การออกแบบและพัฒนาดีเอชซีพีและเกตเวย์ สำหรับป้องกันการปลอมแปลงโพรโทคอลเออาร์พีบนเครือข่ายอีเทอร์เน็ท

Design and Development of DHCP and Gateway ugainst ARP Spoofing on Ethernet Network

พิทักษ์ สุรินทร์วัฒนกุล, ประยงค์ ฐิติธนานนท์, ธีระ สาธุพันธ์**

Pituk Surinwattanakul, Prayong Thititananon, Theera Sathuphan**

บทคัดย่อ

การปลอมแปลโพรโทคอล ARP หรือการ ARP Spoof เป็นปัญหาที่ร้ายแรงในระบบเครือข่ายอีเทอร์เน็ท ซึ่งปัญหาที่สำคัญก็คือ การแทรกแซงระบบหรือการดักจับข้อมูล (MITM : Man in the Middle) ถึงจะมีงานวิจัยต่างๆ ที่จะพยายามมาแก้ไขปัญหาเหล่านี้แต่ก็ยังมีข้อบกพร่องอยู่หลายประการ เช่น ระบบป้องกันที่ไม่ได้ประสิทธิภาพ ความยุ่งยากในการจัดการและค่าใช้จ่ายที่สูง งานวิจัยจึงได้นำกลไกของอัลกอริธึม DepMAC-IP และการนำเทคนิค Gratuitous ARP มาใช้ในการพัฒนาต่อยอดให้กับ DHCP Server กับ Gateway เพื่อทำให้ระบบเครือข่ายมีความมั่นคงและปลอดภัยจากการดักจับข้อมูล ผลที่ได้จากงานวิจัยก็สามารถที่จะเป็นแนวทางในการนำไปประยุกต์ใช้งานกับ DHCP Server กับ Gateway ให้เกิดประสิทธิภาพในการทำงานและความปลอดภัยมากยิ่งขึ้น

คำสำคัญ : การปลอมแปลง, การจู่โจม, อัลกอริธึม DepMAC-IP

สาขาคอมพิวเตอร์และเทคโนโลยีสารสนเทศเพื่อการศึกษา

คณะวิทยาการคอมพิวเตอร์ มหาวิทยาลัยราชภัฏอุบลราชธานี

*E-mail: pikkybrian123@gmail.com, prayong172@gmail.com

Abstract

The counterfeiting Protocol ARP or ARP Spoof is a serious problem in the Ethernet network. The problem relates to the intervention of the system or interception of information (MITM: Man of the Middle). Several research papers try to solve the problems but they still have some drawbacks regarding incompatibility with the communication standard of Protocol ARP. The protection is not effective and difficult to manage and cost more. In this paper, the researcher applies the mechanism of DepMAC-IP algorithm and Gratuitous ARP technique on the DHCP server and Gateway for network security and stability to guard against ARP spoofing on ethernet networks. The result of the research can be applied to the guideline with DHCP server and Gateway. It make the server more robust with regards to security and efficiency.

Keyword : Spoofing, Attack, DepMAC-IP Algorithm

บทนำ

การสื่อสารในระบบเครือข่ายอีเทอร์เน็ต (Ethernet) จะใช้โพรโทคอล ARP (Address Resolution Protocol) (เรืองไกร รังสิพล, 2544) ในการค้นหา MAC address จาก IP address ก่อนการรับและส่งข้อมูล แต่ปัญหาที่เกิดขึ้นในส่วนการทำงานของโพรโทคอล ARP นั้นก็คือ การปลอมแปลงข้อความ ARP ที่เรียกว่า ARP Spoof (ธวัชชัย ชมศิริ, 2547) ซึ่งเป็นปัญหาที่ร้ายแรงในระบบเครือข่ายอีเทอร์เน็ท และอีกหนึ่งวิธีการจู่โจมเครือข่ายก็คือการแทรกแซงการสื่อสาร (MITM : Man in the Middle) (D.Serpanos, 2001)

แม้จะมีการพัฒนาการแก้ไขปัญหา ARP Spoof มาเพื่อใช้ป้องกันการดักจับข้อมูลคอมพิวเตอร์ส่วนบุคคล (Personal Computer : PC) บนระบบเครือข่ายอีเทอร์เน็ท แต่ก็ยังมีปัญหาที่ยังเกิดขึ้น คือ ปัญหาของความเข้ากันได้กับโพรโทคอล ARP เช่น การจัดระบบมีความยุ่งยากซับซ้อนและอุปกรณ์ที่มีราคาสูง (ณรงฤทธิ์ มะสุใส และสมนึก พ่วงพรพิทักษ์, 2555, 456-461)

