acknowledgement

เป็นที่ควรสังเกตว่าเทคนิค CSMA/CD ไม่สามารถนำมาใช้กับ WLAN ซึ่งใช้การสื่อสารแบบไร้สายได้ สาเหตุหลักๆ ก็คือการตรวจสอบการชนกันของสัญญาณในระหว่างที่ทำการส่งสัญญาณจะต้องใช้อุปกรณ์รับส่งคลื่นวิทยุที่เป็น Full Duplex (สามารถรับและส่งสัญญาณในเวลาเดียวกันได้) ซึ่งจะมีราคาแพงกว่าอุปกรณ์รับส่งคลื่นวิทยุที่ไม่สามารถรับและส่งสัญญาณในเวลาเดียวกัน นอกจากนี้แต่ละสถานีใน BSS หรือ IBSS อาจไม่ได้ยินสัญญาณจากสถานีอื่นทุกสถานีหรือปัญหาที่เรียกว่า Hidden Node Problem (ดังในรูปที่ 3: สถานี A ได้ยินสัญญาณจากสถานีแม่ข่าย (Access Point) แต่ไม่ได้ยินสัญญาณจากสถานี C และในทางกลับกันสถานี C ไม่ได้ยินสัญญาณจากสถานี A แต่ได้ยินสัญญาณจากสถานีแม่ข่าย ซึ่งสถานการณ์ดังกล่าวนี้เป็นสถานการณ์เกิดขึ้นใน WLAN โดยทั่วไป) ดังนั้นการตรวจสอบการชนกันของสัญญาณโดยตรงเป็นไปได้ยากหรือเป็นไปไม่ได้เลย มาตรฐาน IEEE 802.11 จึงได้กำหนดให้ใช้เทคนิค CSMA/CA with Acknowledgement สำหรับการจัดสรรการเข้าใช้ช่องสัญญาณของแต่ละสถานีเพื่อแก้ไขปัญหาเหล่านี้ ซึ่งการทำงานของกลไก CSMA/CA โดยหลักแล้วเป็นเช่นเดียวกับที่กล่าวไว้ในส่วนของ CSMA with Random Back-Off แต่จะมีรายละเอียดเพิ่มเติมเกี่ยวกับการหลีกเลี่ยงไม่ให้เกิดการชนกันของสัญญาณและเทคนิคสำหรับการตรวจสอบว่าเกิดการชนของสัญญาณหรือไม่แบบเป็นนัย โดยสถานีผู้ส่งสัญญาณข้อมูลจะต้องรอรับ Acknowledgement จากสถานีที่ส่งข้อมูลไปให้ หากไม่ได้รับ Acknowledgement กลับมาภายในเวลาที่กำหนดจะถือว่าเกิดการชนของสัญญาณขึ้นและต้องทำการส่งข้อมูลเดิมซ้ำอีกต่อไป

สำหรับการหลีกเลี่ยงไม่ให้เกิดการชนกันของสัญญาณนั้น มาตรฐาน IEEE 802.11 ได้ใช้กลไกที่เรียกว่า Virtual Carrier Sense เพื่อแก้ไขปัญหาที่แต่ละสถานีใน BSS หรือ IBSS อาจไม่ได้ยินสัญญาณจากสถานีอื่นบางสถานี (Hidden Node Problem) กลไกดังกล่าวมีการทำงานดังนี้ เมื่อสถานีที่ต้องการจะส่งแพ็กเก็ตข้อมูลได้รับสิทธิในการเข้าใช้ช่องสัญญาณแล้วจะทำการส่งแพ็กเก็ตสั้นๆ ที่เรียกว่า RTS (Request To Send) เพื่อเป็นการจองช่องสัญญาณ ก่อนที่จะส่งแพ็กเก็ตข้อมูลจริง ซึ่งแพ็กเก็ต RTS ประกอบไปด้วยระยะเวลาที่คาดว่าใช้ช่องสัญญาณจนแล้วเสร็จ (Duration ID) รวมถึง Address ของสถานีผู้ส่งและผู้รับ เมื่อสถานีผู้รับได้ยินสัญญาณ RTS ก็จะตอบรับกลับมาด้วยการส่งสัญญาณ CTS (Clear To Send) ซึ่งจะบ่งบอกข้อมูลระยะเวลาที่คาดว่าสถานีที่กำลังจะทำการส่งข้อมูลนั้นจะใช้ช่องสัญญาณจนแล้วเสร็จ หลักการก็คือทุกๆสถานีใน BSS หรือ IBSS ควรจะได้ยินสัญญาณ RTS หรือไม่ก็ CTS อย่างใดอย่างหนึ่งหรือทั้งสองอย่าง เมื่อได้รับ RTS หรือ CTS ทุกๆสถานีจะ

ทราบถึงว่าช่วงเวลาที่ระบุไว้ใน Duration ID ซึ่งช่องสัญญาณจะถูกใช้และทุกสถานีที่ยังไม่ได้รับสิทธิในการเข้าใช้ช่องสัญญาณจะตั้งค่า NAV (Network Allocation Vector) ให้เท่ากับ Duration ID ซึ่งแสดงถึงช่วงเวลาที่ยังไม่สามารถเข้าใช้ช่องสัญญาณได้ ทุกๆสถานีจะใช้กลไก Virtual Carrier Sense ดังกล่าวผนวกกับการฟังสัญญาณในช่องสัญญาณจริงๆ ในการตรวจสอบว่าช่องสัญญาณว่างอยู่หรือไม่

การทำงานเพื่อเชื่อมต่อ

ในการเชื่อมต่อกันของอุปกรณ์นั้น จำเป็นต้องใช้ข้อมูลอันหนึ่งร่วมกันคือชื่อพื้นฐานของการทำงาน (basic name) หรือชื่อของเครือข่ายที่จะติดต่อกัน ซึ่งเราจะเรียกชื่อนี้ว่า SSID (Service Set Identification) ในการเชื่อมต่อระหว่างอุปกรณ์ต่างๆ นั้นจะต้องมีการใช้ SSID ตรงกันเพื่อเชื่อมต่อกันอย่างถูกต้อง แต่ในการทำงานจริงจะไม่มีความปลอดภัย เนื่องจากค่า SSID จะถูก broadcast โดย Access Point

กลไกรักษาความปลอดภัยในมาตรฐาน IEEE 802.11

มาตรฐาน IEEE 802.11 ได้กำหนดให้มีทางเลือกสำหรับสร้างความปลอดภัยให้กับเครือข่าย LAN แบบไร้สาย ด้วยกลไกซึ่งมีชื่อเรียกว่า WEP (Wired Equivalent Privacy) ซึ่งถูกออกแบบมาเพื่อเพิ่มความปลอดภัยกับเครือข่าย LAN แบบไร้สายให้ใกล้เคียงกับความปลอดภัยของเครือข่าย LAN แบบที่ใช้สายนำสัญญาณ (IEEE 802.3 Ethernet) บทบาทของ WEP แบ่งเป็น 2 ส่วนหลักๆ คือ

- การเข้ารหัสข้อมูล (Encryption) เพื่อป้องกันมิให้ผู้ที่ไม่มีรหัสข้อมูลสามารถเข้าใจหรือเปลี่ยนแปลงข้อมูลที่แพร่กระจายอยู่ในอากาศได้
- การตรวจสอบผู้ใช้ (Authentication) เพื่อป้องกันมิให้ผู้ที่ไม่มีรหัสผ่านสามารถเข้าใช้เครือข่ายได้

หมายเหตุ มาตรฐาน IEEE 802.11 จะกำหนดให้มีมาตรการรักษาความปลอดภัยที่แน่นหนาขึ้น โดยคณะทำงาน IEEE 802.11i เป็นผู้รับผิดชอบหน้าที่ดังกล่าว

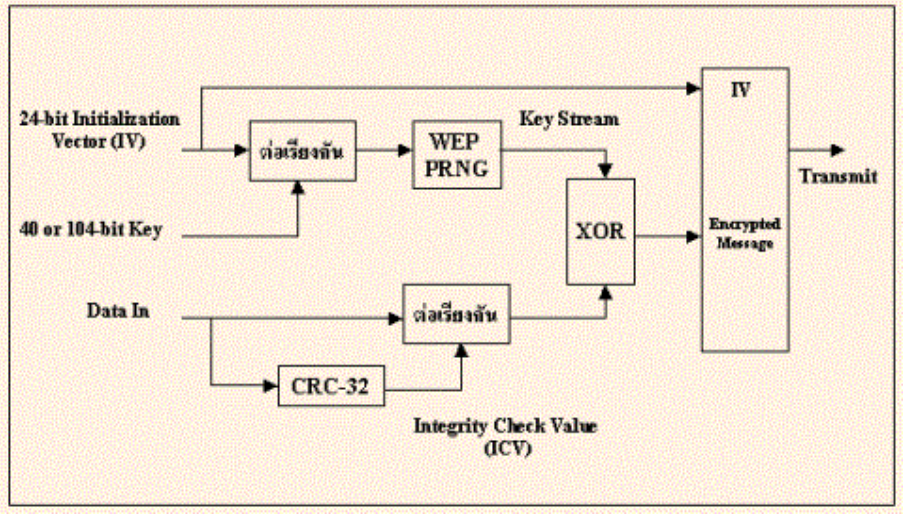
การเข้าและถอดรหัสข้อมูล (WEP Encryption/Decryption)

WEP ใช้หลักการในการเข้าและถอดรหัสข้อมูลที่เป็นแบบ symmetrical (นั่นคือรหัสที่ใช้ในการเข้ารหัสข้อมูลจะเป็นตัวเดียวกันกับรหัสที่ใช้สำหรับการถอดรหัสข้อมูล)

WEP Encryption

การทำงานของการเข้ารหัสข้อมูลในกลไก WEP เป็นดังนี้

- Key ขนาด 64 หรือ 128 บิต ถูกสร้างขึ้นโดยการนำเอารหัสลับซึ่งมีความยาว 40 หรือ 104 บิต มาต่อรวมกับข้อความเริ่มต้น IV (Initialization Vector) ขนาด 24 บิตที่ถูกกำหนดแบบสุ่มขึ้นมา
- Integrity Check Value (ICV) ขนาด 32 บิต ถูกสร้างขึ้นโดยการคำนวณค่า CRC-32 (32-bit Cyclic Redundant Check) จากข้อมูลดิบที่จะส่งออกไป (ICV ซึ่งจะถูกนำไปต่อรวมกับข้อมูลดิบ มีไว้สำหรับตรวจสอบความถูกต้องของข้อมูลหลังจากการถอดรหัสแล้ว)
- ข้อความที่มีความสุ่ม (Key Stream) ขนาดเท่ากับความยาวของข้อมูลดิบที่จะส่งกับอีก 32 บิต (ซึ่งเป็นความยาวของ ICV) ถูกสร้างขึ้นโดยหน่วยสร้างข้อความที่มีความสุ่มหรือ PRNG (Pseudo-Random Number Generator) ที่มีชื่อเรียกว่า RC4 ซึ่งจะใช้ Key ที่กล่าวมาข้างต้นเป็น Input (หรือ Seed) หมายเหตุ PRNG จะสร้างข้อความสุ่มที่แตกต่างกันสำหรับ Seed แต่ละค่าที่ใช้
- ข้อความที่ได้รับการเข้ารหัส (Ciphertext) ถูกสร้างขึ้นโดยการนำเอา ICV ต่อกับข้อมูลดิบแล้วทำการ XOR แบบบิตต่อบิตกับข้อความสุ่ม (Key Stream) ซึ่ง PRNG ได้สร้างขึ้น
- สัญญาณที่จะถูกส่งออกไปคือ ICV และข้อความที่ได้รับการเข้ารหัส (Ciphertext)

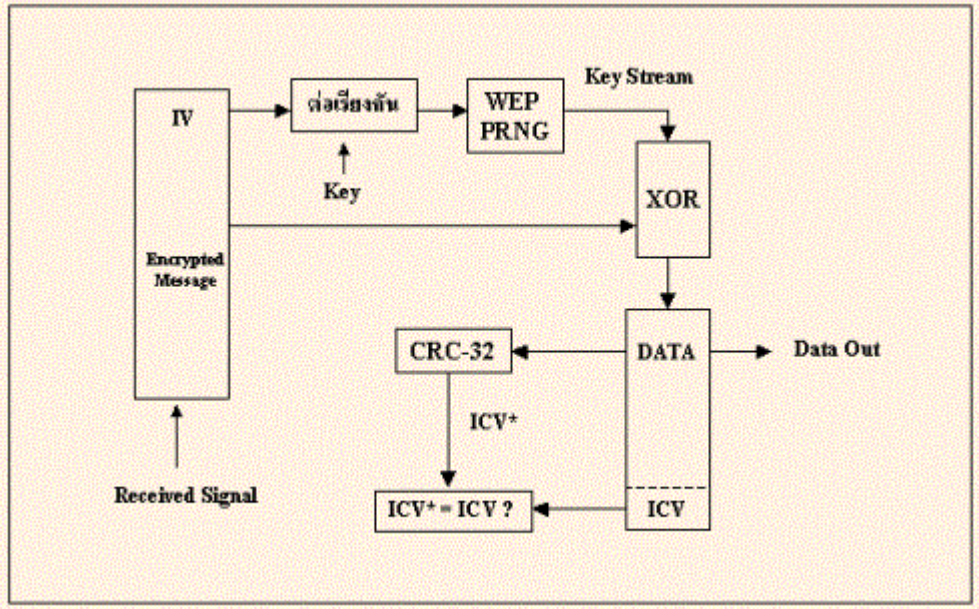


รูปที่ 60 WEP Encryption

WEP Decryption

การทำงานของการถอดรหัสข้อมูลในกลไก WEP เป็นดังนี้

- Key ขนาด 64 หรือ 128 บิต ถูกสร้างขึ้นโดยการนำเอารหัสลับซึ่งมีความยาว 40 หรือ 104 บิต (ซึ่งเป็นรหัสลับเดียวกับที่ใช้ในการเข้ารหัสข้อมูล) มาต่อรวมกับ IV ที่ถูกส่งมากับสัญญาณที่ได้รับ
- PRNG สร้างข้อความสุ่ม (Key Stream) ที่มีขนาดเท่ากับความยาวของข้อความที่ได้รับการเข้ารหัสและถูกส่งมา โดยใช้ Key ที่กล่าวมาข้างต้นเป็น Input
- ข้อมูลดิบและ ICV ถูกถอดรหัสโดยการนำเอาข้อความที่ได้รับมา XOR แบบบิตต่อบิตกับข้อความสุ่ม (Key Stream) ซึ่ง PRNG ได้สร้างขึ้น
- สร้าง ICV' โดยการคำนวณค่า CRC-32 จากข้อมูลดิบที่ถูกถอดรหัสแล้วเพื่อนำมาเปรียบเทียบกับค่า ICV ที่ได้ถูกส่งมา หากค่าทั้งสองตรงกัน (ICV' = ICV) แสดงว่าการถอดรหัสถูกต้องและผู้ที่ส่งมาได้รับอนุญาต (มีรหัสลับของเครือข่าย) แต่หากค่าทั้งสองไม่ตรงกันแสดงว่าการถอดรหัสไม่ถูกต้องหรือผู้ที่ส่งมาไม่ได้รับอนุญาต



รูปที่ 61 WEP Decryption

การตรวจสอบผู้ใช้ (Authentication)

สำหรับเครือข่าย IEEE 802.11 LAN ผู้ใช้ (เครื่องลูกข่าย) จะมีสิทธิในการรับส่งสัญญาณข้อมูลในเครือข่ายได้ก็ต่อเมื่อได้รับการตรวจสอบแล้วได้รับอนุญาต ซึ่งมาตรฐาน IEEE 802.11 ได้กำหนดให้มีกลไกสำหรับการตรวจสอบผู้ใช้ (Authentication) ใน 2 ลักษณะคือ Open System Authentication และ Shared Key Authentication ซึ่งเป็นดังต่อไปนี้

Open System Authentication

การตรวจสอบผู้ใช้ในลักษณะนี้เป็นทางเลือกแบบ default ที่กำหนดไว้ในมาตรฐาน IEEE 802.11 ในการตรวจสอบแบบนี้จะไม่ตรวจสอบรหัสลับจากผู้ใช้ ซึ่งอาจกล่าวได้ว่าเป็นการอนุญาตให้ผู้ใช้ใดๆ ก็ได้สามารถเข้ามารับส่งสัญญาณในเครือข่ายนั่นเอง แต่อย่างไรก็ตามในการตรวจสอบแบบนี้อุปกรณ์ที่ทำหน้าที่เป็นสถานีแม่ข่ายไม่จำเป็นต้องอนุญาตให้สถานีผู้ใช้เข้ามาใช้เครือข่ายได้เสมอไป ในกรณีนี้บทบาทของ WEP จึงเหลือแต่เพียงการเข้ารหัสข้อมูลเท่านั้น กลไกการตรวจสอบแบบ open system authentication มีขั้นตอนการทำงานดังต่อไปนี้

สถานีที่ต้องการจะเข้ามาร่วมใช้เครือข่ายจะส่งข้อความซึ่งไม่ถูกเข้ารหัสเพื่อขอรับการตรวจสอบ (Authentication Request Frame) ไปยังอุปกรณ์ที่ทำหน้าที่เป็นสถานีแม่ข่าย โดยในข้อความดังกล่าวจะมีการแสดงความจำนงเพื่อรับการตรวจสอบแบบ open system

อุปกรณ์ที่ทำหน้าที่เป็นสถานีแม่ข่ายโต้ตอบด้วยข้อความที่แสดงถึงการตอบรับหรือปฏิเสธ Request ดังกล่าว

Shared Key Authentication

การตรวจสอบผู้ใช้แบบ shared key authentication จะอนุญาตให้สถานีผู้ใช้ซึ่งมีรหัสลับของเครือข่ายนี้เท่านั้นที่สามารถเข้ามารับส่งสัญญาณกับอุปกรณ์ที่ทำหน้าที่เป็นสถานีแม่ข่ายได้ โดยมีการใช้เทคนิคการถามตอบที่ใช้กันทั่วไปผนวกกับการเข้ารหัสด้วย WEP เป็นกลไกสำหรับการตรวจสอบ (ดังนั้นการตรวจสอบแบบนี้จะทำได้ก็ต่อเมื่อมีการ Enable การเข้ารหัสด้วย WEP) กลไกการตรวจสอบดังกล่าวมีขั้นตอนการทำงานดังต่อไปนี้

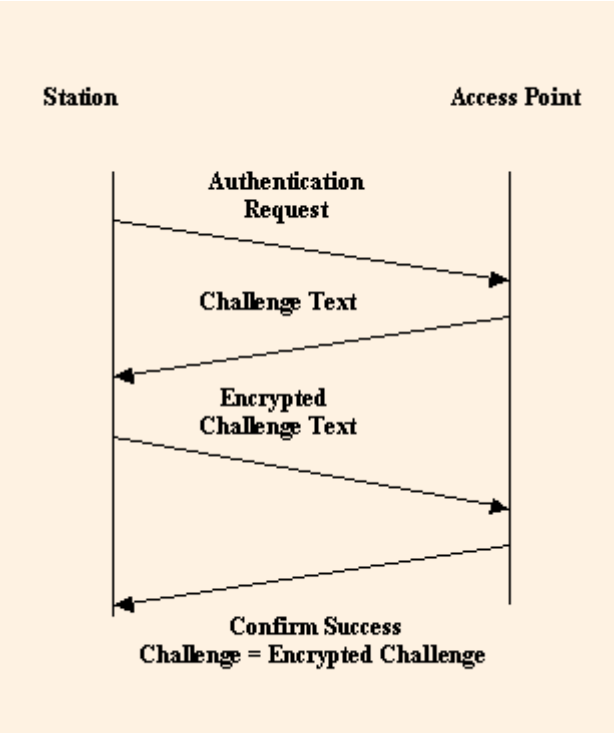
สถานีผู้ใช้ที่ต้องการจะเข้ามาร่วมใช้เครือข่ายจะส่งข้อความซึ่งไม่ถูกเข้ารหัสเพื่อขอรับการตรวจสอบ (Authentication Request Frame) ไปยังอุปกรณ์ที่ทำหน้าที่เป็นสถานีแม่ข่าย โดยในข้อความดังกล่าวจะมีการแสดงความจำนงเพื่อรับการตรวจสอบแบบ shared key

หากสถานีแม่ข่ายต้องการตอบรับ Request ดังกล่าว จะมีการส่งข้อความที่แสดงถึงการตอบรับและคำถาม (challenge text) มายังเครื่องลูกข่าย ซึ่ง challenge text ดังกล่าวมีขนาด 128 ไบต์และถูกสุ่มขึ้นมา (โดยอาศัย PRNG) หากอุปกรณ์แม่ข่ายไม่ต้องการตอบรับ Request ดังกล่าว จะมีการส่งข้อความที่แสดงถึงการไม่ตอบรับ ซึ่งเป็นการสิ้นสุดของการตรวจสอบครั้งนี้

หากมีการตอบรับจากสถานีแม่ข่าย สถานีผู้ใช้ที่ขอรับการตรวจสอบจะทำการเข้ารหัสข้อความคำถามที่ถูกส่งมาโดยใช้รหัสลับของเครือข่ายแล้วส่งกลับไปยังสถานีแม่ข่าย

สถานีแม่ข่ายทำการถอดรหัสข้อความที่ตอบกลับมาโดยใช้รหัสลับของเครือข่าย หลังจากถอดรหัสแล้วหากข้อความที่ตอบกลับมาตรงกับข้อความคำถาม (challenge text) ที่ส่งไป สถานีแม่ข่ายจะส่งข้อความที่แสดง

ถึงการอนุญาตให้สถานีผู้ใช้นี้เข้าใช้เครือข่ายได้ แต่หากข้อความที่ตอบกลับมาไม่ตรงกับข้อความคำถาม สถานีแม่ข่ายจะโต้ตอบด้วยข้อความที่แสดงถึงการไม่อนุญาต



รูปที่ 62 WEP Shared Key Authentication

ในการศึกษาด้านการรักษาความปลอดภัยควรมีลำดับการศึกษา โดยเริ่มต้นที่โพรโตคอลที่เกี่ยวข้องซึ่งในที่นี้คือ IEEE 802.11 และศึกษาเกี่ยวกับปัญหาความปลอดภัยของโพรโตคอลดังกล่าว ซึ่งก็มีมากมายทั้งการดักจับ การรบกวนสัญญาณ การสร้างโหนดปลอม การปลอมแปลงตัวบุคคล การเข้าใช้งานเครือข่ายโดยไม่ได้รับอนุญาต เป็นต้น ซึ่งปัญหาดังกล่าวจะสามารถใช้ CIA มาช่วยแก้ปัญหาได้ หลักจากนั้นจึงวิเคราะห์ปัญหาในมุมมองของ CIA และศึกษาเทคนิคต่างๆ ที่เพิ่มเติมเข้ามาเพื่อสร้าง CIA ในระบบเครือข่ายไร้สายเช่น การทำ MAC Address Filtering การใช้ WEP , WPA , WPA2 การสร้างรูปแบบการ Authentication อย่างเป็นระบบตลอดจนการใช้ VPN สำหรับการใช้งานที่ปลอดภัยมากยิ่งขึ้น

WPA

WPA จะ เข้ารหัสลับ ข้อมูล และจะตรวจสอบเพื่อให้แน่ใจว่าไม่มีการปรับเปลี่ยน คีย์เพื่อความปลอดภัยของเครือข่าย นอกจากนั้น WPA ยังรับรองความถูกต้องผู้ใช้ เพื่อช่วยทำให้มั่นใจว่าเฉพาะบุคคลที่ได้รับอนุญาตเท่านั้นที่จะสามารถเข้าถึงเครือข่ายได้

WPA มีการรับรองความถูกต้องสองประเภท คือ WPA และ WPA2 WPA ได้รับการออกแบบให้ทำงานกับการ์ดเชื่อมต่อเครือข่ายแบบไร้สาย แต่อาจไม่สามารถทำงานกับจุดเข้าใช้งานหรือเราเตอร์รุ่นที่เก่ากว่า WPA2 จะมีความปลอดภัยมากกว่า WPA แต่จะไม่ทำงานกับการ์ดเชื่อมต่อเครือข่ายรุ่นเก่ากว่าบางรุ่น WPA ได้รับการออกแบบให้ใช้กับเซิร์ฟเวอร์การรับรองความถูกต้อง 802.1X ซึ่งจะให้คีย์ที่แตกต่างกันกับผู้ใช้แต่ละราย ซึ่งจะเรียกว่า WPA-Enterprise หรือ WPA2-Enterprise นอกจากนั้นยังสามารถใช้ในโหมดคีย์ก่อนการใช้ร่วมกัน (PSK) ที่ผู้ใช้ทุกคนจะได้รับวลีรหัสผ่านเดียวกัน ซึ่งจะเรียกว่า WPA-Personal หรือ WPA2-Personal

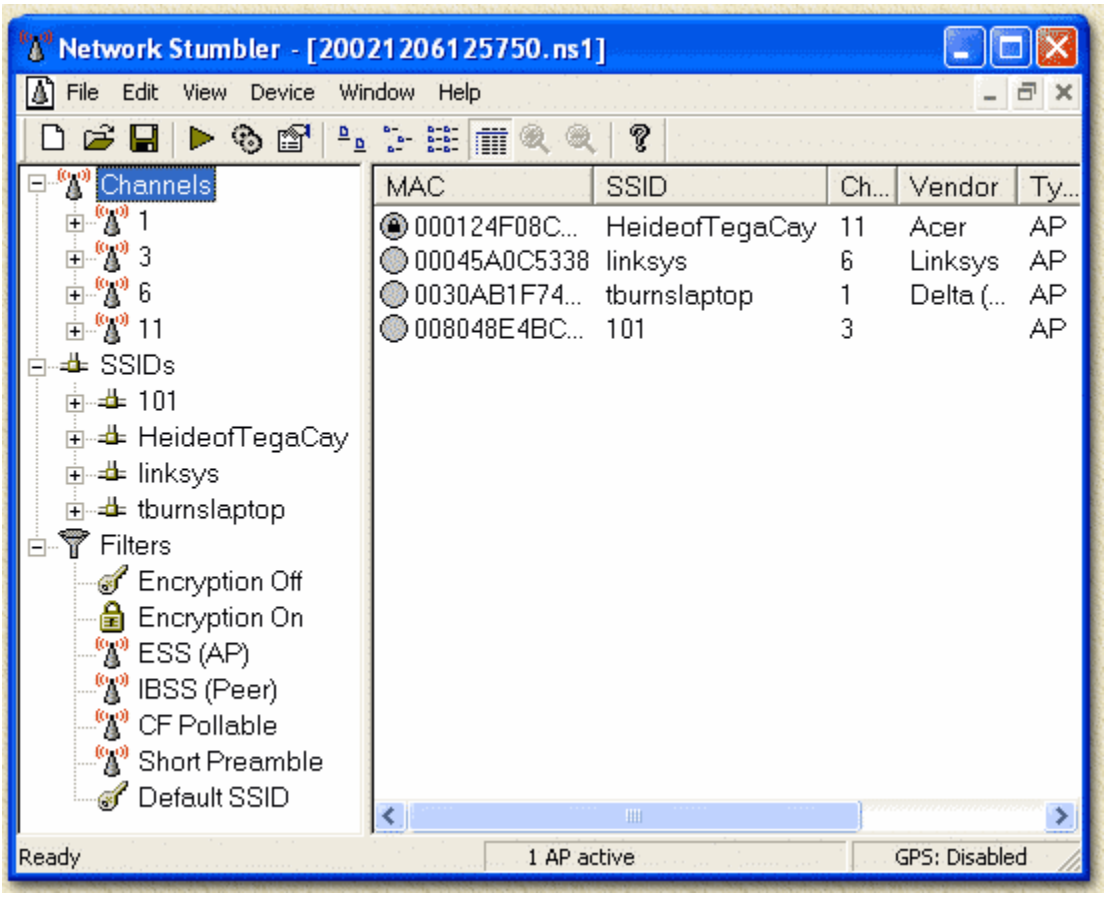
802.1x

การรับรองความถูกต้อง 802.1X สามารถช่วยสนับสนุนการรักษาความปลอดภัยสำหรับเครือข่าย 802.11 แบบไร้สาย และเครือข่าย อีเทอร์เน็ตแบบมีสาย 802.1X จะใช้เซิร์ฟเวอร์การรับรองความถูกต้องเพื่อตรวจสอบผู้ใช้ และกำหนดการเข้าใช้เครือข่าย 802.1X สามารถทำงานกับคีย์ Wired Equivalent Privacy (WEP) หรือ Wi-Fi Protected Access (WPA) บนเครือข่ายแบบไร้สายได้ โดยปกติการรับรองความถูกต้องประเภทนี้จะใช้เมื่อเชื่อมต่อกับเครือข่ายในที่ทำงาน

