การปิดจุดอ่อนและป้องกันภัยให้แลนไร้สาย
Vulnerability Management and Security in Wireless LAN

บุญจรีย์ เจษฎาปกรณ์*

บทคัดย่อ

แลนไร้สายหรือวายฟายเป็นระบบเครือข่ายที่กำลังได้รับความนิยมเพิ่มมากขึ้นเรื่อยๆ เนื่องจากความสะดวกในการใช้งานและสามารถเชื่อมต่อได้ทุกที่ที่ให้บริการแต่ปัญหาหนึ่งของการใช้แลนไร้สายคือปัญหาเรื่องความปลอดภัยในเครือข่ายเนื่องจากเราไม่สามารถกำหนดทิศทางและขอบเขตของคลื่นวิทยุที่ใช้ในระบบแลนไร้สายได้ทำให้อาจมีผู้บุกรุกเข้ามาใช้งานหรือดักจับข้อมูลที่ส่งผ่านเครือข่ายการบริหารจัดการและกำหนดค่าระบบแลนไร้สายอย่างถูกต้องและเหมาะสมจะช่วยลดความเสี่ยงจากภัยเหล่านี้ได้

Abstract

Wireless LAN or Wi-Fi is a network that is gaining more popularity due to the ease of use and the ability to connect anywhere this network is available. One problem of using wireless LAN is the security in network. Since we can not determine the direction and extent of the radio waves used in wireless LAN, the intruder may access it or eavesdrop the data sent through the network. Wireless LAN management and configuration which are correct and suitable can reduce the risk of these threats.

* *อาจารย์ประจำคณะบัญชี ธุรกิจ และมัลติมีเดีย มหาวิทยาลัยคริสเตียน

บทนำ

แลนไร้สาย (Wireless LAN) หรือเรียกอีกอย่างหนึ่งว่า วายฟาย (Wi-Fi : Wireless Fidelity) คือระบบสื่อสารข้อมูลที่เชื่อมโยงคอมพิวเตอร์เข้าด้วยกันเป็นเครือข่ายแบบไร้สาย โดยใช้คลื่นความถี่วิทยุหรือคลื่นแม่เหล็กไฟฟ้า การเชื่อมต่อในเครือข่ายเพื่อใช้งานอินเทอร์เน็ตมักจะเป็นการเชื่อมต่อกับอุปกรณ์ที่เรียกว่า “แอคเซสพอยต์” (Access point) แลนไร้สายในปัจจุบันจะอยู่ภายใต้มาตรฐาน IEEE 802.11 ซึ่งกำหนดโดยสถาบันวิชาชีพวิศวกรไฟฟ้าและอิเล็กทรอนิกส์ (Institute of Electrical and Electronics Engineers : IEEE) ประเทศสหรัฐอเมริกา ปัจจุบันแลนไร้สายเป็นระบบเครือข่ายที่ได้รับความนิยมเพิ่มมากขึ้นเนื่องจากจุดเด่นในเรื่องความสะดวกในการใช้งานและสามารถเชื่อมต่อกับเครือข่ายได้ทุกที่ที่ให้บริการโดยไม่ต้องใช้สายแลน นอกจากนี้ความนิยมในการใช้อุปกรณ์พกพาแบบไร้สาย เช่น คอมพิวเตอร์โน้ตบุ้ค แท็บเล็ต และสมาร์ทโฟน ก็เป็นอีกปัจจัยที่ทำให้หลายคนหันมาใช้แลนไร้สาย แม้จะสะดวกในการใช้งานแต่เมื่อเทียบกับแลนแบบมีสายแล้วแลนไร้สายก็ยังมีข้อเสียหลายอย่าง เช่น มีคลื่นรบกวน มีการลดทอนของสัญญาณซึ่งสิ่งเหล่านี้ทำให้แลนไร้สายมีความเสถียรและความเร็วในการเชื่อมต่อน้อยกว่าแลนแบบมีสายนอกจากนี้แลนไร้สายก็ยังมีจุดอ่อนในเรื่องของความปลอดภัยอีกด้วย

อุปกรณ์ในระบบแลนไร้สาย

อุปกรณ์ที่สำคัญในระบบแลนไร้สายมีดังต่อไปนี้

1. แอคเซสพอยต์ (Access point)

แอคเซสพอยต์ดังรูปที่ 1 เป็นอุปกรณ์ที่ทำหน้าที่กระจายสัญญาณไร้สายเพื่อให้เครื่องคอมพิวเตอร์หรืออุปกรณ์ไร้สายอื่นๆ สามารถเชื่อมต่อเข้ากับเครือข่ายได้และยังทำหน้าที่เป็นศูนย์กลางในการรับส่งข้อมูลและเชื่อมต่อเข้ากับระบบแลนแบบมีสายอีกด้วย จากลักษณะการทำงานเช่นนี้จึงมีการเปรียบเทียบแอคเซสพอยต์ว่าเหมือนกับอุปกรณ์ “ฮับ” (Hub) ในระบบแลนแบบมีสาย

รูปที่ 1 : แอคเซสพอยต์

ที่มา : http://www.amazon.com/Cisco-WAP4410N-Wireless-N-Access-Point/dp/B001IYCMNA

2. การ์ดแลนไร้สาย (Wireless LAN card)

การ์ดแลนไร้สายเป็นอุปกรณ์ที่ทำหน้าที่ในการแปลงข้อมูลดิจิทัลที่ได้จากเครื่องคอมพิวเตอร์ให้เป็นคลื่นวิทยุแล้วส่งผ่านเสาอากาศให้กระจายออกไปและทำหน้าที่ในการรับข้อมูลที่อยู่ในรูปแบบของคลื่นวิทยุมาแปลงเป็นข้อมูลดิจิทัลแล้วส่งให้เครื่องคอมพิวเตอร์หรืออุปกรณ์ที่ต้องการใช้งานแลนไร้สายจะต้องมีการ์ดแลนไร้สายอยู่ในเครื่อง การ์ดแลนไร้สายที่ผลิตออกมาจำหน่ายนั้นสามารถแบ่งได้หลายรูปแบบตามลักษณะของช่องที่เชื่อมต่อกับคอมพิวเตอร์ เช่น แบบ PCI แบบ PCMCIA และแบบ USB ดังรูปที่ 2