งานวิจัยนี้จึงเสนอการนำกลไกของอัลกอริธึม DepMAC–IP (F.Fayyaz and H. Rasheed, 2012) มาใช้เป็นกลไกจับคู่ระหว่าง IP Address กับ MAC Address เพื่อใช้ในการตรวจสอบโพรโทคอล ARP โดยพัฒนาต่อยอด DHCP Server ให้มีฟังก์ชั่นในการจ่าย IP Address ที่สอดคล้องกับ MAC Address ตามอัลกอริธึม DepMAC-IP และพัฒนา Gateway โดยการนำกลไกของอัลกอริธึม DepMAC-IP มาใช้ในการตรวจสอบการจับคู่ระหว่าง IP Address กับ MAC Address และป้องกันการปลอมแปลงโพรโทคอล ARP โดยใช้ Gratuitous ARP (IP ARP Gratuitous, 2014)

ผลจากงานวิจัยได้ DHCP Server (R.Droms, 2001) และ Gateway (Shelly, 2004) ที่มีความมั่นคงจากการจู่โจมด้วยวิธี ARP Spoof และสนับสนุนการใช้งานกับ

มาตรฐานของโพรโทคอล ARP และโพรโทคอล DHCP สามารถช่วยลดต้นทุนการจัดการเครือข่ายองค์กรขนาดเล็กและขนาดกลาง

ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

โพรโทคอล ARP

โพรโทคอล ARP (Address Resolution Protocol) (เรืองไกร รังสิพล, 2544) เป็นโพรโทคอลชนิดหนึ่งที่เป็นตัวกลางในการสื่อสารที่ทำหน้าที่หา MAC Address และจับคู่ระหว่าง IP Address ที่เชื่อมโยงเครือข่ายของระบบการขอหมายเลข IP Address มาใช้บริการเพื่อให้สามารถสื่อสารกันระหว่างระบบเครือข่ายต่างๆ ได้ สามรถส่งข้อมูลระหว่างคอมพิวเตอร์ที่ติดต่อกัน โดยมีฮาร์ดแวร์สร้างเฟรมข้อมูลแล้วโพรโทคอล ARP จะนำข้อมูลเหล่านั้นเข้าที่เครื่อง Host ในระบบเครือข่ายต่อไป

โดยบทบาทของโพรโทคอล ARP มีความสำคัญมาก เพราะโพรโทคอล ARP จะทำหน้าที่ในการจับคู่ระหว่าง IP Address ซึ่งเป็นแอดเดรสทาง Logical กับ MAC Address ซึ่งเป็นแอดเดรสทาง Physical ดังนั้นระบบ IP Address จึงต้องทำการหาแอดเดรสที่ระดับชั้นดาต้าลิงค์ที่รู้จัก ซึ่งก็คือ MAC Address เพื่อที่จะสร้างเฟรมข้อมูลในชั้นดาต้าลิงค์

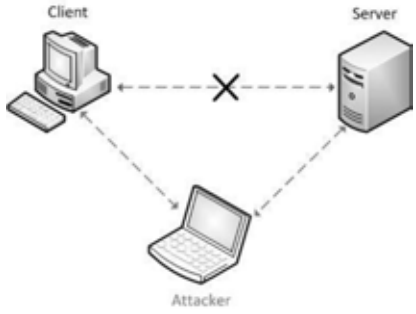
โดยโพรโทคอล ARP จะมีหน้าที่การนำแพ็กเกตที่ระบุเครื่อง Host ในระบบเครือข่ายมาถึง Gateway เครื่องที่ Gateway จะเรียกโพรโทคอล ARP ให้หาเครื่อง Host หรือ MAC Address ที่ตรงกับ IP Address โพรโทคอล ARP จะหา ARP Cache เมื่อพบแล้วจะทำการแปลงแพ็กเกตที่มีความยาวและรูปแบบที่ถูกต้อง เพื่อส่งไปยังเครื่องที่ระบุไว้ได้อย่างถูกต้อง

