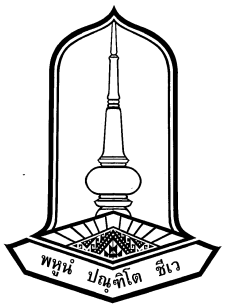


การประเมินและปรับปรุงระบบโทรศัพท์ผ่านอินเทอร์เน็ต ของมหาวิทยาลัยราชภัฏร้อยเอ็ด

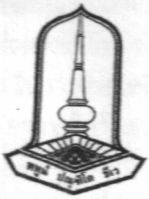
สำเริง คำมีวงษ์

เสนอต่อมหาวิทยาลัยมหาสารคาม เพื่อเป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
ปริญญาวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ
สิงหาคม 2558

การประเมินและปรับปรุงระบบโทรศัพท์ผ่านอินเทอร์เน็ต ของมหาวิทยาลัยราชภัฏร้อยเอ็ด

สำเริง คำมีวงษ์

เสนอต่อมหาวิทยาลัยมหาสารคาม เพื่อเป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
ปริญญาวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ
สิงหาคม 2558



คณะกรรมการสอบการศึกษาค้นคว้าอิสระได้พิจารณาการศึกษาค้นคว้าอิสระของ นายสำเริง คำมีวงษ์ แล้วเห็นสมควรรับเป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิตสาขาวิชาเทคโนโลยีสารสนเทศของมหาวิทยาลัยมหาสารคาม

คณะกรรมการสอบการศึกษาค้นคว้าอิสระ

.....	ประธานกรรมการ
(อาจารย์ ดร.รพีพร ช่ำชอง)	(อาจารย์บัณฑิตศึกษาประจำคณะ)
.....	กรรมการ
(อาจารย์ ดร.สมนึก พ่วงพรพิทักษ์)	(อาจารย์ที่ปรึกษาการศึกษาค้นคว้าอิสระ)
.....	กรรมการ
(ผศ.ดร.จิรัฏฐา ภูบุญอบ)	(กรรมการบัณฑิตศึกษาประจำคณะ)

มหาวิทยาลัยอนุมัติให้รับการศึกษาค้นคว้าอิสระฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิตสาขาวิชาเทคโนโลยีสารสนเทศของมหาวิทยาลัยมหาสารคาม

.....	.....
(ผศ.ดร.สุจิน บุตรดีสุวรรณ)	(ศ.ดร.ประดิษฐ์ เทอดทูล)
คณบดีคณะวิทยาการสารสนเทศ	คณบดีบัณฑิตวิทยาลัย
	วันที่ 9 เดือน ส.ค. พ.ศ. 2558

กิตติกรรมประกาศ

การศึกษาค้นคว้าอิสระฉบับนี้สำเร็จสมบูรณ์ได้ด้วยความกรุณาและความช่วยเหลืออย่างสูงยิ่งจากอาจารย์ที่ปรึกษา อาจารย์ ดร.สมนึก พ่วงพรพิทักษ์ ที่เป็นผู้ผลักดันให้การศึกษาค้นคว้าอิสระนี้จนเสร็จสมบูรณ์ และขอบคุณ คธาวุฒิ จันบัวลา ในการช่วยเหลือการใช้งานโปรแกรม

ขอขอบพระคุณ มหาวิทยาลัยราชภัฏร้อยเอ็ด ที่เอื้อเฟื้ออุปกรณ์และสถานที่สำหรับทำการศึกษาค้นคว้าอิสระจนสำเร็จด้วยดี

ขอขอบพระคุณบิดามารดาและญาติมิตรที่ช่วยเหลือและค่อยให้กำลังใจจนทำการศึกษาค้นคว้าอิสระสำเร็จลุล่วงด้วยดี

สำเริง คำมีวงษ์

ชื่อเรื่อง การประเมินและปรับปรุงระบบโทรศัพท์ผ่านอินเทอร์เน็ต ของมหาวิทยาลัยราชภัฏร้อยเอ็ด
ผู้วิจัย นายสำเริง คำมีวงษ์
ปริญญา วิทยาศาสตรมหาบัณฑิต **สาขาวิชา** เทคโนโลยีสารสนเทศ
กรรมการควบคุม อาจารย์ ดร.สมนึก พ่วงพรพิทักษ์
มหาวิทยาลัย มหาวิทยาลัยมหาสารคาม **ปีที่พิมพ์** 2558

บทคัดย่อ

มหาวิทยาลัยราชภัฏร้อยเอ็ดมหาวิทยาลัย (RERU) ได้มีการใช้งานระบบ Voice over IP (VoIP) ที่ใช้ชุดซอฟต์แวร์ Elastix โดยทำการติดตั้งใช้งานตั้งแต่ ปีค.ศ. 2011 แต่ยังไม่มีการประเมินผลคุณภาพเสียงและความมั่นคงของระบบดังกล่าว ดังนั้นในการศึกษาค้นคว้าอิสระนี้นี้จึงดำเนินการประเมินประสิทธิภาพด้านความมั่นคงและประเมินคุณภาพเสียงบนระบบ VoIP ที่ใช้อยู่จริงของ RERU สำหรับการประเมินประสิทธิภาพด้านความมั่นคง ได้ทดลองโดยใช้การจู่โจม 3 เทคนิค คือ 1) MITM Attack เพื่อดักจับรหัสผ่านและเสียงการสนทนา 2) SIP Flooding Attack เพื่อให้ Server ล่ม ไม่สามารถให้บริการได้ และ 3) Cancel/Bye Attack เพื่อตัดสายที่กำลังสนทนา ซึ่งเป็นเทคนิคการจู่โจมที่ง่ายแต่ส่งผลเสียร้ายแรงต่อระบบ สำหรับเครื่องมือจู่โจมที่ใช้ ได้แก่ Backtrack, Cain & Abel และ Wireshark สำหรับการประเมินคุณภาพเสียง ได้ใช้การวัดค่า R-factor และ MOS ตามมาตรฐาน ITU.T โดยใช้โปรแกรม Commview เป็นเครื่องมือ ผลที่ได้แสดงให้เห็นว่า VoIP ของ RERU มีคุณภาพของเสียงที่ดีผ่านตามมาตรฐาน แต่ก็มีปัญหาใหญ่ที่มีปัญหาด้านความปลอดภัย การศึกษาค้นคว้าอิสระนี้ยังมีการปรับปรุงคุณภาพระบบVoIP RERU โดยใช้ ISANBox รุ่นที่3.0 เป็น IP-PBX Server และมีการทดลองในระบบจริงที่ปรับปรุง ผลการทดลองแสดงให้เห็นว่าสามารถเพิ่มความมั่นคงได้ และพบว่าความมั่นคงที่ได้มามีผลต่อคุณภาพที่ลดลงเล็กน้อย แต่ไม่ก่อให้เกิดปัญหาด้านคุณภาพจากการวัดด้วยค่า MOS

คำสำคัญ: ความมั่นคงระบบโทรศัพท์ผ่านอินเทอร์เน็ต, คุณภาพเสียงของระบบโทรศัพท์ผ่านอินเทอร์เน็ต, ระบบโทรศัพท์ผ่านอินเทอร์เน็ตของมหาวิทยาลัยราชภัฏร้อยเอ็ด

TITLE Evaluation and Enhancement of Rajabhat Roi Et University's VoIP System
AUTHOR Mr. Sumreng Khummeewong
DEGREE Master of Science Program in Information Technology
ADVISORS Somnuk Puangpronpitag, Ph.D.
UNIVERSITY Mahasarakham University **YEAR** 2015

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 Independent Study, we run the evaluation of both security and voice quality issues on the real VoIP of RERU. For the security evaluation, three attacking techniques, namely voice sniffing by MITM, IP-PBX Denial of Service (DoS) by SIP flooding, cutting conversation lines by Cancel/Bye attacks, are chosen as the attacking techniques due to their simplicity and bad effects. The attacking tools are Backtrack, Cain & Abel and Wireshark. For the voice quality evaluation, R-factor and Mean Opinion Score (MOS) are deployed as the metrics corresponding to the ITU-T standard. Commview is the tool to capture the voice quality. The results have shown that the VoIP of RERU provides a very good quality of voice (corresponding to the standard). However, it has a big problem with the security issues. This independent study has then enhanced the security of RERU VoIP system by using ISANBox version 3.0. The experiments on the improved system have been done. The experimental results have demonstrated the improvement of security. We have also found that the security come with some minor quality overhead. Yet, it has not caused the quality problem according to MOS.

Key Words : VoIP Security, VoIP Voice Quality, Voice over IP of Rajabhat

สารบัญ

หน้า

หน้า

หน้า

สารบัญตาราง

หน้า

สารบัญรูป

หน้า

หน้า

บทที่ 1

บทนำ

1.1 หลักการและเหตุผล

ปัจจุบันการติดต่อสื่อสารถือว่ามีความจำเป็นในชีวิตประจำวัน ซึ่งมีความรวดเร็วและมีประสิทธิภาพมากขึ้น ระบบโทรศัพท์อินเทอร์เน็ต เป็นการส่งผ่านข้อมูลเสียงผ่านทางระบบเครือข่ายข้อมูล หรือผ่านทางอินเทอร์เน็ต ซึ่งระบบโทรศัพท์ผ่านอินเทอร์เน็ต กำลังเป็นที่นิยมมาก เพราะสามารถพัฒนาและประยุกต์ใช้งานใหม่ๆได้ ช่วยประหยัดค่าใช้จ่ายในการติดต่อสื่อสารภายในองค์กร รวมถึงการเพิ่มประสิทธิภาพการทำงานขององค์กร

มหาวิทยาลัยราชภัฏร้อยเอ็ด ก่อตั้งขึ้นมาตั้งแต่ปี พ.ศ. 2540 ซึ่งในการใช้บริการโทรศัพท์ภายในมหาวิทยาลัยเป็นแบบตู้ ชุมสายโทรศัพท์ มาเป็นเวลานานในการเพิ่มเติมจำนวนคู่สายโทรศัพท์ภายในนั้นมีความยุ่งยากในการวางระบบชุมสายโทรศัพท์ เนื่องจากการเพิ่มจำนวนคู่สายโทรศัพท์ภายในอาคารที่สร้างขึ้นใหม่ ซึ่งอาจจะมีปัญหาในการเชื่อมต่อกันระหว่างตู้ชุมสายเก่ากับตู้ชุมสายใหม่

ดังนั้น ปี พ.ศ. 2554 ศูนย์คอมพิวเตอร์ จึงได้ทำการติดตั้งระบบโทรศัพท์ผ่านเครือข่ายอินเทอร์เน็ต ภายในมหาวิทยาลัยราชภัฏร้อยเอ็ด ขึ้นมาใช้งานเพื่อลดความยุ่งยากและต้นทุน และการใช้งานได้อย่างคุ้มค่าได้ผลการดำเนินงานที่ดี โดยทั้งนี้ระบบโทรศัพท์ผ่านเครือข่ายอินเทอร์เน็ตในมหาวิทยาลัยราชภัฏร้อยเอ็ดได้มีการใช้งานมาเป็นเวลา 4 ปี แต่ยังไม่มีการศึกษาปัญหาทางด้านความมั่นคงและคุณภาพเสียงของระบบที่ให้บริการ ซึ่งจากศึกษางานวิจัยค้นคว้า [1-3] พบว่าปัญหาภัยคุกคามต่อระบบโทรศัพท์ผ่านอินเทอร์เน็ตนั้น มีอยู่หลากหลายและอาจจะส่งผลต่อระบบโทรศัพท์ผ่านอินเทอร์เน็ตภายในมหาวิยาลัยราชภัฏร้อยเอ็ดได้ ซึ่งการจู่โจมดังกล่าวได้แก่ การดักฟังเสียงที่สนทนา การตัดสายที่สนทนาด้วย Cancel/bye attacks การจู่โจมเครื่องให้บริการด้วย SIP flooding

ดังนั้นการศึกษาค้นคว้าอิสระ จึงได้เสนอการประเมินระบบโทรศัพท์ผ่านอินเทอร์เน็ตมหาวิทยาลัยราชภัฏร้อยเอ็ด โดยจะทำการประเมิน 2 ประเด็น คือ 1) ปัญหาด้านความมั่นคงในการจู่โจมในรูปแบบต่างๆ 2) คุณภาพเสียงของระบบที่ให้บริการปัจจุบัน ตามเกณฑ์การวัดเสียงที่ใช้อยู่ในสากล จากนั้นจะทำการสรุปปัญหาที่พบ และเสนอแนวทางในการปรับปรุงเพื่อที่จะเพิ่มประสิทธิภาพให้ระบบโทรศัพท์ผ่านอินเทอร์เน็ตมหาวิทยาลัยราชภัฏร้อยเอ็ดทั้งในด้านความมั่นคงและคุณภาพเสียงที่ให้บริการ

1.2 วัตถุประสงค์ของการศึกษาค้นคว้าอิสระ

1) วิเคราะห์และประเมินด้านความมั่นคงและคุณภาพเสียงระบบโทรศัพท์ผ่านอินเทอร์เน็ตในมหาวิทยาลัยราชภัฏร้อยเอ็ด

2) เสนอวิธีการปรับปรุงด้านความมั่นคงพร้อมประเมินคุณภาพหลังการปรับปรุงระบบโทรศัพท์ผ่านอินเทอร์เน็ต

1.3 ความสำคัญของการศึกษาค้นคว้าอิสระ

การศึกษาค้นคว้าอิสระในครั้งนี้เป็นการศึกษาใช้งานระบบโทรศัพท์ผ่านอินเทอร์เน็ต ภายในมหาวิทยาลัยราชภัฏร้อยเอ็ด ซึ่งมีความสำคัญดังนี้

1) งานวิจัยได้ทำประโยชน์ต่อกรณีศึกษา

มหาวิทยาลัยราชภัฏร้อยเอ็ดได้ทราบถึงผลการประเมินความมั่นคงของระบบโทรศัพท์ผ่านอินเทอร์เน็ตที่จะช่วยป้องกันจากการจู่โจมต่างๆ ทางด้านความมั่นคงของระบบ พร้อมทั้งคุณภาพเสียงตามมาตรฐาน ได้ข้อเสนอแนะในการปรับปรุงความมั่นคง ของระบบโทรศัพท์ผ่านอินเทอร์เน็ต พร้อมทั้งตระหนักถึงคุณภาพเสียงอยู่ในระดับที่ยอมรับได้

2) องค์ความรู้ทางวิชาการ

ได้แนวคิดในการประเมินและปรับปรุงความมั่นคงและคุณภาพเสียง จากกรณีศึกษา ซึ่งอาจจะเป็นองค์ความรู้สามารถนำไปใช้ในองค์กรอื่นๆ หรือเป็นข้อสังเกตเพื่อให้เกิดประสิทธิภาพมากขึ้น

1.4 ขอบเขตของการศึกษาค้นคว้าอิสระ

1) กรณีศึกษาคือระบบ VoIP ที่ใช้ในมหาวิทยาลัยราชภัฏร้อยเอ็ด

2) เทคนิคการจู่โจมเพื่อใช้สำหรับประเมินปัญหาด้านความมั่นคง ได้แก่

(1) Man-in-the-Middle (MITM) Attack เพื่อดักฟังการสนทนา

(2) SIP Flooding Attack เพื่อให้ปฏิเสธการบริการ

(3) Cancel/Bye Attack เพื่อทำให้การสื่อสารล้มเหลว

เหตุผลที่เลือกใช้ 3 เทคนิค สำหรับการประเมินปัญหาด้านความมั่นคงก็เพราะเป็นเทคนิคที่ทำการจู่โจมบนโพรโทคอลหลักของระบบ VoIP คือ โพรโทคอล SIP และ โพรโทคอล RTP ที่ครอบคลุมและอีกทั้งยังสามารถทำการจู่โจมได้ง่ายไม่ซับซ้อน แฮกเกอร์มือสมัครเล่น (Script - Kiddies) ทั่วไปก็สามารถศึกษาและทำการจู่โจมได้อย่างรวดเร็ว

3) การทดสอบประสิทธิภาพและวัดคุณภาพเสียงของชุดซอฟต์แวร์ VoIP เพื่อทำการเปรียบเทียบประสิทธิภาพการป้องกันปัญหาหลังการพัฒนา และเพื่อเปรียบเทียบคุณภาพเสียงของชุดซอฟต์แวร์ VoIP ที่มีความมั่นคงเพิ่มขึ้นจะแตกต่างกันอย่างไรกับตัวที่ไม่มีการมีการป้องกันด้านความ

มั่นคง ซึ่งทำโดยการใช้การวัดคุณภาพ VoIP ด้วยค่า E-Model บนเครือข่ายจริงของมหาวิทยาลัยราชภัฏร้อยเอ็ด

1.5 นิยามศัพท์เฉพาะ

1) โทรศัพท์ผ่านเครือข่ายอินเทอร์เน็ต (Voice over Internet Protocol : VoIP) เป็นระบบโทรศัพท์ผ่านเครือข่ายไอพีโดยใช้ประสิทธิภาพในการติดต่อสื่อสารผ่านเครือข่ายอินเทอร์เน็ตกับฟังก์ชันของ PSTN (Public Switched Telephone Network) ซึ่งจะเป็นการส่งข้อมูล ผ่านไปบนโครงข่ายของระบบอินเทอร์เน็ตแบบเรียลไทม์

2) ความมั่นคงของระบบโทรศัพท์ผ่านอินเทอร์เน็ต (Voice over Internet Protocol : VoIP) คือ ประสิทธิภาพทางด้านเทคนิคของระบบโทรศัพท์เครือข่ายอินเทอร์เน็ตและการป้องกันภัยคุกคามจากการโจมตีโดยบุคคลผู้ไม่หวังดีที่อาศัยช่องโหว่ของระบบ

3) การประเมินความมั่นคง ในงานศึกษาค้นคว้าอิสระนี้ คือ การประเมินประสิทธิภาพด้านความมั่นคงของระบบโทรศัพท์ผ่านอินเทอร์เน็ต ทดสอบในการจู่โจม

4) การปรับปรุงความมั่นคง ในงานศึกษาค้นคว้าอิสระนี้ คือ การพัฒนาแก้ไขติดตั้งคอนฟิกระบบโทรศัพท์ผ่านอินเทอร์เน็ต ที่มีอยู่ให้มีความสามารถต่อต้านการจู่โจมจากบุคคลที่ไม่หวังดี

5) คุณภาพของระบบโทรศัพท์ผ่านอินเทอร์เน็ต คือ คุณภาพของเสียงโทรศัพท์ผ่านเครือข่ายโดยมีมาตรฐานการวัดอยู่หลายแบบ เช่น MOS, E-Model เป็นต้น

บทที่ 2

ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

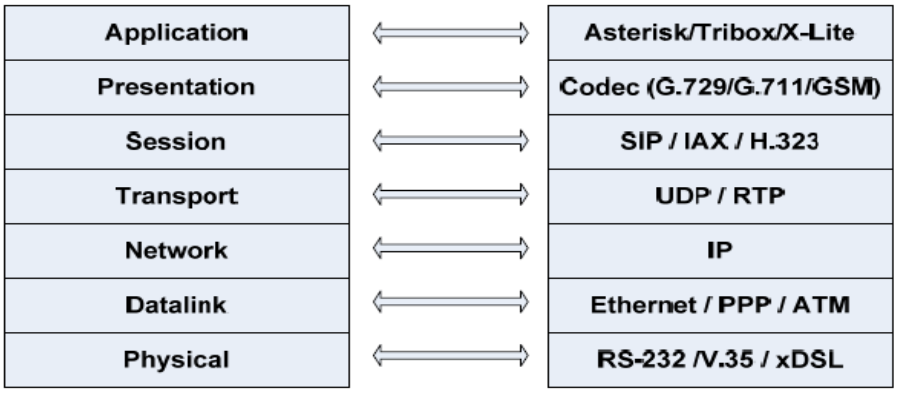
ในการศึกษาระบบสื่อสารแบบ VoIP ได้ทำการศึกษาทฤษฎีและงานวิจัยที่เกี่ยวข้องที่สามารถประยุกต์การใช้งานได้ โดยแบ่งเป็นหัวข้อต่างๆ ดังต่อไปนี้

2.1 ความรู้ทั่วไปเกี่ยวกับ (VoIP over Internet Protocol : VOIP)

VoIP (VoIP over Internet Protocol) เป็นชุดซอฟต์แวร์ที่มีหลายแบบสำหรับอำนวยความสะดวกในการสื่อสารผ่านอินเทอร์เน็ต เป็นระบบที่แปลงสัญญาเสียงในรูปของสัญญาณอนาล็อก (Analog) เป็นสัญญาณดิจิทัล (Digital) หรือกลุ่มข้อมูล (Packet) แล้วส่งผ่านไปทางอินเทอร์เน็ตและจะมี IP-PBX Server ทำหน้าที่ควบคุมการรับหรือส่งข้อมูล แต่เดิมการส่งสัญญาเสียงกับข้อมูล จะถูกส่งผ่านโครงข่ายที่แยกจากกัน แต่ปัจจุบัน เทคโนโลยี VoIP ช่วยให้เครือข่ายอินเทอร์เน็ตสามารถรวมบริการ ทั้งสองอย่างไว้ในเครือข่ายเดียวกันได้ โดยเสียงจะถูกแปลงเป็นข้อมูลก่อนส่งแล้วส่งผ่านโดยใช้โพรโทคอลไอพี (Internet Protocol: IP) ซึ่งกำลังเป็นสิ่งที่ได้รับความสนใจ เป็นอย่างมาก ทั้งในส่วนขององค์กร ธุรกิจ และผู้ให้บริการโครงข่ายหลายราย

การทำงานของ VOIP

เทคโนโลยีการทำงาน VoIP มีการทำงานในรูปแบบของโพรโทคอล ในการส่งสัญญาณเสียง โดยสัญญาณเสียงที่ส่งไปส่วนใหญ่ใช้ส่งแบบ UDP (User Datagram Protocol) มากกว่าแบบ TCP (Transmission Control Protocol) [4] การส่งข้อมูลแบบ UDP นั้นจะมีการส่งข้อมูลได้เร็วกว่าจึงมีความเหมาะสมที่จะนำมาเพื่อใช้ในการส่งข้อมูลเสียงบนเครือข่ายอินเทอร์เน็ต การส่งข้อมูลเสียงนั้นจะต้องอาศัยโพรโทคอลหลัก ที่ใช้ในการส่งสัญญาณระหว่างต้นทางและปลายทาง ซึ่งเป็นโพรโทคอล SIP(Session Initiation Protocol) [5,6] จึงทำให้ต้นทางและปลายทางสามารถสื่อสารกันได้ โดยปกติ SIP Protocol จะมีการใช้พอร์ตสื่อสารแบบ UDP ที่ 5060 ดังรูปที่ 2.1



รูปที่ 2.1 การเปรียบเทียบ OSI Model กับการทำงานของการสื่อสารเทคโนโลยี VoIP
ที่มา : [1]

จาก

รูปที่ 2.1 เป็นการเปรียบเทียบการทำงาน OSI Model เพื่อให้เข้าใจว่าเทคโนโลยี VoIP มีความสอดคล้องกันกับ OSI Model

2.2 โพรโทคอล ที่เกี่ยวข้องกับ VoIP

การสื่อสารด้วย VoIP ประกอบด้วยการสื่อสาร 2 ประเภท คือ การรับส่งข้อมูลเสียงและการรับส่งสัญญาณควบคุมการสื่อสาร ซึ่งสัญญาณควบคุมการสื่อสารนั้นมีหลายโพรโทคอล เช่น SIP, SCCP (Skinny Client Control Protocol) เป็นต้น ส่วนเป็นที่นิยมกันแพร่หลายคือ SIP และ SCCP

2.2.1 Session Initiation Protocol (SIP)

SIP เป็นโพรโทคอลที่ใช้งานสำหรับการสื่อสาร VoIP [5,6] ในการส่งข้อมูลเสียงหรือวีดีโอบนเครือข่าย IP ได้รับการพัฒนาโดย IETF สามารถปรับใช้และนำไปพัฒนาง่าย โดยมีความสามารถในการสร้าง (create), ปรับ (modify) และ ยกเลิก (terminate) การติดต่อสื่อสารระหว่างโหนดที่เป็นแบบหนึ่งต่อหนึ่ง (unicast) หรือแบบกลุ่ม (multicast) ได้ ซึ่ง SIP สามารถปรับเปลี่ยนที่อยู่ address, หมายเลขพอร์ต, เพิ่มสายผู้สนทนา และสามารถเพิ่มหรือลดการส่งข้อมูลมีเดีย media stream บางประเภทได้ ตัวอย่างของโปรแกรมประยุกต์ (application)ที่อาศัยSIPในการเชื่อมต่อเช่น การประชุมด้วยวิดีโอ (video conferencing) การกระจายข้อมูลภาพและเสียง (streaming multimedia distribution) การส่งข้อความด่วน (instant messaging)

SIP Protocol การพัฒนา VoIP จะมีการใช้งานพอร์ต TCP หรือ UDP ที่ 5060 ในการส่งสัญญาณการลงทะเบียนและมีการส่งสัญญาณเสียงโดยพอร์ต UDP ระหว่าง 10000 ถึง 20000

คุณสมบัติของ SIP

1. เป็นโพรโทคอลที่ไม่ซับซ้อน ซึ่งมีประเภทข้อความ 6 ประเภท
2. โพรโทคอลของ SIP สามารถใช้งานได้ทั้ง TCP และ UDP ส่วนมากจะใช้ UDP โดยจะใช้พอร์ต 5080

3. โพรโทคอลของ SIP ใช้ในการส่งข้อความในรูปแบบแอสกี (ASCII) ลักษณะเป็นข้อความ ผู้ใช้ทั่วไปสามารถอ่านข้อความได้

4. โพรโทคอลของ SIP เป็นโพรโทคอลที่ไม่มีการเก็บสถานการณ์เชื่อมต่อ ซึ่งจะไม่มีการบันทึกการแลกเปลี่ยนข้อมูลต่างๆ ซึ่งจะทำให้การแลกเปลี่ยนข้อมูลได้มาก รองรับจำนวนลูกข่ายได้มาก

การทำงานของโพรโทคอล SIP

การทำงานของโพรโทคอล SIP แบ่งได้ออกเป็น 5 ส่วนสำหรับใช้จัดตั้ง และสิ้นสุดการสื่อสารมัลติมีเดีย ดังนี้

(1) User location: กำหนดตำแหน่งที่ตั้งของระบบสำหรับการสื่อสาร

(2) User availability: กำหนดความต้องการสำหรับการโทรเพื่อสร้างเส้นทางในการสื่อสาร

(3) User capabilities: กำหนดสื่อ และพารามิเตอร์อื่นๆ ของสื่อที่จะใช้สื่อสาร

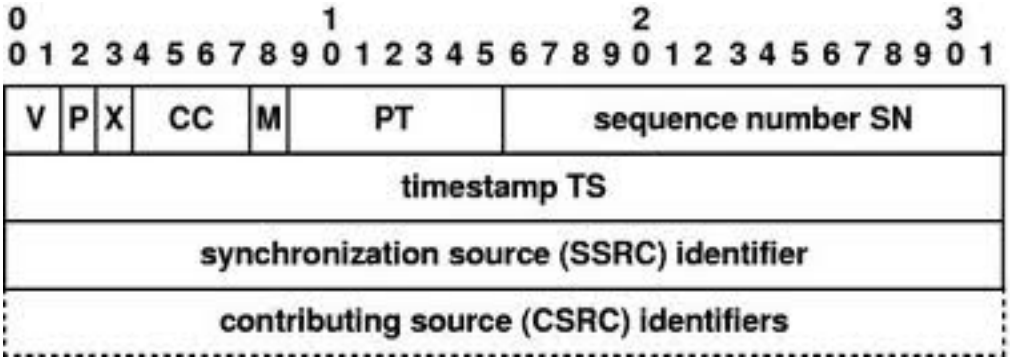
(4) Session setup: "ringing" จัดตั้งพารามิเตอร์ของช่วงเวลาสื่อสาร (Session) ในระหว่างการโทร และในขณะการโทร

(5) Session management: การโอน การปรับเปลี่ยนพารามิเตอร์ และการสิ้นสุดของ Session

