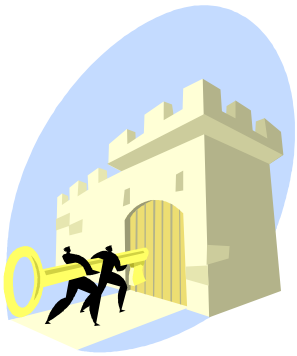


ประตูที่มองไม่เห็น (Invisible Gate)

น.ต.ไกรสิทธิ์ มหิวรรณ
อาจารย์ฝ่ายศึกษา โรงเรียนนายเรือ

โรงเรียนนายเรือตั้งอยู่ริมถนนสุขุมวิท ด้านริมถนนถูกกั้นด้วยกำแพงขาวทึบ ความสูงนั้นยากที่จะปีนข้ามได้ ส่วนอีกด้านก็อยู่ติดแม่น้ำเจ้าพระยาโดยมีเขื่อนเล็ก ๆ กั้นอยู่ ข้าราชการหรือบุคคลพลเรือนโดยส่วนใหญ่แล้ว เมื่อต้องการเข้ามาในพื้นที่โรงเรียนนายเรือก็จะเข้ามาจากทางด้านถนนสุขุมวิท (ยกเว้นข้าราชการที่นั่งเรือด่วนธุรการมาขึ้นที่ท่าเรือด้านฝั่งแม่น้ำเจ้าพระยา) โดยสามารถเข้าได้สองทางคือทางประตูกลางซึ่งเป็นประตูหลักสำหรับผ่านเข้าออก มื่อผ่านเข้ามาทางประตูนี้ก็จะเข้าสู่พื้นที่หลักของโรงเรียนนายเรือได้ทันที และจะมีตึกกองบัญชาการตั้งอยู่ด้านหน้าหลังจากที่ได้ผ่านประตูเข้ามาแล้ว ส่วนอีกทางหนึ่งก็คือเข้าทางประตูด้านทิศเหนือซึ่งเป็นประตูที่อยู่ติดกับอาคารโรงพลศึกษา ประตูด้านนี้จะเป็นประตูที่สามารถผ่านเข้ามายังสโมสรสัญญาบัตร โรงพยาบาลโรงเรียนนายเรือ และแผนกขนส่งโรงเรียนนายเรือ หากต้องการผ่านเข้ามายังพื้นที่หลักภายในโรงเรียนนายเรือก็จะต้องผ่านประตูด้านในอีกชั้นหนึ่งซึ่งเป็นประตูที่อยู่ติดกับอาคารกองวิชาวิศวกรรมศาสตร์

การผ่านเข้าออกประตูต่าง ๆ นั้นผู้ผ่าน เข้าออกจะต้องถูกตรวจสอบเพื่อการรักษาความปลอดภัยตามมาตรการรักษาความปลอดภัยที่มีอยู่ไม่ว่าจะเป็นการตรวจสอบบัตรอนุญาตผ่านเข้า-ออกที่ติดอยู่ที่ยานพาหนะ การตรวจสอบบัตรประจำตัว หรือการแลกเปลี่ยนบัตรประจำตัว หากมีผู้ไม่ประสงค์ดีต้องการเข้ามาเพื่อที่จะเข้าถึงเอกสารหรือข้อมูลที่เป็นความลับของโรงเรียนนายเรือ สามารถกระทำได้ยากเนื่องจากถูกตรวจสอบเบื้องต้นขณะที่ผ่านเข้า-ออก นอกจากนั้นที่อาคารสำนักงานต่าง ๆ ก็ยังมีผู้ที่เข้าหน้าที่เวรยามอยู่ประจำอาคาร ข้อมูลและเอกสารลับ ก็จะถูกเก็บไว้ในห้องหรือสถานที่เข้าถึงได้ยากมีการป้องกันอย่างแน่นหนา และหากเข้ามาในช่วงเวลาราชการก็ยิ่งเป็นไปไม่ได้ที่ผู้ไม่ประสงค์ดีจะเดินค้นหาสิ่งที่ต้องการได้อย่างอิสระเนื่องจากมีข้าราชการปฏิบัติงานอยู่ หากเข้ามานอกเวลาราชการก็มีเวรยามและมีการล็อคป้องกันห้องและสถานที่อย่างแน่นหนา ตู้เก็บเอกสารต่าง ๆ ที่สำคัญก็มีการเก็บอย่างมิดชิด ดังนั้น ถือได้ว่าการที่จะเข้าถึงเอกสารและข้อมูลลับของโรงเรียนนายเรือโดยทางกายภาพมีความยากลำบาก

แต่มีสิ่งหนึ่งที่หลายคนมองข้ามไปนั่นคือโรงเรียนนายเรือยังมีประตูที่สามารถเป็นทางผ่านเข้าออกได้อีกทางหนึ่ง นั่นคือประตูสู่โลกอินเทอร์เน็ต (Internet Gateway) ผู้ใช้อินเทอร์เน็ตที่อยู่ภายในใช้ประตูนี้เป็นประตู **“ออก”** สู่โลกอินเตอร์เน็ตโดยไม่ได้มองเห็นว่ามีผู้ใดเดินสวนทางเข้ามาด้านในหรือไม่มีผู้ใช้อินเทอร์เน็ตภายนอกที่ใช้ประตูนี้เป็นประตูทาง **“เข้า”** สู่โรงเรียนนายเรือโดยด้านหลังของประตูนี้ในสายตาของผู้อยู่ภายนอกก็คือสิ่งที่โรงเรียนนายเรือต้องการแสดงให้กับคนเหล่านั้นเห็น ละสิ่งนั้นคือเว็บเพจที่รวบรวมข้อมูลที่ไม่ได้เป็นความลับทางราชการของโรงเรียนนายเรือ สามารถเปิดเผยแก่บุคคลภายนอกรับรู้ได้ แต่อย่างไรก็ตามยังมีบุคคลบางกลุ่มที่อาศัยประตูนี้โดยอาศัยความรู้เฉพาะทางพยายามจะเข้าถึงพื้นที่ ๆ โรงเรียนนายเรือไม่ประสงค์ให้บุคคลภายนอกรับรู้ สามารถเข้าถึงข้อมูลหรือเอกสารลับ ต่าง ๆ ของทางราชการ แม้ว่าหน่วยงานภายในโรงเรียนนายเรือเองไม่ประสงค์ที่จะให้มีพื้นที่ดังกล่าวเกิดขึ้น แต่บุคคลผู้ไม่ประสงค์ดีเหล่านั้นก็ได้อาศัยความรู้เฉพาะทางที่มีอยู่เข้าถึงพื้นที่ ๆ แม้แต่เจ้าของเองยังไม่ทราบว่าบ้านตนเองนั้นถูกเข้าถึงได้