โพรโทคอล ARP จะปรับปรุง ARP Cache ยาวและส่งแพ็กเกตไปยัง MAC Address หรือเครื่องที่ตอบมา โพรโทคอล ARP ได้กำหนดไว้เป็นมาตรฐานภายใต้ RFC 826 โดยการทำงานของโพรโทคอล ARP จะมีรูปแบบการทำงานในแบบ Broadcast ดังนั้นเครือข่ายที่ใช้งานกับโพรโทคอล ARP ได้จึงต้องเป็นเครือข่ายที่มีการทำงานในแบบ Broadcast ซึ่งระบบอีเทอร์เน็ตส่วนใหญ่จะมีการทำงานเป็นแบบ Broadcast จึงสามารถทำงานร่วมกับโพรโทคอล ARP ได้เป็นอย่างดี

ARP Spoof

ARP Spoof (ธวัชชัย ชมศิริ, 2547) หรือ ARP Cache Poisoning (S.Manwani, 2003) คือการโจมตีโดยใช้ช่องโหว่ของโพรโทคอล ARP เพื่อหลอกให้เหยื่อให้หลงกล โดยมีจุดประสงค์หลักคือ การจู่โจมแบบ (DoS : Denial of Service) เป็นการทำให้เครื่องเหยื่อไม่สามารถสื่อสารกับปลายทางได้อย่างถูกต้อง เป็นผลทำให้ไม่สามารถใช้งานอินเทอร์เน็ตได้ และการแทรกกลาง (MITM : Man In The Middle) เป็นการจู่โจมเพื่อดักจับข้อมูล (Sniff) ต่างๆ ของเหยื่อโดยการทำงานของ ARP จะมีการส่ง ARP Request ออกไปแล้วรอให้มีการ ARP Reply ตอบกลับมา ถ้าหากระหว่างที่กำลังรออยู่นั้น มีผู้ไม่หวังดีตอบ ARP Reply ปลอมกลับมา ผู้ที่ได้รับก็จะไม่สามารถทราบได้ว่า ARP

Reply นั้นเป็นของจริงหรือปลอม และบันทึกข้อมูล MAC Address ที่ไม่ถูกต้องนั้นไว้ใน ARP Table ดังภาพที่ 1



ภาพที่ 1. การ ARP Spoof

DHCP

DHCP (Dynamic Host Configuration Protocol) (R.Droms, 2001) คือโพรโทคอลที่ใช้ในการจัดการจัดสรรการตั้งค่าการเข้าใช้งานเครือข่าย เช่น IP Address, Subnet mark, DNS หรือค่าพารามิเตอร์ต่างๆ โดยอัตโนมัติซึ่งเป็นผลดีต่อผู้ดูแลระบบที่ไม่จำเป็นต้องไปตั้งค่าให้กับเครื่อง Client ทุกๆ เครื่องทีละเครื่องซึ่งจะเป็นการยากแก่การจัดการดูแล ดังนั้นโพรโทคอล DHCP จะนิยมใช้ในกรณีที่ภายในเครือข่ายมีเครื่อง Client เป็นจำนวนมาก เพื่อป้องกันปัญหาการตั้งค่าพารามิเตอร์ที่ซ้ำซ้อนกัน

โพรโทคอลที่ใช้ในการทำงานของ DHCP ส่วนใหญ่เป็นลักษณะแบบ Broadcast ซึ่งกระบวนการแจกจ่าย IP Address นี้ประกอบไปด้วย 4 ขั้นตอน คือ DHCPDiscover DHCPOffer DHCPRequest และ DHCPAck ที่เครื่อง Client กับ DHCP Server จะติดต่อกันจนกระทั่งสุดท้ายได้รับ IP Address ที่ไม่ซ้ำกับ Host อื่นๆ ตลอดจนค่า Configuration ที่สำหรับใช้งาน

Gateway

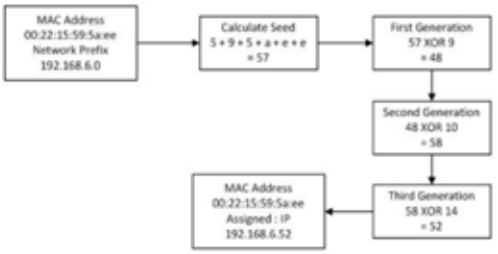
Gateway (Shelly, 2004) เป็นจุดเชื่อมต่อของเครือข่ายที่ทำหน้าที่เป็นทางออกสู่ระบบเครือข่าย บนอินเทอร์เน็ต ทำหน้าที่ให้โพรโทคอลต่างกัน สามารถทำการสื่อสารกันได้ หากโพรโทคคอลของเครือข่าย ทั้งสองไม่เหมือนกัน Gateway จะทำหน้าที่แปลงโพรโทคอลให้ตรงกับปลายทางและเหมาะสมกับอุปกรณ์ที่แต่ละเครือข่ายใช้งานอยู่ด้วย

