การพัฒนาระบบการรักษาความปลอดภัยบนเครือข่ายไร้สาย

A Software Development of Wireless Security Gateway System

โดย

ฐิติ ขุนพรหม

รหัสประจำตัว 45061613

อาจารย์ที่ปรึกษา

ผศ. อัครินทร์ คุณกิตติ

รายงานนี้เป็นส่วนหนึ่งของวิชาโครงการพัฒนาระบบงาน

หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ

ภาคเรียนที่ 2 ปีการศึกษา 2547

คณะเทคโนโลยีสารสนเทศ

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ชื่อหัวข้อ	การพัฒนาระบบการรักษาความปลอดภัยบนเครือข่ายไร้สาย
นักศึกษา	นาย ฐิติ ขุนพรหม
อาจารย์ที่ปรึกษา	ผศ. อัครินทร์ คุณกิตติ
ระดับการศึกษา	วิทยาศาสตร มหาบัณฑิต สาขาเทคโนโลยีสารสนเทศ
แขนงวิชา	วิทยาการสารสนเทศ
ปีการศึกษา	2547

บทคัดย่อ

ในการนำระบบ Wireless LAN มาใช้งานสิ่งที่สำคัญประการหนึ่งก็คือการรักษาความปลอดภัย เพราะอย่างที่ทราบกันดีว่าการรักษาความปลอดภัยของ Wireless LAN นั้นมีช่องโหว่อยู่หลายจุด เช่นในส่วนของการพิสูจน์ตัวตนก่อนเข้าใช้งานระบบและการเข้ารหัสของช่องทางการติดต่อสื่อสาร โดยโครงงานจะทำการนี้เป็นการออกแบบและพัฒนาโปรแกรมเพื่อทำการเพิ่มการรักษาความปลอดภัยให้ระบบที่ทำงานร่วมกับเครือข่ายไร้สายมาตรฐาน 802.11b โดยโครงงานจะทำหน้าที่เป็นเกตเวย์ระหว่างเครือข่ายไร้สายและเครือข่ายใช้สายคอยปกป้องการเข้าใช้งานเครือข่ายใช้สายโดยไม่ได้รับอนุญาต โดยใช้หลักการของไฟร์วอลล์ในการควบคุมการเข้าใช้ระบบกล่าวคือ เมื่อผู้ใช้จากระบบเครือข่ายไร้สายต้องการเข้ามาใช้ทรัพยากรในเครือข่ายใช้สายผู้ใช้ต้องทำการลงทะเบียนเพื่อร้องขอการเข้าใช้งานก่อน จากนั้นผู้ดูแลระบบจะทำการให้สิทธิเข้าใช้งานพร้อมกับส่งรหัสผ่านไปยังผู้ร้องขอ หลังจากผู้ใช้ได้รับรหัสผ่านผู้ใช้งานก็นำข้อมูลนั้นมาทำการพิสูจน์ตัวจริงกับระบบ ถ้าการพิสูจน์ตัวจริงสำเร็จระบบจะนำข้อมูลไอพีของผู้ใช้งาน ประกอบกับข้อมูลสิทธิการเข้าใช้ระบบที่กำหนดโดยผู้ดูแลระบบไว้แล้วนำมาสร้างเป็นไฟร์วอลล์สริปต์และทำการรันสริปต์นั้น ซึ่งจะทำให้ไอพีของผู้ใช้เข้ามาใช้งานในระบบตามสิทธิที่กำหนดไว้ได้ โดยโครงงานนี้ยังได้พัฒนาเพิ่มในส่วนของการดูแลจัดการผู้ใช้ในระบบส่วนของการควบคุมการเข้าใช้งานระบบส่วนของกำหนดสิทธิเข้าใช้ทรัพยากรที่ผู้ดูแลระบบสามารถกำหนดสิทธิให้กับผู้ใช้งานแต่ละคนได้ และจากการทดลองการใช้งานระบบก็สามารถสรุปได้ว่าโครงการนี้สามารถนำไปใช้งานได้จริงและสามารถเพิ่มการรักษาความปลอดภัยขึ้นได้อีกระดับหนึ่ง

Title	A Software Development of Wireless Security Gateway System
Student	Mr. Thiti Khunprom
Advisor	Assist. Prof Akharin Khunkitti
Level of Study	Master of Science in Information Technology
Academic Year	2004

Abstract

One important thing that all users have to concern when using the Wireless LAN is security. Many weak points have been found such as self identification in system accessing process and communication channel encoding. This project aims to design and develop the program in order to enhance the security of the access system which cooperates with 802.11b standard's Wireless LAN. The designed program is working as a gateway staying between wireless LAN and wired LAN. It protects the system from unauthorized wireless LAN usage by asking for registration before accessing the system. Then the system will create a firewall script by using IP from user and user rights information , which has been assigned by administrator.After firewall script completely created system will execute this script to allow IP from authorized user access system. After that, the program will give the result of identification regarding to system authorization. Moreover, this program has also been developed in term of user management, system accessing control and resource authorization to each user. As a result of system testing, it can infer that the program is practical and could extend the security tolerably.

กิตติกรรมประกาศ

การจัดทำโครงการพัฒนาระบบงานนี้สามารถประสบความสำเร็จลุล่วงไปได้ด้วยดีด้วยการสนับสนุนจากบุคคลเหล่านี้ ข้าพเจ้าจึงขอกล่าวคำขอบพระคุณมา ณ โอกาสนี้

ขอขอบพระคุณครอบครัวของข้าพเจ้า อันได้แก่บิดามารดา พี่สาว และน้องชายรวมทั้งนางสาววาสนา เมธาวีกุลชัย ที่ได้สนับสนุนส่งเสริม ทั้งทางด้านทุนทรัพย์ และกำลังใจในการศึกษาและให้คำแนะนำอีกหลายๆ อย่างในการดำเนินชีวิต และให้คำปรึกษาเมื่อประสบปัญหา

ขอขอบพระคุณท่าน ผศ. อัครินทร์ คุณกิตติ อาจารย์ที่ปรึกษา ซึ่งได้แนะนำให้คำปรึกษาชี้แนะ รวมทั้งช่วยแก้ปัญหา ทำให้การทำโครงการพัฒนาระบบงานนี้สำเร็จไปได้ด้วยดี

ขอขอบคุณหัวหน้าสายงานและเพื่อนร่วมงานที่ได้สนับสนุนเอื้อเฟื้อเวลา และให้คำปรึกษาที่ดีเสมอมา

ขอขอบคุณเพื่อนๆ คณะเทคโนโลยีสารสนเทศ รุ่น IS14.2 ทุกคนที่ช่วยเหลือให้คำปรึกษาที่ดีทุกๆ ในด้าน

ฐิติ ขุนพรหม

สารบัญ

หน้า

สารบัญ (ต่อ)

หน้า

บทที่ 1
บทนำ

1.1 ความสำคัญและที่มา

ปัจจุบันเครือข่ายไร้สายที่ใช้มาตรฐาน 802.11b ยังมีความเสี่ยงในเรื่องการรักษาความปลอดภัยค่อนข้างมากเนื่องจาก Algorithm ที่นำมาใช้ในการรักษาความปลอดภัยนั้นยังมีประสิทธิภาพที่ไม่เพียงพอดังนั้นจึงมีบางองค์กรเริ่มเคลื่อนไหวทำการแก้ไขจุดอ่อนที่พบเช่น IETF ได้เพิ่มมาตรฐานการรักษาความปลอดภัยมากขึ้นในมาตรฐาน802.11iซึ่งเป็นมาตรฐานใหม่ของเครือข่ายไร้สายหรือมีผู้ผลิตบางรายได้พัฒนาระบบพิสูจน์สิทธิการเข้าใช้งานขึ้นมาเพื่อตรวจสอบผู้ใช้ได้ดีขึ้นซึ่งนับว่าเป็นอนาคตที่ดีของระบบเครือข่ายไร้สายแต่อย่างไรก็ตามการแก้ไขทั้งสองกรณีจำเป็นที่จะต้องมีการเปลี่ยนตัวอุปกรณ์ที่ใช้หรือไม่ก็ต้องใช้เทคโนโลยีของผู้ผลิตรายนั้นโดยเฉพาะได้อย่างเดียวเท่านั้นถึงจะทำงานได้ ดังนั้นสำหรับองค์กรที่ได้ติดตั้งอุปกรณ์ของมาตรฐาน 802.11b แล้วแต่ต้องการการรักษาความปลอดภัยมากขึ้นจึงอาจเป็นการลงทุนที่สูงเกินไปถ้าหากจะต้องเปลี่ยนอุปกรณ์ หรือซื้อเทคโนโลยีของผู้ผลิตเพื่อแลกกับการรักษาความปลอดภัยที่ดีขึ้นด้วยเหตุนี้จึงได้มีแนวคิดที่จะพัฒนาระบบเพิ่มประสิทธิภาพการรักษาความปลอดภัยบนมาตรฐาน802.11bโดยใช้อุปกรณ์ชุดเดิมโดยทำงานร่วมกับเทคโนโลยีที่เป็นมาตรฐานกลางและเป็น Software Open Source ให้มากที่สุดเพื่อนำไปพัฒนาและประยุกต์ใช้ได้กว้างขวางต่อไป

1.2 จุดประสงค์ของการพัฒนาระบบ

1. เพื่อทำให้ระบบมีการพิสูจน์ตนเองเพื่อเข้าใช้ทรัพยากรมีการตรวจสอบที่ดีขึ้น
2. ระบบสามารถจำกัดสิทธิการเข้าใช้งานระบบ ให้กับผู้ใช้งานแต่ละคนได้
3. การออกแบบระบบนี้ขึ้นมาจะอ้างอิงกับมาตรฐานของ RFC ให้มากที่สุดเพื่อที่จะนำไปประยุกต์ใช้ในระบบอื่นๆได้กว้างขวางต่อไป

1.3 ขั้นตอนการดำเนินโครงการ

ในการพัฒนาโครงงานนี้จะดำเนินตามขั้นตอนการพัฒนาระบบงาน (System Development Life Cycle) หรือ SDLC ซึ่งเป็นมาตรฐานของการพัฒนาระบบงานโดยกระบวนการพัฒนาระบบประกอบไปด้วยขั้นตอน ดังต่อไปนี้

1. วิเคราะห์ปัญหาของระบบงานเดิม (Problem Analysis)

ศึกษาขั้นตอนการทำงานของเทคโนโลยีที่ใช้งานในปัจจุบันคือ 802.11b โดยทำการศึกษาว่ามีขั้นตอนการทำงานอย่างไร อะไรคือปัญหา ของเทคโนโลยีนี้

2. กำหนดความต้องการของระบบ (System Requirement)

หลังจากทราบปัญหาของเทคโนโลยีนี้แล้ว ก็ทำการศึกษาถึงเทคโนโลยีหรือวิธีแก้ไข ที่จะมาแก้ไขหรือทำให้ปัญหานั้นลดน้อยลง ตลอดจนศึกษาถึงความเป็นไปได้ในการพัฒนาโครงงานว่ามีความเป็นไปได้หรือไม่

3. การออกแบบระบบ (System Design)

เป็นการนำเอาความต้องการของระบบผนวกกับแนวทางการแก้ปัญหามาวางโครงสร้างการทำงานของระบบโดยการแจกแจงรายละเอียดที่แน่ชัดของในแต่ละระบบงานว่ามีส่วนไหนทำอะไรบ้าง

4. การพัฒนาระบบ (System Development)

ทำการติดตั้งซอร์ฟแวร์ต่างๆ ที่เกี่ยวข้องกับการพัฒนาระบบใหม่ และทำการจัดเตรียมทรัพยากรต่างๆให้พร้อมสำหรับการพัฒนาระบบ จากนั้นเป็นขั้นตอนการพัฒนาโปรแกรมที่ได้ทำการออกแบบไว้

5. การทดสอบระบบ (System Testing)

ทำการทดสอบระบบ จะต้องมั่นใจว่าระบบที่ได้ไม่มีข้อผิดพลาด ระบบสามารถทำงานได้จริงตามที่ได้ออกแบบไว้

1.4 ขอบเขตของการพัฒนาโครงการ

1. พัฒนาระบบในส่วนของการพิสูจน์ตนเองเพื่อเข้าใช้งานให้มีขั้นตอนและการตรวจสอบที่รัดกุมมากขึ้นจากมาตรฐาน 802.11b
2. ระบบสามารถบันทึก และแสดงเวลาการเข้าใช้งานของผู้ใช้
3. ผู้ดูแลระบบสามารถกำหนดสิทธิการเข้าใช้ทรัพยากรระบบให้กับเครื่องลูกข่ายได้

1.5 เครื่องมือที่ใช้ในการพัฒนา

1. Macromedia Dreamweaver MX 2004 ใช้ในการออกแบบหน้าจออินเทอเฟสและแก้ไขโค้ด
2. MySQL เป็นฐานข้อมูลเก็บข้อมูลต่างๆในระบบ และใช้โปรแกรม phpMyAdmin เพื่อใช้ในการจัดการฐานข้อมูล
3. โปรแกรม IPTABLES ทำหน้าที่เป็น Firewall โดยนำมาประยุกต์ใช้ร่วมกับโปรแกรมที่เขียนขึ้นมาใหม่
4. Ethereal packet analyzer ใช้ในการจับและวิเคราะห์แพ็คเก็ตที่วิ่งอยู่ในเครือข่าย
5. Microsoft Visio ใช้ในการวาดรูปไดอะแกรมต่างๆ
6. Microsoft Word เพื่อใช้ในการจัดทำเอกสารประกอบโครงการ

1.6 ประโยชน์ที่คิดว่าจะได้รับ

1. สามารถนำเทคโนโลยีของ ,MySQL และ PHPไปใช้งานได้กว้างขวางขึ้น
2. สามารถนำขั้นตอนการพัฒนาโครงการในภาคทฤษฎีที่ได้เรียน มาประยุกต์ใช้งานจริง
3. เพิ่มระบบการรักษาความปลอดภัยบนเครือข่ายไร้สายมากขึ้น
4. ลดความเสี่ยงในเรื่องการเข้าใช้งานระบบจากผู้ใช้ที่ไม่ได้รับอนุญาติ
5. ผู้ดูแลระบบสามารถกำหนดขอบข่ายการเข้าถึงทรัพยากรในระบบจากผู้ใช้ที่มาจากเครือข่ายไร้สายได้ง่ายขึ้น

บทที่ 2
ความปลอดภัยของระบบเครือข่ายไร้สายและการป้องกัน

2.1 มาตรฐาน 802.11 Wireless LAN (WLAN)

มาตรฐาน 802.11 ได้ถูกประกาศใช้ขึ้นมาครั้งแรกในวันที่ 26 มิถุนายน พ.ศ. 2540 โดยกลุ่มการทำงาน 802 ของ Institute of Electrical and Electronics Engineers (IEEE) ซึ่งในมาตรฐานจะกล่าวถึงมีด้วยกันหลายเรื่องแต่มีเรื่องหลักๆที่ถูกนำมาใช้อยู่ 2 เรื่องคือการควบคุมการเข้าใช้สื่อ หรือ Medium Access Control (MAC)จะมีหลักการทำงานคล้ายๆบนมาตรฐาน 802.3 ที่ใช้ CSMA/CD แต่บนเครือข่ายไร้สาย ใช้วิธีการที่เรียกว่าCSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) และคุณสมบัติของอุปกรณ์เครือข่ายไร้สายซึ่งในข้อนี้ได้กำหนดไว้ว่าอุปกรณ์สามารถรับส่งข้อมูลได้ด้วยความเร็ว 1, 2, 5.5, 11 และ 54 Mbps บนสื่อต่าง 3 ประเภท ได้แก่ คลื่นวิทยุที่มีความถี่ 2.4 และ 5 GHz และ อินฟราเรด (Infrared) ซึ่งความเร็วในการสื่อสารของสื่อแต่ละประเภทจะไม่เท่ากัน กล่าวคือที่อินฟราเรดอุปกรณ์สามารถสื่อสารกันได้ด้วยความเร็ว 1-2Mbps คลื่นวิทยุความถี่ 2.4 GHz ซึ่งเป็นย่านความถี่ที่มาตรฐาน 802.11b เลือกใช้สามารถสื่อสารด้วยความเร็ว 1-11Mbps และที่คลื่นวิทยุความถี่ 5 GHz อุปกรณ์สามารถสื่อสารกันได้ด้วยความเร็ว 29-54Mbps และสุดท้ายคือวิธีการรักษาความปลอดภัยโดยมีจุดประสงค์หลักอยู่ 3 ประการคือ การเข้ารักษาความลับของข้อมูล การควบคุมการเข้าใช้ระบบ และความถูกต้องของข้อมูล ซึ่งหลังจากมาตรฐานได้ออกมาก็ยังมีการพัฒนาให้คุณสมบัติที่ดีขึ้นโดยมีมาตรฐาน 802.11b เป็นมาตรฐานเริ่มต้นของการพัฒนาซึ่งมีวิวัฒนาการไปหลายด้านเช่น

- มาตรฐาน 802.11a ได้ปรับปรุงในด้านความเร็วในการสื่อสารบนคลื่นวิทยุความถี่ 5 GHz
- มาตรฐาน 802.11d ได้มุ่งเน้นการพัฒนาอุปกรณ์ที่สามารถทำงานกับมาตรฐานอื่นๆได้
- มาตรฐาน 802.11e เพิ่มความสามารถในการทำ QoS (Quality of Service)
- มาตรฐาน 802.11f ได้พัฒนาโปรโตคอลที่ใช้สำหรับทำการ Roaming กันระหว่างผลิตภัณฑ์ที่ต่างกันของ

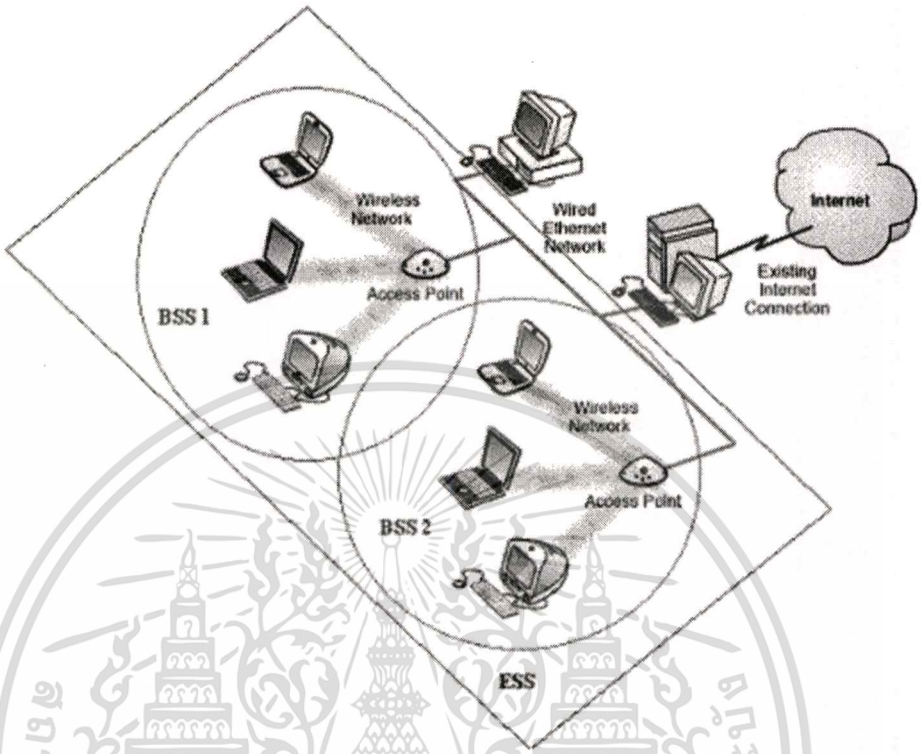
  เครื่องแม่ข่าย
- มาตรฐาน 802.11g ปรับปรุงด้านความเร็วในการสื่อสารโดยใช้เทคนิคการบีบอัดข้อมูลมาใช้โดยเพิ่มความเร็วไปที่ 54 Mbps ที่คลื่นวิทยุความถี่ 2.4 GHz

- มาตรฐาน 802.11i เป็นการปรับปรุงการรักษาความปลอดภัยที่มีช่องโหว่อยู่มากมายเช่นใช้เทคนิคใหม่ๆใน การเข้ารหัสข้อมูล และการตรวจสอบผู้ใช้เป็นต้น

2.1.1 ลักษณะของการเชื่อมต่อ

การเชื่อมต่อของมาตรฐาน 802.11 นั้นมีลักษณะอยู่ 2 แบบคือ Infrastructure Mode และ Ad-Hoc Mode แต่ละแบบจะมีการทำงาน และวิธีการนำไปใช้งานในลักษณะต่างกันดังนี้

- **การเชื่อมต่อแบบจุดต่อจุด (Peer to Peer) หรือ Ad-Hoc Mode** เป็นการติดต่อสื่อสารกันเองระหว่างอุปกรณ์เครือข่ายไร้สายเองโดยไม่ใช้อุปกรณ์ใดๆเพิ่มเติมการเชื่อมต่อแบบนี้สามารถติดต่อกันได้พร้อมๆกันได้หลายเครื่อง
- **การเชื่อมต่อกันแบบ Infrastructure Mode** การเชื่อมต่อแบบเครื่องลูกข่ายจะสามารถสื่อสารกันได้ทั้งระหว่างอุปกรณ์ เครือข่ายไร้สายด้วยกันเองและระหว่าง อุปกรณ์เครือข่ายไร้สายและเครือข่ายที่ใช้ต้องใช้สายสัญญาณ (Wired Network)โดยการเชื่อมต่อกันจะต้องสื่อสารผ่านตัวแม่ข่าย (Access Point) ซึ่งโดยปกตินั้นตัวแม่ข่ายจะมีทั้งอุปกรณ์รับคลื่นวิทยุที่ใช้ในเครือข่ายไร้สาย และอุปกรณ์เชื่อมต่อกับเครือข่ายที่ต้องใช้สายสัญญาณ อย่างเช่น RJ45 เป็นต้นดังนั้นตัวแม่ข่ายนี้จึงเสมือนจุดเชื่อมต่อระหว่างเครือข่ายทั้งสองชนิดได้ โดยที่บริเวณพื้นที่ที่เครื่องแม่ข่าย 1 เครื่องสามารถให้บริการได้เรียกว่า BSS (Basic Service Set) ซึ่งจะอยู่ในช่วงประมาณ 50 เมตร(ในอาคาร) และ 400 เมตร(นอกอาคาร) เพราะBandwidth ของสัญญาณจะลดลงเมื่อระยะทางเพิ่มขึ้น (ที่ระยะประมาณ 400 เมตร Bandwidth จะอยู่ที่ประมาณ 1 Mbps) ซึ่งจะเห็นว่าเครื่องแม่ข่าย 1 เครื่องไม่สามารถให้บริการได้ทั่วถึงมาตรฐาน 802.11 จึงได้มีแนวคิดของ IBSS (Independent Basic Service Set) ซึ่งเป็นแนวคิดที่ว่าเครื่องลูกข่ายไม่จำเป็นต้องยึดติดกับเพียงเครื่องแม่ข่ายเครื่องเดียว ดังนั้นออกแบบให้มีการใช้เครื่องแม่ข่ายหลายๆเครื่องได้เพื่อขยายพื้นที่ให้บริการและเรียกกลุ่มของเครื่องของแม่ข่ายนั้นว่า ESS (Extend Service Set) ดังรูป



รูปที่ 2.1 แสดงการให้บริการในลักษณะต่างๆ ของเครื่องแม่ข่าย

ซึ่งขั้นตอนการเข้าใช้ระบบของเครื่องลูกข่ายมีขั้นตอนดังนี้ เมื่อเครื่องลูกทำการเปิดเครื่องขึ้นมาก็จะทำการค้นหาเครื่องแม่ข่ายที่มีพื้นที่ครอบคลุมการให้บริการที่ตัวอยู่และเริ่มทำการขออนุญาตกับเครื่องแม่ข่ายเพื่อที่จะทำการเข้าใช้ระบบ และเมื่อทำการตรวจสอบกันสำเร็จแล้วก็เริ่มมีการรับส่งข้อมูล ซึ่งในขั้นตอนนี้มีบริการของเครื่องลูกข่าย ใช้อยู่ 4 บริการดังนี้

1. Authentication Service เป็นบริการที่ใช้ตรวจสอบสิทธิการเข้าใช้เครือข่าย
2. De-authentication Service เป็นบริการที่ถูกใช้เพื่อทำการยกเลิกการเข้าใช้งานหรือ logoff ออกจาก เครื่องแม่ข่ายนั้นมีผลให้เครื่องลูกข่ายไม่สามารถเข้าใช้งานได้ บริการนี้จะถูกใช้เมื่อเครื่องลูกข่ายหยุดทำงาน หรือในกรณีที่มีการ roamingแล้วเครื่องลูกข่ายนั้นได้ออกนอกเขตการให้บริการแล้ว เครื่องแม่ข่ายนั้นก็จะปล่อยข้อมูลของเครื่องลูกข่ายนี้ให้กับเครื่องแม่ข่ายอื่น
3. Data Delivery Service เป็นบริการที่ใช้ตรวจสอบว่าข้อมูลที่ส่งไปถึงผู้รับถูกต้องและครบถ้วน
4. Privacy Service เป็นบริการป้องกันข้อมูลที่ส่งไปนั้นปลอดภัยจากผู้อื่นเข้าถึงตัวข้อมูลได้

และหากถ้าเป็นตามแนวคิดของ IBSS แล้วละก็จะมีขั้นตอนของการให้บริการเพิ่มมากขึ้นซึ่งการติดต่อสื่อสารกันระหว่างอุปกรณ์ เครือข่ายไร้สายและเครื่องแม่ข่าย คือ

1. Association Service เป็นบริการที่มาใช้สร้างการเชื่อมต่อกันระหว่างลูกข่าย และแม่ข่ายซึ่งในขณะหนึ่งนั้นลูกข่ายสามารถติดต่อสื่อสารได้กับเครื่องแม่ข่ายได้เครื่องเดียวเท่านั้นแต่สามารถทำกระบวนการตรวจสอบกับเครื่องแม่ข่ายอื่นหลายๆ เครื่อง ได้
2. Reassociation Service เป็นบริการที่ใช้ในกรณีที่เครื่องแม่ข่ายทำการสื่อสารกัน และเครื่องลูกข่าย กำลังติดต่อกับ เครื่องแม่ข่าย เครื่องใหม่เพื่อที่จะทำการเปลี่ยนมาใช้ เครื่องแม่ข่าย อันใหม่ โดย เครื่อง ลูกข่าย จะทำการบอก เครื่องแม่ข่าย เครื่องใหม่ว่าตนเองมาจาก เครื่องแม่ข่ายไหน จากนั้น เครื่องแม่ ข่าย ใหม่จะไปเอาข้อมูลจากเครื่องแม่ข่ายเครื่องเก่ามาใช้งาน
3. Disassociation Service เป็นบริการที่ใช้ในกรณีทำการยกเลิกการเชื่อมต่อกันระหว่างเครื่องแม่ข่ายและเครื่องลูกข่าย อันเนื่องมาจากเครื่องแม่ข่าย ปิดไปหรือเครื่องลูกข่ายได้ออกจากพื้นที่ให้บริการไปแล้ว
4. Distribution Services เป็นบริการที่ใช้ในการตัดสินใจของเครื่องแม่ข่ายว่าจะให้ข้อมูลนั้นสมควรถูกส่งต่อไปทางไหน เช่นส่งต่อไปยังเครื่องแม่ข่ายตัวอื่น หรือส่งเข้ามาทางเครือข่ายที่ต้องใช้สายสัญญาณ
5. Integration Service เป็นบริการที่ใช้ในการแปลงรูปแบบของข้อมูลไปมาระหว่างรูปแบบบน เครือข่ายที่ต้องใช้สายสัญญาณ กับ รูปแบบบนเครือข่ายไร้สาย

2.1.2 ระบบรักษาความปลอดภัยของมาตรฐาน 802.11

วิวัฒนาการของมาตรฐาน 802.11 ที่กล่าวมาข้างต้นนั้นจะเห็นได้ว่ามีการพัฒนาระบบรักษาความปลอดภัยนั้นได้ถูกคำนึงถึง และออกแบบพัฒนามาเพียง 2 มาตรฐานเท่านั้นคือ 802.11i ซึ่งออกแบบมาเพื่อแก้ไขข้อบกพร่องที่มีอยู่หลายประการ บนมาตรฐาน 802.11b ที่ถูกประกาศใช้ขึ้นมาก่อนเช่นการใช้วิธีเข้ารหัสที่ซับซ้อนขึ้น แต่อย่างไรก็ดีในขณะนี้รายละเอียดของมาตรฐานนี้ยังไม่ได้ถูกประกาศใช้ ดังนั้นในขณะนี้จึงควรศึกษาทำความเข้าใจก่อนว่าบนมาตรฐาน 802.11b นั้นใช้เทคนิคอะไรในการรักษาความปลอดภัย และมีจุดอ่อนตรงไหน และมีวิธีแก้ไขช่องโหว่เหล่านั้นอย่างไร

การรักษาความปลอดภัยของมาตรฐาน 802.11b

ระบบรักษาความปลอดภัยบนมาตรฐาน 802.11b นั้นส่วนมากจะออกแบบมาโดยอ้างอิงถึงการเชื่อมต่อแบบ Infrastructure เป็นหลัก และทำงานถึงระดับ Link Layer (แบ่งตาม OSI) เท่านั้น ซึ่งการตั้งค่าความปลอดภัยนั้นประกอบด้วยส่วนต่างๆ ประกอบเข้าด้วยกัน และแต่ละส่วนจะมีหน้าที่ต่างกันดังนี้

SSID

โดยตัว SSID นั้นเป็นการตั้งค่าที่เครื่องแม่ข่ายและที่เครื่องแม่ข่ายเพื่อเป็นการบอกความแตกต่างในการทำการเชื่อมต่อกันว่าเครื่องแม่ข่ายนี้จะเชื่อมต่อเข้ากับเครื่องแม่ข่ายเครื่องไหนซึ่งแต่ละเครื่องแม่ข่ายนั้นจะมีการตั้งค่านี้มาให้แล้วตามแต่ละเจ้าของผลิตภัณฑ์จะกำหนดเช่น Linksysจะมีค่าเริ่มต้นเป็น “linksys” ,Cisco จะมีค่าเป็น ”tsunami” (ค่าพวกนี้เป็น Case Sensitive) ซึ่งประโยชน์ที่ได้รับจากค่านี้นอกจากจะเป็นการแยกการเข้าไปใช้งานของClientแล้วยังสามารถทำตัวเป็นเหมือนPassword ในการเข้าติดต่อในเบื้องต้นเพราะหากกำหนดค่านี้ที่เครื่องลูกข่ายไม่ตรงกับของเครื่องแม่ข่าย เครื่องลูกข่ายนั้นก็ไม่สามารถเข้าไปใช้งานเครื่องแม่ข่ายนั้นได้ ดังนั้นจึงควรแก้ไขค่าเริ่มต้นที่แต่ละผลิตภัณฑ์กำหนดมา และหลักการตั้งค่าควรตั้งให้มีความยากต่อการเดาพอสมควร

โปรโตคอล WEP(Wired Equivalent Privacy)

โปรโตคอล WEP นี้ถูกนำมาใช้เป็นโปรโตคอลหลักในการรักษาความปลอดภัยบนมาตรฐาน 802.11b โดยที่โปรโตคอลดังกล่าวจะถูกออกแบบมาเพื่อใช้รักษาความปลอดภัยในส่วนต่างๆคือ การตรวจสอบการเข้าใช้ระบบ , การรักษาความลับของข้อมูลในระหว่างการสื่อสาร และ ความถูกต้องของข้อมูลเมื่อข้อมูลได้ถึงที่หมายแล้ว สำหรับรายละเอียดในการทำงานของโปรโตคอล WEP(Wired Equivalent Privacy)ที่สามารถทำหน้าที่ในส่วนต่างๆนั้นมีวิธีการและขั้นตอนการทำงานดังนี้

<u>การเข้ารหัส</u>

โปรโตคอล WEP จะทำงานโดยจะอ้างอิงถึง secret key (k) ที่ไว้ใช้ในการเข้ารหัส ซึ่ง secret key นี้จะถูกเก็บไว้ที่ผู้ส่งข้อมูล และผู้รับข้อมูลหรือจะกล่าวอีกนัยหนึ่งก็คือ WEP เป็นการเข้ารหัสแบบสมมาตร (Symmetric) นั่นเอง โดยการทำงานในการเข้ารหัสข้อมูลมีขั้นตอนดังนี้

1. WEP จะทำกลไกในการหาค่า Check Sum (c(M))ของข้อมูลดิบ (M)ที่ต้องการจะส่งแล้วนำมาต่อท้ายที่ข้อมูลดิบ ก็จะได้ข้อมูลมาชุดหนึ่ง(P) หรือเขียนในรูปแบบของสมการได้ดังนี้

   P = (M,c(M))

2. WEP จะคำนวณค่า Key Stream ที่ได้มาจากการทำงานของฟังก์ชัน RC4 ซึ่งตัวแปรนี้มีด้วยกัน 2ตัว คือ

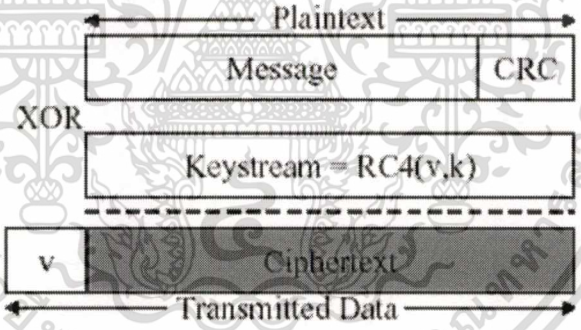
Initial Vector (v) เป็นค่าที่สุ่มออกมา(ซึ่งผลิตภัณฑ์แต่ละชนิดจะมีวิธีการสุ่มค่านี้ออกมาไม่เหมือนกัน) มีจำนวน คงที่ 24 bits ค่านี้จะทำการสุ่มขึ้นมาใหม่ทุกครั้งเมื่อมี packet ใหม่เข้ามาและตัวแปร Key (k) เป็นค่าที่ผู้ใช้สามารถกำหนดเองได้ซึ่งและจะมีความยาว 40,104 หรือ 232 bitsก็ได้ และเมื่อนำตัวแปร v และ k มาเข้ารหัสกันจะได้ Key Stream ความยาว 64 ,128 และ 256 bits ตามลำดับ จากนั้นก็ทำการเข้ารหัสข้อมูลโดยนำข้อมูล P และ Key Stream มาทำการ XOR กัน bit ต่อ bit ก็จะได้ ผลลัพธ์เป็น Cipher Text (C) ออกมาสามารถเขียนในรูปแบบของสมการได้ดังนี้

$C = P \oplus RC4(v,k)$; $\oplus$ = XOR

3. จากนั้นทำการส่งข้อมูลไปที่จุดหมายโดยทำการส่งค่า IV (เป็นรูปแบบ Plain Text) พร้อมกับ Cipher Text ออกไปหาจุดหมาย (ดังขั้นตอนในรูปที่ 3) สามารถเขียนในรูปแบบของสมการได้ดังนี้

$A \rightarrow B : v , P \oplus RC4(v,k)$; $P = (M,c(M))$

หรือรูปแบบของข้อมูลที่ส่งออกไปจะเป็นดังรูปที่ 2



รูปที่ 2.2 แสดงการเข้ารหัสของโปรโตคอล WEP

<u>การถอดรหัสข้อมูล</u>

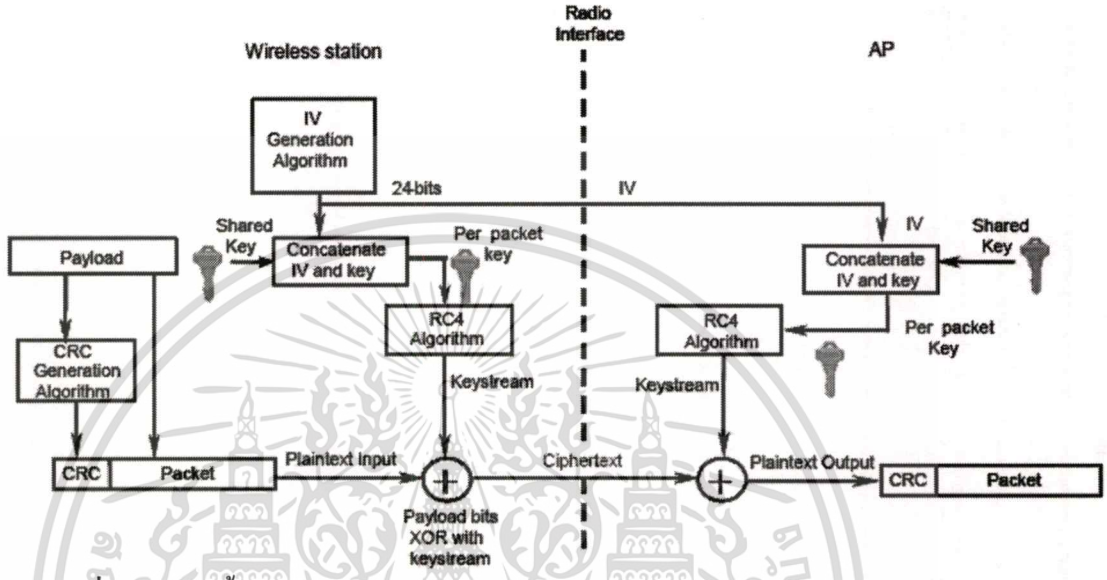
1. เมื่อผู้รับได้ข้อมูลที่ทำการเข้ารหัสมาแล้ว จะดึงเอาค่า v อ อกมาเพื่อนำไปเข้าฟังก์ชัน RC4 โดยใ ช้ key (k) ซึ่งได้กำหนดไว้แล้วก็จะได้ Key Stream ของตัวเองออกมา
2. นำค่า Key Stream นั้นมาทำการ XOR กับข้อมูลที่ถูกเข้ารหัสมา ถ้าหากไม่มีข้อผิดพลาดอะไรก็จะได้ข้อมูลที่ต้องการออกมาสามารถเขียนในรูปแบบของสมการได้ดังนี้

$P' = C \oplus RC4(v,k)$

$= (P \oplus RC4(v,k)) \oplus RC4(v,k)$

$= P$

3. ทำการคำนวณค่า Checksum จากข้อมูลที่ถอดรหัสแล้ว และตรวจสอบว่าค่านั้นตรงกับค่าที่ส่งมาหรือไม่ ถ้าหากค่านั้นไม่ตรงกับค่าที่ส่งมาก็แสดงว่าข้อมูลอาจจะถูกเปลี่ยนแปลงมาแล้ว ดังขั้นตอนในรูปที่ 2.3



รูปที่ 2.3 แสดงขั้นตอนการเข้ารหัสและถอดรหัสข้อความของโปรโตคอล WEP

Authentication Type

การAuthentication เป็นการตรวจสอบสิทธิการเข้าใช้ระบบ โดยมาตรฐานของ 802.11b นั้นจะทำได้ 2 ลักษณะคือ Shared Key Authentication และแบบ Open Authentication ซึ่งแบบ Open Authentication เป็นแบบที่ง่ายที่สุดและเป็นค่าเริ่มต้นที่ถูกกำหนดมาให้ กล่าวคือวิธีนี้จะอนุญาตให้ทุกคนสามารถเข้ามาได้เลยโดยที่ไม่มีการตรวจสอบอะไรทั้งสิ้น ส่วนในแบบ Share key Authentication ก่อนที่เครื่องลูกข่ายจะเข้ามาจะต้องส่งคำร้องขอที่จะเข้าใช้งานไปที่เครื่องแม่ข่ายจากนั้นเครื่องแม่ข่ายจะส่ง challenge text มาที่ เครื่องลูกข่าย และเครื่องลูกข่ายจะทำการเข้ารหัสข้อความนั้นโดยใช้คีย์ตัวเดียวกับ WEP key แล้วส่งกลับไปที่เครื่องแม่ข่าย จากนั้นเครื่องแม่ข่ายจะทำการตรวจสอบว่าเข้ารหัสมาอย่างถูกต้องหรือไม่ถ้าถูกต้องก็อนุญาตให้เข้าใช้ระบบต่อไป

