การประเมินระบบความปลอดภัยของระบบเครือข่ายไร้สาย มหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร

พรคิด อั้นขาว

งานวิจัยนี้ได้รับทุนสนับสนุนจากงบประมาณเงินรายได้ ประจำปีงบประมาณ 2557
มหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร คณะบริหารธุรกิจ

บทคัดย่อ

การศึกษาครั้งนี้ มีวัตถุประสงค์เพื่อวิจัยและประเมินระบบความปลอดภัยของระบบเครือข่ายไร้สายมหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร เพื่อเพิ่มประสิทธิภาพของกระบวนการทำงานของระบบความปลอดภัยของระบบเครือข่ายไร้สาย

งานวิจัยนี้เป็นลักษณะวิจัยและประเมินประสิทธิภาพ เพื่อนำมาปรับปรุงแก้ไขระบบความปลอดภัยของระบบเครือข่ายไร้สาย โดยมีกระบวนการพัฒนาจากการศึกษาขั้นตอนการปฏิบัติงานของระบบความปลอดภัยของระบบเครือข่ายไร้สาย เพื่อนำไปปรับปรุงระบบความปลอดภัย โดยได้เลือกเครื่องมือที่ใช้ในการประเมินคือ โปรแกรมระบบปฏิบัติการ Kali Linux

ผลของงานวิจัย จากการประเมินประสิทธิภาพของเครือข่ายดังกล่าว สามารถนำไปใช้งานจริงกับระบบการรักษาความปลอดภัยของระบบเครือข่ายไร้สาย โดยผู้วิจัยได้ทำแบบประเมินระบบความปลอดภัยของระบบเครือข่ายไร้สาย พบว่ามีความพึงพอใจต่อโปรแกรมอยู่ในระดับดี

ABSTRACT

This study The objective is to research and evaluate the security of wireless networks, Rajamangala University of Technology Phra Nakhon. To enhance the performance of the security of wireless networks.

This research is a research and evaluation. In order to improve the security of wireless networks. The process of developing the procedures for the security of wireless networks. To improve security. It is a tool used in the evaluation is Kali Linux operating system.

The findings The performance evaluation of such networks. Can be proved with the security of wireless networks. The study was done to evaluate the security of wireless networks. Found that satisfaction with the program was good.

กิตติกรรมประกาศ

งานวิจัยเรื่องนี้ได้รับการสนับสนุนทุนการวิจัยจากงบประมาณเงินรายได้ ประจำปีงบประมาณ พ.ศ. 2557 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

ปัจจุบันเทคโนโลยีเครือข่ายแบบไร้สายหรือ Wireless Network ได้รับความนิยมในการใช้งานอย่างมาก เช่น Bluetooth, WLAN, Home RD, GPRS และ 3G เป็นต้น เทคโนโลยีเครือข่ายไร้สาย หรือ WLAN (Wireless LAN) กำลังได้รับความนิยมเป็นอย่างมาก เนื่องจากประโยชน์ของ WLAN มีอยู่มากมายโดยเฉพาะอย่างยิ่ง WLAN สร้างความสะดวกในการใช้งานและติดตั้งได้ง่าย ราคาค่าใช้จ่ายไม่แพงมากเหมือนในอดีตและมีความคล่องตัวในการทำงานมากขึ้น แต่ปัญหาด้านความปลอดภัยบนเครือข่ายไร้สายก็เพิ่มมากขึ้นเช่นเดียวกันกับประโยชน์ที่เราได้รับ กล่าวคือ พื้นฐานของ WLAN นั้นมาจากมาตรฐานของ IEEE 802.11 ที่เราใช้อยู่กันเป็นส่วนใหญ่ก็คือ IEEE.802.11 b/g ซึ่งใช้คลื่นความถี่ย่านไมโครเวฟในการส่งสัญญาณที่ความถี่ 2.4 GHz โดยการเข้ารหัสแบบ DSSS (Direct Sequence Spread Spectrum) เป็นส่วนใหญ่ แต่อย่างไรก็ตาม ความง่ายและสะดวกต่อการติดตั้งและใช้งานของอุปกรณ์ IEEE 802.11 WLAN ก็นำมาซึ่งความไม่ปลอดภัยของเครือข่ายด้วยเช่นกัน เนื่องจากสัญญาณข้อมูลแพร่กระจายอยู่ในอากาศ และไม่จำกัดขอบเขตอยู่บริเวณบริเวณหนึ่งเท่านั้น แต่สัญญาณอาจจะแพร่ไปถึงบริเวณภายนอกเขตความดูแล ซึ่งอาจจะทำให้ผู้โจมตีสามารถดักจับข้อมูล ปลอมแปลงสัญญาณข้อมูล หรือบุกรุกระบบได้โดยไม่ต้องปรากฏตัวให้เห็น อีกทั้งเทคโนโลยี IEEE 802.11 WLAN ควรมีความรู้เกี่ยวกับเทคโนโลยีและตระหนักถึงช่องโหว่ต่างๆ รวมถึงการรักษาความปลอดภัยอย่างเหมาะสม

รูปแบบการรักษาความปลอดภัยที่มีอยู่ เช่น แบบ WEP (Wired Equivalent Privacy) เป็นรูปแบบความปลอดภัยพื้นฐานที่ติดมากับมาตรฐาน IEEE 802.11 แต่เดิมระบบนี้ถูกออกแบบให้มีการรักษาความปลอดภัยที่ดีเทียบเท่ากับระบบเครือข่ายแบบใช้สาย ซึ่งการเข้ารหัสนี้เป็นส่วนหนึ่งของการรักษาความปลอดภัยที่เรียกว่า Cryptographic ซึ่งข้อดีของระบบของการเข้ารหัสก็คือ ข้อมูลที่ส่งออกไปจะทำการเข้ารหัสก่อนนำส่งออก เพื่อป้องกันการถูกดักฟังหรือถูกลักลอบอ่านข้อมูล โดยมีคีย์หรือกุญแจสำหรับการถอดรหัสเพื่อนำข้อมูลนั้นออกมาใช้งานได้ การส่งข้อมูลในรูปแบบของ WEP จะอยู่ในรูปแบบของคีย์คงที่ (Static Key) ซึ่งจะไม่มีการเปลี่ยนแปลงค่าของคีย์ที่ใช้ในการเข้ารหัสและถอดรหัสแต่อย่างใด ทำให้การนำไปใช้งานจริงนั้นยังทำไม่ดีเท่าที่ควร แต่ตัวระบบเองยังง่ายต่อการถูกโจมตี ถึงแม้ว่าเราจะใช้ WEP ในการเข้ารหัส แต่ WEP มีการเข้ารหัสบนพื้นฐาน RC4 Algorithm การเข้ารหัสแบบ RC4 นั้นมีช่องโหว่ (Vulnerability) ที่แฮกเกอร์สามารถเจาะได้ โดย WEP ใช้ 40 Bit Secret Key ในการเข้ารหัสข้อมูล

จากช่องโหว่ด้านความปลอดภัยของเครือข่าย IEEE 802.11 ในรูปแบบการเข้ารหัสของ WEP ผู้วิจัยคิดว่าควรทำการทดลองในการดักจับข้อมูลแพ็กเก็ตในรูปแบบต่างๆ ที่ถูกเข้ารหัสโดย WEP Key แบบ 64 บิต และ 128 บิต ตามลำดับจำนวนหนึ่ง เพื่อประเมินจำนวน Packet ที่มากพอและเวลาที่ใช้ในการแกะรอยกุญแจรหัสลับแบบ WEP และการสำรวจการเข้ารหัสป้องกันของเครือข่ายไร้สายทั่วไปและจุดบริการอินเทอร์เน็ตไร้สาย เพื่อเป็นแนวทางในการหาวิธีป้องกันการลักลอบใช้เครือข่ายไร้สาย และโปรแกรมที่มีความสามารถในการสร้างความเสี่ยงต่อระบบเครือข่ายไร้สาย

1.2 วัตถุประสงค์ของโครงการวิจัย

1. เพื่อศึกษาช่องโหว่การเข้ารหัสและถอดรหัสของ WEP
2. เพื่อสำรวจการเข้ารหัสป้องกันของเครือข่ายไร้สายทั่วไป และจุดบริการอินเทอร์เน็ตไร้สายทั่วมหาวิทยาลัย
3. เพื่อหาวิธีการป้องกันการลักลอบใช้เครือข่ายไร้สาย

1.3 ขอบเขตของการวิจัย

1. การวิจัยพิจารณาเฉพาะการรักษาความปลอดภัยแบบ WEP
2. การเข้ารหัสเป็นแบบ 64 บิต และ 128 บิต
3. การทดลองใช้กับเครือข่ายไร้สายที่ติดตั้งขึ้นเอง
4. โปรแกรมที่ใช้ในการดักจับจำนวน 2 โปรแกรม
5. โปรแกรมที่ใช้ในการถอดรหัสจำนวน 1 โปรแกรม
6. จำนวนของการสำรวจจุดบริการมีจำนวนไม่น้อยกว่า 30 ตัวอย่าง
7. จำนวนของการสำรวจจุดบริการอินเทอร์เน็ตไร้สายไม่น้อยกว่า 10 ตัวอย่าง

1.4 ประโยชน์ที่คาดว่าจะได้รับ

1. ทราบถึงวิธีการรักษาความปลอดภัยในลักษณะต่างๆ ในรูปแบบของการเข้ารหัสและการแกะรอยกุญแจเข้ารหัสข้อมูลของระบบเครือข่ายไร้สาย
2. ทราบถึงการเจาะระบบ การตรวจสอบ และการป้องกันการลักลอบใช้ข้อมูลหรือดักจับข้อมูลบนเครือข่ายไร้สาย
3. ทราบถึงหลักการทำงานของโปรแกรมต่างๆ ที่นำมาใช้ในการดักจับข้อมูล ละการแกะรอยกุญแจเข้ารหัสเพื่อเป็นแนวทางป้องกันความเสี่ยงได้อย่างถูกต้อง

1.5 วิธีการวิจัย

1.5.1 วิธีการดำเนินการวิจัย

1. การจำลองระบบเครือข่ายไร้สายเพื่อทำการทดสอบถึงภัยคุกคามที่อาจเกิดขึ้นบนเครือข่ายไร้สาย
2. การดักจับข้อมูลแพ็กเก็ต
3. การวิเคราะห์เปรียบเทียบจำนวนแพ็กเก็ตและเวลาที่ใช้ในการแกะรอยกุญแจเข้ารหัสแบบ WEP
4. การสำรวจการเข้ารหัสป้องกันของเครือข่ายไร้สายทั่วไปและจุดบริการอินเทอร์เน็ตไร้สาย
5. หาวิธีป้องกันภัยคุกคามบนเครือข่ายไร้สาย

15.2 สถานที่ทำการทดลอง/เก็บข้อมูล

มหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร

บทที่ 2
ระบบงานเดิม และทฤษฎีที่เกี่ยวข้อง

โครงการวิจัย การประเมินระบบความปลอดภัยของระบบเครือข่ายไร้สายมหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร ผู้วิจัยได้ทำการศึกษาค้นคว้าเอกสาร และการศึกษาระบบที่เกี่ยวข้องกับการพัฒนาระบบโดยแบ่งเป็นหัวข้อดังนี้

1. ระบบเครือข่ายคอมพิวเตอร์โดยทั่วไป
2. เครือข่ายไร้สาย Wireless LAN
3. เครือข่าย Wi-Fi
4. ระบบรักษาความปลอดภัยบนเครือข่าย Wi-Fi
5. Wi-Fi Protected Access (WPA)
6. Wi-Fi Protected Access version 2 (WPA2)
7. Kali Linux
8. งานวิจัยที่เกี่ยวข้อง

2.1 ระบบเครือข่ายคอมพิวเตอร์โดยทั่วไป

เครือข่ายคอมพิวเตอร์ (Computer Network) เป็นการเชื่อมต่อคอมพิวเตอร์ตั้งแต่ 2 เครื่องขึ้นไปเข้าหากัน เพื่อใช้สำหรับการติดต่อสื่อสารระหว่างคอมพิวเตอร์ที่อยู่ในองค์กรเดียวกัน หรือเชื่อมต่อระบบคอมพิวเตอร์ระหว่างองค์กรเพื่อแลกเปลี่ยนข้อมูลข่าวสารระหว่างกัน ซึ่งในปัจจุบันนี้การใช้คอมพิวเตอร์ในองค์กรต่างๆ เพื่อใช้ในการจัดการข้อมูลหรือการบริหารงานขององค์กรนั้นมีการขยายตัวเพิ่มขึ้น เนื่องจากองค์กรมีการขยายงานหรือขยายสาขาเพิ่มมากขึ้น การใช้เทคโนโลยีคอมพิวเตอร์เพื่อการประมวลผลข้อมูลขององค์กรก็มีมากขึ้นตามไปด้วย ประกอบกับเทคโนโลยีด้านการสื่อสารด้วยระบบคอมพิวเตอร์ได้ถูกนามาใช้ในการแลกเปลี่ยนข้อมูล การติดต่อสื่อสารกันเพื่อการตัดสินใจ การประมวลผลระหว่างหน่วยงานในองค์กร และการขอใช้ข้อมูลตลอดจนทรัพยากรหรืออุปกรณ์ต่างๆ ของระบบร่วมกัน ทำให้องค์กรมองเห็นความจำเป็นในการใช้ระบบเครือข่ายคอมพิวเตอร์ ดังนั้นการเชื่อมต่อคอมพิวเตอร์เข้าหากันภายในองค์กรให้เป็นเครือข่ายหรือการเชื่อมต่อเครือข่ายขององค์กรเข้ากับเครือข่ายคอมพิวเตอร์กับองค์กรอื่น จึงเป็นสิ่งที่ไม่สามารถหลีกเลี่ยงได้ ซึ่งการเชื่อมต่อเหล่านี้เป็นจุดเริ่มต้นของระบบเครือข่ายคอมพิวเตอร์ และในปัจจุบันทำให้มีการเชื่อมต่อระหว่างเครือข่ายขององค์กรเข้าหากันทั่วโลกจนกลายเป็นเครือข่ายขนาดใหญ่

2.1.1 ประเภทของระบบเครือข่าย (จรวย สาวิถี : 2551)

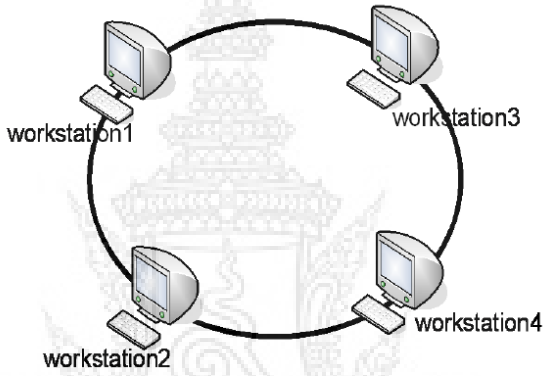
2.1.1.1. LAN (Local Area Network) ระบบเครื่องข่ายท้องถิ่น เป็นเน็ตเวิร์กในระยะทำงานไม่เกิน 10 กิโลเมตร ไม่ต้องใช้โครงข่ายการสื่อสารขององค์การโทรศัพท์ คือจะเป็นระบบเครือข่ายที่อยู่ภายในอาคารเดียวกันหรือต่างอาคาร ในระยะใกล้ๆ

2.1.1.2. MAN (Metropolitan Area Network) ระบบเครือข่ายเมือง เป็นเน็ตเวิร์กที่จะต้องใช้โครงข่ายการสื่อสารขององค์การ โทรศัพท์ หรือการสื่อสารแห่งประเทศไทย เป็นการติดต่อกันในเมือง เช่น เครื่องเวิร์กสเตชั่นอยู่ที่สุขุมวิท มีการติดต่อสื่อสารกับเครื่องเวิร์กสเตชั่นที่บางรัก

2.1.1.3. WAN (Wide Area Network) ระบบเครือข่ายกว้างไกล หรือเรียกได้ว่าเป็น World Wide ของระบบเน็ตเวิร์ก โดยจะเป็นการสื่อสารในระดับประเทศ ข้ามทวีปหรือทั่วโลก จะต้องใช้มีเดีย (Media) ในการสื่อสารขององค์การโทรศัพท์ หรือการสื่อสารแห่งประเทศไทย (คู่สายโทรศัพท์ dial-up / คู่สายเช่า Leased line / ISDN) (Integrated Service Digital Network สามารถส่งได้ทั้งข้อมูล เสียง และภาพในเวลาเดียวกัน)

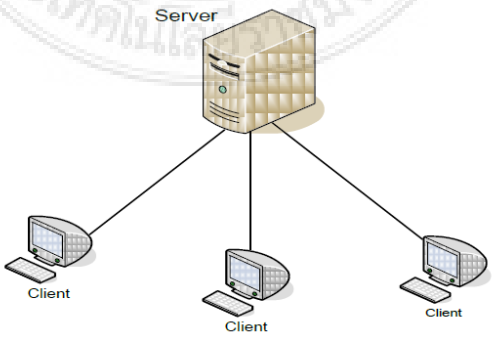
2.1.2 ประเภทตามหน้าที่ของคอมพิวเตอร์ในเครือข่าย

2.1.2.1 Peer To Peer เป็นระบบที่เครื่องคอมพิวเตอร์ทุกเครื่องบนระบบเครือข่ายมีฐานเท่าเทียมกัน คือทุก เครื่องสามารถจะใช้ไฟล์ในเครื่องอื่นได้ และสามารถให้เครื่องอื่นมาใช้ไฟล์ของตนเองได้เช่นกัน ระบบ Peer To Peer มีการทำงานแบบดิสทริบิวท์ (Distributed System) โดยจะกระจายทรัพยากรต่างๆ ไปสู่เวิร์กสเตชั่นอื่นๆ แต่จะมีปัญหาเรื่องการรักษาความปลอดภัย เนื่องจากข้อมูลที่เป็นความลับ จะถูกส่งออกไปสู่ คอมพิวเตอร์อื่นเช่นกันโปรแกรมที่ทำงานแบบ Peer To Peer คือ Windows for Workgroup และ Personal Netware



ภาพที่ 2-1 ระบบการทำงานแบบ Peer To Peer

2.1.2.2 Client / Server เป็นระบบการทำงานแบบ Distributed Processing หรือการประมวลผล แบบกระจาย โดยจะแบ่งการประมวลผลระหว่างเครื่องเซิร์ฟเวอร์กับเครื่องไคลเอ็นต์ แทนที่แอพพลิเคชั่นจะทำงานอยู่เฉพาะบนเครื่องเซิร์ฟเวอร์ ก็แบ่งการคำนวณของโปรแกรมแอพพลิเคชั่น มาทำงานบนเครื่องไคลเอ็นต์ด้วย และเมื่อใดที่เครื่องไคลเอ็นต์ต้องการผลลัพธ์ของข้อมูลบางส่วน จะมีการเรียกใช้ไปยัง เครื่องเซิร์ฟเวอร์ให้นำเฉพาะข้อมูลบางส่วนเท่านั้นส่งกลับ มาให้เครื่องไคลเอ็นต์เพื่อทำการคำนวณข้อมูลนั้นต่อไป



