การเสริมสร้างประสิทธิภาพของระบบควบคุมการเข้าถึงเครือข่ายสำหรับการบันทึกข้อมูลล็อกที่ถูกต้อง

The Enhancement of Egress NAC Systems for Valid Logging

อรรถพล สุวรรณษา,[1] สมนึก พ่วงพรพิทักษ์[1]

Atthapol Suwannasa,[1] Somnuk Puangpronpitag[1]

Received: 28 September 2014 ; Accepted: 14 November 2014

บทคัดย่อ

ระบบควบคุมการเข้าถึงเครือข่ายมีความสำคัญคือใช้ยืนยันตัวตนผู้ใช้ก่อนเข้าใช้งานอินเทอร์เน็ต หนึ่งในส่วนประกอบสำคัญของระบบคือการเก็บข้อมูลการเข้าใช้งานของผู้ใช้ (Log) จากข้อกำหนดของ พรบ. ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ ปี พ.ศ. 2550 หลายหน่วยงานลงทุนจำนวนมหาศาลกับระบบควบคุมการเข้าถึงเครือข่ายและการเก็บ Log ผู้ใช้ และใช้ MAC address เป็นข้อมูลสำคัญที่ใช้ในการอ้างอิงเครื่องผู้ใช้ แต่เครือข่ายเหล่านี้จะต้องมีการเชื่อมต่อผ่านหลาย Hop ทำให้ค่า MAC address ของผู้ใช้เปลี่ยนแปลงไปในแต่ละ Hop ระบบจึงเก็บข้อมูลดังกล่าวผิดพลาดและล้มเหลวต่อการนำข้อมูล Log มาใช้งาน ดังนั้น งานวิจัยนี้จึงนำเสนอวิธีการแก้ไขปัญหาดังกล่าวด้วยการพัฒนาระบบควบคุมการเข้าถึงเครือข่ายที่มีส่วนประกอบของเทคโนโลยี JAVA Applet เพื่อใช้ในการดึงค่า MAC Address ที่ถูกต้องจากเครื่องผู้ใช้ ผลการพัฒนาระบบพบว่าสามารถเก็บบันทึกข้อมูลการเข้าใช้งานของผู้ใช้ได้อย่างถูกต้อง โดยที่ไม่ลดประสิทธิภาพในการทำงาน

คำสำคัญ: ระบบควบคุมการเข้าถึงเครือข่าย ข้อมูลล็อกผิดพลาด หมายเลขแมคแอดเดรส

Abstract

In Egress Network Access Control (egress NAC) it is crucial to authenticate users before they access the Internet. One of the most important parts of the egress NAC is the network traffic log system. According to the Thailand Computer Crime Act of 2007, several organizations spend a lot of money for egress NAC and log keeper systems. In many log systems, MAC Address is used to identify each user's machine. However, most systems are used to control multi-hop connections, in which MAC addresses are changed in each hop. So, these systems end up with storing the invalid user's MAC addresses. When the systems keep the invalid information in their log files, these log files cannot be used as valid evidence to point out the real users. Hence, this paper proposes an enhanced solution by using JAVA Applet technology to collect the real user's MAC addresses. The experimental results have demonstrated that our system can keep valid log information in log files without reducing the system performance.

Keywords: Network Access Control, Invalid Log, MAC Address

[1] *อาจารย์, ภาควิชาวิทยาการคอมพิวเตอร์, คณะวิทยาการสารสนเทศ, มหาวิทยาลัยมหาสารคาม อำเภอกันทรวิชัย จังหวัดมหาสารคาม 44150*

[1] *Lecturer, Department of Computer Science, Faculty of Informatics, Mahasarakham University, Kantharawichai District, Maha Sarakham 44150, Thailand*

บทนำ

ในปัจจุบันระบบควบคุมการเข้าถึงเครือข่ายจากภายในสู่ภายนอก (Egress Network Access Control หรือ Egress NAC) มีความจำเป็นอย่างยิ่งในการควบคุมการใช้งานของผู้ใช้ภายในที่สื่อสารกับเครือข่ายภายนอกอย่างอินเทอร์เน็ต โดยข้อมูลของผู้ใช้แต่ละคนจะถูกเก็บบันทึกลงในบันทึกข้อมูลการจราจรทางเครือข่าย (Network Traffic Log) เพื่อเป็นการยืนยันพฤติกรรมการเข้าถึงเครือข่ายภายนอกของผู้ใช้แต่ละราย โดยหากมีการกระทำความผิดก็สามารถที่จะใช้ข้อมูล Log เพื่อใช้ในการตรวจสอบหาตัวผู้กระทำความผิดและเป็นหลักฐานในการมัดตัวผู้กระทำความผิดได้ ดังนั้นการติดตั้ง Egress NAC จึงมีความจำเป็นอย่างยิ่งต่อทุกหน่วยงานหรือองค์กร

ระบบ Egress NAC ทั้ง Open Source Products เช่น Coovachilli[1] Chilispot[2] และ pfSense[3] หรือ Commercial Products ที่มีมูลค่าค่อนข้างสูง เช่น Consentry[4] Sangfor IAM[5] หรือ BlueSocket[6] เป็นต้น ถูกนำมาติดตั้งในหลายหน่วยงานเพื่อควบคุมผู้ใช้และเก็บ Log การใช้งาน แต่ระบบเหล่านี้ยังคงเผชิญกับปัญหาการการปลอมแปลงหมายเลขแมคแอดเดรส (MAC Address Spoofing[7]) ทำให้ผู้โจมตีสามารถลักลอบเข้าใช้งานทรัพยากรเครือข่ายได้