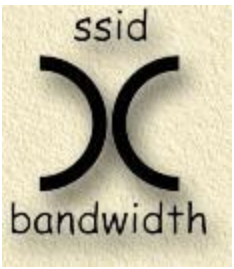
การโจมตีเครือข่ายไร้สาย

1. War-driving, war-walking, war-flying, war-chalking

เป็นกระบวนการในการค้นหา Access-point ที่เปิดให้ใช้บริการได้ โดยการทำงานจะมีลักษณะเดียวกับการทำ war-dialing คือแฮกเกอร์จะใช้วิธีขับรถ , เดิน หรือบิน ไปมาในเมืองแล้วใช้อุปกรณ์ หรือโปรแกรม (NetStumbler) ในการค้นหาว่ามีบริเวณใดบ้างที่มี acces-point เปิดให้ใช้บริการอยู่

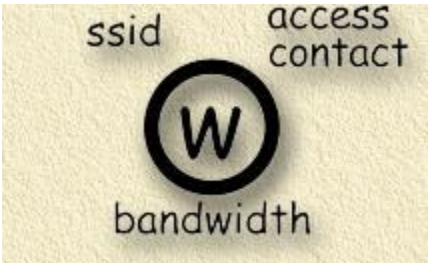


หลังจากนั้นจะมีการทำเครื่องหมาย (war-chalking) บอกว่าบริเวณนั้นมีเครือข่ายเป็นอย่างไรตัวอย่างสัญลักษณ์ที่มีการใช้งานกันอย่างแพร่หลาย



รูปนี้เป็นรูปที่แทนบริเวณดังกล่าวสามารถใช้งานเครือข่ายไร้สายได้ ซึ่งผู้ใช้งานจะมีสิทธิที่จะใช้งานบริเวณนั้นหรือไม่ก็ตาม การรักษาความปลอดภัยในบริเวณดังกล่าวต่ำมาก สัญลักษณ์ดังกล่าวอาจระบุ SSID และ Bandwidth ให้ด้วย

รูปนี้เป็นรูปที่หมายถึงในบริเวณดังกล่าวมีเครือข่ายไร้สาย (SSID) แต่ไม่สามารถใช้งานได้ หรือสามารถลักลอบใช้งานได้ยาก เนื่องจากมีการป้องกันในบางลักษณะ



รูปนี้เป็นรูปที่หมายถึงในบริเวณดังกล่าวมีเครือข่ายไร้สาย (SSID) แต่ป้องกันด้วยการเข้ารหัส (WEP) แต่เมื่อพิจารณาระดับความปลอดภัยของ WEP แล้วก็นับว่ายังไม่ปลอดภัยนักเนื่องจากสามารถใช้โปรแกรมในการแฮกเข้าสู่ระบบได้

2. Insertion Attacks

การทำ Insertion Attack คือการนำเอาอุปกรณ์ที่ไม่ได้รับอนุญาตเข้าไปในพื้นที่ของเครือข่ายไร้สายเพื่อเข้าไปใช้งานระบบเครือข่าย เราสามารถแบ่งได้เป็น 2 รูปแบบคือ

2.1 Plug-in Unauthorized Clients คือการนำเอาเครื่องลูกข่ายเช่น laptop , PDA เข้าไปในพื้นที่ของเครือข่ายไร้สายโดยไม่ได้รับอนุญาต ซึ่งในกรณีนี้ถ้า base station ต้องการรหัสผ่านก็จะไม่สามารถลักลอบเข้าใช้งานเครือข่ายในลักษณะนี้ได้ แต่ถ้า base station ไม่มีการใช้รหัสผ่านเพื่อเข้าใช้งานผู้บุกรุกก็สามารถลักลอบเข้าใช้งานในลักษณะนี้ได้

2.2 Plug-in Unauthorized Renegade Base Station คือการนำเอา base station ไปวางไว้ในพื้นที่ที่มีการใช้งานเครือข่ายไร้สาย โดยเครื่อง base station ที่ใช้จะมีกำลังส่งมากกว่า เมื่อเครื่องลูกข่ายที่ใช้งานในพื้นที่นั้นได้รับสัญญาณที่มีความแรงมากกว่า จะสับเปลี่ยนการเชื่อมต่อไปยัง base station ใหม่โดยอัตโนมัติ ซึ่งผู้บุกรุกที่เป็นเจ้าของ base station นั้นก็จะสามารถโจมตีหรือเปลี่ยนแปลงข้อมูลที่รับส่งอยู่ได้ สำหรับการป้องกันแก้ไขในบริษัทนั้น อาจทำได้โดยการกำหนดนโยบายไม่ให้มีการนำ base station มาเชื่อมต่อเข้าในพื้นที่บริษัทเด็ดขาดเป็นต้น

3. Interception and monitoring wireless traffic

สำหรับการบุกรุกในระบบเครือข่ายแบบใช้สายนั้น การดักจับข้อมูลในเครือข่าย ถือว่าเป็นการบุกรุกระบบที่แพร่หลายอย่างมาก ซึ่งหลักการเดียวกันนี้ก็สามารถนำมาใช้ในเครือข่ายแบบไร้สายเช่นกัน การโจมตีที่มีการดักจับข้อมูลในเครือข่ายเป็นพื้นฐานมีดังนี้

3.1 Wireless Sniffer

สำหรับการดักจับข้อมูลในเครือข่ายแบบมีสายนั้นเป็นวิธีการโจมตีที่มีมานานแล้ว ซึ่งแฮกเกอร์จะใช้สำหรับการดักจับข้อมูล username และ password ของผู้ใช้งานในเครือข่าย สำหรับการดักจับข้อมูลในเครือข่ายไร้สายนั้น แฮกเกอร์สามารถนำวิธีการดังกล่าวไปใช้งานได้

ในการดักจับข้อมูลในเครือข่ายแบบไร้สายกับเครือข่ายแบบมีสายนั้น มีข้อแตกต่างกันอยู่ข้อหนึ่งนั่นคือ ในการดักจับข้อมูลในเครือข่ายแบบมีสายนั้น ผู้บุกรุกจะเจาะระบบแล้ววางโปรแกรม Sniffer ในเครื่องเซิร์ฟเวอร์ หรือเครื่องใดเครื่องหนึ่งใน broadcast domain ในระบบที่ต้องการ ซึ่งวิธีการดังกล่าวผู้บุกรุกสามารถทำกับเครื่องคอมพิวเตอร์เครื่องใดๆ ก็ได้ในโลก โดยที่ผู้บุกรุกจะอยู่ในสถานที่อื่นๆ แต่สำหรับกรณีของเครือข่ายแบบมีสายนั้น ผู้บุกรุกจะต้องนำเอาอุปกรณ์ไปวางไว้ในพื้นที่ของเครือข่ายไร้สายเท่านั้น

3.2 Hijacking the session

เมื่อผู้บุกรุกสามารถดักจับข้อมูลในเครือข่ายได้ ก็สามารถส่งข้อมูลแทรกเข้าไปในการเชื่อมต่อใดๆ ก็ได้ ซึ่งทำให้ผู้บุกรุกสามารถส่งคำสั่งไปยังเครื่องที่เชื่อมต่ออยู่ได้

3.3 Broadcast Monitoring

ในกรณีที่ base station เชื่อมต่อยู่กับฮับ ไม่ใช่สวิทช์ ข้อมูลทั้งหมดในฮับจะส่งเข้ามายัง base station แล้วกระจายอยู่ในเครือข่ายไร้สายด้วยเช่นกัน ในกรณีนี้ผู้บุกรุกที่ดักจับข้อมูลในเครือข่ายไร้สายก็จะสามารถดักจับข้อมูลที่ถูกส่งมาจากฮับได้

3.4 ArpSpoof Monitoring and Hijacking

สำหรับเครือข่ายที่เป็นสวิทช์ทั้งหมด ก็สามารถทำการดักจับข้อมูลและขโมยเซสชั่นได้เช่นกัน โดยผู้บุกรุกจะใช้เทคนิค arpspoof เพื่อให้สวิทช์นำเอาข้อมูลมากระจายในพอร์ทที่เชื่อมต่อกับเครือข่ายไร้สายได้ ซึ่งการกระทำดังกล่าวจะทำให้ผู้บุกรุกดักจับข้อมูลและขโมยเซสชั่นได้
(dsniff:http://www.monkey.org/~dugsong/dsniff/)

นอกจากผู้บุกรุกจะใช้เทคนิคของการทำ arpspoof เพื่อดักจับข้อมูลและขโมยเซสชั่นได้แล้ว ยังสามารถใช้โปรแกรมอื่นๆ เพื่อขโมยเซสชั่นของ ssl และ ssh ได้ด้วย

3.5 BaseStation Clone (Evil Twin) intercept traffic

ในกรณีที่ผู้บุกรุกสามารถนำเอา access-point ที่มีกำลังส่งสูง เข้าไปในเครือข่ายไร้สายได้ ผู้บุกรุกสามารถสร้าง honeypot network และ honeypot server เพื่อให้เครื่องลูกข่ายที่เข้ามาติดต่อเข้ากับ access-point

ของตนเข้ามาใช้งาน honeypot network และลอกอินเข้าสู่ honeypot server ที่ตนสร้างขึ้น เพื่อดักจับข้อมูล รหัสผ่านเป็นต้น

4. AP and Client Misconfiguration

โดยปกติแล้ว base station ที่ส่งมาจากโรงงานนั้นมีการตั้งค่าความปลอดภัยให้ต่ำสุด เพื่อให้การทดสอบและการใช้งานสามารถทำได้โดยง่าย โดยโยนภาระการตั้งค่าเพื่อความปลอดภัยให้แก่ผู้ดูแลระบบ ในกรณีที่ผู้ดูแลระบบไม่มีความรู้ในการสร้างความปลอดภัย ก็จะไม่มีการปรับเปลี่ยนค่าดังกล่าว ทำให้เกิดความไม่ปลอดภัยในการใช้งานสูงมาก โดยความไม่ปลอดภัยที่อาจเกิดขึ้นมีดังนี้

4.1 Server Set ID (SSID) -> default ssid

SSID คือ ID ที่ใช้สำหรับการขอเข้าใช้งานในเครือข่ายไร้สาย หรือเป็นรหัสผ่านในการเชื่อมต่อเข้ากับ base station ซึ่งผู้ใช้งานเครือข่ายจะต้องตั้งค่า SSID ให้ตรงกับ base station เท่านั้นจึงจะเข้าใช้งานได้ สำหรับ base station ยี่ห้อต่างๆ นั้นจะมีค่า Default SSID ซึ่งแตกต่างกันออกไปตามผู้ผลิต ซึ่งผู้บุกรุกสามารถใช้ข้อมูลดังกล่าวในการเจาะเข้าสู่ระบบได้

ตัวอย่างค่า default SSID

“tsunami” - Cisco

“101” – 3Com

“RoamAbout Default Network Name” - Lucent/Cabletron

“Default SSID"

“Compaq” - Compaq

“WLAN” – Addtron, a popular AP

“intel” - Intel

“linksys” – Linksys

“Wireless”

ในกรณีของ Access Point ของ Lucent นั้นจะมีโหมดในการรักษาความปลอดภัยอยู่เรียกว่า secure access mode ซึ่งจำเป็นต้องให้เครื่อง client และ base statioin ต้องมี SID ที่ตรงกันจึงจะเชื่อมต่อกันได้ แต่โดยค่า Default นั้นจะไม่มีการใช้งานความสามารถนี้ ซึ่งเครื่อง client จะติดต่อกับ base station นี้ได้โดยใช้ blank SSID หรือ "any"

4.2 Bruteforce Base Station SSID

เนื่องจาก SSID เป็นเสมือนกับรหัสผ่านในการเข้าใช้งานเครือข่ายไร้สาย ผู้บุกรุกจึงต้องหาวิธีการต่างๆ เพื่อให้ได้รหัสผ่านนี้ วิธีการหนึ่งในการค้นหา SSID คือการทำ Bruteforce Dictionary Attack โดยการทดสอบค่า SSID หลายๆ ค่า ถ้าผู้ดูแลระบบตั้งค่า SSID ที่คาดเดาได้ง่าย ผู้บุกรุกจะสามารถหาได้อย่างรวดเร็ว

วิธีการแก้ปัญหานี้คือการตั้งค่า SSID ให้คาดเดาได้ยาก และเปลี่ยนบ่อยๆ ซึ่งก็ไม่เหมาะกับเครือข่ายที่มีผู้ใช้งานปริมาณมาก เพราะจำเป็นต้องแจ้งให้ผู้ใช้งานแต่ละคนเปลี่ยนค่า SSID อยู่บ่อยๆ ซึ่งไม่สะดวกทั้งผู้ใช้งานและผู้ดูแลระบบ

4.3 สามารถเข้ารหัส SSID ได้หรือไม่ ?

ในเครือข่ายแบบไร้สายนั้น ผู้บุกรุกสามารถดักจับข้อมูลในเครือข่ายเพื่อให้ได้ค่า SSID เพื่อเข้าใช้งานระบบเครือข่าย ซึ่งเป็นปัญหาที่คล้ายๆ กับการดักจับรหัสผ่านในเครือข่ายแบบมีสาย ซึ่งปัญหาในเครือข่ายแบบมีสายนั้นเราจะใช้วิธีการเข้ารหัส รหัสผ่านก่อนส่งข้อมูล จึงน่าจะใช้วิธีการดังกล่าวในการเข้ารหัสค่า SID ได้ด้วยเช่นกัน

ในมาตรฐาน 802.11 นั้น มีวิธีการ Wired Equivalent Privacy (WEP) ซึ่งใช้ในการเข้ารหัสแพ็กเก็ตของข้อมูลในการรับส่งอยู่แล้ว แต่น่าเสียดายที่มาตรฐาน 802.11 ไม่ได้มีการใช้งาน WEP เพื่อเข้ารหัสแพ็กเก็ตควบคุม (management packet) ซึ่งก็หมายความว่า ถึงแม้มีการใช้งาน WEP ค่า SSID ก็ยังรับส่งกันเป็น clear text ซึ่งผู้บุกรุกก็ยังดักจับข้อมูลได้

4.4 การไม่ Broadcast SSID จะช่วยป้องกันการ Sniff SSID ได้หรือไม่

โดยค่า Default ของ AP ส่วนใหญ่จะตั้งค่าให้มีการกระจาย SSID โดย Broadcast Beacon Packet ซึ่งทำให้ผู้บุกรุกสามารถดักจับข้อมูล SID ได้ การตั้งค่าให้ AP ไม่กระจาย SSID ผ่าน Beacon packet นั้นถือว่าเป็นการป้องกันการดักจับ SSID ได้ ทำให้ผู้บุกรุกไม่สามารถดักจับข้อมูล SSID ที่ส่งมาจาก AP

แต่การตั้งค่าไม่ให้ AP กระจาย SSID นั้นก็ไม่สามารถป้องกันการดักจับข้อมูลเพื่อค้นหา SSID ได้ทั้งหมด เนื่องจากผู้บุกรุกสามารถดักจับ SSID ได้จากสถานการอื่นๆ เช่น เมื่อผู้ใช้งานที่มี SSID ที่ถูกต้อง เข้าใช้งาน AP จะมีการส่งค่า SSID ที่ถูกต้องไปยัง AP ซึ่งผู้บุกรุกจะรอเหตุการณ์นี้เพื่อดักจับค่า SSID

4.5 Wired Equivalent Privacy (WEP)

WEP มีโหมดการทำงานในการเข้ารหัสคือ

1. No encryption mode
2. 40 bits encryption
3. 64 bits encryptioin
3. 128 bits encryption

สำหรับอุปกรณ์บางตัวนั้นสามารถทำงานได้ถึง 152 bits encryption ซึ่งเพื่อความปลอดภัยแล้วควรใช้การเข้ารหัสที่ 128 bits ขึ้นไป แต่จากการศึกษาด้านความปลอดภัยพบว่าการใช้งาน WEP เพื่อเข้ารหัสข้อมูลเพื่อความปลอดภัยในเครือข่ายไร้สายนั้น สามารถถอดรหัสข้อมูลได้อย่างง่ายดาย โดยรายละเอียดของการค้นคว้าสามารถดูได้จาก

: http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html

: http://www.cs.rice.edu/~astubble/wep/wep_attack.html

: https://ialert.idefense.com/idcontent/ 2002/papers/Wireless.pdf

สำหรับการ crack ข้อมูลเพื่อให้ได้ WEP key นั้นสามารถทำได้โดยการใช้โปรแกรมชื่อว่า Airsnort และโปรแกรม WEPcrack ซึ่งในการ crack จะต้องเก็บข้อมูลแพ็กเก็ตจำนวนมากจากเครือข่าย ซึ่งต้องใช้เวลามากในเครือข่ายปกติ แต่สำหรับเครือข่ายที่มีข้อมูลหนาแน่นมากๆ ก็อาจใช้เวลาเพียง 15 นาทีเท่านั้น

ถึงแม้ว่า WEP จะสามารถ crack ข้อมูลได้ แต่การใช้ WEP ย่อมดีกว่าไม่ใช้ โดยการใช้ WEP นั้นจะมีข้อดีอันหนึ่งที่สำคัญก็คือ สามารถป้องกันการดักจับข้อมูลโดยตรงได้นั่นเอง แต่ก็ยังมีปัญหาของค่า Default WEP Keys เนื่องจากการใช้ WEP นั้นจะต้องใช้รหัสในการเข้ารหัสข้อมูล ปัญหาที่เกิดขึ้นจึงเป็นปัญหาที่คล้ายๆ กับการใช้ SSID นั่นคือ ค่า default ที่ตั้งค่ามาให้แล้ว ซึ่งผู้ดูแลระบบควรจะเปลี่ยนแปลงค่าดังกล่าวด้วย

สำหรับตัวอย่างค่า default ของ WEP sequence นั้นเช่นใน Netgear Access Point จะมีลำดับของ WEP Key ดังนี้

: 10 11 12 13 14

: 21 22 23 24 25

: 31 32 33 34 35

: 41 42 43 44 45

4.6 SNMP community words

ปัญหาข้อหนึ่งที่เกิดขึ้นในอุปกรณ์เครือข่ายไม่เว้นแม้แต่ใน Access Point นั่นคือการตั้งค่า SNMP community word เนื่องจากอุปกรณ์เครือข่ายทุกรุ่น ทุกยี่ห้อจะมีการฝัง SNMP agent สำหรับช่วยบริหารเครือข่ายอยู่แล้ว ซึ่งจะต้องใช้ community word ในการเข้าใช้งาน ปัญหาที่เกิดขึ้นก็จะคล้ายๆ กับปัญหา default SSID คือ แต่ละยี่ห้อ ก็จะมีค่า community word ที่เป็นค่า default ของตัวเอง ซึ่งถ้าผู้บุกรุกทราบค่าดังกล่าว ก็จะสามารถดู หรือสามารถแก้ไขการตั้งค่าบางอย่างใน AP ได้ หรือถ้ามีการฝัง SNMP agent ที่ฝั่ง client ผู้บุกรุกก็สามารถแก้ไขการตั้งค่าบางอย่างใน client ได้เช่นกัน ยกตัวอย่างเช่น base station ของ 3com สามารถแก้ไขค่าต่างๆ ได้โดยใช้ community word คือ "comcomcom" ซึ่งเป็นค่า default แต่ในอุปกรณ์ของ cisco และ lucent/cabletron จะมีการรักษาความปลอดภัยได้ดีกว่าคือจะต้องมีการตั้งค่า community word ใหม่ทุกครั้งก่อนที่ระบบจะเริ่มทำงาน

สำหรับช่องโหว่ในการทำงานของ SNMP นั้นสามารถตรวจสอบได้โดยใช้โปรแกรมชื่อว่า PROTOS ซึ่งควรใช้ตรวจสอบ Access Point ก่อนใช้งาน และตรวจสอบไปยังผู้ผลิตว่ามีการ patch firmware เพื่อปิดช่องโหว่ของ SNMP เรียบร้อยแล้วหรือไม่สำหรับรายละเอียดเกี่ยวกับโปรแกรมดังกล่าวสามารถดูได้จาก

: http://www.ee.oulu.fi/research/ouspg/protos/

: http://www.iss.net/security_center/alerts/advise110.php

4.7 Configuration Interfaces

ช่องโหว่อีกช่องทางหนึ่งที่ทำให้ผู้บุกรุกสามารถเข้าใช้งานระบบเครือข่ายได้คือ ช่องทางในการตั้งค่าของ AP ซึ่งแต่แต่ละยี่ห้อก็มีช่องทางในการเข้าไปตั้งค่าระบบต่างๆ กันไปเช่น

Cisco สามารถเข้าไปตั้งค่าระบบได้โดยใช้ SNMP , Serial , Web และ Telnet

Lucent / Cabletron สามารถเข้าไปตั้งค่าระบบได้โดย SNMP และ Serial

3Com สามารถเข้าไปตั้งค่าระบบได้โดยใช้ SNMP , Serial , Web และ Telnet

ซึ่งใน base station ของ 3com นั้นไม่มีระบบ access control ในการเข้าไปใช้งานเวป เพื่อดูค่าต่างๆ ที่ตั้งค่าไว้ในระบบ ซึ่งผู้บุกรุกสามารถเข้าไปค้นหาค่า SSID ได้โดยง่าย นอกจากนี้ผู้บุกรุกยังสามารถเข้าไปแก้ไขค่าต่างๆ ได้เพราะในการแก้ไขค่าต่างๆ ระบบจะใช้รหัสผ่านเหมือนกับ community word คือ "comcomcom" ซึ่งทำให้ระบบมีความเสี่ยงสูงมากถ้าผู้ดูแลระบบไม่มีการเปลี่ยนแปลงค่าต่างๆ ก่อนการใช้งาน

4.8 Client side security risk

ในการติดต่อสื่อสารระหว่าง client กับ base station นั้นจำเป็นต้องใช้ข้อมูลในการพิสูจน์ตน (authentication) และการเชื่อมต่อ ซึ่งข้อมูลเหล่านั้นจะเก็บอยู่ใน client และ base station ซึ่งถ้าตั้งค่าเกี่ยวกับความปลอดภัยไม่เหมาะสม อาจทำให้ผู้บุกรุกสามารถเข้าถึงข้อมูลเหล่านี้ได้ ยกตัวอย่างเช่น

ใน client ของ cisco จะเก็บข้อมูล SSID อยู่ใน windows registry และเก็บ WEP key ใน firmware ซึ่งเข้าถึงได้ยาก

ใน client ของ Lucent/Cabletron นั้นจะเก็บข้อมูล SSID อยู่ใน windows registry และเข้ารหัส WEP key เก็บไว้ใน windows registry ซึ่งไม่มีการเปิดเผยอัลกอริทึมในการเข้ารหัส

ใน client ของ 3Com จะเก็บ SSID และ WEP key ไว้ใน windows registry โดยไม่มีการเข้ารหัส

4.9 Installation Risk

ในการติดตั้งโดยทั่วๆ ไป จะพยายามให้มีการตั้งค่าอย่างรวดเร็วและทำให้ผู้ใช้งานสามารถใช้งานได้ทันที ซึ่งทำให้ไม่มีการตั้งค่าความปลอดภัยใดๆ ในระบบเลย หรืออาจมีน้อย

5. Jamming

ในเครือข่ายแบบใช้สายนั้น การโจมตีเพื่อปิดบริการหรือ Denial of Service ถือเป็นรูปแบบการโจมตีที่มีผลต่อระบบเครือข่ายมาก โดยการโจมตีรูปแบบนี้จะมีการสร้างข้อมูลปริมาณมหาศาลส่งไปยังเครื่องหรือให้เกิดขึ้นในระบบเครือข่ายเป้าหมาย ทำให้ไม่สามารถใช้งานระบบเครือข่ายนั้นๆ ได้

สำหรับในเครือข่ายแบบไร้สายก็เช่นเดียวกัน มีวิธีการโจมตีที่ทำให้ระบบเครือข่ายนั้นช้าลงได้ โดยการสร้างข้อมูลปริมาณมหาศาลในรูปแบบเดียวกับในเครือข่ายแบบมีสาย หรือจะใช้วิธีการโจมตีเฉพาะซึ่งไม่เห็นในเครือข่ายแบบมีสายคือการสร้างคลื่นความถี่ขึ้นมารบกวนระบบสื่อสาร เพื่อให้ระบบไม่สามารถทำงานได้

GHz Interfering Technology

ในเครือข่ายแบบไร้สาย ผู้โจมตีสามารถสร้างคลื่นความถี่ในย่าน 2.4 GHz เข้ามารบกวนการสื่อสารทำให้ไม่สามารถสื่อสารกันได้ ซึ่งอุปกรณ์ที่สร้างความถี่ในย่าน 2.4 GHz นั้นก็สามารถทำได้ง่ายเนื่องจากมีอุปกรณ์สื่อสารอื่นๆ ที่ใช้ความถี่ในย่านนี้เช่นกัน เช่น โทรศัพท์ไร้สาย , อุปกรณ์ Bluetooth , baby monitor เป็นต้น

นอกจากนี้การนำอุปกรณ์ที่มีการแผ่รังสีในช่วง 2.4 GHz มาอยู่ใกล้ๆ กับอุปกรณ์เครือข่าย ก็สามารถรบกวนการสื่อสารในเครือข่ายไร้สายได้เช่นกัน ยกตัวอย่างเช่นการวาง Access Point ไปวางไว้ใกล้ๆ กับเตาไมโครเวฟ เป็นต้น

