บทที่ 2
เอกสารและทฤษฎีที่เกี่ยวข้อง

ในปัจจุบันอินเทอร์เน็ตไม่ได้หมายถึงการเชื่อมต่อระบบเครือข่ายเพียงเครือข่ายเดียวอีกต่อไป แต่เป็นการเชื่อมต่อจากทั่วทั้งโลก ที่ซึ่งการเชื่อมต่อจากเครื่องคอมพิวเตอร์สามารถกระทำได้อย่างง่ายดาย โดยอาศัยอุปกรณ์เกตเวย์ (Gateway) อุปกรณ์จัดเส้นทางหรือเราเตอร์ (Router) การเชื่อมต่อหมายเลข (Dialup Connection) และผู้ให้บริการอินเทอร์เน็ต (Internet Service Provider) การเข้าถึงอินเทอร์เน็ตจึงเป็นเรื่องง่ายดายสำหรับทุกคนจากทุกจุดของระบบเครือข่าย โดยไม่ต้องคำนึงถึงข้อจำกัดต่างๆไม่ว่าจะเป็นข้อจำกัดด้านเชื้อชาติ ลักษณะทางภูมิประเทศและเวลา

อย่างไรก็ตามสิ่งที่มาพร้อมกับความสะดวกสบายและความง่ายดายในการเข้าถึงข้อมูลของระบบอินเทอร์เน็ตก็นำมาซึ่งความเสี่ยงใหม่ๆด้วย ได้แก่ ความเสี่ยงในการสูญหาย ลักลอบเปลี่ยนแปลงและถูกขโมยข้อมูลที่มีค่า ไปจนถึงการทำให้ระบบใช้การไม่ได้เนื่องจากข้อมูลต่างๆจะถูกเก็บบันทึกในรูปแบบของแฟ้มข้อมูลอิเล็คทรอนิกส์ที่สามารถเข้าถึงได้จากทุกแห่งบนอินเทอร์เน็ต ซึ่งถือเป็นข้อบกพร่องที่อันตรายมากเมื่อเทียบกับการเก็บบันทึกข้อมูลชุดเดียวกันในรูปแบบของกระดาษหรือเทปแม่เหล็ก ทำให้ผู้บุกรุกไม่จำเป็นต้องเดินเข้าไปในบ้านหรือที่ทำงานเพื่อขโมยข้อมูลที่ต้องการเลย ไม่ต้องเสี่ยงกับการแตะต้องสิ่งของใดๆหรือแม้กระทั่งการถูกบันทึกภาพไว้เป็นหลักฐาน ทั้งยังสามารถซ่อนหลักฐานต่างๆจากการกระทำที่ไม่ได้รับอนุญาตของตนเองจากการตรวจสอบของเจ้าของข้อมูลหรือผู้ดูแลระบบได้

2.1 หลักการพื้นฐานของระบบรักษาความปลอดภัยข้อมูลบนอินเทอร์เน็ต

Marcel Dekker (1997) หลักการพื้นฐานของระบบรักษาความปลอดภัยข้อมูลบนอินเทอร์เน็ตที่ต้องคำนึงถึงมี 3 ประการได้แก่การรักษาความลับ (Confidentiality) ความสมบูรณ์ (Integrity) และความพร้อมใช้งาน (Availability) โดยหลักการทั้งหมดจะเกี่ยวข้องกับการเข้าใช้ข้อมูลของผู้ใช้ 3 ข้อได้แก่ การพิสูจน์ตัวจริง (Authentication) การให้อนุญาต (Authorization) และการห้ามปฏิเสธความรับผิดชอบของผู้ใช้ (Non-repudiation)

การรักษาความลับ หมายถึงการรับรองว่าจะมีการเก็บข้อมูลไว้เป็นความลับ และผู้ที่มีสิทธิ์เท่านั้นจึงจะเข้าถึงข้อมูลนั้นได้ โดยใช้เทคโนโลยีต่างๆเข้ามาช่วยเช่นวิทยาการเข้ารหัสลับ

(Cryptography) ซึ่งพูดถึงการเข้ารหัสถอดรหัสข้อมูล และเป็นพื้นฐานสำคัญของการศึกษาเทคโนโลยีที่ใช้ในทางปฏิบัติจริงเช่น VPN (Virtual Private Network), SSL (Secure Socket Layer) หรือ PKI (Public Key Infrastructure) ซึ่งล้วนแต่ต้องการความรู้ด้านวิทยาการเข้ารหัสลับทั้งสิ้น

ความสมบูรณ์ หมายถึงการรับรองว่าข้อมูลจะไม่ถูกเปลี่ยนแปลงหรือทำลาย ไม่ว่าจะเป็นโดยอุบัติเหตุหรือโดยเจตนาร้าย การส่งข้อมูลผ่านระบบเครือข่ายที่ไม่มีความปลอดภัย เช่นเครือข่ายสาธารณะ อาจทำให้ข้อมูลมีโอกาสถูกดักดูระหว่างทางได้ และเมื่อข้อมูลถูกเปลี่ยนแปลงแก้ไขโดยผู้ที่ไม่ได้รับอนุญาต ข้อมูลนั้นก็จะสูญเสียความถูกต้องไป ถ้าข้อมูลที่มีความสำคัญโดยเฉพาะข้อมูลทางด้านการเงินนั้นถูกเปลี่ยนแปลงแก้ไขจะส่งผลเสียให้กับองค์กรอย่างมากเพราะข้อมูลนั้นจะเชื่อถือไม่ได้อีกต่อไป

ความพร้อมใช้งาน หมายถึงการรับรองว่าข้อมูลและบริการการสื่อสารต่างๆพร้อมที่จะใช้ได้ในเวลาที่จะต้องใช้ เมื่อเราต้องการใช้งานระบบคอมพิวเตอร์แล้ว ระบบต้องมีความสามารถในการรองรับอยู่เสมอ ไม่ใช่ว่าระบบดีบ้างล่มบ้าง หรือเมื่อเกิดปัญหาล่มแล้ว ไม่มีระบบสำรองไว้ใช้งานหรือกว่าจะกู้ระบบได้ก็กินเวลานาน ทำให้เกิดช่วงเวลาเครื่องไม่ทำงาน (Downtime) สูงซึ่งเป็นต้นเหตุทำให้องค์กรหรือธุรกิจของเราติดขัดไม่สามารถดำเนินงานต่อไปได้

ในการอนุญาตการเข้าใช้ข้อมูลได้เฉพาะบุคคลที่ต้องการและไว้ใจได้เท่านั้น เราใช้วิธีการของการพิสูจน์ตัวจริงและการให้อนุญาต

การพิสูจน์ตัวจริง คือกระบวนการพิสูจน์ยืนยันตนเองของผู้ใช้ โดยอาจจะใช้การพิสูจน์โดยบางอย่างที่ผู้ใช้รู้เช่นหรัสผ่าน บางอย่างที่ผู้ใช้มีเช่น บัตรประจำตัว หรือบางอย่างที่สามารถระบุตัวผู้ใช้ได้เองเช่น ลายนิ้วมือ เป็นต้น

การให้อนุญาต คือกระบวนการในการตรวจสอบและพิจารณาว่าผู้ใช้มีสิทธิ์ในการเข้าถึงข้อมูลระดับใด ได้แก่ การอ่าน เขียน หรือสั่งทำงานโปรแกรม

กระบวนการพิสูจน์ตัวจริงและการให้อนุญาตเป็นกระบวนการที่ทำควบคู่กันไป โดยผู้ใช้ต้องยืนยันตัวเองก่อนทำกิจกรรมที่ตัวผู้ใช้เองมีสิทธิ์กระทำได้ ระบบรักษาความปลอดภัยที่ดีจึงต้องเป็นระบบที่ผู้ใช้ไม่สามารถปฏิเสธความรับผิดชอบในการทำกิจกรรมที่ผ่านการยืนยันตัวตนแล้วได้ เรียกว่าการห้ามปฏิเสธความรับผิดชอบของผู้ใช้

2.2 ทำไมจึงต้องสนใจการรักษาความปลอดภัย

เนื่องจากการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาตสามารถกระทำได้อย่างง่ายดาย ภายใต้สภาวะแวดล้อมที่ไม่ปลอดภัยของระบบเครือข่าย และเป็นการยากที่จะจับผู้บุกรุกที่เข้ามา แม้แต่เครื่องคอมพิวเตอร์ที่เราเห็นว่าไม่ได้เก็บข้อมูลหรือทำหน้าที่สำคัญอะไรเลย ก็อาจกลายเป็นจุดอ่อนในการเข้ามายังระบบและเข้าถึงข้อมูลโดยไม่ได้รับอนุญาตก็เป็นได้

การเปิดเผยข้อมูลทั่วไปที่เราเห็นว่าไม่เป็นความลับหรือเป็นอันตรายต่อสาธารณะ ก็อาจถูกใช้โดยผู้บุกรุกเพื่อประโยชน์ในการหาทางเข้ามายังระบบของเราได้ เช่น ข้อมูลเกี่ยวกับฮาร์ดแวร์และซอฟต์แวร์ที่ใช้ การกำหนดค่าต่างๆของระบบ ประเภทของการเชื่อมต่อระบบเครือข่าย กระบวนการในการเข้าถึงและตรวจสอบสิทธิ์การใช้งานระบบ หรือแม้กระทั่งหมายเลขโทรศัพท์ของใช้งานภายในระบบเอง เป็นต้น

หากพิจารณาจากรายงานเหตุการณ์การบุกรุกระบบรักษาความปลอดภัยบนอินเทอร์เน็ตที่ผ่านมาของ CERT Coordination Center (CERT/CC) จะเห็นว่าไม่มีใครบนอินเทอร์เน็ตสามารถหาทางป้องกันได้การบุกรุกเหล่านี้ได้อย่างสมบูรณ์แบบ ทั้งสถาบันการเงิน สถานบันการศึกษา หน่วยงานรัฐบาล หรือแม้แต่บริษัทที่ดำเนินเกี่ยวข้องกับอินเทอร์เน็ตโดยตรงเองก็ตาม

ผลที่ตามมาอาจก่อให้เกิดผลกระทบวงกว้างไม่ว่าจะเป็น การสูญเสียเวลาและค่าชดเชยในการแก้ไขปัญหาที่เกิดขึ้น ผลผลิตลดลง สูญเสียชั่วโมงทำงาน ความน่าเชื่อถือ โอกาสทางธุรกิจ ความสามารถทางการแข่งขัน และอาจรวมถึงความอยู่รอดทางธุรกิจ

2.3 ประวัติและที่มาของปัญหา

อินเทอร์เน็ตได้ถูกสร้างขึ้นมาในปีค.ศ.1969 โดยองค์กรที่เรียกว่า ARPANET ซึ่งเป็นโครงการที่ได้รับเงินสนับสนุนจากองค์กร Advanced Research Projects Agency (ARPA) ของกระทรวงกลาโหมแห่งสหรัฐอเมริกา (U.S. Department of Defense) วัตถุประสงค์อย่างหนึ่งในตอนเริ่มต้นโครงการนี้คือการสร้างระบบเครือข่ายที่สามารถทำงานต่อไปได้แม้ระบบหลักบางส่วนจะใช้งานไม่ได้ก็ตาม ARPANET จึงถูกออกแบบให้สามารถหาเส้นทางในการเชื่อมต่อระบบเครือข่ายได้เองโดยอัตโนมัติเมื่อเกิดปัญหาขึ้น ฉะนั้นจะเห็นได้ว่าระบบอินเทอร์เน็ตในตอนเริ่มต้นจะถูกออกแบบมาให้มีความทนทานต่อการใช้งานในรูปแบบต่างๆ

เช่นเดียวกัน โปรโตคอล (Protocols) ต่างๆบน ARPANET ก็ถูกออกแบบเริ่มต้นมาแบบเปิดกว้างและมีความยืดหยุ่นต่อการใช้งาน แต่ไม่เน้นด้านการรักษาความปลอดภัย เพราะผู้ใช้งานซึ่งมีแต่นักวิจัยในองค์กร ARPA เองต้องการเพียงแค่ความสะดวกในการแบ่งปันและเข้าถึงข้อมูล

โดยปราศจากข้อจำกัดใดๆจากภายในระบบเครือข่าย ซึ่งนับว่าเป็นวิธีการที่เหมาะสม ณ ขณะนั้น แต่ไม่เหมาะกับระบบการใช้งานในปัจจุบันอีกต่อไป

เมื่อมีเครือข่ายคอมพิวเตอร์มาเข้าร่วมในโครงการ ARPANET มากขึ้น ประโยชน์ที่ได้จากการใช้งานบนระบบเครือข่ายก็มากขึ้นตาม เครือข่ายบน ARPANET ส่วนมากประกอบด้วยเครื่องคอมพิวเตอร์จากมหาวิทยาลัยต่างๆและหน่วยงานของรัฐบาล โดยมีโปรแกรมประยุกต์ต่างๆที่ช่วยสนับสนุนการใช้งานบนระบบเครือข่ายเช่น จดหมายอิเล็คทรอนิกส์ (Electronic mail) กลุ่มข่าวสารอิเล็คทรอนิกส์ (Electronic news groups) และบริการการเชื่อมต่อเครื่องคอมพิวเตอร์จากระยะไกล (Remote connection) ในปีค.ศ.1971 มีเครือข่ายกว่า 24 เครือข่ายได้เชื่อมต่อกับ ARPANET นักวิจัยต่างๆเริ่มใช้ประโยชน์ในการแลกเปลี่ยนข้อมูลความรู้กันบนระบบเครือข่ายมากขึ้น และนั่นทำให้ระบบเครือข่ายเริ่มกลายเป็นเครื่องมือสำคัญในการทำการวิจัยร่วมกัน

ต่อมาเริ่มมีการฝ่าฝืนระบบรักษาความปลอดภัยขั้นต่ำกันเองภายในหมู่นักวิจัย โดยเกิดจากคอมพิวเตอร์ที่เชื่อมต่อจากระยะไกล แต่ก็ยังไม่มีใครเชื่อว่าเป็นการบุกรุกเนื่องจากผู้ใช้บน ARPANET ขณะนั้นประกอบด้วยกลุ่มคนไม่มากนัก และทุกคนรู้จักและไว้ใจกัน

ในปีค.ศ.1986 ได้เกิดเหตุการณ์ซึ่งถือว่าเป็นการบุกรุกระบบเครือข่ายระดับนานาชาติขึ้นเป็นครั้งแรก โดยมีการพยายามเชื่อมต่อคอมพิวเตอร์ในสหรัฐอเมริกาโดยผ่านระบบเครือข่าย ARPANET เพื่อขโมยข้อมูลจากเครื่องเหล่านั้น ซึ่งไม่ใช่เพียงแต่จากเครื่องคอมพิวเตอร์ของมหาวิทยาลัยต่างๆเท่านั้น ยังรวมถึงของกองทัพและหน่วยงานรัฐบาลต่างๆด้วย จึงได้มีการแจ้งเตือนภัยที่อาจเกิดขึ้นจากการใช้งานเครือข่าย ARPANET ในทางที่ผิดขึ้น

ในปีค.ศ.1988 ได้เกิดการบุกรุกทางระบบเครือข่ายแบบอัตโนมัติขึ้นเป็นครั้งแรก เรียกว่า "The Morris worm" ซึ่งเกิดจากนักศึกษาในมหาวิทยาลัยคอร์เนล (Ithaca, NY) ชื่อนายโรเบิร์ต ที. มอร์ริส ได้เขียนโปรแกรมขึ้นมาโปรแกรมหนึ่งซึ่งสามารถเชื่อมต่อกับคอมพิวเตอร์เครื่องอื่นโดยทำการค้นหาและใช้ความล่อแหลมของระบบในการสำเนาตัวเองไปยังเครื่องคอมพิวเตอร์เครื่องอื่น แล้วเริ่มทำงานบนเครื่องคอมพิวเตอร์เครื่องที่ติดอีกโดยการค้นหาและส่งโปรแกรมไปยังเครื่องคอมพิวเตอร์อื่นอีกต่อไปแบบอัตโนมัติไปเรื่อยๆ บนเครือข่าย ARPANET ซึ่งโปรแกรมหนอนนี้จะใช้ทรัพยากรของระบบอย่างมากจะทำให้ในที่สุดคอมพิวเตอร์เครื่องนั้นไม่สามารถทำงานได้อีกต่อไป ผลลัพธ์ในครั้งนั้นคือคอมพิวเตอร์ทั่วสหรัฐอเมริกากว่า 10% ที่เชื่อมต่อบน ARPANET หยุดทำงานไปพร้อมๆกัน