2.2.2 Real Time Transport Protocol (RTP)

RTP [7] เป็นมาตรฐานการส่งข้อมูลประเภท ภาพ-เสียง (Media) ผ่านเครือข่าย IP ซึ่งถูกใช้อย่างแพร่หลายในระบบการสื่อสารและความบันเทิงที่เกี่ยวกับการถ่ายทอดผ่านสื่อ เช่น โทรศัพท์ผ่านโพรโทคอลอินเทอร์เน็ต การประชุมวิดีโอ (Video Conference) หรืออื่นๆ ซึ่งมีรูปแบบของ Header แสดงดัง

รูปที่ 2.2



รูปที่ 2.2 RTP Header
ที่มา: [1]

หมายเหตุ V=Version, P=Pending, X=Extension, CC=CSRC count, M=Maker, PT=Payload Type

(1) Version ของโพรโทคอล RTP ปัจจุบันเวอร์ชัน 2

(2) Pedding คือ ฟิลด์ที่บอกว่า Packet นั้นได้ถูกเติมด้วยข้อมูลที่เพิ่มให้พอดีกับขนาดของ Packet หรือไม่ และยังใช้กระบวนการเข้ารหัสข้อมูล (Encryption) อีกด้วย

(3) Extension คือ ฟิลด์ที่แสดงส่วนหัวของ Packet ของ RTP ว่ามีการขยายหรือไม่

(4) CSRC Count บอกจำนวนของ Contribution Source Identifier ใน Packet โดยมีค่า CSRC ได้ตั้งแต่ 0-15

(5) Marker ใช้สำหรับการระบุ Profile และ Specification ของ Packet ของโพรโทคอล RTP

(6) Payload Type เป็นชนิดของข้อมูลภายใน Payload ซึ่งก็คือชนิดของการบีบอัดข้อมูลเสียง

(7) Sequence Number ลำดับของ Packet ซึ่งทำให้ฝั่งรับได้ตรวจสอบ Packet Loss และสามารถใช้เรียงลำดับของ Packet ได้

(8) Timestamp เป็นค่าบอกเวลาที่ใช้ในการ Sample ของข้อมูล Payload ซึ่งนำไปใช้ในการคำนวณ Jitter และค่าเวลาหน่วงของการส่ง (Round Trip Time)

(9) SSRC เป็นเลขประจำ Session ซึ่งก็คือ Package ที่มาจากผู้ส่งเดียวกันและใช้ค่า SSRC เท่ากันแสดงว่าเป็น Session เดียวกัน

(10) CSRC จะถูกใช้เมื่อมีการ Mixer (ในกรณีที่ระบบเครือข่ายไม่สามารถรองรับข้อมูลที่ส่งระหว่างผู้รับและผู้ส่งโดยจะทำการเปลี่ยนรูปแบบข้อมูลใหม่ เพื่อรองรับระบบเครือข่ายที่มีทรัพยากรน้อยได้ โดยการลดขนาดคุณภาพของเสียงที่ส่งไป) ซึ่งเป็นกระบวนการที่ใช้ในการประชุมแบบหลายจุด (Multipoint Conference)

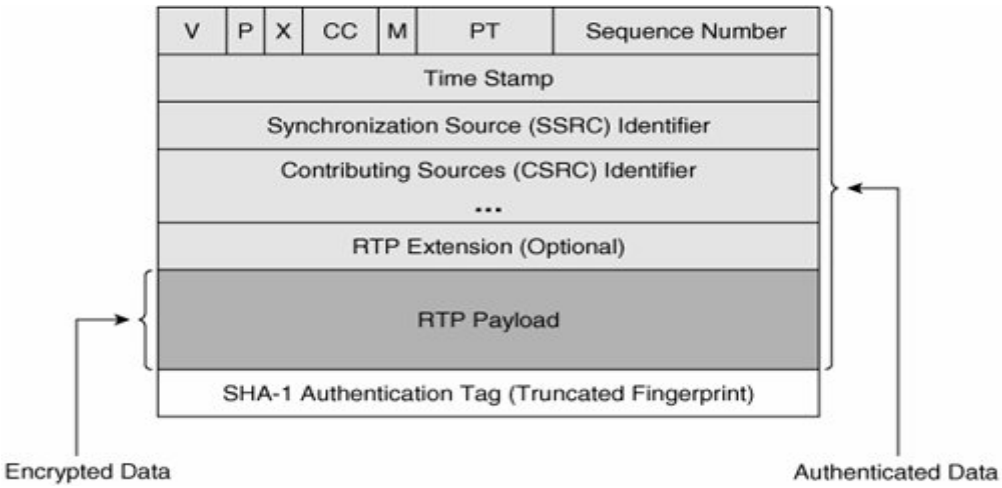
2.2.3 Session Description Protocol (SDP)

Session Description Protocol [8] เป็นโพรโทคอลที่ใช้เพื่อสร้างคำอธิบายรายละเอียดของข้อมูลสื่อสารประเภท วีดีโอหรือข้อมูลมัลติมีเดีย ซึ่งใช้สำหรับกำหนดการสื่อสาร การจัดตั้งพารามิเตอร์ที่ข้อมูลมัลติมีเดียจะใช้สื่อสาร SDP จะใช้สำหรับการเจรจาระหว่างจุดสิ้นสุดของสื่อประเภทรูปแบบและถูกออกแบบมาเพื่อขยายการสนับสนุนประเภทสื่อใหม่และการใช้งานร่วมกับโพโทคอลอย่าง Session Annoucement Protocol (SAP) ใช้สร้างเซสชันกรณีที่ส่งข้อมูลแบบมัลติแคส Real-time Streaming Protocol (RTSP) ในการควบคุมการส่งข้อมูลให้ได้ตามคุณภาพที่ต้องการ

2.3 Secure RTP (SRTP)

SRTP [9] เป็นโพรโทคอลที่ถูกพัฒนามาจาก โพรโทคอล RTP คือ Confidentiality, Message Authentication, Replay Protection รูปแบบ SRTP ซึ่งจะมีกระบวนการร้องขอรูปแบบที่จะใช้เข้า-ถอดรหัส โดยการเข้ารหัสข้อมูล ช่วยในเรื่องขอความมั่นคงปลอดภัยโดยนำมาใช้ใน VoIP ในการส่งข้อมูลมัลติมีเดีย SRTP จะใช้งานได้อย่างมีประสิทธิภาพทั้งในเครือข่ายแบบมีสายและไร้สาย SRTP เป็นโพรโทคอล ทางด้านความปลอดภัย ไม่สูญเสียความลับในการติดต่อสื่อสาร

SRTP ใช้รูปแบบการเข้ารหัส คือ Advanced Encryption Standard (AES) เป็น block cipher ที่มีขนาดความยาวของ Key คือ 128, 192 และ 256 bits ซึ่งเป็นอัลกอริธึมที่มีความแข็งแกร่งต่อการจู่โจม สามารถเข้ารหัสข้อมูลได้อย่างรวดเร็วและมีความยืดหยุ่น จะสามารถทำงานบนแพลตฟอร์มต่างๆ โดยเฉพาะอย่างยิ่ง อุปกรณ์ขนาดเล็กซึ่ง SRTP ซึ่งมีรูปแบบของ SRTP Packet ดังรูปที่ 2.3



รูปที่ 2.3 SRTP Packet
ที่มา: [1]

(1) Version (V) 2 bit รุ่นของโพรโทคอล (ปัจจุบัน 2 bit)

(2) Padding (P) 1 bit padding ของกลุ่มข้อมูล RTP

(3) Extension Header (X) 1 bit สถานะ Extension

(4) Marker (M) 1 bit ใช้บอกเหตุการณ์บางอย่าง เช่น Frame Boundaries

(5) Payload Type (PT) 7 bit รูปแบบของ RTP Payload

(6) Sequence Number 16 bit เพิ่มครั้งละ 1 ในแต่ละกลุ่มข้อมูล RTP และใช้คำนวณการสูญหายของกลุ่มข้อมูล

(7) Timestamp 32 bit เวลาที่ RTP นั้นๆ เกิด

(8) Synchronization Source Identifier (SSRC) 32 bit ใช้ระบุผู้ส่งในแต่ละ Stream

(9) Contributing Source Identifiers (CSRCs) ใช้เพื่อระบุต้นทางของ Stream เมื่อมีการกระจายการส่งไปยังหลายๆ ตำแหน่ง

(10) RTP Extension (Optional) ฟิลด์ที่แสดงส่วนหัวของ Packet ของ RTP มีการขยาย

(11) RTP Payload เนื้อข้อความ RTP

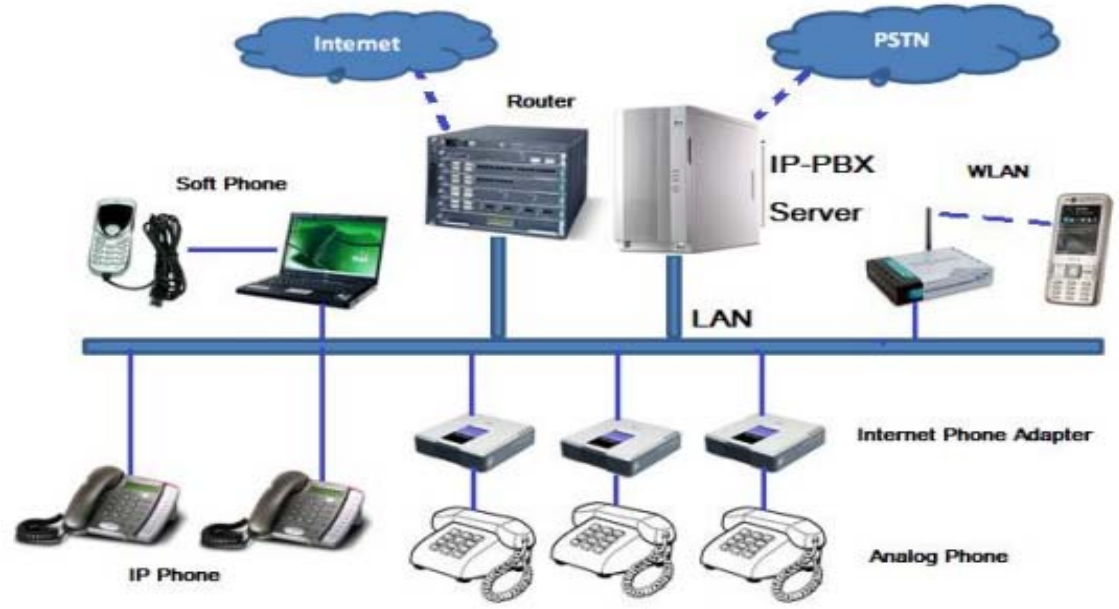
(12) Master Key Identifier (MKI) เป็นการระบุขนาด รูปแบบที่ใช้ในการจัดการกุญแจ MKI ระบุ Master key จาก Session

(13) Authentication Tag ใช้ยืนยันความถูกต้องของ RTP

2.4 ซอฟต์แวร์ตู้ชุมสายโทรศัพท์ (IP-PBX)

ตู้โทรศัพท์สาขา (IP Public Branch exchange: IP-PBX) IP-PBX [27] เป็นอุปกรณ์ที่ใช้ในการเชื่อมโยง ควบคุม เครื่องโทรศัพท์ในระบบ และทำหน้าที่หลักของตู้ชุมสายโทรศัพท์ การติดต่อควบคุมกับคู่สนทนาของคู่สายโทรศัพท์ ในการสื่อสารทางเสียงผ่านระบบเครือข่าย Intranet หรือ Internet โดยการทำงานของ IP-PBX นั้นจะทำหน้าที่เหมือน ตู้ชุมสาย PABX โดยจะทำหน้าที่เป็นศูนย์กลางในการทำงาน เช่น การ Route Call ไปยังปลายทาง หากแต่ IP-PBX นั้นจะทำงานผ่านระบบ IP หรือ ระบบ Computer Network (LAN/WAN) เป็นหลัก ฉะนั้นในการส่งเสียงไปยังปลายทางจำเป็นต้องส่งผ่านระบบ Computer Network โดยเสียงที่จะส่งจะต้องถูกแปลงไปเป็น รูปแบบ digital โดยอุปกรณ์ VoIP ที่สามารถส่งสัญญาณผ่านระบบเครือข่ายได้ก่อนที่จะถูกแปลงเป็นสัญญาณเสียงอีกครั้งที่อุปกรณ์ปลายทาง

Trunk Line [28] คือสายที่เชื่อมต่อระหว่าง ตัว PBX กับ ผู้ให้บริการโทรศัพท์พอผ่าน PBX เสร็จแล้วก็จะผ่านสายที่เรียกว่า Extension ซึ่งก็คือสายที่ต่อออกจาก PBX เข้าไปยังโทรศัพท์แต่ละบุคคล Trunk Line นั้นจะทำให้ลดค่าใช้จ่ายเพราะโดยทั่วไป บริษัทต่างๆ ก็จะใช้สาย Trunk Line แค่ 2-3 สาย หากต้องการโทรศัพท์คุยกันภายในก็ใช้ผ่าน สาย Extension ดังรูปที่ 2.4



รูปที่ 2.4 โทรศัพท์ระบบ IP-PBX
ที่มา : [10]

ประโยชน์และข้อดี

1) การทำงานของ IP-PBX นั้น ต้องทำงานบนระบบ Network จึงไม่จำเป็นต้องเดินสายโทรศัพท์เพิ่มเติม อีกทั้งยังสามารถทำการย้ายเครื่องโทรศัพท์ไปยังตำแหน่งอื่นๆ ที่อยู่บนระบบเครือข่าย Network เดิม

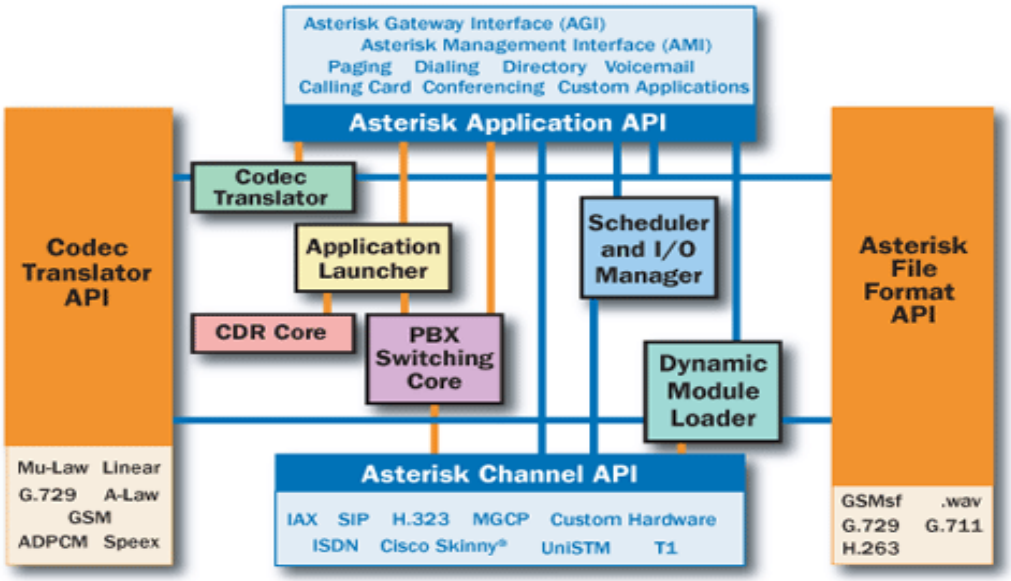
2) ได้รับประโยชน์โดยตรงจากระบบเครือข่าย คือ หากมีการเชื่อมต่อกับระบบเครือข่ายเข้าด้วยกันแล้วนั้น ไม่ว่าเครื่องโทรศัพท์จะอยู่ในที่แห่งใดๆ ในระบบ ก็เสมือนว่าอยู่ในระบบโทรศัพท์เดียวกัน การโทรศัพท์จึงเป็นไปได้โดยง่าย และไม่มีค่าใช้จ่ายในการโทรศัพท์บนระบบ IP-PBX

3) สามารถรองรับการโทรศัพท์แบบเห็นภาพ Video Call ได้ทันทีหากมีอุปกรณ์ที่รองรับในทั้งสองคู่สนทนา

4) รองรับอนาคตสามารถทำงานร่วมกันในทั้งระบบ เพื่อทำให้สามารถโทรศัพท์ไปยังระบบโทรศัพท์ภายนอกได้ในราคาที่ประหยัดกว่ามาก

2.5 Asterisk

Asterisk [1,13] เป็นฟรีซอฟต์แวร์ตู้ชุมสายโทรศัพท์ระบบ VoIP สามารถรันได้ทั้งบนระบบปฏิบัติการ Unix, Linux และAsterisk สามารถรองรับมาตรฐานโพรโทคอลสื่อสารได้หลาย โพรโทคอล ไม่ว่าจะเป็น Session Initiation Protocol (SIP), Media Gateway Control Protocol (MGCP), และSkinny Client Control Protocol (SCCP) หลักการทำงานมีส่วนการควบคุมเป็นเว็บ Web-based Control Panel ทำให้ง่ายต่อการใช้งาน ดังรูปที่ 2.5



รูปที่ 2.5 สถาปัตยกรรมของ Asterisk
ที่มา: [1]

คุณสมบัติและความสามารถของ Asterisk

Asterisk นั้นเป็น IP-PBX Server ที่มีความสามารถเทียบเท่ากับระบบโทรศัพท์ราคาแพงที่มีประสิทธิภาพสูง ซึ่ง Asterisk มีคุณสมบัติและความสามารถต่างๆ

1. Switch (PBX) ตู้ชุมสายสามารถทำหน้าเป็นอุปกรณ์สลับสายโทรศัพท์ไม่ว่าจะเป็นระบบ IP ได้เช่น (ระบบ Voicemail, Interactive Voice Recorder: IVR), รองรับการเชื่อมต่อกับระบบโทรศัพท์พื้นฐานไม่ว่าจะเป็นแบบ analog หรือ digital

2. Gateway สามารถทำหน้าเป็นอุปกรณ์ที่ใช้ในการเชื่อมต่อระหว่าระบบโทรศัพท์พื้นฐานกับระบบ VoIP

3. Feature & Media Server Asterisk คือสามารถทำเป็น ระบบตอบรับหรือระบบการประชุมทางโทรศัพท์ เพื่อให้ทำงานเข้ากับระบบโทรศัพท์ที่มีอยู่เดิม

4. Call Center รองรับการทำงานของระบบ Call-Center อย่างเต็มรูปแบบ เช่น Automatic Call Distributor (ACD), Queue, IVR, Skill-based routing

2.6 ชุดซอฟต์แวร์ VoIP

เป็นชุดซอฟต์แวร์ที่มีการรวมโปรแกรมต่างๆ ที่จำเป็น ต่อระบบ VoIP เช่น Operating System (OS), ซอฟต์แวร์ VoIP (เช่น Asterisk FreeSWITCH Kamailio), Web Server, Database และอื่นๆ

2.6.1 Elastix

Elastix [14] คือ Open Source Software ที่อยู่ภายใต้ลิขสิทธิ์แบบ GPLv2. ถูกติดตั้งอยู่บนระบบปฏิบัติการ Cent OS คือระบบที่นำเอาคุณสมบัติทางด้านเทคโนโลยีการการติดต่อสื่อสารมารวมเข้าไว้ด้วยกัน มีพื้นฐานมาจากระบบ Asterisk ซึ่งเป็นซอฟต์แวร์สำหรับทำตู้สาขา (VoIP) แต่การใช้งาน Asterisk ค่อนข้างจะไม่ค่อยสะดวกนัก เนื่องการคอนฟิกค่าต่างต้องทำผ่านทาง Text mode แต่ Elastix สามารถคอนฟิกค่าต่างๆ แบบ GUI โดยใช้ผ่านทาง Web browser ซึ่งทำให้สะดวกในการใช้งานอย่างมาก โดยที่มหาวิทยาลัยราชภัฏร้อยเอ็ด ได้ทำการติดตั้ง Elastix V 1.8 ขึ้นมาใช้งานเมื่อปี พ.ศ. 2554

2.6.2 AsteriskNow

AsteriskNow [15] เป็น Software Appliance ซึ่งเป็น Customized Linux Distribution ที่ประกอบด้วย Asterisk, AsteriskGUI และซอฟต์แวร์อื่นทั้งหมดที่จำเป็นสำหรับระบบ Asterisk ซึ่ง AsteriskNow สามารถคอนฟิกได้ง่ายด้วย graphical interface และมีความสามารถในการรองรับการใช้งานที่เป็นภาษาไทย ทั้งนี้เพื่อเป็นการสนับสนุนในเชิงพาณิชย์

2.6.3 ISANBox.A

ISANBox.A [16] เป็นชุดซอฟต์แวร์ VoIP ที่พัฒนาโดย สมนึก พ่วงพรพิทักษ์ และทีมวิจัย Information Security and Advanced Network (ISAN) คณะวิทยาการสารสนเทศ มหาวิทยาลัยมหาสารคาม ISANBox.A version ล่าสุด ขณะที่เขียนรายงานการศึกษาค้นคว้าอิสระนี้ (กรกฎาคม พ.ศ. 2557) คือ version 3 [22] ซึ่งถูกใช้ในการศึกษาค้นคว้าอิสระนี้ในการนำไปแทน Elastix เพื่อปรับปรุงความมั่นคงของระบบ VoIP ของมหาวิทยาลัยราชภัฏร้อยเอ็ด ทั้งนี้ ISANBox.A ถูกพัฒนาต่อยอดมาจาก Asterisk ซึ่งมีคุณสมบัติ ดังนี้

(1) สนับสนุนการใช้งาน TLS เพื่อเข้ารหัสสัญญาณก่อนที่จะส่งข้อมูลผ่านเครือข่าย ทำให้มีความมั่นคงทางด้านสัญญาณ (Signal)

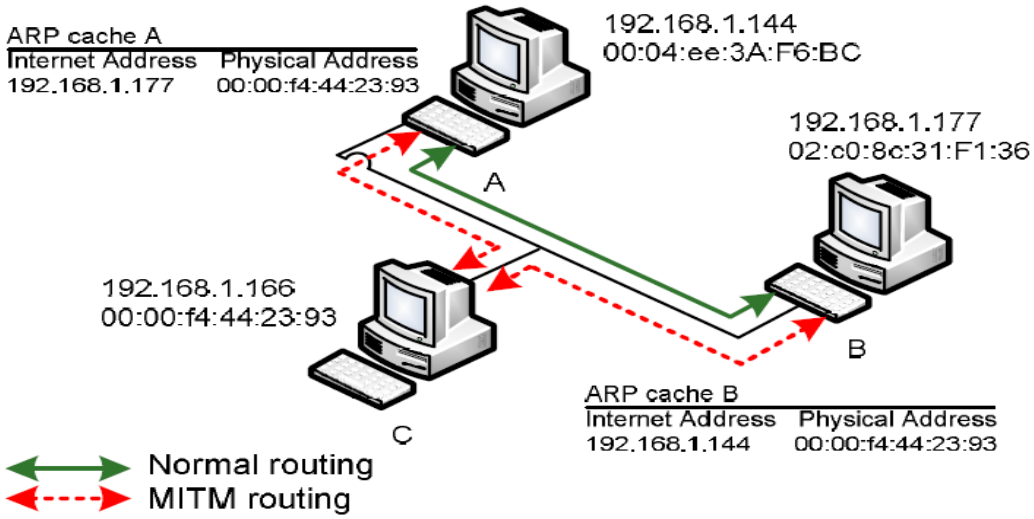
(2) สนับสนุนการใช้งาน SRTP เพื่อเข้ารหัสข้อมูลเสียงสนทนาเพื่อป้องกันการดักฟังระหว่างการสนทนา ทำให้มีความมั่นคงทางด้าน ภาพและเสียง (Media)

(3) ใช้งานได้ง่าย ISANBox.A รองรับการตั้งค่า และควบคุมสามารถทำได้ผ่านหน้าเว็บ ซึ่งทำให้ใช้งานได้ง่าย

(4) สนับสนุนการใช้งานหน้าเว็บที่เป็นภาษาไทยใช้งานได้ฟรี เนื่องจาก ISANBox.A ถูกสร้างจาก Asterisk ซึ่งเป็นซอฟต์แวร์โอเพนซอร์ซที่ไม่เสียค่าลิขสิทธิ์ ดังนั้น ISANBox.A จึงเป็นซอฟต์แวร์โอเพนซอร์ซ โดยมุ่งเน้นให้แก่หน่วยงานราชการ บริษัทขนาดเล็กและขนาดกลาง หรือผู้สนใจทั่วไป

2.7 ปัญหาด้านความมั่นคงในระบบ VoIP

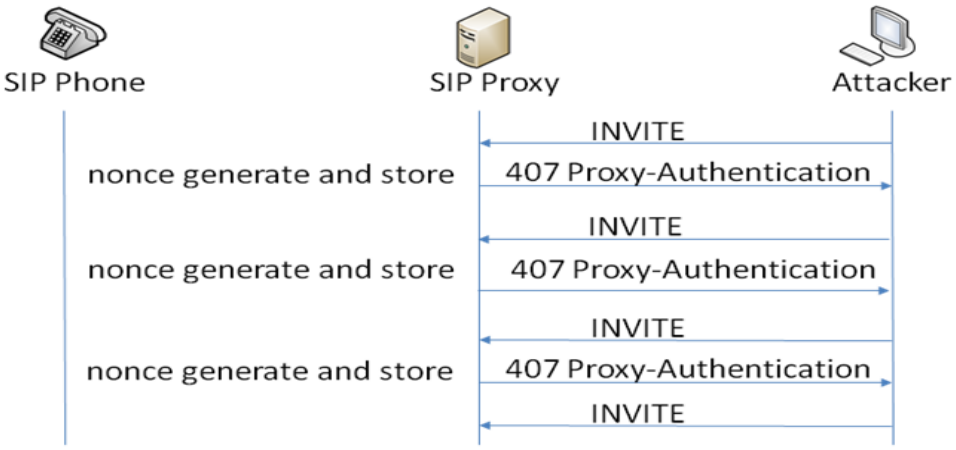
จากงานวิจัยที่ทำการวิเคราะห์ปัญหาด้านความมั่นคงของระบบ VOIP [1-3] สามารถสรุปปัญหาความบกพร่องด้านความมั่นคงในระบบ VoIP เมื่อเกิดขึ้นแล้วสามารถก่อผลเสียร้ายแรงต่อข้อมูลและตัวระบบ VoIP ซึ่งปัญหาเหล่านี้เป็นปัญหาที่ทำการโจมตีบนโพรโทคอลหลักของระบบ VOIP คือ SIP และ RTP โดยตรง สรุปไว้ ดังรูปที่ 2.6



รูปที่ 2.6 Man in the Middle (MITM)
ที่มา: [1]

1) Man-in-the-Middle [16] เป็นการแทรกกลางการสื่อสาร โดยวิธีการโจมตีด้วย ARP Spoof โดยผู้จู่โจมจะสร้าง ARP Reply ปลอมเข้าไปหาเครื่องเป้าหมาย โดยจะโยง IP address ของเครื่อง Server เข้ากับ MAC Address ของเครื่องผู้จู่โจมขึ้นมาแล้วโยง IP Address ของเครื่องเหยื่อเข้ากับ MAC address ทำให้การส่งข้อมูลทั้งหมดต้องผ่านเครื่องผู้จู่โจมซึ่งสามารถที่จะดักฟังข้อมูลข่าวสารหรือแก้ไขรวมไปถึงการขัดขวาง การส่งข้อมูลทั้งหมดก็ย่อมเป็นไปได้โดยผู้โจมตีนั้นต้องทำให้เหยื่อเชื่อว่ากำลังเชื่อมต่อโดยตรงอยู่เช่น รหัสผ่านเข้าสู่ระบบ หรือข้อมูลที่เป็นความลับต่างๆ ก็อาจถูกผู้จู่โจมดักจับได้