6. Client to Client Attacks

เนื่องจากการเชื่อมต่อกันระหว่างอุปกรณ์ไร้สาย สามารถเชื่อมต่อกันได้ในรูปแบบของ adhoc mode ทำให้การโจมตีระหว่างเครื่อง client ทำได้ง่ายกว่าเครือข่ายแบบมีสายมาก เนื่องจากในเครือข่ายแบบมีสายเรายังทราบว่าในเครือข่าย มีใครใช้งานอยู่บ้าง และมีระบบป้องกันเช่น firewall กันอยู่ในระดับหนึ่ง แต่ในเครือข่ายแบบไร้สาย ผู้ใช้งานจะไม่ทราบเลยว่าใครบ้างที่ใช้อุปกรณ์ไร้สายเข้ามาเชื่อมต่อเพื่อโจมตีตนเอง สำหรับการโจมตีก็มีหลายรูปแบบด้วยกัน ยกตัวอย่างเช่น

6.1 Filesharing and other TCP/IP service attacks

ผู้บุกรุกสามารถเจาะระบบผ่านช่องโหว่ของระบบปฏิบัติการ หรือการเปิดให้บริการที่มีช่องโหว่อยู่เช่น เว็บเซิร์ฟเวอร์ หรือการเปิดแชร์ไฟล์ต่างๆ เป็นต้น

6.2 DOS(Denial of Service)

สำหรับเครื่อง Client นั้นสามารถส่ง packet ที่ผิดปรกติเพื่อทำ Denial of Service โจมตีระบบเครือข่าย หรือโจมตีเครื่องที่อยู่ในระบบเครือข่ายเดียวกันได้ หรือผู้บุกรุกอาจตั้งค่า IP Address หรือ MAC Address ในของเครื่องตนเอง ให้ตรงกับเครื่องอื่นๆ เพื่อให้เครื่องๆ นั้นไม่สามารถเชื่อมต่อในระบบเครือข่ายได้เป็นต้น

6.3 Hybrid Threats

ในปัจจุบัน ไวรัสและหนอนต่างๆ มีการพัฒนาตัวเองให้มีความสามารถในการโจมตีที่หลากหลาย ทำให้การกระจายตัวทำได้อย่างรวดเร็วและง่ายดาย ไม่เว้นแม้แต่ในเครือข่ายคอมพิวเตอร์แบบไร้สาย ซึ่งถ้าเครื่องคอมพิวเตอร์เครื่องหนึ่งในเครือข่ายติดไวรัสแล้ว ก็จะกระจายตัวไปในเครือข่ายอย่างรวดเร็ว ซึ่งปัญหาที่จะเกิดขึ้นถัดมาก็คือการนำเครื่อง labtop ที่ติดไวรัส ไปใช้งานในเครือข่ายไร้สายหลายๆ เครือข่าย จะทำให้การกระจายตัวของไวรัสและหนอนทำได้อย่างรวดเร็วและไร้การควบคุม

ปัจจุบันมีการติดตั้งอุปกรณ์ Access Point ในเมืองต่างๆ ให้ประชาชนสามารถใช้งานได้ฟรี (free metro wireless data network) เช่นใน New York , San Francisco , Seattle , British Columbia และ London และเนื่องจากผู้ใช้งานคอมพิวเตอร์มีการใช้งาน wireless network กันมากขึ้น ในบางองค์กรจึงนำกลยุทธเครือข่ายไร้

สายมาจูงใจลูกค้า โดยมีการสร้างพื้นที่เครือข่ายไร้สายที่เรียกว่า Hotspot ขึ้นภายในร้านเพื่อให้ลูกค้าที่เข้ามาในร้าน ใช้เวลาอยู่ในร้านได้นานขึ้น เช่นในร้านกาแฟ Starbucks , ในโรงแรม , ร้านอาหาร หรือในสนามบิน เป็นต้น

โดยการกระทำดังกล่าวก็มีทั้งข้อดีและข้อเสีย โดยข้อดีคือช่วยให้ทุกคนได้เข้าถึงอินเทอร์เน็ตได้ง่ายขึ้น ส่วนข้อเสียก็คือ ทำให้ผู้บุกรุกสามารถใช้งานเครือข่ายดังกล่าวในการโจมตีระบบอื่นๆ โดยที่ไม่สามารถตรวจจับได้ และเป็นเครือข่ายที่เป็นเหมือนกับแหล่งเพาะไวรัสคอมพิวเตอร์ และช่วยให้ไวรัสคอมพิวเตอร์กระจายตัวได้เร็วขึ้นนั่นเอง

การแก้ปัญหา

การจัดการเพื่อลดปัญหาความไม่ปลอดภัยในการใช้งานเครือข่ายไร้สายทำได้โดย

1. Wireless Security Policy and Architecture Design

สำหรับองค์กรต่างๆ ที่มีเครือข่ายไร้สายนั้นควรจะมีการสร้างนโยบายด้านการรักษาความปลอดภัยในเครือข่ายไร้สายเพื่อแจ้งแก่ผู้ใช้งานในองค์กรว่า อนุญาตให้ทำอะไรได้บ้าง และไม่อนุญาตให้ทำอะไรบ้าง และสิ่งที่ควรทำไปควบคู่กับการกำหนดนโยบายก็คือการออกแบบระบบ และการทำงานให้มีความเสี่ยงต่อความไม่ปลอดภัยให้น้อยที่สุดด้วย

วิธีการออกแบบเพื่อรักษาความปลอดภัยวิธีการหนึ่งก็คือการกำหนดขอบเขตและพื้นที่ที่อนุญาตให้ใช้งานระบบเครือข่ายไร้สายได้ โดยการปรับกำลังส่งสัญญาณให้เหมาะสม และการใช้เสาสัญญาณที่สามารถกำหนดทิศทางได้ เป็นต้น

2. Treat BaseStations as Untrusted

ในการออกแบบเครือข่ายนั้นควรกำหนดระดับความน่าเชื่อถือของเครือข่ายแบบไร้สายให้เป็น untrust กับเครือข่ายภายในองค์กร ไม่ควรให้ติดต่อกันได้โดยตรง และในการติดต่อสื่อสารกับอินเทอร์เน็ตนั้น ควรมีการติดตั้ง Wireless DMZ (WDMZ) ซึ่งมี Firewall , VPN , IDS , Vulnerability Assessment และมีการทำการพิสูจน์ตนก่อนที่จะมีการเชื่อมต่อกับอินเทอร์เน็ต ด้วย

3. Base Station Configuration Policy

สำหรับนโยบายเพื่อรักษาความปลอดภัยในเครือข่ายไร้สายนั้นควรกำหนดให้มีมาตรฐานในการตั้งค่าสำหรับ base station ที่ใช้มาตรฐาน 802.11 ทุกเครื่อง เช่นการตั้งค่า SSID , WEP key , การเข้ารหัส , ค่าของ SNMP community word รวมถึงการตั้งค่าบางอย่างเช่น การปิด broadcast ping ซึ่งทำให้โปรแกรมตรวจจับอย่างเช่น NetStumbler ไม่สามารถตรวจจับอุปกรณ์นั้นได้ เป็นต้น

ในการกำหนดนโยบายเพื่อความปลอดภัยควรมีการกำหนดสิ่งต่อไปนี้เป็นพื้นฐานเพื่อความปลอดภัยด้วย

3.1 802.1X Security

ใน Windows XP และในอุปกรณ์หลายๆ ตัวที่สนับสนุนมาตรฐาน 802.1X ซึ่งเป็นมาตรฐานที่ช่วยในการรักษาความปลอดภัยในการใช้งานเครือข่ายไร้สายมากกว่า WEP โดยในมาตรฐาน 802.1X จะมีการเข้ารหัสข้อมูลโดยมีการเปลี่ยนแปลง key เป็นช่วงเวลา ซึ่งถ้าอุปกรณ์ หรือระบบปฏิบัติการสนับสนุนมาตรฐาน 802.1X ก็ควรนำมาใช้งานด้วย

ในการใช้งาน 802.1X มีความปลอดภัยมากกว่า WEP แต่ก็มีการศึกษาว่า 802.1X ก็ยังสามารถโจมตีในลักษณะ Session Hijack และ Man in the middle attack ได้ (http://www.cs.umd.edu/~waa/1x.pdf) ซึ่งในการศึกษานี้แนะนำให้ใช้ VPN ในการทำงานที่ต้องการความปลอดภัยสูงๆ แทน 802.1X

3.2 MAC Address Filtering

ใน Access Point บางรุ่นมีความสามารถในการกรอง MAC Address โดยจะมีรายการของ MAC Address เก็บอยู่ และจะอนุญาตให้ใช้งานเฉพาะอุปกรณ์ที่มี MAC Address ในรายการเท่านั้น การใช้งานลักษณะนี้ไม่เหมาะกับเครือข่ายแบบเปิด ที่อนุญาตให้ใครนำอุปกรณ์มาเชื่อมต่อกับเครือข่ายก็ได้ หรือในบริษัทที่มีการใช้งานเครือข่ายไร้สายมากๆ

ในการรักษาความปลอดภัยแบบนี้ ผู้บุกรุกสามารถดักจับแพ็กเก็ตในเครือข่าย แล้วดักจับ MAC Address ซึ่งรับส่งเป็นแบบ clear text หลังจากนี้จึงใช้โปรแกรมในการปลอมแปลงค่า MAC Address ให้เหมือนกับ MAC Address ที่อนุญาตให้ใช้งานได้ ซึ่งถึงแม้ว่าการรักษาความปลอดภัยแบบนี้จะยังมีกระบวนการเพื่อหลบหลีกได้ แต่ก็ควรจะใช้เพื่อรักษาความปลอดภัยด้วย

3.3 user authentication

มีอุปกรณ์ในการรักษาความปลอดภัยอีกรูปแบบหนึ่งที่ควรนำมาใช้ในเครือข่ายไร้สายนั่นคือ Firewall ที่มีความสามารถในการพิสูจน์ตนในระดับผู้ใช้งาน โดยผู้ใช้งานเครือข่ายไร้สายจะต้องป้อน username และ password ก่อนจึงจะใช้งานระบบเครือข่ายได้

4. Base Station Discovery

สำหรับกรณีของ wardriving ซึ่งจะใช้โปรแกรมชื่อว่า NetStumblers เพื่อตรวจจับหาตำแหน่งที่มี Access Point ในพื้นที่ต่างๆ นั้น เราสามารถใช้โปรแกรมเพื่อป้องกันการค้นหาดังกล่าวได้ โดยโปรแกรมชื่อ FakeAP (http://www.blackalchemy.to/Projects/fakeap/fake-ap.html) สามารถสร้างแพ็กเก็ตของ Access Point ปลอมขึ้นมาปริมาณมาก ซึ่งในสภาวะดังกล่าวการใช้งานโปรแกรม NetStumblers จะไม่สามารถค้นหาตำแหน่งของ Access Point จริงๆ ได้เลย

5. Wireless Client Protection

สำหรับเครื่อง client ที่ใช้ในเครือข่ายไร้สายควรมีการรักษาความปลอดภัยโดยใช้วิธีการดังนี้คือ

firecell ซึ่งเป็น personal firewall ที่มีความสามารถในการป้องกันการเข้าใช้งานเครื่อง client

VPN เป็นกระบวนการเพิ่มความปลอดภัยโดยการเพิ่มการทำงานในการเข้ารหัสและการพิสูจน์ตนในชั้นที่สูงกว่าการทำงานของ 802.11

Intrusion Detection เป็นเครื่องมือในการตรวจสอบและลดความรุนแรงของผู้บุกรุก , ไวรัส , หนอน , โทรจัน และ backdoors

Desktop Scanning เป็นการตรวจหาการตั้งค่าที่ไม่ปลอดภัยในเครื่อง client

บทที่ 12. การ Monitor และ ตรวจสอบระบบ

ในการดูแลระบบให้มีความเสถียรเพียงพอที่จะให้บริการกับผู้ใช้งานได้ตลอดเวลาได้ จำเป็นต้องคอยตรวจสอบดูแลระบบไม่ให้เกิดปัญหาขึ้น โดยการตรวจสอบระบบนั้นผู้ดูแลระบบจะไม่สามารถคอยตรวจตราระบบได้ตลอดเวลา จึงมีการใช้ซอฟต์แวร์ช่วยในการตรวจตราระบบต่างๆ เพื่อให้ผู้ดูแลระบบสามารถทำงานได้ง่ายขึ้น การทำงานของโปรแกรมในกลุ่มนี้จะมีความสามารถในการตรวจสอบรายละเอียดการทำงาน ในส่วนงานที่ผู้ดูแลระบบต้องการเช่น การตรวจสอบจุดบกพร่องภายในระบบ การตรวจจับการทำงานที่ผิดปกติ การตรวจหาช่องโหว่ของระบบ ฯลฯ ซึ่งตัวอย่างโปรแกรมที่ใช้ในงานดังกล่าวได้แก่ Intrusion Detection and Prevention System, Virus Scanner และ Vulnerability Scanner

Intrusion Detection and Prevention System

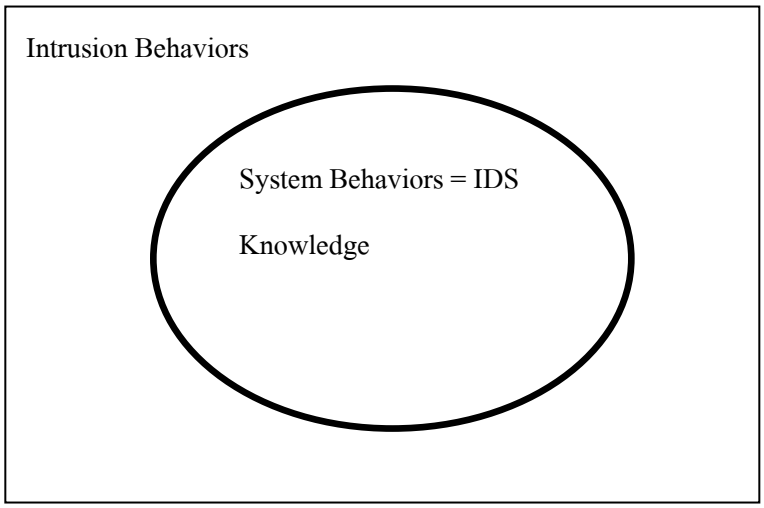
Intrusion Detection System (IDS) คือ ระบบตรวจจับความผิดปกติต่างๆ ที่เกิดขึ้นในระบบ โดยอุดมคติแล้ว IDS จะต้องทราบการทำงานทั้งที่เป็นปกติ และผิดปกติทั้งหมดที่เกิดขึ้นในระบบ แล้วทำการแจ้งเตือนเมื่อเกิดเหตุการณ์ที่ผิดปกติขึ้นในระบบ IPS คือระบบตรวจจับความผิดปกติต่างๆ ที่เกิดขึ้นในระบบและทำการป้องกันการโจมตีหลายๆ รูปแบบได้โดยอัตโนมัติ ซึ่งอาจมองได้ว่า IPS เป็นระบบที่ต่อยอดการทำงานของ IDS สำหรับ IDS และ IPS จะมีการทำงานสามส่วนหลักๆ คือการเก็บข้อมูล การวิเคราะห์ข้อมูล และการตอบสนองต่อการทำงานในรูปแบบต่างๆ

การเก็บข้อมูลใน IDS/IPS นั้นสามารถเก็บข้อมูลได้ทั้งข้อมูลภายในเครื่องเช่นข้อมูลของไฟล์ระบบ (File System), ลอกไฟล์ของระบบ , ลอกไฟล์ของโปรแกรมต่างๆ ที่รันอยู่ในระบบ และข้อมูลที่รับส่งในเครือข่าย ซึ่งการเก็บข้อมูลนี้อาจเก็บอยู่ในลักษณะของข้อมูลดิบ หรือเก็บข้อมูลที่ประมวลผลอยู่ในรูปแบบอื่นๆ เช่น Digital Signature ของไฟล์ระบบ หรือปริมาณข้อมูลที่วิ่งผ่านไปมาในระบบเครือข่ายแยกเป็นเครือข่ายย่อยๆ หรือพอร์ตต่างๆ เป็นต้น ในการวิเคราะห์ข้อมูลจะสามารถวิเคราะห์ข้อมูลได้ใน 2 ลักษณะคือ Anomaly Detection และ Misuse Detection โดยการทำงานของ Anomaly Detection จะทำการเก็บข้อมูลเกี่ยวกับการทำงานต่างๆ ที่เป็นการทำงานปกติไว้แล้วทำการเปรียบเทียบกับเหตุการณ์ที่เกิดขึ้นกับข้อมูลที่มีอยู่ ถ้าเปรียบเทียบแล้วมีความแตกต่างกันจะแปลว่าเกิดการทำงานที่ผิดปกติขึ้นจึงดำเนินการตอบสนองในรูปแบบ

ต่างๆ สำหรับ Misuse Detection จะเป็นการเก็บข้อมูลการทำงานที่ผิดปกติไว้ หากเหตุการณ์ใดตรงกับข้อมูลที่เก็บไว้จะหมายความว่าเกิดเหตุการณ์ผิดปกติขึ้น ในการดำเนินการตอบสนองต่อความผิดปกติต่างๆ นั้น ใน IDS จะทำการตอบสนองโดยการเก็บข้อมูล และแจ้งเตือนต่อผู้ดูแลระบบ ส่วน IPS จะดำเนินการตอบสนองมากกว่า IDS คือการป้องกันความเสียหายที่เกิดขึ้นเช่นการตัดการเชื่อมต่อที่มีปัญหานั้นๆ ทิ้งไป เป็นต้น

ทฤษฎีที่เกี่ยวข้อง

เมื่อพิจารณาถึงหลักการทำงานของ IDS แล้วในทางอุดมคติระบบ IDS ต้องทราบถึงการทำงานต่างๆ ของระบบทั้งหมด โดยขอบเขตการทำงานของระบบ และ Knowledge ของ IDS จะมีขอบเขตเดียวกัน

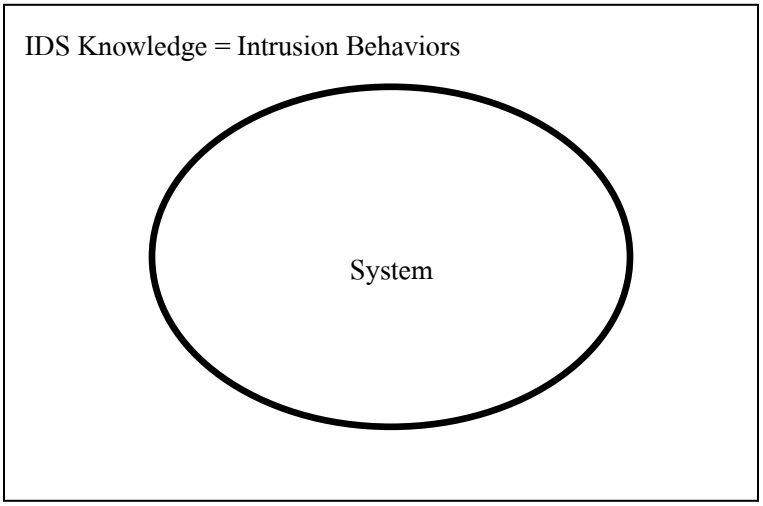


รูปที่ 63 IDS ในอุดมคติ

การสร้างขอบเขต Knowledge ของ IDS เกิดขึ้นได้ใน 2 ลักษณะคือ

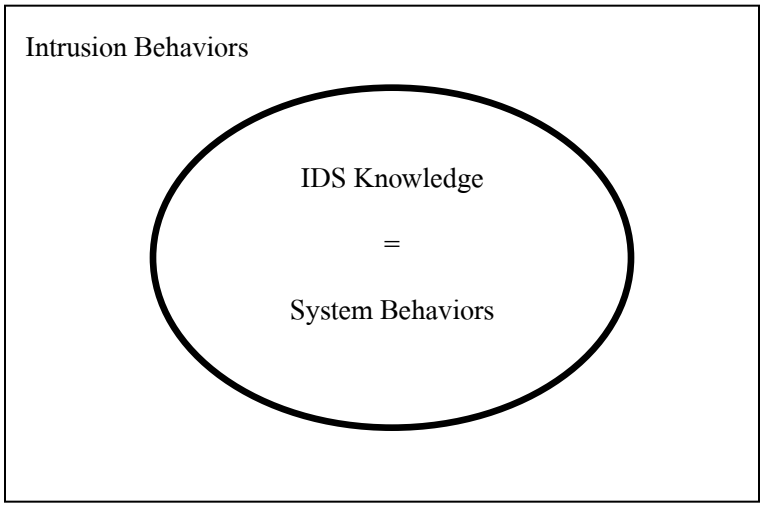
- Misused Detection
- Anomaly Detection

Misused Detection เป็นกระบวนการที่ IDS จะเก็บข้อมูลการทำงานที่ผิดปกติไว้ เมื่อมีการทำงานในระบบที่ตรงกับ Knowledge จะทำการ แจ้งเตือนให้ผู้ดูแลระบบทราบว่าเกิดการบุกรุกขึ้น



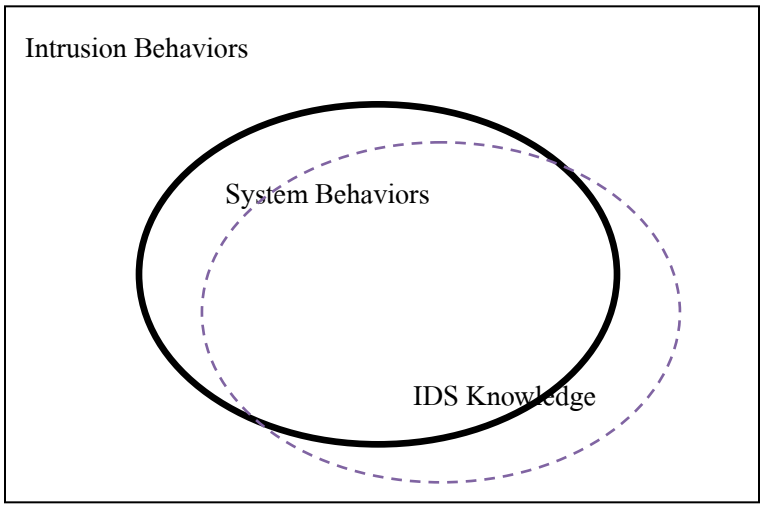
รูปที่ 64 Misuse Detection

Anomaly Detection เป็นกระบวนการที่ IDS จะเก็บข้อมูลการทำงานที่เป็นปกติไว้ เมื่อมีการทำงานในระบบที่แตกต่างจาก Knowledge จะทำการแจ้งเตือนให้ผู้ดูแลระบบทราบว่าเกิดการบุกรุกขึ้น



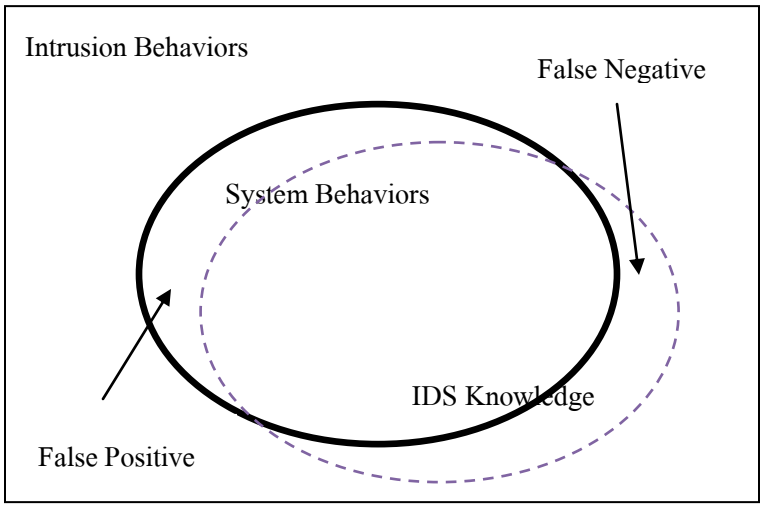
รูปที่ 65 Anomaly Detection

ถึงแม้ว่าการดำเนินการสร้างขอบเขตของ IDS ในการตรวจสอบระบบ ทั้งสองแนวทางจะมีกรรมวิธีที่แน่นอน แต่ในโลกของความเป็นจริงเราไม่สามารถทำให้ Knowledge ของ IDS และ System Behavior เป็นข้อมูลชุดเดียวกันได้เนื่องจากที่มาของ IDS Knowledge และความซับซ้อนในการทำงานของ IDS เช่น ในกรณีของ Misuse Detection อาจมี Knowledge ของการทำงานที่ผิดปกติไม่ครบถ้วน หรือมีความผิดพลาดทำให้ Knowledge ของ IDS มองว่าการทำงานของระบบบางอย่างเป็นการโจมตี หรือในกรณีของ Anomaly Detection การเก็บข้อมูล IDS Knowledge อาจมีการผิดพลาดเช่น เก็บข้อมูลการทำงานที่ผิดปกติ เป็นการทำงานที่เป็นปกติ หรือไม่มีการเก็บข้อมูลการทำงานที่เป็นปกติของระบบใน IDS Knowledge ไม่ว่าจะเป็นโมเดลในการสร้างขอบเขตของ IDS แบบใดก็ตาม ความผิดพลาดดังกล่าวจะทำให้เกิดความเหลื่อมล้ำของขอบเขตระหว่าง IDS กับระบบ



รูปที่ 66 ความสัมพันธ์ระหว่าง IDS Knowledge กับระบบ

จากความเหลื่อมล้ำระหว่าง IDS กับระบบทำให้เกิดความผิดพลาดในการตรวจสอบเรียกว่า “False Alarm” False Alarm เป็นความผิดพลาดในการแจ้งเตือนของ IDS เมื่อ IDS ไม่มี Knowledge ครอบคลุมระบบทั้งหมด จึงเกิดกรณี ความผิดปกติขึ้น 2 กรณีคือ False Positive และ False Negative โดย False Positive คือการที่ IDS ทำการแจ้งเตือนว่าเกิดการบุกรุกขึ้น แต่ในระบบไม่ถูกบุกรุก และ False Negative คือการที่ IDS ไม่ทำการแจ้งเตือนว่าเกิดการบุกรุกขึ้นแต่ในระบบถูกบุกรุก



รูปที่ 67 False Alarm

ในการตรวจจับความผิดปกติต่างๆ ในระบบจะสามารถตรวจสอบได้หลายรูปแบบ ขึ้นอยู่กับ แหล่งที่มาของข้อมูลที่ใช้ในการวิเคราะห์ , ระยะเวลาในการทำงาน, กระบวนการที่ใช้ในการตรวจจับ และผลลัพธ์ในการทำงาน จากปัจจัยที่เกี่ยวข้องต่างๆ ทำให้เกิดโปรแกรม IDS ที่หลากหลายรูปแบบในท้องตลาด ในการวิเคราะห์ถึงความสามารถของโปรแกรม IDS ต่างๆ นั้น เราสามารถวิเคราะห์ตามปัจจัยต่างๆ ที่ได้กล่าวมาแล้ว