เมื่อเครื่องคอมพิวเตอร์ที่อยู่ภายในเครือข่ายของโรงเรียนนายเรือถูกเข้าถึงแล้วเกี่ยวข้องอย่างไรกับเอกสารหรือข้อมูลที่เป็นความลับ? นี่อาจจะเป็นคำถามที่บางคนสงสัย เนื่องจากในปัจจุบันเครื่องคอมพิวเตอร์ เข้ามามีบทบาทสำคัญในชีวิตประจำวัน เครื่องคอมพิวเตอร์ถูกนำมาใช้เป็นอุปกรณ์มาตรฐานในสำนักงานในหน่วยงานแทบจะทุกหน่วยงาน นำมาใช้ในด้านงานธุรการ ในงานเอกสาร และใช้เตรียมการเรียนการสอนสำหรับอาจารย์ ดังนั้นงานเอกสารต่าง ๆ ที่เกิดขึ้นในหน่วยงานเกือบทุกฉบับถูกทำขึ้นมาจากเครื่องคอมพิวเตอร์ในสำนักงาน

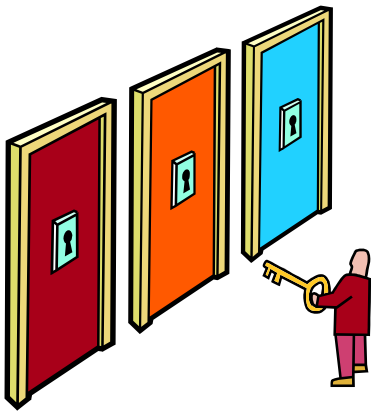
เอกสารลับหรือไม่ลับ ข้อมูลด้านกำลังพล ข้อมูลทางด้านงบประมาณของหน่วย ข้อมูลหรือแผนการปฏิบัติไม่ว่าจะเป็นแผนการฝึกภาคทางทะเลของนักเรียนนายเรือ แผนการจัดซื้อจัดจ้าง หรือแม้กระทั่งข้อสอบที่อยู่ในเครื่องคอมพิวเตอร์ของอาจารย์ และถึงแม้ข้อมูล เหล่านี้จัดทำต้นฉบับที่เป็นฮาร์ดก็อปปี้และทำการประทับตราเอกสาร “ลับ” “ลับมาก” แล้วก็ตามจะมีสักกี่คนที่ลบไฟล์เอกสารต้นฉบับใน เครื่องคอมพิวเตอร์ทิ้ง

นอกจากนั้นก็มีบ่อยครั้งที่ได้มีการแชร์ข้อมูลกันระหว่างเครื่องคอมพิวเตอร์ทิ้งไว้ก็ทำให้ผู้อื่นสามารถเข้าถึงเอกสารได้อย่างง่ายดาย ถึงแม้บางคนไม่ได้แชร์แหล่งข้อมูลของตนเองไว้ จึงคิดว่าข้อมูลในเครื่องคอมพิวเตอร์ของตนเองปลอดภัยแต่ไม่แน่นอนเสมอไป เพราะยังมีวิธีการอีกมากที่สามารถทำให้

ผู้อื่นเข้าถึงแหล่งข้อมูลบนเครื่องคอมพิวเตอร์ที่ต้องการได้ โดยที่เจ้าของเครื่องคอมพิวเตอร์เองไม่สามารถทราบได้ว่าเครื่องคอมพิวเตอร์ของตนเองกำลังถูกเข้าถึงโดยบุคคลภายนอก ข้อดีอีกประการสำหรับผู้ไม่ประสงค์ดีที่การพยายามเข้าถึงข้อมูลภายในโรงเรียนนายเรือโดยใช้ประตูที่มองไม่เห็นนี้ คือผู้ที่พยายามเข้าถึงมีเวลาในการพยายามเข้าถึงที่ไม่จำกัดสามารถใช้เวลาตลอด ๒๔ ชั่วโมงหรือนานเท่าที่เครื่องคอมพิวเตอร์เป้าหมายเปิดไว้พร้อมกับการเชื่อมต่อ กับอินเทอร์เน็ต ซึ่งต่างจากการเข้ามาทางกายภาพหากถูกจับได้ก็สิ้นสุดการพยายามแต่การเข้าทางประตู ที่มองไม่เห็นนี้สามารถถูกตรวจจับได้ยากและหากถูกจับได้ก็หาตัวได้ยากและหากหาตัวได้ก็ยังขาดกฎหมาย ในการเอาผิดผู้ไม่ประสงค์ดีอีก

ความเป็นมาของประตูที่ไม่ลับแต่มองไม่เห็น

เมื่อศูนย์คอมพิวเตอร์โรงเรียนนายเรือยังตั้งอยู่ที่อาคารเรียน ๒ ในขณะนั้นผู้เขียนได้เข้าไปมีส่วนร่วมในการเป็นเจ้าหน้าที่ของศูนย์คอมพิวเตอร์อีกหน้าที่หนึ่ง ซึ่งเพิ่มจากหน้าที่ประจำในฐานะอาจารย์ในกองวิชาวิศวกรรมเครื่องกลเรือ ในขณะนั้นโรงเรียนนายเรือมีช่องสัญญาณการเชื่อมต่ออินเทอร์เน็ตสู่ภายนอกเพียง 64 kbits/s ซึ่งนับว่าน้อยมากสำหรับการใช้งานทั้งหน่วยงาน อีกทั้งระบบเครือข่ายภายในก็ยังมีการเชื่อมต่อไม่มากนัก มีหลายครั้งที่เว็บไซต์ของโรงเรียนนายเรือถูกโจมตี โดยผู้ไม่ประสงค์ดี และเป็นการโจมตีเข้ามาที่เครื่องแม่ข่าย เพื่อเปลี่ยนแปลงข้อมูลในเว็บไซต์จึงถือว่ายังไม่ทำความเสียหายให้แก่หน่วยงานมากเท่าใดนักสามารถแก้ไขให้กลับมาเหมือนเดิมได้ เนื่องจากโรงเรียนนายเรือมีช่องสัญญาณ เชื่อมต่อที่ต่ำยังไม่เป็นที่ดึงดูดใจเหล่าบรรดาผู้ไม่ประสงค์ดีเท่าใดนักจึงไม่เกิดความเสียหายที่รุนแรงในขณะนั้น



