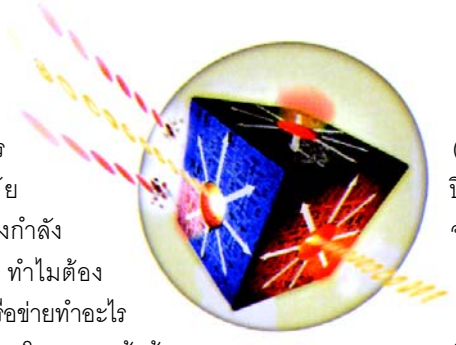
Layer 2
คุณคือจุดอ่อน... เชิญค่ะ!

ข้อควรคำนึงในการรักษาความปลอดภัยที่เลเยอร์ Data Link



เลเยอร์ที่ 2 สำคัญอย่างไร? ในฐานะที่เป็นเลเยอร์ Data Link ใน OSI Model มันคือหนึ่งในเจ็ดเลเยอร์ที่ออกแบบมาเพื่อทำงานร่วมกันแต่เป็นอิสระจากกัน เลเยอร์นี้วางอยู่เหนือเลเยอร์ Physical แต่ก็อยู่ต่ำกว่าเลเยอร์ Network และ Transport ความเป็นอิสระของมันก่อให้เกิดคุณสมบัติในการปฏิบัติงานร่วมกัน และคุณสมบัติในการเชื่อมต่อถึงกัน แต่จากมุมมองเรื่องความปลอดภัยแล้วก็ถือว่าไม่ค่อยดีเท่าไหร่ เนื่องจากความอ่อนแอที่เลเยอร์หนึ่งจะไม่เป็นที่รับทราบของเลเยอร์อื่นที่เหลือเสมอไป หากมีการโจมตีเข้ามาที่เลเยอร์ 2 ก่อน ส่วนที่เหลือในเครือข่ายของคุณก็จะได้ผลกระทบในบัดดล เพราะฉะนั้น เครือข่ายคุณจะแข็งแกร่งหรือไม่จึงขึ้นอยู่กับส่วนที่เป็นจุดอ่อนที่สุด ก็คือส่วนที่เป็นเลเยอร์ Data Link นั่นเอง

เคยสนใจเลเยอร์ 2 บ้างไหม?

ข้อคำนึงอีกประการก็คือ “มุมมอง” บ่อยครั้งทีเดียวที่การปฏิบัติงานเครือข่าย และแนวคิดในการรักษาความปลอดภัยมีมุมมองในสิ่งที่ต้องทำแตกต่างกัน และทั้งคู่ก็ลงเอยด้วยการมองข้ามรายละเอียดในเลเยอร์ที่ 2 ไป

ตัวอย่างหนึ่งก็คือผู้ดูแลเครือข่ายที่ใช้ระบบแลนเสมือนจริง (VLAN) ตลอดเวลา โดยที่หลายอันก็มีเส้นทางส่งผ่านข้อมูลพุ่งเข้าและออกสวิตช์ตัวเดียวกัน เมื่อผู้ดูแลส่วนรักษาความปลอดภัยเดินไปหาผู้ดูแลเครือข่ายเพื่อขอเซ็กเมนต์ในแลนเพิ่ม ทางผู้ดูแลเครือข่ายก็จะสร้าง VLAN และแจกเนื้อที่แอดเดรสส่วนหนึ่งแก่ผู้ดูแลส่วนรักษาความปลอดภัย พอถึงตรงนี้ ส่วนบริหารความปลอดภัยกลับไม่รู้ว่าตัวเองกำลังใช้ VLAN อยู่.. ทำไมต้องสนใจว่าผู้ดูแลเครือข่ายทำอะไรกับสวิตช์ด้วยล่ะ? โดยมากแล้วผู้ดูแลส่วนรักษาความปลอดภัยมักไม่มองที่เลเยอร์ 2 เลยด้วยซ้ำ แต่ไปสนใจที่เลเยอร์ 3 และสูงกว่านั้นแทน