ภาพที่ 2-2 ระบบการทำงานแบบ Client / Server

2.1.3 อุปกรณ์ในระบบเครือข่ายคอมพิวเตอร์ (Network Equipment)

2.1.3.1 สายสัญญาณ (Cable) สายสัญญาณที่นำมาใช้เชื่อมต่อคอมพิวเตอร์และทรัพยากรอื่นๆในเครือข่าย สาย เคเบิลที่ใช้ในปัจจุบันมีหลายแบบด้วยกัน แต่ละแบบก็มี ความเร็วในการรับส่งข้อมูล และราคา แตกต่างกันไป ส่วนการเลือกใช้สายเคเบิลอย่างไรนั้น ขึ้นอยู่กับขนาดและประเภทของเครือข่ายที่ใช้

2.1.3.2 โมเด็ม (Modem) ย่อมาจากคำว่า "Modulator/Demodulator" กระบวนการที่โมเด็มแปลงสัญญาณดิจิทัลให้เป็นสัญญาณอนาล็อกเรียกว่า มอดูเลชั่น (Modulation) โมเด็มที่ทำ หน้าที่นี้เรียกว่า โมดูเล เตอร์ (Modulator) กระบวนการที่โมเด็มแปลงสัญญาณอนาล็อกให้เป็นสัญญาณดิจิทัล เรียกว่า ดีมอ ดูเลชั่น (Demodulation) โมเด็มที่ทำ หน้าที่นี้เรียกว่า ดีโมดูเลเตอร์ (Demodulator)

2.1.3.3 การ์ดเชื่อมต่อเครือข่ายหรือแลนการ์ด (Network Interface Card : NIC) อุปกรณ์ที่ใช้เชื่อมระหว่างคอมพิวเตอร์กับสายเคเบิลคือการ์ดเชื่อมเครือข่าย การ์ดนี้ส่วนใหญ่จะติดตั้งภายในเครื่องคอมพิวเตอร์ โดยเสียบลงบนเมนบอร์ดของคอมพิวเตอร์ ส่วนพอร์ต ในการเชื่อมต่อกับสายเคเบิลจะอยู่ทางด้านหลังของเครื่องคอมพิวเตอร์ ช่วยในการควบคุม การ รับส่งข้อมูล และตรวจสอบข้อผิดพลาดที่เกิดขึ้น

2.1.3.4 ฮับ (Hub) เป็นอุปกรณ์ที่ใช้ในการเชื่อมต่อสายเคเบิลในเครือข่ายมีลักษณะเป็นช่องเสียบสาย เคเบิลระหว่างเครื่องคอมพิวเตอร์เซิร์ฟเวอร์กับเครื่องพีซีอื่นๆ ที่ทำ หน้าที่เป็นเครื่องไคลเอนต์

2.1.3.5 รีพีตเตอร์ (Repeater) เป็นอุปกรณ์ที่ใช้ในการเปลี่ยนตัวกลางนำสัญญาณจากตัวกลางหนึ่งไปยังอีกตัวกลางหนึ่ง เช่น จากไฟเบอร์ออฟติกมายังโคแอกเชียล หรือการเชื่อมระหว่างตัวกลางเดียวกันก็ได้ การใช้รีพีตเตอร์จะทำให้เครือข่ายทั้งสอง เสมือนเชื่อมกัน โดยที่สัญญาณจะวิ่งทะลุถึงกันได้หมดรีพีตเตอร์จึงไม่มีการกันข้อมูล แต่จะมีประโยชน์ในการเชื่อมต่อความยาวให้ยาวขึ้น

2.1.3.6 บริดจ์ (Bridge) เป็นอุปกรณ์ที่มักจะใช้ในการเชื่อมต่อวงแลนเข้าด้วยกัน ทำให้สามารถขยายขอบเขตของ LAN ออกไปได้เรื่อยๆ โดยที่ประสิทธิภาพรวมของระบบ ไม่ลดลงมากนัก มักจะถูกใช้ในการเชื่อมเครือข่ายย่อยๆ ในองค์กรเข้าด้วยกันเป็นเครือข่ายใหญ่ เพียงเครือข่ายเดียว เพื่อให้เครือข่ายย่อยๆ เหล่านั้นสามารถติดต่อกับเครือข่ายย่อยอื่นๆ ได้

2.1.3.7 เราเตอร์ (Router) เป็นอุปกรณ์ที่ทำหน้าที่เชื่อมต่อระบบเครือข่ายหลายระบบเข้าด้วยกัน คล้ายกับบริดจ์ แต่มีส่วนการทำงานที่ซับซ้อนมากกว่าบริดจ์มาก โดยเราเตอร์จะมีเส้นทางการเชื่อมโยงระหว่างแต่ละเครือข่ายเก็บไว้เป็นตารางเส้นทาง เรียกว่า Routing Table ทำให้เราเตอร์สามารถทำหน้าที่จัดหาเส้นทางและเลือกเส้นทางที่เหมาะสมที่สุดในการเดินทาง เพื่อการติดต่อระหว่างเครือข่ายได้อย่างมีประสิทธิภาพ

2.1.3.8 เกตเวย์ (Gateway) เป็นอุปกรณ์ที่มีความสามารถสูงสุด ในการเชื่อมต่อเครือข่ายต่างๆเข้าด้วยกัน โดยไม่มีขีดจำกัด ทั้งระหว่างเครือข่ายต่างระบบ หรือแม้กระทั่งโปรโตคอลจะแตกต่างกันออกไป เกตเวย์จะแปลงโปรโตคอล ให้เหมาะสมกับอุปกรณ์ที่ต่างชนิดกัน จัดเป็นอุปกรณ์ที่มีราคาแพง และติดตั้งใช้งานยุ่งยาก เกตเวย์บางตัวจะรวมคุณสมบัติในการเป็นเราเตอร์ด้วยในตัว หรือแม้กระทั่งอาจรวมเอาฟังก์ชั่นการทำงาน ด้านการรักษาความปลอดภัยที่เรียกว่าไฟร์วอลล์ (Firewall) เข้าไว้ด้วย

2.2 เครือข่ายไร้สาย Wireless LAN (ชาพร โนนสินชัย, มุธิตา นาสมชัย: 2553)

เครือข่ายไร้สาย (Wireless LAN) เป็นเทคโนโลยีเครือข่ายไร้สาย ซึ่งทำให้เกิดการเปลี่ยนแปลงแนวคิดและวิธีการจัดการทางด้านเครือข่ายคอมพิวเตอร์ขององค์กรต่างๆ ทั้งในองค์กรเดิมที่มีเครือข่ายคอมพิวเตอร์อยู่แล้วและองค์กรที่เกิดขึ้นใหม่ที่กำลังวางแผนติดตั้งระบบเครือข่ายคอมพิวเตอร์ ซึ่ง Wireless LAN (WLAN) ไม่ใช่เทคโนโลยีเครือข่ายคอมพิวเตอร์ที่มาทดแทนเครือข่ายแบบใช้สัญญาณ (Wired Network) แต่เป็นเทคโนโลยีที่สามารถขยายเครือข่ายแบบใช้สัญญาณได้ นอกจากนั้นยังถูกไปใช้ในบริเวณที่การติดตั้งสายสัญญาณมีอุปสรรคทางด้านภูมิศาสตร์ หรือในบริเวณที่ต้องการความรวดเร็วในการติดตั้งเครือข่ายใหม่ สำหรับการทำงานแบบชั่วคราว ซึ่ง WLAN มีความสะดวก รวดเร็วในการติดตั้งและรวดเร็วในการเคลื่อนย้ายอุปกรณ์เครือข่ายในปัจจุบันเครือข่าย WLAN ได้มีการพัฒนามาตรฐานมาหลายมาตรฐาน และมาตรฐานที่ได้รับความนิยมใช้มากที่สุด คือ มาตรฐาน IEEE 802.11

IEEE ได้กำหนดคุณสมบัติสำหรับ WLAN มาตรฐาน IEEE 802.11 ซึ่งครอบคลุมทั้ง Physical Layer (PHY) และ Media Access Control (MAC) มาตรฐาน IEEE 802.11 มีการใช้งานครั้งแรกตั้งแต่ปี 1987 โดยเป็นส่วนหนึ่งของมาตรฐาน IEEE 802.11 (Token Bus) และทำงานอยู่ภายใต้กลุ่มที่เรียกว่า IEEE 802.4L ซึ่งการนา WLAN มาใช้งานครั้งแรกนั้นเป็นการใช้ภายในโรงงานอุตสาหกรรมการผลิตรถยนต์สำหรับการควบคุมและการติดต่อสื่อสารระหว่างเครื่องมือในปี 1990 กลุ่ม IEEE 802.4L WLAN ได้เปลี่ยนชื่อเป็น IEEE 802.11 และเป็นมาตรฐานอิสระของ IEEE 802 ที่กำหนดระดับ PHY และ MAC สำหรับ WLAN โดยมาตรฐานแรกของ IEEE 802.11 ใช้อัตราส่ง 1Mbps และ 2Mbps ได้เสร็จสมบูรณ์ตั้งแต่ปี 1997 โดยมีระดับของ PHY เป็นแบบ DSSS, FHSS และ Diffused Infrared (DFIR) เมื่อมาตรฐานแรกเสร็จสมบูรณ์แล้วหลังจากนั้นได้มีการกำหนดให้มี PHY ใหม่ที่รองรับอัตราส่ง 11 Mbps โดยใช้การเข้ารหัสแบบ CCK เรียกว่า IEEE 802.11b และอัตราส่ง 54 Mbps โดยใช้ PHY แบบ OFDM เรียกว่า IEEE 802.11a และทั้งสามรุ่นมีการทำงานในระบบ MAC ที่เหมือนกัน คือ การใช้กลไกของ Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) ในการใช้ช่องสัญญาณสำหรับการติดต่อสื่อสารมาตรฐานของ IEEE 802.11 ตั้งแต่เริ่มต้นจนถึงปัจจุบัน ที่มีการกำหนดสัญญาณความถี่และอัตราการส่ง มีดังนี้

1.) IEEE 802.11 เป็นมาตรฐานเริ่มต้นของ WLAN ที่ประกาศใช้เมื่อปี 1997 มีอัตราการส่ง 1 Mbps และ 2 Mbps โดยใช้สัญญาณวิทยุความถี่ 2.4 GHz และ 2.5 GHz ซึ่งเป็นเทคโนโลยีแบบ DSSS และ FHSS นอกจากนั้นยังมีการใช้คลื่นอินฟาเรดแบบ DFIR ในระดับชั้นของ PHY ด้วย ส่วนของระดับ MAC ใช้กลไกของ CSMA/CA ซึ่งในมาตรฐานเริ่มต้นนี้ยังมีปัญหาในระบบรักษาความปลอดภัยในการรับส่งข้อมูล และไม่มีระบบ Quality of Service (QoS) สำหรับการประกันคุณภาพในการให้บริการ

2.) IEEE 802.11a เป็นมาตรฐานที่ประกาศใช้ในปี 1999 หลังจาก IEEE 802.11b โดยใช้เทคโนโลยี OFDM และสามารถมีอัตราการส่งสูงถึง 54 Mbps โดยใช้คลื่นสัญญาณวิทยุความถี่ 5GHz ซึ่งเป็นคลื่นความถี่วิทยุของ Unlicensed National Information Infrastructure (U-NII) ที่มีสัญญาณรบกวนจากอุปกรณ์อื่นน้อยกว่าในย่านความถี่ 2.4 GHz โดยคลื่นความถี่นี้ไม่ได้รับอนุญาตให้ใช้ในบางประเทศ เช่น ประเทศไทย เพราะได้ถูกจัดสรรสำหรับกิจกรรมอื่นไปก่อนแล้ว

3.) IEEE 802.11b เป็นมาตรฐานที่ประกาศใช้ในปี 1999 หลังจาก IEEE 802.11 แล้ว มาตรฐาน IEEE 802.11b ใช้วิธีการเข้ารหัสสัญญาณข้อมูลแบบ CCK ร่วมกับเทคโนโลยี DSSS มีอัตราการส่งสูงถึง 11 Mbps โดยใช้สัญญาณวิทยุความถี่ 2.4 GHz มาตรฐาน IEEE 802.11b นี้เป็นที่รู้จักกันทั่วไปและเป็นที่ยอมรับกันทั่วโลก มีการผลิตอุปกรณ์สำหรับมาตรฐานนี้ออกมายอมรับการใช้งานเป็นจำนวนมาก โดยมีการเรียกชื่อใหม่ทำงการค้าว่า Wi-Fi (Wireless Fidelity) และกำหนดรายละเอียดโดยสมาคม Wireless Ethernet Compatibility Alliance (WECA) ที่ประกอบด้วยสมาชิกซึ่งเป็นบริษัทที่ผลิตอุปกรณ์ทำงด้านคอมพิวเตอร์และเครือข่ายการสื่อสารจำนวนมาก

4.) IEEE 802.11g มาตรฐานที่ประกาศใช้ในปี 2003 ใช้เทคโนโลยี OFDM และสัญญาณวิทยุความถี่ 2.4 GHz มีอัตราส่งสูงถึง 54 Mbps สามารถทำงานเข้ากันได้กับอุปกรณ์เครือข่าย WLAN มาตรฐาน IEEE 802.11b ที่องค์กรต่างๆได้ติดตั้งไปก่อนหน้านี้แล้ว โดยปัจจุบันเป็นมาตรฐานที่กำลังใช้กันอย่างแพร่หลาย และมีอุปกรณ์ในบางผลิตภัณฑ์ได้พัฒนาอัตราการส่งของ มาตรฐาน IEEE 802.11g ได้สูงถึง 108 Mbps แต่ยังมีปัญหาในการทำงานร่วมกับอุปกรณ์อื่น แต่สามารถทำงานร่วมกันได้กับผลิตภัณฑ์ของตนเองหรือที่ใช้เทคโนโลยีชิปเซ็ตแบบเดียวกัน

5.) IEEE 802.11n เป็นมาตรฐานที่ยังไม่ประกาศใช้อย่างเป็นทำงการ ซึ่งคาดว่าจะทำให้เทคโนโลยี WLAN มีอัตราการส่งเกิน 100 Mbps และอาจสูงถึง 600 Mbps โดยอุปกรณ์ของเครือข่ายมาตรฐาน IEEE 802.11n สามารถติดต่อสื่อสารกันได้มากกว่าหนึ่งช่องทำงการสื่อสาร โดยใช้สัญญาณวิทยุความถี่ทั้ง 2.4 GHz และ 5.8 GHz นอกจากนั้นมาตรฐานใหม่นี้ยังได้รวมเอาความสามารถของเทคโนโลยี Multiple Input Multiple Output (MIMO) ซึ่งเป็นเทคโนโลยีที่ใช้เทคนิค OFDM และเพิ่มอัตราการส่งให้กับอุปกรณ์ไร้สายโดยในขณะนี้ IEEE 802.11n ยังเป็นมาตรฐานสำหรับอนาคต แต่ก็มีบางผลิตภัณฑ์ที่ประกาศออกมาว่าตนเองมีเทคโนโลยีชิปเซ็ตที่สามารถรองรับการใช้เทคโนโลยีตาม Draft Stand นี้ เนื่องจาก WLAN มาตรฐาน IEEE 802.11 เป็นเทคโนโลยีเครือข่ายไร้สายที่ได้รับความนิยมอย่างแพร่หลายในการนำมาติดตั้งและใช้งานกับองค์กรต่างๆ ซึ่งในช่วงเริ่มต้นมีปัญหาในเรื่องของงระบบรักษาความปลอดภัยและไม่มีการรับประกันคุณภาพของการรับส่งข้อมูลหรือ QoS ดังนั้นทาง IEEE ได้ตั้งกลุ่มทำงานเพื่อการศึกษาและพัฒนาให้การใช้งานเครือข่ายมีประสิทธิภาพดีขึ้น ทำให้ปัจจุบันนอกจากมีมาตรฐานทางด้านอัตราความเร็วในการรับส่งข้อมูลที่ได้อธิบายทั้ง 5 มาตรฐานแล้ว ยังมีมาตรฐานอื่นๆที่เป็นเรื่องการเพิ่มประสิทธิภาพและการจัดการในด้านเทคนิคต่างๆ ของระบบเครือข่าย WLAN อีกเป็นจำนวนมาก ซึ่งในบางมาตรฐานได้ประกาศใช้แล้วและมีบางมาตรฐานกำลังอยู่ในช่วงการดำเนินการ โดยมีรายละเอียดดังนี้

1.) IEEE 802.11c เป็นมาตรฐานที่เพิ่มความเร็วในระดับ PHY ให้สูงขึ้น สำหรับสัญญาณความถี่ 2.4 GHz

2.) IEEE 802.11d เป็นมาตรฐานที่ทำให้ IEEE 802.11a และ IEEE 802.11b ดีขึ้นสำหรับการทำโรมมิ่งในพื้นที่บริเวณกว้าง โดยให้มีรายละเอียดที่สามารถตั้งค่าต่างๆ ในระดับ MAC ได้

3.) IEEE 802.11e เป็นมาตรฐานที่ปรับปรุง MAC Layer ของ IEEE 802.11 ให้สามารถรองรับการให้บริการสำหรับแอพพลิเคชั่นทางด้านมัลติมีเดีย โดยมีการรับประกันคุณภาพในการให้บริการ เรียกว่า Qos และสามารถนำไปใช้กับอุปกรณ์ในมาตรฐาน IEEE 802.11 ทุกรุ่น

4.) IEEE 802.11f เป็นมาตรฐานที่กำหนดโปรโตคอลสำหรับการบริการของ AP ที่เรียกว่า Inter Access Point Protocol (IAPP) ซึ่งเป็นโปรโตคอลที่ออกแบบมาสำหรับการจัดการกับ

ผู้ใช้บริการที่เคลื่อนที่ข้ามเขตการให้บริการของ AP ตัวหนึ่งไปยังตัวหนึ่ง AP อีกตัวหนึ่ง เพื่อให้เกิดการโรมมิ่งสัญญาณระหว่างเครือข่าย

5.) IEEE 802.11h เป็นมาตรฐานที่ปรับปรุง MAC Layer ของ IEEE 802.11 และ PHY Layer ของมาตรฐาน IEEE 802.11a ที่ทำงานในย่านความถี่ 5 GHz ให้ดีขึ้นโดยเป็นความพยายามของ IEEE ที่จะเชื่อมต่อกับเทคโนโลยีมาตรฐาน Hiper LAN/2 ของ ETSI ซึ่งเป็นเทคโนโลยี WLAN ที่มีการใช้ในยุโรป และมาตรฐานนี้มีจุดประสงค์เพื่อการพัฒนาอุปกรณ์ให้ได้มาตรฐาน IEEE 802.11h และสามารถทำงานถูกต้องตามความต้องการของประเทศในแถบยุโรป

