การพัฒนาการตรวจสอบและป้องกันการโจมตีแบบ Brute-force บนเครือข่าย eduroam

Development of brute-force detection and protection for eduroam service

ประกาย นาตี[1], ปรีชา สมหวัง[1], ชัยวัฒน์ แดงจันทึก[2], และ อิฐอารัญ ปิติมล[3]
[1]คณะวิศวกรรมศาสตร์และสถาปัตยกรรมศาสตร์ มหาวิทยาลัยเทคโนโลยีราชมงคลอีสาน
[2]สำนักวิทยบริการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีราชมงคลอีสาน
[3]คณะวิศวกรรมศาสตร์ มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี
E-mail: prakai@rmuti.ac.th

บทคัดย่อ

เครือข่ายโรมมิ่งเพื่อการศึกษาและวิจัย (eduroam) เป็นเครือข่ายคอมพิวเตอร์แบบไร้สายสำหรับให้บริการแก่บุคลากรของสถาบันที่เป็นสมาชิกสามารถเข้าถึงเครือข่ายคอมพิวเตอร์ของสถาบันที่เป็นสมาชิกอื่นได้ โดยใช้บัญชีผู้ใช้และรหัสผ่านจากสถาบันต้นสังกัดในยืนยันสิทธิ์เพื่อการเข้าถึงเครือข่าย มีรูปแบบบริการแบบเชื่อถือกันในระดับเครือข่าย สถาบันผู้ให้บริการเข้าถึงเครือข่ายจะยอมรับการยืนยันสิทธิ์จากสถาบันต้นสังกัดของผู้ใช้บริการในทุกกรณี เปิดโอกาสให้เกิดโจมตีเครือข่ายโดยการปลอมตัวการใช้สิทธิ์แทนผู้อื่นด้วยวิธีการทดลองป้อนรหัสผ่านแบบสุ่มทุกค่าที่เป็นไปได้เรียกว่าการโจมตีแบบบรูตฟอร์ซ (Brute-force attack) ได้ งานวิจัยนี้มีวัตถุประสงค์เพื่อตรวจจับและป้องกันการโจมตีแบบบรูตฟอร์ซสำหรับเครือข่ายโรมมิ่งในสถาบันการศึกษาด้วยการเพิ่มกระบวนการเข้าไปในโปรแกรม Radius ที่ใช้รับและประมวลผลการร้องขอบริการจากเครื่องลูกข่าย ทั้งด้านสถาบันผู้ให้บริการเข้าถึงเครือข่ายและด้านสถาบันต้นสังกัด วิธีการตรวจสอบการโจมตีนั้น ใช้การนับจำนวนครั้งของการร้องขอบริการแบบไม่ถูกต้องในช่วงระยะเวลาที่กำหนด หากเกินกว่าที่กำหนดจะถือว่าเป็นการพยายามโจมตีแบบบรูตฟอร์ซ หลังจากนั้นแล้วจะกำหนดให้มีการปฏิเสธการร้องขอบริการของเครื่องลูกข่ายนั้นต่อไป จากผลการทดลองทำให้ทราบถึงประสิทธิภาพของวิธีการที่นำมาใช้ว่า สามารถตรวจสอบการโจมตีแบบบรูตฟอร์ซได้ โดยไม่ได้ลดประสิทธิภาพการทำงานของการบริการ และสามารถปฏิเสธการร้องขอบริการของเครื่องลูกข่ายที่พยายามโจมตีแบบบรูตฟอร์ซได้เร็วขึ้น ทำให้สามารถสร้างความปลอดภัยให้กับระบบเครือข่ายได้

คำสำคัญ: เครือข่ายโรมมิ่งเพื่อการศึกษาและวิจัย, บรูตฟอร์ซ, เครือข่ายไร้สาย, อินเทอร์เน็ต