ความแตกต่างในเรื่องของมุมมองนี้ ยังปรากฏผลแม้กระทั่งที่อุปกรณ์เครือข่ายด้วย เช่น ไฟร์วอลล์จะอยู่ในสภาวะที่ปลอดภัยเมื่อซื้อมา โดยค่าปกติจากโรงงาน พวกมันจะไม่อนุญาตให้มีการสื่อสารข้อมูลเมื่อแรกเปิดเครื่อง จนกว่ามีใครไปแก้ไขค่าปกตินั้น ส่วนสวิตช์และเราเตอร์ ในทางตรงข้ามได้รับการออกแบบมาเพื่ออนุญาตให้เกิดการสื่อสารขึ้น และขณะที่หน้าที่หลักๆ ของมัน (การเปิดช่องทางสื่อสาร) สามารถสร้างภาวะเสี่ยงอันตรายในเครือข่ายได้ แต่สวิตช์และเราเตอร์ก็มีคุณสมบัติรักษาความปลอดภัยหลายอย่างในตัว อย่างไรก็ตาม คุณสมบัติและความสามารถเหล่านี้จะไม่มีวันทำงานได้เลย จนกว่าผู้บริหารเครือข่ายจะเป็นผู้เปิดช่องทาง และบ่อยครั้งที่คุณสมบัติเหล่านี้ไม่ได้ถูกใช้งาน หรือแย่กว่านั้นคือไม่มีใครรู้ด้วยซ้ำว่ามีคุณสมบัติเหล่านี้อยู่

ในการสำรวจ “การก่ออาชญากรรม และละเมิดความปลอดภัยในคอมพิวเตอร์” ที่ดำเนินโดยสถาบัน Computer Security Institute ร่วมกับเอฟบีไอเมื่อปี 2545 แสดงให้เห็นถึงความเปลี่ยนแปลงในหนทางที่เครือข่ายถูกโจมตี (qosci.com) โดยในปี 2539 การโจมตีส่วนมากจะมาจากระบบภายใน ขณะที่ส่วนน้อยมาจากการต่อโมเด็มจากต่างสถานที่ และการสแกนพอร์ตทางอินเทอร์เน็ต พอถึงปี 2545 ปริมาณและรูปแบบของการโจมตีก็เปลี่ยนไป ทุกวันนี้มากกว่า 70 เปอร์เซ็นต์ของการโจมตีทั้งหมดล้วนเป็นการสแกนจากภายนอก ส่วน 30 เปอร์เซ็นต์มาจากระบบภายใน อย่างไรก็ตาม การโจมตีจากภายในยังถือว่ามีสัดส่วนในปริมาณที่มากอยู่ และความเสียหายที่ก่อก็ร้ายแรงกว่าการโจมตีจากภายนอกอีกด้วย

ถึงแม้การสาธยายรูปแบบการโจมตีทั้งหมดที่คุกคามเลเยอร์ 2 จะอยู่เกินขอบเขตของบทความนี้ เราก็สามารถพูดถึงการโจมตีที่เป็นปัญหามากที่สุดในสองอันดับแรกอันได้แก่ MAC Flooding และ VLAN Hopping พร้อมวิธีในการบรรเทาผลกระทบที่เกิดขึ้น ซึ่งจะช่วยให้คุณเข้าใจปัญหาที่เลเยอร์ 2 ประสบได้ดียิ่งขึ้น

การโจมตีแบบ MAC Flooding

ในเลเยอร์ที่ 2 จะมีตาราง CAM (Content Addressable Memory) ที่คอยเก็บแอดเดรส MAC ที่มีอยู่บนพอร์ตของฮาร์ดแวร์ พร้อมกับพารามิเตอร์ VLAN ที่เกี่ยวข้องกับแอดเดรสเหล่านั้น (ทำหน้าที่เหมือนตารางวางเส้นทางเดินข้อมูลในเราเตอร์) นอกจากนี้ตารางนี้ยังคอยติดตามสถานที่ตั้งของเครื่องบนเครือข่าย และรับรู้ว่าทราฟฟิกในอนาคต

จะวิ่งผ่านพอร์ตตัวไหน โดยอิงจากข้อมูลการสื่อสารครั้งล่าสุด ซึ่งการโจมตีแบบ MAC Flooding จะพยายามเปลี่ยนสวิตช์ให้ทำหน้าที่คล้ายฮับมากที่สุด ด้วยการระดมยิงรายการข้อมูล (Entry) เข้าใส่ตาราง CAM ไปเรื่อยๆ จนกระทั่งไม่เหลือเนื้อที่รับรายการเพิ่มได้อีก