2) SIP Flooding Attack [17] ผู้จู่โจมสามารถยิง Packet ข้อมูลเป็นจำนวนมากและเร็วเข้าไปยัง IP-PBX Server และส่งผลให้ IP-PBX Server มีสภาวะการทำงานเพิ่มสูงขึ้นผิดปกติ จนเป็นสาเหตุทำให้ไม่สามารถให้บริการ โดยปกติวิธี Flooding Attack จากต้นทางเดียว (Single Source) เป็นวิธีที่ง่ายต่อการตรวจสอบ และป้องกัน แต่ DDoS ผู้จู่โจมจะปลอมเป็นเครื่องเหยื่อ หรือ IP-PBX Server แล้วจึงส่ง Packet นั้นออกไป ดังนั้น Packet จึงตอบกลับไปยังเครื่องที่ถูกผู้จู่โจมปลอม ซึ่งเป็นวิธีที่ตรวจสอบผู้จู่โจมได้ยาก หรืออาจจะตรวจพบเป็นเครื่องเหยื่อ ดังรูปที่ 2.7

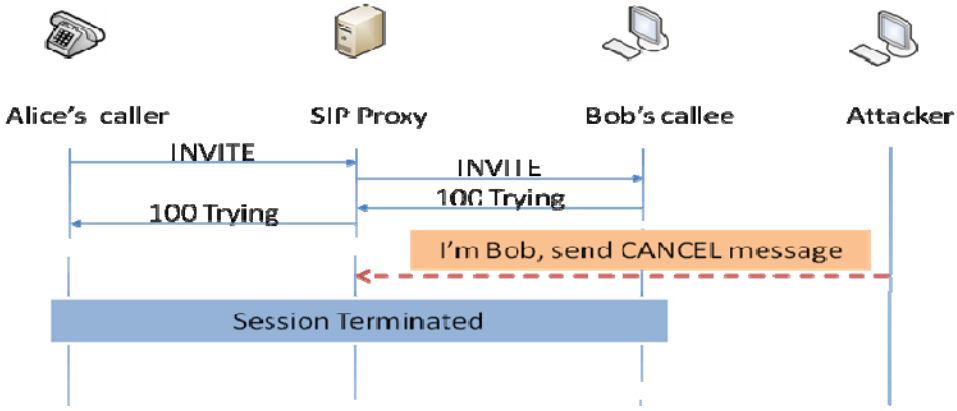


รูปที่ 2.7 SIP Flooding Attack
ที่มา: [1]

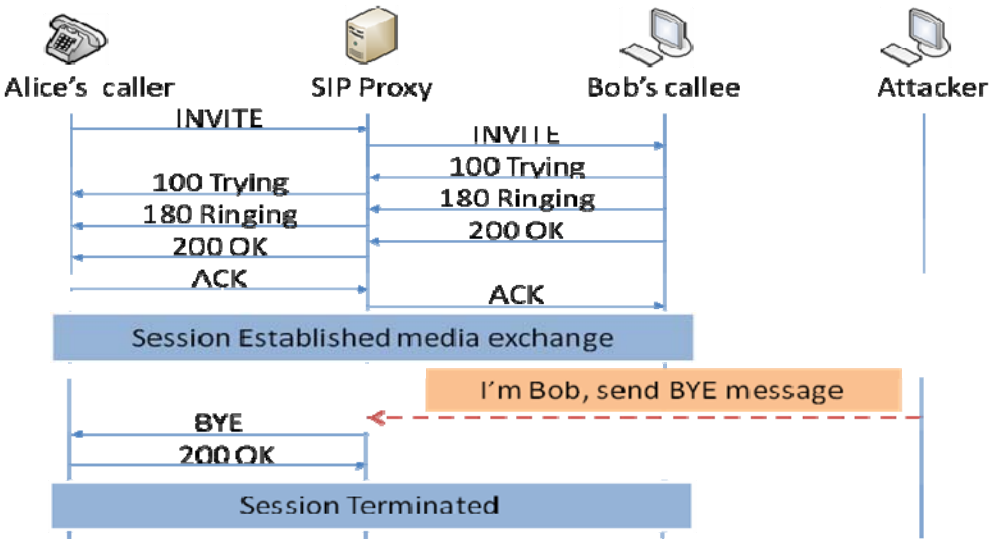
3) Cancel/Bye Attack [18] ผู้จู่โจมสามารถปลอมแปลงข้อความ CANCEL หรือ BYE เพื่อยกเลิก และสิ้นสุดการโทรด้วยวิธีแก้ไข Caller ID, Form tag, To tag ของข้อความ SIP ของเหยื่อดัง

4) รูปที่ 2.8 และดัง

5) รูปที่ 2.9



รูปที่ 2.8 Cancel Attack
ที่มา: [1]



รูปที่ 2.9 Bye Attack
ที่มา: [1]

2.8 มาตรฐานการวัดคุณภาพเสียง

ในการพัฒนาต่อยอดชุดซอฟต์แวร์ VoIP เพื่อให้มีความมั่นคงอาจจะไม่ใช่ประเด็นสำคัญเพียงอย่างเดียว แต่คุณภาพเสียงหลังจากมีการพัฒนาก็เป็นประเด็นสำคัญเช่นกัน ดังนั้น จึงจำเป็นต้องมีการวัดคุณภาพเสียงเพื่อดูผลว่าคุณภาพเสียงของระบบ VoIP ดีขึ้นหรือลดลงหรือไม่ เมื่อได้มีการเพิ่มความมั่นคงให้กับระบบ VoIP ซึ่งเรื่องคุณภาพการให้บริการเป็นเรื่องที่สำคัญและไม่ควรมองข้าม ในปัจจุบันมีมาตรฐานการวัดคุณภาพเสียงที่นิยมและเป็นที่ยอมรับอย่างกว้างขวางอยู่ 2 มาตรฐาน คือ

2.8.1 Mean Opinion Score (MOS)

MOS (Mean Opinion Score) [1,19] เป็นการประเมินคุณภาพเสียง ได้ถูกกำหนดเป็นมาตรฐานอยู่ใน Recommendation P.800 โดยองค์กรสหภาพโทรคมนาคมระหว่างประเทศ (ITU) ซึ่งเป็นวิธีการวัดคุณภาพเสียงที่ได้รับการยอมรับอย่างกว้างขวาง เป็นการวัดคุณภาพเสียงในลักษณะของการประเมินเชิงคุณภาพ (Subjective) วิธีการคือ ให้ผู้ทดสอบจำนวนมากโทรศัพท์พูดคุยซึ่งกันและกัน จากนั้นให้คะแนนคุณภาพของเสียง ผลการทดสอบจะได้จากผู้ที่เข้าร่วมทดสอบทุกคน โดย MOS เป็นค่าเฉลี่ยที่ได้จากความคิดเห็นของผู้ใช้โดยมีระดับความคิดเห็น 1 ถึง 5 ซึ่งมีรายละเอียดดังตารางที่ 2.1

การวัดคุณภาพเสียงแบบ MOS เป็นวิธีที่ง่ายและเป็นที่ยอมรับถึงผลการวัดคุณภาพเสียงที่ได้ เนื่องจากเป็นการวัดที่ตรงจุดหรือกับผู้ใช้งานโดยตรง จำนวนผู้เข้าร่วมวัดคุณภาพยิ่งมากเท่าไหร่ยิ่งทำให้มีความน่าเชื่อถือเพิ่มมากขึ้น จากงานวิจัยหลาย ได้ระบุค่าคุณภาพต่ำสุดของ MOS ที่สามารถยอมรับได้คือ MOS >= 3.5 ซึ่งเมื่อได้ค่า MOS ต่ำกว่า 3.5 จะทำให้ผู้ใช้บริการเกิดความไม่พอใจต่อคุณภาพเสียงของ VoIP ดังตารางที่ 2.1

ตารางที่ 2.1 Listening Quality Scale

MOS	Quality of Voice Rating	User Satisfaction
5 (4.34)	Best	Very satisfied
4 (4.03)	High	Satisfied
3 (3.60)	Medium	Some users dissatisfied
2 (3.10)	Low	Many users dissatisfied
1(2.58)	Poor	Nearly all users dissatisfied

ที่มา: [1]

แต่การวัดคุณภาพเสียงแบบ MOS มีข้อเสียคือ สิ้นเปลืองงบประมาณและเวลาที่ใช้ทดสอบเป็นอย่างมาก ลักษณะการวัดคุณภาพเสียงแบบ MOS ไม่สามารถวิเคราะห์ปัจจัยแวดล้อมต่างๆ ที่มีผลต่อคุณภาพเสียง เช่น Delay, Packet Loss และ Jitter เป็นต้น งานวิจัยนี้จึงได้ทำการเลือกเครื่องมือใหม่ที่ใช้สำหรับวัดคุณภาพเสียงที่เรียกว่า E-Model

2.8.2 E-Model

E-Model [1, 20] คุณภาพเสียงที่ดีก็คือเสียงที่ออกมาจะต้องใกล้เคียง หรือเหมือนกับต้นฉบับให้มากที่สุด ซึ่งการวัดคุณภาพเสียงผ่านเครือข่ายมีอยู่ 2 แบบ คือ

1. แบบ Active Testing เป็นวิธีที่ใช้โดยการใช้เปรียบเทียบกับต้นฉบับ โดยการนำเอา audio file ต้นฉบับมาแบ่งเป็นบล๊อคเล็กๆ มาเปรียบเทียบและทำการให้คะแนน ว่าคะแนนที่ได้จะไม่ค่อยตรงกับคะแนน MOS

2. แบบ Passive Monitoring การนำเอาเสียงที่ผ่านเครือข่ายมาแล้ว และผ่านกระบวนการที่เรียกว่า Pre-Processing จากนั้นก็นำมาประมวลผลเพื่อแยกเอาค่าพารามิเตอร์ของเสียงและค่าความเพี้ยนต่างๆ ออกมา ซึ่งเมื่อได้ค่าพารามิเตอร์ของเสียงและค่าความเพี้ยนต่างๆ แล้ว ก็จะนำมาสร้างเป็นค่า MOS ที่มีค่าตั้งแต่ 1 ถึง5 ซึ่ง International Telecommunication Union (ITU) ใช้เป็นแบบจำลองหรือเครื่องมือในการวิเคราะห์คุณภาพเสียงที่ใช้สำหรับการวางแผนเครือข่าย ซึ่งผลลัพธ์พื้นฐานของ E-model คือ การคำนวณจาก R-factor จะอยู่ระหว่าง 0 ถึง 100 ซึ่งครอบคลุมปัจจัยด้านต่างๆ ที่มีผลต่อคุณภาพเสียง จาก [22] 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

แต่ R-factor เป็นการคำนวณจากพารามิเตอร์หลายตัวซึ่งเป็นสูตรทางคณิตศาสตร์ที่ซับซ้อน ITU-T G.109 ได้มองว่าค่าคำนวณที่มีคุณภาพจะถูกกำหนดโดยค่า ความบกพร่องของความล้าช้า (Delay Impairment I_d ที่ครอบคลุมการสูญเสียของการติดต่อสื่อสาร และค่าความบกพร่องของคุณภาพอุปกรณ์ (Effective Equipment Impairment) I_{ef-eff} ซึ่งครอบคลุมการสูญเสียข้อมูลเนื่องจากการเข้ารหัสรูปแบบและการสูญเสีย Packet (Packet Loss) จึงได้ทำการลดสูตรเพื่อให้ง่ายต่อการคำนวณและได้ค่าคำนวณ R ที่มีคุณภาพ ดังสมการ 2

$$R = 93.2 - I_d - I_{e-eff} \qquad (2)$$

โดยที่

$$I_d = \begin{cases} 0 & ;Ta \le 100ms \\ I_{dd} & ;Ta > 100ms \end{cases}$$

$$I_{dd} = 25 \times \left\{ \left(1 + X^6\right)^{\frac{1}{6}} - 3\left(1 + \left[\frac{X}{3}\right]^6\right)^{\frac{1}{6}} + 2 \right\}$$

$X = \dfrac{\log\left(\dfrac{Ta}{100}\right)}{\log 2}$; โดยที่ Ta = ค่าเวลาความล้าช้า (Delay Time)

$$I_{e-eff} = I_e \times \left\{ \left(95 - I_e\right) \times \frac{Ppl}{Ppl + Bpl} \right\}$$

โดยที่ Ppl = Packet-Loss Probability

I_e = Equipment Impairment Factor ค่าในตารางที่ 2.2

Bpl = Packet-Loss Robustness Factor ค่าในตารางที่ 2.2

ตารางที่ 2.2 ค่า I_e และ Bpl ของแต่มาตรฐาน CODBC

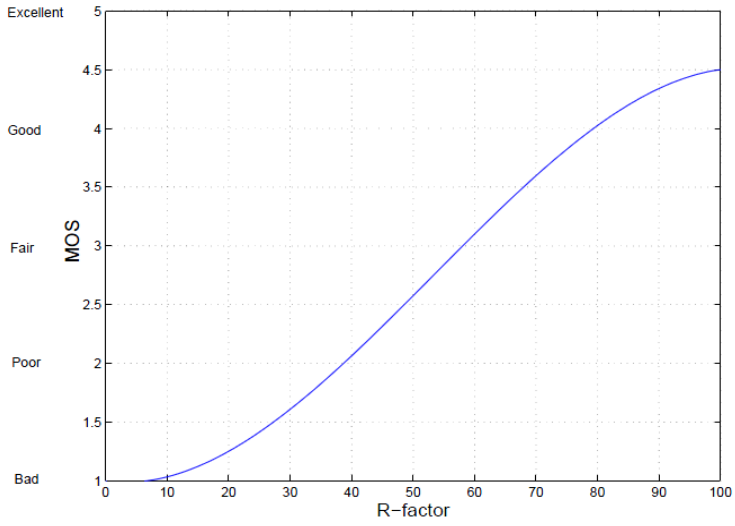
CODBC	I_e	Bpl
G.711	0	4.3
G.723	15	16.1
G.729	11	19

ที่มา: [1]

โดยค่า R-factor ที่ได้มีตั้งแต่กรณีที่ดีที่สุดคือ 100 ถึงกรณีที่เลวร้ายที่สุดคือ 0 ซึ่งค่าคุณภาพต่ำสุดที่ยอมรับได้คือ R-factor >= 70 และค่าคำนวณที่ได้จาก R-factor จะมีความสัมพันธ์กับค่า MOS ดังสมการ 3

$$For\ R<0: MOS=1$$
$$For\ R>100: MOS=4.5 \qquad (3)$$
$$For<R<100: MOS=1+0.035R+7x10^{-6}\ R(R-60)(100-R)$$

จากอัลกอริธึมสมการ 3 สามารถ Plot เป็นกราฟได้



รูปที่ 2.10 กราฟความสัมพันธ์ระหว่าง R-factor และ MOS

ค่า R-factor ที่คำนวณได้สามารถมาเปรียบเทียบกับ Quality of voice rating ในตารางที่ 2.3

ตารางที่ 2.3 ค่าความพึงพอใจของผู้ใช้งานของ R-factor

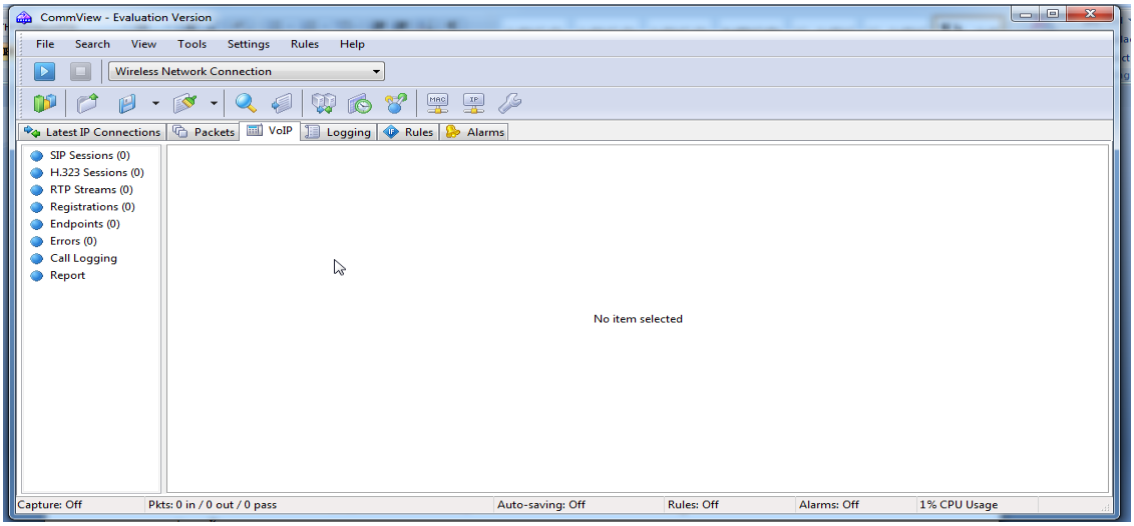
R-Factor (lower value)	User satisfaction
90	Very satisfied
80	Satisfied
70	Some users dissatisfied
60	Many users dissatisfied
50	Nearly all users dissatisfied

ที่มา: [1]

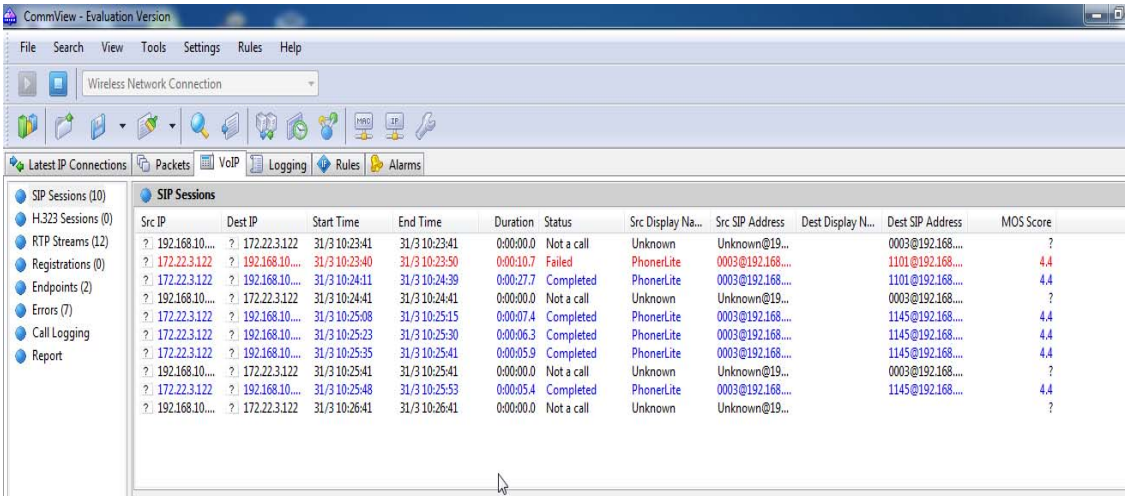
โดย กสทช. ว่าโดยมาตรฐานสำหรับการให้บริการเสียงผ่านการให้บริการอินเทอร์เน็ตให้เป็นไปตามข้อเสนอแนะของ ITU-T โดยผลต่อคุณภาพเสียง จากสมการ (1) MOS ที่สามารถยอมรับได้คือ MOS >= 3.5

2.9 โปรแกรม CommView

CommView [21] เป็นซอฟต์แวร์ที่ถูกพัฒนาโดยบริษัท TamoSoft Ltd. เป็นซอฟต์แวร์ประเภทแชร์แวร์ (Shareware) คุณสมบัติ คือ ใช้ในการตรวจสอบและดูแลเกี่ยวกับระบบเครือข่ายทั่วไปและแบบไร้สายภายในองค์กร ซึ่งซอฟต์แวร์นี้สนับสนุนเครือข่ายไร้สายหลายชนิดไม่ว่าจะเป็น 802.11 a/b/g/n/ac เป็นต้น ซอฟต์แวร์นี้มีการนำเสนอรูปแบบของระบบเครือข่ายแบบภาพรวม พร้อมทั้งรายละเอียดของระบบเครือข่ายที่เข้าใจได้ง่าย สามารถใช้ซอฟต์แวร์นี้ในการดับจับ Packet ในระบบเครือข่ายได้หลายชนิดด้วยกันทั้ง TCP และ Packet ของระบบ VoIP เช่น SIP, H.323, RTP, SRTP และยังสามารถวิเคราะห์คุณภาพเสียงของระบบ VoIP โดยการใช้การวัดคุณภาพเสียงแบบ E-Model ซึ่งที่เป็นมาตรฐานที่มีการยอมรับอย่างแพร่หลาย ซอฟต์แวร์สามารถแสดงข้อมูลคุณภาพได้แบบเวลาจริง (real-time) ซึ่งมีความแม่นยำสูง ลักษณะซอฟต์แวร์ดังรูปที่ 2.11 และ รูปที่ 2.12



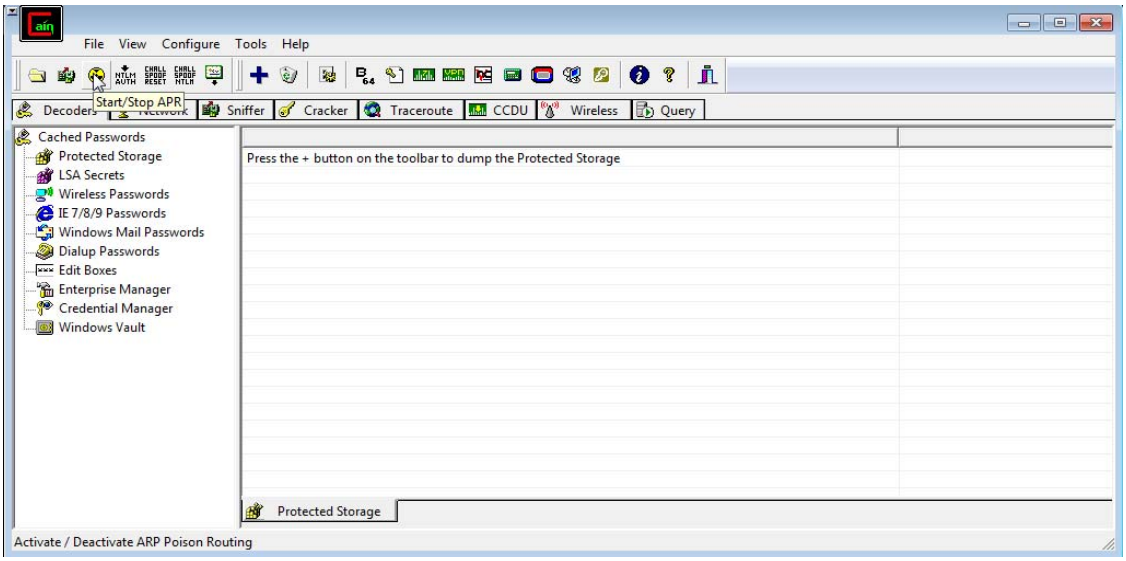
รูปที่ 2.11 CommView 6.1



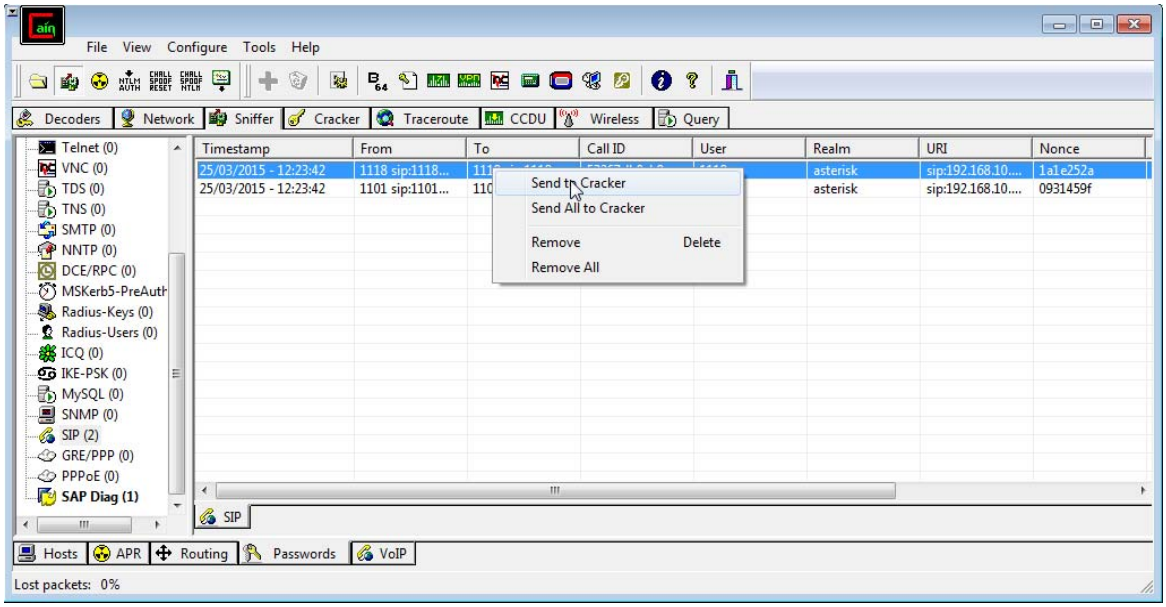
รูปที่ 2.12 ข้อมูล Packet คุณภาพเสียง

2.10 โปรแกรม Cain & Abel

Cain & Abel [23] ที่ใช้ในงานศึกษาค้นคว้าอิสระนี้คือ Version 4.9 เป็นเครื่องมือที่รวมการจู่โจมอย่างมาก สามารถทำการถอดรหัสผ่านได้หลากหลายรูปแบบ เช่น ทำการดักข้อมูลรหัสผ่านจากเครือข่าย, การแฮกรหัสผ่านแบบ Brute-Force และสามารถทำการบันทึกการสนทนาแบบ VoIP และได้รับการจัดเป็นเครื่องมืออันดับที่ 9 ใน Top 100 Network Security Tools จากเว็บไซต์ http://sectools.org เป็นเครื่องมือที่มีความสามารถสูง และได้รับการยอมรับกันอย่างกว้างขวาง ดังรูปที่ 2.13

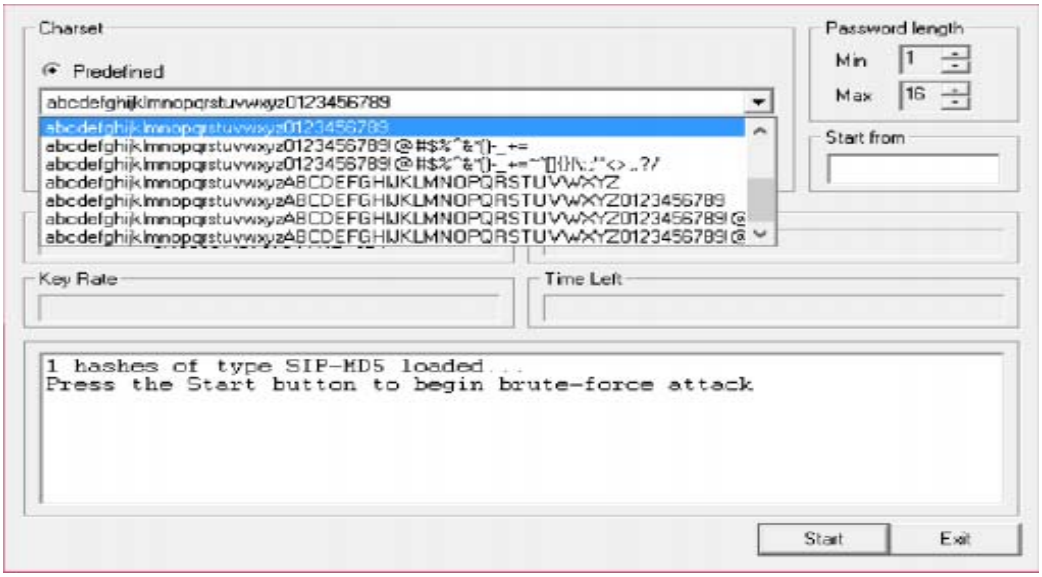


รูปที่ 2.13 Cain & Abel

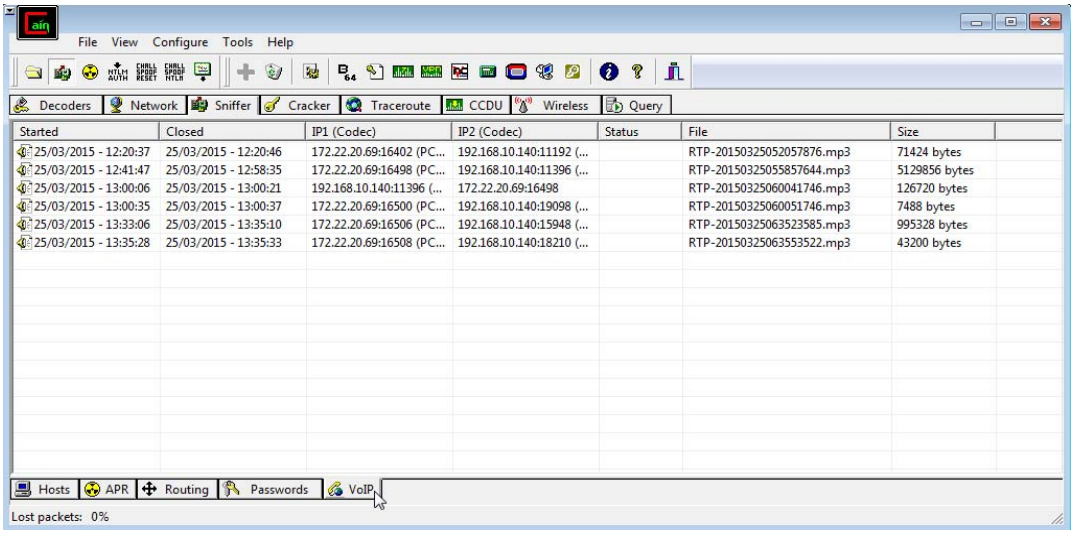


รูปที่ 2.14 ข้อมูล IP Phone ที่ทำการดักจับได้

จากรูปที่ 2.14 ข้อมูล IP Phone ที่ทำการดักจับได้ จะคลิกขวา Send Cracker เพื่อส่งไปทำการถอดรหัสผ่าน โดยBrute-Force attack ดังรูปที่ 2.15



