การพัฒนาระบบการยืนยันตัวตนโดยใช้เทคโนโลยีฟรีแวร์

พรคิด อั้นขาว

งานวิจัยนี้ได้รับทุนสนับสนุนจากงบประมาณเงินรายได้ ประจำปีงบประมาณ 2556
มหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร คณะบริหารธุรกิจ

บทคัดย่อ

การศึกษาครั้งนี้ มีวัตถุประสงค์เพื่อวิจัยและพัฒนาระบบการยืนยันตัวตนโดยใช้เทคโนโลยีฟรีแวร์ เพื่อเพิ่มประสิทธิภาพของกระบวนการทำงานระบบงานระบบการยืนยันตัวตน

งานวิจัยนี้เป็นลักษณะวิจัยและพัฒนาซอฟต์แวร์ เพื่อนำมาประยุกต์ใช้ในการจัดการระบบระบบการยืนยันตัวตน โดยมีกระบวนการพัฒนาจากการศึกษาขั้นตอนการปฏิบัติงานของระบบระบบการยืนยันตัวตน เพื่อนำไปพัฒนาซอฟต์แวร์ โดยได้เลือกเครื่องมือที่ใช้ในการพัฒนาคือ โปรแกรมระบบปฏิบัติการ Linux สำหรับการพัฒนา

ผลของงานวิจัย โปรแกรมดังกล่าวที่ผลิตขึ้นได้นำไปใช้งานจริงกับกลุ่มเป้าหมาย คือ บุคลากรของหน่วยงาน โดยผู้วิจัยได้ทำแบบประเมินการใช้งานสำหรับระบบการยืนยันตัวตนโดยใช้เทคโนโลยีฟรีแวร์ พบว่าผู้ใช้งานมีความพึงพอใจต่อโปรแกรมอยู่ในระดับดี

ABSTRACT

This study Aims to research and develop identity verification using freeware. For optimization of workflow systems, authentication systems.

This research is a research and software development. To be applied to the management system to verify identity. The development process of the study process, the performance of the verification system . To software development It is a tool used for development . Program for the development of the Linux operating system .

The results of research Such programs can be used to produce real target audience is the personnel of the agency. This research has made evaluating its use for system identification using freeware. Users have found that satisfaction with the program was good .

กิตติกรรมประกาศ

งานวิจัยเรื่องนี้ได้รับการสนับสนุนทุนการวิจัยจากงบประมาณเงินรายได้ ประจำปีงบประมาณ พ.ศ. 2556 คณะบริหารธุรกิจ มหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร ซึ่งช่วยให้การดำเนินการวิจัยเสร็จอย่างสมบูรณ์ ผู้วิจัยขอขอบพระคุณมา ณ โอกาสนี้

ขอขอบพระคุณอาจารย์ เจ้าหน้าที่ และนักศึกษา คณะบริหารธุรกิจ ที่ให้ความช่วยเหลือระหว่างการดำเนินงานด้วยดีเสมอมา ตลอดจนหน่วยงานอื่นๆ ที่เกี่ยวข้องของมหาวิทยาลัย ฯ

สุดท้ายนี้ หากงานวิจัยนี้มีข้อผิดพลาดหรือบกพร่องประการใด ผู้วิจัยขออภัยมา ณ ที่นี้ และผู้วิจัยจะพยายามพัฒนางานวิจัยที่มีคุณภาพต่อไป

พรคิด อั้นขาว

สารบัญเรื่อง

สารบัญเรื่อง (ต่อ)

สารบัญตาราง

สารบัญภาพ

สารบัญภาพ (ต่อ)

บทที่ 1
บทนำ

1.1 ที่มาของปัญหา

ตามที่พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มีผลบังคับใช้ตั้งแต่วันที่ 22 สิงหาคม 2550 นั้น มีผลทำให้หน่วยงานต่างๆ ซึ่งเป็นผู้ให้บริการเข้าถึงระบบเครือข่ายอินเตอร์เน็ตจำเป็นต้องเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Traffic Data) ไว้อย่างน้อย 90 วัน ปรากฏว่าหน่วยงานต่างๆ ส่วนใหญ่ยังขาดความรู้ความเข้าใจในเจตนารมณ์ของกฎหมาย และวิธีการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Traffic Data) ที่ถูกต้องและครบถ้วนตามที่กฎหมายกำหนด ดังนั้นเพื่อให้หน่วยงานต่างๆ สามารถเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Traffic Data) ได้ถูกต้องและ ครบถ้วนตามที่กฎหมายกำหนด และสามารถประหยัดงบประมาณในการจัดซื้อซอฟต์แวร์จากต่างชาติ โดยการนำซอฟต์แวร์ Open Source หรือฟรีแวร์ไปใช้ในการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Traffic Data) ให้กับหน่วยงานภาครัฐ ภาคเอกชน และผู้ดูแลระบบสามารถใช้งานระบบได้อย่างมีประสิทธิ์ภาพ ซึ่งจะเป็นการทำให้บุคลากรของหน่วยงานภาครัฐ ภาคเอกชนต่างๆ ในประเทศไทยทันต่อการเปลี่ยนแปลงเทคโนโลยีอยู่เสมอ

1.2 วัตถุประสงค์ของโครงการวิจัย

1.2.1 เพื่อช่วยให้หน่วยงานของภาครัฐ และผู้ดูแลระบบเข้าใจวัตถุประสงค์ที่แท้จริงของการเก็บข้อมูลจราจร (Traffic Data) ตาม มาตรา 26 ของ พรบ. การกระทำผิดด้วยคอมพิวเตอร์ พ.ศ. 2550

1.2.2 เพื่อให้หน่วยงานของภาครัฐ และผู้ดูแลระบบเข้าใจวิธีการเก็บข้อมูลจราจร (Traffic Data) ที่ถูกต้องตามมาตรา 26 ของ พรบ. การกระทำผิดด้วยคอมพิวเตอร์ พ.ศ. 2550

1.2.3 เพื่อให้หน่วยงานของภาครัฐ และผู้ดูแลระบบสามารถเก็บข้อมูลจราจร (Traffic Data) ได้ด้วย ซอฟต์แวร์โอเพนซอร์ส อย่างถูกต้องและครบถ้วนตามที่กฎหมายกำหนด

1.2.4 เพื่อให้หน่วยงานของภาครัฐ สามารถให้คำปรึกษาแก่ผู้รับบริการอย่างถูกต้องและครบถ้วนตามที่กฎหมายกำหนด

1.2.5 เพื่อให้หน่วยงานของภาครัฐ ลดค่าใช้จ่ายในการจัดเก็บข้อมูลจราจร (Traffic Data)

1.3 ขอบเขตของการวิจัย

1.3.1 ศึกษาและสำรวจหน่วยงานของภาครัฐ ที่มีความต้องการติดตั้งระบบ Authentication (พิสูจน์ตัวตน) จำนวน 2 หน่วยงาน

1.3.2 เลือกหน่วยงานของภาครัฐ ที่ใช้ในการวิจัย จำนวน 2 หน่วยงาน โดยพิจารณาจากหน่วยงานที่มีแหล่งข้อมูลที่ใช้ในการวิจัยครบถ้วน เช่น ข้อมูลพื้นฐานของหน่วยงาน, ข้อมูลระบบเครือข่ายคอมพิวเตอร์ เป็นต้น

1.3.3 ให้ความรู้เกี่ยวกับกระบวนการติดตั้งระบบ Authentication (พิสูจน์ตัวตน) จัดเก็บข้อมูลในด้านต่างๆ ที่เกี่ยวข้องกับระบบ เพื่อสร้างระบบทรัพยากรสารสนเทศอย่างเป็นระบบ โดยใช้ซอฟต์แวร์ที่เป็น Open Source หรือฟรีแวร์ เช่น Ubuntu, Fedora หรือ CENTOs ฯลฯ เพื่อสร้างระบบ Authentication ที่มีคุณภาพ มีรายละเอียดดังนี้

1.3.3.1 ระบบ Authentication (พิสูจน์ตัวตน) การเข้าใช้งานของ User

1.3.3.2 ระบบจัดเก็บ Log File ตาม พรบ.คอมพิวเตอร์

1.3.3.3 ระบบ Proxy Server

1.3.3.4 สามารถจำกัด Bandwidth การใช้งานของ User

1.3.3.5 มี Report แสดงการใช้งานอินเตอร์เน็ต

1.3.4 นำเสนอ ติดตั้งระบบ Authentication ที่หน่วยงานของภาครัฐ โดยผู้ที่ดูแลระบบสามารถใช้ระบบ Authentication ได้อย่างเหมาะสม

1.3.5 ศึกษาเปรียบเทียบการติดตามและประเมินผลการใช้งานระบบ Authentication ของผู้ใช้จากการระบบ Authentication

1.4 ประโยชน์ที่คาดว่าจะได้รับ

1.4.1 ได้ระบบต้นแบบนำซอฟต์แวร์โอเพนซอร์สไปใช้เก็บข้อมูลจราจร (Traffic Data)

1.4.2 หน่วยงานภาครัฐสามารถนำความรู้ที่ได้รับไปให้บริการให้คำปรึกษาและติดตั้งระบบเก็บข้อมูลจราจร (Traffic Data) ด้วยซอฟต์แวร์โอเพนซอร์สอย่างถูกต้องและครบถ้วนตามที่กฎหมายกำหนด

1.4.3 System Admin ของหน่วยงานภาครัฐสามารถนำซอฟต์แวร์โอเพนซอร์สไปใช้เก็บข้อมูลจราจร (Traffic Data) ได้อย่างถูกต้องและครบถ้วนตามที่กฎหมายกำหนด

1.5 วิธีการวิจัย

1.5.1 ศึกษาขั้นตอนกระบวนการของระบบงานต่างๆ

1.5.2 ศึกษาทฤษฎีที่เกี่ยวข้องกับการออกแบบระบบระบบ Authentication (พิสูจน์ตัวตน) การเข้าใช้งานของ User

1.5.3 ศึกษาเครื่องมือที่ช่วยในการพัฒนาระบบงาน

1.5.4 วิเคราะห์ระบบงานเก่าและใหม่ของระบบงาน

1.5.5 ออกแบบและสร้างระบบระบบ Authentication (พิสูจน์ตัวตน) การเข้าใช้งานของ

1.5.6 พัฒนาและทดสอบระบบงาน

1.5.7 ทดลองใช้งานจริงกับระบบ และแก้ไขข้อผิดพลาด

1.5.8 สรุปผลการวิจัย

1.5.9 รายงานผลการวิจัย

บทที่ 2
ระบบงานเดิม และทฤษฎีที่เกี่ยวข้อง

โครงการวิจัย การพัฒนาระบบการยืนยันตัวตนโดยใช้เทคโนโลยีฟรีแวร์ ผู้วิจัยได้ทำการศึกษาค้นคว้าเอกสาร และการศึกษาระบบที่เกี่ยวข้องกับการพัฒนาระบบโดยแบ่งเป็นหัวข้อดังนี้

2.1 ระบบเครือข่ายคอมพิวเตอร์โดยทั่วไป

โอเพนซอร์ซ หรือ โอเพนซอร์ส (Open Source) คือการพัฒนาระบบใดระบบหนึ่งทางด้านคอมพิวเตอร์ด้วยเงื่อนไขที่ผู้สร้างสรรค์หรือผู้คิดค้นไม่ถือเอาสิทธิแต่เพียงผู้เดียวในการพัฒนาระบบนั้นๆ พร้อมทั้งเปิดเผยแหล่งต้นกำเนิดของระบบนั้น เช่น ซอฟต์แวร์โอเพนซอร์ซ (Open Source Software - OSS) คือ ซอฟต์แวร์ที่เปิดแผยหลักการหรือแหล่งที่มาของเทคโนโลยีของซอฟต์แวร์นั้นให้บุคคลภายนอกได้ใช้ ภายใต้เงื่อนไขบางประการที่เปิดโอกาสให้ผู้ใช้ทำการแก้ไขดัดแปลงและ เผยแพร่โปรแกรมต้นฉบับ (ซอร์สโค้ด) ได้ภายใต้เงื่อนไขทางข้อตกลงทางกฎหมาย เช่น จีพีแอล หรือ บีเอสดี ซึ่งปัจจุบันมีการกำหนดโดยกลุ่มผู้กำหนดโอเพนซอร์ซที่วางข้อกำหนดคำนิยาม 10 ประการในการกำหนดว่าเงื่อนไขที่เกี่ยวกับโอเพนซอร์ซ คือ

1. เงื่อนไขจะต้องไม่จำกัดผู้หนึ่งผู้ใด ในการจำหน่ายหรือการจ่ายแจกซอฟต์แวร์ให้เป็นส่วนใดส่วนหนึ่งของซอฟต์แวร์แบบแยกส่วนที่ประกอบด้วยซอฟต์แวร์จากหลาหลายแหล่ง และจะต้องไม่มีข้อกำหนดใด ๆ ที่เกี่ยวกันกับค่าใช้สิทธิหรือค่าสิทธิใด ๆ ในการจำหน่ายซอฟต์แวร์นั้น กล่าวคือให้มีการจ่ายแจกได้อย่างไม่มีการคิดค่าตอบแทน

2. โปรแกรมนั้นจะต้องเผยแพร่โปรแกรมต้นฉบับ (ซอร์สโค้ด) และจำต้องยินยอมให้มีการแจกจ่ายโปรแกรมต้นฉบับได้เช่นเดียวกันกับโปรแกรมที่อยู่ในรูปของการแปลงเป็นโปรแกรมที่ใช้งานได้แล้ว โดยหากแม้ไม่สามารถนำสินค้านั้นแจกจ่ายได้พร้อมโปรแกรมต้นฉบับ ก็จำต้องแหล่งแห่งที่อันเป็นสาธารณะที่สามารถเข้าถึงโปรแกรมต้นฉบับ ซอร์สโค้ดได้โดยปราศจากค่าใช้จ่ายหรือต้นทุนอื่นใด ทั้งนี้โปรแกรมต้นฉบับนั้นจะต้องอยู่ในรูปแบบที่นักโปรแกรมสามารถที่จะแก้ไขได้โดยจำต้องปราศจากซึ่งการเขียนโปรแกรมต้นฉบับในลักษณะที่เป็นการสับสนโดยเจตนา รวมทั้งต้องไม่มีลักษณะของโครงสร้างการทำงานของโปรแกรมต้นฉบับที่จำต้องมีตัวแปลภาษาเฉพาะ (translator) หรือมีส่วนที่ต้องนำเข้าสู่โปรแกรมในรูปแบบของโปรแกรมที่แปลงสภาพแล้ว (preprocessor)

3. เงื่อนไขจะต้องยินยอมให้สามารถทำการพัฒนาต่อยอดได้ ภายใต้เงื่อนไขการจ่ายแจกเช่นเดียวกันกับเงื่อนไขของโปรแกรมฉบับเริ่มต้น

4. เงื่อนไขอาจจะวางข้อกำหนดในการจำกัดเผยแพร่โปรแกรมต้นฉบับ ฉบับที่แก้ไขแล้วได้ต่อเมื่อเงื่อนไขนั้นได้ยินยอมให้มีการแจกจ่ายแพตช์ไฟล์ (Patch File) พร้อมโปรแกรมต้นฉบับเพื่อ

ประโยชน์ในการแก้ไขโปรแกรมนั้นในเวลาทำการสร้างโปรแกรม ทั้งเงื่อนไขจำต้องยินยอมให้มีการแจกจ่ายโปรแกรมนั้นที่ได้รับการแก้ไขโปรแกรมต้นฉบับได้ แต่เงื่อนไขนั้นอาจจะกำหนดให้โปรแกรมฉบับต่อยอดใช้ชื่อที่แตกต่างหรือใช้รุ่นที่แตกต่างจากโปรแกรมฉบับเริ่มต้นก็ได้

5. เงื่อนไขจะต้องไม่จำกัดเฉพาะบุคคลหรือกลุ่มบุคคลใด ๆ

6. เงื่อนไขต้องไม่จำกัดการใช้งานของโปรแกรมในรูปแบบใดรูปแบบหนึ่งอันเป็นการเฉพาะ

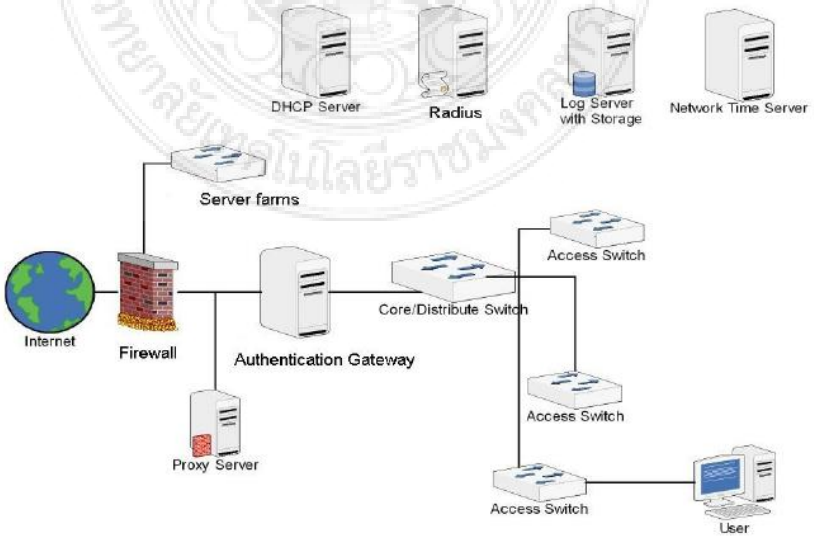
7. เงื่อนไขที่กำหนดจะต้องใช้กับทุกคนที่เกี่ยวข้องกับโปรแกรมนั้น

8. สิทธิใด ๆ ของโปรแกรมนั้นจะต้องไม่มีเงื่อนไขที่เฉพาะเจาะจงกับสินค้าหนึ่งสินค้าใด

9. เงื่อนไขต้องไม่กำหนดอันเกี่ยวกับข้อจำกัดในการใช้ร่วมกันกับโปรแกรมอื่น เช่น กำหนดให้ต้องใช้โปรแกรมดังกล่าวกับโปรแกรมแบบโอเพนซอร์ซเท่านั้น

10. ต้องไม่มีข้อกำหนดใด ๆ ในเงื่อนไขที่กำหนดให้ใช้เทคโนโลยีของใครหรือเทคโนโลยีแบบใดเป็นการเฉพาะ

ระบบการยืนยันตัวตน Authentication เป็นวิธีการที่ใช้ในการตรวจสอบผู้ที่มาใช้งานระบบเครือข่ายอินเทอร์เน็ต โดยระบบจะทำการตรวจสอบจาก username และ password ว่าถูกต้องหรือไม่ จุดประสงค์กลักของการ Authentication คือพิสูจน์ตัวบุคคล ว่าคนๆ นั้นที่เข้าใช้ระบบเครือข่ายอินเทอร์เน็ต คือใคร พร้อมทั้งทำการตรวจสอบสิทธิ์ว่าผู้ใช้งานระบบเครือข่ายอินเตอร์เน็ตของท่านนั้นมีสิทธิ์ใช้ได้นานเท่าไหร่ และสามารถ Upload หรือ Download ได้ด้วยความเร็วเท่าไหร่ ซึ่งระบบนั้นจะทำการตัดผู้ใช้ออกไปจากการให้บริการทันทีที่หมดเวลา อีกทั้งยังสามารถกำหนดเวลาและความเร็วได้ตามความเหมาะสมด้วย ต่อจากนั้นจะทำการบันทึกข้อมูลการใช้งานระบบเครือข่ายอินเทอร์เน็ต ซึ่งจุดประสงค์หลักของกระบวนการนี้เพื่อทำรายงานการใช้ระบบเครือข่ายอินเทอร์เน็ตจะทำการยืนยันบันทึกข้อมูลในการใช้งานระบบเครือข่ายอินเทอร์เน็ตไว้อย่างละเอียด โดยสามารถทำรายงานสรุป และสถิติต่างๆ ได้ตามความต้องการ



