การประเมินคุณภาพและความมั่นคงของระบบโทรศัพท์ผ่านอินเทอร์เน็ตของมหาวิทยาลัยราชภัฏร้อยเอ็ด

Security and Quality Evaluation of Rajabhat Roi-et University's VoIP System

สำเริง คำมีวงษ์,[1] คธาวุฒิ จันบัวลา,[2] สมนึก พ่วงพรพิทักษ์ [3]
Sumreng Khummeewong,[1] Khathawut Chanbuala,[2] Somnuk Puangpronpitag[3]

บทคัดย่อ

มหาวิทยาลัยราชภัฏร้อยเอ็ดมหาวิทยาลัย (RERU) ได้มีการใช้งานระบบ Voice over IP (VoIP) ที่ใช้ชุดซอฟต์แวร์ Elastix โดยทำการติดตั้งใช้งานตั้งแต่ ปี ค.ศ. 2011 แต่ทั้งนี้ยังไม่ได้มีการประเมินผลคุณภาพเสียงและด้านความมั่นคงของระบบ VoIP ดังนั้นในงานวิจัยนี้จึงได้ดำเนินการประเมินประสิทธิภาพด้านความมั่นคงและประเมินคุณภาพเสียง VoIP ของ RERU บนระบบจริง สำหรับการประเมินประสิทธิภาพด้านความมั่นคงได้ทดลองใช้การจู่โจม 3 เทคนิค คือ 1) การแทรกกลางการสื่อสาร เพื่อดักจับรหัสผ่านและเสียงการสนทนา 2) การโจมตี SIP Flooding เพื่อให้เครื่องแม่ข่ายชุมสายล่ม ไม่สามารถให้บริการได้ และ 3) การโจมตีเพื่อตัดสายด้วย Cancel/Bye เพื่อตัดสายที่กำลังสนทนา ซึ่งเป็นเทคนิคการจู่โจมที่ง่าย แต่ส่งผลเสียร้ายแรงต่อระบบ สำหรับเครื่องมือจู่โจมที่ใช้ ได้แก่ Backtrack, Cain & Abel และ Wireshark สำหรับการประเมินคุณภาพเสียง ได้ใช้การวัดค่าที่เรียกว่า R-factor และ MOS โดยใช้โปรแกรม Commview เป็นเครื่องมือในการจับคุณภาพเสียง ผลที่ได้แสดงให้เห็นว่า VoIP ของ RERU มีคุณภาพของเสียงที่ดีมาก แต่อย่างไรก็ตาม ยังมีปัญหาใหญ่เกี่ยวกับด้านความมั่นคงที่จะต้องมีการแก้ไขในการทำงานในอนาคต

คำสำคัญ: VoIP Asterisk ความมั่นคง

Abstract

Rajabhat Roi-et University (RERU) has deployed a Voice over IP (VoIP) system using Elastix package since 2011. Yet, there has no evaluation on both voice quality and security of the VoIP system. So, in this paper, we perform the evaluation of both security and voice quality on the real VoIP system of RERU. For the security evaluation, three attacking techniques, namely voice sniffing by Man In the Middle (MITM) attack, IP-PBX server Denial of Services (DoS) attack by SIP flooding, cutting voice connections by Cancel/Bye attacks, are chosen as the attacking techniques due to their simplicity and severe effects. The attacking tools are Backtrack, Cain & Abel and Wireshark, For the voice quality evaluation, R-factor and MOS are deployed as the metrics. Commview is used as the tool to capture the voice quality. The experimental results have shown that the VoIP of RERU provides a good quality of voice. However, it has a big problem with the security issues that need to be fixed in the future work.

Keywords: VoIP, Elasitx, Security

---

[1] *นิสิตปริญญาโท, [2] ผู้ช่วยวิจัยของ ISAN , [3] อาจารย์, กลุ่มวิจัยความมั่นคงสารสนเทศและเครือข่ายชั้นสูง, คณะวิทยาการสารสนเทศ มหาวิทยาลัยมหาสารคาม อำเภอกันทรวิชัย จังหวัดมหาสารคาม 44150*

[1] *Master's degree student, [2] Research Assistant, [3] Lecturer, Information Security and Advanced Network Group, Faculty of Informatics, Mahasarakham University, Kantarawichai District, Maha Sarakham 44150, Thailand.*

* *Corresponding author: Somnuk Puangpronpitag, ISAN Research Group, Faculty of Informatics, Mahasarakham University, Kantarawichai District, Maha Sarakham 44150, Thailand. somnuk.p@msu.ac.th*

บทนำ

ชุดซอฟต์แวร์วีโอไอพีแบบโอเพนซอร์ส ที่พัฒนาบน Asterisk[1] เป็นที่นิยมทั่วไปสำหรับใช้เป็นระบบโทรศัพท์ผ่านอินเทอร์เน็ต (VoIP: VoIP over Internet Protocol) ให้กับหน่วยงานหรือองค์กรต่าง ๆ เพราะสามารถติดตั้งและใช้งานง่าย ประหยัดงบประมาณ ช่วยประหยัดค่าใช้จ่ายในการติดต่อสื่อสารภายในองค์กร รวมถึงการเพิ่มประสิทธิภาพการทำงานขององค์กร ในอดีตมหาวิทยาลัยราชภัฏร้อยเอ็ดได้ใช้ระบบการติดต่อสื่อสารด้วยเครือข่ายโทรศัพท์สาธารณะ (PSTN : Public Switch Telephone Network) ซึ่งมีค่าใช้จ่ายในการติดต่อสื่อสารทั้งติดต่อออกไปยังภายนอกและภายในมหาวิทยาลัย อีกทั้งจะต้องวางระบบชุมสายโทรศัพท์ใหม่ภายในอาคารที่สร้างใหม่ซึ่งมีความยุ่งยากและเป็นการสิ้นเปลืองงบประมาณ ดังนั้นในปี พ.ศ. 2554 ศูนย์คอมพิวเตอร์มหาวิทยาลัยราชภัฏร้อยเอ็ด จึงได้มีการเปลี่ยนระบบโทรศัพท์ภายในจากระบบเดิมเป็นระบบโทรศัพท์ผ่านอินเทอร์เน็ต โดยใช้ Elastix ซึ่งเป็นชุดซอฟต์แวร์วีโอไอพีแบบโอเพนซอร์สที่เป็นที่นิยมตัวหนึ่ง เพื่อใช้เป็นระบบโทรศัพท์ผ่านอินเทอร์เน็ต

