บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

จากการที่มีพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ซึ่งมีผลบังคับใช้ตั้งแต่วันที่ 18 กรกฎาคม พ.ศ. 2550 มีผลทำให้ผู้ให้บริการอินเทอร์เน็ตทั้งภาครัฐและเอกชน รวมถึงผู้ประกอบการรายย่อยที่เกี่ยวข้องกับการให้บริการอินเทอร์เน็ตมีหน้าที่ ต้องเก็บรักษาข้อมูลจราจรคอมพิวเตอร์ในหน่วยงานของตนเองไว้ไม่น้อยกว่า 90 วัน ไม่เช่นนั้นแล้วจะมีความผิดกฎหมายทางอาญาตามที่ระบุไว้ในพระราชบัญญัติ (คณะกรรมการธุรกรรมทางอิเล็คทรอนิค, 2550)

เมื่อเป็นเช่นนี้จึงทำให้เกิดความตื่นตัวในการดำเนินการเพื่อจัดหาระบบหรืออุปกรณ์ที่สามารถใช้ในการจัดเก็บข้อมูลจราจรคอมพิวเตอร์ โดยอุปกรณ์ที่ใช้เก็บสถิติการใช้งานเครือข่ายเพื่อวิเคราะห์และป้องกันระบบ (Network Access Control) ที่มีจำหน่ายอยู่ในท้องตลาดนั้น มีราคาสูง ใช้งานยาก เหมาะสำหรับเครือข่ายขนาดใหญ่ไม่ครอบคลุมการทำงานในระบบเครือข่ายขนาดเล็ก ไม่สามารถแก้ไข ดัดแปลง เพิ่มเติมระบบได้โดยอิสระ เพราะติดในเรื่องของสัญญาการดูแลรักษาจากเจ้าของผลิตภัณฑ์ (Warranty) หรือหากต้องมีการขยายขนาดเครือข่ายก็จะต้องมีการเพิ่มงบประมาณสำหรับขยายขีดความสามารถของผลิตภัณฑ์ (License) นั้นๆ และปัญหาสำคัญ ที่พบเมื่อใช้งานจริงคือเรื่องของบุคลากรทางคอมพิวเตอร์ที่เรียกว่าผู้ดูแลระบบ (Network Administrator) หากไม่มีความเชี่ยวชาญในตัวผลิตภัณฑ์หรือไม่มีการศึกษาวิธีการใช้งานมาเป็นอย่างดี ซึ่งปกติงานของผู้ดูแลระบบก็มากอยู่แล้ว เมื่อมีปัญหาจะไม่สามารถจัดการได้ด้วยตนเอง ต้องรอบุคลากรของผลิตภัณฑ์เพียงอย่างเดียวซึ่งอาจทำให้เกิดความไม่ต่อเนื่องและเสียหายต่อการจัดเก็บข้อมูลจราจรคอมพิวเตอร์ให้เป็นไปตามวัตถุประสงค์ได้

ซอฟท์แวร์รหัสเปิด (Open Source) คือวิธีการในการออกแบบ พัฒนา และแจกจ่ายสำหรับต้นฉบับของสินค้าหรือความรู้ โดยเฉพาะซอฟต์แวร์ โดยซอฟท์แวร์รหัสเปิดถูกพิจารณาว่าเป็นทั้งรูปแบบหนึ่งในการออกแบบ และแผนการในการดำเนินการ ผู้ใช้งานรวมถึงผู้พัฒนาสามารถนำมาใช้งาน แก้ไข แจกจ่าย โดยสามารถนำมาปรับปรุงทั้งในลักษณะส่วนตัว หรือในหน่วยงานเอกชนได้ ซอฟท์แวร์รหัสเปิดอนุญาตให้ทุกคนสามารถนำซอฟต์แวร์ไปพัฒนาโดยเปิดโอกาสให้บุคคลอื่นนำเอาระบบนั้นไปพัฒนาได้ ในลักษณะไม่เสียค่าใช้จ่าย ในปัจจุบันมีซอฟท์แวร์รหัสเปิดอยู่เป็นจำนวนมากมายตามกลุ่มการใช้งาน เช่น Linux ซึ่งเป็นระบบปฏิบัติการ หรือ