ณ เวลานั้นเครือข่าย ARPANET ได้เติบโตขึ้นมากโดยมีคอมพิวเตอร์กว่า 88,000 เครื่องเชื่อมต่ออยู่ เมื่อเกิดเหตุการณ์นี้ขึ้นและเครือข่าย ARPANET เกิดล่มลง จึงเป็นการยากในการร่วมมือ

กันรับมือปัญหา หลายเครือข่ายจึงจำเป็นต้องแยกตัวออกจาก ARPANET เพื่อป้องกันการแพร่ระบาดและเป็นการแก้ปัญหาเพื่อหยุดการทำงานของโปรแกรมหนอนดังกล่าวที่เกิดขึ้น

การเกิดขึ้นอย่างกะทันหันของโปรแกรมตัวหนอน "The Morris Worm" ทำให้องค์กร Defense Advanced Research Projects Agency (DARPA ชื่อใหม่ของ ARPA) ได้ให้ทุนสนับสนุนในการจัดตั้งทีม (ปัจจุบันคือ CERT® Coordination Center) เพื่อเป็นศูนย์กลางแก่ผู้เชี่ยวชาญในการร่วมมือกันจัดการปัญหาที่เกิดขึ้นบนระบบเครือข่าย และได้มีทีมงานในลักษณะนี้เกิดขึ้นอีกมากมายตามองค์กรและภูมิภาคต่างๆ หลังจากนั้นหนึ่งปี ทีมงานเหล่านี้ก็ได้ร่วมกันจัดตั้งองค์กรอย่างไม่เป็นทางการขึ้น รู้จักกันในนามของ Forum of Incident Response and Security Teams (FIRST) เพื่อทำหน้าที่ประสานความร่วมมือในการจัดการปัญหาที่เกิดขึ้นบนระบบเครือข่ายให้ความช่วยเหลือเครือข่ายคอมพิวเตอร์ต่างๆในการรับมือต่อการโจมตีและให้ความรู้แก่ผู้ใช้งานในการดูแลและป้องกันตนเองจากการบุกรุกทางระบบเครือข่าย

ในปีค.ศ.1989 เครือข่าย ARPANET ได้กลายสภาพเป็นอินเทอร์เน็ตอย่างเป็นทางการและเปลี่ยนจากโครงการวิจัยของรัฐบาลมาเป็นระบบเครือข่ายที่มีการใช้งานกันอย่างจริงจัง โดยมีคอมพิวเตอร์ที่เชื่อมต่อกันมากกว่า 100,000 เครื่อง ในขณะที่ปัญหาทางด้านการรักษาความปลอดภัยก็ยังคงดำเนินไปอย่างต่อเนื่องรวมทั้งเทคโนโลยีในการบุกรุกและการป้องกัน ท่ามกลางเหตุการณ์การบุกรุกสำคัญๆ ที่เกิดขึ้นในช่วงนั้น เช่นในปีค.ศ.1989 เกิด WANK/OILZ Worm ซึ่งเป็นการโจมตีแบบอัตโนมัติบนระบบ VMS และรูโหว่บนโปรแกรมแจกฟรีที่มีการใช้งานกันแพร่หลายอย่างโปรแกรม Sendmail ซึ่งทำงานบนระบบปฏิบัติการยูนิกซ์ (Unix) ในการรับและส่งจดหมายอิเล็กทรอนิกส์ ต่อมาในปีค.ศ.1994 เครื่องมือที่ใช้ในการบุกรุกได้พัฒนาสู่การดักดูข้อมูลที่วิ่งอยู่บนระบบเครือข่ายซึ่งสามารถทำได้อย่างง่ายดาย ผลลัพธ์คือการเปิดเผยของข้อมูลบัญชีชื่อผู้ใช้ (Username)และรหัสผ่าน (Password) จากนั้นในปีค.ศ.1995 ด้วยวิธีของการสร้างความสัมพันธ์แบบการเชื่อถือระหว่างกัน (Trust relationship) บนระบบอินเทอร์เน็ต ได้อำนวยประโยชน์แก่การบุกรุกในรูปแบบใหม่ ซึ่งอาศัยประโยชน์จากความสัมพันธ์นี้ในการบุกรุกไปสู่ระบบอื่น จนมาถึงยุคปัจจุบันในการใช้ประโยชน์จากการติดต่อสื่อสารกันบนเครือข่ายใยแมงมุม (World Wide Web) มาสร้างโอกาสในการบุกรุกระบบเครือข่ายแบบใหม่ๆ อีกมากมาย

จากอินเทอร์เน็ตในยุคเริ่มต้นได้ถูกออกแบบมาให้เป็นระบบเครือข่ายเพื่อประโยชน์ในงานวิจัยและการศึกษา แต่ปัจจุบันรูปแบบการใช้งานได้เปลี่ยนไปอย่างสิ้นเชิง อินเทอร์เน็ตได้กลายมาเป็นที่สำหรับความเป็นส่วนตัว การติดต่อในเชิงธุรกิจ และกำลังขยายบทบาทอย่างรวดเร็วไปยังทุกวงการ สิ่งที่คาดหวังว่าจะเกิดต่อไปบนอินเทอร์เน็ตก็คือการเพิ่มขึ้นของความน่าเชื่อถือและการรักษาความปลอดภัย

2.4 ความปลอดภัยบนระบบเครือข่าย

เหตุการณ์เกี่ยวกับความปลอดภัยบนระบบเครือข่ายที่พูดถึงกันมักจะเป็นกิจกรรมที่มีความหมายไปในเชิงลบของการรักษาความปลอดภัย ซึ่งปกติจะหมายถึงกิจกรรมที่เป็นการละเมิดนโยบายรักษาความความปลอดภัย เหตุการณ์เหล่านี้สามารถมาได้ทุกรูปแบบจากทุกหนทุกแห่งบนอินเทอร์เน็ต การบุกรุกที่เกิดขึ้นอาจเกี่ยวข้องเฉพาะเครื่องใดเครื่องหนึ่งไปจนถึงระดับเครือข่ายหลายเครือข่าย โดยมีจุดประสงค์เพื่อให้ได้มาซึ่งบัญชีรายชื่อผู้ใช้งานระบบ สิทธิ์ในการเข้าใช้งานและการใช้เป็นเหยื่อในการโจมตีระบบอื่นต่อไป

การอธิบายลักษณะของบุคคลที่ก่อให้เกิดเหตุการณ์เกี่ยวกับความปลอดภัยบนระบบเครือข่ายเป็นเรื่องยาก ผู้บุกรุกอาจจะเป็นเพียงเด็กหนุ่มที่อยากรู้อยากเห็นบนอินเทอร์เน็ต เด็กนักเรียนที่อยากทดสอบโปรแกรมที่เพิ่งสร้างเสร็จ หรืออาจจะเป็นผู้เชี่ยวชาญด้านระบบรักษาความปลอดภัยบนระบบเครือข่ายเองก็ได้

2.5 ชนิดของเหตุการณ์ละเมิดความปลอดภัยคอมพิวเตอร์และเครือข่าย

2.5.1 การโพรบ (Probe)

เป็นลักษณะของการพยายามที่ผิดปกติในการเข้าสู่ระบบหรือค้นหาข้อมูลเกี่ยวกับระบบ ตัวอย่างเช่นการพยายามเข้าสู้ระบบด้วยชื่อผู้ใช้ที่ไม่มีในระบบ การโพรบจึงเปรียบเสมือนการทดสอบว่าลูกบิดประตูบานไหนไม่ได้ใส่กลอนไว้และเป็นการง่ายต่อการเข้าไปข้างในสิ่งที่ตามมาหลังการโพรบอาจจะก่อให้เกิดความเสียหายอย่างใหญ่หลวงต่อระบบ หรืออาจจะเป็นเพียงแค่ความอยากรู้อยากเห็นเท่านั้นเองก็ได้

2.5.2 การสแกน (Scan)

เป็นลักษณะของการโพรบจำนวนมากโดยการใช้เครื่องมือช่วยแบบอัตโนมัติ จุดประสงค์ของการสแกนก็คือการค้นหาความผิดพลาดต่างๆของระบบ ซึ่งก็คือรูโหว่หรือความล่อแหลมของระบบนั่นเอง และมักจะเป็นสิ่งที่ผู้บุกรุกกระทำก่อนการบุกรุกเข้ามายังระบบตามรูโหว่ที่เจอ

2.5.3 การแอบใช้บัญชีผู้ใช้ทั่วไป (Account Compromise)

เป็นการเข้าใช้งานระบบจากบัญชีผู้ใช้งานที่มีอยู่จริงในระบบแต่ไม่ใช่โดยเจ้าของบัญชีชื่อผู้ใช้งานนั่น ซึ่งถือเป็นการเข้าสู่ระบบที่ไม่ถูกต้อง และทำให้ผู้บุกรุกได้รับสิทธิ์ ในการใช้งานระบบของผู้ใช้รายนั้นไป อาจทำให้เกิดการสูญเสีย การขโมย แก้ไขดัดแปลงข้อมูล หรือการขโมยบริการที่ผู้ใช้มีสิทธิ์ได้รับไป และมักจะเป็นจุดเริ่มต้นที่ผู้บุกรุกใช้ในการเข้าสู่ระบบในระดับสูงขึ้นต่อไป

2.5.4 การแอบใช้บัญชีผู้ใช้ผู้ดูแลระบบ (Root Compromise)

คล้ายกับ Account Compromise เพียงแต่บัญชีรายชื่อของผู้ใช้รายนั้นเป็นของผู้ที่มีสิทธิ์พิเศษในการใช้งานระบบ ซึ่งอาจจะเป็นของผู้ดูแลระบบเอง เช่น root เป็นบัญชีผู้ใช้งานในระบบยูนิกซ์ ซึ่งมีสิทธิ์ในการใช้งานแบบไม่มีข้อจำกัดใดๆทั้งสิ้น ผู้บุกรุกที่สามารถได้สิทธิ์ของรูตมาจะสามารถทำทุกสิ่งทุกอย่างบนระบบที่ตกเป็นเหยื่อได้ ไม่ว่าจะเป็นสั่งทำงานโปรแกรม เปลี่ยนสิทธิ์การใช้งานของผู้ใช้ต่างๆ เปลี่ยนการทำงานของระบบ และทำลายหลักฐานการแอบเข้าสู่ระบบของตนได้

2.5.5 การดักดูข้อมูล (Packet Sniffer)

เป็นโปรแกรมที่ใช้ในการดักดูข้อมูลที่วิ่งอยู่บนระบบเครือข่าย ซึ่งข้อมูลนั้นประกอบด้วยชื่อผู้ใช้ รหัสผ่าน และค่าต่างๆที่ใช้ในการติดต่อสื่อสารระหว่างกันบนระบบเครือข่าย ซึ่งจะเป็นอันตรายมากถ้าข้อมูลนั้นอยู่ในรูปแบบของตัวอักษรอย่างชัดเจนที่ไม่ได้มีการเข้ารหัสข้อมูลก่อนการส่ง โปรแกรมประเภทนี้ถือเป็นโปรแกรมต้องห้ามบนระบบเครือข่ายถ้าผู้ใช้ใช้อย่างไม่ถูกวิธี ฉะนั้นถ้าระบบเครือข่ายใดมีโปรแกรมประเภทนี้ทำงานอยู่โดยไม่ได้รับอนุญาต ก็อาจหมายถึงระบบนั้นถูกแอบใช้บัญชีผู้ใช้ผู้ดูแลระบบแล้วก็เป็นได้

2.5.6 การทำให้ระบบทำงานผิดพลาด (Denial of Service)

จุดประสงค์ของการบุกรุกแบบนี้ไม่ใช่เพื่อให้ได้มาซึ่งสิทธิ์ในการเข้าใช้งานระบบหรือข้อมูลที่ต้องการ แต่เป็นการทำให้ระบบไม่สามารถทำงานหรือให้บริการแก่ผู้ใช้ได้ตามปกติ ซึ่งสามารถบุกรุกเข้ามาได้หลายรูปแบบ โดยอาจจะส่งข้อมูลจำนวนมหาศาล (Flooding) เข้ามาในระบบ หรือทำบางอย่างเพื่อใช้ทรัพยากรที่มีอยู่จำกัดของระบบให้หมดไปเช่น การเปิดการเชื่อมต่อระบบเครือข่ายทิ้งไว้จำนวนมาก เป็นต้น บางครั้งการบุกรุกยังใช้เพื่อรบกวนส่วนต่างๆบนระบบเครือข่ายเพื่อทำลายกระบวนการส่งผ่านข้อมูลด้วย

2.5.7 การใช้ประโยชน์จากการเชื่อถือระหว่างกัน (Exploitation of Trust)

เครื่องคอมพิวเตอร์บนระบบเครือข่ายมักจะอาศัยความสัมพันธ์แบบการเชื่อถือระหว่างกัน ในการพิจารณาการอนุญาตให้สิทธิ์ในการเข้าใช้งานระบบหรือเข้าถึงข้อมูล ซึ่งถ้าผู้บุกรุกรู้ความสัมพันธ์นี้และทำการปลอมตัวเองเป็นเครื่องคอมพิวเตอร์ที่ได้รับความไว้วางใจนั้นก็จะสามารถได้รับสิทธิ์ในการเข้าถึงระบบนั้นด้วย

2.5.8 การใช้โค้ดที่มีจุดประสงค์ร้าย (Malicious Code)

ในเทอมปกติเราจะหมายถึงโปรแกรมที่ซึ่งเมื่อถูกสั่งให้ทำงานจะให้ผลลัพธ์ที่ไม่พึงประสงค์แก่ระบบ โปรแกรมประเภทนี้ได้แก่ม้าโทรจัน (Trojan horse) ไวรัส (Virus) และหนอน (Worm)

โปรแกรมม้าโทรจันและไวรัสมักจะถูกซ่อนตัวอยู่ในส่วนหนึ่งของโปรแกรมปกติ เพื่อให้ทำบางอย่างที่นอกเหนือไปจากจุดประสงค์หลักของโปรแกรม ส่วนโปรแกรมหนอนเป็นโปรแกรมที่มีความสามารถในการจำลองและแพร่กระจายตัวเองไปยังเครื่องอื่นได้โดยไม่ต้องอาศัยกิจกรรมของมนุษย์ช่วย ในขณะที่โปรแกรมไวรัสก็เป็นโปรแกรมที่สามารถจำลองตัวเองได้ แต่ต้องอาศัยกิจกรรมบางอย่างของมนุษย์ช่วยในการแพร่กระจายไปยังเครื่องอื่น ผลลัพธ์ของโปรแกรมเหล่านี้จะนำมาซึ่งการสูญเสียของข้อมูล ระบบทำงานบกพร่อง และการบุกรุกอื่นๆอีกต่อไป

2.5.9 การโจมตีโครงสร้างพื้นฐานของระบบเครือข่าย (Internet Infrastructure Attacks)

เป็นการบุกรุกที่ไม่ค่อยเกิดขึ้นบ่อยแต่เกิดผลกระทบที่รุนแรงมาก โดยมุ่งโจมตีส่วนประกอบหลักบนโครงสร้างพื้นฐานของระบบเครือข่ายมากกว่าระบบใดระบบหนึ่งบนอินเทอร์เน็ต เช่นเซิร์ฟเวอร์ชื่อโดเมน (Domain Name Servers) ผู้บริการบริการเชื่อมต่อระบบเครือข่าย (Network access providers) หรือเครือข่ายที่มีผู้ใช้งานจำนวนมากๆ ผลกระทบของการโจมตีจะแผ่ขยายเป็นวงกว้างอย่างรวดเร็วต่อระบบเครือข่ายโดยรวมทั้งหมด

2.6 แนวโน้มการบุกรุกบนระบบเครือข่าย

สมัยก่อนรูปแบบการบุกรุกบนระบบเครือข่ายจะเป็นในรูปแบบค่อนข้างตรงไปตรงมา โดยผู้บุกรุกมักจะอาศัยประโยชน์จากจุดที่อ่อนแอของระบบเอง เช่นการตั้งรหัสผ่านอย่างง่ายๆ การปรับแต่งระบบอย่างผิดๆ หรือจุดบกพร่องในโปรแกรม (bugs) ที่คอยให้บริการต่างๆของระบบเอง ต่างก็เป็นตัวการสู่การบุกรุกเข้ายังระบบทั้งสิ้น