จากงานวิจัยของคธาวุฒิ จันบัวลา และ สมนึก พ่วงพรพิทักษ์[2] ได้ทำการประเมินปัญหาด้านความมั่นคงของชุดซอฟต์แวร์วีโอไอพีแบบโอเพนซอร์สที่นิยมใช้กันในปัจจุบัน ซึ่งผลแสดงให้เห็นว่าชุดซอฟต์แวร์วีโอไอพีแบบโอเพนซอร์สบางตัว ไม่มีความมั่นคงที่ดีพอ สำหรับการใช้ในการสื่อสารผ่านระบบเครือข่าย ทำให้ Elastix ที่มหาวิทยาลัยราชภัฏร้อยเอ็ดเลือกใช้เป็นระบบโทรศัพท์ผ่านอินเทอร์เน็ตเข้าค่ายปัญหาเรื่องความมั่นคงที่ต้องได้รับการประเมินเพื่อหาแนวทางสำหรับการป้องกันปัญหาเหล่านั้น ซึ่งแม้มหาวิทยาลัยราชภัฏร้อยเอ็ดได้มีการนำเอาชุดซอฟต์แวร์วีโอไอพีมาใช้มาเป็นเวลานาน แต่กลับยังไม่ได้มีผลการประเมินปัญหาด้านความมั่นคง รวมถึงการทดสอบคุณภาพเสียงที่ให้บริการด้วยว่าได้มาตรฐานหรือไม่

งานวิจัยนี้จึงได้นำเสนอการประเมินปัญหาความมั่นคงระบบโทรศัพท์ผ่านอินเทอร์เน็ตของมหาวิทยาลัยราชภัฏร้อยเอ็ด เพื่อทดสอบข้อเท็จจริงจากงานวิจัย [2,3] ว่า Elastix ที่มหาวิทยาลัยราชภัฏร้อยเอ็ดเลือกใช้เป็นระบบโทรศัพท์ผ่านอินเทอร์เน็ตนั้นเข้าข่ายปัญหาด้านความมั่นคงหรือไม่ และทำการวัดคุณภาพเสียงของระบบโทรศัพท์ผ่านอินเทอร์เน็ตโดยใช้เครื่องมือที่เรียกว่า E-Model [2] ซึ่งข้อมูลที่ได้เพื่อไว้เป็นข้อมูลสำหรับใช้ในการปรับปรุงระบบระบบโทรศัพท์ผ่านอินเทอร์เน็ตของมหาวิทยาลัยราชภัฏร้อยเอ็ดต่อไป

ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

1. VoIP

โทรศัพท์ผ่านเครือข่ายอินเทอร์เน็ต (VoIP: VoIP over Internet Protocol) เป็นขบวนการส่งข้อมูลเสียงและวิดีโอผ่านเครือข่ายอินเทอร์เน็ต โดยอาศัยโพรโทคอลต่อไปนี้

1.1) SIP (Session initiation protocol) [4] เป็น signal protocol เพื่อการสื่อสาร VoIP โดยมีความสามารถในการสร้าง (create), ปรับ (modify) และ ยกเลิก (terminate) การสื่อสารได้ ซึ่ง SIP สามารถปรับเปลี่ยนที่อยู่ (address), หมายเลขพอร์ต เพิ่มสายผู้สนทนา และสามารถเพิ่มหรือลดการส่งข้อมูลมีเดีย (media stream) บางประเภทได้ ตัวอย่างโปรแกรมประยุกต์ที่อาศัย SIP ในการเชื่อมต่อ เช่น video conferencing, streaming multimedia distribution, instant messaging

1.2) RTP (Real Time Protocol) [5] เป็น media protocol ของ VoIP system ทำหน้าที่นำข้อมูลเสียงหรือวิดีโอที่ถูก encode โดย CODEC ไปยังปลายทาง

2. Asterisk

Asterisk[1] เป็นฟรีซอฟต์แวร์ตู้ชุมสายโทรศัพท์ระบบ VoIP สามารถรันได้ทั้งบนระบบปฏิบัติการ Unix, Linux และ Asterisk สามารถรองรับมาตรฐานโพรโทคอล สื่อสารได้หลายโพรโทคอล ไม่ว่าจะเป็น H.232, Session Initiation Protocol (SIP), Media Gateway Control Protocol (MGCP), and Skinny Client Control Protocol (SCCP) หลักการทำงานมีส่วนการควบคุมเป็นเว็บ Web-based Control Panel ทำให้ง่ายต่อการใช้งาน

3. Elastix

Elastix[6] คือ Open Source Software ที่อยู่ภายใต้ลิขสิทธิ์แบบ GPLv2. ถูกติดตั้งอยู่บนระบบปฏิบัติการ Cent OS คือระบบที่นำเอาคุณสมบัติทางด้านเทคโนโลยีการการติดต่อสื่อสารมารวมเข้าไว้ด้วยกัน มีพื้นฐานมาจากระบบ Asterisk ซึ่งเป็นซอฟต์แวร์สำหรับทำตู้สาขา (VoIP) แต่การใช้งาน Asterisk ค่อนข้างจะไม่ค่อยสะดวกนัก เนื่องจากการคอนฟิกค่าต่าง ๆต้องทำผ่านทาง Text mode แต่ Elastix สามารถคอนฟิกค่าต่าง ๆแบบ GUI โดยใช้ผ่านทาง Web brows ซึ่งทำให้สะดวกในการใช้งานอย่างมาก

4. ISANBox

ISANBox.A[7] เป็นชุดซอฟต์แวร์ VoIP ที่พัฒนาโดยทีมนักวิจัยจากกลุ่มวิจัย Information Security and

Advanced Network (ISAN) คณะวิทยาการสารสนเทศ มหาวิทยาลัยมหาสารคาม ISANBox.A พัฒนาขึ้นจาก Asterisk ซึ่งมีคุณสมบัติ เด่นๆ คือ สนับสนุนการใช้งาน TLS เพื่อเข้ารหัสสัญญาณก่อนที่จะส่งข้อมูลผ่านเครือข่ายทำให้มีความมั่นคงทางด้านสัญญาณ (Signal) สนับสนุนการใช้งาน SRTP เพื่อเข้ารหัสข้อมูลเสียงสนทนาเพื่อป้องกันการดักฟังระหว่างการสนทนา ทำให้มีความมั่นคงทางด้าน ภาพและเสียง (Media) ใช้งานได้ง่าย ISANBox.A รองรับการตั้งค่า และการควบคุมสามารถทำได้ผ่านหน้าเว็บ ซึ่งทำให้ใช้งานได้ง่าย สนับสนุนการใช้งานหน้าเว็บที่เป็นภาษาไทย ใช้งานได้ฟรี เนื่องจาก ISANBox.A ถูกสร้างจาก Asterisk ซึ่งเป็นซอฟต์แวร์ โอเพนซอร์สที่ไม่เสียค่าลิขสิทธิ์ ดังนั้น ISANBox.A จึงเป็นซอฟต์แวร์โอเพนซอร์ส โดยมุ่งเน้นให้แก่หน่วยงานราชการ บริษัทขนาดเล็กและขนาดกลาง หรือผู้สนใจทั่วไป

