ระบบตรวจจับและป้องกันการปลอมแปลงโพรโทคอลเออาร์พีแบบยืดหยุ่นสำหรับองค์การ

A Flexible ARP Spoof Detection & Prevention System for Organizations

สมนึก พ่วงพรพิทักษ์[1], ธงชัย เจือจันทร์[2]

Somnuk Puangpronpitag[1], Thongchai Chuachan[2]

Received: 14 January 2015 ; Accepted: 21 April 2015

บทคัดย่อ

โพรโทคอลเออาร์พีทำหน้าที่จับคู่ระหว่างไอพีแอดเดรสกับแมคแอดเดรส โดยในขบวนการดังกล่าว อาร์พแคชจะถูกเปลี่ยนแปลงตามข้อความร้องขอหรือตอบกลับอาร์พ ดังนั้นจึงอ่อนไหวต่อการถูกจู่โจมด้วยวิธีปลอมแปลงโพรโทคอลเออาร์พี และการถูกจู่โจมด้วยวิธีนี้ ทำให้เกิดปัญหาหลายประการ เช่น การจู่โจมเพื่อทำให้ใช้งานระบบอินเทอร์เน็ตไม่ได้ ที่เรียกว่า ดีโอเอส หรือการดักจับข้อมูลที่เป็นความลับ เป็นต้น โดยได้มีงานวิจัยก่อนหน้าที่พยายามพัฒนาระบบตรวจจับและป้องกันการปลอมแปลงโพรโทคอลเออาร์พีไว้หลายแนวทาง แต่แนวทางที่นำเสนอก่อนเหล่านั้น ยังมีจุดบกพร่องหลายประการ และโดยเฉพาะอย่างยิ่งยังไม่เหมาะต่อการนำไปใช้กับเครือข่ายที่มีหลายวงแลนได้ งานวิจัยนี้จึงปรับปรุงการตรวจจับและป้องกันการปลอมแปลงโพรโทคอลเออาร์พี การฟื้นฟูการติดเชื้อและการป้องกันการปลอมแปลงโพรโทคอลเออาร์พีที่เกตเวย์ นอกจากนี้ยังได้พัฒนาต้นแบบโปรแกรมเพื่อใช้งานจริง และได้ทำการทดลองเพื่อทดสอบประสิทธิภาพของโปรแกรมต้นแบบ ผลการทดลองแสดงให้เห็นผลสัมฤทธิ์ของการปรับปรุงกลไกตรวจจับ ป้องกัน และรายงานการบุกรุก

คำสำคัญ: การตรวจจับและป้องกันการปลอมแปลงโพรโทคอลเออาร์พี การแอบดักจับข้อมูล การปฏิเสธการให้บริการ

Abstract

Address Resolution Protocol (ARP) is a crucial mechanism to map between Internet Protocol (IP) and Medium Access Control (MAC) addresses.According tothe ARP process, an ARP cache is always updated by incoming ARP reply or request packets. So, the ARP cache can be poisoned and vulnerable to ARP spoofing attacks. The attacks can cause several problems, such as Denial of Service (DoS) or confidential information eavesdropping. From the literature, several ARP detection and protection solutions have been proposed. However, all of them have several drawbacks. In particular, all previous solutions do not suit to the organization that has multiple LANs. So, this research has proposed to improve the ARP detection/protection techniques by improving the detection technique, gateway rehabilitation mechanism and ARP spoof detection in a network gateway. We have also prototyped our solution and experimented with it on a network test-bed. Our experimental results have demonstrated the improvement of detection, protection and reporting mechanisms.

Keywords: ARP spoofing detection and protection, Information eavesdropping, Denial of Service (DoS)

---

[1] *อาจารย์, สาขาวิทยาการคอมพิวเตอร์, คณะวิทยาการสารสนเทศ, มหาวิทยาลัยมหาสารคาม. E-mail: somnukp@msu.ac.th*

[2] *อาจารย์, สาขาวิทยาการคอมพิวเตอร์, ภาควิชาวิทยาศาสตร์พื้นฐาน, คณะวิทยาศาสตร์และเทคโนโลยี, มหาวิทยาลัยราชภัฏสุรินทร์. E-mail: thongchai@srru.ac.th*

[1] *Lecturer, Department of Computer Science, Faculty of Informatics, Mahasarakham University. E-mail: somnukp@msu.ac.th*

[2] *Lecturer, Department of Computer Science, Faculty of Science and Technology, Surindra Rajabhat University. E-mail: thongchai@srru.ac.th*

บทนำ

การสื่อสารในเครือข่าย Local Area Network (LAN) จำเป็นต้องใช้ Media Access Control (MAC) address ในการใช้แทนตำแหน่ง โดย MAC address จะถูกจับคู่กับInternet Protocol (IP)address โดย Address Resolution Protocol (ARP)[1]เป็นโพรโทคอลสำคัญในเครือข่าย LAN โดยทำหน้าที่ร้องขอ (ARP Request) MAC address ของปลายทางและตอบกลับ (ARP Reply) MAC address ของการ์ด Ethernet กลับไปที่ต้นทาง (Requester) เพื่ออัพเดต ARP cache ให้มีความเป็นปัจจุบัน ซึ่งกลายเป็นช่องโหว่เพราะโพรโทคอล ARP ถูกปลอมแปลงได้ง่าย

การปลอมแปลงโพรโทคอล ARP (ARP spoofing)[2] ก่อให้เกิดภัยคุกคามที่มีความเสี่ยงสูงเช่น การทำให้หลุดจากการใช้เครือข่าย ที่เรียกกันว่า Denial of Service (DoS) attacks โดยใช้โปรแกรม อย่างเช่น Netcut[3]และยังก่อให้เกิดปัญหาการแทรกกลางระหว่างการสื่อสาร (Man in the Middle (MitM) attacks) เพื่อดักจับ (Sniffing) ข้อมูลที่สำคัญของการเชื่อมต่อระหว่างต้นทางและปลายทาง เช่น รหัสผ่านของ Online Banking เป็นต้น ซึ่งปัจจุบัน โปรแกรมที่ใช้ในการ MitM เหล่านี้ สามารถดาวน์โหลดได้ฟรีอย่างง่ายดายจากอินเทอร์เน็ต เช่น Cain&Abel[4], Ettercap[5] และ Kali Linux[6] เป็นต้น

จากการศึกษางานวิจัยที่เกี่ยวข้อง พบว่าได้มีความพยายามที่จะสร้างเครื่องมือป้องกัน ARP spoofing เช่น การคอนฟิกโดยผู้แลระบบ[7]การแก้ไขโพรโทคอล[8-9]การใช้อุปกรณ์ที่มีคุณสมบัติพิเศษ[10] โปรแกรมและระบบป้องกัน[11-23]แต่แนวทางแก้ปัญหาที่กล่าวมา ยังไม่มีผลสัมฤทธิ์การป้องกัน ARP spoof ได้อย่างแท้จริง ดังนั้นทีมวิจัย จึงได้พัฒนาระบบตรวจจับและป้องกัน ARP spoof ไปแล้ว 3 อย่างคือ 1) AVAS[23] เป็นระบบที่อาศัยศูนย์กลางควบคุมให้มีการส่ง Vaccine (การจับคู่ระหว่าง IP และ MAC ที่ถูกต้อง) ซึ่งมีความสามารถในการตรวจจับและป้องกันระดับองค์การที่มี LAN หลายวงได้ดี เพราะมีระบบรายงานการจู่โจม แต่ จากการทดสอบนำ AVAS ไปใช้งานจริง พบว่ามีปัญหาที่การติดตั้ง เนื่องจากมีส่วนประกอบมาก (heavyweight) และหากองค์การไม่ติดตั้งทุกส่วนประกอบครบถ้วน ก็จะมีปัญหาไม่อาจช่วยป้องกันได้2) DAPS[22] เป็นงานวิจัยต่อยอดจาก AVAS โดยปรับให้มีประสิทธิภาพการตรวจจับ ARP spoof โดยอาศัย โพรโทคอล DHCP เข้ามาช่วยเพิ่มความเร็วในการทำงาน แต่ยังคงมีส่วนประกอบค่อนข้างมาก ที่ต้องอาศัย Admin ระดับองค์การในการติดตั้งในครบถ้วนเช่นกัน 3) J-ARP[19] เป็นโปรแกรมขนาดเล็กที่ออกแบบใหม่ โดนเน้นความ lightweight คือ ผู้ใช้ในองค์การสามารถนำไปติดตั้งใช้งานส่วนบุคคล โดยไม่ต้องอาศัย Admin ขององค์การแต่จากการนำ J-ARP ไปใช้งานจริง ได้พบปัญหาว่า J-ARP ยังขาดความสามารถในการตรวจจับควบคุม และป้องกันระดับองค์การของ AVAS และ DAPS นอกจากนี้ J-ARP ยังมีปัญหาที่ไม่สามารถป้องกันการ DoS เพื่อตัดการสื่อสารโดยจู่โจมที่ Gateway ได้ดีนัก กลไกในการป้องกันของ J-ARP เมื่อเผชิญกับเครื่องมือจู่โจมอย่าง NetCut 3.0 จะทำให้เกิด traffic เพิ่มมากและประสิทธิภาพการป้องกันไม่ร้อยเปอร์เซ็นต์