การโจมตีแบบ MAC Flooding ดูเหมือนเป็นทราฟฟิกจากคอมพิวเตอร์นับพันๆ เครื่องวิ่งเข้ารุมสกรัมพอร์ตเพียงพอร์ตเดียว แต่แท้จริงแล้ว ปรากฏการณ์นี้มาจากคอมพิวเตอร์เครื่องหนึ่งที่สร้างแอดเดรส MAC ปลอมของโฮสต์ที่ไม่มีจริงขึ้น ซึ่งเครื่องมือ Macof ที่มีผู้ร้ายนิยมใช้ก่อการโจมตีประเภทนี้มากที่สุด สามารถสร้างเอนทรี MAC ขึ้นมาบนสวิตช์ได้ในปริมาณสูงถึง 155,000 รายการต่อวินาทีเลยทีเดียว สวิตช์จะมองเห็นทราฟฟิกนี้ และคิดว่าแอดเดรส MAC จากแพ็กเก็ตที่ผู้โจมตีส่งเข้ามานั้นมีจริงแล้วก็จะเพิ่มรายการในตารางให้ เป้าหมายคือการยิงทราฟฟิกให้สวิตช์จนเกิดโอเวอร์โฟลว์ โดยเติมรายการปลอมลงในตาราง CAM ให้ท่วม หลังจากภารกิจสำเร็จ สวิตช์ก็จะแพร่ทราฟฟิกที่ปราศจากเอนทรี CAM กระจายออกไปทั่ว VLAN ในเซ็กเมนต์ของตัวเอง ทำให้ผู้โจมตีมองเห็นทราฟฟิกที่ตามปกติจะไม่เห็นได้ การอัดรายการจนท่วมแบบนี้ง่ายมาก แม้กระทั่งกับตารางที่มีขนาดใหญ่มากและสวิตช์ระดับไฮเอนด์

มีหลายวิธีที่จะบรรเทาความรุนแรงของการโจมตีแบบนี้ วิธีหลักๆ ก็คือการจัดรูปแบบรักษาความปลอดภัยพอร์ตบนสวิตช์ ซึ่งผู้ดูแลสามารถจะกำหนดจำนวนพีซีที่ยอมให้ต่อกับพอร์ตใดพอร์ตหนึ่งของสวิตช์ได้ หากขณะใดๆ จำนวนพีซีมีเกินตัวเลขที่ระบุไว้ พอร์ตก็อาจถูกตั้งให้ปิดตัวเองลง หรือบล็อกแอดเดรส MAC ที่เกินเขตจำกัดที่กำหนด แต่ด้วยเหตุที่สมรรถนะที่ด้อยลง มีส่วนเกี่ยวข้องกับการเฝ้าติดตามแอดเดรส MAC ที่เกินมา จึงขอแนะนำให้ใช้ทางเลือกแรกคือปิดพอร์ตที่รับทราฟฟิกเกินนั้นเสีย

ยิ่งกว่านั้น การรักษาความปลอดภัยแก่พอร์ตยังนำเสนอคุณสมบัติอื่นๆ นอกเหนือจากการหยุดยั้งการโจมตีแบบ MAC Flooding เพียงอย่างเดียว ทั้งนี้คุณสามารถศึกษาวิธีทำงาน และวิธีจัดรูปแบบการรักษาความปลอดภัยแก่พอร์ตเพิ่มเติมได้ที่ cisco.com /univercd/cc/td/doc/product/lan/cat5000/rel_5_4/config/sec_port.htm

การโจมตีแบบ VLAN Hopping

ความเข้าใจผิดที่เพิ่มขึ้นในเรื่องการรักษาความปลอดภัยใน VLAN ผสมโรงกับความกลัวและไม่มั่นใจในเรื่องที่ว่า VLAN สามารถถูกโจมตีได้ง่ายได้นำซิสโก้ไปสู่การติดต่อไปยัง @stake ซึ่งเป็นองค์กรที่นานาชาติรับรู้ว่าเป็นผู้เชี่ยวชาญในด้านการรักษาความปลอดภัยในเครือข่ายและแอพพลิเคชัน เพื่อศึกษาความเป็นไปได้ที่การโจมตี VLAN จะเกิดขึ้นบนสวิตช์ Catalyst ของซิสโก้ว่ามีมากน้อยแค่ไหน จากผลการศึกษาของ @stake ปรากฏว่าไม่มีทางใดที่จะทำให้การโจมตีสำเร็จได้ เว้นเสียแต่จะเกิดการจัดรูปแบบการทำงานที่ไม่ดีพอบนสวิตช์ ซึ่งส่วนใหญ่ การจัดรูปแบบที่ไม่ดีพอมักมีสาเหตุมาจากธรรมชาติการออกแบบ ที่มุ่งเน้นให้เปิดช่องทางสื่อสารตลอดเวลาดังที่กล่าวมาในข้างต้น แทนที่จะเกิดจากความผิดพลาดของผู้ปฏิบัติการ เนื่องด้วยเหตุนี้ การรักษาความปลอดภัยใน VLAN จึงกลายเป็นปัญหายิ่งขึ้น เพราะการจัดรูปแบบการทำงานปกติของสวิตช์ทำให้ตัวสวิตช์เสี่ยงต่อการถูกโจมตีในหลากรูปแบบ เช่น VLAN Hopping ธรรมดาๆ หรือ Double Encapsulated VLAN Hopping (มีอธิบายด้านล่าง) ได้ง่าย และสำหรับรายละเอียดเพิ่มเติมเกี่ยวกับการรักษาความปลอดภัยและการโจมตีใน VLAN จะอยู่ในรายงานผลการศึกษาของ @stake ฉบับเดือนสิงหาคม 2545 ที่ cisco.com/warp/public/cc/pd/si/casi/ca6000/tech/stake_wp.pdf