รูปที่ 2.15 Brute-Force attack เพื่อถอดรหัสผ่าน

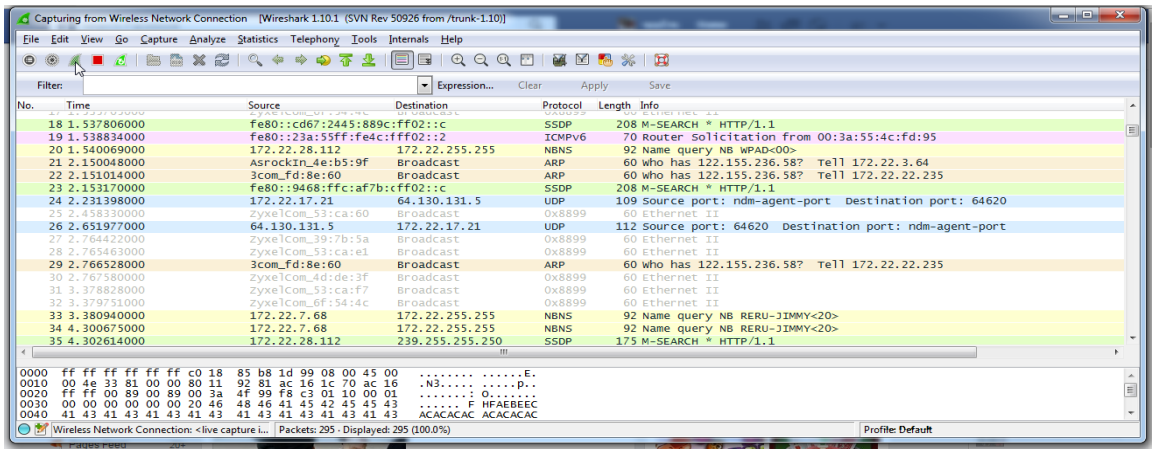


รูปที่ 2.16 ดักฟังเสียงสนทนา

จากรูปที่ 2.16 ดักฟังเสียงสนทนา เมื่อคลิก VoIP ดังรูปก็จะโชว์ข้อมูลเสียงที่ทำการดักจับมาได้ ซึ่งไฟล์ที่ได้เป็น .MP3 สามารถนำมาเปิดฟังได้เลย

2.11 โปรแกรม Wireshark

Wireshark [24] ที่ใช้ในงานศึกษาค้นคว้าอิสระนี้คือ Version 1.10 เป็นเครื่องมือที่สามารถทำการวิเคราะห์ข้อมูลบนเครือข่ายได้หลายรูปแบบ เช่น การดูรายละเอียดต่างๆ ของข้อมูลที่ต้องการการวิเคราะห์แพ็ตเกตที่ดึงมาได้ และทำการวิเคราะห์ข้อมูลแบบ Real time สามารถทำงานได้ทั้งบนระบบปฏิบัติการ UNIX และ Windows และเป็นซอฟต์แวร์แบบ Open Source ดังรูปที่ 2.17



รูปที่ 2.17 โปรแกรม Wireshark

2.12 โปรแกรม Backtrack

Backtrack [25] ที่ใช้ในงานศึกษาค้นคว้าอิสระนี้คือ Version 4 เป็น OS ที่พัฒนามาจาก Ubuntu โดยที่ Backtrack เน้นไปทางระบบความปลอดภัยของคอมพิวเตอร์และระบบเครือข่าย เป็นที่รวมเครื่องมือทดสอบการเจาะระบบหรือเครื่องมือในการแฮกข้อมูล สำหรับงานศึกษาค้นคว้าอิสระนี้จะใช้ในการจู่โจม Cancel/Bye Attack เพื่อทำให้การสื่อสารล้มเหลว และ SIP Flooding Attack เพื่อให้ปฏิเสธการบริการ ซึ่งในปัจจุบัน Backtrack หยุดที่ Version 5 และเปลี่ยนมาเป็น Kali Linux ซึ่งง่ายต่อการติดตั้งและประหยัดเวลา รองรับการปรับแต่งบนระบบปฏิบัติการ

รูปที่ 2.18 โปรแกรม Backtrack 4

2.13 งานวิจัยที่เกี่ยวข้อง

ระบบ VoIP มีความสำคัญและมีการเสนอนำมาใช้ในองค์กร ดังงานวิจัยของ กิตติ เปรมพรวิพุธ [10] ใช้กับมหาวิทยาลัยหอการค้าไทย โดยการศึกษาถึงปัจจัยในด้าน ความเหมาะสมในการเลือกระบบ VoIP ความคุ้มค้าในการลงทุน และการนำมาใช้งานและการบำรุงรักษาอุปกรณ์ ในด้านการบำรุงรักษาสามารถทำได้สะดวก แต่ยังไม่คุ้มค่ากับการลงทุนเนื่องจากค่าโทรศัพท์แบบ IP Phone ยังมีราคาที่สูงมาก ชญาภา พงษ์วิชัย [11] ใช้งานภายในองค์กร โดยการนำระบบ VoIP มาประยุกต์ใช้งานในหน่วยงาน เพื่อให้มีความคุ้มค่า เป็นการจำลองคอมพิวเตอร์เสมือน ขึ้นมาใช้งาน และณัฐภัทร พงศ์พุทธางกูร [12] ได้ศึกษาแนวทางการปรับปรุงและเพิ่มประสิทธิภาพการให้บริการ VoIP การศึกษาสภาพปัญหาในปัจจุบันของธุรกิจบริหาร VoIP ประกอบกับการศึกษามาตรฐานสากล รวมถึงนำเสนอแนวทางในการปรับปรุงและเพิ่มประสิทธิภาพการให้บริการ VoIP ระยะเวลาที่ใช้ในการเชื่อมต่อการเรียก และระยะเวลารอสายสำหรับ Call Center คุณภาพเสียงยังต่ำกว่าคุณภาพระดับ Toll Quality ทั้งสิ้น เนื่องจากทุกวันนี้ VoIP มีความสำคัญมากในทางด้านธุรกิจอย่างมาก ทั้งในด้านคุณภาพเสียง และการส่งข้อมูลที่ถูกต้อง ซึ่งยังเป็นปัญหาที่เกิดขึ้นกับด้านธุรกิจ

มีงานวิจัยพบปัญหาด้านความมั่นคงของระบบ VoIP เช่น ปิยะวัจน์ ค้าสบาย และสมนึก พ่วงพรพิทักษ์ [2] ได้ประเมินปัญหา แล้วพบว่าเทคนิคการจู่โจม การดักฟังเสียงที่สนทนา การตัดสายที่สนทนาด้วย การจู่โจมเครื่องให้บริการด้วย SIP flooding นอกจากนี้ Salsano และคณะ [17] และ Sisalem และคณะ [18] ได้แสดงให้เห็นถึงจุดอ่อนของระบบ VoIP ต่อการถูก SIP Flooding จน IP-PBX ไม่ตอบสนองต่อผู้ใช้ ที่เรียกว่า เกิด DoS (Denial of Services) พบว่าปัญหาภัยคุกคามต่อระบบโทรศัพท์ผ่านอินเทอร์เน็ตนั้น มีอยู่หลากหลายและอาจจะส่งผลต่อระบบโทรศัพท์ผ่านอินเทอร์เน็ตภายในมหาวิยาลัยราชภัฏร้อยเอ็ดได้ ซึ่งการจู่โจมดังกล่าวได้แก่ การดักฟังเสียงที่สนทนา การตัดสายที่สนทนาด้วย Cancel/bye attacks การจู่โจมเครื่องให้บริการด้วย SIP flooding ซึ่งจะได้ทำการประเมินความมั่นคงของระบบโทรศัพท์ผ่านอินเทอร์เน็ตของมหาวิทยาลัยราชภัฏร้อยเอ็ด

จากผลการวิเคราะห์และประเมินปัญหาความมั่นคงเบื้องต้น อีกทั้งมีงานวิจัยของ คธาวุฒิ จันบัวลา และสมนึก พ่วงพรพิทักษ์ [1] ได้ทำการพัฒนาต่อยอดชุดซอฟต์แวร์ ISANBox จาก Asterisk โดยทำให้มั่นคงขึ้น และทำการทดสอบโดยนอกจากจะสนใจด้าน Security แล้ว ยังเสนอว่า ควรสนใจด้านคุณภาพเสียงที่ให้บริการด้วย เพราะการเพิ่มประสิทธิภาพด้านความมั่นคง ย่อมส่งผลกระทบต่อด้านคุณภาพเสียงที่ให้บริการเพราะมี overhead จากขบวนการเข้ารหัสและขั้นตอนต่างๆ ที่เพิ่มขึ้น การวัดคุณภาพเสียงจึงจำเป็นเพื่อดูว่า กลไกด้านความมั่นคง ที่ใส่เข้าไปนั้นส่งผลลบมากเกินไปหรือไม่ หากมากเกินไปจนคุณภาพการให้บริการต่ำมาก ย่อมไม่อาจยอมรับได้ โดยงานวิจัยนี้ เสนอให้ใช้ R-factor [20] และ MOS [19] เป็นตัวชี้วัดผลคุณภาพ

ทั้งนี้ กสทช มีประกาศ มาตรฐานสำหรับการให้บริการเสียงผ่านการให้บริการอินเทอร์เน็ต [26] ว่า คุณภาพเสียงที่ยอมรับได้ในการให้บริการโดยเป็นไปตามข้อเสนอแนะโดยอ้างอิงมาจากมาตรฐาน ITU-T G.107 [20]

งานวิจัยนี้ อาศัยแนวคิดเดียวกัน คือในการวัดประสิทธิภาพของ VoIP System ของ มรภ ร้อยเอ็ด ต้องทำการวัดทั้งด้านความมั่นคงและคุณภาพเสียงที่ให้บริการด้วย โดยเฉพาะอย่างยิ่งหลังการปรับปรุงให้มีความมั่นคงเพิ่มขึ้น เพื่อดูว่าค่าคุณภาพเสียงในการให้บริการนั้นลดลงจนยอมรับได้หรือไม่ โดยอาศัยค่า MOS และ R-factor เช่นเดียวกับงานวิจัยข้างต้น และพิจารณาค่าที่ กสทช กำหนดด้วย

ประดิษฐ์ วงษ์สกุล และคณะฯ [3] ได้พัฒนาชุดซอฟต์แวร์สำหรับ VoIP จาก FreeSWITCH ซึ่งเป็นอีก VoIP IP-PBX Program โดยเชื่อว่า FreeSWITCH อาจมีประสิทธิภาพดีกว่า Asterisk หากมี load ของ IP-PBX ขนาดใหญ่ โดยในงานวิจัยนี้ ทีมวิจัยได้พัฒนาระบบเสริมสร้างความมั่นคงเข้าไปเพิ่มให้กับ FreeSWITCH โดยสามารถป้องกันการจู่โจม เช่น การดักฟังเสียงที่สนทนา การตัดสายที่สนทนาด้วย Cancel/bye attacks การจู่โจมเครื่องให้บริการด้วย SIP flooding ในงานวิจัยนี้ เรียกชุดซอฟต์แวร์ VoIP ของตนว่า ISANBox.A

สมนึก พ่วงพรพิทักษ์ และ เดชสิทธิ์ พรรษา [22] ได้รับทุนวิจัยจาก สำนักงานคณะกรรมการวิจัยแห่งชาติ ในหมวดทุนวิจัยการพัฒนาเทคโนโลยีเพื่อความมั่นคงปลอดภัยไซเบอร์ เพื่อดำเนินการพัฒนาต่อยอด ISANBox.A [16] ให้มีประสิทธิภาพเพิ่มขึ้น กลายเป็น ISANBox.A รุ่นล่าสุด คือ version 3.0 ซึ่งถูกนำมาใช้ในการศึกษาค้นคว้าอิสระนี้ เพื่อใช้แทน Elastix ในการปรับปรุงความมั่นคงระบบ VoIP ของมหาวิทยาลัยราชภัฏร้อยเอ็ด

นอกจากนี้ งานวิจัย [22] นี้ ยังทำการศึกษาปัญหาของ Key Agreement Protocol ของระบบ VoIP ที่ยังเป็นจุดอ่อนต่อการจู่โจมและเสนอต่อยอดเพิ่มความมั่นคงให้แก่ VoIP Key Agreement Protocols ด้วย

2.14 วิธีการประเมินคุณภาพของเครือข่าย

1) Analytical modeling เป็นการวิเคราะห์แบบจำลองทางคณิตศาสตร์ที่มีรูปแบบวิธีการแก้ปัญหาสมการ

2) Simulation การนำเสนอหรือจำลองระบบลักษณะการทำงาน ตลอดช่วงเวลาที่สนใจตั้งแต่เริ่มต้นการทำงานจนสิ้นสุดการทำงาน

3) Measurement การวัดค่าเครื่องมือทดสอบด้านเทคนิคทำได้ 2 อย่างคือ

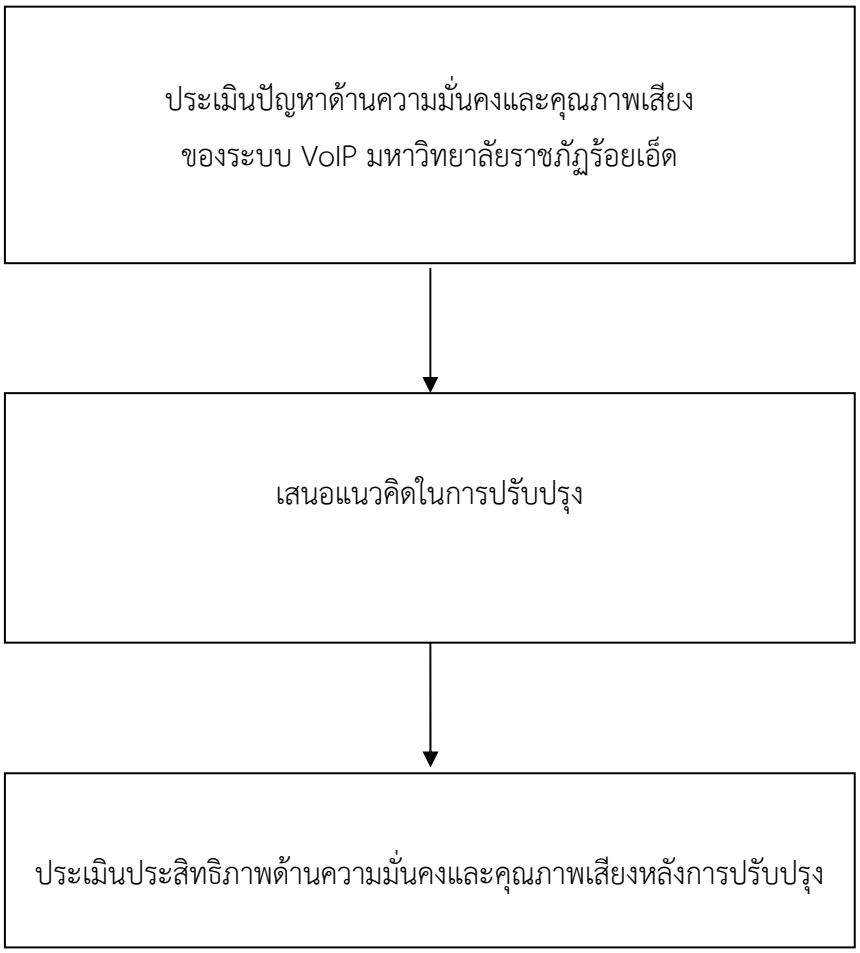
(1) Real bed การทำเครือข่ายจำลอง ขึ้นมาเพื่อวัดค่า

(2) Real Network คือการวัดค่าจากระบบจริง

บทที่ 3

วิธีดำเนินการวิจัย

3.1 ภาพรวมงานวิจัย



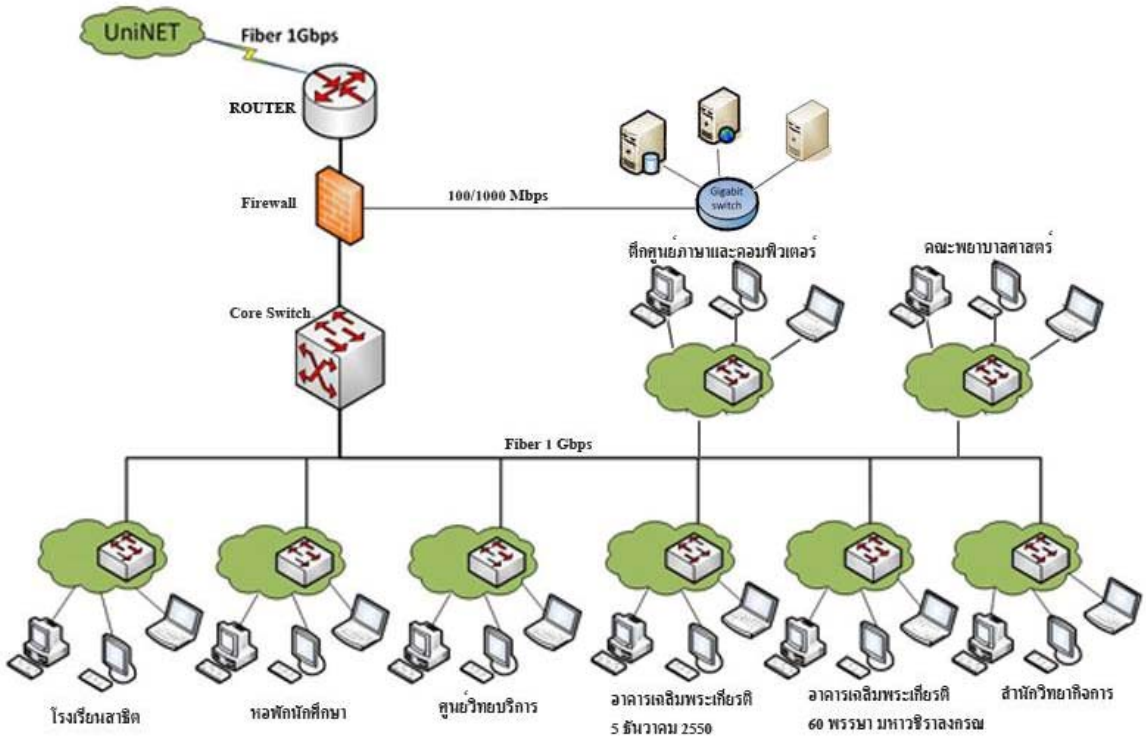
รูปที่ 3.1 ภาพรวมงานวิจัย

จากรูปที่ 3.1 เป็นภาพรวมการค้นคว้าอสิระโดยแบ่งเป็น 3 ส่วน ได้แก่ ประเมินปัญหาด้านความมั่นคงและคุณภาพเสียงของระบบ VoIP มหาวิทยาลัยราชภัฏร้อยเอ็ด เสนอแนวคิดในการปรับปรุง และประเมินประสิทธิภาพด้านความมั่นคงและคุณภาพเสียงหลังการปรับปรุงระบบ VoIP มหาวิทยาลัยราชภัฏร้อยเอ็ด

3.2 การประเมินปัญหาด้านความมั่นคงและคุณภาพเสียงของระบบ VoIP มหาวิทยาลัยราชภัฏร้อยเอ็ด

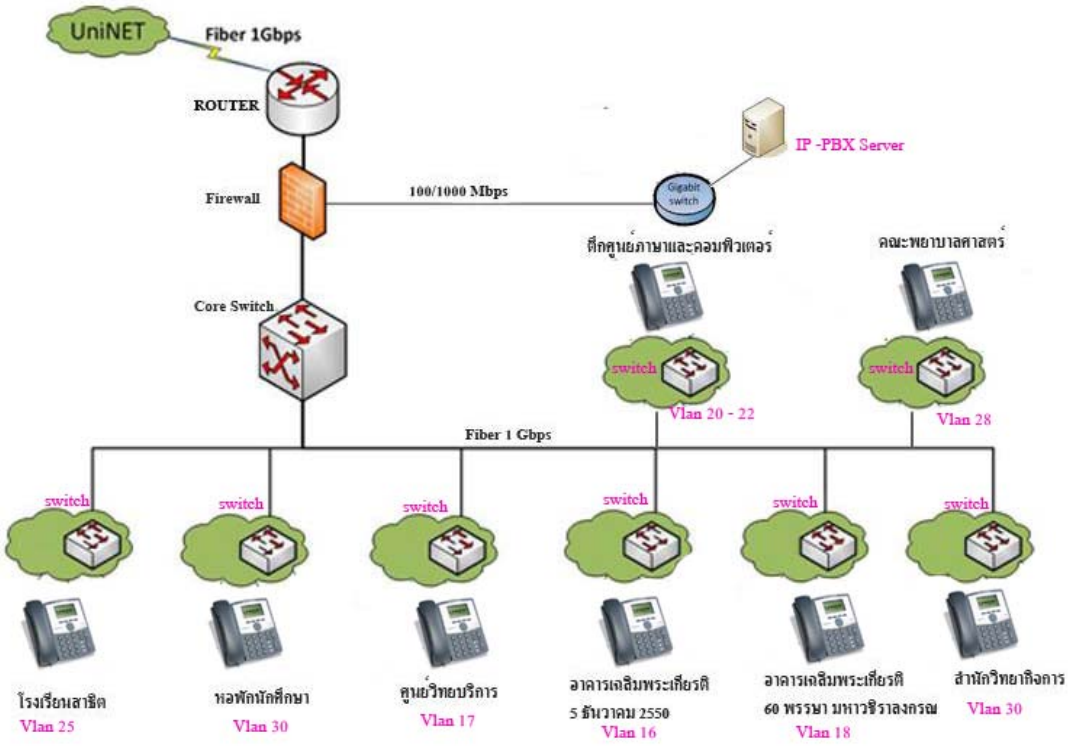
3.2.1 วิเคราะห์และประเมินภาพรวมของระบบ VoIP ภายในมหาวิทยาลัยราชภัฏร้อยเอ็ด

ขั้นตอนนี้เป็นการสังเกตโดยผู้วิจัยเข้าสังเกตการณ์ ระบบเครือข่ายอินเทอร์เน็ตภายในมหาวิทยาลัยราชภัฏร้อยเอ็ด โดยมหาวิทยาลัยราชภัฏร้อยเอ็ดที่ได้ทำการติดตั้งระบบโทรศัพท์ผ่านอินเทอร์เน็ต โดยใช้ฟรีชุดซอฟต์แวร์ Elastix v.2.3.0 (Asterisk v.1.8.7) ซึ่งเป็น VoIP Open Source Software และระบบปฏิบัติการ Linux Cent OS โดยการทำวิเคราะห์และประเมินตามอาคารที่มีการใช้งาน โดยมีจำนวน 8 อาคาร อาคารเฉลิมพระเกียรติ 60 พรรษามหาวชิราลงกรณ อาคาร 80 พรรษา 5 ธันวาคม พ.ศ. 2550 อาคารวิทยกิจทีปังกร คณะพยาบาลศาสตร์ ศูนย์ภาษาและคอมพิวเตอร์ ศูนย์วิทยบริการ โรงเรียนสาธิต หอพักนักศึกษาชายหญิง จำนวน 2 หอ ดังรูปที่ 3.2



รูปที่ 3.2 แผนผังโครงสร้างเครือข่ายอินเทอร์เน็ต มหาวิทยาลัยราชภัฏร้อยเอ็ด

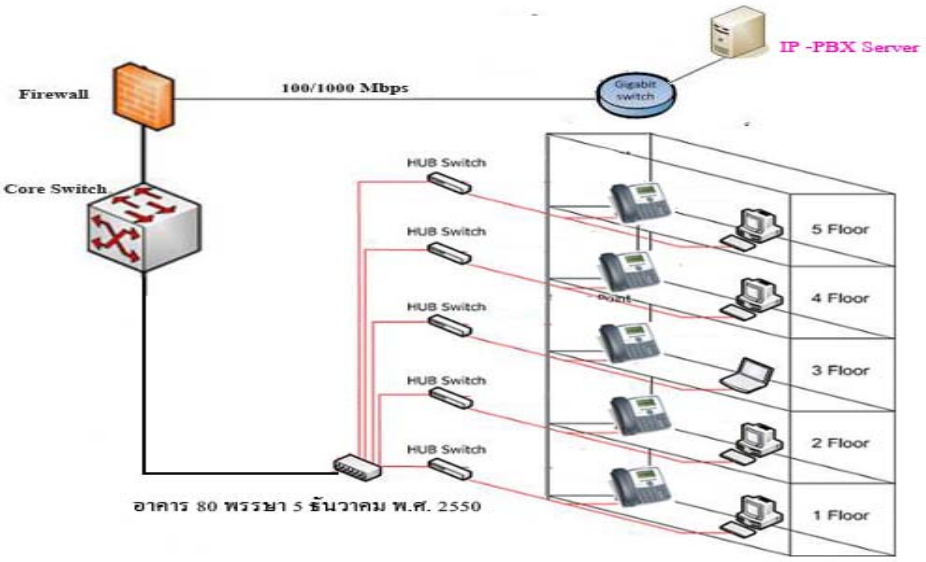
จากรูปที่ 3.2 ระบบเครือข่ายอินเทอร์เน็ตภายในมหาวิทยาลัยราชภัฏร้อยเอ็ดนั้นได้มีการแบ่ง VLAN การใช้งานอินเทอร์เน็ตแต่ไม่ได้มีระดับการป้องกันที่สมบูรณ์ซึ่งสามารถทำการจู่โจมระบบได้ง่าย