MAC Filter

เป็นวิธีการตรวจสอบการเข้าใช้ระบบอีกวิธีหนึ่งซึ่งทำโดยตรวจสอบ MAC Address ที่เข้ามาติดต่อว่าเป็น MAC ที่ได้รับอนุญาตหรือไม่ โดยผู้ดูแลระบบจะต้องทำกับเพิ่ม MAC Address ที่อนุญาตเข้าไปที่เครื่องแม่ข่ายที่ละMAC Address ซึ่งจุดนี้จะเป็นข้อเสียหนึ่งของวิธีนี้เพราะถ้าหากเป็นระบบใหญ่มีเครื่องแม่ข่ายอยู่เป็นจำนวนมากจะทำให้เป็นงานหนักมากสำหรับผู้ดูแลระบบ

2.1.3 ช่องโหว่ของการรักษาความปลอดภัยของมาตรฐาน 802.11b

เนื่องจากวิธีการรักษาความปลอดภัยของมาตรฐาน 802.11bที่เลือกใช้ ยังมีช่องโหว่อยู่เป็นจำนวนมาก และในขณะนี้ในInternet ก็ได้มีโปรแกรมที่ใช้ในการโจมตีช่องโหว่เหล่านี้เป็นจำนวนมาก ซึ่งจุดอ่อนเหล่านั้นสามารถแบ่งเป็นส่วนๆ ตามวิธีการที่ใช้รักษาความปลอดภัยรูปแบบต่างๆได้ดังนี้

จุดอ่อนของ SSID

การกำหนดค่า SSID นี้จะแสดงออกมาให้เห็นเป็น plain text ธรรมดาจะไม่มีการซ่อนหรือปิดบังค่าเหล่านั้น เหมือนกับการใส่Password ทั่วๆไป และช่องโหว่อีกข้อหนึ่งก็คือ การออกแบบมาเพื่อให้ผู้ใช้ หรือเครื่องแม่ข่ายเข้ามาใช้งานได้สะดวกมากขึ้น ดังนั้นพฤติกรรมของเครื่องแม่ข่ายนั้นจะทำการกระจายข้อมูลSSIDของตัวเองออกมาทุกๆ1-2 วินาที เพื่อให้เครื่องลูกข่ายนั้นใช้ติดต่อเข้ามาโดยอัตโนมัติซึ่งเป็นค่าที่ถูกกำหนดมาจากโรงงาน แต่จุดนี้จะเปิดช่องทางให้ผู้ไม่หวังดีเชื่อมต่อเข้าได้ง่ายเหมือนกัน ดังนั้นเพื่อความปลอดภัยที่เพิ่มขึ้นก็ควรจะปิดคุณสมบัติการกระจายข้อมูลในส่วนนี้ออกไป

จุดอ่อนของวิธีการAuthenticate แบบ Shared key

ช่องโหว่นี้สามารถนำไปสู่ค่าคีย์ที่ใช้กับการเข้ารหัสของข้อมูลได้โดยการรวบรวมข้อมูลในขั้นตอนต่างๆกล่าวคือ

1. ในขั้นตอนการที่เครื่องแม่ข่ายส่ง Challenge Text ออกมานั้น(เป็นในรูปแบบของ Plain text)
2. ข้อมูล Challenge Text ที่ถูกเข้ารหัสแล้ว ในช่วงการตอบรับ Challenge Text จาก node

เมื่อนำค่าดังกล่าวมาเข้าฟังก์ชันRC4 ก็จะได้ผลลัพธ์ออกมาเป็นคีย์ที่ใช้เข้ารหัสตัว Challenge text ซึ่งเป็นคีย์ของที่ใช้ในการเข้ารหัสของโปรโตคอลWEP นั่นเอง ดังนั้นหากเราใช้วิธีการ Shared key ในการ Authenticate อาจเป็นการเพิ่มจุดอ่อนของระบบมากกว่าเป็นทางที่จะรักษาความปลอดภัยก็ได้

จุดอ่อนของโปรโตคอล WEP

การนำฟังก์ชัน RC4 มาใช้ในโปรโตคอลนี้ทำให้เกิดช่องโหว่เนื่องจาก Packet ของ เครือข่ายไร้สาย ที่ทำการติดต่อสื่อสารกันอยู่นั้นประกอบไปด้วยค่า IV และ Cipher Text (ค่า IV จะมีค่าเปลี่ยนไปเรื่อยทุกครั้งที่ทำการส่ง Packet)ซึ่งส่วนของ Cipher Text นั้นถูกเข้ารหัสไว้เรียบร้อยแล้วในส่วนของค่า IV นั้นไม่ได้ทำการเข้ารหัสใด ๆเลย ดังนั้นผู้ไม่ประสงค์ดีก็จะสามารถดักจับค่านี้มาใช้ประโยชน์ในการเป็นส่วนหนึ่งของการถอดรหัสข้อมูลได้ โดยผู้บุกรุกจะทำการดักจับ Packet ที่ใช้ค่า IV ที่เหมือนกันในการเข้ารหัส ซึ่งมีความเป็นไปได้เป็นอย่างยิ่ง เนื่องจากความยาวของ IV นั้นมีเพียง 24 bit หรือมีเป็นจำนวน 16,77,216 ค่า (2^24) ซึ่งเป็นค่าที่น้อยมาก เมื่อเทียบกับจำนวนครั้งที่ทำการ Packet ใน Network ที่มีการใช้อย่างหนาแน่นและยังมีในกรณีที่การ์ด PCMCIA เมื่อทุกครั้งที่ทำการ Re-

Initialize ก็จะทำการรีเซตค่า IV มีค่าเป็น “0” เสมอ ดังนั้นจึงมีโอกาสที่จะสุ่มค่า IV ที่เหมือนกันขึ้นมาใช้ หลังจากนั้นก็นำ Packet ทั้งสองมา XOR กันจะได้ผลลัพธ์ดังสมการ

$C1 = P1 \oplus RC4(v,k)$;เป็น Cipher Text1

$C2 = P2 \oplus RC4(v,k)$;เป็น Cipher Text2

ซึ่ง ค่าของ v(v = IV) และ k ที่ C1 และ C2 ใช้เป็นค่าเดียวกัน และนำทั้งสองสมการมา XOR กันจะได้

$C1 \oplus C2 = (P1 \oplus RC4(v,k)) \oplus (P2 \oplus RC4(v,k))$

$C1 \oplus C2 = P1 \oplus P2$

ซึ่งในตอนนี้จะทราบค่าของ $C1 \oplus C2$ จากนั้นผู้บุกรุกจะทำการหาค่า P1 หรือ P2 ให้ได้โดยใช้เทคนิคต่างๆเช่นทำการสุ่มแทนค่าของ P ตัวใดตัวหนึ่งลงในสมการแล้วดูผลลัพธ์ของ P อีกตัวว่าเป็นคำที่มีความหมายหรือไม่ ซึ่งคำที่ใช้สุ่มนั้นอาจเป็นคำที่ระบบ หรือโปรโตคอลใดโปรโตคอลหนึ่งใช้เป็นประจำ หรือเป็นค่า IP Address มีมีอยู่ในNetwork วงนั้น เช่น Password: , Login: , Ack , 192.168.1.255 หรืออาจจะใช้วิธีที่ดูเป็นตัวอักษรเลยก็ได้ โดยดูว่ามีตัวอักษร 2 ตัวใดๆ ที่สามารถทำการ XOR แล้วจะมีค่าเท่ากับค่าของที่ C1 XOR C2 บ้าง หรือไม่ผู้บุกรุกได้เตรียมการตั้งแต่ต้นโดยทำการส่ง spam mail ซึ่งข้อความในเนื้อจดหมายผู้บุกรุกเป็นผู้กำหนดเอง เข้าไปในระบบ เครือข่ายไร้สายแล้วดักจับ Packet รอจนกว่าจะมีการตอบกลับมาแล้วทำการสุ่มเอา Packet ที่มีค่า IV เหมือนกันคู่หนึ่งมาทำกระบวนการข้างต้นแล้วทำการ Brute Force ด้วยข้อความที่อยู่ในจดหมาย ซึ่งหลังจากได้ค่าต่างๆครบแล้วผู้บุกรุกก็สามารถทำการหาค่า คีย์ ที่ใช้ในการเข้ารหัสของทุกๆ Packet ได้ และที่แย่ไปกว่านั้นยังมีค่า IV บางค่านั้นเรียกว่า Weak IV ซึ่งเมื่อ WEP นำค่านี้ไปใช้เข้ารหัสแล้วก็จะพบว่า Cipher Text ที่ได้จะเผยให้เห็นค่า WEP key บางส่วนออกมาให้เห็นด้วย นอกจากนี้ยังมีคุณสมบัติบางข้อของ WEP Protocol ที่ทำให้ไม่สามารถรักษา Integrity ของข้อมูลได้ดังนี้

การ Check Sum ของโปรโตคอล WEP มีลักษณะเป็นฟังก์ชันแบบเชิงเส้นกับข้อมูลที่ทำการ Check Sum กล่าวคือ ถ้าทำการหา Checksum ของข้อความ x ที่ทำการ XOR กับข้อความ y ก็จะมีค่าเท่ากับค่า Checksum ของข้อความ x ทำการ XOR กับข้อความ y

จากสมการในการหา Cipher Text คือ

$C = RC4(v,k) \oplus (M,c(M))$ ----------(1)

จะสามารถหา C’ ที่สามารถถอดรหัสได้ M’ โดยนำค่าๆหนึ่งที่เปลี่ยนแปลงไปจากเดิมพร้อมด้วย Checksum ของค่านั้น $(\Delta , c(\Delta))$ มาทำการ XOR ทั้งสองด้านของสมการ (1) จะได้

$C' = C \oplus (\Delta , c(\Delta)) = RC4(v,k) \oplus (M,c(M)) \oplus (\Delta , c(\Delta))$

$= RC4(v,k) \oplus (M \oplus \Delta , c(M) \oplus c(\Delta))$

$= RC4(v,k) \oplus (M' , c(M \oplus \Delta))$

$= RC4(v,k) \oplus (M' , c(M')) \text{ ----------(2)}$

ดังนั้นจากสมการ (2) แสดงให้เห็นว่าข้อมูล A->B : (v,C) สามารถถูกเปลี่ยนค่าภายในใหม่ได้ (M') โดยทำการคำนวณหาค่า Cipher Text ใหม่จะได้ C' โดยที่ข้อมูลนี้ถ้าถูกส่งออกไปแล้วทางผู้รับจะไม่ทราบเลยว่าข้อมูลนั้นถูกเปลี่ยนแปลงเรียบร้อยแล้ว จากจุดอ่อนตรงนี้ทำให้ผู้ไม่ประสงค์ดีสามารถนำไปประยุกต์เพื่อทำการขโมยข้อมูลหรือทำการโจมตีแบบ Man in the middle ได้โดยการทำการเปลี่ยนหมายเลข IP ต้นทางและปลายทางได้โดยที่เครื่องปลายทางไม่รู้ตัว และคุณสมบัติอีกประการที่เป็นจุดอ่อนที่สำคัญก็คือ Checksum ของ WEPเป็นฟังก์ชันที่ไม่ได้นำ WEP คีย์มาเป็นส่วนประกอบของฟังก์ชันทำให้ผู้บุกรุกสามารถทำการติดต่อสื่อสารกับเครื่องแม่ข่ายได้โดยไม่จำเป็นต้องทราบค่า WEP คีย์โดยผู้บุกรุกสามารถใช้ประโยชน์จากจุดอ่อนนี้ได้โดยจะต้องรู้ค่าของ Plain Text (P) ชุดหนึ่งเมื่อถูกเข้ารหัสแล้วจะได้ข้อมูลเป็นอย่างไร (C)แล้วนำข้อมูลสองชุดนั้นมา XOR กัน ตามสมการ

$P \oplus C = P \oplus (P \oplus RC4(v,k)) = RC4(v,k) \text{ ----------(3)}$

จากสมการ (3) จะได้ค่า RC4(v,k) ออกมา และเนื่องจากค่า v นั้นเป็นค่าที่ WEP อนุญาตให้เป็นค่าที่ใช้ซ้ำได้ดังที่ได้กล่าวมาแล้ว ดังนั้นจึงสามารถสร้างค่า M' ได้โดยใช้ค่า C' จากสมการ

$C' = (M' , c(M')) \oplus RC4(v,k) \text{ ----------(4)}$

จากสมการ (4) จะเห็นว่าค่า Checksum ของ M' เป็นฟังก์ชันที่ไม่เกี่ยวกับ WEP คีย์ดังนั้นจึงสามารถหาค่า C' ได้จึงมีผลทำให้สามารถติดต่อกับเครื่องแม่ได้โดยไม่จำเป็นต้องทราบค่า WEP คีย์

จุดอ่อนของ MAC Filter

จากจุดอ่อนของโปรโตคอล WEP ที่สามารถหาค่า WEP key ออกมาได้นั้นทำให้สามารถเข้าถึงข้อมูลบน เครือข่ายไร้สายได้ทั้งหมดรวมถึงค่า MAC Address ที่ใช้งานอยู่ในระบบด้วย ดังนั้นการปลอม MAC Address (Spoof) ให้เหมือนกับค่า MAC Address ที่ใช้อยู่ ก็จะทำให้เกิดการบุกรุกขึ้นได้

2.1.4 รูปแบบการโจมตีช่องโหว่และข้อเสนอแนะในการแก้ไขจุดอ่อนบนระบบรักษาความปลอดภัยบนเครือข่ายไร้สาย

1. เครื่องแม่ข่าย ที่ติดตั้งไม่ได้รับอนุญาตจากผู้ดูแลระบบ

การที่มีการติดตั้งเครื่องแม่ข่ายที่ไม่ได้รับอนุญาตจากผู้ดูแลระบบไม่ว่าจะเป็นการกระทำโดยรู้เท่าไม่ถึงการณ์ของคนในองค์กร นั้นอาจนำมาสู่ช่องโหว่ที่ทำให้ระบบถูกโจมตีได้โดยง่าย เนื่องจากเครื่องแม่ข่ายที่ทำการติดตั้งขึ้นมาใหม่นั้นอาจจะมีการปรับใช้ค่าความปลอดภัยที่ไม่ดีพอหรือไม่ตรงกับนโยบายขององค์กร หรืออาจจะเป็นในกรณีการจงใจติดตั้งเครื่องแม่ข่ายเพื่อเป็น

ช่องทางในการเข้าใช้ระบบของเราของผู้ไม่ประสงค์ดี ดังนั้นเรื่องนี้เป็นเรื่องที่ค่อนข้างสำคัญที่ผู้ดูแลระบบควรทำการตรวจสอบหรือทำ site survey บริเวณในองค์กรเพื่อตรวจสอบอุปกรณ์เครือข่ายไร้สายที่ไม่พึงประสงค์อาจจะเล็ดลอดเข้ามาในระบบ

2. การออกแบบการวางเครื่องแม่ข่าย และปรับแต่งเสาอากาศ

ตำแหน่งการวางเครื่องแม่ข่ายก็สิ่งที่สำคัญอย่างหนึ่ง เนื่องจากเป็นการบอกขอบเขตการให้บริการว่าจะครอบคลุมถึงพื้นที่ไหนบ้าง บ่อยครั้งที่ผู้ดูแลระบบไม่ได้นึกถึงเรื่องนี้ทำให้พื้นที่ให้บริการของเครื่องแม่ข่ายเกินขอบเขตพื้นที่ที่ดูแลอยู่ ดังนั้นจุดนี้จึงเป็นจุดที่เปิดโอกาสให้ผู้อื่นสามารถเข้ามาแอบเข้ามาใช้งานระบบเราได้ดังนั้นทางผู้ดูแลระบบนั้นควรจะตอบคำถามได้ว่าจุดให้บริการนั้นครอบคลุมถึงบริเวณไหนบ้าง อยู่ในพื้นที่ๆดูแลได้ทั่วถึงได้หรือไม่ และบริเวณที่ไม่สามารถเข้าไปดูแลได้นั้นจะเปิดโอกาสให้ผู้อื่นเข้ามาได้หรือไม่ ซึ่งในขณะนี้มีผลิตภัณฑ์บางเจ้าเปิดโอกาสให้มีการปรับแต่งค่าความแรงของสัญญาณคลื่นวิทยุบนเครื่องแม่ข่ายได้ หรืออาจใช้เทคนิคบางอย่างในการปรับแต่งเสาอากาศของเครื่องแม่ข่ายเพื่อกำหนดพื้นที่ให้บริการได้

3. การติดตั้งและปรับแต่งการใช้งานไม่ถูกวิธี

ส่วนมากอุปกรณ์เมื่อได้จัดซื้อมาเราแทบจะไม่ต้องมีการปรับแต่งค่าใดๆเลยก็สามารถทำงานได้เลยทันทีเพราะทางผู้ผลิตได้ตั้งค่าพื้นฐานไว้แล้วซึ่งค่าเหล่านั้นไม่ได้ใช้ความสามารถทางการป้องกันความปลอดภัยอย่างเต็มที่ ตรงจุดนี้หากปล่อยให้มีการใช้งานไปเรื่อยๆโดยไม่ได้ศึกษาว่าความสามารถที่ไม่ได้ใช้นั้น เช่นการเข้ารหัสข้อมูล การตรวจสอบการเข้าใช้ระบบ ก็จะทำให้ความปลอดภัยในระบบลดลง ในทางที่ดีเราควรจะศึกษาถึงความสามารถของผลิตภัณฑ์นั้นแล้วนำมาประยุกต์ใช้งานให้เข้ากับนโยบายขององค์กร ในปัจจุบันได้มีบุคคลหรือกลุ่มคนได้ทำการสำรวจหาจุดที่มีสัญญาณของเครื่องแม่ข่ายที่มีการปรับแต่งค่าไม่ถูกต้องซึ่งมีผลให้สามารถเข้าไประบบนั้นๆและใช้ทรัพยากรต่างๆได้จากนั้นจะนำมาเผยแพร่จุดหรือสถานที่ดังกล่าวบน Internet ซึ่งเราเรียกวิธีการนี้ว่า War Driving หรือ War Chalking (http://www.warchalking.org/)

4. อุปกรณ์สูญหายหรือถูกขโมย

ส่วนมากอุปกรณ์ไร้สายนั้นถูกออกแบบมาเพื่อให้พกพาสะดวก เคลื่อนย้ายง่ายดังนั้นก็เป็นการง่ายที่จะสูญหายหรือถูกขโมยเช่นกันทำให้ผู้ที่ได้ครอบครองไปนั้นมีโอกาสเข้ามาใช้งานในระบบได้หากมีระบบรักษาความปลอดภัยที่ไม่ดีพอดังนั้นในองค์กรควรมีนโยบายหรือข้อกำหนดหลังจากอุปกรณ์นั้นสูญหายไปผู้รับผิดชอบต้องปฏิบัติอย่างไรเช่นต้องทำการแจ้งผู้ดูแลระบบภายในกี่ชั่วโมง หรือใช้หลักการของ 2 Factor Authentication เพื่อแก้ปัญหานี้

5. การถูกดักจับข้อมูล

ดังที่ได้อธิบายว่าจุดอ่อนของโปรโตคอล WEP นั้นมีจุดอ่อนหลายจุดที่สามารถทำให้ทราบถึง WEP key ที่ใช้ในการเข้ารหัส Packet ซึ่งในขณะนี้มีเครื่องมือมากมายเช่น Air Snort (http://airsnort.shmoo.com/) ,Aero Peek (http://www.wildpackets.com/), NetStumbler (http://www.netstumbler.com/)ที่นำจุดอ่อนตรงนี้มาใช้ประโยชน์ซึ่งแม้แต่ผู้ใช้ไม่จำเป็นต้องมีความรู้ในเรื่องช่องโหว่ใดๆเลยแต่ก็สามารถดักจับและ Decode Packet เหล่านั้นได้ดังนั้นมีข้อแนะนำให้ใช้การเข้ารหัสในส่วนอื่นเช่นในระดับ Application พวก SSH , SSL ในระดับ Internet Network เช่นพวก IPSec, VPN เพิ่มเติมเพราะถึงแม้ว่า WEP key จะถูกถอดรหัสออกมาได้แต่ก็ยังติดการเข้ารหัสอีกทีหนึ่ง แต่วิธีนี้จะทำให้มี over head ในการทำงานเพิ่มขึ้นตามไปด้วย

6. การส่งสัญญาณรบกวนระบบ และการขัดขวางการให้บริการ

ในย่านความถี่วิทยุ 2.4GHz และครอบคลุมความถี่เต็มย่านความถี่ระหว่าง 2,400HZ ถึง 2,483HZ ที่มาตรฐาน802.11มาใช้เป็นสื่อในการสื่อสารนั้นเป็นย่านความถี่ในย่านที่เรียกว่า ISM (Industrial Scientific Medicine) ที่เป็นย่านที่ไว้ใช้ในวงการอุตสาหกรรม วงการวิจัยทางวิทยาศาสตร์และการแพทย์ทั่วโลกดังนั้นการใช้อุปกรณ์บางอย่างเช่น โทรศัพท์ไร้สาย หรืออุปกรณ์ที่ใช้เทคโนโลยี Bluetooth ในระบบเครือข่ายไร้สายอาจมีผลผกระทบกับการทำงานของระบบ เครือข่ายไร้สาย ได้ดังนั้นจึงควรระวังเรื่องสิ่งแวดล้อมของสถานที่ที่จะนำระบบนี้มาใช้ซึ่งในกรณีนี้เราสามารถตรวจสอบและป้องกันได้ แต่ในกรณีที่มีผู้บุกรุกที่ผลิตอุปกรณ์ที่สามารถส่งคลื่นวิทยุในย่านดังกล่าวออกมาเพื่อทำการปล่อยออกมาเพื่อรบกวนและขัดขวางการทำงานของระบบนั้นเป็นการยากที่ทำการป้องกันได้ ดังนั้นควรจะมีระบบหรือ software ที่คอยทำการตรวจสอบว่ามีอุปกรณ์หรือสัญญาณใดแปลกปลอมเข้ามาในระบบหรือไม่ถ้าเจอก็อาจจะทำการแจ้งเตือนต่อผู้ดูแลระบบหรือทำการปิดระบบที่มีปัญหาลงไป

7. พยายามสุ่มหา Password ด้วยเทคนิค Brute force และ Dictionary Attack

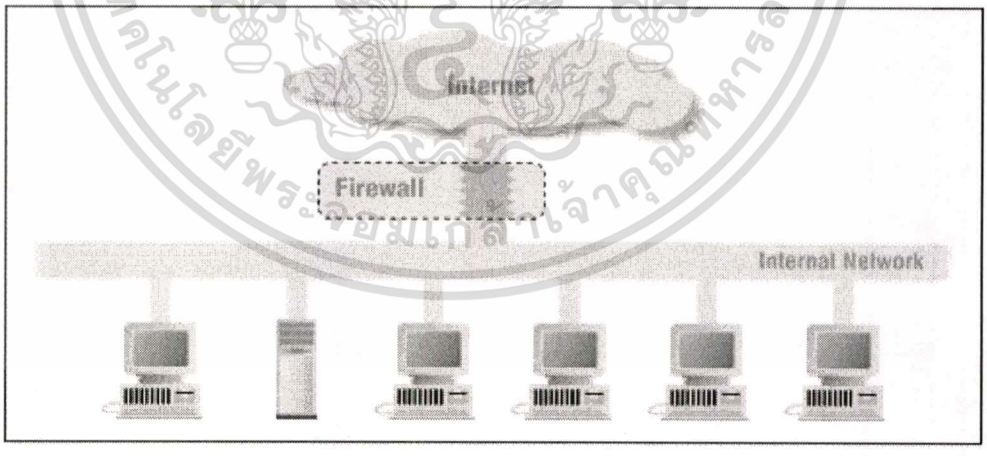
เนื่องจากการเข้าใช้ระบบหากมีการทำการตรวจสอบการเข้าใช้โดยการทำ Authenticate ซึ่งแน่นอนว่าเมื่ออุปกรณ์ใดๆที่มีการทำAuthenticate นั้นก็จะหนีไม่พ้นที่จะโดนโจมตีที่เรื่องว่า Brute force Attack หรือ Dictionary Attack เพื่อทำการสุ่มหา user และ password ที่ใช้เข้าระบบ สิ่งที่เข้ามาช่วยในเรื่องนี้ก็จะเป็นระบบsoftware ที่ใช้ในการAuthentication ด้วยเทคนิคต่างๆ เช่น RADIUS ซึ่งจะช่วยเพิ่มความปลอดภัยในเรื่องของการตรวจสอบสิทธิการเข้าใช้ ,นโยบายการเข้าใช้ระบบและบันทึกพฤติกรรมการเข้าใช้ระบบ

8. Man In the Middle Attack

การโจมตีรูปแบบนี้ผู้โจมตีจะทำเรียนรู้ลำดับขั้นตอน และรายละเอียดค่าต่างๆในการสื่อสารระหว่างคู่สื่อสารหนึ่งๆ หลังจากที่ได้เรียนรู้ค่าต่างแล้วก็เริ่มทำการหลอกล่อให้ Session ในการสื่อสารของทั้งฝั่งที่ทำการส่งนั้นทำการสื่อสารกับผู้โจมตีก่อนแทนที่จะสื่อสารกันเองโดยตรงซึ่งอาจใช้วิธีการเปลี่ยนหมายเลข IP Address ในส่วนของ Source และ Destination โดยใช้จุดอ่อนของ WEP คีย์ดังที่ได้กล่าวมา จากนั้นผู้โจมตีค่อยทำการส่งข้อมูลนั้นๆ ต่อไปให้กับฝั่งรับอีกทีหนึ่งซึ่งทำให้คู่สื่อสารนั้นติดต่อกันได้ปกติ แต่ที่จริงแล้วเป็นการติดต่อผ่านตัวกลางอีกทีหนึ่งซึ่งเปิดโอกาสให้ผู้โจมตีสามารถดักจับข้อมูลการสื่อสารนั้นๆได้ หรืออาจขยายผลโดยทำการขโมย Session นั้นไปเลยซึ่งทำให้ผู้บุกรุกสามารถติดต่อสื่อสารกับฝั่งใดฝั่งหนึ่งของคู่สื่อสารนั้นๆได้เลย

2.2 ไฟร์วอลล์

ไฟร์วอลล์เป็นคอมโพเน็นต์หรือกลุ่มของคอมโพเน็นต์ที่ทำหน้าที่ในการควบคุมการเข้าถึงระหว่างเน็ตเวิร์กภายนอกหรือเน็ตเวิร์กที่เราคิดว่าไม่ปลอดภัย กับเน็ตเวิร์กภายในหรือเน็ตเวิร์กที่เราต้องการจะป้องกัน โดยที่คอมโพเน็นต์นั้นอาจจะเป็นเราเตอร์ คอมพิวเตอร์ หรือเน็ตเวิร์ก ประกอบกันก็ได้ ขึ้นอยู่กับวิธีการหรือ Firewall Architecture ที่ใช้



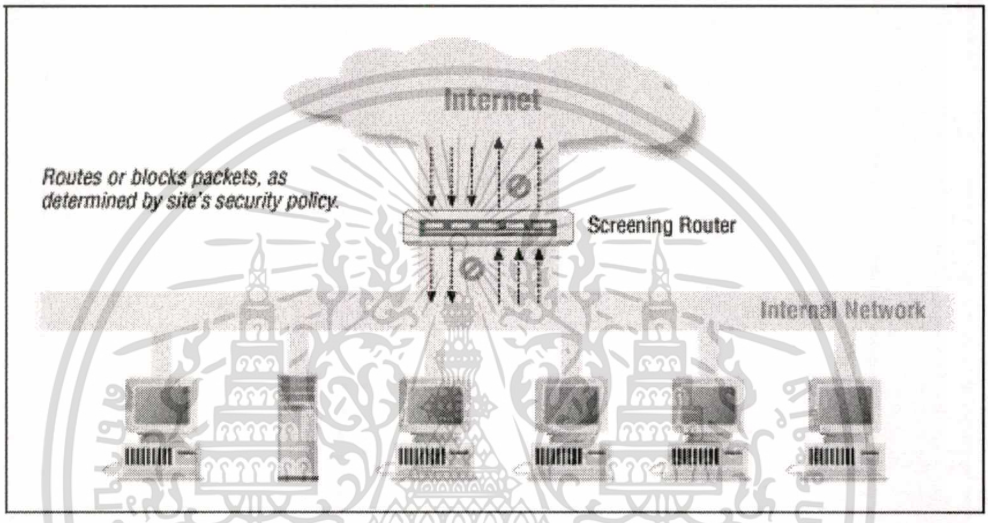
รูปที่ 2.4 ไฟร์วอลล์กั้นระหว่างอินเตอร์เน็ตกับเน็ตเวิร์กภายใน

การควบคุมการเข้าถึงของไฟร์วอลล์นั้น สามารถทำได้ในหลายระดับและหลายรูปแบบขึ้นอยู่ชนิดหรือเทคโนโลยีของไฟร์วอลล์ที่นำมาใช้ เช่น เราสามารถกำหนดได้ว่าจะให้มีการเข้ามาใช้เซอร์วิสอะไรได้บ้าง จากที่ไหน เป็นต้น

2.2.1 ชนิดของไฟร์วอลล์

1. Packet Filtering

Packet Filter คือเราเตอร์ที่ทำการหาเส้นทางและส่งต่อ (route) อย่างมีเงื่อนไข โดยจะพิจารณาจากข้อมูลส่วนที่อยู่ในเฮดเดอร์ (header) ของแพ็กเก็ตที่ผ่านเข้ามา เทียบกับกฎ (rules) ที่กำหนดไว้และตัดสินว่าควรจะทิ้ง (drop) แพ็กเก็ตนั้นไปหรือว่าจะยอม (accept) ให้แพ็กเก็ตนั้นผ่านไปได้



รูปที่ 2.5 ใช้ Screening Router ทำหน้าที่ Packet Filtering

ในการพิจารณาเฮดเดอร์ Packet Filter จะตรวจสอบในระดับของอินเตอร์เน็ตเลเยอร์ (Internet Layer) และทรานสปอร์ตเลเยอร์ (TransportLayer) ในอินเตอร์เน็ตโมเดลซึ่งในอินเตอร์เน็ตเลเยอร์จะมีแอตทริบิวต์ที่สำคัญต่อ Packet Filtering ดังนี้

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

และในระดับของทรานสปอร์ตเลเยอร์ มีแอตทริบิวต์ที่สำคัญคือ

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

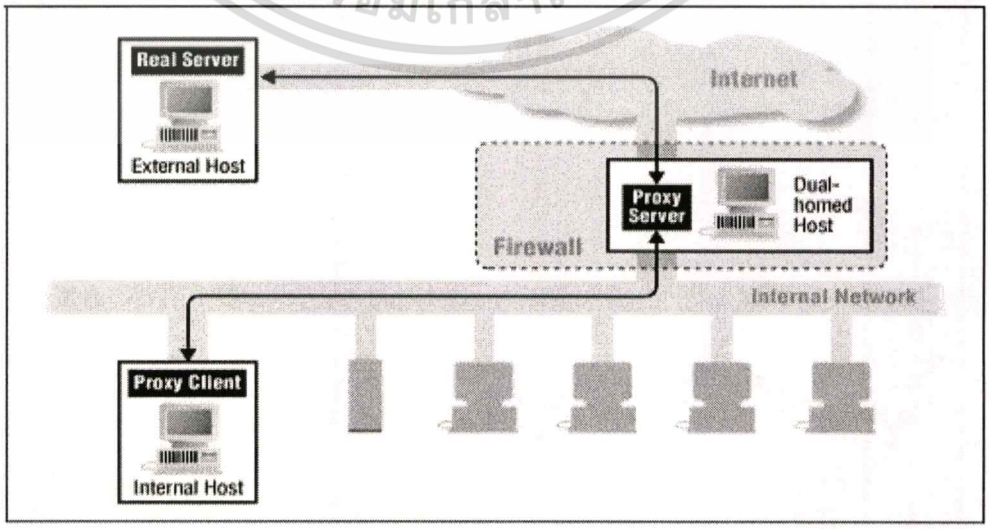
ซึ่งพอร์ตของทรานสปอร์ตเลเยอร์ คือทั้ง TCP และ UDP นั้นจะเป็นสิ่งที่บอกถึงแอพพลิเคชันที่แพ็กเก็ตนั้นต้องการติดต่อด้วยเช่น พอร์ต 80 หมายถึง HTTP, พอร์ต 21 หมายถึง FTP เป็นต้น ดังนั้นเมื่อ Packet Filter พิจารณาเฮดเดอร์ จึงทำให้สามารถควบคุมแพ็กเก็ตที่มาจากที่ต่างๆ และมีลักษณะต่างๆ (ดูได้จากแฟล็กของแพ็กเก็ต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

Packet Filtering สามารถอิมพลีเมนต์ได้จาก 2 แพล็ตฟอร์ม คือ

- เราเตอร์ที่มีความสามารถในการทำ Packet Filtering
- คอมพิวเตอร์ที่ทำหน้าที่เป็นเราเตอร์

2. Proxy

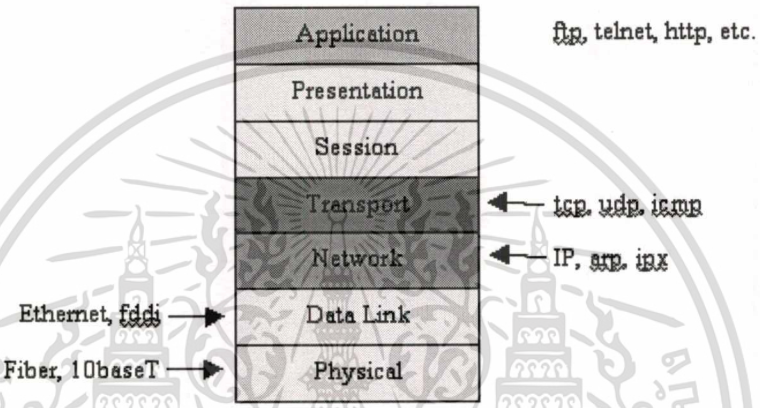
Proxy หรือ Application Gateway เป็นแอพพลิเคชันโปรแกรมที่ทำงานอยู่บนไฟร์วอลล์ที่ตั้งอยู่ระหว่างเน็ตเวิร์ก 2 เน็ตเวิร์ก ทำหน้าที่เพิ่มความปลอดภัยของระบบเน็ตเวิร์กโดยการควบคุมการเชื่อมต่อระหว่างเน็ตเวิร์กภายในและภายนอก Proxy จะช่วยเพิ่มความปลอดภัยได้มาก เนื่องจากมีการตรวจสอบข้อมูลถึงในระดับของแอพพลิเคชันเลเยอร์ เมื่อไคลเอนต์ต้องการใช้เซอร์วิสภายนอก 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 2.6 ใช้ Dual-homed Host เป็น Proxy Server

3. Stateful Inspection Technology

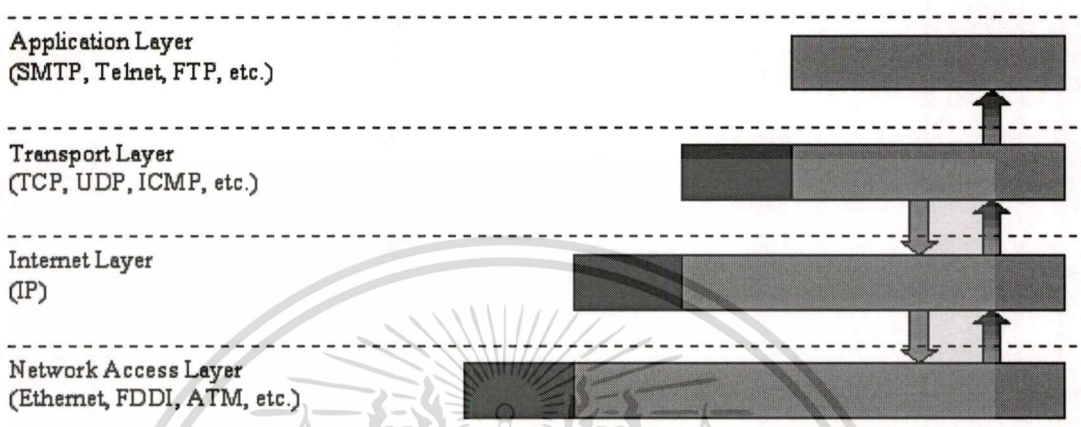
การที่จะทำความเข้าใจหลักการทำงานของ stateful firewall ให้ได้ดีนั้น จำเป็นต้องมีความรู้พื้นฐานเกี่ยวกับ 7-layers OSI model ซึ่งแสดงให้เห็นดังภาพที่ 2.7



รูปที่ 2.7 OSI 7 Layers

ทั้งนี้เราจะพิจารณาเฉพาะ layer ที่ 3,4 และ 7 ซึ่งเกี่ยวข้องกับ TCP/IP เท่านั้น สิ่งที่สำคัญพอๆ กับ OSI model ก็คือการทำความเข้าใจภาพรวมของโครงสร้างของข้อมูลดังที่เห็นในภาพ ในชั้น application layer นั้น ชุดของข้อมูลมีแค่ส่วนของข้อมูลที่ต้องการส่งเท่านั้น แต่ใน layer ชั้นถัดๆ ลงไป ชุดของข้อมูลจะประกอบไปด้วยส่วนของ header และ body โดยส่วนของ header เป็นส่วนที่เกี่ยวข้องกับ layer ชั้นนั้นๆ ในขณะที่ส่วนของ body เป็นส่วนของ body + header ของ layer ชั้นที่อยู่ด้านบน ลักษณะของการกระทำกับข้อมูลดังกล่าวเรียกว่า encapsulation และในชั้นของ transport layer ตัว IP protocol ที่ผู้ใช้เรียกใช้ ซึ่งอาจจะเป็น TCP, UDP, ICMP ก็จะปะส่วน header ของมันรวมไปกับข้อมูล และส่งต่อ segmentใหม่นี้ไปยัง layer ที่อยู่ด้านล่างถัดไป และที่ชั้น IP layer ข้อมูลทุกอย่างที่มาจาก transport layer จะถูกมองว่าเป็นข้อมูล มันจะแปะส่วน header รวมกับข้อมูลนั้น เพื่อส่งผ่าน packetไปยัง layer ที่อยู่ด้านล่างถัดไป เมื่อข้อมูลมาถึงชั้น data link layer มันจะแปะส่วน header รวมกับข้อมูลนั้น และในที่สุดข้อมูลก็จะถูกส่งออกไป เมื่อได้รับ packet กระบวนการทำงานย้อนกลับก็เริ่มขึ้น โดยข้อมูลจะถูกส่งไปยัง data link layer เพื่อเก็บข้อมูลที่มันต้องการจาก header จากนั้นก็จะลบส่วนของ header ออก พร้อม

