การประเมินสภาพปัญหาด้านความมั่นคงของชุดซอฟต์แวร์วีโอไอพีแบบโอเพนซอร์ซ

คธาวุฒิ จันบัวลา[1]* และ สมนึก พ่วงพรพิทักษ์[2]

บทคัดย่อ

มีชุดซอฟต์แวร์วีโอไอพีที่เป็นโอเพนซอร์ซหลายแบบบนอินเทอร์เน็ต ในจำนวนเหล่านี้ AsteriskNOW, Trixbox, Elastrix, EZY IP-PBX และ ISANBox.A ได้รับความนิยมมากที่สุด ชุดซอฟต์แวร์เหล่านี้มีประโยชน์อย่างมากสำหรับผู้ดูแลระบบวีโอไอพี เนื่องจากสามารถติดตั้งและจัดการกับระบบได้ง่าย อย่างไรก็ตามประสิทธิภาพด้านความมั่นคงของชุดซอฟต์แวร์เหล่านี้ยังมีปัญหา ดังนั้นงานวิจัยนี้จึงนำเสนอการประเมินเพื่อเปรียบเทียบประสิทธิภาพด้านความมั่นคงของชุดซอฟต์แวร์เหล่านี้ โดยทดลองใช้การจู่โจมหลายเทคนิคบนเครือข่ายการทดสอบ (Test-bed) จากผลการทดลอง ISANBox.A ได้แสดงให้เห็นประสิทธิภาพด้านความมั่นคงสูงที่สุดในบรรดาชุดซอฟต์แวร์ทั้ง 5 ตัว ดังที่ได้กล่าวในข้างต้น นอกจากนี้ผลการทดลองยังแสดงให้เห็นปัญหาด้านความปลอดภัยที่ยังไม่ได้รับการแก้ไขของ ISANBox.A ปัญหาด้านความมั่นคงที่พบจากการทดลองสามารถเป็นแนวทางในการปรับปรุงชุดซอฟต์แวร์วีโอไอพีได้ในอนาคต

คำสำคัญ: วีโอไอพี ชุดซอฟต์แวร์วีโอไอพีแบบโอเพนซอร์ซ

[1] นิสิต ภาควิชาเทคโนโลยีสารสนเทศ คณะวิทยาการสารสนเทศ มหาวิทยาลัยมหาสารคาม

[2] อาจารย์ ภาควิชาวิทยาการคอมพิวเตอร์ คณะวิทยาการสารสนเทศ มหาวิทยาลัยมหาสารคาม

* ผู้นิพนธ์ประสานงาน โทรศัพท์ 08-4954-4774 อีเมล: khathawut.c@gmail.com

รับเมื่อ 30 สิงหาคม 2555 ตอบรับเมื่อ 26 พฤศจิกายน 2555

Security Problem Evaluation of Open Source VoIP Software Packages

Khathawut Chanbuala[1]* and Somnuk Puangpronpitag[2]

Abstract

There are several open-source VoIP software packages on the Internet. Of these, AsteriskNOW, Trixbox, Elastrix, EZY IP-PBX and ISANBox.A are the most popular ones. These packages are very useful for VoIP administrators since they can be easily installed and managed. However, the security performance of these packages is still questionable. Hence, this paper comparatively evaluates their security performance using several attacking techniques. The attacking experiments are run on a test-bed. From the experimental results, ISANBox. A has demonstrated the highest security performance among the aforementioned five packages. Yet, the experimental results have also demonstrated some unsolved security problems of ISANBox.A. The security problems, found from the experiments, can be a guideline to improve the VoIP software packages in the future.

Keywork: VoIP, Open-source VoIP Software Packages, Security Problem, Security Performance

1 Student, Department of Computer Science, Faculty of Informatics, Mahasarakham University.

2 Lecturer, Department of Computer Science, Faculty of Informatics, Mahasarakham University.

* Corresponding Author, Tel. 08-4954-4774, E-mail: khathawut.c@gmail.com

Received 30 August 2012; Accepted 26 November 2012

1. บทนำ

โทรศัพท์ผ่านเครือข่ายอินเทอร์เน็ต Voice over Internet Protocol (VoIP) ในปัจจุบันกำลังได้รับความนิยมเพิ่มมากขึ้นเรื่อยๆ เนื่องจากช่วยลดภาระค่าใช้จ่ายด้านโทรศัพท์ได้จำนวนมากและไม่จำเป็นต้องวางระบบใหม่เพื่อติดตั้งระบบ VoIP เพราะโครงสร้างของ VoIP สามารถติดตั้งใช้งานได้บนระบบเครือข่ายเดิมที่มีอยู่ และเพื่อแทนที่เครือข่ายโทรศัพท์สาธารณะ (PSTN : Public Switch Telephone Network) แบบเดิมที่นิยมใช้อยู่ก่อน

ในอดีตการติดตั้งและใช้งานระบบ VoIP มีความยุ่งยากและซับซ้อนเป็นอย่างมาก Admin จำเป็นต้องมีความรู้ความเข้าใจมากพอสมควรจึงจะสามารถติดตั้งระบบ VoIP เพื่อให้สามารถใช้งานได้ จากปัญหาเหล่านี้ปัจจุบันจึงได้มีผู้พัฒนาชุดซอฟต์แวร์ VoIP ซึ่งรวบรวม Application ต่างๆ ที่จำเป็นต่อการติดตั้งและใช้งานระบบ VoIP โดยรวมไว้ในหนึ่งแผ่นการติดตั้ง เพื่อให้ง่ายต่อการติดตั้งใช้งาน IP-PBX แบบโอเพนซอร์ซตัวที่นิยมนำมาพัฒนาเป็นชุดซอฟต์แวร์ VoIP คือ Asterisk [1] ซึ่งในประเทศไทยมีหน่วยงาน เช่น คณะกรรมการกิจการโทรคมนาคมแห่งชาติ (กทช. หรือ กสทช. ในปัจจุบัน) สถาบันวิจัยและพัฒนาอุตสาหกรรมโทรคมนาคม (TRIDI) โดยร่วมมือกับสถาบันอุดมศึกษาพัฒนาชุดซอฟต์แวร์ VoIP โดยใช้ Asterisk เป็น IP-PBX ชุดซอฟต์แวร์ VoIP ที่นิยมใช้กันซึ่งพัฒนาขึ้นทั้งในประเทศและต่างประเทศ เช่น Trixbox [2] Elastix [3] AsteriskNOW [4] EZY IP-PBX [5] และ ISANBox.A [6] ซึ่งทั้งหมดใช้ Asterisk เป็น IP-PBX แบบโอเพนซอร์ซ