6.) IEEE 802.11i เป็นมาตรฐานที่ปรับปรุง MAC Layer ของ IEEE 802.11 ให้ดีขึ้นในด้านการรักษาความปลอดภัยของการใช้เครือข่ายไร้สาย โดยมาตรฐานนี้ได้นาเอาเทคนิคขั้นสูงมาใช้ในการเข้ารหัส (Encryption) ด้วยคีย์ที่มีการเปลี่ยนค่าอยู่เสมอ โดยเรียกว่า Advanced Encryption Standard (AES) ซึ่งก่อนหน้านี้จะมีการเข้ารหัสข้อมูลด้วยคีย์ที่ไม่มีการเปลี่ยนแปลง นอกจากนั้นยังมีการพัฒนาเทคนิคในการรองรับสิทธิ์ (Authentication) ของการใช้เครือข่ายไร้สาย

7.) IEEE 802.11j เป็นมาตรฐานและข้อกำหนดของประเทศญี่ปุ่นสำหรับการเพิ่มคุณสมบัติของมาตรฐาน IEEE 802.11a ในช่วงความถี่ 4.9 – 5.0 GHz

8.) IEEE802.11k เป็นมาตรฐานที่ดาเนินในการเพิ่มประสิทธิภาพของระบบเครือข่าย WLAN เช่น การตัดสินใจในการโรมมิ่ง การจัดการช่องสัญญาณการจัดการ Hidden Node และการปรับแต่งค่าต่างๆให้เหมาะสมกับการทำงานของเครือข่าย

9.) IEEE 802.11m เป็นมาตรฐานและข้อกำหนดในการดูแลระบบเครือข่ายตามมาตรฐาน IEEE 802.11 ทั้งหมด ซึ่งกำลังมีการปรับและแก้ไขเพื่อให้มีเอกสารสำหรับอ้างอิง

10.) IEEE 802.11o เป็นมาตรฐานที่ดาเนินการในเรื่องของ Voice over WLAN หรือการใช้สัญญาณเสียงบนเครือข่ายไร้สายตามมาตรฐาน IEEE 802.11 ซึ่งเป็นการทำ Handoff ที่รวดเร็วขึ้นระหว่างที่มีการใช้สัญญาณเสียง และมีการจัดระดับความสาคัญของการจราจรทำเสียงบนข้อมูลทั่วไป

11.) IEEE 802.11p เป็นมาตรฐานที่ใช้ในการติดต่อสื่อสารในช่วงสั้นๆ ของ WLAN ที่สภาพแวดล้อมของการใช้งานในยานพาหนะ

12.) IEEE 802.11q เป็นมาตรฐานที่ดาเนินการในเรื่องของการใช้เครือข่าย WLAN ในรูปแบบของ VLAN

13.) IEEE 802.11r เป็นมาตรฐานที่ดาเนินการในเรื่องของการทำโรมมิ่งในระบบเครือข่าย WLAN โดยเป็นส่วนของการทำโรมมิ่งที่รวดเร็วระหว่าง AP หรือที่เรียกว่า Fast Handoff

14.) IEEE 802.11s เป็นมาตรฐานที่ดาเนินการสำหรับการเชื่อมต่อเครือข่าย WLAN แบบเมซ (Mesh Network) และให้โหนดในเครือข่ายแบบเมซสามารถตั้งค่าต่างๆในเครือข่ายได้

15.) IEEE 802.11t เป็นมาตรฐานของการทำงานในลักษณะคาดการณ์ล่วงหน้าของเครือข่ายไร้สายหรือ Wireless Performance prediction (WPP)

16.) IEEE 802.11u เป็นมาตรฐานที่เพิ่มเติมรายละเอียดต่างๆ เพื่อให้การทำงานดีขึ้นสำหรับการเชื่อมต่อเครือข่าย WLAN มาตรฐาน IEEE 802.11 กับเครือข่ายภายนอกอื่นๆ ที่ไม่ใช่มาตรฐาน IEEE 802

17.) IEEE 802.11v ดาเนินการสำหรับการจัดการเครือข่ายไร้สายหรือ Wireless Network Management ตามมาตรฐาน IEEE 802.11

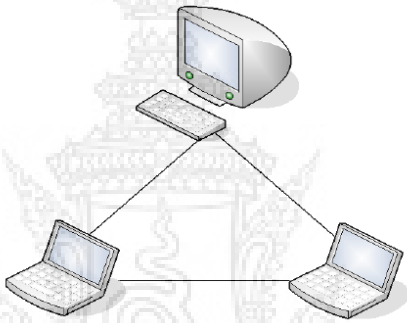
18.) IEEE 802.11w เป็นมาตรฐานที่จัดการและป้องกันเฟรมของ IEEE 802.11

19.) IEEE 802.11x เป็นหมายเลขที่ถูกสงวนไว้ไม่ให้มีการใช้งาน เพราะว่าจะทำให้สับสนกับมาตรฐาน IEEE 802.11x ซึ่งเป็นมาตรฐานที่กำหนดและควบคุมความปลอดภัยให้กับเครือข่ายในระดับพอร์ต

20.) IEEE 802.11y เป็นมาตรฐานที่กำหนดใช้งานในสหรัฐอเมริกา

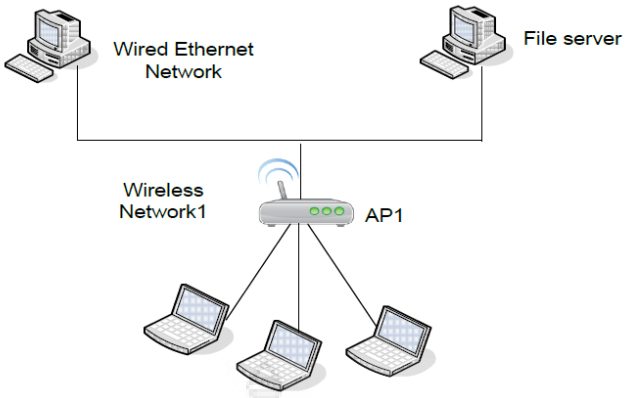
2.2.1 รูปแบบการเชื่อมต่อของระบบเครือข่ายไร้สาย

2.2.1.1 Peer-to-Peer (ad hoc mode) รูปแบบการเชื่อมต่อแลนไร้สายแบบ Peer to Peer เป็นการเชื่อมต่อแบบโครงข่ายโดยตรงระหว่างเครื่องคอมพิวเตอร์ โดยเครื่องคอมพิวเตอร์แต่ละเครื่องนั้นจะมีความเท่าเทียมกัน สามารถทำงานของตนเองได้ และขอใช้บริการเครื่องอื่นได้ จึงเหมาะสำหรับนามาใช้งานเพื่อจุดประสงค์ด้านความรวดเร็ว หรือติดตั้งได้โดยง่ายเมื่อไม่มีโครงสร้างพื้นฐานที่จะรองรับ ตัวอย่างเช่น ในศูนย์ประชุมหรือการประชุมที่จัดนอกสถานที่



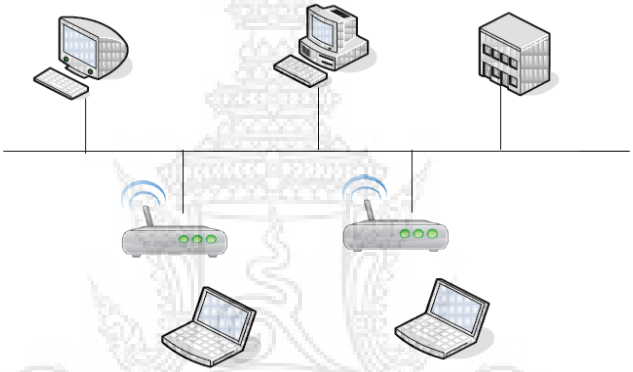
ภาพที่ 2-3 การเชื่อมต่อแบบ Peer-to-Peer (ad hoc mode)

2.2.1.2 Client/Server (Infrastructure mode) ระบบเครือข่ายไร้สายแบบ Client/Server (Infrastructure mode) มีลักษณะการรับส่ง ข้อมูลโดยอาศัย Access Point (AP) หรือเรียกว่า "Hot Spot" ทำ หน้าที่เป็นสะพานเชื่อมต่อระหว่าง ระบบเครือข่ายแบบใช้สาย กับคอมพิวเตอร์ลูกข่าย (Client) โดยจะกระจายสัญญาณคลื่นวิทยุเพื่อ รับ -ส่งข้อมูลเป็นรัศมีโดยรอบซึ่ง AP 1 จุด สามารถให้บริการเครื่องลูกข่ายได้ถึง 15-50 อุปกรณ์ เหมาะสำหรับการนาไปขยายเครือข่าย หรือใช้ร่วมกับระบบเครือข่ายแบบใช้สายเดิมใน Office ห้องสมุด หรือในห้องประชุม เพื่อเพิ่มประสิทธิภาพในการทำ งานให้มากขึ้น



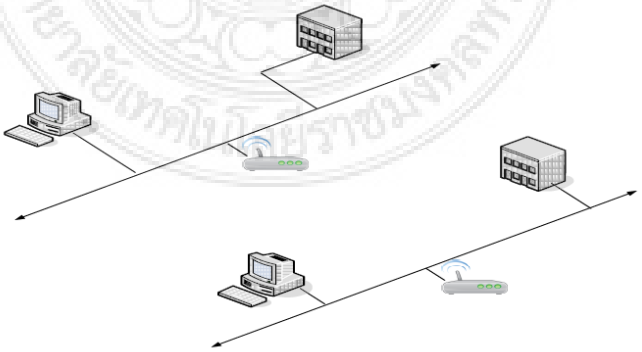
ภาพที่ 2-4 การเชื่อมต่อแบบ Client/Server

2.2.1.3 Multiple access points and roaming เป็นการเพิ่มจุดการติดตั้ง AP ให้มากขึ้น เพื่อให้การรับส่งสัญญาณในบริเวณของเครือข่าย ขนาดใหญ่เป็นไปอย่างครอบคลุมทั่วถึง



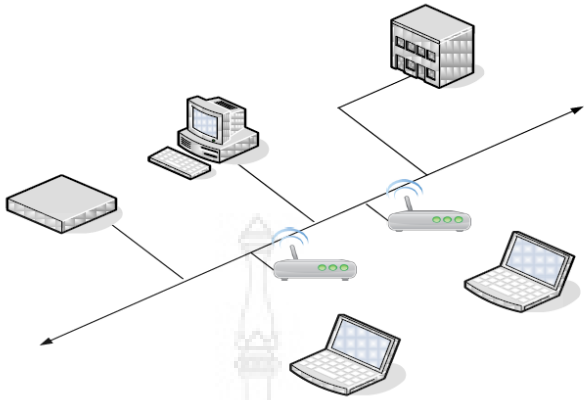
ภาพที่ 2-5 การเชื่อมต่อแบบ Multiple access points and roaming

2.2.1.4 Use of an Extension Point มีคุณสมบัติเหมือนกับ Access Point แต่ไม่ต้องผูกติดไว้กับเครือข่ายไร้สาย



ภาพที่ 2-6 การเชื่อมต่อแบบ Use of an Extension Point

2.2.1.5 The Use of Directional Antennas ระบบแลนไร้สายแบบนี้เป็นแบบใช้เสาอากาศในการรับส่งสัญญาณระหว่างอาคารที่อยู่ห่างกัน โดยการติดตั้งเสาอากาศที่แต่ละอาคารเพื่อส่งและรับสัญญาณระหว่างกัน



ภาพที่ 2-7 การเชื่อมต่อแบบ The Use of Directional Antennas

2.2.2 เทคโนโลยีในการส่งสัญญาณ 2.2.2.1 ประเภทที่ใช้สัญญาณคลื่นความถี่วิทยุ

1.) Narrow Band Technology เป็นระบบวิทยุแบบความถี่แคบ เป็นการรับส่งความถี่ 902 MHz ถึง 928 MHz, 2.14 MHz ถึง 2.484 และ 5.725 MHz ถึง 5.850 MHz สัญญาณจะมีกำลังต่ำ (โดยทั่วไปประมาณ 1 มิลลิวัตต์) และใช้ในการรับ-ส่งข้อมูลระหว่างต้นทางกับปลายทางเพียง 1 คู่เท่านั้น

2.) Spread Spectrum Technology ระบบเครือข่ายไร้สายส่วนใหญ่นิยมใช้เทคนิค Spread Spectrum Technology ซึ่งใช้ความถี่ที่กว้างกว่า Narrow Band Technology ซึ่ง Spread Spectrum คือ ช่วงความถี่ระหว่าง 902-928 MHz และ 2.4-2.484 GHz โดยการส่งสัญญาณเทคนิค Spread Spectrum สามารถแบ่งได้เป็น 2 แบบ คือ Direct Sequence และ Frequency-Hopping

3.) Direct Sequence Spread Spectrum (DSSS) Direct Sequence Spread Spectrum เป็นเทคนิคที่ยังใช้คลื่นพาหะที่ต้องระบุความถี่ที่ใช้ โดยมันสามารถส่งข้อมูลได้มากกว่าแบบ Narrow Band วิธีนี้เป็นวิธีที่เหมาะกับสภาพแวดล้อมที่มีการแทรกสอดรบกวนจากคลื่นวิทยุอื่น ๆ อย่างรุนแรง

4.) Frequency - Hopping Spread Spectrum (FHSS) การส่งสัญญาณรูปแบบนี้จะใช้ความถี่แคบพาหะเพียงความถี่เดียว (Narrow Band) โดยเน้นการนาไปใช้งาน ซึ่งจะเป็นตัวกำหนดว่า ถ้าคานึงถึงปัญหาทำงด้านประสิทธิภาพและคลื่นรบกวนก็ควรใช้ วิธี DSSS ถ้าต้องการใช้ Adapter ไร้สายขนาดเล็กและราคาไม่แพงสำหรับเครื่อง Notebook หรือเครื่อง PDA ก็ควรเลือกแบบ FHSS 5.) Orthogonal Frequency Division Multiplex (OFDM) เทคนิคนี้ถูกนามาใช้เพื่อเพิ่มความเร็วในการส่งข้อมูลตามมาตรฐานใหม่ ๆ ของระบบเครือข่ายไร้สาย คือ IEEE 802.11a และ 802.11g การส่งสัญญาณคลื่นวิทยุแบบนี้เป็นการ Multiplex สัญญาณโดยช่องสัญญาณความถี่จะถูกแบ่งออกเป็นความถี่พาหะย่อย (subcarrier) หลาย ๆ ความถี่ โดยแต่ละความถี่พาหะย่อยจะตั้งฉากซึ่งกันและกัน ทำให้มันเป็นอิสระต่อกัน ความถี่ที่คลื่นพาหะที่ตั้งฉากกันนั้นทำให้ไม่มีปัญหาการซ้อนทับของสัญญาณที่อยู่ติดกัน

2.2.2.3 Infrared Technology ลาแสงอินฟราเรด (Infrared : IR) เป็นส่วนหนึ่งของสเปกตรัมแม่เหล็กไฟฟ้าอยู่ในย่านความถี่ของแสงที่อยู่ต่ากว่าแสงสีแดงที่ตาของคน เราจะไม่สามารถมองเห็น ถูกนามาใช้เพื่อการสื่อสารที่ใช้ในระยะใกล้ ได้แก่ อุปกรณ์ควบคุมแบบไร้สาย (Wireless Remote Control) ที่ควบคุมเครื่องรับโทรทัศน์ เครื่องเล่นวีดีโอ เครื่องคอมพิวเตอร์ Notebook คุณสมบัติเด่นของคลื่นอินฟราเรดและคลื่นสั้น คือ เดินทางเป็นแนวตรง ราคาถูก แต่คลื่นประเภทนี้ไม่สามารถเดินทางผ่านวัตถุหรือสิ่งกีดขวางได

2.2.3 อุปกรณ์ใน WLAN

2.2.3.1 LAN Adapters

ทำหน้าที่เป็น Interface ระหว่าง OS ของระบบเครือข่ายกับเสาอากาศ เพื่อจะสร้างการเชื่อมต่อไปยังโครงข่ายอื่นต่อไป แบ่งได้ดังนี้

1.) แลนการ์ดไร้สายแบบ PCMCIA ใช้ติดตั้งกับเครื่องคอมพิวเตอร์แล็ปท็อป

2.) แลนการ์ดไร้สายแบบ PCI ใช้ติดตั้งกับเครื่องคอมพิวเตอร์เดสก์ท็อป

3.) แลนการ์ดไร้สายแบบ USB ใช้ได้ทั้งเครื่องคอมพิวเตอร์เดสก์ท็อปและแล็ปท็อป

4.) แลนการ์ดไร้สายแบบ CF ใช้ติดตั้งบนเครื่อง Pocket PC หรือ PDA

ภาพที่ 2-8 แสดงรูปการ์ดแลนไร้สายแบบต่างๆ

2.2.3.2 Wireless Access Point

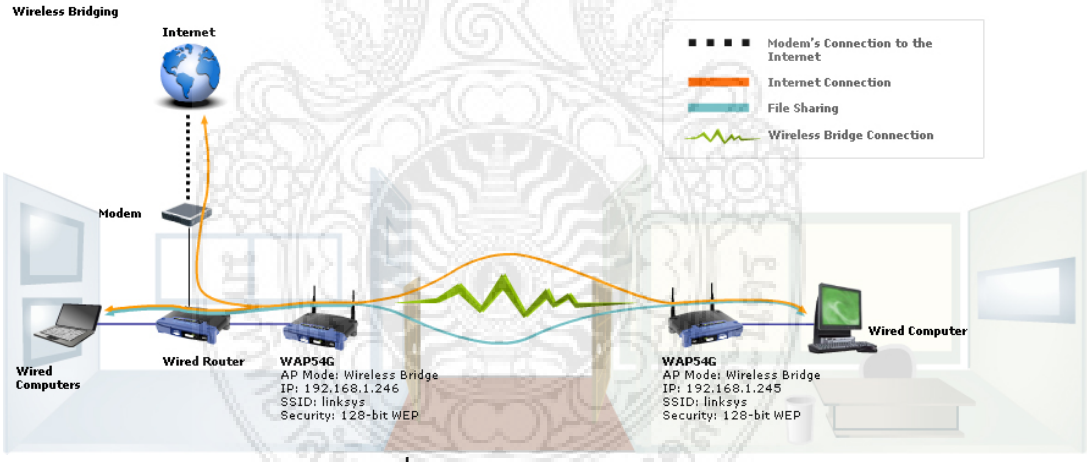
ทำหน้าที่คล้าย Hub ของระบบ LAN แบบใช้สาย โดยที่จะเป็นตัวรับเป็น Buffers และส่งข้อมูลระหว่าง WLAN และโครงสร้างแบบใช้สาย สนับสนุนการใช้งานของอุปกรณ์ไร้สายแบบเป็นกลุ่ม ซึ่งตัว AP มันจะเชื่อมต่อกับ Backbone ของโครงข่ายใช้สายผ่านมาตรฐานเคเบิลแบบ Ethernet และสื่อสารกับอุปกรณ์ไร้สายผ่านเสาอากาศ AP เป็นอุปกรณ์กระจายสัญญาณที่ใช้เป็นตัวกลางในการรับส่งข้อมูลระหว่างเครื่องคอมพิวเตอร์ที่ติดตั้งเครือข่ายไร้สายให้สมารถติดต่อสื่อสาร