การโจมตีแบบ VLAN Hopping ถูกออกแบบให้ผู้โจมตีเลี่ยงอุปกรณ์เครือข่ายในเลเยอร์ที่ 3 ได้เมื่อต้องการสื่อสารจาก VLAN วงหนึ่งไปยัง VLAN อีกวงหนึ่ง การโจมตีนี้ทำงานโดยใช้ประโยชน์จากพอร์ตช่องทางสื่อสาร (Trunk Port) ที่จัดรูปแบบไว้ผิดพลาด โดยค่าปกติพอร์ตช่องทางสื่อสารจะเข้าถึง VLAN ได้ทุกแห่ง และพอร์ตเหล่านี้ถูกใช้ในการวางเส้นทางเดินทราฟฟิกของ VLAN หลายแห่งรวมอยู่ในลิงก์ทางกายภาพเดียวกัน (มักจะเป็นลิงก์ระหว่างสวิตช์) ทั้งนี้ข้อมูลที่วิ่งไปในลิงก์เหล่านี้สามารถได้รับการห่อหุ้ม (Encapsulate) ด้วย IEEE 802.1Q หรือ ISL (Inter-Switch Link) ก็ได้

โพรโตคอล DTP (Dynamic Trunking Protocol) รับหน้าที่จัดรูปแบบช่องทางสื่อสาร ISL/802.1Q อัตโนมัติ และปฏิบัติงานคั่นกลางระหว่างสวิตช์ โดย DTP ซึ่งจะ

โมดูลรักษาความปลอดภัย Cisco Catalyst 6500 Series

จริงอยู่ที่การเตรียมพร้อมรับภัยคุกคาม และเพิ่มความเข้มงวดใน VLAN ที่เลเยอร์ 2 นั้นสำคัญ แต่มีสิ่งอื่นๆ ที่คุณสามารถทำได้อีกเพื่อปกป้องสินทรัพย์อันมีค่ามหาศาลในเครือข่าย โดยเฉพาะอย่างยิ่ง เมื่อคุณซื้อสวิตช์ในตระกูล Catalyst 6500 Series มาใช้

ซิสโก้ปรับปรุงการรักษาความปลอดภัยที่เลเยอร์ 2 ให้ดีขึ้นอีกระดับ ด้วยการผนวกชุดโมดูลรักษาความปลอดภัยชั้นสูง เพื่อส่งเสริมประสิทธิภาพแก่เครื่องมือรักษาความปลอดภัยแบบซอฟต์แวร์ อาทิ FWSM (Firewall Services Module), SSL (Secure Socket Layer) Module, IPSec VPN (IP Security Virtual Private Network)Services Module และ NAM (Network Analysis Module)