รูปที่ 2 : การ์ดแลนไร้สาย

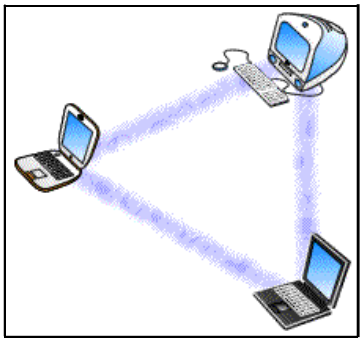
ที่มา : http://www.itvoe.com/blog/Laptop-Internal-wireless-Wifi-card-failure-and-fix

รูปแบบการเชื่อมต่อในระบบแลนไร้สาย

รูปแบบการเชื่อมต่อในระบบแลนไร้สาย (Wireless LAN Topology) แบ่งออกเป็น 2 ประเภทหลักๆ ดังนี้

1. Ad-Hoc หรือ Peer-to-Peer Ad-Hoc

เป็นรูปแบบการเชื่อมต่อโดยตรงระหว่างเครื่องคอมพิวเตอร์หรืออุปกรณ์ไร้สายโดยไม่มีอุปกรณ์ที่ทำหน้าที่เป็นศูนย์กลางในกลางรับส่งข้อมูลและไม่ได้เชื่อมต่อกับระบบแลนแบบมีสาย ดังรูปที่ 3 จึงไม่สามารถใช้งานอินเทอร์เน็ตได้หากไม่มีการตั้งค่าเพิ่มเติมแต่การเชื่อมต่อแบบนี้ทำให้คอมพิวเตอร์ในเครือข่ายสามารถแชร์ไฟล์หรือแชร์พริ้นเตอร์ร่วมกันได้อย่างรวดเร็ว และเป็นรูปแบบที่ติดตั้งได้ง่ายและสะดวก

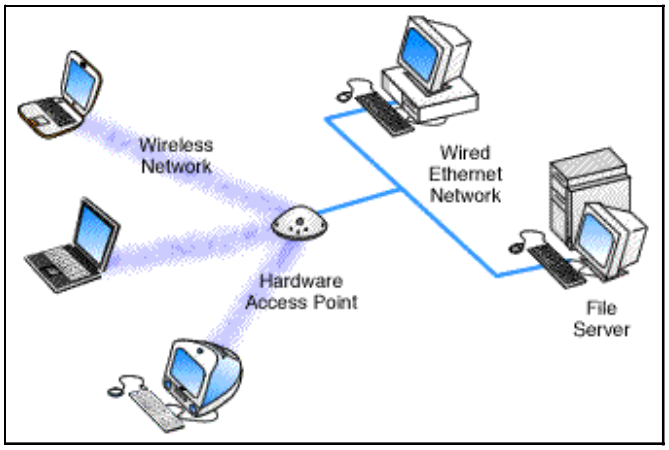


รูปที่ 3 : รูปแบบการเชื่อมต่อแลนไร้สายแบบ Ad-Hoc

ที่มา : http://www.vicomsoft.com/images/learning-center/wireless-networking

2. Infrastructure หรือ Client-Server Infrastructure

เป็นรูปแบบการเชื่อมต่อโดยมีแอคเซสพอยต์เป็นศูนย์กลางในการรับส่งข้อมูล และแอคเซสพอยต์นี้ยังเชื่อมต่อกับระบบแลนแบบมีสาย ดังรูปที่ 4 ทำให้สามารถใช้งานอินเทอร์เน็ตได้ การกำหนดค่าต่างๆของเครือข่ายมักทำที่แอคเซสพอยต์การเชื่อมต่อรูปแบบนี้เป็นที่นิยมมากที่สุดในปัจจุบัน



รูปที่ 4 : รูปแบบการเชื่อมต่อแลนไร้สายแบบ Infrastructure
ที่มา : http://www.vicomsoft.com/images/learning-center/wireless-networking

จุดอ่อนของระบบแลนไร้สาย

แลนไร้สายที่นำมาใช้งานในปัจจุบันจะอิงตามมาตรฐาน IEEE 802.11 ซึ่งกำหนดให้ใช้คลื่นวิทยุเป็นตัวกลางในการรับส่งข้อมูลโดยช่วงความถี่ของคลื่นวิทยุที่นำมาใช้งานสำหรับแลนไร้สายคือ 2.4 กิกกะเฮิรตซ์ และ 5 กิกกะเฮิรตซ์ เนื่องจากคลื่นวิทยุมีคุณสมบัติในการแพร่กระจายทุกทิศทางจากจุดกำเนิดและสามารถเดินทางผ่านวัตถุได้ ดังนั้นผู้ที่อยู่ในบริเวณรัศมีที่มีสัญญาณจากแอคเซสพอยต์ก็สามารถเชื่อมต่อกับเครือข่ายได้ไม่จำเป็นต้องนำคอมพิวเตอร์มาตั้งให้อยู่ตรงกันกับแอคเซสพอยต์ และไม่ถูกจำกัดพื้นที่การใช้งานเหมือนแลนแบบมีสายที่จะใช้งานได้เมื่อสถานที่นั้นมีพอร์ตแลนให้เสียบสาย นอกจากนี้แม้ผู้ใช้งานอยู่ในห้องและแอคเซสพอยต์อยู่ข้างนอกโดยที่ไม่ไกลกันมากก็ยังคงเชื่อมต่อกับแลนไร้สายได้เพราะคลื่นวิทยุสามารถทะลุผ่านเข้ามาในห้องได้