ในการที่ Gateway สามารถส่งข้อมูลจากเครือข่ายหนึ่งไปยังอีกเครือข่ายหนึ่งได้อย่างถูกต้องนั้น ตัวของ Gateway เองจะต้องสร้างตารางการส่งข้อมูล หรือเรียกว่า Routing Table ขึ้นมาให้กับตัวเอง ซึ่งในตารางนี้จะทำการบอกว่า Server อยู่ในเครือข่ายใดบ้าง และอยู่ภายใต้ของ Gateway ใด ซึ่งตารางนี้จะมีการปรับเปลี่ยนข้อมูลทุกๆระยะ สำหรับเครือข่ายที่มีขนาดใหญ่ และหน้าที่ของ Gateway บางตัวอาจจะมีการนำฟังก์ชั่นของ Firewall ซึ่งเป็นเหมือนกำแพงที่ทำหน้าที่ป้องกันไม่ให้คอมพิวเตอร์ที่อยู่เครือข่ายภายนอก เข้ามาเชื่อมต่อกับเครือข่ายภายในเพื่อเข้าถึงข้อมูลต่างๆ

อัลกอริธึม DepMAC-IP

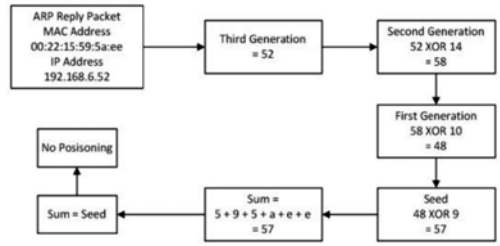
DepMAC-IP (F.Fayyaz and H.Rasheed, 2012) เป็นอัลกอริธึมที่ถูกสร้างขึ้นมาตรวจสอบการจับคู่ของ IP Address กับ

MAC Address โดยใช้กลไกอัลกอริธึม Dep-MAC-IP ทำการดึงค่าหมายเลข MAC Address ของตัวอุปกรณ์เครือข่าย (OUI, 2014) จำนวน 3 ไบต์สุดท้าย ในแบบเลขฐาน 16 มาทำการหาผลรวมทั้งหมด เพื่อให้ได้ผลรวมค่า Seed ออกมา จากนั้นนำผลรวมที่ได้มาแปลงค่า โดยใช้ Word ที่ 2 ของไบต์ที่ 1 ไบต์ที่ 2 และไบต์ที่ 3 ตามลำดับ มาทำแปลงค่าแบบ XOR จำนวน 3 ครั้งจนได้เป็นตัวเลข เพื่อมาใส่ใน IP Address ชุดสุดท้าย ดังรูปภาพที่ 2



ภาพที่ 2. ขั้นตอนการแปลงอัลกอริธึม DepMAC-IP

การตรวจสอบความสอดคล้องของ IP Address กับ MAC Address อัลกอริธึมจะทำการแปลค่ากลับ โดยใช้แบบย้อนกลับ โดยใช้หมายเลข MAC Address ของตัวอุปกรณ์เครือข่ายใน Word ที่ 2 ของ ไบต์ที่ 3 ไบต์ที่ 2 และไบต์ที่ 1 ตามลำดับ มาทำการแปลงค่าแบบ XOR จำนวน 3 รอบ เพื่อให้ได้ผลรวมค่า Sum แล้วจึงนำค่า Sum ที่ได้มาตรวจสอบกับค่า Seed ที่ได้มีการคำนวณไว้ในก่อนหน้านี้ว่ามีค่าที่ตรงกันหรือไม่ (Sum = Seed) ถ้าค่าของทั้งคู่ตรงกัน แสดงว่าไม่ได้เกิดการปลอมแปลง (No Posisoning) ของ IP Address กับ MAC Address ที่ได้ส่งมา ดังรูปภาพที่ 3