5. วิธีการจู่โจมระบบ VoIP เพื่อประเมินปัญหาความมั่นคง

การจู่โจมด้วย MITM Attack[8] เป็นการแทรกกลางการสื่อสาร โดยวิธีการโจมตีด้วย ARP Spoof โดยผู้จู่โจมจะสร้าง ARP Reply ปลอมเข้าไปหาเครื่องเป้าหมาย โดยจะโยง IP address ของเครื่อง Server เข้ากับ MAC Address ของเครื่องผู้จู่โจมเพื่อเป็นการลวงให้มีการ Update ARP table ขึ้นใหม่และใช้วิธีการเดียวกันในการลวง Server โดยจะสร้าง ARP Reply ขึ้นมาแล้วโยง IP Address ของเครื่องเหยื่อเข้ากับ MAC address ทำให้การส่งข้อมูลทั้งหมดต้องผ่านเครื่องผู้จู่โจมซึ่งสามารถที่จะดักฟังข้อมูลข่าวสารหรือแก้ไขรวมไปถึงการขัดขวาง การส่งข้อมูลทั้งหมดก็ย่อมเป็นไปได้โดยผู้โจมตีนั้นต้องทำให้เหยื่อเชื่อว่ากำลังเชื่อมต่อโดยตรงอยู่เช่น รหัสผ่าน เข้าสู่ระบบ หรือข้อมูลที่เป็นความลับต่างๆ ก็อาจถูกผู้จู่โจมดักจับได้

การจู่โจมด้วย SIP Flooding Attack[9] ผู้จู่โจมสามารถปลอมแปลงข้อความ (Malformed Message) ส่งให้ IP-PBX Server ในที่จำนวนมหาศาล ส่งผลให้ IP-PBX Server มีสภาวะการทำงานเพิ่มสูงขึ้นผิดปกติ จนเป็นสาเหตุทำให้ไม่สามารถให้บริการ หรือที่เรียกว่า Denial of Service (DoS)[10] โดยปกติวิธี Flooding Attack จากต้นทางเดียว (Single Source) เป็นวิธีที่ง่ายต่อการตรวจสอบ และป้องกัน แต่ DDoS ผู้จู่โจมจะปลอมเป็นเครื่องเหยื่อ หรือ IP-PBX Server แล้วจึงส่ง Packet นั้นออกไป ดังนั้น Packet จึงตอบกลับไปยังเครื่องที่ถูกผู้จู่โจมปลอม ซึ่งเป็นวิธีที่ตรวจสอบผู้จู่โจมได้ยาก หรืออาจจะตรวจพบเป็นเครื่องเหยื่อ

การจู่โจมด้วย Cancel/Bye Attack[11] ผู้จู่โจมสามารถปลอมแปลงข้อความ CANCEL หรือ BYE เพื่อยกเลิกและสิ้นสุดการโทรด้วยวิธีแก้ไข Caller ID, Form tag, To tag ของข้อความ SIP ของเหยื่อ

จากการศึกษางานวิจัยที่เกี่ยวข้อง พบว่าทั้งสามเทคนิคขั้นต้นเป็นเทคนิคสำคัญที่ใช้ในการจู่โจมระบบ VoIP โดยมีข้อน่าสนใจที่การดำเนินการนั้นทำได้ง่าย และมีเครื่องมือปรากฏเพื่อ download มาใช้ได้จากอินเทอร์เน็ต แต่มีผลลบที่รุนแรง

6. E-Model

E-Model[12] ถูกกำหนดเป็นมาตรฐานใน Recommendation G.107 โดย International

Telecommunications Union (ITU) เป็นแบบจำลองหรือเครื่องมือในการวิเคราะห์คุณภาพเสียงที่ใช้สำหรับการวางแผนเครือข่าย ซึ่งผลลัพธ์พื้นฐานของ E-Model คือการคำนวณจาก R-factor ซึ่งครอบคลุมปัจจัยสภาพแวดล้อมต่างๆ ที่มีผลต่อคุณภาพเสียง เช่น Delay, Packet Loss และ Jitter เป็นต้น สูตรคำนวณหา R-factor สำหรับ E-model ดังสมการ 1

$$R = R_o - I_s - I_d - I_{ef-eff} + A \qquad (1)$$

โดยที่ R_o = อัตราส่วนระหว่างสัญญาณต่อเสียงรบกวน (Signal to Noise Ratio)

I_s = ค่าความบกพร่องทั้งหมดที่เกิดขึ้นมากหรือน้อยที่เกิดขึ้นพร้อมกันกับสัญญาณเสียง

I_d = ค่าความบกพร่องที่เกิดจากความล้าช้า (Delay)

I_{ef-eff} = ค่าการสูญเสีย Packet (Packet Loss) ที่มีผลขึ้นอยู่กับความบกพร่องของอุปกรณ์

A = ค่าปัจจัยความได้เปรียบการเข้าถึงการเชื่อมต่อของอุปกรณ์

สำหรับการวัดคุณภาพเสียงยังมีอีกวิธีหนึ่งคือวิธีการที่เรียกว่า MOS (Mean Opinion Score)[13] ซึ่งการวัดคุณภาพเสียงแบบ MOS เป็นวิธีที่ง่ายและเป็นที่ยอมรับถึงผลการวัดคุณภาพเสียงที่ได้ โดยให้ผู้ประเมินจำนวนมากทดสอบฟังเสียงการสนทนาเพื่อให้คะแนนคุณภาพเสียง แต่วิธีการนี้มีข้อเสียคือ เสียเวลามากและสิ้นเปลืองงบประมาณ งานวิจัยจึงได้เลือกใช้การวัดคุณภาพเสียงแบบ E-Model เพราะสามารถใช้โปรแกรมวิเคราะห์ผลของเสียงที่ได้จากสมการที่ 1 ได้โดยไม่จำเป็นต้องใช้ผู้คนจำนวนมากเพื่อประเมินคุณภาพเสียง