จากงานวิจัย [7] - [10] ได้แสดงให้เห็นถึงปัญหาด้านความมั่นคงจำนวนมากบนระบบ VoIP และจากงานวิจัย [11] ซึ่งได้ทำการประเมินปัญหาความมั่นคงของ IP-PBX Server 3 ตัว คือ FreeSWITCH [12] Asterisk OpenSER [13] ผลคือทั้งหมดมีปัญหาด้านความมั่นคง จากปัญหาเหล่านี้จึงทำให้ชุดซอฟต์แวร์ VoIP ที่ใช้ Asterisk เป็น IP-PBX เข้าข่ายปัญหาด้านความมั่นคง ซึ่งในปัจจุบันยังไม่มีงานวิจัยใดทำการประเมินด้านความมั่นคงกับชุดซอฟต์แวร์ VoIP เหล่านี้อย่างเป็นรูปธรรม

งานวิจัยนี้จึงนำเสนอการประเมินปัญหาความมั่นคงของชุดซอฟต์แวร์ VoIP ที่ใช้ Asterisk เป็น IP-PBX แบบโอเพนซอร์ซ ได้แก่ Trixbox, Elastix, Asterisk NOW, EZY IP-PBX และ ISANBox.A โดยเปรียบเทียบปัญหาด้านความมั่นคงแต่ละตัวว่าแตกต่างกันอย่างไร เพื่อเป็นข้อมูลสำหรับการเลือกใช้ชุดซอฟต์แวร์ VoIP ที่มีประสิทธิภาพด้านความมั่นคง และเป็นแนวทางสำหรับการวิจัยเพื่อแก้ไขความบกพร่องด้านความมั่นคงในอนาคต

2. ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

2.1 VoIP

VoIP ย่อมาจาก Voice over Internet Protocol หรือ IP Telephony เป็นการสื่อสารทางเสียงผ่านโครงข่ายอินเทอร์เน็ต สัญญาณเสียงจะถูกตัดแบ่งเป็น Packet วิ่งผ่านไปบนโครงข่ายที่ใช้สำหรับการสื่อสารข้อมูลทั่วไป แทนการใช้วงจรเฉพาะตามวิธีการสื่อสารในระบบโทรศัพท์สาธารณะแบบดั้งเดิม โดยแบ่งหน้าการทำงานของโพรโทคอลออกเป็น 2 ลักษณะ คือ โพรโทคอลที่ใช้สื่อสารสัญญาณ เช่น Session Initiation Protocol (SIP) [14] และโพรโทคอลที่ใช้ สื่อสารเสียง เช่น Real Time Transport Protocol (RTP) [15] สำหรับกระบวนการสื่อสารเสียงผ่านเครือข่ายอินเทอร์เน็ตจะมีซอฟต์แวร์ที่ทำหน้าที่แปลงสัญญาณ เสียงประเภทอนาล็อก (Analog) เป็นสัญญาณดิจิทัล (Digital) หรือกลุ่มข้อมูล (Packet) แล้วส่งผ่านไปทางอินเทอร์เน็ตและจะมี IP-PBX ทำหน้าที่ควบคุมการรับหรือส่งข้อมูลนั้นก่อนที่จะแปลงข้อมูลดิจิทัลกลับมาเป็นสัญญาณเสียงเมื่อปลายทางได้รับ

2.2 Asterisk

Asterisk [1] คือซอฟต์แวร์เสรีที่อยู่ภายใต้ GNU General Public License (GPL) สามารถดาวน์โหลดใช้ได้ฟรี Asterisk สร้างขึ้นใน ค.ศ. 1999 โดย Spencer ซึ่งทำหน้าที่หลักเป็น Softswitch, IP-PBX หรือที่เรียกว่าตู้ชุมสายโทรศัพท์ระบบ IP มีหน้าที่ในการควบคุมและจัดการบริหารการเชื่อมต่อ ระหว่างอุปกรณ์โทรศัพท์ผ่านโครงข่ายอินเทอร์เน็ต

ในประเทศไทยมีหลายหน่วยงานสำคัญ เช่น คณะกรรมการกิจการโทรคมนาคมแห่งชาติ (กทช. หรือ กสทช. ในปัจจุบัน) สถาบันวิจัยและพัฒนาอุตสาหกรรมโทรคมนาคม (TRIDI) ต่างสนับสนุนการใช้งานและพัฒนาชุดซอฟต์แวร์ VoIP ที่ใช้ Asterisk เป็น IP-PBX

Asterisk จึงเป็นซอฟต์แวร์ VoIP ตัวหนึ่งที่ประเทศไทยให้ความให้ความสนใจและถูกจับตามองเป็นอย่างมาก

2.3 ชุดซอฟต์แวร์ VoIP

ชุดซอฟต์แวร์ VoIP คือซอฟต์แวร์ที่รวม Application ต่างๆ ที่จำเป็นต่อการติดตั้งและใช้งานระบบ VoIP เช่น Operating System (OS), IP-PBX (เช่น Asterisk FreesWITCH OpenSER), Web-Interface, Database และอื่นๆ ไว้ในหนึ่งแผ่นการติดตั้ง ทำให้ติดตั้งและใช้งานได้ง่าย ชุดซอฟต์แวร์ VoIP ที่นิยมใช้ เช่น Trixbox [2], Elastix [3], AsteriskNOW [4]

EZY IP-PBX [5] เป็นชุดซอฟต์แวร์ VoIP ที่พัฒนาจากความร่วมมือระหว่างคณะเทคโนโลยีสารสนเทศมหาวิทยาลัยเทคโนโลยีพระจอมเกล้าธนบุรีและสถาบันวิจัยและพัฒนาอุตสาหกรรมโทรคมนาคม (TRIDI) ซึ่งเป็นชุดซอฟต์แวร์สำหรับการใช้งาน ระบบ Voice Over IP (VoIP) ที่สนับสนุนการใช้งานที่เป็นภาษาไทย

ISANBox.A [6] เป็นชุดซอฟต์แวร์ VoIP ที่กลุ่มผู้พัฒนาได้กล่าวอ้างว่ามีจุดเด่นเรื่องประสิทธิภาพด้านความมั่นคง แต่ก็ยังไม่มีงานวิจัยเพื่อทำการประเมินปัญหาด้านความมั่นคงอย่างเป็นรูปธรรม

2.4 Secure RTP (SRTP)

SRTP [16] เป็นโพรโทคอลที่ถูกพัฒนามาจากโพรโทคอล RTP [15] ซึ่งออกแบบมาเพื่อจุดประสงค์ คือ Confidentiality, Message Authentication, Replay Protection รูปแบบ SRTP เกิดขึ้นจากกระบวนการเข้า-ถอดรหัสของ RTP Payload ซึ่งในแต่ละ SRTP Stream จะมีกระบวนการร้องขอรูปแบบที่จะใช้เข้า-ถอดรหัส (Cryptographic Context) โดยมีพารามิเตอร์ที่จำเป็นต้องร้องขอ เช่น Chosen Cipher, Block Size, Master Key, Session Key เป็นต้น SRTP จะใช้กุญแจสองชนิด คือ Session Key และ Master Key โดย Session Key ใช้ในกระบวนการเข้ารหัสเนื้อความ (Payload Encryption) และรับรองความน่าเชื่อถือ (Message Authentication) ส่วน Master Key เป็นกุญแจที่ถูกสุ่มขึ้นมาใช้ในกระบวนการแลกเปลี่ยนกุญแจเพื่อทำให้ Session Key มีความมั่นคง