กันได้ ลักษณะการทำงาน AP ทำหน้าที่เช่นเดียวกันกับ Switch ในระบบเครือข่ายใช้สาย โดย AP จะมีพอร์ต (Port) RJ-45 สำหรับใช้เพื่อเชื่อมต่อเข้ากับเครือข่ายใช้สายที่ใช้งานกันอยู่

ภาพที่ 2-9 แสดงรูป Access Point

2.2.3.3 Outdoor Wireless Bridge

ใช้สำหรับเชื่อมต่อระบบเครือข่ายกับอาคารอื่น ๆ ให้อัตรารับส่งข้อมูลสูง และมีรัศมีการรับส่งหลายกิโลเมตร แต่ต้องอยู่ในลักษณะระดับสายตา line-of-sight



ภาพที่ 2-10 แสดง Wireless Bridge

2.3 เครือข่าย Wi-Fi

Wi-Fi หรือที่ย่อมาจาก Wireless Fidelity เป็นเทคโนโลยีเครือข่ายไร้สาย LAN 802.11b ใช้หลักการทำงานไร้สาย โดยใช้จุดเชื่อมต่อสัญญาณ hotspots ติดตั้งตามจุดต่างๆ ทำให้สามารถนา Notebook ที่มี wireless lan และ CPU Intel Centrino ไปใช้ได้ทุกที่ที่ติดตั้งจุดเชื่อมต่อสัญญาณ hotspots ไว้ ให้สามารถทำงานได้ทุกที่ ไม่ว่าจะเป็นร้านกาแฟ สนามบิน ห้างสรรพสินค้า โรงแรม ให้ใช้งานผ่านเครือข่ายในการถ่ายโอนข้อมูลและใช้อินเตอร์เน็ตได้ทุกที่ที่มีสัญญาณจาก hotspot

2.3.1 ลักษณะการเชื่อมต่อของอุปกรณ์

2.3.1.1 โหมด Infrastructure โดยทั่วไปแล้วอุปกรณ์ในเครือข่ายวายฟาย จะเชื่อมต่อกันในลักษณะของโหมด Infrastructure ซึ่งเป็นโหมดที่อนุญาตให้อุปกรณ์ภายใน WLAN

สามารถเชื่อมต่อกับเครือข่ายอื่นได้ ในโหมด Infrastructure นี้จะประกอบไปด้วยอุปกรณ์ 2 ประเภทได้แก่ สถานีผู้ใช้ (Client Station) ซึ่งก็คืออุปกรณ์คอมพิวเตอร์ (Desktop, Laptop, หรือ PDA ต่างๆ) ที่มีอุปกรณ์ Client Adapter เพื่อใช้รับส่งข้อมูลผ่านวายฟาย และสถานีแม่ข่าย (Access Point) ซึ่งทำหน้าที่ต่อเชื่อมสถานีผู้ใช้เข้ากับเครือข่ายอื่น (ซึ่งโดยปกติจะเป็นเครือข่าย IEEE 802.3 Ethernet LAN) การทำงานในโหมด Infrastructure มีพื้นฐานมาจากระบบเครือข่ายโทรศัพท์มือถือ กล่าวคือสถานีผู้ใช้จะสามารถรับส่งข้อมูลโดยตรงกับสถานีแม่ข่ายที่ให้บริการ แก่สถานีผู้ใช้นั้นอยู่เท่านั้น ส่วนสถานีแม่ข่ายจะทำหน้าที่ส่งต่อ (forward) ข้อมูลที่ได้รับจากสถานีผู้ใช้ไปยังจุดหมายปลายทางหรือส่งต่อข้อมูลที่ได้ รับจากเครือข่ายอื่นมายังสถานีผู้ใช้

2.3.1.2 โหมด Ad-Hoc หรือ Peer-to-Peer เครือข่ายวายฟายในโหมด Ad-Hoc หรือ Peer-to-Peer เป็นเครือข่ายที่ปิดคือไม่มีสถานีแม่ข่ายและไม่มีการเชื่อมต่อกับเครือข่าย อื่น บริเวณของเครือข่ายวายฟายในโหมด Ad-Hoc จะถูกเรียกว่า Independent Basic Service Set (IBSS) ซึ่งสถานีผู้ใช้หนึ่งสามารถติดต่อสื่อสารข้อมูลกับสถานีผู้ใช้อื่นๆในเขต IBSS เดียวกันได้โดยตรงโดยไม่ต้องผ่านสถานีแม่ข่าย แต่สถานีผู้ใช้จะไม่สามารถรับส่งข้อมูลกับเครือข่ายอื่นๆได้

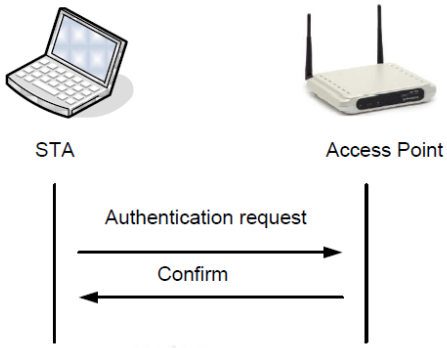
2.4 ระบบรักษาความปลอดภัยบนเครือข่าย Wi-Fi

เครือข่าย Wi-Fi มาตรฐาน IEEE 802.11 ในช่วงเริ่มต้นยังมีปัญหาในการรักษาความปลอดภัยสำหรับการส่งข้อมูล และเมื่อเครือข่ายประเภทนี้ได้รับความสนใจจากองค์กรต่างๆในการนำมาใช้งานอย่างแพร่หลาย กลุ่มทำงานของ IEEE 802.11 และผู้ผลิตอุปกรณ์เครือข่าย Wi-Fi ได้มีการพัฒนาระบบรักษาความปลอดภัยเพิ่มขึ้น ทำให้ปัจจุบันเทคโนโลยีและระบบรักษาความปลอดภัยที่รองรับการใช้งานได้อย่างมีประสิทธิภาพ และมีความปลอดภัยเพิ่มมากขึ้น โดยมีรายละเอียดต่างๆของเทคโนโลยีการรักษาความปลอดภัยสำหรับมาตรฐาน IEEE 802.11 มีดังนี้

2.4.1 Wired Equivalent Privacy (WEP) เป็นระบบการเข้ารหัสข้อมูลสำหรับมาตรฐาน IEEE 802.11 ที่ใช้อัลกอริทึ่มในการเข้ารหัส แบบ RC4 โดยมีการเข้ารหัส 2 รูปแบบ คือ การเข้ารหัสแบบ 64 บิท (คีย์ 40 บิทและอีก 24 บิทเป็น ข้อมูลที่ระบบสร้างขึ้น) และการเข้ารหัสแบบ 128 บิท ซึ่งในปัจจุบันใช้การเข้ารหัสแบบ 128 บิทมาก ขึ้นเพราะมีความปลอดภัยสูงกว่า โดยหลักการของ WEP นั้นได้กำหนดให้ระดับความปลอดภัยของ เครือข่าย Wireless เทียบเท่ากับเครือข่าย Wired

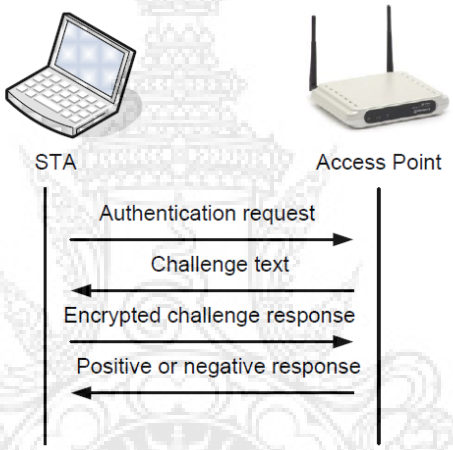
2.4.2 Authentication การทำ Authentication หรือการพิสูจน์สิทธิ์ของ STA ในมาตรฐาน IEEE 802.11 มี 2 วิธี คือ

2.4.2.1 Open System Authentication เป็นวิธีการพิสูจน์สิทธิ์ในแบบ 2 ทาง (2way) ซึ่งจะเริ่มต้นจากการที่ STA ส่ง Authentication request และรอรับคา ตอบที่เป็นการตอบรับหรือปฏิเสธจากการร้องขอนั้น



ภาพที่ 2-11 แสดงการทำ Open system Authentication

2.4.2.2 Shared Key Authentication เป็นกลไกของการพิสูจน์สิทธิ์ที่เป็นแบบ 4 ทำง (4way) โดยใช้วิธีการแชร์ Secret Key และมีหลักการทำ งานที่ดีกว่าแบบแรก ซึ่ง กระบวนการของ 4 way สามารถอธิบายละเอียด การทำ งานได้ดังนี้



ภาพที่ 2-12 แสดงการทำ Shared Key Authentication

1.) STA ส่งเฟรม Authentication request

2.) AP ตอบกลับด้วย Challenge text ซึ่งเกิดจากการสุ่มค่า

3.) STA เข้ารหัส Challenge text โดยใช้วิธีแบ่งปัน Secret Key และส่งกลับไปที่ AP

4.) AP ถอดรหัสโดยใช้วิธีการแชร์ Secret Key และเปรียบเทียบกับ Challenge text เดิม ก่อนที่จะส่งไปให้ STA ถ้า Challenge text ตรงกัน AP จะให้การตอบรับ Authentication request ของ STA นั้น

2.4.3 Advanced Encryption Standard (AES) เป็นรูปแบบของการเข้ารหัสข้อมูลแบบใหม่ที่กำลังมาแทนที่ WEP ที่ใช้อัลกอริทึม RC4 โดย AES ใช้อัลกอริทึม Rijndale ซึ่งกำหนดความยาวของคีย์ในการเข้ารหัสเป็น 3 รูปแบบคือการเข้ารหัส แบบ 128 บิท แบบ 192 บิทและ 256 บิท ซึ่งอัลกอริทึมของ AES เป็นระบบที่มีความปลอดภัยสูง สำหรับการเข้ารหัสข้อมูลและเป็นมาตรฐานที่เสร็จสิ้นแล้ว ดังนั้นจึงนำ AES ไปใช้กับเครือข่าย WLAN ในระดับ Campus Network ได้

โดยมีเซิร์ฟเวอร์เป็นศูนย์กลางที่สามารถส่งออกคีย์ได้โดย อัตโนมัติที่เรียกว่า Centralized Encryption Key Server

2.4.4 Wi-Fi Protected Access เป็นวิธีการเข้ารหัสที่มีการพัฒนามาพร้อมกับมาตรฐาน IEEE 802.11b หรือ Wi-Fi ซึ่งในปัจจุบันได้มีการพัฒนาอย่างต่อเนื่องถึงรุ่นที่ 2 โดยรายละเอียดการทำงานของ Wi-Fi Protected Access ทั้ง 2 รุ่นเป็นดังนี้

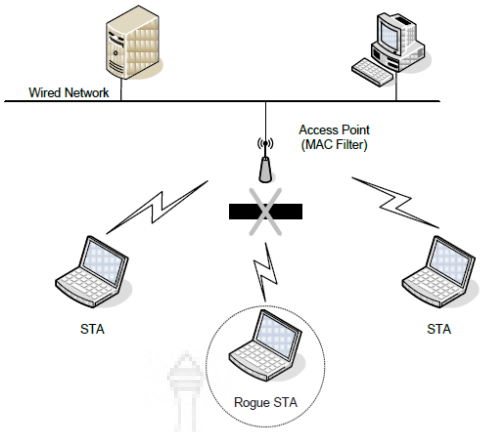
2.4.4.1 Wi-Fi Protected Access (WPA) เป็นวิธีการเข้ารหัสข้อมูลของกลุ่มทำงานในมาตรฐาน IEEE 802.11i ซึ่งเป็นการเข้ารหัสข้อมูลด้วยคีย์ 128 บิท และ 48 บิท IV(Initialization Vector) ที่ใช้ RC4 Stream cipher นอกจากนั้น WPA ยังมีการตรวจสอบความถูกต้องของความปลอดภัยได้มากกว่าการใช้วิธีการของ WEP ซึ่ง WPA จะใช้อัลกอริทึม Michael ที่ทำงานบนพื้นฐานของ MIC (Message Integrity Code) โดย MIC ที่ใช้ใน WPA จะรวมอยู่กับเฟรม Counter ซึ่งจะสามารถให้ความปลอดภัยกับข้อมูลได้

2.4.4.2 Wi-Fi Protected Access version 2 (WPA2) เป็นรุ่นที่ 2 ของ WPA ทำงานบนพื้นฐานของมาตรฐาน IEEE 802.11i และได้รับการทดสอบและแก้ไขโดย Wi-Fi Alliance วิธีการของ WPA2 เป็นปัจจัยสำคัญของมาตรฐาน IEEE 802.11i โดยเฉพาะเรื่องของการพิสูจน์สิทธิ์ของเมสเสจ และเมื่อมีการใช้วิธีการ WPA 2 ในการให้ความปลอดภัยข้อมูลในเครือข่าย WLAN อย่างเต็มรูปแบบแล้วจะสามารถนำมาใช้แทนที่อัลกอริทึม Michael ของ WPA ได้ ซึ่งจะเหมือนกับอัลกอริทึม RC4 ที่จะถูกแทนที่โดย AES

2.4.5 Filtering เป็นเทคนิคพื้นฐานด้านความปลอดภัยที่ใช้ตั้งแต่เริ่มต้นของการพัฒนามาตรฐาน โดย Filtering จะทำงานคล้ายกับ Access List ในเราเตอร์โดยกำหนดให้สถานีจะต้องทำตามคาสั่งในการเข้าใช้เครือข่าย ถึงแม้ว่า WLAN มีสถานีเป็นจำนวนน้อย แต่การมีระบบ Filtering ก็ถือได้ว่าระบบเครือข่ายมีระบบจัดการที่ดีและเหมาะสมในระดับหนึ่ง และหลักการพื้นฐานของการทำ Filtering ในเครือข่าย WLAN มี 3 ประเภท คือ

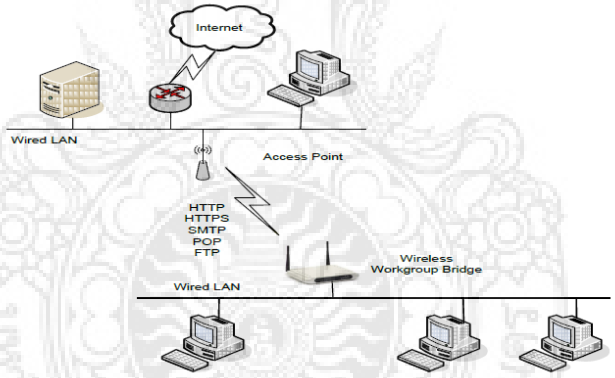
2.4.5.1 SSID Filtering เป็นวิธีการขั้นต้นของการทำ Filtering โดย Service Set IDdentifier (SSID) เป็นชื่อของเครือข่ายและเมื่อมีการนาไปใช้งานชื่อ SSID ของ STA จะต้องตรงกับ AP ใน Infrastructure Mode หรือตรงกับ STA อื่น ใน Ad-hoc Mode เพื่อยืนยันสิทธิ์ในการเข้าร่วมกับ BSS หรือ IBSS ดังนั้นผู้ที่ต้องการเข้าใช้งานเครือข่ายจะต้องรู้จักค่า SSID ของเครือข่ายเพื่อขอรับการตรวจสอบสิทธิ์ในการเข้าใช้บริการของเครือข่ายได้

2.4.5.2 MAC Address Filtering การใช้ AP ในเครือข่าย WLAN แบบ IEEE 802.11 จะมีฟังก์ชั่น และความสามารถที่ รองรับการกรองหมายเลข MAC Address ของ STA ที่ร้องขอและต้องการเข้าใช้เครือข่าย WLAN ว่า จะอนุญาตหรือไม่อนุญาตให้ใช้เครือข่าย โดยหลักการแล้วหมายเลข MAC Address ของ STA จะมีเพียงหมายเลขเดียวและคงที่ ทำ ให้สามารถจัดการและควบคุมการเข้าถึงเครือข่ายได้โดยการ ตรวจสอบ MAC Address และอนุญาตให้กับ MAC Address ที่รู้จักเท่านั้น



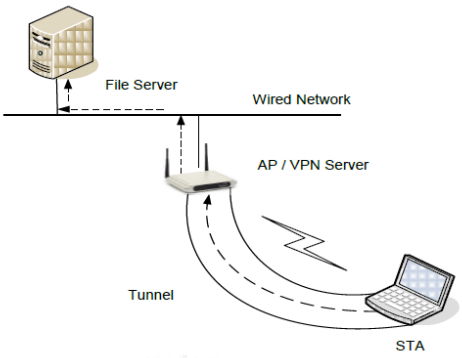
ภาพที่ 2-13 แสดงการทำ งาน MAC Filter

2.4.5.3 Protocol Filtering เป็นความสามารถในการเลือกข้อมูลที่จะทำการรับ - ส่งบนระบบเครือข่าย ที่ ต้องการจะให้ข้อมูลบางชนิดที่จะสามารถทำ การรับ-ส่งบนเครือข่าย WLAN ที่ทำ งานอยู่บน โปรโตคอลที่กำหนดไว้ได้เท่านั้น ถ้าเป็นข้อมูลที่อยู่บนโปรโตคอลอื่นๆ ก็จะไม่สามารถรับ-ส่งบน เครือข่าย WLAN ได้ ทำให้สามารถจัดการผู้ใช้ในระดับโปรโตคอลได้โดยไม่ต้องกรองในระดับแพค เก็ต