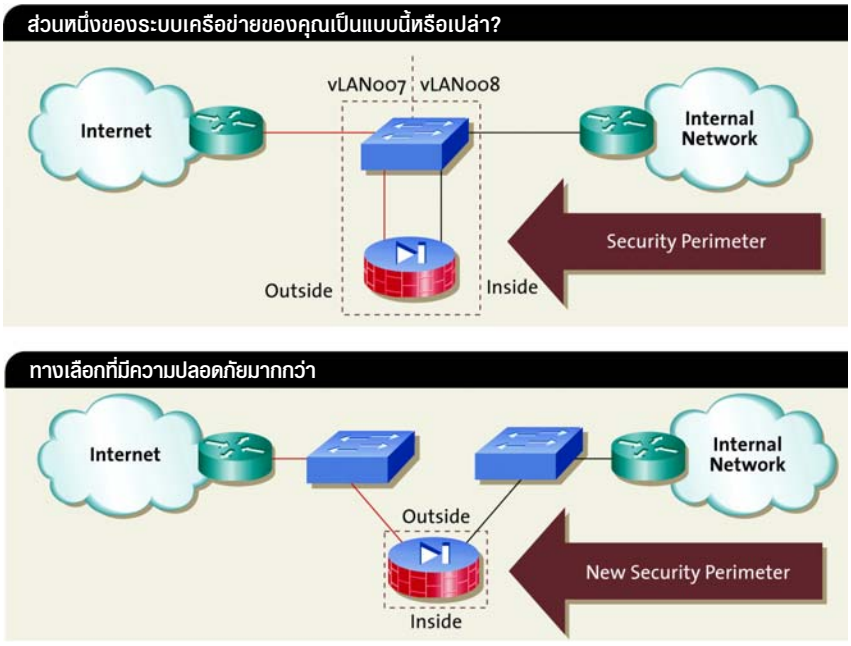
เมื่อปฏิบัติงานควบคู่กับ IDSM (Intrusion Detection System Module) ที่มีอยู่ ก็จะทำให้โมดูลเหล่านี้สามารถจัดวางระบบรักษาความปลอดภัยไว้ภายในสวิตช์ได้ โดยที่ไม่จำเป็นต้องสั่งซื้อ ติดตั้ง และบริหารอุปกรณ์รักษาความปลอดภัยแยกต่างหากอีก การจัดวางโมดูลเหล่านี้เพียงหนึ่งตัวหรือมากกว่าจะช่วยให้สวิตช์แข็งแกร่งขึ้น พร้อมๆ กับเพิ่มความเร็ว ความสามารถด้านการจัดการ และลดค่าใช้จ่ายโดยรวมในการเป็นเจ้าของ (Total cost of ownership) ลงได้อีกด้วย

สำหรับรายละเอียดเพิ่มเติมเกี่ยวกับโมดูลรักษาความปลอดภัย Cisco Catalyst 6500 โปรดเยี่ยมชมได้ที่เว็บเพจ cisco.com/en/US/products/hw/modules/ps2706/prod_models_home.html

ซิงโครไนซ์โหมดช่องทางสื่อสารบนปลายลิงก์ทั้งสองฝั่งเอง ทั้งนี้จะช่วยให้เจ้าหน้าที่ไม่ต้องไปยุ่งเรื่องนี้ที่สวิตช์เลย ส่วนผู้บริหารเครือข่ายสามารถตั้งสถานะของ DTP บนพอร์ตได้ 5 สถานะ ได้แก่ On, Off, Desirable, Auto และ Non-Negotiate ซึ่งแต่ละสถานะก็มีพฤติกรรมดังต่อไปนี้:

- **On:** "ฉันต้องการเป็นช่องทางสื่อสาร และไม่สนใจว่าเธอจะคิดอะไร" เป็นสภาวะที่ใช้เมื่อสวิตช์อีกฝั่งหนึ่งไม่รู้จักโพรโตคอล DTP
- **Off:** "ฉันไม่ต้องการเป็นช่องทางสื่อสาร และไม่สนใจว่าเธอจะคิดอะไร" เป็นสภาวะที่ใช้เมื่อไม่มีเจตนาจะให้พอร์ตนี้เป็นพอร์ตช่องทางสื่อสาร
- **Desirable:** "ฉันเต็มใจที่จะเป็นช่องทางสื่อสารของ VLAN.. เธอสนใจไหม?" เป็นสภาวะที่ใช้เมื่อสวิตช์นั้นสนใจที่จะเป็นช่องทางสื่อสาร
- **Auto:** "ฉันเต็มใจที่จะเป็นในทุกสิ่งที่เธอต้องการ!" เป็นสภาวะที่ตั้งไว้ปกติบนสวิตช์ส่วนมาก
- **Non-Negotiate:** "ฉันต้องการเป็นช่องทางสื่อสาร และนี่คือชนิดของช่องทางสื่อสารที่ฉันจะเป็น!" เป็นสภาวะที่ใช้เมื่อผู้บริหารระบบต้องการระบุชนิดของช่องทางสื่อสารว่าเป็น ISL หรือ .1Q

สิ่งสำคัญเกี่ยวกับ DTP ที่ต้องจำก็คือ ภาวะปกติบนสวิตช์ส่วนใหญ่จะเป็น Auto



ภาพที่ 1: แทนที่จะใช้แลนเสมือนจริงที่ต้องเฝ้าติดตามตลอด ก็ขอให้พิจารณาติดตั้งสวิตช์สองตัวที่ปราศจากแลนเสมือนจริงบ้าง เพราะหากสวิตช์ตัวใดตัวหนึ่งถูกเจาะ ผู้โจมตีก็ยังไม่สามารถกระโดดข้ามไฟร์วอลล์เข้ามาได้อยู่ดี