2.5 Transport Layer Security (TLS)

Transport Layer Security (TLS) [17] หรือที่รู้จักในวงการ VoIP คือ Secure SIP (SIPS) ซึ่งพื้นฐานเดิมคือ Secure Sockets Layer (SSL) เป็นโพรโทคอลที่ใช้เข้ารหัสข้อมูลที่ส่งในอินเทอร์เน็ต เช่น เว็บเพจ จดหมายอิเล็กทรอนิกส์ โปรแกรมสนทนา และอื่นๆ เพื่อความปลอดภัยในการส่งข้อมูล

2.6 เทคนิคการจู่โจมระบบ VoIP เพื่อใช้ประเมินปัญหาด้านความมั่นคง

จากงานวิจัย [7]-[11] แสดงให้เห็นถึงข้อบกพร่องด้านความมั่นคงจำนวนมากในระบบ VoIP และให้เราทราบถึงเทคนิคการจู่โจมระบบ VoIP ว่าสามารถจู่โจมได้หลากหลายเทคนิคด้วยกัน แต่สำหรับงานวิจัยนี้เราได้เลือกเทคนิคการจู่โจมที่เป็นปัญหาสำคัญ ซึ่งสามารถส่งผลเสียร้ายแรงต่อระบบ VoIP เพื่อนำมาใช้ในประเมินความมั่นคงของชุดซอฟต์แวร์ VoIP (ที่ได้กล่าวไว้ข้างต้น)

Svmap [18] เป็นส่วนหนึ่งของชุดเครื่องมือที่เรียกว่า SIPVicious และเป็นโอเพนซอร์ซ ซึ่งมีความสามารถในการสแกนหาอุปกรณ์ที่เปิดใช้งานโพรโทคอล SIP และ IP-PBX Server บนเครือข่าย Svmap ถูกออกแบบมาให้มีความเร็วในด้านการสแกนหาโพรโทคอล SIP เทคนิคนี้ทำให้แฮกเกอร์รู้ได้ว่าเครื่องไหนเป็น IP-PBX Server และใช้ IP ที่ได้มาทำการจู่โจม Server เหล่านั้น

SIP Registration Hijacking ลักษณะการทำงานคือ UAC (User Agent Client) ต้องทำการยืนยันตัวตนและบอกตำแหน่ง (User location) กับ IP-PBX Server (Registrar) ก่อนจึงสามารถใช้งานได้ ในขณะเดียวกันหากแฮกเกอร์ทำการแทรกแซงการสื่อสาร และแก้ไข Contact

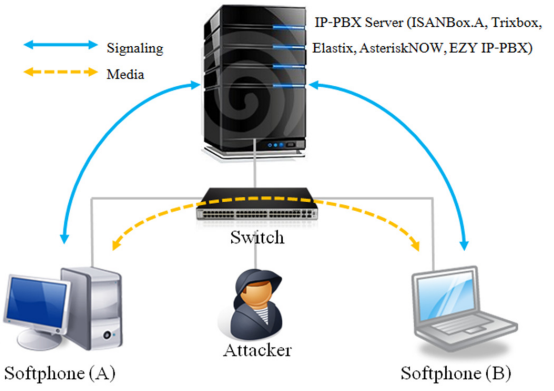
Field ของข้อความ SIP ให้เปลี่ยนเป็น IP Address ของแฮกเกอร์ เมื่อมีสายเรียกเข้า (INVITE) IP-PBX Server จะทำการส่ง Packet ไปยัง IP ของแฮกเกอร์ จากนั้นแฮกเกอร์จะพยายามคันหารหัสผ่านที่ใช้ลงทะเบียนจากข้อความ SIP (REGISTER) ที่ดักจับได้ด้วยวิธีต่างๆ เช่น Directory Attack, Brute-force Attack เป็นต้น

Man-in-the-Middle (MitM) คือการที่แฮกเกอร์ทำการปลอมแปลงการทำงานของโพรโทคอล Address Resolution Protocol (ARP) เพื่อเข้าแทรกแซงการสื่อสารในการสนทนาระหว่างสองฝ่าย แล้วทำหน้าที่เป็นตัวกลางในการรับส่งข้อมูลของคู่สนทนา โดยที่คู่สนทนาไม่สามารถทราบได้ว่ามีผู้อื่นเป็นผู้รับและส่งสารต่อกับคู่สนทนาของตนอยู่ ทำให้แฮกเกอร์สามารถใช้รูปแบบการโจมตีในลักษณะนี้ ในการดักฟังการสนทนาหรือเปลี่ยนแปลงข้อมูลที่ทั้ง 2 ฝั่งสื่อสารกันอยู่ได้

SIP Flooding Attack เป็นการจู่โจมบนโพรโทคอล SIP โดยแฮกเกอร์สามารถปลอมแปลงข้อความ (Malformed Message) เพื่อทำการส่ง INVITE Message จำนวนมากไปยัง IP-PBX Server ส่งผลให้ IP-PBX Server ประมวลผลเพียง INVITE Message ที่แฮกเกอร์ส่งมา ซึ่งจะไม่ตอบสนอง Message อื่นใดนอกจากนี้ส่งผลให้ปฏิเสธการบริการแก่เครื่องลูกข่าย หรือที่เรียกว่า DDoS (Distributed Denial of Service) [10] โดยปกติวิธี Flooding Attack จากต้นทางเดียว (Single Source) เป็นวิธีที่ง่ายต่อการตรวจสอบและป้องกัน แต่ DDoS แฮกเกอร์จะปลอมเป็นเครื่องเหยื่อ หรือ IP-PBX Server แล้วจึงส่ง Packet นั้นออกไป ดังนั้น Packet จึงตอบกลับไปยังเครื่องที่ถูกแฮกเกอร์ปลอม ซึ่งเป็นวิธีที่ตรวจสอบผู้จู่โจมได้ยาก หรืออาจจะตรวจพบเป็นเครื่องเหยื่อ

RTP Flooding Attack เป็นเทคนิคการจู่โจมที่คล้ายกับ SIP Flooding Attack แต่เป็นการจู่โจมบนโพรโทคอล RTP เพื่อทำการรบกวน RTP Packet ปกติ เป็นผลทำให้เสียงที่ได้ยินมีคุณภาพต่ำ

Cancel/Bye attack แฮกเกอร์สามารถปลอมแปลงข้อความ CANCEL หรือ BYE เพื่อยกเลิก และสิ้นสุดการโทรด้วยวิธีแก้ไขข้อความ SIP ของเหยื่อ



รูปที่ 1 เครือข่ายการทดสอบ (Test-bed)