ผู้ขายก็มักจะส่งเครื่องที่พร้อมใช้งานแต่ไม่มีการปรับแต่งค่าใดๆของระบบ ซึ่งง่ายต่อการบุกรุกเข้ามายังระบบอย่างยิ่ง การปรับแต่งระบบให้มีความปลอดภัยจึงเป็นหน้าที่ของผู้ดูแลระบบเอง ปัญหาที่ตามก็คือผู้ดูแลระบบนั้นไม่มีเวลา ไม่มีความรู้ความชำนาญในการปรับแต่งระบบตลอดจนขาดแคลนเครื่องมือในการตรวจสอบและเตือนภัยจากการบุกรุกเข้ามายังระบบ

จะเห็นได้ว่าการบุกรุกสมัยก่อนยังมีรูปแบบที่ไม่ซ้ำซ้อนหรือมีความชำชองมากเท่าปัจจุบัน ตามรายงานของ CERT Coordination Center ได้แสดงว่าผู้บุกรุกได้มีการพัฒนาความรู้และเทคโนโลยีใหม่ๆในการใช้ประโยชน์จากความล่อแหลมต่างๆของระบบมากขึ้น ในขณะเดียวกันผู้บุกรุกรายใหม่ที่มีความรู้น้อยก็เริ่มมีบทบาทมากขึ้นจากการแบ่งปันความรู้และเครื่องมือจากผู้บุกรุกรายเก่าที่มีความรู้ความสามารถและชำชองมากกว่านั่นเอง

รายงานจาก CERT Coordination Center ได้ระบุแนวโน้มการบุกรุกบนระบบเครือข่ายไว้ดังนี้

แนวโน้มที่ 1 ความเร็วในการบุกรุกเพิ่มขึ้น

1.) การตรวจสอบความเป็นไปได้ของเป้าหมาย

การตรวจสอบระบบโดยการสแกน เริ่มแพร่หลายมาตั้งแต่ปีค.ศ.1997 จนกระทั่งถึงปัจจุบัน มีเครื่องมือที่ช่วยอำนวยความสะดวกในการตรวจสอบระบบอย่างมีประสิทธิภาพได้อย่างรวดเร็วอยู่อย่างมากมาย

2.) การใช้ประโยชน์จากความล่อแหลมของระบบ

เมื่อก่อนการบุกรุกเข้าระบบโดยการใช้ประโยชน์จากความล่อแหลมของระบบจะกระทำได้หลังจากได้ทำการตรวจสอบระบบเสร็จแล้ว แต่ปัจจุบันเครื่องมือที่ช่วยในการบุกรุกเข้าระบบโดยวิธีนี้ได้ร่วมเป็นส่วนหนึ่งอยู่ในการตรวจสอบระบบแล้ว ทำให้ความเร็วในการบุกรุกเข้าสู่ระบบเพิ่มขึ้นเป็นสองเท่า

3.) การแพร่กระจายของการบุกรุก

การบุกรุกในสมัยก่อนจำเป็นต้องอาศัยคนในการเริ่มต้นการบุกรุกในครั้งต่อไป แต่ปัจจุบันมีการบุกรุกสามารถสร้างวงจรในการบุกรุกต่อไปได้ด้วยตัวเอง เช่นโปรแกรมตัวหนอน Code red, Nimda และ Slammer อันโด่งดังที่สามารถกระจายตัวไปสร้างความเสียหายทั่วโลกได้ภายในเวลาไม่ถึง 18 ชั่วโมง

4.) ความร่วมมือในการจัดการเครื่องมือที่ใช้บุกรุก

ตั้งแต่ปีค.ศ.1999 ที่ได้มีการแพร่กระจายเครื่องมือต่างๆที่ใช้การบุกรุก ทำให้บรรดาผู้บุกรุกสามารถหาและใช้ประโยชน์จากเครื่องมือเหล่านั้นได้อย่างมากมายบนอินเทอร์เน็ต มาถึงในปัจจุบันเครื่องมือที่มีแพร่กระจายยังมีความสามารถที่สูงขึ้นในการโจมตีแบบ Denial of service การตรวจสอบระบบ และการใช้ประโยชน์จากความล่อแหลมของระบบ

แนวโน้มที่ 2 เทคโนโลยีที่ใช้ในการบุกรุกซับซ้อนมากขึ้น

ผู้บุกรุกได้แสดงออกถึงการเพิ่มขึ้นของความรู้ทางด้านเทคโนโลยีโครงสร้างระบบเครือข่าย และกลไกการทำงานของโปรโตคอลต่างๆอยู่อย่างตลอดเวลา

การตรวจสอบการบุกรุกจึงเป็นเรื่องที่ยากขึ้นกว่าเดิม โดยเฉพาะเครื่องมือตรวจจับที่ใช้วิธีอ้างอิงจากรูปแบบการบุกรุก (Signature-based) เช่นโปรแกรมแอนตี้ไวรัสและระบบตรวจสอบผู้บุกรุก โดยการบุกรุกเหล่านี้มีลักษณะที่สำคัญอยู่ 3 ประการได้แก่

1.) พยายามหลีกเลี่ยงการถูกตรวจจับ (Anti-forensics)

ผู้บุกรุกจะใช้เทคนิคต่างๆทำให้กระบวนการบุกรุกดูซับซ้อนและยุ่งเหยิง ซึ่งการวิเคราะห์ตรวจจับจะทำได้ยากและต้องใช้เวลามากขึ้นในการทำความเข้าใจกับรูปแบบการบุกรุกใหม่ๆที่ถูกพัฒนาออกมาอยู่ตลอดเวลา

2.) พฤติกรรมพลวัต (Dynamic behavior)

จากรูปแบบพฤติกรรมการบุกรุกในสมัยก่อนที่เป็นลำดับอันแน่นอนตามที่ได้กำหนดไว้ เปลี่ยนมาเป็นรูปแบบพฤติกรรมที่หลากหลายและสามารถเปลี่ยนแปลงได้

3.) เครื่องมือที่ใช้ในการบุกรุกแยกเป็นส่วนจำเพาะ (Modularity of attack tools)

จากสมัยก่อนเครื่องมือในการบุกรุกจะถูกออกแบบมาเพื่อการบุกรุกในรูปแบบใดรูปแบบหนึ่งเท่านั้น แต่ปัจจุบันเครื่องมือเหล่านี้ได้ถูกออกแบบให้แยกเป็นส่วนๆ (Modular) ทำให้สามารถรองรับการปรับเปลี่ยนการใช้งานได้อย่างรวดเร็ว หลากหลายและมีประสิทธิภาพมากขึ้น

แนวโน้มที่ 3 การค้นพบความล่อแหลมต่างๆได้เร็วขึ้น

จากการใช้ประโยชน์จากความล่อแหลม (Vulnerability) ของระบบที่เป็นที่รู้จักดีไปสู่สำรวจรหัสต้นฉบับ (Source code) ของโปรแกรมเพื่อค้นหาจุดอ่อน โดยเฉพาะโปรแกรมประเภทรหัสเปิด (Open source) ซึ่งเป็นโปรแกรมที่ใช้กันอย่างแพร่หลายในปัจจุบัน เพราะมีการแจกฟรี สามารถหาได้ทั่วไปบนอินเทอร์เน็ต และมักมีการแจกซ้อสโค้ดมาพร้อมกับโปรแกรมด้วย

และเนื่องจากปกติจุดประสงค์หลักของการเขียนโปรแกรมหนึ่งๆจะอยู่ที่เพื่อต้องการให้โปรแกรมนั้นสามารถทำงานได้อย่างที่ต้องการด้วยประสิทธิภาพที่ดีเยี่ยมเท่านั้น โดยมีการคำนึงถึงเรื่องความปลอดภัยหรือการใช้งานโปรแกรมแบบผิดๆน้อยมาก บวกกับความรู้ความชำนาญที่เพิ่มขึ้นของผู้บุกรุก จึงเป็นเหตุผลหนึ่งที่ทำให้เกิดการค้นพบจุดล่อแหลมต่างๆในระบบอยู่เสมอ

จากรายงานการค้นพบจุดล่อแหลมต่างๆของ CERT Coordination Center ได้เพิ่มขึ้นในทุกๆปี และผู้บุกรุกมักจะเป็นคนที่ค้นพบจุดล่อแหลมเหล่านี้ได้ก่อนเจ้าของโปรแกรมด้วย ฉะนั้นจึงเป็นการยากสำหรับผู้ดูแลระบบในการคอยติดตามปิดรูโหว่เหล่านั้น

แนวโน้มที่ 4 การรั่วไหลผ่านระบบรักษาความปลอดภัยหรือไฟร์วอลล์มีมากขึ้น

ระบบรักษาความปลอดภัย(Firewall)มักจะถูกใช้เป็นด่านแรกในการป้องกันภัยจากบรรดาผู้บุกรุกระบบเครือข่าย แต่อย่างไรก็ตามยังมีเทคโนโลยีบางตัวที่ถูกออกแบบมาให้

สามารถทะลุผ่าน(Bypass) ระบบรักษาความปลอดภัยที่มีการกำหนดค่า(Configuration)แบบปกติได้ เช่น IPP (the Internet Printing Protocol) และ WebDAV (Web-based Distributed Authoring and Versioning) เป็นต้น หรือพวก Mobile-code อย่าง ActiveX controls, Java และ Java Script ต่างก็อาจเป็นตัวทำให้เกิดอันตรายต่อระบบได้

แนวโน้มที่ 5 ความหลากหลายในการบุกรุกเพิ่มขึ้น

ระบบแต่ละระบบบนอินเทอร์เน็ตต่างเปิดโอกาสให้ถูกบุกรุกเข้ามาได้ทั้งสิ้น ด้วยความก้าวหน้าของเทคโนโลยีทางการบุกรุก ยิ่งความเร็วในการบุกรุกและความซับซ้อนในการบุกรุกเพิ่มขึ้นเท่าใด ธรรมชาติของการบุกรุกก็จะยิ่งหลากหลายมากขึ้นเท่านั้น

แนวโน้มที่ 6 ภัยจากการคุกคามโครงสร้างพื้นฐานระบบเครือข่ายเพิ่มขึ้น

การโจมตีส่วนประกอบหลักบนโครงสร้างพื้นฐานของระบบเครือข่ายมีผลกระทบต่อส่วนต่างๆในอินเทอร์เน็ตเป็นวงกว้าง ยิ่งมีการเพิ่มขึ้นของเครือข่ายและผู้ใช้บนอินเทอร์เน็ตมากขึ้นเท่าใด ผลกระทบของมันก็มากขึ้นเท่านั้น

2.7 ความล่อแหลมบนอินเทอร์เน็ต (Internet Vulnerabilities)

ความล่อแหลมที่เราพูดถึงในที่นี้ก็คือจุดอ่อนหรือรูโหว่ที่เปิดโอกาสให้ใครคนใดคนหนึ่งสามารถใช้ประโยชน์ในการกระทำการใดการหนึ่งได้สำเร็จโดยไม่ได้รับอนุญาตหรือไม่ถูกต้องตามกฎการใช้งานของระบบหรือเครือข่ายนั้น เมื่อความล่อแหลมนั้นได้ถูกใช้ประโยชน์อย่างผิดๆในการบุกรุกเข้ามายังระบบหรือข้อมูลของระบบ ผลลัพธ์ที่ตามมาก็คือการเกิดเหตุการณ์ที่ไม่ปลอดภัยต่อระบบขึ้นนั่นเอง

2.7.1 ทำไมจึงอินเทอร์เน็ตจึงเปราะบางต่อการถูกบุกรุก

เริ่มจากโปรโตคอลที่ใช้กันบนอินเทอร์เน็ตในปัจจุบันนั้นพัฒนามาจากโปรโตคอลบนระบบเครือข่ายในสมัยที่ยังเป็น ARPANET ซึ่งถูกออกแบบมาโดยไม่ได้คำนึงถึงระบบความปลอดภัย เมื่อโครงสร้างปราศจากพื้นฐานความปลอดภัย การป้องกันจึงเป็นเรื่องยาก ยิ่งไปกว่านั้นอินเทอร์เน็ตยังเต็มไปด้วยสภาวะแวดล้อมที่เปลี่ยนแปลงอยู่ตลอดเวลา ทั้งทางด้านรูปแบบการเชื่อมต่อและเทคโนโลยีที่เกิดใหม่อย่างรวดเร็ว

ด้วยคุณสมบัติในการเปิดกว้างและการออกแบบโปรโตคอลที่ติดตัวมาจากยุคเริ่มต้นของอินเทอร์เน็ต ทำให้อินเทอร์เน็ตถูกบุกรุกได้อย่างรวดเร็ว ง่ายดาย ไม่แพง และยังยากต่อการตรวจจับและแกะรอยด้วย ผู้บุกรุกไม่จำเป็นต้องแสดงตัวทางกายภาพในการบุกรุก พวกเขา

สามารถเริ่มต้นการบุกรุกได้จากทุกแห่งที่เชื่อมต่ออินเทอร์เน็ตบนโลก และซ่อนแหล่งที่มาได้อย่างง่ายดาย

ปัจจุบันยังมีเครือข่ายอีกหลายแห่งบนอินเทอร์เน็ตที่ไม่ระวังหรือไม่ให้ความสนใจทางด้านระบบความปลอดภัยมากเท่าที่ควร เช่น ผู้ดูแลระบบเหล่านั้นมักจะไม่สนใจว่ามีอะไรเกิดขึ้นกับข้อมูลและระบบของตนตราบเท่าที่ระบบยังสามารถให้บริการได้ ไม่เชื่อว่าระบบของตนจะตกเป็นเป้าหมายในการบุกรุกเนื่องจากไม่ได้ให้บริการหรือเก็บข้อมูลที่สำคัญไว้ หรืออาจจะคิดว่าการป้องกันระบบของตนดีเพียงพอแล้ว ซึ่งในความเป็นจริงที่เทคโนโลยีมีการเปลี่ยนแปลง ผู้บุกรุกก็มีการพัฒนาเครื่องมือและเทคโนโลยีใหม่ๆอยู่เสมอเช่นกัน ฉะนั้นจึงไม่มีการป้องกันใดที่ดีที่สุดและยังคงประสิทธิภาพในการป้องกันได้ตลอดไป

และยังมีการส่งข้อมูลจำนวนมากบนอินเทอร์เน็ตที่ไม่อยู่ในรูปของการเข้ารหัส การรักษาความลับและความจริงแท้ของข้อมูลจึงเป็นเรื่องยาก ซึ่งไม่เพียงเป็นอันตรายต่อระบบที่เกี่ยวกับการเงิน ยังเป็นอันตรายต่อกระทั่งกลไกการทำงานพื้นฐานของระบบด้วย ได้แก่การพิสูจน์ยืนยันตนเองและการห้ามปฏิเสธความรับผิดชอบของผู้ใช้ ผลลัพธ์ที่ตามมาคือระบบของเราอาจจะถูกละเมิดความปลอดภัยจากเครือข่ายอื่นที่อยู่นอกเหนือการควบคุมได้ ตัวอย่างเช่นมีโปรแกรมประเภท Packet Sniffer คอยดักดูข้อมูลอยู่บนเครือข่ายหนึ่ง ทำให้ผู้บุกรุกสามารถดักดูข้อมูลของเครือข่ายอื่นที่ส่งผ่านเครือข่ายนี้ได้

เหตุผลอีกประการที่อินเทอร์เน็ตเปราะบางต่อการถูกบุกรุกคือการเติบโตและการใช้งานที่เพิ่มขึ้นอย่างรวดเร็ว ซึ่งมาพร้อมกับการใช้งานบริการต่างๆที่ซับซ้อนมากมายบนอินเทอร์เน็ต และที่สำคัญคือบ่อยครั้งที่บริการต่างๆเหล่านี้มักจะไม่ได้รับการออกแบบ ตั้งค่า หรือมีการดูแลด้านระบบความปลอดภัยเลย การรีบเร่งผลิตสินค้าออกสู่ตลาดก็อาจเป็นเหตุให้ผู้พัฒนาไม่มีเวลาพอในการทดสอบหรือตรวจหาข้อผิดพลาดที่อาจนำไปสู่การเป็นความล่อแหลมของระบบในอนาคตได้

ประกอบกับปัญหาด้านการทำธุรกิจ ผู้ค้ามักจะขายของตามความต้องการของลูกค้าคือง่ายต่อการใช้ บำรุงรักษา ให้คำแนะนำและถูก ผลก็คือการทำให้ใช้งานง่ายมักไปไม่ได้กับการทำให้ระบบมีความปลอดภัย เพราะผู้ใช้ไม่ต้องการติดตั้งหรือกำหนดค่าอะไรเพิ่มเติมอีกหลังจากการติดตั้งและระบบสามารถใช้งานได้ตามความต้องการแล้ว