เมื่อศูนย์คอมพิวเตอร์ย้ายมายังอาคารเรียน ๖ อาคารกองวิชาวิศวกรรมเครื่องกลเรือ จึงมีการปรับเปลี่ยนระบบเพื่อให้สามารถรองรับการใช้งานให้เหมาะสมขึ้นโดยเริ่มจากเปลี่ยนระบบปฏิบัติการของเครื่องแม่ข่ายและลูกข่ายไปใช้ระบบปฏิบัติการที่สามารถควบคุมการใช้งาน และสิทธิการเข้าถึงแหล่งข้อมูลต่างๆ โดยเฉพาะในห้องบริการคอมพิวเตอร์ เพื่อควบคุมไม่ให้นักเรียนนายเรือเข้าถึงเครื่องคอมพิวเตอร์เครื่องอื่น ๆ ในระบบเครือข่ายได้ ป้องกันการใช้งานเครื่องคอมพิวเตอร์ในทางที่ไม่เหมาะสมหรือไม่

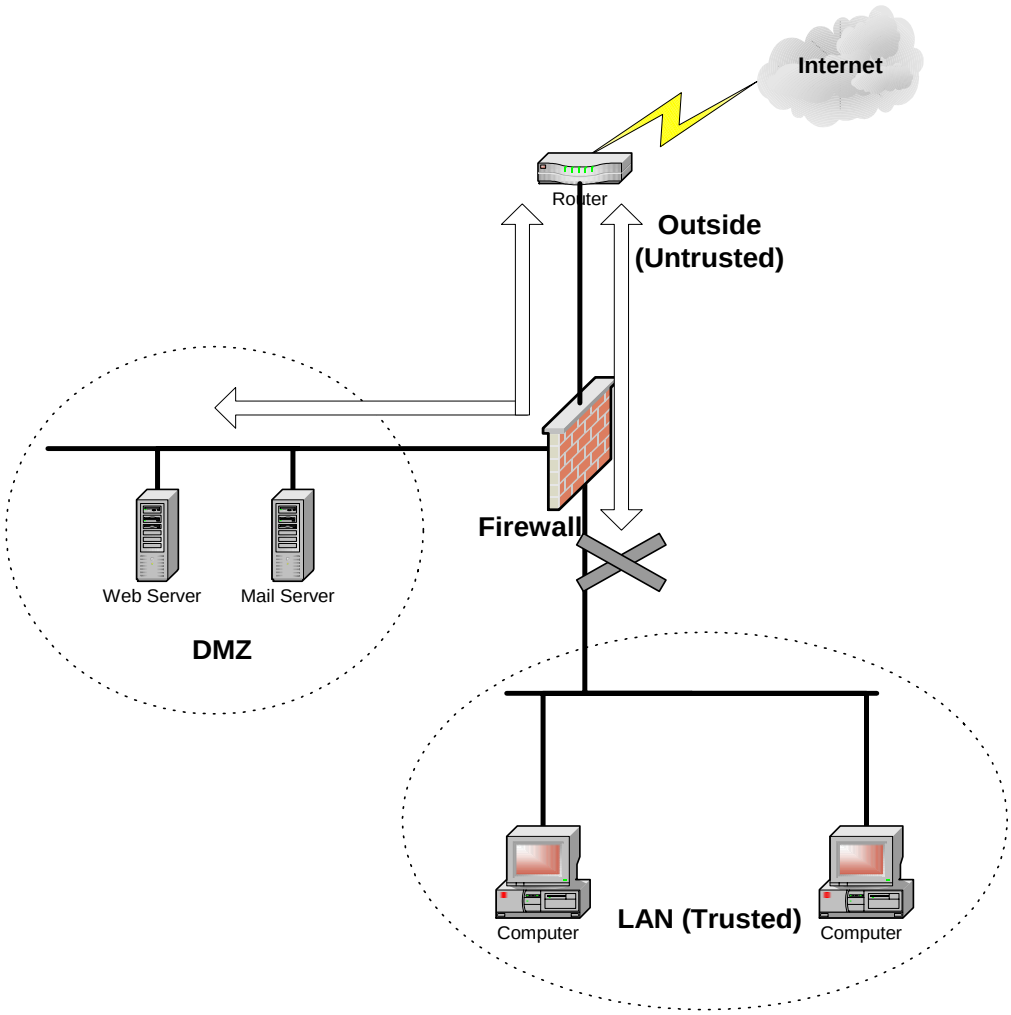
เกี่ยวข้องกับการศึกษา เปลี่ยนระบบพร็อกซี่เซิร์ฟเวอร์จากเดิมที่ใช้พร็อกซี่เซิร์ฟเวอร์ของระบบปฏิบัติการเก่าที่ไม่สามารถควบคุมการใช้งานได้เท่าใดนัก เป็นพร็อกซี่เซิร์ฟเวอร์รุ่นใหม่ของค่ายไมโครซอฟท์ที่ให้มาทดลองใช้ ปรากฏว่าสามารถใช้งานได้ดีเมื่อรวมกับช่องสัญญาณเชื่อมต่ออินเทอร์เน็ตที่มีความเร็วสูงขึ้นเป็น 128 kbps ทำให้การใช้งานในระบบเครือข่ายดีขึ้น แต่ระบบพร็อกซี่ดังกล่าวยังขาดคุณสมบัติในการกำหนดสิทธิในการใช้งานของผู้ใช้ โดยห้ามการเข้าถึงเว็บไซต์ที่ไม่เหมาะสมต่าง ๆ หากไม่กำหนดการใช้งานดังกล่าวก็จะทำให้ผู้ที่ต้องการใช้งาน เพื่อประโยชน์ทางด้านการศึกษาต้องประสบปัญหาความล่าช้าในการใช้งาน อีกทั้งระบบที่ใช้อยู่เป็นรุ่นทดลองใช้และจะหมดอายุการใช้งานจึงได้ทำการเปลี่ยนระบบพร็อกซี่เซิร์ฟเวอร์มาใช้ระบบพร็อกซี่เซิร์ฟเวอร์ที่สามารถใช้งานได้โดยไม่ต้องเสียค่าใช้จ่าย และมีขีดความสามารถตามที่ต้องการนั่นคือระบบพร็อกซี่เซิร์ฟเวอร์ที่รันอยู่บนระบบปฏิบัติการลีนุกส์