แต่การใช้คลื่นวิทยุเป็นตัวกลางในการรับส่งก็มีข้อเสียเช่นกัน เพราะยากที่เราจะกำหนดทิศทางและขอบเขตของคลื่นวิทยุดังนั้นสัญญาณจากแอคเซสพอยต์อาจจะครอบคลุมไปถึงอาคารใกล้เคียง หากมีผู้ที่ต้องการโจมตีระบบเข้ามาอยู่ในบริเวณนั้นก็สามารถเชื่อมต่อกับแลนไร้สายหรือดักจับข้อมูลที่ส่งผ่านเครือข่ายได้อีกทั้งการตามหาผู้โจมตีก็ทำได้ยาก เพราะไม่รู้ว่าอยู่ตำแหน่งใด

แนวทางการปิดจุดอ่อนและป้องกันภัยให้แลนไร้สาย

การบริหารจัดการและกำหนดค่าระบบแลนไร้สายอย่างถูกต้องและเหมาะสมจะช่วยปิดจุดอ่อนและป้องกันภัยให้แลนไร้สายได้วิธีพื้นฐานที่ควรทำมีดังต่อไปนี้

1. เปลี่ยนค่าดีฟอลต์ของแอคเซสพอยต์

แอคเซสพอยต์ที่เพิ่งซื้อมาใช้งานจะมีการกำหนดค่าที่ตัวอุปกรณ์มาให้แล้วซึ่งเป็นค่าเริ่มต้น

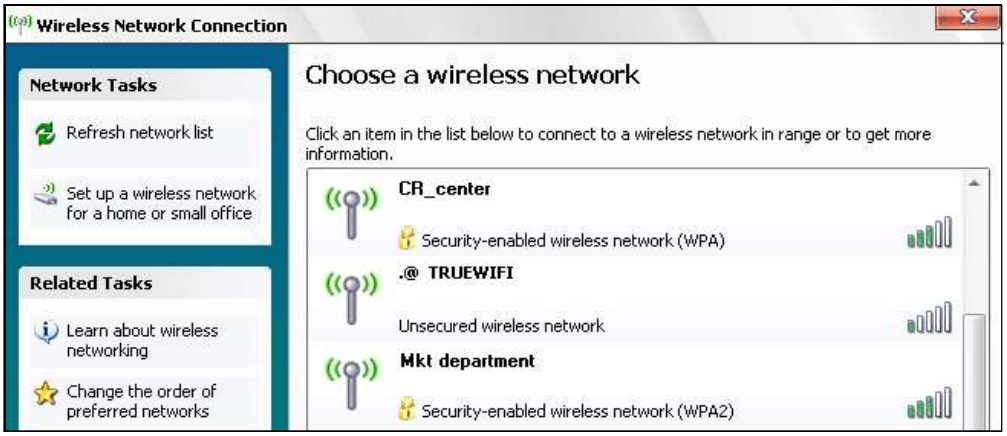
ที่ตั้งมาจากโรงงาน หรือที่เรียกว่า “ค่าดีฟอลต์” (default) เช่น ชื่อเครือข่าย (SSID) หมายเลขไอพี (IP address) ช่องสัญญาณ (Channel) และรหัสผ่านสำหรับเข้าไปกำหนดค่าให้แอคเซสพอยต์ ทั้งนี้เพื่อช่วยอำนวยความสะดวกให้ผู้ซื้อสามารถนำไปใช้งานได้ทันที เมื่อนำแอคเซสพอยต์นี้มาใช้งานควรจะเปลี่ยนค่าดีฟอลต์บางค่าเพื่อรักษาความปลอดภัยให้เครือข่าย โดยเฉพาะอย่างยิ่งการเปลี่ยนรหัสผ่านเพื่อป้องกันไม่ให้ผู้อื่นเข้าระบบมาแก้ไขค่าในแอคเซสพอยต์ได้เพราะค่าดีฟอลต์ของแอคเซสพอยต์แต่ละรุ่นนั้นมีอยู่ในคู่มือการใช้งานและสามารถค้นได้จากอินเทอร์เน็ตดังตารางที่ 1 หากมีคนที่รู้ว่าเครือข่ายนี้ใช้แอคเซสพอยต์รุ่นใดก็สามารถรู้ค่าดีฟอลต์ได้โดยง่าย

Brand	Model	SSID	IP Address	Username	Password
Dlink	713P	Default	192.168.0.1	admin	<blank>
Dlink	DWL 900AP	WLAN	192.168.0.1	admin	public
LevelOne	WBR-3405TX	default	192.168.1.1	admin	admin
Linksys	WRT54AG, WAP54G	linksys	192.168.1.1	<blank>	admin
Netgear	WAG102	NETGEAR	192.168.0.232	admin	password

ตารางที่ 1 : ตัวอย่างค่าดีฟอลต์ของแอคเซสพอยต์ที่ค้นได้จากอินเทอร์เน็ต
ที่มา : http://www.wirelessdefence.org/Contents/DefaultWIFISettings.htm

2. ซ่อนชื่อเครือข่าย

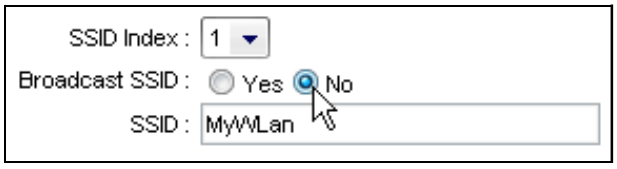
ชื่อเครือข่ายของแลนไร้สาย หรือ SSID (Service Set Identification) มักจะถูกกำหนดไว้ที่แอคเซสพอยต์ ซึ่งตั้งเป็นชื่อใดก็ได้โดยชื่อนั้นสามารถประกอบด้วยตัวอักษรตั้งแต่ 1 ถึง 32 ตัว เราสามารถกำหนดให้แอคเซสพอยส์แสดง (Broadcast) ชื่อเครือข่ายให้คอมพิวเตอร์ของผู้ใช้งานเห็นหรือไม่ก็ได้ หากตั้งค่าให้แสดงชื่อเครือข่ายคอมพิวเตอร์ของผู้ใช้งานก็สามารถสแกนพบดังรูปที่ 5 ทำให้ผู้ใช้งานเห็นและเลือกเชื่อมต่อกับเครือข่ายที่ต้องการได้ทันทีโดยไม่ต้องพิมพ์ชื่อเครือข่ายเอง แต่อาจทำให้เครือข่ายนี้ไม่ปลอดภัย เนื่องจากผู้โจมตีก็เห็นชื่อเครือข่ายเช่นกัน



รูปที่ 5 : ชื่อเครือข่าย (SSID)

ที่มา : บุญจรีย์ เจษฎาปกรณ์. (2557). การปิดจุดอ่อนและป้องกันภัยให้แลนไร้สาย. นครปฐม : มหาวิทยาลัยคริสเตียน.