ในงานวิจัยนี้ จึงเสนอแนวคิดใหม่ในการออกแบบระบบตรวจจับและป้องกัน ARP spoof โดยอาศัยบูรณาการความสามารถของทั้ง AVAS/DAPS และ J-ARP เข้าด้วยกัน และนำเสนออัลกอลิธึมในการตรวจจับและป้องกันเพิ่มเติม ซึ่งการตรวจจับและป้องกันมีประสิทธิภาพมากขึ้น ทำให้ผู้ใช้ทั่วไปสามารถมีเครื่องมือที่ติดตั้งง่าย ในการป้องกันตนเอง และหากองค์การสนับสนุนการติดตั้งระบบป้องกันบนเครือข่ายของตน เครื่องมือของผู้ใช้ก็จะสามารถร่วมมือกันสนับสนุนการตรวจจับป้องกัน และรายงานการจู่โจม สมบูรณ์แบบยิ่งขึ้น ซึ่งจะเป็นเครื่องมือป้องกันที่ยืดหยุ่น (flexible) คือ สามารถทำงานในโหมด lightweight สำหรับผู้ใช้ในการป้องกันตนเองอย่างง่ายๆ เมื่อไม่ได้รับการสนับสนุนจาก Admin ขององค์การ และ สามารถต่อเชื่อม ทำงานในโหมดบูรณาการ ที่มีประสิทธิภาพในการตรวจจับและป้องกันระดับองค์การที่สมบูรณ์ เมื่อ Admin ขององค์การติดตั้งส่วนประกอบสำคัญเพิ่มเติม

นอกจากนี้ งานวิจัยนี้ยังปรับปรุงวิธีการตรวจจับและป้องกัน ให้มีประสิทธิภาพเพิ่มขึ้น ในการป้องกัน DoS แบบจู่โจมทั้งทางเดียวและสองทางเพิ่มประสิทธิภาพในการป้องกันการจู่โจมด้วยวิธี MitM โดยอัลกอริธึม DepMAC-IP และเพิ่มประสิทธิภาพในการฟื้นฟู Gateway จากการโจมตีด้วยกลไก Gateway-Rehabilitation (GR) นอกจากนี้ ยังได้พัฒนาเพิ่มเติมกลไกวิเคราะห์การจับคู่ระหว่าง MAC address และ IPaddress ก่อนตอบ ARP Reply ให้กับ Gateway

ในเนื้อหาส่วนถัดไป จะได้กล่าวรายละเอียดต่อไปนี้ คือ วัตถุประสงค์ของงานวิจัยในส่วนที่ 2 ทฤษฎีและงานวิจัยที่เกี่ยวข้องในส่วนที่ 3 แนวคิดของงานวิจัยนี้ ในส่วนที่ 4 การออกแบบแนวทางตรวจจับและป้องกันในส่วนที่ 5 ผลการประเมินประสิทธิภาพการตรวจจับและป้องกัน ในส่วนที่ 6 และสรุปการวิจัยในส่วนที่ 7

วัตถุประสงค์

(1) เพื่อออกแบบ ปรับปรุงกลไกการตรวจจับและป้องกันการปลอมแปลงโพรโทคอลเออาร์พี (2) เพื่อพัฒนาระบบป้องกันการปลอมแปลงโพรโทคอลเออาร์พี และ (3) ทดลองเพื่อประเมินประสิทธิภาพ

ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

โพรโทคอลเออาร์พี

โพรโทคอล ARP[1] เป็นโพรโทคอลที่ทำงานอยู่ในชั้น Data Link และมีความสำคัญมากในเครือข่าย Ethernet เพราะ ARP ทำหน้าที่ในการจับคู่ระหว่าง IPaddress กับ MAC address ดังแสดงใน Figure 1 เมื่อ A ซึ่งมี IP คือ 192.168.1.144 ต้องการสื่อสารกับ C ซึ่งมี IP คือ 192.168.1.166 A จะร้องขอ MAC address ของ C ด้วยการส่ง ARP Request message แบบ broadcast ภายใน LAN โดย ARP request message ดังกล่าวจะกระจายไปยังทุกๆ เครื่องใน LAN และผู้ที่ถูกร้องขอคือ C ก็จะเก็บคู่ IP address และ MAC address ของ A ไว้ใน ARP cache คือ 192.168.1.166 และ 00:00:f4:44:23:93 ตามลำดับดัง Figure 3 จากนั้น C จึงส่ง ARP Reply message แบบ Unicast กลับไปให้ A (ดังแสดงใน Figure 2) โดยใส่ MAC address ของ C เข้าไปใน ARP Reply message

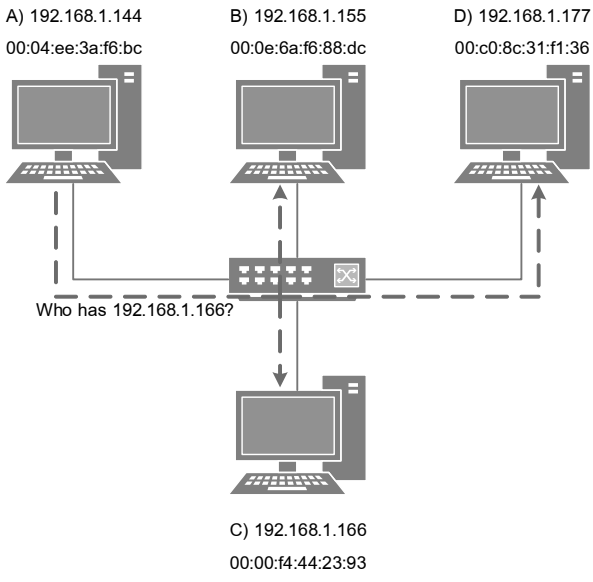

Figure 1 Broadcasting ARP Request messages

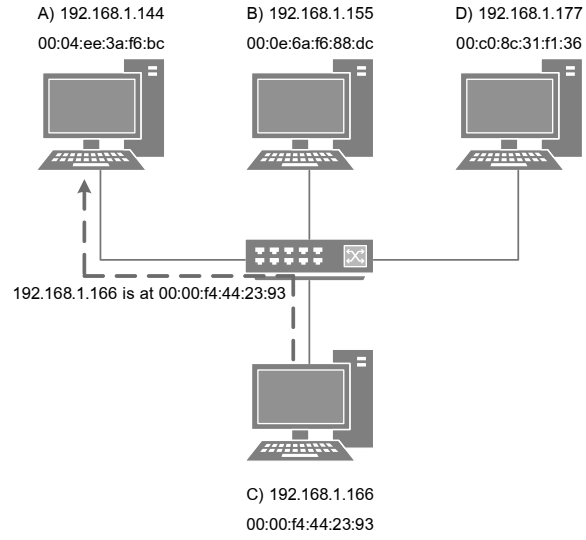

Figure 2 Sending ARP Reply message

เมื่อ A ได้รับ ARP Reply จาก C เครื่อง A ก็นำ MAC address ของ C มาเก็บไว้ที่ ARP cache ของ A เป็น 192.168.1.166 และ 00:00:f4:44:23:93 ดังแสดงใน Figure 4

```
[C@isan ~]$ arp -a 192.168.1.144
? (192.168.1.144) at 00:04:ee:3a:f9:bc [ether] on eth0
```