ผู้เขียนได้ทำการติดตั้งระบบพร็อกซี่เซิร์ฟเวอร์ขึ้นมาสามเครื่องให้ทำงานในลักษณะสมดุลภาระซึ่งกันและกัน (Load balancing) พร้อมกับได้ทำการจำกัดการเข้าถึงเว็บไซต์ที่ไม่เหมาะสมบางประเภท เช่น เว็บการพนัน เว็บเกี่ยวกับสิ่งเสพติด เว็บเกี่ยวกับความรุนแรง และเว็บเกี่ยวกับภาพลามกอนาจาร (รวมแล้วมากกว่าหนึ่งแสนเว็บไซต์) หลังจากได้ใช้งานระบบใหม่ทำให้การใช้งานอินเทอร์เน็ตมีความคล่องตัวขึ้น แต่เมื่อช่องสัญญาณในการเชื่อมต่อเร็วขึ้นปัญหาที่ตามมาก็คือเครื่องแม่ข่ายและเครื่องคอมพิวเตอร์ในระบบเครือข่ายถูกผู้ไม่ประสงค์ดีเข้ามาโจมตีบ่อยขึ้น

โดยเฉพาะเครื่องแม่ข่ายที่ใช้ระบบปฏิบัติการของบริษัทยักษ์ใหญ่ในวงการคอมพิวเตอร์ถูกทั้งบรรดาผู้ไม่ประสงค์ดีเข้ามาเปลี่ยนแปลงแก้ไขสิ่งต่าง ๆ มากมาย บนเครื่องคอมพิวเตอร์ในระบบเครือข่ายและยังถูกบรรดาหนอนอินเทอร์เน็ตจากระบบเครือข่ายภายนอก เจาะทะลุผ่านประตูที่มองไม่เห็นนี้เข้ามาภายในระบบเครือข่าย ทำให้ระบบเครือข่ายประสบปัญหาใช้การไม่ได้บ่อยครั้ง และในขณะนั้นโรงเรียนนายเรือกำลังจะได้รับการเพิ่มช่องสัญญาณจาก 128 kbps ให้เป็น 1024 kbps ซึ่งจะเร็วกว่าของเดิมถึง ๘ เท่า (ปัจจุบัน 512 kbps) หากช่องสัญญาณได้เพิ่มขึ้นดังกล่าวแล้วปัญหาที่ประสบอยู่ก็จะทวีความรุนแรงมากขึ้น และที่สำคัญระบบเครือข่ายภายในโรงเรียนนายเรือก็ได้ขยายตัวโดยมีเครื่องคอมพิวเตอร์เชื่อมต่อกับระบบเครือข่ายหลักมากขึ้นด้วย หากยังคงถูกบุกรุกระบบเครือข่ายโดยที่ไม่มีเครื่องมือป้องกันหรือตรวจสอบได้ก็จะทำให้เกิดปัญหาที่รุนแรงมากยิ่งขึ้น

ช่วงเวลาดังกล่าวเครื่องคอมพิวเตอร์ของผู้เขียนเองก็โดนแฮกเกอร์เข้ามาบุกรุกโดยได้ทำการเปลี่ยนสิทธิ์ของบัญชีผู้ใช้งานที่ไม่มีสิทธิ์ให้มีสิทธิ์เยี่ยงผู้ดูแลระบบบนเครื่องคอมพิวเตอร์ หมายความว่าผู้บุกรุกสามารถเข้าถึงทุกอย่างภายในเครื่องคอมพิวเตอร์ และควบคุมเครื่องคอมพิวเตอร์ดังกล่าวนี้ได้อย่างเต็มความสามารถ ซึ่งเป็นตัวอย่างได้เป็นอย่างดีว่ามีการบุกรุกเกิดขึ้นภายในระบบเครือข่าย ผู้เขียนจึงได้ทำการติดตั้งระบบกำแพงไฟ (Firewall) (เพื่อการรักษาความปลอดภัยผู้เขียนขอข้ามรายละเอียดและชนิดของระบบกำแพงไฟ) ขึ้นมาพร้อมทั้งแบ่งแยกกลุ่มของระบบเครือข่ายที่เป็นระบบเครือข่ายภายใน

และกลุ่มของระบบเครือข่ายที่สามารถให้ผู้ใช้งานอินเทอร์เน็ตจากภายนอกเข้าถึงได้ออกจากกัน โดยกลุ่มของระบบเครือข่ายภายใน (LAN or Trusted Zone) นั้นจะกำหนดให้เครือข่ายภายนอกไม่สามารถเข้าถึงได้ ส่วนกลุ่มของระบบเครือข่ายที่ให้บริการต่าง ๆ (Demilitarized zone, DMZ) เช่น เว็บไซต์ของโรงเรียนนายเรือ ระบบจดหมายอิเล็กทรอนิกส์ เป็นต้น ให้ระบบเครือข่ายภายนอกเข้าถึงได้เฉพาะบริการที่จำเป็นเท่านั้น ดังรูปที่ ๑



รูปที่ ๑

จากที่กล่าวมาข้างต้นแสดงให้เห็นว่าประตูเข้าสู่โรงเรียนนายเรือที่ไม่สามารถมองเห็นได้แต่ไม่ลับนี้เกิดขึ้นตั้งแต่โรงเรียนนายเรือเริ่มมีระบบเครือข่ายเชื่อมต่อกับระบบเครือข่ายภายนอกแต่ในเบื้องต้นนั้นประตูยังเล็กและแคบยังไม่มีสิ่งของมีค่าเท่าใดนักอยู่ภายในบ้านจึงไม่ค่อยมีผู้คนสนใจนัก แต่หลังจากนั้นไม่นานประตูก็เปิดกว้างขึ้นผู้คนที่ผ่านไปผ่านมาเริ่มให้ความสนใจภายในบ้านมากขึ้น ข้าวของภายในบ้าน