ทั้งส่งข้อมูลไปยัง IP layer ตัว IP layer เองก็จะอ่านข้อมูลจาก header ลบ header ออก และส่งผ่านข้อมูลไปยัง transport layer และเป็นเช่นนี้จนกระทั่งข้อมูลถูกส่งไปยังชั้นที่ต้องการในที่สุด



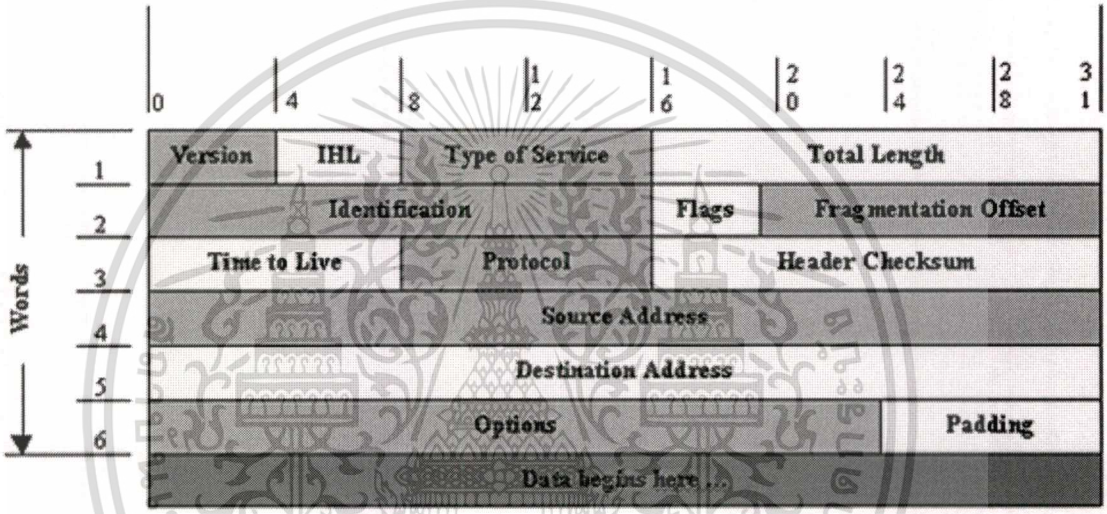
รูปที่ 2.8 การ Encapsulate ของ packet

กระบวนการที่กล่าวไปแล้วนั้นเป็นสิ่งที่สำคัญสำหรับ simple packet filter, application proxy และ stateful packet-filtering technology ทั้งสามตัวนี้จะต้องเข้าถึงข้อมูลในส่วนของ header ในแต่ละ layer ซึ่งบรรจุข้อมูลที่แตกต่างกันไป โดยข้อมูลเหล่านี้จะถูกใช้เพื่อพิจารณาว่ามันเป็นข้อมูลที่อนุญาตให้ผ่านไปหรือไม่ชั้น IP layer นั้นเป็นชั้นที่ทั้ง simple packet filter และ stateful filter ใช้เป็นจุดเริ่มต้นในการพิจารณาข้อมูล ซึ่งจุดนี้ที่ผู้ผลิต packet-filtering firewall ใช้เป็นข้อโต้แย้งว่า application proxy ไม่สามารถมองเห็นข้อมูลในชั้น network และ transport layer (ตามมาตรฐานของ OSI stack) ได้ ในปัจจุบัน simple packet filter บางตัวเช่น border router สามารถทำ access filtering ได้ที่ชั้น IP layer นี้ นอกจากนี้ router ส่วนใหญ่ยังสามารถทำงานที่ชั้น transport layer ได้อีกด้วย สิ่งที่ simple packet filter และ stateful firewall ทำเหมือนกันก็คือ ตรวจสอบข้อมูล header ของ IP packet โดยสิ่งที่ถูกตรวจสอบคือ

- source address
- destination address
- protocol
- options

นโยบายของไฟร์วอลล์ส่วนใหญ่มักจะตรวจสอบความถูกต้องของ address (ทั้ง source address และ destination address) ด้วย ยกเว้นกรณีที่ระบุเป็น "all" และข้อมูลในส่วนของ protocol นั้นก็จะเป็นตัว

บอกว่า ส่วนของ data นั้นบรรจุข้อมูลชนิดใดอยู่ เช่น TCP, UDP, ICMP หรือบางทีอาจจะเป็น IPSEC, ESP, ISAKMP กระบวนการในการตรวจสอบรูปแบบของ header นั้นจะอยู่ที่ layer ชั้นบนถัดไป และข้อมูลในส่วน options นั้น โดยปกติมักจะไม่มีค่าอะไร แต่อาจจะมี flag ที่แสดงถึง source routing ได้ (source routing ใช้ในกรณีที่ผู้ส่งต้องการให้ผู้รับส่งข้อมูลผ่านเส้นทางที่ผู้ส่งได้กำหนดไว้) โดยปกติแล้วมักจะถูกใช้โดยผู้บุกรุก ดังนั้น packet filter ส่วนใหญ่จะ drop packet ที่ถูกส่งมาพร้อมกับ flag ดังกล่าว โดยไม่มีการตรวจสอบข้อมูลอย่างอื่นเพิ่มเติม



รูปที่ 2.9 TCP Header

TCP header บรรจุข้อมูล 3 ส่วนที่สำคัญใน transport layer ไว้คือ source port , destination port และ flags โดยในส่วนของ flag นั้น สามารถประกอบไปด้วย URG(urgent), ACK(acknowledgment), PSH(push), RST(reset), SYN(syncronize) และ FIN(finish) และยังมีส่วนที่สี่ที่บรรจุ sequence number ซึ่งผู้ผลิตบางค่ายนำมาใช้พิจารณาด้วยสำหรับ flag นั้นเป็นส่วนที่สำคัญมากใน stateful firewall เช่น การทำ TCP 3-way handshake ส่วน UDP header บรรจุข้อมูลเพียงแค่ source port และ destination port เท่านั้นเอง ไม่มีส่วนของ flag และ sequence number แต่อย่างใด เนื่องจาก UDP เป็น connectionless protocol อยู่แล้วนั่นเอง และใน ICMP header นั้น ไม่ได้บรรจุข้อมูล port แต่อย่างใด แต่บรรจุชนิดของ ICMP (ICMP message type) เช่น "Echo request" , "Destination unreachable"

Simple packet filter จะพิจารณา TCP packet เพื่อตรวจสอบว่า

- packet นั้น มี address ที่ถูกต้องหรือไม่
- packet นั้น ถูกสร้างมาจาก external address จริงหรือไม่

- protocol หรือ service นั้น ผ่านการตรวจสอบแล้วหรือไม่
- option หรือ flag ที่ส่งมานั้น ถูกต้องตามข้อกำหนดหรือไม่

โดยทั่วไป border router มักจะทำหน้าที่ตรวจสอบระหว่างภายในและภายนอกเครือข่าย เพราะมันเป็นอุปกรณ์ที่สามารถบอกได้ว่า packet ถูกสร้างมาจากภายในหรือภายนอก และถ้า packet ถูกส่งมาจากภายนอกแต่มี address เป็นภายใน ก็แสดงว่า packet นั้นถูก spoof address มา และ packet นั้นควรที่จะถูก drop ทิ้งไป และนอกจากนี้ simple packet filter ยังไม่มีข้อมูลที่แสดงถึงการเชื่อมต่อที่เปิดขึ้นก่อนหน้านี้หรือในขณะนี้แต่อย่างใด ดังนั้นสมมติว่ามันได้รับ ACK packet มันก็จะพิจารณาว่า packet นี้เป็นส่วนหนึ่งของ connection ที่เกิดขึ้นแล้ว และส่วนใหญ่ก็จะส่งต่อ packet ต่อไป จุดนี้ไม่ใช่ปัญหาของ established connection แต่มันเป็นปัญหาในกรณีที่การส่ง ACK packet ดังกล่าวถูกส่งมาโดยเจตนาร้าย เพราะเมื่อเครื่องปลายทางได้รับ ACK มันมักจะส่งสัญญาณ RST กลับไป ซึ่งจะแสดงให้เห็นว่าเครื่องปลายทางนั้นยังเปิดอยู่ และเปิดให้บริการใน port ดังกล่าว บางครั้งยังสามารถใช้ตรวจสอบระบบปฏิบัติการของเครื่องปลายทางได้อีกด้วยเพราะระบบปฏิบัติการในแต่ละระบบนั้นมักจะมีวิธี response ที่แตกต่างกันออกไป

สำหรับ packet-filtering firewall (stateful) แล้วมันก็ทำเช่นเดียวกันกับ simple packet filter แต่มันจะบันทึกข้อมูลเกี่ยวกับ connection ที่เกิดขึ้นลงใน state table ก่อนที่จะส่ง packet นั้นไปยัง IP stack ตัว table นี้จะมีส่วนสำหรับบันทึกข้อมูลสำหรับแต่ละ connection ที่ถูกต้อง โดยปกติจะเก็บข้อมูล source and destination address, protocol, port, flag แต่มีไฟร์วอลล์บางยี่ห้อที่เก็บข้อมูล sequence number เพิ่มด้วย เพื่อใช้ในการตรวจสอบ packet ที่กำลังจะเข้ามาและป้องกันการทำ session hijacking เมื่อ packet-filtering firewall ได้รับ packet มันจะตรวจสอบข้อมูลกับ state table ว่าเป็นส่วนของ connection ที่สร้างไว้แล้วหรือไม่ โดยจะพิจารณาจากข้อมูล source adderss, destination address, source port, destnation port จะต้องสอดคล้องกับ state table ซึ่งถ้าเป็นส่วนหนึ่งของ connection จริงก็ไม่มีความจำเป็นใดๆ ที่ต้องตรวจสอบซ้ำอีก แต่ในไฟร์วอลล์บางยี่ห้อนั้นจะพิจารณา sequence number ของ packet เพิ่มเติมด้วย ดังนั้น stateful firewall สามารถ drop/return packet ที่ผิดปกติได้ และถ้า packet ที่ส่งมาเป็นส่วนหนึ่งของ connection ที่สร้างไว้แล้ว มันก็จะส่งผ่านเลย ซึ่งทำให้ประหยัด cost มากกว่าการตรวจสอบ firewall ruleset ใหม่อีกรอบ ดังนั้นจึงทำให้ packet-filtering firewall ทำงานได้เร็วมาก ถ้า packet ที่ส่งมาไม่ตรงกับ connection ที่สร้างไว้แล้ว และไม่ใช่ SYN packet ตัว packet นั้นๆ ก็จะถูก drop ทิ้งไป และแม้แต่ packet ที่ผสม flag แปลกๆ เช่น SYN/FIN ก็จะถูก drop ทิ้งไปเช่นเดียวกัน ทั้งนี้ไฟร์วอลล์ส่วนใหญ่สามารถบันทึกล็อกได้ด้วย ซึ่งขึ้นอยู่กับการตั้งค่าของผู้ดูแลระบบเองว่าต้องการเก็บข้อมูลใด ในกรณีที่ packet-filtering firewall ได้รับ UDP packet เนื่องจากไม่มี

กระบวนการ 3-way handshake เพราะมันเป็น stateless protocol ไม่มี sequence number แต่มันก็ยังมี source port และ destination port ซึ่งจะถูกสร้างขึ้นใน state table ซึ่งรวมเอา source address , destination address มาไว้ด้วยกัน ทั้งนี้ เนื่องจาก UDP ไม่มี FIN หรือ RST ซึ่งใช้สำหรับยกเลิกการเชื่อมต่อเหมือนกับ TCP ดังนั้นมันจึงต้องมี timeout เพื่อลบข้อมูลออกจาก state tableอย่างไรก็ตาม จำเป็นต้องมีวิธีในการลบข้อมูลออกจาก state table โดยเฉพาะสำหรับ TCP connection ซึ่งอาจจะถูกโจมตีโดยการส่ง SYN packetจำนวนมากเข้ามายังไฟร์วอลล์ ซึ่งก่อให้เกิด Denial of Service ได้ เพราะมันทำให้ state table เต็ม ปัญหานี้สามารถแก้ไขได้โดยการตั้ง timeout ของ แต่ละ connection ไว้

สำหรับ application proxy จะทำการตรวจสอบข้อมูลในชั้น network layer และ transport layer และยังสามารถตรวจสอบความถูกต้องในชั้น application layer ได้อีกด้วย ซึ่งทำให้ application proxy สามารถกลั่นกรอง commands, protocol, packet length, authorization, content, invalid header หรือสามารถส่งผ่าน packet ไปได้เลย application proxy เป็น stateful firewall แต่สิ่งที่สร้างความแตกต่างคือ proxy server จะสร้าง IP packet ใหม่ เพื่อส่งต่อไปยังเป้าหมาย ทั้งนี้เพื่อป้องกัน malformed packet และ proxy จะสร้าง packet ใหม่เพื่อส่งต่อก็ต่อเมื่อ packet นั้นผ่านการตรวจสอบแล้ว

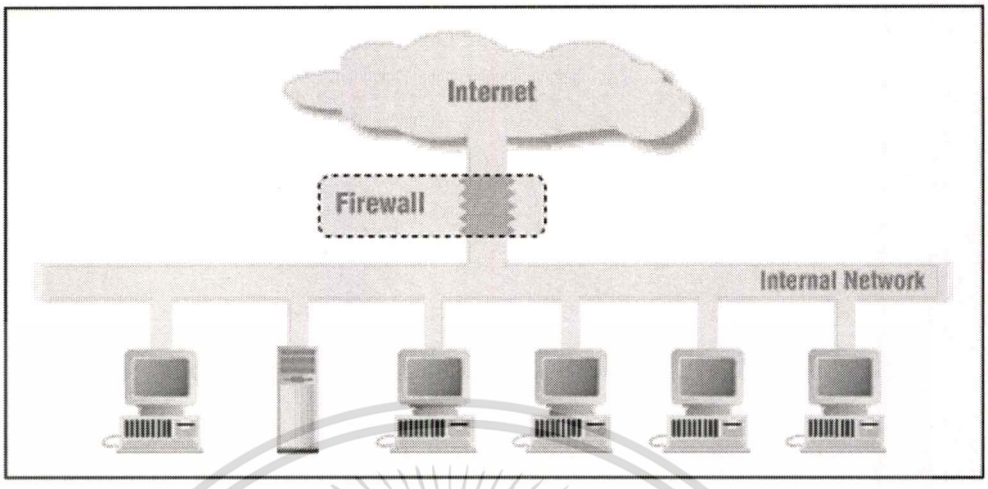
ในกรณีของ simple packet filter จำเป็นต้องระบุ rule ทั้ง incoming packet และ ทั้ง outgoing packet ในขณะที่ stateful firewall สามารถระบุได้แค่ข้างเดียวเท่านั้นเอง เพราะ packet ที่ return กลับมานั้น จะถือว่าเป็นส่วนหนึ่งของ connection ที่สร้างไว้ก่อนแล้ว

2.2.2 Firewall Architecture

ในส่วนของ Firewall Architecture นั้น จะพูดถึงการจัดวางไฟร์วอลล์คอมโพเน็นต์ในแบบต่างๆ เพื่อทำให้เกิดเป็นระบบไฟร์วอลล์ขึ้น

1. Single Box Architecture

Single Box Architecture เป็น Architecture แบบง่ายๆ ที่มีคอมโพเน็นต์ทำหน้าที่เป็นไฟร์วอลล์เพียงอันเดียวตั้งอยู่ระหว่างเน็ตเวิร์กภายในกับเน็ตเวิร์กภายนอก ข้อดีของวิธีนี้ก็คือการที่มีเพียงจุดเดียวที่หน้าที่ไฟร์วอลล์ทั้งหมด ควบคุมการเข้าออกของข้อมูล ทำให้ดูแลได้ง่าย เป็นจุดสนใจในการดูแลความปลอดภัยเน็ตเวิร์ก ในทางกลับกันข้อเสียของวิธีนี้ก็คือ การที่มีเพียงจุดเดียวนี้ ทำให้มีความเสี่ยงสูง หากมีการคอนฟิกูเรชันผิดพลาดหรือมีช่องโหว่เพียงเล็กน้อย การผิดพลาดเพียงจุดเดียวอาจทำให้ระบบถูกเจาะได้



รูปที่ 2.10 Firewall Architecture แบบชั้นเดียว

คอมโพเน็นต์ที่ใช้ใน Architecture นี้อาจเป็น Screening Router , Dual-Homed Host หรือ Multi-purposed Firewall Box ก็ได้

1) Screening Router

สามารถใช้เราเตอร์ทำ Packet Filtering ได้ วิธีนี้จะทำให้ประหยัดค่าใช้จ่ายเนื่องจากส่วนใหญ่จะใช้เราเตอร์ต่อกับเน็ตเวิร์กภายนอกอยู่แล้ว แต่วิธีนี้อาจไม่ยืดหยุ่นมากนักในการคอนฟิกกูเรชัน Architecture แบบนี้เหมาะสำหรับ

- เน็ตเวิร์กที่มีการป้องกันความปลอดภัยในระดับของโฮสต์ (Host security) เป็นอย่างดีแล้ว
- มีการใช้โปรโตคอลไม่มาก และโปรโตคอลที่ใช้ก็เป็นโปรโตคอลที่ไม่ซับซ้อน
- ต้องการไฟร์วอลล์ที่มีความเร็วสูง

2) Dual-Homed Host

สามารถใช้ Dual-Homed Host ใช้การบริการเป็น Proxy ให้กับเครื่องภายในเน็ตเวิร์ก Architecture แบบนี้เหมาะสำหรับ

- เน็ตเวิร์กที่มีการใช้งานอินเตอร์เน็ตค่อนข้างน้อย
- เน็ตเวิร์กที่ไม่ได้มีข้อมูลสำคัญๆ

3) Multi-purposed Firewall Box

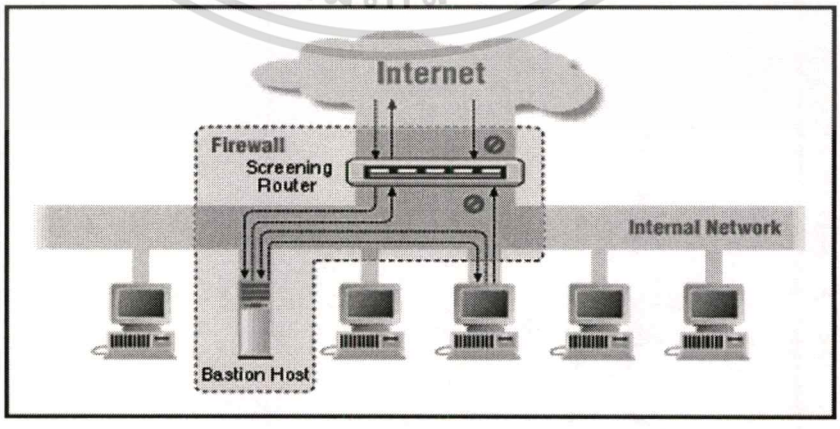
มีผลิตภัณฑ์หลายชนิดที่ผลิตออกมาเป็นกล่องๆ เดียว ซึ่งทำหน้าที่ได้หลายอย่าง ทั้ง Packet Filtering, Proxy แต่ก็อย่าลืมว่านี่คือ Architecture แบบชั้นเดียว ซึ่งถ้าพลาดแล้วก็จะเสียหายทั้งเน็ตเวิร์กได้

2. Screened Host Architecture

Screened Host Architecture จะมีโฮสต์ซึ่งให้บริการ Proxy เหมือนกับใน Single Box Architecture ที่เป็น Dual-homed Host แต่จะต่างกันตรงที่ว่า โฮสต์นั้นจะอยู่ภายในเน็ตเวิร์ก ไม่ต่ออยู่กับเน็ตเวิร์กภายนอกอื่นๆ (ดังนั้นก็ไม่จำเป็นที่จะต้องใช้ Dual Homed Host) และจะมี เราเตอร์ที่ทำหน้าที่ Packet Filtering ช่วยบังคับให้เครื่องภายในเน็ตเวิร์กต้องติดต่อเซอร์วิสผ่าน Proxy โดยไม่ยอมให้ติดต่อใช้เซอร์วิสจากภายนอกโดยตรง และก็ให้ภายนอกเข้าถึงได้เฉพาะ Bastion host (คือโฮสต์ที่มีความเสี่ยงสูงต่อการถูกโจมตี มักจะเป็นโฮสต์ที่เปิดให้บริการกับอินเตอร์เน็ต ดังนั้นโฮสต์นี้ต้องมีการดูแลเป็นพิเศษ) เท่านั้น จากรูปที่ 2.11 ใน Architecture แบบนี้จะประกอบไปด้วยเราเตอร์ทำหน้าที่ Packet Filtering และภายในเน็ตเวิร์กจะมี Bastion Host ให้บริการ Proxy อยู่ โดยที่เราเตอร์นั้นอาจจะถูกเซ็ตดังนี้

- อาจจะอนุญาตให้เครื่องภายในใช้เซอร์วิสบางอย่างได้โดยตรง
- ส่วนเซอร์วิสอื่นๆ จะไม่ยอมให้เครื่องภายในติดต่อผ่านออกไปโดยตรง ยกเว้น Bastion Host เท่านั้นที่สามารถติดต่อกับเน็ตเวิร์กภายนอกได้ทั้งนี้เพื่อเป็นการบังคับให้ใช้บริการ Proxy ผ่านทาง Bastion Host เท่านั้น

หรืออาจจะเซ็ตให้เซอร์วิสส่วนใหญ่ผ่านเราเตอร์ออกไปได้โดยตรงแล้ว ให้บางส่วนต้องใช้เซอร์วิสผ่าน Proxy ก็แล้วแต่นโยบายและความเหมาะสมขององค์กร



รูปที่ 2.11 Screened Host Architecture

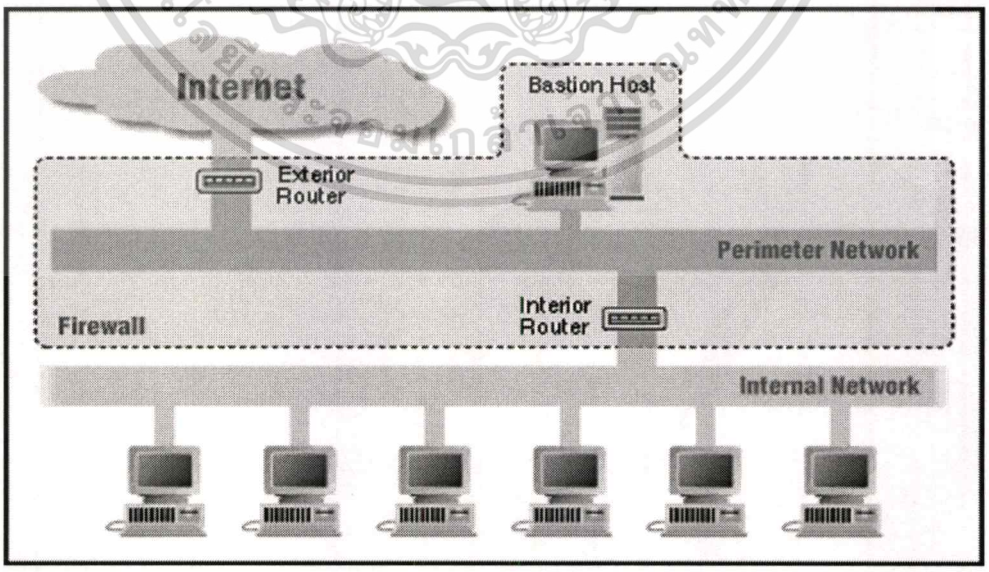
วิธีนี้ถึงแม้ว่าจะมีทั้ง Proxy และเราเตอร์ทำหน้าที่ Packet Filtering แต่ก็ยังคงอันตรายอยู่ เพราะว่าเราเตอร์ต้องยอมให้ภายนอกสามารถติดต่อกับ Bastion Host ได้อยู่แล้ว หากแฮกเกอร์สามารถเจาะเข้ามายัง Bastion Host ได้ก็เสร็จ

Architecture นี้เหมาะสำหรับ

- เน็ตเวิร์กที่มีการติดต่อกับเน็ตเวิร์กภายนอกน้อย
- เน็ตเวิร์กที่มีการป้องกันความปลอดภัยในระดับของโฮสต์เป็นอย่างดีแล้ว

3. Multi Layer Architecture

ในสถาปัตยกรรมแบบหลายชั้น ไฟร์วอลล์จะเกิดขึ้นจากคอมโพเน็นต์หลายๆส่วนทำหน้าที่ประกอบกันขึ้นเป็นระบบ วิธีการนี้สามารถเพิ่มความปลอดภัยได้มาก เนื่องจากเป็นการลดความเสี่ยงต่อความผิดพลาดที่อาจเกิดขึ้น ถ้าหากมีไฟร์วอลล์เพียงจุดเดียวแล้วมีเกิดความผิดพลาดเกิดขึ้น ระบบทั้งหมดก็จะเป็นอันตราย แต่ถ้ามีการป้องกันหลายชั้น หากในชั้นแรกถูกเจาะ ก็อาจจะมีความเสียหายเพียงบางส่วน ส่วนที่เหลือระบบก็ยังคงมีชั้นอื่นๆ ในการป้องกันอันตราย และยังลดความเสี่ยงได้โดยการที่แต่ละชั้นนั้นมีการใช้เทคโนโลยีที่แตกต่างกัน เพื่อให้เกิดความหลากหลาย เป็นการหลีกเลี่ยงการโจมตีหรือช่องโหว่ที่อาจมีในเทคโนโลยีชนิดใดชนิดหนึ่ง โดยทั่วไปแล้วสถาปัตยกรรมแบบหลายชั้นจะเป็นการต่อกันเป็นซีรี่โดยมี Perimeter Network (หรือบางทีเรียกว่า DMZ Network) อยู่ตรงกลาง เรียกว่า Screened Subnet Architecture



รูปที่ 2.12 Screened Subnet Architecture

Screened Subnet Architecture

Screened Subnet Architecture เป็นสถาปัตยกรรมที่มีการเพิ่ม Perimeter Network เข้าไปกั้นระหว่างอินเตอร์เน็ตกับเน็ตเวิร์กภายในไม่ให้เชื่อมต่อกันโดยตรง ทำให้เน็ตเวิร์กภายในมีความปลอดภัยมากขึ้น

ในรูปที่ 2.12 แสดง Screened Subnet Architecture อย่างง่าย ประกอบไปด้วย เราเตอร์ 2 ตัว ตัวนึงอยู่ระหว่างอินเตอร์เน็ตกับ Perimeter Network ส่วนอีกตัวหนึ่งอยู่ระหว่าง Perimeter Network กับเน็ตเวิร์กภายใน ถ้าหากแฮกเกอร์จะเจาะเน็ตเวิร์กภายในต้องผ่านเราเตอร์เข้ามาถึง 2 ตัวด้วยกัน ถึงแม้ว่าจะเจาะชั้นแรกเข้ามายัง Bastion host ได้ แต่ก็ยังต้องผ่านเราเตอร์ตัวในอีก ถึงจะเข้ามายังเน็ตเวิร์กภายในได้ คอมโพเน็นต์ของ Screened Subnet Architecture ในรูปที่ 2.12

- Perimeter Network เป็นเน็ตเวิร์กที่เพิ่มเข้ามาเพื่อความปลอดภัย อยู่ระหว่างเน็ตเวิร์กภายนอกกับเน็ตเวิร์กภายใน ประโยชน์ของ Perimeter Network ที่เห็นได้ชัดก็คือ การแบ่งเน็ตเวิร์กออกเป็นส่วนๆ ทำให้การไหลของข้อมูลถูกแบ่งออกเป็นส่วนๆตามเน็ตเวิร์กด้วย เนื่องจากโดยทั่วไปแล้ว เน็ตเวิร์กที่เป็นแลนนั้น จะเป็นแบบ Ethernet ซึ่งจะมีการส่งข้อมูลแบบ Broadcast ดังนั้นถ้ามีใครคอยดักจับข้อมูลอยู่ในเน็ตเวิร์กนั้น ก็จะได้พาสเวิร์ด ข้อมูลต่างๆ ไปหมด ดังนั้นหากไฟร์วอลล์เรามีชั้นเดียวและแฮกเกอร์สามารถเข้ามาได้ โดนดักจับข้อมูลก็เสร็จหมด แต่ถ้าเรามี Perimeter Network ถึงจะดักจับข้อมูลได้แต่ก็จะได้เพียงที่อยู่บน Perimeter Network เท่านั้น
- Bastion Host ตั้งอยู่บน Perimeter Network ทำหน้าที่ให้บริการ Proxy กับเน็ตเวิร์กภายใน และให้บริการต่างๆ กับผู้ใช้บนอินเตอร์เน็ต Bastion Host นั้นจะมีความเสี่ยงต่อการโจมตีสูง จึงต้องมีการดูแลความปลอดภัยเป็นพิเศษ
- Interior Router ตั้งอยู่ระหว่าง Perimeter Network กับเน็ตเวิร์กภายใน ทำหน้าที่ Packet Filtering ป้องกันเน็ตเวิร์กภายในจาก Perimeter Network ในการเซ็ต configuration ระหว่าง เน็ตเวิร์กภายในกับ Perimeter Network ควรกำหนดอย่างรอบคอบ อนุญาตเฉพาะเซอร์วิสที่จำเป็นเท่านั้นอย่างเช่น DNS, SMTP
- Exterior Router ตั้งอยู่ระหว่างเน็ตเวิร์กภายนอกกับ Perimeter Network เนื่องจาก Exterior Router นี้เป็นจุดที่ต่ออยู่กับเน็ตเวิร์กภายนอก จึงมีหน้าที่ที่สำคัญอย่างหนึ่งคือ การป้องกันแพ็กเก็ตที่มีการ Forged IP Address เข้ามา โดยอ้างว่ามาจากเน็ตเวิร์กภายในทั้งๆ ที่จริงๆ แล้วมาจากเน็ตเวิร์กภายนอก

บทที่ 3

การวิเคราะห์และการออกแบบระบบ

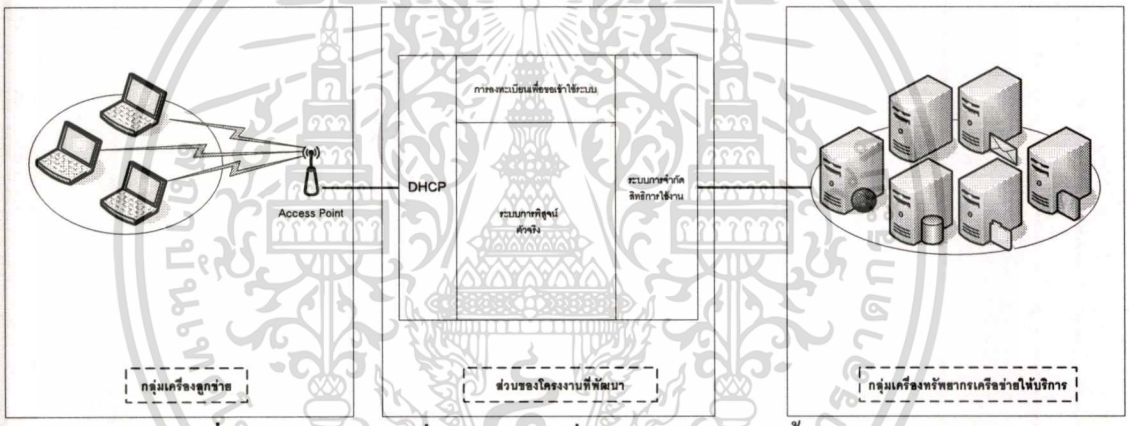
ปัญหาการรักษาความปลอดภัยดังที่กล่าวมาในบทที่สองนั้นพอจะสรุปสาเหตุของปัญหาว่าน่าจะแบ่งได้เป็นประเด็นใหญ่ๆ คือ

1. ปัญหาการขาดความรู้ความระวังในการใช้งานระบบเช่นการประมาทเลินเล่อรูปเท่าไม่ถึงการณ์ ในส่วนนี้ควรแก้ไขในเชิงของการให้ความรู้เกี่ยวกับการใช้งานระบบเพื่อให้ผู้ใช้ตระหนักถึงอันตรายที่สามารถเกิดขึ้นได้กับระบบ ประกอบกับการออกนโยบายเชิงควบคุมพฤติกรรมการใช้งานของผู้ใช้งาน
2. ปัญหาที่เกิดจากการจงใจเพื่อที่จะทำลายหรือพยายามเข้ามาใช้ทรัพยากรเครือข่ายโดยไม่ได้รับอนุญาต โดยอาศัยช่องโห่วของเทคโนโลยี ซึ่งการแก้ปัญหาในกลุ่มนี้สามารถแก้ไขได้ในเชิงของเทคนิคซึ่งพอจะสรุปได้ดังนี้
   a. ปัญหาการเข้ารหัสข้อมูลสามารถแก้ไขได้โดยการใช้เทคโนโลยีของ VPN เข้ามาช่วย
   b. ปัญหาการพิสูจน์ตัวจริงของผู้ใช้ที่เข้ามาใช้งานระบบ สามารถเพิ่มความสามารถได้โดยการใช้หลักของ 2 Factors Authentication คือใช้สิ่งที่ผู้ใช้มีคือการเช็คของที่ผูกติดกับผู้ใช้นั่นคือการตรวจสอบ MAC Address ซึ่งถูกกำหนดมาแล้วในมาตรฐาน และสิ่งที่น่าจะเพิ่มขึ้นมาได้แก่การตรวจสอบสิ่งที่ผู้ใช้งานรู้ นั่นก็คือการนำหลักการของ users – password เข้ามาช่วย
   c. ปัญหาของการกำหนดสิทธิ คือนอกจากการพิสูจน์ตัวตนแล้วควรมีการจำกัดสิทธิให้กับผู้ใช้งานแต่ละคนว่าผู้ใช้คนไหน สามารถใช้งานอะไรในระบบได้บ้าง ในส่วนนี้สามารถนำเทคโนโลยีหลายๆตัวมาประยุกต์ใช้ได้ แต่ในโครงงานนี้จะนำเทคโนโลยีของไฟวอลล์มาใช้งาน

3.1 หลักการออกแบบระบบ

หลักการออกแบบระบบแยกส่วนของระบบโดยรวมออกเป็นสองส่วนคือส่วนของทรัพยากรเครือข่ายที่ให้บริการบนเครือข่ายแลนปกติกับส่วนของผู้ที่เข้ามาใช้งานผ่านเครือข่ายไวร์เลสแลน ซึ่งทั้งสองส่วนถูกแยกออกจากกันโดยระบบของโครงงานนี้(ดังรูปที่ 3.1) ซึ่งมีหน้าที่หลักๆ ดังนี้

1. ทำหน้าที่เป็น DHCP Server ให้บริการจ่าย ค่ากำหนดของเน็ตเวิร์ค ให้แก่เครื่องลูกข่าย เช่น IP Address ,Default Gateway
2. ทำหน้าที่รับการลงทะเบียนขอเข้าใช้งานระบบผ่านเวบ
3. ทำหน้าที่ในการพิสูจน์ตัวจริงของผู้เข้ามาใช้งาน
4. ทำหน้าที่จำกัดสิทธิการเข้าใช้ทรัพยากรในเครือข่าย



รูปที่ 3.1 แสดงวิธีการเชื่อมต่อของเครื่องไวร์เลสซีเคยวริตี้เกตเวย์ (WSG)

จากรูปที่ 3.1 จะเห็นได้ว่าในส่วนของโครงงาน WSG นั้นเป็นส่วนที่มาคั่นกลางระหว่างกลุ่มของเครื่องลูกข่าย และกลุ่มของทรัพยากรเครือข่ายที่ให้บริการ การทำงานของโครงงานนี้จะประกอบด้วยกัน 4 ส่วนด้วยกันคือ

1. ส่วนของ DHCP การแจกค่าเน็ตเวิร์คพารามิเตอร์ให้กับเครื่องลูกข่ายเมื่อเครื่องลูกข่ายทำการเชื่อมต่อเข้ามา ในส่วนนี้ทางระบบจะติดตั้งโปรแกรม dhcpd ซึ่งเป็นโปรแกรมทำหน้าที่เป็น DCHP Server โอเพ่นซอร์สโปรแกรมหนึ่ง (รายละเอียดการติดตั้งอยู่ในภาคผนวก) โดยค่าพารามิเตอร์ที่จะถูกแจกไปให้เครื่องลูกข่ายจะมีรายละเอียดดังนี้

- ค่าไอพีแอดเดรสและสับเน็ตมาร์ค จะเป็นค่าคนละเน็ตเวิร์คกับวงของกลุ่มเครือข่ายใช้สาย
- ค่า Default Gateway ค่าที่กำหนดจะต้องเป็นเบอร์ไอพีในส่วนของที่ติดต่อกับเครือข่ายไร้สายของเครื่อง WSG

- Name Server เป็นไอพีของเครื่อง DNS Server ที่ให้บริการอยู่ในระบบ

2. ส่วนของการลงทะเบียนเป็นส่วนของโครงงานที่พัฒนาขึ้นมาใหม่ทำหน้าที่สำหรับให้ผู้ใช้งานที่ต้องการเข้าใช้ระบบติดต่อเข้าไปเพื่อกรอกข้อมูลส่วนตัวที่เป็นความจริงแล้วระบบจะทำการส่งข้อมูลเหล่านั้นไปให้ผู้ดูแลระบบเพื่อทำการพิจารณาว่าจะอนุญาตให้ผู้ร้องขอคนนั้นเข้ามาใช้ระบบหรือไม่ พร้อมกับแจ้งผลการร้องขอผ่านทางอีเมล์โดยผู้ที่ได้รับอนุญาตจะได้รับยูสเซอร์เนมและรหัส ผ่าน เพื่อใช้ในการเข้าระบบต่อไป ซึ่งในส่วนนี้ทางผู้ดูแลระบบสามารถทำการจัดการผู้ใช้งานได้ ซึ่งรายละเอียดการทำงานในส่วนนี้ถูกอธิบายอยู่ในบทที่ 4

3. ส่วนของการพิสูจน์ตัวจริงก่อนเข้าระบบและการล็อคเอาท์ เป็นส่วนของโครงงานที่ถูกพัฒนาเพิ่มขึ้นมาเองโดยทำหน้าที่ในการพิสูจน์ตัวจริงของผู้ร้องขอโดยอาศัยหลักการของการตรวจสอบข้อมูลยูสเซอร์เนมและรหัสผ่าน ที่ผู้ใช้งานทำการ login ผ่านเข้ามาโดยระบบจะทำการบันทึกเวลาการเข้าใช้ระบบ และนำข้อมูลของผู้ใช้อันได้แก่ยูสเซอร์เนม,พาสเวิร์ดและไอพีของผู้ใช้เข้ามาตรวจสอบกับฐานข้อมูลที่ผู้ใช้ทำการลงทะเบียนและได้รับอนุญาตหาก การพิสูจน์ตัวจริงสำเร็จผู้ใช้ก็สามารถเข้าใช้งานระบบได้ แต่หากการพิสูจน์ตัวจริงไม่สำเร็จผู้ร้องขอจะไม่สามารถเข้าใช้งานระบบได้ ในส่วนของการล็อคเอาท์เมื่อผู้ใช้ส่งคำสั่งที่จะต้องการออกจากระบบในการทำงานในส่วนนี้จะทำหน้าที่เคลียร์กฎของไฟร์วอลล์ที่ถูกประยุกต์ใช้อยู่แล้วจากระบบพร้อมกับบันทึกเวลาการออกจากระบบ