Figure 3 the ARP cache of C

```
[A@isan ~]$ arp -a 192.168.1.166
? (192.168.1.166) at 00:00:f4:44:23:93 [ether] on eth0
```

Figure 4 the ARP cache of A

ถึงแม้โพรโทคอล ARP ถูกออกแบบให้สามารถค้นหา MAC จาก IP ได้ แต่ก็มีปัญหาที่การออกแบบโพรโทคอลไม่คำนึงถึงความมั่นคงทางเครือข่ายตั้งแต่ต้น คือ 1) โพรโทคอล ARP ไม่มีการยืนยันความถูกต้องของ ARP messages 2) การอัพเดต ARP cache ตาม ARP Reply ที่ได้รับไม่สอดคล้อง (Correspond) กับการส่ง ARP Request 3) ARP cache ถูกอัพเดตตามข้อความ ARP ใดๆ ที่เข้ามาจึงเป็นที่มาของการจู่โจมด้วยวิธี ARP spoof ซึ่งเป็นภัยคุกคามที่สร้างความเสียหายต่อผู้ใช้ที่อยู่ในเครือข่าย LAN จำนวนมาก

การจู่โจมแบบ DoS ด้วย ARP

การจู่โจมด้วยวิธีส่ง ARP Reply ในลักษณะ DoS เพื่ออัพเดต ARP cache เครื่องเหยื่อให้การจับคู่ระหว่าง IP กับ MAC ที่ไม่มีอยู่จริงดัง Figure 5 เส้นหมายเลข (1) คือการ

ส่งข้อมูลปกติระหว่าง A และ C ในขณะที่เส้นหมายเลข (2) คือการส่ง ARP Reply ปลอมของผู้จู่โจม D ให้กับA โดยแจ้ง IP หมายเลข 192.168.1.166 ถูกจับคู่กับ MAC หมายเลข 00:11:22:33:44:55 ทำให้ ARP cache ของ A เปลี่ยนแปลง ทำให้การเชื่อมต่อของ A กับ C ถูกระงับ เส้นหมายเลข (3) คือการทำ ARP DoS ไปที่เครื่อง C เพื่อระงับการเชื่อมต่อกับ A โดยทำเช่นเดียวกันกับที่ส่ง ARPDoS Reply ไปให้ A

ถ้า C ติดตั้งโปรแกรมป้องกัน ARP spoof โปรแกรมจะสังเกตค่า Owner Unique Identifier (OUI)[24] ปลอมและการส่ง ARP Reply ปลอมแปลง MAC ของ Gateway ผู้จู่โจม D สามารถหลีกเลี่ยงการป้องกันด้วยการส่ง ARPDoS Reply ไปที่ Gateway A ทางเดียวตามเส้นหมายเลข (2) ใน Figure 5 ก็สามารถตัดการเชื่อมต่อระหว่าง A และ C ได้

การจู่โจมแบบ MitM

วิธีจู่โจม LAN แบบ Man in the Middle (MitM) attacks หรือที่เรียกว่า การจู่โจมแบบแทรกกลางการสื่อสาร เป็นการจู่โจมเพื่อดักจับข้อมูลที่สำคัญ เช่น Username และ Password โดยเฉพาะอย่างยิ่ง Online Banking

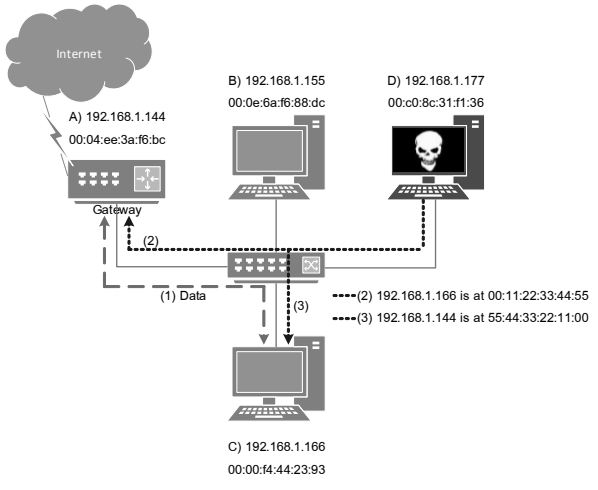

Figure 5 DoS by ARP

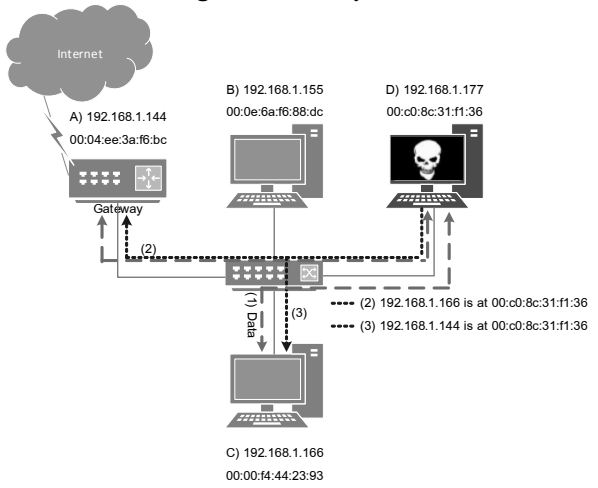

Figure 6 MitM Attack by ARP

Figure 6 เส้นหมายเลข (2) ผู้จู่โจม D ปลอม ARP Reply โดยกำหนด IP หมายเลข 192.168.1.166 ให้ถูกเชื่อมกับ MAC หมายเลข 00:c0:8c:31:f1:36 และเส้นหมายเลข (3) การทำแบบเดียวกัน คือ ปลอมตัวเป็น A เพื่อสื่อสารกับ C เมื่อเสร็จทุกขั้นตอน D สามารถดักจับข้อมูล ก่อนที่จะส่งต่อแพ็กเกตต่อเสมือนว่า A และ C สื่อสารกันอย่างปกติ

ถ้า C ติดตั้งระบบป้องกันผู้จู่โจม D อาจปล่อยให้การเชื่อมต่อของ A และ C เป็นไปอย่างปกติ จากนั้น D เริ่มทำให้ A ถูก poisoning โดยให้แพ็กเกตบางส่วนถูกส่งไปที่ D จากนั้นจากนั้นวิเคราะห์หาข้อมูลที่สำคัญ เช่น Session ก็สามารถเข้าใช้ระบบโดยไม่ต้องมีกระบวนการ Authentication ได้

แนวทางแก้ไขที่นำเสนอในวงการวิจัยมาก่อน

การป้องกัน ARP poof จากงานวิจัยก่อนหน้านี้สามารถแบ่งเป็น 6 แนวทาง คือ

(1) การให้ผู้ดูแลระบบจัดการ ARP cache ของผู้ใช้ให้เป็นแบบถาวร (Static ARP entry)[7] ถึงแม้วิธีนี้จะให้ความปลอดภัยกับผู้ใช้ แต่มีปัญหาด้านการจัดการ เพราะ 1) หากมีการเปลี่ยนการ์ดเครือข่ายที่ Gateway อาจทำให้ทุก End user ไม่สามารถเข้าถึงอินเทอร์เน็ตได้ 2) หากผู้จู่โจมทำ ARP DoS ไปที่ Gateway เพื่อตัดการเชื่อมต่อสู่อินเทอร์เน็ต End user ก็ไม่สามารถป้องกันตนเองได้ ซึ่งงานวิจัยนี้จะเสนอแนวทางแก้ไข