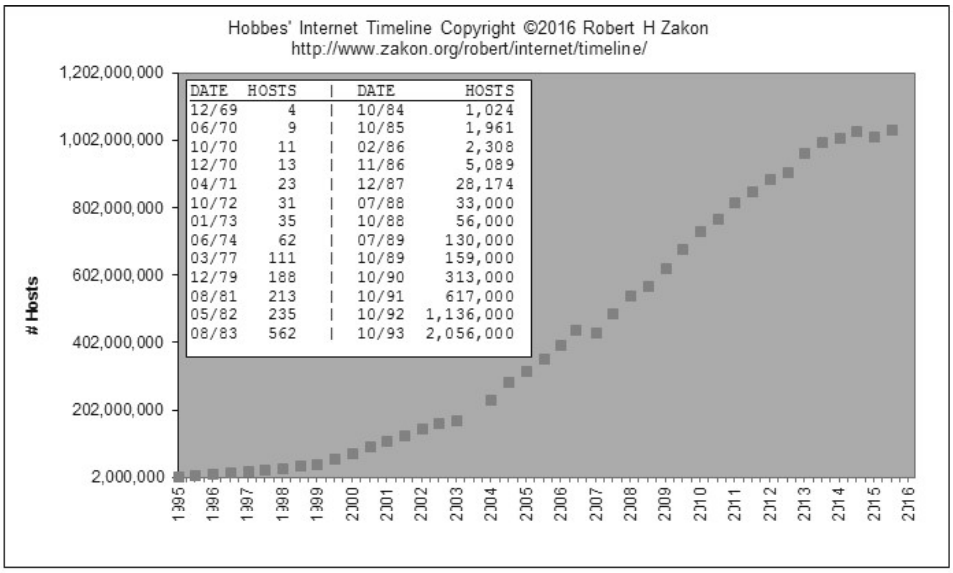
Abstract

eduroam (education roaming) is a network access service developed for the international research and education community. The service allows staff from member institution access to the computer network of other institutions (Service Provider: SP). They use a user account and password issued by home institution (Identity Provider) in order to access to network. eduroam is a trusted network. Service provider accepts the assertion of user from other institutions in all cases. Attacker can attack the network by brute-force attack technique using random password of target user of other institution. This research aims to develop a technique for detect and prevent brute-force attack for eduroam. The methodology used is adding a module into the radius which is used to receive and process requests from clients. The technique of attack detection is counting the number of invalid requests from client during the period. If number of invalid requests is exceeded, that client is marked as attacker. After that, all requests from that client will be rejected. The test results indicate the effectiveness of the methodology used does not reduce the performance of the service. The invalid request can be rejected faster.

Keywords: eduroam, Brute-force, Wireless LAN, Internet

คำนำ

นับตั้งแต่มีการนำเทคโนโลยีอินเทอร์เน็ตเข้ามาใช้ จนกลายเป็นศูนย์รวมข้อมูลข่าวสารแล้วนั้น อินเทอร์เน็ตยังเป็นเครื่องมือในการติดต่อสื่อสารระหว่างบุคคลที่มีประสิทธิภาพ กลายเป็นส่วนหนึ่งของการศึกษา การค้นคว้าวิจัย รวมถึงการดำเนินชีวิตประจำวัน และนับวันเพิ่มจำนวนผู้ใช้งานมากขึ้นเรื่อยๆ (Robert H. Zakon, 2016) ดังแสดงในภาพที่ 1



DATE	HOSTS	DATE	HOSTS
12/69	4	10/84	1,024
06/70	9	10/85	1,961
10/70	11	02/86	2,308
12/70	13	11/86	5,089
04/71	23	12/87	28,174
10/72	31	07/88	33,000
01/73	35	10/88	56,000
06/74	62	07/89	130,000
03/77	111	10/89	159,000
12/79	188	10/90	313,000
08/81	213	10/91	617,000
05/82	235	10/92	1,136,000
08/83	562	10/93	2,056,000

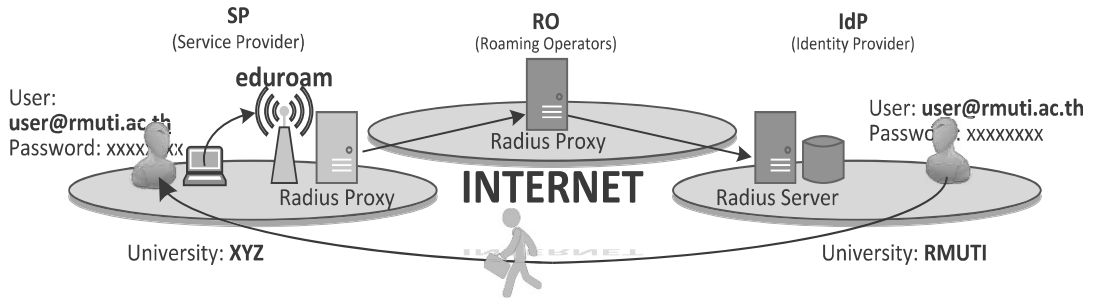
ภาพที่ 1 การเพิ่มขึ้นของจำนวนผู้ใช้อินเทอร์เน็ต

G. López et al. (2008) การใช้งานอินเทอร์เน็ตสำหรับสถาบันการศึกษานั้นมีความจำเป็นสำหรับกระบวนการจัดการเรียนการสอน การค้นคว้างานวิจัย ซึ่งมีการให้บริการระบบสารสนเทศที่หลากหลายรูปแบบ โดยเฉพาะอย่างยิ่งการให้บริการระบบเครือข่ายไร้สาย ที่กลายเป็นการให้บริการเครือข่ายพื้นฐานที่ทุกสถาบันต้องมีเพื่ออำนวยความสะดวกแก่บุคคลากร เมื่อหลายสถาบันได้มีการประสานงานแลกเปลี่ยนข้อมูลสารสนเทศร่วมกันระหว่างสถาบันการศึกษา ทำให้เกิดการสร้างระบบเครือข่าย eduroam ขึ้นมาเพื่อให้บุคคลากรทางการศึกษาสามารถใช้งานระบบเครือข่ายอินเทอร์เน็ตจากต่างสถาบันการศึกษาร่วมกันได้ทั้งในประเทศและต่างประเทศ โดยมีเงื่อนไขว่าการยืนยันสิทธิ์การใช้งานต้องได้รับการตรวจสอบสิทธิ์จากต้นสังกัด และมีหน่วยงานกลางสำหรับทำหน้าที่เชื่อมต่อระหว่างแต่ละสถาบันการศึกษา สำหรับประเทศไทยมีสำนักงานบริหารเทคโนโลยีสารสนเทศเพื่อพัฒนาการศึกษา หรือเรียกว่ายูนิเน็ต (UniNet) เป็นหน่วยงานภายใต้สำนักงานคณะกรรมการการอุดมศึกษา ทำหน้าที่เป็นหน่วยงานกลางในประเทศไทยเพื่อเชื่อมต่อไปยังสถาบันการศึกษาอื่นทั่วโลก (eduroam.uni.net.th, 2016)