4. ระบบการจำกัดสิทธิการเข้าใช้งานเป็นส่วนของโครงงานที่พัฒนาเพิ่มขึ้นมาโดยทำการที่ในการจำกัดสิทธิการเข้าใช้งานของแต่ละคนโดยอาศัยการทำงานของไฟร์วอลล์ในการจำกัดสิทธิการใช้งานของแต่ละคน ซึ่งไฟล์วอล์ที่ถูกนำมาใช้งานคือโปรแกรม IPTABLES ซึ่งเป็น Stateful Inspection Firewallโดยหลักการทำงานคือหลังจากผู้ร้องขอลงทะเบียนขอเข้าใช้งานระบบและผู้ดูแลระบบอนุญาตให้เข้าใช้งานแล้วผู้ดูแลระบบจะต้องทำการกำหนดสิทธิว่าจะให้ผู้ใช้คนนั้นสามารถเข้าใช้งานระบบในส่วนใดได้บ้างโดยจะเก็บข้อมูลในส่วนนี้ลงในฐานข้อมูล จากนั้นเมื่อผู้ใช้งานผ่านขั้นตอนพิสูจน์ตัวจริงแล้วระบบจะทำการสืบค้นสิทธิการเข้าใช้งานที่ถูกกำหนดไว้ในฐานข้อมูล และทำการสร้างเป็นสคริปต์ของไฟร์วอลล์ซึ่งมีกฎต่างๆ ที่เหมาะสมกับผู้ใช้คนนั้น และทำการรันสคริปต์นี้เพื่อให้ไฟล์วอลล์ทำการประยุกต์ใช้งานกฎที่สร้างมาใหม่นี้ซึ่งรายละเอียดการทำงานของนโยบายการกำหนดค่าในไฟวอล์จะใช้หลักการ DROP ทุก Packet ที่เข้ามา และจะอนุญาตบาง Packet ที่เหมาะสมเท่านั้นโดยรายละเอียดมีดังต่อไปนี้

1. กำหนดให้เครื่องมีความสามารถในการฟอร์เวิร์ดและ Routing Packet ได้โดยการแก้ไข ค่าของ net.ipv4.ip_forward ในไฟล์_/etc/sysctl.conf จาก “0” ให้เป็น “1” และใช้คำสั่ง /sbin/sysctl –p เพื่อประยุกต์ใช้ค่าที่เปลี่ยนแปลงใหม่

2. ได้นโยบายของ Chain INPUT และ chain FORWARD ในตาราง Filter จะเป็น DROP ทั้งหมดเพื่อเป็นการกำหนดว่าถ้าแพคเก็ตที่เข้ามาไม่ตรงกับกฎไหนเลยใน chain INPUT และ FORWARD แพคเก็ตนั้นจะถูก DROP มีรูปแบบการสั่งงานดังนี้

   $iptables –A FORWARD –P DROP

   $iptables –A INPUT –P DROP

3. อนุญาตแพคเก็ตที่เกี่ยวข้องกันกับ Connection ที่สร้างไว้แล้ว เช่น packet ที่ส่งข้อมูลออกไปจาก web server เมื่อมี request web service เข้ามา และอนุญาตแพคเก็ตที่เกี่ยวข้องกับ connection ที่สร้างไว้แล้ว แต่ไม่ใช่ส่วนหนึ่งส่วนใดของ connection นั้น เช่น FTP data packet (port 20) ที่เกิดขึ้นจากการใช้คำสั่งใน FTP command (port 21) โดยมีรูปแบบคำสั่งดังนี้

   $iptables –A FORWARD –m state –state ESTABLISHED,RELATED –j ACCEPT

4. อนุญาตให้เครื่องลูกข่ายสามารถเข้ามาลงทะเบียนเพื่อขอเข้าใช้ระบบ และอนุญาตให้ผู้ใช้งานสามารถเข้ามาทำการ Login เข้าระบบได้โดยระบบจะเปิด Port 443 เพื่อรอการเชื่อมต่อโดยใช้โปโตคอล HTTPS จากผู้ใช้งานโดยใช้คำสั่ง

   $iptables –A INPUT –p TCP - -dport 443 –j ACCEPT

5. เป็นการกำหนดสิทธิของแต่ละ user ที่เข้ามาใช้งาน ซึ่งกฎที่ใช้จะมีรูปแบบเดียวกันทั้งหมดแต่จำนวนสิทธิที่ได้ของแต่ละคนจะไม่เท่ากันตามแต่ผู้ดูแลระบบจะอนุญาต ซึ่งรูปแบบของกฎที่ใช้งานคือ

   $iptables –A FORWARD –p <Protocol> - -dport <Destination Port> -s <Source IP> -d <Destination IP> -j ACCEPT

   <Protocol> : คือโปรโตคอลที่อนุญาตให้ใช้ได้โดยระบบจะมีให้เลือกอยู่ 3 โปรโตคอลคือ TCP , UDP และ ICMP (กำหนดโดยผู้ดูแลระบบ)

   <Destination Port> : คือ Service ที่อนุญาตให้ใช้งานบน <Destination IP> (กำหนดโดยผู้ดูแลระบบ)

   <Source IP> : เป็นไอพีต้นทางของผู้ใช้งานที่ใช้เข้ามาทำการเชื่อมต่อกับระบบซึ่งค่านี้ระบบจะทำการจัดเก็บมาในขณะที่ผู้ใช้งานผ่านขั้นตอนพิสูจน์ตัวจริงเข้ามาแล้ว

   <Destination IP> : เป็นไอพีต่างๆ ของทรัพยากรที่มีอยู่ในระบบ (กำหนดโดยผู้ดูแลระบบ)

3.2 ขั้นตอนการทำงานโดยรวมของระบบ

การทำงานของระบบจะแบ่งออกเป็นสองส่วนด้วยกันได้แก่ในส่วนของผู้ใช้ และส่วนของผู้ดูแลระบบ ซึ่งข้อแตกต่างระหว่างสองส่วนนั้นคือการใช้งานของผู้ใช้งานจะสามารถเข้าใช้งานระบบทรัพยากรที่เตรียมไว้ให้แล้ว และสามรถจัดการข้อมูลของตนเองได้เท่านั้น แต่การใช้งานของผู้ดูแลระบบนั้นนอกจากสามารถเข้าใช้ทรัพยากรได้แล้ว ยังสามารถจัดการการเข้าส่วนต่างๆในระบบได้อีก คือ

1. สามารถดูแลจัดการยูสเซอร์ข้อมูลของยูสเซอร์ทุกๆคนได้
2. สามารถจัดการเข้าใช้งานระบบระบบได้
3. สามารถกำหนดทรัพยากรที่สามารถใช้งานได้ให้แต่ละยูสเซอร์
4. สามารถดูข้อมูลการเข้าใช้งานระบบของยูสเซอร์ได้

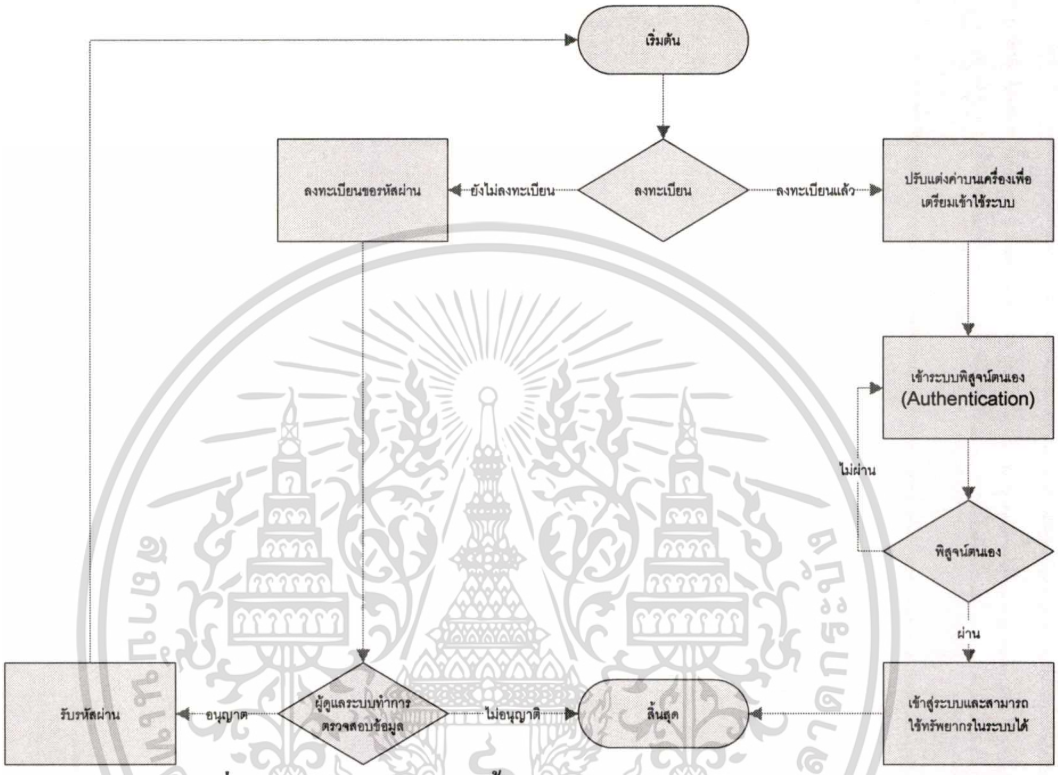
ซึ่งสามารถเขียนให้อยู่ในรูปของคอนเท็กซ์ไดอะแกรมได้ดังแสดงตามรูปที่ 3.2

รูปที่ 3.2 คอนเท็กซ์ไดอะแกรมแสดงการทำงานของระบบงานใหม่

รายละเอียดขั้นตอนการทำงานของระบบทั้งของยูสเซอร์ และผู้ดูแลระบบจะอยู่ในหัวข้อถัดไป

3.3 การใช้งานระบบของยูสเซอร์

การใช้งานระบบของยูสเซอร์สามารถแสดงเป็น Flow chart ได้ดังต่อไปนี้



รูปที่ 3.3 แสดง Flow Chart ขั้นตอนการเข้าใช้ระบบของยูสเซอร์

1. เริ่มต้นผู้ใช้งานจะต้องทำการลงทะเบียนเพื่อขอเข้าใช้งานระบบโดยการเปิดหน้าเว็บที่ให้บริการลงทะเบียน เพื่อขอเข้าใช้ระบบ โดยผู้ใช้ลงทะเบียนจะต้องทำการกรอกข้อมูลที่เป็นความจริง เพราะข้อมูลนี้จะถูกนำไปพิจารณาโดยผู้ดูแลระบบว่าจะอนุญาตให้เข้าใช้งานหรือไม่
2. ผู้ใช้รอรับอีเมล์ตอบรับจากผู้ดูแลระบบสำหรับผู้ที่ได้รับอนุญาตในอีเมล์จะกำหนดยูสเซอร์เนมและรหัสผ่านมาให้ โดยรหัสผ่านนี้ผู้ใช้สามารถทำการเปลี่ยนได้ทีหลัง
3. เมื่อเริ่มต้นใช้งานในเครื่องลูกข่ายต้องถูกกำหนดให้รับค่ากำหนดของเน็ตเวิร์คจากระบบ
4. หลังจากที่ผู้ใช้ได้รับการตั้งค่าเน็ตเวิร์คแล้วจากนั้นต้องทำการเชื่อมต่อกับระบบผ่านวีพีเอ็นเพื่อที่จะทำการพิสูจน์ตัวจริงกับระบบ ซึ่งถ้าผู้ใช้ไม่ทำการเชื่อมต่อแบบวีพีเอ็น ระบบจะไม่ยอมให้เข้าใช้งาน
5. เริ่มใช้งานผู้ใช้ต้องทำการกรอกล็อกอินแอคเคาน์และรหัสผ่านของตนเองที่ได้จากอีเมล์ผ่านทางเว็บที่ระบบได้เตรียมไว้ให้

6. ระบบนำข้อมูลการล็อกอินเข้ามาตรวจสอบกับฐานข้อมูลของตนเอง ถ้าหากข้อมูลนั้นถูกต้องก็จะอนุญาตให้เข้าใช้งานระบบได้แต่ถ้าไม่ถูกต้องก็จะไม่อนุญาตให้เข้าใช้

3.3.1 การออกแบบการไหลของข้อมูลของระบบในระดับที่ 1 ของการใช้งานระบบของยูสเซอร์

ในรูป 3.3 ได้แสดงภาพ Flow Chart Diagram ซึ่งเป็นการออกแบบระบบในระดับความคิดไปแล้ว ในหัวข้อนี้ จึงเป็นการออกแบบระบบในระดับการไหลของข้อมูลของระบบในระดับที่ 1 สามารถแสดงได้ดังรูปที่ 3.4 (อยู่ในหน้าถัดไป)

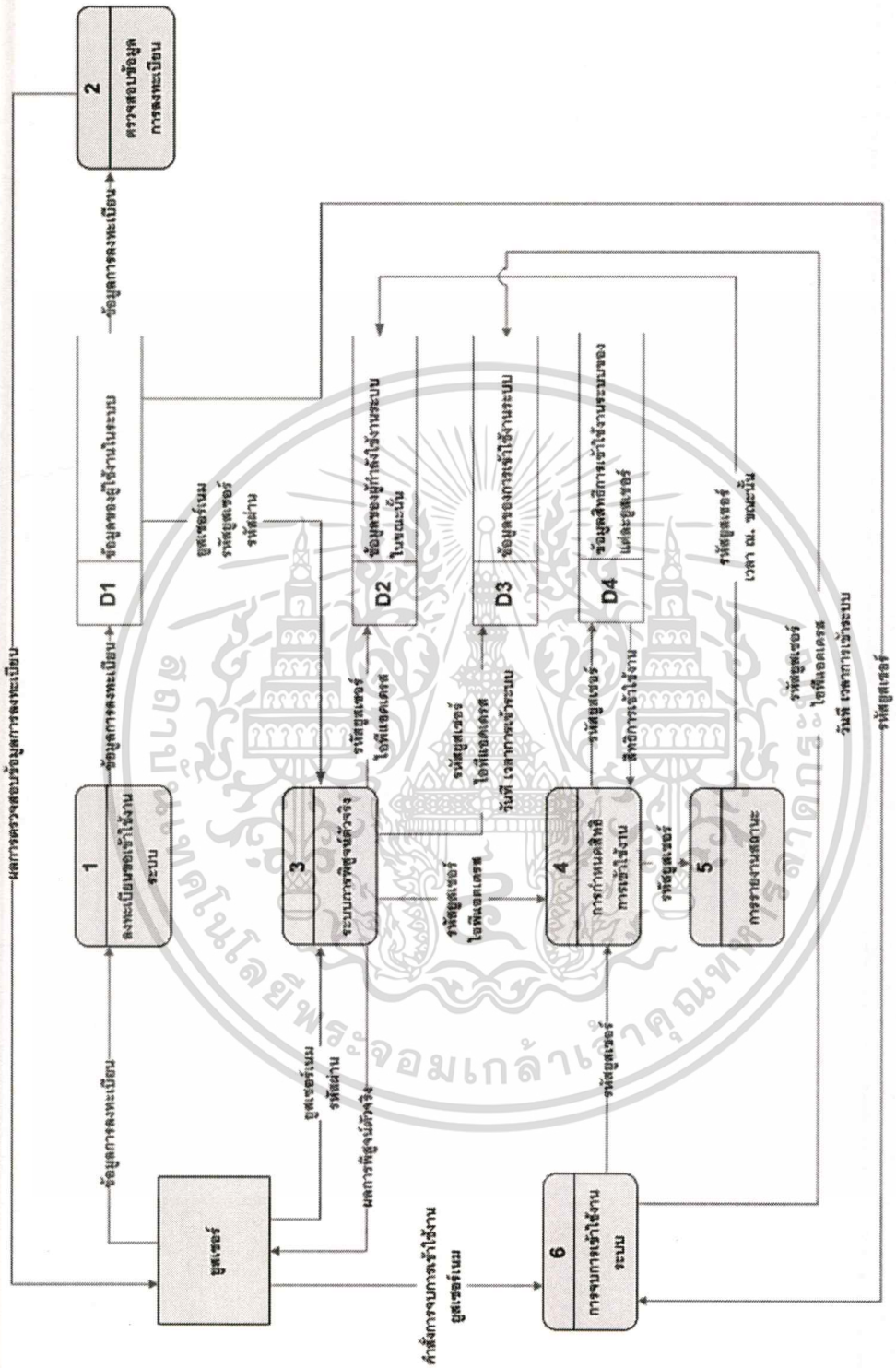
จากรูปที่ 3.4 มีโปรเซสในระบบในระดับที่ 1 ทั้งหมด 6 โปรเซสคือ

1. ลงทะเบียนขอเข้าใช้ระบบ
2. ตรวจสอบข้อมูลการลงทะเบียน
3. ระบบการพิสูจน์ตัวจริง
4. การกำหนดสิทธิการเข้าใช้งาน
5. การรายงานสถานะ
6. การจบการเข้าใช้งานระบบ

รายละเอียดการทำงานของแต่ละโปรเซส มีดังต่อไปนี้

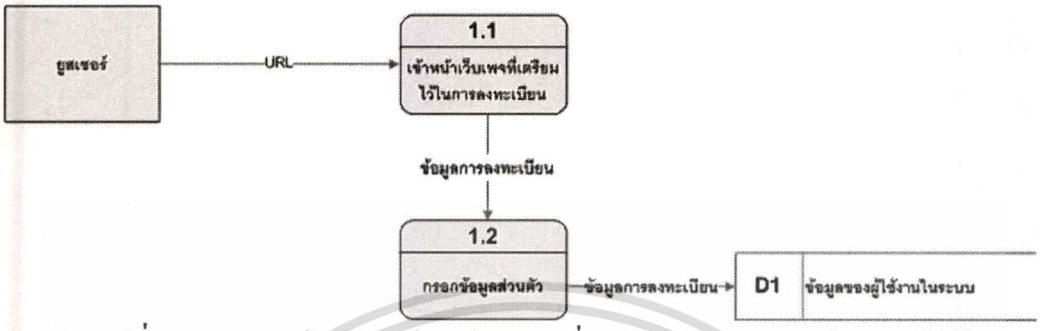
3.3.1.1 การออกแบบการไหลของข้อมูลในระดับที่ 2

การออกแบบในระดับนี้เป็นการแสดงแผนภาพการไหลของข้อมูลในระดับที่ 2 ซึ่งเป็นการแสดงรายละเอียดของโปรเซส 1-4 ใน รูปที่ 3.3 ที่แสดงได้ในหัวข้อที่ 3.3.1



รูปที่ 3.4 แสดงแผนภาพการไหลของข้อมูลในระดับที่ 1

การไหลของข้อมูลในระดับที่ 2 ของโปรเซสลงทะเบียนขอเข้าใช้ระบบ

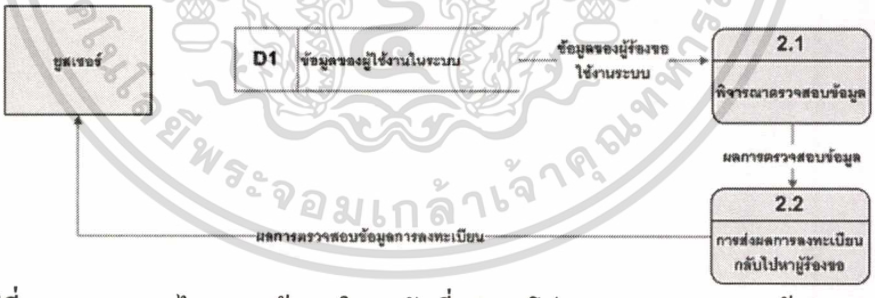


รูปที่ 3.5 แสดงการไหลของข้อมูลในระดับที่ 2 ของโปรเซสลงทะเบียนขอเข้าใช้ระบบ

รายละเอียดการทำงานสามารถอธิบายได้ดังนี้

1. ผู้ใช้งานเปิดหน้าเว็บเพจที่รองรับการลงทะเบียนเข้าใช้ระบบผ่าน URL ที่กำหนด
2. ผู้ใช้งานทำการกรอกข้อมูลส่วนตัวลง จากนั้นข้อมูลนี้จะถูกจัดเก็บลงในฐานข้อมูลของผู้ใช้งานระบบเพื่อรอให้ผู้ดูแลระบบเข้ามาตรวจสอบข้อมูลต่อไป

การไหลของข้อมูลในระดับที่ 2 ของโปรเซสการตรวจสอบข้อมูลการลงทะเบียน



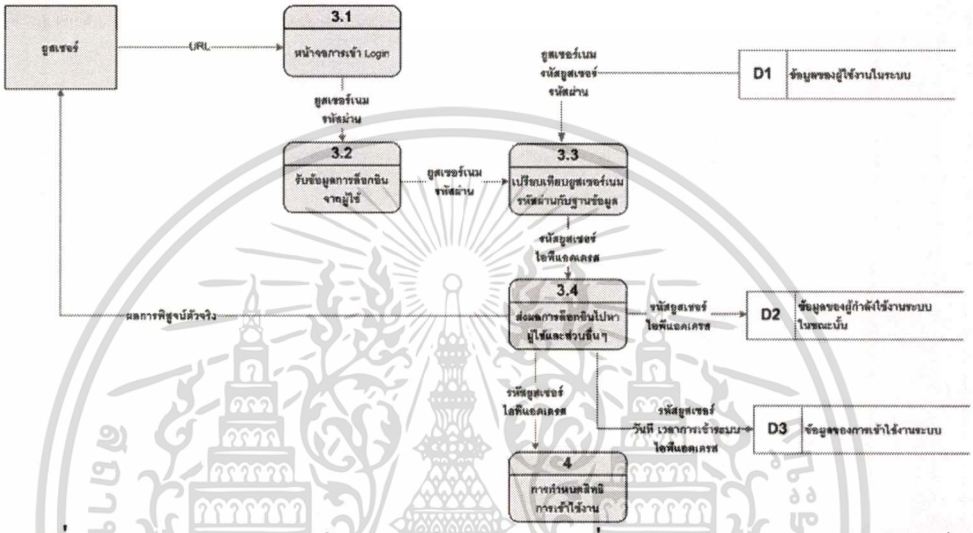
รูปที่ 3.6 แสดงการไหลของข้อมูลในระดับที่ 2 ของโปรเซสการตรวจสอบข้อมูลการลงทะเบียน

รายละเอียดการทำงานสามารถอธิบายได้ดังนี้

1. ผู้ดูแลระบบทำการดึงข้อมูลจากฐานข้อมูลผู้ใช้งานระบบซึ่งในส่วนนี้จะดึงออกมาเฉพาะในส่วนของผู้ที่ร้องขอเข้ามาแต่ยังไม่ได้รับอนุญาตเท่านั้น

2. หลังจากทำการพิจารณาแล้วทำการส่งผลการลงทะเบียนกลับไปหาผู้ร้องขอผ่านทางอีเมล์ที่ผู้ร้องขอได้ให้ข้อมูลไว้หากผ่านการพิจารณาในอีเมล์จะมีข้อมูลยูสเซอร์เนมและรหัสผ่านสำหรับใช้ในการเข้าระบบแนบติดไปด้วย

การไหลของข้อมูลในระดับที่ 2 ของโปรเซสระบบการพิสูจน์ตัวจริง

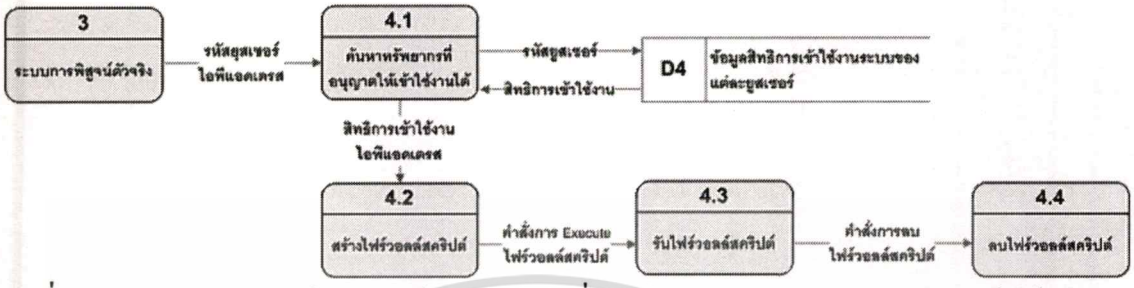


รูปที่ 3.7 แสดงแผนภาพการไหลของข้อมูลในระดับที่ 2 ของโปรเซสระบบการพิสูจน์ตัวจริง

รายละเอียดการทำงานสามารถอธิบายได้ดังนี้

1. ผู้ใช้งานเปิดหน้าเว็บเพจที่รองรับการล็อกอินเข้าใช้ระบบผ่าน URL ที่กำหนด
2. ผู้ใช้งานกรอกยูสเซอร์เนมและรหัสผ่านส่งเข้าสู่ระบบ
3. ระบบทำการรับข้อมูลการล็อกอินของผู้ใช้เข้ามา และดึงข้อมูลของผู้ใช้คนนั้นจากฐานข้อมูลมาเปรียบเทียบ
4. ระบบส่งผลการพิสูจน์ตัวจริงกลับไปหาผู้ใช้งานถ้าการพิสูจน์ตัวจริงผ่านระบบจะทำการหาไอพีแอดเดรสของผู้ใช้และทำการส่งข้อมูลไปยังส่วนต่างๆดังนี้
    a. ส่งรหัสยูสเซอร์และไอพีแอดเดรสเข้าฐานข้อมูลของผู้กำลังใช้งานระบบอยู่ในขณะนั้น
    b. ส่งรหัสยูสเซอร์วันที่เวลาการเข้าใช้ระบบข้าฐานข้อมูลของการเข้าใช้งานระบบ
    c. ส่งรหัสยูสเซอร์และไอพีแอดเดรสไปยังส่วนของการกำหนดสิทธิการเข้าใช้งาน เพื่อทำการเปิดอนุญาตการเข้าใช้งานให้เฉพาะตามสิทธิที่กำหนด

การไหลของข้อมูลในระดับที่ 2 ของโปรเซสการกำหนดสิทธิการเข้าใช้งาน

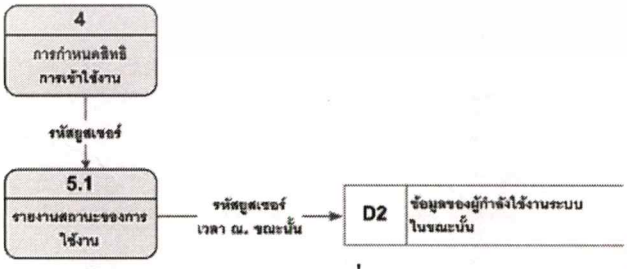


รูปที่ 3.8 แสดงแผนภาพการไหลของข้อมูลในระดับที่ 2 ของโปรเซสการกำหนดสิทธิการเข้าใช้งาน

รายละเอียดการทำงานสามารถอธิบายได้ดังนี้

1. หลังจากผ่านการพิสูจน์ตัวจริงแล้วระบบการพิสูจน์ตัวจริงจะส่งรหัสยูเซอร์ และไอพีมาให้กับระบบการกำหนดสิทธิการเข้าใช้งาน
2. ระบบทำการค้นหาสิทธิของยูสเซอร์คนนี้ในฐานข้อมูลซึ่งข้อมูลสิทธิของแต่ละบุคคลจะถูกกำหนดไว้ให้อยู่แล้วโดยผู้ดูแลระบบ
3. นำไอพี และข้อมูลสิทธิการใช้งานระบบของผู้ถูกอนุญาตมาสร้างเป็นไฟร์วอลล์สคริปต์
4. ทำการรันไฟร์วอลล์สคริปต์เพื่อประยุกต์เพิ่มกฎใหม่ให้กับไฟร์วอลล์เพื่อให้ผู้ใช้คนนี้สามารถเข้าใช้ระบบได้ตามสิทธิที่มีอยู่
5. เมื่อรันไฟร์วอลล์สคริปต์เสร็จแล้วก็ทำการลบสคริปต์นี้ทิ้งไปเพราะจะไม่มีการเรียกใช้อีกต่อไป เพราะถ้าผู้ใช้คนเดิมเข้ามาใช้ระบบอีกที ทางระบบก็จะสร้างสคริปต์อันใหม่ให้อีกที

การไหลของข้อมูลในระดับที่ 2 ของโปรเซสการรายงานสถานะ

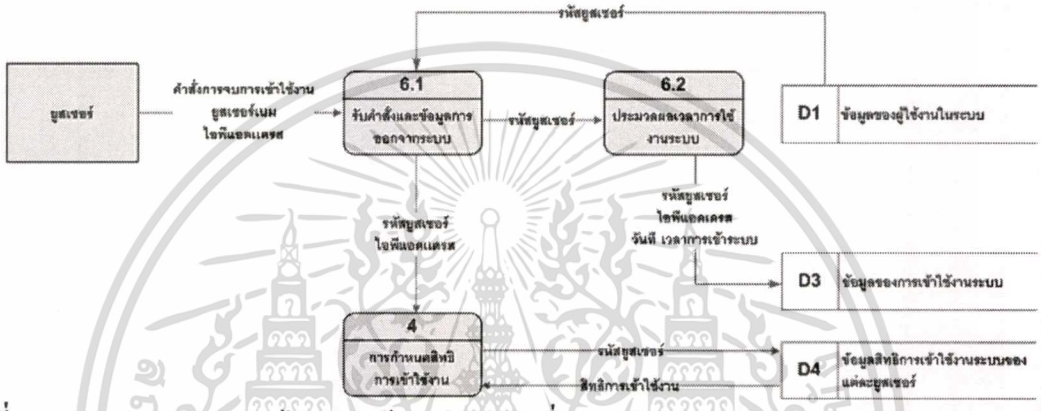


รูปที่ 3.9 แสดงแผนภาพการไหลของข้อมูลในระดับที่ 2 ของโปรเซสการรายงานสถานะ

รายละเอียดการทำงานสามารถอธิบายได้ดังนี้

เมื่อผู้ใช้ผ่านการพิสูจน์สิทธิ และได้รับสิทธิการเข้าใช้ระบบแล้ว ระบบทางฝั่งผู้ใช้จะมีการรายงานสถานะของตนโดยส่งรหัสผู้ใช้งานของตนและเวลา ณ.ขณะนั้น ไปยังฝั่งเซิร์ฟเวอร์ทุกๆ5-10 วินาที เพื่อยืนยันว่ามีการใช้งานระบบอยู่

การไหลของข้อมูลในระดับที่ 2 ของโปรเซสการจบการเข้าใช้งานระบบ



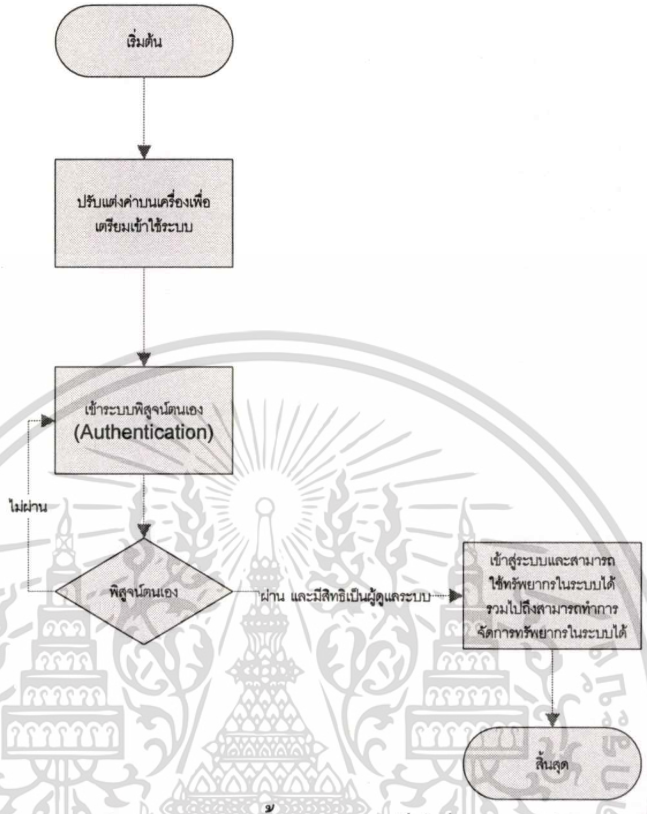
รูปที่ 3.10 แสดงแผนภาพการไหลของข้อมูลในระดับที่ 2 ของโปรเซสการกำหนดสิทธิการจบการเข้าใช้งานระบบ

รายละเอียดการทำงานสามารถอธิบายได้ดังนี้

1. ผู้ใช้ทำการส่งคำสั่งจบการทำงานพร้อมทั้งยูสเซอร์เนมเข้าสู่ระบบ
2. ระบบทำการค้นหารหัสยูสเซอร์จากฐานข้อมูลจากนั้นส่งต่อไปยังส่วนของการประมวลผลเวลาการใช้งานระบบ และส่วนของการกำหนดสิทธิการใช้งาน
3. ส่วนของการประมวลผลเวลาการใช้งานระบบทำการประมวลผลเวลาและเก็บบันทึกลงฐานข้อมูล
4. ส่วนของการกำหนดสิทธิเข้าใช้งานจะมีกระบวนการทำงานเหมือนตอนเข้ามาขอเข้าใช้งานดังที่ได้กล่าวไว้ในหัวข้อที่แล้วแต่จะทำการสร้างสคริปต์ไฟร์วอลล์ในการลบกฎที่อนุญาตการเข้าใช้งานของผู้ใช้คนนี้ออกไปทั้งหมด จากนั้นทำการรันสคริปต์นี้และลบสคริปต์นี้ออกไปเมื่อรันเสร็จแล้ว

3.4 การใช้งานระบบของผู้ดูแลระบบ

การใช้งานระบบของยูสเซอร์ที่เป็นผู้ดูแลระบบสามารถแสดงเป็น Flow chart ได้ดังต่อไปนี้

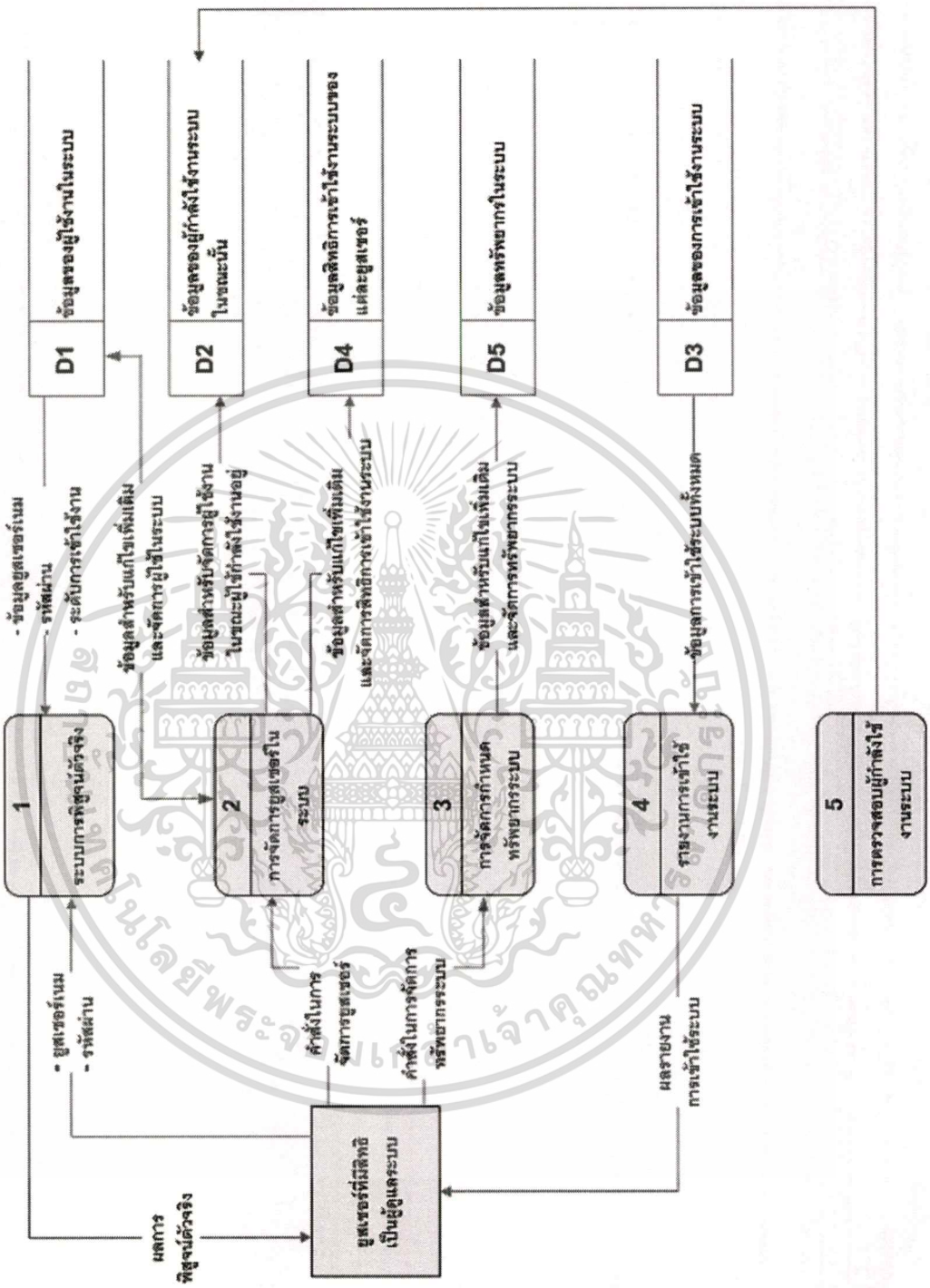


รูปที่ 3.11 แสดง Flow Chart ขั้นตอนการเข้าใช้ระบบของยูสเซอร์

1. ผู้เข้าใช้งานระบบทำการกำหนดเครื่องลูกข่ายให้รับค่าเน็ตเวิรคพารามิเตอร์จากระบบ
2. ทำการพิสูจน์ตัวจริงกับระบบโดยการกรอกข้อมูลยูสเซอร์และพาสเวิร์ดของตนผ่านทางหน้าเว็บที่ระบบเตรียมไว้
3. เมื่อผ่านการพิสูจน์ตัวจริงแล้วผู้ดูแลระบบสามารถเข้าใช้ระบบได้พร้อมกับสามารถเข้าหน้าจอการจัดการเกี่ยวกับระบบได้ โดยรายละเอียดในแต่ละส่วนนั้นมีดังต่อไปนี้

3.4.1 การออกแบบการไหลของข้อมูลของระบบในระดับที่ 1 การใช้งานระบบของผู้ดูแลระบบ

ดังที่ได้กล่าวมาแล้วในหัวข้อที่ 3.2 คือการเข้าใช้ระบบของยูสเซอร์ที่เป็นผู้ดูแลนอกจากการเข้ามาใช้ทรพยากรในระบบได้แล้ว ก็ยังสามารถดูแลจัดการทรัพยากรต่างๆในระบบได้อีก ซึ่งในรายละเอียดส่วนของการเข้าใช้ระบบนั้นจะมีขั้นตอนรายละเอียดวิธีการออกแบบการไหลของข้อมูลเหมือนกับการที่ผู้ใช้ทั่วไปเข้ามาใช้งานระบบ ดังนั้นในหัวข้อนี้จึงขอกล่าวรายละเอียดเฉพาะส่วนที่เพิ่มเติมออกมาของผู้ดูแลระบบเท่านั้น ซึ่งการไหลของข้อมูลในระดับที่ 1 ของผู้ดูแลระบบสามารถแสดงออกมาเป็นDataFlowDiagramได้ดังต่อไปนี้