ภาพที่ 2-1 แผนภาพระบบเครือข่ายคอมพิวเตอร์โดยทั่วๆ ไป

ทำความรู้จักกับการพิสูจน์ตัวตน (Authentication) การพิสูจน์ตัวตน หนทางสู่ความปลอดภัยของข้อมูล

2.2 การพิสูจน์ตัวตน (Authentication)

การพิสูจน์ตัวตน คือขั้นตอนการยืนยันความถูกต้องของหลักฐาน (Identity) ที่แสดงว่าเป็นบุคคลที่กล่าวอ้างจริง ในทางปฏิบัติจะแบ่งออกเป็น 2 ขั้นตอน คือ

1. การระบุตัวตน (Identification) คือขั้นตอนที่ผู้ใช้แสดงหลักฐานว่าตนเองคือใครเช่น ชื่อผู้ใช้ (Username)

2. การพิสูจน์ตัวตน (Authentication) คือขั้นตอนที่ตรวจสอบหลักฐานเพื่อแสดงว่าเป็นบุคคลที่กล่าวอ้างจริง

การแสดงกระบวนการพิสูจน์ตัวตน ในขั้นแรกผู้ใช้จะทำการแสดงหลักฐานที่ใช้ในการพิสูจน์ตัวตนต่อระบบ ซึ่งในขั้นนี้คือการระบุตัวตน และในขั้นตอนต่อมาระบบจะทำการตรวจสอบหลักฐานที่ผู้ใช้นำมากล่าวอ้างซึ่งก็คือการพิสูจน์ตัวตน หลังจากระบบได้ทำการตรวจสอบหลักฐานเรียบร้อยแล้วถ้าหลักฐานที่นำมากล่าวอ้างถูกต้องจึงอนุญาตให้เข้าสู่ระบบได้ หากหลักฐานที่นำมากล่าวอ้างไม่ถูกต้องผู้ใช้จะถูกปฏิเสธจากระบบ (พ.อ.หญิงยุวดี พนาเวศร์ : 2553)

หลักฐานที่ผู้ใช้นำมากล่าวอ้างที่เกี่ยวกับเรื่องของความปลอดภัยนั้นสามารถจำแนกได้ 2 ชนิด

1. Actual Identity คือหลักฐานที่สามารถบ่งบอกได้ว่าในความเป็นจริงบุคคลที่กล่าวอ้างนั้นเป็นใคร

2. Electronic Identity คือหลักฐานทางอิเล็กทรอนิกส์ซึ่งสามารถบ่งบอกข้อมูลของบุคคลนั้นได้ แต่ละบุคคลอาจมีหลักฐานทางอิเล็กทรอนิกส์ได้มากกว่า 1 หลักฐาน ตัวอย่างเช่น บัญชีชื่อผู้ใช้

2.3 ลักษณะของการพิสูจน์ตัวตน

การพิสูจน์ตัวตนในปัจจุบันมีอยู่ 3 ลักษณะ ได้แก่

1. **สิ่งที่คุณรู้ (Something you know)** หมายถึง การใช้ User Name และ Password ในการเข้าสู่ระบบโดยทั่วไป เช่น การใช้อินเทอร์เน็ตด้วยการหมุน Modem จากบ้านเข้าสู่ ISP หรือการทำงานในบริษัทที่ต้องมีการ Log in โดยใช้ User Name และ Password ซึ่งการพิสูจน์ตัวตนในลักษณะนี้ถือเป็นแบบที่ระดับความปลอดภัยน้อยที่สุด เพราะถ้าใครรู้ User Name และ Password ของเราก็สามารถเข้าใช้งานระบบได้ทันที นอกจากนี้เรายังตรวจสอบตัวตน (Authenticity /Accountability) ของผู้ใช้ระบบไม่ได้ว่าใครเป็นใครอีกด้วย

2. **สิ่งที่คุณมี (Something you have)** เป็นการพิสูจน์ตัวตนในลักษณะที่เรียกว่า Multi Factor กล่าวคือ นอกจากจะมี Password ที่ต้องจำแล้วยังต้องใช้อุปกรณ์เสริมเข้ามาใช้ในการเข้าระบบด้วยเช่น บัตร ATM, RSA Token, Swipe Card, Access Card และ Smart Card เป็นต้น การตรวจสอบผู้ใช้ระบบโดยใช้สมาร์ทการ์ดเข้ามาช่วยนั้นจะช่วยตรวจสอบตัวตนของผู้ใช้งานระบบได้คล้าย ๆ กับที่ธนาคารตรวจสอบผู้ใช้งานบัตร ATM ของธนาคารว่าเป็นเจ้าของบัตรหรือไม่ เพราะบัตรควรจะต้องอยู่กับเจ้าของบัตรเท่านั้น และเจ้าของบัตรเท่านั้นที่ทราบรหัสของตน ผู้อื่นถึงแม้จะขโมยบัตรไปแต่ก็ไม่ทราบรหัสที่อยู่ในบัตร ทำให้ยากไปอีกขั้น หนึ่ง ในการเจาะเข้าสู่ระบบ

3. **สิ่งที่คุณเป็น (Something you are)** ก็คือการนำเทคโนโลยี Biometric เข้ามาใช้ในการตรวจสอบตัวตนโดยอาศัยอวัยวะที่คนเรามีอยู่ และมีลักษณะที่เป็นหนึ่งเดียวคือ ไม่ซ้ำกัน ได้แก่ ลายนิ้วมือ, ม่านตา หรือเสียง เป็นต้น การใช้งานสมาร์ทการ์ดสามารถร่วมกับระบบ Biometric ได้ กล่าวคือ เราสามารถเก็บลายนิ้วมือของคนลงไปใน Microchip ที่อยู่ในสมาร์ทการ์ดได้ด้วย ซึ่งจะเพิ่มระดับของความปลอดภัยมากขึ้น แต่ค่าใช้จ่ายก็จะสูงขึ้นเช่นกัน

กระบวนการพิสูจน์ตัวตนนั้นจะนำ 3 ลักษณะข้างต้นมาใช้ในการยืนยันหลักฐานที่นำมากล่าวอ้าง ทั้งนี้ขึ้นอยู่กับระบบวิธีการที่นำมาใช้เพียงลักษณะอย่างใดอย่างหนึ่ง (Single-factor Authentication) นั้นมีข้อจำกัดในการใช้ ตัวอย่างเช่น สิ่งที่คุณมี (Possession Factor) นั้นอาจจะสูญหายหรือถูกขโมยได้ สิ่งที่คุณรู้ (Knowledge Factor) อาจจะถูกดักฟัง เดา หรือขโมยจากเครื่องคอมพิวเตอร์ สิ่งที่คุณเป็น (Biometric Factor) จัดได้ว่าเป็นวิธีที่มีความปลอดภัยสูงอย่างไรก็ตามการที่จะใช้เทคโนโลยีนี้ได้นั้นจำเป็นต้องมีการลงทุนที่สูง เป็นต้น

ดังนั้นจึงได้มีการนำแต่ละคุณลักษณะมาใช้ร่วมกัน (Multi-factor Authentication) ตัวอย่างเช่น ใช้สิ่งที่คุณมีกับสิ่งที่คุณรู้มาใช้ร่วมกัน เช่น การใช้ลายมือชื่อร่วมกับการใช้บัตรเครดิต หรือการใช้รหัสผ่านร่วมกับการใช้บัตร ATM เป็นต้น การนำแต่ละลักษณะของการพิสูจน์ตัวตนมาใช้ร่วมกันมากกว่า 1 ลักษณะ จะช่วยเพิ่มประสิทธิภาพในการรักษาความปลอดภัยของข้อมูล

ข. การกำหนดสิทธิ์ (Authorization)

การกำหนดสิทธิ์ คือขั้นตอนในการอนุญาตให้แต่ละบุคคลสามารถเข้าถึงข้อมูลหรือระบบใดได้บ้าง ก่อนอื่นต้องทราบก่อนว่าบุคคลที่กล่าวอ้างนั้นคือใครตามขั้นตอนการพิสูจน์ตัวตนและต้องให้แน่ใจด้วยว่าการพิสูจน์ตัวตนนั้นถูกต้อง

ค. การเข้ารหัส (Encryption)

การเข้ารหัส คือการเก็บข้อมูลให้เป็นส่วนบุคคลจากบุคคลอื่นที่ไม่ได้รับอนุญาต ส่วนประกอบ 2 ส่วนที่สำคัญที่จะช่วยทำให้ข้อมูลนั้นเป็นความลับได้ก็คือ การกำหนดสิทธิ์และการพิสูจน์ตัวตนเพราะว่าก่อนการอนุญาตให้บุคคลที่กล่าวอ้างเข้าถึงข้อมูลหรือถอดรหัสข้อมูลนั้นต้องสามารถแน่ใจได้ว่าบุคคลที่กล่าวอ้างนั้นเป็นใครและได้รับอนุญาตให้สามารถเข้ามาดูข้อมูลได้หรือไม่

ในการเข้ารหัสนั้นวิธีการหนึ่งที่ทำได้คือการเข้ารหัสในรูปแบบของกุญแจลับ (Secret key) ซึ่งในการใช้คีย์รูปแบบนี้ต้องเฉพาะผู้ที่มีกุญแจลับนี้เท่านั้นที่สามารถรับข้อมูลที่เข้ารหัสแล้วได้

ง. การรักษาความสมบูรณ์ (Integrity)

การรักษาความสมบูรณ์ คือการรับรองว่าข้อมูลจะไม่ถูกเปลี่ยนแปลงหรือทำลายไปจากต้นฉบับ (source) ไม่ว่าจะเป็นโดยบังเอิญหรือดัดแปลงโดยเจตนาที่อาจส่งผลเสียต่อข้อมูล การคุกคามความสมบูรณ์ของข้อมูลคือการที่บุคคลที่ไม่ได้รับอนุญาตสามารถที่จะเข้าควบคุมการจัดการของข้อมูลได้

จ. การตรวจสอบ (Audit)

การตรวจสอบ คือการตรวจสอบหลักฐานทางอิเล็กทรอนิกส์ ซึ่งสามารถใช้ในการติดตามการดำเนินการเพื่อตรวจสอบความถูกต้องและแม่นยำ ตัวอย่างเช่นการตรวจสอบบัญชีชื่อผู้ใช้ โดยผู้ตรวจบัญชี ซึ่งการตรวจสอบความถูกต้องของการดำเนินการเพื่อให้แน่ใจว่าหลักฐานทางอิเล็กทรอนิกส์นั้นได้ถูกสร้างและสั่งให้ทำงานโดยบุคคลที่ได้รับอนุญาต และในการเชื่อมต่อเหตุการณ์เข้ากับบุคคลจะต้องทำการตรวจสอบหลักฐานของบุคคลนั้นด้วย ซึ่งถือเป็นหลักการพื้นฐานของขั้นตอนการทำงานของการพิสูจน์ตัวตนด้วย

การพิสูจน์ตัวตนจัดเป็นการตรวจสอบหลักฐานขั้นพื้นฐานที่สำคัญที่สุดใน 5 ระดับชั้นของการควบคุมความปลอดภัย ดังนั้นการพิสูจน์ตัวตนดีจะช่วยเพิ่มความมั่นคงปลอดภัยขั้นพื้นฐานให้กับระบบมากยิ่งขึ้น

ประเภทของการพิสูจน์ตัวตน (Authentication Types)

ส่วนประกอบพื้นฐานของการพิสูจน์ตัวตนสมบูรณ์แบ่งได้เป็น 3 ส่วน คือ

การพิสูจน์ตัวตน (Authentication) คือ ส่วนที่สำคัญที่สุดเพราะเป็นขั้นตอนแรกของการเข้าใช้ระบบ ผู้เข้าใช้ระบบต้องถูกยอมรับจากระบบว่าสามารถเข้าสู่ระบบได้ การพิสูจน์ตัวตนเป็นการตรวจสอบหลักฐานเพื่อแสดงว่าเป็นบุคคลนั้นจริง

การกำหนดสิทธิ์ (Authorization) คือ ข้อจำกัดของบุคคลที่เข้ามาในระบบ ว่าบุคคลคนนั้นสามารถทำอะไรกับระบบได้บ้าง

การบันทึกการใช้งาน (Accountability) คือ การบันทึกรายละเอียดของการใช้ระบบและรวมถึงข้อมูลต่างๆที่ผู้ใช้กระทำลงไปในระบบ เพื่อผู้ตรวจสอบจะได้ตรวจสอบได้ว่า ผู้ใช้ที่เข้ามาใช้บริการได้เปลี่ยนแปลงหรือแก้ไขข้อมูลในส่วนใดบ้าง

การพิสูจน์ตัวตนมีความสำคัญที่สุดกับการเข้าใช้ระบบ มีการแจกแจงชนิดของการพิสูจน์ตัวตนใช้กันอยู่ในปัจจุบันว่ามีอะไรบ้างและแต่ละชนิดมีลักษณะอย่างไร ดังนี้

1. **ไม่มีการพิสูจน์ตัวตน (No Authentication)**

ตามหลักการแล้วการพิสูจน์ตัวตนไม่มีความจำเป็น ถ้าเงื่อนไขต่อไปนี้เป็นจริง ข้อมูลเหล่านั้นเป็นข้อมูลสาธารณะ ที่อนุญาตให้ทุกคนเข้าใช้บริการและเปลี่ยนแปลงได้ หรือข้อมูลข่าวสารหรือแหล่งของข้อมูลนั้น ๆ สามารถเข้าถึงได้เฉพาะบุคคลที่ได้รับอนุญาตเท่านั้น

ข้อดี : ง่ายต่อการใช้งานและค่าใช้จ่ายต่ำ

ข้อเสีย : ความปลอดภัยของข้อมูลจะขึ้นอยู่กับผู้ใช้ว่าจะนำข้อมูลเหล่านั้นไปใช้ในทางที่ควรหรือไม่

2. **การพิสูจน์ตัวตนโดยใช้รหัสผ่าน (Authentication by Passwords)**

รหัสผ่านเป็นวิธีการที่ใช้มานานและนิยมใช้กันแพร่หลาย รหัสผ่านควรจำกัดให้เฉพาะผู้ใช้ที่มีสิทธิเท่านั้นที่ทราบ แต่ว่าในปัจจุบันนี้ การใช้แค่รหัสผ่านไม่มีประสิทธิภาพมากพอที่จะรักษาความมั่นคงปลอดภัยให้กับระบบคอมพิวเตอร์หรือระบบเครือข่ายคอมพิวเตอร์ เนื่องจากการตั้งรหัสผ่านที่ง่ายเกินไป และวิทยาการและความรู้ที่ก้าวหน้าทำให้รหัสผ่านอาจจะถูกขโมยโดยระหว่างการสื่อสารผ่านเครือข่ายได้

ข้อดี : สามารถใช้ได้กับทุกระบบ

ข้อเสีย : จะไม่ปลอดภัยเมื่อมีการส่งข้ามระบบเครือข่ายที่เป็นสาธารณะหรือไม่มีการเข้ารหัสข้อมูล

3. **การพิสูจน์ตัวตนโดยใช้ PIN (Personal Identification Number)**

เป็นรหัสลับส่วนบุคคลที่ใช้เป็นรหัสผ่านเพื่อเข้าสู่ระบบ ซึ่ง PIN ใช้อย่างแพร่หลายโดยเฉพาะการทำธุรกรรมทางด้านธนาคาร เช่นบัตร ATM และเครดิตการ์ดต่าง ๆ การใช้ PIN ทำให้มีความปลอดภัยในการสื่อสารข้ามระบบเครือข่ายสาธารณะมากขึ้น เนื่องจาก PIN จะถูกเข้ารหัสเอาไว้และจำเป็นต้องมีเครื่องมือที่สามารถถอดรหัสนี้ออกมาได้ เช่นฮาร์ดแวร์ที่ออกแบบมาโดยเฉพาะและถูกติดตั้งไว้ในเครื่องของผู้รับและผู้ส่งเท่านั้น

ข้อดี : ง่ายต่อการจำและความปลอดภัยค่อนข้างดีบัตร ATM) และสามารถสื่อสารข้ามเครือข่ายสาธารณะได้อย่าง

ข้อเสีย : ต้องใช้ฮาร์ดแวร์เฉพาะในการอ่าน PIN ไม่สามารถใช้กับต่างระบบกันได้ และ ราคาแพง

4. **การพิสูจน์ตัวตนโดยใช้ Password Authenticators หรือ Tokens**

Authenticator หรือ Token เป็นฮาร์ดแวร์พิเศษที่ใช้สร้าง รหัสผ่านซึ่งเปลี่ยนแปลงได้ (Dynamic Password) ในขณะที่กำลังเข้าสู่ระบบเครือข่าย มี 2 วิธี คือ ซิงโครนัสและอะซิงโครนัส การพิสูจน์ตัวตนแบบซิงโครนัส แบ่งออกเป็น 2 ประเภทตามลักษณะของการใช้งาน คือ

การพิสูจน์ตัวตนแบบซิงโครนัสโดยขึ้นอยู่กับสถานการณ์ (Event-synchronous Authentication) เมื่อผู้ใช้ต้องการที่จะเข้าสู่ระบบ ผู้ใช้จะต้องกด Token เพื่อให้ Token สร้างรหัสผ่านให้ จากนั้นผู้ใช้นำรหัสผ่านที่แสดงหลังจากกด Token ใส่ลงในฟอร์ม เพื่อเข้าสู่ระบบ ระบบ

จะทำการตรวจสอบกับเซิร์ฟเวอร์ก่อน ว่ารหัสผ่านที่ใส่มีอยู่ในเซิร์ฟเวอร์จริง จึงจะยินยอมให้ผู้ใช้เข้าสู่ระบบ

การพิสูจน์ตัวตนแบบซิงโครนัสโดยขึ้นอยู่กับเวลา (Time-synchronous Authentication) เป็นวิธีการที่สร้างรหัสผ่านโดยมีการกำหนดช่วงระยะเวลาการใช้งาน โดยปกติแล้วรหัสผ่านจะถูกเปลี่ยนทุก ๆ หนึ่ง นาที การสร้างรหัสผ่านจะเป็นไปอย่างต่อเนื่อง ทำให้บางครั้งรหัสผ่านที่สร้างออกมาอาจจะซ้ำกันกับรหัสผ่านตัวอื่นที่เคยสร้างมาแล้วก็ได้ เมื่อผู้ใช้ต้องการเข้าสู่ระบบก็ใส่รหัสผ่านและเวลาที่รหัสผ่านตัวนั้นถูกสร้างขึ้นมา (รหัสผ่านจะถูกสร้างขึ้นมาจาก Token) ลงในฟอร์ม เพื่อเข้าสู่ระบบ ระบบจะทำการตรวจสอบเวลาและรหัสผ่านที่ผู้ใช้ใส่ลงไป กับเซิร์ฟเวอร์ว่ารหัสผ่านที่ใส่ตรงกับเวลาที่ Token สร้าง และมีอยู่ในเซิร์ฟเวอร์จริง จึงยินยอมให้ผู้ใช้เข้าสู่ระบบ ข้อดี : มีความปลอดภัยมากกว่าการใช้การจำรหัสผ่าน แบบธรรมดา ไม่ต้องใช้เครื่องอ่านการ์ด และผู้ที่ละเมิดเข้ามาไม่สามารถจะเข้ามาจู่โจมได้

ข้อเสีย : การใช้งานยุ่งยากกว่าแบบจำรหัสผ่าน และAuthenticator เป็นวัตถุจึงง่ายต่อการสูญหาย และการถูกขโมยได้