การซ่อนชื่อเครือข่ายก็เป็นอีกวิธีการหนึ่งในการรักษาความปลอดภัย เพราะเมื่อไม่เห็นก็ไม่รู้ว่ามีเครือข่าย และไม่มีความพยายามที่จะเชื่อมต่อเข้ามา หากตั้งค่าแอคเซสพอยต์ให้ซ่อนชื่อเครือข่ายดังรูปที่ 6 คอมพิวเตอร์ของผู้ใช้งานจะสแกนไม่พบเมื่อต้องการเชื่อมต่อกับเครือข่าย ผู้ใช้งานจะต้องเพิ่มเครือข่ายในเครื่องเอง พร้อมทั้งพิมพ์ชื่อเครือข่ายให้ถูกต้องทั้งตัวพิมพ์เล็กและตัวพิมพ์ใหญ่ซึ่งไม่สะดวกต่อผู้ใช้งานและบางคนก็ไม่ทราบวิธีการดังนั้นการซ่อนชื่อเครือข่ายนี้ไม่เหมาะกับแลนไร้สายที่มีผู้ใช้งานเป็นจำนวนมาก เพราะจะต้องคอยให้คำแนะนำกับผู้ใช้งานที่มีเป็นจำนวนมาก ทั้งในเรื่องวิธีการเชื่อมต่อการแจ้งชื่อเครือข่ายและทุกครั้งที่มีการเปลี่ยนชื่อเครือข่ายก็ต้องแจ้งให้ทุกคนทราบด้วย



รูปที่ 6 : การตั้งค่าในแอคเซสพอยต์ให้ซ่อนชื่อเครือข่าย

ที่มา : บุญจรีย์ เจษฎาปกรณ์. (2557). การปิดจุดอ่อนและป้องกันภัยให้แลนไร้สาย. นครปฐม : มหาวิทยาลัยคริสเตียน.

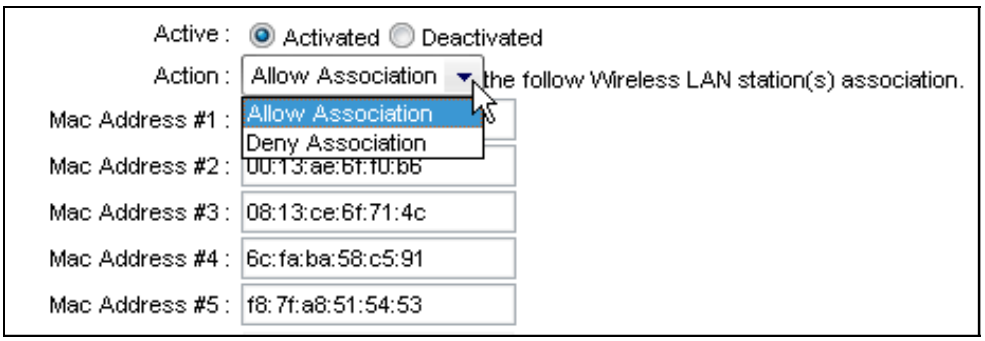
แม้ตั้งค่าให้แอคเซสพอยต์ซ่อนชื่อเครือข่ายแล้วผู้โจมตีก็ยังสามารถทราบได้โดยใช้ซอฟต์แวร์ที่มีความสามารถในการสแกนหาเครือข่ายแม้จะถูกซ่อนไว้เหตุที่ซอฟต์แวร์เหล่านี้สามารถสแกนหาได้ก็เนื่องจากในการสื่อสารระหว่างแอคเซสพอยต์กับคอมพิวเตอร์ในเครือข่าย จะมีการส่งชื่อเครือข่ายออกมาเป็นระยะๆ โดยข้อมูลนี้ไม่มีการเข้ารหัสไว้จึงสามารถดักเอาข้อมูลได้โดยง่ายดังนั้นการซ่อนชื่อเครือข่าย