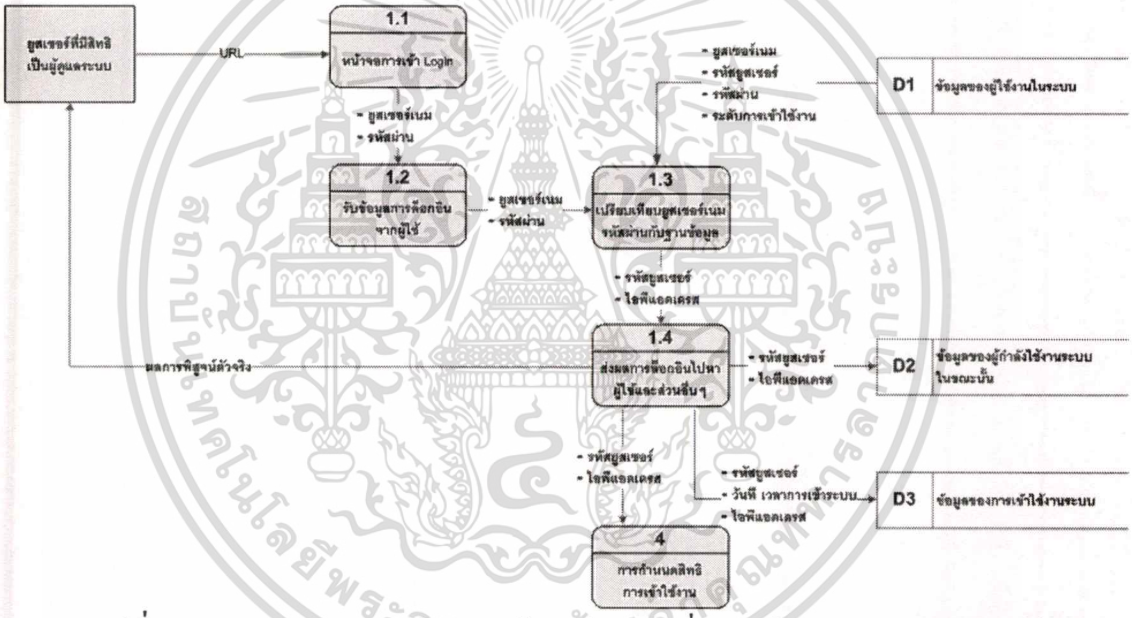
รูปที่ 3.12 แสดงแผนภาพการไหลของข้อมูลในระดับที่ 1

จากรูปที่ 3.12 มีโปรเซสในระบบในระดับที่ 1 ทั้งหมด 5 โปรเซสคือ

1. ระบบพิสูจน์ตัวเอง
2. การจัดการยูสเซอร์ในระบบ
3. การจัดการกำหนดทรัพยากรในระบบ
4. รายงานการเข้าใช้งานของระบบ
5. การตรวจสอบผู้กำลังใช้งานระบบ

รายละเอียดการทำงานของแต่ละโปรเซส มีดังต่อไปนี้

การไหลของข้อมูลในระดับที่ 2 ของโปรเซสระบบพิสูจน์ตัวจริง



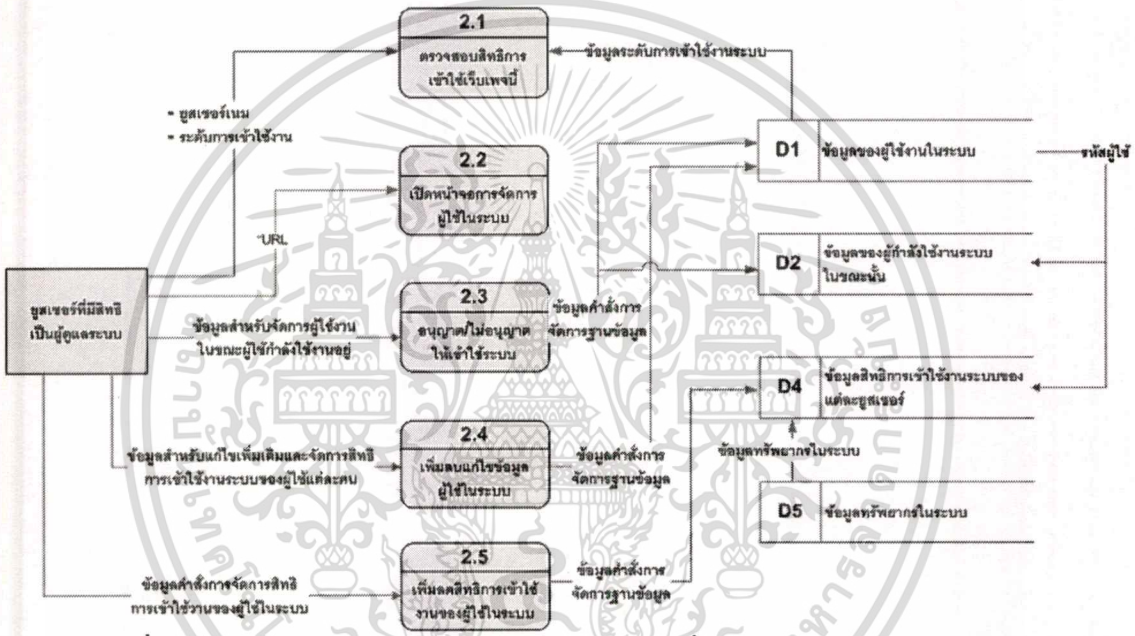
รูปที่ 3.13 แสดงแผนภาพการไหลของข้อมูลในระดับที่ 2 ของโปรเซสระบบการพิสูจน์ตัวจริง

รายละเอียดการทำงานสามารถอธิบายได้ดังนี้

1. ผู้ใช้งานเปิดหน้าเว็บเพจที่รองรับการล็อกอินเข้าใช้ระบบผ่าน URL ที่กำหนด
2. ผู้ใช้งานกรอกยูสเซอร์เนมและรหัสผ่านส่งเข้าสู่ระบบ
3. ระบบทำการรับข้อมูลการล็อกอินของผู้ใช้เข้ามาและดึงข้อมูลของผู้ใช้คนนั้นจากฐานข้อมูลมาเปรียบเทียบ
4. ระบบส่งผลการพิสูจน์ตัวจริงกลับไปหาผู้ใช้งานถ้าการพิสูจน์ตัวจริงผ่านระบบจะทำการหาไอพีแอดเดรสของผู้ใช้และทำการส่งข้อมูลไปยังส่วนต่างๆดังนี้

a. ส่งรหัสยูสเซอร์และไอพีแอดเดรสเข้าฐานข้อมูลของผู้กำลังใช้งานระบบอยู่ในขณะนั้น
b. ส่งรหัสยูสเซอร์วันที่เวลาการเข้าใช้ระบบข้าฐานข้อมูลของการเข้าใช้งานระบบ
c. ส่งรหัสยูสเซอร์และไอพีแอดเดรสไปยังส่วนของการกำหนดสิทธิการเข้าใช้งานเพื่อทำการเปิดอนุญาตการเข้าใช้งานทุกอย่างในระบบ

การไหลของข้อมูลในระดับที่ 2 ของโปรเซสการจัดการผู้ใช้ในระบบ



รูปที่ 3.14 แสดงแผนภาพการไหลของข้อมูลในระดับที่ 2 ของโปรเซสการจัดการผู้ใช้ในระบบ

รายละเอียดการทำงานสามารถอธิบายได้ดังนี้

1. ผู้ใช้ที่เข้ามาที่หน้าเพจนี้จะถูกทำการตรวจสอบระดับการเข้าใช้งานว่ามีสิทธิเข้าใช้งานหรือไม่ ถ้าผู้ใช้มีสิทธิเป็นผู้ดูแลระบบก็จะสามารถเข้ามาใช้งานในส่วนนี้ได้ โดยจะมีฐานข้อมูลเก็บระดับการเข้าใช้งานระบบ
2. ในส่วนนี้ผู้ใช้สามารถทำการอนุญาต,ไม่อนุญาตหรือระงับการเข้าใช้งานระบบชั่วคราวในบางยูสเซอร์ได้ในส่วนนี้จะถูกบันทึกลงในฐานข้อมูลของผู้ใช้งานในระบบ
3. ผู้ใช้สามารถทำการเพิ่มลบแก้ไขข้อมูลของผู้ใช้ และสามารถแก้ไขระดับการเข้าใช้งานของผู้ใช้แต่ละคนได้ในส่วนนี้จะถูกบันทึกลงในฐานข้อมูลของผู้ใช้งานในระบบ

4. ผู้ใช้สามารถทำการเพิ่มหรือลดสิทธิการเข้าใช้งานระบบของผู้ใช้งานแต่ละคนได้ โดยข้อมูลของทรัพยากรระบบจะถูกดึงมาจากฐานข้อมูลทรัพยากรในระบบ ซึ่งข้อมูลนี้สามารถปรับแต่งได้ซึ่งรายระเอียดอยู่ในข้อถัดไป

การไหลของข้อมูลในระดับที่ 2 ของโปรเซสการจัดการกำหนดทรัพยากรในระบบ

รูปที่ 3.15 แสดงแผนภาพการไหลของข้อมูลในระดับที่ 2 ของโปรเซสการจัดการผู้ใช้ในระบบ

จากรูปที่ 3.15 รายละเอียดการทำงานสามารถอธิบายได้ดังนี้

1. ผู้ใช้ที่เข้ามาที่หน้าเพจนี้จะถูกทำการตรวจสอบระดับการเข้าใช้งานว่ามีสิทธิเข้าใช้งานหรือไม่ ถ้าผู้ใช้มีสิทธิเป็นผู้ดูแลระบบก็จะสามารถเข้ามาใช้งานในส่วนนี้ได้ โดยข้อมูลระดับการเข้าใช้งานระบบจะถูกเรียกจากฐานข้อมูลของผู้ใช้งานในระบบ
2. ผู้ใช้สามารถส่งคำสั่งการเพิ่มลบหรือแก้ไขข้อมูลทรัพยากรในระบบ โดยลักษณะข้อมูลทรัพยากรระบบจะถูกเก็บลงในฐานข้อมูลทรัพยากรระบบซึ่งเก็บชุดข้อมูลดังต่อไปนี้
    a. ไอพีของเครื่องที่อนุญาตให้เข้าไปใช้งาน
    b. เซอร์วิสที่เปิดให้บริการที่เครื่องไอพีนั้น

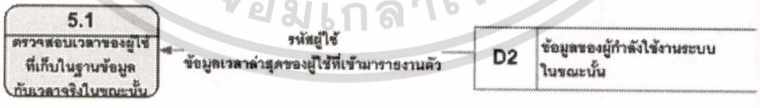
การไหลของข้อมูลในระดับที่ 2 ของโปรเซสรายงานการเข้าใช้งานของระบบ

รูปที่ 3.16 แสดงแผนภาพการไหลของข้อมูลในระดับที่ 2 ของโปรเซสรายงานการเข้าใช้งานของระบบ

จากรูปที่ 13.16 รายละเอียดการทำงานสามารถอธิบายได้ดังนี้

1. ผู้ใช้ที่เข้ามาที่หน้าเพจนี้จะถูกทำการตรวจสอบระดับการเข้าใช้งานว่ามีสิทธิเข้าใช้งานหรือไม่ ถ้าผู้ใช้มีสิทธิเป็นผู้ดูแลระบบก็จะสามารถเข้ามาใช้งานในส่วนนี้ได้ โดยข้อมูลระดับการเข้าใช้งานระบบจะถูกเรียกจากฐานข้อมูลของผู้ใช้งานในระบบ
2. ผู้ใช้เรียกดูข้อมูลการใช้งานระบบโดยการส่งคำสั่งให้แสดงรายงานการเข้าใช้ระบบ โดยโปรเซสนี้จะดึงข้อมูลจากฐานข้อมูลของการเข้าใช้งานระบบมาระมวลผลเป็นรูปแบบรายงานส่งกลับไปหาผู้ใช้งาน

การไหลของข้อมูลในระดับที่ 2 ของโปรเซสการตรวจสอบผู้กำลังใช้งานระบบ



รูปที่ 3.17 แสดงแผนภาพการไหลของข้อมูลในระดับที่ 2 ของโปรเซสการตรวจสอบผู้กำลังใช้งานระบบ

จากรูปที่ 13.17 รายละเอียดการทำงานสามารถอธิบายได้ดังนี้

โปรเซสนี้มีเพื่อการตรวจสอบในกรณีที่ผู้ใช้งานไม่ได้ทำการส่งคำสั่งเพื่อออกจากระบบ แต่ได้ออกจกระบบไปแล้ว เช่นครื่องทางฝั่งผู้ใช้งานถูกปิดไปโดยไม่ตั้งใจ การทำงานจะทำโดยมีการตั้งเวลาเข้าไปตรวจสอบข้อมูลในฐานข้อมูลโดยตรวจสอบว่าเวลาของผู้ใช้ในฐานข้อมูล กับเวลาปัจจุบันห่าง

กันเกิน 5 นาทีหรือไม่ถ้าพบว่าเกิน 5 นาทีโปรเซสนี้จะทำการล็อคเอาท์ผู้ใช้คนนั้นออกจากระบบโดยอัตโนมัติ

3.5 รายละเอียดของฐานข้อมูล

ในหัวข้อที่ผ่านมาเป็นการแสดงการไหลของข้อมูลในระดับที่ 1และ 2 ซึ่งในแผนภาพมีการเก็บข้อมูลลงในฐานข้อมูล ซึ่งประกอบไปด้วย 5 ตารางด้วยกัน ซึ่งแต่ละตารางมีความสัมพันธ์ และรายละเอียดดังนี้

D1 : ข้อมูลของผู้ใช้งานในระบบ (T_Members) ทำหน้าที่เก็บข้อมูลส่วนตัวของผู้ใช้งานแต่ละคน รวมไปถึงรหัสผ่าน ซึ่งเป็นข้อมูลที่ถูกเข้ารหัสไว้ และข้อมูลแสดงสถานะการเข้าใช้งานว่าจะเข้าไปใช้งานได้หรือไม่

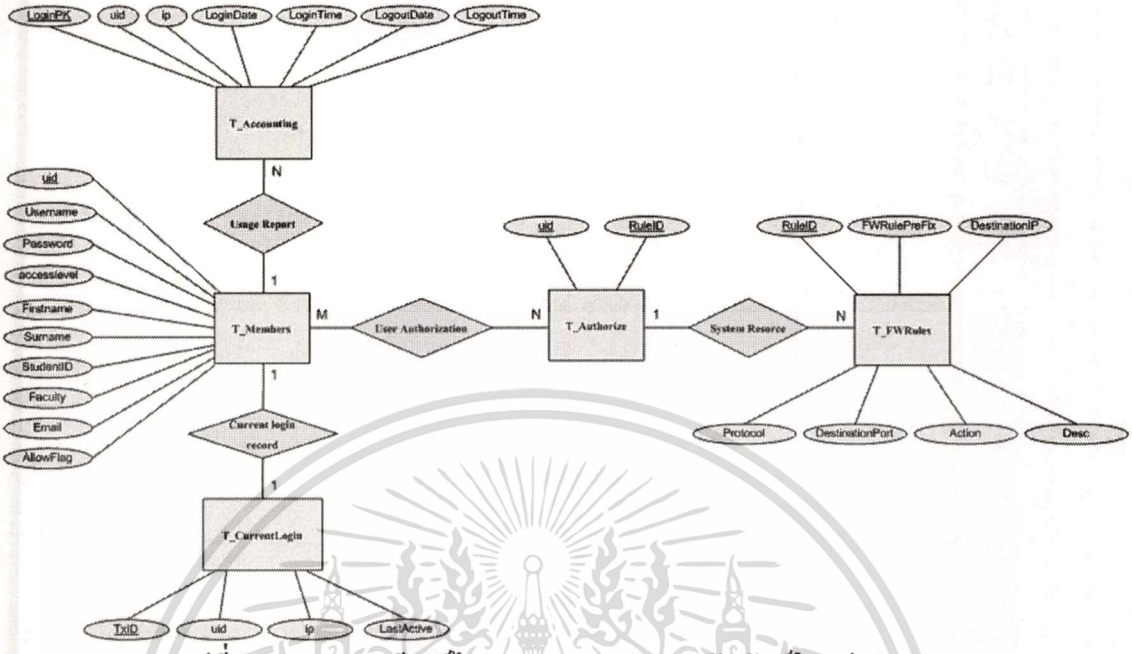
D2 : ข้อมูลของผู้ที่กำลังใช้งานระบบขณะนั้น (T_CurrentLogin) ทำหน้าที่เก็บข้อมูลว่ามีผู้ใช้คนใดบ้างที่กำลังใช้งานระบบอยู่ และเวลาล่าสุดที่ผู้ใช้มารายงานตัว

D3 : ข้อมูลของการเข้าใช้งานในระบบ (T_Accounting) เป็นตารางการบันทึกวันที่ เวลาการเข้าใช้ และจบการทำงานของผู้ใช้แต่ละคน

D4 : ข้อมูลสิทธิการเข้าใช้งานระบบของแต่ละยูสเซอร์ (T_Authorize) เป็นตารางบันทึกสิทธิการเข้าใช้ระบบว่าผู้ใช้งานผู้นี้สามารถเข้าใช้งานส่วนใดของระบบได้บ้าง

D5 : ข้อมูลทรัพยากรในระบบ (T_FWRules) เป็นตารางบันทึกข้อมูลทรัพยากรที่ระบบเปิดให้ใช้งานอยู่

ซึ่งความสัมพันธ์ในแต่ละตารางและเอ็นทิตี้สามารถเขียนเป็นอีอาร์ไดอะแกรมได้ดังรูปที่ 3.18



รูปที่ 3.18 แผนภาพอีอาร์ไดอะแกรมแสดงความสัมพันธ์ในแต่ละตาราง

3.5.1 D1 : ข้อมูลของผู้ใช้งานในระบบ (T_Members) มีรายละเอียดดังนี้

ตารางที่ 3.1 ข้อมูลของผู้ใช้งานในระบบ (T_Members)

Attribute Name	Attribute Type	Description
uid (pk)	bigint	ข้อมูล User ID ใช้ในการอ้างอิงกันในฐานข้อมูล
username	varchar	User name ที่ใช้ในการ Login
password	varchar	รหัสผ่านที่ใช้ในการ Login
accesslevel	varchar	ระดับสิทธิของผู้ใช้งาน
Firstname	varchar	ชื่อจริงของผู้ใช้งาน
Surname	varchar	นามสกุลของผู้ใช้งาน
StudentID	varchar	รหัสนักศึกษา
Faculty	varchar	คณะของผู้ใช้งาน
Email	varchar	อีเมล์
AllowFlag	tinyint	อนุญาตให้ใช้งานหรือไม่

3.5.2 D2 : ข้อมูลของผู้ที่กำลังใช้งานระบบขณะนั้น (T_CurrentLogin) มีรายละเอียดดังนี้

ตารางที่ 3.2 ข้อมูลของผู้ที่กำลังใช้งานระบบขณะนั้น (T_CurrentLogin)

Attribute Name	Attribute Type	Description
TxID (pk)	bigint	ลำดับของทรานเซคชั่น
uid (fk)	bigint	ข้อมูล User ID ใช้ในการอ้างอิงกันในฐานข้อมูล
ip	varchar	ไอพีแอดเดรสที่ได้รับ
LastActive	varchar	เวลาล่าสุดที่ผู้ใช้มารายงานตัว

3.5.3 D3 : ข้อมูลของการเข้าใช้งานในระบบ (T_Accounting)

ตารางที่ 3.3 ข้อมูลของการเข้าใช้งานในระบบ (T_Accounting)

Attribute Name	Attribute Type	Description
LoginPK (pk)	varchar	เก็บข้อมูลเพื่อใช้เป็น Primary key ในตารางนี้
uid (fk)	bigint	ข้อมูล User ID ใช้ในการอ้างอิงกันในฐานข้อมูล
ip	varchar	ไอพีแอดเดรสที่ได้รับ
LoginDate	varchar	วันที่ที่เข้ามาใช้งานระบบ
LoginTime	varchar	ชั่วโมงที่เข้ามาใช้งานระบบ
LogoutDate	varchar	วันที่ที่ออกจากการใช้งานระบบ
LogoutTime	varchar	ชั่วโมงที่ออกจากการใช้งานระบบ

3.5.4 D4 : ข้อมูลสิทธิการเข้าใช้งานระบบของแต่ละยูสเซอร์ (T_Authorize)

ตารางที่ 3.4 ข้อมูลสิทธิการเข้าใช้งานระบบของแต่ละยูสเซอร์ (T_Authorize)

Attribute Name	Attribute Type	Description
Uid (pk)	bigint	ข้อมูล User ID ใช้ในการอ้างอิงกันในฐานข้อมูล
RuleID (pk)	bigint	เลขที่ทรัพยากรในระบบ

3.5.5 D5 : ข้อมูลทรัพยากรในระบบ (T_FWRules)

ตารางที่ 3.5 ข้อมูลทรัพยากรในระบบ (T_FWRules)

Attribute Name	Attribute Type	Description
RuleID (pk)	bigint	เลขที่ทรัพยากรในระบบ
FWRULEPREFIX	varchar	คำสั่งในการเรียกใช้คำสั่ง iptables
DestinationIP	varchar	ไอพีปลายทาง
Protocol	varchar	โปรโตคอล
DestinationPort	varchar	พอร์ตปลายทาง
Action	varchar	การกระทำต่อทรัพยากรนี้
DESC	varchar	คำบรรยาย

บทที่ 4

การพัฒนาระบบงาน

4.1 หลักการพัฒนาระบบ

โครงงานนี้ถูกพัฒนาขึ้นมาเพื่อที่จะทำงานบน *nix ได้ทุกแพลตฟอร์มที่สามารถรองรับการเทคโนโลยีของ PHP และสามารถใช้งานโปรแกรม IPTABLES ได้ เพราะการระบบจะทำการติดต่อสื่อสารกับผู้ใช้เป็นลักษณะของเว็บเบสทั้งหมดและใช้โปรแกรม IPTABLES เป็นโปรแกรมหลักที่ระบบต้องใช้ในการควบคุมการเข้าออกของทราฟฟิกในระบบ ซึ่งการพัฒนาระบบจะแบ่งเป็นสองส่วนใหญ่ๆ คือ

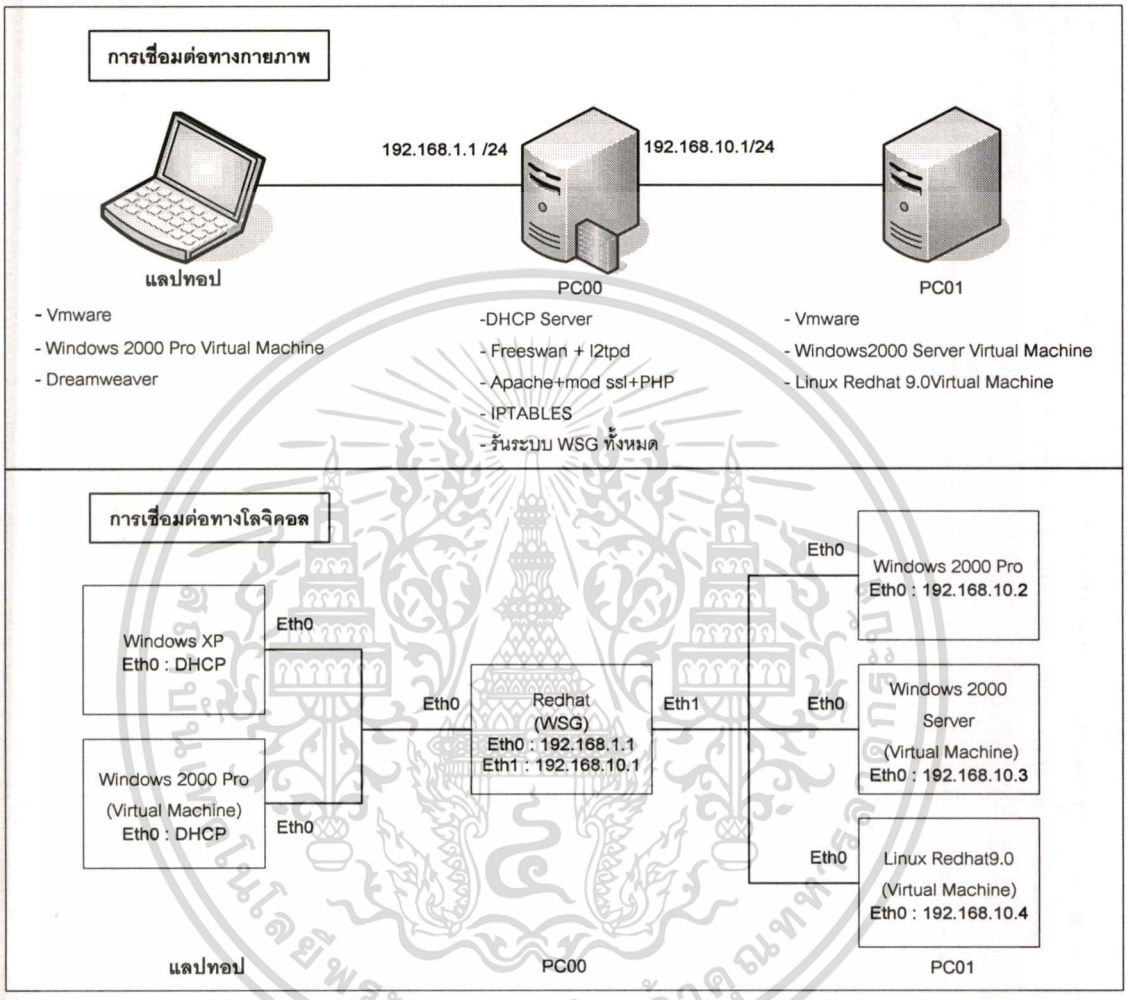
1. ส่วนของผู้ใช้งานระบบ โครงการทำการพัฒนาระบบการลงทะเบียน การเข้าล็อคอิน และการแก้ไขข้อมูลส่วนตัวของผู้ใช้คนนั้น
2. ส่วนของผู้ดูแลระบบ โครงงานทำการพัฒนาส่วนของการเข้าจัดการระบบในส่วนต่างๆ ขึ้นมาเช่น การจัดการผู้ใช้งานในระบบ การจัดการทรัพยากรในระบบ การจัดการการเข้าใช้งานระบบ และ การบันทึกและแสดงข้อมูลการเข้าใช้งานระบบ

หลักการพัฒนาระบบข้อหนึ่งที่ระบบคำนึงถึงได้แก่การรักษาความปลอดภัยในระบบ ทางโครงการได้ทำการออกแบบและพัฒนาการรักษาความปลอดภัยในระบบขึ้นมาคือข้อมูลรหัสผ่านของผู้ใช้งานที่เก็บในฐานข้อมูลระบบจะจัดเก็บไว้ในรูปแบบการเข้ารหัส MD5 ซึ่งทำให้ไม่มีใครสามารถทราบรหัสผ่านตัวนี้ได้แม้กระทั่งผู้ดูแลระบบ ยกเว้นผู้ใช้คนนั้นคนเดียวที่จะทราบซึ่งเป็นการรักษาความเป็นส่วนตัววิธีหนึ่ง นอกจากนั้นระบบงานได้พัฒนาการตรวจสอบการเข้าถึงหน้าเพจบางเพจที่ผู้ดูแลระบบเท่านั้นที่สมควรเข้าถึงได้ โดยทำการตรวจสอบสิทธิของผู้ใช้งานในขณะนั้นว่ามีสิทธิเข้าใช้งานเพจดังกล่าวได้หรือไม่ ถ้าไม่มีสิทธิเข้าใช้งานก็ไม่สามารถเข้าใช้งานเพจนั้นได้ ซึ่งโดยสภาพแวดล้อมและเครื่องมือที่ใช้ในการพัฒนาระบบงานมีดังต่อไปนี้

4.2 ซอฟต์แวร์ที่ใช้งานในระบบ

1. โปรแกรม VMware Workstation ใช้ในการจำลองเครื่องลูกข่ายและเครื่องทรัพยากรของระบบที่เครื่องลูกข่ายต้องการเข้าใช้งานและสร้างสภาพแวดล้อมทั้งหมดที่ใช้ในการพัฒนา
2. ระบบปฏิบัติการ Lixnu Redhat 9.0 Kernel 2.4-18 เป็น Linux Distribution ที่ใช้ในการรองรับการทำงานของระบบทั้งหมด
3. ระบบปฏิบัติการ Windows 2000 Professional และ Windows XP Pro และโปรแกรม VPN Client ที่รวมมากับระบบปฏิบัติการ โดยทำหน้าที่เป็นเครื่องลูกข่ายที่เข้ามาใช้งานระบบ
4. Apache เวอร์ชัน 1.3.33 ทำหน้าที่เป็นเว็บเซิร์ฟเวอร์ซึ่งถูกคอนฟิกให้รองรับการทำงานของ PHP และรองรับการทำงานของโปรโตคอล HTTPS โดยใช้โปรแกรม mod_ssl เวอร์ชัน 2.8.22-1.3.33 และ openssl เวอร์ชัน 0.9.7e เข้ามาช่วย
5. ภาษาที่ใช้ในการพัฒนาเว็บเพจคือ HTML และเลือกใช้ PHP เวอร์ชัน 4.3.10 เป็นภาษาสคริปต์ที่ทำงานในฝั่งเซิร์ฟเวอร์ ที่เลือกใช้ภาษา PHP เนื่องจาก Apache เว็บเซิร์ฟเวอร์สามารถทำงานรองรับการทำงานของภาษานี้ได้เป็นอย่างดี อีกทั้งเป็นภาษาที่ง่ายและมีประสิทธิภาพเพียงพอกับการพัฒนาระบบนี้
6. โปรแกรม MySQL เวอร์ชัน 3.23.55-1 ใช้เป็นโปรแกรมฐานข้อมูลที่ใช้จัดเก็บข้อมูลทุกอย่างในระบบ แต่เนื่องจากว่าการอินเทอร์เฟสกับผู้ใช้งานเป็นลักษณะของเท็กซ์โหมดซึ่งไม่ค่อยสะดวกในการใช้งาน ดังนั้นจึงใช้โปรแกรม phpMyAdmin เวอร์ชัน 2.6.1ซึ่งเป็นโปรแกรมเว็บเบสซึ่งสามารถเข้าไปควบคุมการใช้งาน MySQL ได้ในกราฟฟิกโหมด
7. Macromedia Dreamweaver MX 2004 เป็นโปรแกรมที่ใช้ในการช่วยในเรื่องของการเขียนโปรแกรมให้มีความสะดวกง่ายดายขึ้น รวมถึงออกแบบหน้าตาเว็บเพจได้สะดวกขึ้น
8. IPTABLES เป็นโปรแกรมไฟร์วอลล์ประเภท Stateful Inspection ซึ่งโปรแกรมที่พัฒนาขึ้นมาใหม่จะเรียกโปรแกรมนี้ใช้งานเพื่อช่วยในส่วนของการควบคุมการเข้าออกของทราฟฟิกในระบบ

4.3 ฮาร์ดแวร์ที่ใช้งานในระบบและรูปแบบจำลองการเชื่อมต่อ



รูปที่ 4.1แสดงการเชื่อมต่อทางกายภาพและโลจิคอลของเครือข่ายที่ใช้พัฒนา

การจำลองการเชื่อมต่อจะใช้สายแลนเป็นสื่อทั้งหมดซึ่งรายละเอียดการเชื่อมต่อเป็นดังรูปที่ 4.1 และหน้าที่ของแต่ละเครื่องมีดังนี้

1. แลปทอป IBM R31 CPU Pentium III 1 GHz RAM 384 MB 1 LAN Card ใช้ในการพัฒนาโปรแกรม และทำหน้าที่เป็นลูกข่ายเพื่อทดสอบการใช้งานของระบบ
2. เครื่องคอมพิวเตอร์ CPU AMD 300 MHz RAM 128 MB 2 LAN Cards เป็นเครื่องที่ใช้ในการรันโปรแกรมที่ใช้ในระบบ และโปรแกรมในส่วนที่พัฒนาเพิ่มขึ้นมาทั้งหมด

3. เครื่องคอมพิวเตอร์ CPU INTEL 500 MHz RAM 256 MB 1 LAN Card ใช้เป็นเครื่องที่จำลองทรัพยากรที่เปิดให้บริการของระบบ

4.4 การติดตั้งและปรับแต่งสภาพแวดล้อมที่ต้องใช้ในระบบ

เตรียมสภาพแวดล้อมในการทำงานโดยการเตรียมลงระบบปฏิบัติการ รวมไปถึงโปรแกรมต่างๆ และปรับแต่งค่าของโปรแกรมเหล่านั้น เพื่อให้รองรับการทำงานของระบบใหม่ที่พัฒนาขึ้นมา โดยที่รายละเอียดการติดตั้งระบบปฏิบัติการรวมไปถึงการติดตั้งเวบเซิร์ฟเวอร์เพื่อให้รองรับฐานข้อมูล MySQL และโปรโตคอล HTTPS จะอยู่ในภาคผนวก ก. ส่วนรายละเอียดในส่วนอื่นมีดังนี้

4.4.1 สร้างไฟร์วอลล์สริปต์ซึ่งเป็นสริปต์เริ่มต้นที่ใช้ทุกครั้งเมื่อมีการรีบูตระบบ

สคริปที่สร้างมีชื่อว่า initialfwrules และจะกำหนดให้ระบบมีค่าเริ่มต้นดังนี้

1. Policy ใน Chain Forward มีค่าเป็น DROP ทั้งหมด เพื่อทำการ drop ทุก packet ที่พยายามเข้ามาในระบบเครือข่ายที่ให้บริการ

```
/sbin/iptables -P FORWARD DROP
```

2. กำหนดให้อนุญาต packet ที่เคยผ่านเข้ามาแล้วหรือที่เกี่ยวข้องกันสามารถผ่านเข้าออกได้โดยไม่ต้องเพิ่มรูลใหม่

```
/sbin/iptables -A FORWARD -m state --state ESTABLISH,RELATED -j ACCEPT
```

เมื่อสร้างสริปต์นี้เสร็จแล้วก็ไปกำหนดให้รันสคริปต์นี้ทุกครั้งที่รีบูตระบบ โดยใส่พาทของสริปต์นี้ในท้ายสุดของไฟล์ \etc\rc.d\rc.local

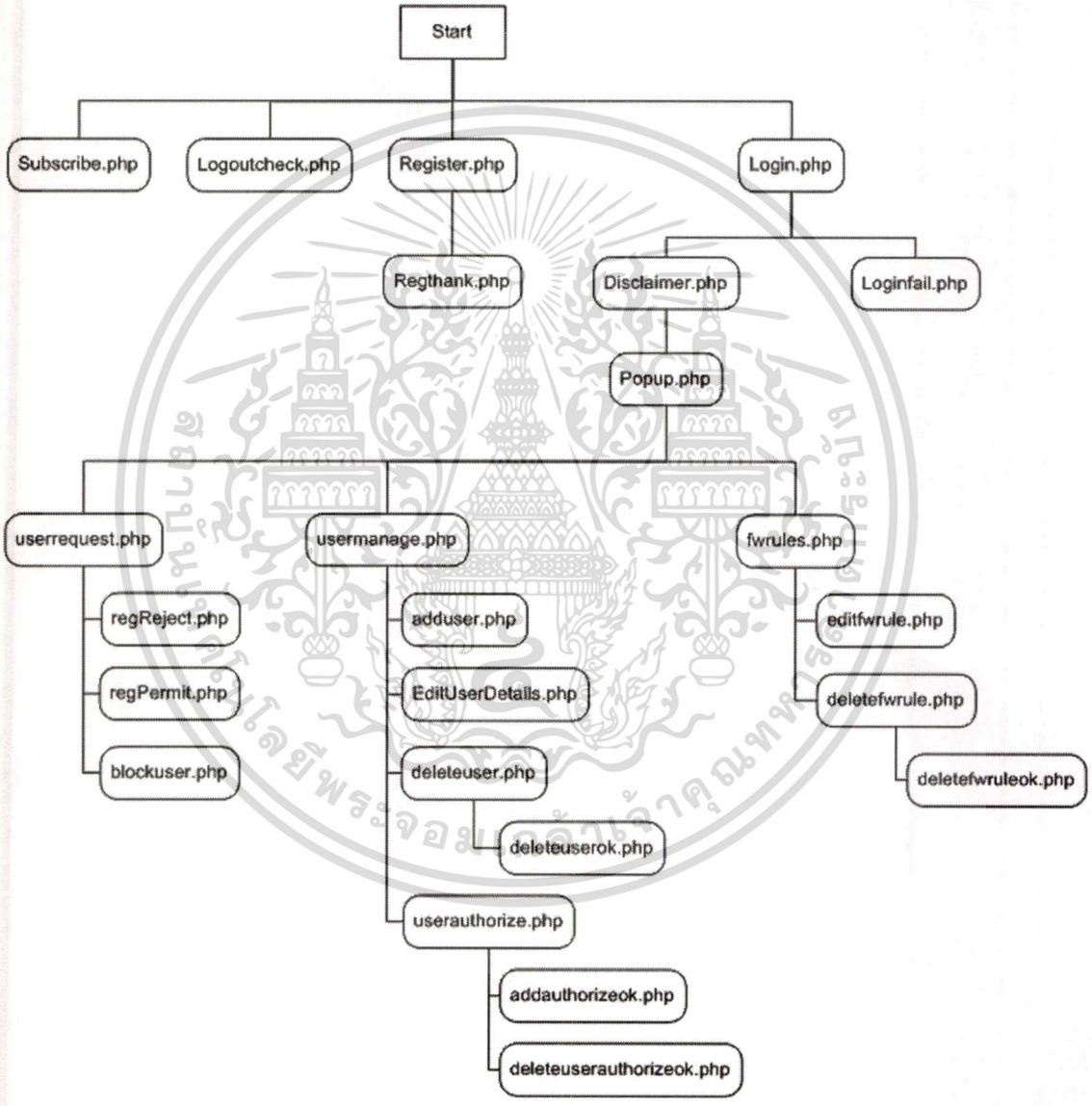
4.4.2 กำหนดให้ระบบมีการเข้าไปตรวจข้อมูลในตาราง T_CurrentLogin

ทำการกำหนดให้ระบบเข้าไปตรวจข้อมูลในตาราง T_CurrentLogin โดยใช้โปรแกรม Crontab ตั้งเวลาเรียกเพจ logoutcheck.php ทุกๆ 1 นาทีโดยเพจนี้จะเข้าไปตรวจสอบว่ามีผู้ใช้คนไหนไม่มีการใช้งานระบบโดยเกินเวลาที่กำหนดไว้แล้ว ก็จะทำการ logout ผู้ใช้คนนั้นออกจากระบบ โดยคำสั่งที่ใช้ในการกำหนดโปรแกรม Crontab มีดังนี้

```
*/1 * * * *  /usr/local/bin/lynx -dump http://192.168.1.1/wsg/logoutcheck.php
```

4.5 การพัฒนาโปรแกรม

ในส่วนนี้เป็นรายละเอียดของการทำงานของโปรแกรมในส่วนต่างๆ ซึ่งโปรแกรมที่พัฒนาขึ้นมาใหม่นั้นมีจำนวน 5 โมดูลย่อย ซึ่งบางโมดูลจะมีการส่งข้อมูลไปมาหากันโดยสามารถอ้างอิงได้จากการไหลของข้อมูลในระดับต่างๆ ดังที่ได้อธิบายในบทที่ 3 ซึ่งรายละเอียดโครงสร้างของโปรแกรมจะมีดังนี้



