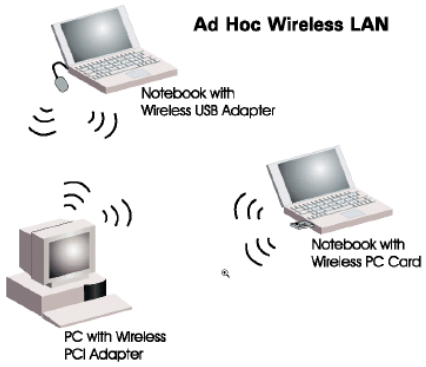
เปิดโลกระบบเครือข่ายไร้สาย
การเชื่อมต่อ ช่องโหว่ และการรักษาความปลอดภัย (ตอนที่ 3)

อำนาจ สุคนเขตร์*

การเชื่อมต่อของระบบเครือข่ายไร้สาย มี 2 รูปแบบด้วยกัน

รูปแบบการเชื่อมต่อแบบที่ 1 เรียกว่าแบบ Ad-Hoc หรือแบบ Peer-to-Peer เป็นรูปแบบการเชื่อมต่อกันระหว่างเครื่องคอมพิวเตอร์ไร้สายและอุปกรณ์ต่าง ๆ ตั้งแต่สองเครื่องขึ้นไป เป็นการเชื่อมต่อกันโดยตรงระหว่างเครื่องคอมพิวเตอร์ไร้สาย หรือระหว่างเครื่องคอมพิวเตอร์ไร้สายกับอุปกรณ์ไร้สายอื่น ๆ โดยไม่มีอุปกรณ์ศูนย์กลางควบคุม เรียกว่า Access Point ดังภาพที่ 1 ผู้ส่งจะใช้วิธีการแพร่กระจายสัญญาณออกไปทุกทิศทาง โดยไม่ทราบว่าเครื่องผู้รับอยู่ที่ใด เครื่องผู้รับจะต้องอยู่ในขอบเขตพื้นที่ให้บริการที่สัญญาณมาถึงและคอยตรวจสอบสัญญาณว่าใช่ของตนหรือไม่ จะตรวจสอบจากค่า MAC Address ของเครื่องผู้รับ ซึ่งถ้าใช่ก็จะนำสัญญาณไปทำงานต่อไป รูปแบบการเชื่อมต่อแบบนี้จะไม่สามารถเชื่อมต่อเข้ากับระบบเครือข่ายแบบมีสายสัญญาณได้ เว้นเสียแต่ว่าจะต้องติดตั้งอุปกรณ์ที่เรียกว่า Bridge แบบไร้สาย หรือ Access Point



ภาพที่ 1 แสดงรูปแบบการเชื่อมต่อแบบ Adhoc หรือ Peer-to-Peer

* **นักวิชาการศึกษา** กลุ่มงานพัฒนาและเผยแพร่นวัตกรรมเทคโนโลยีทางการศึกษา
ฝ่ายเทคโนโลยีทางการศึกษา สำนักวิทยบริการ
มหาวิทยาลัยสงขลานครินทร์ วิทยาเขตปัตตานี

รูปแบบการเชื่อมต่อแบบที่ 2 เรียกว่าแบบ Infrastructure หรือทั่วไปมักจะเรียกว่า Client/Server การเชื่อมต่อแบบนี้เครื่องคอมพิวเตอร์ไร้สายสามารถติดต่อสื่อสารกันระหว่างเครื่องคอมพิวเตอร์แบบมีสายและอุปกรณ์อื่น ๆ ที่เชื่อมต่ออยู่บน LAN เดียวกันได้ ดังภาพที่ 2 โดยอาศัยอุปกรณ์ศูนย์กลางควบคุมเรียกว่า Access Point ซึ่งทำหน้าที่คล้ายคลึงกับฮับ (HUB) ลักษณะของอุปกรณ์ตัวนี้ด้านหนึ่งสามารถเชื่อมต่อกับสายสัญญาณ UTP โดยเชื่อมต่อไปยังสวิตช์ชิ่งฮับ (Switching HUB) ของ LAN กับตัวมันเอง ดังภาพที่ 3 อีกด้านจะแพร่กระจายสัญญาณออกมาโดยจะทำหน้าที่แปลงสัญญาณวิทยุไปเป็นสัญญาณที่ LAN ใช้งานอยู่ หรือในทางกลับกัน การใช้ Access Point จะทำให้เครื่องคอมพิวเตอร์ไร้สายสามารถติดต่อกับเครื่องคอมพิวเตอร์แบบมีสายและอุปกรณ์อื่น ๆ ที่เชื่อมต่ออยู่บน LAN เดียวกันได้ และสามารถใช้ LAN เพื่อเป็นทางผ่านออกไปสู่อินเทอร์เน็ตได้

ภาพที่ 2 แสดงรูปแบบการเชื่อมต่อแบบ Infrastructure

ภาพที่ 3 แสดง Access Point แบบต่าง ๆ

ภาพที่ 4 แสดง Wireless Card แบบต่าง ๆ

ช่องโหว่ของระบบเครือข่ายไร้สาย

โดยทั่วไปแล้วระบบเครือข่ายไร้สายมีความเสี่ยงต่อการถูกโจมตีมากกว่าระบบเครือข่ายที่ใช้สายนำสัญญาณ เนื่องจากสัญญาณข้อมูลแพร่กระจายอยู่ในอากาศ และไม่จำกัดขอบเขตอยู่เพียงแต่ในห้อง ๆ เดียว หรือบริเวณแคบ ๆ เท่านั้น แต่สัญญาณจะแพร่ไปถึงบริเวณภายนอกเขตความดูแลของผู้บริหารระบบได้ ซึ่งอาจจะทำให้ผู้โจมตีสามารถดักฟัง ปลอมแปลงสัญญาณข้อมูล หรือบุกรุกระบบได้โดยไม่ต้องปรากฏตัวให้เห็น ยิ่งไปกว่านั้นผู้โจมตีอาจใช้อุปกรณ์สายอากาศพิเศษที่ทำให้สามารถรับส่งสัญญาณจากบริเวณภายนอกที่ไกลออกไปได้มาก อีกทั้งเทคโนโลยีสำหรับการรักษาความปลอดภัยที่ติดตั้งกับตัวระบบเครือข่ายไร้สายนั้น ปัจจุบันมีช่องโหว่อยู่มาก ดังนั้นผู้ที่ใช้ระบบเครือข่ายไร้สายควรตระหนักถึงความเสี่ยงและช่องโหว่ด้านความปลอดภัยของระบบเครือข่ายไร้สายดังที่จะกล่าวถึงในส่วนต่อไปนี้

สัญญาณรบกวน (Jamming)

สัญญาณรบกวนเป็นปัญหาที่สำคัญอีกปัญหาหนึ่งสำหรับระบบเครือข่ายไร้สาย ซึ่งยากที่จะหลีกเลี่ยงได้เนื่องจากเป็นธรรมชาติของการสื่อสารแบบไร้สาย โดยทั่วไปแล้วสัญญาณรบกวนในช่องสัญญาณจะสร้างปัญหาให้กับอุปกรณ์ภาครับ โดยทำให้ไม่ให้สามารถแปลสัญญาณข้อมูลที่ถูกส่งมาได้อย่างถูกต้อง สำหรับระบบเครือข่ายไร้สาย นอกจากปัญหาดังกล่าวแล้วหากสัญญาณรบกวนในช่องสัญญาณที่ใช้อยู่มีกำลังสูงพอประมาณ กลไก CSMA/CA ที่ได้กล่าวถึงในตอนที่ 1 แล้ว มีหน้าที่ควบคุมสิทธิในการส่งสัญญาณของอุปกรณ์ระบบเครือข่ายไร้สาย จะไม่อนุญาตให้อุปกรณ์ใด ๆ ทำการส่งสัญญาณได้เลย สรุปก็คือสัญญาณรบกวนในช่องสัญญาณนอกจากจะทำให้สมรรถนะของระบบเครือข่ายไร้สายลดลงแล้วยังอาจทำให้ระบบเครือข่ายตกอยู่ในสภาวะ Denial-of-Service ด้วย