ภาพที่ 2-14 แสดงรูปแบบการทำ งานของ Protocol Filtering

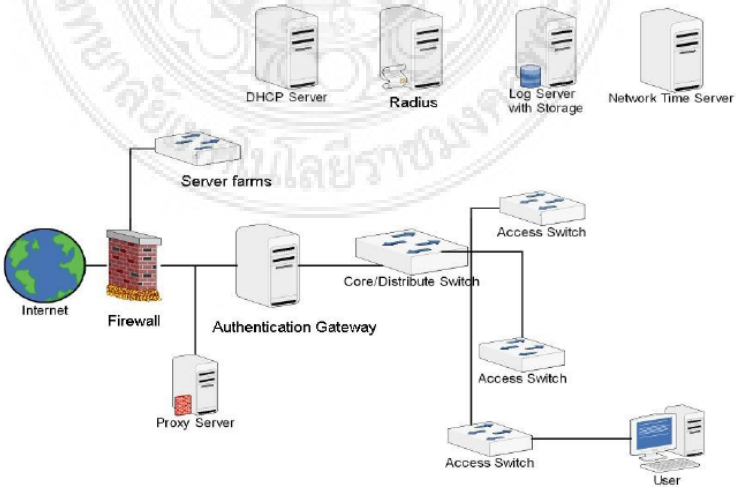
2.4.6 Wireless VPN เป็นเทคนิคที่ใช้ในการสร้างความปลอดภัยตั้งแต่ปี 1990 ซึ่งเป็นการใช้เพื่อเชื่อมต่อระหว่าง คอมพิวเตอร์หรือเครือข่ายที่อยู่ห่างไกลเข้ากับเครือข่ายขององค์กรโดยผ่านอินเตอร์เน็ต ซึ่งจาก หลักการเดิมของ VPN ก็คือเป็นการใช้งานโดยการเข้ารหัสแบบ Point to Point สำหรับผู้ใช้งานจาก ระยะไกล (Remote Users) ที่ต้องการเชื่อมต่อกับเครือข่ายขององค์กรโดยผ่าน Tunnel และในปัจจุบัน ยังมีการนำเอาเทคโนโลยี VPN มาประยุกต์ใช้ในเครือข่ายแบบ Wi-Fi มาตรฐาน IEEE 802.11 โดย การสร้าง VPN Tunnel เท่านั้น โดยการจราจรภายใน Tunnel เป็นการเข้ารหัสข้อมูลจนถึง VPN Gateway ดังนั้น จึงทำให้ผู้ไม่หวังดีกับเครือข่ายถูกบล็อกในการสื่อสารข้อมูลกับเครือข่ายทั้งหมด



ภาพที่ 2-15 การใช้ VPN ของ Wi-Fi

2.4.7 Remote Authentication Dial-in User Server (RADIUS) เป็นโปรโตคอลการพิสูจน์สิทธิ์ที่ได้รับความนิยมเป็นอย่างมากในการพิสูจน์สิทธิ์ของการใช้ งานเครือข่าย ซึ่งในช่วงเริ่มต้นเป็นโปรโตคอลที่ได้รับการออกแบบมาสำหรับรองรับการใช้งานกับ ระบบ Dial-in ผ่านอุปกรณ์โมเด็มของผู้ใช้งานเครือข่ายระยะไกล และสำหรับการใช้งานในเครือข่าย Wi-Fi นั้น RADIUS ถูกนำไปใช้เป็นเครื่องมือในการพิสูจน์สิทธิ์และการใช้ VPN

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 2-16 แผนภาพระบบเครือข่ายคอมพิวเตอร์โดยทั่วๆ ไป

ทำความรู้จักกับการพิสูจน์ตัวตน (Authentication) การพิสูจน์ตัวตน หนทางสู่ความปลอดภัยของข้อมูล

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

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 และมีสักษณะที่เป็นหนึ่งเดียวคือ 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) และสามารถสื่อสารข้าม

เครือข่ายสาธารณะได้อย่าง

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 ระบบจะทำการตรวจสอบกับเซิร์ฟเวอร์ก่อน 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 และเป็นวิธีการป้องกันที่ดีที่สุดเมื่อเปรียบเทียบกับวิธีการใช้การพิสูจน์ตัวตนโดยใช้ 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 เป็นต้น จึงมีการนำเทคโนโลยีนี้มาช่วยในการพิสูจน์ตัวตน เพื่อเพิ่มความปลอดภัยก่อนเข้าสู่ระบบ เช่น การใช้ควบคู่กับการใช้รหัสผ่าน ในขั้นตอนของการเก็บหลักฐานทางชีวภาพ จากตัวอย่างของภาพที่ 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) เป็นกุญแจที่ผู้สร้างจะส่งออกไปให้ผู้ใช้

อื่น 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)

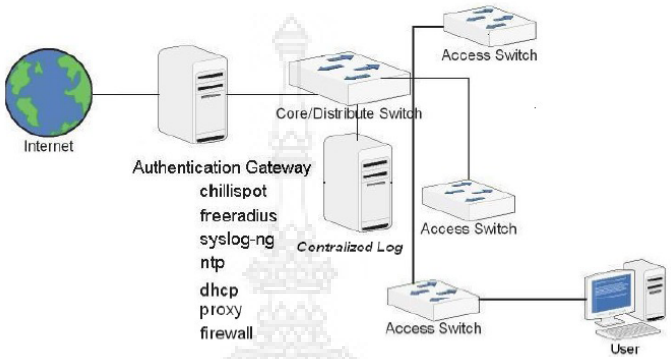
ในระบบเครือข่ายแบบเปิดหรืออินเตอร์เน็ต การพิสูจน์ตัวตนถือได้ว่าเป็นกระบวนการเริ่มต้นและมีความสำคัญที่สุดในการปกป้องเครือข่ายให้ปลอดภัย โพรโตคอลในการพิสูจน์ตัวตน คือ โพรโตคอลการสื่อสารที่มีกระบวนการพิสูจน์ตัวตนรวมอยู่ในชุดโพรโตคอล
โพรโตคอลหลักของการพิสูจน์ตัวตนที่นิยมใช้อย่างแพร่หลายบนอินเตอร์เน็ตในปัจจุบัน ประกอบไปด้วย

Secure Socket Layer (SSL)
Secure Shell (SSH)
Internet Security (IPSEC)
Kerberos

การรักษาความมั่นคงปลอดภัยของระบบคอมพิวเตอร์ หรือ ระบบเครือข่ายคอมพิวเตอร์เป็นสิ่งที่ควรตระหนักเป็นอย่างยิ่งในปัจจุบัน เพราะโลกในยุคปัจจุบันเป็นโลกแห่งข้อมูลข่าวสาร การเก็บรักษาข้อมูลให้ปลอดภัยจึงเป็นสิ่งสำคัญกับตัวบุคคลและองค์กร เพราะฉะนั้นการที่จะอนุญาตให้บุคคลใดบุคคลหนึ่งสามารถเข้าถึงข้อมูลจึงเป็นสิ่งที่ควรระมัดระวัง เพราะข้อมูลบางอย่างของบุคคลและองค์กรมีความสำคัญและไม่สามารถเปิดเผยต่อบุคคลภายนอกได้

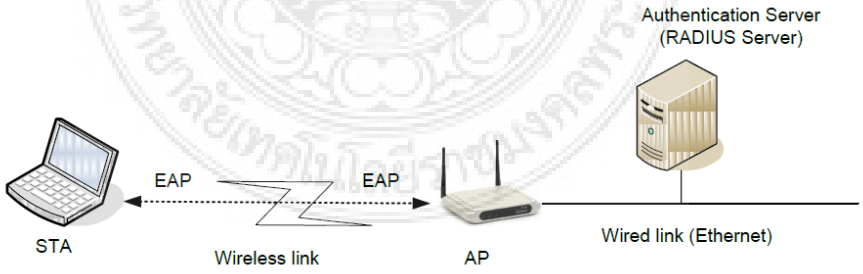
การพิสูจน์ตัวตนจึงมีความสำคัญ เนื่องจากว่าการที่บุคคลใดบุคคลหนึ่งจะเข้าสู่ระบบได้จะต้องได้รับการยอมรับว่าได้รับอนุญาตจริง การตรวจสอบหลักฐานจึงเป็นขั้นตอนแรกก่อนอนุญาตให้เข้าสู่ระบบ การยืนยันตัวตนยิ่งมีความซับซ้อนมาก นั่นก็หมายถึงว่าความปลอดภัยของข้อมูลก็มี

มากขึ้นด้วย องค์กรต่าง ๆ จะต้องกระทำสิ่งที่จะเป็นในการปกป้องข้อมูลที่สำคัญ ไม่เพียงแค่ป้องกันการบุกรุกเท่านั้น แต่จะต้องหลีกเลี่ยงผลกระทบที่อาจตามมา ดังนั้นถ้าหากว่าข้อมูลได้รับการป้องกันนั้นมีความสำคัญอย่างยิ่งต่อความสำเร็จขององค์กร ระบบในการตรวจสอบผู้ใช้งานที่มีประสิทธิภาพเป็นสิ่งที่จะต้องพิจารณาอย่างยิ่ง โดยที่มีอยู่หลายวิธีให้เลือกใช้กันในปัจจุบัน ดังนั้นการเลือกวิธีที่นำมาใช้นั้นจะต้องเป็นวิธีที่ให้ความมั่นใจได้เป็นอย่างดี การพิจารณาจะต้องไม่เพียงแค่จะต้องสามารถทำงานได้ในปัจจุบันเท่านั้น แต่วิธีการที่เลือกระบบรักษาความปลอดภัยจะต้องสามารถทำงานได้ดีในอนาคตอีกด้วย



ภาพที่ 2-17 แผนภาพระบบเครือข่ายคอมพิวเตอร์ที่ติดตั้งซอฟต์แวร์ที่ตัวอุปกรณ์ Authentication Gateway

2.4.8 มาตรฐาน 802.1x และโปรโตคอล EAP มาตรฐาน 802.1x เป็นสถาปัตยกรรมแบบใหม่ของการพิสูจน์สิทธิ์ที่กำหนดโดย คณะกรรมการ IEEE 802 ซึ่งหลักการของมาตรฐาน 802.1x เป็นแนวทำงในการพิสูจน์สิทธิ์(ไม่ใช่ โปรโตคอล) โดย 802.1x ถูกนำไปใช้ในเครือข่ายแบบ Wi-Fi และเครือข่ายแบบ Ethernet หลักการ ของสถาปัตยกรรม 802.1x ถูกเรียกว่า Port-based Network Access Control เพราะเกี่ยวข้องกับการ รองรับและอนุญาตให้กับผู้ใช้เครือข่ายที่มีสิทธิ์ในการเข้าใช้งานอย่างถูกต้อง โดยมีการเชื่อมต่อที่ ระดับ Layer 2 เท่านั้น สำหรับเครือข่ายแบบ IEEE 802.11 นั้นมีมาตรฐาน 802.1x มีความสามารถในการทำงานได้เป็นอย่างดีกับ AP



ภาพที่ 2-18 สถาปัตยกรรมของ 802.1x

EAP เป็นโปรโตคอลที่ทำงานในระดับ Layer 2 ซึ่งถูกพัฒนามาแทนโปรโตคอล PAP (Password Authentication Protocol) และ CHAP (Challenge Handshake Authentication Protocol) ที่ ทำงานภายใต้โปรโตคอล PPP (Point to Point Protocol) บนเครือข่ายแลน โดย EAP เป็นโปรโตคอลที่อนุญาตให้มีการแสดงสิทธิ์ของการใช้เครือข่าย Wi-Fi

2.5 Wi-Fi Protected Access (WPA)

เป็นมาตรฐานความปลอดภัยข้อมูลที่พัฒนาขึ้นมาโดยองค์กร Wi-Fi Alliance (WECA) เพื่อแก้ไขจุดอ่อนของ WEP ในเรื่องการเข้ารหัสข้อมูล ถูกประกาศให้เป็นมาตรฐานในเดือนพฤศจิกายน ค.ศ.2002 การพัฒนา WPA อยู่บนพื้นฐานเดียวกับมาตรฐาน IEEE802.11i ของสถาบันวิศวกรรมไฟฟ้าและอิเล็กทรอนิกส์ (IEEE) WPA จะถูกนำมาใช้ทดแทน WEP เพื่อแก้ไขจุดอ่อนในเรื่องการเข้า/ถอดรหัสข้อมูลด้วย WEP Key โดยการนำเอา Dynamic Key Distribution และการตรวจสอบและพิสูจน์สิทธิผู้ใช้งาน IEEE802.1X มารวมไว้เป็นกลไกของ WPA อุปกรณ์ไวร์เลสที่สนับสนุนมาตรฐาน WPA จะมีโหมดการทำงานให้เลือก 2 โหมด ดังนี้

2.5.1 WPA Pre-Shared Key โหมดการทำงาน Pre-Shared Key ออกแบบมาสำหรับเครือข่ายไวร์เลสแลนที่ใช้ภายในบ้านหรือในสำนักงานขนาดเล็ก (Home Office Small Office : SOHO) เพื่อสร้างความปลอดภัยให้แก่ข้อมูล เนื่องจากโหมดนี้ไม่ต้องการ RADIUS Server สำหรับการตรวจสอบและพิสูจน์สิทธิของผู้ใช้งาน Pre-Shared Key จะใช้กลไกการเข้า/ถอดรหัสข้อมูลสองแบบคือ แบบแรกใช้ TKIP(Temporal Key Integrity Protocol) ร่วมกับ MIC(Message Integrity Code หรือเรียกว่า Michael) และแบบที่สอง AES (Advanced Encryption Standard) ทั้งสองกลไกมีระดับความปลอดภัยสูงกว่า WEP หลายเท่า

2.5.2 Temporal Key Integrity Protocol เทคนิคการใช้คีย์ชั่วคราวเพื่อเข้ารหัส TKIP เป็นกลไกการเข้ารหัสที่ยังคงใช้เทคนิค RC4 เช่นเดียวกับ WEP แต่ได้มีการปรับปรุงการทำงานให้มีประสิทธิภาพที่เหนือกว่า WEP ดังนี้

1.) ทุกๆ แพ็กเก็ตข้อมูลที่สร้างขึ้นจากการสื่อสารระหว่าง AP กับเครื่องคอมพิวเตอร์ไร้สายจะถูกเข้ารหัสด้วยคีย์ที่แตกต่างกันออกไป (Dynamic Ciphering Keys) ทำให้ยากแก่การเดาคีย์ที่ถูกต้อง

2.) ใช้กลไก Message Integrity Checking (MIC) เพื่อทำให้แน่ใจว่าข้อมูลที่อยู่ระหว่างการสื่อสารจะไม่ถูกปลอมแปลงจากผู้บุกรุก

3.) จำนวนบิต Initialization Vector (IV) hashing ขนาด 48 บิต ซึ่งสูงกว่า IV ของ WEP ที่มีจำนวนแค่ 24 บิต (ค่า IV นี้ถูกนาไปรวมกับคีย์ที่ผู้ใช้ต้องใส่เพื่อใช้สำหรับการเข้ารหัสและถอดรหัส) การที่มีจำนวนบิตมากกว่าทำให้การเดาค่านี้ทำได้ยากขึ้น

2.6 Wi-Fi Protected Access version 2 (WPA2)

จากเทคโนโลยี WPA ในหัวข้อที่ 2.5 ที่ไม่สามารถแก้ปัญหาการคำนวณหา IV ของ WEP ได้อย่างสิ้นเชิง ทำให้มีการพัฒนา WPA เป็น WPA2 ขึ้น มาตรฐาน WPA2 ได้พัฒนาโดยใช้พื้นฐานของ IEEE 802.1X รวมถึงใช้วิธีการเข้ารหัสแบบ AES (Advanced Encryption Standard) ด้วยกุญแจขนาด 128,192 หรือ 256 บิต เทคโนโลยี AES มีชื่อเรียกว่า AES-CCMP (Advanced Encryption Standard – Counter Mode CBC-MAC Protocol) ซึ่งเป็นวิธีการเข้ารหัสแบบเป็นบล็อก โดยอ้างอิงจากการเข้ารหัสบล็อกที่ผ่านมา เพื่อทำให้การเข้ารหัสเปลี่ยนแปลงตลอดเวลา ทำให้ผู้บุกรุกไม่สามารถคาดเดาการเข้ารหัสได้ ร่วมกับวิธีการตรวจสอบความถูกต้องของข่าวสารที่ว่า CBC (Cipher

Block Chaining) โดย CBC จะสร้างรหัส MIC (Message Integrity Code) เพื่อใช้เป็นรหัสตรวจสอบว่าข่าวสาร (Message Authentication Code, MAC) จึงเป็นที่มาของ CBC-MAC องค์ประกอบอีกส่วนของ AES-CCMP คือ CCM (Counter mode-CBC MAC) ทั้งนี้ CCM ใช้ Counter เพื่อเปลี่ยนแปลงตัวเลขของข้อมูลหลังการเข้ารหัสในแต่ละครั้งไม่ให้เหมือนกัน เพื่อไม่ให้ได้ Ciphertext ที่เหมือนกัน ด้วยความที่ AES ซึ่งเป็นวิธีที่ทำให้ผู้บุกรุกไม่สามารถอ่านข่าวสารได้นามาแทนวิธีเข้ารหัสแบบเดิมที่ใช้ RC4 Cipher และ IV จึงสามารถแก้ปัญหาของ WEP ได้ WPA2 ได้ยกเลิกการใช้ RC4 และ IV ที่เป็นพื้นฐานของ WEP และ WPA ทำให้การเจาะเข้าระบบทำได้ยากกว่า WEP และ WPA2 ยังมีการพิสูจน์ตัวตน 2 รูปแบบด้วยกันคือ

2.6.1 WPA2 Personal เป็นการสร้างการพิสูจน์ตัวตนเสมือน ระหว่างผู้ใช้และ Access Point ด้วย PSK (Pre Share Key) หรือ PMK (Pairwise Master Key) ซึ่ง PMK ที่สร้างขึ้นจะเหมือนกันในทุก ๆ เครื่องลูกข่ายโดยที่ PTK (Pairwise Transient Key) จะถูกสร้างขึ้นต่อจาก PMK

2.6.2 WPA2 Enterprise เป็นการเชื่อมต่อด้วยมาตรฐาน 802.1X บนโปโตคอลที่ชื่อ RADIUS โดย WPA รูปแบบนี้จะประกอบด้วย 2 ส่วนหลักคือการควบคุมพอร์ททีใช้รับส่งข้อมูลและโปรโตคอลที่จัดการเกี่ยวกับวิธีการรับส่งกุญแจ ซึ่ง WPA2 Enterprise จะใช้การพิสูจน์ตัวตนที่อ้างอิงผู้ใช้เป็นหลัก ระหว่างเครื่องลูกข่ายและ EAP Server

2.7 Kali Linux

ภาพที่ 2-19 Logo ของ Software Kali Linux

ระบบเครือข่ายไร้สายนั้นมีส่วนสำคัญยิ่งในปัจจุบัน เพราะอิทธิพลของอินเทอร์เน็ต โซเชี่ยลเน็ตเวิร์ก ฯลฯ ทำให้ทุกคนต่างมีความต้องการเข้าถึงระบบอินเทอร์เน็ต และระบบเครือข่ายไร้สายหรือ Wi-Fi ก็ถือว่าเป็นช่องทำงที่สะดวกมากที่สุด และมีคนนิยมใช้มากที่สุดเช่นกันอะไรที่มีคนนิยมใช้มากที่สุด ก็ย่อมตกเป็นเป้าหมายของคนอีกกลุ่มหนึ่ง ที่เรามักจะรู้จักกันดีในนาม “แฮกเกอร์” ที่ผ่านมาหลายคนคงเคยได้ยินข่าวคราวเป็นระยะๆ ที่เกี่ยวข้องกับแฮกเกอร์ในการพยายามแฮกหรือโจมตีระบบความปลอดภัยต่างๆ คำว่า “แฮกเกอร์” นั้นมาจากคำว่า Hack ซึ่งหมายถึงการเจาะช่องโหว่หรือ ทำลายระบบ ที่มีคนป้องกันไว้ ในอีกแง่หนึ่ง การแฮกนั้นก็ทำเพื่อทดสอบระบบความปลอดภัยว่ามีความแข็งแรงมากแค่ไหน มีช่องโหว่ตรงไหนบ้าง เพื่อที่จะได้แก้ไขและอุดรอยรั่วนั้น