- สำหรับที่มาของข้อมูลที่ใช้ในการวิเคราะห์ของ IDS นั้น สามารถใช้ข้อมูลต่างๆ ที่มีอยู่หรือเกิดขึ้นในระบบ นำมาใช้ในการตรวจจับผู้บุกรุกได้ โดยข้อมูลที่เป็นไปได้ ได้แก่ข้อมูลต่างๆที่มีอยู่ภายในระบบ , Log File ของการทำงาน และการใช้ทรัพยากรต่างๆ , ข้อมูลที่วิ่งผ่านไปมาในเครือข่าย , File System , System Call หรืออื่นๆ ซึ่งมีความหลากหลายมาก
- ระยะเวลาในการทำงานของ IDS แบ่งออกได้เป็น 2 รูปแบบคือ แบบ Realtime และแบบ Batch โดยแบบ Realtime คือระบบ IDS ที่ทำงานอยู่ตลอดเวลา และส่งผลลัพธ์ในการทำงานทันที หลังจากพบ

ความผิดปกติ และแบบ Batch คือระบบ IDS ที่ทำงานเป็นช่วงเวลาเช่น ทุกๆ เที่ยงคืน ทุกวันเสาร์ หรือช่วงเวลาใดๆ ที่ผู้ดูแลระบบกำหนด ซึ่งการทำงานของ IDS จะเป็นแบบ Realtime หรือ Batch นั้นขึ้นอยู่กับการออกแบบ และวัตถุประสงค์ของการตรวจจับ แต่โดยทั่วไปแล้ว มีปัจจัย 2 ข้อที่ทำให้ IDS ทำงานเป็นแบบ Realtime หรือ Batch นั่นคือความเร็วในการตอบสนอง และ ทรัพยากรที่ต้องใช้ในการวิเคราะห์ ในบางสถานการณ์เช่นการโจมตีทางเครือข่าย ผู้ดูแลระบบจำเป็นต้องทราบและตอบสนองทันทีเมื่อเกิดปัญหาขึ้น IDS ที่ตรวจจับการโจมตีทางเครือข่ายจะต้องสามารถทำงานแบบ Realtime ส่วนการตรวจจับไวรัสในเครื่องซึ่งไม่จำเป็นต้องมีการตรวจจับอยู่ตลอดเวลาจะทำงานแบบ Batch เป็นต้น

- กระบวนการที่ใช้ในการตรวจจับแบ่งออกเป็น 2 รูปแบบคือ Misuse Detection และ Anomaly Detection ซึ่ง Misuse Detection (หรือ Signature-Based) เป็นการตรวจจับความผิดปกติต่างๆ ในระบบโดยมี Signature ของความผิดปกติต่างๆ ในระบบและจะแจ้งเตือนต่อผู้ดูแลระบบเมื่อมีข้อมูลใดๆ Match กับ Signature ยกตัวอย่างเช่น Network Intrusion Detection และ Virus Scan เป็นต้น สำหรับ Anomaly Detection เป็นการตรวจจับความผิดปกติของระบบโดยจะมีการเก็บ Profile การทำงานที่เป็นปกติไว้แล้วทำการเปรียบเทียบข้อมูลที่รับเข้ามากับ Profile หากมีข้อมูลใดแตกต่างจาก Profile จะถือว่ามีการบุกรุกเกิดขึ้น
- ผลลัพธ์ในการทำงานของ IDS ส่วนใหญ่จะเป็นการแจ้งเตือนและเก็บข้อมูลการแจ้งเตือนในรูปแบบต่างๆ เช่น การแสดง Alert Message ในหน้าจอ , การส่งอีเมล์แจ้งเตือน , การส่ง SMS แจ้งเตือน , การส่งเสียงแจ้งเตือน, ไฟกระพริบ หรืออื่นๆ

ยกตัวอย่างระบบตรวจจับผู้บุกรุกต่างๆ

1. ระบบตรวจจับผู้บุกรุกทางเครือข่าย (Network Intrusion Detection System : NIDS) เป็นระบบตรวจจับแพ็กเก็จที่วิ่งอยู่ในเครือข่ายพยายามตรวจสอบว่ามีผู้บุกรุกพยายามบุกรุกเข้าสู่ระบบหรือไม่ ตัวอย่างของระบบนี้คือ ระบบที่ตรวจสอบว่ามีแพ็กเกจของการเชื่อมต่อแบบทีซีพี/ไอพี (TCP/IP) ชื่อว่า SYN ส่งเข้ามายังระบบเป็นจำนวนมากอย่างผิดปกติในเครื่องเป้าหมาย ซึ่งการกระทำแบบนี้สามารถตรวจสอบว่ามีผู้บุกรุกพยายามสแกนพอร์ตทีซีพี (TCP port) ของเครื่องอยู่หรือไม่ ซึ่งระบบตรวจจับ ผู้บุกรุกทางเน็ตเวิร์กสามารถทำงานที่เครื่องเป้าหมาย หรือเครื่องที่ทำหน้าที่เฉพาะในการเฝ้าดูเหตุการณ์ไม่ปกติในเครือข่ายได้ ดังนั้นระบบ

ตรวจจับผู้บุกรุกทางเครือข่ายสามารถตรวจสอบเครื่องใด ๆ ก็ได้ในเครือข่าย หรือโปรแกรมที่ใช้ตรวจสอบรูปแบบของข้อมูลที่ผ่านไปมาในเครือข่ายว่าเหมือนกับรูปแบบของ ไวรัส หรือไม่ แล้วทำการแจ้งเตือนให้ผู้ดูแลระบบทราบเช่นโปรแกรม SNORT

2. ระบบตรวจสอบความถูกต้องของข้อมูลในระบบ (System Integrity Verifiers : SIV) ตรวจสอบความถูกต้องของข้อมูลในระบบ เพื่อค้นหาว่ามีผู้บุกรุกพยายามเปลี่ยนแปลงข้อมูลของไฟล์ระบบ หรือส่วนประกอบอื่นๆ (component) เช่น ไฟล์ที่เป็นรีจิสตรี ของวินโดว์ส หรือครอน (Cron) ในระบบปฏิบัติการยูนิกซ์หรือไม่ และสามารถตรวจสอบการเปลี่ยนแปลงในไฟล์ระบบเช่นโปรแกรม Tripwire เป็นต้น

3. ระบบมอนิเตอร์ไฟล์ล็อก (Log File Monitor : LFM) ตรวจสอบไฟล์ล็อกที่สร้างขึ้นมาโดยเซอร์วิสในเน็ตเวิร์ก ทำงานคล้ายกับระบบตรวจจับผู้บุกรุกทางเน็ตเวิร์ก ระบบนี้เฝ้าดูรูปแบบของไฟล์ล็อกที่เกิดขึ้นว่าตรงกับพฤติกรรมการบุกรุกที่เคยเกิดขึ้นแล้วหรือไม่ ถ้าตรงก็สามารถตั้งข้อสงสัยได้ว่าเข้าข่ายการบุกรุกระบบ ตัวอย่างของระบบตรวจจับผู้บุกรุกแบบนี้ เช่นโปรแกรม SWATCH โดยสร้างเซอร์วิสปลอมขึ้นมาหลอกว่าเป็นช่องโหว่ของระบบ ทำหน้าที่เป็นกับดักล่อให้ผู้บุกรุกเข้ามาติดกับ

ดังนั้น IDS/IPS จึงมีความสามารถในการตรวจจับแตกต่างกันไปตามการเก็บข้อมูล การวิเคราะห์ข้อมูลและการแสดงผล ยกตัวอย่างโปรแกรม SNORT ซึ่งเป็นโปรแกรมที่ใช้ในการตรวจจับความผิดปกติที่เกิดขึ้นในเครือข่าย ซึ่งการทำงานจะทำงานเป็น IDS เก็บข้อมูลจากข้อมูลที่วิ่งผ่านไปมาในเครือข่าย ทำงานแบบ Misuse Detectoin โดยจะเปรียบเทียบข้อมูลที่ดักจับได้กับกฎต่างๆของ SNORT ถ้าเหมือนกันโปรแกรม SNORT จะตอบสนองโดยการเก็บข้อมูลสิ่งที่เกิดขึ้นแล้วแจ้งเตือนให้กับผู้ดูแลระบบ

ตัวอย่างคุณสมบัติของอุปกรณ์ Network Intrusion Detection System

- การทำงานแบบ Inline Packet Flow Inspection
- การประมวลผลของระบบประมวลผลแบบ Parallel processing
- มี Interface แบบ UTP ความเร็ว 10/100/1000 Mbps
- สามารถป้องกันการบุกรุกระบบเครือข่ายแยกเป็น Segment ต่างๆ
- มีการกำหนด IPS Throughput เช่นไม่น้อยกว่า 200 Mbps
- กำหนดค่า Latency Time ที่ใช้ในการประมวลผลของอุปกรณ์เช่นไม่เกิน 1 ms

- กำหนดค่าการเชื่อมต่อพร้อมกัน (Concurrent Connection) เช่นไม่น้อยกว่า 2,000,000 การเชื่อมต่อ
- กำหนดค่าความเร็วในการเชื่อมต่อใหม่เช่นความเร็วไม่ต่ำกว่า 250,000 การเชื่อมต่อต่อวินาที
- กำหนดค่าความสามารถในการสแกนข้อมูลซึ่งอาจมี Spyware, Trojan และ Virus ในส่วนของ FTP และ HTTP (เช่นActiveX, Java Applet, Malicious Scripts, Phishing, Backdoor, Cookies หรือ Key word check)
- กำหนดความสามารถในการสแกนข้อมูลซึ่งอาจมี Spyware, Trojan และ Virus ในส่วนของ SMTP, IMAP หรือ POP3
- กำหนดความสามารถป้องกันการโจมตีจาก Worm, Virus, Trojan, Spyware, DoS
- ความสามารถในการ Filter ได้แบบ Block, Permit, Alert, Log, Quarantine และ Rate Limit
- ความสามารถในการทำ Traffic classification และ Rate Shape ได้ เช่น Peer-to-Peer/Instant Messaging applications ได้
- ความสามารถในการป้องกันการโจมตีแบบ Anti-Phishing และ VoIP Security
- สามารถทำ Fail Open (Bypass Traffic) ได้ในกรณีที่อุปกรณ์เกิด Software Error

Virus Scan

โปรแกรมสแกนไวรัสก็ถือว่าเป็นระบบตรวจจับผู้บุกรุกเช่นเดียวกัน ไม่ว่าจะเป็นการสแกนไฟล์ระบบในเครื่องคอมพิวเตอร์ หรือใน Mailbox แต่วัตถุประสงค์ไม่ได้ใช้ในการตรวจจับ Hacker แต่เป็นการตรวจจับโปรแกรมหรือการทำงานที่ผิดปกติต่างๆ ในระบบ หลักการทำงานจะคล้ายกับ Host Based Intrusion Detection System สภาพแวดล้อมในการตรวจจับคือไฟล์ต่างๆ ในระบบ รวมถึง Registry โปรแกรมดังกล่าวมีการทำงานแบบ Batch หรือ Schedule มี Knowledge คือ Virus Signature การทำงานเป็นแบบ Misuse Detection เมื่อการทำงานของโปรแกรมสแกนไวรัสเป็นแบบ IDS ดังนั้นปัญหา False Alarm จึงเกิดได้เสมอ

การตรวจสอบระบบว่าระบบมีความปลอดภัยหรือไม่เป็นหน้าที่หลักของผู้ดูแลระบบเพื่อให้ระบบสามารถให้บริการกับผู้ใช้งานตลอดเวลา ซึ่งการตรวจสอบระบบโดยผู้ดูแลระบบนั้น อาจทำได้ไม่เต็มที่เนื่องจากความซับซ้อนของระบบและขนาดของระบบ ซึ่งระบบที่ให้บริการผู้ใช้งานโดยทั่วไปมักมีขนาดใหญ่

และมีความซับซ้อนสูงทำให้ผู้ดูแลระบบไม่สามารถตรวจสอบระบบได้ด้วยตนเอง จึงมีการนำเอาซอฟต์แวร์ที่ทำหน้าที่เกี่ยวกับการตรวจสอบระบบมาใช้โดยซอฟต์แวร์ที่ทำหน้าที่ดังกล่าวจะเรียกว่า “Vulnerability Scanner”

Vulnerability Scanner

เป็นเครื่องมือที่ผู้ดูแลระบบใช้ในการตรวจสอบระบบเมื่อแบ่งแยกตามรูปแบบการทำงานสามารถแบ่งออกได้เป็น 2 ชนิดคือ

1. Network-Based Scanner
2. Host-Based Scanner

Network Based Scanner เป็น Scanner ที่สามารถตรวจสอบความบกพร่องในระบบคอมพิวเตอร์โดยสามารถตรวจสอบผ่านเครือข่ายได้ ทำให้ผู้ดูแลระบบสามารถตรวจสอบเครื่องคอมพิวเตอร์ภายในเครือข่ายได้อย่างรวดเร็ว แต่มีข้อเสียเล็กน้อยคือข้อมูลที่ได้จากการตรวจสอบจะไม่ละเอียดมาก เนื่องจากเป็นการส่งข้อมูลทดสอบไปยังเครื่องคอมพิวเตอร์ที่ต้องการทดสอบผ่านระบบเครือข่าย แล้วเปรียบเทียบผลลัพธ์ของการทำงานกับฐานข้อมูลช่องโหว่ที่มีอยู่ในโปรแกรม ทำให้ไม่สามารถตรวจจับถึงระดับไฟล์ใดที่มีปัญหา หรือการตั้งค่าระบบค่าใดที่มีปัญหา ตัวอย่างซอฟต์แวร์ที่เป็น Network Based Scanner ได้แก่ Nessus และ Retina เป็นต้น

Host-Based Scanner เป็น Scanner ที่สามารถตรวจสอบความบกพร่องภายในระบบคอมพิวเตอร์ได้โดยละเอียด เนื่องจากผู้ดูแลระบบจะต้องนำโปรแกรม Scanner ไปติดตั้งและสแกนในเครื่องคอมพิวเตอร์นั้นๆ ทำให้ทราบรายละเอียดของซอฟต์แวร์ต่างๆ ในระบบ การตั้งค่าระบบ registry และค่าอื่นๆ จึงทำให้ Host-Based Scanner สามารถตรวจพบความผิดปกติได้ทั้งหมด แต่ข้อเสียของ Host-Based Scanner คือการตรวจสอบระบบในเครือข่ายขนาดใหญ่จะทำได้ยาก ดังนั้นจึงมักนำ Host-Based Scanner มาตรวจสอบการตั้งค่าของเครื่องเซิร์ฟเวอร์เท่านั้น

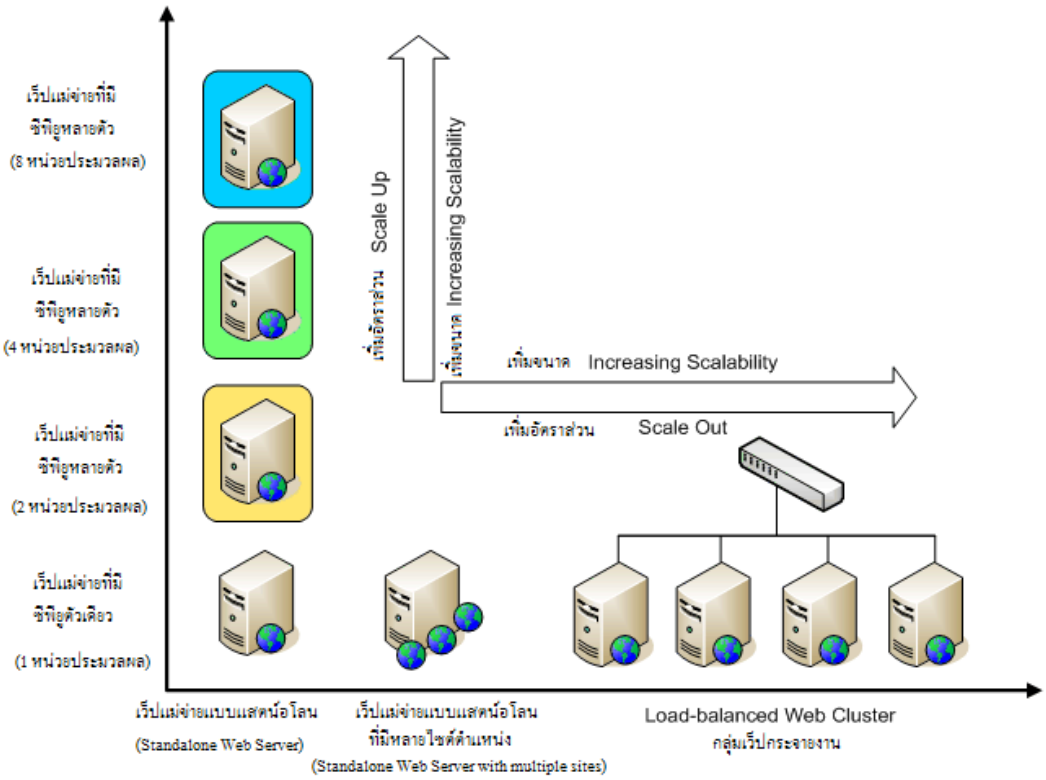
บทที่ 13. การออกแบบระบบให้พร้อมใช้งานสูง (Hi-Availability)

ในการรักษาความปลอดภัยระบบสารสนเทศนั้น ปัญหาความปลอดภัยที่เกิดขึ้นนอกจากจะเกิดจาก Hacker แล้ว ก็ยังมีสาเหตุอื่นๆ ที่ทำให้ระบบไม่สามารถให้บริการได้อย่างเหมาะสมเช่นอุบัติเหตุ ปริมาณการใช้งานระบบที่มีการใช้งานสูงขึ้น การทำให้ระบบสามารถรองรับความเปลี่ยนแปลง หรืออุบัติเหตุต่างๆ ที่อาจเกิดขึ้นนั้น ผู้ดูแลระบบต้องออกแบบระบบให้รองรับการขยายตัวในอนาคต รวมถึงมีการออกแบบระบบให้สามารถทำงานได้อย่างต่อเนื่องถึงแม้ว่ามีอุบัติเหตุต่างๆ ที่ทำให้อุปกรณ์บางตัวหยุดทำงานเกิดขึ้นก็ตาม ในการออกแบบระบบให้มีความสามารถในการทำงานอย่างต่อเนื่องภายใต้สถานการณ์ต่างๆ นั้น ผู้ดูแลระบบต้องมีความเข้าใจในหลักการต่างๆ ต่อไปนี้คือ Scalability และ Hi-Availability

ความสามารถในการขยายขนาด (Scalability)

โดยธรรมชาติของระบบสารสนเทศ จะมีแนวโน้มความต้องการในการใช้งานระบบมากขึ้นเรื่อยๆ ไม่ว่าจะเป็นผู้ใช้งานระบบที่จะมีจำนวนมากขึ้น แอปพลิเคชั่นต่างๆ ที่จะมีปริมาณและความหลากหลายมากขึ้น อีกทั้งแอปพลิเคชั่นต่างๆ จะมีการใช้งานข้อมูลและระบบเครือข่ายสูงมากขึ้น จากลักษณะดังกล่าวจะทำให้ผู้ดูแลระบบจำเป็นต้องมีการวางแผนและออกแบบระบบให้รองรับความต้องการการใช้งานที่ขยายตัวขึ้นเรื่อยๆ อย่างเหมาะสม

ความสามารถในการขยายขนาด **(Scalability)** เป็นความสามารถหนึ่งของระบบสารสนเทศที่จำเป็นต้องมีอย่างยิ่ง ซึ่งการขยายตัวของระบบนั้นสามารถทำได้สองรูปแบบคือการขยายตัวในแนวราบและการขยายตัวในแนวดิ่ง โดยการขยายตัวในแนวดิ่ง คือการเพิ่มจำนวนทรัพยากร เช่น หน่วยประมวลผลคอมพิวเตอร์หรือหน่วยความจำ ซึ่งเป็นวิธีที่ใช้ทั่วไปสำหรับระบบฐานข้อมูลและเครือข่ายต่างๆ ส่วนการขยายแบบแนวราบคือการเพิ่มเครื่องคอมพิวเตอร์ในเครือข่าย เช่น เครื่องคอมพิวเตอร์แม่ข่ายเป็นต้น ซึ่งวิธีนี้จะใช้สำหรับเครื่องคอมพิวเตอร์ที่ให้บริการด้านเว็บไซต์ และเครื่องคอมพิวเตอร์ที่ให้บริการแอพพลิเคชั่นต่างๆ เพื่อรองรับกับการใช้บริการที่เพิ่มขึ้นของผู้ใช้งานโดยเฉพาะ



รูปที่ 68 การขยายตัวในแนวดิ่งและแนวราบ (Vertical and Horizontal Scalability)

ความพร้อมในการใช้งานสูง (High Availability)

ในกรณีของการขยายตัวของผู้ใช้งานในระบบ ผู้ดูแลระบบจะสามารถแก้ไขได้โดยการออกแบบระบบให้มีความสามารถในการขยายตัว แต่สำหรับปัญหาอุปกรณ์ชำรุด โปรแกรมหยุดทำงาน หรือปัญหาอื่นๆ ที่ทำให้ระบบสารสนเทศไม่สามารถให้บริการได้ ซึ่งที่สำคัญปัญหาเหล่านั้นเกิดขึ้นโดยอุบัติเหตุ ผู้ดูแลระบบจะแก้ปัญหาเหล่านี้อย่างไร

โดยตัวปัญหาอันเกิดจากอุบัติเหตุนั้น คงไม่มีใครสามารถห้ามไม่ให้เกิดขึ้นได้ ในระบบที่มีมูลค่าไม่สูงมากนัก การเกิดปัญหาดังกล่าวก็ยังพอยอมรับกันได้ แต่สำหรับระบบที่จำเป็นต้องให้บริการอย่างต่อเนื่อง และตลอดระยะเวลาการให้บริการต้องไม่มีความผิดพลาดเกิดขึ้นจนทำให้ระบบหยุดให้บริการเช่น ตลาดหุ้น ธนาคาร ผู้ดูแลระบบจำเป็นต้องออกแบบระบบให้ระบบมีความพร้อมใช้ในการใช้งานสูง (Hi-Availability)

การมีความพร้อมในการใช้งานสูงคือความพร้อมในการใช้ทรัพยากรในระบบคอมพิวเตอร์และเครือข่าย ทำให้ระบบสามารถทำงานได้ตลอดเวลา ไม่ติดขัดหรือเกิดการหยุดชะงักในการให้บริการ ถึงแม้ว่าอาจมีความบกพร่องในการปฏิบัติงานส่งผลกระทบต่อความพร้อมในการให้บริการ และทำให้ระบบล่มเป็นช่วงๆ ไม่สามารถดำเนินการบริการตามปกติได้ ในการพิจารณาความพร้อมในการใช้งานถึงแม้ว่าปริมาณผู้ใช้บริการไม่ใช่ปัจจัยหลักที่จะมีผลกระทบต่อความพร้อมใช้ของระบบแต่เป็นปัจจัยหนึ่งที่ควรให้ความสำคัญเช่นกัน

การทำให้ระบบบริการอิเล็กทรอนิกส์มีความพร้อมในการใช้งานสูงสามารถทำได้โดยการตรวจสอบและทดสอบระบบ พร้อมทั้งส่วนประกอบต่างๆ ทั้งหมดในโครงสร้างพื้นฐานที่ให้บริการเช่น อุปกรณ์ฮาร์ดแวร์ , ซอฟต์แวร์ และระบบเครือข่าย โดยจะทดสอบความสามารถในการทำงาน ความสามารถในการฟื้นกลับภายหลังจากระบบล้มเหลวได้มากน้อยเพียงใด หรือต้องไม่มีอุปกรณ์ใดที่จะทำให้ระบบโดยรวมมีปัญหาเมื่ออุปกรณ์นั้นเพียงตัวเดียวไม่สามารถทำงานได้เป็นปกติ และต้องทดสอบการให้บริการกับผู้ใช้งาน โดยผู้ใช้งานต้องเข้าถึงบริการต่างๆได้ตามปกติถึงแม้ว่าอุปกรณ์บางตัวในระบบมีปัญหาก็ตาม

วิธีที่จะทำให้ระบบบริการอิเล็กทรอนิกส์มีความพร้อมในการใช้งานสูง (High Availability) จะคล้ายกับวิธีการขยายขนาดของระบบ (Scalability) ได้แก่การติดตั้งอุปกรณ์เพิ่มเติม โดยการติดตั้งอุปกรณ์เพิ่มเติมนี้จะกำหนดให้เครื่องคอมพิวเตอร์แม่ข่ายต่างๆ ทำงานในลักษณะเป็นกลุ่ม (Cluster) เพื่อให้ความล้มเหลวที่อุปกรณ์ฮาร์ดแวร์หรือซอฟต์แวร์ในเครื่องคอมพิวเตอร์แม่ข่ายหนึ่งไม่มีผลกระทบต่อการปฏิบัติงานของทั้งหมดได้ นอกจากนี้เครือข่ายจะต้องสามารถทำการปรับระบบให้อุปกรณ์เครือข่ายรองรับการเข้าทำงานแทนที่กันได้ ทำให้เครื่องคอมพิวเตอร์ในเครือข่ายสามารถติดต่อกันผ่านช่องทางหลักและช่องทางสำรองได้

การปรับปรุงระบบที่ได้กล่าวมานั้น อาจไม่เพียงพอหากมีการล้มเหลวของอุปกรณ์ภายในทั้งหมดพร้อมๆ กันอาทิเช่น เครื่องคอมพิวเตอร์แม่ข่ายในกลุ่มอาจเกิดปัญหาทีละตัวตลอดเวลาหรืออย่างต่อเนื่อง ดังนั้นผู้ดูแลรับผิดชอบระบบจะต้องตรวจสอบสภาพของเครื่องคอมพิวเตอร์แม่ข่ายเป็นประจำและทำการเปลี่ยนอุปกรณ์ที่ไม่อยู่ในสภาพที่ทำงานได้ออกทันที ทั้งนี้เพื่อลดความเสี่ยงในการเกิดความล้มเหลวของอุปกรณ์จำนวนมากในช่วงเวลาเดียวกัน และถึงแม้ว่าจะมีการตรวจสอบและดูแลอุปกรณ์อย่างสม่ำเสมอ ก็ยังมีโอกาสที่จะเกิดความผิดปกติกับอุปกรณ์หลายๆตัวในเวลาเดียวกัน เพราะเหตุการณ์ดังกล่าวสามารถเกิดขึ้นได้ในช่วงที่เกิดเหตุภัยพิบัติต่างๆ เช่น แผ่นดินไหว น้ำท่วม หรือไฟไหม้ สำหรับวิธีรับมือกับเหตุการณ์ผิดปกติเหล่านี้ คือการจัดตั้งศูนย์กู้คืนข้อมูลจากภัยพิบัติ (Disaster Recovery Center) ซึ่งตั้งอยู่ในพื้นที่อื่น ตามหลักการการกระจายความเสี่ยง โดยศูนย์ข้อมูลของหน่วยงาน ควรได้รับการเชื่อมต่อเข้าสู่เครือข่ายและใช้งานได้ทั้งสองระบบ นอกจากนี้ เพื่อให้ศูนย์กู้คืนข้อมูลจากภัยพิบัติสามารถเข้าปฏิบัติงานแทนระบบหลักได้ทันทีหากมีเหตุการณ์เกิดขึ้นโดยผู้ใช้งานระบบไม่รู้สึกถึงปัญหา ผลกระทบหรือการเปลี่ยนแปลงใดๆ ที่เกิดขึ้นควรมีการสำรองข้อมูลและอัพเกรดแอพพลิเคชั่นของทั้งสองศูนย์ข้อมูลเป็นประจำ