ทำให้ในที่สุดแล้วการเติบโตขึ้นของอินเทอร์เน็ตได้เพิ่มความต้องการทางด้านการจัดการระบบรักษาความปลอดภัยไปด้วย ผู้เชี่ยวชาญทางด้านระบบรักษาความปลอดภัยจึงเป็นที่ต้องการสูง แต่ไม่เพียงพอต่อความต้องการของตลาด บุคลากรที่ยังขาดประสบการณ์ทางด้านนี้จึง

ถูกดึงขึ้นมาแทน และทำหน้าที่เปิดหน้าต่างรอให้ผู้บุกรุกตรวจพบเจอและบุกรุกเข้ามาสู่ระบบโดยไม่รู้ตัว

2.7.2 สาเหตุที่ทำให้ผู้บุกรุกสามารถเข้ามายังระบบ

Robert Graham (2000)ได้แบ่งสาเหตุที่ทำให้ผู้บุกรุกสามารถเข้ามายังระบบไว้ดังนี้

2.7.2.1 บั๊กของซอฟต์แวร์ (Software bugs)

บั๊กของซอฟต์แวร์มีอยู่ในทั้งเดมอนของเซิร์ฟเวอร์ แอพลิเคชันของไคลเอนต์ ระบบปฏิบัติการ และระดับของโปรโตคอลที่ใช้บนระบบเครือข่าย โดยสามารถแบ่งประเภทได้ดังนี้

- บัฟเฟอร์โอเวอร์โฟล (Buffer Overflows) รูโหว่เกี่ยวกับระบบความปลอดภัยที่ตรวจพบเจอในปัจจุบัน ส่วนมากมาจากปัญหา Buffer Overflows ทั้งสิ้น ตัวอย่างเช่น ผู้พัฒนาโปรแกรมคนหนึ่งกำหนดขนาดตัวแปรในการเก็บชื่อผู้ใช้งานระบบไว้ 256 ตัวอักษร ซึ่งผู้พัฒนาระบบคิดว่าไม่มีใครที่จะตั้งชื่อยาวขนาดนั้นแน่ แต่บรรดาผู้บุกรุกไม่คิดอย่างนั้น อะไรจะเกิดขึ้นถ้าเขาใส่ชื่อผู้ใช้งานปลอมที่ยาวกว่า 256 ตัวอักษรเข้าไป? ตัวอักษรที่เกินมาจะไปไหน? ถ้าทำอย่างถูกวิธี ผู้บุกรุกจะสามารถส่งตัวอักษร 300 ตัวอักษร ซึ่งรวมโค้ดที่จะส่งไปทำงานที่เครื่องเซิร์ฟเวอร์และในที่สุดก็จะสามารถเข้ามายังระบบได้ บรรดาผู้บุกรุกสามารถหาข้อบกพร่องเหล่านี้ได้หลายวิธี เช่นหนึ่ง ค้นหาจากซ้อสโค้ดของโปรแกรมประเภทโอเพนซอสที่มีอยู่มากมายบนอินเทอร์เน็ต สอง อ่านจากเอาท์พุตของโปรแกรมเป็นแอสเซมบลีซึ่งยากกว่าวิธีแรก และสามตรวจสอบจากทุกอินพุตของโปรแกรมและพยายามโอเวอร์โฟลด้วยค่าข้อมูลแบบสุ่ม ซึ่งปัญหาแบบนี้มักจะพบได้ทั่วไปในโปรแกรมที่เขียนด้วยภาษา C หรือ C++ แต่ไม่ค่อยพบในโปรแกรมที่เขียนด้วยภาษา Java

- การส่งคำสั่งที่มีลักษณะการบุกรุก (Unexpected combinations) ในหลายโปรแกรมมักจะมีการสร้างโค้ดไว้หลายชั้น โดยวางชั้นที่เป็นส่วนของระบบปฏิบัติการไว้ที่ชั้นล่างสุด ซึ่งผู้บุกรุกสามารถส่งอินพุตที่ไม่มีความหมายสำหรับการทำงานชั้นหนึ่งแต่มีความหมายสำหรับการทำงานในชั้นอื่นได้ เช่นการทำงานในส่วนรับอินพุตบนเว็บโดยใช้ภาษา Perl ซึ่งปกติจะมักจะมีการส่งอินพุตที่รับเข้ามาไปทำงานต่อยังโปรแกรมในส่วนอื่นต่อ จึงเป็นเทคนิคที่ผู้บุกรุกใช้ได้เช่นกันเช่น "| mail < |/etc/passwd" ซึ่งสามารถทำได้เพราะ Perl จะบอกให้ระบบปฏิบัติการเป็นตัวสั่งให้โปรแกรม mail ทำงานโดยใช้อินพุตที่รับเข้ามา (ในที่นี้คือ /etc/passwd) เป็นผลให้ไฟล์ passwd ถูกส่งไปให้ผู้บุกรุกโดยผ่านอีเมล์

- อินพุตที่ผิดปกติ (Unhandled input) โปรแกรมส่วนมากจะถูกเขียนให้สามารถจัดการกับข้อมูลอินพุตที่กำหนดให้ใช้ได้เท่านั้น โดยผู้พัฒนาโปรแกรมมักจะละเลยไม่พิจารณาว่าจะเกิดอะไรขึ้นถ้ามีคนใส่อินพุตที่ไม่เหมาะสมเข้ามา

- เงื่อนไขของการแข่งขัน (Race conditions) ระบบส่วนมากในปัจจุบันนี้เป็นแบบ multitasking/multithreaded ซึ่งสามารถทำงานได้หลายโปรแกรมในเวลาเดียวกัน ปัญหาที่เกิดขึ้นคือเมื่อโปรแกรมสองโปรแกรม(A,B)ต้องการเขียนข้อมูลชุดเดียวกันพร้อมกัน แต่ละโปรแกรมจะต้องอ่านข้อมูลไปเก็บไว้ในหน่วยความจำก่อน จากนั้นจึงค่อยทำการแก้ไขในหน่วยความจำ แล้วทำการสำเนากลับมาเก็บไว้ยังไฟล์ จึงเกิดเงื่อนไขของการแข่งขันขึ้น เมื่อโปรแกรม A อ่านไฟล์ไปเก็บไว้ในหน่วยความจำและทำการแก้ไข แต่ก่อนที่โปรแกรม A จะได้เขียนกลับมายังไฟล์ โปรแกรม B ก็ได้ทำการอ่านและแก้ไขไฟล์นี้แล้วเช่นกัน เมื่อโปรแกรม A ทำการเขียนกลับไปยังไฟล์ สิ่งที่โปรแกรม B ได้ทำการแก้ไขแต่ยังไม่ทันเขียนกลับจะหายหมด ฉะนั้นเราจึงจำเป็นต้องมีการจัดการลำดับของเหตุการณ์ให้เป็นไปอย่างถูกต้อง ซึ่งปกติปัญหานี้มักจะพบไม่บ่อยนัก

2.7.2.2 การปรับแต่งระบบ (System configuration)

ข้อบกพร่องที่เกิดจากการปรับแต่งระบบสามารถแบ่งประเภทได้ดังนี้

- การตั้งค่าเริ่มต้นโดยปริยาย (Default configurations) ส่วนมากเครื่องที่ถูกส่งมาถึงมือลูกค้ามักจะถูกตั้งค่าเริ่มต้นโดยปริยายมาจากโรงงานหรือผู้ขายอยู่แล้ว ซึ่งทำให้ผู้ใช้สะดวกและสามารถใช้งานได้เลย แต่โชคร้ายที่ความง่ายต่อการใช้งานนี้สำหรับผู้บุกรุกหมายถึงความง่ายต่อการบุกรุกเข้าสู่ระบบด้วยเช่นกัน เช่นเครื่องที่ลงระบบปฏิบัติการยูนิกซ์ (Unix) หรือไมโครซอฟต์วินโดวส์ (MS Windows) มักจะถูกส่งมาในลักษณะนี้ ซึ่งสามารถทำการบุกรุกได้อย่างง่ายดาย

- ผู้ดูแลระบบที่เกียจคร้าน (Lazy administrators) ไม่น่าแปลกใจที่ยังมีระบบอีกมากที่ไม่การตั้งรหัสผ่านหรือตั้งรหัสผ่านอย่างง่ายๆในการเข้าระบบ เนื่องจากความขี้เกียจของผู้ดูแลระบบเพราะความประมาทและต้องการความสะดวกในการเข้าใช้ระบบของตนเอง จึงเป็นการง่ายต่อผู้บุกรุกในการเข้าสู่ระบบด้วยเช่นกัน เพราะสิ่งแรกที่ผู้บุกรุกมักจะทำก่อนคือการสำรวจหาเครื่องที่ไม่มีการตั้งรหัสผ่านหรือตั้งรหัสผ่านแบบค่าปริยายไว้

- การสร้างรูโหว่ (Hole creation) ผู้ดูแลระบบมักจะเปิดรูโหว่บนเครื่องตัวเองไว้อย่างไม่ตั้งใจ ฉะนั้นในคู่มือการดูแลจัดการระบบจึงมักมีคำแนะนำให้ผู้ดูแลระบบทำการปิดทุกสิ่งทุกอย่างที่ไม่จำเป็นต่อการใช้งานบนเครื่อง เพื่อหลีกเลี่ยงปัญหาจากรูโหว่ของระบบที่อาจเกิดขึ้น

- ความสัมพันธ์ในการเชื่อถือระหว่างกัน (Trust relationships) ผู้บุกรุกมักจะอาศัยประโยชน์จากความสัมพันธ์ในการเชื่อถือระหว่างกันเพื่อบุกรุกไปสู่ระบบ และบุกรุกจากระบบหนึ่งไปสู่อีกระบบหนึ่งได้

2.7.2.3 การแคร็กรหัสผ่าน (Password cracking)

การแคร็กรหัสผ่านสามารถแบ่งประเภทได้ดังนี้

- รหัสผ่านที่ไม่ดี (Really weak passwords) ได้แก่ผู้ใช้งานระบบที่ตั้งรหัสผ่านของตนอย่างง่ายๆ หรือนำชื่อตนเอง ลูก คู่สมรส สัตว์เลี้ยง หรือสิ่งที่ตนชอบมาตั้งเป็นรหัสผ่าน ซึ่งผู้บุกรุกสามารถเดาคำที่อาจเป็นไปได้อย่างน้อย 30 คำในการเข้าสู่ระบบจากปัญหานี้

- รหัสผ่านที่มีในพจนานุกรม (Dictionary attacks) ถ้าการบุกรุกจากสาเหตุข้างต้นไม่สำเร็จ วิธีต่อไปที่ผู้บุกรุกจะใช้คือการใช้คำจากในพจนานุกรม โดยใช้โปรแกรมที่สามารถใช้คำทุกคำจากในพจนานุกรมในการลองเข้าสู่ระบบ และสามารถเพิ่มคำเข้าไปในฐานข้อมูลพจนานุกรมตามต้องการได้ด้วย ฉะนั้นผู้ดูแลระบบจึงต้องแนะนำผู้ใช้งานระบบว่าไม่ควรใช้คำที่มีในพจนานุกรมมาตั้งเป็นรหัสผ่าน

- รหัสผ่านที่ไม่มีในพจนานุกรม (Brute force attacks) ถ้ารหัสผ่านไม่ใช่คำที่พบในพจนานุกรม ผู้บุกรุกจะใช้วิธีในการผสมตัวอักษรมาใช้ในการลองรหัสผ่านเอง รหัสผ่านที่ตั้งจากตัวอักษรพิมพ์เล็ก4 ตัวจะถูกเดาได้ภายในเวลาไม่กี่นาที ส่วนรหัสผ่านที่ตั้งจากตัวอักษร 7 ตัวซึ่งประกอบด้วยตัวพิมพ์ใหญ่-เล็กและตัวเลขผสมกัน จะต้องอาศัยเวลาเป็นเดือนในการเดาออกมา

2.7.2.4 การดักดูข้อมูลบนเครือข่ายที่ไม่มีความปลอดภัย (Sniffing unsecured traffic)

การดักดูข้อมูลบนเครือข่ายที่ไม่มีความปลอดภัยสามารถแบ่งประเภทได้ดังนี้

- การใช้อุปกรณ์กระจายสัญญาณร่วมกัน (Shared media) บนการใช้งานระบบอีเตอร์เน็ต(Ethernet)สมัยก่อนจะสามารถทำการดักดูข้อมูลที่วิ่งบนระบบเครือข่ายได้อย่างง่ายดาย เนื่องจากการใช้ Hub เป็นอุปกรณ์ในการเชื่อมต่อและกระจายสัญญาณ แต่ปัจจุบันทำได้ยากขึ้นเพราะมีการใช้งานอุปกรณ์ Switch ซึ่งจะไม่กระจายสัญญาณไปยังทุกพอร์ตที่เชื่อมต่ออยู่แทน

- การดักดูข้อมูลบนเซิร์ฟเวอร์ (Server sniffing) อย่างไรก็ตามแม้กระทั่งบนระบบเครือข่ายที่มีการใช้อุปกรณ์ Switch การดักดูข้อมูลก็ยังสามารถกระทำได้บนเครื่องเซิร์ฟเวอร์ที่ทำหน้าที่เป็น Gateway เพราะสามารถดักดูข้อมูลที่ต้องการวิ่งข้ามระบบเครือข่ายได้อยู่ดี

- การดักดูข้อมูลจากระยะไกล (Remote sniffing) อุปกรณ์บนระบบเครือข่ายหลายตัวมักจะเปิดให้ใช้บริการ RMON ได้ด้วยการกำหนด community string เป็น public ซึ่งเปิดโอกาสให้ผู้บุกรุกในการสำรวจระบบเครือข่ายเราด้วยเช่นกัน

2.7.2.5 ข้อบกพร่องจากการออกแบบ (Design flaws)

แม้โปรแกรมจะถูกพัฒนามาด้วยการออกแบบที่ถูกต้องสมบูรณ์แบบอย่างไรก็ตาม แต่ก็ยังคงมีข้อบกพร่องในการออกแบบในส่วนอื่นอยู่ดี ข้อบกพร่องจากการออกแบบสามารถแบ่งประเภทได้ดังนี้

- ข้อบกพร่องที่โปรโตคอลและซอฟต์แวร์ (Protocol and software flaws) โปรโตคอลมีหน้าที่ในการกำหนดกฎระเบียบที่ใช้ในการติดต่อสื่อสารกันสำหรับคอมพิวเตอร์บนระบบเครือข่าย ถ้าตัวโปรโตคอลมีความบกพร่องในการออกแบบตั้งแต่ขั้นพื้นฐานอยู่ก่อนแล้ว ไม่ว่าจะถูกนำไปพัฒนาเป็นโปรแกรมหรือเครื่องมือที่ดีขนาดไหนก็ตาม ก็ยังคงมีความล่อแหลมให้ผู้บุกรุกใช้ประโยชน์ได้อยู่ดี เช่นโปรโตคอล NFS (Network File System) ที่ใช้ในการแชร์ไฟล์ระหว่างระบบ ซึ่งไม่ต้องผ่านการขออนุญาตและยืนยันตัวผู้ใช้ก่อนเข้าใช้งาน ส่วนตัวซอฟต์แวร์นั้นการออกแบบการสร้างในขึ้นเริ่มแรกมักจะไม่รวมส่วนของระบบรักษาความปลอดภัยไว้ด้วย แต่จะทำเป็นส่วนที่สามารถเพิ่มเติมได้ในภายหลัง ซึ่งในท้ายที่สุดไม่ว่าตัวโปรโตคอลหรือซอฟต์แวร์จะถูกออกแบบมาดีแค่ไหน แต่ถ้าการพัฒนานำไปใช้อย่างไม่ถูกวิธี ก็ยังคงนำมาซึ่งความบกพร่องของระบบอยู่ดี

- ข้อบกพร่องที่โปรโตคอลระบบเครือข่าย (Network protocol flows) จากการออกแบบโปรโตคอล TCP/IP สำหรับใช้งานบนระบบเครือข่ายในสมัยก่อน จะเห็นว่าไม่ได้ถูกออกแบบมาสำหรับการใช้งานแบบผิดวัตถุประสงค์อย่างในปัจจุบัน ทำให้เกิดปัญหาข้อบกพร่องในการออกแบบต่างๆมากมาย ซึ่งนำมาสู่ความเป็นไปได้ในการถูกบุกรุกเข้าสู่ระบบในที่สุด เช่น การโจมตีแบบ Smurf attacks, ICMP unreachable disconnects, IP spoofing และ SYN floods เป็นต้น ปัญหาที่ใหญ่ที่สุดคือตัวโปรโตคอล IP เองทำงานโดยอาศัยความเชื่อใจในหมายเลขไอพีแอดเดรส ที่กำหนดอยู่ในตัวข้อมูลมากเกินไป ทำให้ผู้บุกรุกสามารถใช้ประโยชน์จากจุดนี้ได้โดยการปลอมหมายเลขไอพีได้อย่างลอยนวล โปรโตคอล IPSec จึงถูกพัฒนาออกมาโดยการออกแบบให้แก้ปัญหาเหล่านี้ แต่การใช้งานยังไม่กว้างขวางนัก