การโจมตีแบบ VLAN Hopping ธรรมดา: การโจมตีแบบนี้เกิดขึ้นเมื่อผู้โจมตีหลอกสวิตช์ให้เข้าใจผิดว่าเขาเป็นสวิตช์อีกตัวที่ต้องการช่องทางสื่อสาร และการโจมตีแบบนี้ต้องการภาวะ Auto เพื่อให้ภารกิจสำเร็จ ตอนนี้ผู้โจมตีจะกลายเป็นส่วนหนึ่งของ VLAN ทุกแห่งที่เชื่อมต่อบนสวิตช์ และก็สามารถส่งหรือรับทราฟฟิกบน VLAN เหล่านั้นได้ด้วย

วิธีป้องกันการโจมตีแบบ VLAN Hopping ที่ดีที่สุดก็คือ ให้ปิดช่องทางสื่อสารทุกพอร์ตยกเว้นพอร์ตที่จำเป็นต้องใช้ช่องทางสื่อสารจริงๆ เท่านั้น

การโจมตีแบบ Double Enncapsulated VLAN Hopping: การโจมตีแบบนี้ใช้ประโยชน์จากกรรมวิธีที่ฮาร์ดแวร์บนสวิตช์ส่วนใหญ่ทำงาน กล่าวคือสวิตช์ทุกวันนี้ส่วนใหญ่มีการถอดค่า (Decapsulate) IEEE 802.1Q แค่หนึ่งชั้นเท่านั้น ซึ่งช่วยให้ผู้โจมตีมีสิทธิที่จะฝังแท็ก .1Q ซ่อนไว้ในเฟรม และระบบก็จะปล่อยเฟรมให้วิ่งไปยัง VLAN ที่แท็ก .1Q ชั้นนอกไม่ได้ระบุไว้ ลักษณะพิเศษ

ข้อพึงปฏิบัติในการดูแลเครือข่ายเลเยอร์ที่ 2

นอกจาก MAC Flooding และ VLAN Hopping แล้ว เครือข่ายก็อาจถูกโจมตีด้วยรูปแบบอื่นๆ อีก เช่น Spanning-tree, การสร้าง ARP (Address Resolution Protocol) หลอกๆ เพื่อตบตาระบบรักษาความปลอดภัย หรือการโจมตีโดยใช้ DHCP (Dynamic Host Control Protocol) ซึ่งล้วนแล้วสามารถย่ำยีเครือข่ายในเลเยอร์ที่ 2 ได้ทั้งสิ้น รายละเอียดเกี่ยวกับการโจมตีเหล่านี้ และข้อปฏิบัติเพื่อบรรเทาความรุนแรง สามารถหาอ่านจากบทความที่ฌอน คอนเวรี นักวิจัยระบบรักษาความปลอดภัยประจำฝ่ายรับประกันโครงสร้างขั้นวิกฤต (Critical Infrastructure Assurance) ของซิสโก้เขียนไว้ในเว็บไซต์ Blackhat.com (www.blackhat.com/presentations/bh-usa-02/bh-us-02-convery-switches.pdf) และต่อไปนี้คือข้อปฏิบัติบางส่วนที่คัดลอกมา:

- จำกัดขอบเขตการเข้าบริหารในสวิตช์ เพื่อให้ผู้ที่อยู่บนเครือข่ายที่ไม่น่าวางใจ ไม่สามารถใช้ประโยชน์จากอินเทอร์เฟซการบริหารและโพรโตคอลอย่าง SNMP (Simple Network Management Protocol) ได้
- ป้องกันการโจมตีที่หวังให้ระบบหยุดบริการ (Denial-of-service) และการแฝงเข้าไปใช้ประโยชน์จากเครือข่ายอย่างผิดๆ โดยยุติการใช้ Spanning-tree และโพรโตคอลแบบไดนามิกอื่นๆ
- ใช้ ACL ประเภทฮาร์ดแวร์ในทุกตำแหน่งที่มีให้ใช้ เพื่อบล็อกทราฟฟิกอันไม่พึงประสงค์
- ใช้ VLAN ID แยกเฉพาะสำหรับพอร์ตช่องทางสื่อสารทั้งหมด
- ปิดพอร์ตที่ไม่ได้ใช้งานใน VLAN
- ใช้กลไกการรักษาความปลอดภัยที่พอร์ตจำกัดจำนวนแอดเดรส MAC เพื่อป้องกันการโจมตีแบบ MAC Flooding
- หลีกเลี่ยงการใช้ VLAN 1 ในพอร์ตช่องทางสื่อสารและพอร์ตยูสเซอร์ในทุกที่ที่เป็นไปได้