ก็เริ่มเพิ่มมากขึ้นถึงแม้จะถูกเก็บไว้มิดชิดอย่างไรก็ตามก็ยังเป็นที่ดึงดูดให้ผู้คนที่ผ่านไปมาพยายามที่จะเสาะแสวงหาสิ่งต่าง ๆ ภายในบ้านโดยเฉพาะบ้านที่เปิดประตูทิ้งไว้และไม่มียามเฝ้าสามารถผ่านเข้า-ออกได้โดยอิสระ เมื่อเข้ามาแล้วหาสิ่งที่ต้องการไม่พบก็กลับออกไปหากมีเวลาก็กลับเข้ามาหาใหม่ใช้วิธีการใหม่หาสิ่งที่ต้องการในที่ใหม่หรือในบางครั้งก็ใช้เวลาหาได้ทั้งวัน **การนำระบบกำแพงไฟมาใช้เปรียบเสมือนการปิดประตูบ้านไม่ให้คนแปลกหน้าเข้ามาภายในได้ และจัดให้มีระบบตรวจสอบผู้ที่ผ่านเข้าออกประตูโดยให้ผ่านได้เฉพาะบุคคลบางกลุ่ม ซึ่งสามารถเพิ่มความปลอดภัยให้แก่สิ่งของที่อยู่ภายในบ้านได้**

มีระบบกำแพงไฟแล้วปลอดภัยหรือไม่?

เมื่อมีระบบกำแพงไฟป้องกันแล้วก็น่าจะมีความปลอดภัยจากผู้บุกรุก จากที่กล่าวในข้างต้นการติดตั้งระบบกำแพงไฟเปรียบเสมือนการปิดประตูและตรวจสอบให้ผ่านได้เฉพาะบางกลุ่ม และเข้าสู่พื้นที่กำหนดให้เท่านั้น ผู้เขียนขอยกตัวอย่างบ้านหลังหนึ่งที่จัดงานเลี้ยงแล้วอนุญาตให้แขกที่มาร่วมงานสามารถเข้าไปในบริเวณห้องโถงที่ใช้สำหรับจัดงานได้อย่างอิสระและปิดห้องอื่น ๆ ทั้งหมด ไม่อนุญาตให้แขกเดินขึ้นไปยังชั้นสองของบ้าน หากมีขโมยที่อาศัยโอกาสนี้ปลอมเป็นแขกเข้ามาในงานผ่านประตูบ้านเข้ามาได้แล้วพยายามแอบขึ้นไปบนชั้นที่สองของบ้านเพื่อเข้าไปยังห้องต่าง ๆ โดยอาศัยสารพัดเครื่องมือ เช่น กุญแจผี ไขควง สว่าน เพื่อที่จะเจาะเข้าไปในห้องที่ต้องการ หรือตัวอย่างบ้านที่ปิดประตูปิดหน้าต่างก็ยังถูกโจรกรรมได้อยู่บ่อยครั้ง ในกรณีตัวอย่างแรกก็เหมือนที่โรงเรียนนายเรือได้จัดทำเว็บไซต์ให้บุคคลภายนอกหรือแขกสามารถเข้ามาชมได้อย่างอิสระ แต่ก็อาจจะมีบุคคลบางกลุ่มพยายามที่จะอาศัยช่องทาง เหล่านั้นหรือช่องทางอื่นเข้าสู่พื้นที่หวงห้ามตลอดเวลา แต่สิ่งที่แตกต่างอีกอย่างคือในกรณีงานเลี้ยงขโมยไม่สามารถใช้วิธีการที่รุนแรงเช่นใช้ค้อนทุบประตูเข้าไปในห้องได้เพราะเจ้าของบ้านที่อยู่บริเวณนั้นจะได้ยิน แต่ในกรณีของระบบเครือข่ายภายในของโรงเรียนนายเรือเปรียบเสมือนเจ้าของบ้านออกไปทำงานต่างจังหวัดดังนั้นขโมยจะใช้วิธีการใดก็ได้ในการพยายามที่จะเข้าสู่พื้นที่หวงห้าม ขโมยสามารถใช้ระเบิดพังประตูเข้าสู่พื้นที่ภายในได้แล้วหยิบฉวยสิ่งที่ต้องการโดยเจ้าของบ้านจะกลับมาเห็นว่า ของบางอย่างถูกหยิบหรือขโมยออกไปเมื่อเวลาผ่านไปนานแล้วและไม่สามารถที่จะตามจับขโมยนั้นได้

การมีระบบกำแพงไฟขึ้นในระบบเครือข่ายเป็นเพียงวิธีการหนึ่ง เพื่อเพิ่มความปลอดภัยให้แก่ระบบเครือข่ายภายในแต่ไม่ได้หมายความว่าระบบเครือข่ายภายในจะมีความปลอดภัยหนึ่งร้อยเปอร์เซ็นต์ ยังมีวิธีการอีกหลายวิธีการที่ผู้อื่นทราบแต่เรายังไม่มีผู้เชี่ยวชาญในเรื่องดังกล่าว อีกทั้งหากต้องการเพิ่มความปลอดภัยก็จะต้องมีการเฝ้า และตรวจสอบการเข้า-ออกระบบเครือข่ายอยู่ตลอดเวลาหรืออย่างน้อยต้องสม่ำเสมอในช่วงเวลาที่เหมาะสม

รู้ได้อย่างไรว่ามีผู้พยายามบุกรุก?