การพิสูจน์ตัวตนแบบอะซิงโครนัส หรือเรียกอีกอย่าง หนึ่ง ว่า Challenge-response ถูกพัฒนาขึ้น เป็นลำดับแรก ๆ ของระบบการใช้ รหัสผ่านซึ่งเปลี่ยนแปลงได้ ซึ่งถือได้ว่าเป็นการป้องกันการจู่โจมที่ปลอดภัยที่สุด เพราะเนื่องจากว่าเมื่อผู้ใช้ต้องการจะเข้าสู่ระบบ ผู้ใช้จะต้องทำการร้องของไปยังเซิร์ฟเวอร์ จากนั้นเซิร์ฟเวอร์ก็จะส่ง Challenge String มาให้ผู้ใช้ เพื่อให้ผู้ใช้ใส่ลงใน Token ที่ผู้ใช้ถืออยู่ จากนั้น Token จะทำการคำนวณรหัสผ่านออกมาให้ผู้ใช้ ผู้ใช้จึงสามารถนำรหัสผ่านนั้นใส่ลงในฟอร์มเพื่อเข้าสู่ระบบได้

ข้อดี : มีความปลอดภัยมากกว่าการใช้การจำรหัสผ่าน แบบธรรมดา ไม่ต้องใช้เครื่องอ่านการ์ด และเป็นวิธีการป้องกันที่ดีที่สุดเมื่อเปรียบเทียบกับวิธีการใช้การพิสูจน์ตัวตนโดย
ใช้ Password Authenticators หรือ Tokens

ข้อเสีย : การใช้งานยุ่งยากกว่าแบบจำรหัสผ่าน Authenticator เป็นวัตถุจึงง่ายต่อการสูญหาย และการถูกขโมยได้ไม่สามารถป้องกันผู้ที่ ละเมิดเข้ามาในระบบได้ และ การใช้งานค่อนข้างยุ่งยากกว่าวิธีการใช้ รหัสผ่านซึ่งเปลี่ยนแปลงได้ (Dynamic Password) วิธีอื่น

การพิสูจน์ตัวตนแบบซิงโครนัสทั้งไคลเอ็นต์และเซิร์ฟเวอร์จะมีรหัสผ่านเก็บเอาไว้ แต่แบบอะซิงโครนัส ไคลเอ็นต์จะต้องติดต่อเซิร์ฟเวอร์ก่อน ก่อนจะได้รับรหัสผ่านจริง ทำให้การพิสูจน์ตัวตนแบบอะซิงโครนัสมีขั้นตอนที่ซับซ้อนกว่าแบบซิงโคนัส

5. **การพิสูจน์ตัวตนโดยใช้ลักษณะเฉพาะทางชีวภาพของแต่ละบุคคล (Authentication by Biometric traits)**

ลักษณะทางชีวภาพของแต่ละบุคคลเป็นลักษณะเฉพาะและลอกเลียนแบบกันไม่ได้ การนำมาใช้ในการพิสูจน์ตัวตนจะเพิ่มความน่าเชื่อถือได้มากขึ้นเช่นการใช้ลายนิ้วมือ เสียง ม่านตา เป็น

ต้น จึงมีการนำเทคโนโลยีนี้มาช่วยในการพิสูจน์ตัวตน เพื่อเพิ่มความปลอดภัยก่อนเข้าสู่ระบบ เช่น การใช้ควบคู่กับการใช้รหัสผ่าน ในขั้นตอนของการเก็บหลักฐานทางชีวภาพ จากตัวอย่างของรูปที่ 2 ในขั้นแรกระบบจะทำการเก็บภาพของเรตินาจากบุคคลที่ถือ Token การ์ดหรือสมาร์ทการ์ด จากนั้นจะนำภาพเรตินาที่ได้มาแยกแยะเพื่อหาลักษณะเด่นของแต่ละบุคคลเพื่อไม่ให้ซ้ำกับบุคคลอื่น แล้วเก็บไว้เป็น Template ซึ่ง Template ที่ได้จะถูกบันทึกเป็นกุญแจคู่กับรหัสผ่านที่มีอยู่ใน Token การ์ด หรือสมาร์ทการ์ดของแต่ละบุคคล ในขั้นตอนของการตรวจสอบหลักฐาน ผู้ใช้ที่ถือ Token การ์ด หรือสมาร์ทการ์ด จะนำบัตรมาผ่านเครื่องอ่านบัตรและแสดงเรตินาให้เครื่องเก็บภาพ เมื่อเครื่องอ่านบัตร อ่านค่าเลขที่ได้จากบัตรแล้ว ก็จะนำไปหากุญแจ ซึ่งในขณะเดียวกันภาพเรตินาที่เครื่องเก็บไว้ได้ ก็จะนำไปแยกแยะเพื่อหาลักษณะเด่น แล้วเก็บค่าไว้เป็น Template และนำ Template ที่ได้ไปตรวจสอบกับ Template ที่เก็บไว้เพื่อหากุญแจ และนำกุญแจที่ได้มาเปรียบเทียบกันว่าตรงกันหรือไม่ ถ้าตรงกันก็แสดงว่าผู้ที่ถือบัตรกับผู้ใช้เป็นคนเดียวกัน จึงอนุญาตให้เข้าสู่ระบบได้

ข้อดี : มีความปลอดภัยสูงเพราะเลียนแบบกันได้ยาก

ข้อเสีย : ระบบมีความซับซ้อนสูง ยังไม่ได้รับความนิยมกันอย่างแพร่หลาย และ ค่าใช้จ่ายสูง

6. **การพิสูจน์ตัวตนโดยใช้รหัสผ่านที่ใช้เพียงครั้งเดียว One-Time Password (OTP)** ถูกพัฒนาขึ้นเพื่อหลีกเลี่ยงปัญหาที่เกิดจากการใช้รหัสผ่านเพียงตัวเดียวซ้ำ ๆ กัน OTP จะทำให้ระบบมีความปลอดภัยมากขึ้น เพราะรหัสผ่านจะถูกเปลี่ยนทุกครั้งก่อนที่ผู้ใช้จะเข้าสู่ระบบ

การทำงานของ OTP คือเมื่อผู้ใช้ต้องการจะเข้าใช้ระบบ ผู้ใช้จะทำการร้องขอไปยังเซิร์ฟเวอร์ จากนั้นเซิร์ฟเวอร์จะส่ง Challenge String กลับมาให้ผู้ใช้ จากนั้นผู้ใช้จะนำ Challenge String และรหัสลับที่มีอยู่กับตัวของผู้ใช้นำไปเข้าแฮชฟังก์ชันแล้วออกมาเป็นค่า Response ผู้ใช้ก็จะส่งค่านั้นกลับไปยังเซิร์ฟเวอร์ เซิร์ฟเวอร์จะทำการตรวจสอบค่าที่ผู้ใช้ส่งมาเปรียบเทียบกับค่าที่เซิร์ฟเวอร์เองคำนวณได้ โดยเซิร์ฟเวอร์ก็ใช้วิธีการคำนวณเดียวกันกับผู้ใช้ เมื่อได้ค่าที่ตรงกันเซิร์ฟเวอร์ก็จะยอมรับให้ผู้ใช้เข้าสู่ระบบ

ข้อดี : ทำให้การเดาหรือขโมยรหัสผ่านเป็นไปได้ยาก

ข้อเสีย : ไม่สะดวกต่อการใช้งาน เพราะผู้ใช้ต้องจำรหัสผ่านหลายตัว และ ถ้าผู้ใช้จำรหัสผ่านไม่ได้ หรือ ทำรหัสผ่านสูญหาย ก็ไม่สามารถเข้าใช้ระบบได้

7. **การพิสูจน์ตัวตนโดยการเข้ารหัสโดยใช้กุญแจสาธารณะ (Public-key cryptography)**

เป็นการรักษาความปลอดภัยของข้อมูลระหว่างการส่งข้ามเครือข่ายวิธีหนึ่งที่นิยมใช้กันอยู่ในปัจจุบัน การเข้ารหัสแบบคู่รหัสกุญแจนี้จะมีความปลอดภัยมากกว่าการเข้ารหัสข้อมูลแบบธรรมดา แต่ก็ไม่ได้หมายความว่าการเข้ารหัสแบบคู่รหัสกุญแจนี้จะเป็นวิธีที่เหมาะสมที่สุดของวิธีการเข้ารหัส ทั้งนี้ขึ้นอยู่กับประเภทงานของแต่ละองค์กรหรือบุคคล

การเข้ารหัสโดยใช้กุญแจสาธารณะ ประกอบไปด้วยกุญแจ 2 ชนิด ที่ต้องใช้คู่กันเสมอในการเข้ารหัสและถอดรหัส คือ กุญแจสาธารณะ (Public Key) เป็นกุญแจที่ผู้สร้างจะส่งออกไปให้ผู้ใช้อื่น ๆ ทราบหรือเปิดเผยได้ กุญแจส่วนตัว (Private Key) เป็นกุญแจที่ผู้สร้างจะเก็บไว้ โดยไม่เปิดเผยให้คนอื่นรู้

กระบวนการของการเข้ารหัสแบบคู่รหัสกุญแจ มีดังนี้

1. ผู้ใช้แต่ละคนจะสร้างคู่รหัสกุญแจของตัวเองขึ้นมา เพื่อใช้สำหรับการเข้าการถอดรหัส
2. กุญแจสาธารณะจะถูกส่งออกไปยังผู้ใช้คนอื่น ๆ แต่กุญแจส่วนตัวจะถูกเก็บที่ตนเอง
3. เมื่อจะส่งข้อมูลออกไปหาผู้ใช้คนใด ข้อมูลที่ส่งจะถูกเข้ารหัสด้วยกุญแจสาธารณะ ก่อนถูกส่งออกไป
4. เมื่อผู้รับได้รับข้อความแล้วจะใช้กุญแจส่วนตัวซึ่งเป็นคู่รหัสกันถอดรหัสออกมา

การเข้ารหัสโดยใช้กุญแจสาธารณะสามารถใช้ได้ทั้งในการเข้ารหัส (Encryption) และการพิสูจน์ตัวตน (Authentication)

การประยุกต์ใช้ในการเข้ารหัสข้อมูล (Encryption) เป็นการนำข้อมูลที่จะส่งไปยังผู้รับมาเข้ารหัสด้วยกุญแจสาธารณะของผู้รับ และเมื่อผู้รับได้รับข้อความนั้นแล้วจะถอดรหัสออกมาด้วยกุญแจส่วนตัว จึงจะเห็นได้ว่ามีเพียงผู้รับเท่านั้นที่จะสามารถถอดรหัสออกมาได้

การประยุกต์ใช้ในการพิสูจน์ตัวตน (Authentication) เป็นการนำข้อมูลที่ผู้ส่งต้องการส่งมาเข้ารหัสด้วยกุญแจส่วนตัวของผู้ส่ง แล้วนำข้อมูลนั้นส่งไปยังผู้รับ ซึ่งผู้รับจะใช้กุญแจสาธารณะซึ่งเป็นคู่รหัสกันถอดรหัสออกมา ผู้รับก็สามารถรู้ได้ว่าข้อความนั้นถูกส่งมาจากผู้ส่งคนนั้นจริง ถ้าสามารถถอดรหัสข้อมูลได้อย่างถูกต้อง

ข้อดี : การจัดการกุญแจทำได้ปลอดภัย เพราะ ใช้กุญแจในการเข้ารหัส และถอดรหัสต่างกัน 2.สามารถระบุผู้ใช้โดยการใช้ร่วมกับลายมือชื่ออิเล็กทรอนิกส์

ข้อเสีย :ใช้เวลาในการเข้าและถอดรหัสค่อนข้างนานเพราะต้องใช้การคำนวณอย่างมากและต้องใช้ระบบที่สนับสนุนการทำงาน

8. **การพิสูจน์ตัวตนโดยการใช้ลายเซ็นอิเล็กทรอนิกส์ (Digital Signature)**

เป็นการนำหลักการของการทำงานของระบบการเข้ารหัสแบบใช้คู่รหัสกุญแจเพื่อการพิสูจน์ตัวตนมาประยุกต์ใช้ ระบบของลายเซ็นดิจิตอลสามารถแบ่งเป็นขั้นตอนได้ดังนี้

เมื่อผู้ใช้ต้องการจะส่งข้อมูลไปยังผู้รับ ข้อมูลนั้นจะถูกนำไปเข้าฟังก์ชันทางคณิตศาสตร์ที่เรียกว่า แฮชฟังก์ชัน ได้เมสเซจไดเจสต์ (Message Digest) ออกมา

การใช้กุญแจส่วนตัวเข้ารหัสข้อมูล หมายถึงว่าผู้ส่งได้ลงลายเซ็นดิจิตอล ยินยอมที่จะให้ผู้รับ สามารถทำการตรวจสอบด้วยกุญแจสาธารณะของผู้ส่งเพื่อพิสูจน์ตัวตนของผู้ส่งได้ การตรวจสอบข้อมูลว่าถูกส่งมาจากผู้ส่งคนนั้นจริงในด้านผู้รับ โดยการนำข้อมูลมาผ่านแฮชฟังก์ชันเพื่อคำนวณหาค่าเมสเซจไดเจสต์ และถอดรหัสลายเซ็นอิเล็กทรอนิกส์ด้วยกุญแจสาธารณะของผู้ส่ง

ถ้าสามารถถอดได้อย่างถูกต้อง จะเป็นการยืนยันข้อมูลจากผู้ส่งคนนั้นจริง และถ้าข้อมูลเมสเซจไดเจสต์ที่ได้จากการถอดรหัสเท่ากันกับค่าเมสเซจไดเจสต์ในตอนต้นที่ทำการคำนวณได้ จะถือว่าข้อมูลดังกล่าวนั้นถูกต้อง

ลายเซ็นอิเล็กทรอนิกส์นิยมนำไปใช้ในระบบรักษาความปลอดภัยในการชำระเงินผ่านระบบอินเตอร์เนต ซึ่งในปัจจุบันนี้การทำธุรกรรมการเงินอิเล็กทรอนิกส์ได้รับความนิยมเป็นอย่างมาก

ข้อดี : สามารถระบุตัวผู้ส่งได้ชัดเจน ป้องกันข้อมูลถูกแก้ไขระหว่างการส่งได้ หรือสามารถตรวจสอบข้อมูลได้ว่าผ่านการแก้ไขมาหรือไม่

ข้อเสีย : ใช้เวลาในการเข้าและถอดรหัสค่อนข้างนาน เพราะต้องใช้การคำนวณอย่างมาก

9. **การพิสูจน์ตัวตนโดยใช้การถาม-ตอบ (zero-knowledge proofs)**

เป็นวิธีการพิสูจน์ตัวตนโดยใช้การถาม-ตอบ เมื่อผู้ใช้เข้ามาในระบบแล้ว ระบบจะแน่ใจได้อย่างไรว่าผู้ใช้คนนั้น เป็นคนที่ได้รับอนุญาตให้เข้ามาใช้ระบบได้จริง การใช้ชื่อผู้ใช้และรหัสผ่าน ในปัจจุบันนี้ไม่มีความปลอดภัยเพียงพอต่อการเข้าใช้ระบบ เนื่องจากความรู้และวิทยาการที่ก้าวหน้า ทำให้เกิดผู้ที่ต้องการจะเข้ามาละเมิดระบบต่าง ๆ มีมากขึ้น ทำให้ชื่อผู้ใช้และรหัสผ่าน อาจจะถูกลักลอบดักข้อมูลระหว่างการสื่อสารกันได้

การที่จะทำให้ระบบมั่นใจได้ว่า ผู้ที่เข้าไปในระบบผู้นั้นเป็นผู้ที่ได้รับอนุญาตจริง นั่นก็คือระบบจะใช้การถาม-ตอบ ซึ่งคำถามและคำตอบเหล่านี้ ผู้ใช้จะเป็นคนสร้างคำถามและคำตอบขึ้นมาเอง จากนั้นจะส่งให้กับเซิร์ฟเวอร์ ซึ่งคำถาม-คำตอบที่ผู้ใช้สร้างขึ้นมา ผู้ใช้เท่านั้นจะเป็นคนที่ทราบคำตอบของแต่ละคำถามที่ถูกสร้าง และเมื่อผู้ใช้คนนั้น ๆ เข้าสู่ระบบได้ ระบบจะถามสุ่มคำถามเหล่านั้นที่ผู้ใช้คนนั้น ๆ สร้างขึ้นมา ถามผู้ใช้คนนั้น ๆ ก่อนที่จะยอมให้เข้าใช้ระบบได้จริง การให้ใช้ระบบได้จริงจะได้รับการยินยอมก็ต่อเมื่อการตอบคำตอบที่ผู้ใช้ตอบ นั้นสัมพันธ์กับคำตอบที่มีอยู่ในเซิร์ฟเวอร์

วิธีการพิสูจน์ตัวตนวิธีนี้ เป็นวิธีการที่ต้องใช้ความรู้ขั้นสูงในการนำมาใช้ เนื่องจากระบบจะใช้การเรียนรู้จากข้อมูลที่ได้รับ อาจจะเรียกระบบนี้ได้ว่าเป็นการนำความรู้ด้าน AI (Artificial Intelligence) มาใช้

ข้อดี : ความปลอดภัยค่อนข้างสูง เพราะคำถามและคำตอบจะมีเพียงผู้ใช้ และเซิร์ฟเวอร์เท่านั้นที่ทราบ

ข้อเสีย : ความปลอดภัยค่อนข้างสูง เพราะคำถามและคำตอบจะมีเพียงผู้ใช้ และเซิร์ฟเวอร์เท่านั้นที่ทราบ และความซับซ้อนของระบบเพิ่มขึ้นตามความฉลาดของระบบ

โพรโตคอลในการพิสูจน์ตัวตน(Authentication Protocol)

ในระบบเครือข่ายแบบเปิดหรืออินเตอร์เน็ต การพิสูจน์ตัวตนถือได้ว่าเป็นกระบวนการเริ่มต้นและมีความสำคัญที่สุดในการปกป้องเครือข่ายให้ปลอดภัย โพรโตคอลในการพิสูจน์ตัวตน คือ โพรโตคอลการสื่อสารที่มีกระบวนการพิสูจน์ตัวตนรวมอยู่ในชุดโพรโตคอล

โพรโตคอลหลักของการพิสูจน์ตัวตนที่นิยมใช้อย่างแพร่หลายบนอินเตอร์เน็ตในปัจจุบัน ประกอบไปด้วย

Secure Socket Layer (SSL)

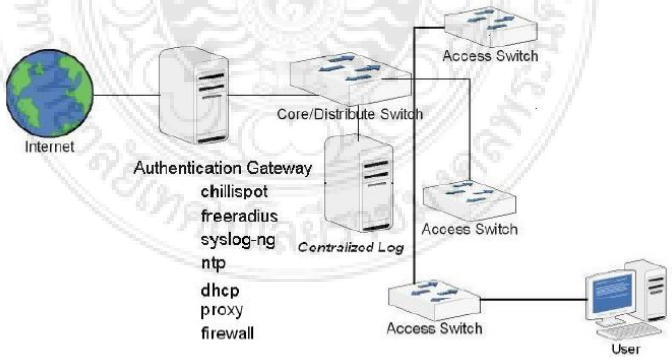
Secure Shell (SSH)

Internet Security (IPSEC)

Kerberos

การรักษาความมั่นคงปลอดภัยของระบบคอมพิวเตอร์ หรือ ระบบเครือข่ายคอมพิวเตอร์เป็นสิ่งที่ควรตระหนักเป็นอย่างยิ่งในปัจจุบัน เพราะโลกในยุคปัจจุบันเป็นโลกแห่งข้อมูลข่าวสาร การเก็บรักษาข้อมูลให้ปลอดภัยจึงเป็นสิ่งสำคัญกับตัวบุคคลและองค์กร เพราะฉะนั้นการที่จะอนุญาตให้บุคคลใดบุคคลหนึ่งสามารถเข้าถึงข้อมูลจึงเป็นสิ่งที่ควรระมัดระวัง เพราะข้อมูลบางอย่างของบุคคลและองค์กรมีความสำคัญและไม่สามารถเปิดเผยต่อบุคคลภายนอกได้