มหาราช ทศศะ (2555) การเชื่อมต่อเข้ากับอินเทอร์เน็ตร่วมกันระหว่างสถาบันการศึกษานั้นมีทั้งประโยชน์และโทษเนื่องจากผู้ใช้งานที่เชื่อมต่อเข้าสู่ระบบมีทั้งบุคคลของสถาบันและผู้ประสงค์ร้าย บางครั้งก่อให้เกิดความเสียหายให้กับระบบเครือข่ายเป็นอย่างมาก ส่งผลต่อการให้บริการไม่มีประสิทธิภาพ ตลอดจนแม้กระทั่งหยุดการให้บริการของระบบเครือข่าย ซึ่งภัยคุกคามที่ส่งผลกระทบต่อระบบเครือข่าย eduroam มากที่สุดคือการโจมตีในรูปแบบการพยายามขโมยข้อมูลส่วนบุคคล โดยเฉพาะอย่างยิ่ง บัญชีผู้ใช้และรหัสผ่าน การโจมตีรูปแบบนี้เรียกว่าการโจมตีแบบบรูตฟอร์ซ

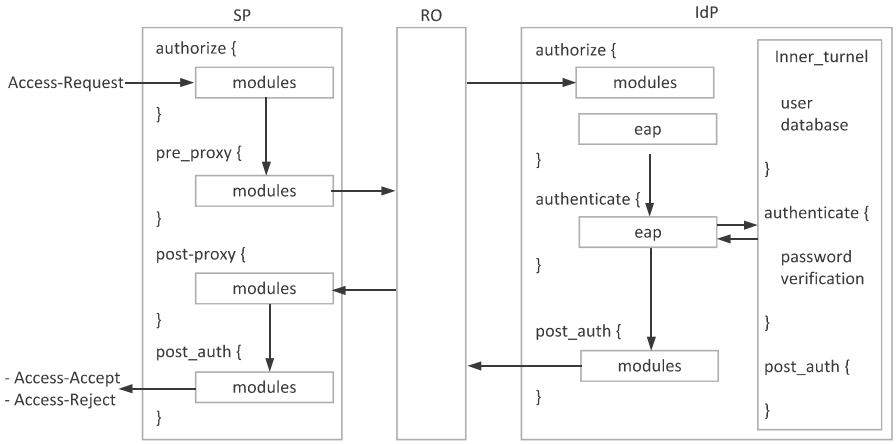
(Brute-force attack) รูปแบบการโจมตีเป็นการสุ่มใช้บัญชีผู้ใช้และรหัสผ่าน ทั้งในรูปแบบโปรแกรมพจนานุกรม (Dictionary) และพยายามสุ่มตัวอักษรทีละตัวไปเรื่อยๆ จนครบทุกตัวที่เป็นไปได้ เพื่อหารหัสผ่านที่ตรงกับบัญชีผู้ใช้ ที่มีอยู่จริงในระบบฐานข้อมูล ผลกระทบที่เกิดนั้นสามารถสร้างความเสียหายให้กับระบบเป็นอย่างมากเนื่องจากเป็นการโจมตีแบบต่อเนื่อง ทำให้เกิดการใช้งานทรัพยากรระบบเครือข่ายโดยสิ้นเปลือง และหากการโจมตีสามารถทำได้สำเร็จจะทำให้เกิดข้อมูลรั่วไหล ดังนั้น จึงจำเป็นต้องหาทางป้องกันการโจมตีและระงับเหตุการณ์ที่เกิดขึ้น งานวิจัยนี้มีวัตถุประสงค์เพื่อตรวจสอบและป้องกันการโจมตีแบบบรูตฟอร์ซ โดยสร้างกฎและเงื่อนไขเพื่อวิเคราะห์พฤติกรรมของผู้ใช้งานระบบเครือข่าย eduroam จากพฤติกรรมจงใจโจมตีระบบเครือข่ายและผู้ใช้งานโจมตีเครือข่ายแบบไม่รู้ตัวจากเครื่องคอมพิวเตอร์ที่ใช้งานมีไวรัส ได้นำเสนออุปกรณ์และวิธีการ ผลการวิจัย อภิปรายและสรุปผลการวิจัย ดังมีรายละเอียดในหัวข้อดังต่อไปนี้