- ข้อบกพร่องที่ตัวระบบ (System flaws) ในระบบปฏิบัติการต่างๆมักจะมีข้อบกพร่องมากมายที่มักนำมาสู่การบุกรุกเข้าสู่ระบบ เช่นในระบบปฏิบัติการยูนิกซ์มีปัญหาที่สำคัญเกี่ยวกับระบบควบคุมการเข้าใช้งานระบบคือมีเฉพาะผู้ใช้งานรูต (root) เท่านั้นที่ได้รับสิทธิ์ในการจัดการทุกสิ่งทุกอย่างในระบบ, File share brute forcing และการขโมยไฟล์ที่เก็บรหัสผ่าน

2.8 ขั้นตอนหลักในการบุกรุกเข้าสู่ระบบ

ปริญญา หอมเอนก (2545) ได้แบ่งขั้นตอนหลักในการบุกรุกเข้าสู่ระบบไว้ดังนี้

2.8.1 การสำรวจหาข้อมูลเบื้องต้น (Foot printing)

ผู้บุกรุกจะเริ่มต้นขั้นตอนแรกของการบุกรุกเข้าสู่ระบบด้วยการหาข้อมูลเบื้องต้นที่จำเป็นต่อการบุกรุกในขั้นต่อไป โดยเป็นการสำรวจระบบจากภายนอก ผู้บุกรุกสามารถปลอมแปลงตนเองเพื่อไม่ให้ใครรู้ว่าตนเองเป็นใครและมีเจตนาอะไรได้ ด้วยการปลอมเป็นผู้ใช้งานทั่วไป ซึ่งในขั้นนี้เราจะไม่สามารถตรวจสอบพบผู้บุกรุกได้ เทคนิคทั่วไปที่ผู้บุกรุกใช้ได้แก่บริการ whois ทั่วไปบนอินเทอร์เน็ตเพื่อใช้ค้นหาข้อมูลของเครือข่าย คำสั่ง nslookup หรือ dig เพื่อหาชื่อเครื่องคอมพิวเตอร์ในเครือข่าย

2.8.2 การสำรวจระบบ (Scanning)

ผู้บุกรุกจะขยายการสำรวจระบบเป้าหมาย เพื่อหาช่องทางในการเข้าสู่ระบบ เทคนิคทั่วไปที่ผู้บุกรุกใช้ได้แก่การ ping กวาดไปทั้งระบบเพื่อดูว่ามีเครื่องไหนทำงานอยู่ การสำรวจพอร์ต TCP/UDP บนเครื่องเป้าหมายเพื่อตรวจสอบดูพอร์ตต่างๆที่เครื่องเป้าหมายเปิดให้บริการไว้ และการตรวจสอบระบบปฏิบัติการที่ใช้ ซึ่ง ณ จุดนี้สิ่งที่ผู้บุกรุกกระทำยังเป็นพฤติกรรมปกติที่เกิดขึ้นได้บนระบบเครือข่ายและยังไม่มีสิ่งใดระบุได้ว่าเป็นการบุกรุก แต่ระบบตรวจสอบ ผู้บุกรุกบนเครือข่ายจะสามารถบอกได้ว่ามีใครบางคนกำลังสำรวจระบบของเราอยู่ แต่ยังไม่ได้ทำอะไร

2.8.3 การสำรวจภายในระบบ (Enumeration)

เมื่อผู้บุกรุกเริ่มเจาะระบบเข้ามาทางรูโหว่ที่ตรวจพบเจอของระบบ ก็จะเริ่มทำการสำรวจรายชื่อผู้ใช้งานระบบหรือการแบ่งปันทรัพยากรภายในระบบที่มีการป้องกันไม่ดีนัก เทคนิคทั่วไปที่ผู้บุกรุกใช้ได้แก่ List user accounts, List file shares และ Identify applications

2.8.4 การได้รับสิทธิ์ในการใช้งานระบบ (Gaining access)

เมื่อผู้บุกรุกมาถึงจุดนี้และได้ข้อมูลเพียงพอแล้ว ก็จะพยายามทำการให้ได้มาซึ่งสิทธิ์ในการใช้งานระบบ เทคนิคทั่วไปที่ผู้บุกรุกใช้ได้แก่ การดักดูรหัสผ่าน และการทำให้เกิด Buffer overflows

2.8.5 การยกระดับสิทธิ์การใช้งานระบบ (Escalating privilege)

ถ้าสิทธิ์การใช้งานระบบที่ผู้บุกรุกได้มาจากในขั้นตอนที่แล้วเป็นเพียงระดับผู้ใช้งานทั่วไป ผู้บุกรุกจะพยายามยกระดับสิทธิ์การใช้งานเพื่อให้ได้มาซึ่งความสามารถในการควบคุมได้ทั้งระบบ เทคนิคทั่วไปที่ผู้บุกรุกใช้ได้แก่ การแคร็ก รหัสผ่าน (Password cracking) และการใช้ประโยชน์จากรูโหว่ต่างๆของระบบ

2.8.6 การลักลอบใช้งานระบบ (Pilfering)

เมื่อผู้บุกรุกได้รับสิทธิ์ในการใช้งานระบบก็มักจะลักลอบใช้งานระบบบางอย่าง เพื่อสร้างความเชื่อใจต่อระบบหรือแสวงหาผลประโยชน์จากสิทธิ์ที่ตนได้รับ เช่นแอบสร้างบัญชีผู้ใช้ใหม่ที่ถูกต้องไว้สำหรับในการใช้งานเอง ขโมยรหัสผ่านข้อมูลที่สำคัญของผู้ใช้ในระบบ หรือการเปลี่ยนแปลงแก้ไขไฟล์หรือค่าฟอนฟิกูเรชั่นต่างๆของระบบ เป็นต้น

2.8.7 การลบหลักฐาน (Covering Tracking)

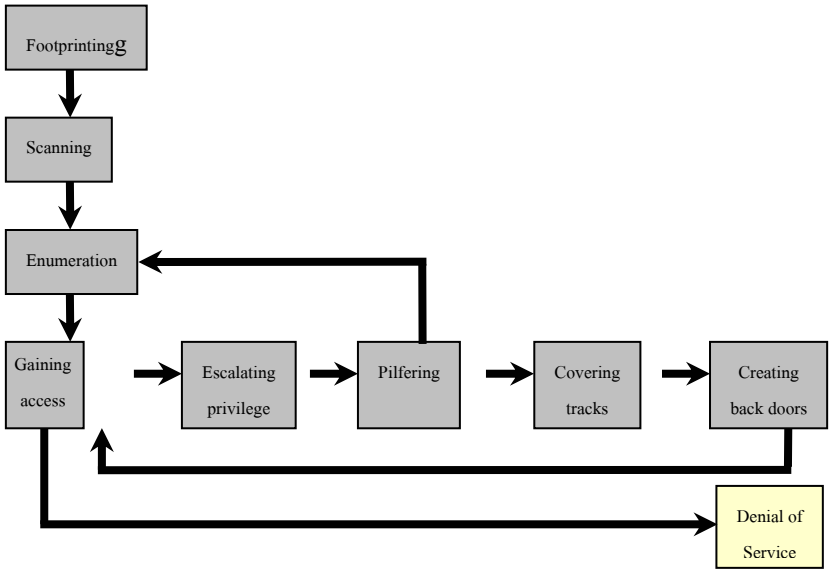
เมื่อผู้บุกรุกแน่ใจว่าระบบเป้าหมายอยู่ในการควบคุมของตนแล้ว ก็จะทำการซ่อนหรือลบหลักฐานที่ใช้ในการเข้าสู่ระบบอย่างผิดปกติของตน เพื่อหลีกเลี่ยงการถูกผู้ดูแลระบบตัวจริงตรวจจับได้ เทคนิคทั่วไปที่ผู้บุกรุกใช้ได้แก่การเข้าไปลบในล็อคไฟล์ (Log file) ซึ่งเก็บสถานะการใช้งานต่างๆของระบบไว้

2.8.8 การสร้างช่องทางลับ (Creating back door)

ผู้บุกรุกมักจะทำการสร้างช่องทางลับทิ้งไว้ในระบบ เพื่อให้แน่ใจว่าสามารถกลับเข้ามาได้อีกครั้งตามที่ตนต้องการ เทคนิคทั่วไปที่ผู้บุกรุกใช้ได้แก่การสร้างบัญชีผู้ใช้ใหม่ การลงโปรแกรมประเภทที่สามารถควบคุมจากระยะไกลไว้ หรือลงโปรแกรมประเภทโทรจันไว้

2.8.9 การทำให้ระบบทำงานผิดพลาด (Denial of Service)

ถ้าผู้บุกรุกไม่สามารถบุกรุกเข้ามายังระบบได้สำเร็จ ก็อาจจะใช้ประโยชน์จากรูโหว่ของระบบในการทำให้ระบบทำงานผิดพลาดหรือไม่สามารถให้บริการได้ตามปกติ เทคนิคทั่วไปที่ผู้บุกรุกใช้ได้แก่ SYN flood, ICMP techniques, Identical src/dst, SYN requests, Overlapping fragment/offset bugs, Out of bound TCP option (OOB) และ Ddos เป็นต้น



รูปที่ 2.1 แสดงขั้นตอนหลักในการบุกรุกเข้าสู่ระบบ

2.9 รูปแบบในการบุกรุก

Robert Graham (2000) แบ่งได้เป็น 3 ประเภทหลักๆได้ดังนี้

2.9.1 การสำรวจระบบ (Reconnaissance)

เป็นการสำรวจเป้าหมายขั้นต้นของผู้บุกรุกเพื่อที่จะนำข้อมูลนั้นมาวิเคราะห์หาจุดอ่อนในการบุกรุกเข้ามายังระบบ โดยทั่วไปจะไม่ส่งผลกระทบต่อระบบ เพราะยังไม่ใช่การโจมตี แต่เป็นเพียงกระบวนการเริ่มต้นของการบุกรุกเท่านั้น การสำรวจระบบนั้นทำได้หลายวิธีด้วยวัตถุประสงค์และเทคนิคที่แตกต่างกัน ซึ่งหากเรารู้และตรวจผลของการกระทำได้แต่เนิ่นๆ ย่อมทำให้สามารถเพิ่มความระมัดระวังและเตรียมพร้อมก่อนการถูกบุกรุกจริงได้ อีกนัยหนึ่งคือถ้าเราทราบว่าระบบของเรามีจุดที่ถูกสำรวจได้ง่ายก็จะสามารถป้องกันส่วนนั้นได้ โดยการสำรวจนั้นสามารถแบ่งได้เป็น 3 แบบ คือ

- การสำรวจเครือข่าย (Network reconnaissance)

เพื่อตรวจสอบเครือข่ายเป้าหมาย ผลที่ได้จะบอกถึงจำนวนและลักษณะการใช้งานของเครื่องที่มีอยู่ในเครือข่ายนั้น

- การสำรวจเครื่อง (Host reconnaissance)

เพื่อวิเคราะห์รายละเอียดในแต่ละเครื่องที่คาดว่าจะเจาะเข้าไปได้โดยง่าย ว่ามีพฤติกรรมการใช้งานเป็นอย่างไร ลักษณะจะประกอบด้วยการสำรวจที่สำคัญดังนี้คือ การสำรวจพอร์ต การสำรวจข้อมูลระบุแอพพลิเคชั่น และการสำรวจข้อมูลระบบปฏิบัติการ

- การสำรวจแอพพลิเคชั่น (Application reconnaissance)

ได้แก่การสำรวจหาแอพพลิเคชั่นเฉพาะเจาะจงที่ทราบจุดอ่อนอยู่แล้วหรือการหาโปรแกรมโทรจัน(Trojan)หรือช่องทางลับ(Back doors)ต่างๆ

2.9.2 การใช้ประโยชน์จากระบบ (Exploits)

ผู้บุกรุกใช้ประโยชน์จากคุณลักษณะที่ซ่อนอยู่หรือข้อผิดพลาดต่างๆ (Bugs) เพื่อให้ได้มาซึ่งเข้าถึงระบบ ตัวอย่างของลักษณะนี้ได้แก่บัฟเฟอร์โอเวอร์โฟล (Buffer Overflow) การส่งคำสั่งที่มีลักษณะบุกรุก (Unexpected Combination) และอินพุตที่ผิดปกติ (Unhandled Input)

2.9.3 การทำให้ระบบทำงานผิดพลาด (Denial of Services)

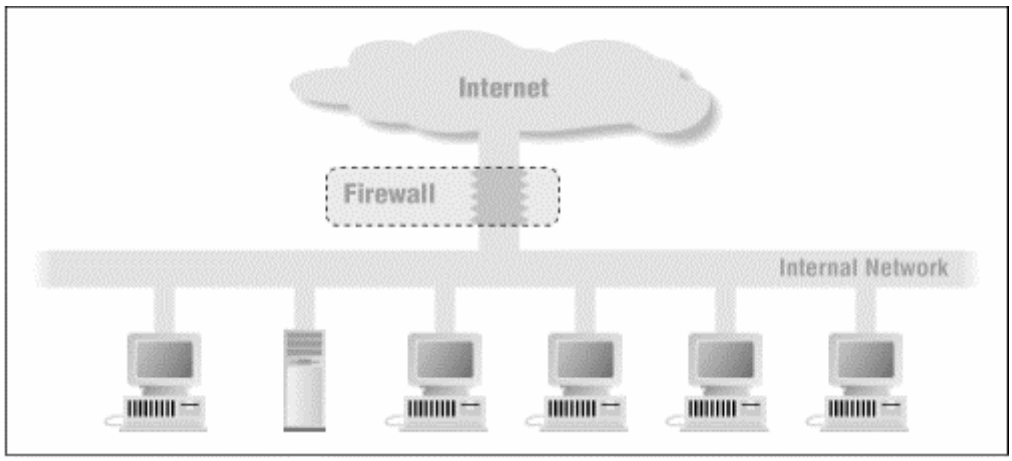
หมายถึงการกระทำใดๆ ที่ทำให้ระบบเป้าหมายทำงานผิดพลาดหรือไม่สามารถให้บริการตามปกติต่อไปได้อีก โดยทั่วไปจะเป็นการโจมตีที่พอร์ตของ TCP/IP ซึ่งเชื่อมต่อกับบริการที่รองรับพอร์ตนั้นๆ ดังนั้นการโจมตีพอร์ตจึงเท่ากับการโจมตีบริการของระบบนั่นเอง ซึ่งการโจมตีแบบนี้ถือเป็นความเสียหายที่รุนแรงมากในระบบที่ต้องให้บริการข้อมูลที่รวดเร็ว

2.10 เทคโนโลยีการรักษาความปลอดภัย

ปัจจุบันได้มีการพัฒนาเทคโนโลยีออกมามายมากเพื่อช่วยในการรักษาความปลอดภัยระบบและข้อมูลสารสนเทศจากบรรดาผู้บุกรุกทั้งหลาย โดยเทคโนโลยีเหล่านี้จะใช้ในการป้องกันการบุกรุก ตรวจสอบพฤติกรรมที่ผิดปกติหรือน่าสงสัย และการตอบสนองต่อเหตุการณ์ที่สร้างความไม่ปลอดภัยเหล่านั้น ซึ่งสามารถแบ่งได้เป็นสองประเภทหลักๆคือเทคโนโลยีทางด้านปฏิบัติการ (Operational techonology) และการเข้ารหัสลับ (Cryptography) จุดประสงค์ของการรักษาความปลอดภัยโดยใช้เทคโนโลยีทางด้านปฏิบัติการนั้นคือเพื่อป้องกันและรักษาความพร้อมใช้งานของแหล่งข้อมูล ส่วนเทคโนโลยีทางด้านการเข้ารหัสลับคือเพื่อการรักษาความลับ ความสมบูรณ์ และการพิสูจน์ตัวตนเพื่อเข้าใช้งานแหล่งข้อมูล โดยในเอกสารรายงานการค้นคว้าอิสระฉบับนี้จะขอกล่าวถึงแต่เทคโนโลยีทางด้านปฏิบัติการเฉพาะบางส่วนเท่านั้น