จากปัญหาข้างต้น จึงได้มีการพัฒนาระบบ Egress NAC ที่สามารถป้องกันปัญหา MAC Address Spoofing ได้ คือ ISAN-SNAC[8] โดยตัวระบบจะมีการติดตั้ง Lightweight Agent ที่เครื่องผู้ใช้งานตัวจริงหลังจากที่ผ่านการยืนยันตัวตนเรียบร้อยแล้ว เพื่อให้สามารถแยกแยะผู้ใช้งานตัวจริงกับผู้โจมตีได้ แต่ระบบดังกล่าวมีข้อบกพร่องในการเก็บข้อมูล Log อย่าง MAC Address ของผู้ใช้ เมื่อต้องส่งผ่านเครือข่ายขนาดใหญ่ที่ประกอบไปด้วยเครือข่ายย่อยๆ หลายเครือข่าย ซึ่งข้อมูล MAC Address ที่เก็บจะมีความผิดพลาด โดยแทนที่จะเก็บเป็น MAC Address ของผู้ใช้ แต่กลับเก็บเป็น MAC Address ของ Router หรืออุปกรณ์เครือข่ายตัวที่เชื่อมต่อโดยตรงกับ Egress NAC Server ซึ่งปัญหานี้ไม่ได้เป็นเพียงปัญหาของ ISAN-SNAC เท่านั้น แต่ระบบ Egress NAC ทั้ง Open Source และ Commercial ที่กล่าวมาในข้างต้นและระบบ อื่นๆ อีกหลายระบบ ยังคงมีปัญหาการเก็บ Log ผิดพลาดอันมีสาเหตุมาจากเครื่อง Egress NAC Server (ตั้งอยู่ที่เครือข่ายหลัก เช่น Server Farm) อยู่ต่างเครือข่ายกับเครื่องผู้ใช้ (เครือข่ายย่อย)

ปัญหาการเก็บข้อมูล MAC Address ผิดพลาดทำให้ระบบ Egress NAC และ Log ที่หน่วยงานหรือองค์กรลงทุกอย่างมหาศาลทำงานโดยเปล่าประโยชน์ และไม่สามารถใช้เป็นหลักฐานในการมัดตัวผู้กระทำความผิดได้ตามข้อกำหนดของ พรบ. ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ ปี พ.ศ. 2550 ได้

งานวิจัยนี้ มุ่งเน้นที่จะออก ระบบ Egress NAC โดยแก้ไขข้อบกพร่องของระบบ Egress NAC ส่วนใหญ่ที่มีปัญหาการเก็บ Log ผิดพลาด ในกรณีที่ติดตั้ง Egress NAC ในเครือข่ายขนาดใหญ่เพื่อควบคุมเครือข่ายย่อยภายในหลายๆ เครือข่าย เช่น เครือข่ายของมหาวิทยาลัย เป็นต้น โดยทำการพัฒนาต่อยอดจาก ISAN-SNAC ที่ได้มีการนำเสนอก่อนหน้า

ทฤษฎีที่เกี่ยวข้อง

ระบบยืนยันตัวตนแบบภายในสู่ภายนอก (Egress NAC)

ระบบ Egress Network Access Control หรือ Egress NAC เป็นระบบที่ใช้ในการควบคุมผู้ใช้งานภายในก่อนออกสู่เครือข่ายภายนอก ระบบ Egress NAC ส่วนใหญ่ผู้ใช้จะต้องผ่านการยืนยันตัวตน เช่น กรอกข้อมูล Username และ Password เป็นต้น หลังจากที่ผู้ใช้กรอกข้อมูลเพื่อยืนยันตัวตน Egress NAC ก็จะทำการตรวจสอบกับฐานข้อมูล หากพบในฐานข้อมูลก็จะทำการเก็บข้อมูล IP Address หรือ MAC Address เพื่อใช้ในการตรวจสอบว่าผู้ใช้ที่มี IP Address และ MAC Address ดังกล่าวผ่านการยืนยันตัวตนแล้ว ไม่จำเป็นต้องยืนยันตัวตนอีกจนกว่าจะ Logout หรือเวลาในการใช้งานหมด (Session Timed Out) และยังส่งต่อข้อมูลของผู้ใช้ เช่น Username IP Address MAC Address และ เวลาของการ Login/Logout ไปเก็บบันทึกเป็น Log ของผู้ใช้

หมายเลข MAC Address

ในการสื่อสารบนระบบเครือข่าย การที่เครื่องลูกข่ายจะสามารถสื่อสารได้จำเป็นต้องใช้ IP Address และ MAC Address (Media Access Control Address) ในการสื่อสาร ซึ่ง IP Address ส่วนใหญ่จะถูกแจกจ่ายมาจาก DHCP Server หรือผู้ใช้สามารถทำการตั้งค่าหมายเลข IP Address ของตนเองแบบ Static ให้ถูกต้องกับเครือข่ายที่ใช้งานอยู่ ส่วนหมายเลข MAC Address ถูกกำหนดมาจากทางผู้ผลิต โดยการสื่อสารระดับ MAC Address จะทำงานอยู่ในระดับชั้นที่ 2 ของ OSI Model นั่นทำให้การสื่อสารระบบ MAC ไม่สามารถสื่อสารข้ามเครือข่ายได้ จึงต้องอาศัย IP Address ร่วมกับ MAC Address สื่อสารทีละ Hop หากต้องมีการสื่อสารไปยังเครือข่ายอื่นๆ ก็จะอาศัยความสามารถของ Address Resolution Protocol (ARP)[9] ในการสอบถามหมายเลข MAC Address ของปลายทางเพื่อที่จะสื่อสารในแต่ละ Hop