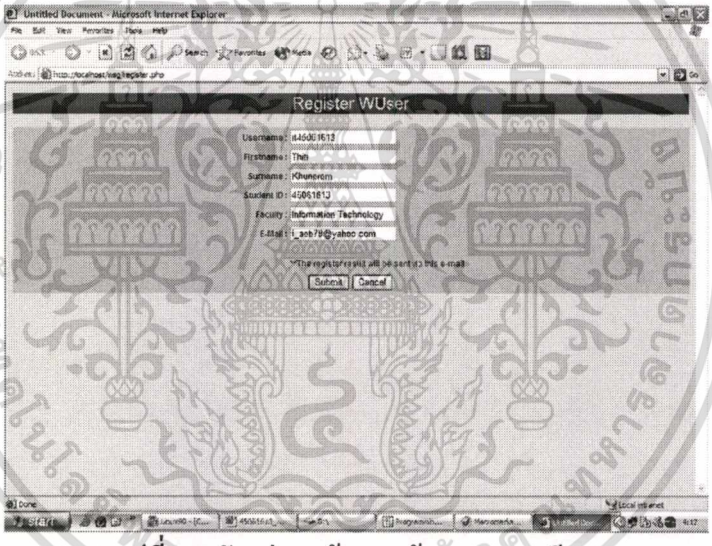
รูปที่ 4.2 แสดงโครงสร้างและความสัมพันธ์ของหน้าเพจต่างๆ

รายละเอียดการทำงานของแต่ละหน้าเพจมีดังนี้

1. ไฟล์ Subscribe.php เป็นเพจที่ใช้ในการรับการเข้ารายงานตัวจากเครื่องลูกข่าย โดยเครื่องลูกข่ายจะส่งรหัสยูสเซอร์ และเวลา ณ.ขณะนั้นมา update ทุกๆ 10 วินาที และเมื่อรับข้อมูลเหล่านั้นมาแล้วก็ทำการบันทึกลงในฐานข้อมูล ในตาราง T_CurrentLogin ต่อไป

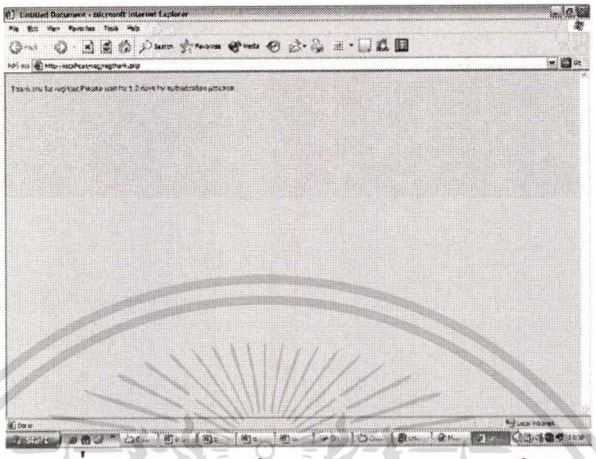
2. ไฟล์ LogoutCheck.php เป็นไฟล์ที่ถูกเรียกใช้โดยระบบทุกๆ 1 นาที ซึ่งไฟล์นี้จะทำการตรวจว่ามีผู้ใช้งานคนใดออกจากระบบโดยไม่ได้ทำการlogoutบ้างโดยจะเทียบข้อมูลเวลาที่ผู้ใช้ update มาในตารางT_CurrentLogin กับเวลาจริงในขณะนั้นว่าห่างกันเกินช่วงเวลาที่ตั้งไว้แล้วหรือยัง ถ้าเกินเวลาที่กำหนดไว้แล้ว ระบบก็จะทำการ logout ผู้ใช้คนนั้นออกจากระบบโดยอัตโนมัติ

3. ไฟล์ register.php เป็นเพจการเข้าลงทะเบียนขอเข้าใช้งานระบบ เมื่อทำการยืนยันข้อมูลแล้วระบบจะบันทึกลงตาราง T_Members



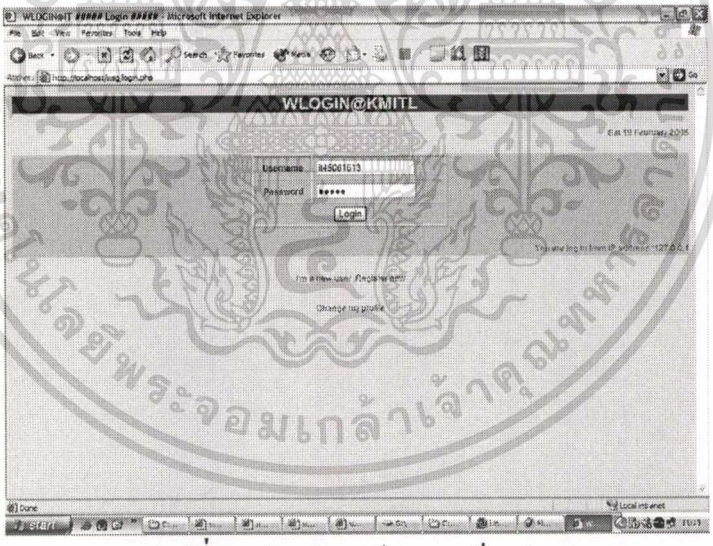
รูปที่ 4.3 ตัวอย่างหน้าจอหน้าการลงทะเบียน

4. ไฟล์ regthank.php เป็นการขอบคุณที่สนใจเข้ามาใช้งานระบบ และแจ้งบอกให้รอผลการลงทะเบียนที่จะส่งผ่านทางอีเมล์ออกไป



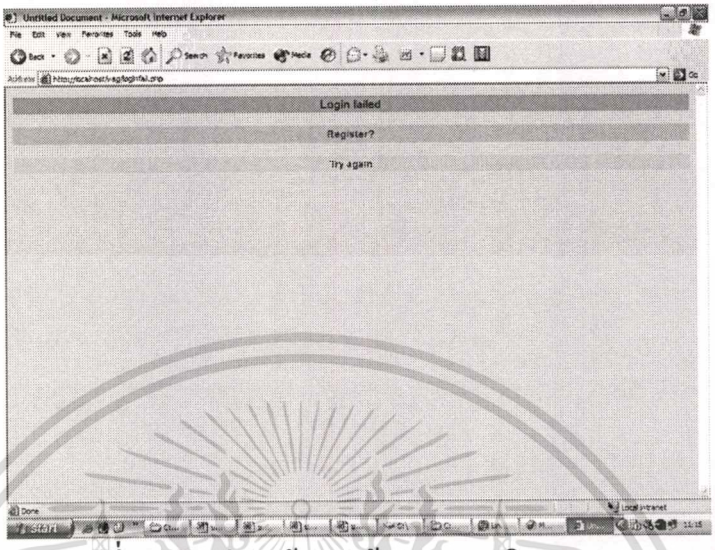
รูปที่ 4.4 ตัวอย่างหน้าจอหลังจากการลงทะเบียน

5. ไฟล์ login.php หน้าเพจที่ใช้ในการล็อคอินเข้าสู่ระบบ



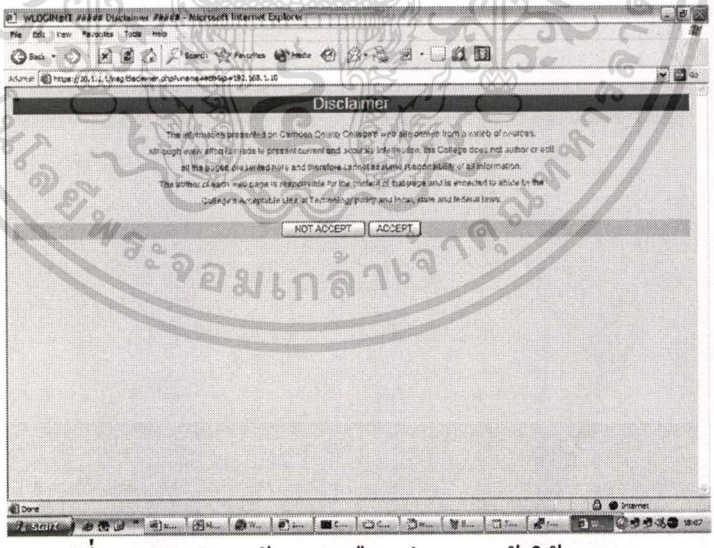
รูปที่ 4.5 ตัวอย่างหน้าจอการล็อคอิน

6. ไฟล์ loginfail.php เป็นการแจ้งเตือนผลการพิสูจน์ตัวจริงว่ามีการผิดพลาดเกิดขึ้น



รูปที่ 4.6 ตัวอย่างหน้าจอหน้าการ login ผิดพลาด

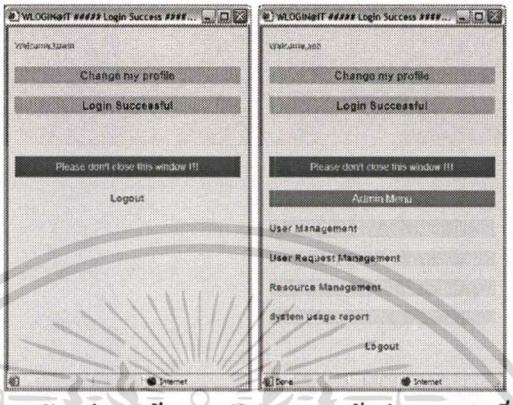
7. ไฟล์ disclaimer.php เป็นการแจ้งบอกระเบียบการเข้าใช้งานระบบซึ่งผู้ใช้งานจะต้องยอมรับระเบียบการใช้งานเท่านั้นถึงจะสามารถเข้าใช้งานระบบได้



รูปที่ 4.7 ตัวอย่างหน้าจอคำเตือนก่อนการเข้าใช้ระบบ

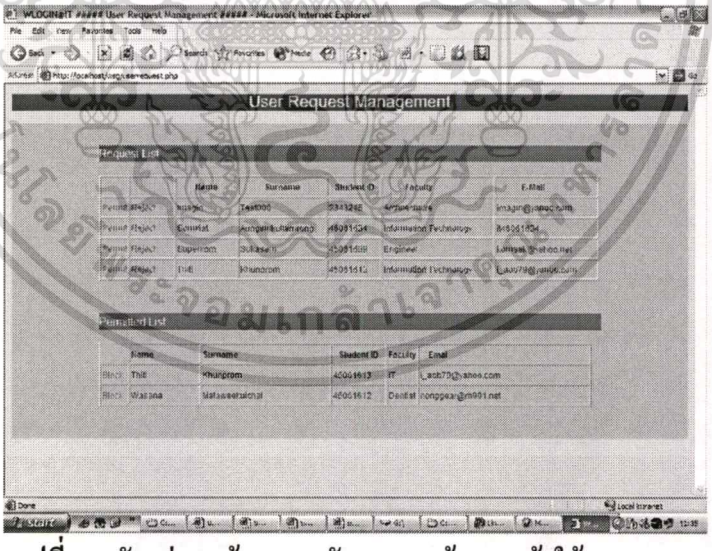
8. ไฟล์ pop.php เป็นการแจ้งบอกผู้ใช้งานว่าตอนนี้สามารถเข้าใช้ระบบได้แล้ว โดยในเพจนี้ผู้ใช้สามารถทำการเปลี่ยนพาสเวิร์ดได้ และถ้าหากผู้ใช้มีสิทธิเป็นผู้ดูแลระบบ ผู้ใช้ก็จะสามารถเข้าถึงหน้าเพจการจัดการระบบในส่วนต่างๆได้โดยผ่านระบบนี้ ซึ่งในไฟล์นี้จะมีสคริปต์การ

ตรวจสอบว่าผู้ใช้คนนี้มีสิทธิเข้าใช้ระบบส่วนใดบ้างโดยทำการตรวจดูที่ตาราง T_Authorize จากนั้นจะทำนำข้อมูลเหล่านั้นรวมกับข้อมูลไอพีของผู้ใช้งานที่ล็อคอินเข้ามา สร้างเป็นไฟร์วอลล์สคริปต์ และทำการรันสคริปต์นั้นเพื่อเปิดให้บริการกับผู้ใช้คนนั้น



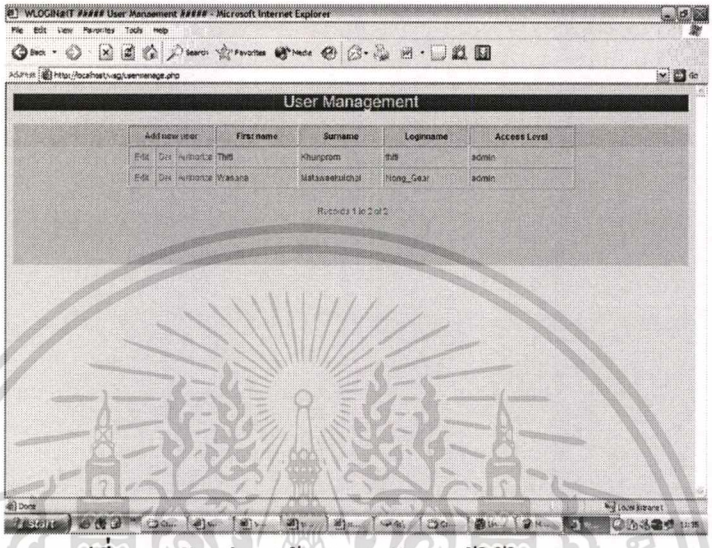
รูปที่ 4.8 ตัวอย่างหน้าจอหลังจากการเข้าสู่ระบบสำเร็จ

9. ไฟล์ userrequets.php ใช้สำหรับผู้ดูแลระบบจัดการเรื่องคำขอการเข้าใช้งานระบบ ซึ่งผู้ดูแลระบบสามารถจะอนุญาต หรือปฏิเสธการเขาใช้งานได้จากเพจนี้ รวมไปถึงสามารถยกเลิกการใช้งานชั่วคราวของผู้ใช้งานที่ได้รับอนุญาตแล้ว ได้ทางเพจนี้เช่นกัน



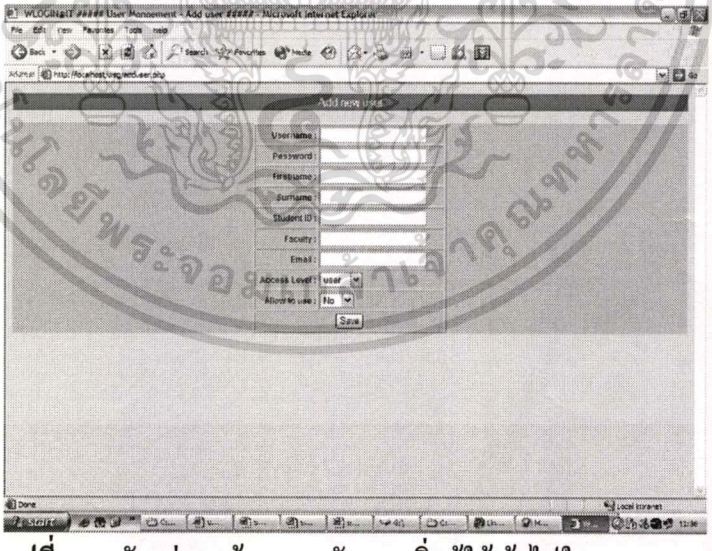
รูปที่ 4.9 ตัวอย่างหน้าจอการจัดการการร้องขอเข้าใช้ระบบ

10. ไฟล์ usermanage.php เป็นเพจสำหรับผู้ดูแลระบบใช้จัดการเกี่ยวกับผู้ใช้ทั้งหมดกล่าวคือ สามารถเพิ่ม ลบ แก้ไขข้อมูลของผู้ใช้ได้ รวมไปถึงการกำหนดสิทธิของผู้ใช้ว่าสามารถใช้งานอะไรในระบบได้บ้าง



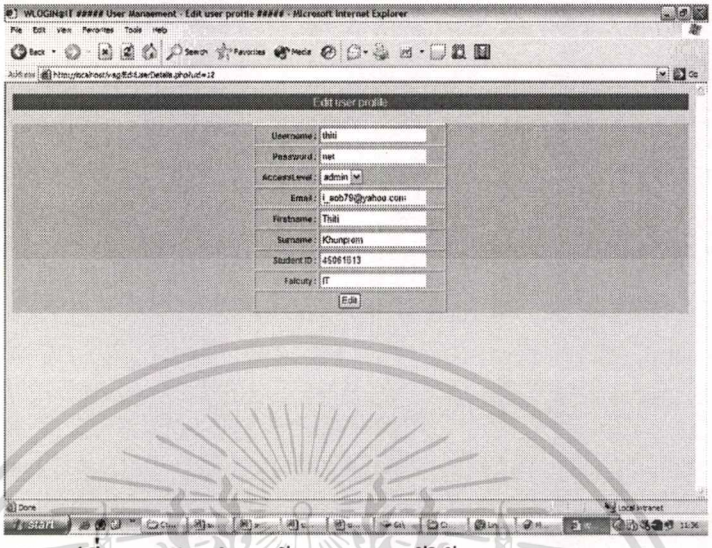
รูปที่ 4.10 ตัวอย่างหน้าจอการจัดการผู้ใช้ในระบบ

11. ไฟล์ adduser.php ใช้ในการเพิ่มผู้ใช่งานในระบบ



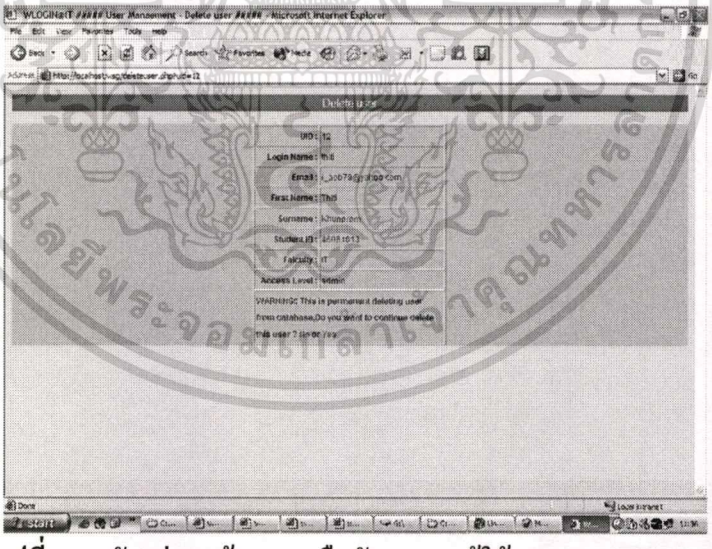
รูปที่ 4.11 ตัวอย่างหน้าจอการจัดการเพิ่มผู้ใช้เข้าไปในระบบ

12. ไฟล์ edituserdetail ใช้แก้ไขข้อมูลผู้ใช้ในระบบ



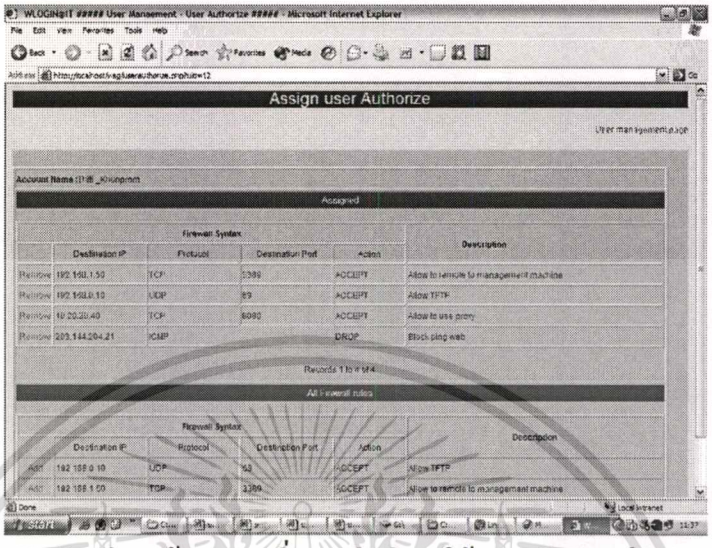
รูปที่ 4.12 ตัวอย่างหน้าจอการลบผู้ใช้ออกจากระบบ

13. ไฟล์ deleteuser.php ใช้ลบผู้ใช้งานในระบบ โดยมีการเรียกสคริปต์ในไฟล์ deletefwruleok.php หลังจากได้รับการยืนยันการลบแล้ว



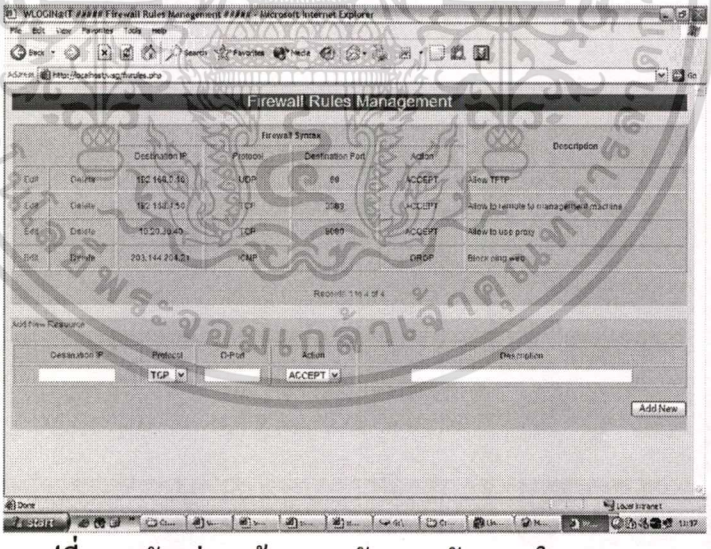
รูปที่ 4.13 ตัวอย่างหน้าจอการยืนยันการลบผู้ใช้ออกจากระบบ

14. ไฟล์ userauthorize.php ใช้ในการเพิ่มลดสิทธิการเข้าใช้งานระบบของแต่ละยูสเซอร์



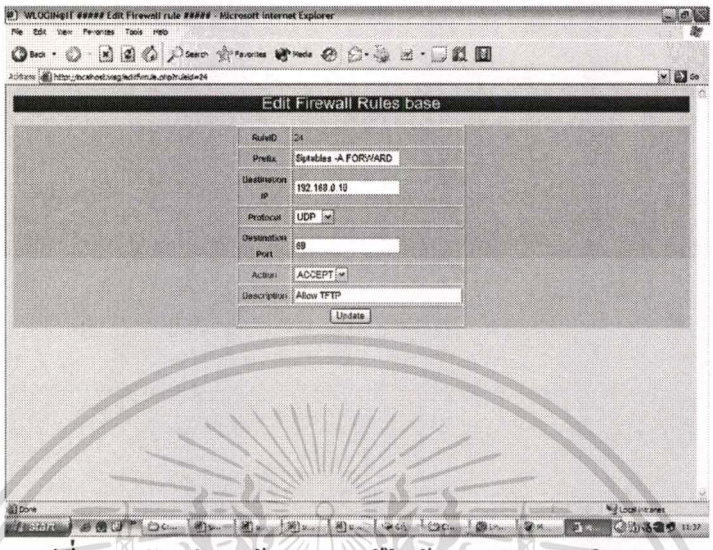
รูปที่ 4.14 ตัวอย่างหน้าจอการเพิ่ม ลดสิทธิการใช้งานทรัพยากรในระบบ

15. ไฟล์ fwrule.php ใช้ในการจัดการทรัพยากรในระบบว่ามีอะไรบ้างและสามารถใช้อะไรได้บ้าง ในเพจนี้ผู้ดูแลระบบสามารถเพิ่ม ลบ แก้ไขข้อมูลทรัพยากรในระบบได้



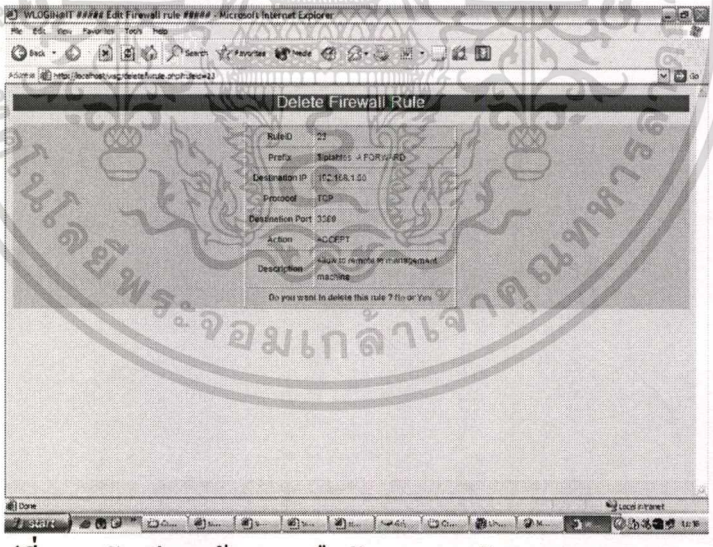
รูปที่ 4.15 ตัวอย่างหน้าจอการจัดการทรัพยากรในระบบ

16. ไฟล์ editfwrule.php ใช้ในการแก้ไขข้อมูลทรัพยากรในระบบ



รูปที่ 4.16 ตัวอย่างหน้าจอการแก้ไขข้อมูลทรัพยากรในระบบ

17. ไฟล์ deletefwrule.php ใช้ในการลบข้อมูลทรัพยากรในระบบโดยมีการเรียกสคริปต์ในไฟล์ deletefwruleok.php หลังจากได้รับการยืนยันการลบแล้ว



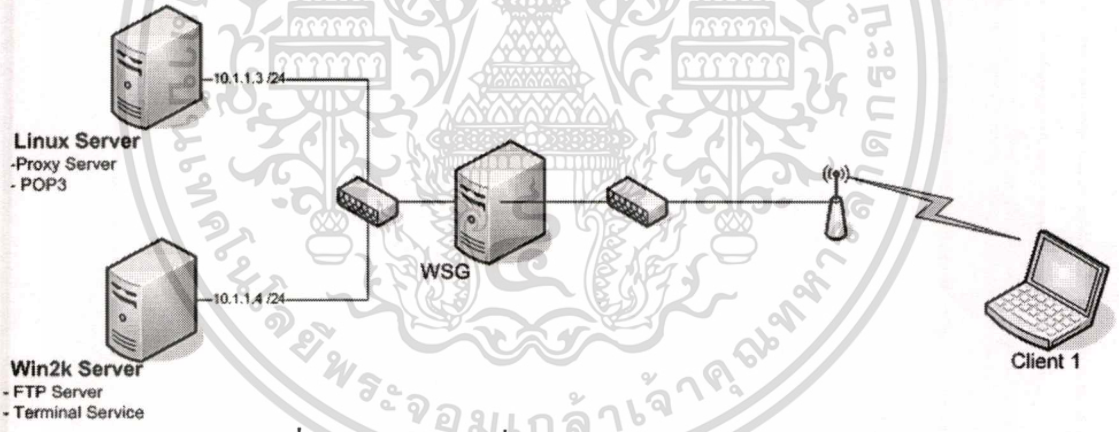
รูปที่ 4.17 ตัวอย่างหน้าจอการยืนยันการบลทรัพยากรออกจากระบบ

บทที่ 5
การทดสอบการใช้งานระบบ

การทดสอบการใช้งานระบบจะอ้างอิงอิงขั้นตอนการทำงานของระบบที่ได้กล่าวมาแล้วในหัวข้อที่ 3.2 โดยจุดประสงค์การทดสอบระบบจะทำการเปรียบเทียบระหว่างเหตุการณ์ก่อนที่ผู้ใช้จะทำการล็อคอินเข้าสู่ระบบและหลังจากที่ผู้ใช้ได้ผ่านเข้ามาใช้งานในระบบรวมถึงความสามารถต่างๆ ของระบบ

5.1 รูปแบบการเชื่อมต่อที่ใช้ในการทดสอบ

การเชื่อมต่อระบบจะทำการเชื่อมต่อในลักษณะเดียวกับที่ได้ออกแบบไว้คือนำเครื่องที่เป็นโครงงาน(WSG) มาวางคั่นระหว่างเน็ตเวิร์คเครือข่ายไร้สาย กับเครือข่ายที่ให้บริการ (10.1.1.0/24) โดยที่เครื่องลูกข่ายจะทำการรับค่าเน็ตเวิร์คมาจาก DHCP ที่ทำงานบนเครื่อง WSG ดังรูปที่ 5.1

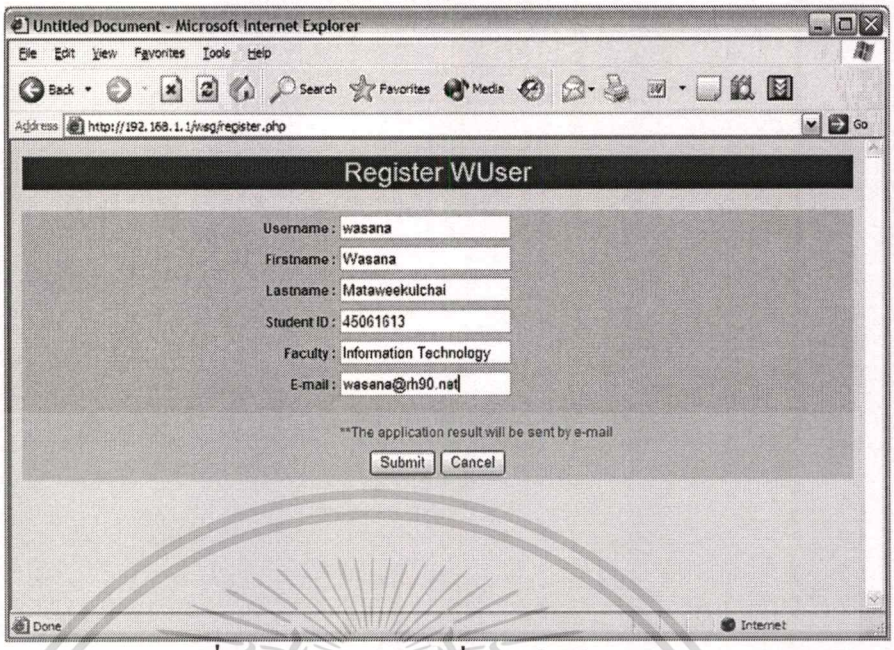


รูปที่ 5.1 รูปแบบการเชื่อมต่อขณะทำการทดสอบระบบ

5.2 การทดสอบระบบ

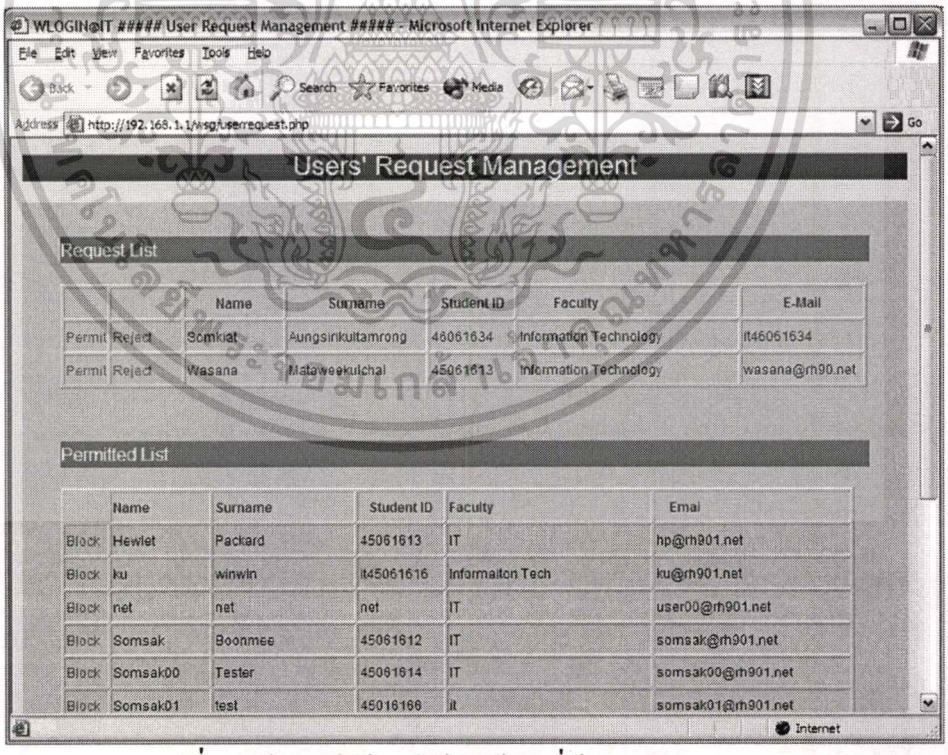
ความสามารถการทำงานของระบบนี้มีทั้งในด้านของผู้ดูแลระบบและด้านของผู้ใช้งานระบบ ซึ่งในมุมของผู้ดูแลระบบนั้นจะเป็นการควบคุมและจัดการระบบเสียส่วนใหญ่ดังนั้นในบทนี้จะไม่ทำการทดสอบในส่วนนี้แต่สามารถดูรายระเอียดการใช้งานระบบได้ในคู่มือการใช้งานระบบในภาคผนวก ดังนั้นในส่วนนี้จะเป็นการทดสอบในด้านของผู้ใช้งานซึ่งมีรายละเอียดดังนี้

1. ผู้ใช้งานสามารถทำการลงทะเบียนเพื่อขอใช้งานระบบและได้รับรหัสผ่านเข้าใช้งานผ่านทางอีเมล์ได้ โดยเริ่มจากผู้ใช้งานเข้าทำการลงทะเบียนเพื่อขอเข้าใช้ระบบดังรูปที่ 5.2



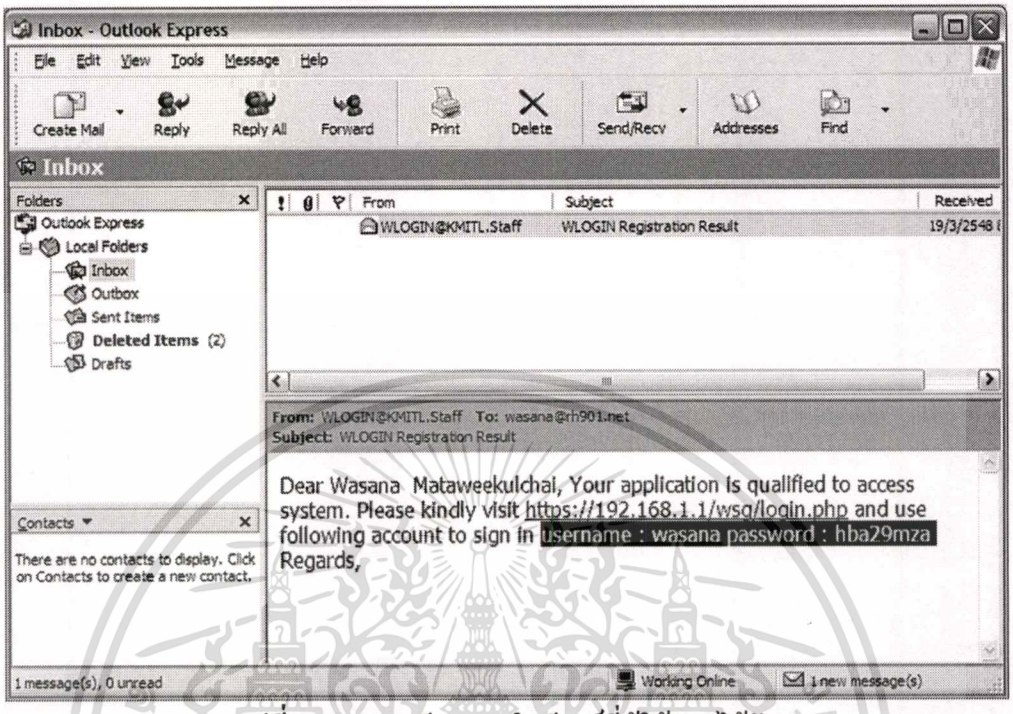
รูปที่ 5.2 การลงทะเบียนเพื่อขอเข้าใช้งาน

จากนั้นข้อมูลจะถูกส่งไปที่ผู้ดูแลระบบจากนั้นผู้ดูแลระบบจะทำการอนุญาตให้ผู้ใช้เข้ามาใช้งานระบบได้ดังรูปที่ 5.3



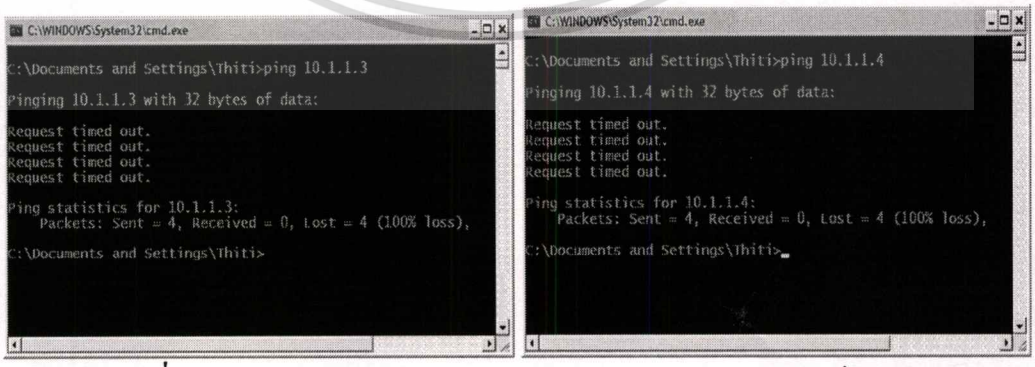
รูปที่ 5.3 ข้อมูลผู้ใช้งานได้ส่งเข้ามาที่ผู้ดูแลระบบ

ผู้ใช้งานทำการตรวจสอบผลการร้องขอผ่านทางอีเมล์ โดยจะมีรายละเอียดที่ต้องใช้ในการล็อคอิน คือชื่อการเข้าใช้งานและรหัสผ่านดังรูปที่ 5.4

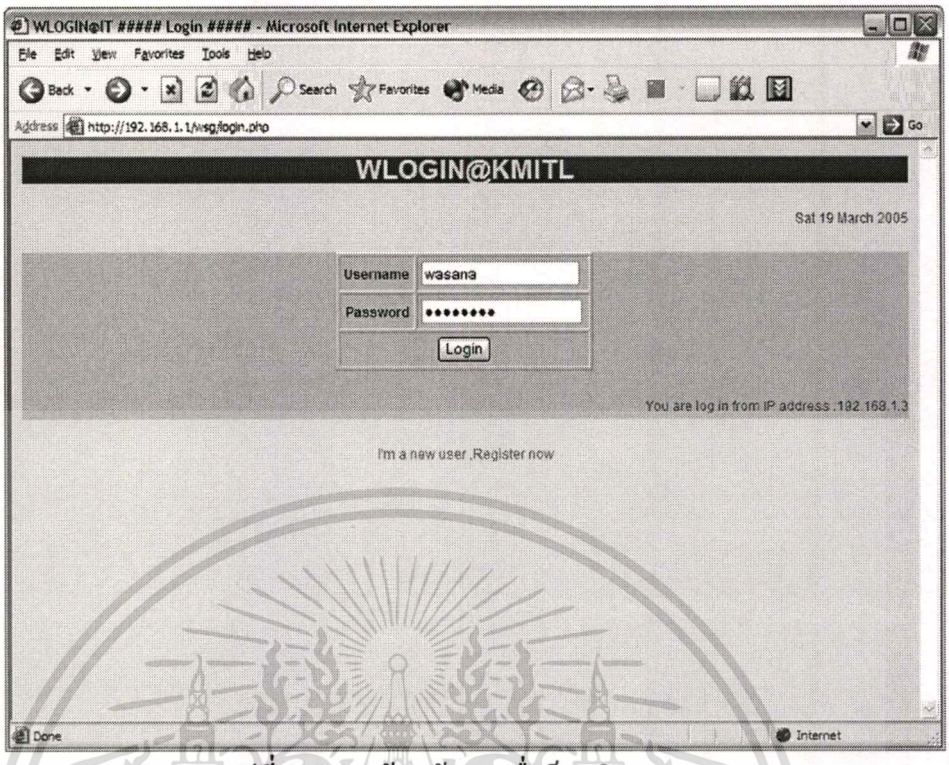


รูปที่ 5.4 รายละเอียดภายในอีเมล์ที่ผู้ใช้งานได้รับ

2. ทดสอบการเข้าใช้งานระบบโดยใช้ข้อมูลที่ได้รับจากอีเมล์ โดยผู้ใช้งานเข้าหน้าเพจการล็อคอินและทำการกรอกรหัสผ่านและชื่อผู้ใช้งานลงในเพจนี้ดังรูปที่ 5.6 เมื่อผู้ใช้งานผ่านการพิสูจน์ตนเองแล้วจะสามารถเข้าใช้งานระบบได้ โดยในการทดสอบนี้จะให้ผู้ใช้คนนี้สามารถทำการ Ping ไอพี 10.1.1.3 ได้เท่านั้น ไม่สามารถ Ping ไอพี 10.1.1.4 ได้ โดยในรูปที่ 5.5 จะแสดงการ Ping ไอพี 10.1.1.3 ขณะก่อนที่ทำการล็อคอินซึ่งจะไม่สามารถ Ping ได้

