COVER STORY

ปกป้องเครือข่ายไร้สาย ให้พ้นจากภัยคุกคาม

ซิสโก้อุดช่องโหว่ความปลอดภัยที่มีอยู่ในมาตรฐาน 802.11 ได้สำเร็จแล้ว

เครือข่าย LAN ไร้สาย (WLAN-Wireless LAN) ของคุณมั่นคงปลอดภัยดีหรือไม่?

WLAN กำลังได้รับความนิยมเพิ่มขึ้น เนื่องจากการติดตั้งง่าย และให้การเข้าถึงทรัพยากรขององค์กรได้ทุกหนแห่งภายในอาณาเขตขององค์กรนั้น แต่คุณเชื่อหรือไม่ว่ามีองค์กรจำนวนมากที่ไม่ใส่ใจจะใช้ฟีเจอร์รักษาความปลอดภัยแบบไร้สายเลย หนังสือพิมพ์ The Wall Street Journal ฉบับวันที่ 27 เมษายน 2544 มีการกล่าวถึงแฮ็กเกอร์สองคนที่มีแลปทอปกับสายอากาศขับรถวนไปทั่งซิลิคอนแวลลีย์ เพื่อดักจับคลื่นข้อมูลที่รับส่งกันเครือข่ายแล้วเครือข่ายเล่า ผู้ที่ตกเป็นเหยื่อส่วนมากเป็นบริษัทที่ไม่ได้มีรายชื่ออยู่ใน Fortune 500 ตามคำบอกเล่าของแฮ็กเกอร์ดังกล่าว

David Halasz ผู้จัดการฝ่ายพัฒนาซอฟต์แวร์ของ Wireless Networking Business Unit ที่ซิสโก้ และประธานของ IEEE 802.11 Secutirity Task Group กล่าวว่า "องค์กรต้องตระหนักถึงภัยที่เกิดจากการใช้เทคโนโลยีไร้สายเสียแต่วันนี้ ถึงแม้คุณอาจอยู่ภายนอกตัวอาคารหรืออยู่ใกล้บ้านของพนักงานก็สามารถเข้าไปมีส่วนร่วมในเครือข่ายวงนั้นได้ ฉะนั้น การเสริมความแข็งแกร่งของระบบความปลอดภัยในเครือข่ายไร้สาย จึงจำเป็นสำหรับองค์กรอย่างยิ่ง"

อย่างไรก็ตาม แม้ว่าองค์กรจะกระตุ้นระบบรักษาความปลอดภัยของ WLAN ให้ทำงานบนมาตรฐาน 802.11 แล้ว แต่ก็มิได้หมายความว่าคลื่นที่ส่งไปในอากาศจะปลอดภัย ตามรายงานของทีมวิจัยที่มหาวิทยาลัยแคลิฟอร์เนีย เบิร์กเลย์ รายงานนี้เผยให้เห็นช่องโหว่ความปลอดภัยของมาตรฐาน Wired Equivalent Privacy (WEP) แบบสถิต ซึ่งก่อให้เกิดคำถามตามมาว่า เหตุใดจึงมีการยอมรับ WEP แบบสถิตมาใช้เลยทันที "ถ้า WEP ถูกตรวจสอบโดยองค์กรที่ทำงานด้านการเข้ารหัสลับ ก่อนที่จะเปิดตัวเป็นมาตรฐานสากลแล้ว ข้อบกพร่องจำนวนมากก็คงไม่เกิดขึ้นแน่นอน"

จริงๆ ความเชื่อที่กำลังแผ่กระจายในประชาคมผู้ใช้เครือข่ายอยู่ก็คือหนทางเดียวที่จะคุ้มครอง WLAN ได้คือการเรียกใช้เทคโนโลยีเครือข่ายส่วนบุคคลเสมือน (VPN) โดยยอมเสียค่าใช้จ่ายและใช้การจัดการเพิ่ม รายงานของเบิร์กเลย์แถลงว่า "ในตลาดไม่มีระบบที่เรารู้จักใดๆ เลยที่มีกลไกสนับสนุนเทคนิคเช่นนั้น" ซึ่งสามารถป้องกันการโจมตีผ่านการเชื่อมต่อไร้สายอย่างมีประสิทธิภาพเพียงพอ