2.10.1 ไฟร์วอลล์ (Firewall)

ปราการ โกลากุล (2545) ไฟร์วอลล์เป็นคอมโพเน็นต์หรือกลุ่มของคอมโพเน็นต์ที่ทำหน้าที่ในการควบคุมการเข้าถึงระหว่างเครือข่ายภายนอกหรือเครือข่ายที่เราคิดว่าไม่ปลอดภัยกับเครือข่ายภายในหรือเครือข่ายที่เราต้องการจะป้องกัน โดยที่คอมโพเน็นต์นั้นอาจจะเป็นเราเตอร์คอมพิวเตอร์หรือเครือข่าย



รูปที่ 2.2 แสดงไฟร์วอลล์กั้นระหว่างอินเทอร์เน็ตกับเครือข่ายภายใน

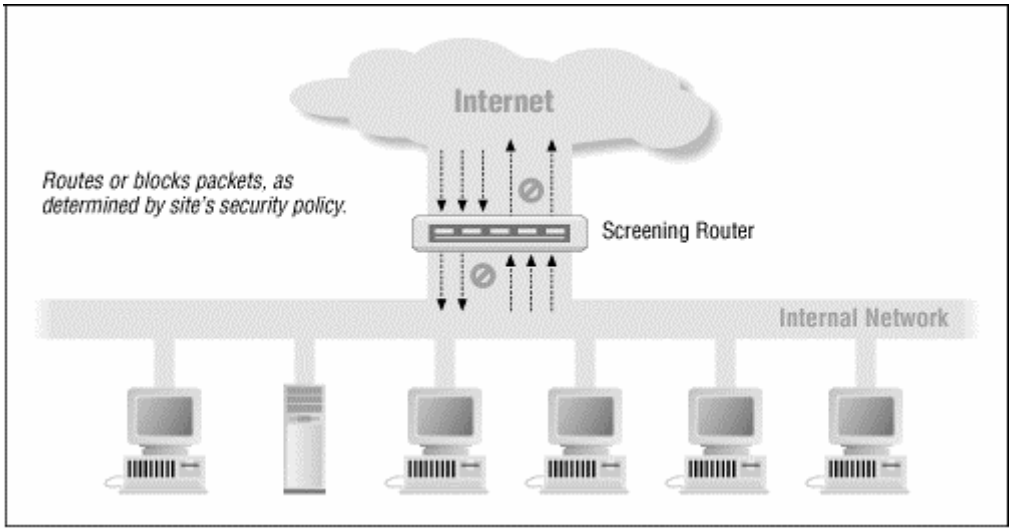
การควบคุมการเข้าถึงของไฟร์วอลล์นั้น สามารถทำได้ในหลายระดับและหลายรูปแบบขึ้นอยู่ชนิดหรือเทคโนโลยีของไฟร์วอลล์ที่นำมาใช้ เช่น เราสามารถกำหนดได้ว่าจะให้มีการเข้ามาใช้บริการอะไรได้บ้าง จากที่ไหน เป็นต้น

2.10.1.1 ชนิดของไฟร์วอลล์

ปราการ โกลากุล (2545) ชนิดของไฟร์วอลล์แบ่งตามเทคโนโลยีที่ใช้ในการตรวจสอบและควบคุม แบ่งได้เป็น

1. Packet Filter

Packet Filter คือเราเตอร์ที่ทำการหาเส้นทางและส่งต่อ (route) อย่างมีเงื่อนไข โดยจะพิจารณาจากข้อมูลส่วนที่อยู่ในเฮดเดอร์ (header) ของแพ็กเก็ตที่ผ่านเข้ามา เทียบกับกฎที่กำหนดไว้และตัดสินว่าควรจะทิ้ง(drop)แพ็กเก็ตนั้นไปหรือว่าจะยอม (accept) ให้แพ็กเก็ตนั้นผ่านไปได้



รูปที่ 2.3 แสดงใช้ Screening Router ทำหน้าที่ Packet Filtering

ในการพิจารณาเฮดเดอร์ Packet Filter จะตรวจสอบในระดับของอินเทอร์เน็ตเลเยอร์ (Internet Layer) และทรานสปอร์ตเลเยอร์ (Transport Layer) ในอินเทอร์เน็ตโมดล ซึ่งในอินเทอร์เน็ตเลเยอร์จะมีแอตทริบิวต์ที่สำคัญต่อ Packet Filtering ดังนี้

- ไอพีต้นทาง
- ไอพีปลายทาง
- ชนิดของโปรโตคอล (TCP UDP และ ICMP)

และในระดับของทรานสปอร์ตเลเยอร์ มีแอตทริบิวต์ที่สำคัญคือ

- พอร์ตต้นทาง
- พอร์ตปลายทาง
- แฟล็ก (Flag ซึ่งจะมีเฉพาะในเฮดเดอร์ของแพ็กเก็ต TCP)
- ชนิดของ ICMP message (ในแพ็กเก็ต ICMP)

ซึ่งพอร์ตของทรานสปอร์ตเลเยอร์ คือทั้ง TCP และ UDP นั้นจะเป็นสิ่งที่บอกถึงแอพพลิเคชันที่แพ็กเก็ตนั้นต้องการติดต่อด้วยเช่น พอร์ต 80 หมายถึง HTTP พอร์ต 21 หมายถึง FTP เป็นต้น ดังนั้นเมื่อ Packet Filter พิจารณาเฮดเดอร์ จึงทำให้สามารถควบคุมแพ็กเก็ตที่มาจากที่ต่างๆ และมีลักษณะต่างๆ (ดูได้จากแฟล็กของแพ็กเก็ต หรือ ชนิดของ ICMP ในแพ็กเก็ต ICMP) ได้ เช่น ห้ามแพ็กเก็ตทุกชนิดจาก crack.cracker.net เข้ามายังเครือข่าย 203.154.207.0/24 ห้ามแพ็กเก็ตที่มีไอพีต้นทางอยู่ในเครือข่าย 203.154.207.0/24 ผ่านเราเตอร์เข้ามา (ในกรณีนี้เพื่อเป็นการป้องกัน ip spoofing) เป็นต้น

Packet Filtering สามารถอิมพลีเมนต์ได้จาก 2 แพล็ตฟอร์ม คือ

- เราเตอร์ที่มีความสามารถในการทำ Packet Filtering (ซึ่งมีในเราเตอร์ส่วนใหญ่อยู่แล้ว)
- คอมพิวเตอร์ที่ทำหน้าที่เป็นเราเตอร์

ซึ่งจะมีข้อได้เปรียบเสียเปรียบกันดังนี้

	ข้อดี	ข้อเสีย
เราเตอร์	ประสิทธิภาพสูงมีจำนวนอินเตอร์เฟสมาก	เพิ่มเติมฟังก์ชันการทำงานได้ยาก อาจต้องการหน่วยความจำมาก
คอมพิวเตอร์ที่ทำหน้าที่เป็นเราเตอร์	เพิ่มฟังก์ชันการทำงานได้ไม่จำกัด	ประสิทธิภาพปานกลางจำนวนอินเตอร์เฟสน้อยอาจมีความเสี่ยงจากระบบปฏิบัติการที่ใช้

ตารางที่ 2.1 เปรียบเทียบข้อดีข้อเสียในการเลือกอุปกรณ์มาทำหน้าที่ Packet Filtering

ข้อดีของ Packet Filtering

- ไม่ขึ้นกับแอพพลิเคชัน
- มีความเร็วสูง
- รองรับการขยายตัวได้ดี

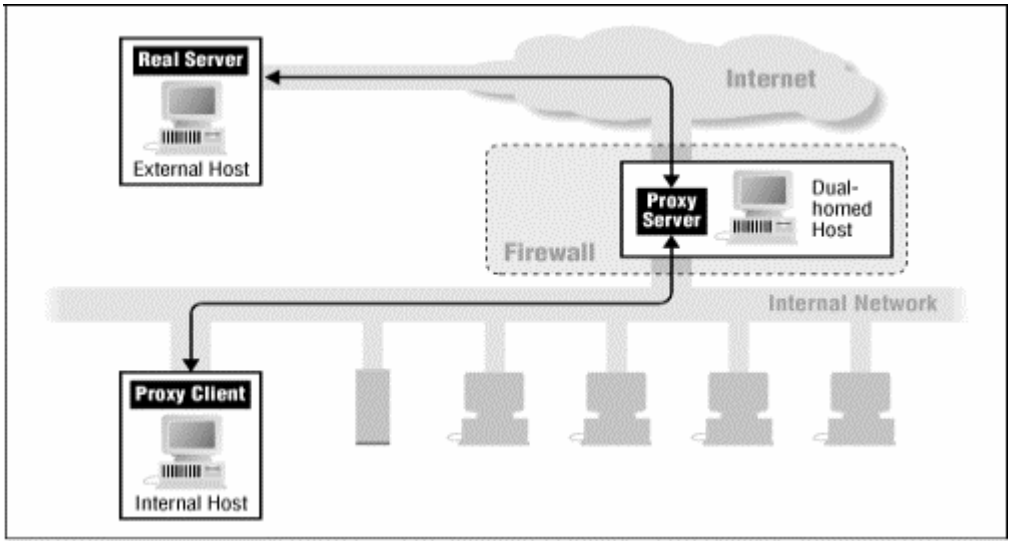
ข้อเสียของ Packet Filtering

- บางโปรโตคอลไม่เหมาะสมกับการใช้ Packet Filtering เช่น FTP, ICQ ซึ่งมีการทำงานแบบไดนามิกพอร์ต

2. Proxy หรือ Application Gateway

เป็นแอพพลิเคชันโปรแกรมที่ทำงานอยู่บนไฟร์วอลล์ที่ตั้งอยู่ระหว่างเครือข่าย 2 เครือข่าย ทำหน้าที่เพิ่มความปลอดภัยของระบบเครือข่ายโดยการควบคุมการเชื่อมต่อระหว่างเครือข่ายภายในและภายนอก Proxy จะช่วยเพิ่มความปลอดภัยได้มากเนื่องจากมีการตรวจสอบข้อมูลถึงในระดับของแอพพลิเคชันเลเยอร์ (Application Layer)

เมื่อไคลเอนต์ต้องการใช้บริการภายนอก ไคลเอนต์จะทำการติดต่อไปยัง Proxy ก่อน ไคลเอนต์จะเจรจา (negotiate) กับ Proxy เพื่อให้ Proxy ติดต่อไปยังเครื่องปลายทางให้ เมื่อ Proxy ติดต่อไปยังเครื่องปลายทางให้แล้วจะมีการเชื่อมต่อ (connection) 2 การเชื่อมต่อ คือ ไคลเอนต์กับ Proxy และ Proxy กับเครื่องปลายทาง โดยที่ Proxy จะทำหน้าที่รับข้อมูลและส่งต่อข้อมูลให้ใน 2 ทิศทาง ทั้งนี้ Proxy จะทำหน้าที่ในการตัดสินใจว่าจะให้มีการเชื่อมต่อกันหรือไม่ จะส่งต่อแพ็กเก็ตให้หรือไม่



รูปที่ 2.4 แสดงใช้ Dual-homed Host เป็น Proxy Server

ข้อดีของ Proxy

- มีความปลอดภัยสูง
- รู้จักข้อมูลในระดับแอพพลิเคชัน

ข้อเสียของ Proxy

- ประสิทธิภาพต่ำ
- แต่ละบริการมักจะต้องการโปรเซสของตนเอง
- สามารถขยายตัวได้ยาก

3. Stateful Inspection Technology

โดยปกติแล้ว Packet Filtering แบบธรรมดา (ที่เป็น Stateless แบบที่มีอยู่ในเราเตอร์ทั่วไป) จะควบคุมการเข้าออกของแพ็กเก็ตโดยพิจารณาข้อมูลจากเฮดเดอร์ของแต่ละแพ็กเก็ต นำมาเทียบกับกฎที่มีอยู่ ซึ่งกฎที่มีอยู่ก็จะเป็นกฎที่สร้างจากข้อมูลส่วนที่อยู่ในเฮดเดอร์เท่านั้น ดังนั้น Packet Filtering แบบธรรมดาจึงไม่สามารถทราบได้ว่า แพ็กเก็ตนี้อยู่ส่วนใดของการเชื่อมต่อ เป็นแพ็กเก็ตที่เข้ามาติดต่อใหม่หรือเปล่า หรือว่าเป็นแพ็กเก็ตที่เป็นส่วนของการเชื่อมต่อที่เกิดขึ้นแล้ว เป็นต้น

Stateful Inspection เป็นเทคโนโลยีที่เพิ่มเข้าไปใน Packet Filtering โดยในการพิจารณาว่าจะยอมให้แพ็กเก็ตผ่านไปนั้น แทนที่จะดูข้อมูลจากเฮดเดอร์เพียงอย่างเดียว Stateful Inspection จะนำเอาส่วนข้อมูลของแพ็กเก็ต (message content) และข้อมูลที่ได้จากแพ็กเก็ตก่อนหน้านี้ที่ได้ทำการบันทึกเอาไว้ นำมาพิจารณาด้วย จึงทำให้สามารถระบุได้ว่าแพ็กเก็ตใดเป็นแพ็กเก็ตที่ติดต่อเข้ามาใหม่ หรือว่าเป็นส่วนหนึ่งของการเชื่อมต่อที่มีอยู่แล้ว

ตัวอย่างผลิตภัณฑ์ทางการค้าที่ใช้ Stateful Inspection Technology

- Check Point Firewall-1
- Cisco Secure Pix Firewall
- SunScreen Secure Net
- และส่วนที่เป็น open source แจกฟรี ได้แก่
- NetFilter ใน Linux (Iptables ในระบบปฏิบัติการลีนุกซ์เคอร์เนล 2.4 เป็นต้นไป)

2.10.2 ระบบตรวจสอบผู้บุกรุก (Intrusion Detection System หรือ IDS)

ร.อ.วิวัต เรืองมี (2545) ระบบตรวจสอบการบุกรุกคือระบบที่ใช้ในการตรวจสอบการใช้งานและความพยายามในการใช้งานคอมพิวเตอร์หรือเครือข่ายคอมพิวเตอร์ซึ่งขัดกับข้อบังคับและเจตุจำนงค์การใช้งาน ส่งผลต่อความปลอดภัยของระบบคอมพิวเตอร์หรือเครือข่ายคอมพิวเตอร์ 3 ประการคือ การรักษาความลับ (Confidentiality) ความสมบูรณ์ (Integrity) และความพร้อมใช้งาน(Availability)

2.10.2.1 ทำไมถึงจำเป็นต้องใช้ระบบตรวจสอบผู้บุกรุก

เมื่อคำนึงถึงเรื่องความปลอดภัยของคอมพิวเตอร์มักเป็นการยากในการมองภาพที่ชัดเจนว่า อะไรที่จะบ่งบอกได้ว่าการใช้งานคอมพิวเตอร์มีความปลอดภัย เนื่องจากความปลอดภัยของคอมพิวเตอร์เป็นสิ่งที่จับต้องไม่ได้และยากต่อการวัด แต่อย่างไรก็ตามเราสามารถเปรียบเทียบความปลอดภัยของคอมพิวเตอร์กับการรักษาความปลอดภัยสถานที่ ในการรักษา

ความปลอดภัยสถานที่นั้นนอกจากการ จัดบริเวณที่ต้องการรักษาความปลอดภัยให้มีรั้วรอบขอบชิด มีกุญแจที่ใช้ล็อกประตูหรือทางเข้าออก สิ่งหนึ่งที่จะขาดไม่ได้คือการจัดให้มีบุคคลหรืออุปกรณ์ที่คอยตรวจสอบ การละเมิดต่ออุปกรณ์หรือเครื่องกีดขวางที่จัดตั้งเพื่อความปลอดภัย ทั้งนี้เนื่องจากอาจมีผู้ไม่หวังดีพยายามบุกรุกโดยทำลายอุปกรณ์หรือเครื่องกีดขวางดังกล่าวดังนั้นเราจึงต้องอาศัยระบบที่ใช้ตรวจสอบเมื่อมีการทำลายหรือล่วงล้ำต่ออุปกรณ์หรือเครื่องกีดขวางที่ได้ติดตั้งไว้อีกชั้นหนึ่ง ตัวอย่างอุปกรณ์ที่ใช้ตรวจสอบเช่น ระบบสัญญาณเตือนขโมยที่ใช้ควบคู่กับรั้วที่แข็งแรง