สัญญาณรบกวนอาจเกิดมาจากอุปกรณ์สื่อสารหรืออุปกรณ์ระบบเครือข่ายไร้สายอื่น ๆ ที่ถูกใช้งานอยู่ในบริเวณใกล้เคียงซึ่งมีการรับส่งสัญญาณด้วยคลื่นความถี่ย่านเดียวกับอุปกรณ์ระบบเครือข่ายไร้สาย ในระบบที่ใช้งานอยู่ ส่วนใหญ่แล้วอุปกรณ์ระบบเครือข่ายไร้สายที่นิยมใช้กันอยู่ทั่วไปมีการรับส่งสัญญาณด้วยคลื่นวิทยุในย่านความถี่ 2.4 GHz หรือที่มีชื่อเรียกว่าย่านความถี่ ISM (Industrial Scientific Medical) ซึ่งเป็นย่านความถี่สาธารณะสากลที่ถูกจัดสรรสำหรับการใช้งานร่วมกันของอุปกรณ์หรือเครื่องมือสื่อสารต่าง ๆ เช่น เครื่องไมโครเวฟ โทรศัพท์แบบไร้สาย (Cordless Phone) อุปกรณ์ Bluetooth และอุปกรณ์ระบบเครือข่ายไร้สาย เป็นต้น ซึ่งระบบเครือข่ายไร้สายที่เราใช้งานอยู่อาจไม่สามารถทำงานอย่างเต็มประสิทธิภาพ หรือตกอยู่ในสภาวะ Denial-of-Service หากมีการใช้งานอุปกรณ์ดังกล่าวในบริเวณใกล้เคียง นอกจากนี้แล้วสัญญาณรบกวนอาจเกิดมาจากการกระทำของผู้โจมตีโดยจงใจ ผู้โจมตีอาจนำอุปกรณ์สื่อสารที่ใช้ความถี่เดียวกับอุปกรณ์ระบบเครือข่ายไร้สายที่ถูกดัดแปลงให้ส่งสัญญาณออกมารบกวนมาติดตั้ง และกระจายสัญญาณในบริเวณใกล้เคียงเพื่อรบกวน หรือปิดกั้นการทำงานของระบบเครือข่ายไร้สาย นอกจากนี้ผู้โจมตีอาจใช้วิธีส่งสัญญาณข้อมูลหรือคำสั่งต่าง ๆ โดยไม่ตรงกับมาตรฐานเพื่อครอบครองช่องสัญญาณไว้เพียงผู้เดียวหรือกีดกันไม่ให้ผู้อื่นเข้าใช้ช่องสัญญาณได้

ไม่มีการใช้ WEP (Wired Equivalent Privacy)

อุปกรณ์ระบบเครือข่ายไร้สายที่ไม่มีการใช้งานกลไกรักษาความปลอดภัยเป็นช่องโหว่ของระบบที่อันตรายมาก ซึ่งทำให้มีความเสี่ยงสูงที่ระบบจะถูกโจมตีหรือใช้เป็นฐานสำหรับโจมตีระบบ อื่น ๆ และการแกะรอยผู้โจมตีเป็นไปได้ยาก จริงอยู่ที่การไม่ติดตั้งกลไกรักษาความปลอดภัยสำหรับระบบเครือข่ายไร้สายจะทำให้ผู้ใช้สามารถเชื่อมต่อเข้ากับระบบเครือข่ายไร้สาย และอินเตอร์เน็ตได้อย่างสะดวก (Plug-n-Play) แต่ในขณะเดียวกันการไม่ติดตั้งกลไกรักษาความปลอดภัยก็เป็นการอำนวยความสะดวก ให้ผู้โจมตีบุกรุกระบบได้อย่างง่ายดายด้วยกัน โดยปกติแล้วความสามารถในการรับส่งสัญญาณของอุปกรณ์ระบบเครือข่ายไร้สาย ไม่ได้จำกัดขอบเขตอยู่เพียงแต่ในห้อง ๆ เดียวหรือบริเวณแคบ ๆ เท่านั้น แต่จะครอบคลุมไปถึงบริเวณภายนอกด้วย ดังนั้นผู้โจมตีสามารถบุกรุกระบบในขณะที่หลบซ่อนตัวอยู่ในบริเวณใกล้เคียง และไม่ต้องปรากฏตัวให้เห็น ยิ่งไปกว่านั้นผู้โจมตีอาจใช้อุปกรณ์สายอากาศพิเศษที่สามารถรับส่งสัญญาณจากบริเวณภายนอกที่ไกลออกไปมากซึ่งทำให้การจับตัวผู้โจมตีเป็นไปได้ยากขึ้นอีกด้วย การไม่ใช้งานกลไกรักษาความปลอดภัยสำหรับระบบเครือข่ายไร้สายเท่ากับเป็นการเปิดประตูและท้าทายให้ผู้โจมตีบุกรุกเข้ามาในเครือข่าย และสร้างความเสียหายให้กับระบบได้มากมายหลายรูปแบบ อาทิ

- ดักฟัง และตีความหมาย หรือปลอมแปลงสัญญาณข้อมูลที่ถูกรับส่งในระบบเครือข่ายไร้สายได้อย่างเสรี โดยเฉพาะอย่างยิ่งข้อมูลเกี่ยวกับ Username และรหัสผ่านต่าง ๆ
- ลักลอบใช้อินเทอร์เน็ตได้ฟรี หากระบบเครือข่ายไร้สายมีการเชื่อมต่อกับอินเทอร์เน็ตด้วย
- เข้าถึง ดัดแปลง หรือทำลายข้อมูลทรัพยากรต่าง ๆ ที่ได้รับการ Share ไว้ ทั้งในระบบเครือข่ายไร้สาย และระบบเครือข่ายมีสาย สำหรับผู้ใช้ทั่วไปในระบบนั้น ๆ

-ฉวยโอกาสใช้ ช่องโหว่ของซอฟต์แวรต่าง ๆ ในระบบเพื่อเพิ่มขีดความสามารถในการโจมตี ซึ่งผู้โจมตีอาจจะสามารถนำโค้ดต่าง ๆ มาติดตั้งและเรียกใช้ในระบบได้ในที่สุด

-ตกเป็นเหยื่อที่ถูกใช้เป็นฐานสำหรับโจมตีระบบอื่น ซึ่งผู้โจมตีสามารถกลบเกลื่อนร่องรอย และป้ายความผิดได้อย่างแนบเนียนเนื่องจากหลักฐานทุกอย่างจะชี้ไปยังเครือข่ายของเหยื่อ

การที่อุปกรณ์ระบบเครือข่ายไร้สายถูกติดตั้งโดยไม่มีการใช้กลไกรักษาความปลอดภัยไว้นั้นอาจเนื่องมากจากสาเหตุต่อไปนี้

- ระบบเครือข่ายไร้สายถูกติดตั้งเป็นเครือข่ายสาธารณะที่อนุญาตให้ผู้ใช้ทั่วไปสามารถเข้ามาใช้เครือข่ายได้อย่างสะดวกและอิสระ เช่น ระบบเครือข่ายไร้สายในห้องสมุด โรงเรียน มหาวิทยาลัย หรือศูนย์ประชุม เป็นต้น การติดตั้งรหัสผ่านในกรณีนี้อาจไม่เหมาะสมหรือเป็นไปได้ยากในทางปฏิบัติ
- ผู้ใช้ต้องการความสะดวกในการติดตั้งและใช้งาน
- ผู้ดูแลระบบไม่ต้องการความยุ่งยากที่จะต้องบริหารและแจกจ่ายรหัสผ่านให้กับอุปกรณ์ระบบเครือข่ายไร้สายทุกชิ้น ซึ่งจะต้องเสียเวลาค่อนข้างมากในการกำหนดหรือเปลี่ยนค่ารหัสผ่านในเครือข่าย
- อุปกรณ์ระบบเครือข่ายไร้สายถูกติดตั้งด้วยค่า default ซึ่งโดยปกติแล้วอุปกรณ์ระบบเครือข่ายไร้สาย จะถูกตั้งค่ามาโดย defaultให้ไม่มีการใช้กลไกรักษาความปลอดภัยเพื่อเป็นการอำนวยความสะดวกในการใช้อุปกรณ์ระบบเครือข่ายไร้สาย ซึ่งผู้ติดตั้งระบบเครือข่ายไร้สายที่ไม่มีความรู้ประสบการณ์ หรือความพยายามเพียงพอส่วนมากมักจะติดตั้งด้วยค่า default นั่นเอง

-อุปกรณ์ระบบเครือข่ายไร้สายที่มาพร้อมกับเครื่องคอมพิวเตอร์ (โดยเฉพาะอย่างยิ่งคอมพิวเตอร์แบบพกพาสมัยใหม่ซึ่งมักจะมีอุปกรณ์ระบบเครือข่ายไร้สายแบบ built-in มาด้วย) อาจจะไม่มีการ enable กลไกรักษาความปลอดภัยไว้

-พนักงานในองค์กรทำการติดตั้งอุปกรณ์ระบบเครือข่ายไร้สายโดยไม่ได้รับอนุญาต

-ผู้โจมตีแอบติดตั้งอุปกรณ์ระบบเครือข่ายไร้สายไว้

- ช่องโหว่ของกลไก WEP (Wired Equivalent Privacy)

เนื่องจาก WEP ถูกออกแบบมาเพื่อสร้างความปลอดภัยให้กับระบบเครือข่ายไร้สาย ในระดับที่ใกล้เคียงกับระบบเครือข่ายแบบมีสาย จึงไม่น่าประหลาดใจเลยว่ากลไกดังกล่าวมีช่องโหว่อยู่หลายประการ ดังจะกล่าวถึงในส่วนต่อไปนี้

ช่องโหว่ของ WEP Encryption

กลไกการเข้ารหัสข้อมูลของ WEP มีช่องโหว่ซึ่งอาจทำให้ผู้โจมตีสามารถคำนวณหา key stream หรือรหัสลับที่ใช้ในระบบเครือข่ายไร้สายได้ การเจาะกลไกการเข้ารหัสของ WEP มีหลายรูปแบบเช่น การทดสอบรหัสทุกค่าที่เป็นไปได้ การสร้างพจนานุกรมของ Key Stream และการทำนายรหัสลับจาก Key Stream ซึ่งจะกล่าวถึงดังต่อไปนี้