7. งานวิจัยที่เกี่ยวข้อง

จากงานวิจัยของคธาวุฒิ จันบัวลา และสมนึก พ่วงพรพิทักษ์[2] ได้ทำการประเมินปัญหาด้านความมั่นคงชุดซอฟต์แวร์ VoIP ที่เป็นที่นิยมใช้กันทั่วไป 5 ตัวได้แก่ Trixbox, Elastix, AsteriskNOW, EZY IP-PBX, ISANBox.A โดยใช้การจู่โจมเพื่อประเมินผล ได้แก่ Svmap, SIP Registration Hijacking, MITM Attack, SIP Flooding Attack, RTP Flooding Attack และ Cancel/Bye Attack ผลปรากฏว่าชุดซอฟต์แวร์ที่มีความมั่นคงดีที่สุด คือ ISANBox.A และได้มีการวัดคุณภาพเสียงเพื่อดูผลกระทบความมั่นคงที่มีของ ISANBox.A จะมีผลอย่างไรต่อคุณภาพการให้บริการ โดยใช้เครื่องมือการวัดที่เรียกว่า E-model ผลที่ได้คือ ISANBox.A ได้คุณภาพเสียงที่อยู่ในเกณฑ์เสียงที่มีคุณภาพ

จากงานวิจัยของปิยวัจน์ ค้าสบาย และสมนึก พ่วงพรพิทักษ์[3] ได้ทำการประเมินปัญหาด้านความมั่นคงของซอฟต์แวร์ VoIP แบบโอเพนซอร์ส 3 ตัว ได้แก่ Asterisk, FreeSWITCH และ Kamailio ซึ่งซอฟต์แวร์เหล่านี้เป็นที่รู้จักและนิยมใช้กันมากทั้งในและต่างประเทศ แต่ยังไม่มีการประเมินปัญหาด้านความมั่นคงที่ชัดเจน เพื่อเปรียบเทียบปัญหาที่เกิดขึ้นกับซอฟต์แวร์ VoIP แต่ละตัว โดยใช้เทคนิคการจู่โจม คือ SIP Flooding Attack, Cancel/Bye Attack, MITM Attack ผลที่ได้คือ ซอฟต์แวร์ VoIP ทั้ง 3 ตัวถูกจู่โจมด้วย 3 เทคนิคอย่างสมบูรณ์

จากการศึกษางานวิจัยเหล่านี้แล้วพบว่าระบบโทรศัพท์ผ่านอินเทอร์เน็ตของมหาวิทยาลัยราชภัฏร้อยเอ็ดใช้อยู่ในปัจจุบันสุ่มเสี่ยงต่อการมีปัญหาเรื่องความมั่นคงเพราะได้มีการใช้งาน Elastix เป็น IP-PBX Server ซึ่งสอดคล้องกับผลงานวิจัยข้างต้นว่าไม่มีความมั่นคงที่ดี แต่ยังไม่มีงานวิจัยที่ทำการประเมินในระบบจริง ว่ามีปัญหามากน้อยอย่างไร

วิธีดำเนินการวิจัย

1. การประเมินปัญหาด้านความมั่นคงระบบโทรศัพท์ผ่านอินเทอร์เน็ตของมหาวิทยาลัยราชภัฏร้อยเอ็ด

งานวิจัยนี้ทำการประเมินปัญหาด้านความมั่นคงบนเครือข่าย Network จริงของมหาวิทยาลัยราชภัฏร้อยเอ็ด โดยมหาวิทยาลัยราชภัฏร้อยเอ็ดได้ใช้งาน Elastix v.2.3.0 (Asterisk v.1.8.7) เพื่อเป็น IP-PBX Server ของระบบโทรศัพท์ผ่านอินเทอร์เน็ตบนเครื่อง Server 1 เครื่อง และทำการติดตั้ง IP Phone ซึ่งกระจายไปทั้ง 8 อาคาร ซึ่งได้แก่ อาคารเฉลิมพระเกียรติ 60 พรรษามหาวชิราลงกรณ อาคาร 80 พรรษา 5 ธันวาคม พ.ศ. 2550 อาคารวิทยกิจที่ปังกร คณะพยาบาลศาสตร์ ศูนย์ภาษาและคอมพิวเตอร์ ศูนย์วิทยบริการ โรงเรียนสาธิต และหอพักนักศึกษาดัง Figure 1

1.1 เครื่องมือและสำหรับการประเมินปัญหาด้านความมั่นคง

1) เครื่องผู้จู่โจม (Attacker): Intel(R) Core(TM) i7-4702MQ CPU@2.20GHz, 8 GB of RAM, 10/100 Mbps Ethernet Interface Card

2) ซอฟต์แวร์ ที่ใช้ในการจู่โจมและดักจับข้อมูล

- Cain & Abel v4.9.56
- Kali Linux v1.1.0a
- Wireshark v1.12.4

1.2 วิธีการจู่โจมที่ใช้สำหรับการประเมินปัญหาด้านความมั่นคง

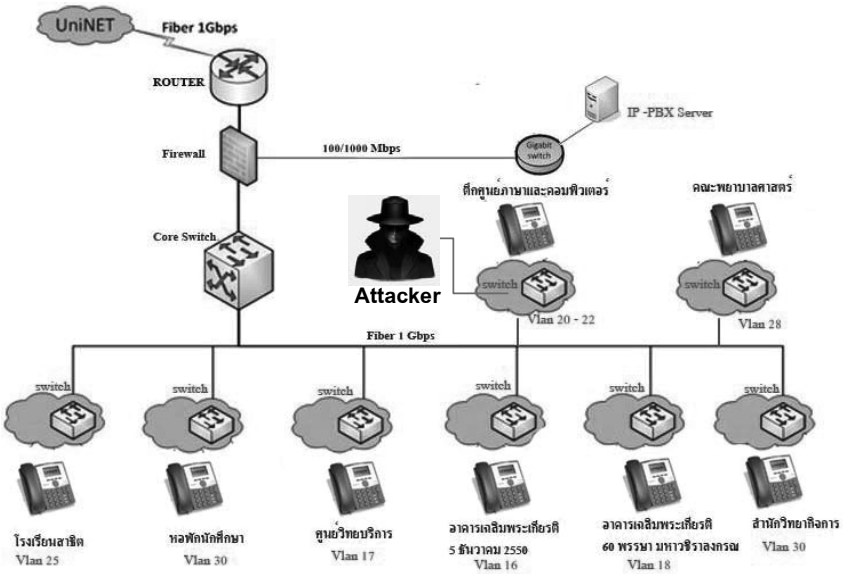

Figure 1 The Structure of VoIP System of RERU

งานวิจัยเลือกใช้วิธีการจู่โจมที่ทำได้ง่ายแต่ส่งผลเสียร้ายแรงต่อระบบโทรศัพท์ผ่านอินเทอร์เน็ต 3 วิธีดังนี้