รูปที่ 3.3 แผนผังโครงสร้างระบบโทรศัพท์ผ่านอินเทอร์เน็ต มหาวิทยาลัยราชภัฏร้อยเอ็ด

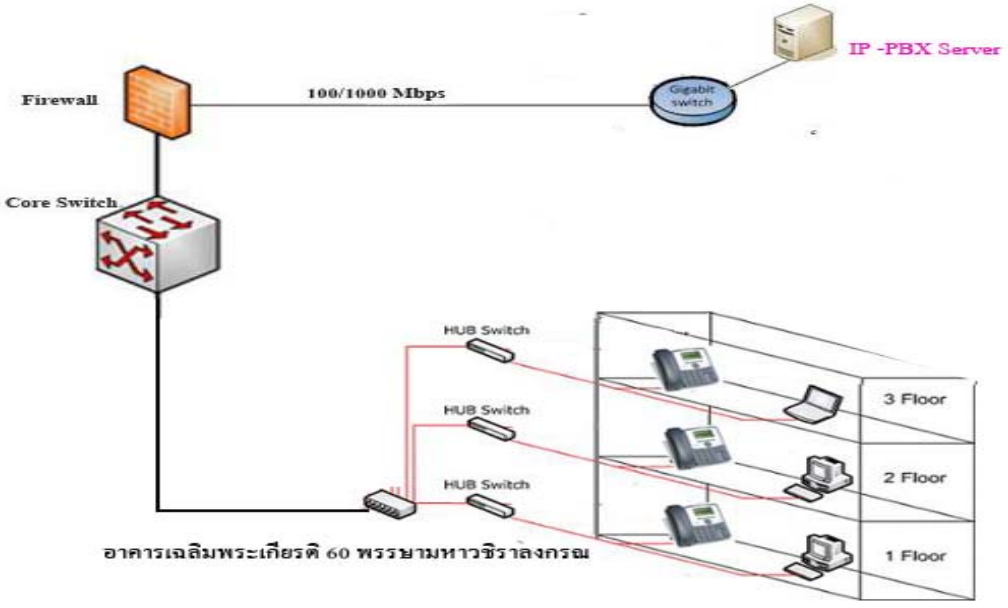
จากรูปที่ 3.3 แผนผังโครงสร้างระบบโทรศัพท์ผ่านอินเทอร์เน็ต ซึ่งไม่ได้มีการแบ่ง VLAN เฉพาะ VoIP แต่มีการใช้งานร่วมกันกับเครือข่ายภายใน ซึ่งในบางจุดมีการเชื่อมต่อจาก โทรศัพท์ VoIP ไปยัง Server นั้นมีจำนวนประมาณ 5 Hops ซึ่งควรมีการทดสอบคุณภาพของเสียงที่ให้บริการผ่านระบบ VoIP ว่ามีปัญหาด้านคุณภาพหรือไม่ เนื่องจากมี data traffic อื่นๆ ของมหาวิทยาลัยปนไปกับ voice traffic ของระบบ VoIP System ซึ่งปนอยู่ในเครือข่ายเดียวกัน ทั้งระดับ Physical ที่ไม่ได้มีการแยกสาย และระดับ logical ที่ไม่มีการแยก VLAN เป็นพิเศษให้กับ VoIP

การไม่แยก VLAN ให้กับระบบ VoIP ยังอาจเป็นจุดให้ผู้ใช้ทั่วไปในระบบ LAN วงเดียวกันกับผู้ใช้งานระบบ VoIP ซึ่งรวมถึงผู้บริหารมหาวิทยาลัย อาจถูกดักจูโจม หรือดักฟังเสียงได้ ซึ่งควรต้องมีการทดสอบความมั่นคงของระบบดังกล่าว



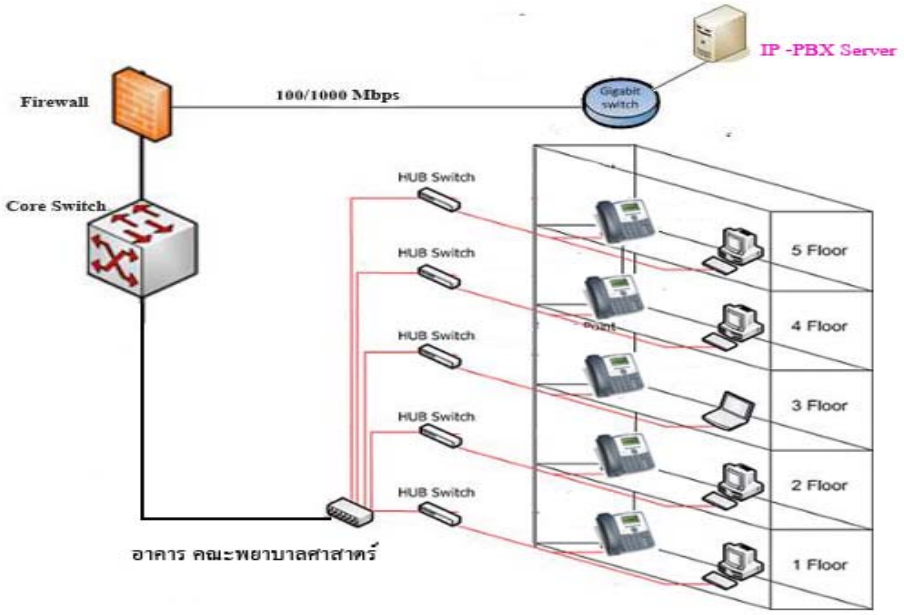
รูปที่ 3.4 แผนผังระบบโทรศัพท์ผ่านอินเทอร์เน็ตอาคาร 80 พรรษา 5 ธันวาคม พ.ศ. 2550

จากรูปที่ 3.4 ระบบโทรศัพท์ผ่านอินเทอร์เน็ตอาคาร 80 พรรษา 5 ธันวาคม พ.ศ. 2550 ซึ่งอาคารเรียนรวมจำนวน 9 ชั้น และจะมีหน่วยในต่างๆภายในอยู่ในอาคารซึ่งมีการใช้งาน ซึ่งมีการใช้งานจำนวนโทรศัพท์เป็นจำนวน 30 เครื่อง



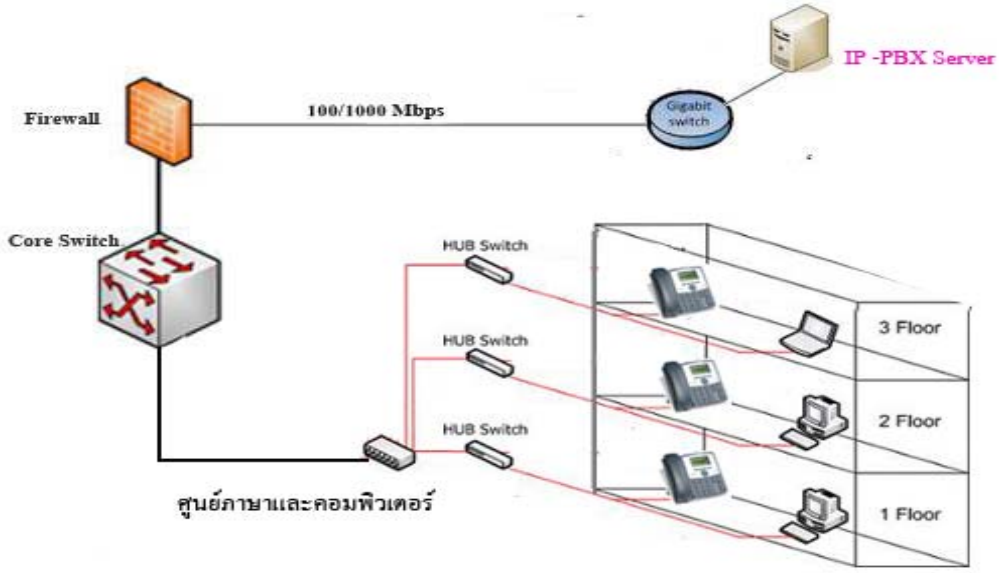
รูปที่ 3.5 แผนผังระบบโทรศัพท์ผ่านอินเทอร์เน็ต อาคารเฉลิมพระเกียรติ 60 พรรษามหาวชิราลงกรณ

จากรูปที่ 3.5 โทรศัพท์ผ่านอินเทอร์เน็ต อาคารเฉลิมพระเกียรติ 60 พรรษามหาวชิราลงกรณ เป็นอาคารเรียนรวม มีจำนวน 7 ชั้น มีหน่วยงานภายในอยู่ 3 ชั้น ซึ่งมีการใช้งานโทรศัพท์ VoIP จำนวน 6 เครื่อง



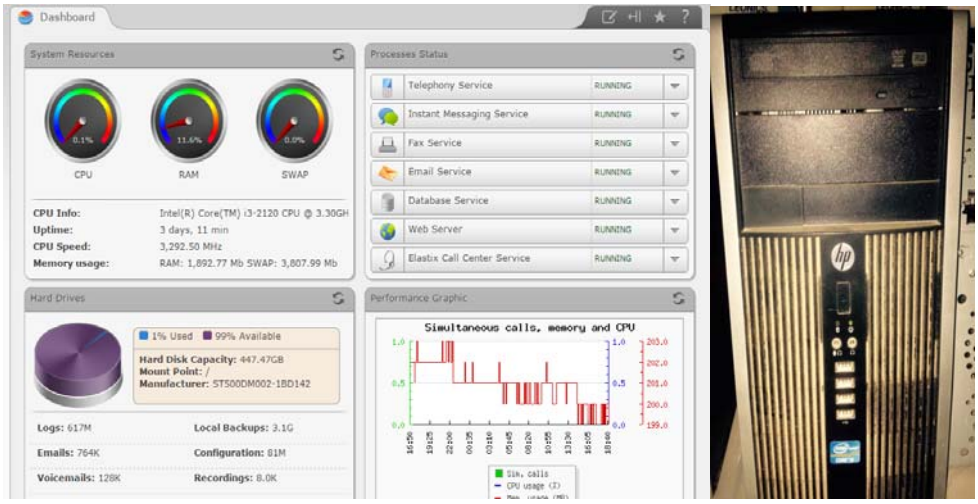
รูปที่ 3.6 แผนผังระบบโทรศัพท์ผ่านอินเทอร์เน็ต คณะพยาบาลศาสตร์

จากรูปที่ 3.6 ระบบโทรศัพท์ผ่านอินเทอร์เน็ต คณะพยาบาลศาสตร์ เป็นอาคารเรียนที่อยู่ห่างจาก Server เป็นระยะห่างประมาณ 1 กิโลเมตร เป็นอาคารเรียนจำนวน 5 ชั้น มีการใช้งานโทรศัพท์ VoIP จำนวน 4 เครื่อง



รูปที่ 3.7 แผนผังระบบโทรศัพท์ผ่านอินเทอร์เน็ต ศูนย์ภาษาและคอมพิวเตอร์

จากรูปที่ 3.7 ระบบโทรศัพท์ผ่านอินเทอร์เน็ต ศูนย์ภาษาและคอมพิวเตอร์ เป็นอาคารเรียนจำนวน 4 ชั้น มีหน่วยในอยู่ชั้น 1 และชั้น 2 มาการใช้งานโทรศัพท์ VoIP จำนวน 6 เครื่อง



รูปที่ 3.8 Server IP-PBX

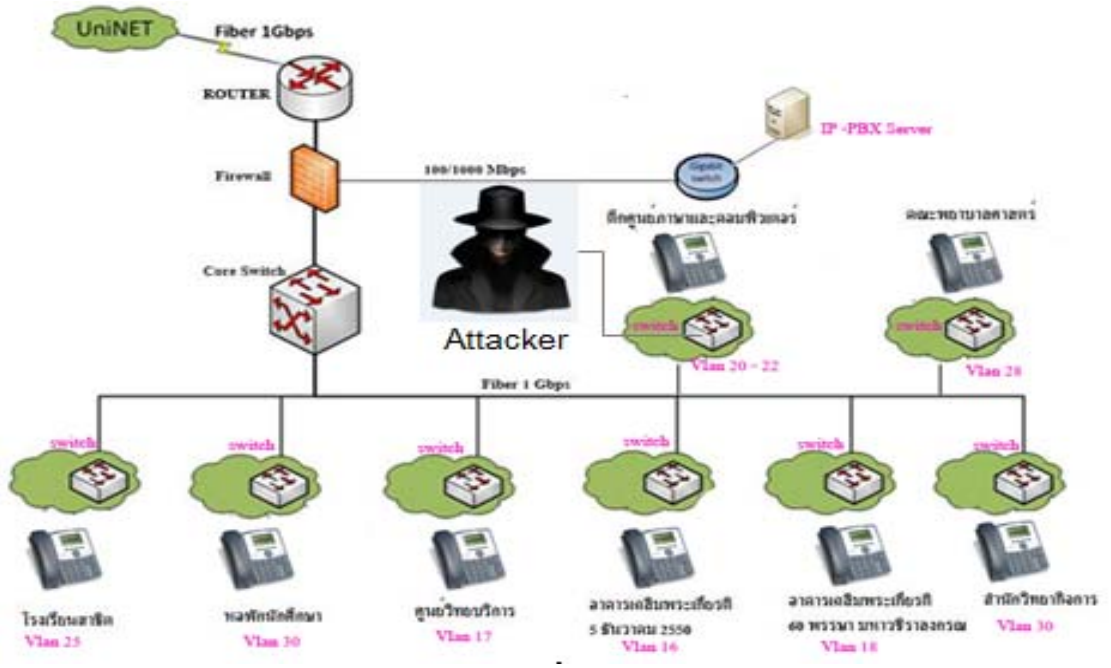
จากรูปที่ 3.8 เครื่องแม่ข่าย Server IP-PBX ชุดซอฟต์แวร์ Elastix v.2.3.0 ที่ให้บริการโทรศัพท์ผ่านอินเทอร์เน็ต เครื่องแม่ข่าย (Server): Intel(R) Core (TM) i3-2120 CPU @ 3.30 GHz Memory of RAM 4.00 GB Hard disk Memory 500 GB 10/100 Mbps Ethernet interface card

รูปที่ 3.9 เครื่องโทรศัพท์ IP Phone Cisco 303

เครื่องโทรศัพท์ IP Phone Cisco 303 จากรูปที่ 3.9 เป็นเครื่องใช้เป็นโทรศัพท์สำหรับสื่อสาร ซึ่งมีจำนวน 60 เครื่องซึ่งเป็นรุ่นเดียวกันทั้งหมดภายในมหาวิทยาลัยราชภัฏร้อยเอ็ด

3.2.2 การประเมินปัญหาด้านความมั่นคงของระบบ VoIP มหาวิทยาลัยราชภัฏร้อยเอ็ด

การประเมินปัญหาด้านความมั่นคงจะทำการทดสอบบนเครือข่ายบนระบบโทรศัพท์จริง โดยจะมี เครื่องผู้จู่โจม (Attacker) ก็ทำการติดตั้งเครื่องมือสำหรับการจู่โจมต่างๆ ที่ต้องใช้และเชื่อมต่อเข้ากับ Switch ตัวเดียวกัน โดยจะทำการจู่โจม จากศูนย์ภาษาและคอมพิวเตอร์ไปยังอาคารเฉลิม-พระเกียรติ 60 พรรษามหาวชิราลงกรณ และจู่โจมจากศูนย์ภาษาและคอมพิวเตอร์ไปยังอาคาร 80 พรรษา 5 ธันวาคม พ.ศ. 2550 ดังรูปที่ 3.10



รูปที่ 3.10 โครงสร้างการจู่โจมด้านความมั่นคง

จากรูปที่ 3.10 เป็นการประเมินปัญหาด้วนความมั่นคงโดยจะทำการทดลองบนเครือข่ายจากสถานการณ์จริงที่อยู่ภายใต้สภาพแวดล้อมที่เราสามารถกำหนดได้ ซึ่งเป็นจู่โจม (Attacker)

เทคนิคการจู่โจมสำหรับการประเมินปัญหาด้านความมั่นคง

อุปกรณ์ที่ใช้ในการประเมินความมั่นคง อุปกรณ์ เครื่องแม่ข่าย (Server): Intel(R) Core (TM) i3-2120 CPU @ 3.30 GHz Memory of RAM 4.00 GB Hard disk Memory 500 GB 10/100 Mbps Ethernet interface card เครื่อง VoIP Hardphone : Cisco IP Phone 303

เครื่องผู้จู่โจม (Attacker): ระบบปฏิบัติการ Microsoft Windows 7 Intel(R) Core (TM) i3-2120 CPU @ 3.30 GHz Memory of RAM 6.00 GB Hard disk Memory 500 GB 10/100 Mbps Ethernet interface card Switch L2: D-Link des-1024d 16-Port

ซอฟต์แวร์ที่ใช้ในการประเมินความมั่นคง ชุดซอฟต์แวร์ VoIP ที่ใช้ในการประเมินปัญหาด้านความมั่นคง Asterisk เป็น IP-PBX Server ได้แก่ Elastix 2.0.3

ซอฟต์แวร์สำหรับการจู่โจม Cain & Abel v4.9.4, Wireshark v1.4.7, Backtrack 4 สำหรับวิธีการจู่โจมที่เลือกใช้ เป็นเทคนิคการจู่โจมที่มีการโจมตีบนโพรโทคอลหลักของระบบ VoIP คือ SIP และ RTP เทคนิคการจู่โจมที่เลือกใช้ ได้แก่ SIP Flooding Attack เพื่อให้ปฏิเสธการบริการ MITM Attack เพื่อดักฟังการสนทนา และ Cancel/Bye Attack เพื่อทำให้การสื่อสารล้มเหลว ซึ่งขั้นตอนและวิธีการจู่โจมที่ได้กล่าวมานั้นจะมีวิธีการที่แตกต่างกัน ดังต่อไปนี้

2.1 การจู่โจมด้วย SIP Flooding Attacks

การจู่โจมด้วยวิธี SIP Flooding Attack เพื่อให้ปฏิเสธการบริการ Denial of Service (DoS) สามารถส่งผลกระทบหลายด้านต่อ IP-PBX Server ไม่ว่าจะเป็นคุณภาพการให้บริการ การทำงานของหน่วยประมวลผลกลาง (CPU) ในการประเมินจึงต้องพิจารณาตัวชี้วัด ดังนี้

1) การทำงานของหน่วยประมวลผลกลาง (CPU) โดยทำการประเมินร้อยละของการทำงานทั้งหมดของหน่วยประมวลผลกลางและการฟื้นตัวหลังการจู่โจม

2) ปฏิเสธการให้บริการหรือไม่ในขณะที่ทำการจู่โจมหน่วยประมวลผลกลางและหน่วยความจำมีการทำงานเพิ่มสูงขึ้นผิดปกติ จนไม่สามารถประมวลผลคำสั่งอื่นในขณะนั้น ทำให้ไม่สามารถให้บริการเครื่องลูกข่ายในขณะนั้นได้จากรูปที่ 3.11

```
top - 13:18:18 up 4 days,  2:34,  1 user,  load average: 8.62, 21.37, 16.01
Tasks: 161 total,   1 running, 160 sleeping,   0 stopped,   0 zombie
Cpu(s):  0.0%us,  0.0%sy,  0.0%ni, 99.8%id,  0.0%wa,  0.2%hi,  0.0%si,  0.0%st
Mem:   1938200k total,  1438860k used,   499340k free,   159052k buffers
Swap:  3899384k total,        0k used,  3899384k free,   615640k cached

  PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
    1 root      15   0  2172  648  556 S  0.0  0.0   0:00.95 init
```

รูปที่ 3.11 ภาพการทำงาน CPU

จากรูปที่ 3.11 เป็นการเข้าไปเครื่อง Server โดยทำการตรวจการทำงานของ CPU ก่อนมีการจู่โจม จากรูปการทำงานของ CPU ทำงานปกติ

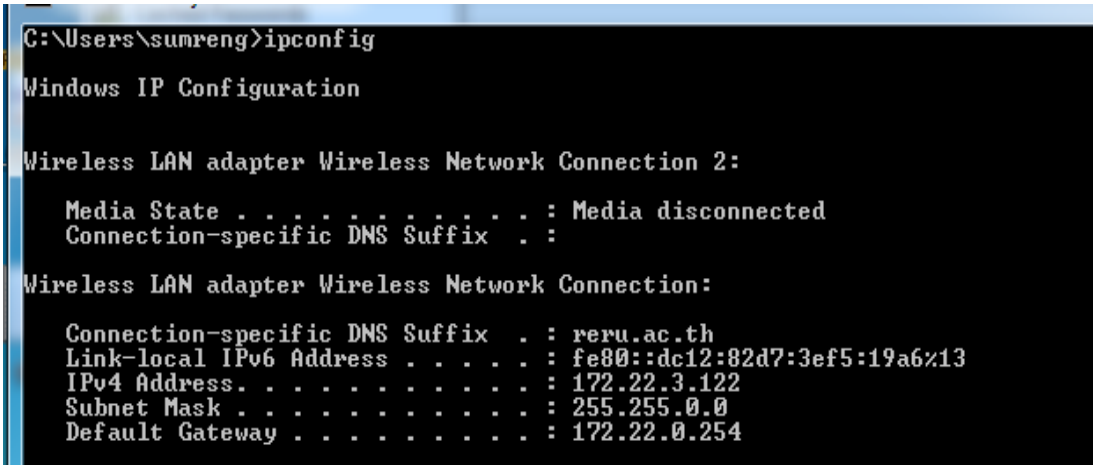
```
root@bt:/pentest/voip/inviteflood# ./inviteflood eth0 1145 192.168.10.140 192.168.10.140 100
0000000

inviteflood - Version 2.0
              June 09, 2006

source IPv4 addr:port   = 172.22.64.222:9
dest   IPv4 addr:port   = 192.168.10.140:5060
targeted UA             = 1145@192.168.10.140

Flooding destination with 1000000000 packets
sent: 3182517
exiting...
```

รูปที่ 3.12 ภาพการจู่โจม โดยใช้ back track

จากรูปที่ 3.12 เราจะทำการเปิดโปรแกรม Backtrack ขึ้นมาใช้งาน เพื่อจะทำการจู่โจม โดยจะการพิมพ์ pentest/VoIP/inviteflood กด enter ต่อด้วย./inviteflood eth0 (การ์ดที่เราใช้อินเทอร์เน็ต) 1145 (หมายเลยโทรศัพท์) 192.168.10.140 (เครื่อง Server) 192.168.10.140 ตามด้วยจำนวนครั้งของแพ็กเกตที่เราจะจู่โจม

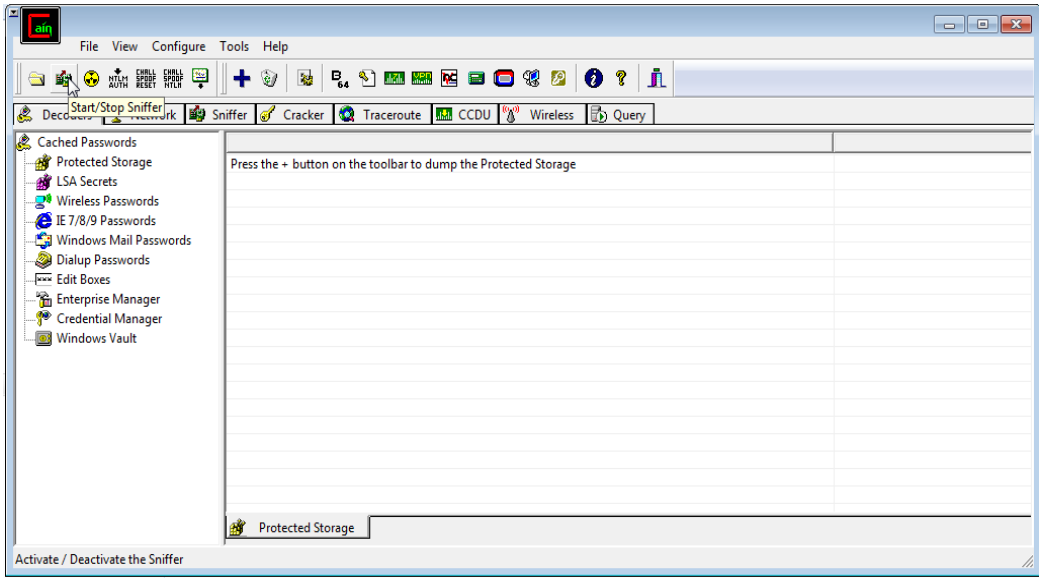
2.2 การจู่โจมด้วย MITM Attack

เป็นการจู่โจมเพื่อดักฟังเสียงการสนทนาของเหยื่อขณะทำการสนทนากัน ทดสอบโดยใช้ Cain&Abel ทำการแทรกแซงการสื่อสารและดักจับเสียงการสนทนาของเหยื่อโดยทำการจู่โจมระบบโทรศัพท์ภายในมหาวิทยาลัยราชภัฏร้อยเอ็ด แล้วเก็บรวบรวมผลจาก Cain&Abel ซึ่งลักษณะข้อมูลที่ถูกดักจับได้จะถูกบันทึกในรูปแบบของไฟล์ .mp3 และหลังจากนั้นทำการเปิดฟังเสียงที่บันทึกไว้ว่าเสียงที่ได้ยินนั้นเป็นอย่างไร ดูผลลัพธ์ที่เกิดขึ้นจากรูปที่ 3.14 และรูปที่ 3.15



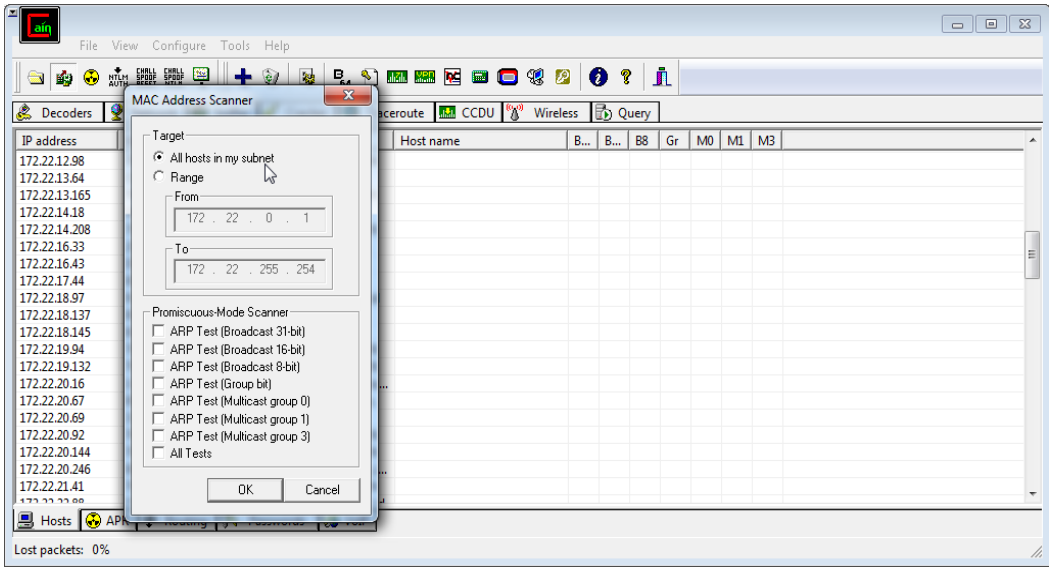
รูปที่ 3.13 การตรวจสอบ IP

จากรูปที่ 3.13 จะทำการตรวจสอบ IP ภายในเครื่องที่เราใช้งานเพื่อจะได้รู้ว่า IP อยู่ในช่วงไหน โดยวิธีการการเข้า cmd กด enter เมื่อเข้ามาแล้วพิมพ์ IPconfig กด enter

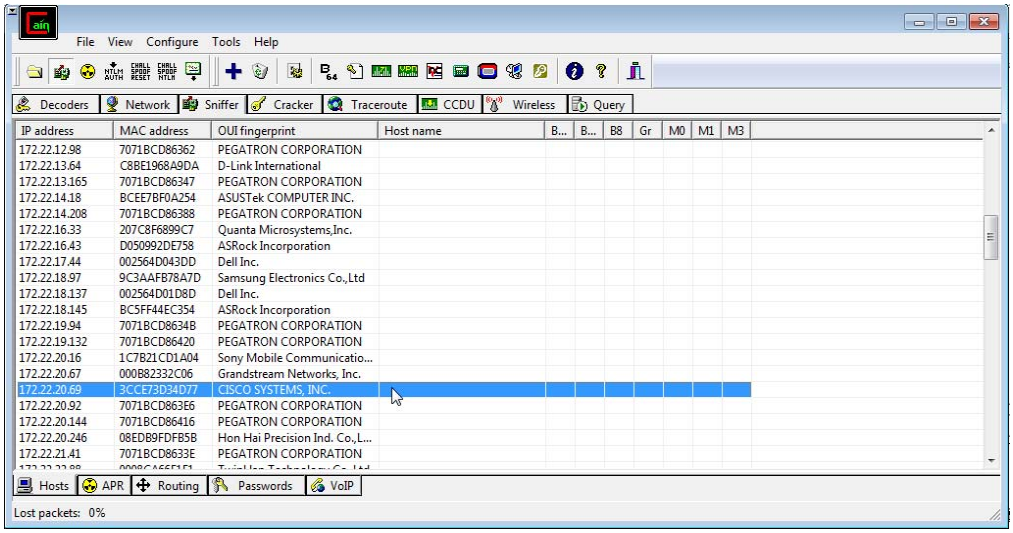


รูปที่ 3.14 หน้าตาโปรแกรม Cain & Abel

จากรูปที่ 3.14 เมื่อทำการเปิดโปรแกรม Cain & Abel ก็กด start sniffer เพื่อดักจับแพ็กเกจทั้งหมดที่วิ่งอยู่ในเครือข่าย หลังจากนั้นก็เลือก Sniffer > Hosts แล้วคลิกขวาบนพื้นที่ว่าง เลือก Scan MAC Addresses จากรูปที่ 3.15