ระบบเครือข่ายที่ใช้งานในประเทศไทยและอีกหลายแห่งทั่วโลก ส่วนใหญ่ยังคงเป็น IPv4 ซึ่งหมายเลข MAC

Address ถูกกำหนดให้มีขนาด 6 ไบต์ หรือ 48 บิต (8 บิต = 1 ไบต์) จากทางผู้ผลิตอุปกรณ์เครือข่าย

ตัวอย่างของ MAC address:
00-0C-G1-54-29-E3

3 ไบต์แรก (00-0C-G1) ระบุถึงโรงงานผู้ผลิต ค่านี้ได้ถูกกำหนดมาจาก Institute of Electrical and Electronics Engineers หรือ IEEE ส่วน 3 ไบต์หลัง (54-29-E3) ถูกกำหนดโดยโรงงานผู้ผลิต แต่ในบางผู้ผลิตก็ไม่ได้กำหนด 3 ไบต์แรกตามมาตรฐาน

การเก็บข้อมูล Log ที่ผิดพลาด

เนื่องด้วย พรบ. ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ ปี พ.ศ. 2550 ทุกหน่วยงานต้องติดตั้งระบบยืนยันตัวตนเพื่อทำการตรวจสอบผู้ใช้และเก็บ Log การเข้าใช้งานของผู้ใช้ ประกอบไปด้วยข้อมูลดังต่อไปนี้

1) ข้อมูล Log ที่มีการบันทึกไว้เมื่อมีการเข้าถึงระบบเครือข่าย

2) ข้อมูลเกี่ยวกับวัน และเวลาติดต่อของเครื่องที่เข้ามาใช้บริการและเครื่องให้บริการ

3) ข้อมูลเกี่ยวกับชื่อที่ระบุตัวตนผู้ใช้

4) ข้อมูลหมายเลขชุดอินเทอร์เน็ตที่ถูกกำหนดให้โดยระบบผู้ให้บริการ (IP Address)

5) ข้อมูลที่บอกถึงหมายเลขสายที่เรียกเข้ามา (เช่น MAC Address)

แต่ในเครือข่ายขนาดใหญ่ที่จะต้องควบคุมเครือข่ายขนาดย่อยหลายเครือข่าย ดัง Figure 1 การเก็บ MAC Address ให้ถูกต้องตามผู้ใช้งานจริงๆ ยังมีความผิดพลาดเนื่องจาก MAC Address สื่อสารได้เฉพาะเครือข่าย LAN (Local Area Network) เดียวกัน แต่ Egress NAC Sever มักถูกติดตั้งที่ Core Layer ของระบบ ซึ่งอยู่ต่างเครือข่ายกับเครื่องผู้ใช้ (จะต้องมีการส่งผ่านข้อมูลหลาย Hop) หมายเลข MAC Address ที่ได้ จะเป็นหมายเลขของอุปกรณ์ตัวที่เชื่อมต่อกับ Egress NAC โดยตรง (เช่น 00:21:5b:42:3a:68 ที่ Switch ดัง Figure 1) ไม่ได้เป็น MAC Address ของผู้ใช้จริง (เช่น c8:a3:b9:d9:2f:5d ของเครื่อง User ใน Figure 1) นั่นทำให้การเก็บข้อมูล MAC Address ผิดพลาด อันส่งผลให้การนำไปใช้เป็นหลักฐานตาม พรบ. ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ล้มเหลว

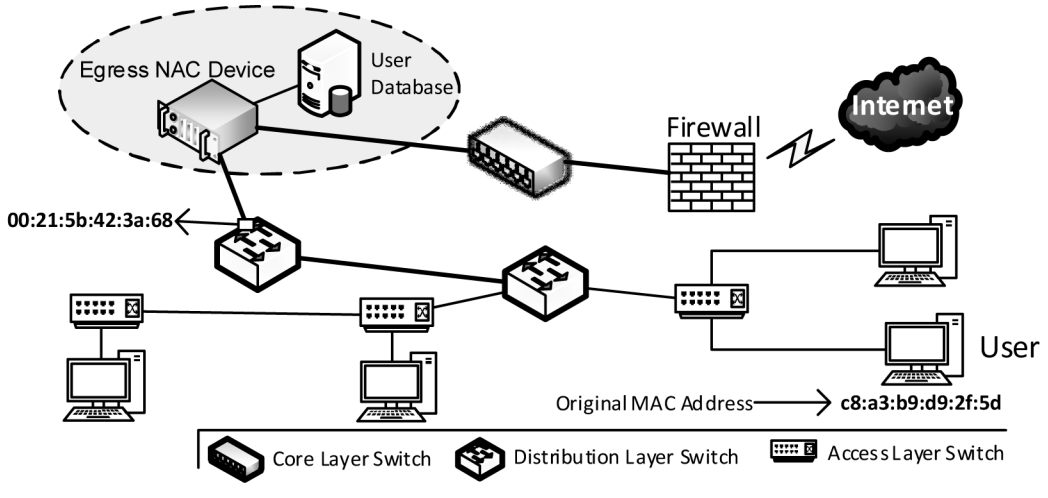

Figure 1 Egress NAC Connection Scenario

ระบบ Egress NAC ในปัจจุบัน

ระบบ Egress NAC ที่เป็น Open Source ส่วนใหญ่มีคุณสมบัติในการควบคุมเครือข่ายเพียงหนึ่งเครือข่าย เช่น Coovachilli[1] Chilispot[2] และ pfSense[3] จึงสามารถที่จะเก็บข้อมูล MAC Address ได้อย่างถูกต้อง เนื่องจากไม่ได้มีการเชื่อมต่อผ่านหลาย Hop ในเครือข่าย ดังนั้น เครื่องของผู้ใช้จึงสามารถสื่อสารไปที่ Egress NAC Server โดยตรง แต่หากต้องการตรวจสอบเครือข่ายย่อยๆ หลายเครือข่าย จะต้องใช้จำนวน Server เท่ากับจำนวนเครือข่าย ซึ่งเป็นการสิ้นเปลืองและยากต่อการควบคุม