สำหรับรายละเอียดเพิ่มเติมเกี่ยวกับการรักษาความปลอดภัยใน VLAN โปรดเข้าไปดูที่ cisco.com/go/safe และ cisco.com/en/US/netsol/ns110/ns170/ns171/ns128/networking_solutions_package.html

คุณทราบหรือไม่ว่า.. ?

คุณเคยทราบหรือไม่ว่าผลิตภัณฑ์ของซิสโก้หลายๆ ตัวที่นำมาใช้งานในเลเยอร์ที่ 2 มีคุณสมบัติการรักษาความปลอดภัยในตัว รวมไปถึงการรักษาความปลอดภัยที่พอร์ต, VLAN ส่วนบุคคล และ ACL อยู่แล้ว? ต่อไปนี้คือสิ่งที่คุณสมบัติแต่ละตัวรับผิดชอบ:

■ **การรักษาความปลอดภัยที่พอร์ต** : ยอมให้ผู้บริหารเครือข่ายระบุจำนวนพีซีสูงสุดที่อนุญาตให้ต่อกับพอร์ตใดพอร์ตหนึ่งบนสวิตช์

■ **แลนเสมือนจริงส่วนบุคคล:** เสนอความคุ้มครอง และจัดพอร์ตต่างๆ บนสวิตช์ ซึ่งล้วนเป็นสมาชิกของ แลนเสมือนจริงวงเดียวกันแยกจากกันต่างหาก คุณสมบัตินี้ทำให้มั่นใจว่า ผู้ใช้จะสามารถสื่อสารได้ก็เฉพาะกับเกตเวย์ปกติของตนเองเท่านั้น ไม่ใช่กับเกตเวย์ของผู้อื่นด้วย ทั้งนี้ แลนเสมือนจริงส่วนบุคคลมีประโยชน์มากในสภาพแวดล้อมแบบที่มีเขตกันชนระหว่างอินเทอร์เน็ตกับเครือข่ายในองค์กร หรือ DMZ (Demilitarized Zone)

■ **การคุ้มกันรูต STP/BPDU:** สามารถบรรเทาความรุนแรงของการโจมตีที่ใช้ STP (Spanning Tree Protocol) ได้ โดยปิดพอร์ตที่จะเป็นสาเหตุให้โทโพโลยีของเลเยอร์ที่ 2 เปลี่ยนไป

■ **การสนับสนุน SSH:** ให้ความสามารถในการเชื่อมต่อข้ามสถานที่แก่อุปกรณ์ในเลเยอร์ที่ 2 และ 3 ซึ่ง SSH จะให้ความปลอดภัยสูงกว่า Telnet โดยมีการเข้ารหัสอันแข็งแกร่งเมื่ออุปกรณ์ได้รับการพิสูจน์ยืนยันตัวตน (Authentication) คุณสมบัตินี้มีทั้งในรูปแบบของ SSH Server และ SSH Client

คุณสมบัติต่างๆ ที่สวิตช์ Cisco Crtalyst รองรับ

	Cat 2900 XL	Cat 3500 XL	Cat 2950	Cat 3550	Cat 29xx G	CatOS 4000	CatOS 6000	IOS 4000	IOS 6000
Port Security	X	X	X	X	X	X	X		
Private VLANs	X	X	X	X		X	X	X	X
STP BPDU Guard			X	X		X	X	X	X
STP Root Guard	X	X	X	X	X	X	X	X	X
SSH Support					X	X	X		
VMPS Client	X	X	X	X	X	X	X	X	X
VMPS Server					X	X	X		
802.1X Auth			X	X	X	X	X		
Wire-Rate ACLs			X	X		X	X	X	X

■ **VMPS (VLAN Membership Policy Server):** สามารถผูกโยงแอดเดรส MAC บางหมายเลขไว้กับแลนเสมือนจริงเฉพาะวง เพื่อให้ผู้ใช้ที่ถือเครื่องเดินไปมาได้ใช้สิทธิด้านความปลอดภัยอันเดียวกันทุกจุดในองค์กร