การพิสูจน์ตัวตนจึงมีความสำคัญ เนื่องจากว่าการที่บุคคลใดบุคคลหนึ่งจะเข้าสู่ระบบได้จะต้องได้รับการยอมรับว่าได้รับอนุญาตจริง การตรวจสอบหลักฐานจึงเป็นขั้นตอนแรกก่อนอนุญาตให้เข้าสู่ระบบ การยืนยันตัวตนยิ่งมีความซับซ้อนมาก นั่นก็หมายถึงว่าความปลอดภัยของข้อมูลก็มีมากขึ้นด้วย องค์กรต่าง ๆ จะต้องกระทำสิ่งที่จะเป็นในการปกป้องข้อมูลที่สำคัญ ไม่เพียงแค่ป้องกันการบุกรุกเท่านั้น แต่จะต้องหลีกเลี่ยงผลกระทบที่อาจตามมา ดังนั้นถ้าหากว่าข้อมูลได้รับการป้องกันนั้นมีความสำคัญอย่างยิ่งต่อความสำเร็จขององค์กร ระบบในการตรวจสอบผู้ใช้งานที่มีประสิทธิภาพเป็นสิ่งที่จะต้องพิจารณาอย่างยิ่ง โดยที่มีอยู่หลายวิธีให้เลือกใช้กันในปัจจุบัน ดังนั้นการเลือกวิธีที่นำมาใช้นั้นจะต้องเป็นวิธีที่ให้ความมั่นใจได้เป็นอย่างดี การพิจารณาจะต้องไม่เพียงแค่จะต้องสามารถทำงานได้ในปัจจุบันเท่านั้น แต่วิธีการที่เลือกระบบรักษาความปลอดภัยจะต้องสามารถทำงานได้ดีในอนาคตอีกด้วย



ภาพที่ 2-2 แผนภาพระบบเครือข่ายคอมพิวเตอร์ที่ติดตั้งซอฟต์แวร์ที่ตัวอุปกรณ์ Authentication Gateway

2.4 งานวิจัยที่เกี่ยวข้อง

นริศ รังษีนพมาศ (2537) การรักษาความปลอดภัยของข้อมูลด้วยการเข้ารหัสลับตามมาตรฐาน EDS(Data Ekncyption Standard) ที่มีโหมดในการเข้ารหัสทั้ง 4 โหมด คือ ECB (Electronic Codebook), CBC (Cipher Block Chaining), CFB (Cipher Feedback) และ OFB (Output Feedback)ในคาร์ดเดียวกัน ซึ่งแต่ละโหมดจะมีคุณสมบัติที่ดีเหมาะสำหรับชนิดของข้อมูลที่ แตกต่างกัน และยังได้นำเสนอวิธีรับรองข้อความที่ต้องการลงทะเบียนไฟล์(File Registration) ก่อน เพื่อป้องกันข้อมูลถูกแก้ไขในขณะที่ถูกเก็บอยู่ ในที่ที่ไม่มีการควบคุมการเข้าถึง โดยวิธีนี้จะสร้างรหัสรับรองข้อความ(Authentication Code) จากไซเฟอร์เท็กซ์แทนการสร้างจากเพลนเท็กซ์ทำให้มีความปลอดภัยมากขึ้น อย่างไรก็ตามวิธีการที่นำเสนอนี้จะใช้เวลาในการรับรองข้อความสูงขึ้น คาร์ดดังกล่าวจะใช้ร่วมกับเครื่องไมโครคอมพิวเตอร์ โดยผู้วิจัยได้พัฒนาโปรแกรมควบคุมการทำงานและโปรแกรมอรรถประโยชน์สำหรับแสดงเวลาที่ใช้ในการเข้ารหัสโหมดต่าง ๆ และสามารถดูข้อมูลเปรียบเทียบก่อนและหลังจากเข้ารหัส นอกจากนี้ยังสามารถพิมพ์ข้อมูลซึ่งประกอบด้วยอักขระพิเศษออกทางเครื่องพิมพ์เพื่ออำนวยความสะดวกแก่ผู้ใช้งาน

ปรัชญา ไชยเมือง และ สมนึก พ่วงพรพิทักษ์ (2553) การยืนยันตัวตนของผู้ใช้กับเว็บแอปพลิเคชั่นส่วนใหญ่อาศัย Username/Password โดย Password แม้ว่าจะสามารถถูกดักจับและพบการรั่วไหลได้หลายทาง จึงได้มีการเสนอวิธีแก้ปัญหานี้มาก่อน เช่น Aradiom SolidPass AuthAnvil, FiveBarGate, RSA SecurID ที่อาศัย “User Possession” เพิ่มเข้าไปอีกปัจจัยหนึ่ง อย่างไรก็ตาม การแก้ปัญหาตามข้อเสนอดังกล่าว ยังมีจุดอ่อนอยู่หลายประการ ในงานวิจัยนี้ จึงวิเคราะห์จุดอ่อนดังกล่าว และได้ออกแบบพร้อมพัฒนาโปรแกรม วิธีแก้ปัญหาใหม่ โดยอาศัยเทคโนโลยีเว็บเซอร์วิสและเจทูเอ็มอี เพื่อทำให้กระบวนการยืนยันตัวตนในเว็บแอปพลิเคชั่นดีขึ้น โดยใช้การยืนยันตัวตนด้วยปัจจัยสองลักษณะร่วมกับเทคนิคการท้าทายและตอบสนอง (challenge-respond) และ HOTP ทำให้แนวคิดในการแก้ปัญหาแบบใหม่ มีประสิทธิผลสูงกว่า มีต้นทุนที่ถูกกว่าและง่ายกว่าในการติดตั้งใช้งาน

มาริต ปรัชญพฤทธิ์ (2545) งานวิจัยที่จัดทำขึ้นนี้มีวัตถุประสงค์เพื่อที่จะพัฒนาระบบเทคโนโลยีสารสนเทศ RADIUS ของผู้ให้บริการอินเตอร์เน็ต โดยมีขั้นตอนของการปฏิบัติงานและข้อมูล เฉพาะของเอเซียเน็ตสาขานครปฐมเป็นกรณีศึกษา เหตุผลประการสำคัญในการพัฒนาระบบสารเทศนี้ขึ้นมา เพื่อเพิ่มความสามารถในการทำงานให้กับระบบ RADIUS งานวิจัยนี้ได้ศึกษาและพัฒนาระบบตามหลักการของ System Development Life Cycle (SDLC) เพื่อที่จะจัดทำโปรแกรมต้นแบบของระบบ RADIUS 1.6 เพื่อที่จะเพิ่มขีด ความสามารถในการทำงานที่ไม่มีอยู่ใน Livingston RADIUS 1.6 แต่เป็นความสามารถที่ จำเป็นต้องใช้ในงานที่เกี่ยวข้องกับผู้ให้บริการอินเตอร์เน็ต ในการพัฒนาระบบ ดังกล่าวนี้ประกอบด้วยการเก็บรวบรวมข้อมูลการศึกษาการปฏิบัติในระบบงานที่เสนอไป การ ใช้ flowchart ในการวิเคราะห์และออกแบบระบบและการเก็บข้อมูลในเท็กส์ไฟล์ โดยใช้ GNU C++(GCC) ในการพัฒนาโปรแกรม และใช้ Perl สำหรับการแสดงผลในการ

เชื่อมต่อกับฐาน ข้อมูลและการแสดงผลในรูปแบบของ HTML ผลจากการวิจัยนี้ทำให้ได้โปรแกรมประยุกต์ที่ใช้ในการบริหารจัดการลูกค้าของ ผู้ให้บริการอินเตอร์เน็ต โดยที่ระบบจะช่วยให้ผู้ใช้สามารถบริหารจัดการระบบ RADIUS ได้ อย่างมีประสิทธิภาพ ทั้งนี้ระบบยังช่วยทำงานเบื้องหลังเช่น การตัดการเชื่อมต่อ อัตโนมัติ และการบริหารจัดการรายชื่อลูกค้า วิทยานิพนธ์นี้มีข้อเสนอแนะสำหรับการ นำไปพัฒนาต่อในการเพิ่มขีดความสามารถอื่น ๆ ที่ต้องใช้ในระบบอื่น ๆ เช่น การเข้าใช้งานเป็นช่วงเวลา หรือ การเก็บข้อมูลโดยใช้ฐานข้อมูลเพื่อที่จะทำให้ระบบรองรับผู้ใช้ งานได้มากขึ้น

อนงค์พร ไศลวรากุล (2545) ในปัจจุบันมีการนำส่วนประกอบซอฟต์แวร์มาใช้ในการสร้างและพัฒนาระบบงานซอฟต์แวร์อย่างแพร่หลาย ซึ่งสถาปัตยกรรมเอ็นเตอร์ไพรส์จาวาบีนส์เป็นแนวคิดหนึ่งของการนำส่วนประกอบซอฟต์แวร์มาใช้ ปัญหาหนึ่งของการใช้ส่วนประกอบซอฟต์แวร์คือการรักษาความมั่นคงในการเรียกใช้ส่วนประกอบซอฟต์แวร์ ซึ่งการรักษาความมั่นคงนี้โดยส่วนมากจะเกี่ยวข้องกับการพิสูจน์ตัวจริงผู้เรียกใช้ และการจำกัดสิทธิในการเรียกใช้ ดังนั้นวิทยานิพนธ์นี้จึงเสนอแนวทางในการรักษาความมั่นคงด้านการพิสูจน์ตัวจริงและการจำกัดสิทธิในการเรียกใชส่วนประกอบซอฟต์แวร์ โดยการนำผลิตภัณฑ์เอ็นเตอร์ไพรส์จาวาบีนส์เซิฟเวอร์ มาเป็นกรณีศึกษา และนำข้อกำหนดซีซีมาสร้างเป็นโครงร่างหัวข้อในการเปรียบเทียบผลิตภัณฑ์ทั้งสอง ซึ่งจากการวิเคราะห์เปรียบเทียบทำให้พบข้อดีและข้อด้อยของผลิตภัณฑ์ จึงได้นำเสนอแนวทางด้านรักษาความมั่นคงให้สำหรับผู้พัฒนาเอ็นเตอร์ไพรส์จาวาบีนส์เซิฟเวอร์และผู้ใช้หรือผู้พัฒนาเอ็นเตอร์ไพรส์บีน เพื่อช่วยเสริมความมั่นคงในการใช้เทคโนโลยีเอ็นเตอร์ไพรส์จาวาบีนส์

บทที่ 3
การศึกษาระบบงานปัจจุบัน

ในการศึกษาระบบงานมีความมุ่งหมายเพื่อทำการพัฒนาระบบการยืนยันตัวตนโดยใช้เทคโนโลยีฟรีแวร์ ให้มีการทำงานที่ง่ายและสะดวกแก่การทำงาน ซึ่งผู้ใช้งานระบบในหน่วยงานสามารถติดตั้งระบบด้วยตัวเองได้ โดยการจัดทำเป็นการวิจัยและพัฒนาระบบงานการยืนยันตัวตนโดยใช้เทคโนโลยีฟรีแวร์ ซึ่งมีการค้นคว้าและหาข้อมูลที่เกี่ยวกับระบบงาน โดยการสอบถามลักษณะงานที่ใช้งานในปัจจุบัน และปัญหาต่างๆ ที่เกิดขึ้น โดยมีขั้นตอนการวิจัยและพัฒนาระบบงานบริการดังนี้

3.1 ขั้นเตรียมการ

ผู้ศึกษาได้มีการสอบถามผู้ที่เกี่ยวข้องกับระบบงาน ในด้านความต้องการระบบงานของผู้ใช้งานระบบ จึงได้ทำการเตรียมการ ดังนี้

3.1.1 การเตรียมวัสดุอุปกรณ์

3.1.1.1 คอมพิวเตอร์และอุปกรณ์ต่าง ๆ

1) เครื่องคอมพิวเตอร์ PC

2) เครื่องคอมพิวเตอร์ Notebook

3) เครื่องพิมพ์

4) wifi

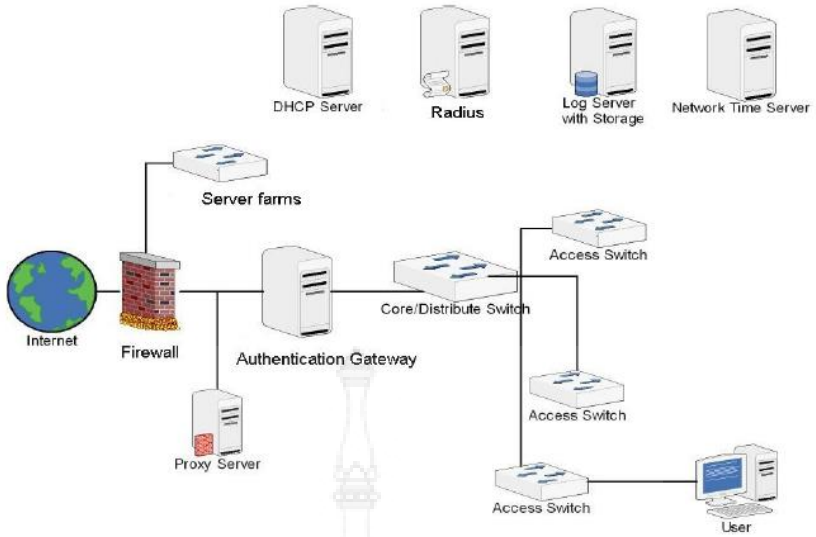
3.1.1.2 ซอฟต์แวร์

1) ระบบปฏิบัติการ Linux

2) โปรแกรมระบบการจัดการฐานข้อมูล MySQL

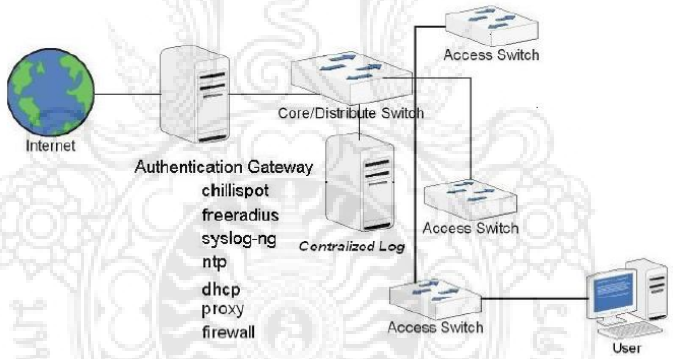
3.2 การออกแบบระบบงาน

แผนผังการวางระบบงานเดิมที่ใช้งานในปัจจุบันของหน่วยงาน



ภาพที่ 3-1 แผนภาพระบบเครือข่ายคอมพิวเตอร์ของหน่วยงานโดยทั่วๆ ไป

เมื่อรวบรวมข้อมูลเรียบร้อยแล้วก็นำข้อมูลมาจัดกระทำให้เป็นระบบและวิเคราะห์หาความเป็นไปได้ในการจัดทำระบบ โดยออกแบบระบบงานดังนี้



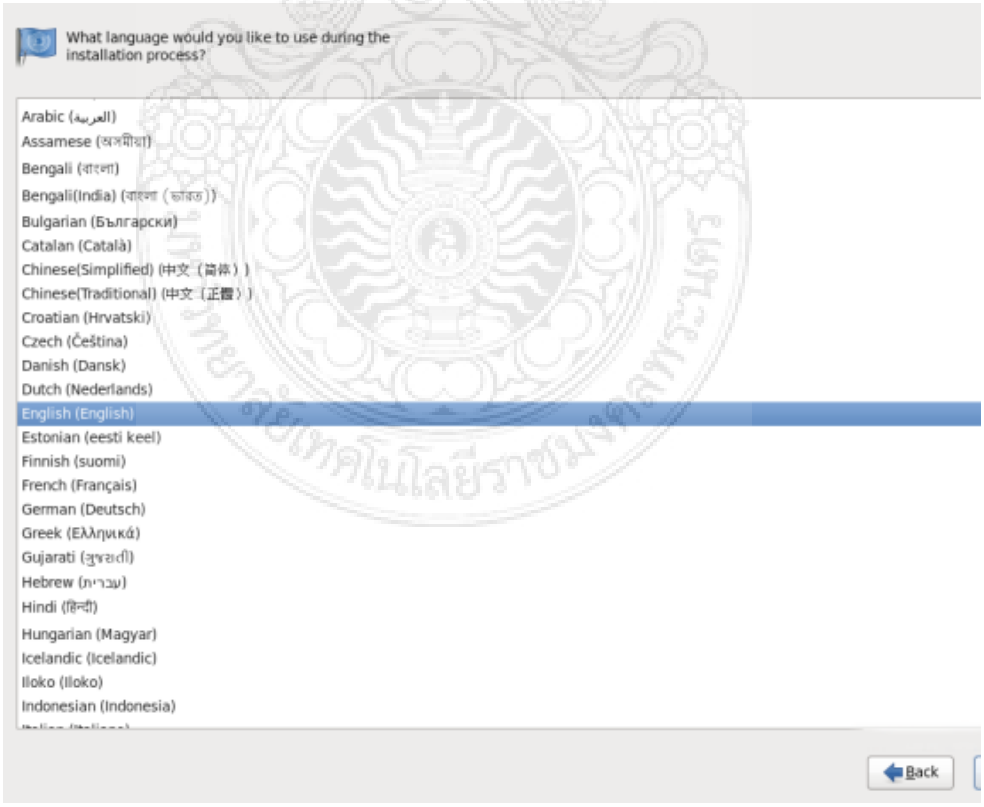
ภาพที่ 3-2 แผนภาพระบบเครือข่ายคอมพิวเตอร์ที่ติดตั้งซอฟต์แวร์ที่ตัวอุปกรณ์ Authentication Gateway

3.3 การติดตั้งระบบปฏิบัติการ Linux Server CentOS 6.3

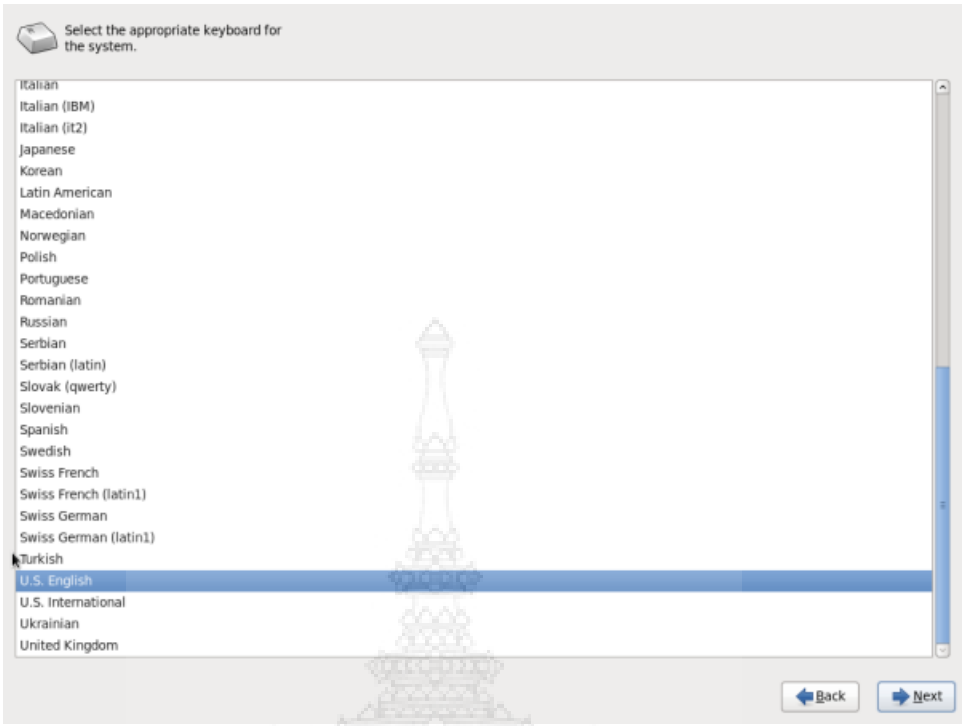
ภาพที่ 3-3 เลือก Install or Upgrade existing system options.