ระบบที่เป็น Commercial ส่วนใหญ่จะมาในรูปแบบของ Appliance Box เช่น Consentry[4] Sangfor IAM[5] (ที่กำลังใช้งานในมหาวิทยาลัยมหาสารคาม) หรือ BlueSocket[6] โดยถูกออกแบบมาเพื่อรองรับผู้ใช้จำนวนมากที่สื่อสารมาจากเครือข่ายย่อยหลายเครือข่ายได้ ตัวอุปกรณ์มักถูกติดตั้งที่ Core Layer ของระบบเครือข่าย (เช่น NAC Device ใน Figure 1)

แต่เนื่องด้วยระบบเครือข่ายจะสื่อสารแบบ Hop by Hop นั่นคือ Packet จากต้นทางจะถูกส่งไปยังปลายทางผ่านหลายอุปกรณ์เครือข่าย ค่า MAC Address ใน Packet จะมีการเปลี่ยนแปลงตามอุปกรณ์นั้นๆ ซึ่งเมื่อ Packet ส่งไปถึง Egress NAC Device ค่า MAC Address ก็จะเปลี่ยนเป็นของอุปกรณ์เครือข่ายล่าสุดที่เชื่อมต่อกับตัว NAC Device ซึ่งไม่ใช่ค่าเดิมที่มาจากผู้ใช้ตัวจริง หากนำค่านี้ไปเก็บใน Log ก็จะทำให้ข้อมูลที่เก็บผิดพลาด

จากการทดลองของ สมนึก พ่วงพรพิทักษ์[10] ได้แสดงให้เห็นว่า commercial NAC products ที่ใช้อยู่หลายยี่ห้อ เช่น Consentry ทำการเก็บ log ในส่วน MAC address ของผู้ใช้ผิดพลาด หรือถูกตั้งค่าไม่ให้เก็บ MAC address ของผู้ใช้ระบบ NAC เลย ซึ่งไม่ตรงตามประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่องหลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2550 ได้กำหนดไว้

จากปัญหาดังกล่าวทำให้ไม่สามารถที่จะนำข้อมูล Log ไปใช้ในการมัดตัวผู้กระทำความผิดได้ หรือข้อมูลมีความผิดพลาดในการชี้ตัวผู้กระทำความผิด และแม้ว่าได้มีการเสนอวิธีการป้องกัน MAC Address Spoofing โดยให้ชื่อว่า ISAN-SNAC[8] ซึ่งมีประสิทธิภาพในการป้องกันปัญหา MAC Address Spoofing แต่ระบบดังกล่าวออกแบบมาเพื่อใช้งานในเครือข่ายเดียวหากนำไปใช้ควบคุมหลายเครือข่ายข้อมูล Log ของผู้ใช้ก็จะมีการบันทึกข้อมูลผิดพลาดตามที่กล่าวมาแล้วในข้างต้น

ออกแบบวิธีการรายงานข้อมูลล็อกที่ถูกต้อง

เนื่องจากปัญหาในการเก็บ Log ไม่ถูกต้องในเครือข่ายขนาดใหญ่ คือ Egress NAC Device ไม่ได้เชื่อมต่อโดยตรงกับเครือข่ายของเครื่องของผู้ใช้ จึงไม่สามารถใช้ ARP ในการสอบถาม MAC Address ของเครื่องผู้ใช้โดยตรงได้ งานวิจัยนี้ได้พัฒนาต่อยอดจาก ISAN-SNAC[8] ที่มีคุณสมบัติในการป้องกัน MAC Address Spoofing แต่ยังคงมีปัญหาในการเก็บข้อมูล Log ของ MAC Address ที่ผิดพลาด โดยระบบ NAC ดังกล่าว ได้มีการ ติดตั้ง JAVA Applet ในเครื่องผู้ใช้ เพื่อที่จะทำการดึงเอาข้อมูล Packet ของผู้ใช้ไปสร้างเป็น Authentication Visa เพื่อเปิดทางให้เฉพาะ Packet ที่ผ่านการยืนยันตัวตนสามารถสื่อสารได้

จากแนวคิดในการใช้เทคโนโลยีของ JAVA Applet ใน ISAN-SNAC ทำให้มีการพัฒนาระบบ JAVA Applet ขึ้นใหม่ในงานวิจัยนี้ โดยตัว Applet มีหน้าที่ในการดึงเอาค่า MAC Address ของเครื่องผู้ใช้ เพื่อส่งกลับไปยัง ตัว NAC Server เพื่อทำการเก็บ Log โดยมีขั้นตอนการทำงานดังนี้