3. การทดลอง

3.1 เครื่องมือและเทคนิคที่ใช้

ในงานวิจัยนี้ทำการประเมินปัญหาด้านความมั่นคงบนเครือข่ายการทดสอบ (Test-bed) โดยทำการติดตั้งชุดซอฟต์แวร์ VoIP ที่เครื่อง Server จากนั้นเชื่อมต่อกับ Switch L2 เครื่องลูกข่ายทั้ง 2 เครื่องติดตั้ง Softphone และเชื่อมต่อเข้ากับ Switch ส่วนเครื่อง Attacker เชื่อมต่อเข้ากับ Switch L2 ตัวเดียวกันดังรูปที่ 1

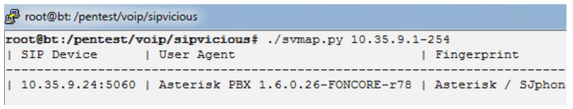
3.1.1 เครื่องมือ

1) เครื่อง IP-PBX Server: Intel(R) Core(TM) 2 Duo CPU E7300 2.66 GHz, 2 GB of RAM, 10/100 Mbps Ethernet Interface Card ชุดซอฟต์แวร์ VoIP ที่ใช้ติดตั้งบนเครื่องแม่ข่าย ได้แก่ Trixbox CE 2.8.0.4, Elastix 2.0.3, AsteriskNOW 1.7.1, EZY IP-PBX ver21T, ISANBox.A 1.0 ซึ่งการทดลองจะสลับการติดตั้ง IP-PBX Server ทีละตัวบนเครื่อง Server ตัวเดิม

2) เครื่องลูกข่าย 2 เครื่อง: ระบบปฏิบัติการ Microsoft Windows 7, Intel(R) Core(TM)2 Duo CPU 1.83 GHz, 3 GB of RAM 10/100 Mbps Ethernet Interface Card และติดตั้ง PhonerLite [19] เพื่อเป็น Softphone

3) เครื่อง Attacker: ระบบปฏิบัติการ Microsoft Windows 7 Intel(R) Core(TM)i5-2500 CPU 3.30 GHz, 4 GB of RAM, 10/100 Mbps Ethernet Interface Card

4) Switch Layer 2: 1 ตัว ซอฟต์แวร์ที่ใช้ใน



รูปที่ 2 ข้อมูลการสแกนหา **IP-PBX Server**

การจู่โจม ได้แก่ Cain&Abel v4.9.40, Backtrack 5, Wireshark v1.4.7

3.1.2 เทคนิคที่ใช้จู่โจมเพื่อประเมินปัญหาด้านความมั่นคง

เทคนิคการจู่โจมที่เลือกใช้เป็นปัญหาที่สำคัญและส่งผลเสียร้ายแรงต่อระบบ VoIP มี 6 เทคนิค ดังนี้

1) SVMAP เพื่อสแกนหา Server ที่เปิดใช้งาน SIP โพรโทคอล

2) SIP Registration Hijacking เพื่อดักจับข้อมูล SIP (REGISTER) และค้นหารหัสผ่านของผู้ใช้บริการ

3) MITM Attack เพื่อดักฟังการสนทนา

4) SIP Flooding Attack เพื่อให้ Server ปฏิเสธการบริการ

5) RTP Flooding Attack เพื่อรบกวนการสนทนา

6) Cancel/Bye Attack เพื่อทำให้การสื่อสารล้มเหลว

4. ผลการทดลอง

4.1 Svmap เพื่อสแกนหา Server ที่เปิดใช้งาน SIP

ทดลองใช้ Svmap ที่อยู่ใน Backtrack 5 สแกนหาโพรโทคอล SIP ที่ถูกเปิดใช้งานในเครือข่ายโดยระบุช่วง IP (ตัวอย่าง: 192.168.1.1-254) ข้อมูลที่ได้จากการสแกนเมื่อพบ IP-PBX Server จะประกอบไปด้วยหลายเลข IP ของ IP-PBX Server Port ที่เปิดใช้งานโพรโทคอล SIP และเวอร์ชันของ IP-PBX ดังรูปที่ 2

วิธีการนี้เป็นวิธีทำให้ได้มาซึ่ง IP เครื่อง IP-PBX Server ซึ่งแฮกเกอร์จะเลือกใช้ IP ที่สแกนพบเพื่อทำการจู่โจมต่อไป จากผลทดลองพบว่า IP-PBX Server เกือบทั้งหมดถูกสแกนพบการเปิดใช้งานโพรโทคอล SIP ยกเว้น ISANBox.A ที่สแกนไม่พบ ดังแสดงในตารางที่ 1

ตารางที่ 1 ผลการสแกนหาโพรโทคอล SIP

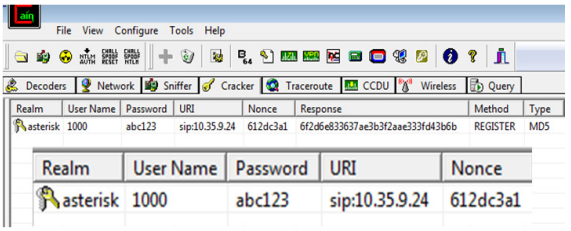
IP PBX Server	สแกนโพรโทคอล SIP
Trixbox	✓
Elastix	✓
AsteriskNOW	✓
EZY IP-PBX	✓
ISANBox.A	×

(✓) สแกนพบโพรโทคอล SIP (×) สแกนไม่พบโพรโทคอล SIP

4.2 SIP Registration Hijacking

ในการทดลอง IP-PBX Server ทุกตัวจะตั้งชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ที่เหมือนกัน Username คือ 1000 และ Password คือ abc123 ทดลองจู่โจมโดยใช้ Cain&Abel ทำการแทรกแซงการสื่อสารเพื่อดักจับข้อมูล SIP (REGISTER) ของ User ที่ลงทะเบียนมาที่ IP-PBX Server เพื่อขอใช้บริการ ซึ่งข้อมูล SIP (REGISTER) ที่ดักจับได้จะประกอบไปด้วยส่วนที่สำคัญคือชื่อผู้ใช้งานและรหัสผ่าน โดยรหัสผ่านจะอยู่ในรูปข้อมูลของ Hash MD5 โดยในตอนแรกรหัสผ่านจะไม่ปรากฏในคอลัมน์ Password ของ Cain&Abel ซึ่งเราสามารถค้นหารหัสผ่านได้ด้วยวิธี Brute-force Attack, Dictionary Attack ส่วนเวลาในการค้นหานั้นจะขึ้นอยู่กับรูปแบบการตั้งรหัสผ่านและความเร็วของเครื่องที่ใช้ประมวลผล ซึ่งเป็นที่แน่นอนว่าถ้าผู้ใช้ตั้งรหัสผ่านที่ง่ายเกินไปแฮกเกอร์สามารถค้นหารหัสได้อย่างรวดเร็ว