จากการที่ได้ติดตั้งระบบกำแพงไฟซึ่งเปรียบเสมือนการปิดประตู แล้วจำกัดการผ่านเข้าออกนั้น ระบบดังกล่าวทำงานโดยการตรวจสอบว่าข้อมูลที่ผ่านเข้า - ออกนั้นเป็นข้อมูลที่ประสงค์จะให้ผ่านได้หรือไม่ ถ้าให้ผ่านได้ก็อนุญาต แต่ถ้าเป็นข้อมูลที่อยู่ในกลุ่มที่ไม่อนุญาตก็จะไม่ให้ผ่านแต่กำแพงไฟไม่ได้ทำการวิเคราะห์และทำการบันทึกว่าข้อมูลที่ไม่ได้อนุญาตนั้นเป็นข้อมูลลักษณะใดและมีแนวโน้ม มีความพยายาม หรือมีความตั้งใจที่จะเข้ามาเพื่อทำอะไรกับระบบเครือข่ายภายใน ยกตัวอย่างเช่นหากยามที่เฝ้าประตูพบว่ามีผู้บุกรุกพยายามที่จะปีนข้ามกำแพงก็จะไม่สนใจ และไม่ทำการบันทึกลงในสมุดบันทึกเหตุการณ์เพราะรู้แต่เพียงว่า ไม่สามารถปีนข้ามกำแพงได้และก็ไม่ได้แจ้งเจ้าของบ้านให้เพิ่มความระมัดระวัง หรือในกรณีที่มีบุคคลที่พยายามใช้บัตรผ่านปลอมผ่านประตู แล้วบอกกับยามว่าจะขอเข้าไปที่แผนกการเงิน ยามทำการตรวจสอบพบว่าเป็นบัตรผ่านปลอมจึงไม่อนุญาตให้ผ่านเข้าไปแต่ก็ไม่ได้รายงานให้เจ้าของบ้านทราบ และไม่ได้บันทึกลงในสมุดบันทึกทำให้เจ้าของบ้านไม่ทราบว่าแผนกการเงินกำลังตกเป็นเป้าปฏิบัติงานของผู้บุกรุก ดังนั้นการใช้งานระบบกำแพงไฟให้มีประสิทธิภาพมากขึ้นก็จะต้องมีการตรวจสอบและวิเคราะห์การผ่านเข้า-ออกด้วยว่า ผู้บุกรุกมีเจตนาอะไรในการบุกรุกเข้ามาเพื่อเป็นข้อมูลในการแก้ไข หรือปรับปรุงระบบเพื่อป้องกันความเสียหายที่อาจจะเกิดขึ้นได้จากการบุกรุก หรือป้องกันไม่ให้การบุกรุกนั้นประสบความสำเร็จได้

มีเครื่องมืออีกประเภทหนึ่งที่สามารถวิเคราะห์และตรวจสอบว่าบ้านเราหรือระบบเครือข่ายนั้นถูกพยายามบุกรุกด้วยวิธีการใดบ้าง มีความพยายามบุกรุกเกิดขึ้นบ่อยครั้งเท่าใด และเป้าหมายของการบุกรุกคืออะไร เครื่องมือดังกล่าวคือ “ระบบตรวจสอบการบุกรุก (Intrusion Detection System, IDS)” ผู้เขียนได้นำระบบ IDS มาติดตั้งใช้งานร่วมกับระบบกำแพงไฟเพื่อตรวจสอบการบุกรุกระบบเครือข่ายของโรงเรียนนายเรือซึ่งรายละเอียดของระบบตรวจสอบการบุกรุกผู้เขียนจะไม่ขอกล่าว เพื่อวัตถุประสงค์ทางด้านการรักษาความปลอดภัย แต่จะขอนำข้อมูลที่ได้จากระบบตรวจสอบการบุกรุกมาแสดงให้ผู้อ่านเห็นว่า ประตูที่เรามองไม่เห็นนี้กำลังถูกบุกรุกโดยบุคคลภายนอกอยู่ตลอดเวลาดังตัวอย่างในรูปที่ ๒

Date	Attack	Source Host	Source Port	Target Host	Target Port
Sun Mar 28 22:59:44 2004	Scanning attack	192.175.48.1	53	203.147.5.58	2634
Mon Mar 29 22:57:47 2004	Scanning attack	192.175.48.1	53	203.147.5.58	4058
Tue Mar 30 22:57:42 2004	Scanning attack	192.175.48.1	53	203.147.5.58	1498
Wed Mar 31 08:20:34 2004 - Wed Mar 31 08:20:34 2004	Options not valid	203.218.112.236	4615	203.147.5.59	2745
Wed Mar 31 08:20:37 2004 - Wed Mar 31 08:20:37 2004	Options not valid	203.218.112.236	4615	203.147.5.59	2745
Wed Mar 31 08:48:40 2004	Scanning attack	192.175.48.1	53	203.147.5.58	3712
Wed Mar 31 13:31:03 2004 - Wed Mar 31 13:31:03 2004	Options not valid	203.218.60.7	4615	255.255.255.255	2745
Wed Mar 31 13:31:09 2004 - Wed Mar 31 13:31:09 2004	Options not valid	203.218.60.7	4622	255.255.255.255	80
Wed Mar 31 22:57:50 2004	Scanning attack	192.175.48.1	53	203.147.5.58	3007
Thu Apr 1 08:48:35 2004	Scanning attack	192.175.48.1	53	203.147.5.58	1318
Thu Apr 1 13:42:07 2004 - Thu Apr 1 13:42:08 2004	ISS Unicode attack	203.236.112.222	1148	203.147.5.58	80
Thu Apr 1 22:57:48 2004	Scanning attack	192.175.48.1	53	203.147.5.58	4481
Fri Apr 2 08:48:40 2004	Scanning attack	192.175.48.1	53	203.147.5.58	2826
Fri Apr 2 22:57:55 2004	Scanning attack	192.175.48.1	53	203.147.5.58	2005
Fri Apr 2 23:20:06 2004 - Fri Apr 2 23:20:06 2004	Options not valid	203.176.227.186	1509	203.147.5.62	2745
Fri Apr 2 23:20:09 2004 - Fri Apr 2 23:20:09 2004	Options not valid	203.176.227.186	1509	203.147.5.62	2745
Sat Apr 3 08:48:40 2004	Scanning attack	192.175.48.1	53	203.147.5.58	4054
Sat Apr 3 17:24:19 2004 - Sat Apr 3 17:24:20 2004	ISS Unicode attack	203.236.112.209	3485	203.147.5.58	80
Sat Apr 3 19:53:04 2004 - Sat Apr 3 19:53:04 2004	Options not valid	203.218.97.32	3498	203.147.5.62	2745
Sat Apr 3 19:53:07 2004 - Sat Apr 3 19:53:07 2004	Options not valid	203.218.97.32	3505	203.147.5.62	80
Sat Apr 3 19:53:13 2004 - Sat Apr 3 19:53:13 2004	Options not valid	203.218.97.32	3505	203.147.5.62	80
Sat Apr 3 22:57:48 2004	Scanning attack	192.175.48.1	53	203.147.5.58	2968
Sun Apr 4 09:48:49 2004	Scanning attack	192.175.48.1	53	203.147.5.58	1054
Sun Apr 4 11:42:49 2004 - Sun Apr 4 11:42:49 2004	ISS Unicode attack	203.70.197.24	4822	203.147.5.4	80
Sun Apr 4 11:42:52 2004	ISS Unicode attack	203.70.197.24	4915	203.147.5.4	80
Sun Apr 4 11:42:57 2004	ISS Unicode attack	203.70.197.24	1048	203.147.5.4	80
Sun Apr 4 23:57:42 2004	Scanning attack	192.175.48.1	53	203.147.5.58	3886
Mon Apr 5 04:14:25 2004 - Mon Apr 5 04:14:25 2004	ISS Unicode attack	203.72.83.90	4411	203.147.5.58	80
Mon Apr 5 04:14:29 2004 - Mon Apr 5 04:14:30 2004	ISS Unicode attack	203.72.83.90	4420	203.147.5.58	80
Mon Apr 5 23:57:46 2004	Scanning attack	192.175.48.1	53	203.147.5.58	1226
Tue Apr 6 01:30:21 2004 - Tue Apr 6 01:30:21 2004	Options not valid	203.99.181.185	4048	203.147.5.56	6129