การทำงานโดยรวมของระบบ

ระบบ Egress NAC แบ่งการทำงานออกเป็น 2 ระดับชั้น (Upper Layer และ Lower Layer ดัง Figure 2) โดยในส่วนของ Upper Layer เริ่มจากผู้ใช้ทำการป้อน Username และ Password ผ่านหน้า Login.php จากนั้นทำการดึงเอาข้อมูล MAC Address ของผู้ใช้ผ่าน Applet แล้วทำการส่งข้อมูลของผู้ใช้ไปตรวจสอบที่ RADIUS ที่ทำการเชื่อมต่อกับ LDAP ซึ่งเป็นฐานข้อมูลที่เก็บข้อมูลผู้ใช้หากว่ากระบวนการตรวจสอบผู้ใช้สำเร็จ RADIUS ก็จะทำการเก็บ Log ของผู้ใช้ และที่ Login.php ก็จะทำการส่งผ่าน ข้อมูลผู้ใช้ (ประกอบไปด้วย Username, IP Address, MAC Address) ไปที่ Core Service โดยส่งผ่านที่ XML-RPC

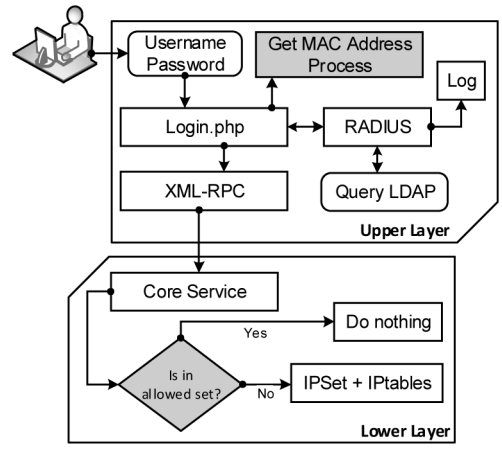

Figure 2 Egress NAC Operation

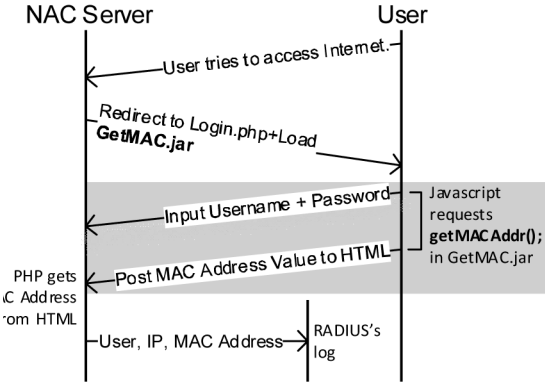

Figure 3 Process to get a client's MAC Address

ในส่วนของ Lower Layer เมื่อมีการติดต่อจาก XML-RPC นั่นแสดงว่ามีการส่งข้อมูลผู้ใช้ (ประกอบไปด้วย Username, IP Address, MAC Address) ที่ผ่านการยืนยันตัวตนเพื่อที่จะขอให้ Core Service อนุญาตให้ผู้ใช้ดังกล่าวสามารถสื่อสารได้ โดยข้อมูล IP Address ที่ได้รับ จะถูกนำไปตรวจสอบว่าอยู่ใน Set ที่ได้รับการอนุญาตแล้วหรือไม่ หากไม่

ก็จะทำการเพิ่ม IP Address เข้าไปใน Set แต่ถ้ามีข้อมูลอยู่แล้วใน Set นั่นแสดงว่าผู้ใช้สามารถสื่อสารได้อยู่ก่อนแล้ว ก็จะไม่ทำการเพิ่มข้อมูลเข้าไปใน Set

ขั้นตอนการดึงค่า MAC Address จากเครื่องผู้ใช้

ในส่วนของกระบวนการดึงค่า MAC Address จริงจากเครื่องผู้ใช้มีขั้นตอนดัง Figure 3 เริ่มจากการที่ผู้ใช้ทำการร้องขอไปยังปลายทางใน Internet ซึ่งจะมี Packet ของผู้ใช้วิ่งผ่านไปยังตัว NAC Server หากยังไม่ได้ผ่านการยืนยันตัวตน ที่ NAC Server ก็จะทำการ Redirect Packet ของผู้ใช้ไปที่ Login.php โดยในขั้นตอนนี้จะมีการติดตั้ง GetMAC.jar (ถูกพัฒนาขึ้นในการดึงค่า MAC Address) โดยทำการ Pre-Load ไว้ที่เครื่องของผู้ใช้ โดยผู้ใช้จะต้องทำการยอมรับ Applet ที่จะถูกติดตั้ง เมื่อติดตั้ง GetMAC.jar สำเร็จ ผู้ใช้ป้อน Username และ Password เมื่อผู้ใช้คลิกเพื่อที่จะส่งข้อมูลไปยืนยันตัวตนที่ Server ก็จะมีการเรียกใช้ Javascript เพื่อที่จะเรียก function getMACAddr(); ที่เขียนไว้ใน GetMAC.jar ซึ่ง function ดังกล่าวทำการดึงค่า MAC Address และส่งค่ากลับไปที่ Javascript หลังจากนั้นค่าจะถูก Post ไปที่ HTML Form และ PHP ทำการดึงค่าจาก HTML Form เพื่อที่จะนำค่า MAC Address ที่ถูกต้องไปเก็บไว้ใน RADIUS's log รวมกับข้อมูลของผู้ใช้ เช่น Username IP Address หรือ เวลาในการเข้าใช้งาน เพื่อให้ตรงตามข้อกำหนดของ พรบ. ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ ปี พ.ศ. 2550