-Brute-Force Attack การเจาะรหัสลับโดยใช้วิธีทดสอบรหัสทุก ๆ ค่า (brute-force) ในกรณีที่รหัสลับในระบบเครือข่ายไร้สาย มีขนาดสั้นเกินไป (40 บิต) ผู้โจมตีสามารถใช้วิธีทดสอบรหัสทุก ๆ ค่าที่

เป็นไปได้กับข้อมูลที่รวบรวมจากเครือข่ายว่าเป็นรหัสผ่านที่ใช้หรือไม่ (โดยการคำนวณและตรวจสอบค่า ICV (Integrity Check Value)) นอกจากนี้ผู้โจมตีอาจสามารถใช้ dictionary เพื่อช่วยในการสืบหารหัสลับได้เร็วขึ้นด้วย หากมีการใช้รหัสลับที่ยาวมากขึ้นวิธีการโจมตีแบบนี้ก็อาจจะสำเร็จได้ยาก

-Key Stream Dictionary คำนวณหา key stream ที่ใช้ในการเข้ารหัสข้อความสำหรับ IV (Initialization Vector) แต่ละค่า ผู้โจมตีจะต้องรู้ข้อมูลดิบก่อนเข้ารหัสถึงจะสามารถคำนวณหา key stream ได้โดยการทำ XOR ระหว่างข้อมูลดิบและข้อความรหัสที่รวบรวมได้จากเครือข่าย ซึ่งผู้โจมตีอาจรู้ข้อมูลดิบของ packet หนึ่ง ๆ ที่ส่งมาได้โดยการล่อลวงผู้ใช้หรือเครือข่ายให้มีการส่งข้อความที่ต้องการหรือทำนายได้ เมื่อผู้โจมตีทราบ key stream สำหรับ IV ค่าหนึ่ง ๆ ผู้โจมตีจะสามารถเข้ารหัสข้อมูลที่จะส่งผ่านกลไก WEP หรืออ่าน packet ที่ถูกเข้ารหัสด้วย key stream และ IV ดังกล่าวได้แล้วโดยไม่จำเป็นต้องรู้รหัสลับ นอกจากนี้ผู้โจมตีอาจจะสามารถรวบรวมข้อมูลโดยวิธีดังกล่าวได้มากจนกระทั่งสร้างฐานข้อมูลของ key stream สำหรับทุก ๆ ค่าที่เป็นไปได้ของ IV (ซึ่งมีทั้งหมด 2^24 = 16,777,216 ค่า) ซึ่งจะทำให้ผู้โจมตีสามารถอ่าน packet ที่ถูกเข้ารหัสด้วย key stream และ IV แต่ละค่าได้อย่างสมบูรณ์ แต่อย่างไรก็ตามการที่จะสร้างฐานข้อมูลดังกล่าวได้นั้นผู้โจมตีอาจต้องใช้เวลานานและความพยายามสูง

-Weak IVs Attack ผู้โจมตีสามารถอาศัยช่องโหว่ที่เกิดขึ้นเมื่อ IV บางค่า + รหัสลับ ถูกใช้ใน RC4 PRNG ซึ่งจะทำให้ผู้โจมตีสามารถทำนายรหัสลับที่ใช้ในเครือข่ายได้จากไบต์แรก ๆ ของ key stream ซึ่งค่า IV ที่ทำให้เกิดช่องโหว่ดังกล่าวเรียกว่า Weak IV ในการเจาะรหัสลับนี้ผู้โจมตีจะต้องทราบข้อมูลดิบในไบต์แรกของ packet เพื่อนำมาคำนวณหาไบต์แรกของ key stream ซึ่งเป็นโชคร้ายของระบบที่ข้อความใน IEEE 802.11 packet มักจะเริ่มต้นด้วยค่าคงที่ [เช่น 0xAA (Hex)] ซึ่งเป็น header ของโพรโตคอลที่อยู่ layer เหนือขึ้นไป แต่อย่างไรก็ตามการทำนายรหัสลับด้วยวิธีดังกล่าวไม่ได้ให้ผลลัพธ์ถูกต้องเสมอไป ผู้โจมตีจะต้องพยายามทำนายรหัสลับจาก packet ที่ถูกเข้ารหัสด้วย Weak IV ที่แตกต่างกันออกไปหลาย ๆ ครั้ง ซึ่งผลที่ได้รับจากการทำนายซ้ำ ๆ กันมากที่สุดจะมีโอกาสเป็นรหัสลับที่ต้องการนั่นเอง ในปัจจุบันซอฟต์แวร์สำหรับเจาะรหัสลับด้วยวิธีดังกล่าวได้ถูกเผยแพร่สู่สาธารณชนทั่วไปแล้ว ซอฟต์แวร์ที่ว่านี้ได้แก่ Airsnort และ WEPcrack (สำหรับระบบปฏิบัติการ Linux) ซึ่งสามารถทำนายรหัสลับได้อย่างค่อนข้างแม่นยำหลังจากรวบรวมข้อมูลจากเครือข่ายได้ประมาณ 1,000,000 - 5,000,000 packet (ซึ่งอาจต้องใช้เวลานานหลายชั่วโมงในการรวบรวมข้อมูลจำนวนดังกล่าว)

ช่องโหว่ของ WEP Authentication

กลไกการตรวจสอบผู้ใช้ (WEP Authentication) แบบ Shared Key ที่กำหนดไว้ในมาตรฐาน IEEE 802.11 มีช่องโหว่ทำให้ผู้โจมตีสามารถล่วงรู้ความลับส่วนหนึ่งของระบบเครือข่ายไร้สายได้ ซึ่งผู้โจมตีสามารถนำไปใช้เพื่อผ่านการตรวจสอบและได้รับอนุญาตให้ใช้เครือข่ายได้อย่างถูกต้อง หรือใช้ในการเข้ารหัสข้อมูลได้ นอกจากนั้นผู้โจมตียังสามารถที่จะถอดรหัสข้อมูลได้บางส่วนหรืออาจจะสามารถ ถอดรหัสลับของเครือข่ายได้ในที่สุดเมื่อผู้โจมตีรวบรวมข้อมูลดังกล่าวจนเพียงพอ เนื่องจากในระหว่างการทำ

งานของกลไก WEP Authentication จะมีการส่งข้อความคำถาม (Challenge Text) โดยไม่มีการเข้ารหัสสัญญาณมายังผู้ที่ขอรับการตรวจสอบ จากนั้นผู้ขอรับการตรวจสอบทำการเข้ารหัสข้อความคำถามที่ได้รับแล้วส่งกลับไปเพื่อรับการตรวจสอบ ดังนั้นผู้โจมตีซึ่งสามารถดักฟังเพื่อทราบถึงข้อความคำถามทั้งก่อนและหลังการเข้ารหัสข้อมูลจึงสามารถคำนวณหา Key Stream และ IV ที่ถูกใช้ได้โดยการ XOR แบบบิตต่อบิตระหว่างข้อความทั้งสอง เมื่อทราบ Key Stream และ IV แล้วผู้โจมตีสามารถใช้ Key Stream และ IV ดังกล่าวในการเข้ารหัสข้อความคำถาม (Challenge Text) ระหว่างขอรับการตรวจสอบ เนื่องจาก Key Stream และ IV ดังกล่าวมีความถูกต้อง ผู้โจมตีจึงสามารถที่จะผ่านการตรวจสอบของกลไก WEP Authentication ได้อย่างถูกต้อง นอกจากนี้เนื่องจากในระบบเครือข่ายไร้สาย รหัสลับที่ใช้ในกระบวนการ Authentication เป็นรหัสลับเดียวกันกับที่ใช้ในการเข้ารหัสข้อมูล และเป็นรหัสลับหนึ่งเดียวที่ทุกคนในเครือข่ายใช้ร่วมกัน ดังนั้น Key Stream และ IV ที่ผู้โจมตีได้รับดังกล่าวจึงสามารถถูกนำไปใช้ในการเข้ารหัสข้อมูลเพื่อส่งผ่านเครือข่ายได้ด้วยโดยทำการ XOR ระหว่าง Key Stream และข้อมูลที่ต้องการส่ง นั่นหมายความว่าช่องโหว่ที่กล่าวถึงนี้ได้ทำให้ผู้โจมตีผ่านการตรวจสอบ และทำการส่งข้อความสั้น ๆ (128 ไบต์ ซึ่งเป็นขนาดของ Challenge Text ที่ใช้ในกระบวนการ Authentication) ได้อย่างเสรี นอกจากนี้ผู้โจมตีสามารถนำเอา Key Stream และ IV ที่คำนวณได้ไปใช้ในการถอดรหัสข้อความในเครือข่ายซึ่งถูกเข้ารหัสด้วย IV และ Key Stream ดังกล่าวได้บางส่วนด้วย เนื่องจากในกระบวนการ Authentication แต่ละครั้งอาจมีการใช้ IV ที่แตกต่างกันออกไป ดังนั้นเมื่อเกิดกระบวนการ Authentication หลาย ๆ ครั้ง ผู้โจมตีอาจจะสามารถรวบรวมข้อมูลดังกล่าวได้อย่างสมบูรณ์จนสร้างฐานข้อมูลของ Key Stream สำหรับทุก ๆ ค่าที่เป็นไปได้ของ IV เพื่อนำไปใช้ในการถอดรหัสข้อความซึ่งถูกเข้ารหัสด้วย IV และ Key Stream นั้น ๆ ได้ ในกรณีนี้ผู้โจมตีสามารถก่อให้เกิดกระบวนการ Authentication จำนวนมากได้โดยการส่งสัญญาณ Request-for-Deauthentication เพื่อขอให้เครือข่ายระงับสิทธิของผู้ใช้หนึ่ง ๆ (ซึ่งมาตรฐาน IEEE 802.11 ได้กำหนดให้ Request ดังกล่าวไม่สามารถถูกปฏิเสธได้) ทำให้ผู้ใช้นั้น ๆ ต้องขอรับการตรวจสอบครั้งใหม่ซ้ำ ๆ อย่างต่อเนื่อง ยิ่งไปกว่านั้นผู้โจมตีอาจจะสามารถคำนวณหารหัสลับที่ใช้ในเครือข่ายได้จาก Key Stream ที่ถูกสร้างจากค่า IV ที่อ่อนแอ (Weak IV) จำนวนหนึ่งได้ เมื่อนั้นก็หมายความว่ากลไกสำหรับการรักษาความปลอดภัยของเครือข่ายที่กำหนดไว้ในมาตรฐาน IEEE 802.11 ได้ถูกพิชิตลงแล้วอย่างสิ้นเชิง เห็นได้ว่ากลไกการตรวจสอบและอนุญาตผู้ใช้แบบใช้รหัสผ่าน (Shared-Key WEP Authentication) ที่กำหนดไว้ในมาตรฐาน IEEE 802.11 ถูกเจาะได้ไม่ยากและยังเป็นช่องโหว่ให้ผู้โจมตีสามารถคำนวณหารหัสลับของเครือข่ายได้ซึ่งจะทำให้ความปลอดภัยของระบบเครือข่ายไร้สายหมดไปโดยสิ้นเชิง