Open Office เป็นโปรแกรมประเภทจัดทำเอกสารสำนักงาน Firefox เป็นซอฟท์แวร์ที่ใช้สำหรับเปิดหน้าเว็บ ซึ่งซอฟท์แวร์เหล่านี้ไม่มีค่าลิขสิทธิ์ใดๆ สามารถหาใช้ได้ เป็นต้น (http://www.nectec.or.th/rd/rd-opensource-th.html, สืบค้นวันที่ 5 สิงหาคม 2553)

เมื่อเป็นดังนี้ผู้ทำวิจัยได้พิจารณาแล้วว่าการสร้างระบบจัดเก็บข้อมูลจราจรคอมพิวเตอร์ด้วยซอฟท์แวร์รหัสเปิด โดยการผสมผสานกันของซอฟท์แวร์ประเภทต่างๆ ที่มีอยู่แล้วในระบบเครือข่ายโดยไม่ติดปัญหาเรื่องลิขสิทธิ์ สามารถพัฒนา เปลี่ยนแปลงแก้ไขให้เหมาะสมกับสภาวะแวดล้อมของแต่ละเครือข่ายได้ ย่อมจะทำให้เกิดระบบที่ประหยัดงบประมาณในการจัดทำและค่าใช้จ่ายที่มีต่อการซ่อมบำรุง และได้ระบบที่มีประสิทธิภาพตรงตามวัตถุประสงค์ในการจัดเก็บข้อมูลจราจรคอมพิวเตอร์

1.2 วัตถุประสงค์ของการวิจัย

เพื่อศึกษาและพัฒนาระบบจัดเก็บข้อมูลจราจรคอมพิวเตอร์ด้วยซอฟท์แวร์รหัสเปิดที่สามารถใช้ในการจัดเก็บข้อมูลและยืนยันตัวตนของผู้ใช้งานเครือข่ายคอมพิวเตอร์ของหน่วยงานให้เป็นไปตามที่กำหนดไว้ในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

1.3 ประโยชน์ที่คาดว่าจะได้รับ

1.3.1 มีระบบจัดเก็บข้อมูลจราจรคอมพิวเตอร์ที่พัฒนาด้วยซอฟท์แวร์รหัสเปิดและสามารถใช้งานได้

1.3.2 มีระบบมีระบบจัดเก็บข้อมูลจราจรคอมพิวเตอร์ที่ใช้ต้นทุนในการจัดทำต่ำ แต่มีการทำงานที่ดี

1.4 ขอบเขตของการวิจัย

เพื่อให้การจัดเก็บข้อมูลจราจรคอมพิวเตอร์เป็นไปอย่างมีประสิทธิภาพผู้วิจัยได้ออกแบบระบบให้มีการทำงานในด้านต่างๆ ดังนี้

1.4.1 ต้องสามารถระบุตัวตนของผู้ใช้งานอินเทอร์เน็ตได้อย่างชัดเจน โดยการให้ผู้ใช้ยืนยันตัวตนก่อนเข้าใช้งาน (Authentication)

1.4.2 ต้องสามารถตรวจสอบข้อมูลที่แท้จริงของผู้เข้าใช้ เช่น ชื่อ นามสกุล เลขบัตรประชาชน เพื่อระบุตัวตนที่แท้จริงผ่านระบบฐานข้อมูลได้ (Member Database System)

1.4.3 มีระบบรายงานข้อมูลการใช้งานของผู้ใช้ และสามารถสรุปแยกย่อยได้ตามช่วงเวลา เช่น จำนวนผู้เข้าใช้รายวัน รายเดือน รายสัปดาห์