Load Balancing

Load Balancing เป็นกระบวนการทำงานหนึ่งที่ทำให้ระบบสารสนเทศสามารถขยายตัวในแนวราบได้ ในการทำงานดังกล่าว จำเป็นต้องใช้งานอุปกรณ์หรือซอฟต์แวร์ Loadbalancer เพื่อให้สามารถกระจายภาระงานให้กับอุปกรณ์ที่เพิ่มเติมเข้ามาในระบบ และทำงานสอดประสานกันได้เป็นอย่างดี โดยทั่วไปอุปกรณ์ Load Balancer จะเป็นอุปกรณ์ที่ประสานงานให้กับโพรโตคอลต่างๆ โดยเฉพาะโพรโตคอล HTTP จึงอาจเรียกอุปกรณ์ชนิดนี้เป็น Layer 4 Switch หรือ Layer 4+ Switch ในการทำงานเพื่อกระจายการร้องขอบริการไปยังเซิร์ฟเวอร์เครื่องต่างๆ ที่ให้บริการ

สำหรับผลิตภัณฑ์ในท้องตลาดที่ทำงานเป็น Loadbalancer ได้แก่

1. ซอฟแวร์เช่น StoneBeat , Resonate และ Rainfinity
2. Appliances ซึ่งเป็นอุปกรณ์ที่ออกแบบเพื่อทำงาน Load Balancing โดยเฉพาะเช่น F5 และ Radware
3. Switch Based ซึ่งเป็น Switch ที่เพิ่มความสามารถ Load Balancing เช่น Cisco , Nortel , Foundry

สำหรับการทำงานของอุปกรณ์หรือซอฟต์แวร์ Load Balancer จะมีการทำงานพื้นฐานดังนี้คือ

1. กลุ่มของเซิร์ฟเวอร์ (Server Farm) จะถูกมองว่าเป็นเซิร์ฟเวอร์เพียงตัวเดียว และใช้งาน IP Address เดียว
2. สามารถบริหารจัดการโปรแกรมที่ให้บริการต่างๆ ในเซิร์ฟเวอร์ได้อย่างอิสระ สามารถติดตั้งโปรแกรมที่ให้บริการในเซิร์ฟเวอร์ต่างๆ ได้มากกว่า 1 ในแต่ละเครื่อง ตามความเหมาะสม แล้วใช้ Load Balancer กระจายงานไปยังเครื่องต่างๆ โดยอัตโนมัติ
3. มีกระบวนการตรวจสอบว่าบริการต่างๆ ยังทำงานอยู่หรือไม่ (Service/Application Health Check)
4. สามารถใช้งานกับเซิร์ฟเวอร์ที่หลากหลาย
5. สามารถกระจายงานให้กับเซิร์ฟเวอร์ต่างๆ ได้อย่างเหมาะสม เพื่อให้มีการใช้งานระบบต่างๆ ได้อย่างมีประสิทธิภาพ

อัลกอริทึมในการกระจายภาระงานตัวอย่างเช่น

1. Round Robin เป็นกระบวนการกระจายภาระงานแบบวนรอบ คล้ายการแจกไพ่ หรือเข็มนาฬิกาที่ชี้ตัวเลข 1-12 แล้วกลับไปชี้ตัวเลข 1 อีกครั้ง ในการทำงานแบบ Round Robin หากมีเซิร์ฟเวอร์ 12 ตัว ให้บริการ จะจ่ายการร้องขอไปยังแต่ละเครื่องเรียงตามลำดับเครื่องที่ 1,2,3,…,12 แล้วกลับไปจ่ายการร้องขอให้ตัวแรกใหม่อีกครั้ง
2. Least Connection เป็นการกระจายงานตาม Connection ที่เชื่อมต่อในระบบแต่ละระบบ โดยมองว่าแต่ละเครื่องที่ให้บริการควรมี Connection เท่าๆ กัน
3. Weight Distribution เป็นการกระจายงานตามค่า Weight ที่ผู้ดูแลระบบตั้งค่าไว้
4. Response Time เป็นการกระจายงานตามค่า Response Time ของแต่ละระบบ โดยเครื่องที่มี Response Time สูงควรได้รับภาระงานมากกว่าเครื่องที่มี Response Time ต่ำกว่า
5. Least Connection & Response Time เป็นรูปแบบการกระจายงานตามจำนวนการเชื่อมต่อและค่า Response Time
6. Primary & Backup Server เป็นรูปแบบการกระจายงานโดยแบ่งเซิร์ฟเวอร์ที่ให้บริการเป็นเซิร์ฟเวอร์หลัก และ Backup Server การทำงานดังกล่าวสามารถทำให้ระบบมี Avaliability สูงขึ้นด้วย

เทคนิคต่างๆ ที่ใช้ในการส่งคำร้องขอต่างๆ ไปยังเซิร์ฟเวอร์ที่ให้บริการ

1. Server Load Balance เป็นกระบวนการทำงานคล้ายกับการทำ Network Address Translation
2. Source Nat เป็นกระบวนการกระจายงานโดยทำงานคล้ายกับ Application Proxy โดยจะทำการตั้งค่าระบบให้อุปกรณ์ Load Balance เป็นผู้ร้องขอการให้บริการจากเซิร์ฟเวอร์เอง
3. Direct Server Return เป็นกระบวนการ Redirect แพ็กเก็ตที่ร้องขอไปยังเซิร์ฟเวอร์โดยการปรับแต่ง Destination MAC Address ให้ Redirect ไปยังเครื่องเซิร์ฟเวอร์ปลายทาง แล้วให้เซิร์ฟเวอร์ปลายทางตอบกลับไปยังผู้ร้องขอเองอัตโนมัติ ในการตั้งค่าระบบให้สามารถดำเนินการเช่นนี้ได้ต้องมีการตั้งค่า Loop Back Address เป็นไอพีเดียวกันกับอุปกรณ์ Load Balancer ด้วย

ความสามารถอื่นๆ ของ Load Balancer

Application Level Health Check

เนื่องจากลักษณะการทำงานของ Load Balancer อยู่ในลักษณะการแจกจ่ายงานไปยังบริการที่เปิดอยู่ในเซิร์ฟเวอร์ต่างๆ ซึ่งปัญหาที่เกิดขึ้นจะเกิดขึ้นเมื่อจ่ายงานไปแล้ว เซิร์ฟเวอร์ต่างๆ ไม่สามารถให้บริการกับการร้องขอนั้นๆ ได้ ทำให้การร้องขอนั้นไม่ได้รับบริการที่ถูกต้อง อุปกรณ์ Load Balancer จึงต้องมีการตรวจสอบเป็นกระบวนการตรวจสอบว่าบริการต่างๆ ยังสามารถให้บริการได้อย่างเหมาะสมหรือไม่ หากตรวจสอบแล้วพบว่าบริการของเซิร์ฟเวอร์ตัวใดไม่สามารถให้บริการได้ จะไม่ส่งงานไปยังบริการของเซิร์ฟเวอร์นั้นๆ ซึ่งกระบวนการตรวจสอบว่าระบบยังสามารถให้บริการได้นั้นเรียกว่า Health Check

Content Management

จากการให้บริการในลักษณะแจกงานไปยังเซิร์ฟเวอร์ที่ให้บริการส่วนงานนั้นๆ ทำให้เซิร์ฟเวอร์แต่ละตัวจำเป็นต้องมีการติดตั้ง Application ที่ให้บริการไว้เหมือนๆ กัน รวมถึงข้อมูลที่ให้บริการต้องเป็นข้อมูลชุดเดียวกันด้วย ส่งผลให้การอัพเดทข้อมูลในเซิร์ฟเวอร์ทุกตัวที่ทำงานซ้ำซ้อนกันก็ทำได้ยาก จากเหตุการณ์ดังกล่าวทำให้ผู้ดูแลระบบสามารถออกแบบระบบให้ได้ผลดีทั้งการกระจายงาน และการกระจายข้อมูลที่เก็บ เพื่อหลีกเลี่ยงปัญหาข้อมูลซ้ำซ้อน ยากแก่การอัพเดทข้อมูลให้เหมือนกันในทุกๆ ระบบ หรือทำให้มีระบบที่จะเกิดข้อมูลซ้ำซ้อนกันน้อยที่สุดได้ โดยแบ่งการเก็บข้อมูลเป็นไดเร็กทอรี แล้วกำหนดเซิร์ฟเวอร์แต่ละตัวว่าต้องรับผิดชอบการเก็บข้อมูลไดเรกทอรีใดบ้าง

จากการทำงานดังกล่าวทำให้ Load Balancer จำเป็นต้องมีความสามารถในการ Redirect ข้อมูลให้ตรงกับ URL ที่ร้องขอมา โดยเมื่อมีการร้องขอใช้บริการและมีรายละเอียด URL มายัง Load Balancer จะต้องส่งข้อมูลไปยังเซิร์ฟเวอร์ที่ให้บริการที่เก็บข้อมูลไดเรกทอรีนั้นๆ ได้ ความสามารถดังกล่าวจะเรียกว่า URL Switching ซึ่งสามารถดำเนินการได้ทั้งการตั้งกฎ โดยดูจาก Prefix, Suffix หรือรูปแบบของ URL หรือทำ URL Hashing เพื่อส่งการร้องขอไปยังเซิร์ฟเวอร์ตามกฎได้

Session Persistence

อีกปัญหาหนึ่งที่ Load Balance จำเป็นต้องมีกระบวนการดำเนินการเพื่อให้การทำงานของผู้ใช้งานเป็นปกติคือ การทำให้ผู้ใช้งานระบบสามารถใช้งานระบบได้อย่างต่อเนื่อง และยังคงสิทธิการใช้งานระบบอยู่ตลอดเวลา แต่โดยการทำงานของ Load Balancer จะดำเนินการส่งการร้องขอไปยังเซิร์ฟเวอร์ต่างๆ โดยใช้อัลกอริทึมที่หลากหลาย การจะทำให้ผู้ใช้งานสามารถคงสิทธิการใช้งานได้ตลอดนั้น จำเป็นต้องมีกระบวนการที่ทำให้การจ่ายงานของผู้ใช้งานที่มีการระบุ Session เรียบร้อยแล้ว จะต้องไปยังเซิร์ฟเวอร์เดียวกันตลอดการใช้งาน หรือต้องมีการตั้งค่าระบบให้มีการใช้ค่า Session เดียวกันทั้งหมดจึงทำให้ระบบสามารถทำงานได้โดยไม่ติดขัด แต่โดยทั่วไปจะใช้กระบวนการแรกคือการทำให้การจ่ายงานของผู้ใช้งานที่มีการระบุ Session เรียบร้อยแล้วส่งไปยังเซิร์ฟเวอร์เดียวกันตลอดการใช้งาน โดยวิธีการในการดำเนินการมีตัวอย่างดังนี้

1. Cookie Based Switching
2. Cookie Based Hashing
3. SSL ID Switching

High Availability Load Balance

อุปกรณ์ Load Balance เป็นอุปกรณ์หนึ่งที่อาจเกิดปัญหาจนไม่สามารถทำงานได้ ดังนั้นจึงต้องพึ่งพาการออกแบบระบบให้มีความพร้อมในการใช้งานสูงเช่นเดียวกับอุปกรณ์อื่นๆเช่นกัน ในการออกแบบสามารถติดตั้งระบบ Load Balance ในสองรูปแบบคือ

1. Active – Active สำหรับเพิ่มความสามารถในการให้บริการ (Scalability)
2. Active – Standby สำหรับเพิ่มความพร้อมในการใช้งาน (Fault Tolerant)

Global Server Load Balance

สำหรับระบบที่มีการขยายตัวของผู้ใช้งานมากที่สุดคืออินเตอร์เน็ต และบริการต่างๆ ที่ให้บริการกับผู้ใช้งานในโลกอินเตอร์เน็ตนั้น ยิ่งมีความจำเป็นต้องมีการออกแบบระบบให้สามารถรองรับผู้ใช้งานที่มีปริมาณ

มาก มีแนวโน้มเพิ่มสูงขึ้นอย่างมาก และกระจายตัวอยู่ในทุกมุมโลก โดยการออกแบบที่ใช้งานในองค์กรระดับโลกต่างๆ ใช้คือการแบ่งโซนของการให้บริการเป็นส่วนๆ โดยอาจแบ่งเป็นทวีปต่างๆ หรือประเทศต่างๆ แล้วจัดวางเซิร์ฟเวอร์ที่ให้บริการเพื่อรอรับการร้องขอจากผู้ใช้งานตามโซนที่แบ่ง เมื่อเทียบกับทฤษฎีของ Load Balance แล้วกลุ่มของเซิร์ฟเวอร์ที่กระจายตัวกันอยู่ในแต่ละจุดในโลก จะเหมือนกับ Server Farm ในระบบสารสนเทศ การทำงานของ Load Balance จึงต้องมีการปรับเปลี่ยนเล็กน้อยเพื่อให้การร้องขอจากผู้ใช้งาน จะถูกจ่ายไปยังเซิร์ฟเวอร์ที่เหมาะสม

ข้อกำหนดบางอย่างสำหรับการทำ Global Server Load Balance มีดังนี้

1. ผู้ใช้งานทั้งหมดจะต้องเห็นว่าเว็บไซต์ที่ให้บริการมีเพียงเว็บไซต์เดียวเท่านั้น
2. ต้อง Redirect การร้องขอของผู้ใช้งานไปยังเว็บไซต์ที่ใกล้ที่สุดเพื่อให้ผู้ใช้งานได้รับข้อมูลเร็วที่สุด
3. ต้อง Rediract การร้องขอของผู้ใช้งานไปยังเว็บไซต์ที่เหมาะสม หากเว็บไซต์แรกไม่สามารถให้บริการได้
4. มีระบบการ Backup บริการหากมีอุบัติเหตุ ทำให้ระบบปลายทางไม่สามารถให้บริการได้

สำหรับแนวทางการออกแบบระบบให้สามารถทำ Global Server Load Balance ได้สามารถทำได้หลากหลายรูปแบบ สำหรับรูปแบบที่ง่ายที่สุดคือการใช้ DNS โดยการตั้งค่าสามารถทำได้การกำหนดค่า IP Address ของเว็บไซต์เป็นกลุ่มของเซิร์ฟเวอร์ทั้งหมด แต่กระบวนการดังกล่าวมีข้อจำกัดดังนี้คือ

1. ไม่มี Server Health Check
2. ไม่มี Application Health Check
3. ไม่สามารถ Redirect การร้องขอของผู้ใช้งานไปยังเซิร์ฟเวอร์ที่เหมาะสมที่สุดได้
4. มีการทำงานแบบ Round Robin ประสิทธิภาพการทำงาน Load Balance จึงไม่ดีนัก
5. กระบวนการดังกล่าวทำให้ Local DNS จะเก็บข้อมูล (cache) IP Address ของเว็บไซต์ปลายทางไว้ถึงแม้ว่าจะมีการ Update ข้อมูลไปแล้ว

อีกวิธีการหนึ่งคือการใช้ความสามารถของ HTTP โดยใช้ HTTP Redirect เป็นเครื่องมือหลัก ในการร้องขอบริการจากผู้ใช้งานทุกคนจะวิ่งไปยังเว็บไซต์หลัก แล้วเว็บไซต์หลักจะส่ง HTTP Redirect กลับไปยังผู้ใช้งาน

โดยกำหนดให้ผู้ใช้งานร้องขอไปยังเว็บเพจของเว็บไซต์รองที่ตั้งค่าไว้ ซึ่งกระบวนการนี้การตั้งค่าระบบจะอยู่ที่เว็บไซต์หลักเท่านั้น สำหรับระบบนี้จะมีข้อจำกัดคือจะใช้ได้กับ HTTP เท่านั้น และแต่ละไซต์จะต้องมีชื่อที่แตกต่างกัน

สำหรับวิธีการที่สนับสนุนการทำงานในลักษณะ Global Server Load Balance ที่มีความสามารถสูงและตอบโจทย์ด้านการบริหารจัดการได้ดีที่สุด คือการใช้อุปกรณ์ Load Balance มาใช้ โดยแต่ละเว็บไซต์ไม่ว่าจะเป็นเว็บไซต์กลาง หรือเว็บไซต์ที่ให้บริการในส่วนย่อยๆ จะมีอุปกรณ์ Load Balance คอยบริหารจัดการ

บทที่ 14. การจัดการระบบรักษาความปลอดภัยข้อมูล

การจัดการระบบการรักษาความปลอดภัยข้อมูลอาศัย Information Security Management Framework มีขั้นตอนต่างๆ ดังนี้

ขั้นตอนที่ 1 การบริหารความเสี่ยง, การทำ Vulnerability Assessment และ Penetration Testing

ขั้นตอนที่ 2 การทำ Critical Hardening / Patch และ Fixing

ขั้นตอนที่ 3 การจัดทำ Information Security Policy ที่สามารถนำมาใช้งานจริงได้

ขั้นตอนที่ 4 การป้องกันในระดับลึก และการทำ Best Practice Implementation

ขั้นตอนที่ 5 การสร้างการตระหนักรู้เกี่ยวกับการรักษาความปลอดภัย และการฝึกอบรมเพื่อการส่งผ่านความรู้ทางเทคนิคต่างๆ

ขั้นตอนที่ 6 การทำ Internal และ external audit และการทำ Re-assessment และ Re-hardening

ขั้นตอนที่ 7 การทำ Managed Security Service (MSS) และ Realtime Monitoring โดยใช้ระบบ IDS และ IPS

โดยรายละเอียดของการทำงานแต่ละขั้นตอนมีดังนี้

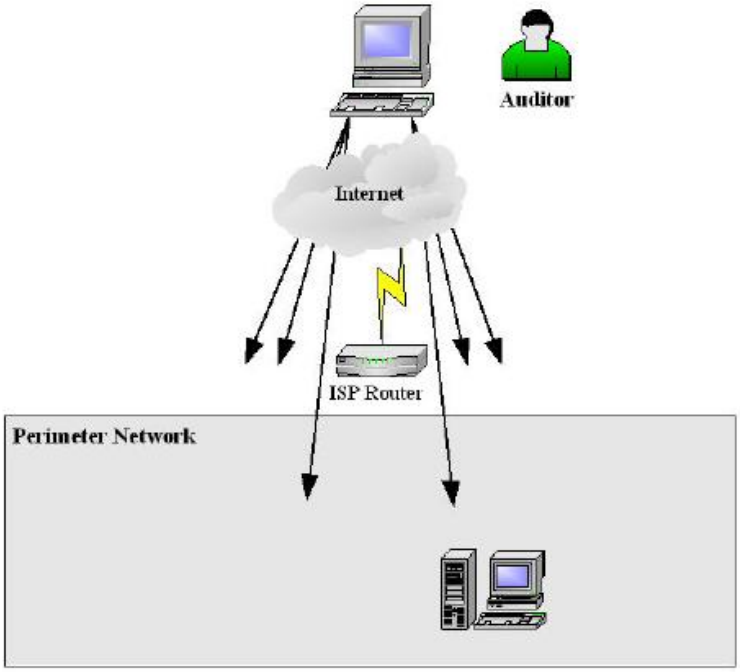
ขั้นตอนที่ 1 การบริหารความเสี่ยง,การทำ Vulnerability Assessment และ Penetration Testing

ขั้นตอนแรกในการจัดการระบบการรักษาความปลอดภัยข้อมูลคือการบริหารความเสี่ยง การทำ Vulnerability Assessment และ การทำ Penetration Testing ซึ่งวัตถุประสงค์ในขั้นตอนแรกนี้คือการหาข้อมูลคุณลักษณะของระบบในมุมมองด้านการรักษาความปลอดภัย โดยผลลัพธ์ที่ได้คือปัญหาด้านความปลอดภัยในระบบและแนวทางในการแก้ไขปัญหาต่างๆ

การทำ Vulnerability Scanner คือการวิเคราะห์ตรวจสอบหาช่องโหว่ต่างๆ ในระบบโดยใช้ Security Tools ต่างๆเครื่องมือที่ใช้งานทั่วไปเช่น Acunetix Web Vulnerability Scanner , GFI LANguard Network Security Scanner , Nessus™ vulnerability scanner , Retina Network Security Scanner , SAINT , QualysGuard N-Stalker Web Application Security Scanner

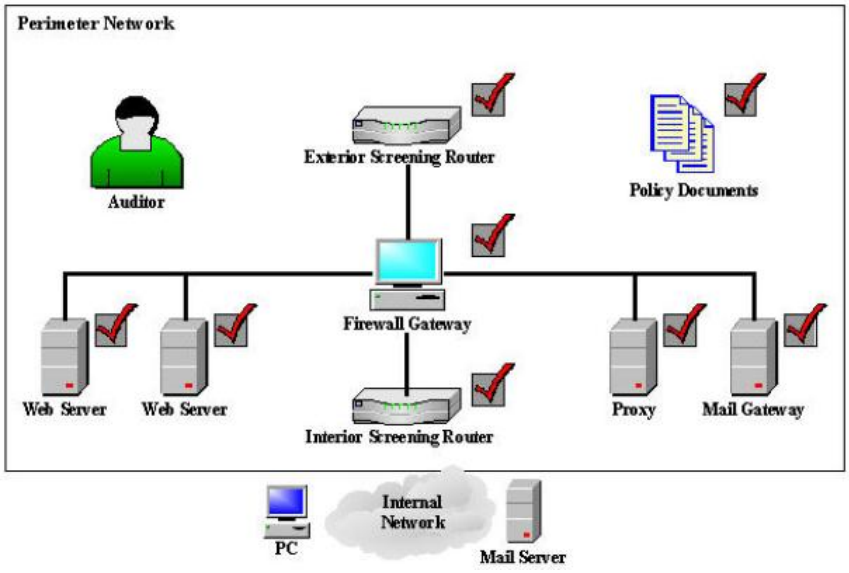
การทำ Penetration Testing คือการทดสอบเจาะระบบเพื่อนำเอาข้อมูลสำคัญเช่น บัญชีผู้ใช้พร้อมทั้งรหัสผ่าน รวมถึงข้อมูลอื่นๆ ที่สำคัญ โดยการทดสอบในลักษณะนี้จะดำเนินการเหมือนกับการเจาะระบบโดยแฮกเกอร์ การทำ Penetration Testing แบ่งออกเป็น 2 รูปแบบคือ Black-Box Penetration Testing และ White-Box Penetration Testing

Black-Box Penetration Testing คือ กระบวนการทดสอบระบบโดยการเจาะระบบโดยผู้ทดสอบจะไม่ได้รับข้อมูลรายละเอียดของระบบ โดยจะได้รับข้อมูลเพียง URL หรือ IP Address เท่านั้น ซึ่งผู้ทดสอบระบบจะดำเนินการทดสอบระบบโดยแฮกเข้าสู่ระบบผ่านอินเตอร์เน็ต ในการทดสอบจะได้ผลลัพธ์เชิงรายละเอียดมากน้อยเพียงใดขึ้นอยู่กับความสามารถของผู้ทำการทดสอบ ข้อดีของการทำ Black-Box Penetration Testing คือ สามารถประเมินความแข็งแกร่งของระบบได้จากภายนอกระบบโดยข้อสรุปที่ได้จะเป็นข้อสรุปในลักษณะความยากง่ายและความเป็นไปได้ในการเจาะระบบผ่านอินเตอร์เน็ต ข้อเสียของการทำ Black-Box Penetration Testing คือการเจาะระบบจากภายนอก อาจไม่สามารถเจาะเข้าระบบได้ เพราะข้อมูลมีน้อย หรือผู้ทดสอบระบบมีความสามารถไม่มากพอ และผลลัพธ์ที่ได้ไม่ได้บ่งบอกว่าระบบย่อยต่างๆ ที่ทำงานร่วมกันในระบบทดสอบ มีช่องโหว่มากน้อยเพียงใด และต้องดำเนินการกับระบบย่อยเหล่านั้นอย่างไรบ้าง



รูปที่ 69 Black-Box Penetration Testing

White –Box Penetration Testing คือการทดสอบการเจาะระบบ โดยผู้ทดสอบจะดำเนินการเจาะระบบจากภายในระบบที่ต้องการทดสอบ ข้อดีของการทำ White-Box Penetration Testing คือผู้ทดสอบระบบจะสามารถประเมินความเสี่ยงได้ใกล้เคียงกับความเป็นจริงมากกว่าแบบ Black-Box Testing เนื่องจากผู้ทดสอบระบบจะทราบข้อมูลภายในของระบบได้มากกว่า ข้อเสียของการทำ White-Box Penetration Testing คือ การเจาะระบบจากภายในจะให้ผลลัพธ์คือความปลอดภัยของระบบย่อยต่างๆ แต่ไม่สามารถระบุปัญหาในกรณีที่มีแฮกเกอร์โจมตีจากภายนอกระบบได้



รูปที่ 70 White-Box Penetration Testing

เนื่องจากข้อมูลของ White-Box Penetration Testing และ Black-Box Penetration Testing จะให้ผลลัพธ์การทดสอบแตกต่างกัน แต่เป็นการให้ข้อมูลช่องโหว่ของระบบในคนละมุมมองกัน การทดสอบระบบจึงควรทดสอบทั้ง White-Box Penetration Testing และ Black-Box Penetration Testing แล้วนำข้อมูลทั้งสองมาประมวลผลร่วมกัน จากการดำเนินการทั้ง การทำ Vulnerability Assessment และ Penetration Testing จะให้ผลลัพธ์คือช่องโหว่ต่างๆ ที่สำคัญพร้อมทั้งแนวทางในการแก้ไขช่องโหว่ดังกล่าว

ขั้นตอนที่ 2 การทำ Critical Hardening / Patch และ Fixing

หลังจากที่ทำการหาช่องโหว่โดยกระบวนการ Scan และกระบวนการ Penetration Testing จะทำการจัดลำดับความสำคัญของช่องโหว่ที่พบว่า ช่องโหว่ใดที่มีความจำเป็นเร่งด่วนที่ต้องแก้ไข โดยสามารถจัดเป็นลำดับ หรือจัดเป็นกลุ่ม เช่นกลุ่มช่องโหว่ที่ทำให้เกิดความเสี่ยงในระดับ สูง กลาง ต่ำ เป็นต้น สำหรับกระบวนการค้นหาช่องโหว่ในระบบโดยใช้โปรแกรม Vulnerability Scanner เช่น Nessus, Retina, Internet Scanner และ Shadow Security Scanner จะสามารถจัดลำดับความสำคัญได้โดยอัตโนมัติ จากช่องโหว่ต่างๆ ใน