(2) กลุ่มแก้ไขโพรโทคอลเออาร์พีเช่น TARP[8] และ S-ARP[9] ป้องกัน ARP spoof ด้วยการปรับปรุงโพรโทคอล ARP ให้สามารถระบุตัวตนของผู้ส่ง เช่น การใช้ Public Key Infrastructure (PKI) แต่การนำไปใช้จริงมีความล่าช้าจากกลไกของ PKI และใช้แบนด์วิดท์ขององค์การสูง เพราะการทำงานของ ARP จะมีการ Broadcast หลายครั้งจาก End user ซึ่งงานวิจัยนี้สามารถหลีกเลี่ยงปัญหานี้ได้โดยการเพิ่มขั้นตอนการสร้าง Vaccine และการส่งข้อความ ARP ที่เป็นแบบ Unicast ซึ่งจะได้กล่าวในรายละเอียดต่อไป

(3) กลุ่มปรับปรุงเคอร์เนลของระบบปฏิบัติการเช่น Anticap[13] และ Antidote[14] แต่วิธีนี้ต้องแก้ไขเคอร์เนลของระบบปฏิบัติการและคอมไพล์เพื่อให้ได้ปฏิบัติการใหม่ ซึ่งปัจจุบันไม่สามารถนำไปใช้ได้จริง เพราะไม่สามารถแก้ไขและคอมไพล์ระบบปฏิบัติการให้กับผู้ใช้ได้อย่างทั่วถึงโดยเฉพาะอย่างยิ่งระบบปฏิบัติการที่ไม่ใช่ Open Source แตกต่างจากข้อเสนองานวิจัยนี้ที่ป้องกัน ARP spoof โดยไม่มีการคอมไพล์เคอร์เนลใหม่และสนับสนุนการทำงานบนระบบปฏิบัติการ Linux และ Windows

(4) การใช้อุปกรณ์ที่มีคุณสมบัติพิเศษ เช่น Dynamic ARP Inspection และ Port Security[10] ในอุปกรณ์ Switch ที่มีราคาสูง ซึ่งใช้วิธีกำหนดการจับคู่ระหว่าง MAC Address และเลขพอร์ตของอุปกรณ์ Switch เมื่อเกิดการจู่โจม ก็จะสามารถตรวจสอบการปลอม MAC Address และป้องกัน ARP spoof ได้ แต่มีความยุ่งยากในการจัดการและราคาสูงเกินความจำเป็นสำหรับองค์การโดยทั่วไป ซึ่งต่างจากงานวิจัยนี้ ที่ไม่จำเป็นต้องใช้อุปกรณ์พิเศษเหล่านี้

(5) กลุ่มระบบป้องกันเช่น DAPS[22] และ AVAS[23] เป็นวิธีป้องกัน ARP spoof ที่อาศัยการทำงานของหลายส่วนร่วมกัน เช่น การติดตั้งโปรแกรมที่ End user การใช้ระบบศูนย์กลางในการจัดการ และการสร้างตัวป้องกัน Gateway เป็นต้น แต่ระบบเหล่านี้ ยากแก่การติดตั้งให้สมบูรณ์ในองค์การ อาศัยหลายส่วนทำงานร่วมกัน โดยเฉพาะระบบที่ทำหน้าที่เป็นศูนย์กลางควบคุม มีความเสี่ยงต่อการถูกจู่โจมสูง และอาจกลายเป็น Single point of failure ได้

(6) โปรแกรมป้องกันเช่น AntiNetcut[11], AntiARP[12], J-ARP[19] และ Netcut Defender[20] ป้องกัน ARP spoof โดยใช้กลไกเฉพาะของแต่ละโปรแกรม เพื่อตรวจสอบการปลอมแปลง ARP โดย End user เพียงติดตั้งโปรแกรมเสริมป้องกัน แต่วิธีนี้ยังมีจุดด้อย คือ ผู้จู่โจมเปลี่ยนเป้าหมาย ไปที่ปลายทางของเหยื่อ แทนที่จะอัพเดต ARP cache ของเหยื่อโดยตรง เช่น การทำ ARP DoS ไปที่ Gateway เพื่อทำให้ Gateway ไม่รู้จักเหยื่อ ซึ่งทำให้การเชื่อมต่อล้มเหลว เป็นต้น ประเด็นการติดตั้งโปรแกรมเสริมขนาดเล็กเพื่อป้องกัน ARP spoof มีความเหมาะสมต่อองค์การต่าง ๆ เพราะมีความสะดวก จัดการได้ง่าย แต่ยังมีบางจุดที่ต้องปรับปรุง เช่น การป้องกันการติดเชื้อที่ Gateway ซึ่งเป็นที่มาของงานวิจัยนี้ที่ปรับปรุงวิธีป้องกันที่มีอยู่ให้มีความแข็งแกร่งมากขึ้น

แนวคิดของงานวิจัย

Static ARP entry เป็นเครื่องมือการป้องกัน ARP spoof ที่มีประสิทธิภาพสูง หาก IP Address และ MAC Address ถูกจับคู่อย่างถูกต้อง ก่อนที่จะทำ Static ARP จะทำให้ คู่ IP Address และ MACAddress ดังกล่าวเป็นเหมือนวัคซีนป้องกัน ARP Spoof เพราะการจู่โจมด้วย ARP Spoof จะไม่สามารถเปลี่ยนค่ามันได้เพียงแต่ยากที่ ผู้ใช้ไม่อาจใช้คำสั่งเพื่อ setstatic ARP ได้เอง

งานวิจัยนี้เห็นข้อดีของโปรแกรมขนาดเล็ก ที่สามารถตรวจสอบการปลอมแปลงโพรโทคอล ARP ได้ จึงพัฒนาในแนวทางเดียวกันแต่ได้แก้จุดอ่อน โดยปรับปรุงอัลกอริธึมตรวจจับการปลอมแปลงโพรโทคอล ARP การฟื้นฟูการติดเชื้อระบบตรวจ ARP ปลอมที่ Gateway ก่อนที่จะส่ง ARP Reply ข้อเสนอและอัลกอริธึมในการแก้ปัญหา

การปรับปรุงกลไกการสร้าง Vaccine

งานวิจัยก่อนหน้านี้ในวงการ เช่น J-ARP ใช้วิธีตรวจสอบหมายเลข MAC ของผู้ส่ง ARP Reply ต้องอยู่ใน OUI และ ARP Reply จาก IP ต้นทางเดียวต้องมี MAC ที่ไม่ซ้ำซ้อนกัน แล้วทำ Static ARP entry

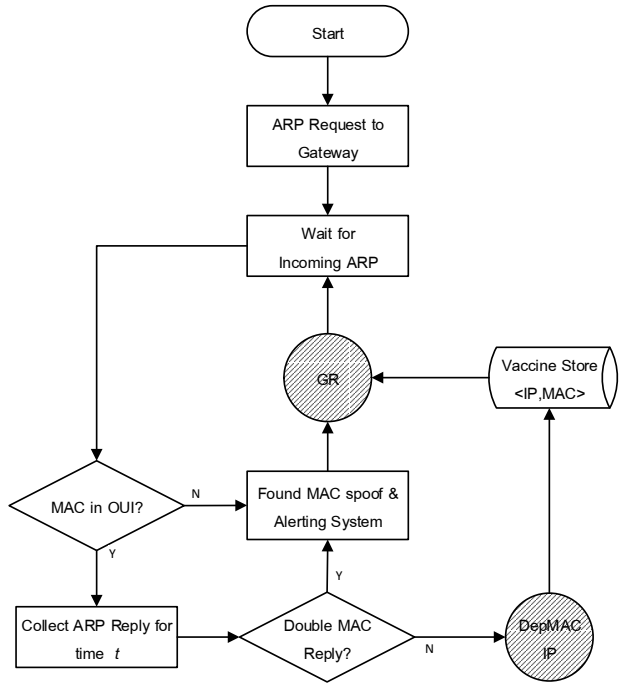

Figure 7 Our New Algorithm

Figure 7 คืออัลกอริธึมใหม่ที่ได้ปรับปรุงเพื่อแก้จุดอ่อนของ J-ARP ซึ่งได้ปรับการตรวจสอบดังนี้