ซิสโก้ยอมรับว่าในมาตรฐาน 802.11 WEP แบบสถิตมีจุดบกพร่องตามที่อ้างไว้ในรายงานของเบิร์กเลย์จริง แต่โชคไม่ดีที่บรรดานักวิจัยของเบิร์กเลย์ ดูเหมือนจะไม่ทราบว่าในตลาดยังมีโซลูชันระบบเครือข่ายไร้สาย Cisco Aironet เหลืออยู่อีกตัวหนึ่ง โดยการใช้ระบบความปลอดภัยบนมาตรฐานฉบับร่าง IEEE 802.1x สำหรับโครงกรอบ 802.11 ระบบความปลอดภัยของ Cisco Aironet จะให้การทำงานของ WEP แบบไดนามิก (ขึ้นกับผู้ใช้ ขึ้นกับเซสชัน) ที่ช่วยบรรเทาความกังวลที่บ่งชี้ภายในรายงานฯ และเพิ่มพูนความแข็งแกร่งโดยรวมของการเข้ารหัสตามมาตรฐาน 802.11 WEP

ฟีเจอร์ความปลอดภัยเหล่านี้ประกอบด้วย การรับรองยืนยันซึ่งกันและกัน (Mutual Authentication) การใช้กุญแจรักษาความปลอดภัย (Secure Key) การใช้กุญแจ WEP แบบไดนามิก (Dynamic WEP Key) นโยบายการรับรองยืนยันซ้ำ (Reauthentication Policy) และการเปลี่ยนค่า Initialization Vector (IV)

การรับรองยืนยันซึ่งกันและกัน

ผลิตภัณฑ์ที่จำหน่ายส่วนใหญ่จะใช้การรับรองยืนยันแบบทางเดียวง่ายๆ ซึ่งเท่ากับเชื้อเชิญให้บุคคลที่อยู่กลางทางเข้าโจมตีง่ายๆ ด้วย แฮ็กเกอร์จะสามารถดักจับข้อมูลที่ส่งโดยใช้อุปกรณ์ตัวโกง เช่นแอ็กเซสพอยนต์ และรวบรวมข้อมูลที่เป็นความลับจากสถานีไคลเอ็นต์ ก๊อบปี้หรือแก้ไขแพ็กเก็ต และแทรกกลับเข้าไปในเครือข่ายในฐานะแพ็กเก็ตที่ถูกต้องใช้ได้ Halasz กล่าวว่า "ในเครือข่ายแบบไร้สาย คุณจะไม่สามารถเชื่อใจใครได้เลย คุณจะทำได้แค่พิสูจน์ความถูกต้องของฝั่งไคลเอ็นต์และโครงสร้างที่ให้การเข้าถึงเครือข่ายเท่านั้น ซึ่งวิธีรับรองยืนยันซึ่งกันและกันคือหนทางเดียวที่จะทำได้ (ในการป้องกันการโจมตีจากแฮ็กเกอร์ระหว่างทาง)"

สำหรับโซลูชัน Aironet ทางซิสโก้ได้สร้างแบบแผนการรับรองยืนยันบนพื้นฐานของ Extensible Authentication Protocol (EAP) อย่างหนึ่งที่มีชื่อว่า EAP - Cisco Wireless หรือ LEAP โดยการใช้มาตรฐานฉบับร่าง 802.1x สำหรับการรักษาความปลอดภัยที่ขึ้นกับพอร์ตเป็นพื้นฐาน พร้อมกับการดัดแปลงแก้ไขที่จำเป็นสำหรับเครือข่ายไร้สาย LEAP จะให้การรับรองยืนยันซึ่งกันและกันระหว่างการ์ดไคลเอ็นต์ Cisco Aironet และเซิร์ฟเวอร์ Remote Authentication Dial-In

User Service (RADIUS) ที่ฝั่งแบ็กเอนด์ (ดูภาพประกอบ)