จากผลการทดลอง Trixbox, Elastix, AsteriskNOW และ EZY IP-PBX สามารถถูกดักจับข้อมูล SIP (REGISTER) ซึ่งลักษณะข้อมูลที่ Cain&Abel สามารถดักจับได้และสามารถทำการค้นหารหัสผ่านออกมาได้ดังแสดงในรูปที่ 3 แต่สำหรับ ISANBox.A เมื่อจู่โจมแล้วไม่สามารถดักจับข้อมูล SIP (REGISTER) ได้ ซึ่งข้อมูลใน Cain&Abel จะไม่มีปรากฏดังเช่นในรูปที่ 3 และไม่มีข้อมูลที่จะนำมาใช้สำหรับการค้นหารหัสผ่าน เนื่องจาก ISANBox.A สามารถเปิดใช้งานโพรโทคอล TLS โดยมี



รูปที่ 3 ข้อมูลการดักจับ SIP (REGISTER)

เอกสารแนะนำการเปิดใช้งานที่ชัดเจน แต่สำหรับ IP-PBX Server อีก 4 ตัว ซึ่งเป็นเวอร์ชันล่าสุดไม่ค้นพบฟังก์ชันการเปิดใช้งานโพรโทคอล TLS ทำให้ข้อมูลไม่ได้ถูกเข้ารหัส เกิดความไม่มั่นคงในการสื่อสารบนเครือข่าย สรุปผลการทดลองในตารางที่ 2

ตารางที่ 2 ผลการทดลองดักจับ SIP (REGISTER)

IP PBX Server	ดักจับข้อมูล SIP (Register) ได้	ค้นหารหัสผ่านด้วยวิธี Brute-force attack, Dictionary attack
Trixbox	✓	✓
Elastix	✓	✓
AsteriskNOW	✓	✓
EZY IP-PBX	✓	✓
ISANBox.A	×	×

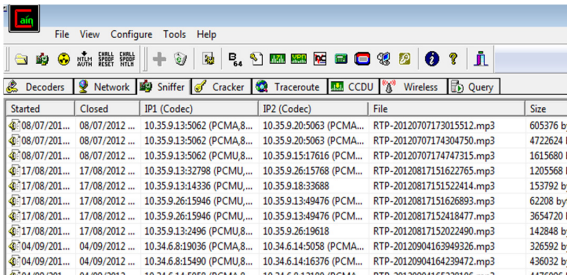
(✓) จู่โจมสำเร็จ (×) จู่โจมไม่สำเร็จ

4.2 MITM Attack เพื่อดักฟังการสนทนา

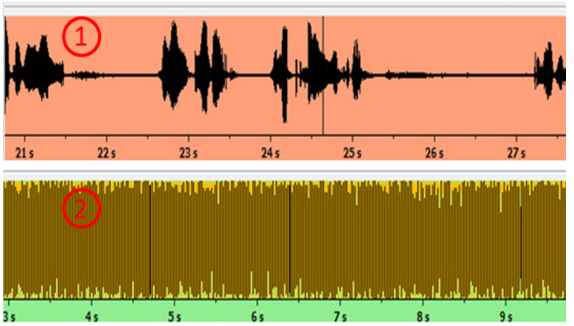
ทดลองใช้ Cain&Abel ทำการแทรกแซงระหว่างการสื่อสาร เพื่อทำการดักฟังการสนทนาของผู้ใช้งานทั้งสองฝั่ง ลักษณะข้อมูลเสียงที่ Cain&Abel สามารถดักจับได้จะทำถูกบันทึกเป็นไฟล์ .mp3 ดังตัวอย่างในรูปที่ 4

จากผลการทดลอง IP-PBX Server ทั้ง 5 ตัว ถูกดักจับข้อมูลเสียงได้ แต่เมื่อเปิดดูลักษณะคลื่นเสียงที่ดักจับได้จะพบว่ามีความแตกต่างกันอยู่ 2 ลักษณะ ดังแสดงในรูปที่ 5

จากรูปที่ 5 หมายเลข 1 คือลักษณะคลื่นเสียงที่ดักจับได้จาก Trixbox, Elastix, AsteriskNOW, EZY IP-PBX ซึ่งแฮกเกอร์สามารถฟังได้เข้าใจเพราะไม่มีการเข้ารหัสเสียง ส่วนหมายเลข 2 เป็นลักษณะคลื่นเสียง



รูปที่ 4 การดักฟังเสียงการสนทนา



รูปที่ 5 ลักษณะคลื่นเสียง ไม่เข้ารหัส (1) –เข้ารหัส (2)

ของ ISANBox.A ซึ่งแฮกเกอร์ไม่สามารถฟังได้เข้าใจจะได้ยินเพียงเสียงซ่าๆ เนื่องจาก ISANBox.A สามารถเปิดใช้งานโพรโทคอล SRTP ได้ จึงทำให้เสียงถูกเข้ารหัส ซึ่งทาง ISANBox.A มีเอกสารบ่งชี้การเปิดใช้งานโพรโทคอล SRTP ที่ชัดเจน แต่สำหรับ IP-PBX Server อีก 4 ตัวนั้นไม่พบฟังก์ชันสำหรับการเปิดใช้งานโพรโทคอล SRTP ทำให้เสียงการสนทนาไม่ถูกเข้ารหัส เกิดความไม่มั่นคงในสนทนาผ่านเครือข่าย ดังสรุปในตารางที่ 3

ตารางที่ 3 ผลการทดลองดักฟังการสนทนา

IP PBX Server	**ดักจับเสียงที่กำลังสนทนากันได้**	**เป็นเสียงที่มนุษย์ฟังเข้าใจ ฟังเข้าใจ**
Trixbox	✓	✓
Elastix	✓	✓
AsteriskNOW	✓	✓
EZY IP-PBX	✓	✓
ISANBox.A	✓	×

(✓) จู่โจมสำเร็จ (×) จู่โจมไม่สำเร็จ

4.3 SIP Flooding Attack เพื่อให้ Server ปฏิเสธการบริการ

SIP Flooding Attack เป็นเทคนิคการจู่โจมที่สามารถส่งผลกระทบหลายด้านต่อ IP-PBX Server ไม่ว่าจะเป็นคุณภาพการให้บริการ การทำงานของหน่วยประมวลผลกลาง (CPU) และหน่วยความจำ (Memory) ดังนั้นในการประเมินจึงต้องพิจารณาตัวชี้วัดดังนี้

1) ปฏิเสธการให้บริการหรือไม่: ในขณะทำการจู่โจม หน่วยประมวลผลกลางและหน่วยความจำมีภาระการทำงานเพิ่มสูงผิดปกติ จนไม่สามารถประมวลผลคำสั่งอื่นๆ ในขณะนั้นได้ จนเป็นสาเหตุทำให้ไม่สามารถให้บริการเครื่องลูกข่ายอื่นๆ ได้ การทดลองใช้ Softphone (PhonerLite 2.0) ทำการลงทะเบียนเพื่อขอใช้บริการจาก IP-PBX Server ขณะที่แฮกเกอร์ทำการจู่โจม จากนั้นดูผลที่เกิดขึ้นว่าจะถูกปฏิเสธการให้บริการจาก IP-PBX Server หรือไม่