ดังนั้นผู้ดูแลระบบจึงควรหลีกเลี่ยงการใช้กลไกตรวจสอบดังกล่าวในระบบเครือข่ายไร้สาย และเปลี่ยนไปใช้เทคนิคอื่นเพื่อทำการตรวจสอบและอนุญาตผู้ใช้

การโจมตีแบบ Man-in-Middle

ในการโจมตีแบบ Man-in-Middle ผู้โจมตีจะลวงให้ผู้ใช้เชื่อมต่อเข้ากับ Access Point ของผู้โจมตีซึ่งจะทำให้ผู้โจมตีสามารถเข้าถึงข้อมูลที่ผู้ใช้รับส่งอยู่ได้ เนื่องจากมาตรฐาน IEEE 802.11 ไม่ได้บังคับให้เครื่องคอมพิวเตอร์ของผู้ใช้ต้องทำการ Authenticate Access Point ก่อนเข้ารับบริการ ซึ่งเครื่องคอมพิวเตอร์ของผู้ใช้สามารถเชื่อมต่อเข้ากับ Access Point ใด ๆ ก็ได้ที่ให้บริการ และโดยปกติเครื่องคอมพิวเตอร์ของผู้ใช้จะเลือกที่จะเชื่อมต่อเข้ากับ Access Point ที่มีกำลังรับส่งสูงกว่า ดังนั้นผู้โจมตีอาจสามารถล่อลวงให้เครื่องคอมพิวเตอร์ของผู้ใช้เชื่อมต่อกับ Access Point ของผู้โจมตีที่มีกำลังรับส่งสูงกว่าได้

การรักษาความปลอดภัย

ระบบเครือข่ายไร้สายมีช่องโหว่หลายประการซึ่งทำให้ผู้โจมตีสามารถบุกรุกระบบเครือข่ายไร้สายหรือใช้ระบบเครือข่ายไร้สายเป็น back-door เพื่อโจมตีระบบเครือข่ายในส่วนอื่น ๆ ของระบบได้ หรือใช้ระบบเครือข่ายไร้สายเป็นฐานสำหรับโจมตีระบบอื่นแล้วป้ายความผิดให้ระบบเครือข่ายไร้สายที่ตกเป็นเหยื่อแทน ถึงแม้ว่าระบบเครือข่ายไร้สายในความดูแลของท่านจะได้รับการติดตั้งกลไกการรักษาความปลอดภัยที่เหมาะสมแล้วเพื่อป้องกันไม่ให้ผู้โจมตีสามารถบุกรุกผ่าน Firewall เข้ามาโจมตีระบบได้ แต่หากไม่มีการป้องกันผู้โจมตีจากการบุกรุกเข้ามาทางระบบเครือข่ายไร้สาย ซึ่งเป็นส่วนอ่อนแอที่สุดส่วนหนึ่งของระบบ การลงทุนติดตั้งระบบรักษาความปลอดภัยอย่างแน่นหนาดังกล่าวจะไม่เกิดประโยชน์ เพราะผู้โจมตีสามารถใช้ระบบเครือข่ายไร้สายเป็น back-door อย่างดีเพื่อบุกรุกระบบ

ดังนั้นจึงจำเป็นอย่างยิ่งที่ผู้ดูแลระบบจะต้องใช้มาตรการต่าง ๆ อย่างเหมาะสม เพื่อป้องกันการโจมตีให้กับระบบเครือข่ายไร้สาย หรืออย่างน้อยทำให้ผู้โจมตีไม่สามารถบุกรุกระบบเครือข่ายไร้สายได้โดยง่าย

การรักษาความปลอดภัยเป็นการเสริมสร้างความปลอดภัยให้กับระบบเครือข่ายไร้สาย ในขั้นต้นนั้นสามารถทำได้โดยการติดตั้งค่าการทำงานของอุปกรณ์ระบบเครือข่ายไร้สายอย่างเหมาะสม รวมถึงการใช้ Firewall, VPN (Virtual Private Network), และ IDS (Intruder Detection System) มาตรการรักษาความปลอดภัยในระดับเบื้องต้นดังที่จะกล่าวถึงในส่วนต่อไปนี้จะทำให้ระบบเครือข่ายไร้สายมีความปลอดภัยในระดับที่ยอมรับได้สำหรับการใช้งานตามบ้านเรือนหรือองค์กรที่ไม่ต้องการความปลอดภัยมากนัก

1. เปลี่ยน Login ID และรหัสผ่านของอุปกรณ์และหลีกเลี่ยงการใช้งาน SNMP สิ่งที่ผู้ดูแลระบบควรทำเป็นสิ่งแรกเมื่อติดตั้งอุปกรณ์ระบบเครือข่ายไร้สาย คือเปลี่ยน Login ID และรหัสผ่านสำหรับการตั้งค่าการทำงานของอุปกรณ์ดังกล่าว ผู้ดูแลระบบควรเลือกใช้ Login ID และรหัสผ่านที่มีความแข็งแรงสูงเพื่อให้ผู้โจมตีไม่สามารถเดาหรือเจาะรหัสได้โดยง่ายและควรมีการเปลี่ยน Login ID และรหัสผ่านอย่างสม่ำเสมอ นอกจากนี้ผู้ดูแลระบบไม่ควรอนุญาตให้มีการตั้งค่าการทำงานของอุปกรณ์ผ่านอินเทอร์เน็ตด้วย SNMP เพื่อป้องกันไม่ให้ผู้โจมตี (ซึ่งอาจทราบข้อมูลของ Login ID และรหัสผ่านจากการดักฟัง

หรือเจาะรหัส) สามารถอ่านหรือปรับเปลี่ยนค่าการทำงานของอุปกรณ์ผ่านเครือข่ายได้ มาตรการเหล่านี้เป็นสิ่งที่ผู้ดูแลระบบควรปฏิบัติในการติดตั้งอุปกรณ์ทุกชนิดมิใช่แต่เพียงอุปกรณ์ระบบเครือข่ายไร้สายเท่านั้น

2. การตั้งชื่อและปกปิด SSID ของอุปกรณ์แม่ข่าย Service Set Identifier (SSID) ทำหน้าที่เป็นชื่อเรียกของเครือข่ายระบบเครือข่ายไร้สายแต่ละเครือข่าย ซึ่งผู้ที่ประสงค์จะเข้ามาใช้เครือข่ายจะต้องรู้ชื่อหรือ SSID ของเครือข่ายจึงจะสามารถขอรับการตรวจสอบเพื่อใช้งานเครือข่ายนั้น ๆได้ โดยปกติแล้วอุปกรณ์แม่ข่ายจะส่งสัญญาณทุก ๆช่วงเวลาที่กำหนดไว้เพื่อให้ทุกอุปกรณ์ทราบถึง SSID ของเครือข่าย ซึ่งเป็นการอำนวยความสะดวกให้ผู้โจมตีรู้ SSID ของเครือข่ายได้โดยง่าย ดังนั้นผู้ดูแลระบบจึงควรที่จะหลีกเลี่ยงการเปิดเผยชื่อของเครือข่ายโดยปรับตั้งค่าอุปกรณ์แม่ข่ายให้ระงับใช้งานฟังก์ชัน "Broadcast SSID" แต่อย่างไรก็ตามผู้โจมตีก็ยังสามารถค้นหา SSID ของเครือข่ายโดยใช้วิธีอื่นหรือซอฟต์แวร์บางอย่างเช่น Windows XP ได้ แต่อย่างไรก็ตามการงดใช้ฟังก์ชัน Broadcast SSID ก็ยังดีกว่าการใช้งานฟังก์ชันดังกล่าว นอกจากนี้แล้วในการตั้งชื่อเครือข่ายผู้ดูแลระบบควรใช้ SSID ที่ไม่มีความเกี่ยวข้องใด ๆ กับเครือข่ายเพื่อผู้โจมตีจะได้ไม่สามารถคาดเดาหน้าที่หรือโครงสร้างของเครือข่ายจาก SSIDได้โดยง่ายและควรมีการเปลี่ยนชื่อ SSID อย่างสม่ำเสมอ