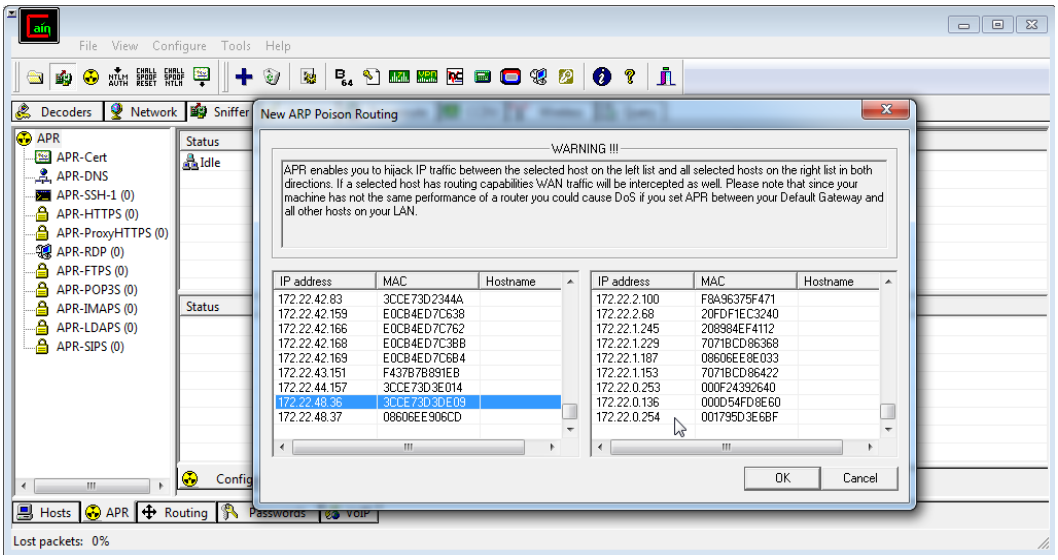


รูปที่ 3.15 เลือก Range ที่จะทำการ Scan



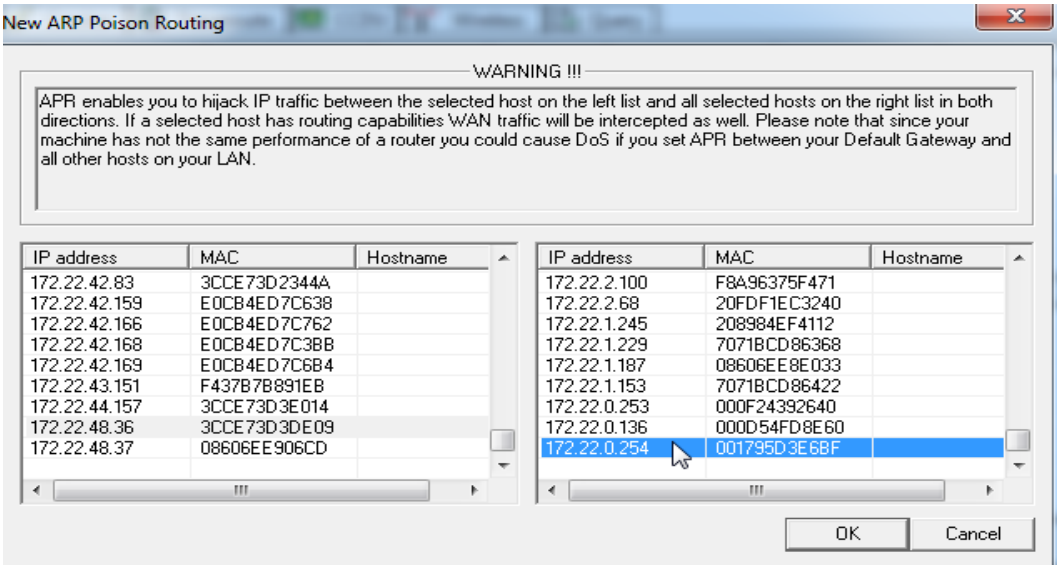
รูปที่ 3.16 เลือก IP ที่แสดงว่าเป็น VoIP

จากรูปที่ 3.16 เมื่อได้ Range หมายเลขของ IP ก็กด ok จากนั้นจะทำการวิเคราะห์หมายเลข IP ที่เป็นของระบบโทรศัพท์ VoIP เมื่อได้แล้วก็คลิกเลือก จะปรากฏดังรูปที่ 3.17



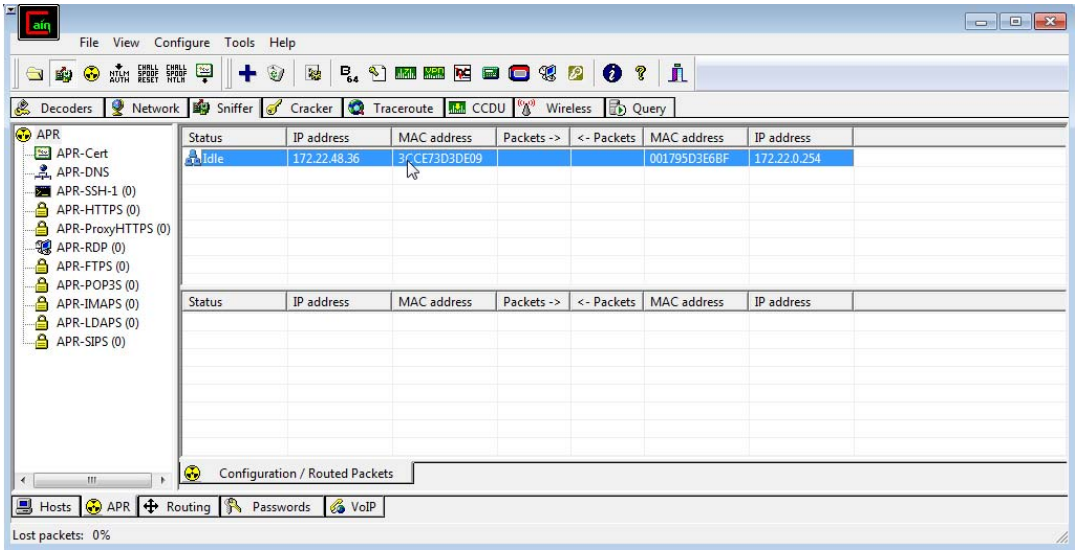
รูปที่ 3.17 การเลือก IP ที่จะทำการจู่โจม

จากรูปที่ 3.17 เมื่อได้ IP ที่เป็นโทรศัพท์ VoIP ก็ไปที่ ARP จากนั้นคลิกตรงพื้นที่ว่างในโปรแกรมและกดเครื่องหมาย + จะแสดงหน้าต่างขึ้นมา ด้านซ้ายเป็น IP ของโทรศัพท์ VoIP ด้านขวาเป็นเกตเวย์ในการวิ่งของระบบเครือข่าย ซึ่งในที่นี้เป็น 172.22.0.254 ทำการเลือกเสร็จ กด OK จากรูปที่ 3.18

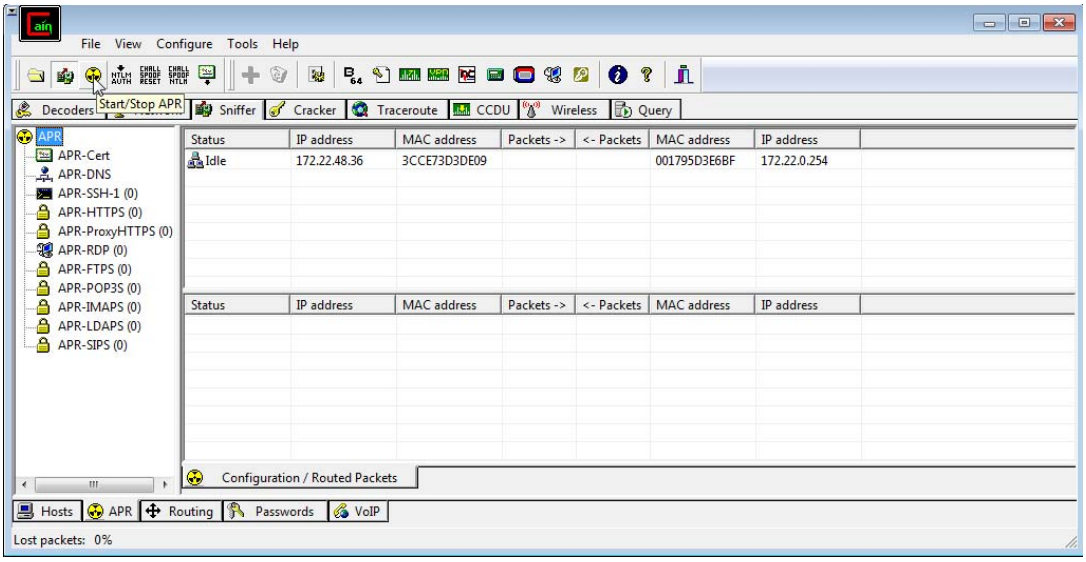


รูปที่ 3.18 การเลือก IP เกตเวย์

จากรูปที่ 3.18 เราจะทำเลือกเกตเวย์ หลังจากนั้นก็กด ok จะปรากฏดังรูปที่ 3.19

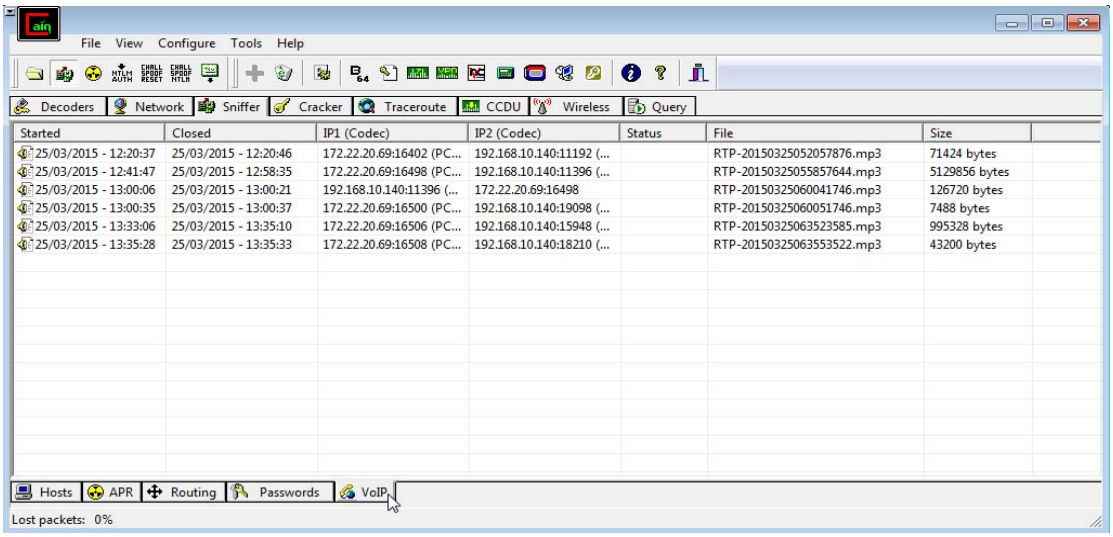


รูปที่ 3.19 เตรียมการจู่โจม



รูปที่ 3.20 ทำการจู่โจม

จากรูปที่ 3.20 เป็นการจู่โจม MITM (ดักฟังเสียงการสนทนา) กด start/stop ARP จากนั้นก็ทำการทดลองโทรไปหาเบอร์อื่นๆ และเริ่มการสนทนา จากนั้นวางสาย

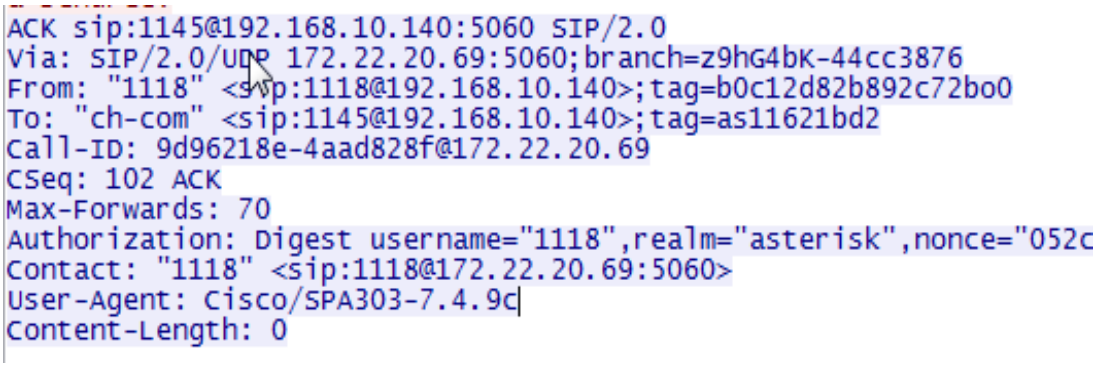


รูปที่ 3.21 ไฟล์เสียงที่ดักจับ

จากรูปที่ 3.21 เป็นไฟล์ที่ดักจับได้โดยไปที่ Sniffer และเลือก VoIP ก็จะเห็นไฟล์เสียงที่ทำการสนทนาโดยมีการบันทึกไว้เป็นไฟล์ .MP3

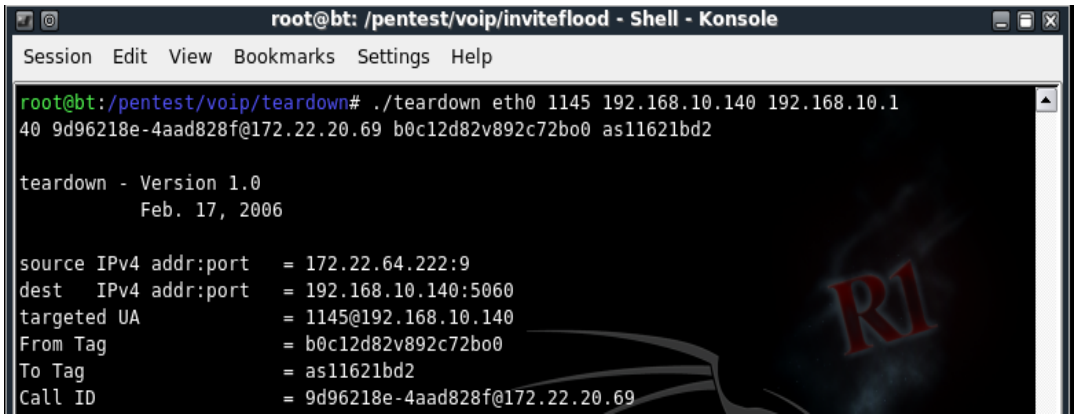
2.3 การจู่โจมด้วย Cancel/Bye Attack

Cancel/Bye Attack เป็นการจู่โจมเพื่อขัดขวางหรือทำให้การสื่อสารล้มเหลว ขั้นตอนแรกทำการแทรกแซงการสื่อสาร ใช้ Wireshark ดักจับค่า SIP OK Response ของเหยื่อ ดังรูปที่ 3.24



รูปที่ 3.22 ดักจับค่า SIP OK Response

จากรูปที่ 3.22 เมื่อทำการจับข้อมูล Call-ID ได้มาแล้วก็จะทำการจู่โจมด้วย Backtrack 4 โดยจะใช้ข้อมูลใน SIP OK Response เพื่อทำการจู่โจมดังรูปที่ 3.23



รูปที่ 3.23 การจู่โจมแบบ Cancel/Bye Attack

จากรูปที่ 3.23 เราจะทำการเปิดโปรแกรม Backtrack ขึ้นมาใช้งาน เพื่อจะทำการจู่โจม โดยจะการพิมพ์ pentest/VoIP/teardown กด enter ต่อด้วย ./teardown eth0 (การ์ดที่เราใช้อินเทอร์เน็ต) 1145 (หมายเลยโทรศัพท์) 192.168.10.140 (เครื่อง Server) 192.168.10.140 ตามด้วย Call-ID ที่ได้มาแล้วทำการจู่โจม

3.2.3 การประเมินคุณภาพเสียงของระบบ VoIP มหาวิทยาลัยราชภัฏร้อยเอ็ด

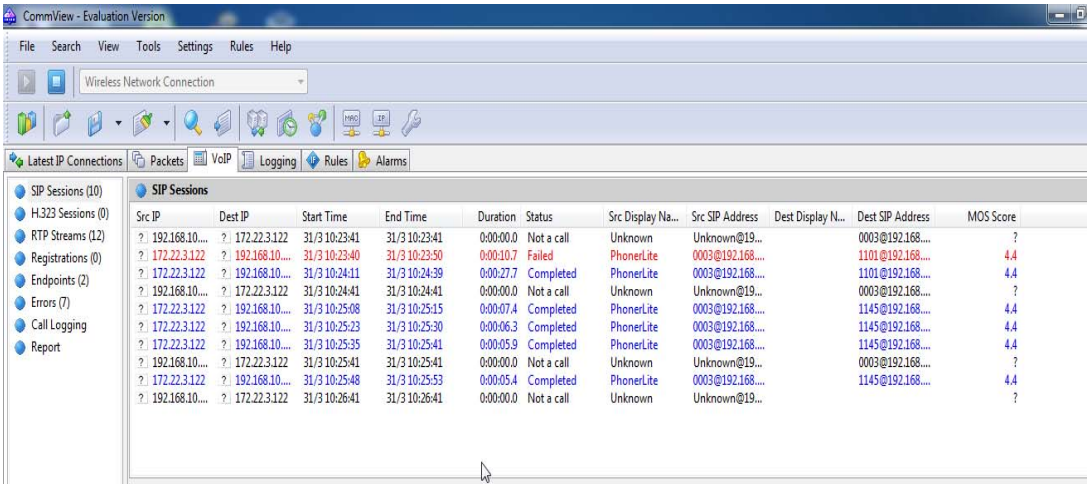
ในการให้บริการโทรศัพท์ผ่านเครือข่ายอินเทอร์เน็ตจำเป็นต้องคำนึงถึงคุณภาพการให้บริการแก่ผู้ใช้งาน ไม่ใช่แค่ด้านความมั่นคงเพียงอย่างเดียว เพราะโทรศัพท์ผ่านเครือข่ายอินเทอร์เน็ตที่ดีต้องมีคุณสมบัติครบทุกด้าน ดังนั้นงานวิจัยนี้จึงได้ทำวัดคุณภาพเสียงของชุดซอฟต์แวร์ VoIP เพื่อแสดงข้อมูลคุณภาพเสียง เพื่อให้ทราบข้อมูลคุณภาพเสียงของ VoIP ว่าความมั่นคงจะมีผลกระทบต่อคุณภาพการให้บริการหรือไม่ โดยใช้เครื่องมือวัดคุณภาพเสียงที่เรียกว่า E-Model จะทำการเลือกจุดที่มีความเสี่ยงมากที่สุด โดยจากการศึกษาโครงสร้างจึงได้พบอยู่ 3 จุด คือ อาคารวิทยกิจทีปังกร คณะพยาบาลศาสตร์ ศูนย์ภาษาและคอมพิวเตอร์ และอาคารเฉลิมพระเกียรติ 60 พรรษามหาวชิราลงกรณ อาคาร 80 พรรษา 5 ธันวาคม พ.ศ. 2550 จะมีความเสี่ยงด้านคุณภาพสุดเพราะเป็นหน่วยงานภายในมหาวิทยาลัย

สำหรับการวัดคุณภาพเสียงงานวิจัยได้ทำการเลือกช่วงเวลาออกเป็น 2 ช่วงคือ ช่วงเวลาที่มีการใช้งานเครือข่ายมากที่สุด (Peak Time) เวลาตั้งแต่ 15.00 น. ถึง 16.00 น. และช่วงเวลาที่มีการใช้งานเครือข่ายน้อยที่สุด (Off Peak Time) เวลาตั้งแต่ 6.00 น. ถึง 7.00 น. โดยการพิจารณาจากกราฟแสดงค่า Traffic การใช้งานอินเทอร์เน็ตของมหาวิทยาลัยราชภัฏร้อยเอ็ดดังรูปที่ 3.26 ซึ่งการวัดคุณภาพเสียงทั้ง 2 ช่วงเวลา จะวัดช่วงเวลาละ 30 ครั้งเป็นเวลาหนึ่งสัปดาห์ และคำนวณหาค่าเฉลี่ยที่ระดับความเชื่อมั่น 95% ซึ่งผลการวัดเสียงที่มีคุณภาพที่สามารถยอมรับได้ ค่า R-factor ต้องไม่น้อยกว่า 70 หรือ ค่า MOS ต้องไม่น้อยกว่า 3.5 ตามเกณฑ์ กสทช [26]

การวัดผลจากระบบจริง อาจมีปัญหาคือ 1) การควบคุมสิ่งแวดล้อมที่ยากและหลากหลาย ผลอาจมีทั้งดีมากและไม่ดี ในสภาพแวดล้อมที่เปลี่ยนแปลง แต่ในงานวิจัยนี้ ได้เลือกทดสอบในสภาพแวดล้อมและช่วงเวลาที่ให้ผลลัพธ์เลวร้ายที่สุด ซึ่งหากได้ผลการประเมินไม่ผ่านแสดงว่า คุณภาพอาจไม่ผ่านเกณฑ์ในการใช้งานของ User ในบางเวลา หรือบางสถานที่ในมหาวิทยาลัยราชภัฏร้อยเอ็ด แต่หากการประเมินผ่านแสดงให้รู้ว่าในช่วงเวลาที่เลวร้ายที่สุด การให้บริการคุณภาพเสียงก็เป็นปกติ 2) การทดสอบในระบบจริง อาจสร้างความเสียหายให้กับระบบ หรือรบกวนระบบจริงได้ และอาจไม่มีอำนาจในการเข้าทดสอบจริง แต่งานวิจัยนี้ ผู้วิจัยได้ขออนุญาตไปยังผู้ที่มีอำนาจแล้ว และผลดำเนินการสุดท้ายจะเป็นประโยชน์ต่อ มหาวิทยาลัยราชภัฏร้อยเอ็ด จึงได้รับอนุญาต โดยการทดสอบจู่โจม อาจมีการขัดจังหวะการทำงานของระบบ VoIP บางส่วน ก็ได้แจ้งให้ผู้ใช้ทราบล่วงหน้า และควบคุมไม่ให้การขัดจังหวะสร้างความเสียหายในการใช้งานขององค์กรนานเกินไป และสำหรับการโจมตีทาง Security ที่ส่งผลต่อเหยื่อ เช่น การดักฟังเสียง หรือการตัดสาย ก็ไม่ได้ใช้ผู้ใช้ทั่วไปจริงๆเป็นเหยื่อ แต่ใช้เหยื่อที่ถูกสร้างขึ้นมาเพื่อการทดสอบโดยเฉพาะ

ขั้นตอนการวัดคุณภาพเสียง

เราจะเปิดโปรแกรม Commview ขึ้นมาเพื่อจับข้อมูลการโทรเข้าโทรออกของคู่สาย เพื่อตรวจสอบค่า MOS Score สำหรับการวัดคุณภาพเสียงจะทำการวัดเป็นจำนวน 30 ครั้ง เก็บรวบรวมค่า R-factor ที่ได้จากโปรแกรม Commview เพื่อหาค่าเฉลี่ยและ Error Bar ที่ระดับค่าความเชื่อมั่น 95% พร้อมกับเปรียบเทียบตามตาราง Recommendation P.800



รูปที่ 3.24 การวัดคุณภาพเสียง

จากรูปที่ 3.24 เป็นการแสดงค่าการโทรของโทรศัพท์ VoIP ที่มีการโทรเข้าโทรออกพร้อมกับการจับวัดคุณภาพเสียงที่ให้บริการ

ตารางที่ 3.1 Listening Quality Scale

MOS	Quality of Voice Rating	User Satisfaction
5 (4.34)	Best	Very satisfied
4 4.03)	High	Satisfied
3 (3.60)	Medium	Some users dissatisfied
2 (3.10)	Low	Many users dissatisfied
1(2.58)	Poor	Nearly all users dissatisfied

จากตารางที่ 3.1 เป็นการเปรียบเทียบ ค่า MOS ซึ่งจะนำค่าที่วัดได้จากโปรแกรม Commview เพื่อหาค่าเฉลี่ยและ Error Bar ที่ระดับค่าความเชื่อมั่น 95% จากสูตรสมการ (2)

$$R = 93.2 - I_d - I_{e-eff}$$

I_d = ค่าความบกพร่องที่เกิดจากความล้าช้า (Delay)

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

3.3 เสนอแนวคิดการปรับปรุง

จากผลการวิเคราะห์และประเมินปัญหาความมั่นคงเบื้องต้น อีกทั้งมีงานวิจัยของ [1] ที่สนับสนุนว่าการใช้งาน Elastix ที่มหาวิทยาลัยราชภัฏร้อยเอ็ดใช้เป็นระบบ VoIP อยู่ในปัจจุบันนั้น ยังไม่มีความมั่นคงและปลอดภัยที่ดีพอ ผู้วิจัยจึงได้เสนอแนวคิดในการแก้ปัญหาด้านความมั่นคง ด้วยการนำเอา ISANBox v.3.0 มาใช้แทน Elastix ที่เป็นระบบ VoIP เดิมของมหาวิทยาลัยราชภัฏร้อยเอ็ด เพราะจากงานวิจัยของ [1,22] ได้มีการทดสอบและวิจัยออกมาแล้วว่า ISANBox สามารถแก้ปัญหาด้านความมั่นคงเหล่านี้ได้รวมป้องกันเทคนิคการจู่โจมที่ผู้วิจัยนำมาใช้ในการประเมินปัญหาด้านความมั่นคงอีกด้วย และหลังจากมีการเปลี่ยนระบบ VoIP ใหม่จะทำการประเมินประสิทธิภาพด้านความมั่นคงและคุณภาพเสียงในสภาพแวดล้อมการใช้งานจริงบนเครือข่าย

หลังจากใช้ ISANBox มีการทดสอบประสิทธิภาพความมั่นคงและคุณภาพ เพราะจากงานวิจัยเดิม การทดลองด้านความมั่นคงและคุณภาพ ISANBox ผ่านทั้งสอง โดยมีความแข็งแกร่งต่อต้านการโจมตีแบบต่างๆ ได้ และไม่ก่อให้เกิดปัญหากับคุณภาพ แม้มี overhead ด้าน Security จนคุณภาพลดลงบ้าง แต่การทดลองของผู้วิจัย ISANBox ทำแค่บนเครือข่าย Test-bed ขนาดเล็กที่มีการควบคุมสภาพแวดล้อมไว้อย่างดี ซึ่งอาจมีสภาพแวดล้อม ไม่เหมือนกับเครือข่ายจริงๆ ที่ไม่มีการควบคุมและมีการปะปนของ data traffic กับ voice traffic จนอาจเกิด cross traffic มารบกวนในช่วงเวลาที่มีการใช้งานเครือข่ายในองค์กรสูงๆ อย่างมหาวิทยาลัยราชภัฏร้อยเอ็ด