ภาพที่ 3-4 เลือก Skip media test

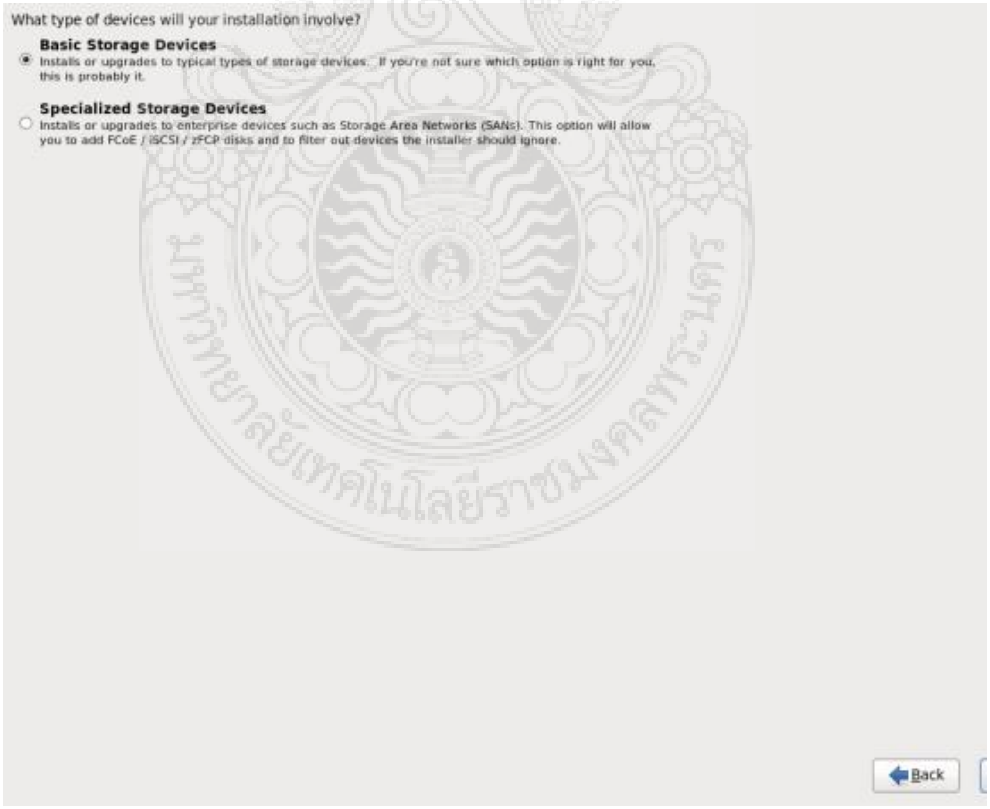
ภาพที่ 3-5 เมื่อหน้าจอแสดง CentOS 6.3 Welcome Screen กด Next



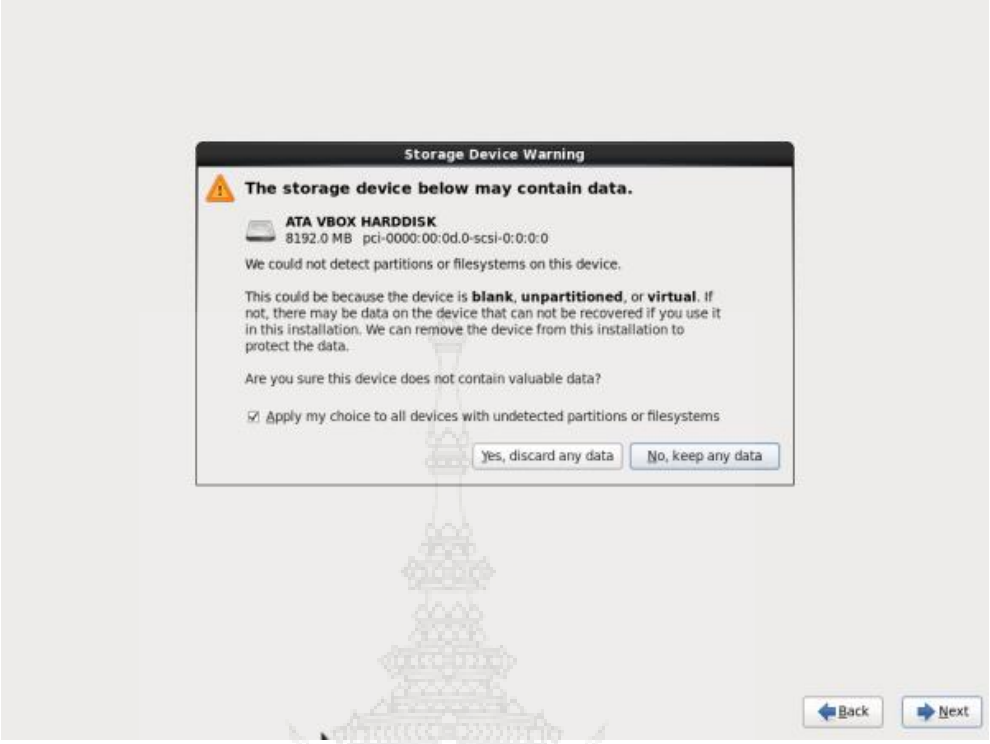
ภาพที่ 3-6 เลือก Language



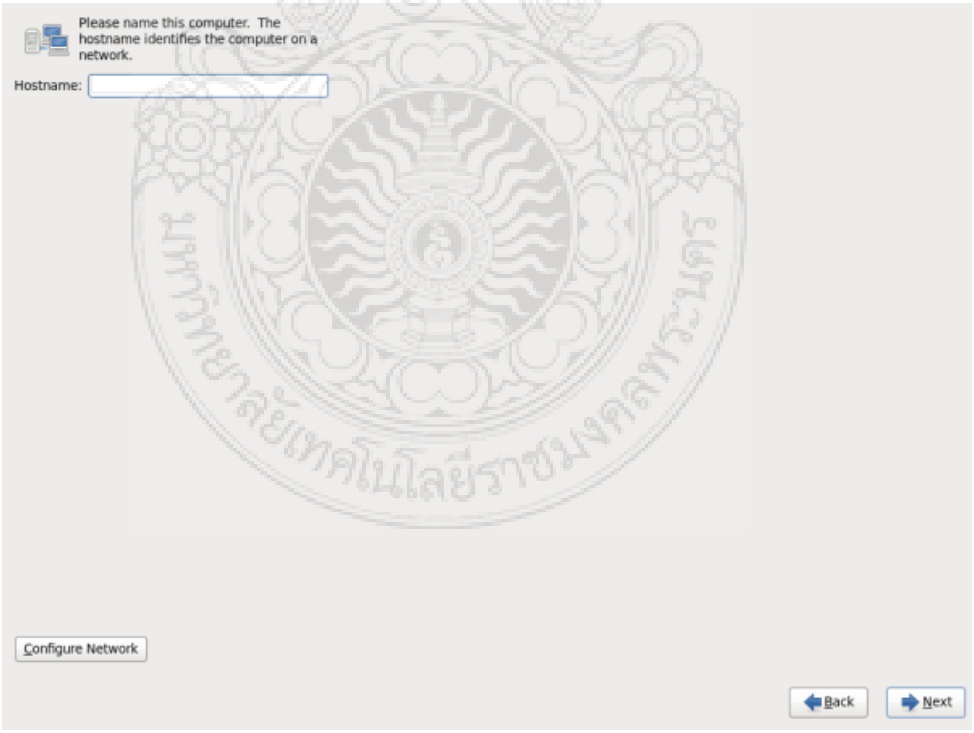
ภาพที่ 3-7 เลือก Appropriate Keyboard



ภาพที่ 3-8 เลือก Basic Storage Device

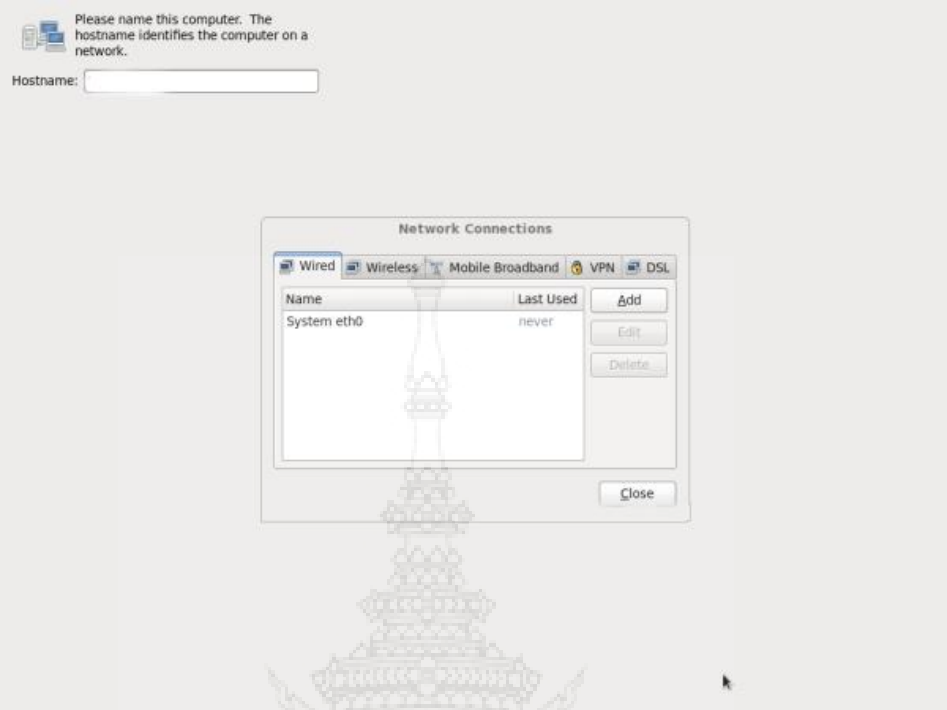


ภาพที่ 3-9 ถ้าเจอ Storage Device Warning สามารถกด Yes เพื่อทิ้ง Data เหล่านั้นเพื่อติดตั้งต่อ

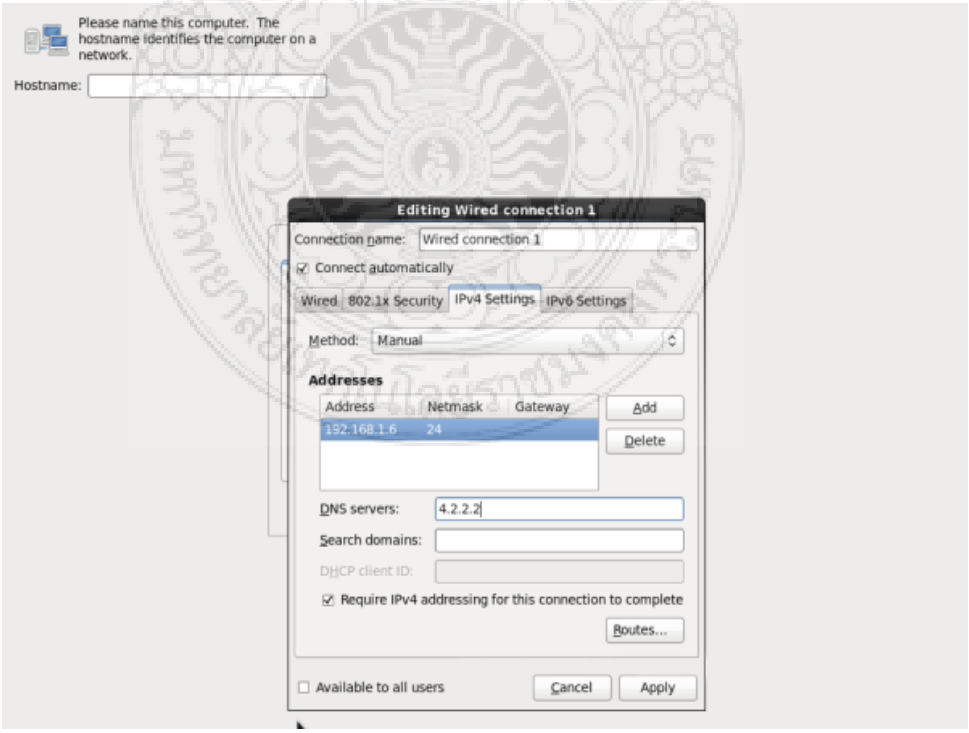


ภาพที่ 3-10 ใส่ชื่อ Hostname ให้กับ Server และ กด Configure Network ถ้าคุณต้องการตั้งค่า

Network ขณะติดตั้ง

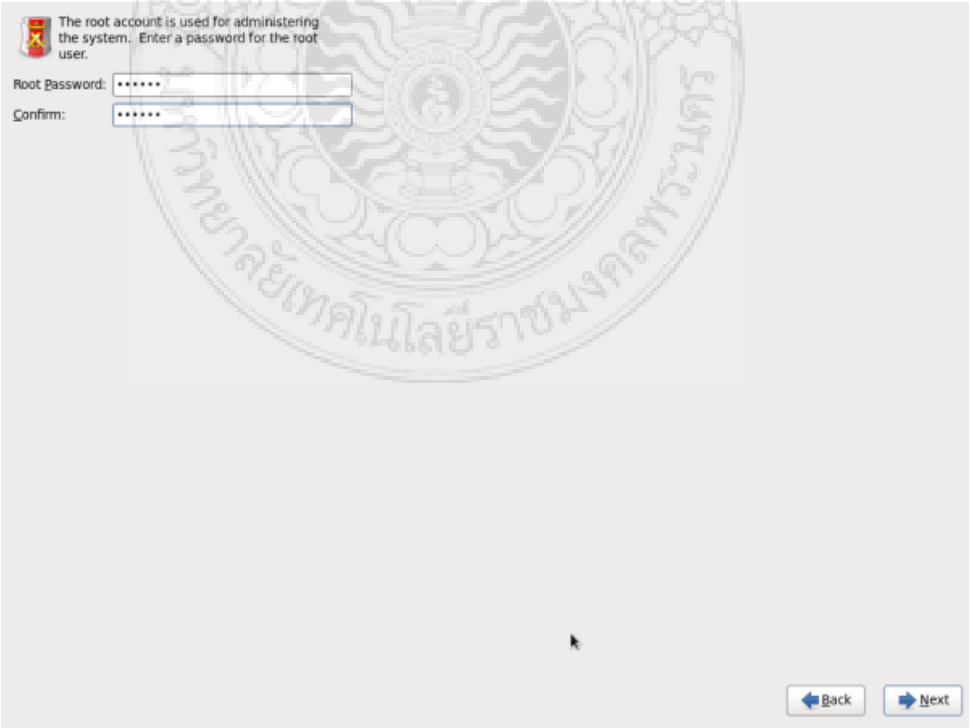


ภาพที่ 3-11 กด Wired tab และ กดปุ่ม Add

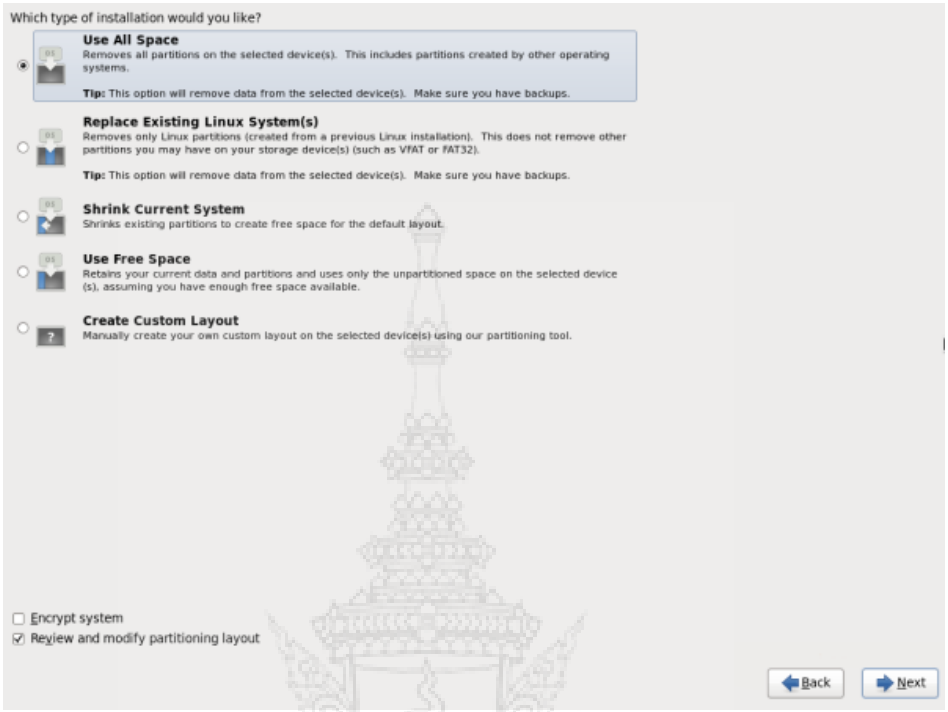


ภาพที่ 3-12 เลือก Connect Automatically, กด IPv4 Settings และเลือก Method เป็น Manual กด Add เพื่อใส่ Address box ด้วย IP Address, Netmask, Gateway และ DNS Server ตัวอย่างเช่น เราใช้ IP Address 192.168.1.6 และ DNS Server เป็น 4.2.2.2 สำหรับตัวอย่าง