เพียงอย่างเดียวจึงยังไม่พอ ควรใช้ร่วมกับวิธีการอื่นๆ ในการรักษาความปลอดภัยด้วย

3. กรองผู้ใช้งานโดยใช้หมายเลขของการ์ดแลนไร้สาย

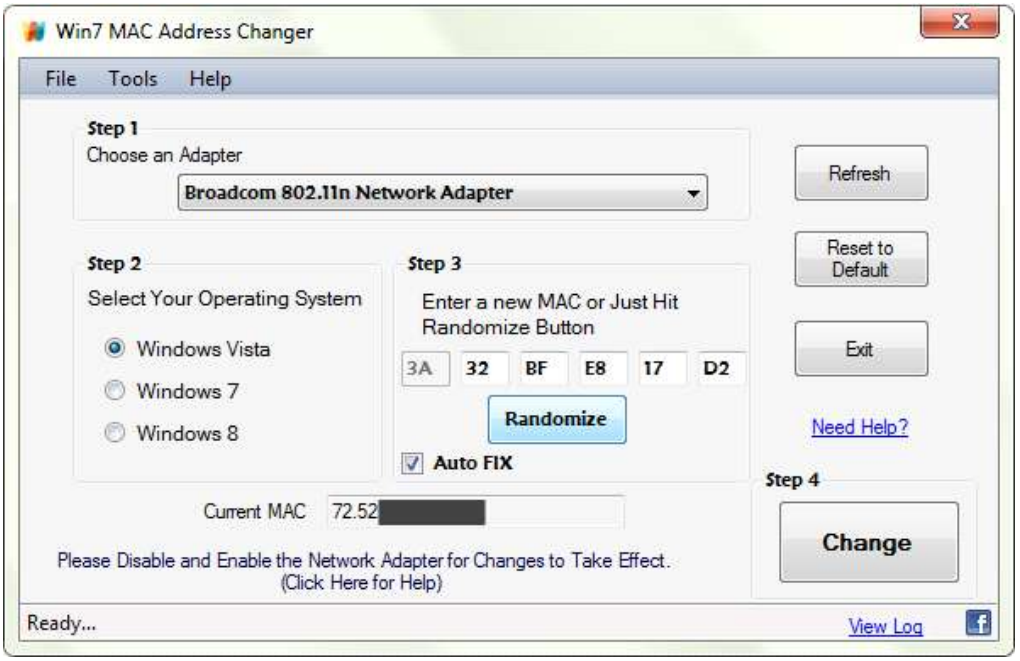
หมายเลขของการ์ดแลน หรือที่เรียกว่า “MAC address” (Media Access Control address) จะมีอยู่ในการ์ดแลนโดยทั่วไป ไม่ว่าจะเป็นแลนแบบมีสายหรือแลนไร้สาย MAC address ประกอบด้วยตัวเลขจำนวน 6 ชุด โดยแต่ละชุดเป็นเลขฐานสิบหกจำนวน 2 ตัว และคั่นแต่ละชุดด้วยเครื่องหมาย “ - ” หรือ “ : ” เช่น 80-00-27-0E-27-B8 หรือ 80:00:27:0E:27:B8 ในตัวเลข 6 ชุดนี้ สามชุดแรกใช้ระบุบริษัทผู้ผลิต ส่วนสามชุดหลังเป็นเลขที่บริษัทผู้ผลิตกำหนดขึ้นเอง เนื่องจากการ์ดแลนแต่ละใบจะมี MAC address ไม่ซ้ำกันจึงสามารถนำมาใช้ในการกรองผู้ใช้งานเครือข่ายได้

การกรองผู้ใช้งานโดยใช้หมายเลขของการ์ดแลนไร้สายจะมีอยู่ 2 รูปแบบคือ “อนุญาต” (Allow) และ “ไม่อนุญาต” (Deny) ดังรูปที่ 7 หากเลือก “อนุญาต” หมายถึงอนุญาตให้เฉพาะ MAC address ตามรายการที่บันทึกไว้สามารถใช้งานเครือข่ายได้ หากเลือก “ไม่อนุญาต” ก็จะมีความหมายในทางกลับกันคือ ไม่อนุญาตให้ MAC address ตามรายการนั้นใช้งานเครือข่าย ส่วน MAC address อื่นๆ ที่ไม่ได้บันทึกไว้สามารถใช้งานได้โดยทั่วไปเรามักนิยมกำหนดค่าเป็น “อนุญาต”



รูปที่ 7 : การกรองผู้ใช้งานโดยใช้หมายเลขของการ์ดแลนไร้สาย
ที่มา : บุญจรีย์ เจษฎาปกรณ์. (2557). การปิดจุดอ่อนและป้องกันภัยให้แลนไร้สาย. นครปฐม : มหาวิทยาลัยคริสเตียน.

MAC address เป็นหมายเลขที่บันทึกลงในการ์ดแลนมาตั้งแต่ขั้นตอนการผลิตในโรงงาน ดังนั้นจึงไม่สามารถเปลี่ยนแปลงได้แต่ก็มีวิธีการทำให้คอมพิวเตอร์เข้าใจผิดว่า MAC address เป็นอีกหมายเลขหนึ่งได้อย่างเช่นในระบบปฏิบัติการวินโดว์ คอมพิวเตอร์จะอ่านค่า MAC address จากรีจิสทรี (Registry) ซึ่งเป็นตำแหน่งที่เก็บการตั้งค่าของระบบก่อน หากไม่พบจึงไปอ่านจากการ์ดแลน ดังนั้น หากเราเข้าไปแก้ค่า MAC address ในรีจิสทรีด้วยตนเองหรือใช้ซอฟต์แวร์ช่วยในการแก้ค่าดังรูปที่ 8 ก็สามารถเปลี่ยน MAC address ได้ ผู้โจมตีก็อาจใช้วิธีเดียวกันนี้เพื่อปลอม MAC address ของตนเองให้เป็น MAC address ของผู้ที่มีสิทธิ์ใช้งานเครือข่ายดังนั้นการกรองผู้ใช้งานโดยใช้หมายเลขของการ์ดแลนไร้สายควรใช้ร่วมกับวิธีการรักษาความปลอดภัยอื่นๆ ก็จะทำให้ปลอดภัยมากขึ้น

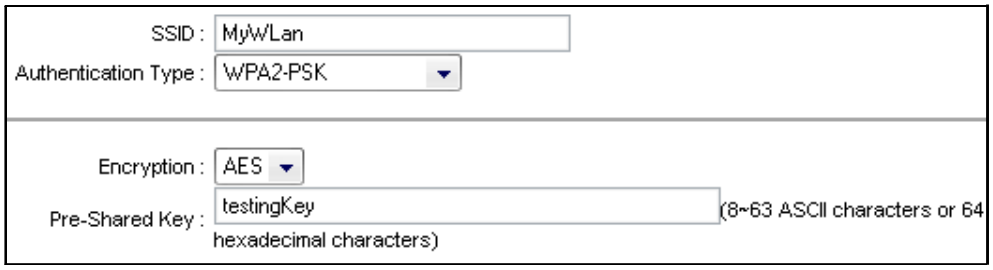


รูปที่ 8 : ซอฟต์แวร์สำหรับเปลี่ยน MAC address
ที่มา : http://www.zokali.com/softwares