3. ปิดกั้นการทำงานในโหมด Adhoc หรือ Peer-to-Peer การใช้งานในโหมด Adhoc หรือ Peer-to-Peer ทำให้อุปกรณ์ระบบเครือข่ายไร้สายสามารถติดต่อสื่อสารถึงกันได้โดยไม่ต้องผ่านอุปกรณ์แม่ข่าย ในกรณีที่คอมพิวเตอร์ของผู้ใช้มีการติดตั้งอุปกรณ์ระบบเครือข่ายไร้สาย และอนุญาตให้มีการใช้งานในโหมดดังกล่าว ผู้โจมตีซึ่งอยู่ในบริเวณใกล้เคียงภายในระยะของคลื่นสัญญาณวิทยุอาจจะสามารถเชื่อมต่อเข้ากับคอมพิวเตอร์ของผู้ใช้นั้นได้โดยตรง ซึ่งผู้โจมตีอาจสามารถใช้ประโยชน์จากช่องโหว่ของซอฟต์แวร์ต่าง ๆเพื่อบุกรุกระบบได้ต่อไป ซึ่งผู้บุกรุกอาจสามารถเข้าถึง ดัดแปลงหรือทำลายไฟล์และข้อมูลความลับ สร้าง backdoor เรียกใช้งานโค้ดต่าง ๆ หรือกระทำการอื่น ๆได้ตามประสงค์บนระบบ ทางที่ดีควรจะมีการปิดกั้นไม่ให้อุปกรณ์ระบบเครือข่ายไร้สายบนระบบภายใต้ความดูแลของท่านทำงานในโหมด Peer-to-Peer เพื่อป้องกันการโจมตีโดยตรงดังกล่าวจากผู้ไม่ประสงค์ดี ซึ่งการปิดกั้นการทำงานในโหมด Peer-to-Peer ไม่ส่งผลกระทบต่อการใช้งานของผู้ใช้ทั่วไปเนื่องจาก โดยปกติแล้วอุปกรณ์ระบบเครือข่ายไร้สายจะถูกติดตั้งให้ใช้งานในโหมด Infrastructure เพื่ออนุญาตให้ผู้ใช้สามารถเชื่อมต่อเข้ากับอินเตอร์เน็ตได้ ดังนั้นผู้ดูแลระบบไม่ควรจะอนุญาตให้อุปกรณ์ระบบเครือข่ายไร้สายทำงานในโหมด Peer-to-Peer หากไม่มีความจำเป็นจริง ๆ

4. ใช้งาน WEP Encryption ผู้ดูแลระบบควรเลือกใช้กลไกการเข้ารหัสของ WEP ในระบบเครือข่ายไร้สาย หากไม่มีกลไกสำหรับเข้ารหัสข้อมูลอื่น ๆที่ปลอดภัยกว่าให้เลือกใช้ ถึงแม้ว่ากลไกการเข้ารหัสของ WEP จะมีช่องโหว่ก็ตามแต่ก็สามารถสร้างความปลอดภัยในกับเครือข่ายได้ในระดับ หนึ่ง เนื่องจากซอฟต์แวร์ Airsnort หรือ WEPCrack สำหรับเจาะรหัสลับในระบบเครือข่ายไร้สาย ซึ่งถูกพัฒนาบนระบบปฏิบัติการ Linux มีการติดตั้งที่ค่อนข้างยุ่งยากโดยเฉพาะอย่างยิ่งสำหรับผู้ไม่มีความชำนาญ กับระบบ

ปฏิบัติการ Linux ดังนั้นกลไกการเข้ารหัสของ WEP จึงสามารถกีดกันผู้โจมตี (สมัครเล่น) จำนวนหนึ่งซึ่งไม่สามารถติดตั้งซอฟต์แวร์ดังกล่าวได้ นอกจากนี้ในการเจาะรหัสลับจะต้องมีการรวบรวมข้อมูลจากเครือข่ายจำนวนมากซึ่ง ต้องใช้เวลานานหลายชั่วโมงซึ่งผู้โจมตีที่ไม่มีความมุ่งมั่นเพียงพออาจจะไม่ พยายามที่เจาะรหัสลับของเครือข่ายที่มีการใช้กลไกการเข้ารหัสของ WEP นั่นหมายความว่าการเลือกใช้กลไกเข้ารหัสของ WEP จะช่วยทำให้ระบบเครือข่ายไร้สายเป็นเป้าหมายการโจมตีที่ยากขึ้น ซึ่งผู้โจมตีทั่วไปอาจเลี่ยงไปบุกรุกเป้าหมายอื่นที่ง่ายกว่าแทน พูดง่าย ๆก็คือเลือกใช้กลไกเข้ารหัสของ WEP ก็ยังดีกว่าไม่ใช้การเข้ารหัสอะไรเลย

5. ควบคุม MAC Address ของผู้ใช้ วิธีหนึ่งที่อาจป้องกันไม่ให้ผู้โจมตีสามารถเข้าใช้ระบบเครือข่ายไร้สาย ได้คือการควบคุม MAC Address ของอุปกรณ์ระบบเครือข่ายไร้สายที่มีสิทธิในการใช้เครือข่ายได้ โดยอนุญาตเฉพาะอุปกรณ์ที่มี MAC Address ดังที่กำหนดไว้เท่านั้นให้ใช้เครือข่ายได้อย่างถูกต้อง ซึ่งโดยปกติแล้วอุปกรณ์ศูนย์กลางควบคุม หรือ Access Point ที่ใช้งานกันอยู่ทั่วไปจะมีฟังก์ชันดังกล่าวติดตั้งไว้ให้เลือกใช้ได้ด้วย แต่ปัญหาอย่างหนึ่งสำหรับการควบคุมผู้ใช้ด้วยวิธีนี้ก็คือต้องมีการจัดการ และบริหารรายชื่อดังกล่าวซึ่งอาจสร้างความไม่สะดวกโดยเฉพาะอย่างยิ่งสำหรับ เครือข่ายที่มีผู้ใช้จำนวนมาก ๆ ยิ่งไปกว่านั้นวิธีการป้องกันผู้โจมตีแบบนี้มีช่องโหว่เนื่องจากผู้โจมตี สามารถปลอมแปลง MAC Address ของตนเพื่อให้อยู่ในรายชื่อได้ (หรือที่เรียกกันว่า MAC Address spoofing) ผู้โจมตีอาจทราบรายชื่อของ MAC Address ที่ได้รับอนุญาตได้โดยการดักฟัง packet ในเครือข่าย ซึ่งผู้โจมตีสามารถทราบข้อมูลดังกล่าวได้ถึงแม้จะมีการเข้ารหัสข้อความก็ตาม แต่ MAC Header จะไม่ถูกเข้ารหัส แต่อย่างไรก็ตามถ้าการจัดการและบริหารรายชื่อ MAC Address เป็นไปได้ไม่ยากนักและไม่มีมาตรการป้องกันผู้โจมตีที่ดีกว่านี้ ผู้ดูแลระบบควรเลือกใช้วิธีการควบคุม MAC Address ของผู้ใช้ ถึงแม้ว่าวิธีดังกล่าวจะมีช่องโหว่ก็ตามแต่ก็สามารถสร้างความไม่สะดวกให้กับ ผู้โจมตีได้บางส่วน (เล็ก ๆน้อย ๆก็ยังดีกว่าไม่มีการป้องกันไว้เลย) ดังนั้นระบบเครือข่ายไร้สายที่มีจำนวนผู้ใช้จำนวนไม่มาก เช่น ในหน่วยงานเล็กที่มีการเชื่อมต่อระบบเครือข่ายไร้สายไม่เกิน 40-50 เครื่อง ควรมีการเลือกใช้มาตรการรักษาความปลอดภัยดังกล่าว

6. หลีกเลี่ยงการใช้ DHCP การใช้ DHCP เป็นกลไก เพื่อกำหนด IP Address ของอุปกรณ์คอมพิวเตอร์โดยอัตโนมัติ ก่อให้เกิดความสะดวกต่อผู้ใช้มากในการเชื่อมต่อเข้ากับอินเทอร์เน็ต แต่ในขณะเดียวกันการใช้ DHCP ก็ทำให้ผู้โจมตีที่บุกรุกระบบเครือข่ายไร้สาย ได้แล้วสามารถเชื่อมต่อเข้ากับอินเทอร์เน็ตได้โดยสะดวกเช่นเดียวกัน ดังนั้นผู้ดูแลระบบควรหลีกเลี่ยงการใช้ DHCP ซึ่งจะทำให้ผู้โจมตีต้องใช้ความพยายามสูงขึ้นอีกในการเชื่อมต่อเข้ากับเครือข่ายอินเทอร์เน็ต