ระบบเครือข่ายคอมพิวเตอร์ก็เช่นเดียวกัน บุคคลทั่วไปมักคิดว่าการติดตั้งไฟร์วอลล์ตามลำพังก็สามารถทำให้เครือข่ายคอมพิวเตอร์มีความปลอดภัย แต่อย่างไรก็ตามการติดตั้งไฟร์วอลล์ ให้กับระบบเครือข่ายคอมพิวเตอร์ก็เปรียบเสมือนการสร้างรั้วหรือกำแพงเพื่อตรวจสอบบุคคลที่จะเข้ามาในสถานที่ที่จะการรักษาความปลอดภัยแต่หากมีบุคคลไม่หวังดีสามารถปีนรั้วเข้ามาได้ การรักษาความปลอดภัยโดยใช้รั้วก็หมดความหมาย ดังนั้นในการเพิ่มความปลอดภัยอีกประการหนึ่งคือการใช้ระบบตรวจสอบการบุกรุกซึ่งมีคุณลักษณะที่กล่าวมาในตอนต้น

2.10.2.2 ชนิดของระบบตรวจสอบผู้บุกรุก

Earl Carter (2002) ได้แบ่งประเภทของระบบตรวจสอบผู้บุกรุกสามารถแบ่งได้เป็น 2 ประเภทหลักดังนี้

1.) แบ่งตามวิธีการตรวจจับการบุกรุก

- Anomaly Detection หรือ Profile-based Detection

การตรวจจับโดยวิธีนี้ต้องอาศัยการสร้างแฟ้มข้อมูล (Profile) ของผู้ใช้หรือกลุ่มของผู้ใช้งานในระบบขึ้นมา เพื่อใช้เก็บพฤติกรรมการใช้งานที่เป็นปกติจากกิจกรรมหรืองานที่ต้องทำอยู่เป็นประจำ แฟ้มข้อมูลเหล่านี้จึงเปรียบเสมือนบรรทัดฐานที่ใช้ในการตรวจจับพฤติกรรมที่ผิดปกติไปจากการทำงานตามปกติของผู้ใช้ในระบบ

ด้วยวิธีนี้ระบบตรวจสอบผู้บุกรุกจะสามารถตรวจจับการบุกรุกได้โดยดูจากพฤติกรรมการที่ผิดไปจากการใช้งานปกติของระบบ ซึ่งจะไม่มีรูปแบบที่แน่นอนสำหรับทุกระบบขึ้นอยู่กับพฤติกรรมการใช้งานปกติของระบบนั้นๆเอง ฉะนั้นการกำหนดบรรทัดฐานของพฤติกรรมปกติในระบบจึงเป็นเรื่องที่สำคัญและละเอียดอ่อนมาก ถ้าระบบสามารถกำหนดบรรทัดฐานที่ครอบคลุมพฤติกรรมการใช้งานปกติของระบบได้หมด การเกิด False Positive[1] จาก

---

[1] False Positive หมายถึงการที่ IDS ตรวจพบการบุกรุกที่เกิดจากกิจกรรมการทำงานปกติ ซึ่งไม่ใช่การบุกรุกจริง ซึ่งการเกิด False Positive จะทำให้เกิดการสูญเสียทั้งเวลาและทรัพยากรของระบบโดยเปล่าประโยชน์

ระบบตรวจสอบผู้บุกรุกประเภทนี้ก็จะมีโอกาสเกิดขึ้นน้อย ในขณะที่การเกิด False Negative[2] ก็มีโอกาสเกิดขึ้นได้จากการบุกรุกที่มีพฤติกรรมเหมือนการใช้งานตามปกติในระบบ ซึ่งในกรณีนี้แทบจะเป็นไปไม่ได้เลยที่ระบบตรวจสอบผู้บุกรุกประเภทนี้จะสามารถแยกแยะได้ว่าพฤติกรรมใดเป็นการใช้งานตามปกติหรือว่าเป็นบุกรุก

- Misuse Detction หรือ Signature-based Detection

เป็นการตรวจจับพฤติกรรมการบุกรุกโดยเปรียบเทียบจากข้อมูลลักษณะเฉพาะ (Signature) ที่ใช้อ้างอิง ซึ่งลักษณะเฉพาะเหล่านี้จะเป็นกลุ่มของกฎต่างๆที่เป็นรูปแบบหรือพฤติกรรมของผู้บุกรุกที่ใช้ในการบุกรุกเข้าสู่ระบบ

ฉะนั้นการกำหนดรูปแบบลักษณะเฉพาะที่ใช้อ้างอิงเปรียบเทียบที่ดีจะสามารถลดโอกาสในการเกิด False Positive ได้ ในขณะที่การป้องกันการเกิด False Negative จะขึ้นอยู่กับการหมั่นปรับปรุงฐานข้อมูลลักษณะเฉพาะเหล่านี้ให้ทันสมัยต่อรูปแบบการบุกรุกที่เกิดขึ้นใหม่ๆอยู่ตลอดเวลา

2.) แบ่งตามตำแหน่งในการตรวจจับการบุกรุก

- Host-based IDS (HIDS)

ทำงานอยู่บนเครื่องคอมพิวเตอร์ที่ต้องการตรวจสอบการบุกรุกเอง โดยตรวจจับการบุกรุกที่เกิดขึ้นในระดับระบบปฏิบัติการ (Operating System) ซึ่งข้อมูลที่ได้จากระบบตรวจสอบประเภทนี้เป็นข้อมูลที่ได้หลังการบุกรุกไปยังเครื่อง เป้าหมายแล้วจริงๆเท่านั้น ในขณะที่ระบบตรวจสอบผู้บุกรุกประเภท Network-based IDS จะไม่สามารถทำได้ เพราะการส่งสัญญาณเตือนภัยเมื่อตรวจพบพฤติกรรมที่เข้าข่ายการบุกรุกที่เข้ามายังระบบเครือข่ายทั้งหมด จึงมีแต่ Host-based IDS เท่านั้นที่สามารถตัดสินได้ว่าการบุกรุกที่ตรวจพบครั้งนั้นสำเร็จหรือล้มเหลว

- Network-based IDS (NIDS)

ทำงานอยู่บนเครือข่ายจะทำการเฝ้าดูและตรวจสอบข้อมูลแพ็กเก็ตต่างๆจะถูกตรวจสอบโดยตัวตรวจจับหรือเซ็นเซอร์ (Sensor) ของระบบ ซึ่งตัวตรวจจับจะมองเห็นเฉพาะแพ็กเก็ตที่วิ่งผ่านบนเครือข่ายที่ตัวตรวจจับนั้นติดตั้งอยู่เท่านั้น ซึ่งระบบตรวจสอบประเภทนี้สามารถตรวจสอบการบุกรุกได้ทั้งระบบเครือข่าย ไม่เกิดความยุ่งยากในการติดตั้งระบบตรวจสอบผู้บุกรุกบนเครื่องที่ต้องการตรวจสอบทุกเครื่องเหมือน Host-based IDS และการเก็บบันทึกข้อมูล

---

[2] False Negative หมายถึงการที่ IDS ตรวจไม่พบการบุกรุกที่เกิดขึ้นจริง ซึ่งการเกิด False Negative จะให้ผลลัพธ์ที่เลวร้ายกว่า False Positive มาก แต่ก็เป็นการยากที่จะออกแบบ IDS ไม่ให้เกิด False Negative ขึ้น ในขณะที่เราออกแบบให้ระบบมี False Negative ให้น้อยเท่าไหร่ แนวโน้มที่ระบบจะเกิด False Positive ก็มีมากขึ้นเท่านั้น

การบุกรุกที่แยกต่างหาก ทำให้ปลอดภัยจากการทำลายร่องรอยการบุกรุกหลังจากผู้บุกรุกสามารถเข้าสู่ระบบแล้ว

แพ็กเก็ตต่างๆจะเป็นที่สนใจของตัวตรวจจับก็ต่อเมื่อแพ็กเก็ตนั้นเข้ากับรูปแบบที่กำหนดไว้ ซึ่งปกติแล้วรูปแบบจะมีอยู่ 3 ประเภทคือ

1.) รูปแบบทางตัวอักษร (String signature)

ซึ่งอาจบ่งบอกถึงการโจมตี ตัวอย่างเช่น " cat " + + " 7% rhost " อาจทำให้ระบบยูนิกซ์ เกิดช่องโหว่ต่อการโจมตีบนเครือข่ายได้

2.) รูปแบบทางพอร์ต (Port signature)

เป็นการพยายามติดต่อเข้ามาทางพอร์ตที่รู้จักกันดีและมักจะถูกโจมตี เช่น telnet จะใช้ TCP พอร์ต 23, FTP จะใช้ TCP พอร์ต 21/20, SUNRPC ใช้ TCP/UDP พอร์ต 111 และ IMAP จะใช้ TCP พอร์ต 143 ซึ่งถ้าระบบของเราไม่ได้เปิดพอร์ตดังกล่าว แต่มีการพยายามเชื่อมต่อเข้ามา แสดงว่าแพ็กเก็ตดังกล่าว อาจจะมีความประสงค์ร้ายก็ได้

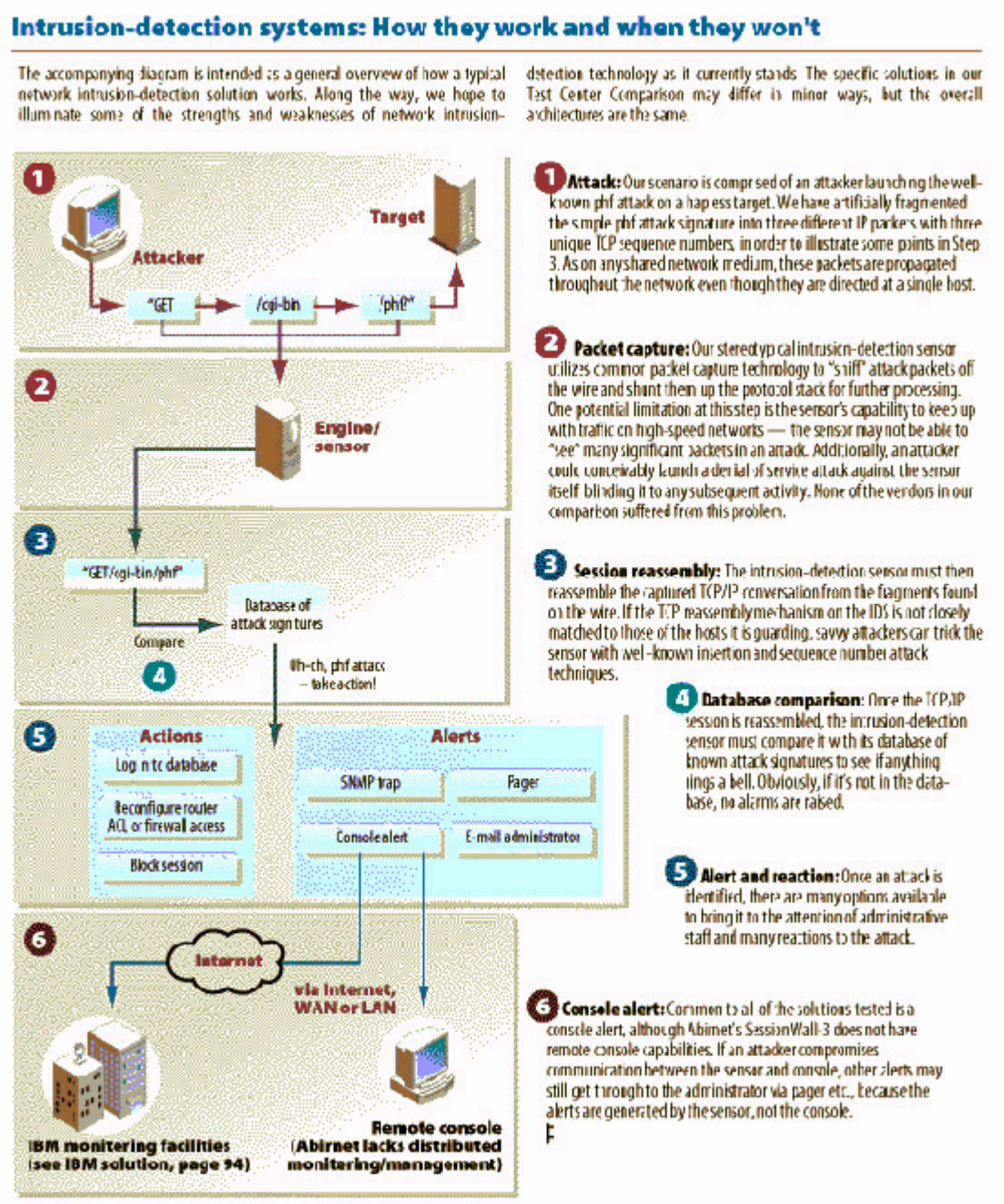
3.) รูปแบบทางเงื่อนไขในส่วนเฮดเดอร์ (Header condition signature)

เป็นพยายามส่งข้อมูลที่มีลักษณะเป็นอันตรายและผิดกฎของการกำหนดคาในส่วนของเฮดเดอร์ ตัวอย่างที่เห็นได้ชัดคือแพ็กเก็ต TCP ซึ่งมีทั้ง SYN และ FIN Flags

2.10.2.3 กลไกระบบตรวจสอบผู้บุกรุก

ระบบตรวจสอบผู้บุกรุกจะทำการวิเคราะห์กิจกรรมต่างที่เกิดขึ้นบนระบบคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์ว่าเป็นการบุกรุกหรือความพยายามในการบุกรุกหรือไม่โดยอาศัยค่าต่างๆ อาทิเช่น Network traffic การใช้งาน CPU, I/O,ไฟล์ หรือที่อยู่ของผู้ใช้ โดยใช้แบ่งวิธีวิเคราะห์หลักๆออกเป็น 2 วิธีคือการตรวจสอบกับข้อกำหนดการใช้งานและการตรวจสอบจากสถิติการใช้งาน

ระบบตรวจจับการบุกรุกโดยทั่วไปจะใช้วิธีตรวจสอบกับข้อกำหนดการใช้งาน ทั้งนี้เนื่องจากมีความง่าย มาก กว่าการตรวจสอบจากสถิติซึ่งมักมีกรณีใหม่เกิดขึ้นตลอดเวลาทำให้การระบุว่าการกระทำนั้นเป็นการบุกรุกมีความยากและอาจเกิดการระบุที่ผิดพลาด (Fault Alarm)



รูปที่ 2.5 แสดงการทำงานของระบบตรวจจับการบุกรุก ที่มา: http://www.infoworld.com

รูปที่ 2.5 แสดงตัวอย่างการทำงานของระบบตรวจสอบการบุกรุกสามารถที่จะอธิบายประกอบแผนภาพได้ดังนี้

1.) ผู้บุกรุกพยายามโจมตีโดยใช้ phf attack

2.) ระบบตรวจสอบการบุกรุกคัดลอกข้อมูลทุกๆแพ็กเก็ตที่วิ่งอยู่บนเครือข่าย

3.) ระบบตรวจสอบการบุกรุกประกอบแพ็กเก็ตทุกๆแพ็กเก็ตเข้าด้วยกัน

4.) ทำการตรวจสอบแพ็กเก็ตที่ประกอบแล้ว ว่ามีลักษณะเป็นความพยายามในการบุกรุกหรือไม่ โดยใช้เทคนิคดังต่อไปนี้

- การตรวจสอบสแตร็คโปรโตคอล Protocol stack

มีการบุกรุกหลายชนิดที่ละเมิดกฎพื้นฐานของการใช้งานโปรโตคอล IP, TCP, UDD และ ICMP เพื่อใช้ประโยชน์ในการบุกรุก เช่น Ping of death หรือ TCP stealth scanning เป็นต้น

- การตรวจสอบ Application Protocol

การบุกรุกบางชนิดใช้ประโยชน์จากจุดบกพร่องในการทำงานของโปรโตคอลบางชนิดเช่นโปรแกรม Winnuke ซึ่งใช้ประโยชน์จากจุดบกพร่องของโปรโตคอล NetBIOS ดังนั้นเพื่อที่จะทำให้เกิดการตรวจสอบที่มีประสิทธิภาพ ระบบตรวจสอบผู้บุกรุกจำเป็นต้องตรวจสอบการใช้งานของโปรโตคอลในชั้น Appication-layer ใหม่ในการตรวจจับพฤติกรรมที่น่าสงสัย