กุญแจรักษาความปลอดภัย

ผลิตภัณฑ์ตามมาตรฐาน 802.11 ยุคแรกใช้กุญแจ WEP แบบสถิตสำหรับการรับรองเช่นเดียวกับการเข้ารหัส ทำให้ WLAN เสี่ยงต่อการถูกโจมตีด้วยการป้อนรหัสผ่านกลับด้วยวิธีต่างๆ โซลูชัน Cisco Aironet จึงมีการแยกส่วนของการรับรองออกจากการเข้ารหัส การล่วงรู้ความลับร่วมกันของจุดปลายฝั่ง ถูกนำมาใช้สร้างการตอบสนองต่อการร้องขอระหว่างขั้นตอนรับรองยืนยันซึ่งกันและกัน ซึ่งการตอบสนองนี้จะได้รับการเข้ารหัสด้วยฟังก์ชันสับข้อมูลทางเดียวที่ขึ้นกับความลับอันเป็นที่รู้กันดังกล่าว ตัวรหัสผ่านเองไม่มีทางเป็นที่เปิดเผย และการร้องถามก็เป็นไปแบบสุ่ม Kittur Nagesh ผู้จัดการสายผลิตภัณฑ์ของ Wireless Networking Business Unit ที่ซิสโก้กล่าวว่า วิธีเหล่านี้ พร้อมด้วยการเลือกใช้รหัสผ่านที่ดี และการเปลี่ยนแปลงนโยบายต่างๆ ทำให้แน่ใจเลยว่าการโจมตีอย่างรุนแรงจะสามารถบรรเทาลงได้"

ลูกกุญแจที่ใช้เฉพาะกับหนึ่งเซสชัน จะได้มาโดยการใช้ฟังก์ชันสับข้อมูลทางเดียว Messege Digest 5 (MD5) จากความลับอันเป็นที่รู้กัน และข้อความตอบสนองการร้องถามซึ่งกันและกัน วิธีนี้จะป้องกันแฮ็กเกอร์ได้กุญแจเซสชัน โดยการดักจับการตอบสนองระหว่างทาง ดังคำกล่าวของ Nagesh ที่ว่า "คุณไม่มีทางที่จะถอดรหัสฟังก์ชันสับข้อมูลทางเดียวได้ ในทำนองเดียวกับที่คุณไม่สามารถได้ไข่เป็นฟองๆ คืนมาจากไข่ที่แตกจนละเอียดแล้ว" การผูกติดการตอบสนองคำร้องขอกับการได้กุญแจ ทำให้แน่ใจว่ากุญแจเซสชันจะเปลี่ยนไปทุกครั้งที่มีการรับรองยืนยันซ้ำหลังจากไทม์เอาต์หรืออันเนื่องจากการโรมมิง

กุญแจ WEP แบบไดนามิก

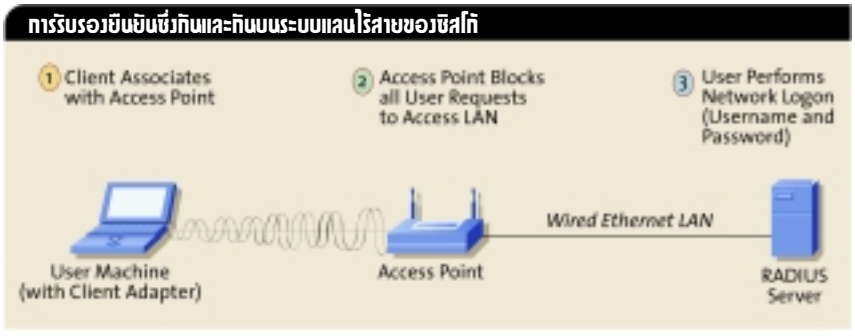
มาตรฐาน 802.11 ปล่อยให้การอิมพลีเมนต์แผนการบริหารกุญแจ WEP ให้เป็นเรื่องของผู้ผลิต โดยผลิตภัณฑ์ตามมาตรฐาน 802.11 ยุคแรกส่วนใหญ่จะใช้กุญแจดอกเดียวร่วมกันสำหรับผู้ใช้ทุกคนในเครือข่าย ซึ่งก่อให้เกิดปัญหามากมายตามมา ที่เห็นได้ชัดเจนที่สุด คือความเสี่ยงอันเกิดจากอุปกรณ์ที่มีกุญแจนั้นถูกโจรกรรม หรือสูญหายไป