พัฒนาระบบ

ระบบที่ได้ทำการพัฒนาต่อยอดจาก ISAN-SNAC โดยประกอบไปด้วย 3 ส่วนหลักๆ ได้แก่

1) ส่วนของ Core Service เพื่อที่จะเพิ่มความเร็วในการตรวจสอบ Packet ของผู้ใช้ ตัว Egress NAC ทำการพัฒนาโดยใช้ IPSet 4.2[11] เพื่อที่จะทำการสร้าง Set ที่ใช้ในการตรวจสอบ IP Address ของผู้ใช้ที่ผ่านการยืนยันตัวตนเรียบร้อยแล้ว โดยควบคุมการเพิ่มลบ IP Address ด้วยโปรแกรมที่พัฒนาด้วยภาษา C และใช้ IPtables 1.4.4[12] ในการกรอง Packet ของผู้ใช้

2) ส่วนติดต่อผู้ใช้ ทำการพัฒนาด้วย PHP ซึ่งจะใช้ในการควบคุม Session ผู้ใช้ (ประกอบไปด้วย login, logout, session terminating) อีกทั้งทำการติดตั้ง XML-RPC เพื่อใช้ในการติดต่อ Core Service และติดตั้ง PHP-RADIUS, PHP-LDAP เพื่อใช้ในการตรวจสอบผู้ใช้ และเก็บบันทึก Log การใช้งาน

3) ส่วนของการดึงค่า MAC Address จริง จากเครื่องผู้ใช้ พัฒนาโดยการใช้ JAVA Applet ซึ่งจะถูกติดตั้งโดยส่งผ่าน Web browser ของผู้ใช้ ซึ่งผู้ใช้ไม่ต้องเสียเวลาในการติดตั้งตัว Applet เอง

ระบบทั้งหมดพัฒนาบนระบบปฏิบัติการ CentOS Kernel 2.6 และทำการติดตั้ง Apache 2.0 Web Server เพื่อทำการเปิดการใช้งานในส่วนของ PHP นอกจากนี้สนับสนุนการเชื่อมต่อแบบ Bridge Mode นั่นคือ ผู้ดูแลระบบไม่ต้องทำการเปลี่ยนแปลงการตั้งค่าต่างๆ ในระบบเครือข่าย เพียงนำระบบที่พัฒนาไปติดตั้งในส่วนของ Core Layer ก็สามารถใช้งานได้ ซึ่งลดความยุ่งยากในการตั้งค่า

การเชื่อมต่อเครือข่าย

เครือข่ายที่ใช้ในการทดลองได้มีการเชื่อมต่อดัง Figure 1 ซึ่งเป็นลักษณะของการเชื่อมต่อในเครือข่ายขนาดใหญ่ และเพื่อป้องกันปัจจัยภายนอกที่อาจส่งผลต่อความผิดพลาดของผลการทดลองเครือข่ายที่เชื่อมต่อจึงเป็นระบบปิด (test-bed) ที่ไม่มี Cross Traffic ใดๆ

Egress NAC Server ทำการติดตั้งระหว่าง Core Layer Switch และ Distribution Layer Switch ดัง Figure 1 ในส่วนของคุณสมบัติของ Server คือ Intel Xenon 2 processors with 4-GB RAM, 1-TB local hard disk, และ two 10 Base-T/100Base-TX/1000Base-TX interfaces และติดตั้งระบบปฏิบัติการ CentOS ซึ่งสนับสนุนการทำงานของ IPSet และ IPtables

เครื่องผู้ใช้ ทดลองด้วยเครื่อง PC ที่มีคุณสมบัติคือ Intel Core i5 3.30-GHz with 4-GB RAM, 320-GB local hard disk, และ Intel PRO/1000 network interface card โดยติดตั้ง JAVA Runtime Environment (JRE) version 7 update 67 เพื่อใช้ในการ Run JAVA Applet ที่ใช้ดึงค่า MAC Address

Core Layer Switch และ Distribution Layer Switch ที่ใช้คือ Cisco 2960 ที่ทำการ update firmware ใหม่[13] เพื่อให้สนับสนุนการทำงานของ IP Routing ในส่วนของ Access Layer Switch ใช้ 3com Gigabit Switch เพื่อที่จะเชื่อมต่อกับเครื่องผู้ใช้

การวัดประสิทธิภาพและประสิทธิผล

การวัดประสิทธิผล (Effectiveness)

เนื่องจากระบบที่พัฒนามีกระบวนการดึงค่า MAC Address ที่ถูกต้องผ่านตัว JAVA Applet ที่ได้พัฒนาขึ้น ดังนั้นระบบจึงมีประสิทธิผลในการเก็บข้อมูล Log ที่ถูกต้อง โดยหมายเลข MAC Address ที่ได้เป็นหมายเลขที่ได้มาจากเครื่องผู้ใช้งานตัวจริง ดัง Figure 4 (C8-A3-B9-D9-2F-5D) ไม่ได้เป็นหมายเลขที่มาจากอุปกรณ์เครือข่ายตัวล่าสุดที่เชื่อมต่อกับตัว Egress NAC Server

จากข้อมูล Log ที่ได้ พบว่า ข้อมูลมีความถูกต้องและสามารถนำไปเป็นหลักฐานในการชี้ตัวผู้กระทำความผิดได้

```
Fri Sep  5 19:32:36 2014
        Acct-Session-Id = "d3d048041e3b347e"
        Acct-Status-Type = Start
        Acct-Authentic = Local
        NAS-Port-Type = Ethernet
        User-Name = "test"
        Framed-IP-Address = 192.168.0.2
        Calling-Station-Id = "C8-A3-B9-D9-2F-5D"
        NAS-Identifier = "SNAC-01"
        NAS-IP-Address = 192.168.4.1
        NAS-Port = 1
        Acct-Unique-Session-Id = "06096d0c50c52d91"
        Timestamp = 1406896356
```

Figure 4 Authentication log from RADIUS

การวัดประสิทธิภาพ (Efficiency)