Date	Attack	Source Host	Source Port	Target Host	Target Port
Tue Apr 6 09:48:37 2004	Scanning attack	192.175.48.1	53	203.147.5.58	3229
Tue Apr 6 23:57:40 2004	Scanning attack	192.175.48.1	53	203.147.5.58	2066
Wed Apr 7 09:48:37 2004	Scanning attack	192.175.48.1	53	203.147.5.58	4273
Wed Apr 7 23:57:42 2004	Scanning attack	192.175.48.1	53	203.147.5.58	3349
Thu Apr 8 09:48:38 2004	Scanning attack	192.175.48.1	53	203.147.5.58	1681
Fri Apr 9 09:48:35 2004	Scanning attack	192.175.48.1	53	203.147.5.58	3216

รูปที่ ๒

จากตัวอย่างที่ระบบตรวจสอบผู้บุกรุกได้ทำการตรวจจับได้ จะเห็นได้ว่ามีทั้งการโจมตีระบบเครือข่ายโดยการส่งโค๊ดเข้ามาและมีการโจมตีโดยการสแกนระบบเครือข่ายทุกวัน ๆ ละหลายครั้งหากวันใดที่ไม่มีระบบกำแพงไฟและระบบ IDS ก็จะทำให้ระบบเครือข่ายภายในนั้นอยู่ในสภาวะล่อแหลมต่อการถูกโจมตีได้

มีทั้ง Firewall และ IDS ก็คงปลอดภัย?

จากที่กล่าวมาผู้อ่านคงจะเริ่มรู้สึกว่าเราน่าจะปลอดภัยในเมื่อระบบเครือข่ายของโรงเรียนนายเรือมีทั้งระบบกำแพงไฟและระบบตรวจสอบผู้บุกรุก แต่ในความเป็นจริงแล้วระบบทั้งสองเป็นเพียงเครื่องมือเพิ่มความปลอดภัยเพิ่มเกราะป้องกันตนเองให้มากขึ้นเท่านั้น ระบบทั้งสองก็อาจจะมีจุดอ่อนในบางจุดที่สามารถถูกนำมาใช้ในการโจมตีในภายหลังเมื่อมีการค้นพบก็ได้ ดังเช่นระบบปฏิบัติการของบริษัทยักษ์ใหญ่ในวงการคอมพิวเตอร์ที่ถูกค้นพบรอยรั่วมากมายและต้องคอยออกโปรแกรมแก้ไขและอุดรอยรั่ว อยู่เป็นระยะ ๆ ระบบกำแพงไฟก็เช่นเดียวกันอาจจะมีรอยรั่วที่ถูกค้นพบแล้วหรือยังไม่ถูกค้นพบโดยที่ผู้ใช้งานเองยังไม่ทราบได้ จึงจำเป็นต้องมีการติดตามข้อมูลข่าวสารของระบบที่นำมาใช้อย่างใกล้ชิดและผู้เขียนเองถึงแม้จะมีหน้าที่เกี่ยวข้องกับศูนย์คอมพิวเตอร์โรงเรียนนายเรือ แต่อย่างไรก็ตามภารกิจหลักที่ได้รับมอบหมาย คือหน้าที่ในการสอนหนังสือให้แก่นักเรียนนายเรือในวิชาทางด้านวิศวกรรมเครื่องกล อีกทั้งผู้เขียนไม่ได้เป็นผู้ที่มีจบการศึกษาทางด้านคอมพิวเตอร์ หรือระบบเครือข่ายคอมพิวเตอร์จึงมีเวลาในการติดตามข้อมูลข่าวสารเกี่ยวกับระบบเครือข่ายได้อย่างจำกัด แม้กระทั่งการตรวจสอบข้อมูลของระบบตรวจสอบผู้บุกรุกในบางช่วงเวลาไม่ได้เข้ามาตรวจสอบว่ามีอะไรเกิดขึ้นบ้างในระบบเครือข่าย และอาจจะเกิดปัญหาแล้วจึงเข้ามาตรวจสอบว่าสาเหตุของปัญหาคืออะไรแล้วจึงแก้ไขต่อไป ดังนั้นระบบที่มีอยู่ก็ยังให้ประสิทธิภาพในการป้องกันได้ไม่เต็มที่นัก

นอกจากมีการบุกรุกโดยผู้บุกรุกจากภายนอกระบบเครือข่ายแล้ว ยังมีการบุกรุกระบบเครือข่ายโดยการส่งโปรแกรมบางชนิดแอบเข้ามาทำงานอยู่ภายในระบบเครือข่าย แล้วขโมยสิ่งที่ต้องการส่งออกไปยังปลายทางหรือโดยการให้โปรแกรมดังกล่าวเปิดช่องทางการติดต่อ เพื่อให้ผู้อยู่ภายนอกสามารถใช้ช่องทางดังกล่าว เข้ามาขโมยสิ่งที่ต้องการโดยที่ระบบกำแพงไฟไม่สามารถตรวจสอบได้ โปรแกรมที่ถูก