โครงสร้างการให้บริการของเครือข่าย eduroam ประกอบด้วยเครื่องแม่ข่ายอย่างน้อย 3 ส่วน คือ Service Provider (SP), Roaming Operator (RO) และ Identity Provider (IdP) ใช้โปรแกรม Radius ในการรับและประมวลผลการร้องขอบริการจากเครื่องลูกข่าย ขั้นตอนการทำงานของโปรแกรม Radius ในแต่ละส่วนของทั้ง 3 ส่วนมีความต่อเนื่องกัน ดังแสดงในภาพที่ 2



ภาพที่ 2 โครงสร้างการให้บริการของเครือข่าย eduroam

Tomo et al. (2014) เมื่อเครื่องลูกข่ายต้องการเชื่อมต่อเครือข่าย eduroam ต้องส่งข้อมูลการร้องขอการเชื่อมต่อผ่านอุปกรณ์เครือข่ายไร้สายไปยัง Radius server ของ SP ข้อมูลที่ร้องขอคือ Access-Request มีข้อมูลที่จำเป็นที่อย่างน้อยประกอบด้วย User-Name คือบัญชีผู้ใช้ตามรูปแบบของการใช้งาน eduroam เช่น user@rmuti.ac.th และ Calling-Station-Id คือหมายเลข MAC Address ของเครื่องลูกข่ายที่เป็นผู้ร้องขอเชื่อมต่อ เมื่อ Radius ใน SP ได้รับข้อมูลการร้องขอของเครื่องลูกข่าย จึงเริ่มต้นกระบวนการประมวลผลข้อมูลจากการเรียกใช้โมดูลในส่วน authorize เรียกใช้โมดูล ซึ่งมักเป็นโมดูล suffix เพื่อดำเนินการแยกส่วนของข้อมูล User-Name ออกเป็น 2 ข้อมูลย่อยคือ Striped-User-Name และ Realm หลังจากนั้น Radius ของ SP ต้องใช้ข้อมูล Realm สำหรับพิจารณาว่าเป็นบัญชีผู้ใช้ภายในหรือสถาบันอื่น หากเป็นบัญชีผู้ใช้จากสถาบันอื่น ต้องเรียกใช้โมดูลเพื่อประมวลผลข้อมูลในส่วนของ pre_proxy ก่อนส่งการร้องขอต่อไปยัง RO ต่อไป ดังแสดงรายละเอียดในภาพที่ 3