(1)โปรแกรมจับและอ่าน ARP Packet และดึงหมายเลข MAC และหมายเลข IP โดยเมื่อโปรแกรมเริ่มทำงาน ARP Request ถูกส่งเพื่อตรวจสอบความซ้ำซ้อนของ MAC ของ Gateway (2) ตรวจสอบ MAC Address ที่ได้รับจาก ARP Request และ ARP Reply ถ้าอยู่ในรายการ OUI ก็จะตรวจสอบในข้อ 3 แต่ถ้าไม่พบในรายการโปรแกรมจะรู้ว่าแพ็กเกตเป็นของปลอม และเข้าขั้นตอนการฟื้นฟูในข้อ 5(3) ถ้า MAC อยู่ใน OUI ระบบจะรอเก็บแพ็กเกต ARP Reply ในระยะเวลา *t* และตรวจสอบ MAC ที่มาจาก IP ของต้นทางเดียวกัน ถ้าหากเกิดการซ้ำซ้อนกัน ระบบจะแจ้งเตือนผู้ใช้และดำเนินการตามข้อ 5 จากนั้นใช้อัลกอริธึม DepMAC-IP (ซึ่งจะอธิบายในรายละเอียดในหัวข้อถัดๆ ไป) เพื่อตรวจสอบการจับคู่ระหว่าง IP และ MAC (4) เมื่อผ่านการตรวจสอบด้วยอัลกอริธึม Dep MAC-IP โปรแกรมจะเก็บ Vaccine<IP,MAC>ไว้ที่ Vaccine

Store (VS) เพื่อใช้ในครั้งถัดไป (5) หากพบการจู่โจมกลไกการฟื้นฟูเกตเวย์ Gateway-Rehabilitation(GR) ที่ Gateway จะถูกเรียกใช้งาน

อัลกอริธึม Gateway-Rehabilitation

Gateway-Rehabilitation (GR) ดังแสดงใน Figure 8 เป็นวิธีฟื้นฟูการติดเชื้อของไอพีปลายทาง ในงานวิจัยนี้จะเน้นการฟื้นฟู Gateway ดังนี้

(1) เริ่มแรกโปรแกรมจะอ่านเวลา *T* ที่ใช้ในการฟื้นฟูการติดเชื้อ (2) ดึง Vaccine<IP,MAC> จาก VS แล้วสร้าง Process ย่อยทำงานอิสระ และส่วนงานหลักก็จะกลับเข้าสู่การตรวจสอบโพรโทคอล ARP (3) ที่การสร้าง Process ย่อย (New Child Process) โปรแกรมเริ่มสร้างแพ็กเกตARP Reply แบบ Unicast โดยส่ง IP และ MAC ของผู้ใช้ไปที่ IP และ MAC ที่ดึงมาจาก Vaccine ในข้อที่ 1 และลบค่า *T* ครั้งละ 1 เรื่อย ๆ จนกว่า *T* จะน้อยกว่าหรือเท่ากับ 0 จึงจะหยุด Process (4) การส่ง ARP Reply แต่ละครั้งจะต้องหน่วงเวลาไว้ 1 นาที เพื่อป้องกันการ Flood แพ็กเกตไปที่ปลายทาง

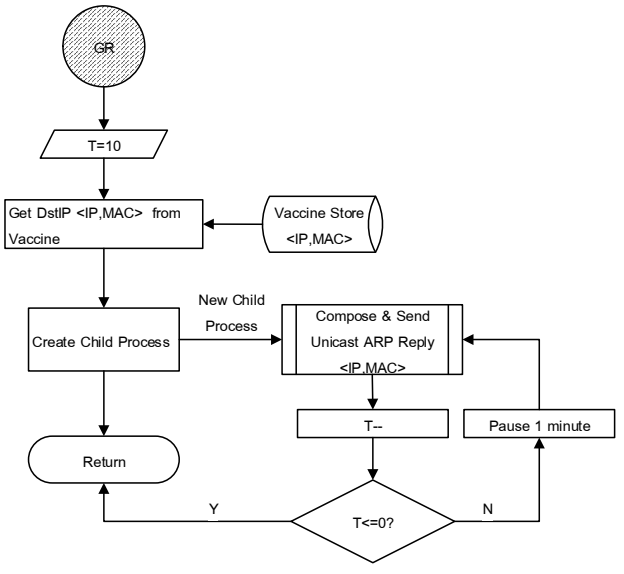

Figure 8 Gateway Rehabilitation Algorithm

อัลกอริธึม DepMAC-IP

DepMAC-IP[21] เป็นอัลกอริธึมที่แบ่งเป็น 2 ส่วน คือ คำนวนหา IP ที่สามารถผูกโยงกับ MAC ได้จากสูตร และส่วนการพิสูจน์การปลอมแปลงโพรโทคอล ARP ซึ่งขั้นตอนทั้งหมดแสดงใน Figure 9 และสามารถคำนวณได้ดังนี้

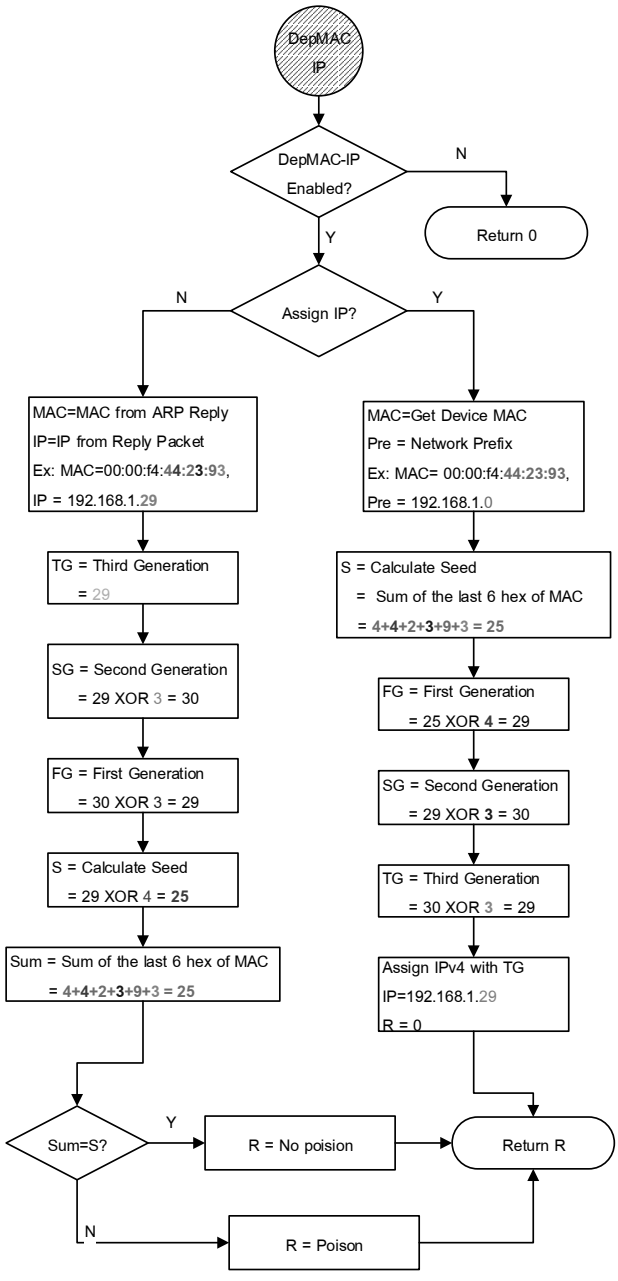

Figure 9 DepMAC-IP Algorithm

1. การคำนวณหา IP จากการนำ MAC มาประมวลผล เริ่มจากนำ MAC address การ์ด Ethernet ของผู้ใช้จำนวน 3 ไบต์สุดท้าย และใช้ Network Prefix (NetPre) ของเครือข่าย ตัวอย่างเช่น MAC ของผู้ใช้ คือ 00:00:f4:44:23:93 และ NetPre คือ 192.168.1.0 จะได้