1.4.4 มีระบบจัดเก็บข้อมูลของผู้เข้าใช้อินเทอร์เน็ตย้อนหลังไว้ได้นานไม่น้อยกว่า 90 วัน เพื่อให้เป็นไปตามข้อกำหนดของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

1.4.5 มีระบบบริหารจัดการบัญชีข้อมูลผู้ใช้ เช่น การเพิ่มชื่อผู้ใช้ การแก้ไขชื่อผู้ใช้ การแก้ไขรหัสผ่านฯ รวมถึงการจัดการล็อกไฟล์ต่างๆ อยู่บนระบบแม่ข่ายกลาง (Centralized Server System Management)

1.4.6 ระบบสามารถหยุดให้บริการกับผู้ใช้รายใดก็ได้ หากพบว่าผู้ใช้รายนั้นมีการกระทำอันไม่เหมาะสม ขัดกับนโยบายในการให้บริการ

1.4.7 มีระบบการจัดการ ค้นหา ข้อมูลการจราจรย้อนหลัง เพื่อใช้สำหรับค้นข้อมูลหากมีคำร้องขอจากเจ้าพนักงานเพื่อระบุตัวตนว่าใครเป็นผู้กระทำความผิดโดยการออกเป็นรายงาน (Report)

1.5 ข้อตกลงเบื้องต้น

ระบบจัดเก็บข้อมูลจราจรคอมพิวเตอร์ด้วยซอฟท์แวร์รหัสเปิด เป็นซอฟท์แวร์ประยุกต์ที่มีพื้นฐานการทำงานทั้งหมดโดยใช้ซอฟท์แวร์รหัสเปิด ใช้ระบบปฏิบัติการ (Operating System) ลินุกซ์ (Linux) เป็นหลัก ระบบการจัดการข้อมูลผู้ใช้และการยืนยันตัวตน ทำงานอยู่บนเครื่องแม่ข่ายเพียงที่เดียว (Centralized Log Serve) ผู้ใช้ทำการยืนยันตัวตนผ่านระบบเว็บแคช (Proxy) ที่ทำงานร่วมกับระบบ Radius Server ซึ่งเชื่อมต่อการทำงานไปยังระบบฐานข้อมูลมายเอสคิวแอล (MySQL Database) เพื่อใช้ในการเก็บข้อมูลผู้ใช้ (Log File)

ในการเข้าใช้งานอินเทอร์เน็ตของผู้ใช้นั้น จะต้องทำการล็อกอินผ่านหน้าล็อกอินที่โปรแกรมกำหนดให้ในครั้งแรกที่ผู้ใช้เปิดโปรแกรมเบราว์เซอร์ (Web Browser) เพื่อเข้าถึงเว็บเพจ หากผู้ใช้ใส่ชื่อผู้ใช้ (UserName) และรหัสผ่าน (Password) ถูกต้องก็จะสามารถเข้าถึงเว็บเพจต่างๆ ได้