4. ตั้งรหัสผ่านในการเข้าใช้งาน

การตั้งรหัสผ่านสามารถเลือกได้ 3 รูปแบบคือ WEP (Wired Equivalent Privacy) WPA (Wi-Fi Protected Access) และ WPA2 (Wi-Fi Protected Access version 2) โดย WPA2 เป็นมาตรฐานล่าสุด ทั้ง WPA และ WPA2 ยังสามารถแบ่งย่อยได้อีก 2 ประเภทคือ แบบ Personal หรือ Pre-Shared Key (PSK) ซึ่งผู้ใช้งานทุกคนจะใช้รหัสผ่านเดียวกันในการใช้งานเครือข่าย กับแบบ Enterprise ซึ่งผู้ใช้งานแต่ละคนสามารถมีรหัสผ่านที่แตกต่างกันได้ เนื่องจากมีเครื่องคอมพิวเตอร์แม่ข่ายที่เรียกว่า RADIUS Server (Remote Authentication Dial-In User Service Server) ทำหน้าที่จัดเก็บรหัสผ่านของผู้ใช้งานไว้ นอกจากนี้ WPA และ WPA2 ยังสามารถเลือกวิธีการเข้ารหัสได้ 2 แบบ คือ TKIP (Temporary Key Integrity Protocol) และ AES (Advanced Encryption Standard) โดย TKIP เป็นค่าดีฟอลต์ของ WPA และ AES เป็นค่าฟอลต์ของ WPA2 ซึ่งเป็นการเข้ารหัสที่มีความปลอดภัยมากกว่า ดังรูปที่ 9

การตั้งรหัสผ่านโดยใช้ WEP มีความปลอดภัยน้อยกว่าใช้ WPA และ WPA2 เพราะเป็นรูปแบบที่มีมานานแล้วผู้โจมตีจึงรู้อัลกอริทึมต่างๆ เป็นอย่างดี อีกทั้งยังมีซอฟต์แวร์ที่ใช้ในการเจาะระบบที่ใช้ WEP นี้เป็นจำนวนมาก ปัจจุบันระบบที่ใช้ WEP สามารถถูกเจาะได้โดยใช้เวลาเพียงไม่กี่นาที ดังนั้น การตั้งรหัสผ่านควรเลือกมาตรฐานล่าสุดซึ่งก็คือ WPA2 เพราะจะปลอดภัยมากที่สุด

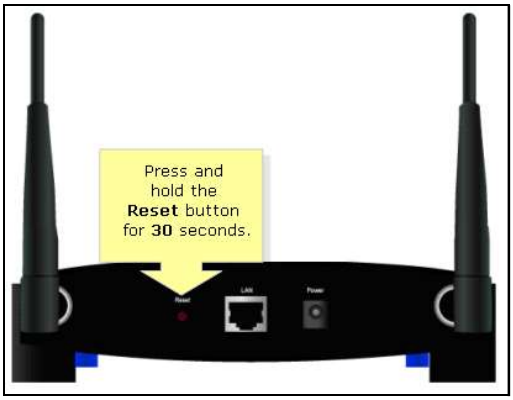


รูปที่ 9 : การตั้งรหัสผ่านในการเข้าใช้งาน
ที่มา : บุญจรีย์ เจษฎาปกรณ์. (2557). การปิดจุดอ่อนและป้องกันภัยให้แลนไร้สาย. นครปฐม : มหาวิทยาลัยคริสเตียน.

5. ติดตั้งแอคเซสพอยต์ในตำแหน่งที่เหมาะสม

ตำแหน่งในการติดตั้งแอคเซสพอยต์ก็เป็นสิ่งสำคัญอีกประการที่ควรพิจารณาในการรักษาความปลอดภัย ควรหลีกเลี่ยงการติดตั้งแอคเซสพอยต์ในตำแหน่งที่คนทั่วไปสามารถหยิบจับได้ง่าย เช่น บนโต๊ะ บนชั้นวางของโดยทั่วไปตำแหน่งที่เหมาะสมในการติดตั้งแอคเซสพอยต์คือที่สูง เช่น เพดานผนังห้องด้านบน เพราะนอกจากจะช่วยให้แอคเซสพอยต์กระจายสัญญาณได้ดีไม่มีสิ่งกีดขวางแล้วการขโมยแอคเซสพอยต์ก็ทำได้ยากและการเข้าถึงตัวอุปกรณ์แอคเซสพอยต์ก็ทำได้ยากด้วย

หากผู้โจมตีสามารถเข้าถึงอุปกรณ์แอคเซสพอยต์ได้ก็สามารถนำคอมพิวเตอร์มาเสียบสายเข้ากับพอร์ตแลนที่ด้านหลังของแอคเซสพอยต์ได้ทันทีนอกจากนี้ก็ยังสามารถกดปุ่มรีเซ็ต (Reset) ซึ่งอยู่ด้านหลังของอุปกรณ์แอคเซสพอยส์ดังรูปที่ 10 เพื่อให้คืนการตั้งค่าเป็นค่าดีฟอลต์ทั้งหมด ทำให้ผู้โจมตีสามารถเข้าไปควบคุมและตั้งค่าใหม่ให้กับแอคเซสพอยต์ได้



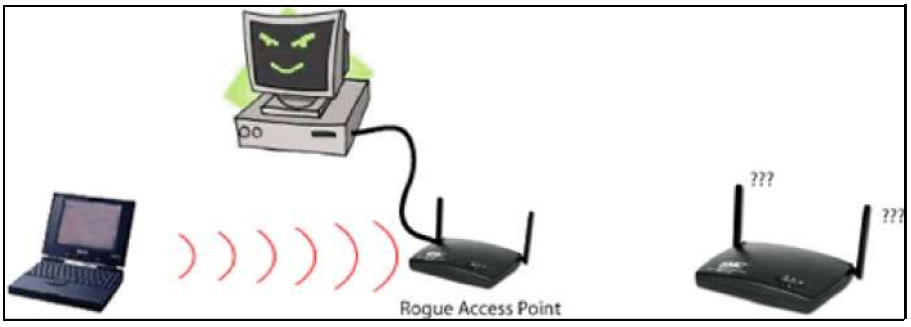
รูปที่ 10 : ปุ่มรีเซตของแอคเซสพอยต์
ที่มา : http://sw.nohold.net/Linksys/Images/kb4123-001_en.png