ปัญหาข้อที่สองอยู่ที่การบริหารกุญแจ WEP กุญแจที่ใช้ร่วมกับ WEP แบบสถิตต้องได้รับการป้อนเข้าไปในแอ็กเซสพอยนต์ทุกตัวและอุปกรณ์ของผู้ใช้ทุกคน ซึ่งเสียเวลามาก โดยเฉพาะอย่างยิ่งถ้าผู้บริหารเครือข่ายต้องสร้างกุญแจดอกใหม่ให้ทั้งเครือข่ายทุกครั้งที่มีแลปทอปของผู้ใช้คนใดคนหนึ่งหายไป Bill Rossi ผู้จัดการทั่วไปของ Wireless Networking Business Unit ที่ซิสโก้กล่าวว่า "การทำเช่นนั้นไม่มีทางสำเร็จได้ เมื่อเครือข่ายของคุณมีผู้ใช้เป็นพันๆ คน แต่เรามีแผนการรักษาความปลอดภัยแบบไดนามิก คือเมื่อคุณล็อกอินแล้วได้รับการรับรอง กุญแจการเข้ารหัสจะถูกสร้างขึ้นอัตโนมัติเฉพาะกับเซสชันของคุณครั้งนั้นเท่านั้น"

นโยบายการรับรองยืนยันซ้ำ

การมีเครือข่ายไร้สายเท่ากับเป็นการเปิดโอกาสให้แฮ็กเกอร์ศึกษารูปแบบที่คาดเดาล่วงหน้า สำหรับแทรกแพ็กเก็ตของตนเข้าไปในเครือข่ายแลนของบริษัทได้ง่ายๆ ขณะที่มาตรฐาน 802.11 WEP มีแนวป้องกันการโจมตีทั้งแบบแทรกแพ็กเก็ตเข้าไปในทราฟฟิก (Traffic Injection) และแบบเชิงสถิติ (Statistical Attack) แต่ก็เป็นไปอย่างหละหลวมไร้ประสิทธิภาพ

สายข้อมูลรหัสลับจะขยายกุญแจดอกสั้นให้เป็นสายกุญแจเสมือนจะสุ่มที่มีความยาวอนันต์ โดยผู้ส่งจะดำเนินการ XOR สายกุญแจนั้นกับข้อความธรรมดาเพื่อสร้างข้อความที่เข้ารหัส ส่วนผู้รับก็ใช้กุญแจเดียวกันนี้สร้างสายกุญแจที่มีความเหมือนกันทุกประการ ซึ่งผู้บุกรุกสามารถใช้ประโยชน์จากจุดอ่อนนี้ได้ โดยการดักจับทราฟฟิก สลับบิต และยิงแพ็กเก็ต



รักษาความปลอดภัยซึ่งกันและกัน: *ไคลเอ็นต์จะรับรองยืนยันเครือข่ายผ่านทางเซิร์ฟเวอร์ RADIUS และในขณะเดียวกันเซิร์ฟเวอร์ RADIUS ก็รับรองยืนยันไคลเอ็นต์ ซึ่งแผนการรับรองยืนยันสองฝั่งนี้จะแยกกันทำบนคนละช่องทาง โดยมีแอ็กเซสพอยนต์คั่นตรงกลาง*

ที่ถูกแก้ไขกลับเข้าไปในเครือข่าย ถ้าผู้บุกรุกสามารถดักจับข้อความลับที่เข้ารหัสด้วยสายกุญแจและ IV ตัวเดียวกันได้ ข้อความลับนั้นก็จะถูกเปิดเผยในระหว่างการโจมตีแบบเชิงสถิติ

โซลูชัน Cisco Aironet ยอมให้ผู้บริหารเครือข่ายจัดสร้าง และบริหารนโยบายการรับรองยืนยันซ้ำจากส่วนกลางในระหว่างเซสชันได้ เป็นต้นว่าทุกๆ 30 นาที วิธีการนี้จะขัดขวางความสามารถของแฮ็กเกอร์ที่จะดักจับ ถอดรหัส และใช้กุญแจเซสชันเข้าถึงเครือข่าย รวมถึงลดโอกาสที่จะถูกโจมตีด้วยวิธีการอื่นๆ จนถึงระดับต่ำสุด