จึงต้องมีการตรวจสอบประเมินคุณภาพของระบบ VoIP ในงานวิจัยนี้ จะทำการติดตั้ง ISANBox 3.0 โดยคุณสมบัติเครื่อง Server เดียวกันกับ Elastix ซึ่งจะใช้การตรวจสอบประเมินในเครือข่ายจริง โดยวัดค่าจากจุดที่มีการใช้งานเครือข่ายสูงสุด มีจำนวน hop ของคู่สนทนาในการใช้ VoIP มากสุด และทดสอบในเวลาที่มีความคับคั่งในเครือข่ายสูงที่สุด

3.4 ประเมินประสิทธิภาพด้านความมั่นคงและคุณภาพเสียงหลังการปรับปรุง

ภายหลังจากที่มีการเสนอแนวคิดการปรับปรุงปัญหาด้านความมั่นคงระบบ VoIP ของมหาวิทยาลัยราชภัฏร้อยเอ็ด จึงต้องมีการประเมินประสิทธิภาพความมั่นคงของระบบเครือข่าย VoIP ตัวใหม่เพื่อให้ได้ผลที่เป็นรูปธรรมในระบบเครือข่าย VoIP ที่ใช้งานจริงของมหาวิทยาลัยราชภัฏร้อยเอ็ด โดยจะประเมิน ดังนี้

ด้านความมั่นคงกับระบบ VoIP ตัวใหม่ของมหาวิทยาลัยราชภัฏร้อยเอ็ด ซึ่งจะการทำการประเมินด้านความมั่นคง ด้วยเทคนิคเดิมที่ได้ทำการจู่โจมกับระบบ VoIP ตัวเก่า ได้แก่

1. SIP Flooding Attack เพื่อให้ปฏิเสธการบริการ
2. MITM Attack เพื่อดักฟังการสนทนา และ
3. Cancel/Bye Attack เพื่อทำให้การสื่อสารล้มเหลว

ด้านคุณภาพเสียงของระบบ VoIP ตัวใหม่จะทำการวัดคุณภาพเสียงโดยใช้การวัดคุณภาพเสียงแบบ E-Model เป็นจำนวน 30 ครั้ง เก็บรวบรวมค่า R-factor ที่ได้จากโปรแกรม Commview เพื่อหาค่าเฉลี่ยและ Error Bar ที่ระดับค่าความเชื่อมั่น 95% ซึ่งเหมือนกับการวัดคุณภาพเสียงระบบ VoIP เดิมของมหาวิทยาลัยราชภัฏร้อยเอ็ด ว่าโดยมาตรฐานสำหรับการให้บริการเสียงผ่านการให้บริการอินเทอร์เน็ต ให้เป็นไปตามข้อเสนอแนะของสหภาพโทรคมนาคมระหว่างประเทศ ITU-T Recommendation G.107: The E-model

บทที่ 4

ผลการวิจัย

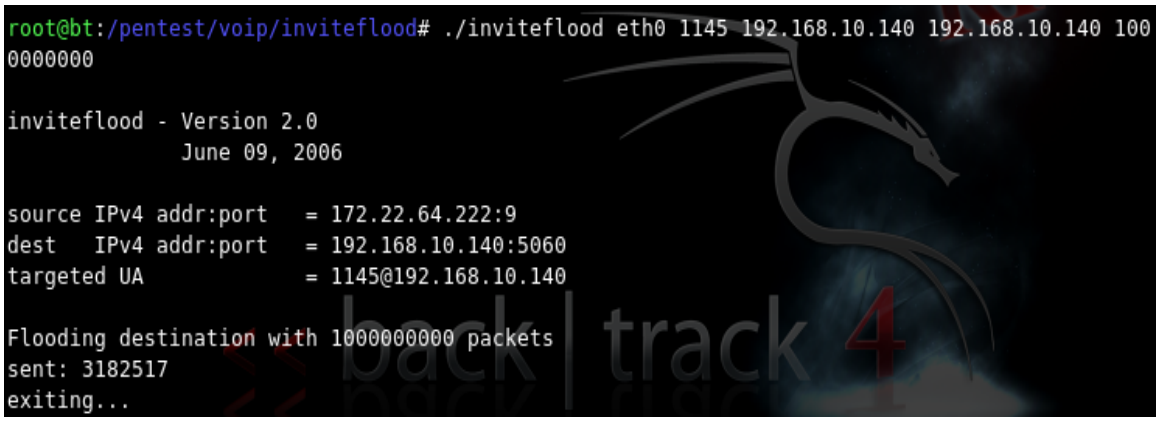
การประเมินและปรับปรุงระบบโทรศัพท์ผ่านอินเทอร์เน็ตของมหาวิทยาลัยราชภัฏร้อยเอ็ด ผลการวิจัยสามารถแบ่งออกเป็น 3 ส่วนหลักดังนี้

1. ผลการประเมินปัญหาด้านความมั่นคงของระบบโทรศัพท์ผ่านอินเทอร์เน็ต มหาวิทยาลัยราชภัฏร้อยเอ็ด
2. ผลการวัดคุณภาพเสียงของระบบโทรศัพท์ผ่านอินเทอร์เน็ต มหาวิทยาลัยราชภัฏร้อยเอ็ด
3. ผลการทดสอบประสิทธิภาพด้านความมั่นคงและคุณภาพเสียงหลังการปรับปรุงระบบโทรศัพท์ผ่านอินเทอร์เน็ต มหาวิทยาลัยราชภัฏร้อยเอ็ด

4.1 ผลการประเมินปัญหาด้านความมั่นคงของระบบโทรศัพท์ผ่านอินเทอร์เน็ต มหาวิทยาลัยราชภัฏร้อยเอ็ด

งานวิจัยได้เลือกใช้เทคนิคการจู่โจม 3 เทคนิค คือ 1. SIP Flooding Attack เพื่อให้ปฏิเสธการบริการ 2. MITM Attack เพื่อดักฟังการสนทนา 3. Cancel/Bye Attack เพื่อทำให้การสื่อสารล้มเหลว ซึ่งเทคนิคเหล่านี้เป็นเทคนิคการจู่โจมที่ทำการโจมตีบนโพรโทคอลหลักของระบบ VoIP SIP และ RTP ซึ่งมีผลกระทบทั้งด้าน Security และ Quality จากการประเมินด้านความมั่นคงได้ผล ดังนี้

4.1.1 ผลการจู่โจม SIP Flooding Attack เพื่อให้ปฏิเสธการบริการ



รูปที่ 4.1 ขณะทำการจู่โจม SIP Flooding Attack

จากรูปที่ 4.1 การจู่โจมด้วย SIP Flooding Attack เป็นการจู่โจมเพื่อให้ IP-PBX Server ล่มจนไม่ได้สามารถให้บริการได้ โดยการจู่โจมงานวิจัยใช้ BackTrack 4 เพื่อทำการยิง INVITE Message

จำนวนมากไปยัง IP-PBX Serverจนทำให้การทำงานของหน่วยประมวลผลกลาง (CPU) และหน่วยความจำ (Memory) เพิ่มสูงจนไม่สามารถประมวลผลคำสั่งอื่นๆ ที่เข้ามายัง IP-PBX Server ได้ จนเป็นสาเหตุทำให้ไม่สามารถให้บริการโทรศัพท์ผ่านอินเทอร์เน็ตได้ โดยก่อนการจู่โจมได้ทำการเปิดหน้าตาการทำงานของหน่วยประมวลผลกลาง และหน่วยความจำของ IP-PBX Server เพื่อดูการทำงานการปกติ ดังรูปที่ 4.2

```
top - 13:18:18 up 4 days,  2:34,  1 user,  load average: 8.62, 21.37, 16.01
Tasks: 161 total,   1 running, 160 sleeping,   0 stopped,   0 zombie
Cpu(s):  0.0%us,  0.0%sy,  0.0%ni, 99.8%id,  0.0%wa,  0.2%hi,  0.0%si,  0.0%
Mem:   1938200k total,  1438860k used,   499340k free,   159052k buffers
Swap:  3899384k total,        0k used,  3899384k free,   615640k cached

  PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
    1 root      15   0  2172  648  556 S  0.0  0.0   0:00.95 init
    2 root      RT  -5     0    0    0 S  0.0  0.0   0:00.01 migration/0
    3 root      34  19     0    0    0 S  0.0  0.0   0:00.00 ksoftirqd/0
    4 root      RT  -5     0    0    0 S  0.0  0.0   0:00.00 watchdog/0
```

รูปที่ 4.2 การทำงานของ CPU และ Memory ก่อนจู่โจม

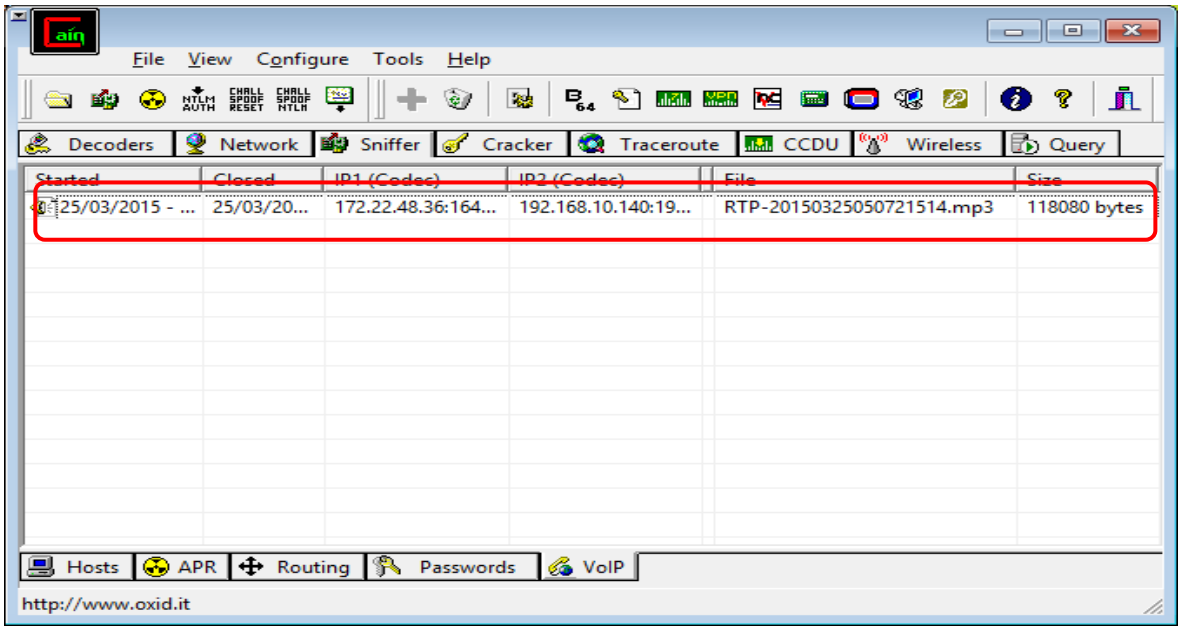
เมื่อทำการจู่โจมไปยัง IP-PBX Server การทำงานของหน่วยประมวลผลกลาง และหน่วยความจำ มีการทำงานเพิ่มขึ้นมากอย่างเห็นได้ชัดดัง จากนั้นทดลองใช้ IP Phone ทำการลงทะเบียนไปยัง IP-PBX เพื่อขอใช้บริการ จากผลการทดลองที่ได้คือ IP-PBX Server ไม่มีการตอบสนองใดๆ ต่อ IP Phone ที่ร้องขอการลงทะเบียนขณะมีการจู่โจมดังรูปที่ 4.3

```
top - 13:19:36 up 4 days,  2:35,  1 user,  load average: 85.85, 39.95, 22.74
Tasks: 161 total,   2 running, 159 sleeping,   0 stopped,   0 zombie
Cpu(s): 64.4%us, 21.4%sy,  0.0%ni,  7.1%id,  0.8%wa,  0.7%hi,  5.5%si,  0.0%s
Mem:   1938200k total,  1612708k used,   325492k free,   159076k buffers
Swap:  3899384k total,        0k used,  3899384k free,   628932k cached

  PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
 3229 asterisk  15   0  852m 460m  10m S 229.6 24.3  13:23.67 asterisk
 3453 asterisk  25   0 16576  12m 1852 R 43.6  0.6   8:12.18 op_server.pl
 3342 asterisk  15   0 26588 6652 2060 S 30.3  0.3   1:41.28 dialerd
```

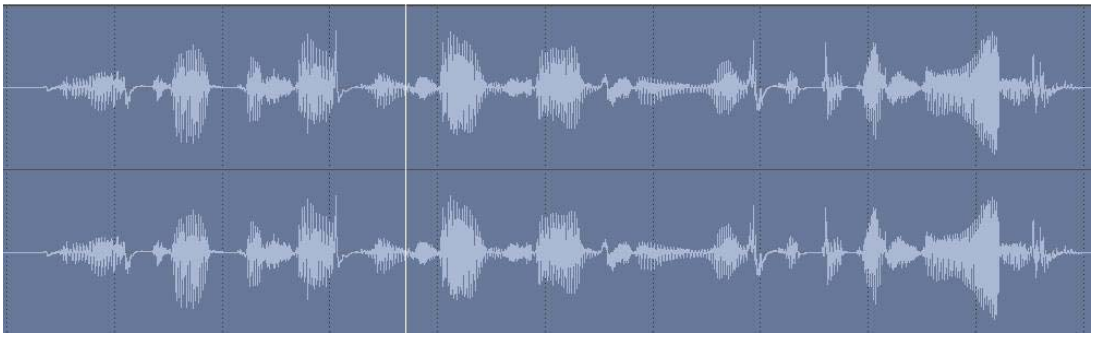
รูปที่ 4.3 การทำงานของ CPU และ Memory ขณะถูกจู่โจม

4.1.2 ผลการจู่โจมด้วย MITM Attack เพื่อดักฟังการสนทนา

สำหรับการจู่โจมด้วย MITM Attack จะแบ่งเป็นการจู่โจม เพื่อดักฟังเสียงการสนทนาของคู่สายที่สื่อสารบนระบบโทรศัพท์ผ่านอินเทอร์เน็ต โดยเครื่องมือที่ใช้คือ Cain & Able โดยโปรแกรมสามารถบันทึกเป็นไฟล์ MP3 ซึ่งสามารถเปิดฟังเสียงได้ทันที ดังรูปที่ 4.4



รูปที่ 4.4 ดักฟังเสียงการสนทนา

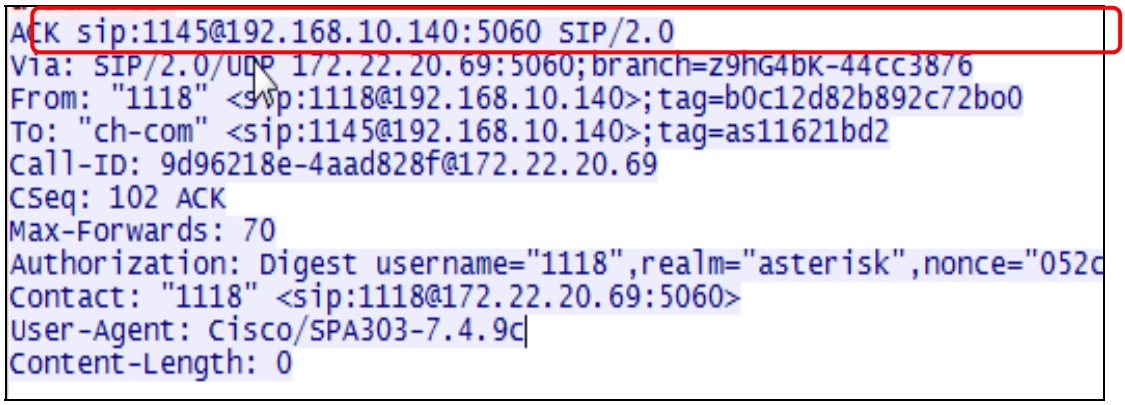


รูปที่ 4.5 เสียงการสนทนา

จากรูปที่ 4.5 เป็นไฟล์เสียงทำการเปิดขึ้นมาเพื่อฟังการสนทนาระหว่างคู่สายที่ดักจับการสนทนาดักจับได้จาก Elastix ระบบโทรศัพท์ผ่านอินเทอร์เน็ตภายในมหาวิทยาลัยราชภัฏร้อยเอ็ด

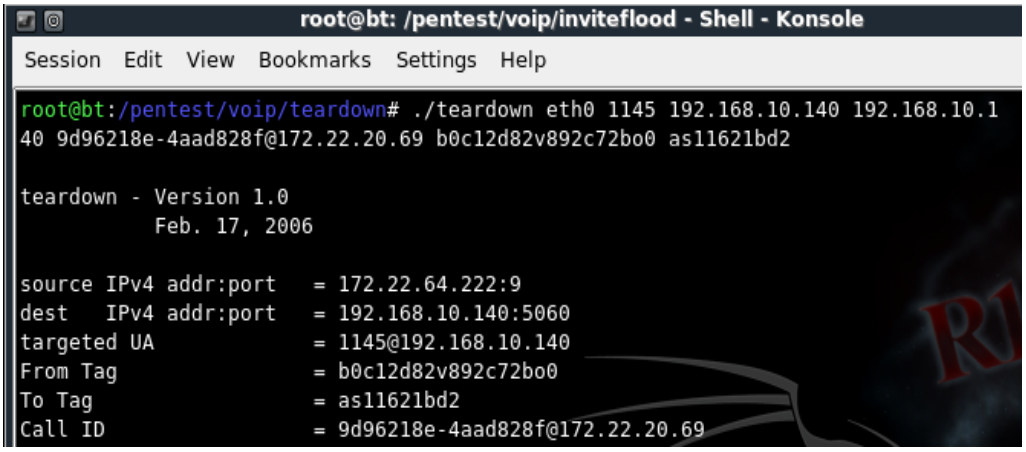
4.1.3 ผลการจู่โจมด้วย Cancel/Bye Attack เพื่อทำให้การสื่อสารล้มเหลว

การจู่โจมด้วย Cancel/Bye Attack เป็นการยิงแพ็คเกจเพื่อตัดสายการสนทนาของคู่สายที่สื่อสารบนระบบโทรศัพท์ผ่านอินเทอร์เน็ต โดยการจู่โจมจะทำการใช้ Cain & Able เพื่อแทรกกลางการสื่อสารระหว่างเครื่องเหยื่อที่กำลังสนทนา จากนั้นใช้ Wireshark ดักจับแพ็คเกจ ของโพรโทคอล SIP เพื่อให้ได้ SIP OK Response จากนั้นทำการค้นหา ACK Message หรือ Call- ID ดังรูปที่ 4.5 ซึ่งภายใน ACK Message จะใช้เป็นข้อมูลสำหรับการจู่โจม



รูปที่ 4.6 ACK Message

เมื่อได้ข้อมูลที่ต้องการในขั้นตอนการจู่โจมจะใช้ BackTrack 4 ยิงแพ็คเกจไปตัดสายการสนทนาของเหยื่อโดยเราจะนำ ACK Message หรือ Call- ID มาพิมพ์เพิ่ม ดังรูปที่ 4.6 จากผลการทดลองสามารถตัดสายของเหยื่อที่กำลังสนทนาลงได้โดยสมบูรณ์



รูปที่ 4.7 การจู่โจมด้วย Cancel/Bye Attack

จากรูปที่ 4.6 จะทำการ รันโปรแกรม Back Track 4 โดยจะเข้าไปในpentest/VoIP/teardown กด enter และพิมพ์ ./teardown eth0 ตามด้วยหมายเลขเบอร์ IP Phone และเครื่อง IP-PBX Server ตามด้วย Call-ID เมื่อทำการ enter จะสามารถตัดสายการสนทนาของคู่สายได้สมบูรณ์

ตารางที่ 4.1 สรุปผลการประเมินปัญหาด้านความมั่นคงของระบบ VoIP มหาวิทยาลัยราชภัฏร้อยเอ็ด

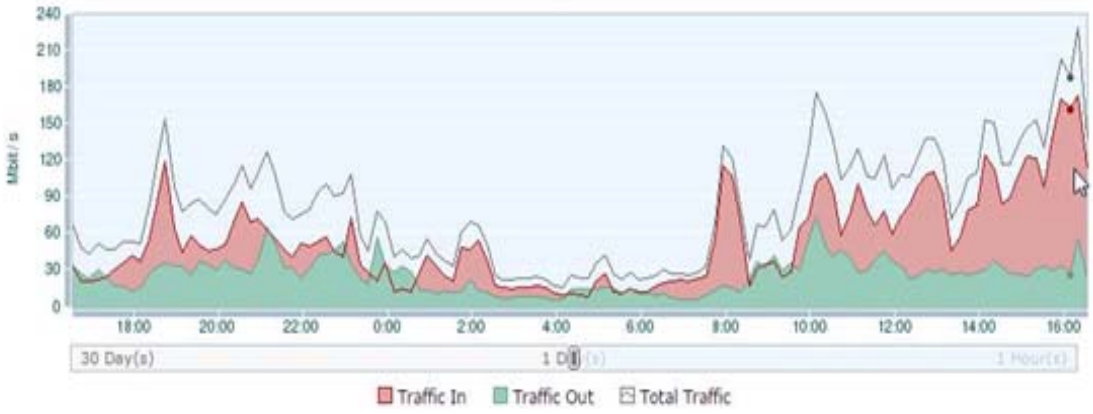
เทคนิคการจู่โจม	ผลการจู่โจม
1. SIP Flooding Attack เพื่อให้ปฏิเสธการบริการ	จู่โจมสำเร็จ
2. MITM Attack เพื่อดักชื่อผู้ใช้งาน/รหัสผ่านและเสียงฟังการสนทนา	จู่โจมสำเร็จ
3. Cancel/Bye Attack เพื่อทำให้การสื่อสารล้มเหลว	จู่โจมสำเร็จ

จากตารางที่ 4.1 เป็นการสรุปผลการประเมินปัญหาด้านความมั่นคงของระบบ VoIP มหาวิทยาลัยราชภัฏร้อยเอ็ด จากที่งานวิจัยได้เลือกใช้เทคนิคการจู่โจม 3 เทคนิค ซึ่งผลคือทั้ง 3 เทคนิค สามารถการจู่โจม IP-PBX Server ที่ใช้เป็นระบบโทรศัพท์ผ่านอินเทอร์เน็ตของมหาวิทยาลัยราชภัฏร้อยเอ็ด ได้สำเร็จ โดยเทคนิคการจู่โจมทั้ง 3 นี้เป็นการจู่โจมที่ส่งผลต่อร้ายแรงโดยตรงต่อระบบโทรศัพท์ผ่านอินเทอร์เน็ต อีกทั้งสามารถทำการจู่โจมได้ง่ายโดยที่ผู้จู่โจมไม่จำเป็นต้องมีความรู้ด้านการเทคนิคการจู่โจมมากนักก็สามารถทำได้ ซึ่งมันเป็นสิ่งที่ส่งผลเสียร้ายแรงต่อระบบความมั่นคงของระบบ ซึ่งจากผลที่ได้ทำให้สามารถสรุปได้ว่าระบบโทรศัพท์ผ่านอินเทอร์เน็ตของมหาวิทยาลัยราชภัฏร้อยเอ็ดที่ใช้อยู่ในปัจจุบันไม่มีความมั่นคงที่ดีพอ สุ่มเสี่ยงต่อการโดนจู่โจมระบบจากผู้ไม่หวังดี

4.2 ผลการวัดคุณภาพเสียงของระบบโทรศัพท์ผ่านอินเทอร์เน็ต มหาวิทยาลัยราชภัฏร้อยเอ็ด

งานวิจัยได้ทำการวัดคุณภาพเสียงบนเครือข่ายจริงของระบบโทรศัพท์ผ่านอินเทอร์เน็ต มหาวิทยาลัยราชภัฏร้อยเอ็ด เช่นเดียวกันการประเมินปัญหาด้านความมั่นคง โดยเลือกใช้วิธีการวัดคุณภาพเสียงระบบโทรศัพท์ผ่านอินเทอร์เน็ตที่เรียกว่า E-Model ซึ่งเป็นแบบจำลองหรือเครื่องมือในการวิเคราะห์คุณภาพเสียงที่ใช้สำหรับการวางแผนเครือข่าย ซึ่งผลลัพธ์พื้นฐานของ E-Model คือการคำนวณค่าจาก R-factor โดยใช้โปรแกรม Commview ซึ่งสามารถวัดค่า R-factor ออกมาได้ทันทีและสามารถแปลงไปเป็นค่า MOS เพื่อเป็นค่าที่ดูได้ง่ายและเข้าใจสำหรับการวัดคุณภาพเสียงงานวิจัยได้ทำการเลือกช่วงเวลาออกเป็น 2 ช่วงคือ ช่วงเวลาที่มีการใช้งานเครือข่ายมากที่สุด (Peak Time) เวลาตั้งแต่ 15.00 น. ถึง 16.00 น. และช่วงเวลาที่มีการใช้งานเครือข่ายน้อยที่สุด (Off Peak Time) เวลาตั้งแต่ 6.00 น. ถึง 7.00 น. โดยการพิจารณาจากกราฟแสดงค่า Traffic ดังรูปที่ 4.7 การใช้งานอินเทอร์เน็ตของมหาวิทยาลัยราชภัฏร้อยเอ็ด การวัดคุณภาพเสียง ทั้ง 2 ช่วงเวลา จะวัดช่วงเวลาละ 30 ครั้งและคำนวณหาค่าเฉลี่ยที่ระดับความเชื่อมั่น 95% ซึ่งผลการวัดเสียงที่มีคุณภาพที่สามารถยอมรับได้คือ ค่า R-factor ต้องไม่น้อยกว่า 70

จากการทดลองการวัดคุณภาพเสียงของระบบโทรศัพท์ผ่านอินเทอร์เน็ต มหาวิทยาลัยราชภัฏร้อยเอ็ด ได้ผลดังตารางที่ 4.2



รูปที่ 4.7 กราฟแสดงค่า Traffic

ตารางที่ 4.2 ผลการวัดคุณภาพเสียงของระบบโทรศัพท์ผ่านอินเทอร์เน็ต มหาวิทยาลัยราชภัฏร้อยเอ็ด

ช่วงเวลา	จำนวนครั้ง	R-factor	MOS
15.00-16.00 น.(Peak Time)	30	92.75±0.92	5
6.00-7.00 น.(off peak time)	30	93.20±1.08	5

จากตารางที่ 4.2 เป็นค่าเฉลี่ยของ R-factor ที่ได้จากการวัดคุณภาพเสียงของระบบโทรศัพท์ผ่านอินเทอร์เน็ต มหาวิทยาลัยราชภัฏร้อยเอ็ด ทั้ง 2 ช่วงเวลา คือ ช่วงเวลา 15.00-16.00 น.(Peak Time) ได้ค่าเฉลี่ย R-factor = 92.75±0.92 และ 6.00-7.00 น.(Off Peak Time) ได้ค่าเฉลี่ย R-factor = 93.20±1.08 ผลของค่า R-factor ของทั้ง 2 ช่วงเวลาเมื่อเปรียบเทียบแล้ว ช่วงเวลา Off Peak Time จะค่าเฉลี่ย R-factor จะได้คุณภาพเสียงที่ดีกว่า ช่วงเวลา Peak Time เล็กน้อย แต่ภาพรวมของคุณภาพเสียงของระบบโทรศัพท์ผ่านอินเทอร์เน็ต มหาวิทยาลัยราชภัฏร้อยเอ็ด ที่ได้จากการวัดทั้ง 2 ช่วงเวลาอยู่ในเกณฑ์เสียงที่มีคุณภาพคือค่าเฉลี่ย R-factor ไม่น้อยกว่า 70 สรุปได้ว่าทั้ง 2 ช่วงเวลา คือ Peak Time และ Off Peak Time ได้คุณภาพเสียง ดีมาก

4.3 ผลการทดสอบประสิทธิภาพด้านความมั่นคงและคุณภาพเสียงหลังการปรับปรุงระบบโทรศัพท์ผ่านอินเทอร์เน็ตมหาวิทยาลัยราชภัฏร้อยเอ็ด