2) การทำงานของหน่วยประมวลผลกลาง (CPU Utilization) เพิ่มสูงผิดปกติหรือไม่: ทำการจู่โจม IP-PBX Server จากนั้นตรวจสอบการทำงานของหน่วยประมวลผลกลาง โดยทำการประเมินผลร้อยละของการทำงานทั้งหมดซึ่งแบ่งเป็น 3 ช่วงคือก่อนการจู่โจม ขณะทำการจู่โจม และการฟื้นตัวหลังการจู่โจม

3) หน่วยความจำ (Memory Usage) มีการใช้งานเพิ่มสูงผิดปกติหรือไม่: รูปแบบการประเมินผลหน่วยความจำจะเหมือนกับการประเมินผลของหน่วยประมวลผลกลาง

ทดลองจู่โจมด้วยเทคนิค SIP Flooding Attack โดยใช้ Backtrack 5 ทำการส่งข้อความ INVITE ไปยัง IP-PBX Server ในอัตราความเร็วเฉลี่ย 11,111 Packets ต่อวินาทีดังตัวอย่างในรูปที่ 6 จากนั้นทำการประเมิน IP-PBX Server ตามตัวชี้วัดทั้ง 3 ข้อ (ที่กำหนดไว้ข้างต้น) จากผลการทดลองซึ่งสรุปตามตัวชี้วัดที่กำหนดไว้ได้ผลดังนี้

1) ขณะทำการจู่โจม IP-PBX Server ทดลองใช้ Softphone ที่ติดตั้งบนเครื่องลูกข่าย ทำการลงทะเบียนเพื่อขอใช้บริการจาก IP-PBX Server ผลคือเครื่องลูกข่ายถูกปฏิเสธการให้บริการโดยสิ้นเชิง จาก IP-PBX Server ทั้ง 5 ตัว ซึ่งสรุปคือทั้งหมดไม่สามารถป้องกัน SIP Flooding Attack ได้

```
./inviteflood eth0 target_extension target_domain target_ip
number_of_packets
root@bt:/pentest/voip/inviteflood# ./inviteflood eth0 1000 10.35.9.24
 10.35.9.24 10000000

inviteflood - Version 2.0
              June 09, 2006

source IPv4 addr:port   = 10.35.9.19:9
dest   IPv4 addr:port   = 10.35.9.24:5060
targeted UA             = 1000@10.35.9.24

Flooding destination with 10000000 packets
sent: 141[illegible]709
```

รูปที่ 6 การจู่โจมแบบ SIP Flooding Attack

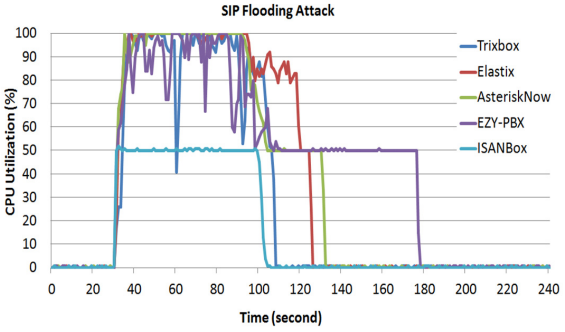
2) เก็บข้อมูลการใช้งานของหน่วยประมวลผลกลางทุกๆ 1 วินาที โดยแบ่งเป็น 3 ช่วงเวลา ได้แก่ ก่อนทำการจู่โจม 30 วินาที ขณะจู่โจม 60 วินาที หลังการจู่โจม 150 วินาที หรือจนกว่าหน่วยประมวลผลกลางของ IP-PBX Server ทุกตัวจะฟื้นตัวกลับเป็นปกติ โดยทำการทดลอง 30 ครั้ง เพื่อให้ได้ผลการทดลองโดยเฉลี่ย (x) ที่ระดับความเชื่อมั่น 95% ดังสรุปในตารางที่ 4

ตารางที่ 4 CPU Utilization

IP PBX Server	Before 30	Attack 60	After 150
	x(%)	*x*(%)	*x*(%)
Trixbox	0.13 ± 0.13	91.28 ± 4.93	8.48 ± 3.80
Elastix	0.17 ± 0.14	96.45 ± 3.21	18.75 ± 5.56
AsteriskNOW	0.27 ± 0.18	96.95 ± 2.54	16.32 ± 4.44
EZY IP-PBX	0.26 ± 0.17	88.98 ± 3.56	30.89 ± 4.37
ISANBox.A	0.27 ± 0.17	50.3 ± 0.13	3.83 ± 2.03

จากตารางที่ 4 พบว่าขณะทำการจู่โจมการทำงานของหน่วยประมวลกลางที่มีการทำงานสูงสุดคือ AsteriskNOW 96.95±2.54 และ Elastix 96.45±3.21 รองลงมาเป็น Trixbox 91.28±4.93, EZY IP-PBX 88.98±3.56, ISANBox.A 50.3±0.13 ตามลำดับ ผลการทดลองแสดงให้เห็นว่า ISANBox.A มีการทำงานของหน่วยประมวลผลกลางในขณะถูกจู่โจมเพิ่มขึ้นน้อยที่สุด

จากข้อมูลในรูปที่ 7 พบว่าเมื่อเริ่มทำการจู่โจมในช่วงเวลาที่ 30 วินาที การทำงานหน่วยประมวลผลกลาง



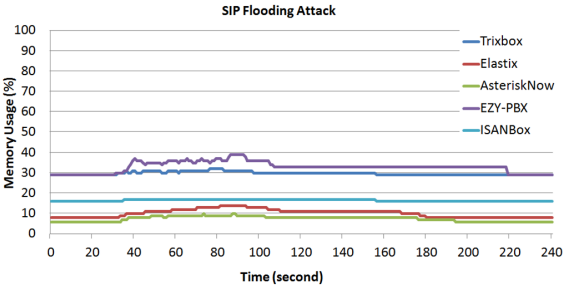
รูปที่ 7 SIP Flooding Attack (CPU Utilization)

ของ IP-PBX Server ทั้งหมดมีการทำงานเพิ่มขึ้นอย่างผิดปกติ โดยเกือบทั้งหมดทำงานเกือบเต็ม 100% มีเพียง ISANBox.A ที่มีการทำงานเฉลี่ย 50% และเมื่อหยุดการจู่โจมที่ช่วงเวลา 90 วินาที การทำงานของหน่วยประมวลผลกลางของเกือบทั้งหมดเริ่มฟื้นตัวจนกลับเป็นปกติในช่วงเวลาที่ 130 วินาทีโดยเฉลี่ย ยกเว้น EZY IP-PBX ที่ใช้เวลาฟื้นตัวกลับเป็นปกติที่ช่วงเวลา 180 วินาทีสรุปคือ ISANBox.A มีการทำงานของหน่วยประมวลผลกลางน้อยที่สุดเมื่อถูกจู่โจม และ EZY IP-PBX ใช้เวลาฟื้นกลับมาเป็นปกติตัวนานที่สุดเมื่อการจู่โจมได้สิ้นสุดลง