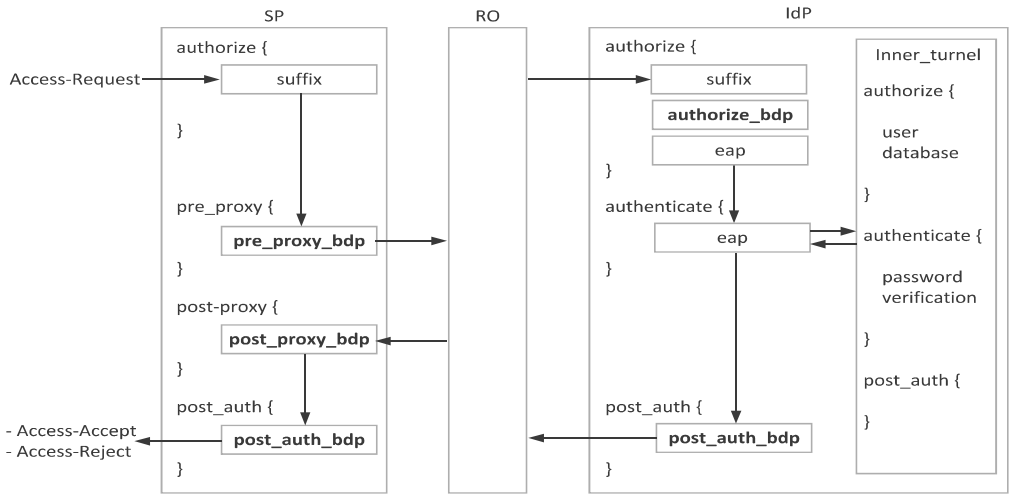


ภาพที่ 3 ลำดับขั้นการประมวลผลการร้องขอบริการของโปรแกรม Radius

หลังจากนั้น Radius ของ RO จะดำเนินการเช่นเดียวกับส่วนของ authorize ของ Radius ของ SP และส่งต่อการร้องขอบริการไปยัง IdP ที่เป็นสถาบันของผู้ใช้ตามข้อมูล Realm ที่ได้จากบัญชีผู้ใช้ เมื่อข้อมูลร้องขอส่งถึง IdP โปรแกรม Radius จะเริ่มกระบวนการประมวลผลเหมือนกับ SP คือการทำงานในส่วน authorize แต่มีส่วนแตกต่างที่ต้องเรียกใช้โมดูล eap เพื่อส่งต่อกระบวนการไปยังโมดูล eap ในกระบวนการ authenticate โมดูล eap จะดำเนินการเข้ารหัสข้อมูลของผู้ใช้และรหัสผ่านระหว่างเครื่องผู้ใช้กับ IdP และส่งต่อข้อมูลของผู้ใช้และรหัสผ่านที่ได้จากเครื่องลูกข่ายไปยังส่วนของ inner-tunnel เพื่อให้ดำเนินการตรวจสอบตัวตนของผู้ใช้จากฐานข้อมูลผู้ใช้ภายในสถาบัน ผลการตรวจสอบได้ผล 2 แบบคือ ข้อมูลผู้ใช้และรหัสผ่านถูกต้อง จะให้คำตอบเป็น Access-Accept แต่หากข้อมูลผู้ใช้และรหัสผ่านไม่ถูกต้อง จะให้คำตอบเป็น Access-Reject เมื่อโมดูล eap ได้รับผลการตรวจสอบตัวตนของผู้ใช้จาก inner-tunnel แล้วก็ส่งต่อไปประมวลผลในส่วน post_auth เพื่อประมวลผลข้อมูลก่อนจะตอบผลการร้องขอกลับไปยัง RO หลังจาก RO ได้รับข้อมูลผลการร้องขอก็ส่งต่อผลไปยัง SP ต่อไป เมื่อ Radius ของ SP ได้รับข้อมูลผลการร้องขอ ก็นำไปประมวลผลในส่วน post_proxy ก่อน หากผลการร้องขอเป็น Access-Accept จึงตอบผลการร้องขอกลับไปยังเครื่องลูกข่ายทันที แต่หากผลการร้องขอเป็น Access-Reject ข้อมูลก็ถูกส่งไปประมวลผลในส่วน post_auth ส่วน post_auth ก็ประมวลข้อมูลผลการร้องขอก่อนส่งผลการร้องขอกลับไปยังเครื่องลูกข่ายต่อไป (Fernando et al., 2009)

อุปกรณ์และวิธีการ

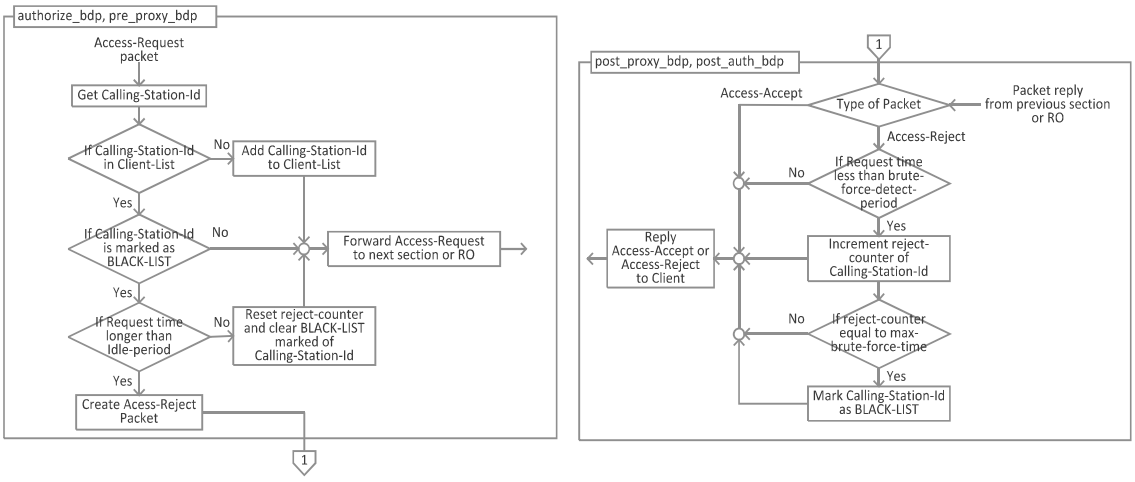
การพัฒนาการตรวจสอบและป้องกันการโจมตีแบบแบบบรูตฟอร์ซ (Brute-force Detection and Protection: BDP) สำหรับเครือข่าย eduroam นั้น เป็นการพัฒนาในลักษณะของโมดูลเพิ่มเข้าไปในโปรแกรม Radius เพื่อแทรกกระบวนการตรวจสอบและป้องกันการโจมตีเข้าไปในกระบวนการประมวลผลของโปรแกรม Radius โดยเพิ่มโมดูลเข้าไปทั้งด้านของ SP และด้าน IdP ดังภาพที่ 4



ภาพที่ 4 โมดูล BDP ในการประมวลผลของ Radius

โมดูลของ BDP ที่แทรกกระบวนการประมวลผลเข้าไปในการทำงานของ Radius มีจำนวน 5 ตำแหน่ง โดยหากต้องการป้องกันการโจมตีแบบบรูตฟอร์ซที่ด้านของ SP ต้องแทรกกระบวนการทำงานของ BDP ลงไป 3 ตำแหน่ง ประกอบด้วยฟังก์ชั่น pre_proxy_dbp post_proxy_bdp และ post_auth_bdp แต่หากต้องการป้องกันการโจมตีที่ด้านของ IdP จะแทรกกระบวนการของ BDP ลงไป 2 จุด ประกอบด้วยฟังก์ชั่น authorize_bdp และ post_auth_bdp