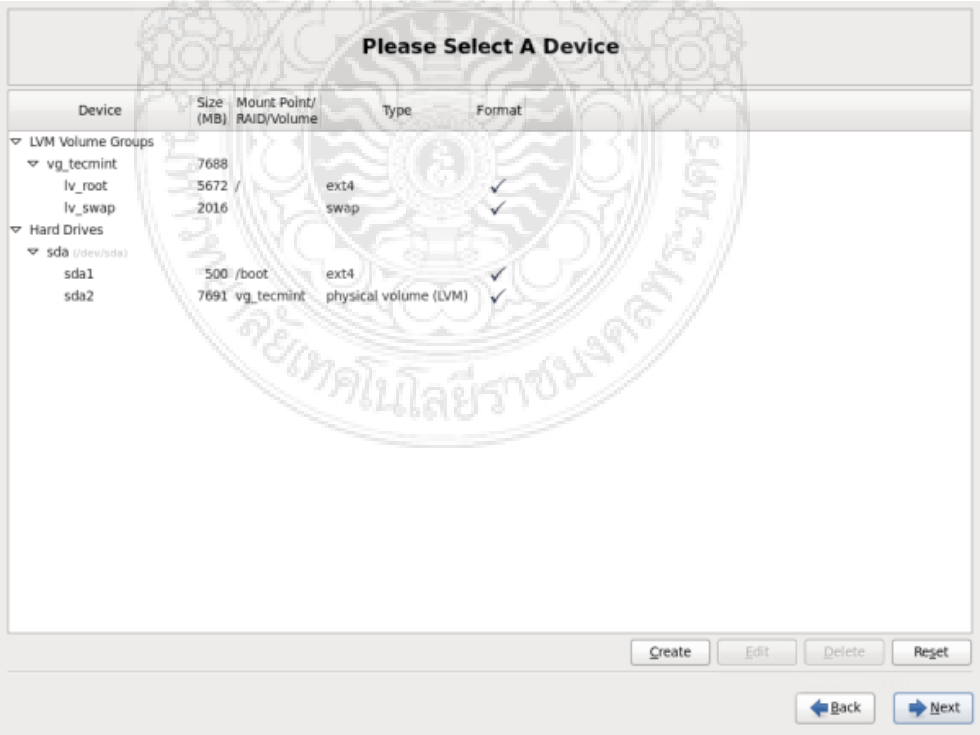
ภาพที่ 3-13 เลือก Timezone



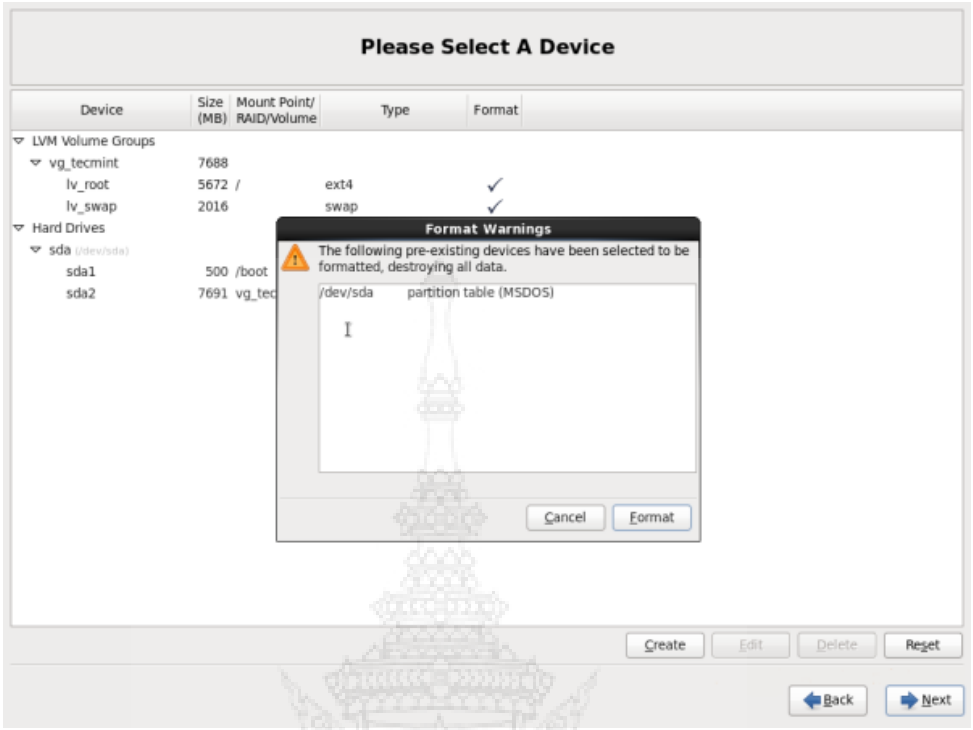
ภาพที่ 3-14 ใส่ root password



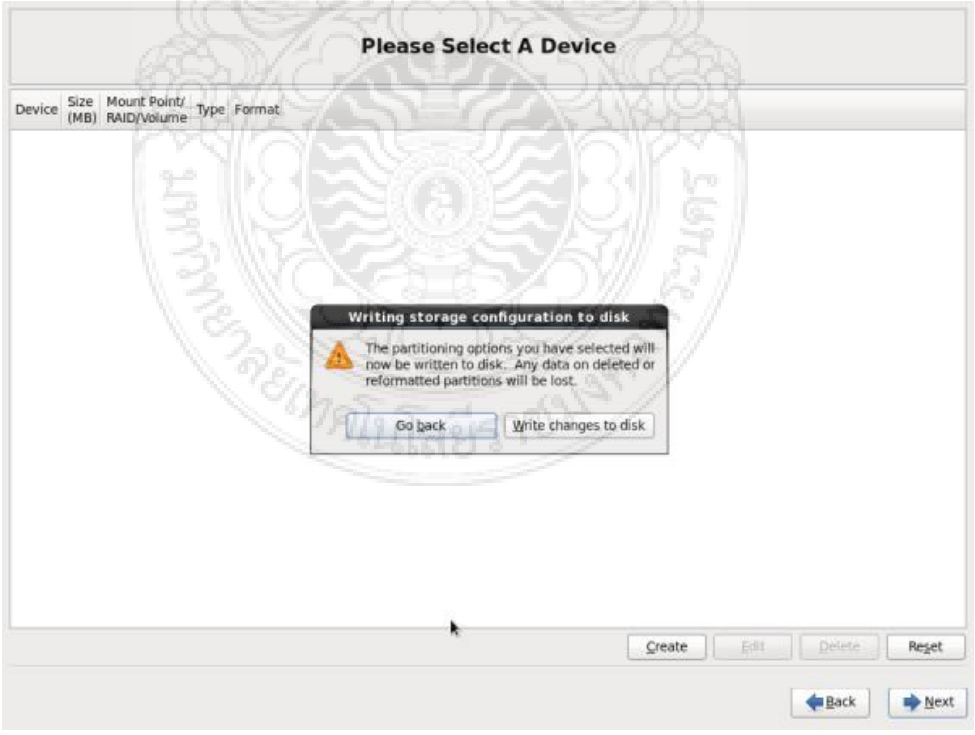
ภาพที่ 3-15 เลือกการติดตั้งลงบน Hard Disk ตามต้องการ



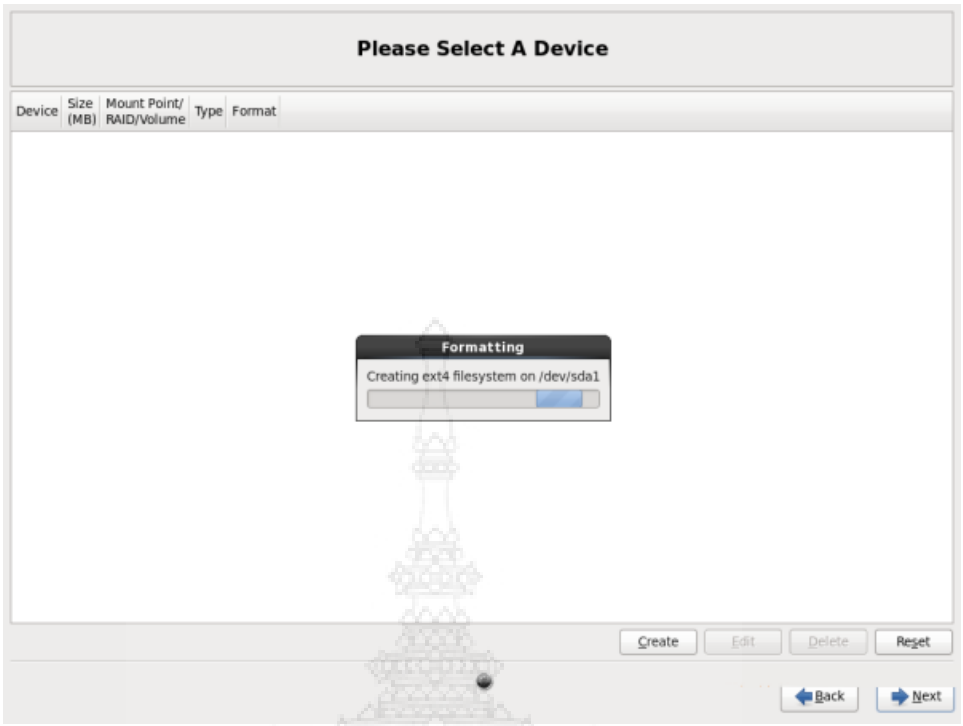
ภาพที่ 3-16 ระบบจะทำงานตรวจสอบ File System. เราสามารถแก้ไขตามที่ต้องการได้



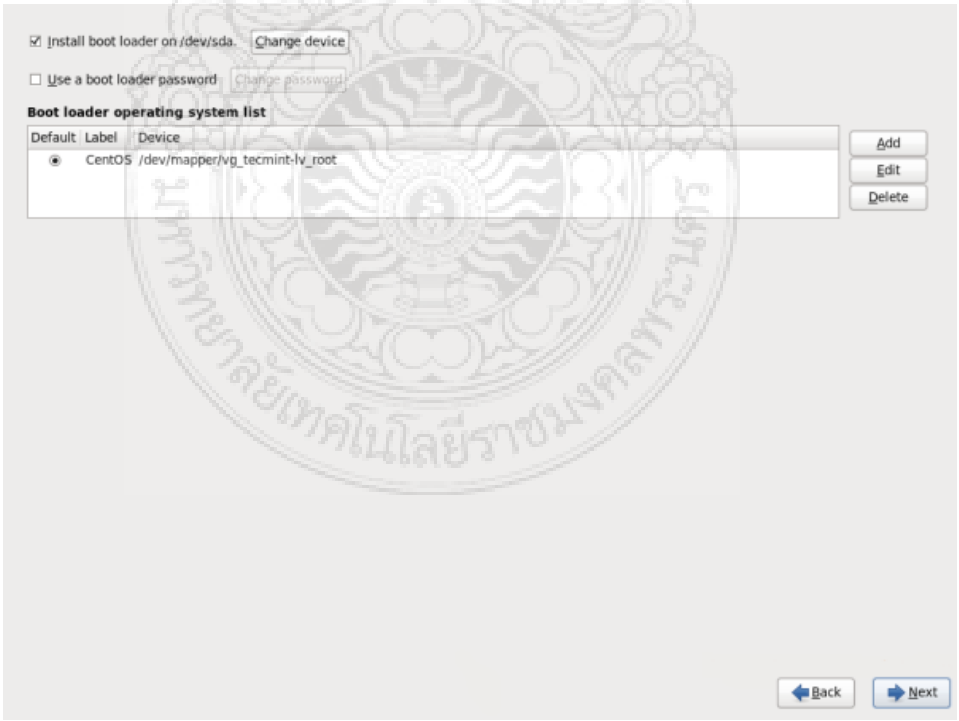
ภาพที่ 3-17 Disk Format Warning กด Format



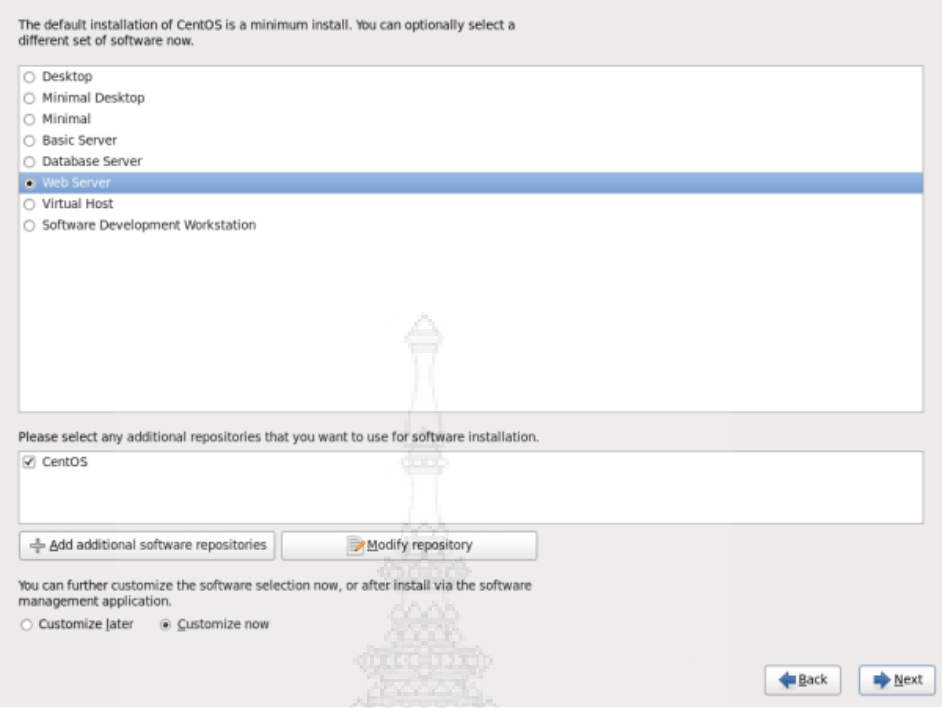
ภาพที่ 3-18 เลือก Write Changes to disk



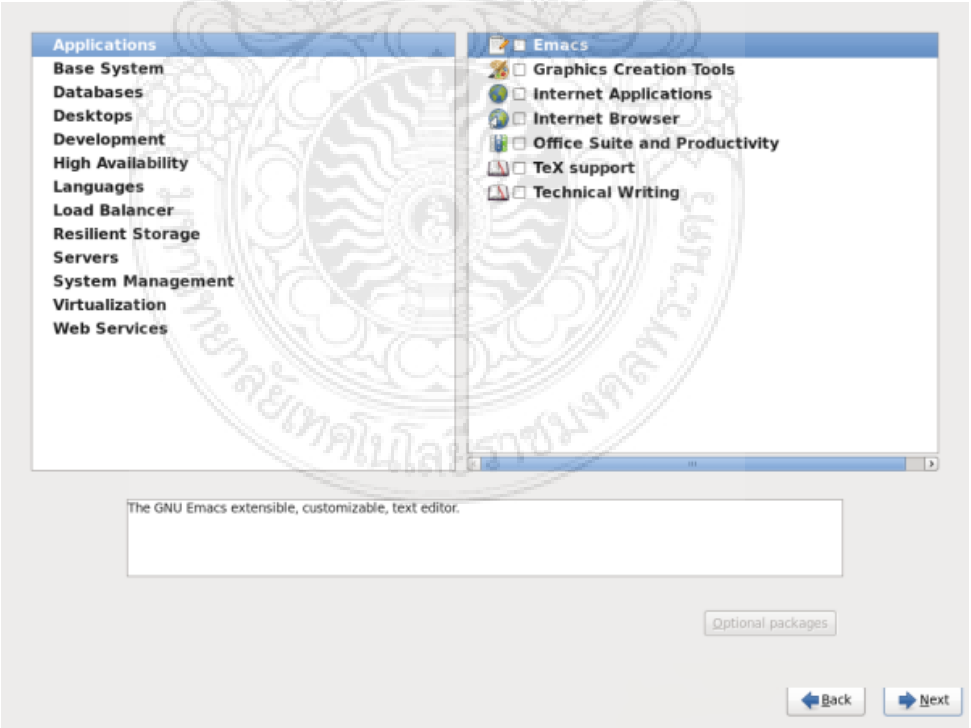
ภาพที่ 3-19 Hard Drive กำลังถูก Format



ภาพที่ 3-20 ต่อมาสามารถใช้ Boot loader Password เพื่อ Security ที่ดีขึ้น

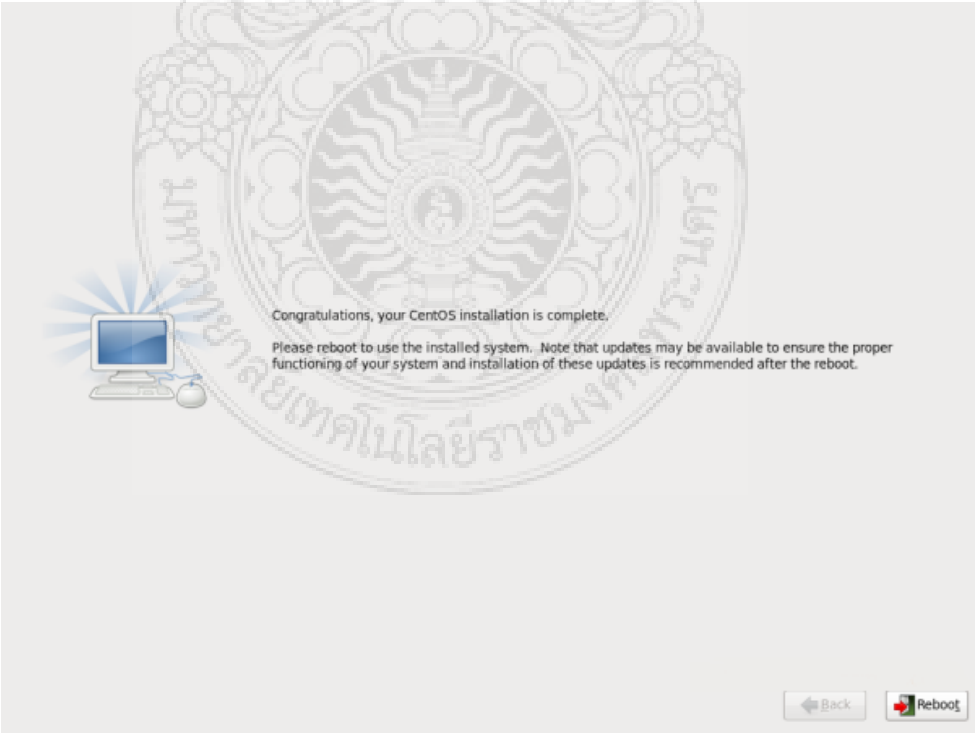


ภาพที่ 3-21 เลือก Application ที่ต้องการติดตั้งสามารถเลือก Customize now และกด Next

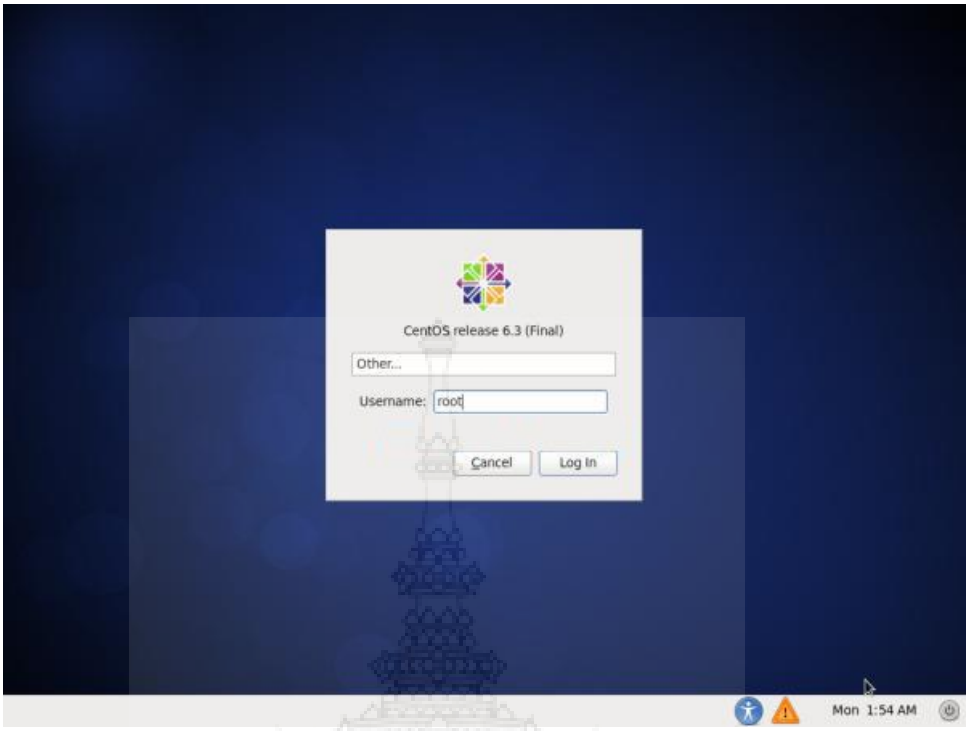


ภาพที่ 3-22 เลือก Applications ที่เราต้องการติดตั้งและกด Next

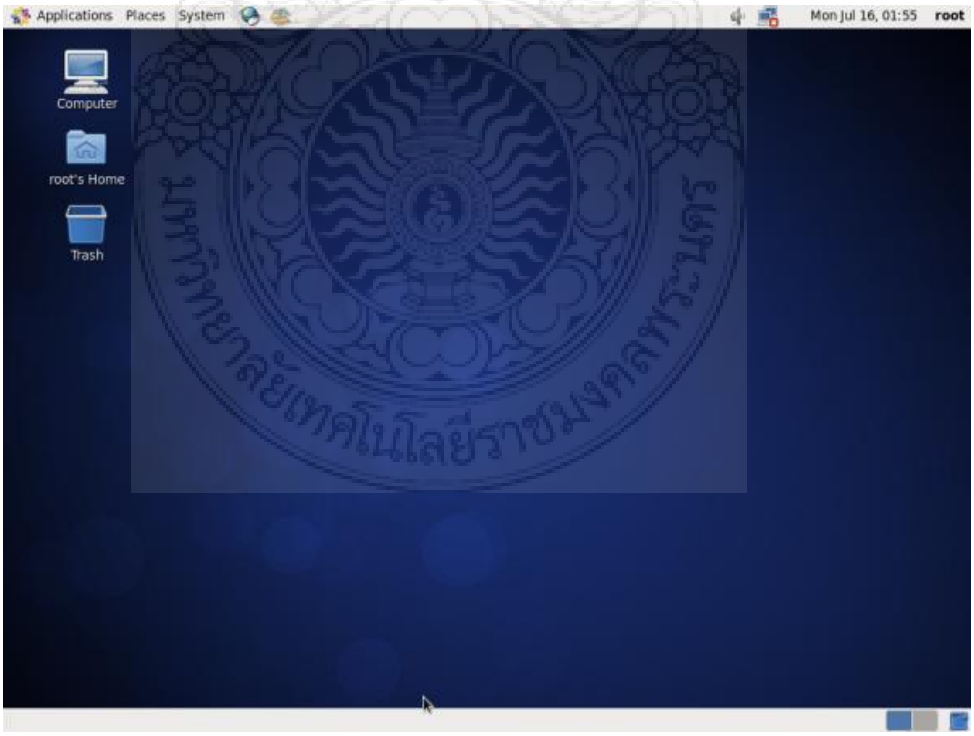
ภาพที่ 3-23 การติดตั้งจะเริ่มต้น เวลาจะขึ้นอยู่กับว่าติดตั้ง packages มากน้อยเท่าใด



ภาพที่ 3-24 เมื่อการติดตั้งเสร็จสิ้น ทำการนำ CD/DVD ออกและกด Reboot



ภาพที่ 3-25 Welcome to CentOS 6.3 Login Screen.