1) การจู่โจมด้วย MITM Attack เพื่อดักจับ รหัสผ่านและเสียงการสนทนา

2) การจู่โจมด้วย SIP Flooding Attack เพื่อให้ Server ล่มไม่สามารถให้บริการได้

3) การจู่โจมด้วย Cancel/Bye Attack เพื่อ ตัดสายที่กำลังสนทนา

2. การประเมินคุณภาพเสียงระบบโทรศัพท์ผ่านอินเทอร์เน็ต ของมหาวิทยาลัยราชภัฏร้อยเอ็ด

งานวิจัยได้ทำการวัดคุณภาพเสียงบนเครือข่ายจริงของระบบโทรศัพท์ผ่านอินเทอร์เน็ต มหาวิทยาลัยราชภัฏร้อยเอ็ด และการประเมินปัญหาด้านความมั่นคง ดัง Figure 2 โดยเลือกใช้วิธีการวัดคุณภาพเสียงระบบโทรศัพท์ผ่านอินเทอร์เน็ตที่เรียกว่า E-Model ซึ่งเป็นแบบจำลองหรือเครื่องมือในการวิเคราะห์คุณภาพเสียงที่ใช้สำหรับการวางแผนเครือข่าย ซึ่งผลลัพธ์พื้นฐานของ E-Model คือ การคำนวณค่าจาก R-factor โดยใช้โปรแกรม Commview ซึ่งสามารถวัดค่า R-factor ออกมาได้ทันทีและ

สามารถแปลงไปเป็นค่า MOS เพื่อเป็นค่าที่ดูได้ง่ายและเข้าใจ

สำหรับการวัดคุณภาพเสียง งานวิจัยได้ทำการทดลองที่อาคารศูนย์ภาษาและคอมพิวเตอร์ และ อาคาร 80 พรรษา 5 ธันวาคม พ.ศ. 2550 เนื่องจากดูจากสถิติการใช้งานเครือข่ายของมหาวิทยาลัย แล้วพบว่า เป็นจุดที่มี traffic หนาแน่น และมี delay สูงที่สุด และได้เลือกช่วงเวลาออกเป็น 2 ช่วงคือ ช่วงเวลาที่มีการใช้งานเครือข่ายมากที่สุด (Peak Time) เวลาตั้งแต่ 15.00 น. ถึง 16.00 น. และช่วงเวลาที่มีการใช้งานเครือข่ายน้อยที่สุด (off peak time) เลือกเวลาตั้งแต่ 6.00 น. ถึง 7.00 น. โดยการพิจารณาจากสถิติย้อนหลังแสดงค่า Traffic การใช้งานอินเทอร์เน็ตของมหาวิทยาลัยราชภัฏร้อยเอ็ดดัง Figure 2 ซึ่งการวัดคุณภาพเสียงทั้ง 2 ช่วงเวลาจะวัดช่วงเวลาละ 30 ครั้งและคำนวณหาค่าเฉลี่ยที่ระดับความเชื่อมั่น 95% ซึ่งผลการวัดเสียงที่มีคุณภาพที่สามารถยอมรับได้ ค่า R-factor ต้องไม่น้อยกว่า 70 หรือ ค่า MOS ต้องไม่น้อยกว่า 3.5 ซึ่งเป็นไปตามมาตรฐานที่ กสทช. ใช้ในการวัดคุณภาพ Voice over Internet Protocol หรือ Internet Telephony ที่ยอมรับได้

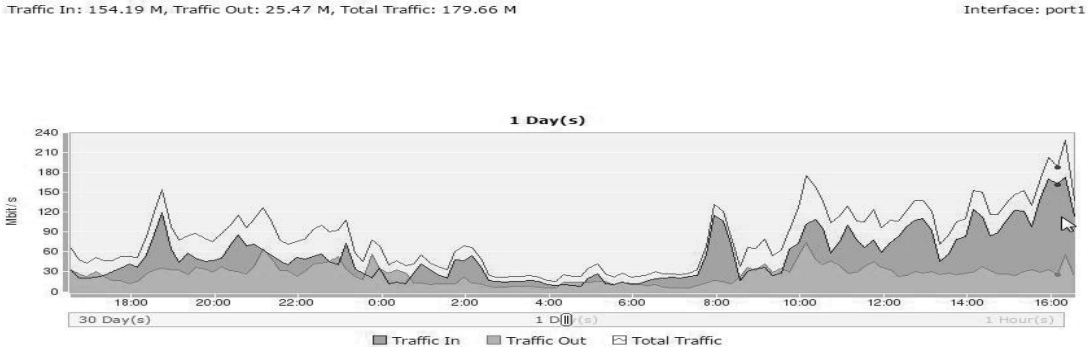

Figure 2 Internet Traffic of RERU

ผลการวิจัย

จากที่งานวิจัยได้ทำการประเมินปัญหาด้านความมั่นคงและวัดคุณภาพเสียงระบบโทรศัพท์ผ่านอินเทอร์เน็ตได้ผลการวิจัยดังนี้

1. ผลการประเมินปัญหาด้านความมั่นคงระบบโทรศัพท์ผ่านอินเทอร์เน็ตของมหาวิทยาลัยราชภัฏร้อยเอ็ด

1.1 ผลการจู่โจมด้วย MITM Attack เพื่อดักจับรหัสผ่านและเสียงการสนทนา สำหรับการจู่โจมด้วย MITM Attack จะแบ่งเป็นการจู่โจม 2 ส่วนคือ 1) เพื่อดักจับ SIP User และ Password ที่ใช้สำหรับการลงทะเบียนเพื่อขอใช้บริการโทรศัพท์ผ่านอินเทอร์เน็ตจาก IP-PBX Server ผลที่ได้คือ Cain & Able สามารถแทรกกลางการสื่อสารและดักจับ SIP User ได้ แต่ในส่วนของ Password ยังไม่แสดงค่าให้เห็นดัง Figure 3 สำหรับการให้ได้มาซึ่ง Password จะด้วยวิธีการที่เรียกว่า Brute-Force Attack หรือการสุ่มเดารหัสผ่าน ซึ่งผลที่ได้คือ Cain & Abel สามารถสุ่มเดา Password ออกมาได้ดัง Figure 4 ซึ่งระยะการสุ่มนั้นจะขึ้นอยู่กับความเร็วของเครื่องที่ใช้จู่โจม