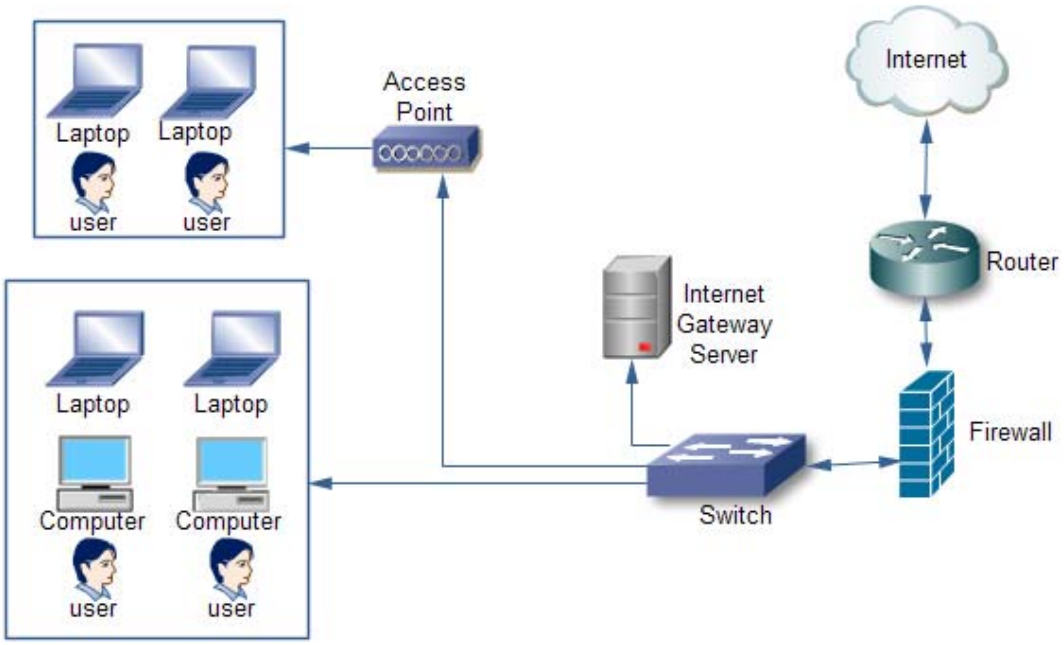
1.6 ข้อจำกัดการวิจัย

ระบบจัดเก็บข้อมูลจราจรคอมพิวเตอร์ด้วยซอฟท์แวร์รหัสเปิด ที่ผู้วิจัยจัดทำขึ้นนี้ ได้ใช้วิธีการประยุกต์จากระบบพร็อกซี่เซิร์ฟเวอร์ (Proxy Server) โดยต้องมีการกำหนดหมายเลขไอพีเครื่องแม่ข่ายที่ทำหน้าที่เป็นพร็อกซี่เซิรฟ์เวอร์ไว้ในเบราว์เซอร์ของเครื่องลูกข่ายทุกเครื่อง ไม่สามารถข้ามขั้นตอนนี้ และไม่สามารถทำงานในแบบอัตโนมัติที่เรียกว่า Transparent Proxy ได้

โดยผู้ทำวิจัยมองเห็นว่าเป็นข้อดีกับระบบการยืนยันตัวตน เพราะทำให้รู้การเคลื่อนไหวของผู้ใช้ได้ กรณีที่มีการเพิ่มเครื่องเข้ามาในระบบ แม้ว่าการทำแบบนี้จะสร้างภาระให้กับผู้ดูแลระบบก็ตาม