7. หลีกเลี่ยงการใช้ Shared-Key Authentication ผู้ดูแลระบบควรหลีกเลี่ยงการใช้กลไกการตรวจสอบผู้ใช้แบบ Shared-Key Authentication ของ WEP เนื่องจากกลไกดังกล่าวถูกเจาะได้ง่าย และสามารถทำให้ผู้โจมตีล่วงรู้ key stream เพื่อนำไปใช้เข้ารหัส หรือสามารถถอดรหัสลับในระบบเครือข่ายไร้สายได้ในที่สุด ดังนั้นหากเป็นไปได้ผู้ดูแลระบบควรหลีกเลี่ยงการใช้กลไกดังกล่าว และอาจติดตั้งอุปกรณ์หรือซอฟต์แวร์เพิ่มเติมเช่น ระบบ RADIUS เพื่อช่วยทำหน้าที่ตรวจสอบผู้ใช้ให้มีความปลอดภัยมากขึ้น

8. ควบคุมการแพร่กระจายของสัญญาณ ผู้ดูแลระบบควรพยายามควบคุมไม่ให้สัญญาณของอุปกรณ์ระบบเครือข่ายไร้สายรั่วไหลออกไปนอกบริเวณที่ใช้งาน เพื่อป้องกันไม่ให้ผู้โจมตีสามารถรับส่งสัญญาณจากภายนอกอาคารหรือบริเวณขอบเขตที่ควบคุมได้ การวางตำแหน่งและกำหนดกำลังส่งของอุปกรณ์อย่างเหมาะสมจะสามารถช่วยลดการรั่วไหลของสัญญาณออกไปภายนอกได้ โดยทั่วไปแล้วผู้ดูแลระบบไม่ควรติดตั้ง Access Point ไว้ติดกับพื้น, เพดาน, หรือผนังตึก ควรติดตั้งไว้กลางบริเวณที่ใช้งานเพื่อลดการรั่วไหลของสัญญาณ อุปกรณ์ระบบเครือข่ายไร้สายบางยี่ห้ออนุญาตผู้ใช้สามารถปรับตั้งกำลังในการส่งสัญญาณได้ด้วย ซึ่งในกรณีดังกล่าวผู้ดูแลระบบควรเลือกใช้กำลังส่งให้เหมาะสมกับพื้นที่ใช้งานและควรสำรวจว่าสัญญาณรั่วไหลออกไปภายนอกหรือไม่ นอกจากนี้การใช้เสาอากาศพิเศษที่สามารถกำหนดทิศทางการแพร่กระจายของสัญญาณอาจช่วยลดการรั่วไหลของสัญญาณได้ดีขึ้นด้วย

9. ระงับความสามารถในการเชื่อมต่อกับระบบเครือข่ายไร้สายแบบอัตโนมัติ หรือ Plug-n-Play ระบบปฏิบัติการบางระบบ เช่น Microsoft Windows XP กำหนดให้เครื่องคอมพิวเตอร์ไร้สายมีความสามารถที่เชื่อมต่อเข้ากับ Access Point หรือเครื่องคอมพิวเตอร์ไร้สายอื่นได้โดยอัตโนมัติ ซึ่งผู้ใช้อาจไม่ตระหนักถึงว่าเครื่องคอมพิวเตอร์ไร้สายของตนได้รับการเชื่อมต่อเข้ากับ Access Point หรือเครื่องคอมพิวเตอร์ไร้สาย ทำให้ผู้ใช้สามารถถูกโจมตีแบบ Man-in-Middle ได้โดยง่าย ดังนั้นผู้ดูแลระบบควรระงับความสามารถในการเชื่อมต่อเข้ากับระบบเครือข่ายไร้สายแบบอัตโนมัติดังกล่าว และทางที่ดีควรจะมีการ Prompt ถามผู้ใช้ทุกครั้งเมื่อจะเริ่มการเชื่อมต่อเข้ากับอุปกรณ์ระบบเครือข่ายไร้สาย

10. ติดตั้ง Firewall ที่ระบบเครือข่ายไร้สาย และใช้ VPN (Virtual Private Network) เนื่องจากระบบเครือข่ายไร้สายมีโอกาสที่จะถูกบุกรุก และครอบครองได้ง่าย หากไม่มีการรักษาความปลอดภัยที่เหมาะสม ระบบเครือข่ายไร้สายอาจถูกใช้ประโยชน์เป็น back door ได้อย่างดี เพื่อทำการโจมตีระบบภายในอื่น ๆ ได้ต่อไป ดังนั้นระบบเครือข่ายไร้สายควรจะถูกแยกออกจากระบบเครือข่ายภายในส่วนอื่น ๆ ซึ่งการแยกระบบเครือข่ายไร้สายออกจากระบบเครือข่ายภายในอื่น ๆ จะช่วยป้องกันไม่ให้ผู้โจมตีที่บุกรุกและต้องการครอบครองระบบเครือข่ายไร้สายได้แล้ว สามารถบุกรุกต่อไปยังระบบเครือข่ายภายในอื่นได้โดยง่าย นั่นคือควรจะมีการติดตั้ง Firewall ระหว่างระบบเครือข่ายไร้สายกับระบบเครือข่ายภายใน หรือใช้วิธีติดตั้งระบบเครือข่ายไร้สายไว้ในเขต De-Militarized Zone (DMZ) ก็ได้ อย่างไรก็ตามมาตรการนี้ไม่ได้เป็นการป้องกันการโจมตีระบบเครือข่ายไร้สาย เพียงแต่ช่วยป้องกันไม่ให้ระบบเครือข่ายไร้สายถูกใช้เป็น back door สำหรับโจมตีระบบภายในองค์กรส่วนอื่น ๆ ได้ในระดับหนึ่ง แต่อย่างไรก็ตามผู้โจมตียังคงสามารถดักฟังข้อมูลที่รับส่งอยู่ในระบบเครือข่ายไร้สาย ซึ่งอาจทำให้ผู้โจมตีล่วงรู้ username และ password เพื่อเข้าถึงระบบเครือข่ายภายในได้ เพื่อจะแก้ไขปัญหาดังกล่าวควรจะนำ VPN (Virtual Private Network) ซึ่งเป็นเทคนิคที่ได้รับการยอมรับ และใช้กันอย่างแพร่หลายทั่วไปมาใช้กับระบบเครือข่ายไร้สายด้วย เพื่อสร้างความปลอดภัยอีกชั้นหนึ่ง ในกรณีนี้ระบบเครือข่ายไร้สายจะถูกพิจารณาเสมือนเป็นเครือข่ายอินเทอร์เน็ตซึ่งไม่ได้รับการไว้ใจ จึงมีการสร้าง VPN Tunnel ขึ้นมาในบนระบบเครือข่ายไร้สาย เพื่อใช้ในการรับส่งข้อมูลได้อย่างปลอดภัย นอกจากนี้ควรมีมาตรการเพื่อไม่อนุญาตให้ผู้ใช้ในระบบเครือข่ายไร้สาย

ติดต่อสื่อสารโดยไม่ต้องผ่าน VPN เช่น กำหนดให้ผู้ใช้ในระบบเครือข่ายไร้สายติดต่อสื่อสารได้เฉพาะกับ VPN Concentrator เท่านั้น ทั้งนี้ก็เพื่อป้องกันไม่ให้ผู้โจมตีสามารถบุกรุกระบบเครือข่ายไร้สายได้ การติดตั้ง VPN บนระบบเครือข่ายไร้สายอย่างถูกต้องจะช่วยป้องกันการโจมตีได้มาก แต่ข้อเสียจากการใช้ VPN คือสมรรถนะของระบบเครือข่ายไร้สายจะลดลง เนื่องจากต้องมี overhead เพิ่มขึ้นมากซึ่งความเร็วของการรับส่งข้อมูลอาจลดลงเกินกว่าครึ่งก็เป็นได้

11. ใช้ IDS (Intruder Detection System) และ Auditor เช่นเดียวกับในระบบเครือข่ายแบบใช้สายสัญญาณทั่วไปที่ควรจะมีการติดตั้งซอฟต์แวร์ IDS (Intruder Dectection System) ไว้เพื่อคอยตรวจสอบและบันทึกว่ามีกิจกรรมใดที่น่าสงสัยเกิดขึ้นในระบบเครือข่ายหรือไม่ ในระบบเครือข่ายไร้สายจึงควรจะมีการติดตั้งซอฟต์แวร์หรือฮาร์ดแวร์ IDS สำหรับตรวจสอบและบันทึกกิจกรรมที่น่าสงสัยในระบบเครือข่ายไร้สายไว้ด้วย นอกจากนี้ผู้ดูแลระบบควรตรวจตราความปลอดภัยของระบบเครือข่ายไร้สาย โดยใช้ซอฟต์แวร์หรือฮาร์ดแวร์สำหรับ Audit ระบบเครือข่ายไร้สายอย่างสม่ำเสมอ ในปัจจุบันมีซอฟต์แวร์และฮาร์ดแวร์ IDS และ Audit สำหรับระบบเครือข่ายไร้สายจากผู้ผลิตหลายราย เช่น AiroPeek โดย WildPackets, Internet Scanner & RealSecure โดย ISS, AirMagnet, และ NetStumbler เป็นต้น

สำหรับองค์กรที่มีการติดตั้งระบบเครือข่ายไร้สาย และต้องการความปลอดภัยสูง ควรเพิ่มการรักษาความปลอดภัยดังต่อไปนี้