ภาพที่ 3. ขั้นตอนการตรวจสอบอัลกอริธึม DepMAC-IP

งานวิจัยที่เกี่ยวข้อง

DAPS (ณรงฤทธิ์ มะสุใส และสมนึก พ่วงพรพิทักษ์, 2555) เป็นระบบการป้องกันการปลอมแปลงโพรโทรคอล ARP โดยจะมีการทำงานออกเป็น 2 ส่วนก็คือ Gateway Protection (GP) และ Client Protection (CP) โดยจะต้องติดตั้งโปรแกรม CP ในเครื่อง Client และ CP จะทำการส่ง DHCPRequest ไปยัง DHCP Server เมื่อทาง DHCP Server ได้รับจะทำการตอบกลับ DHCPAck และ GP จะทำการดึงข้อมูล IP Address กับ MAC Address และทำ Static ARP ไว้ในตาราง ARP ของทาง Gateway เมื่อเครื่อง Client ได้รับ DHCPAck ก็จะทำการ Static ARP ไว้ที่เครื่อง Client ไว้ด้วย เพื่อป้องกันการปลอมแปลง IP Address กับ MAC Address ของเครื่อง Client ที่เข้ามาใหม่ในระบบเครือข่าย

ซึ่งระบบ DAPS จะต้องทำการติดตั้งโปรแกรมบนเครื่อง Client ซึ่งเป็นวิธีการที่ยุ่งยาก ในกรณีที่มีจำนวนเครื่อง Client เป็นจำนวนมาก และหากมีการทำงานในเครือข่ายที่เป็นแบบ Dynamic IP ซึ่งไม่สามารถทำงาน

กับเครือข่ายที่เป็นแบบ Static IP และหากระบบ DAPS ใน DHCP Server เกิดความไม่ปลอดภัย ก็จะทำให้ข้อมูลของ IP Address กับ MAC Address เกิดความผิดพลาดด้วย และการตั้งค่าแบบ Authentication (R. Droms & W. Arbugh, 2001) ก็อาจจะทำให้เกิดการ ARP Spoof ในระบบเครือข่ายได้

การดำเนินการวิจัย

1. การออกแบบและพัฒนา DHCP Server

การออกแบบ DHCP Server (Droms, 2001) โดยทำการเพิ่มโมดูลของอัลกอริธึม DepMAC-IP ที่พัฒนาด้วยการโปรแกรมภาษาจาวาเข้าไปไว้ในโค้ดของ MDHCP (MDHCP, 2014) ซึ่งเป็นโค้ดที่เป็นมาตรฐานการทำงานของ DHCP Server ขั้นตอนมีดังนี้

1) เมื่อเครื่อง Client ทำการเชื่อมต่อกับระบบเครือข่ายจะทำการร้องขอ IP Address กับทาง DHCP Server ให้ทำการจ่ายหมายเลข IP Address มาให้ยังเครื่องของตน

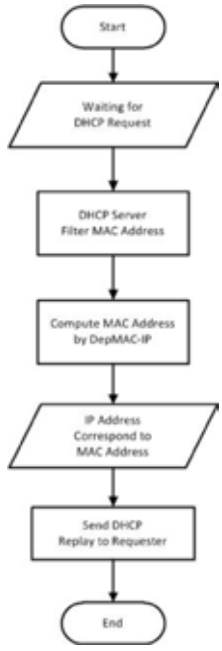
2) เครื่อง Client จะทำการส่ง DHCP Massage ซึ่งเป็นหมายเลข MAC Address ที่เป็นหมายเลขของตัวอุปกรณ์เครือข่าย เป็นเลขฐาน 16 จำนวน 6 Byte ไปยังทาง DHCP Server

3) DHCP Server จะนำหมายเลข MAC Address ทำการคำนวณหาหมายเลขของ IP Address โดยจะนำหมายเลขจำนวน 3 Byte สุดท้าย โดยใช้ Word ที่ 2 ของไบต์ที่ 1 ไบต์ที่ 2 และไบต์ที่ 3 ใช้ในการคำนวณหา IP Address โดยใช้กลไกอัลกอริธึม DepMAC-IP เพื่อในการคำนวณให้ออกมาเป็นหมายเลข IP Address ชุดสุดท้ายให้กับเครื่อง Client

4) เมื่อได้ IP Address กับ MAC Address ที่ มีความสอดคล้องกัน DHCP Server จะทำการ DHCPOffer กลับไปยังเครื่อง Client ทันที