1.7 กรอบแนวคิดในการวิจัย

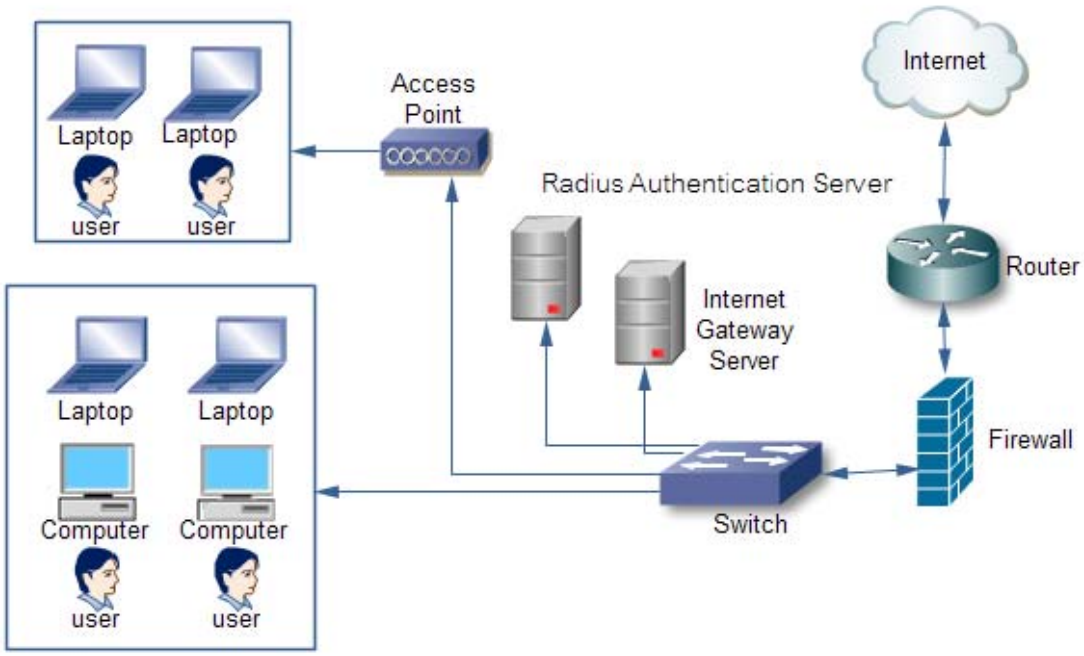
จากข้อมูลความต้องการและขอบเขตการทำงานข้างตน ทำให้กรอบแนวคิดในการวิจัยที่จะสร้างระบบ มีดังต่อไปนี้



ภาพที่ 1-1 การเชื่อมต่อเครือข่ายอินเทอร์เน็ต

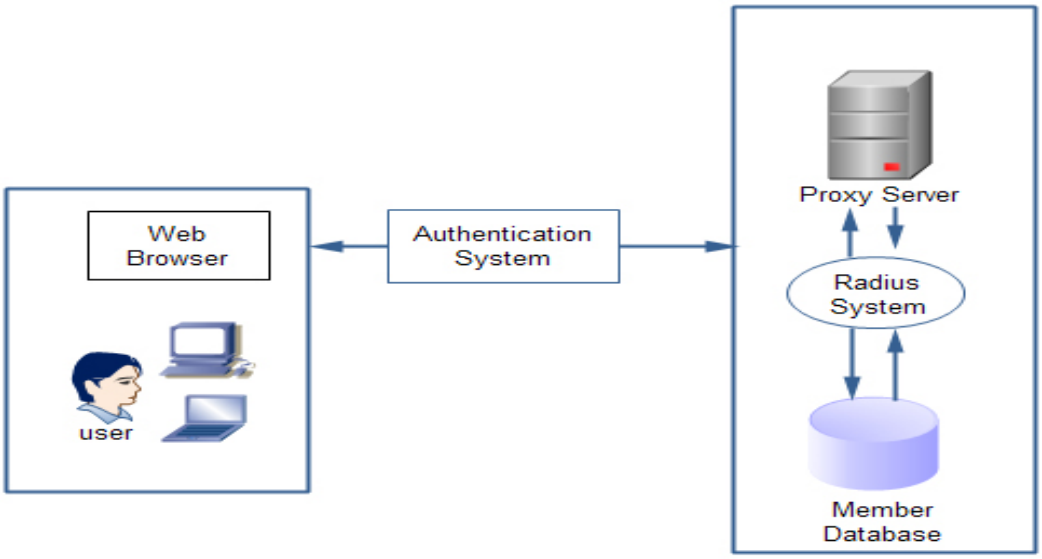
จากภาพเป็นการเชื่อมต่อเครือข่ายอินเทอร์เน็ตในรูปแบบทั่วไป และเป็นเส้นทางของเครื่องคอมพิวเตอร์ลูกข่าย (Client) ที่จะเข้าสู่ระบบอินเทอร์เน็ต โดยจะเห็นได้ว่าคอมพิวเตอร์ที่จะเข้าสู่เครือข่ายหรือใช้งานอินเทอร์เน็ตมีอยู่ 2 กลุ่มหลักๆ คือ กลุ่มที่เป็นเครื่องคอมพิวเตอร์ที่เชื่อมต่อโดยใช้สาย (Wired Network) กับเครื่องคอมพิวเตอร์ที่ไม่ใช้สายหรือที่เรียกว่า ไร้สาย (Wireless Network) โดยคอมพิวเตอร์ทั้งหมดจะเชื่อมต่ออยู่กับอุปกรณ์พื้นฐานเบื้องต้นก่อน ในภาพคือ Switch ผ่านอุปกรณ์ตรวจจับผู้บุกรุก (Firewall) เข้าสู่อุปกรณ์เชื่อมต่อเครือข่ายภายนอก (Router) ก่อนออกสู่อินเทอร์เน็ต กระบวนการเหล่านี้คือขั้นตอนทั่วไปของเครื่องคอมพิวเตอร์ในหน่วยงานหรือที่เรียกว่าเครือข่ายท้องถิ่น (Local Area Network) จัดเป็นรูปแบบที่ปรากฏและใช้งานอยู่ทั่วไปซึ่งกระบวนการแบบนี้จะเห็นได้ว่าเครื่องคอมพิวเตอร์ลูกข่ายทุกเครื่องสามารถออกไปใช้งานเครือข่ายภายนอกหรืออินเทอร์เน็ตได้โดยไม่มีการตรวจสอบสิทธิ์ใดๆ ดังนั้นการวิจัยในครั้งนี้จะทำการบังคับให้เครื่องลูกข่ายทุกเครื่องจะต้องถูกตรวจสอบสิทธิ์และยืนยันตัวตนเสียก่อนจึงจะ