ส่งเข้ามาทำงานอยู่ภายในระบบเครือข่ายนั้นอยู่ในกลุ่มที่เรียกว่า “ม้าโทรจัน” หรือ “Trojan horse” โปรแกรมประเภทนี้ใช้ชื่อตามเรื่องเล่าของกรีกที่ใช้กลอุบายซ่อนทหารในม้าไม้ขนาดใหญ่ แล้วมอบให้กับชาวเมืองทรอย พอตกกลางคืนพวกทหารก็ได้ลักลอบมาเปิดประตูเมืองให้พวกตนเองเข้ามาตีเมืองทรอยได้อย่างง่ายดาย เปรียบเสมือนแฮกเกอร์ใช้โปรแกรมบางชนิดเข้ามาในระบบเครือข่ายแล้วแอบส่งข้อมูลหรือสิ่งที่ต้องการออกไปให้ตนเอง โดยส่วนใหญ่โปรแกรมดังกล่าวจะถูกส่งเข้ามาทางจดหมายอิเล็กทรอนิกส์ เพราะเป็นช่องทางที่แทบจะไม่ได้รับการตรวจสอบ และเป็นช่องทางที่ระบบกำแพงไฟอนุญาตให้ผ่านเข้าสู่ระบบเครือข่ายภายในได้ เมื่อผู้ได้รับจดหมายอิเล็กทรอนิกส์เปิดไฟล์ที่ได้รับโดยไม่ทันระวังโปรแกรมดังกล่าวก็จะทำงานทันทีโดยอัตโนมัติ โทรจันบางชนิดได้ใช้พอร์ท ๘๐ ในการทำงานซึ่งพอร์ทดังกล่าวนี้เป็นพอร์ทตั้งต้น (Default port) สำหรับโปรแกรมเว็บเซิร์ฟเวอร์และเว็บไคลแอนท์สำหรับเว็บเพจต่างๆดังนั้นเป็นพอร์ทที่ได้รับการอนุญาตให้ข้อมูล วิ่งผ่านเข้าออกได้กำแพงไฟ ระบบเครือข่ายภายในก็อาจถูกบุกรุกหรือขโมยข้อมูลได้โดยโทรจันเหล่านี้

สรุป

จะเห็นได้ว่าเหล่าบรรดาแฮกเกอร์จะมีวิธีการอันแยบยลและวิธีการใหม่ ๆ ออกมาใช้ตลอดเวลา ถึงแม้ว่าระบบเครือข่ายภายในจะมีการป้องกันแน่นหนาเพียงใดก็ตามก็ยังคงมีช่องทางหรือรอยรั่วเล็ก ๆ ที่บรรดาแฮกเกอร์นำมาใช้ประโยชน์ในการบุกรุกระบบเครือข่ายได้ ข้อมูลต่าง ๆ จึงถือได้ว่ายังไม่มีความปลอดภัยอย่างสมบูรณ์ การที่จะให้ข้อมูลมีความปลอดภัยจากบรรดาผู้บุกรุกโดยใช้ประตูที่มองไม่เห็นนี้อย่างสมบูรณ์ก็คือการแยกเครื่องคอมพิวเตอร์เครื่องนั้น ๆ ออกจากระบบเครือข่าย หากไม่สามารถทำได้ผู้ใช้ก็จะต้องมีวินัยในการใช้เครื่องคอมพิวเตอร์ ระมัดระวังไม่เปิดจดหมายอิเล็กทรอนิกส์ที่ได้รับจากคนไม่รู้จัก ไม่นำโปรแกรมที่ไม่รู้จักแหล่งที่มา ๆ ใช้ ร่วมมือกันศึกษาหาข้อมูลใหม่ ๆ ที่เกิดขึ้นในโลกของอินเทอร์เน็ต ติดตามข่าวสารเกี่ยวกับไวรัสและหนอนอินเทอร์เน็ตอย่างสม่ำเสมอและหาทางป้องกันไม่ให้ตนเองตกเป็นเป็นเป้าโจมตี **หากในสำนักงานหรือหน่วยงานของตนเองมีเอกสารประเภท “ลับ” หรือ “ลับมาก” ควรจะเก็บไว้ในเครื่องคอมพิวเตอร์ที่ไม่ได้เชื่อมต่ออยู่กับระบบเครือข่าย ห้ามทำการเก็บไว้ในเครื่องคอมพิวเตอร์ที่มีการแชร์ไฟล์อย่างไม่ระมัดระวัง การเก็บไฟล์ข้อสอบของอาจารย์ก็ไม่ควรเก็บไว้ในเครื่องคอมพิวเตอร์ที่ใช้งานส่วนรวม ควรจะทำการบันทึกเก็บในสื่อสำหรับบันทึกไฟล์ส่วนตัวเช่น สื่อบันทึกชนิดพกพาได้ประเภท thumb drive หรือ handy drive (ปัจจุบันนี้ราคาถูกลงมาก) และเก็บไว้เฉพาะส่วนตัวจะได้ไม่เกิดกรณีข้อสอบรั่ว** และที่สำคัญทุกคนควรระลึกถึงเสมอว่าโรงเรียนนายเรือยังมีประตูทางเข้าอยู่อีกหนึ่งแห่งนั่นคือ“ประตูสู่โลกอินเทอร์เน็ต” ของผู้ใช้งานภายในหรือ “**ประตูเข้าสู่โรงเรียนนายเรือ**” สำหรับบุคคลภายนอกและมีผู้พยายามเข้าสู่โรงเรียนนายเรือโดยผ่านทางประตูนี้อยู่ตลอดเวลา หากปล่อยให้ผู้บุกรุกพยายามหาหนทางเข้าสู่ระบบเครือข่ายโดยไม่มีมาตรการใดๆเพิ่มเติมให้ทันผู้บุกรุกอาจจะมีข้อมูลสำคัญหลุดรอดออกไปเผยแพร่สู่โลกอินเทอร์เน็ตภายนอกได้