2. การออกแบบและพัฒนา Gateway

การออกแบบ Gateway (Shelly, 2004) โดยทำการเพิ่มโมดูลของอัลกอริธึม DepMAC-IP ที่พัฒนาด้วยการโปรแกรมภาษาจาวาเข้าไปไว้ในส่วนการทำงานของ Gateway โดยต้องทำการปิด Function ARP เพื่อที่จะสามารถแก้ไข้โค้ดโปรแกรม ขั้นตอนมีดังนี้



ภาพที่ 4. การออกแบบการจ่าย IP Address ของ DHCP Server

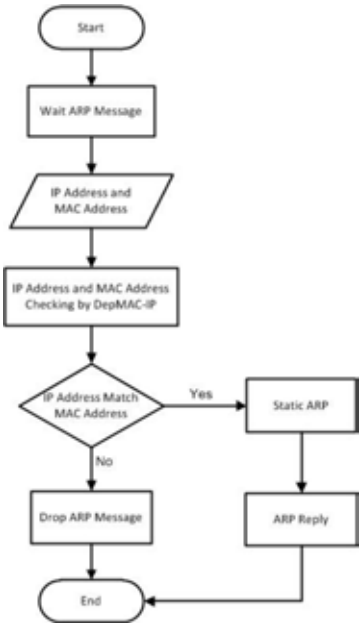
1) เมื่อมีการส่ง ARP Request จากเครื่อง Client มา Gateway โดยภายในแพ็กเกตที่ทางเครื่อง Client ส่งมานั้นจะมี IP Address กับ MAC Address และหมายเลข IP Address ของเครื่อง Gateway

2) เมื่อทาง Gateway ได้รับแพ็ตเกต ARP Request ที่ส่งมาแล้ว ทางฝั่ง Gateway จะทำการกรองหมายเลข IP Address กับ MAC Address ที่ส่งมาจากเครื่อง Client เพื่อตรวจสอบว่าทั้งคู่มีความสอดคล้องกันหรือไม่

3) หาก IP Address กับ MAC Address ที่ส่งมามีความสอดคล้องกัน แสดงว่าไม่เกิดการปลอมแปลงโพรโทคอล ARP (No Poisoning) ทางด้าน Gateway จะทำการ Static ARP เพื่อที่จดจำ IP Address กับ MAC Address คู่นี้ไว้ในระบบ และทำการส่งแพ็กเกต ARP Reply ที่มี IP Address กับ MAC Address ของ Gateway กลับไปยังเครื่อง Client และอนุญาตให้สามารถใช้งานอินเทอร์เน็ตได้ตามปกติ

4) แต่ถ้าหาก IP Address กับ MAC Address ที่ส่งมาไม่มีความสอดคล้องกัน (Poisoning) แสดงว่าได้เกิดการปลอมแปลงโพรโทคอล ARP ขึ้น ทาง Gateway จะไม่ตอบกลับ ARP Reply กลับไปยังเครื่อง Client และจะใช้เทคนิคของ Gratuitous ARP (IP ARP Gratuitous, 2014) โดยส่งแพ็กเก็จให้เปล่ากลับไปยังเครื่อง Client ที่อยู่ในระบบทั้งหมด

5) เครื่อง Client ในระบบก็จะได้รับแพ็กเก็จที่ทาง Gateway ส่งมาให้ โดยจะมีมี IP Address กับ MAC Address ที่ถูกต้องเพื่อจับคู่กันและสามารถใช้งานอินเทอร์เน็ตได้ปกติ



ภาพที่ 5. การออกแบบการตรวจสอบของทางฝั่ง Gateway

การประเมินผลการวิจัย

งานวิจัยนี้ได้ทำการทดสอบที่ห้องปฏิบัติการคอมพิวเตอร์ สาขาวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยราชภัฏสุรินทร์ จำนวน 3 เครื่อง คือ

1) เครื่องคอมพิวเตอร์ DHCP Server และ Gateway ที่มีการแก้ไขฟังก์ชั่นการทำงานให้มีการคำนวณและตรวจสอบ IP Address จาก MAC Address โดยใช้กลไกอัลกอริทึม DepMAC-IP

2) เครื่องคอมพิวเตอร์ PC ที่เป็นเหยื่อมีการใช้งานอินเทอร์เน็ตทั่วไป

3) เครื่องคอมพิวเตอร์ PC ที่ใช้สำหรับการทำ ARP Spoofing กับเครื่องคอมพิวเตอร์ PC ที่เป็นเหยื่อในระบบเครือข่ายอีเทอร์เน็ท