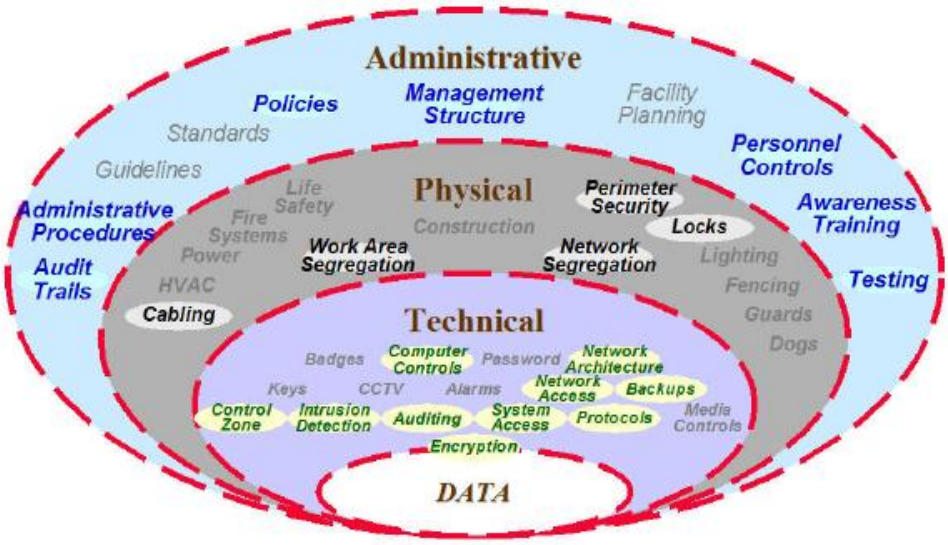
ระบบนั้น จำเป็นต้องมีการทำ Harddening เพื่อปิดช่องโหว่ต่างๆ โดยจะเน้นไปที่ช่องโหว่ที่มีนัยสำคัญในระดับสูงก่อน กระบวนการทำ Harddening ที่สำคัญได้แก่

- ปิด Port ของบริการต่างๆ ที่ไม่จำเป็นต้องใช้งานของ Host/Server ต่างๆ ในระบบ
- แก้ไขการตั้งค่าระบบที่เป็นค่า Default ในการติดตั้งระบบครั้งแรก
- ทำการติดตั้ง Patch หรือ Hotfix
- ติดตั้งและใช้งานโปรแกรม Personal Firewall ในการป้องกันและตรวจจับ IP Address ของผู้บุกรุก
- ปิด Port หรือบริการต่างๆ ที่ Border Firewall และ Border Router ACL

ขั้นตอนที่ 3 การจัดทำ Information Security Policy ที่สามารถนำมาใช้งานจริงได้

ขั้นตอนนี้เป็นขั้นตอนที่ให้ความสำคัญกับการจัดทำ Information Security Policy ที่ต้องสามารถนำมาใช้งานจริงได้ สำหรับการกำหนดนโยบายต่างๆ จะมีการกำหนดขอบเขตของการควบคุมไว้เป็นหลายชั้นดังนี้

1. Administrative Level
2. Physical Level
3. Technical Level
4. Data Level



รูปที่ 71 ลำดับชั้นการกำหนดขอบเขตการควบคุม

ในชั้น Administrative Level เป็นการกำหนดนโยบายด้านการบริหารจัดการต่างๆ ในระบบได้แก่

- การกำหนดโครงสร้างการบริหารจัดการ
- การกำหนดนโยบายต่างๆ
- การกำหนดมาตรฐานต่างๆ
- การกำหนดแนวทางปฏิบัติ (Guideline) ต่างๆ
- กระบวนการบริหารจัดการ
- การตรวจสอบระบบ
- การวางแผนการใช้งานทรัพยากรระบบ
- การควบคุมในระดับบุคคล
- การฝึกอบรมเพื่อตระหนักรู้ด้านการรักษาความปลอดภัยระบบ
- การทดสอบระบบ

ในชั้น Physical Layer เป็นการกำหนดนโยบายเพื่อควบคุมองค์ประกอบต่างๆ ในระบบได้แก่

- นโยบายเรื่องการใช้งานอาคารและสิ่งก่อสร้างต่างๆ
- นโยบายเรื่องการใช้พื้นที่ปฏิบัติงานต่างๆ
- นโยบายเรื่องการรักษาความปลอดภัยพื้นที่ต่างๆ
- นโยบายเรื่องการปิดกั้นพื้นที่ต่างๆ

ในชั้น Technical Layer เป็นการกำหนดนโยบายเพื่อกำหนดองค์ประกอบทางเทคนิคต่างๆ ในระบบได้แก่

- การควบคุมระบบคอมพิวเตอร์
- การควบคุม Network Zone ต่างๆ
- การตรวจจับผู้บุกรุก
- สถาปัตยกรรมเครือข่าย
- การเข้าถึงระบบเครือข่าย และระบบคอมพิวเตอร์ต่างๆ
- การสำรองข้อมูล
- การตรวจสอบระบบ
- โพรโตคอลต่างๆ

ในชั้น Data Layer เป็นการกำหนดนโยบายเกี่ยวกับการบริหารจัดการข้อมูลต่างๆ ในระบบได้แก่

- การเข้ารหัสข้อมูลที่สำคัญ
- การกำหนดกระบวนการในการเข้าถึงข้อมูลต่างๆ
- การกำหนดสิทธิในข้อมูลสำหรับผู้ใช้งานระบบต่างๆ

ตัวอย่าง Security Policay ที่เป็นมาตรฐานหรือมีการใช้งานอย่างแพร่หลายได้แก่

1. BS ISO/IEC 17799 เป็นมาตรฐานที่มักนำไปอ้างอิงในการเขียนนโยบายด้านการรักษาความปลอดภัยข้อมูลคอมพิวเตอร์ซึ่งเน้นในรูปแบบการทำงาน และภาพรวมของระบบโดยไม่มีรายละเอียดแนวทางการปฏิบัติเชิงรายละเอียดการปฏิบัติ
2. CobiT (Control Objective for Information and Related Technology) เป็นนโยบายที่เน้นในการตรวจสอบโดยผู้ตรวจสอบด้าน Information System โดยตรง ซึ่งธนาคารหรือสถาบันการเงินมักนำมาใช้งาน
3. CBK (Common Body of Knowledge) เป็นข้อมูลพื้นฐาน หรือองค์ความรู้สำคัญที่จำเป็นในการกำหนดนโยบายด้านการรักษาความปลอดภัยระบบข้อมูลคอมพิวเตอร์ซึ่งคิดค้นขึ้นโดยสถาบัน ISC^2 (www.isc2.org)
4. SANS / FBI Top20 Vulnerability เป็นข้อมูลเกี่ยวกับช่องโหว่และการสำคัญสำหรับผู้ดูแลระบบในการนำไปใช้กับระบบที่ตนเองดูแล

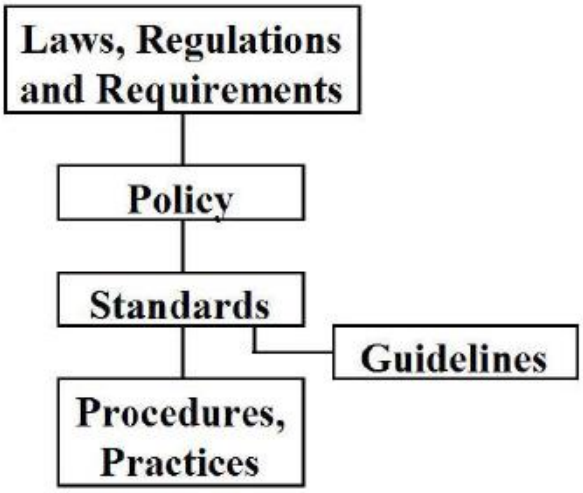
Security Policy Plan

Policy หมายถึง นโยบายในภาพรวมที่กระชับและได้ใจความเรียกว่า “Goal” หรือเป้าหมายที่ต้องการบรรลุ

Standard หมายถึง มาตรฐานที่ต้องบังคับใช้ในการปฏิบัติจริงเช่นมาตรฐานเกี่ยวกับการตั้งรหัสผ่าน เป็นต้น

Guideline หมายถึงแนวทางในการปฏิบัติที่ไม่ได้บังคับแต่แนะนำเพื่อให้ผู้ปฏิบัติสามารถบรรลุเป้าหมายได้ง่ายขึ้น

Procedure หมายถึง รายละเอียดปลีกย่อยเป็นข้อๆ ที่ต้องนำมาปฏิบัติเพื่อให้ได้มาซึ่ง Standard ที่ได้วางไว้



รูปที่ 72 Policy Diagram

จะเห็นได้ว่าเราไม่สามารถนำ Information Security Policy จากแหล่งต่างๆ มาใช้งานได้ทันที เนื่องจากเราต้องมีการประเมินสถานการณ์ความเสี่ยงขององค์กรก่อน ถ้าขาดขั้นตอนนี้จะทำให้ขาดข้อมูลในการจัดการและไม่สามารถนำนโยบายที่กำหนดขึ้นมาใช้งานได้จริง

ขั้นตอนที่ 4 การป้องกันในระดับลึก และการใช้สูตรสำเร็จต่างๆ มาใช้

ในขั้นตอนนี้เป็นกระบวนการที่มีรายละเอียด ใช้กำลังคน งบประมาณ ระยะเวลาในการดำเนินการและความรู้เชิงลึกในด้าน Information Security สูงมาก เพื่อทำให้ระบบขององค์กรมีความปลอดภัยทั้งในปัจจุบันและอนาคต ในการป้องกันในระดับลึกจะดำเนินการดังต่อไปนี้

- การจัดการแบบ “Layered Security” โดยจัดแบ่งระบบออกเป็นชั้นๆ แล้วทำการป้องกันระบบแต่ละชั้น โดยมีรายละเอียดในการป้องกันแตกต่างกันออกไปในแต่ละชั้น ในทางเทคนิคเราจะรวมวิธีการดังกล่าวว่า “Compartmentalization” เช่นการทำ VLAN แยกระบบออกจากกัน การแบ่งเครือข่ายออกเป็นเครือข่ายย่อยๆ หรือการแบ่ง DMZ (Demilitarized Zone) หลายๆ Zone เป็นต้น
- ออกแบบระบบเครือข่ายใหม่โดยเน้นความปลอดภัยในการใช้งานมากขึ้น
- ปรับแต่ง Configuration ต่างๆ ในระบบให้มีช่องโหว่ในระบบน้อยที่สุด

- จัดทำแผนการจัดการกับการเปลี่ยนแปลงต่างๆ ที่อาจเกิดขึ้นในระบบ
- การสร้างระบบ Log Monitoring ในระบบ
- ดำเนินการจัดการรักษาความปลอดภัยระบบย่อยๆ ต่างๆ เช่น Web Application , Database , Web Server เป็นต้น
- วางแผนการกู้ระบบฉุกเฉินและแผนการจัดการกับความเสียหายในระบบสารสนเทศเพื่อให้ธุรกิจสามารถดำเนินการได้อย่างต่อเนื่อง

ในการบริหารจัดการที่ง่าย และสามารถใช้งานได้ทันทีคือการนำเอาสูตรสำเร็จใจการบริหารจัดการมาใช้งาน (Best Practice Implementation) เช่นถ้ามีการใช้งาน IIS ควรนำ IIS Best Practice มาใช้เป็นหลักในการติดตั้ง ตรวจสอบระบบซึ่ง Best Practice โดยทั่วไปจะประกอบไปด้วยรายละเอียดทางด้านเทคนิคที่ผู้ดูแลระบบควรปฏิบัติ ตั้งแต่การติดตั้งระบบจนถึงการใช้งานรายวัน รายละเอียดการปิดช่องโหว่ต่างๆ เช่นการจัดการกับค่า Default การลบไฟล์ตัวอย่าง (Example Files) ต่างๆที่ไม่ได้ใช้งานเป็นต้น

ขั้นตอนที่ 5 การสร้างการตระหนักรู้เกี่ยวกับการรักษาความปลอดภัย และการฝึกอบรมเพื่อการส่งผ่านความรู้ทางเทคนิคต่างๆ

ในขั้นตอนการฝึกอบรมเพื่อการตระหนักรู้เกี่ยวกับการรักษาความปลอดภัยนี้เป็นขั้นตอนที่มีความสำคัญสูง แต่เป็นขั้นตอนที่หลายๆ คนมองข้ามและมองว่าควรจะมีการฝึกอบรมเฉพาะฝ่าย IT และฝ่าย Security เท่านั้น แต่ความเป็นจริงแล้วผู้บริหารระดับสูงและระดับกลางตลอดจนพนักงานที่ต้องใช้งานคอมพิวเตอร์ในองค์กรก็มีความจำเป็นที่จะต้องถูกฝึกอบรมด้วย

ในการฝึกอบรมต่างๆ ควรมีการแสดงกรณีตัวอย่างหรือ Case Study ให้ผู้เข้ารับการฝึกอบรมเห็นว่า Hacker และ Virus มีวิธีการโจมตีอย่างไรบ้าง ซึ่งเมื่อทุกคนได้เห็นตัวอย่างแล้วก็จะเกิดความตระหนักได้ว่า จากนี้ต้องใช้งานเครือข่ายและอินเตอร์เน็ตด้วยความระมัดระวังมากขึ้น โดยไม่ต้องมีฝ่าย IT คอยบังคับพฤติกรรมการใช้งานอีกต่อไป

สำหรับการฝึกอบรมด้านการตระหนักรู้ทางด้านการรักษาความปลอดภัยระบบจะถูกแบ่งออกเป็นหลายระดับตามกลุ่มผู้ใช้งานได้แก่

- กลุ่มผู้บริหารระดับสูง
- กลุ่มผู้บริหารระดับกลาง
- กลุ่มผู้ดูแลระบบ (System Administrator)
- กลุ่มผู้ดูแลความปลอดภัยระบบคอมพิวเตอร์ (Security Administrator)
- กลุ่มผู้ตรวจสอบระบบสารสนเทศ (IT Auditor)
- กลุ่มผู้ใช้งานคอมพิวเตอร์ทั่วไป (User)

ขั้นตอนที่ 6 การทำ Internal และ external audit และการทำ Re-assessment และ Re-hardening

ในกระบวนการที่ดำเนินการตามขั้นตอนตั้งแต่ขั้นตอนแรกนั้น จะมีการดำเนินการตรวจสอบหาช่องโหว่ในระบบแล้วจึงปิดช่องโหว่ด้วยกระบวนการต่างๆ มากมาย แต่ผู้ดูแลระบบจะแน่ใจได้อย่างไรว่าระบบที่ผ่านกระบวนการ Harddening แล้วจะมีช่องโหว่หลงเหลืออยู่หรือไม่ ดังนั้นจึงต้องมีกระบวนการในการตรวจสอบอีกครั้ง โดยขั้นตอนนี้จะเป็นการดำเนินการซ้ำในขั้นตอน Assessment และมีการทำ Harddening ในส่วนของช่องโหว่ที่ยังค้างอยู่ในระบบ

นอกจากนี้ยังต้องดำเนินการประเมินความเสี่ยงที่เกิดขึ้นกับระบบ (Risk Assessment) หรือแม้กระทั่งขององค์กรทั้งหมด ซึ่งมีขั้นตอนที่ต้องปฏิบัติคือ

- การระบุปัจจัยที่มีผลต่อความเสี่ยง และการระบุความเสี่ยงต่างๆที่มีโอกาสเกิดขึ้น (Risk Identification)
- การวิเคราะห์ความเสี่ยง (Risk Analysis)
- การบริหารจัดการกับความเสี่ยง (Risk Management)

กระบวนการที่ทำให้ทราบข้อมูลเกี่ยวกับระบบได้ดีที่สุดคือกระบวนการตรวจสอบ (Audit) โดยกระบวนการตรวจสอบต่างๆ นั้นจำเป็นต้องพิจารณาถึงการควบคุมการทำงานต่างๆ ว่าทำได้ถูกต้องหรือไม่โดยการควบคุมต่างๆ ในระบบแบ่งออกได้เป็น 3 ประเภทคือ

- การควบคุมแบบป้องกันล่วงหน้า (Preventive Control)
- การควบคุมแบบค้นหาประวัติเหตุการณ์ที่เกิดขึ้น (Detective Control)
- การควบคุมแบบแก้ไขปัญหาจากเหตุการณ์ที่เกิดขึ้น (Corrective Control)

สำหรับการตรวจสอบระบบสารสนเทศ (IT Audit) ควรพิจารณาการควบคุมใน 3 มุมมองพร้อมๆ กัน ได้แก่

- มุมมองด้านการบริหารจัดการ (Administrative Control)
- มุมมองด้านเทคนิค (Technical Control)
- มุมมองด้านกายภาพ (Physical Control)

ประเภทของ IT Audit สามารถแบ่งออกเป็น 7 ประเภทได้แก่

- การตรวจสอบระบบปฏิบัติการ
- การตรวจสอบอุปกรณ์เครือข่าย
- การตรวจสอบอุปกรณ์รักษาความปลอดภัย
- การตรวจสอบโปรแกรมฐานข้อมูล
- การตรวจสอบโปรแกรมประยุกต์และโปรแกรมที่ให้บริการทางเครือข่ายต่างๆ (Server)
- การตรวจสอบกระบวนการบริหารจัดการควบคุมด้านสารสนเทศ (Administrative Control)
- การตรวจสอบด้านกายภาพ (Physical Control)

ปัญหาที่เกิดขึ้นของ IT Auditor ส่วนใหญ่จะเป็นปัญหาด้านความรู้และประสบการณ์ของผู้ตรวจสอบระบบเช่น

- ความรู้ทางด้านVulnerability Assessment และ Penetration Testing ในลักษณะ Ethical Hacking หรือ White Hat Hacking
- ความรู้พื้นฐานทางด้านเครือข่าย
- ความรู้พื้นฐานด้านการใช้งานระบบปฏิบัติการ
- ความรู้พื้นฐานในการใช้งานอุปกรณ์เครือข่าย Router หรือ Switching
- ความรู้ด้านการรักษาความปลอดภัยข้อมูล

จากปัญหาที่พบของ IT Auditor ทำให้ผู้ที่จะทำหน้าที่เป็น IT Auditor ควรมีคุณสมบัติดังนี้

- มี Certificate ด้านการทำ IT Audit เช่น CISA
- มีความรู้พื้นฐานทางเทคนิค
- มีการฝึกอบรมด้านเทคนิคเพิ่มเติม
- หาความรู้ด้วยตนเองอยู่ตลอดเวลา

ขั้นตอนที่ 7 การทำ Managed Security Service (MSS) และ Realtime Monitoring โดยใช้ระบบ IDS และ IPS

สำหรับระบบที่ต้องการการดูแลจากผู้เชี่ยวชาญ และยังไม่มีทีมผู้ดูแลระบบที่สามารถดูแลระบบทั้งหมดได้ การจัดจ้าง Outsource ด้านการรักษาความปลอดภัยในระบบโดยเฉพาะ เป็นแนวคิดที่ต้องการให้ Outsource มาช่วยในการบริหารความเสี่ยงที่อาจจะเกิดขึ้นในระบบ และช่วยลดความเสี่ยงในระบบโดยรวม การเลือก Managed Security Service Provider (MSSP) จึงเป็นหัวใจสำคัญในการบริหารระบบ ขณะเดียวกันต้องมีการกำหนดข้อตกลงเกี่ยวกับระดับการให้บริการและการรับผิดชอบ (Service Level Agreement) ให้ชัดเจนโดยควรมีรายละเอียดให้มากที่สุดเท่าที่จะทำได้เช่น

- ขอบเขตในการให้บริการของ MSSP
- ระยะเวลาในการให้บริการ และการตอบสนองของ MSSP

- ค่าใช้จ่ายที่เกิดขึ้นในแต่ละเดือน
- ความรับผิดชอบของ MSSP ในแง่กฎหมายและบทปรับ

สำหรับหน้าที่ความรับผิดชอบของ MSSP ควรให้บริการครอบคลุมหัวข้อต่างๆ ดังต่อไปนี้

- บริหารจัดการและเฝ้าระวัง ดำเนินการเกี่ยวกับ Network Perimeter Security ที่ External Firewall , Border Router, IDS/IPS, VPN ตลอดจน Server บริเวณ DMZ
- บริหารจัดการ Vulnerability ให้กับระบบขององค์กรอย่างต่อเนื่อง เช่นการทำ Vulnerability Assessment และทำ Penetration Testing รายเดือน เป็นต้น
- เฝ้าระวัง Internal Network จาก Virus และ Hacker
- เฝ้าระวัง Internal Firewall และ Server Farm ภายในระบบ LAN ขององค์กร
- รับปรึกษาในกรณีที่เกิดปัญหาความปลอดภัย รับแก้ปัญหาในลักษณะ Incedent Response และ Digital Forensic
- บริหารจัดการ Centralize Log Management และ Centralize Patch Management อย่างเป็นระบบ
- บริการแจ้งข่าวความเคลื่อนไหวด้าน Information Security โดยเฉพาะเรื่องเกี่ยวกับช่องโหว่ใหม่ๆ ไวรัสที่กำลังแพร่ระบาดในขณะนั้น ให้ทราบในลักษณะวันต่อวัน

สำหรับข้อดีของการจัดจ้าง MSSP คือ

- สามารถช่วยลดต้นทุนการดำเนินการในองค์กรด้านอัตรากำลัง ของบุคลากรเชี่ยวชาญได้รวมถึง Hardware / Software ต่างๆ
- สามารถได้รับข่าวสารใหม่ๆ ด้าน Information Security
- ได้รับคำปรึกษาเมื่อเกิดปัญหา
- คอยเตือนภัยทางอินเตอร์เน็ตให้องค์กรทราบอยู่ตลอดเวลา

ข้อเสียของการจัดจ้าง MSSP

- ถ้าสัญญาไม่รัดกุมพอจะทำให้เกิดปัญหาในทางปฏิบัติได้
- หาก MSSP ไม่มีความเชี่ยวชาญพอจะทำให้ไม่คุ้มค่าในการลงทุน
- อาจเกิดกรณีที่ระบบเกิดปัญหาแต่ MSSP ไม่สามารถแก้ไขปัญหาหรือให้คำปรึกษาที่เหมาะสมได้ตามที่คาดหวังไว้

ถึงแม้ว่าจะมีข้อเสียในการจัดจ้าง MSSP แต่ข้อดีก็มีมากกว่า การตกลงทำงานร่วมกันกับ MSSP ในลักษณะที่ช่วยเหลือซึ่งกันและกัน โดยงานที่ต้องใช้ความสามารถเฉพาะทางจะมอบให้ MSSP เป็นผู้ดูแลส่วนองค์กรจะเป็นผู้ตรวจสอบการทำงานของ MSSP ว่าปฏิบัติตาม Service Level Agreement หรือไม่ จะทำให้ไม่เกิดปัญหาในระยะยาวกับ MSSP และเป็นการบริหารความเสี่ยงที่ถูกหลัก “IT Outsourcing”

บทที่ 15. การกำหนดนโยบายการรักษาความปลอดภัยตามมาตรฐานสากล

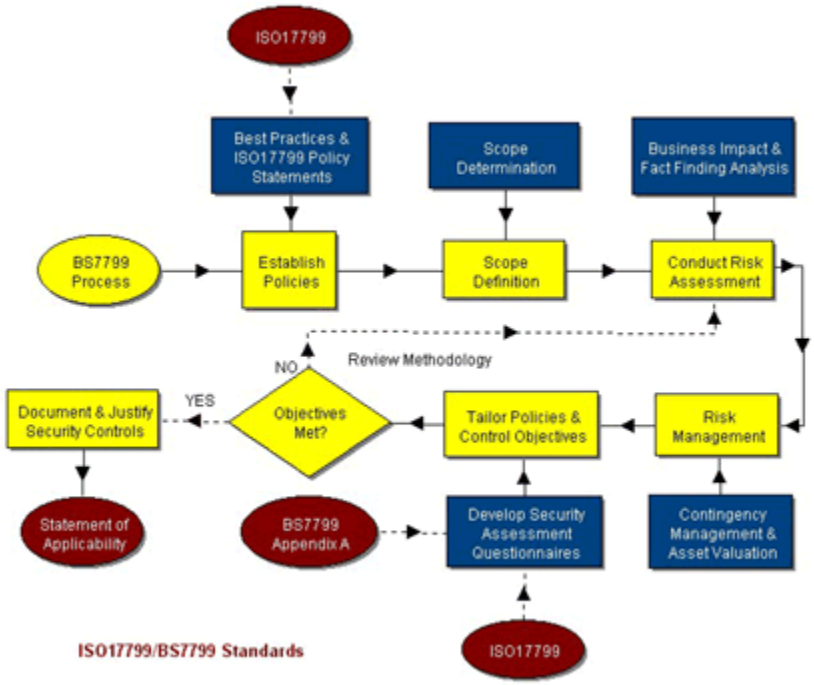
BS7799 (British Standard 7799) เป็นมาตรฐานเกี่ยวกับการจัดการในเรื่องความปลอดภัยของข้อมูล ที่ออกโดย British Standards Institution ซึ่งถูกตีพิมพ์ครั้งแรกในเดือนเมษายน ค.ศ. 1991 โดยใช้ชื่อว่า BS7799:1999 มาตรฐานนี้เป็นส่วนหนึ่งของมาตรฐาน ISO (International Standard Organization)ต่อมาในเดือนตุลาคมปี ค.ศ.2000 ได้มีการปรับปรุงบางส่วนของมาตรฐาน และถูกตีพิมพ์เป็นครั้งที่ 2 ภายใต้ชื่อ ISO/IEC17799:2000 ในวันที่ 1 ธันวาคม ค.ศ. 2000 มาตรฐานนี้ถูกกำหนดขึ้นมาเพื่อเป็นแนวทางในการจัดการด้านความปลอดภัยของข้อมูลภายในองค์กร โดยการกำหนดแนวทางสำหรับการพัฒนามาตรฐานความปลอดภัยและการปฏิบัติงานเพื่อให้เกิดการจัดการที่มีประสิทธิภาพ รวมไปถึงการสร้างความมั่นใจในการติดต่อระหว่างองค์กร เนื่องจากข้อมูลถือเป็นสินทรัพย์ที่มีความสำคัญเช่นเดียวกับสินทรัพย์ทางธุรกิจอื่นๆ ดังนั้นการรักษาความปลอดภัยข้อมูล,การประเมินและการบริหารความเสี่ยงที่เกิดขึ้นจึงถือเป็นสิ่งสำคัญในการบริหารงานองค์กรให้มีประสิทธิภาพ หากกล่าวถึงความปลอดภัยข้อมูล จะต้องประกอบด้วย 3 องค์ประกอบ ดังนี้

1. Confidentiality ในการรักษาความปลอดภัยข้อมูล สิ่งสำคัญที่ต้องคำนึงคือ สิทธิ์ในการเข้าถึงข้อมูลต่างๆ ในระบบงาน ดังนั้นผู้ที่จะสามารถเข้าถึงข้อมูลในระบบนั้น ๆ ได้ จะต้องได้รับการกำหนดสิทธ์ในการเข้าใช้ ซึ่งเป็นไปตามหลัก need-to-know และ need-to-do basis ตัวอย่างเช่น ในการจัดการเกี่ยวกับข้อมูลเงินเดือนของพนักงานในองค์กร ก็จะมีเจ้าหน้าที่ของฝ่ายทรัพยากรบุคคลเท่านั้นที่จะสามารถเข้าถึงข้อมูลนี้ได้ เพราะข้อมูลดังกล่าวเป็นข้อมูลสำคัญและไม่สามารถเปิดเผยได้