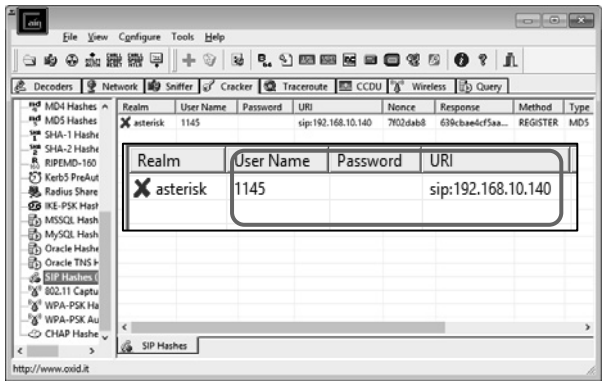

Figure 3 Sniffing SIP Username and Password

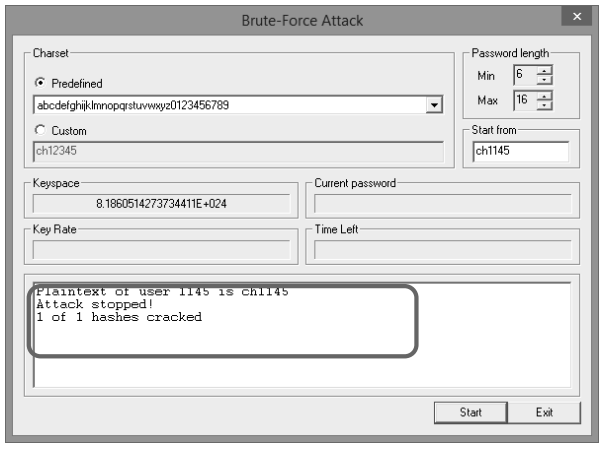

Figure 4 Brute-force Attack

2) ผลการจู่โจมด้วย MITM Attack เพื่อดักฟังเสียงการสนทนา ผลที่ได้คือ Cain & Able สามารถดักจับเสียงที่สนทนาบนระบบโทรศัพท์ผ่านอินเตอร์เน็ตได้ โดยโปรแกรมสามารถบันทึกเป็นไฟล์ .MP3 ซึ่งสามารถเปิดฟังเสียงได้ทันที ดัง Figure 5

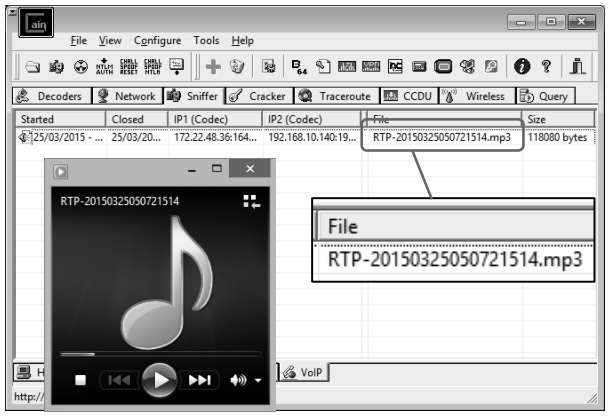

Figure 5 Voice Sniffing

1.2 ผลการจู่โจมด้วย SIP Flooding Attack เป็นการจู่โจมเพื่อให้ IP-PBX Server ล่มจนไม่ได้สามารถให้บริการได้ โดยการ จู่โจมในงานวิจัยใช้ Kali Linux เพื่อทำการยิง INVITE Message จำนวนมากไปยัง IP-PBX Server ดัง Figure 6 จนทำให้ การทำงานของหน่วยประมวลผลกลาง (CPU) และหน่วยความจำ (Memory) เพิ่มสูงจนไม่สามารถประมวลผลคำสั่งอื่นๆ ที่เข้ามายัง IP-PBX Server ได้ จนเป็นสาเหตุทำให้ไม่สามารถให้บริการโทรศัพท์ผ่านอินเทอร์เน็ตได้ โดยก่อนการจู่โจมได้ทำการเปิดหน้าตาการทำงานของหน่วยประมวลผลกลาง และหน่วยความจำของ IP-PBX Server เพื่อดูการทำงานการปกติ ดัง Figure 7 เมื่อทำการจู่โจมไปยัง IP-PBX Server การทำงานของหน่วยประมวลผลกลาง และหน่วยความจำ มีการทำงานเพิ่มขึ้นมากอย่างเห็นได้ชัดดัง Figure 8 จากนั้นทดลองใช้ IP Phone ทำการลงทะเบียนไปยัง IP-PBX เพื่อขอใช้บริการ จากผลการทดลองที่ได้คือ IP-PBX Server ไม่มีการตอบสนองใดๆ ต่อ IP Phone ที่ร้องขอการลงทะเบียนขณะมีการจู่โจม ซึ่งสรุปได้ว่าการจู่โจมดังกล่าวได้ผล