MAC = 44:23:93

NetPre = 192.168.1.0

คำนวณหา Seed (S) โดยนำ hex ของแต่ละไบต์มารวมกัน

S = 4+4+2+3+9+3= 25

จากนั้นหา First Generation (FG) โดยนำ hex หลักที่ 2 ของไบต์แรกมา XOR กับ S

FG = 25 XOR 4 = 29

หา Second Generation (SG) จากการนำ FG มา XOR กับ hex หลักที่ 2 ของไบต์ที่ 2ได้

SG = 29 XOR 3 = 30

หา Third Generation (TG) จากการนำ SG มา XOR กับ hex หลักที่ 2 ของไบต์ที่ 3 ได้

TG = 30 XOR 3 = 29

เมื่อได้ TG ก็จะนำมากำหนด IP ของผู้ใช้ใหม่ จากตัวอย่างจะได้คู่ของ IP และ MAC ที่เชื่อมโยงกันได้ คือ

IP = 192.168.1.29

MAC = 00:00:f4:44:23:93

2. การพิสูจน์ความถูกต้องของการจับคู่ระหว่าง IP และ MAC ใน ARP Reply ดัง Figure 9 ด้านซ้าย เมื่อได้รับ ARP Reply อัลกอริธึมเริ่มจากการนำไบต์สุดท้ายของ IP ผู้ส่งมาคำนวณหา S โดยเริ่มจากการหา TG SG FG และได้ S จากนั้นนำ 3 ไบต์สุดท้ายของ MAC ผู้ส่งมาแยกเป็น hex แล้วรวมกัน (Sum) และตรวจสอบถ้า S เท่ากับ Sum หมายความว่า IP และ MAC จับคู่ได้ถูกต้อง ผลแบบอื่น คือเกิดการ ARP spoof ขึ้น ตัวอย่างเช่น เมื่อได้รับ ARP Reply (IP=192.168.1.29,MAC=00:00:f4:44:23:93) สามารถตรวจสอบได้โดย

MAC = 44:23:93

TG = 29

หา SG จากการนำ TG มา XOR กับ hex หลักที่ 2 ของของไบต์ที่ 3 ได้

SG = 29 XOR 3 = 30

หา FG จากการนำ SG มา XOR กับ hex หลักที่ 2 ของของไบต์ที่ 2 ได้

FG = 30 XOR 3 = 29

สุดท้ายหา S จากการนำ FG มา XOR กับ hex หลักที่ 2 ของของไบต์แรกได้

S = 29 XOR 4 = 25

หาค่า Sum โดยเอา hex ทั้ง 3 ไบต์มารวมกันได้

Sum = 4+4+2+3+9+3= 25

เมื่อได้ S และ Sum แล้วจึงตรวจสอบถ้าค่าตรงกันหมายความว่า ARP Reply ดังกล่าวไม่ถูกปลอมแปลง

การป้องกันที่ Gateway

สำหรับ Gateway ได้พัฒนาเซอร์วิสตรวจสอบ ARP Request บนระบบปฏิบัติการ Linux โดยปิดการตอบ ARP Reply อัตโนมัติของ Kernel ด้วยการกำหนด arp_ignore ให้มีค่าเป็น 8 แล้วดักจับ IP และ MAC ของผู้ส่ง ARP Request มาตรวจสอบ MAC ต้อง OUI และใช้ DepMAC-IP ตรวจสอบแล้วถูกต้อง จึงทำ Static ARP entry และตอบ ARP Reply กลับไปที่ต้นทาง

การพัฒนาและทดลองโปรแกรมต้นแบบ

การพัฒนาระบบ

โปรแกรมต้นแบบพัฒนาด้วย JKD1.8.0 ร่วมกับไลบรารีจับแพ็กเกต JNetPcap โดยได้เพิ่มอัลกอริธึม GR และ DepMAC-IP หน้าต่างการใช้งานโปรแกรมได้ปรับจากการใช้ Java Swing เป็น JavaFx ซึ่งสนับสนุนใน JRE รุ่น 1.8

ระบบวิเคราะห์ ARP เพื่อเลือกตอบ ARP Reply ที่ Gateway พัฒนาโดยใช้ JKD1.8.0 ร่วมกับ JNetPcap บนระบบปฏิบัติการลินุกส์ CentOS 6.5

สภาพแวดล้อมในการทดลอง

Figure 10 แสดงแผนผังที่ใช้ในการทดลองของงานวิจัยนี้ ซึ่งเครือข่าย LAN กำหนดไอพีอยู่ใน subnet 192.168.9.0/24 และกำหนดให้ผู้ใช้เป็นเครื่องเหยื่อใช้ซีพียู Intel(R) Core(TM) i5-3337U 1.80GHz แรม 4GB และดิสก์ความจุ 500GB โดยเหยื่อได้รับการคอนฟิกไอพีจาก DHCP ก่อนจากนั้นจะกำหนดใหม่จากการคำนวณของโปรแกรมป้องกันส่วน Gateway ของ LAN นี้ใช้ระบบปฏิบัติการลินุกส์ CentOS 6.5 ซีพียู Intel(R) Core(TM)2 Duo E6550 2.33GHz แรม 4 GB ดิสก์ความจุ 500GB และ IP ของ Gateway ได้จากคำนวณตามอัลกอริธึม DepMAC-IP

ผู้จู่โจมทำการจู่โจมด้วยวิธี ARP DoS และ MitM โดยใช้ Kali Linux ดังนี้ (1) ARP DoS แบบทางเดียว คือ แยกจู่โจมตามเส้น ARP DoS 1 ก่อน แล้วจึงจู่โจมตามเส้น ARP DoS 2 (ดัง Figure 10) (2) DoS แบบ 2 ทาง คือ ส่ง ARP แพ็กเกตปลอมไปที่ Victim และ Gateway พร้อม ๆ กัน ตามเส้น ARP DoS 1 และ ARP DoS 2 (ดัง Figure 10) (3) MitM เพื่อดักจับข้อมูลของผู้ใช้

การทดสอบโปรแกรมเพื่อประเมินประสิทธิภาพการป้องกัน ARP spoof จู่โจมทั้ง 3 แบบดังกล่าว แล้วใช้โปรแกรม iperf[25] ตรวจสอบการสูญหายของแพ็กเกตเมื่อถูกจู่โจม โดย Link มีขนาด 100 Mbps ทดลองโดยใช้ TCP ที่มี window size ขนาด 85.3 KByte และทดลองซ้ำจำนวน 30 ครั้ง ครั้งละ 10 วินาที ภายใต้สภาวะที่ถูกจู่โจมด้วย ARP spoof แบบต่าง ๆ และกำหนดความเชื่อมั่นที่ระดับร้อยละ 95

การส่งข้อมูลของเหยื่อควรส่งแพ็กเกตได้ใกล้เคียง 100 Mbyte และใช้แบนด์วิดท์ใกล้เคียง 100 Mbps

การตั้งค่าเบื้องต้นของโปรแกรมประกอบด้วย เวลาที่ใช้รอ ARP Reply (t) 5 วินาที เวลาที่ใช้ฟื้นฟูการติดเชื้อของ Gateway ในอัลกอริธึม GR(T) ใช้ 30 นาที