■ **การพิสูจน์ยืนยันตัวตน 802.1X:** สามารถปกป้องเครือข่ายโดยให้ผู้ใช้ลงทะเบียนรับการพิสูจน์ตัวตนต่อฐานข้อมูลกลาง ก่อนยอมให้การเชื่อมต่อเครือข่ายไม่ว่าในรูปแบบใดๆ เกิดขึ้น แต่ในทางกลับกันเครือข่ายภายในส่วนใหญ่จะเข้าถึงได้ เพียงแค่เสียบสายเข้ากับคอนเน็กชันอีเทอร์เน็ตภายในเท่านั้น

■ **Wire-rate ACL:** ทำให้รายชื่อควบคุมการเข้าถึง (Access Control List) ได้รับการประมวลผล โดยไม่ทำให้สมรรถนะเครือข่ายลดลง และคุณสมบัตินี้ช่วยให้ ACL สามารถถูกใช้ในสถานการณ์ที่ตามปกติจะใช้ ACL ไม่ได้อีกด้วย

ของการโจมตีแบบนี้ คือจะสามารถทำงานได้แม้ว่าพอร์ตช่องทางสื่อสารถูกตั้งสถานะเป็น OFF แล้วก็ตาม

การขัดขวางรูปแบบการโจมตีนี้ไม่ง่ายเหมือนการหยุด VLAN Hopping ธรรมดา ๆ วิธีการที่ดีที่สุดก็คือดูให้แน่ใจว่า VLAN ดั้งเดิมของพอร์ตช่องทางสื่อสารแตกต่างจาก VLAN ดั้งเดิมของพอร์ตยูสเซอร์ สำหรับรายละเอียดเพิ่มเติมเกี่ยวกับการหยุดการโจมตีแบบ Double Encapsulated VLAN Hopping นี้ โปรดดูในกรอบ “ข้อพึงปฏิบัติในการดูแลเครือข่ายเลเยอร์ที่ 2”

การบริหารสวิตช์ และควบคุมแอ็กเซส

นับมาจนถึงปัจจุบัน พรมแดนเครือข่ายที่เปิดสู่อินเทอร์เน็ตในบางลักษณะ ได้ใช้สวิตช์เพียงตัวเดียวในการควบคุมทั้งบริเวณที่วางใจได้ (Trusted) กับที่วางใจไม่ได้ (Untrusted) ของเครือข่ายภายในองค์กร (ดูภาพที่ 1 ช่องบน) ในการออกแบบลักษณะนี้ จะมีการใช้ VLAN ตั้งแต่หนึ่งแห่งขึ้นไป แบ่งแยกทราฟฟิกจากแหล่งที่วางใจได้กับที่วางใจไม่ได้ ซึ่งจากผลการศึกษาของ @stake นั้น VLAN สามารถที่จะใช้แบ่งแยกทราฟฟิกในวิธีนี้ได้ ถ้าได้รับการจัดรูปแบบทำงานอย่างเหมาะสม แต่โชคร้ายที่การใช้มาตรการรักษาความปลอดภัยหลายอย่างซ้อนกันบนสวิตช์อันเดียว กลับจะเป็นการเพิ่มความซับซ้อนของรูปแบบทำงาน และเพิ่มความน่าจะเป็นในการเกิดข้อผิดพลาดจากผู้ปฏิบัติงาน นอกจากนี้ หากสวิตช์มีจุดอ่อนตลอดเวลา ผู้โจมตีก็สามารถหลีกหนีไฟร์วอลล์ได้อย่างสมบูรณ์ ส่งผลให้เกิดการเชื่อมต่อระหว่างอินเทอร์เน็ตกับเครือข่ายในองค์กรโดยปราศจากกำแพงกั้นในที่สุด

สิ่งสำคัญที่ต้องจำ ก็คือ แนวป้องกันของเครือข่ายคุณประกอบด้วยสวิตช์เช่นเดียวกับไฟร์วอลล์ และด้วยเหตุที่ในเครือข่ายส่วนใหญ่ทีมเจ้าหน้าที่รักษาความปลอดภัยไม่ได้เป็นคนควบคุมสวิตช์เอง นี่จึงอาจก่อให้เกิดปัญหาขึ้น ส่วนการออกแบบอีกลักษณะหนึ่งที่ใช้สวิตช์หลายๆ ตัว โดยไม่ใช้ VLAN (ดูภาพที่ 1 ช่องล่าง) ซึ่งในกรณีนี้ หากสวิตช์ตัวใดตัวหนึ่งถูกโจมตี อุปกรณ์ในการรักษาความปลอดภัยที่เหลือก็ยังคงรับมือได้อยู่