สามารถเชื่อมต่อออกสู่ระบบอินเทอร์เน็ตได้โดยการเพิ่มอุปกรณ์ในการตรวจสอบสิทธิ์ผู้ใช้ขึ้นมา เรียกว่า Radius Authentication Server ดังภาพ



ภาพที่ 1-2 ระบบยืนยันตัวตน (Radius Authentication System)

หลังจากมีการเพิ่มส่วนของการตรวจสอบและยืนยันตัวตน (Radius Authentication Server) เข้าไปในระบบเดิม กระบวนการออกสู่อินเทอร์เน็ตของเครื่องคอมพิวเตอร์จะเปลี่ยนไป โดยเมื่อผู้ใช้เปิดโปรแกรมเว็บเบราว์เซอร์เพื่อใช้งานอินเทอร์เน็ต ระบบจะเริ่มตรวจสอบตัวตนของผู้ใช้โดยปรากฏหน้าต่าง (Popup Windows) ให้ผู้ใช้กรอกชื่อผู้ใช้ (UserName) และรหัสผ่าน (Password) หากข้อมูลถูกต้องระบบก็จะยินยอมให้ออกสู่อินเทอร์เน็ตได้ตามกระบวนการเดิม



ภาพที่ 1-3 การยืนยันตัวตนของผู้ใช้

จากกรอบแนวความคิดทั้งหมดที่ผู้ทำวิจัยเสนอไว้ ทำให้สรุปได้ว่าระบบที่จัดทำขึ้นนั้นจะมีกระบวนการทำงานโดยผู้ใช้ทุกคนที่ต้องการใช้งานอินเทอร์เน็ตจะต้องผ่านการตรวจสอบสิทธิ์ก่อนเสมอ และระบบการยืนยันตัวตนของผู้ใช้จะมีเครื่องคอมพิวเตอร์แม่ข่ายที่ทำงานเป็น Proxy Server คอยตรวจสอบข้อมูลความถูกต้องของผู้ใช้ที่จัดเก็บไว้ในระบบฐานข้อมูล ดังภาพ

1.8 นิยามศัพท์เฉพาะ

ซอฟท์แวร์รหัสเปิด , โอเพ่นซอร์ส , ล็อกไฟล์ , พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 , พร็อกซี่