ภาพที่ 3-26 CentOS 6.3 Desktop Screen.

3.4 สถิติที่ใช้ในการประเมินระบบ

ในการประเมินระบบ ได้จัดทำแบบประเมินความพึงพอใจต่อระบบ ซึ่งเป็นการให้คะแนนแบบ Rating Scale ตามวิธีการของ Likert โดยแบ่งระดับไว้ 5 ระดับ ดังนี้

ตารางที่ 3-1 แสดงระดับความพอใจสำหรับแบบประเมินผล

ระดับ	ความหมาย
1	ควรปรับปรุงแก้ไข
2	พอใช้
3	ปานกลาง
4	ดี
5	ดีมาก

จากนั้นนำค่าคะแนนของผู้ประเมินระบบของแต่ละคนนำมาหาค่าเฉลี่ย โดยใช้สูตร

$$\overline{X} = \frac{\sum f_i x_i}{N}$$

โดยที่ $\overline{X}$ แทนค่าเฉลี่ย

fi แทนจำนวนผู้ประเมินที่มีความคิดเห็นในระดับคะแนน i

xi แทนค่าคะแนนประจำคำตอบ

N แทนจำนวนผู้ประเมินทั้งหมดที่ตอบแบบสอบถาม

โดยผู้ศึกษาได้นำค่าเฉลี่ยที่ได้เปรียบเทียบกับช่วงระดับความพอใจระบบซึ่งแบ่งได้เป็น 5 กลุ่ม โดยใช้สูตรการคำนวณ ดังนี้

$$\text{ความกว้างชั้น} = \frac{\text{ค่าสูงสุด} - \text{ค่าต่ำสุด}}{\text{จำนวนชั้น}} = \frac{5 - 1}{5} = 0.8$$

เมื่อทำการคำนวณหาความกว้างของช่วงระดับคะแนน เพื่อจัดช่วงคะแนนความพึงพอใจของผู้ตอบแบบประเมินการใช้ระบบ สามารถจัดช่วงระดับความพอใจเป็น 5 กลุ่ม ได้ดังนี้

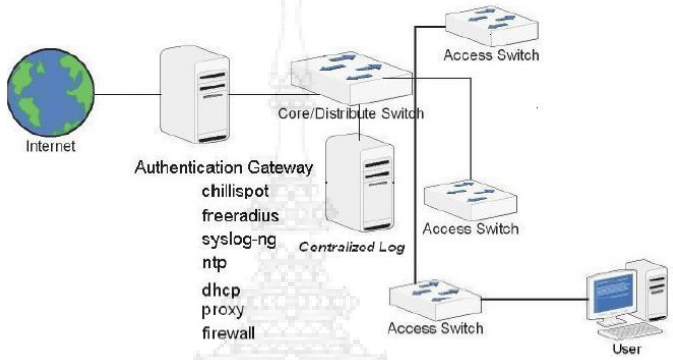
ตารางที่ 3-2 แสดงช่วงระดับคะแนนความพึงพอใจ

ช่วงคะแนน	**ช่วงระดับความพึงพอใจ**
$1.0 \leq X \leq 1.8$	ควรปรับปรุง
$1.8 \leq X \leq 2.6$	พอใจ
$2.6 \leq X \leq 3.4$	ปานกลาง
$3.4 \leq X \leq 4.2$	ดี
$4.2 \leq X \leq 5.0$	ดีมาก

บทที่ 4
การติดตั้งระบบ

4.1 ขั้นตอนการติดตั้งระบบ

เมื่อรวบรวมข้อมูลเรียบร้อยแล้วก็นำข้อมูลมาจัดกระทำให้เป็นระบบและวิเคราะห์หาความเป็นไปได้ในการจัดทำระบบ ตามแผนผังระบบงานดังนี้



ภาพที่ 4-1 แผนภาพระบบเครือข่ายคอมพิวเตอร์ที่ติดตั้งซอฟต์แวร์ที่ตัวอุปกรณ์ Authentication Gateway

4.2 การติดตั้งโปรแกรมต่างๆ ในเครื่อง PC ที่ติดตั้งระบบปฏิบัติการ Linux

มีโปรแกรมต่างๆ ดังนี้

- การติดตั้งโปรแกรม httpd
- การติดตั้งโปรแกรม freeradius
- การติดตั้งโปรแกรม mysql
- การติดตั้งโปรแกรม squid

เมื่อติดตั้งโปรแกรมต่างๆ เสร็จเรียบร้อยก็จะทำการ config โปรแกรมเพื่อให้โปรแกรมทำตามรายละเอียดของข้อมูลหน่วยงาน

ซึ่งการติดตั้งและการ config โปรแกรมมีขั้นตอน แสดงดังภาพ ดังนี้

```
[root@dhcp160 ~]# yum install httpd
================================================================================
 Package              Arch      Version         Repository       Size
================================================================================
Updating:
 httpd                i386      2.2.6-1.fc6     updates          1.0 M

Transaction Summary
================================================================================
...
Complete!
[root@dhcp160 ~]# yum install httpd-manual
================================================================================
 Package              Arch      Version         Repository       Size
================================================================================
Installing:
 httpd-manual         i386      2.2.6-1.fc6     updates          812 k

Transaction Summary
================================================================================
...
Complete!
[root@dhcp160 ~]# yum install mod_ssl
================================================================================
 Package              Arch      Version         Repository       Size
================================================================================
Installing:
 mod_ssl              i386      1:2.2.6-1.fc6   updates          84 k
Installing for dependencies:
 distcache            i386      1.4.5-14.1      base             120 k

Transaction Summary
================================================================================
...
Complete!
[root@dhcp160 ~]#
```

ภาพที่ 4-2 การติดตั้งโปรแกรม httpd

```
[root@dhcp160 ~]# service httpd start
Starting httpd:                                            [  OK  ]
[root@dhcp160 ~]#
```

ภาพที่ 4-3 คำสั่งให้ httpd ทำงาน

```
[root@dhcp160 ~]# yum install freeradius
================================================================================
 Package              Arch      Version         Repository       Size
================================================================================
Installing:
 freeradius           i386      1.1.7-3.1.fc6   updates          1.2 M
Installing for dependencies:
 lm_sensors           i386      2.10.1-1.fc6    updates          506 k
 net-snmp             i386      1:5.3.1-15.fc6  updates          695 k
 net-snmp-utils       i386      1:5.3.1-15.fc6  updates          179 k
 perl-DBI             i386      1.52-1.fc6      base             605 k

Transaction Summary
================================================================================
Install      5 Package(s)
Update       0 Package(s)
Remove       0 Package(s)

Total download size: 3.1 M
Is this ok [y/N]: y
Downloading Packages:
...
Complete!
[root@dhcp160 ~]# chkconfig radiusd on
[root@dhcp160 ~]# service radiusd start
radiusd is stopped
Starting RADIUS server:                                    [  OK  ]
[root@dhcp160 ~]#
```

ภาพที่ 4-4 การติดตั้งโปรแกรม freeradius

```
[root@dhcp160 ~]# adduser chilli
[root@dhcp160 ~]# passwd chilli
Changing password for user chilli.
New UNIX password:
BAD PASSWORD: it is too simplistic/systematic
Retype new UNIX password:
passwd: all authentication tokens updated successfully.
[root@dhcp160 ~]#
```

ภาพที่ 4-5 คำสั่งทดสอบ authentication โดยใช้ username/password ของ unix

```
[root@dhcp160 ~]# radtest chilli abcd1234 localhost 0 testing123
Sending Access-Request of id 232 to 127.0.0.1 port 1812
        User-Name = "chilli"
        User-Password = "abcd1234"
        NAS-IP-Address = 255.255.255.255
        NAS-Port = 0
Re-sending Access-Request of id 232 to 127.0.0.1 port 1812
        User-Name = "chilli"
        User-Password = "abcd1234"
        NAS-IP-Address = 255.255.255.255
        NAS-Port = 0
rad_recv: Access-Reject packet from host 127.0.0.1:1812, id=232, length=20
[root@dhcp160 ~]#
```

ภาพที่ 4-6 ทดสอบระบบโดยใช้คำสั่ง radtest chilli abcd1234 localhost 0 testing123

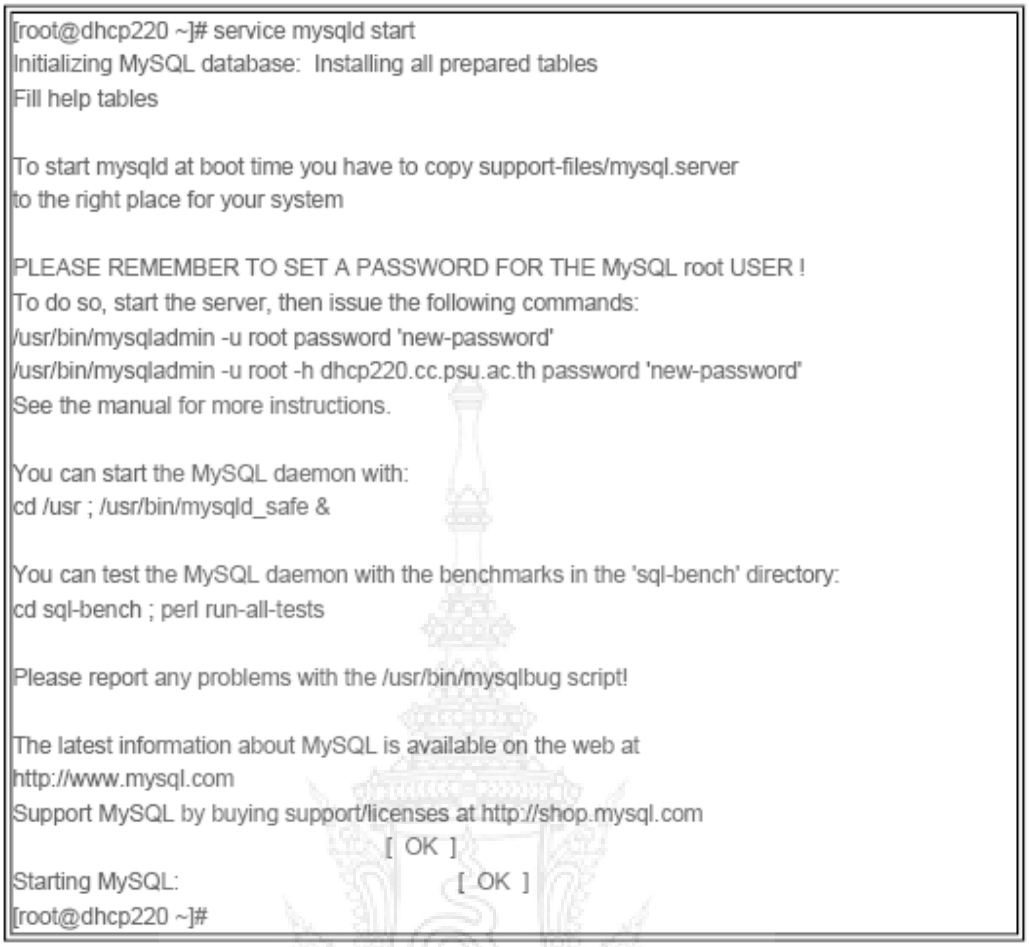
```
[root@dhcp220 ~]# yum install mysql
================================================================================
 Package            Arch      Version          Repository      Size
================================================================================
Installing:
 mysql              i386      5.0.27-1.fc6     updates         3.3 M

Transaction Summary
================================================================================
...
Complete!

[root@dhcp220 ~]# yum install mysql-server
================================================================================
 Package            Arch      Version          Repository      Size
================================================================================
Installing:
 mysql-server       i386      5.0.27-1.fc6     updates         10 M
Installing for dependencies:
 perl-DBD-MySQL     i386      3.0007-1.fc6     base            147 k

Transaction Summary
================================================================================
```

ภาพที่ 4-7 การติดตั้งโปรแกรม mysql



ภาพที่ 4-8 คำสั่งให้ mysql ทำงาน

ข้อมูลสำหรับใช้ในการทดสอบ (วิบูลย์ วราสิทธิชัย : 2553)

INSERT INTO radcheck (UserName, Attribute, Op, Value) VALUES ('fredf', 'Password', '==', 'wilma');

INSERT INTO radcheck (UserName, Attribute, Op, Value) VALUES ('fredf', 'Max-Daily-Session', ':=', '10800');

INSERT INTO radcheck (UserName, Attribute, Op, Value) VALUES ('fredf', 'Max-All-Session', ':=', '324000');

INSERT INTO radcheck (UserName, Attribute, Op, Value) VALUES ('barney', 'Password', '==', 'betty');

INSERT INTO radcheck (UserName, Attribute, Op, Value) VALUES ('barney', 'Max-Daily-Session', ':=', '10800');

INSERT INTO radcheck (UserName, Attribute, Op, Value) VALUES ('dialrouter', 'Password', '==', 'dialup');

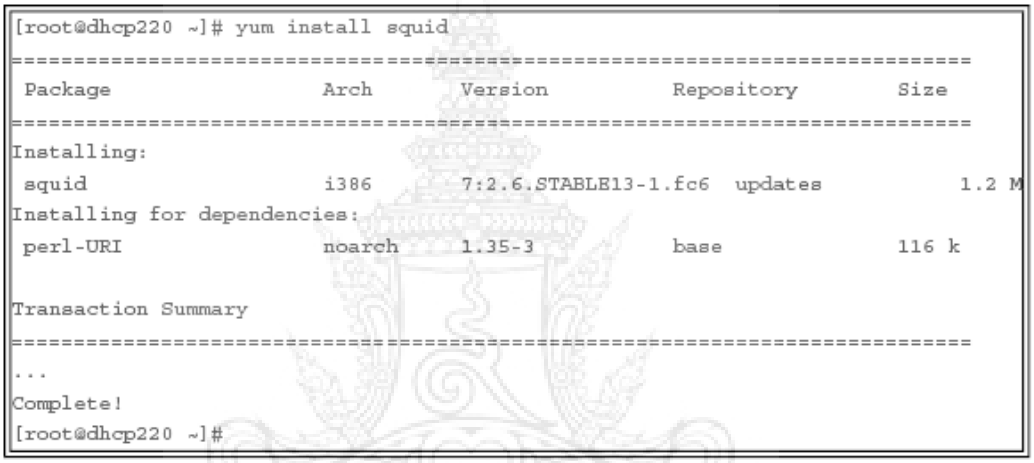
```
INSERT INTO radcheck (UserName, Attribute, Op, Value) VALUES ('dialrouter', 'Max-Monthly-Session', ':=', '324000');
INSERT INTO radreply (UserName, Attribute, Op, Value) VALUES ('fredf', 'Idle-Timeout', ':=', '1800');
INSERT INTO radreply (UserName, Attribute, Op, Value) VALUES ('fredf', 'Session-Timeout', ':=', '3600');
INSERT INTO radreply (UserName, Attribute, Op, Value) VALUES ('fredf', 'WISPr-Bandwidth-Max-Down', ':=', '56000');
INSERT INTO radreply (UserName, Attribute, Op, Value) VALUES ('fredf', 'WISPr-Bandwidth-Max-Up', ':=', '33400');
INSERT INTO radreply (UserName, Attribute, Op, Value) VALUES ('barney', 'Idle-Timeout', ':=', '1800');
INSERT INTO radreply (UserName, Attribute, Op, Value) VALUES ('barney', 'Session-Timeout', ':=', '3600');
INSERT INTO radreply (UserName, Attribute, Op, Value) VALUES ('dialrouter', 'Idle-Timeout', ':=', '900');
INSERT INTO radreply (UserName, Attribute, Op, Value) VALUES ('dialrouter', 'Session-Timeout', ':=', '1800');
INSERT INTO usergroup (UserName, GroupName) VALUES ('fredf', 'dynamic');
INSERT INTO usergroup (UserName, GroupName) VALUES ('barney', 'static');
INSERT INTO usergroup (UserName, GroupName) VALUES ('dialrouter', 'netdial');
INSERT INTO radgroupcheck (GroupName, Attribute, Op, Value) VALUES ('dynamic', 'Auth-Type', ':=', 'Local');
INSERT INTO radgroupcheck (GroupName, Attribute, Op, Value) VALUES ('dynamic', 'Simultaneous-Use', ':=', '1');
INSERT INTO radgroupcheck (GroupName, Attribute, Op, Value) VALUES ('static', 'Auth-Type', ':=', 'Local');
INSERT INTO radgroupcheck (GroupName, Attribute, Op, Value) VALUES ('static', 'Simultaneous-Use', ':=', '1');
INSERT INTO radgroupcheck (GroupName, Attribute, Op, Value) VALUES ('netdial', 'Auth-Type', ':=', 'Local');
```

INSERT INTO radgroupcheck (GroupName, Attribute, Op, Value) VALUES ('netdial', 'Simultaneous-Use', ':=', '1');

INSERT INTO radgroupreply (GroupName, Attribute, Op, Value) VALUES ('dynamic', 'Service-Type', ':=', 'Login-User');

INSERT INTO radgroupreply (GroupName, Attribute, Op, Value) VALUES ('static', 'Service-Type', ':=', 'Login-User');

INSERT INTO radgroupreply (GroupName, Attribute, Op, Value) VALUES ('netdial', 'Service-Type', ':=', 'Login-User');



ภาพที่ 4-9 การติดตั้งโปรแกรม squid

บทที่ 5
ผลการศึกษา สรุป และข้อเสนอแนะ

การวิจัยและพัฒนาระบบการยืนยันตัวตนโดยใช้เทคโนโลยีฟรีแวร์ เป็นการจัดการระบบสารสนเทศอย่างหนึ่งของระบบสารสนเทศที่ใช้ในการพัฒนาระบบ Server โดยใช้ระบบปฏิบัติการที่เป็น Open Source ซึ่งในปัจจุบันเป็นที่นิยมใช้งานกันอย่างแพร่หลาย แต่ก็ยังประสบปัญหาในการปรับพื้นฐานความรู้ของบุคลากรของแต่ละหน่วยงาน เนื่องจากมีการบุคลากรมีความรู้พื้นฐานที่แตกต่างกันค่อนข้างมาก ทำให้เกิดความยุ่งยากในการติดตั้งระบบ Server