การทำงานของ pre_proxy_bdp และ authorize_bdp ทำหน้าที่ 3 หน้าที่ ประกอบด้วย สร้างรายการเครื่องลูกข่าย (Client-List) โดยใช้ข้อมูลการร้องขอชื่อ Calling-Station-Id เป็นตัวบ่งชี้เครื่องลูกข่าย ตรวจสอบสถานะของเครื่องลูกข่ายว่าเป็นเครื่องที่ถูกกำหนดว่าเป็นเครื่องที่พยายามโจมตีแบบบรูตฟอร์ซหรือไม่ (BLACK-LIST status) หากสถานะเป็นเครื่องที่พยายามโจมตีแบบบรูตฟอร์ซต้องดำเนินการตอบผลการร้องขอเป็น Access-Reject หรือปฏิเสธการร้องขอไปยังเครื่องลูกข่ายทันที และตรวจสอบระยะเวลาการทิ้งช่วงการพยายามโจมตีแบบบรูตฟอร์ซอย่างต่อเนื่องของเครื่องลูกข่าย (idle-period) หากเครื่องที่ถูกกำหนดสถานะว่าเป็นเครื่องพยายามโจมตีแบบบรูตฟอร์ซนั้นได้ทิ้งช่วงการร้องขอมากกว่าเวลาที่กำหนด จะเปลี่ยนสถานะกลับสู่สถานะปกติ ดังแสดงรายละเอียดในภาพที่ 5

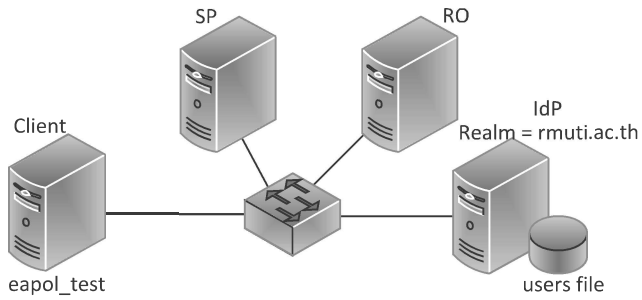


ภาพที่ 5 ขั้นตอนการทำงานในโมดูลของ BDP

การทำงานของ post_proxy_bdp และ authorize_bdp หากได้รับผลการร้องขอบริการเป็น Access-Reject จากส่วนก่อนหน้านี้ ดำเนินการบันทึกจำนวนครั้ง (reject-counter) และตรวจสอบความถี่การร้องขอ หากมีความถี่เกินกว่าที่กำหนด (max-brute-force-time) จะกำหนดสถานะของเครื่องลูกข่ายให้เป็นเครื่องที่พยายามโจมตีแบบบรูตฟอร์ซ (BLACK-LIST status) ทันที แต่หากได้รับผลการร้องขอบริการเป็น Access-Accept จากส่วนก่อนหน้านี้ ดำเนินการล้างข้อมูลความถี่การการร้องขอ และเพื่อเริ่มกระบวนการตรวจสอบรอบใหม่ต่อไป

ผลการวิจัย

การทดสอบประสิทธิภาพการทำงานโครงสร้างการเชื่อมต่อเครือข่ายสำหรับการทดสอบประสิทธิภาพ ประกอบด้วย เครื่องลูกข่ายสำหรับทดสอบการร้องขอบริการ โดยการใช้โปรแกรม eapol_test เครื่องแม่ข่าย SP ที่กำหนดคุณสมบัติให้ Radius ส่งต่อการร้องขอบริการของ rmuti.ac.th ไปยัง RO เครื่องแม่ข่าย RO กำหนดคุณสมบัติให้ Radius ส่งต่อการร้องขอบริการของ rmuti.ac.th ไปยัง IdP และเครื่องแม่ข่าย IdP ที่กำหนดคุณสมบัติให้ Radius ใช้ข้อมูลบัญชีผู้ใช้จากไฟล์ข้อความ (users) เพื่อให้สามารถตรวจสอบตัวตนของผู้ใช้ได้รวดเร็ว ดังแสดงรายละเอียดในภาพที่ 6



ภาพที่ 6 ผังการเชื่อมต่อเครือข่ายสำหรับการทดสอบ

วิธีการทดสอบนั้น ใช้การเขียนเป็นสคริปต์เพื่อวนรอบเรียกใช้โปรแกรม rad_eap_test + eapol_test (http://deployingradius.com/scripts/eapol_test/) เพื่อสร้างการร้องขอบริการหลายครั้งอย่างต่อเนื่อง และจับเวลาการทำงานตามจำนวนครั้งที่กำหนด รูปแบบคำสั่งสำหรับการร้องขอแต่ละครั้งคือ

```
rad_eap_test -H 192.168.1.11 -P 1812 -S testing123 -u 'user@rmuti.ac.th' -p 'password' \
-m IEEE8021X -s eduroam -e PEAP -2 MSCHAPv2
```