ดังนั้นจะเห็นได้ว่า การแฮกระบบเครือข่ายไร้สายนั้นทำได้ กระบวนการและวิธีต่างๆ นั้น เรียกได้ว่าพัฒนามาควบคู่กับการเริ่มต้นระบบความปลอดภัยเลยทีเดียว ซึ่งวิธีที่ผมนำมาแฉในวันนี้ เรียกได้ว่าเป็นแค่วิธีการหนึ่งที่แฮกเกอร์ใช้ โดยที่ผมเองก็ไม่ได้มีความรู้เรื่องระบบเน็ตเวิร์กอะไร มากมาย แต่ก็สามารถพิสูจน์ให้คุณผู้อ่านเห็นภาพว่า แม้เป็นแค่แฮกเกอร์มือสมัครเล่น ก็สามารถใช้ เครื่องไม้เครื่องมือที่มีให้ดาวน์โหลดอยู่ทั่วไปตามอินเทอร์เน็ต และนำมาแฮกระบบได้อย่างไม่ยากเย็น อะไรเลย

สำหรับผู้ที่มีอาชีพในการรทดสอบเจาะระบบเพื่อตรวจสอบความปลอดภัย รวมไปถึงผู้ที่ สนใจย่อมคุ้นเคยกับชื่อ BackTrack ดีอยู่แล้ว มันเป็นระบบปฏิบัติการลินุกซ์ซึ่งได้รับความนิยมอย่าง แพร่หลายในการใช้งานด้านความปลอดภัย สำหรับตอนนี้ทำง Offensive Security ทีมผู้พัฒนา BackTrack ได้เปิดตัวระบบปฏิบัติการขึ้นใหม่ภายใต้ชื่อ Kali Linux โดยมุ่งไปยังกลุ่มเป้าหมายระดับ ในธุรกิจ

Kali Linux ในเวอร์ชันแรกนี้มีความแตกต่างจาก BackTrack ตรงที่ Kali Linux ได้เชื่อมต่อ โดยตรงกับ repositories ของทำง Debian ซึ่งทำให้การอัพเดตนั้นง่ายขึ้นและประหยัดเวลาลง รองรับการปรับแต่งตัวระบบปฏิบัติการเพื่อสร้างเวอร์ชันที่เหมาะสำหรับตัวผู้ใช้เอง อีกทั้งยังรองรับ การทำงานของ ARM ทำให้สามารถติดตั้งได้ทั้งบน Chromebook, Raspberry Pi หรือแท็บเลต รวมถึงสามารถพัฒนาโปรเจคทำงด้านฮาร์ดแวร์ได้จากเครื่องมือที่ถูกเตรียมมาแล้วได้อีกด้วย ซึ่ง แน่นอนว่ายังรองรับหลากหลาย desktop environments แล้วแต่ผู้ใช้งาน

2.8 งานวิจัยที่เกี่ยวข้อง

ศุภวิทย์ วรรณภิละ, ตรัสพงศ์ ไทยอุปถัมภ์, ธัญลักษณ์ จิระเพชรอำไพ และ สัจจะ ตันจันทร์ พงศ์ (2549: บทคัดย่อ) ได้ทำการวิจัยเกี่ยวกับเรื่อง การใช้งานและการเปรียบเทียบประสิทธิภาพ ระบบความปลอดภัยเครือข่ายท้องถิ่นไร้สายกรณีศึกษา ระบบเครือข่ายไร้สายมหาวิทยาลัยเชียงใหม่ จากที่มหาวิทยาลัยเชียงใหม่ได้ติดตั้งเครือข่ายไร้สายขึ้นที่ใช้ชื่อว่า Jumbo-Net ซึ่งบริการตามจุด ต่างๆ ในบริเวณมหาวิทยาลัยซึ่งมีการให้บริการสองแบบคือแบบไม่เข้ารหัสสัญญาณ (Jumbo-Net) และแบบเข้ารหัสสัญญาณด้วย WPA (Jumbo-Secure) โครงงานนี้เป็นการเปรียบเทียบประสิทธิภาพ ระหว่างทั้งสองแบบ โดยใช้การทดลองสามแบบคือ การทดลองที่หนึ่งเป็นการทดลองส่งผ่านข้อมูล แบบไม่ขึ้นกับเวลาจริง ซึ่งทดลองโดยการหาค่าเวลาเฉลี่ยจากการดาวน์โหลดไฟล์ขนาด 5M, 15M และ 30M จาก FTP Server การทดลองที่สองเป็นการทดลองส่งผ่านข้อมูลแบบที่ขึ้นกับเวลาจริง ทดลองโดยการวัดแบนด์วิธเฉลี่ยในการรับชมวีดีโอสตรีมมิ่งที่ส่งมายังเครื่องลูกข่ายจำนวน 1, 2 และ 3 post และการทดลองที่สามเป็นการหาค่าเฉลี่ยเวลาตอบสนองระบบโดยการ ping จำนวน 1000 package ที่ขนาด package 64, 512 และ 1024 bytes ผลการทดลองปรากฏว่าแบบเข้ารหัสมี ประสิทธิภาพต่ำกว่าเพียงเล็กน้อย แต่จากการสำรวจความคิดเห็นของผู้ใช้บริการพบว่าผู้ใช้บริการ ส่วนใหญ่ยังใช้บริการแบบที่ไม่เข้ารหัสสัญญาณมากกว่าเนื่องจากการเข้าใช้บริการมีความยุ่งยากน้อย กว่า จึงควรส่งเสริมให้ผู้ใช้บริการมาใช้บริการแบบที่เข้ารหัสสัญญาณเนื่องจากมีความปลอดภัย มากกว่าโดยที่ประสิทธิภาพลดลงเพียงเล็กน้อย

จิตรพี สุริยะโชติ (2551: บทคัดย่อ) ได้ทำการวิจัยเกี่ยวกับเรื่อง การปรับปรุงประสิทธิภาพใน มาตรฐาน IEEE 802.11i สำหรับองค์กรขนาดเล็ก อุปกรณ์สื่อสารแบบไร้สายส่งข้อมูลด้วยคลื่นวิทยุ ไปในอากาศทำให้ง่ายต่อการดักจับข้อมูล หากไม่มีการป้องกัน อีกทั้งยังทำให้ถูกโจมตีได้ง่ายด้วยการ

โจมตีแบบ Man-in-the-Middle Attack ที่ใช้อุปกรณ์สื่อสารไร้สายที่สร้างขึ้นเพื่อปลอมแปลงการส่งข้อมูล การใช้เทคโนโลยีความมั่นคงแบบ WPA2 Enterprise สามารถป้องกันการโจมตีประเภทนี้ได้ด้วยการใช้เครื่องแม่ข่ายสำหรับพิสูจน์ตัวตน ทำให้มีค่าใช้จ่ายเพิ่มขึ้นซึ่งไม่เหมาะสมสำหรับองค์กรขนาดเล็กที่มีเครือข่ายขนาดเล็ก งานวิจัยนี้จึงนาเสนอการใช้งานเครือข่ายไร้สายที่มีความปลอดภัยแบบ WPA2 Enterprise โดยจาลองการทำงานของเครื่องแม่ข่ายสำหรับพิสูจน์ตัวตนภายในอุปกรณ์ Access Point ทำให้ไม่มีค่าใช้จ่ายเพิ่มขึ้น และนำเสนอผลการทดสอบของระบบด้วยโปรโตคอล EAP-TLS, EAP-TTLS, EAP-PEAP แบบที่ใช้การพิสูจน์ตัวตนแบบ RSA และแบบ Elliptic Curve ที่เหมาะสำหรับใช้กับ Access Point ที่มีความเร็วในการประมวลต่ำ โดยผลการทดสอบพบว่าสามารถช่วยลดเวลาในการคานวณได้ประมาณ 69 % เมื่อเทียบกับแบบที่ใช้ RSA

กานน ยิ่งวรรณะ, สุนีย์ แซ่ตัน (2550: บทคัดย่อ) ระบบการส่งข้อมูลผ่านเครือข่ายไร้สายอย่างปลอดภัย โครงงานนี้ได้ทำการศึกษาเกี่ยวกับระบบความปลอดภัยในการสื่อสารระหว่างระบบเครือข่ายไร้สายกับเครือข่ายอินเตอร์เน็ต และทำการเขียนโปรแกรมจำลองระบบเพื่อเป็นแนวทางในการเพิ่มความปลอดภัยให้แก่การสื่อสารในระบบนี้มากยิ่งขึ้น เนื่องจากในระบบดั่งเดิมยังมีข้อบกพร่องกล่าวคือ ในส่วนของ WPA Gateway จะมีข้อมูลที่ไม่ได้ถูกเข้ารหัสทำให้ผู้บุกรุกสามารถนำข้อมูลไปใช้ได้โดยไม่ได้รับอนุญาต ดังนั้นผู้จัดทำโครงงานจึงทำการเข้ารหัสข้อมูลก่อนที่จะมีการส่งข้อมูลจากเครือข่ายไร้สายไปยังเครือข่ายอินเทอร์เน็ตเพิ่มขึ้นจากระบบเดิม เพื่อทำให้ระบบการสื่อสารเป็นแบบ End-to-End โดยใช้ภาษา WML และ WMLScript ในการเขียนโปรแกรมเข้ารหัสข้อมูลก่อนที่จะส่งผ่านเครือข่ายไร้สาย และภาษา PHP ในการเขียนโปรแกรมเพื่อถอดรหัสข้อมูลที่เครือข่ายอินเทอร์เน็ต ซึ่งทำหน้าที่เสมือนเป็นเครื่องแม่ข่ายเว็บ จากการพัฒนาโปรแกรมดังกล่าวได้ทำการประเมินประสิทธิภาพของโปรแกรม 3 ด้าน คือ ด้านความถูกต้องของข้อมูล ด้านความเร็วในการเข้ารหัสข้อมูล และด้านความปลอดภัยในการรับ – ส่งข้อมูล

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 จึง

วิเคราะห์จุดอ่อนดังกล่าว และได้ออกแบบพร้อมพัฒนาโปรแกรม วิธีแก้ปัญหาใหม่ โดยอาศัยเทคโนโลยีเว็บเซอร์วิสและเจทูเอ็มอี เพื่อทำให้กระบวนการยืนยันตัวตนในเว็บแอปพลิเคชั่นดีขึ้น โดยใช้การยืนยันตัวตนด้วยปัจจัยสองลักษณะร่วมกับเทคนิคการท้าทายและตอบสนอง (challenge-respond) และ HOTP ทำให้แนวคิดในการแก้ปัญหาแบบใหม่ มีประสิทธิผลสูงกว่า มีต้นทุนที่ถูกกว่า และง่ายกว่าในการติดตั้งใช้งาน

พีระ พาทัน (2547) ได้วิจัยถึงการประเมินนโยบายการรักษาความปลอดภัยในจุดบริการระบบเครือข่ายไร้สาย ประเมินนโยบายความปลอดภัยและภัยคุกคามในจุดบริการของผู้ให้บริการอินเทอร์เน็ตไร้สาย(WISP) ที่เปิดให้บริการในเขตพื้นที่กรุงเทพฯ ซึ่งผลลัพธ์การสำรวจจุดบริการที่เปิดให้บริการอิสระจำนวน 454 APs พบว่า 23.12 % เปิดใช้งาน WEP (Wired Equivalent Privacy) เพื่อเข้ารหัสลับของข้อมูลผู้ใช้งานและมีการตั้งชื่อเครือข่าย (SSID) เป็นค่าดีฟอลต์ 29.51% และจากการสุ่มสารวจจุดบริการอินเทอร์เน็ตไร้สาย (Hotspot) จำนวน 12 แห่ง พบว่าไม่มีจุดบริการรายใดใช้งาน WEP เพื่อเข้ารหัสลับข้อมูลของลูกค้าทำให้ไม่มีจุดบริการที่ได้ทำการสำรวจผ่านเกณฑ์การประเมินที่ผู้วิจัยสร้างขึ้นมา และอาจส่งผลให้ข้อมูลลูกค้าที่ไม่ได้เข้ารหัสนั้นสามารถถูกดักจับได้ ดังนั้นในการใช้งานระบบเครือข่ายไร้สายผู้ใช้งานควรมีมาตรการรักษาความปลอดภัยของผู้ใช้งานเอง เช่น การใช้งานไฟร์วอลส่วนบุคคลหรือเลือกใช้งาน VPN ซึ่งผู้บริการอินเทอร์เน็ตไร้สายบางรายมีให้เป็นบริการเสริม เป็นต้น

สิรีวรรณ ตติยรัตน์ (2554) ได้ทำการวิจัยเพื่อทดสอบความปลอดภัยระบบเครือข่ายไร้สายมหาวิทยาลัยมหาสารคาม โดยเครือข่ายไร้สายมีการเข้ารหัสแบบ WEP (Wired Equivalent Privacy) เพื่อ เข้ารหัสลับของข้อมูลผู้ใช้งานและมีการตั้งชื่อเครือข่าย SSID (Service Set Identifier) เป็นค่าที่กำหนดขึ้นเอง WEP เป็นรูปแบบความปลอดภัยพื้นฐานที่ติดมากับมาตรฐาน 802.11 ขั้นตอนการดำเนินงาน ได้แก่ จำลองระบบเครือข่ายไร้สายเพื่อทำการทดสอบถึงภัยคุกคามที่อาจเกิดขึ้นบนเครือข่ายไร้สาย จัดตั้ง APs (Access Point) จานวน 1 เครื่อง โดยมีเครื่องลูกข่ายจำนวน 2 เครื่อง และเครื่องที่ใช้ดักจับแพ็กเก็ตข้อมูลและแกะรอยกุญแจที่เข้ารหัสแบบ WEP 64 บิต และ 128 บิต จำนวน 1 เครื่อง ผลการวิเคราะห์เปรียบเทียบจำนวนแพ็กเก็ตและเวลาที่ใช้ในการแกะรอยกุญแจ สรุปได้ว่าการเข้ารหัสแบบ WEP 128 บิต มีความปลอดภัยในการแกะรอยกุญแจมากกว่าการเข้ารหัสแบบ WEP 64 บิต เนื่องจากจำนวนแพ็กเก็ตที่ดักจับโดยการเข้ารหัสแบบ WEP 128 บิต ต้องใช้จำนวนแพ็กเก็ตมากกว่าการเข้ารหัสแบบ WEP 64 บิตถึง 2.17 เท่า แสดงให้เห็นถึงความสามารถในการรักษาความปลอดภัยบนเครือข่ายที่สูงกว่า ผลการสำรวจเครือข่ายไร้สายทั่วไปจานวน 77 APs พบว่า 58% เปิดใช้งาน WEP และการสำรวจจุดบริการอินเทอร์เน็ตไร้สายจำนวน 41 APs พบว่า 31.7 % เปิดใช้งาน WEP

บทที่ 3
การศึกษาระบบงานปัจจุบัน

ในการศึกษาระบบงานมีความมุ่งหมายเพื่อทำการประเมินระบบความปลอดภัยของระบบเครือข่ายไร้สายมหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร โดยการจัดทำเป็นการวิจัยและประเมินระบบความปลอดภัยของระบบเครือข่ายไร้สาย ซึ่งมีการค้นคว้าและหาข้อมูลที่เกี่ยวกับระบบงานโดยการสอบถามลักษณะงานที่ใช้งานในปัจจุบัน และปัญหาต่างๆ ที่เกิดขึ้น โดยมีขั้นตอนการวิจัยดังนี้

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

5) Access point ยี่ห้อ Alcatel รุ่น AP 104
D-Link รุ่น DAP-1360, D-Link รุ่น DWL-2100AP

3.1.1.2 ซอฟต์แวร์

1) ระบบปฏิบัติการ Kali Linux v. 1.0.8

3.2 การออกแบบระบบงาน

แผนผังการวางระบบงานเดิมที่ใช้งานในปัจจุบันของหน่วยงาน

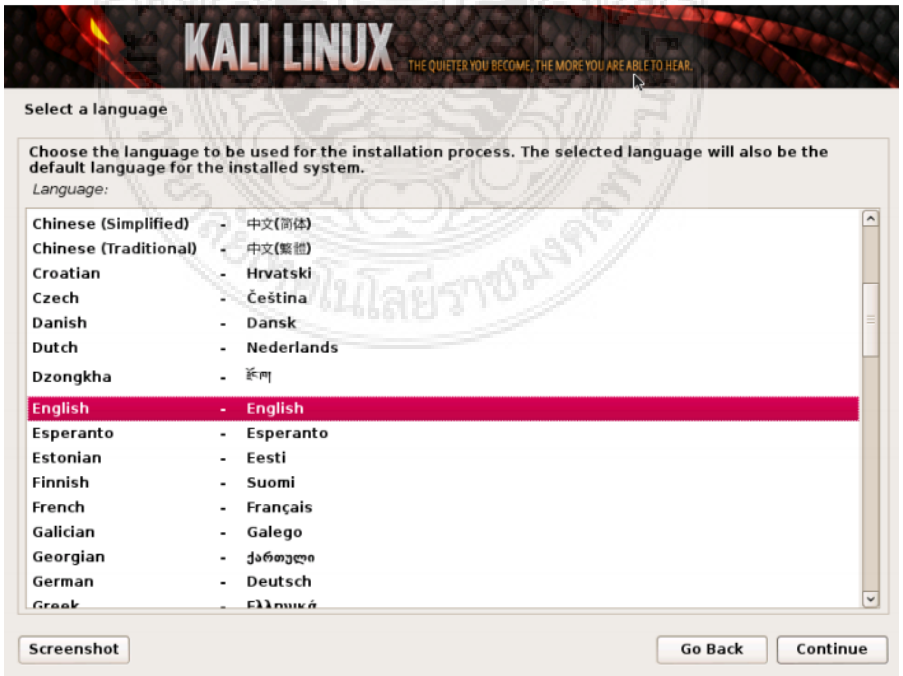
Access Point mode

ภาพที่ 3-1 แผนภาพระบบเครือข่ายไร้สายของหน่วยงาน

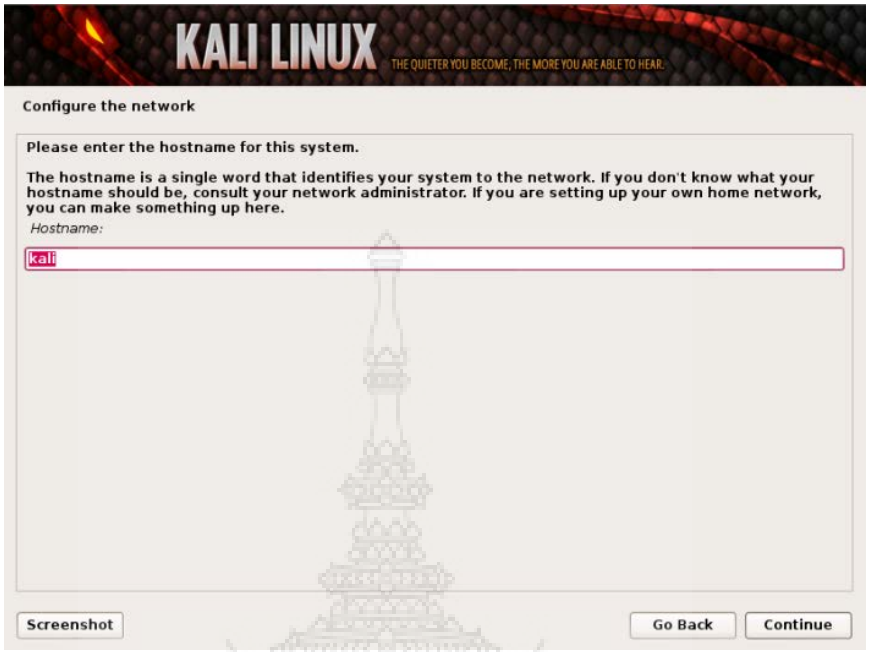
เมื่อรวบรวมข้อมูลเรียบร้อยแล้วก็นำข้อมูลมาจัดทำการประเมินระบบความปลอดภัยของระบบเครือข่ายไร้สาย