การวิจัยและพัฒนาระบบการยืนยันตัวตนโดยใช้เทคโนโลยีฟรีแวร์ จึงได้มีการออกแบบระบบมาเพื่ออำนวยความสะดวกในการติดตั้งระบบปฏิบัติการ Linux ทำให้บุคลากรของหน่วยงานเรียนรู้ได้อย่างรวดเร็ว ซึ่งการวิจัยและพัฒนาระบบงานนี้ โดยการใช้ระบบปฏิบัติการ Linux CentOS ซึ่งนิยมใช้งานกันอย่างแพร่หลาย

5.1 ผลการศึกษา

การพัฒนาระบบการยืนยันตัวตนโดยใช้เทคโนโลยีฟรีแวร์ ผู้จัดทำระบบได้ทำการประเมินผลการทำงานของระบบงาน เพื่อช่วยให้ผู้จัดทำทราบถึงปัญหาต่างๆ ที่เกิดจากการใช้งานระบบ เพื่อให้สามารถนำข้อผิดพลาดต่างๆ เหล่านั้นไปทำการปรับปรุงแก้ไข เพื่อให้ได้ระบบงานที่พัฒนาอย่างมีประสิทธิภาพ และประสิทธิผลในการใช้งานของบุคลากรในหน่วยงาน

โดยผู้จัดทำได้ทำการประเมินผลการใช้งานระบบการยืนยันตัวตนโดยใช้เทคโนโลยีฟรีแวร์ จากการรวบรวมข้อมูลแบบประเมินผลการใช้งานของระบบ จำนวน 32 ชุด ทำให้ผู้พัฒนาระบบทราบถึงความต้องการของผู้ใช้ระบบและสามารถสรุปความคิดเห็นเป็นคะแนนเฉลี่ยของผู้ใช้ที่มีต่อระบบดังตารางต่อไปนี้

ตารางที่ 5-1 ผลการวิเคราะห์ข้อมูลจากผู้ใช้ในหน่วยงาน

ลำดับ	ลักษณะการใช้งาน	ค่าผลการวิเคราะห์	การแปรความหมาย
1	ความสะดวกต่อการใช้งาน	3.57	ดี
2	ความยากง่ายในการติดตั้งโปรแกรมระบบปฏิบัติการ	3.43	ดี
3	ความยากง่ายในการ Config ระบบ	3.59	ดี
4	ความถูกต้องของโปรแกรม	3.67	ดี
5	ความสมบูรณ์ของรายงานสรุปผล	3.68	ดี

6	การแก้ไขปรับปรุงทำได้ง่ายและสะดวก	3.67	ดี
ลำดับ	**ลักษณะการใช้งาน**	**ค่าผลการวิเคราะห์**	**การแปรความหมาย**
7	การค้นหาข้อมูลทำได้ง่ายและสะดวก	3.70	ดี
8	การทำงานสะดวกมากขึ้นในการเรียกดูข้อมูล	3.40	ดี
9	คู่มือการใช้มีความชัดเจน และสะดวกต่อการใช้งาน	3.67	ดี
10	สามารถนำไปใช้กับระบบงานได้จริง	4.28	ดีมาก
ค่าเฉลี่ยคะแนนต่อการใช้โปรแกรม		**3.66**	**ดี**

การแปลผลการวิเคราะห์ข้อมูล

จากการนำระบบงานครุภัณฑ์ไปทดสอบกับผู้ใช้แต่ละหน่วยงาน จำนวน 32 คน พบว่า ผู้ใช้มีความคิดเห็นเกี่ยวกับการใช้งานของระบบในภาพรวมอยู่ในระดับดี โดยผู้ใช้มีความพอใจเกี่ยวกับสามารถนำไปใช้กับระบบงานได้จริง มีความคิดเห็นอยู่ในระดับดีมาก ส่วนความสะดวกต่อการใช้งาน ความยากง่ายในการติดตั้งโปรแกรมระบบปฏิบัติการ ความยากง่ายในการ Config ระบบ ความถูกต้องของโปรแกรม ความสมบูรณ์ของรายงานสรุปผล การแก้ไขปรับปรุงทำได้ง่ายและสะดวก การค้นหาข้อมูลทำได้ง่ายและสะดวก การทำงานสะดวกมากขึ้นในการเรียกดูข้อมูล และคู่มือการใช้มีความชัดเจน และสะดวกต่อการใช้งาน มีความคิดเห็นอยู่ในระดับดี

5.2 ปัญหาและอุปสรรคที่พบ

เนื่องจากการวิจัยและพัฒนาระบบงาน เป็นการพัฒนาระบบขึ้นมาเป็นครั้งแรก ดังนั้น ปัญหาที่ผู้วิจัยได้พบในการวิจัยดังกล่าว มีดังนี้

5.2.1 ปัญหาในด้านระบบงาน ไม่สามารถติดตั้งระบบงาน เพื่อให้บุคลากรได้ทำการทดลองใช้งานได้อย่างต่อเนื่อง ตลอดเวลา ทำให้ผู้ใช้งานเกิดความไม่สนใจที่จะใช้ระบบงานใหม่

5.2.2 ปัญหาที่เกิดขึ้นจากข้อจำกัดของระบบงาน ทำให้การทำงานของระบบยังไม่ครอบคลุมระบบงานมากนัก

5.2.3 ปัญหาที่เกิดขึ้นจากบุคลากรของหน่วยงาน มีความรู้พื้นฐานทางด้านการติดตั้งระบบ Server ที่แตกต่างกันค่อนข้างมาก ทำให้การติดตั้งระบบ Server ล่าช้า
ครอบคลุมระบบงานมากนัก

5.3 ข้อเสนอแนะ

ควรมีการอบรมความรู้พื้นฐานทางด้านการติดตั้งระบบ Server ให้กับบุคลากรของแต่ละหน่วยงาน เพื่อจะได้ปรับให้มีความรู้พื้นฐานที่เท่าเทียมกัน

เอกสารอ้างอิง

[1] บุญลือ อยู่คง. การติดตั้ง Internet Server ด้วย Linux. นครราชสีมา: บริษัทซายเอ็นเทค จำกัด, 2545.

[2] บุญลือ อยู่คง. ป้องกัน Linux Server อย่างมืออาชีพ. เชียงใหม่: บริษัท ดวงกมลเชียงใหม่ กรุ๊ป จำกัด, 2546.

[3] บุญลือ อยู่คง. ติดตั้ง Log Server ด้วย Linux. พิษณุโลก: โฟกัสมาสเตอร์พรินต์, 2551.

[4] ยุวดี พนาเวศร์, http://www.gotoknow.org/blog/yuvadeepanaves

[5] วิบูลย์ วราสิทธิชัย, http://mamboeasy.psu.ac.th/~wiboon.w/index2.php?option=com_content&task=view&

[6] "Ethereal", http://www.ethereal.com/

[7] "Cain & Abel", http://www.oxid.it/cain.html

[8] "September 2009 Web Server Survey", http://news.netcraft.com/archives/web_server_survey.html

[9] "Aradiom SolidPass", http://www.aradiom.com/Sol idPass/2fa-OTP-security-token.htm,

[10] "AuthAnvil", http://www.scorpionsoft.com/

[11] "FileID", http://www.fireid.com/technical/token.html,

[12] "FiveBarGate", http://www.fivebargate.net/

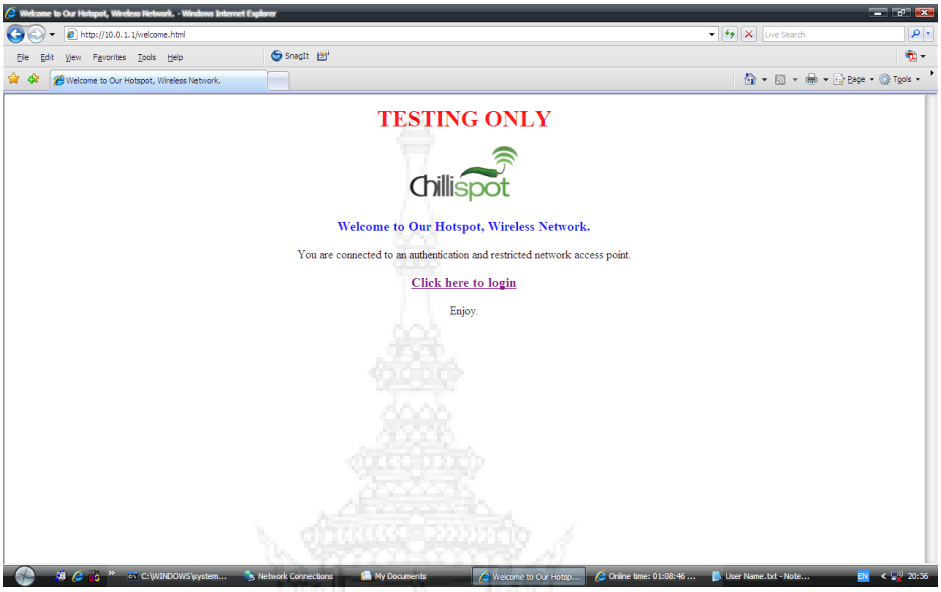
[13] "Diversinet", http://www.diversinet.com/Products/Authentication/Authentication.html

ภาคผนวก ก

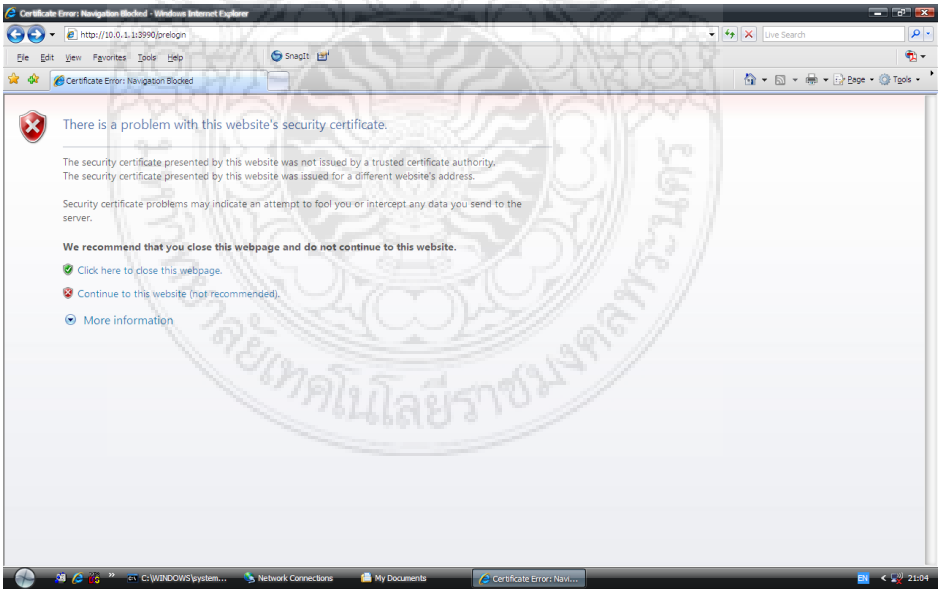
คู่มือการใช้งานระบบ

คู่มือการใช้งานระบบระบบการยืนยันตัวตนโดยใช้เทคโนโลยีฟรีแวร์

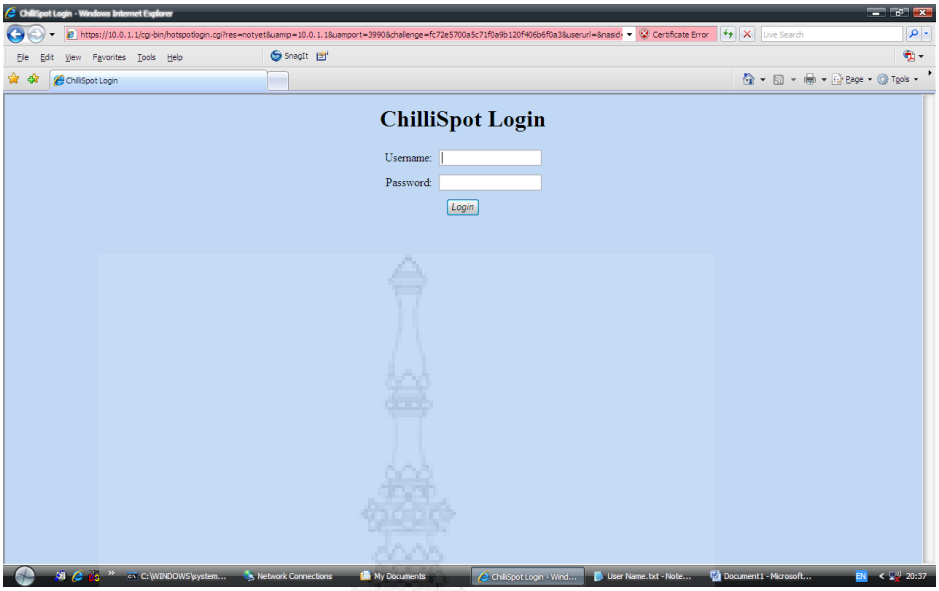
การใส่ User Name & Password



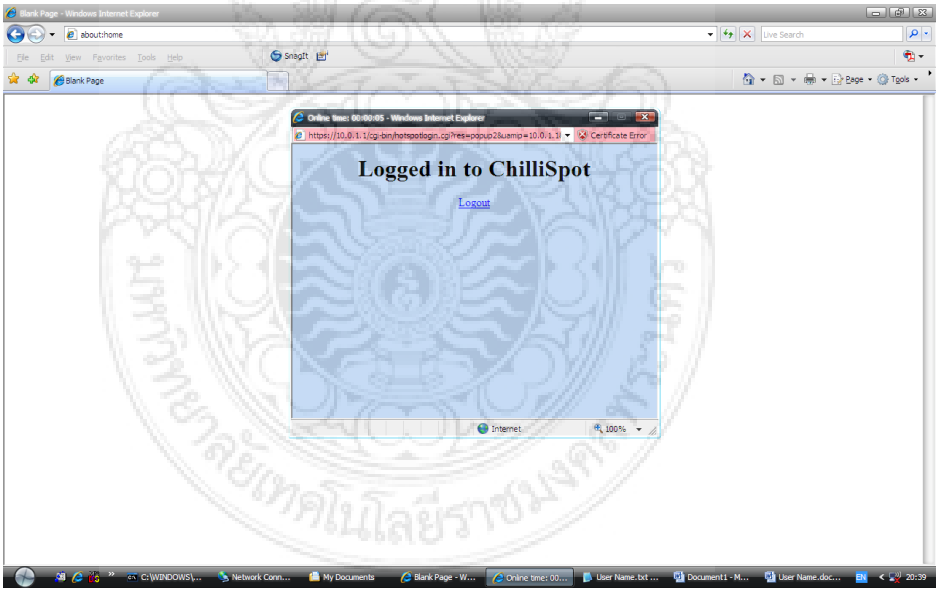
ภาพที่ ก-1 ให้ Click ที่ Click here to login



ภาพที่ ก-2 คลิ๊กที่ Continue to this website เพื่อทำการใส่ user name & password



ภาพที่ ก-3 ใส่ user name & password



ภาพที่ ก-4 เมื่อใส่ user name & password ถูกต้อง จะสามารถเข้าเว็บไซต์ตามปกติ

ภาคผนวก ข

แบบสอบถาม

แบบสอบถาม

แบบสอบถามนี้เป็นแบบสอบถามสำหรับประเมินการใช้งาน “ระบบการยืนยันตัวตนโดยใช้เทคโนโลยีฟรีแวร์” ของมหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร เพื่อประเมินการใช้งานระบบการยืนยันตัวตน โดยมีลักษณะการตอบเป็นมาตราส่วนประมาณค่า 5 อันดับ ดังนี้

มากที่สุด หมายถึง เมื่อผู้ตอบเห็นว่าข้อความนั้นตรงกับความรู้สึกของผู้ตอบมากที่สุด
มาก หมายถึง เมื่อผู้ตอบเห็นว่าข้อความนั้นตรงกับความรู้สึกของผู้ตอบมาก
ปานกลาง หมายถึง เมื่อผู้ตอบเห็นว่าข้อความนั้นตรงกับความรู้สึกของผู้ตอบปานกลาง
น้อย หมายถึง เมื่อผู้ตอบเห็นว่าข้อความนั้นตรงกับความรู้สึกของผู้ตอบน้อย
น้อยที่สุด หมายถึง เมื่อผู้ตอบเห็นว่าข้อความนั้นตรงกับความรู้สึกของผู้ตอบน้อยที่สุด

ให้ผู้ตอบแบบสอบถาม แสดงความคิดเห็นลงในรายละเอียด ดังนี้

แบบประเมินการใช้โปรแกรม
ระบบการบริการอิเล็กทรอนิกส์คณะบริหารธุรกิจผ่านเครือข่ายอินเตอร์เน็ต

ตอนที่ 1 ข้อมูลทั่วไป

<u>คำชี้แจง</u> กรุณาใช้เครื่องหมาย ✓ ในช่องตามความเป็นจริง

1. เพศ

   ☐ ชาย ☐ หญิง

2. ตำแหน่งทดสอบ

   ☐ อาจารย์ / เจ้าหน้าที่ ☐ นักศึกษา

ตอนที่ 2 ความคิดเห็นเกี่ยวกับโปรแกรมในด้านต่าง ๆ

<u>คำชี้แจง</u> กรุณาใช้เครื่องหมาย ✓ ในช่องตามความเป็นจริง

ลำดับ	ลักษณะการใช้งาน	ระดับความคิดเห็น				
		มากที่สุด	มาก	ปานกลาง	น้อย	น้อยที่สุด
1	ความสะดวกต่อการใช้งาน					
2	ความยากง่ายในการติดตั้งโปรแกรมระบบปฏิบัติการ					
3	ความยากง่ายในการ Config ระบบ					
4	ความถูกต้องของโปรแกรม					
5	ความสมบูรณ์ของรายงานสรุปผล					
6	การแก้ไขปรับปรุงทำได้ง่ายและสะดวก					
7	การค้นหาข้อมูลทำได้ง่ายและสะดวก					
8	การทำงานสะดวกมากขึ้นในการเรียกดูข้อมูล					
9	คู่มือการใช้มีความชัดเจน และสะดวกต่อการใช้งาน					
10	สามารถนำไปใช้กับระบบงานได้จริง					

ตอนที่ 3 ข้อเสนอแนะอื่น ๆ เกี่ยวกับโปรแกรม

.....

.....

.....

.....

***** ขอขอบคุณที่กรุณาให้ความร่วมมือในการตอบแบบสอบถาม *****

ประวัติผู้วิจัย

1. ชื่อ-นามสกุล (ภาษาไทย) นายพรคิด อั้นขาว

(ภาษาอังกฤษ) Mr. Pornkid Unkaw

2. ตำแหน่งปัจจุบัน อาจารย์

3. ที่อยู่หน่วยงานที่ติดต่อได้สะดวก

มหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร คณะบริหารธุรกิจ สาขาวิชาระบบสารสนเทศ

86 ถนนพิษณุโลก แขวงจิตรลดา เขตดุสิต กรุงเทพมหานคร 10300

โทร. 0-2282-9101-2 ต่อ 7201 โทรสาร. 0-2282-9711

E-mail : nuna29@hotmail.com

4. ประวัติการศึกษา

วศ.บ. (วิศวกรรมคอมพิวเตอร์) สถาบันเทคโนโลยีราชมงคล

วท.ม. (เทคโนโลยีสารสนเทศ) สถาบันเทคโนโลยีพระจอมเกล้าพระนครเหนือ