จากผลการประเมินปัญหาด้านความมั่นคงของระบบโทรศัพท์ผ่านอินเทอร์เน็ตมหาวิทยาลัยราชภัฏร้อยเอ็ด แสดงให้เห็นว่าระบบของระบบโทรศัพท์ผ่านอินเทอร์เน็ตที่ใช้อยู่ในปัจจุบันนั้นไม่มีความมั่นคงที่ดีอีกทั้งมีหลายงานวิจัยที่สนับสนุนว่า Elastix ที่มหาวิทยาลัยราชภัฏร้อยเอ็ดใช้อยู่ไม่มีความมั่นคง รวมทั้ง IP Phone ของมหาวิทยาลัยราชภัฏร้อยเอ็ด ไม่สนับสนุนซึ่งเป็น Cisco IP Phone 303 นั้นไม่รองรับการเข้ารหัส SRTP ไม่อาจทำ Security ได้ ถึงจะใช้ระบบ ISANBox 3.0 เป็น IP-PBX server จึงมีข้อเสนอแนะให้มหาวิทยาลัยราชภัฏร้อยเอ็ด ทำเปลี่ยนโทรศัพท์ IP Phone ที่รองรับการ

เข้ารหัส SRTP และเพื่อให้การทดสอบดำเนินต่อได้ จึงเสนอให้แก้โดยใช้ PhonerLite 2.17 ซึ่งเป็น Softphone ในการทดสอบ และใช้โทรศัพท์ IP Phone Linksys SPA942 จาก Lab ISAN มาทำการทดสอบ งานวิจัยจึงได้เสนอแนวคิดการปรับปรุงระบบโทรศัพท์ผ่านอินเทอร์เน็ตของมหาวิทยาลัยราชภัฏร้อยเอ็ด โดยการเปลี่ยน IP-PBX Server จาก Elastix มาเป็น ISANBox.A Version 3.0 [22] ซึ่งเป็น IP-PBX Server ที่มีความมั่นคงสามารถป้องการจู่โจมได้หลายรูปแบบและรวมไปถึงเทคนิคการจู่โจมที่งานวิจัยใช้ในการประเมินปัญหาด้านความมั่นคงในข้างต้นอีกด้วย แต่อย่างไรก็ตามเมื่อมีการปรับปรุงระบบโทรศัพท์ผ่านอินเทอร์เน็ตมหาวิทยาลัยราชภัฏร้อยเอ็ดใหม่ จึงจำเป็นต้องมีการทดสอบประสิทธิด้านความมั่นคงและวัดคุณภาพเสียงของระบบโทรศัพท์ผ่านอินเทอร์เน็ตบนเครือข่ายการใช้งานจริงอีกครั้ง เพื่อใช้เป็นข้อมูลสนับสนุนความน่าเชื่อถือในการใช้ระบบโทรศัพท์ผ่านอินเทอร์เน็ตของมหาวิทยาลัยราชภัฏร้อยเอ็ดว่าเป็นระบบที่มีความมั่นคงและน่าเชื่อถือ จากผลการการทดสอบประสิทธิด้านความมั่นคงและวัดคุณภาพเสียงของระบบโทรศัพท์ผ่านอินเทอร์เน็ต ของมหาวิทยาลัยราชภัฏร้อยเอ็ดหลังการปรับปรุง ได้ผลดัง ตารางที่ 4.3 และ ตารางที่ 4.4

ตารางที่ 4.3 ผลการประเมินประสิทธิภาพด้านความมั่นคงหลังการปรับปรุงระบบใหม่

เทคนิคการจู่โจม	**ผลการจู่โจม**
1. SIP Flooding Attack เพื่อให้ปฏิเสธการบริการ	จู่โจมไม่สำเสร็จ
2. MITM Attack เพื่อดักชื่อผู้ใช้งาน/รหัสผ่านและเสียงฟังการสนทนา	จู่โจมไม่สำเร็จ
3. Cancel/Bye Attack เพื่อทำให้การสื่อสารล้มเหลว	จู่โจมไม่สำเร็จ

ตารางที่ 4.4 ผลการวัดคุณภาพเสียงระบบโทรศัพท์ผ่านอินเทอร์เน็ตหลังการปรับปรุงระบบใหม่

ช่วงเวลา	**จำนวนครั้ง**	R-factor	MOS
15.00-16.00 น.(peak time)	30	91.40±1.74	5
6.00-7.00 น.(off peak time)	30	92.30±1.27	5

จากตารางที่ 4.3 คือผลการทดสอบประสิทธิภาพด้านความมั่นคงระบบโทรศัพท์ผ่านอินเทอร์เน็ตหลังการปรับปรุงใหม่ โดยทำการเปลี่ยน IP-PBX Server จาก Elastix มาเป็นการใช้ ISANBox.A แทน ซึ่งผลจากการทดสอบประสิทธิภาพพบว่าเทคนิคการจู่โจมทั้ง 3 เทคนิค ที่ใช้สำหรับการประเมินปัญหาด้านความมั่นคงในข้างต้น ไม่สามารถทำการจู่โจมระบบโทรศัพท์ได้ ซึ่งผลที่ได้เป็นข้อยืนยันได้ว่า ISANBox.A เป็นชุดซอฟต์แวร์ VoIP สำหรับการใช้เป็น IP-PBX Server ที่มีความมั่นคงและมีความน่าเชื่อถือ สำหรับการใช้เป็นระบบโทรศัพท์ผ่านอินเทอร์เน็ตของมหาวิทยาลัยราชภัฏร้อยเอ็ด และจากตารางที่ 4.4 คือผลการวัดคุณภาพเสียงของระบบโทรศัพท์ผ่านอินเทอร์เน็ตหลังการปรับปรุงใหม่ โดยทำการวัด 2 ช่วงเวลาเช่นเดิมเพื่อหาผลของความมั่นคงที่เพิ่มขึ้นส่งผลต่อคุณภาพเสียงของระบบโทรศัพท์ผ่านอินเทอร์เน็ตหรือไม่ ผลที่ได้คือ ช่วงเวลาการใช้งานเครือข่ายสูงสุด (Peak Time) ได้ค่าเฉลี่ย R-factor = 91.40±1.74 และช่วงเวลาการใช้งานเครือข่ายน้อยสุด (Off Peak Time)

ได้ค่าเฉลี่ย R-factor = 92.30±1.27 หลังการปรับปรุง ค่าคุณภาพลดลงเล็กน้อย จากตารางที่ 4.2 กับตารางที่ 4.3 แสดงให้เห็นว่าช่วงเวลาการใช้งานเครือข่ายน้อยสุดได้คุณภาพที่ดีกว่าช่วงเวลาการใช้งานเครือข่ายสูงสุดเล็กน้อย แต่ผลคุณภาพเสียงโดยรวมอยู่ในเกณฑ์เสียงที่มีคุณภาพคือค่าเฉลี่ย R-factor ไม่น้อยกว่า 70 และเมื่อเปรียบเทียบกับผลการวัดคุณภาพจากตารางที่ 4.2 ก่อนมีการปรับปรุงโทรศัพท์ผ่านอินเทอร์เน็ตใหม่อยู่ในเกณฑ์คุณภาพเสียงที่ใกล้เคียงกัน เมื่อเทียบกับ MOS มีคุณภาพอยู่ในระดับดีมาก

จะเห็นได้ชัดว่า bandwidth และสภาพเครือข่ายภายในของมหาวิทยาลัยราชภัฏร้อยเอ็ดสามารถรองรับ overhead ของ ISANBox.A version 3.0 ได้อย่างไม่มีปัญหาต่อคุณภาพเสียงที่ให้บริการ

บทที่ 5

สรุปผล อภิปรายผล และข้อเสนอแนะ

งานวิจัยได้นำเสนอการประเมินปัญหาด้านความมั่นคงระบบโทรศัพท์ผ่านอินเทอร์เน็ต มหาวิทยาลัยราชภัฏร้อยเอ็ด โดยเลือกใช้เทคนิคการจู่โจม 3 เทคนิค ซึ่งเป็นเทคนิคที่สามารถจู่โจมได้ง่ายแต่ส่งผลเสียร้ายแรงต่อระบบโทรศัพท์ผ่านเครือข่ายอินเทอร์เน็ต ทำการการวัดคุณภาพเสียงเพื่อหาตรวจว่าเสียงที่ได้อยู่ในเกณฑ์คุณภาพหรือไม่ โดยใช้เครื่องมือการวัดที่เรียกว่า E-Model ทำการปรับปรุงโทรศัพท์ผ่านอินเทอร์เน็ต มหาวิทยาลัยราชภัฏร้อยเอ็ด และทำการทดสอบประสิทธิภาพด้านความมั่นคง วัดคุณภาพเสียงหลังการปรับปรุงใหม่

5.1 สรุปและอภิปรายผล

ปัจจุบันการติดต่อสื่อสารถือว่ามีความจำเป็นในชีวิตประจำวัน ซึ่งมีความรวดเร็วและมีประสิทธิภาพมากขึ้น ระบบโทรศัพท์อินเทอร์เน็ต เป็นการส่งผ่านข้อมูลเสียงผ่านทางระบบเครือข่ายข้อมูล หรือผ่านทางอินเทอร์เน็ต ซึ่งระบบโทรศัพท์ผ่านอินเทอร์เน็ต กำลังเป็นที่นิยมมาก เพราะสามารถพัฒนาและประยุกต์ใช้งานใหม่ๆได้ ช่วยประหยัดค่าใช้จ่ายในการติดต่อสื่อสารภายในองค์กร รวมถึงการเพิ่มประสิทธิภาพการทำงานขององค์กร ด้วยการเล็งเห็นถึงประโยชน์และความจำเป็น มหาวิทยาลัยราชภัฏร้อยเอ็ดจึงได้ทำการติดตั้งระบบโทรศัพท์ผ่านเครือข่ายอินเทอร์เน็ต ภายในมหาวิทยาลัยราชภัฏร้อยเอ็ด ใน ปี พ.ศ. 2554 เพื่อลดความยุ่งยากและต้นทุนการใช้งานและติดตั้งโทรศัพท์สาธารณะ แต่ทั้งนี้ระบบโทรศัพท์ผ่านอินเทอร์เน็ตที่ มหาวิทยาลัยราชภัฏใช้อยู่ในปัจจุบัน ยังไม่มีการศึกษาปัญหาทางด้านความมั่นคงและคุณภาพเสียงของระบบที่ให้บริการ โดยมีหลายงานวิจัยพบว่าปัญหาภัยคุกคามต่อระบบโทรศัพท์ผ่านอินเทอร์เน็ตนั้น มีอยู่หลากหลายและอาจจะส่งผลต่อระบบโทรศัพท์ผ่านอินเทอร์เน็ตภายในมหาวิยาลัยราชภัฏร้อยเอ็ดได้ ซึ่งการจู่โจมดังกล่าวได้แก่ การดักฟังเสียงที่สนทนา การตัดสายที่สนทนาด้วย Cancel/bye attacks การจู่โจมเครื่องด้วย SIP flooding

ดังนั้นการศึกษาค้นคว้าอิสระ จึงได้เสนอการประเมินปัญหาด้านความมั่นคง โดยเลือกใช้การจู่โจม 3 เทคนิคคือ SIP Flooding Attack, MITM Attack และ Cancel/Bye Attack ผลที่ได้คือทั้ง 3 เทคนิคสามารถจู่โจมระบบโทรศัพท์ผ่านอินเทอร์เน็ตของมหาวิทยาลัยราชภัฏร้อยเอ็ดได้ทั้งหมด ส่วนการวัดคุณภาพเสียงผลที่ได้คือเสียงที่ได้อยู่ในเกณฑ์ที่ยอมรับได้คือ ค่าเฉลี่ย R-factor ไม่น้อยกว่า 70 ทั้งในช่วงเวลาที่มีการใช้งานเครือข่ายสูงสุดและน้อยสุด ซึ่งเป็นไปตามมาตรฐานที่ กสทช. ใช้ในการวัดคุณภาพ Voice over Internet Protocol ที่ยอมรับได้

การปรับปรุงและประเมินระบบโทรศัพท์ผ่านอินเทอร์เน็ตหลังการปรับปรุง ได้เปลี่ยนมาเป็น ISANBox.A Version 3.0 ซึ่งผลจากการทดสอบประสิทธิภาพพบว่าเทคนิคการจู่โจมทั้ง 3 เทคนิคที่ใช้สำหรับการประเมินปัญหาด้านความมั่นคงในข้างต้น ไม่สามารถทำการจู่โจมระบบโทรศัพท์ได้ ซึ่งผลที่ได้เป็นข้อยืนยันได้ว่า ISANBox.A Version 3.0 เป็นชุดซอฟต์แวร์ VoIP สำหรับการใช้เป็น IP-PBX Server ที่มีความมั่นคง สำหรับการใช้เป็นระบบโทรศัพท์ผ่านอินเทอร์เน็ตของมหาวิทยาลัยราชภัฏ

ร้อยเอ็ด ผลคุณภาพเสียงโดยรวมอยู่ในเกณฑ์เสียงที่มีคุณภาพคือค่าเฉลี่ย R-factor ไม่น้อยกว่า 70 เกณฑ์คุณภาพเสียงที่ใกล้เคียงกัน เมื่อเทียบกับ MOS มีคุณภาพอยู่ในระดับดีมาก

5.2 ผลสัมฤทธิ์

1) ผลต่อกรณีศึกษา

ผลการประเมินปัญหาด้านความมั่นคงระบบโทรศัพท์ผ่านอินเทอร์เน็ตของมหาวิทยาลัยราชภัฏร้อยเอ็ด แสดงให้เห็นว่าระบบระบบโทรศัพท์ผ่านอินเทอร์เน็ตที่ใช้อยู่ปัจจุบันไม่มีความมั่นคงที่ดีพอ จึงได้มีการปรับปรุงระบบโทรศัพท์ผ่านอินเทอร์เน็ตใหม่ โดยการเปลี่ยน IP-PBX Server จากเดิมที่ใช้ Elastix มากเป็นการใช้ ISANBox.A Version 3.0 แทน เพื่อปรับปรุงประสิทธิภาพด้านความมั่นคงให้ดีขึ้นและทดสอบพบว่าคุณภาพดีมากไม่ตกจากเดิม

2) ได้ผลการทดสอบ ISANBox.A Version 3.0

ในเครือข่ายจริงของมหาวิทยาลัยราชภัฏร้อยเอ็ด ผลการทดลองประเมินด้านความมั่นคงของระบบโทรศัพท์ผ่านอินเทอร์เน็ตมหาวิทยาลัยราชภัฏร้อยเอ็ด โดยใช้ ISANBox 3.0 สามารถป้องกันการจู่โจมทั้ง 3 เทคนิคได้ คือ MITM Attack เพื่อดักฟังเสียงการสนทนา Cancel/Bye Attack เพื่อทำให้การสื่อสารล้มเหลว SIP Flooding Attack เพื่อให้ปฏิเสธการบริการ ซึ่งทั้ง 3 การจู่โจม ISANBox 3.0 สามารถป้องกันได้สำเร็จ ซึ่งยืนยันว่ามีประสิทธิภาพด้าน Security และoverhead ต่ำไม่ส่งผลต่อคุณภาพเสียงในการให้บริการ แม้เครือข่ายของมหาวิทยาลัยราชภัฏร้อยเอ็ด ไม่ได้มีการแยก VLAN หรือแยก Physical Network แต่ใช้ data traffic กับ Voice traffic ผสมกัน

3) ได้ตัวอย่างการทดสอบประเมินผลความมั่นคงและคุณภาพเสียง ที่นำไปใช้กับองค์กรอื่นได้

5.3 ข้อเสนอแนะและแนวทางการวิจัยต่อ

เทคนิคการจู่โจมที่เลือกใช้ประเมินปัญหาด้านความมั่นคงระบบโทรศัพท์ผ่านอินเทอร์เน็ตของมหาวิทยาลัยราชภัฏร้อยเอ็ด เนื่องจากเป็นวิธีที่ง่ายและไม่ซับซ้อนแฮกเกอร์มือสมัครเล่นทั่วไปก็สามารถใช้งานเทคนิคจู่โจมเหล่านี้ได้และส่งผลเสียร้ายแรงต่อระบบโดยตรง แต่อย่างไรก็ตามในปัจจุบันแฮกเกอร์ก็จะสรรหาวิธีการใหม่เพื่อมาโจมตีระบบโทรศัพท์ผ่านอินเทอร์เน็ตอยู่เสมอ จึงต้องมีการทำวิจัยเลือกความมั่นคงกันต่อไปเพื่อหาแนวทางป้องกันการโจมตีของแฮกเกอร์ต่อไปในอนาคต

เอกสารอ้างอิง

เอกสารอ้างอิง

[1] คธาวุฒิ จันบัวลา, สมนึก พ่วงพรพิทักษ์. การประเมินปัญหาด้านความมั่นคงของชุดซอฟต์แวร์โอเพนซอร์ซสำหรับโทรศัพท์ผ่านเครือข่ายอินเทอร์เน็ต. การประชุมวิชาการระดับชาติด้านคอมพิวเตอร์และเทคโนโลยีสารสนเทศ; 13 กุมภาพันธ์ 2555; เชียงใหม่.

[2] ปิยวัจน์ ค้าสบาย, สมนึก พ่วงพรพิทักษ์. การประเมินปัญหาด้านความมั่นคงของซอฟต์แวร์เสรีสำหรับโทรศัพท์ผ่านเครือข่ายไอพี. การประชุมวิชาการระดับชาติด้านคอมพิวเตอร์และเทคโนโลยีสารสนเทศ; 13-15 มกราคม 2553; จันทบุรี. หน้า 33-38

[3] ประดิษฐ์ วงษ์สกุล, ปิยะณัฐ สุยังกุล, สมนึก พ่วงพรพิทักษ์ ระบบให้บริการโทรศัพท์ผ่านอินเทอร์เน็ตแบบมั่งคงโดยการต่อยอดฟรีสวิตช์ การประชุมวิชาการระดับชาติด้านคอมพิวเตอร์และเทคโนโลยีสารสนเทศ; 12 มีนาคม 2555

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

[5] วิกิพีเดีย. Session_Initiation_Protocol. [Online]. 2015 [สืบค้นวันที่ 26 กรกฎาคม 2558]; https://th.wikipedia.org/wiki/Session_Initiation_Protocol

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

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

[8] Handley M, Jacobson V. Session Description Protocol (SDP). IETF, RFC 2327, April 1998.

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

[10] กิตติ เปรมพรวิพุธ. ศึกษาการในนำระบบ VoIP Over IP (VoIP) มาใช้ในมหาวิทยาลัยหอการค้าไทย. การศึกษาค้นคว้าด้วยตนเอง วท.ม. การจัดการเทคโนโลยีสารสนเทศและการสื่อสาร, มหาวิทยาลัยหอการค้าไทย, 2549.

[11] ชญาภา พงษ์วิชัย. การนำระบบการจัดการสื่อสารด้วยเทคโนโลยีระบบ Voice Over IP (VoIP) มาใช้งานภายในองค์กร. การศึกษาค้นคว้าด้วยตนเอง วท.ม. เทคโนโลยีอินเทอร์เน็ตและสารสนเทศ, มหาวิทยาลัยนเรศวร, 2552.

[12] ณัฐภัทร พงศ์พุทธางกูร. แนวทางการปรับปรุงและเพิ่มประสิทธิภาพการให้บริการ VoIP กรณีศึกษา บริษัท SSS จำกัด. การศึกษาค้นคว้าด้วยตนเอง บบ.ม. การจัดการโลจิสติกส์, มหาวิทยาลัยหอการค้าไทย, 2550.

[13] Asterisk. [online]. 2010 [สืบค้นวันที่ 15 มกราคม 2558]; http://www.asterisk.org.

[14] Elastix. [online]. 2011 [สืบค้นวันที่ 15 มกราคม 2558]; http://www.elastix.org.

[15] AsteriskNOW. [online]. 2010 [สืบค้นวันที่ 15 มกราคม 2558]; http://www.asterisk.org/downloads/asterisknow.

[16] Puangpronpitag S, Kasabai P, Chanbuala K, Wongsakul P. ISANBox. [online]. 23 May 2011 [สืบค้นวันที่ 15 มกราคม 2558]; http://www.isan.msu.ac.th/ISANBox.A

[17] Salsano S, Veltri L, Papalilo D. SIP security issues: the SIP authentication procedure and its processing load. Network, IEEE 2002; 16[6]: 38-44.

[18] 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]: 26-31.

[19] Methods for subjective determination of transmission quality. ITU-T, Recommendation P.800, June 1996.

[20] The E-model: a computational model for use in transmission planning. ITU-T, Recommendation G.107, June 1998.

[21] CommView. [online]. 2011 [สืบค้นวันที่ 15 มกราคม 2558]; http://www.tamos.com/products/commview/.

[22] สมนึก พ่วงพรพิทักษ์, เดชสิทธิ์ พรรษา. การปรับปรุงความมั่นคงชุดซอฟต์แวร์บริการโทรศัพท์ผ่านอินเทอร์เน็ตพร้อมทั้งประเมินคุณภาพ. ทุนวิจัยการพัฒนาเทคโนโลยีเพื่อความมั่นคงปลอดภัย ไซเบอร์, สำนักงานคณะกรรมการวิจัยแห่งชาติ, งบประมาณ 2556.

[23] Cain & Abel. [online]. 2008 [สืบค้นวันที่ 15 มกราคม 2558]; http://windowsvista4u.blogspot.com/2008/11/kb003.html.

[24] Wireshark. [online]. 2008 [สืบค้นวันที่ 15 มกราคม 2558]; http://nisaratmsit.exteen.com/

[25] BackTrack. [online]. 2012 [สืบค้นวันที่ 15 มกราคม 2558]; http://www.itclickme.com/2012/12/backtrack-backtrack.html

[26] คณะกรรมการกิจการโทรคมนาคมแห่งชาติ, “มาตรฐานสำหรับการให้บริการเสียงผ่านการให้บริการอินเทอร์เน็ต”, http://standard1.nbtc.go.th/getattachment/5b040c16-0dba-4e3c-bbb5-971c91ab68ed/qosvoip.aspx, 13 ตุลาคม 2551.

[27] IP-PBX. [online]. 2012 [สืบค้นวันที่ 25 กรกฎาคม 2558]; http://asteriskvoipkmitl.blogspot.com/2009/09/ip-pbx.html

[28] รู้จักกับ Asterisk ผู้นำโอเพ่นซอร์ส IP-PBX. [online]. 2012 [สืบค้นวันที่ 25 กรกฎาคม 2558]; http://voip.sit.kmutt.ac.th/asterisk.html

ภาคผนวก

ภาคผนวก ก
การติดตั้งและการใช้งาน isanbox V 3.0 เบื้องต้น

การติดตั้งและใช้งาน isanbox v 3.0 เบื้องต้น สามารถดาวน์โหลดเอกสารเพิ่มได้ที่ https://isan.msu.ac.th

1. หน้าเริ่มต้นการติดตั้ง isanbox กด enter

2. เลือกภาษา(English) กด ok

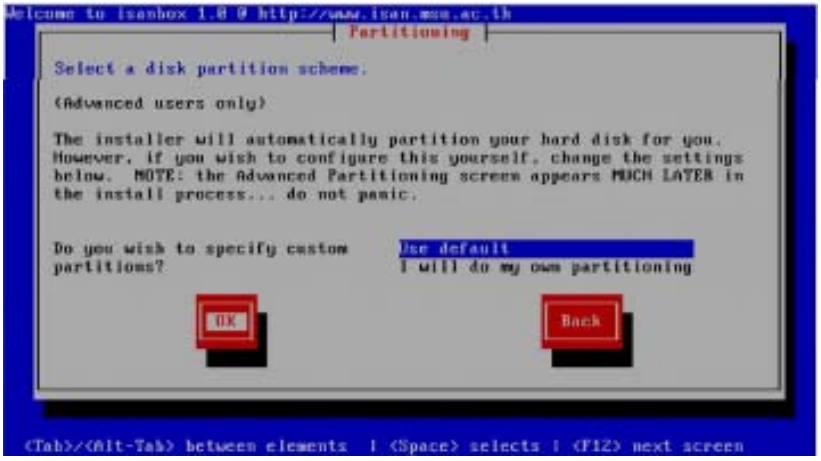
3. เลือกคีบอร์ด (us) กด ok

4. เลือกการติดตั้ง (local CDROM) กด ok

5. ทำการกำหนด IP address โดยเลือก Manual configuration แล้วกด ok

6. กำหนด IP address (IP ,Gateway , DNS) เสร็จแล้ว กด ok

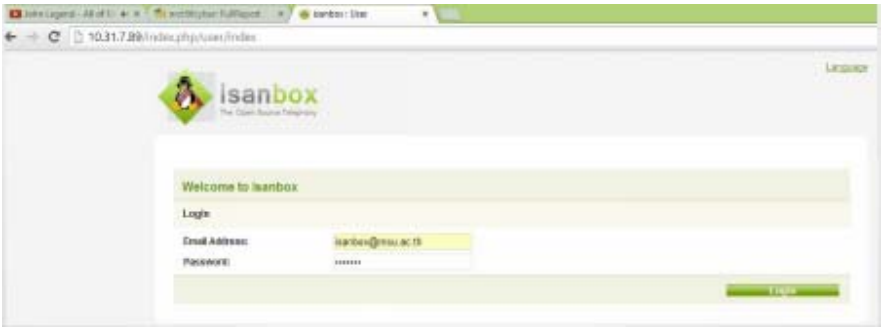
7. กำหนดรหัสผ่านให้กับ root เสร็จแล้ว กด ok



8. กำหนด partition เลือก Use default แล้วกด ok รอให้ระบบทำการติดตั้งเสร็จสิ้น

9. การติดตั้งระบบเสร็จสมบูรณ์ กด Reboot

10. Reboot เข้าใช้งาน isanbox



11. เปิด Browser แล้วพิมพ์ IP address ในช่อง URL ก็จะปรากฏ หน้า Login ของ isanbox จากนั้น กรอก email address และ password เพื่อเข้าระบบ

12. หน้า admin

13. เพิ่มเบอร์โทรไปที่ Routing >> Number Manger ซึ่งจะเข้าหน้าสำหรับจัดการหมายเลข เบอร์ทั้งหมด ต้องการเพิ่มหมายเลขใหม่ ก็ กด add a number

14. จากนั้นใส่หมายเลขเบอร์โทรที่ต้องการ และกดเลือกการจัดการดังรูป จากนั้น กด save

15. การจัดการ Device การเพิ่มอุปกรณ์ Device ไปที่ Destinations >> Device ซึ่งจะเข้าสู้หน้าสำหรับจัดการอุปกรณ์ รวมถึง SIP User ต้องการเพิ่ม กด Add device

16. การตั้งชื่อ Device ตามหมายเลข1 กำหนดเบอร์ให้ Device ตามหมายเลข 2 กำหนด Username และ Password กรอกข้อมูลเสร็จ กด save ตามหมายเลข 3

ประวัติย่อผู้วิจัย

ประวัติย่อผู้วิจัย

ชื่อ นามสกุล	นายสำเริง คำมีวงษ์
วัน เดือน ปีเกิด	วันที่ 28 กรกฎาคม พ.ศ. 2525
จังหวัด และประเทศที่เกิด	จังหวัดศรีสะเกษ ประเทศไทย
ประวัติการศึกษา	พ.ศ. 2540 มัธยมศึกษาตอนต้น โรงเรียนไพรบึงวิทยาคม อำเภอไพรบึง จังหวัดศรีสะเกษ
	พ.ศ. 2543 มัธยมศึกษาตอนปลาย โรงเรียนขุนหาญวิทยาสรรค์ อำเภอขุนหาญ จังหวัดศรีสะเกษ
	พ.ศ. 2547 ปริญญาครุศาสตรบัณฑิต (ค.บ.) สาขาคอมพิวเตอร์ศึกษา มหาวิทยาลัยราชภัฏร้อยเอ็ด
	พ.ศ. 2558 ปริญญาวิทยาศาสตรมหาบัณฑิต (วท.ม.) สาขาวิชาเทคโนโลยีสารสนเทศ มหาวิทยาลัยมหาสารคาม
ตำแหน่ง สถานที่ทำงาน	นักวิชาการคอมพิวเตอร์ ศูนย์คอมพิวเตอร์ มหาวิทยาลัยราชภัฏร้อยเอ็ด
ที่อยู่ที่สามารถติดต่อได้	บ้านเลขที่ 108 หมู่ 4 ตำบลโพธิ์กระสังข์ อำเภอขุนหาญ จังหวัดศรีสะเกษ