Figure 6 SIP Flooding Attack

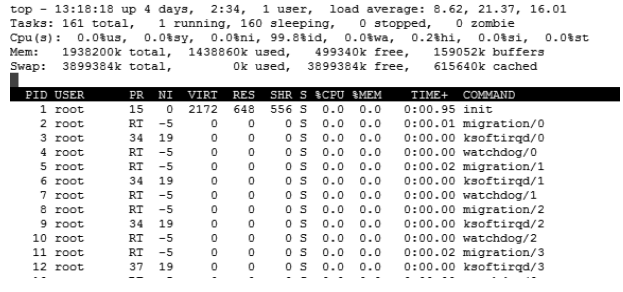

Figure 7 CPU and Memory Loads before Attack

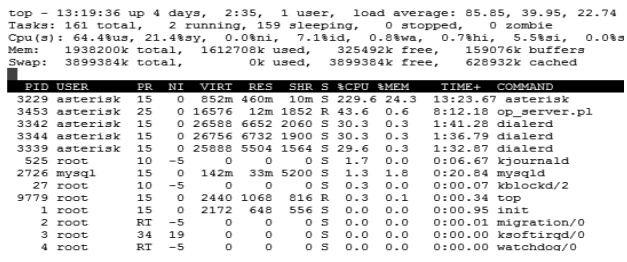

Figure 8 CPU and Memory Loads after Attack

1.3 ผลการจู่โจมด้วย Cancel/Bye Attack เป็นการยิงแพ็คเก็ตเพื่อตัดสายการสนทนาของคู่สายที่สื่อสารบนระบบโทรศัพท์ผ่านอินเทอร์เน็ต โดยการจู่โจม จะทำการใช้ Cain & Able เพื่อแทรกกลางการสื่อสารระหว่างเครื่องเหยื่อที่กำลังสนทนา จากนั้นใช้ Wireshark ดักจับแพ็คเก็ต ของโพรโทคอล SIP เพื่อให้ได้ SIP OK Response จากนั้นทำการค้นหา ACK Message ดัง Figure 9 ซึ่งภายใน ACK Message จะใช้เป็นข้อมูลสำหรับการจู่โจม

```
ACK sip:1145@192.168.10.140:5060 SIP/2.0
Via: SIP/2.0/UDP 172.22.20.69:5060;branch=z9hG4bK-44cc3876
From: "1118" <sip:1118@192.168.10.140>;tag=b0c12d82b892c72b0
To: "ch-com" <sip:1145@192.168.10.140>;tag=as11621bd2
Call-ID: 9d96218e-4aad828f@172.22.20.69
CSeq: 102 ACK
Max-Forwards: 70
Authorization: Digest username="1118",realm="asterisk",nonce="052c
Contact: "1118" <sip:1118@172.22.20.69:5060>
User-Agent: Cisco/SPA303-7.4.9c
Content-Length: 0
```

Figure 9 ACK Message

เมื่อได้ข้อมูลที่ต้องการในขั้นตอนการจู่โจมจะใช้ Kali Linux ยิงแพ็คเก็ตไปตัดสายการสนทนาของเหยื่อดัง Figure 10 จากผลการทดลองสามารถตัดสายของเหยื่อที่กำลังสนทนาลงได้โดยสมบูรณ์

Figure 10 Cancel/Bye Attack

Table 1 1Summary of VoIP Security

วิธีการจู่โจม	ผลการจู่โจม
MITM Attack	สำเร็จ
SIP Flooding Attack	สำเร็จ
Cancel/Bye Attack	สำเร็จ

จาก Table 1 ผลพบว่าวิธีจู่โจมสำหรับการประเมินความมั่นคง ทั้ง 3 วิธี คือ 1) MITM Attack 2) SIP Flooding Attack เพื่อให้ Server ล่มไม่สามารถให้บริการได้ 3) Cancel/Bye Attack ทั้งหมดสามารถจู่โจมระบบโทรศัพท์ผ่านอินเทอร์เน็ตของมหาวิทยาลัยราชภัฏร้อยเอ็ดได้

2. ผลการวัดคุณภาพเสียงระบบโทรศัพท์ผ่านอินเทอร์เน็ตของมหาวิทยาลัยราชภัฏร้อยเอ็ด

การวัดคุณภาพเสียงระบบโทรศัพท์ผ่านอินเทอร์เน็ตของมหาวิทยาลัยราชภัฏร้อยเอ็ด งานวิจัยได้ใช้โปรแกม Commview ดัง Figure 11 เพื่อเป็นเครื่องมือในการวัดคุณภาพเสียงและทำการแบ่งช่วงเวลาการวัดออกเป็น 2 ช่วงเวลา ซึ่งได้ผลดัง Table 2

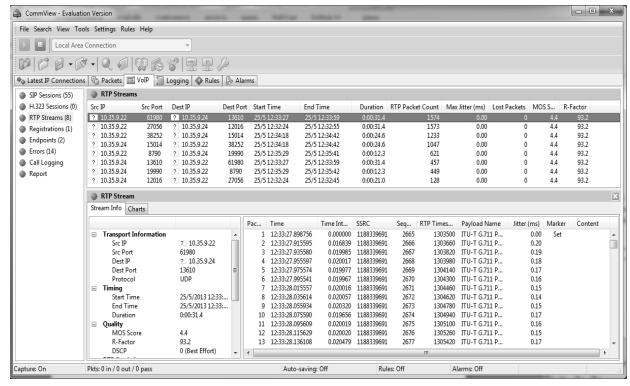

Figure 11 Commview Interface

Table 2 Voice Quality according to E-Model

ช่วงเวลา	จำนวนครั้ง	ค่าเฉลี่ย R-Factor
15.00-16.00 น. (Peak Time)	30	92.75±0.92
6.00-7.00 น. (off peak time)	30	93.20±1.08

จาก Table 2 คือผลเฉลี่ย R-Factor ที่ได้จากการวัดคุณภาพเสียงระบบโทรศัพท์ผ่านอินเทอร์เน็ตของมหาวิทยาลัยราชภัฏร้อยเอ็ด เมื่อพิจารณาในแต่ละช่วงเวลา ได้แก่ ช่วงเวลา 15.00-16.00 น. (Peak Time) ได้ค่าเฉลี่ย R-Factor = 92.75±0.92 และช่วงเวลา 6.00-7.00 น. (off peak time) ได้ค่าเฉลี่ย R-Factor =93.2±1.08 ซึ่งมีค่าเฉลี่ยคุณภาพเสียงดีกว่า ช่วง Peak Time เล็กน้อย แต่ผลโดยรวมของทั้ง 2 ช่วงเวลาอยู่ในเกณฑ์เสียงที่มีคุณภาพและอยู่ในเกณฑ์ที่สามารถยอมรับได้คือ R-Factor มีค่ามากกว่า 70 ซึ่งเป็นไปตามมาตรฐานที่ กสทช. ใช้ในการวัดคุณภาพ Voice over Internet Protocol หรือ Internet Telephony ที่ยอมรับได้

วิจารณ์และสรุปผล

จากที่ได้ทำการประเมินปัญหาด้านความมั่นคงและคุณภาพเสียงระบบโทรศัพท์ผ่านอินเทอร์เน็ต ของมหาวิทยาลัยราชภัฏร้อยเอ็ด ผลพบว่าวิธีจู่โจมสำหรับการประเมินความมั่นคง ทั้ง 3 วิธี คือ 1) การจู่โจมด้วย MITM