2. Integrity ข้อมูลต่าง ๆ ในระบบจะต้องมีความถูกต้อง เช่น ข้อมูลที่เผยแพร่ทางอินเตอร์เน็ต ซึ่งเป็นข้อมูลที่ไม่ได้จำกัดสิทธิ์ในการเข้าถึง จึงส่งผลให้บุคคลภายนอกสามารถเข้าถึงข้อมูลดังกล่าวได้อย่างง่ายดาย ดังนั้นจะต้องมีการกำหนดมาตรการหรือแนวทางในการป้องกันการแก้ไขเปลี่ยนแปลงข้อมูล เพื่อป้องกันความผิดพลาดหรือการบิดเบือนข้อมูลหรือแม้กระทั่งผู้ที่มีสิทธิ์เข้าถึงระบบงานเพื่อทำการแก้ไขข้อมูลก็จะต้องได้รับการอนุมัติจากผู้บังคับบัญชาก่อน เช่น เจ้าหน้าที่ที่ทำการแก้ไขข้อมูลดอกเบี้ยเงินฝากต้องได้รับการอนุมัติจากผู้บังคับบัญชาเท่านั้น

3. Availability ผู้มีสิทธิ์สามารถที่จะเข้าถึงข้อมูลในระบบงานต่าง ๆ ได้ตามต้องการโดยผ่านช่องทางที่องค์กรกำหนด เช่น เจ้าหน้าที่ที่มีสิทธิ์ในการเข้าถึงระบบซื้อขายหลักทรัพย์ของธนาคารสามารถเข้าใช้ข้อมูลใน

ช่วงเวลาที่ต้องการได้อย่างต่อเนื่องโดยไม่เกิดเหตุขัดข้อง เช่น ระบบฐานข้อมูลมีปัญหา ไม่สามารถดึงข้อมูลออกมาได้



รูปที่ 73 ISO17799/BS7799

การบริหารจัดการและส่งเสริมด้านความปลอดภัยข้อมูล จะต้องมีการกำหนดนโยบายการดำเนินงานภายในองค์กรที่ชัดเจน มีการให้ข้อมูล-เผยแพร่เอกสารเกี่ยวกับนโยบายดังกล่าวให้แก่พนักงานทุกคนได้รับทราบ เข้าใจวัตถุประสงค์ ขอบเขตการดำเนินงาน หลักการ และเป้าหมายของความปลอดภัยข้อมูล รวมไปถึงมาตรฐานที่ สอดคล้องกับการดำเนินธุรกิจขององค์กรเพื่อถือปฏิบัติตรงกัน จากนั้นจะต้องมีการประเมินผลว่าบรรลุตามนโยบายที่กำหนดไว้หรือไม่ ส่งผลการทบต่อการดำเนินธุรกิจอย่างไร และผลจากการเปลี่ยนแปลงส่งผลต่อเทคโนโลยีอย่างไร

การรักษาความปลอดภัยข้อมูล เกี่ยวข้องกับการจัดการในด้านต่างๆ ดังนี้

ความปลอดภัยเกี่ยวกับองค์กร

เป็นการบริหารจัดการความปลอดภัยข้อมูลภายในองค์กร โดยมีหลักการดังนี้

1. มีการกำหนดโครงสร้าง, บทบาท – หน้าที่ความรับผิดชอบของผู้เกี่ยวข้อง เพื่อควบคุมการดำเนินงานให้เป็นไปตามขั้นตอนที่ถูกต้องและมีประสิทธิภาพ
2. มีการกำหนดมาตรการในการรักษาความปลอดภัยของข้อมูลและอุปกรณ์ประมวลผลต่างๆ จากบุคคลภายนอก เพราะจะก่อให้เกิดความเสี่ยง / ความเสียหายต่อองค์กรได้ หากไม่มีแนวทางการควบคุมที่รัดกุม
3. กรณีที่มีการว่าจ้างหน่วยงานอื่นให้ดำเนินงานทางด้านการประมวลผลข้อมูล จะต้องระบุมาตรการในการควบคุมไว้ในสัญญาอย่างชัดเจน
4. การดำเนินงานทางด้านความปลอดภัยข้อมูลของแต่ละองค์กร ควรมีการว่าจ้างที่ปรึกษาเพื่อให้ความรู้, คำแนะนำ และช่วยในการตัดสินใจเพื่อหาแนวทางที่ดี และเหมาะสมกับองค์กรมากที่สุด

การควบคุมและการจำแนกสินทรัพย์

จะช่วยในการกำหนดระดับการป้องกันความเสียหายที่อาจเกิดขึ้น โดยแบ่งการจำแนกประเภทของสินทรัพย์ภายในองค์กร ได้ดังนี้

1. สินทรัพย์สารสนเทศ ได้แก่ ข้อมูลต่างๆ ที่ถูกจัดเก็บไว้ในฐานข้อมูล เอกสาร คู่มือใช้งาน สื่อการเรียนการสอน ขั้นตอนการปฏิบัติงาน และแผนงาน
2. สินทรัพย์ซอฟต์แวร์ ได้แก่ ซอฟต์แวร์ประยุกต์ ซอฟต์แวร์ระบบ เครื่องมือต่างๆ ที่ใช้ในการพัฒนาระบบ
3. สินทรัพย์ที่จับต้องได้ได้แก่อุปกรณ์คอมพิวเตอร์ อุปกรณ์สื่อสาร อุปกรณ์จัดเก็บข้อมูล เฟอร์นิเจอร์
4. การให้บริการในด้านต่างๆ ได้แก่ การให้บริการในทางด้านคอมพิวเตอร์ การติดต่อ สื่อสาร สาธารณูปโภค และบริการทั่วๆ ไป เพื่อให้การใช้สินทรัพย์เป็นไปอย่างมีประสิทธิภาพจะต้องมีมาตรการในการควบคุมการใช้สินทรัพย์ดังกล่าวให้เป็นไปตามที่กำหนดไว้ โดยคำนึงถึงลักษณะและความสำคัญ และความจำเป็นในการใช้งาน

ความปลอดภัยตัวบุคคล

เป็นการกำหนดมาตรการเพื่อลดความเสี่ยงอันเกิดจากความผิดพลาดของมนุษย์ โดยมีหลักการดังนี้

1. เริ่มตั้งแต่ขั้นตอนของการว่าจ้างจะต้องมีการกำหนดบทบาทหน้าที่ความรับผิดชอบทางด้านความปลอดภัยไว้ในสัญญาอย่างชัดเจน และติดตามผลการปฏิบัติงานเป็นรายบุคคล

2. กำหนดข้อตกลงร่วมกันว่าข้อมูลของแต่ละฝ่ายถือเป็นความลับ ห้ามมิให้นำข้อมูลของอีกฝ่ายไปเผยแพร่ให้แก่บุคคลอื่น ซึ่งข้อตกลงดังกล่าวจะต้องสอดคล้องกันกับสัญญาการว่าจ้าง
3. อบรมให้พนักงานทราบและตระหนักถึงความสำคัญของการรักษาความปลอดภัยข้อมูล เพื่อเป็นแนวทางในการปฏิบัติงานที่สนับสนุนนโยบายความปลอดภัยขององค์กร
4. รายงานผลกรณีที่เกิดเหตุการณ์ต่างๆ อันส่งผลกระทบต่อความปลอดภัยขององค์กรให้แก่ผู้บริหารได้รับทราบโดยด่วน เพื่อพิจารณาหาแนวทางแก้ไข

ความปลอดภัยเกี่ยวกับสถานที่และสภาพแวดล้อม

เพื่อป้องกันการเข้าถึงจากบุคคลภายนอกที่ไม่ได้รับอนุญาต รวมไปถึงป้องกันความเสียหายและการแทรกแซงข้อมูลต่างๆ โดยมีหลักการดังนี้

1. กำหนดพื้นที่การรักษาความปลอดภัยที่ชัดเจน โดยที่ผู้ถูกอนุญาตเท่านั้นที่จะสามารถเข้าได้
2. มีสัญญาณเตือนภัยกรณีเกิดเหตุฉุกเฉิน เช่น มีเสียงเตือนกรณีเกิดไฟไหม้
3. จัดเก็บเครื่องมือและอุปกรณ์ที่ใช้ในการประมวลผลข้อมูลทางธุรกิจไว้ในบริเวณที่มีความปลอดภัย และมีการควบคุมที่ดี
4. ควบคุมดูแลความปลอดภัยของอุปกรณ์ เพื่อลดความเสี่ยงจากการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต และป้องกันความเสียหายที่อาจเกิดขึ้น เช่น การจัดการเกี่ยวกับระบบสำรองไฟเพื่อรองรับเหตุฉุกเฉินกรณีที่ไฟฟ้าดับ, การบำรุงรักษาอุปกรณ์ให้อยู่ในสภาพดี เหมาะต่อการใช้งาน และมีความถูกต้อง

การบริหารจัดการด้านการปฏิบัติงานและการติดต่อสื่อสาร

เป็นการกำหนดแนวทางในการปฏิบัติงานและเพิ่มความปลอดภัยของอุปกรณ์ประมวลผลข้อมูล เพื่อลดความผิดพลาดของระบบ ได้แก่

<u>การกำหนดบทบาทหน้าที่และความรับผิดชอบในการปฏิบัติงาน</u>

โดยมีหลักการดังนี้

1. จัดทำเอกสารเกี่ยวกับวิธีการปฏิบัติงานที่ถูกกำหนดขึ้นเป็นนโยบายทางด้านการรักษาความปลอดภัย โดยระบุขั้นตอนที่ชัดเจน เช่น เริ่มต้นการการเก็บรวบรวมข้อมูล วิธีการการประมวลผล การวิเคราะห์ผลลัพธ์ กรณีที่เกิดข้อผิดพลาดจะมีแนวทางการจัดการอย่างไร
2. ควบคุมการเปลี่ยนแปลงเกี่ยวกับการปฏิบัติงาน ซึ่งหากควบคุมไม่ดีพอก็จะก่อให้เกิดความล้มเหลวของระบบได้ การควบคุมที่ดีจะต้องคำนึงถึง ขั้นตอนการดำเนินงานการที่เปลี่ยนแปลงไปจะส่งผลให้การปฏิบัติงานเป็นไปในทิศทางใด รวมทั้งการประเมินผลกระทบที่อาจเกิดขึ้นจากการเปลี่ยนแปลงดังกล่าว
3. การจัดการกับเหตุการณ์ที่เกิดขึ้น เช่น กรณีระบบจัดเก็บข้อมูลมีปัญหา การให้บริการที่ผิดพลาด และความผิดพลาดซึ่งเกิดจากข้อมูลทางธุรกิจที่ไม่สมบูรณ์และไม่ถูกต้อง โดยการกำหนดแนวทางการจัดการกับเหตุการณ์ดังกล่าว ต้องเริ่มจากการวิเคราะห์และเพื่อหาสาเหตุของปัญหา วางแผนและกำหนดแนวทางแก้ไขเพื่อป้องกันไม่ให้เกิดเหตุการณ์นี้ขึ้นอีกในอนาคต ท้ายสุดจะต้องมีการรายงานผลให้กับผู้ที่เกี่ยวข้องได้รับทราบเพื่อตระหนักถึงปัญหาที่เกิดขึ้น
4. การแบ่งภาระหน้าที่ความรับผิดชอบ เพื่อติดตามผลการดำเนินงานทางด้านความปลอดภัยขององค์กร ซึ่งจะช่วยลดความเสี่ยงที่เกิดจากการทำงานที่ไม่ถูกต้อง

<u>การวางแผนระบบและการยอมรับระบบงาน</u>

เพื่อเป็นการลดความเสี่ยงที่เกิดจากความล้มเหลวของระบบให้น้อยที่สุด เพราะการวางแผนและการเตรียมการที่ดีจะช่วยสร้างความมั่นใจเกี่ยวกับความเพียงพอของ capacity และ resource โดยมีหลักการดังนี้

1. วางแผนเกี่ยวกับ capacity ของระบบ โดยจะต้องคำนึงถึงความต้องการในอนาคต เพื่อให้สามารถรองรับการประมวลผลและการจัดเก็บข้อมูล
2. การยอมรับระบบงาน ในกรณีที่องค์กรได้ทำการพัฒนาระบบขึ้นมาใหม่ ก่อนอื่นระบบนั้นก็จะต้องผ่านการทดสอบเพื่อพิสูจน์ว่าสามารถรองรับการทำงาน และตอบสนองความต้องการได้ โดยจะต้องกำหนดหลักเกณฑ์ในการพิจารณาไว้อย่างชัดเจน ซึ่งได้แก่ การคำนึงทางด้าน performance และ capacity ของเครื่องคอมพิวเตอร์, การกู้ระบบกรณีที่ระบบมีปัญหา หรือเกิดข้อผิดพลาด, การเตรียมการและการทดสอบขั้นตอนการทำงานตามมาตรฐานที่กำหนดไว้ และท้ายสุดจะต้องมีการอบรมเกี่ยวกับการใช้งานระบบใหม่ให้แก่ผู้ที่เกี่ยวข้อง

<u>การรักษาความถูกต้องของ software และข้อมูล</u>

ควรมีมาตรการในการตรวจจับและหลีกเลี่ยงเข้อผิดพลาดเพื่อป้องกัน software ที่จะก่อให้เกิดความเสียหายต่อระบบ โดยอยู่บนพื้นฐานของความปลอดภัย การเข้าถึงระบบอย่างถูกต้อง และการจัดการที่ดี โดยมีหลักการดังนี้

1. กำหนดนโยบายที่สอดคล้องกับ software licenses และข้อห้ามในการใช้งาน
2. กำหนดนโยบายต่อการบริหารความเสี่ยงที่เกิดจากการได้รับข้อมูลผ่าน network
3. ติดตั้ง และ update โปรแกรม anti virus
4. มีการ back up ข้อมูล และ โปรแกรมไว้ เพื่อสามารถกู้คืนกรณีที่ถูก virus ควรมีการ back-up ข้อมูลทางธุรกิจและโปรแกรมการใช้งานเป็นประจำ ซึ่งจะช่วยสร้างความมั่นใจได้ว่าข้อมูลที่สำคัญเหล่านั้นจะถูกกู้คืนได้กรณีที่ระบบมีปัญหา

<u>การจัดการทางด้าน Network</u>

เพื่อสร้างความมั่นใจเกี่ยวกับความถูกต้องของข้อมูลในระบบ Network โดยมีการควบคุมที่ดี และป้องกันการเข้าถึงจากบุคคลภายนอกที่ไม่ได้รับอนุญาต

<u>การจัดการเกี่ยวกับความปลอดภัยและการควบคุมสื่อต่างๆ</u>

เพื่อป้องกันความเสียหายเกี่ยวกับสินทรัพย์และการดำเนินงานทางธุรกิจ วิธีการปฏิบัติงานที่เหมาะสมควรคำนึงถึงการป้องกันเอกสาร อุปกรณ์จัดเก็บข้อมูล (เทป, ดิสก์) ข้อมูลนำเข้า – ข้อมูลผลลัพธ์ และการเข้าถึงข้อมูลของบุคคลภายนอกที่ไม่ได้รับอนุญาต

<u>การจัดการเกี่ยวกับอุปกรณ์จัดเก็บข้อมูล</u>

อาทิเช่น เทป, ดิสก์, และรายงาน มีการควบคุมดังนี้

1. หากข้อมูลที่ถูกจัดเก็บบนสื่อต่างๆ ไม่มีการดึงมาใช้งานอีกต่อไป ควรลบทิ้ง
2. ควรเก็บรักษาสื่อต่างๆ ที่เก็บข้อมูลไว้ในสถานที่ที่ปลอดภัย

<u>การแลกเปลี่ยนข้อมูลและ software</u>

ควรมีการกำหนดแนวทางเพื่อป้องกันความเสียหาย, การเปลี่ยนแปลง และการใช้งานที่ผิดวิธีของข้อมูลที่มีการแลกเปลี่ยนระหว่างองค์กร ซึ่งจะต้องมีการควบคุมที่ดีและต้องสอดคล้องตามที่กฎหมายกำหนด โดยมีหลักการดังนี้

1. ข้อตกลงเกี่ยวกับการแลกเปลี่ยน software และข้อมูล ควรพิจารณาถึงภาระหน้าที่ในการจัดการควบคุมและแจ้งให้รับทราบเกี่ยวกับการส่งผ่านข้อมูล มาตรฐานทางเทคนิคในการส่งข้อมูล การรับผิดชอบกรณีที่ข้อมูลเกิดการสูญหาย

2. ความปลอดภัยของสื่อที่ใช้ส่งข้อมูล วิธีการส่งที่น่าเชื่อถือ มีความถูกต้อง มีการจัดเก็บที่ดีเพื่อป้องกันการถูกทำลาย มีการควบคุมเป็นกรณีพิเศษ อาทิ เช่น การใช้ตู้เก็บ การส่งด้วยมือ การแบ่งส่งข้อมูลตามเส้นทางต่างๆ การใช้ลายมือชื่อดิจิทัล และการเข้ารหัสข้อมูล
3. ความปลอดภัยของพาณิชย์อิเล็กทรอนิกส์ ซึ่งเกี่ยวข้องกับการแลกเปลี่ยนข้อมูลอิเล็กทรอนิกส์ (Electronic Data Interchange: EDI), e-mail, และการทำ transaction ผ่าน network สาธารณะ เช่น Internet จะต้องพิจารณาถึงความถูกต้อง เพื่อสร้างความเชื่อมั่นให้แก่ลูกค้า, การอนุญาต / การให้สิทธิ์ เช่น ผู้ใดมีสิทธิ์ในการกำหนดราคาของสินค้า, ข้อมูลเกี่ยวกับราคา วิธีการชำระเงิน การส่งสินค้า การรับใบเสร็จ ต้องมีความถูกต้องน่าเชื่อถือ
4. ความปลอดภัยของ e-mail เนื่องจาก e-mail ถูกนำมาใช้ในการสื่อสารทางธุรกิจกันอย่างแพร่หลาย ดังนั้นจึงมีความจำเป็นอย่างยิ่งในการควบคุมเพื่อลดความเสี่ยงที่เกิดจากการสื่อสารด้วยวิธีนี้ โดยการกำหนดนโยบายการใช้ e-mail ขึ้นภายในองค์กร เช่น การกำจัดไวรัสที่ติดมา, การปกป้องไฟล์-ข้อมูลที่แนบมากับ e-mail, การให้คำแนะนำว่าเมื่อไหร่ไม่สมควรที่จะใช้ e-mail, ใช้เทคนิคการเข้ารหัส-ถอดรหัสเพื่อเพิ่มความปลอดภัย และความถูกต้อง
5. ความปลอดภัยของระบบสำนักงานอิเล็กทรอนิกส์ ควรมีการกำหนดนโยบายในการควบคุมธุรกิจและความเสี่ยงที่สัมพันธ์กันกับระบบสำนักงานอิเล็กทรอนิกส์ เพื่อเพิ่มโอกาสและความรวดเร็วในการแบ่งปันข้อมูลทางธุรกิจ โดยการนำคอมพิวเตอร์ การสื่อสารไร้สาย, mail, voice-mail, multimedia และอุปกรณ์อำนวยความสะดวกต่างๆ มาใช้
6. การแลกเปลี่ยนข้อมูลในรูปแบบอื่นๆ จะต้องมีการกำหนดขั้นตอนวิธีและการควบคุมข้อมูลที่ถูกส่งผ่านมาตามอุปกรณ์สื่อสารต่างๆ ถ้าหากอุปกรณ์ดังกล่าวไม่สามารถทำงานได้ หรือ ถูกใช้งานมากจนเกินไป อาจส่งผลให้การปฏิบัติงานหยุดชะงัก

การควบคุมการเข้าถึงของข้อมูล

เป็นส่วนที่องค์กรต่างๆ ต้องให้ความสนใจอย่างมาก โดยแต่ละองค์กรควรมีการกำหนดนโยบาย บทบาท กระบวนการจัดการ และมีการควบคุมการเข้าถึงของข้อมูล อย่างชัดเจน เพื่อให้ทุกคนในองค์กรมีความเข้าใจ และเกิดความตระหนักถึงความสำคัญของข้อมูลภายในองค์กร โดยมาตรฐาน BS7799 ได้มีการแบ่งการควบคุมการเข้าถึงของข้อมูลออกเป็น 2 ประเภท คือ การเข้าถึงข้อมูลจากในองค์กร เช่น การใช้ e-mail, การเข้าสู่โปรแกรมต่างๆ ทางคอมพิวเตอร์ขององค์กร และนอกจากนี้ยังมีต้องมีการควบคุมการเข้าถึงข้อมูลจากภายนอกองค์กร โดยผ่านระบบเครือข่ายต่าง ๆ เช่น การใช้ internet เพื่อเข้ามาดึงข้อมูลต่างๆ ภายในองค์กร

การป้องกันผู้ที่ไม่มีอำนาจเข้าถึงข้อมูลนั้น องค์กรควรมีกฎระเบียบที่มีความครอบคลุมทุกขั้นตอนของกระบวนการเข้าถึงข้อมูลของผู้ใช้ โดยเริ่มตั้งแต่การลงทะเบียนผู้ใช้ ตลอดจนถึงกระบวนการยกเลิกสิทธิแก่ผู้ใช้ที่ไม่มีการเข้าถึงข้อมูลและบริการเป็นเวลานาน การลงทะเบียนแก่ผู้ใช้นั้นควรมีการเก็บรายละเอียดที่สำคัญต่างๆ เพื่อให้มีความสะดวกในการตรวจสอบการเข้าถึงข้อมูลของผู้ใช้ได้ในภายหลัง หรือสามารถใช้เป็นหลักฐานได้ โดยรายละเอียดที่ควรจะมีการจัดเก็บได้แก่

รหัสของผู้ใช้ - โดยรหัสของผู้ใช้ในแต่คนนั้นไม่ควรซ้ำกัน เช่นการใช้รหัสประจำตัวของพนักงาน
สิทธิของผู้ใช้ - โดยมีการเก็บว่าผู้ใช้แต่ละคนสามารถเข้ามาทำอะไรกับระบบได้บ้าง เช่น สามารถเข้ามาดูได้เพียงอย่างเดียว หรือ สามารถแก้ไขข้อมูลได้
ระดับการเข้าถึงของข้อมูล - เนื่องจากพนักงานบางคนสามารถเข้าถึงข้อมูลได้แค่บางระดับเท่านั้น ดังนั้นจึงต้องมีการระบุถึงระดับการเข้าถึงของข้อมูล เพราะข้อมูลขององค์กรแต่ละประเภทนั้นมีความสำคัญที่แตกต่างกัน เช่น ข้อมูลทางแผนกบัญชีนั้น บุคคลโดยทั่วไปก็จะไม่ได้รับอนุญาตให้เข้าถึงข้อมูลทางบัญชีขององค์กรได้ เพราะข้อมูลทางการเงินของบริษัทโดยส่วนใหญ่นั้นถือว่าเป็นความลับ

นอกจากนี้ องค์กรควรมีการจัดตั้งหน่วยงานหรือบุคลากรที่มีอำนาจหน้าที่ในการตรวจสอบการใช้ข้อมูลต่างๆ ภายในองค์กร โดยกระบวนการตรวจสอบนั้นควรมีการตรวจสอบอย่างสม่ำเสมอว่ามีรหัสผู้ใช้ที่ซ้ำซ้อนกันหรือไม่ ทำการลบสิทธิ์ในการเข้าถึงข้อมูลหากมีบุคคลใดในองค์กรลาออก ทำการปรับปรุงสิทธิ์ในการเข้าถึงข้อมูลอย่างเหมาะสมหากมีพนักงานภายในองค์กรมีการเปลี่ยนแปลงงานที่ได้รับผิดชอบ และนอกจากนี้การลงทะเบียนผู้ใช้นั้น ผู้ใช้จะต้องมีการเซ็นรับรองลงไปในระเบียบการเพื่อให้ผู้ใช้ได้เข้าใจถึงเงื่อนไขในการเข้าถึงข้อมูล ควรมี log file เพราะ log file สามารถใช้เป็นหลักฐานในเรื่องความปลอดภัยของข้อมูลได้ ดังนั้นจึงมีความจำเป็นที่จะต้องมีการเก็บ log file ที่สำคัญไปยังอีกระบบหนึ่ง และนอกจากนี้ควรมีการปรับนาฬิกาของแต่ละเครื่องคอมพิวเตอร์ให้ตรวจกันเพื่อให้เกิดความมั่นใจในเรื่องความแม่นยำของ log file และง่ายต่อการตรวจสอบ

กระบวนการจัดการในเรื่องรหัสผ่านเพื่อเข้าถึงข้อมูลนั้นควรได้รับการควบคุมและจัดการอย่างเหมาะสม เพราะรหัสผ่านถูกใช้เป็นเครื่องมือในการตรวจสอบว่าบุคคลใดได้ทำการเข้าถึงข้อมูลต่างๆภายในองค์กร ดังนั้น องค์กรควรมีการความรู้ ความเข้าใจ และมีการสร้างจิตสำนึกในเรื่องการเก็บรักษารหัสผ่าน ความสำคัญของรหัสผ่าน โดยผู้ใช้ควรมีการเซ็นรับรองเพื่อเป็นการแสดงการรับทราบว่ารหัสผ่านของแต่ละคนควรเก็บเป็นความลับ สำหรับรหัสผ่านบางประเภทที่มีการใช้เป็นแบบกลุ่มนั้น ก็ควรจะมีแค่กลุ่มของตนเอง

เท่านั้นที่รู้รหัสผ่าน ระบบความมีความยืดหยุ่นที่จะให้ผู้ใช้สามารถทำการปรับเปลี่ยนรหัสผ่านของตนเองได้ โดยในครั้งแรกที่ผู้ใช้ได้รับรหัสผ่านนั้นจะเป็นรหัสผ่านแบบชั่วคราว ซึ่งผู้ใช้จะต้องแก้ไขเป็นรหัสผ่านถาวร โดยทันทีเมื่อมีการเข้าสู่ระบบในครั้งแรก การเก็บรหัสผ่านนั้นไม่ควรเก็บไว้ในระบบคอมพิวเตอร์ที่ไม่ได้มีการป้องกันอย่างเหมาะสม เนื่องจากระบบคอมพิวเตอร์บางระบบผู้ใช้สามารถเข้าสู่ระบบได้โดยง่ายเพราะไม่ต้องใช้รหัสผ่านเป็นต้น การตรวจสอบสิทธิ์ในการเข้าถึงข้อมูลและการบริการต่างๆ ที่องค์กรได้จัดไว้ให้นั้น ควรได้รับการตรวจสอบอยู่เป็นระยะ เช่น ควรมีการตรวจสอบสิทธิในการเข้าถึงข้อมูลทุกๆ 3 เดือน