๖. ป้องกันแอคเซสพอยส์แปลกปลอมที่นำมาติดตั้ง

แอคเซสพอยต์แปลกปลอม คือแอคเซสพอยต์ที่ถูกเพิ่มเข้ามาในระบบเครือข่ายโดยไม่ได้รับอนุญาต ซึ่งแอคเซสพอยต์นี้อาจจะมาจากผู้ใช้งานหรือผู้ที่ต้องการโจมตีระบบเครือข่ายก็ได้

แอคเซสพอยต์แปลกปลอมที่มาจากผู้ใช้งาน โดยทั่วไปเกิดจากผู้ใช้งานที่ต้องการใช้เครือข่ายไร้สาย แต่บริเวณนั้นไม่มีแอคเซสพอยต์หรือเป็นจุดอับของสัญญาณจึงนำแอคเซสพอยต์ของตนเองมาเสียบสายเข้ากับพอร์ตแลนเพื่อกระจายสัญญาณทำให้สามารถใช้งานเครือข่ายไร้สายได้ซึ่งเหตุการณ์เช่นนี้มักเกิดในสถานที่ทำงานผลเสียที่เกิดขึ้นคือแอคเซสพอยต์ที่เพิ่มเข้ามาใหม่นี้กลายเป็นจุดอ่อนของระบบเครือข่าย เพราะผู้โจมตีจะเจาะระบบผ่านแอคเซสพอยต์ตัวนี้ เนื่องจากแอคเซสพอยต์ที่ผู้ใช้งานนำมามักเป็นแอคเซสพอยต์ที่เหมาะกับการใช้งานตามบ้าน เพราะมีราคาไม่แพงดังนั้นฟังก์ชันในการรักษาความปลอดภัยจึงน้อยกว่าแอคเซสพอยต์ที่ใช้ในสถานที่ทำงานซึ่งเป็นแอคเซสพอยต์ในระดับองค์กรอีกทั้งผู้ใช้งานบางคนไม่รู้วิธีการตั้งค่าในแอคเซสพอยส์จึงไม่ได้เปลี่ยนแปลงค่าใดเลย ค่าต่างๆในแอคเซคพอยส์ที่นำมาจึงเป็นค่าดีฟอลต์จากโรงงานซึ่งก็ทำให้ง่ายต่อการถูกเจาะระบบมากขึ้นเพื่อป้องกันแอคเซสพอยต์แปลกปลอมที่มาจากผู้ใช้งานนี้องค์กรจำเป็นจะต้องออกกฎระเบียบห้ามพนักงานนำแอคเซสพอยต์ของตนเองมาติดตั้งพร้อมทั้งชี้แจงให้พนักงานทราบถึงผลเสียหายที่อาจเกิดขึ้น

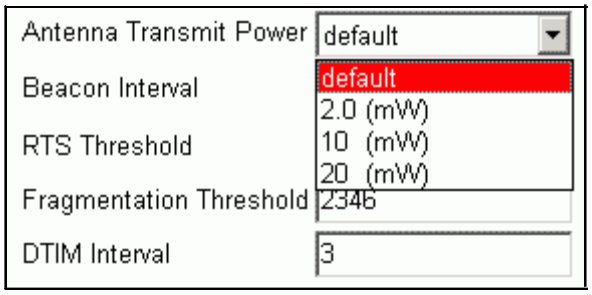
แอคเซสพอยต์แปลกปลอมจากผู้โจมตีเป็นแอคเซสพอยต์ที่ผู้โจมตีนำมาติดตั้งไว้หรือผู้โจมตีอาจลงซอฟต์แวร์ที่เครื่องคอมพิวเตอร์ของตนเองเพื่อให้เป็นเหมือนกับแอคเซสพอยต์จากนั้นผู้โจมตีจะตั้งค่าแอคเซสพอยต์ของตนเอง เช่น SSID รูปแบบการใช้รหัสผ่าน ให้เหมือนกับแอคเซสพอยต์ที่ต้องการปลอมตัวหากคอมพิวเตอร์ของผู้ใช้งานอยู่ใกล้แอคเซสพอยต์ของผู้โจมตีมากกว่าแอคเซสพอยต์จริงเครื่องก็จะเชื่อมต่อเข้ากับแอคเซสพอยต์ของผู้โจมตีนั้นเนื่องจากหลักการทำงานของแลนไร้สายจะเชื่อมต่อกับแอคเซสพอยต์ที่มีสัญญาณแรงที่สุดผู้โจมตีก็สามารถเจาะเข้าไปเอาข้อมูลจากเครื่องของผู้ใช้งานได้ ดังรูปที่ 11 เพื่อป้องกันแอคเซสพอยต์แปลกปลอมจากผู้โจมตีผู้ดูแลระบบเครือข่ายจำเป็นจะต้องตรวจตราดูแลเครือข่ายอยู่เสมอโดยอาจใช้ซอฟต์แวร์ช่วยในการสแกนเครือข่ายไร้สายและตรวจดูข้อมูลของแอคเซสพอยต์ที่มีในระบบ



รูปที่ 11 : แอคเซสพอยต์แปลกปลอมของผู้โจมตี
ที่มา : http://wlanbook.com/wifi-phishing

7. ปรับกำลังส่งของ Access Point ให้เหมาะสม

โดยทั่วไปผู้ใช้งานมักต้องการแอคเซสพอยต์ที่มีกำลังส่งมากเพราะทำให้แพร่กระจายสัญญาณไร้สายไปได้ไกลและคลอบคลุมพื้นที่ในการใช้งานได้เป็นวงกว้างแต่แอคเซสพอยต์ที่มีกำลังส่งมากเกินไปก็อาจจะก่อให้เกิดผลเสียได้เช่นกัน เพราะทำให้สัญญาณไร้สายทะลุไปยังอาคารข้างเคียงซึ่งนอกจากสัญญาณจะไปรบกวนแลนไร้สายของผู้อื่นแล้ว ไร้สายของเราได้อีกด้วยการปรับกำลังส่งของแอคเซสพอยต์ให้อยู่ภายในขอบเขตที่ต้องการจึงเป็นเรื่องสำคัญ โดยสามารถเลือกทำได้ 2 วิธีคือ การเปลี่ยนเสาอากาศของแอคเซสพอยต์สำหรับรุ่นที่สามารถถอดเปลี่ยนเสาได้ และการเข้าไปที่เมนูตั้งค่ากำลังส่งของอุปกรณ์แอคเซสพอยต์ดังรูปที่ 12 ซึ่งเมนูนี้มักมีในแอคเซสพอยต์รุ่นที่ใช้งานในระดับองค์กร



รูปที่ 12 : การตั้งค่าเพื่อปรับกำลังส่งของแอคเซสพอยต์

ที่มา : http://wireless.gumph.org/content/3/1/041-dlink-variable-transmit.html.