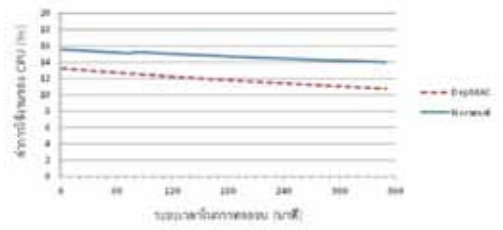
โดยผลการประเมินผลของงานวิจัยจะแบ่งออกเป็น 2 ส่วนดังนี้

1. ผลการทดสอบประสิทธิภาพการทำงานของ DHCP Server กับ Gateway

การทดสอบจะใช้วิธีการการวัดประสิทธิภาพการทำงานของเครื่องคอมพิวเตอร์ที่เป็น DHCP Server และ Gateway โดยเปรียบเทียบการทำงานของคอมพิวเตอร์ระหว่างคอมพิวเตอร์ DHCP Server กับ Gateway ในรูปแบบทั่วไปกับคอมพิวเตอร์ DHCP Server และ Gateway ที่มีการใช้กลไกของอัลกอริธึม DepMAC-IP ทั่วไป เพื่อเก็บค่าการประมวลผลของ CPU และค่าการใช้พื้นที่ของหน่วยความจำ เป็นเวลาทั้งสิ้น 360 นาที

ผลของประสิทธิภาพการทำงานของ CPU

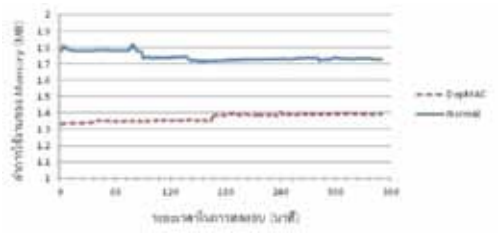
CPU มีการทำงานที่ลดลงเนื่องจาก DHCP Server กับ Gateway มีการทำงานจากการตรวจสอบโพรโทคอล ARP เพียงครั้งเดียว และทำการเก็บค่าของ Static ARP ที่ถูกต้องไว้ในกรณีที่มีการทำงานโพรโทคอล ARP ใหม่จึงไม่มีความจำเป็นที่จะต้องประมวลผล IP Address กับ MAC Addressขึ้นมาใหม่ดังภาพที่ 6



ภาพที่ 6. ประสิทธิภาพการทำงานของ CPU

ผลของประสิทธิภาพการทำงาน Memory

มีการใช้หน่วยความจำในปริมาณที่น้อยลง เนื่องจาก DHCP Server กับ Gateway มีการตรวจสอบโพรโทคอล ARP เพียงครั้งเดียว และทำการเก็บค่าของ Static ARP ไว้ จึงปริมาณของหน่วยความจำก็จะเก็บแค่ค่าของ Static ARP ที่ถูกต้องไว้เท่านั้นดังภาพที่ 7



ภาพที่ 7. ประสิทธิภาพการทำงานของ Memory

2. ผลทดสอบความสามารถในการป้องกันการปลอมแปลงโพรโทคอล ARP

การทดสอบการดักจับข้อมูลจากโปรแกรม Cain and Abel (Cain & Abel, 2009), Arp Spoof (Kali Linux, 2014) และ Ettercap (Kali Linux, 2014) บนระบบปฏิบัติการ Kali Linux (Kali Linux, 2014) โดยจะทำการปลอมแปลงโพรโทคอล ARP จำนวน 30 รอบ โดยกำหนดค่าความเชื่อมั่นของ (Confident Interval) (Easton & McColl, 2004) โดยจะทำการตรวจจับการปลอมแปลงโพรโทคอล ARP ในรูปแบบการทำงานของเครือข่ายอีเทอร์เน็ทในรูปแบบการทำงานทั่วไปเปรียบเทียบกับระบบเครือข่ายอีเทอร์เน็ทที่มีการใช้กลไกของอัลกอริธึม DepMAC-IP เข้าไปเพื่อใช้ในการตรวจสอบการทำงานของโพรโทคอล