รูปแบบการทดสอบประสิทธิภาพนี้เป็นการทดสอบเพื่อวัดประสิทธิภาพที่แตกต่างกัน 3 กรณีคือ กรณีที่ไม่มีการทำงานของ BDP เพื่อวัดประสิทธิภาพปกติของระบบสำหรับใช้เปรียบเทียบกับกรณีที่มีการทำงานของ BDP ที่ด้าน SP และกรณีที่ให้ BDP ทำงานที่ด้าน IdP โดยมีการวัดประสิทธิภาพจากรูปแบบของการร้องขอบริการ 2 ลักษณะ คือ การร้องขอบริการที่ถูกต้องหรือการร้องขอบริการแบบปกติ (Request with Valid user) และการร้องขอบริการที่ไม่ถูกต้อง (Request with Invalid user) หรือการพยายามโจมตีแบบบรูตฟอร์ซ ในการทดสอบ จะวัดระยะเวลาที่ใช้ในการเรียกใช้โปรแกรมเพื่อร้องขอบริการจำนวน 1000 ครั้ง และแปลงเป็นอัตราความเร็วในการให้บริการ ผลการทดสอบประสิทธิภาพแสดงดังตารางที่ 1 และมีผลสรุปดังนี้

ตารางที่ 1 อัตราการตอบสนองการร้องขอบริการ (จำนวนครั้งต่อวินาที)

	Without BDP	BDP on IdP	BDP on SP
Request with Valid user	25	25	25
Request with Invalid user	27	76	89

- เมื่อเทียบความเร็วในการให้บริการของการร้องขอบริการแบบถูกต้อง ระหว่างที่ไม่มีการติดตั้งใช้งาน BDP และมีการติดตั้งใช้งาน BDP ทั้งที่ด้าน SP และด้าน IdP มีความเร็วเท่ากันที่ 25 ครั้งต่อวินาที หรือสรุปได้ว่า แม้จะมีการติดตั้งใช้งาน BDP ใน Radius แล้วก็ยังทำให้ประสิทธิภาพการบริการของ Radius มีเท่าเดิม
- ความเร็วในการให้บริการกรณีการร้องขอแบบถูกต้องเทียบกับการให้บริการกรณีการร้องขอแบบไม่ถูกต้องหรือการพยายามโจมตีแบบบรูตฟอร์ซนั้น พบว่า ความเร็วในการให้บริการกรณีไม่ได้ติดตั้งใช้งาน BDP จะช้ากว่ากรณีที่มีการติดตั้งใช้งาน BDP เล็กน้อย เป็นเพราะกระบวนการประมวลผลของ Radius ในกรณีของการร้องขอบริการแบบถูกต้องนั้นมีขั้นตอนการทำงานมากกว่าการประมวลผลการกรณีการร้องขอบริการแบบไม่ถูกต้อง
- ความเร็วในการให้บริการกรณีการร้องขอบริการแบบไม่ถูกต้องเมื่อมีการติดตั้งใช้งาน BDP ที่ด้าน IdP มีความเร็วกว่ากรณีไม่ได้ติดตั้งใช้งาน BDP 2.8 เท่า และกรณีการติดตั้งใช้งาน BDP ที่ด้าน SP มีเร็วกว่ากรณีการไม่ติดตั้งใช้งาน BDP 3.3 เนื่องจากเมื่อเครื่องลูกข่ายถูกกำหนดสถานะให้เป็นเครื่องที่พยายามโจมตีแบบบรูตฟอร์ซแล้ว การร้องขอในภายหลังของเครื่องลูกข่ายนั้นถูกปฏิเสธทันทีในส่วน authorize โดยไม่มีการตรวจสอบตัวตนของการร้องขอนั้นอีก โดยความเร็วของการให้บริการร้องขอแบบผิดปกติเมื่อมีการติดตั้งใช้งาน BDP ที่ด้าน SP มีความเร็วมากกว่าการติดตั้งใช้งาน BDP ที่ด้าน IdP ที่ 1.2 เท่า เนื่องจากการปฏิเสธการร้องขอที่ด้าน SP ทำได้ทันทีโดยไม่ต้องส่งต่อการร้องขอผ่านไปยัง RO และ IdP ก่อนแล้วจึงดำเนินการปฏิเสธการร้องขอ

การติดตั้งใช้งาน BDP นั้น จะสามารถป้องกันการโจมตีระบบเครือข่ายแบบบรูตฟอร์ซได้ทั้งในด้าน SP และด้าน IdP โดยทั้งสองด้านสามารถติดตั้งและทำงานอิสระจากกัน มีข้อดีและข้อเสียต่างกัน การติดตั้งใช้งาน BDP ที่ด้าน SP นั้น เป็นการป้องกันที่ต้นทาง มีข้อดีคือ มีประสิทธิภาพสูงกว่า เพราะเมื่อพบว่ามีเครื่องลูกข่ายพยายามโจมตีแบบบรูตฟอร์ซแล้ว จะสามารถปฏิเสธการร้องขอของเครื่องลูกข่ายได้ทันที ระงับผลกระทบที่จะมีต่อ RO และ IdP ได้โดยไม่ต้องส่งต่อการร้องขอไปยัง RO และ IdP แต่มีข้อเสียคือ จำเป็นต้องมีการติดตั้ง BDP ใน SP ของทุกสถาบันที่เป็นสมาชิกของ eduroam ส่วนการติดตั้งใช้งาน BDP ที่ด้าน IdP นั้นมีข้อดีคือ สามารถป้องกันข้อมูลของผู้ใช้ของสถาบันของตนเองได้อย่างเต็มที่ โดยไม่ต้องอาศัย SP อื่น แต่มีข้อเสียคือ ยังคงมีข้อมูลการพยายามโจมตีแบบบรูตฟอร์ซถูกส่งต่อไปในเครือข่าย eduroam