การเปลี่ยนแปลง Initialization Vector

มาตรฐาน 802.11 WEP จัดให้มีการตรวจสอบความถูกต้องของข้อมูลด้วยตัวเลข IV ในเฮดเดอร์ของแต่ละแพ็กเก็ต อย่างไรก็ตาม ฟิลด์ของ IV นั้นมีความยาวเพียง 24 บิต ซึ่งสำหรับหนึ่งเซสชันจะมีการเรียกใช้ตัวเลข IV ใหม่ซ้ำแล้วซ้ำอีกทุกๆ ประมาณห้าชั่วโมง เมื่อเซสชันมากกว่าหนึ่งสื่อสารผ่านแอ็กเซสพอยนต์ตัวเดียวกัน ค่า IV จึงอาจเกิดความซ้ำซ้อน ซึ่งจะเพิ่มโอกาสที่ข้อความลับสองข้อความที่เข้ารหัสด้วยกุญแจดอกเดียวกันถูกดักจับ และเป็นฐานของการโจมตีแบบใช้ตารางสถิติในที่สุด เพราะผู้บุกรุกสามารถสร้างตารางถอดรหัสได้หลังจากศึกษาข้อความธรรมดาสำหรับบางแพ็กเก็ต จากนั้นก็ประมวลกุญแจ RC4 ที่สร้างโดยค่า IV ที่กำลังใช้อยู่ และถอดรหัสแพ็กเก็ตอื่นๆ ในสายข้อมูลนั้นต่อไป เมื่อเวลาผ่านไป ผู้บุกรุกจะสามารถสร้างตารางของค่า IV และสายกุญแจต่างๆ ได้สำเร็จ

โซลูชัน Cisco Aironet 802.1x สามารถอุดช่องโหว่นี้ โดยการเปลี่ยนค่า IV บนพื้นฐานของแพ็กเก็ตขณะนั้น เพื่อที่แฮ็กเกอร์จะไม่สามารถค้นหาลำดับข้อมูลที่กะไว้ล่วงหน้าได้ ยิ่งกว่านั้น Aironet 802.1x ยังเริ่มต้นเซสชันด้วยค่า IV แบบสุ่มแทนการใช้ค่าเดียวกันสำหรับแต่ละเซสชัน ซึ่งเมื่อผนวกกับนโยบายรับรองยืนยันซ้ำแล้ว การเปลี่ยนค่า IV จะทำให้แฮ็กเกอร์ประสบความยากลำบากในการโจมตีแบบใช้ตารางสถิติมากขึ้น

CRC-32 Checksum

ฟังก์ชันตรวจสอบความถูกต้องของมาตรฐาน 802.11 มีความเสี่ยงต่อการโจมตีเนื่องจากใช้ CRC-32 Checksum แบบเชิงเส้น ซึ่งทำให้เป็นไปได้ที่จะคำนวณความแตกต่างระหว่าง CRC สองค่าโดยการสลับบิตภายในข้อความ ไม่ว่าจะเป็นมาตรฐาน 802.1x หรือ 802.11 ก็ไม่มีหนทางสำหรับแก้ปัญหานี้เลย

ตามความเห็นของ Nagesh “แฮ็กเกอร์สามารถแก้ไขแพ็กเก็ต และสลับบิตเพื่อทำให้ CRC ดูเหมือนถูกต้อง และเลียนแบบพฤติกรรมของโพรโตคอลที่ทราบกันอยู่แล้วต่อแพ็กเก็ตที่ผ่านการแก้ไขเหล่านี้ หนทางเดียวที่จะอุดช่องโหว่นี้ได้ ก็คือการตรวจสอบความถูกต้องของข้อมูลแพ็กเก็ตต่อแพ็กเก็ต ซึ่งเราพิจารณาที่จะบรรจุลงผลิตภัณฑ์รุ่นต่อไปๆ พร้อมกับสร้างมาตรฐานใหม่ตามออกมา”