การวัดประสิทธิภาพของระบบ Egress NAC ที่พัฒนามุ่งเน้นที่จะทดสอบความเร็วในการดึงค่า MAC Address จากเครื่องของผู้ใช้ และความเร็วทั้งหมดเริ่มจากผู้ใช้ยืนยันตัวตนจนสิ้นสุดกระบวนการ เทียบกับระบบที่ไม่ได้ติดตั้ง JAVA Applet เพื่อใช้ดึงค่า MAC Address โดยแบ่งออกเป็นสองส่วนคือ ส่วนเฉพาะความเร็วในการดึงค่า MAC Address ของ JAVA Applet และ ส่วนของความเร็วรวมในการยืนยันตัวตนของผู้ใช้งาน

ส่วนแรก ทำการวัดค่าความเร็วในการทำงานของ function getMACAddr(); โดยเริ่มตั้งแต่เรียกใช้งาน Applet ผ่าน Web Browser จนกระทั่งส่งค่า MAC Address กลับไปที่ Javascript ซึ่งทำการทดลองโดยการ Login เข้าสู่ระบบจากเครื่องผู้ใช้ 1 เครื่อง จำนวน 30 ครั้ง โดยต้องการทราบถึงความเร็วในการดึงค่า MAC Address ว่าส่งผลกระทบต่อการใช้งานของผู้ใช้หรือไม่

ส่วนที่สอง เริ่มจากผู้ใช้ทำการส่ง Username และ Password มาที่ Egress NAC Server จนกระทั่งยืนยันตัวตนสำเร็จ (ประกอบไปด้วยขั้นตอนย่อยๆ คือการบันทึก Log และการนำ IP Address ของผู้ใช้ไปเก็บไว้ใน Set ของผู้ใช้ที่ผ่านการยืนยันตัวตนแล้ว) โดยทดลองจากเครื่อง 1 เครื่อง ให้ผู้ใช้ Login จำนวน 30 ครั้ง เพื่อให้ทราบว่าระบบที่มีกระบวนการของ Applet เพิ่มขึ้นมาจะสร้างความล่าช้าในการทำงานหรือไม่

ผลการทดลอง

ในการวัดประสิทธิภาพส่วนแรก นั่นคือ การวัดความเร็วในการดึงค่า MAC Address ผลที่ได้ ปรากฏดัง Figure 5 (a) จากรูปจะเห็นว่า ในการทดสอบแต่ละครั้ง ค่าที่ได้จะไม่เกิน 0.044 วินาที (ค่าเฉลี่ย = 0.039±0.001 วินาที ที่ช่วงความเชื่อมั่น 95%) ซึ่งเป็นค่าเวลาที่น้อยมาก นั่นแสดงว่า การดึงค่า MAC Address ของเครื่องผู้ใช้สามารถทำได้อย่างรวดเร็ว ไม่ส่งผลกระทบต่อการใช้งานของผู้ใช้

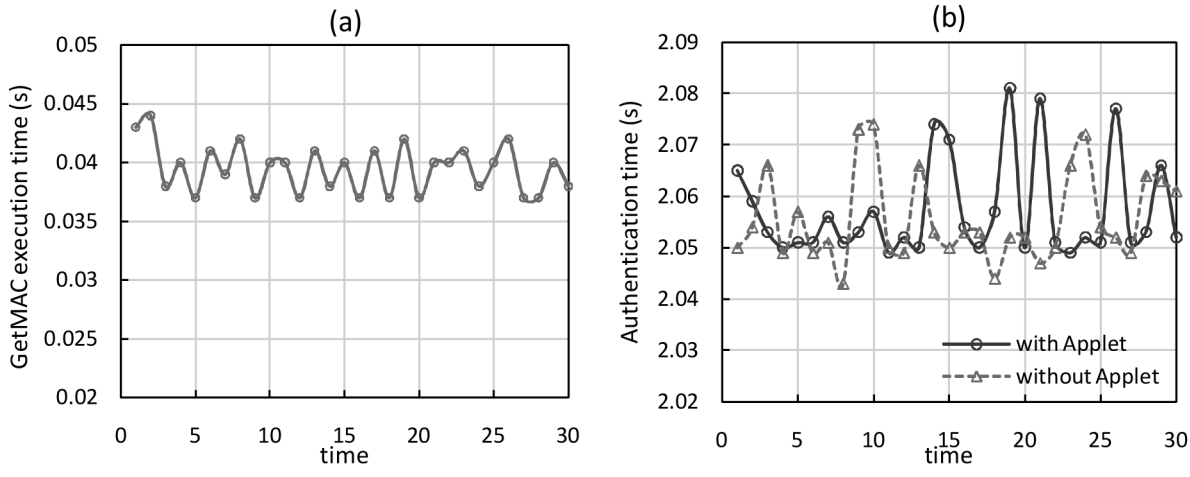

Figure 5 Efficiency Evaluation: (a) execution time for the applet to get MAC address (in second), (b) authentication time of user (in second)

สำหรับการวัดประสิทธิภาพในส่วนที่สอง นั่นคือการวัดเวลาทั้งหมดที่ผู้ใช้ทำการยืนยันตัวตนเข้าสู่ระบบ โดยเปรียบเทียบระหว่างระบบที่มีกระบวนการทำงานของApplet เพื่อดึงค่า MAC Address และระบบที่ไม่มีกระบวนการดังกล่าว โดยผลการทดลองปรากฏดัง Figure 5 (b) จากผลที่ได้แสดงให้เห็นว่า ค่าเวลารวมในการยืนยันตัวตนมีค่าที่ใกล้เคียงกันมาก โดยระบบที่มีกระบวนการทำงานของ Applet มีค่าเฉลี่ยเวลายืนยันตัวตนอยู่ที่ 2.057±0.003 วินาที ที่ช่วงความเชื่อมั่น 95% ส่วนระบบที่ไม่มีกระบวนการดังกล่าวมีค่าเฉลี่ยอยู่ที่ 2.055±0.003 วินาที ที่ช่วงความเชื่อมั่น 95% นั่นคือ