การสร้างจิตสำนึก ความรับผิดชอบในการใช้งานและการบำรุงรักษารหัสผ่านนั้น องค์กรควรให้คำแนะนำในการบำรุงรักษาและการเก็บรหัสผ่านแก่ผู้ใช้ เช่น ผู้ใช้ควรหลีกเลี่ยงการเขียนรหัสผ่านลงบนกระดาษยกเว้นจะได้รับการรักษาความปลอดภัยเป็นอย่างดี ผู้ใช้ควรมีการเปลี่ยนแปลงรหัสผ่านอยู่สม่ำเสมอ เช่น อาจมีการเปลี่ยนแปลงรหัสผ่านทุกๆ 3 เดือน หรืออาจจะพิจารณาจากความถี่ในการเข้าสู่ระบบ เพราะถ้าผู้ใช้เข้าสู่ระบบเป็นประจำควรมีการเปลี่ยนแปลงรหัสผ่านถี่ขึ้น ซึ่งอาจจะน้อยกว่า 3 เดือนเป็นต้น ควรเลือกใช้รหัสผ่านที่เหมาะสม เช่นควรมีความยาวอย่างน้อย 6 ตัวอักษร และ ง่ายต่อการจดจำ อย่าใช้รหัสผ่านที่ง่ายต่อการคาดเดา เช่น การนำชื่อหรือเบอร์โทรศัพท์มาใช้เป็นรหัสผ่าน พนักงานควรเปลี่ยนรหัสผ่านชั่วคราวโดยทันทีเมื่อมีการ log-on เข้าสู่ระบบเป็นครั้งแรก ไม่ควรใช้วิธีการ log-on โดยอัตโนมัติ เพราะจะทำให้บุคคลอื่นที่มาแอบใช้เครื่องคอมพิวเตอร์สามารถเข้าถึงข้อมูลได้โดยง่าย ไม่ควรให้ผู้อื่นล่วงรู้รหัสผ่านของแต่ละคน ผู้ใช้ควรมีการเอาใจใส่ต่ออุปกรณ์ที่ตนเองใช้อยู่ตลอดเวลา เช่น เมื่อจบการทำงานควร log-off ออกจากระบบโดยทันที ยกเว้นจะได้รับการป้องกันอย่างเหมาะสมเนื่องจากมีการติดตั้งรหัสผ่านในโปรแกรม screen saver เป็นต้น

กระบวนการป้องกันการเข้าถึงข้อมูลโดยผ่านระบบเครือข่ายนั้นควรได้รับการควบคุมการเข้าสู่ระบบเครือข่ายทั้งภายในและภายนอกองค์กรที่เหมาะสม มีกลไกในการมอบอำนาจสำหรับผู้ใช้และอุปกรณ์ และสามารถควบคุมการเข้าสู่การบริการข้อมูลได้ การเชื่อมต่อกับระบบเครือข่ายที่ไม่มีความปลอดภัยจะส่งผลโดยรวมต่อองค์กร เช่นการแพร่ระบาดของไวรัสคอมพิวเตอร์ ซึ่งในปัจจุบันปัญหาไวรัสคอมพิวเตอร์เป็นปัญหาสำคัญที่ทุกๆองค์กรประสบปัญหาอยู่ เพราะไวรัสบางประเภททำให้ข้อมูลภายในองค์กรได้รับความเสียหายและในบางครั้งอาจทำให้ระบบเครือข่ายภายในองค์กรไม่สามารถใช้งานได้ เป็นต้น ดังนั้นผู้ที่เข้าถึงข้อมูลโดยผ่านระบบเครือข่ายได้นั้นควรเป็นผู้ที่ได้รับอำนาจหน้าที่เท่านั้น ที่จะสามารถเข้าสู่ระบบเครือข่ายได้ ซึ่งการควบคุมการเข้าสู่ระบบเครือข่ายเป็นเรื่องที่สำคัญของแต่ละองค์กร และมักจะมีความเสี่ยงสูงหากผู้ใช้เข้าสู่ระบบโดยผ่านระบบเครือข่ายเมื่ออยู่ภายนอกบริษัท ดังนั้นนโยบายควรครอบคลุมถึงกระบวนการป้องกันการเข้าถึงข้อมูลโดยผ่านระบบเครือข่าย และ การบริการของระบบเครือข่ายที่อนุญาตให้สามารถเข้าถึงได้ กระบวนการ

มอบอำนาจนั้นจะต้องมีการระบุว่าบุคคลใดจะเป็นผู้ที่ได้รับอนุญาตในการเข้าสู่ระบบเครือข่าย และการบริการต่างๆบนระบบเครือข่าย มีกระบวนการในการควบคุม และ ระเบียบในการป้องกันการเชื่อมต่อเครือข่าย และการบริการบนระบบเครือข่าย เส้นทางการเชื่อมต่อจากคอมพิวเตอร์ของผู้ใช้ จนถึงการบริการของระบบคอมพิวเตอร์ ต้องได้รับการควบคุม โดยเฉพาะอย่างยิ่งกรณีที่ผู้ใช้ทำการเชื่อมต่อเข้าสู่ระบบเครือข่ายจากภายนอกองค์กร ควรได้รับการควบคุมเช่นกัน เพื่อลดความเสี่ยงที่อาจเกิดขึ้นได้ และป้องกันผู้ใช้ที่ไม่ได้รับอนุญาตไม่สามารถเข้าสู่ระบบเครือข่ายได้ ซึ่งกระบวนการควบคุมนั้นจะขึ้นกับวิธีการในการเข้าสู่ระบบเครือข่าย เพราะการเข้าสู่ระบบเครือข่ายสามารถทำได้หลายวิธีเช่น จากโทรศัพท์ทั่วไป หรือจาก dedicated lines เป็นต้น และควรมีการควบคุมการสื่อสารระหว่างต้นทางและปลายทางโดยผ่าน security gateway เช่น firewall ซึ่งเป็นระบบหนึ่งหรือหลายระบบรวมกันที่สร้างหรือบังคับให้มีเส้นแบ่งเขตระหว่างสองเครือข่ายขึ้นไป เป็น gatewayที่จำกัดการเข้าถึงในเครือข่ายต่างๆ ให้เป็นไปตามนโยบายการรักษาความปลอดภัยของเครือข่ายนั้นๆ โดย firewall ที่ใช้กันโดยทั่วไปมีเป็นเครื่องคอมพิวเตอร์ที่ราคาไม่สูงมากนัก และไม่มีข้อมูลที่สำคัญอยู่จะมีเพียงโมเด็มหรือพอร์ตต่างๆที่เชื่อมต่อกับเครือข่ายภายนอก และมีอีกหนึ่งพอร์ตที่ใช้ในการต่อกลับมายังเครือข่ายภายใน

สำหรับการเชื่อมต่อจากภายนอกบริษัทควรจะมีกลไลในการป้องกันอย่างเหมาะสม เช่น การเข้าสู่ระบบเครือข่ายควรผ่านจาก Diagnostic ports, การใช้ cryptographic techniques (Cryptography เป็นการเข้ารหัสลับ ซึ่งเกี่ยวเนื่องกับหลักการ ตัวกลางและวิธีการในการทำให้ข้อความธรรมดาไม่สามารถถูกอ่านได้ และแปลงข้อความที่ถูกเข้ารหัสลับกลับเป็นข้อความธรรมดา) และการเลือกใช้ฮาร์ดแวร์และซอฟต์แวร์ที่เหมาะสม เพื่อช่วยเพิ่มความแข็งแกร่งในการป้องกันระบบเครือข่าย ควรเลือกอุปกรณ์ฮาร์ดแวร์และซอฟต์แวร์ที่มีคุณภาพ โดยรับการรับรองจากมาตรฐานสากลหรือได้รับการยอมรับอย่างกว้างขวางในวงการคอมพิวเตอร์

การควบคุมการเข้าถึงข้อมูลในระดับของระบบปฏิบัติการ (operating system) สามารถนำมาใช้ในการจำกัดการเข้าใช้ทรัพยากรคอมพิวเตอร์ โดยระบบปฏิบัติการนั้นควรที่จะมีความสามารถที่จะระบุและพิสูจน์ได้ถึงเครื่องคอมพิวเตอร์เครื่องใดที่ทำการเข้าถึงข้อมูลอยู่ เครื่องคอมพิวเตอร์นั้นถูกติดตั้งไว้ที่ใด มีการเก็บบันทึกว่าการเข้าสู่ระบบนั้นสำเร็จหรือล้มเหลว มีการกำหนดระยะเวลาในการเชื่อมต่อของเครื่องคอมพิวเตอร์แต่ละเครื่องเนื่องจากในบางครั้งผู้ใช้อาจลืมที่จะ log-off ออกจากระบบ ทำให้เป็นการเปิดโอกาสให้ผู้ที่ไม่มีสิทธิ์สามารถเข้าถึงข้อมูลได้

การ log-on จากเครื่องคอมพิวเตอร์นั้นควรปฏิบัติตามระเบียบของการ log-on ซึ่งเป็นการป้องกันในเบื้องต้น เพื่อไม่ให้ผู้ใช้ที่ไม่มีสิทธิ์นั้นสามารถเข้าถึงข้อมูลได้ โดยถ้าการเข้าสู่ระบบนั้นไม่ควรแสดงโปรแกรมประยุกต์หรือระบบต่างๆ ทางคอมพิวเตอร์ จนกว่าการ log-on จะเสร็จสมบูรณ์ ควรมีการแสดงข้อความเพื่อแจ้งให้ผู้ใช้ทราบว่า การเข้าถึงข้อมูลจะทำได้เฉพาะผู้ใช้ที่ได้รับสิทธิ์ ไม่ควรแสดงข้อความช่วยเหลือในระหว่างที่ผู้ใช้ทำการ log-on เพราะจะทำให้ผู้ที่ไม่มีสิทธิ์สามารถเข้าสู่ระบบได้ ควรมีการจำกัดจำนวนในกรณีที่ผู้ใช้ใส่รหัสผ่านผิด เช่นถ้าใส่รหัสผิด 3 ครั้งใน 1 วัน รหัสผ่านนั้นจะถูกล็อคโดยทันที

การเชื่อมต่อด้วยอุปกรณ์สื่อสารประเภทไร้สายได้แก่ notebooks, palmtops, laptops และ mobile phones นั้นนโยบายควรได้รับการแก้ไขเพื่อให้เหมาะสมกับความเสี่ยงต่างๆที่อาจเกิดขึ้นได้จากการเชื่อมต่อด้วยอุปกรณ์สื่อสารไร้สายประเภทต่างๆ เช่น นโยบายควรมีการอ้างถึงความจำเป็นในการป้องกันระดับกายภาพ มีการใช้กระบวนการ cryptographic กระบวนการสำรองข้อมูล และการป้องกันไวรัสคอมพิวเตอร์ โดยนโยบายควรมีการอ้างถึงกฎระเบียบ และข้อแนะนำในการเชื่อมต่อด้วยอุปกรณ์ไร้สายต่างๆ

การรักษาความปลอดภัยของข้อมูลนั้นเป็นสิ่งที่มีความสำคัญมาก ดังนั้นควรได้รับความเห็นชอบก่อนที่จะพัฒนาระบบสารสนเทศขึ้นมา โดยการวิเคราะห์ความต้องการในเรื่องความปลอดภัยของระบบนั้น ควรได้รับการพิจารณาในระบบที่เกิดขึ้นใหม่ หรือการขยายระบบจากระบบเดิมที่มีอยู่เพื่อป้องกันความสูญหาย การเปลี่ยนแปลง หรือการใช้งานที่ผิดพลาดของผู้ใช้ ดังนั้นจึงต้องมีการควบคุม และตรวจสอบอย่างเหมาะสม เช่น ข้อมูลที่ผู้ใช้งานใส่ลงไปในระบบควรได้รับการตรวจสอบเพื่อให้เกิดความมั่นใจได้ว่าข้อมูลนั้นเป็นข้อมูลที่ถูกต้องและเหมาะสม มีการสุ่มตรวจจากเอกสารที่ได้รับการใส่เข้าไปในระบบ กำหนดความรับผิดชอบแก่ผู้ใช้ทุกคนที่เกี่ยวข้องกับการใส่ข้อมูลลงไปในระบบ มีการตรวจสอบเพื่อให้เกิดความมั่นใจว่าโปรแกรมได้ทำงานในเวลาที่เหมาะสม เช่นโปรแกรมจะไม่สามารถทำงานได้หากผู้ใช้ยังไม่ log-on เข้าสู่ระบบ มีการตรวจสอบการใช้งานต่างๆ โดยผู้ที่ไม่มีสิทธิ์จะไม่สามารถทำการเปลี่ยนแปลงข้อมูลได้ ซึ่งอาจมีการใช้ฮาร์ดแวร์หรือซอฟต์แวร์ในการรองรับความเป็นตัวตนที่แท้จริงของผู้ใช้ ควรมีการตรวจสอบผลลัพธ์ของข้อมูลที่ได้จากโปรแกรมเพื่อให้เกิดความมั่นใจได้ว่าการทำงานของระบบนั้นได้จัดเก็บข้อมูลได้อย่างถูกต้องและเหมาะสม มีนโยบายในการใช้ cryptographic technique เพื่อให้เกิดความมั่นใจว่าข้อมูลที่เป็นความลับนั้นได้รับการป้องกันอย่างเหมาะสม โดยการใช้ cryptographic technique นั้นเป็นสิ่งที่จำเป็นเพื่อให้ได้รับประโยชน์สูงสุด และลดความเสี่ยงต่างๆ

การจัดทำแผนฉุกเฉิน

เป็นการจัดทำแผนงานเพื่อรองรับเหตุการณ์ในกรณีที่ระบบหรือข้อมูลได้รับความเสียหาย อาทิเช่น ภัยจากธรรมชาติ อุบัติเหตุต่างๆ เครื่องมือเครื่องใช้เสียหาย เป็นต้น เป็นการลดความเสี่ยงและเสริมสร้างความมั่นใจให้แก่องค์กร หัวใจสำคัญก็คือ กระบวนการการจัดทำแผนฉุกเฉิน การวิเคราะห์เหตุการณ์และผลกระทบที่อาจจะเกิดขึ้น ขอบเขตของแผนที่จะรองรับเหตุการณ์ การเขียนแผนและการลงมือปฏิบัติจริง และได้ ทดสอบและปรับปรุงแผนอย่างสม่ำเสมอ

กุญแจสำคัญของกระบวนการการจัดทำแผนฉุกเฉิน คือ รู้จักและเข้าใจถึงความเสี่ยงขององค์กรเป็นอย่างดีในแง่ของความเป็นไปได้และผลกระทบที่อาจจะเกิดขึ้น รวมถึงสามารถอธิบาย แยกแยะ และจัดลำดับตามความสำคัญได้ พิจารณาจัดซื้อประกันอย่างเหมาะสม เขียนกลยุทธ์ที่สอดคล้องกับลำดับความสำคัญและจุดประสงค์ด้านธุรกิจขององค์กร เขียนแผนงานในแต่ละกลยุทธ์ ทดสอบและปรับปรุงแผนรวมถึงกระบวนการที่ใช้ ต้องมั่นใจว่าแผนฉุกเฉินที่จัดทำขึ้นไม่ขัดแย้งกับกระบวนการทำงานและโครงสร้างขององค์กร ระบุหน้าที่ความรับผิดชอบของผู้ที่ได้รับมอบหมายงาน ตลอดจนถึงระบุการจัดการต่างๆ ในกรณีที่เกิดเหตุการณ์รุนแรงขึ้น

การวิเคราะห์แผนฉุกเฉินจะต้องระบุและอธิบายถึงสาเหตุที่เกิดขึ้นโดยละเอียด เช่น ไฟไหม้ น้ำท่วม หรือเครื่องมือได้รับความเสียหาย ตลอดจนถึงการประเมินความเสี่ยงและผลกระทบที่อาจจะเกิดขึ้น (ต้องอยู่ในรูปที่บอกถึงระดับความเสียหายและช่วงเวลาที่จำเป็นจะต้องแก้ไขให้แล้วเสร็จ) โดยได้รับความเห็นชอบจากเจ้าของธุรกิจหรือองค์กร ซึ่งการประเมินนี้จะต้องพิจารณาทุกๆ กระบวนการธุรกิจขององค์กรและผู้บริหารต้องเซ็นรับรอง

ก่อนที่จะวางระบบ จะต้องแน่ใจว่าแผนที่เขียนมานั้นจะสามารถบำรุงรักษาและสามารถกู้ระบบคืนได้ภายในระยะเวลาที่กำหนดไว้ตามความเสียหายแต่ละประเภท สิ่งสำคัญก็คือ ระบุข้อตกลงและรายละเอียดของความรับ ผิดชอบและกระบวนการทั้งหมด ให้ความรู้แก่เจ้าหน้าที่ผู้รับผิดชอบ จัดทำเอกสารประกอบการปฏิบัติงานโดยละเอียด ตลอดจนทดสอบและปรับปรุงแผนการปฏิบัติงานอยู่เสมอ

การบำรุงรักษาและการพัฒนาระบบ

การวางแผนกรอบงานเกี่ยวกับกระบวนการเมื่อเกิดเหตุฉุกเฉินนั้น จะต้องพิจารณาถึงเงื่อนไขที่ต้องทำตามแผน เช่น จะประเมินสถานการณ์อย่างไร มีใครมาเกี่ยวข้องบ้าง เป็นต้น กระบวนการจัดการเมื่อเกิดเหตุการณ์ฉุกเฉินขึ้นจะต้องอธิบายถึงวิธีที่ต้องปฏิบัติตามเกี่ยวกับชีวิตและทรัพย์สิน ซึ่งควรจะบอกเรื่องที่เกี่ยวกับการจัดการที่เกี่ยวข้องกับงานบริการของรัฐด้านต่างๆ ด้วย เช่น ตำรวจ ตำรวจดับเพลิง เจ้าหน้าที่ท้องถิ่นของรัฐบาล เป็นต้น ส่วนการวางแผนกรอบงานเกี่ยวกับกระบวนการย้อนกลับนั้น จะต้องระบุถึงการปฏิบัติการเพื่อย้ายสถานที่ประกอบธุรกรรมขององค์กรชั่วคราว และการย้ายกลับได้ทันเวลาที่ต้องการ การวางกรอบงานเพื่อให้กิจกรรมขององค์กรกลับคืนสู่สภาพเดิม และจัดตารางเวลาในการบำรุงรักษาว่าจะทำอย่างไรและเมื่อไหร่ ตลอดจนถึงการระบุความรับผิดชอบและหน้าที่ของแต่ละคน และผู้ที่จะทำหน้าที่แทนเมื่อคนที่ได้รับมอบหมายนั้นไม่สามารถปฏิบัติหน้าที่ได้

แผนใดๆ ก็ตาม พบว่ามักล้มเหลวได้เสมอหากอยู่บนสมมุติฐานที่ไม่ถูกต้อง หรือปฏิบัติตามในโอกาสที่เปลี่ยนแปลงไป ดังนั้นจึงต้องทดสอบและปรับปรุงแผนให้ทันสมัยอยู่เสมอ ซึ่งการทดสอบแต่ละครั้งสมาชิกและ เจ้าหน้าที่ทั้งหมดจะต้องรับทราบจะปฏิบัติได้จริงในชีวิตประจำวัน ซึ่งการทดสอบนี้เราอาจจะได้หลายรูปแบบ เช่น การจำลองสถานการณ์จริง คือ เป็นการฝึกให้ทุกคนรู้หน้าที่ของตนเองว่าในขณะนั้นควรกระทำอย่างไร การทดสอบการกู้ระบบคืน การทดสอบการกู้ระบบคืนในสิ่งแวดล้อมอื่นๆ ที่ไม่เหมือนเดิม ทดสอบว่าองค์กร คนในองค์กร เครื่องมือเครื่องใช้ และกระบวนการทำงานต่างๆ สามารถรับมือกับเหตุการณ์ฉุกเฉินได้อย่างมีประสิทธิภาพ

อย่างไรก็ตามแผนต่างๆ ที่จัดทำมา ควรตรวจสอบและปรับปรุงประสิทธิภาพอย่างสม่ำเสมอ กระบวนการต่างๆ ควรจัดให้เป็นโปรแกรมการเปลี่ยนแปลงขององค์กรอย่างจริงจัง การแบ่งงานความรับผิดชอบที่มอบหมายให้เจ้าหน้าที่แต่ละคนนั้น ควรปรับปรุงให้เข้ากับแผนที่เปลี่ยนแปลงไป ข้อมูลที่พบว่ามักจะต้องปรับปรุงอยู่เสมอ ได้แก่ ข้อมูลส่วนตัวต่างๆ ที่อยู่หรือเบอร์โทรศัพท์ที่สามารถติดต่อได้ทันที กลยุทธ์ทางธุรกิจขององค์กร สถานที่ทำการ เครื่องมือและทรัพยากรต่างๆ กฎหมาย กระบวนการขั้นตอนการทำงาน ความเสี่ยง เป็นต้น

การหลีกเลี่ยงการกระทำที่อาจก่อให้เกิดการละเมิดต่อทางกฎหมายหรือสัญญา ต้องมีเอกสารหรือประกาศ นโยบายที่ชัดเจนในแต่ระบบของเทคโนโลยีสารสนเทศ โดยระบุเรื่องการนำซอฟต์แวร์ไปใช้ การ

ควบคุม ความรับผิดชอบของแต่ละคน ระเบียบการที่เหมาะสมที่จะนำมาใช้นั้น มีขึ้นเพื่อให้เกิดความมั่นใจว่าเป็นไปตามข้อบังคับทางกฎหมายที่ว่าด้วยเรื่องของทรัพย์สินทางปัญญา ลิขสิทธิ์ เครื่องหมายการค้า ควรพิจารณาจากส่วนต่างๆ ได้แก่ ประกาศเกี่ยวกับซอฟต์แวร์ที่อนุญาตให้ใช้ได้ และซอฟต์แวร์ที่ใช้ไม่ควรละเมิดลิขสิทธิ์ซอฟต์แวร์ เช่น ติดประกาศบนกระดานประกาศข่าวเพื่อให้ทราบโดยทั่วกัน สร้างวินัยให้แก่บุคคลในองค์กร เพื่อให้เกิดความตระหนักในเรื่องลิขสิทธิ์ซอฟต์แวร์ เช่น กำหนดบทลงโทษเมื่อตรวจพบว่ากระทำผิดจากที่ได้ประกาศไว้ จดบันทึก และตรวจสอบในเรื่องผู้รับผิดชอบในด้านลิขสิทธิ์ แผ่นต้นฉบับ และเอกสารที่เป็นคู่มือต่างๆ ควบคุมจำนวนผู้ใช้เพื่อไม่เกินจำนวนลิขสิทธิ์ที่ได้จัดซื้อเอาไว้ ใช้เครื่องมือในการตรวจสอบที่เหมาะสม เป็นต้น

เรื่องการเก็บรักษาข้อมูลขององค์กร จัดเป็นเรื่องสำคัญอีกเรื่องหนึ่งที่ต้องดูแล เนื่องจากในบางครั้งข้อมูลอาจสูญหายได้ ดังนั้นควรจัดแบ่งข้อมูลเป็นประเภทต่าง ๆ เช่นข้อมูลทางบัญชี ข้อมูลที่เป็นธุรกรรม (transaction) เป็นต้น เพื่อจะได้จัดเก็บได้อย่างเหมาะสม และนอกจากนี้ต้องคำนึงถึงวัสดุอุปกรณ์ที่จะนำมาใช้ในการจัดเก็บด้วยเพื่อให้การเข้าถึงเป็นได้โดยง่าย และป้องกันการสูญเสียข้อมูลอันเนื่องมาจากเทคโนโลยีมีการเปลี่ยนแปลง ดูแลรักษาคลังที่จัดเก็บข้อมูลสารสนเทศ ข้อมูลที่สำคัญมากๆ ต้องจัดเก็บและดูแลเป็นพิเศษ เช่น หากข้อมูลที่สำคัญคือข้อมูลส่วนตัวของลูกค้า ก็จำเป็นที่จะต้องจัดตั้งกระบวนการเพื่อจัดเก็บรักษาข้อมูลเป็นพิเศษและทำตามกระบวนการที่ได้จัดตั้งนั้นไว้อย่างเคร่งครัด จะเห็นได้ว่าในหลายๆ ประเทศ มีการใช้ Cryptographic control ซึ่งเป็นเครื่องมือที่ใช้ในการควบคุมการเข้าถึงของข้อมูล ดังนั้นการถ่ายเทข้อมูลผ่านทางด้านฮาร์ดแวร์หรือซอฟต์แวร์ ควรออกแบบให้มีส่วนของ cryptographic เข้าไปด้วย ทั้งนี้จะต้องไม่ขัดต่อกฎหมายของแต่ละประเทศ (กรณีที่มีถ่ายโอนข้อมูลสารสนเทศข้ามประเทศ)

สิ่งที่จำเป็นอย่างยิ่งเมื่อมีผู้ลักลอบเข้าถึงข้อมูลสารสนเทศขององค์กรคือ การรวบรวมหลักฐาน โดยเฉพาะอย่างยิ่งเมื่อการกระทำนั้นเกี่ยวข้องกับกฎหมาย เช่น การโจรกรรมข้อมูล สิ่งสำคัญที่ต้องคำนึงถึงได้แก่ การเก็บรวบรวมหลักฐานให้ได้มากที่สุดไม่ว่าหลักฐานนั้นจะใช้ในศาลหรือไม่ก็ตาม ให้น้ำหนักแก่หลักฐานแต่ละชิ้น นำหลักฐานนั้นมาพิจารณาเพื่อควบคุมมิให้เกิดเหตุการณ์ซ้ำอีกต่อไป เป็นต้น

การปฏิบัติตามกฎระเบียบ

การตรวจสอบในเรื่องนโยบายทางด้านความปลอดภัยเป็นสิ่งสำคัญอีกประเด็นหนึ่งที่ต้องพิจารณา โดยจะต้องหมั่นตรวจสอบนโยบายทางด้านความปลอดภัยของข้อมูลในระบบอยู่เสมอ เพื่อให้เกิดความมั่นใจใน

เรื่องนโยบาย และมาตรฐานของความปลอดภัย ผู้จัดการหรือผู้ที่รับผิดชอบแต่ละส่วนต้องมั่นใจได้ว่าระเบียบในเรื่องความปลอดภัย นั้นได้ปฏิบัติอย่างถูกต้องในพื้นที่ที่ตนรับผิดชอบอยู่ โดยนโยบายและมาตรฐานทางด้านความปลอดภัยของข้อมูลต้องระบุถึงระบบสารสนเทศ ผู้จัดหาระบบ ผู้เป็นเจ้าของสารสนเทศและสินทรัพย์สารสนเทศ ผู้ใช้ และการจัดการ โดยเจ้าของระบบสารสนเทศต้องเป็นผู้ที่ทำการตรวจสอบว่ามีน โยบาย หรือมาตรฐานทางด้านความปลอดภัยในระบบนั้นเหมาะสมหรือไม่เพียงใด นอกจากนี้ต้องมีการตรวจสอบและควบคุมทั้งทางด้านซอฟต์แวร์และฮาร์ดแวร์ด้วย เพื่อให้เกิดการนำไปใช้อย่างถูกต้องและเหมาะสม

การตรวจสอบและพิจารณาระบบนั้นมีขึ้นเพื่อให้เกิดประสิทธิภาพสูงสุดแก่ระบบ สิ่งสำคัญที่จะต้องคำนึงถึงได้แก่ มีการวางแผนอย่างละเอียด และได้รับการเห็นชอบจากผู้ที่มีอำนาจ มีการกำหนดขอบเขตในการตรวจสอบและควบคุม การตรวจสอบนั้นทำได้แค่การอ่านข้อมูลเพียงอย่างเดียว ห้ามทำการแก้ไขข้อมูล มีการจัดทำเอกสารในเรื่องระเบียบขั้นตอน ความต้องการ และความรับผิดชอบ