มาตรฐานความปลอดภัยร่วมกัน

ซิสโก้กำลังร่วมมือกับบริษัทต่างๆ ในการพัฒนากรอบโครงสร้างรักษาความปลอดภัยสำหรับใช้ร่วมกันในเครือข่ายท้องถิ่นไร้สาย ทั้งซิสโก้, ไมโครซอฟท์ และบริษัทอื่นๆ ได้ร่วมกันเสนอกรอบโครงสร้างความปลอดภัยขั้นต่ำบนมาตรฐานตั้งแต่ IEEE 802.1x ไปจนถึง IEEE 802.11 โดยขึ้นกับมาตรฐานอย่าง EAP และ RADIUS มาตรฐาน 802.1x สำหรับ 802.11 จะให้กรอบโครงสร้างขยายขนาดได้ ที่สนับสนุนกรรมวิธีรับรองยืนยันหลากหลายรูปแบบ อาทิ ไบโอเมตริกซ์ ใบประกาศดิจิตอล หรือการป้อนรหัสผ่าน

อย่างไรก็ตาม เพื่อที่จะสนองความจำเป็นพื้นฐานของเครือข่ายไร้สาย ในแง่ของการรับรองยืนยันซึ่งกันและกัน และการเสนอการปกป้องแบบกลับไปมา ซึ่งพิเศษไม่เหมือนใคร แผนการรับรองยืนยันเหล่านี้ก็จำเป็นต้องวิวัฒนาการจากสิ่งที่อยู่ในเครือข่ายแบบมีสายและเครือข่ายแบบ Dial-Up ให้ดียิ่งขึ้นด้วย

ไม่มีโซลูชันใดที่แก้ปัญหาได้ทุกอย่าง

การสร้างความมั่นคงปลอดภัยให้กับ WLAN เป็นเพียงองค์ประกอบหนึ่งของกรอบโครงสร้างความปลอดภัยภายในองค์กรเท่านั้น ผู้เชี่ยวชาญด้านการรักษาความปลอดภัยล้วนเสนอให้องค์กรวางแนวป้องกันซ้อนทับหลายๆ ชั้น เพื่อบรรเทาความรุนแรงของภัยคุกคาม ส่วนองค์ประกอบเกี่ยวกับการรักษาความปลอดภัยอื่นๆ ที่เพิ่มเข้ามานั้น ก็อาจมีตั้งแต่ไฟร์วอลล์ ระบบดักจับการบุกรุก ไปจนถึงการแบ่งเครือข่ายออกเป็นส่วนย่อย

การที่ซิสโก้อิมพลีเมนต์ระบบรักษาความปลอดภัยตามมาตรฐาน 802.1x นั้นมีผลอย่างยิ่งในการช่วยลดความรุนแรงของภัยคุกคาม ซึ่งเกิดจากช่องโหว่ของมาตรฐาน WEP แบบสถิต โซลูชัน Cisco Aironet สามารถปกป้องค์กรให้รอดพ้นจากรูปแบบการโจมตีส่วนใหญ่ อีกทั้งซิสโก้ และบริษัทพันธมิตรต่างกำลังทำงานผ่านร่างมาตรฐาน เพื่ออุดช่องโหว่ที่ยังเหลืออยู่ ซึ่งต้องเร่งมือทำเนื่องจากความนิยมในการสื่อสารไอพีไร้สายทางพีซี-แลปทอปและพีดีเอกำลังพุ่งสูงขึ้น

สุดท้าย Rossi ทำนายว่า “จากนี้อีกหนึ่งปี คุณจะไม่มีทางซื้อแลปทอปหรือพีดีเอโดยปราศจากฟีเจอร์การเชื่อมต่อไร้สายที่ฝังตัวในแผงวงจรหลักเลย และเมื่อไหร่ที่เครือข่าย 802.11 กลายเป็นมาตรฐานในโน้ตบุ๊ก ผู้คนจะสื่อสารกันได้ไม่ว่าอยู่ ณ แห่งหนตำบลใดในโลก และนั่นคือเป้าหมายสูงสุดของการทำเครือข่ายไร้สาย”