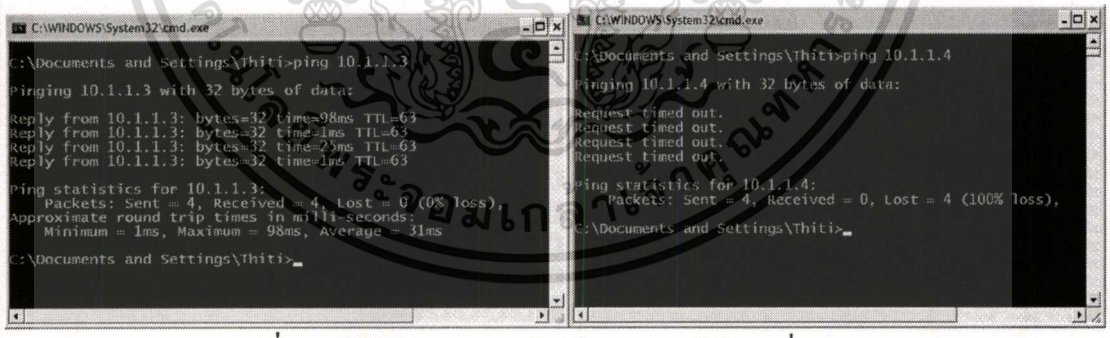


รูปที่ 5.5 รูปการ Ping IP 10.1.1.3 และ 10.1.1.4 ขณะก่อนทำการล็อคอิน



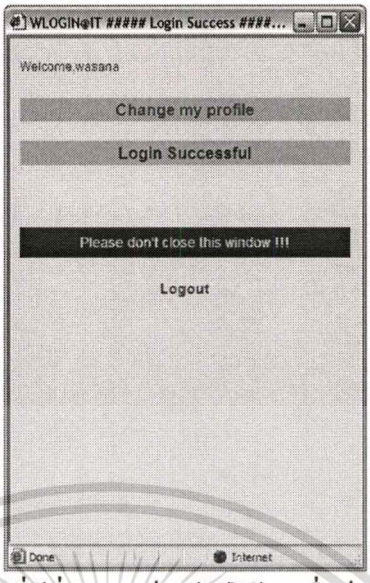
รูปที่ 5.6 การเข้าหน้าเพจเพื่อล็อคอิน

เมื่อทำการพิสูจน์ตนเองผ่านแล้วทำการลอง Ping ไอพี 10.1.1.3 จะพบว่าเมื่อผ่านการพิสูจน์ตนเองแล้วก็สามารถเข้าใช้งานระบบได้ตามที่ผู้ดูแลระบบกำหนดให้ได้ดังรูปที่ 5.7 คือสามารถ Ping 10.1.1.3 ได้แต่ไม่สามารถ Ping ไปที่ไอพี 10.1.1.4 ได้



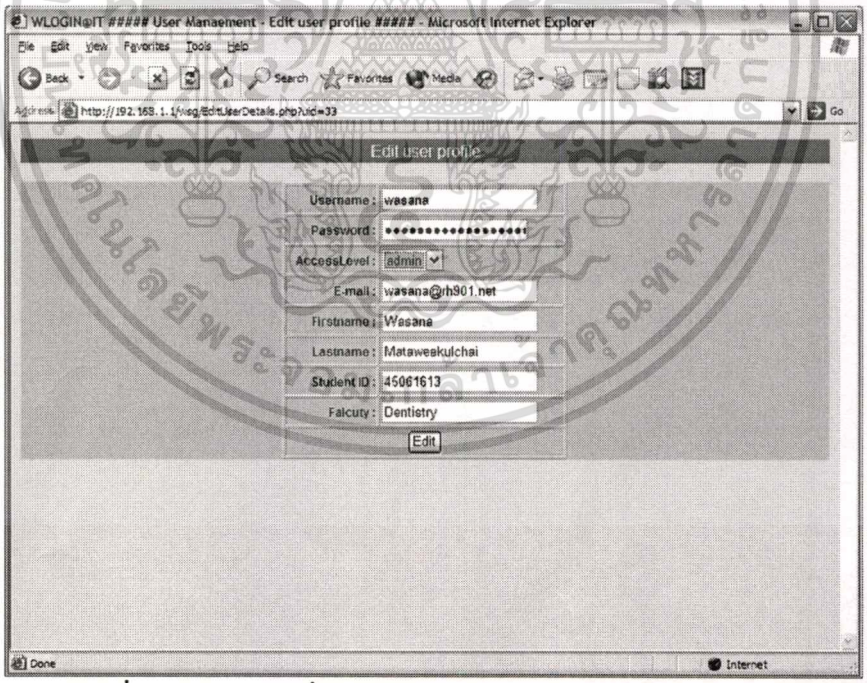
รูปที่ 5.6 ผู้ใช้งานสามารถเข้าใช้งานระบบได้ตามที่กำหนด

3. ทำการทดสอบการเข้าถึงเมนูการควบคุมดูแลระบบโดยจะทำการล็อคอินโดยใช้สิทธิเป็นผู้ใช้ หน้าเพจที่ได้จะไม่แสดงเมนูการเข้าถึงเมนูการควบคุมดูแลระบบได้ ดังรูปที่ 5.7 ผู้ใช้ Wasana มีสิทธิเป็นผู้ใช้งานดังนั้นเมื่อล็อคอินสำเร็จแล้วจะได้หน้าเพจที่ไม่แสดงเมนูการควบคุมดูแลระบบ

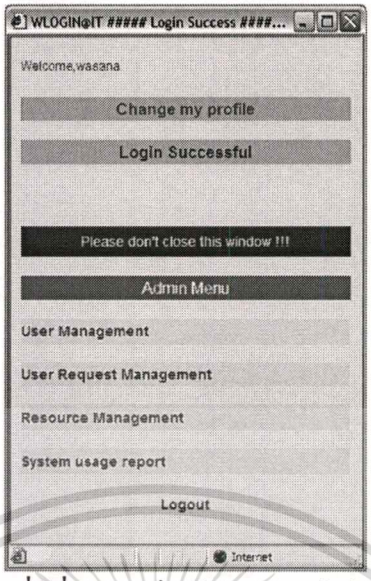


รูปที่ 5.7 หน้าจอเพจที่ผู้ที่มีสิทธิเป็นผู้ใช้ได้รับเมื่อล็อคอินสำเร็จ

ต่อไปจะทำการเพิ่มสิทธิของ Wasana ให้มีสิทธิเป็นผู้ดูแลระบบดังรูปที่ 5.8 และทำการล็อคอินเข้าระบบอีกครั้งก็จะได้เพจที่แสดงเมนูที่สามารถเข้าควบคุมระบบได้ดังแสดงในรูปที่ 5.9

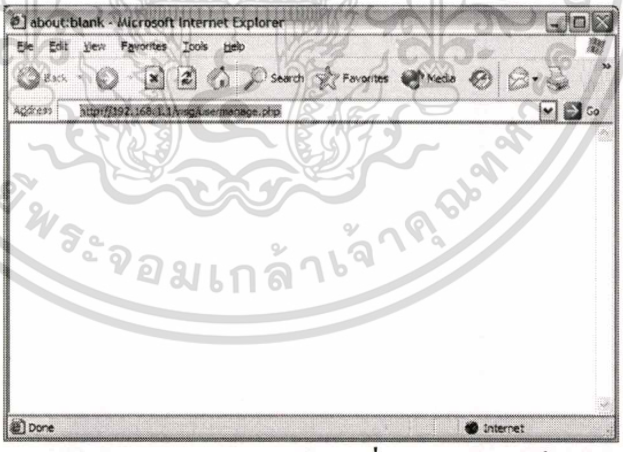


รูปที่ 5.8 แสดงการเพิ่มสิทธิผู้ใช้งานจากผู้ใช้ไปเป็นผู้ดูแลระบบ



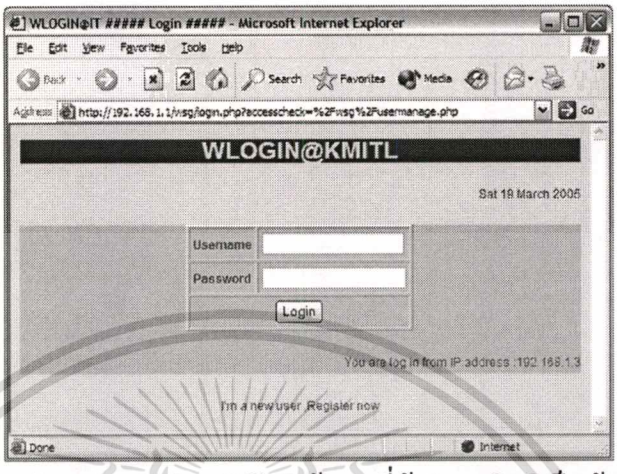
รูปที่ 5.9 หน้าจอเพจที่ผู้ที่มีสิทธิเป็นผู้ดูแลระบบได้รับเมื่อล็อคอินสำเร็จ

3. ทดสอบเข้าถึงเพจที่จำกัดไว้เฉพาะผู้ใช้ที่มีสิทธิเป็นผู้ดูแลระบบนั้นจึงจะสามารถเข้าใช้งานระบบได้ ถ้าผู้ใช้คนนั้นไม่มีสิทธิจะถูกพาไปหน้าล็อคอินใหม่ ดังรูปที่ 5.10 จะทดสอบให้ผู้ใช้ที่มีสิทธิเป็นผู้ใช้พยายามเข้าหน้าเพจ https://192.168.1.1/wsg/usermanage.php ซึ่งเพจนี้อนุญาตให้ผู้ใช้ที่มีสิธิเป็นผู้ดูแลระบบเท่านั้นที่เข้าถึงได้



รูปที่ 5.10 แสดงการทดลองเปิดหน้าเพจที่ต้องการสิทธิเป็นผู้ดูแลระบบ

ระบบจะทำการตรวจสอบสิทธิการเข้าใช้งาน และพบว่าเป็นการเปิดโดยที่ไม่มีสิทธิเป็นผู้ดูแลระบบ จึงทำการเปิดไปหน้าล็อคอินแทน ดังรูปที่ 5.11



รูปที่ 5.11 แสดงผลการทดลองเปิดหน้าเพจที่ต้องการสิทธิเป็นผู้ดูแลระบบ

บทที่ 6

สรุปผลการพัฒนาระบบและข้อเสนอแนะ

เนื้อหาในบทนี้เป็นการสรุปผลการพัฒนาระบบงานผลการทดสอบการใช้งานรวมถึงข้อเสนอแนะ และแนวทางในการพัฒนาระบบงานต่อไป

6.1 สรุปผลการทดสอบระบบงาน

จากการทดสอบใช้ระบบงานระบบสามารถเพิ่มการรักษาความปลอดภัยบนเครือข่ายไร้สายได้ตามที่ได้ตามจุดประสงค์ที่ต้องการกล่าวคือ

1. ระบบมีการพิสูจน์ตนเองที่ดีขึ้นและปลอดภัยขึ้นเพราะเพิ่มขั้นตอนการพิสูจน์ตนเองจะมีการตรวจสอบใช้ยูสเซอร์เนมและรหัสผ่านก่อนที่จะสามารถเข้ามาใช้งานระบบได้และกระบวนการการพิสูจน์ตนเองนั้นถูกทำบนโปรโตคอล HTTPS ซึ่งทำให้มีความปลอดภัยมากขึ้นในขั้นตอนของการsign in
2. ระบบสามารถทำการจำกัดสิทธิการเข้าใช้งานระบบในระดับยูสเซอร์ เป็นการเพิ่มความปลอดภัยให้กับระบบที่ให้บริการมากยิ่งขึ้น
3. มีระบบการเก็บประวัติการเข้าใช้งานระบบทำให้เมื่อระบบมีปัญหาก็สามารถนำข้อมูลนี้มาเป็นส่วนประกอบในการแก้ไขปัญหาได้

แม้การทำงานของระบบโดยรวมจะมีความคล้ายคลึงกับโปรแกรมที่มีเผยแพร่ทางอินเทอเน็ตอยู่แล้วคือโปรแกรม ChilliSpot และโปรแกรม NoCat แต่โครงงานนี้ได้พัฒนาเพิ่มความสามารถในหลายๆด้านที่ซึ่งสามรถช่วยในการจัดการระบบได้ง่าย และเพิ่มการรักษาความปลอดภัยมากขึ้นกล่าวคือ

- เพิ่มส่วนของการทำการจัดการในส่วนต่างๆ เช่น การจัดการผู้ใช้งาน การจัดการทรัพยากรระบบ
- เพิ่มการรักษาความปลอดภัยในการเข้าถึงเพจในส่วนของผู้ดูแลระบบ เพื่อไม่ให้ผู้ใช้งานทั่วไปเข้าไปควบคุมเปลี่ยนแปลงค่าคอนฟิกในระบบได้
- เพิ่มส่วนของการกำหนดสิทธิการเข้าใช้งานของผู้ใช้แต่ละคนได้
- เพิ่มส่วนของการจัดทำรายการเพื่อตรวจสอบการใช้งานของระบบจากผู้ใช้

6.2 ข้อเสนอแนะ

1. ควรมีการตรวจสอบข้อมูล Input ที่ป้อนเข้ามาสู่ระบบในขณะใช้งาน เช่นข้อมูล อีเมล์, ไอพี แอดเดรส
2. ในส่วนของการพิจารณาข้อมูลการลงทะเบียนเพื่อขอเข้าใช้งานระบบควรมีระบบอื่นมาช่วยในการตรวจสอบข้อมูลของผู้ร้องขอเพื่อให้ผู้ดูแลระบบทำงานได้สะดวกขึ้น เช่นมีระบบดึงข้อมูลจากศูนย์กลางเข้ามาเปรียบเทียบกับข้อมูลที่ได้โดยอัตโนมัติ
3. น่าจะมีการกำหนดสิทธิการเข้าใช้งานในลักษณะของการกำหนดเป็นกลุ่มเพิ่มขึ้นมา
4. ระบบนี้ยังมีการตรวจสอบการออกจากระบบยังไม่ดีนัก ควรพัฒนาเพิ่มในส่วนของการตรวจสอบ activity ของผู้ใช้งานว่ายังมีอยู่หรือไม่ และมีการ log off ผู้ใช้คนนั้นออกโดยอัตโนมัติเมื่อผู้ใช้ไม่มีการเคลื่อนไหวเมื่อถึงเวลาที่กำหนด

บรรณานุกรม

Alan Dennis ,Barbara Haley Wixon ,David Tegarden.2002.**System Analysis & Design** .John Wiley & Son.

Paul `Rusty' Russell.2000**. LinuxWorld**.[Online]. Available: http://www.netfilter.org/documentation/tutorials/lw-2000/

Phuvadhul Danrahan.2002.**Linux 2.4 Stateful Firewall : IPTABLES**.[Online]. Available: http://thaicert/nectec.or.th/paper /firewall /iptables.php

Arson Hsiao.2001.**Linux Security Basics in 24 Hours.** Sams Publishing.

ภาคผนวก

ภาคผนวก ก

การติดตั้งและปรับแต่งสภาพแวดล้อมที่ใช้ในระบบ

ติดตั้งระบบปฏิบัติการ Redhat 9.0

ทำการติดตั้งตามปกติแต่ในขั้นตอนการเลือกแพ็คเกจที่จะลงให้เลือกเฉพาะที่ต้องใช้งานจริงๆเท่านั้นเช่น Complier , Text editor , DHCP Server (dhcpd), iptables, โปรแกรม Sendmail เป็นต้นแต่จะไม่เลือกแพ็คเกจของ Web Server และส่วนของ Database เพราะเราต้องการทำการติดตั้งเองเพื่อให้ระบบรองรับการทำงานของ PHP ,HTTPS และ MySQL และเมื่อติดตั้งเสร็จเรียบร้อยแล้วทำการปรับแต่งการทำงานของโปรแกรมดังต่อไปนี้

- โปรแกรม iptables โดยใช้คำสั่ง iptables –version เพื่อดูว่า iptable ถูกติดตั้งมาด้วยหรือไม่ จากนั้นทำการรันไฟล์วอลสคริปต์ที่เตรียมไว้เพื่อทำการคอนฟิกกฎเบื้องต้นที่ต้องใช้งานดังต่อไปนี้

```
#!/bin/sh
echo "1" > /proc/sys/net/ipv4/ip_forward
iptables="/sbin/iptables"
$iptables -P FORWARD DROP
$iptables -P INPUT DROP
```

ติดตั้งฐานข้อมูล MySQL

1. Download โปรแกรม MySQL-3.23.55-1.i386.rpm , MySQL-client-3.23.55-1.i386.rpm และ MySQL-devel-3.23.55-1.i386.rpm
2. ทำการติดตั้งโดยใช้คำสั่ง ดังต่อไปนี้

```
# rpm –ivh MySQL-3.23.55-1.i386.rpm
# rpm –ivh MySQL-client-3.23.55-1.i386.rpm
# rpm –ivh MySQL-devel-3.23.55-1.i386.rpm
```

3. ทำการตรวจสอบว่ามีโปรเซสของ MySQL รันอยู่โดยใช้คำสั่ง

```
# ps –e
```

ซึ่งผลที่ได้ควรจะมีโปรเซสเหล่านี้รันอยู่

Safe_mysqld

Mysqld

Mysqld

Mysqld

4. ทำการรัน sql สคริปต์ที่เตรียมไว้เพื่อทำการสร้างดาต้าเบสของระบบโดยใช้คำสั่ง

mysql -uroot –p*(rootpassword)* < *(ชื่อไฟล์สคริปต์.sql)*

ติดตั้ง Apache เว็บเซิร์เวอร์เพื่อรองรับการทำงานของ PHP ,HTTPS และ Mysql

1. ดาวน์โหลดและขยายไฟล์โดยใช้คำสั่งดังต่อไปนี้

tar xvfz apache_1.3.33.tar.gz

tar xvfz mod_ssl-2.8.22-1.3.33.tar.gz

tar xvfz openssl-0.9.7e.tar.gz

tar xvfz php-4.3.10.tar.gz

1. คอมไพล์ openssl

cd openssl-*

./config

make

2. ทำการสร้างสคริปต์ที่ช่วยในการติดตั้งโดยจะมีด้วยกัน 2 สคริปต์ดังนี้

Apache_install

```
cd mod_ssl-2.8.22-1.3.33
./configure --with-apache=../apache_1.3.33 --with-ssl=../openssl-0.9.7e
--prefix=/www --activate-module=src/modules/php4/libphp4.a
--enable-module=rewrite --enable-module=setenvif --enable-module=mime
--enable-module=mime_magic --enable-module=dir --enable-module=auth
--enable-module=access --enable-module=alias --enable-module=userdir
--enable-module=vhost_alias --enable-module=env --enable-module=log_referer
--enable-module=log_config --enable-module=log_agent --enable-
module=headers
```

PHP_install

cd php-4.3.10

./configure –with-mysql --with-apache=/usr/local/src/webserver/apache_1.3.33 --with-openssl-dir=/usr/local/src/webserver/openssl-0.9.7e --enable-trans-sid

จากนั้นทำการเปลี่ยนแอตทริบิวต์ทั้งสองไฟล์นี้ให้สามารถทำการเอ็กซีคิวต์ได้โดยการ

chmod 700 Apache_install

chmod 700 PHP_install

3. ทำการรันสคริปต์ Apache_install และ PHP_install เพื่อทำการคอมไพล์ Apache และ PHP ตามลำดับ
4. ทำการติดตั้ง PHP และคัดลอกไฟล์คอนฟิกของ PHPไว้ในที่ๆเหมาะสม

cd php*

make

make install

cp php.ini-dist /usr/local/lib/php.ini

5. แก้ไขไฟล์คอนฟิก /usr/local/lib/php.ini เพื่อให้ PHP ใช้ฟังก์ชันการส่งอีเมล์ได้โดยการใส่พาทของคำสั่ง sendmail

[mail function]

Sendmail_path = /usr/sbin/sendmail

6. ทดสอบการติดตั้ง PHP โดยใช้คำสั่ง

php –v

PHP 4.3.4 (cli) (built: Feb 8 2004 15:47:14)

Copyright (c) 1997-2003 The PHP Group

Zend Engine v1.3.0, Copyright (c) 1998-2003 Zend Technologies

7. คอมไพล์ ติดตั้งและปรับแต่ง Apache

./Apache_install

cd apache_1.3.33

make

make certificate TYPE=custom

make install

ทำการแก้ไขค่าคอนฟิกของไฟล httpd.conf

<IfModule mod_dir.c>

DirectoryIndex index.php index.html index.htm default.php default.html

</IfModule>

และเพิ่มค่าต่อไปนี้ที่ท้ายไฟล์

AddType application/x-httpd-php .php .php3

AddType application/x-httpd-php-source .phps

8. สตาร์ทเซอร์วิส

apachectl startssl

9. สร้างหน้าเวบเพจโดยใช้ PHP สคริปต์และทดสอบใช้งาน

Info.php

```
<?php
        phpinfo();
>
```

ทดสอบการทำงานโดยการเปิดหน้าเว็บเพจ https://localhost/info.php

ภาคผนวก ข

รายละเอียดไฟล์คอนฟิกในระบบ

ไฟล์ initialfwrules เป็นไฟล์กำหนดการทำงานของไฟร์วอลล์เมื่อเริ่มทำงาน

เก็บอยู่ในพาธ /www/htdocs/wsg/ มีรายละเอียดดังนี้

```
/sbin/iptables -F
/sbin/iptables -P FORWARD DROP
/sbin/iptables -A FORWARD -m state --state ESTABLISH,RELATED -j ACCEPT
```

ไฟล์คอนฟิก rc.local

เก็บอยู่ที่พาธ /etc/ มีรายละเอียดดังนี้

```
touch /var/lock/subsys/local
/www/bin/apachectl startssl
/etc/init.d/l2tpd start
/www/htdocs/wsg/initialfwrules
```

ไฟล์คอนฟิก httpd.conf

เก็บอยู่ในพาธ /www/conf/ มีรายละเอียดที่เพิ่มเข้าไปดังนี้

```
<VirtualHost _default_:443>
DocumentRoot "/www/htdocs"
ServerName rh901
ServerAdmin root@rh901
ErrorLog /www/logs/error_log
TransferLog /www/logs/access_log
SSLEngine on
SSLCipherSuite
ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP:+eNU
LL
SSLCertificateFile /www/conf/ssl.crt/server.crt
```

```
SSLCertificateKeyFile /www/conf/ssl.key/server.key
<Files ~ "\.(cgi|shtml|phtml|php3?)$">
    SSLOptions +StdEnvVars
</Files>
<Directory "/www/cgi-bin">
    SSLOptions +StdEnvVars
</Directory>
SetEnvIf User-Agent ".*MSIE.*" \
        nokeepalive ssl-unclean-shutdown \
        downgrade-1.0 force-response-1.0
CustomLog /www/logs/ssl_request_log \
        "%t %h %{SSL_PROTOCOL}x %{SSL_CIPHER}x \"%r\" %b"
</VirtualHost>
```

ไฟล์คอนฟิก sudoers

เก็บอยู่ในพาธ /etc/ มีรายละเอียดที่เพิ่มเข้าไปดังนี้

```
root    ALL=(ALL) ALL
nobody ALL=(root) NOPASSWD: /sbin/iptables
nobody ALL=(root) NOPASSWD: /usr/sbin/sendmail
nobody ALL=(root) NOPASSWD: /bin/chmod
```

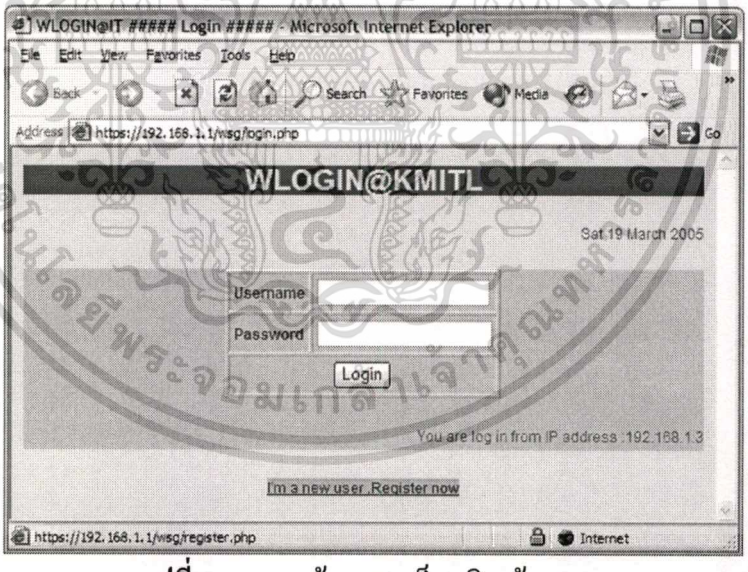
ภาคผนวก ค
คู่มือการใช้งานระบบ

ดังที่ได้กล่าวมาข้างต้นแล้วว่าในระบบนี้มีอยู่ด้วยกันสองส่วนหลักคือในส่วนของผู้ดูแลระบบ และผู้ใช้งานระบบ ดังนั้นในคู่มือการใช้งานระบบนี้จึงอธิบายแยกสองส่วนนี้ออกจากกันเพื่อความง่ายในการทำความเข้าใจ ดังนี้

ส่วนของผู้เข้าใช้งาน

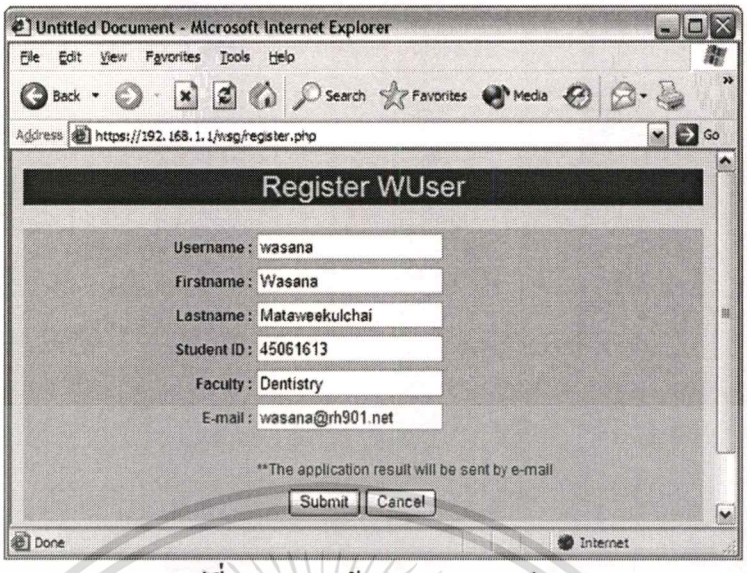
1. การลงทะเบียนเพื่อขอเข้าใช้งาน

1. ผู้ใช้ที่ต้องการใช้งานเข้ามาทำการลงทะเบียนเพื่อขอใช้ระบบ ผู้ใช้งานสามารถเข้าลงทะเบียนโดยทำการเปิดลิงค์ https://192.168.1.1/wsg/login.php และเลือกลิงค์ "I'm a new user, Register now"



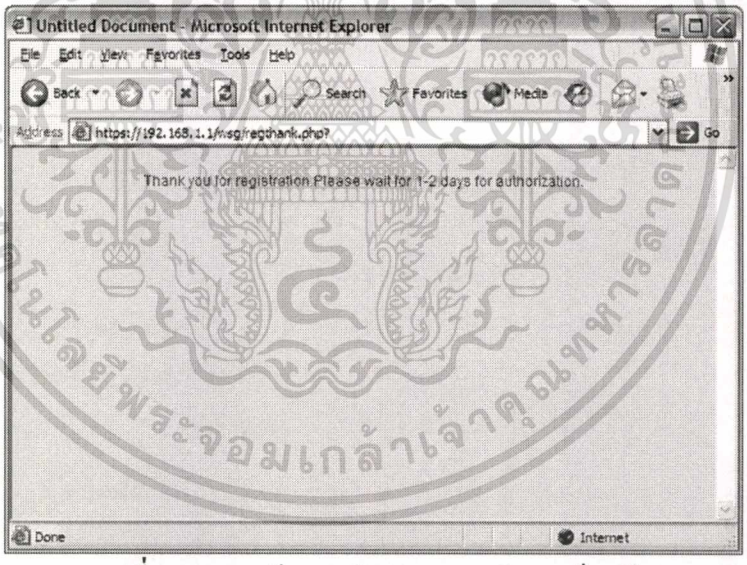
รูปที่ 1 แสดงหน้าจอการล็อคอินเข้าระบบ

2. ผู้ใช้ทำการกรอกข้อมูลส่วนตัวลงในหน้าลงทะเบียน เมื่อกรอกข้อมูลทั้งหมดเสร็จแล้วทำการกดที่ปุ่ม Submit เพื่อยืนยันหรือ Cancel เพื่อยกเลิกการลงทะเบียน



รูปที่ 2 แสดงหน้าจอการลงทะเบียน

3. หลังจากยืนยันการลงทะเบียนแล้วก็ต้องรอจนกว่าผู้ดูแลระบบส่งผลการลงทะเบียนมาให้ผ่านทางอีเมล์ที่ได้ให้ข้อมูลไว้



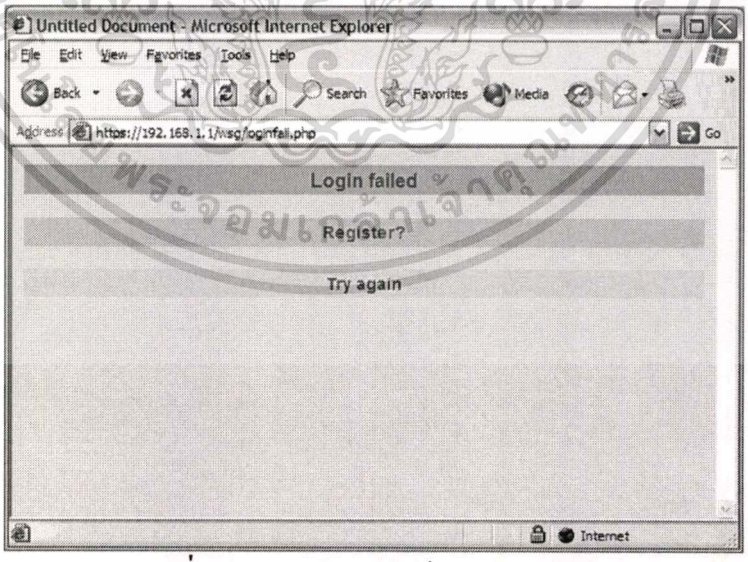
รูปที่ 3 แสดงหน้าจอหลังจากลงทะเบียนเสร็จแล้ว

2. การล็อคอินเพื่อเข้าใช้งานระบบ และการล็อคเอาท์ออกจากระบบ

1. ผู้เข้าใช้งานสามารล็อคอินได้โดยเปิดลิงค์ https://192.168.1.1/wsg/login.php จากนั้นทำการกรอกชื่อผู้ใช้งานและรหัสผ่าน จากนั้นทำการกดปุ่ม Login เพื่อทำการเข้าระบบ

รูปที่ 4 แสดงการล็อคอินเข้าระบบ

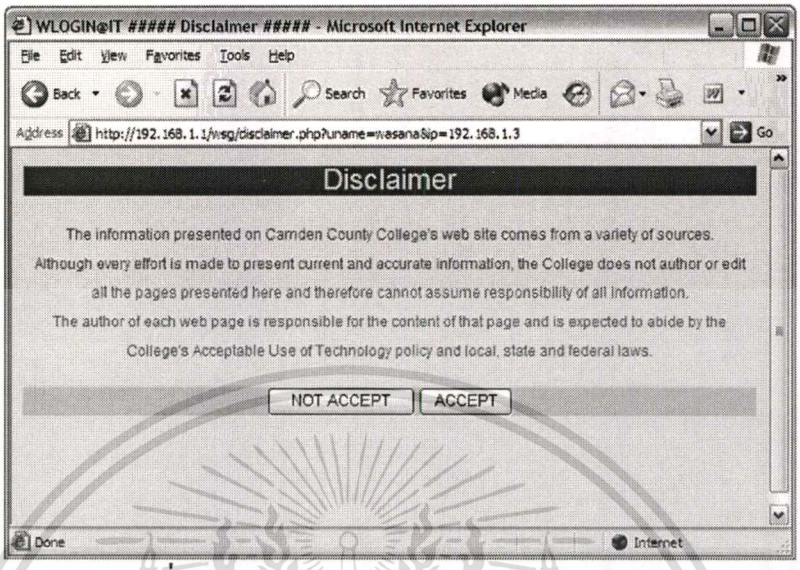
2. ถ้าชื่อผู้ใช้งานและรหัสผ่านไม่ตรงกับข้อมูลที่มีอยู่ในระบบ ระบบจะให้ผู้ใช้งานเลือกว่าจะทำการลองล็อคอินใหม่โดยกดที่ลิงค์ Try Again หรือจะทำการลงทะเบียนใหม่โดยการกดที่ลิงค์ Register ?