3.3 การติดตั้งระบบปฏิบัติการ Kali Linux v. 1.0.8

ภาพที่ 3-2 หน้าแรกของการติดตั้ง Kali Linux

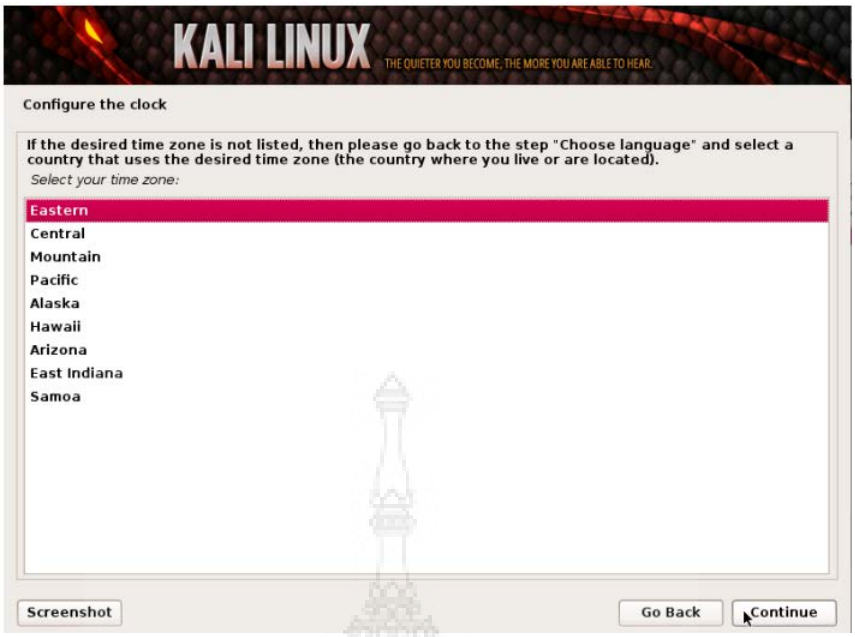


ภาพที่ 3-3 เลือกภาษา

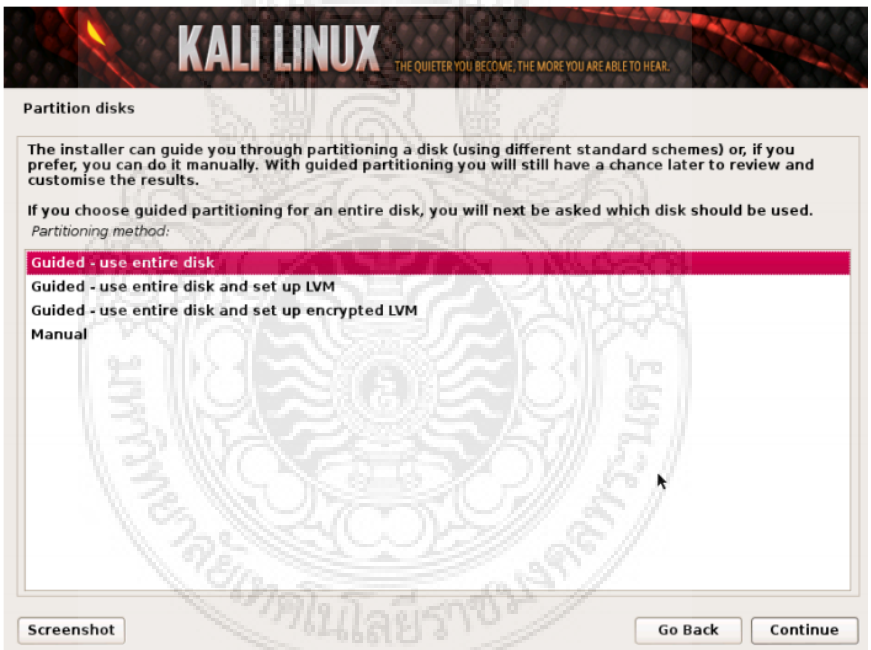


ภาพที่ 3-4 ตั้งชื่อ hostname

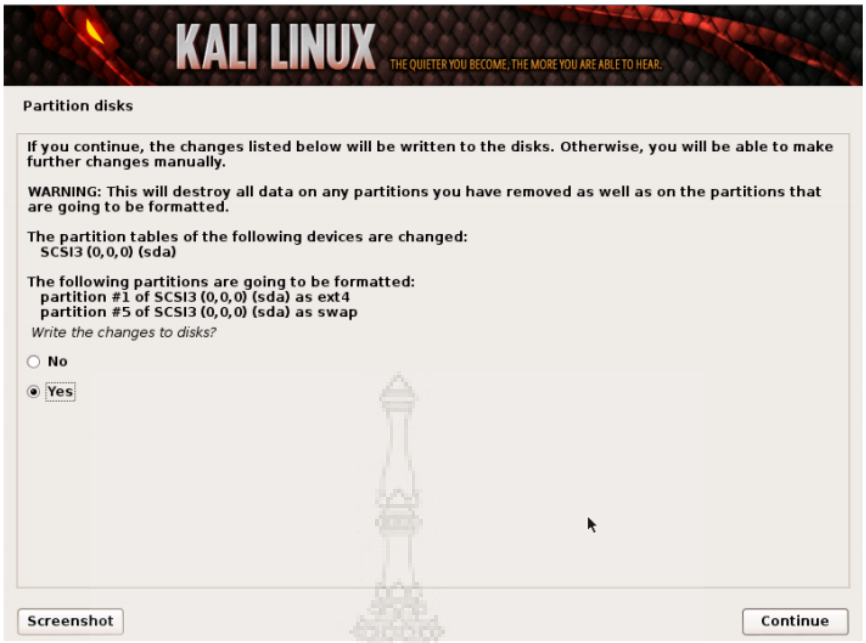
ภาพที่ 3-5 ตั้งรหัสผ่าน



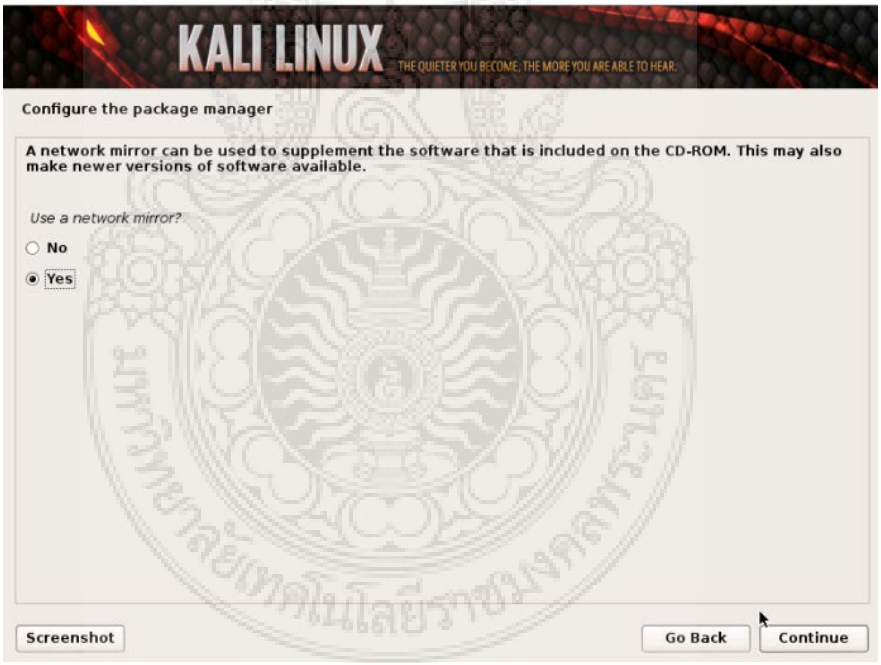
ภาพที่ 3-6 เลือก Time Zone



ภาพที่ 3-7 สร้าง Partition disks

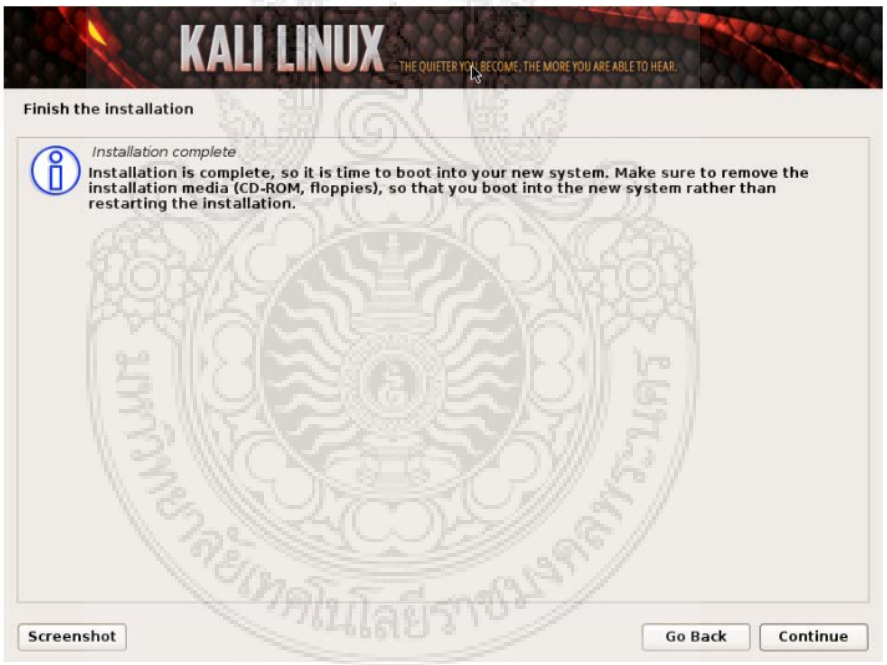


ภาพที่ 3-8 ทำการเขียน Partition disks

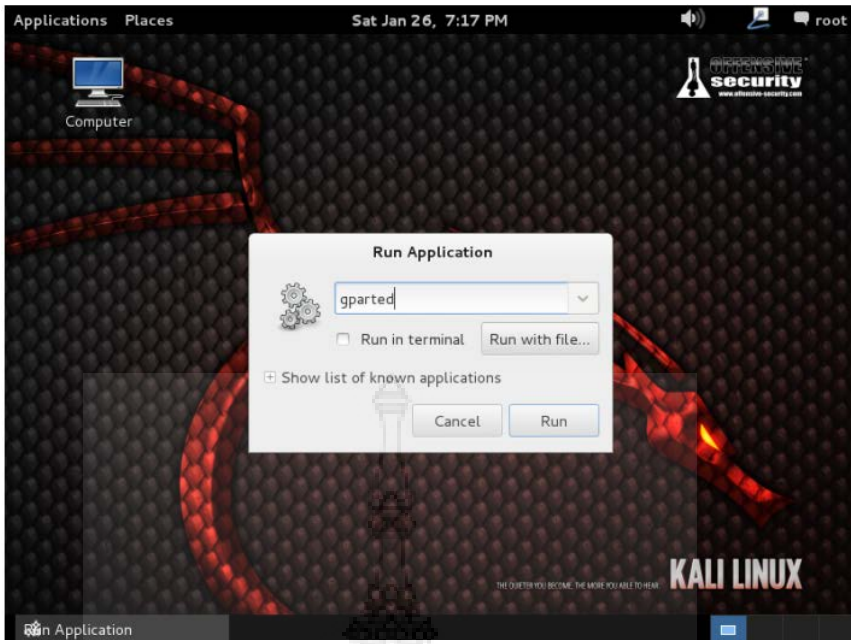


ภาพที่ 3-9 ติดตั้ง Package Manager

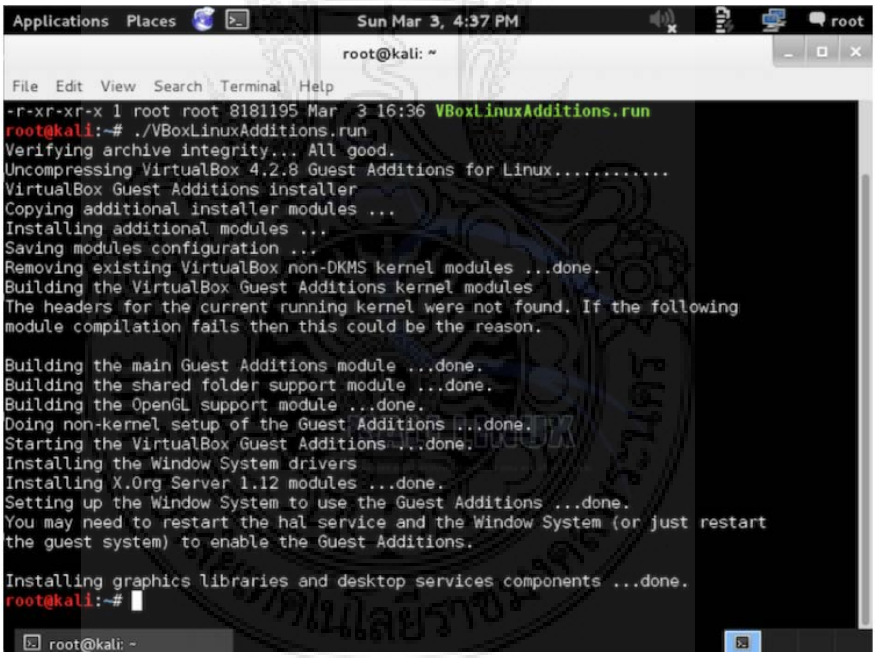
ภาพที่ 3-10 ติดตั้ง GRUB Boot loader



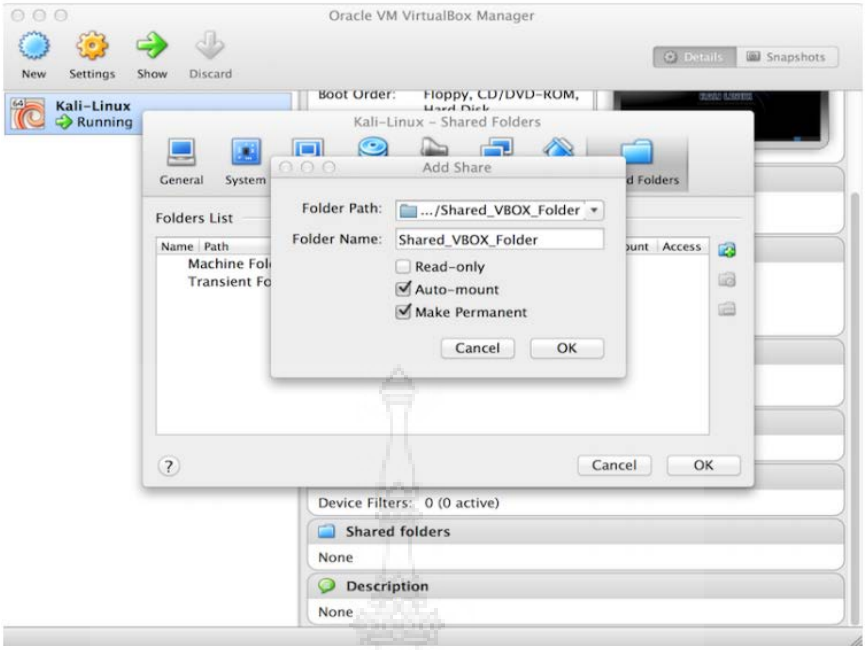
ภาพที่ 3-11 จบการติดตั้ง



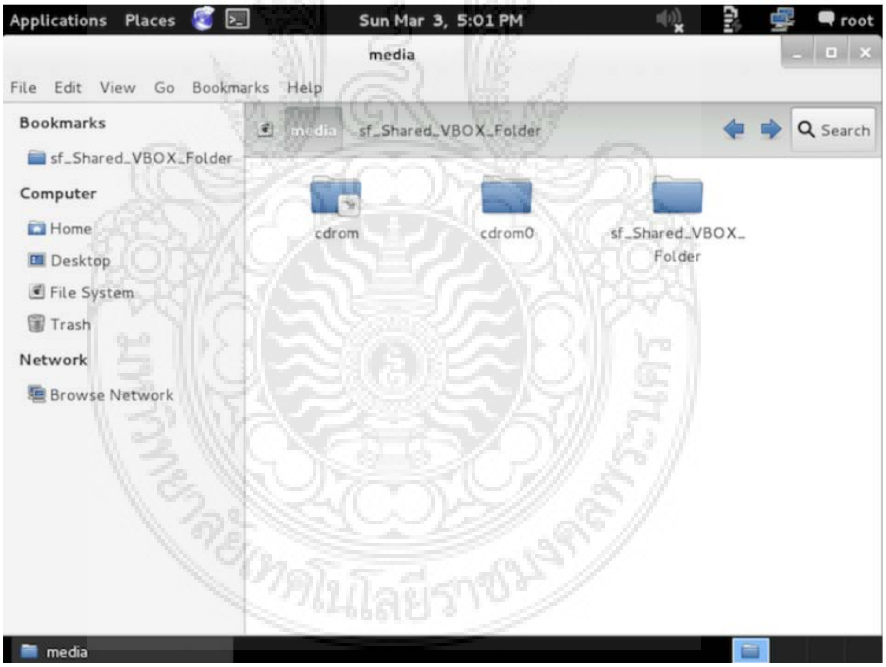
ภาพที่ 3-12 หน้า Login



ภาพที่ 3-13 หน้า Comand



ภาพที่ 3-14 หน้า GUI



ภาพที่ 3-15 หน้า GUI media

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

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

เมื่อทำการคำนวณหาความกว่างของช่วงระดับคะแนน 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
การประเมินระบบความปลอดภัยของระบบเครือข่ายไร้สาย