สรุป

แม้แลนไร้สายจะทำให้เกิดความสะดวกในการใช้งานเครือข่าย และการเชื่อมต่อกับอินเทอร์เน็ต แต่ก็มีจุดอ่อนในเรื่องของความปลอดภัยเช่นกัน การปิดจุดอ่อนและป้องกันภัยให้แลนไร้สายจึงเป็นเรื่องสำคัญที่ผู้ดูแลระบบเครือข่ายควรทำ ซึ่งการจะเลือกวิธีใดนั้นต้องพิจารณาถึงความเหมาะสมในการใช้งานด้วย เช่นการซ่อนชื่อเครือข่ายไม่เหมาะกับแลนไร้สายที่มีผู้ใช้งานเป็นจำนวนมากเพราะบริหารจัดการได้ยาก การตั้งรหัสผ่านในการใช้งานโดยใช้มาตรฐาน WPA2 แม้จะเป็นรูปแบบที่ปลอดภัยที่สุดแต่ก็ต้องตรวจสอบด้วยว่าเครื่องคอมพิวเตอร์ของผู้ใช้งานรองรับหรือไม่หากเครื่องคอมพิวเตอร์ของผู้ใช้งานส่วนใหญ่เป็นรุ่นเก่าไม่รองรับมาตรฐานนี้ก็อาจต้องใช้ WPA แทน นอกจากนี้วิธีรักษาความปลอดภัยบางวิธีอาจต้องใช้ร่วมกับวิธีการอื่นๆ เพื่อให้ปลอดภัยมากขึ้น เช่น การกรองผู้ใช้งานโดยใช้หมายเลขของการ์ดแลนไร้สายอาจใช้ร่วมกับการซ่อนชื่อเครือข่ายและการตั้งรหัสผ่านเพื่อทำให้ผู้โจมตีเชื่อมต่อและเจาะระบบเครือข่ายได้ยากยิ่งขึ้น

บรรณานุกรม

จตุชัย แพงจันทร์. (2550). *Master in Security*. กรุงเทพฯ : บริษัท ไอดีซี อินโฟร์ ดิสทริบิวเตอร์ เซ็นเตอร์ จำกัด.

จตุชัย แพงจันทร์ และ อนุโชต วุฒิพรพงษ์. (2555). *เจาะระบบ Network*. พิมพ์ครั้งที่ 3. กรุงเทพฯ : บริษัท ไอดีซี พรีเมียร์ จำกัด.

ธวัชชัย ชมศิริ. (2553). *Computer & Network Security*. กรุงเทพฯ : บริษัท โปรวิชัน จำกัด.

อรรณพ ขันธิกุล และ อำนาจ มีมงคล. (2553). *ออกแบบและติดตั้งระบบ Wireless LAN*. พิมพ์ครั้งที่ 2. กรุงเทพฯ : บริษัท ไอดีซี พรีเมียร์ จำกัด.

Amazon. (2557). *Wireless Access Pointss*. [ออนไลน์]. สืบค้นเมื่อวันที่ 9 พฤษภาคม 2557, จาก http://www.amazon.com/Cisco- WAP4410N-Wireless- N-Access-Point /dp/ B001IYCMNA.

ITvoe.com. (2557). *Laptop Internal wireless (Wi-Fi) card failure and fix*. [ออนไลน์]. สืบค้นเมื่อวันที่ 9 พฤษภาคม 2557, จาก http://www.itvoe.com/blog/ Laptop-Internal-wireless-Wifi-card-failure-and-fix.

Nohold.net. (2557). *Linksys*. [ออนไลน์]. สืบค้นเมื่อวันที่ 9 พฤษภาคม 2557, จาก http:// sw.nohold.net/Linksys/Images /kb4123-001_en.png.

Vicomsoft. (2557). *Wireless Networking*. [ออนไลน์]. สืบค้นเมื่อวันที่ 8 พฤษภาคม 2557, จาก http: //www.vicomsoft.com/images /learning-center/ wireless-networking.

Wikipedia. (2557). *Wireless LAN*. [ออนไลน์]. สืบค้นเมื่อวันที่ 7 พฤษภาคม 2557, จาก http://en.wikipedia.org/wiki/Wireless_LAN.

Wireless.gumph.org. (2557). *D-Link supports longrange Wi-Fi*. [ออนไลน์]. สืบค้นเมื่อวันที่ 9 พฤษภาคม 2557, จาก http://wireless.gumph.org/content/3/1/ 041-dlink-variable- transmit.html.

Wirelessdefence.org. (2557). *Default Wireless Router Setting*. [ออนไลน์]. สืบค้นเมื่อวันที่ 9 พฤษภาคม 2557, จาก http: //www.wirelessdefence.org/Contents/ DefaultWIFISettings.htm.

WLANBook. (2557). *WiFi Phishing*. [ออนไลน์]. สืบค้นเมื่อวันที่ 12 พฤษภาคม 2557, จาก http:// wlanbook.com/wifi-phishing.

Zokali Softwares. (2557). *Softwares*. [ออนไลน์]. สืบค้นเมื่อวันที่ 9 พฤษภาคม 2557, จาก http:// www.zokali.com/softwares.