รูปที่ 5 แสดงหน้าจอการล็อคอินผิดพลาด

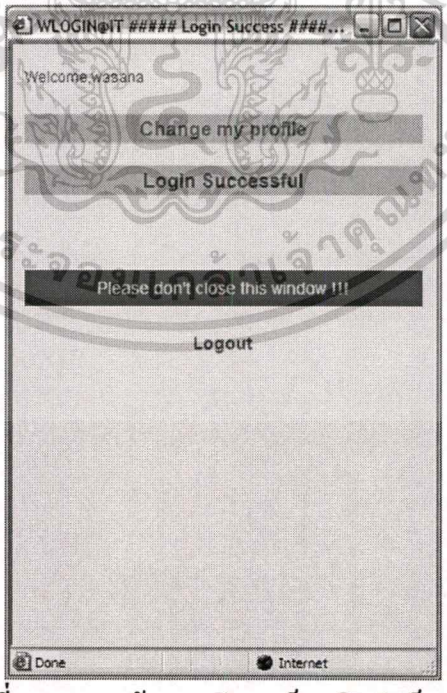
3. ถ้าการพิสูจน์ตนเองสำเร็จระบบจะทำการเปิดหน้าเพจคำเตือนการเข้าใช้งานระบบ มาเพื่อให้ผู้ใช้ยอมรับคำเตือนการใช้งานระบบ ถ้าผู้ใช้ยอมรับคำเตือนการเข้าใช้ระบบก็ทำการกดปุ่ม ACCEPT ซึ่งในขั้นนี้ผู้ใช้งานก็สามารถเข้าสู่ระบบโดยสมบูรณ์ แต่ผู้ใช้งานก็

สามารถไม่ยอมรับคำเตือนการเข้าใช้งานก็ได้โดยกดปุ่ม NOT ACCEPT ระบบก็จะเปิดหน้าที่ใช้ทำการล็อคอินอีกครั้ง



รูปที่ 6 แสดงหน้าจอคำเตือนก่อนเข้าใช้งานระบบ

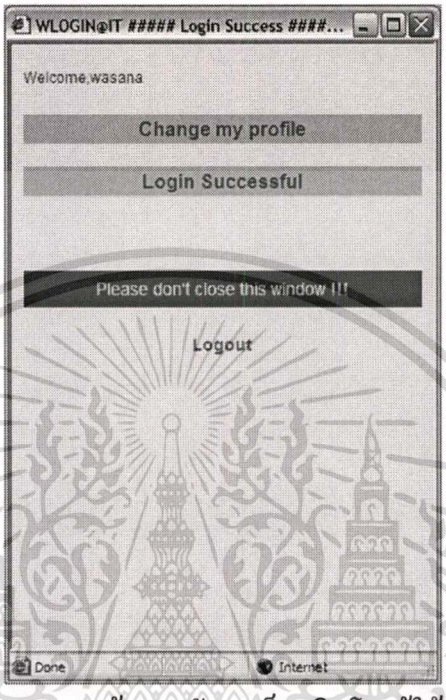
4. เมื่อผู้ใช้ยอมรับคำเตือนการเข้าใช้งานแล้วระบบจะเปิดหน้าเพจมาหน้าหนึ่งเพื่อทำการแจ้งบอกว่าได้ล็อคอินเข้าสู่ระบบเรียบร้อยแล้ว ซึ่งในหน้านี้ผู้ใช้ก็สามารถทำการล็อคเอาท์จากระบบได้โดยเลือกที่ลิงค์ Logout



รูปที่ 7 แสดงหน้าจอหลังจากล็อคอินสำเร็จแล้ว

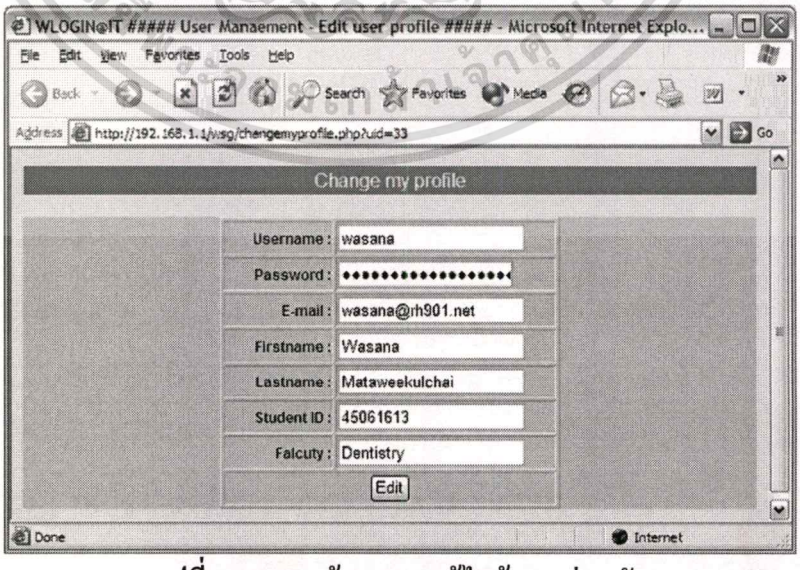
3. การเปลี่ยนรหัสผ่าน และข้อมูลส่วนตัวของผู้ใช้งาน

1. หลังจากที่ผู้ใช้ทำการล็อคอินเข้าสู่ระบบโดยสมบูรณ์แล้วระบบจะทำการเปิดหน้าเพจแจ้งบอกว่าได้เข้าสู่ระบบโดยสมบูรณ์แล้ว ซึ่งผู้ใช้สามารถทำการเปลี่ยนข้อมูลส่วนตัว รวมไปถึงรหัสผ่านได้ในหน้านี้โดยเลือกที่ลิงค์ Change my profile



รูปที่ 8 แสดงหน้าจอหลังจากล็อคอินโดยผู้ใช้ระบบ

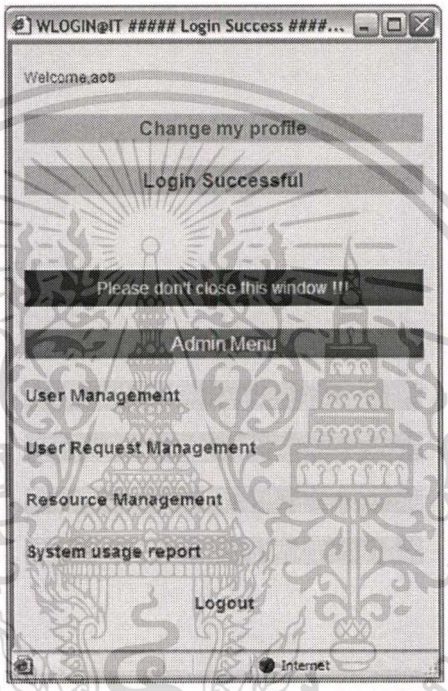
2. เมื่อผู้ใช้ทำการเปลี่ยนรหัสผ่านหรือข้อมูลส่วนตัวเสร็จแล้วก็ทำการกดปุ่ม Edit เพื่อทำการบันทึกข้อมูลลงฐานข้อมูล



รูปที่ 9 แสดงหน้าจอการแก้ไขข้อมูลส่วนตัว

ส่วนของผู้ดูแลระบบ

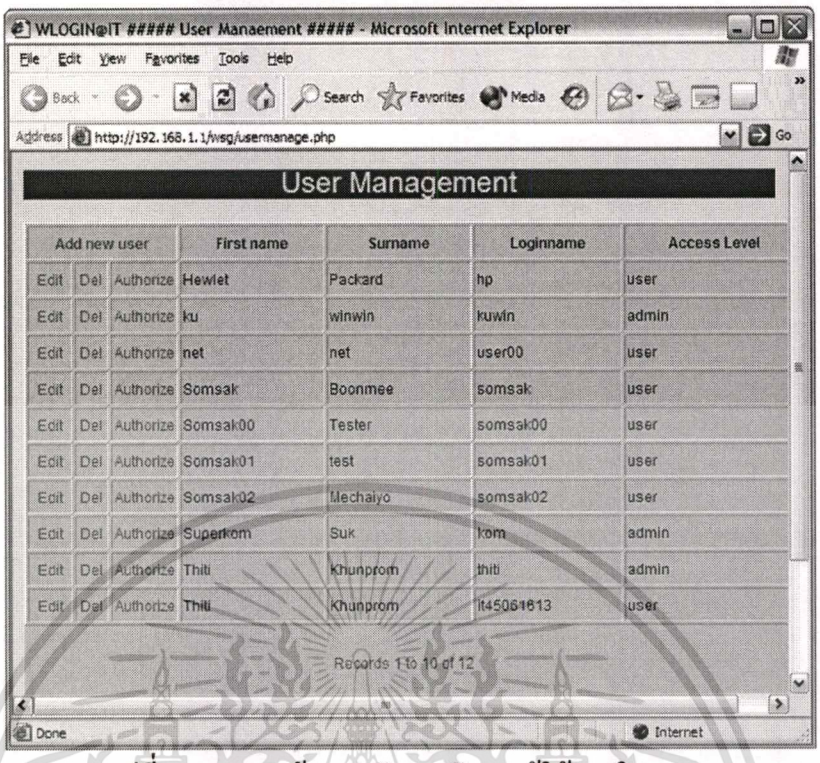
ในส่วนของผู้ดูแลระบบนั้นจะมีการเพิ่มการดูแลจัดการระบบเพิ่มขึ้นมาโดยนอกจากนั้น เช่นการล็อคอิน ล็อคเอาท์ หรือเปลี่ยนข้อมูลส่วนตัวจะมีขั้นตอนเหมือนกับส่วนของผู้ใช้งานระบบ ดังนั้นจึงไม่ขอกล่าวถึงรายละเอียดในส่วนนี้ การเข้าถึงเมนูที่จะสามารถเข้าจัดการระบบได้นั้นโดยผู้ดูแลระบบทำการล็อคอินเข้าสู่ระบบโดยสมบูรณ์แล้วระบบจะทำการเปิดหน้าเพจแจ้งบอกว่าได้เข้าสู่ระบบโดยสมบูรณ์แล้ว แต่ในเพจนี้สำหรับผู้ดูแลระบบจะมีเมนูการเข้าจัดการระบบในส่วนต่างๆ ได้ดังรูป



รูปที่ 10 แสดงหน้าจอหลังจากล็อคอินโดยผู้ดูแลระบบ

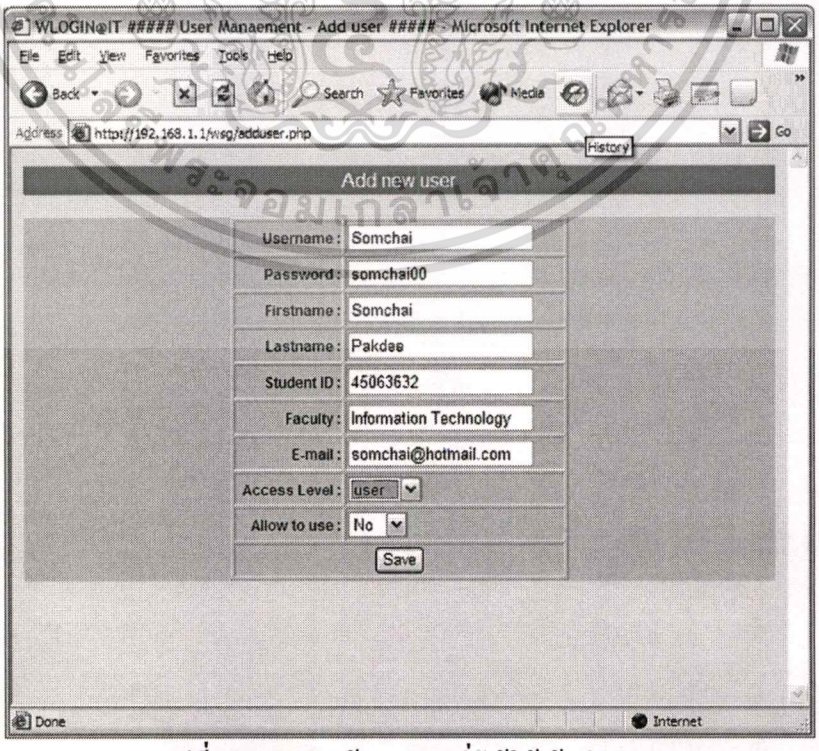
1. การเข้าจัดการดูแลผู้ใช้งานในระบบ

ผู้ดูแลระบบสามารถจัดการกับผู้ใช้งานในระบบอันได้แก่ เพิ่ม ลบ แก้ไข ข้อมูลของผู้ใช้ในระบบได้ทุกคน รวมไปถึงการกำหนดสิทธิการเข้าใช้ทรัพยากรในระบบของแต่ละคนได้โดยเลือกลิงค์ User Management ในเมนูผู้ดูแลระบบ



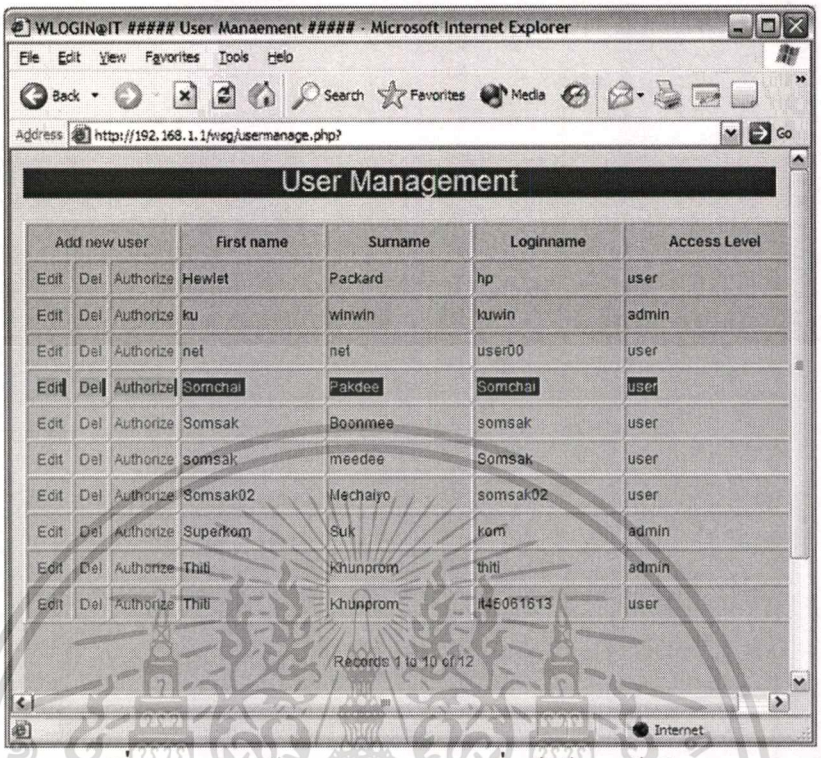
รูปที่ 11 แสดงหน้าจอหลักการจัดการผู้ใช้งานในระบบ

1. การทำการเพิ่มผู้ใช้งานใหม่เข้าสู่ระบบ ผู้ดูแลระบบทำการเพิ่มผู้ใช้งานระบบได้โดยเลือกลิงค์ Add new user จากนั้นทำการกรอกข้อมูลทุกอย่างจนครบและกดปุ่ม Save เพื่อบันทึกข้อมูลลงระบบ



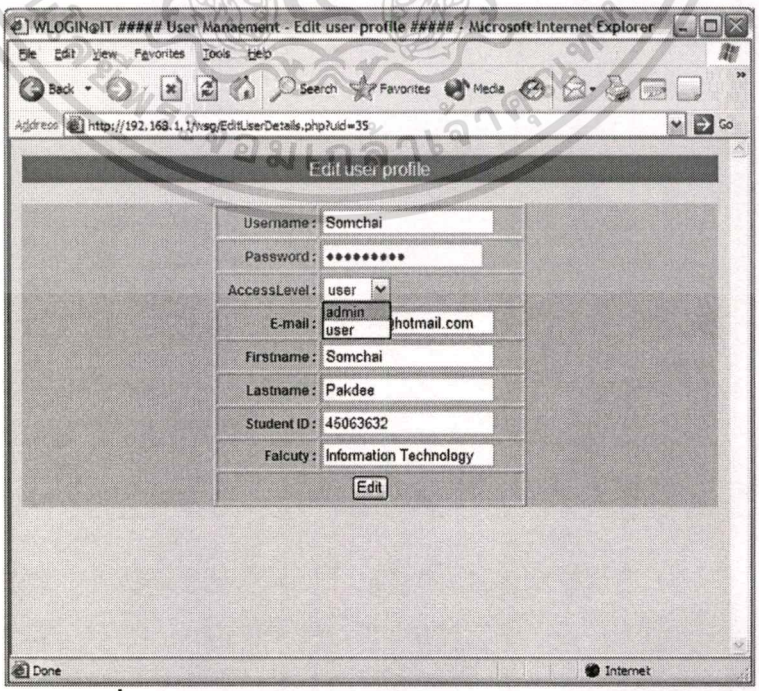
รูปที่ 12 แสดงหน้าจอการเพิ่มผู้ใช้เข้าสู่ระบบ

ข้อมูลผู้ใช้งานจะถูกบันทึกลงฐานข้อมูลและผู้ใช้คนนี้สามารถเข้ามาใช้งานระบบได้ทันที



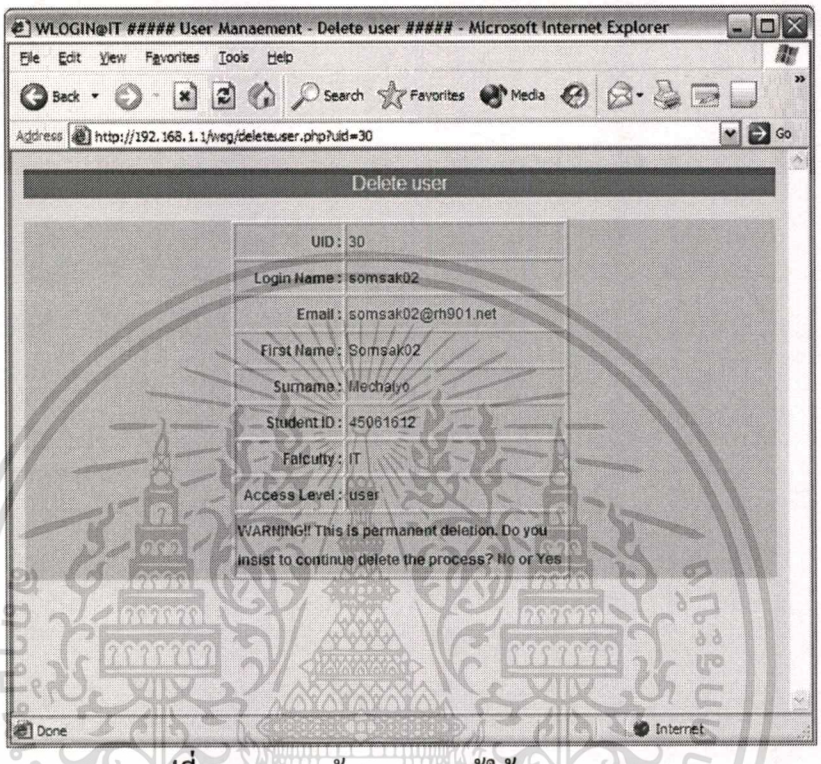
รูปที่ 13 แสดงหน้าจอหลังจากมีการเพิ่มผู้ใช้งานเข้าสู่ระบบ

2. การแก้ไขข้อมูลส่วนตัวของผู้ใช้งานระบบ รวมไปถึงการแก้ไขสิทธิการเข้าใช้ระบบได้โดยทำการเลือกลิงค์ Edit ที่ชื่อของผู้ใช้ที่ต้องการจะแก้ไข แล้วทำการแก้ไขข้อมูลต่างๆ จากนั้นกดปุ่ม Edit เพื่อทำการบันทึกข้อมูลลงฐานข้อมูล



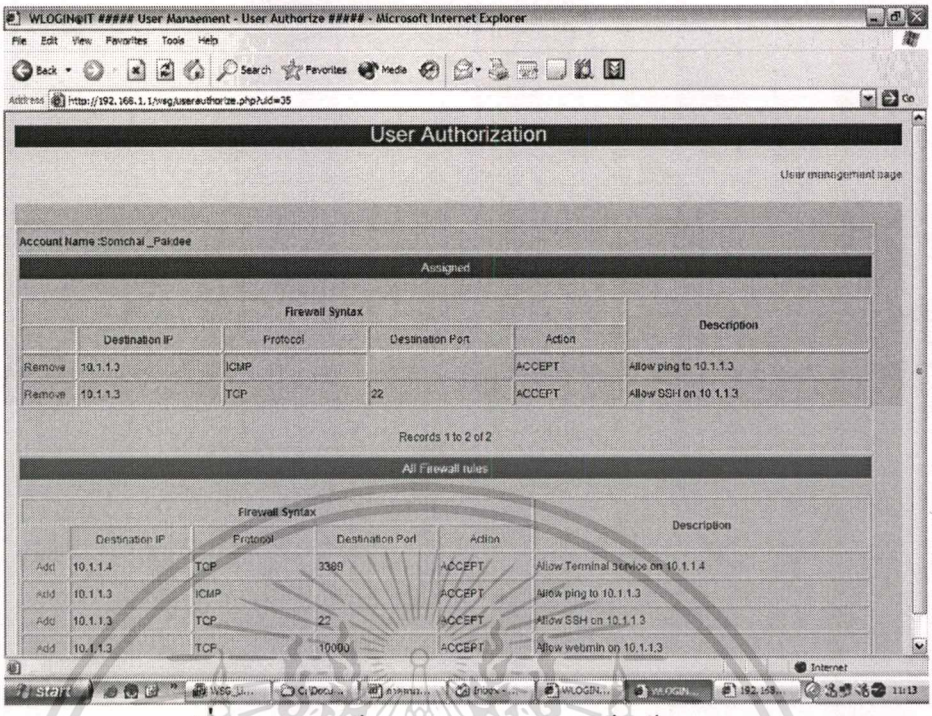
รูปที่ 14 แสดงหน้าจอการแก้ไขข้อมูลผู้ใช้งานในระบบ

3. การลบข้อมูลผู้ใช้ออกจะระบบทำได้โดยเลือกลิงค์ Del ที่ชื่อของผู้ใช้ที่ต้องการจะลบ ระบบจะถามเพื่อยืนยันการลบผู้ใช้ออกจากระบบอีกครั้งโดยเลือกลิงค์ Yes เพื่อยืนยันการลบ หรือ No เพื่อยกเลิกการลบ



รูปที่ 15 แสดงหน้าจอการลบผู้ใช้ออกจากระบบ

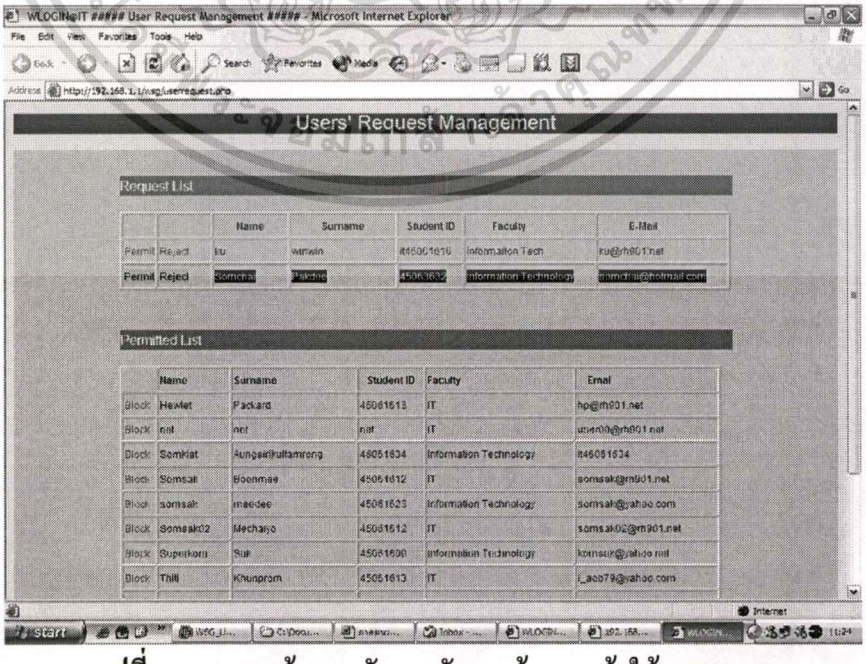
4. การกำหนด หรือแก้ไขสิทธิการเข้าใช้งานระบบทำได้โดยเลือกลิงค์ Authorize ที่ชื่อของผู้ใช้ที่ต้องการจะแก้ไข จากนั้นก็สามารถแก้ไขเพิ่มเติมสิทธิการเข้าใช้งานระบบได้โดยถ้าต้องการเพิ่มสิทธิให้กับผู้ใช้ในข้อไหน ก็เลือกลิงค์ Add ในสิทธิข้อนั้น หรือต้องการลดสิทธิก็ทำได้โดยการเลือกลิงค์ Remove ที่สิทธิข้อนั้น



รูปที่ 16 แสดงหน้าจอการกำหนดสิทธิเข้าใช้งานระบบ

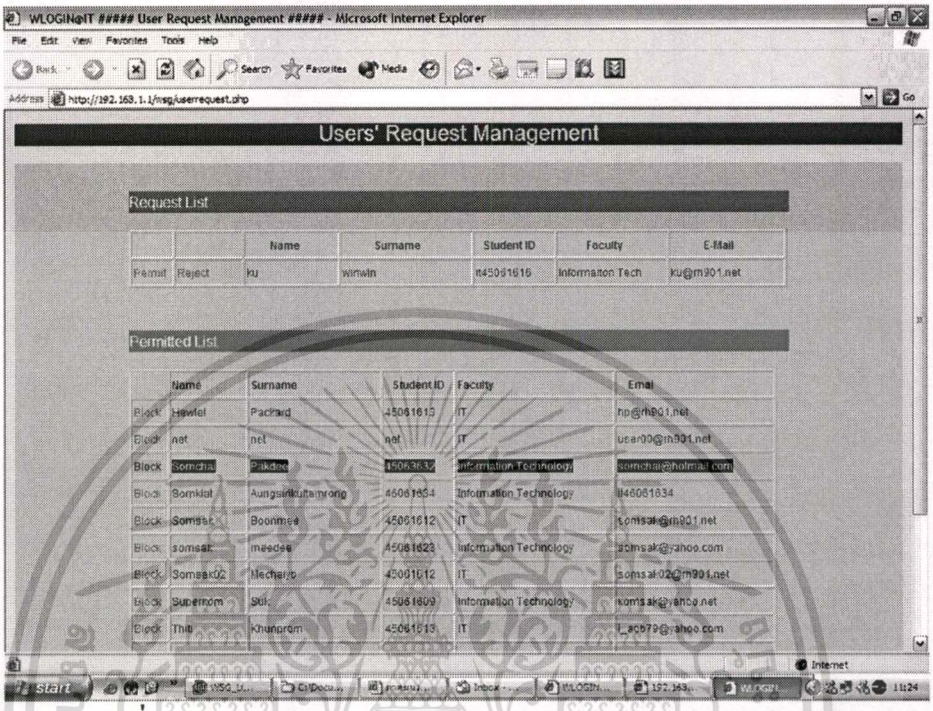
2. การจัดการร้องขอการเข้าใช้ระบบ

ผู้ดูแลระบบสามารถจัดการร้องขอการเข้าใช้ระบบอันได้แก่การอนุญาต หรือไม่อนุญาตให้เข้าใช้งาน หรือทำการระงับการเข้าใช้งานของผู้ใช้ชั่วคราวได้โดยเลือกลิงค์ User Request Management ในเมนูผู้ดูแลระบบ ซึ่งผู้ที่ได้รับอนุญาตให้เข้าใช้แล้วจะอยู่ใน Permit List และใน Request List เป็นส่วนขอผู้ร้องขอใหม่ที่เพิ่งจะทำการลงทะเบียนเข้าใช้งานระบบ



รูปที่ 17 แสดงหน้าจอหลักการจัดการร้องขอเข้าใช้งานระบบ

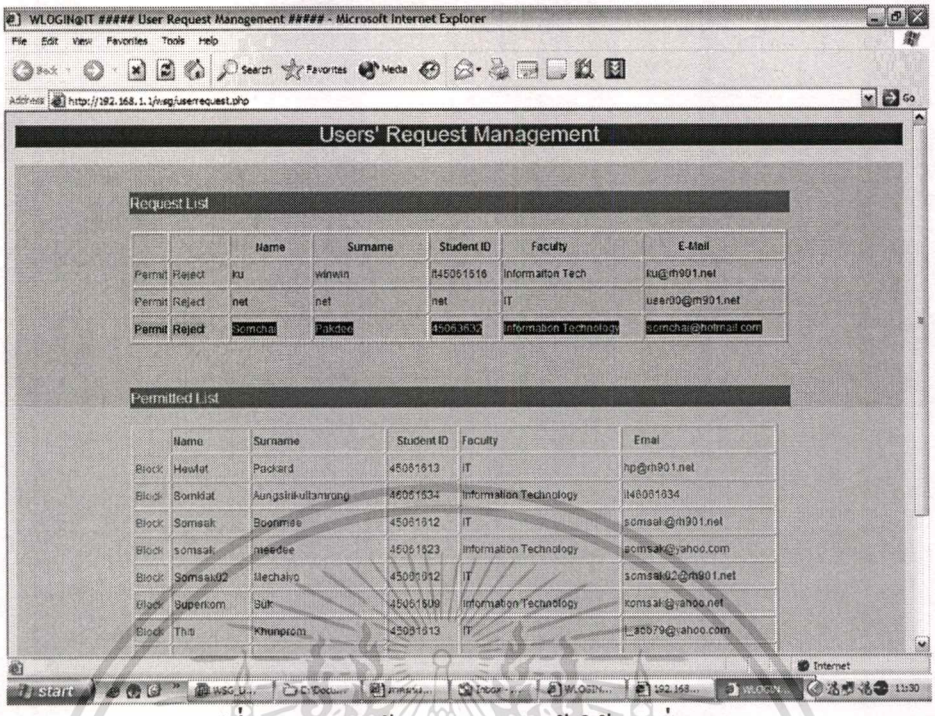
1. การอนุญาตให้ผู้ร้องขอเข้าใช้ระบบได้ โดยทำการเลือกลิงค์ Permit ที่ชื่อของผู้ร้องขอคนนั้นโดยระบบจะย้ายผู้ร้องขอคนนั้นมาที่ Permitted List และทำการสุ่มรหัสผ่านจากนั้นทำการส่งผ่านอีเมล์ไปยังผู้ใช้งานคนนั้น



รูปที่ 18 แสดงหน้าจอการทำการอนุญาตให้ผู้ใช้เข้าใช้งานระบบได้

2. ผู้ดูแลระบบสามารถปฏิเสธการเข้าใช้งานได้โดยทำการเลือกลิงค์ Reject ที่ชื่อของผู้ร้องขอคนนั้น ระบบจะทำการลบข้อมูลการร้องขอของผู้ใช้งานคนนั้นออกจากระบบ

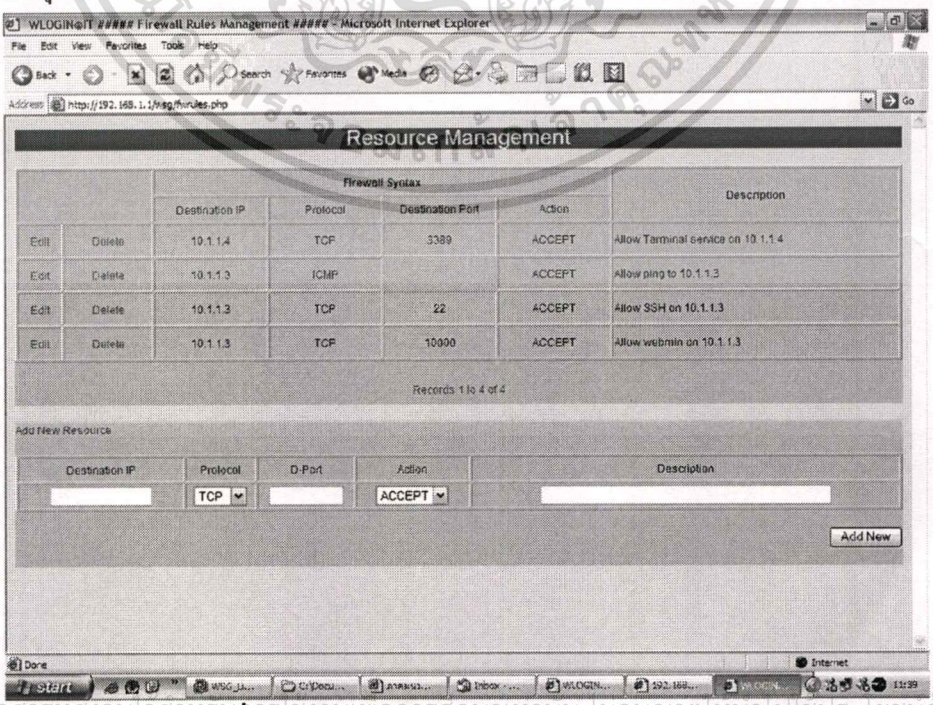
3. ผู้ดูแลระบบสามารถระงับการเข้าใช้งานระบบชั่วคราวได้โดยการเลือกลิงค์ Block ที่ชื่อของผู้ใช้คนนั้น ระบบจะย้ายผู้ใช้คนนี้เข้าไปใน Request List และผู้ใช้ระบบก็สามารถยกเลิกการระงับการเข้าใช้งานได้โดยเลือกลิงค์ Permit ที่ชื่อผู้ใช้คนนั้น



รูปที่ 19 แสดงหน้าจอการระงับเข้าใช้งานชั่วคราว

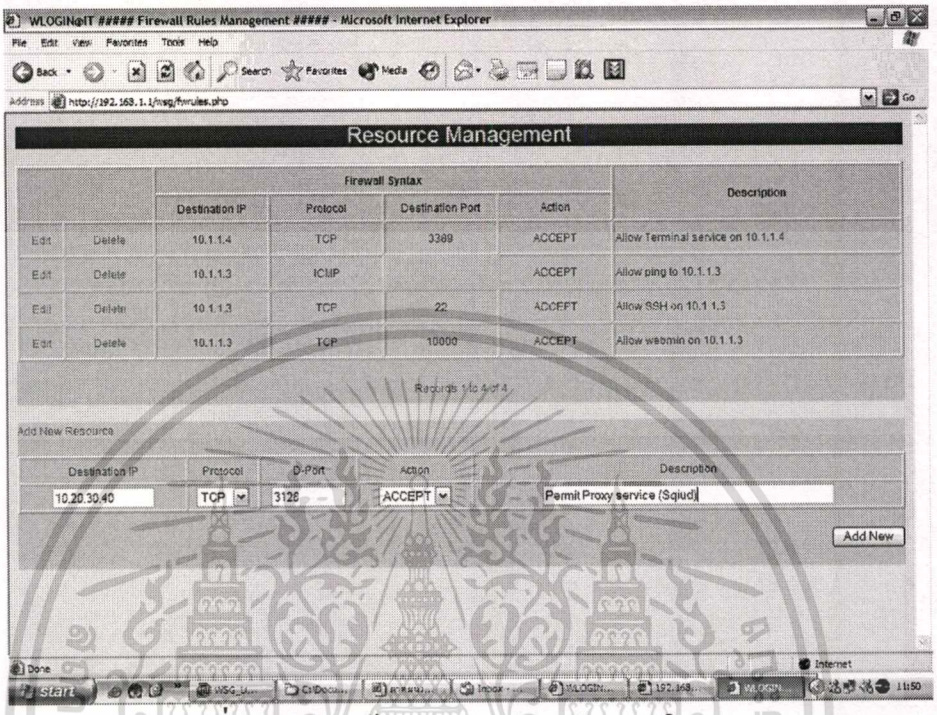
3. การจัดการกำหนดทรัพยากรในระบบ

ผู้ดูแลระบบสามารถทำการกำหนดการเพิ่มลด และแก้ไขการกำหนดทรัพยากรในระบบได้ โดยเลือกลิงค์ Resource Management จากเมนูผู้ดูแลระบบ ซึ่งการกำหนดทรัพยากรระบบนั้นเป็นการกำหนดโดยมีรูปแบบเดียวกับการกำหนดกฎการทำงานของไฟร์วอลล์ แต่แตกต่างกันตรงที่จะไม่มีการระบุต้นทางเท่านั้น



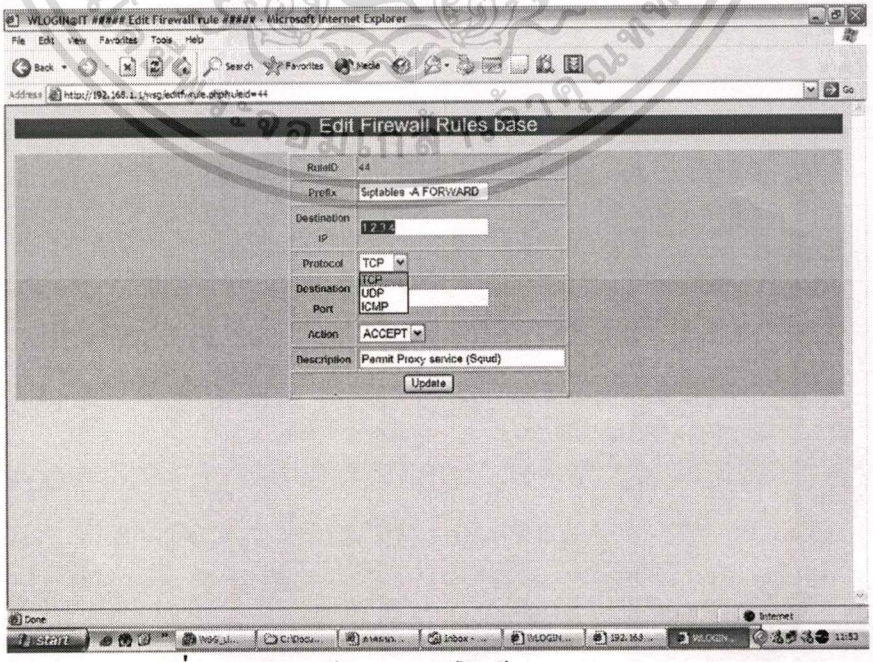
รูปที่ 20 แสดงหน้าจอการจัดการทรัพยากรระบบ

1. การเพิ่มทรัพยากรใหม่ในระบบทำได้โดยเพิ่มไอพีต้นทาง, โปรโตคอล, พอร์ตที่เปิดให้บริการ , Action และคำอธิบายของทรัพยากรนี้ จากนั้นเมื่อทำการกรอกข้อมูลต่างๆ เรียบร้อยแล้วก็กดปุ่ม Add New เพื่อทำการบันทึกลงระบบ



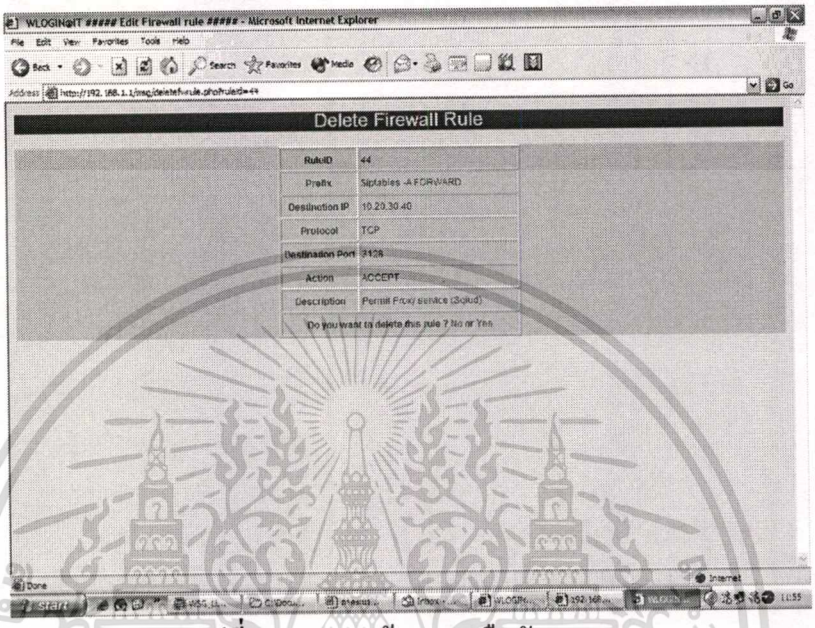
รูปที่ 21 แสดงหน้าจอการกำหนดทรัพยากรในระบบ

2. ผู้ดูแลระบบสามารถทำการแก้ไขข้อมูลทรัพยากรที่มีในระบบได้โดยการเลือกลิงค์ Edit และเมื่อทำการแก้ไขเสร็จแล้วก็ทำการกดปุ่ม Update เพื่อทำการบันทึกข้อมูลลงฐานข้อมูล



รูปที่ 22 แสดงหน้าจอการแก้ไขข้อมูลทรัพยากรระบบ

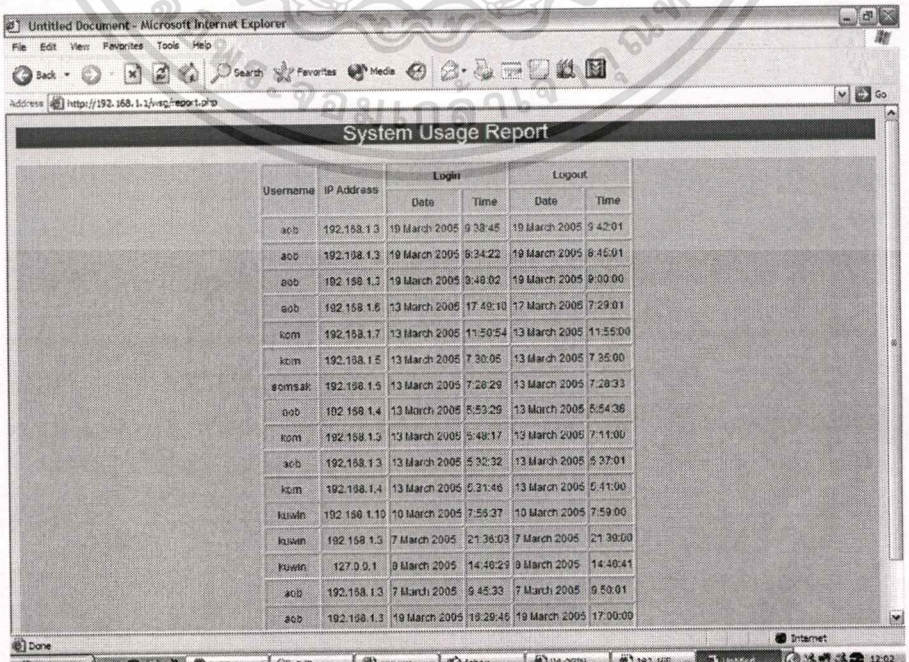
3. ผู้ดูแลระบบสามารถลบการกำหนดทรัพยากรในระบบได้โดยการเลือกลิงค์ Delete ที่หน้าทรัพยากรนั้น โดยระบบจะทำการถามการยืนยันการลบ ถ้ายืนยันการลบก็เลือกลิงค์ Yes แต่ถ้าต้องการยกเลิกการลบก็เลือกลิงค์ No



รูปที่ 23 แสดงหน้าจอการยืนยันการลบ

4. การเข้าดูรายงานการเข้าใช้งานระบบ

ผู้ดูแลระบบสามารถเข้าไปดูรายระเอียดการเข้าใช้งานระบบของผู้ใช้ทั้งหมดได้โดยเลือกลิงค์ System usage Report จากเมนูผู้ดูแลระบบ โดยระบบจะทำการแสดงวันและเวลาการใช้งานทั้งหมดของระบบ



รูปที่ 24 แสดงหน้าจอรายงานการเข้าใช้งานระบบ

ประวัติผู้เขียนโครงงาน

ชื่อผู้จัดทำโครงงาน	**นายฐิติ ขุนพรหม**
วันเดือนปีเกิด	17 พฤษาคม 2522
สถานที่เกิด	จังหวัดนครสวรรค์
ประวิติการศึกษา	
ประถมศึกษา	โรงเรียนอนุบาลนครสวรรค์
มัธยมศึกษาตอนต้น	โรงเรียนนครสวรรค์
มัธยมศึกษาตอนปลาย	โรงเรียนนครสวรรค์
ปริญญาตรี	มหาวิทยาลัยนเรศวร