อภิปรายและสรุปผลการวิจัย

บทความนี้นำเสนอการพัฒนาการตรวจสอบและป้องกันการโจมตีแบบบรูตฟอร์ซ (BDP) สำหรับใช้ในการบริการของเครือข่าย eduroam โดยการเพิ่มกระบวนการตรวจสอบและป้องกันการโจมตีเข้าไปในการทำงานของโปรแกรม Radius ที่ทำหน้าที่รับและประมวลผลการร้องขอบริการของเครื่องลูกข่าย วิธีการตรวจสอบใช้การนับจำนวนครั้งของการร้องขอบริการแบบไม่ถูกต้องในช่วงเวลาหนึ่งของเครื่องลูกข่ายแต่ละเครื่อง โดยหากมีจำนวนครั้งเกินกว่าที่

กำหนดจะถือว่าลูกข่ายเครื่องนั้นพยายามโจมตีเครือข่ายแบบบรูตฟอร์ซ และจะให้โปรแกรม Radius ปฏิเสธการร้องขอของเครื่องลูกข่ายนั้น จากการทดสอบประสิทธิภาพ พบว่าเมื่อติดตั้งใช้งาน BDP ใน Radius แล้ว ในขณะที่มีการร้องขอบริการแบบถูกต้องนั้นไม่ได้ทำให้ประสิทธิภาพการทำงานลดลง และยังสามารถปฏิเสธการร้องขอบริการแบบไม่ถูกต้องได้เร็วกว่ากรณีไม่ได้ติดตั้งใช้งาน การติดตั้งใช้งาน BDP นั้น จะสามารถป้องกันการโจมตีระบบเครือข่ายแบบบรูตฟอร์ซได้ทั้งในด้าน SP และด้าน IdP มีข้อดีและข้อเสียต่างกัน การติดตั้งใช้งาน BDP ที่ด้าน SP มีข้อดีคือ มีประสิทธิภาพสูงกว่า สามารถปฏิเสธการร้องขอของเครื่องลูกข่ายได้ทันทีเมื่อตรวจสอบว่าเครื่องลูกข่ายนั้นโจมตีเครือข่าย และระงับผลกระทบที่จะมีต่อ RO และ IdP ได้ ส่วนการติดตั้งใช้งาน BDP ที่ด้าน IdP นั้นมีข้อดีคือ สามารถป้องกันข้อมูลของผู้ใช้ของสถาบันของตนเองได้อย่างเต็มที่ แต่มีข้อเสียคือ ยังคงมีการส่งต่อข้อมูลการพยายามโจมตีเข้าไปในเครือข่าย eduroam บทความนี้นำเสนอโดยเน้นที่การพัฒนาจุดทดสอบและป้องกันการโจมตีแบบบรูตฟอร์ซให้กับบริการเครือข่าย eduroam โดยได้ใช้กระบวนการตรวจสอบการโจมตีแบบบรูตฟอร์ซที่ไม่ซับซ้อนอันเกิดจากการโจมตีที่ชัดเจน แต่สามารถปรับปรุงส่วนของกระบวนการตรวจสอบด้วยวิธีการที่ซับซ้อนขึ้นเพื่อให้รับรู้รูปแบบการโจมตีซับซ้อนขึ้นได้อีก

เอกสารอ้างอิง

มหาราช ทศศะ. (2555). *การวิเคราะห์ข้อมูลกิจกรรมการใช้งานไดเรกทอรีเซอร์วิส เพื่อตรวจสอบภัยคุกคามจากการโจมตีแบบบรูตฟอร์ซ (brute-force attack).* สารนิพนธ์วิทยาศาสตรมหาบัณฑิต สาขาวิชาวิทยาการคอมพิวเตอร์ ภาควิชาวิทยาการคอมพิวเตอร์และสารสนเทศ บัณฑิตวิทยาลัย มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ.

eduroam.uni.net.th. (2016). http://eduroam.uni.net.th/eduroam-th/index.php?var=index&lang=thai.

Fernando Bernal, Manuel Sanchez, Gabriel Lopez, Antonio F. Gomez-Skarmeta and Óscar Canovas. (2009). Trusted Network Access Control in the eduroam federation. *Third International Conference on Network and System Security*. 170 – 175.

Gabriel López, Óscar Cánovas, Antonio F. Gómez-Skarmeta and Manuel Sánchez. (2008). A proposal for extending the eduroam infrastructure with authorization mechanisms. *International Journal of Computer Standards & Interfaces*. *30*, 418–423.

I. Kim. (2012). Keypad against brute force attacks on smart phones. *International of The Institution of Engineering and Technology*. *6*(2), 71 – 76.

Robert H. Zakon. (2016). *"Hobbes' Internet Timeline 11*". http://www.zakon.org/robert/internet/timeline/.

Tomo Niizuma and Hideaki Goto. (2014). Centralized Online Sign-Up and Client Certificate Issuing System for Eduroam. *38th Annual International Computers, Software and Applications Conference Workshops*. 174 - 179.