3) การเก็บข้อมูลการใช้งานหน่วยความจำของ IP-PBX Server จะทำการเก็บข้อมูลไปพร้อมๆ กับการเก็บข้อมูลการทำงานของหน่วยประมวลผลกลาง โดยจะเก็บข้อมูลทุกๆ 1 วินาที โดยแบ่งเป็น 3 ช่วงเวลา ได้แก่ ก่อนทำการจู่โจม 30 วินาที ขณะจู่โจม 60 วินาที หลังการจู่โจม 150 วินาที เช่นเดียวกับการเก็บข้อมูลหน่วยประมวลผลกลาง ซึ่งผลการทดลองดังแสดงในตารางที่ 5

ตารางที่ 5 Memory Usage

IP PBX Server	Before 30	Attack 60	After 150
	x(%)	*x*(%)	*x*(%)
Trixbox	29.0 ± 0.0	30.83 ± 0.17	29.49 ± 0.09
Elastix	8.0 ± 0.0	11.62 ± 0.43	9.95 ± 0.29
AsteriskNOW	6.0 ± 0.0	8.53 ± 0.42	7.35 ± 0.16
EZY IP-PBX	29.0 ± 0.0	35.27 ± 0.57	32.83 ± 0.31
ISANBox.A	16.0 ± 0.0	16.92 ± 0.07	16.44 ± 0.08



รูปที่ 8 SIP Flooding Attack (Memory Usage)

```
./rtpflood sourcename destinationname srcport destport numpackets
seqno timestamp SSID
root@bt:/pentest/voip/rtpflood# ./rtpflood 10.35.9.23 10.35.9.24
 8000 8002 10000 15000 2000 18800532

Will flood port 8002 from port 8000 10000 times
Using sequence_number 15000 timestamp 2000 SSID 18800532

We have IP_HDRINCL

Number of Packets sent:

Sent 16631 160 1631
```

รูปที่ 9 การจู่โจมแบบ RTP Flooding Attack

จากตารางที่ 5 การเปรียบข้อมูลการใช้งานหน่วยความจำ จะเปรียบเทียบก่อนและหลังการจู่โจมของแต่ละ IP-PBX Server โดยจะไม่เปรียบเทียบกับทั้งหมด เพราะ IP-PBX Server แต่ละตัวใช้งานหน่วยความจำหน่วยความจำที่เพิ่มขึ้นของแต่ละตัว ผลที่ได้พบว่าขณะทำการจู่โจมตัวที่มีการใช้งานหน่วยความจำสูงสุดคือ EZY IP-PBX 6.72% รองลงคือ Elastix 3.62%, AsteriskNOW 2.53%, Trixbox 1.82% และ ISANBox.A 0.92% ตามลำดับ จากข้อมูลพบว่าในขณะจู่โจมการใช้งานหน่วยความจำของแต่ละตัวเพิ่มขึ้นเพียงเล็กน้อย ดังแสดงในรูปที่ 8 และช่วงเวลาการฟื้นตัวของหน่วยความจำจะสอดคล้องกับรูปที่ 7

4.4 RTP Flooding Attack เพื่อรบกวนการสนทนา

ทดลองใช้ Backtrack 5 ทำการจู่โจม IP-PBX Server ขณะที่ Softphone (A) และ Softphone (B) กำลังทำการสนทนา โดยใช้คำสั่งดังตัวอย่างในรูปที่ 9 จากนั้นฟังเสียงการสนทนาเพื่อประเมินคุณภาพเสียงที่ได้ยิน

จากผลการทดลองพบว่า Trixbox, Elastix, Asterisk NOW, EZY IP-PBX เมื่อถูกจู่โจมมีเสียงรบกวนเกิดขึ้นซึ่งทำให้เสียงที่ได้ยินมีคุณภาพต่ำลงอย่างเห็นได้ชัด ส่วน ISANBox.A ไม่มีผลกระทบใดๆ เกิดขึ้นขณะทำการจู่โจม ดังแสดงในตารางที่ 6

ตารางที่ 6 ผลการทดลอง RTP Flooding Attack

IP PBX Server	RTP Flooding Attack
Trixbox	✓
Elastix	✓
AsteriskNOW	✓
EZY IP-PBX	✓
ISANBox.A	×

(✓)จู่โจมสำเร็จ (×) จู่โจมไม่สำเร็จ

4.5 Cancel/Bye Attack เพื่อทำให้การสื่อสารล้มเหลว

ขั้นแรกใช้ Wireshark ดักจับค่า SIP OK Response ของ Softphone (A) และ Softphone (B) ขณะลงทะเบียนเพื่อขอใช้บริการจาก IP-PBX Server ซึ่งมีลักษณะข้อมูลดังรูปที่ 10 จากนั้นจู่โจมด้วย Backtrack 5 โดยใช้ข้อมูลใน SIP OK Response เพื่อทำการจู่โจมดังรูปที่ 11

จากผลการทดลองพบว่า IP-PBX Server เกือบทั้งหมดเมื่อถูกจู่โจมเป็นผลให้การสื่อสารล้มเหลวหรือสิ้นสุดการสนทนาโดยสิ้นเชิง มีเพียง ISANBox.A ที่ไม่เกิดผลกระทบใดๆ ในขณะทำการจู่โจม ดังแสดงในตารางที่ 7

ตารางที่ 7 Cancel/Bye Attack

IP PBX Server	Cancel/Bye Attack
Trixbox	✓
Elastix	✓
AsteriskNOW	✓
EZY IP-PBX	✓
ISANBox.A	×