4.1 การติดตั้งโปรแกรม Kali Linux ในเครื่องคอมพิวเตอร์ Note Book

ซึ่งมีโปรแกรมต่างๆ ดังนี้

- airmon-ng
- aireplay-ng
- airodump-ng
- aircrack-ng

เมื่อติดตั้งโปรแกรม Kali Linux เสร็จเรียบร้อยก็จะสามารถเรียกใช้ Module หรือโปรแกรมต่างๆ ได้ และสามารถทำการประเมินระบบความปลอดภัยของระบบเครือข่ายไร้สายภายในมหาวิทยาลัยฯ โดยใช้ความสามารถของโปรแกรมดังกล่าว

4.2 ประเมินระบบความปลอดภัยของระบบเครือข่ายไร้สายที่เปิดให้บริการ

เมื่อติดตั้งโปรแกรมเสร็จเรียบร้อยแล้วก็นำเครื่องคอมพิวเตอร์ Note Book มาทดสอบรับสัญญาณจาก Access Point ซึ่งผู้ทดลองได้แบ่งการทดลองออกเป็น 2 ระบบ คือ

1. Access Point ที่ผู้วิจัยได้ติดตั้งขึ้นเอง โดยเชื่อมต่อกับระบบเครือข่ายคอมพิวเตอร์ของมหาวิทยาลัย
2. Access Point ที่เปิดให้บริการของมหาวิทยาลัยฯ ซึ่งเป็นระบบเครือข่ายไร้สายที่มีการบริหารจัดการจากศูนย์กลางจากทางมหาวิทยาลัย

ซึ่งแบ่งเป็นการทดสอบดังนี้

1. เข้ารหัสแบบ wep ชนิด open system 64 bit
   - 1.1 password จะใช้อย่างน้อย 10 ตัว " abcdef1234 " ใช้ data 5000 ivs ถอดรหัสได้
   - 1.2 password จะใช้อย่างน้อย 10 ตัว " 1234abcdef " ใช้ data 5000 ivs ถอดรหัสได้
   - 1.3 password จะใช้อย่างน้อย 10 ตัว " abcdefabcd " ใช้ data 5000 ivs ถอดรหัสได้
   - 1.4 password จะใช้อย่างน้อย 10 ตัว " abababababab " ใช้ data 5000 ivs ถอดรหัสได้
   - 1.5 password จะใช้อย่างน้อย 10 ตัว " abcdefedcb " ใช้ data 5000 ivs ถอดรหัสได้
   - 1.6 password จะใช้อย่างน้อย 10 ตัว " feedbeebee " ใช้ data 5000 ivs ถอดรหัสได้
   - 1.7 password จะใช้อย่างน้อย 10 ตัว " 1234567890 " ใช้ data 5000 ivs ถอดรหัสได้
   - 1.8 password จะใช้อย่างน้อย 10 ตัว " 1234554321 " ใช้ data 5000 ivs ถอดรหัสได้
   - 1.9 password จะใช้อย่างน้อย 10 ตัว " fedcba9876 " ใช้ data 5000 ivs ถอดรหัสได้
   - 1.10 password จะใช้อย่างน้อย 10 ตัว " abcdef4321 " ใช้ data 5000 ivs ถอดรหัสได้

   ซึ่งสามารถถอดรหัสผ่านได้ทุกข้อ และใช้ data เพียง 5000 ivs

2. เข้ารหัสแบบ wep ชนิด open system 128 bit
   - 2.1 password จะใช้อย่างน้อย 26 ตัว ใช้ data 10000 ivs ถอดรหัสได้

"abcdef1234abcdef1234abcdef"

2.2 password จะใช้อย่างน้อย 26 ตัว ใช้ data 10000 ivs ถอดรหัสได้ "abcdef12345678901234abcdef"

2.3 password จะใช้อย่างน้อย 26 ตัว ใช้ data 10000 ivs ถอดรหัสได้ "abcdefabcdabcdef1234abcdef"

2.4 password จะใช้อย่างน้อย 26 ตัว ใช้ data 10000 ivs ถอดรหัสได้ "abcdefedcbabcdef1234abcdef"

2.5 password จะใช้อย่างน้อย 26 ตัว ใช้ data 10000 ivs ถอดรหัสได้ "1234561234abcdef1234abcdef"

2.6 password จะใช้อย่างน้อย 26 ตัว ใช้ data 10000 ivs ถอดรหัสได้ "aaaaaa1234abcdef1234abcdef"

2.7 password จะใช้อย่างน้อย 26 ตัว ใช้ data 10000 ivs ถอดรหัสได้ "beebee1234abcdef1234abcdef"

2.8 password จะใช้อย่างน้อย 26 ตัว ใช้ data 10000 ivs ถอดรหัสได้ "feedab1234abcdef1234abcdef"

2.9 password จะใช้อย่างน้อย 26 ตัว ใช้ data 10000 ivs ถอดรหัสได้ "abcdefbedaabcdef1234abcdef"

2.10 password จะใช้อย่างน้อย 26 ตัว ใช้ data 10000 ivs ถอดรหัสได้ "abcdef12341234561234abcdef"

ซึ่งสามารถถอดรหัสผ่านได้ทุกข้อ และใช้ data เพียง 10000 ivs

3. เข้ารหัสแบบ wpa-psk

3.1 password จะใช้อย่างน้อย 8-63 ตัว ใช้ data 10000 ivs ถอดรหัสได้ "abcdef12"

3.2 password จะใช้อย่างน้อย 8-63 ตัว ใช้ data 10000 ivs ถอดรหัสได้ "12345612"

3.3 password จะใช้อย่างน้อย 8-63 ตัว ใช้ data 10000 ivs ถอดรหัสได้ "abababab12"

3.4 password จะใช้อย่างน้อย 8-63 ตัว ใช้ data 10000 ivs ถอดรหัสได้ "beebee12"

3.5 password จะใช้อย่างน้อย 8-63 ตัว ใช้ data 10000 ivs ถอดรหัสได้ "abcd1234"

3.6 password จะใช้อย่างน้อย 8-63 ตัว ใช้ data 10000 ivs ถอดรหัสได้ "12345678"

3.7 password จะใช้อย่างน้อย 8-63 ตัว ใช้ data 10000 ivs ถอดรหัสได้ "87654321"

3.8 password จะใช้อย่างน้อย 8-63 ตัว ใช้ data 10000 ivs ถอดรหัสได้ "aaaaaaaa"

3.9 password จะใช้อย่างน้อย 8-63 ตัว ใช้ data 10000 ivs ถอดรหัสได้ "feedfeed"

3.10 password จะใช้อย่างน้อย 8-63 ตัว ใช้ data 10000 ivs ถอดรหัสได้ "abcdef98"

ซึ่งสามารถถอดรหัสผ่านได้ทุกข้อ และใช้ data เพียง 10000 ivs แต่ถ้าใช้รหัสที่มีตัวอักษรมากกว่า 8 ตัว การถอดรหัสจะใช้ data เยอะขึ้น และบางครั้งก้ไม่สามารถถอดรหัสได้

4. เข้ารหัสแบบ wpa2-psk

4.1 password จะใช้อย่างน้อย 8-63 ตัว ใช้ data 10000 ivs ถอดรหัสได้ "abcdef12345"

4.2 password จะใช้อย่างน้อย 8-63 ตัว ใช้ data 10000 ivs ถอดรหัสได้ "abcdefabcde"

4.3 password จะใช้อย่างน้อย 8-63 ตัว ใช้ data 10000 ivs ถอดรหัสได้ "abcdeffeeda"

4.4 password จะใช้อย่างน้อย 8-63 ตัว ใช้ data 10000 ivs ถอดรหัสได้ "abcdef54321"

4.5 password จะใช้อย่างน้อย 8-63 ตัว ใช้ data 10000 ivs ถอดรหัสได้ "abcdef55455"

4.6 password จะใช้อย่างน้อย 8-63 ตัว ใช้ data 10000 ivs ถอดรหัสได้ "abcdef12321"

4.7 password จะใช้อย่างน้อย 8-63 ตัว ใช้ data 10000 ivs ถอดรหัสได้ "abcbee12345"

4.8 password จะใช้อย่างน้อย 8-63 ตัว ใช้ data 10000 ivs ถอดรหัสได้ "ab123412345"

4.9 password จะใช้อย่างน้อย 8-63 ตัว ใช้ data 10000 ivs ถอดรหัสได้ "a1234512345"

4.10 password จะใช้อย่างน้อย 8-63 ตัว ใช้ data 10000 ivs ถอดรหัสได้ "abfeedf12345"

ซึ่งสามารถถอดรหัสผ่านได้ทุกข้อ และใช้ data เพียง 10000 ivs แต่ถ้าใช้รหัสที่มีตัวอักษรมากกว่า 8 ตัว การถอดรหัสจะใช้ data เยอะขึ้น และบางครั้งก้ไม่สามารถถอดรหัสได้

5. เข้ารหัสแบบ wpa-auto-psk

5.1 pass word จะใช้อย่างน้อย 8-63 ตัว ใช้ data 10000 ivs ถอดรหัสได้ "abcdef12"

5.2 pass word จะใช้อย่างน้อย 8-63 ตัว ใช้ data 10000 ivs ถอดรหัสได้ "12345612"

5.3 pass word จะใช้อย่างน้อย 8-63 ตัว ใช้ data 10000 ivs ถอดรหัสได้ "12345678"

5.4 pass word จะใช้อย่างน้อย 8-63 ตัว ใช้ data 10000 ivs ถอดรหัสได้ "87654321"

5.5 pass word จะใช้อย่างน้อย 8-63 ตัว ใช้ data 10000 ivs ถอดรหัสได้ "abcbee12"

5.6 pass word จะใช้อย่างน้อย 8-63 ตัว ใช้ data 10000 ivs ถอดรหัสได้ "abababab12"

5.7 pass word จะใช้อย่างน้อย 8-63 ตัว ใช้ data 10000 ivs ถอดรหัสได้ "abcdefee"

5.8 pass word จะใช้อย่างน้อย 8-63 ตัว ใช้ data 10000 ivs ถอดรหัสได้ "abcabc12"

5.9 pass word จะใช้อย่างน้อย 8-63 ตัว ใช้ data 10000 ivs ถอดรหัสได้ "abcdabcd"

5.10 pass word จะใช้อย่างน้อย 8-63 ตัว ใช้ data 10000 ivs ถอดรหัสได้ "abcdefaa"

ซึ่งสามารถถอดรหัสผ่านได้ทุกข้อ และใช้ data เพียง 10000 ivs แต่ถ้าใช้รหัสที่มีตัวอักษรมากกว่า 8 ตัว การถอดรหัสจะใช้ data เยอะขึ้น และบางครั้งก้ไม่สามารถถอดรหัสได้

บทที่ 5
ผลการศึกษา สรุป และข้อเสนอแนะ

การประเมินระบบความปลอดภัยของระบบเครือข่ายไร้สายมหาวิทยาลัยเทคโนโลยีราช-มงคลพระนคร เป็นการตรวจสอบจำนวนรหัสผ่านที่ใช้ ซึ่งพิจารณาจากจำนวนของตัวอักษรที่ใช้ในการตั้งเป็นรหัสผ่านสำหรับใช้ในการ Connect กับตัว Access Point ที่เปิดให้บริการ จะสังเกตุได้ว่าถ้าใช้จำนวนอักษรตามจำนวนขั้นต่ำที่ได้กำหนดไว้ ก็จะสามารถถูกถอดรหัสผ่านได้ค่อนข้างง่าย และใช้เวลาเพียงไม่กี่นาทีก็จะสามารถถอดรหัสได้ ถ้าหากผู้ใช้ตั้งรหัสผ่านตรงกับคำใน Dictionary ก็ยิ่งทำให้ถอดรหัสได้ง่ายและเร็วยิ่งขึ้น

การวิจัยและการประเมินระบบความปลอดภัย ของระบบเครือข่ายไร้สายมหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร ที่ติดตั้ง Access Point โดยไม่มีระบบบริหารการจัดการจากระบบศูนย์กลาง ซึ่งเป็น Access Point จะถูกถอดรหัสผ่านได้โดยง่าย ทำให้เกิดความเสี่ยงต่อระบบความปลอดภัยเป็นอย่างยิ่ง ปัจจุบันทางมหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร ได้ยกเลิกระบบ Access Point ธรรมดาทั่วๆ ไปออกทั้งหมด และใช้เป็นระบบ Access Point ที่มีระบบบริหารการจัดการจากระบบศูนย์กลาง จึงสามารถดูแลควบคุมได้ง่าย อีกทั้งมหาวิทยาลัยฯ ยังมีระบบ Authentication จึงทำให้มีความปลอดภัยยิ่งขึ้น ซึ่งระบบการบริหารการจัดการแบบมีศูนย์กลางควบคุมเป็นนิยมใช้งานกันอย่างแพร่หลาย เพราะมีความปลอดภัยสูง

5.1 ผลการศึกษา

การประเมินระบบความปลอดภัยของระบบเครือข่ายไร้สายมหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร ผู้จัดทำระบบได้ทำการประเมินผลการถอดรหัสผ่านจาก Access Piont เพื่อเข้าใช้บริการจาก Access Point แต่ละตัว จะสังเกตุได้ว่า Access Point ที่ใช้การเข้ารหัสเป็นแบบ WEP จะถูกถอดรหัสได้ง่ายกว่าเข้ารหัสแบบ WPA หากใช้วิธีการเข้ารหัสแบบ WPA การถอดรหัสผ่านก็จะต้องใช้เวลานานขึ้น จึงทำให้การถอดรหัสผ่านใช้เวลานานขึ้นตามไปด้วย ซึ่งปัจจุบันการเข้ารหัสแบบ WPA มีการพัฒนาเป็น WPA2, wpa-auto-psk เป็นต้น จะสังเกตุได้ว่าถ้าหากมีการตั้งรหัสผ่านที่มีจำนวนตัวอักษรน้อยกว่า 8 ตัวอักษร ระบบโปรแกรม Kali Linux สามารถถอดรหัสได้อย่างรวดเร็ว จึงทำให้สามารถเข้าถึงระบบเครือข่ายได้โดยง่าย

ตารางที่ 5-1 ผลการวิเคราะห์ข้อมูลจากการประเมินระบบความปลอดภัยของระบบเครือข่ายไร้สาย

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

5	ความสมบูรณ์ของรายงานสรุปผล	3.70	ดี
6	การแก้ไขปรับปรุงทำได้ง่ายและสะดวก	3.67	ดี
7	การค้นหาข้อมูลทำได้ง่ายและสะดวก	3.68	ดี
8	การทำงานสะดวกมากขึ้นในการเรียกดูข้อมูล	3.40	ดี
9	คู่มือการใช้มีความชัดเจน และสะดวกต่อการใช้งาน	3.67	ดี
10	สามารถนำไปใช้กับระบบงานได้จริง	4.28	ดีมาก
ค่าเฉลี่ยคะแนนต่อการใช้โปรแกรม		**3.66**	**ดี**

การแปลผลการวิเคราะห์ข้อมูล

จากการประเมินระบบความปลอดภัยของระบบเครือข่ายไร้สาย ที่ไปทดสอบกับอุปกรณ์ Access Point ภายในมหาวิทยาลัย พบว่า โปรแกรมที่ใช้ในการประเมินระบบความปลอดภัยมีการใช้งานของระบบในภาพรวมอยู่ในระดับดี โดยสามารถนำไปใช้กับระบบงานได้จริง มีความคิดเห็นอยู่ในระดับดีมาก ส่วนความสะดวกต่อการใช้งาน ความยากง่ายในการติดตั้งโปรแกรมระบบปฏิบัติการ ความยากง่ายในการ Config ระบบ ความถูกต้องของโปรแกรม ความสมบูรณ์ของรายงานสรุปผล การแก้ไขปรับปรุงทำได้ง่ายและสะดวก การค้นหาข้อมูลทำได้ง่ายและสะดวก การทำงานสะดวกมากขึ้นในการเรียกดูข้อมูล และคู่มือการใช้มีความชัดเจน และสะดวกต่อการใช้งาน มีความคิดเห็นอยู่ในระดับดี

5.2 ปัญหาและอุปสรรคที่พบ

เนื่องจากการประเมินระบบความปลอดภัยของระบบเครือข่ายไร้สายเป็นการ เป็นการประเมินแบบสุ่ม ดังนั้นปัญหาที่ผู้วิจัยได้พบในการวิจัยดังกล่าว มีดังนี้

5.2.1 ปัญหาในด้านระบบงาน ไม่สามารถติดตั้งระบบงาน เพื่อให้บุคลากรได้ทำการทดลองใช้งานได้อย่างต่อเนื่อง ตลอดเวลา ทำให้ผู้ใช้งานเกิดความไม่สนใจที่จะใช้ระบบงานใหม่

5.2.2 ปัญหาที่เกิดขึ้นจากข้อจำกัดของระบบงาน ทำให้การทำงานของระบบยังไม่ครอบคลุมระบบงานมากนัก

5.2.3 ปัญหาที่เกิดขึ้นจากบุคลากรของหน่วยงาน มีความรู้พื้นฐานทางด้านการติดตั้งระบบเครือข่ายไร้สาย

5.3 ข้อเสนอแนะ

ควรตั้งรหัสผ่านที่มีจำนวนตัวอักษร ผสมตัวเลข มีจำนวนไม่น้อยกว่า 8 ตัวอักษร และเลือกการเข้ารหัสผ่านเป็นแบบ wpa-auto-psk ซึ่งจะทำให้มีความปลอดภัยสูง ดีกว่าการเข้ารหัสแบบ WEP

เอกสารอ้างอิง

[1] จรวย สาวิถี. การสื่อสารข้อมูลและเครือข่ายคอมพิวเตอร์ในงานธุรกิจ. พิมพ์ครั้งที่ 1. กาฬสินธุ์: โรงพิมพ์ประสานการพิมพ์, 2551.

[2] ฑิชาพร โนนสินชัย, มุธิตา นาสมชัย เปรียบเทียบระบบรักษาความปลอดภัยบน Wi-Fi ด้วย WPA และ WPA2 มหาวิทยาลัยมหาสารคาม ปี การศึกษา 2553

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

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

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

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

[7] วิบูลย์ วราสิทธิชัย, http://mamboeasy.psu.ac.th/~wiboon.w/index2.php?Option8com_content&task=view&

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

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

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

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

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

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

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

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

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