12. มาตรฐาน IEEE 802.1x และ RADIUS องค์กรที่มีการติดตั้งระบบเครือข่ายไร้สายและต้องการความ และบริหารให้ key ในการเข้ารหัสข้อมูลของแต่ละผู้ใช้มีค่าไม่ซ้ำกันและเปลี่ยนแปลงอย่างสม่ำเสมอด้วย ในกรณีนี้องค์กรควรเลือกติดตั้งอุปกรณ์ระบบเครือข่ายไร้สายที่มีความสามารถเพิ่มเติมในการรองรับการทำงานของมาตรฐาน IEEE 802.1x และการทำงานร่วมกับ RADIUS (Remote Authentication Dial-In User Service) เซิร์ฟเวอร์ เช่น Access Point ของ Cisco เป็นต้น มาตรฐาน IEEE 802.1x เป็นมาตรฐานใหม่สำหรับ MAC Layer ที่ช่วยเสริมให้การตรวจสอบผู้ใช้ (Authentication) ในระบบเครือข่ายแบบมีสายสัญญาณและไร้สายมีความปลอดภัยสูงขึ้น ในกรณีนี้เมื่อผู้ใช้ต้องการเข้าใช้ระบบเครือข่ายไร้สาย จะต้องมีการแสดงหลักฐานสำหรับประกอบการตรวจสอบ (credential) ต่อ Access Point หลังจากนั้น Access Point จะส่งผ่านหลักฐานดังกล่าวต่อไปยัง RADIUS เซิร์ฟเวอร์ ซึ่งเป็นระบบสำหรับตรวจสอบผู้ใช้โดยเฉพาะที่ใช้กันอยู่ทั่วไป โดยการแลกเปลี่ยนข้อมูลกันระหว่าง RADIUS เซิร์ฟเวอร์กับ Access Point จะเป็นไปตามโพรโตคอลที่เรียกว่า EAP (Extensible Authentication Protocol) ซึ่งมีความยืดหยุ่นสูง ทำให้ผู้พัฒนาระบบสามารถนำไปใช้สร้างกลไกการตรวจสอบอย่างที่ต้องการได้ ในปัจจุบันมีการใช้โพรโตคอลดังกล่าวใน 4 รูปแบบหลัก ๆ คือ EAP-MD5, LEAP, EAP-TLS, และ EAP-TTLS

EAP-MD5 ในกรณีนี้หลักฐานที่ส่งผ่านไปยัง RADIUS เซิร์ฟเวอร์ คือ username และ password ซึ่งจะถูกเข้ารหัสด้วยเทคนิคที่เรียกว่า MD5 การใช้กลไก EAP-MD5 ช่วยแก้ไขปัญหาเรื่องการตรวจสอบผู้ใช้ในระบบเครือข่ายไร้สายให้มีความปลอดภัยมากขึ้น แต่ไม่ได้ช่วยแก้ไขปัญหาเรื่องความไม่ปลอดภัยของการใช้รหัสลับเครือข่าย (WEP Key) ซึ่งมีความคงที่ (static) ดังนั้นผู้โจมตียังคงสามารถ

ดักฟังและเจาะรหัสลับของเครือข่ายซึ่งมีความคงที่ได้ถึงแม้จะมีการใช้ EAP-MD5 เมื่อผู้โจมตีทราบรหัสลับของเครือข่ายแล้วก็จะสามารถเข้าใจข้อมูลที่รับส่งอยู่ในเครือข่ายและอาจทราบ username และ password โดยอาศัยเทคนิคต่าง ๆสำหรับการเจาะรหัส MD5 ได้ในที่สุดนอกจากนี้ข้อบกพร่องในกลไก EAP-MD5 อีกอย่างหนึ่งคือผู้ใช้ไม่สามารถตรวจสอบ Access Point ซึ่งทำให้ผู้โจมตีอาจจะสามารถหลอกลวงให้ผู้ใช้ต่อเชื่อมเข้ากับ Access Point ของผู้โจมตีได้

LEAP หรือ EAP-Cisco Wireless โพรโตคอล LEAP (Lightweight Extensible Authentication Protocol) ได้รับการพัฒนาขึ้นโดยบริษัท Cisco ซึ่งในโพรโตคอลนี้นอกจากจะมีกลไกในการส่งผ่านข้อมูลเกี่ยวกับ username และ password ของผู้ใช้ไปยัง RADIUS เซิร์ฟเวอร์ เพื่อทำการตรวจสอบแล้ว ยังมีการจัดการและบริหารรหัสลับของเครือข่าย (WEP Key) ให้มีการเปลี่ยนแปลงค่า นั่นคือเมื่อผู้ใช้ผ่านการตรวจสอบเรียบร้อยแล้วจะได้รับ WEP Key เพื่อใช้ในการเข้ารหัสข้อมูลสำหรับผู้ใช้นั้น ๆ ซึ่งหมายความว่า WEP Key ของแต่ละผู้ใช้สามารถมีความแตกต่างกันออกไปได้ และเมื่อใช้งานร่วมกับ RADIUS ซึ่งสามารถกำหนดอายุของแต่ละ sessionได้ จะทำให้ WEP Key ของแต่ละผู้ใช้เปลี่ยนค่าไปทุก ๆช่วงเวลาสั้น ๆด้วย ในกรณีเทคนิคการเจาะรหัสลับเครือข่าย (WEP Key) ที่มีอยู่ในปัจจุบันจะไม่สามารถนำมาใช้ประโยชน์ได้ นอกจากนี้ LEAP ยังกำหนดให้มีการตรวจสอบทั้งเครื่องแม่ข่ายและผู้ใช้ (Mutual Authentication) เพื่อป้องกันไม่ให้ผู้โจมตีสามารถหลอกลวงผู้ใช้ให้เชื่อมต่อกับเครื่องแม่ข่ายของผู้โจมตีได้ จะเห็นได้ว่า LEAP สามารถเพิ่มความปลอดภัยให้กับเครือข่าย WLAN ได้มาก แต่อย่างไรก็ตามข้อเสียอย่างหนึ่งก็คือในปัจจุบัน LEAP ยังถูกจำกัดอยู่แต่ในผลิตภัณฑ์ของ Cisco เท่านั้น

EAP-TLS โพรโตคอล EAP-TLS (Transport Layer Security) ได้รับการพัฒนาขึ้นโดยบริษัท Microsoft ซึ่งมีการอ้างอิงไว้ใน RFC 2716 <http://www.ietf.org/rfc/rfc2716.txt> ในโพรโตคอลนี้จะไม่มีการใช้ username และ password ในการตรวจสอบผู้ใช้ แต่จะใช้ X.509 certificates <http://verisign.netscape.com/security/pki/understanding.html> แทน การทำงานของโพรโตคอลนี้จะอาศัยการส่งผ่าน PKI ผ่าน SSL (Secure Sockets Layers) มายัง EAP เพื่อใช้กำหนด WEP Key สำหรับผู้ใช้แต่ละคน EAP-TLS กำหนดให้มีการตรวจสอบทั้งเครื่องแม่ข่ายและผู้ใช้ (Mutual Authentication) ด้วยเช่นเดียวกับ LEAP แต่อย่างไรก็ตามปัญหาหลักของ EAP-TLS ความยุ่งยากและค่าใช้จ่ายในการติดตั้งจัดการและบริหารระบบ PKI Certificate

EAP-TTLS โพรโตคอล EAP-TTLS ถูกเริ่มพัฒนาโดยบริษัท Funk Software ซึ่งการทำงานของ EAP-TTLS คล้ายกับ EAP-TLS คือจะมีการตรวจสอบเครื่องแม่ข่ายโดยใช้ Certificate แต่ผู้ใช้จะถูกตรวจสอบโดยการใช้ username และ password ซึ่งความปลอดภัยของ EAP-TTLS จะน้อยกว่า EAP-TLS และที่สำคัญ EAP-TTLS อาจไม่ได้รับความนิยมมากนักในเวลาต่อไปเนื่องจาก Microsoft และ Cisco ได้ร่วมมือกันพัฒนาโพรโตคอลขึ้นมาใหม่ชื่อว่า PEAP (Protected EAP) ซึ่งมีการทำงานเช่นเดียวกับ EAP-TLS

การติดตั้งระบบเครือข่ายไร้สายที่มีความปลอดภัยสูงโดยใช้มาตรฐาน IEEE 802.1x จะต้องมีองค์ประกอบ 3 ส่วนด้วยกัน คือ

1. IEEE 802.1x Enabled AP ส่วนใหญ่แล้ว Access Point ที่ผลิตมาจำหน่ายในท้องตลาดจะมีความสามารถในการส่งผ่านข้อมูลไปยัง RADIUS ด้วย IEEE 802.1x ได้อยู่แล้ว หรือไม่ก็สามารถที่จะได้รับการปรับเปลี่ยน Firmware เพื่อให้ใช้งานตามมาตรฐาน IEEE 802.1x ได้ ส่วนอุปกรณ์ระบบเครือข่ายไร้สายที่ผลิตมาจำหน่ายในท้องตลาดทั่วไปซึ่งจะมีราคาต่ำกว่า จะไม่สามารถนำไปใช้งานร่วมกับ IEEE 802.1x ได้ แต่อย่างไรก็ตามผู้ติดตั้งระบบสามารถดัดแปลงอุปกรณ์เหล่านั้นเพื่อให้สามารถทำงานร่วมกับ IEEE 802.1x ได้โดยเทคนิคที่เรียกว่า "Hacking an Orinoco RG-1100 to accept 802.1x"