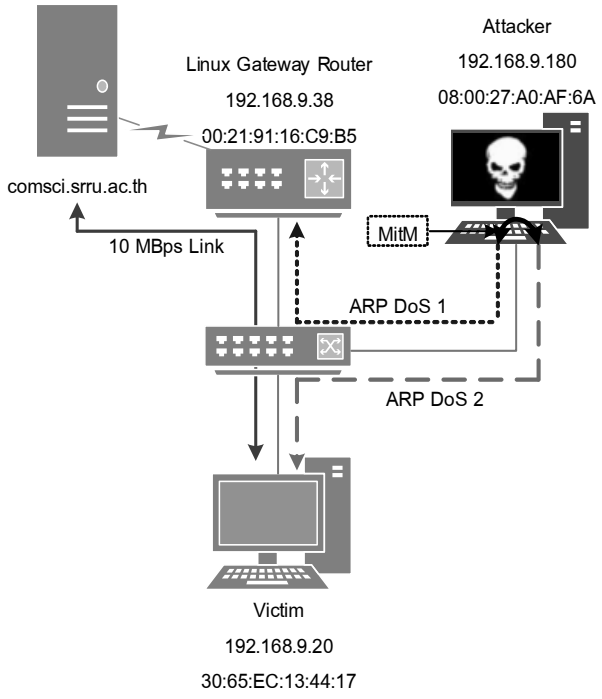

Figure 10 Experimental Testbed

Figure 11 Our User Interface

ผลการทดลองประสิทธิภาพ

Figure 11 แสดงผลการพัฒนาในส่วนของ User interface ของโปรแกรม ซึ่งประกอบด้วย การ์ดเครือข่ายที่โปรแกรมตรวจสอบได้อัตโนมัติ หรือกรณีโปรแกรมเลือกการ์ด Ethernet ไม่ถูกต้องผู้ใช้สามารถเลือกการ์ดอื่น ๆ ได้ และข้อมูลอื่น ๆ เช่น IP และ MAC ของเกตเวย์ โพรโทคอล ARP ที่ได้รับทั้งหมด และ ARP ปลอมที่ตรวจสอบพบ เป็นต้น

จากผลการทดลองจะเห็นว่ามีแพ็กเกตสูญหายไม่ถึงร้อยละ 1 และแบนด์วิดท์ไกล้เคียง 100 Mbps ทุกการทดลอง ดังนั้นการจู่โจมทั้ง 4 แบบไม่ส่งผลต่อการส่งแพ็กเกตไปที่ปลายทาง ดังนั้น โปรแกรมต้นแบบของงานวิจัยนี้สามารถป้องกันการจู่โจมด้วย ARP spoof อย่างสมบูรณ์

Figure 12 แสดงการจู่โจมของ Attacker โดยที่เส้นประคือ MAC ของ Gateway ที่ผู้จู่โจมได้รับ ซึ่งเป็นหมายเลข

00:00:00:00:00:00 เกิดจาก Attacker ไม่ได้รับ ARP Reply จาก Gateway ดังนั้น Attacker จึงไม่สามารถรู้ MAC ของ Gateway ได้

Figure 13 แสดงภาพการส่ง DoSแบบ 2 ทางเพื่อระงับการสื่อสาร และ MitM ก็ทำเช่นเดียวกัน ผลการทดลองจะเห็นว่า Attacker ไม่มี MAC ของ Gateway และส่ง ARP Reply ไปที่ Victim ได้ แต่ Victim ไม่อัพเดต ARP cache ตาม ARP Reply ดังกล่าว เพราะได้ทำ Static ARP entry ก่อนหน้านี้แล้ว Victim จึงปลอดภัยจากการจู่โจมของ Attacker

Table 1 แสดงผลการทดลองจู่โจมทั้ง 4 แบบ จากแบนด์วิดท์ 10 Mbps ใช้แพ็กเกต Window Size 64 ไบต์และถูกจู่โจมแบบ ARP DoS 1, ARP DoS 2, ARP DoS 1 & 2 และ MitM สามารถส่งแพ็กเกตได้ 99.7±0.2, 99.9±0.05, 99.1±0.1 และ 99.8±0.1 Mbyte ตามลำดับ ส่วนแบนด์วิดท์ที่ใช้อยู่ที่ 83.6±0.1, 83.7±0.09, 82.9±0.1 และ 83.5±0.09Mbps ตามลำดับ

Table 1 Experimental Results

Transfer/Bandwidth / Attacking Methods	10 Mbps Link	
	Transfer (Mbyte)	Bandwidth (Mbps)
ARP DoS 1	99.7±0.2	83.6±0.1
ARP DoS 2	99.9±0.05	83.7±0.09
DoS 1 & 2	99.1±0.1	82.9±0.1
MitM	99.8±0.1	83.5±0.09