ระบบที่เพิ่มการทำงานของ Applet ไม่ได้ส่งผลต่อการลดประสิทธิภาพการทำงานของระบบยืนยันตัวตน จากกระบวนการออกแบบที่ได้กล่าวมาแล้วในข้างต้น ตัว Applet ได้ถูก Pre-Load เพื่อติดตั้งก่อนหน้าที่ผู้ใช้จะส่งข้อมูลยืนยันตัวตน ดังนั้น การเรียกใช้งานเพื่อที่จะดึงค่า MAC Address จึงไม่ได้มีความล่าช้า ซึ่งจะใช้เวลาเพียงเล็กน้อยเท่านั้น (ดังแสดงใน Figure 5 (a))

สรุปผล

ระบบ Egress NAC จำเป็นอย่างยิ่งในการยืนยันตัวตน และเก็บบันทึก Log การใช้งานผู้ใช้ หลายหน่วยงานลงทุนซื้อผลิตภัณฑ์ NAC เพื่อควบคุมผู้ใช้ในเครือข่ายที่ต้องเชื่อมต่อผ่านหลาย Hop โดยคาดหวังว่าระบบจะสามารถตรวจสอบและเก็บบันทึก Log ผู้ใช้ได้ถูกต้อง แต่ปัญหาที่งานวิจัยนี้ค้นพบคือ ค่า MAC Address ที่บันทึกลงใน Log เป็นค่าของอุปกรณ์เครือข่ายที่เชื่อมต่อโดยตรงกับ Egress NAC ไม่ได้เป็นค่าจากเครื่องของผู้ใช้ตัวจริง ส่งผลให้ไม่สามารถนำข้อมูลที่ได้ไปใช้เป็นหลักฐานในการชี้ตัวผู้กระทำความผิดตามข้อกำหนด พรบ. ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ ปี พ.ศ. 2550 ได้ ทำให้ระบบ Log ที่ลงทุนจำนวนมหาศาลล้มเหลวต่อการใช้งาน

งานวิจัยนี้จึงนำเสนอวิธีการแก้ปัญหาการเก็บข้อมูล Log ผิดพลาด โดยพัฒนาส่วนของ JAVA Applet เพื่อใช้ในการดึงค่า MAC Address ที่ถูกต้องจากเครื่องของผู้ใช้ ซึ่งผลที่ได้คือระบบสามารถเก็บ Log ได้อย่างถูกต้อง โดยที่ไม่ได้ลดทอนประสิทธิภาพในการใช้งานระบบควบคุมการเข้าถึงเครือข่ายแต่อย่างใด

เอกสารอ้างอิง

1. Coovachilli. Open Source Captive Portal Access Controller and RADIUS Software. Available from http://coova.org/. Accessed September 1, 2014.
2. ChilliSpot. ChilliSpot - Open Source Wireless LAN Access Point Controller. Spice up your HotSpot with Chilli. Available from http://www.chillispot.info/. Accessed May 9, 2014.
3. Coreteam p. pfSense Open Source Firewall Distribution. Available from http://www.pfsense.org/. Accessed October 1, 2014.
4. Consentry. ConSentry Networks - Network Access Control. Available from http://consentry.com/. Accessed September 2, 2014.
5. SangforIAM. Leading vendor of Web Security, WAN Optimization and Internet Access Management in Asia Pacific Region. Available from http://www.sangfor.com/product/Internet%20Access%20Management/outline.html. Accessed September 2, 2014.
6. Bluesocket. Enterprise Wireless LAN Security and Management Solutions - Bluesocket. Available from http://www.adtran.com/. Accessed May 9, 2014.
7. Puangpronpitag S, Suwannasa A. A Lightweight Agent-based Egress NAC on Wireless LAN. International Conference on Computer & Information Science (ICCIS); Kuala Lumpur, Malaysia. IEEE 2012;
8. Puangpronpitag S, Suwannasa A. A design of egress NAC using an authentication visa checking mechanism to protect against MAC address spoofing attacks. 8th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON); 2011; 300-303.
9. Plummer DC. An Ethernet Address Resolution Protocol or Converting Network Protocol Addresses. IETF RFC 826 1982;
10. สมนึก พ่วงพรพิทักษ์. ระบบควบคุมผู้ใช้งานการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ สำหรับมหาวิทยาลัยราชภัฏกาฬสินธุ์, รายงานวิจัยโครงการวิจัยร่วมระหว่าง Information Security & Advanced Network Lab กับ บริษัท นอร์ทอีสเทิร์นไอที; กรกฎาคม 2554
11. Kadlecsik J. The netfilter.org ipset project. Available from http://www.netfilter.org/projects/ipset/index.html. Accessed June 6, 2014.
12. Netfilter. The netfilter.org iptables project. Available from http://www.netfilter.org/projects/iptables/index.html. Accessed June 6, 2014.
13. Cisco. Cisco Catalyst 2960G-8TC-L Compact Switch IOS Software-12.2.55-SE9. Available from http://software.cisco.com/download/release.html?mdfid=280836706&softwareid=280805680&release=12.2.55-SE9. Accessed June 6, 2014.