ARP ซึ่งการทำงานในเครือข่ายอีเทอร์แบบเดิมจะไม่สามารถป้องกันการเข้าแทรกการสื่อสารได้ แต่ระบบที่ได้มีการพัฒนาขึ้นสามารถที่จะป้องกันการเข้าแทรกการสื่อสารได้ร้อยละ 100 ดังตารางที่ 1

ตารางที่ 1 ผลการทดสอบการเข้าแทรกการสื่อสาร (MITM)

LAN / Programs	เดิม	ใหม่
Cain and Abel	X	/
ARP Spoof	X	/
Ettercap	X	/

สรุปผลงานวิจัยและข้อเสนอแนะ

ปัญหาการปลอมแปลงโพรโทคอล ARP เป็นปัญหาที่ส่งผลเสียอย่างมากต่อระบบเครือข่ายอีเทอร์เน็ท มีความพยายามในการออกแบบและพัฒนาระบบที่ยังไม่สามารถนำไปใช้งานได้จริง เนื่องจากปัญหาหลายประการ งานวิจัยนี้จึงออกแบบและพัฒนา DHCP Server และ Gateway ที่สามารถทำให้ IP Address และ MAC Address มีความสอดคล้องกัน ซึ่งนำไปใช้การตรวจสอบการปลอมโพรโทคอล ARP ได้ โดยได้พัฒนาระบบโดยใช้ภาษาจาวา แล้วทำการทดลองบนเครือข่ายจริง พบว่าสามารถป้องการเข้าแทรกการสื่อสารได้ร้อยละ100 สรุปได้ว่าผู้ใช้งานจะได้ระบบเครือข่ายที่มีความมั่นคงและปลอดภัยจากการดักจับข้อมูล

ในการพัฒนาต่อยอดของการป้องกันการปลอมแปลงโพรโทคอล ARP นั้น อาจเพิ่มเติมในส่วนของการตรวจสอบหมายเลข IP Address โดยการแปลงค่าของ MAC Address จาก 3 byte เป็น 6 byte เพื่อให้เชื่อมั่นได้ว่าจะได้หมายเลข IP Address ที่ไม่มีความซ้ำซ้อนกัน

บรรณานุกรม

เรืองไกร รังสิพล. (2544). *เจาะระบบ TCP/IP : จุดอ่อนของโปรโตคอลและวิธีป้องกัน.* กรุงเทพฯ : บริษัทโปรวิชั่น จำกัด.

ธวัชชัย ชมศิริ. (2547). *Hack Step by Step.* กรุงเทพฯ : บริษัท ซีเอ็ดยูเคชั่น จำกัด.

Serpanos D. Lipton R. (2001). Defense Against Man-in-the-Middle Attack in Client-Server System. *Proceeding of* 6th IEEE *Symposium of Computer and Communication*.

ณรงค์ฤทธิ์ มะสุใส และสมนึก พ่วงพรพิทักษ์. (2555). ระบบป้องกันการปลอมแปลงโพรโทคอลเออาร์ พีแบบพลวัตในเครือข่ายเอสเอ็มอีจริง. *ECIT-CARD* 2010, 456-461.

F. Fayyaz, H. Rasheed. (2012). Using JPCAP to Prevent Man-in-the-Middle Attacks in a Local Area Network. *IEEE*, 35-37.

Cisco Company. (2014). IP ARP Gratuitous. Retrieved September 20, 2014, from : https://www.cisco.com/c/en/us/td/docs/iosxml/ios/ipaddr/command/ipaddr-cr-book/ipaddr-i1.pdf.

R. Droms. (1997). Standards Track (Dynamic Host Configuration Protocol). *IETF*.

R. Droms, W.Arbaugh. (2001). Authentication for DHCP Messages. *IETF*.

Shelly, G.B. (2004). A Gateway to Information Web Enhanced. Computer Discovering.

Manwani S. (2003). *ARP Cache Poisoning Detection and Prevention.* MSc thesis, San Jose State University, San Jose.

Standard IEEE. (2014). OUI (Organizational Unique Identifier). Retrieved September 30, 2014, from:https://standards.ieee.org/deverlop/regauth/oui/public.html.

MDHCP. (2014). Retrieved October 2, 2014, from : https://github.com/hero-m/MDHCP.

Cain & Abel Version 4.9.31, (Software). (2009). Massimiliano Montoro.

Kali Linux Verions 10.0.9, (Operation). (2014) Offensive Security Ltd.

Valerie J. Easton, John H. McColl. (2014) Confident Intervals. *Statistics Glossary v*(1).(1).