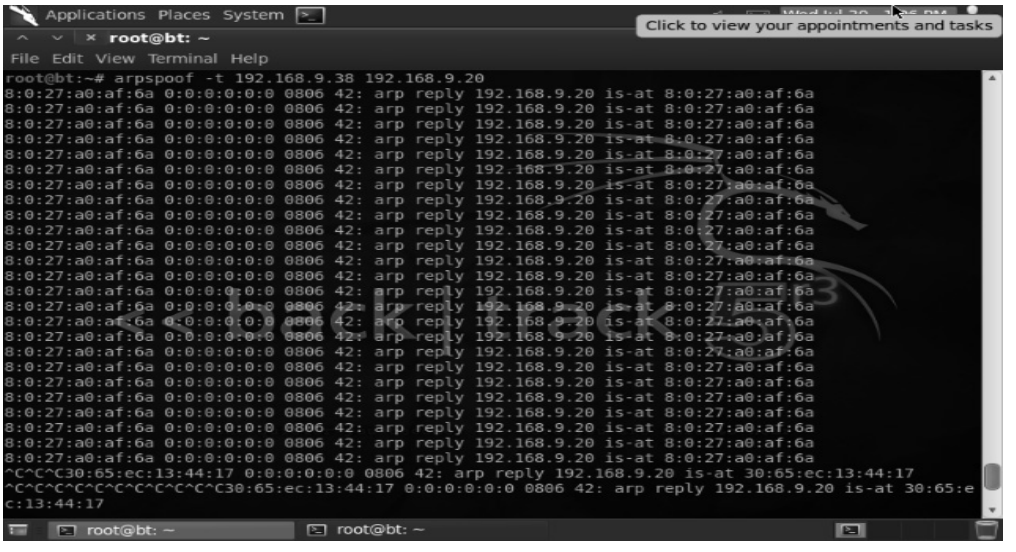

Figure 12 One Way ARP DoS Attack to Gateway

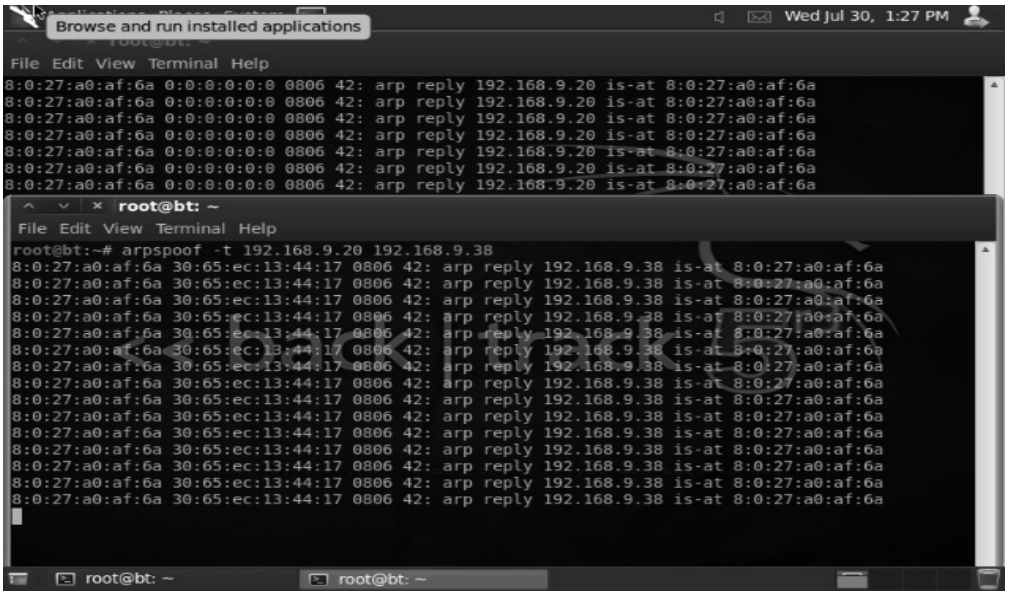

Figure 13 Two-way ARP DoS Attack

สรุปและอภิปรายผล

การจู่โจมเครือข่าย LAN ด้วยวิธี ARP spoof เป็นภัยคุกคามที่ทำให้ผู้ใช้ใน LAN เดียวกันมีความเสี่ยงสูง ต่อการถูกระงับการสื่อสารและการถูกดักจับข้อมูลที่สำคัญเช่น ชื่อผู้ใช้และรหัสผ่านระบบธนาคารออนไลน์ เป็นต้น โดยก่อนหน้านี้ มีผู้พัฒนาเครื่องมือและนำเสนอแนวทางแก้ปัญหา ARP spoof หลากหลาย แต่เครื่องมือเหล่านี้ยังมีปัญหาด้านการใช้งานจริง เช่น เป็นระบบขนาดใหญ่ การติดตั้งมีความยุ่งยาก การปรับเคอร์เนลให้สนับสนุนการป้องกัน และการปรับปรุงโพรโทคอล ARP ซึ่งใช้กับมาตรฐานของ ARP ปกติไม่ได้

งานวิจัยนี้จึงพัฒนาเพื่อปรับปรุงแก้ไขวิธีแก้ปัญหาที่เสนออยู่เดิม เช่น ป้องกันการจู่โจมแบบ ARP DoS ทางเดียว การรายงานสู่ส่วนกลาง ระบบฟื้นฟูการติดเชื้อที่เกตเวย์ และการตรวจจับการปลอมแปลงโพรโทคอล ARP ที่ยังไม่มีประสิทธิผลดีเท่าที่ควร โดยเพิ่มอัลกอริธึมตรวจจับการปลอมแปลงโพรโทคอล ARP จากแนวคิด DepMAC-IP กลไก Gateway-Rehabilitation และกลไกตรวจสอบที่ Gateway ผลการทดลอง ต่อวิธีการใหม่ที่นำเสนอ ภายใต้การจู่โจมแบบ DoSด้วย ARP ทางเดียวและสองทาง และ MitMพบว่ามีประสิทธิผลในการป้องกัน ตรวจจับและรายงานได้ดีมาก โดยมี overhead จากค่าแพ็กเกตสูญหายไม่ถึงร้อยละ 1 ดังนั้นเห็นได้ว่าวิธีการใหม่ที่นำเสนอสามารถป้องกันการถูกระงับการเชื่อมต่อด้วย ARP spoof และป้องกันการการรั่วไหลของข้อมูลได้จึงเป็นวิธีการในการตรวจจับและป้องกัน ARP Spoof ที่มีประสิทธิภาพเพิ่มขึ้น โดยเฉพาะอย่างยิ่ง เมื่อเทียบกับซอฟต์แวร์ที่มีมาก่อน และรวมถึงวิธีแก้ไขอื่นๆ ในงานวิจัยก่อนหน้านี้ ซึ่งมีทั้งหมด 6 แนวทาง ที่พยายามแก้ปัญหาเดียวกัน (ดังที่ได้กล่าวในส่วนต้นของบทความวิจัยนี้) เป้าหมายต่อไปในอนาคต คือการพัฒนาโปรแกรมเต็มรูปแบบ จากต้นแบบนี้เพื่อทดลองกับ site งานจริง คือเป้าหมายต่อไป

กิตติกรรมประกาศ

งานวิจัยนี้ ได้รับการสนับสนุนจากทุนวิจัยคณะวิทยาการสารสนเทศ มหาวิทยาลัยมหาสารคาม

เอกสารอ้างอิง

1. Plummer D. An Ethernet Address Resolution Protocol. IETF RFC 826; Nov 1982.
2. Sanjeev K. Impact of Distributed Denial of Service (DDoS) Attack Due to ARP Storm. Proceedings of International Conference on Networking, France; 2005. pp. 997–1002.
3. Netcut. [cited 1 Jul 2014]. from: http://www.arcai.com/arcai-netcut-faq.html
4. Cain & Abel. [cited 18 Jul 2014]. from: http://www.oxid.it/cain.html
5. Ettercap. [cited 18 Jul 2014]. Availfrom: http://ettercap.github.io/ettercap/
6. Kali Linux. [cited 26 Jan 2014]. from: http://www.kali.org/
7. Abad C, Bonilla R. An Analysis on the Schemes for Detecting and Preventing ARP Cache Poisoning Attacks. Proceedings of Distributed Computing Workshop, Toronto, Canada; 2007.
8. Lootah W, Enck W, McDaniel P. TARP: Ticket-based address resolution protocol. Computer Networks. Oct 2007;51(15):4322–4437.
9. Brusch D, Ornaghi A, Rosti E. S-ARP: a secure address resolution protocol. Proceedings of Computer Security Applications Conference, Dec2003. pp. 66–74.
10. King J, Lauerman K. Layer 2 Attacks and Mitigation Techniques for the Cisco Catalyst 6500 Series. Cisco; 2010 p. 1–87. Report No.: C11603839-00.
11. Anti NetCut 3 1.0. [cited 27 Mar 2014]. from: http://anti-netcut3.software.informer.com/1.0/
12. AntiARP. [cited 1 Jul 2014]. from: http://antiarp.software.informer.com/
13. Barnaba M. Anticap. [cited 4Jul 2014]. from: http://cvs.antifork.org/cvsweb.cgi/anticap
14. Teterin I. Antidote. [cited 4 Jul 2014]. from: http://online.securityfocus.com/archive/1/299929
15. Manwani S. ARP Cache Poisoning Detection and Prevention [MSc Thesis]. San Jose State University; 2003.
16. Prasertsang W, Sriwiset S, Puangpronpitag S. ARP Spoof Attack Detection, Protection and Alert System. Proceeding of National Conference on Computing and Information Technology, Bangkok, Thailand; 2013.
17. Serpanos DN, Lipton RJ. Defense against man-in-the-middle attack in client-server systems. Proceedings of Symposium on Computing and Communication, 2001. pp. 9–14.

18. Ramachandran V, Nandi S. Detecting ARP Spoofing: An Active Technique. Proceedings of the International Conference on Information Security, India; pp. 239–250.
19. Kasabai P, Puangpronpitag S. J-ARP: Light-weight ARP Spoof Protection Software. Proceedings of Joint Conference on Computer Science and Software Engineering, Thailand; 2010. pp. 416–421.
20. Netcut-Defender. [cited 1 Jul 2014]. from: http://www.arcai.com/netcut-defender
21. Fayyaz F, Rasheed H. Using JPCAP to Prevent Man-in-the-Middle Attacks in a Local Area Network Environment. IEEE Potentials. Aug 2012;31(4):35–37.
22. Puangpronpitag S, Masusai N. An Efficient and Feasible Solution to ARP Spoof Problem. Proceedings of International Conference on Electrical Engineering/ Electronics, Computer, Telecommunication and Information Technology, Thailand. 2009. pp. 910–913.
23. Kasabai P, Chuachan T, Puangpronpitag S. ARP Spoof Vaccination and Surveillance System. Proceeding of the National Computer Science and Engineer Conference, Thailand; 2008. pp. 217–224.
24. Organizationally Unique Identifier (OUI) [cited 21 Jan 2014]. from: http://standards.ieee.org/develop/regauth/oui/oui.txt
25. Iperf. [cited 14 Jun 2014]. from: https://iperf.fr/