2. RADIUS Server ที่สามารถทำงานร่วมกับ EAP ที่ต้องการได้ อาทิเช่น

- Microsoft Internet Authentication Service (IAS) ซึ่งเป็นองค์ประกอบหนึ่งของระบบ Windows 2000 มีความสามารถทำงานร่วมกับ EAP-TLS และ EAP-MD5 ได้ และติดตั้งโดยอาศัยฟังก์ชัน Add/Remove Program ใน Control Panel ของระบบ Windows 2000

- Access Control Software ของ Cisco ซึ่งสามารถทำงานร่วมกับ LEAP และ EAP-TLS บนระบบปฏิบัติการ Windows หรือ UNIX/Linux ได้

-ซอฟต์แวร์ Steel Belted RADIUS หรือ Odyssey โดยบริษัท Funk Software ซึ่งสามารถใช้งานกับ EAP-MD5, EAP-TLS, LEAP, และ EAP-TTLS ได้

-ซอฟต์แวร์ AEGIS โดยบริษัท Meetinghouse Data ซึ่งสามารถใช้งานกับ EAP-TLS และ EAP-TTLS บนระบบปฏิบัติการ Linux ได้

-ซอฟต์แวร์ FreeRadius ซึ่งเป็นโปรแกรมโอเพนซอร์สสำหรับระบบ Linux ซอฟต์แวร์นี้สามารถทำงานร่วมกับ EAP-MD5 และ EAP-TLS

ซอฟต์แวร์สำหรับ Client ซึ่งสามารถทำงานร่วมกับ RADIUS และ IEEE 801.1x เช่น

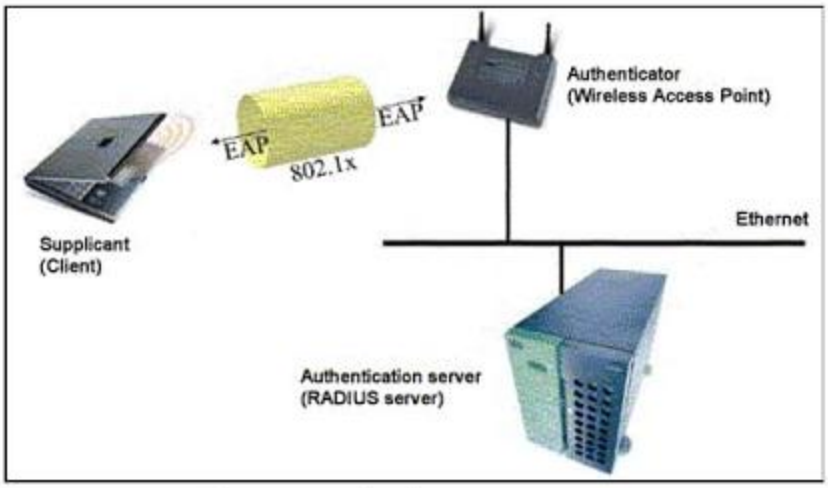
-ซอฟต์แวร์ ACU สำหรับอุปกรณ์ IEEE 802.11 WLAN ของ Cisco ซึ่งสามารถใช้งานกับ LEAP ได้บนระบบปฏิบัติการ Windows, Apple, และ Linux

-Windows XP มีซอฟต์แวร์ที่มากับระบบเพื่อทำให้อุปกรณ์ระบบเครือข่ายไร้สายสามารถใช้งานกับ EAP-TLS และ EAP-MD5 ได้ แต่ต้องมีการใช้ Certificate ที่ออกโดย Microsoft อย่างถูกต้อง

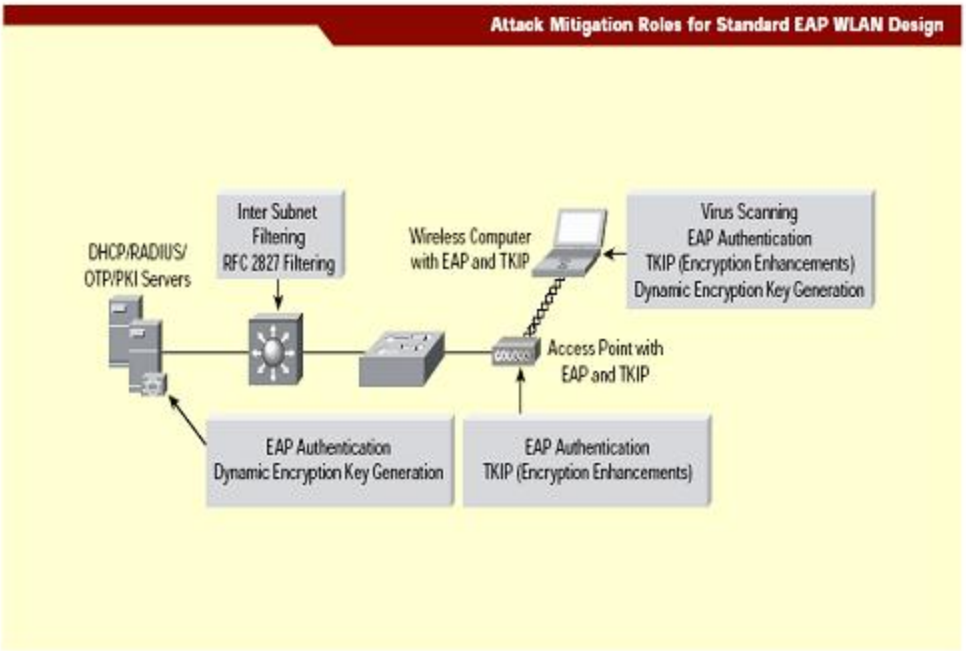
-ซอฟต์แวร์ Odyssey Client โดย Funk Software ซึ่งทำให้อุปกรณ์ระบบเครือข่ายไร้สาย Client ทุกยี่ห้อที่ support โพรโตคอล IEEE 802.1x สามารถใช้งานกับ EAP-MD5, EAP-TLS, EAP-TTLS, และ LEAP ได้บนระบบปฏิบัติการ Windows และ Linux

-ซอฟต์แวร์ AEGIS Client ซึ่งสามารถใช้งานกับ EAP-MD5, EAP-TLS, และ EAP-TTLS บนระบบปฏิบัติการ Windows และ Linux

-ซอฟต์แวร์สำหรับ Client แบบโอเพนซอร์สบนระบบ Linux ซึ่งกำลังถูกพัฒนาอยู่ในขณะนี้ เช่น Xsupplicant และ open1X เป็นต้น



ภาพที่ 5 แสดงการเชื่อมต่อตามมาตรฐาน IEEE 802.1x



ภาพที่ 6. แสดงการออกแบบระบบเครือข่ายไร้สายตามมาตรฐาน IEEE 802.1x

เอกสารอ้างอิง

วรินทร์ เมฆประดิษฐสิน. 2547. **คัมภีร์ระบบเครือข่ายแบบฉบับอาจารย์วรินทร์ เล่ม 1**, กรุงเทพฯ : ซีเอ็ดยูเคชั่น.

ศิวรักษ์ ศิวโมกษธรรม. 2546. **มาตรฐาน IEEE 802.11 WLAN : ความรู้เบื้องต้น ช่องโหว่ และการรักษาความปลอดภัย (ตอนที่ 1)**, กรุงเทพ : ศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์ ประเทศไทย ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ.

---------. 2546. **มาตรฐาน IEEE 802.11 WLAN: ความรู้เบื้องต้น ช่องโหว่ และการรักษาความปลอดภัย (ตอนที่ 2)**, กรุงเทพ:ศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์ ประเทศไทย ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ.

---------. 2546. **มาตรฐาน IEEE 802.11 WLAN: ความรู้เบื้องต้น ช่องโหว่ และการรักษาความปลอดภัย (ตอนที่ 3)**, กรุงเทพ : ศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์ ประเทศไทย, ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ.

---------. 2546. **มาตรฐาน IEEE 802.11 WLAN : ความรู้เบื้องต้น ช่องโหว่ และการรักษาความปลอดภัย (ตอนที่ 4)**. กรุงเทพ : ศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์ ประเทศไทย ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ.

อนันต์ ผลเพิ่ม. 2547. **Wireless LAN Implememtaion Demo and Workshop,** กรุงเทพ : สำนักบริการคอมพิวเตอร์ มหาวิทยาลัยเกษตรศาสตร์บางเขน.

Institute of Electrical and Electronic Engineer. 2005. **The Working Group for WLAN Standards IEEE 802.11TM WIRELESS LOCAL AREA NETWORKS.** (Online) Available: http://grouper.ieee.org/groups/802/11 [2005-09-25]

Institute of Electrical and Electronic Engineer. 2001. **IEEE 802.11b High Rate Wireless Local Area Network.** (Online) Available: http://alpha.fdu.edu/~kanoksri/IEEE80211b.html [2005-09-25]

Internet Security Systems Technical White Paper, Wireless LAN security 802.11b and Corporate Networks.(Online) Available: http://documents.iss.net/whitepapers/wireless_LAN_security.pdf [2005-09-25]