- การสร้างเหตุการณ์ที่สามารถตรวจสอบได้ใหม่

ระบบตรวจสอบผู้บุกรุกอาจใช้เป็นส่วนเสริมในการตรวจสอบเครือข่ายร่วมกับโปรแกรมจัดการเครือข่ายได้ เช่น การเปรียบเทียบล็อกไฟล์ของระบบตรวจสอบผู้บุกรุกซึ่งบันทึกการใช้งานต่างๆบนระบบเครือข่ายไว้ กับล็อกไฟล์ของแต่ละภายในระบบเองเช่น WinNT Event, UNIX Syslog หรือ SNMP TRAPS เป็นต้น ก็จะสามารถวิเคราะห์เหตุการณ์ต่างๆ ที่เกิดขึ้นบนระบบเครือข่ายกับภายในระบบเองได้

5.) ทำการแจ้งเตือนหากพบว่าเป็นการบุกรุก

6.) การแจ้งเตือนอาจกระทำได้หลายทางเช่นการแจ้งเตือนผ่านจอภาพ ผ่านวิทยุติดตามตัวหรือผ่านอิเล็กทรอนิกส์เมล์

2.11 หลักการพื้นฐานของโปรโตคอล TCP/IP

ในการสื่อสารระหว่างมนุษย์นั้น ต้องใช้ภาษาในการสื่อสาร และภาษาที่ใช้ในการสื่อสารนั้นก็มีความแตกต่างกันไปตามเชื้อชาติ การสื่อสารในชนชาติเดียวกันก็ต้องใช้ภาษาเดียวกัน แต่ในการสื่อสารกับชนชาติอื่น ต้องใช้ภาษาที่สามารถเป็นสื่อกลางได้เช่น ภาษาอังกฤษเป็นต้น

คอมพิวเตอร์ก็เช่นกัน ในการที่จะให้คอมพิวเตอร์ทำการติดต่อสื่อสารซึ่งกันและกันได้นั้นก็ต้องใช้ภาษาในการติดต่อสื่อสารเช่นกัน แต่ในทางคอมพิวเตอร์นั้นจะไม่เรียกว่าภาษาแต่จะถูกเรียกว่า โปรโตคอล (Protocol) และเช่นเดียวกันโปรโตคอลที่ใช้ในการสื่อสารของคอมพิวเตอร์ก็มีอยู่หลายโปรโตคอลด้วยกัน การที่จะให้คอมพิวเตอร์สามารถสื่อสารกันได้ก็ต้องใช้โปรโตคอลเดียวกันด้วย และชุดโปรโตคอลที่เป็นมาตรฐานที่ใช้งานทางด้านอินเทอร์เน็ตก็จะเป็นชุดโปรโตคอลที่เรียกว่า TCP/IP

ดังนั้น TCP/IP ก็คือชุดโปรโตคอลที่ถูกพัฒนาขึ้นมาเป็นมาตราฐานในการติดต่อสื่อสารกันระหว่างเครื่องคอมพิวเตอร์ ทำให้เครื่องคอมพิวเตอร์สามารถใช้งานทรัพยากรเช่น แฟ้มข้อมูล หรือ เนื้อที่ไดรว์ร่วมกันได้ โดยผ่านระบบเครือข่าย

ในความเป็นจริงแล้ว TCP/IP ประกอบไปด้วยโปรโตคอลที่แตกต่างกันในหลายชั้นเลเยอร์ด้วยกัน เช่น TCP (Transmission Control Protocol), IP (Internet Protocol) เป็นต้น ซึ่งเป็นโปรโตคอลที่เป็นที่รู้จักและใช้งานกันอย่างแพร่หลาย ดังนั้นในปัจจุบันเมื่อกล่าวถึงการใช้งานอินเทอร์เน็ตจึงมักจะเรียกชุดโปรโตคอลนี้รวมกันว่า TCP/IP

2.11.1 ลำดับชั้นการทำงานของโปรโตคอล

ในการศึกษาหลักการทำงานของโปรโตคอลในระบบเครือข่าย(Network Protocols) ใดๆ จะเริ่มต้นด้วยการมองการทำงานของมันเป็นชั้น ๆ หรือที่เรียกว่าเลเยอร์ (Layer) การทำงานทั้งหมดของโปรโตคอลจะประกอบไปด้วยหลาย ๆ เลเยอร์ซึ่งนำมาวางซ้อนกันได้ออกมาเป็นรูปแบบที่เราเรียกว่า Protocol Stack แต่ละเลเยอร์ก็จะมีหน้าที่การทำงานที่ชัดเจนและไม่เกี่ยวข้องกัน แต่ละชั้นจะรู้เพียงวิธีการส่งข้อมูลไปยังชั้นอื่นๆ จะไม่รู้ถึงการทำงานข้างในเลย แต่ละชั้นจะมีการแบ่งการทำงานออกเป็นโปรโตคอลต่างๆจำนวนไม่เท่ากัน ทำให้เป็นการยากที่จะระบุว่าโปรโตคอลในระบบเครือข่ายโดยรวมแล้วมีทำงานกี่เลเยอร์ แต่ก็มีมาตรฐานที่เป็นที่ยอมรับกันโดยทั่วไป เรียกว่า Open System Interconnect (OSI) Reference Model ซึ่งทำการแบ่งการทำงานของโปรโตคอลในระบบเครือข่ายออกเป็น 7 เลเยอร์ ดังนี้

7	***Application Layer*** Consists of application programs that use the network
6	***Presentation Layer*** Standardizes data presentation to the applications.
5	***Session Layer*** Manages sessions between applications.
4	***Transport Layer*** Provides end-to-end error detection and correction.
3	***Network Layer*** Manages connections across the network for the upper layers.
2	***Data Link Layer*** Provides reliable data delivery across the physical link.
1	***Physical Layer*** Defines the physical characteristics of the network media.

รูปที่ 2.6 โมเดล OSI[3]

แต่ละชั้นก็มีข้อกำหนดและการทำงานที่แน่นอนและไม่เกี่ยวข้องกับชั้นอื่น สำหรับการศึกษาโปรโตคอล TCP/IP นั้นบางที่ก็จะไม่อ้างอิง OSI Reference Model เนื่องจากมีการแบ่งชั้นการทำงานอย่างละเอียดทำให้เข้าใจยาก ดังนั้นจึงมีจะสร้างโมเดลขึ้นมาใหม่เพื่อให้ในการอธิบายการทำงานของโปรโตคอล TCP/IP โดยแบ่งออกเป็น 4 ชั้นดังนี้

[3] Obert N. Myhre, CCNA Certification: Routing Basics for Cisco Crtified Ntwork Associates Exam 640-407 (NJ : Prentice Hall PTR, 1999), pp. 6

Application Layer	Telnet, FTP, e-mail, etc
Transport Layer	TCP, UDP
Internet Layer	IP, ICMP, IGMP
Link Layer	Device driver and interface card

รูปที่ 2.7 โมเดล Internet Reference TCP/IP[4]

1.) เลเยอร์ Application ทำหน้าที่จัดการเกี่ยวกับแอพริเคชันหรือโปรแกรมต่างๆที่ถูกใช้งานโดยผู้ใช้ ตัวอย่างของแอพริเคชันที่ใช้งานโดยทั่วไป เช่น

- Telnet หรือ Remote login เป็นบริการให้ผู้ใช้งานสามารถเรียกใช้งานเครื่องคอมพิวเตอร์จากเครื่องคอมพิวเตอร์ที่อยู่ห่างออกไปได้
- FTP (File Transfer Protocol) เป็นบริการในการโอนถ่ายแฟ้มข้อมูลระหว่างเครื่องคอมพิวเตอร์
- SMTP (Simple Mail Transfer Protocol) เป็นบริการในการรับ-ส่งจดหมายอิเล็กทรอนิกส์
- DNS (Domain Name Service) เป็นบริการแปลงชื่อจากรูปแบบของโดเมนเนม เช่น cmu.chiangmai.ac.th เป็นแบบไอพีแอดเดรส เช่น 202.28.249.1 หรือทำกลับกันในการแปลงไอพีแอดเดรสไปเป็นชื่อโดเมนเนม
- NFS (Network File System) เป็นบริการในการใช้ทรัพยากร เช่น แฟ้มข้อมูลหรือเนื้อที่ระหว่างเครื่องคอมพิวเตอร์ผ่านระบบเครือข่าย

2.) เลเยอร์ Transport ทำหน้าที่ในการจัดเตรียมช่องทางในการส่งผ่านข้อมูลของเลเยอร์ Application ระหว่างโฮสต์ ในเลเยอร์ Transport นี้ยังแบ่งออกเป็น 2 โปรโตคอล ได้แก่

- UDP (User Datagram Protocol)

มีหน้าที่เพียงแค่ทำการจัดส่งข้อมูลที่เรียกว่า Datagram ไปยังโฮสต์ปลายทางโดยไม่มีการตรวจสอบกับปลายทางว่ามีผู้รับหรือไม่ ดังนั้น Datagram ที่ถูกส่งไปอาจจะไม่ถึงปลายทางก็ได้ โดยปกติแล้วถ้าหากใช้โปรโตคอลนี้แล้วต้องการตรวจสอบว่าข้อมูลถึงปลายทางจริงหรือไม่ จะให้โปรแกรมในเลเยอร์ Application ทำหน้าที่ในการตรวจสอบแทน

---

[4] W. Richard Stevens, TCP/IP Illustrated, Volume 1 The Protocols (Bangalore : Addison Wesley Longman, Inc, 1999), pp. 6

- TCP (Transmission Connection Protocol)

มีหน้าที่ในการจัดเตรียมเกี่ยวกับความถูกต้องแน่นอนของข้อมูลระหว่างโฮสต์ มีการตรวจสอบข้อมูลระหว่างต้นทางและปลายทาง รวมถึงการจัดการแบ่งข้อมูลจากแอพริเคชันให้มีขนาดพอเหมาะกับเลเยอร์ Network กำหนด Time out ของสัญญาณตอบรับจากโฮสต์ปลายทาง และอื่นๆ

3.) เลเยอร์ Network หรือเรียกอีกชื่อหนึ่งว่าเลเยอร์ Internet ทำหน้าที่จัดการเกี่ยวกับการส่งผ่านข้อมูลไปมาของแพ็กเก็ตในเครือข่ายหรือทำการจัดการเกี่ยวกับการหาเส้นทาง (Routing) นั้นเอง โปรโตคอลในเลเยอร์นี้ได้แก่

- IP (Internet Protocol)

เป็นโปรโตคอลหลักที่ทำงานอยู่ในโปรโตคอล TCP/IP ทำหน้าที่ในการติดต่อกับโปรโตคอลต่างๆทั้ง TCP, UDP, ICMP, และ IGMP ในรูปของไอพีดาตาแกรม (IP Datagram) ซึ่งการส่งข้อมูลนั้นจะเป็นการส่งแบบ Connectionless คือจะไม่มีการตรวจสอบปลายทางว่ามีผู้รับหรือไม่ โปรโตคอล IP จะทำหน้าที่เพียงส่งข้อมูลแต่ละดาตาแกรมออกไป และถ้าหากเกิดความผิดพลาดบางอย่างเช่น เกิดปัญหาที่เราเตอร์ก็จะทำเพียงแค่การส่งข้อความด้วย ICMP กลับไปบอกแก่ต้นทางเท่านั้น การตรวจสอบข้อมูลจะเป็นหน้าที่ของเลเยอร์ที่อยู่สูงกว่าขึ้นไป

- ICMP (Internet Control Message Protocol)

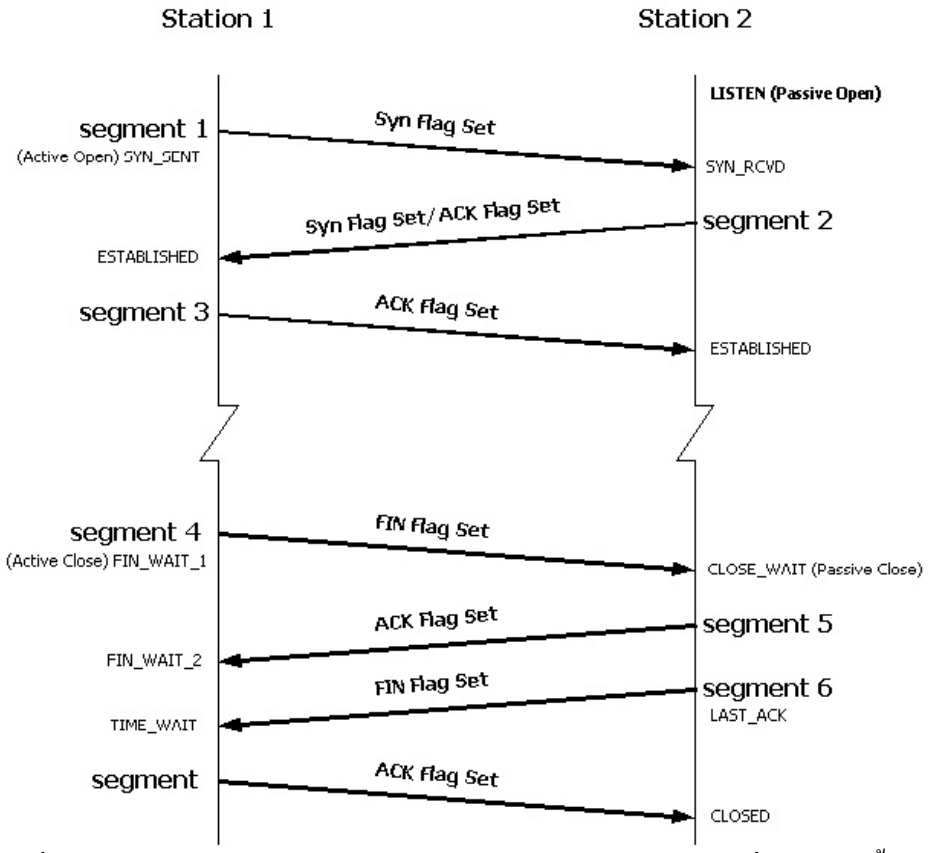
เป็นส่วนประกอบของ IP ซึ่งถูกใช้โดยเลเยอร์ IP ในการเปลี่ยนข้อมูลความผิดพลาดที่สำคัญต่างๆ อันเกิดจากเลเยอร์ IP ของโฮสต์หรือเราเตอร์ต่างๆ ให้เป็นข้อความโดยปกติแล้ว ICMP จะถูกใช้โดยเลเยอร์ IP แต่ก็สามารถถูกใช้โดยเลเยอร์ Application ก็ได้ ตัวอย่างเช่น โปรแกรม Ping และ Traceroute ซึ่งคำสั่งทั้งคู่เป็นแอพริเคชันที่ใช้โปรโตคอล ICMP

- IGMP (Internet Group Management Protocol)

เป็นโปรโตคอลที่ถูกใช้งานโดยโฮสต์และเราเตอร์ที่สนับสนุนการทำงานแบบมัลติแทสกิง (Multicasting) ทำหน้าที่ในการเก็บและส่งข้อมูลเกี่ยวกับมัลติแทสกิงกรุ๊ปของโฮสต์ต่างๆในระบบเครือข่าย โปรโตคอล IGMP เป็นโปรโตคอลที่คล้ายกับ ICMP คือเป็นโปรโตคอลที่เป็นส่วนประกอบของเลเยอร์ IP และข้อมูลถูกส่งออกสู่เครือข่ายด้วยไอพีดาตาแกรม จุดที่แตกต่างจากโปรโตคอลอื่นๆคือ IGMP message จะมีขนาดคงที่เสมอ

4.) เลเยอร์ Link หรือเรียกอีกชื่อหนึ่งว่าเลเยอร์ Data-link โดยปกติแล้วจะหมายถึงไดฟ์เวอร์ของอุปกรณ์ ระบบปฏิบัติการ เน็ตเวิร์คอินเตอร์เฟสการ์ด (Network Interface Card) ของคอมพิวเตอร์ รวมถึงรายละเอียดเกี่ยวกับเคเบิ้ลอินเตอร์เฟส (Cable Interface) ด้วย

2.11.2 สถานะของโปรโตคอล TCP ในการเชื่อมต่อการทำงาน



รูปที่ 2.8 แสดงลำดับและสถานะต่างๆของโปรโตคอล TCP ในการเริ่มต้นและสิ้นสุดการเชื่อมต่อ[5]

[5] W. Richard Stevens, TCP/IP Illustrated, Volume 1 The Protocols (Bangalore : Addison Wesley Longman, Inc, 1999), pp. 242

3-Character abbreviation	คำอธิบาย
URG	The urgent pointer is valid
ACK	The acknowledgement number is valid
PSH	Push data to receiving process as soon as possible
RST	Reset connection
SYN	Synchronize sequence numbers
FIN	Sender is finished sending data

ตารางที่ 2.2 แสดง Flag การทำงานของโปรโตคอล TCP ที่สถานะต่างๆ[6]

[6] Ibid., pp.225-230