Attack เพื่อดักจับรหัสผ่านและเสียงการสนทนา 2) การจู่โจมด้วย SIP Flooding Attack เพื่อให้ Server ล่มไม่สามารถให้บริการได้ 3) การจู่โจมด้วย Cancel/Bye Attack เพื่อตัดสายที่กำลังสนทนา ทั้งหมดสามารถจู่ระบบโทรศัพท์ผ่านอินเทอร์เน็ตของมหาวิทยาลัยราชภัฏร้อยเอ็ดได้

จากผลการจู่โจมทำให้เห็นว่าระบบโทรศัพท์ผ่านเครือข่ายอินเทอร์เน็ต ของมหาวิทยาลัยราชภัฏร้อยเอ็ด ไม่มีความมั่นคงที่ดีและวิธีที่นำมาทดลองจู่โจมล้วนแต่เป็นวิธีที่ทำได้ง่ายโดยไม่จำเป็นต้องเป็นมืออาชีพหรือมีความรู้ในเรื่องเทคนิคมากนัก ซึ่งนั้นถือว่าเป็นสิ่งที่ร้ายแรงต่อระบบโทรศัพท์ผ่านเครือข่ายอินเทอร์เน็ตเป็นอย่างมาก เพราะระบบโทรศัพท์ผ่านเครือข่ายอินเทอร์เน็ตเป็นระบบที่มีการใช้งานจริงภายในของมหาวิทยาลัยและมีผู้ใช้งานทั้งผู้บริหาร อาจารย์และบุคลากรภายในมหาวิทยาลัย ซึ่งอาจจะมีผู้ไม่หวังดีคอยอาศัยช่องโหว่เหล่านี้ในสร้างความเดือนร้อนให้กับผู้ที่ใช้งานระบบ

ส่วนการวัดคุณภาพเสียงของระบบโทรศัพท์ผ่านเครือข่ายอินเทอร์เน็ตทั้งในช่วงที่มีการจราจรเครือข่ายที่หนาแน่นและเบาบาง ต่างอยู่ในเกณฑ์เสียงที่มีคุณภาพคือ R-Factor มีความมากกว่า 70 ซึ่งไม่มีปัญหาทางด้านคุณภาพเสียงที่ให้บริการ แต่ในด้านความมั่นคงต้องมีการปรับปรุง

ข้อเสนอแนะ

จากผลการวิจัยแสดงให้เห็นว่าระบบโทรศัพท์ผ่านอินเตอร์เน็ตที่มหาวิทยาลัยราชภัฏร้อยเอ็ดใช้อยู่นั้นไม่มีความมั่นคงที่ดีพอ ซึ่งอาจจะส่งเสียได้ในภายหลัง งานวิจัยมีแนวคิดที่จะทำการปรับปรุงระบบโทรศัพท์ผ่านอินเตอร์เน็ตที่มหาวิทยาลัยราชภัฏร้อยเอ็ดให้มีความมั่นคงที่ดีขึ้น โดยจะมีการทดลองปรับเปลี่ยน IP-PBX Server จาก Elastix มาเป็นการใช้ ISANBox แทน เนื่องจากงานวิจัยของ สมนึก พ่วงพรพิทักษ์ และปิยวัจน์ ค้าสบาย [7] ได้ทำการวิจัยแล้วว่า ISANBox เป็นชุดซอฟต์แวร์วีโอไอพีแบบโอเพนซอร์สที่มีความมั่นคงสูงสุดเมื่อเทียบกับชุดซอฟต์แวร์วีโอไอพีแบบโอเพนซอร์สตัวอื่นๆ ที่เป็นที่นิยม และทำการประเมินความมั่นคงและคุณภาพเสียงของ ISANBox บนระบบการใช้งานจริงอีกครั้ง ซึ่งแนวคิดเหล่านี้จะเป็นแนวทางสำหรับการทำวิจัยต่อไปในอนาคต

เอกสารอ้างอิง

1. Asterisk. [online]. 2010 [cited 8 August 2011]; http://www.asterisk.org.
2. คธาวุฒิ จันบัวลา และสมนึก พ่วงพรพิทักษ์. การประเมินปัญหาด้านความมั่นคงของชุดซอฟต์แวร์โอเพนซอร์สสำหรับโทรศัพท์ผ่านเครือข่ายอินเทอร์เน็ต. Proceedings of National Conference on Computer Information Technologies (CIT); 13 กุมภาพันธ์ 2555; เชียงใหม่.
3. ปิยวัจน์ ค้าสบาย และสมนึก พ่วงพรพิทักษ์. การประเมินปัญหาด้านความมั่นคงของซอฟต์แวร์เสรีสำหรับโทรศัพท์ผ่านเครือข่ายไอพี. Proceedings of National Conference on Computer Information Technologies (CIT); 13-15 มกราคม 2553; จันทบุรี. หน้า 33-38
4. Rosenberg J. et al. SIP: Session Initiation Protocol, IETF RFC3261, June 2002
5. Schulzrinne H. et al. RTP: a Transport Protocol for Real-time Application, IETF RFC 3550, July 2003.
6. Elastix. [online]. 2011 [cited 18 June 2011]; http://www.elastix.org.
7. สมนึก พ่วงพรพิทักษ์ และปิยวัจน์ ค้าสบาย. ISANBox. [ออนไลน์]. 23 มีนาคม 2554; http://www.isan.msu.ac.th/isan/ISANBox.
8. Kasabai P, Puangpronpitag S, Chanbuala K, Wongsakul P. ISANBox. [online]. 23 May 2011 [cited 19 November 2011]; http://www.isan.msu.ac.th/isan/ISANBox.php.
9. Salsano S, Veltri L, Papalilo D. SIP security issues: the SIP authentication procedure and its processing, IEEE Network 2002; 16[6]: pp. 38-44.
10. Sawda S, Urien P. SIP Security Attacks and Solutions: A state-of-the-art review. In Proceedings of ICTTA '06; 24-28 April 2006; Damascus, Syria. pp. 3187-3191.
11. Sisalem D, Kuthan J, Ehlert S. Denial of Service Attacks Targeting a SIP VoIP Infrastructure: Attack Scenarios and Prevention Mechanisms. Network, IEEE 2006; 20[5]: pp. 26-31.
12. The E-model: a computational model for use in transmission planning. ITU-T, Recommendation G.107, June 1998.
13. Methods for subjective determination of transmission quality. ITU-T, Recommendation P.800, June 1996.