(✓) จู่โจมสำเร็จ (×) จู่โจมไม่สำเร็จ

5. อภิปรายผลและสรุป

งานวิจัยนี้ได้นำเสนอการประเมินปัญหาด้านความมั่นคงของชุดซอฟต์แวร์ VoIP ที่ใช้ Asterisk เป็น IP-PBX ซึ่งได้แก่ Trixbox, Elastix, AsteriskNOW, EZY IP-PBX และ ISANBox.A โดยการเลือกใช้เทคนิคการจู่โจม 6 เทคนิค เพื่อใช้สำหรับการประเมิน ได้แก่ SVMAP, SIP Registration Hijacking, MITM Attack, SIP Flooding Attack, RTP Flooding Attack, Cancel/Bye Attack จากผลการประเมินปัญหาด้านความมั่นคงพบว่า Trixbox, Elastix, AsteriskNOW และ EZY IP-PBX ทั้งหมดถูกจู่โจมโดยสมบูรณ์จากการจู่โจม 6 เทคนิค มีเพียง ISAN Box.A ที่สามารถป้องกันเทคนิคการจู่โจมได้เกือบทั้งหมด ยกเว้น SIP Flooding Attack ที่ยังเป็นปัญหา สาเหตุปัญหาด้านความมั่นคงที่แตกต่างกันของชุดซอฟต์แวร์ VoIP ที่ใช้ Asterisk เป็น IP-PBX เพราะความแตกต่างของ Asteisk ที่นำมาใช้เป็น IP-PBX ที่เห็นได้ชัดคือ Trixbox, Elastix, AsteriskNOW และ EZY IP-PBX ใช้ Asterisk 1.6 ซึ่งในเวอร์ชันนี้ยังมีปัญหาด้านความมั่นคงอยู่มาก ส่วน ISANBox.A ใช้ Asterisk 1.8 ซึ่งเป็นเวอร์ชันที่มีการแก้ไขปัญหาด้านความมั่นคงเช่น สนับสนุนการใช้งาน TLS และ SRTP ทำให้การสื่อสารในเครือข่ายเกิดความมั่นคง

ความมั่นคงน่าจะเป็นปัจจัยแรกๆ สำหรับการเลือกใช้ชุดซอฟต์แวร์ VoIP ตัวใดตัวหนึ่งเพื่อเป็น IP-PBX Server ในองค์กรหรือหน่วยงาน ในกรณีที่ IP-PBX มีปัญหาด้านความมั่นคงอาจเป็นสาเหตุทำให้ข้อมูลที่สำคัญๆ และเป็นความลับอาจรั่วไหล ทำให้เกิดผลเสีย

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 10.35.9.13;branch=z9hG4bKkfnyfaol;received=10.35.9.13;rport=5060
From: "1000" ;tag=hcykd
To: "1000" ;tag=as644fe807
Call-ID: jwtgckolqnoylqf@backtrack
CSeq: 134 REGISTER
User-Agent: Asterisk PBX
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY
Supported: replaces
Expires: 3600
Contact: ;expires=3600
Date: Tue, 01 Feb 2011 17:55:42 GMT
Content-Length: 0
```

รูปที่ 10 SIP OK Response

```
root@bt: /pentest/voip/teardown
root@bt:/pentest/voip/teardown# ./teardown eth0 1000 10.35.9.24 10.35.9.24
jwtgckolqnoylqf@backtrack hcykd as644fe807

teardown - Version 1.0
           Feb. 17, 2006

source IPv4 addr:port   = 10.35.9.19:9
dest   IPv4 addr:port   = 10.35.9.24:5060
targeted UA             = 1000@10.35.9.24
From Tag                = hcykd
To Tag                  = as644fe807
Call ID                 = jwtgckolqnoylqf@backtrack
```

รูปที่ 11 การจู่โจมแบบ Cancel/Bye Attack

ร้ายแรงต่อองค์กรหรือหน่วยงาน ซึ่งยากที่จะแก้ไขในภายหลัง การป้องกันปัญหาจึงน่าจะเป็นแนวทางที่ดีกว่า ซึ่งผลในงานวิจัยนี้สามารถใช้ข้อมูลสำหรับการตัดสินใจได้ จากผลการประเมินปัญหาด้านความมั่นคงของชุดซอฟต์แวร์ VoIP สรุปโดยรวมแล้ว ISANBox.A เป็นชุดซอฟต์แวร์ VoIP ที่มีประสิทธิภาพด้านความมั่นคงสูงสุด เมื่อเทียบกับทั้งหมดที่ยังมีปัญหาอยู่มาก แต่อย่างไรก็ตาม เทคนิคการจู่โจมแบบ SIP Flooding Attack ก็ยังเป็นปัญหาที่ยังไม่สามารถป้องกันได้ ซึ่งจะเป็นแนวทางสำหรับการทำวิจัยเพื่อแก้ปัญหาในอนาคตต่อไป

6. กิตติกรรมประกาศ

งานวิจัยนี้ได้รับทุนอุดหนุนการวิจัยงบประมาณเงินรายได้ ประจำปีงบประมาณ 2556 มหาวิทยาลัยมหาสารคาม

เอกสารอ้างอิง

[1] Asterisk. (2011, August 8).[Online]. Available: http://www.asterisk.org

[2] Trixbox. (2011, August 8). [Online]. Available: http://www.fonality.com/trixbox

[3] Elastix. (2011, June 18). [Online]. Available: http://www.elastix.org

[4] Asterisk. (2011, August 8). [Online]. Available: http://www.asterisk.org

[5] EZY IP-PBX. (2010, September 8). [Online]. Available: http://voip.sit.kmutt.ac.th/vcww.php

[6] P. Kasabai and S. Puangpronpitag. (2011, November 19). *ISANBox*. [Online]. Available: http://www.isan.msu.ac.th/isan/ISANBox.php

[7] M. Luo, T. Peng, and C. Leckie, "CPU-based DoS Attacks Against SIP Servers," in *Proceedings of Network Operations and Management Symposium (NOMS), IEEE*, 2008, pp. 41-48.

[8] S. Sawda and P. Urien, "SIP Security Attacks and Solutions: A state-of-the-art review," in *Proceedings of ICTTA '06*, Damascus, Syria, 2006, pp. 3187-3191.

[9] D. Butcher, X. Li, and J. Guo, "Security Challenge and Defense in VoIP Infrastructures," *IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews*, vol. 37, pp. 1152-1162, 2007.

[10] D. Sisalem, J. Kuthan, and S. Ehlert, "Denial of Service Attacks Targeting a SIP VoIP Infrastructure: Attack Scenarios and Prevention Mechanisms," *IEEE Network*, vol. 20, pp. 26 - 31, 2006.

[11] P. Kasabai and S. Puangpronpitag, "Problem Evaluation of Security Issues in IP telephony Open Source software," in *Proceedings of National Conference on Computer Information Technologies (CIT)*, Jantaburi, 2010, pp. 33-38.

[12] FreeSWITCH. (2011, August 20). [Online]. Available: http://www.freeswitch.org

[13] Kamailio. (2011, August 30). [Online]. Available: http://www.kamailio.org

[14] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, and R. Spark, "SIP: Session Initiation Protocol," RFC 3261, IETF, 2002.

[15] H. Schulzrinne, S. Casner, R. Frederick, and V. Jacobson, "RTP: A Transport Protocol for Real-Time Applications," RFC 3550, IETF, July 2003.

[16] M. Baugher, D. McGrew, M. Naslund, E. Carrara, and K. Norrman, "The Secure Real-time Transport Protocol (SRTP)," RFC 3711, IETF, March 2004.

[17] T. Dierks and E. Rescorla, "Transport Layer Securiry (TLS)," RFC 5246, IETF, August 2008.

[18] SIPVicious. (2011, August 19). [Online]. Available: http://code.google.com/p/sipvicious

[19] PhonerLite. (2011, January 3). [Online]. Available: http://www.phonerlite.de